人と組織の社会貢献を支えるセキュリティ技術

Information Security Technologies Enhancing Social Contributions of Individuals and Organizations

遠藤　直樹　■ ENDO Naoki
川村　信一　■ KAWAMURA Shinichi
大熊　建司　■ OHKUMA Kenji

情報システムの担う役割とそのセキュリティの確保の重要性はますます高まっている。社会における人や組織のあらゆる活動が情報システムなしには考えられなくなっている。

東芝は，1980年初頭から情報セキュリティ技術の重要性に着目して研究開発を進めてきた。その応用分野は，社会インフラや，企業情報システム，半導体製品など多種多様である。それらを支える先進コア技術の暗号や電子透かしなどを開発しこれらを活用したソリューションを提供し続けていくことで，人と組織の社会貢献を支えていく。

With all activities of both individuals and organizations having become heavily dependent on information systems, safeguarding the security of information systems is now a crucial issue.

Since the early 1980s, Toshiba has been researching and developing information security technologies for application in a broad range of fields including social infrastructure systems, corporate information systems, and semiconductor products. These fields of application are supported by core technologies such as cryptography and digital watermarking. We are making continuous efforts to enhance the social contributions of individuals and organizations by developing these core technologies and solutions.

情報ネットワークにおける脅威の動向

情報ネットワークが，われわれの仕事や生活に活用されるようになってから長い年月が経過した。その間，情報やそのほかの資産に対する脅威とリスクが顕在化するとともに，その対策の必要性が認識され，幾多のセキュリティソリューションが実現され，活用されてきた。しかし，情報ネットワークにおける資産の保護は，新しい脅威の出現や人間の行動特性に関連するミスなどが原因となって，常に大きな課題として存在しているのも事実である。

個人情報と技術情報の漏えいや盗難の問題は，従来から広く認知されている。これらは正当な企業や組織などの活動を停滞させる原因となるものである。一方，多くの人や組織に広範な影響を与える社会インフラにおける脅威も見逃してはならない。

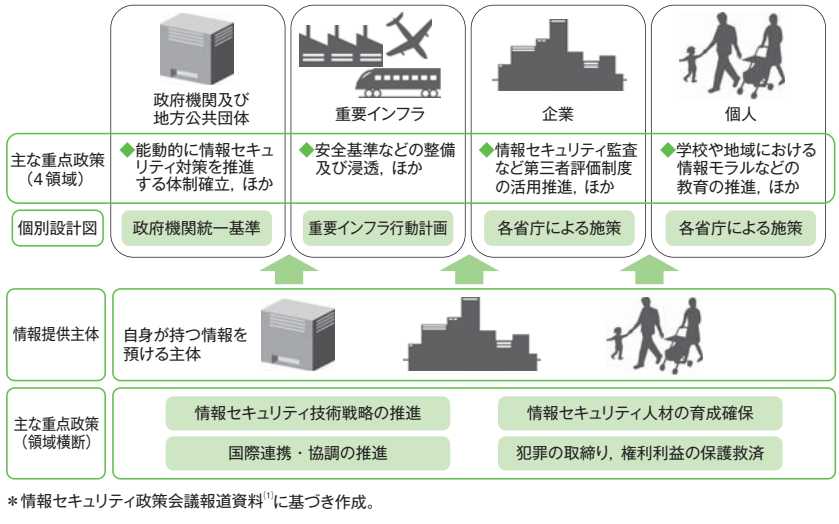
世界におけるでき事を見ると，例えば，発電や電力供給のシステムが侵害を受け，通信や電力供給など重要なインフラを妨害できるツールが植えつけられていたことが報告されている。また，水処理プラントに対する元社員からのアタック事例では，処理前の汚水の制御システムが攻撃を受けてバルブの制御を乗っ取られ，汚水が公園や川に流出してしまったという報告もある。これらの事例を見て言えることは，一部の心ない攻撃者の狙いが，人や組織の社会貢献能力を低下させることにある，ということである。これは正当な企業や組織活動を営む人々の基本的な希望を打ち砕くものであり，あらゆる道具立てを駆使して阻止していく必要がある。

