社会インフラを取り巻く脅威と情報セキュリティへの東芝グループの取組み

Security Threats Surrounding Social Infrastructures and Toshiba Group's Approach to Information Security Technologies

秋山　浩一郎　■AKIYAMA Koichiro
遠藤　直樹　■ENDO Naoki
岡田　光司　■OKADA Koji

社会インフラへのサイバー攻撃が現実のものとなり，情報セキュリティは個人や企業を守る技術から人間社会を守る技術へと発展し，ますます重要性を増している。

東芝グループは1980年初頭から情報セキュリティ技術の研究開発を行っており，研究成果として得られた暗号技術やソフトウェア保護技術，システム分析技術が，これまで数々の製品を支えてきた。現在，これらの要素技術は，社会インフラにおいて，スマートグリッドなどの次世代システムをはじめ，サーバ環境やクライアント環境，それらをつなぐ情報ネットワークなどに応用され，社会インフラを支える技術として結実しつつある。

As cyberattacks on social infrastructures have transformed from a threat to a reality, information security technologies have become increasingly important in recent years to protect society overall as well as individuals and businesses.

Since the early 1980s, the Toshiba Group has been engaged in the research and development of information security technologies, including cryptographic technologies, software protection technologies, and security analysis technologies, to protect a large number of products. These core component technologies are currently embedded in server environments, client environments, and information networks connecting these environments, which form the basis of many social infrastructures, and are being applied to advanced systems such as smart grids.

社会インフラを取り巻く脅威

情報ネットワークは人々の仕事や生活にとって不可欠なものであると同時に，情報やその他の資産に対する脅威とリスクが存在していることも事実である。そこで，情報セキュリティ対策が実施され，リスクの低減が図られてきたが，政治・経済状況や産業動向などの変化に伴い，脅威とリスクの状況も変化してきている。最近の顕著な変化としては，制御システムを含む社会インフラに対する脅威を挙げることができる。

■制御システムへの脅威

制御システムとは，機器やシステムを監視し制御するシステムである。従来は閉じたネットワーク内で動作していたが，スマートグリッドなど情報ネットワークと連携したシステムが出現するに従い，外部からの侵入が可能となり，攻撃事例が増えている。

このような例としては，2010年に起こったStuxnetと呼ばれる悪意あるプログラムによる攻撃が著名である。このプログラムは特定の会社が製造した監視制御システム（SCADA）を攻撃対象とする。攻撃されたSCADAはその制御対象であるプラントの機械設備を異常な状態で稼働させ，結果的に破壊に至らせることがある。SCADAは今後発展するスマートグリッドやスマートコミュニティなどの重要インフラのキーとなる仕組みである。このような攻撃が成立するかぎり，エネルギーや各種資源，サービスなどの安定供給を阻害されるという意味で，重大な脅威を受け続けることになる。

■標的型攻撃

また，標的型攻撃の出現も顕著な変化の一つである。標的型攻撃は，特定の組織や個人から技術情報，個人情報，営業情報などを搾取することを主たる目的とした攻撃手法である。電子メールに添付した悪意あるプログラムを開かせるために，送信者として，攻撃対象である組織や個人に関連の深い組織名を名乗り，業務に関連したメール本文を書いていることもある。また，悪意あるプログラムはこの攻撃に特化して作られたものであり，従来のウイルス対策ソフトウェアでは検知できないように作られているケースも多い。前述のStuxnetは標的型攻撃手法を制御システム攻撃に応用したとも解釈することができる。

わが国や諸外国のセキュリティ対策の考え方

わが国では1990年頃から技術的対策の推進や早期警戒態勢の整備が進められてきた。2006～2008年度にわたる第1次情報セキュリティ基本計画及び，2009～2011年度までの第2次情報セキュリティ基本計画では，政府や自治体，重要インフラ（エネルギー，水，交通，物流，金融，医療など10分野），一般企業，家庭などの組織階層における対策方針の立案と実現が図られてきた。

