

遠藤 淳\*  
(Jun Endo)  
鈴木 博\*\*  
(Hiroshi Suzuki)  
近藤 誠一\*\*\*  
(Seiichi Kondou)  
相浦 利治\*\*\*  
(Toshiharu Aiura)  
今井 功\*\*\*  
(Isao Imai)

# 情報セキュリティガバナンスを確立する セキュリティマネジメントソリューション

Security Management Solution for Information Security Governance

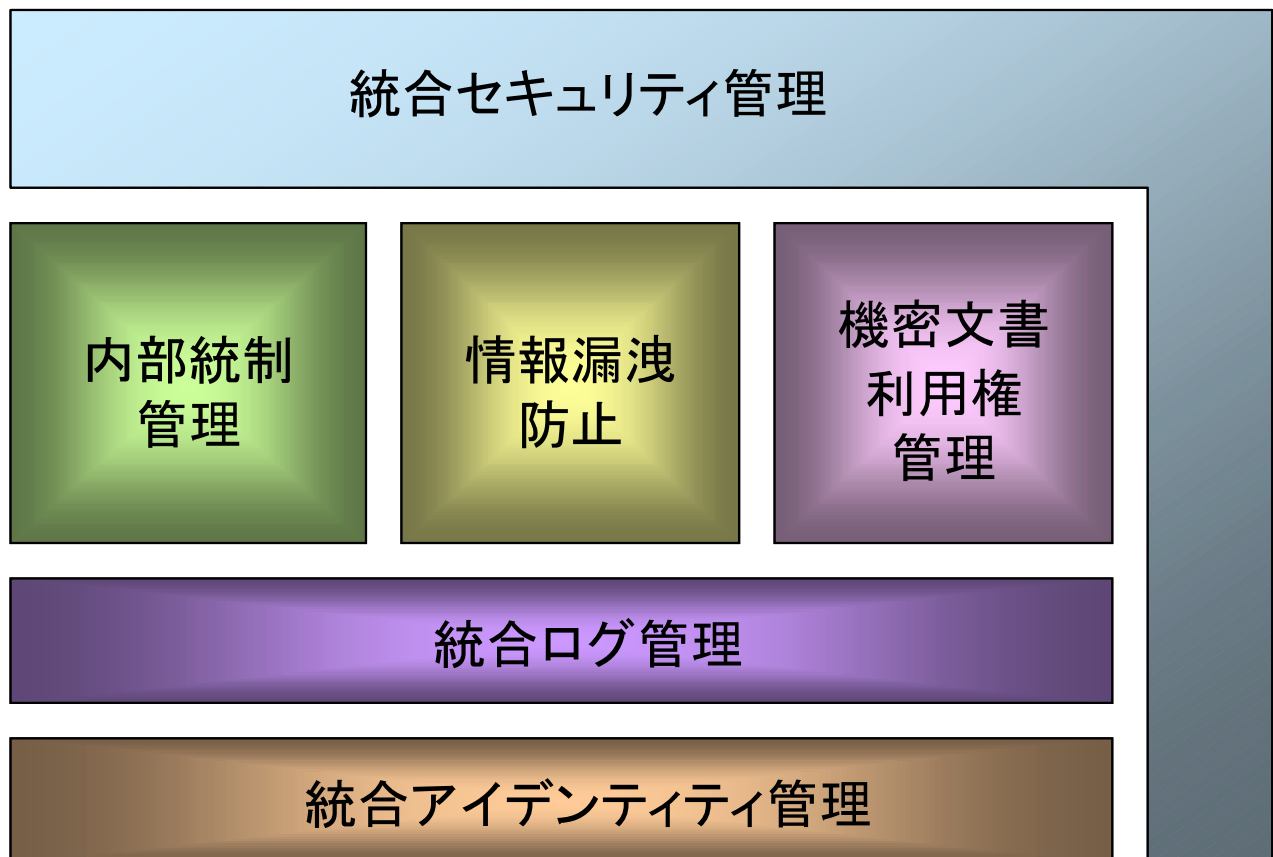
## 要 旨

事業活動における IT への依存度が増大しており、機密漏洩や不正アクセス、システムダウンなどの IT 事件・事故は企業経営に直結するリスクとして認知され始めている。特に企業の営業機密である個人情報が大量に流出する事件が多発する中、個人情報保護法の施行により、ファイル暗号やアクセス制御など、情報セキュリティ対策を導入する企業が急増している。

