TREND

社会生活に貢献する東芝のセキュリティ技術

Toshiba Security Technologies and Their Contribution to Society

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

インターネットなどのオープンな通信環境が日常的に利用可能になったことで，オンラインショッピング，官公庁での手続きの電子化など，私たちの社会生活の一部はリアルな世界からバーチャルな世界にシフトしている。それに伴い，バーチャルな世界で価値の源泉となる情報の安全性を確保するためのセキュリティ技術も生活に浸透してきた。
より豊かなバーチャルライフ実現のために，東芝はより確実なセキュリティ技術の研究，開発，適用を行っている。

As an open communication environment exemplified by the Internet has become commonplace in daily life, certain aspects of people's lives are shifting from the real world to the virtual world as seen in online shopping and in online registration services provided by public offices. Security technology has therefore become necessary to protect the personal information that has value in the virtual world.
To realize a richer virtual world, Toshiba continues its efforts in research, development, and application of more secure technologies.

私たちの生活とセキュリティ技術

セキュリティ技術は私たちの日常生活に浸透してきているが，セキュリティ技術とのかかわり方は，家庭で過ごすとき，オフィスで仕事をするとき，官公庁への届出を行うときなど，生活の側面によって異なる。家庭での生活では，Webにおける SSL（Secure Sockets Layer）など，誰でも使えるセキュリティ技術が導入されている。オフィスでの生活では，組織の意思が反映され，より先進的なセキュリティ技術に接する機会が多い。電子政府を推進する官公庁では，法制度に準拠し証拠性を確保できるセキュリティ技術が適用されている。

私たちが利用するシステムのセキュリティを実現する技術は，いくつかの層を成している。ここでは，システムが利用するセキュリティ技術と，それらセキュリティ技術を支える基盤技術に分けて，技術動向と東芝の取組みについて述べる（**図1**）。

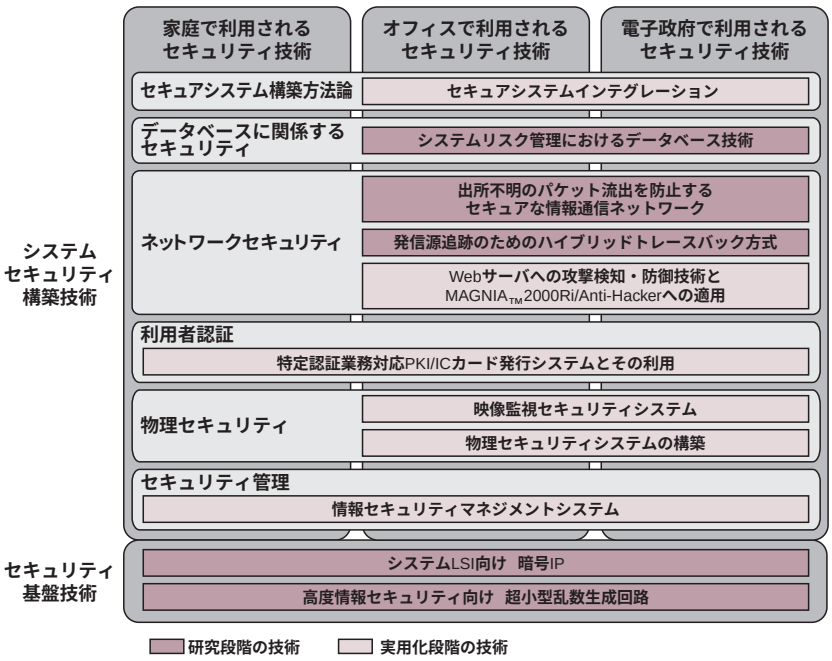

図1．東芝のセキュリティ技術が貢献する社会生活の領域 ― 当社は，家庭，オフィス，電子政府に貢献するシステムセキュリティ構築技術と，それらを支えるセキュリティ基盤技術を研究・開発・適用している。

