eTrust® Access Control for Windows

導入ガイド

r8 SP1

CA 製品の参照

このマニュアルが参照している CA の製品は以下のとおりです。

- eTrust® Access Control（eTrust AC）
- eTrust® Single Sign-On（eTrust SSO）
- eTrust® Web Access Control（eTrust Web AC）
- eTrust® CA-Top Secret®
- eTrust® CA-ACF2®
- eTrust® Audit
- Unicenter® TNG
- Unicenter® Network and Systems Management（Unicenter NSM）
- Unicenter® Software Delivery

テクニカル サポートの連絡先

オンライン 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.caj.co.jp/support/）を参照してください。

目次

第 1 章: e ビジネスの統合的なセキュリティの紹介

このセクションには、以下のトピックが含まれます。

本書の目的

本書では eTrust AC についてご紹介します。 本書を最後までご覧いただくことにより、この製品の概要と使いやすさを理解していただけます。 eTrust AC を実際にご利用いただく前に、製品に関する理解を深めていただくことが、本書の目的です。

CA 技術サービス: エンタープライズ IT 管理の構想の実現

CA Technology Services(tm) は、オペレーションの効率化を実現し、IT インフラストラクチャの管理を向上させるエンタープライズ IT 管理ソリューションを提供します。これによって、重要なビジネス価値を促進し、財務上優れた結果を生み出します。 CA Technology Services は、エンタープライズ システム管理、ビジネス サービスの最適化、セキュリティ管理、およびストレージ管理分野のグローバルな専門知識と認定専門家を活用して、お客様の IT への投資効率を最大限に高めます。

27 年以上の管理ソフトウェア分野での経験、1,000 人を超えるテクノロジ サービスの専門家(その多くが CISSP、ITIL、および SNIA 認定)、および業界をリードするサービス パートナーのサービス提供能力を補足的に利用して、ベスト プラクティスと、長年の実績を持つ手法を提供します。

エデュケーションおよびトレーニング： CA テクノロジのビジネス価値の最大化

CA Technology Services エデュケーションおよびトレーニングでは、効率化された実装、価値に対する時間の短縮、および向上した生産性によって CA テクノロジのビジネス価値が最大化されることを実感していただくことに重点を置いています。 CA では、エンタープライズ IT 管理(EIM)のための、CA の完全な統合およびオープン ソリューションについて、自分のペースで学習可能な、インストラクタによる拡張学習ソリューションを提供しています。また、主要な付加価値教育プロバイダと提携し、エンタープライズシステム管理、セキュリティ管理、ストレージ管理、およびビジネス サービスの最適化の分野の提供コースを拡充しています。 CA の経験豊富で精力的な認定専門家チームは、CA ソフトウェア製品の最適化および実績のある IT プロセス モデルの活用について、リアルタイムの専門知識を提供します。これにより、お客様の企業は、現在の IT 環境でベスト プラクティスを実際に適用する方法を学ぶことができます。

エデュケーションおよびトレーニング コースの詳細については、
http://www.caj.co.jp/education/ を参照してください。

eTrust ソリューション

eTrust ソリューションは、企業が自社の環境を容易に保護できる革新的なテクノロジを提供することによって、e ビジネスの実現を可能にします。 この統合的なセキュリティ パッケージを使用すると、リスク査定、攻撃の検知、損失の防止などのソリューションによって、あらゆる e ビジネスに機会と利益をもたらします。 企業は、製品単体でも、セキュリティ スイートとしても、あるいは完全に Unicenter NSM と統合しても、eTrust をセキュリティ ソリューションとして柔軟に展開できます。 Unicenter NSM との併用によって、eTrust のソリューションは、エンタープライズ マネジメントにおける大規模なタスクの一部として、セキュリティの構築、導入、および管理を実現するための一貫性のあるアプローチを提供します。

CA： e ビジネスを管理するソフトウェア

次世代の e ビジネスでは、既存のビジネス基盤の活用と新しい技術の採用によって無限の機会がもたらされます。 その反面、管理が非常に複雑になるため、コンピュータの管理から、組織の内外のアプリケーション、データ、およびビジネス プロセスの統合および管理まで、さまざまな課題が発生します。 このような課題の解決は CA にお任せください。 CA は、e ビジネスがこれらの重要な課題に対処するためのソリューションを提供しています。 CA は、業界トップの e ビジネス業務管理、e ビジネス情報管理、および e ビジネス インフラストラクチャ管理製品を通して、拡大した世界経済においてすべての利害関係者を満足させる、最先端の統合的ソリューションを提供している唯一の企業です。

詳細情報

この「導入ガイド」をひととおり読み終えた後、多数のリソースから詳細情報を入手できます。 製品版 CD には、ソフトウェアの説明ドキュメントに加えて、この製品の統合的で多機能な各コンポーネントが詳しく解説されているドキュメントが含まれています。

詳細については、テクニカル サポート(http://ca.com/support)にお問い合わせください。

オープンな分散ネットワーク環境は安全ですか?

ほとんどの企業では、財務取引、顧客情報、極秘の人事記録などの重要な情報を分散サーバに保管しています。 このようなデータへのアクセスを保護および管理することは、企業にとって重要なビジネス要件です。 しかし、残念ながら、オープン システム サーバは充分なデータ セキュリティを備えていません。 実際、基礎となるオペレーティング システムに「セキュリティ ホール」が存在するために、分散サーバは不正なアクセスを許してしまうことがあります。 Windows および UNIX のオペレーティング システムは、いずれもスーパーユーザという管理者の概念に基づいて設計されています。アプリケーション、データ、および監査ログへのフル アクセス権を持つこの特権ユーザ アカウントがシステムの脆弱性の原因となっています。

注: 特に明記されている場合を除いて、Windows という用語は、eTrust AC がサポートする任意の Microsoft Windows オペレーティング システムを指します。

Windows および UNIX のスーパーユーザ特権

これらのシステムにおける最も深刻な問題の 1 つに、システムのスーパーユーザ(管理者)が原因でセキュリティが脅かされるということがあります。 管理者は、システム上であらゆるタスクを実行したり、すべてのファイルを表示または変更したりできる、特別な権限を持つユーザです。 スーパーユーザは、これらのオペレーティング システムにおける最大のリスクの 1 つと考えられます。スーパーユーザ アカウントを使用すると、システム サービスの終了、重要なファイルの削除、機密情報へのアクセス、およびその監査証跡の削除を実行できるためです。 また、多くの場合、スーパーユーザ アカウントは、データのバックアップ、アカウントの作成および削除、またはパスワードの再設定を行うために、他のシステム管理オペレータにも与えられています。 スーパーユーザは、ハッカーによる攻撃を最も受けやすいユーザ アカウントでもあります。ハッカーは、このアカウントを攻撃して侵入することさえできれば、ほとんど何でもできることを知っています。

コンピューティング環境の保護

eTrust AC によって、企業はユーザのアクセス権を一元管理し、あらかじめ設定されている基本的なセキュリティ ポリシーをすぐに実行できます。 eTrust AC は、適切なユーザが適切な情報にアクセスすることを保証します。 eTrust Access Control は、企業全体の Windows システム サーバに存在するデータやアプリケーションへのアクセスに対するセキュリティを事前に確保します。

eTrust AC は、Dynamic Security(DSX)技術によって、システム設定に介入することなく、信頼性の高い保護機能を提供します。DSX は、セキュリティを脅かす恐れのある要求をリアルタイムでダイナミックにインターセプトします。このために、オペレーティング システムのカーネル部分に永久的な変更を加える必要はありません。 これにより、サーバの処理に影響を与えることなく、高レベルのセキュリティが提供されます。 汎用ファイル保護などの、eTrust AC の高度な機能により、Windows オペレーティング システムのセキュリティが大幅に強化されます。 管理者は、汎用ファイル保護のワイルドカード オプションを利用して、関連するファイルやプログラムのグループを保護できます。 この機能によって、強力で包括的なアクセス ポリシーを簡単に作成できます。

ホストベースの侵入防止

eTrust AC には、ホストベースの侵入防止システム(HIPS)の多数の機能が備わっており、外部からのワーム攻撃またはマルウェアによる障害といったセキュリティ リスクを軽減します。 eTrust AC のスタック オーバーフロー防止(STOP)機能、トロイの木馬防止機能、事前定義されたアプリケーション セキュリティ テンプレートのサンプル、およびアプリケーション動作プロファイリング プログラムを使用することで、管理者は重要なサーバをさらに強力に保護でき、セキュリティ パッチを配布してシステムの脆弱性を修正する時間を得ることもできます。

データとアプリケーションの保護

企業の成功は、データとアプリケーションの完全性と機密保全にかかっています。 eTrust AC を使用すると、ユーザおよびプログラムは必要な情報に適切にアクセスできます。情報への不正なアクセスはすべて阻止され、ログに記録されます。

eTrust AC では、アプリケーションのセキュリティを強化するために、セキュリティ ポリシーをカスタマイズできます。また、CA は、業界の主要なソフトウェア ベンダと提携することにより、eTrust AC で特定のアプリケーションへのアクセスを制御できるようにしています。 この強力なソリューションにより、ビジネス クリティカルなアプリケーションが完全に保護されます。

ユーザ アカウントとパスワードの管理

e ビジネス マーケットにおける企業の成長に伴い、異なる地域またはシステムのドメイン、および多様な部門にわたってユーザを管理する必要があるため、システム管理者の仕事量は大幅に増加します。 さまざまなシステムまたはプラットフォームでユーザ アカウント、パスワード、およびセキュリティ ポリシーを同期化することは非常に困難な作業です。この作業ではエラーや複雑な処理を伴い、応答時間が長くなり、コストもかかります。

複数のサーバの保護

ネットワーク上の複数のサーバに関するセキュリティの問題を解決するために、eTrust AC には、Policy Model データベース(PMDB)インフラストラクチャが用意されています。 PMDB では、アカウント、パスワード、およびセキュリティ ポリシーの同期化作業を、サブスクライブした階層ノードに対して安全かつ正確に実行できます。 eTrust AC の設計上の重要な目標の 1 つに、ネットワーク接続が正常に機能していない場合でも、指定されたサーバに対するセキュリティを強化することがあります。 結果的に、ルールを分散管理することによって、各サーバを独自に保護できます。

一貫性のあるクロスプラットフォーム セキュリティの促進

全体的なビジネス要件を満たすために、eTrust AC を使用して、各システムのセキュリティ レベルを向上させることができます。 1 つの eTrust AC セキュリティ ポリシーを一元的に作成し、さまざまな Windows および UNIX オペレーティング システムに自動的に配布して適用できます。 最終的には、最小限の時間と労力で、堅牢で一貫性のある高レベルのサーバ セキュリティを実現します。

これに対し、eTrust AC を使用しない場合、管理者はコンピュータ システムごとに個別のセキュリティ ポリシーを作成して維持する必要があります。これには、膨大な時間と作業を伴います。 また、企業規模のセキュリティ基準は、セキュリティ レベルが最低のシステムをベースに作成される場合が多いため、ほとんどの組織のセキュリティ要件は満たされないことになります。

ポリシーは、企業レベルで作成、管理、配布することも、特定のアプリケーションのセキュリティ要件に応じてカスタマイズすることもできます。 この完全なセキュリティ ソリューションは、会計部門や開発部門など個々の部門から、大規模な企業全体に至るまで、あらゆる規模の組織に導入できます。 ポリシーの導入により、オペレーティング システムのセキュリティと監査機能が強化されます。また、クロスプラットフォームでのアクセス制御により、分散システムで重要なプロセスおよび機密情報のセキュリティが確保されます。

オープンで拡張可能なこのポリシーは、業界標準のすべてのプラットフォーム、データベース、およびアプリケーションをサポートし、あらゆるリソースを保護する公開インターフェースを備えている強力なソリューションです。 eTrust AC は Unicenter TNG との通信ができるため、エンタープライズ マネジメントにおける大規模なタスクの一部として、セキュリティの構築、導入、および管理を行うための強力で統合的なソリューションを提供します。

特徴

eTrust AC には、企業のセキュリティを管理するための多数の機能が備わっています。

集中管理

eTrust AC により、管理者のワークステーション、および eTrust AC がインストールされている他のすべてのワークステーションを集中管理できます。

自己防衛機能

自己防衛メカニズムは、ハッカーやその他のユーザによる eTrust AC サービスの停止を防止します。 また、eTrust AC のファイルと監査データも保護します。

プロファイル グループ

eTrust AC により、グループ メンバシップに基づいてセキュリティの役割を設定できます。 たとえば、管理者グループと、そのグループのメンバであるユーザに与える権限を制限することができます。

レジストリ保護機能

eTrust AC では、権限のないユーザがシステム パラメータを変更しないように、レジストリが保護されます。 権限のあるユーザは、必要に応じてレジストリの設定を更新できます。

プロセス保護機能

eTrust AC は指定されたプロセスを保護し、強制終了(kill)されないようにします。また eTrust AC のプロセス保護機能は、Windows サービスおよび他の非対話形式の Windows アプリケーションの保護にも役立ちます。

ネットワーク保護

eTrust AC は、送受信ネットワーク接続を規制して、ネットワーク サービスおよびポートへのアクセスを制御します。

SPECIALPGM 保護機能

eTrust AC では、論理ユーザだけがアクセスできるように、通常 SYSTEM アカウントとして実行する必要があるシステム サービスなどの特定のプログラムが保護されます。

ログオン保護機能

アカウントの有効期限や日時の制限など、さまざまな方法でユーザのログオンを制限できます。

プログラムおよびファイルのシグネチャ

eTrust AC では、プログラムおよびファイルにシグネチャを追加することで、プログラムおよびファイルが保護されます。 署名を変更すると、プログラムまたはファイルは untrusted になり、アクセスできなくなります。

タスクの委任

eTrust AC では、一般ユーザが管理タスクを実行できるように、必要な権限を一般ユーザに与えることができます。 これを「タスクの委任」といいます。 このようなきめ細かな方法でタスクを委任できる(つまり、管理権限を付与できる)機能は、eTrust AC の最も重要な機能の 1 つです。

ファイル保護の強化

現在 Windows で使用されている、Windows File System(NTFS)や File Allocation Table(FAT)などのすべてのファイル システムが保護されます。 また、CDFS と HPFS もサポートされます。

スタック オーバーフロー防止機能 (STOP)

STOP は、ハッカーがスタック オーバーフローを悪用できないようにします。ハッカーはシステムに侵入するために、スタック オーバーフローを悪用してあらゆるコマンドを実行します。

クロスプラットフォームのサポート

管理者は、Windows および UNIX のコンピュータに対して、類似するセキュリティ ポリシー、または同一のセキュリティ ポリシーを作成、実装、および維持できます。

Active Directory のサポート

多くの組織はユーザ データ ストアを Active Directory または LDAP ベースのリポジトリに一元管理する方向に進んでいます。 eTrust AC では、eTrust Identity and Access Management を使用することで、外部ユーザ(外部リポジトリで定義されたユーザ)をサポートします。つまり、外部ディレクトリにユーザを定義でき、eTrust Identity and Access Management は、これらのユーザを eTrust AC データベースに関連付けます。 また、eTrust AC では、Active Directory または Windows NT ユーザ アカウント データベースであるセキュリティ アカウント マネージャ(SAM)のいずれかに保存されているネイティブ ユーザを作成、変更、または削除できます。

ポリシー管理システム

eTrust AC は、管理者がポリシー セット(バージョン管理、配布、およびリモート ダウンロードの可否)を使用して、部署内のセキュリティ ポリシーを簡単に管理できる、独立したポリシー管理システムを提供しています。これにより、すべてのサブスクリプション サーバが最新のセキュリティ ポリシーを確実に取得することができ、バージョン制御が簡単になります。

eTrust AC を使用すると、以下の 2 通りの方法で 1 台の中央コンピュータから複数のデータベースを管理できます。

- 自動的なルール ベース ポリシー更新

  中央のデータベース(PMDB)で定義した通常のルールは、設定された階層内のデータベースに自動的に伝達されます。

- 拡張ポリシー ベース管理およびレポート

  集中管理されたポリシー(ルールのグループ)は、設定された階層内のすべてのデータベースに自動的に展開、伝達されます。 展開したポリシーのバージョンを削除(展開を解除)したり、展開のステータス、展開の偏差、および展開の階層について報告することもできます。 この機能を使用するには、追加のコンポーネントをインストールおよび設定する必要があります。

アプリケーション ポリシー生成プログラム

自動ポリシー生成プログラムが提供されており、適宜アプリケーションの動作をプロファイリングしてセキュリティ ポリシーを生成できます。 この自動ポリシー生成プログラムによって、アプリケーションに対してセキュリティ エンベロープが作成され、これらのルールを構築するのに必要な展開の労力が大幅に軽減されます。

第 2 章: オペレーティング システム セキュリティの強化

このセクションには、以下のトピックが含まれます。

コンポーネント、機能、およびインストールに関する考慮事項

オープンな分散コンピューティングという新しいパラダイムの登場により、コンピュータ セキュリティに対する新たな要求が発生しました。 種類の異なるプラットフォームを統合するタスクは、いっそう複雑なものになります。 セキュリティに関する重要な課題として、異種システムに対応し、一貫したセキュリティを保証するセキュリティ ソリューションの導入が急務になっています。 一方、大手企業による吸収合併はますます盛んに行われています。 これに伴い、急激な拡張、分散処理能力、合理化された集中管理、複数のプラットフォームに対するサポートなど、新しいレベルのセキュリティ要件が発生しました。

eTrust AC には基本的なポリシーが組み込まれているので、細かい設定を行わずにすぐに使用できます。オープンで拡張可能なこのポリシーは、業界標準のすべてのプラットフォーム、データベース、およびアプリケーションをサポートし、あらゆるリソースを保護する公開インターフェースを備えている強力なソリューションです。

ユーザとアクセス権限の管理を一元化した使い勝手のよさによって、企業は目下の eビジネスのチャンスを確実に開拓することができます。 eTrust セキュリティ ソリューションの一部である eTrust AC は、Unicenter NSM との相互運用ができるため、エンタープライズ マネジメントにおける大規模なタスクの一部として、セキュリティの構築、導入、および管理を実現できる強力で包括的なソリューションを提供します。

eTrust AC のコンポーネント

eTrust AC には、データベース(seosdb)、2 つのドライバ(seosdrv および drveng)、多数のサービス(Watchdog、Agent、Engine、Policy Model、タスク委任機能など)、およびグラフィカル ユーザ インターフェースが含まれます。

