

# CA ControlMinder

リリースノート

12.8



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし、CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負いません。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2012 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

## サードパーティに関する通知

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2  
Technology Edition, Version 1.4 Modules

© Copyright IBM Corporation 1999, 2002

All Rights Reserved

## サンプル スクリプトおよびサンプル SDK コード

CA ControlMinder 製品に含まれているサンプル スクリプトおよびサンプル SDK コードは、情報提供のみを目的として現状有姿のまま提供されます。これらは特定の環境で調整が必要な場合があるため、テストや検証を実行せずに実稼働システムにデプロイしないでください。

CA Technologies では、これらのサンプルに対するサポートを提供していません。また、これらのスクリプトによって引き起こされるいかなるエラーにも責任を負わないものとします。

## CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA ControlMinder
- CA ControlMinder
- CA Single Sign-On (CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management (CA NSM、旧 Unicenter NSM and Unicenter TNG)
- CA Software Delivery (旧 Unicenter Software Delivery)
- CA Service Desk (旧 Unicenter Service Desk)
- CA User Activity Reporting Module (旧 CA User Activity Reporting)
- CA IdentityMinder

## ドキュメントの表記規則

CA ControlMinder のドキュメントには、以下の規則があります。

形式	意味
等幅フォント	コードまたはプログラムの出力
斜体	強調または新規用語
太字	表示されているとおりに入力する必要がある要素
スラッシュ (/)	UNIX および Windows のパスの記述で使用される、プラットフォームに依存しないディレクトリの区切り文字

また、本書では、コマンド構文およびユーザ入力の説明に（等幅フォントで）以下の特殊な規則を使用します。

形式	意味
斜体	ユーザが入力する必要のある情報
角かっこ ([]) で囲まれた文字列	オプションのオペランド
中かっこ ({} ) で囲まれた文字列	必須のオペランドセット
パイプ ( ) で区切られた選択項目	代替オペランド (1つ選択) を区切ります。 たとえば、以下の例は「ユーザ名またはグループ名のいずれか」を意味します。  <code>{username groupname}</code>
...	前の項目または項目のグループが繰り返し可能なことを示します
下線	デフォルト値
スペースに続く、行末の円記号 (¥)	本書では、コマンドの記述が 1 行に収まらない場合があります。このような場合、行末の空白とそれに続く円記号 (¥) は、そのコマンドが次の行に続くことを示します。 <b>注:</b> このような円記号はコピーしないでください。また、改行はコマンドに含めないようにしてください。これらの文字は、実際のコマンド構文の一部ではありません。

### 例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

この例の内容

- 標準的な等幅フォントで表示されているコマンド名 (`ruler`) は表示されているとおりに入力します。
- 斜体で表示されている `className` オプションは、クラス名 (`USER` など) のプレースホルダです。

- 2 番目の角かっこで囲まれた部分を指定しなくても、コマンドは実行できます。この部分は、オプションのオペランドを示します。
- オプションのパラメータ (props) を使用する場合は、キーワード *all* を選択するか、またはカンマで区切られたプロパティ名を 1 つ以上指定します。

## ファイル ロケーションに関する規則

CA ControlMinder のドキュメントには、ファイル ロケーションに関する以下の規則があります。

- *ACInstallDir* -- CA ControlMinder のデフォルトのインストールディレクトリ。
  - Windows -- <インストールパス>
  - UNIX -- <インストールパス 2>
- *ACSharedDir* -- CA ControlMinder for UNIX で使用される、デフォルトのディレクトリ。
  - UNIX -- /opt/CA/AccessControlShared
- *ACServerInstallDir* -- CA ControlMinder エンタープライズ管理 のデフォルトのインストールディレクトリ。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir* -- デフォルトの配布サーバインストールディレクトリ。
  - /opt/CA/DistributionServer
- *JBoss\_HOME* -- デフォルトの JBoss インストールディレクトリ。
  - /opt/jboss-4.2.3.GA

## CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

# 目次

---

<b>第 1 章: ようこそ</b>	<b>13</b>
CA ControlMinder インストールイメージファイル .....	13
補完 CA User Activity Reporting Module ライセンス .....	15
単一ドキュメントセット .....	15
<b>第 2 章: 新機能と変更された機能</b>	<b>17</b>
CA ControlMinder の拡張機能.....	18
UNAB 拡張機能 .....	20
ドキュメントの拡張機能.....	21
このリリースで修正された問題 .....	22
<b>第 3 章: システム要件</b>	<b>23</b>
オペレーティング システムのサポート .....	23
エンタープライズ管理サーバの要件 .....	23
エンタープライズ管理サーバ統合コンポーネント .....	24
CA ControlMinder エンドポイント管理 の要件 .....	25
UNIX エンドポイントの要件.....	26
Windows エンドポイントの要件.....	26
エンタープライズ レポート機能 .....	27
配布サーバの要件.....	27
Policy Model データベースの要件 .....	28
<b>第 4 章: マニュアル</b>	<b>29</b>
ガイド.....	29
<b>第 5 章: FIPS 準拠</b>	<b>31</b>
FIPS 操作モード.....	31
FIPS 専用モードでサポートされないオペレーティング システム.....	31
FIPS 暗号化ライブラリ .....	32
使用される FIPS アルゴリズム .....	32
鍵と証明書のストレージ.....	33
影響を受ける機能 (UNIX) .....	33

---

影響を受ける機能 (Windows) .....	34
--------------------------	----

## 第 6 章: 機能サポートの制限事項 37

IPv6 のサポート .....	37
Windows エンドポイントの制限事項 .....	37
x64 機能サポートの制限事項 .....	38
IA64 での機能のサポート制限 .....	38
Windows Server 2008 機能サポートの制限事項 .....	39
SAN のサポート .....	40
McAfee Entercept バッファ オーバフロー .....	41
短いファイル名ルール (8.3 形式) がサポートされない .....	41
UNIX エンドポイントの制限事項 .....	41
HP-UX での機能のサポート制限 .....	41
HP-UX Itanium および RHEL Itanium で Unicenter 統合がサポートされない .....	42
Linux IA64 上で SAM エージェントがサポートされない .....	42
SAN のサポート .....	42
UNAB の制限事項 .....	43
一方向の信頼関係を持つドメイン環境でのアカウント パスワード形式 .....	43
UNAB が Linux IA64 上でサポートされない .....	43
UNAB が FIPS140-2 および IPV6 に対応していない .....	43
SAM の制限事項 .....	43
SAM が FIPS140-2 および IPV6 に対応していない .....	43

## 第 7 章: インストールに関する考慮事項 45

サポートされるインストール言語 .....	46
Windows エンドポイントに関する考慮事項 .....	46
Windows Server 2008 上でのインストール、アンインストール、アップグレード時に再起動メッセージが表示される .....	47
UNIX エンドポイントに関する考慮事項 .....	47
AIX 6.1 では、CA ControlMinder の起動に TL3 以降が必要です。 .....	47
Linux390 のメッセージキューに J2SE バージョン 5.0 が必要 .....	47
x86_64bit Linux の互換性ライブラリがない .....	48
CA ControlMinder をインストールまたはアンインストールすると UNAB が再起動する .....	48
CA ControlMinder および UNAB を新しい Solaris ゾーンへ伝達 .....	48
CA ControlMinder を Solaris 11 にインストールする際の制限事項 .....	48
UNAB エンドポイント インストールに関する考慮事項 .....	49
UNAB for Linux 390 のリモート管理用に J2SE バージョン 5.0 が必要 .....	49
サーバコンポーネントのインストールに関する考慮事項 .....	49

エンタープライズ管理サーバを Red Hat Linux 6 にインストールするには 32 ビット パッケージが必要.....	49
CA ControlMinder の Linux へのインストール時に Libc ライブラリがない.....	52
RDP ハードニングの未サポート .....	52
同じタイム ゾーンへのプライマリおよび負荷分散エンタープライズ管理サーバのインストール .....	52
64 ビット Linux へのエンドポイント管理のインストール.....	53
管理者名の特殊文字.....	53
サポートされている JDK および JBoss のバージョン.....	53
前提条件キット インストーラの考慮事項.....	53
サーバコンポーネントのインストールにはスーパーユーザのアカウントが必要.....	53
Java が見つからない場合、インストール時に RDBMS 接続が失敗する.....	54
エンタープライズ管理サーバインストールがインストール パス中のスペースをサポートしない .....	54
別のドメインの Active Directory を使用できるように CA ControlMinder エンタープライズ管理をセットアップ.....	54
CA ControlMinder エンドポイント管理 インストール手順が CA ControlMinder の両方に該当 .....	55
ポート番号 8080 への CA ControlMinder エンドポイント管理 のショートカット .....	56
CA User Activity Reporting Module では trusted SSL 接続のみサポートされる .....	56
CA ControlMinder エンタープライズ管理 から CA User Activity Reporting Module レポートを表示するには特殊なサブスクリプションが必要.....	57
CA ControlMinder エンタープライズ管理 およびレポート ポータル コンピュータのシステム時刻の同期.....	57
スーパーユーザ以外ではインストールが失敗する .....	57

## 第 8 章: アップグレードに関する留意事項 59

アップグレード元のバージョン .....	59
Windows エンドポイントのアップグレードに関する考慮事項 .....	60
データベースへのデフォルト アクセスの変更.....	60
UNIX エンドポイントのアップグレードに関する考慮事項 .....	60
デフォルトのインストール場所.....	60
FIPS 140-2 ライブラリのアップグレード .....	60
UNIX でのシステム全体の監査モードのアップグレード .....	61
認証でのリソース グループの所有権の認識 .....	61
優先度が下げられた syslog メッセージ .....	61
サーバコンポーネントのアップグレードに関する考慮事項 .....	62
12.8 エンタープライズ管理サーバには 12.8 配布サーバが必要 .....	62
12.6 から 12.8 にアップグレードするための要件 .....	62
エンタープライズ管理サーバを r12.7 にアップグレードすると、ロールおよびタスクが保持されない.....	62

CA ControlMinder r12.6 では、CA ControlMinder r12.5 および r12.0.01 での Policy Model の管理に 対してホットフィックスが必要です。.....	63
ポリシーをエンドポイントにデプロイするために必要なソフトウェア パッチ.....	63

## 第 9 章: 一般的な考慮事項 65

Windows エンドポイントに関する考慮事項.....	65
Windows Server 2008 で管理者として実行による CA ControlMinder の開始.....	65
アンインストールで CA ライセンス ファイルが削除されない.....	65
UNAB に関する考慮事項.....	65
SELinux が有効な場合に、ログイン時にホーム ディレクトリが作成されない.....	66
パスワード変更の試行が Red Hat Linux 上で失敗する.....	66
移行後のローカルユーザアカウントの無効化.....	67
unab_refresh_interval トークンの値は短い間隔に設定しない.....	67
Kerberos dns_lookup_realm を True に設定しない.....	67
UNAB ユーザが指定されたパスワードポリシーに従ってアカウントパスワードを変更できな い.....	67
sepass と UNAB エンドポイントの統合.....	68
Active Directory アカウントを使用した UNAB へのログイン.....	68
UNAB がインストールされている場合、管理者アカウントを使用して CA ControlMinder for UNIX にログインできない.....	68
サーバコンポーネントに関する考慮事項.....	69
CA ControlMinder コンポーネントと CA ControlMinder メッセージキューの間の通信の問題.....	69
Oracle でのアップグレード.....	70
CA ControlMinder ホスト名の制約.....	70
ポリシー デプロイ解除スクリプトの自動生成.....	70
DNS ドメイン名ではなく、SAM エンドポイント NETBIOS 名を指定する.....	71
ログインアプリケーションスクリプトを使用して、ドメインのメンバにログオンします。.....	72
複数の CA IdentityMinder プロビジョニング コネクタ サーバを設定できない.....	73
SSL ポートを使用して CA IdentityMinder プロビジョニング コネクタ サーバを設定できない.....	73
SAM を使用してエキスパートアカウントのパスワードを変更できない.....	73
SQLCMD ユーティリティが空のパスワードをサポートしない.....	73
Oracle11g サーバ証明書が必要.....	74

## 第 10 章: 既知の問題 75

インストールの既知の問題.....	75
Windows エンドポイントのインストールの既知の問題.....	75
UNIX エンドポイントのインストールの既知の問題.....	76
UNAB エンドポイントのインストールの既知の問題.....	77
アップグレードの既知の問題.....	78

---

Windows エンドポイントのアップグレードの既知の問題.....	78
UNIX エンドポイントのアップグレードの既知の問題.....	78
一般的な既知の問題.....	79
Windows エンドポイントの既知の問題.....	79
UNIX エンドポイントの既知の問題.....	81
UNAB の既知の問題.....	84
サーバコンポーネントの既知の問題.....	91
マニュアルの既知の問題.....	107



# 第 1 章: ようこそ

---

CA ControlMinder 12.8 をご利用いただき、誠にありがとうございます。本書では、新しい拡張機能、既存機能の変更内容、オペレーティングシステムのサポート、システム要件、ドキュメント情報、インストールの考慮事項と一般的な考慮事項、公開されているソリューション、および CA ControlMinder の既知の問題について説明します。

CA ControlMinder には、エンタープライズ管理機能、レポート機能、および拡張ポリシー管理機能があります。

これ以降、本書の全体でこの製品を CA ControlMinder と呼びます。

このセクションには、以下のトピックが含まれています。

[CA ControlMinder インストールイメージファイル \(P. 13\)](#)

[補完 CA User Activity Reporting Module ライセンス \(P. 15\)](#)

[単一ドキュメントセット \(P. 15\)](#)

## CA ControlMinder インストール イメージ ファイル

CA ControlMinder コンポーネントは、以下のイメージファイルから入手できます。

以下のイメージファイルには、Windows 用のエンタープライズ管理サーバとレポートポータルコンポーネントが含まれています。

- CA ControlMinder Server Components for Windows

CA ControlMinder エンドポイント管理、CA ControlMinder 配布サーバ、および CA ControlMinder エンタープライズ管理のインストールファイルを収録しています。

CA ControlMinder エンタープライズ管理には、CA ControlMinder エンドポイント管理、CA ControlMinder Endpoint Components for Windows、CA ControlMinder 配布サーバコンポーネント、およびデプロイメントマップサーバ (DMS) が含まれます。

このイメージファイルには、CA Business Intelligence にインポートするためのレポートパッケージも含まれています。

- CA ControlMinder Third Party Components for Windows

必要なサードパーティ ソフトウェア (JDK および JBoss) を Windows 上にインストールする前提条件インストーラを収録しています。CA ControlMinder サーバ コンポーネントをインストールするには、これらのソフトウェアをあらかじめインストールしておく必要があります。

以下のイメージファイルには、Linux 用のエンタープライズ管理サーバとレポート ポータル コンポーネントが含まれています。

- CA ControlMinder Server Components for Linux

CA ControlMinder エンドポイント管理、CA ControlMinder 配布サーバ、および CA ControlMinder エンタープライズ管理 のインストール ファイルを収録しています。

CA ControlMinder エンタープライズ管理 には、CA ControlMinder エンドポイント管理、Linux 用 CA ControlMinder エンドポイント コンポーネント、CA ControlMinder 配布サーバ コンポーネント、およびデプロイメント マップ サーバ (DMS) が含まれます。

このイメージファイルには、CA Business Intelligence にインポートするためのレポート パッケージも含まれています。

- CA ControlMinder Third Party Components for Linux

Linux で必要なサードパーティ ソフトウェア (JDK および JBoss) が含まれています。CA ControlMinder サーバ コンポーネントをインストールするには、これらのソフトウェアをあらかじめインストールしておく必要があります。

## 補完 CA User Activity Reporting Module ライセンス

CA ControlMinder の所有者は、CA User Activity Reporting Module 製品の CA ControlMinder 監査ログでの収集、管理、レポートも制限付きで使用することができます。まず、「CA User Activity Reporting Module Server for CA ControlMinder」のライセンスを取得します（コード ELMSAC99100/ELMSAC991）。これは象徴的価格で CA ControlMinder の顧客に提供されるものです。

北米で CA User Activity Reporting Module のライセンスを取得するには、お住まいの地域のアカウント担当者にお問い合わせください。お住まいが北米以外の場合は、最寄りの代理店または CA Technologies の事務所にお問い合わせください。CA User Activity Reporting Module は、CA ControlMinder ダウンロードリンクの下にある CA Support Online の Web サイト (<http://ca.com/support>) の Download Center から、オンラインでダウンロードできます。

