Trend

社会の発展に貢献する当社の情報セキュリティ技術

Overview of and Trends in Information Security Technology

才所　敏明 SAISHO Toshiaki
川村　信一 KAWAMURA Shin-ichi
遠藤　直樹 ENDOH Naoki

政治，経済，文化など，私たちの周囲に存在するすべての環境において，IT（情報技術）の活用による発展は必須のものになった。これらのどの領域においても，守るセキュリティから発展のためのセキュリティに変わってきたと見られる。セキュリティが確立されないと，新しい住民サービスや，新しい市場，新しいコンテンツは，手に入らないのである。当社が社会で果たすべき役割は，まさに情報セキュリティ技術があってこそ，全うされる。

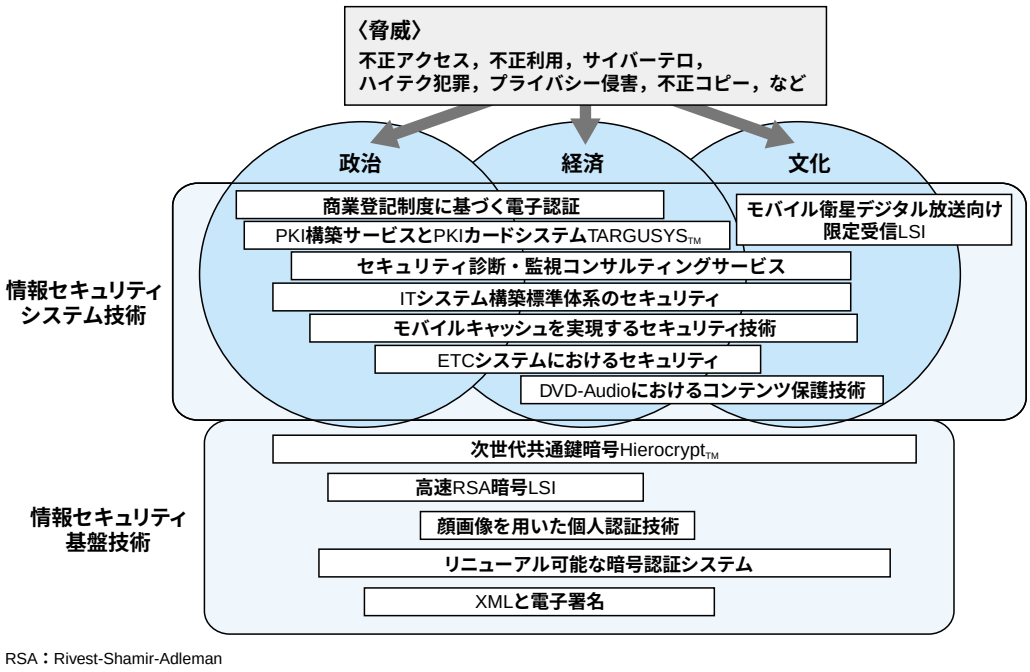
The intensive use of information technology in the political, economic, and cultural areas is essential for the development of society.　In any of these areas, security for development has become more important than security for protection.　If security is inadequate, new government services, new markets for business, and new entertainment contents cannot be offered.
The fulfillment of Toshiba's role in society is embodied by our superior information security technologies.

ますます重要になる情報セキュリティ技術の役割

従来，情報セキュリティ技術に対する期待は，主にネットワーク化やコンピュータ利用の一般化による弊害への対策，とされていた感がある。例えば，不正アクセス，不正コピー，違法・不正行為，プライバシー侵害，などである。

これらが完全に解決されたとは言えないが，情報セキュリティは別の重い使命も負っている。それは，ネットワーク上のサービスを実現し，世の中に繁栄をもたらす基盤技術になることである（図1）。

セキュリティが整っている環境が作れれば，世界中から，ビジネスもマネーもコンテンツも流れ込んでくる。そして，ビジネスや金融や創作が活発化する生産的，発展的な地となる。わ



RSA：Rivest-Shamir-Adleman

図1．当社のセキュリティ技術が貢献する領域　政治，経済，文化に直接貢献するシステム技術及びサービスと，それらを成立させる基盤技術とから成る。
Toshiba security technologies contributing to entire society

れわれの役割は，この目標に向かって技術を磨き上げていくことである。ここでは，この特集で紹介される当社での情報セキュリティ技術への取組みと，その動向について述べる。

当社での情報セキュリティ技術への取組み

暗号技術は，情報セキュリティを実現するうえで欠かすことのできない基本技術である。1970年代後半に，64ビットブロック，56ビット鍵（かぎ）のDES（Data Encryption Standard）方式が米国の暗号規格となった。その後，DESを三重に適用する112，又は168ビット鍵のトリプルDESで安全性を維持してきた。更に，米国は128ビットを処理ブロックとし，128/192/256ビット鍵に対応したAES（Advanced Encryption Standard)方式を公募し，ベルギーから提案されたRijndaelが選定された。

