マネージドセキュリティサービス

Managed Security Service

武　井　英　直，　入　貝　健　介

要　約　マネージドセキュリティサービス（MSS）は企業内の情報セキュリティに関わる運用や保守などを一括して外部委託するアウトソーシングサービスである．その利便性，コスト削減効果などから MSS を利用する企業は年々増加している．しかしながら，マルチテナント型でサービスが提供されていることや，情報システムの基幹部分のセキュリティ管理を外部委託することによる情報漏洩などの懸念から，MSS 導入を留まるユーザも少なくない．

本稿では，MSS を導入することによって得られる効果，および導入時に留意しなければならない点とともに，事例としてユニアデックスが提供する当該サービスの概要と，それを提供するためのリモート運用基盤の特長や優位性を説明する．また，ユニアデックスが提供する MSS を含めた IT マネジメントサービス基盤のセキュリティ対策についても言及する．

Abstract　Managed security service (MSS) is an outsourcing service where the operations and maintenance of information security in the enterprise are entrusted to the external professional firms. Due to the convenience and cost reduction effect of MSS services, the number of enterprises using MSS services has been increasing year by year. However, because of the anxiety about information leakage by the fact that the service is offered in the multi-tenant form and that security management, an essential part of information system is outsourced, some enterprises give up adopting of MSS services from their operational choice.

This technical paper explains the features and superiority of MSS services offered by UNIADEX and the remote operation service platform from the viewpoint of effectiveness and considerations on adopting the MSS services, and also refers to the security countermeasures to the IT management service base including MSS services offered by UNIADEX.

1. は　じ　め　に

システム管理者が日常的に管理しなければならない項目は多岐に渡る．その中でも，特に重要性が増しているのが「情報セキュリティ」に関連したものではないだろうか．ウィルス感染や顧客情報漏えいなど，情報セキュリティ管理の綻びから生じたトラブルは，最優先で管理すべき項目となっている．さらに IT が社会インフラの一つになっている現在では，情報セキュリティに関する事件/事故を起こすと，その影響は当事者の企業だけに留まらず，関連企業やユーザ，取引先，さらには社会全体に及ぶ場合さえあり，企業の情報セキュリティ対策はもはや社会的責任（CSR）の一環となっている．このような背景から情報セキュリティ対策においては単に内部，外部からのセキュリティ脅威に対処するだけでなく，企業が所有する情報資産について CIA（Confidentiality：機密性，Integrity：完全性，Availability：有効性）を維持するための施策をも講じなければならず，これを効果的に行い，事業活動を継続するために必要とされるセキュリティ全般の管理（セキュリティマネージメント）が必要となってくる．

ひと口にセキュリティマネージメントといっても，それが単純に管理ツールを指すことや，

またはセキュリティポリシーの策定を意味するケースも存在するが，本来はポリシー，ツール，運用の全てがセキュリティマネージメントにより適正化されなくてはならない．しかしシステム管理者が企業内システム全般に渡ってセキュリティを管理することは決して容易なことではなく，システム管理者の負荷はシステムの増加や複雑化に伴い増すばかりである．このような問題に対応すべく各プロバイダから，情報セキュリティのアウトソーシングサービスであるマネージドセキュリティサービス（以降，MSS）が提供されるようになり，システム管理者の負荷を減らすための選択肢の一つとなっている．本稿では MSS について解説し，事例としてユニアデックス株式会社（以降ユニアデックス）が提供する MSS について紹介する．

2. MSS とは

MSS は，ユーザ企業のネットワークセキュリティに関わる運用や保守などを一括して外部委託するアウトソーシングサービスであり，そのようなサービスを提供する企業を MSSP と呼ぶ．2010 年現在，様々な MSSP から多種多様な MSS が提供されているが，それらのサービスは次のように大別することができる．

1） インシデント監視

24 時間 365 日を通してネットワークを監視し，セキュリティインシデントを検知した場合には即時にユーザ管理者に対して通知する．セキュリティインシデントにはネットワーク機器の障害，悪意あるハッキング（不正アクセス），DoS 攻撃あるいはウィルス感染等が含まれる．

