ユビキタス時代のコミュニケーション基盤に求められるセキュリティ

北風 二郎

要　旨

企業の通信環境は、“いつでもどこでも”を実現するユビキタスな利用環境へと拡大しています。一方でセキュリティに対する課題は、コンプライアンス、内部統制、リスク管理といったマネジメントへとフォーカスされてきています。本稿では、今後のコミュニケーション環境の発展に伴って要求されるセキュリティマネジメントについての考え方と具体的なソリューションについて紹介します。

キーワード

●セキュリティ ●コンプライアンス ●ユビキタス ●コミュニケーション

1. はじめに

企業活動におけるコミュニケーションの手段は、電話、FAXといった旧来からの情報伝達手段から、メール、Web会議システム、TV会議システム、インスタントメッセージといった、様々なIT技術を利用したメッセージングシステムへと急速な広がりを見せています。

また、コミュニケーションの利用範囲も、上記のコミュニケーションツールがすべてIPネットワーク上の基盤で動作するように統合されていくことによって、企業内に閉じた利用から営業現場、様々な業態での作業現場（流通、建築、医療、教育など）、工場、自宅、移動中の車内など、あらゆるユビキタスな利用環境へと社内外を問わず急速に拡大しています。これにより企業活動におけるコミュニケーション基盤の重要性は、ますます増大の一途をたどっています。

しかし、一方でこのようなコミュニケーション環境の変化に伴い、企業のセキュリティ対策の考え方も従来の防御偏重型のセキュリティ対策から、マネジメント型のセキュリティ対策へと変化してきており、その重要性を認識し早急な対策を講じることが急務となっています。

以下に、コミュニケーション基盤の進化とともに、コンプライアンス、リスクマネジメントの観点から求められるセキュリティ対策の考え方、およびソリューションについて具体的に紹介します。

2. 企業コミュニケーション環境の変化

企業の重要なコミュニケーション手段としては、かつては電話やファクシミリ（FAX）が用いられてきましたが、1990年代から登場したインターネット（特に電子メール）の企業の通信伝達手段としての導入に伴い、大きくその様相が変わってきました。

従来は、緊急時の重要な伝達手段であったFAX利用のほとんどが電子メールに移行されるとともに、緊急性を要さない電話連絡での伝言などにも、積極的に電子メールが利用されるようになりました。

その後、企業のコミュニケーションは、映像も交えたWeb会議システムの利用、電子メールシステムよりも即時性の高いインスタントメッセージの利用、コミュニケーションだけではなく実際に遠隔地間でのドキュメント作成、開発作業までを進めるコラボレーションツールの利用など、ますます多様化の一途をたどっています。

また、様々なコミュニケーションツールが氾濫した結果、ツールの選択、操作が煩雑になるという弊害も出始めています。そのような中、IPテレフォニー環境を核としてコミュニケーションツールを統合し、より効率化しようという、ユニファイドコミュニケーション（Unified Communications: UC）への取り組みが加速しています。これらの環境は、前述の通りすべてIPネットワーク基盤上で動作することから、企業内イントラネット利用にとどまらず、社内外のユビキタス環境への利用をも急速に拡大していきます。

3. セキュリティ対策における課題

ユニファイドコミュニケーションへの取り組みとユビキタス環境への利用拡大に伴い、新たなコミュニケーション基盤におけるセキュリティの課題も、新たな局面を迎えることとなっています。環境変化を含め、最近の企業を取り巻くセキュリティの課題として、以下のような点が挙げられます。

(1) コンプライアンス・内部統制の観点での取り組み

「会社法」「金融商品取引法」などにおいて、大会社および上場会社の内部統制への取り組みが義務化されました。これに伴う内部統制（特にIT全般統制部分）におけるセキュリティ対策としては、ITシステムにおける「アクセスコントロール」「ログ収集・分析」「コンテンツ管理、ワークフロー・承認」が特に重要な対策と位置づけられています（**図1**）。

