2.4 ネットワークセキュリティ技術

2.4.1　第1期中期計画

(1) 概要

第1期中期計画においては、ネットワーク領域の研究開発の一分野として「情報セキュリティ分野の研究開発」が位置づけられ、「情報通信危機管理基盤技術の研究開発」及び「ネットワークセキュリティ技術の研究開発」が実施された。計画当初は、「情報通信部門非常時通信グループ」が情報通信危機管理基盤技術の研究開発に取り組んだが、平成16年1月に「情報セキュリティセンター(通称)」が発足し、1室3グループ体制(情報セキュリティ推進室、セキュアネットワークグループ、セキュリティ高度化グループ、セキュリティ基盤グループ)にてネットワークセキュリティ技術の研究開発を含む情報セキュリティ研究を一体的に推進し、かつ対外的な連携を一層強化するために産学官有識者から成る「情報セキュリティサポートメンバー会議」を開催するなど、社会ニーズも踏まえ、NICTにおける情報セキュリティ研究への取組みを本格化させた。

(2) 研究成果

a) 情報通信危機管理基盤技術の研究開発

①被災者安否情報登録検索(IAA)システム(図2.4.1)の有効性を実際の災害を通じ社会にアピール。不正アクセス再現について、実験系の連携を実現。

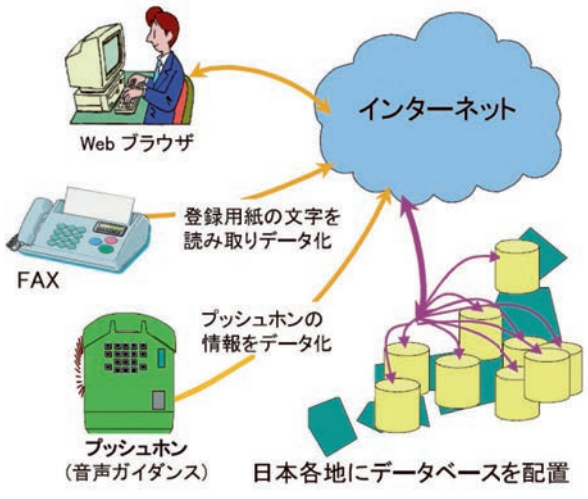


図2.4.1　IAA システムの概念図

- 平成13年に開発した大規模IAAシステムはこれまでにいくつかの動作実績を積み重ね、新潟県中越地震等(表2.4.1)で実際に運用すると共に、大量アクセスにも耐えられる体制にした。

表2.4.1　IAA システムの稼働実績

対応年月	実験運用対応内容
2000年4月	有珠山の噴火
2000年6月	伊豆諸島三宅島
2001年9月	米国同時多発テロ事件
2003年3月	イラク関連
2003年7月	宮城県北部地震
2003年9月	2003年十勝沖地震
2004年10月	新潟県中越地震
2004年12月	スマトラ沖地震
2005年3月	福岡県西方沖地震
2005年3月	スマトラ沖地震

- 不正アクセス再現実験を、目的に応じて実機の集合体(SIOS)あるいは仮想マシンの集合体(VM nebula)で実施可能とした。不正アクセスの模倣や過去の事案検索の環境も整備した。

②実時間トラフィック中のセキュリティイベントを2分以内に自動分析が可能な技術基盤を構築

- イベントログ分析では、Telecom-ISAC、大学研究機関等との連携体制を確実なものとし、イベント分析用プラットフォームを構築すべく、要素技術、連携技術を確立した。

③匿名パスワード認証型グループ鍵交換スキームの概念と、Tempest fontsの有効性を確認し新たな画面再現対策手法を提案

- 匿名パスワード認証型グループ鍵交換(APAKE)スキームの概念を提案し、その実現手法としてプロトタイプを設計すると共に、その安全性を証明した(平成17年度)。
- 電磁波による画面再現攻撃に対するソフトウェア的対策技術であるTempest fontsの有効性と限界を実験により評価し、改良方法を提案した(平成16年度)。PCから漏洩するモニタ表示画像情報に関する定量的評価手法を提案した(平成17年度)。

b) ネットワークセキュリティ技術の研究開発

①ハッシュ関数 SHA-1 の危殆化等に対し、セキュリティ技術への影響を解析し、問題点を調査報告することにより政府の政策に貢献

- 独立行政法人情報処理推進機構（IPA）と共同で CRYPTREC（**2.4.3 (2) d**）参照）の中の暗号技術検討会の下に設置された暗号技術監視委員会を開催し、電子政府システムに利用されるべき安全性と処理性能を持つ暗号アルゴリズムを選定し、推奨暗号リストを策定した。

