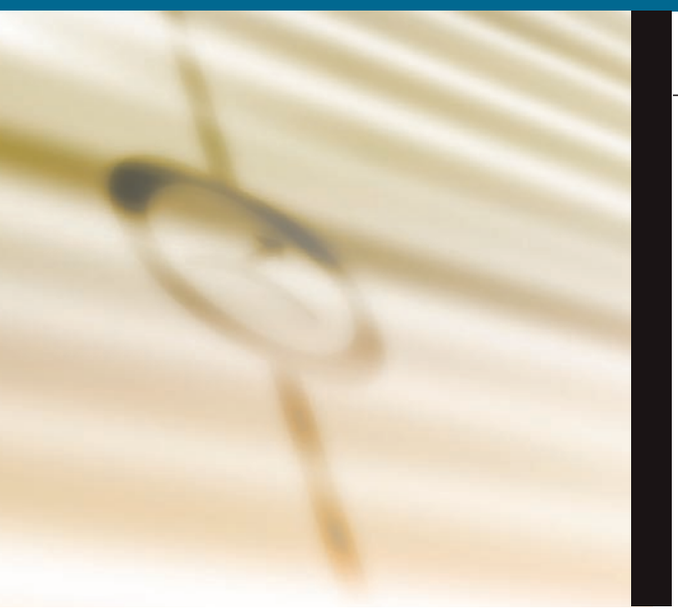
特集

情報セキュリティ研究開発の動向

1. 情報セキュリティの研究開発の動向
2. ミクロな分析技術の動向
3. マクロな分析技術の動向
4. 分析の結果に基づく対策技術の動向
5. インシデント対応におけるミクロ分析とマクロ分析の融合に向けて
6. セキュリティホールを作り込まない技術の動向
7. プライバシ保護のためのアーキテクチャ
8. プライバシ保護のための要素技術の動向



編集にあたって

村瀬一郎 （株）三菱総合研究所

本特集「情報セキュリティ研究開発の動向」では，主として文部科学省科学技術振興調整費重要課題解決型研究「セキュリティ情報の分析と共有システムの開発」を中心に取り上げた．

従来の情報セキュリティの研究開発は，暗号技術を中心に発展してきた．暗号技術およびその関連領域においては，問題を定式化し，定式化された問題に対して定量的な回答を得るというアプローチによって着実な発展を遂げ，我が国の暗号技術研究は世界的にも非常に高い水準になっている．

一方，現実世界の情報セキュリティ対策においては，セキュリティマネジメント，コンピュータウイルス，脆弱性，定点観測システム，セキュアプログラミング，プライバシ保護等々のキーワードが並び，これらの対策に関して定式化することは非常に難しい状況となっている．

こうした状況を鑑み，情報セキュリティインシデントの予兆の発見から対策立案，対策遂行，対策情報の流通という一連のプロセスに注目し，プロセス全体をあらかじめ想定した上で先進的なアーキテクチャの研究開発を目指したプロジェクトが，「セキュリティ情報の分析と共有システムの開発」である．

最初の記事「情報セキュリティの研究開発の動向」では，プロジェクト全体の概要紹介がなされている．2番目の「ミクロな分析技術の動向」は，コンピュータウイルスに代表される不正コードの収集，検出，分析からなる，不正コードの精緻な分析技術（ミクロな分析技術）の動向についての解説である．3番目の「マクロな分析技術の動向」では，定点観測システム，脆弱性データベース等からなる広域的な分析技術（マクロな分析技術）について述べている．4番目の「分析の結果に基づく対策技術の動向」においては，トレースバック技術，ネットワーク層でのアクセス制御，侵入防御システムなどの対策技術について紹介している．5番目の「インシデント対応におけるミクロ分析とマクロ分析の融合に向けて」では，本プロジェクトにおけるミクロ分析とマクロ分析の融合の内容や成果に触れ，今後の方向性を示している．6番目の「セキュリティホールを作り込まない技術の動向」においては，汎用的なセキュアプログラミング，セキュアなWebアプリケーション，セキュアプロトコル，セキュアな組み込みソフトウェアについて，本プロジェクトでの取り組みを中心に解説している．7番目の「プライバシ保護のためのアーキテクチャ」においては，本プロジェクトの成果として，アイデンティティアクセス管理の領域に対して，プライバシ保護，セキュリティ保全，コンプライアンスの3つの観点から，情報のライフサイクル，プロセスモデルなどを分析しシステム要件を導出し策定したプライバシ保護システムについて述べている．最後の「プライバシ保護のための要素技術の動向」においては，匿名署名技術，暗号化メール，分散認証技術，匿名性のあるIPモビリティ通信技術等を含むプライバシ保護のための要素技術を紹介している．

本特集では，「セキュリティ情報の分析と共有システムの開発」を中心に，情報セキュリティ研究開発の動向を俯瞰した．特集の執筆者およびプロジェクトの関係者の協力に深く感謝したい．また，本特集を起点に，情報セキュリティ技術の研究開発が進展すれば幸いである．

（平成19年6月19日）