(2) コミュニケーションツールの利用に対する課題

コミュニケーションツールの発展に伴い、様々なツールの利用に対してのセキュリティリスクの評価と対策が求められるようになってきています。たとえば、利便性が非常に高いツールの1つとして、P2Pソフトなどが挙げられますが、セキュリティ面からみると企業内の情報漏洩につながる大きなリスクを生み出す脅威ともなっています（代表的なものとして、悪名高いWinnyもこの中に含まれます）。

このように、様々なコミュニケーション手段とその連携、統合が実現されていく中では、常にそのセキュリティに対する継続的な検証・評価の体制構築も、今後大きな課題となっていくことが想定されます。

(3) アイデンティティ（ID）管理の重要性

ID管理の重要性は、ITシステム利用が加速し始めた2000年ごろから認識され、活発に議論され始めました。当時、基幹業務システムのオープン化に伴い乱立した、Webシステムのユーザアカウントの氾濫、グループウェア、メールシステム、Windows ® ネットワーク、基盤ネットワーク、さらには物理的な入退管理システムに至るまで、あらゆるシステムが個別にユーザIDを持って個別に管理されているという状況の中で、本来なら人に付属したユニークな属性情報として管理されるべきID情報の統制がまったく取れていない、という由々しき事態を引き起こしていました(**図2**)。

この状態での顕著な問題としては、

1) IDの不正利用、なりすまし

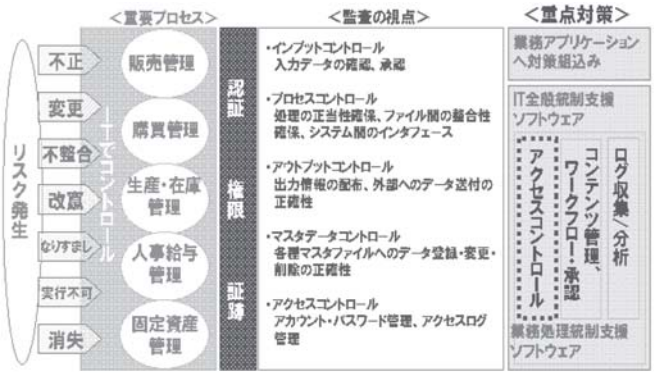

図1　ITにかかわる全般統制の監査の視点と重点対策

図2　ID情報がシステムに個別に分散している状態

2) パスワードの漏洩

3) ID、パスワード管理業務の工数の肥大化

などが挙げられます。これらは、セキュリティ面、管理面での重大な問題を引き起こす結果となりました。

また、内部統制、コンプライアンス重視の観点での重要な対策項目となる「アクセスコントロール」「ログ管理」「承認・ワークフロー」について、そのキー情報となるID情報の信憑性が無いということは、これら重要な対策がまったく機能していないことを意味することとなり、企業のセキュリティ対策として、深刻な問題となっていました。

これらの課題への取り組みとして、IDを管理するデータベースをディレクトリシステムと呼ばれるサーバ上に、一元的に統合する試みが盛んに実施されました。ところがその結果は、Windows ® のPCネットワークのID管理を主目的としたActive Directory ®（AD）、グループウェアが個別に持つベンダー固有のディレクトリシステム（例：Lotus Notes Domino Directoryなど）、業務アプリケーションIDを