② IP トレースバック・アルゴリズム及び IP トレースバック技術について、基本的な機能設計を完了

- ログ収集管理システム及び不正アクセス発信源探査技術を開発し、増加の一途をたどるネットワーク上の脅威に対して、対策を可能とするシステムを開発した。
- 2.4 Gbps クラスのトラフィックに対して、超高速プローブシステムがトラフィック分析、情報収集、更に上位の情報収集システムへ必要な情報の引き渡しが可能であることを確認し、実用的プローブシステム開発への基盤を構築した。

2. 4. 2　第 2 期中期計画

(1) 概要

第 2 期中期計画においては、安心・安全のための情報通信技術領域の研究開発の一分野として「情報セキュリティ分野の研究開発」が位置づけられ、「ネットワークセキュリティ技術の研究開発」、「暗号・認証技術及びコンテンツ真正性保証技術の研究開発」、及び「防災・減災のための情報通信技術の研究開発」が実施された。研究体制としては「情報通信セキュリティ研究センター」の下、1 室 4 グループ体制（推進室、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、セキュリティ基盤グループ、防災・減災基盤技術グループ）となった。

(2) 研究成果

a) ネットワークセキュリティ技術に関する研究開発

①インシデント分析センター “NICTER” の構築及び運用

- 平成 17 年度にインシデント分析センター “NICTER”（ニクター）の基礎検討を開始し、平成 18 年度の第 2 期中期計画期間開始時から研究開発を本格化させ、当該期間中に実用化レベルの技術水準を持つシステムを構築した。なお、NICTER の研究開発は第 3 期中期計画においても継続中であるため、詳細については **2.4.3 (2)** においてまとめて記述する。
- 現状のインターネットだけではなく、IPv6 環境におけるセキュリティ対策技術の研究開発を推進した。本取組の一環として、NICT が中心となって「IPv6 技術検証協議会」を設立し、IPv6 の一般家庭・企業等への本格的な普及に先立つ、抜本的なセキュリティ対策技術の検討を開始した。

②トレーサブルネットワーク技術の確立

- トレーサブルネットワーク技術による遡及解析、現象の再現、情報漏洩範囲の特定に関する研究では、仮想マシンを用いた追跡技術において、Peer-to-peer（P2 P）型ネットワークにおける情報漏洩の追跡方式を開発した。
- 発信元追跡技術に関しては、仮想マシンモニタを改良し、不正アクセス発生時点のメモリ、ディスク内容を捕捉可能とすることにより、メモリ内容を自動分析し、99%以上の確率でメモリ内の攻撃ベクタを捕捉できる機械学習アルゴリズムを開発した。
- 再現ネットワークの活用による検証技術に関しては、大規模な再現・検証に必要となるインターネットの模倣技術として、インターネットの中核部分である自律システム（AS）間ネットワークの模倣について、実際の AS 間ネットワークの規模の 3 分の 1 に相当する 10,000 AS から成る模倣 AS 間ネットワークの構築に成功した。
- トレースバックの追跡性能向上のための研究開発の一環として、プライバシーを確保しつつ発信元追跡を実現する要素技術の研究を行った。プライバシー確保のため、紛失通信プロトコルを利用した秘匿共通集合計算プロトコルの研究を行い、紛失通信技術においては従来方式と比べ、数学的制約を大幅に緩和（DDH assumption）することに成功した。

• 組織間でサイバーセキュリティ情報の交換を実現すべく、情報をコンピュータ上で扱うためのセキュリティの情報オントロジを構築した。本オントロジは、サイバーセキュリティの観点から必要なオペレーションドメイン、エンティティ、情報をモデル化しているため、交換すべき情報とその情報の利用形態を抽象化し共通化できる。サイバーセキュリティ情報交換フレームワーク（CYBEX）として国際標準化に貢献した。

b）暗号・認証技術及びコンテンツ真正性保証技術の研究開発

①離散対数問題解読の世界記録（676ビット）を樹立（平成21年度）するとともに、離散対数問題に安全性を帰着させる暗号技術において適切なパラメータ選択を可能にすることで安全性向上に貢献した。

②公開鍵暗号RSAの安全性に関する予測を、素因数分解アルゴリズムの計算量コストと計算機環境の進化予想からまとめた。また、日本銀行と共同で暗号アルゴリズムの移行期間について定量的見積り手法を導出するなど、公的機関との連携を深めた（平成21年度）。