## 単一ドキュメント セット

以下では、CA ControlMinder のドキュメントについて説明します。

- リリース ノート
- 実装ガイド
- エンタープライズ管理ガイド
- アップグレードガイド
- 実装ガイド
- Windows エンドポイント管理ガイド
- UNIX エンドポイント管理ガイド
- リファレンス ガイド
- selang リファレンス ガイド
- トラブルシューティング ガイド



## 第 2 章：新機能と変更された機能

---

このセクションには、以下のトピックが含まれています。

[CA ControlMinder の拡張機能](#) (P. 18)

[UNAB 拡張機能](#) (P. 20)

[ドキュメントの拡張機能](#) (P. 21)

[このリリースで修正された問題](#) (P. 22)

## CA ControlMinder の拡張機能

以下の UNAB 拡張機能および修正は、前回のリリース以降に行われたものです。

- **新しい CA ControlMinder エンタープライズ管理 ユーザ インターフェース**

CA ControlMinder エンタープライズ管理 では、ユーザ操作性および使いやすさが改善された新しいユーザ インターフェースが提供されています。

- **Active Directory エンドポイント検出**

Active Directory エンドポイント検出ウィザードを使用して迅速に環境を設定できます。詳細については、「エンタープライズ管理ガイド」を参照してください。

- **エンドポイント ステータスおよびモニタリング**

CA ControlMinder エンタープライズ管理 では、環境内の各エンドポイントに対してインストール ステータス、ヘルス ステータス、および実行ステータスが表示されるようになりました。詳細については、「エンタープライズ管理ガイド」を参照してください。

- **強化された共有アカウント監査**

CA ControlMinder エンタープライズ管理 は、事前定義フィルタによって、アクセス、リクエスト、Break Glass およびパスワード変更イベントの共有アカウント監査レコードを表示できるようになりました。詳細については、「エンタープライズ管理ガイド」を参照してください。

- **クラウド オペレーティング システムのサポート**

CA ControlMinder を Debian および Ubuntu のオペレーティング システムにインストールできるようになりました。詳細については、「インストールガイド」を参照してください。

- **CA ControlMinder エンドポイントでの並列アップグレード**

CA ControlMinder は、Solaris、Linux、AIX のオペレーティング システムでの並列アップグレードをサポートするようになりました。詳細については、「アップグレードガイド」を参照してください。

- **CA AuthMinder との統合**

CA ControlMinder を CA AuthMinder と統合して、UNIX エンドポイントで強力な認証機能を利用できるようになりました。詳細については、「統合ガイド」を参照してください。

- **CA ControlMinder の Microsoft Windows Server 2012 および SQL Server 2012 のサポート**

エンタープライズ管理サーバを Microsoft Windows Server 2012 および SQL Server 2012 にインストールできるようになりました。CA ControlMinder を Microsoft Windows Server 2012 にインストールすることもできます。

- **Sepromote ユーティリティ**

sepromote ユーティリティを使用して、CA AuthMinder によって生成された OTP (ワンタイムパスワード)を検証できます。詳細については、「リファレンスガイド」を参照してください。

## UNAB 拡張機能

以下の UNAB の機能拡張および修正は、前回のリリース以降に行われました。

- **部分的なユーザのログインポリシー**

対応するポリシーが展開している場合にのみ、部分的なユーザがエンドポイントにログインするように制限できます。部分的なユーザのログインを制御するには、`partial_user_login_policy` トークンを使用します。詳細については、「リファレンスガイド」を参照してください。

- **チルダ (~) を含むユーザ名のサポート**

Linux でチルダ (~) 記号を含む Active Directory ユーザアカウントを使用できるようになりました。

- **AIX PAM フラグ `pam_silent` のサポート**

UNAB は、PAM メッセージを除去する AIX PAM モジュール制御フラグ `pam_silent` をサポートするようになりました。

- **UNAB データベースの確認**

UNAB エージェントは定期的にユーザおよびグループのデータベースを確認し、破損している場合はデータベースを再構築します。

- **UNAB によるコンピュータ パスワードの更新**

UNAB エージェントは、コンピュータを Active Directory に登録するために使用されたコンピュータ オブジェクト パスワードを更新できるようになりました。`computer_password_change_interval` トークンを使用します。詳細については、「リファレンスガイド」を参照してください。

## ドキュメントの拡張機能

以下のドキュメントの拡張機能が、前回のリリース以降行われました。

- シナリオベースのコンテンツ

以下のシナリオが追加されました。

- CA ControlMinder を Debian または Ubuntu Linux にインストールする方法

CA ControlMinder を Debian または Ubuntu の Linux オペレーティングシステムにインストールする方法を説明します。

注: 詳細については、「実装ガイド」を参照してください。

- Linux 上の CA ControlMinder をアップグレードする方法

RPM を使用して、Linux 上で CA ControlMinder の並列アップグレードを実行する方法を説明します。

注: 詳細については、「アップグレード」を参照してください。

- CA ControlMinder を AIX でアップグレードする方法

AIX 上で CA ControlMinder の並列アップグレードを実行する方法を説明します。

注: 詳細については、「アップグレード」を参照してください。

- CA ControlMinder を Solaris でアップグレードする方法

Solaris 上で CA ControlMinder の並列アップグレードを実行する方法を説明します。

注: 詳細については、「アップグレード」を参照してください。

- CA ControlMinder を Solaris ゾーンでアップグレードする方法

Solaris ゾーン上で CA ControlMinder の並列アップグレードを実行する方法を説明します。

注: 詳細については、「アップグレード」を参照してください。

- ユーザパスワードリセットの有効化および忘れたパスワードのリセット

ユーザが自身のパスワードをリセットできるようにユーザアカウントおよびプロファイルを設定する方法、および忘れたパスワードのリセット方法を説明します。

**注:** 詳細については、「エンタープライズ管理ガイド」を参照してください。

- CA AuthMinder との統合

オペレーティングシステムの特権ユーザおよび他のネイティブユーザ用に強力な認証オプションを提供する CA AuthMinder との統合方法を説明します。

**注:** 詳細については、「統合ガイド」を参照してください。

- Veritas Cluster Server を使用した Linux 上の CA ControlMinder ハイアベイラビリティの実装

Veritas Cluster Server を使用して、Linux に CA ControlMinder のハイアベイラビリティ展開を実装する方法を説明します。

**注:** 詳細については、「実装ガイド」を参照してください。

- [エンタープライズ管理サーバ展開をアップグレードする方法](#)

移行によってエンタープライズ管理サーバ展開を新しいバージョンにアップグレードする方法を説明します。

- [Apache ロードバランサの設定方法](#)

Apache HTTPD を使用して、負荷分散用にエンタープライズ管理サーバを設定する方法を説明します

## このリリースで修正された問題

このリリースに含まれている修正は、Release FIXLIST に記載されています。CA サポートの [[CA ControlMinder 最新メンテナンス リリース](#)] ページから FIXLIST にアクセスできます。

## 第 3 章：システム要件

---

このセクションには、以下のトピックが含まれています。

[オペレーティング システムのサポート](#) (P. 23)

[エンタープライズ管理サーバの要件](#) (P. 23)

[エンタープライズ管理サーバ統合コンポーネント](#) (P. 24)

[CA ControlMinder エンドポイント管理の要件](#) (P. 25)

[UNIX エンドポイントの要件](#) (P. 26)

[Windows エンドポイントの要件](#) (P. 26)

[エンタープライズ レポート機能](#) (P. 27)

[配布サーバの要件](#) (P. 27)

[Policy Model データベースの要件](#) (P. 28)

### オペレーティング システムのサポート

サポートされているオペレーティング システムのリストについては、[CA サポート](#) サイト上の CA ControlMinder 製品ページで提供されている CA ControlMinder Compatibility Matrix を参照してください。

### エンタープライズ管理サーバの要件

エンタープライズ管理サーバの最小要件は以下のとおりです。

- プロセッサ -- Intel (EM64T)、AM (AMD-V)、またはそれ以降の 64 ビットプロセッサ
- メモリ - 4 GB の RAM
- 使用可能なディスク領域 -- 10 GB (インストールディレクトリ)、2 GB (Windows : %TEMP% または UNIX : /tmp)、4 GB のスワップファイル、1.5 GB (JBoss ディレクトリ)

注: 推奨されるハードウェア仕様については、「実装ガイド」の「エンタープライズ実装の計画」の章を参照してください。

さらに、以下のソフトウェアをエンタープライズサーバにインストールします。

- **JDK** - Java Development Kit (JDK) 1.7 以降
- **アプリケーションサーバ** - JBoss Application Server バージョン 4.2.3.GA
- **中央データベース (RDBMS)** - Oracle Database 10g、Oracle Database 11g、Microsoft SQL Server 2005、Microsoft SQL Server 2008 または Microsoft SQL Server 2012

注: 中央データベースは、別のコンピュータにインストールできます。RDBMS のシステム要件については、お使いの製品のマニュアルを参照してください。

エンドユーザのコンピュータでは、1024 x 768 ピクセル以上の画面解像度と以下の Web ブラウザが必要です。

- **Windows** -- Microsoft Internet Explorer 8.x、Mozilla Firefox、Chrome
- **Linux** -- Mozilla Firefox

## エンタープライズ管理サーバ統合コンポーネント

エンタープライズ管理サーバは、以下の製品との統合をサポートします。

- **Active Directory** - (オプション) エンタープライズユーザストア。

注: このユーザストアは、エンタープライズ管理サーバと同じコンピュータにインストールする必要はありません。

- **CA Directory** - (オプション) CA 固有のユーザストア。

- **Sun ONE** - (オプション) エンタープライズユーザストア。

注: このユーザストアは、エンタープライズ管理サーバと同じコンピュータにインストールする必要はありません。

- **レポートポータル** - CA Business Intelligence。

注: このソフトウェアは、エンタープライズ管理サーバと同じコンピュータにインストールする必要はありません。レポートポータルの最小システム要件については、「CA Business Intelligence インストールガイド」を参照してください。

注: CA Business Intelligence の詳細については、[CA Technologies サポート](#)から入手可能な「CA Business Intelligence インストールガイド」を参照してください。

- **CA User Activity Reporting Module - r12.0**

注: このソフトウェアは、エンタープライズ管理サーバと同じコンピュータにインストールしないでください。CA User Activity Reporting Module のシステム要件の詳細については、「CA User Activity Reporting Module リリース ノート」を参照してください。

- **CA Service Desk—r12.1**

注: このソフトウェアは、エンタープライズ管理サーバと同じコンピュータにインストールする必要はありません。CA Service Desk のシステム要件の詳細については、「CA Service Desk リリース ノート」を参照してください。

- **CA SiteMinder**

CA SiteMinder のシステム要件の詳細については、CA SiteMinder の「リリース ノート」を参照してください。

- **CA AuthMinder**

CA AuthMinder のシステム要件の詳細については、CA AuthMinder の「リリース ノート」を参照してください。

## CA ControlMinder エンドポイント管理 の要件

CA ControlMinder エンドポイント管理 コンピュータの最小要件は、以下のとおりです。

- プロセッサ - (Windows) Pentium PC 2.66 GHz
- メモリ - 2 GB の RAM
- 使用可能なディスク領域 - 2 GB (インストール ディレクトリ)、3 GB (Windows : %TEMP%、UNIX : /tmp)

さらに、以下のソフトウェアを CA ControlMinder エンドポイント管理 コンピュータにインストールします。

- **JDK** - Java Development Kit (JDK) 1.7 以降
- **アプリケーション サーバ** - JBoss Application Server バージョン 4.2.3.GA
- **CA ControlMinder** - エンドポイント インストールの最新バージョン

エンドユーザのコンピュータでは、1024 x 768 ピクセル以上の画面解像度と以下の Web ブラウザが必要です。

- **Windows** - Microsoft Internet Explorer 6.x、7.x、8.x、または Mozilla Firefox 2.x、3.0、3.5
- **Linux** - Mozilla Firefox 2.x、3.0、または 3.5

## UNIX エンドポイントの要件

CA ControlMinder UNIX エンドポイントの最小要件

- **メモリ** - 1 GB の RAM（2 GB 推奨）
- **使用可能なディスク領域** - 250 MB（標準インストールでは 300 MB）

上記のほかに、CA ControlMinder データベース用の空きディスク領域が必要です。このデータベースは、ユーザとユーザグループ、保護ファイルとその他のリソース、およびリソースに対する制限付きアクセスを許可する権限が記述されたレコードのリポジトリです。たとえば、データベースに 1,000 人のユーザ、1,000 個のファイル、500 種類のアクセスルールを格納する場合は、約 2 MB のディスク領域が必要です。

## Windows エンドポイントの要件

CA ControlMinder Windows エンドポイントの最小要件

- **プロセッサ** - Intel Pentium 4 1.6 GHz 搭載 PC
- **メモリ** - 1 GB RAM
- **利用可能なディスク領域** - 100 MB

さらに、CA ControlMinder データベース用のディスク領域も必要です。たとえば、データベースに 1,000 人のユーザ、1,000 個のファイル、500 種類のアクセスルールを格納する場合は、約 2 MB のディスク領域が必要です。

## エンタープライズ レポート機能

中央データベース (RDBMS) として Oracle Database 10g または Oracle Database 11g を使用する場合は、CA ControlMinder エンタープライズ管理をインストールする前に以下を実行します。

- Oracle ホストと CA Business Intelligence ホストが通信できることを確認します。
- CA Business Intelligence ホストに Oracle クライアント ソフトウェアをインストールします。
- CA Business Intelligence ホスト上の Oracle TNS 定義が中央データベースを指していることを確認します。

中央データベース (RDMBS) として Microsoft SQL Server 2005、Microsoft SQL Server 2008 または Microsoft SQL Server 2012 を使用する場合は、レポートサーバをインストールする前に以下を実行します。

- MS SQL ホストと CA Business Intelligence ホストが通信できることを確認します。

**重要:** レポートデータベースとして Microsoft SQL Server を使用する場合は、サポートされている Windows オペレーティング システムにレポートポータルをインストールします。

## 配布サーバの要件

配布サーバの最小要件は以下のとおりです。

- プロセッサ - Pentium 266 MHz 搭載 PC
- メモリ - 2 GB の RAM
- 使用可能なディスク領域 -- 2 GB (インストールディレクトリ)、1 GB (Windows : %TEMP%) (UNIX : /tmp) 、

さらに、配布サーバコンピュータには、以下のソフトウェアをインストールする必要があります。

- JRE - Java Runtime Environment (JRE) 1.5.0\_18 以降

## Policy Model データベースの要件

エンドポイントのディスク領域の要件に加えて、ホスト上に作成する Policy Model ごとに、追加のディスク領域も必要になります。各 Policy Model にはデータベースが含まれているため、CA ControlMinder データベースに対して行ったのと同様に、必要な領域を計算する必要があります。

すべての Policy Model データベース (PMDB) がすでに作成されている状態でアップグレードを行う場合、事前に各 PMDB が `ACInstallDir/policy_model_path/pmdb_name` ディレクトリで使用する領域を記録してください。各 PMDB をアップグレードするのに必要な追加のディスク領域を見積もるには、以下の計算式を使用します。

- `ACInstallDir/policies/pmdb_name/subscribers.dat` (サイズ) x 2
- `ACInstallDir/policies/pmdb_name/updates.dat` (サイズ) x 5 + 1000 KB

# 第 4 章: マニュアル

---

このセクションには、以下のトピックが含まれています。

[ガイド](#) (P. 29)

## ガイド

CA ControlMinder 12.8 のガイドは以下のとおりです。

- リリース ノート
- 実装ガイド
- Windows エンドポイント管理ガイド
- UNIX エンドポイント管理ガイド
- エンタープライズ管理ガイド
- 統合ガイド
- アップグレードガイド
- リファレンスガイド
- selang リファレンスガイド
- トラブルシューティングガイド

注: PDF ファイルを表示するには、PDF (Portable Document Format) 閲覧ソフトウェアをダウンロードしてインストールする必要があります。CA ControlMinder のマニュアルを表示するには、Adobe Reader 7.0.7 以降が必要です。Adobe Reader をコンピュータにインストールしていない場合は、Adobe 社の Web サイトからダウンロードしてインストールしてください。