2） セキュリティ運用

ファイアウォール，VPN，IDS/IPS 等のハードウエアやソフトウエアへのパッチ適用やアップグレードをユーザに代わって運用する．また適切なセキュリティポリシーに従い，これらネットワーク機器のコンフィグレーション設定やシグネチャ更新等を管理する．その他，不正通信の遮断やコンピュータウィルスの除去などセキュリティインシデントが検知された場合の対応をサポートする．

3） ログ管理

ファイアウォール，VPN，IDS/IPS 等のセキュリティ機器から収集されたアクセスログやインシデントログから，外部からの不正アクセスやセキュリティポリシーに違反する通信を解析する．これらの解析結果は潜在的リスクの発見やセキュリティインシデントの対応に利用することができる．ログ解析にはセキュリティに関する高度な専門知識や技術が必要とされているが，MSSP から提供されるサービスを利用することでユーザ企業はセキュリティ専任技術者を確保しなくても，高いセキュリティを保つことが可能となる．

4） セキュリティ情報提供

セキュリティ製品ベンダーと連携し，最新のウィルスや脆弱性に関する情報，セキュリティパッチの情報をユーザに提供し対応を促す．また，発生したセキュリティインシデントの統計を定期的にレポートとして提出し，前述した脆弱性に関する情報と併せてユーザと共に対策やセキュリティ計画を作成する．ユーザ企業に設置されているファイアウォールや外部に公開されている Web サーバ，ネットワーク内に存在する各種サーバに対してソフトウエアスキャンやハッキングを試行して脆弱性検査を行い，結果をレポートとして提出するプロバイダも存在する．

図1にユニアデックスのマネージドセキュリティサービスの概念図を示す．なお，図中の統合ログ管理については，5章参照のこと．

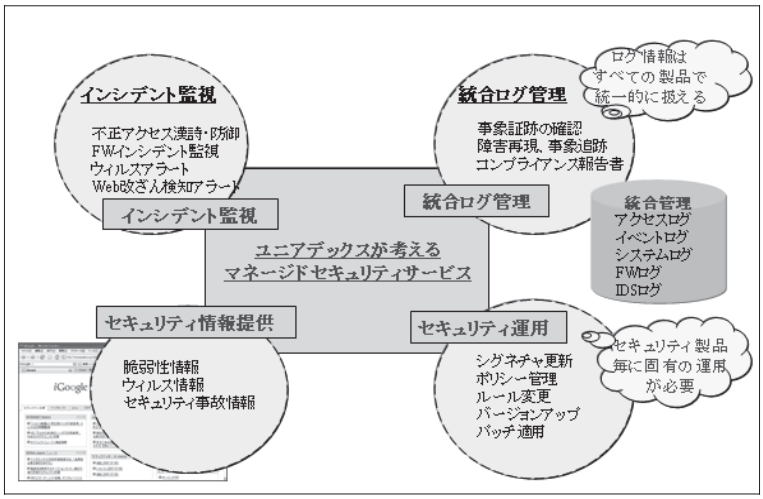

図1　ユニアデックスのマネージドセキュリティサービス概念図

3.　MSSの利点

MSSは情報セキュリティに関わる運用のアウトソーシングサービスであり，ユーザにとってはセキュリティ要員不足の解決や運用コストの低減を図ることができる．またそれだけに留まらず，以下のような高い付加価値を持ったサービスであり，ユーザはMSSを利用することで多くのメリットを享受することができる．

1)　情報セキュリティ専門スタッフによる対応

MSSPに所属する情報セキュリティ専門スタッフが日々ユーザのセキュリティ問題に対応している．MSSのユーザは自社内でそのような人員を内部調達する場合に比べて遥かに低コストで同等のサービスをMSSPから調達することができる．情報セキュリティ専門スタッフは常に最新の情報セキュリティ技術や事例に関する情報を取得しており高い技術レベルを保っているが，ユーザ企業内でセキュリティ要員を内部調達した場合，そのようなスタッフの教育はコストが掛かる上に非常に困難である．ユーザは情報セキュリティ要員を外部調達することで，内部リソースをより重要な事業活動に集中させることができるようになる．

またMSSPが提供する専門スタッフは，多くの場合同時に複数のユーザを担当している．これによりあるユーザ内で発生したセキュリティインシデントが，他のユーザで既出であった場合，MSSPはそのような事例をノウハウとして所持しているため，迅速な原因究明や事態の収拾が期待できる．

