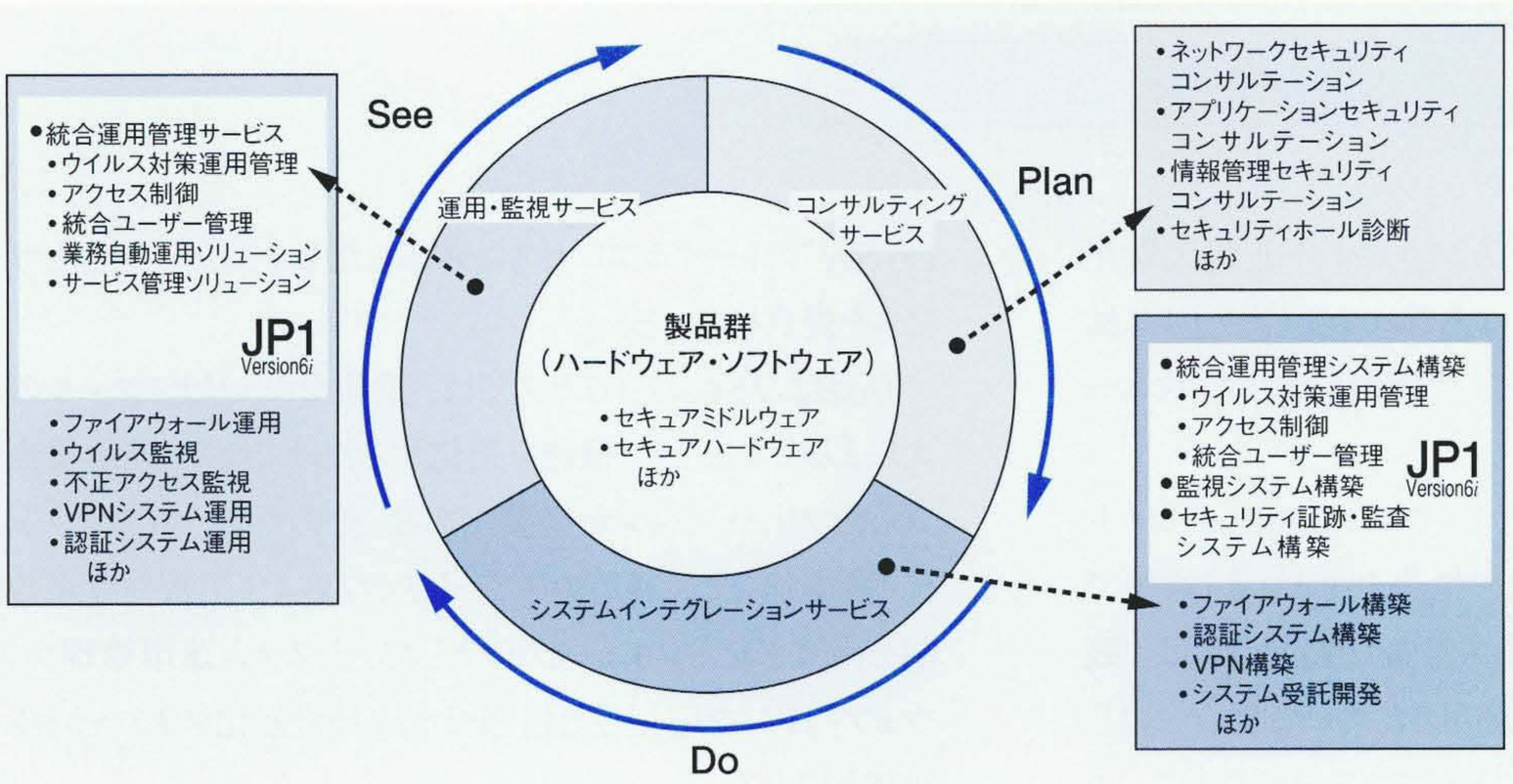
情報セキュリティ強化ソリューションと適用事例

Reinforced Cyber Security Solutions for Enterprise Information Systems Integration