2010年5月には，新たに2010～2013年度を対象にして「国民を守る情報セキュリティ戦略」が策定された[1]。これは，従来の取組みでは不十分であるとの判断

暗号の2013年問題―危殆化と移行に関わる諸問題

■暗号の2013年問題とは

コンピュータ能力の向上や暗号解析技術の進歩に伴い，広く使用されてきた一部の暗号（共通鍵暗号Triple DES（Data Encryption Standard），公開鍵暗号RSA（Rivest-Shamir-Adleman）1024，ハッシュ関数SHA-1（Secure Hash Algorithm 1））の安全性が低下しているとして，米国政府は2010年末までにこれらの暗号の利用を終了し，新しい強度基準に対応した暗号アルゴリズム（それぞれAES（Advanced Encryption Standard），RSA2048，SHA-2など）に移行するよう勧告した。

この勧告を受けて，インターネットのSSL（Secure Sockets Layer）通信などで広く用いられている電子証明書について，証明書発行会社は現行の強度基準にしか対応していない証明書の発行を2013年で終了する予定であり，新しい強度基準に対応した証明書への切替えを進めている。

一方日本政府も，政府機関の情報システムで使用している暗号アルゴリズムを2013年度末までに移行する計画を発表し，民間システムでの移行も呼びかけている。

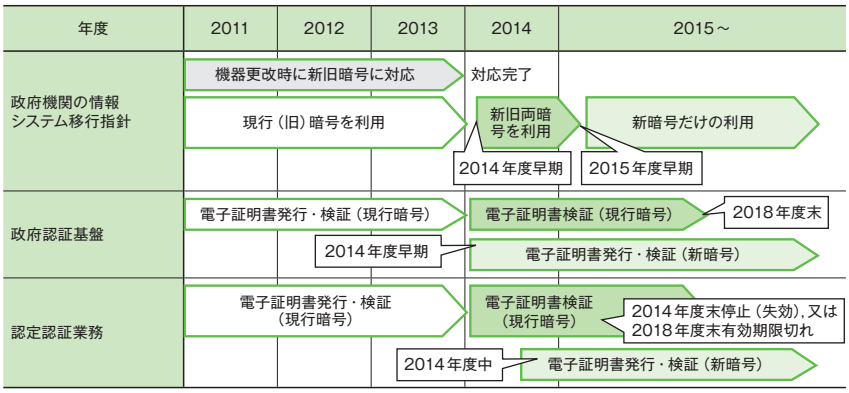
これら暗号の危殆化と移行に関わる諸問題が，いわゆる“暗号の2013年問題”である。

■暗号の移行に関わる諸問題

暗号の移行は，機器やソフトウェアが対応していない，システムの運用期間が長く移行計画がない，移行のコストを誰が負担するのか，といった問題があり，一律的な移行が難しい状況ではある。しかし，移行に対応しない場合，暗号の強度不足による通信データの盗聴や，偽造証明書によるサーバのなりすまし，被害予防や被害拡大防止のための運用停止，証明書発行停止によるWebサイトの運用停止といった問題が発生する可能性がある。また，潜在的に増大するリスクと脆弱（ぜいじゃく）性を抱え続けることとなり，実際に被害に遭わなくても信頼を損なうおそれがあるため，リスクマネジメントの一環として対応する必要がある。

更に，今後も暗号の安全性は時間とともに低下していくと予想されるため，より安全性の高い暗号への移行も見据えた設計・対応計画も必要である。特にハッシュ関数については，NIST（米国国立標準技術研究所）がSHA-2に続く標準ハッシュ関数SHA-3の公募選定を行っており，現在五つの候補まで絞られ，2012年3月に決定され，2013年には規格の発行が予定されている。したがって，SHA-3への移行対応計画も今のうちから検討を進めるべきであろう。

暗号の移行は情報システムに限らず，今後情報システムとの融合やオープン化が進む制御システムについても同様な対応が必要である。特に可用性の確保や長期運用が必要になることから，暗号強度の見通しや移行対応計画について長期的視点で検討していかなければならない。



