

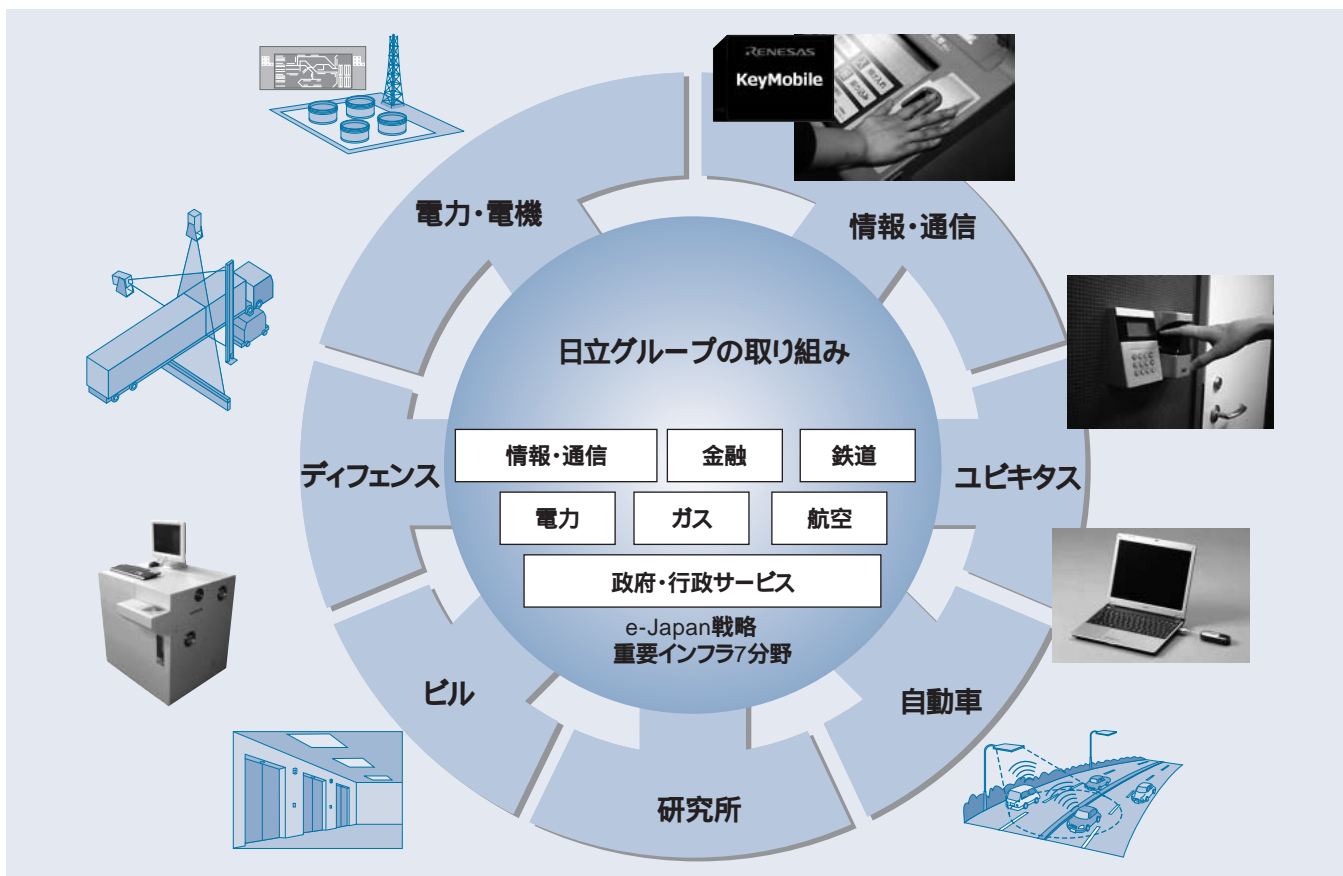
安心・安全な社会の実現に向けた セキュリティの研究開発

R&D of Security for Realization of the Safe and Secure Society

手塚 悟 Satoru Tezuka
洲崎 誠一 Seiichi Susaki

小林 賢 Ken Kobayashi
荒井 正人 Masato Arai

藤城 孝宏 Takahiro Fujishiro



日立グループが取り組む事業領域と「e-Japan戦略」の重要社会基盤分野

IT(情報技術)分野と重要社会基盤分野の両方で事業を展開する日立グループは、事業と研究とを有機的に結合して、セキュリティの面からも企業や社会のライフラインを支えていく。