CA ControlMinder のマニュアルは、PDF 版のガイドとしてだけでなく、HTML 形式でも提供されています。また、オンラインヘルプにはさまざまな Web ベースのインターフェースからアクセスできます。



# 第 5 章: FIPS 準拠

---

このセクションには、以下のトピックが含まれています。

[FIPS 操作モード \(P. 31\)](#)

[FIPS 専用モードでサポートされないオペレーティング システム \(P. 31\)](#)

[FIPS 暗号化ライブラリ \(P. 32\)](#)

[使用される FIPS アルゴリズム \(P. 32\)](#)

[鍵と証明書ストレージ \(P. 33\)](#)

[影響を受ける機能 \(UNIX\) \(P. 33\)](#)

[影響を受ける機能 \(Windows\) \(P. 34\)](#)

## FIPS 操作モード

CA ControlMinder には、FIPS 専用モードと通常モードの 2 種類の FIPS 操作モードがあります。FIPS 専用モードでは、CA ControlMinder は FIPS 140-2 準拠の暗号化機能のみを使用します。これは、CA ControlMinder 機能の一部は FIPS 専用モードでは無効になることを意味します。通常モードでは、CA ControlMinder は FIPS 140-2 準拠の暗号化機能と FIPS 非準拠の機能の両方を使用します。

注: FIPS 専用モードと通常モードを切り替えるには、`crypto` セクションの `fips_only` 環境設定を使用します。

## FIPS 専用モードでサポートされないオペレーティング システム

FIPS 専用モードは、以下の CA ControlMinder サポート対象オペレーティング システム アーキテクチャではサポートされていません。

- Linux s390
- Linux Itanium (IA64)
- Solaris x64
- Windows Itanium (IA64)

## FIPS 暗号化ライブラリ

FIPS 専用モードでは、CA ControlMinder は CAPKI 暗号化ライブラリを使用します。UNIX システムの場合、パスワード暗号化（「crypt」方式）用に OS の暗号化ライブラリが使用されます。通常モードでは、CA ControlMinder は非 FIPS 暗号化ライブラリに加えて CAPKI 4.1.3 暗号化ライブラリを使用します。

## 使用される FIPS アルゴリズム

CA ControlMinder コンポーネントは、以下の暗号化アルゴリズムを使用します。コンポーネントの種類が異なれば、使用されるアルゴリズムの種類も異なります。

- FIPS 専用モードの場合
  - SSL (TLS 1.0) - クライアント/サーバ通信
  - CBC モードの AES - PMD 更新ファイルの暗号化 (Windows) 、双方向パスワード履歴 (Windows)
  - SHA-1 - 単方向パスワード暗号化 (Windows) 、trusted プログラム、ポリシーのシグネチャ (拡張ポリシー管理)
- 通常モードの場合
  - CA ControlMinder r8 SP1 暗号化ライブラリ (DES、Triple DES、AES、MD5 など)
  - SSL (SSL V2、SSL V3、および TLS 1.0) - クライアント/サーバ通信
  - SHA-1 (CAPKI) - trusted プログラムのシグネチャ、ポリシーのシグネチャに対して使用
  - AES (CAPKI) - 双方向パスワード履歴の処理時のパスワード認証用に使用

## 鍵と証明書のストレージ

CA ControlMinder は、以下のように鍵と証明書を保管します。

- 対称鍵は、eTrust Access Control r8 SP1 と同様に保管されます。
- 証明書（所有者の証明書、秘密鍵、ルート証明書）はファイルシステムで保管され、CA ControlMinder によって保護されます。

注：CA ControlMinder は CA ControlMinder の対称鍵（共通鍵）を使用する AES 対称暗号化（CAPKI ライブラリ）に基づいて、秘密鍵を暗号化します。

## 影響を受ける機能 (UNIX)

FIPS 操作モードは、CA ControlMinder の以下の UNIX 向け機能に影響を及ぼす可能性があります。

機能	非 FIPS モード	FIPS モード
PMD 更新ファイル暗号化	デフォルト対称鍵暗号化（双方向）	無効
trusted プログラム	CAPKI SHA-1 および MD5	CAPKI SHA-1 のみ
双方向パスワード暗号化	デフォルト対称鍵暗号化	無効
単方向パスワード暗号化	オペレーティング システムの crypt/bigcrypt 方式	オペレーティング システムの crypt/bigcrypt 方式
PMD TNG コマンド	デフォルト対称鍵暗号化	無効
CA ControlMinder TNG デモン	デフォルト対称鍵暗号化	無効
LDAP パスワード暗号化使用 (sebuildla -u -n)	デフォルト対称鍵暗号化	無効
LDAP パスワード暗号化生成 (seldapcred)	デフォルト対称鍵暗号化	無効
TCP 通信	デフォルト対称鍵暗号化（双方向）または SSL V2、SSL V3、および TLS V1 の CAPKI ソケット	TLS V1 の CAPKI ソケット

## 影響を受ける機能 (Windows)

機能	非 FIPS モード	FIPS モード
seversion ユーティリティ	CAPKI SHA-1	CAPKI SHA-1
trusted プログラム (watchdog および seretrust)	CAPKI SHA-1	CAPKI SHA-1
拡張ポリシー管理ポリシー 配布	CAPKI SHA-1 シグネチャおよび下 位互換性用の CA ControlMinder 内部 SHA-1 シグネチャ	CAPKI SHA-1 シグネチャのみ
selogrd 暗号化	デフォルト対称鍵暗号化および MD5	無効
sechkey 鍵変更	デフォルト対称鍵暗号化	無効
iRecorder ログ ファイル シ グネチャ	MD5 暗号化	無効
レポート エージェント	有効	無効
SAM エージェント	有効	無効
DMS	有効	UNAB エンドポイント管理無効

注: FIPS 操作モードの結果としてある機能が無効になると、関連するプログラムはエラーメッセージを出力して終了するか、非対話式プロセスが発生している場合はエラーメッセージをシステムログに書き込みます。  
例: レポート エージェントまたは SAM エージェント。

## 影響を受ける機能 (Windows)

FIPS 操作モードは、CA ControlMinder の以下の Windows 向け機能に影響を及ぼす可能性があります。

機能	非 FIPS モード	FIPS モード
PMD 更新ファイル暗号化	デフォルト対称鍵暗号化 (双方 向)	CAPKI AES 対称鍵暗号化
パスワード履歴 (非双方向)	CAPKI SHA-1 として保存  CAPKI SHA-1 によるパスワード認 証、および暗号化の失敗	CAPKI SHA-1 として保存  CAPKI SHA-1 によるパスワード 認証のみ

機能	非 FIPS モード	FIPS モード
パスワード履歴 (双方向)	デフォルト対称鍵暗号化 デフォルト対称鍵暗号化による パスワード認証	CAPKI AES 対称鍵暗号化 CAPKI AES によるパスワード認 証のみ
sechkey 鍵変更、パスワード 履歴	デフォルト対称鍵暗号化による パスワード履歴の復号化および 暗号化	CAPKI AES 対称鍵暗号化による パスワード履歴の復号化および 暗号化
sechkey 鍵変更、ポリシー モデル	デフォルト対称鍵暗号化による Policy Model 更新ファイルの復号 化および暗号化	CAPKI AES 対称鍵暗号化による Policy Model 更新ファイルの復 号化および暗号化
trusted プログラム	CAPKI SHA-1 および MD5	CAPKI SHA-1 のみ
メインフレームのパスワー ド同期	有効	無効
iRecorder	有効	無効
TNG 統合	有効	無効
拡張ポリシー管理ポリシー 配布	CAPKI SHA-1 シグネチャおよび下 位互換性用の CA ControlMinder 内部 SHA-1 シグネチャ	CAPKI SHA-1 シグネチャのみ
レポート エージェント	有効	無効
SAM エージェント	有効	無効
DMS	有効	UNAB エンドポイント管理無効

注: FIPS 操作モードの結果としてある機能が無効になると、関連するプログラムはエラーメッセージを出力して終了するか、非対話式プロセスが発生している場合はエラーメッセージをシステムログに書き込みます。  
例: レポート エージェントまたは SAM エージェント。

以下の点も考慮する必要があります。

- 非 FIPS から FIPS に移行した場合、Policy Model は古いコマンドを読み取ることができなくなります。
- FIPS から非 FIPS に移行した場合、Policy Model は古いコマンドを読み取ることができます。
- 非双方向パスワード履歴では、FIPS モードで crypt を使用しない場合でも影響はありません。crypt は、下位互換性のみを目的として使用されます。
- 双方向パスワード履歴では、非 FIPS から FIPS に移行すると、CA ControlMinder では古いパスワードの復号化は実行できなくなります。

# 第 6 章：機能サポートの制限事項

---

このセクションには、以下のトピックが含まれています。

[IPv6 のサポート \(P. 37\)](#)

[Windows エンドポイントの制限事項 \(P. 37\)](#)

[UNIX エンドポイントの制限事項 \(P. 41\)](#)

[UNAB の制限事項 \(P. 43\)](#)

[SAM の制限事項 \(P. 43\)](#)

## IPv6 のサポート

CA ControlMinder は、IPv4 のみの環境、IPv6 のみの環境、または IPv4 と IPv6 両方の混在環境で動作します。

注：（UNIX）selogrd と selogrcd は、IPv6 のみの環境では動作しません。

CA ControlMinder は現在、IPv6 ネットワーク上でのネットワーク アクセス制御をサポートしていません。この結果、HOST、CONNECT、および TCP クラスに影響が及びます。

CA ControlMinder に対しては、IPv6 形式で IP アドレスを指定できます。ただし、HOSTNET クラス レコードの mask と match 部分には、IPv4 形式でアドレスを指定する必要があります。

## Windows エンドポイントの制限事項

このセクションでは、Windows エンドポイントの機能サポートの制限について説明します。

## x64 機能サポートの制限事項

以下は Windows 2003 x64 に関する既知の制限事項です。

- Unicenter TNG の移行と統合
- メインフレームのパスワード同期
- SurrogateInterceptionMode が「1」に設定されている場合の、インパーソネーションインターセプト (SURROGATE クラスの機能)

**重要:** インパーソネーションインターセプトは、デフォルトで、RunAs プラグイン (SurrogateInterceptionMode を「0」に設定) を使用して、x64、IA64 および x86 プラットフォームでサポートされています。

**注:** SurrogateInterceptionMode レジストリ設定の詳細については、「リファレンスガイド」を参照してください。

## IA64 での機能のサポート制限

以下の機能は、IA64 プラットフォームではサポートされていません。

- Unicenter TNG の移行と統合
- メインフレームのパスワード同期
- STOP
- レポート エージェント
- SAM エージェント
- SSL
- FIPS 140-2 準拠

## Windows Server 2008 機能サポートの制限事項

以下は Windows Server 2008 に関する既知の制限事項です。

- SurrogateInterceptionMode が「1」に設定されている場合の、インパーソネーションインターセプト (SURROGATE クラスの機能)

**重要:** インパーソネーションインターセプトは、デフォルトで、RunAs プラグイン (SurrogateInterceptionMode を「0」に設定) を使用して、x64、IA64 および x86 プラットフォームでサポートされています。

**注:** SurrogateInterceptionMode レジストリ設定の詳細については、「リファレンスガイド」を参照してください。

## SAN のサポート

CA ControlMinder を以下にインストールしたとき、CA ControlMinder は SAN (Storage Area Network) 環境をサポートします。

- ローカルファイルシステム。SAN に 1 つのホストからアクセス可能な場合、それを使用して SAN 上のファイルを保護します。

**注:** SAN に複数のホストからアクセス可能な場合は、SAN にアクセス可能なホストごとに CA ControlMinder をインストールし、各インストールを使用して SAN 上のファイルを保護します。

- SAN のディスク。以下の制限事項があります。
  - CA ControlMinder のドライバは、ローカルファイルシステムにインストールする必要があります。
  - コンピュータを起動または再起動するたびに、SAN のディスク上で CA ControlMinder を手動で起動する必要があります。コンピュータを起動または再起動したときに、CA ControlMinder は自動的に起動しません。

**注:** SAN ディスク上に CA ControlMinder をインストールする場合のみ、上記の条件が適用されます。ローカルファイルシステムに CA ControlMinder をインストールし、それを使用して SAN 上のファイルを保護する場合、コンピュータを再起動するたびに CA ControlMinder を手動で起動する必要はありません。

SAN が複数のホストからアクセス可能で CA ControlMinder が SAN 上にインストールされているときに、CA ControlMinder を別のホストから SAN 上の同じ場所にインストールしたい場合は、開始する前に以下を考慮してください。

- CA ControlMinder の新規インストールは CA ControlMinder の既存のインストールを置き換え、既存の CA ControlMinder 構成ファイルおよびデータベースを上書きします。
- 新規インストールを開始する前に、CA ControlMinder の既存のインストールを停止する必要があります。

## McAfee Enterecept バッファ オーバフロー

CA ControlMinder の STOP 機能は McAfee Enterecept のバッファ オーバフロー技術と互換性がありません。

CA ControlMinder の STOP 機能または McAfee Enterecept バッファ オーバフロー保護機能のどちらかを無効にしてください。

## 短いファイル名ルール(8.3 形式)がサポートされない

CA ControlMinder では、短いファイル名 (8.3 形式) として作成されたルールはサポートされません。以下のクラスのいずれかを定義する場合、ファイルまたはディレクトリの完全パス名を入力する必要があります。

FILE、PROGRAM、PROCESS、SECFILE、SPECIALPGM

以下に、完全パス名を使用したルールの例を示します。

```
nr file ("C:%program files%text.txt")
```

以下に、サポートされていない短いパス名を使用したルールの例を示します。

```
nr file ("C:%progra~1%test.txt")
```

## UNIX エンドポイントの制限事項

このセクションでは、UNIX エンドポイントの機能サポートの制限について説明します。

### HP-UX での機能のサポート制限

以下は、HP-UX オペレーティング システム上での UNAB および CA ControlMinder の既知の制限事項です。

- seversion ユーティリティで SHA-1 シグネチャが表示されません。

## HP-UX Itanium および RHEL Itanium で Unicenter 統合がサポートされない

Unicenter 統合は、HP-UX Itanium (IA64) および Red Hat Linux Itanium IA64 ではサポートされていません。

## Linux IA64 上で SAM エージェントがサポートされない

SAM エージェントは、Linux Itanium (IA64) 上ではサポートされていません。インストール時の選択にかかわらず、CA ControlMinder は SAM エージェントをこれらのオペレーティングシステム上にインストールしません。

注: UNAB は Linux IA64 上でもサポートされていません。

## SAN のサポート

ローカルファイルシステムに CA ControlMinder をインストールし、SAN 上のファイルを保護するためにそれを使用する場合、また CA ControlMinder がインストールされた単一ホストから SAN にアクセス可能な場合に CA ControlMinder は SAN (storage area network) 環境をサポートします。

注: SAN に複数のホストからアクセス可能な場合、SAN にアクセス可能なホストごとに CA ControlMinder をインストールし、各インストールを使用して SAN 上のファイルを保護します。

SAN が複数のホストからアクセス可能で CA ControlMinder が SAN 上にインストールされているときに、CA ControlMinder を別のホストから SAN 上の同じ場所にインストールしたい場合は、開始する前に以下を考慮してください。

- CA ControlMinder の新規インストールは CA ControlMinder の既存のインストールを置き換え、既存の CA ControlMinder 構成ファイルおよびデータベースを上書きします。
- 新規インストールを開始する前に、CA ControlMinder の既存のインストールを停止する必要があります。

注: CA ControlMinder を SAN 上にインストールし、CA ControlMinder が接続されている複数のホストから CA ControlMinder を実行したときの動作は不明です。

## UNAB の制限事項

このセクションでは、UNAB エンドポイントの機能サポートの制限について説明します。

### 一方向の信頼関係を持つドメイン環境でのアカウントパスワード形式

uxconsole ユーティリティを使用して、登録ドメインとは異なるドメインの Active Directory アカウントパスワードを変更する場合、以下のコマンド形式を使用する必要があります。

```
uxconsole -krb -passwd user@DOMAIN
```

