

Arcot RiskFort™

管理ガイド

バージョン 2.2.6



455 West Maude Avenue, Sunnyvale, CA 94085

Arcot RiskFort 管理ガイド

バージョン 2.2.6

2010 年 9 月

部品番号：RF-0226-00AG-10

Copyright © 2010 Arcot Systems, Inc. All rights reserved.

本書、および本書に記載されたソフトウェアは、ライセンスに基づいて提供され、ライセンスの条件に従ってのみ使用またはコピーすることが許可されています。本書の内容は情報提供のみを目的としています。本書は予告なしに改訂される場合があります、Arcot Systems は内容に関する責任は問われないものとします。

Arcot Systems は、本書に関して一切の保証も負わないものとします。本書は、商品性の黙示の保証、特定目的適合性の黙示の保証、または第三者の権利の不侵害の黙示の保証から構成されています（ただし、これらに限定されません）。Arcot Systems は、本書の記載の誤り、または本書の提供、記載内容の実行、あるいは使用に関連する、直接的、間接的、特例的、付帯的、もしくは結果的損害について責任を負いません。

ソフトウェア ライセンスによって許可される場合を除き、Arcot Systems, Inc の書面による事前の承諾なしに、本書のいかなる部分も、いかなる形式または手段であっても、複製、検索システムへの保存、または伝送を行うことはできません。

商標

Arcot®、ArcotID®、WebFort、WebFort VAS® は、Arcot Systems, Inc の登録商標です。Arcot logo™、認証機関のキャッチ コピー、ArcotID Client™、ArcotOTP™、ProxyFort™、RegFort™、RiskFort™、SignFort™、TransFort™、および Arcot Adapter™ はすべて Arcot Systems, Inc の商標です。

他のすべての製品名または会社名は、それぞれ各社の商標です。

特許

このソフトウェアは、米国特許第 6,170,058 号、6,209,102 号および他の出願中の特許によって保護されます。

Arcot Systems, Inc., 455 West Maude Avenue, Sunnyvale, CA 94085

サードパーティ ソフトウェア

RiskFort および関連するコンポーネントによって使用されるサードパーティ ソフトウェアはすべて、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の付録 G 「サードパーティ ソフトウェア ライセンス」にリスト表示されています。

目次

序文	xiii
対象読者	xiii
このガイドに含まれる情報	xiv
関連出版物	xv
本書の表記規則	xvi
サポートへのお問い合わせ	xvii
第 1 章	
Administration Console の概要	1
Administration Console について	1
Administration Console のエレメント	2
サポートされているロール	4
ユーザ	5
デフォルトの管理ロール	5
管理ロールのスコープ	7
Master Administrator	8
Global Administrator	9
Organization Administrator	9
User Administrator	10
管理者権限のサマリ	10
カスタム ロール	14
次の手順：迅速な管理	15
単純な展開の場合	15
複雑な展開の場合	17
第 2 章	
はじめに	21
Administration Console へのアクセス	21
パスワードとプロフィール情報の変更	23
Administration Console の設定	25
UDS の設定の更新	25

組織のグローバル設定の指定	29
キャッシュ リフレッシュ設定の指定	31
基本認証ポリシー設定の指定	32
基本認証のパスワード ポリシーの指定	33
第 3 章	
カスタム ロールの操作.....	35
カスタム ロールについて	35
カスタム ロールについて知っておくべきこと	36
事前定義済みカスタム ロール	36
カスタム ロールの作成	37
カスタム ロール情報の更新	39
カスタム ロールの削除	41
第 4 章	
RiskFort サーバ インスタンスの管理	43
サーバ接続の設定	43
トラスト ストアの作成	47
通信プロトコルの設定	48
SSL 通信の設定 (オプション)	53
サーバ インスタンスのリフレッシュまたはシャットダウン	54
サーバ インスタンスのリフレッシュ	54
Windows の場合	54
UNIX ベースのプラットフォームの場合	55
サーバ インスタンスの再起動	55
Windows の場合	55
UNIX ベースのプラットフォームの場合	55
第 5 章	
RiskFort ルールの基礎知識.....	57
評価ルール	59
既定ルール	59
設定可能な組み込みのルール	60
設定できない組み込みのルール	60
アドオン ルール	61
評価コールアウト	61
スコアリング エンジン	62

第 6 章**アドオン ルールの準備：ルール タイプの操作.....63**

システム定義のルール タイプ	63
数値比較	65
組み合わせ	65
RiskFort モデル	65
頻度	66
簡易リスト	66
マッピング（または導出）リスト	67
カスタム ルール タイプの操作	69
新しいルール タイプの追加	69
既存のルール タイプの表示	71
入力定義 XML のサンプル	73

第 7 章**グローバル ルール設定の管理.....75**

Global Administrator としてのログイン	76
Administration Console からのログアウト	79
Administration Console 使用時のセキュリティに関する推奨事項	80
ルール セットの設定	80
ルール セットについて	80
ルール セットの作成	81
トラステッド IP アドレスの設定	83
トラステッド IP アドレス範囲の追加	84
トラステッド IP アドレス範囲の更新	86
トラステッド IP アドレス範囲の削除	87
トラステッド アグリゲータの設定	87
トラステッド アグリゲータの追加	88
トラステッド アグリゲータの更新	93
トラステッド アグリゲータの削除	95
拒否 IP アドレスの設定	95
IP アドレス範囲の追加または削除	97
拒否 IP タイプの設定	98
[Negative Country List] の設定	102
ユーザ頻度の設定	105
デバイス頻度の設定	108

ゾーン ホッピングの設定	111
その他のルールの設定	115
関連コンセプト	115
ユーザ作成モード	115
マシン FingerPrint (MFP) のしきい値	116
その他のルール設定の指定	116
第 8 章	
スコアリングの設定	121
RiskFort のスコアリングについて	121
スコアリングの設定	122
運用環境への移行	125
第 9 章	
コールアウトの設定	131
コールアウトについて	132
コールアウトの実装	133
コールアウトのタイプ	135
評価コールアウト	135
スコアリング コールアウト	136
コールアウトの設定	137
評価コールアウトの設定	138
スコアリング コールアウトの設定	142
サンプル コールアウトでの作業	146
サンプル コールアウトの展開	147
Windows の場合	147
UNIX ベースのプラットフォームの場合	148
サンプル コールアウトと通信するために RiskFort サーバを設定する	148
サンプル コールアウトの使用	150
第 10 章	
組織の管理	151
組織の作成およびアクティブ化	152
Arcot リポジトリでの組織の作成	152
LDAP リポジトリでの組織の作成	156
組織の検索	162
組織情報の更新	164
組織情報の更新	165

RiskFort 固有の設定の更新	166
組織の無効化	167
組織の有効化	168
初期状態の組織のアクティブ化	169
組織の削除	170
第 11 章	
組織固有の RiskFort の設定の管理	173
組織固有の RiskFort 設定へのアクセス	173
ルール セットの作成	176
ルール セットの割り当て	176
グローバル設定の使用	179
組織のための RiskFort の設定	180
第 12 章	
アドオン ルールの操作.....	181
アドオン ルールについて	182
アドオン ルールの作成に使用するデータ エレメントと演算子	184
データ エレメント	184
論理演算子	185
アドオン ルールによって使用される追加入力エレメント	186
追加入力に関連する重要な注意事項	186
アドオン ルールの例	186
高額チェック	186
予期しない場所からの高速のユーザ頻度	187
予期しない場所からの高速のデバイス頻度	187
予期しない場所からの電子送金	188
アドオン ルールの操作	188
アドオン ルールの展開	188
展開したアドオン ルールの属性の編集	190
展開したアドオン ルールの削除	190
アドオン ルールのリスト データのアップロード	192
(単純な) リスト データのアップロード	192
マッピング (導出リスト) データのアップロード	195
第 13 章	
管理者の管理	199
管理者の作成	200

管理者アカウントのプロファイル情報の変更	203
管理者の検索	206
管理者アカウント情報の更新	209
管理者アカウントの無効化	213
管理者アカウントの有効化	214
管理者アカウントの削除	215
第 14 章	
ユーザの管理	217
ユーザの検索	218
ユーザ情報の更新	220
ユーザを管理者レベルへ上げる	222
ユーザ アカウントの無効化	225
ユーザ アカウントの有効化	227
ユーザ アカウントの削除	228
第 15 章	
ケースの管理	231
RiskFort ケースについて	232
ケースの基本	232
ケース管理のコンポーネント	233
ケース キュー	235
キュー サーバ	236
キュー監視スレッド	236
ケース ディスパッチャ モジュール	237
有効期限監視スレッド	238
ケース ロール	239
テクニカル サポート 担当者	239
ケースでの作業	239
カスタマ コールの処理	240
キュー マネージャ	240
不正行為アナリスト	241
ケース ロール権限サマリ	242
ケースの状態	243
新規	243
オープン	243
実行中	244

On Hold	244
期限切れ	244
Closed	245
ケースの状態権限の一覧	245
ケース管理ワークフロー	246
ケースの生成	246
ケースのキュー	247
ケースの割り当て	247
ケースの処理	248
ケースの期限切れ	249
不正行為の分析	249
ケース キューの管理	249
キューのステータスの表示	250
キューのステータスの更新	251
トランザクションの分析	253
手順 1：トランザクション サマリの表示	254
手順 2：ケース詳細の表示	257
手順 3：類似トランザクションの表示	262
関連するトランザクションの表示	263
手順 4：トランザクションに詳細調査のマークを付ける	263
ケースの処理	264
ケースでの作業（CSR）	264
顧客からの着信電話の管理（CSR）	269
不正行為統計レポートの生成	272
第 16 章	
レポートの管理	275
すべての管理者が使用可能なレポートのサマリ	276
管理者レポート	278
アクティビティ レポート	278
管理者アクティビティ レポート	280
ユーザ アクティビティ レポート	281
組織レポート	283
RiskFort レポート	285
リスク評価詳細アクティビティ レポート	286
リスク アドバイス サマリ レポート	290

トラステッド IP/ アグリゲータ レポート	291
トラステッド IP レポート	292
トラステッド アグリゲータ レポート	292
拒否 IP アドレス レポート	294
拒否国レポート	295
例外ユーザ レポート	295
アドオン ルール レポート	296
ルール データ レポート	298
ルール データ分類レポート	299
ケース管理レポート	300
レポートの生成	300
レポートを生成する場合の注意事項	300
レポートの生成	300
レポートをエクスポートする方法	301
第 17 章	
システム管理者のためのツール	303
DBUtil: RiskFort データベース ツール	303
マスタ キーをセットアップする	304
データベース ユーザ名とパスワードを挿入する	305
追加の DBUtil オプションを使用する	306
arrfversion: RiskFort モジュール バージョン表示ツール	307
arrfadmin: サーバリフレッシュとシャットダウン ツール	308
ツールを使用する前に	309
ツールの使用	310
サーバとの双方向 SSL 通信用のツールの設定	311
手順 1 : riskfortadminclient.ini の編集	311
サーバ管理プロトコルの設定	312
arrfserver: RiskFort サーバ ツール	314
ツールを対話型モードで実行する	314
arrfupload: Quova データ アップロード ツール	315
ツールを使用する前に	316
ツールの使用	317
付録 A	
RiskFort ロギング.....	321
ログ ファイルについて	321

インストール ログ ファイル	322
トランザクション ログ ファイル	323
RiskFort サーバ ログ	323
Case Management サーバ ログ ファイル	323
UDS ログ ファイル	324
Administration Console ログ ファイル	325
RiskFort サーバおよび Case Management サーバ ログ ファイルの形式	326
UDS および Administration Console のログ ファイルの形式	326
サポートされている重要度レベル	327
各ログ レベルのサンプル エントリ	328
FATAL	329
WARNING	329
INFO	329
DETAIL	330
付録 B	
用語集	333
索引	337

序文

Arcot RiskFort 2.2.6 管理ガイドでは、Arcot Administration Console を使用して Arcot RiskFort 2.2.6 をセットアップおよび管理するための情報を提供します。このガイドでは、Windows および UNIX ベースのプラットフォーム（Solaris SPARC® および Red Hat Enterprise Linux 4.0）の両方の情報について説明します。

このガイドで使用されているスクリーンショットでは、以下の表に指定されている**管理者名**を使用します。

表 A-1. このガイドのスクリーンショットで使用されている管理者

管理者名	管理者のロール
MASTERADMIN	Master Administrator
MPARKER	Global Administrator
RLAURIE	Organization Administrator
FANTONY	User Administrator
PRUSH	キュー マネージャ
RGRAHAM	不正行為アナリスト
JHUME	テクニカル サポート担当者（CSR）

対象読者

このガイドは Arcot RiskFort の管理者を対象としています。このガイドでは、Administration Console を使用して、メンテナンス、プロビジョニング、更新、パフォーマンスの監視、および RiskFort の設定変更に関連する通常の管理タスクを実行する方法について説明しています。

このガイドは、以下の経験を持つユーザを対象としています。

- オペレーティング システム ベースの管理
- 該当する Oracle または MS SQL データベース、あるいはその両方
- アプリケーション サーバおよび Web サーバの管理

このガイドに含まれる情報

このガイドは、以下の部分で構成されています。

- 第 1 章の「[Administration Console の概要](#)」では、RiskFort Administration Console インターフェースおよび管理階層について説明します。
- 第 2 章の「[はじめに](#)」では、システムを使い始めるために Master Administrator が実行する必要がある基本的な管理タスク（管理者の作成、Administration Console へのログインおよびログアウト、管理者パスワードの変更など）について説明します。また、管理者アカウントの作成、更新、および削除する手順についても説明します。
- 第 3 章の「[カスタム ロールの操作](#)」では、RiskFort でカスタムのロールを作成して適用するための Master Administrator の機能について取り上げます。
- 第 4 章の「[RiskFort サーバ インスタンスの管理](#)」では、Master Administrator が RiskFort サーバおよび Case Management Queuing Server インスタンスをセットアップおよび管理する方法について説明します。
- 第 5 章の「[RiskFort ルールの基礎知識](#)」では、RiskFort のルールの基本事項について説明します。また、ルール カテゴリについても説明します。
- 第 6 章の「[アドオン ルールの準備：ルール タイプの操作](#)」では、Master Administrator がルール タイプを追加してアドオン ルールをサポートする方法について説明します。
- 第 7 章の「[グローバル ルール設定の管理](#)」では、Global Administrator がグローバルレベルで設定できる設定、およびシステムに設定された個別の組織が継承できる設定について説明します。
- 第 8 章の「[スコアリングの設定](#)」では、組織のビジネス ニーズに合わせて、Global Administrator が RiskFort のスコアリングを設定する方法について説明します。
- 第 9 章の「[コールアウトの設定](#)」では、ビジネス ニーズに合わせて、Global Administrator がカスタムのコールアウトを設定する方法について説明します。
- 第 10 章の「[組織の管理](#)」では、Organization Administrator が RiskFort で組織の作成、検索、アクティブ化、有効化、無効化、削除を行う方法について説明します。また、この章ではグローバルレベルでは設定できない組織固有の設定を管理するためのタスクについても説明します。
- 第 11 章の「[組織固有の RiskFort の設定の管理](#)」では、グローバルレベルでは設定できない組織固有の設定を Organization Administrator が管理するためのタスクについて説明します。

- 第 12 章の「アドオン ルールの操作」では、RiskFort の機能を拡張してビジネス ニーズを満たすために、Organization Administrator が追加のビジネス ルールを設定す る方法について説明します。
- 第 13 章の「管理者の管理」では、システムでさまざまな管理者の作成、検索、アク ティブ化、有効化、無効化、削除を行う方法について説明します。
- 第 14 章の「ユーザの管理」では、Administration Console を使用してエンド ユーザの 検索、アクティブ化、有効化、無効化、削除を行う方法について説明します。
- 第 15 章の「ケースの管理」では、ケース管理と呼ばれる RiskFort の機能、ケース管 理者が実行する機能、およびケースを表示および更新する手順について説明します。
- 第 16 章の「レポートの管理」では、各管理レベルで使用可能なレポートについて説 明します。また、これらのレポートの使用方法についても説明します。
- 第 17 章の「システム管理者のためのツール」では、システムの監視および管理のた めにシステム管理者が使用できる RiskFort のツールについて説明します。
- 付録 A の「RiskFort ロギング」では、RiskFort のすべてのログ ファイル、そのファ イルに記録される重大度レベル、およびこれらのファイルのエントリ形式に関する 情報を取り上げます。
- 付録 B の「用語集」では、ガイドで使用される重要な用語をリスト表示していま す。

関連出版物

その他の関連出版物には以下のものが含まれます。

Arcot RiskFort 2.2.6 インストールおよ び展開ガイド	このガイドでは、RiskFort とそのコンポーネントのインストール および設定について説明します。
Arcot RiskFort 2.2.6 Java 開発者ガイド	このガイドでは、RiskFort が提供する Java API と、その API の 使用方法についても説明します。
Arcot RiskFort 2.2.6 クイック インス トール ガイド	このガイドでは、RiskFort のインストールに必要なタスクの概要 を説明します。

本書の表記規則

このマニュアルの表記規則、形式、および範囲を以下のパラグラフで説明します。

表記規則

このマニュアルでは以下の表記規則を使用しています。

<i>斜体</i>	強調、ガイド名
太字	ユーザ入力、GUI 画面のテキスト
固定幅フォント	ファイルおよびディレクトリ名、拡張子、コマンド プロンプト、CLI のテキスト、実行時のテキストのコード
固定幅太字フォント	パスのターゲット ファイルまたはディレクトリ名
固定幅フォント	コマンド プロンプト、CLI のテキスト、コード
固定幅斜体フォント	ユーザごとに異なる場合があるファイルまたはディレクトリ名
リンク	このガイド内のリンク、URL リンク

形式

このマニュアルでは、以下の形式を使用して特別なメッセージを強調表示しています。

	注： 重要な情報、または特に注目すべき情報を強調表示します。
	ヒント： 時間やリソースを節約する手順を強調表示します。
	警告： このタイプの注意を無視すると、機器に誤動作または損傷が発生する場合があります。



重要：操作を実行する前に知っておくべき情報を示します。



注意：考えられる危険性に対してユーザの注意を喚起します。



関連文書：他のガイドへの参照情報を提供します。

サポートへのお問い合わせ

サポートが必要な場合は、以下の Arcot サポートにお問い合わせください。

E-MAIL (電子メール)	support@arcot.com
Web サイト	http://www.arcot.com/support/index.html

第 1 章

Administration Console の概要

Arcot Administration Console（本ガイドでは以下「Administration Console」）は、操作およびシステム管理用の Web ベースのツールです。Administration Console は、すべての Arcot 製品を管理するための、一貫性のある統合されたインターフェースを提供します。

このコンソールは真のマルチテナント アーキテクチャを提供します。これにより、コンソールの 1 つのインスタンスを使用して、企業内の複数の組織または業務部門を管理できます。このモデルでは、組織または業務部門にそれぞれ独自の設定を使用して個別にセットアップできます。一方で、Administration Console では、システム レベルの設定データを継承して、各組織の特定の設定のみを構築することができます。

この章では、Administration Console のインターフェース、およびサポートされている管理者階層について説明します。この章では、以下のトピックについて説明します。

- [Administration Console について](#)
- [Administration Console のエレメント](#)
- [サポートされているロール](#)
- [次の手順：迅速な管理](#)



注：Administration Console で推奨されているデスクトップ画面の解像度は 1024 x 768 です。

Administration Console について

Administration Console は Web ブラウザ ベースのグラフィカル ユーザ インターフェースです。Administration Console には、サーバにネットワークからアクセスできるサポート対象のすべての Web ブラウザからアクセスできます。このコンソールを使用して、展開されたすべての RiskFort インスタンスを管理できます。インスタンスとは、特定のポートで使用可能な RiskFort サーバを表します。

Administration Console を使用して、RiskFort を設定したり、ユーザおよび管理用のロールをセットアップしたり、以下のようなその他の管理操作および設定タスクを実行できます。

- サーバとその他の RiskFort コンポーネント間の通信パラメータの設定
- ビジネス要件に沿った RiskFort ルールの設定
- 組織、管理者、およびユーザの管理
- 管理、トランザクション、ケース管理、および設定のレポートの生成

実行が承認されているタスクは、Administration Console のさまざまなタブに表示されます。これらのタスクは、所属するユーザグループ（またはロール）、およびこのロールが持つ管理者権限に基づきます。

Administration Console のエレメント

通常の管理画面は、以下のエレメントに分けることができます。

- ヘッダ
- メインメニュー
- サブメニュー
- タスク
- 本体

図 1-1 に、これらのエレメントの Administration Console 内の配置を示します。

図 1-1 Administration Console の一般的なレイアウト

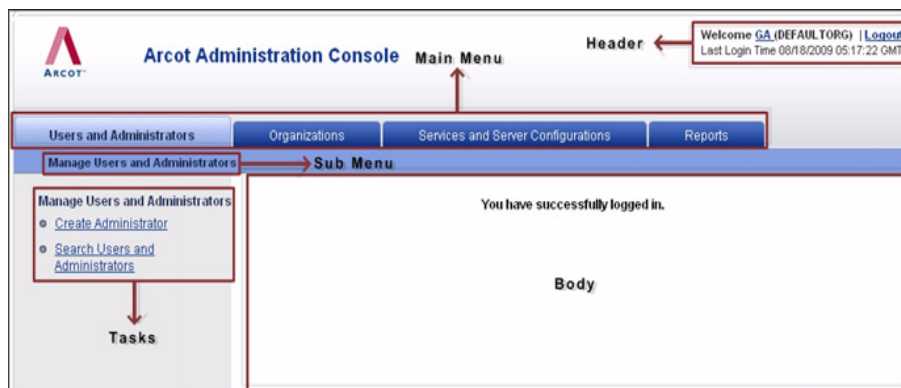


表 1-1 では、これらのエレメントについて説明します。

表 1-1. Administration Console のエレメント

エレメント	説明
ヘッダ	ログイン情報（管理者名、現在の組織、最終ログイン日時）を表示します。 ヘッダのリンクを使用して、以下を行うことができます。 - プロフィール情報（名前、電話番号、電子メール ID）および現在のパスワードの変更。今後実行するすべてのタスクで、優先される組織として使用する組織を指定することもできます。 - Administration Console からのログアウト。
メイン メニュー	現在の管理者が使用可能なメイン設定および管理オプションを表示します。
サブ メニュー	クリックしたメイン メニュー項目で使用可能なオプションを表示します。
タスク	クリックしたサブ メニュー項目で使用可能なタスクを表示します。
本体	選択したタスクの対応するページを表示します。

コンソール メッセージ

図 1-2 に示すように、Administration Console の使用中に生成されるすべての情報、警告、およびエラー メッセージは本体ページの [Title] の下に表示されます。

エラー メッセージは赤で表示され（図 1-2 を参照）、成功を示すメッセージは青で表示されます。図 1-3 に示すように、追加の手順もこれらのメッセージに含まれます。

図 1-2 コンソール メッセージ：エラー

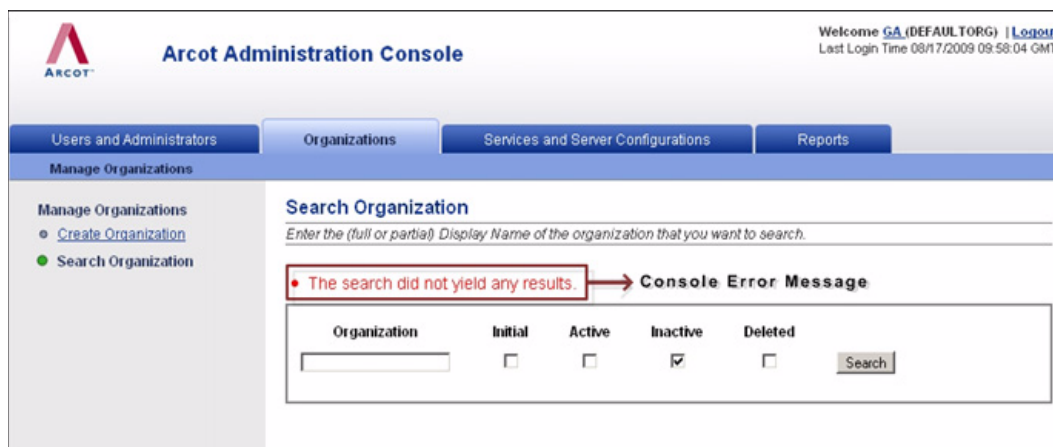
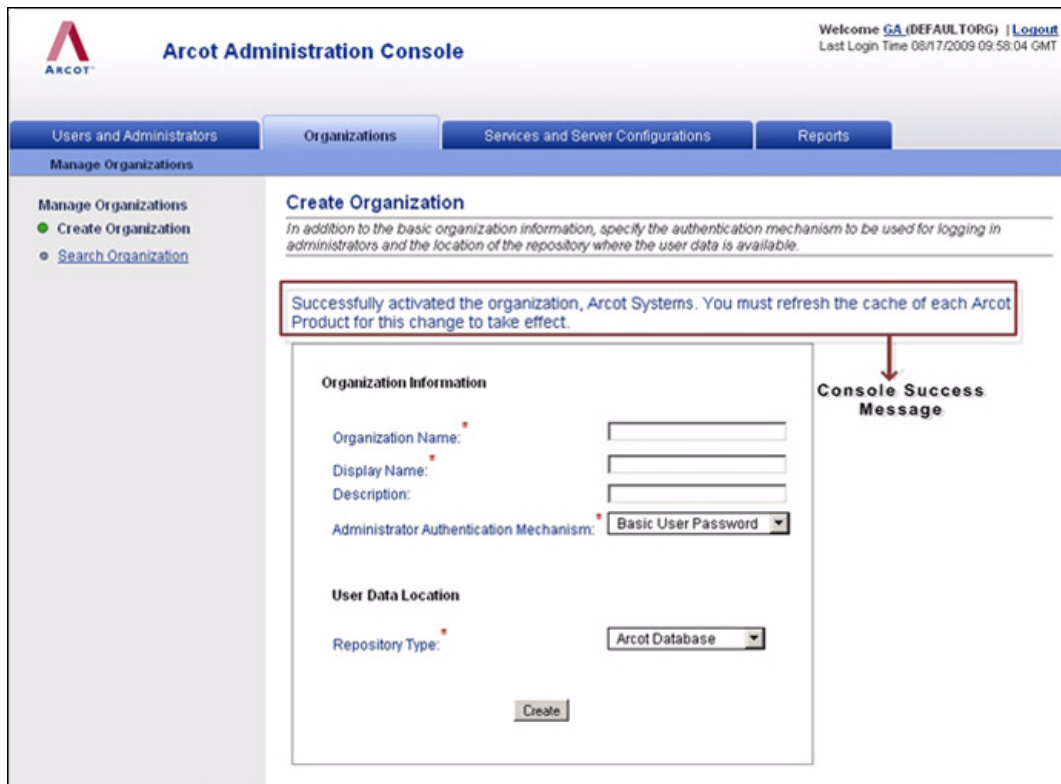


図 1-3 コンソール メッセージ：成功



サポートされているロール

ロールを使用すると、ユーザまたは同様の責務を共有するユーザセットに割り当てる操作および権限を指定できます。ユーザが特定のロールに割り当てられると、ユーザはそのロールに関連付けられたタスクと呼ばれる機能セットを使用できるようになります。その結果、管理者はシステム内の各ユーザに割り当てるタスクを細かく管理することができます。

Arcot Administration Console では、管理階層のセットアップや管理者への権限の割り当てを柔軟に行うことができます。さまざまなレベルの管理者を作成し、それぞれに異なるレベルのアクセス権を持たせることができます。また、他のユーザに管理タスクを順に委任できる管理者を作成することもできます。

Administration Console では、以下のタイプのロールをサポートしています。

- ユーザ
- デフォルトの管理ロール
- カスタム ロール

ユーザ

Arcot Administration Console では、オンライン アプリケーション システムのすべてのエンド ユーザをユーザと呼びます。このユーザは、Lightweight Directory Access Protocol (LDAP) リポジトリまたは Arcot データベースのいずれかに存在します。

ユーザがすでに LDAP システムに存在する場合は、組織の LDAP 属性を Arcot のサポートされている属性にマップする必要があります。その方法の詳細については、[第 10 章の「LDAP リポジトリでの組織の作成」](#)を参照してください。

RiskFort データベースにユーザを登録するには、リポジトリ タイプが Arcot データベースである組織を選択します。その方法の詳細については、[第 10 章の「Arcot リポジトリでの組織の作成」](#)を参照してください。

デフォルトの管理ロール

Administration Console には、詳細な設定を実行できる、[Master Administrator](#) と呼ばれる既定の管理ユーザが付属しています。これ以外は、ユーザに管理ロールを割り当てて、RiskFort システムの管理およびビジネス データへのアクセスを行う必要があります。通常、管理ロールは、ジョブ機能プロファイルとこれらの権限を適用できるスコープに基づいた権限セットで構成されます。管理権限を持つユーザは、管理ユーザと呼ばれます。



注：各管理ロールで使用可能な権限の全体的なリストについては、[「管理者権限のサマリ」](#)を参照してください。

Administration Console では、以下の事前定義済みの管理ロールをサポートしています。

- [Master Administrator](#)
- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

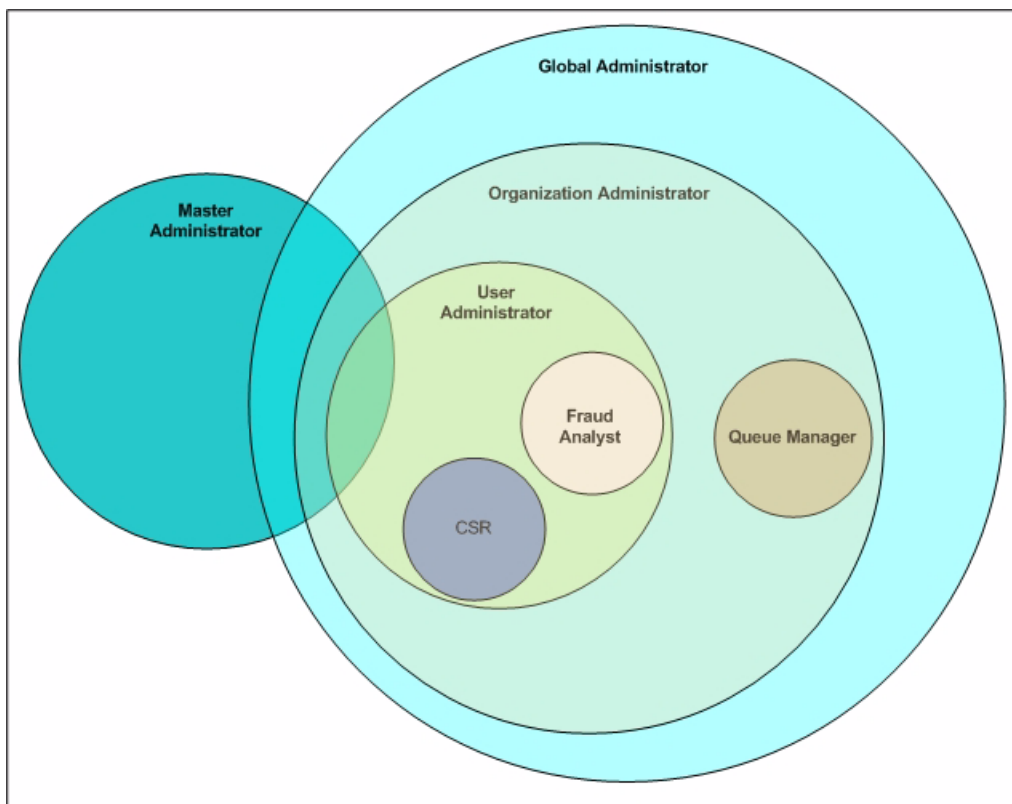
また、**カスタム ロール**を作成することもできます。



注：管理者もシステムのユーザと見なされます。

図 1-4 に、管理ロールと、管理ロールで使用可能な権限の関係を示します。また、この図の後のセクションでは、サポートされている管理者レベルを詳しく説明します。

図 1-4 管理ロールおよびロール間の関係



注：図 1-4 に見られるように、権限は階層的に分配されているため、管理者が固定された境界を越えてアクセスすることはできません。各レベルには事前定義済みの権限またはロールがあります。

管理ロールのスコープ

Arcot Administration Console での管理ロールのスコープは、以下のもので構成されています。

- 特定のロールを持つ管理者が管理できるすべての組織。
- ロールに関連付けられた権限。

スコープに関する重要な注意事項

管理ロールを作成する場合は、以下の点に注意する必要があります。

- **Master Administrator** のスコープは、デフォルトでは**すべての組織**が対象です。またこの管理者は、既存の組織と今後作成されるその他の組織の**すべて**を管理します。
- ロール (**Global Administrator**、**Organization Administrator**、または **User Administrator**) は管理階層の下のみを管理でき、上を管理することはできません。つまり、子ロールを管理するロールは、その子の親を管理しないように定義されています。

たとえば Global Administrator は、スコープが自分よりも狭い他の Global Administrator、Organization Administrator、および User Administrator を管理できます。一方で、Master Administrator を管理することはできません。

- **Global Administrator** ロールのスコープを、すべての組織に設定することができます。その場合、既存のすべての組織に加えて、将来作成される組織もこのロールで管理できます。
- **Organization Administrator**、または **User Administrator** のロールは、特定の組織のみを管理するように制限できます。
- 管理者が**カスタム ロール**を使用して作成された場合、作成された管理者は親レベルと同じレベルに所属します。

たとえば、Global Administrator から *MyGlobalAdmin* という管理者を作成した場合、*MyGlobalAdmin* に *Organization Administrator* や *User Administrator* よりも少ない**権限**を割り当てたととしても、*MyGlobalAdmin* は *Global Administrator* であると見なされます。



注： **Organization Administrator** または **User Administrator** のスコープをすべての組織に設定しないでください。

Master Administrator

Master Administrator (MA) はシステムのスーパーユーザです。Master Administrator にはシステム全体に対して無制限のアクセス権があります。MA のデフォルト スコープはすべての組織です。そのため、既存のすべての組織に加えて、今後 Master Administrator または他の管理者が作成する組織を管理できます。

MA の主な職責は以下のとおりです。

- インストールの後にシステムのブートストラップを実行します（または初期化します）。
- ユーザ データ サービス (UDS) の接続パラメータを設定します。
- 組織のグローバル設定、および Administration Console のキャッシュ リフレッシュの設定を行います。
- RiskFort サーバの通信パラメータを設定します。
- RiskFort サーバのプロトコルを設定します。
- Administration Console およびサーバ コンポーネントの認証メカニズム、およびその他の設定を行います。
- 必要に応じて組織を作成し、管理します。
- 必要に応じて、任意のロール (Global Administrator、Organization Administrator、または User Administrator) の管理者を作成し、管理します。
- **カスタム ロール**を管理します。

Administration Console の展開が成功したら、最初は MA としてログインする必要があります。MA アカウント ([masteradmin](#)) の出荷時のデフォルト パスワードは [master1234!](#) です。MA のアクションはシステム全体のセキュリティに影響する可能性があるため、コンソールに初めてログインしたときにこのパスワードを変更することを強くお勧めします。また、このパスワードを保護し、定期的に変更することをお勧めします。



注： MA アカウントがロックされた場合は、Arcot テクニカル サポート (support@arcot.com) に連絡する必要があります。

MA は、データを追跡して分析するために、自分のすべてのアクティビティの総合的なレポートを生成できるだけでなく、システム内の他の管理者のアクティビティのレポートも生成できます。また、すべての組織のレポートやすべてのサーバ設定のレポートも生成できます。

Global Administrator

Global Administrator (GA) は、管理階層の 2 番目のレベルです。この管理者は、システムのブートストラップ、Administration Console の初期設定の実行、サーバ設定の指定、カスタム ロールの管理を除く、MA のほとんどのタスクを実行できます。

通常、GA を作成する場合は、GA のスコープを指定する必要があります。スコープを指定しないと、組織を管理できません。

GA の主なタスクは以下のとおりです。

- 必要に応じて、他の Global Administrator、Organization Administrator、または User Administrator を作成し、管理します。
- Administration Console の認証ポリシーを設定します。
- 必要に応じて組織を作成し、管理します。



注：これには組織の詳細の編集が含まれます。

- ユーザのクレデンシャルを管理します。
- RiskFort ルールおよびスコアリングを設定します。
- 設定を割り当てます。
- コールアウトおよびアドオン ルールを設定します。

GA は、使用可能な情報を追跡して分析するために、自分の管理権限の範囲内にある組織のすべての管理アクティビティ、設定、およびケース管理のレポートを生成して表示できます。また、自分に割り当てられたすべての組織と User Administrator のレポートも表示できます。

Organization Administrator

Organization Administrator (OA) は、管理階層の 3 番目のレベルです。この管理者は、MA または GA のいずれかが OA に割り当てた組織と、その組織に所属するユーザの管理に関連するすべてのタスクを実行できます。タスクには、以下のものがあります。

- 必要に応じて、他の Organization Administrator または User Administrator を作成し、管理します。
- 自分の権限の範囲内にある組織を管理します。
- Administration Console の認証ポリシーを設定します。

- 組織固有の設定を管理（更新）します。
- 自分の権限の範囲内にある組織に所属するユーザを管理します。

OA を作成する場合は、OA のスコープを指定する必要があります。スコープを指定しないと、組織を管理できません。

OA は、自分の管理権限の範囲内にある組織の管理アクティビティ、設定、およびトランザクションのレポートを生成して表示できます。また、自分に割り当てられたすべての User Administrator のレポートも表示できます。

User Administrator

User Administrator (UA) ロールは、管理階層の一番下のレベルです。この管理者は、MA または GA のいずれかが UA に割り当てた組織のユーザ管理に関連するすべてのタスクを実行できます。タスクには、以下のものがあります。

- 必要に応じて他の UA を作成し、管理します。
- 必要に応じて、自分の権限の範囲内にある組織のユーザを管理します。



注：これにはユーザの詳細の編集が含まれます。

- エンド ユーザのケースを管理します。

UA を作成する場合、UA のスコープを指定する必要があります。スコープを指定しないと、組織を管理できません。

UA は、自分の管理権限の範囲内にある組織のユーザおよび UA アクティビティのレポートを生成して表示できます。

管理者権限のサマリ

表 1-2 に、サポートされている 3 つのレベルの管理者が使用可能な権限を要約して示します。

表で使用されている列名の頭字語の意味は以下のとおりです。

- Master Administrator -> **MA**
- Global Administrator -> **GA**
- Organization Administrator -> **OA**
- User Administrator -> **UA**



注：✓ という記号は、指定されたレベルの管理者が使用可能なアクション（または権限）であることを示します。

表 1-2. 管理者権限のサマリ

機能	タスク	MA	GA	OA	UA
ユーザ データ サービス (UDS) の管理	グローバル ユーザ データ サービス (UDS) の設定の更新	✓			
デフォルトの組織の管理	デフォルトの組織の設定	✓			
キャッシュ管理	キャッシュ リフレッシュ設定の更新	✓			
認証ポリシーの管理	基本認証ポリシーの更新	✓	✓	✓	
システム設定管理	RiskFort の接続	✓			
	信頼された証明機関	✓			
	プロトコルの設定	✓			
アドオン ルールの管理	ルール タイプの追加	✓			
	既存のルール タイプの表示	✓			
カスタム ロールの管理	カスタム ロールの作成	✓			
	カスタム ロールの更新	✓			
	カスタム ロールの削除	✓			
Global Administrator アカウ ントの管理	Global Administrator アカウ ントの作成	✓	✓		
	Global Administrator の詳細の検索また は表示	✓	✓		✓
	Global Administrator アカウ ント情報の 更新	✓	✓		✓
	Global Administrator アカウ ントの有効 化	✓	✓		
	Global Administrator アカウ ントの無効 化	✓	✓		
	Global Administrator アカウ ントの削除	✓	✓		

表 1-2. 管理者権限のサマリ

機能	タスク	MA	GA	OA	UA
Organization Administrator アカウントの管理	Organization Administrator アカウントの作成	✓	✓	✓	
	Organization Administrator の詳細の検索または表示	✓	✓	✓	✓
	Organization Administrator アカウント情報の更新	✓	✓	✓	✓
	Organization Administrator アカウントの有効化	✓	✓	✓	
	Organization Administrator アカウントの無効化	✓	✓	✓	
	Organization Administrator アカウントの削除	✓	✓	✓	
User Administrator アカウントの管理	User Administrator アカウントの作成	✓	✓	✓	
	User Administrator の詳細の検索または表示	✓	✓	✓	✓
	User Administrator アカウント情報の更新	✓	✓	✓	✓
	User Administrator アカウントの有効化	✓	✓	✓	✓
	User Administrator アカウントの無効化	✓	✓	✓	✓
	User Administrator アカウントの削除	✓	✓	✓	
組織管理	組織の作成	✓	✓	✓	
	組織の詳細の検索および表示	✓	✓	✓	✓
	組織情報の更新	✓	✓	✓	
	組織のアクティブ化	✓	✓	✓	✓
	組織の非アクティブ化	✓	✓	✓	✓
	組織の削除	✓	✓		

表 1-2. 管理者権限のサマリ

機能	タスク	MA	GA	OA	UA
ユーザの管理	ユーザの詳細の検索および表示	✓	✓	✓	✓
	ユーザ情報の更新	✓	✓	✓	✓
	ユーザのアクティブ化	✓	✓	✓	✓
	ユーザの非アクティブ化	✓	✓	✓	✓
	ユーザの削除	✓	✓	✓	✓
RiskFort の設定	ルール セットの作成		✓	✓	
	ルール セットの割り当て		✓	✓	
	拒否 IP アドレス リスト		✓	✓	
	拒否 IP タイプ		✓	✓	
	拒否国リスト		✓	✓	
	トラステッド IP/ アグリゲータ		✓	✓	
	ユーザ頻度		✓	✓	
	デバイス頻度		✓	✓	
	ゾーン ホッピング		✓	✓	
	アドオン ルールの設定		✓	✓	
	コールアウトの設定		✓	✓	
	ユーザ作成モード		✓	✓	
	マシンの FingerPrint (MFP) しきい値の許容範囲		✓	✓	
	スコアリングの設定		✓	✓	
	運用環境への移行		✓	✓	
ケース管理	ケースでの作業		✓	✓	✓
	着信コールの管理		✓	✓	✓
	トランザクションの分析		✓	✓	
	不正行為統計レポート		✓	✓	
	キューの表示		✓	✓	
	キューの管理		✓	✓	

表 1-2. 管理者権限のサマリ

機能	タスク	MA	GA	OA	UA
レポート	アクティビティ レポート	✓	✓	✓	✓
	管理者アクティビティ レポート	✓	✓	✓	✓
	ユーザ アクティビティ レポート		✓	✓	✓
	組織レポート	✓	✓	✓	
	リスク評価詳細アクティビティ レポート		✓	✓	✓
	リスク アドバイス サマリ レポート		✓	✓	✓
	トラステッド IP/ アグリゲータ レポート		✓	✓	
	拒否 IP レポート		✓	✓	
	拒否国レポート		✓	✓	
	例外ユーザ レポート		✓	✓	✓
	アドオン ルール レポート		✓	✓	
	ルール データ レポート		✓	✓	
	ルール データ分類レポート		✓	✓	

カスタム ロール

MA は、以下のいずれかの事前定義済みの親ロールから権限のサブセットを継承する新しい管理ロールを作成することもできます。

- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

これらの役割はカスタム ロールと呼ばれ、親のロールに関連付けられたデフォルト権限の一部を**無効にすること**で作成されます。たとえば、GA の「組織の作成権限」を無効にする必要がある場合、この権限を無効にしてカスタム ロールを作成できます。

カスタム ロールを作成した場合、管理アカウントを作成または更新するときに、ロールオプションとして使用できるようになります。カスタム ロールは、作成するだけでなく更新および削除も行えます。

作成できるカスタム ロールの他に、RiskFort にはケース管理に必要な 3 つの事前定義済みカスタム ロール（図 1-4 を参照）が付属しています。これには以下のロールが含まれます。

- **QM：キュー マネージャ** ロールには、ケースを管理するために必要な権限が付属しています。
- **CSR：テクニカル サポート 担当者** のロールには、ケースに関する作業の場合や、必要に応じてエンド ユーザからの着信コールに対応する場合に必要な権限が付属しています。
- **FA：不正行為アナリスト** のロールには、ケースを分析して隠れた傾向やパターンを見つけるために必要な権限が付属しています。

これらのカスタム ロールの操作の詳細については、第 3 章の「カスタム ロールの操作」を参照してください。ケース管理の詳細については、第 15 章の「ケースの管理」を参照してください。

次の手順：迅速な管理

これまでに RiskFort Administration Console の概念を十分に理解していただいたため、このセクションでは展開を管理するための準備手順について簡単に説明します。そのため、ここでは以下のシナリオの簡単な概要について説明します。

- [単純な展開の場合](#)
- [複雑な展開の場合](#)

単純な展開の場合

通常、RiskFort の最も単純な実装では、小規模なユーザ基盤に適応可能な認証を提供します。この実装は、単一のシステムにインストールされたすべての RiskFort コンポーネントと Web アプリケーションで構成されます。データベースは、RiskFort がインストールされているのと同じシステム、または別のシステムで使用できます。



関連文書： このタイプの展開の詳細については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の第 2 章「展開の計画」を参照してください。

表 1-3 に、この展開タイプの一般的な特徴の概要を示します。

表 1-3. 単純な展開の特徴

特徴	詳細
展開のタイプ	• 開発、概念実証、初期テスト、または初期パイロット • 中小企業（SMB） • 企業内の地方展開
地理的な拡張	通常は 1 つの場所に制限
展開の必要条件	実装と管理の容易性

小規模の展開の場合には、ほとんどのデフォルト設定をすぐに使用できます。これは単一組織のシステムであるため、デフォルトの組織を使用できます。デフォルトの組織は、新しい組織をセットアップせずにシステムを初期化する場合に自動的に作成されます。したがって、OA アカウントも不要である場合があります。その場合は、必要な GA および UA アカウントのみを作成する必要があります。



注： このシステムに付属の SDK を使用して、RiskFort にエンド ユーザを作成できます。

SDK に付属の Javadoc を参照してください。また、「Arcot RiskFort 2.2.6 Java 開発者ガイド」でも詳しく説明しています。

ユーザの強力な認証をセットアップして管理を開始するための手順の**簡単な概要**を以下に示します。

1. RiskFort が正しくインストールおよび設定され、Administration Console およびユーザデータ サービスの WAR ファイルが展開されていることを確認します。



関連文書： RiskFort のインストール、WAR ファイルの展開、およびその他のインストール後タスクの実行については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の第 4 章「単一システムへの RiskFort の展開」を参照してください。

2. MA として Administration Console にログインし (2-21 ページの「[Administration Console へのアクセス](#)」を参照)、ブートストラップ ウィザードの手順に従ってシステムを初期化します。



関連文書： 詳細については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の第 4 章「システムのブートストラップ」を参照してください。

3. 必要な GA および UA アカウントを作成します。
詳細については、13-200 ページの「[管理者の作成](#)」を参照してください。
4. GA として、ビジネス要件を満たすために必要な RiskFort ルールを設定します。
詳細については、第 7 章の「[グローバル ルール設定の管理](#)」を参照してください。
5. ユーザを RiskFort に登録します。



注： 7-115 ページの「[暗黙ユーザ作成モード](#)」で組織を設定する場合、この手順は任意である場合があります。その場合、ユーザは最初のリスク評価の実行中に自動的に登録されます。

この目的のためには、RiskFort に付属の Java SDK を使用します。SDK 2.2.6 に付属の Javadoc を参照してください。

これにより、システムのリスク評価の設定が行われます。また、これでシステム (第 4 章の「[RiskFort サーバ インスタンスの管理](#)」)、管理者 (第 13 章の「[管理者の管理](#)」) およびユーザ (第 14 章の「[ユーザの管理](#)」) を管理できます。

複雑な展開の場合

展開が複雑な大企業で高可用性が不可欠である場合、大規模なユーザ基盤に適応可能な認証と、システムを管理する管理者を提供するように RiskFort を実装できます。このような展開では、RiskFort コンポーネントは異なるサーバにインストールされます。これは、セキュリティ、パフォーマンス、高可用性のために行われます。また、複数のアプリケーションで適応性のある認証機能を使用できます。



関連文書： このタイプの展開の詳細については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の第 2 章「展開の計画」を参照してください。

表 1-4 に、この展開タイプの一般的な特徴の概要を示します。

表 1-4. 分散された展開の特徴

特徴	詳細
展開のタイプ	• 中規模から大規模の複雑なビジネス • 企業での展開 • 段階的な展開
地理的な拡張	世界中に分散
展開の必要条件	• 実装と管理の容易性 • グローバルな可用性 • 高可用性

ユーザの強力な認証をセットアップして管理を開始するための手順の**簡単な概要**を以下に示します。

1. RiskFort が正しくインストールおよび設定され、Administration Console およびユーザデータ サービスの WAR ファイルが展開されていることを確認します。

	関連文書： RiskFort のインストール、WAR ファイルの展開、およびその他のインストール後タスクの実行については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の第 5 章「分散システムへの RiskFort の展開」を参照してください。

2. MA として Administration Console にログインし（[2-21 ページの「Administration Console へのアクセス」](#)を参照）、ブートストラップ ウィザードの手順に従ってシステムを初期化します。

	関連文書： 詳細については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の第 4 章「システムのブートストラップ」を参照してください。

3. Administration Console を設定します。これには、UDS の設定、組織のグローバル設定、Administration Console のキャッシュ設定、およびコンソールにログインするための基本的なユーザ名 / パスワード認証ポリシーが含まれます。

詳細については、[2-25 ページの「Administration Console の設定」](#)を参照してください。

4. さまざまなシステムの RiskFort サーバ インスタンスをセットアップします。

詳細については、[4-43 ページの「RiskFort サーバ インスタンスの管理」](#)を参照してください。

- Administration Console、SDK、および Web サービスが RiskFort サーバとの通信に使用するプロトコルを設定します。

詳細については、[4-48 ページの「通信プロトコルの設定」](#)を参照してください。

- 組織を計画して作成します。組織アーキテクチャはフラットです。また、作成した各組織を企業内の業務部門にマップできます。

詳細については、[10-152 ページの「組織の作成およびアクティブ化」](#)を参照してください。

- 必要に応じて、管理者 ([13-200 ページの「管理者の作成」](#)を参照) とカスタム ロール ([第 3 章の「カスタム ロールの操作」](#)を参照) を計画して作成します。

- ビジネス要件を満たすための適切なルールおよびルールセットを作成し、これらの設定を割り当てます。

詳細については、[7-75 ページの「グローバル ルール設定の管理」](#)を参照してください。

- ユーザを RiskFort に登録します。



注：暗黙ユーザ作成モードで組織を設定する場合、この手順は任意である場合があります。その場合、ユーザは最初リスク評価の実行中に自動的に登録されます。

この目的のためには、RiskFort に付属の Java SDK を使用します。SDK 2.2.6 に付属の Javadoc を参照してください。

- 必要に応じて、RiskFort サーバとクライアントの間に SSL ベースの通信を設定します。

詳細については、[4-47 ページの「トラスト ストアの作成」](#)を参照してください。

- アドオン ルールまたはコールアウトを使用して RiskFort 機能を拡張する場合は、必要な設定を定義して設定します。

詳細については、[第 12 章の「アドオン ルールの操作」](#) および [第 9 章の「コールアウトの設定」](#)を参照してください。

これにより、システムのリスク評価の設定が行われます。また、これでシステム ([第 4 章の「RiskFort サーバ インスタンスの管理」](#))、管理者 ([第 13 章の「管理者の管理」](#)) およびユーザ ([第 14 章の「ユーザの管理」](#)) を管理できます。

第 2 章 はじめに

この章では、RiskFort を正常にインストールし、コンソールを展開し、ブートストラップした後に、[Master Administrator](#) として Administration Console にログインして基本情報を設定するための手順について説明します。



関連文書： RiskFort のインストール、Administration Console の展開、およびそのブートストラップの詳細については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」を参照してください。

この章では、以下の内容について説明します。

- [Administration Console へのアクセス](#)
- [パスワードとプロファイル情報の変更](#)
- [Administration Console の設定](#)

Administration Console へのアクセス

デフォルトの Master Administrator (MA) アカунツは、Administration Console に初めてログインする場合に使用します。以下のデフォルトのクレデンシャルを使用してコンソールにログインします。

- ユーザ名 : `masteradmin`
- パスワード : `master1234!`

Administration Console にログインする方法

1. Web ブラウザ ウィンドウを開きます。
2. URL を入力して、Administration Console にアクセスします。Administration Console のデフォルトのアドレスは以下のとおりです。

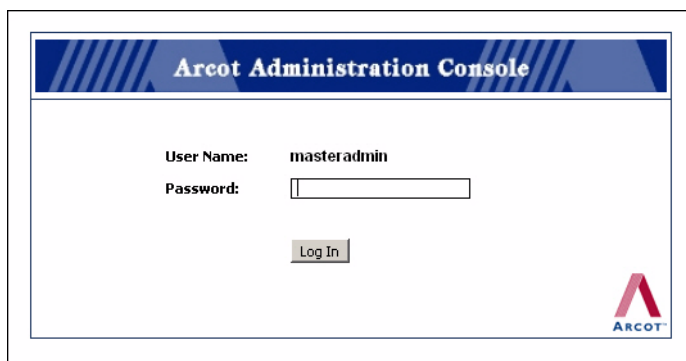
<http://< ホスト名 >:< ポート >/arcotadmin/masteradminlogin.htm>

前述の URL で以下の作業を行います。

- **ホスト名**および**ポート**は、それぞれ Administration Console を展開したシステムのホスト名または IP アドレスと、コンソールがリスニングしているポートに置換します。
- デフォルトのアプリケーション コンテキスト (`arcotadmin`) を変更した場合は、これを新しい値に置換する必要があります。

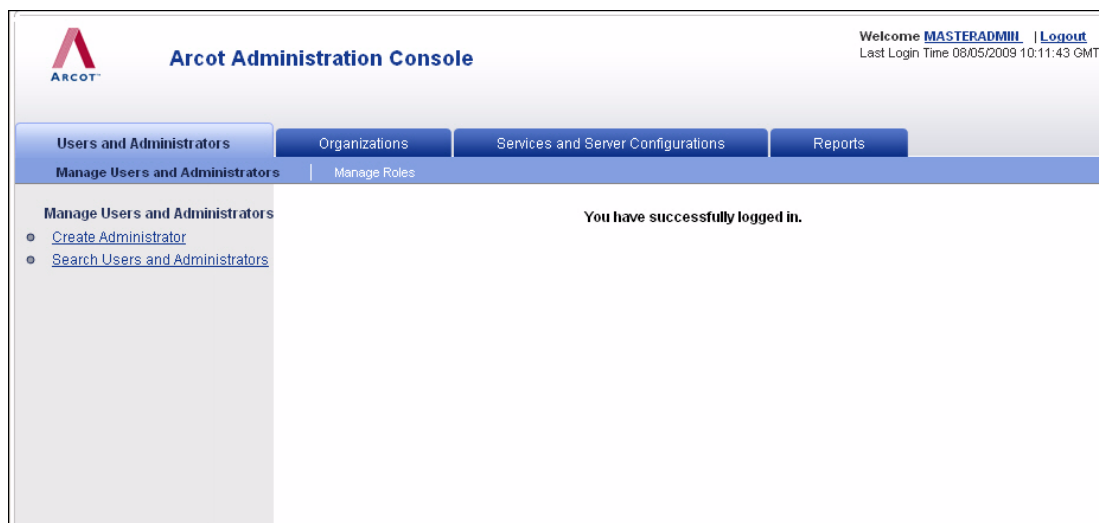
[Master Administrator Login] ページが表示されます (図 2-1 を参照)。

図 2-1 [Master Administrator Login] ページ



3. **master1234!** を [Password] フィールドに入力し、[Log In] をクリックします。Administration Console の先頭ページが表示されます (図 2-2 を参照)。

図 2-2 Master Administrator: Successfully Logged In



Administration Console 使用時のセキュリティに関する推奨事項

Administration Console の使用中にブラウザ セッションを悪用した悪意のある攻撃から RiskFort を保護するには、以下の内容を確認します。

- 他のアプリケーションとブラウザ セッションを共有しないようにします。
- コンソールでの作業中に他のサイトを開かないようにします。
- Administration Console には厳密なパスワード制限を設定します。
- Administration Console を使用した後は必ずログアウトします。
- セッションが終了したらブラウザ ウィンドウを閉じます。
- 実行する必要があるタスクに応じて、管理者に適切なロールを割り当てます。

Administration Console からのログアウト

Administration Console からログアウトするには、コンソールの右上隅にあるヘッダ領域で、[Logout] リンクをクリックします。

パスワードとプロフィール情報の変更

Arcot は、Master Administrator パスワードを定期的に変更し、高いセキュリティを維持することを強く推奨します。これにより、権限のないユーザが MA クレデンシャルを使用して Administration Console にアクセスするのを防ぐことができます。

 図 2-3 に示すように、[My Profile] ページを使用して、現在のパスワードと、今後実行する管理者関連のすべてのタスクがデフォルトで反映されている基本設定を変更します。

図 2-3 Master Administrator の [My Profile] ページ

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/15/2010 08:12:05 GMT

Users and Administrators Organizations Services and Server Configurations Reports

My Profile

Update your personal details and preferences.

Change Password

Current Password:

New Password:

Confirm Password:

Administrator Preferences

Enable Preferred Organization: ☐

Preferred Organization:

Time Zone:

現在のパスワードを変更する方法、および（または）ユーザの組織の基本設定を設定する方法

1. MA としてログインしていることを確認します。
2. コンソールヘッダの **[MASTERADMIN]** リンクをクリックします。
[My Profile] ページが表示されます（図 2-3 を参照）。
3. **[Change Password]** セクションで、以下のフィールドを指定します。
 - a. **[Current Password]**。
 - b. **[New Password]**。
 - c. **[Confirm Password]** フィールドに、新しいパスワードをもう一度入力します。
4. **[Administrator Preferences]** セクションで、以下のフィールドを指定します。
 - a. **[Enable Preferred Organization]** をオンにするかどうか。

この組織は、今後実行するすべての管理者関連のタスクの [Organization] フィールドで、デフォルトで選択されます。たとえば管理者を検索する場合、デフォルトでは優先される組織内で管理者が検索されます。

- b. 今後 [Organization] フィールドでデフォルトで選択される [Preferred Organization]。
- c. 優先される [Time Zone]。

この [Time Zone] は、今後コンソール ヘッダの [Last Login] のタイム スタンプで表示されます。さらに、[Transaction Date] などのレポート データや、ケース関連の日付およびタイム スタンプで、このタイムゾーンが使用されます。

- 5. [Save] をクリックします。

Administration Console の設定

RiskFort に固有の設定を行う前に、Administration Console のグローバル設定を行うことをお勧めします。グローバル設定には以下のものが含まれます。

- ユーザ データ サービス (UDS) の設定
- 組織のグローバル設定
- キャッシュ リフレッシュの設定
- 基本認証ポリシーの設定

以下のサブセクションでは、これらのグローバル設定を行うための手順について説明します。

UDS の設定の更新

ユーザ データ サービス (UDS) は、組織が展開したサードパーティのデータ リポジトリ (LDAP ディレクトリ サーバなど) へのアクセスを可能にするための Administration Console モジュールです。RiskFort および Administration Console は、UDS を使用して既存のデータにシームレスにアクセスしたり、エンド ユーザの情報を活用することができます。標準の Arcot SQL データベース テーブルにデータを複製する必要はありません。

通常、システムをブートストラップする間に UDS パラメータを指定します。ただし、UDS パラメータ設定を更新する場合は、[User Data Service Configuration] ページ (図 2-4) を使用して更新を行います。



注：UDS パラメータの設定の詳細については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の「システムのブートストラップ」のセクションを参照してください。

図 2-4 ユーザ データ サービスの設定：1 ページ

Arcot Administration Console

Welcome [MASTERADMIN](#) | [Logout](#)
Last Login Time 10/28/2009 09:40:02 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports

RiskFort | Administration Console

Administration Console

- **UDS Configuration**
 - [Organization Global Configuration](#)
 - [Cache Refresh Configuration](#)
- Authentication
 - [Basic Authentication Policy](#)

User Data Service Configuration

Configure the User Data Service (UDS) to access user information.
Note: It is optional to configure SSL between UDS and the Arcot Products.