③ CRYPTRECの運営について貢献し、次期電子政府推奨暗号の評価、利用者・運用者向けのガイドとなるリストガイドの作成、平成17年に発生したハッシュ関数SHA-1危殆化対策及びRSA-1024移行問題について貢献した。なお、CRYPTRECについては**2.4.3（2）d）**にまとめて記述する。

また、上記①～③に加えて、電磁波セキュリティの研究開発の取組として第1期中期計画で実施した**2.4.1（2）a）**③の研究を継続し、以下のような成果が得られた。

• IT機器が放射する電磁波に含まれる情報量を定量的に評価する手法を確立し、電磁波の受信から情報漏洩する脅威を明らかにした。電磁波と漏洩情報量の関係を明らかにし、適切な測定手法及び対策技術の効果の評価手法を確立した。

• 情報通信機器から漏洩する電磁波を介した情報漏洩について定量的な評価手法を確立した。また、対策技術については画面情報漏洩対策としてソフトウェアで実現する手法（図2.4.2）を開発した。この手法に関して特許を取得した上、ベンチャー企業へ技術移転し製品化を実現した。

• 学術貢献だけでなく情報通信機器の利用や設計上の電磁波情報漏洩対策について、金融機関やATM開発ベンダーなどに提言を行い、NICTとして電磁波セキュリティを推進していく中心機関の役割を果たした。

電磁波情報漏洩対策強化ソフトウェア　CrypType

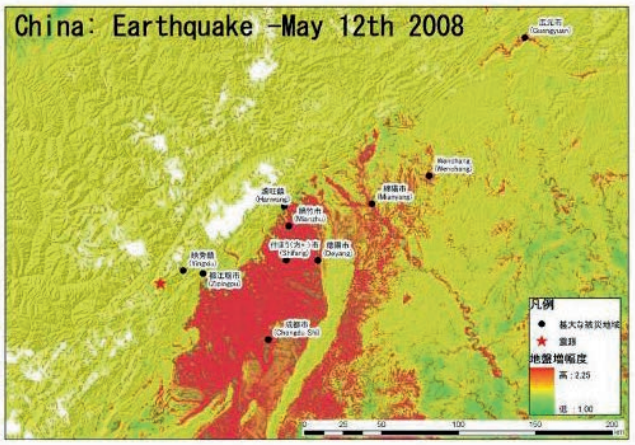
図2.4.2　電磁波による情報漏洩対策イメージ図

c）防災・減災のための情報通信技術の研究開発

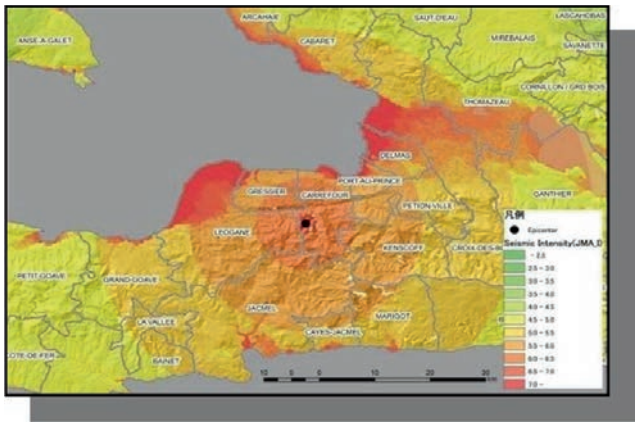
①「大規模災害時に強い通信技術」について、通信時間制限による輻輳制御技術や携帯電話ネットワーク及びアドホックネットワークについて、現実に近い詳細なモデルを用いてシミュレーション評価を実施。また、有無線統合アドホックネットワークによる自営通信機能の開発により、大規模災害時にも切れない通信技術を達成し、その技術を用いて災害対応ロボットの災害時の通信技術を開発した。

②「防災・減災情報を的確に収集・利用できる技術」について、被災地からの詳細情報が届かない段階で

あっても建物被害を迅速・大まかに推定する手法及び地震被害推定システムを開発し、技術移転を行った。図2.4.3に震度分布の推定結果および図2.4.4に地震被害推定システムを用いたデモの様子を示す。



