

3.12.2 社会還元促進部門 情報システム室

室長 青木哲郎 ほか4名

情報インフラの整備・運用や情報セキュリティ維持を通して研究活動をサポート

【概要】

NICTの情報インフラである共用ネットワーク、共用サーバ、外部接続ネットワーク、事務部門用共用パソコン、テレビ会議システム等の整備・運用及び情報セキュリティの維持・監視を行い、研究しやすい環境を提供することで、NICTの研究活動の推進に貢献している。

(1) 情報インフラの整備・運用

役職員が活発な研究活動を行うために必要な情報インフラを提供し、利便性を向上させるとともに業務の効率化等を図る。

(2) 情報セキュリティの維持・監視

情報社会で大きな課題である情報セキュリティに関して、不正ソフトウェアの侵入等の不正アクセスやウイルス感染等、NICTのネットワークを防御し、安心して研究活動等ができるようにする。

(3) 研究開発のサポート

研究活動に必要な情報基盤の構築をサポートし、研究成果の実証と外部への発信をサポートする。また、NICTで研究開発された技術を、NICT内の実際のネットワークで実運用することにより、NICT発技術のショーケースとしての役割を果たすとともに、その成果を研究現場にフィードバックを行って、研究開発に寄与する。

【平成24年度の活動実績】

(1) 情報インフラの整備・運用

- NICTで使用されている複数の業務系システムの統合設計を進め、新規に構築した勤務管理システムと既存システム（共用スケジューラ、電子決裁システム）を仮想化技術を使って平成25年3月に統合し、リソースの有効活用を進めることで、業務の効率化や運用コストの削減を進めた。
- ネットワークの柔軟な利用を可能とする共用無線LAN環境を本部の全建物で整備し、ペーパーレス会議等を可能にすることで、会議運用の省力化・効率化を進めた。
- 新設された研究拠点である耐災害ICT研究センター（東北大学構内）のネットワーク構築及び共通基盤整備を行い、NICTと他大学・他研究機関など、複数の組織に所属する職員がそれぞれのセキュリティポリシーに準じて円滑でセキュリティが確保できるネットワーク環境を整備し研究活動を支援した（図1）。

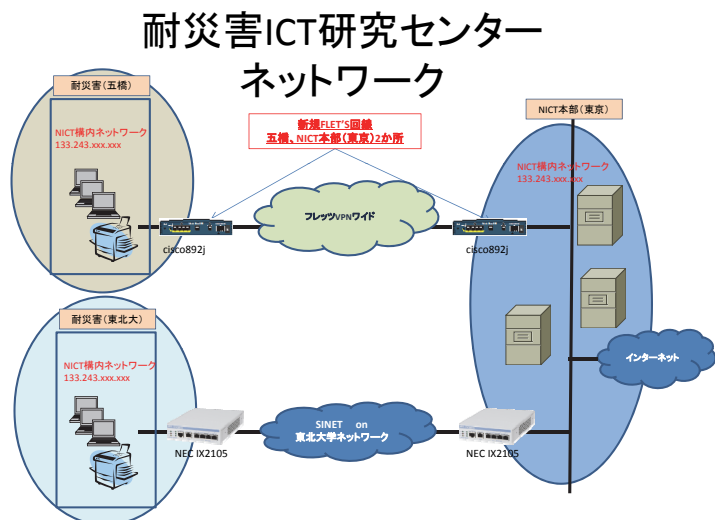


図1 耐災害ICT研究センターの新設ネットワーク。仮設の建物間を低コストで安全に接続し、業務を行えるようにした。

(2) 情報セキュリティの維持・監視

外部からの攻撃に対して防御するファイアウォールを更新し、NICT全体のセキュリティ向上に資した。

- NICT内に設置したセキュリティチェック装置及びファイアウォールからの情報を365日24時間常時監視する体制を構築し運用することによって、不正アクセス等の外部からの攻撃による障害発生を防ぐとともに被害が最小限で抑えられるようにした。特に不正アクセス遮断装置の新規導入により、外部向けWebサーバへの攻撃を自動遮断し、サーバの設定不良を検出し是正した。

- 外部向け Web サーバの脆弱性チェックを定期的実施し、研究部門でのネットワーク実験や成果公開のセキュリティ維持に資した。
- 情報セキュリティポリシーの啓発のため、全職員等を対象としたセキュリティ研修（e-ラーニング方式）を平成 24 年 12 月に、自己点検を平成 24 年 8 月に実施し、個々のセキュリティ意識の向上を図った。
- 全職員を対象として標的型メール訓練を平成 24 年 12 月及び平成 25 年 2 月に実施し、標的型メール攻撃に対する意識向上及び対応の向上を図った。
- 情報セキュリティインシデントに対して迅速に対応するための CSIRT（Computer Security Incident Response Team）を設置し、インシデント対応の専門部隊として迅速に対応することで、被害をできるだけ小さくし、かつ適切な解決・フォローアップができるようになった。

(3) 研究開発のサポート

ネットワークセキュリティ研究所の研究成果であるトラフィック可視化ツール NIRVANA を NICT 内ネットワークで運用し、可視化してモニターすることによりセキュリティリスクの事前発見などができるようになり、NICT のセキュリティ確保に貢献した（図 2）。また、NIRVANA の実データ運用による知見を開発元の研究者にフィードバックすることによりシステムの改良に貢献した。NIRVANA の運用ノウハウ、技術情報を蓄積した上でサイバーセキュリティ研究室と協力して NIRVANA の社会展開、技術移転にも貢献した。

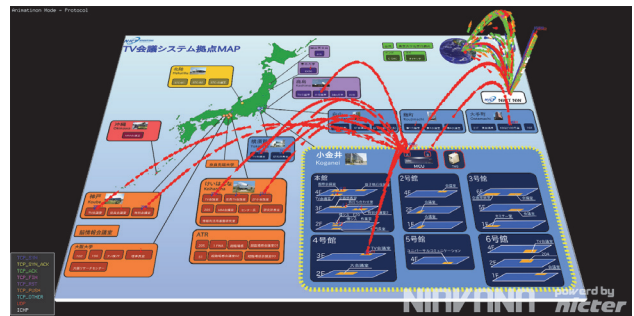


図 2 NIRVANA による NICT 内ネットワークトラフィックの監視(TV 会議の運用を監視している)。NICT 内のどの建物からどのサーバに向けてどのような種類のパケット（種類により色分けされている）が流れているかをモニターしている。パケットをクリックすることにより、詳細な情報をリアルタイムで調べることが可能。