情報セキュリティでは安全性のレベルを維持・管理するために、技術的なセキュリティ対策と同時に情報セキュリティポリシーに基づいた PDCA(Plan Do Check Action)サイクルを継続的にまわすセキュリティ運用管理を実施する必要がある。セキュリティマネジメントソリューションは、

このセキュリティの運用管理に関わる作業を IT 化することで、高信頼で安全なセキュリティ運用環境（情報セキュリティガバナンス）を確立する。

セキュリティマネジメントソリューションでは、情報漏洩防止、文書のコンテンツ管理による内部統制管理、機密文書利用権管理などと、各種セキュリティ対策で必要となるユーザー及びユーザーに割り当てられるアクセス権の管理（統合アイデンティティ管理）やユーザーのアクセス履歴の管理（統合ログ管理）が連携する。また、セキュリティ監査及び是正・予防処置の検討を行うセキュリティ点検とを組み合わせることで、統合セキュリティ管理による PDCA サイクルを実現している。



## 三菱電機グループのセキュリティマネジメントソリューション

セキュリティマネジメントソリューションは、PDCA サイクルを実現するセキュリティ運用管理の作業を IT 化することにより高信頼で安全なセキュリティ運用環境を提供する。

\* 三菱電機（株）インフォメーションシステム事業推進本部  
\*\* 三菱電機インフォメーションシステムズ（株）  
\*\*\* 三菱電機（株）情報技術総合研究所

## 1. ま え が き

PC(Personal Computer)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(2005年4月)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。主要なセキュリティ対策として、PCへのセキュリティツールの導入や、情報セキュリティマネジメントシステム ISMS (Information Security Management System) <sup>(1)</sup>の実施などが行われているが、運用でのPDCAサイクルによるセキュリティレベルの向上が困難であるといった課題が報告されている。

三菱電機グループでは、情報セキュリティガバナンスを確立するセキュリティマネジメントソリューションを開発しており、本ソリューションによって、セキュリティ運用の”快適・安心・発展”を実現する。

## 2. 背景・課題

セキュリティ管理を担当している顧客や情報システム部門の担当者にヒアリングを行った結果、現状のセキュリティ運用に次のような課題を抱えていることが分かった。

- セキュリティに関する資産情報の棚卸や維持管理、

大量のPCに展開したセキュリティツールの設定変更作業の負荷が高い。

- 職制に応じたアクセス権を設定したいが、人事異動や組織変更への対応が困難で、厳密に設定できていない。
- セキュリティ監査業務(運用ルールや記録の調査、監査基準に基づく評価、報告書の作成)を行うためのスキルやノウハウが不足している。

これらの課題の主な要因は、セキュリティ運用のための作業負荷や、セキュリティ管理に対する専門知識の不足である。対策として、人的リソースの投入やコンサルタントの導入が考えられるが、管理コストの増加につながるため、そこまで至っていないのが現状である。

## 3. セキュリティマネジメントソリューションとは

### 3.1 概要

三菱電機グループが提供するセキュリティマネジメントソリューションの全体像を図1に示す。本ソリューションは、ISMSで規定されたPDCAサイクルの各フェーズで行う作業を支援する7つの機能から構成されている。