(1) 中国四川地震の震度分布推定結果



(2) ハイチ地震の震度分布推定結果

図2.4.3　震度分布の推定結果

図2.4.4　APEC における地震被害推定システムを用いた日本–タイ間の国際デモの様子

2.4.3　第3期中期計画

(1) 概要

第3期中期計画においては、ネットワーク基盤技術の研究開発の一分野として「ネットワークセキュリティ技術の研究開発」に焦点を当て、「サイバーセキュリティ技術の研究開発」、「セキュリティアーキテクチャ技術の研究開発」及び「セキュリティ基盤技術の研究開発」が進められている。研究体制としては「ネットワークセキュリティ研究所」の下、1室3研究室体制（企画室、サイバーセキュリティ研究室、セキュリティアーキテクチャ研究室、セキュリティ基盤研究室）となった。

(2) 研究成果

a) サイバーセキュリティ技術の研究開発（第2期中期計画期間の成果を含む）

平成17年度にインシデント分析センター“NICTER”の基礎検討を開始し、ダークネット（未使用のIPアドレス群）に届くトラフィックからインシデントの自動検出を行う分析エンジンや世界地図上でのダークネットトラフィック可視化エンジン（図2.4.5）のプロトタイプ開発を行うなど、ダークネット観測に関する実現可能性の検証を行った。

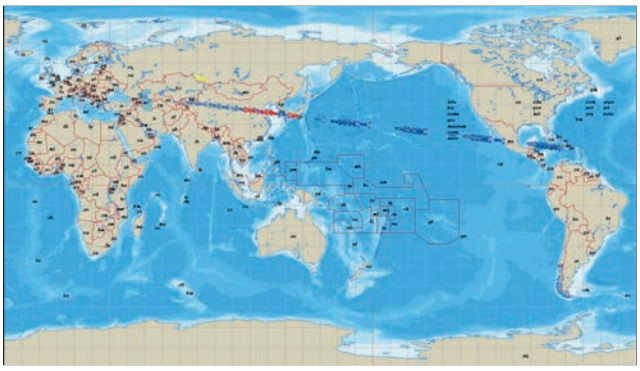


図2.4.5　2D版ダークネットトラフィック可視化エンジン（平成17年度）

平成18年度は、マルウェアの自動解析システムの研究開発に着手するとともに、マルウェア検体の収集機構の整備を開始した。また、ダークネットトラフィックを3D表示する可視化エンジン（図2.4.6）のプロトタイプ開発を行った。

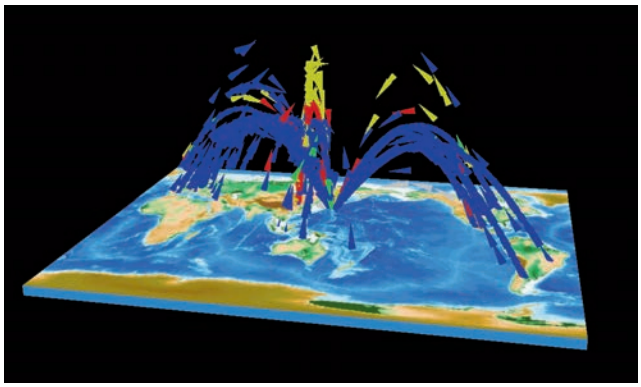


図2.4.6　3D 版ダークネットトラフィック可視化エンジン（平成18年度）

平成19年度には、国内のダークネット観測規模を倍増させ、NICTER の情報収集能力が大幅に向上した。また、NICTER のシステムデザインを一新し、大規模ネットワーク観測に基づくマクロ解析、マルウェア自動解析に基づくミクロ解析、そしてマクロとミクロを融合させたインシデント発生原因の自動推定という基本コンセプトを確立した。さらに、ダークネットトラフィック可視化エンジンの高度化を進めた（図2.4.7）。

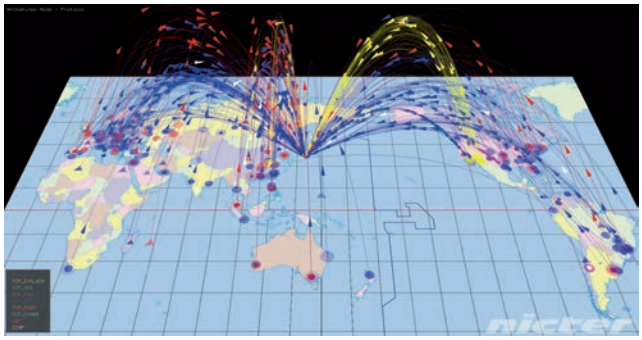


図2.4.7　ダークネットトラフィック可視化エンジン Atlas（平成19年度）

平成20年度は、マルウェア検体の収集体制を強化し、複数の機関からマルウェア検体の提供を受け、ミクロ解析システムにおいて1日あたり数千検体の自動解析を開始した。さらに、ミクロ解析システムを応用した、マルウェア駆除ツールの自動生成及びユーザへの自動配布システムのプロトタイプ開発を行った。