Toshiba security technologies and their contribution to society

システムに適用されるセキュリティ技術

私たちが日常接する IT（情報技術）システムには，セキュリティ製品が利用され，セキュリティ機能を備えたアプリケーションが実装されている。しかし，セキュリティの実現は，技術だけで達成されるのではなく，組織経営とも密接に関係する。以下では，後述する情

報セキュリティマネジメント規格ISO/IEC17799(ISO：国際標準化機構，IEC：国際電気標準会議)の観点に沿って，セキュリティ技術の動向について述べる(**囲み記事参照**)。

組織のセキュリティポリシー策定

組織経営という観点で情報セキュリティを考えると，組織を情報犯罪から守るためのコストというとらえ方と，インターネットを利用した組織目標実現への投資というとらえ方がある。どちらにしても，組織経営方針に基づいたリスクアセスメントや組織体制なしには考えられない。つまり，情報セキュリティとは，ITだけの問題ではなく，むしろ組織経営の一部であると言える。そこで，組織経営の観点から組織の情報セキュリティを適切に管理することが重要となる。この考え方は国際的にも認められ，組織の情報セキュリティ管理基準としてISO/IEC17799が策定された。国内ではJIS X5080として標準化され，それとともに第三者機関による認定制

情報セキュリティマネジメント規格ISO/IEC17799について

情報システムは組織の業務の一部をITの世界で実現したものであり，組織の業務は組織の方針に基づいて行われる。したがって，情報システムは組織の方針に基づいていることになる。情報セキュリティの観点からも，情報システムは組織の方針に基づいているはずである。しかし，実際は必ずしもそうなっていない。情報システムが業務全体の一部をIT化したものであって，IT化されない部分との間でセキュリティ面での一貫性が取れていないことが，その原因の一つであると考えられる。すなわち，情報システムのセキュリティだけを求めても，組織が持つ情報全体のセキュリティは実現されないのである。

ITのセキュリティと非ITのセキュリティを総合的に考え，トップダウンアプローチで組織のセキュリティを実現するという考えは自然である。その考えに基づく規格が，ISO/IEC17799である。ISO/IEC17799は，英国規格BS7799-1を国際規格としたもので，2000年12月に発行され，2002年2月にはJIS X5080としてJIS化された。

ISO/IEC17799では，情報セキュリティは，組織の情報資産を守るために，次の三つを維持することとして特徴づけられている。

(1) 機密性　アクセスを認可された者だけが情報にアクセスすることを確実にする。

(2) 完全性　情報及び処理方法が，正確であること及び完全であることを保護する。

(3) 可用性　認可された利用者が，必要なときに，情報及び関連する資産にアクセスできることを確実にする。

ISO/IEC17799では，表に示す10の領域を設け，それぞれの領域に対してセキュリティ上の目的と，それぞれの目的を実現するための管理策をリストアップしている。目的の総数は36，管理策の総数は127に及ぶ。ISO/IEC17799に基づいた情報セキュリティ管理とは，リスク分析結果に応じて，127の管理策の中から適切な管理策を選択して，機密性，完全性，可用性を維持することである。ISO/IEC17799による組織のセキュリティ実現の考え方を以下に紹介する。

セキュリティ実現の根幹となるのが“セキュリティ基本方針”である。セキュリティ基本方針には，組織の経営層の関与が求められている。従来，主流であった，情報システム部門を中心に置く考え方とは大きく異なる。セキュリティ基本方針は，経営における経営方針と対比される。セキュリティの基本方針であるセキュリティ基本方針をトップダウンで展開することで，組織全体に整合性のあるセキュリティを実現する。そのためには，方針を展開するための組織体制の整備が必要である(“組織のセキュリティ”)。

情報セキュリティの目的は，情報資産を守ることである。情報資産のうち何を優先して守るのかを決めるには，情報資産を特定し，重要度を決める必要がある。“資産の分類及び管理”は，情報セキュリティの出発点と言える。

