■ Network Security Platform 導入事例 ―

NTTコミュニケーションズ株式会社

NTTコミュニケーションズ株式会社

企業プロファイル

日本最大級の長距離通信およびICTサービス企業。従業員数8150人、年商1兆334億円。1999年の設立以来「グローバル化」を積極的に推進。国内16拠点の他、欧米やアジアなど全世界73都市に拠点を有し、サービス提供エリアは150ヶ国を超える。

「ビジョン2015」としてアジアでの現在の強みをさらに強化し、世界中のお客さまにとって最適なパートナーとして選ばれる、真のリーディンググローバルプレーヤーとなることを目標にしている。

「世界規模のセキュリティサービス、『Bizセキュリティ　グローバルマネジメント』を展開しています。Network Security Platformは、IPSサービスのための機器として活用しています」

グローバルセキュリティサービスのIPS機器としてNetwork Security Platformを活用

― *NTTコミュニケーションズではNetwork Security Platform（以下 NSP）をどう使っていますか。*

NTTコミュニケーションズでは、「Bizセキュリティ グローバルマネジメント（以下Bizセキュリティ グローバル）」というセキュリティサービスのメニューの一つである、IPS（ネットワーク不正コード検出・防止）を提供するためのアプライアンスとして、NSPを活用しています。

Bizセキュリティ グローバルは、NTTコミュニケーションズのセキュリティ技術者チームにより構成される、「セキュリティオペレーションセンター（以下 SOC）」により提供されます[1]。名称のとおり「グローバル（世界規模）」を基本コンセプトに据えたサービスです。

1. 「Bizセキュリティ　グローバルマネジメント」は、お客さまシステムにセキュリティ機器を導入し、セキュリティ脅威からのシステム保護やインシデント発生時のサポートを行うサービスです。ホスティングサービス「Bizホスティング エンタープライズ」や国内外のデータセンターサービスのセキュリティオプションとして利用が可能です。

基本コンセプトは、「グローバルシームレスマネジメント」

― 「Bizセキュリティ グローバル」の基本コンセプトを教えてください。

いくつかのキーワードを使って、根本から説明いたします。

キーワード1.

「ネットワークセキュリティでは国内・国外という区分けは意味がない（最初からグローバルに構想するべき）」

世界でビジネスを行う企業では、ネットワークも世界規模です。Bizセキュリティ グローバルでは、サービス体系に「国内向け」「国外向け」という境界を設けていません。ネットワーク管理において、国内・国外という境界は無意味だと考えるからです。「グローバルなサービス提供がデフォルトであり、国内向けサービスはその部分集合」と見なしています。

キーワード2.

「一箇所のセキュリティ脆弱性が、全体に悪影響を与える（被害もグローバルになる）」

グローバルな企業ネットワーク環境で、国境を越えた企業内通信が行われるということは、ウイルスなどのセキュリティ脅威が発生した時、それがグローバルに拡散しうることを意味しています。どこかの国のどれかのパソコンで、うっかりミス（あるいは悪意）により、ワームなどセキュリティ脅威の侵入が発生したとき、それはグローバルな企業ネットワーク全体に広がりうるのです。

キーワード3.

「ネットワーク全体を一元的に把握する仕組みが必要」

ここまで「ネットワークは本質的にグローバルなもの」「それだけに一箇所から脅威が入り込むと、被害がグローバルに拡散しうる」と述べました。この状況に対処するには、ネットワーク全体を、一括して管理、把握し、脅威が起きたときには素早く対処する仕組みが必要になります。この「管理・把握・対処」の役割をアウトソーシングの形で担うのがNTTコミュニケーションズのSOCとなります。

「グローバルな企業ネットワークでは様々なセキュリティ問題が生じます」

ITマネジメントサービス事業部
NWマネジメントサービス部
セキュリティオペレーション部門
担当課長
竹内文孝 氏

Bizセキュリティ グローバルのカバレージ

・世界3極でのグローバル標準SOC
・各地域のローカルSOCが連携・統合した体制
（10ヶ国、22拠点、300名を超えるセキュリティエンジニア体制）

McAfee

グローバルな企業ネットワークでのIPSの役割

― 「Bizセキュリティ グローバル」のコンセプトの中での、IPSの役割、位置づけについて教えてください。

IPSは、エンドポイントの対策や、ファイアウォールなどアクセス制御などが有する弱点を補完する手法であると考えています。まず「エンドポイントの対策」ですが、ネットワーク内部への脅威の侵入を防ぐために、例えば、「ウイルス定義ファイルやセキュリティパッチを常に最新にする」といった「エンドポイントの保護を強化する」手段があります。

（エンドポイント強化 vs IPS）

エンドポイントが世界中に大量散在しているグローバルな企業ネットワークにおいては、全エンドポイントのウイルス定義ファイルやセキュリティパッチを、常に最新の状態に保つのは大変な作業です。また、未知のウイルスや亜種については、エンドポイントだけでは防ぐことができませんし、先に述べたとおり、セキュリティ脅威がそこからネットワーク全てに拡散する恐れがあります。

この問題はIPSにより解決可能です。IPSは、ネットワークの要所でパケットを集中監視します。したがって万が一、不完全なエンドポイントからセキュリティ脅威が発生し、拡散しようとしたとしても、それをパケットレベルで検知し、食い止めることができるからです。

（ファイアウォールによるアクセス制御 vs IPS）

ファイアウォールの場合、ある個人（または部門）が、ネットワークの特定エリアにアクセスして良いかいけないかを、主に職責や職位などに基づいてスタティックに定義し、その定義に基づいてアクセス制御を行います。いわば「身分証による入室許可（不可）」のような手法ですが、このやり方の場合、「身元の確かさ」は分かっても「危険物を所持しているかどうか」は確かめられません。最悪の場合は、「身元の確かな人が、セキュリティ脅威と一緒に、ネットワークの重要エリアにアクセスする」という事態が発生し得ます。