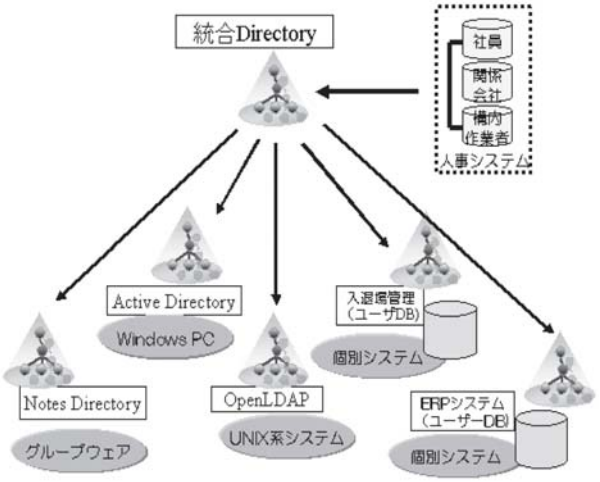

図3　統合Directoryによるアプローチ

リポジトリするためのディレクトリシステム、入退室管理のセキュリティカード（ICカード）で利用されるIDの管理システムなど、様々なID管理システムが並存、乱立する状況となり、完全に統合されたディレクトリシステムでのID管理の運用が成功している事例は数少ない、と言わざるをえない状況となっています（**図3**）。
様々なコミュニケーションツールの登場とこれらの統合利用が進展する中で、システム利用のアクセスログ管理と利用者個人を結び付ける重要な管理対象として、ID管理はさらに重要性を増しており、企業のセキュリティ対策の中でも、優先度の高いテーマの1つとなっています。

4. 最新のセキュリティ対策ソリューションの紹介

最新のセキュリティ対策ソリューションを紹介します。

(1) 統合ID管理

上記課題を解決するセキュリティ対策として、第3章の（1）で示した通り、内部統制の視点でのリスク管理における重要な対策は、システムの「アクセスコントロール」「ログ収集・分析」「コンテンツ管理、ワークフロー・承認」であることは前述の通りですが、これらの対策の最も根幹となるのがID管理です。なぜなら、アクセスコントロールの制御のための拠り所となるのが、人に付属する属性（IDおよびIDに付随する権限・属性）であり、これのID

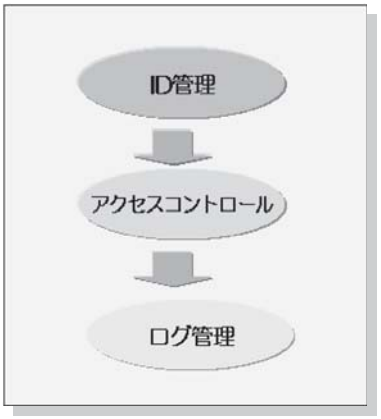

図4　セキュリティマネジメントの３大要素

情報に紐づいた証跡管理こそが、内部統制・コンプライアンス対策で最も重要となるからです（**図4**）。
しかし、第3章（3）の課題で示した通り、IDの統合管理を目的とした統合Directoryへのアプローチは、システムが日々成長する中での継続的な運用において、大きな課題を含んでいます。そこで新たなアプローチとして生まれたのが、複数に分散したID情報を一元的にプロビジョニング、マネジメント可能とする、統合ID管理の考え方です。
図5 には、NECが提供する統合ID管理システムWebSAM SECUREMASTER/EIMによる、統合管理のイメージを示しています。
統合ID管理のアプローチは、Windows ® のActive Directory ®、IBM Lotus NotesのDomino Directoryを始め、各種業務アプリケーション（EXPLANNER、Flow Lites他）、入退管理システム、グループウェア（StarOffice21他）、各種LDAP（Open LDAP、Sun Java System Directory Server、他LDAPv3）へのデータ配信コネクタが準備されており、人事DB情報に基づいた、ユーザID、パスワードの登録、更新、削除が可能となります。これらユーザ管理機能のほかにも、パスワード管理、承認ワークフロー機能も提供するので、万全なID情報およびパスワード管理の一元的な運用を実現します。
また、ID管理機能だけではなくSECUREMASTER/EIM自身もまた、Directory Systemとしてユーザ情報をリポジトリする機能も包含しているため、分散したDirectoryや個別システムのID情報管理に利用することも可能となります。

