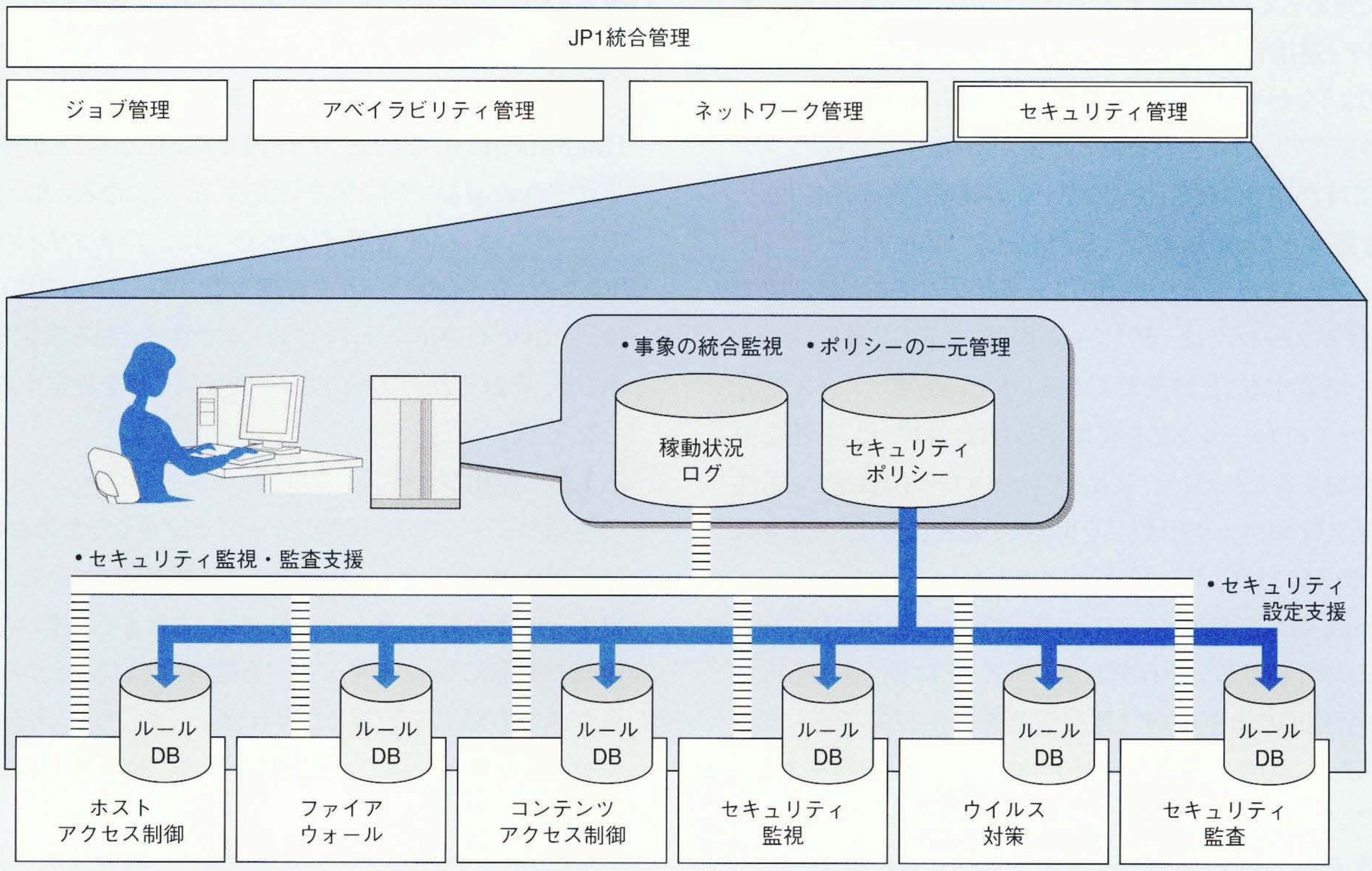
# eビジネスの信頼性を高めるセキュリティ管理ソリューション

## Security Management Solutions for Reliable e-Busineses

長田 清人 *Kiyoto Osada*　萱島　信 *Makoto Kayashima*
妹尾　徹 *Tôru Senoo*　服部 泰明 *Yasuaki Hattori*




