情報セキュリティ技術の発展と東芝グループの取組み

Toshiba Group's Efforts in Information Security Technology Field

山田　朝彦　■ YAMADA Asahiko
新保　淳　■ SHIMBO Atsushi
北折　昌司　■ KITAORI Shoji

情報の保護を目的とする情報セキュリティ技術は，社会生活でIT（情報技術）が適用される範囲や機会の増大，それに伴う脆弱（ぜいじゃく）性をついた攻撃の増加などに対応することによって発展し，もはやITに不可欠の技術となった。更に，設計や実装の妥当性が問われるようにもなり，情報セキュリティに関するこれら諸側面の評価・認証制度も確立された。

東芝グループは，システム構築における情報セキュリティ技術の確実な実装，コンテンツ保護をはじめとする諸製品への適用，及び次世代情報セキュリティの基盤となる技術の研究開発を進めることで，社会生活における諸活動の発展に貢献している。

Information security technologies are an increasingly critical element of information technology for the protection of information. As information security technologies become more widespread, an important issue is how securely they are designed and implemented.

In line with these trends, the Toshiba Group is working on the development of secure implementation methodologies for system integration, the application of information security technologies to various products including digital contents protection, and next-generation fundamental technologies. Our aim in these development activities is to contribute to the improvement of people's lives.

情報セキュリティ技術の発展

社会における諸活動の成長と発展のために，IT革新による機会創造は欠かせないものとなっている（**図1**①）。インターネットを利用した商取引，オンラインショッピング，及び官公庁の電子申請などはその典型である。

しかし，ITの革新はリスクを内在している。なぜなら，多くのITが必ずしも完全なものではなく，何らかの脆弱性を持っているからである。こうした脆弱性の存在が，ウィルスの蔓延（まんえん）による業務不能，貴重な情報の外部持出しなど犯罪的行為誘発の要因にもなっている（図1②）。

ITに潜むこれらの脆弱性とそれに伴う犯罪的行為は，社会を混乱させ，社会的問題になっている場合もある。その結果として，情報セキュリティに対する社会的要求が起こり，それに伴って法制度も整備されるようになってきた（図1③）。2003年に施行された個人情報保護法は，その一例である。

それぞれの組織は，こうした社会情勢を背景に，遵法だけでなく，社会に対して情報セキュリティを確保する責任を負うべき主体として，重要な役割を果たすことが求められている。企業の場合には，これはCSR（Corporate Social Responsibility）の一環と考えられ，企業の成長と発展には不可欠な要素となっている（図1④）。

情報セキュリティ技術は，IT革新をシーズ（種）とし，社会的要求や法制度整備をニーズ（要求）としながら，ITシステムに潜む脆弱性を軽減し犯罪的行為を抑止するために，発展を遂げてきている（図1⑤）。

また，情報セキュリティ技術もITの一部であるから，冒頭に述べたように私たちの諸活動を成長及び発展させている（図1⑥）。交通システムの料金収受やコンテンツの保護は，その一例である。情報セキュリティ技術からは犯罪的行為を

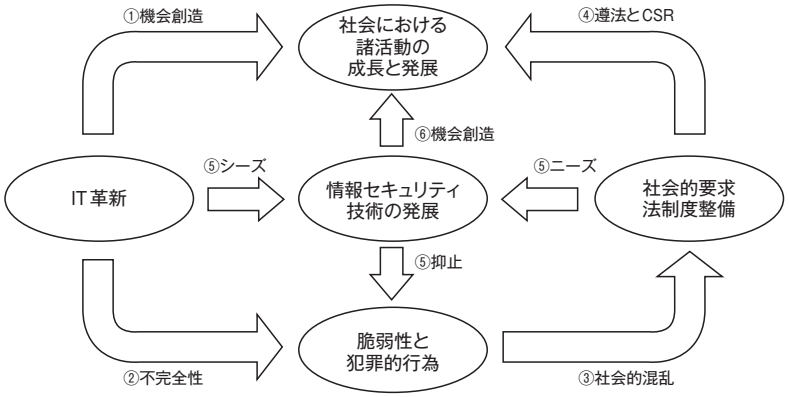


図1. 情報セキュリティ技術の発展要因 — 情報セキュリティ技術の発展は，種々の技術的・社会的な要因によって成されている。
Factors in development of information security technology

