3.2.6　情報通信部門　セキュリティ高度化グループ

グループリーダー　中尾康二　ほか6名

セキュリティ高度化技術の研究開発

概　要

インターネットに代表されるサイバー空間の安全性及び信頼性を確保するための基礎技術、応用技術に関する以下の研究開発を実施する。

(1)　サイバー空間上で発生する各種攻撃に対する事前対策、インシデント対応、事後対策にかかわる総合技術の研究である「サイバー攻撃対策技術」の開発を行う。同技術の開発では、サイバー空間上で発生する各種攻撃に対する事前対策（予兆検知等）、インシデント対応（トレンド分析、緊急対策等）、事後対策（不正発信源の高度追跡等）にかかわる総合技術の研究開発を実施する。

(2)　サイバー空間上で実施される各種ビジネスを不正利用、サービス妨害などから保護するための高度なセキュリティ機能を具備したサービスプラットフォーム構築技術にかかわる研究開発として、「高度セキュアサービスプラットフォーム構築技術」の開発を行う。同技術の開発では、サイバー空間上で実施される各種ビジネスを不正利用、なりすまし、盗聴・改ざんなどから保護するための高度なセキュリティ機能を具備したサービスプラットフォーム構築技術にかかわる研究開発を実施する。

(3)　セキュアな利用者レベルのネットワーク応用基盤の構築にかかわる「コンテンツセキュリティ技術」の開発を行う。同技術の開発では、ユビキタス社会なども視野に入れた広範囲なアプリケーションにおけるコンテンツ利用の安全性（プライバシー、知的財産権等）を確保するための研究開発を実施する。

平成17年度の成果

- イベントログ分析では、分析エンジンの並列処理化、実時間処理化、視覚化処理及び詳細分析処理にかかわる実装、評価を実施した。具体的には、インシデント分析センターのβ版としてnicter（Network Incident analysis Center for Tactical Emergency Response）を構築し（図1）、観測トラヒックにおけるインシデントの自動検出を行う実時間分析モジュール群、検出されたインシデントの詳細を解析するための詳細分析モジュール群、さらに、観測トラヒックをオペレータが直感的に把握するためのトラヒック可視化モジュール群（図2）を組み込んだ。
- 高度セキュアサービスプラットフォームの構築では、経路制御に着目したセキュアオーバーレイ技術に係るプロトタイプシステムの構築と評価を実施し、機能的な実現性の目途を得た。
- コンテンツセキュリティでは、プライバシー付き認証機能具備のRFIDフレームワークを試作し、機能検証を実施した。自然言語テキスト及び音声信号に秘匿情報を埋め込む手法の方式設計、試作・検証を実施した。
- 外部との連携により、不正コード影響度解析技術とアプリケーショントレースバック技術の試作装置を開発し評価を実施した。

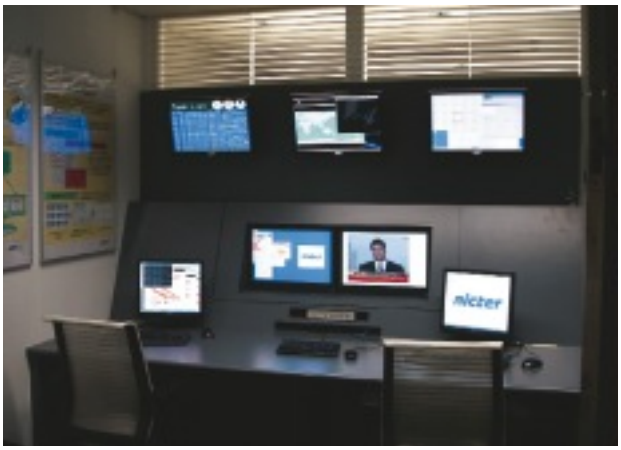

図1　インシデント分析センターnicterのオペレーションルーム

図2　観測トラヒック可視化モジュール出力例