宮崎義弘 *Yoshihiro Miyazaki*　神山　哲 *Satoru Kôyama*　高山聡一郎 *Sôichirô Takayama*



日立製作所の提供する情報セキュリティ強化ソリューション

“JP1 Version6*i*”を応用した情報セキュリティ統合運用管理を含む，情報システムのトータルプロセスに適応したセキュリティ製品・サービス体系を提供する。

注：略語説明
VPN（Virtual Private Network）

ウイルス問題や顧客情報漏えい問題など，IT（Information Technology）環境での企業の情報セキュリティについてのリスクマネージメントは，近年ますますその重要性を増している。情報セキュリティを強化するには，最新のセキュリティツールを個別に導入するだけでは十分とは言えない。統合運用管理により，企業内外の環境の変化にスピーディーかつ柔軟に対応することが大切である。

日立製作所は，情報セキュリティ分野用としてシステム運用管理ソフトウェア“JP1”シリーズのレパートリーを拡張した。さらに，これを応用した「情報セキュリティ強化ソリューション」によって柔軟かつセキュアなIT環境の構築を支援している。

1 はじめに

インターネット時代に突入し，企業の内外はインターネットやイントラネットでつながれ，グローバルな環境でスピーディに企業活動が進められるようになった。その反面，ウイルスや情報漏えいなどの問題も頻発し，ひとたび被害が出ると，その波及スピードも速く，被害範囲は甚大なものとなっている。したがって，企業の情報セキュリティについてのリスクマネージメントは，ますます重要性を増している。

情報セキュリティを強化するには，最新のセキュリティツールを導入することが有効であるが，それだけではきめ細かさや即時性が不十分である。そのために，個別のツールを統合して運用管理することによって迅速，柔軟に対応する必要がある。

日立製作所は，システム運用管理ソフトウェアとしてすでに定評のある“JP1”シリーズに，情報セキュリティ分野用としてのレパートリーを加え，これを応用した「情報セキュリティ強化ソリューション」により，柔軟かつセキュアなIT環境の構築を支援している。

