これからの社会を守る日立の先進セキュリティ技術

Hitachi Advanced Security Technologies for the Future Life

手塚 悟 Satoru Tezuka
三村 昌弘 Masahiro Mimura
越前 功 Isao Echizen
宝木 和夫 Kazuo Takaragi
高田 安章 Yasuaki Takada

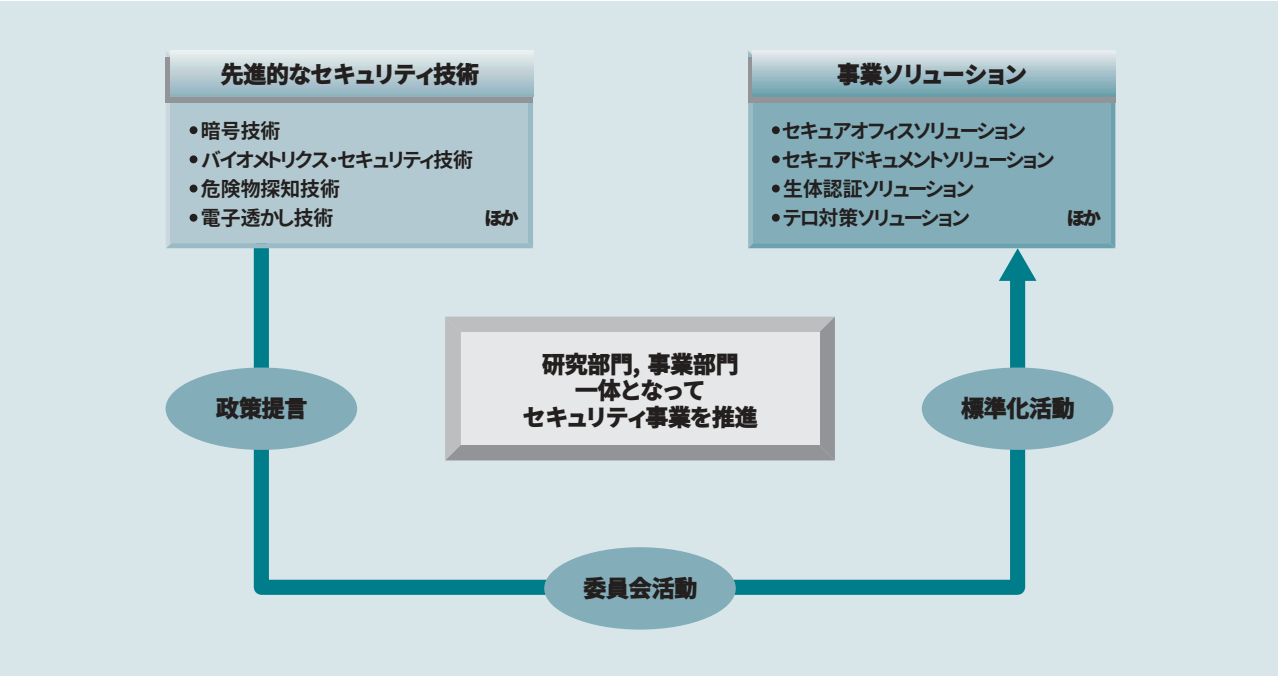


図1 日立グループのトータルセキュリティ事業
日立グループは，安全・安心な社会の実現に貢献するために，先進的なセキュリティ技術の研究開発に注力し，サイバーとフィジカルの両面にわたって幅広くセキュリティ事業を展開している。

1. はじめに

米国同時多発テロ以降，わが国においても，重要インフラの防護など危機管理体制の確立に向けたさまざまな取り組みが検討されはじめている。一方，キャッシュカードの偽造や個人情報の漏えいなど，日常生活を脅かすセキュリティ問題が頻繁に発生しており，その対策が急務となっている。

ここでは，安全・安心な社会生活を実現するために研究開発を進めている，「日立の先進セキュリティ技術」について述べる（図1参照）。

2. 日立の先進セキュリティ技術

2.1 暗号技術

暗号は情報セキュリティを実現するうえで基本となる技術である。周知のように，1980年代のデジタル通信の初期においては，情報を秘匿（とく）することを主な目的として米国標準DES（Data Encryption Standard：データ暗号化規格）が広く用いられた。一方，日立製作所は，わが国のデジタル衛星放送という特殊用途向けに独自暗号「MULTI2」を開発し，標準暗号として提供した。このMULTI2は，現在でも地上波デジタル放送の標準暗号として採用されている。