わが国や諸外国におけるセキュリティ対策の考え方

わが国や米国をはじめ各国は，情報ネットワークの危機管理の面から様々な政策を打ってきた。わが国では，1990年代から技術的対策の推進や早期警戒体制の整備などが進められ，情報セキュリティソリューションの基盤技術である暗号技術の評価及び強化や，ソリューションの評価，認証制度の創設が行われている。また，コンピュータウィルスや不正アクセスに関する届出制度も1990年代に創設された。最近では，2006年から2008年にわたる第1次情報セキュリティ基本計画，そして2009年からの第2次情報セキュリティ基本計画が策定され，実行されている。

第2次情報セキュリティ基本計画は，政府機関統一基準，重要インフラ行動計画，企業や個人に対する各省庁による施策が柱となり，官公庁自治体，産業界，個人のレベルまでの一貫した取組みが定義されている（**図1**）。このうち重要インフラ行動計画では，対象となる重要インフラ（情報通信，金融，航空，鉄道，電力，ガス，政府・行政サービス，医療，水道，及び物流）サービスと重要システムやその検証レベルなどに関し，詳細な指針が示されており，東芝としてもこの計画に沿った行動を進めていく。

一方，米国では，2009年1月に国土安全保障アジェンダ（行動計画）においてネットワークセキュリティの課題を公表している。技術面では，安全なコン



＊情報セキュリティ政策会議報道資料[1]に基づき作成。

図1.「第2次情報セキュリティ基本計画」に基づく取組み — わが国政府による2009年から3年間の重点施策である。

Approach based on Second National Strategy on Information Security

ピュータの研究開発への取組みの始動及び米サイバーインフラの強化，米国経済の安全が維持できるIT（情報技術）インフラの保護，犯罪者の利益獲得機会を最小限にとどめるサイバー犯罪戦略の構築などが含まれている。

セキュリティ関連学会や組織の活動

政府の施策に連携して関連する学会や組織も活発な活動を進めており，当社もその重要な一員として行動している。学会では，電子情報通信学会，情報処理学会などにより，暗号と情報セキュリティシンポジウムや，コンピュータセキュリティシンポジウム，セキュリティ心理学とトラストに関するシンポジウムが定期的に開催され，暗号や認証のような基盤技術や，セキュア通信プロトコル技術，システムレベルの設計・構築・評価技術など幅広い技術の向上が図られている。

一方，制御システムセキュリティカンファレンスや重要インフラ情報セキュリティフォーラム，デジタル社会推進シンポジウムなど，制御システムやサイバー攻撃対策などに的を絞った取組みも近年活発化している。更には，電子政府推奨暗号リストの作成や改訂を目的とした評価委員会CRYPTREC（Cryptography Research and Evaluation Committees）もある（**囲み記事参照**）。

重要インフラや企業に求められること

重要インフラや企業の視点から見たとき，その社会貢献能力を保護し発展させることが重要である。その策は，サイバー攻撃や，重大事故，自然災害などに強い体質を持つことである。

一方，従来より複雑化する情報システムやオープン技術の利用拡大と，社会全体の最適化による産業間又は企業間の相互依存関係の進展があり，問題を複雑化させている。この複雑化する問題へのアプローチは，総合的，合理的，かつ定量的な対策を実施していくことであり，まさに，第2次情報セキュリティ基本計画の基本理念どおりである。情報システムの現状を把握すること，情報システムを適切に管理すること，そして事業継続を担保する情報システムに成長させていくことが重要となる。

セキュリティに対する東芝の取組み

当社は主に1990年代から，多くの事業領域におけるセキュリティ技術の開発と実用化を進めてきた。

官公庁自治体や企業の情報システムに対しては，総合的なセキュリティインフラ構築のほか，認証基盤や政府向け電子コマース，ICカードシステム，情報セキュリティマネジメントシステム（ISMS）の構築，製品のセキュリティ認証取得などがある。交通分野では自動料金収受システム（ETC），入退室管理ではICカードや生体認証システム，電力では運転情報セキュリティや，イントラネットシステム，プラント丸ごとの総合セキュリティインフラ構築などに実績がある。医療では電子カルテセキュリティや総合的な病院情報システム構築，医用画像情報セキュリティなどがある。デジタルメディアでは，デジタル放送セキュリティ，及びDVD製品群やSDメモリカードのコンテンツ保護などがあり，規格化の主導も実施した。