共通鍵暗号 Hierocrypt™

このような暗号の世代交代の時期を迎えるにあたって，当社も次世代の暗号方式としてAES仕様に準拠した独自暗号方式Hierocrypt™-3と，トリプルDES相当仕様のHierocrypt™-L1を開発し，情報処理振興事業協会（IPA）による政府調達向け暗号の評価プロジェクトにこれを応募した。国内，国外の専門家による多角的な評価の結果，Hierocrypt™は安全性及び処理性能の両面において優れた方式であることが確認された。

Hierocrypt™は，独自の入れ子型SPN（Substitution Permutation Network）構造を採用し，もっとも汎用性が高く強力な暗号解読法と考えられている差分解読法と線形解読法に対して理論的に安全性を保証している。また，Hierocrypt™は，SQUARE攻撃というSPN構造に特化した攻撃法に対しても十分な耐性を持つことがAES（Rijndael）提案者らによって学会にて発表されている(1)。Hierocrypt™は，ソフトウェア及びハードウェアの処理速度も高速であり，特に処理の並列度が高いため，ハードウェアでの処理速度は世界トップレベルである（**囲み記事参照**）。

電子署名とそのための高速LSI

電子政府(注1)の本格稼働を前に，電子署名法が2001年4月から施行されている。これにより，電子署名の利用がいっそう拡大する。現在，電子署名は公開鍵暗号方式によって実現されるのが一般的である。

電子署名の普及を図るうえで，公開鍵暗号方式には実装上二つの技術課題がある。一つは，小型化低消費電力化の進む端末機器で，処理ステップ数の大きい電子署名作成を効率よく行うことである。二つ目の課題は，サーバなどセンター側で多数の署名を発行する際のオーバヘッドを小さくすることである。

両課題とも専用の公開鍵暗号処理LSIの開発が解決策となるが，その仕様はまったく異なる。前者は小型・低消費電力であること，後者は高速であることが重視される。当社は，並列処理可能な計算アルゴリズムを考案し，センター側処理にも対応できるLSIの開発を手がけている。

顔画像を用いた個人認証技術

あらかじめ登録された人物かどうかを認証する技術で，極めて有用である。

この特集では，当社が開発した顔画像による個人識別について紹介する。ここでの処理の流れは，カメラにより取り込まれた画像から顔の領域を抽出し，次に正規化画像の切出しにより特徴点を抽出し，最後に登録されている顔画像との照合による識別処理を行う。

技術課題は，顔の向きや表情の変化への対応，照明の変動への対応，顔の経年変化への対応がある。

認識性能と処理時間との間にはトレードオフがあるが，当社の顔画像識別技術によればPentium®(注2) Ⅱ（450 MHz）でのリアルタイムの識別でも約99.5 %の識別率を達成できる。

この顔画像識別技術は，当社のカメラ付きミニノートパソコン（Libretto ff1100V）にSmartface™という名称でバンドルされており，スクリーンロックの解除や個人ごとに設定したソフトウェアの起動などを行うことができる。

リニューアル可能な暗号認証システム

暗号認証技術が応用され実現されたシステムにおいて，暗号や認証のセキュリティ強度は，コンピュータ技術の進歩などで，年を経るとともに相対的に低下する。また，新たな標準化やデファクト スタンダード（事実上の標準）化により，新たなアルゴリズムに移行する必要性も生ずる。一方，暗号化の対象は，テキスト，映像，音楽など様々で，セキュリティの強度やコストのバランスが異なることが多い。

これらの要請を満たすためには，暗号認証アルゴリズムをセキュア（安全）に，かつ低コストで更新する必要性が生ずる。この必要性に基づいて，暗号認証システムのリニューアル技術を開発した。

XMLと電子署名

インターネットにおけるXML（eXtensible Markup Language）の利用が注目されている一方，電子署名の必要性が高まっている。XMLに署名をする場合，部分署名や多重署名などが可能である。標準として，W3C（World Wide Web Consortium）でXML-Signatureが提案されている。

（注1） 行政を効率化し国民負担の軽減を図るため，申請届出手続きや政府調達など，行政手続きの電子化を実現するシステム。
（注2） Pentiumは，米国Intel Corporationの登録商標。