インターネットやコンピュータシステムが行政や企業活動の基盤として広く活用される中で、フィッシング詐欺や個人情報流出などの問題が多発し、情報セキュリティに対する社会的ニーズが増大している。これを受けて、「e-Japan戦略」といった国家政策や、個人情報保護法などの法整備が推進されており、特に「e-Japan戦略」では、先導的取り組み7分野、IT社会基盤整備5分野のい

ずれでもセキュリティが重要なキーワードとなっている。

日立グループの研究開発部門は、セキュリティを通じて社会に貢献できるように、電子透かしや指静脈認証といったセキュリティコア技術の創生だけでなく、e-Japan戦略をはじめとする社会動向を的確にとらえた研究開発をミッションとし、国家戦略への政策提言などにより、安心・安全な社会基盤の実現を目指している。

1 はじめに

近年、キャッシュカードのスキミングによる不正出金問題やフィッシング詐欺、さらに、情報漏えい問題などが個人の生活や企業活動を脅かすようになり、対策が急務であるセキュリティ問題は多岐にわたっている。

今後、個人の生活から企業活動や行政まで、IT(情報技術)への依存度がいっそう高まるにつれて、さまざまなセキュリティ問題が社会に与える影響度はこれまで以上に大きくなると予想できる。したがって、ITの利活用を推進する「e-Japan戦略」においては、セキュリティへの取り組みが不可欠となっている。

ここでは、日立グループがセキュリティを通じて社会貢献するために研究開発部門が果たすべき役割と、その取り組み内容について述べる。

2 日立グループのセキュリティ研究開発戦略

日立グループにおけるセキュリティ研究開発のミッションは、安心・安全な社会の実現に貢献することであると考えている。そのための研究開発戦略として、次の2点を掲げている。

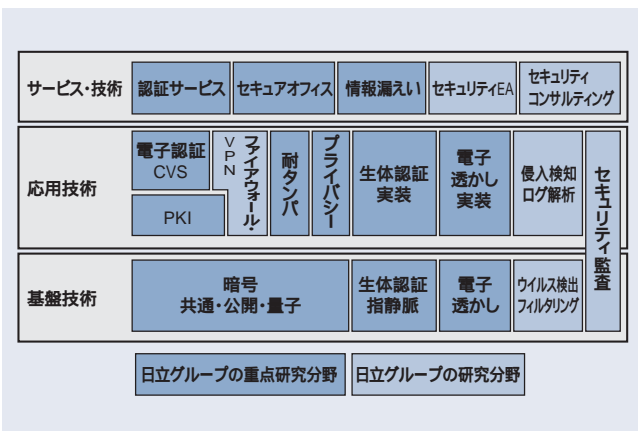
(1) 世界トップクラスの技術創生とソリューションの開発

社会貢献のために強い技術を開発することは、研究所の重要課題である。しかし、グローバル化した今日においては、ただ強いというだけでなく、世界トップクラスの技術である必要がある。そのための取り組みとして、コアとなる技術への研究開発資源の集中と選択、および、他社に先駆けた研究開発の着手と成果を発表している(図1参照)。また、その手段として、国内外のトップレベルにある大学、研究機関などとの共同研究や、国際標準機関に対する標準化提案を積極的に進めている。