抑止するというネガティブな印象を受けやすいが，このように，新たな価値やビジネスを生み出すというポジティブな側面もある。

以上のように，情報セキュリティ技術は，図1のサイクルを円滑に循環させることで，結果的に私たちの生活のいっそうの発展と情報化社会の安定に不可欠なけん引役として，今後ますます重要性を増すものと考えられる。

情報セキュリティ技術をいかに確実に作り込むか

10年前であれば，製品やシステムの開発において，情報セキュリティは後回しと考えられていたかもしれない。しかし，ほとんどすべてのコンピュータがネットワークにつながり，各組織のシステムがインターネットに接続されるようになって，情報セキュリティを考慮せずに製品やシステムを開発することは不可能になった。情報セキュリティ技術の適用を専門家だけに任せていた時代は既に終わり，それは開発者みずから担当すべき業務だとする認識が常識になりつつある。

情報セキュリティ技術は，情報を保護する技術なので，確実に作り込まれていなければ意味がない。確実に作り込まれていることを示すには，一般に第三者評価という方法が取られる。情報セキュリティ分野についても同様であり，CC（Common Criteria）が登場し，1999年に国際標準化されてISO/IEC 15408(注1)になり，続いて各国でこれに基づく評価・認証制度が開始された。東芝グループにおいても，旅券冊子用ICなど経済産業省による認証を取得した製品やシステムが増えている。また，政府機関統一基準が2005年末に作成され，ISO/IEC 15408認証取得は官公庁システムの調達基準になった。今後，ISO/IEC 15408が官公庁以外のシステムにも影響を与えていくことは，確実である。

暗号モジュールについても，客観的な評価が必要であると考えられるようになり，米国標準のFIPS140-2(注2)を基に2006年に国際標準ISO/IEC 19790が発行された。国内でも2006年から情報処理推進機構が，FIPS140-2に基づく評価・認証制度JCMVP（Japan Cryptographic Module Validation Program）の運用を開始した。東芝ソリューション（株）の暗号モジュールは，その第1号の認証を取得している。

情報セキュリティ技術の適用範囲が広がったことから，専門家以外の技術者による技術適用が一般化したと同時に，確実な実装への要求も高まってきている。クレジットカード情報と取引情報を扱うシステムについて，国際クレジットカード会社5社はPCIDSS（Payment Card Industry Data Security Standard）を策定した。これは，確実な情報セキュリティを要求する動きの一例である。こうした動きに対応するためには，確実な情報セキュリティを作り込むための開発標準及び開発方法論が必須である。