組織の情報セキュリティ実現の主体となるのは，やはり組織の構成員である。構成員が組織に属している間，情報セキュリティに対する認識を高め，状況に応じた行動を取って行くことを促さなくてはならない。そのためには，契約，教育，事故への対応方法などが必要である(“人的セキュリティ”)。

ISO/IEC17799の10の領域

1. セキュリティ基本方針
2. 組織のセキュリティ
3. 資産の分類及び管理
4. 人的セキュリティ
5. 物理的及び環境的セキュリティ
6. 通信及び運用管理
7. アクセス制御
8. システムの開発及び保守
9. 事業継続管理
10. 適合性

“物理的及び環境的セキュリティ”，“通信及び運用管理”，“アクセス制御”は，技術も論じられ，製品にも実装されているが，ISO/IEC17799では技術的側面だけではなく，管理的側面も含めて総合的な管理策を提示していることが特徴である。一例を示すと，利用者アクセス権の見直しにおいては，利用者アクセス権を定期的に，また，何らかの変更があった後に，見直すことを管理策として述べている。

“システムの開発及び保守”では，ライフサイクル全体の中では見落とされやすい開発と保守の管理策を挙げている。

“事業継続管理”は可用性について，“適合性”は法的要求や技術標準などへの適合について述べている。

情報システムを運用した経験の中でこそ得られる管理策を，ベストプラクティスという形で，体系的にまとめていることにISO/IEC17799の価値がある。

度，情報セキュリティ管理システム（ISMS：Information Security Management System）が発足するに至っている。

この特集の論文“情報セキュリティマネジメントシステム”（p.7～10）では，ISMSの考え方を活用した組織セキュリティポリシーの策定やISMS取得に向けたコンサルテーションサービス，e-Learningを利用した教育サービスについて述べている。

物理的セキュリティの適用

セキュリティ技術は，組織セキュリティポリシーに基づいて，機密性，完全性，可用性についての要件を定め，トップダウンアプローチで適用され運用される。情報セキュリティの保護対象は，紙及び電子化された情報である。前者の保護は物理的にも行われる必要があるが，後者の保護においても，ITの適用だけでなく物理的な対策が必要である。電子的情報を格納するコンピュータの物理的な破壊や直接アクセスなどの外部犯行を妨げ，情報持出しなどの内部犯行も防止する必要があるからである。

物理的対策の基本は，当該施設への入退管理である。また，犯行があった場合には，犯行の記録が犯行解明の助けになる。これらを総合的に対策するには，ITを利用した，よりシステマティックなアプローチが重要である。

当社は，顔照合技術などによる入退管理を，費用とセキュリティレベルに応じて提供するとともに，記録映像やライブ映像を自由にどこでも見ることを可能にした映像監視システムを提供している（“映像監視セキュリティシステム”（p.19～22），“物理セキュリティシステムの構築”（p.23～26）参照）。

利用者認証と電子的文書の真正性確認

文書が電子化され，現在は書面で行われている商取引が完全に電子化されたとき，契約書などの署名押印は電子署名となる。2001年4月に施行された“認証業務及び電子署名に関する法律”は，電子署名に法的な根拠を与えるとともに，“特定認証業務”という電子証明書発行業務を規定し，その認定制度を発足させた。電子証明書は，当事者同士が相対して取引を行わない電子的な世界においては，相手を信頼するための根拠となるものであり，情報セキュリティの基礎となるものである。それゆえ，上記法律は情報セキュリティの根幹であり，今後，私たちの社会生活の中でも重要性は増してくると考えられる。

電子署名が押印のイメージを持って利用されるとすると，特定認証業務は印鑑（実印）を作るところにあたる。特定認証業務は電子的な印鑑としてICカードを発行し，利用者は印鑑を扱うイメージでICカードを利用すると考えるのが自然であろう。