＊次の資料に基づいて作成

- 第17回情報セキュリティ政策会議．資料1-2「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」．2008-04-22決定．
- 第20回情報セキュリティ政策会議．資料5-2「「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針（平成20年4月22日情報セキュリティ政策会議決定）」に基づく検討状況について」．2009-02-03．
- 経済産業省．「電子署名法における暗号アルゴリズム移行研究会報告書」．2010-03．
- 行政情報システム各省庁連絡会議 共通システム専門部会了承．「政府認証基盤相互運用性仕様書（移行期間編）」．2010-03-30改訂．

図．日本政府及び関連機関の暗号アルゴリズム移行スケジュール

によるもので，以下のような状況を踏まえたものである。

(1) 大規模なサイバー攻撃による脅威の増大　　ガンブラーウイルス，米国及び韓国への大規模サイバー攻撃など

(2) 社会経済活動の情報通信技術への依存度の増大　　情報家電や電子タグなどのネットワーク接続など

(3) 急速な技術革新　　暗号の危殆（きたい）化（**囲み記事参照**），クラウドコンピューティング，IPv6（Internet Protocol Version 6）など

(4) グローバル化の進展　　国境を越えた瞬時の情報流通，各国のセキュリティ制度の調和など

米国でも情報セキュリティ対策の活動強化が図られている。サイバーセキュリティ調整官の設置による国家的取組みの強化や，「Cybersecurity Enhancement Act of 2010」の成立（2010年2月），「サイバースペースのための国際戦略」の策定（2011年5月）などの動きがある。

最近の産官学による情報セキュリティ対策検討の事例

標的型攻撃や制御システムなど社会インフラへの攻撃の阻止と，そのための人材育成のあり方などを検討するために，経済産業省 商務情報政策局主催の「サイバーセキュリティと経済」研究会が開催された（2010年12月～2011年7月）。

経済成長や経済安全保障の観点から必要な情報セキュリティ政策について検討しまとめる，という目的で，最近事例が増大しているインフラ輸出の活性化などを視野に置いた検討が行われた。

この中で制御システムセキュリティへの対応としては，タスクフォースを設置して実務を検討することとなっている。実務として，未然防止の観点から，セキュリティ基準策定や，国際標準化，将来の国際相互承認，評価認証スキームと共通評価設備の構築，脆弱（ぜいじゃく）性ハンドリングの仕組み構築などが盛り込まれた。更に事後対策の観点ではインシデント対応体制の構築が，共通の対策の観点では人材育成や企業への普及・啓発推進が盛り込まれている。東芝グループは，人を大切にし，豊かな価値を創造し，社会に貢献する観点から，積極的に参画している。

情報セキュリティへの東芝グループの取組み

東芝グループでは，多くの事業領域で常にリスクとなる脅威を意識し，そこにセキュリティ技術を応用することで，安全・安心な社会の構築に貢献してきた。

社会インフラ事業では，自動料金収受システム（ETC）やICカードシステムのセキュリティの設計と構築に実績がある。これらのシステムでは機器の偽造による不払いなどの不正行為を防ぐため，機器認証機能が重要である。また，多くの人が関与するシステムでは適切な運用管理も重要なセキュリティ要件である。この観点からは情報セキュリティマネジメントシステム（ISMS）の構築に関与し，多くのシステムに応用してきた。

デジタルプロダクツ事業では，DVDなどのコンテンツ保護技術と，ダビング10のような安全なコンテンツ転送技術に取り組んできた。コンテンツを無許可コピーなどの不正利用から守るための機器認証と暗号化が重要である。また，著作者の権利を守りつつもユーザーの利便性を損なわない仕組み作りのため，コンテンツ保護方式の標準化にも積極的に参画してきた。

電子デバイス事業では，他の事業や産業で活用される暗号機能や認証機能が内蔵されたハードウェアデバイスの開発と製品化を行ってきた。ハードウェアはその中の機密情報を抜き取られにくいため，社会インフラを中心に広く用いられている。しかし近年では動作時にハードウェアから検出される消費電力波形などを用いて内部の秘密情報を推定するサイドチャネル攻撃の可能性が指摘されており，これら攻撃に対する対策と耐性評価が重要となってきている。