ここでは，企業の情報セキュリティ強化における統合運用管理の重要性と，“JP1”による「情報セキュリティ強化ソリューション」の適用事例について述べる。

2 情報セキュリティ喪失の脅威

企業は，さまざまなセキュリティ喪失の脅威に囲まれている。情報セキュリティ喪失の主な脅威の例を**図1**に示す。

セキュリティの対応に失敗すると，信用の失墜や責任問題，膨大な損害の発生，企業経営破綻（たん）などの危険性が生

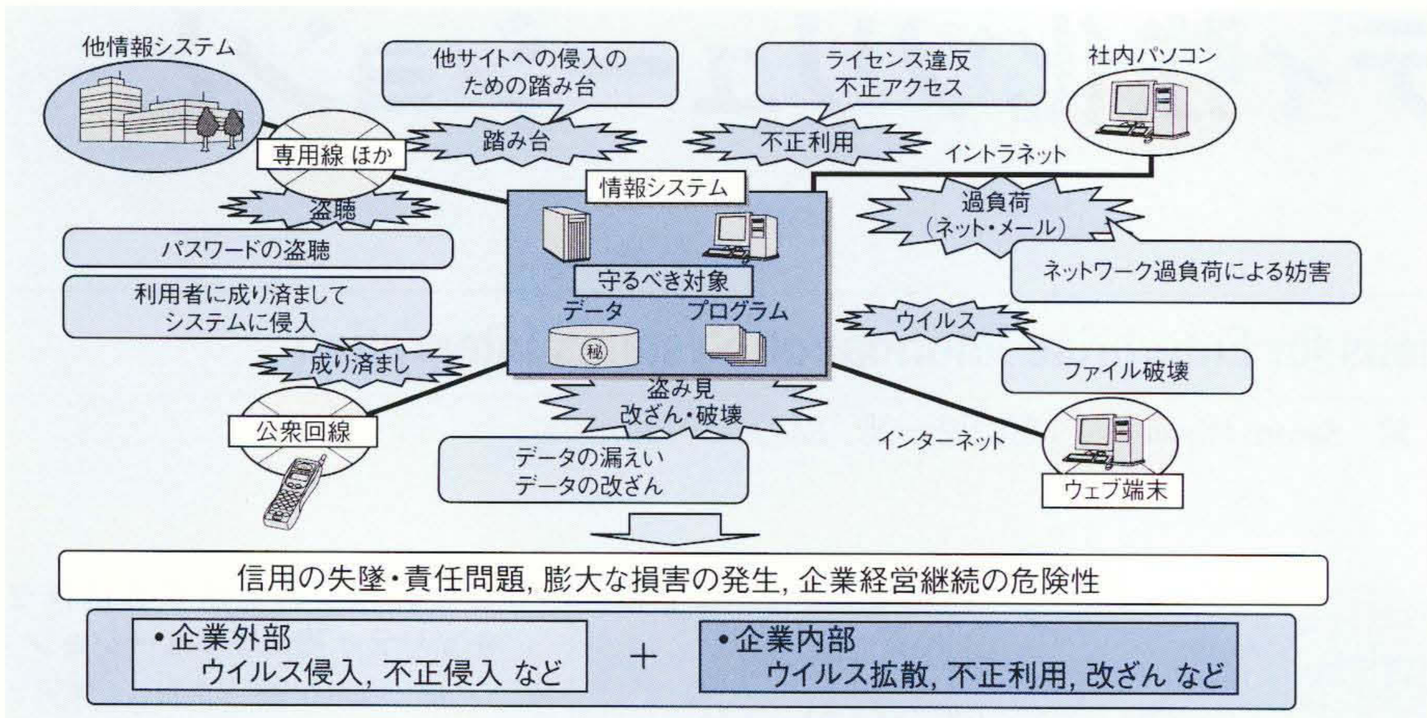


図1 情報セキュリティ喪失の脅威

ウイルスや不正アクセスなどで情報セキュリティが喪失することは重大な問題である。企業外部だけでなく，企業内部にもリスクマネージメントが必要である。

じる。この対策には，ウイルスの侵入防止や，不正侵入防止など，企業外部からの入口に着目するだけでなく，ウイルス拡散防止，不正利用・改ざん防止など，企業内部のリスクマネージメントも必要である。

2001年に猛威をふるったワームウイルスのCodeRed（コードレッド），Nimda（ニムダ）は，従来の情報セキュリティ対策では十分でないことを示した。ウイルス対策ソフトウェアは，既知のウイルスのパターンファイルが適用されている場合にはじめてウイルスを検知して駆除することができるのであって，未知のウイルスが発生した場合，そのパターンファイルが供給，適用されるまでは感染の危険がある。ここで重要なことは，未知のウイルスのほとんどが既知のぜい弱性を利用して作られているということである。つまり，ぜい弱性が既知となった時点で，ウイルス対策ソフトウェアやセキュリティパッチをすみやかに適用すれば，被害をなくすか最小限に抑えられるはずである。しかし，現実には多くの企業に被害が拡散しており，迅速にウイルス対策をとるためにはなんらかの運用支援手段が必要である。

また，最近は顧客個人情報の保護についての規制が厳しくなっており，データの漏えい・改ざんの防止について，その重要性がますます高まっている。この課題に対応して，ファイアウォールや各サーバのアクセス制御機能を用いることにより，技術視点で防護することができる可能性がある。しかし，運用視点から言えば課題は多い。ファイアウォールや各サーバのアクセス制御の設定を漏れなく行うことや，組織変更，サーバ増設・分担変更，バーチャルプロジェクト体制構築などにタイムリーに対応することができること，許容されるリソースの中でセキュリティを維持して運用できることなどが求められており，これらの運用課題を解決するには何らかの運用支援手段が必要である。

