ユビキタス環境のセキュリティ管理

則房 雅也・桑田 雅彦
一宮 隆祐・進藤 章治

要　旨

ユビキタス環境では、ネットワークやサービスの利便性が飛躍的に向上する一方、利用者、アクセス場所、アクセス経路を特定することが難しく、セキュリティ管理面で新しい課題が生じます。ユビキタスというインフラの利便性によるので、セキュリティ管理の基本にたって対策を考えるべきであり、アクセス時のユーザ認証とその後の行動追跡への取り組みが重要な鍵になります。そのために、ID管理とログ管理が基本情報を提供します。これら管理を統合化すると新しい分析が可能となり、広い範囲でユーザの行動を追跡できるようになります。本稿では、IDとログ管理の統合化が向上させるセキュリティ管理について説明します。

キーワード

●統合ID ●統合ログ ●特権ユーザ ●セキュリティ管理 ●コンプライアンス ●証跡 ●監査

1. はじめに

ユビキタスなブロードバンドネットワークが、これまでとは比較にならないほど充実していきます。これを有効活用する鍵は、持ち運ぶことのできるPCや携帯端末などでどのようなサービスが得られるか、にかかっています。

「ユビキタスの活用＝サービスの活用」となる場合、インターネットの特長ともいうべき匿名性は、ユビキタスやサービス普及の足かせとなります。ユビキタス環境からアクセスするユーザに安全なサービスを提供し、多くの誠実なユーザが不祥事に巻き込まれないためには、これまで実装してきたセキュリティ対策を慎重に再評価しなければなりません。その中でも、匿名性を排除する「ID管理」と、不正利用がなかったことを証明する「ログ管理」は今後特に重要になるといえます。本稿では、IDやログ管理を、ネットワーク規模で統合的に管理することの必要性と、それがセキュリティ管理のインフラとして不可欠であることを説明します。

2. 今後の情報セキュリティ

ユビキタス環境になり新たな問題が発生する場合が予測できます。例えば、

1) ネットワーク再接続のたびに端末のIPアドレスが変わり、IPアドレスでユーザのアクセス管理は行えない
2) インターネットでさまざまなサービスを利用すると、いつか不正プログラムを端末にインストールされてしまう
3) 端末と一緒に個人情報や機密情報も持ち運ばれるので、情報漏えい管理により注意を払う必要がある

などがあり、実環境ではもっと多くの状況が発生します。

上記1）～3）では、運用者から遠いところで問題が発生し、ユーザは発生を認識できず、運用者が気付くまでに時間がかかるなど、問題を把握するタイミングが遅れます。

これらはユビキタスという新しいインフラの利便性から発生するので、発生するたびに対策するのではなく、インフラの一部として本質的な対策を考えるべきといえます。それらが「ID」と「ログ」の統合的な管理になるのです。

どのような装置やシステムにもログが残りますが、それぞれの情報は限られています。しかし、PCとシステムとネットワーク装置などのログを統合的に見ると、ユーザや装置を示すID間の関連性、そのIDでの作業履歴などから、1ヵ所のログを越えて何を行ったかをたどり、これまで見えなかったネットワーク範囲でのユーザの挙動が分かってきます。

3. 統合的なID管理とログ管理

3.1 ID管理

ITを利用するすべてのユーザが毎日使う情報がIDです。IDとして扱われる情報は増えており、電子メールアドレスはその例です。個人情報でもあり、ID管理の重要性は日々ましています。

(1) 従来のID管理の課題

ユビキタス環境で使われるネットワーク装置やサーバには、同一ユーザが別々のIDを用いており、それらIDを関連付け

て管理したいという課題があります。また1つのID（特に特権ID）を共用している場合には、実ユーザを特定したいという課題があります。更にユーザの属性、所属（グループ）、役割（ロール）がアクセス条件に使われている場合、人事異動が反映されないと、異動後も不要にサーバにアクセスしていたといった問題につながる恐れがあります。