2)　付加価値の高いソリューションとセキュリティ技術

ファイアウォール，IDS，VPNや脆弱性診断ツールなどの情報セキュリティに関するソリューションや技術は，スキルの高いセキュリティ専門家によって管理・運用されており，ユーザのネットワーク監視を効果的に行っている．ユーザネットワーク内で侵入などのセキュリティインシデントが検知された場合，MSSPはまずアラームが正当なものかどうか判断し，セキュリティインシデントの可能性が高い場合はリモート監視で使用している接続回線

を使用してユーザに代わり対応することもある．

MSSP によっては，ファイアウォール，IDS 等のネットワークセキュリティ機器の再販あるいはレンタル/リースによってユーザに付加価値の高いセキュリティ機器を提供している．MSSP は製品プロバイダと提携し，新しい攻撃手法や脆弱性が見つかった際にはシグネチャやパターンファイルの更新などにより即時に対応できるような体制を取っており，未知のセキュリティインシデントに対しても迅速に対応できる．

4. MSS 利用時の考慮点

MSS は先に述べたように，ネットワークセキュリティに関わる運用や保守などのアウトソーシングサービスである．コストやリソースの問題から専任の情報セキュリティ要員を確保できないユーザ企業にとって，MSS は非常に有効なソリューションとなっている．しかしその反面，そのサービスの特性から利用者側で留意しなければならないリスクも存在するが，リスクを最小限に抑えることで MSS をより効果的に利用することができる．

本章では，MSS 利用時にユーザが考慮すべき点について解説する．

1） MSSP が所有するファシリティのセキュリティ

MSSP は，それぞれ独自の監視センター（SOC：セキュリティ・オペレーション・センター）を持ち，ユーザのネットワーク内にあるネットワーク機器やサーバを監視している．図 2 は一般的なユーザネットワークと SOC のネットワーク接続形態，図 3 は SOC のネットワークトポロジを表したものである．

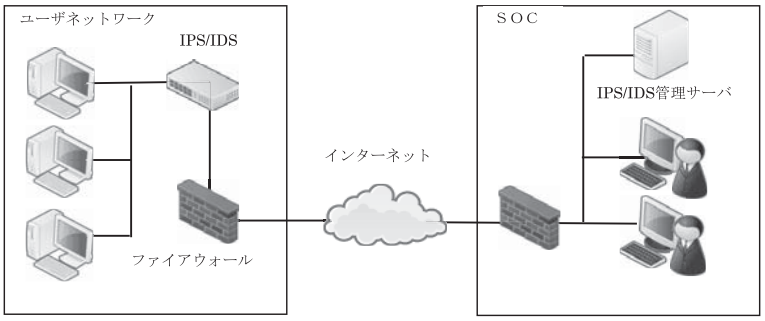

図 2　一般的な SOC のネットワーク接続形態

通常，SOC のファシリティは複数のユーザデータを共有しており，あるユーザの情報が他のユーザに流出する潜在的リスクを持つ．当然のことながら MSSP は SOC のセキュリティ対策を最高に保つよう対策を取っているが，ユーザ側でも，採用しようとしている MSSP が持つ SOC のセキュリティ対策について十分調査する必要がある．SOC でのセキュリティ対策の目安として，ISMS 認証の取得が挙げられる．ISMS とは，外部からの脅威への対策のみならず，内部からの脅威に対して，権限制限や操作ログ管理などの対策が十分なされているかなど技術的対策の他，入退室管理などの物理的対策，教育などの人的対策を含めたセキュリティマネジメントシステムである．

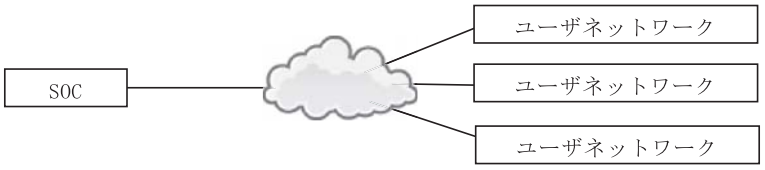

図 3　SOC のネットワークトポロジ

2)　MSSP への高い依存

情報セキュリティに関わる管理・監督を全て MSSP にアウトソースするユーザは，MSSP への依存度が高くなる．この場合，MSSP が提供するサービスの停止により，ユーザ本来の事業に影響を及ぼすこともあり得る．ユーザはこのリスクに対応すべく，契約前に SLA などでサービス稼働率や品質を十分調査し，事業継続の上で問題がないか確認しておく必要がある．また利用中の MSSP に何か問題が発生した場合に，自衛するか，他の MSSP にアウトソースし直せるよう予め方針や手続きを準備しておくべきである．