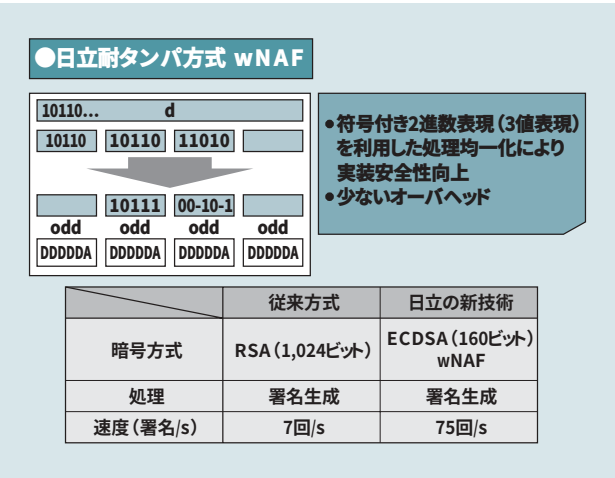
その後，DESの後継としては安全性が強化された米国標準AES（Advanced Encryption Standard）が開発され，2005年にISO18033-3として国際標準暗号となったが，日立製作所は，同じ時期に，ストリーム暗号という原理に基づく，AESに比べ6～7倍高速な「MUGI」を開発し，ISO18033-4国際標準暗号として提供した[1),2)]。さらに，デファクトの利点を生かせるAES，高速性に優れるMUGIをともに製品化し，顧客のニーズに対応できるようにしてきた。現在，本格化しつつあるユビキタス情報化時代をにらみ，従来型の情報秘匿だけでなく，強固な耐タンパ性，情報の改ざん防止，通信相手の認証，著作権保護，プライバシー保護といった要求が強くなっていることから，いっそう高度な暗号方式の研究開発を進めている。

現在，世界各国において無差別テロや広域犯罪などが頻発しており，政府は，電力や交通，通信などといった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。一方，企業活動や個人生活においても機密情報の漏えいやフィッシング詐欺，子どもを狙った犯罪などが急増しており，早期の対策実施が望まれている。日立の研究開発部門では，技術動向や社会情勢を的確にとらえ，指静脈認証技術や危険物探知技術などといった世界ナンバーワンのセキュリティ技術を開発し，安全・安心な社会の実現を目指している。

耐タンパ性とは，暗号処理部分の近くにセンサを当てられても，内部情報を容易に盗まれないように防御する耐性のことであり，携帯電話やICカード，RFID（Radio-Frequency Identification）タグなどといったユビキタス機器のセキュリティを確保するうえで，ことさらに重要な技術である。日立製作所は，「wNAF」と呼ぶ耐タンパ性を有した楕（だ）円曲線暗号の実装方法を開発し，良好な結果を得ている（図2参照）。

2.2 バイオメトリクスセキュリティ技術

バイオメトリクスは，利用者の身体的あるいは行動的な特徴（生体情報）を利用して本人を確認する技術である。近年，バイオメトリクスは電子パスポートや金融機関の指静脈認証装置付きATM（Automated Teller Machine）に採用されるなど，急速に普及しつつある。このような公共性の高い分野にバイオメトリクスを適用するには，装置の性能（精度・処理時間）だけでなく，バイオメトリクス認証装置，あるいはシステムのセキュリティがいっそう重要になる。



	従来方式	日立の新技術
暗号方式	RSA（1,024ビット）	ECDSA（160ビット）wNAF
処理	署名生成	署名生成
速度（署名/s）	7回/s	75回/s

注：略語説明　wNAF（Width-w Non-Adjacent Form）
RSA（Rivest Shamir Adelman）
ECDSA（Elliptic Curve Digital Signature Algorithm）

図2　耐タンパ技術
ICカードなどは外部に露出した端子から容易に電力消費波形などを読まれ，そこから暗号解読される恐れがある。日立はECDSA wNAF手法を開発してこの解読攻撃を回避しながら，従来のRSA公開鍵暗号よりも大幅な性能の向上を得た。速度は株式会社ルネサス テクノロジのICカード用チップ「AE-5」での実装値である。