**重要:** ドメイン名は大文字で表記する必要があります。

### UNAB が Linux IA64 上でサポートされない

現在、Linux IA64 オペレーティングシステム上に UNAB をインストールすることはできません。

### UNAB が FIPS140-2 および IPV6 に対応していない

現在、UNAB は FIPS140-2 および IPV6 に対応していません。

## SAM の制限事項

このセクションでは、SAM エンドポイントおよびサーバコンポーネントの機能サポートの制限について説明します。

### SAM が FIPS140-2 および IPV6 に対応していない

現在、SAM は FIPS140-2 および IPV6 に対応していません。



# 第 7 章: インストールに関する考慮事項

---

このセクションには、以下のトピックが含まれています。

[サポートされるインストール言語 \(P. 46\)](#)

[Windows エンドポイントに関する考慮事項 \(P. 46\)](#)

[UNIX エンドポイントに関する考慮事項 \(P. 47\)](#)

[UNAB エンドポイントインストールに関する考慮事項 \(P. 49\)](#)

[サーバ コンポーネントのインストールに関する考慮事項 \(P. 49\)](#)

## サポートされるインストール言語

エンタープライズ管理サーバと CA ControlMinder のインストールに使用される言語を指定できます。以下の言語 ID はサポート対象になっているので、それに対応する言語を指定できます。

エンタープライズ管理サーバは、以下の言語をサポートします。

- 1033 - 英語
- 1041 - 日本語
- 1042 - 韓国語
- 2052 - 中国語（簡体字）
- 1031 - ドイツ語
- 1040 - イタリア語
- 1036 - フランス語
- 1046 - ポルトガル語（ブラジル）
- 1034 - スペイン語

注: CA ControlMinder レポートを生成できるのは、英語、日本語および韓国語でのみです。

CA ControlMinder for Windows、CA ControlMinder for UNIX および UNAB は、以下の言語をサポートします。

- 1033 - 英語
- 1041 - 日本語
- 1042 - 韓国語
- 2052 - 中国語（簡体字）

## Windows エンドポイントに関する考慮事項

このセクションでは、Windows エンドポイントへの CA ControlMinder のインストール時に考慮する必要がある項目について説明します。

## Windows Server 2008 上でのインストール、アンインストール、アップグレード時に再起動メッセージが表示される

Windows Server 2008 上で CA ControlMinder のインストール、アンインストール、アップグレードを行う場合、プロセス完了後に再起動が必要なことを通知するダイアログボックスが表示されます。続行するには、[OK] を選択してダイアログボックスを閉じます。

## UNIX エンドポイントに関する考慮事項

このセクションでは、UNIX エンドポイントへの CA ControlMinder のインストール時に考慮する必要がある項目について説明します。

### AIX 6.1 では、CA ControlMinder の起動に TL3 以降が必要です。

#### AIX 6.1 に該当

CA ControlMinder を AIX 6.1 にロードするには、TL3 以降がインストールされていることを確認します。

### Linux390 のメッセージ キューに J2SE バージョン 5.0 が必要

Linux s390 および s390x エンドポイント上でメッセージキュー機能を使用するには、J2SE バージョン 5.0 以降がエンドポイントにインストールされていることを確認します。メッセージキュー機能によって、レポートデータをレポートポータルへ送信し、監査データを CA User Activity Reporting へ送信することができます。

**注:** accommon.ini ファイル内の java\_home 環境設定を設定する必要がある場合があります。詳細については、「実装ガイド」を参照してください。

## x86\_64bit Linux の互換性ライブラリがない

デフォルトでは、インストール時に、x86\_64 Linux オペレーティングシステムに 32 ビットの互換性ライブラリが含まれるべきではありません。CA ControlMinder エンドポイントでは、ライブラリ `libstdc++.so.6` が rpm `libstdc++` の `usr/lib` ディレクトリに存在する必要があります。

CA ControlMinder をインストールする前に、このライブラリがエンドポイント上に存在することを確認してください。

## CA ControlMinder をインストールまたはアンインストールすると UNAB が再起動する

UNAB が実行されているエンドポイントから CA ControlMinder をインストールまたはアンインストールすると、UNAB エージェント (`uxauthd`) が停止され、開始されます。

## CA ControlMinder および UNAB を新しい Solaris ゾーンへ伝達

新しい Solaris ゾーンを設定した場合、ネイティブ オペレーティングシステムがパッケージのインストール後の要素を完全に伝達および実行し、ユーザが CA ControlMinder および UNAB を新しいゾーンに伝達する前に、インストール後の手順をいくつか実行する必要があります。

注: 新しいゾーンの正しい設定方法の詳細については、Sun の「[System Administration Guide: Solaris Containers--Resource Management and Solaris Zones](#)」を参照してください。このドキュメントは Sun Microsystems Documentation の Web サイトにあります。

## CA ControlMinder を Solaris 11 にインストールする際の制限事項

Solaris 11 における制限のために、CA ControlMinder パッケージはインストール中に非グローバル ゾーンには追加されません。Solaris ネイティブパッケージング ツール (`pkgadd`) を使用して、各ゾーンへ個別に CA ControlMinder をインストールすることをお勧めします。

## UNAB エンドポイント インストールに関する考慮事項

このセクションでは、UNAB エンドポイントのインストール時に考慮する必要がある項目について説明します。

### UNAB for Linux 390 のリモート管理用に J2SE バージョン 5.0 が必要

Linux s390 および s390x エンドポイントをリモートで管理するには、J2SE バージョン 5.0 以降がエンドポイントにインストールされていることを確認します。リモート管理では、CA ControlMinder エンタープライズ管理を使用して UNAB エンドポイントを管理できます。

注: accommon.ini ファイル内の java\_home 環境設定を設定する必要がある場合があります。詳細については、「実装ガイド」を参照してください。

## サーバコンポーネントのインストールに関する考慮事項

このセクションでは、サーバコンポーネント（エンタープライズ管理サーバ、CA ControlMinder エンドポイント管理 および Enterprise Reporting）をインストールする際に考慮する必要がある項目について説明します。

### エンタープライズ管理サーバを Red Hat Linux 6 にインストールするには 32 ビットパッケージが必要

Red Hat Linux 6 で該当

エンタープライズ管理サーバを Red Hat Linux 6 にインストールする前に以下を行う必要があります。

1. 最小ハードウェア要件である 4 GB の RAM および 4 GB のスワップ領域が使用可能であることを確認します。
2. 以下のパッケージをインストールします。  
audit-libs、compat-libstdc++、glibc、libgcc、libSM、libXext、LibXp、LibXt、ncurses、pam、libstdc++、Ksh、dos2unix

### rpm --requires -- ライブラリの依存関係を検出

エンタープライズ管理を Linux にインストールする場合、CAeAC パッケージが依存するライブラリを知る必要があります。

このコマンドは、以下の構文を使用します。

```
rpm -qp --requires package
```

コマンドのパラメータは以下のとおりです。

-q

RPM パッケージ情報を照会することを指定します。

-p

RPM パッケージファイルを照会します。インストールされていないパッケージの情報も取得します。

--requires package

パッケージによって必要とされる依存関係を取得します。

### 例

CA ControlMinder 12.8 SP0 の依存関係情報を取得したい場合：

```
root> rpm -qp --requires CAeAC-1280-0.0.1275.i386.rpm
rpm >= 4.0
libcrypt.so.1
libc.so.6
libdl.so.2
libgcc_s.so.1
libm.so.6
libnsl.so.1
libpam.so.0
libpthread.so.0
libresolv.so.2
libstdc++.so.6
rpmLib(PayloadFilesHavePrefix) <= 4.0-1
rpmLib(CompressedFileNames) <= 3.0.4-1
```

一覧表示されたパッケージについて 1 つずつ rpm コマンドの実行を継続し、さらなる依存関係を取得します。

```
root> rpm -qp --requires libcrypt
```

詳細情報：

[rpm --whatprovides -- ライブラリが存在することを確認 \(P. 51\)](#)

## rpm --whatprovides -- ライブラリが存在することを確認

エンタープライズ管理を Linux にインストールする前に、すべての必要なライブラリがターゲットシステムに存在することを確認します。

このコマンドは、以下の構文を使用します。

```
rpm -q --whatprovides capability
```

コマンドのパラメータは以下のとおりです。

**-q**

RPM パッケージ情報を照会することを指定します。

**--whatprovides capability**

特定の機能をどのパッケージが提供しているかに関する情報を取得することを指定します。

### 例: ライブラリがインストールされていることを確認

この例では、`libcrypt.so.1` がインストールされていることを確認します。正の回答（\$? が 0）を受信した場合、`libcrypt.so.1` を提供するのが `glibc-2.5-42` パッケージであることがわかります。

```
root> rpm -q --whatprovides libcrypt.so.1
glibc-2.5-42
root> echo $?
0
```

### 例: ライブラリがインストールされていないことを検出

この例では、`libexample.so.1` がインストールされているかどうかを確認したいとします。負の回答（\$? が 1）を受信した場合、この機能を提供するパッケージがインストールされていないこととなります。

```
root> rpm -q --whatprovides libexample.so.1
libexample.so.1 を提供するパッケージはありません
root> echo $?
1
```

必要なライブラリがない場合は、インストールを続行する前にライブラリをインストールしてください。

詳細情報:

[rpm --requires -- ライブラリの依存関係を検出 \(P. 50\)](#)

## CA ControlMinder の Linux へのインストール時に Libc ライブラリがない

### 症状:

ネイティブ Linux パッケージを使用して CA ControlMinder をインストールすると、以下のエラーメッセージで失敗します。

バイナリ ファイルは実行できません。

理由: プラットフォームが一致しないか、一部の必要なライブラリがありません。

アクション: 正しいシステム ライブラリ (**libc**) が使用されていることを確認してください。

### 解決方法:

Linux への CA ControlMinder インストールでは、システムアーキテクチャに関係なく、32 ビットの **libc** ライブラリが **libpath** にインストールおよび設定されている必要があります。Linux システムが、32 ビットバージョンの **libc** がない 64 ビットの最小インストールである場合、インストールは失敗します。

32 ビットバージョンの **libc** をインストールして、インストールを再実行してください。

## RDP ハードニングの未サポート

CA ControlMinder は、RDP ハードニング サーバコンポーネント構成をサポートしません。 [常にパスワードの入力を求める] オプションが含まれる展開済みハードニング ポリシーが選択されている場合、PUPM の自動ログインは動作しません。

## 同じタイムゾーンへのプライマリおよび負荷分散エンタープライズ管理サーバのインストール

高可用性を目的にエンタープライズ管理サーバを設定する場合は、同じタイムゾーンにプライマリおよび負荷分散サーバの両方がインストールされることを確認します。

## 64 ビット Linux へのエンドポイント管理のインストール

64 ビットの Linux サーバにエンドポイント管理をインストールするには、32 ビットバージョンの CA ControlMinder エンドポイント管理をインストールします。エンドポイント管理が 32 ビットの Web サービスをインストールするため、32 ビットバージョンが必要です。

## 管理者名の特殊文字

Windows で有効

管理アカウントユーザ名に特殊文字を使用することはできません。例: '!' 文字。

## サポートされている JDK および JBoss のバージョン

CA ControlMinder Third Party Components DVD 上に、サポートされている JDK および JBoss のバージョンがあります。

## 前提条件キット インストーラの考慮事項

CA ControlMinder エンタープライズ管理の DVD を挿入するように要求された後で、前提条件キット インストーラユーティリティを使用してメディアから CA ControlMinder エンタープライズ管理をインストールする際、続行するには [完了] を選択する必要があります。さらに、DVD を挿入した際に表示された ProductExplorer のウィンドウを閉じなければならない場合があります。

## サーバコンポーネントのインストールにはスーパーユーザのアカウントが必要

CA ControlMinder サーバコンポーネント（エンドポイント管理およびエンタープライズ管理など）のいずれかをインストールするには、スーパーユーザ（UNIX では root、Windows では Administrator グループ）としてログインする必要があります。

## Java が見つからない場合、インストール時に RDBMS 接続が失敗する

CA ControlMinder エンタープライズ管理 のインストール時に、CA ControlMinder エンタープライズ管理 が RDBMS への接続を試みると、接続障害が発生する場合があります。この原因として、`java.exe` が見つからなかったことが挙げられます。

`java.exe` のフルパス名がシステムの PATH 環境変数に指定されていることを確認してください。

## エンタープライズ管理サーバ インストールがインストール パス中のスペースをサポートしない

### UNIX に該当

エンタープライズ管理サーバをインストールするとき、インストールパス中にスペースを入れないでください。

## 別のドメインの Active Directory を使用できるように CA ControlMinder エンタープライズ管理 をセットアップ

使用する Active Directory が CA ControlMinder エンタープライズ管理 をインストールしたドメイン外にある場合、ホストの TCP/IP 設定を変更する必要があります。

### 別のドメインの Active Directory を使用できるように CA ControlMinder エンタープライズ管理 をセットアップする方法

#### Windows 側

1. [スタート] - [設定] - [コントロール パネル] - [ネットワーク接続] を選択します。  
[ネットワーク接続] ウィンドウが開きます。
2. アクティブなネットワーク接続を右クリックし、[プロパティ] をクリックします。  
[全般] タブが開いた状態で、[プロパティ] ダイアログ ボックスが開きます。

3. [Internet Protocol (TCP/IP)] を選択して、[プロパティ] をクリックします。  
[Internet Protocol (TCP/IP) のプロパティ] ダイアログ ボックスが表示されます。
4. Click Advanced and click the DNS tab in the open dialog.kakko [詳細設定] をクリックし、開いたダイアログ ボックスで [DNS] タブをクリックします。  
[TCP/IP 詳細設定] ダイアログ ボックスが表示されます。
5. [追加] をクリックして、Active Directory があるドメインの DNS サーバの IP アドレスを入力します。
6. [以下の DNS サフィックスを順に追加する] を選択し、[追加] をクリックして、サフィックスを追加します。  
[TCP/IP ドメイン サフィックス] ダイアログ ボックスが表示されます。
7. ドメイン サフィックスを入力します。  
例 : *company.com*
8. 開いているすべてのダイアログ ボックスで [OK] をクリックして変更内容を確認し、終了します。

#### UNIX の場合

Active Directory が存在するドメインの DNS サーバ名が正しい値に設定されていることを確認します。

DNS ドメイン名を検証するには、`/etc/resolv.conf` ファイルを開いてドメインが適切な値に設定されていることを確認します。

## CA ControlMinder エンドポイント管理 インストール手順が CA ControlMinder の両方に該当

「実装ガイド」の「CA ControlMinder エンドポイント管理のインストール」の章で説明されている CA ControlMinder エンドポイント管理のインストール手順は、CA ControlMinder と CA ControlMinder の両方に該当します。CA ControlMinder エンドポイント管理をインストールする CA ControlMinder 以外のユーザはこれらの手順に従い、プレミアムではないサーバの DVD を使用する必要があります。

## ポート番号 8080 への CA ControlMinder エンドポイント管理 のショートカット

デフォルトでは、CA ControlMinder エンドポイント管理 インストーラはショートカットをポート番号 8080 に設定します。デフォルト設定を変更するには、CA ControlMinder エンドポイント管理 インストーラを、ProductExplorer からではなく CA ControlMinder の DVD から直接実行する必要があります。

以下のコマンドラインを使用して、CA ControlMinder エンドポイント管理をインストールする際に使用するポートを定義します。

```
install_EM.exe -DJB055_PORT=<18080>
```

または、インストール後に、CA ControlMinder エンドポイント管理のショートカットを編集して別のポートを指定できます。

## CA User Activity Reporting Module では trusted SSL 接続のみサポートされる

CA User Activity Reporting Module サーバの接続設定を定義する際に、SSL 接続設定を定義します。CA User Activity Reporting Module では SSL 以外の接続をサポートしません。

**注:** CA User Activity Reporting Module との統合については、「*実装ガイド*」を参照してください。

## CA ControlMinder エンタープライズ管理 から CA User Activity Reporting Module レポートを表示するには特殊なサブスクリプションが必要

CA ControlMinder エンタープライズ管理 インターフェースから CA User Activity Reporting Module レポートを表示するには、特殊なサブスクリプション更新を CA User Activity Reporting Module サーバに適用します。

### サブスクリプション更新の適用方法

1. CA User Activity Reporting Module で、[管理] タブ、[サービス] サブタブをクリックし、[サブスクリプション モジュール] を選択します。
2. 以下の RSS フィード URL を指定します。

`http://securityupdates.ca.com/CA-ELM/r12/OpenAPI/RSSFeed.xml`

3. すべてのモジュールをダウンロードし、CA User Activity Reporting Module へ適用します。

これで、CA User Activity Reporting Module レポートを CA ControlMinder エンタープライズ管理 から表示できるようになります。

