3.6　第三研究部門　情報通信セキュリティ研究センター

研究センター長　　篠田陽一

研究センター概要

インターネットに代表される情報通信ネットワークは、我々の重要な生活インフラの一つとなり、国民の生活においてその利便性は大いに享受されているが、それと同時に様々なセキュリティ上の問題がクローズアップされている。

情報通信セキュリティ研究センターは、このような問題に対応していくため、「安心・安全のためのICT」研究領域において、情報通信の、そして情報通信による安心・安全な生活をリードする研究開発拠点を形成すべく平成18年4月に設置された。

当センターでは、ネットワークにおいて大きな脅威となっているサイバー攻撃・不正通信等への対策技術や、その発信元を追跡するトレースバック技術、そして情報を守るための暗号・認証技術や情報漏えい対策技術を組み合わせることで、トラクタブルなネットワークの実現を目指すとともに、災害時などのいざという時に生命や財産を救うためにも利用できるICTによる防災・減災基盤技術の開発も推進している。

このような活動の下、コミュニケーションの安心・安全をリードする研究開発拠点(COE)として、国民が常に安心・安全なコミュニケーションを享受できる環境の実現に向け、最先端の情報セキュリティ研究基盤、人材などを幅広く結集し技術基盤を形成する研究センターを目指している。

さらに、産業界や政府の取り組み、大学・企業・研究機関等の研究活動や人材と積極的に連携しながら、情報通信セキュリティに関する先端的かつ実践的な研究を行うことにより、社会への迅速な還元を目指している。

(1)　サイバー攻撃・不正アクセスに対する検出・分析・対策等を行うネットワークセキュリティ技術の研究開発(インシデント対策グループ、トレーサブルネットワークグループ)

(2)　情報・プライバシー保護のための暗号・認証技術等の研究開発(セキュリティ基盤グループ)

(3)　災害による被害の防止・軽減を目指した情報通信技術の研究開発(防災・減災基盤グループ)

主な記事

(1)　情報セキュリティ政策会議において定められた2月2日の「情報セキュリティの日」の関連事情として、情報通信セキュリティシンポジウム「トラクタブルネットワークの実現に向けて」を開催した(図1)。

(2)　NICT機関誌や研究発表会及び展示会(図2)などを通じて、情報通信セキュリティ研究センターの研究成果を積極的にPRした。

図1　情報通信セキュリティシンポジウム
「トラクタブルネットワークの実現に向けて」
(平成19年2月7日)

図2　危機管理産業展における展示の模様
(平成18年10月24-26日)

3.6.1　情報通信セキュリティ研究センター　インシデント対策グループ

グループリーダー　　中尾康二　ほか6名

ネットワークセキュリティ技術の研究開発

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ネットワークセキュリティにかかわる基盤技術、応用技術の研究開発を行う。

サイバー空間上で発生する各種攻撃の分析を目指し、各収集点で効率的・効果的に攻撃イベントを収集管理する技術の研究開発を行う。

サイバー空間上で発生する(又は蓄積された)各種イベントの挙動傾向、挙動原因、他挙動との因果関係等を実時間で解析するイベント分析技術の研究開発を行う。

イベント分析の結果とその結果情報の蓄積ノウハウに基づき、各種攻撃に対する事前対策、インシデント対応、事後対策に係る総合技術の研究開発を行う。

各種データ収集法の研究開発と、サイバー空間上でのイベントの効果的収集と、以後の分析のための管理・運用を行う。

各種イベントに対してそれぞれ異なる単体分析を実時間で実施し､それぞれの分析結果間の相関分析により、イベント挙動傾向・原因・他イベントとの関連を導出する。

過去のイベント分析結果等に基づき、各種イベントに起因する攻撃の予兆を洞察し、イベントがインシデントと認識される場合の対応、事後緊急対策の研究を行う。

上記を総合的に関連させてシステムとして機能化し、その有効性の評価のため、イベント分析のシステム化として(nicter-γ)を構築する。

平成18年度の成果

(1)　イベント収集管理技術の研究開発

①　マルウェア検体収集

ア　サイバークリーンセンター(CCC)からの検体提供体制確立：総務省・経済産業省の連携プロジェクトCCCにおいて収集されたマルウェア検体をnicterのミクロ解析システムで分析すべく、検体受信体制を確立した。

イ　honeypotによる検体収集：NICTがアドレスを持つネットワークにおいて、オープンソースのマルウェア検体収集システムを稼働させ、検体の収集を開始した。

ウ　メールシステムを利用したマルウェア検体の収集システム：メールに含まれるヘッダや添付ファイルのエンコーディングワードなどのテキスト情報からの特徴選出により、ウィルスが添付されたメールから検体を収集するシステムを開発した。

