ITセキュリティ評価基準ISO/IEC15408と三菱電機グループの取り組み

泉　幸雄*
森垣　努**
山本俊輔**

ISO/IEC15408 IT Security Evaluation Criteria and Our Activities

Yukio Izumi, Tsutomu Morigaki, Shunsuke Yamamoto

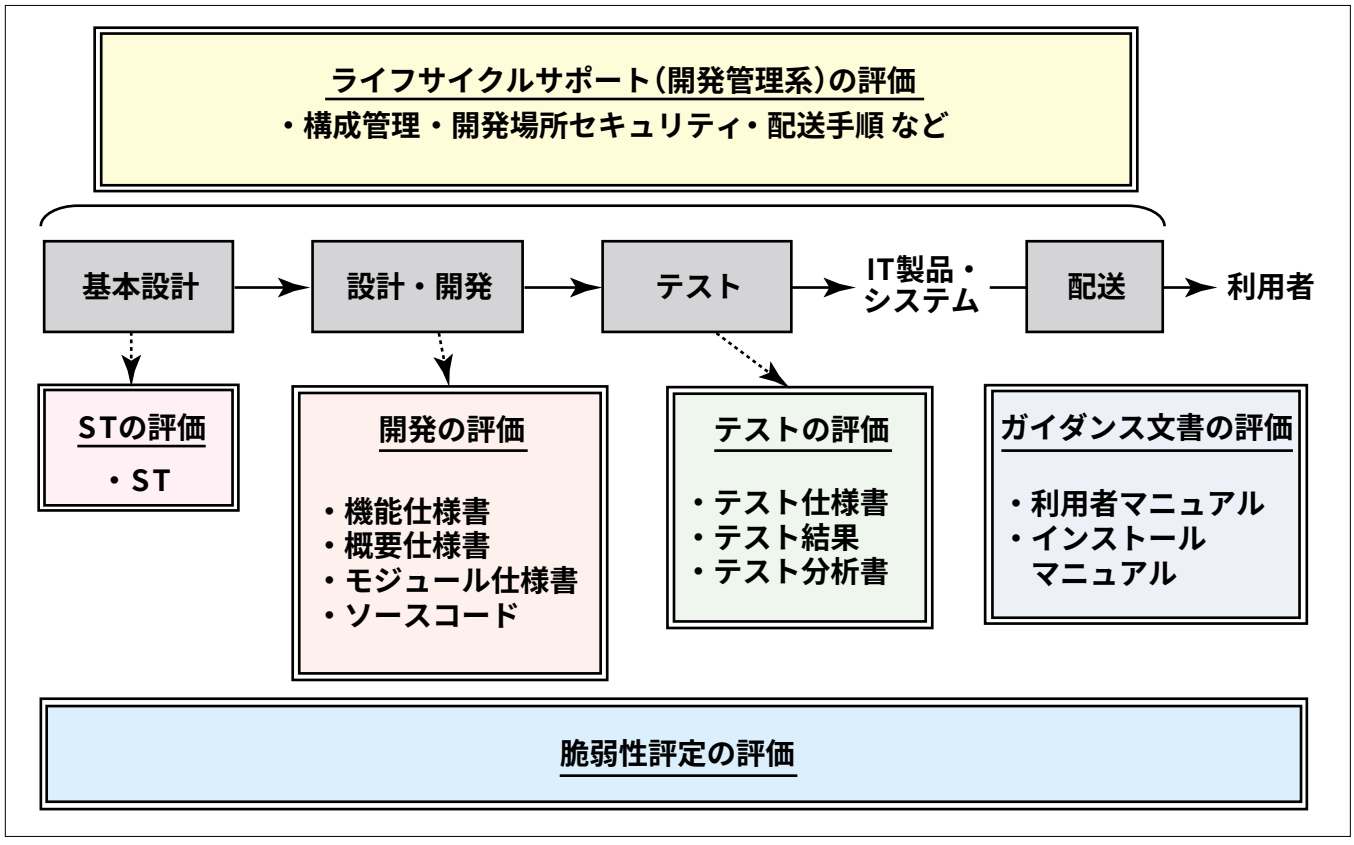
要　旨

近年，ITの普及とともに情報資産の価値が増加し，情報資産を扱うIT製品・システムのセキュリティの重要性が増している。このような状況で，IT製品・システムの利用者は，自分の環境に合ったセキュリティ機能を具備したものを多数の製品の中から調達する必要があるが，自らセキュリティ評価を行うことは多大のコスト・時間がかかるという問題点があった。また，IT製品・システムの開発者は，製品を幅広く販売したくても，それまで国ごとに運用されていたセキュリティ評価制度で，認証取得することはコスト・時間の面で問題があった。

このような背景のもと，公的に認められた第三者がIT製品・システムのセキュリティ評価をするための国際的統一基準CC（Common Criteria）が1999年に作られ，同年ISO/IEC（International Organization for Standardization/International Electrotechnical Commission）15408として国際標準化された。我が国でも，この評価基準を用いた第三者評価認証制度の運用が2001年４月から開始された。

ISO/IEC15408におけるセキュリティ評価はIT製品・システムを様々な側面から検査するため，セキュリティ基本設計書（ST），設計文書，マニュアル，開発管理文書等の証拠資料が必要となる。評価申請した開発者は，ISO/IEC 15408で規定された要件を満たし，所定の内容を含む証拠資料を評価機関に提出し，評価機関によって第三者評価が行われる。

本稿では，このITセキュリティ評価基準ISO/IEC15408及び三菱電機グループにおける取り組みについて述べる。



開発フローとISO/IEC15408評価の観点

図中，一重枠が開発フローを，二重枠が評価の観点を表す。ISO/IEC15408に基づく評価では，セキュリティ基本設計文書（ST），設計文書，テスト，マニュアルの評価のほか，開発管理にかかわる評価も実施される。また，評価者が独自に脆弱（ぜいじゃく）性分析を行う。評価形態には，開発者が提出した設計文書等の証拠資料の検査，サイト監査，テスト実施がある。ただし，評価保証レベルに応じて評価内容は異なる。

*三菱電機㈱ 情報技術総合研究所　**三菱電機インフォメーションシステムズ㈱