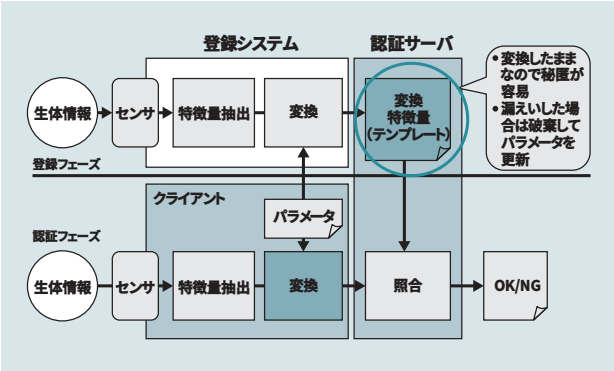


図3　テンプレートを無効化するバイオメトリクス
生体情報に任意のパラメータで特殊な変換を施すことにより，また，漏えい時にはテンプレートを破棄してパラメータを更新することによって，テンプレートを無効化する。

日立製作所は，従来からバイオメトリクスの高セキュリティ化を目的に，複数の生体情報を利用して偽造耐性と精度を高める「マルチモーダル認証技術」[3]，体内の生体情報である指静脈を利用することで，偽造耐性と利便性を高めた「指静脈認証技術」などの研究開発を行ってきた。これらの技術はすでに企業や金融機関の実システムや実証実験システムなどに採用されている。

今後さらなる普及を目指すうえで，バイオメトリクスにはまだいくつかのセキュリティ上の課題がある。その一つは，利用者の生体情報が生涯変更できないため，一度漏えいしてしまうと安全上その生体情報を使用できなくなることである。日立製作所は，これに対応し，システムに登録する生体情報（テンプレート）を無効化する技術の開発を進めている（図3参照）。この技術では，生体情報から抽出した特徴量に任意のパラメータで特殊な変換を施し，変換後の特徴量をテンプレートとして保存する。パラメータがわからなければ変換特徴量から元の特徴量を再構成することはできない。照合は変換特徴量によって行われるため，元の生体情報の秘匿が容易であり，しかもテンプレートが漏えいした場合にはこれを破棄し，新たなパラメータでテンプレートを再生成することで，漏えいしたテンプレートを無効化することができる[4]。

もう一つの課題は，バイオメトリクス認証装置の安全性保証

である。バイオメトリクスには他の情報機器にはない特有のぜい弱性が存在するため，これらのぜい弱性に対して適切な対策がとられていることを確認しなければならない。日立製作所はぜい弱性評価に関する体系的な検討を通じ，ISO/IEC（国際標準化機構/国際電気標準会議）によるバイオメトリクスのセキュリティ評価規格の標準化に貢献している。

2.3 化学分析に基づく危険物探知技術

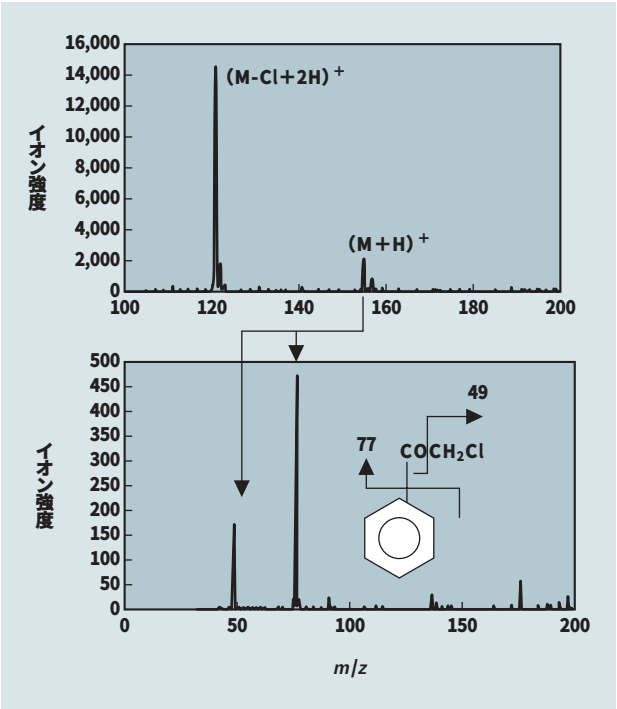
テロや犯罪の未然防止において，最後のとりでとなるのが水際セキュリティである。特に，重要施設の直前で危険物を発見する「危険物探知技術」への期待が大きく，新技術の開発が世界各国で行われている。