3 情報セキュリティ強化ソリューションへの取り組み

日立製作所は，前述したニーズにこたえるため，“Plan-Do-See”のトータルプロセスに適応したセキュリティ製品とサービスを提供している。

DoおよびSeeのプロセスでは，最新セキュリティツールの導入によるセキュリティ機能を強化するだけでなく，運用視点に立ったソリューションが必要である。そのため，情報セキュリティ機能強化と，運用のスピードアップおよび工数や費用の抑制を両立させるソリューションとして，システム運用管理ソフトウェア“JP1”を応用した情報セキュリティ強化ソリューションを提供している。

企業内の情報セキュリティ強化を推進するには，組織としての対応が必要である。その推進手順の概要について以下に述べる。

(1) セキュリティポリシーの策定

セキュリティの対象とセキュリティ喪失の脅威を整理し，セキュリティ確保の基本方針を明確化する。

(2) セキュリティ機能の実装

セキュリティポリシーに基づき，具体的な対策としてセキュリティ設計を行い，セキュリティ製品を導入することによってセキュリティ機能を実装する。

(3) 運用ルールの制定

セキュリティ製品を運用するだけでなく，監視方法や情報の管理，行動をルール化する。場合によってはネットワークの切断，サーバの停止なども含めた緊急時の対応を想定し，権限・実行手順を取り決めておく必要がある。

(4) 外部情報の把握

セキュリティ喪失の脅威については，最新の情報（ウイルス，セキュリティホール，対策方法）を日々入手する。これにより，例えば，ウイルスが世界的に蔓（まん）延する前に企業内の対応方針を決定することができる。

(5) 内部実態の把握

セキュリティホールの対策が必要な場合，影響度合いを把握し，セキュリティ対策の対象となる機器（パソコンを含む。）を特定する。

(6) セキュリティ対策の実施

対策対象となる機器（パソコンを含む。）にセキュリティ対策

を実施する。

(7) セキュリティ状況の把握

対策対象にセキュリティ対策の実施状況を把握する。

実態の把握や，対策，状況の把握については，日々繰り返して実施することが必要である。しかし，それを現実に企業内で運用することは容易ではない。“JP1”を応用した情報セキュリティ統合運用管理ソリューションは，情報セキュリティ強化対策を運用レベルで支援している。

4 情報セキュリティ強化ソリューションの適用事例

4.1 ウイルス対策運用管理

多くの企業では，従業員全員にイントラネット接続のパソコンを配備している。情報セキュリティ対策で最も労力や時間が掛かるのが，これらのパソコンの運用管理である。パソコンの導入や更新を一時期に行えないので，頻繁にパソコンの部分更新が発生し，搭載しているOS(Operating System)のバージョンが異なったものも混在している。パソコンに搭載したソフトウェアに新たなセキュリティホールが見つかれば，セキュリティパッチで修正を行う必要がある。しかし，OSのバージョンや，搭載ソフトウェアの種類とバージョンにより，対策の要・不要や対策方法が異なるので，対象となるパソコンを特定するのは容易なことではない。対象となるパソコンを特定することができても，セキュリティ対策を各パソコンユーザーに委託すると，対策がなされなかったり，対策完了までに時間がかかることが多く，対策状況を正確に把握することも困難であった。また，ノート型パソコンの普及によって設置場所の制約がなくなり，エンドユーザーの利便性は向上したが，セキュリティの運用にとっては，対策が必要なパソコンがどこにあるのかを把握することが困難となる。

このような課題に対応して，“JP1”を応用した情報セキュリティ強化ソリューションでは，運用まで含めたTCO(Total Cost of Ownership)の低減と，セキュリティレベルの向上を図ることができる。その基本構成を**図2**に示す。