今日，これらの取組みはスマートグリッド（スマートコミュニティ）のような個人環境と社会環境の統合を目指す大規模な社会インフラ構想の中で安全・安心を守るシステム技術あるいはその要素技術として結実しつつある。

■社会インフラにおけるセキュリティ

スマートグリッドは発電，送電，及び配電から成る電力系統を情報ネットワークで結び，より効率的な電力利用を行うとともに，太陽光発電など再生可能エネルギーを利用した発電との統合を容易にする大規模社会インフラである。

現在，世界各地でシステム構築や実証実験が行われており，これらの取組みを通してセキュリティ要件が次第に明らかになってくるものと考えられる。東芝グループはこれに先立ってスマートグリッドにおける電力計であるスマートメータに焦点を当て，その認証や暗号化のための統合鍵管理技術AMSO$_{TM}$（Advanced Meter Sign-On）の開発やメータデータを送信する際のプライバシー保護技術の開発を行っている（この特集のp.6－9参照）。

スマートグリッドを含む社会インフラは，個人環境（クライアント環境）と社会環境（サーバ環境）を持っており，それらを情報ネットワークが結んでいる（**図1**）。

東芝ソリューション（株）はこのような社会インフラの構築に向けて，国際セキュリティ標準（ISO/IEC 15408：国際標準化機構／国際電気標準会議規格15408）を満たすシステムを構築する手法“セキュアSI$_{TM}$”をベースに新たな手法を開発している。セキュアSI$_{TM}$では守らなければならない保護資産とそれに対する脅威を網羅的に挙げて分析するとともに，各脅威に対する対策を検討している。しかし，大規模な社会インフラシステムに向けては，より効率的な分析が必要になる。そこで社会インフラをいくつかの部分システムに分け，その内部の分析と外部インタフェースの分析を行う手法を開発した（同，p.10－13参照）。

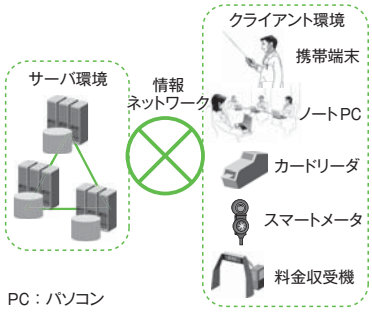


図1．社会インフラの構成（概念図）— 社会インフラはクライアント環境とサーバ環境を持ち，それらが情報ネットワークで結ばれている。
Conceptual configuration of social infrastructures

■サーバ環境におけるセキュリティ

サーバ環境におけるもっとも重要なセキュリティ要件は可用性の実現である。現在のサーバ環境は，システムを多重化するなどの対策を講ずることで可用性を向上させている。

パブリッククラウドではデータの秘匿性もまた重要なセキュリティ要件である。クラウドの運営者に不正がなくても，運用上のミスや無知によりサイバー攻撃を受け，情報漏えいが起こる可能性は否定できない。東芝グループはデータストレージサービスをターゲットに，データを暗号化したまま複数人で共有することができる技術（再暗号化技術）の開発を行っている。（同，p.18－22参照）。

一方，紙や外部記録メディアなどの物理的な形態で散在する文書からの情報

漏えいも深刻な問題である。これに対して，東芝ソリューション（株）は東芝テック（株）と連携して情報統御システムを開発している。情報統御システムはこれら散在している文書に対する出力・複製権限を文書管理サーバで一括管理し，それを出力装置であるデジタル複合機に伝達し，統御管理する。権限は社員ごとに定められ，社員は開示先として指定されていない文書を出力や複製することができない（同，p.35－39参照）。

■クライアント環境におけるセキュリティ

利用者個人が関与するクライアント環境には様々な脅威が存在する。特に不特定多数が関わる社会インフラにあっては，利用者自身の攻撃による脅威も想定しておかなくてはならない。また，利用者に攻撃の意図がなくてもインストールしたアプリケーションや基本ソフトウェア（OS）の脆弱性を突いた第三者による攻撃もある。クライアントが攻撃を受けても正しく動作することを保証できる仕組みが望まれる。

