社会システムの安全性を支える東芝グループの情報セキュリティ技術

Toshiba's Approaches toward Information Security Technologies Enhancing Social Systems

秋山　浩一郎　■AKIYAMA Koichiro
島田　毅　■SHIMADA Tsuyoshi
斯波　万恵　■SHIBA Masue

クラウドサービスの利用が進み，実証実験を通してスマートコミュニティの具体的な方向性が示されるなど，社会の新たなニーズによって，情報セキュリティのあり方が変わってきている。特に，効率的な社会を実現するため，制御システムがインターネットに接続されることになり，重要インフラのサイバー攻撃からの保護が喫緊の課題となってきている。

東芝グループは，モバイル端末やセンサなどのエンドポイントから制御システムやクラウドシステムまでをトータルに考え，社会システムとしての安全性を支える情報セキュリティ技術の実現を目指した研究開発を進めている。

The expanding use of cloud-based services and the implementation of various demonstration experiments have been providing concrete directions for smart communities. The technologies essential for information security are shifting with the changes taking place in these contemporary social needs. In order to construct efficient communities, control systems for social infrastructures are inevitably being connected to the Internet. The protection of critical social infrastructures against cyberattacks has therefore become an issue of vital importance.

The Toshiba Group has been engaged in research and development aimed at realizing information security technologies to support safe and secure social systems through totally optimized management from endpoints including mobile terminals and sensors to control systems and cloud-based systems.

IT環境の変化

スマートコミュニティでは，社会インフラがネットワークでクラウドシステムに接続され，相互の情報交換やビッグデータの活用により，より効率的な社会の実現を目指している。あらゆる場所の多種多様な“モノ”がインターネットを介してクラウドシステムにつながり，人とモノ，モノとモノの間のコミュニケーションを通して，クラウドサービスやアプリケーションを利用するInternet of Thingsが進展している。

2012年には87億個のモノがネットワークにつながっており，2020年には，全世界で500億個のモノがインターネットに接続されるといわれている。これらのモノはネットワークの末端にあるエンドポイントと呼ばれ，そこで作られるデータはクラウドシステムに収集，蓄積されて様々なサービスに活用されるようになり，新たな価値を創造することが期待されている。

その代表的な例が，エネルギーや，水，交通，物流，医療，情報通信など，あらゆるインフラの統合的な管理と最適制御を実現した次世代のコミュニティであるスマートコミュニティである。スマートコミュニティでは，エンドポイントのデータやSNS（Social Networking Service）のデータがネットワーク上を行き交い，複数のシステムにわたるデータの分析と機器のコントロールができるようになる。スマートコミュニティを実現するうえで，これまで企業システムを中心に形成されてきたIT（情報技術）と，社会インフラシステムの運用と制御技術，いわゆるOT（Operation Technology）の融合は不可欠であり，それは既に始まっている。

情報セキュリティリスクの変化

一方で，ITとOTの融合により新たなセキュリティリスクが生まれている。

世界では，鉄道の信号機システムへのハッキングや，核施設へのサイバー攻撃が発生している。これまで独自の仕様に基づいて開発され，オープンなネットワークから切り離された環境で運用されてきた制御システムが，汎用技術の採用やインターネットとの接続といった“オープン化”により，サイバー攻撃の対象となっている。

米国の国土安全保障省（DHS）のICS-CERT（Industrial Control Systems Cyber Emergency Response Team）のレポートによると，米国における制御システムに対する攻撃のインシデント報告件数は，2010年の39件から2012年には約5倍の197件と増加している。このレポートでは，産業制御システムや重要インフラの運営企業に対する標的型攻撃の事例が報告されている。この報告からも，標的型攻撃が，企業システムだけでなく，制御システムにも及んでいると言える。

制御システムや重要インフラへのサイバー攻撃は，情報の漏えいだけでなく，システムの誤動作や停止に伴う障害などにより，ライフラインが脅かされるといった危険性を秘めている。