## CA ControlMinder エンタープライズ管理 およびレポート ポータル コンピュータのシステム時刻の同期

レポート ポータルを CA ControlMinder エンタープライズ管理 とは別のコンピュータにインストールする場合、コンピュータのシステム時刻を同期する必要があります。システム時刻を同期しない場合、CA ControlMinder エンタープライズ管理 が生成するレポートのステータスが保留または循環のままになります。

## スーパーユーザ以外ではインストールが失敗する

いずれかの CA ControlMinder サーバコンポーネント (エンドポイント管理 およびエンタープライズ管理など) をアンインストールするには、スーパーユーザ (UNIX では root、Windows では Administrator) としてログインする必要があります。スーパーユーザとしてログインしていなければ、アンインストールは失敗します。



# 第 8 章: アップグレードに関する留意事項

---

このセクションには、以下のトピックが含まれています。

[アップグレード元のバージョン \(P. 59\)](#)

[Windows エンドポイントのアップグレードに関する考慮事項 \(P. 60\)](#)

[UNIX エンドポイントのアップグレードに関する考慮事項 \(P. 60\)](#)

[サーバコンポーネントのアップグレードに関する考慮事項 \(P. 62\)](#)

## アップグレード元のバージョン

CA ControlMinder エンドポイントを以下のバージョンから **12.8** にアップグレードできます。

- 12.7
- 12.6.02
- 12.6.01
- 12.6
- 12.5.5
- 12.5 SP4
- 12.5 SP3

CA ControlMinder エンドポイントを以下のバージョンから **12.8** にアップグレードすることはできません。

- 8.0 SP1 GA

8.0 SP1 GA エンドポイントをアップグレードするには、**12.8** にアップグレードする前に、**8.0 SP1** 用の最新の **CR** をインストールします。

- 5.2 および 5.3

5.2 または 5.3 エンドポイントをアップグレードするには、**12.8** にアップグレードする前に、**8 SP1** 用の最新の **CR** をインストールします。

## Windows エンドポイントのアップグレードに関する考慮事項

このセクションでは、Windows エンドポイント上で CA ControlMinder をアップグレードする際に考慮する必要がある項目について説明します。

### データベースへのデフォルト アクセスの変更

seosdb (CA ControlMinder データベース) へのデフォルト アクセスは「none」です。r12.5 SP2 以前では、データベースへのデフォルト アクセスは読み取りでした。

**注:** CA ControlMinder 内部プロセスはデータベースにフルアクセスできます。また、NT AUTHORITY¥System ユーザはデータベースに読み取りアクセスできます。

## UNIX エンドポイントのアップグレードに関する考慮事項

このセクションでは、UNIX エンドポイント上で CA ControlMinder をアップグレードする際に考慮する必要がある項目について説明します。

### デフォルトのインストール場所

デフォルトのインストール場所は、r12.0 で以下のように変更されています。

```
/opt/CA/AccessControl
```

### FIPS 140-2 ライブラリのアップグレード

CA ControlMinder の本リリースでは、ETPKI 3.2 の代わりに CAPKI 4.1.2 が使用されます。アップグレードは自動的に実行され、コンピュータ上の ETPKI 3.2 ライブラリは他のコンポーネントで使用されている場合は保持されます。他のコンポーネントで ETPKI 3.2 が使用されているかどうかを判別するために、CAPKI では内部参照カウントが使用されます。このカウントが 0 のとき、ETPKI 3.2 はアップグレード時にアンインストールされます。

## UNIX でのシステム全体の監査モードのアップグレード

SEOS クラスの `SYSTEM_AAUDIT_MODE` プロパティでは、ユーザおよびエンタープライズユーザのデフォルト監査モード（システム全体の監査モード）を指定します。CA ControlMinder r12.5 SP1 以降にアップグレードすると、CA ControlMinder は `SYSTEM_AAUDIT_MODE` プロパティの値を `lang.ini` ファイルの `[newusr]` セクションにある `DefaultAudit` 設定の値に設定します。

注: `SYSTEM_AAUDIT_MODE` プロパティおよび `DefaultAudit` 設定の両方のデフォルト値は、`Failure LoginSuccess LoginFailure` です。

## 認証でのリソース グループの所有権の認識

CA ControlMinder では、リソースに対するユーザ認証をチェックするときに、リソース グループの所有権が考慮されます。これは、r12.0 で導入されました。以前のリリースでは、認証プロセスではリソースの所有者のみが考慮されていました。

たとえば、FILE リソースはデフォルト アクセスの `none` および指定された所有者のいる GFILE リソースのメンバである所有者なしで定義します。CA ControlMinder r12.0 以降では、指定されたグループ所有者にそのファイルの完全なアクセス権が与えられます。以前のリリースでは、誰にもそのファイルのアクセス権が与えられていませんでした。

## 優先度が下げられた syslog メッセージ

以下の syslog メッセージの優先度が、情報に下げられました（ERROR ではなく INFO）。

- CA ControlMinder デーモンが停止します。
- START-UP: CA ControlMinder PID=%d
- SEOS\_load: use\_streams=\$use\_streams unload\_enable=\$unload\_enable
- CA ControlMinder カーネル拡張をロードしています。
- \$prodname のカーネル拡張はすでにロードされています。
- \$SeosBinDir/seosd デーモンを開始しています。(CA ControlMinder)
- Watchdog を起動しました。
- Watchdog の拡張機能が初期化されました。

## サーバコンポーネントのアップグレードに関する考慮事項

このセクションでは、サーバコンポーネント（エンタープライズ管理サーバ、CA ControlMinder エンドポイント管理、および Enterprise Reporting）をアップグレードする際に考慮する必要がある項目について説明します。

### 12.8 エンタープライズ管理サーバには 12.8 配布サーバが必要

エンタープライズ管理サーバを 12.8 にアップグレードした場合、その配布サーバも 12.8 にアップグレードする必要があります。

### 12.6 から 12.8 にアップグレードするための要件

エンタープライズ管理環境には配布サーバホストが含まれている場合、リリース 12.8 にアップグレードする前に以下の手順に従います。

次の手順に従ってください：

1. エンタープライズ管理データベースにログインします。
2. ENDPOINT というテーブルを参照します。
3. FRIENDLY\_NAME 列を参照し、配布サーバホスト名が重複していないことを確認します。

ホスト名が重複している場合は、2つの行の1つを削除します。

### エンタープライズ管理サーバを r12.7 にアップグレードすると、ロールおよびタスクが保持されない

エンタープライズ管理サーバを 12.7 にアップグレードする際に、アップグレード前に作成されたロールおよびタスクは保持されません。

エンタープライズ管理サーバは、メンバシップポリシーのみを保持します。

## CA ControlMinder r12.6 では、CA ControlMinder r12.5 および r12.0.01 での Policy Model の管理に対してホットフィックスが必要です。

CA ControlMinder 12.7 サーバを使用して CA ControlMinder r12.5 または r12.0.01 上の Policy Model を管理している場合は、以下のホットフィックスをインストールします。

- r12.5 のエンドポイントについては、ホットフィックス T537526 をインストールします
- r12.0.01 のエンドポイントについては、ホットフィックス T537569 をインストールします

注: 詳細については、CA サポート (<http://www.ca.com/jp/support/>) までお問い合わせください。

## ポリシーをエンドポイントにデプロイするために必要なソフトウェア パッチ

CA ControlMinder エンタープライズ管理 r12.6 から CA ControlMinder r12.5 エンドポイント上にポリシーをデプロイするには、パッチ T537526 をエンタープライズ管理サーバにインストールする必要があります。

ソフトウェア パッチを [CA サポートの Web サイト](#) からダウンロードします。



# 第 9 章：一般的な考慮事項

---

このセクションには、以下のトピックが含まれています。

[Windows エンドポイントに関する考慮事項 \(P. 65\)](#)

[UNAB に関する考慮事項 \(P. 65\)](#)

[サーバコンポーネントに関する考慮事項 \(P. 69\)](#)

## Windows エンドポイントに関する考慮事項

このセクションでは、Windows エンドポイント上で CA ControlMinder を使用する際に考慮すべき事項について、説明します。

### Windows Server 2008 で管理者として実行による CA ControlMinder の開始

Windows Server 2008 に該当

ユーザアカウントコントロール (UAC) オプションが有効になっている場合、コマンドラインオプション (seload -start) を使用して CA ControlMinder を開始するには、管理者権限が必要です。RunAs オプションを使用して、コマンドプロンプトを実行し、管理者権限のあるユーザアカウントを指定します。

### アンインストールで CA ライセンス ファイルが削除されない

CA ControlMinder をアンインストールしたとき、CA ライセンス ファイルが削除されません。デフォルトでは、CA ライセンス ファイルは CA\_license ディレクトリ (たとえば、C:\Program Files\CA\SharedComponents\CA\_LIC など) にあります。

## UNAB に関する考慮事項

このセクションでは、UNAB を使用する際に考慮すべき事項について説明します。

## SELinux が有効な場合に、ログイン時にホーム ディレクトリが作成されない

Linux で該当

症状:

SSH クライアントを使用して Linux ホストにログインすると、SELinux が有効な場合、アカウントのホーム ディレクトリが作成されません。

解決方法:

SSH クライアントを使用してログインを試行すると、ホーム ディレクトリは作成されません。この問題を回避するには、次の操作を行ってください。

1. `password-auth` ファイルを開きます。このファイルは、デフォルトで以下のディレクトリにあります。

```
¥etc¥pam.d¥
```

2. `session` セクションを見つけます。
3. `pam_uxauth` セクションの前に以下の行を追加します。

```
session required pam_makehomedir.so
```

4. ファイルを保存して閉じます。

## パスワード変更の試行が Red Hat Linux 上で失敗する

Red Hat Linux で有効

症状:

パスワードの変更を求められたとき、パスワード変更プロセスが完了した後、ホストでの作業を続行できません。SSH クライアントまたは Telnet を使用してログインすると、この問題が発生します。

解決方法:

この問題を解決するには、アカウントパスワードを変更し、ホストをログアウトしてから、新しいパスワードでログインします。

## 移行後のローカル ユーザ アカウントの無効化

ユーザ アカウントを Active Directory に完全に移行した後、`/etc/passwd` ファイルのアカウント エントリの先頭にアスタリスク (\*) を追加することによって、ローカルの UNIX アカウントを無効にすることができます。

## `unab_refresh_interval` トークンの値は短い間隔に設定しない

UNAB でパフォーマンス上の問題が発生するのを避けるため、`unab_refresh_interval` トークン値を短い間隔に設定しないようにしてください。

## Kerberos `dns_lookup_realm` を True に設定しない

SSO モードに該当

必須でない限り、Kerberos `dns_lookup_realm` の値を `true` に設定しないことをお勧めします。True に設定した場合、Kerberos は UNAB ログインプロセスの実質的な遅延の原因となる、不要な DNS 検索を開始します。

## UNAB ユーザが指定されたパスワード ポリシーに従ってアカウント パスワードを変更できない

UNAB ユーザがアカウント パスワードを変更できない場合、使用するドメイン コントローラのセキュリティ ポリシーで、それらのアカウント パスワードの変更が禁止されていないことを確認します。

## sepass と UNAB エンドポイントの統合

sepass ユーティリティは UNAB と統合されます。この統合によって、CA ControlMinder および UNAB の両方がインストールされているエンドポイント上で、ユーザが自分の Active Directory パスワードを変更することが可能になります。

sepass と UNAB を統合する方法

- seos.ini ファイルで、"change\_pam" トークンの値が **yes** に設定されていることを確認します。このトークンを設定して、sepass では PAM インターフェースを使用してパスワードが変更されるようにします。
- seos.ini ファイルで、"auth\_login" トークンの値が **pam** に設定されていることを確認します。このトークンを設定して、sepass では PAM インターフェースを使用して既存のパスワードが検証されるようにします。

**注:** seos.ini 初期化ファイルのトークンの詳細については、「リファレンスガイド」を参照してください。

## Active Directory アカウントを使用した UNAB へのログイン

以前はローカルホストに存在しなかった Active Directory アカウントを使用して UNAB にログインする場合、以下の手順に従います。

1. UNAB ホストを Active Directory に、以下のように登録します。

```
uxconsole -register
```

2. UNAB を以下のようにアクティブ化します。

```
uxconsole -activate
```

3. UNAB ログイン認可 (ログインポリシー) またはローカルログインポリシー (users.allow、users.deny、groups.allow、groups.deny) を作成して、Active Directory ユーザがログインできるようにします。

## UNAB がインストールされている場合、管理者アカウントを使用して CA ControlMinder for UNIX にログインできない

UNAB がエンドポイントにインストールされている場合、Active Directory の「管理者」アカウントを使用して、UNIX 用 CA ControlMinder エンドポイントにアクセスできません。この問題を回避するには、このアカウント用に userPrincipleName を作成します。

## サーバコンポーネントに関する考慮事項

このセクションでは、CA ControlMinder のサーバコンポーネント（CA ControlMinder エンドポイント管理、CA ControlMinder エンタープライズ管理、およびエンタープライズレポート）使用時に考慮すべき事項について説明します。

### CA ControlMinder コンポーネントと CA ControlMinder メッセージキューの間の通信の問題

以下の CA ControlMinder コンポーネントは、その機能の一部に関して、CA ControlMinder メッセージキューとの通信に依存しています。

- エンタープライズ管理サーバ
- レポートエージェント
- DMS
- DH
- UNAB
- SAM パスワードコンシューマ
- エージェントマネージャ

メッセージキューが実行されていない場合、メッセージキューのホストまたはキューの設定オプションが正しく設定されていない場合、または一般的なネットワークエラーが発生した場合、これらのコンポーネントはメッセージキューと通信できない場合があります。

これらのコンポーネントのいずれかとメッセージキューの間の通信が確立できないか、接続が解除された場合、問題が解決されても、通信は自動的に再確立されません。この問題を回避するには、まず通信の問題を解決し、次に CA ControlMinder コンポーネントを再起動する必要があります。

## Oracle でのアップグレード

Oracle データベースでアップグレードが実行される前に、以下の手順に従って、記録されているコマンドを Oracle 上で実行します。

1. コマンドラインからの **SQLPLUS** のオープン
2. データベースに接続します。
3. システムまたは **sysdba** ユーザとしてログインします。

4. 以下のコマンドを実行します。

```
GRANT EXECUTE ON SYS.DBMS_CRYPT0 TO vpm20;  
GRANT UNLIMITED TABLESPACE TO vpm20;  
ALTER SYSTEM SET transactions=275 SCOPE=SPFILE;  
ALTER SYSTEM SET sessions=250 SCOPE=SPFILE;  
ALTER SYSTEM SET processes=200 SCOPE=SPFILE;
```

## CA ControlMinder ホスト名の制約

CA ControlMinder エンドポイントのホスト名は 15 文字以下である必要があります。CA ControlMinder コンピュータのホスト名が 15 文字を超える場合、CA ControlMinder エンドポイント管理を使用してエンドポイントにログインすることはできません。

## ポリシー デプロイ解除スクリプトの自動生成

デプロイ解除スクリプトが関連付けられていないポリシーをデプロイ解除すると、CA ControlMinder はポリシーを削除するために必要なスクリプトを自動的に生成します。このスクリプトは、デプロイ スクリプトに基づいています。

ポリシーを削除する一方で、(デプロイ スクリプトの) ポリシー ルールを保持する必要がある場合は、何も変更しないルール (たとえば、**er GPOLICY policyName**) を含むデプロイ解除スクリプトを作成します。

## DNSドメイン名ではなく、SAM エンドポイント NETBIOS 名を指定する

CA ControlMinder エンタープライズ管理 で SAM エンドポイントを作成する場合、名前フィールドで指定するホスト名は、ワールド ビューに表示されるホスト名と一致させる必要があります。

エンドポイントが **Active Directory** エンドポイントである場合は、[ホストドメイン] フィールドに **NETBIOS** ドメイン名を指定します。エンドポイントが **Active Directory** エンドポイントではない場合は、**DNS** ドメイン名ではなく **NETBIOS** ホスト名を [ホストドメイン] フィールドに指定します。たとえば、エンドポイントが **Active Directory** エンドポイントではない場合は、エンドポイント **DNS** ドメイン名 (acserver.company.com) ではなく、**NETBIOS** ホスト名 (**ACSERVER**) を [ホストドメイン] フィールドに指定します。

