# セキュリティ手順統制を行うセキュリティ運用管理システムの構築と評価

鷲尾　元太郎　　山田　耕一　　近藤　誠一

三菱電機株式会社

## 1　はじめに

### 1.1　背景

PC の普及やインターネットによる情報流通の利便性が向上する一方，個人情報保護法の全面施行や，機密情報の漏洩による賠償問題など，企業や団体におけるセキュリティ対策はますます重要になってきている．しかし，現状ではセキュリティ管理者の作業負荷やスキル不足，管理コスト等の課題があり，厳密にセキュリティ運用を行えていない．そこで，これらを解決するために IT によるセキュリティ運用自動化を行うセキュリティ運用管理システムが提案されている．[1] [2]

一般的なセキュリティ運用管理システムの構成を図 1 に示す．セキュリティ運用管理システムは一般利用者の PC など監視対象端末からセキュリティに関連する情報を収集し，あらかじめセキュリティ管理者により入力されたセキュリティポリシー情報や，資産情報からセキュリティポリシー監査を実施する．また，セキュリティ監査情報はセキュリティ管理者に通知されるだけでなく，自動の是正実行なども可能なシステムも提案されている．[1]

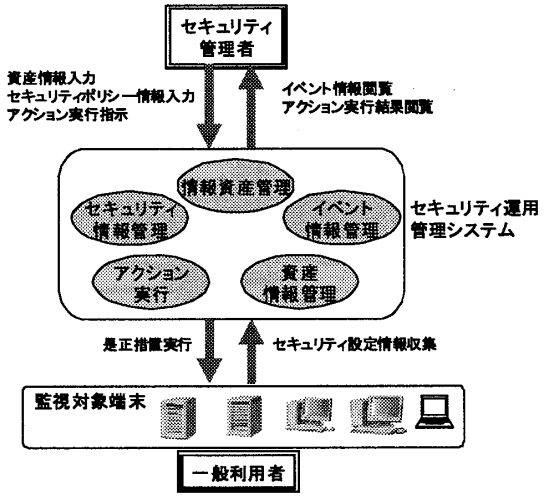


図1 一般的なセキュリティ運用管理システム

Construction and Evaluation of Information Security Management System for Security Procedures Governance.
G.Washio, K.Yamada and S.Kondo
Mitsubishi Electric Corporation

### 1.2　セキュリティ手順監査

組織のセキュリティ規則や ISMS 等の規則には，セキュリティ設定について規定されている訳ではなく，運用手順で定義されるセキュリティ項目も存在する．しかし，従来のセキュリティ運用管理システムでは，これら運用手順について監査することができないという課題があった．

そこで，本稿では上記課題を解決することを目的とした，セキュリティ運用手順について監査が可能なセキュリティ運用管理システムを構築した．また，セキュリティ手順についても管理が必要な会社資産 PC 外部持出しワークフローに本運用管理システムを適用し，評価を行った．

## 2　セキュリティポリシー

セキュリティ手順統制を実現するために，図 2 に示す通りセキュリティポリシー情報を概念ポリシー，設定ポリシー，手続きポリシーの 3 種類に分類した．

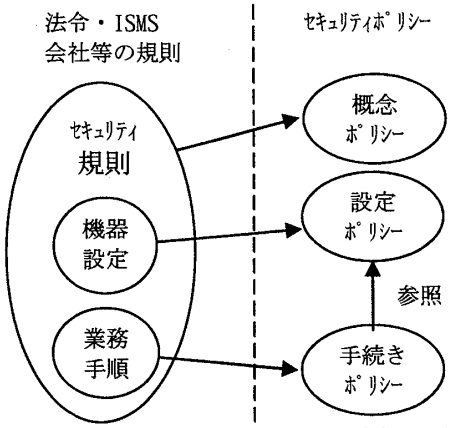


図2 セキュリティポリシーの分類と関係

(1) 概念ポリシー

社内規則や運用手順等の文書として管理されている規則を，本システムで扱えるように記述したもの．

(2) 設定ポリシー

規則のうち，PC の設定，インストールすべきソフトウェア等，管理対象としてあるべき機器の設定を，コンポーネント統制技術で監視できるように記述したもの．

(3) 手続きポリシー

規則のうち，手順で示されるものをコンポーネント統制技術で実行できる形式に記述したもの．手順を実行するワークフローでのプログラム実行，設定ポリシーが遵守されているかどうかを確認するための設定ポリシーの参照，承認ルート，KPI(Key Performance Indicator，起票から承認までの期限などの重要評価指標)を記述する．