“JP1”は，パソコンにあらかじめ配布したエージェントとの連携により，パソコン上のソフトウェアの登録・利用情報をサーバに収集する。また，ウイルス対策パッチなどのソフトウェアをパソコンにリモート配布することにより，漏れなく，すばやいウイルス対策ができる。また，このソリューションを用いることにより，ウイルス対策運用管理に加え，ソフトウェアライセンス管理，リモート配布，利用状況管理をサポートすることができる。

ウイルス対策運用管理の具体的な運用の手順について以下に述べる。

(1) パソコン利用者・設置場所の特定

パソコンの利用者や設置場所の変更がある場合，エンドユーザーに入力を促す画面を出力する。パソコンの利用者や設置場所が変更されても，変更情報を集中管理することができる。

(2) エンドユーザーへの表示

ウイルスの蔓延などをエンドユーザーに警告する画面を表示する。通常，利用者が自発的に参照するプル型表示に加え，ウェブページを全パソコンに強制的に表示するプッシュ型表示をサポートする。

(3) セキュリティ対策が必要な対象の特定

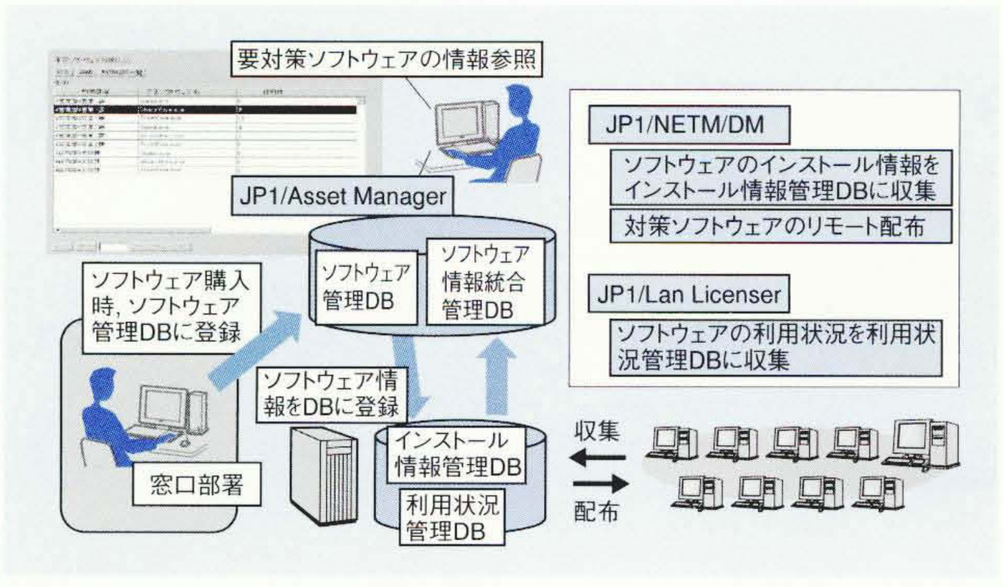
セキュリティホールの対策が必要なパソコンを特定するための情報(OSのバージョン，インストールしたソフトウェアなど)を日々収集する。

(4) セキュリティ対策の実施

セキュリティパッチを対象パソコンに一斉に配布して反映する。

(5) セキュリティ状況の把握

セキュリティパッチの対策状況を管理画面上でリアルタイムに表示する。



注：略語説明　DB(Database)

図2 ウイルス対策運用管理

JP1は，パソコンにあらかじめ配布したエージェントとの連携により，パソコンに搭載されているソフトウェアの情報収集と，パソコンへのセキュリティ対策ソフトウェアのリモート配布をサポートする。これを応用したソリューションにより，ウイルス対策を漏れなく，すばやく実施することができる。

4.2 アクセス制御と統合ユーザー管理

アクセス制御による不正利用防止について，その適用事例を述べる。

ウェブサーバに対応するアクセス制御機能の概要を**図3**に示す。ウェブ掲載情報へのアクセスを限定し，不正な内部ユーザー，クラッカー，ウイルスによる改ざん・漏えいを防止する。