注：略語説明
DB（Database）

**JP1統合セキュリティ管理“JP1/Security Integrated Manager”**※）

JP1/Security Integrated Managerは，各種セキュリティ製品との連携を深め，一元的な統合監視からセキュリティ監査の支援までを実現する。

企業システムを中心に，オープンなネットワークを利用したe（Electronic）ビジネスが飛躍的に拡大している。ここで利用される情報資産を保護するのがセキュリティであり，システムの運用管理では，さまざまなセキュリティ技術が必要となってきている。

これまでは，ファイアウォール，ウイルス対策といった個々のセキュリティ技術を導入して運用を進めてきた。しかし，システムの規模が大きくなるに従い，各部門のセキュリティレベルのばらつきをなくし，システム全体のセキュリティを統一的に管理することが困難になってきており，これがシステムの運用管理面で大きな課題となっている。

JP1統合セキュリティ管理は，この課題を解決し，安全な情報システムを構築することができる。

※）JP1/Security Integrated Managerは，情報処理振興事業協会（IPA）が推進する「創造的ソフトウェア育成事業」の一環として技術開発された内容を含む。

# 1 はじめに

近年，インターネットをベースとする情報システムは，組織や社会の情報基盤として重要な役割を果たすようになりつつある。しかし，インターネットはオープンなシステムであることから，ウェブページの不正書き換えや，メールシステムと連動するウイルスによる社内文書の流出など，セキュリティ問題が過去に発生している。このような問題を防ぐためには，ファイアウォールやウイルス対策プログラムを導入するだけでなく，情報システムに対応して定期的にセキュリティ監査を実施するなど，セキュリティ運用管理を合わせて実行することが大切である。

このようなセキュリティ運用管理を正しく実施するには，システムのライフサイクル全体を見る必要がある。すなわち，システム運用時だけではなく，情報システムの設計，構築の各フェーズも考慮することが求められる。例えば，設計フェーズでは，対象システムのセキュリティポリシーを策定することが必要であり，構築フェーズでは，ポリシーに基づいて正しくセキュリティ機能を実装することが重要である。また，運用フェーズでも，単にファイアウォールなどを利用するだけではなく，不正な侵入を検知するセキュリティ製品や，セキュリティ脆（ぜい）弱性の診断を行うセキュリティ製品を用いて，新たに発生したセキュリティホールに対応することが必要である。

しかし，これまでのセキュリティ運用管理で使用されているセキュリティ製品は，それぞれフェーズごとに独立したものであり，全体的なセキュリティ運用管理を行うことを考慮していなかった。このため，ライフサイクルの部分的な支援をすることはできても，ライフサイクル全体にわたるセキュリティ運用管理を効率よく，効果的に支援するには十分ではなかった。

ここでは，対象システムの設計，構築，運用の各フェーズのさまざまなセキュリティ製品によって得られる情報を活用し，体系的な管理を実現することができるセキュリティ運用管理システムについて述べる。

# 2 セキュリティ運用管理

## 2.1 セキュリティ運用管理の現状

### 2.1.1 設計フェーズ

設計フェーズでは，まず，そのサイトで必要となるセキュリティポリシーを策定し，導入するセキュリティ製品を決定する必要がある。導入するセキュリティ製品には，ファイアウォール，ウイルス対策プログラムから不正侵入検知，アクセス制御など，多くのカテゴリーがあり，一つのカテゴリーのセキュリティ製品では，そのサイトで必要としているセキュリティポリシーを実現することができないのが現状である。

インターネットからの不正侵入を防御するためにはファイアウォール，ウイルスの検知にはウイルス対策プログラム，バッファオーバーフローなどの攻撃検知には不正侵入検知，コンテンツなどの不正アクセス検知にはアクセス制御のようにそれぞれのセキュリティ製品があり，これらを組み合わせることによってセキュリティポリシーを実現することができるようになる。

