巻頭論文

情報セキュリティマネジメント基盤



茂木　強*　今井直治**　遠藤　淳***

IT Platform for Information Security Management

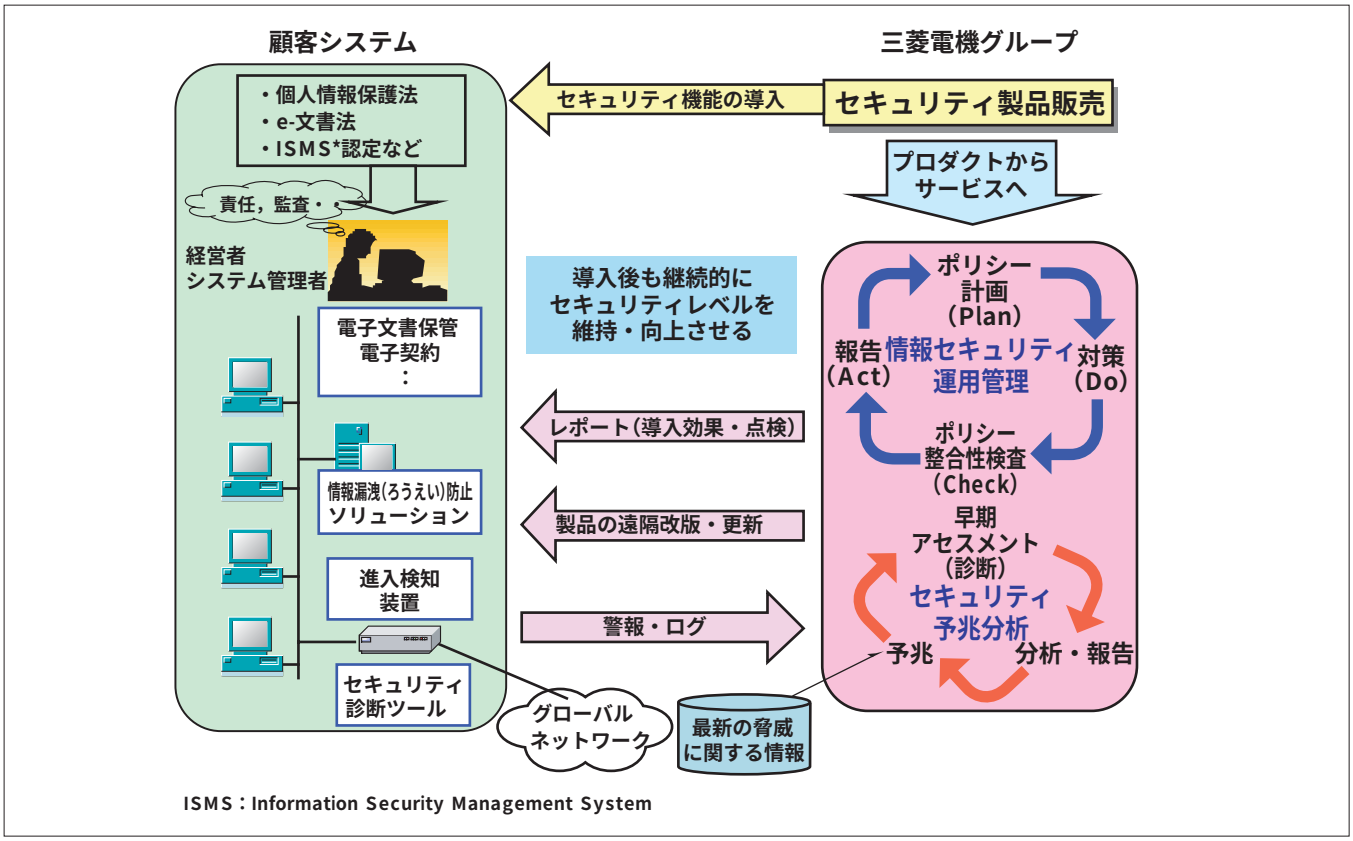
Tsuyoshi Motegi, Naoharu Imai, Jun Endo

要　旨

IT利活用の進展に伴い，情報セキュリティ対策の範囲が拡大している。また，新たなセキュリティ脅威は年々増加・多様化の一途をたどっている。このように環境が変化し続ける状況においては，個別のセキュリティ製品を導入しただけでは対策として十分でなく，導入後も継続的にセキュリティレベルを維持する仕組みを構築することが重要な課題となっている。

本稿では，環境の変化を企業・社会の内部と外部とに分けて考えている。内部の変化への対応として，情報システムを構成する“モノ”やソフトウェアの変化を許容するポリシーベースセキュリティ運用管理機能，“ヒト”・組織の変化を許容するロールベースのアイデンティティ管理機能及びそれらの変化を漏れなく記録する大容量ログ機能について述べる。また，外部の変化への対応として，セキュリティリスクの予兆を捕捉してプロアクティブな対応を可能とするセキュリティ予兆分析システムについて述べる。

三菱電機グループでは，情報セキュリティ及び物理セキュリティを体系化し，トータルなセキュリティソリューションを提案してきた。本誌2004年４月号で“情報セキュリティ技術”を，同年８月号で“物理セキュリティ技術”を，2006年４月号で“情報セキュリティマネジメントソリューション”を述べてきたが，今回の特集では，情報セキュリティの継続的な維持向上を顧客へのサービスとして提供するための“情報セキュリティマネジメント基盤”について，全体的な考え方と，個別のソリューション，サービス，コンポーネント技術について述べる。



情報セキュリティマネジメント基盤の全体構成

情報セキュリティの脅威は日々進化増大するため，企業や社会の情報システムは，そのセキュリティレベルを常に維持・向上させるための仕組みを必要としている。この特集で述べる情報セキュリティマネジメント基盤は，ポリシーに基づきセキュリティ運用のPDCAを支援するセキュリティ運用管理機能と，攻撃の予兆と対策の提示を行うセキュリティ予兆分析機能とから構成され，顧客システムのセキュリティレベルの継続的な維持・向上に寄与するものである。

*情報技術総合研究所 情報ネットワークシステム部長　**インフォメーションシステム事業推進本部 新事業開発プロジェクト グループマネージャー　***同本部 情報セキュリティ推進センター長