これらの取組みは最終的に半導体製品で製品化されることが多く，ICカードやデジタルテレビ（TV）用LSIほか，多くの開発実績がある。

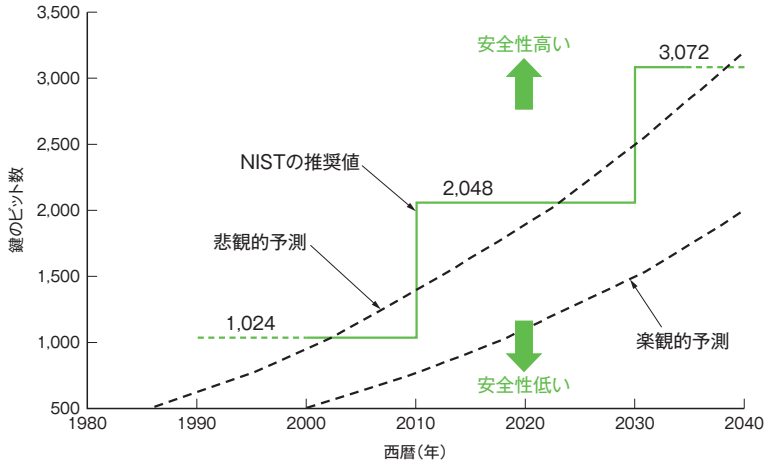
当社は，情報セキュリティのための基盤技術である暗号・認証技術，及びそのハードウェア又はソフトウェアによる実装技術を基本とし，これを用いて実現される用途向けセキュリティプロトコルと応用システムの技術を培ってきている。不正を許さずミスを誘起させにくいシステム技術，システムに安定性や柔軟性，信頼性を付与するアプリケーション依存又は非依存のコンポーネント技術，更には，コンポーネント技術の強度を担保する暗号・認証技術という階層構造で，バランスの良い技術開発とその製品化を進めている。

求められる先進的なコア技術の開発

情報セキュリティ対策は様々な分類方法が考えられるが，一つの方法として，(1)管理運用，(2)システム技術，(3)コア技術，の三つに分けることができる。

暗号の危殆化と2010年問題

暗号技術の安全性は一定ではなく，攻撃方法や計算機の進歩とともに低下する。暗号の安全性が低下し，攻撃が現実的脅威となることを“危殆（きたい）化”と言う。実際，2-key Triple DES（Data Encryption Standard）や1024ビット鍵のRSA（Rivest−Shamir−Adleman）暗号などの暗号方式と，ハッシュ関数のSHA（Secure Hash Algorithm）-1は近いうちに危殆化する可能性があり，米国政府機関NIST（National Institute of Standards and Technology）は，2010年以降にこれらの暗号技術を米国標準から外すことを表明した。ベンダーなどは，この“暗号の2010年問題”への対応に追われている。



＊CRYPTREC Report 2006−暗号技術監視委員会報告[2]に基づき作成。

RSA暗号の安全な鍵サイズの推移予測 — 上下の破線は素因数分解の世界記録から外挿した上限と下限であり，緑の折れ線はNISTが推奨する鍵のサイズである。

図は，RSA暗号における安全な鍵サイズの推移予測である。横軸が西暦，縦軸が鍵のビット数である。グラフは多くの仮定の下に描かれており，解釈に注意を要するが，RSAの鍵サイズに関するNISTの推奨期限がおおむね妥当であることを示している。

ハッシュ関数では，SHA-1をより安全性が高いSHA-2ファミリー（SHA-256など5方式）に置き換えることが推奨されているが，SHA-1と類似の構造を持ち，同様の弱点を持つおそれがある。そこで，NISTはSHA-2に続く標準ハッシュ関数SHA-3の公募プロジェクトを2006年に開始し，2012年内に標準方式を決定する計画である。