しかし，アクセス制御にも運用視点でのアプローチが必要である。運用課題として，次の3点があげられる。

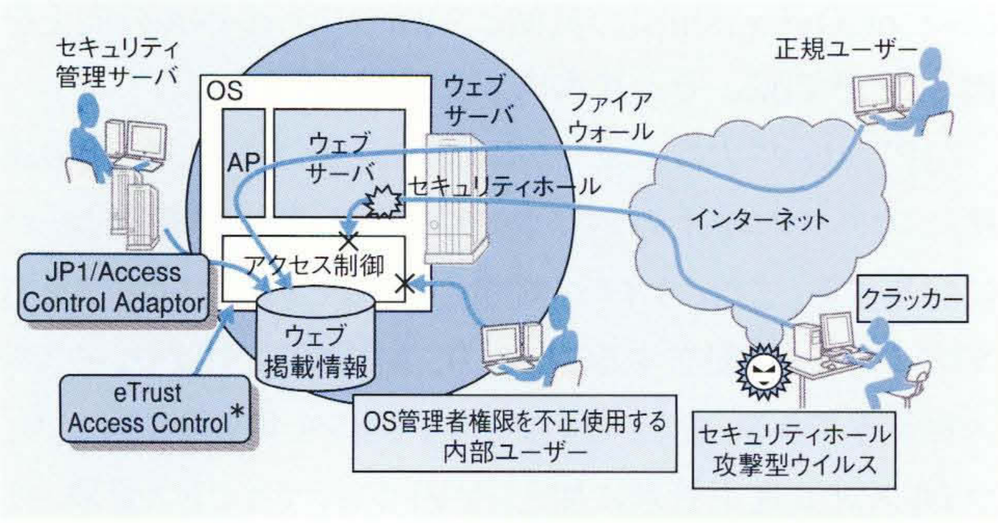
(1) ファイアウォールや各サーバのアクセス制御のポリシー設定について，全サーバの設定を漏れなく正確に行うことができるか。

(2) 組織や機器の変更にタイムリーに対応することができるか。

(3) 許容される工数内で維持運用することができるか。

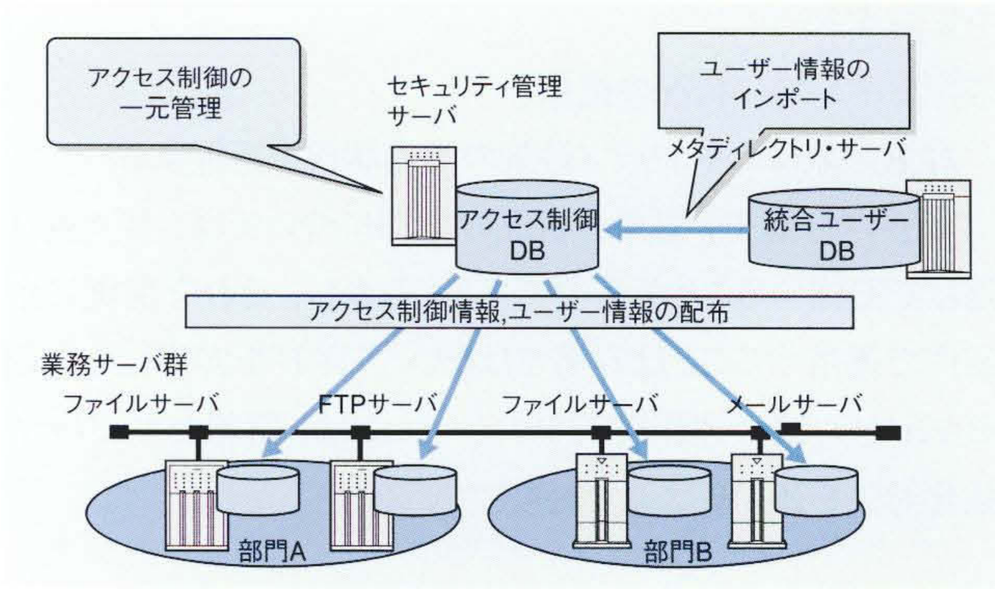
今後，適用アプリケーションが拡大し，多様化すれば，ユーザーごとのきめ細かな設定も必要となる。