それと同時に、強みとなるコア技術を生かして、個人情報情報の漏えい防止など、社会動向を見据えたソリューションの開発も進めている。

(2) 国家戦略への政策提言

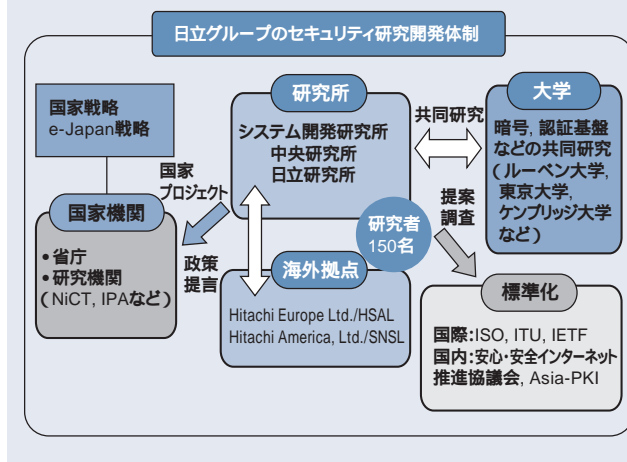
セキュリティは比較的新しい分野であり、国際的にも、米国での「9.11同時多発テロ」以降、急速に立ち上がってきている分野である。そのため、わが国の政府も、セキュリティ対策の立ち上げ期にあたり、さまざまな対策、方針を検討、立案中である。このような状況下では、強い技術を持つだけでは、研究所の活動として十分ではないと考えている。強い技術を先行的に開発する必要性は言うまでもないが、その技術を社会が求めるときが



注:略語説明 EA(Enterprise Architecture), CVS(Certificate Validation Server), PKI(Public Key Infrastructure), VPN(Virtual Private Network)

図1 日立グループのセキュリティ重点研究分野
社会基盤を支える中核的技術は自社開発を進めており、特に、暗号、生体認証、電子認証、電子透かしなどの研究を重点的に推進している。

研究開発戦略 「世界トップクラスの技術創生に向けた研究開発」と「国家戦略への政策提言」とを両輪に推進



注:略語説明

NICT(National Institute of Information and Communications Technology; 独立行政法人情報通信研究機構), IPA(Information-Technology Promotion Agency, Japan; 独立行政法人情報処理推進機構), HSAL(Hitachi Sophia Antipolis Laboratory) SNSL(SAN Solutions Laboratory), ISO(International Organization for Standardization) ITU(International Telecommunication Union), IETF(Internet Engineering Task Force)

図2 日立グループのセキュリティ研究開発戦略と体制

日立グループの研究開発部門は、国内外のトップレベルの大学、研究機関との共同研究や、国の政策と連携した研究開発を推進している。

来るまで待つということでは、あまりにも受け身的であり、消極的である。セキュリティ分野での研究開発に限らず、社会が求めるであろう技術を先行開発することにとどまらず、その技術の価値をユーザーや社会に対して研究者みずから積極的に示していく必要がある。そのための取り組みとして、国の政策と連携した研究開発を進めていくことが重要と考える。具体的には、経済産業省、総務省などIT関連政策を実施する省庁に、国家として取り組むべきセキュリティ対策、ならびにその施策としての研究開発、実証実験を提案している。このような検討は、官民の共同による研究会や委員会などで行われる。

これらの取り組みにより、日立グループが持つ強い技術を核として、国家施策の実現に貢献するとともに、研究開発のさらなる推進に努めている(図2参照)。

3 世界トップクラスの技術創生とソリューションの開発

3.1 日立グループのセキュリティ技術

(1) 暗号・耐タンバ技術

日立グループは早くから暗号の研究を進めており、海外の大学との連携など、国際的な研究開発体制を構築して、共通鍵暗号、公開鍵暗号、暗号実装技術の研究を進めている。

例えば、DES(Data Encryption Standard)に代わ

る次世代の標準暗号であるAES(Advanced Encryption Standard)を開発したベルギーのルーベン大学との共同研究による暗号技術の開発や、ISO(国際標準化機構)での標準化活動を推進している。

(2) 電子透かし技術

電子透かし技術は、コンテンツに情報を目立たないように埋め込む技術であり、コンテンツの著作権保護や流通追跡に威力を発揮する。

近年は、二値画像電子透かし¹⁾²⁾とリアルタイム動画電子透かしの研究を進めている。二値画像電子透かしは、2種類の画素値しか持たないコンテンツ(例えば白黒画像)に情報を埋め込むきわめて難しい技術である。日立グループの二値画像電子透かしは、世界最高レベルの画質を実現している。また、リアルタイム動画電子透かしでは、普及モデルのパソコン上で、QVGA(Quarter Video Graphics Array)サイズの動画に対するリアルタイムでの電子透かし埋め込み処理を世界で初めて実現した。