(2) IDの統合管理

統合ID管理システムを使って、ネットワーク装置やサーバ、また不特定に接続される端末のID管理を連携させて、どこにアクセスしても個人を特定できるID管理を実現します。このとき、既存のID運用を変更せずに、各ユーザがそれぞれで使っているIDの関連管理をシステム化します。また、IDの共用には、統合ID管理システムで認証を受けさせ、どのユーザが共用IDを利用したかを特定します。更に、ユーザの属性、所属、役割を統合ID管理システムで一元管理し、更新をネットワーク装置、サーバ、端末それぞれに対して自動配信（プロビジョニング）します。人事異動で変更があると同期をとり、異動したユーザへのアクセス制御漏れを起こすこともなくなります。

(3) NECの統合ID管理製品SECUREMASTER

NECでは統合ID管理製品「SECUREMASTER」を提供しています。日本のカスタマに固有のID管理要件を考慮し、大量の一斉定期人事異動、複数組織への兼務、階層の深い組織構造などに合わせた権限管理を行えます。また、コンサルテーションや技術サポートを充実させており、複雑な要件に柔軟に対応します。SECUREMASTERの中でIDのプロビジョニングを実現するのがEnterprise Identity Manager（EIM）で、基本動作は**図1**に示す通りです。

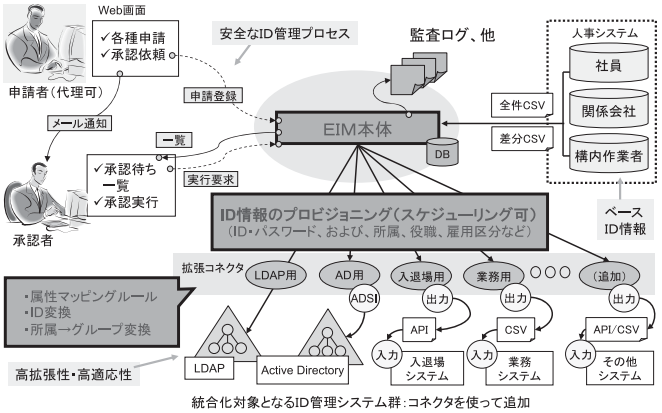

図1　Enterprise Identity Manager 基本構成

EIMには監査機能があり、EIMが保有するIDマスタ情報と、統合管理される対象システムの個別IDを突き合わせることにより、削除漏れIDや使用されなくなったIDを洗い出すなど、IDの棚卸しを実施します。

3.2 特権ユーザ管理

代表的な特権IDが、UNIXのroot、WindowsのAdministratorです。システムリソースのあらゆる変更権限が与えられ、アクセス範囲を制限されません。

(1) 従来の特権ユーザ管理の課題

特権IDが持つアクセス権限は、サイバー犯罪の標的になっています。ソフトウェアには、設計ミスやバグ、利用条件に起因する脆弱性が内在しており、後にセキュリティホールとして顕在化します。プロの犯罪者はこのセキュリティホールを攻撃して特権を奪います。

1ヵ所で特権が奪われ、周囲の装置やサーバまで特権IDでアクセスできては被害がどこまでも広がります。特権IDが共用されていると、この危惧は現実になります。

ネットワーク装置などインフラの安全・安心の確保は最も重要です。これらを管理する特権ユーザのアクセス管理に対し抜本的な対策が求められています。

(2) NECの特権ユーザ管理製品SecuveTOS

UNIXやWindowsの任意アクセス制御（Discretionary Access Control）機構では、ファイル所有者がアクセス権を設定します。しかし、特権ユーザはこの制御をバイパスでき、アクセスログも残りません。この問題を、OSから独立したアクセス制御の仕組みを導入して解決できます。これにより、セキュリティポリシーの適用を保障する「強制アクセス制御（Mandatory Access Control）」を実現します。アプリケーションとOSの間でアクセス制御を強制することで（**図2**）、特権ユーザも管理され、作業証跡を記録します。

通常、悪意ある第三者が特権IDを使うと、正当な管理者と区別できません。しかし、強制アクセス制御では、特権ユーザに対してであっても、重要ファイルを読み取り専用にして保護できます。また、実行中のプロセスを不正な停止や再起動から保護できます。重要ファイルを変更する場合には、電子証明書を組み合わせて高度なユーザ認証を行い、不正な特権IDの利用と区別することが可能です。

