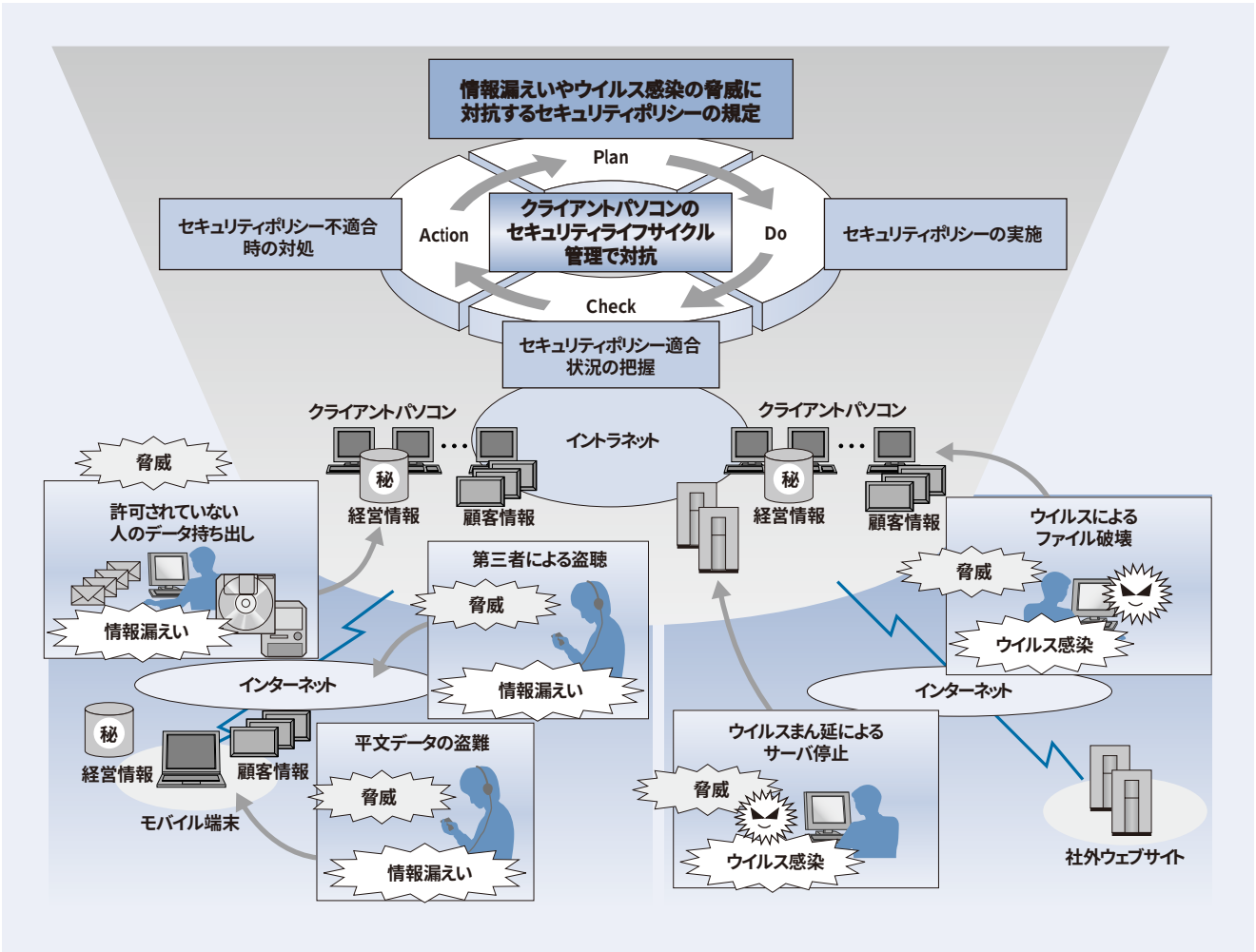
ビジネスの信用を支えるセキュリティライフサイクル管理ソリューション

Security Lifecycle Management Solutions for Supporting Trust in Business

豊田英樹 *Hideki Toyoda*　高山聡一郎 *Sôichirô Takayama*　萱島 信 *Makoto Kayashima*



クライアントパソコンのセキュリティライフサイクルの概要

統合システム運用管理ソフトウェア“JP1”では，情報漏えい防止やウイルス感染防止など，複数のセキュリティ対策に関するセキュリティポリシーの規定（Plan），実施（Do），適合状況の把握（Check），不適合時の対処（Action）を一元管理し，セキュリティ対策管理コストの低減とセキュリティ対策の徹底を支援する。