5.　ユニアデックスが提供する MSS

この章では，ユニアデックスが提供する MSS について具体的に紹介する．ユニアデックスでは，ネットワーク機器や業務アプリケーションサーバ等の各種サーバから出力されるログや IT データを統合管理し，セキュリティインシデント監視・運用やコンプライアンス対策，更にはリモート型の運用支援サービスの基盤インフラとして活用している．

5. 1　サービス概要

図 4 はユニアデックスが提供する MSS の概要を表したものである．ISMS 認証を取得した SOC は，高いセキュリティが保たれており（詳細は 6 章参照），24 時間 365 日の体制でユーザネットワークのセキュリティ監視・運用を行っている．高度なスキルを要するセキュリティ監

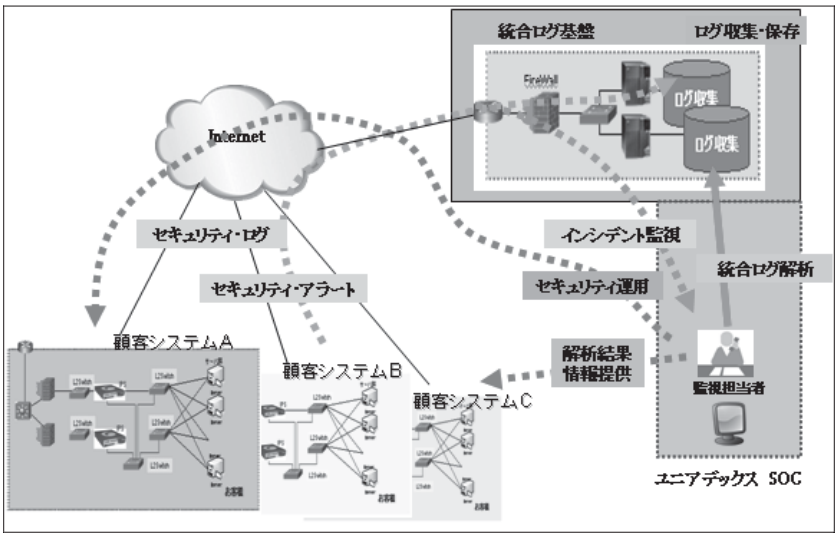

図 4　ユニアデックスが提供する MSS の概要

視・運用は，ユーザに代わってSOC内のセキュリティ監視要員が行い，検知したセキュリティインシデントやユーザ管理者からの問い合わせに対して迅速に対応することが可能である．ユーザネットワーク内にある管理・監視対象機器から出力されるログはSOC内にある統合ログサーバに収集され，セキュリティ監視要員によって分析・レポートされる．これらのセキュリティレポートをユーザ管理者はポータルサイトから参照することができる．ポータルサイトではセキュリティレポートの他，最新のウィルス情報や脆弱性情報，セキュリティ事故情報を提供している．

5. 2　不正アクセス監視・防御サービス

ここでは，ユニアデックスのSOCが提供するMSSの例として，IPS（Proventia）による不正アクセス監視防御サービス（図5）を紹介する．IPS（Proventia）とは，IBM社が提供する不正アクセス監視防御装置（IPS）である．当該サービスでは，ユーザネットワークにIPS（Proventia）を設置し，挙がってくるインシデントおよびログデータは，SOCに設置された専用の管理マネージャで管理している．将来的には，図4に示した統合ログ管理基盤にて統合管理する予定である．