暗号アルゴリズム標準化

暗号アルゴリズムについて標準化が進められつつある。情報セキュリティ技術の中で，暗号アルゴリズムはもっとも基本的な部品であり，次に挙げる五つがその主なものである。

(1) 共通鍵ブロック暗号
(2) 公開鍵暗号
(3) (共通鍵)ストリーム暗号
(4) ハッシュ関数
(5) 乱数生成アルゴリズム

また，暗号アルゴリズムの標準化が現在進められている背景には，次のようないくつかの要因がある。

(1) インターネットなどITの普及によるニーズの高まり
(2) 従来使われてきたアルゴリズムの陳腐化
(3) 国際協調

標準方式を定めることで，相互接続性の向上，製造コストの低減が期待できることは言うまでもない。

米国のNIST(National Institute of Standards and Technology)は，これまで標準共通鍵ブロック暗号方式として広く使われてきたDES方式の安全性が十分でなくなったことを受けて，次世代向け政府調達規格としてAESの選定を2000年に終え，その出版準備を進めている。

わが国では，総務省と経済産業省が連携して2003年の電子政府での利用を目指して方式を公募し，暗号技術評価委員会(CRYPTREC)により暗号技術(1)～(5)の評価を進めている。CRYPTRECは，初年度にあたる2000年度の評価結果を“暗号技術評価報告書”とし公表(http://www.ipa.go.jp/security/enc/home.html)しているが，その中で当社提案のHierocrypt$_{TM}$-3(128ビットブロック暗号)及びHierocrypt$_{TM}$-L1(64ビットブロック暗号)は，当該カテゴリにおいて安全性，処理速度ともに最高レベルである，との評価を得ている。

一方，欧州では産業界のサポートを受けて，CRYPTRECとほぼ同じカテゴリについて方式公募を行い，暗号技術の専門家による評価プロジェクト“NESSIE”(New European Schemes for Signatures, Integrity, and Encryption)を推進中である。更に，国際標準化機構(ISO)でも暗号アルゴリズムの標準化の審議が始まっている。これらの状況を**上表**にまとめた。

このような，国家レベル標準化の動きのほかに，DVDの著作権保護方式のように特定システムや特定業界向けに固有の方式を選定する動きもある。適用範囲が特定システムに閉じている場合には，他システムとの相互接続性の重要度が高くないため，特定システムに最適な方式を選べること，他のシステムで採用されている暗号が解読された場合でもその影響が波及しないなど，利点も少なくない。

多数の暗号アルゴリズムが提案され，既に少なからぬ数の業界固有の方式が普及していることを考えると，今後は国際規格などに定められた標準方式と，複数の業界固有の暗号方式が共存していくことになろう。

暗号アルゴリズム標準化の動き

	米　国	日　本	欧　州	ISO/IEC JTC1
名　称	AES	CRYPTREC	NESSIE	−
期　間(年)	1997 − 2001	2000 − 2003	2000 − 2002	2000 − 2003?
目　的	FIPS制定	電子政府向け	欧州域内利用	国際規格
対　象	・128ビット共通鍵ブロック暗号	・共通鍵ブロック暗号 ・公開鍵暗号 ・ストリーム暗号 ・ハッシュ関数 ・乱数生成	・共通鍵ブロック暗号 ・公開鍵暗号 ・ストリーム暗号 ・ハッシュ関数 ・乱数生成	・共通鍵ブロック暗号 ・ストリーム暗号 ・公開鍵暗号
窓　口	NIST	IPA/TAO	ルーベン大学	SC27/WG2

FIPS　：Federal Information Processing Standards
IPA　：Information-technology Promotion Agency
TAO　：Telecommunications Advancement Organization of Japan
IEC　：International Electrotechnical Commission
JTC1　：Joint Technical Committee 1
SC27/WG2：Sub Committee 27/Working Group 2

当社では，この標準規格をベースとして，Webブラウザ上でXMLに署名可能なプラグインを開発した。応用分野として，電子申請，電子商取引(EC：Electronic Commerce)，医療情報分野などがある。

商業登記制度に基づく電子認証

インターネットを利用したECは，急速な勢いで広まってきている。時間や場所の制限を受けないインターネットは，商取引を効率的に行うためのもっとも有効な手段であると言える。一方，従来の商取引は印鑑証明書や対面に立脚した世界を前提としているため，ECにはこれまでの法律や制度だけでは決して十分とは言えず，新たな仕組みが必要となってきている。

今般，法務省はデジタル社会において印鑑証明書と同等の意味を持つ電子証明書を発行する電子認証局を設立し，併せて法律の整備も実施した。

こうした動向のなかで当社は，民間企業が法務省の電子証明書を取得するために必要な申請受付端末を開発し，全国の登記所へ納入を開始した。また，電子証明書を扱うために必要な企業向けの利用者ソフトウェアを開発した。