②　トラフィック収集

ア　新観測ポイントからのトラフィックの受信開始：これまで観測していた環境に加えて、新たな観測ポイントのネットワークの提供を受け、マクロ解析システムのための観測ポイントを倍増した。新観測ポイントに到達する大量のトラフィックをJGNⅡにより、高速に小金井本部へ転送した。

イ　センサ拡充へのその他の取り組み：上述のセンサ群に加えて、新たに大学からトラフィックの提供を受けるべく準備を推進した。

③　収集情報分散管理

nicterで収集されている多様な情報の漏えいや欠損に対して、情報の分散管理によって安全性を高めるため、特に重要度の高い情報として、マルウェアの検体ファイルの保護に重点を置いた検討を実施した。すべての検体ファイルに暗号化を施した上で、その暗号化鍵を秘密情報分散技術を用いて分散管理することにより、安易な情報の漏えい防止が可能である。

④　マルウェア検体の取扱手順の策定

手順の確立とそのために必要なシステムの開発を行い、これにより電子的・物理的な情報の漏えいを防ぐ統一的なマルウェア検体を管理する手法の実現に着手した。

⑤　センサの安全な運用機構

nicterへの入力情報を提供するセンサは国内外の複数か所に設置されているが、これらのネットワークアドレスを秘匿し、かつ、セキュアな情報収集を実現するために、情報ハイディング技術、匿名通信技術、暗号技術、認証技術からなる安全な情報収集機構のアーキテクチャを検討した。

⑵　イベント分析技術の研究開発

①　マクロ解析

ア　トラヒック3D表示、世界地図表示の機能を拡張し、多数のチャネルからのトラヒックの選択的表示と、3D表示に関する様々な視点からの可視化を実現した。統合的なインターフェイスの構築により、システムのユーザビリティを向上した。振る舞い分析・長期振る舞い分析に検索機能を付加し、多種多様な検索条件から過去のホストごとの挙動情報の抽出機能を実現した。ボットネットの検出のため、同様の振る舞いを示すホストの可視化結果を強調表示する機能を付加した。

イ　時系列データ中の周期成分除去により、変化点検出エンジンの誤検知率低減を実現。監視中のパラメータ(ポート番号など)のリストと、対応する時系列データのグラフ表示を行うインターフェイスを付加した。

ウ　自己組織化マップ(SOM)分析エンジンに、単位時間ごとの出力を連続表示し、時間経過に伴う攻撃ホストのクラスタの変化を表現する機能と、急激に増加するクラスタを強調表示する機能を付加した。

②　ミクロ解析

マルウェア検体の収集・分析を行うミクロ分析では、静的解析と動的解析システムから成る自動化されたミクロ解析システムを構築し運用開始した。

ア　収集されたマルウェアをメモリ上に展開し、それを逆アセンブルするマルウェア静的解析システムを構築した。

イ　インターネット環境をエミュレートした擬似解析環境にてマルウェアを実際に動作させ、解析を行うマルウェア動的解析システムを構築した。

③　マクロ－ミクロ相関分析

マクロ解析からの各ホストごとの挙動情報と、ミクロ解析からのマルウェアごとの挙動情報をプロファイル化し、分析する手法を提案し、マクロ－ミクロ相関分析システム(NemeSys)として構築しnicterへ導入した。

⑶　サイバー攻撃対策導出技術の研究開発

①　インシデントハンドリングシステム構築・導入

nicterのマクロ分析システムにおいて自動検出されたインシデント候補のアラート群を管理し、その解析状況を管理するインシデントハンドリングシステムを構築し、nicterへ導入した。該システムに、オペレータによるインシデントレポート作成の補助機能を付加し、過去の分析手順の履歴に基づき、オペレータの分析手順を自動的に提示するワークフローエンジンを設計・開発した。

②　インシデント予測

特定のポートへのアクセス数に関する長期的観測データ(数年程度)と該当ポートに関する脆弱性情報公開のリリース時期を基に、新たな脆弱性情報公開による将来的な影響を予測する学習アルゴリズムに関して基礎検討を実施した。

③　アプリケーショントレースバック

WebサーバへのSQLインジェクション等の攻撃を検知し、HTTPレスポンス内にマークを混入することで、攻撃が多段のプロキシサーバを介して行われた際にも、攻撃元を追跡することが可能なアプリケーショントレースバックシステム(MapTB：Marking-based Application Traceback)方式を提案し、実験環境の構築と提案システムの実装を実施した。