### 2.1.2 構築フェーズ

構築フェーズでは，策定したセキュリティポリシーを実現するために導入したセキュリティ製品の設定に反映する必要がある。策定したセキュリティポリシーをそれぞれどの製品で実現するのかを明確にし，セキュリティ設定を行う。セキュリティ設定では，各製品で同じ値を設定することもあるが，それぞれの製品で個々に設定する必要がある。

例えば，ログを保存する期間，管理者のユーザID（Identification）などは，サイト内で共通となることが多いが，それぞれの製品で同じ値を設定することになる。また，複数のファイアウォールを設置するサイトでは，フィルタリングするアドレスや，ファイアウォールを管理するマネージャのアドレスなどは，そのサイト内のファイアウォールで共通となる設定項目であるが，それぞれのファイアウォールで同じ値を設定することになる。

### 2.1.3 運用フェーズ

運用フェーズでは，構築フェーズで設定したおのおのの製品により，サイトのセキュリティが正しく維持できていることを監視する必要がある。多くのサイトでは，これまでに述べたように複数の製品によってセキュリティを維持していることから，それらすべての製品を監視しなければならず，セキュリティ障害が発生した場合には，タイムリーな調査，対策をすることができないのが現状である。

また，不正アクセスなどがあった場合，調査は不正侵入検知製品で行うが，その不正アクセスを防ぐ対策はファイアウォールで行う。このように，調査と対策を別の製品で行う場合もある。サイトの管理者は，複数の製品を常に監視し，セキュリティ障害が発生した場合，その原因を究明したうえで，適切な製品で対策を行う必要がある。

対策が完了してもセキュリティホールは日々発見され，不正アクセスの手口もますます複雑・巧妙になる。このため，サイトの管理者は，導入したそれぞれのセキュリティ製品を継続的に監視し続け，必要に応じてセキュリティポリシーにフィードバックをかけ，各製品のセキュリティ設定を見直さなければならない。

## 2.2 セキュリティ運用管理の課題

このように，サイトのセキュリティを維持するためには，複数の製品を導入し，それぞれを個々に構築，運用する必要がある。また，サイトの管理者はそれぞれの製品の運用を理解し，障害時には各製品を調査し，対策を行うことになる。このようなセキュリティの運用管理は，システム管理者の負担を増

大させ，システム全体の管理コストを増やすだけではなく，セキュリティポリシーにのっとった運用が正しく行われずに，サイトの運用に影響を及ぼす恐れがある。

日立製作所は，これらのセキュリティツールを運用管理する際の問題を解決するために，JP1統合セキュリティ管理を開発した。

## 3 統合セキュリティ管理

### 3.1 JP1統合セキュリティ管理の概要

JP1統合セキュリティ管理“JP1/Security Integrated Manager”（以下，JP1/SCIMと略す。）は，統合システム運用管理JP1シリーズの「ジョブ管理」，「アベイラビリティ管理」，「ネットワーク管理」などの管理機能と並んで，システム全体のセキュリティ管理を実現することができる製品である。

JP1/SCIMは，日立製作所の製品だけでなく，他社のセキュリティ製品の管理機能を一元的に管理することもできる。したがって，セキュアなシステムの構築フェーズ・運用フェーズでは，システム全体のセキュリティ運用管理の利便性を向上させ，システム管理者の負荷を軽減することができる。

また，システム全体のセキュリティ事象（不正侵入の検知やウイルスの発見など）を一元的に監視することで，不正な侵入やウイルスを検知した際には，リアルタイムに管理者に通知することができる。さらに，各セキュリティ製品の稼動ログを収集した結果に基づいて，セキュリティ監査を支援する情報も提供する（**図1**参照）。「統合セキュリティ管理」JP1/SCIMの特徴である三つの機能について，以下に述べる。

### 3.2 セキュリティ製品管理機能の一元管理

JP1/SCIMの管理コンソールから管理対象としているセキュリティ製品の管理機能を，GUI（Graphic User Interface）を用いて呼び出すことができる。これにより，各セキュリティ製品のポリシー情報を確認したり，管理情報のカスタマイズが一元的に行えるため，システム全体として統一的なセキュリティポリシーの設定を行うことができる（**図2**参照）。また各セキュリティ製品に対する運用が省力化できるうえ，迅速に対応することもできる。