当社は，PKI（Public Key Infrastructure）/ICカードシステムTARGUSYS™を特定認証業務の認定に対応させたICカード発行システムを開発した。これによって，電子入札，電子契約といった場面で，社印や実印に相当するICカードを発行することができる。こうした技術は，まさにセキュリティを身近にし，インターネットを現実社会に適応させるための基礎となる技術である（“特定認証業務対応PKI/ICカード発行システムとその利用”（p.15～18）参照）。

より高度なネットワークセキュリティを求めて

今日，私たちが利用しているコンピューティング環境は，ネットワークなしに考えられない。ネットワークは，私たちを世界につなげ，多くの情報を提供してくれる。その反面，ネットワークにつながっていることによって，悪意ある第三者からの脅威に私たちはさらされてもいる。

ネットワークセキュリティ対策は，従来は，ファイアウォールや侵入検知システム（IDS：Intrusion Detection System）を用いたものであった。しかし，これだけでは，Webサーバや基本ソフトウェア（OS）の欠陥を突いて行われる侵入，分散型サービス不能攻撃（DDoS：Distributed Denial of Services）などを防ぐことはできない。当社のアプライアンスサーバMAGNIA™ 2000Ri/Anti-Hackerは，Webサーバにやってくるパケットを監視し，Webサーバの欠陥を突いたHTTP（Hyper-Text Transfer Protocol）上の攻撃はもちろん，DDoSに使われる不信なパケットを検知し，これを遮断することでWebサーバを守ることができるIDP（Intrusion Detection and Protection）である。新しい侵入攻撃情報は，インターネットを経由して自動的にアップロードされるため，常に最新の情報に基づく防御が可能になる。Webサーバを簡単確実に防御するのに非常に有用なアプライアンスである（“Webサーバへの攻撃検知・防御技術とMAGNIA™ 2000Ri/Anti-Hackerへの適用”（p.27～30）参照）。

ファイアウォールのフィルタリングルールは，組織のセキュリティポリシーに基づき，通信プロトコルごとの通信可否をファイアウォールのために書き下したものである。矛盾のない記述をするのは難しいなど，運用の観点からも優れているとは言い難い。今日では，より柔軟かつ運用性に優れた通信制御の研究がなされてきている。この特集の論文“出所不明のパケット流通を防止するセキュアな情報通信ネットワーク”（p.31～34）では，セキュリティポリシーを事前に交換し合い，ポリシーに合致した相手との通信だけを可能にするというアプローチを示している。

ネットワーク犯罪が増加する一方であることは，犯罪が行われた場合に犯罪者の特定が難しいことに一因がある。発信源のIP（Internet Protocol）アドレス詐称，不正アクセス後のログの

削除は，ネットワーク犯罪の常とう手段である。これらに対抗する技術として，攻撃者の正確な発信源を特定するためのIPトレースバック技術が注目されている。この特集の論文“発信源追跡のためのハイブリッドトレースバック方式”(p.35～38)では，当社の提案するIPトレースバック方式を紹介している。

データベースのセキュリティ確保

情報の核であるデータベースのセキュリティ確保は，非常に重要である。基本的には，機密性，完全性，可用性の観点から検討し対策すればよいが，機密性については特別な注意が必要である。なぜなら，特殊な条件下においては，公開情報を基に非公開情報が推論できてしまう場合があるからである。例えば，ある集団に属する個人の情報はプライバシー保護の観点から公開できない場合でも，統計情報であれば公開することは問題がないと考えてしまう傾向がある。統計情報を公開する場合でも，個人の情報を推論できないことの検証が必要である(“システムリスク管理におけるデータベース技術”(p.39～42)参照)。

システムをセキュアに構築し保証するために

開発した製品やシステムがセキュアであることを客観的に示すことは難しい。そのための方法論や制度として，古くは米国の軍調達のためのオレンジブックがあったが，近年ではCC(Common Criteria)が欧米の政府調達基準として注目されるようになった。後者は，国際的にはISO/IEC15408として，国内でもJIS X5070として標準化され，国内外の標準となった。