④　マルウェア対策導出システム・マルウェア対策検証システム

マルウェアの動的解析から得られる挙動情報を基に、マルウェアの感染の様子をネットワークシミュレータ(MIRAI-SF)上で再現し、マルウェアの影響度を測定するシステムを構築した。さらに、流量制限等によるネットワーク的なマルウェア対策をシミュレータで反映させることで、対策効果の測定を実施した。

⑤　インターネットサービスプロバイダ(ISP)からの要件抽出

真に有用なインシデント対策とは何かを探るため、Telecom-ISACに加盟している複数のISPに対して、nicterのオペレーション結果を基にヒアリング調査を行い、ISPの要件抽出を実施した。

⑷　イベント分析用システム化の研究開発

①　分析システムアーキテクチャ

ネットワークモニタリングを基にしたマクロ解析システムと、マルウェア解析を基にしたミクロ解析システム、さらにそれらの解析結果を結合させるマクロ－ミクロ相関分析システムによる、インシデントの発見・分析・対策を行うnicterのアーキテクチャを明確化し、該アーキテクチャに基づくシステム化を実施した。

②　各モジュール間の連携の強化と自動化

マクロ分析モジュール間の連携、マクロ／ミクロ解析システム間の連携、マクロ－ミクロ相関分析システムの開発を実施した。該機能の大部分を全自動化し、オペレータの日常的な監視業務の強力な支援を可能とした。

⑸　展示会出展、見学対応、その他の研究

展示会出展としてINTEROP2006、危機管理産業展2006等へ出展した。そのほかに圧縮データへの情報ハイディング、非常時警報音への情報ハイティング、二次利用ポリシを記述可能なメールシステム、DNSSECの運用展開に関する研究を実施した。

3.6.2　情報通信セキュリティ研究センター　トレーサブルネットワークグループ

グループリーダー　　関口博久　ほか6名

ネットワークセキュリティ技術の研究開発

概　要

発信元のアドレスを特定する空間方向の追跡技術と、発信元からのパケットの推移を解明する時間軸方向の追跡技術の開発を実施する。本技術の評価のため再現ネットワーク技術の研究開発を実施する。また、不正・異常なパケットの存在下における通信方式としてセキュア・オーバーレイ技術の開発を実施する。

⑴　2010年のバックボーンネットワークの規模を想定してパケットの発信元を低誤検知率で追跡する技術を開発する。

⑵　1日以内の発信元からのパケットの推移を短時間に解明する技術を開発する。

⑶　ネットワークのエッジからコアにまたがる広範囲な技術を対象として、追跡機能を付与した装置を開発する。

上記評価を1Gbpsに縮小した模擬環境で行う再現ネットワーク技術を開発する。不正・異常なパケットの存在下で、トレーサブルネットワーク装置間の通信性能の劣化が一定値以下であるセキュアオーバーレイ技術を開発する。

従来のIPトレースバック技術の高速化・実用化についてはNICT委託研究の成果を前提としつつ、2010年のバックボーンで用いられるネットワークを対象として、各種解析処手法を応用した新たなアプローチによる飛躍的精度向上と高速化を目指す。時間軸方向のトレースバックに取り組むため再現テストベッド技術を核として理論的アプローチとシステム的アプローチを融合し、発信元からのパケットの推移を時間軸に沿ってトレースバックする技術の開発を行う。

平成18年度の成果

⑴　時系列を含む多次元、多様性に対応できる発信元追跡技術の研究開発

グランドチャレンジ(2010年のバックボーンネットワークの規模を想定、低誤検知率、短時間で解明)を設定し、プロジェクト終了時に実用性をもたらす研究開発を推進した。これにより、基本問題への帰着と方式研究の推進を実施することができた。

①　高速な機械学習アルゴリズム

k-Nearest Neighborを改良した高速な機械学習アルゴリズムを開発し、公開されているデータセットにてその有効性を確認した。

②　多次元、多様性に対応できる発信元追跡

サポートベクタマシンは多次元で、多様性のある問題を取り扱うのに適していると考えられている。そこで、サポートベクタマシンにDARPAのデータセットを適用した場合の検討を実施した。その結果、DARPAデータセットでは次元が1.6と低くベンチマーク用データセットとしては不適切であることが明らかとなった。