User Data Service Configuration

Protocol :

Host :

Port :

Application Context Root :

Connection Timeout (in milliseconds) :

Read Timeout (in milliseconds) :

Idle Timeout (in milliseconds) :

Server Root Certificate : [Browse...](#)

Client Certificate : [Browse...](#)

Client Private Key : [Browse...](#)

Minimum Connections :

Maximum Connections :

[Next](#)

UDS の設定を更新する方法

1. MA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。
3. タブのサブメニューにある [Administration Console] をクリックします。
4. まだ [User Data Service Configuration] ページが表示されない場合は、[UDS Configuration] ページをクリックしてこのページを表示します (図 2-4 を参照)。
5. 表 2-1 で説明している [User Data Service Configuration] セクションのパラメータを指定します。このページのパラメータはすべて必須です。

表 2-1. UDS 設定パラメータ

パラメータ	デフォルト値	説明
Protocol	TCP	Administration Console を使用して UDS サービスに接続するプロトコル。使用可能なオプションは、以下のとおりです。 • TCP • One-Way SSL • Two-Way SSL
Host	localhost	UDS サービスが使用可能な IP アドレス。
Port	8080	UDS サービスが使用可能なポート。
Application Context Root	arcotuds	現在実行中の複数の Administration Console のアプリケーション サーバ インスタンスで、UDS がアクセス可能な一意のベース URL。
Connection Timeout (ミリ秒)	30000	UDS サービスが到達不可能とみなされるまでの最大時間 (ミリ秒)。
Read Timeout (ミリ秒)	10000	UDS からのレスポンスを待機する最大時間 (ミリ秒)。
Idle Timeout (ミリ秒)	30000	リクエストを処理しないアイドル接続が閉じられるまでの時間 (ミリ秒)。
Server Root Certificate		UDS サーバの CA 証明書ファイルへのパス。このファイルは PEM 形式である必要があります。
Client Certificate		Administration Console の CA 証明書ファイルへのパス。このファイルは PEM 形式である必要があります。
Client Private Key		CA の秘密キーが含まれるファイルの場所。パスには、絶対パスまたは ARCOT_HOME に対する相対パスを使用できます。

表 2-1. UDS 設定パラメータ

パラメータ	デフォルト値	説明
Minimum Connections	4	RiskFort サーバと UDS サーバ間で作成される接続の最小数。
Maximum Connections	32	RiskFort サーバと UDS サーバ間で作成可能な接続の最大数。

6. [Next] をクリックして設定を続行します。
次のページが表示されます（図 2-5 を参照）。

図 2-5 ユーザ データ サービスの設定：2 ページ

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/10/2010 10:23:18 GMT

Users and Administrators | Organizations | Services and Server Configurations | Reports

User Data Service Configuration

Configure the User Data Service (UDS) parameters to access user information.
Note: It is optional to configure SSL between UDS and the Arcot products.

Configure UDS Parameters

Search Configuration

Maximum Search Return Count:

LDAP Configuration

LDAP Connection Pool Initial Size:

LDAP Connection Pool Maximum Size:

LDAP Connection Pool Preferred Size:

LDAP Connection Pool Timeout (in milliseconds):

Authentication Token Configuration

Token Purge Interval (in seconds):

Authentication Token Validity Period (in seconds):

7. 表 2-2 で説明している [User Data Service Configuration] セクションのパラメータを指定します。このページのパラメータはすべて必須です。

表 2-2. UDS 検索、LDAP、および認証設定パラメータ

パラメータ	デフォルト値	説明
Search Configuration		
Maximum Search Return Count	500	Administration Console でのすべての検索操作で返されるレコードの最大数。
LDAP Configuration		
LDAP Connection Pool Initial Size	2	プールで作成される、UDS と LDAP 間の接続の初期数。
LDAP Connection Pool Maximum Size	5	UDS と LDAP 間で使用可能な接続の最大数。
LDAP Connection Pool Preferred Size	2	UDS と LDAP 間で優先される接続数。
LDAP Connection Pool Timeout (ミリ秒)	30000	新しい接続がリクエストされたとき、UDS が LDAP からのレスポンスを待機する時間。
Authentication Token Configuration		
Token Purge Interval (ミリ秒)	3600	トークンの有効期限が切れた後に、認証トークンがデータベースから削除されるまでの最大間隔。
Authentication Token Validity Period (秒)	86400	発行された認証トークンが期限切れになるまでの最大期間 (デフォルトは 1 日)。

8. 変更を保存するには、[Save] をクリックします。
9. 展開されたすべての RiskFort サーバインスタンスをリフレッシュします。その方法の手順については、4-54 ページの「サーバインスタンスのリフレッシュまたはシャットダウン」を参照してください。

組織のグローバル設定の指定

Administration Console を展開すると、デフォルトで MA アカウントと一緒に組織が作成されます。この既定の組織は、デフォルトの組織 (DEFAULTORG) と呼ばれます。

単一組織のシステムであるデフォルトの組織は、ユーザが新しい組織を作成する必要がないため便利です。デフォルトの組織の設定を行い、その表示名を変更して、管理目的でその表示名をそのまま使用できます。一方で複数組織のシステムの場合は、デフォルトの組織の表示名を変更し、設定を行い、それをデフォルトとしてそのまま使用するか、新しい組織を作成して、それをデフォルトの組織として設定できます。



注：通常、管理者を作成する場合、またはユーザの組織を指定せずにユーザを登録する場合は、デフォルトの組織に作成されます。

[Organization Global Configuration] ページ (図 2-6 を参照) を使用すると、デフォルトの組織として使用する組織を選択できます。また、今後システムのすべての組織がデフォルトの組織の設定を継承するのか、あるいはこれらの設定を個別に編集して上書きできるかどうかをコントロールします。

図 2-6 [Organization Global Configuration] ページ

デフォルトの組織、および設定を組織レベルで実行できるかどうかを指定する方法

1. MA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。

3. タブのサブメニューにある **[Administration Console]** をクリックします。
4. タスク ペインで **[Organization Global Configuration]** リンクをクリックし、対応するページを表示します (図 2-6 を参照)。
5. 組織に固有の設定を行わない場合は、**[Organization Configuration]** の下にある **[Allow Configuration at Organization Level]** をオフにします。
デフォルトでは、有効になっています。
6. **[Default Organization]** の下で、**[Organization Name]** リストからデフォルトの組織として設定する組織を選択します。
7. このページで行った変更を保存するには、**[Save]** をクリックします。

キャッシュ リフレッシュ設定の指定

Administration Console では、特定のデータをキャッシュします。これにより、頻繁にアクセスされるコンソール ページや UDS データをより速く提供できます。通常は組織とロールがキャッシュされます。この設定を更新するには、**[Cache Refresh Configuration]** ページ (図 2-7) を使用します。

図 2-7 **[Cache Refresh Configuration]** ページ

The screenshot displays the Arcot Administration Console interface. The top navigation bar includes tabs for 'Users and Administrators', 'Organizations', 'Services and Server Configurations', and 'Reports'. The 'Services and Server Configurations' tab is active, showing the 'Cache Refresh Configuration' page. The left sidebar lists 'Administration Console' with sub-items: 'UDS Configuration', 'Organization Global Configuration', 'Cache Refresh Configuration' (selected), and 'Authentication' with 'Basic Authentication Policy'. The main content area is titled 'Cache Refresh Configuration' and contains two sections: 'User Data Service' and 'Administration Console'. Each section has a checkbox for 'Enable Automatic Refresh' (checked) and a text input for 'Refresh Interval (in minutes)' (set to 30). 'Save' and 'Refresh Now' buttons are present at the bottom of each section. The top right corner shows a welcome message for 'MASTERADMIN' and the last login time.

UDS および（または）Administration Console のキャッシュ設定を更新する方法

1. MA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. タブのサブメニューにある **[Administration Console]** をクリックします。
4. タスク ペインで **[Cache Refresh Configuration]** リンクをクリックし、対応するページを表示します（[図 2-7](#) を参照）。
5. **[User Data Service]** および（または）**[Administration Console]** セクションで以下の設定を行います。
 - a. 必要に応じて、**[Enable Automatic Refresh]** オプションをオンまたはオフにします。
 - b. **[Refresh Interval]** の値を編集します。
指定した間隔でキャッシュがリフレッシュされます。たとえば **60** と入力すると、1 時間毎に自動的にリフレッシュされます。デフォルト値は 30 分です。
 - c. **[Save]** をクリックして変更内容を保存します。
 - d. 変更をすぐにリフレッシュする場合は、**[Refresh Now]** をクリックします。

基本認証ポリシー設定の指定

基本認証ポリシーまたは WebFort ユーザパスワード メカニズムのいずれかを使用して、Administration Console にログインする管理者を認証することができます。使用されるメカニズムは、組織の作成時に選択したオプションによって決まります。

- 組織の作成時に **[Basic]** オプションを選択した場合は、[「基本認証のパスワード ポリシーの指定」](#) で説明しているデフォルトの認証ポリシーを使用できます（グローバル レベル）。
- **[WebFort User Password]** オプションを選択した場合は、Arcot WebFort 6.0 が展開され、アクセス可能であることを確認します。



関連文書： ご使用の環境に WebFort をインストールおよび設定する場合の詳細については、「Arcot WebFort 6.0 インストールおよび展開ガイド」および「Arcot WebFort 6.0 管理ガイド」を参照してください。

基本認証のパスワード ポリシーの指定

基本認証方法では、名前が意味するように、管理者がユーザ ID と対応するパスワードを使用してコンソールにログインします。

[Basic Authentication Policy] ページ (図 2-8) を使用して、パスワード長、使用可能な特殊文字の数、アカウントをロックする前に許可されたログインの失敗回数などの制限を実施することでパスワード ポリシーを強化することができます。

図 2-8 [Basic Authentication Policy] ページ

The screenshot shows the Arcot Administration Console interface. The top navigation bar includes 'Users and Administrators', 'Organizations', 'Services and Server Configurations', and 'Reports'. The 'Services and Server Configurations' tab is active, and the 'Administration Console' sub-tab is selected. The main content area is titled 'Basic Authentication Policy' and contains a 'Password Policy Configuration' form. The form includes fields for Minimum Password Length (6), Maximum Password Length (25), Maximum Failed Attempts (5), Minimum Numeric Characters (1), Minimum Alphabetic Characters (4), Minimum Special Characters (1), Allowed Special Characters (a list of special characters), and Validity Period (180 days). A 'Save' button is at the bottom of the form.

基本認証ポリシーを指定する方法

1. MA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。
3. タブのサブメニューにある [Administration Console] をクリックします。

4. タスク ペインで **[Basic Authentication Policy]** リンクをクリックし、対応するページを表示します (図 2-8 を参照)。
5. 表 2-3 で説明している **[Password Policy Configuration]** セクションのパラメータを指定します。このページのパラメータはすべて必須です。

表 2-3. 基本認証ポリシー パラメータ

パラメータ	デフォルト値	説明
Minimum Password Length	6	パスワードで使用する必要がある文字の最小数。6 ～ 32 文字の値を設定できます。
Maximum Password Length	25	パスワードで利用できる文字の最大数。6 ～ 32 文字の値を設定できます。
Maximum Failed Attempts	5	クレデンシャルがロックされるまでに、管理者がパスワードを間違えて指定できる最大連続回数。3 ～ 10 の値を設定できます。
Minimum Numeric Characters	1	パスワードで使用する必要がある数字 (0 ～ 9) の最小数。0 ～ 32 文字の値を設定できます。
Minimum Alphabetic Characters	4	パスワードで使用する必要がある英字 (a ～ z、および A ～ Z) の最小数。0 ～ 32 文字の値を設定できます。
Minimum Special Characters	1	パスワードで使用する必要がある Allowed Special Characters の最小数。0 ～ 32 文字の値を設定できます。
Allowed Special Characters (オプション)	!@#\$%^&*()_+ +	パスワードで利用できる特殊文字のリスト。
Validity Period	180 日	パスワードの有効期間の最大日数。

6. このページで行った変更を保存するには、**[Save]** をクリックします。

第 3 章

カスタム ロールの操作



重要：この章で説明されているロール管理タスクは、**Master Administrator** のみが実行できます。

RiskFort には、事前定義された権限に関連付けられたビルトイン ロールが同梱されています。（このトピックの詳細については、[第 1 章の「サポートされているロール」](#)を参照してください。）ただし、RiskFort では、これらの事前定義されたロールを以下のような場合に操作できる機能も提供しています。

- デフォルトのロールが組織の要件を満たしていない場合。
- RiskFort によって提供されるものとは異なるロール情報を管理する必要がある場合。

この章では、重要な利点である、RiskFort でカスタム ロールを作成して適用する機能について説明します。この章では以下について説明します。

- [カスタム ロールについて](#)
- [カスタム ロールの作成](#)
- [カスタム ロール情報の更新](#)
- [カスタム ロールの削除](#)

カスタム ロールについて

Master Administrator は、以下のいずれかの事前定義された親ロール（[第 1 章の「Administration Console の概要」](#)で詳述）からの権限のサブセットを継承する新しい管理ロールを作成できます。

- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

これらの役割はカスタム ロールと呼ばれ、親のロールに関連付けられたデフォルト権限の一部を**無効にすること**で作成されます。たとえば、GA の「組織の作成権限」を無効にする必要がある場合、この権限を無効にすることによってカスタム ロールを作成できます。

カスタム ロールを作成する場合、管理アカウントを作成または更新する際にロール オプションとして利用可能になります。カスタム ロールは、作成するだけでなく更新および削除も行えます。カスタム ロールの管理の詳細については、この章の以下のセクションを参照してください。

カスタム ロールについて知っておくべきこと

- Master Administrator のみがカスタム ロールを作成できます。
- カスタム ロールは、単一ロールの権限のサブセットのみを継承できます。すなわち、カスタム ロールは、2 つの異なるロールからの権限を継承できません。
たとえば、ユーザを管理 (UA 権限) し、かつ組織を作成 (OA 権限) する権限を持つカスタム UA ロールを作成することはできません。
- 親ロールが権限を持っていない場合、カスタム ロールに新しい権限を割り当てることはできません。
たとえば、事前定義された OA ロールに組織の作成権限がない場合は、この OA ロールに基づいたカスタム ロールもその権限を持つことができません。
- カスタム ロールを作成する場合、少なくとも 1 つの権限が利用可能である限り、その 1 つ以上の権限を表すタスクは引き続き表示されます。
たとえば、Activate、Deactivate および Delete 権限が無効になっても、Update 権限がまだ利用可能である場合は、[Search Organizations] リンクは引き続き表示されます。
- 新しいカスタム ロールが Administration Console の他のインスタンスに利用可能になるのは、Master Administrator が Administration Console サーバ キャッシュをリフレッシュした後だけです。

事前定義済みカスタム ロール

作成できるカスタム ロールに加えて、RiskFort にも、ケース管理に必要な 3 つの事前定義されたカスタム ロール (第 1 章の「[Administration Console の概要](#)」の図 1-4 に表示) が同梱されています。これらのロールには次のものが含まれます。

- **QM : Queue Manager** ロールには、ケースの監督に必要な権限が備えられています。このロールはデフォルトの [Organization Administrator](#) ロールから派生しています。

- **CSR : テクニカル サポート担当者** ロールには、ケースでの作業およびエンド ユーザの呼び出しの処理に必要な権限が備えられています。このロールはデフォルトの **User Administrator** ロールから派生しています。
- **FA : Fraud Analyst** ロールには、隠れた傾向およびパターンを検索するケースの分析に必要な権限が備えられています。このロールもデフォルトの **User Administrator** ロールから派生しています。



注： ケース管理および Queue Manager、テクニカル サポート担当者、および Fraud Analyst ロールに関する詳細については、[第 15 章の「ケースの管理」](#)を参照してください。

カスタム ロールの更新ページ ([3-40 ページの図 3-2](#)) でこれらの既定のカスタム ロールを参照できます。

カスタム ロールの作成

カスタム ロールを作成する方法

1. MA としてログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Roles]** の下で、**[Create Custom Role]** リンクをクリックします。カスタム ロールの作成ページ ([図 3-1](#)) が表示されます。

図 3-1 カスタム ロールの作成ページ

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/15/2010 08:12:05 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports**

Manage Roles

Manage Roles

- **Create Custom Role**
- [Update Custom Role](#)
- [Delete Custom Role](#)

Create Custom Role

Create a custom administrator role. This role must be derived from one of the predefined roles and can have a subset of the base role's privileges.

Role Details

Role Name:

Role Display Name:

Role Description:

Role Based On:

Set Privileges

Available Privileges

- Update Administrator
- RiskFort - Evaluate Risk
- View Advice Summary Report
- RiskFort - Get User Details
- View User Activity Report
- RiskFort - Post Evaluate
- View Exception User Report
- View Administrator Activity Report
- Deactivate User
- Delete User

Unavailable Privileges

4. **[Role Details]** で、以下の情報を指定します。
 - **[Role Name]**：新規ロールを識別する一意の名前。この名前は、この新規ロールを認証して認可するために RiskFort によって内部で使用されます。
 - **[Role Display Name]**：他のすべての Administration Console ページおよびレポートに表示されるロールの説明的な名前。
 - **[Role Description]**：後で参照するためのロールに関連する有用な情報。
 - **[Role Based On]**：このカスタム ロールの派生元である既存のロール。
5. **[Set Privileges]** で、新規ロールには利用できないロールを指定します。
 - a. **[Available Privileges]** リストで、カスタム ロールに対して無効にする必要のある権限をすべて選択します。

このリストは「**Role Based On**」フィールドで選択した管理ロールに利用可能な権限をすべて表示します。



注： **Ctrl** キーを押したまま、一度に複数の権限を選択することができます。

- b. 「**Unavailable Privileges**」 リストに選択された権限を移動するには、[>] ボタンをクリックします。
6. カスタム ロールを作成するには、「**Create**」をクリックします。

カスタム ロール情報の更新

既存のカスタム ロールの定義を更新する方法

1. MA としてログインしていることを確認します。
2. 「**Users and Administrators**」 タブをアクティブにします。
3. 「**Manage Roles**」 の下のタスク メニューで、「**Update Custom Role**」 リンクをクリックします。

図 3-2 に示されているように、カスタム ロールの更新ページが表示されます。

図 3-2 カスタム ロールの更新ページ

Arcot Administration Console

Welcome MASTERADMIN | Logout
Last Login Time 06/15/2010 08:12:05 GMT

Users and Administrators | Organizations | Services and Server Configurations | Reports

Manage Users and Administrators | Manage Roles

Manage Roles

- Create Custom Role
- Update Custom Role
- Delete Custom Role

Update Custom Role

Update a custom role.

Role Details

Role Name: * --Select--

Role Display Name: *

Role Description:

Role Based On:

Set Privileges

Available Privileges

Unavailable Privileges

> >> < <<

Update

4. 更新する **[Role Name]** を選択します。
5. **[Role Details]** で 1 つまたはすべてのフィールドに必要な変更を加えます。
6. **[Set Privileges]** で、必要に応じてロールに利用できない権限のリストを指定します。
 - a. **[Available Privileges]** リストで、新規ロールに対して無効にする必要のある権限をすべて選択します。

このリストは **[Role Based On]** フィールドで選択した管理ロールに利用可能な権限をすべて表示します。

または
 - b. **[Unavailable Privileges]** リストで、新規ロールのために有効にする権限を選択します。

このリストは「**Role Based On**」フィールドで選択した管理ロールに利用できない権限をすべて表示します。



注：Ctrl キーを押したまま、一度に複数の権限を選択することができます。

- c. 「**Unavailable Privileges**」リストに選択された権限を移動するには、[>] ボタンをクリックします。

7. カスタム ロール定義を更新するために「**Update**」をクリックします。

カスタム ロールの削除



重要：管理者に現在割り当てられるカスタム ロールを削除することはできません。

そのようなロールを削除する必要がある場合は、管理者の更新ページ (図 13-8) を使用して、最初にこのロールを割り当てられている管理者のロールを変更する必要があります。その後で、このセクションの手順に従います。

既存のカスタム ロールを削除する方法

1. MA としてログインしていることを確認します。
2. 「**Users and Administrators**」タブをアクティブにします。
3. 「**Manage Roles**」の下タスク メニューで、「**Delete Custom Role**」リンクをクリックします。

図 3-3 に示されているように、カスタム ロールの削除ページが表示されます。

図 3-3 カスタム ロールの削除ページ

The screenshot shows the Arcot Administration Console interface. At the top, there is a header with the Arcot logo, the title 'Arcot Administration Console', and a user welcome message 'Welcome MASTERADMIN | Logout' with the last login time '01/07/2010 09:18:41 GMT'. Below the header is a navigation bar with four tabs: 'Users and Administrators', 'Organizations', 'Services and Server Configurations', and 'Reports'. The 'Users and Administrators' tab is active, and within it, the 'Manage Roles' sub-tab is selected. On the left side, there is a sidebar with the heading 'Manage Roles' and three links: 'Create Custom Role', 'Update Custom Role', and 'Delete Custom Role'. The 'Delete Custom Role' link is highlighted with a green dot. The main content area is titled 'Delete Custom Role' and contains a sub-section 'Role Details' with a form. The form has four fields: 'Role Name' (a dropdown menu with '--Select--' as the current selection), 'Role Display Name' (a text input field), 'Role Description' (a text input field), and 'Role Based On' (a text input field). Below the form is a 'Delete' button. A note above the form states: 'Delete a custom role. A role can be deleted only if no administrators have currently been assigned that role.'

4. [Role Details] で、[Role Name] リストから削除する必要のあるカスタム ロールを選択します。
5. [Delete] をクリックして選択したカスタム ロールを削除します。

第 4 章

RiskFort サーバ インスタンスの管理



重要：この章で説明するすべての設定およびタスクは、**Master Administrator** のみが実行できます。

Master Administrator は、RiskFort インスタンスをローカルで管理する必要があります。ただし、サーバ インスタンスを管理するには、インスタンスに接続するための接続パラメータを設定する必要があります（設定方法の詳細については、「[サーバ接続の設定](#)」を参照してください）。

接続パラメータを設定してからのみ、RiskFort サーバ インスタンスを管理できます。インスタンスを管理するためのタスクには、以下のものがあります。

- [サーバ接続の設定](#)
- [トラスト ストアの作成](#)
- [通信プロトコルの設定](#)
- [サーバ インスタンスのリフレッシュまたはシャットダウン](#)



注：最後のタスク（サーバ インスタンスのリフレッシュまたはシャットダウン）は、システム ツールを使用して実行することもできます（[第 17 章の「システム管理者のためのツール」](#)で詳述）。

サーバ接続の設定

RiskFort には以下の 2 つのサーバ コンポーネントが含まれています。

- **RiskFort サーバ。**このサーバはリスク評価のコア エンジンです。
- **Case Management Queuing Server。**このサーバはケース管理のコア エンジンであり、キューの定義に応じてケースの構築と優先順位付けを行います。



注：Administration Console のすべてのインスタンスは、常に Case Management Queuing Server の 1 つのインスタンスのみに接続できます。

[RiskFort Connectivity] ページ（[図 4-1](#)）を使用して、RiskFort サーバおよび Case Management Queuing Server インスタンスに接続するために Administration Console が使用する接続設定を行う必要があります。

図 4-1 [RiskFort Connectivity] ページ

The screenshot displays the Arcot Administration Console interface. The top navigation bar includes 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (selected), and 'Reports'. The left sidebar shows 'RiskFort' and 'Administration Console' tabs, with 'RiskFort' expanded to show 'System Configuration' (including 'RiskFort Connectivity', 'Trusted Certificate Authorities', and 'Protocol Configuration') and 'Extensible Configurations' (including 'Add Rule Type' and 'View Existing Rule Types').

The main content area is divided into two sections:

RiskFort Connectivity

Specify the configurations that will be used by the Administration Console to connect to the RiskFort Server instance.

Fields for configuration:

- Server: localhost
- Port: 7777
- Transport: TCP (dropdown)
- Server CA Root Certificate: [Browse...]
- Client Certificate-Key Pair in PKCS#12: [Browse...]
- Client PKCS#12 Password: []

[Save]

Case Management Queuing Server Connectivity

Specify the configurations that will be used by the Administration Console to connect to the Case Management Queuing Server instance.

Fields for configuration:

- Host: localhost
- Backup Host: []
- Port: 7779
- Transport: TCP (dropdown)
- Server CA Root Certificate: [Browse...]
- Client Certificate-Key Pair in PKCS#12: [Browse...]
- Client PKCS#12 Password: []

[Save]

2つのサーバ モジュールの接続パラメータを指定する方法

1. MA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. ページがまだ表示されていない場合は、タスク ペインの **[RiskFort Connectivity]** リンクをクリックして対応するページを表示します (図 4-1 を参照)。
4. 表 4-1 の情報を使用して、**[RiskFort Connectivity]** セクションのフィールドを編集します。

表 4-1. RiskFort サーバと Administration Console 間の接続パラメータ

フィールド	説明
[Server]	必要な RiskFort サーバ インスタンスをインストールしたシステムの IP アドレスを入力します。 注：RiskFort サーバがインストールされているシステムがネットワーク上の <code>hostname</code> からアクセス可能であることを確認する必要があります。
[Port]	そのプロトコルのサービスが提供されているポートを入力します。
[Transport]	対応するコンポーネント (Server Management Web サービス、Administration Web サービス、Transaction Web サービス、および Authentication Native) のトランスポート モード (TCP または SSL) を指定して、指定された RiskFort サーバ インスタンスに接続します。
[Server CA Root Certificate]	サーバの CA ルート証明書を参照してアップロードします。 注：サーバ証明書は PEM 形式である必要があります。
[Client Certificate-Key Pair in PKCS#12]	クライアント証明書および秘密キーを含む PKCS#12 ストアを参照してアップロードします。
[Client PKCS#12 Password]	クライアントの PKCS#12 ストアのパスワードを入力します。

5. 表 4-2 の情報を使用して、**[Case Management Queuing Server Connectivity]** セクションのフィールドを編集します。

表 4-2. Case Management Queuing Server と Administration Console 間の接続パラメータ

フィールド	説明
[Host]	Queuing Server インスタンスをインストールしたシステムの IP アドレスを入力します。 注：Queuing Server がインストールされているシステムがネットワーク上の <code>hostname</code> からアクセス可能であることを確認する必要があります。
[Backup Host]	バックアップの Queuing Server インスタンスが使用可能なシステムの IP アドレスを入力します（インストールされている場合）。 注：Queuing Server がインストールされているシステムがネットワーク上の <code>hostname</code> からアクセス可能であることを確認する必要があります。
[Port]	そのプロトコルのサービスが提供されているポートを入力します。
[Transport]	対応するコンポーネント（Server Management Web サービス、Administration Web サービス、Transaction Web サービス、および Authentication Native）のトランスポート モード（TCP または SSL）を指定して、指定された RiskFort サーバ インスタンスに接続します。
[Queueing Server CA Root Certificate]	サーバの CA ルート証明書を参照してアップロードします。 注：サーバ証明書は PEM 形式である必要があります。
[Client Certificate-Key Pair in PKCS#12]	クライアント証明書および秘密キーを含む PKCS#12 ストアを参照してアップロードします。
[Client PKCS#12 Password]	クライアントの PKCS#12 ストアのパスワードを入力します。

- 設定した内容を保存し、Administration Console がインスタンスの詳細を取得していることを確認するには、[Save] をクリックします。

トラスト ストアの作成

トラスト ストアを作成して、SSL ベースの通信の実行中に、RiskFort サーバ インスタンスに対して RiskFort コンポーネント（Administration Console や Java SDK を含む）またはその他のクライアントを認証することができます。トラスト ストアには、RiskFort サーバ インスタンスおよび Case Management Queuing Server が信頼している CA ルート証明書セットが含まれます。

[Trusted Certificate Authorities] ページ（図 4-2）を使用して、トラスト ストアを作成したり、トラスト ストアに新しいルート証明書を追加したりすることができます。

図 4-2 [Trusted Certificate Authorities] ページ

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo and 'Arcot Administration Console'. On the right, it says 'Welcome MASTERADMIN | Logout' and 'Last Login Time 06/15/2010 08:12:05 GMT'. Below the header is a navigation bar with tabs: 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (which is active), and 'Reports'. Under 'Services and Server Configurations', there's a sub-tab 'RiskFort' and 'Administration Console'. The left sidebar has a 'RiskFort' section with 'System Configuration' expanded, showing links for 'RiskFort Connectivity', 'Trusted Certificate Authorities' (which is selected), 'Protocol Configuration', and 'RiskFort Queueing Server Connectivity'. Below that is 'Extensible Configurations' with 'Add Rule Type' and 'View Existing Rule Types'. The main content area is titled 'Trusted Certificate Authorities' and has a subtitle 'Upload multiple CAs and group them to create an SSL Trust Store.' It contains a form with a 'Name' field, a 'Root CAs' section with two 'Browse...' buttons and an 'Add More' button, and a 'Save' button at the bottom right.

RiskFort サーバ インスタンス用のトラスト ストアを作成する方法

1. MA としてログインしていることを確認します。
2. メイン メニューの [Services and Server Configurations] タブをアクティブにし、サブメニューの [RiskFort] タブがアクティブになっていることを確認します。
3. [System Configuration] セクションの下で、[Trusted Certificate Authorities] リンクをクリックして、[Trusted Certificate Authorities] ページを表示します（図 4-2 を参照）。
4. [Name] フィールドに、作成する新しいトラスト ストアの名前を入力します。

5. 対応する **[Browse]** ボタンをクリックし、信頼された CA の 1 つ以上のルート証明書をアップロードします。**[Add More]** をクリックすると、証明書をアップロードするための追加フィールドを表示できます。
6. 必要な証明書のアップロードがすべて完了したら、**[Save]** をクリックします。

通信プロトコルの設定

[Protocol Configuration] ページは、**[RiskFort Protocol Configuration]** セクションと **[Case Management Queuing Server Protocol Configuration]** セクションの 2 つのセクションに分かれています。

[RiskFort Protocol Configuration] セクション (図 4-3) を使用して、認証と管理を行うために、Administration Console、SDK、および Web サービスが RiskFort サーバ インスタンスと通信するために使用するプロトコルを設定できます。サーバがこれらの使用可能な各コンポーネントをリスンするポートに加えて、トランスポートのセキュリティ メカニズム (TCP または SSL) も指定できます。また、メカニズムとして SSL を指定した場合、有効で信頼できるクライアント コンポーネントの証明書と秘密キーを指定する必要があります。これらは安全な接続を確立するために必要です。

図 4-3 [RiskFort Protocol Configuration] セクション



Arcot Administration Console

Welcome MASTERADMIN | [Logout](#)
Last Login Time 07/06/2010 16:15:06 GMT

Users and AdministratorsOrganizationsServices and Server ConfigurationsReports

RiskFortAdministration Console

RiskFort

System Configuration

- [RiskFort Connectivity](#)
- [Trusted Certificate Authorities](#)
- [Protocol Configuration](#)**

Extensible Configurations

- [Add Rule Type](#)
- [View Existing Rule Types](#)

RiskFort Protocol Configuration

Configure the protocols for the RiskFort Server instance. If you are using SSL security, both the Certificate Chain and the Private Key must be uploaded in PEM format. The changes made using this screen are not effective until the RiskFort Server is restarted.

Enabled	Protocol	Port Number	Transport Security	Client Store	SSL Certificate Details
☒	Native (TCP)	7680	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☒	Server Management	7980	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☒	Administration Web Service	7777	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☒	Transaction Web Service	7778	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☐	Native (SSL)	7681	SSL	--Select--	Certificate Chain : Browse... Private Key : Browse...

Save

表 4-3 では、このページの **[RiskFort Protocol Configuration]** セクションに表示されるプロトコルについて説明し、そのデフォルト ポート番号をリスト表示しています。

表 4-3. RiskFort のプロトコルおよびポート番号

プロトコル	デフォルト のポート 番号	説明
Native (TCP)	7680	このプロトコルは、RiskFort サーバ インスタンスと RiskFort Java SDK (リスク評価および発行を含む) の間の通信を有効にするための、Arcot 専用プロトコルです。
Server Management	7980	arrfadmin ツールは、サーバ管理アクティビティ (正常シャットダウンやサーバキャッシュのリフレッシュ) を行うために、このプロトコルを使用して RiskFort サーバ インスタンスと通信します。 Administration Console ツールの詳細については、 17-308 ページの「arrfadmin: サーバ リフレッシュとシャットダウン ツール」 を参照してください。
Administration Web Service	7777	これは、RiskFort サーバと Administration Web サービス間の通信用のプロトコルです。 RiskFort サーバは、このポートで Administration Web サービスからのコールをリスンします。 注: これらのコールには RiskFort 発行コールやリスク評価コールは含まれません。
Transaction Web Service	7778	このプロトコルは、リスク評価および発行 Web サービスが RiskFort サーバ インスタンスに接続する場合に使用されます。 注: これらのコールには管理サービス コールは含まれません。
Native (SSL)	7681	このプロトコルは、RiskFort サーバ インスタンスと RiskFort Java SDK (リスク評価および発行を含む) の間の通信を有効にするための、Arcot 専用プロトコルです。

同様に、**[Case Management Queuing Server Protocol Configuration]** セクション (図 4-4) を使用して、認証と管理を行うために、Administration Console と Case Management Queuing Server が RiskFort サーバ インスタンスと通信するために使用するプロトコルを設定できます。サーバがこれらの使用可能な各コンポーネントをリスンするポートに加えて、トランスポートのセキュリティ メカニズム (TCP または SSL) も指定

できます。また、メカニズムとして SSL を指定した場合、有効で信頼できるクライアント コンポーネントの証明書と秘密キーを指定する必要があります。これらは安全な接続を確立するために必要です。

図 4-4 [Case Management Queuing Server Protocol Configuration] セクション

Case Management Queuing Server Protocol Configuration

Configure the protocols for the Case Management Queuing Server instance. If you are using SSL security, both the Certificate Chain and the Private Key must be uploaded in PEM format. The changes made using this screen are not effective until the Case Management Queuing Server is restarted.

Enabled	Protocol	Port Number	Transport Security	Client Store	SSL Certificate Details
☒	Case Management Queuing Server	7779	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☒	Case Management Queuing Administration	7780	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...

Save

表 4-4 では、このページの [Case Management Queuing Server Protocol Configuration] セクションに表示されるプロトコルについて説明し、そのデフォルト ポート番号をリスト表示しています。

表 4-4. Case Management Queuing Server のプロトコルとポート番号

プロトコル	デフォルト のポート 番号	説明
Queueing Server	7779	このプロトコルは、キューイング サーバがケース マネージメント リクエストを（サーバ側の）指定されたポートでリスンするために使用されます。
Queueing Administration	7780	これは、RiskFort サーバと Administration Web サービス間の通信用のプロトコルです。 RiskFort サーバは、このポートで Administration Web サービスからのコールをリスンします。

RiskFort サーバおよび Case Management Queuing Server のネットワーク プロトコルを設定する方法

1. MA としてログインしていることを確認します。
2. メイン メニューの **[Services and Server Configurations]** タブをアクティブにします。
3. サブ メニューの **[RiskFort]** タブがアクティブであることを確認します。
4. **[System Configuration]** セクションの下で、**[Protocol Configuration]** リンクをクリックして、**[Protocol Configuration]** ページを表示します (図 4-3 を参照)。
5. 必要に応じて、このページのフィールドを編集します。表 4-5 でこれらのフィールドについて説明します。

表 4-5. RiskFort および Case Management Queuing Server のセットアップ ページのフィールド

ページの列	アクションの説明
[Protocol]	必要なプロトコルを有効にするには、 [Enabled] 列のチェック ボックスを使用します。 サポートされているプロトコルの詳細については、表 4-3 を参照してください。
[Port Number]	対応する RiskFort サービスが使用可能なポート番号を入力します。RiskFort プロトコルのデフォルト ポート番号を以下に示します。 • RiskFort ネイティブ (TCP) : 7680 • RiskFort ネイティブ (SSL) : 7681 • Administration Web Services : 7777 • Transaction Web Services : 7778 • Queuing Server : 7779 • Queueing Administration : 7780 • Server Management : 7980
[Transport Security]	データ転送でサポートされている以下のいずれかのモードを指定します。 • [TCP] : TCP (Transmission Control Protocol) モードは、両方の RiskFort プロトコルによってサポートされているデフォルトのモードです。クリア テキスト形式でデータを送信します。 • [SSL] : SSL (Secure Sockets Layer) はトランザクションに高度なセキュリティを提供します。これは、データを暗号化して転送し、受信後復号化するためです。

表 4-5. RiskFort および Case Management Queuing Server のセットアップ ページのフィールド

ページの列	アクションの説明
[Client Store]	信頼された CA のルート証明書が含まれるトラスト ストアを選択します。トラスト ストアの設定の詳細については、「 トラスト ストアの作成 」を参照してください。
[SSL Certificate Details]	トランスポートのセキュリティ モードが SSL の場合に使用される証明書チェーンを指定します。対応するフィールドの [Browse] ボタンを使用して、証明書の証明書チェーンおよび秘密キーをアップロードします。 重要: ここでアップロードしたチェーン内の証明書は、リーフ証明書 --> 中間 CA 証明書 --> ルート証明書の階層に従う必要があります。証明書とキーは PEM 形式である必要があります。

6. ページ上で設定を完了したら、[**Save**] をクリックします。
7. 前の変更を加えた RiskFort サーバ インスタンスをリフレッシュします。手順については、「[サーバ インスタンスの再起動](#)」を参照してください。

SSL 通信の設定（オプション）

デフォルトでは、Administration Console は Transmission Control Protocol (TCP) を使用して RiskFort サーバと通信します。ただし、TCP はスプーフィングおよび man-in-the-middle 攻撃に対しては脆弱です。Administration Console を使用して、以下のコンポーネント間の安全な通信を保証するように SSL を設定できます。

- Administration Console と RiskFort サーバ
- RiskFort サーバと Java SDK
- RiskFort サーバと [arrfadmin](#) ツール
- [arrfadmin](#) ツールと Case Management Queuing Server

	関連文書: これらのコンポーネント間の SSL ベースの通信の段階的な設定については、「Arcot RiskFort 2.2.6 インストールおよび展開ガイド」の付録 F「SSL の設定」を参照してください。 arrfadmin ツールの詳細については、第 17 章の「arrfadmin: サーバリフレッシュとシャットダウン ツール」を参照してください。

サーバ インスタンスのリフレッシュまたはシャットダウン

このセクションでは、以下の内容について説明します。

- [サーバ インスタンスのリフレッシュ](#)
- [サーバ インスタンスの再起動](#)

サーバ インスタンスのリフレッシュ

RiskFort サーバと Case Management Queuing Server インスタンスの両方をリフレッシュするには、**arrfadmin** ツールを使用できます。



重要：以下のサブセクションで指図するように、RiskFort サーバの **arrfadmin** ツールを実行する前に、**riskfortadminclient.ini** の **Host** と **Port** の値を設定します。詳細については、[17-311 ページの「サーバとの双方向 SSL 通信用のツールの設定」](#)を参照してください。

ツールの詳細については、[17-308 ページの「arrfadmin: サーバ リフレッシュとシャットダウン ツール」](#)を参照してください。

Windows の場合

以下のように、**arrfadmin** ツールを実行して RiskFort サーバのキャッシュをリフレッシュします。

1. コマンド プロンプト ウィンドウを開きます。
2. 以下のディレクトリに移動します。
`<install_location>\Arcot Systems\bin\`
3. リフレッシュするには、以下の手順を実行します。

- **RiskFort サーバ インスタンスの場合**

```
arrfadmin -r
```

- **Case Management Queuing Server インスタンスの場合**

```
arrfadmin <host_name> <port> -r
```

UNIX ベースのプラットフォームの場合

以下のように、**arrfadmin** ツールを実行して RiskFort サーバのキャッシュをリフレッシュします。

1. ターミナル ウィンドウを開きます。
2. 以下のディレクトリに移動します。
`<install_location>/arcot/bin/`
3. リフレッシュするには、以下の手順を実行します。
 - **RiskFort サーバ インスタンスの場合**
`arrfadmin -r`
 - **Case Management Queuing Server インスタンスの場合**
`arrfadmin <host_name> <port> -r`

サーバ インスタンスの再起動

以下のサブセクションでは、RiskFort サーバおよび Case Management Queuing Server インスタンスを再起動するための手順について説明します。

Windows の場合

Windows でサーバ インスタンスを起動する方法

1. インスタンスが停止したコンピュータにログインします。
2. デスクトップの [スタート] ボタンをクリックします。
3. [設定] - [コントロール パネル] - [管理ツール] - [サービス] に移動します。
4. 以下を再起動します。
 - **RiskFort サーバ インスタンス**：リスト表示されたサービスから [Arcot RiskFort Service] をダブルクリックします。
 - **Case Management Queuing Server**：リスト表示されたサービスから [Arcot RiskFort Case Management Queuing Service] をダブルクリックします。
5. [開始] をクリックしてサービスを開始します。

UNIX ベースのプラットフォームの場合

UNIX ベースのプラットフォームでサーバ インスタンスを起動する方法

1. インスタンスを開始する必要があるコンピュータにログインします。
2. 以下のディレクトリに移動します。

`<install_location>/arcot/bin/`

3. 再起動するには、以下のコマンドを実行します。

- **RiskFort サーバ インスタンスの場合**
`./riskfortserver start`
- **Case Management Queuing Server インスタンスの場合**
`./casemanagementserver start`

第 5 章

RiskFort ルールの基礎知識



重要：この章で説明する概念に関連するほとんどのタスクを実行できるのは、**Global Administrator** および **Organization Administrator** のみですが、この章は、RiskFort が使用するルールの基本事項を理解したい人に役立ちます。

RiskFort では、さまざまなルールを使用して、各トランザクションに関連付けられたリスクを評価します。これらのルールは、以下の 2 つのカテゴリに大きく分類することができます。

- [評価ルール](#)
- [スコアリング エンジン](#)

ルールが属するカテゴリに関係なく、RiskFort のすべてのルールには以下の 3 つの特性があり、ルールがどのように処理されるかを制御しています。

- ルール セット
- ルールの実装（グローバル レベルまたは組織レベル）
- ルール タイプ

ルールとルール セットのタイプは密接に関連しています。各ルールは[ルール セット](#)に属する必要があります。ルール セットを選択すると、ルールで使用可能なオプションが決まります。同様に、[ルールの実装](#)によって、ルールをグローバル レベルに適用できるか（テンプレートとして組織で利用可能）、個々の組織レベルに適用できるかどうかが決まります。[ルール タイプ](#)はルールの機能および範囲を決定し、[アドオン ルール](#)と密接に関連しています。



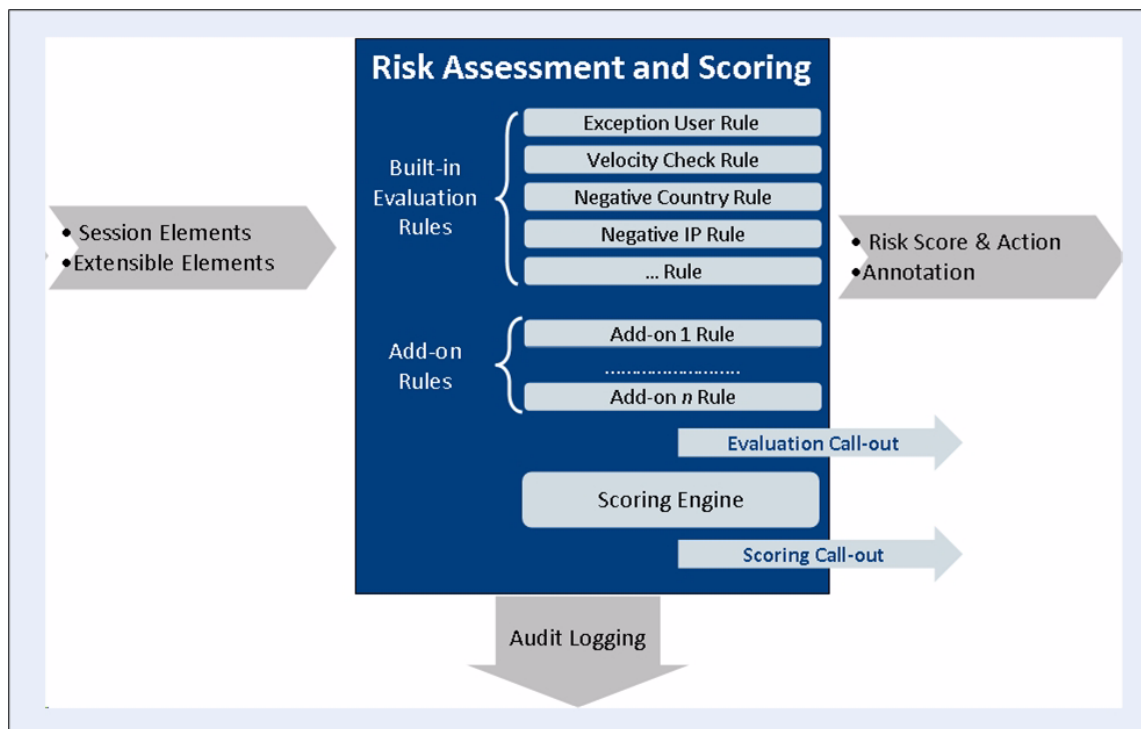
注：ルール セットの操作の詳細については、[第 7 章の「ルール セットの作成」](#)を参照してください。

グローバル レベルおよび組織レベルでのルールの実装については、それぞれ [第 7 章の「グローバル ルール設定の管理」](#) および [第 11 章の「組織固有の RiskFort の設定の管理」](#) を参照してください。

RiskFort でのルール タイプの管理の詳細については、[第 6 章の「アドオン ルールの準備：ルール タイプの操作」](#) を参照してください。

[図 5-1](#) は、さまざまなルールに関する RiskFort ルールとそのスコアリングのスキーマ図を表しています。[図 5-1](#) に示すすべての評価ルールおよびスコアリング ルールのサブタイプについては、図の後のサブセクションで説明します。

図 5-1 RiskFort ルールとスコアリングの順序



評価ルール

評価ルールとはそれぞれ事前設定済みのロジックであり、ブール値を返します。アプリケーションからリスク評価のリクエストがあった場合、このロジックはリクエストの入力トランザクションデータに適用されます。ルールロジックとの照合で、ルールと一致する場合はそれぞれ **TRUE** を返し、ルールと一致しなかった場合はそれぞれ **FALSE** を返します。



重要：スコアリングの際、評価ルールは一致が検出されるまで優先度に従ってスコアリングされます。

RiskFort では以下のタイプの評価ルールを提供しています。

- [既定ルール](#)
- [アドオンルール](#)
- [評価コールアウト](#)

既定ルール

これは終端ルールです。つまり、スコアリングの際に任意の評価ルールに一致した (**TRUE** が返された) 場合、リスクエンジンはこのカテゴリの以降のルールに対するスコアリングを中止し、一致したルールに対応するリスクスコアを生成します。

これらのルールは以下のように分類できます。

- [設定可能な組み込みのルール](#)
- [設定できない組み込みのルール](#)

設定可能な組み込みのルール

表 5-1 に、RiskFort をインストールするとデフォルトでインストールおよび展開される、既定のルールをリスト表示します。

表 5-1. 設定可能な組み込みのルール

ルール名	ルールの説明
例外ユーザ チェック	組織では、指定された期間にリスク評価から一時的にユーザを除外することを選択する場合があります。たとえば、あるユーザが拒否国に移動する必要があったとします。このようなユーザは例外ユーザ リストに追加され、例外ユーザとして参照されます。 例外ユーザ リストで見つかった場合、デフォルトでは、RiskFort は例外ユーザから発生したトランザクションに対して低いスコアと許可アドバイスを返します。
不明ユーザ チェック	ユーザが RiskFort データベースに存在しません。その場合、RiskFort は ALERT を返します。 アプリケーションでは、RiskFort API を呼び出して RiskFort にユーザを作成するか、または適切なアクションを取ることができます。
トラステッド IP/ アグリゲータ チェック	詳細については、「 トラステッド IP アドレスの設定 」および「 トラステッド アグリゲータの設定 」を参照してください。
拒否 IP チェック	詳細については、「 拒否 IP アドレスの設定 」を参照してください。
拒否国チェック	詳細については、「 [Negative Country List] の設定 」を参照してください。
ユーザ頻度	詳細については、「 ユーザ頻度の設定 」を参照してください。
デバイス頻度	詳細については、「 デバイス頻度の設定 」を参照してください。
ゾーン ホッピング	詳細については、「 ゾーン ホッピングの設定 」を参照してください。

設定できない組み込みのルール

前述の設定可能なルールに加えて、RiskFort では以下の内容も確認します。

- （トランザクションが評価されている）ユーザが RiskFort データベースに存在するかどうか。この情報はマシンの FingerPrint との照合に使用されます。
- また、対応するユーザとデバイスの関連付けが存在するかどうか（ユーザとデバイスの関連付けの一致）。

これらの一致に基づいて、以下の 4 つの（既定の）条件を組み合わせることができます。

- ユーザとデバイスの関連付けとマシンの **FingerPrint** がいずれも一致する
- ユーザとデバイスの関連付けは一致するが、マシンの **FingerPrint** は一致しない
- ユーザとデバイスの関連付けは一致しないが、マシンの **FingerPrint** は一致する
- ユーザとデバイスの関連付け、およびマシンの **FingerPrint** のいずれも一致しない



注：これらの各ルールは、このルールに一致しているかどうかを相互に判断する条件の組み合わせです。

アドオン ルール

RiskFort の既定ルールは汎用的であり、すべてに適用可能なルールに基づいてリスクを評価するために設定されます。RiskFort がデフォルトで提供しているルールと大きく異なるカスタム ルール、または業界固有のルールが必要な場合は、アドオン ルールを展開する必要があります。

組み込みのルールとは異なり、これらのルールはインストールはされていますが、自動的に展開されません。



注：アドオン ルールの展開の詳細については、[第 12 章の「アドオン ルールの操作」](#)を参照してください。

アドオン ルールを展開する前に、Master Administrator がルール タイプを設定する必要があります。MA がこれを実行する方法の詳細については、[第 6 章の「アドオン ルールの準備：ルール タイプの操作」](#)を参照してください。

評価コールアウト

ビジネス要件に基づいて、独自のカスタム評価ルールを作成することもできます。このルールは、RiskFort サーバの外部のアプリケーション側で実行されます。

RiskFort では、すべてのスタンドアロンおよびアドオン ルールが実行された後に、このルールが実行されます。このコールアウトは、以前のすべてのルールの結果と追加入力を入力として受け入れ、レスポンス (SUCCESS/FAILURE)、修飾文字列 (スコアリング コールアウトによって使用される追加情報)、および注釈文字列 (コールアウトの実装 モジュールによって RiskFort サーバに返された理由または説明) を返します。



注：評価コールアウトの操作の詳細については、第 9 章の「コールアウトの設定」を参照してください。

スコアリング エンジン

評価ルールに加えて、RiskFort では、前の評価ルールからの入力を受け入れて最終的なスコアとアドバイスを生成するスコアリング エンジンも提供しています。

また、ビジネス要件に基づいて、RiskFort の標準のスコアリング ロジックのほかにも独自のカスタム スコアリング ロジックを追加できる柔軟性も備わっています。これを行うには、スコアリング コールアウトを利用します。スコアリング コールアウトを実装して独自のカスタム スコアリング ロジックを作成し、RiskFort の標準のスコアリング プログラムによって生成されたスコア、アドバイス、およびリスク評価の結果を処理できます。スコアリング コールアウトは最終的なリスク スコアを返します。このスコアは RiskFort の標準のスコアリング プログラムによって計算されたスコアと異なるため、これを上書きする場合があります。

また、評価コールアウトと同様に、RiskFort の標準のスコアリング プログラムの後に最後に実行されるカスタム ルールであり、最終的なスコアとアドバイスを返します。



注：スコアリング コールアウトの操作の詳細については、第 9 章の「コールアウトの設定」を参照してください。

第 6 章

アドオン ルールの準備：ルール タイプの操作



重要：この章で説明するすべての設定およびタスクは、**Master Administrator** のみが実行できます。

RiskFort では、ルール タイプを使用して、アドオン ルールの機能と範囲を定義します。たとえば、使用しているルール タイプに基づいてアドオン ルールを定義し、リストのマッピング データまたは導出データを調べたり、評価を行う際にユーザとデバイスの関連付けとの一致および MFP との一致を使用したり、評価目的で数値の比較を実行できます。

この章では、以下の基本事項について説明します。

- システム定義のルール タイプ
- カスタム ルール タイプの操作
- 入力定義 XML のサンプル

システム定義のルール タイプ

RiskFort にはそのまま使用できる事前設定済みの以下のルール タイプが付属しています。表 6-1 ではこれらのルールについて説明します。

表 6-1. システム定義のアドオン ルール タイプ

ルール タイプ	カテゴリ	ルール タイプの説明
AMOUNT_CHECK	数値比較	アドオン ルールで、指定された通貨のしきい値の金額と比較してトランザクションを追跡する必要がある場合。
CARDHOLDER_MERCHANT_AMOUNT	頻度	アドオン ルールで、指定された期間内のカード所有者、業者、および金額別のトランザクション数を追跡する必要がある場合。

表 6-1. システム定義のアドオン ルール タイプ

ルール タイプ	カテゴリ	ルール タイプの説明
COMBINATION RULE	組み合わせ	アドオン ルールで、組み込みの RiskFort ルールや以前に論理演算子と組み合わせで定義した任意のアドオン ルールを使用する場合。
COUNTRY_LIST_LOOKUP	簡易リスト	アドオン ルールでデフォルトの国リストを検索する必要がある場合。
DERIVED_LIST_LOOKUP	マッピング（または導出）リスト	アドオン ルールでマッピング リスト（または導出リスト）の導出データを検索する必要がある場合。
PREDECTIVE MODEL	RiskFort モデル	リスク査定の場合に、アドオン ルールが RiskFort 予測モデルからの入力が必要とする場合。
PREDECTIVE MODEL SCORE ANALYSIS		注：このようなアドオン ルールを設定する前にモデルを構築する必要があります。モデルを構築する場合は、 services@arcot.com から Arcot プロフェッショナル サービスにお問い合わせください。
IPADDRESS_MERCHANT_AMOUNT	頻度	アドオン ルールで、指定された業者サイトでのトランザクション金額を追跡する必要がある場合。
IP_VELOCITY	頻度	アドオン ルールで、指定された期間内のデバイスからのトランザクション回数を追跡する必要がある場合。
MERCHANT_CATEGORY_LOOKUP	マッピング（または導出）リスト	アドオン ルールでマッピング（または導出）リストで業者対カテゴリのマッピング データを検索する必要がある場合。
MERCHANT_REGION_LOOKUP	マッピング（または導出）リスト	アドオン ルールでマッピング リスト（または導出リスト）から業者対地域のマッピング データを検索する必要がある場合。
NUMERIC_COMPARISON	数値比較	アドオン ルールがしきい値に対する数値比較に基づく場合。
SIMPLE_LIST_LOOKUP	簡易リスト	アドオン ルールが簡易リストのデータを検索する必要がある場合。
TRANSACTION_TYPE_CHECK	簡易リスト	リスク評価の場合に、アドオン ルールが Arcot TransFort トランザクション タイプも使用する場合。



注：アドオン ルールを設定する際にルール タイプとして *_LIST_LOOKUP を選択する場合、GA または OA が関連する検索データをアップロードする必要があります。

その方法の詳細については、第 12 章の「アドオン ルールのリスト データのアップロード」を参照してください。

以下のサブセクションでは、表 6-1 で指定されているルール タイプ カテゴリについて説明します。

数値比較

このカテゴリを使用すると、より大きい /GT (>)、以上 /GTE (>=)、等しい /EQ (=)、より小さい /LT (<)、以下 /LTE (<=)、および等しくない /NEQ (!=) などの論理演算子を活用して、2 つの数式を比較できます。

組み合わせ

このカテゴリでは、既定の RiskFort ルールと展開されたアドオン ルールを組み合わせ、論理演算子 ((、))、AND、OR、NOT など) を活用して複雑な式を作成できます。

RiskFort モデル

RiskFort では高度な不正行為モデリング機能を提供しています。このモデリング機能は、履歴データに基づいて、RiskFort 内への組み込みおよび作成を行うことができます。モデルは、使用可能なトランザクション データおよびシステム データを使用して、トランザクションが本物であるかどうかをモデルが疑っている程度を表すスコアを生成します。通常、このスコアの範囲は 0 ～ 100 までであり、数値が大きいほど不正行為の可能性が高くなります。RiskFort では、このモデル スコアに基づいて、コール元のアプリケーションに対して異なるレスポンスを送信するように設定できます。

モデル スコアは、アドオン ルールを設定する際にシステム パラメータの一部 (ModelScore) として使用することもできます。このスコアはリスク アドバイスに達するその他のデータ エLEMENT と一緒に使用できます。

頻度

このカテゴリは、ユーザとデバイスに関する標準装備の基本的な頻度ルールを拡張したものです。基本的な頻度ルールを理解するには、「[ユーザ頻度の設定](#)」および [第 7 章の「デバイス頻度の設定」](#)を参照してください。

簡易リスト

このデータセットはリスト形式の単純なデータ エントリで構成されます。たとえば、安全であると考えられる国リストは、このカテゴリに分類されます。リスト内の各エントリは、以下のようなフォーマットで、改行文字によって他のエントリと区別されます。

```
<entry1>
<entry2>
.....
<entryn>
```

たとえば以下のリストには、「安全である」と考えられるホワイト リストの国の名前が含まれています。

```
オーストラリア
オーストリア
ベルギー
カナダ
デンマーク
エストニア
フィンランド
フランス
ドイツ
ギリシャ
アイスランド
イタリア
リヒテンシュタイン
ルクセンブルグ
モンテネグロ
```


オランダ
 ノルウェー
 ポルトガル
 サウジアラビア
 シンガポール
 スペイン
 スウェーデン
 スイス
 アラブ首長国連邦
 United Kingdom
 米国
 バチカン

マッピング（または導出）リスト

このデータセットは、ユーザのアプリケーションによって渡される拡張可能エレメントから導出されるもので、名前と値のペアの形式の複雑なデータで構成されます。

たとえば、**ギャンブル**または**アダルト コンテンツ**のカテゴリに属する業者から発生したすべてのトランザクションをハイリスクとしてマークする場合、アドオンルールによって**業者情報**を取得し、この業者情報からグループ情報を導出し、このグループ情報を使用してトランザクションのリスクを計算する必要があります。これを行うには、ルールがマッピング データまたは導出データにアクセスできる必要があります。

リスト内の各エントリは、以下のようなフォーマットで、改行文字によって他のエントリと区別されます。例

```

<name1, value1>
<name2, value2>
.....
<namen, valuen>
  
```

たとえば、**Merchant_Name**、**Category** のフォーマットで以下のようなリストがあります。

800florals, 花配達
AdultReviews, アダルト コンテンツ
Amazon, オンライン ショッピング
American Airlines, 航空会社
BEST-BUY-DEAL, オンライン ショッピング
British Airways, 航空会社
Casinogamblingweb, ギャンブル
Cliphunter, アダルト コンテンツ
Costco, オンライン ショッピング
eBay, オンライン ショッピング
Emirates, 航空会社
Holiday Inn, サービス業
JackpotFinder, ギャンブル
Kingfisher, 航空会社
Marriott, サービス業
Ramada, サービス業
Shopping.com, オンライン ショッピング
SkyMall, オンライン ショッピング
Taj, サービス業
TWA, 航空会社
US Airways, 航空会社
Walmart, オンライン ショッピング
Yellow Cab, 運送業

カスタム ルール タイプの操作

RiskFort では、ビジネス要件に応じて任意のカスタム ルール タイプを定義して追加することもできます。



注：Master Administrator として RiskFort に新しいルール タイプを追加できます。一方で、Global Administrator および Organization Administrator は、そのカスタム ルール タイプを展開し、自分の権限の範囲内で組織のための新しいアドオン ルールを作成できます。

このセクションでは、以下の手順について説明します。

- [新しいルール タイプの追加](#)
- [既存のルール タイプの表示](#)

新しいルール タイプを追加する場合は、入力定義 XML ファイルを提供する必要があります。このファイルには、ルール パラメータ、属性、および適用可能な名前と値のペアを定義します。この実例を示すために、RiskFort のインストール時にサンプル XML ファイルもインストールされます。「[入力定義 XML のサンプル](#)」では、このサンプル XML ファイルについて説明しています。

新しいルール タイプの追加

新しいルール タイプを追加する方法

1. MA としてログインしていることを確認します。
2. メイン メニューの **[Services and Server Configurations]** タブをアクティブにします。
3. サブ メニューの **[RiskFort]** タブがアクティブであることを確認します。
4. **[Extensible Configurations]** セクションの下で、**[Add Rule Type]** リンクをクリックします。
[Add Rule Type] ページ ([図 6-1](#)) が表示されます。

図 6-1 [Add Rule Type] ページ

The screenshot shows the 'Arcot Administration Console' interface. The top navigation bar includes 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (selected), and 'Reports'. Below this, a sub-navigation bar shows 'RiskFort' and 'Administration Console'. The left sidebar lists 'System Configuration' (with links to RiskFort Connectivity, Trusted Certificate Authorities, Protocol Configuration, and RiskFort Queueing Server Connectivity) and 'Extensible Configurations' (with 'Add Rule Type' selected and a link to View Existing Rule Types). The main content area is titled 'Add Rule Type' and includes a note: 'Add new Add-On Rule Type to RiskFort. Note: Ensure that the Library Name does not contain the path or the extension.' The form contains three input fields: 'Name of the Rule Type', 'Library Name (Without Extension)', and 'Input Definition XML'. There is a 'Browse...' button next to the 'Input Definition XML' field and a 'Create' button at the bottom.

