産総研プレス発表資料
解禁日時：資料配付と同時
【平成 24 年 4 月 2 日 14:00】

（別紙 2）

「セキュアシステム研究部門」を設立

― 産業に安全の価値を付加し、セキュアな社会生活実現へ ―

平成 24 年 4 月 2 日
独立行政法人 産業技術総合研究所

■ ポイント ■

・IT システムや情報資産に対する悪意の攻撃や設計の不具合に対する安全策の研究
・電力、鉄道などの国の産業インフラを構成する制御システムの情報セキュリティ対策
・IC チップの安全や高機能の暗号系など先進的セキュリティ研究

■ 概　要 ■

独立行政法人 産業技術総合研究所【理事長 野間口 有】（以下「産総研」という）は、安全・安心で持続可能な社会の実現に向けて、拡大する IT システムと IT サービスの安全な設計と運用のための技術開発を推進するため、セキュアシステム研究部門【研究部門長 松井 俊浩】を平成 24 年 4 月 1 日に設立した。

近年、情報セキュリティの問題は、コンピューターウイルスや政府ウェブサイト改ざんにとどまらず、広範な情報漏えいや原子力関連施設などの重要施設の停止、誤作動など、産業と社会を揺るがすサイバー攻撃被害に発展するリスクをはらんでいる。また、自動車、情報家電などさまざまな機器や設備に組み込まれたソフトウエアの信頼性向上は、産業自体の信頼性確保の重要な要素になっている。また、今や IT 製品、IT サービス産業は、高速性や容量などの性能だけでなく、環境配慮性、ブランド、デザインなどの付加的な価値が競争力を生む時代に入っている。暗号や形式検証など、システムの安全性を保証する技術に関する学術的な蓄積を元に、産業に安全の価値を付加する研究についても戦略的に進める必要がある。

本研究部門は、「インターネットやクラウドにおける IT サービスの安全性向上」、「電力、ガス、鉄道などの産業インフラ防御のための制御システム安全」、「システムの高信頼、高安全に貢献する安全なシステム開発技法」、「量子暗号や関数暗号などの次世代システム安全基盤の整備」の 4 つをターゲットとして研究を行う。

＿＿＿＿＿は【用語の説明】参照

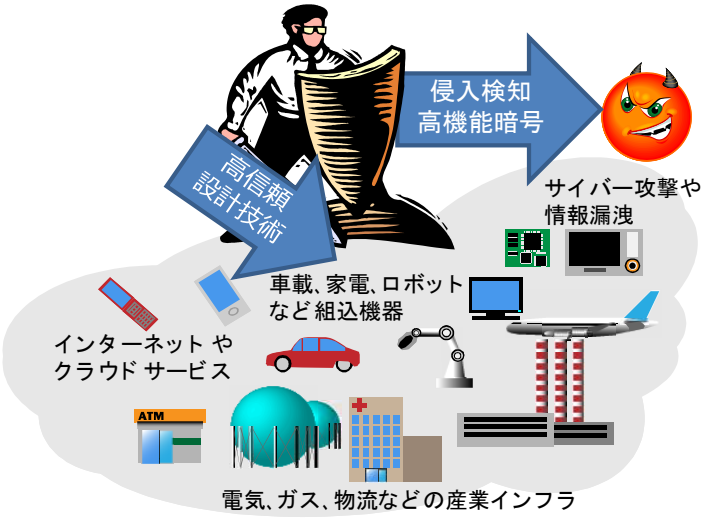

図　セキュアシステム研究部門の研究ターゲット

■ 設立の経緯 ■

本研究部門は、産総研の 6 つの研究分野の 1 つである情報通信・エレクトロニクス分野に属する。情報セキュリティ研究センター、組込みシステム技術連携研究体、情報技術研究部門などに所属する職員から構成される。情報セキュリティ研究センターでは、これまでインターネット閲覧中に情報を抜き取られることを防ぐ HTTP 相互認証、情報漏えいに備えるポータブル暗号･認証システム LR-AKE、メモリー安全コンパイラ Fail-Safe C、仮想化技術を用いてコンピューターウイルスなどマルウエアを検出する技術、サイドチャネル攻撃評価ボード SASEBO シリーズなどの成果を上げてきた。また、広く使われているソフトウエアの脆弱性の発見、無線 LAN 暗号化の脆弱性、署名偽造の影響評価などの情報セキュリティ技術に関連する警告・注意喚起情報を発信してきた。システムのリスクは、これら狭義の情報セキュリティだけでなく、システム設計やヒューマンファクターにも潜んでいる。そこで、これらの情報セキュリティ技術に、システム検証研究センターや情報技術研究部門で行ってきたソフトウエア工学やシステム安全化の技術、さらにデジタルヒューマン工学研究センターで実施してきたヒューマンファクターの研究を統合し、より総合的かつ系統的なシステム安全技術を開発することとした。