③　秘匿計算プロトコルの基礎理論及び実装

本プロジェクトでは通信の秘密が実用上の大きな課題となっている。このため、通信の秘密を確保しつつ発信元追跡を行うための暗号プロトコルに取り組み、準同型暗号技術に基づく暗号プロトコルを開発した。また、同技術に基づく共通集合計算プロトコルの実用性を検証するため、実証システムを開発した。

⑵　発信元からのパケット解明技術の研究開発

不正・異常なパケットはますます先鋭化・多様化しており、パケットの捕捉能力と解析能力の向上が急務である。このため以下の研究開発を行った。

①　仮想マシン技術を応用したデータ捕捉機構

仮想マシンモニタを改良し、ゲストOSにおける不正アクセスが発生した場合に仮想マシンモニタに対して通知する機構を実現した。これにより不正アクセス発生時点のメモリ、ディスク内容を捕捉することが可能となった。

②　不正コードベクタの解析能力向上

定理証明器を用いて、難読化されたコードに対しバイナリコード解析を行うシステムを実現した。本シ

ステムにより難読化された不正コードベクタの検出を高速に行うことが可能となった。また、難読化されたコードのシグニチャを自動生成することが可能となった。

③　暗号化ネットワーク上のマルウェア捕捉機構

Winny等のPeer-to-peer型ネットワークにおいて拡散しているマルウェアを捕捉するシステムを開発した。本システムにより、暗号化されたファイル交換ネットワーク等で拡散している、従来検出することが難しかったマルウェアを捕捉し解析に供することができるようになった。

⑶　再現ネットワーク技術の研究開発

①　インシデント再現方式の検討

プロセッサ仮想化技術によるインシデント再現方式の検討を行い、実際に存在する脆弱性に対して観測された未知の不正コードベクタを用いてインシデントが再現できることを示した。これらの成果を国内研究会にて2件発表した。

②　再現実験環境を応用した実験システムの研究開発

プロトタイプ実装を用いて検証実験を実施した。これらの成果を国際学会に2件、国内学会誌に1件投稿し、国内研究会にて計2件発表した。

③　インシデント対策チームからの検体入手・解析

協力関係にある複数の大学の事案対策チームから検体を入手し、実際に再現テストベッドにおいてインシデントを再現・解析できることを示した。

⑷　セキュアオーバーレイ技術の研究開発

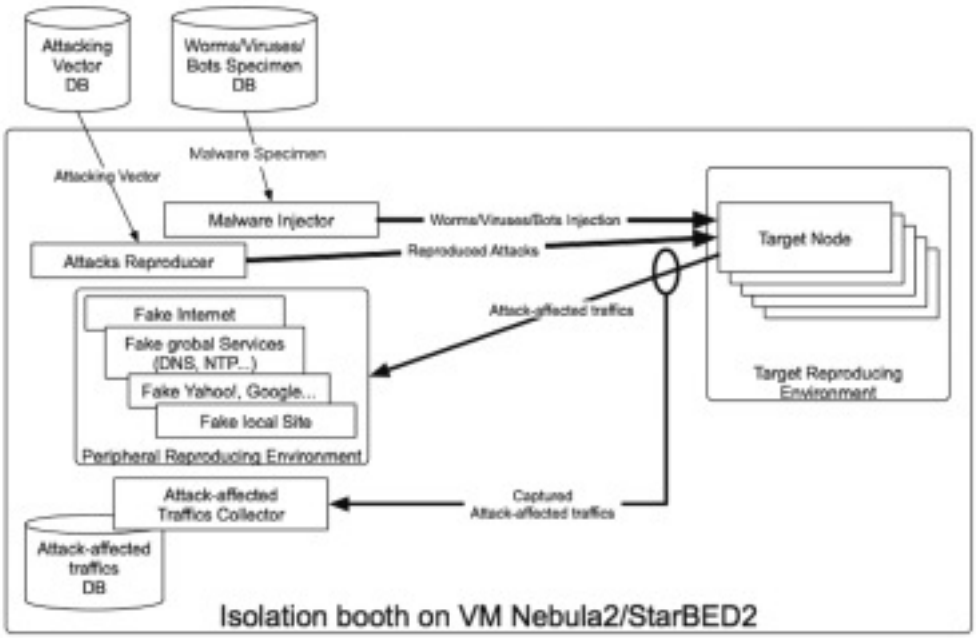
不正・異常なパケットの存在下においても通信性能の劣化を抑えるため、セキュアオーバーレイの研究開発に取り組んだ。

①　ハードウェアトークンを用いた認証

PKCS11暗号化インターフェース、PKCS15証明書インターフェースを利用し、スマートカードに内蔵された証明書を用いてオーバーレイに加入する実証システムを開発した。並行して、近接通信による物理的認証の概念実証として、Bluetoothデバイスを認識しオーバーレイに加入する実証システムを開発した。