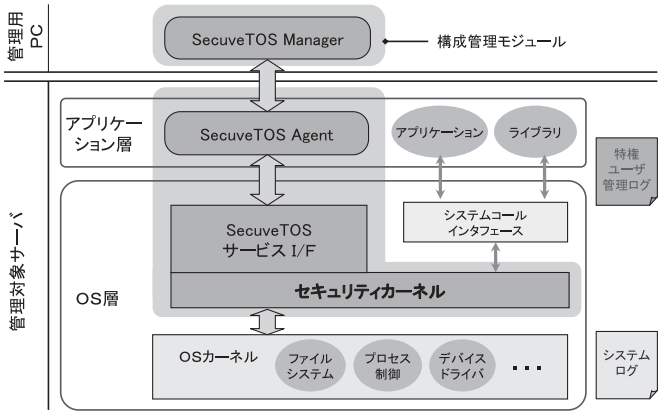

図2　SecuveTOSのアーキテクチャ

NECでは、特権ユーザ管理製品「SecuveTOS」を提供し、特権IDの管理を強化してセキュリティポリシーの強制を実現します。

3.3 ログ管理

装置やサーバが残すログは、運用者がシステム障害を確認することに使われ、普段は参照されない情報でした。近年この用途が拡大し、セキュリティやコンプライアンスへの対応状況を確認するために使われようとしています。

(1) 従来のログ管理の課題

上記用途のためログ管理に新しい要件が出ています。1点目は分散して別々に管理されているログの有効活用です。2点目はログ保管期間の長期化と後で再利用できることです。

情報漏えいが生じたとき、初めに疑わしいサーバやネットワーク機器、PCのログが調べられます。金融商品取引法（J-SOX）では監査のためにログを長期保管すること、財団法人金融情報システムセンター（FISC）の金融機関向けガイドラインでは7年間の保管が義務付けられています。

故意に不正が行われた場合、その痕跡を消すために必ずログを削除または改ざんします。訴訟時の法的証拠や、内部統制の有効性を示す報告書として使うためには、ログが改ざんされていないことを証明しなければなりません。

(2) ログの統合管理

新しいログ管理要件を満たすには、分散したログを統合管理し、安全に保管する必要があります。統合化するとき、大量のログを効率よく収集する性能と安全に保管しておくストレージの容量と完全性という課題があり、情報のフィルタリング、圧縮、セキュリティが重要になります。集めた情報は有効活用して価値が出るため、大量情報の検索、加工、相関分析、見える化という技術が重要になります。

こういった高い要求を満たすのが、統合ログ管理製品です。大量の情報を処理するため、企業では統合ログ製品を導入し、管理コストの大幅な削減に取り組むことができます。

(3) NECの統合ログ管理製品「RSA enVision powered by Express5800」

NECでは統合ログ管理製品「RSA enVision powered by Express5800」を提供し、あらゆる形式のログを収集し、データを圧縮、秘匿化してデータベースへ保存します。

外部ストレージをつけることでどんな大量ログの長期保管も可能です。ログを収集しながら相関分析、アラートの発生、レポートの作成を行います。

ハードウェア、ソフトウェア、データベースが一体となったアプライアンス製品で、これらの性能、信頼性、障害対策が設計、保障されています。

3.4 IDとログの統合管理により得られる解

統合化したID管理によって本人確認と追跡性が改善しますが、悪意のある内部犯行は発見できません。内部犯行には、内部システムの利用監視が効果的で、ログを内部広範囲から集めて統合的に分析することで、早期発見を期待できます。

一方、集めたログには、装置やサーバによって固有のIDが残っています。例えば、ネットワーク装置には、ユーザIDではなくユーザPCのIPアドレスが残ります。

通常これらの関連性は分かりませんが、ネットワーク装置、サーバ、端末に残る別々のIDを、同一ユーザのIDとして関連付ける分析を行うことで、ユビキタス環境全体でのユーザの一連の行動を追跡できるのです（**図3**）。

4. 情報漏えい不祥事に見るケース・スタディ

社内のしかるべき立場にいた人が特権的な立場を利用して、アクセス制限のある情報を持ち出し、第三者に渡して報酬を得たという不祥事がありました。その犯行プロセスについて、おおよそ以下のような指摘をすることができます。