5. **[Name of the Rule Type]** フィールドに、作成したルール タイプを指定します。
6. **[Library Name]** フィールドに、ルールのライブラリのファイル名を拡張子とパスを付けずに指定します。

このファイルは以下のディレクトリで使用可能である必要があります。

- **Windows の場合**

`<install_location>\Arcot Systems\plugins\rules\addon\`

- **UNIX プラットフォームの場合**

`<install_location>/arcot/plugins/rules/addon/`

7. **[Browse]** をクリックして、入力定義 XML ファイルの場所に移動します。

RiskFort に付属の[入力定義 XML のサンプル](#)を参照してください。

8. **[Create]** をクリックして、指定したアドオンルール タイプを作成します。
9. ルール タイプを追加したら、アプリケーション サーバの適切な場所にある `\arcotadmin` ディレクトリに移動します。

たとえば Apache Tomcat の場合は以下の場所になります。

`<APP_SERVER_HOME>/arcotadmin/WEB-INF/classes/`

10. エディタを使用して、`riskfort-admin-message.properties` ファイルを開きます。

11. ファイルに、以下の行を追加します。

```
txt.riskserver.addonrule.$RULE_TYPE_NAME=$DISPLAYNAME
```

ここで、`$RULE_TYPE_NAME` は追加されたルール タイプの名前であり、`$DISPLAYNAME` は画面（レポート）に表示される値を表します。

例

```
txt.riskserver.addonrule.WhiteListedIp=White Listed IP
```

12. 変更を保存してファイルを閉じます。
13. 必要に応じてアプリケーション サーバを再起動します。

既存のルール タイプの表示

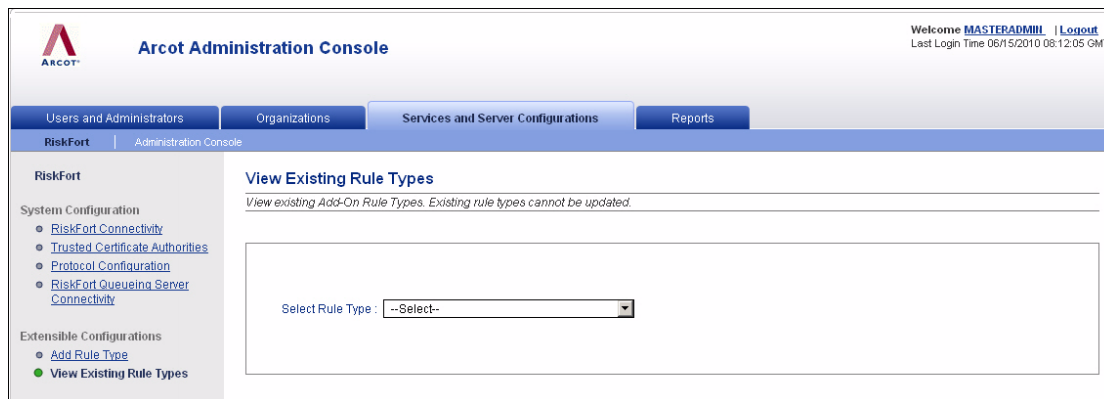
RiskFort では、ユーザが追加したアドオン ルール タイプを更新できません。ただし、システム定義のルール タイプまたは [Add Rule Type] ページ (図 6-1) を使用して追加した任意のカスタム ルール タイプを表示できます。

現在システムに存在するルール タイプを表示する方法

1. MA としてログインしていることを確認します。
2. メイン メニューの [Services and Server Configurations] タブをアクティブにします。
3. サブ メニューの [RiskFort] タブがアクティブであることを確認します。
4. [Extensible Configurations] セクションの下で、[View Existing Rule Types] リンクをクリックします。

[View Existing Rule Types] ページ (図 6-2) が表示されます。

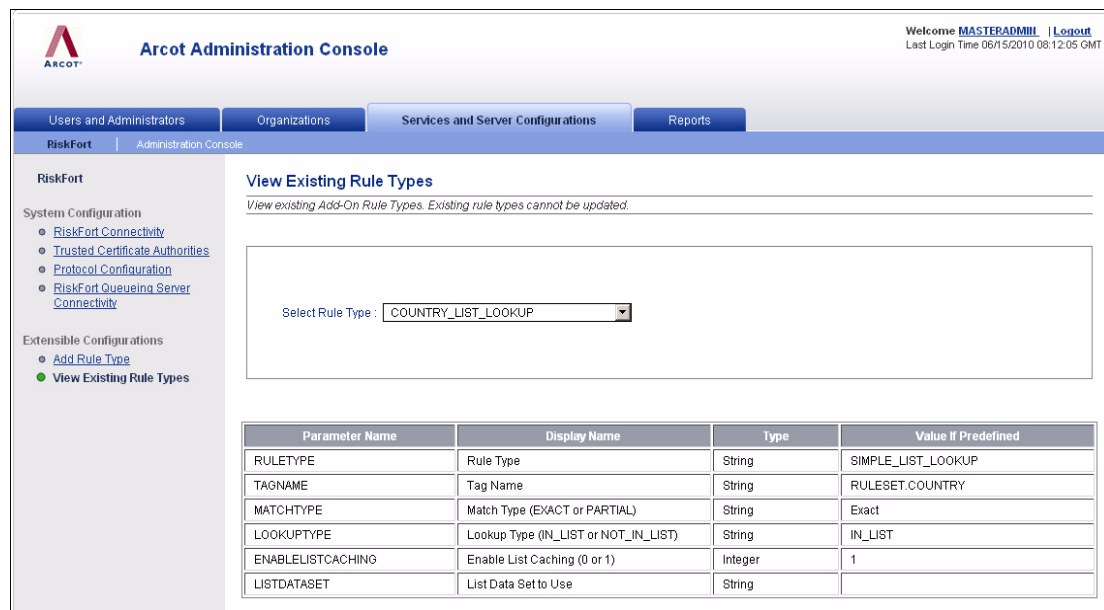
図 6-2 [View Existing Rule Types] ページ



5. [Select Rule Type] リストから、作成済みの必要なアドオンルールタイプを選択します。

選択したルールタイプの詳細がページに表示されます（図 6-2 を参照）。

図 6-3 [View Existing Rule Types] ページ



入力定義 XML のサンプル

RiskFort にはサンプルの XML ファイル ([SampleAddonRuleType.xml](#)) が付属しています。このファイルは、アドオン ルール タイプを定義する方法の一般的なフォーマットとそのタイプのパラメータについて説明しています。



注：現在は、テキスト ボックスの入力フィールドのみを使用できます。サポートが必要な場合は、Arcot テクニカル サポート (support@arcot.com) にお問い合わせください。

このサンプル ファイルは以下の場所にあります。

Windows の場合

```
<install_location>\Arcot Systems\samples\addonruletype\
```

UNIX プラットフォームの場合

```
<install_location>/arcot/samples/addonruletype/
```

[SampleAddonRuleType.xml](#) には以下の XML 定義が含まれます。

```
<ADDONTYPE>
  <NAME>MYNEWTYPE</NAME>
  <ORGNAME>DEFAULTORG</ORGNAME>
  <PARAMETER>
    <NAME>MerchId</NAME>
    <VALUE>MID</VALUE>
    <TYPE>1</TYPE>
    <ATTRIBUTE>
      <NAME>DISPNAME</NAME>
      <VALUE>Merchant ID</VALUE>
      <TYPE>1</TYPE>
    </ATTRIBUTE>
    <ATTRIBUTE>
      <NAME>DISPTYPE</NAME>
      <VALUE>TEXTBOX</VALUE>
```

```
<TYPE>1</TYPE>
</ATTRIBUTE>
<ATTRIBUTE>
  <NAME>DISPROW</NAME>
  <VALUE>1</VALUE>
  <TYPE>2</TYPE>
</ATTRIBUTE>
</PARAMETER>
<PARAMETER>
  <NAME>ListID</NAME>
  <VALUE>LID</VALUE>
  <TYPE>1</TYPE>
  <ATTRIBUTE>
    <NAME>DISPNAME</NAME>
    <VALUE>List ID</VALUE>
    <TYPE>1</TYPE>
  </ATTRIBUTE>
  <ATTRIBUTE>
    <NAME>DISPTYPE</NAME>
    <VALUE>TEXTBOX</VALUE>
    <TYPE>1</TYPE>
  </ATTRIBUTE>
  <ATTRIBUTE>
    <NAME>DISPROW</NAME>
    <VALUE>2</VALUE>
    <TYPE>2</TYPE>
  </ATTRIBUTE>
</PARAMETER>
</ADDONTYPE>
```


第 7 章

グローバル ルール設定の管理



重要：この章で説明するすべての設定およびタスクは、**Global Administrator** のみが実行できます。

RiskFort 設定は 2 つのレベルで管理できます。

- グローバル レベル（すべての組織で利用可能）



注：これらのルールは、ルールを設定した **Global Administrator** のスコープ内にあるすべての組織に利用可能ですが、組織レベルでそのまま使用することはできません。たとえば、**Global Administrator** がグローバルレベルに拒否 IP アドレス ルールを設定しても、個々の組織は、グローバルルールからコピーするか、または同じルールを参照することによってこのルールを設定する必要があります。

- 組織レベル（個別の組織で利用可能）

これらの設定は、特定の設定対象の組織にのみ適用されます。

Global Administrator はシステム内のすべての組織に対してデフォルトのルール設定を個別に変更できますが、ほとんどの組織は何度も繰り返して同じ設定を使用している可能性があります。また、個々の組織にルール設定を行うことは、設定された組織が多数ある場合、厄介なタスクになります。この場合、ルールにグローバル設定を設定すると、**Organization Administrator**（OA）は毎回同じ設定を指定する必要がなくなります。



注：全体的または組織レベルで設定に加える変更は、自動的に適用されません。これらの設定変更を適用するには、すべてのサーバ インスタンスをリフレッシュする必要があります。

グローバル ルール設定の管理は、**RiskFort** 管理および最適化の重要な部分であり、**Global Administrator** の重要な責任です。この章では、システム内の現在と将来のすべての組織のために「テンプレート」として **GA** が設定できる、グローバル設定および **RiskFort** ルールについて説明します。これらの設定には次のものが含まれます。

- ルール セットの設定
- トラステッド IP アドレスの設定
- トラステッド アグリゲータの設定
- 拒否 IP アドレスの設定
- 拒否 IP タイプの設定
- [Negative Country List] の設定
- ユーザ頻度の設定
- デバイス頻度の設定
- ゾーン ホッピングの設定
- その他のルールの設定



注：これらの設定は、設定する GA の権限の範囲内にあるすべての組織に適用可能です。個別の組織を設定する場合は、Global Administrator (GA)、または対象組織の Organization Administrator (OA) としてログインする必要があります。

詳細については、第 11 章の「組織固有の RiskFort の設定の管理」を参照してください。

これらのタスクに加えて、GA は以下も行うことができます。

- 基本認証ポリシーの設定（実行方法の詳細については、[2-32 ページの「基本認証ポリシー設定の指定」](#)を参照）。
- プロファイル情報の変更（実行方法の詳細については、[2-23 ページの「パスワードとプロファイル情報の変更」](#)を参照）。

Global Administrator としてのログイン

最初の GA アカウントは MA が作成する必要があります。GA としてログインして設定を続行するには、MA からアカウントの詳細を取得する必要があります。

ログインする前に、最初のアカントへのログインに必要な ID とパスワードが通知されていることを確認します。何らかの理由でこのパスワードを紛失してしまった場合は、管理者に再度送信してもらうように連絡する必要があります。

基本クレデンシャル（ユーザ名 / パスワード）を使用して GA として Administration Console にログインする方法

1. Web ブラウザ ウィンドウを開きます。
2. URL を入力して Administration Console にアクセスします。デフォルトの Administration Console URL は次のとおりです。

<http://<hostname>:<port>/arcotadmin/adminlogin.htm>

上記の URL の [hostname](#) および [port](#) は、Administration Console が展開されているシステムのホスト名または IP アドレス、およびコンソールがリスンしているポートにそれぞれ置き換えます。



注： Administration Console にアクセスするためのこの URL にブックマークを付けることを推奨します。すべての GA、OA および UA は、この URL を使用して RiskFort のユーザ名 / パスワード クレデンシャルにより Administration Console にログインすることができます。

図 7-1 に示されているように、[Administrator Login] ページが表示されます。

図 7-1 管理者ログイン : 1 ページ

3. ログインする [Organization Name] を入力します。

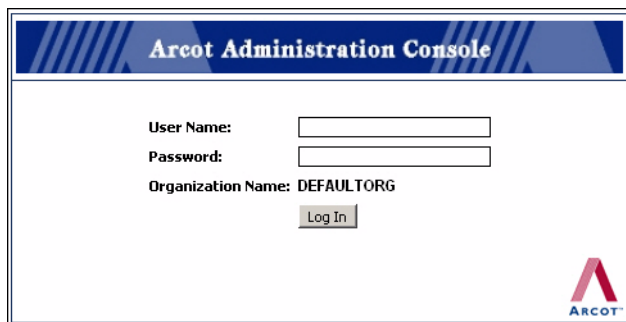


重要： 組織の表示名は入力しないでください。組織の一意の ID（組織名によって定義）を入力する必要があります。たとえば、デフォルトの組織（表示名は Arcot Systems）にログインする場合は、この組織の一意の ID（デフォルト）である **defaultorg** を入力する必要があります。ここで **Arcot Systems** を指定しないでください。

4. [Log In] をクリックします。

図 7-2 に示されているように、[Login] ページが表示されます。

図 7-2 管理者ログイン : 2 ページ



5. [User Name] フィールドにユーザ ID を指定して [Password] フィールドに通知された該当のパスワードを入力し、[Log In] をクリックします。

初めてログインする場合は、図 7-3 に示されているように、パスワードを変更するように求められます。

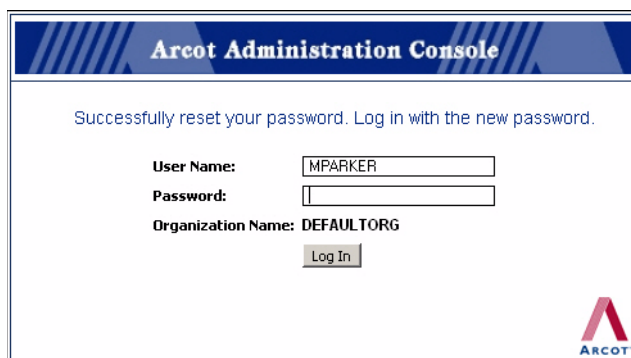
図 7-3 管理者ログイン : パスワードのリセット



6. [New Password]、[Confirm Password] を指定し、次に、[Log In] をクリックします。

図 7-4 に示されているように、ログイン ページにリダイレクトされます。

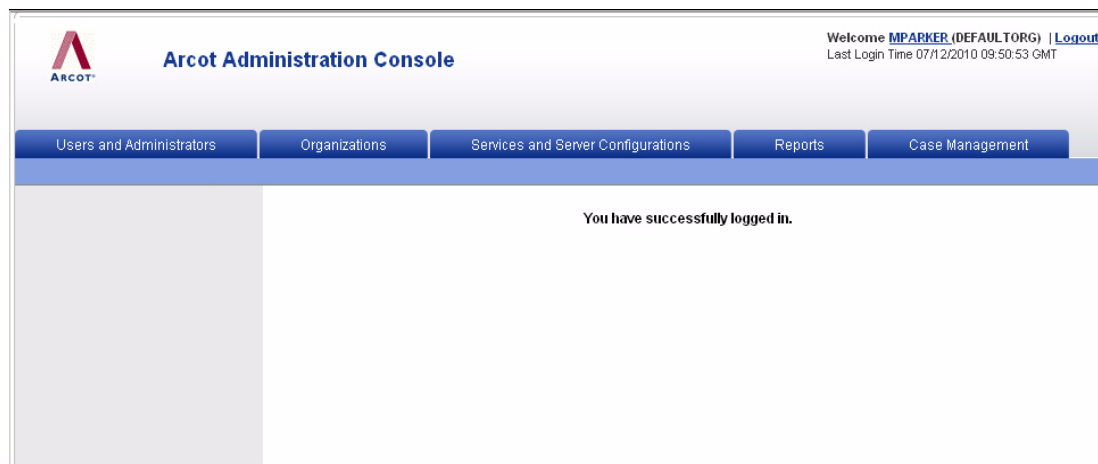
図 7-4 管理者ログイン : 2 ページ



7. 再度 **[Password]** を指定し、**[Log In]** をクリックします。

図 7-5 に示されているように、Administration Console のランディング ページが表示されます。

図 7-5 管理者ログイン : ログイン成功



Administration Console からのログアウト

Administration Console からログアウトするには、右上角にあるコンソールのヘッダ領域の **[Logout]** リンクをクリックします。

Administration Console 使用時のセキュリティに関する推奨事項

Administration Console を使用している間、ブラウザ セッションを介した悪意のある攻撃から RiskFort を保護するために、次のことを確認してください。

- 他のアプリケーションとブラウザ セッションを共有しない。
- コンソールで作業しているときに他のサイトを開かない。
- Administration Console に厳格なパスワード制限を実施する。
- Administration Console を使用した後は常にログアウトする。
- セッションが終わった後は、ブラウザ ウィンドウを閉じる。
- 実行が必要なタスクに応じて、ユーザに適切なロールを割り当てる。

ルール セットの設定

このセクションは、以下のトピックから構成されています。

- [ルール セットについて](#)
- [ルール セットの作成](#)

ルール セットについて

ルール セットは、設定した 1 つ以上の RiskFort ルール（[評価ルール](#)および[スコアリングエンジン](#)）の集合体で、実行順序およびスコアリングの優先度も含まれます。ルール セットはそれぞれが以下の観点から異なる場合があります。

- 設定されたルールのセット
- セット内の各ルールのスコアおよび優先度
- セット内のルールの有効化または無効化
- 各ルールの設定されたパラメータおよびデータ

Global Administrator は、スコープ内にあるすべての組織で利用可能な複数のグローバルルール セットを設定することができます。これらのルール セットを組織の他の GA または OA が使用し、既存のルール セットから「コピー」するだけで新しいルール セット

トを作成することができます。さらに、ルールセット内の「コピーされた」ルールは編集することもできます。これは、組織のために個別にルールを再度設定する時間および労力を大幅に節約するだけでなく、エラーの数も削減されます。



重要 : RiskFort には **DEFAULT** と呼ばれるすぐに使えるグローバル ルール セットが同梱されています。

ルール セットの作成



重要 : Global Administrator (GA) がグローバル ルール セットを作成した後、個々の組織の Organization Administrator (OA) はそれぞれの組織にこれらのルール セットを割り当てる必要があります。

これを実行する方法の詳細については、[11-176 ページの「ルール セットの割り当て」](#)を参照してください。

ルール セットの作成方法

1. GA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。
3. サイド バー メニューの [Ruleset] の下で、[Create Ruleset] リンクをクリックします。

ルール セットの作成ページ (図 7-6) が表示されます。

図 7-6 ルール セットの作成ページ

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

RiskFort | Administration Console

Ruleset

- **Create Ruleset**

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Create Ruleset

*Creates Rulesets. Rulesets can be copied.
If the new ruleset does not copy some other ruleset, the ruleset will be created with factory settings.*

Name :

- Advanced Options

☐ Copy from an Existing Ruleset

Create

4. **[Name]** フィールドにルール セットの名前を指定します。
5. **[Advanced Options]** で、必要に応じて以下の手順に従います。
 - a. 既存のルール セットからルール設定をコピーする場合は、**[Copy from an Existing Ruleset]** オプションを選択します。
 - b. 対応するリストから設定をコピーするルール セットの名前を選択します。
6. **[Create]** をクリックして新しいルール セットを作成して保存します。

ルール セットはまだアクティブでなく、エンド ユーザに利用可能ではありません。

7. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

トラステッド IP アドレスの設定

RiskFort では、トラステッド IP アドレス リストに属している IP アドレスまたは範囲から発信されるか、これらを経由するトランザクションは低リスクと考えます。その結果、RiskFort は、これらのトランザクションのリスク評価を省略し、低リスクのスコアと許可のアドバイスを割り当てます。

トラステッド IP アドレスおよび範囲に関連する以下のタスクを実行するには、[図 7-7](#)に示されているように、トラステッド IP/ アグリゲータの設定ページを使用します。

- [トラステッド IP アドレス範囲の追加](#)
- [トラステッド IP アドレス範囲の更新](#)
- [トラステッド IP アドレス範囲の削除](#)

図 7-7 トラステッド IP/ アグリゲータの設定ページ

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the text 'Arcot Administration Console' is in the center. On the right, it says 'Welcome MPARKER (DEFAULTORG) | Logout' and 'Last Login Time 07/12/2010 09:50:53 GMT'. Below this is a navigation bar with tabs: 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (which is active), 'Reports', and 'Case Management'. Under 'Services and Server Configurations', there are sub-tabs: 'RiskFort' and 'Administration Console'. The main content area is titled 'Trusted IP/Aggregator Configuration'. It includes a sub-header 'Select either Trusted IPs or Trusted Aggregators that you want to configure and click Next.' Below this is a large box containing two radio buttons: 'Trusted IPs' (which is selected) and 'Trusted Aggregators'. At the bottom right of this box is a 'Next' button. On the left side of the console, there is a sidebar menu. Under the 'RiskFort' section, there are links for 'Ruleset' (Create Ruleset) and 'Rules' (Trusted IP/Aggregator, Negative IP Address, Negative IP Types, Negative Country List, User Velocity, Device Velocity, Zone Hopping, Add-On Rules, Callout Configuration, Miscellaneous Rule Configurations). Under 'Data Upload', there are links for 'Upload List Data' and 'Upload Mapping Data'. Under 'Scoring', there is a link for 'Scoring Configuration'. Under 'Migrate to Production', there is a link for 'Migrate to Production'.

トラステッド IP アドレス範囲の追加

トラステッド IP アドレスまたは範囲を追加するには、以下のタスクを実行します。

1. GA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. サイド バー メニューの **[Rules]** の下で、**[Trusted IP/Aggregator]** リンクをクリックします。

トラステッド IP/ アグリゲータの設定ページ (図 7-7) が表示されます。

4. **[Trusted IPs]** オプションが選択されていることを確認し、**[Next]** をクリックします。

トラステッド IP の設定ページが表示されます。

5. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。
6. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
7. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。

- **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

トラステッド IP の設定ページ (図 7-8) が更新されて表示されます。

図 7-8 トラステッド IP の設定ページ

Arcot Administration Console

Welcome **MPARKER** (DEFAULTTORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted IP Configuration

Specify the range of IP addresses that are trusted. If this rule is scored first, then transactions originating from these IP addresses will receive an advice of Allow. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrtadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

Advanced Options

☒ Use Own
 ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

IP Address : [] . [] . [] . []
☒ **Subnet Mask :** [] . [] . [] . []
☐ **End IP Address :** [] . [] . [] . []

Add Range

Save Configuration

8. [Trusted IP List] に追加される必要な [IP Address] を指定します。
9. 以下のいずれかを指定します。
 - [Subnet Mask] : サブネット マスクに基づいて [Trusted IP List] に追加される IP アドレスの範囲を指定する場合。
 - [End IP Address] : [Trusted IP List] に追加される IP アドレスの単純な範囲を指定する場合。

10. **[Add Range]** をクリックして IP アドレスまたは範囲を **[Trusted IP List]** に追加します。

[Trusted IP List] テーブル (図 7-9) (追加した範囲の) が、ページの最後に表示されます。

図 7-9 トラストッド IP リスト

Trusted IP List			
Select	IP Address	Subnet Mask	End IP Address
☐	156 . 120 . 59 . 28	. . .	156 . 120 . 60 . 10

Delete Update

11. **[Save Configuration]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

12. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

トラストッド IP アドレス範囲の更新

トラストッド IP アドレスまたは範囲を更新する方法

1. [手順 1](#) から [手順 5](#) までを実行してトラストッド IP の設定ページを表示します。
2. **[Trusted IP List]** テーブルで必要な変更を加えます。
3. **[Trusted IP List]** テーブルで影響を受けた IP アドレスの範囲をすべて選択します。
4. **[Update]** をクリックして加えた変更を更新します。
5. **[Save Configuration]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

6. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

トラステッド IP アドレス範囲の削除

トラステッド IP アドレスまたは範囲を追加するには、以下のタスクを実行します。

1. [手順 1](#) から [手順 5](#) までを実行して *トラステッド IP の設定* ページを表示します。
2. **[Trusted IP List]** テーブルで、削除が必要な IP アドレス範囲を選択します。
3. **[Delete]** をクリックして選択した範囲を削除します。
4. **[Save Configuration]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

5. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

トラステッド アグリゲータの設定

アグリゲータは、複数の企業にわたってユーザのログイン情報を照合することによりアカウント集約サービスを提供するサードパーティ ベンダーです。多くの企業が、これらのアカウントとデータの集約サービス プロバイダのサービスを使用し、オンラインサービスの範囲を拡大しています。ユーザが保護されているポータルからログインする場合とそのようなアグリゲータを介してアクセスする場合とでは、発信元となる IP アドレスは異なります。

組織に信頼されているアグリゲータが発信元である（または経由している）トランザクションは低リスクであると考えられます。このため、RiskFort では、これらのアグリゲータのリストを設定する機能を提供し、アグリゲータの IP アドレスが発信元となっているすべてのトランザクションに低いリスク スコアおよび許可アドバイスを割り当てるようにします。

アグリゲータの IP は、IP の範囲と Aggregator ID を組み合わせて使用することにより、RiskFort によって一意に識別されます。Administration Console を使用して、トラステッド アグリゲータごとに 1 つの Aggregator ID が発行されます。この Aggregator ID はトランザクションと共に RiskFort に送信される必要があります。

また RiskFort では、各アグリゲータにつき 3 つまでの一意の ID をいつでも指定できます。これにより、セキュリティを強化する目的で ID を定期的にローテーションすることができます。このローテーション中に、RiskFort は、アグリゲータで後で更新できるように、新しい ID に加えて前の ID を引き続き認識します。

トラステッド IP アドレスおよび範囲に関連する以下のタスクを実行するには、[図 7-10](#)に示されているように、トラステッド IP/ アグリゲータの設定ページを使用します。

- [トラステッド アグリゲータの追加](#)
- [トラステッド アグリゲータの更新](#)
- [トラステッド アグリゲータの削除](#)

図 7-10 トラステッド IP/ アグリゲータの設定ページ

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title 'Arcot Administration Console' is in the center. On the right, a user greeting 'Welcome MPARKER (DEFAULTORG)' and a 'Logout' link are shown, along with the 'Last Login Time 07/12/2010 09:50:53 GMT'. Below the header is a navigation bar with tabs: 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (which is active), 'Reports', and 'Case Management'. Under the 'Services and Server Configurations' tab, there is a sub-tab 'RiskFort' and a link to 'Administration Console'. The main content area is titled 'Trusted IP/Aggregator Configuration'. It includes a instruction: 'Select either Trusted IPs or Trusted Aggregators that you want to configure and click Next.' Below this is a large box containing two radio buttons: 'Trusted IPs' (which is selected) and 'Trusted Aggregators'. A 'Next' button is located at the bottom right of this box. On the left side of the console, there is a sidebar menu with sections: 'RiskFort' (containing 'Ruleset' with a 'Create Ruleset' link and 'Rules' with a list of links including 'Trusted IP/Aggregator', 'Negative IP Address', 'Negative IP Types', 'Negative Country List', 'User Velocity', 'Device Velocity', 'Zone Hopping', 'Add-On Rules', 'Callout Configuration', and 'Miscellaneous Rule Configurations'), 'Data Upload' (with 'Upload List Data' and 'Upload Mapping Data' links), 'Scoring' (with 'Scoring Configuration' link), and 'Migrate to Production' (with 'Migrate to Production' link).

トラステッド アグリゲータの追加

トラステッド アグリゲータを追加するには、以下のタスクを実行します。

1. GA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。

3. サイド バー メニューの **[Rules]** の下で、**[Trusted IP/Aggregator]** リンクをクリックします。

トラステッド IP/ アグリゲータの設定ページ (図 7-10) が表示されます。

4. **[Trusted Aggregators]** オプションを選択し、**[Next]** ボタンをクリックします。

トラステッド アグリゲータの設定ページが表示されます。

5. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。

図 7-11 に示されているように、トラステッド アグリゲータの設定ページが更新されて表示されます。

6. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
7. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。

- **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

トラステッド アグリゲータの設定ページ (図 7-11) が更新されて表示されます。

図 7-11 トラステッド アグリゲータの設定ページ

Arcot Administration Console

Welcome **MPARKER** (DEFAULTTORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | **Administration Console**

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted Aggregator Configuration

Add a new aggregator that you trust or update the settings for an existing aggregator.

Update Existing Ruleset

SYSTEM - DEFAULT

Advanced Options

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name --Select--

Update Aggregator --Select--

Add Aggregator

Next

Save Configuration

8. **[Add Aggregator]** フィールドで新しいアグリゲータの名前を指定し **[Next]** をクリックします。

☒ 7-12 に示されているように、トラステッド アグリゲータの設定ページが更新されて表示されます。

図 7-12 トラストッド アグリゲータの設定ページ

Arcot Administration Console

Welcome **MPARKER** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted Aggregator Configuration

An aggregator is uniquely identified by using a combination of IP range and Aggregator ID. You can specify upto three unique IDs for each aggregator at any time. This enables you to periodically rotate or change the ID for the purpose of enhanced security. NOTE: RiskFort will continue to recognize the previous ID, in addition to the new ID to allow update on the aggregator at a later time.

Aggregator ID1 jsPKy5GG0jQuUxPVy3cf3I61JD0AwPnQlkrBIM4C+ZKsLJFUSAOM5g==

Aggregator ID2

Aggregator ID3

[Update Aggregator ID](#)

[Next](#)

9. **[Next]** をクリックして続行します。

図 7-13 に示されているように、トラストッド アグリゲータの設定ページが表示されます。

図 7-13 トラストッド アグリゲータの設定ページ

Arcot Administration Console

Welcome **MPARKER** (DEFAULT.ORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted Aggregator Configuration

Specify the range of IP addresses that are assigned to an aggregator. If this rule is scored first, then transactions originating from these IP addresses will receive an advice of Allow. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrtadmin` tool.

Aggregator: HSBC

IP Address : . . .

☒ **Subnet Mask :** . . .

☐ **End IP Address :** . . .

[Add Range](#)

10. トラストッド アグリゲータの設定ページで、以下の手順に従います。

- [**IP Address**] フィールドに開始 IP アドレスを入力します。
- 以下のいずれかのオプションを選択します。
 - [**Subnet Mask**] : サブネット マスクに基づいて [Trusted IP List] に追加される IP アドレスの範囲を指定する場合。
 - [**End IP Address**] : [Trusted Aggregator List] に追加される IP アドレスの単純な範囲を指定する場合。
- [**Add Range**] をクリックしてこの IP アドレスまたは範囲をデータベースに追加します。

アグリゲータに追加した範囲の [Trusted IP List] テーブル (図 7-14) が、ページの最後に表示されます。

図 7-14 アグリゲータのためのトラステッド IP リスト

Trusted IP List

Select	IP Address	Subnet Mask	End IP Address
☐	197 . 139 . 182 . 131	255 . 255 . 252 . 0	. . .

Delete
Update

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

11. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページ](#)の「[運用環境への移行](#)」を参照してください。

トラステッド アグリゲータの更新

RiskFort では Aggregator ID を更新できます。これらの ID の定期的な更新は Aggregator ID のローテーションと呼ばれています。



重要：アルコットでは、セキュリティ目的に Aggregator ID の定期的なローテーションまたは変更を推奨しています。このローテーション期間はビジネスルールに応じて決定できます。

ID が更新された後、最新の Aggregator ID がアグリゲータに伝えられていることを確認する必要があります。Aggregator ID の伝達には遅延が生じる場合があります。この期間、RiskFort は、新しい Aggregator ID と同様に古い ID も IP アドレスに関連付けられていることを認識します。



注：アグリゲータ側から始まるトランザクションには、RiskFort API によって指定された形式でこのアグリゲータ ID が含まれている必要があります。

アグリゲータ ID を更新する方法

1. [手順 1](#) から [手順 5](#) までを実行して、トラステッド アグリゲータの設定ページを表示します。
2. [Update Aggregator] リストから既存のアグリゲータを選択して [Next] をクリックします。

図 7-12 に示されているように、トラステッド アグリゲータの設定ページに、選択されたアグリゲータの Aggregator ID が表示されます。

3. [Update Aggregator ID] をクリックして新しい Aggregator ID を生成します。

図 7-15 に示されているように、アグリゲータの更新された Aggregator ID が表示され、次の空の Aggregator ID が表示されます。

図 7-15 トラステッド アグリゲータの設定ページ

The screenshot shows the Arcot Administration Console interface. The top navigation bar includes links for Users and Administrators, Organizations, Services and Server Configurations, Reports, and Case Management. The main content area is titled 'Trusted Aggregator Configuration' and contains a table with the following data:

Aggregator ID	Aggregator ID
Aggregator ID1	4p3q/9QMj0qGArG2LpW1aX+AhF9717c /aAukD7bm55y55Wb+SUcceg==
Aggregator ID2	jSPKy5GG0jQuUxPW3cf3l61JDoAwpNqlkrBIM4C+ZKsLJFUSAOM5g==
Aggregator ID3	

Below the table is a button labeled 'Update Aggregator ID'. At the bottom right of the main content area is a 'Next' button.

4. [Next] をクリックして続行します。

トラステッド アグリゲータの設定ページ (図 7-13) が表示されます。このページでは必要に応じて IP アドレス、範囲または指定された IP アドレスまたは範囲のサブネット マスクを更新できます。

5. [Trusted IP List] で、更新するアグリゲータ IP アドレスまたは範囲を選択します。
6. 必要な変更を加え、[Update] をクリックします。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

7. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

トラステッド アグリゲータの削除

トラステッド アグリゲータを追加するには、以下のタスクを実行します。

1. [手順 1](#) から [手順 5](#) までを実行して、トラステッド アグリゲータの設定ページを表示します。
2. **[Update Aggregator]** リストから既存のアグリゲータを選択して **[Next]** をクリックします。

Aggregator ID を更新するためのトラステッド アグリゲータの設定ページ ([図 7-12](#)) が表示されます。

3. **[Next]** をクリックします。

IP アドレス範囲を更新するためのトラステッド アグリゲータの設定ページ ([図 7-13](#)) が表示されます。

4. **[Trusted IP List]** で、削除するアグリゲータ IP アドレスまたは範囲を選択します。
5. **[Delete]** をクリックして、選択した情報を削除します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

6. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

拒否 IP アドレスの設定

拒否 IP アドレス リストは、過去に既知のアノニマイザ プロキシまたは詐欺や悪意のあるトランザクションの発信元となった IP アドレスの集合体です。このリストは、[「拒否 IP タイプの設定」](#)で説明されている [Negative](#) カテゴリのソースです。

[図 7-16](#) に示されているように、拒否 IP アドレス リスト ページを使用して組織の拒否 IP アドレス範囲を設定します。

図 7-16 拒否 IP アドレス リスト ページ

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- Negative IP Address**
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Negative IP Address List

Add to a list of Negative IP Address Range. Negative IP ranges can be added along with specifying whether the end IP address is a mask or an IP. Also one can specify the type of range added. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrfadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

Advanced Options

☒ Use Own
 ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Upload Negative IP Ranges

☒ Append
 ☐ Replace

Upload Data File: [Browse...](#)

[Upload](#)

Add/Delete Negative IP Range

IP Address: . . .
☒ Subnet Mask: . . .
☐ End IP Address: . . .
 Information Source:

[Add Range](#) [Delete Range](#)

[Save Configuration](#)

IP アドレス範囲の追加または削除

組織の拒否 IP アドレスおよび範囲を追加または削除する方法

1. GA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. サイド バー メニューの **[Rules]** の下で、**[Negative IP Address]** リンクをクリックします。

拒否 IP アドレス リスト ページが表示されます。

4. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

5. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
6. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。

- **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

更新されたページが表示されます (図 7-16)。

7. **[Advanced Options]** の下のセクションで以下の手順を行います。
 - a. **[IP Address]** フィールドに開始 IP アドレスを入力します。
 - b. 以下のいずれかのオプションを選択します。
 - **[Subnet Mask]** : サブネット マスクに基づいて **[Negative IP Address List]** に追加される IP アドレスの範囲を指定する場合。

- **[End IP Address]** : **[Negative IP Address List]** に追加される IP アドレスの単純な範囲を指定する場合。
- c. 拒否 IP アドレス範囲の**情報ソース**（またはベンダー）を指定します。
8. 必要に応じて、以下のいずれかのボタンをクリックします。
- **[Add Range]** : 指定された IP アドレスまたは範囲をデータベースに追加する場合。
 - **[Delete Range]** : データベースから指定された IP アドレスまたは範囲を削除する場合。
- 適切なメッセージが表示されます。
- 変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
9. 変更をアクティブにするには、それらを運用環境に移行する必要があります。
- これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

拒否 IP タイプの設定

RiskFort では、入力パラメータの 1 つとしてユーザのコンピュータの IP アドレスを使用して各トランザクションのリスクを評価します。RiskFort は受信トランザクションを評価して、拒否タイプとしてマークが付けられている IP アドレスからの発信であるか確認します。そのようなトランザクションは通常拒否されます。別の拒否タイプのカテゴリは次のとおりです。

• Negative

これが指定されている IP アドレスは、過去に不正トランザクションの発信元となっていました。



重要 : 拒否 IP アドレスの追加ページで IP アドレスを拒否対象として手動で設定（[「拒否 IP アドレスの設定」](#)で詳述）した場合は、このオプションを使用します。

• アクティブ

これが指定されている IP アドレスは、不正トランザクションの発信元となったことがあり、過去 6 か月間アクティブであった匿名プロキシの疑いがあります。

- **Suspect**

これが指定されている IP アドレスは、過去 2 年にわたってアクティブであったが、過去 6 か月はアクティブではなかった匿名プロキシの疑いがあります。

- **プライベート**

これが指定されている IP アドレスは、公にアクセス可能でない匿名プロキシの疑いがあります。これらのアドレスは、一般的に公に匿名サービスを販売する商業的企業に属しています。

- **非アクティブ**

これが指定されている IP アドレスは、不正トランザクションの発信元となった疑いがあり、過去 2 年間は非アクティブであったことがわかっています。

- **不明**

これが指定されている IP アドレスは、匿名プロキシの疑いがあり、現在それを否定する結果が得られていません。



注：アクティブ、Suspect、プライベート、非アクティブ、および不明の拒否タイプのカテゴリは、Quova データから派生しています。

組織に適切な拒否 IP アドレスのタイプを設定するには、[図 7-17](#) に示されているように、拒否 IP タイプの設定ページを使用します。

図 7-17 拒否 IP タイプの設定ページ



Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
 Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators

Organizations

Services and Server Configurations

Reports

Case Management

RiskFort

Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)**
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Negative IP Types Configuration

Select the IP Types that RiskFort will use to determine whether an incoming IP address is negative or not. For the changes to take effect, migrate them to production and refresh the server cache by running the `arradmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name --Select--

IP Type	Default	Active	Proposed
Negative <i>Negative IP addresses that you have manually configured.</i>	☒	☒	☒
Active <i>Anonymizers that have tested positive within the last six months.</i>	☒	☒	☒
Suspect <i>Anonymizers that have tested positive within the last two years, but not the last six months.</i>	☒	☒	☒
Private <i>Anonymous proxies that are not publicly accessible.</i>	☒	☒	☒
Inactive <i>Anonymizers that have not tested positive within the last two years.</i>	☐	☐	☐
Unknown <i>Anonymizers for which no positive test results are currently available.</i>	☐	☐	☐

Save

組織に適切な拒否 IP アドレスのタイプを設定する方法

1. GA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. サイド バー メニューの **[Rules]** の下で、**[Negative IP Types]** リンクをクリックします。

[Negative IP Types Configuration] ページが表示されます。

4. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

5. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
6. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。

- **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

図 7-17 に示されているように、更新された拒否 IP タイプの設定ページが表示されます。

7. **[Proposed]** 列で、各 **[IP Type]** に対して該当する拒否 IP アドレス カテゴリのタイプを選択します。
8. **[Save]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

9. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

[Negative Country List] の設定

[*Negative Country list*] は、不正または悪意のあるトランザクションが過去に発信されたと知られている国をすべて含みます。企業は、その国の規制に沿ってこのリストを保持することもできます。

RiskFort では、入力 IP アドレスに基づいて国情報を導き出します。その後、このデータを使用して、そのような国から発信されたオンライン トランザクションの不正の可能性をスコアリングします。このため、RiskFort では Quova と統合し、各 IP アドレスの詳細な地理情報を領域にマッピングすることによって提供して、分析を強化します。

Quova およびサービスの詳細については、以下を参照してください。

<http://www.quova.com>

RiskFort では受信トランザクションを評価し、これらのトランザクションが拒否対象としてマークが付けられた国に属している IP アドレスから発信されているかどうかを確認します。そのようなトランザクションは通常拒否されます。

[図 7-18](#) に示されているように、拒否国リスト ページを使用して、国を拒否国リストに追加するかまたはリストから削除します。

図 7-18 拒否国リスト ページ

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Log](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- Negative Country List**
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Negative Country List

Add or update the list of countries that have been source of high-risk transactions. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrfadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

Advanced Options

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Available Countries

AFGHANISTAN
ALAND ISLANDS
ALBANIA
ALGERIA
AMERICAN SAMOA
ANDORRA
ANGOLA
ANGUILLA
ANTARCTICA
ANTIGUA AND BARBUDA

Selected Countries

Save

[Negative Country List] を更新する方法

1. GA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. サイド バー メニューの **[Rules]** の下で、**[Negative Country List]** リンクをクリックします。

拒否国リスト ページが表示されます。

4. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。
5. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
6. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。
 - **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

図 7-18 に示されているように、拒否国リストページが更新されて表示されます。

7. **[Available Countries]** リストから **[Selected Countries]** リストに追加する国を選択します。
8. 選択した国をリストに移動するには、> または < ボタンをクリックします。また、すべての国を対象のリストに移動するには、>> または << ボタンをクリックします。



注：一度に 1 つ以上の国を選択するには、**Ctrl** キーを押します。

9. **[Save]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

10. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、8-125 ページの「運用環境への移行」を参照してください。

ユーザ頻度の設定

ユーザ頻度ルールでは、指定された期間のユーザからのトランザクション数のチェックを行います。ルールは以下のパラメータに基づきます。

- [Number of Risk Evaluations per User]

アドバイスまたはリスク スコアに関係なく指定されたユーザのための RiskFort に
よって実行されたトランザクション（**N**）の数を示します。

このパラメータのデフォルト値は **5** 秒です。

- [Time Interval]

トランザクションの数を追跡した期間（**T**）を示します。

このパラメータのデフォルト値は **60** 秒です。

- [Unit for Time Interval]

測定された期間（**T**）の単位を示します。

このパラメータのデフォルト値は**分**です。

 **7-19** に示されているように、ユーザ頻度の設定ページを使用してこのルールを設定
します。

図 7-19 ユーザ頻度の設定ページ

 **Arcot Administration Console** Welcome **MPARKER** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

[Users and Administrators](#) | [Organizations](#) | **[Services and Server Configurations](#)** | [Reports](#) | [Case Management](#)

RiskFort | [Administration Console](#)

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)**
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

User Velocity Configuration

Specify the maximum number of successive transactions allowed from the same user in the specified interval of time. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrtadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Parameter	Default	Active	Proposed
Number of Risk Evaluations per User	5	5	5
Time Interval	60	60	60
Unit for Time Interval	MINUTES	MINUTES	MINUTES

[User Velocity] ルールを設定する方法

1. GA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。
3. サイド バー メニューの [Rules] の下で、[User Velocity] リンクをクリックします。

ユーザ頻度の設定ページが表示されます。

4. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。
5. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
6. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。
 - **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

図 7-19 に示されているように、ユーザ頻度の設定ページが更新されて表示されます。

7. ページのテーブルで、以下の手順に従います。
 - a. **[Number of Risk Evaluations per User]** パラメータに **Proposed** 値を指定します。
 - b. **[Time Interval]** パラメータに **Proposed** 値を指定します。
 - c. **[Unit for Time Interval]** パラメータに **Proposed** 単位を選択します。

この値は、(指定された時間内で) 安全であると考えられるユーザのトランザクションの最大数を示します。指定された時間内のトランザクションの実数がこの数を超えると、RiskFort はリスクとして追跡し、結果として **[User Velocity]** ルールと一致させます。

8. **[Save]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

9. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

デバイス頻度の設定

デバイス頻度ルールでは、指定された期間のデバイスからのトランザクション数のチェックを行います。ルールは以下のパラメータに基づきます。

- **[Time Interval]**

トランザクションの数を追跡した期間（**T**）を示します。

このパラメータのデフォルト値は **60** 秒です。

- **[Unit for Time Interval]**

測定された期間（**T**）の単位を示します。

このパラメータのデフォルト値は**分**です。

- **[Number of Risk Evaluations per Device]**

リスク評価の結果が成功または失敗であるかに関係なく、指定されたデバイスの RiskFort によって実行されたトランザクション（**M**）の数を示します。

このパラメータのデフォルト値は **10** 秒です。

[図 7-20](#) に示されているように、デバイス頻度の設定ページを使用してこのルールを設定します。

図 7-20 デバイス頻度の設定ページ

Arcot Administration Console

Welcome **MPARKER** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- Device Velocity**
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Device Velocity Configuration

Specify the maximum number of successive transactions allowed from the same enduser-device in the specified interval of time. For the changes to take effect, migrate them to production and refresh the server cache by running the **arrfadmin** tool.

Update Existing Ruleset

SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Parameter	Default	Active	Proposed
Number of Risk Evaluations per Device	10	10	10
Time Interval	60	60	60
Unit for Time Interval	MINUTES	MINUTES	MINUTES

Save

「Device Velocity」ルールを設定するには、以下の手順に従います。

1. GA としてログインしていることを確認します。
2. 「Services and Server Configurations」タブをアクティブにします。
3. サイドバーメニューの「Rules」の下で、「Device Velocity」リンクをクリックします。

デバイス頻度の設定ページが表示されます。

4. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。
5. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
6. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。
 - **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

 **7-20** に示されているように、デバイス頻度の設定ページが更新されて表示されます。

7. ページのテーブルで、以下の手順に従います。
 - a. **[Number of Risk Evaluations per Device]** パラメータに **Proposed** 値を指定します。
 - b. **[Time Interval]** パラメータに **Proposed** 値を指定します。
 - c. **[Unit for Time Interval]** パラメータに **Proposed** 単位を指定します。

この値は、(指定された時間内で) 安全であると考えられるデバイスのトランザクションの最大数を示します。指定された時間内のトランザクションの実数がこの数を超えると、RiskFort はリスクとして追跡し、結果として **[Device Velocity]** ルールと一致させます。

8. **[Save]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

9. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

ゾーン ホッピングの設定

ゾーン ホッピングは、短い時間の間に別々の離れた場所（かなりの距離で）で合理的に可能ではない速度で発生する、同じユーザからの連続のトランザクションを追跡します。たとえば、ボブが午前 9 時（GMT）にニューヨークからログインし、再度午前 10 時（GMT）にロンドンからログインした場合、[Zone Hopping] ルールは後者のトランザクションを危険として追跡します。

[Zone Hopping] ルールは、以下のパラメータ上に基づきます。

- **ユーザが移動できる最高速度**

ユーザが飛行機、自動車、列車のような通常の交通手段を使用して、物理的に移動できる最高速度（S、時速マイル）を示します。

（連続する 2 つのトランザクション間に）ユーザが移動したとみられる速度がこのあらかじめ設定されたしきい値速度（S）を超えた場合、RiskFort はそれを、ゾーン ホッピングとみなします。

デフォルトでは、この値は 500 マイルですが、ゾーン ホッピングの設定ページの **[Maximum Speed at which a User can Travel]** フィールドの値を設定することにより、設定できます。

- **[Maximum Number of Users Sharing the Same User ID]**

複数のユーザ（たとえば夫婦）が同じユーザ名を使用することがあります。そのような場合、ユーザが別々のゾーンに居る可能性があります。そのような場合、RiskFort がこれをゾーン ホッピングと見なさないようにする必要があります。たとえば、夫が午前 10 時（GMT）にニューヨークからログインし、妻が午前 11 時（GMT）にロンドンからログインした場合、RiskFort はこれらのトランザクションを危険としてマークしません。

デフォルトではこの値は 1 ですが、ゾーン ホッピングの設定ページの **[Maximum Number of Users Sharing the Same Username]** フィールドを編集することにより、値を 2 に設定できます。

- **[Maximum Distance Tolerance for IP Address Locations]**

ISP が提供する IP アドレスの場所にはばらつきがあるため、公の IP アドレスを使用してユーザの物理的な場所（地理緯度と経度）を厳密に特定することはできません。これを解決するために、RiskFort では、不確実性の補正（U、マイル単位）を使用して、トランザクションの発信元である IP アドレスの物理的な場所におけるばらつきを調整します。

デフォルトでは、このばらつきは約 50 マイルですが、ゾーン ホッピングの設定ページの **Maximum Distance Tolerance for IP Address Location** フィールドに値を設定することにより、それを設定できます。

このルールを設定するには、ゾーン ホッピングの設定ページ（[図 7-21](#)）を使用します。

図 7-21 ゾーン ホッピングの設定ページ

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- Zone Hopping**
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Zone Hopping Configuration

*If multiple transactions from a single user are originating from different geographic locations in quick succession, specify the speed at which the user can possibly travel. Also specify if the user account is shared between two people. For the changes to take effect, migrate them to production and refresh the server cache by running the **arrfdadmin** tool.*

Update Existing Ruleset
SYSTEM - DEFAULT

Advanced Options

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Parameter	Default	Active	Proposed
Maximum Speed at which a User can Travel (Miles per Hour)	500	500	500
Maximum Number of Users Sharing the Same User ID	1	1	1
Maximum Distance Tolerance for IP Address Locations (Miles)	50	50	50

Save

[Zone Hopping] ルールを設定する方法

1. GA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. サイド バー メニューの **[Rules]** の下で、**[Zone Hopping]** リンクをクリックします。

ゾーン ホッピングの設定ページが表示されます。

4. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。
5. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
6. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。
 - **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

図 7-21 に示されているように、ゾーン ホッピングの設定ページが更新されて表示されます。

7. **[Maximum Speed at which a User can Travel]** パラメータに **Proposed** 値を指定します。
8. **[Maximum Number of Users Sharing the Same User ID]** パラメータに **Proposed** 値を指定します。
9. **[Maximum Distance Tolerance for IP Address Locations]** パラメータに **Proposed** 値を指定します。
10. **[Save]** をクリックして変更を保存します。
11. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

その他のルールの設定

システムで**その他のルール設定の指定**（ユーザ作成モードおよびマシン **FingerPrint** のしきい値を含む）を続ける前に、まず**関連コンセプト**を理解する必要があります。

その他のルールの設定ページ（[図 7-22](#)）を使用して必要なユーザ作成モードを指定します。

関連コンセプト

その他のルールの設定ページ（[図 7-22](#)）の情報を正しく指定するために、以下を理解する必要があります。

- ユーザ作成モード
- マシン **FingerPrint** (MFP) のしきい値

ユーザ作成モード

以下のサブセクションで説明されているユーザ作成モードのいずれか 1 つを使用して、RiskFort データベースにユーザを作成することができます。

明示的なユーザ作成モード

この場合、(`evaluateRisk()` API を呼び出して) ユーザのトランザクションのリスク評価を実行する前に、`createUser()` API を明示的に呼び出して RiskFort 内にユーザを作成する必要があります。

ユーザを作成する前に `evaluateRisk()` を呼び出すと、RiskFort の既知のユーザ ルール（第 5 章の「**RiskFort ルールの基礎知識**」）に一致しないため、**ALERT** リスク アドバイスが表示されてしまいます。

暗黙ユーザ作成モード

ユーザ作成モードを暗黙に設定すると、`createUser()` API を呼び出して RiskFort 内にユーザを作成する必要はありません。この場合、トランザクションに対して `evaluateRisk()` API を呼び出すと、RiskFort は自動的に RiskFort 内にユーザを作成します（まだ存在しない場合）。

前にユーザが存在しなかった場合、指定されたユーザに対して `evaluateRisk()` が初めて呼び出される際に、RiskFort は既知のユーザ ルールに照合せずに **ALERT** アドバイスを返します。このユーザに対する `evaluateRisk()` へのすべての後続の呼び出しについては、RiskFort はこのユーザが RiskFort データベースに存在すると判断するため、ルールは一致します。

マシン FingerPrint (MFP) のしきい値

リスク プロファイルをリアルタイムで開発して、対応するリスク スコアおよびアドバイスを生成するため、RiskFort では、現在のトランザクションのためにユーザによって使用されているエンド ユーザ デバイスから広範囲の情報を収集します。この情報は以下に示すような多数のカテゴリに分類できます。

- オペレーティング システム情報
- ブラウザ情報
- 画面設定
- ユーザ設定

この情報はマシン FingerPrint (MFP) またはデバイス シグネチャと呼ばれます。指定されたユーザによる各トランザクションに対して、RiskFort は送られてくる MFP と保管されている MFP を照合します。この一致パーセンテージ (%) が [System Configuration] 画面中で指定された値以上である場合、それは「安全である」と考えられます。

その他のルール設定の指定

ユーザ作成モードおよび MFP しきい値パーセンテージを指定する方法

1. GA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。
3. サイド バー メニューの [Rules] の下で、[Miscellaneous Rule Configurations] リンクをクリックします。

その他のルールの設定ページが表示されます。

4. [Update Existing Ruleset] リストから、この設定が適用可能なルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

5. 必要な場合は、[+] 記号をクリックして [Advanced Options] を展開します。
6. 必要に応じて、[Advanced Option] で以下のいずれか 1 つのオプションを選択します。
 - [Use Own] : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、[Use Own] を選択し、[Copy from an Existing Ruleset] オプションを選択し、次に、[Ruleset Name] リストからその設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- [Refer an Existing Ruleset] : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更を行うことができません。

このオプションを使用するには、[Refer an Existing Ruleset] を選択し、[Ruleset Name] リストから参照したい設定のルールセットの名前を選択します。

図 7-22 に示されているように、指定されたルール セットの設定テーブルが表示されます。

図 7-22 その他のルールの設定ページ

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- Miscellaneous Rule Configurations**

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Miscellaneous Rule Configurations

Specify the mode in which users will be created in RiskFort database and the the Machine FingerPrint (MFP) match percentage at which a user transaction will be considered safe. The changes that you make on this page will not be effective unless you migrate them to production and refresh the server cache by running the **arrfadmin** tool.

Update Existing Ruleset

SYSTEM - DEFAULT

Advanced Options

☒ Use Own
 ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Parameter	Default	Active	Proposed
User Creation Mode	Explicit	Explicit	☐ Implicit ☒ Explicit
Machine FingerPrint (MFP) Threshold, in Percentage	50	50	50

Save

7. **[Proposed]** 列の下で、**[User Creation Mode]** に必要なオプション (**[Implicit]** または **[Explicit]**) を選択します。
8. **[Proposed]** 列の下で、**[Machine FingerPrint (MFP) Threshold, in Percentage]** オプションに必要な値を指定します。
9. **[Save]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

10. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

これを行うための手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

第 8 章 スコアリングの設定

この章では、ビジネス要件に合わせて RiskFort のスコアリングを設定する方法について説明します。RiskFort のデフォルトの（既定の）設定を更新しても、変更はすぐにアクティブ（エンド ユーザが使用可能な状態）にはなりません。Administration Console のサイド バー メニューにある **[Migrate to Production]** リンクを使用して、提示された設定変更をすべて運用環境のデータベースに「移動する」必要があります。RiskFort によって使用される、デフォルトの設定データ、提示された設定データ、アクティブな設定データの概念を理解するには、「[運用環境への移行](#)」を参照してください。

この章では、以下の内容について説明します。

- [RiskFort のスコアリングについて](#)
- [スコアリングの設定](#)
- [運用環境への移行](#)



注：設定関連のアクティビティを実行する管理者には、これらの操作を実行する権限が必要です。各レベルの管理者が使用可能な権限の詳細については、[第 1 章の「管理者権限のサマリ](#)」を参照してください。

RiskFort のスコアリングについて

アプリケーションからリスク評価リクエストが発生すると、RiskFort は[評価ルール](#)を実行してリスク スコア（またはスコア）を生成します。通常、このスコアは 0 ～ 100 までの値であり、推奨されるリスク アドバイス（またはアドバイス）にマップされます。その後で RiskFort は[スコアリング エンジン](#)を使用して、最終的なスコアおよび対応するアドバイスを生成します。

表 8-1 では、事前定義済みスコアの値範囲と対応するアドバイスのマッピングについて説明します。

表 8-1. リスク アドバイスのマトリクス

スコアの値（最小値）	スコアの値（最大値）	アドバイス	デフォルトの推奨アクション
0	30	許可	トランザクションの続行を許可します。
31	50	ALERT	適切なアクションを実行してください。 たとえば、現在ユーザ名が不明である場合、アラートを取得したらすぐに CSR にリダイレクトするか、RiskFort にユーザを作成することができます。
51	70	INCREASEAUTH	追加の認証を実行してから次の処理に進みます。
71	100	否認	トランザクションを拒否します。

スコアリングの設定

次の図（図 8-1）に示すスコアリングの設定ページを使用して、以下を設定します。

- デフォルト ルール、アドオン ルール、およびコールアウトを有効または無効にする
- リスク スコアおよびルールของスコアリングの優先度を設定する

図 8-1 スコアリングの設定ページ

Scoring Configuration

Enable or disable rules for execution and scoring, and configure the risk score and scoring priority of each rule. The Default Score is used, if none of the rules in the first table matched.