②　信頼性分散管理システムの実装

単一の認証局に依存せずに真正性と一貫性の検証を行うため、セキュアオーバーレイ上でSDSI/SPKIを用いて信頼の連鎖を分散管理するシステムの構築について、開発に着手し、今年度基本検討を実施した。



再現実験環境を応用した実験システムの研究開発における、影響トラフィックの再現・収集機構の構成図

3.6.3　情報通信セキュリティ研究センター　セキュリティ基盤グループ

グループリーダー　　山村明弘　ほか5名

セキュリティ基盤技術(暗号プリミティブ、暗号プロトコル)の評価手法・設計手法及び電磁波・情報セキュリティとサイドチャネル攻撃にかかわる研究開発

概　要

安全で安心な通信を実現するセキュリティ基盤技術の研究開発を行う。

⑴　暗号理論と代数系：新しい原理(ラティス等)に安全性の根拠を持つ暗号技術の提案を目指す。また、代数系とそのアルゴリズムについて研究を進め、セキュリティ技術への応用を目指す。数論的アルゴリズムについて通信複雑性の視点から調査する。

⑵　暗号プロトコルの設計•安全性検証：パスワードベースの認証手法を暗号プロトコルへ応用する。ハッシュ関数の暗号プロトコル(タイムスタンプ等)への影響を調査する。形式的手法による暗号プロトコルの検証を行い、暗号アルゴリズムの理論的解析手法を開発する。

⑶　暗号技術の解析手法：ブロック暗号、ストリーム暗号とハッシュ関数の評価手法及び乱数検定法を提案し、暗号技術の応用システムの構成に利用する。

⑷　漏えい電磁波による情報セキュリティへの脅威とその対策：漏えい電磁波に含まれる情報の評価手法を確立し国際標準(ITU-T)に提案し、対策手法等の研究開発成果を民間に技術移転する。

⑸　CRYPTREC活動を通して電子政府暗号への貢献：電子政府推奨暗号リストに掲載の暗号技術の安全性に関する監視活動を行い、公開鍵暗号ワーキンググループを運営し、電子政府システムへの政策的アドバイスを行う。

平成18年度の成果

⑴　暗号理論と代数系

米国NISTによるハッシュ関数の国際的コンテストAHS(Advance Hash Standard)に関連して、ハッシュ関数に求められる暗号理論的な安全性及び実装性能要件を求め、またハッシュ関数をその利用方法の視点から分類し、NISTが主催する国際ワークショップにて発表した。

De Santis等により提案された閾値型匿名グループ認証スキームが、正当なユーザグループであっても認証されないことが頻繁に起こり得ること、つまりプロトコルとして不完全であることを、チャレンジーレスポンスで利用される行列の性質を厳密に検査することにより示し、システムが正しく動作するための必要かつ十分条件を求めた。更に完全性を満たす新しい閾値型匿名グループ認証スキームを構築し国内研究集会で発表した。

型付きの形式体系に対する高階圏論を利用した意味論構成について国際論文誌で発表した。

⑵　暗号プロトコルの設計・安全性

匿名資格証明技術を用いた認証済み鍵交換方式の提案を行った。先行研究であるC. Y. Ng等による匿名資格証明技術では、資格証明書の検証者を指定し、検証者による利用済み証明書の使い回しを防止した。しかし、検証者に対して利用者の証明書利用履歴が秘匿されていないため、プライバシが守られていなかった。そこで、発行された証明書をランダマイズ可能にし、検証済み鍵交換に応用することで鍵共有相手が指定可能な新しい鍵交換方式を提案し国内研究集会で発表した。

紛失通信スキームは暗号プロトコルの構成における重要な構成要素である一方、既存の紛失通信スキームをリソースが限られた環境下で利用することは通信量が大きいことから難しい。そこで、可換共通鍵暗号族を利用し、秘匿された情報を掲示板に示すことで通信量を低減させる手法の安全性評価を行い国内研究集会で発表した。

形式的手法による暗号プロトコルの安全性検証に関する研究において、定理証明ツールによる形式検証の新たな実例を構成した。暗号プロトコルTLSについて、Paulsonによる形式的モデル化を、型理論に基く定理証明支援ツールであるCoq上へ移植し、その安全性をCoqを用いて証明し国内研究集会にて発表した。

