情報システムセキュリティ（2）情報システム基盤からの取り組み

黒田清隆*　今井　功*
安田　忍*
柳瀬賢治*

Introduction to Information System Security Infrastructure in Mitsubishi Electric Group

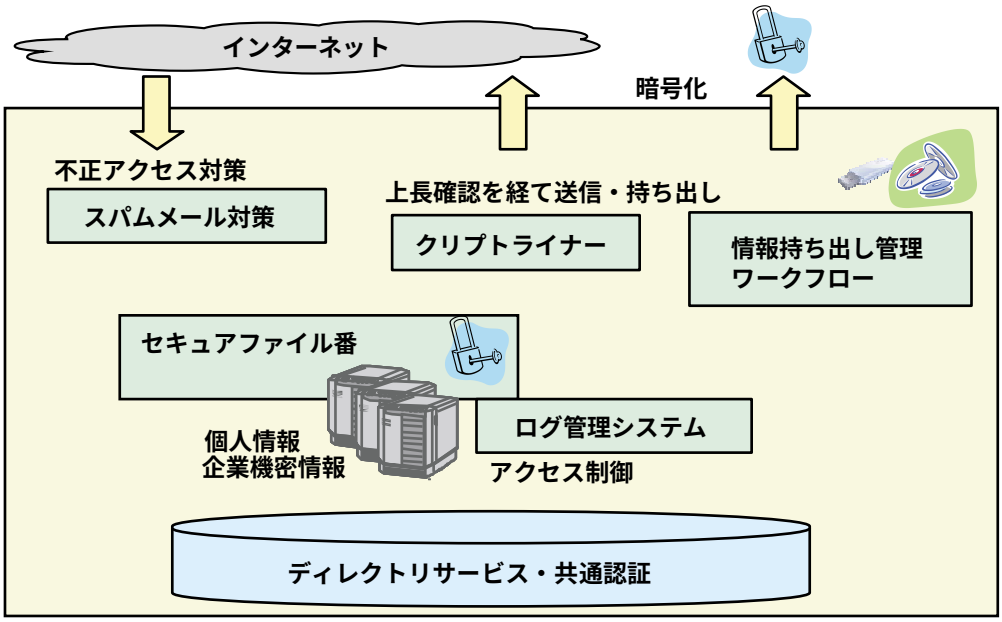
Kiyotaka Kuroda, Shinobu Yasuda, Kenji Yanase, Isao Imai

要　旨

近年，ITの発展によって情報のデジタルデータ化と蓄積が進み，情報システムによるデータ活用やネットワークによる即時大容量の伝送がもたらす利便性は，企業活動に不可欠なものとなっている。一方で，情報のデジタルデータ化は，大量のコピーを容易に生み出し，また，ネットワークや小型ポータブルメディアの発達によって，企業外部へ大量の情報を容易に持ち出すことが可能な状況を現出してきた。このような状況下で，情報漏洩(ろうえい)対策は企業にとって重要な経営課題としてクローズアップされ，情報管理のあり方から，情報システム上の具体的な対策まで見直しがなされてきた。

三菱電機は，個人情報保護，及び企業機密管理のため適切な安全管理措置を講じており，特に技術的対策では情報システムが重要な役割を担っている。

本稿では，当社の情報システム基盤における情報セキュリティの主要な取り組みについて述べる。まず，情報セキュリティで基本となるアクセス制御を適切に運用していくためのユーザーID管理とログ管理について触れ，企業機密情報の社外への漏洩を防ぐための情報システム基盤での取り組みをいくつか述べる。１つは情報の持ち出しに関するルールと運用の徹底を図るためのワークフローシステム，次に，社外へのデータ送信に関するルールとそれをサポートするシステムの事例，３つ目は厳格な管理が必要な文書に関して利用権付暗号を適用したシステム事例である。最後に，ネットワーク基盤における近年の取り組みを述べ，今後の方向について考察する。



情報システム基盤における主要な取り組み事例

①ログ管理システム：ファイルサーバの機密情報へのアクセスログ管理と不審利用検知を行う。②情報持ち出し管理ワークフロー：ポータブルメディア等に格納した情報を社外へ持ち出す際の上長承認を行うワークフローシステム。③クリプトライナー：大容量データの社外への送信を安全に行う。④セキュアファイル番：利用権付暗号を利用しOA文書の保護を行う。⑤スパムメール対策：メール受信時にスパムメールを遮断する。