個人情報保護法が本格施行される一方，OSやアプリケーションのぜい弱性をついた，ワームなどと呼ばれるコンピュータウイルスによる業務システムの停止といった被害のリスクが高まっていることから，企業内のセキュリティ対策が急務となっている。

日立製作所が開発した統合システム運用管理ソフトウェア“JP1 Version 7*i*”では，企業内クライアントパソコンの情報漏えいや，ウイルス感染を防止するため，セキュリティポリシーの規定，実施，適合状況の把握，および不適合時の対処といったセキュリティライフサイクル管理を実現し，クライアントパソコンのセキュリティ確保と管理コストの低減を実現している。

また，サーバ ベースト コンピューティングなど，新しいシステム形態に移行した場合にも，システムの特質に合わせてセキュリティライフサイクル管理ソリューションを提供し，トータル セキュリティ ソリューション“Secureplaza”とともに，迅速にセキュリティ管理ソリューションを提案していく。

1 はじめに

現在の多くの企業情報システムでは，従業員ごとにパソコンが配布され，膨大な数のクライアントパソコンが企業内ネットワークに接続されている。また，企業外ネットワークへのアクセスやノートパソコンの社外利用が一般的になり，ウイルス感染対策や情報漏えい防止対策の徹底，および対策状況の把握が困難な状況にある。その結果，OS(Operating System)やアプリケーションのぜい弱性をついたBlasterやWelchiaなどと呼ばれる感染力の強いウイルスにより，企業情報システムがダウン(動作停止)した事例も多数報告されている。

情報漏えいやウイルスによる企業情報システムのダウンが発生した場合，自社だけの問題では済まず，パートナー企業に対して加害者となり，企業のブランドイメージ低下や企業の信用失墜にもつながる可能性がある。このため，セキュリティ対策の不足は，企業経営にも影響を及ぼすことになる。

このような情勢に合わせて，わが国の法制度の強化も進み，2005年4月に本格施行された個人情報保護法では，情報漏えい防止など安全管理に必要な措置が義務づけられ，義務に違反した企業には罰則が規定されている。コンプライアンス(順法)の面からもセキュリティポリシーの明確化と，セキュリティ対策が急務である。

ここでは，クライアントパソコンのセキュリティポリシーの規定と，セキュリティポリシーに基づくセキュリティ対策について述べる。

2 セキュリティ対策の課題

クライアントパソコンのセキュリティ対策を徹底するためには，情報漏えいとウイルス感染を防止するセキュリティポリシーの規定(Plan)と実施(Do)だけでなく，セキュリティポリシーへの適合状況の把握(Check)と，適合していないクライアントパソコンへの対処(Action)を行い，管理する必要がある。しかし，クライアントパソコンの数が増加することに伴い，セキュリティ対策に要する管理コストが増大し，セキュリティ対策の徹底も困難となっている。また，情報漏えいとウイルス感染を防止するセキュリティ対策としては，企業外への情報の不正な持ち出しを制限しなければならない。情報を持ち出す場合は，情報を暗号化する情報漏えい防止ソフトウェアを適用し，最新のセキュリティパッチ(修正プログラム)や，最新ウイルスパターンを適用し，ぜい弱性のあるソフトウェアを排除する必要がある(**図1**参照)。

このような課題を解決するために，日立製作所の統合システム運用管理ソフトウェア“JP1 Version 7*i*”では，セキュリティライフサイクルと，情報漏えい・ウイルス感染を防止するセキュリティ対策要件を満たすセキュリティライフサイクル管理ソリューションを提供している。