従来のセキュリティ運用管理システムでは，概念ポリシーと設定ポリシーに相当するものをセキュリティポリシーとして管理してきたが，本運用管理システムでは手続きポリシーを導入することで，新たにセキュリティ手順統制を実現した．

## 3 セキュリティ手順統制の適用例

### 3.1 システム構成

外部へ持ち出す企業機密情報の内容について管理職の承認が必要などの業務プロセスを規定している場合や，持ち出す機密情報の暗号化の確認，持ち出すPCのウイルスチェックを手作業で行っている場合がある．しかし，これらの業務プロセスは人の手で行うもののため，チェック漏れによる漏洩が発生する可能性がある．また，従来使用しているワークフローを利用して管理職の承認を行った場合においても手作業でのチェックが必要となるなど作業負荷が高くなる問題がある．

そこで，今回セキュリティ手順統制を可能とするセキュリティ運用管理システムを構築した．

構築したシステムの構成を図3に示す．

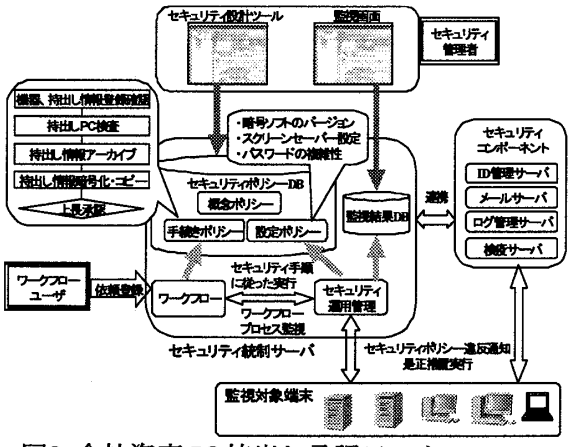


図3 会社資産PC持出し承認ワークフロー

セキュリティ統制サーバは，従来のセキュリティ運用管理機能である管理対象端末のセキュリティ設定の自動監査機能に加え，セキュリティ手順を実施するワークフロー機能を備える．ワークフロー機能がセキュリティ運用管理機能と連携することにより，前章で述べたセキュリティポリシー情報の設定ポリシー，手続きポリシーの実行を可能としている．

### 3.2 適用評価

従来のセキュリティ監査システムでは，監視対象端末や監査を行うサーバ負荷などの課題から多くても1日に1回セキュリティ自動監査を行っていることが多い．しかし，今回の会社資産外部持ち出しワークフローと連携するシステムでは，出張時など緊急を要することが多く，リアルタイム監査の実施が必要である．

そこで，本ワークフローでは，以下のように監査項目ごとに重み付けを行うことで，これらの課題を解決した．

・30分に1回の頻度で収集する項目
・1ヶ月に1回の頻度で収集する項目
・リアルタイムに収集して監査を行う項目

今回適用を実施した会社資産PC持出し承認ワークフローでは、すべての監査項目をリアルタイムに実施する必要がないため、上記重み付けにより実現することが可能であったが、今後セキュリティ漏洩リスク低減のためにより厳密にリアルタイムに監査することが要求されることが想定される。今後は可能な限り高速にセキュリティ監査を行うエージェントの開発などを通して，より完全なセキュリティ監査を実現する予定である．

## 4 おわりに

本稿では，セキュリティ手順統制を行う機能を追加したセキュリティ運用管理システムを構築し，会社資産PC持出しワークフローに実際に適用・評価を行った．その結果，ワークフローと連携することにより，会社資産PC持出しワークフローなどにおいて従来のPCセキュリティ設定情報の収集に加え，業務手順についてのセキュリティ監査を実施することが可能であることがわかった．今後はさらに適用対象を拡大し，さらなる評価を実施していく予定である．

## 参考文献

[1] 國分，他：情報セキュリティガバナンス確立に向けたセキュリティ運用の自動化，電子情報通信学会 2006 総合大会講演論文集，A-7-16，2006

[2] 國分，他：情報セキュリティマネジメントの IT 化によるセキュリティレベルの維持と PDCA サイクルの実現，情報処理学会研究報告 Vol.2007, No.16(20070301) pp. 453-458