ISO/IEC15408は，セキュリティ機能要件カタログと開発に対する要件から成る，セキュリティ指向の設計・開発基準と言うことができる。また，2001年4月には，政府のセキュリティ評価認証体制も整った。ISO/IEC15408にのっとって構築された製品及びシステムに対しては，評価機関に評価依頼をして一定の評価に合格した場合は，独立行政法人製品評価技術基盤機構(NITE)によって認証書が与えられることになった。官公庁向けのシステムから適用されてきているが，社会インフラを支えるシステムに徐々に適用が進んでいる。

当社は，セキュリティ組込みのためのシステムインテグレーションの方法論を独自に開発し，これを応用してISO/IEC15408への対応を図っている(“セキュアシステムインテグレーション”(p.11～14)参照)。

セキュリティ基盤技術

情報セキュリティの基盤技術としては，暗号技術，電子透かし技術，ネットワークセキュリティ技術が挙げられる。このうち，暗号技術は，実用面での技術開発ばかりでなく，学術面でももっとも体系的に研究が進んでいる。暗号技術における最近の動向として，AES(Advanced Encryption Standard)に代表される次世代アルゴリズムの開発及び安全性理論の研究，暗号の実用化に伴う実装技術と耐タンパ技術の開発，量子暗号や量子コンピュータといった先端技術の開発などが挙げられる。

次世代暗号の設計と安全性理論

共通鍵暗号では，DES(Data Encryption Standard)の強度低下の結果として，米国政府機関において次世代アルゴリズムAES(Advanced Encryption Standard)が2001年に制定された。AESはブロック暗号であり，ブロック長は128ビット，鍵長は128ビット以上の指定された3種類をサポートする。アルゴリズムは公募され，評価と選定が一連のステップを経て実施された。AESの公募と選定は，共通鍵暗号の理論研究に拍車をかけるイベントとなった。

わが国でも，行政サービスの電子化を加速する“e-Japan計画”のもと，申請手続きや調達手続きの電子化，ネットワーク化を実現する電子政府システムに向け，そこで利用する暗号方式の公募が行われた。公募と選定は，情報処理振興事業協会(IPA)と通信・放送機構(TAO)が組織した暗号技術評価委員会CRYPTREC(Cryptography Research & Evaluation Committees)によって，2000年4月から3年間のプロジェクトとして実施された。その成果は，2003年3月に経済産業省と総務省から，電子政府推奨暗号として発表された。

当社は，近年の共通鍵暗号の理論研究を基に，高い安全性が保証可能な設計原理を開発した。これを適用して，Hierocrypt™-3とHierocrypt™-L1の2方式を設計し，CRYPTRECに提案した。Hierocrypt™-3は，AESと同じブロック長と鍵長の方式である。Hierocrypt™-L1は，現行のDESと同じ64ビットのブロック長であるが，鍵長は128ビットの方式である。Hierocrypt™の2方式はいずれも高い評価を獲得し，電子政府推奨暗号の一つとなった。

公開鍵暗号，デジタル署名の分野でも，安全性評価の研究が活発に行われている。安全性の根拠とする問題が破られない限り，対象とする暗号方式や署名方式が攻撃できないことを証明する技法の研究が進んでいる。暗号方式や署名方式で補助関数として利用されるハッシュ関数などのランダム性を仮定したうえで，上記性質を証明する技法が利用される場合が多い。デファクト標準であるRSA(Rivest-Shamir-Adleman)方式を安全性の根拠として，RSA-OAEP(Optimal Asymmetric Encryption Padding)暗号方式，RSA-PSS(Probabilistic Signature Scheme)署名方式が考案されたのが代表例であり，いずれの方式も電子政府推奨暗号となっている。