セキュリティの新たな方向性

こうした情報セキュリティリスクの変化に対して，セキュリティの取組みや技術開発には，新たな方向性が求められている。

高度化するサイバー攻撃への対応，重要インフラなどの制御システムの安全性の確保，クラウドシステムに集約されるビッグデータを安全かつ高速に処理する基盤技術の開発，大量に流通するパーソナルデータを含むデータの保護や信頼性の確保といったセキュリティの課題に対応していかなければならない。

サイバー攻撃に対しては，システムへの侵入を前提とした早期発見，出口対策の実施に加え，ネットワークを常時監視して攻撃の危機を抽出することが重要になってくる。また，同じ業界への攻撃の有無や手口などの情報の収集や，個人や企業のITユーザーとITベンダー，一般社団法人 JPCERT（Japan Computer Emergency Response Team）コーディネーションセンターなどの専門機関との連携が必要である。更に，セキュリティ演習への参加を通して，攻撃への対応能力を高めることが望ましい。

また，人やモノとクラウドシステムをつなぐエンドポイント，特に，近年利用が広まっているモバイル端末のセキュリティ対策は，重要性を増している。エンドポイントからの情報を安全に活用し，適切な情報として出力するには，送られてくるデータの真正性や秘匿性を確保することが重要である。これにはエンドポイントそのものをマルウェアなど外部からの攻撃から保護するとともに，通信路上でのデータの安全性確保のための仕組みが必要である。

これらの方向性に対して，東芝グループは様々な取組みを展開している。

東芝グループの取組み

東芝グループは1980年代に，来るべき情報化社会でのセキュリティ技術の重要性に着目して，その基盤技術である暗号技術の研究開発を開始した。

1990年代には，デジタルコンテンツを不正コピーから守る著作権保護技術が求められるようになり，暗号技術をベースに著作権保護システムを構築した[1]。

2000年代には，デジタル機器のネットワーク化や，社会インフラのIT化が進み，ICカードシステムや，現在広く普及している高速道路のETC（自動料金収受システム）の実現に，東芝グループの暗号技術や著作権保護システムで培ったセキュリティシステム技術が貢献した[2]。またこの頃から，機器やシステムに組み込まれるセキュリティシステムを第三者の認証により評価しようとする動きが出てきた。

ISO/IEC 15408（国際標準化機構／国際電気標準会議規格 15408）はその代表的なものである。東芝グループはセキュリティ評価及び認証のコンサルテーションにおける実績と，これまで構築してきたセキュリティシステムをベースに，セキュリティ構築を手法化し[3]，ユーザーに対して安全と安心を提供している。

セキュリティに新たな方向性が求められる今日，これらの技術や手法は，システム実装や運用に携わる技術者の知見とも合流し，新たなステージに入ってきている。スマートコミュニティが目指す社会と東芝グループのセキュリティ技術の概要を，**図1**に示す。

■サーバシステムのセキュリティ

社会インフラの心臓部である制御システム（図1の右下）も，インターネットに接続されるためサイバー攻撃を受ける可能性が出てくる。

特に標的型攻撃など，ターゲットを絞って周到に準備される攻撃では，攻撃者は運用も含めたシステムの脆弱（ぜいじゃく）性を探索し，段階を踏んで攻撃を行う。これに対抗するにはシステムを常時監視するとともに，システムログを解析して，不穏な動きを察知し，実際に攻撃を受ける前に対策を行うアクティブディフェンスが重要になってきている（**囲み記事参照**）。アクティブディフェン