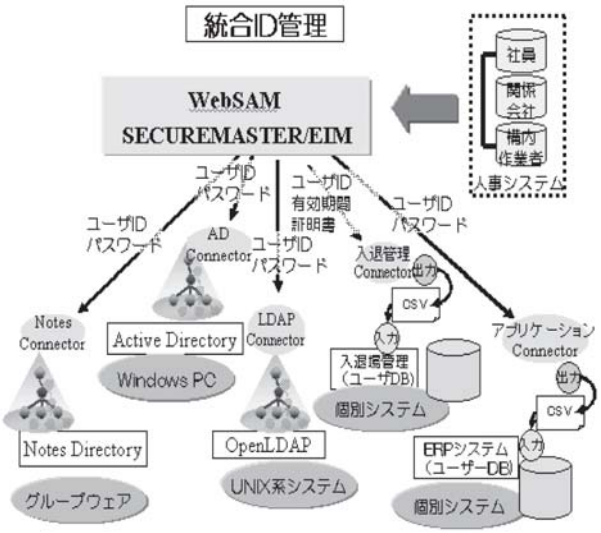

図5　NECの提供する統合ID管理システム

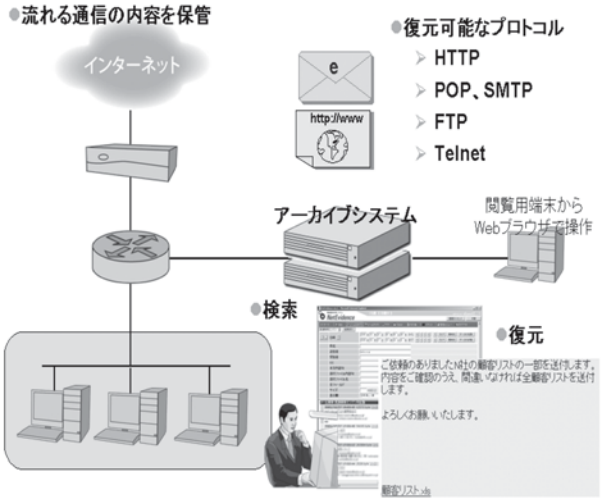

図6　ネットワークアーカイブの適用事例

このような特長を生かして、大規模な入退管理システムのユーザIDの情報管理や、無線LANの認証システムとして利用されるLDAP ServerとWindows® PC認証のActive Directory®の統合運用など、すでに多様な導入実績があります。

(2) ネットワークアーカイブ

多様なコミュニケーション手段が共存するユニファイドコミュニケーションの基盤としてさらに重要となるセキュリティ対策として、証跡管理があります。内部統制に関連するITの統制（IT全般統制）における最も重要なポイントは、この証跡管理の基盤構築にあります。

証跡管理を実施するためのアクションでは、「ログ収集・分析」という対策が必要なのに加え、システムログのみでなくネットワーク上の通信データを記録・保存・分析（アーカイブ）する対策「ネットワークアーカイブ」が注目され始めています。ネットワークアーカイブは、通信のパケットを記録・補完するだけでなく、利用アプリケーション単位での復元する機能をも提供しています。

たとえば、Webサイトにアクセスした際のブラウザでの表示画面の復元、メールの通信パケットからメール本文の復元などが可能となっています。これにより、証跡管理の目的でもある、インシデント発生時の証拠データのレポート作成、解析といった作業が短時間で行えます。

これは、ただログやパケットを収集保存するだけでは内部

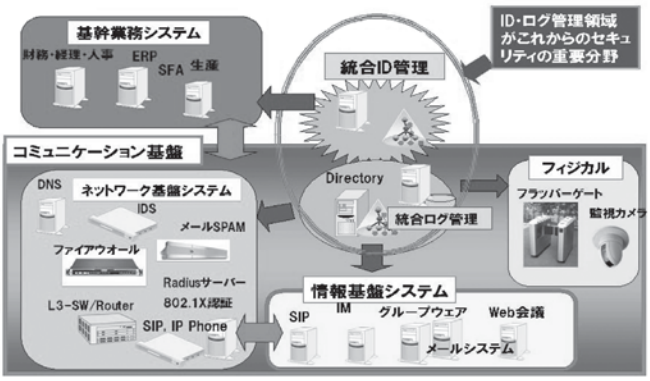

図7　コミュニケーションを支えるセキュリティ

統制の観点からは本来の目的を達していないことを考慮すると非常に重要なポイントとなります。現在、こういったネットワークアーカイブの導入は、まずは社外との情報の出入り口となるインターネットの接続ポイントから進んでいます（**図6**）。