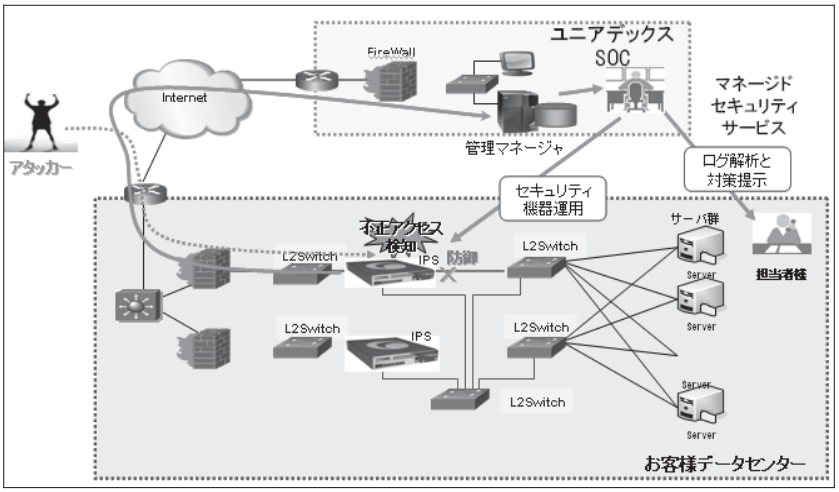

図5　ユニアデックスSOCが提供する不正アクセス監視防御サービス概念図

表1にユニアデックスのSOCが提供する不正アクセス監視防御サービスの内容を示す．なお，当該サービス提供に当たり，ユニアデックスのSOCでは，要件ヒアリング，設計，導入構築，セキュリティ監視，運用，更にはハードウェア/ソフトウェア保守までのすべてのフェーズを一貫してサポートしている．

表1　ユニアデックスの SOC が提供する不正アクセス監視防御サービス内容

基本サービス	IPS機器稼動監視 (死活監視)	お客様ネットワークに設置されているIPS機器の死活監視をセキュリティー監視センターより行います。
	通信状況監視・不正アクセス防御 (ブロック内容の通知)	IPSのシグネチャ及びポリシーに応じて、攻撃や不正アクセスを防御します。ブロックした通信内容をメールにて報告します
	シグネチャの更新、サイトポリシー管理など	対象ネットワーク内に設置されたIPS機器のシグネチャ更新、マスターポリシーの提供、サイト・セキュリティ・ポリシー管理さらに必要に応じてポリシーチューニングやソフトウェア更新を行ないます。
	緊急ポリシーチューニング	誤検知により防御された通信と確認された場合、お客様の依頼により、対象ネットワーク内に設置されたIPS機器に対して緊急ポリシーチューニングを実施し、当該通信に関する防御の解除を行います。
	月次レポート	基本サービスで作成されるレポートをもとに当セキュリティ監視センターにて収集した情報を加味した詳細版の月次レポートを提供します。
	技術質問に対する回答	報告内容に関するお問い合わせを電子メールにて受付・回答します。

5.3　統合ログ管理基盤

これまでログは，システムが正常に稼働しているかどうかを確認するための位置付けであった．かつては IT システムで発生する問題の多くは，ハードウエアやソフトウエアの障害であり，ログもシステム管理者が障害の検知や調査の目的で使うことが殆どであった．ところが，個人情報保護法の施行や，Winny などのファイル共有ソフトに起因する情報漏えいの多発により，情報セキュリティの観点からログの活用が注目されるようになった．例えば，社内のファイルサーバに置かれた重要な機密情報ファイルが漏えいした疑いがある場合，情報セキュリティ担当部門はファイルサーバへのアクセスログや PC クライアントの操作ログ，さらにはオフィスへの入退室ログなどを横断的に調査する必要がある．また，「日本版 SOX 法」や「e-文書法」などにより，ログは内部統制やコンプライアンスにおいても非常に重要な役割を果たすようになってきている．

このような背景からユニアデックスでは，ネットワーク機器や業務アプリケーションサーバ等の各種サーバから出力されるログや IT データを統合管理し，情報セキュリティやコンプライアンス対策，更にはリモート型の運用支援サービスの基盤インフラとして活用している．この統合ログ管理基盤には，以下のような機能的な特徴がある．

1)　一元管理

様々なフォーマットで出力される各システムのログを，フォーマットを問わず一元管理することが可能である．それにより，一括検索が可能になり，一見関連性のないログファイル間の相関検索で問題解決に繋がる可能性が高まる．

2)　生ログの保存

各システムが出力するログデータは，加工せず出力されたままの状態で保存している．加工されていない状態の生ログは非常に大きなものとなり，そのままでは視認性が良くないため，フィルタをかけて閲覧することになるが，フォレンジックやコンプライアンスという観点では証跡として原本性が求められているため，保存時にフィルタをかける等の処理はせずに圧縮保存される．