**DNS** ドメイン名を指定すると、**SAM** 自動ログインなどの高度な機能は失敗します。

ログインアプリケーションスクリプトを使用して、ドメインのメンバにログオンします。

**症状:**

CA ControlMinder エンドポイント管理 ログインアプリケーションスクリプトを使用して、ドメインのメンバであるサーバにログインする際に、FTP にログインできますが、FTP ユーザ コマンドに "未接続" と表示されます。

**解決方法:**

FTP と PuTTY は、ドメインユーザをサポートしません。自動ログインアプリケーションスクリプトを使用して、ドメインメンバであるサーバへの FTP および PuTTY 自動ユーザログインを有効にできません。FTP または PuTTY を使用して、ドメインメンバサーバにログインするパスワードをチェックアウトするには、新しい自動ログインスクリプトを作成します。

**次の手順に従ってください:**

1. サーバに FTP または PuTTY スクリプトを配置します。
2. FTP または PuTTY スクリプトをコピーします。
3. 既存のスクリプトに基づいて、別のログインアプリケーションスクリプトを作成します。
4. ユーザ名およびドメイン属性をすべて指定して、スクリプトを以下のように変更します。

```
userName = "#userName#"
```

```
userDomain = "#userDomain#"
```

```
password = "#password#"
```

```
serverName = "#host#"
```

```
fullUserName = userDomain & "¥" & username
```

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
```

```
hwnd = pupmObj.LaunchPUTTY(serverName, fullUserName, password)
```

5. 新しいログインアプリケーションをエンドポイントへ割り当てます。

自動ログインアプリケーションスクリプトの詳細については、「SAM 自動ログインアプリケーション Visual Basic スクリプト」を参照してください。

## 複数の CA IdentityMinder プロビジョニング コネクタ サーバを設定できない

CA ControlMinder エンタープライズ管理 では、複数の CA IdentityMinder プロビジョニング コネクタ サーバを設定しないでください。

## SSL ポートを使用して CA IdentityMinder プロビジョニング コネクタ サーバを設定できない

CA IdentityMinder プロビジョニング サーバを設定する際は、CA IdentityMinder プロビジョニング サーバの SSL ポート (20390) を指定しないでください。コネクタ サーバの SSL ポートを指定すると、コネクタ サーバへの接続に失敗します。

## SAM を使用してエキスパート アカウントのパスワードを変更できない

SSH エンドポイント上で Check Point ファイアウォールを使用する場合、エンドポイント上で SAM を使用してエキスパート アカウントのパスワードを変更することはできません。これは、エキスパート アカウントは SAM で接続が切断されている必要があることを意味します。

## SQLCMD ユーティリティが空のパスワードをサポートしない

### SQL Server に該当

SQL Server コマンドユーティリティ sqlcmd は、空のパスワードをサポートしていません。CA ControlMinder エンタープライズ管理 で SQL Server エンドポイントをパスワード コンシューマとして定義しており、SAM からパスワードをチェックアウトする場合は、パスワードフィールドを空にすることはできません。アカウントパスワードまたはその他の任意の文字列をパスワードとして指定できます。

## Oracle11g サーバ証明書が必要

Oracle 11g サーバに接続するには、サーバ証明書をエンドポイントにインストールする必要があります。

**注:** Oracle サーバから SSL 制限を削除することで、SSL のないサーバに接続できます。

# 第 10 章：既知の問題

---

このセクションには、以下のトピックが含まれています。

[インストールの既知の問題 \(P. 75\)](#)

[アップグレードの既知の問題 \(P. 78\)](#)

[一般的な既知の問題 \(P. 79\)](#)

## インストールの既知の問題

このセクションでは、CA ControlMinder コンポーネントのインストールの既知の問題について説明します。

### Windows エンドポイントのインストールの既知の問題

このセクションでは、Windows エンドポイントのインストールの既知の問題について説明します。

#### MSI ファイルからインストールしようとする「有効なリソースが見つかりませんでした」というメッセージが表示される

CA ControlMinder をアップグレードする際に、「有効なリソースが見つかりませんでした」というメッセージが表示されます。このメッセージが表示されるのは、現在使用しているメディアと、CA ControlMinder のインストールに使用したメディアとで、MSI ファイルのパスが異なっている場合です。

この問題を回避するには、「MediaPackage」というレジストリ文字列を追加し、CA ControlMinder msi パッケージに対する相対パスを指定します。以下のパスにレジストリ文字列を追加します。

```
HKLM\Software\Classes\Installer\Products\CDAFB228040EC5F40AA08B5E852A6D61\SourceList\Media
```

たとえば、32 ビット Windows オペレーティング システムに CA ControlMinder をインストールする場合、msi ファイルのフルパスは E:\x86\ です。「E:」は、リムーバブルなメディア ドライブです。MediaPackage 値には、値「\x86\」を指定します。

### UNIX エンドポイントのインストールの既知の問題

このセクションでは、UNIX エンドポイントのインストールの既知の問題について説明します。

#### RPM パッケージの検証でエラーが返される場合がある

RPM パッケージのインストールを検証する場合、検証エラーが返される場合があります。

それらのエラーはインストールした製品の機能に問題があることを示すものではないので、無視しても構いません。

#### クライアント サーバ通信モードの非互換性

`non_ssl` または `all_modes` が設定されたクライアントは、`fips_only` 通信モードが設定されたサーバと通信できません。

#### Linux zSeries の API ライブラリが 32 ビットである

CA ControlMinder で Linux zSeries (s390x) 用に提供している API ライブラリは、32 ビットです。

CA ControlMinder は Linux zSeries (s390x) 用の 64 ビット ライブラリを提供していません。

#### HP-UX ではパッチレベルの更新が必要

HP-UX では、CA ControlMinder のインストールを正常に行うには、事前にパッチレベルの更新が必要です。以下の OS パッチを推奨します。

- 11.23 (IA64) - パッチ PHSS\_37492 または OS QPK1123 バンドル (2006 年 9 月以降のもの)
- PA-RISC 上の 11.11 -- "dld\_getenv" をサポートする OS パスまたは OS QPR バンドル (2006 年 12 月以降のもの)
- 11.23 (PA-RISC) - OS QPK バンドル (2006 年 12 月以降のもの)

## 古い /lib64/libc.so.6 ライブラリを使用する場合、PAM が Linux s390x 上で機能しない

ホスト上の /lib64/libc.so.6 ライブラリが、CA ControlMinder PAM ライブラリのコンパイルに使用されたバージョンより古い場合、Linux s390 および s390x 上で PAM は動作しません。

ライブラリのバージョンは、2.3.2 以降である必要があります。

## UNAB エンドポイントのインストールの既知の問題

このセクションでは、UNAB エンドポイントのインストールの既知の問題について説明します。

### CA ControlMinder のインストール時に UNAB が 2 回再起動します

#### IBM AIX で該当

CA ControlMinder を IBM AIX にインストールし、UNAB がすでに実行中の場合、UNAB は 2 回再起動します。この動作は、AIX が追加のカーネルチェックを実行するためです。

### CA ControlMinder と UNAB を同じデフォルト以外の場所 [UNAB] にインストールするためにネイティブ インストールがカスタマイズされている場合、アンインストールが失敗します

#### AIX および HP-UX で該当

##### 症状:

ネイティブ インストールを使用して CA ControlMinder および UNAB をインストールし、インストールディレクトリをデフォルトではない場所の同じパスに変更した場合、UNAB のアンインストールが失敗します。

##### 解決方法:

CA ControlMinder をアンインストールすると、UNAB インストールが破壊され、失敗します。CA ControlMinder と UNAB の両方が同じディレクトリにインストールされているため、アンインストールが失敗します。ネイティブ インストールをデフォルトではない宛先フォルダへ変更している場合、製品名 (uxauth または UNAB) を宛先パスに連結することをお勧めします。

### CA ControlMinderr8.0 SP1 および r12.0 SP1 で UNAB がサポートされない

現在、CA ControlMinderr8.0 SP1 および r12.0 SP1 エンドポイントに UNAB をインストールすることはできません。さらに、UNAB および CA ControlMinder は同一のバージョンまたはサービスパックである必要があります。

## アップグレードの既知の問題

このセクションでは、CA ControlMinder コンポーネントのアップグレードの既知の問題について説明します。

### Windows エンドポイントのアップグレードの既知の問題

このセクションでは、Windows エンドポイントのアップグレードの既知の問題について説明します。

#### アップグレード時に「ファイルを変更するための権限が不足」というメッセージが表示される

CA ControlMinder エンドポイントをアップグレードする際に、ファイルを変更するための権限がインストーラに不足していることを伝えるメッセージが表示されたら、メッセージを確認してアップグレードを続行します。

### UNIX エンドポイントのアップグレードの既知の問題

このセクションでは、UNIX エンドポイントのアップグレードの既知の問題について説明します。

#### r12.0 以前のバージョンでは暗号化鍵の文字数を 54 文字までにする必要があります

運用する環境に r12.0 以前のバージョンの CA ControlMinder が含まれている場合は、暗号化鍵の文字数を 54 文字までにする必要があります。

## 一般的な既知の問題

このセクションでは、CA ControlMinder コンポーネントの既知の問題について説明します。

### Windows エンドポイントの既知の問題

このセクションでは、CA ControlMinder for Windows の既知の問題について説明します。

#### eAC\_r12.8--[プログラムの追加と削除]に[CA Access Control for ActiveX]が表示される

Windows で該当

**症状:**

以下のアプリケーションが [プログラムの追加と削除] リストに表示されます。

CA Access Control for ActiveX

**解決方法:**

このアプリケーションは CA ControlMinder に属していますので、削除しないでください。

#### エンドポイント作成画面の[全般]タブの情報の消失

**症状:**

エンドポイント作成画面の [全般] タブでエンドポイント名、ホスト、アカウント名およびパスワードを入力します。 [情報] タブで、所有者を選択するか、または管理アカウントを選択したとします。 [全般] タブに戻ると、すでに入力したデータが失われています。

**解決方法:**

[情報] タブに入力する前に、 [全般] タブ上で [サブミット] をクリックします。

## アンインストールしても Data および Log ディレクトリが削除されない

Windows で有効

症状:

システムから CA ControlMinder を削除した後、アンインストールプロセスによって以下のパスから Data および Log ディレクトリが削除されませんでした。

¥ProgramFiles¥CA¥AccessControl¥

解決方法:

アンインストール処理では、Data および Log ディレクトリは削除されません。プロセスの完了後、手動でディレクトリを削除できます。

## Microsoft Internet Explorer 7.0 と CA ControlMinder の互換性の問題

CA ControlMinder との互換性の問題のために、Microsoft Internet Explorer 7.0 が応答を停止する場合があります。この問題を回避するには、Microsoft Internet Explorer 8.0 をインストールするか、以下を行います。

**重要:** この手順を開始する前に、Microsoft ソフトウェアパッチ KB957388 を適用します。このソフトウェアパッチは、Microsoft の Web サイトからダウンロードできます。

1. すべての CA ControlMinder サービスを停止します。
2. コマンドライン ウィンドウを開き、以下のコマンドを実行します。

```
net stop cainstrm
```

3. [ファイル名を指定して実行] コマンドライン ウィンドウから regedit ユーティリティを開きます。

4. 以下のパスに移動します。

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSset¥Services¥cainstrm¥parameters
```

5. ExcludeProcess レジストリ エントリ値を変更して、iexplorer.exe ファイルを含めます。

6. コマンドライン ウィンドウから以下のコマンドを実行します。

```
net start cainstrm
```

7. CA ControlMinder サービスを開始します。

## 特権プロセスは、権限がなくとも、レジストリ ツリーの保存およびリストアが可能

Windows Server 2003 以降では、プロセスが特殊な権限 SE\_BACKUP\_NAME および SE\_RESTORE\_NAME を取得すると、CA ControlMinder の権限なしに、レジストリ ツリーを保存、リストアできます。

## x64 Windows 上での FIPS のみモード

x64 Windows 用 CA ControlMinder エンドポイントでは、CAPKI 4.1.2 はサポートされません。しかし、RSA の既知の問題により、FIPS が有効になったモードで CAPKI 4.1.2 を実行すると、著しい通信遅延が発生します。

## selang で実行されるホスト名変更イベントが CA User Activity Reporting レポートで不明なイベントと表示される

selang で実行されるホスト名変更イベントが、CA User Activity Reporting レポートで不明なイベントとして表示されます。

## UNIX エンドポイントの既知の問題

このセクションでは、CA ControlMinder for UNIX の既知の問題について説明します。

## CAWIN インストールに Ncurses が必要です

### Linux 64 ビット サーバに該当

CAWIN を Linux 64 ビット サーバ上にインストールする前に、Ncurses 32 ビットをインストールします。

## serevu デーモンの実行中に失敗したログイン イベントが監査されない

VMware vCenter 4.0 u2 で該当

CA ControlMinder の VMware vCenter バージョン 4.0 u2 へのインストール時に serevu デーモンが実行されていると、以下が発生します。

- 失敗したログイン イベントの LOGIN レコードが監査ファイルに表示されまない
- pam\_seos\_failed\_login.log ファイルのサイズが 0

この問題を回避するには、以下の操作を行います。

1. すべての CA ControlMinder デーモンを停止します。
2. 以下のディレクトリに移動します。

```
/etc/pam.d/
```

3. system-auth ファイルを編集して、pam\_seos.so への参照をすべて削除します。例：

```
account required pam_per_user.so /etc/pam.d/login.map
auth required pam_per_user.so /etc/pam.d/login.map
password required pam_per_user.so /etc/pam.d/login.map
session required pam_per_user.so /etc/pam.d/login.map
```

4. system-auth-generic ファイルを編集して、pam\_seos.so への参照を追加します。例：

```
password sufficient pam_seos.so
auth optional pam_seos.so
account optional pam_seos.so
session optional pam_seos.so
```

5. system-auth-local ファイルを編集して、pam\_seos.so への参照を追加します。例：

```
password sufficient pam_seos.so
auth optional pam_seos.so
account optional pam_seos.so
session optional pam_seos.so
```

6. ファイルを保存して閉じます。
7. CA ControlMinder デーモンを開始します。

## Linux 上で JBoss JDBC パスワード コンシューマを設定できない

### Linux に該当

現在、Linux 上で JBoss JDBC パスワード コンシューマを設定できません。

## CA ControlMinder にログインするには PAM\_login フラグが有効になっていることが必要

### AIX に該当

PAM\_login フラグが有効になっていない場合、CA ControlMinder は Active Directory ユーザアカウントを正しく検出できません。

この問題を回避するには、設定したログインプログラム (LOGINAPPL) で PAM\_login フラグを有効にします。 [pam\_seos] セクションで seos.ini の PamPassUserInfo トークンを 1 に設定して、seosd デーモンが PAM モジュールからログインリクエストを受け取ることを確認します。

以下のコマンドを使用して、ログインフラグを設定します。

```
er LOGINAPPL SSH loginflags(pamlogin)
```

## デフォルトのシェルが /etc/shells に定義されていないときにユーザ セッションが記録されない

### キー ロガーに該当

/etc/shells に定義されていないシェルでユーザがログインすると、CA ControlMinder はユーザ セッションを記録しません。

## PAM がアクティブな場合、FTP および SSH の猶予ログインで segrace が呼び出されない

PAM をアクティブにした場合、FTP および SSH サービスへの猶予ログインを行う segrace は、自動的に呼び出されません。

FTP に関するこの問題を回避するには、FTP サービスの LOGINAPPL レコードで LOGINFLAGS プロパティの値を nograce に変更します。

SSH に関するこの問題を回避するには、PAM から segrace を呼び出しません。代わりに、ユーザまたはオペレーティング システム起動スクリプトから segrace を呼び出します。

### 猶予期限が終了すると、CA ControlMinder はパスワードをリセットしない

HPUX および AIX で該当

CA ControlMinder エンドポイントへの UNAB のインストールでは、ユーザパスワードの猶予期間が期限切れになった場合に、CA ControlMinder PAM は、アカウントパスワードをリセットするための「sepass」ユーティリティの呼び出しを実行しません。

