

全社的サーバーセキュリティ対策と外部サービス

津田邦康

ウイルスやワームによるコンピュータシステムへの攻撃、個人情報漏洩などが多発している。これら情報セキュリティに関する事件（セキュリティインシデント）は毎年増え続けており、企業はこれらの脅威に適切に対応することが必須となっている。全社的なサーバーセキュリティ対策では、セキュリティホール（弱点）への対応、セキュリティ設定不備の修正、ID・パスワードの管理が重要であるが、そのためには多くの煩雑な作業が必要になる。そこで、サーバー管理者をサポートする外部のセキュリティサービスを利用することが有効な選択肢となる。

増え続けるセキュリティインシデント

2003年は、セキュリティホールを狙った「SQLスラマー」「MSブラスター」といったワーム（自己増殖を繰り返しながら破壊活動を行うウイルス）が大流行した。

MSブラスターは、マイクロソフト社がセキュリティホールを公開した25日後に発生し、猛威をふるった。このワームは、ノートパソコンなど内部ネットワークからの感染被害が多数報告されてお

り、企業のセキュリティ対策の期間や内容について見直しを迫るものとなった。

また、ユーザーIDやパスワードの盗用、セキュリティホールを狙った不正アクセス事件も数多く報告された。

統計情報によれば、2003年のセキュリティホールの報告件数は、前年に比べるとやや減少した。しかし、1日当たり10件を超える数のセキュリティホールが報告されており、セキュリティインシデ

ントの件数は急激に増加する傾向にある（表1）。

サーバーに求められるセキュリティ対策

ウイルスやワームによる攻撃や不正アクセスを防御するためのセキュリティ対策としては、セキュリティホールへの対応、セキュリティ設定不備の修正、ID・パスワードの管理が重要になる。これらの対策を、企業で使用しているすべてのサーバーに対して、どのように行えばよいだろうか。

まず、セキュリティホールについては以下の対応が必要になる。

- すべてのサーバーについて、使用している製品のバージョン、セキュリティパッチ（修正プログラム）の情報を整理する
- 各サーバーの役割や保持しているデータなどを考慮して、重要度を定める
- セキュリティホールの内容を理解し、影響を判断する

また、セキュリティ設定については、OS（基本ソフト）や各アプリケーション製品のセキュリティ項目を調査して正しく設定すること、フォルダーおよびファイル単位のアクセス制限を適切に行う

表1 セキュリティホール、セキュリティインシデントの報告件数

	2001年	2002年	2003年
セキュリティホール	2,437	4,129	3,784
セキュリティインシデント	52,658	82,094	137,529

出所) 米国CERT/CC (コンピュータ緊急対応センター) の統計より作成

ことが必要である。

IDとパスワードの管理では、パスワードに使用する文字数や種類、変更サイクルなどのルールを定め、ルールが守られているかを適時検査する必要がある。

サーバーセキュリティ対策における課題

上述したサーバーのセキュリティ対策を行うためには、次のような煩雑な作業が必要になる。

- 毎日のように報告される、膨大な数のセキュリティホール情報の継続的な収集
- セキュリティの設定やセキュリティホールの内容を理解するための、広範かつ高度な、システムおよびセキュリティに関する知識
- パスワード変更の管理や、人事異動や退職により交代した管理者のアカウントの管理を継続的に監査する仕組み

また、大規模なウェブサイトや全社規模でのサーバーのセキュリティ管理を行うためには、以下のような課題にも対応していく必要がある。

- サーバー情報（使用製品のバージョン、セキュリティパッチ情報）の収集・管理

- サーバー管理者情報（連絡先）の管理、連絡体制の整備
- セキュリティ問題が発生したときの対応の管理

ウェブサイト管理者やサーバー管理者が、通常の運用管理業務に加えて、上記のようなセキュリティ対策を独自に行うためには高度のスキルが必要であり、負荷も大きい。

セキュリティサービスの利用

以上のような状況から、サーバー管理者をサポートするためのセキュリティサービスが求められてきている。

NRIセキュアテクノロジーズでは、以下のような機能を有するサーバーセキュリティ管理サービス「SecureCube/Site Security Check（セキュアキューブ・サイトセキュリティチェック）」を提供している。

サーバーセキュリティ情報管理機能

サーバーで使用しているOSやウェブサーバーなどの製品情報を管理し、それらの製品のセキュリティに問題がないか診断を行う。

セキュリティホール対応状況管理機能

各サーバーで使用している製品

にセキュリティホール情報が報告されると、自動的にメールで管理者に通知を行う。全社、ウェブサイト、サーバー単位でセキュリティホールへの対応状況が一覧可能であり、全社的なセキュリティ対応管理をサポートする。また、セキュリティホールの危険度に応じて対応予定期間を設定することが可能であり、対応予定期間を過ぎても対応が行われていないサーバーの管理者にはメールで通知を行う。

サーバーセキュリティ状態監視機能

サーバー管理用ソフトを導入することで、バージョンおよびパッチ情報の自動収集機能、ファイル改ざん検知機能が提供される。

包括的で実効あるサーバーセキュリティ対策を行うために、このような外部サービスの利用は有効な選択肢となるだろう。

『ITソリューションフロンティア』
2004年4月号より転載

津田邦康（つだくにやす）
NRIセキュアテクノロジーズ（株）
事業開発部上級セキュリティエンジニア