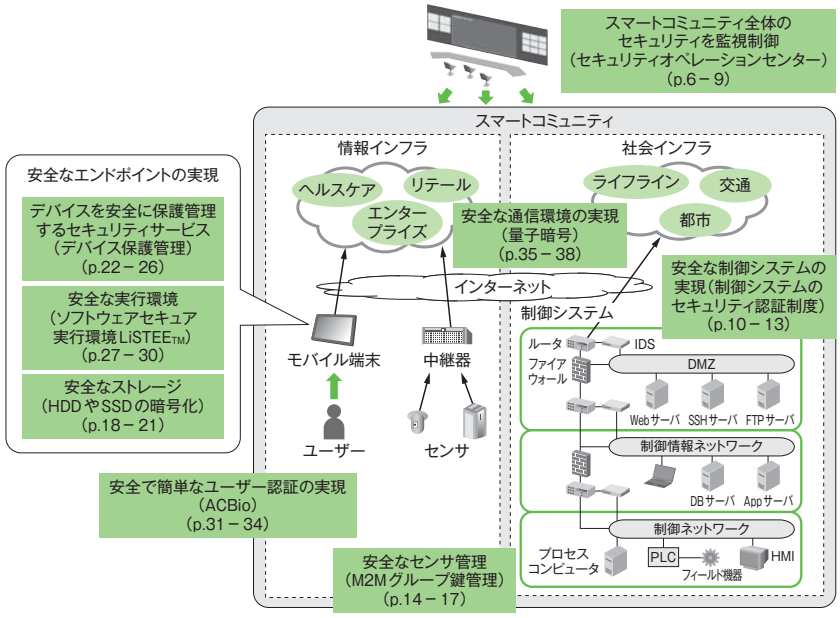

図1．スマートコミュニティを守るセキュリティ技術 ― 東芝グループは，スマートコミュニティが目指す社会を実現するため，それを支える様々な情報セキュリティ技術の開発を進めている。

Information security technologies to protect smart communities

複雑・高度化するサイバー攻撃とアクティブディフェンス

2013年6月に内閣官房情報セキュリティセンター（NISC）情報セキュリティ政策会議から「サイバーセキュリティ戦略」[4]及び「サイバーセキュリティ2013」[5]が発表された。前者は，サイバー空間におけるリスクについて多角的に分析し，サイバーリスクへの対応が産業活性化の観点から不可欠としている。一方，後者では，これまでクローズドな独立系システムであった制御システムも，サイバー攻撃の対象であると述べている。これらは，サイバー攻撃の高度化や今後想定される被害の大きさから示された施策であると言える。

サイバー攻撃が複雑化及び高度化している背景には，攻撃目的の変化がある。これまでは政治・思想的な主張を背景とした攻撃が主であったが，最近では特定の相手を狙って盗み取った情報を転売したり，盗んだ情報を脅迫に使って金銭を得るなど金銭目的の標的型攻撃が増えている。また，情報やツールの提供，攻撃の代行，仲介など攻撃が分業化されていると見られ，組織的な集団によるものとも言われている。一方で，攻撃のためのツールがインターネットから容易に入手でき，クラウドシステムを利用して，それを大規模に実行できるなど，特別な知識がなくても攻撃ができる環境となってきている。

このように標的を定めて，組織的かつ継続的に行われる攻撃では，外部からの侵入を防ぎ，また，情報を漏えいから守るといった既存の対策アプローチだけでは不十分である。ロッキード・マーティン社によって提唱されたサイバーキルチェーンのように標的型攻撃を軍事作戦における多段の攻撃フェーズになぞらえ，それに対するインシデントレスポンスを考えるアプローチもある（**図A**）。このような深化する多段攻撃の各フェーズにおける脅威を知り，リスクを分析し，脆弱性を排除する仕組みをシステムに取り入れるといった基本的なセキュリティ対策を徹底することに加え，システム全体の網羅的な監視により，インシデントを検出し対策を実施することが必要である。また，防御や検出された攻撃への対策だけでなく，システムの監視から得られるログやインシデントの情報を収集してデータを分析し，脅威の特徴を捉え未来の脅威に対処するアクティブディフェンスが，今後は重要になってくる。