平成21年度には、ダークネット観測規模を14万アドレスまで拡大するとともに、マルウェア検体収集能力強化を図るため高対話型ハニーポットを開発し、運用を開始した。また、外部の研究者に NICTER の各種収集情報を安全に提供するためのオープンプラットフォーム“NONSTOP”（ノンストップ）の開発と試験運用を開始した。さらに、ライブネット（稼働中のネットワーク）のリアルタイム可視化システム“NIRVANA”（ニルヴァーナ）（図2.4.8）を開発し、国内企業への技術移転を行った。

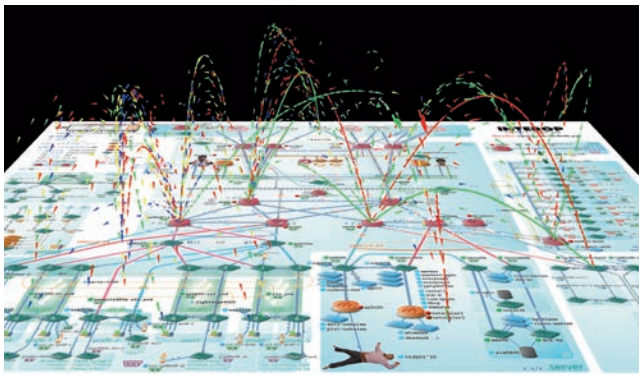


図2.4.8　ネットワークリアルタイム可視化システム NIRVANA（平成21年度）

平成22年度は、大規模ダークネットに基づくアラートシステム“DAEDALUS”（ダイダロス）の開発を本格化させ、アラートの集約手法を確立するとともに、アラート管理用の Web インターフェイスの開発を行った。また、機構内ネットワークに DAEDALUS 及び NIRVANA を導入し、実環境での試験運用を開始した。

平成23年度は、異種センサを能動的に切り替え可能にする新たなダークネット観測アーキテクチャを設計し、基礎評価を行った。また、ダークネット観測結果を応用し、被災地周辺のネットワークの死活状況の推定を行うシステム ACTIVATE の提案と基礎評価を行った。さらに、Web を介したドライブ・バイ・ダウンロード攻撃対策フレームワークの基礎設計及びプロトタイプ開発を行った。また、NICTER の観測結果の一部について、Web サイト“NICTER Web”（ニクター・ウェブ）（図2.4.9）での外部公開を開始した。

平成24年度には、DAEDALUS のアラート発生状況をリアルタムに俯瞰可能な可視化エンジン“DAEDALUS-VIZ”（ダイダロス・ヴィズ）（図2.4.10）を開発するとともに、DAEDALUS のアラート情報を外部展開するための仕組みを整備し、国内企業への技術移転を行った。また、ダークネット観測規模を21万アドレスに拡大するとともに、サイバーセキュリティ分野における国際連携の一環として、NICTER センサの海外展開を実施した。

さらに、標的型攻撃対策技術の研究開発に着手し、ライブネットに対する各種異常検知エンジンのプロトタイプ開発を行い、NICT 内ネットワークでの実証実験を開始した。

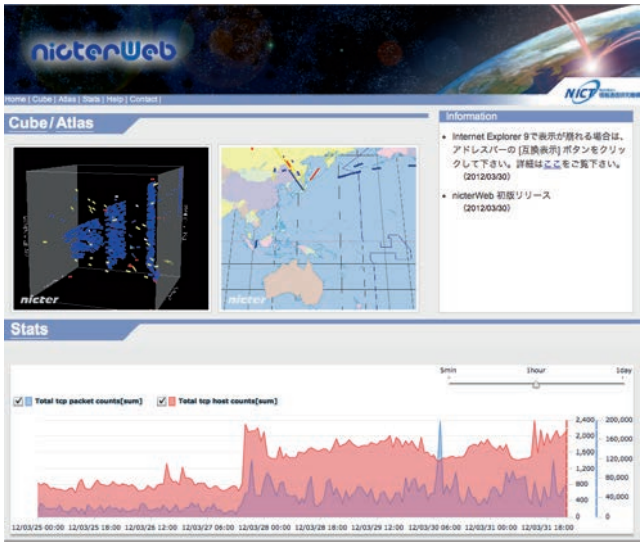


図2.4.9　NICTER Web（平成23年度）

図2.4.10　DAEDALUS-VIZ（平成24年度）

平成25年度は、標的型攻撃対策技術として、サイバー攻撃統合分析プラットフォーム“NIRVANA 改”（ニルヴァーナ・カイ）（図2.4.11）を開発し、ライブネット観測・分析機能に加えて、各種分析エンジンからのアラート集約を可能にする分析基盤技術を確立した。また、NICTER センサの国内外への展開を引き続き実施し、ダークネット観測規模を約24万アドレスに拡大させた。さらに、財団法人地方自治情報センター（LASDEC）との連携の下、地方自治体への DAEDALUS アラートの提供を開始し、研究開発成果の実社会への導入・活用を進めた。