このように暗号技術は，常時監視し，危殆化が予想されれば，より安全なものに置き換えていく必要がある。わが国では，2003年に発表された電子政府向けの推奨暗号リストを改訂する作業が開始されており，2013年度までに改訂版が発表される予定である。

危殆化は，数学的問題の難しさに安全性の根拠を置く暗号では重大な問題となる。そこで，無限の計算能力があっても破ることのできない，情報理論的に安全な暗号方式の研究も行われている。情報理論的に安全な暗号方式は，大量の乱数ビットを必要とするが，長期の安全性が要求される社会インフラなどでは，そのコストに見合う効果が期待できる。

また，最近注目されている量子暗号では，光子や電子などの量子物理学的性質を利用して，無限の計算能力でも破れない無条件に安全な暗号を実現しようとしている。わが国での研究も活発であるが，欧州のETSI（European Telecommunications Standards Institute）は量子暗号の標準化検討に着手した。

いずれも欠くことのできない重要な側面であるが，この特集は，これら三つの側面のうちコア技術に焦点を当てている。

東芝レビューでは1999年7月号以来，2年に1度情報セキュリティ特集を組んできた。近年の特集ではシステム技術に焦点を当ててきたが，今回の特集では再びコア技術に焦点を当てることにした。

以下，コア技術について，この特集で取り上げられている暗号技術，電子透かし技術，実装技術，及び応用技術の順で，研究開発の背景を述べる。

■次世代の暗号方式

暗号技術は情報セキュリティ対策の基本技術の一つである。そのため，当社は早くから暗号技術とその応用の研究開発に取り組んできた。

現在広く利用されている暗号の安全性は計算量的な安全性に根拠を置いている。ある暗号が計算量的に安全であるとは，現在知られているどのような解読方法を用いても，現在利用できる計算機の能力では，解読に膨大な時間が掛かってしまうということである。したがって，計算量的な安全性に根拠を置く暗号方式は，何も対策を施さなければ，計算機の能力向上とともに暗号の強度が低下していくという運命を背負っている。

● **高速量子暗号**（p.7－11）

量子暗号は，従来の暗号の多くが計算量的な安全性に根拠を置いているのに対して，物理学，特に量子力学の根本原理の一つを安全性の根拠とする暗号方式である。したがって，将来極めて高速な計算機が出現しても方式の安全性が揺らぐことがないという意味で，次世代を担う暗号と言える。

量子暗号を今後広く普及させるためにはいくつかの課題がある。その中でも重要なのが，鍵の配送速度の向上と通信距離を伸ばすことである。当社は2008年10月までに，他社に先駆けて，通信距離20 kmで1 Mビット/sの速度を達

成できる量子暗号技術を開発した。

今後は，当社の強みであるデバイス技術を生かし，方式の標準化や更に大きな課題である量子中継の実現にも貢献していきたい。

● **高速匿名認証**（p.12－15）

高速匿名認証は，自分の名前を相手に知らせることなしに，認められたサービスを受ける権利を持つことを相手に示す方式である。

暗号技術を駆使することによって，プライバシーと利便性を両立させる方式を実現することができる。当社が開発した匿名認証技術は計算量が極めて少なくてよく，処理の高速性に特長がある。

実際にICカードや携帯電話といった比較的計算能力の限られた装置上でも，1秒未満の時間で処理が完了することを確認しており，十分な実用性がある。それ以前の方式ではこの速度は達成できなかった。

プライバシーと安全性を両立する方式として様々な応用が見込まれる。

● **代数的トーラス暗号**（p.16－19）

代数的トーラス暗号として，よりコンパクトで少ない計算量で処理できる公開鍵暗号方式の構成法を提案している。公開鍵暗号方式は，インターネットなどで不特定多数の人が暗号を利用する場合に，鍵の管理が容易な暗号方式である。デジタル署名と呼ぶ電子データに対する印鑑機能を実現するのにも適している。

従来の公開鍵暗号の欠点は，鍵が長いことと計算量が大きいことであった。これを解決できる方式として期待される次世代公開鍵暗号の代表的方式は，だ円曲線暗号である。当社が提案している代数的トーラス暗号は，このだ円曲線暗号に肉薄する性能を持っている。今後，更に改良を加えることで，次世代の公開鍵暗号として普及させたい。