3） 高速検索

生ログの状態で各システムのログを保存していくと，データ量が非常に多くなり，データの取り出しに時間がかかってしまう恐れがあるが，ユニアデックスが提供する統合ログ管理サービスでは，保存時にインデックスを付与することにより，生ログの状態でも高速検索が可能となっている．

4） 横串（相関）検索・集計

ログを統合管理することにより，それまでのシステムごと，サーバごとの管理では困難だった横断的な検索や集計が可能である．例えば，重要なデータが持ち出されたことが発覚した場合に，PC クライアントの操作ログ，ファイルサーバのログ，メールサーバのログなどを横串（相関）検索して，迅速な対応が可能である．

5. 4　統合ログ管理基盤で扱うログデータについて

この節では，ユニアデックスの統合ログ管理基盤についてもう少し掘り下げて説明する．まず，当管理基盤では，監視対象 IT インフラの状況（例えばシステムの構成やユーザの利用状況など）を知るために必要なすべてのログデータ（IT データ）を扱うことができる．つまり，構成情報，変更イベント情報，診断コマンドの処理結果等も含まれ，ネットワークセキュリティやコンプライアンスを中心とする従来のログデータの概念を少し拡張したものとなる．具体的には，以下に挙げるログファイルが含まれる（図 6）．

・Syslog，WMI 等

Unix，Linux の syslog，および Windows の WMI などの OS ログには，使用者のログイン情報や実行コマンド，タイムスタンプなどが記録される．DNS，DHCP，その他のネットワークサービスが出力するログには，IP アドレスやホスト名やドメイン名と IP アドレスとの対応などが記録される．ルータ，スイッチ，ネットワーク機器の syslog には，ネットワーク接続の状態とコンポーネント故障情報が記録される．

・OS メトリックス，ステータス，診断コマンド

Unix や Linux では ps や iostat，Windows では perform のようなユーティリティを使って，CPU とメモリの使用率やステータス情報等を取得でき，故障対応や傾向分析，セキュリティインシデント調査に重要なデータソースである．

・構成ファイル

インフラの設定を知るには最新の構成情報が必要である．構成ファイルが予定外に変更された場合は，攻撃者によるバックドア等の脅威も考慮する必要がある．

・アプリケーションログ

社内開発のアプリケーションは，通常ミドルウェアに実装されているロギングサービスを利用してローカルログファイルにログを書き込む．これらのログファイルはアプリケーションのデバッグや性能監視にも活用される．

・Web アクセスログ

Web サーバで処理されるすべてのリクエストに関し，クライアント IP，URL 情報，リクエストの成功，失敗等が記録される．これらはユーザから問い合わせのあった問題を調べる際，調査の手始めとしても重要なデータソースである．

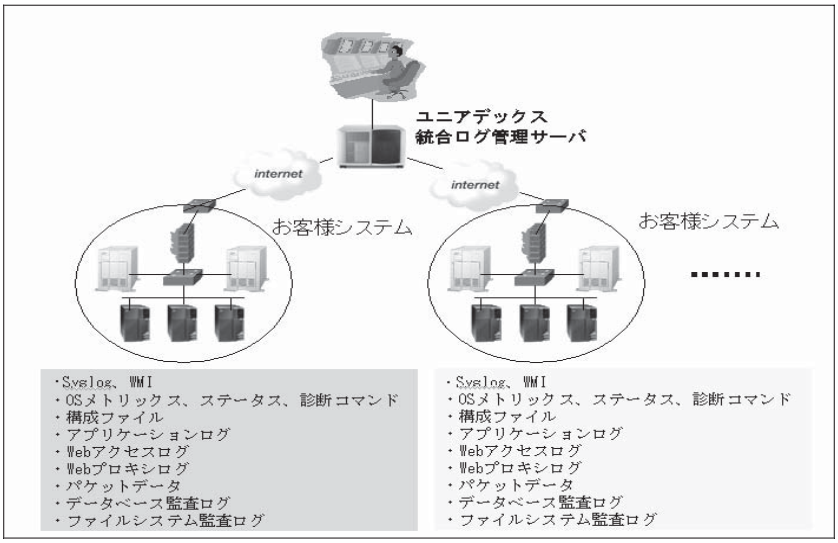

図 6　統合ログ管理基盤で扱うログデータについて

・Web プロキシログ

通常企業システムでは，ユーザの Web リクエストはすべてプロキシを介して処理されるため，データ漏えいの調査と監視を効率的に行うためにもプロキシログは重要なデータソースである．