Update Existing Ruleset
 SYSTEM - DEFAULT

- Advanced Options

☐ Copy from an Existing Ruleset --Select--

RULENAME	ACTIVE				PROPOSED				
	Enabled Execution	Enabled Scoring	Risk Score	Priority	Enabled Execution	Enabled Scoring	Risk Score	Advice	Priority
Exception User Check	☒	☒	30	10	☒	☒	30	ALLOW	↓
Negative IP Check	☒	☒	100	20	☒	☒	100	DENY	↑ ↓
Negative Country Check	☐	☐	100	30	☐	☐	100	DENY	↑ ↓
Trusted IP/Aggregator Check	☒	☒	30	40	☒	☒	30	ALLOW	↑ ↓
Unknown User Check	☒	☒	50	50	☒	☒	50	ALERT	↑ ↓
DeviceID Check	☒	☒	65	60	☒	☒	65	INCREASEAUTH	↑ ↓
User Velocity Check	☒	☒	65	70	☒	☒	65	INCREASEAUTH	↑ ↓
Device Velocity Check	☒	☒	65	80	☒	☒	65	INCREASEAUTH	↑ ↓
Zone Hopping Check	☐	☐	65	90	☐	☐	65	INCREASEAUTH	↑ ↓
User Associated with Device and Device-MFP Matched	☒	☒	10	100	☒	☒	10	ALLOW	↑ ↓
Device-MFP Matched but User Not Associated with Device	☒	☒	65	110	☒	☒	65	INCREASEAUTH	↑ ↓
User Associated with Device but Device-MFP Does Not Match	☒	☒	65	120	☒	☒	65	INCREASEAUTH	↑ ↓
User Not Associated with Device and Device-MFP Does Not Match	☒	☒	65	130	☒	☒	65	INCREASEAUTH	↑

	ACTIVE	PROPOSED
DEFAULT SCORE	30	30

Save

ルールを有効または無効にする方法、およびリスク スコアとルールのスコアリングの優先度を設定する方法

1. GA または OA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。
3. サイド バー メニューの **[Scoring]** セクションの下で、**[Scoring Configuration]** リンクをクリックします。
スコアリングの設定ページが表示されます。
4. **[Update Existing Ruleset]** リストから、この設定を適用できるルール セットを選択します。
指定されたルール セットの設定情報が表示されます (図 8-1 を参照)。
5. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
6. 必要に応じて、**[Advanced Options]** セクションから **[Copy From an Existing Ruleset]** オプションを選択し、コピーする設定を持つルール セットの名前をリストから選択します。
このオプションを選択すると、必要に応じて既存のルール セットから設定をコピーして、その設定を変更できます。



注： このページで行った変更は、コピー元のルール セットには影響しません。

7. 表示された表の **[Proposed]** 列で、各ルールに対して以下の操作を行います。
 - a. **[Enabled Execution]** オプションをオン (ルールを有効) またはオフ (ルールを無効) にします。
 - b. **[Enabled Scoring]** オプションをオン (ルールのスコアリングを有効) またはオフ (ルールのスコアリングを無効) にします。
 - c. 必要なリスク スコアを指定します。
 - d. 上矢印 (↑) をクリックしてスコアリングの相対的優先度を上げるか、下矢印 (↓) をクリックして優先度を下げます。

8. **[DEFAULT SCORE]**（このページの 2 番目の表）の **[PROPOSED]** 列に、必要なリスク スコアを指定します。



注：RiskFort では、前の表に一致するルールがない場合に、この値を使用して最終的なリスク スコアとアドバイスを生成します。

9. **[Save]** をクリックして、この画面で行った変更を保存します。
変更はまだアクティブになっておらず、まだエンド ユーザは使用できません。
10. 変更をアクティブにするには、それらを運用環境に移行する必要があります。
移行の手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

運用環境への移行

RiskFort には、以下のルールおよび設定のデフォルトの（すぐに使用できる）設定が付属しています。

- トラストド IP アドレスおよびアグリゲータ
- 拒否 IP アドレス
- 拒否 IP タイプ
- 拒否国リスト
- ユーザ頻度
- デバイス頻度
- ゾーン ホッピング
- その他のルール設定
- スコアリング

さらに、以下を設定することもできます。

- アドオン ルール
- コールアウト

前のリストに関連するデータを設定している場合、そのデータは提示データと呼ばれます。このデータは、ある期間において、複数の管理セッションで作成できます。このデータを設定している場合、このデータは提示設定領域として保存され、対応する設定ページの **[Proposed]** 列に反映されます。その結果、**[Proposed]** 列に加えられた変更がこのデータに反映されます。

ユーザの要件に従ってすべてのデータを設定したら、そのデータを運用環境に移行し、[arrfadmin: サーバリフレッシュとシャットダウン ツール](#) ツールを使用して RiskFort サーバキャッシュをリフレッシュすることで、提示データをアクティブ データ（対応する設定ページの **[Active]** 列）に変換できます。



注： 任意の時点で、RiskFort サーバはアクティブ データの設定のみを使用して動作するようになります。

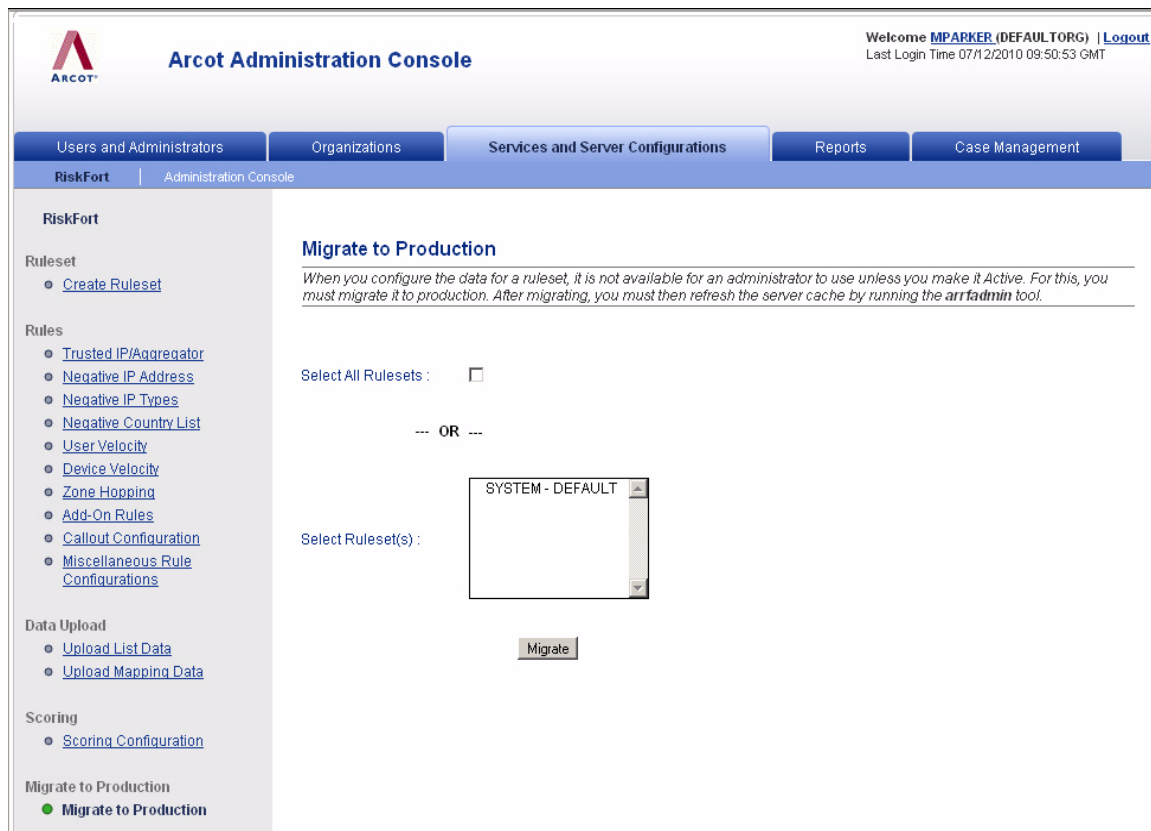
提示データがアクティブ データに移行された後に再度データを設定すると、提示設定領域にアクティブ データのコピーが作成されます。設定を運用環境に移行する準備ができるまで、さらに提示データの追加および削除を実行できます。すべての変更は提示データのみに反映されます。ただし、レポートはアクティブな設定または提示設定として表示することができます。



注： RiskFort の設定データに対する変更を記録するため、アクティブ データではバージョン管理が行われます。提示データが運用環境に移行されるたびに、新しいアクティブ設定データ セットに一意のデータ バージョンが作成されます。

図 8-2 に、この作業に使用できる **[Migrate to Production]** ページを示します。

図 8-2 [Migrate to Production] ページ



提示設定領域からアクティブ データ領域に変更を移行する方法

1. GA または OA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。
3. サイド バー メニューの [Migrate to Production] セクションの下で、[Migrate to Production] リンクをクリックします。

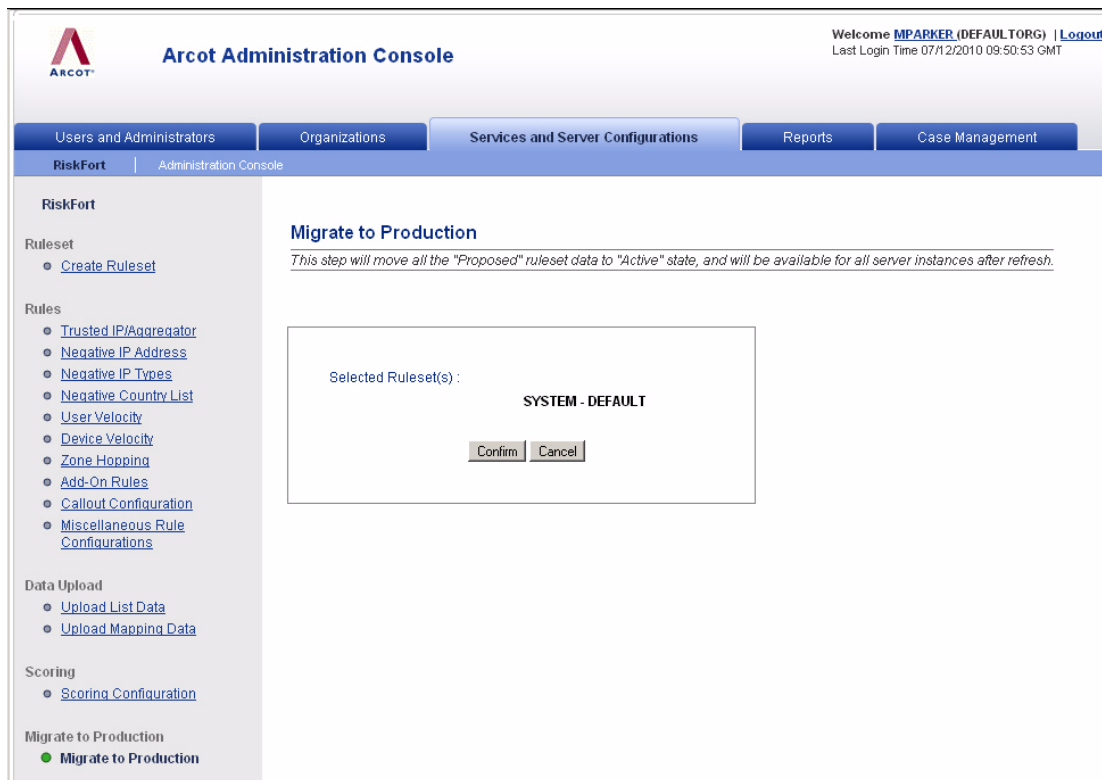
[Migrate to Production] ページが表示されます (図 8-2 を参照)。

4. このページで、以下のいずれかを実行します。
 - すべての設定済みのルール セットに対して行ったすべての変更を移行する場合は、[Select All Rulesets] オプションをオンにします。

または

- 現在のルール セットに対して行った変更を移行する場合は、[**Select Ruleset (s)**] リストから特定のルール セットを選択します。
5. [**Migrate**] をクリックします。
- アクションを確認するページが表示されます (図 8-3 を参照)。

図 8-3 Migrate to Production : 確認ページ



6. 確認ページで [**Confirm**] をクリックし、移行処理を開始します。

	注：運用環境に移行するデータ量によっては、この処理に数分かかる場合があります。

移行が完了すると、「The proposed data has been successfully migrated to Production.」というメッセージが表示されます。

7. 以下のように **arrfadmin** ツールを実行して、RiskFort サーバのキャッシュをリフレッシュします。

a. 以下のディレクトリに移動します。

- **Windows の場合**

```
<install_location>\Arcot Systems\bin\
```

- **UNIX ベースのプラットフォームの場合**

```
<install_location>/arcot/bin/
```

b. 以下のコマンドを実行します。

arrfadmin -r

コマンドを使用する前に、`riskfortadminclient.ini` に `Host` と `Port` の値を設定します。詳細については、[17-311 ページの「サーバとの双方向 SSL 通信用のツールの設定」](#)を参照してください。

第 9 章 コールアウトの設定



重要：この章で説明されているすべての設定およびタスクは、**Global Administrator** がルールを全体的に適用したり、**Organization Administrator** が組織にルールを適用する場合に実行できます。

組織に固有の設定を実行するためのタスク ページにアクセスする方法の詳細については、[第 11 章の「組織固有の RiskFort の設定の管理」](#)を参照してください。

コールアウトは、RiskFort の標準的な機能を変更または拡張するためのカスタム コンポーネント（任意のプログラミング言語で記述可能）です。コールアウトは通常、外部プロセスです。つまり、コールアウトは RiskFort サーバ コンテキストの「外部」に存在し、別の HTTPS ベースのサーバでホストされます。外部プロセスであるため、コールアウトは **Administration Console** を使用して設定する必要があります。設定することにより、必要に応じて起動できるようになります。

この章では、RiskFort がサポートするコールアウトのタイプ、およびビジネス要件を満たすコールアウトを設定する方法について説明します。さらに、RiskFort パッケージに同梱されているサンプル コールアウトの展開、設定、および使用方法についても説明します。

- [コールアウトについて](#)
- [コールアウトの設定](#)
- [サンプル コールアウトでの作業](#)



注：設定関連のアクティビティを実行する管理者には、これらの操作を実行する権限が必要です。各レベルの管理者が使用可能な権限の詳細については、[1-10 ページの「管理者権限のサマリ」](#)を参照してください。

コールアウトを設定した後、変更はすぐに**アクティブ**（エンド ユーザに利用可能）にはなりません。**提示された設定変更**を運用環境データベースにすべて「移動」するには、Administration Console のサイド バー メニューの **[Migrate to Production]** リンクを使用する必要があります。運用環境データベースに移行する手順については、[8-125 ページ](#)の「**運用環境への移行**」を参照してください。

コールアウトについて

ビジネス要件に基づいて、独自のカスタム評価ロジックおよびスコアリング ロジックを作成することができます。実装した場合、RiskFort コンテキストの外部にあるアプリケーション側で実行されます。これらのカスタム評価またはスコアリング プログラムは、アプリケーションのバックエンド システムとの対話用に実装できる**コールアウト**としても知られています。



注： RiskFort には、簡易評価コールアウトおよびスコアリング コールアウトを作成して実装する方法を示す基本的なサンプル コールアウト WAR ファイル（[riskfort-2.2.6-sample-callouts.war](#)）が同梱されています。このファイルを展開して設定する方法については、「[サンプル コールアウトでの作業](#)」を参照してください。

たとえば金融機関では、各トランザクションの発信元の追跡に加えて、トランザクションの金額に基づいた通常の銀行取引と電信送金のリスクの評価も希望します。銀行はトランザクションが普通取引であるか電信送金であるかに関係なく、30,000ドル以上のトランザクションすべてのリスクを評価します。この場合、RiskFort の **[Negative Country]**、**[Negative IP]**、**[Zone Hopping]** および **[Velocity]** チェックの使用に加えて、金融機関は評価コールアウト（アプリケーションの範囲内で）を作成することでこの動作を追跡することができます。



注： コールアウトが展開されたら、**[Callout Configuration]** ページ（[図 9-2](#)）を使用してコールアウトを有効にする必要があります。

コールアウトの実装



注：コールアウトの実装はオプションです。

コールアウトを実装した場合、RiskFort サーバはデータベースからコールアウトに関連する設定をすべて読み取り、スタートアップ時に情報をキャッシュします。トランザクションの間、以下の操作が行われます。

1. RiskFort サーバは、事前定義済みルールとアドオン ルール（評価コールアウトの場合）または標準的なスコアリング エンジン（スコアリング コールアウトの場合）をすべて実行した後にコールアウト フレームワークを呼び出します。



注：コールアウト フレームワークは RiskFort サーバの一部で、その他の RiskFort 評価ルールと同様に、サーバのスタートアップ中にロードされます。これは `.dll` または `.so` ファイルとして実装されます。

2. フレームワークは、コールアウトのタイプ（**[Evaluation]** または **[Scoring]**）に応じて RiskFort サーバから必要なデータをすべて収集し、`HTTP` または `HTTPS` データを準備します。



注：RiskFort では、`HTTPS` データの場合に RiskFort サーバとコールアウトの間で一方向および双方向の両方の SSL ベース接続をサポートしています。

3. その後、このデータはコールアウトの（設定されている）URL に投稿されます（`HTTP` または `HTTPS`）。

これで、コールアウト フレームワークはコールアウトからのレスポンスを待ちます。

評価コールアウトからのレスポンスが指定されたタイムアウト期間内に受信された場合、フレームワークはレスポンスを解析し、RiskFort サーバに結果を送信します。

レスポンスが指定されたタイムアウト期間内に受信されなかった場合、フレームワークは、ルールの結果として **FAILURE** を返し、修飾子と注釈には空の文字列 ("") を返します。

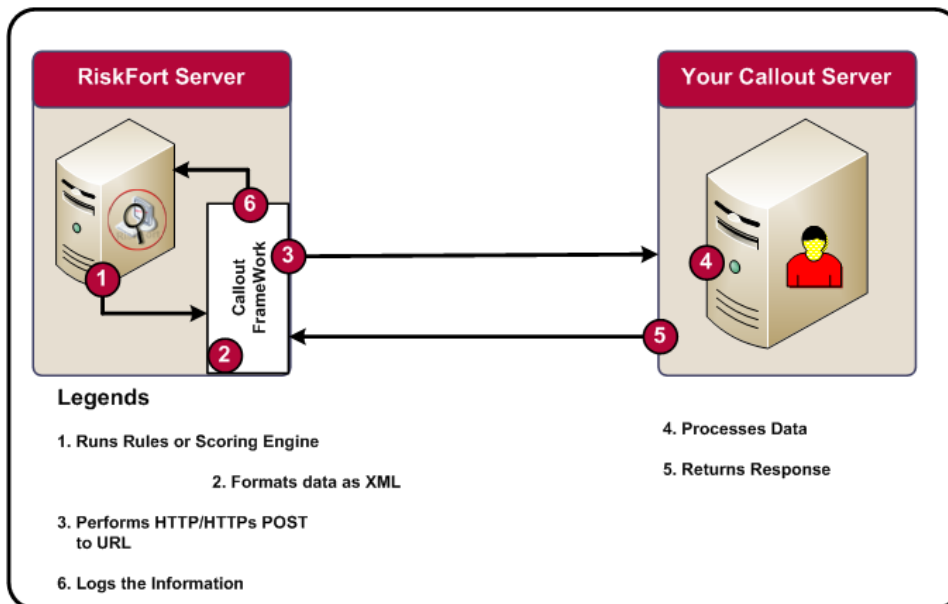


注： タイムアウト期間は **Administration Console** を使用することによって設定できます。

4. コールアウトではカスタム ロジックを使用してデータを処理します。
5. その後、コールアウトはコールアウト フレームワークに適切なレスポンスを返し、コールアウト フレームワークは RiskFort サーバに同じレスポンスを転送します。
6. RiskFort サーバは、レポートおよび監査目的のためにフレームワークによって返された情報をすべてログに記録します。

図 9-1 では、RiskFort サーバ、コールアウト フレームワーク、およびユーザのコールアウトの間の対話を示します。

図 9-1 コールアウトと RiskFort の間の対話





注：スコアリング コールアウトと同様に評価コールアウトも実装している場合は、それらを同じサーバ、または別々のサーバに実装することができます。

コールアウトのタイプ

RiskFort では、以下の 2 つのタイプのコールアウトをサポートしています。

- 評価コールアウト
- スコアリング コールアウト

評価コールアウト

評価コールアウトはリスク評価の一部として実行されます。評価コールアウトが実装された場合

1. RiskFort は Standalone、Add-On および Combination ルールをすべて実行し、コールアウト フレームワークを呼び出します。
2. RiskFort コールアウト フレームワークは、XML 形式でデータをフォーマットします。
3. RiskFort コールアウト フレームワークは、評価コールアウトに以下の情報の HTTP または HTTPS POST を実行します。
 - 各 RiskFort 評価ルールに渡される **コンテキスト情報**（ユーザ名、IP アドレスおよびデバイス ID など）。
 - 実行された各評価ルールの **ルール結果**。
 - RiskFort SDK から RiskFort サーバに入力データとして提供された **追加の入力**（ある場合）。
4. コールアウトでは、カスタム ロジックを処理するために RiskFort によって渡されたデータを使用します。
5. その後、コールアウトは RiskFort に以下の情報を返します。
 - **Y**（SUCCESS）または **N**（FAILURE）の形式による **ルール結果**。

- スコアリング コールアウト（実装されている場合）によって使用される追加の情報（ある場合）を持つ**修飾子文字列**。



注： RiskFort サーバは修飾子文字列を一切処理しません。スコアリング コールアウトも実装されている場合、RiskFort サーバはこのデータをスコアリング コールアウトに投稿します。

- RiskFort サーバに送り返された理由または説明が含まれている**注釈文字列**。



注： この情報はレポートおよび監査目的のためのログ（データベースで）に使用されます。

6. RiskFort サーバは、コールアウトによって返された情報をログに記録します。

スコアリング コールアウト

スコアリング コールアウトは標準的な RiskFort スコアリング ロジックが実行された後で実行されます。スコアリング コールアウトが実装された場合

- RiskFort サーバは標準的なスコアリング プログラムを実行し、コールアウト フレームワークを呼び出します。
- RiskFort コールアウト フレームワークは、XML 形式でデータをフォーマットします。
- RiskFort コールアウト フレームワークは、スコアリング コールアウトに以下の情報の [HTTP](#) または [HTTPS](#) POST を実行します。
 - 標準的な RiskFort ビルトイン スコアリング エンジンによって計算された**全体のスコア**。
 - 実行された各評価ルール**のルール結果**。
 - `evaluateRisk()` API 呼び出しの一部として呼び出し元アプリケーションによって提供された**追加の入力**（ある場合）。
 - 評価コールアウトによって最初に返された**修飾子文字列**。
- コールアウトでは、カスタム ロジックを処理するために RiskFort によって渡されたデータを使用します。
- その後、コールアウトは RiskFort に以下の情報を返します。

- [0 ~ 100] の範囲で整数の形式による**最終スコア**。



注：スコアリング コールアウトによって返されたスコアは、RiskFort スコアリング エンジンによって計算されたスコアを常に上書きします。RiskFort の標準的なスコアリング エンジンによって計算されたスコアを保持する場合は、レスポンスの戻り値と同じスコアを渡す必要があります。

- RiskFort サーバに送り返された理由または説明が含まれている**注釈文字列**。たとえば、[Annotation] フィールドにスコアを変更する理由を入力することができます。



注：この情報はレポートおよび監査目的のためのログ（データベースで）に使用されます。

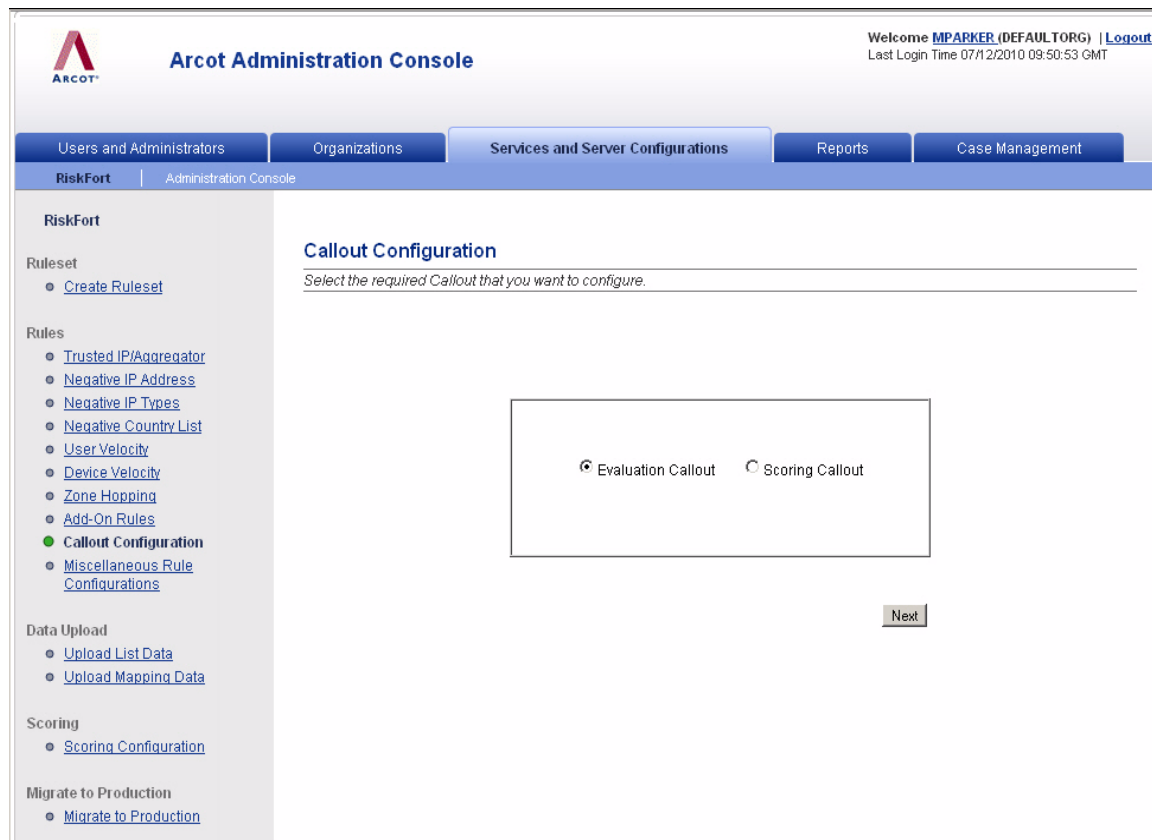
6. RiskFort サーバは、コールアウトによって返された情報をログに記録します。

コールアウトの設定

図 9-2 に示されているように、[Callout Configuration] ページを使用して以下を実行します。

- [評価コールアウトの設定](#)
- [スコアリング コールアウトの設定](#)

図 9-2 [Callout Configuration] ページ



注： RiskFort には、評価コールアウトおよびスコアリング コールアウトを作成して実装する方法を示す基本的なサンプル コールアウト WAR ファイル ([riskfort-2.2.6-sample-callouts.war](#)) が同梱されています。このファイルを展開して設定する方法の詳細については、この章の後半の「[サンプル コールアウトでの作業](#)」を参照してください。

評価コールアウトの設定

評価コールアウトを設定するには、以下の手順に従います。

1. GA としてログインしていることを確認します。
2. [Services and Server Configurations] タブをアクティブにします。

3. サイド バー メニューの **[Rules]** の下で、**[Callout Configuration]** リンクをクリックします。

図 9-2 のように、**[Callout Configuration]** ページが表示されます。

4. **[Evaluation Callout]** オプションが選択されていることを確認し、**[Next]** をクリックします。

図 9-3 のように、**[Evaluation Callout Configuration]** ページが表示されます。

5. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

6. 必要な場合は、**[+]** 記号をクリックして **[Advanced Options]** を展開します。
7. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。

- **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストから設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。



注：このオプションを選択した場合は変更が一切できなくなります。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

図 9-3 のように、**[Update Evaluation Callout Configuration]** ページが表示されます。

図 9-3 [Evaluation Callout Configuration] ページ

Arcot Administration Console Welcome **MPARKER** (DEFAULT.ORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

[Users and Administrators](#) [Organizations](#) [Services and Server Configurations](#) [Reports](#) [Case Management](#)

RiskFort | Administration Console

RiskFort

Ruleset
[Create Ruleset](#)

Rules
[Trusted IP/Aggregator](#)
[Negative IP Address](#)
[Negative IP Types](#)
[Negative Country List](#)
[User Velocity](#)
[Device Velocity](#)
[Zone Hopping](#)
[Add-On Rules](#)
[Callout Configuration](#)
[Miscellaneous Rule Configurations](#)

Data Upload
[Upload List Data](#)
[Upload Mapping Data](#)

Scoring
[Scoring Configuration](#)

Migrate to Production
[Migrate to Production](#)

Organization Name: _____ Display Name: _____ Status: _____

Evaluation Callout Configuration

*Specify the settings to deploy your custom Evaluation logic, which will be executed as a part of risk evaluation. The changes that you make on this page will not be effective unless you migrate them to production and refresh the server cache by running the **arradmin** tool.*

Update Existing Ruleset
 SYSTEM - DEFAULT

Advanced Options

☒ Use Own
 ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Callout Elements	Active	Proposed
Callout Elements		
Callout Server Root Certificate	Not Available	Browse
RiskFort Server Certificate and Private Key	Not Available	Certificate: Browse Private Key: Browse
Callout Description	Not Available	

Save

8. 表の **[Proposed]** 列で、以下の手順を実行します。

- a. サーバ認証 SSL に対して適切な SSL オプションを選択します。



重要： RiskFort サーバとコールアウトの間に SSL ベースの通信を設定する場合は、**[YES]** を選択する必要があります。

- b. クライアント認証 SSL に対して適切な SSL オプションを選択します。



注： このクライアントはユーザのコールアウトです。

- RiskFort サーバとコールアウトの間に双方向 SSL 接続を設定する場合は、**[YES]** を選択し、**サーバ認証 SSL** も **[YES]** に設定します。
 - RiskFort サーバとコールアウトの間に一方向 SSL 接続を設定する場合は、**[NO]** を選択します。この場合、**サーバ認証 SSL** が **[YES]** に設定されていることも確認してください。
 - SSL ベースの接続を設定しない場合は **[NO]** を選択する必要があります。この場合、**サーバ認証 SSL** も **[NO]** に設定しておく必要があります。
- c. **[Callout URL]** に対して使用可能なコールアウトの URL を指定します。
- **サーバ認証 SSL** が **[YES]** に設定されているか、または**クライアント認証 SSL** が **[YES]** に設定されている場合、評価コールアウトの URL は <https://> から始まる必要があります。
 - **サーバ認証 SSL** が **[NO]** に設定されていて、かつ**クライアント認証 SSL** も **[NO]** に設定されている場合、評価コールアウトの URL は <http://> から始まる必要があります。
- d. **[Connection Timeout]** の値を秒単位で指定します。
- [Connection Timeout]** は、RiskFort サーバとユーザのコールアウトの間の接続が期限切れになるまでの時間を示します。
- e. **[Read Timeout]** の値を秒単位で指定します。
- [Read Timeout]** は、RiskFort サーバがユーザのコールアウトからのレスポンスが戻るまでの予測時間を示します。

- f. **[Browse]** をクリックしてコールアウト サーバのルート証明書が配置されている場所へ移動します。

	注：以下を確認してください。 - サーバ認証 SSL が [YES] に設定されているか、クライアント認証 SSL が [YES] に設定されている場合は、コールアウト サーバルート証明書を指定する必要があります。 - コールアウト サーバルート証明書は PEM（Base64 にエンコードされた）形式である必要があります。

- g. **[Browse]** をクリックして **RiskFort** サーバ証明書および秘密キーが配置されている場所に移動します。

	注：以下を確認してください。 - クライアント認証 SSL が [YES] に設定されている場合、コールアウト サーバルート証明書および RiskFort サーバ証明書および秘密キーを指定する必要があります。 - RiskFort サーバ証明書および秘密キーは PEM（Base64 にエンコードされた）形式である必要があります。

- h. **[Callout Description]** に対してコールアウトに関する有用な詳細を指定します。

9. **[Save]** をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

10. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

移行手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

スコアリング コールアウトの設定

スコアリング コールアウトを設定するには、以下の手順に従います。

1. GA としてログインしていることを確認します。
2. **[Services and Server Configurations]** タブをアクティブにします。

3. サイド バー メニューの **[Rules]** の下で、**[Callout Configuration]** リンクをクリックします。

[Callout Configuration] ページ (図 9-2) が表示されます。

4. **[Scoring Callout]** オプションを選択し、**[Next]** ボタンをクリックします。

[Scoring Callout Configuration] ページが表示されます。

5. **[Update Existing Ruleset]** リストから、この設定が適用可能なルール セットを選択します。

6. **[+]** 記号をクリックして **[Advanced Options]** (図 9-4) を展開します。

7. 必要に応じて、**[Advanced Option]** で以下のいずれか 1 つのオプションを選択します。

- **[Use Own]** : このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、次に、**[Ruleset Name]** リストから設定をコピーするルール セットの名前を選択します。

このページで加えた変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択した場合は、変更が一切できなくなります。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

図 9-4 のように、**[Update Scoring Callout Configuration]** ページが表示されます。

図 9-4 [Scoring Callout Configuration] ページ



Arcot Administration Console

Welcome **MPARKER (DEFAULT TORG)** | [Logout](#)
 Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators

Organizations

Services and Server Configurations

Reports

Case Management

RiskFort

Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- **Callout Configuration**
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

• [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Organization Name: _____ **Display Name:** _____ **Status:** _____

Scoring Callout Configuration

Specify the settings to deploy your custom Scoring logic, which will be executed after RiskFort's Scoring logic. The changes that you make on this page will not be effective unless you migrate them to production and refresh the server cache by running the `arrfadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT ▼

[Advanced Options](#)

☒ Use Own
☐ Copy from an Existing Ruleset
 Ruleset Name: --Select-- ▼

☐ Refer an Existing Ruleset

☒ Use Own
☐ Copy from an Existing Ruleset
 Ruleset Name: --Select-- ▼

☐ Refer an Existing Ruleset

Server Authentication SSL	NO	YES ☒ NO ☒
Client Authentication SSL	NO	YES ☒ NO ☒
Callout URL	Not Available	
Connection Timeout (Seconds)	Not Available	
Read Timeout (Seconds)	Not Available	
Callout Server Root Certificate	Not Available	Browse...
RiskFort Server Certificate and Private Key	Not Available	Certificate: Browse...
		Private Key: Browse...
Callout Description	Not Available	

8. 表の **[Proposed]** 列で、以下の手順を実行します。

a. サーバ認証 SSL に対して適切な SSL オプションを選択します。

	重要 : RiskFort サーバとコールアウトの間に SSL ベースの通信を設定する場合は、 [YES] を選択する必要があります。

b. クライアント認証 SSL に対して適切な SSL オプションを選択します。

	注 : このクライアントはユーザのコールアウトです。

- RiskFort サーバとコールアウトの間に双方向 SSL 接続を設定する場合は、**[YES]** を選択し、**サーバ認証 SSL** も **[YES]** に設定します。
 - RiskFort サーバとコールアウトの間に一方向 SSL 接続を設定する場合は、**[NO]** を選択します。この場合、**サーバ認証 SSL** が **[YES]** に設定されていることも確認してください。
 - SSL ベースの接続を設定しない場合は **[NO]** を選択する必要があります。この場合、**サーバ認証 SSL** も **[NO]** に設定しておく必要があります。
- c. **[Callout URL]** に対して使用可能なコールアウトの URL を指定します。
- **サーバ認証 SSL** が **[YES]** に設定されているか、または**クライアント認証 SSL** が **[YES]** に設定されている場合、評価コールアウトの URL は <https://> から始まる必要があります。
 - **サーバ認証 SSL** が **[NO]** に設定されていて、かつ**クライアント認証 SSL** も **[NO]** に設定されている場合、評価コールアウトの URL は <http://> から始まる必要があります。
- d. **[Connection Timeout]** の値を秒単位で指定します。
- [Connection Timeout]** は、RiskFort サーバとユーザのコールアウトの間の接続が期限切れになるまでの時間を示します。
- e. **[Read Timeout]** の値を秒単位で指定します。
- [Read Timeout]** は、RiskFort サーバがユーザのコールアウトからのレスポンスが戻るまでの予測時間を示します。

- f. **[Browse]** をクリックしてコールアウト サーバのルート証明書が配置されている場所へ移動します。

	注：以下を確認してください。 - サーバ認証 SSL が [YES] に設定されているか、クライアント認証 SSL が [YES] に設定されている場合は、コールアウト サーバルート証明書を指定する必要があります。 - コールアウト サーバルート証明書は PEM (Base64 にエンコードされた) 形式である必要があります。

- g. **[Browse]** をクリックして **RiskFort** サーバ証明書および秘密キーが配置されている場所へ移動します。

	注：以下を確認してください。 - クライアント認証 SSL が [YES] に設定されている場合、コールアウト サーバルート証明書および RiskFort サーバ証明書および秘密キーを指定する必要があります。 - RiskFort サーバ証明書および秘密キーは PEM (Base64 にエンコードされた) 形式である必要があります。

- h. **[Callout Description]** に対してコールアウトに関する有用な詳細を指定します。
9. **[Save]** をクリックして変更を保存します。
- 変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
10. 変更をアクティブにするには、それらを運用環境に移行する必要があります。
- 移行手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

サンプル コールアウトでの作業

RiskFort 2.2.6 には、以下のような操作をデモする基本的な非 GUI のサンプル コールアウト WAR ファイル ([riskfort-2.2.6-sample-callouts.war](#)) が同梱されています。

- カスタム プログラムからの RiskFort サーバの基本的な操作（呼び出しと後処理）。
- コールアウトの RiskFort との統合。

このサンプル コールアウト WAR ファイルは、RiskFort の**完全**インストールの一部として自動的にインストールされます。**カスタム** インストールの一部として、この WAR ファイルにアクセスするには **RiskFort サーバ** コンポーネントのインストールを選択する必要があります。



重要： サンプル コールアウトは RiskFort サーバがインストールされている同じアプリケーション サーバ上で展開する必要があります。

このセクションでは次のものについて説明します。

- [サンプル コールアウトの展開](#)
- [サンプル コールアウトと通信するために RiskFort サーバを設定する](#)
- [サンプル コールアウトの使用](#)

サンプル コールアウトの展開

このセクションでは、サンプル コールアウトを展開するための手順について説明します。

- [Windows の場合](#)
- [UNIX ベースのプラットフォームの場合](#)

Windows の場合

RiskFort に同梱されているサンプル コールアウトをアプリケーション サーバの Windows に展開する方法

1. [設定] - [コントロール パネル] - [管理ツール] - [サービス] に移動します。
2. アプリケーション サーバのサービスを停止します。
3. [riskfort-2.2.6-sample-callouts.war](#) ファイルを以下の場所から展開します。

```
<install_location>\Arcot Systems\samples\java\
```



注: [riskfort-2.2.6-sample-callouts.war](#) はパッケージにも表示されますが、上記の場所からサンプル アプリケーション WAR ファイルを展開することをお勧めします。

4. [設定] - [コントロール パネル] - [管理ツール] - [サービス] に移動します。
5. アプリケーション サーバのサービスを再開します。

UNIX ベースのプラットフォームの場合

RiskFort に同梱されているサンプル コールアウトをアプリケーション サーバの UNIX ベースのプラットフォームに展開する方法

1. アプリケーション サーバのサービスを停止します。
2. [riskfort-2.2.6-sample-callout.war](#) ファイルを以下の場所から展開します。

```
<install_location>/arcot/samples/java/
```



注: [riskfort-2.2.6-sample-callout.war](#) はパッケージにも表示されますが、上記の場所からサンプル アプリケーション WAR ファイルを展開することをお勧めします。

3. アプリケーション サーバのサービスを再開します。

サンプル コールアウトと通信するために RiskFort サーバを設定する

サンプル コールアウトを設定するには、以下の手順に従います。

1. [手順 1](#) から [手順 7](#) までのタスクを実行して [Evaluation Callout Configuration] の表を表示します。
2. 表の [Proposed] 列で
 - a. サーバ認証 SSL に [NO] を選択します。
 - b. クライアント認証 SSL に [NO] を選択します。



注: このクライアントはサンプル コールアウトです。

- c. [Callout URL] オプションに対して以下を指定します。
<http://<host>:<port>/riskfort-2.2.6-sample-callouts/SampleEvalCalloutServlet>
 <host> はコールアウト WAR が展開されたサーバのホスト名または IP アドレスを示し、<port> はこのサーバが利用可能なポートを示します。
 - d. [Connection Timeout] の値を秒単位で指定します。デフォルト値は 30 秒です。
 - e. [Read Timeout] の値を秒単位で指定します。デフォルト値は 30 秒です。
 - f. [Callout Description] に対してコールアウトに関する有用な詳細を指定します。
 - g. [Save] をクリックして変更を保存します。
3. 手順 1 から 手順 6 までのタスクを実行して [Scoring Callout Configuration] の表を表示します。
 4. 表の [Proposed] 列で
 - a. サーバ認証 SSL に [NO] を選択します。
 - b. クライアント認証 SSL に [NO] を選択します。



注：このクライアントはサンプル コールアウトです。

- c. [Callout URL] オプションに対して以下を指定します。
<http://<host>:<port>/riskfort-2.2.6-sample-callouts/SampleScoringCalloutServlet>
 <host> はコールアウト WAR が展開されたサーバのホスト名または IP アドレスを示し、<port> はこのサーバが利用可能なポートを示します。
 - d. [Connection Timeout] の値を秒単位で指定します。デフォルト値は 30 秒です。
 - e. [Read Timeout] の値を秒単位で指定します。デフォルト値は 30 秒です。
 - f. [Callout Description] に対してコールアウトに関する有用な詳細を指定します。
 - g. [Save] をクリックして変更を保存します。
5. サイド バー メニューの [Scoring] の下で、[Scoring Configuration] リンクをクリックします。
 [Scoring Configuration] ページが表示されます。
 6. 表の最後にある [Evaluation Callout] および [Scoring Callout] までスクロールして、各々 [PROPOSED] 列の下で以下の変更を加えます。

- a. **[Enabled Execution]** を選択します。
- b. **[Enabled Scoring]** を選択します。
- c. **[Risk Score]** を指定します。
- d. **[Save]** をクリックして変更内容を保存します。

今まで加えたすべての変更はまだアクティブではなく、ユーザのエンド ユーザに利用可能ではありません。

7. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

移行手順については、[8-125 ページの「運用環境への移行」](#)を参照してください。

サンプル コールアウトの使用

RiskFort に同梱されたサンプル アプリケーションと異なり、サンプル コールアウトにはブラウザを使用してアクセスできるユーザ インターフェースがありません。これは、データがそれぞれのコールアウト（評価またはスコアリング）に投稿される方法、および RiskFort サーバにレスポンスが送信される方法をデモするだけのものです。ただし、サンプル コールアウトをサンプル アプリケーションと組み合わせて使用することにより、それがデフォルトのリスク評価およびスコアリング動作にどのように影響するか確認することができます。以下の手順に従ってください。

1. Web ブラウザ ウィンドウでサンプル アプリケーションを開始します。サンプル アプリケーションのデフォルトの URL は次のとおりです。
<http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp>
[RiskFort Sample Application] ページが表示されます。
2. **[Create User]** をクリックして新しいユーザを作成します。
3. ユーザが作成されたら、**[Main Page]** をクリックして [RiskFort Sample Application] ページに戻ります。
4. **[Evaluate Risk]** をクリックして作成した新規ユーザのリスク評価を実行します。

デフォルトでは、サンプル アプリケーションは、65 のリスク スコアと INCREASEAUTH のリスク アドバイスを生成します。ただし、サンプル コールアウトを展開して設定した後では、85 のリスク スコアと DENY のリスク アドバイスが表示されます。

第 10 章 組織の管理



注：この章のほとんどのタスクは、Global Administrator (GA) または Organization Administrator (OA) によって実行できます（その管理者が組織に対して必要なスコープを持っている場合）。

Arcot Administration Console では、組織を企業（または会社）全体、または特定の部門、部署、あるいは企業内のその他のエンティティのいずれかにマップすることができます。Administration Console で提供される組織構造はフラットです。つまり、組織階層（親子形式の組織）はサポートされていません。また、すべての組織はデフォルトの組織と同じレベルに作成されます（デフォルトの組織の詳細については、[2-29 ページの「組織のグローバル設定の指定」](#)を参照してください）。

企業が大きければ大きいほど、その組織構成は複雑になります。そのため、組織の管理は、管理の重要な部分を占めます。RiskFort では、以下の組織管理操作がサポートされています。

- [組織の作成およびアクティブ化](#)
- [組織の検索](#)
- [組織情報の更新](#)
- [組織の無効化](#)
- [組織の有効化](#)
- [初期状態の組織のアクティブ化](#)
- [組織の削除](#)



注：組織管理に関連する前述のタスク リストに加えて、OA は組織固有の設定も管理できます。これに関連する詳細については、[第 11 章の「組織固有の RiskFort の設定の管理」](#)を参照してください。

組織の作成およびアクティブ化

組織を作成したら、RiskFort リポジトリまたは既存の LDAP ベースのディレクトリ サーバの実装（Microsoft Active Directory や Sun ONE Directory Server など）のいずれかにそのデータを格納できます。



注：小規模の展開の場合には、新しい組織を作成する代わりに、デフォルトの組織の名前を変更できます。

このセクションでは、実装に基づいて、以下の手順について説明します。

- [Arcot リポジトリでの組織の作成](#)
- [LDAP リポジトリでの組織の作成](#)

必要な権限

組織の作成およびアクティブ化を可能にするには、これを行うための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべての組織を作成してアクティブにすることができます。GA は、自分のスコープ内のすべての組織を作成してアクティブにすることができます。

Arcot リポジトリでの組織の作成

Arcot リポジトリで組織を作成する方法

1. 組織を作成するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションで **[Create Organization]** リンクをクリックし、組織の作成ページ（[図 10-1](#)）を表示します。

図 10-1 組織の作成ページ



Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:00 GMT

Users and Administrators

Organizations

Services and Server Configurations

Reports

Case Management

Manage Organizations

Manage Organizations

Create Organization

[Search Organization](#)

Create Organization

In addition to the basic organization information, specify the authentication mechanism to be used for logging in administrators and the location of the repository where the user data is available.

Organization Information

Organization Name: *

Display Name: *

Description:

Administrator Authentication Mechanism: *

Basic User Password

User Data Location

Repository Type: *

Arcot Database

Create

4. 表 10-1 で説明するように、組織の詳細を入力します。

表 10-1. 組織の作成ページのフィールド

フィールド	説明
[Organization Information]	
[Organization Name]	作成する組織の一意の ID を入力します。 注：この組織にログインするには、 [Display Name] ではなく、この値を指定する必要があります。
[Display Name]	組織の説明を含む名前を入力します。 注：この名前は他のすべての Administration Console ページやレポートに表示されます。

表 10-1. 組織の作成ページのフィールド

フィールド	説明
[Description]	この組織を管理する管理者のための説明を入力します。 注：このフィールドを使用して、後で参照できるように組織の追加の詳細を入力できます。
[Administrator Authentication Mechanism]	この組織に所属する管理者の認証に使用されるメカニズムを選択します。Administration Console では、以下の 2 つタイプの認証メカニズムをサポートしています。 基本的なユーザ パスワード これは、Administration Console が提供する組み込みの認証メカニズムです。このオプションを選択する場合、管理者は自分の ID とパスワードを指定してコンソールにログインします。 WebFort ユーザ パスワード これは、WebFort のユーザ名 / パスワード認証方式です。このオプションを選択する場合、WebFort サーバによって管理者のクレデンシャルが発行されて認証されます。 このメカニズムを使用するには、Arcot WebFort 6.0 をインストールし、このオプションが動作するように設定する必要があります。WebFort の展開方法詳細については、「Arcot WebFort 6.0 インストールおよび展開ガイド」を参照してください。
[User Data Location]	
[Repository Type]	[Arcot Database] を選択します。このオプションを指定すると、新しい組織のユーザおよび管理者の詳細が、WebFort がサポートしている RDBMS リポジトリに格納されます。

5. **[Create]** をクリックして新しい組織を作成します。

管理者の追加ページ (図 10-2) が表示されます。

	注：現在システムに存在するすべての管理者の管理スコープがすべての組織である場合、このページは表示されません。

図 10-2 管理者の追加

6. **[Available Administrators]** リストから組織を管理する管理者を選択し、**[>]** ボタンをクリックして管理者を **[Managing Administrators]** リストに追加します。

[Available Administrators] リストに新しい組織を管理できるすべての管理者が表示されます。

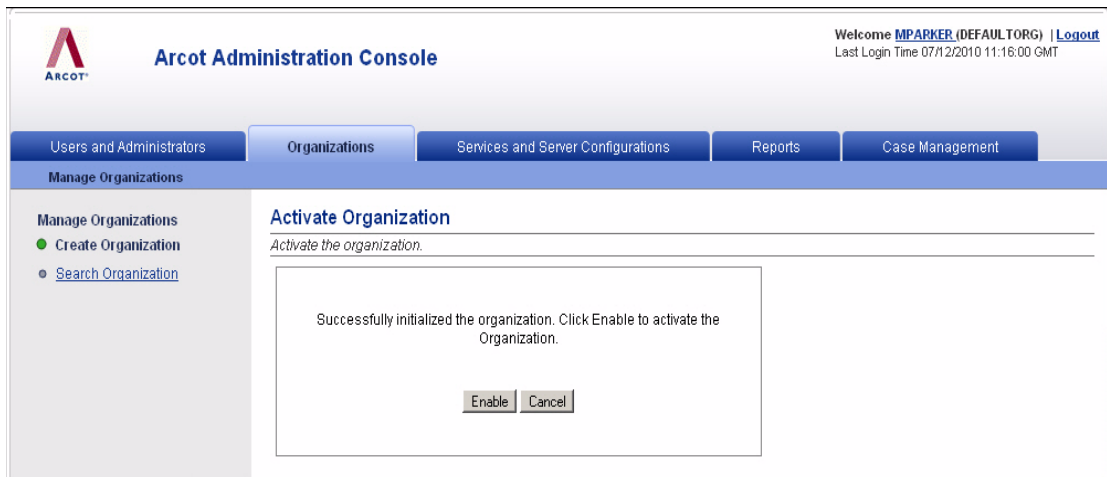


注：一部の管理者の管理スコープがシステムのすべての組織である場合、このリストにその管理者に対応するエントリは表示されません。

[Managing Administrators] リストには、この組織を管理するために選択した管理者が表示されます。

7. **[Next]** をクリックして、先に進みます。
組織のアクティブ化ページ (図 10-3) が表示されます。

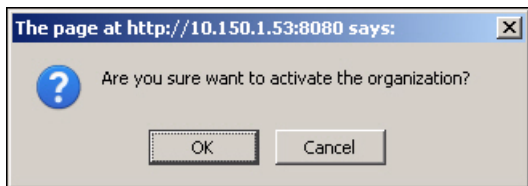
図 10-3 組織のアクティブ化



8. [Enable] をクリックして、新しい組織をアクティブにします。

図 10-4 に示すメッセージ ボックスが表示されます。

図 10-4 組織のアクティブ化：メッセージ



9. [OK] をクリックして、処理を完了します。
10. 展開されたすべての RiskFort サーバ インスタンスをリフレッシュします。その方法の手順については、[4-54 ページの「サーバ インスタンスのリフレッシュまたはシャットダウン」](#)を参照してください。

LDAP リポジトリでの組織の作成

LDAP ユーザ ディレクトリをサポートするには、Arcot リポジトリで組織を作成してから、Arcot の属性を LDAP 属性にマップする必要があります。以下の手順に従ってください。

1. 組織を作成するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションで **[Create Organization]** リンクをクリックし、組織の作成ページ (表 10-1) を表示します。
4. 表 10-2 で説明するように、組織の詳細を入力します。

表 10-2. LDAP リポジトリを使用する場合の **[Create Organization]** フィールド

フィールド	説明
[Organization Information]	
[Organization Name]	作成する組織の一意の ID を入力します。 注： Administration Console 使用してこの組織にログインするには、組織の [Display Name] ではなくこの値を指定します。
[Display Name]	組織の説明を含む名前を入力します。 注： この名前は他のすべての Administration Console ページやレポートに表示されます。
[Description]	この組織を管理する管理者のための説明を入力します。 注： このフィールドを使用して、後で参照できるように組織の追加の詳細を入力できます。
[Administrator Authentication Mechanism]	この組織に所属する管理者の認証に使用されるメカニズムを選択します。Administration Console では、以下の 2 つタイプの認証メカニズムをサポートしています。 • 基本的なユーザ パスワード これは、Administration Console が提供する組み込みの認証メカニズムです。このオプションを選択する場合、管理者は自分の ID とプレーン テキストのパスワードを指定してコンソールにログインします。 • WebFort ユーザ パスワード これは、WebFort のユーザ名 / パスワード 認証方式です。このオプションを選択する場合、WebFort サーバによって管理者のクレデンシャルが発行されて認証されます。 このメカニズムを使用するには、Arcot WebFort 6.0 をインストールし、このオプションが動作するように設定する必要があります。WebFort の展開方法詳細については、「Arcot WebFort 6.0 インストールおよび展開ガイド」を参照してください。
ユーザ データの場所	
[Repository Type]	[Enterprise LDAP] を選択します。このオプションを指定すると、新しい組織のユーザおよび管理者の詳細が、次のページで指定する LDAP リポジトリに格納されます。

5. **[Create]** をクリックして新しい組織を作成します。
LDAP リポジトリの詳細を収集する組織の作成ページ (図 10-5) が表示されます。

図 10-5 組織の作成 : エンタープライズ LDAP の詳細

The screenshot shows the Arcot Administration Console interface. The top navigation bar includes 'Users and Administrators', 'Organizations' (selected), 'Services and Server Configurations', 'Reports', and 'Case Management'. The left sidebar shows 'Manage Organizations' with 'Create Organization' highlighted. The main content area is titled 'Create Organization' and contains a form for 'Enterprise LDAP Details'. The form fields are: Host Name, Port Number, Schema Name, Base Distinguished Name, Connection Type (set to TCP), Login Name, Login Password, Server Trusted Root Certificate (with a Browse button), Client Key Store (with a Browse button), and Client Key Store Password. A 'Next' button is located at the bottom of the form.

6. 表 10-3 で説明するように、LDAP リポジトリに接続するための詳細を入力します。

表 10-3. LDAP リポジトリの詳細

フィールド	説明
[Host Name]	LDAP リポジトリが使用可能なシステムのホスト名を入力します。
[Port Number]	LDAP リポジトリ サービスが待ち受けるポート番号を入力します。

表 10-3. LDAP リポジトリの詳細

フィールド	説明
[Schema Name]	LDAP リポジトリが使用する LDAP スキーマを指定します。このスキーマには、LDAP リポジトリに含めることができるオブジェクトのタイプを指定します。また、各オブジェクト タイプの必須属性とオプションの属性を指定します。 通常、Active Directory のスキーマ名は <code>user</code> です。また、SunOne Directory では <code>inteorgperson</code> です。
[Base Distinguished Name]	LDAP リポジトリのベース識別名を入力します。この値は、LDAP リポジトリで検索する際に LDAP 階層の開始ノードを示します。 たとえば、 <code>cn=rob laurie</code> 、 <code>ou=sunnyvale</code> 、 <code>o=arcot</code> 、 <code>c=us</code> という DN を持つユーザを検索または取得するには、ベース DN を以下のように指定する必要があります。 • <code>ou=sunnyvale, o=arcot, c=us</code> 注：通常、このフィールドでは大文字と小文字が区別され、入力されたベース DN の下のすべてのサブノードが検索されます。
[Connection Type]	Administration Console と LDAP リポジトリの間で使用する接続のタイプを選択します。サポートされているタイプは以下のとおりです。 • TCP • 一方向 SSL • 双方向 SSL
[Login Name]	リポジトリ サーバにログインし、[Base Distinguished Name] を管理する権限を持つ LDAP リポジトリ ユーザの完全な識別名を入力します。 例を以下に示します。 <code>uid=gt,dc=arcot,dc=com</code>
[Login Password]	[Login Name] に入力したユーザのパスワードを入力します。
[Server Trusted Root Certificate]	必要な SSL オプションが選択されている場合、[Browse] ボタンを使用して、LDAP サーバへの SSL 証明書を発行した信頼済みルート証明書のパスを入力します。
[Client Key Store Path]	必要な SSL オプションが選択されている場合、[Browse] ボタンを使用してクライアント証明書と対応するキーを含むキー ストアのパスを入力します。 注：PKCS#12 または JKS キー ストア タイプのいずれかをアップロードする必要があります。
[Client Key Store Password]	必要な SSL オプションが選択されている場合、クライアント キー ストアのパスワードを入力します。

7. [Next] をクリックして、先に進みます。
- リポジトリ属性をマップするページ (図 10-6) が表示されます。

図 10-6 組織の作成：リポジトリ属性のマッピング

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/05/2010 05:21:50 GMT

Users and Administrators | **Organizations** | Services and Server Configurations | Reports | Case Management

Manage Organizations

Manage Organizations

- **Create Organization**
- [Search Organization](#)

Create Organization

Specify the LDAP Attribute Mapping details for the organization.
Note: The USERNAME Mapping is mandatory. You will not be able to change these mappings after the organization has been activated.

Repository Attribute Mapping

Arcot Database Attributes	Enterprise LDAP Attributes	Mapped Attributes
DATECREATED	audio	
DATEMODIFIED	businessCategory	
EMAILADDR	carLicense	
FNAME	cn	
LNAME	departmentNumber	
MNAME	description	
PAM	destinationIndicator	
STATUS	displayName	

Map UnMap Reset

Next

8. このページで以下の作業を行います。
- a. [Arcot Database Attributes] リストから属性を選択し、次に Arcot 属性にマップする必要がある適切な属性を [Enterprise LDAP Attributes] リストから選択し、[Map] をクリックします。

	重要：UserName 属性のマッピングは必須です。Active Directory を使用している場合は、cn に UserName をマップします。SunOne Directory を使用している場合は、uid に UserName をマップします。

- b. 必要なすべての属性のマッピングが完了するまで、プロセスを繰り返して複数の属性をマップします。



注： [Arcot Database Attributes] リストのすべての属性をマップする必要はありません。使用する属性のマッピングのみが必要です。

マップした属性は [Mapped Attributes] リストに移動されます。

必要に応じて、属性のマッピングを解除することができます。一度に 1 つの属性のマッピングを解除する場合は、属性を選択して [Unmap] をクリックします。[Mapped Attribute] リストをクリアする場合は、[Reset] をクリックしてマップされたすべての属性のマッピングを解除します。

9. [Next] をクリックして、先に進みます。

管理者の追加ページ (図 10-2) が表示されます。



注： 現在システムに存在するすべての管理者が管理を担当するスコープがすべての組織である場合、このページは表示されません。

10. [Available Administrators] リストから組織を管理する管理者を選択し、[>] ボタンをクリックして管理者を [Managing Administrators] リストに追加します。



注： 既存の管理者のスコープを更新したり、新しい管理者を作成して組織を管理させることで、いつでも組織を管理者に割り当てることができます。

[Available Administrators] リストに新しい組織を管理できるすべての管理者が表示されます。



注： 一部の管理者の管理スコープがシステムのすべての組織である場合、このリストにその管理者の対応するエントリは表示されません。

[Managing Administrators] リストには、この組織を管理するために選択した管理者が表示されます。

11. [Next] をクリックして、先に進みます。

組織のアクティブ化ページ（図 10-3）が表示されます。

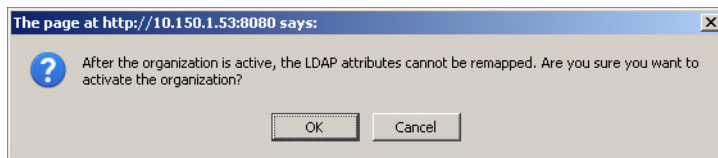


注：組織をアクティブにした後は、マッピングの詳細を変更したり更新することはできません。

12. [Enable] をクリックして、新しい組織をアクティブにします。

図 10-7 に示す警告メッセージが表示されます。

図 10-7 LDAP ベースの組織のアクティブ化



13. [OK] をクリックして、処理を完了します。

組織の検索

必要な権限

組織の更新、アクティブ化、または非アクティブ化を実行する必要がある限り、検索するために権限は必要ありません。ただし、検索する組織のスコープを担当している必要があります。たとえば OA は、ターゲットの組織がその OA の権限の範囲内にあれば、その組織を検索できます。

組織の検索

名前とステータスを使用して組織を検索できます。1 つ以上の組織を検索するには、以下の手順に従います。

1. 組織を作成するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. [Organizations] タブをアクティブにします。

3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして、組織の検索ページを表示します (図 10-8 を参照)。

図 10-8 組織の検索ページ

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo and 'Arcot Administration Console'. On the right, it says 'Welcome PLAUPIE (DEFAULTORG) | Logout' and 'Last Login Time 07/12/2010 11:16:24 GMT'. Below the header, there are tabs: 'Users and Administrators', 'Organizations' (selected), 'Reports', and 'Case Management'. Under 'Organizations', there's a sub-tab 'Manage Organizations'. In the left sidebar, under 'Manage Organizations', 'Search Organization' is selected with a green dot. The main content area is titled 'Search Organization' and contains a text input field with the placeholder 'Enter the (full or partial) Display Name of the organization that you want to search.' Below this is a table with columns: 'Organization', 'Initial', 'Active', 'Inactive', and 'Deleted'. The 'Active' checkbox is checked. To the right of the table is a 'Search' button.