1) 機密情報へのアクセスにはシステム運用管理者の特権ID

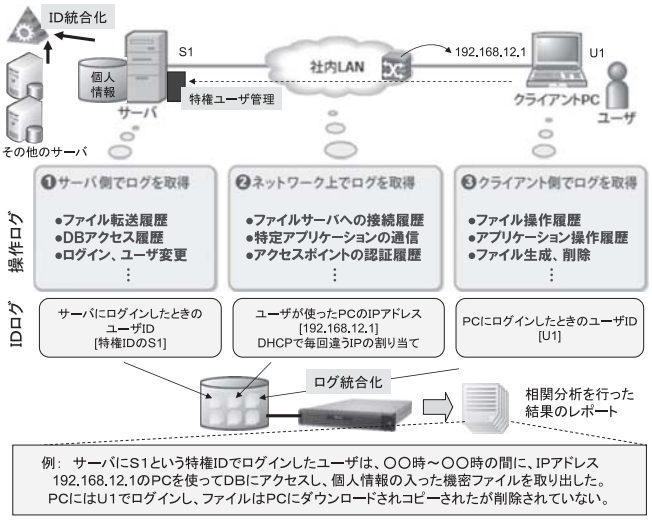

図3　ログを統合化することであぶり出せる情報

が利用された

2) この運用管理者は会社を辞めていたにもかかわらず、特権IDは削除されていなかった

3) 犯行者のIDでは情報を移動できないが、運用管理者を管理する立場にあり、その特権IDを利用できた

4) 運用管理者の特権IDで使えるサーバを、情報持ち出しの踏み台に使った

5) 情報を暗号化して中身をチェックする機構が途中で働かないようにしてサーバにアップロードした

6) 最後は、ソーシャルエンジニアリングを使って第三者を動かしてサーバから情報を持ち出した

セキュリティポリシーも技術的対策も十分行われている組織で起こった不祥事です。大きなポイントは、特権IDの管理が甘い、不正行為を途中で検知する仕組みがない、などです。

2）を不使用IDの棚卸しで、3），4）を特権ユーザ管理の強化で、2）～5）に対してはログを統合して相関分析し、不正行為の兆候を早期発見することで、問題の発生をどこかで食い止められたと思われます。このようにIDとログの統合管理、ログ分析が、特に内部ユーザの不審な行為の検知に有効な手段を提供するのです。

5. おわりに

本稿では、ユビキタス環境でネットワークやサービスを安全・安心に利用するためには、ネットワーク範囲での統合的なID管理とログ管理が基本であることを示しました。特に、ネットワーク装置やサーバを制限なく変更できる特権IDの管理が重要で、すべてがネットワークでつながった社会では厳重な対策が不可欠であることを指摘しました。また、IDとログを統合的に管理すると、異なるIDを使っても、同じ人がアクセスしたネットワークやサーバ、そこで行った作業を把握し追跡することができ、不審な挙動をネットワーク範囲で検知することができることを示しました。

セキュリティに限らず、このような管理の統合は年々増えるコンプライアンス要件を満たす上でも有効です。

新しい脅威は必ず現れますが、普段と異なる挙動が必ずあるはずで、ネットワーク上のどこかに形跡が残っていると検知し対策を検討できます。また、対策技術が今ない場合でも、周辺のセキュリティ管理を強化して問題発生を抑える手を打つことができます。このように、いつでもセキュリティ問題を回避してビジネスを続けさせられる骨太のセキュリティ対策が重要になります。

NECは今後もこういう骨太のセキュリティ対策を研究し、簡単に使える手法として具体化し市場に提供していきます。

参考文献

1) 「次世代の情報セキュリティ政策に関する研究会報告書」、総務省情報通信政策局、2008年7月

2) 則房、他「従来のセキュリティ対策の限界を破る「協調型セキュリティ」」、NEC技報Vol.60、2007年1月

執筆者プロフィール

則房 雅也
システムソフトウェア事業本部
第一システムソフトウェア事業部
上席アドバンストテクノロジスト

桑田 雅彦
システムソフトウェア事業本部
第一システムソフトウェア事業部
エンジニアリングマネージャー

一宮 隆祐
システムソフトウェア事業本部
第一システムソフトウェア事業部

進藤 章治
NECソフトウェア東北
事業推進部
主任