■ 研究部門の内容 ■

本研究部門では、数学、物理、ソフトウエア、暗号理論、電子工学、ヒューマンファクターなど、幅広い分野の研究者を集結し、経済産業省 商務情報政策局 情報セキュリティ政策室、独立行政法人 情報処理振興機構、内閣官房情報セキュリティセンター、独立行政法人 情報通信研究機構など関連する外部機関と連携しつつ、以下にあげる 4 点を主要研究項目として実施していく。主要研究項目の概要について、表にまとめる。

1. IT サービスの安全性向上

インターネット上で拡大が続く IT サービスや、そのクラウド化における情報セキュリティ、プライバシー侵害、信頼性への対策を研究する。これら IT サービスに対して、制度や新サービスの技術基準や標準的手法を提案し、システムとしての安全性と利便性の向上に貢献する。より広く IT 社会の安全性を向上させるため、電子情報システムにおける暗号の利用法や、携帯アプリにおけるプライバシー情報の扱い方に関するガイドラインの策定を行う。

2. 産業インフラ防御のための制御システム安全

近年、ウイルスに感染して半導体工場が停止するなど、国内外において制御システムへのサイバー攻撃による被害が発生しており、発電所、鉄道、石油プラントなどの重要産業インフラをサイバーテロから守るための対策技術の開発が求められている。そこで、国内外の制御システム関係者と連携し、従来システムとの親和性・可用性なども考慮に入れながら、システムの乗っ取り検知・対応技術、システムの動的更新技術、多重承認技術などの高可用性確保技術や、各種攻撃テストや評価ツールなどを活用した包括的アセスメント（評価および対応策の検討提示、実施）手法を研究開発することにより、防御策・対応策を講じ、産業インフラの耐性強化に貢献する。また、今後整備される国際規格に準拠した評価･認証制度の確立によって国際競争力増強に貢献する。

3. 安全なシステム開発技法

今や、システムには必ずコンピューターソフトウエアが介在し、多様化するソフトウエアの利用形態や利用期間などに配慮して、最適な品質特性を妥当なコストで実現することが求められている。システムを論理式で記述することで、バグ、エラーの発生を低減させる形式技法や、網羅的なテスト条件を自動生成すること、また、安全なプログラム言語やテストツールの開発など工学的手法によって、主に車載や家電などの組込みシステムの高信頼性、高安全性の実現に貢献する。

4. 次世代システム安全基盤の整備

情報セキュリティの歴史は、攻撃と防御のせめぎ合いであり、攻撃側優位の現状を打開するためには、防御側が先進技術を先回りして開発しておく必要がある。現在は非常に高度で、複雑であるために統一的かつ基盤的な対応が困難と考えられているハードウエアや IC チップのための新しい情報セキュリティ対策技術や、また量子コンピューターによって覆される危険性のある現行の暗号に代わる次世代暗号など、先進的なシステムへの予防的対策技術の創出や科学的解明を行う。システムセキュリティの基盤となる、暗号プロトコルやその LSI 実装に対して、攻撃・評価・対策技術を研究し、方式の標準化と ISO/IEC15408(CC)に基づく試験および認証制度の発展に貢献する。また、ヒューマンファクターの面から、システムを安全に開発･運用する手法を研究する。

表　セキュアシステム研究部門の 4 つの主要な研究項目

	特徴的領域（目的）	守る情報の性質	期待される成果	想定されるパートナー
ITサービスの安全性向上	クラウド、携帯電話やインターネットサービス、電子政府 (サービスの広域化に伴う情報セキュリティ対策)	機密性	・新規サービスへの開発技術の導入 ・業界への技術導入ガイドラインの策定 ・電子政府などのサービス効率化、技術移転など	企業、経済産業省、内閣官房セキュリティセンター（NISC）
産業インフラ防御のための制御システム安全	インフラ系、監視制御系、スマートグリッド (サイバー攻撃被害の激甚化への対応)	可用性	・産学官連携による、産業インフラ防御機能・国際競争力強化への貢献 ・従来システムとの親和性、可用性などを損なうことなく強化可能な防御機能・対応策 ・成果の規格・基準への反映	経済産業省、技術研究組合制御システムセキュリティセンター（CSSC）、電子商取引安全技術研究組合（ECSEC）
安全なシステム開発技法	組込機器、ソフトウエアの開発運用ライフサイクル(高信頼・高安全なシステム実現のための根本対策)	完全性 一貫性 信頼性	・安全なソフトウェアを経済的に開発する手法をパッケージ化 ・情報化社会の脆弱性リスクに伴う無駄なコストの削減への貢献 ・知的財産（ツール・開発指標など）の適用、産業展開	企業
次世代システム安全基盤の整備	ICカードなど向けLSI、クラウドなど応用向き次世代暗号 (次の脅威への備え)	機密性 可用性 完全性	・産学官連携による評価認証制度の発展 ・機能強化された次世代暗号の規格、その実システムへの採用 ・CRYPTRECや脆弱性情報共有など、国の取組みへの貢献 ・論文、知的財産	企業