⑶　暗号技術の解析手法

線形化手法による線形複雑度の見積り手法を提案した。従来の評価手法であるBerlekamp-Masseyアルゴリズムや Games-Chanアルゴリズムと比較し計算量が少なく、実行に必要なデータ量が小さいことを示し

た。提案手法は生成アルゴリズムから線形複雑度を求めることに特徴があり、出力系列から求める従来の手法と大きな違いがある。そのため、従来法は適用できなかった非常に長い周期を持つ暗号用擬似乱数生成器のようなものに対しても本手法は適用できる場合がある。国内研究集会において発表を行った。

高い計算効率性を実現し、幅広いユビキタスプラットフォームに活用できる軽量公開鍵暗号技術の設計と解析に関する調査研究を行った。

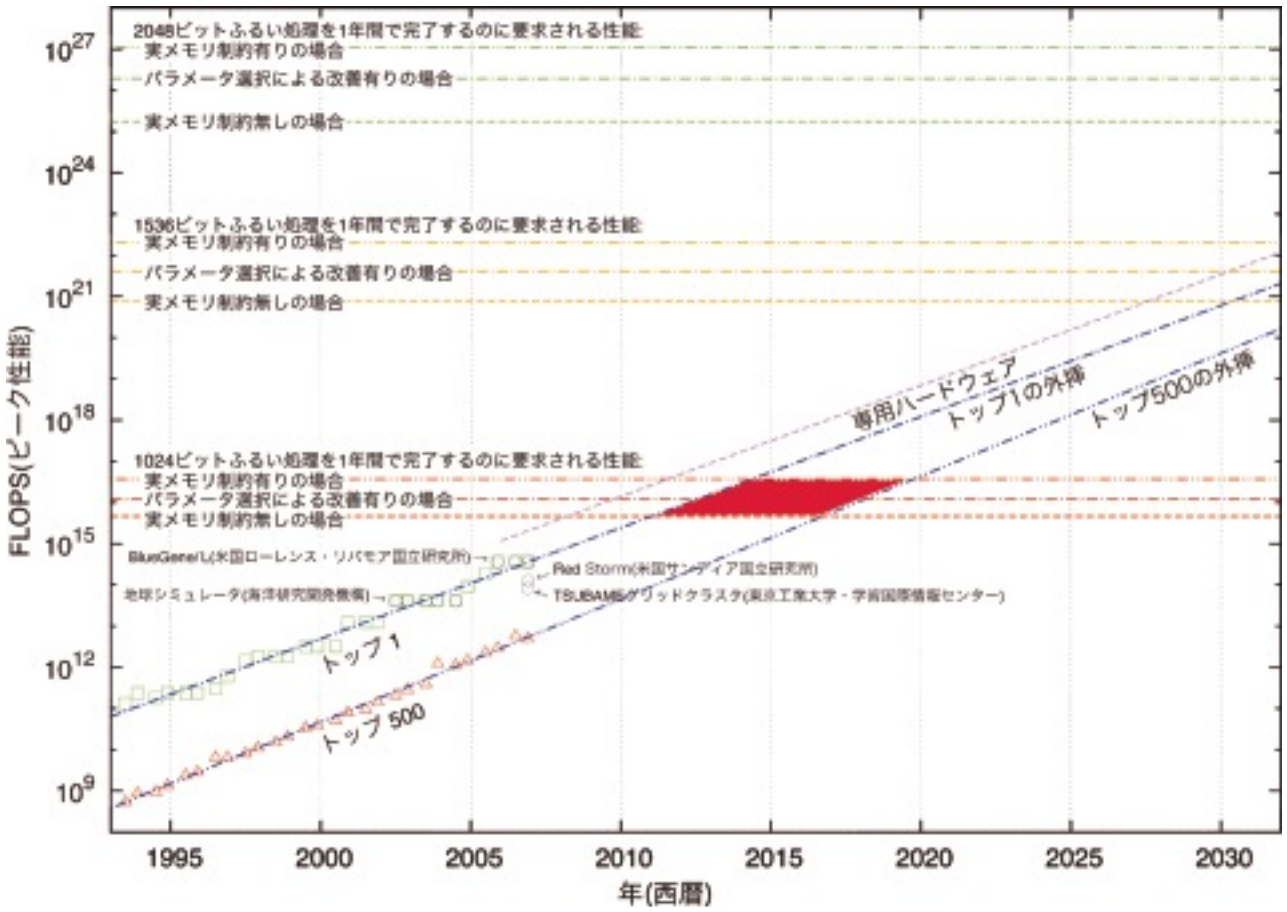
⑷　漏えい電磁波による情報セキュリティへの脅威とその対策

IT機器が動作時に生じる消費電力、電磁波、光、熱などのエネルギー放射に含まれる情報量について、通信路容量を利用して評価する手法を提案し、測定実験を行い検証した。本手法では通信路容量を、対象の機器と受信機の間は連続通信路と考えることにより算出している。IT機器から放出される電磁波は、通信を目的としていないものはすべて雑音としてとらえられる。しかしながら本手法では、ある特定の周波数帯域は処理情報に関連があることからその帯域のみ信号と定義しS/Nを算出した。結果を国内研究集会において発表した。

