情報セキュリティガバナンスシステム

近藤誠一* 佐伯保晴***
撫中達司** 遠藤 淳***
鶴川達也*

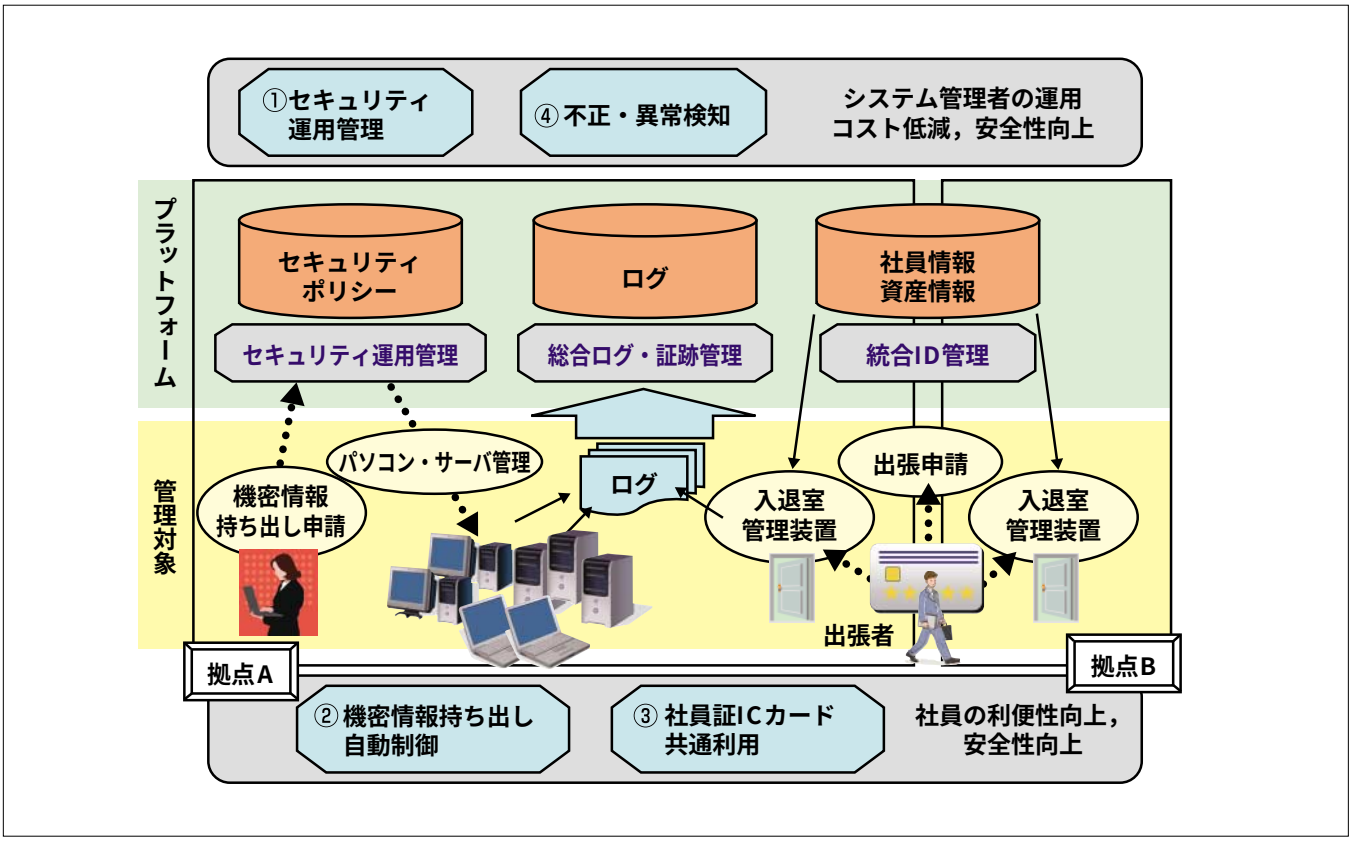
Information Security Governance System

Seiichi Kondo, Tatsuji Munaka, Tatsuya Tsurukawa, Yasuharu Saeki, Jun Endo

要 旨

増加・多様化するセキュリティ脅威によるデータ破壊や情報漏えい事故など，情報セキュリティ対策の不備が原因で被る経済的な損害は，社会的責任も含めると膨大なものになる。一方で，2005年に個人情報保護法，2006年に会社法，金融商品取引法が施行され，コンプライアンス経営が，企業にとって不可欠な課題となっている。しかし，そのための技術的な対策が人に依存している限り，周知・教育だけでは徹底は難しく，継続的にセキュリティを維持・向上していくためには，体系的な統制が有効であると考えられている。そこで，セキュリティ統制で必要とされるセキュリティポリシー，社員情報・資産情報，ログをデータベース化して集中管理し，セキュリティ運用管理技術，統合ID管理技術，統合ログ・証跡管理技術を適用した情報セキュリティガバナンスシステムを三菱電機のモデル地区に構築し，その検証を行った。

システム構築の結果，①パソコン・サーバのルール適合性チェック自動化によるシステム管理者の運用コスト低減，安全性向上，②機密情報の外部持ち出し時の社員の利便性向上，安全性向上，③出張先での本人の社員証ICカードを使用した入退室による社員の利便性向上，安全性向上，④異種ログの組み合わせ分析による不正・異常検知，といった効果が得られた。このシステムの構築・運用ノウハウを今後のセキュリティシステム構築に活用していく所存である。



情報セキュリティガバナンスシステムのモデル地区適用全体構成

①セキュリティ運用管理：資産情報として管理されるパソコン・サーバを対象にセキュリティポリシーの管理実施支援，監査，是正を行う。
②機密情報持ち出し自動制御：セキュリティポリシーで定められた持ち出し手順に則って許可された資産の持ち出し，証跡管理を行う。
③社員証ICカード共通利用：セキュリティポリシーで定められた出張先入場承認手順に則って別拠点の入退室装置に社員証情報を配布する。
④不正・異常検知：多様なログ，外部持ち出しファイルを集中管理し，社員情報，資産情報を補って追跡し，セキュリティポリシー違反を検知する。

*情報技術総合研究所 **同研究所(工博) ***本社