攻撃の深化

フェーズ	検知	拒否	中断	封じ込め
偵察	Web分析	ファイアウォールアクセス制御	―	ファイアウォールアクセス制御
武装化	ネットワーク侵入検知システム	ネットワーク侵入防止システム	―	ネットワーク侵入防止システム
配送	慎重なユーザー	プロキシフィルタ	電子メールアンチウイルス	フィルタリングファイアウォール
エクスプロイト*	ホスト侵入検知システム	パッチ	データ実行防止	内部ネットワーク侵入防止システム
インストール	ホスト侵入検知システム	アプリケーションのホワイトリスト	アンチウイルス	―
遠隔操作	ネットワーク侵入検知システム	ファイアウォールアクセス制御	ネットワーク侵入防止システム	トラストゾーン
目的の実行	ログの監査	アクセス制御	情報漏えい防御	トラストゾーン

＊脆弱性を突いて攻撃すること

図A．サイバーキルチェーン

スの実現に向けて東芝グループは，クラウドサービス事業で培った知見を生かし，制御システムのインシデント分析・検出技術の開発を行っている（この特集のp.6－9参照）。

一方，スマートコミュニティの中核となっている電力システムにおいては，発電・送配電設備，ビルなどのエネルギー管理設備，及びAMI（Advanced Metering Infrastructure）がネットワークにつながりつつある。これらの制御システムは，個々に，また互いに連携してアクティブディフェンスを実現しなくてはならない。そのためにはセキュリティ要件の定義（Plan），セキュリティ要件に沿った設計と実装（Do），セキュリティ演習（Check），及びその対策（Act）といった改善サイクル（PDCAサイクル）の確立が必須となる。東芝グループは経済産業省による国家プロジェクトとして2012年に設立された技術研究組合 制御システムセキュリティセンター（CSSC）に参画し，宮城県多賀城市に模擬プラントを設置して，PDCAサイクルで重要なステップであるセキュリティ演習の準備を進めている（同p.10－13参照）。

スマートコミュニティでの制御はスマートメータに代表されるセンサなどの端末機器からの情報に基づいて行われる。これらセンサは人間が介在することなく，自律的に他のセンサや上位の中継器との通信を行う。多くの機器から構成される大規模な通信システムでは，通信量を抑え，効率的な運用と制御を行うために，グループでの機器管理とグループ通信が重要になる。東芝グループは，グループ鍵による効率的かつ安全なグループ管理を行う技術を研究開発し，国際標準規格化を進めている（同p.14－17参照）。

■端末機器のセキュリティ

モバイル端末などの端末機器は個人，企業を問わず広く利用されており，ユースケースに応じたセキュリティ対策が求められている。東芝グループは安全なモバイル端末の対策を，図1の左に示す技術で実現している。

モバイル端末に対する脅威のうちもっとも深刻なものとして，情報の流出が挙げられる。これは紛失や盗難に起因す

るものと，不正アプリケーションの導入に起因するものがあり，それぞれ対策が異なる。

紛失や盗難への対策として，東芝グループはHDD（ハードディスクドライブ）やSSD（ソリッドステートドライブ）に保存するデータを自動的に暗号化するSED（Self Encrypting Drive）を開発した。SEDは紛失・盗難時にリモートで復号鍵を消去することにより，情報の秘匿性が保たれるため，個人利用のモバイル端末の紛失時対策となる。また，クラウドサービスを運営する企業などの機器廃棄対策にも効果を発揮する（同p.18－21参照）。

不正アプリケーションの導入への対応に関して，東芝グループは米国Google社が開発したOS（基本ソフトウェア）が搭載されているモバイル端末について，アプリケーションを認証することによって正当なアプリケーションだけがインストールできる環境を構築した。更にこれを発展させ，ビジネス向けに接続するデバイスや無線通信を制限できる，よりセキュアな環境をセキュアプラットフォームとして実現し，これを利用して，社内全てのモバイル端末に統一したセキュリティポリシーを設定できる保護管理技術を構築した（同p.22－26参照）。