(3) 生体認証技術

日立グループは、生体認証技術にも早くから取り組んでいる。近年では、生体情報の流出が困難で、認識精度が高く、装置が小型で済む点に特徴がある指静脈認証技術や、顔・指紋・指静脈などの複数の生体認証を組み合わせて、認証精度・受容性・可用性の向上を実現するマルチモーダル生体認証の研究開発を進めている。

3.2 強み技術を生かしたソリューション

日立グループは、強み技術を生かしたさまざまなソリューションを提供している。主なソリューションは以下のとおりである。

- (1) 生体認証ソリューション
- (2) セキュアクライアントソリューション
- (3) 都市セキュリティソリューション
- (4) セキュリティ認証サービス基盤
- (5) 電子透かしプリントソリューション

電子透かしプリントソリューションは、個人情報などの情報漏えいの社会問題化に対応した印刷文書の情報漏えい対策ソリューションとして、日立グループが他社に先駆けて製品化したものである(図3参照)。

このソリューションは、市販のプリンタやスキャナで利用が可能であり、印刷時に「いつ、誰が、どこで印刷したか」という情報を二値画像電子透かしで印刷物に埋め込むことで、その印刷元が特定できるものである。これにより、情報漏えいの抑止と、漏えい時の印刷物追跡管理を実現している。

4 重要インフラ対応セキュリティ

4.1 日立グループが果たすべき役割

政府が世界最先端のIT国家になることを目標にインフラの整備や利活用の促進に取り組んできた結果、日常生活のさまざまな場面でITが普及、浸透してきている。一方、コンピュータウイルスや不正アクセス、フィッシング詐欺などといったサイバー攻撃による被害も著しく増加しており、対策技術の確立が急務となっている。

これに対応し、2005年4月に発表された「情報セキュリティ基本問題委員会」の第二次提言³⁾では、電力や交通、通信など重要インフラの防護を、わが国の「能力保全」、「安全保障」、「危機管理」のための施策であり、官民が協力して強固な基盤を構築することが必要と位置づけている。

日立グループは、社会基盤の整備からITシステムの構築まで幅広く事業を行っている数少ない企業群の一つであることから、重要インフラの防護は、正に日立グループが社会に貢献できる分野であり、今後も重点的に取り組む考えである。

4.2 サイバー攻撃対策技術の確立に向けた研究開発

サイバー攻撃から重要インフラを守るためには、ネットワークの状態を常に監視し、インシデントが発生した際になるべく速やかに対策を講じることが重要である。そのため、複数のネットワーク機器からリアルタイムに収集した情報(マルチレイヤ監視)を、相関関係の有無などの観点で分析(相関分析)し、その結果をネットワーク管理者にわかりやすく伝達する(意思決定支援)とともに、ネットワーク機器のフィルタリング設定などに適切にフィードバック

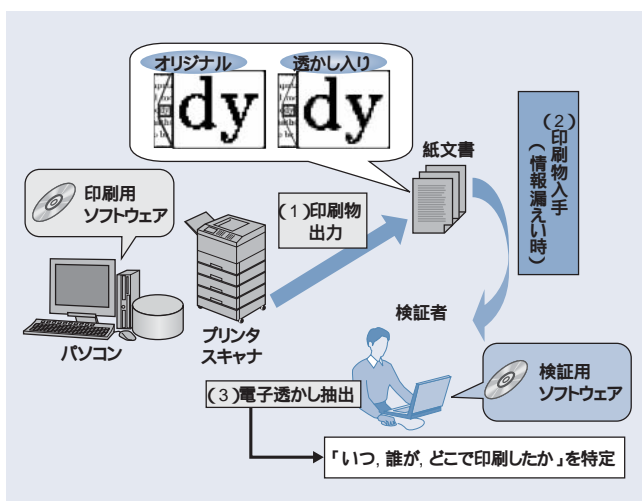


図3 電子透かしプリントソリューションの概要

電子透かし技術により、印刷物に「いつ、誰が、どこで印刷したか」の情報を埋め込むことで、印刷物から印刷元の特定が可能となる。これにより、情報漏えいの抑止と、漏えい時の印刷物追跡管理が実現できる。