モバイル衛星デジタル放送向け限定受信LSI

衛星デジタル音声放送に関する電気通信技術審議会の答申では，正当な契約者にだけ情報を提供するための限定受信シンタックス（文法）として，既存のシンタックスのほかに，衛星デジタル音声放送に適した新シンタックスが規定されている。当社は，この規定に従ってモバイル向けの衛星デジタル音声放送システムを開発している。当社が開発した限定受信LSIは，このシンタックスに準拠するとともに，安全で処理効率の良い暗号認証技術（鍵配送や契約情報管理などのため）を用いている。

PKI構築サービスとPKIカードシステムTARGUSYS™

当社は，PKI（Public Key Infrastructure）構築サービスを実施している。このサービスにおいて，デファクト スタンダードとなっているシステムをベースとして，認証局構築サービス，及び，当社の暗号ミドルウェアを活用したPKIカードシステムTARGUSYS™によるPKIカード管理システム構築サービスを実施している。

セキュリティ診断・監視コンサルティングサービス

インターネットに接続されたコンピュータシステムを利用し，運用管理する場合，そのセキュリティ上の問題がどこにあり，対策は何かをあらかじめ知り実行することがたいせつである。また，その対策をとった後でも，不正な侵入が実行されていないかを監視することが，たいせつな情報資産を守るために不可欠になった。

当社では，セキュリティ診断・監視，セキュリティポリシー作成支援などのサービス，及びコンサルティングを実施している。セキュリティ基準やポリシーに対する国際標準化や認定制度発足もにらみながら活動している。

ITシステム構築標準体系のセキュリティ

当社では，Web-Topシステムを中心としたITシステム構築の標準体系を整備している。この体系におけるブラウザ，Webサーバ，Webアプリケーション，データベースアクセスなどについて，セキュリティを確保する標準的な仕組みを開発した。

モバイルキャッシュを実現するセキュリティ技術

携帯電話若しくは携帯端末と自動販売機とをBluetooth™(注3)無線技術により接続し，自動販売機の商品の購入，決済を行うモバイルキャッシュシステムを試作した。楕円（だえん）曲線暗号に基づく電子署名技術により，簡便な処理が可能な，商品を購入するためのバリュー（一種の電子マネー）を携帯端末へ格納するセキュア プロトコル，及び購入のためのプロトコルを提案している。

ETCシステムのセキュリティ

近年注目の集まっているITS（高度道路交通システム）の中で，実用化段階に入ったETCシステム（ノンストップ料金収受システム）を開発，事業化した。ETCでは，料金を自動的に，正当にかつ安全に収受する仕組みが，システム実現のキーポイントである。

DVD-Audioにおけるコンテンツ保護技術

当社は，松下電器産業（株），Intel社及びIBM社と共同で，DVD-AudioのためのCPPM（Content Protection for Prerecorded Media）技術を開発した。主な技術要素は，ブロック暗号C2（Cryptomeria Cipher）及び鍵管理技術MKB（Media Key Block）である。

（注3） Bluetoothは，その商標権者が所有しており，当社はライセンスに基づき使用している。

社会の発展を支える情報セキュリティ

当社は，政治，経済，文化に寄与する広範な事業分野を持ち，それぞれの分野における社会の発展を目的とした情報セキュリティ技術，及び応用システムの開発を実施してきた。インターネット利用は更に普及し，社会制度，ビジネス上の取引き，国民生活に深く浸透していく。また，新たな高速ネットワークの研究開発が行われているとともに，次世代の多機能放送システムの構築も進められている。

このような情勢を考慮して，当社は，新しい社会的要請にこたえることのできるセキュリティ技術開発とその普及にまい進している。

文　献

(1) Baretto, P.S.L.M., et al. "Improved SQUARE Attacks Against Reduced-Round HIERO-CRYPT". Preproceedings of Fast Software Encryption Workshop 2001, 2001.

才所　敏明
SAISHO Toshiaki
e-ソリューション社　SI技術開発センター　戦略企画担当参事。
暗号・情報セキュリティの研究・開発に従事。情報処理学会，CSI，ACM，IEEE会員。
Systems Integration Technology Center

川村　信一
KAWAMURA Shin-ichi, D.Eng.
研究開発センター　コンピュータ・ネットワークラボラトリー主任研究員，工博。暗号・セキュリティ技術の研究・開発に従事。電子情報通信学会，情報処理学会，IEEE，IACR，SITA会員。
Computer & Network Systems Lab.

遠藤　直樹
ENDOH Naoki
e-ソリューション社　戦略企画室参事。
情報セキュリティ技術及び同技術応用システムの開発に従事。電子情報通信学会，日本セキュリティマネジメント学会会員。
e-Solution Co. Strategic Planning Div.