データベース

データベースには、組織内のユーザおよびグループの定義、保護が必要なシステム リソース、およびユーザとグループによるシステム リソースへのアクセスを管理するルールが格納されます。

ドライバ

ドライバを使用して、ファイルを開く要求、レジストリ キーにアクセスする要求、プロセスを終了する要求、またはネットワーク アクティビティを実行する要求をインターセプトします。 ドライバは、これらの要求を Engine に渡し、Engine から要求の許可または拒否の決定を受け取り、この決定をオペレーティング システムの元のシステム コールに転送します。オペレーティング システムは、ドライバから受け取った応答に基づいて処理を継続します。

Watchdog

Watchdog は、他の eTrust AC サービスが実行されていることを常時チェックします。 Watchdog は、他のサービスが停止していることを検出すると(ただし、停止することはほとんどありません)、ただちにそのサービスを再開します。

Agent

Agent は、TCP/IP 上の専用アプリケーション プロトコルを使用し、eTrust AC ユーザのセキュリティを管理することで、eTrust AC クライアントと通信します。

Engine

Engine はデータベースを管理します。すべてのデータベースの更新を制御し、ドライバおよび Agent から受信したアクセス権の要求を付与するかどうかを決定し、Watchdog サービスが実行中かどうかをチェックし、Watchdog が停止した場合は Watchdog を再開します。

Engine では、データベース アクセス要求および意思決定の両方が処理されます。これによって、プロセス間通信を最小限に抑えて最大の効率を達成しています。

Policy Model

何百もの eTrust AC データベースを個々に管理することは、現実的ではありません。eTrust AC には、1 台のコンピュータから多数のコンピュータを管理できるコンポーネントである Policy Model サービスが用意されています。 Policy Model サービスの使用は任意ですが、このサービスを使用すると、大規模なサイトでの管理を大幅に簡略化できます。

タスクの委任

eTrust AC では、一般ユーザが管理タスクを実行できるように、必要な権限を一般ユーザに与えることができます。 これを「タスクの委任」といいます。

グラフィカル ユーザ インターフェース

ポリシー マネージャは、eTrust AC のすべての機能を実行できるグラフィカル ユーザ インターフェース(GUI)です。

注: ポリシー マネージャの詳細については、「管理者ガイド」を参照してください。

eTrust AC の機能

eTrust AC では、複数のネイティブ Windows を集中管理し、ネイティブ Windows のセキュリティを大幅に向上させることができます。また、eTrust AC はそれ自体を保護することもできます。 以降のセクションでは、Access Control の各機能について説明します。

Windows の管理

ネットワークに分散している Windows 端末に eTrust AC をインストールすると、中央の 1 つの端末からそれらの端末(各端末が属しているドメインに関係なく)をすべて一元管理できます。 これを行うには、ポリシー マネージャを使用するか、selang というコマンド ライン言語を使用します。

ポリシー マネージャ

ポリシー マネージャは eTrust AC の GUI です。ポリシー マネージャを使用することで、eTrust AC のすべての機能を実行できます。

注: ポリシー マネージャの詳細については、「管理者ガイド」を参照してください。

selang

selang は eTrust AC のコマンド ライン言語です。 selang を使用してスクリプトを記述することもできます。 コマンド プロンプト ウィンドウ、または ポリシー マネージャの[コマンドとスクリプト]ツールから selang を呼び出して、selang のコマンドを実行できます。

注: selang とそのコマンドの詳細については、「リファレンス ガイド」を参照してください。

eTrust AC の自己防衛機能

ハッカーまたはユーザが eTrust AC のサービスを故意または過失により停止させることは事実上不可能です。 eTrust AC の実行中に、権限のないユーザが eTrust AC のファイルおよびデータを変更または消去することも実質的に不可能です。これは eTrust AC が特別なファイル シグネチャを使用しているためです。

管理者アカウントの制限

通常、Windows を管理するユーザ(管理者)は、システム セットアップ時に自動的に作成される、事前定義されたグループのメンバです。 事前定義された各グループは、特定のシステム機能のセットを実行します。 グループのメンバであるユーザは、グループの機能をすべて実行できます。

Windows で最も強い権限を持つグループは、Administrators グループです Windows では、Administrator という 1 つのアカウントが Administrators グループに作成されます。 Administrators グループのすべてのメンバは、ユーザの作成、削除、および変更から、サーバのロック、環境設定の変更、およびシャットダウンまでの広範なタスクを実行できます。

Windows におけるセキュリティ上の主なリスクの 1 つは、権限のないユーザが Administrators グループのユーザ アカウントに対する制御権を手に入れる可能性があることです。 Administrator アカウントへのアクセスを許可してしまうと、システムは重大な危険にさらされることになります。

eTrust AC を使用すると、Administrator アカウントに与える権限を制限し、Administrators グループに属するユーザの権限を制限できます。 これにより、Windows システムの脆弱性をカバーします。

ネイティブ Windows セキュリティの管理

eTrust AC を使用すると、Windows セキュリティに関する以下の要素を管理できます。

レジストリ保護機能

Windows レジストリは、デバイス ドライバ、環境設定の詳細、ハードウェア、環境、およびセキュリティの設定を制御するパラメータをはじめ、大半のオペレーティング システム パラメータを集中管理するデータベースです。

eTrust AC では、権限のないユーザがシステム パラメータを変更しないように、レジストリが保護されます。 権限のあるユーザは、必要に応じてレジストリの設定を更新できます。

ファイルの保護

Windows では、異なる複数の種類のファイル システムの 1 つが使用されます。 最も一般的なファイル システムは、FAT および NTFS です。 NTFS ファイル システムを使用している場合は、各ファイルに対して Access Control List（ACL）を作成および更新することにより、システム内のファイルが Windows によって保護されます。eTrust AC では、ファイルの ACL がサポートされます。

パスワード保護機能

eTrust AC では、Windows のネイティブ セキュリティと同様に、パスワードを保護し、パスワード品質を向上させることができます。この場合、独自のメカニズムが使用されます。eTrust AC では、以下の操作を行うことができます。

- パスワードの最長有効期間の指定
- パスワードの最低文字数の指定
- ユーザのパスワード履歴を最大 20 件まで保存できます。
- ログインに繰り返し失敗した場合のアカウントのロック
- パスワード変更前の Windows へのログインの強制

Server Manager の機能

eTrust AC では、Windows NT のプログラム バーの[サーバ マネージャ]で、他のネイティブ Windows リソースを管理できます。 保護されている Windows リソースは、以下のとおりです。

COM

COM クラスのレコードでは、[コントロール パネル]-[ポート]で表示される、シリアル ポート(COM)またはパラレル ポート(LPT)を備えたデバイスを定義します。

デバイス

DEVICE クラスのレコードでは、Windows ハードウェア デバイス([コントロール パネル]-[デバイス]で表示される)を定義します。

ディスク

DISK クラスのレコードでは、システム ボリュームを定義します。

ドメイン管理

DOMAIN クラスのレコードでは、共通のデータベースとセキュリティ ポリシー(ドメイン)を共有するコンピュータの集合を定義します。

プリンタ

PRINTER クラスのレコードでは、メディアに視覚的なイメージを複製できる Windows コンピュータ システムに接続されたデバイス(PRINTERS フォルダに表示される)を定義します。

プロセス

PROCESS クラスのレコードでは、実行可能プログラム、一連の仮想メモリ アドレス、およびスレッド(Windows のタスク マネージャに表示されます)で構成されているオブジェクトを定義します。

サービス

SERVICE クラスのレコードでは、Windows サービス([コントロール パネル]-[サービス]で表示されます)を定義します。

Share

SHARE クラスのレコードでは、ディレクトリ、ファイル、プリンタ、および名前付きパイプなど、ネットワーク ユーザが使用するデバイス、データ、プログラムなどの共有リソースを定義します。

Windows セッション

SESSION クラスの各レコードは、ローカル ホスト上のユーザ セッションを定義します。 このレコードには、ユーザ名、コンピュータ名、接続経過時間、および使用中のリソースが含まれます。

Windows ネイティブ セキュリティの拡張

以下の eTrust AC の機能により、ネイティブ Windows セキュリティが拡張されます。

一般ユーザに与える管理者権限

eTrust AC では、Administrators グループのメンバでなくても管理タスクを実行できるように、必要な権限を一般ユーザに与えることができます。 これを「タスクの委任」といいます。 このようなきめ細かな方法でタスクを委任できる(つまり、管理権限を付与できる)機能は、eTrust AC の最も重要な機能の 1 つです。

ファイル保護の強化

eTrust AC では、現在 Windows で使用されているすべてのファイル システムが保護されます。 最も一般的に使用されるファイル システムは、Windows File System (NTFS)と File Allocation Table(FAT)の 2 種類です。 eTrust AC では、CDFS (CD-ROM ファイル システム)および HPFS(OS/2 のファイル システム)もサポートしています。

eTrust AC により、File Allocation Table(FAT)に対する総合的なセキュリティ ソリューション、および NTFS や CDFS などその他のファイル システムに対する特別なセキュリティ レイヤが提供されます。

汎用ファイル保護

汎用ファイル保護は、指定されたワイルドカード パターン(正規表現)に一致するすべてのファイルを保護する機能です。 指定したワイルドカード パターンに一致する名前のリソースが、指定した包括的なアクセス ルールによって保護されます。 eTrust AC により、ファイルを包括的に保護できます。

リソースが複数の包括的なアクセス ルールに一致する場合は、eTrust AC によって、ファイルに対して最も厳密に一致するルールが選択されます。

汎用ファイル保護の機能を使用すると、ほんのわずかなセキュリティ ルールを定義するだけで、保護の必要な多数のファイルを保護できます。

パスワード保護の強化

Windows ネイティブ セキュリティによって、非常に多くのユーザ パスワードに関する保護『P. 23』が提供されます。 eTrust AC では、パスワード保護が大幅に拡張されているため、ハッカーによるパスワード盗用の可能性はきわめて小さくなりました。

eTrust AC を使用すると、より安全で確実なパスワードをユーザが選択するように、ルールを追加できます。 たとえば、最低限必要な英字、数字、特殊文字、小文字、または大文字の数を選択するようにユーザに要求できます。 また、置き換えられる旧パスワードと、ユーザが選択した新しいパスワードで、前者の文字列が後者の文字列に含まれないようにすることもできます。

プロセス保護機能

eTrust AC は指定されたプロセスを保護し、強制終了(kill)されないようにします。また、eTrust AC プロセス保護機能は、Windows サービスおよび他の非対話形式の Windows アプリケーションの保護に役立ちます。

SPECIALPGM 保護機能

eTrust AC では、論理ユーザだけがアクセスできるように、通常 System アカウントとして実行する必要があるシステム サービスなどの特定のプログラムが保護されます。

プログラムおよびファイルの保護機能

eTrust AC では、プログラムおよびファイルにシグネチャを追加することで、プログラムおよびファイルが保護されます。 署名を変更すると、プログラムまたはファイルは untrusted になり、アクセスできなくなります。

スタック オーバーフロー防止機能 (STOP)

STOP により、ハッカーはスタック オーバーフローを悪用できなくなります。ハッカーはシステムに侵入するために、スタック オーバーフローを悪用してあらゆるコマンドを実行します。

Program Pathing

Program Pathing は、特定のファイルが特定のプログラムを介してのみアクセスされるように要求する機能です。 Program Pathing により、機密ファイルのセキュリティを大幅に強化できます。 eTrust AC の Program Pathing を使用すると、システム内のファイルに対する保護を強化できます。

B1 セキュリティ レベル認証

eTrust AC には、セキュリティ レベル、セキュリティ カテゴリ、およびセキュリティ ラベルという「Orange Book」の B1 機能があります。

Active Directory の管理

以下の eTrust AC の機能により、Windows Active Directory サービスが拡張されます。

ユーザのプロパティとグループのプロパティ

新しいバージョンの Windows では、ユーザを一意に識別する複数のプロパティ(Full Name、Logon Name など)が使用されますが、旧バージョンの Windows でユーザ プロパティを管理する Microsoft Net API ではこれらのプロパティをサポートしていません。

<eTrust AC ではこれらのプロパティがサポートされているため、ユーザおよびグループの Active Directory レコードのユーザ定義プロパティを管理できます。 これらのプロパティをサポートすることで、組織単位の管理も強化されます。

コンテナの管理

eTrust AC では、Active Directory の組織単位(OU)の作成および編集をサポートしています。 OUは、ユーザ、グループ、コンピュータ、および他のオブジェクト タイプが配置される論理コンテナです。 eTrust AC では、**ユーザ、グループ、**および**コンピュータ**という 3 つの一般的な種類のオブジェクトがサポートされています。また、オブジェクトの種類として OU をサポートすることにより、OU のネスト化もサポートされます。 これにより、以下の操作を行うことができます。

- OU、またはデフォルトのコンテナ USERS 以外のコンテナに新しいユーザとグループを作成する
- Active Directory からコンテナまたは OU を作成または削除する
- あるコンテナまたは OU から別のコンテナまたは OU にユーザまたはグループを移動する
- eTrust AC 内から Active Directory の階層構造(親子関係)を参照できます。

プライマリ ドメイン コントローラに OU クラスのオブジェクトを作成できます。

注: OU クラスは、Active Directory がインストールされている Windows 2000 Advanced Server 端末でのみ利用できます。 その他の構成のコンピュータで eTrust AC を実行している場合は、このクラスを適用できません。

Windows および UNIX のセキュリティ管理

大規模な組織では、Windows および UNIX の 2 つのシステムが混在する場合がよくあります。 こうした状況では、完全なセキュリティを維持することは困難です。 最も望ましいのは、すべてのシステムに実装できる単一のセキュリティ ポリシーを作成することです。

eTrust AC を使用して、以下の作業を行うことができます。

- UNIX および Windows に使用する、単一の共通セキュリティ ポリシーを作成する
- eTrust AC を使用して、作成したポリシーを実装できます。
- 1 台の Windows ワークステーションを使用して、Windows および UNIX の両方の環境のセキュリティを管理する

行った変更を異なる環境の多数のワークステーションに伝達する eTrust AC の機能により、管理のオーバーヘッドを大幅に削減できます。

以降のセクションでは、共通のセキュリティ ポリシーで特に重要ないくつかの要素について説明します。

ユーザの一括メンテナンス

サイトに eTrust AC をインストールすると、すべてのユーザを含む 1 つの eTrust AC データベースに対してメンテナンスを行うことができます。 これは、ユーザ メンテナンスを一度だけ行う必要があることを意味します。 eTrust AC では、更新内容を受け取る必要があるすべてのワークステーション(UNIX および Windows の両方)に対して、追加、変更、および削除を伝達できます。

グループの一括メンテナンス

多くの場合、特定のプロジェクト、または組織内の特定の部門に所属するユーザをグループ化すると管理が容易になります。 Windows、UNIX、および eTrust AC のすべてで、ユーザのグループを定義できます。 ユーザに権限を割り当てるのと同様に、グループに対して権限を割り当てることができます。 グループを使用すると、同じ権限を個々のユーザに繰り返し割り当てるのではなく、グループに対して 1 度割り当てればよいため、作業の負荷を軽減できます。 グループに権限を割り当てたら、各ユーザはグループの権限を受け取ります。

eTrust AC を使用して管理を行うと、UNIX および Windows の両方の環境で使用できるグループを作成し、メンテナンスできます。

アクセス ルールの一括メンテナンス

Policy Model サービスにより、Windows および UNIX の両方に使用できる 1 組のアクセス ルールを作成し、メンテナンスできます。 Policy Model データベース(PMDB)により、セキュリティ データベースの内容およびセキュリティ データベースに対して加えられた変更をすべてのサブスクライバに伝達できます。 Windows および UNIX の両方のワークステーションを同一の PMDB にサブスクライブできます。

PMDB とサブスクライバ間の通信は、通常、PMDB のデータベースからサブスクライバに変更内容を送信する一方向通信です。 サブスクライバは、オンラインであることを PMDB に通知するときにのみ PMDB と通信し、サブスクライバの停止中に PMDB が送信したすべての変更内容の再送を要求します。 このように設計されているため、ネットワーク トラフィックが最小限に抑えられ、サブスクライバの整合性が保証されます。

パスワードの同期

適切なセキュリティ ポリシーの主な機能の 1 つは、ユーザに適切なパスワードを選択させることです。 ユーザにとっては、システム全体で使用できる 1 つのパスワードを覚えるだけでよければ、その方が簡単です。 eTrust AC を実装すると、1 組のパスワード ルールを適用し、2 つのシステム間でパスワードの同期をとることができます。

PMDB により、適切なパスワードを定義するルールを伝達できます。 また、新規パスワードおよび変更したパスワードを、メインフレーム コンピュータを含むすべてのサブスクライバ端末に伝達することもできます。

注: 詳細については、「実装ガイド」を参照してください。

eTrust AC サービスの管理

デフォルトでは、すべての eTrust AC サービスが自動的に開始されます。 eTrust AC サービスの開始を自動から手動に変更したり、サービスを無効にしたりすることができます。 サービスにアクセスするには、以下の手順に従います。

1. eTrust AC を閉じます。
2. Windows のコントロール パネルから[Services]を起動します。
3. 変更または無効にするサービスを右クリックします。
4. [Startup Type]で[Automatic]、[Manual]、または[Disable]を選択して、サービスの開始方法を指定し、[OK]をクリックします。

eTrust AC ドキュメント

eTrust AC のドキュメントは PDF ファイル形式で提供されています。 PDF ファイルを参照するには、Adobe Reader が必要です。ご使用のコンピュータにインストールされていない場合は、Adobe Web サイトからダウンロードし、インストールしてください。

最新のガイドは、http://www.caj.co.jp/support/ で入手できます。

注: 製品版 CD にも適切なバージョンの Adobe Reader が用意されています。

readme ファイルに eTrust AC ドキュメントの全一覧があります。

次の章について

この章では、eTrust AC の特徴および機能について説明しました。次の章では、企業のシステムの完全性およびデータの機密性の保護について説明します。 次の章では、プログラムおよびファイルをユーザやグループから保護する方法について説明します。