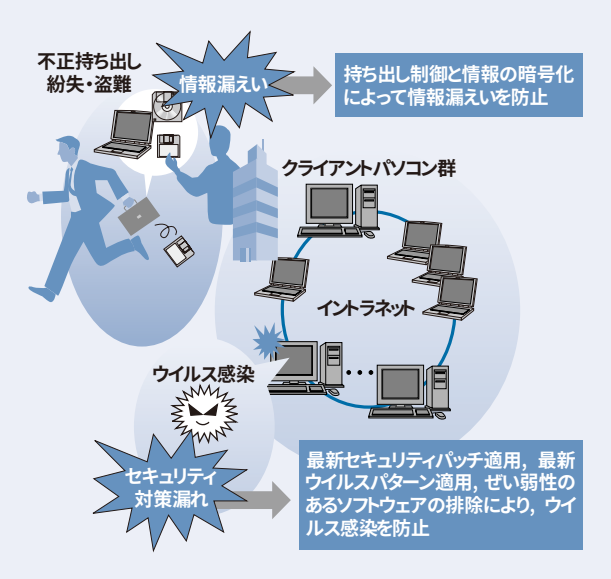


図1 セキュリティ対策の要件
情報漏えいやウイルス感染を防止する対策をライフサイクルとして管理することが重要となる。

3 セキュリティポリシーの実現

3.1 セキュリティライフサイクルの実現

企業情報システムでは，次々とクライアントパソコンが導入され，日々最新のセキュリティパッチやウイルスパターンが提供されている。クライアントパソコンをセキュアな状態に保つために

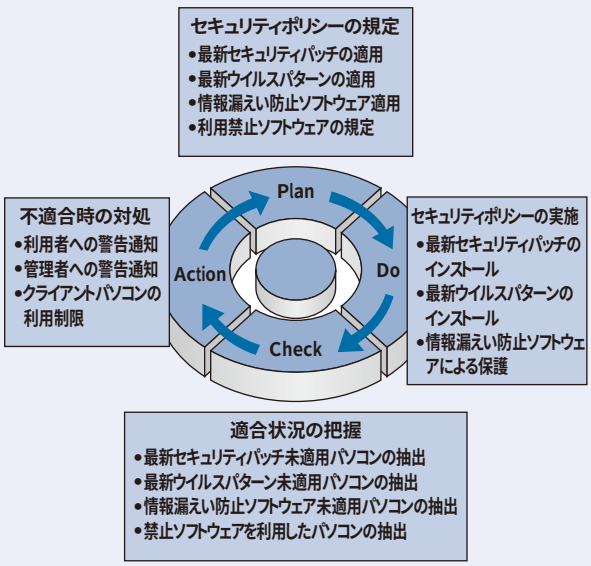


図2 セキュリティライフサイクルの概要
クライアントパソコンのセキュリティライフサイクル管理をサポートする。

は，セキュリティポリシーの規定，実施，適合状況の把握，不適合時の対処を継続的に行い，ライフサイクルとして管理する必要がある（図2参照）。

IT（Information Technology）資産であるクライアントパソコンは，JP1統合資産管理で管理することができる。そのため，JP1クライアントセキュリティ管理では，クライアントパソコンのセキュリティ対策を，セキュリティを観点とした資産・配布管理と位置づけ，JP1統合資産管理とシームレスに連携したクライアントパソコンのセキュリティライフサイクル管理を実現している。

3.2 セキュリティポリシーの規定

企業がクライアントパソコンに実施するセキュリティ対策要件をセキュリティポリシーとして，必要となる最新のセキュリティパッチ，必要となる最新ウイルスパターン，情報漏えい防止を実現するソフトウェア情報，利用を禁止するソフトウェア情報を規定する。JP1クライアントセキュリティ管理では，以下の項目を不適合時のぜい弱性レベル情報と併せて規定できるようにし，柔軟なセキュリティポリシーの規定を実現している。

（1）必要となるWindows※）更新プログラムポリシー
（2）必要となるウイルス パターン ポリシー
（3）適用が必要なソフトウェアポリシー
（4）利用を禁止するソフトウェアポリシー

※）Windowsは，米国およびその他の国における米国Microsoft Corp.の登録商標である。

3.3 セキュリティポリシーの実施

規定されたセキュリティポリシーに従い，以下のセキュリティ対策要件を実施する。

（1）ソフトウェア，ウイルスパターン適用の実施

クライアントパソコンの数が膨大になった場合，セキュリティポリシーに規定された最新セキュリティパッチや，最新ウイルスパターン，情報漏えい防止ソフトウェアの適用（配布）を実現する管理コストが問題となる。JP1ソフトウェア配布・資産管理では，オンライン適用（配布）を実現することにより，管理コストの低減を図っている（図3参照）。