PCからの雑音放出によるモニタ表示画像の情報漏えいに関し、物理的セキュリティ要求条件や情報の重要性、コスト等を考慮した評価・対策方法を検討し、ITU-T(SG5)に寄書を提出した。また、モニタに表示される文字画像の情報漏えいを防止するソフトウェア的対策方法を考案して、特許を出願した。さらに、タッチパネル式情報入力装置における操作時のボタン入力情報の漏えいを防止するソフトウェア的対策方法を考案し、特許を出願した。本研究に関し、国内研究集会で発表を行った。

⑸　CRYPTREC

暗号技術監視委員会において、公開鍵暗号ワーキンググループを設置し、公開鍵暗号のパラメータの選択及び利用期限に関して、素因数分解問題の解法アルゴリズムである数体ふるい法の計算量を実験により見積もり、現状の計算機の能力の成長率から、世界最高峰のスーパーコンピュータにより1,024ビットの合成数が分解される時期をおおよそ2010年から2015年の間と推定した。また、NICT委託研究(素因数分解ハードウェア、富士通)の結果を利用して、ハードウェアによる素因数分解問題の妥当性を検証し、ハードウェアはソフトウェア的手法のおおよそ5倍程度高速に分解ができると推定した。これらの知見は電子政府推奨暗号監視活動(CRYPTREC)を通して、総務省、経済産業省、内閣官房に報告した。



3.6.4　情報通信セキュリティ研究センター　防災・減災基盤技術グループ

グループリーダー　　滝澤　修　ほか4名

「災害に強い通信」と「災害時に役立つICT」を目指して

概　要

大規模災害から小規模災害までを幅広く対象とする防災・減災のためのICT基盤技術を総合的に研究開発し、災害による被害の未然防止から発災後の被害の軽減まで広く役立つ「防災・減災ICT」を確立し、安心・安全な国民生活の実現に寄与する。そして、開発する技術が有効に使われるための普及活動を、防災関連機関等を取り込んで継続的に実施する。

具体的には、輻輳制御や異種アクセスネットワーク間制御、アドホックネットワーク形成技術など、災害時の様々な通信ニーズを満たすことを目的とした「非常時通信網構築技術」、災害情報授受用に工夫したRFID、センサー、マイクロサーバ等のデバイスを用いて防災・減災に役立つ情報を正確に授受するとともに、アプリケーションレベルでの情報の多重化により伝送可能情報量を増やし、災害時の限られた通信容量を最大限に生かすための「ユビキタス防災・減災通信技術」の研究開発を行う。

平成18年度の成果

⑴　非常時通信網構築技術

①　非常時ネットワーク制御基盤技術の研究開発

近年の大規模災害時の度に起こり問題になる安否確認等による携帯電話の輻輳と平成16年の新潟県中越地震の時に特に問題になった停電や伝送路断による携帯電話基地局の損壊(機能停止)に注目し、ネットワーク制御技術の基礎検討を行うとともに、簡易シミュレータを一部開発した。その結果、輻輳制御法に関する特許を2件取得し、1件出願した。損壊基地局が存在した場合の携帯電話ネットワークへ与える影響を評価した結果を発表した。また、通信時間制限のトラヒック理論解析を行った結果を発表した。

②　アドホックネットワーク形成技術の研究開発

被災地における非常時通信のための、既存ネットワークとアドホックネットワークのハイブリッドネットワークを用いてQoS(Quality of Service)を保証しつつシステム全体の通信を最適化するスキームを提案し、性能評価により接続成功率について従来方式より優れた結果を得た。結果は学会で発表するとともに論文投稿を行った。

アドホックネットワーク端末が実際の市街地における道路を模擬した経路に沿って移動する場合のモデルを作成し、シミュレータによりネットワーク性能評価を行った(図1)。端末初期位置、プロトコル属性、端末移動モデルの違いによるデータ配信率の差異及び特性を明らかにし、学会で発表した。【総務省SCOPE委託研究「遠隔ロボットを用いた災害時マルチメディア情報収集技術に関する研究開発」】