第 3 章: 管理インターフェースの使用

このセクションには、以下のトピックが含まれます。

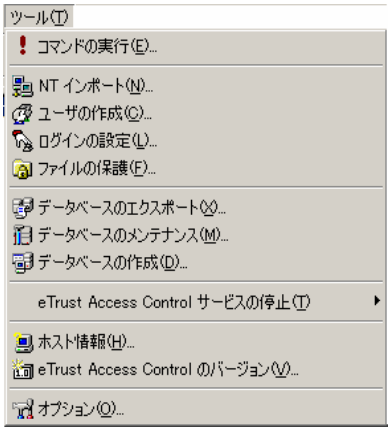
セキュリティ ポリシーの実装およびメンテナンス

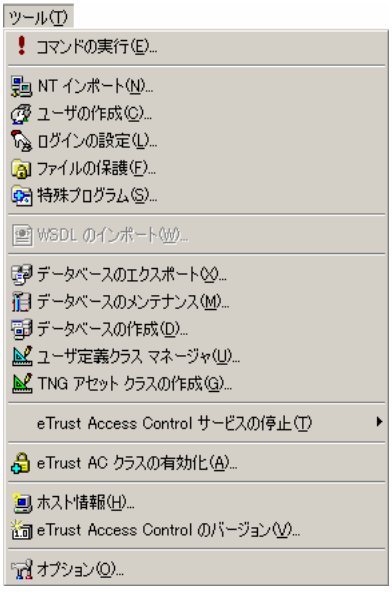
この章では、ポリシー マネージャについて説明します。ポリシー マネージャは、Windows および UNIX プラットフォーム上にあるデータベースを管理できる eTrust AC のグラフィカル ユーザ インターフェースです。

メニュー バーとツールバー

メニューには、開いているウィンドウに応じて、適切な情報が表示されます。 たとえば、[User]ウィンドウと[Resources]ウィンドウの[Edit]メニューは次のように異なります。

他の例として、[Tools]メニューを示します。 [User]ウィンドウと[Resources]ウィンドウの[Tools]メニューは次のように異なります。





[View]メニューから、ツールバーおよびウィンドウの表示を制御できます。

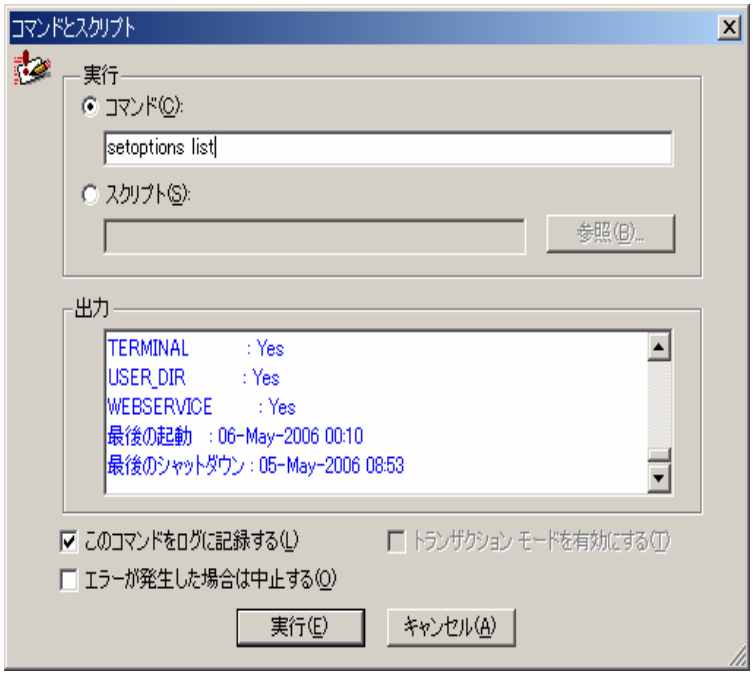
プログラム バー

ポリシー マネージャの機能は、eTrust アクセサとリソース、NT リソース、およびツールの 3 つのプログラム バーに分類されます。［File］-［Open］を使用して同一の機能を使用できます。

注: eTrust Web AC をインストールした場合は、eTrust Web AC 機能を管理する第 4 のバーが表示されます。 詳細については、eTrust Web ACのドキュメントを参照してください。

selang のコマンド

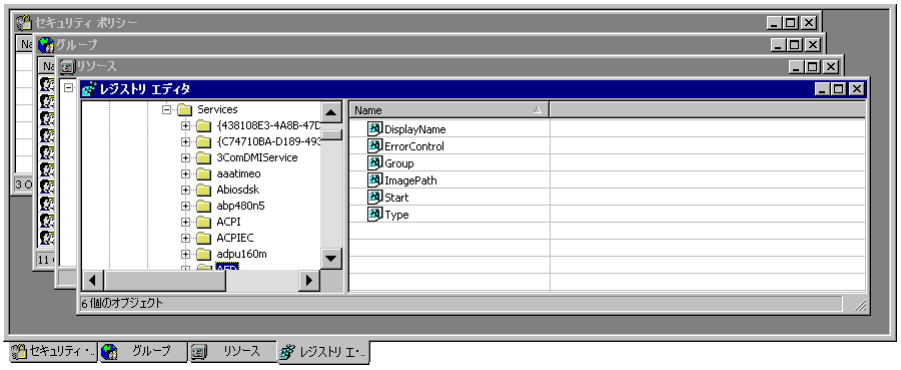
ポリシー マネージャの[ツール]メニューから[コマンドの実行]を選択して、selang のコマンドを発行できます。 [Commands and Scripts]ダイアログ ボックスの[Execute Command]フィールドにコマンドを入力します。



Admin のデフォルトの設定

GUI のデフォルトを設定するには、[Tools]メニューの[Options]を選択します。

すべてのオプションを変更できます。 [Appearance]タブおよび[Format]タブを使うとインターフェースをカスタマイズできます。 使いやすいように変更してください。 たとえば、[Workbook]モードではウィンドウにタブが表示されます。 このオプションは、多数のウィンドウを開いて作業する場合に便利です。



[Startup]タブでは、起動時のデフォルトを設定し、カスタム スプラッシュ画面をアクティブにします。 [作成]タブでは、新規ユーザおよびグループを作成するデフォルトの環境を定義します。 ツアーを実行するときのみに、eTrust のデフォルトを変更することをお勧めします(ツアー終了時の処理を最小限にすることができます)。

注: 設定は、[OK]をクリックするとただちに有効になります。

[ウィザード]

eTrust AC では、一般的な手順を実行するのに役立つウィザードが用意されています。

Login Protection Setup Wizard の使用

eTrust AC では、セキュリティにより、ユーザは権限のない端末からログインすることができません。 具体的には、各端末が TERMINAL クラス レコードに定義されていて、ユーザが使用する各端末の Access Control List(ACL)に各ユーザのアクセス権が定義されていることが必要となります。 これらの作業は、Login Protection Setup Wizard で行います。

1. ウィザード マネージャのツールバー ボタンをクリックして、ログイン保護設定ウィザードを起動します。 [Login Protection]を選択します。
2. 保護対象のユーザおよびグループを選択します。

   注: [保護されたユーザとグループ]ページでは、複数のユーザおよびグループを定義できます。
3. [ログイン端末]ページで、ユーザとグループがログインに使用できる端末、およびログインに使用できない端末を指定します。
4. [ユーザ アカウントの制限]ページで、指定したユーザおよびグループがログインできる曜日と時間帯を指定します。

   注: [平日]ボタンを使用すると、1 回のクリックで土曜日と日曜日の選択を解除できます。
5. 次のページで休日のログイン認証を指定して、[完了]をクリックします。

注: 特定の休日にログインを許可または禁止するには、このダイアログ ボックスを使用する前に休日を定義しておく必要があります。

Create User Wizard の使用

Create User Wizard を使用して、ユーザを特定します。 ウィザードの指示にしたがい、ユーザ属性(operator や administrator など)、パスワード、およびグループ メンバシップを指定します。

File Protection Wizard の使用

File Protection Wizard を使用すると、指定したファイルおよびディレクトリを保護できます。File Protection Wizard の指示にしたがい、保護対象のファイル、ファイルにアクセスできるユーザとグループ、およびこれらのユーザとグループのアクセス権のレベルを選択します。

NT Import Wizard の使用

インストール時に Windows ユーザおよびグループをインポートしなかった場合は、NT Import Wizard を使用して次の操作を行います。

- Windows データベースから、ローカル ホストのデータベースまたは PMDB にユーザをインポートする
- Windows データベースから、ローカル ホストのデータベースまたは PMDB にグループをインポートする

リモート ホストにインポートすることはできません。 Windows データベースを直接インポートするか、またはデータベースをスクリプト ファイル (.lng) として保存できます。

Special Program Wizard の使用

Create Special Program Wizard を使用して特殊なプログラムを保護できます。

システム サービスなどのプログラムに対して権限付与による保護を設定できます (通常、このようなプログラムは SYSTEM アカウントとして実行する必要があります)。 論理ユーザを使用するか、または省略するかによって、指定したプログラムへのアクセスを制限できます。

このウィザードでは、SPECIALPGM リソースが作成され、[ポリシー マネージャ]ウィンドウの[出力バー]に結果が表示されます。

Copy User Wizard の使用

Copy User Wizard を使用すると、次の操作を行うことができます。

- あるホストから別のホストまたは同じホストの PMDB にユーザ レコードをコピーする
- ユーザをコピーしながらグループに配属する
- 複数のユーザ レコードを別のホストまたは同じホストの PMDB にコピーする
- あるユーザ レコードをテンプレートとして使用し、同じホスト上に別のレコードを作成する
- ユーザ レコードをコピーするスクリプトを作成する

注: ユーザ コピー ウィザードにアクセスするには、Access Control のプログラム バーの[ユーザ]をクリックし、[編集]メニューから[ユーザのコピー]を選択します。

Copy Group Wizard の使用

グループ コピー ウィザードを使用すると、以下の操作を行うことができます。

- あるホストから別のホストまたは同じホストの PMDB にグループ レコードをコピーする
- あるホストから別のホストまたは同じホストの PMDB に、グループとともにメンバ ユーザ レコードをコピーする
- あるホストから別のホストまたは同じホストの PMDB に複数のグループ レコードをコピーする
- あるグループ レコードをテンプレートとして使用し、同じホスト上に別のレコードを作成する
- グループ レコードをコピーするスクリプトを作成する

注: グループ コピー ウィザードにアクセスするには、Access Control のプログラム バーの[グループ]アイコンをクリックし、[編集]メニューから[グループのコピー]を選択します。

次の章について

この章では、ポリシー マネージャについて説明しました。次の章では、アクセス許可やアカウントの制限などの設定と、この新しいソフトウェアの使用法について説明します。

第 4 章: 保護機能の紹介

このセクションには、以下のトピックが含まれます。

プログラムの保護とシステム ファイルの監視

本章では、eTrust AC をさらに活用するための次のステップとして、新規ユーザとグループの登録、ファイルとディレクトリの保護、権限のないユーザからのファイルの保護、Program Pathing とファイル名パターンによるファイルの保護、その他について説明します。

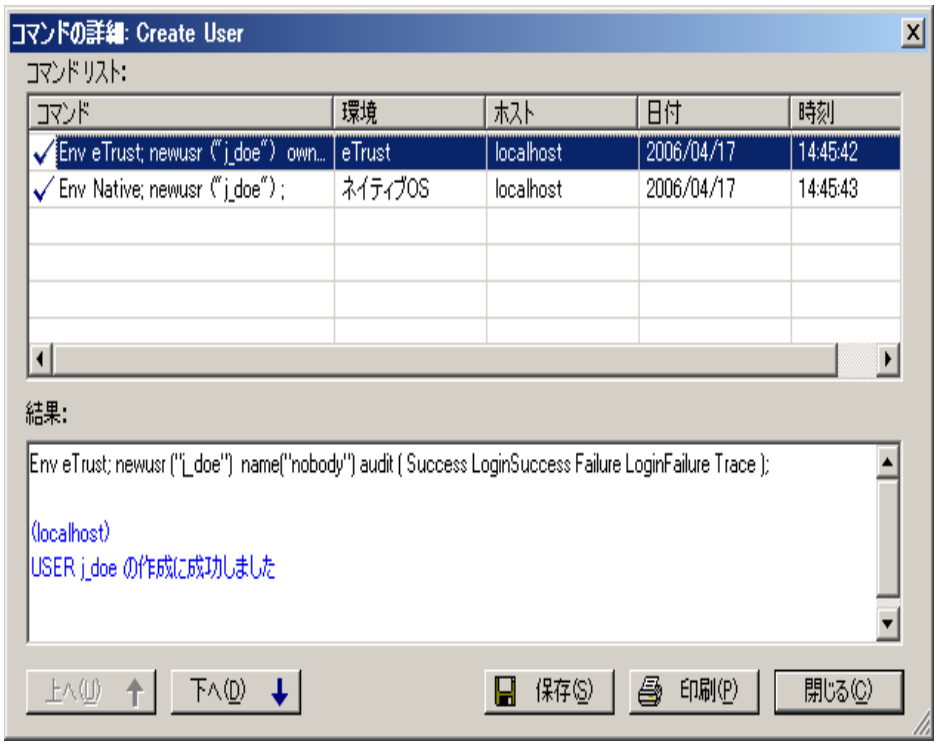
ユーザおよびグループの作成

ユーザを作成するには、以下の手順に従ってください。

1. ウィンドウの左側にあるプログラム バーの[ユーザ]アイコンをクリックします。
2. ツールバーの[新規作成]アイコンをクリックします。 [ユーザ名]テキスト ボックスに「j_doe」と入力します。 この時点ではパスワード オプションは省略します。
3. [User Attributes]をクリックします。 [所有者]フィールドに「**nobody**」と入力します。 j_doeは一般ユーザなので、[User Type]チェック ボックスはいずれもオンにしないでください。
4. [Miscellaneous]アイコンをクリックし、[Audit Information]を選択します。

   注: タイトルを見ると、作業中のパネルがわかります。
5. [All]をクリックし、[OK]をクリックして各ウィンドウを閉じます。

ウィンドウの下部の[Output Bar]に、新規ユーザが作成されたことを示すメッセージが表示されます。 エントリ行をダブルクリックし、[Details]ウィンドウを表示します。



ウィンドウの上部には、ポリシー マネージャによって生成された selang のコマンドが表示され、下部にはコマンドの実行結果が表示されます。 コマンドの実行結果を表示するには、各コマンドを選択します。

この例は非常に簡単なものでしたが、 より多くのパラメータを eTrust AC データベースのユーザ レコードに追加することも非常に簡単に行えます。

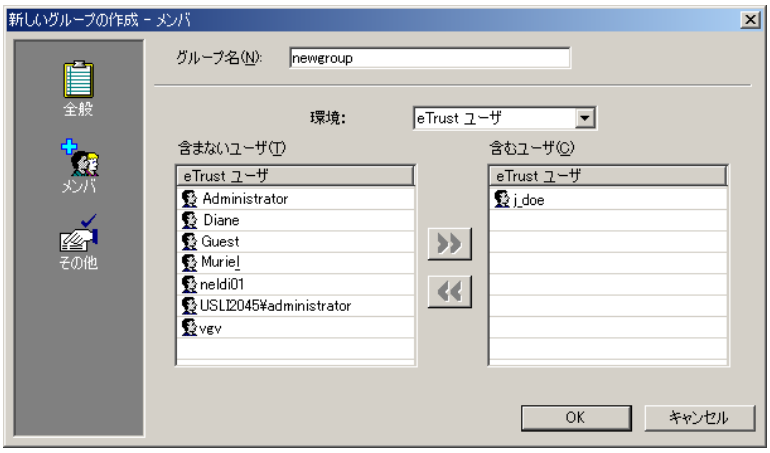
次に別の例を示します。 今度はグループを作成します。

1. プログラム バーの[Groups]アイコンをクリックし、次にツールバーの[New]アイコンをクリックします。 [新しいグループの作成]ウィンドウが表示されます。このウィンドウは[新しいユーザの作成]ウィンドウと同様です。

   注: [グループ]ウィンドウのどこかをマウスでポイントして右クリックしても、同じウィンドウを開くことができます。 [新しいグループ]は右クリックすると表示されるショートカット メニューのオプションです。

2. グループに名前を付けて、[所有者]に[**nobody**]を指定します。 スーパー グループを割り当てることもできます。 スーパー グループを割り当てると、新しく作成するグループはサブグループになり、作成時に変更または追加するプロパティ以外のすべてのプロパティがスーパー グループから継承されます。

3. [メンバ]アイコンをクリックし、新しいグループにメンバを追加します。

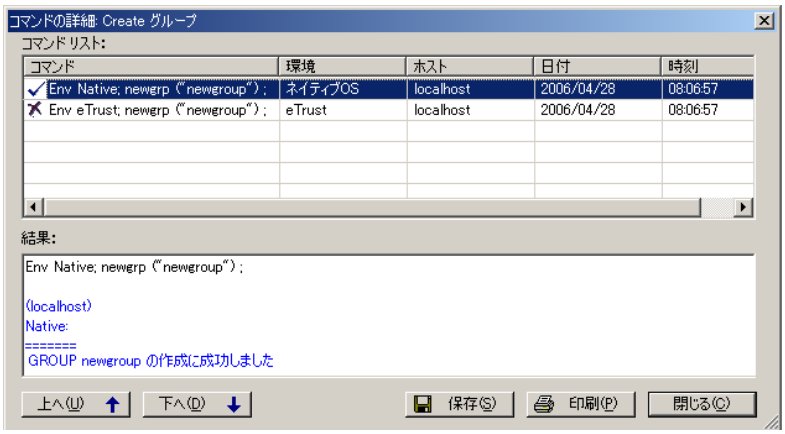


   この例では、1 人のユーザのみが追加されています。 さらにユーザを追加できます。一度に複数のユーザを追加するには、Shift キーまたは Ctrl キーを押しながらグループを選択します。

4. グループにユーザを追加した後に、[Miscellaneous]アイコンをクリックします。 日時の制限を追加し、[OK]をクリックして新しいグループを作成します。

   注: ユーザに割り当てた制限は、グループに割り当てた制限よりも優先されます。

5. ここで、コマンド詳細を表示して結果を確認します。



ファイルおよびディレクトリの保護

どのコンピュータ システムにも、最低 2 種類のファイルがあります。 オペレーティング システムが正常に機能するために必要なシステム ファイルと、 アプリケーションによってユーザが作成し、使用するアプリケーション ファイルの 2 種類です。