（2）情報漏えいの防止

情報漏えいの多くは，情報を許可なく外部に持ち出すことによって起こる。そのため，許可のない情報の持ち出しを排除することで情報漏えいの可能性は大幅に削減できる。また，暗号化して情報を持ち出すことで第三者には意味のない情報となり，情報漏えいのリスクを大幅に削減することができる。JP1情報漏えい防止では，情報の持ち出し制御や，持ち出し情報の暗号化だけでなく，持ち出し手段の制御をサポートしている。これにより，組織の特性に合わせた柔軟な持ち出し制御ポリシー，利便性とセキュリティを両立させた情報漏えいの防止を実現している（図4参照）。

3.4 セキュリティポリシー適合状況の把握と対処

情報漏えいとウイルス感染は，クライアントパソコンのセキュリティポリシー適合状況が把握されず，適合しないまま放置されていることが最大の原因である。JP1クライアントセキュリティ管理では，JP1ソフトウェア配布・資産管理で収集したクライアン

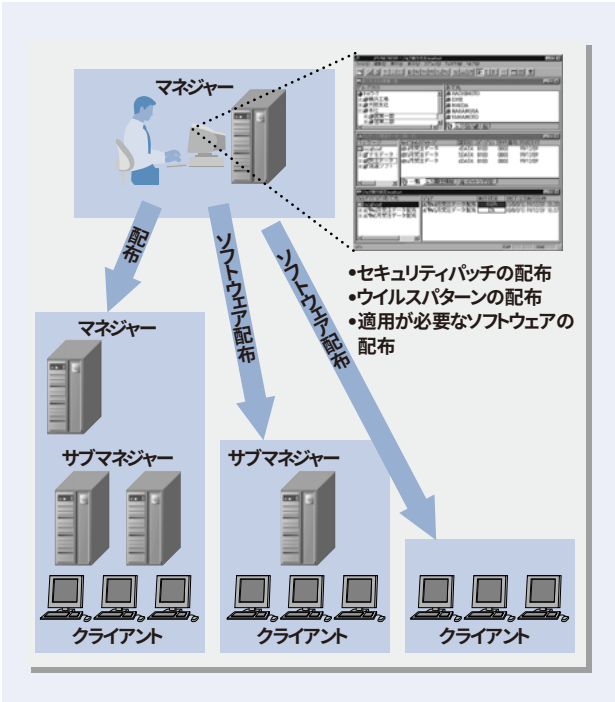
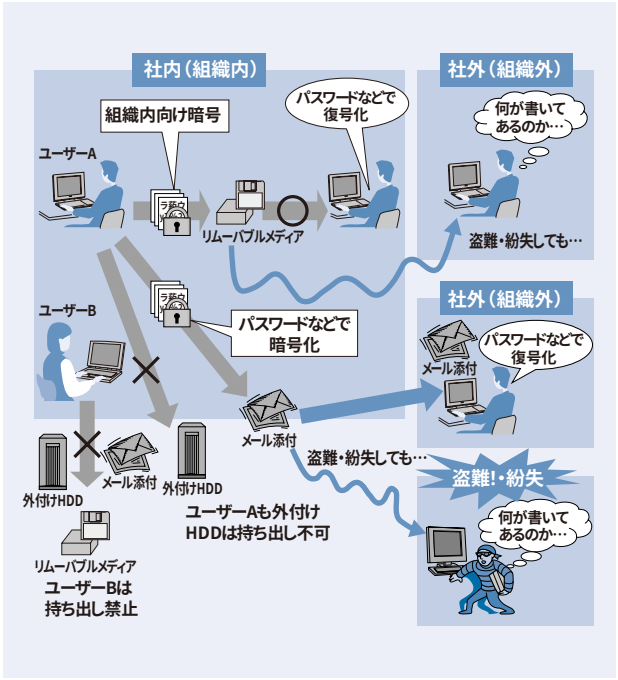