東芝グループにおける最近の情報セキュリティ研究開発

この特集では，東芝グループにおける情報セキュリティ技術の研究開発の一端を紹介する。東芝グループは，社会インフラを含むシステム構築，ITをは

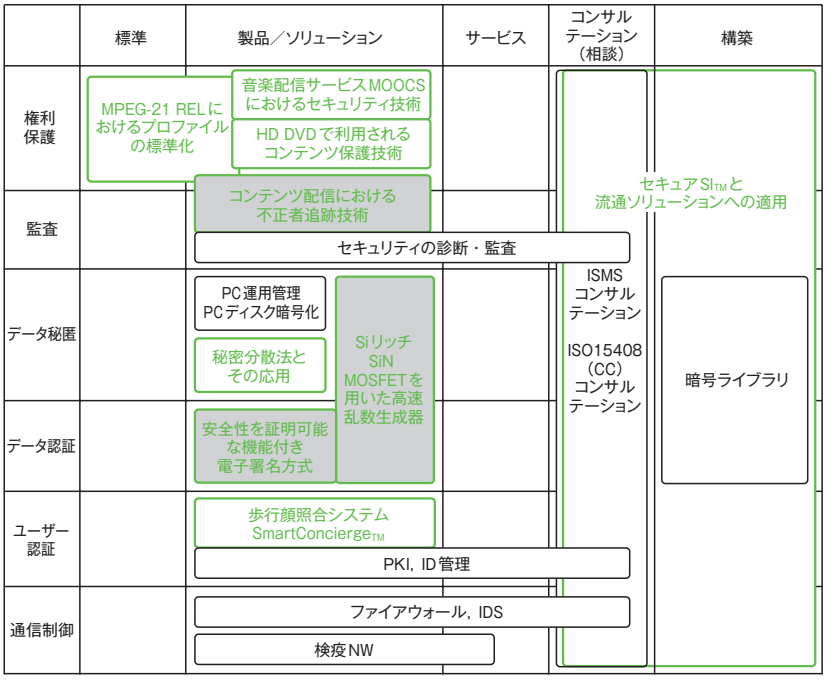


図2．掲載論文と東芝グループ情報セキュリティ商品の関連 ― 技術分類を縦軸，適用分類を横軸として，それぞれの位置を表現した。
Information security technologies appearing in papers in this volume and relevant Toshiba products

（注1） ISO/IEC 15408（国際標準化機構／国際電気標準会議規格15408）
IT製品（ハードウェア・ソフトウェア）及び情報システムの開発や製造，運用などに関する国際標準規格であり，情報セキュリティの国際評価基準として1999年6月に承認された。この評価基準の原案であるCCとも呼ばれ，同義で扱われている。

（注2） FIPS140-2（連邦情報処理規格140-2）
米国商務省の管轄する研究所（NIST）が暗号モジュールのセキュリティ要件を規定した。

じめとする製品製造，コンテンツ販売などの事業を行なっている。情報セキュリティの研究開発も，これらの事業に活用することを目的としている。また，次世代の情報セキュリティ技術への適用を目的とした基盤技術の開発も並行して進めている。掲載論文と東芝グループにおける情報セキュリティ商品の関連の一部を**図2**に示す。

■システム構築のための研究開発

システム構築における情報セキュリティの課題は，まさに“情報セキュリティ技術をいかに確実に作り込むか”の章で述べたことであり，情報セキュリティ技術者の増強が急務である。このため，システム開発における一般的課題と同様に，開発者のスキル（見識や熟練度）にできるだけ依存しない開発の仕組みの確立が要求されている。解決策として，開発方法論とソフトウェア部品が注目されている。東芝ソリューション（株）は，情報セキュリティ技術も含めて，こうした取組みを強化している。この特集では，情報セキュリティを対象にした開発方法論であるセキュアSI$_{TM}$を取り上げた（“セキュアSI$_{TM}$と流通ソリューションへの適用”（p.7－10））。

開発方法論を持つシステム構築ベンダーが増加している。しかし，情報セキュリティ技術も含めた開発方法論はまだ少ない。セキュアSI$_{TM}$は，ISO/IEC 15408のコンサルテーション及び開発への適用を繰り返して蓄積したノウハウを結集して得られた，手順レベルまで具体化した方法論である。この特集で取り上げた流通ソリューション以外にも様々な業種への適用実績があり，顧客からも高い評価を得ている。

■コンテンツ保護のための研究開発

コンテンツ保護技術は，著作権保護のニーズに応え，著作権保護法に沿ったコンテンツ利用を可能にすることを目的に成立した技術である。記録メディア上での保護や入出力信号における保護を中心に，様々な規格が作られている（**囲み記事参照**）。

“HD DVDで利用されるコンテンツ保護技術”（p.11－14）では，HD DVDで採用されているコンテンツ保護技術AACS（Advanced Access Content System）の概要を述べている。高画質コンテンツやインタラクティブ コンテンツを扱えるHD DVDでは，これまでのDVDで採用されているコンテンツ保護技術に比べ，強度の高い暗号アルゴリズムが利用されているほかに，不正機器や不正コンテンツの無効化に関する機能が強化されたことが一つの特長である。コンテンツの不正流出の元となった機器を特定する技術も採用されている。更に，パッケージメディア上のコンテンツをパソコン（PC）のハードディスク装置（HDD）などにコピーできるようにする，マネージド コピー機能をはじめとしたネットワーク連携機能への拡張も検討され，ユーザーの利便性向上にも配慮した仕様となっている。

コンテンツ配布の形態は，特定の媒体（CDやDVD）に保存されたものからネットワークダウンロードに広がってきた。コンテンツの購入とは，コンテンツを保存した媒体を購入することであろうか，それともコンテンツを再生する権利を購入することであろうか。CDやDVDに保存され販売されているコンテンツは前者であろうが，後者の考えに立ったほうが利用者の利便性は増加する。“音楽配信サービスMOOCS(注3)におけるセキュリティ技術 MQbic$_{TM}$”（p.15－18）は，コンテンツとは独立した“再生する権利”をSDメモリカードに格納された再生のための鍵として提供することによって，ダウンロード先の機器だけに限定されることのない音楽再生を可能にした。