ファイルの種類に応じてどのような保護が必要かを判断し、その保護を実装する必要があります。 eTrust AC の主な利点の 1 つは、システム管理者も含めて、ファイルやディレクトリへの不正なアクセスを規制し、この保護を NTFS 以外のファイル システムにまで拡大できることです。

まず、この演習用にダミー ファイルを 1 つ作成します。

1. プログラム バーの[リソース]アイコンをクリックして、[リソース]ウィンドウを開きます。[System Resources]で、[File]をクリックします。
2. ツールバーの[新規作成]アイコンをクリックし、[参照]ボタンを使用してファイルを参照して、[所有者]として「**nobody**」を指定します。
3. 一部のユーザまたはグループにファイルへのアクセス権を与えます。 一部のユーザまたはグループにファイルへのアクセス権を与えるには、[権限の付与]をクリックし、[アクセサの追加]リスト ボックスの横にある[追加]ボタンをクリックします。 ユーザまたはグループを選択して[OK]をクリックします。 追加した名前が[Add Accessors]リスト ボックスに表示されます。

4. 各ユーザまたはグループを順に選択して、各ユーザまたはグループのアクセス権を選択します。

   管理者 adm1 には、[Delete]のみが選択されています。 これは管理者のアクセス権を制限する極端な例です。

   ユーザ p_jones にはフル アクセス権を与えました（p_jones のアクセス権は上の図に示されています）。 ただし、ユーザ Jones は Newgroup のメンバでもあります。このグループに与えられているのは読み取り許可のみです。 権限は追加されるので、ユーザ Jones は、Newgroup のメンバであることによって権限を制限されることはありません。

   このグループにはプログラム（Word）を選択したことに注意してください。 これは「Program Pathing」といい、このグループに属するユーザは指定されたプログラムを使用した場合にのみ、ファイルにアクセスできます。 Program Pathing により、機密ファイルのセキュリティを大幅に強化できます。 たとえば、この例の場合には、グループのユーザは誰も、メタデータを読み込むアプリケーションを使用してこのファイルを開くことはできません。

5. 最後に監査モードを指定し、[OK]をクリックしてファイル リソースを作成します。

6. コマンドの詳細をチェックし、selang のどのコマンドが発行されたかを確認します。

注: ファイル保護の詳細については、「リファレンス ガイド」の FILE クラスに関する説明を参照してください。

ファイル グループ

データベースにファイルを定義した後に、ファイルをグループに分け、グループ単位でアクセス許可を割り当てることができます。 たとえば、財務部のファイルを Finance という名前のグループにまとめ、役員と財務部の社員にのみアクセスを許可することができます。

部署内の個人やグループがアクセスする必要があるファイルに応じて、グループの個々のファイルやパターンにはそれぞれ異なるアクセサ許可を設定できます。 また、ファイル グループの中にファイル グループをネストして、ファイル アクセス許可の階層をきめ細かく管理することが可能です。

プログラムの保護

eTrust AC は、trusted computing base の一部とみなされるプログラムを定義します。 このクラスに属するプログラムは、変更されたかどうかが Watchdog 機能によって監視されるため、保護されたものとして信頼できます。 trusted プログラムが変更されると、変更されたプログラムは eTrust AC によって自動的に untrusted のマークが付けられ、実行できなくなります。

注: PROGRAM クラスにプログラムを定義する場合は、そのプログラムの FILE クラスのレコードも作成する必要があります。 レコードの作成順序は任意です。

プログラムを保護するには、[リソース]ウィンドウのシステム リソース セクションを確認します。

1. [プログラム]をクリックします。

   データベースには、すでに Microsoft Word のレコードがあります。 このレコードは、前の練習で NewGroup のプログラム パス手続きを実行したときに、eTrust AC によって自動的に作成されたものです。

2. Microsoft Word のエントリを右クリックして[プロパティ]を選択します。

   アクセサに対して、Execute アクセス許可のみを割り当てることができます。 アクセス許可を拒否すると、プログラムへのアクセスが拒否されます。

3. [全般]アイコンをクリックします。

   [全般]パネルには[信頼]チェック ボックスがあります。 Program レコードを作成すると、eTrust AC によってこのプロパティが設定されます。 プログラムが変更されると、eTrust AC によってこのプロパティが「untrusted」にリセットされ、プログラムの実行が制限されます。 問題を解決した後、このウィンドウで[trust]プロパティをリセットできます。

ファイルの監視

eTrust AC により、重要なシステム ファイルを監視できます。 SECFILE クラス(保護されたファイルを表すオブジェクトを持つクラス)のレコードを作成することにより、頻繁には変更されることのない重要なシステム ファイルを、権限のないユーザが変更しないことを確認できます。 Watchdog 機能は対象ファイルをスキャンして、これらのファイルに関する既知の情報に変更がないことを確認します。

監視対象として考慮すべきファイルの例を次に示します。

- \Winnt\system32\drivers\etc\hosts
- *\etc\services
- *\etc\protocol
- *\etc\networks

強制終了(kill)からのプロセスの保護

それぞれのアドレス空間で実行する実行可能ファイルは、kill コマンドによって強制終了されないように保護する必要があります。 特に、主要なユーティリティおよびデータベース サーバはサービス妨害(DoS)攻撃の主な標的になりやすいため、eTrust AC でプロセスを保護することをお勧めします。 また eTrust AC のプロセス保護機能は、Windows サービスおよび他の非対話形式の Windows アプリケーションの保護にも役立ちます。

eTrust AC は、通常の終了シグナル(TERM)と、アプリケーションがマスクできない 2 つのシグナル(Terminate Process および STOP)の 3 つの終了(Kill)シグナルからプロセスを保護します。

例として、タスク マネージャ(Taskmgr.exe)を保護します。

1. [Process]を選択し、[New]をクリックします。
2. ¥system32 サブ ディレクトリに Taskmgr.exe の新しいレコードを作成します。

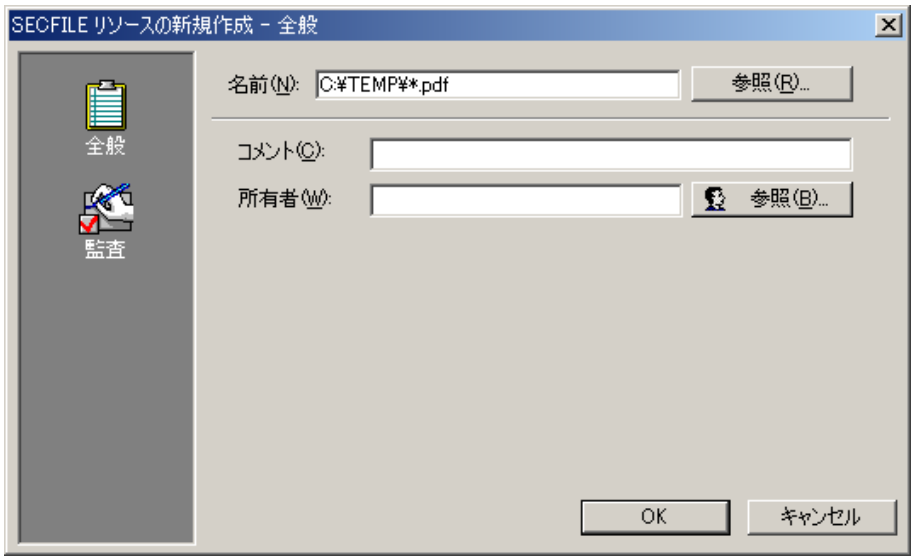
   注: Taskmgr.exe を[参照]ボタンで参照できるようにするには、アクティブ化する(つまり、Windows のタスクバーに表示されている)必要があります。
3. ユーザに対して、プロセスを強制終了(kill)できる権限を与えます。 [Read]許可を有効にすると、ユーザはプロセスを強制終了(kill)できるようになります。[Deny]チェック ボックスをオンにした場合、ユーザはプロセスを強制終了(kill)できません。

プログラム パターン

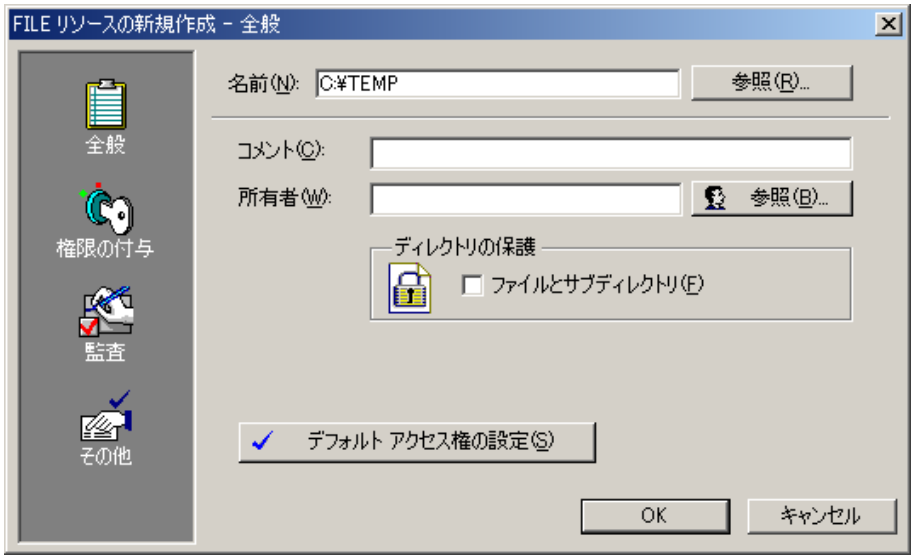
システム内の各ファイルのファイル リソースを定義するのは面倒な作業です。 eTrust AC には、この作業をスピード アップするツール群が用意されています。

ファイル グループを保護する簡単な方法の例を次に示します。 特定の名前ではなくパターンを指定することで、そのパターンに一致するすべてのファイルに同じアクセス制限を適用できます。

[リソース]ウィンドウで[Monitored Files]を選択し、[新規作成]をクリックします。



同様に、ディレクトリも保護できます。



ファイルおよびサブディレクトリの保護を設定するチェック ボックスに注意してください。このボックスをオンにした状態とオフにした状態で、それぞれファイル リソースを作成します。 リソース リストで 2 つのファイル リソースの違いを確認します。 コマンドの詳細をチェックし、発行されたコマンドの違いを確認します。

他のリソースの保護

eTrust AC では、他の種類のリソースも保護できます。 [リソース]ウィンドウでツリーを展開すると、eTrust AC でネットワークおよび Windows レジストリなどの重要なシステム コンポーネントの監視が可能であることを確認できます。

事前定義されたグループを使用したアクセス制限

eTrust AC では、以下の 4 つのグループが事前定義されています。これらのグループを使用してファイルへのアクセスを制限できます。

- _abspath
- _interactive
- _network
- _restricted

_restricted グループの使用

_restricted グループのメンバに追加されたユーザは、明示的にアクセスを許可されたファイルにのみアクセスできます。 これには、データベースで管理されていないファイルも含まれます。 これらのファイルは、FILE クラスのデフォルト アクセス値によって制御されます。 インストール時に、このデフォルト値は自動的に[None]に設定されます。

注: データベースに FILE アクセス ルールがほとんど含まれていない場合に、ユーザを _restricted グループのメンバに追加すると、_restricted ユーザは何も操作ができなくなります。 FILEクラスに対するデフォルトのアクセス権として[NONE]が指定された_restrictedグループにユーザを追加する場合は、WARNINGモードの使用を検討してください。 このモードを使用すると、監査イベントを使用して、_restrictedユーザがどのファイルにアクセスする必要があるかを調べることができます。 その後、適切な権限をユーザに割り当てて、WARNINGモードをオフにします。

ユーザをグループのメンバに追加する方法についてはすでに説明しました。 ユーザを _restricted グループのメンバに追加する方法も手順は同じです。

セキュリティを強化するには、FILE クラスの監査モードをリセットします。

1. [Resources]ウィンドウで、Administration フォルダを開いて[Access by Class]をクリックします。 FILE をダブルクリックします。

   注: [デフォルト アクセス権の設定]ボタンの上にカーソルを置くと、ツール ヒントに現在のデフォルトのアクセス権が表示されます。

2. [Auditing]パネルを開きます。 [失敗]をオフにし、[警告モード]をオンにします。

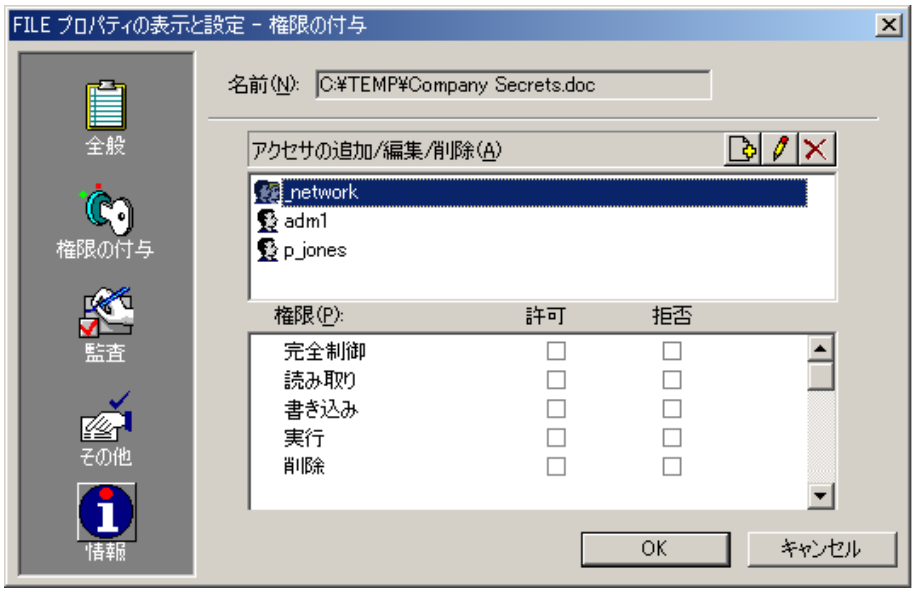
3. 次に、ユーザを_restricted グループに追加した結果をテストします。

注: eTrust AC の起動時にのみ、_restricted ユーザのリストが読込まれます。 _restricted グループにユーザを追加した場合、または _restricted グループからユーザを削除した場合、変更を有効にするには eTrust AC を再起動する必要があります。

_network グループと_interactive グループの使用

_network グループは、ネットワークから特定のリソースへのアクセスを定義します。 _interactive グループは、特定のリソースが存在するコンピュータから、そのリソースに対するアクセス許可を定義します。 この 2 つのグループは、ファイルのみでなく、すべてのリソースに適用されます。 また、すべてのユーザに対して適用されるため、ユーザを明示的にグループのメンバに追加する必要はありません。

例を示します。



ここでは、Company Secrets.doc ファイルの Access Control List（ACL）へのアクセス許可がない _network が追加されています。 これは、ネットワークからこのファイルにアクセスできないことを意味します。 _interactive の機能はローカル ホストでも同じです。 これら 2 つのグループには、ユーザをメンバとして追加しないでください。

注: eTrust AC では、_network グループと _interactive グループの間に関係はありません。 2 つのグループを同じリソースに適用しても問題はありません。

次の章について

この章では、ユーザとグループの作成や、ファイル、ディレクトリ、およびプログラムの保護について説明しました。 次の章では、管理者インターフェースについて説明します。

第 5 章: ユーザ アカウント管理の強化

このセクションには、以下のトピックが含まれます。

ユーザ アクセスと権限の制限

本章では、Administrator 権限の設定、端末からのアクセスの制限、時間帯と曜日のルールの設定、条件付きアクセスの設定など、eTrust AC をさらに活用するための方法について説明します。

Administrator 権限の使用の制限

コンピュータ ネットワークにおける重大なセキュリティ リスクの 1 つは、不正なユーザによって Administrators グループのユーザ アカウントの管理権限が奪われることです。Administrator アカウントへのアクセスを許可してしまうと、システムは重大な危険にさらされることになります。

eTrust AC を使用すると、管理者アカウントに与える権限を制限し、管理者グループに属するユーザの権限を制限することができます。 このように権限を制限した後で、Administrator の権限と許可を一般ユーザに配布すれば、Administrators グループに属さないユーザも管理タスクを実行できるようになります。 これを「タスクの委任」といい、eTrust AC の最も重要な機能の 1 つです。

ユーザ タイプ

eTrust AC では、Administrator 権限の一部を持つ多数のユーザ タイプを提供しています。 通常は、ユーザにこれらの属性を割り当てることが、管理者権限を配布する最初のステップになります。

eTrust AC では以下のユーザ タイプがサポートされています。

グループ管理者

特定の 1 つのグループ内でほとんどの管理機能を実行できるユーザ。

サブ管理者

管理者指定のクラスとリソースを管理できるユーザ。

パスワード管理者

他のユーザのパスワード設定を変更する権限を持つユーザ。

グループ パスワード管理者

ある特定のグループ内で、他のユーザのパスワード設定を変更する権限を持つユーザ。

監査者

監査ログの読み取り権限を持つユーザ。 ログインやリソースへのアクセスが試みられたときに実行する監査の種類を決定する権限もあります。

グループ監査担当者

特定の 1 つのグループに関する監査ログの読み取り権限を持つユーザ。 そのグループ内で実行される監査の種類を決定する権限もあります。

オペレータ

データベースのすべての情報を表示(読み取り)できるユーザ。

グループ オペレータ

データベースの、自分が定義されているグループに関するすべての情報を表示できるユーザ。

注: Windows 固有の Administrators グループと、Windows 固有ではない「グループ管理者」を混同しないように注意してください。

これらの特別なユーザ タイプは、Windows のネイティブ環境と eTrust 環境の両方で定義できます。 ただし、各ユーザ タイプに設定できる特別な許可は eTrust の一部であって、Windows の一部ではありません。

ユーザ属性は、新規ユーザの作成時に割り当てるか、既存のユーザ レコードを変更して割り当てることができます。 ポリシー マネージャは、eTrust データベースでの属性の割り当てをサポートしています。

既存のユーザにユーザ属性を割り当てるには、[Users]アイコンをクリックします。 表示されたリストでユーザ名を選択して、[ユーザ属性]をクリックします。

グループ内でのみ適用されるユーザ属性を割り当てるには[グループ]アイコンをクリックします。 [Member of]の下に表示されたグループ名をクリックし、[Group Attributes]をクリックします。

この属性により、ユーザ j_doe に、Administrators というグループが所有するアクセサおよびリソースを監査する権限が与えられます。

注: アクセサまたはリソースの所有者としてグループを指定すると、そのグループの管理者、監査者、および他のメンバが、そのアクセサやグループに対してそれぞれ該当する管理権限を持つことになります。