この問題は、loginflags (pamlogin) を使用するログインアプリケーション (SSH ログイン、rlogin、FTP、Telnet など) に影響します。Solaris ログインは、HPUX および AIX 上の CA ControlMinder ではログインアクションとして認識されません。この問題を回避するには、SSH ログインアプリケーションで loginflags (none) を使用します。

以下のコマンドを実行して、トークンを設定します。

```
er LOGINAPPL SSH loginflags(none)
```

### 一部のプロセスで、Solaris ネットワーク イベントのバイパスが機能しない

Solaris の場合、CA ControlMinder は、CA ControlMinder が起動する前に開始されたプロセスについては、ネットワーク イベント (SPECIALPGM レコードのバイパスの種類 PBN) をバイパスしません。

### Stat インターセプト呼び出しが AIX システムでサポートされない

STAT\_intercept トークンが「1」に設定された stat システム コールにおけるファイルアクセス チェックは AIX システムではサポートされません。

## UNAB の既知の問題

このセクションは、UNAB の既知の問題について説明します。

## 一方向の信頼機能が UNAB アップグレード後に失敗する

### 症状:

UNAB を 12.6、12.6.1 または 12.6.2 から 12.8 にアップグレードした後、一方向の信頼機能が機能しませんでした。

### 解決方法:

この問題を解決するには、12.8 へのアップグレード後に、UNAB を一方向の信頼ドメインに登録する必要があります。

## UNAB エージェントは信頼される側のドメインへの接続を失いました

### 症状:

ユーザ チケットが失効する前にドメインセキュリティ ポリシー Kerberos サービス チケットの有効期限が失効するよう設定した後、UNAB エージェント (uxauthd) では信頼される側のドメインへの接続が失われました。

### 解決方法:

uxauth.ini の tgt\_renew\_lifetime トークン値を Kerberos サービス チケットの最長有効期限よりも小さく設定します。

## AD ユーザが HP-UX 上で現在のパスワードを 2 回要求される

### HP-UX IA64 で有効

Active Directory ユーザがパスワードを変更するには、現在のパスワードを 1 回ではなく 2 回要求され、2 回指定する必要があります。

## マップされたユーザによる AIX へのログイン試行の失敗がログに記録されない

### AIX に該当

### 症状:

マップされたユーザとして、SSH を使用して AIX UNIX ホストへのログインを試行するとき、失敗した試行が uxaudit によってログに記録されません。

### 解決方法:

ユーザが間違ったパスワードを入力した場合、マップされたユーザが失敗した最初のログイン試行は、Seaudit によってログに記録されません。以降のログイン試行は uxaudit によってログに記録されます。

## HP-UX 上で、次回ログイン時にパスワードの変更が失敗する

HP-UX に該当

Active Directory で、「ユーザは次回ログイン時にパスワード変更が必要」オプションを選択しました。SSH または Telnet を使用してログインすると、ユーザがログインできないかパスワードを変更できません。

## PAM 設定の変更によりユーザ ログインがブロックされる

Red Hat Linux 5.0 以上に該当

症状:

UNAB および CA ControlMinder を Red Hat Linux にインストールし、制御フィールドで "value=action" 構文を使用するように PAM 設定ファイルを設定しました。Linux ホストへのログインを試行すると、ログイン動作が拒否されます。

解決方法:

UNAB は、PAM 設定ファイルで制御フィールドの "value=action" 構文をサポートしません。

## 一方向の信頼関係を持つドメイン環境で UNAB を登録解除した後、不正なユーザ ID が表示される

一方向の信頼関係を持つドメイン環境で UNAB を Active Directory から登録解除した後、一方向の信頼関係を持つドメインのユーザ ID 詳細が、表示されるべきではない場合にも表示されます。

## 信頼されているユーザ SSH ログインが AIX で失敗しました

症状:

SSH を使用して AIX 5.3 エンドポイントにログインしようとしたのですが、ログインに失敗しました。

解決方法:

このエラーは、AIX と SSH のバージョンの一部の組み合わせで発生する、IBM の既知の問題です。この問題は APAR ((Authorized Program Analysis Report) 番号 IV10231 として IBM 開発部門にログ記録されています。

## watchdog\_enabled トークンが No に設定されても uxauthd が開始する

### 症状:

watchdog\_enabled トークンを no に設定して UNAB を再起動すると、uxauthd が開始されます。

### 解決方法:

watchdog スクリプトは、最初に uxauthd を開始した後で watchdog\_enabled トークンに行なわれた変更を無視します。登録処理中に `-n` を指定し、トークンに変更を加えて、`uxauthd.sh` スクリプトを別に開始することをお勧めします。

## 試行ログインとしてのローカルアカウントパスワードを使用した監査ログ レコード ログイン

### 症状:

UNAB にログインし、ユーザアカウントがローカルパスワードファイルおよび Active Directory にある場合、監査ログに以下のレコードが表示されます。

```
<audit_record_date_and_time> A LOGIN map3
```

### 解決方法:

これは UNAB の既知の問題です。監査ログは、P LOGIN ではなく A LOGIN を記録します。

## ログイン エントリが 2 回記録される

### Linux に該当

UNAB がインストールされているホストに `rlogin` を使用してログインすると、ログインの試行が監査に 2 回表示されます。

## パフォーマンスを向上させるための Microsoft Windows Server 2003 用ホット フィックス

Windows Server 2003 SP1、Windows Server 2003 64 ビットで該当

LDAP\_MATCHING\_RULE\_IN\_CHAIN を使用した拡張検索で LDAP が Active Directory のクエリ結果を返すのに失敗します。

この問題の回避策として、Microsoft Windows 2003 Server 用の最新のサービス パックをインストールするか、wingrp\_update\_login トークンを「no」に設定して、ログイン中の UNAB グループの更新を無効にします。

注: 詳細については、Microsoft ナレッジベース記事 914828 を参照してください。

## Uxpreinstall ユーティリティがホスト名の解決に失敗する

UNAB のインストールした後、および Active Directory への登録前に、uxpreinstall ユーティリティはホスト名解決の検証に失敗します。

この問題を回避するには、-d 引数を使用して、Active Directory ドメイン名を指定します。以下に例を示します。

```
./uxpreinstall -d domain_name
```

## Telnet および rlogin プログラムが監査レコードに表示されない

Linux、HP-UX に該当

UNAB 監査レコードに、telnet および rlogin のログインプログラムが表示されません。Linux では、UNAB 監査レコードに telnet または rlogin の代わりに "remote" と表示されます。HP-UX では、UNAB 監査レコードに telnet または rlogin の代わりに "login" と表示されます。

## uxconsole -register コマンドと -deregister コマンドの間隔

Active Directory に UNAB ホストを登録し、その後登録を解除する場合、ホストの登録を解除する前に、ドメインコントローラ レプリケーションで必要となる時間を待機することをお勧めします。

注: UNAB ホストを登録解除する場合、配布されなかったポリシーは削除されます。

## 新規ドメイン ユーザの最初のログインが失敗する場合がある

### SSH に対して有効

Active Directory でユーザを作成し、新規ユーザがすぐに UNAB エンドポイントへのログインを試行する場合、最初のログインは失敗しますが、それ以降のログインは問題なく行われます。最初のログインが失敗するのは、ユーザがエンドポイントに認識されていないためです。ただし、失敗したログインプロセス中に、`uxauthd` はローカル NSS ストレージをユーザ情報で更新します。それ以降のログインは成功します。これは、ユーザがエンドポイントに認識されるようになったためです。

デフォルトでは、`uxauthd` は NSS ストレージ内のユーザ情報を 1 時間おきに更新します。`uxauthd` が NSS ストレージを更新した後に新規ユーザがエンドポイントへのログインを試行すると、ログインは成功します。

## ログイン サービスが SSO ログインで PAM をバイパスする

SSO ログインでは、ログイン サービスは PAM をバイパスします。ログイン ポリシーは適用されず、監査イベントも生成されません。

## ホストへのログインが成功した後、エラー メッセージが生成される

### Linux、AIX、HP-UX に有効

UNIX PAM フローに制限があるため、UNAB ホストへのログインが成功した後、アカウント認証に失敗したことを示すエラー メッセージが `syslog` ファイルに生成されます。

## sepass でパスワードを変更しようとすると、パスワード不一致のメッセージが表示される

### AIX 5.3 に該当

マップされたユーザが `sepass` を使用して、アカウント パスワードを変更しようとすると、パスワード不一致のエラー メッセージが表示されます。エラー メッセージが表示されても、アカウント パスワードは Active Directory 上で変更されています。

### Active Directory ユーザは Solaris 上でパスワードを変更できない

Sun Solaris のパスワードに関する制限事項により、Active Directory アカウントで UNIX ホストにログインするユーザは、Solaris のパスワードツールを使用してアカウントを変更できません。初回ログイン時にユーザがアカウントパスワードを変更する必要がある場合、ユーザは Solaris 以外のシステムからログインする必要があります。

UNAB が UNIX ホスト上で実行されている場合、以下のコマンドを使用してローカルアカウントのパスワードを変更します。

```
passwd -r files username
```

CA ControlMinder が UNIX ホスト上で実行されている場合、sepass ユーティリティを使用してローカルアカウントのパスワードを変更します。

### Active Directory ユーザの代理実行では監査記録が作成されない

su を使用して Active Directory ユーザを代理実行する場合、代理実行の試行は監査されません。

### sshd プログラム名が SFTP セッションの監査記録に表示される

sftp プログラムを使用し終えたログインセッションの監査記録は、sftp プログラムではなくプログラムフィールド内の sshd デーモンを表示する場合があります。

### イベントビューアの UNAB エントリに空白フィールドが含まれる

Windows イベントビューアに空白フィールドのある UNAB イベントが表示されます。

### エンタープライズ ユーザの FTP SSO ログインが監査されない

Solaris に該当

Kerberized FTP およびテルネットプログラムは PAM スタックをバイパスします。そのため UNAB は、エンタープライズユーザによる FTP およびテルネット SSO ログインを監査しません。

## SSO が有効な UNAB を登録解除しても keytab ファイルからレコードが削除されない

以前に SSO を有効にして登録していた UNAB ホストを登録解除すると、そのコンピュータ オブジェクトは Active Directory から削除されますが、対応するレコードは keytab ファイルから削除されません。その UNAB ホストを再び登録しようとしても、Kerberos チケットは作成されません。

この問題を回避するため、UNAB ホストを登録解除しないようにするか、UNAB ホストにのみ使用される場合は、keytab ファイルを削除することを推奨します。

## HP-UX のパスワードで @ 記号がサポートされない

HP-UX に該当

HP-UX の制限事項により、HP-UX エンドポイント上では、パスワードに @ 記号を使用しないでください。

## 完全修飾ドメイン名による HP-UX へのログインがサポートされていない

HP-UX に該当

HP-UX では、完全修飾ドメイン名（例：user@domain）ではログインできません。

## サーバコンポーネントの既知の問題

このセクションでは、CA ControlMinder サーバ コンポーネント（CA ControlMinder エンドポイント管理、CA ControlMinder エンタープライズ管理、およびエンタープライズ レポート）の既知の問題について説明します。

## 操作管理者アカウント パスワードのチェックアウトを試行するとエラー メッセージが表示される

### 症状:

操作管理者アカウントのパスワードを SSH エンドポイント タイプからチェックアウトすると、以下のメッセージが表示されます。

```
java.lang.Exception: too many results found for account  
handle:ACCOUNT_HANDLE_NOT_INITIALIZED
```

### 解決方法:

これは SAM フィーダの既知の問題です。複数の操作管理者アカウントが定義されている場合、フィーダ (`ADMIN_ACCOUNT_IS_DISCONNECTED=false`) を使用して作成した接続済み操作管理者アカウントのパスワードをチェックアウトしようとする問題が発生します。

この問題を回避するには、以下の手順に従います。

- SAM フィーダのポーリング タスクを実行して、SSH エンドポイント タイプを作成し、操作管理者アカウントを接続解除 (`ADMIN_ACCOUNT_IS_DISCONNECTED=true`) として設定します。
- 各操作管理者アカウントに対して SAM フィーダ ポーリングを実行し、アカウントを変更して接続解除されたシステムに対するアカウントであることを指定します (`DISCONNECTED_SYSTEM=false`)。

## エンタープライズ管理サーバのインストール後に JBoss サーバ ログ ファイルにエラー メッセージが表示される

### 症状:

サードパーティのコンポーネントおよびエンタープライズ管理サーバをインストールした後にエンタープライズ管理サーバを再起動すると、`server.log` ファイルに以下のエラーが示されます。

- 593 エラー
- 597 エラー
- 604 エラー
- 737 エラー
- 229 エラー
- 329 エラー
- 805 エラー

### 解決方法:

これは既知の問題です。CA ControlMinder サービスが開始されていることを確認します。エンタープライズ管理で CA ControlMinder が実行されていることが必要 JBoss アプリケーションサーバ サービスが開始されていない場合、以下のいずれかを実行します。

- (Windows) [スタート] - [プログラム] - [CA] - [ControlMinder] - [タスク エンジンの開始] をクリックします。

注: タスク エンジンを開始すると、初回のロードには多少時間がかかる場合があります。

- (Windows) [サービス] パネルから JBoss アプリケーションサーバ サービスを開始します。
- (Linux) 「./JBOSS\_HOME/bin/run.sh -b 0.0.0.0」と入力します。

## 日本語文字を含む Active Directory ユーザを無効にできない

### 症状:

CA ControlMinder エンタープライズ管理で、日本語の文字を含む Active Directory ユーザを無効にすると、タスクは失敗します。ユーザは、引き続きエンタープライズ管理サーバにログインできます。

### 解決方法:

これは既知の問題です。

## パスワード コンシューマ イベントの変更アクションが不明なアクションとして表示される

### 症状:

パスワード コンシューマ イベントを変更し、アクションを確認すると、それが「不明アクション」として表示されます。

### 解決方法:

これは既知の問題です。

## SAM のパスワード履歴内の誤ったタイムゾーン

### 症状:

特権アカウント パスワード履歴の変更日は、Web ブラウザを実行しているクライアントのタイムゾーンではなく JBoss サーバのタイムゾーンで表示されます。

### 解決方法:

なし

## アップグレード後に dbmgr -export 機能が有効な割り当て済みポリシーのエクスポートに失敗する

Linux で該当

### 症状:

エンタープライズ管理サーバのアップグレード後に、割り当て済みの有効なポリシーがホストで見つかりません。

### 解決方法:

エンタープライズ管理サーバのアップグレード処理中に、インストールでは dbmgr -export 機能を使用して、既存のポリシーを selang コマンドにエクスポートします。処理でのエラーにより、インストールはポリシーをデータベースに再インポートしませんでした。

この問題を解決するには、エンタープライズ管理サーバをアップグレードする前に、以下のテスト修正をインストールします。

- 12.7 の場合 -- T537745
- 12.6.01 の場合 -- T537746
- 12.5SP5 の場合 -- T537747
- 12.5SP4 の場合 -- T537738

## インストール中に表示される .NET Framework のエラー メッセージ

CA エンタープライズ管理のインストール中に、[ロールと機能の追加] ウィザードにエラーメッセージ「次の機能をインストールできませんでした: NET Framework3.5 (.NET2.0 および 3.0 を含む)」が表示されます。

エラーメッセージポップアップボックスを閉じて、インストールを続行します。このエラーメッセージはサーバインストールに影響しません。

## 特権アカウント リクエストと夏時間(DST)

エンタープライズ管理サーバまたは依頼者のいずれかが夏時間 (DST) の時間帯にある場合、特権アカウント リクエストをサブミットする際に、以下が発生します。

- エンタープライズ管理サーバが夏時間の時間帯にあり、依頼者が夏時間の時間帯にない場合、リクエストされた期間は元のリクエストから 1 時間遅くなります。
- エンタープライズ管理サーバが夏時間の時間帯になく、依頼者が夏時間の時間帯にある場合、リクエストされた期間は元のリクエストより 1 時間早くなります。

## アンインストールで JBoss と JDK のファイルが削除されない

### 症状:

デフォルト以外のドライブについてエンドポイント管理アンインストール手順を実行すると、JBoss および JDK のパッケージ制限により、すべての JBoss と JDK のファイルが削除されません。