日立製作所は，バイオ計測や環境計測で培った質量分析法を活用し，各種危険物の即時検出法を検討してきた。検出対象は，主に爆薬，不正薬物，化学兵器剤である。質量分析法は，物質をイオン化し，その分子量や分子構造情報を得る化学分析法である。物質識別能力に優れているため，高精度の探知が可能である（**図4**参照）。

なお，この研究の成果の一部は，すでに実用化されており，空港向けの爆発物探知機や，工事現場で発見された化学兵器剤の漏えい監視などに用いられている。

この分野においては，爆発物，不正薬物，化学兵器剤などの対象に対して，それぞれ個別に探知機が開発されてきた。しかし，今後は多種多様な物質を同時に監視する能力が求められると考えている。例えば，駅構内の大気雰囲気を採取し，大気中に含まれる化学物質のプロファイリングをすばやく実施できれば，爆発物，引火物，有毒ガス，細菌類など，人間あるいは施設に危害を及ぼす脅威を一度に把握できる。

日立製作所は，今後，試料採取法，イオン化法，質量分析法，分子分解法をいっそう進化させ，高スループットな分子プロファイリング技術を確立し，統合型危険物監視システムの構築を目指す。



注：略語説明　*m/z*（質量電荷比，単位：原子質量単位）

図4　催涙剤クロロアセトフェノンのタンデム質量分析
化学反応により，催涙剤の擬似分子イオンを生成し，そのイオンを質量分析によってより分けた後に分解させて分解物イオンを検出する。分解前後の質量の組み合わせにより，成分を正確に特定する。

2.4 電子透かし技術

日立製作所は，デジタルコンテンツの著作権保護や流通追跡を目的として，「電子透かし技術」の研究開発を進めている。電子透かし技術は，画像や映像などのデジタルコンテンツに，作成者や配布先などの識別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の主張・確認や，不正流出元の特定などさまざまな用途への活用が期待されている。主たる研究テーマである2値画像電子透かしとリアルタイム動画電子透かしについて技術的な特徴を述べる。

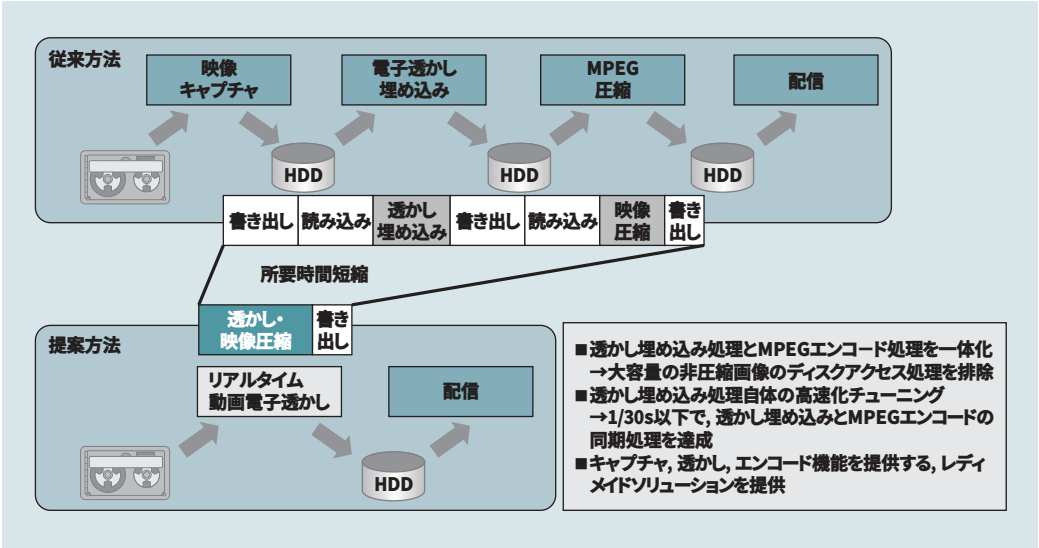
（1）2値画像電子透かし

紙の印刷でよく用いられる2値画像は，情報が白と黒だけで表現されるため，画質が劣化しないように識別情報を埋め込むことが技術課題であった。日立製作所は，これまで開発してきた濃淡画像向け電子透かし技術を生かしながら，認知科学で実証されているゲシュタルトの法則※）などさまざまな人間の視覚特性を利用し，2値画像特有の情報の埋め込みやすさを定量化することで，画質の劣化を回避しながら識別情報を埋め込む方式を開発した。この技術は，印刷文書の情報漏えいの抑止や，漏えい時の印刷物追跡管理に適用可能であり，電子透かしプリント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ている。