コンテンツ保護の発展は，コンテンツの配布形態の変化のほかに，より柔軟な著作権管理技術の実現にも向けられている。この特集では，そのような流れの一つとして，コンテンツ利用許諾情報の記述言語（REL：Rights Expression Language）の規格を，“MPEG-21 RELにおけるプロファイルの標準化”（p.19－22）で述べている。MPEG-21 RELは汎用性を意識して設計されているが，逆に，特定の応用を意識した言語拡張や最低限のスキーマ定義を行うプロファイル規格の開発も行われている。携帯端末やDVDなど光ディスク機器への応用を志向したMAM（Mobile And optical Media）プロファイルの規格化には東芝も積極的に貢献している。このプロファイルのHD DVDへの応用により，これまでになく様々なコンテンツ利用シナリオが実現できるものと期待される。

■基盤技術の研究開発

この特集では，情報セキュリティの基盤技術として秘密分散技術，ユーザー認証技術，及び暗号技術を取り上げ，研究成果や適用製品を述べている。

秘密分散は，秘密情報を分散管理する手法であり，個人情報保護法などの法制度に基づいた組織による情報管理のニーズに応える技術である。秘密にしたい情報をn個（例えば3個）の情報に分散し，n個のうちのk個（例えば2個）が集まれば元の情報を復元できる技術である。ある企業が顧客に情報を持参する際に，訪問する3人が上記の分散情報を持って移動し，客先で少なくとも2人の情報があれば元の情報を復元できる。しかも，ひとりの分散情報を紛失したとしても，まったく秘密は漏れない。“秘密分散法とその応用”（p.23－26）で示した方式は，高速処理ができるという特長がある。

ユーザー認証においては，生体認証が注目されてきている。記憶（パスワード）や所持品（トークン）よりも生体情報のほうが，本人性の確認においては強い根拠と考えることができるし，利用者の利便性の要求に応えることができるか

(注3)　MOOCSは，ニフティ（株）の登録商標。

コンテンツ保護技術の広がり

これまでの地上アナログ放送は，特別なスクランブルが掛けられておらず，コピー制御情報（CCI：Copy Control Information）も挿入されていない。そのため，VHS（Video Home System）ビデオレコーダやHDD&DVDレコーダを使って録画したコンテンツを何度でもコピーすることができる。著作権法で許可された範囲での用途を超えて，例えばインターネット上で配布されるという問題も指摘されている。

このようなコンテンツの違法利用を技術的に回避するための手段として，わが国のデジタル放送ではスクランブルが掛けられるとともに，2007年5月時点では主に1世代コピー可のCCIが挿入されている。これによって，録画したコンテンツからコピーを作成することができなくなっている。

同様に，DVD-Videoコンテンツのスクランブルに採用されているCSS（Content Scramble System），DVDレコーダでコンテンツの暗号化に採用されているCPRM（Content Protection for Recordable Media），及びHD DVDでコンテンツの暗号化に採用されているAACSなど，デジタルコンテンツの違法利用を防ぐために様々なコンテンツ保護技術が実際に利用されている。

更に，コンテンツの保護は，メディア上に記録された状態での保護だけでなく，コンテンツ視聴時のプレーヤ出力にも必要不可欠な機能である。出力は，デジタル信号だけでなくアナログ信号もある。