・パケットデータ

tcpdump や tcpflow のようなツールは，ネットワークパケットデータを情報として生成することができ，ネットワークの障害分析に重要なデータソースである．

・データベース監査ログと監査テーブル

データベースに誰がアクセスしたか，いつ何のデータを変更したかを知るために重要なデータソースである．

・ファイルシステム監査ログ

データ漏えいを監視するにあたって重要なデータソースである．

このようにユニアデックスの統合ログ管理基盤では，サーバやネットワーク機器から syslog を直接受け取り，WMI ポーリングの結果を取り込み，ファイルシステムや Windows レジストリの変更を監視する．また，スクリプトで定期的にシステムのパフォーマンスデータを取得するなど，様々な手段で様々な種類のログデータを取り込むことができる．各ログファイルにはインデックスが付与され，高速な検索が可能である．オリジナルのログデータとインデックスデータは，監査と認証に必要なデータと共に圧縮され，マルチテナントを扱えるよう階層化され蓄積される．また，セキュリティの確保は十分に考慮されており，すべてのトランザクションは認証を受け，操作者に応じてロール管理されている．

5. 5　統合ログ管理基盤の活用について

5. 4 節で見てきた通り，ユニアデックスの統合ログ管理基盤で一元管理されるデータは多種多様であり，システム全体の運用に係わる証跡データのほぼ全域をカバーしているため，これ

ら諸データを整理編集することで，顧客の運用環境の「見える化」ならびに「コンプライアンスレポート」に対応したサービスを提供できる．また，セキュリティ監視サービスでは，ファイアウォールやIPS/IDS，WAF，統合UTMなどの既存セキュリティ機器の機種毎の監視手法の違いを特に意識する必要なく，セキュリティログによる一元監視が可能となるため，セキュリティ機器単独のログ監視に加え，Proxyサーバ，Webサーバ，データベースサーバなどのアクセスログと相関検索することで，不正なアクセスが検知された場合の影響範囲の特定も容易になる．また，エラーログや操作ログ，各種Syslog，構成ファイル，パラメタファイルなどと相関検索することで，障害原因の特定も容易になる．

このように，ユニアデックスが提供するMSSを含めたITマネジメントサービスでは，安全性，利便性の確保，耐障害性，属人性の低減，ファーストコンタクトから障害特定，障害対応までの所要時間の短縮等を実現させ，より高品質でプロアクティブな運用サービスを顧客に提供することを目指している．

6. ITマネジメントサービス環境のセキュリティ対策

これまでは，ユニアデックスがユーザに提供するサービスについて述べてきたが，この章では，MSSも含めたユニアデックスのITマネジメントサービス基盤のセキュリティ対策について述べる．ITマネジメントサービスは，ユニアデックスの監視センターからユーザ情報システムにリモートで接続してサービスを提供している．他のMSSPと同様，監視センター側にサービスに必要なユーザ情報などを保持しており，場合によってはユーザの重要なデータをインターネットを経由して取得することもある．このような環境下では外部からの脅威，内部からの脅威に対して十分なセキュリティ対策を講じる必要がある．図7はユニアデックスが実施しているセキュリティ対策を表したものである．

6.1 外部からの脅威への対策

ITマネジメントサービスの対象となるユーザの情報システムと監視センター間のネットワークを流れるデータの「盗聴」や「改ざん」，監視センターに対する悪意のある第三者からの攻撃に備えた対策が必要となる．

1） 安全な通信の確保

データの盗聴や改ざんなどの不正アクセスを防止し安全な通信を可能にするために，監視センターとユーザ情報システム間はVPN接続により通信パケットを暗号化する．

2） 不正アクセス・不正侵入防止対策

ファイアウォールは外部から許可しているネットワークサービス以外の不正アクセスを防御する．しかし許可しているサービスに対し悪意あるコードが紛れていたとしても，通常のアクセスとして許可してしまう．これを監視し不正侵入や怪しい振る舞いを検出/遮断するためにIPS/IDS装置を設置する．