今後、様々なコミュニケーションツールが統合され運用されるユニファイドコミュニケーションの基盤において、ネットワークアーカイブによる証跡管理のソリューションは非常に効果的であり、一層有効な対策となっていくと考えられます。以上述べてきた、様々なシステムが統合管理されているイメージを**図7**に示します。

5. まとめ

ユニファイドコミュニケーションへの期待は、直近ではオフィス業務の効率化から始まり、さらには、様々な業種アプリケーションシステムがコミュニケーション手段を直接キックすることによって、今までは人が介在していたプロセスに対する効率化への期待へと繋がっています。

このような新たなコミュニケーション活用の基盤を支えるセキュリティ対策では、「統合ID管理」「証跡管理（ログ管理、アーカイブ）」「認証」の3つの要素と、これをベースとしたアクセスコントロールが最重要課題となっています（**図8**）。

さらに最近では、ネットワーク基盤を支えるLANスイッチにもこの考え方が積極的に応用され始めています。従来アプリケーション単位（あるいはサーバ単位）でしか実現できていなかったアクセスコントロールを、ネットワーク基盤が提供することでシステム全体の統制をより強化し、個々の管理工数を削減するとともに、セキュリティレベルの向上の効果が期待できる、ネットワークアクセスコントロール（NAC）という仕組み（インテリジェントなLANスイッチ）の導入も進み始めています（**図9**）。

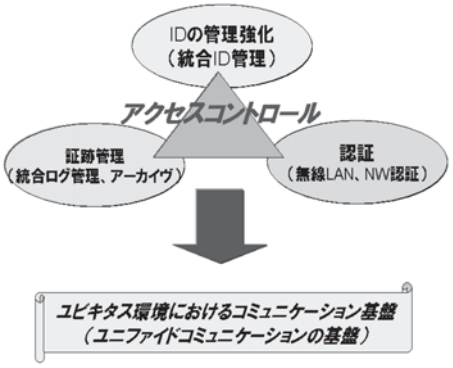

図8　コミュニケーションを支えるセキュリティ

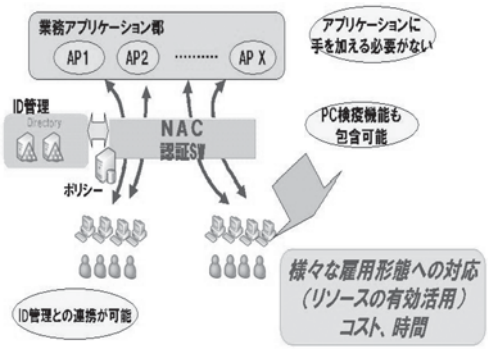

図9　ネットワークアクセスコントロール（NAC）

6. むすび

以上、コンプライアンス・内部統制とこれに対応したセキュリティ対策について紹介しました。NECは、こういったニーズに対しての具体的な対策を進めるためのセキュリティマネジメントシステムを提供するとともに、企業内で対策を進めるに当たっての要件定義に対する支援サービスや、既存セキュリティシステムとの接続検証、導入支援、システムインテグレーション等広範囲でのサービス提供をしています。

現状、国内の企業におけるこれらのセキュリティ対策への取り組みは、法制度の整備や業界でのレギュレーションの確立を待ってからという受身の姿勢がまだまだ伺えます。しかし、これまで述べてきたセキュリティ対策に対して積極的に取り組み実現していくことが、新たなコミュニケーション基盤の整備や活用を検討する上で不可欠な取り組みとなってきます。一歩先を見据えたセキュリティ対策へのアプローチこそが、数年後の企業活動におけるIT活用度において大きな差を生み出していく源となります。

NECは、UNIVERGEを通じて、UCを活用した企業コミュニケーションの革新へとつながるセキュリティソリューションの提供を続けていきます。

執筆者プロフィール

北風 二郎
エンタープライズソリューション事業本部
UNIVERGEソリューション推進本部
部長