### 解決方法:

エンタープライズ管理アンインストールの後、JBoss および JDK の ControlMinder フォルダを手動で削除します。

## ポリシー管理レポートデータの読み込みエラー

### 症状:

2つの CA ControlMinder Deployment Mapping Server (DMS) のうち1つを削除すると、削除された DMS からのデータが引き続きポリシー管理レポートに表示されます。

### 解決方法:

エンタープライズ管理データベースで以下のコマンドを実行します。

```
Delete from SNAPSHOTINFO where HOSTID = host_to_delete_name
```

例:

- エンドポイントデータを削除する方法  

```
Delete from SNAPSHOTINFO where HOSTID = 'hostname@ca.com'
```
- DMS データを削除する方法  

```
Delete from SNAPSHOTINFO where HOSTID = DMS__@hostname@ca.com
```

## [記録済みセッションの表示]での検索

CA ControlMinder エンドポイント管理の [記録済みセッション] タブで [記録済みセッションの表示] を検索するために [表示] をクリックすると、以下の既知の問題が発生します。

- アクティビティログコンテンツ (デフォルト) を検索する際に、結果またはメッセージは表示されません。
- UserID または LoginID を検索する際に、[UserName] フィールドに「n¥a/n¥a」が表示されます。

## iOS 5 でオープンセッションが機能しない

iOS の問題により、iOS 5 でオープンセッションは機能しません。iOS でオープンセッションを選択するコマンドは、クローズされたセッションも返します。

## PMDB 名が 25 文字を超過する場合、PMDB サブスクリバがリスト表示されない

### 症状:

25 文字を超過する文字数で PMDB が作成される場合、エンドポイント管理ユーザ インターフェースを使用してそのサブスクリバをリスト表示すると、サブスクリバは表示されません。

### 解決方法:

これは、エンドポイント管理ユーザ インターフェースの既知の問題です。サブスクリバリストを表示するには、`sepmdb` ユーティリティを使用します。コマンドの形式は以下のとおりです。

```
sepmdb -l pmd
```

```
-l
```

Policy Model のサブスクリバを一覧表示します。

```
pmd
```

Policy Model の名前を指定します。

## telnet セッションがオープン セッションでサポートされない

### Windows で有効

オープンセッションは telnet セッションをログインとして検出および認識しません。telnet セッションは、Windows ではオープンセッションでサポートされていません。

## デフォルトのリクエスト承認者が設定されない

### SunOne および CA Directory で該当

SunOne または CA Directory ユーザ ディレクトリを使用する場合は、デフォルトのリクエスト承認者を設定します。すべての特権アカウントパスワードリクエストのサブミット先となる、デフォルトのリクエスト承認者を定義します。

#### 次の手順に従ってください:

1. システム マネージャとして CA ControlMinder エンタープライズ管理にログインします。
2. [ユーザおよびグループ] - [タスク] - [管理タスクの変更] を選択します。  
[管理タスクの変更: 管理タスクの選択] ウィンドウが表示されます。
3. [名前] フィールド内に「特権アカウント リクエスト」と入力し、[検索] をクリックします。  
CA ControlMinder エンタープライズ管理 は、検索条件に一致する結果を表示します。
4. 特権アカウントリクエストを選択し、[選択] をクリックします。  
[管理タスクの変更: 特権アカウント要求] ウィンドウが表示されます。
5. [イベント] タブに移動し、[ワークフロー プロセス] を選択します。  
[ワークフロー プロセス] 画面が表示されます。
6. [デフォルト承認者] セクションで [ユーザの追加] を選択します。  
[ユーザの選択] 画面が表示されます。
7. デフォルト承認者として割り当てるユーザの名前を入力し、[検索] を選択します。  
CA ControlMinder エンタープライズ管理 は、検索条件に一致する結果を表示します。
8. [選択] をクリックします。  
選択したユーザは、デフォルト リクエスト承認者として追加されます。
9. [OK] をクリックして終了します。

注: 定義したデフォルト リクエスト承認者は、エンタープライズ管理サーバをインストールする前に作成したユーザには適用されません。以前ユーザディレクトリに存在していたユーザのデフォルト リクエスト承認者は、`superamdin` です。

### バッチ操作の実行時に「No Managed Connections Available Within Configured Blocking Timeout (設定されたブロックタイムアウト内に利用可能な管理対象接続が存在しません)」というエラーメッセージが表示される

バッチタスクの実行時に、「No Managed Connections Available Within Configured Blocking Timeout」というエラーメッセージを受信します。たとえば、大きなグループまたはアカウントに対して、パスワードの自動リセットタスクの実行を試みるとします。このエラーメッセージは、JBossアプリケーションサーバで利用可能な接続がすべて使用されたため、タスクを完了できないことを示しています。

この問題を回避するには、プール内で利用可能な接続数を増やす必要があります。

1. JBoss アプリケーションサーバを停止します。
2. 以下のディレクトリに移動します。ここで、`JBoss_HOME` は JBoss をインストールしたディレクトリを示しています。

```
JBoss_HOME/server/default/deploy/
```

3. ファイル `imtaskpersistencedb-ds.xml` を開いて、編集します。
4. `<max-pool-size>` タグを見つけて、値を「40」に設定します。
5. `<idle-timeout-minutes>` タグを見つけて、値を「1」に設定します。
6. (`<!--`) the `<blocking-timeout-millis>` タグを、以下のようにコメントアウトします。

```
<!--blocking-timeout-millis>5000</blocking-timeout-millis-->
```

7. ファイルを保存して閉じます。
8. JBoss アプリケーションサーバを始動します。

プール内の利用可能な接続数が増加しました。これで、タスクを実行できるようになりました。

## Windows サンプル ポリシー用の JBoss の展開に失敗する

Windows サンプル ポリシー用の JBoss のエンドポイントへの展開が失敗します。このポリシー展開プロセスは、PROGRAM リソースがすでに存在することを示す内部エラー メッセージで終了します。

この問題を回避するには、JBoss サンプル ポリシーを使用し、それを変更してから、展開して、PROGRAM リソースを明示的に作成します。

## CA ControlMinder エンタープライズ管理 でポリシー管理レポートを表示するとエラー メッセージが表示される

ポリシー管理レポートの表示を試行すると、CA ControlMinder エンタープライズ管理 はそのタスクが失敗したという旨のメッセージを表示します。

この問題を回避するには、JBoss アプリケーション サーバおよび CA Business Intelligence サーバ (レポート ポータル) を再起動します。

## パスワードが定義されていない CA ControlMinder ユーザは CA ControlMinder エンタープライズ管理 サーバにログインできない

パスワードを持たない CA ControlMinder ユーザアカウントは CA ControlMinder エンタープライズ管理 サーバにログインできません。

## アクセス ロールが CA ControlMinder エンタープライズ管理 でサポートされない

管理ロールルールを定義するとき、管理ロールのメンバであるユーザを選択します。CA ControlMinder エンタープライズ管理 はアクセス ロールをサポートしません。アクセス ロール オプションはインターフェースに表示されません。

## UNAB ホストまたはホスト グループの変更時に、「操作の必要なし」というメッセージが表示される

UNAB ホストまたはホスト グループの設定を変更し、変更をサブミットする際に、CA ControlMinder エンタープライズ管理 に "操作の必要なし" というメッセージが表示されます。このメッセージは、何のアクションも実行されなかったことを示していますが、UNAB ホストまたはホスト グループに対して行った変更は適用されています。

### 制御文字によりアプリケーション例外が発生する可能性がある

CA ControlMinder データベースで制御文字を使用すると、CA ControlMinder エンドポイント管理 および CA ControlMinder エンタープライズ管理 でアプリケーション例外や誤表示が発生する可能性があります。

### ユーザ インターフェース上に判読できない文字が表示される

#### 症状:

CA ControlMinder エンタープライズ管理 ユーザ インターフェースにログインすると、判読できない文字が表示されます。

#### 解決方法:

問題の原因は、使用しているデータベース インスタンスが国際化キャラクターセット UTF8 を完全にはサポートしない点にあります。この問題を修正するには、完全に国際化されたデータベース インスタンス上に CA ControlMinder エンタープライズ管理 を再インストールする必要があります。

### 監視対象ファイルの Trust プロパティを変更できない

CA ControlMinder エンドポイント管理 で、監視対象ファイル (SECFILE) のリソースの [監査] タブで [Trust] チェック ボックスをオフにして変更を保存しようとするすると失敗します。

この問題を回避してこのリソース属性を変更するには、`selang` を使用します。

### 大容量のポリシーの作成時に CA ControlMinder エンタープライズ管理 がタイムアウトする

6000 を超えるコマンドが含まれているポリシーを作成する場合、CA ControlMinder エンタープライズ管理 ユーザ インターフェースがタイムアウトになります。CA ControlMinder エンタープライズ管理 がポリシーを作成するまで、ユーザ インターフェースを使用した作業を続行することができません。この問題を回避するには、ブラウザを新規に起動して CA ControlMinder エンタープライズ管理 にログインし、セッションを新たに開始します。

## 末尾に円記号を含むポリシーをデプロイできない

`selang` の表記法では、行の最後の文字に円記号文字 (¥) を使用して、コマンドが次の行に続くことを示すことができます。これは拡張ポリシー管理ではサポートされません。ポリシー コマンドが複数の行にまたがらないようにしてください。

注: CA ControlMinder に用意されている以下のサンプル ポリシーには末尾に円記号が含まれます。\_AC\_WEBSERVICE、\_APACHE、\_JBOSS、\_MS\_SQL\_SERVER、\_ORACLE

## ポリシー スクリプト検証エラー メッセージが別の言語で表示される

### CA ControlMinder エンタープライズ管理 で有効

ポリシーがデプロイされたがエラーがある場合、CA ControlMinder エンタープライズ管理 で表示される `selang` 結果メッセージはエンタープライズ管理サーバ上の CA ControlMinder エンドポイントのインストール言語で表示され、CA ControlMinder エンタープライズ管理 のインストール言語ではありません。

これらのメッセージをローカライズされた言語で表示するには、CA ControlMinder エンタープライズ管理 をインストールする前に、ローカライズされた言語でエンタープライズ管理コンピュータ上に CA ControlMinder エンドポイントをインストールする必要があります。

## 名前が 30 文字を超える端末の監査レコードを表示できない

端末名が 30 文字を超える場合、監査レコードを表示できません。この現象は、Windows コンピュータ上で動作している CA ControlMinder エンドポイント管理で UNIX エンドポイントを管理する場合に発生します。

## PMDB 管理時に、PMDB 監査レコードを表示できない

CA ControlMinder エンドポイント管理 を使用して PMDB を管理すると、PMDB の監査レコードは参照できません。

この問題を回避して PMDB の監査レコードを表示するには、PMDB が存在するホストに接続します。

## ネットワーク デバイス用のオープン セッションが失敗します

特権アカウント名が 10 文字を超えている場合、ネットワーク デバイス用のオープンセッションが失敗します。

SAM エンドポイントタイプの Access Control に対する、「そのようなメソッドは存在しません。」または、「パスワードをリセットできませんでした。」というエラー メッセージ

### Linux に該当

Linux コンピュータにエンタープライズ管理サーバをインストールする際に、SAM エンドポイント用の Access Control を定義すると、「そのようなメソッドは存在しません。」というエラー メッセージが表示されます。

チェックイン時に CA ControlMinder エンタープライズ管理 が特権アカウントパスワードをリセットするように指定している場合、ユーザが SAM エンドポイント用の Access Control で特権アカウントにチェックインすると、「パスワードをリセットできませんでした。」というエラー メッセージが表示されます。

### 次の手順に従ってください:

1. Java コネクタ サーバを停止します。以下の手順を実行します。
  - a. 以下のディレクトリに移動します。ここで `ACServerInstallDir/Connector_Server/bin` は、エンタープライズ管理サーバがインストールされているディレクトリを示します。

```
ACServerInstallDir/Connector_Server/bin
```

- b. 以下のコマンドを実行します。

```
./im_jcs stop
```

Java コネクタ サーバが停止します。

2. `im_jcs` スクリプトを編集できる形で開きます。
3. スクリプトから以下の行を見つけて削除します。

```
PREJAR="$FULLBASEPATH/bin/jcs-bootstrap.jar:$FULLBASEPATH/  
conf:$FULLBASEPATH/lib/jcs.jar:"`echo $FULLBASEPATH/  
lib/apacheds-server-main-*app.jar`
```

- 以下の行をコピーし、スクリプトに貼り付けます。

```
PREJAR="$FULLBASEPATH/bin/jcs-bootstrap.jar:$FULLBASEPATH/  
conf:$FULLBASEPATH/lib/jcs.jar:$FULLBASEPATH/  
lib/nlog4j__V1.2.25.jar:"`echo  
$FULLBASEPATH/lib/apacheds-server-main-*-app.jar`
```

**重要:** スクリプトに張り付けた後、行のキャリッジリターンを削除します。

- ファイルを保存します。
- Java コネクタ サーバを起動します。

```
./im_jcs start
```

Java コネクタ サーバが起動します。これで、SAM エンドポイントタイプの Access Control を設定できます。

## アップグレード後に Telnet 自動ログインが Solaris 上でサポートされない

Solaris で該当

CA ControlMinder r12.7 へのアップグレード以降は、Telnet 自動ログインは Solaris 上でサポートされません。

## Windows サービスと Windows スケジュール タスクの変更が検出されない

Windows Server 2003 に該当

症状:

ユーザが Windows サービスまたは Windows スケジュール タスクを変更する際に、それらの変更は検出できません。

解決方法:

これは Microsoft の既知の問題です。 エンドポイント上でサービスまたはタスクを変更した後、既存のパスワード コンシューマを削除します。サービス アカウント検出ウィザードを使用して、パスワード コンシューマを作成します。

## サービス アカウント パスワード要求の承認に失敗する

サービス アカウント パスワード要求をサブミットしても、要求がリクエスト承認者に送信されず、サービス アカウント パスワードをチェックアウトできません。

## JDBC パスワード コンシューマによるパスワード取得の監査レコードがない

JDBC パスワード コンシューマが CA ControlMinder エンタープライズ管理からパスワードを取得する際、エンタープライズ管理サーバは監査レコードを書き込みません。

## 自動ログインを使用して Oracle Enterprise Manager にログインしようとするエラー メッセージが表示される

### Oracle に該当

管理者アカウント パスワードのチェックアウト後に、自動ログインオプションを使用して Oracle Enterprise Manager にログインしようとする、エラー メッセージが表示されます。このエラー メッセージは、前回のセッションをログ オフせずに、ブラウザ ウィンドウを閉じて終了した場合に表示されます。

## エンドポイントによるパスワードの要求時に、リモート デスクトップ接続ができない

### Windows で有効

エンドポイントの端末サービス設定が、ログイン時に常にパスワードを要求するよう設定されている場合、Windows リモート デスクトップの自動ログイン スクリプトはエンドポイントへのログインに失敗します。

## SAM がクローズされた CA Service Desk チケットのチケット番号を受け取る

### CA Service Desk との統合に有効

特権アカウントへのアクセス要求時にクローズされた CA Service Desk の発行またはリクエスト チケット（チケットの種類 = iss または cr）の番号を指定すると、CA ControlMinder エンタープライズ管理は承認者に要求を転送します。

## CA Service Desk 変更指示チケット番号を指定できない

### CA Service Desk との統合に有効

特権アカウントへのアクセス要求時に CA Service Desk 変更指示チケット（チケットの種類 = ch）の数を指定すると、CA ControlMinder エンタープライズ管理は承認者に要求を転送しません。

## マニュアルの既知の問題

このセクションでは、CA ControlMinder のマニュアルセットの既知の問題について説明します。

### 「SDK 開発者ガイド」にグラフィクスの代替テキストがない

「SDK 開発者ガイド」のグラフィクスに、代替テキストがありません。「SDK 開発者ガイド」は CA ControlMinder の旧バージョンで最初に翻訳され、CA ControlMinder r12.5 のマニュアルでも、変更なく提供されています。

### PDF マニュアルには Adobe Reader 7.0.7 が必要

PDF 形式の CA ControlMinder マニュアルを参照するには、Adobe Reader 7.0.7 以降をインストールする必要があります。Adobe Reader をコンピュータにインストールしていない場合は、Adobe 社の Web サイトからダウンロードしてインストールしてください。

**注:** Adobe Reader は、HP-UX Itanium (IA64) および Red Hat Linux Itanium IA64 では使用できません。