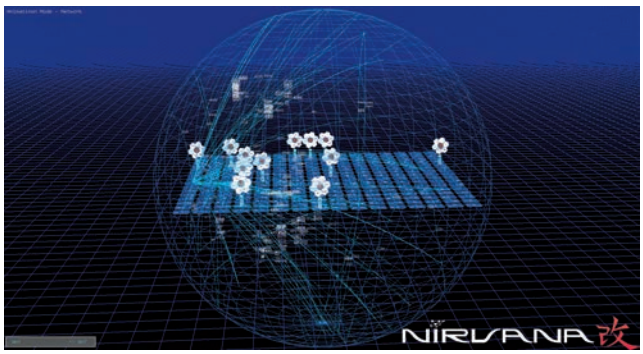


図2.4.11　NIRVANA 改（平成25年度）

b）セキュリティアーキテクチャ技術の研究開発

平成23年度には、ネットワーク利用において適材適所にセキュリティ技術を自動選択し最適に構成するためのセキュリティアーキテクチャの研究開発として、過不足のないセキュリティ技術を判断するための、「セキュリティ知識ベース」及び「分析エンジン」の構築に着手するとともに、個別のネットワーク利用方法におけるセキュリティ上のリスクを可視化する「Risk Visualizer」の構築（図2.4.12）を行った。これは5万レコードの脆弱性データベースからネットワーク利用におけるリスクを可視化することが可能である。

図2.4.12　Risk Visualizer プロトタイプ

ネットワーク上に存在する様々なセキュリティ情報をお互いにリンクし、検索可能にすることにより、インターネットを巨大なセキュリティ知識ベースとする「Discovery」技術を構築した。また、インシデント発生時の情報交換を自動化し、オペレーションの自動化を補助する技術として、セキュリティ情報交換フレームワーク「CYBEX」及びインシデント情報を記述するフォーマット「IODEF extension」を構築した。

平成24年度には、ネットワーク利用者のセキュリティリスクを安全性理論に基づき分析し、可視化する「REGISTA」の構築を行い、その有効性を実証した。また、RFIDタグなどのデバイスにおいても安全な認証方式PUF（物理的複製困難関数）について、世界で初めて物理デバイスを用いて評価を行った。

10兆個のデバイスが接続されることを想定する新世代ネットワークにおいて、スケーラビリティ上問題となる、利用しないデバイスの認証の無効化処理について、従来のlogオーダーの時間で処理が可能な「Revocable IBE/IBS」を確立し、性能上の実証を行った。これは特に使えなくなるデバイスが多数発生する災害発生時に、認証に必要な運用コストを低下させる効果が大きい技術である。

平成25年度には、StarBED[3]（**2.6.3**参照）上にREGISTAシステムと、仮想的なエンタープライズネットワークを構築し、エンタープライズネットワークへのリモートアクセスにおけるリスク評価を行った。また、REGISTAをスマートフォン対応とするために、Androidのアプリケーション解析機能の追加及びその解析結果と脆弱性情報をセキュリティ知識ベースに蓄積できるようにした。さらに、スマートフォン向けのリスク解析結果可視化アプリケーションを開発した。

クラウド上で流通する情報におけるプライバシー保護方式として、匿名認証と部分秘匿認証を同時に行える黒塗り認証、情報を秘匿したまま計算ができる秘匿集合演算方式、インデックスサイズを1/7に削減した検索可能暗号方式を構築し、その安全性を検証した。

c）セキュリティ基盤技術の研究開発

情報通信ネットワークを誰もが安心・安全に利用できるためのセキュリティ基盤技術の研究開発として、量子セキュリティ技術、長期利用可能暗号技術、実用セキュリティ技術、暗号安全性評価技術の高度化をテーマに掲げ、実施している。