● **安全性の自動証明**（p.20－23）

安全性の自動証明とは，暗号や暗号を利用したプロトコル（通信手順）の安全性を，計算機で証明する技術である。

暗号の分野では方式の安全性を証明によって示すことが多い。ある暗号が安全であることを証明するには，その暗号を解読することが，歴史的に解くのが難しい数学的問題と同じくらいに難しいことを証明する。

従来，このような証明は専門家が人手によって与えるのが通例であった。しかし，人手による証明では証明者に専門知識が必要であるうえに，何十行，何百行にもわたる証明の場合には，途中の誤りが見過ごされることも少なくない。

学術的にも注目を集めている自動証明技術を研究し，製品やシステムの開発に適用することを目指している。

■電子透かし技術と応用

暗号技術を情報セキュリティの基本を支える技術と述べたが，映像や音楽などのコンテンツ保護を考えると，暗号以外の技術も必要となる。暗号は伝送路上での盗聴やコピーを防ぐのに有効であるが，映像や音楽などを利用する段階では復号される。ひとたび復号されてしまえば，その効力を発揮できない。そのような状況で活躍するのが，電子透かし技術である。

電子透かしとは，例えば動画の中に人が知覚できない程度のわずかな変更を加えることによって埋め込む付加情報である。電子透かしは，通常コンテンツの不正コピーの防止を目的として利用されるが，その利用方法は更にコピー制御と電子指紋の二つに大別される。

● **結託耐性符号**（p.24－27）

結託耐性符号は，電子指紋を実現するのに不可欠な符号化方式である。電子指紋方式は，動画などのコンテンツをユーザーに配布する際に，ユーザーごとに異なる符号を生成し，電子透かし技術を用いてこれを埋め込む技術である。不正に流通したと思われるコンテンツが発見された際に，そこに埋め込まれている符号から，コンテンツを横流しした不正なユーザーを特定することが可能になる。

このような状況において，複数の不正なユーザーが結託して，埋め込まれた符号から不正なユーザーが特定できないようにしようとすることを結託攻撃と呼ぶ。結託攻撃に対しても電子指紋が有効に働くようにするには，結託攻撃を想定しない場合に比べて，埋め込む符号を長くする必要がある。結託攻撃を防止しつつ，どこまで符号長を短く抑えることができるかが課題となる。

当社は，動画への埋込みを想定した場合，はじめて実用可能なレベルの符号長を達成することに成功した。

■実装の視点からのセキュリティ

暗号や結託耐性符号それ自体は，アルゴリズム（処理手順）として定義され，アルゴリズムとしての安全性も厳密に定義される。

一方で，これらのアルゴリズムが実際に利用されるためには，ソフトウェアやハードウェアでこれを実現する必要がある。このような作業を実装と呼ぶ。

アルゴリズムとして安全に設計された暗号や符号でも，それが実装されると安全でなくなることがしばしばある。

与えられた暗号アルゴリズムが安全である，という場合いくつかの前提条件があり，それらが満たされているときに安全性が保証される。

例えば，暗号の安全性には，“鍵が秘密に保たれていること”という前提条件がある。暗号化を行うパッケージソフトウェアがあって，そのソフトウェアでは秘密の鍵をハードディスク上に保存しているものとする。ハードディスク上の鍵をなんらかの手段によって特定できた攻撃者にとって，もはやこの暗号化ソフトは効果を発揮しない。

これは一つの例であるが，アルゴリズム自身が安全であるだけでは不十分であり，それを実装する段階では，アルゴリズムが前提としている条件を満たすように十分な注意を払わなければならない。

● **暗号モジュールの実装攻撃対策**（p.28－31）

LSIに暗号機能を実装する際の中心的な課題は，暗号化の処理がLSIで実

行されるときに，処理時間の変動や消費電力の変動から秘密の鍵が漏えいしないことである。現象的にはささいな事がらのように思えるかもしれないが，電子マネーや身分証などとして広く使われているICカードや無線タグなどでは，そのセキュリティを揺るがしかねない大きな課題となっている。