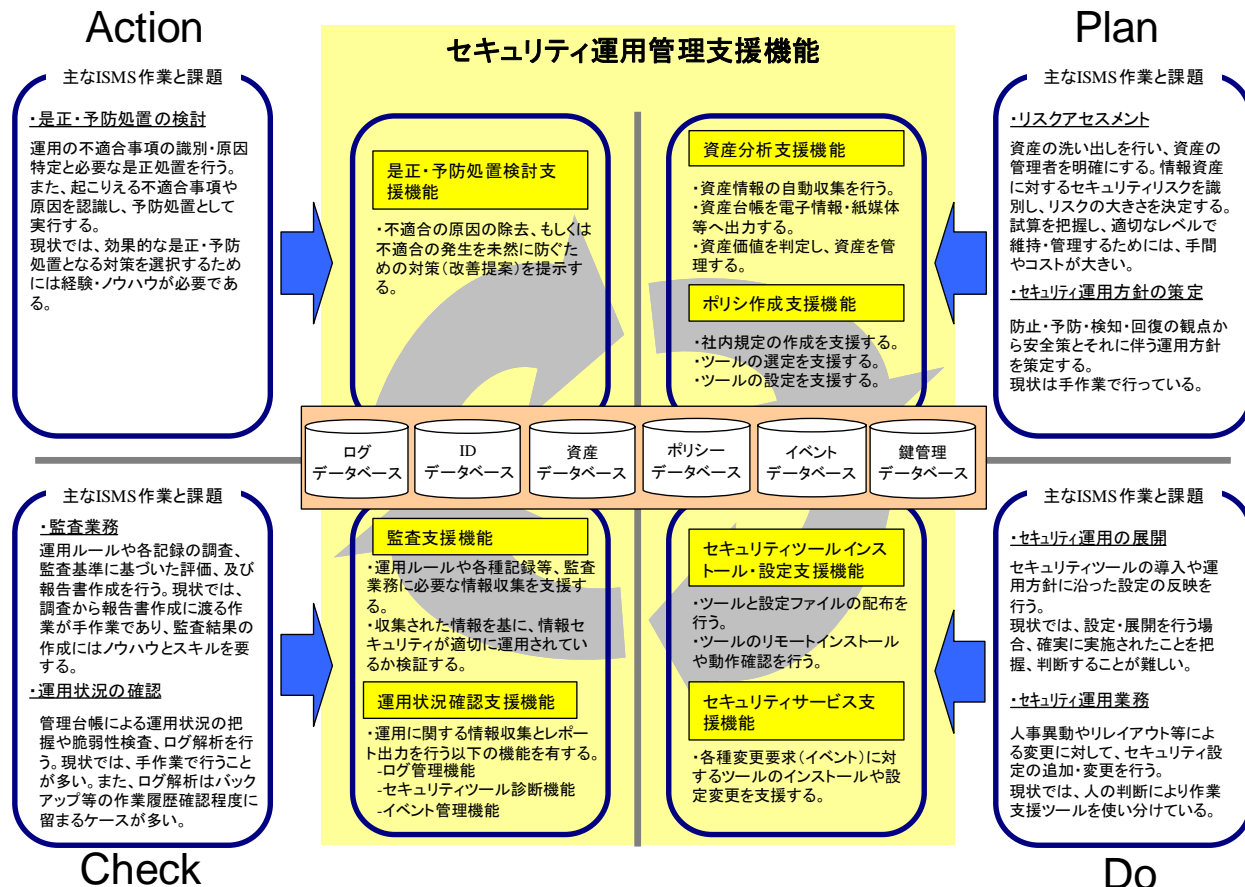


図1. PDCAサイクルの実現に向けてセキュリティマネジメントソリューションが提供する機能

各機能は、個別に収集・管理されている資産情報、ID情報、ポリシー情報、イベント情報、ログ情報を PDCA の全サイクルにおいて共有・管理・活用することで、安全性の高い効率的なセキュリティ運用環境の提供を目指すものである。

### 3. 2 セキュリティ運用管理

セキュリティ運用管理は、図2に示すように PDCA サイクルにおける Plan, Do, Check の作業を IT 化することで、セキュリティ管理者に対して“快適”なセキュリティ運用を提供する。

- (1) Plan : セキュリティに関わる資産情報、PC のセキュリティ設定、情報資産の機密度などをデータベース化し、Web ブラウザからの操作やネットワーク経由での自動収集により、管理作業を支援する。
- (2) Do : ログ管理サーバやワークフローシステムから、資産登録/ポリシー変更/人事異動/リレイアウトなどをイベントとして入力し、各々のイベントに対するアクションとして、PC に対するセキュリティツールの配布や関連データベースの変更処理を実行し、PC に対する設定作業や変更管理作業を支援する。
- (3) Check : PC や機密情報の持ち出し申請と同期して、PC の設定や持ち出し資料の暗号化状況などを自動的に確認。結果をセキュリティイベントとしてデータベースで一元管理し、セキュリティ管理者に報告する。

セキュリティ運用管理は、資産やポリシーといったセキュリティ情報のデータベース化による一元管理と、それらに基づいたセキュリティ運用の展開及び運用状況の確認作業の IT 化によって、セキュリティ管理者の負担を削減しつつセキュリティ運用の機密性、完全性、可用性を実現する。

## 3. 3 ID 管理

### 3. 3. 1 ID 統合管理

ID 管理では、計画にて作成されたポリシーのうち、ユーザー及びユーザーに割り当てられるアクセス権の管理を行う。個々の脅威に対応した対策システムを個別に導入すると、ID 管理に関して、次の課題が生じる。