6.2 内部からの脅威への対策

監視センターには，監視に利用するユーザシステム環境の情報など，重要なデータが保持されている．悪意を持ったシステム利用者による情報窃取では，外部からの攻撃に比べて重要な情報を窃取される可能性が高い．従って，監視センター内についても十分なセキュリティ対策

が必要である．

1)　アクセス制御

監視センターの監視サーバ，リモート運用端末は，特定の担当者のみのアクセスしか許可しないようにする必要がある．しかし，ID・パスワードを利用した認証には，セキュリティ上の盲点がある．ID・パスワードが盗まれれば，本人以外でもアクセスが可能となってしまう．さらに，PC の操作履歴を収集してもログに残されたユーザ名と本人が一致しなければ，追跡調査してもユーザを特定することは困難である．そこでリモート運用端末の認証には，社員証でもある IC カードを利用したソリューションによって「厳格な本人認証」と「なりすましの防止」を実現している．

2)　操作ログの取得

リモート運用端末からの操作を記録することで，情報漏えいに繋がる不正行為の追跡が可能となる．また，操作員にログが記録されていると認識させることで不正行為の抑止効果もある．

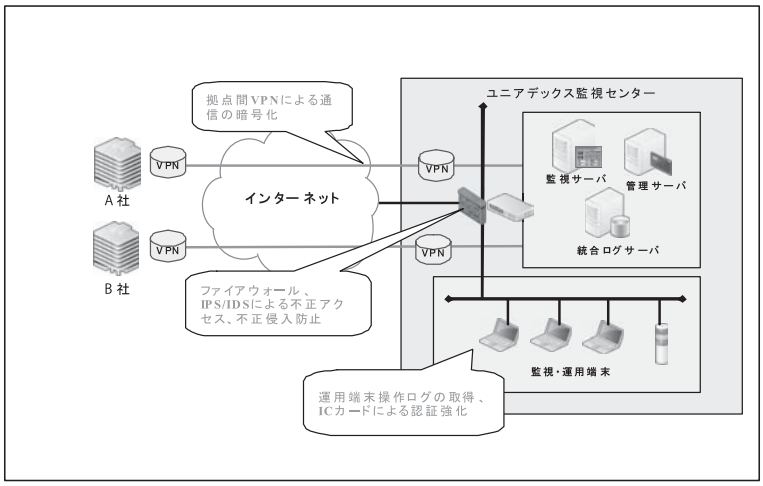

図7　ユニアデックスの IT マネジメントサービス基盤のセキュリティ対策

7. お わ り に

本稿では，マネージドセキュリティサービス（MSS）の背景や動向，特徴とともに，ユニアデックスが提供する MSS の概要とそれを提供するためのリモート運用基盤について紹介した．また，ユニアデックスが提供する MSS を含めた IT マネジメントサービス基盤のセキュリティ対策についても言及した．また本稿で紹介した MSS を採用することにより，ユーザのセキュリティ運用の問題や課題に対して有効な手段を提供できることを示した．

内部統制や J-SOX 法など，いわゆる「企業の見える化」の対処策の一つとして，また昨今の経済状況を反映した SaaS ビジネスなどに代表されるアウトソーシングの潮流から，MSS が今後さらに重要なサービスになっていくことが予想される．

参考文献 ［1］ Julia Allen, Derek Gabbard, Christopher May,「Outsourcing Managed Security Services」, Carnegie Mellon Software Engineering Institute, 2003. 1

※ ユニアデックスでは，通信技術が今日の情報システムにとって重要な位置づけであることから，商品名に‘ICT’（Information Communication Technology：情報通信技術）と表記している．ただし本論文では，より一般的な表現である‘IT’に統一して表記した．

執筆者紹介 武 井 英 直（Toshitada Takei）

1999年日本ユニシス(株)入社．2001年ユニアデックス(株)転籍．ネットワーク関連のプロダクト開発業務に従事．現在は運用基盤サービス部に所属し，ネットワークセキュリティに関する監視および保守業務を担当．

入 貝 健 介（Kensuke Irigai）

1980年日本ユニバック(株)入社．2001年ユニアデックス(株)転籍．汎用機のオペレーティングシステムの受入保守，日本語ソフトウェアの開発保守，性能評価関連，セキュリティ関連製品の受入保守および利用技術サービスのマネジメント業務に従事．現在は運用基盤サービス部に所属．