端末からのアクセスの制限

eTrust AC では、いくつかの方法でユーザ アクセスを制限できます。 これらの方法には、アカウントに有効期限を設定する、猶予ログインを設定する、ログインを特定の日時に限定する、およびユーザがログインする端末を制御するなどの方法があります。このセクションでは端末制限について説明し、次のセクションでは時間制限について説明します。

ウィザードを使用して新規ユーザを作成したときに、Login Setup Wizard を使用してユーザの端末を定義しました。 ユーザと端末を一致させないことで、そのユーザが保護されたリソースにログインしたり、アクセスするのを防止することができました。 ここでは端末リソースについてさらに詳しく説明します。

まず、ネイティブ環境に 1 組のユーザを定義する必要があります。 まだ定義していない場合は、ここで定義してください。 時間を節約するために、以下の手順にしたがって、既存の eTrust ユーザをネイティブ環境に追加します。

1. ユーザを 1 人選択し、ツールバーの[Properties]アイコンをクリックします。次に、[Advanced]ボタンをクリックしてネイティブ環境を追加します。

   注: ユーザを右クリックして、ショートカット メニューから[プロパティ]を選択することもできます。

2. 以下の手順に従って、ユーザに端末許可を割り当てます。

   a. プログラム バーの[Resources]アイコンをクリックし、[Login Protection]の横にあるプラス記号(+)をクリックしてツリーを展開します。

   b. [Terminal]を選択し、ローカル ホストをダブルクリックします。

   c. [Authorize]パネルを開いて、[Add Accessors]の[Insert]アイコンをクリックします。

   d. [Browse]ボタンをクリックしてユーザを追加し、[OK]をクリックします。

   e. 読み取り/書き込み許可の[Deny]チェック ボックスをオンにします。

   これでユーザ j_doe は、workstation1 という端末を使用できなくなりました。

3. もう 1 人のユーザにも同じ権限を与えます。ただし、このユーザには読み取り許可を割り当てます。

   注: ユーザが端末を管理できるようにするには、読み取りと書き込み許可を割り当てます。

4. いったんコンピュータからログオフし、各ユーザとしてログインします。 ユーザ j_doe がログインすると、ログイン エラー メッセージが表示されますが、ユーザ b_raines は、端末にアクセスできます。

重要: この演習を終了するときにコンピュータから端末リソースを削除**しないでください**。(リモート コンピュータの端末リソースは削除してもかまいません)。 自分のコンピュータの読み取り/書き込み権限は削除または変更**しないでください**。 権限を削除または変更すると、eTrust AC の管理ができなくなります。 削除した権限を取り戻すには、ソフトウェアを再インストールする必要があります。

端末グループ

複数のコンピュータに同じ制限を割り当てるには、対象となるコンピュータを端末グループにまとめて、一度に権限を与えます。

1. [リソース]ウィンドウで[端末グループ]を選択し、ツールバーの[新規作成]アイコンをクリックします。
2. グループに名前を付けて、所有者を指定します。
3. [Membership]パネルを開きます。 [Add/Delete Members]の[New]アイコンをクリックして端末を選択します。

   注: 複数の端末を選択する場合は、Ctrl キーまたは Shift キーを押しながら選択します。
4. 前に説明した手順に従って、権限設定と監査を実行します。
5. コマンドの詳細をチェックし、生成された selang のコマンドを確認します。

IMPERSONATION 要求の制限

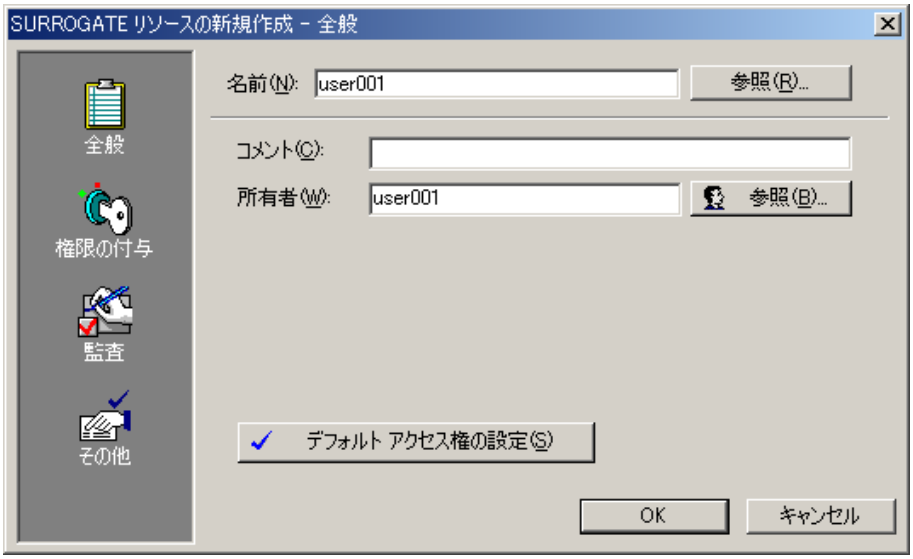
「別のユーザとしての実行要求」は、ユーザが自分のユーザ名を別のユーザ名に切り替えようとする場合に生成されます。 別のユーザとしての実行要求は、RunAs コマンドによって直接生成される場合や、適切な Win32 API を使用するプログラムによって生成される場合があります。

eTrust AC では、別のユーザとしての実行要求に制限を適用することにより、管理者とその他のユーザを保護します。 次の手順に従ってください。

1. パスワードがわかっているユーザ名を選択します。 以下のコマンドの user001 は、選択したユーザ名を示します。

   [リソース]ウィンドウで、[ユーザ識別コントロール]-[ユーザ ID の置換]を選択し、ツールバーの[新規作成]をクリックします。

2. ポリシー マネージャで以下のルールを定義します。



このルールは、明示的な許可がないかぎり、ユーザ usr001 としての実行要求を退け、他のユーザが usr001 として実行できないように eTrust AC に指示します。

代理ルールをテストするには、以下の手順に従います。

- Windows のシェルで、以下のコマンドを入力します。

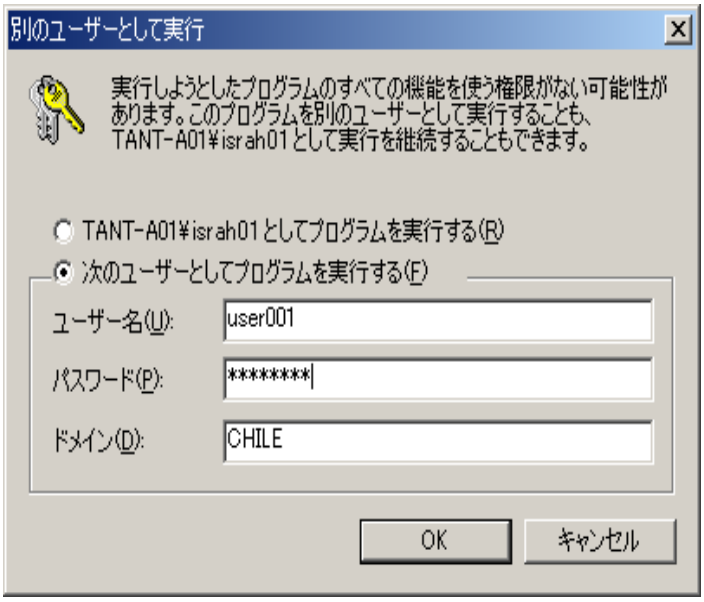
  ```
  cmd> RunAs /profile /USER:CHILE\user001 cmd.exe
  ```

  – 次のユーザのパスワードを入力してください。 CHILE¥user001

    システムは、以下のメッセージを返します。

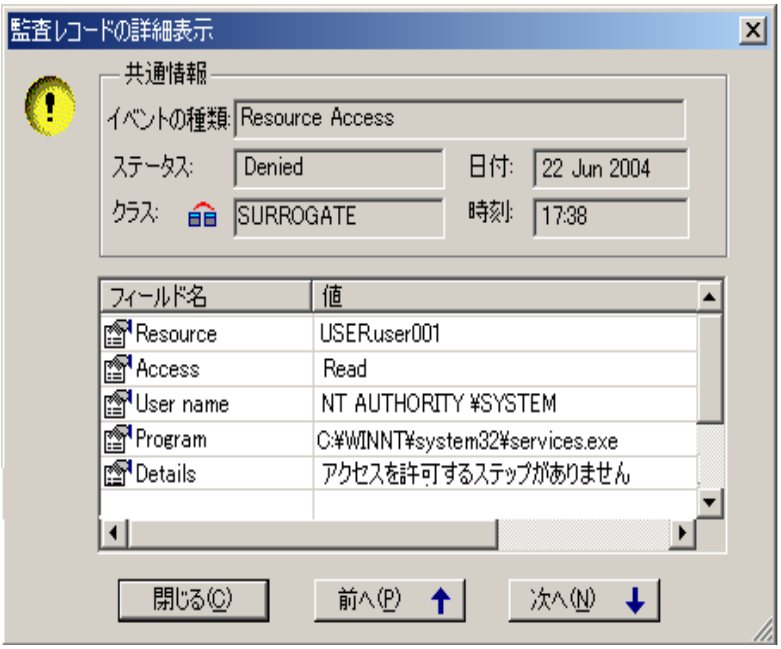
    ```
    開始するプログラム: "cmd.exe" ユーザー: "CHILE\user001"...
    RUNAS エラー： 実行できません - cmd.exe
    5: アクセスが拒否されました。
    ```

- Windows の［別のユーザとして実行］ダイアログ ボックスで、次のように入力します。

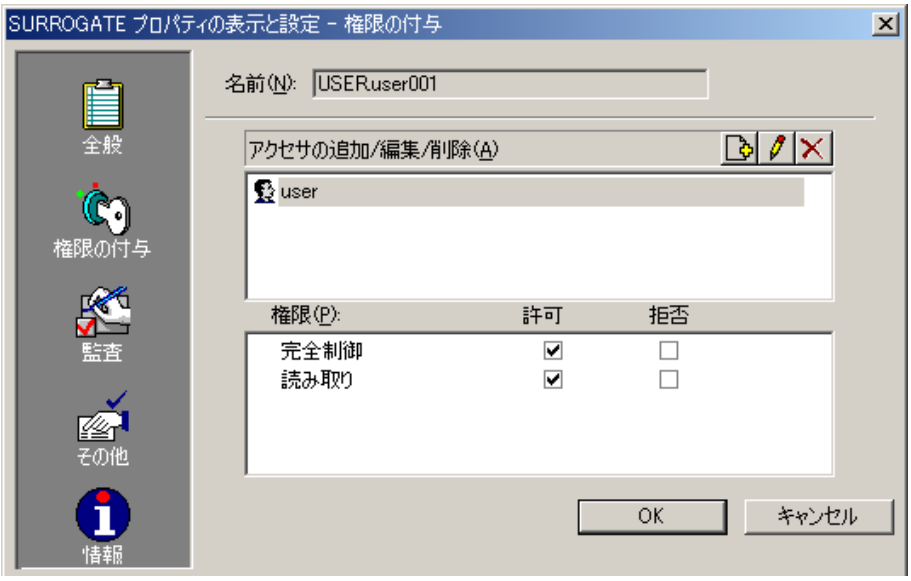


システムは、以下のメッセージを返します。

このユーザにアクセス権を与えるルールがなかったために、別のユーザとしての実行イベントが拒否されたことを監査のウィンドウで確認できます。



eTrust AC で user001 としての実行を許可するように指示するには、eTrust ポリシーマネージャのウィンドウで以下のルールを指定します。 自分が user001 として実行できる唯一のユーザとなる場合は、自分のユーザ名を指定します。eTrust AC で定義されているすべてのユーザが user001 として実行できるように許可する場合は、user 部分にアスタリスク(*)を指定します。



注: authorize コマンドを使用して、このような別のユーザとしての実行要求が明示的に許可されないかぎり、スーパーユーザでも user001 として実行することはできません。

時間帯と曜日のルールの設定

システムにとって最も危険な時間帯は、監査者やその他のスタッフがいなくなる深夜や週末です。 eTrust AC では、ユーザのログインを特定の時間帯や曜日に制限して、セキュリティ レベルを大幅に高めることができます。

まず、ユーザに時間制限を追加します。

1. ユーザを選択し、[User Properties]ウィンドウを表示します。 [Miscellaneous]パネルの[Day/Time Restrictions]ボタンをクリックして、時間制限を設定します。

   デフォルトでは、週7日間、1日24時間です。 任意の曜日の選択を解除できます。時間は選択したすべての曜日に適用されます。つまり、各曜日に異なる時間帯を設定することはできません。

   Unicenter TNG カレンダを選択して、カレンダ機能を使用することもできます。
2. 制限の設定を完了したら、[OK]をクリックします。
3. 許可された時間帯と許可されていない時間帯にユーザとしてログインを試みて、結果を確認します。

アカウントのロックアウト

前の例では、Peter Jones に標準の 9 時から 5 時に加えて、前後にログイン アクセス可能時間を追加しました。 この時間制限はログインのみに適用されます。 決められた時間内にログインすれば、後は何時間でもネットワークに接続していることができます。 Peter が午後 6 時にネットワークに接続できないようにするには、以下のように設定する必要があります。

[Policies]メニューの[Account]を選択します。 [Account Lockout]タブの下に、強制ログオフのチェック ボックスが表示されます。

休日情報の設定

システムへのユーザ アクセスの時間帯を制限するもう1つの方法は、休日を定義することです。 休日を設定すると、特別な許可が与えられたユーザを除く全ユーザに対してシステムへのアクセスを制限できます。

注: 自分がシステムからロックアウトされないようにするには、この演習を始める前に、自分のユーザ属性の[休日を無視する]をオンに変更してください。 これですべての休日にログインする許可が与えられます。 次の図を確認してください。

休日を設定するには、以下の手順に従います。

1. 再度［Resource］ウィンドウを開きます。
2. ［Login Protection］の［Holiday］を選択します。
3. ツールバーの［New］アイコンをクリックして、新しい Holiday リソースを作成します。

   ［Holiday］アイコンを選択すると日付を追加できます。 1 つの Holiday リソースに複数の休日を設定できます。または、複数の Holiday リソースに分けて休日を定義すると、より許可を制限できます。
4. 開始日と終了日を入力するか、日付フィールドの矢印をクリックし、表示されたカレンダから日付を選択します。 デフォルトでは、休日は毎年および終日に設定されますが、適切なチェック ボックスをオフにすると設定を変更できます。
5. 次に、許可を割り当てます。 読み取り許可を与えた各ユーザまたはグループは、指定した休日にもログインできます。
6. 今日の Holiday リソースを作成してみましょう。 一部のユーザに読み取り許可を与え、他のユーザには許可を与えないように（None）設定し、残りのユーザはすべてリストから除外します。
7. 設定が終了した後、各ユーザとしてログインします。

［Resources］

リソースにも時間制限を適用できます。 端末、ファイル、ネットワーク保護オブジェクト、コンテナ オブジェクト、レジストリ オブジェクトをはじめ、どのリソースについても、アクセスを特定の曜日や時間帯に制限できます。

ユーザの時間制限を設定する場合と手順は同じです。 リソースを選択し、［Properties］ウィンドウを開いて［Miscellaneous］パネルで制限を入力します。

次の章について

この章では、ユーザ アクセスと権限を制限し、ネットワークのセキュリティを強化する方法について説明しました。次の章では、ネットワークの保護や外部接続の制御などについて説明します。

第 6 章: ネットワーク アクティビティの保護

このセクションには、以下のトピックが含まれます。

ネットワーク レベル アクセスの制御

本章では、eTrust AC をさらに活用するための次のステップとして、ネットワークの TCP/IP 接続の保護について説明します。

ネットワークの保護(TCP/IP)

TCP/IP ネットワークの開放性は、最も魅力のある特徴であると同時に、セキュリティの面では大きな欠陥でもあります。 ネットワークの安全性を確保するため、eTrust AC にはファイアウォール機能が備えられています。このために、保護を目的とした特別な専用コンピュータは必要ありません。 eTrust AC を使用すると、特定のクライアントが特定の TCP/IP サービスを特定のホストへ送信することを許可したり、特定のホストのみが特定の TCP/IP サービスをローカル ホストへ送信することを許可したりできます。

受信接続の制御

eTrust AC でネットワークからの不正なアクセスに対してコンピュータを保護する方法を確認するには、以下の手順に従います。

1. HOST クラスがアクティブかどうかを確認します。
   a. [ツール]メニューから[eTrust AC クラスの有効化]を選択します。

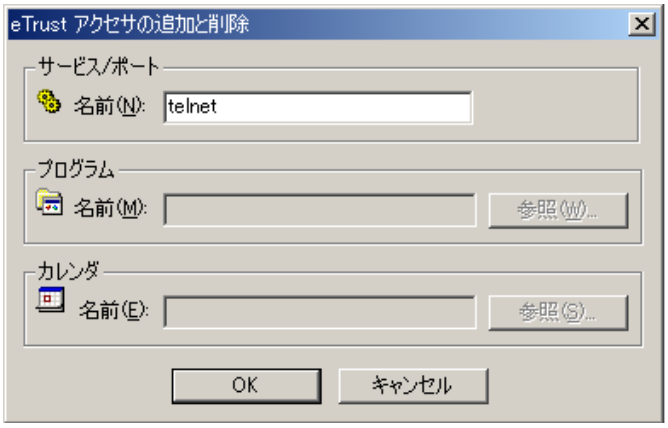
      [Activate eTrust Classes]ダイアログ ボックスが表示されます。

   b. [HOST]が表示されるまでスクロールします。[HOST]チェック ボックスがオフの場合は、このチェック ボックスをオンにして[OK]をクリックします。
2. eTrust AC を実行しているコンピュータに接続している別のコンピュータを選択し、ホストとして定義します。 次の例の workstation2 は、選択したコンピュータを示します。

3. workstation2 をホストとして定義します。

   [Access Control]プログラム バーから[Resources]アイコンをクリックし、[Network Protection]を展開して、[HOST]を選択します。 ツールバーの[New]アイコンをクリックします。 [Create New HOST Resource-General]ダイアログ ボックスが表示されます。

   左のアイコンを使用して、新しい HOST レコードの情報を入力します。 [Authorize]アイコンを使用して、サービス(TCP/IP など)またはポートを含む権限情報を入力します。