当社は，対策技術及び評価技術に注目し，安全な暗号モジュールを開発している。また，第三者による評価を受け認証も得ている。

- **トラステッドコンピューティング**（p.32－35）

トラステッドコンピューティングも実装にかかわるセキュリティを扱っているが，当社が参加しているTCG（Trusted Computing Group）という標準化組織で規格が策定されているTPM（Trusted Platform Module）の活用を図っている。

TPMは，暗号化などの機能を持ったモジュールで，データの保護やシステム状態の検証に利用できる。TPMが搭載されているパソコン（PC）も多く，例えば，ソフトウェアだけでは解決できなかった鍵の保護の問題を解決することができる。

新たに開発したソフトウェアを安全に実行する環境構築にも適用が図られている。今後は，TPMの機能や考え方をPCだけでなく，組込みシステムや情報家電などのセキュリティ実装にも展開していく。

■応用の視点からの課題

ここまでは，モジュールレベルの実装まで見てきたが，これよりも上位のシステム層の課題も多数ある。基本ソフトウェア（OS）や通信プロトコルについても非常に多くの課題が残されている。また，セキュリティ技術が多くのシステムに横断的に関係することから，個別の応用システムについてはこの特集では割愛した。

ここでは，汎用のコア技術として重要な本人確認技術と，建物やエリア内での人の所在を管理する技術について述べる。

- **生体認証**（p.36－39）

本人を本人と確認することは情報セキュリティ技術の基本である。本人確認手段には，パスワードのような記憶によるもの，ICカードや無線タグのような所有物によるもの，又は指紋や虹彩（こうさい）など生体情報によるものがある。

これらの認証手段は既に様々な形で実用化されている。生体認証は，生体情報を読み取るセンサとサービスを提供するサイトとが離れている場合，正しい認証をどのように保証するか，また，生体情報という個人と直結する情報をどう保護するか，といった点に多くの問題を抱えている。

当社は，このような状況において，センサで取り込まれた生体情報を遠隔のサイトで認証するための，認証コンテキストACBioを開発し，国際標準化機構（ISO）での標準化を進めている。

従来技術では，離れた場所での認証の安全性は必ずしも十分とは言えなかった。ACBioを用いることによって，ネットを介した様々なサービスで生体認証を利用できることになる。

- **統合エリアセキュリティソリューション**（p.40－43）

統合エリアセキュリティソリューションは，施設内の人の動きを管理するもので，個々の人物はICカードか無線タグにより識別する。これは所有物による本人確認である。更にセキュリティレベルの高い場合には，生体情報による認証も設定できる。

統合管理されるセキュリティエリアに対して，人の区分ごとにアクセス権のレベルを設定できる。

無線タグを用いた場合には，ユーザーが意識的に操作をしなくても居場所の管理ができる。

今後の展望

今回の特集では，当社が開発している情報セキュリティのコア技術を中心に取り上げた。

ITが社会システムの様々な階層や側面に入り込んでいる現在，情報セキュリティの実現は，人類及び社会の健全な発展のために不可欠である。

当社は，それを支える先進のコア技術の開発とそれらを活用したソリューションの提供を続けていくことで，人と組織の社会貢献を支えていく。

文　献

(1) 内閣官房セキュリティセンター（NISC）．2009年5月8日付報道発表資料 “情報セキュリティ政策会議第21回会合の開催について”．<http://www.nisc.go.jp/conference/seisaku/dai21/pdf/21seisakupress.pdf>，（参照 2009-06-11）

(2) CRYPTREC Report 2006－暗号技術監視委員会報告（2007-03）．<http://www.cryptrec.go.jp/report.html>，（参照 2009-06-11）．

遠藤　直樹
ENDO Naoki
東芝ソリューション（株）技術統括部技監。情報セキュリティ技術ほか新規技術を用いた事業開発に従事。電子情報通信学会，情報処理学会，日本セキュリティマネジメント学会会員。
Toshiba Solutions Corp.

川村　信一
KAWAMURA Shinichi, 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研究主幹，工博。暗号及び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.

大熊　建司
OHKUMA Kenji, D.Sc.
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，理博。暗号及び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，IACR，日本物理学会会員。
Computer & Network Systems Lab.