図3 ソフトウェアのオンライン配布の仕組み
セキュリティポリシーで規定されたソフトウェアのオンライン配布をサポートする。



注：略語説明　HDD（Hard Disc Drive）

図4 情報漏えい防止の概要
持ち出し情報の制御と暗号化をサポートする。

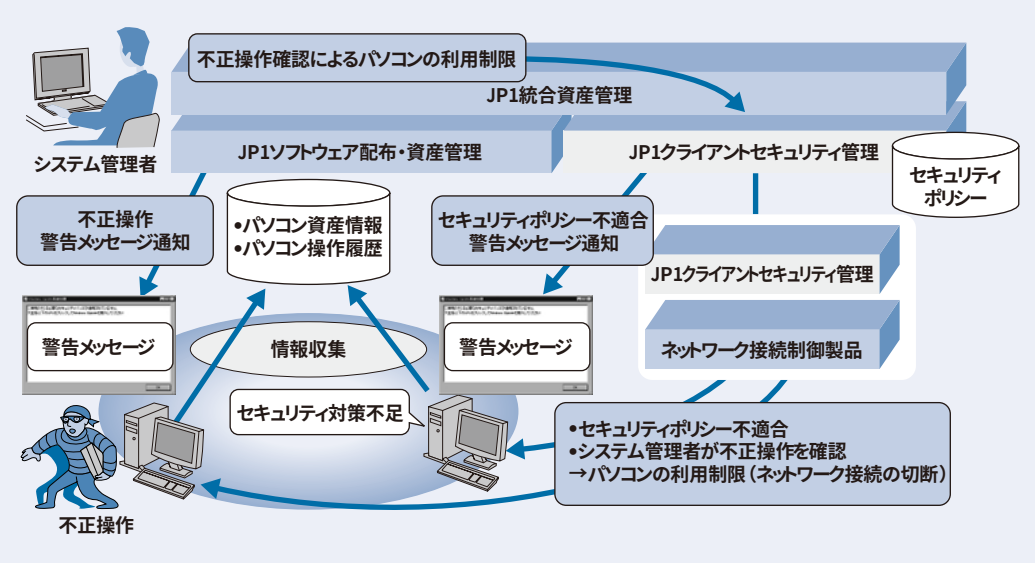


図5 セキュリティポリシー適合状況の把握と対処の流れ
セキュリティポリシーに適合しない，ぜい弱性のあるクライアントパソコンや，不正操作が行われているクライアントパソコンへの対処をサポートする。

トパソコンの資産情報（セキュリティパッチ適用情報，ウイルスパターン適用情報，ソフトウェアインストール情報など）を基に，規定されたセキュリティポリシーへの適合状況を危険，警告，注意，および安全の4段階で把握し，適合していないクライアントパソコンに対しては，そのぜい弱性に応じて警告メッセージの送信や，利用制限（ネットワークの切断）などの対処を行う。これにより，クライアントパソコンへのセキュリティポリシー適用を徹底し，セキュリティを確保するとともに，クライアントパソコンのセキュリティライフサイクル管理を実現し，管理コストを低減する。

また，JP1ソフトウェア配布・資産管理ではクライアントパソコンの操作履歴についても収集しており，システム管理者はクライアントパソコンの操作内容を把握し，不正操作が行われているクライアントパソコンへの警告メッセージ送信や，JP1クライアントセキュリティ管理を使用した利用制限を行うことができる。これにより，問題のあるユーザーへの警告や，不正な操作・行動を防止することが可能となる（図5参照）。

4 次世代のセキュリティライフサイクル管理ソリューション

情報漏えいやウイルス感染の被害拡大はシステム形態の変遷に起因しているため，サーバ ベースト コンピューティングなど，新しいシステム形態に移行した場合，新たなセキュリティ脅威が想定される。その対策としては，日立製作所のトータル セキュリティ ソリューション“Secureplaza[1)]”とともに，JP1セキュリティライフサイクル管理ソリューションを提供していく。

5 おわりに

ここでは，クライアントパソコンのセキュリティライフサイクルに関するセキュリティポリシー運用の具体化の方法を中心に，JP1セキュリティ管理について述べた。

日立製作所は，今後も企業システム全体のセキュリティを確保し，顧客のビジネスを確実に支える製品を提案していく考えである。

参考文献

1）金野，外；セキュアなサービスプラットフォームを実現するセキュリティソリューション“Secureplaza”，日立評論，**86**，6，437～442（2004.6）

執筆者紹介

豊田英樹
1991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ウェア設計部 所属
現在，JP1セキュリティ製品の開発に従事
E-mail：h_toyoda @ 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ウェア設計部 所属
現在，JP1セキュリティ製品の開発に従事
E-mail：taka_so @ 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6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，
日本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