### 3.3 セキュリティ事象の統合監視

システム管理者は，システムに発生するさまざまなセキュリティ事象を，JP1/SCIMの管理コンソールから統合的かつリアルタイムに監視することができる。さらに，JP1/SCIMでは，セキュリティ事象の発生をJP1ネットワーク管理“JP1/Cm2/Network Node Manager”や，JP1統合管理“JP1/Integrated Manager”にも通知することができる。これにより，システム管理者は，従来導入しているJP1製品を利用して，セキュリティの管理も統合的に行うことができる。

### 3.4 セキュリティ監査支援

JP1/SCIMでは，管理対象のセキュリティ製品が出力するログを収集，蓄積し，製品カテゴリー・期間・組織などのさまざまな条件によって検索，並べ替え，分類する機能を提供する。これにより，セキュリティポリシーの維持を確認するために定期的に実施する必要のある，膨大なログの解析作業を大幅に効率化，自動化し，システム全体のセキュリティ監査をサポートすることができる。また，収集，蓄積したログを，JP1/SCIMによって安全に保管することもできる。

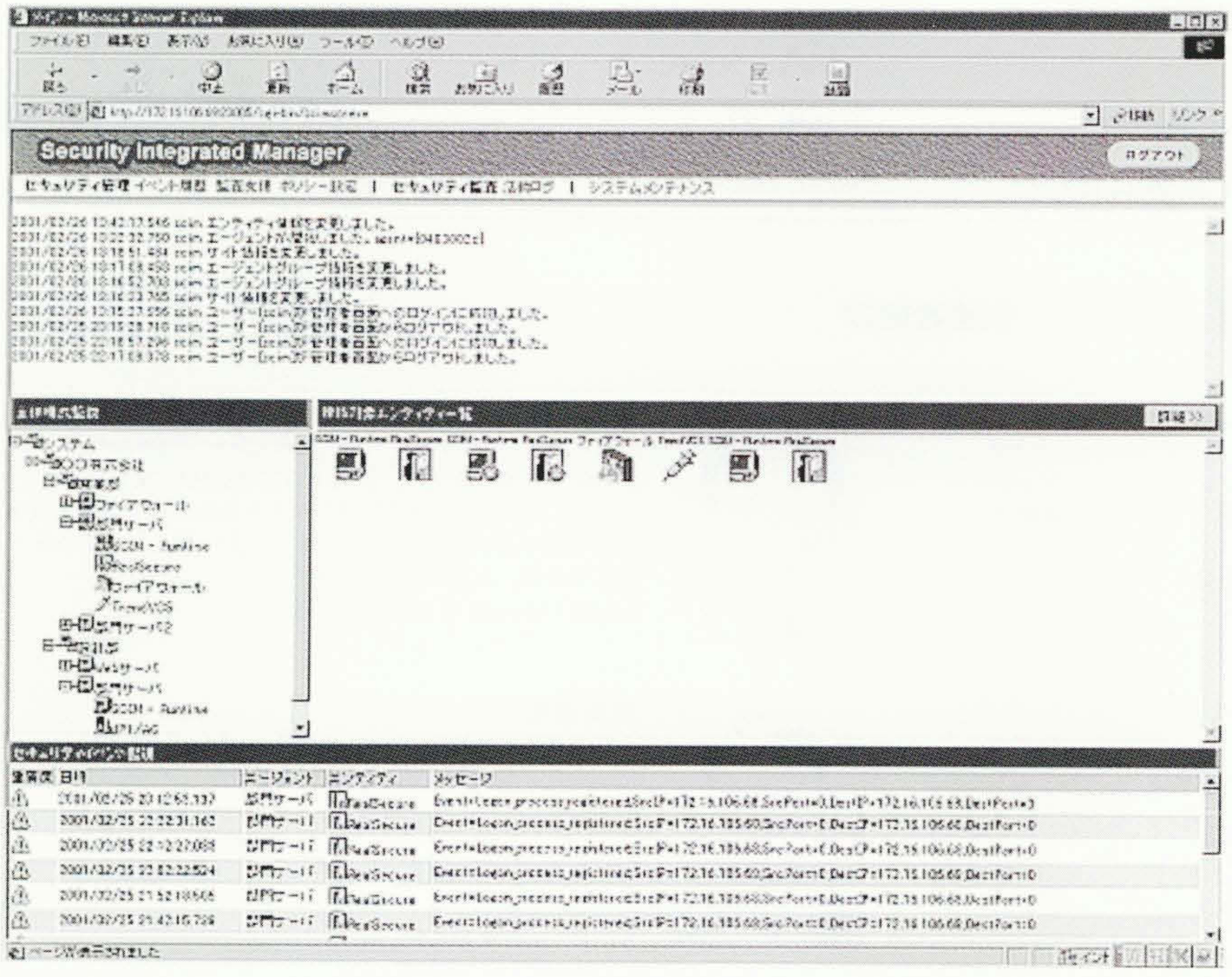



**図1 統合セキュリティ管理，セキュリティ事象の監視画面**

管理対象としている各セキュリティ製品のセキュリティイベントを，統合的かつリアルタイムに監視することができる。