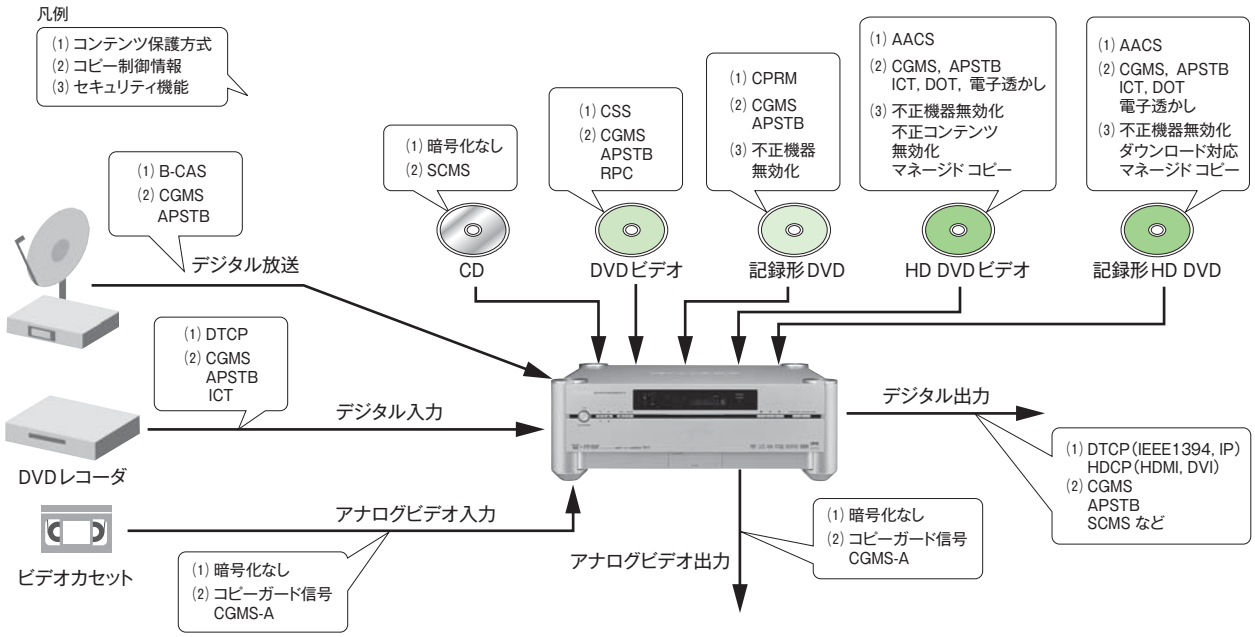
デジタル信号には，主に圧縮データの入出力用途に用いられるIEEE1394（米国電気電子技術者協会規格1394）やIP（Internet Protocol）用のDTCP（Digital Transmission Content Protection），ベースバンド信号の入出力用途に用いられるDVI（Digital Visual Interface）/HDMI（High-Definition Multimedia Interface）用のHDCP（High-bandwidth Digital Content Protection）が，利用されている。

アナログ信号には，CCI情報を伝送するためのCGMS-A（Copy Generation Management System-Analog）や，アナログコピーを防止するためのアナログコピーガード信号などが利用されている。

例えば，DVDビデオをビデオプレーヤで再生してテレビで視聴する場合には，DVDビデオに掛けられているCSSを外した後，HDCPで保護を掛けたうえでHDMI出力を経由してテレビに伝送される。

このように，コンテンツを記録・再生する場合には，もともと施されているコンテンツ保護技術だけでコンテンツを守ることができるわけではなく，コンテンツの保護は連鎖的に継承されていなければならないため，コンテンツを扱う機器は遵守規定（Compliance Rules）で定められた入出力ルールに従わなければならない。

商用コンテンツを扱う場合には，コンテンツ保護は必要不可欠の技術となっており，1台の機器に多くのコンテンツ保護技術を実装しなければならなくなってきている。



B-CAS ：BS Conditional Access Systems
APSTB：Analog Protection System Trigger Bit
SCMS ：Serial Copy Management System
RPC ：Region Playback Control
ICT ：Image Constraint Token
DOT ：Digital Only Token

様々なコンテンツ保護技術 — 用途に応じて様々なコンテンツ保護技術が適用されている。

らである。“歩行顔照合システムSmart Conciergeᵀᴹ”（p.27－30）は，生体認証を物理セキュリティに適用し，利用者の利便性を更に追及した製品である。従来認証時に立ち止まる必要があったシステムを改良し，歩行したままでの顔照合を可能にした。従来の顔照合製品が通行量が多くない場所で利用されていたのに対し，通行量が多い場所でも利用可能になった。適用分野の拡大が期待される。