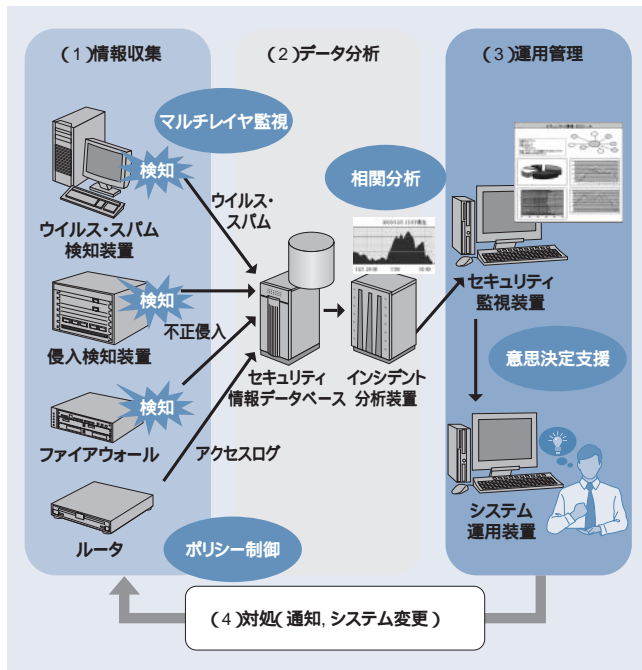


図4 サイバー攻撃対策システムの概要
サイバー攻撃に対処するためには、情報収集から分析、判定、対応措置までの一連のサイクルを適切に実行する必要があります。

くポリシー制御させることを可能とするサイバー攻撃対策システムの研究開発を進めている(図4参照)。

5 おわりに

ここでは、日立グループがセキュリティを通じて社会貢献するために研究開発部門が果たすべき役割と、その取り組み内容について述べた。

高度情報化社会を取り巻く環境では、新たなセキュリティ問題が次々と発生している。日立グループの研究開発部門では、今後も、さまざまなセキュリティ問題に対応するため、さらに進化したセキュリティコア技術の開発を推進するとともに、引き続き、事業と研究とを有機的に結合しながら、いっそう安心・安全・便利な社会の実現を目指す考えである。

参考文献など

- 1) 藤井, 外: 局所特徴量を用いた二値画像用電子透かしの画質維持方式, 情報処理学会論文誌, Vol.44, No.8, 1872~1883(2003)
- 2) 藤井, 外: 電子透かし検出に適した誤り訂正符号の拡張方式, 情報処理学会論文誌, Vol.45, No.8, 1980~1997(2004)
- 3) 内閣官房情報セキュリティ対策推進室ホームページ, <http://www.bits.go.jp/itso/kaigi/kihon/>

執筆者紹介



手塚 悟

1984年日立製作所入社, システム開発研究所 第七部 所属
現在, セキュリティソリューションの研究開発に従事
工学博士
情報処理学会会員
E-mail: tezuka@sdl.hitachi.co.jp



洲崎 誠一

1991年日立製作所入社, システム開発研究所 第七部 所属
現在, サイバー攻撃対策技術の研究開発に従事
工学博士
システム制御情報学会会員, 情報処理学会会員
E-mail: susaki@sdl.hitachi.co.jp



小林 賢

1992年日立製作所入社, システム開発研究所 第七部 所属
現在, コンテンツセキュリティの研究開発に従事
E-mail: k-kobaya@sdl.hitachi.co.jp



荒井 正人

1992年日立製作所入社, システム開発研究所 第七部 所属
現在, セキュリティ評価・監査技術の研究開発に従事
情報処理学会会員
E-mail: m-arai@sdl.hitachi.co.jp



藤城 孝宏

1993年日立製作所入社, システム開発研究所 第七部 所属
現在, セキュリティ認証サービス基盤技術の研究開発に従事
電子情報通信学会会員
E-mail: fujisi@sdl.hitachi.co.jp