

# eXsenjuのサーバーセキュリティ

情報システムの運用は、リソース管理、オペレーション管理、アクセス管理、セキュリティ管理（パッチ管理）、バックアップ管理など、多岐にわたる。日々10件以上のセキュリティホールが発見されている昨今、セキュリティを確保するためのシステム運用への負荷は高まる一方である。こうしたセキュリティ管理の状況を踏まえ、解決策の一端を紹介する。

## システム運用と自動化の限界

システム運用には、さまざまな役割の人間（以後、ロール）が必要となる。テープ交換運用や24時間監視を行うオペレーター、システム全体を管理するシステム管理者、ビジネスのフィジビリティを保障する統括マネージャーなどである。

業務システム化の目的を考えるならば、システム運用もすべて自動化されるのが理想であるが、現実にはそれは困難である。システム運用を自動化するツールや機器は存在するものの、それらによって自動化されるのは一部分に過ぎない。よって、自動化されない部分について、上述のようなロールが存在している。

システム運用上の項目は極力自動化する、

自動化が不可能な項目は極力オペレーターに対応させる、オペレーターで対応できない項目はシステム管理者が行う、というのが現在の実態と言えよう。

セキュリティの管理/運用について言えば、その複雑さからオペレーターではなく、システム管理者自らが行っているのが現状である。こうした状況のなか、これらを簡略化したいというニーズが強まってきている。

なかでも、セキュリティパッチ運用は重大な判断事項が多く、運用頻度も高いため、システム管理者の簡略化への期待が最も大きい。以下、この問題について検証していく。

## セキュリティ管理/運用の難しさ

一般的なセキュリティパッチ運用は、セキュリティ情報の収集、セキュリティ情報の内容把握、適用範囲の情報収集、適用範囲の判断（システムへの影響把握）、という流れで行われる。そして、これらは、ベンダーからセキュリティパッチが公開されるたびに、システム管理者自らが行っている。

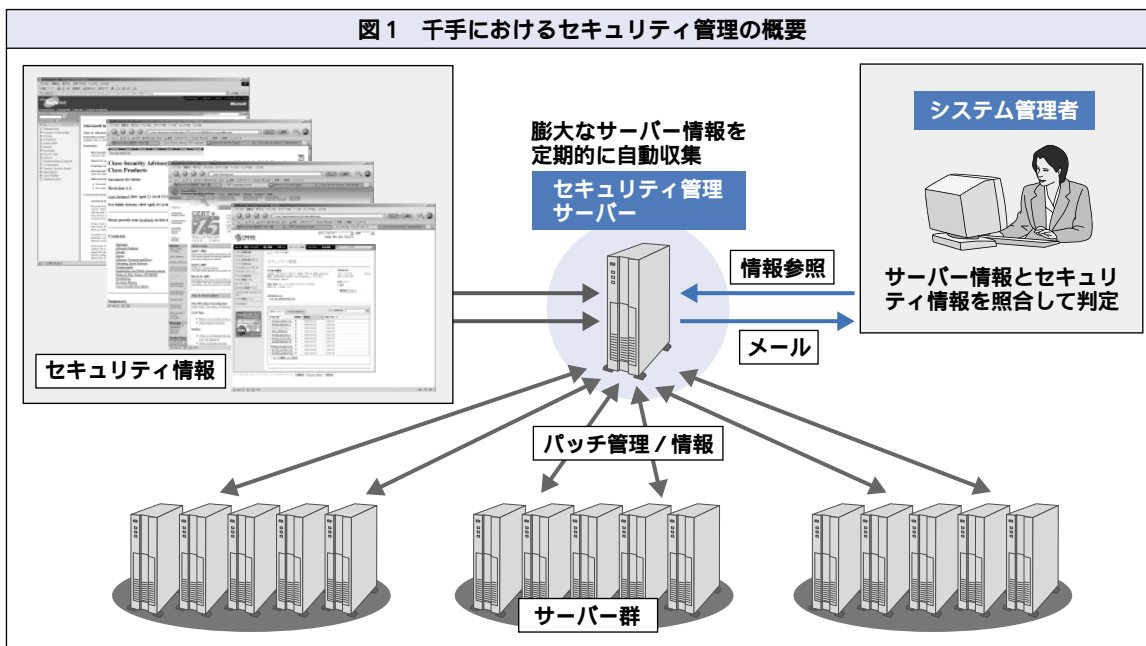
セキュリティパッチを自動的に適用するウイルス対策ソフトウェアは存在する。しかし、基幹系の業務システムなどでは、パッチがアプリケーションに影響を及ぼす危険があるため、導入できないのである。

さらに、上記の一般的な流れで運用すると、膨大なセキュリティホール情報の継続的な収集、高度化するセキュリティについての広範かつ高度な知識収集、膨大なサーバー群を含むシステム情報の把握、サーバーのシステム情報とセキュリティホール情報のマッチング、緊急度が高いセキュリ

NRIデータサービス  
 アウトソーシング営業本部  
 千手サービス事業部  
 副主任システムエンジニア  
**大歳 岳**（おとしがく）  
 専門は運用基盤システムの設計構築



図1 千手におけるセキュリティ管理の概要



ティホールの常時監視がシステム管理者に求められることになるため、その運用負荷がきわめて大きくなってしまふ。

### セキュリティ管理を運用に乗せる

しかし、こうした運用負荷を軽減することができないわけではない。そのためのツールとして、NRIデータサービスでは、「eXsenju」のサブシステム、「千手/セキュリティ管理」を提供しているが、その基本的な考え方は次のとおりである。

緊急度の高いセキュリティホールは常時監視されていることが望ましい。このため、セキュリティホール情報/パッチ情報のなかで、緊急度が高いものを自動的に入手すると同時に、対象となるシステムの情報も自動的に入

手する。そしてこれらをマッチングした上で適用範囲を自動的に算出し、アラートを発信する。これにより、システム管理者は、サーバー情報とセキュリティ情報を照合して判定する部分のみを行えばよいこととなり、大幅な負荷軽減が図れる、というわけである。

なお、これらを自動化するエンジンには、システムセキュリティを専門とするNRIセキュアテクノロジーズ「SecureCube/Site Security Check」が採用されており、「eXsenju」サーバー監視や「eXsenju」ジョブ管理と統合されているため、簡略化のためサブシステムどうしが不整合をきたさぬよう、配慮されている。

こうしたセキュリティ管理ツールの有効活用は、今後、システム運用の簡略化、自動化を推進する重要なカギを握るであろう。 ■