暗号技術は，情報セキュリティの基盤技術の一つとして位置づけられ，既に実際の様々なシステムで利用されている。暗号の機能としては情報を盗聴から防ぐ秘匿機能，使用する機器の正当性の確認，情報の改ざんの検出，情報作成者の確認のための認証機能があるが，共通鍵暗号，公開鍵暗号，署名，及びハッシュ関数の各要素技術を適材適所で組み合わせることで，対象システムで必要とされる基本的なセキュリティ機能が設計できる場合が少なくない。暗号技術の研究動向としては，2000年ごろに日米欧の各国や地域で行われた次世代暗号アルゴリズムの標準化が一段落し，暗号の要素技術を組み合わせたより複雑な暗号プロトコルの研究や，暗号方式と暗号プロトコルの安全性に関する研究が盛んになっている。特に公開鍵暗号系の暗号方式や暗号プロトコルでは，“証明可能安全性”が重要かつ標準的な要件となってきた。証明可能安全性とは，背理法によって暗号方式が破れないことを示す技法である。すなわち，暗号方式を破る手法の存在を仮定すると，安全性の前提としている問題の解法が構成できてしまうことを証明し，矛盾を導く技法である。

“コンテンツ配信における不正者追跡技術”（p.31－34）は，コンテンツ配信における暗号プロトコルの一種である。放送型有料コンテンツ配信におけるセッション鍵配送のためのヘッダサイズの削減と，端末内の復号鍵が不正に横流しされた場合の不正者特定を要件として，プロトコルが構成されている。押収した海賊版端末が，その内部解析が困難であったり，入力される情報から不正者特定の意向を検知して妨げるなど，より強力な攻撃機能を備えていても不正者特定を可能とし，更にヘッダサイズを削減した方式を考案した。

“安全性を証明可能な機能付き電子署名方式”（p.35－38）では，電子署名方式の一種である多重署名方式の証明可能安全性を検討した。多重署名は，複数の署名者による効率的な承認を実現する技術であり，稟議（りんぎ）書などに応用できる。通常の電子署名に比べ，プロトコルに登場する参加者が多く，攻撃も多岐にわたるため，安全性を議論するうえでどのようなモデルを考えるかが重要である。この論文では，署名者の登録フェーズまで考慮してモデル化した。具体的な多重署名方式として，RSA署名(注4)を応用した方式で，署名者ひとり当たりの署名長の増加を最小限に抑えた方式を考案した。

暗号の安全性を実現するうえで重要な要素部品に乱数生成回路がある。先に述べた証明可能安全性は，暗号で利用される鍵がランダムに生成されていることはもちろん，暗号方式のなかで利用されるランダムなパラメータは，すべて理想的な乱数生成回路により生成されることを前提として成り立っている。東芝は，理想的な乱数生成器をLSIに搭載可能な小型回路で実現する技術の開発に数年前から取り組んでおり，既にICカードに搭載可能なレベルで実現した回路もある。この特集では，新たな乱数生成源としてSiN（シリコン窒化膜）MOSFET（金属酸化物半導体型電界効果トランジスタ）を利用して開発した小型乱数生成回路と，生成される乱数の評価結果を示している（“SiリッチSiN MOSFETを用いた高速乱数生成器”（p.39－42））。両立が難しい乱数の質と回路の小型化の両方を改良する回路構成として期待される。

これからの取組み

これからも発展を続ける情報セキュリティ技術を，東芝グループはそれぞれの事業分野で確実に適用していく。重要性を増すコンテンツ保護技術に今後も注力を続けるとともに，従来は利便性とのトレードオフととらえられてきた情報セキュリティ技術を更に利便性の高いものにしていくことによって，よりしっかりと社会を支える技術にするための努力を続ける。

（注4） RSA署名
代表的な公開鍵暗号方式の一つで，3名の開発者（R. Rivest，A. Shamir，L. Adelman）の頭文字から命名された。RSAは，RSA Security, Inc.の登録商標。

山田　朝彦
YAMADA Asahiko, D.Sc.
東芝ソリューション（株）IT技術研究所 研究開発部主査，理博。運用を中心とした，システムセキュリティの研究・開発に従事。情報処理学会会員。
Toshiba Solutions Corp.

新保　　淳
SHIMBO Atsushi
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。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer & Network Systems Lab.

北折　昌司
KITAORI Shoji
東芝ソリューション（株）プラットフォームソリューション事業部 プラットフォームソリューション第三部参事。セキュリティソリューション事業に従事。
Toshiba Solutions Corp.