- ・ 複数の対策システムで利用する ID の整合性・セキュリティ強度の維持

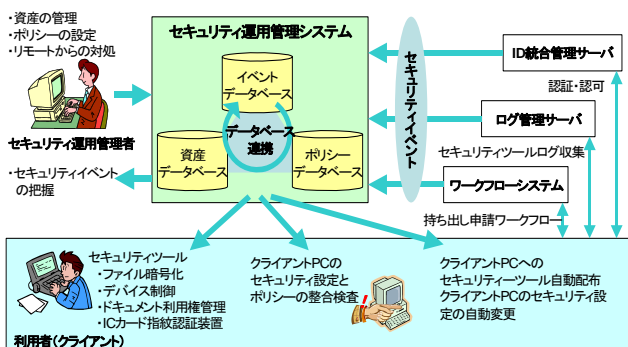


図2. セキュリティ運用管理

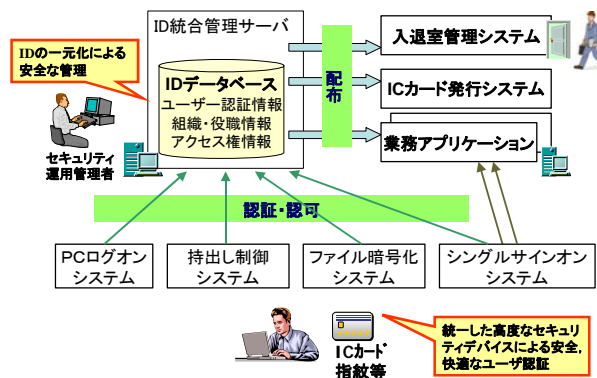


図3. ID管理の構成

- ・ 利用者の認証手段の統一による利便性向上

本 ID 管理では、図3に示すように、ユーザー情報、アクセス権といった ID をデータベース、ディレクトリで統合管理し、“安心”で“快適”なユーザー認証・認可を実現する。ID は、入退室管理システム、IC カード発行システム、業務アプリケーションなどに配布される。また、ID を、LDAP (Lightweight Directory Access Protocol)、AD(Active Directory<sup>(注1)</sup>)で管理し、PC ログオンシステム、持ち出し制御システム、ファイル暗号化システム、Web 業務アプリケーションシングルサインオンシステムなどにおけるユーザー認証、アクセス権に従った認可に利用する。

### 3. 3. 2 ID ライフサイクル管理

ID 管理は、“発展”のため、システム導入後、以下の2種類のライフサイクル管理が必要となる。

- (1) アクセスポリシーのライフサイクル  
セキュリティ対象の追加削除、PDCA サイクルを経たポリシー改善による変更
- (2) ユーザー情報のライフサイクル  
入社、退職、異動、昇進、組織変更といったアクセス制御の基になるユーザー属性の変更

本 ID 管理ではロールベースアクセス制御 RBAC (Role-Based Access Control)モデル<sup>(2)</sup>を基に組織を独立させた拡張及び変更履歴管理を行うことにより、事業継続性を実現する<sup>(3)</sup>。PDCA サイクルの各段階において、以下に示す処理を行う。

- (1) Plan : セキュリティ対象のアクセスが許可されるユーザーの集合としてロールを定義し、その設定を行う。
- (2) Do : ユーザーのライフサイクルに従って、ロールへのユーザーの設定、変更を行う。
- (3) Check : 過去のログに含まれるユーザーID を補足するため、変更履歴を含めた ID 情報を提供する。

### 3. 4 セキュリティ点検システム

コンピュータウイルスや不正アクセスなど、情報システムに対する脅威は日々変化している。企業や団体などの組織が、有効かつ効率的に事業活動を遂行するためには、情報セキュリティの維持確保が不可欠であり、定期的な監

(注1) Active Directory は、米国 Microsoft Corporation の米国及びその他の国における登録商標である。

査により情報システムを継続的に検証する必要がある。

セキュリティ点検システムは、図4に示すように、PDCA サイクルにおける Check, Action を実践するために必要な作業を支援する。また、本システムによる継続的な検証を通じて、情報セキュリティ対策を段階的に向上させることを目的とする。