この問題に対してもIPSは有効です。IPSのパケット内容検査は、まさに「所持品検査」そのものだからです。

以上、グローバルな企業ネットワークで十全なセキュリティを根本確保するために、IPSが有効であると考える所以です。

「IPSは従来のセキュリティ対策の弱点を解決できる手法です」

ITマネジメントサービス事業部
NWマネジメントサービス部
セキュリティオペレーション部門
主査
山崎秀樹 氏

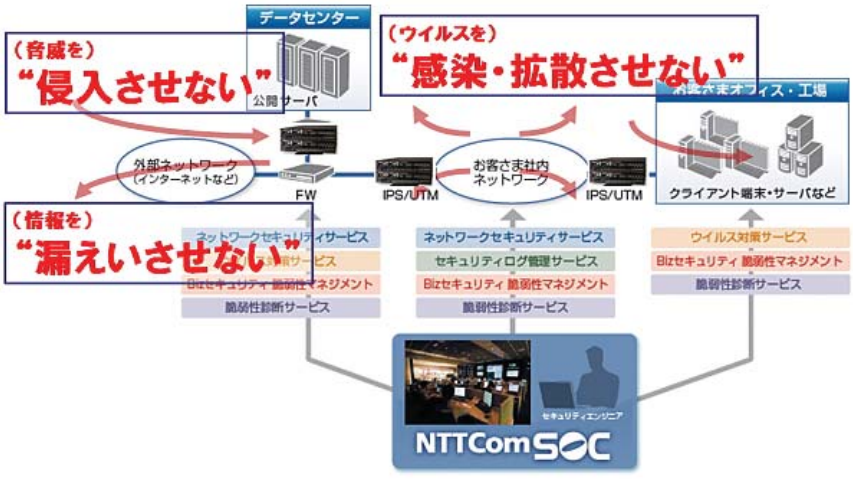
NSPへの評価 ～ 性能評価試験で好スコア

― NTTコミュニケーションズでのNSPへの評価を教えてください。

セキュリティサービスをユーザーに提供する立場としてNTTコミュニケーションズから見た、NSPへの評価は、次のとおりです。

1. IPSとしての基礎性能が（他製品と比べても）優れている

NSPは、セキュリティ脅威の検知能力、広帯域ネットワークでの使用に耐えうる可用性と安定性に優れています。なお弊社ではNSPの他に数種類のIPSを活用しています。NSPの導入にあたり、社内の試験環境で、可用性、安定性についての性能評価試験を行いましたが、NSPは他のIPSに比べても、特に優秀な試験成績を収めました。



ネットワーク型IPSの役割

1. 企業内の拠点間にて、パケット監視によるウイルスの感染・拡散を防止します。
2. 外部ネットワークとの境界に配置し、外部からの不正アクセス・脅威を排除します。
3. ウイルス感染、不正アクセスを抑制することで、情報漏えいの原因を排除します。

McAfee

2. グローバルな知名度、信頼性、契約及びデリバリーの体制

マカフィーは、1). グローバルな知名度(信頼性)があり、2). また、世界各地にサービス拠点を有しており、3). 世界規模での包括業務契約とデリバリーを可能にする基盤を持っているので、顧客に薦めやすい製品であるといえます。

3. 運用が容易であること

NSPの管理画面(NSM:Network Security Manager)は、「(技術者にとって)知りたい情報がシンプルかつ的確に探せる」インターフェースである点が評価できます。

4. ログが的確である。

SOCの技術者が、セキュリティ脅威(あるいはその兆候)がネットワークの中にないかどうかを見極める際に、その判断の根拠となるのが、IPSのログです。NSPのログは多すぎず少なすぎず「的を得て確かに分かる」内容である点を高く評価しています。

5. 優れたセキュリティ研究機関を有している

セキュリティ研究所、Global Threat Intelligenceの情報、知見は、SOCにとっても重要な参考資料となります。

ログ分析に基づく継続的なチューニングが重要

― これからIPSを導入しようとしている企業にアドバイスなどあればお願いいたします。

先ほどIPSの特色は「危険物の所持を見破れることだ」と述べましたが、IPSをフル活用するには、その「危険物」の定義が重要になります。

ネットワークの中で何がセキュリティ上の脅威となりうるかは、ネットワーク環境およびその外部環境が変わるにつれ、「基準それ自体が刻一刻と変わる」ので、それに合わせて、常にIPSのチューニングや設定内容を更新し続ける必要があります。そのチューニング判断の原資となるのがIPSのログです。したがって、IPSをフル活用するにはログの解読・分析が必須になります。

今後の期待

― マカフィーへの今後の期待をお聞かせください。

今回、NSPという優れたIPSを採用したことで、NTTコミュニケーションズのグローバルなセキュリティサービスの提供力はさらに向上しました。マカフィーには今後も優れた技術と基礎研究力とを継続提供していただき、NTTコミュニケーションズのセキュリティサービス品質の向上を支援していただくことを希望します。これからもよろしくお願いします。

「マカフィーにはグローバルなサービスを期待しています」

ITマネジメントサービス事業部
NWマネジメントサービス部
セキュリティオペレーション部門
担当課長
生嶋大也 氏

取材日時 2011年4月

McAfee マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

東京本社　〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL:03-5428-1100(代) FAX:03-5428-1480

西日本支店　〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL:06-6344-1511(代) FAX:06-6344-1517

名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL:052-954-9551(代) FAX:052-954-9552

福岡営業所　〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL:092-287-9674(代) FAX:092-287-9675

MCACS-NTT-1106-MC