① 量子セキュリティ技術

量子セキュリティ技術のネットワーク化を進める上で統一的なセキュリティ評価手法を開発するため、量子秘匿雑音通信方式の安全性評価等を平成23年度に行った。また、量子鍵配送技術と秘密分散技術を組み合わせ、情報理論的に安全な認証機能付き秘密分散方式（図2.4.13）の基本設計を行い、平成24年度には機能拡張及び安全性検証を行った。平成25年度には量子ICT研究室等との連携プロジェクト「量子鍵配送を利用したセキュアネットワークの研究開発」において本認証機能付秘密分散方式を量子ネットワーク上で実装し、秘匿・認証ともに情報理論的安全性が保証された方式の世界初の実装となった。

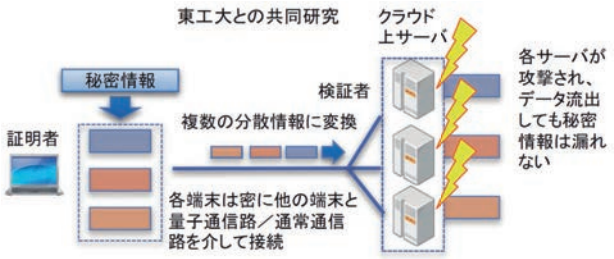


図2.4.13　認証機能付秘密分散方式

② 長期利用可能暗号技術

量子計算機が実現しても安全性を維持できる次世代の公開鍵暗号方式として、平成23年度には格子理論、符号理論の一種であるLPN問題を使った方式の基本設計を行った。また、Braid群を用いた方式の基本設計を行うと共に安全性評価を行った。安全性評価においてはランダムサンプルアルゴリズムを改良し、従来の30倍の高速化を達成した。平成24年度は、格子理論に基づく方式に重点をおいた研究を行い、特に格子暗号の安全性評価に関してはその根拠となる最短ベクトル問題の難しさの評価を行い、これまでの世界記録を上回る825次元の問題を解くことに成功した。平成25年度は、格子理論に基づく新方式として、暗号化後にセキュリティレベルを変更できる世界で初めての方式を創出した。また、格子暗号の安全性評価を進展させた。

③　実用セキュリティ技術

サイドチャネル攻撃等の実装攻撃に対する耐性を備えた実用的なセキュリティ技術の研究として、平成23年度は、コールド・ブート攻撃等による秘密鍵漏洩に対して耐性を持つ内積述語暗号の設計を行い、平成24年度には、機能拡張を行うと共に実装性能評価を行った。また、平成24年度には、センサに実装可能な軽量暗号をクラウド上で高速に並列復号処理する実装法を世界で初めて開発するとともに、軽量暗号に求められる安全性・実装性等の要件を規定した国際標準 ISO/IEC29192 -1 の規格化を完了した。平成25年度は、軽量暗号の評価基盤の構築を開始した。センサ及びクラウドサーバ上で様々な実装性能評価を行い、軽量ブロック暗号の既存暗号に対する優位点を明確化した。さらに、軽量暗号の活用が期待できるアプリケーションとして自動車や制御系、医療機器等でのニーズを調査した。また、機密レベルに応じた処理が可能なセキュアストレージシステム PRINCESS（図2.4.14）を開発した。

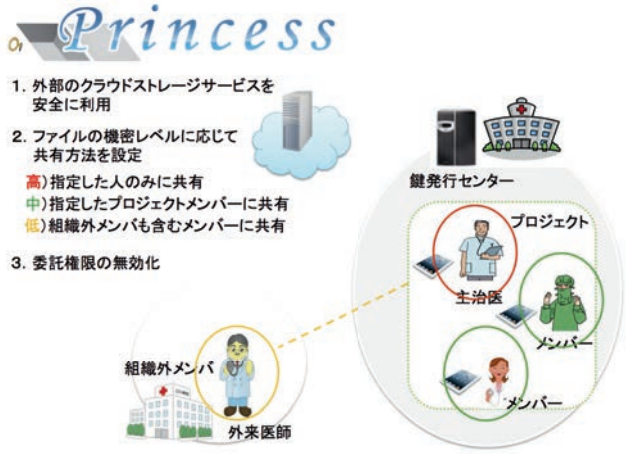


図2.4.14　PRINCESS の医療データ管理への応用例
ファイルの機密レベルに応じた共有方法を設定でき、ストレージ上で暗号化したまま、指定メンバーと安全にファイル共有できる。