東芝は2000年から，正しい動作を保証できる仕組みを構築するための基礎研究を行ってきた。はじめに着手したのがソフトウェア保護技術である。ソフトウェアには秘密情報のように保護すべき情報が変数の形で含まれている。ソフトウェア保護技術は秘密情報が格納されている変数を保護変数として特別な手段で保護することにより，OSなど周囲の環境が脆弱であっても正しく動作させることができる。現在，データフロー解析を行うことでソフトウェア内の保護変数を自動的に決定する手段を備えたソフトウェア開発支援技術を開発している（同，p.27－30参照）。

ソフトウェア保護技術は，OSやハードウェアなどプラットフォームを選ばない共通の技術であり，汎用性が高いが，ソフトウェア開発に保護機構を定義するプロセスが必要である。

一方，OS自体に前述のような保護機構があればソフトウェア開発自体は変更しなくてもよい。この観点から，スレート端末や携帯電話のOSとして急激に普及しているAndroid™ (注1)プラットフォームをターゲットとして，Webアプリケーションから端末機能の不正利用を防ぐWebアプリケーションプラットフォームを開発した（同，p.23－26参照）。

更に，ICカードのようなデバイスもクライアント環境にある。ICカードはハードウェア実装されているため，ソフトウェア実装に比べて保護しやすい。しかし近年では，前述のサイドチャネル攻撃によって，なんら対策を実施しなければ内部に格納されている秘密情報（鍵情報）が簡単に漏えいしてしまう。このような実装攻撃は年々進化しており，実装攻撃に対する安全性評価がICカードを製品化するうえで重要になっている。この評価を効率化するため，組込み型相関電力解析を開発した（同，p.31－34参照）。

■情報ネットワークにおけるセキュリティ

サーバ環境とクライアント環境をつなぐ情報ネットワークにも脅威が存在する。しかし，これらは適切な暗号技術と認証技術を利用することで解決することが多い。一方で，国家機密レベルの情報は現在でも情報ネットワークによらずにクローズドな通信路か，手渡しによる送達が行われている。これは暗号技術や認証技術の危殆化に関連している。すなわち，危殆化が予想外に早く，数年後にその問題を容易に解くアルゴリズムが発見されると，それに気づくまでの間は情報が漏れることになる。

このような観点から東芝グループは，安全性が物理的に保証できる量子暗号通信の研究を行っている。量子暗号は単一光子を送信するとともに，その量子状態が観測（盗聴）されることで変化することから，盗聴を検出するものである。逆に，盗聴が検出されなかったことをもって安全な鍵を共有できる。このように量子暗号は物理的に安全性が保証された暗号として，今後機密性の高い社会インフラを中心に活用されていくと考えている（同，p14－17参照）。

（注1）　Androidは，Google Inc.の商標又は登録商標。

今後の展望

社会インフラを重要な事業領域の一つとする東芝グループではスマートグリッドなどの世界的な情報統合化の流れを推進している。これまで人間が行ってきた制御の一部を情報に基づいて自動化することは効率化及び合理化の観点から望ましい反面，脆弱性も生まれやすい。

東芝グループは今後とも社会インフラに関わる脅威を分析し，それが顕在化する前に対策を行うことによって，人々に安全・安心な利便性の高い社会の実現に貢献していく。

文　献

(1)　情報セキュリティ政策会議．“国民を守る情報セキュリティ戦略”．2010-05．内閣官房情報セキュリティセンターホームページ．<http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf>，（参照2011-07-25）

秋山　浩一郎
AKIYAMA Koichiro, D.Eng.
研究開発センター　コンピュータアーキテクチャ・セキュリティラボラトリー研究主幹，博士（工学）。暗号及び情報セキュリティ技術の研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer Architecture & Security Systems Lab.

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など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.

岡田　光司
OKADA Koji, D.Eng.
東芝ソリューション（株）IT技術研究所 情報セキュリティラボラトリー室長，博士（工学）。情報セキュリティ技術の研究・開発に従事。国際暗号学会（IACR），電子情報通信学会会員。
Toshiba Solutions Corp.