二次元閉鎖空間内においてネットワークを構築するロボットと探査を行うロボットが協調し有線及び無線を統合的に用いて複数映像を伝送するシナリオを作成し、シミュレータを用いてネットワーク性能解析を行った(図2)。

【NEDO委託研究「戦略的先端ロボット要素技術開発プロジェクト・被災建物内移動RTシステム・閉鎖空間内高速走行探査群ロボット」】

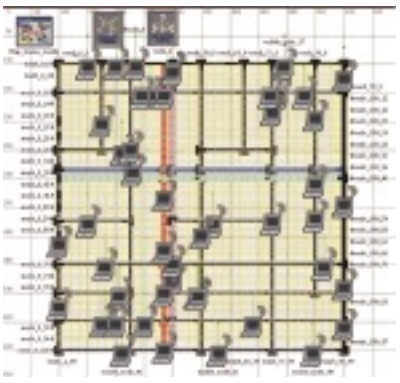


図1　仙台市中心部を模擬した端末移動モデル

図2　計算機シミュレーションで用いた探索エリア(クランク状)とロボットの軌跡の例

(2)　ユビキタス防災・減災通信技術

①　ユビキタスデバイスによる災害時情報収集・共有技術の研究開発

大規模災害時にRFID(電子タグ)を「電子貼り紙」として被災地にまき、被災情報の収集•共有に供するシステムの開発を進めた。建築物の応急危険度判定、安否確認、要救助者探索など、様々な応用を想定している。平成18年度は、パッシブタグ(無電池)とアクティブタグ(電池内蔵)とを組み合わせた「ハイブリッドRFID」のリーダライタユニットを新たに開発した(図3)。これらを用いて、被災地の調査員がアクティブタグからのビーコンをキャッチし、タグに近づいてパッシブタグと詳しい情報のやりとりをするという、現実に即した利用法を可能にした。消防本部訓練、国際緊急援助隊訓練、自治会防災訓練等に開発システムを投入して想定されるユーザによる評価を行った(図4)ほか、前年度までの成果を含めて、論文誌発表、国際会議発表、国内会議発表を行った。【大都市大震災軽減化特別プロジェクト委託研究「レスキューロボット等次世代防災基盤技術の開発」】【科学研究費補助金・基盤研究B「大規模災害の事前事後における消防活動支援及び情報共有化システムに関する研究」】

RFIDを位置情報の発信源とし、測位から防災•防犯まで幅広く対象とする研究プロジェクトを、平成18年度から開始した。我々は、消防庁(消防研究センター•消防技術政策室)及び科学警察研究所と連携して、安全・安心のためのアプリケーションを開発するサブプロジェクトを担当している。また、アクティブRFIDリーダを内蔵した携帯電話端末を用い、GPS測位や基地局測位よりも高い精度で発信者の位置を特定したり、緊急通報先を自動選択したりするプロトタイプシステムの開発を行った(図5)。【一部は科学技術振興調整費委託研究「電子タグを利用した測位と安全・安心の確保」】

図3　ハイブリッドRFIDリーダライタユニット

図4　国際緊急援助隊訓練におけるRFIDシステムのデモ

図5　RFIDの受信による測位機能付き携帯電話端末

②　災害時等情報重畳技術の研究開発

サイレン等の警報音響に電子透かし的な手法でデジタル情報を重畳して、音響が届く範囲に防災情報を合わせて伝送する技術を開発している。無線等の別個の伝送路を経ずに情報伝送できるため、通信インフラがダメージを受けて情報伝達手段が限られる大規模災害時には、特に有効な技術と考えられる。平成18年度は、空気伝搬中の騒音及びドップラー効果への耐性を考慮した実装手法を2種類提案し、国際学会で発表した。現時点で数ビット／秒の情報重畳を計算機上で実現している。今後は手法の改良とともに、フィールド実験により性能の評価を行う。

前年度に提案したウェーブレット係数の量子化インデクス変調を用いた手法を基本とし、ウェーブレットパケット法の導入により1オクターブ未満の微量なピッチスケーリングへの耐性を高めた、音楽用電子透かし手法を開発し、学会発表した。

人間の感覚情報を鍵とする新しいユーザ認証の研究に着手した。聴覚の個人差を応用し、自声聴取音(本人が聴取している自分の音声)に対する反応が本人と他人とで有意な違いがあることを想定した聴取実験を行い、本人と他人との感覚差を抽出できる可能性が示唆された。今後は自声聴取音の作成方法の改善を図る。