4. 必要な組織の方法を一部または全部入力します。以下のオプションを選択すると検索範囲を広げることができます。



注： **[Organization]** フィールドには、実際の組織名ではなく、組織の表示名を一部または全部入力する必要があります。

- **[Initial]** (作成されたが、まだアクティブにされていない組織を表示する)。
- **[Active]** (作成され、アクティブにされた組織を表示する)。
- **[Inactive]** (無効にされた組織を表示する)。
- **[Deleted]** (削除された組織を表示する)。

5. [Search] をクリックして、指定された条件に一致するすべての内容をページ (図 10-9 と同様) に表示します。

図 10-9 組織の検索ページ：結果

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Arcot Administration Console

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations
● Search Organization

Search Organization

Click the Organization Name link to view or edit the details of the selected organization. To enable, disable, or delete multiple organizations, select the required organizations and click the applicable button.
Tip: You can also reorder the list of organizations by clicking the Organization column heading.

Organization	Initial	Active	Inactive	Deleted
	☐	☒	☐	☐

Select Organizations to Modify

☐	Organization	Display Name	Description	Status
☐	HSBC	HSBC		Active
☐	DEFAULTORG	DEFAULT ORGANIZATION	This is the initial default Organization.	Active
☐	SAFEBANK	Safe Bank		Active

組織情報の更新

Administration Console を使用して、組織の以下の情報を更新できます。

- 組織情報（組織の表示名、説明、ステータス、および組織を管理する管理者が含まれる（「[組織情報の更新](#)」を参照））
- 組織の **RiskFort 固有の設定**（クレデンシャルプロファイル、認証ポリシー、拡張可能な設定、および割り当てられたデフォルト設定が含まれる（「[RiskFort 固有の設定の更新](#)」を参照））

必要な権限

組織の更新を可能にするには、更新を行うための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべての組織を更新できます。GA と OA は、自分のスコープ内のすべての組織情報を更新できます。

組織情報の更新

基本的な組織情報を更新する方法

1. 組織を作成するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして、組織の検索ページを表示します (図 10-8 を参照)。
4. 検索する組織の情報を一部または全部入力し、**[Search]** ボタンをクリックします。
検索条件に一致した組織のリスト (図 10-9 と同様) が表示されます。
5. **[Organization]** 列の下で、必要な組織の `<ORGANIZATION_NAME>` リンクをクリックします。

組織情報ページ (図 10-10 と同様) が表示されます。

図 10-10 組織情報ページ

The screenshot displays the Arcot Administration Console interface. At the top, the header includes the Arcot logo, the title "Arcot Administration Console", and a user welcome message: "Welcome **BLAURIE** (DEFAULTORG) | Logout". Below the header, a navigation bar contains tabs for "Users and Administrators", "Organizations", "Reports", and "Case Management". The "Organizations" tab is active, and the "Manage Organizations" section is selected in the left sidebar. The main content area shows the details for the "DEFAULTORG" organization. A summary bar at the top of the details section lists "Organization Name: DEFAULTORG", "Display Name: DEFAULT ORGANIZATION", and "Status: Active". Below this, there are two sub-tabs: "Basic Organization Information" (selected) and "RiskFort Configuration". The "Basic Organization Information" section is titled "Organization Information" and includes a note: "Edit the required fields and click Next to save the changes." The "Organization Details" form contains the following fields and values:

Organization Name:	DEFAULTORG
Display Name: *	DEFAULT ORGANIZATION
Description:	This is the initial default Organ
Administrator Authentication Mechanism:	Basic User Password
Date Created:	07/02/2010 05:02:51 GMT
Last Modified:	07/02/2010 05:10:12 GMT
Default Organization:	Yes

At the bottom of the form, there is a "Next" button.

6. **[Organization Details]** セクションの必要なフィールド (**[Display Name]** および **[Description]**) を編集します。
7. **[Next]** をクリックして、追加の設定に進みます。
 - 組織が **Arcot リポジトリ** に作成され、かつ組織の管理者がシステムのすべての組織を管理するスコープを持っている場合、管理者の更新ページ (図 10-2 と同様) が表示されます。
 このページで、組織を管理する管理者を更新し、**[Update]** をクリックして変更を保存して、プロセスを完了します。
 - 組織が **LDAP リポジトリ** に作成された場合は、組織の編集ページ (図 10-5) が表示されます。
 - i. 必要に応じて、表 10-3 の情報を使用してフィールドを更新し、**[Next]** をクリックしてページを表示して、リポジトリ属性のマッピング (図 10-6) を編集します。
 - ii. 組織を作成したときに作成したマッピングを編集することはできません。
[Update] をクリックして、管理者の更新ページ (図 10-6) を表示します。
 - iii. 管理者の更新ページで組織を管理する管理者を更新し、**[Update]** をクリックして変更を保存し、プロセスを完了します。

RiskFort 固有の設定の更新

組織の RiskFort 設定を更新する方法

1. 組織を更新するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして、組織の検索ページを表示します (図 10-8 を参照)。
4. 検索する組織の情報を一部または全部入力し、**[Search]** ボタンをクリックして、検索条件に一致する組織のリスト (図 10-9 と同様) を表示します。
5. **[Organization]** 列の下で、必要な組織の **<ORGANIZATION_NAME>** リンクをクリックし、組織情報ページ (図 10-10 と同様) を表示します。
6. **[RiskFort Configuration]** タブをアクティブにして、タスク パネルの RiskFort 設定のリンクを表示します。
7. これらの設定の詳細については、第 11 章の「組織固有の RiskFort の設定の管理」を参照してください。

組織の無効化

組織のすべての管理者が Administration Console にログインしないようにし、組織のエンド ユーザが RiskFort メカニズムを使用してアプリケーションへの認証を行わないようにするには、組織を無効にします。

必要な権限

組織の無効化を可能にするには、無効にするための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべての組織を無効にすることができます。GA と OA は、自分のスコープ内のすべての組織を無効にすることができます。

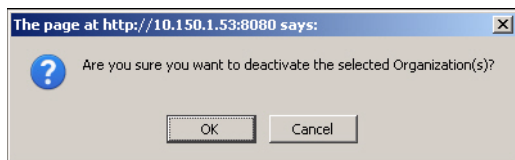
組織の無効化

1 つ以上の組織を無効にする方法

1. 組織を無効にするために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして、組織の検索ページを表示します (図 10-8 を参照)。
4. 検索する組織の情報を一部または全部入力し、**[Search]** をクリックします。
検索条件に一致した組織のリスト (図 10-9 と同様) が表示されます。
5. 無効にする 1 つ以上の組織を選択します。
6. **[Deactivate]** をクリックして選択された組織を無効にします。

図 10-11 に示すメッセージ ボックスが表示されます。

図 10-11 組織の非アクティブ化：メッセージ



7. **[OK]** をクリックして、非アクティブ化を確定します。

組織の有効化

無効にした組織を再び有効にする必要がある場合があります。この場合、組織の検索ページで検索条件を指定するときに、**[Inactive]** オプションをオンにする必要があります。

必要な権限

組織の有効化を可能にするには、有効にするための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべての組織を有効にすることができます。GA と OA は、自分のスコープ内のすべての組織を有効にすることができます。

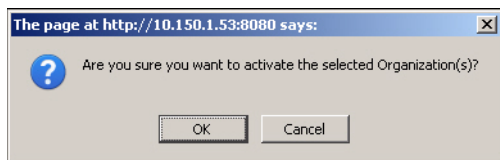
組織の有効化

非アクティブ化した組織を有効にする方法

1. 組織を有効にするために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして、組織の検索ページを表示します（[図 10-8](#) を参照）。
4. 検索する組織の情報を一部または全部入力し、**[Search]** をクリックします。
検索条件に一致した組織のリスト（[図 10-9](#) と同様）が表示されます。
5. 有効にする 1 つ以上の組織を選択します。
6. **[Activate]** をクリックして選択された組織を有効にします。

[図 10-12](#) に示すメッセージ ボックスが表示されます。

図 10-12 組織のアクティブ化：メッセージ



7. **[OK]** ボタンをクリックして確定します。

初期状態の組織のアクティブ化

組織を作り始めても、それをアクティブにしない場合があります。たとえば、組織の作成ページで **[Organization Information]** と **[User Data Location]** を指定する一方で、LDAP リポジトリや組織を管理する管理者の詳細を指定しない場合があります。そのような場合、組織は作成されますがアクティブではないため、**[Initial]** オプションをオンにして検索しなければ、通常は検索では表示されません。

そのような組織は、アクティブにしない限り、システムに初期状態のまま残ります。その後で、その初期状態の組織と同じ詳細を使用して新しい組織を作ろうとしても、システムでは許可されません。これは、その組織が存在するためです。

必要な権限

初期状態の組織のアクティブ化を可能にするには、これを行うための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべての組織をアクティブにすることができます。GA と OA は、自分のスコープ内のすべての組織をアクティブにすることができます。

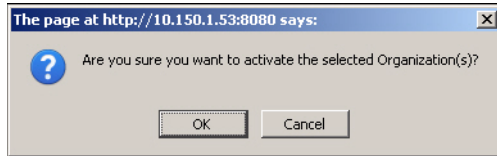
初期状態の組織のアクティブ化

初期状態の組織をアクティブ化する方法

1. 組織を作成するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして、組織の検索ページを表示します (図 10-8 を参照)。
4. 必要な組織の情報を一部または全部入力して、**[Initial]** オプションをオンにします。
5. **[Search]** をクリックして、指定された条件に一致するすべての内容をページ (図 10-9 と同様) に表示します。
6. アクティブにする組織を選択します。

7. **[Activate]** をクリックして選択された組織を有効にします。図 10-13 に示すメッセージ ボックスが表示されます。

図 10-13 組織のアクティブ化：メッセージ



8. **[OK]** ボタンをクリックして確定します。

組織の削除

組織を削除すると、組織に関連付けられた管理者は **Administration Console** を使用してログインすることができません。また、この組織に属するエンド ユーザを認証できません。ただし、組織に関連する情報はそのままシステムに保持されます。削除された組織がスコープ内にある管理者は、組織の詳細を読み取ることができます。

必要な権限

組織の削除を可能にするには、削除を行うための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべての組織を削除できます。GA と OA は、自分のスコープ内のすべての組織を削除できます。

組織の削除

組織を削除する方法

1. 組織を削除するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして、組織の検索ページを表示します (図 10-8 を参照)。
4. 検索する組織の情報を一部または全部入力し、**[Search]** をクリックします。

検索条件に一致した組織のリスト（図 10-14 と同様）が表示されます。

図 10-14 組織の削除

Arcot Administration Console

Welcome **PLAURIE (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Manage Organizations

Search Organization

Click the Organization Name link to view or edit the details of the selected organization. To enable, disable, or delete multiple organizations, select the required organizations and click the applicable button.
Tip: You can also reorder the list of organizations by clicking the Organization column heading.

Organization	Initial	Active	Inactive	Deleted
	☐	☒	☐	☐

[Search](#)

Select Organizations to Modify

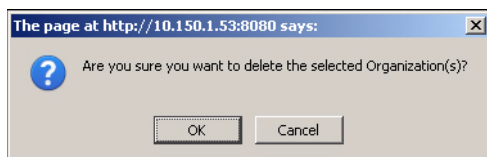
☐	Organization	Display Name	Description	Status
☒	HSBC	HSBC		Active
☒	DEFAULTORG	DEFAULT ORGANIZATION	This is the initial default Organization.	Active
☐	SAFEBANK	Safe Bank		Active

[Activate](#) [Deactivate](#) [Delete](#)

- 削除する 1 つ以上の組織を選択し、[Delete] をクリックします。

図 10-15 に示すメッセージ ボックスが表示されます。

図 10-15 組織の削除：メッセージ



- [OK] ボタンをクリックして確定します。

第 11 章

組織固有の RiskFort の設定の管理



注：組織の設定を管理できるようにするには、ユーザ（**Organization Administrator**）が管理を行うための適切な権限およびスコープを持っていることを確認する必要があります。

Master Administrator は組織に固有の設定を管理できません。GA と OA は、スコープ内のすべての組織の設定を管理できます。

第 7 章の「[グローバルルール設定の管理](#)」で説明したように、Global Administrator (GA) によって設定された「テンプレート化された」ルール設定のコピーを参照または作成できますが、自分の権限の範囲内で組織の特定のビジネス要件を満たすためには、このルール設定を上書きしても良いでしょう。

組織レベルでルール設定を行うと、変更は設定した特定の組織に限定されます。また、設定に対して行われた変更内容は自動的に適用されません。これらの設定変更を適用するには、すべてのサーバインスタンスをリフレッシュする必要があります。

指定された組織にスコープがある場合は、OA として以下のタスクを実行できます。

- [組織固有の RiskFort 設定へのアクセス](#)
- [ルールセットの作成](#)
- [ルールセットの割り当て](#)
- [グローバル設定の使用](#)
- [組織のための RiskFort の設定](#)

組織固有の RiskFort 設定へのアクセス

組織固有の設定はグローバル設定に似ていますが、タスク ページへのナビゲーションパスが異なります。組織固有の設定を実行するためのタスク ページにアクセスするには、以下の手順に従います。

1. 組織を作成するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. **[Manage Organizations]** セクションの下で、**[Search Organization]** リンクをクリックして **[Search Organization]** ページを表示します (図 10-8 を参照)。
4. 検索する組織の完全な情報または部分的な情報を入力し、**[Search]** ボタンをクリックします。

検索条件に一致した組織のリスト (図 10-9 と同様) が表示されます。

5. **[Organization]** 列の下で、必要な組織の `<ORGANIZATION_NAME>` リンクをクリックします。

[Organization Information] ページ (図 11-1 と同様) が表示されます。

図 11-1 **[Organization Information]** ページ

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo and 'Arcot Administration Console' title are visible. The top right shows a welcome message for 'BLAURIE (DEFAULTORG)' with a 'Logout' link and 'Last Login Time'. The main navigation bar includes 'Users and Administrators', 'Organizations' (selected), 'Reports', and 'Case Management'. Below this, the 'Manage Organizations' section is active, showing 'Manage Organizations' and 'Search Organization' links. The left sidebar lists 'Basic Organization Information' with sub-links for 'Organization Details' and 'Basic Authentication Policy'. The main content area shows the 'Organization Information' page for 'DEFAULTORG'. It includes a summary box with 'Organization Name: DEFAULTORG', 'Display Name: DEFAULT ORGANIZATION', and 'Status: Active'. Below this, there are tabs for 'Basic Organization Information' (selected) and 'RiskFort Configuration'. The 'Organization Information' section contains a form with fields for 'Organization Name', 'Display Name', 'Description', 'Administrator Authentication Mechanism', 'Date Created', 'Last Modified', and 'Default Organization'. The 'Next' button is at the bottom of the form.

6. [RiskFort Configuration] タブをアクティブにします。
 タスク ペインに組織固有の設定リンクが表示されます (図 11-2 を参照)。

図 11-2 組織固有の RiskFort の設定

The screenshot displays the Arcot Administration Console interface. At the top, the header shows the Arcot logo and the title 'Arcot Administration Console'. On the right, it says 'Welcome PLAUPIE (DEFAULTORG) | Logout' and 'Last Login Time 07/05/2010 06:13:49 GMT'. Below the header is a navigation bar with tabs: 'Users and Administrators', 'Organizations', 'Reports', and 'Case Management'. The 'Organizations' tab is active, showing a sub-tab 'Manage Organizations'. The left sidebar contains a tree view with categories: 'Manage Organizations' (with a link to 'Search Organization'), 'RiskFort Configuration' (with links to 'Create Ruleset' and 'Assign Ruleset'), 'Rules' (with a list of rule types like 'Trusted IP Aggregator', 'Negative IP Address List', etc.), 'Data Upload' (with links to 'Upload List Data' and 'Upload Mapping Data'), 'Scoring' (with a link to 'Scoring Configuration'), and 'Migrate to Production' (with a link to 'Migrate to Production'). The main content area is titled 'Organization Name: DEFAULTORG' and 'Display Name: DEFAULT ORGANIZATION' with a 'Status: Active'. Below this, there are two sub-tabs: 'Basic Organization Information' and 'RiskFort Configuration'. The 'RiskFort Configuration' sub-tab is active, showing the 'Create Ruleset' form. The form includes a text field for 'Name', a section for '- Advanced Options' with a checkbox for 'Copy from an Existing Ruleset' and a dropdown menu, and a 'Create' button at the bottom right.

7. 必要なルール セットおよびリスク評価ルールを設定して割り当てます。



注： 必要なルールを設定して、必要に応じて割り当てる方法の詳細については、第 7 章の「グローバル ルール設定の管理」を参照してください。ただし、この章で説明している設定は組織レベルですが、第 7 章の「グローバル ルール設定の管理」で説明している操作はグローバルレベルです。設定はどちらも同じですが、このセクションの初めに説明したように、タスク ページにアクセスする方法のみが異なります。

ルール セットの作成

7-80 ページの「ルールセットについて」のセクションで説明しているように、ルールセットとは、Global Administrator (GA) または Organization Administrator (OA) によって設定される一連のルールです。



重要：GA によって作成された場合、ルールセットは個々の組織用にコピーすることだけが可能です。そのため、OA はグローバルルールセットをコピーして新しいルールセットを作成するか、組織レベルで再度ルールセットを作成する必要があります。

ルールセットの作成方法の詳細については、7-81 ページの「ルールセットの作成」を参照してください。



重要：ルールセットを作成したら、それを運用環境に移行してアクティブ化に使用できるようにする必要があります。

ルール セットの割り当て

OA が自分の組織のルールセットを作成し、それを運用環境に移行したら、スコープ内で組織のルールセットをアクティブ化して、そのルールセットを有効にする必要があります。現在の組織に既存のルールセットを割り当てるには、以下の手順に従います。

1. 組織を作成するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. [Organizations] タブをアクティブにします。
3. [Manage Organizations] セクションの下で、[Search Organization] リンクをクリックして [Search Organization] ページを表示します (図 11-3 を参照)。

図 11-3 [Search Organization] ページ

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations
● Search Organization

Search Organization
Enter the (full or partial) Display Name of the organization that you want to search.

Organization Initial Active Inactive Deleted Search

☐ ☒ ☐ ☐

4. 検索する組織の完全な情報または部分的な情報を入力し、[Search] ボタンをクリックします。

検索条件に一致した組織のリスト（図 11-4 と同様）が表示されます。

図 11-4 [Search Organization] ページ：結果

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations
● Search Organization

Search Organization
Click the Organization Name link to view or edit the details of the selected organization. To enable, disable, or delete multiple organizations, select the required organizations and click the applicable button.
Tip: You can also reorder the list of organizations by clicking the Organization column heading.

Organization Initial Active Inactive Deleted Search

☐ ☒ ☐ ☐

Select Organizations to Modify

☐	Organization	Display Name	Description	Status
☐	HSBC	HSBC		Active
☐	DEFAULTORG	DEFAULT ORGANIZATION	This is the initial default Organization.	Active
☐	SAFEBANK	Safe Bank		Active

5. [Organization] 列の下で、必要な組織の <ORGANIZATION_NAME> リンクをクリックします。

[Organization Information] ページ (図 11-1 と同様) が表示されます。

6. [RiskFort Configuration] タブをアクティブにします。
7. [Ruleset] セクションの下で、[Assign Ruleset] リンクをクリックします。
[Assign Ruleset] ページ (図 11-5) が表示されます。

図 11-5 [Assign Ruleset] ページ

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo and 'Arcot Administration Console'. On the right, it says 'Welcome PL AUPRIE (DEFAULTORG) | Logout' and 'Last Login Time 07/05/2010 06:13:49 GMT'. Below the header, there are tabs: 'Users and Administrators', 'Organizations', 'Reports', and 'Case Management'. The 'Organizations' tab is selected. On the left, there's a sidebar with 'Manage Organizations' and 'RiskFort Configuration'. Under 'Manage Organizations', there's a search bar and a list of links: 'Create Ruleset', 'Assign Ruleset' (highlighted with a green dot), and 'Rules'. Under 'RiskFort Configuration', there's a list of links: 'Trusted IP Aggregator', 'Negative IP Address List', 'Negative IP Types', 'Negative Country List', 'User Velocity', 'Device Velocity', 'Zone Hopping', 'Add-On Rules', 'Callout Configuration', 'Miscellaneous Rule Configurations', 'Data Upload', 'Upload List Data', 'Upload Mapping Data', 'Scoring', 'Scoring Configuration', 'Migrate to Production', and 'Migrate to Production' (highlighted with a green dot). The main content area shows 'Organization Name: DEFAULTORG', 'Display Name: DEFAULT ORGANIZATION', and 'Status: Active'. Below this, there's a section for 'Assign Ruleset' with a dropdown menu for 'Select Ruleset to assign:' and a 'Save' button. The dropdown menu currently shows '--Select--'.

8. [Select Ruleset to Assign] リストから、アクティブにするルール セットを選択します。
9. [Save] をクリックして、現在の組織で指定されたルール セットをアクティブにします。

グローバル設定の使用

スコープ内の各組織のルール設定を個別に変更することもできますが、おそらく、組織の大部分で同じ設定を何度も繰り返して使用する可能性があります。また、設定された組織が数多くある場合、個々の組織にルール設定を行うのは煩わしいタスクになる場合があります。このような場合、同じ設定を毎回指定する必要がなくなるように、GA が設定したグローバル設定をカスタマイズすると良いでしょう。

組織をスコープとする GA がグローバルレベルでルール設定を行うと、その後はすべての組織がこれらの設定を継承します。これらの設定を参照するかコピーを作成することで、これらの設定を使用できます。

各ルールの設定ページに表示される **[Advanced Options]** セクションを使用します。ルール設定ページを表示すると、ページに **[+ Advanced Configuration]** セクションが表示されます。このセクションは折りたたまれているため、+ 記号をクリックしてセクションを展開し、使用可能なオプションを表示します（[図 11-6](#) を参照）。

図 11-6 [Advanced Options] セクション（すべてのルール設定ページで使用可能）

[図 11-6](#) に示すように、GA によって設定されたグローバル設定を使用する場合に使用可能なオプションは以下の 2 つです。これらのオプションのいずれか一方のみを使用できます。

- **[Use Own]**：このオプションを選択すると、独自の設定値を指定できます。

RiskFort では、既存のルール セットから設定またはデータをコピーすることにより、既存のルール セットを変更することもできます。このオプションを使用するには、**[Use Own]** を選択し、**[Copy from an Existing Ruleset]** オプションを選択し、設定をコピーするルール セットの名前を **[Ruleset Name]** リストから選択します。



注： このページで行った変更は、コピー元のルール セットには影響しません。

- **[Refer an Existing Ruleset]** : このオプションを選択した場合、RiskFort は指定されたルール セットをそのまま使用します。このオプションを選択すると、変更できないことに注意してください。

このオプションを使用するには、**[Refer an Existing Ruleset]** を選択し、**[Ruleset Name]** リストから参照したい設定のルールセットの名前を選択します。

組織のための RiskFort の設定

ルール セットの作成と割り当てのほかに、Organization Administrator (OA) は、[第 7 章の「グローバル ルール設定の管理」](#)で説明したほとんどのタスクを実行できます。これには、以下のようなものがあります。

- スコープ内の組織の既定ルールの設定。
詳細な手順については、[第 7 章の「グローバル ルール設定の管理」](#)を参照してください。
- スコープ内の組織のスコアの設定、および運用環境への設定の移行。
詳細な手順については、[第 8 章の「スコアリングの設定」](#)を参照してください。
- スコープ内の組織のアドオン ルールの展開。
詳細な手順については、[第 12 章の「アドオン ルールの操作」](#)を参照してください。
- スコープ内の組織のコールアウトの設定。
詳細な手順については、[第 9 章の「コールアウトの設定」](#)を参照してください。

第 12 章 アドオン ルールの操作



重要：この章で説明するすべての設定およびタスクは、主に **Organization Administrator** が実行する必要があります。組織固有の設定を行うためにタスク ページにアクセスする場合の詳細については、[第 11 章の「組織固有の RiskFort 設定へのアクセス」](#) を参照してください。

必要に応じて、**Global Administrator** もこれらの手順を実行できます。ただし、Global Administrator は **[Organizations]** タブを使用して **組織レベル** で実行する必要があります。

RiskFort のデフォルトの **評価ルール** は汎用的であり、一般的なトランザクションのリスクを評価するために設定されます。アプリケーションがこれらの汎用的なルールに基づいてリスクを評価する必要がある場合、正当と不正の評価を誤る可能性が高くなります。デフォルト ルールのスコアや優先度を調整したり、ホワイト リストやブラック リストを作成して結果を改善することもできますが、すべてのケースで十分ではない可能性があります。このような場合、RiskFort がデフォルトで提供しているルールとは大きく異なるカスタム ルール、または業界固有のルールが必要となります。これらの終端ルールを、アドオン ルールと呼びます。



重要：アドオン ルールは、既定のリスク評価ルールの実行が完了した **後** のみ実行されます。ただし、スコアリングの優先度を既定のルールよりも高くすることができます。

この章では、アドオン ルールの基本について説明し、ビジネス固有の要件を満たすためにアドオン ルールを設定するプロセスについて説明します。

- [アドオン ルールについて](#)
- [アドオン ルールの作成に使用するデータ エレメントと演算子](#)
- [アドオン ルールの例](#)
- [アドオン ルールの操作](#)
- [アドオン ルールのリスト データのアップロード](#)



注：設定関連のアクティビティを実行する管理者には、これらの操作を実行する権限が必要です。各レベルの管理者が使用可能な権限の詳細については、[第 1 章の「管理者権限のサマリ」](#)を参照してください。

RiskFort のデフォルトの（既定の）設定を更新しても、変更はすぐにアクティブ（エンド ユーザが使用可能な状態）にはなりません。必ず、サイドバーメニューにある **[Migrate to Production]** リンクを使用して、**提示された設定変更**をすべて運用環境のデータベースに「移動」してください。RiskFort によって使用される、デフォルトの設定データ、提示された設定データ、アクティブな設定データの概念を理解するには、[「運用環境への移行」](#)を参照してください。

アドオン ルールについて

事前定義済みのデフォルト ルールとは異なり、アドオン ルールは RiskFort のインストール時に自動的に展開されません。Master Administrator（MA）は、まずアドオン ルール用の対応するルール タイプを追加する必要があります（[第 6 章の「アドオン ルールの準備：ルール タイプの操作」](#)で説明）。次に（Global Administrator または Organization Administrator として）アドオン ルールの設定ページ（[図 12-1](#)）を使用して、ルール固有の設定を指定する必要があります。

図 12-1 アドオン ルールの設定ページ

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/05/2010 06:53:43 GMT

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations

- Search Organization

RiskFort Configuration

Ruleset

- Create Ruleset
- Assign Ruleset

Rules

- Trusted IP/Aggregator
- Negative IP Address List
- Negative IP Types
- Negative Country List
- User Velocity
- Device Velocity
- Zone Hopping
- Add-On Rules
- Callout Configuration
- Miscellaneous Rule Configurations

Data Upload

- Upload List Data
- Upload Mapping Data

Scoring

- Scoring Configuration

Migrate to Production

- Migrate to Production

Organization Name: DEFAULTORG Display Name: DEFAULT ORGANIZATION Status: Active

Basic Organization Information RiskFort Configuration

Add-On Rules Configuration

Add a new Add-On rule, update the settings for an existing Add-On rule, or remove a deployed Add-On rule. If you are adding a new rule, then ensure that you enable the rule for execution and scoring on the Scoring Configuration page.

Update Existing Ruleset

DEFAULTORG - DEFAULT

☒ Add ☐ Update

Rule Mnemonic :

Rule Display Name :

Description :

Rule Type :

Save Delete

このページ（図 12-1）では、既定のルール（頻度ルールなど）またはアップロードされたリストを、トランザクションとシステムのエレメント、数学演算子、およびブール関数と組み合わせて、不正なトランザクションを識別することもできます。



注：アドオン ルールを展開したら、それを有効にするために、スコアリングの設定ページ（第 8 章の「スコアリングの設定」の図 8-1 を参照）を使用してそのルールを有効化する必要があります。

アドオン ルールの作成に使用するデータ エLEMENT と演算子

アドオン ルールを作成するには、以下のELEMENTが必要です。

- データ ELEMENT
- 論理演算子
- アドオン ルールによって使用される追加入力ELEMENT

データ ELEMENT

アドオン ルールを展開するには、以下のものがが必要です。

- **ルールの短縮名**：ログの記録と API で使用するルールの短縮名。短縮名の最大文字数は 15 文字です。スペースは使用できません。
- **ルールの表示名**：スコアリングの設定画面に表示される表示名。
- **ルール タイプ**：ルールのタイプ。既存のタイプを使用するか、MA が定義できます。



注：デフォルトのルール タイプの詳細については、[第 6 章の「システム定義のルール タイプ」](#)を参照してください。

選択したルール タイプに応じて、以下の追加のデータ ELEMENT が使用可能です。これらのELEMENTは以下のとおりです。

- **通貨および金額**：AMOUNT_CHECK ルール タイプによって使用されます。
- **期間**：CARDHOLDER_MERCHANT_AMOUNT、IPADDRESS_MERCHANT_AMOUNT、IP_VELOCITY、および TRANSACTION_TYPE_CHECK ルール タイプによって使用されます。
- **頻度**：CARDHOLDER_MERCHANT_AMOUNT、IPADDRESS_MERCHANT_AMOUNT、および IP_VELOCITY ルール タイプによって使用されます。
- **ルール**：すべての組み込みのルールと、これまでに定義されたすべてのアドオン ルール。COMBINATION_RULE タイプによって使用されます。
- **タグ名**：パラメータ定義。DERIVED_LIST_LOOKUP、NUMERIC_COMPARISON、SIMPLE_LIST_LOOKUP によって使用されます。

- **リスト キャッシュの有効化**：有効でない場合は **0**、有効の場合は **1**。
DERIVED_LIST_LOOKUP と SIMPLE_LIST_LOOKUP ルール タイプによって使用されます。
- **マッピング キャッシュの有効化**：有効でない場合は **0**、有効の場合は **1**。
DERIVED_LIST_LOOKUP ルール タイプによって使用されます。
- **マッピング データ セット**：アドオン ルールによって使用されるデータ セット（またはマッピング リスト）。DERIVED_LIST_LOOKUP、MERCHAND_CATEGORY_LOOKUP、および MERCHAND_REGION_LOOKUP ルール タイプによって使用されます。
- **処理の無効化、許可の上限、および追加認証の上限**：GDP（または RiskFort モデル）ルール タイプによって使用されます。
- **しきい値**：NUMERIC_COMPARISON ルール タイプによって使用されます。
- **前のトランザクション タイプ**：Arcot TransFort によってサポートされているすべてのトランザクション。TRANSACTION_TYPE_CHECK ルール タイプによって使用されます。

論理演算子

現在、ルール タイプに基づいて、以下のカテゴリの論理演算子がサポートされています。

- **式**：AND、OR、NOT、(、) 演算子を含みます。COMBINATION_RULE タイプによって使用されます。
- **一致タイプ**：使用可能な演算子には EXACT と PARTIAL が含まれます。
DERIVED_LIST_LOOKUP と SIMPLE_LIST_LOOKUP ルール タイプによって使用されます。
- **検索タイプ**：使用可能な演算子には IN_LIST と NOT_IN_LIST が含まれます。
DERIVED_LIST_LOOKUP と SIMPLE_LIST_LOOKUP ルール タイプによって使用されます。
- **演算子**：使用可能な演算子には、EQ (=)、NEQ (!=)、GTE (>=)、LTE (<=)、GT (>)、および LT (<) が含まれます。NUMERIC_COMPARISON ルール タイプによって使用されます。

アドオン ルールによって使用される追加入力エレメント

通常、アドオン ルールは追加入力を使用します。これらの追加入力は追加の名前と値のカスタム パラメータです。各トランザクションからのリアルタイムの入力をキャプチャし、リスク評価を正常に行うためのアドオン ルールによって処理されます。

追加入力に関連する重要な注意事項

- RiskFort では、ベース エレメントとして IP アドレス、デバイス ID、MFP、`username`、および `transactiontype` を使用します。これら既定のエレメント以外のエレメントは、すべて追加入力と見なされます。
- 追加入力はプログラムで設定するエレメントであり、Administration Console を使用して設定することはできません。
- アドオン ルールでは追加入力をまったく使用しない場合があります。

アドオン ルールの例

以下のサブセクションでは、デフォルトの RiskFort ルールまたはアドオン ルールを組み合わせ、複合的な要因と条件を使用してカスタムの組み合わせルールを定義する方法について説明します。



注：以下の例にあるルール（`SAFE_COUNTRIES` など）は、アップロードされたリスト（`*_LIST_LOOKUP`）を表すものです。

高額チェック

トランザクション金額が 500 ドルを超えるかどうかをチェックする必要がある `AMOUNT_CHECK` ルールの以下の詳細について検討します。

- **ルールの短縮名**：HIGHAMTCHK
- **ルールの表示名**：High Amount Check
- **説明**：このルールは 500 ドルを超える高額の特ランザクション金額をチェックします。
- **ルール タイプ**：AMOUNT_CHECK
- **金額**：500

この例のルールは、以下の内容を実行します。

1. `Amount` という名前のタグによって `evaluateRisk()` API 呼び出しで渡される `AdditionalInput` の文字列 (`Amount=750`) を解析し、このタグの変数 `ActualAmount` の値を抽出します。



注： `AdditionalInput` エレメントの解析に関する詳細は、Javadoc を参照してください。

2. ルールのパラメータ値 (`500`) を抽出し、それを `ParameterAmount` という変数に保存します。
3. この場合、`ActualAmount` (`750`) が `ParameterAmount` (`500`) より大きいため、`Matched` が返されます。

予期しない場所からの高速のユーザ頻度

`SAFE_COUNTRIES` が `SIMPLE_LIST_RULE` (`US`、`CA`、`UK`、`DE` などのエレメントを含む) を参照している場合を考えます。この場合、以下のようにカスタムの `COMBINATION_RULE` を定義して、通常以外の場所からのユーザ頻度が高速のトランザクションを見つけることができます。

```
USERVELOCITY AND T SAFE_COUNTRIES
```

予期しない場所からの高速のデバイス頻度

前の例と同様、以下のようにカスタムの `COMBINATION_RULE` を定義して、通常以外の場所からのデバイス頻度が高速のトランザクションを見つけることができます。

```
DEVICEVELOCITY AND NOT SAFE_COUNTRIES
```

予期しない場所からの電子送金

HIGHAMTCHK と呼ばれるアドオン ルールを作成した場合を考えます（「**高額チェック**」で前述）。また、**SAFE_COUNTRIES** ルールで送金元が安全であると考えられる国のリストを使用すると、以下のようなカスタムの **COMBINATION_RULE** を定義して、通常ではない場所からの小額または高額の電子送金を追跡できます。

(HIGHAMTCHK OR Amount < 20) AND NOT SAFE_COUNTRIES

アドオン ルールの操作



重要：アドオン ルールを展開、編集、または削除する前に、Master Administrator (MA) によって対応するルール タイプが追加されていることを確認する必要があります（[6-69 ページの「カスタム ルール タイプの操作」](#)を参照）。その後、アドオン ルールの設定ページ（[図 12-1](#)）を使用して、ルール固有の設定に進むことができます。

アドオン ルールの設定ページは以下の場合に使用します。

- [アドオン ルールの展開](#)
- [展開したアドオン ルールの属性の編集](#)
- [展開したアドオン ルールの削除](#)

アドオン ルールの展開

アドオン ルールを展開する方法

1. OA または GA としてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. このページの **[Search]** ボタンをクリックして、組織のリストを表示します。
4. **[Select Organizations to Modify]** の下で、アドオン ルールを適用する組織名のリンクをクリックします。
5. **[RiskFort Configuration]** タブをクリックします。
6. サイド バー メニューの **[Rules]** セクションの下で、**[Add-On Rules]** リンクをクリックします。

図 12-1 に示すように、アドオン ルールの設定ページが表示されます。

7. **[Update Existing Ruleset]** リストから、この設定を適用できるルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

8. **[Add]** オプションをオンにして、新しいアドオン ルールを追加します。
9. **[Rule Mnemonic]** フィールドにルールの短縮名を入力します。



注： 短縮名の最大文字数は 15 文字です。スペースは使用できません。

10. **[Rule Display Name]** フィールドに新しいルールの名前を指定します。
この名前は、スコアリングの設定画面および対応するアドオン ルール レポートで使用されます。
11. 後で参照できるように、**[Description]** フィールドにアドオン ルールに関連する便利な情報を入力します。
12. **[Rule Type]** リストから既存のルール タイプのいずれかを選択するか、Master Administrator によって定義されたカスタム ルール タイプを選択します。



注： 詳細については、6-69 ページの「カスタム ルール タイプの操作」を参照してください。

MA が作成したルール タイプによっては、追加フィールドが表示される場合があります。

13. 表示された新しいフィールドに必要な情報を指定します。
14. **[Save]** をクリックしてルールを展開します。
15. 展開したアドオン ルールを有効にします。この手順については、「[スコアリングの設定](#)」を参照してください。

ここで展開したアドオン ルールはまだアクティブではなく、エンド ユーザに利用可能ではありません。

16. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

この手順については、「[運用環境への移行](#)」を参照してください。

展開したアドオン ルールの属性の編集

展開したアドオン ルールの属性を編集するには、以下の手順に従います。

1. OA または GA としてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. このページの **[Search]** ボタンをクリックして、組織のリストを表示します。
4. **[Select Organizations to Modify]** の下で、アドオン ルールを適用する組織名のリンクをクリックします。
5. **[RiskFort Configuration]** タブをクリックします。
6. サイド バー メニューの **[Rules]** セクションの下で、**[Add-On Rules]** リンクをクリックします。

図 12-1 に示すように、アドオン ルールの設定ページが表示されます。

7. **[Update Existing Ruleset]** リストから、この設定を適用できるルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

8. **[Update]** オプションを選択して、展開したアドオン ルールの設定を編集します。
9. **[Add-On Rule]** リストから更新するルールを選択します。
そのルールに定義された追加のフィールドが表示されます。

10. 必要な変更を行います。

11. **[Save]** をクリックしてルールを更新します。

12. 展開したアドオン ルールを有効にします。この手順については、[「スコアリングの設定」](#)を参照してください。

ここで展開したアドオン ルールはまだアクティブではなく、エンド ユーザに利用可能ではありません。

13. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

この手順については、[「運用環境への移行」](#)を参照してください。

展開したアドオン ルールの削除

展開したアドオン ルールを削除するには、以下の手順に従います。

1. OA または GA としてログインしていることを確認します。

2. **[Organizations]** タブをアクティブにします。
3. このページの **[Search]** ボタンをクリックして、組織のリストを表示します。
4. **[Select Organizations to Modify]** の下で、アドオン ルールを適用する組織名のリンクをクリックします。
5. **[RiskFort Configuration]** タブをクリックします。
6. サイド バー メニューの **[Rules]** セクションの下で、**[Add-On Rules]** リンクをクリックします。

図 12-1 に示すように、アドオン ルールの設定ページが表示されます。

7. **[Update Existing Ruleset]** リストから、この設定を適用できるルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

8. **[Update]** オプションを選択して、展開したアドオン ルールを表示します。
9. **[Add-On Rule]** リストから削除するルールを選択します。
10. **[Delete]** をクリックしてルールを削除します。

変更はまだアクティブではなく、エンド ユーザは使用できません。

11. 展開したアドオン ルールを有効にします。この手順については、「[スコアリングの設定](#)」を参照してください。

ここで展開したアドオン ルールはまだアクティブではなく、エンド ユーザに利用可能ではありません。

12. 変更をアクティブにするには、それらを運用環境に移行する必要があります。この手順については、「[運用環境への移行](#)」を参照してください。

アドオン ルールのリスト データのアップロード



重要：このセクションで言及したいいずれかのタスクを実行する場合、最初に、リストに対応するアドオン ルールが展開されていることを確認する必要があります。その詳細な手順については、「[アドオン ルールの展開](#)」を参照してください。

展開したアドオン ルール（[12-188 ページの「アドオン ルールの展開」](#)）が単純リストまたは導出リスト形式の追加データを必要とする場合は、このセクションのタスクを実行する必要があります。リスト タイプに応じて、次のタスクが含まれます。

- [（単純な）リスト データのアップロード](#)
- [マッピング（導出リスト）データのアップロード](#)

（単純な）リスト データのアップロード

SIMPLE_LIST_LOOKUP ルール タイプを使用するアドオン ルールのデータをアップロードする方法

1. OA または GA としてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. このページの **[Search]** ボタンをクリックして、組織のリストを表示します。
4. **[Select Organizations to Modify]** セクションの下で、アドオン ルールを適用する組織名のリンクをクリックします。
5. **[RiskFort Configuration]** タブをクリックします。
6. サイド バー メニューの **[Data Upload]** セクションの下で、**[Upload List Data]** リンクをクリックします。

ルールのリスト データのアップロード ページが表示されます。

7. **[Update Existing Ruleset]** リストから、この設定を適用できるルール セットを選択します。

指定されたルール セットの設定情報が表示されます。

8. **[Select Dataset]** リストから、対応するアドオン ルールの作成中に指定した **<Rule Mnemonic>** を選択します。

ルールのリスト データのアップロード ページ（[図 12-2](#)）が更新されて表示されます。

9. **[Upload File Or Enter Data]** セクションで、データを書き込む際の適切なモードを選択します。

- **[Append]** : このオプションは、アップロードするデータをリストまたはデータセットに追加します。



注 : リストが存在しない場合は、このオプションを選択する必要があります。

- **[Replace]** : このオプションは、指定されたリストまたはデータセットの既存のデータを上書きします。

10. 以下のいずれかを実行します。

- **[Brows]** をクリックし、改行文字によって区切られたエントリのリストを含むデータファイルに移動します。

または

- データファイルが存在しない場合は、**[Enter Data]** フィールドにエントリを入力します。



重要 : エントリが改行文字 (ENTER) で区切られていることを確認します。

11. **[Upload]** をクリックしてタスクを完了します。

図 12-2 ルールのリスト データのアップロード ページ

Arcot Administration Console

Welcome [RLAUIPIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/05/2010 09:28:14 GMT

Users and Administrators | **Organizations** | **Reports** | **Case Management**

Manage Organizations

Manage Organizations

- [Search Organization](#)

RiskFort Configuration

Ruleset

- [Create Ruleset](#)
- [Assign Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address List](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Organization Name: DEFAULTORG **Display Name:** DEFAULT ORGANIZATION **Status:** Active

Basic Organization Information | **RiskFort Configuration**

Upload Rules List Data

Select the dataset and upload a file or enter data.

Update Existing Ruleset
DEFAULTORG - DEFAULT

Select Dataset: SAFE_COUNTRIES_CHECK

Upload File Or Enter Data

☒ Append ☐ Replace

Upload Data File: [Browse...](#)

--OR--

Enter Data:

[Upload](#)

マッピング（導出リスト）データのアップロード

DERIVED_LIST_LOOKUP、MERCHANT_CATEGORY_LOOKUP、または MERCHANT_REGION_LOOKUP ルール タイプを使用するアドオン ルールのデータをアップロードする方法

1. OA または GA としてログインしていることを確認します。
2. **[Organizations]** タブをアクティブにします。
3. このページの **[Search]** ボタンをクリックして、組織のリストを表示します。
4. **[Select Organizations to Modify]** セクションの下で、アドオン ルールを適用する組織名のリンクをクリックします。
5. **[RiskFort Configuration]** タブをクリックします。
6. サイド バー メニューの **[Data Upload]** セクションの下で、**[Upload Mapping Data]** リンクをクリックします。
ルールのマッピング データのアップロード ページが表示されます。
7. **[Update Existing Ruleset]** リストから、この設定を適用できるルール セットを選択します。
指定されたルール セットの設定情報が表示されます。
8. **[Select Dataset]** リストから、対応するアドオン ルールの作成中に指定した **<Mapping Data Set>** を選択します。
ルールのリスト データのアップロード ページ (図 12-2) が更新されて表示されます。

図 12-3 ルールのマッピング データのアップロード ページ

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo and 'Arcot Administration Console' title are on the left, while the user 'PLAURIE (DEFAULTORG)' and login details are on the right. The main navigation bar includes 'Users and Administrators', 'Organizations' (selected), 'Reports', and 'Case Management'. Below this, the 'Manage Organizations' section is active, showing details for 'DEFAULTORG' with a status of 'Active'. The left sidebar lists various configuration options under 'RiskFort Configuration', including 'Ruleset' and 'Rules'. The main content area is titled 'Upload Rules Mapping Data' and contains two tabs: 'Basic Organization Information' and 'RiskFort Configuration' (selected). The page prompts the user to 'Select the dataset and upload a file or enter data.' It features a dropdown for 'Update Existing Ruleset' set to 'DEFAULTORG - DEFAULT' and another dropdown for 'Select Dataset' set to 'MERCHANT_CATEGORY_MAPPING'. At the bottom, there is a section for 'Upload File Or Enter Classification Data' with radio buttons for 'Append' (selected) and 'Replace', a file upload field with a 'Browse...' button, and a text area for 'Enter Data:'. An 'Upload' button is located at the very bottom.

9. **[Upload File Or Enter Classification Data]** セクションで、データを書き込む際の適切なモードを選択します。

- **[Append]** : このオプションは、アップロードするデータをリストまたはデータセットに追加します。



注 : リストが存在しない場合は、このオプションを選択する必要があります。

- **[Replace]** : このオプションは、指定されたリストまたはデータセットの既存のデータを上書きします。

10. 以下のいずれかを実行します。

- **[Browse]** をクリックし、改行文字によって区切られたエントリのリストを含むデータ ファイルに移動します。

または

- データ ファイルが存在しない場合は、**[Enter Data]** フィールドにエントリを入力します。



重要 : エントリが改行文字 (ENTER) で区切られていることを確認します。

11. **[Upload]** をクリックしてタスクを完了します。

第 13 章 管理者の管理

管理者のタイプ、および管理者のロールと責任は、展開の規模に依存します。小規模な単独組織への展開では、Master Administrator (MA) 1 人だけと、エンド ユーザのために組織を管理する Global Administrator (GA) を配置する場合があります。一方、大規模で複数組織の展開では、展開の複雑さとエンド ユーザの数に基づいて複数の GA を設定する必要がある場合があります。GA は、組織とユーザの管理作業をさらに複数の Organization Administrator (OA) および User Administrator (UA) に委任できます。

サポートされている管理ロールの詳細については、[1-4 ページの「サポートされているロール」](#)を参照してください。[1-11 ページの表 1-2](#)に、これらの管理者がそれぞれ実行できるタスクの簡単なサマリを示します。この章では、以下の管理者の管理操作について説明します。

- [管理者の作成](#)
- [管理者アカウントのプロファイル情報の変更](#)
- [管理者の検索](#)
- [管理者アカウント情報の更新](#)
- [管理者アカウントの無効化](#)
- [管理者アカウントの有効化](#)
- [管理者アカウントの削除](#)



注： Master Administrator は、この章で説明するすべての操作に加えて、[1-14 ページの「カスタム ロール」](#)を作成する権限を持っています。これは WebFort でサポートされている既存のデフォルト ロールから派生するロールです。

管理者の作成

管理者の作成に必要な権限

管理者は、管理階層の同じまたは低いレベルに属し、かつ同じまたは小さいスコープを持っている他の管理者を作成できます。以下に例を示します。

- Master Administrator は、他のすべてのタイプの管理者を作成できます。
- Global Administrator (GA) は、自分のスコープ内に以下を作成できます。
 - 他の GA
 - Organization Administrator (OA)
 - User Administrator (UA)
- OA は自分のスコープ内に以下を作成できます。
 - 他の OA
 - UA
- UA は自分のスコープ内に他の UA を作成できます。

基本クレデンシャル（ユーザ名 / パスワード）を使用して管理者アカウントを作成する方法

1. 管理ユーザの作成に必要な権限とスコープでログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションで、**[Create Administrator]** リンクをクリックして、**[Create Administrator]** ページ ([図 13-1](#)) を表示します。

図 13-1 Create Administrator : 1 ページ

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo and the text 'Arcot Administration Console'. On the right, it says 'Welcome BLAURIE (DEFAULTORG) | Logout' and 'Last Login Time 07/12/2010 11:16:24 GMT'. Below the header, there are tabs for 'Users and Administrators', 'Organizations', 'Reports', and 'Case Management'. The 'Users and Administrators' tab is active, showing a sub-tab 'Manage Users and Administrators'. On the left sidebar, under 'Manage Users and Administrators', there are links for 'Create Administrator' (highlighted with a green dot), 'Search Users and Administrators', and 'Administer Users and Administrators'. The main content area is titled 'Create Administrator' and contains a form for entering administrator details. The form fields are: 'User Name' (text input), 'Organization' (dropdown menu showing 'DEFAULT ORGANIZATION'), 'First Name' (text input), 'Middle Name' (text input), 'Last Name' (text input), 'Email Address' (text input), and 'Phone Number' (text input). A 'Next' button is located at the bottom of the form.

4. [Administrator Details] セクションで、管理者の詳細を入力します。表 13-1 で、このページ上のフィールドについて説明します。

表 13-1. 管理者を作成するための入力

入力	説明
[User Name]	管理者の一意のユーザ名。
[Organization]	管理者が属する組織の表示名。 注：これはこの管理者が管理する組織ではありません。
[First Name]	管理者の名。
[Middle Name] (オプション)	管理者のミドル ネーム (ある場合)。
[Last Name]	管理者の姓。

表 13-1. 管理者を作成するための入力

入力	説明
[Email Address]	管理者の電子メール アドレス。
[Phone Number] (オプション)	管理者に連絡する際の電話番号。

5. [Next] ボタンをクリックして続行します。
 [Create Administrator] ページの次のページ (図 13-2) が表示されます。

図 13-2 Create Administrator : 2 ページ

Arcot Administration Console

Welcome [BLAURIE \(DEFAULT.ORG\)](#) | [Logout](#)
 Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- Create Administrator
- [Search Users and Administrators](#)

User Name: DCHEN Organization: DEFAULT ORGANIZATION Status: Initial

Create Administrator

Set the Administrator's Role, Scope, and Password credential.
Note: To reset the credential, the target administrator will need to go through the reset flow.

Role

Role:

Set Password

Password:

Confirm Password:

Manages

All Organizations: ☐

Available Organizations: DEFAULT ORGANIZA, HSBC, Safe Bank

Selected Organizations:

Back Create

6. このページで以下の作業を行います。
 - **[Role]** ドロップダウン リストから新しい管理者のロールを指定します。
 - **[Manages]** セクションで、管理者のスコープとなる組織を選択します。
 - その管理者にシステムの現在の組織と今後作成される組織をすべて管理させる場合は、**[All Organizations]** オプションをオンにします。または
 - **[Available Organizations]** リストから必要な組織を選択し、**[>]** ボタンをクリックしてこれらの組織を **[Selected Organizations]** に追加します。

[Available Organizations] リストには、この新規アカウントを作成する管理者のスコープ内で選択可能なすべての組織が表示されます。**[Selected Organizations]** に、管理者が管理するために選択した組織のリストが表示されます。
7. **[Create]** ボタンをクリックすると、変更が保存され、アカウントが作成されてアクティブになります。
8. 管理者に新しいパスワードを伝えます。

管理者アカウントのプロファイル情報の変更

アカウントのプロファイル情報には以下の項目が含まれます。

- 個人情報（姓、名、ミドル ネーム、および連絡先情報）
- アカウントのパスワード
- 優先される組織（今後実行するすべての管理者関連タスクの **[Organization]** フィールドで、デフォルトで選択される組織）。



注：管理者はいつでも各自のアカウントのプロファイル情報を変更できます。他の管理者アカウントの情報を変更する場合は、[「管理者アカウント情報の更新」](#)を参照してください。

基本ユーザ名 - パスワード クレデンシャルを使って作成された自分のアカウントの管理者プロファイル情報を変更する方法

1. 自分のアカウントにログインしていることを確認します。

2. ヘッダ フレームで <ADMINISTRATORNAME> リンクをクリックし、[My Profile] ページ (図 13-3) を表示します。
3. このページには以下の 3 つのセクションがあります。
 - 個人情報
このセクションでは、姓、名、ミドル ネーム、電子メール ID および電話番号を変更できます。
 - パスワードの変更
このセクションでは、新しいパスワードを設定できます。
 - Administrator Preferences
このセクションでは、管理者が対応するデフォルトの組織を設定できます。

図 13-3 [My Profile] ページ

Arcot Administration Console

Welcome **RLAURIE** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

User Name: RLAURIE Organization: DEFAULTORG Role: Organization Adminis...

My Profile
Update your personal details and preferences.

Personal Information

First Name: *
Middle Name:
Last Name: *
Email: *
Phone:

Change Password

Current Password:
New Password:
Confirm Password:

Administrator Preferences

Enable Preferred Organization: ☐
Preferred Organization:
Time Zone:

4. このページで、以下のように各セクション内の必要な設定を編集します。
 - a. 必要に応じて、**[Personal Information]** セクション内のフィールドを編集します。

- b. 現在のパスワードを変更する場合は、[**Change Password**] セクションで [**Current Password**] を入力し、[**New Password**] フィールドと [**Confirm Password**] フィールドで新しいパスワードを指定します。
 - c. [**Administrator Preferences**] セクションで、以下の設定を行います。
 - [**Enable Preferred Organization**] オプションをオンにし、[**Preferred Organization**] リストから組織を選択します。この組織は、今後実行するすべての管理者関連タスクで選択されます。
 - [**Time Zone**] リストから必要なオプションを選択します。このタイム スタンプは、今後コンソールヘッダの [**Last Login**] 情報、すべてのレポート、およびケース管理アクティビティ（使用可能な場合）に反映されます。
5. [**Save**] ボタンをクリックすると、プロフィール情報が変更されます。

管理者の検索



注：管理者アカウントを更新、アクティブ化、または非アクティブ化する必要がない限り、検索する権限は必要ありません。ただし、管理者が属する組織がスコープに含まれている必要があります。たとえば、対象となる組織が UA の権限の範囲内にあれば、UA はその組織の管理者を検索できます。

条件を指定して管理者を検索する方法

1. 必要な権限とスコープでログインしていることを確認します。
2. [**Users and Administrators**] タブをアクティブにします。
3. [**Manage Users and Administrators**] セクションの下で、[**Search Users and Administrators**] リンクをクリックして、[**Search Users and Administrators**] ページを表示します（図 13-4 を参照）。

図 13-4 [Search Users and Administrators] ページ

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Arcot Administration Console

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)**

Search Users and Administrators

Specify the search criteria to display the list of users. Use the [Advanced Search](#) link to additionally search on Status or Role.
Tip: You need not enter the complete values in the fields. Also, you can specify the organization's Display Name to search for the user in an organization.

First Name	Last Name	User Name	Organization	Email	
					Search Advanced Search

- 管理者のリストを表示するための検索条件を指定します。以下の操作を行うことができます。
 - このページの各フィールドに管理者の情報の一部または全部を指定して管理者を検索する。
 - 組織の表示名を指定して管理者を検索する。
 - 条件を指定せずに **[Search]** をクリックするだけで管理者を検索する。
 - [Advanced Search]** リンクをクリックして **[Advanced Search]** ページ (図 13-5) を表示し、**[Status]** または **[Role]** を指定して必要な管理者を検索する。

図 13-5 [Advanced Search] ページ

Arcot Administration Console

Welcome **BLAURIE (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Advanced Search

Click the User Search Criteria tab to specify the type of credential you want to base your search on.

User Search Criteria

User Details

First Name:

Middle Name:

Last Name:

User Name:

Organization:

Email Address:

User Status

Include Active Users: ☒

Include Inactive Users: ☐

Include Deleted Users: ☐

Available Roles

Role:
Customer Service Rep(CSR)
Fraud Analyst
Global Administrator

Search

5. 管理者の必要な詳細を指定し、**[Search]** ボタンをクリックします。
検索条件に一致した管理者のリストが表示されます。

管理者アカウント情報の更新



注：管理ユーザ アカウントを更新できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。MA は任意のアカウントを更新できます。GA は、MA アカウントを除き、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを更新できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを更新できます。一方、UA は自分のスコープに含まれる自分の同格者のアカウントのみを更新できます。

管理者の基本的な詳細（名、ミドル ネーム、姓、連絡先情報など）や管理者の管理ロール、パスワード、管理スコープを更新する方法

1. 管理ユーザの更新に必要な権限でログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションで **[Search Users and Administrators]** リンクをクリックし、対応するページ（[図 13-4](#)）を表示します。
4. 前のセクションの説明に従ってアカウントを更新する管理者の情報の一部または全部を入力し、**[Search]** ボタンをクリックします。
検索条件に一致した管理者のリストが表示されます。
5. アカウントを編集する管理者の *<user name>* リンクをクリックします。

[図 13-6](#) のような **[Basic User Information]** ページが表示されます。

図 13-6 [Basic Administrator Information] ページ

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title "Arcot Administration Console" is in the center. On the right, a welcome message for "PLAURIE (DEFAULTORG)" is shown with a "Logout" link and the last login time "07/12/2010 11:16:24 GMT". Below the header, there are four tabs: "Users and Administrators" (selected), "Organizations", "Reports", and "Case Management". Under the "Users and Administrators" tab, there is a sub-section "Manage Users and Administrators". On the left side of this section, there are links: "Create Administrator", "Search Users and Administrators", and "Basic User Information". Under "Basic User Information", the "User Details" link is selected. The main content area shows the details for user "FANTONY", including the organization "DEFAULT ORGANIZATION" and status "Active". Below this, there is a "Basic User Information" section with a "User Information" table. The table lists the user's first name (Francis), middle name (N/A), last name (Antony), email address (fantony@arcot.com), creation date (07/09/2010 09:12:09 GMT), last modified date (07/09/2010 09:12:09 GMT), and phone number (N/A). At the bottom of the table, there are "Edit" and "Return to Search" buttons.