暗号の実装技術

半導体プロセスの微細化が進み，CPUを内蔵した製品が増えている。また，インターネットや無線LAN，携帯電話などの通信・ネットワーク技術の急速な普及に伴い，暗号技術の利用が従来のコンピュータシステムから様々な民生品へと拡大した。

携帯電話やICカードなどの小型機器にも暗号技術が利用されるが，消費電力や処理能力面から専用の暗号ハードウェアの需要がある。また，情報家電向けにも暗号回路を内蔵したシステムLSIが活用されている。

この特集の論文のうち，“システムLSI向け暗号IP”(p.43～46)と“高度情報セキュリティ向け超小型乱数生成回路”(p.47～51)は，こうした背景で技術開発した成果を述べている。暗号IP(Intellectual Property)の開発では，主要な暗号方式のラインアップをそろえると同時に，いくつかのIPでは小型化や高速化などの面で特長を出している。乱数生成回路では，高品質の物理乱数生成器をシステムLSI上に実現する手法を開発した。一般に，暗号機能の安全性は生成される乱数の予測困難性を前提とするため，こうした乱数生成回路のニーズも高い。

暗号モジュールで利用される鍵などの秘密情報を各種攻撃から保護する耐タンパ技術も，実装面でのキーテクノロジーとなる。モジュール内部を直接プロービングする物理的な攻撃以外にも，暗号回路動作時の消費電力の変動を利用するサイドチャネル攻撃や，暗号回路に物理的な外乱を作用させ，結果として生じる出力のエラーを利用するフォルト攻撃などが脅威となる場面がある。これらの攻撃に対する対策技術の開発を進めている。

量子暗号や量子コンピュータ

近年進展が著しい量子技術を情報セキュリティに適用する動きが活発化している。

量子暗号は，量子力学における不確定性原理を利用した暗号システムであり，安全な鍵配送を実現する。第三者が盗聴を行った場合に，その痕跡(こんせき)が検出できることを安全性の根拠としている。単一光子の生成，変復調，伝送，検出が実用化への課題であり，当社では単一光子の生成と検出をそれぞれワンチップで実現する技術を開発した。

量子コンピュータは，量子ビットの重ね合わせ状態を利用して，現在のコンピュータでは困難な超並列計算を可能とする。量子コンピュータの実現には，集積化が可能な量子ビット素子の開発が課題であるが，実現されれば，計算量的困難性をベースとしている現在の暗号の安全性が崩れ，暗号方式にパラダイムシフトをもたらす。

当社では，量子ビットを固体素子で実現できる方式を研究しており，他方式と比べて量子ビット数を増やすのに有利と期待される。

更にITで社会を豊かにしていくために

今までのITの進歩においては，セキュリティ技術が本来組み込まれるべきである場合でも，セキュリティ以外の技術が，先行して開発され利用されてきた。しかし，これからの社会生活をITで豊かなものにしていくためには，プライバシーとセキュリティの確保は必須であり，ほかの技術と同時にセキュリティ技術を進化させていく必要がある。

ユビキタスコンピューティングやGRIDコンピューティング(注1)などの新規技術開発において，当社は，構想段階からのセキュリティ機能の作り込みによって，より完成度の高い技術開発に注力し，豊かなIT社会の創造に貢献していく。

(注1) 送電網Power Gridに由来することばで，電源につなげればどこで発電された電気かということを意識することなく電気を利用することができると同様に，利用するコンピュータ資源がどこにあるのかを意識することなくコンピュータ資源を利用できるようにする技術のこと。

文　献

(1) (財)日本規格協会．JIS X 5080(ISO/IEC 17799)情報技術－情報セキュリティマネジメントの実践のための規範．2002，78p.

山田　朝彦
YAMADA Asahiko, D. Sc.
e-ソリューション社 SI技術開発センター SI技術担当主査，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。
Systems Integration Technology Center

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
e-ソリューション社 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担当参事。セキュリティプラットフォームサービスに従事。
Platform Solutions Div.