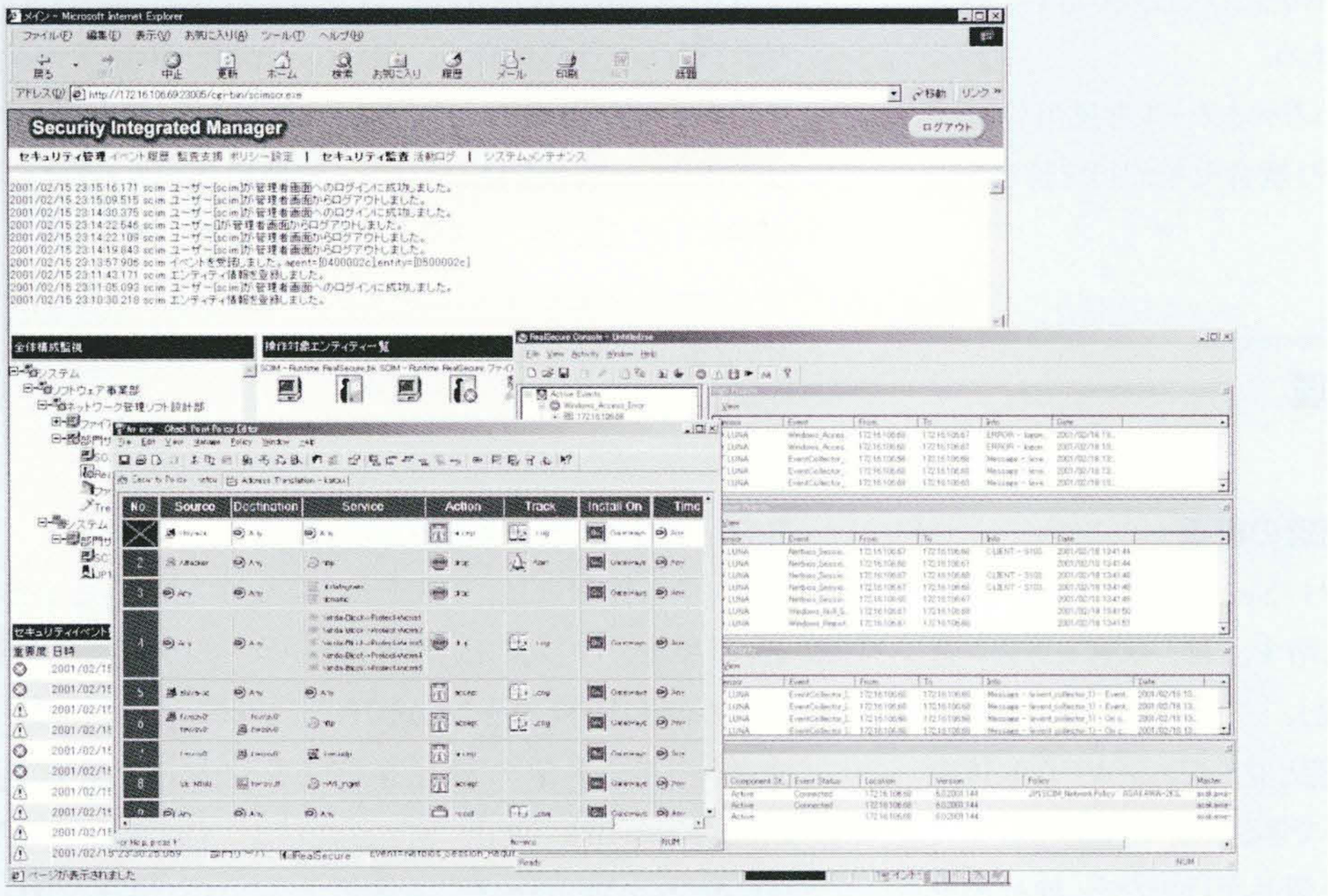



**図2 各セキュリティ製品の管理機能の一元化**

JP1/SCIMの管理コンソールから各セキュリティ製品の管理機能を呼び出すことで，セキュリティ製品のポリシー情報の確認・設定が行える。

## 4 おわりに

ここでは，JP1/SCIMが，複数のセキュリティ製品を一元的に統合し，セキュリティのライフサイクルであるポリシー設定，セキュリティ事象の監視，セキュリティ製品の出力するログの監査機能を持ち，システムのセキュリティ運用管理を支援する製品であることについて述べた。

JP1/SCIMにより，システムの管理者は個々のセキュリティ製品を個別に管理する必要がなくなり，セキュリティ障害にタイムリーな対応ができる。この結果，システムの障害を最小限にとどめるだけではなく，システム管理の費用削減にも効果が期待できる。

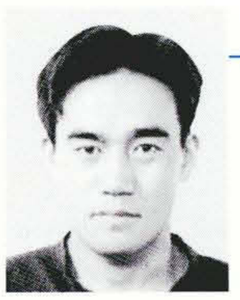
日立製作所は，各セキュリティツールを体系的に管理するためのセキュリティ運用管理システムを提案し，製品化した。今後は，統合する各セキュリティ製品を拡充させるとともに，さらなるセキュリティ運用管理の利便性の向上を図っていく。また，JP1/SCIMで収集した情報をシステムのセキュリティ設計や構築に反映させられるようにするなど，いっそうトータルなセキュリティ運用管理ができる製品の開発を目指していく考えである。

### 参考文献


1) 萱島，外：統合セキュリティ運用管理システムの実現に向けて，情報処理学会全国大会(2001.4)