4. ローカル ホストに、Telnet を除くすべての TCP/IP サービスを workstation2 から受信する許可を与えます。 これを行うには、Telnet のパーミッションを拒否します。

5. workstation2 から Telnet 接続を試みます。この試みは拒否されます。

6. workstation2 から FTP 接続を試みます。FTP は Telnet TCP サービスとは異なるため、FTP 要求は許可されます。

注: ホスト グループ レベル、ネットワーク レベル、および名前パターン レベルで、TCP/IP アクセス ルールを指定することもできます。

ホスト グループ レベルでの保護

ホスト グループを定義するには、eTrust AC データベースに GHOST クラスのレコードを作成します。 このホスト グループは、単一のホストの場合と同じ方法で許可を受けます。

注: 個々のユーザの場合と同様に、ホスト別に定義されたルールは、グループに適用されるルールよりも優先されます。

リソースに対する TCP/IP のアクセス ルールを[Access Control]プログラム バーから設定するには、[Resources]アイコンをクリックし、[Network Protection]を展開して、[Host Groups]を選択します。 ツールバーの[New]アイコンをクリックします。

ネットワーク レベルでの保護

eTrust AC アクセス ルールは、ネットワーク レベルでも指定することができます。 ネットワークを定義するには、HOSTNET クラスのデータベース レコードを作成します。 このネットワークは、単一の HOST レコードの場合と同じ方法で許可を受けます。

注: ホスト グループ レベルのルールは、ネットワーク レベルのルールよりも優先されます。

リソースに対する TCP/IP のアクセス ルールを[Access Control]プログラム バーから設定するには、[Resources]アイコンをクリックし、[Network Protection]を展開して、[Host Network]を選択します。 ツールバーの[New]アイコンをクリックします。

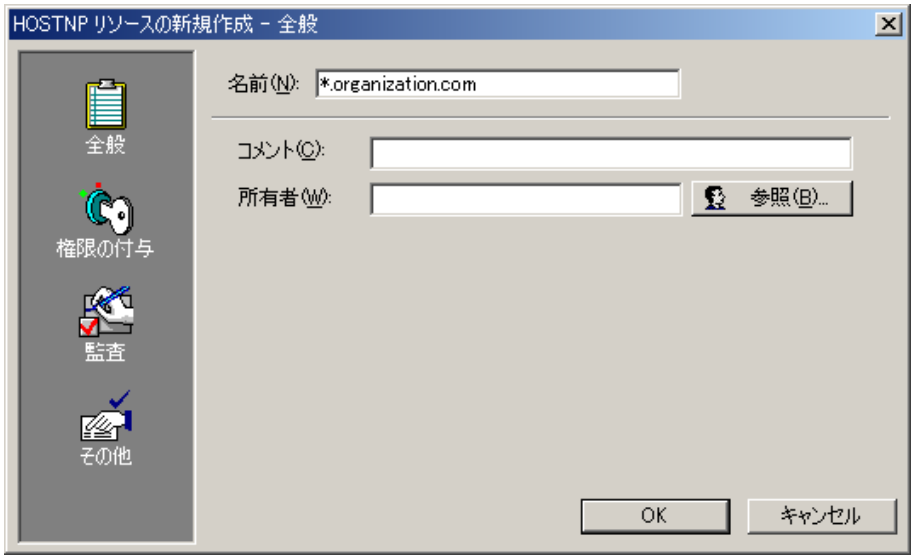
名前パターンを使用した保護

TCP/IP アクセス ルールを定義する別の方法は、HOSTNP（ホスト名パターン）クラスを使用して、名前パターン サービスを経由する方法です。 このネットワークは、単一の HOST レコードの場合と同じ方法で許可を受けます。

注: ネットワーク レベルのルールは、名前パターン レベルのルールよりも優先されます。

リソースに対する TCP/IP アクセス ルールを設定するには、[Access Control]プログラム バーの[Resources]アイコンをクリックし、[Network Protection]を展開して、[Host Protection by Name Pattern]を選択します。 ツールバーの[New]アイコンをクリックします。

[Create New HOST Resource]ダイアログ ボックスが表示されます。



外部への接続の制御

各コンピュータの送信接続は、別のタイプのリソースとして管理できます。

ネットワークから外部への接続を制限することで、ファイアウォールを通り抜ける不正侵入者からの被害を最小限に抑えることができます。 また、正当なインターネット アクセスに対しても、アクセス範囲をネットワーク内の特定のサービスとシステムに限定できます。 たとえば、電子メールおよびデータベース アクセスに必要な特定フォームのみを許可することができます。

eTrust AC で送信接続を制限する方法を確認するには、以下の手順に従います。

1. CONNECT クラスがアクティブかどうかを確認します。
   a. [ツール]メニューから[eTrust AC クラスの有効化]を選択します。

      [Activate eTrust Classes]ダイアログ ボックスが表示されます。

   b. [CONNECT]が表示されるまでスクロールします。[CONNECT]チェック ボックスがオフの場合は、このチェック ボックスをオンにして[OK]をクリックします。
2. eTrust AC を実行しているコンピュータに接続している別のコンピュータを選択し、接続リソースとして定義します。 次の例の workstation2 は、選択したコンピュータを示します。
3. workstation2 を接続リソースとして定義します。 これを行うには、[Access Control]プログラム バーで[Resources]アイコンをクリックし、[Common and Network Protection]フォルダを展開して、[Outgoing Connection by Host]を選択します。 次に、[新規作成]ボタンをクリックします。
4. 自分のマシンから workstation2 へ Telnet または FTP 接続を試みます。この試みは拒否されます。
5. 以下の手順に従って、ユーザ j_doe に接続許可を割り当てます。
   a. プログラム バーの[Resources]アイコンをクリックし、[Network Protection]の横にあるプラス記号(+)をクリックしてツリーを展開します。
   b. [Outgoing Connection by Host]を選択し、workstation2 をダブルクリックします。
   c. [Authorize]アイコンをクリックして[Authorize]ページを開き、[Add Accessors]の[Insert]アイコンをクリックします。
   d. [Browse]ボタンを使用してユーザ j_doe を追加し、[OK]をクリックします。
   e. [Read]許可の[Allow]チェック ボックスをオンにします。

   すべてのユーザに対して拒否ルールが設定されていますが、ユーザ j_doe は、workstation2 に Telnet 接続または FTP 接続することが許可されています。

サービス指向の TCP/IP ルール

eTrust AC では、この章でこれまでに説明したホスト指向のルールだけでなく、サービス指向の TCP/IP アクセス ルールも使用できます。

この種類のアクセス ルールを使用すると、特定の TCP サービス(ポート)を使用して、受信接続および送信接続を制御できます。 このようなルールを定義するには、TCP クラスを使用します。

eTrust AC でサービス指向の TCP/IP ルールを使用してコンピュータを保護する方法について確認するには、以下の手順に従います。

1. HOST クラスおよび CONNECT クラスを無効にします。
   a. [ツール]メニューから[eTrust AC クラスの有効化]を選択します。

      [Activate eTrust Classes]ダイアログ ボックスが表示されます。
   b. [HOST]が表示されるまでスクロールします。[HOST]チェック ボックスがオフになっていることを確認します。
   c. [CONNECT]が表示されるまでスクロールします。[CONNECT]チェック ボックスがオフになっていることを確認します。
   d. [OK]をクリックします。
2. Telnet を TCP サービスとして定義します。

   [リソース]ウィンドウで、[ネットワーク保護]-[TCP の保護]を選択し、ツールバーの[新規作成]をクリックします。

   ローカル ホストに、workstation2 からの Telnet 通信の受信を除く、すべてのコンピュータとの Telnet 通信に対する許可を与えます。これを行うには、[TCP リソースの新規作成 - 全般]ダイアログ ボックスで[デフォルト アクセス権の設定]ボタンをクリックし、[すべて]を選択します。[OK]をクリックします。
3. [Authorize]アイコンをクリックして、権限情報を入力します。[TCP リソースの新規作成 - 権限の付与]ダイアログ ボックスで、[挿入]アイコンをクリックします。[eTrust アクセサの追加と編集]ダイアログ ボックスで、[参照]ボタンをクリックし、[ホスト]を選択して workstation2 を選択します。

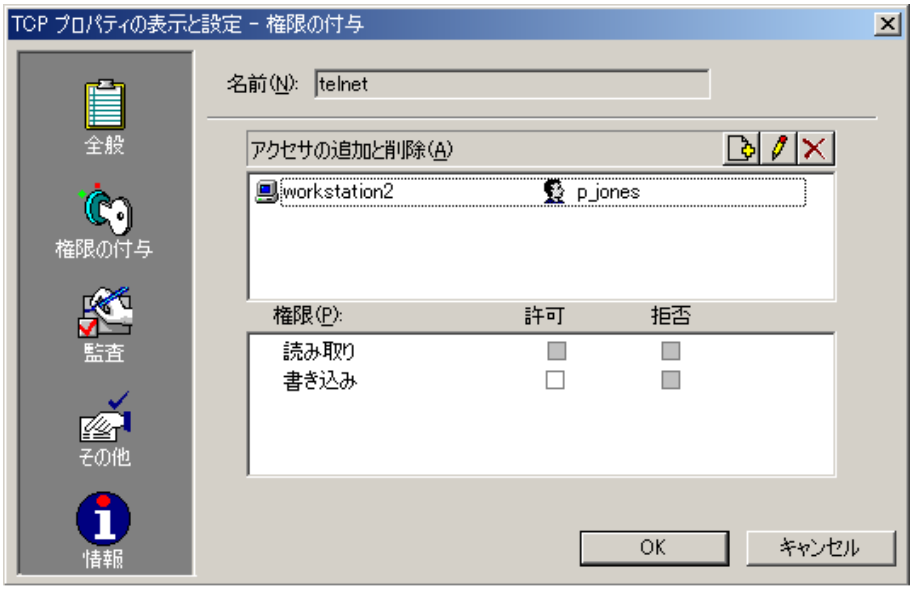
   workstation2 の[読み取り]許可チェック ボックスおよび[書き込み]許可チェック ボックスがオフになっていることを確認します。
4. workstation2 から Telnet 接続を試みます。この試みは拒否されます。
5. Telnet 通信を workstation2 に送信するユーザ p_jones を除くすべてのコンピュータに、ローカル ホストとの Telnet 通信に対する許可を与えます。

   注: Telnet リソースのデフォルトのアクセス権は、すでに[すべて]に設定されています。
   a. [View or Set TCP Resource]ダイアログ ボックスで、[Authorize]アイコンをクリックします。

b. [Insert]アイコンをクリックします。次に、[Add/Edit eTrust Accessor]ダイアログ ボックスで、[Browse]ボタンをクリックし、[Host]を選択して workstation2 を選択します。

c. [外部接続]チェック ボックスをオンにして、[名前]フィールドに「p_jones」と入力します。

d. [OK]をクリックします。 このダイアログ ボックスは次のように表示されます。



6. ユーザ p_jones としてログインし、workstation2 への Telnet 接続を試みます。この試みは拒否されます。

次の章について

この章では、ネットワークの保護について説明しました。次の章では、パスワード ポリシーの設定について説明します。

第 7 章: パスワード ポリシーおよび監査ポリシーの設定

このセクションには、以下のトピックが含まれます。

パスワード、ログイン、および監査のルール

この章では、パスワード ポリシーの定義、パスワードの変更、ポリシー チェックの有効化、ポリシーの監査などについて説明します。 ポリシー マネージャを使用すると、デフォルトのセキュリティ ポリシーを簡単に設定できます。

セキュリティ ポリシーは、パスワード ルール、ログイン ルール、および監査ルールで構成されます。 ユーザに対して 1 つの全般的なポリシーを設定し、グループに対して複数の異なるポリシーをグループ単位で設定できます。 グローバルな設定もあれば、個々のユーザ設定によって変更できる設定(たとえば、有効期限および猶予の最小値と最大値)もあります。

パスワード ポリシーの設定

パスワード ポリシーを定義するには、まずパスワード ポリシー チェックが有効になっていることを確認します（新規インストールではデフォルトで有効になります）。

1. [ツール]メニューから[eTrust AC クラスの有効化]を選択します。

   [Activate eTrust Classes]ダイアログ ボックスが表示されます。

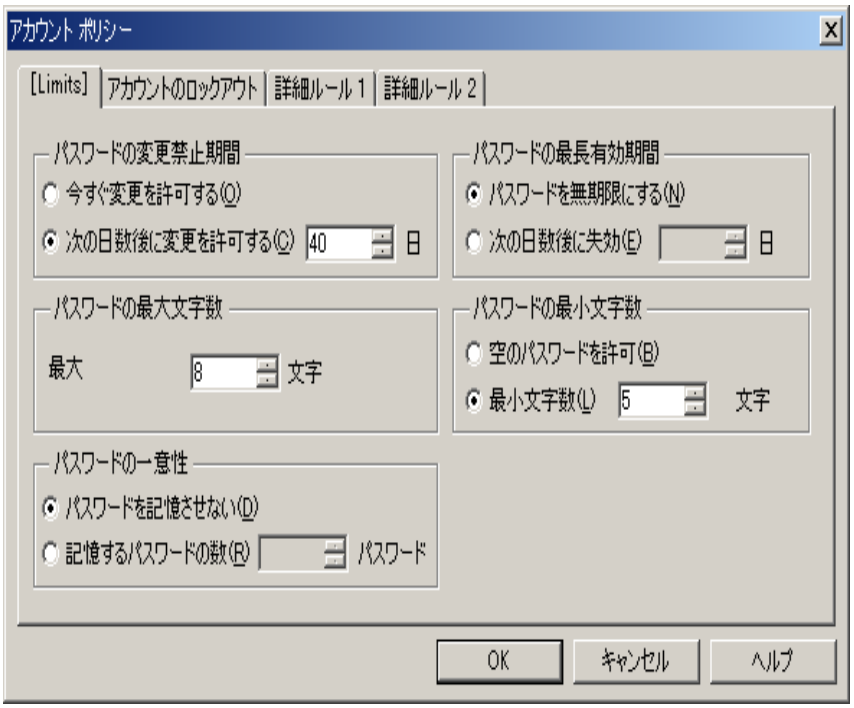
2. [PASSWORD]が表示されるまでスクロールします。[PASSWORD]チェック ボックスがオフの場合は、このチェック ボックスをオンにして[OK]をクリックします。

   この変更またはその他の変更を行う前に、デフォルトのパスワード ルールを確認します。 このセクションの練習を終了するときにデフォルト設定に戻せるように、デフォルト設定をメモしておきます。

3. eTrust AC の現在の設定値を確認した後、サイトのニーズに合わせて値を変更できます。 詳細については、「管理者ガイド」を参照してください。

4. 一般的なユーザ アカウント ポリシーを設定するには、[User]ウィンドウをアクティブにします。 プログラム バーの[User]アイコンをクリックします。 メニュー バーの[Policies]を選択します。 このメニューからアカウント ポリシーを設定できます。

   [アカウント ポリシー]ウィンドウには3つのタブがあります。 最初のタブでは、ネイティブ オペレーティング システムおよびeTrust ACデータベースの両方に適用するルールを設定します。 残りの2つの[詳細ルール]タブでは、eTrustのポリシーのみを設定します。



5. いくつかのパラメータを変更します。 設定の結果は、システム上の制限をテストすることで確認できます。

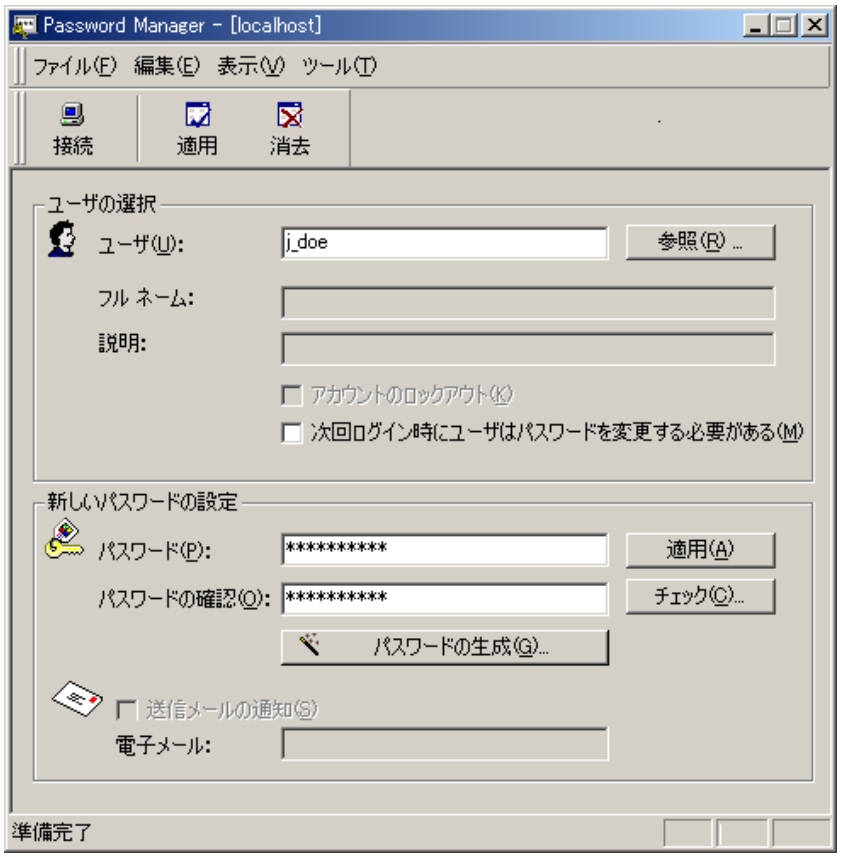
   詳細ルールでは、eTrust のパスワード ポリシーを設定します。 [ログオンを許可する回数]フィールドは、猶予ログインのパラメータです。

   注: 猶予ログインの詳細については、「管理者ガイド」を参照してください。

パスワードの変更

パスワードを変更する場合、ポリシー マネージャは必要ありません。 データベースでパスワード マネージャとして指定されているユーザは、使用するワークステーションに Password Utility (SetPwd.exe) のみをインストールして、タスクバーの[スタート]ボタンからアクセスできます。

[スタート]-[プログラム]-[CA]-[eTrust Access Control]-[パスワード マネージャ]を選択します。 Password Manager ユーティリティを使用すると、ネイティブ環境で定義されているすべてのユーザのパスワードを変更できます。