【用語の説明】

◆制御システム

産業用制御システムのこと。発電所、送電網、鉄道、水道、ガス、石油などのプラントといった重要なインフラ設備を制御・管理するシステムが典型である。一般に制御システムは、ライフラインなどに影響し、連続して安定的に稼働することが求められるため、定期的にシステムを停止してソフトウエアを更新することなどが困難であり、セキュリティ対策が不十分のまま稼働している、させざるを得ないケースが多いという特徴がある。従来は外部ネットワークに接続しない特注のシステムを利用している場合が多かったため、攻撃を受ける頻度は少なかったが、近年はコスト削減などの関係もあり、共通基盤的な制御システムが構築されるとともに、ネットワークに接続して利用されるシステムが多くなっており、ネットワーク経由や内部でのデータのやり取りに用いられる USB メモリーなどを経由してウイルスが混入する事案が報告されている。また、Stuxne など、特定の種類の制御システムをターゲットとしたウイルスによる標的型攻撃が増えて、世界各国で被害が出ている。重要なインフラ設備における制御システムにおいて停止、または、情報漏えいなどが起きると、非常に広範囲に回復不能な被害が発生するため、平時からの適切な対策が必要である。

◆量子暗号

量子効果を利用した暗号技術の総称。旧来の技術では実現できなかった、通信経路中での盗聴があれば盗聴されたことを検出できる、量子鍵配送プロトコル（暗号で用いる鍵情報を送る通信手順）などがある。

◆関数暗号

複数の暗号文を、元のメッセージに戻すことなく、暗号文のままの状態で演算することで、複数の元のメッセージの演算結果の暗号文に変換することが可能な暗号。暗号文のままで意図した計算が行えるため、個人情報などの秘密情報を安全に外部サーバへ送信し、計算処理を委託できる。

◆メモリー安全コンパイラ

C 言語で書かれたプログラムを、不適切なメモリーの書き換えを防止するコンピューター実行形式に変換するプログラム（コンパイラ）。コンピューターのメモリー上にはプログラムやデータが配置され、それらに基づき計算が行われているが、例えば C 言語で書かれたメモリー管理が不適切なプログラムでは、データが配置されていた場所にプログラムを上書きして実行できる場合が存在する。これを悪用したコンピューターウイルスも多数存在する。

◆サイドチャネル攻撃

ハードウエア・ソフトウエアの振る舞いを観測することで、それら内部の状態（典型的には秘密に保持されている鍵情報）を推測する攻撃。暗号を直接解読して、秘密情報を抜き出すのでは

なく、暗号処理にかかる時間、消費電力の変化、回路から発生する電磁波の変化など、ハードウエア・ソフトウエアが動作する際の副次（side channel:サイドチャネル）情報を用いることからこのように呼ばれる。

◆ヒューマンファクター

情報システムなどにおいて、そのシステムの安全性、効率性を考える上で考慮すべき人的要因のこと。

◆IC チップ、LSI チップ

IC（Integrated Circuit：半導体集積回路）をパッケージ化したもの。指先程度の小さな部品であることからこのように呼ばれる。さらに、集積度を向上したものを LSI（Large Scale Integration）チップという。

◆ISO/IEC 15408（CC）

情報技術に関連した製品およびシステムにおいて、情報技術セキュリティ対策が適切に設計され、その設計が正しく実装されているかどうかを評価し、適切な対策が取られている場合に、その製品などを認証するための国際標準規格。IT 製品、IT システムが高度化、複雑化することにより、製品などの安全性について、利用者が独自に評価、確認することが困難になったため、製造者、利用者ではない、中立の第三者の専門家がその対策が適切であるかを評価し、認証する枠組みとして構築され国際的に活用されている。一般に CC（Common Criteria：コモンクライテリア）とも呼ばれる。

◆機密性、可用性、完全性、一貫性、信頼性（表中の語句）

機密性とは、許可された者だけが情報にアクセスできるようにすること。
可用性とは、許可された利用者が必要な時に情報にアクセスできること。
完全性とは、情報が改ざんされていないことを保証すること。
一貫性とは、システムが意図したとおりに動作すること。
信頼性とは、システムが故障しないで動作すること。