User Information	
First Name:	Francis
Middle Name:	N/A
Last Name:	Antony
Email Address:	fantony@arcot.com
Creation Date:	07/09/2010 09:12:09 GMT
Last Modified:	07/09/2010 09:12:09 GMT
Phone Number:	N/A

[Edit](#) [Return to Search](#)

6. [Edit] ボタンをクリックし、以下の図（図 13-7）に示すページで管理者の情報を変更します。

図 13-7 [User Information] ページ

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- **User Details**

User Name: FANTONY **Organization: DEFAULT ORGANIZATION** **Status: Active**

Basic User Information

User Information

Edit the required user information. Click the Next button to reset their password and the scope of management, if this user belongs to an administrative role.

Administrator Details

Date Created: 07/09/2010 09:12:09 GMT
Last Modified: 07/09/2010 09:12:09 GMT
First Name:
Middle Name:
Last Name:
Email Address:
Phone Number:

7. **[Administrator Details]** セクションで、必要なフィールド（**[First Name]**、**[Middle Name]**、**[Last Name]**、**[Email Address]**、および **[Phone Number]**）を編集します。
8. **[Save]** ボタンをクリックして変更を保存し、**[User Information]** ページに戻るか、または **[Next]** をクリックして追加の設定に進みます。
[Next] をクリックすると、**[Update Administrator]** ページ（図 13-8）が表示されます。

図 13-8 [Update Administrator] ページ

Arcot Administration Console

Welcome **PLAURIE** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- User Details

User Name: FANTONY **Organization:** DEFAULT ORGANIZATION **Status:** Active

Basic User Information

Update Administrator

Update the details of the specified administrative user.
Note: To reset the credential, the target administrator will need to go through the reset flow.

Role

Role: *

Set Password

Password: *

Confirm Password: *

Manages

Manages

9. このページで以下のように必要なフィールドを編集します。

- **[Role]** ドロップダウン リストを使って管理者のロールを変更します。

- 管理者の **[Set Password]** を行います。
- 管理者が管理する組織を選択します。また、**[Selected Organizations]** から **[Available Organizations]** に特定の組織を移動させることにより、スコープから組織を削除できます。

10. **[Save]** ボタンをクリックして更新を保存します。

管理者アカウントの無効化

セキュリティ上の理由で管理者が自分のアカウントにログインすることを禁止する場合は、アカウントを削除せずに無効にすることができます。管理者アカウントを無効にすると、管理者は自分のアカウントからロックアウトされ、アカウントが再度有効にならない限りログインできません。



注：管理ユーザ アカウントを無効化できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。MA は任意のアカウントを無効化できます。一方、GA は、MA アカウントを除き、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを無効化できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを無効化できます。一方、UA は自分のスコープに含まれる自分の同格者のアカウントのみを無効化できます。

管理者アカウントを無効にする方法

1. 管理ユーザ アカウントの無効化に必要な権限でログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、**[Search Users and Administrators]** ページを表示します（図 13-4 を参照）。
4. アカウントを無効にする管理者の情報の一部または全部を入力し、**[Search]** をクリックします。

また、**[Advanced Search]** リンクをクリックして、ステータス（アクティブか非アクティブ）またはロール（GA、OA、または UA）に基づいてユーザを検索できます。

[Search Results] ページ（図 13-9）に、指定された条件に一致したすべてのユーザが表示されます。

図 13-9 検索結果

Arcot Administration Console

Welcome **PLAUBIE (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- **Search Users and Administrators**

Search Results

Click the [User Name](#) link to view or edit the details. To enable, disable, or delete multiple user accounts, select the users and click the applicable button.
Note: You can also reorder the user list by clicking the [User Name](#) column heading.

First Name Last Name User Name Organization Email Search [Advanced Search](#)

Select Users to Modify

☐	User Name	Full Name	Organization	Email	Role	User Status
☐	FRANK	FNAME LNAME	DEFAULT ORGANIZATION	user@arcot.com	User	Active
☒	LWARD	Lauren Ward	DEFAULT ORGANIZATION	lward@arcot.com	Organization Adminis...	Active

Results 11-12 of 12

[Enable](#) [Disable](#) [Delete](#)

5. アカウントを無効にする管理者を 1 人以上選択します。
6. **[Disable]** をクリックして、選択した管理者アカウントを無効にします。

管理者アカウントの有効化

無効になっているアカウントを有効にする必要がある場合があります。たとえば、管理者が長期休暇を取っている場合は、管理者アカウントを無効にします。これにより、その管理者アカウントへの不正なアクセスを防ぐことができます。

[Search Users and Administrators] ページで検索条件を指定して **[Search]** ボタンをクリックしても、無効になっているアカウントを直接検索することはできません。このようなユーザには **[Advanced Search]** を実行し、**[Include Inactive Users]** オプションを使用して検索する必要があります。



注：管理ユーザ アカウントを有効化できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。MA は任意のアカウントを有効化できます。一方、GA は、MA アカウントを除き、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを有効化できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを有効化できます。一方、UA は自分のスコープに含まれる自分の同格者のアカウントのみを有効化できます。

効になっている管理者アカウントを有効にする方法

1. 管理ユーザ アカウントの有効化に必要な権限でログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、**[Search Users and Administrators]** ページを表示します（図 13-4 を参照）。
4. **[Advanced Search]** リンクをクリックして、ステータス（アクティブまたは非アクティブ）に基づいてユーザを検索します。
[Advanced Search] ページ（図 13-5）が表示されます。
5. **[User Account]** セクションに管理者の情報を一部または全部入力します。
6. **[User Status]** セクションで、すべての非アクティブな管理者アカウントを検索するために **[Include Inactive Users]** オプションを選択します。
7. **[Search]** ボタンをクリックすると、検索条件と一致するすべての管理者のリストが表示されます。
8. アカウントを有効にする管理者を選択します。
9. **[Enable]** をクリックして管理者アカウントを有効にします。

管理者アカウントの削除

管理者アカウントを削除すると、その管理者アカウントに関連付けられた権限はすべて完全に削除されます。その結果、その管理者は **Administration Console** にログインできなくなります。ただし、そのアカウント情報とクレデンシャルはシステムから削除されません。

同じ組織内では、以前に削除された管理者アカウントと同じ名前で新しい管理者アカウントを作成することはできませんが、別の組織では作成できます。



注：管理ユーザ アカウントを削除できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。**MA** は任意のアカウントを削除できます。一方、**GA** は、**MA** アカウントを除き、自分のスコープに含まれる（他の **GA** を含む）すべてのアカウントを削除できます。**OA** は、自分の権限の範囲内にある他のすべての **OA** アカウントと **UA** アカウントを削除できます。

ただし、**UA** は、自分のスコープ内のピアを削除できません。

管理者アカウントを削除する方法

1. 管理ユーザ アカウントの削除に必要な権限でログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、**[Search Users and Administrators]** ページを表示します（図 13-4 を参照）。
4. アカウントを削除する管理者の情報の一部または全部を入力し、**[Search]** ボタンをクリックします。

また、**[Advanced Search]** リンクをクリックして、ステータス（アクティブか非アクティブ）またはロール（**GA**、**OA**、または **UA**）に基づいてユーザを検索できます。

[Search Results] ページ（図 13-9 と同様）に、指定された条件に一致したすべてのユーザが表示されます。

5. アカウントを削除する管理者を 1 人以上選択します。
6. **[Delete]** をクリックします。



注：管理者を削除しても、そのアカウント情報はデータベースに引き続き保持されます。

第 14 章 ユーザの管理

RiskFort は、ユーザのアプリケーションと連携して、管理者とエンド ユーザのための強力な認証を管理します。ただし、RiskFort では、ユーザが Administration Console を使用して直接エンド ユーザを作成することはできません。一括操作で既存のユーザを移行したり RiskFort データベースに新しいユーザを作成するために、RiskFort では豊富な SDK と Web サービスを提供しています。RiskFort にユーザを作成するプロセスは、移行と呼ばれます。



関連文書：ユーザ登録のワークフローを理解するには、「Arcot RiskFort 2.2.6 Java 開発者ガイド」の第 2 章「登録ワークフロー」を参照してください。

ユーザ情報の管理は、安全なシステムの維持において重要な部分を占めます。この目的のために RiskFort がサポートするエンド ユーザ管理操作には、以下のものが含まれます。

- ユーザの検索
- ユーザ情報の更新
- ユーザを管理者レベルへ上げる
- ユーザ アカウントの無効化
- ユーザ アカウントの有効化
- ユーザ アカウントの削除

ユーザの検索



注：ユーザ アカウントの更新、アクティブ化、または非アクティブ化を実行する必要がない限り、検索するために権限は必要ありません。ただし、ターゲット ユーザが所属する組織の範囲を担当している必要があります。たとえば、ある組織の GA は、別の組織がその GA の権限の範囲内にあれば、その組織のユーザを検索できます。

条件を指定してユーザを検索する方法

1. 適切なスコープを持つユーザでログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、ユーザと管理者の検索ページを表示します (図 14-1 を参照)。

図 14-1 ユーザと管理者の検索ページ

The screenshot shows the Arcot Administration Console interface. At the top, there is a header with the Arcot logo and the text "Arcot Administration Console". On the right side of the header, it says "Welcome RL AURIE (DEFAULTORG) | Logout" and "Last Login Time 07/12/2010 11:16:24 GMT". Below the header, there is a navigation bar with four tabs: "Users and Administrators", "Organizations", "Reports", and "Case Management". The "Users and Administrators" tab is selected. Under this tab, there is a sub-section "Manage Users and Administrators". On the left side of this sub-section, there is a list of links: "Create Administrator", "Search Users and Administrators", and "Manage Users and Administrators". The "Search Users and Administrators" link is highlighted. The main content area of the page is titled "Search Users and Administrators". It contains a text box with the following text: "Specify the search criteria to display the list of users. Use the Advanced Search link to additionally search on Status or Role. Tip: You need not enter the complete values in the fields. Also, you can specify the organization's Display Name to search for the user in an organization." Below this text box, there is a search form with five input fields: "First Name", "Last Name", "User Name", "Organization", and "Email". To the right of these fields are two buttons: "Search" and "Advanced Search".

4. ユーザのリストを表示するための検索条件を指定します。以下のことが可能です。
 - このページのフィールドにユーザの情報を一部または全部指定してユーザを検索する。
 - 組織の表示名を指定してユーザを検索する。
 - 条件を指定せずに **[Search]** をクリックするだけでユーザを検索する。

- **[Advanced Search]** リンクをクリックして詳細検索ページ（[図 14-2](#)）を表示し、**[Status]** または **[Role]** を指定してユーザを検索する。

図 14-2 詳細検索ページ

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Advanced Search

Click the User Search Criteria tab to specify the type of credential you want to base your search on.

User Search Criteria

User Details

First Name:

Middle Name:

Last Name:

User Name:

Organization:

Email Address:

User Status

Include Active Users: ☒

Include Inactive Users: ☐

Include Deleted Users: ☐

Available Roles

Role:

User
Customer Service Rep(CSR)
Fraud Analyst
Global Administrator

Search

5. 必要なユーザの詳細を指定して、**[Search]** をクリックします。
検索条件に一致したユーザのリストが表示されます。

ユーザ情報の更新



注：ユーザ アカウントの設定の更新を可能にするには、更新を行うための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべてのユーザ アカウントを更新できます。GA は、自分のスコープ内のすべてのユーザ アカウントを更新できます。OA と UA は、自分の権限の範囲内にあるユーザ アカウントを更新できます。

ユーザの基本的な詳細（姓、名、ミドルネーム、および連絡先情報など）を更新する方法

1. ユーザ情報を更新するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、ユーザと管理者の検索ページを表示します（[図 14-1](#) を参照）。
4. 前のセクションで説明したように、アカウントを更新するユーザの情報を一部または全部入力して、**[Search]** をクリックします。
検索条件に一致した管理者のリストが表示されます。
5. アカウントを編集するユーザの *<user name>* リンクをクリックします。
[図 14-3](#) のようなユーザの基本情報ページが表示されます。

図 14-3 ユーザの基本情報ページ

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title "Arcot Administration Console" is in the center. On the right, a welcome message reads "Welcome RLAURIE (DEFAULTORG) | [Logout](#)" with "Last Login Time 07/12/2010 11:16:24 GMT" below it. A navigation bar contains four tabs: "Users and Administrators" (selected), "Organizations", "Reports", and "Case Management". Below this, a sub-tab "Manage Users and Administrators" is active. The left sidebar lists "Manage Users and Administrators" with sub-links "Create Administrator" and "Search Users and Administrators". Under "Basic User Information", "User Details" is selected. The main content area shows a summary box with "User Name: PETER", "Organization: DEFAULT ORGANIZATION", and "Status: Active". Below this is a "Basic User Information" tab. A "User Information" box contains the following details: First Name: FNAME, Middle Name: N/A, Last Name: LNAME, Email Address: user@arcot.com, Creation Date: 07/09/2010 09:16:02 GMT, Last Modified: 07/09/2010 09:16:02 GMT, and Phone Number: N/A. At the bottom of this box are "Edit" and "Return to Search" buttons.

6.  14-4 に示すように、[Edit] をクリックして、このページでユーザ情報を変更します。

図 14-4 ユーザ情報ページ

Arcot Administration Console

Welcome **PLAURIE** (DEFAULT ORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- User Details**

User Information

User Name: PETER Organization: DEFAULT ORGANIZATION Status: Active

Basic User Information

User Information

Edit the required user information. Click the Next button to reset their password and the scope of management, if this user belongs to an administrative role.

Administrator Details

Date Created: 07/09/2010 09:16:02 GMT
Last Modified: 07/09/2010 09:16:02 GMT
First Name:
Middle Name:
Last Name:
Email Address:
Phone Number:

- 必要なフィールド（[First Name]、[Middle Name]、[Last Name]、[Email Address]、および [Phone Number]）を編集します。
- [Save] をクリックして変更内容を保存し、ユーザ情報ページに戻ります。

ユーザを管理者レベルへ上げる



注： ユーザを管理者レベルへ上げることができるようには、レベルを上げるための適切な権限およびスコープを持っていることを確認する必要があります。MA はいずれのユーザのレベルも上げることができます。GA、OA、および UA は、自分のスコープ内のユーザのレベルを上げることができます。

ユーザの管理ロール、パスワード、および管理スコープを更新する方法

1. 管理者を作成したりユーザ情報を更新するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、ユーザと管理者の検索ページを表示します (図 14-1 を参照)。
4. 前のセクションで説明したように、アカウントを更新するユーザの情報を一部または全部入力して、**[Search]** をクリックします。
検索条件に一致したユーザのリストが表示されます。
5. アカウントを編集するユーザの *<user name>* リンクをクリックします。
図 14-3 のようなユーザの基本情報ページが表示されます。
6. **[Edit]** をクリックして、編集可能なユーザ情報ページ (図 14-4 と同様) を開きます。
7. ユーザの **[Email Address]** が指定されていない場合は、同様に入力します。この属性は管理者には必須です。
8. **[Promote as Administrator]** をクリックして、管理者の作成ページ (図 14-5) を表示します。

図 14-5 管理者の作成ページ

Arcot Administration Console

Welcome **RLAURIE** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- User Details**

User Name: PETER **Organization:** DEFAULT ORGANIZATION **Status:** Active

Basic User Information

Create Administrator

Set the Administrator's Role, Scope, and Password credential.
Note: To reset the credential, the target administrator will need to go through the reset flow.

Role

Role: * --Select--

Set Password

Password: *

Confirm Password: *

Manages

All Organizations: ☐

Available Organizations

- DEFAULT ORGANIZATION
- HSBC
- Safe Bank

Selected Organizations

9. このページで以下の作業を行います。

- **[Role]** ドロップダウン リストから新しい管理者のロールを指定します。

- **[Password]** と **[Confirm Password]** のフィールドに、管理者アカウントのパスワードを入力します。
- **[Manages]** セクションで、管理者のスコープとなる組織を選択します。
 - その管理者にシステムの現在の組織と今後作成される組織をすべて管理させる場合は、**[All Organizations]** オプションをオンにします。

または

- **[Available Organizations]** リストから必要な組織を選択し、**[>]** ボタンをクリックしてこれらの組織を **[Selected Organizations]** に追加します。

[Available Organizations] リストに、ログインした管理者のスコープで選択可能なすべての組織が表示されます。**[Selected Organizations]** に、管理者が管理するために選択した組織のリストが表示されます。

10. **[Create]** をクリックして変更を保存し、管理者アカウントを作成してアクティブにします。

ユーザ アカウントの無効化

セキュリティ上の理由でユーザがアカウントにログインできないようにするには、アカウントを削除するのではなくアカウントを無効にすることができます。ユーザ アカウントを無効にすると、そのアカウントがロックされ、アカウントが再び有効にされるまでログインできなくなります。



注： ユーザ アカウントの無効化を可能にするには、無効にするための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべてのユーザ アカウントを無効にすることができます。一方で、GA は自分のスコープ内のすべてのユーザ アカウント（他の GA を含む）を無効にすることができます。OA と UA は、自分の権限の範囲内にあるすべてのユーザ アカウントを無効にすることができます。

ユーザ アカウントを無効にする方法

1. ユーザ アカウントを無効するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。

3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、ユーザと管理者の検索ページを表示します (図 14-1 を参照)。
4. アカウントを無効にするユーザの情報を一部または全部入力して、**[Search]** をクリックします。

また、**[Advanced Search]** リンクをクリックして、ステータス (アクティブか非アクティブ) またはロール (GA、OA、または UA) に基づいてユーザを検索できます。

検索結果ページ (図 14-6) に、指定された条件に一致したすべてのユーザが表示されます。

図 14-6 検索結果

Arcot Administration Console

Welcome **RLAURIE (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

- [Create Administrator](#)
- Search Users and Administrators**

Search Results

Click the User Name link to view or edit the details. To enable, disable, or delete multiple user accounts, select the users and click the applicable button.
Note: You can also reorder the user list by clicking the User Name column heading.

First Name: Last Name: User Name: Organization: Email: [Search](#) [Advanced Search](#)

Select Users to Modify ◀◀ 1 2 ▶▶

☐	User Name	Full Name	Organization	Email	Role	User Status
☒	FRANK	FNAME LNAME	DEFAULT ORGANIZATION	user@arcot.com	User	Active
☐	LWARD	Lauren Ward	DEFAULT ORGANIZATION	lward@arcot.com	Organization Adminis...	Active

Results 11-12 of 12

[Enable](#) [Disable](#) [Delete](#)

5. アカウントを無効にする 1 人以上のユーザを選択します。
6. **[Disable]** をクリックして選択したユーザアカウントを無効にします。

ユーザ アカウントの有効化

無効にしたアカウントを有効にする必要がある場合があります。たとえば、管理者が長期休暇を取る場合は、管理者アカウントを無効にする場合があります。これにより、その管理者アカウントへの不正なアクセスを防ぐことができます。

ユーザと管理者の検索ページで検索条件を指定して **[Search]** ボタンをクリックしても、無効になっているアカウントを直接検索することはできません。このようなユーザには **[Advanced Search]** を実行し、**[Include Inactive Users]** オプションを使用して検索する必要があります。



注： ユーザ アカウントの有効化を可能にするには、有効にするための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべてのアカウントを有効にすることができます。一方で、GA は自分のスコープ内のすべてのアカウントを有効にすることができます。OA と UA は、自分の権限の範囲内にあるすべてのユーザ アカウントを有効にすることができます。

ロックされたユーザ アカウントを有効にする方法

1. ユーザ アカウントを有効にするために必要な権限を持つユーザとしてログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、ユーザと管理者の検索ページを表示します (図 14-1 を参照)。
4. **[Advanced Search]** リンクをクリックして、ステータス (アクティブまたは非アクティブ) に基づいてユーザを検索します。
詳細検索ページ (図 14-2) が表示されます。
5. **[User Account]** セクションにユーザの部分的または完全な情報を入力します。
6. **[User Status]** セクションで、**[Include Inactive Users]** オプションをオンにして、非アクティブなユーザ アカウントをすべて検索します。
7. **[Search]** をクリックして、検索条件に一致するすべてのユーザのリストを表示します。
8. アカウントを有効にするユーザを選択します。
9. **[Enable]** をクリックして、ユーザ アカウントを有効にします。

ユーザ アカウントの削除

ユーザ アカウントが削除されると、そのアカウントに関連付けられた権限はすべて永久に削除されます。その結果、そのユーザはアプリケーションにログインできなくなります。ただし、そのアカウント情報とクレデンシャルはシステムから削除されません。

以前に削除したユーザと同じ名前の新しいユーザ アカウントを作成しても、その新しいアカウントが自動的に以前に削除されたアカウントの権限をそのまま使用すると見なされることはありません。削除されたアカウントを複製する必要がある場合は、手動ですべての権限を再作成する必要があります。



注：ユーザ アカウントの削除を可能にするには、削除するための適切な権限およびスコープを持っていることを確認する必要があります。MA はすべてのアカウントを削除できます。一方で、GA は自分のスコープ内のすべてのアカウント（他の GA を含み、MA アカウントを除く）を削除できます。OA と UA は、自分の権限の範囲内にあるすべてのユーザ アカウントを削除できます。

ユーザ アカウントを削除する方法

1. ユーザ アカウントを削除するために必要な権限を持つユーザとしてログインしていることを確認します。
2. **[Users and Administrators]** タブをアクティブにします。
3. **[Manage Users and Administrators]** セクションの下で、**[Search Users and Administrators]** リンクをクリックして、ユーザと管理者の検索ページを表示します（[図 14-1](#) を参照）。
4. アカウントを削除するユーザの情報を一部または全部入力して、**[Search]** をクリックします。

また、**[Advanced Search]** リンクをクリックして、ステータス（アクティブか非アクティブ）またはロール（ユーザ）に基づいてユーザを検索できます。

検索結果ページ（[図 14-6](#) と同様）に、指定された条件に一致したすべてのユーザが表示されます。

5. アカウントを削除する 1 人以上のユーザを選択します。

6. **[Delete]** をクリックします。



注：ユーザを削除しても、そのアカウント情報はそのままデータベースに保持されます。

第 15 章

ケースの管理



重要：この章では、テクニカル サポート 担当者が実行できるタスク（[ケースの処理](#)）、不正行為アナリストのみが実行できるタスク（[トランザクションの分析](#)）、およびキュー マネージャが実行できるタスク（[ケース キューの管理](#)）があります。これらの 3 つのケース ロールの間では、タスクは相互に排他的です。

ただし、Organization Administrator（OA）および Global Administrator（GA）には、範囲内にある組織でこれらのタスクを処理するためのすべての権限があります。

RiskFort のケース管理機能は、User Administrator（UA）および不正行為アナリスト（FA）にケースに、関連データの単一の統一ビューを提供します。これによってより効率的にデータを分析し、ケースの解決に向けてより速く、適切な情報に基づいて決定を行うことができます。さらに、アナリストは、ケースのステータスおよび進捗状況を常時追跡し、ケースの完全な履歴を保持すると共に、すべての関連情報へ即座にアクセスできます。

この機能を使用すると、以下の作業が可能です。

- 顧客サービスおよびサポートを効率的に管理する
- 多数のケースおよび調査を管理する
- 期限付きのアクションおよびタスクを作成する
- 期限付きのアクションを割り当てる
- ユーザに提供する調査メモや解決策を記録する
- ケースとタスクをより効率的に処理する
- ケースにおけるアクションの明瞭な追跡記録または履歴を保持する
- 傾向を分析する
- 不正行為に関連するレポートを生成する

この章では、RiskFort のケース管理の基本について説明し、以下のトピックについて説明します。

- RiskFort ケースについて
- ケース ロール
- ケースの状態
- ケース管理ワークフロー
- ケース キューの管理
- トランザクションの分析
- ケースの処理
- 不正行為統計レポートの生成

RiskFort ケースについて

ケース管理機能により、トランザクションを調査し、疑わしいとマークされたトランザクションを直観的および効率的に管理できます。この機能により、明確で包括的なアクティビティの記録が作成され、調査の各局面を記録して文書化するという課題に容易に取り組むことができます。また、この機能では、理由の詳細なリスト、推奨事項、地理的位置情報、接続詳細およびリスク評価の詳細など、検索結果のレポートが自動的に作成されるため、時間を節約できます。

このセクションでは、以下のセクションの情報を参考にして、管理対象のケース（以下「ケース」）に関連する重要なポイントについて説明します。

- ケースの基本
- ケース管理のコンポーネント

ケースの基本

RiskFort で管理されるケースの要点を以下に示します。

- RiskFort システムでアドバイスの結果が**否認**または **Increase Authentication** となったユーザのすべてのトランザクション（ログイン、電子送金、またはアプリケーションが評価するすべてのトランザクション）は、ケースと見なされます。

言い換えれば、1 つのケースに複数の疑わしいユーザ トランザクションが含まれる場合があります。

- すべてのケースは、ユーザ、トランザクション詳細、およびケース履歴に関連する情報を提供します。

言い換えれば、ユーザと開かれたケースは、厳密に 1 対 1 で対応します。そのため、ユーザに対してケースがすでに開かれている場合、疑わしい新規トランザクションは既存のケースに追加されます。ユーザにすでに開かれているケースがある場合、新しいケースは作成されません。

- いかなる時にも、1 人のユーザはシステム内に開かれたケースを 1 つだけ持つことができます。
- Administration Console からケースを表示する場合、管理者によって処理されておらず、したがって不正行為ステータスがまだ決定されていないケース内のすべてのトランザクションが常に表示されます。
- システム内でケースが作成されると、そのケースのすべてのトランザクションが処理（[Fraud] または [Not A Fraud]）としてマーク付け）されない限り、閉じることができません。

テクニカル サポート 担当者（CSR）がこれらのトランザクションをすべて処理した場合は、そのケースを明示的に閉じる必要があります。その時初めてそのケースは閉じられたと見なされます。

- ケースが閉じられた場合、指定されたユーザに新しい警告または疑わしいトランザクションが表示されると、システムに新しいケースが作成されます。新規およびそれ以降のトランザクションはすべてこの新しいケースに割り当てられます。

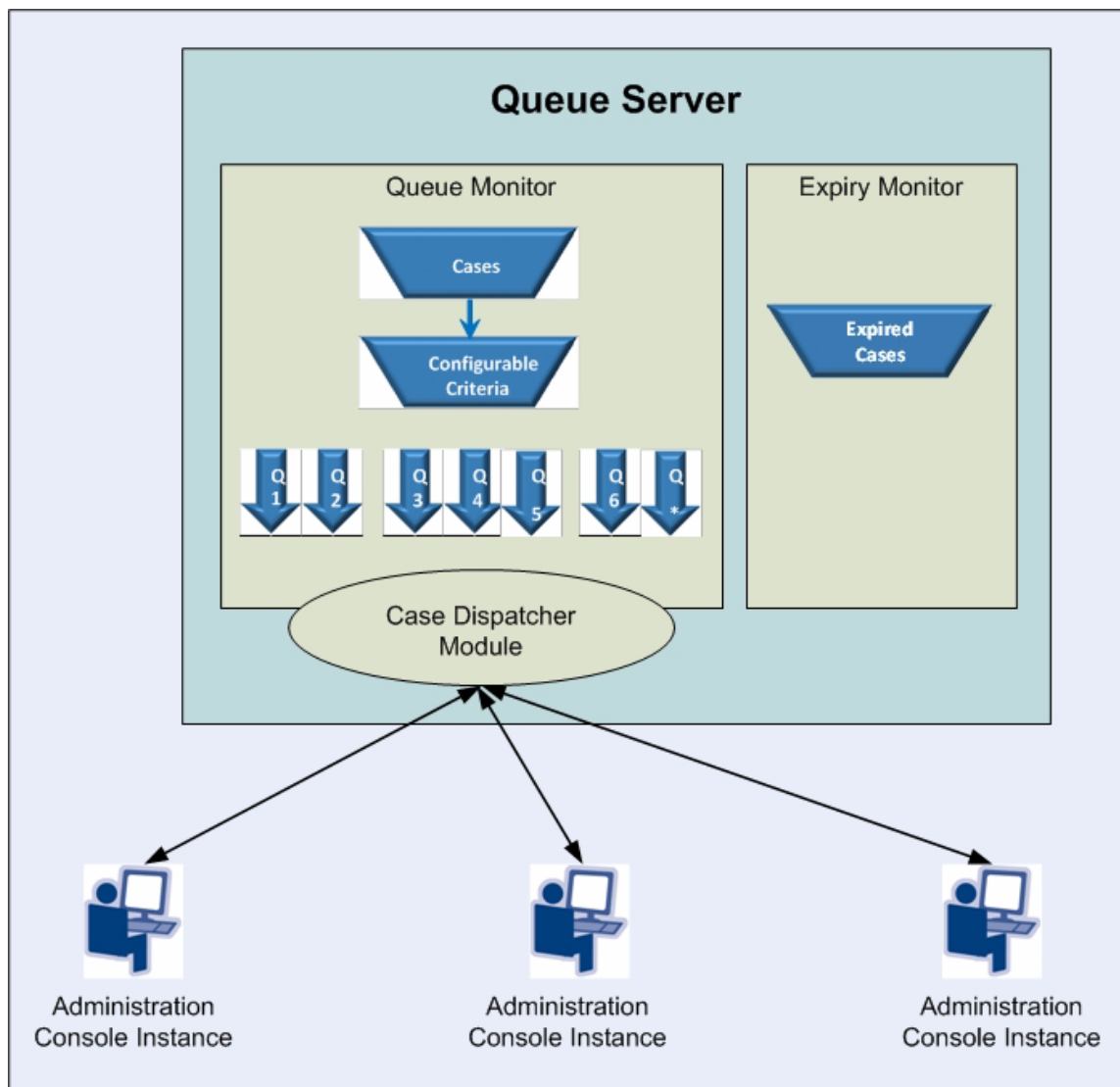
ケース管理のコンポーネント

ケース管理モジュールのコンポーネントには次のものが含まれます。

- ケース キュー
- キュー サーバ
- キュー監視スレッド
- ケース ディスパッチャ モジュール
- 有効期限監視スレッド

図 15-1 では、これらのコンポーネントがどのように連携するのかを図解します。

図 15-1 ケース管理のコンポーネント

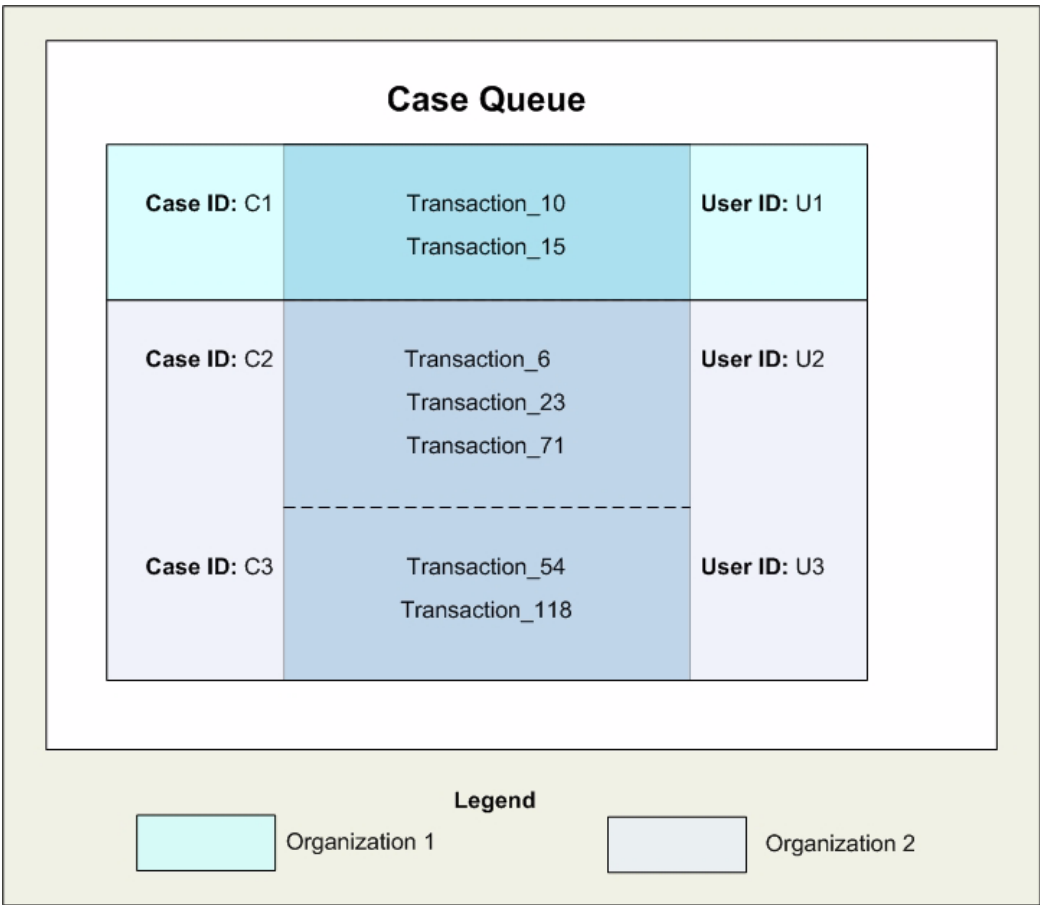


ケース キュー

ケース キュー（または単にキュー）は、作成日時、更新日時、開かれているトランザクション数、および次のアクション日時のような条件に基づいてグループ化されるケースのリストです。現在、RiskFort は、システムの各組織につき 1 つのキューをサポートします。

図 15-2 に、標準的なキューの例を示します。

図 15-2 ケース キュー



キューはキュー マネージャによって管理され、キュー名、キュー内のケース順序基準、およびケースの優先度に関連付けられています。キュー監視スレッドは、システム内で処理が必要なすべてのケースを調べて、それらのケースをそれぞれのキュー基準に基づいて個々のキューに割り当てます。

ケースが個々のキューに割り当てられた後、キュー マネージャはキューから CSR へのマッピングを作成します。このマッピングは、Case Management Queuing Server が開始された時にキャッシュされ、その後キュー サーバがこれを使用してケースを割り当てます。テクニカル サポート 担当者は、(Administration Console インターフェースを介して) ケースを割り当てられ、それぞれのキューから操作を行います。



注：1つの組織の1つのキューを複数のCSRに割り当てることができます。また、CSRの権限の範囲内に複数の組織がある場合は、CSRを複数のキューに割り当てることができます。

キュー サーバ

キュー サーバは以下の処理に関与します。

- キュー監視スレッドを使用して、ケース キューおよびキューと管理者のマッピングをキャッシュする。
- ケース ディスパッチャ モジュールを使用して、ケース キュー内のケースをアクティブな Administration Console インスタンスに送信する。
- 有効期限監視スレッドを使用して、期限切れになったケースの更新済みリストを保持する。

キュー監視スレッド

キュー監視（スケジューラと呼ばれることもある）スレッドはキュー サーバ側で実行され、ケース スケジュールの作成に関与し、ケース キューにケースを投入し、ケース ディスパッチャ モジュールのためのキューを準備します。

このスレッドは以下のように動作します。

1. 事前に定義された間隔で起動し、以下に示すデータベースから最新のケースすべてのリストを取得します。
 - 少なくとも1つのトランザクションの [Fraud Status] が [Undetermined] と表示されている。

および

 - ケースが期限切れになっていない。
2. キューをケースと共にキャッシュします。

3. その後、ケースの状態（詳細については、[15-243 ページの「ケースの状態」](#)を参照）およびその他の基準（[Transaction Date]、[Transaction Amount]、[Next Action Date] など）に基づいて、ケースを[ケース キュー](#)に割り当てます。
4. ケースがキューに割り当てられる際に、キュー用のメモリ内リストが作成されます。
5. キューへのケース割り当てが完了すると、すべての割り当てられたケースの状態は [OPEN] に変更されます。
6. [テクニカル サポート担当者](#)（CSR）が [Save and Go to Next Case] または [Go to Next Case] をクリックすると、以下のようになります。
 - a. キュー内の次のケースを取得するリクエストが[キュー サーバ](#)を介して[キュー監視スレッド](#)に送信されます。
 - b. これに応じて、[ケース ディスパッチャ モジュール](#)はメモリ キューからそのケースを選択し、リクエストが発信された Administration Console インスタンスにその Case ID を返します。
7. その後、そのケースの状態は [IN PROGRESS] に変更され、CSR はそのケースの処理を実行できます。
8. Case ID を受信するとすぐに、Administration Console インスタンスは、データベースからそのケースのトランザクションをすべて取得し、CSR に同じものを表示します。

ケースの確認プロセスに基づいて、ケースの状態は変更する場合があります。詳細については、[15-243 ページの「ケースの状態」](#)を参照してください。

ケース ディスパッチャ モジュール

ケース ディスパッチャ モジュール（またはディスパッチャ）は、[キュー サーバ](#)側で個々の[テクニカル サポート担当者](#)（CSR）からのケース リクエストをリスンし、要求に応じて[ケース キュー](#)から個々の Administration Console インスタンスに、（キュー内の順序に従い）ケースを「プッシュ」します。

このモジュールは以下のように動作します。

1. CSR がログインすると、ディスパッチャにリクエストが送信され、次のケースを取得します。
2. ディスパッチャはこの CSR に割り当てられたキューから次のケースを取得します。
3. その後、ディスパッチャは RiskFort データベース内の選択されたケースに対してロックを取得します。

4. ディスパッチャはまた、そのケースのステータスを **OPEN** から **IN PROGRESS** に変更し、**Administration Console** インスタンスからリクエストを送信した **CSR** の名前を付けて、影響を受けたテーブルを更新します。
5. ディスパッチャはその後、**Administration Console** インスタンスにケースの詳細を送り返します。**Administration Console** は、そのケースに対するトランザクションを取得し、それらを **CSR** の画面に表示します。
6. **Administration Console** インスタンスはまた、表示されたケースの詳細に対してタイムアウトも設定します。
これにより、**CSR** がケース ページを開いたまま、作業せずに事前定義された時間間隔が経過するのを防ぎます。**CSR** への現在のケース割り当てがタイムアウトした場合、適切なメッセージが **CSR** に表示されます。そのケースはその後タイムアウトして、そのステータスは **OPEN** に変更されます。
7. 現在表示されているケースがタイムアウトせずに、**CSR** が（画面で **[Go To Next Case]** ボタンをクリックして）キュー内の次のケースに移動した場合、ケースステータスは **[INPROGRESS]** から **[OPEN]** に変更されます。

有効期限監視スレッド

有効期限監視スレッドは、スレッドが最後に実行されてから期限切れになったすべてのケースにマークを付ける処理に関与します。これは、**キュー監視スレッド** よりもかなり少ない頻度で起動します。

このスレッドは以下のように動作します。

1. 事前定義済みの設定可能な間隔で起動し、以下に示したすべてのケースのリストを取得します。
 - **[OPEN]** または **[NEW]** ステータスのケース。および
 - 設定された有効期間より後に更新されたケース。すなわち、このスレッドはまだ処理されていないケース、および新しいアラートが生成されていないケースを検索します。
2. 次に、スレッドは、前の手順で **[EXPIRED]** と識別された RiskFort データベース内のすべてのケースのステータスを更新します。
3. スレッドはスリープに戻ります。

ケース ロール

ケース管理機能は以下の広範なカテゴリのロールをサポートします。

- [テクニカル サポート担当者](#)
- [キュー マネージャ](#)
- [不正行為アナリスト](#)

「[ケース ロール権限サマリ](#)」では、これらのロールが利用可能な権限の概要について説明します。

テクニカル サポート 担当者

名前が示唆するように、テクニカル サポート担当者（CSR）はエンド ユーザとの組織のインターフェースです。以下の責任を担います。

- [ケースでの作業](#)
- [カスタマ コールの処理](#)

ケースでの作業

通常、自動的に割り当てられるケースを確認して、それらのケースの処理を行います。ケースの処理を開始すると、そのケースはその CSR の名前でマークされます。その結果、そのケースは別の CSR の画面には表示されません。ただし、[キュー マネージャ](#)はキューに別の CSR を割り当てることによって、ケースを別の CSR に再割り当てすることができます。

また、エンド ユーザに電話をかけて、疑わしいトランザクションの信頼性を確認します。CSR のメイン アクティビティには次のものが含まれます。

- 必要に応じて、エンド ユーザに電話をかけてトランザクションが不正かどうか確認する。
- ユーザ入力に基づいて、指定された期間ユーザを「**Exception User List**」に追加する。

デフォルト期間は 10 日ですが、必要に応じて変更できます。

- ケースを確認した後に、ケースを更新できる。その結果によって、ケース ステータスを「**In Progress**」から以下のいずれかに変更できます。
 - **On Hold**
 - **Closed**

- また、調査の進捗状況をキャプチャするために、自由形式フィールドに適切なメモを取ることもできる。

カスタマ コールの処理

CSR はエンド ユーザからの着信を処理することもあります（すなわち、彼らはカスタマ コールに対応します）。たとえば、顧客が実行しなかったトランザクションが表示されたため、コールセンターに電話をする場合があります。そのような場合、指定されたユーザのケースがすでに存在すれば、オペレータはカスタマからの入力を記録します。カスタマに対するケースが存在しない場合は、ケースは自動的に生成されます。



注： CSR によって収集された入力データは、不正行為アナリストによって分析に使用されます。

この場合、CSR は以下の処理を行います。

- ユーザ コールを処理する。
- ユーザからの情報を記録する。
また、調査の進捗状況をキャプチャするために、自由形式フィールドに適切なメモを取ることができます。
- ユーザの最近のアクティビティを確認する。
- ユーザ入力に基づいて、指定された期間ユーザを [**Exception User List**] に追加する。
デフォルト期間は 10 日ですが、必要に応じて変更できます。
- 指定された期間のユーザによるトランザクションを検索する。

キュー マネージャ

キュー マネージャ（または単にスーパーバイザ）は、ケースがキューに割り当てられる順序を決定します。次のことができます。

- スコープ内のすべての組織でキューを管理します。
キューの詳細については、[15-235 ページの「ケース キュー」](#)を参照してください。

- スコープ内のキューへの CSR の割り当て、および再割り当てを行います。



注：デフォルトでは、キュー マネージャは、不正行為アナリストのタスクを実行できません。ただし、**カスタム ロール**を使用してキュー マネージャに基づいた新規ロールを作成し、このロールに FA 最高位を割り当てることができます。

カスタム ロールを作成する方法の詳細については、[第 3 章の「カスタム ロールの作成」](#)を参照してください。

不正行為アナリスト

不正行為アナリスト (FA) は、トランザクションでの詐欺パターンを調査して分析し、詐欺対策の戦略を定義します。また、他の[テクニカル サポート担当者](#)および利用可能なフィルタによって収集された以下に示すような真のデータを使用することにより、トランザクションの傾向を分析します。

- 指定された期間内の同じユーザによるトランザクション。
- 指定された期間内の同じユーザのデバイスからのトランザクション。
- 指定された期間内の同じ IP アドレスからのトランザクション。

これらの分析に基づいて、FA は RiskFort の微調整についてシステム管理者に助言できます。さらに、不審なトランザクションの疑いがある場合は、それまでシステムがそのトランザクションを疑ったことがない場合でも、エンド ユーザに電話してその疑わしいトランザクションに関連する詳細情報を見つけるように[テクニカル サポート担当者](#)にリクエストを要求することができます。

以下のリストでは、不正行為アナリストによって実行される主な機能について説明します。

- トランザクションのリストにログインして、リアル タイムで表示することができます。
- フィルタ条件の組み合わせを設定し、一定期間内に特定のリスク ステータスの値に一致するすべてのユーザのトランザクションを表示することができます。
- 調査の一部として、FA は、同様のトランザクションも検索できます。以下の条件に基づいて類似性を検出するようにフィルタを定義することができます。
 - 指定された期間内の同じユーザによるトランザクション。
 - 指定された期間内の同じユーザのデバイスからのトランザクション。
 - 指定された期間内の同じ IP アドレスからのトランザクション。

- トランザクションのセットが大きい場合は、データをオフラインでエクスポートし、それを分析することもできます。
- 疑わしいパターンが検索された場合は、CSR による詳細な調査が行われるように、それらのトランザクションに対してアラートを生成することができます。「アラートが生成された」トランザクションは、問題になっているユーザのケースに自動的に追加されます。



注：不正行為アナリストはケースを更新できません。

ケース ロール権限サマリ

表 15-1 は、前のセクションで説明したケース ロールに使用可能な権限を要約します。

表 15-1. ケース ロール権限サマリ

権限	CSR	キュー マネージャ	不正行為アナリスト
ケースの表示	✓	--	--
ケースの検索	✓	--	--
ケースの更新	✓	--	--
ケースのフィルタリング	✓	--	--
例外ユーザ リストへのユーザの追加	✓	--	--
キューの管理 (詳細については「キュー」を参照)	--	✓	--
トランザクションの表示	--	--	✓
トランザクションのフィルタリングと検索	--	--	✓
ケースへのトランザクションの追加 (アラートの生成)	✓	--	✓
トランザクションの分析	--	--	✓
トランザクション データのオフライン エクスポート	--	--	✓

ケースの状態

ケースはそのライフサイクルで、以下の状態を経て進行することができます。

- 新規
- オープン
- 実行中
- On Hold
- 期限切れ
- Closed

新規

ユーザのトランザクションが **[Increase Authentication]** または **[Deny]** アドバイスの結果となった場合、対応するケースがまだ存在しなければ、ユーザに対して新しいケースが作成されます。

テクニカル サポート担当者 (CSR) がそのケースを開くか、またはケースが期限切れになるまで、ケースは **[New]** 状態で残ります。

オープン

テクニカル サポート担当者 (CSR) がそれらに割り当てられた新しいケースを開くと、そのケースはアクティブになり、その状態は **[Open]** に変わります。ケースが **[Open]** 状態である場合は、新しいトランザクションまたはイベントをそのケースに追加できます。

ケースの状態が **[On Hold]** または **[Closed]** のいずれかでない限り、すべてのケースは **[Open]** 状態で残ります。

実行中

テクニカル サポート担当者 (CSR) がケースで作業している間、ケースの状態は **[In Progress]** のままです。すなわち、現在のケースで **[Cancel]** をクリックするか、**[Go To Next Case]** をクリックしてそれらに割り当てられた次のケースに移動すると、現在開いているケースの状態は **[Open]** に変わるか、または明示的にそのケースを変更した状態に変わります。



注： どちらの場合でも、テクニカル サポート担当者 (CSR) は、ケースを **[On Hold]** 状態から **[In Progress]** 状態に変更できます。

On Hold

テクニカル サポート担当者 (CSR) が **[In Progress]** ケースに **[Next Action Date]** を指定することにより、ケースの詳細調査を延期した場合は、ケースの状態は **[On Hold]** に変わります。



注： **[Next Action Date]** の時間枠内に生成されたすべてのイベントはケースに追加されます。

指定された **[Next Action Date]** に到達すると、ケースの状態は自動的に **[Open]** に変わります。

期限切れ

テクニカル サポート担当者 (CSR) が事前定義された日数内に **[New]** ケースで作業しなかった場合、ケース状態は **[Expired]** に変わります。



注： 最後のトランザクションがそのケースに追加された時間、または更新された時間がそのケースの開始日と見なされます。ケースの有効期限は、開始日 + N 日として計算されます。ここで、 N は設定可能な値です。 N のデフォルト値は **10 日** です。

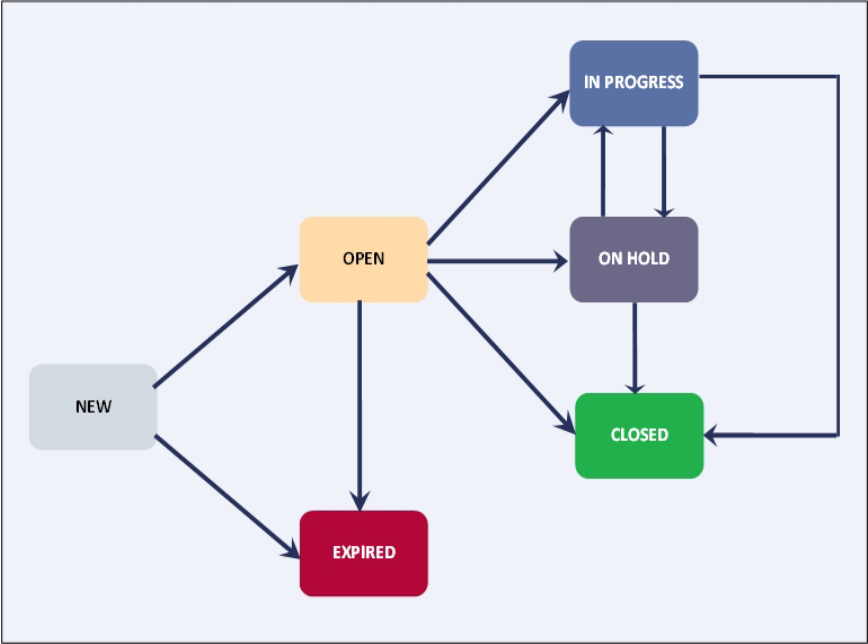
新しいトランザクションは期限切れのケースに追加できません。新しいケース（およびそのための新しい **Case ID**）が作成されて、新しいトランザクションまたはイベントはこの新しいケースに追加されます。

Closed

テクニカル サポート担当者（CSR）がオープンの場合を解決し、それに [Closed] として明示的にマークを付けると、ケースの状態は [Closed] に変わります。

図 15-3 では、ケースの状態が変化する方法を示します。

図 15-3 ケースの状態



ケースの状態権限の一覧

表 15-2 に、前のセクションで説明したケース ロールが使用可能なケースの状態操作権限を要約します。

表 15-2. ケースの状態変更権限サマリ

ケースの状態	ケース オペレータ		不正行為アナリスト
	CSR	キュー マネージャ	
New	--	--	--
Open	✓	--	--
In Progress	--	--	--

表 15-2. ケースの状態変更権限サマリ

ケースの状態	ケース オペレータ		不正行為アナリスト
	CSR	キュー マネージャ	
On Hold	✓	--	--
Expired	--	--	--
Closed	✓	--	--

ケース管理ワークフロー

このセクションでは、ケースのライフサイクルにおける以下の段階のワークフローについて説明します。

1. ケースの生成
2. ケースのキュー
3. ケースの割り当て
4. ケースの処理
5. ケースの期限切れ
6. 不正行為の分析

ケースの生成

通常、ケースはシステムによって自動的に作成されます。ただし、ケース オペレータがユーザの不審なトランザクションに対して手動でフラグを付けた場合、または不正行為アナリストがユーザのトランザクションで不審なパターンを検出した場合は、ケースに不審なトランザクションを追加できます。

ケースは以下の場合に生成されます。

- トランザクションのリスク評価のアドバイスが **[Increase Authentication]** または **[Deny]** のいずれかである場合。



注： ユーザに対してすでにケースが開かれている場合、このトランザクションは既存のケースに追加されます。

- あるトランザクションについてユーザからコールセンターに訴えがあった場合。
この場合オペレータは、訴えのあったトランザクションをより詳細な調査に回すか、不正トランザクションとしてマークすることができます。どちらの場合でも、トランザクションはケースに自動的に追加されます。
- 不正行為アナリストが、いくつかのトランザクションを（通常以前に検出されたパターンに基づいて）不正であると疑って、より詳細な調査を行うためにマークを付けた場合。



注：その後、これらのトランザクションは既存のケースに追加されます。

ケースのキュー

ケースが作成され、トランザクションがそのケースに追加されると、組織が所有しているキューにそのケースを割り当てる必要があります。さらに、これらのケースに取り組むことができる管理者（CSR）も各キューに割り当てる必要があります。[キュー監視スレッド](#)はこの場合、極めて重要なロールを担います。

このスレッドがケースをキューに登録する方法の詳細については、[15-236 ページの「キュー監視スレッド」](#)を参照してください。

ケースの割り当て

ケースがキューに登録された後で、それを各 CSR の画面にディスパッチする必要があります。[ケース ディスパッチャ モジュール](#)はこの場合、極めて重要なロールを担います。

このスレッドがケースをディスパッチする方法の詳細については、[15-237 ページの「ケース ディスパッチャ モジュール」](#)を参照してください。

ケースの割り当てに関する注意事項

このトピックで注意すべき点を以下に示します。

- 新しいケースはそのケースが属する組織から CSR に割り当てられます。
- ケースはケース キューの順序に基づいて割り当てられます。順序の基準には次のものを含めることができます。
 - 次の連絡 / アクション日
 - ケースで開いているトランザクションの数

- ケースの経過日数（作成された日付）
- ケースが最後に更新された日時
- すべてのケースは、組織内の CSR によって最終的に処理されます。

ケースの処理

ケースは、**テクニカル サポート担当者**（CSR）によって以下のように処理されます。

- 新しいトランザクションに FA によってフラグが付けられたり、トランザクションに [Deny] または [Increase Authentication] アドバイスが生成されると、新しいケースが作成されます。**キュー監視スレッド**のスケジュールの前では、ケースのステータスは [NEW] と予定されます。**キュー監視スレッド**はそのステータスを [OPEN] に変更し、CSR がそのケースを表示した時に、ケースのステータスは [INPROGRESS] に変更されます。



注：ケースが CSR によって処理される前に、フラグ付きのトランザクションがさらにそのケースに追加される場合があります。

- CSR には、作業するケースが自動的に割り当てられます。
- 電子メールを送信したり、指定された連絡先番号に電話をすることにより、オフラインのユーザに連絡します。
- 進行中の調査およびエンド ユーザとの連絡の結果に基づいて、CSR はケースを以下のように展開して更新することができます。
 - 特定の時間間隔に基づいてトランザクションを検索する。
 - ユーザとのやり取りの間で、以前疑われていなかったトランザクションをケースに追加する。
 - ケース内の 1 つ以上のトランザクションに対する解決策を選択する。
 - ケースに追跡のためのマークを付けて [Next Action Date] を設定する。

通常、そのようなケースのステータスは [INPROGRESS] または [ON HOLD] のいずれかに更新されます。また、ユーザには後で CSR から連絡があります。
- ユーザの入力データに基づいて、ユーザを指定された期間 [Exception User List] に追加する。
- ケースを解決し、[Case Status] を [CLOSED] に変更する。
- 必要に応じて、**キュー マネージャ**は期限切れのケースを再開できます。

ケースの期限切れ

トランザクションのすべてが規定された時間内に処理されない場合、または事前定義された期間のケースでアクティビティがない場合、ケースは期限切れになります。

このスレッドが期限切れのケースを管理する方法の詳細については、[15-238 ページの「有効期限監視スレッド」](#)を参照してください。

不正行為の分析

不正行為アナリスト によるトランザクションの不正行為分析ワークフローの要点を以下に示します。

- FA は、トランザクション日、2 次認証ステータス、トランザクションのタイプ、リスク アドバイスおよびケース ステータスなどの基準に基づいてトランザクションを検索できます（「[手順 1：トランザクション サマリの表示](#)」を参照）。
 - すべてのトランザクションは最初に [Transaction Summary] ビューに表示されます。
 - 最初、すべてのトランザクションのケース ステータスは [New] です。
 - トランザクションのリストは、[.csv](#) ファイルにエクスポートして Microsoft Excel で処理することができます。
- FA は、ケースをクリックしてその詳細を表示することができます（「[手順 2：ケース詳細の表示](#)」を参照）。
- FA は、ケースに類似しているすべてのトランザクションを検索できます（「[手順 3：類似トランザクションの表示](#)」を参照）。
- 分析中に疑わしいトランザクションおよび潜在的な不正行為のパターンが検索された場合、FA は CSR によって詳細な調査が行われるようにトランザクションをマークできます（「[手順 4：トランザクションに詳細調査のマークを付ける](#)」を参照）。

ケース キューの管理



重要：OA またはキュー マネージャ (QM) のみがこのセクションのタスク（スコープ内にある組織で）を実行できます。MA、GA、UA、FA および CSR はこれらのタスクを実行できません。

このセクションでは、ケース キュー管理に関連する以下のタスクについて説明します。

- キューのステータスの表示
- キューのステータスの更新

キューのステータスの表示

キュー ステータスの表示ページを使用することにより、**DEFAULT Queue** に関連する最新の統計（**[Open Cases]**、**[In-Progress Cases]**、**[Total Cases]** および **[Number of Administrators Assigned]**）を表示することができます。また、**[Cases Handled in the Last 8 Hours]** の詳細も表示します。

キュー ステータスを表示する方法

1. OA または QM としてログインします。
2. **[Case Management]** タブをアクティブにします。
3. **[Queue Management]** セクションの下で、**[View Queue Status]** リンクをクリックして対応するページを表示します。

図 15-4 キュー ステータスの表示ページ



4. **[Select Organization]** リストからキュー ステータスを表示する組織を指定します。

更新されたキューの詳細と共に更新されたページ（図 15-5）が表示されます。

図 15-5 キュー ステータスの表示ページ

**Arcot Administration Console**

Welcome **PRUSH** (DEFAULTTORG) | [Logout](#)
Last Login Time 07/12/2010 05:34:38 GMT

Users and AdministratorsOrganizationsReports**Case Management**

Case Management

Case Management

Queue Management

- View Queue Status**
- Manage Queues

Select Organization: **DEFAULT ORGANIZATION**

Queue Status
This report gives current status of the queue.

Queue Name	Open Cases	In-Progress Cases	Total Cases	No. of Administrators Assigned
DEFAULT	6	0	6	0

Cases Handled in Last 8 Hours
This report gives information for last 8 hours.

Duration	Inbound Cases	Outbound Cases	Total Number of Cases Handled
Last 1 hour	0	0	0
Last 2 hour	0	0	0
Last 3 hour	0	0	0
Last 4 hour	0	0	0
Last 5 hour	0	0	0
Last 6 hour	0	0	0
Last 7 hour	0	0	0
Last 8 hour	0	0	0

キューのステータスの更新

以下のいずれかの方法を使用することにより、**DEFAULT** キューのステータスを更新できます。

- 前のセクション（15-250 ページの「キューのステータスの表示」）で説明されているように、[**View Queue Status**] リンクをクリックして対応するページを表示し、次に [Queue Status] で **DEFAULT** リンクをクリックする。
- [Queue Management] の下の [**Update Queues**] リンクを使用する。

後のオプションを使用して DEFAULT Queue のステータスを更新する方法

1. OA または QM としてログインします。
2. [Case Management] タブをアクティブにします。
3. [Queue Management] の下で、[Update Queues] リンクをクリックして、キューの更新ページを表示します。
4. [Select Organization] リストからキュー ステータスを更新する組織を指定します。
更新されたページ（図 15-6 に表示）が表示されます。

図 15-6 キュー ステータスの更新ページ

Arcot Administration Console

Welcome **PRUSH** (DEFAULTORG) | [Logout](#)
Last Login Time

Users and Administrators Organizations Reports **Case Management**

Case Management

Queue Management
• [View Queue Status](#)
• **Manage Queues**

Manage Queues

Assign administrators who will work on Cases. Use 'Order By' to change the order in which Cases are displayed to the Case Handlers.
For the changes to take effect, refresh the Case Management Queuing Server Cache by running the `arrfadmin` tool.