ネイティブ環境での監査ポリシーの設定

［Policies］メニューから［Audit］を選択し、監査ポリシーを設定します。

いくつかのパラメータを変更してみてください。 コマンド ラインの詳細を見て結果を確認します。

変更の結果を確認するには、Windows のイベント ビューアを開きます。

最後に

パスワードおよび監査ポリシーを元のデフォルト設定に戻します。

次の章について

この章では、eTrust AC のパスワードおよび監査ポリシーについて説明しました。次の章では、複数のホストの管理について説明します。 また、Policy Model データベースの作成、ワークステーションからの PMDB の参照、Policy Model の使用などについても説明します。

第 8 章: 集中管理

このセクションには、以下のトピックが含まれます。

ユーザ、セキュリティ ポリシーなどの作成

この章では、Policy Model データベース(PMDB)の作成と、ユーザ、許可、およびパスワードの登録について説明します。トランザクション マネージャは、ローカル ホストで実行される eTrust AC のトランザクションを自動的に複数のホストに送信します。

PMDB の作成

次の例では、policy1 という名前の PMDB を作成し、workstat1 および workstat2 という PMDB をサブスクライバとして登録します。 分かりやすくするために、この例では同じホストにサブスクライバを作成します。

PMDB を管理する権限を持つ adm1 および adm2 という 2 人のユーザを登録するには、以下の手順に従います。

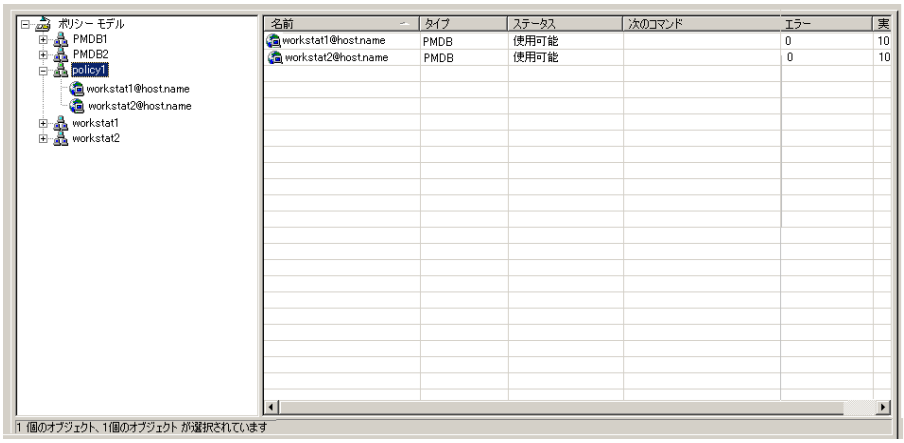
1. bighost に接続します。 管理者のユーザ アカウントを作成します。
   - PMDB の管理者は、PMDB のプロパティを変更する権限があるユーザです。
   - PMDB の監査者は、PMDB の監査ログ ファイルを参照する権限があるユーザです。
   - PMDB のパスワード管理者は、PMDB のパスワードを変更する権限があるユーザです。
2. 3 つすべての属性を使用して、ユーザを作成します。
3. 管理者に端末へのアクセス権限を与えて、ワークステーションから管理します。
4. 次に、いったんログオフした後に、いずれかの管理者でログインします。
5. プログラム バーの[Tools]をクリックして、[Policy Model]を選択します。
6. ツール バーの[新規作成]アイコンをクリックして、新しい PMDB を作成します。PMDB の名前を入力し、[管理者]アイコンをクリックします。
7. [New]を選択し、名前を入力するか、[Browse]ボタンをクリックして名前を選択します。 もう 1 人の管理者についても同じ手順を繰り返します。
8. [Terminal]を選択します。 [New]をクリックし、ホストの名前を入力するか、[Browse]ボタンをクリックしてホストを選択します。

9. PMDB が作成できました。次はサブスクライバを追加します。 既存の PMDB または eTrust AC データベースをサブスクライバとして指定できます。 この例では、サブスクライバ PMDB がすでに bighost 上に作成されていますが、サブスクライバ PMDB はネットワーク内のどこに作成してもかまいません。

   PMDB policy1 を右クリックします。

10. [Add Subscriber]を選択します。 subscriber@host という書式で名前を入力します。

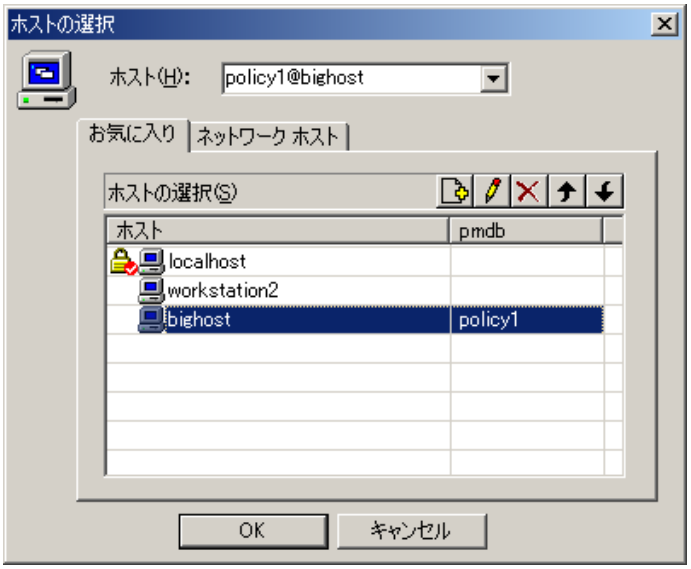
11. もう 1 つのサブスクライバについても同じ手順を繰り返します。 ツリーに Policy Model 階層が表示されます。



PMDB の使用

次に、新しいユーザを作成して、変更がモデル全体にどのように伝達されるかを見てみましょう。

1. まず、Policy Model に接続します。



2. ユーザ jsmith（Jennifer Smith）を作成します。
3. いずれかのサブスクライバに接続します

   注: ホストが[Favorites]リストに表示されない場合は、接続ダイアログ ボックスの最上部に名前を入力してください。
4. [Users]ウィンドウを開きます。

   新しいユーザ jsmith がリストに表示されます。

トランザクション マネージャ - もう 1 つの簡単な方法

トランザクション マネージャは、ローカル ホストで実行される eTrust AC のトランザクションを自動的に複数のホストに送信します。 このトランザクション モードは、Policy Model に代わるスピーディで効率的な方法です。 すべてのサブスクライバのセキュリティ データベースに対する情報の伝達を保証するものではありませんが、この トランザクション モードは、Policy Model より使いやすく、Policy Model 階層の一部として定義されていない複数のデータベースに対して変更を行う場合には特に有効です。

トランザクション マネージャのセットアップ

トランザクション マネージャを使用する前に、以下のことを確認します。

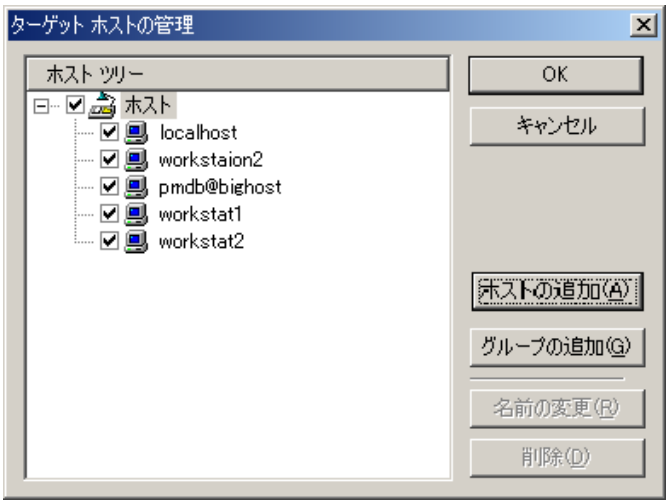
- ローカル ホストおよびアクセス先の各リモート ホストに対する ADMIN 権限があること。
- アクセス先の各ホスト上に、管理元のコンピュータの TERMINAL レコードが作成されていること。

これらの要件は、リモート ホストを管理する場合も同じです。トランザクション マネージャは、有効にしてから使用する必要があります。

1. ポリシー マネージャから[ツール]-[オプション]を選択し、[トランザクション マネージャ]タブをクリックします。
2. リストの上部にある[マルチホスト トランザクションを有効にする]チェック ボックスをオンにします。

   また、有効にするその他のトランザクション マネージャ オプションを選択することもできます。
3. [ファイル]-[ターゲット ホスト]を選択して、ターゲット ホスト ファイルを作成します。
4. ターゲット ホスト リストにホスト、workstat1 と workstat2 を追加します。

   コマンドを伝達するホストを選択します。



ホストにはローカル データベースまたは PMDB を指定できます。 ホストのグループを作成して、選択を効率化することもできます。 グループ名をクリックすると、そのグループのすべてのメンバが選択されます。 また、ホストを個別に選択または選択解除することも可能です。 [OK]をクリックすると、選択はただちに有効になり、次に変更するまでその選択が有効になります。 別のホスト グループにトランザクションを送信する場合は、毎回ターゲット ホスト ファイルを手動でリセットする必要があります。

注: [トランザクション モード]を有効にすると、[Host Selection]の設定は、トランザクション マネージャの他に、Copy User Wizard および Copy Group Wizard にも適用されます。

5. 手順を実行する前に、再び bighost に接続します。 ツールバーの[トランザクション モード]アイコンをクリックします。

   実行するトランザクションはすべて、選択したホストにも伝達されます。 もう一度[トランザクション モード]アイコンをクリックすると、コマンドは伝達されません。

ここで、さきほど作成したユーザを削除します。

1. ユーザ jsmith を選択して、ツールバーの[Delete]をクリックします。

   結果を確認するには、Windows のタスクバー トレイにある[トランザクション マネージャ]アイコンを右クリックし、[Open Transaction Manager]を選択します。 以下のダイアログ ボックスには、workstat1 の結果が表示されています。

2. workstat2 を選択して、そのホストでの結果を表示します。

   この例では、ログが赤で表示されています。これは、コマンドが伝達できなかったことを示しています。

3. ログ項目をダブルクリックしてコマンド詳細を表示し、詳細を確認してください。

注: 問題の修正後、トランザクションを選択し、[Run Again]アイコンをクリックして、伝達を実行できます（[Run Again]アイコンは、2 つの歯車のアイコンです）。

次の章について

この章では、Policy Model、PMDB、および トランザクション マネージャ について説明しました。 次の章では、eTrust AC と Unicenter TNG との統合について説明します。

第 9 章: Unicenter との統合

このセクションには、以下のトピックが含まれます。

Unicenter と eTrust AC の統合

eTrust AC は、Unicenter TNG のエンタープライズ マネジメント環境と完全に統合されています。 本章では、eTrust AC で統合がどのように行われるかについて説明します。

注: 統合するためには、Unicenter TNG と eTrust AC が同じマシンにインストールされている必要があります。また、以下のコマンドを使用して Unicenter TNG Security を有効にしておく必要があります。

```
SETOPT CA_ROUTER_CAUSECU 1
SETLOCAL CAIACTSECSV YES
```

Unicenter Integration ツールのインストール

以下の手順に従って、Windows環境でUnicenter Integrationをセットアップします。eTrust AC のインストール中に、各ノードに対して以下の手順を行います。

1. Installation Wizard の［Select Components］ダイアログ ボックスで［Unicenter Integration］を選択して、［Next］をクリックします。
2. eTrust AC により、Unicenter TNG の環境設定パラメータで指定されたホストまたは選択されたホストに監査データが送信されます。 統合するには、監査データを Unicenter TNG に送信するように指定し、eTrust AC が監査データを送信するホストを選択します。
3. ユーザとアクセス権を Unicenter TNG カレンダと統合する場合は、Unicenter Calendar ホスト サーバからアップデートを取得する頻度を指定して、［Next］をクリックします（デフォルトでは 10 分ごとです）。
4. Unicenter セキュリティ データを移行する場合、インストール ウィザードの［Unicenter の移行］ダイアログ ボックスで［Unicenter セキュリティ データの eTrust Access Control への移行］を選択して、［次へ］をクリックします。

   注: Unicenter セキュリティ データを移行しない場合は、［Unicenter セキュリティ データの eTrust Access Control への移行］を選択**しないでください**。

   このオプションを選択しない場合、Unicenter セキュリティは eTrust AC へ移行されません。また、eTrust AC でのユーザ名は完全修飾（DOMAINNAME¥USERNAME のように）されて表示されます。 移行では、ユーザ名は修飾されません（USERNAME のように表示されます）。
5. 残りのインストール プロセスを続行します。
6. ［Database Import］ダイアログ ボックスが表示された場合は、［Yes］または［No］を選択して、データベースに Windows のデータをインポートするかどうかを指定します。

   注: ［Unicenter セキュリティ データの eTrust Access Control への移行］オプションを**選択しなかった**場合、［データベースのインポート］ダイアログ ボックスは表示されません。

インストール上の注意事項

- Unicenter Integration および Migration Installation プロセスの実行後に、Unicenter TNG のログイン インターセプトを実行しないことをお勧めします。Unicenter Integration および Migration Installation プロセスが正常に実行された後で、Unicenter TNG のログイン インターセプトが無効になっていることを確認する必要があります。
- Unicenter のデータ スコーピング ルール（-DT サフィックスの付いた Unicenter TNG のアセット タイプを対象とするルール）は、eTrust AC の移行プロセスではサポートされていません。 移行プロセスでは、このタイプのルールは無視されます。
- Unicenter セキュリティは現在使用されていないため、Unicenter セキュリティのアセット タイプ（CA-USER、CA-ACCESS、CA-USERGROUP、CA-ASSETGROUP、CA-ASSETTYPE、および CA-UPSNODE）に対して実装された Unicenter セキュリティ ルールはどれも使用されていません。 このようなアセット タイプまたはそれらから派生したタイプを対象とするルールは、移行プロセスではすべて無視されます。
- Unicenter Integration プロセスの実行後に Unicenter TNG をアップグレードする場合、または Unicenter TNG の修正プログラムを適用する場合は、%CAIGLBL000%\BIN ディレクトリの CAUSECR.DLL ファイルが置き換えられていないことと、CAUSECR.DLL ファイルが eTrustACDir\bin ディレクトリの CAUSECR.DLL.EAC ファイルと同じであることを確認する必要があります。
- eTrust AC がアンインストールされた場合、Unicenter セキュリティ オプションの CA_ROUTER_CAUSECU が 1 にリセットされます。また、Unicenter セキュリティ オプションの SETLOCAL CAIACTSECSV が yes にリセットされ、%CAIGLBL000%\BIN ディレクトリの CAUSECR.DLL ファイルが Unicenter のデフォルトのものに置き換えられます。 アンインストール プロセス後にこれらのオプションをカスタマイズする必要がある場合があります。

注: Unicenter Integration の機能とその動作の一覧については、「管理者ガイド」を参照してください。

次の章について

次の章では、eTrust AC に関するよくある質問とその答えを紹介します。有用な情報が一覧になっていて、eTrust AC についての理解をさらに深めることができます。

第 10 章: よくある質問

この章では、一般的なセキュリティ ポリシーに関する質問と回答を示し、eTrust AC によって UNIX、Linux、および Windows のセキュリティの管理と適用がどのように簡略化されるかについて説明します。 ユーザ、グループ、システム リソースと同様に、セキュリティ ポリシーも GUI を使用して集中管理できます。

Q: eTrust AC とは何ですか。

A: eTrust AC とは、UNIX、Linux、および Windows のサーバを保護し、システム管理者がアクセスを管理できるようにするソフトウェア パッケージです。

これまでは、脅威に対処したり、脆弱性を評価したり、root ユーザになる方法に制限を加えたりすることに焦点を当てて、UNIX および Linux システムを保護してきました。 対応策としては、頻繁な監査レポートの実行、システムの脆弱性を明らかにするためのシェアウェア ツールの使用、ベンダーから提供された CERT 推奨パッチのインストールなどが行われてきました。

UNIX または Linux のセキュリティを強化するには、システム リソースへアクセス許可を与える方法を根本的に変更する必要があるという事実を認識した上で、eTrust AC は設計されました。 eTrust AC では、シンプルで容易に構成できるアクセス ルールに基づいて、異なる OS リソースへのアクセスを制御することができます。 これにより、保護対象データに直結したセキュリティ レイヤが追加されます。 このソリューションによって、UNIX または Linux の動作や管理者の作業内容が変更されることはありません。

Q: eTrust AC の機能は、サポート対象の各プラットフォームで同じですか。

A: はい。 eTrust AC の機能はサポート対象のすべてのプラットフォーム上で同じです。 eTrust AC のすべてのインターフェースで、基礎になる OS の違いを意識させないクロスプラットフォーム管理が可能です（初期設定時を除く）。 その結果、OS ごとにリソースの名前が異なる場合でも、eTrust AC ではネイティブ OS との整合性が維持されます。

Q: eTrust AC Dynamic Security Extension（DSX）テクノロジとは何ですか。

A: DSX技術は、セキュリティに関連したシステム コールを動的にインターセプトする技術です。 システム コール（またはシステム ベクター）テーブルには、システム コール カーネル コードのメモリ アドレス ポインタが保存されます。 それらのアドレス ポインタは、eTrust AC によって保存された後、対応する eTrust AC コードを参照するように変更されます。

アクセスが承認されると、要求は元の syscall コードで続行され、アクセスが拒否されると、要求は終了します。

Q: eTrust AC は、システムのすべてのイベントをインターセプトしますか。

A: いいえ。eTrust AC によってインターセプトされるのは、特定の syscall のみです。syscall がインターセプトされると、eTrust AC エンジンは、eTrust AC データベースで定義された eTrust AC ルールに基づいて、インターセプトされたリソースへのアクセスの許可または拒否の決定を行います。

eTrust AC は、ファイルまたはデバイスへの最初のアクセスをインターセプトしますが、その後ファイルに対して実行される I/O イベント(読み取りおよび書き込み)はインターセプトしません。

これは、ネットワーク接続でも同様です。 eTrust AC は、ネットワーク ソケットの確立(ポートと IP アドレスの組み合せなど)をインターセプトしますが、その後のデータ転送はインターセプトしません。

eTrust AC は、プロセスにメモリを割り当てるルーチンもインターセプトしません。

Q: eTrust AC 実行中に発生する CPU のオーバーヘッドはどのくらいですか。

A: これは、ホストの機能により異なります。 メール サーバでは、通常、データベース サーバのホスト システムよりもパフォーマンスへの影響は少なくなります。

弊社のユーザ事例では、高いパフォーマンスが要求されるシステムでも、CPU のオーバーヘッドは標準パフォーマンスの範囲に対して 1 ～ 5% の増加であることが示されています。

Q: アクセス ルールはどこに保存されますか?