このシステムでは，前記の3点を解決するために，多数・多種のサーバがある場合でも，ユーザー情報やアクセス制御情



注：略語説明ほか
OS（Operating System），AP（Application）
＊eTrust Access Controlは，米国Computer Associates International, Inc.の商標である。

図3 ウェブアクセスの制御機能
ウェブ掲載情報へのアクセスを限定し，不正な内部ユーザー，クラッカー，ウイルスによる改ざん，漏えいを防止する。



注：略語説明　FTP（File Transfer Protcol）

図4 アクセス制御の一元管理と統合ユーザー管理
複数・異機種のOSのアクセス制御を共通のインタフェースで一元管理し，また，ユーザー情報を一元管理する統合ユーザーデータベースと連携することにより，システム全体で漏れのないアクセス制御の運用管理を容易に行うことができる。

報を一元管理，監査することにより，ユーザーIDの追加，削除などの作業を各サーバで個別に行うことなく，管理サーバで一括して実施することができる。

その基本構成を**図4**に示す。“JP1”を活用することにより，複数・異機種のOSのアクセス制御を，共通のインタフェースで一元管理することができる。また，ユーザー情報を一元管理するメタディレクトリサーバの統合ユーザー情報をセキュリティ管理サーバのアクセス制御情報にインポートする機構を構築することにより，統合ユーザー管理とアクセス制御とを連携することができる。

これによって，以下の効果が期待できる。

(1) 統合ユーザー管理データベース（メタディレクトリ）をメンテナンスすることにより，各サーバにユーザー情報を自動的に反映することができるので，管理者の工数が低減できる。

(2) セキュリティホールとなりやすい幽霊ID（利用者のいないユーザーアカウント）を検出して排除することができる。

(3) 統合的アクセス制御や網羅的な監査が可能になり，セキュリティレベルの向上を図ることができる。

(4) 各サーバ，アプリケーションの利用者登録の申請が一括して実施しやすくなるので，エンドユーザーの工数を低減することができる。

5 おわりに

ここでは，企業の情報セキュリティ強化における統合運用管理の重要性と，これを解決するソリューションおよびその適用事例について述べた。

日立製作所は，システム運用管理ソフトウェア“JP1”シリーズを応用した「情報セキュリティ強化ソリューション」を広く提供していくとともに，今後も新たな脅威に対応できるように，最新セキュリティツールの取り組みと，ソリューションの拡張を図っていく考えである。

参考文献

1) 金野，外：トータルな情報システムセキュリティを提案する製品・サービス体系“Secureplaza”，日立評論，**81**，6，393～398（1999.6）
2) 山口，外：特集 ネットワークセキュリティ，情報処理学会誌，42，12（2001.12）

執筆者紹介

宮崎義弘
1977年日立製作所入社，情報・通信グループ 産業・流通システム事業部 産業第二システム本部 産業第四システム部所属
現在，製造業用情報システムの拡販・建設取りまとめに従事
情報処理学会会員，電気学会会員，IEEE会員
E-mail：yosmiya @ itg. hitachi. co. jp

神山　哲
1985年日立製作所入社，情報・通信グループ 産業・流通システム事業部 産業第二システム本部 産業第四システム部所属
現在，製造業用情報システムの構築に従事
E-mail：skouyama @ itg. hitachi. co. jp

高山聡一郎
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，セキュリティ運用管理製品の拡販に従事
E-mail：taka_so @ itg. hitachi. co. jp