#### (1) 事前調査機能

組織におけるセキュリティ運用ルールや同ルールに対する実施状況を効率的に調査する手段として、チェックリスト形式による調査機能を提供する。ここで得られた運用ルールを基に、組織におけるセキュリティ対策状況を監査するために必要な評価基準を設定する。また、情報システムの実態を調査するため、各種セキュリティツールと連携し、アクセス記録、入退室記録、脆弱性診断情報などの運用記録や、資産管理情報、システム設定情報、ユーザー管理情報などの管理情報を収集する。収集された情報は、定期的な監査に活用するため監査データベースに集積する。

#### (2) 監査報告機能

セキュリティ監査では、上記で設定された評価基準に従い、収集された運用実施状況や運用記録を参照し、情報セキュリティの状況を自動的に評価する。また、監査データベースに集積された過去の監査結果と比較することにより、セキュリティレベルの向上性についても評価する。報告書作成では、監査レポートのテンプレートに従い評価結果を入力し、監査レポートを自動的に作成する。是正・予防措置となる改善提案は予め監査データベースに登録しておき、評価結果で不適合となる問題点が検出された場合には、データベースから対応する改善提案を抽出し、監査レポートに追記する。

#### (3) セキュリティポリシー作成支援機能

セキュリティ運用管理システムによるセキュリティポリシー作成のため、是正・予防措置（改善提案）を活用する連携方式を実現する。

### 4. 機密情報持ち出し管理への適用

PC や機密情報を持ち出す場合、担当者が所定の様式に PC の管理番号／持出情報／目的などを記載し、職制管理

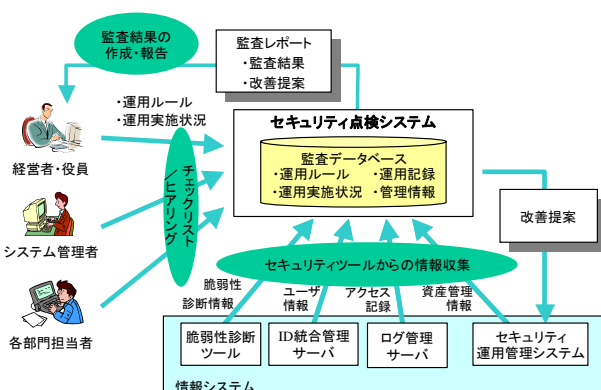


図4. セキュリティ点検システムの構成

者の検印を受けた後に、エビデンスとして保管する方法が一般的であり、ワークフローシステムの導入によってペーパーレス化を図ることができる。しかし、持ち出すPCのセキュリティツールの設定や、機密情報の暗号化処理などの状況について、管理者が1台1台確認を行うことが困難であることから担当者に一任されており、セキュリティの完全性の観点からは十分とはいえない。このような機密情報持ち出し管理に、セキュリティマネジメントソリューションを適用した場合、以下のような効果がある。

- (1) 持ち出し申請のあったPCのセキュリティツールが持ち出し可能な設定となっているか、また、機密情報が暗号化されているかを自動的に確認することで、セキュリティ運用の完全性を確保し、管理者の確認作業負担を低減する。
- (2) 機密情報と持ち出し申請をした担当者のアクセス権限をID管理によって確認することで、権限に沿った機密性の高い情報管理が可能となる。
- (3) PCや機密情報の持ち出し頻度、返却手続きの期限遅れ状況などを基に監査レポートを提供し、PDCAサイクルによる改善活動に繋げていくことができる。

## 5. むすび

情報セキュリティガバナンスを実現するためには、運用のための作業負担の軽減、セキュリティ管理に対する専門知識が必須であり、三菱電機グループでは、これらをIT化したセキュリティマネジメントソリューションを提供することで、セキュリティ運用の“快適・安心・発展”を目指している。今回紹介した技術の一部は、現在製品化に向けて開発中のものも含まれており、使いやすいインタフェースや高品質化を実現し、一日も早く市場に提供できるように開発を加速していく。

## 参考文献

- (1) (財)日本情報処理開発協会：“情報セキュリティマネジメントシステム (ISMS) 適合性評価制度”，<http://www.isms.jp/dec/index.html>
- (2) Ferraiolo, D. and Kuhn, R.: Role-Based Access Control, *Communications of the 15<sup>th</sup> NIST-NSA National Computer Security Conference* (1992)
- (3) 近藤誠一，ほか：ロールベースアクセス制御情報の多バージョン並行処理制御を利用した監査ログトラッキング手法，情報処理学会論文誌 TOD 28 (2005)