モバイル端末では，利用者による不正利用の防止も必要である。Linux®(注1)などの汎用OSはモバイル端末に限らず，家電や制御機器など組込み機器に広く採用されてきている。汎用OSは脆弱性が発見されやすく，これを利用して認証を突破し管理者権限が奪われると，OSのセキュリティ機構が無効化され，情報漏えいや機器の不正利用へとつながる。東芝グループは，これに対抗するため，外部からアクセスできないセキュアOSを構築し，セキュリティを考慮していないOSと切り替えることによってアプリケーションを実行するソフトウェアプラットフォームLiSTEE$_{TM}$を開発した。これを用いることで，従来はハードウェアでしか実装できなかったような復号鍵を用いる復号処理など機密性の高い処理を，セキュアOSで実行するソフトウェアとして実装できることになり，製品開発期間を大幅に短縮できる（同p.27－30参照）。

また，東芝グループは，安全な個人認証を行うという観点から生体認証の実用化に向けた取組みを続けてきた。生体認証を利用するシステムでは通常，指紋や虹彩などの生体情報を取得する機器とそれを照合する機器がセキュアなネットワークで接続されている。しかし，クラウドサービスの利用が進むなか，インターネットを介したサービスのユーザー認証に生体認証を使いたいというニーズがある。認証を含むID（Identity）管理システムを独立したサービスとして提供する動きもある。これらに対応して，東芝グループが主導して国際標準化を実現したオンライン生体認証技術ACBio（Authentication Context for Biometrics）を利用して生体認証をクラウドサービスとして実現する手法を開発した（同p.31－34参照）。

■将来の脅威に備えて

近年，サイバー攻撃に変化があったように（囲み記事参照），情報システムに対する攻撃手法はこれまでも進化してきており，これからも新たな脅威が出現するものと考えなければならない。東芝グループは，通信の秘匿性を物理的な意味で保証できる，量子暗号に注目している。これまでの研究で東芝グループは世界最高速(注2)の鍵配信となる1Mビット/sを実現しており，その実用化に向けたネットワーク技術の開発も進めている（同p.35－38参照）。

今後の展望

東芝グループは，デバイス事業，社会インフラ事業などを通して，社会に新たな価値を創造してきた。これからはヘルスケア事業も含め，スマートコミュニティという，より大きな構想の中で，より多くの社会貢献が求められている。

情報セキュリティ技術はこれらを支える重要技術として，今後のニーズを先行して捉え，東芝グループの知見を結集して技術開発を進めていく。

(注1)　Linuxは，Linus Torvalds氏の日本及びその他の国における登録商標又は商標。
(注2)　2013年12月現在，当社調べ。

文　献

(1) 石原　淳. DVDのコンテンツ保護. 東芝レビュー. 58, 6, 2003, p.28－31.
(2) 上野秀樹 他. ETCシステムにおけるセキュリティ. 東芝レビュー. 56, 7, 2001, p.50－53.
(3) 小田原育也 他. セキュアシステムインテグレーション. 東芝レビュー. 58, 8, 2003, p.11－14.
(4) 情報セキュリティ政策会議. “サイバーセキュリティ戦略”. NISCホームページ. <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>,（参照2013-11-05).
(5) 情報セキュリティ政策会議. “サイバーセキュリティ2013”. NISCホームページ. <http://www.nisc.go.jp/active/kihon/pdf/cs2013.pdf>,（参照2013-11-05).

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。電子情報通信学会会員。
Computer Architecture & Security Systems Lab.

島田　　毅
SHIMADA Tsuyoshi
東芝ソリューション（株）IT研究開発センター主幹。システムセキュリティ評価技術の研究・開発に従事。IEEE会員。
Toshiba Solutions Corp.

斯波　万恵
SHIBA Masue
東芝ソリューション（株）IT研究開発センター 研究開発部グループ長。情報セキュリティ技術の研究・開発に従事。電子情報通信学会会員。
Toshiba Solutions Corp.