（2）リアルタイム動画電子透かし

ネット上のコンサートや遠隔教育など，ライブ映像をリアルタイムで配信するサービスが注目されている中，それら映像の著作権や肖像権保護の対策が急務となっている。ライブ映像では事前にセキュリティ処理ができないため，リアルタイムで映像に識別情報を埋め込む電子透かしが必要となるが，従来の動画電子透かしの処理プロセスでは1時間の映像の処理に数時間を要するなど，ライブ映像配信には実用的ではなかった。日立製作所は，処理コストの大きかった埋め込みやすさの分析処理を高速化するとともに，従来の処理プロセスを全面的に見直すことにより，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

※）ゲシュタルトの法則とは，図形の中に単純な規則性や意味を見いだそうとする心理的機能をいう。人間には，近いものをグループ化して見る，閉じた図形を見いだす，同じ性質を持つものをグループ化しようとするなどの性向がある。



注:略語説明
MPEG(Moving Picture Experts Group)
HDD(Hard Disk Drive)

図5　リアルタイム動画電子透かしの概要
普及モデルのパソコン上で，QVGAサイズの動画に，映像データの取り込み，電子透かし埋め込み，MPEG圧縮のすべてをリアルタイムで処理する技術を世界で初めて実現した。

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(図5参照)。このシステムは，コンサートやスポーツの映像をはじめ，企業の株主総会・記者会見の映像配信や，eラーニングなどを対象とした著作権保護・不正利用検知用途での利用が期待されている。

3. おわりに

ここでは，安全・安心な社会の実現に向けて，日立製作所が研究開発を進めている先進技術の概要について述べた。

新たなセキュリティ問題は，日々刻々と発生している。日立製作所は，今後も，先進的なセキュリティ技術の研究開発にまい進していく考えである。

参考文献など

1) ISO/IEC 18033-4，Stream Ciphers(2005.7)
2) **大和田，外:**MUGI，AES，SHA-1/256**統合ハードウェアの実装，**SCIS2006(2006.1)
3) **日立製作所ホームページ，「ユビキタス時代の個人認証インフラになるマルチモーダルバイオメトリクスシステム」**
http://www.sdl.hitachi.co.jp/japanese/people/bio/
4) **高橋，外:コンピュータセキュリティシンポジウム**2005**，キャンセラブル指紋照合方式の提案**(2005.10)
5) M. Yamada, et al. : On-line Monitoring of Dioxin Precursors in Flue Gas, Analytical Science, 17, 559(2001)
6) Y. Takada, et al. : Detection of Military Explosives by Atmospheric Pressure Chemical Ionization Mass Spectrometry with Counter-Flow Introduction, Propellants, Explosives, Pyrotechnics, 27, 224(2002)

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

宝木 和夫
1977年日立製作所入社，システム開発研究所 所属
現在，暗号技術等セキュリティ基盤技術の研究開発に従事
工学博士
IEEE会員，電子情報通信学会会員，情報処理学会会員，電気学会会員
E-mail:takara@sdl.hitachi.co.jp

三村 昌弘
1997年日立製作所入社，システム開発研究所 第七部 所属
現在，バイオメトリクス認証システムの研究開発に従事
工学博士
情報処理学会会員，電子情報通信学会会員
E-mail:mmimura@sdl.hitachi.co.jp

高田 安章
1990年日立製作所入社，中央研究所 ライフサイエンス研究センタ 所属
現在，質量分析法を用いたリアルタイム計測技術の研究開発に従事
工学博士
日本質量分析学会会員，日本分析化学会会員，日本鑑識科学技術学会会員，火薬学会会員
E-mail:takada@crl.hitachi.co.jp

越前 功
1997年日立製作所入社，システム開発研究所 第七部 所属
現在，電子透かし技術の研究開発に従事
工学博士
IEEE会員，情報処理学会会員，電子情報通信学会会員，映像情報メディア学会会員
E-mail:iechizen@sdl.hitachi.co.jp