A: eTrust AC のアクセス ルールはローカル ホスト上の保護された eTrust AC データベースに保存されます。

Q: eTrust AC には API が用意されていますか。

A: はい。 eTrust AC には多数の API が用意されており、それらの API は eTrust AC のオープン アーキテクチャを構成しています。 API は、アクセス制御から警告通知までのあらゆる処理に使用できます。 各 API の詳しい使用法は eTrust AC のマニュアルで説明されています。また、C 言語で書かれたサンプル プログラムがソフトウェアに付属しています。 eTrust AC の API を以下に示します。

- **Authorization API**： 任意のリソースへのユーザ アクセスをチェックするためにアプリケーションで使用します。 この API コールを使用すると、独自に作成したアプリケーションからでも、eTrust AC でサイトのセキュリティを集中管理できます。
- **Administration API**： eTrust AC によって処理される Windows、UNIX、または Linux セキュリティのさまざまな側面をアプリケーションで管理する場合に使用します。
- **Auditing API**： eTrust AC の監査機能をカスタマイズできます。
- **Password API**： パスワード品質チェックをカスタマイズし、製品で提供されているパスワード品質チェックに追加できます。

Q: eTrust AC には、ネットワーク プロセス通信のための暗号が用意されていますか。

A: はい。eTrust AC に関連するすべてのネットワーク通信が暗号化されます。

Q: eTrust AC の保護対象は何ですか。

A: eTrust AC は、保護されたホスト上にあるオペレーティング システムおよびアプリケーション リソースを保護します。 これは、システム リソースへのアクセスを制御することによって実現されます。 以下に示すのは、eTrust AC によって保護されるリソースの種類および制御されるアクセスの種類です。

ファイル（包括、個別）

拡張ファイル アクセス制御は、オペレーティング システムの制限範囲を越えてファイルを保護します。 たとえば、ある特定のファイルへのアクセス権がないユーザは、root アクセス権があっても、そのファイルにアクセスできません。 eTrust AC では、ファイルにアクセスする方法（どのプログラムまたはアプリケーションを使用するかなど）を制御することも可能です。

ネットワーク接続

eTrust AC は、送受信ネットワーク接続を規制して、ネットワーク サービスおよびポートへのアクセスを制御します。

プロセス

eTrust AC は、プロセスが権限のないユーザに強制終了（kill）されないように、プロセスを保護します。 Windows サービスを保護することをお勧めします。

ユーザ ID およびグループ ID(su)

UNIX のみ。 eTrust AC は su によって代わったユーザ ID およびグループ ID を制御できます。 別のユーザのパスワードを知っていても、それだけでは su でそのユーザにはなれません。

特権プログラム

特別権限によって実行されるプログラムは、システム リソースへの不正なアクセスの主要な発生源です。 eTrust AC は、特権プログラムの信頼基盤が変更されないように保護し、承認されていない新しい特権プログラムの実行を阻止します。

SPECIALPGM

プログラムやシステム サービスなどのアプリケーションによっては、特別な eTrust AC の権限保護が必要になります。 SPECIALPGM は、論理ユーザ名(eTrust AC データベースの USER レコードとして定義)をプログラムの実行に必要な Windows ユーザ名(たとえば、SYSTEM)に関連付けることによって、特定のプログラムを保護し、この論理ユーザのみにプログラムを実行する権限を付与します。

スタック オーバーフロー防止機能 (STOP)

STOP は、ハッカーがスタック オーバーフローを悪用できないようにします。ハッカーはシステムに侵入するために、スタック オーバーフローを悪用してあらゆるコマンドを実行します。

端末

eTrust AC は、ログイン可能な条件、端末、およびユーザを定義して、システム アクセスのエントリ ポイントを制御します。

ユーザ定義のリソース

管理者は、eTrust AC の Authorization API およびデータベース ツールを使用してサイト固有のルールを定義し、eTrust AC サーバに接続しているアプリケーションからデータへのアクセスを保護できます。

別のユーザおよびグループとしての実行

Windows のみ。 eTrust AC は、別のユーザおよびグループとしての実行を制御します。 別のユーザのパスワードを知っていても、それだけではそのユーザとしては実行できません。

Windows レジストリ

Windows のみ。 eTrust AC は、レジストリ キーへのユーザのアクセスを制限します。 ユーザに対して、READ、WRITE、DELETE などのアクセス権限を 1 種類以上与えることができます。 アクセス権限は、個々のレジストリ キーに対して、または類似した名前を持つレジストリ キーの集合に対して指定できます。

Q: eTrust AC は root のアクセス権を獲得した攻撃者からリソースを保護できますか。

A: はい。 実際に、これは eTrust AC が UNIX および Linux のセキュリティを強化する主要な方法の 1 つです。 ネイティブ UNIX では、ID がゼロ(0)のユーザは、すべてのシステム リソースにアクセスできます。 ユーザ パスワードとファイル許可は、root の奪取に成功したユーザに対して効果がないばかりか、監査証跡を残さずにルールを変更される可能性もあります。

Q: eTrust AC は、どのように root 権限を管理しますか。

A: UNIX および Linux のセキュリティに対する最大の脅威は、組織内のユーザに個別にアクセスできる強力なユーザ ID としてのスーパーユーザ、すなわち root の存在にあります。 eTrust AC では、以下の処理が行われます。

- root へのアクセスを監視する
- root の実行可能な操作を定義し制限する
- 無制限に root 権限を公開しないように修正する
- 責任の所在が明らかなユーザに特別な権限を移す
- 攻撃者が root のアクセス権を使用して与えるダメージを制限する
- この画期的な機能は、既存のセキュリティ ソリューションでは実現されていませんでした。

Q: root 権限は、使用目的に応じてどのように委任されますか。

A: 管理者およびオペレータには、職務を遂行するために root アクセス権が必要です。eTrust AC を使用しない場合は、管理者とオペレータに root パスワードを知らせることによって、root アクセス権を与えます。これは「オール オア ナッシング」という方法です。eTrust AC には、「役割」を定義するためのルールが用意されています。このルールの適用は簡単です。役割によって、責任の所在が明らかなユーザに root 権限を委任します。

Q: eTrust AC のファイル アクセス制御は、UNIX または Linux のファイル アクセス許可に代わるものですか。

A: いいえ。UNIX のファイル アクセス許可に代わるものではなく、UNIX のファイル アクセス許可を拡張するものです。 ネイティブ UNIX には、root アクセス権を獲得した攻撃者に対するファイルのセキュリティ保護機能がありません。また、グループ化したファイルへのアクセス権を指定して管理する、ワイルドカード定義を使用したファイルの包括的なセキュリティ保護機能もありません。

eTrust AC は、すべてのファイル アクセス要求をインターセプトし、要求した方法でファイルにアクセスする権限がユーザに与えられているかどうかを ACL に従って判定することで、ファイルを完全に保護します。

eTrust AC では、/etc/* または $DIR/webserver/ht-docs/* のように指定して、ディレクトリ全体の内容を保護することができます。 eTrust AC のルールでは、$HOME/*/.rhosts のようにファイルを指定して保護することもできるため、すべてのユーザの .rhosts ファイルを保護することができます。 また、同名のファイルの集合を保護するルールを設定することもできます。たとえば、/app/config* と指定すると、 /app/config.dat および /app/config.tar が保護されます。

1 つのディレクトリにまとめられないファイル、または共通命名規則で指定できないファイルを保護する必要が生じた場合は、GFILE クラスを使用できます。 このクラスを使用すると、特定のファイルを定義し、そのすべてのファイルを対象に、共通するアクセス制御ルールのセットを適用できます。

さらに、プログラム アクセス制御リスト(PACL)を用いて、機密リソースが必ず承認済みのプログラムのみを使用してアクセスされるようにすることができます。 たとえば、人事データベース ファイルへの書き込みが、特定のデータベース アプリケーションのみを使用して行われるようにすることができます。 ネイティブ UNIX の ACL(Solaris および HP-UX)をサポートするオペレーティング システムでは、eTrust AC によって、eTrust AC の ACL とオペレーティング システムを同期させることができます。

Q: ルールの制限の程度をどのようにして判断できますか?

A: 必要とされるルールを本番稼動前にすべて準備するというのは、現実的ではありません。 そのため、eTrust AC には警告モードという監視のみを行うアクセス状況を調査するためのモードが用意されています。 アクセス権のないユーザが、リソースにアクセスを試みたとします。 リソースが警告モードになっている場合、アクセス ルールは適用されません(オペレーティング システムから許可が得られると、ユーザはリソースにアクセスできます)。しかし、本番稼動時であれば拒否されるべきアクセスであることを示す特別な監査ログ エントリが作成されます。

リソースへの警告付きアクセスの監査ログ エントリを調べることで、実際にルールを適用しなくても制限が厳しすぎるかどうかを判断できます。 これは、新しいルールを開発する場合に特に便利です。アプリケーションを中断して OS に突発的な影響を与えるリスクがないからです。

Q: インターフェースとバッチ プロセスの両方を使用して eTrust AC を管理することはできますか。

A: はい。 selang のコマンド ライン インターフェースは、ポリシー マネージャ(管理インターフェース)およびバッチ プロセスの両方で使用できます。

Q: Policy Model とは何ですか?

A: Policy Model は、複数のシステムにアクセス ルールを伝達し、サブスクライバとしてさまざまなホストが設定されたアクセス ルール セットのモデルを作成するためのシンプルな階層メカニズムです。 個々の PMDB は、独立した eTrust AC データベースであり、PMDB には、特定のホスト システムに関連付けられた eTrust AC データベースと同じ種類のルールが保存されています。 マスタ PMDB にルールを適用すると、そのルールは、マスタ PMDB に対して定義したすべてのサブスクライバ データベースに伝達されます。

Q: eTrust AC では、Windows と UNIX の両方のオペレーティング システムを管理できますか。

A: はい。 eTrust AC は、管理者が Windows と UNIX の両方のユーザ アカウントおよびリソースを集中管理できる、強力でわかりやすい GUI を提供します。

Q: ユーザの追加は、UNIX または Linux と eTrust AC で 1 回ずつ、合計 2 回行う必要がありますか。

A: いいえ。ただし、リソースへの明示的なアクセス権が必要なユーザは、両方の環境で定義する必要があります。 つまり、ネイティブ UNIX および eTrust AC データベースの両方に定義する必要があります。 ポリシー マネージャのインターフェースを使用して、UNIX および eTrust AC の両方のユーザおよびグループの定義と定義変更を行うことができます。

Q: eTrust AC では、UNIX および Linux オペレーティング システムと同様に Windows オペレーティング システムを管理できますか。

A: はい。 eTrust AC は、管理者が複数のオペレーティング システムのユーザ アカウントおよびリソースを集中管理できる、強力でわかりやすい GUI を提供します。

Q: eTrust AC は、SecureID のようなハードウェア ベースの認証をサポートしますか。

A: eTrust AC は認証プロセスを中断しないので、すべての認証ソフトウェアと互換性があります。

Q: eTrust AC とファイアウォールとの違いは何ですか。

A: ファイアウォールは、ネットワーク、ホスト、ユーザ、プロトコル、サービス、およびアプリケーションを使用して、ネットワーク経由で行う外部ソースとの送受信を制限するために使用されます。 企業のネットワーク ベース接続の増加に伴い、より大量のデータをファイアウォール経由で送信する必要が生じてきました。

ファイアウォールの内側では、サーバやデータは無防備です。 eTrust AC は、DMZ 内にあるシステムのリソースと同様に、ファイアウォールの内側にあるシステムのリソースを保護します。

Q: ファイアウォールがあっても eTrust AC が必要ですか。

A: ファイアウォールは送受信ネットワーク トラフィックをフィルタ処理するために重要です。 優れたファイアウォールは、システムに入り込もうと画策するユーザの数を大幅に減らし、貴重な情報がインターネットに流出しないように保護します。

しかし、ファイアウォールでは、ユーザがネットワークに入り込んでしまうと、防御することはできません。 さらにファイアウォールは、クラッカーの標的になっています。

Q: eTrust AC が事前対処（Proactive）セキュリティを提供するとはどういう意味ですか。

A: ほとんどのセキュリティ ソリューションでは、事後対処的な性質の手法が採用されています。 コンピュータ セキュリティにおいて、事後対処的な性質の手法は、セキュリティの侵害にアプリケーション レベルで対処するに過ぎず、一時的な解決にしかならないことが歴史的に実証されています。 eTrust AC は、システムおよびシステム コールのレベルでセキュリティ イベントを処理するように設計されています。

このアプローチが採用されている理由は、リソース アクセス要求（アプリケーションまたはその他）はすべて、システムによって処理され、カーネルを経由しなければならないからです。 eTrust AC では、セキュリティを脅かす要求が発生したときに要求をインターセプトして拒絶し、セキュリティに対する脅威を未然に防止することが可能です。

Q: eTrust AC が一般的なフリーウェアのセキュリティ ソリューションよりも優れている点は何ですか。

A: フリーウェア ソリューションは、本質的に事後対処的なものです。 つまり、提供される処置はroot攻撃やシステム攻撃に対しては無防備であり、原因を取り除くのではなく症状に対処します。

以下に eTrust AC がフリーウェアより優れている点を簡単に示します。

- 自己防衛機能
- 自己チェック機能（データベースやサービスまたはデーモンの管理）
- 実行中に環境設定ファイルを保護する
- インストールおよび管理時の少ないオーバーヘッド
- ベンダー サポート
- 段階的な導入方法が用意されています。 eTrust AC には警告モードがあり、 平常の業務に支障のないように、ルールを適用できます。
- フリーウェア ソリューションのスーパーセットとして、また、複数マシンおよび複数プラットフォームを管理するための一元管理ポイントとして、共通ソリューションを提供します。

よく知られているホスト ベースのソリューションとして、sudo、監査、Tripwire、および tcp_wrappers があります。 eTrust AC は、これらのソリューションの機能のスーパーセットを単独のパッケージで提供し、カーネルで事前対処セキュリティを提供することによって、症状ではなく根本的な問題に対処します。

おそらく「root アカウントが攻撃されても、フリーウェア ソリューションによる保護は可能でしょうか。」という質問がでてくることでしょう。答えは「いいえ」です。これらのツールを使用していれば安心だという考えは間違っています。 eTrust AC を使用すれば、答えは「はい」です。重要なリソースを保護できます。

Q: eTrust AC とネイティブのファイル アクセス許可との違いは何ですか。

A: ネイティブのファイル アクセス許可では、Read、Write、および Execute のアクセス権が、所有者、1 つのグループ、または全員に与えられるだけです。 ネイティブのファイル アクセス許可では、どのファイルについても、root アクセス権またはそのファイルの所有者が上書きできます。

eTrust AC は、Update、Delete、Create などのアクセス権によって、通常のオペレーティング システムのアクセス モードを拡張します。 eTrust AC のアクセス モードは、ファイル所有者や root アカウントによって変更されることはありません。 UNIX または Linux ではアクセス権が 1 つのグループに制限されていますが、eTrust AC では複数のグループに異なるアクセス権を与えることができます。

eTrust AC は、どのプログラムがファイルにアクセスできるかという条件でもファイル アクセス権を拡張します。この機能は、ネイティブ UNIX または Linux では提供されていません。

Q: eTrust AC は、完璧なセキュリティ ソリューションですか。

A: 完璧なセキュリティ ソリューションはありえません。 しかし、eTrust AC は、オペレーティング システムのセキュリティ問題の原因に対処することで、これまでにない包括的でより合理的なソフトウェア ソリューションを提供します。 セキュリティの側面は、ソフトウェア制御の範囲を越えて、物理的なアクセスやアカウント共有に関する常識的なポリシーを確立し、適用することで処理されます。

Q: ハッカーは「rootkit」のようなツールを使用してマシンへのアクセス権を獲得すると聞きました。 eTrust AC で、このようなツールを使用した攻撃に対処できますか。

A: rootkit は最近使用されるようになったツールで、マシンへの不正アクセスに使用されている数あるツールの 1 つです。 不正アクセスを行うツールはこのツールが初めてではありません。また、今後、同様のツールが現れないとも限りません。 eTrust AC がこれらの問題に対処する方法を理解するために、ハッカーの目的と一般的な特徴、ハッカーのツール、および eTrust AC による対処方法について説明します。

ハッカーの目的は、root アカウントを獲得し、システムの完全な制御を取得することです。eTrust AC は、root ユーザになることができるユーザやその設定方法を制限することでこの問題に対処します。 権限のない root アクセスが実行された場合、eTrust AC は、何にアクセスできるかを制御できます。

ハッカーの脅威に対する防御を以下に示します。

攻撃の特徴	ハッカーの攻撃	eTrust AC の防御
A) 侵入	A1)既知のサービスの欠点	A1a)有効なリモート ソースへのアクセスを無効化または制限する
	A2)不正なパスワードのアカウント	A2a)繰り返して攻撃されているアカウントを無効にする
		A2b)機密アカウントをローカル アクセスのみに制限する

攻撃の特徴	ハッカーの攻撃	eTrust AC の防御
		A2c)パスワード品質制御を実施する
B)root の獲得	B1)プログラムの欠点	B1a)root でアクセスできるプログラムを制限する
	B2)root パスワードの推測	B2a)root をローカル アクセスのみに制限する
		B2b)パスワードが知られた場合でも、root になれるユーザを制限する
C)oot の維持	C1)既存の特権プログラムの変更	C1a)特権プログラムを改ざんから保護する
	C2)新規特権プログラムの混入	C2a)未承認の特権プログラムが混入しないようにシステムを保護する
	C3)侵入を隠すためシステム ログを変更	C3a)システム ログを改ざんから保護する
		C3b)システムとは別のログを作成する

さらに、eTrust AC は新しい eTrust テクノロジを採用しています。このテクノロジは STOP(スタック オーバーフロー防止機能)といい、スタック オーバーフローまたはバッファ オーバーフロー攻撃に対する防御を提供します。これにより、eTrust AC のシステム保護機能がより強化されます。