④　暗号安全性評価技術の高度化

電子政府推奨暗号の継続的な安全性評価と、将来の暗号技術移行指針への寄与として、電子政府推奨暗号リストに記載されている暗号及び新規応募暗号の安全性評価を行っている。平成23年度から平成24年度にかけては、次世代公開鍵暗号として注目されているペアリング暗号の安全性評価を行うため、その根拠となっている離散対数問題を解く計算機実験を国立大学法人九州大学、株式会社富士通研究所と連携して行い、923ビットの離散対数問題を解くことに、世界で初めて成功した（図2.4.15）。なお、この記録は平成21年に、公立大学法人公立はこだて未来大学と共同で行って達成した世界記録をも遙かに上回る成果となった。また、ネットワーク上での安全な通信を支えている公開鍵認証基盤における公開鍵証明書のデータを収集し、そこで用いられている公開鍵の安全性を高速に検証し、脆弱性の分布を可視化するシステムの構築を平成24年度に開始し、平成25年度には SSL サーバ証明書公開鍵検証システム XPIA（エクスピア）として完成した。

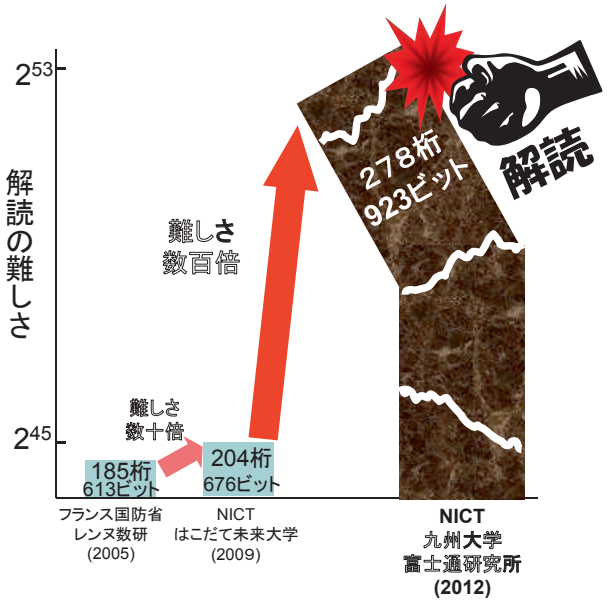


図2.4.15　離散対数問題ベース暗号解読世界記録

d) CRYPTREC

情報通信におけるセキュリティの基盤技術であり、社会インフラに組み込まれつつある暗号技術がその機能を十分に果たしていくためには、容易に解読・危殆化されるものであってはならず、コンピュータの性能の向上や予期せぬ解読技術の発見等を考慮に入れれば、より安全性の高い暗号技術の開発・普及が必要不可欠となってくる。

総務省、経済産業省、NICT 及び独立行政法人情報処理推進機構（IPA）が共同で運営する CRYPTREC は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリストアップすることを目的に評価活動を

開始し、電子政府推奨暗号リスト（平成15年2月20日）を公表し、その後、平成15年度から暗号技術の監視及び評価活動を継続して行ってきた。

さらに、平成24年度には、この電子政府推奨暗号リストを改定し、暗号技術の安全性及び実装性の観点に加えて、政府調達等における入手し易さや導入コスト、相互運用性と普及度合いの観点も取り入れた新しいリストとして、CRYPTREC 暗号リスト（平成25年3月1日）を公表した。

以下に年代ごとの主な活動を記す。

(1) 平成16～20年度

・電子政府推奨暗号の監視を含む、暗号技術の安全性に関する調査（ハッシュ関数 MD5・SHA-1 及び1024ビットの素因数分解問題に対する安全性に関する見解等）を行った。
・暗号モジュール評価基準及び試験基準の策定、暗号モジュールへの非破壊攻撃及び破壊攻撃に関する調査（ISO/IEC 19790及び ISO/IEC 24759策定への協力等）を行った。
・電子政府推奨暗号リスト（平成15年2月20日）の改定に向けた骨子及び公募要項の作成を行った。

(2) 平成21～24年度

・電子政府推奨暗号リスト（平成15年2月20日）の改定に向けた暗号技術の公募及び安全性・実装性評価を行った。
・リストの改定における暗号技術に対する製品化・利用実績等の評価について評価方針や評価基準、国際標準技術等との整合性等の検討を行った。

(3) 平成25年度以降

・CRYPTREC 暗号リスト（平成25年3月1日）記載の暗号技術等の安全性・実装性に関する検討を行った。
・注意喚起レポートの公表や暗号技術ガイドライン（SSL/TLS や SHA-1）の作成を行った。
・暗号の普及促進・セキュリティ産業の競争力強化及び暗号政策の中長期的視点からの取組の検討を行った。