2) 妹尾，外：ネットワークセキュリティにおける運用管理の実現方法，情報処理学会全国大会(2001.9)


### 執筆者紹介

**長田清人**

1986年日立製作所入社，情報・通信グループ ソフトウェア事業部 システム管理ソフトウェア本部 ネットワーク管理ソフト設計部 所属
現在，JP1セキュリティ製品の開発に従事
情報処理学会会員
E-mail：k_osada @ itg. hitachi. co. jp

**妹尾　徹**

1995年日立製作所入社，情報・通信グループ ソフトウェア事業部 システム管理ソフトウェア本部 ネットワーク管理ソフト設計部 所属
現在，JP1セキュリティ製品の開発に従事
E-mail：senoo @ itg. hitachi. co. jp

**萱島　信**

1989年日立製作所入社，システム開発研究所 第7部 所属
現在，セキュリティ運用管理システム技術の研究開発に従事
情報処理学会会員，電子情報通信学会会員，ソフトウェア科学会会員，人工知能学会会員
E-mail：kayashi @ sdl. hitachi. co. jp

**服部泰明**

1983年日立製作所入社，情報・通信グループ ソフトウェア事業部 企画本部 計画部 所属
現在，ネットワークやセキュリティに関するソフトウェア製品の企画・計画に従事
情報処理学会会員
E-mail：hattor_y @ itg. hitachi. co. jp