Select Organization: **DEFAULT ORGANIZATION**

Queue Name: **DEFAULT**

Queue Description: This is the default queue for **DEFAULTORG**

Assign Administrators:

Administrators: FANTONY (DEFAULTORG), JHUME (DEFAULTORG), MPARKER (DEFAULTORG), RLaurie (DEFAULTORG)

Selected Administrators:

Order By: -- Select Element --, Ascending

Then By: -- Select Element --, Ascending

Then By: -- Select Element --, Ascending

Then By: -- Select Element --, Ascending

Save Cancel

5. 必要に応じて、[Queue Description] を指定します。

6. [Assign Administrators] の場合

- a. [Administrators] リストから、キューに割り当てる必要な管理者を選択します。



ヒント：複数の管理者を選択するには、SHIFT キーを押しながら必要な管理者をクリックします。

- b. [Selected Administrators] リストに選択された管理者を移動するには、[>] ボタンをクリックします。



注：[Selected Administrators] リストにすべての管理者を移動させる場合は、[>>] ボタンをクリックします。

7. [Order By] の場合

- a. キューを並べ替える要素（次の連絡日時、作成日時、更新日時、または開かれて
いるトランザクション数）を指定します。
- b. 対応する要素を並べ替える順序（昇順または降順）を指定します。
8. [Save] をクリックして画面で行った更新を保存します。
9. Case Management Queuing Server インスタンスを再起動します。これを実行する方法の詳細は、第4章の「サーバ インスタンスのリフレッシュまたはシャットダウン」を参照してください。

トランザクションの分析



重要：OA および不正行為アナリスト（FA）のみが、スコープ内にある組織のユーザトランザクションを分析できます。MA、GA、UA および CSR はこのタスクを実行できません。

トランザクションの分析には、以下のような複数の手順が含まれています。

- 手順 1：トランザクション サマリの表示
- 手順 2：ケース詳細の表示
- 手順 3：類似トランザクションの表示

- 手順 4：トランザクションに詳細調査のマークを付ける

トランザクション サマリ ページ (図 15-8) に指定された基準に基づいてすべてのトランザクションを検索する際に、1 つ以上の疑わしいトランザクションが見つかった場合は、それらのトランザクションの詳細 (手順 2：ケース詳細の表示) をさらに詳しく検索することができます。類似したトランザクション (手順 3：類似トランザクションの表示) を表示することによりさらにパターンを検索することができます。詳細を分析し、パターンを発見したら、疑わしいトランザクションに CSR による詳細な調査が行われるようにマークを付けることができます (手順 4：トランザクションに詳細調査のマークを付ける)。

手順 1：トランザクション サマリの表示

トランザクション サマリ レポートを表示するには、以下の手順に従います。

1. 適切なクレデンシアル (OA または不正行為アナリスト) でログインしていることを確認します。
2. メイン メニューで [Case Management] タブをアクティブにします。
3. [Case Management] の下で、[Analyze Transactions] リンクをクリックします。
4. [Select Organization] リストから、レポートでデータをフィルタする組織を選択します。

図 15-7 に示されているように、トランザクションの選択ページが表示されます。

図 15-7 トランザクションの選択ページ

Arcot Administration Console

Welcome **RGRAHAM (DEFAULTORG)** | [Logout](#)
Last Login Time 07/06/2010 14:54:47 GMT

Users and Administrators | Organizations | Reports | **Case Management**

Case Management

Case Management
 ● **Analyze Transactions**
 ● [Fraud Statistics Report](#)

Select Transactions
 Select your filter criteria for viewing risk evaluations.

Select Organization: **DEFAULT ORGANIZATION**

User Name:

☒ Transaction Date From: To:

☐ Last Transactions:

Risk Advice
 All Advice
 Allow
 Alert
 IncreaseAuth
 Deny

Secondary Authentication Status
 All Status
 Success
 Failure

Fraud Status
 All Status
 Undetermined
 Confirmed Fraud
 Not a Fraud

Matched Rule: **All Rules**

5. 必要に応じて、トランザクションを表示する **[User Name]** を指定します。



注： **[User Name]** を指定しない場合は、指定された **Organization** のトランザクションがすべて表示されます。

6. 以下のいずれかの基準に基づいてトランザクションをフィルタする方法
- トランザクション データをフィルタする **[Transaction Date From]** および **[To]** フィールドに基づいて、事前定義された日付範囲を選択します。
- または
- [Last Transactions]** オプションを選択し、次に、実行された最新のトランザクションを参照する時間間隔（分単位）を選択します。
7. **[Risk Advice]** リストから、データをフィルタするアドバイスの基づいて、アドバイスを選択します。

8. **[Secondary Authentication Status]** リストから、データをフィルタするステータスに基づいて、ステータスを選択します。
9. **[Fraud Status]** リストから、データをフィルタするステータスに基づいて、ステータスを選択します。
10. **[Matched Rules]** リストから、トランザクション データをフィルタするルールに基づいて、ルールを選択します。



注： 一致したすべてのルールのトランザクションを参照する場合は、デフォルトの **[All Rules]** オプションが選択されていることを確認します。

11. **[Submit]** をクリックして、トランザクション サマリ ページ (図 15-8) を生成します。

[Export] をクリックすることにより情報を CSV ファイルに直接エクスポートできます。

図 15-8 トランザクション サマリ ページ

Transactions Summary

From 07/01/2010 To 07/06/2010

Number of transactions matching the search criteria: 4

Click the corresponding Detail link to view the details of a transaction.

☐	Details	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	detail	PENNY	Undetermined		10.150.1.255	USER_DEVICE_NOT_ASSOCIATE...	07/06/2010 06:37:40 GMT	IncreaseAuth	Success	360
☐	detail	PENNY	Undetermined		10.150.1.255	USER_DEVICE_NOT_ASSOCIATE...	07/06/2010 06:37:30 GMT	IncreaseAuth	Failure	358
☐	detail	MONICA	Undetermined		10.150.1.255	USER_DEVICE_ASSOCIATED_AN...	07/06/2010 06:37:17 GMT	Allow		356
☐	detail	MONICA	Confirmed Fraud		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353

Mark For Investigation

Export

Cancel

表 15-3 では、トランザクション サマリ ページにリスト表示されたフィールドについて説明します。

表 15-3. トランザクション サマリ ページのフィールド

フィールド	説明
[Details]	
[User Name]	トランザクションを実行するユーザの名前。
[Fraud Status]	ケースの不正ステータス。このフィールドには、以下のいずれかのステータスを含めることができます。 • Undetermined • Confirmed Fraud • Not a Fraud
[Country]	[IP Address] を基に判別した、トランザクションが実行された国。
[IP Address]	購入トランザクションに使用したシステムまたはデバイスの IP アドレス。
[Matched Rule]	一致し、RiskFort がトランザクションにリスクがあるとしてフラグを付けたルール。
[Transaction Date]	トランザクションが実行されたタイム スタンプ。
[Risk Advice]	トランザクションの Risk Score を評価した後に RiskFort によって提案されたアクション（許可、アラート、否認または INCREASE AUTHENTICATION）。
[Secondary Auth Status]	[Risk Advice] が INCREASE AUTHENTICATION である場合、この列ではアプリケーションがフィードバックとして RiskFort に返した追加の認証の結果を指定します。
[Transaction ID]	各ユーザ トランザクションに生成された一意の ID。

手順 2：ケース詳細の表示

[Transactions Summary] ページを使用して、特定のトランザクションまたはケースの詳細を表示することもできます。特定のケースの詳細を表示するには、以下の手順に従います。

1. [Transactions Summary] ページ（図 15-8）で、対応する [Details] 列で該当する [detail] リンクをクリックします。

図 15-9 に示されているように、トランザクションの詳細がページに表示されます。このページでは、選択されたトランザクションの詳細をリスト表示し、使用可能なパラメータ（表 15-4）に基づいてさらにトランザクションをフィルタすることもできます。

図 15-9 トランザクションの詳細

Basic Transaction Details			
Transaction ID:	356	Transaction Date:	07/06/2010 06:37:17 GMT
Action:	Login	User Name:	MONICA
Fraud Status:	Undetermined	Risk Advice:	Allow
Matched Rule:	USER_DEVICE_ASSOCIATED_AND_DEVICE_MFP_MATCHED Secondary Auth Status:		
Location Details			
IP Address:	10.150.1.255	City:	
State:		Country:	
Connection Type:		Line Speed:	
IP Routing Type:		Anonymizer Type:	
Risk Assessment Details			
User Known:	YES	Exception User:	NO
Device ID Matched:	YES	User Velocity Exceeded:	NO
User-Device Associated:	YES	Device Velocity Exceeded:	NO
Machine FingerPrint (MFP) Matched:	YES	Zone Hopped:	Not Available
MFP Match %:	80.0	Evaluation Callout Matched:	Not Available
Trusted IP:	NO	Negative IP:	NO
Trusted Aggregator:	NO	Negative Country:	Not Available

表 15-4 では、トランザクションの詳細ページにリスト表示されたフィールドについて説明します。

表 15-4. トランザクションの詳細ページのフィールド

フィールド	説明
[Basic Transaction Details]	
[Transaction ID]	トランザクションの一意の識別子。
[Transaction Date]	トランザクションが実行されたタイム スタンプ。
[Action]	ユーザによって実行されたトランザクションのタイプ。以下の値にすることができます。 • ログイン • 電子送金 • アプリケーション経由で指定したその他の任意の値
[User Name]	トランザクションを実行したユーザの名前。

表 15-4. トランザクションの詳細ページのフィールド

フィールド	説明
[Fraud Status]	現在の不正ステータス。以下の値を使用できます。 • Under investigation • Not a Fraud • Fraud
[Risk Advice]	選択されたトランザクションのリスク スコアを評価した後に Risk Assessment モジュールによって提案されたアクション（許可、アラート、拒否、INCREASEAUTH）。
[Matched Rule]	一致し、RiskFort がトランザクションにリスクがあるとしてフラグを付けたルール。
[Secondary Authentication Status]	[Risk Advice] が INCREASE AUTHENTICATION である場合、この列ではアプリケーションがフィードバックとして RiskFort に返した追加の認証の結果を指定します。
[Location Details]	
[IP Address]	購入トランザクションに使用したシステムまたはデバイスの IP アドレス。
[City]	トランザクションがユーザによって実行された都市。
[State]	ユーザの所在地の都道府県。
[Country]	ユーザの所在地の国。
[Connection Type]	ユーザのデバイスとインターネット サービス プロバイダの間の接続のタイプ。以下の値を指定できます。 • Satellite • OCX • Frame Relay • TX • Dialup • Cable • DSL • ISDN • Fixed Wireless • Mobile Wireless
[Line Speed]	ユーザのインターネット接続の速度。これは、[Connection Type] に基づきます。

表 15-4. トランザクションの詳細ページのフィールド

フィールド	説明
[IP Routing Type]	接続に使用した IP ルーティング メソッド。以下の値を指定できます。 • Fixed (ケーブル、DSL、OCX) • AOL (AOL ユーザ) • POP (地域 ISP までのダイアルアップ) • Super POP (多地域 ISP までのダイアルアップ) • Cache Proxy (アクセラレータ プロキシ、コンテンツ配信サービス) • Regional Proxy (国内の多地域用プロキシ) • Anonymizer (匿名プロキシ) • Satellite (民生用衛星またはバックボーン衛星 ISP) • International Proxy (国際トラフィックを収束するプロキシ) • Mobile Gateway (インターネットへのモバイル デバイス ゲートウェイ) • 不明 (現在特定できません)
[Anonymizer Type]	アノニマイザのタイプ (ある場合) は、接続に使用されます。以下の値を指定できます。 • Private (公衆アクセスが可能でない匿名のプロキシ。通常企業が所有しています) • Active (過去 6 か月以内に陽性のテスト結果が出た匿名のプロキシ) • Suspect (過去 6 か月以内にはなく、過去 2 年以内に陽性のテスト結果が出た、匿名のプロキシ) • Inactive (過去 2 年以内に陽性のテスト結果が出なかった匿名のプロキシ) • Unknown (陽性のテスト結果が現在まで得られていない匿名のプロキシ)
[Risk Assessment Details]	
[User Known]	既知のユーザ ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[Exception User]	例外ユーザ ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[Device ID Matched]	[Whether the Device-ID rule matched.] 以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。

表 15-4. トランザクションの詳細ページのフィールド

フィールド	説明
[User Velocity Exceeded]	ユーザ頻度チェック ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[User-Device Associated]	ユーザとデバイスの関連付けが RiskFort データベース内で見つかったかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[Device Velocity Exceeded]	デバイス頻度チェック ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[Machine FingerPrint (MFP) Matched]	MFP ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[Zone Hopped]	ゾーン ホッピングのチェック ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[MFP Match %]	受信されたマシン FingerPrint (MFP) と RiskFort データベースに格納されている値との一致率。 これは数値です。
[Trusted IP]	トラステッド IP ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[Negative IP]	拒否 IP ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。

表 15-4. トランザクションの詳細ページのフィールド

フィールド	説明
[Trusted Aggregator]	トラステッド アグリゲータ ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。
[Negative Country]	拒否国ルールが一致したかどうか。以下の値を指定できます。 • Yes : ルールが一致した場合。 • No : ルールが一致しなかった場合。 • N/A : リスク評価中に情報を得られなかった場合。

手順 3 : 類似トランザクションの表示

トランザクション詳細 (図 15-10) の最後にある小さなテーブルを使用することによって、RiskFort データベースから類似したトランザクションについてのより詳細なデータを抽出するフィルタ条件を指定できます。

図 15-10 関連するトランザクション テーブルの表示

Show Related Transactions For: ☐ Same User Name ☐ Same Device ID ☐ Same IP Address
☒ Transaction Date From: 07/01/2010 [Hrs] [Mins] To: 07/06/2010 [Hrs] [Mins]
☐ Last Transactions: --Select--
 [Show]

図 15-10 に示されているように、トランザクションを以下のパラメータに基づいてさらにフィルタすることができます。

- **[Same User]** : このオプションを選択すると、現在表示しているデータを所有するユーザに属するすべてのトランザクションを抽出できます。
- **[Same Device ID]** : このオプションを選択すると、現在詳細を表示しているトランザクションに使用されたのと同じデバイスを使用して実行されたトランザクションをすべて抽出できます。
- **[Same IP Address]** : このオプションを選択すると、現在詳細を表示しているトランザクションと同じ IP アドレスを持つトランザクションをすべて抽出できます。
- **[Transaction Date]** : ([From] フィールドと [To] フィールドを使用して) 日付範囲を指定することによって、指定された期間内に実行されたすべてのトランザクションをさらにフィルタすることができます。

または

- **[Last Transactions]** : 必要な時間間隔（分単位）を選択することによって、指定された間隔で実行された最新のすべてのトランザクションをさらにフィルタすることができます。

関連するトランザクションの表示

関連するトランザクションを表示する方法

1. トランザクションの詳細ページで、以下のオプションのいずれかまたはすべてを選択します。
 - **Same User**
 - **Same Device ID**
 - **Same IP Address**
2. 以下のいずれかを行います。
 - a. **[With Transaction Date From]** フィールドおよび **[To]** フィールドに日付の範囲を入力します。

または

- b. **[Last Transactions]** オプションを選択し、関連するトランザクションを参照する最新の時間間隔を選択します。
3. **[Show]** をクリックします。

トランザクション サマリ ページ（[図 15-8](#) と同じ）が表示され、基準と一致したレコードが表示されます。

手順 4 : トランザクションに詳細調査のマークを付ける

疑わしいトランザクションの詳細を分析し、パターンを発見したら、疑わしいトランザクションに CSR による詳細な調査が行われるようにマークを付けることができます。以下の手順に従ってください。

1. 必要な権限（OA または不正行為アナリスト）でログインしていることを確認します。
2. [15-254 ページの「手順 1 : トランザクション サマリの表示」](#) で説明されているように、トランザクション サマリ ページを表示します。
3. 指定した基準で表示されるトランザクションを確認します。

[15-257 ページの「手順 2 : ケース詳細の表示」](#) を参照してください。

4. 類似するパターンを表示する場合は、[15-262 ページの「手順 3：類似トランザクションの表示」](#)の手順に従います。
5. スクロールしてトランザクション サマリ テーブルに戻ります。
6. テーブル内のトランザクションに対応するチェック ボックスをオンにすることにより、疑わしいトランザクションを選択します。
7. **[Mark for Investigation]** をクリックして、マークしたトランザクションのケースを生成します。
これにより、これらのケースがリストに表示され、CSR はケースを処理できます。

ケースの処理

	重要： OA およびテクニカル サポート担当者（CSR）のみが、スコープ内にある組織に属しているケースを処理できます。MA、GA、UA および FA はこれらのタスクを実行できません。

このセクションでは、ケースの処理およびエンド ユーザとの直接対話に関連する以下のタスクについて説明します。

- [ケースでの作業（CSR）](#)
- [顧客からの着信電話の管理（CSR）](#)

ケースでの作業（CSR）

RiskFort がトランザクションを疑わしいとしてマークした場合、または FA が詳細な調査を行うようにトランザクションにマークした場合は、自動的に CSR のケース リストに表示されます。

リストのケースで作業する方法

1. CSR としてログインします。
2. **[Case Management]** タブをアクティブにします。

[図 15-11](#) に表示されているように、（ケースに割り当てられた優先度の順序で）最初のケースが表示されます。

図 15-11 ケース ページ

Arcot Administration Console

Welcome JHUME (DEFAULTORG)
Last Login Time 07/06/2010 15:25:52

Users and AdministratorsOrganizationsReportsCase Management

Management

Management
Management
Work On Cases
Page Inbound Calls

User Name: JOSHUA(DEFAULTORG)Next Action Date: 07/06/2010 15:24:33 GMT

None

Case History:

Alerts on this case

☐	Mark Selected As	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	Undetermined		10.150.1.255		07/06/2010 15:24:37 GMT	IncreaseAuth	Success	38

From: 06/06/2010To: 07/06/2010

Show TransactionsHide Transactions

Case Status: INPROGRESS

Note: -- Select --

Additional Note:

☐ Next Action Date: 07/06/2010Hrs: 00Mins: 00

☐ Add User to Exception List

From: 07/06/2010To: 07/06/2010

Reason:

SaveSave and Go To Next CaseGo To Next CaseCancel

ページのフィールドについては、表 15-5 に説明されています。

表 15-5. ケースで作業するためのフィールド

フィールド	説明
[User Name]	電話をしてきたユーザの名前。
[Next Action Date]	ユーザに次に連絡する必要のある日付。

表 15-5. ケースで作業するためのフィールド

フィールド	説明
[Case History]	前のコール対応者によって入力された最新のケースの [Note] および [Additional Note]。 このフィールドにあるすべてのメモを確認する場合は、[More...] リンクをクリックします。
[Alerts on This Case]	
[Mark Selected As]	トランザクションの Fraud Status。このフィールドに指定できる値は次のとおりです。 • Undetermined • Confirmed Fraud • Not a Fraud アラートが発生し、対応が必要なトランザクションが複数あり、かつユーザと対話した後でそれらの [Fraud Status] がすべて同じ（[Confirmed Fraud] または [Not a Fraud] など）であると判断した場合は、このドロップダウン リストを使用して 1 回のアクションで同じ設定を行うことができます。
Fraud Status	[[Mark Selected As]] フィールドの前のエントリに基づいて、このフィールドには以下のいずれかのステータスを指定できます。 • Undetermined • Confirmed Fraud • Not a Fraud
[Country]	[IP Address] を基に判別した、トランザクションが実行された国。
[IP Address]	ユーザのトランザクションに使用したシステムまたはデバイスの IP アドレス。
[Matched Rule]	一致し、RiskFort がトランザクションにリスクがあるとしてフラグを付けたルール。
[Transaction Date]	指定されたトランザクションが実行されたタイム スタンプ。
[Risk Advice]	指定されたトランザクションのリスク スコアを評価した後に RiskFort によって提案されたアクション（許可、アラート、否認または INCREASE AUTHENTICATION ）。
[Secondary Auth Status]	[Risk Advice] が INCREASE AUTHENTICATION である場合、この列ではアプリケーションがフィードバックとして RiskFort に返した追加の認証の結果を指定します。

表 15-5. ケースで作業するためのフィールド

フィールド	説明
[Transaction ID]	ユーザ トランザクションに対する一意のシステム生成識別子。 注：必要な場合は、[Transaction ID] をクリックすると、詳細を表示できます。(図 15-12 を参照)。
[From] [To]	データをフィルタする事前定義された日付範囲。
[Show Transactions]	前の [[From]] および [[To]] フィールドに基づいてアラートされたトランザクションを表示するボタン。
[Hide Transactions]	表示されているアラートが発生したトランザクションを非表示にするボタン。
[Case Status]	ケースの現在のステータス。以下の値を指定できます。 • INPROGRESS • On Hold • CLOSED
[Note]	事前に特定された更新の理由。
[Additional Note]	ケース ステータスまたはフィールドのいずれかが変更された理由を説明する（前の [Note] に追加する）任意の追加情報。 重要： このフィールドには 250 文字以上入力することはできません。
[Next Action Date]	追加のフォローアップのため、次にユーザに連絡する必要がある日付。
[Add User to Exception List]	ユーザ入力に基づいて、指定された期間のリスク評価からユーザを一時的に除外することができます。 たとえば、ユーザが拒否国の 1 つに旅行している場合に、その国からのユーザのトランザクションを拒否したくないとします。この場合は、ユーザを例外ユーザ リストに追加できます。ユーザが例外ユーザ リストに見つかれば、デフォルトでは、RiskFort はこれらのユーザから発信されるトランザクションに低いスコアおよび ALLOW アドバイスを返します。

表 15-5. ケースで作業するためのフィールド

フィールド	説明
[From] [To]	ユーザを RiskFort リスク評価から免除されるようにする日付範囲。
[Reason]	ユーザが例外ユーザ リストに追加されている理由。

図 15-12 ケースのトランザクション サマリ

Arcot Administration Console

Welcome **JHUME (DEFAULT TORG)** | [Logout](#)
Last Login Time 07/06/2010 15:25:52 GMT

Users and Administrators | Organizations | Reports | **Case Management**

Case Management

Case Management
 ● Work On Cases
 ● [Manage Inbound Calls](#)

Transactions Summary
 Click the corresponding Detail link to view the details of a transaction.

Basic Transaction Details

Transaction ID:	38	Transaction Date:	07/06/2010 15:24:37 GMT
Action:	Login	User Name:	JOSHUA
Fraud Status:	Undetermined	Risk Advice:	IncreaseAuth
Matched Rule:		Secondary Auth Status:	Success

Location Details

IP Address:	10.150.1.255	City:	
State:		Country:	
Connection Type:		Line Speed:	
IP Routing Type:		Anonymizer Type:	

Risk Assessment Details

User Known:	YES	Exception User:	NO
Device ID Matched:	YES	User Velocity Exceeded:	NO
User-Device Associated:	NO	Device Velocity Exceeded:	NO
Machine FingerPrint (MFP) Matched:	YES	Zone Hopped:	Not Available
MFP Match %:	80.0	Evaluation Callout Matched:	Not Available
Trusted IP:	NO	Negative IP:	NO
Trusted Aggregator:	NO	Negative Country:	Not Available

[Back](#)

- 表 15-5 に説明されているフィールドを使用して、ユーザ入力をキャプチャするために必要なアクションを実行します。
- 完了したら、ページ上で以下のいずれかのボタンをクリックします。
 - [Save]** をクリックして、ケースへの変更を更新します。

- **[Save and Go To Next Case]** をクリックして、ケースへの変更を更新して割り当てられた次のケースに移動します。
- **[Go To Next Case]** をクリックして、変更を保存せずに割り当てられた次のケースに移動します。
- **[Cancel]** をクリックして、ページで加えたすべての変更をキャンセルします。

顧客からの着信電話の管理（CSR）

エンド ユーザがトランザクションについて訴えるためにテクニカル サポート センターに電話した場合に、応対した CSR は、**着信電話の管理**ページ（図 15-13）を使用してユーザによって提供される情報をキャプチャし、この情報に基づいてケースに必要な変更を加える必要があります。

図 15-13 着信電話の管理ページ

User Name: MONICA
Next Action Date:

Case History:

None

Alerts on this case

	Mark Selected As	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353

From: 06/06/2010 To: 07/06/2010
Show Transactions Hide Transactions

	Mark Selected As	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353
☐	Undetermined	MONICA	Undetermined		10.150.1.255	USER_DEVICE_ASSOCIATED_AN...	07/06/2010 06:37:17 GMT	Allow		356

Case Status: INPROGRESS
Note: -- Select --
Additional Note:

☐ Next Action Date: 07/06/2010 Hrs: 00 Mins: 00

☐ Add User to Exception List
From: 07/06/2010 To: 07/16/2010
Reason:

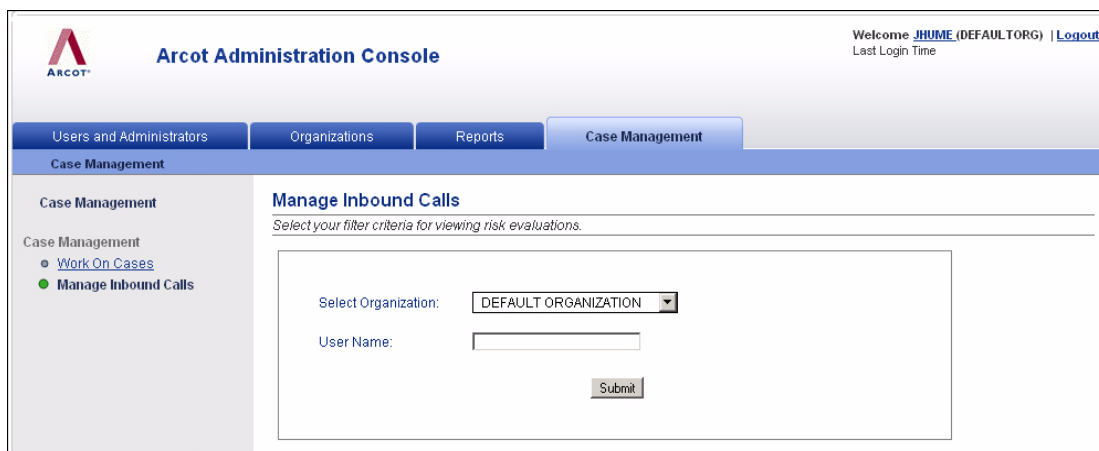
Save Cancel

着信電話の管理ページを使用してケースに必要な変更を加える方法

1. CSR としてログインします。
2. [Case Management] タブをアクティブにします。
3. [Case Management] の下で、[Manage Inbound Calls] リンクをクリックして、着信電話の管理ページを表示します。
4. [Select Organization] リストから、必要な組織を選択します。

図 15-13 に表示されているように、更新された着信電話の管理ページが表示されます。

図 15-14 着信電話の管理ページ



The screenshot shows the Arcot Administration Console interface. At the top, there is a header with the Arcot logo, the title 'Arcot Administration Console', and a user welcome message 'Welcome JHUME (DEFAULTORG) | Logout' with 'Last Login Time' below it. Below the header is a navigation bar with tabs: 'Users and Administrators', 'Organizations', 'Reports', and 'Case Management'. The 'Case Management' tab is selected. On the left side, there is a sidebar with 'Case Management' and two sub-items: 'Work On Cases' (with a blue dot) and 'Manage Inbound Calls' (with a green dot). The main content area is titled 'Manage Inbound Calls' and contains the instruction 'Select your filter criteria for viewing risk evaluations.' Below this, there is a form with two fields: 'Select Organization:' with a dropdown menu showing 'DEFAULT ORGANIZATION', and 'User Name:' with a text input field. A 'Submit' button is located at the bottom right of the form.

5. 電話をかけてきた [User Name] を指定し、[Submit] をクリックします。

図 15-15 に表示されているように、着信電話の管理ページは指定されたユーザのケース情報でリフレッシュされます。

図 15-15 ユーザ情報が入力された着信電話の管理ページ

User Name: MONICA

Next Action Date:

None

Case History:

Alerts on this case

☐	Mark Selected As ▼	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined ▼	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353

From: 06/06/2010

To: 07/06/2010

Show Transactions

Hide Transactions

☐	Mark Selected As ▼	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined ▼	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353
☐	Undetermined ▼	MONICA	Undetermined		10.150.1.255	USER_DEVICE_ASSOCIATED_AN...	07/06/2010 06:37:17 GMT	Allow		356

Case Status

INPROGRESS ▼

Note:

-- Select -- ▼

Additional Note:

☐ Next Action Date: 07/06/2010

Hrs: 00 ▼

Mins: 00 ▼

☐ Add User to Exception List

From: 07/06/2010

To: 07/16/2010

Reason:

Save

Cancel

ページのフィールドについては、表 15-5 に説明されています。

6. 表 15-5 に説明されているフィールドを使用して、ユーザ入力をキャプチャするために必要なアクションを実行します。
7. 完了したら、[Save] をクリックしてケースへの変更を更新します。
加えた変更を保存しない場合は、[Cancel] をクリックします。

不正行為統計レポートの生成



重要：OA および不正行為アナリスト（FA）のみが、スコープ内にある組織でこのレポートを生成できます。MA、GA、UA および CSR はこのレポートを生成できません。

不正行為統計レポート（図 15-17）は、RiskFort が指定された期間内に生成する各リスクアドバイスの全体的統計データを表示します。

不正行為統計レポートを生成する方法

1. 適切なクレデンシャル（OA または不正行為アナリスト）でログインしていることを確認します。
2. メインメニューで **[Case Management]** タブをアクティブにします。
3. **[Case Management]** の下で、**[Fraud Statistics Report]** リンクをクリックします。

図 15-16 に示されているように、不正行為統計レポート ページが表示されます。

図 15-16 不正行為統計レポート

Arcot Administration Console

Welcome RGRAHAM (DEFAULTORG) | Logout
Last Login Time 07/06/2010 15:04:57 GMT

Users and Administrators Organizations Reports Case Management

Case Management

Case Management

- Analyze Transactions
- Fraud Statistics Report

Fraud Statistics Report

Specify the criteria to generate the report.

Organization Name
DEFAULT ORGANIZATION

Date Range
Custom

From
07/06/2010

To
07/06/2010

Display Report

4. **[Organization Name]** リストからのこのレポートを生成する必要な組織を選択します。

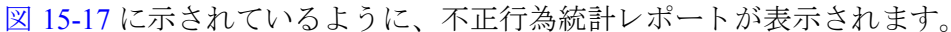
- ドロップダウンメニューから **[Date Range]** を選択します。
また、**[From]** と **[To]** のフィールドに事前定義済みの日付範囲を選択することもできます。
- [Display Report]** をクリックして生成されたレポートを表示します。
 図 15-17 に示されているように、不正行為統計レポートが表示されます。

図 15-17 不正行為統計レポート

Fraud Statistics Report				
This report displays the overall statistics for each Risk Advice generated by RiskFort that matched the criteria that you specified.				
Export New Report				
Date Range: From: 01/01/2009 To: 07/06/2010				
Risk Advice	Fraud	Not a Fraud	Unknown	Total
Allow	0 (0%)	0 (0%)	1 (100%)	1
Increase Authentication	1 (33%)	0 (0%)	2 (67%)	3
Alert	0 (0%)	0 (0%)	0 (0%)	0
Deny	0 (0%)	0 (0%)	0 (0%)	0
Total	1 (25%)	0 (0%)	3 (75%)	4

表 15-6 に説明されているように、不正行為統計レポートは全体的なトランザクション リスクに関連する情報を表示します。

表 15-6. 不正行為統計レポートのフィールド

パラメータ	説明
Risk Advice	各トランザクションのリスクを評価した後に RiskFort によって提案されたアクションを示します。 生成されたリスク アドバイスは以下のいずれかになります。 • Allow • Increase Authentication • Alert • Deny
Fraud	RiskFort によって不正行為としてレポートされたすべてのトランザクションの総数およびパーセンテージを示します。
Not a Fraud	RiskFort によって不正行為ではないと見なされたすべてのトランザクションの総数およびパーセンテージを示します。

表 15-6. 不正行為統計レポートのフィールド

パラメータ	説明
Unknown	RiskFort がリスク アドバイスを生成するための十分なデータを持っていなかったすべてのトランザクションの総数およびパーセンテージを示します。
Total	以下のトランザクションすべての合計を示します。 • Fraud • Not a Fraud • Unknown

7. **[Export]** をクリックしてレポートをファイルに保存するか、または **[New Report]** をクリックして別の基準を指定することにより新規レポートを生成します。

第 16 章 レポートの管理

管理者レベルに基づいてレポートを使用することで、RiskFort データベースの情報をすぐに要約して分析できます。たとえばレポートでは、どの管理者がシステムにアクセスしたか、アクセスした時刻、およびその管理者が実行したアクティビティについて、より高いレベル管理者に伝えることができます。「すべての管理者が使用可能なレポートのサマリ」では、さまざまな管理者が使用できるすべてのレポートの概要を一覧できる表形式で説明します。表 16-1 の後のセクションではこれらのレポートについて説明します。

- 管理者レポート
- RiskFort レポート
- ケース管理レポート

Administration Console から使用可能なレポートは、指定したパラメータ（またはフィルタ）に基づいて生成されます。そのため、レポートの実行時に、設定した値に基づいてレポートの出力をコントロールできます。フィルタ データとして使用可能なパラメータには、以下のものがあります。

- 日付範囲
- 管理者名
- 組織
- ユーザ名

16-300 ページの「レポートの生成」では、管理者のアクティビティ レポートおよび RiskFort 固有のレポートを生成するための一般的なプロセスについて説明します。

作成済みレポートをすべてローカル ファイルにエクスポートすることもできます。その手順については、16-301 ページの「レポートをエクスポートする方法」を参照してください。

すべての管理者が使用可能なレポートのサマリ

表 16-1 に、すべての管理者がシステムで使用可能なすべてのカテゴリのレポート（管理者レポート、RiskFort レポート、およびケース管理レポート）の概要を示します。これらのレポートについては、以降のセクションで詳しく説明します。

表 16-1. すべての管理者が使用可能なレポート：概要

管理者	レポートのカテゴリ		
	管理者レポート	RiskFort レポート	ケース管理レポート
Master Administrator	アクティビティ レポート	--	--
	管理者アクティビティ レポート		
	組織レポート		
Global Administrator	アクティビティ レポート	リスク評価詳細アクティビティ レポート	不正行為統計レポート
	管理者アクティビティ レポート	リスクアドバイスサマリ レポート	
	ユーザ アクティビティ レポート	トラステッド IP/ アグリゲータ レポート	
	組織レポート	拒否 IP アドレス レポート	
		拒否国レポート	
		例外ユーザ レポート	
		アドオン ルール レポート	
		ルール データ レポート	
		ルール データ分類レポート	

表 16-1. すべての管理者が使用可能なレポート：概要

管理者	レポートのカテゴリ		
	管理者レポート	RiskFort レポート	ケース管理レポート
Organization Administrator	アクティビティ レポート	リスク評価詳細アクティビティ レポート	不正行為統計レポート
	管理者アクティビティ レポート	リスクアドバイス サマリ レポート	
	ユーザ アクティビティ レポート	トラステッド IP/ アグリゲータ レポート	
	組織レポート	拒否 IP アドレス レポート	
		拒否国レポート	
		例外ユーザ レポート	
		アドオン ルール レポート	
		ルール データ レポート	
		ルール データ分類レポート	
User Administrator	アクティビティ レポート	リスク評価詳細アクティビティ レポート	不正行為統計レポート
	管理者アクティビティ レポート	リスクアドバイス サマリ レポート	
	ユーザ アクティビティ レポート	例外ユーザ レポート	
不正行為アナリスト	アクティビティ レポート	--	不正行為統計レポート
テクニカル サポート 担当者	アクティビティ レポート	例外ユーザ レポート	--

以下のセクションでは、これらのレポートについて詳しく説明します。

管理者レポート

システムで使用可能なすべての管理者レポートには、以下のものが含まれます。

- アクティビティ レポート
- 管理者アクティビティ レポート
- ユーザ アクティビティ レポート
- 組織レポート

アクティビティ レポート

このレポートには、現在ログインし、これまでに実行されたアクションと操作に関連するレポートを生成している管理者によって実行されたすべての操作がリスト表示されます。

ログインした管理者は[管理者アクティビティ レポート](#)を使用して自分のアクティビティを表示できますが、このレポートは以下の理由で個別に提供されます。

- 管理者は、自分が所属している組織のスコープを担当していない場合があります。たとえば、管理者 *Alan* は *MyOrg* という組織に属しますが、*ScopeOrg* というスコープを担当しています。この場合、*Alan* は必要なスコープを担当していないため、管理者アクティビティ レポートを使用して自分のアクティビティを表示することができません。
- 管理者アクティビティ レポートでは、ユーザ名が指定されたユーザ名に完全または部分的に一致するすべての管理者のアクティビティをリスト表示します。そのため、管理者は、自分のアクティビティ レポートを取得するために、レポートのすべてのページを検索する必要があります。アクティビティ レポートではログインした管理者のみのアクティビティを表示するため、この問題が解決されます。

図 16-1 に、アクティビティ レポートのサンプルを示します。

図 16-1 アクティビティ レポート

My Activity Report

This report displays the activity of the logged in administrator.

ExportNew Report

Date Range:

From: 01/01/2009

To: 01/08/2010

Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID	
01/08/2010 13:53:45	MASTERADMIN	MASTERADMIN	1043	Admin Login	Success	N/A	N/A	N/A	Admin Console	DFCC647A7DEFB2F6AE6A0D1D6579D4...	1	
01/08/2010 13:23:44	MASTERADMIN	MASTERADMIN	1015	Admin Logout	Success	N/A	N/A	N/A	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1	
01/08/2010 13:23:38	MASTERADMIN	MASTERADMIN	1014	Create Administrator	Success	N/A	GA1	DEFAULT ORGANIZATION	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1	
01/08/2010 13:22:16	MASTERADMIN	MASTERADMIN	1011	Admin Login	Success	N/A	N/A	N/A	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1	
01/08/2010 13:22:15	MASTERADMIN	MASTERADMIN	1009	Admin Login	Success	N/A	N/A	N/A	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1	
01/08/2010 12:40:06	MASTERADMIN	MASTERADMIN	11534	Session Expired	Success	N/A	N/A	N/A	Admin Console	A99C24A68603B104BC7DAB41F3991D...	1	
01/08/2010 11:35:29	MASTERADMIN	MASTERADMIN	11525	Admin Login	Success	N/A	N/A	N/A	Admin Console	A99C24A68603B104BC7DAB41F3991D...	1	
01/07/2010 17:27:47	MASTERADMIN	MASTERADMIN	11521	Session Expired	Success	N/A	N/A	N/A	Admin Console	837C41D0947055D7494FDC6E2214B...	1	
01/07/2010 17:07:48	MASTERADMIN	MASTERADMIN	33	Admin Logout	Success	N/A	N/A	N/A	Admin Console	C3374580545B2C30284198F2DD0FC8...	1	
01/07/2010 17:06:00	MASTERADMIN	MASTERADMIN	24	Admin Login	Success	N/A	N/A	N/A	Admin Console	C3374580545B2C30284198F2DD0FC8...	1	

表 16-2 では、このレポートのフィールドについて説明します。

表 16-2. アクティビティ レポートのフィールド

レポート フィールド	説明
[Date]	アクティビティの日時。
[Administrator Name]	レポートを生成している管理者の名前。
[Administrator Organization]	管理者が属する組織の名前。
[Transaction ID]	管理者によって実行された各アクティビティ用に生成された一意の ID。
[Event Type]	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）。
[Status]	実行したアクションのステータス。 • [Success] - アクションが正常に完了した場合。 • [Failure] - 管理者がアクションに失敗した場合。
[Reason]	操作が失敗した理由。
[Target User]	属性が管理者によって管理されているユーザの名前。

表 16-2. アクティビティ レポートのフィールド

レポート フィールド	説明
[Target Organization]	アクティビティが実行された組織。
[Component]	タスクを実行するために使用されたリソース。この列の値は以下のいずれかです。 • [Administration Console] • [WebFort]
[Session ID]	管理者がログインしている Administration Console のセッション識別子。
[Instance ID]	アプリケーションの複数のインスタンスが実行されている場合、Administration Console アプリケーション インスタンスの一意の識別子。

管理者アクティビティ レポート

このレポートでは、指定された管理者、または指定された組織に所属する管理者によって実行されたすべてのアクティビティをリスト表示します（その管理者がこのレポートを生成する管理者のスコープを担当している場合）。

このレポートを使用すると、特定の管理者のアクティビティをフィルタリングしたり、1 つまたは複数の組織のすべての管理者のアクティビティを表示できます。このレポートには、管理者のログインおよびログアウトのタイム スタンプ、組織検索、管理者アカウントの更新、および関連する詳細などの情報が含まれます。

図 16-2 に、管理者アクティビティ監査レポートのサンプルを示します。

図 16-2 管理者アクティビティ レポート

Administrator Activity Report

This report displays the administrative activities performed using the Arcot Administration Console.

Export

New Report

Date Range:

From: 01/01/2009

To: 01/08/2010

◀◀◀ 1 2 3 4 5 6 ▶▶▶

Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID
01/08/2010 13:54:20	MASTERADMIN	MASTERADMIN	1045	View Report: My Activity Repor...	Success	N/A	N/A	MASTERADMIN	Admin Console	DFCC647A7DEFB2F6AE6A0D1D6579D4...	1
01/08/2010 13:53:45	MASTERADMIN	MASTERADMIN	1043	Admin Login	Success	N/A	N/A	N/A	Admin Console	DFCC647A7DEFB2F6AE6A0D1D6579D4...	1
01/08/2010 13:53:35	GA1	DEFAULT ORGANIZATION	1041	Admin Logout	Success	N/A	N/A	N/A	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:41:23	GA1	DEFAULT ORGANIZATION	1039	View Report: Administrator Act...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:40:10	GA1	DEFAULT ORGANIZATION	1037	View Report: My Activity Repor...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:35:13	GA1	DEFAULT ORGANIZATION	1035	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:24:17	GA1	DEFAULT ORGANIZATION	1018	Admin Login	Success	N/A	N/A	N/A	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:24:13	GA1	DEFAULT ORGANIZATION	1017	Update Password	Success	N/A	N/A	N/A	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:23:44	MASTERADMIN	MASTERADMIN	1015	Admin Logout	Success	N/A	N/A	N/A	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1
01/08/2010 13:23:38	MASTERADMIN	MASTERADMIN	1014	Create Administrator	Success	N/A	GA1	DEFAULT ORGANIZATION	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1

◀◀◀ 1 2 3 4 5 6 ▶▶▶

このレポートのフィールドはアクティビティ レポートのフィールドと同じです。フィールドの詳細については、表 16-2 を参照してください。

ユーザ アクティビティ レポート

このレポートは、ユーザ属性に対して実行されたすべてのアクティビティをリスト表示します。これには、ユーザの作成、ユーザの更新、PAM の設定、ユーザの削除、ユーザ ステータスの更新、およびユーザの認証が含まれます。レポートには、ユーザ名、ユーザのステータス、実行された操作タイプなどの詳細が含まれます。また、ユーザ システムの IP アドレスも含まれます。

このレポートを生成するには、以下の項目を指定する必要があります。

- 日付範囲。
- (オプション) ユーザ名。
- 必要な組織名。

図 16-3 に、ユーザ アクティビティ レポートのサンプルを示します。

図 16-3 ユーザ アクティビティ レポート

User Activity Report									
This report displays the user activity in the system.									
Events to Display: All Events Export New Report									
Date Range: From: 01/08/2009 To: 01/08/2010									
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20									
Date	User Name	Event Type	Organization	Status	Transaction ID	Reason	Client IP Address	Caller ID	
01/08/2010 14:01:44	UA1	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:D6BD2EF7C0F7873...	N/A	127.0.0.1	N/A	
01/08/2010 14:01:12	OA1	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:D6BD2EF7C0F7873...	N/A	127.0.0.1	N/A	
01/08/2010 13:25:08	GA1	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:D6BD2EF7C0F7873...	N/A	127.0.0.1	N/A	
01/07/2010 16:42:30	961753102595826	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A	
01/07/2010 16:38:46	871311873732775	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A	
01/07/2010 16:38:42	395723421848553	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A	
01/07/2010 16:37:14	877169446285705	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A	
01/07/2010 16:35:56	194574794370722	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A	
01/07/2010 16:34:38	848770808795672	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A	
01/07/2010 16:30:16	207713997468285	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A	
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20									

表 16-3 では、このレポートのフィールドについて説明します。

表 16-3. ユーザ アクティビティ レポートのフィールド

レポート フィールド	説明
[Date]	アクティビティの日時。
[User Name]	アクティビティの実行対象のユーザ名。
[Event Type]	管理者によって実行されたアクティビティのタイプ（ユーザの作成、更新、および削除など）。
[Organization]	ユーザが所属している組織名。
[Status]	操作のステータス。 • [Success] - 操作が正常に完了した場合。 • [Failure] - ユーザが操作の実行に失敗した場合。
[Transaction ID]	ユーザによって実行された各アクティビティ用に生成された一意の ID。
[Reason]	操作が失敗した理由。

表 16-3. ユーザ アクティビティ レポートのフィールド

レポート フィールド	説明
[Client IP Address]	エンド ユーザ システムの IP アドレス。
[Caller ID]	アプリケーションの呼び出し元によって設定された一意の識別子。 注：呼び出し元のアプリケーションが値を設定しなかった場合は、[Caller ID] が空白である可能性があります。

組織レポート

このレポートは、指定された組織で実行されたすべての操作の詳細を提供します。このレポートには、ルールや設定に関係なく、管理者の権限の範囲内にある組織のアクティビティがすべて表示されます。

このレポートを生成するには、以下の項目を指定する必要があります。

- 日付範囲。
- 組織名（必要な場合）。

図 16-4 に、組織レポートのサンプルを示します。

図 16-4 組織レポート

Organization Report This report displays the activity of the administrators on the selected organization.											
ExportNew Report											
Date Range:From: 01/08/2009To: 01/08/2010											
◀◀ 1 2 ▶▶											
Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID
01/08/2010 16:13:52	OA1	DEFAULT ORGANIZATION	1090	View Report: Organization Repo...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	507AB71B528834EC05F28EF6E19DFD...	1
01/08/2010 14:37:55	GA1	DEFAULT ORGANIZATION	1070	View Report: View Risk Advice ...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:37:55	GA1	DEFAULT ORGANIZATION	1068	View Report: View Risk Advice ...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:24:21	GA1	DEFAULT ORGANIZATION	1066	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:05:36	GA1	DEFAULT ORGANIZATION	1058	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:00:14	GA1	DEFAULT ORGANIZATION	1057	Create Administrator	Success	N/A	UA1	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 13:59:43	GA1	DEFAULT ORGANIZATION	1055	Create Administrator	Success	N/A	OA1	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 13:41:23	GA1	DEFAULT ORGANIZATION	1039	View Report: Administrator Act...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:40:10	GA1	DEFAULT ORGANIZATION	1037	View Report: My Activity Repor...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:35:13	GA1	DEFAULT ORGANIZATION	1035	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
◀◀ 1 2 ▶▶											

表 16-4 では、このレポートのフィールドについて説明します。

表 16-4. 組織レポートのフィールド

レポート フィールド	説明
[Date]	アクティビティの日時。
[Administrator Name]	アクティビティを実行した管理者の名前。
[Administrator Organization]	管理者が属する組織の名前。
[Transaction ID]	管理者によって実行されたすべてのアクティビティ用に生成された一意の識別子。

表 16-4. 組織レポートのフィールド

レポート フィールド	説明
[Event Type]	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）。
[Status]	実行したアクションのステータス。 • [Success] - アクションが正常に完了した場合。 • [Failure] - 管理者がアクションに失敗した場合。
[Reason]	操作が失敗した理由。
[Target User]	属性が管理者によって管理されているユーザの名前。
[Target Organization]	ユーザが所属している組織。
[Component]	タスクを実行するために使用されたリソース。この列の値は以下のいずれかです。 • Administration Console (Admin Console) • RiskFort (RiskFortResourcePack)
[Session ID]	管理者がログインした Administration Console のセッション識別子。
[Instance ID]	アプリケーションの複数のインスタンスが実行されている場合、Administration Console アプリケーション インスタンスの一意の識別子。

RiskFort レポート

システムで使用可能な RiskFort 設定関連のすべてのレポートには、以下のレポートがあります。

- [リスク評価詳細アクティビティ レポート](#)
- [リスク アドバイス サマリ レポート](#)
- [トラステッド IP/ アグリゲータ レポート](#)
- [拒否 IP アドレス レポート](#)
- [拒否国レポート](#)
- [例外ユーザ レポート](#)
- [アドオン ルール レポート](#)
- [ルール データ レポート](#)
- [ルール データ分類レポート](#)

リスク評価詳細アクティビティ レポート

このレポートは、RiskFort サーバによって実行されたすべてのトランザクションを表示します。

このレポートを生成するには、以下の項目を指定する必要があります。

- 日付範囲。
- 組織名（必要な場合）。
- ユーザ名（必要な場合）。

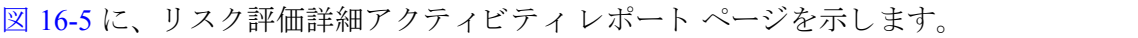
 16-5 に、リスク評価詳細アクティビティ レポート ページを示します。

図 16-5 リスク評価詳細アクティビティ レポート

Risk Evaluation Detail Activity Report

This report displays the risk evaluation details for all user transactions that matched the criteria that you specified.

Export

New Report

Date Range:

From: 01/03/2009

To: 01/03/2010

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

Date	User Name	Organization	Event Type	Event Status	Risk Score	Risk Advice	Matched Rule	Secondary Authentication Result	RuleSet	Action	Caller ID	Transaction ID	Session ID	Instance ID	Country	Client IP Address	HTTP DeviceID	Flash DeviceID	Outgoing DeviceID	Exception User	Negative IP Address	Negative Country	Trusted IP	Trusted Aggregator	User Home	Machine Fingerprint Match	User Velocity	Device Velocity	Zone Hopping	Evaluation Callout	User Associated with Device and Device MFP	Device Matched but User Not Associated with Device MFP	User Not Associated with Device and Device MFP	Add On Rules Result	
01/07/2009 18:44:17	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	635	1635	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:43:59	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	95	Increase Authentication	DEVICE_VELOCITY	Not Available	DEFAULT	LOOEN	NA	634	1634	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	Yes	No	NA	Yes	No	No	No	NA
01/07/2009 18:43:52	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	95	Increase Authentication	DEVICE_VELOCITY	Not Available	DEFAULT	LOOEN	NA	633	1633	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	Yes	No	NA	Yes	No	No	No	NA
01/07/2009 18:43:50	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	632	1632	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	631	1631	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:58	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	630	1630	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:58	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	629	1629	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:58	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	628	1628	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:52	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	627	1627	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:41:40	BB1753102595026	DEFAULTORG	Evaluate Risk	Success	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV	Not Available	DEFAULT	LOOEN	NA	626	1626	1	NA	101.150.174	NA	NA	rsz2tqg2innh55u4wCh83imv2Bo	No	No	No	No	No	Yes	Yes	No	No	No	NA	Yes	No	No	No	NA

表 16-5 に、リスク評価詳細アクティビティに含まれる情報をリスト表示します。

表 16-5. リスク評価詳細アクティビティ レポートのフィールド

フィールド	説明
[Date]	ユーザのリスク評価が実行されたときのタイム スタンプ。
[User Name]	リスク評価アクティビティを実行したユーザの一意の ID。
[Organization]	ユーザが所属している組織。

表 16-5. リスク評価詳細アクティビティ レポートのフィールド (continued)

フィールド	説明
[Event Type]	RiskFort サーバによって実行されたリスク評価アクティビティのタイプ。これには以下のアクティビティが含まれます。 • リスクの評価 • 属性の更新 • 関連付けの作成 • 関連付けの削除
[Event Status]	実行されたイベント アクションのステータス。以下のステータスを使用できます。 • [Success] - RiskFort はリスク評価アクティビティを正常に実行することができました。 • [Failure] - RiskFort はリスク評価アクティビティを正常に実行することができませんでした。
[Risk Score]	指定されたトランザクションのために生成されたスコア。
[Risk Advice]	生成されたスコアに応じて RiskFort が生成したアドバイス。次のアドバイスを 사용할 수 있습니다。 • 許可 • 拒否 • アラート • 追加認証
[Matched Rule]	一致したルール。
[Secondary Authentication Result]	RiskFort によって生成されたリスク アドバイスが「追加認証」だった場合、アプリケーションによって RiskFort に返されたセカンダリ認証の結果。
[Ruleset]	ユーザが所属する組織用に設定されたルール セット。
[Action]	現在のイベントで実行された対応するアクション（ログインなど）。
[Caller ID]	呼び出し元のアプリケーションによって RiskFort API に渡された一意の識別子。 注：呼び出し元のアプリケーションが値を設定しなかった場合は、[Caller ID] が空白である可能性があります。
[Transaction ID]	実行された各アクティビティに対して RiskFort サーバが提供する内部的な一意の ID。
[Session ID]	管理者がログインしている Administration Console のセッション識別子。
[Instance ID]	RiskFort サーバのすべてのインスタンスの一意の識別子（インストールに複数のインスタンスが展開されている場合）。
[Country]	トランザクションが発生した国。 注：これは [Client IP Address] の値から導出されます。

表 16-5. リスク評価詳細アクティビティ レポートのフィールド (continued)

フィールド	説明
[Client IP Address]	エンド ユーザ システムの IP アドレス。
[HTTP DeviceID]	ユーザ エンド システムで HTTP デバイス ID が見つかったかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Flash DeviceID]	ユーザのエンド システムでフラッシュ デバイス ID が見つかったかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Outgoing DeviceID]	エンド ユーザ システムからの初めてのトランザクションである場合、トランザクションの実行中に生成された対応するデバイス ID。
[Exception User]	ユーザが例外ユーザ リストに存在するかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Negative IP Address]	拒否 IP ルールが適用されたかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Negative Country]	拒否国ルールが適用されたかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Trusted IP]	トラステッド IP ルールが適用されたかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Trusted Aggregator]	トラステッド アグリゲータ IP ルールが適用されたかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[User Known]	既知のユーザ ルール (ユーザが RiskFort に登録されているかどうか) が適用されたかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Machine FingerPrint Match]	ユーザのマシンの FingerPrint チェックに合格したかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[User Velocity]	ユーザのユーザ頻度チェックに合格したかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。

表 16-5. リスク評価詳細アクティビティ レポートのフィールド (continued)

フィールド	説明
[Device Velocity]	ユーザのデバイス頻度チェックに合格したかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Zone Hopping]	ユーザのゾーン ホッピングのチェックに合格したかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Evaluation Callout]	評価コールアウトが設定されているかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[User Associated with Device and Device-MFP Matched]	「ユーザとデバイスが関連付けられ、かつデバイスと MFP が一致」ルールが設定されているかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Device-MFP Matched but User Not Associated with Device]	「デバイスと MFP が一致し、かつユーザとデバイスが関連付けられていない」ルールが設定されているかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[User Associated with Device but Device-MFP Does Not Match]	「ユーザとデバイスが関連付けられ、かつデバイスと MFP が不一致」ルールが設定されているかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[User Not Associated with Device and Device-MFP Does Not Match]	「ユーザとデバイスが関連付けられておらず、かつデバイスと MFP が不一致」ルールが設定されているかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。
[Add-On Rules Result]	アドオン ルールが設定されているかどうか。 これが適用された場合、結果 ([Yes] または [No]) は、ルールが一致を返したかどうかを示します。

リスク アドバイス サマリ レポート

アドバイス サマリ レポートでは、指定された期間に RiskFort が返したアドバイスの全体のサマリを提供します (表 16-6 を参照)。また、別の表に、すべてのセカンダリ認証結果の詳しい内容を示します (表 16-7 を参照)。



注： RiskFort は、ユーザが試行したトランザクションごとにリスク アドバイスを返します。RiskFort が送信したアドバイスに基づき、アプリケーションは、ユーザがトランザクションを完了することを許可したり、そのトランザクションを拒否したりすることができます。

このレポートを生成するには、以下の項目を指定する必要があります。

- 日付範囲。
- 組織名 (必要な場合)。

図 16-6 にリスク アドバイス サマリ レポート ページを示します。

図 16-6 リスク アドバイス サマリ レポート

Risk Advice Summary Report				
<i>This report displays the summary of all Risk Advices generated by RiskFort for the criteria that you specified.</i>				
Risk Advice		Total		
Allow		170		
Increase Authentication		101		
Alert		67		
Deny		30		
Total		368		

Secondary Authentication Results Summary				
<i>This report displays the summary of all Secondary Authentication results that your application returned to RiskFort, if the original Risk Advice was "Increase Authentication".</i>				
Result	Success	Failure	Unknown	Total
Count	65	4	32	101
%	64%	4%	32%	100%

表 16-6 に、RiskFort アドバイス サマリ レポートに含まれる情報をリスト表示します。

表 16-6. リスク アドバイス サマリ レポートのフィールド

フィールド	説明
[Risk Advice]	トランザクションごとに RiskFort から与えられたアドバイス。 • [Allow] - アプリケーションは、トランザクションの続行を許可する必要があります。 • [Increase Authentication] - アプリケーションは、トランザクションをさらに進める前に、2 次認証または追加の認証（秘密の質問の入力や OTP 認証など）を実行する必要があります。 • [Alert] - アプリケーションは、RiskFort データベースにユーザを作成する必要があります。 • [Deny] - アプリケーションはトランザクションのこれ以上の進行を拒否する必要があります。
[Total]	生成されたリスク アドバイスの総数。

表 16-7 に、2 次認証結果サマリ レポートに含まれる情報をリスト表示します。

表 16-7. 2 次認証結果サマリのフィールド

フィールド	説明
[Result]	RiskFort が [Increase Authentication] アドバイスを生成し、アプリケーションがユーザに追加認証を要求したときの結果のサマリ。
[Success]	成功したすべての 2 次認証の試行回数。
[Failure]	ユーザによる、失敗したすべての 2 次認証の試行回数。
[Unknown]	2 次認証の結果がアプリケーションから RiskFort に転送されなかった場合のすべてのインスタンス数。
[Total]	生成された結果に関係なく、実行された 2 次認証の総数。

トラステッド IP/ アグリゲータ レポート

このレポートは、システムに設定されているすべてのトラステッド アグリゲータのリストまたはトラステッド IP アドレスの範囲を表示します。このレポートは、提示データおよびアクティブ データの両方で提供されます。

- [トラステッド IP レポート](#)
- [トラステッド アグリゲータ レポート](#)

トラステッド IP レポート

このレポートを生成するには、以下のオプションを指定します。

- 必要な組織名。
- 必要なルール セット名。
- ステータス。ACTIVE または PROPOSED のどちらかです。
- [Trusted IP/Trusted Aggregator] フィールドからの [Trusted IP] オプション。

図 16-7 に、トラステッド IP レポートのサンプルを示します。

図 16-7 トラステッド IP レポート

Trusted IP/Aggregator Report			
This report displays the details for the Trusted IPs or Aggregators based on the criteria that you specified.			
			Export New Report
Start IP Address	End IP Address	Mask	Date Added
5.0.0.1	5.0.0.10	N/A	12/31/2007 18:30:00
5.1.7.7	N/A	255.255.255.0	12/31/2007 18:30:00
71.0.0.10	71.0.0.20	N/A	12/31/2007 18:30:00
203.203.205.0	N/A	255.255.0.255	12/31/2007 18:30:00
72.0.0.10	72.0.0.10	N/A	12/31/2007 18:30:00
203.203.203.203	203.203.203.204	N/A	12/31/2007 18:30:00
203.203.204.0	203.203.204.1	N/A	12/31/2007 18:30:00
71.1.0.0	N/A	255.255.255.0	12/31/2007 18:30:00

表 16-8 では、トラステッド IP レポートに表示される列について説明します。

表 16-8. トラステッド IP アドレス レポートのフィールド

フィールド	説明
[Start IP Address]	トラステッド アグリゲータの IP アドレス。
[End IP Address]	最後のアドレス (IP アドレス範囲を指定している場合)。
[Mask]	トラステッド アグリゲータの IP アドレスのサブネット マスク値。
[Date Added]	最初のアグリゲータ デバイス ID が作成された日付。

トラステッド アグリゲータ レポート

このレポートを生成するには、以下のオプションを指定します。

- 必要な組織名。
- 必要なルール セット名。

- ステータス。ACTIVE または PROPOSED のどちらかです。
- [Trusted IP/Trusted Aggregator] フィールドからの [Trusted Aggregator] オプション。

図 16-8 に、トラステッド アグリゲータ レポートのサンプルを示します。

図 16-8 トラステッド アグリゲータ レポート

Trusted IP/Aggregator Report										
This report displays the details for the Trusted IPs or Aggregators based on the criteria that you specified.										
ExportNew Report										
Aggregator Name	Start IP Address	End IP Address	Mask	Date Added	Aggregator ID 1	Date Created	Aggregator ID 2	Date Created	Aggregator ID 3	Date Created
AGG	109.56.87.123	109.57.8.23	N/A	01/08/2010 09:42:14	Pj42w6E3oXRfbVQcUzdJH2fZYus+tt...	01/07/2010 13:15:28	N/A	N/A	N/A	N/A
AGG	217.198.32.175	N/A	255.255.225.242	01/08/2010 09:45:01	Pj42w6E3oXRfbVQcUzdJH2fZYus+tt...	01/07/2010 13:15:28	N/A	N/A	N/A	N/A

表 16-9 に、RiskFort のトラステッド アグリゲータ レポートに含まれる情報をリスト表示します。

表 16-9. トラステッド アグリゲータ レポートのフィールド

フィールド	説明
[Aggregator Name]	アグリゲータの名前。
[Start IP Address]	トラステッド アグリゲータの IP アドレス。
[End IP Address]	最後のアドレス（IP アドレス範囲を指定している場合）。
[Mask]	トラステッド アグリゲータの IP アドレスのサブネット マスク値。
[Date Added]	2 番目のアグリゲータ デバイス ID が作成された日付。
[Aggregator ID 1]	トラステッド アグリゲータの一意的デバイス ID。
[Date Created]	最初のアグリゲータ デバイス ID が作成された日付。
[Aggregator ID 2]	アグリゲータ用に生成された 2 番目のデバイス ID。
[Aggregator ID 3]	アグリゲータ用に生成された 3 番目のデバイス ID。
[Date Created]	3 番目のアグリゲータ デバイス ID が作成された日付。

拒否 IP アドレス レポート

このレポートは、システムに設定されているすべての拒否 IP アドレスおよび範囲を表示します。このレポートは、提示データおよびアクティブ データの両方で提供されます。(拒否 IP リストの詳細については、[7-95 ページの「拒否 IP アドレスの設定」](#)を参照してください)。

このレポートを生成するには、以下のオプションを指定します。

- 必要な**組織名**。
- 必要な**ルール セット名**。
- ステータス。ACTIVE または **PROPOSED** のどちらかです。

[図 16-9](#) に、拒否 IP アドレス レポート ページを示します。

図 16-9 拒否 IP アドレス レポート

Negative IP Address Report				
This report displays the details for the Negative IP address ranges that matched the criteria that you specified.				
				Export New Report
Start IP Address	End IP Address	Mask	Information Source	Date Added
66.178.80.48	66.178.80.55	N/A	QUOVA	01/08/2010 09:56:34
85.236.136.15	85.236.236.79	N/A	QUOVA	01/08/2010 09:57:39
195.112.196.56	195.112.196.59	N/A	ARCOT	01/08/2010 09:58:23
198.165.197.192	198.165.197.223	N/A	ANONYMOUS PROXY	01/08/2010 09:59:01

[表 16-10](#) に、拒否 IP アドレス レポートに含まれる情報をリスト表示します。

表 16-10. 拒否 IP アドレス レポートのフィールド

フィールド	説明
[Start IP Address]	悪意のあるユーザの IP アドレス。
[End IP Address]	最後のアドレス (IP アドレス範囲を指定している場合)。
[Mask]	悪意のあるユーザの IP アドレスのサブネット マスク値。
[Information Source]	拒否 IP 範囲を提供したベンダー。
[Date Added]	エントリが作成された日付。

拒否国レポート

このレポートは、システムに設定されているすべての拒否国のリストを表示します。このレポートは、提示データとアクティブ データの両方で提供されます（拒否国リストの詳細については、[7-102 ページの「\[Negative Country List\] の設定」](#)を参照してください）。

このレポートを生成するには、以下のオプションを指定します。

- 必要な**組織名**。
- 必要な**ルール セット名**。
- **ステータス**。ACTIVE または **PROPOSED** のどちらかです。

[図 16-10](#) に、拒否国レポート ページを示します。

図 16-10 拒否国レポート

Negative Country Report		
This report displays the details for the Negative countries that matched the criteria that you specified.		
ExportNew Report		
ISO Country Code	Country	Date Added
AF	AFGHANISTAN	01/08/2010 10:07:24
BD	BANGLADESH	01/08/2010 10:07:24
CN	CHINA	01/08/2010 10:07:24
IR	IRAN	01/08/2010 10:07:24
IQ	IRAQ	01/08/2010 10:07:24
KE	KENYA	01/08/2010 10:07:24
LY	LIBYA	01/08/2010 10:07:24
PK	PAKISTAN	01/08/2010 10:07:24

[表 16-11](#) では、拒否国レポートに表示される情報について説明します。

表 16-11. 拒否国レポートのフィールド

フィールド	説明
[ISO Country Code]	ISO によって各国に割り当てられたコード。
[Country]	国の名前。
[Date Added]	国がリストに追加された日付。

例外ユーザ レポート

このレポートは、RiskFort システムに設定されているすべての例外ユーザのリストを表示します。

このレポートを生成するには、以下の項目を指定する必要があります。

- 日付範囲。
- 必要な組織名。
- ユーザ名。

図 16-11 に、RiskFort 例外ユーザ レポート ページを示します。

図 16-11 例外ユーザ レポート

Exception User Report

This report displays the details for the Exception users that matched the criteria that you specified.

Export

New Report

Date Range:

From: 01/01/2010

To: 01/08/2010

Start Date	End Date	User	Reason	Organization
01/07/2010 15:58:09	01/09/2010 15:58:09	EXUSER1	testing	DEFAULTORG
12/29/2009 15:58:09	01/07/2010 15:58:09	EXUSER2	testing	DEFAULTORG
01/03/2010 15:58:09	01/13/2010 15:58:09	EXUSER4	testing	DEFAULTORG
01/08/2010 15:58:09	01/10/2010 15:58:09	EXUSER5	testing	DEFAULTORG

表 16-12 に、RiskFort 例外ユーザ レポートに含まれる情報をリスト表示します。

表 16-12. RiskFort 例外ユーザ レポートのフィールド

フィールド	説明
[Start Date]	ユーザがシステムで例外ユーザと見なされるようになった日時。
[End Date]	ユーザがシステムで例外ユーザではなくなる日時。
[User]	一意のユーザ名。
[Reason]	システムでそのユーザを例外ユーザにした理由。
[Organization]	管理者が属する組織。

アドオン ルール レポート

アドオン ルール レポートは、指定された組織に展開されたすべてのアドオン ルールの全体的なサマリを提供します（アドオン ルールの詳細については、[12-188 ページの「アドオン ルールの操作」](#)を参照してください）。

このレポートを生成するには、以下の項目を指定する必要があります。

- 必要な組織名。
- 必要なルール セット名。
- ターゲット情報のステータス。

図 16-12 に、アドオン ルール レポート ページを示します。

図 16-12 アドオン ルール レポート

Add-On Rules Report						
This report displays the overall summary of the deployed Add-On rules that matched the criteria that you specified.						
					Export	New Report
Rule Name	Enabled	Rule Mnemonic	Library Name	Rule Type	Parameters	Description
High Amount Check	NO	HIGHAMTCHK	rfulenumericcomparison_ex	AMOUNT_CHECK	THRESHOLD=500:840]	This rule checks for transaction amounts that exceed \$500.
High Device Velocity from Unexpected Locations	NO	HIGHDEVICEVELOCITYCHECK	rfulecombination	COMBINATION_RULE	EXP= DEVICEVELOCITY AND NOT (COUNTRY IN \$\$SAFE_COUNTRIES)	This rule checks for transactions with high Device Velocity from unexpected locations.

表 16-13 に、アドオン ルール レポートに含まれる情報をリスト表示します。

表 16-13. アドオン ルール レポートのフィールド

フィールド	説明
[Rule Name]	アドオン ルールの名前。
[Enabled]	レポートの実行時点でルールが使用されているかどうか。
[Rule Mnemonic]	アドオン ルールの短縮名。
[Library Name]	ルールに関連付けられた .dll または .so ファイルの名前。
[Rule Type]	Master Administrator によって作成されたアドオン ルールのタイプ。
[Parameters]	ルールが各トランザクションに対してリアル タイムでチェックする必要があるデフォルト値。
[Description]	後で参照するためのルールの詳細な説明。

ルール データ レポート

ルール データ レポートは、組織のためにアップロードされた、選択済みの簡易リストの要約データを表示します（リスト データ、およびアドオンルールで使用するリストをアップロードする方法の詳細については、[12-188 ページの「アドオン ルールの操作」](#)を参照してください）。

このレポートを生成するには、以下の項目を指定する必要があります。

- 必要な**組織名**。
- 必要な**ルール セット名**。
- ターゲット情報の**ステータス**。
- アップロードされた**データ セット名**（またはリストの名前）。

図 16-13 に、[SAFE_COUNTRUIES](#) と呼ばれるアップロードされたリスト用のルール データ レポート ページを示します。

図 16-13 ルール データ レポート

Rules Data Report	
This report provides the list data.	
ExportNew Report	
Data	Date Added
India	03/22/2010 12:10:05
US	03/22/2010 12:10:05
Denmark	03/22/2010 12:10:05
Iceland	03/22/2010 12:10:05
Norway	03/22/2010 12:10:05
Sweden	03/22/2010 12:10:05
Canada	03/22/2010 12:10:05
Germany	03/22/2010 12:10:05
Italy	03/22/2010 12:10:05

表 16-14 に、ルール データ レポートに含まれる情報をリスト表示します。

表 16-14. ルール データ レポートのフィールド

フィールド	説明
[Data]	リスト内の対応するエントリ（またはデータ値）。
[Date Added]	対応するエントリが追加された日付。

ルール データ分類レポート

ルール データ分類レポートは、組織のためにアップロードされた、選択済みのマッピング リストの要約データを表示します。(リスト データ、およびアドオン ルールで使用するリストをアップロードする方法の詳細については、[12-188 ページの「アドオン ルールの操作」](#)を参照してください)。

このレポートを生成するには、以下の項目を指定する必要があります。

- 必要な**組織名**。
- 必要な**ルール セット名**。
- ターゲット情報の**ステータス**。
- アップロードされた**データ セット名** (またはリストの名前)。

 **図 16-14** に、**MERCHANT_CATEGORY_MAPPING** と呼ばれるアップロードされたリスト用のルール データ分類レポート ページを示します。

図 16-14 ルール データ分類レポート

Rules Data Classification Report
This report provides data classification.

ExportNew Report

123▶▶▶

Param Value	Category	Date Added
800florals	Flower Delivery	03/23/2010 06:16:40
AdultReviews	Porn	03/23/2010 06:16:41
Amazon	Online Shopping	03/23/2010 06:16:41
American Airlines	Airline	03/23/2010 06:16:41
BEST-BUY-DEAL	Online Shopping	03/23/2010 06:16:41
British Airways	Airline	03/23/2010 06:16:41
Casinogamblingweb	Gambling	03/23/2010 06:16:41
Cliphunter	Porn	03/23/2010 06:16:41
Costco	Online Shopping	03/23/2010 06:16:41
eBay	Online Shopping	03/23/2010 06:16:41

123▶▶▶

表 16-15 に、ルール データ分類レポートに含まれる情報をリスト表示します。

表 16-15. ルール データ分類レポートのフィールド

フィールド	説明
[Parameter Value]	リスト内の対応するエントリ (またはデータ値)。
[Category]	エントリが所属している対応するカテゴリ (管理者が定義)。
[Date Added]	エントリが追加された日付。

ケース管理レポート

詐欺統計レポートは、システムで使用可能な唯一のケース管理関連のレポートです。このレポートの詳細については、[第 15 章の「ケースの管理」の 15-272 ページの「不正行為統計レポートの生成」](#)を参照してください。

レポートの生成

このセクションでは、以下の内容について説明します。

- [レポートを生成する場合の注意事項](#)
- [レポートの生成](#)

レポートを生成する場合の注意事項

レポートを生成する場合は、以下の点に注意してください。

- 管理者は、自分のスコープの組織のレポートのみを生成できます。
- 管理者は、自分の下位またはピアのレポートを生成できます。

たとえば Organization Administrator (OA) は、OA と User Administrator (UA) のレポートを生成できます。

- カスタム ロールを使用して作成された管理者ロールの場合、派生した管理者ロールは親と同じレベルに属します。

たとえば、GA から *MyGlobalAdmin* という管理者を作成した場合、*MyGlobalAdmin* に OA または UA よりも少ない数の権限を割り当てたとしても、*MyGlobalAdmin* は GA であると見なされます。

- Oracle データベースを使用している場合は、[UNLIMITED TABLESPACE](#) 権限が有効であることを確認します。

レポートの生成

管理者固有または RiskFort 固有のレポートを生成する方法

1. 適切なクレデンシャル (MA、GA、OA、または UA) でログインしていることを確認します。
2. メイン メニューの **[Reports]** タブをアクティブにします。

3. 次の手順に従います。
 - 管理者アクティビティ レポートを生成する場合は、[**Administrator Reports**] サブメニューをクリックします。
 - RiskFort 固有のレポートを生成する場合は、[**RiskFort Reports**] サブメニューをクリックします。レポート タイプの対応するリンクが左側のタスク パネルに表示されます。
4. 生成するレポートに応じて、左側のサブメニューから必要なリンクをクリックします。
5. 選択に応じて以下の条件を 1 つ以上指定し、レポートを表示します。
 - ドロップダウン リストの [**Date Range**].
 - または
 - 事前定義済みの日付範囲の [**From**] と [**To**] のフィールド。
6. レポートによっては、さらに以下の情報を指定する必要がある場合があります。
 - レポートに含めるデータを持つ、必要な組織の**組織名**。
 - **ユーザ名**または**管理者名**（生成するレポートに基づく）。
 - ユーザ名を入力します（ユーザ アクティビティ レポートの場合）。
 - または
 - 管理者名を入力します（管理者アクティビティ レポートの場合）。
 - レポートに含めるデータを持つ、必要なルール セットの**ルール セット名**。
7. [**Display Report**] をクリックし、指定した条件に基づいてレポートを生成します。

レポートをエクスポートする方法

Administration Console では、ファイルにレポートをエクスポートする機能を提供しています。レポートをエクスポートして、レポートのローカル コピーを保存できます。これを使用して傾向を追跡できます。また、保存されたレポート データを用いて別のアプリケーションで作業することもできます。

エクスポートされたレポートはカンマ区切り値 (CSV) フォーマットで生成され、テキスト エディタや Microsoft Excel などのスプレッドシート アプリケーションを使用して表示できます。[**Export**] ボタンを使用するとエクスポート オプションを使用できます。このボタンは、表示されたすべてのレポートの右上に表示されます。

ローカル ファイルにレポートをエクスポートする方法

1. 必要なレポートを生成します。その詳細な手順については、「[レポートの生成](#)」を参照してください。レポートが開きます。

2. **[Export]** をクリックします。

レポートを保存するか、または開くかを尋ねるプロンプトが表示されます。

3. **[Open (with)]** または **[Save (file)]** をクリックします。レポートの保存を選択した場合は、ダウンロード場所を指定する必要があります。

後で適切なアプリケーションを使用して、このファイルを表示できます。

第 17 章

システム管理者のためのツール

この章では、RiskFort が提供するツールについて説明します。これらのツールを使用して管理者はシステムを監視し管理することができます。これらのツールは、下記の場所にあります。

Windows の場合

```
<install_location>\Arcot Systems\bin\
```

UNIX プラットフォームの場合

```
<install_location>/arcot/bin/
```

この章では以下のツールについて説明します。

- [DBUtil: RiskFort データベース ツール](#)
- [arrfversion: RiskFort モジュール バージョン表示ツール](#)
- [arrfadmin: サーバ リフレッシュとシャットダウン ツール](#)
- [arrfserver: RiskFort サーバ ツール](#)
- [arrfupload: Quova データ アップロード ツール](#)

DBUtil: RiskFort データベース ツール

RiskFort インストール中に、インストーラは、RiskFort データベースに接続するための情報を収集します。インストールが終了した後、データベースに接続するための RiskFort サーバの情報は `securestore.enc` と呼ばれるファイルに暗号化されたフォーマットで格納されます。このファイルは、RiskFort データベースに接続するのに必要な以下の暗号化された情報を格納します。

- マスタ キー名
- データベース ユーザ名およびパスワード

何らかの理由により、インストール後にマスタ キー値を変更したり、新しいデータベース ユーザ名、パスワードまたは DSN を追加する必要がある場合は、DBUtil を使用して以下を実行します。

- マスタ キーをセットアップする
- データベース ユーザ名とパスワードを挿入する
- 追加の DBUtil オプションを使用する

マスタ キーをセットアップする

インストール中に指定されたマスタ キーは `securestore.enc` ファイル内の値を暗号化するために使用されます。また、RiskFort データベース内に格納されている暗号化キーもすべて暗号化します。

何らかの理由で、`securestore.enc` 内のマスタ キー値を変更する必要がある場合は、以下のようにします。



重要：以下の手順はインストール中にマスタ キーのセットアップに失敗した場合にのみ実行する必要があります。Arcot テクニカル サポート (support@arcot.com) にご連絡ください。

1. 現在の `securestore.enc` ファイルをバックアップします。

現在の `securestore.enc` は以下の場所にあります。

- Windows の場合

`<install_location>\Arcot Systems\conf\`

- UNIX ベースのプラットフォームの場合

`<install_location>/arcot/conf/`

2. 現在の `securestore.enc` を確実に削除します。

3. ツールが配置されている場所へ移動します。

- Windows の場合

`<install_location>\Arcot Systems\bin\`

- UNIX ベースのプラットフォームの場合

`<install_location>/arcot/bin/`

4. 以下のコマンドを実行します。

```
dbutil -init encryptKeyName
```

ツールは指定されたマスタ キー名を持った `securestore.enc` を再作成します。

データベース ユーザ名とパスワードを挿入する

RiskFort インストーラは、`securestore.enc` にデータベース ユーザ名 / パスワードおよびデータベース DSN / パスワード情報を自動的に設定します。ただし、この情報を手動で挿入する必要がある場合は、`dbutil -insert` オプションを使用する必要があります。このオプションでは、情報が上書きまたは更新されるのではなく、ファイルに必要な値が追加されます。



注：DSN とパスワード情報は RiskFort とデータベース サーバによって使用されますが、ユーザ名とパスワード情報は Java コンポーネントによって使用されます。

1. `DBUtil` ツールが配置されている場所へ移動します。
2. 提供されたデータベース `ユーザ名` および `パスワード` の値を `securestore.enc` に挿入するには、以下のコマンドを入力します。

```
dbutil -pi dbUser dbPassword
```

前のコマンドでは、`dbUser` はデータベース ユーザ名で、`dbPassword` は指定されたユーザ名に関連付けられたパスワードです。例：

```
dbutil -pi arcotuser dbpassword
```

追加の DBUtil オプションを使用する

表 17-1 に、`dbutil` オプションの一覧を示します。この表では、**キーと値**のペアは DSN/パスワードまたはデータベース ユーザ名 / パスワード ペアのいずれかを指します。RiskFort サーバは DSN/パスワードを使用しますが、Administration Console および User Data Service はユーザ名 / パスワードを使用します。

表 17-1. 追加の DBUtil オプション

オプション	説明
<code>-h</code>	ツールのヘルプを表示します。 構文： <code>dbutil -h</code>
<code>-init</code>	<code>securestore.enc</code> が <code>conf</code> ディレクトリにない場合、新しい <code>securestore.enc</code> を作成します。 構文： <code>dbutil -init key</code> 例： <code>dbutil -init MasterKeyNew</code> <code>dbutil -init RiskFortDatabaseMKNew</code> 重要： このコマンドは <code>conf</code> ディレクトリに <code>securestore.enc</code> がない場合にのみ、成功します。
<code>-pd</code>	<code>securestore.enc</code> から指定されたキーと値のペアを削除します。 構文： <code>dbutil -pd key</code> 例： <code>dbutil -pd RiskFortDatabaseDSNold</code> <code>dbutil -pd Jack</code>

表 17-1. 追加の DBUtil オプション

オプション	説明
-pi	追加のキーと値のペアを <code>securestore.enc</code> に挿入します（前の「データベース ユーザ名とパスワードを挿入する」で詳述）。 構文： <pre>dbutil -pi key value</pre> 例： <pre>dbutil -pi RiskFortBackupDSN dbapassword dbutil -pi Jack userpassword</pre> 重要：各キーは 1 つの値のみを持つことができます。すでにキーと値のペアを挿入している場合、同じキーに別の値を挿入することはできません。
-pu	<code>securestore.enc</code> で既存のキーと値のペアの値を更新します。この機能はデータベース パスワードを更新する必要がある場合に使用できます。 構文： <pre>dbutil -pu key value</pre> 例： <pre>dbutil -pu RiskFortDatabaseDSN newPassword dbutil -pu Jack userPassword</pre>

arrfversion: RiskFort モジュール バージョン表示ツール

`arrfversion` ツールを使用すると、RiskFort ルールおよびプラグイン モジュール（Windows 上の `.dll` ファイルおよび UNIX ベース プラットフォーム上の `.so`）のバージョンをチェックして表示することができます。これらのモジュールは以下のディレクトリにあります（`ARCOT_HOME` からの相対パス）。

- `/bin/`
- `/plugin/rules/`
- `/plugin/rules/addon/`

展開と操作に関連する問題が発生した場合、Arcot テクニカル サポート（support@arcot.com）に問い合わせるときに、展開したモジュールのバージョンを指定することをお勧めします。これは問題をより早く識別して解決するのに役立ちます。

構文：

このツールを使用するための構文は以下のとおりです。

```
arrfversion <library1_path> [<library2_path> ...]
```

前の構文では、<libraryN_path> 文字列に以下のように個々のモジュールの名前を指定します。

- Windows の場合は `aradminprotocol.dll`
- UNIX ベースのプラットフォームの場合は `libaradminprotocol.so`

ライブラリ モジュールの絶対パスを指定しなかった場合、指定されたモジュールは標準的な環境変数によって指定されたフォルダ内で参照されます。例：

- Windows の場合は `%PATH%`
- UNIX ベースのプラットフォームの場合は `$LD_LIBRARY_PATH`

例：

Windows の場合

```
arrfversion ScoreEngine.dll
```

UNIX ベースのプラットフォームの場合

```
arrfversion /opt/arcot/plugins/rules/libaradminprotocol.so
```

arrfadmin: サーバ リフレッシュとシャットダウン ツール

設定変更を行うと、サーバをリフレッシュする必要がある場合が多数あります。たとえば、`.ini` ファイルを変更する場合はすべて、サーバを再起動する必要があります。また、Administration Console を使用して変更を行った場合にも、サーバを再起動またはリフレッシュする必要がある場合があります。そのような場合、Administration Console は必要に応じてリフレッシュまたは再起動するようにユーザに通知します。



注：リフレッシュを選択した場合、サーバのダウン タイムは一切発生しません。ほとんどの設定変更では、サーバの再起動は不要です。

`arrrfadmin` ツールを使用することにより、正常にサーバをシャットダウンしたり、再起動せずにキャッシュをリフレッシュすることができます。正常にシャットダウンした場合、サーバでは、既存のリクエストはすべて処理できますが、新規のリクエストは一切受理しません。

ツールを使用する前に

ツールを使用する前に、`riskfortadminclient.ini` の設定を構成する必要があります。このファイルは以下の場所にあります。

Windows の場合

`<install_location>\Arcot Systems\conf\`

UNIX プラットフォームの場合

`<install_location>/arcot/conf/`



注: `riskfortadminclient.ini` に関する詳細情報については、「*Arcot RiskFort 2.2.6 インストールおよび展開ガイド*」の付録 B 「設定ファイルおよびオプション」を参照してください。

ツールが正しく動作するために最低限設定する必要があるこのファイル内のパラメータを、表 17-2 に示します。

表 17-2. riskfortadminclient.ini に最低限設定する必要があるパラメータ

パラメータ	デフォルト	説明
Host	localhost	RiskFort サーバを実行しているシステムのホスト名または IP アドレス。
Port	7980	サーバがサーバ管理リクエストをリッスンしているポート番号。
Transport	tcp	サーバ管理リスナのためのトランスポート モード。以下の値を指定できます。 • TCP • SSL

これらの設定は、ツールと RiskFort サーバ間の典型的な TCP ベースの通信を保証します。これら 2 つの間に双方向 SSL 通信を設定する場合は、「[サーバとの双方向 SSL 通信用のツールの設定](#)」を参照してください。

ツールの使用

構文：

`riskfortadminclient.ini` に最低限の設定を行ったら、ツールを使用できるようになります。ツールを使用するには、以下のいずれかの構文を使用します。

- **arrfadmin [`<options>`]**

前の構文を使用する場合、`riskfortadminclient.ini`（表 17-2 に記載）にパラメータが設定されていることを確認する必要があります。

- **arrfadmin `<server_ipaddress>` `<server_adminport>` `<options>`**

表 17-3 に、`arrfadmin` ツールで使用するパラメータを示します。

表 17-3. `arrfadmin` サーバ接続パラメータ

パラメータ	説明
Host または <code>server_ipaddress</code>	RiskFort サーバまたは Case Management Queuing サーバが利用可能な IP アドレスまたはホスト名。
Port または <code>server_adminport</code>	RiskFort サーバまたは Case Management Queuing サーバが操作リクエストをリッスンするポート番号。 注：デフォルトでは、RiskFort サーバはポート 7980 で利用可能です。

表 17-4 に、ツールでサポートしている <options> を示します。

表 17-4. arrfadmin オプション

オプション	説明
-h	このオプションでは、ツールのヘルプを表示します。このオプションにはパラメータはありません。 例： arrfadmin -h
-d	このオプションでは、サーバの正常なシャットダウンを開始します。 例： arrfadmin -d または arrfadmin 10.150.1.40 7980 -d
-r	このオプションでは、サーバにリフレッシュ リクエストを送信します。 例： arrfadmin -r

サーバとの双方向 SSL 通信用のツールの設定

RiskFort サーバとの双方向 SSL 通信用の `arrfadmin` ツールを設定するには、以下を実行する必要があります。

1. 手順 1 : `riskfortadminclient.ini` の編集
2. サーバ管理プロトコルの設定

手順 1 : `riskfortadminclient.ini` の編集

このファイルを編集する方法

1. `riskfortadminclient.ini` ファイルのある `ARCOT_HOME` の `conf` ディレクトリに移動します。
2. ファイル内の `Host` と `Port` のパラメータに対する値が必要な RiskFort サーバ インスタンスを指していることを確認します。

3. 表 17-5 に示したパラメータに必要な値を指定します。

表 17-5. riskfortadminclient.ini に設定する双方向 SSL パラメータ

パラメータ	デフォルト	説明
Transport	tcp	トランスポート モードとして SSL を指定します。
SSLClientKey	デフォルト値 なし	arrrfadmin ツールによって使用される base64 にエンコードされた (PEM にフォーマット済みの) SSL キーの絶対パスを指定します。
SSLClientCertChain	デフォルト値 なし	arrrfadmin ツールによって使用される base64 にエンコードされた (PEM にフォーマット済みの) SSL 証明書または証明書チェーンの絶対パスを指定します。
SSLServerCACert	デフォルト値 なし	ツールと RiskFort サーバの間の SSL 通信中に arrrfadmin ツールが信頼する必要がある base64 にエンコードされた (PEM にフォーマット済みの) SSL CA 証明書の絶対パスを指定します。 例： ServerCACert=<install_location>/Arcot Systems/certs/riskfort_ca.pem



重要：証明書に関連付けられたキーは暗号化解除される必要があります。秘密キーが PEM フォーマットで暗号化されている場合、Administration Console はエラー メッセージを表示します。

サーバ管理プロトコルの設定

双方向 SSL 用の RiskFort サーバ管理プロトコルの設定方法

1. MA としてログインしていることを確認します。
2. メイン メニューの **[Services and Server Configurations]** タブをアクティブにします。
3. サブ メニューの **[RiskFort]** タブがアクティブであることを確認します。
4. **[System Configurations]** の下で、**[Protocol Management]** リンクをクリックして **[Protocol Configuration]** ページを表示します。
5. SSL 用の RiskFort サーバ管理プロトコルを設定するには、以下の手順に従います。
 - a. **[Enabled]** 列で、**[Server Management]** に対応するチェック ボックスがオンになっていることを確認します。

- b. **[Port]** 列で、デフォルト以外のポート番号でサーバ管理プロトコルを設定する場合は、ポート番号を指定します。
- c. **[Transport Security]** 列で、ドロップダウン リストから **[SSL]** を選択します。
- d. **[Client Store]** 列で、信頼された認証機関 (CA) のルート証明書が含まれている必要な信頼ストアを選択します。



注： 選択できる信頼ストアがない場合、Master Administrator は、**[System Configuration]** の下の **[Trusted Certificate Authorities]** リンクを使用して、まず信頼ストアを設定する必要があります。

- e. **[SSL Certificate Details]** 列で以下の手順に従います。
 - i. **[Certificate Chain]** に対して **[Browse]** をクリックして適切な場所へ移動し、サーバ用の SSL 証明書チェーンをアップロードします。



注： チェーン内の証明書は、リーフ証明書、中間認証局証明書、ルート証明書の順にアップロードを開始する必要があります。

- ii. **[Private Key]** に対して **[Browse]** をクリックして適切な場所へ移動し、証明書に対応する秘密キーをアップロードします。



注： 証明書チェーンおよび秘密キーはどちらも PEM フォーマットである必要があり、アップロードされた秘密キーはパスワード保護されていない必要があります。

- f. **[Save]** をクリックして変更内容を保存します。
- 6. ページ上で設定を完了したら、**[Save]** をクリックします。
 - 7. 前の変更を加えた RiskFort サーバ インスタンスをリフレッシュします。リフレッシュ方法については、[4-55 ページの「サーバ インスタンスの再起動」](#)を参照してください。

arrfserver: RiskFort サーバ ツール

`arrfserver` ツールは、中核的なリスク評価サーバ モジュールで、対話型モードでコマンド ラインから実行することもできます。これにより、以下を設定することができます。

- RiskFort Web サービスのための認証と許可の設定。
- ほとんど使用されないか、または特定の展開シナリオ下でのみ必要な RiskFort の設定。
- Administration Console では表示されない RiskFort の設定。

ツールを対話型モードで実行する

このツールは、`-i` オプションを指定することにより対話型モードで実行できます。このモードでは、すべてのサーバ設定はサービス モードと同様の方法で実行されます。ただし、リスナは開始されません。

このモードで実行すると、サーバは固有のコンソール プロンプト (`#`) を開始します。`arrfserver` ツールを実行するには、以下の手順に従います。

1. ツールが配置されている場所へ移動します。
 - **Windows の場合**
`<install_location>\Arcot Systems\bin\`
 - **UNIX ベースのプラットフォームの場合**
`<install_location>/arcot/bin/`
2. 以下のコマンドを実行します。
 - **Windows の場合**
`arrfserver -i`
 - **UNIX ベースのプラットフォームの場合**
`riskfortserver -i`

ツールは対話型モードで開始されます。

3. 表 17-6 に示したオプションを指定して、必要なタスクを実行します。

表 17-6. arrfserver オプション

オプション	説明
?	<code>arrfserver</code> によってサポートされているすべてのオプションのコマンドを表示します。 たとえば、「 <code>help setsaconf</code> 」と入力すると、コマンドの使用方法的簡単な説明が表示されます。
??	提供されるパターンに基づいてコマンドを検索します。 たとえば、「 <code>??conf</code> 」と入力すると、パターンに一致するすべてのツール オプションが表示されます。
<code>setsaconf</code>	RiskFort サーバによって認証と許可のために提供される Web サービス API を設定できます。 アクセスをセキュリティ保護する場合は <code>1</code> を、標準アクセスの場合は <code>0</code> を入力します。
<code>q</code>	対話型モードを終了します。

arrfupload: Quova データ アップロード ツール

RiskFort は、Quova データを使用してトランザクションの送信元であるシステムの IP アドレスを使用することにより、ユーザの地理的な場所の情報を識別します。その後、このデータを使用して、[Negative Country] ルール、[Negative IP] ルールおよび [Zone Hopping] ルールを評価します。

詳細については、7-98 ページの「拒否 IP タイプの設定」、7-95 ページの「拒否 IP アドレスの設定」および 7-111 ページの「ゾーンホッピングの設定」を参照してください。

Quova およびサービスの詳細については、以下を参照してください。

<http://www.quova.com>



注： Quova データは定期的にダウンロードする必要があります。地理的な場所に関する情報のデータ ファイルは毎週ダウンロードする必要がありますが、アノマイザ関連のデータ ファイルは毎月ダウンロードする必要があります。ダウンロード手順に関する詳細については、Arcot サポート (support@arcot.com) にお問い合わせください。

Arcot RiskFort データ アップロード ツール ([arrfupload](#)) は、Quova ファイルから RiskFort データベースに地理的な場所のデータをアップロードできるコマンド ライン ユーティリティです。

ツールを使用する前に

[riskfortdataupload.ini](#) ファイルは、Arcot RiskFort データ アップロード ツールの動作を制御します。これは以下の場所にあります。

Windows の場合

<install_location>\Arcot Systems\conf\

UNIX プラットフォームの場合

<install_location>/arcot/conf/

ツールを使用するには、このファイル (表 17-7) にパラメータを設定する必要があります。

表 17-7. riskfortdataupload.ini の設定パラメータ

パラメータ	デフォルト	説明
Tables	ロードしない	ユーザが作業できる表。 以下の値を使用できます。 • GeoPoint • Anonymizer
Load	0	表にデータをアップロードするかどうかを示すインジケータ。 以下の値を使用できます。 • 0 (ロードしない) • 1 (ロードする)

表 17-7. riskfortdataupload.ini の設定パラメータ

パラメータ	デフォルト	説明
Swap	0	GeoPoint または GeoAnonymizer のデータがアップロードされたばかりの表を使用して開始するように RiskFort 設定を切り替えるかどうかを示すインジケータ。 重要： RiskFort サーバ キャッシュはこの変更の後にリフレッシュする必要があります (<code>arrfadmin -r</code> コマンドを使用)。 以下の値を使用できます。 • 0 (交換しない) • 1 (交換する)
Filename	--	Quova データをロードする必要があるファイルの名前。 重要： ファイル名だけでなく、ファイルへの絶対パスを指定する必要があります。



注： Load および Swap がどちらも 1 に設定されている場合、表はロードされてから交換されます。

ツールの使用

このツールは以下の場所にあります。

Windows の場合

<install_location>\Arcot Systems\bin\

UNIX プラットフォームの場合

<install_location>/arcot/bin/

このツールは、`arcotcommon.ini` ファイルのデータベース情報を使用して RiskFort データベースに接続し、`securestore.enc` ファイルに指定されているユーザ名とパスワードを使用してデータベースへの認証を行います。

構文：

ツールを使用するには、以下のコマンドを実行します。

```
arrfupload <option>
```

	重要： このツールを使用してアップロードした Quova 情報は、 <code>arrfadmin -r</code> コマンドを使用して RiskFort サーバ キャッシュをリフレッシュするまで使用することはできません。

表 17-8 に、ユーティリティでサポートしているオプションを示します。

表 17-8. arrfupload のオプション

オプション	説明
-help	ツールでサポートしているオプションをすべて表示し、オプションの簡単な使用方法をその後に示します。
-config	このオプションを使用して <code>riskfortdataupload.ini</code>（ツールが使用する設定ファイル）から情報を読み取り、必要なアクションを実行します。 このオプションでは以下のフラグを使用します。 • Tables : ユーザが更新する表のセット。指定可能な値は <code>Geopoint</code> または <code>Anonymizer</code> のいずれかです。どちらも指定されない場合、データはアップロードされません。このオプションにはデフォルト値はありません。 • Load : <code>1</code> に設定されている場合はデータがアップロードされることを示し、<code>0</code> に設定されている場合はデータがアップロードされないことを示します。デフォルト値は <code>0</code> です。 重要：<code>1</code> に設定する場合は、<code>Filename</code> と <code>Tables</code> のフラグを設定する必要があります。 • Swap : <code>1</code> に設定されている場合は表が交換されることを示し、<code>0</code> に設定されている場合は表が交換されないことを示します。デフォルト値は <code>0</code> です。 重要：<code>Tables</code> フラグが正しく設定されている場合のみ、このフラグは有効です。また、新規の表を使用できるようにするには RiskFort サーバ キャッシュをリフレッシュする必要があります。 • Filename : アップロードされるデータが含まれている Quova ファイルの名前とパスを示します。 重要：<code>Load</code> フラグが <code>1</code> に設定される場合のみ、このフラグは有効です。

表 17-8. arrfupload のオプション

オプション	説明
-tnames	このオプションを使用して、RiskFort データベースによって使用されている現在の ARQGeoPoint および ARQGeoAnonymizer の表を表示します。
-prompt	このオプションを使用して、ユーザが最新の Quova データを使用して更新する表 (ARQGeoPoint または ARQAnonymizer) を選択できるようにする対話型コマンド ライン メニューを表示します。ユーザによって指定された表に基づいて、以下のオプションを選択するサブメニューが表示されます。 • [Load Quova Data] : メイン メニューから選択された表のセットに応じて、データを指定された表にロードすることができます。Quova データをロードする必要があるファイルの名前を指定する際は、必ずこのファイルのパスも指定してください。 • [Swap Quova Tables] : メイン メニューで選択された表のセットに応じて、ユーザは表を交換することができます。 • [Exit to the previous menu] : ユーザはメイン メニューに移動することができます。 • [Exit the program] : ユーザはツールを終了することができます。

付録 A

RiskFort ロギング

RiskFort サーバとユーザのアプリケーションの間の通信を効率的に管理するには、サーバおよび他のコンポーネントのアクティビティおよびパフォーマンスに加えて、発生する可能性のある問題に関する情報を取得することが必要です。

この付録では、RiskFort でサポートされている各種ログ ファイル、これらのファイルに表示される重要度レベル、およびこれらのログ ファイルの形式について説明します。この章には、以下のトピックがあります。

- ログ ファイルについて
- RiskFort サーバおよび Case Management サーバ ログ ファイルの形式
- UDS および Administration Console のログ ファイルの形式
- サポートされている重要度レベル

ログ ファイルについて

RiskFort ログ ファイルは次のように分類できます。

- インストール ログ ファイル
- トランザクション ログ ファイル
- UDS ログ ファイル
- Administration Console ログ ファイル

ログ関連のパラメータ（`[arcot/riskfort/logger]` セクションに指定されている）はすべて、`riskfortserver.ini` ファイルによって制御されます。これらのログ設定オプションには次のものが含まれます。

- **[Specifying log file name and path]** : RiskFort がログ ファイルの書き込みを行い、バックアップ ログ ファイルを格納するためのディレクトリを指定できます。診断ログ用のディレクトリを指定すると、管理者はシステムとネットワークのリソースを管理できます。

- **[Log file size]** : ログ ファイルの最大バイト数。ログ ファイルがこのサイズに到達すると、指定された名前を持つ新規ファイルが作成され、古いファイルはバックアップ ディレクトリに移動されます。
- **[Using log file archiving]** : RiskFort コンポーネントが実行され、診断メッセージが生成されるにつれて、ログ ファイルのサイズは増加します。ログ ファイルのサイズが増加し続けるよう設定した場合、管理者はログ ファイルを手動で監視してデータを消去する必要があります。RiskFort では、収集されて保存されるログ ファイルデータの量を制限する設定オプションを指定できます。この設定オプションを指定することにより、RiskFort で診断ログ ファイルのサイズを制御できます。このオプションにより、ログ ファイルの最大サイズが決まります。最大サイズに到達すると、新しいログ情報が保存される前に、古いログ情報がバックアップ ファイルに移動されます。
- **[Setting logging levels]** : RiskFort では、ロギング レベルを設定することもできます。ロギング レベルを設定することによって、診断ログ ファイルに保存するメッセージの数を減らすことができます。たとえば、システムが重要なメッセージだけを記録し保存するように、ロギング レベルを設定できます。サポートされているログ レベルの詳細については、[A-327 ページの「サポートされている重要度レベル」](#)を参照してください。
- **[Specifying time zone information]** : RiskFort では、ログ記録された情報のタイムスタンプにローカル タイムゾーンを使用するか、または GMT を使用することができます。

インストール ログ ファイル

RiskFort をインストールすると、インストーラは `Arcot_RiskFort_InstallLog.log` ファイルで実行されるアクションをすべて記録します。このファイルの情報は、RiskFort インストールが正常に完了しなかった場合、問題の原因を特定するのに非常に役立ちます。

このファイルのデフォルトの場所は以下のとおりです。

Windows の場合

```
<install_location>\Arcot Systems\logs\
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```


トランザクション ログ ファイル

トランザクション ログには次のファイルがあります。

- [RiskFort サーバ ログ](#)
- [Case Management サーバ ログ ファイル](#)

RiskFort サーバ ログ

RiskFort では、[arcotriskfort.log](#) ファイルにサーバによって処理されたすべてのリクエストおよび関連するアクションを記録します。このファイルのデフォルトの場所は以下のとおりです。

Windows の場合

```
<install_location>\Arcot Systems\logs\
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```



注： RiskFort ロガーを使用してユーザ アプリケーションのログを設定することはできません。これらのログには、アプリケーションをホストしているサードパーティ アプリケーション サーバ（Apache Tomcat や IBM Websphere など）が使用するツールを使用することにより、アクセスできます。

ログ関連のパラメータ（[\[arcot/riskfort/logger\]](#) セクションに指定されている）はすべて、[riskfortserver.ini](#) ファイルによって制御されます。[riskfortserver.ini](#) ファイルは [ARCOT_HOME](#) の [conf](#) フォルダにあります。

Case Management サーバ ログ ファイル

Case Management サーバ モジュールを展開して開始した場合、そのすべてのアクションおよび処理されたリクエストの詳細は [arcotriskfortcasemgmtserver.log](#) ファイルに記録されます。このファイルのデフォルトの場所は以下のとおりです。

Windows の場合

```
<install_location>\Arcot Systems\logs\
```

UNIX ベースの場合

<install_location>/arcot/**logs**/



注： RiskFort ロガーを使用してユーザ アプリケーションのログを設定することはできません。これらのログには、アプリケーションをホストしているサードパーティ アプリケーション サーバ（Apache Tomcat や IBM Websphere など）が使用するツールを使用することにより、アクセスできます。

ログ関連のパラメータ（[\[arcot/riskfortcasemgmtserver/logger\]](#) セクションに指定されている）はすべて、[riskfortcasemgmtserver.ini](#) ファイルによって制御されます。riskfortcasemgmtserver.ini ファイルは [ARCOT_HOME](#) の [conf](#) フォルダにあります。

UDS ログ ファイル

ユーザ データ サービス (UDS) 情報およびアクションはすべて [arcotuds.log](#) ファイル内に記録されます。この情報には、以下のものが含まれます。

- UDS データベースの接続情報
- UDS データベースの設定情報
- UDS インスタンス情報、およびこのインスタンスによって実行されたアクション

このファイル内の情報は、Administration Console が UDS インスタンスに接続できなかった場合、その問題の原因を特定するのに非常に役立ちます。このファイルのデフォルトの場所は以下のとおりです。

Windows の場合

<install_location>\Arcot Systems**logs**\

UNIX ベースの場合

<install_location>/arcot/**logs**/

このファイルのロギングを制御するパラメータは [udsserver.ini](#) ファイルを使用することによって設定できます。udsserver.ini ファイルは [ARCOT_HOME](#) の [conf](#) フォルダにあります。

ロギング レベル、ログ ファイル名およびパス、ファイルの最大サイズ（バイト）およびアーカイブする情報に加えて、

[log4j.appender.debuglog.layout.ConversionPattern](#) に適切な値を指定することにより、UDS のロギング パターンのレイアウトを制御することもできます。

このファイルに使用されているデフォルトの形式の詳細については、[A-326 ページの「UDS および Administration Console のログ ファイルの形式」](#)を参照してください。

Administration Console ログ ファイル

Administration Console を展開して開始した場合、そのすべてのアクションおよび処理されたリクエストの詳細は `arcotadmin.log` ファイルに記録されます。この情報には、以下のものが含まれます。

- データベースの接続情報
- データベースの設定情報
- インスタンス情報、およびこのインスタンスによって実行されたアクション
- UDS 設定情報
- キャッシュ リフレッシュのように Master Administrator によって指定されたその他の Administration Console の情報

このファイルの情報は、Administration Console が起動しなかった場合、その問題の原因を特定するのに非常に役立ちます。このファイルのデフォルトの場所は以下のとおりです。

Windows の場合

```
<install_location>\Arcot Systems\logs\
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```

このファイルのロギングを制御するパラメータは `adminserver.ini` ファイルを使用することによって設定できます。`adminserver.ini` ファイルは `ARCOT_HOME` の `conf` フォルダにあります。

ロギング レベル、ログ ファイル名およびパス、ログ ファイルの最大サイズ（バイト）およびログ ファイルのアーカイブ情報に加えて、

`log4j.appender.debuglog.layout.ConversionPattern` に適切な値を指定することにより、コンソールのロギング パターンのレイアウトを制御することもできます。

このファイルに使用されているデフォルトの形式の詳細については、[A-326 ページの「UDS および Administration Console のログ ファイルの形式」](#)を参照してください。

RiskFort サーバおよび Case Management サーバ ログ ファイルの形式

表 A-1 には、A-323 ページの「RiskFort サーバ ログ」で説明した RiskFort ロガー (arcotriskfort.log) のエントリの形式を示します。

表 A-1. RiskFort ログ形式

列	説明
タイム スタンプ	エントリがログに記録された時刻（指定されたタイム ゾーンに変換された値）。この情報のログの形式を以下に示します。 <pre>www mmm dd HH:MM:SS.mis yy timezone</pre> 上記の形式では、 • <code>www</code> は曜日を表します。 • <code>mis</code> はミリ秒を表します。 • <code>timezone</code> は、<code>riskfortserver.ini</code> ファイルで指定したタイムゾーンを表します。
ログ レベル (または重要度)	ログに記録されたエントリの重要度レベル。詳細については、「サポートされている重要度レベル」を参照してください。
プロセス ID (pid)	エントリをログに記録したプロセスの ID。
スレッド ID (tid)	エントリをログに記録したスレッドの ID。
トランザクション ID	エントリをログに記録したトランザクションの ID。
モジュール ID (非推奨)	エントリをログに記録した RiskFort モジュール（ルール エンジンやスコアリング エンジンなど）の ID。 注：これは非推奨のエントリで、常に 0 になります。
Message	サーバにより、フリーフロー形式でログに記録されたメッセージ。 注：このメッセージの精度は、<code>riskfortserver.ini</code> に設定した ログ レベル によって変わります。

UDS および Administration Console のログ ファイルの形式

表 A-2 に、以下のロガーのエントリの形式を示します。

- `arcotuds.log` (UDS ログ ファイル)

- `arcotadmin.log` ([Administration Console ログ ファイル](#))

表 A-2. UDS および Administration Console のログ形式

列	関連付けられたパターン (ログ ファイルで)	説明
タイム スタンプ	<code>%d{yyyy-MM-dd hh:mm:ss,SSS z} :</code>	エントリがログに記録された時刻。このエントリではアプリケーション サーバのタイムゾーンが使用されます。この情報のログの形式を以下に示します。 <code>yyyy-MM-dd hh:mm:ss,SSS z</code> 上記の形式では、 • <code>SSS</code> はミリ秒を表します。 • <code>z</code> はタイムゾーンを表します。
スレッド ID	<code>[%t] :</code>	エントリをログに記録したスレッドの ID。
ログ レベル (または重要度)	<code>%-5p:</code>	ログに記録されたエントリの重要度レベル。詳細については、「 サポートされている重要度レベル 」を参照してください。
Logger Class	<code>%-5c{3} (%L) :</code>	ログ リクエストをしたロガーの名前。
Message	<code>%m%n:</code>	サーバによってログ ファイルにフリーフロー形式でログされたメッセージ。 注：メッセージの精度は、ログ ファイルに設定した ログ レベル によって変わります。

UDS および Administration Console のログ ファイル内の `PatternLayout` パラメータをカスタマイズする方法については、以下の URL を参照してください。

<http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html>

サポートされている重要度レベル

ログ レベル (または重要度レベル) では、RiskFort ログに格納されている情報の詳細のレベルを指定できます。また、このパラメータを使用してログ ファイルの大きさを制御することもできます。

表 A-3 には、すべてのログ ファイルに表示されるログ レベルを重要度の高いものから順に示します。

表 A-3. RiskFort ログ レベル（重要度の高い順）

ログ レベル		説明
0	FATAL	RiskFort サービスの突然の終了を引き起こす可能性がある、深刻で修復できないエラーに対してこのログ レベルを使用します。
1	WARNING	FATAL ほどではないが望ましくないランタイム例外、有害な可能性のある状況、回復可能な問題に対してこのログ レベルを使用します。
2	INFO	ランタイム イベントについての情報をキャプチャする場合にこのログ レベルを使用します。 つまり、この情報では主にアプリケーションの進捗状況を扱います。進捗状況には、以下のような変化が含まれる場合があります。 • 開始、停止および再起動のようなサーバの状態。 • サーバのプロパティ。 • サービスの状態。 • サーバ上のプロセスの状態。
3	LOW DETAIL	デバッグ目的で詳細情報をログに記録する場合にこのログ レベルを使用します。プロセス追跡およびサーバ状態の変化が含まれる場合があります。



注： ログ レベルを指定すると、そのレベルよりも重要度の高いメッセージもすべてレポートされます。たとえば、LogLevel が 3 に指定されている場合、**FATAL**、**WARNING** および **INFO** レベルのログ レベルが設定されたメッセージもキャプチャされます。

各ログ レベルのサンプル エントリ

以下のサブセクションではいくつかの **RiskFort** ログ ファイルのサンプル エントリ（ログ レベルに基づいた）を示します。

FATAL

```
May 27 18:31:01.585 2010 GMT FATAL: pid 4756 tid 5152: 0: 0: Cannot  
continue due to ARRF_LIB_init failure, SHUTTING DOWN
```

WARNING

```
May 24 14:47:39.756 2010 GMT WARNING: pid 5232 tid 5576: 0: 110000:  
EVALHTTPCALLOUT : Transport Exception : create: No Transports Available
```

INFO

```
May 24 14:41:43.758 2010 GMT INFO: pid 3492 tid 4904: 0: 109002: Error  
in ArPFExtRuleSetEval::evaluate Could not get user context (two  
parallel requests)
```

```
May 25 10:01:28.131 2010 GMT WARNING: pid 1048 tid 3104: 8: 0: Error in  
ArRFCaseStatus::startInit: No data found
```

DETAIL

```
May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering USERRISKEVALVELOCITY Rule Evaluation
function

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE: VELOCITY_DURATION=[60],
VELOCITY_DURATION_UNIT=[MINUTES],                VELOCITY_TRANSACTION_COUNT=[5]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering UserRiskEvalVelocityRule
durationToTimeConvertor

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting UserRiskEvalVelocityRule
durationToTimeConvertor

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering UserRiskEvalVelocityRule
callUserEvalVelocityRule

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering
ArUserRiskEvalVelocityDBO::decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT INFO: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting
ArUserRiskEvalVelocityDBO::decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting UserRiskEvalVelocityRule
callUserEvalVelocityRule

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.RESULT=[0]
```



```
May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:  
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.DETAIL=[RESULT=0;TCOUNT=2;  
ACT=mecction]
```

```
May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:  
USERRISKEVALVELOCITYRULE : Exiting USERRISKEVALVELOCITY Rule Evaluation  
function
```


付録 B

用語集

CSR (Customer Support Representatives、テクニカル サポート担当者)	セキュリティ システムのユーザに関連する日常業務を担当する管理者。 たとえば、管理者は、ユーザの登録支援、パスワードのリセット、登録レポートの生成を行うことができます。
Global Administrator	CSR (Customer Support Representatives、テクニカル サポート担当者) アカウントのセットアップおよびシステムの設定を担当する管理者。
Master Administrator	RiskFort 管理者の最高レベル。主な担当業務は、RiskFort を初期化し、Global Administrator アカウントを作成することです。
PKI (Public Key Infrastructure)	ネットワーク環境における公開キー暗号化法および証明書の使用を促進する標準およびサービス。
RiskFort	RiskFort には、指定されたトランザクションのリスクを評価するメカニズムが用意されています。
RiskFort ネイティブ プロトコル	RiskFort サーバ、そのコンポーネント、および Administration Console の間の通信用の Arcot 専用プロトコル。
SSL (Secure Sockets Layer)	公衆ネットワーク上でのメッセージ伝送のセキュリティを管理するためのプロトコル。
TCP (Transmission Control Protocol)	保証されたデータ伝送を行うためのインターネット プロトコル。暗号化されていないデータを送信します。
アグリゲータ	複数の企業にまたがってユーザ情報を照合することによってアカウント集約サービスを提供するサードパーティ ベンダー。
アドオン ルール	RiskFort に付属する追加のリスク評価ルール。
クレデンシャル	ユーザ ID を証明するもの。デジタル クレデンシャルは、スマートカードまたは USB トークンなどのハードウェアまたはサーバ上に保存されている場合があります。そのクレデンシャルは認証時に検証されます。
コールアウト	外部 (RiskFort の外) で実行するカスタム プログラム。
サーバ管理プロトコル	RiskFort サーバを起動およびシャットダウンするための Arcot 専用プロトコル。
スコアリング エンジン	個別の評価ルールからリスク スコアを収集し、スコアリングの優先順位順にそれら进行处理する RiskFort サーバのコンポーネント。

スコアリング コールアウト	RiskFort のスコアリング エンジンによってスコアが付けられた後で動作し、最終リスク スコアを変更するカスタムのスコアリング ロジックを含むコールアウト。
スコアリング ルール	他のすべての設定済みルールの実行結果を受け取り、最終リスク スコアおよびリスク アドバイスを返す最後のルール。
ゾーン ホッピング	現実的な速度で移動可能な距離以上に隔たった場所からの、同一ユーザによる連続するトランザクション。
デジタル証明書	個人、コンピュータ システム、または組織の ID およびキーの所有権の証明となるデジタルドキュメント。この認証方式は公開キー暗号化 (PKI) 法に基づいています。
デバイス頻度	指定された時間内に同一デバイスから発行されるトランザクションの数。
トラステッド IP アドレス	組織に信頼されているため今後のリスク評価から除外される IP アドレス。
トラステッド アグリゲータ	組織に信頼されているため今後のリスク評価から除外されるアグリゲータ。
ユーザ ID/ パスワード	登録時にユーザに発行されるクレデンシャルの 1 つ。
ユーザ頻度	指定された時間内に同一ユーザから発行されるトランザクションの数。
リスク アドバイス	トランザクションのリスクを評価した後に RiskFort によって呼び出し元のアプリケーションに示されるアクション (ALLOW、ALERT、DENY、INCREASEAUTH)。
リスク スコア	評価結果に応じて RiskFort から通知されるスコア。スコアは 0 ～ 100 です。数字が大きいほど、リスクも高くなります。
暗号化	内容を判読できないように情報にスクランブルをかける処理。
一方向 SSL	SSL セッションが確立される前に、クライアント アプリケーションが (サーバのデジタル証明書を受理することによって) サーバアプリケーションの ID を検証します。
拡張可能エレメント	リスク評価のためにアドオン ルールによって使用されるトランザクションに関連する追加のエレメント。
拒否 IP アドレス	過去において、アノニマイザ プロキシ、不正なトランザクション、または悪意のあるトランザクションの要求元であったことがわかっている IP アドレス。
拒否国	過去において、不正なトランザクションまたは悪意のあるトランザクションの要求元であったことがわかっている国。

公開キー	PKI で使用される 1 対のキーの一方。このキーは自由に配布され、証明書の一部として発行されます。 通常、公開キーの所有者に送信されたデータを暗号化するために使用されます。その後、公開キーの所有者は、対応する秘密キーを使用して、データを復号化します。
終端ルール	単独で全体的な リスク スコア を決定するルール。
証明書	「 デジタル証明書 」を参照してください。
双方向 SSL	SSL セッションが確立される前に、クライアント アプリケーションとサーバ アプリケーションの両方が（それぞれの デジタル証明書 を提示することによって）互いの ID を確認します。
追加認証	現在のトランザクションが安全でないと RiskFort によって判断される場合に、RiskFort から与えられる リスク アドバイス 。 たとえば、ユーザが初めて大量のトランザクションを実行する場合は挙げられます。そのような場合、ユーザは、より強力な認証方式を使用して認証サーバに再認証されることを求められます。
認証	エンティティのログイン情報が本人のものであることを証明するプロセス。
秘密キー	PKI で使用される 1 対のキーの一方。このキーは秘密に保持され、データの復号化または暗号化に使用できます。
非終端ルール	全体的な リスク スコア は、このルール単独では決定されません。他のルールも必要です。
評価コールアウト	すべての 評価ルール の後で実行され、カスタムのリスク評価ロジックを含む コールアウト 。
評価ルール	着信トランザクション データに適用される、事前に設定された RiskFort ロジック。
頻度チェック	「 デバイス頻度 」および「 ユーザ頻度 」を参照してください。
例外ユーザ	RiskFort に「登録」されており、指定された期間、リスク評価から除外されるユーザ。

A

Administration Console [1](#)

Arcot RiskFort データ アップロード ツール [316](#)

arrfserver [314](#)

B

BA [33](#)

C

CSR [239](#)

D

DBUtil

 オプション [306](#)

 ユーザ ID とパスワードの挿入 [305](#)

R

RiskFort データ

 アクティブ データ [126](#)

 提示されたデータ [126](#)

RiskFort 予測モデル [64](#)

U

UDS [25](#)

あ

アクティブ データ [105](#)

アグリゲータ [87](#)

アドオン ルール [61](#)

 ルール タイプ [63](#)

 カスタム [69](#)

 既存 [63](#)

アドバイス [121](#)

い

インスタンス [1](#)

か

拡張可能エレメント [186](#)

管理ユーザ

 Global Administrator [9](#)

 Master Administrator [8](#)

 Organization Administrator [9](#)

 User Administrator [10](#)

き

基本認証 [33](#)

拒否 IP アドレス リスト [95](#)

拒否国リスト [102](#)

け

ケース管理 [232](#)

 ケース [232](#)

ケース管理ロール

 キュー マネージャ [240](#)

 テクニカル サポート 担当者 [239](#)

 不正行為アナリスト [241](#)

こ

コールアウト [131](#)

 スコアリング [62](#)

 評価 [61](#)

さ

サードパーティ [ii](#)

し

システム管理ツール [303](#)

 aradmin [308](#)

 arrfadmin [309](#)

 DBUtil [304](#)

 dbutil [303](#)

修飾子文字列 [62](#)

終端ルール 59

す

スーパバイザ 240

スコア 121

スコアリング コールアウト 136, 62

スコアリング ルール 62

スコープ 7

ステージング データ 105

せ

設定

運用環境への移行 125, 146

拒否 IP アドレス リスト 105

拒否国リスト 105

トラステッド アグリゲータ 87

プロトコルのセットアップ 122, 137

接続タイムアウト 141

そ

組織 151

ゾーン ホッピング 111

た

対象読者 xiii

ち

注釈文字列 62

て

データのマッピング 67

デフォルトの組織 29

と

登録 217

特徴

リスク アドバイスのサンプル マト
リクス 122

トラステッド IP アドレス リスト 83

トラスト ストア 47

導出データ 67

ひ

評価コールアウト 61

頻度チェック

デバイス頻度 108

ユーザ頻度 105

へ

ベース エレメント 186

ま

マスタ キー 304

マルチテナント アーキテクチャ 1

ゆ

ユーザ データ サービス 25

ユーザ作成モード 115

暗黙的 115

明示的 115

優先される組織 203

よ

読み取りタイムアウト 141

り

リスク アドバイス 121

リスク アドバイスのマトリクス 122

リスク スコア 121

リスト データ 66

る

ルール タイプ

終了 59

スコアリング 62

評価

スタンドアロン

アドオン 61

組み込み 59

ルール セット 80

れ

例外ユーザ 60

例外ユーザ リスト 60

ろ

ロール 4

カスタム ロール 36, 14

管理ユーザ 5

ユーザ 5

ログ

重大度レベル [327](#)

ログ レベル [327](#)

