富士通が目指すこれからのセキュリティ

FUJITSU Security Initiative

● 太田大州

あらまし

21世紀に入って15年が経過し，従来では考えられない不確実性の時代を迎えている。ICTが広く社会基盤として活用され，インターネットの普及が一層拡大する中で，ICTの安心・安全な運用が強く求められている。従来，個人情報漏えいなど事故，およびその予防措置を中心に捉えられていたセキュリティは，サイバー攻撃の増加に伴い，事件・事故が起こることを前提とした新しい考えに基づいたICT，および組織運用が必要になってきた。

本稿では，この新たなセキュリティへの考え方を体系化したFUJITSU Security Initiativeを紹介する。また，この体系の中で特に今後強化が必要な三つの技術要件と，それらに対する取組みについても述べる。IoT(Internet of Things)が進化しデータがより高い価値を持つ時代を迎える中，これらの取組みを社会の多くの組織が理解し積極的に対応することで，安心・安全なICTの運用を確立するとともに，安全と成長を両立できる社会の実現を目指したい。

Abstract

We are now 15 years into the 21st century and seeing an age of uncertainty that was unthinkable in the past. As information and communications technology (ICT) is utilized as social infrastructure and use of the Internet is increasingly widespread, safe and secure operation of ICT is strongly desired. Security has conventionally been seen mostly from the perspective of accidents including personal information leakage and preventive measures. However, as cyber attacks are increasing, there are needs for ICT and organization operation based on a new concept, on the assumption that incidents and accidents are bound to occur. This paper presents FUJITSU Security Initiative, which systematizes the new concept of security. It also describes the three technical requirements that particularly need strengthening in the future and approaches to them. We intend to work on establishing safe and secure operation of ICT by ensuring that many organizations in society understand and proactively implement these approaches. In addition, as we are now in the age in which the Internet of Things (IoT) has evolved and data have a higher value than ever, we also aim to help realize a society where competitive advantage is ensured with both safety and development achieved.

ま え が き

2005年4月に制定された個人情報保護法は，ICTにおいて機密性・利便性・生産性のバランスが取られた最適解を社会に求めることになったが，多くの組織は利便性や生産性を犠牲にした。また，2008年に施行された金融商品取引における内部統制報告制度（J-SOX法）による内部不正対策の具現化は，ICTによる効果を更に縮小させ，定型的なマネジメント強化を促進することになった。

しかし，セキュリティに関する事件・事故はとどまることがなく，更に2011年からは標的型のサイバー攻撃が繰り広げられてきた。セキュリティに関して，予防的に安全が確立されることはない。このため，今後のマネジメントにおいては事件・事故が発生することを前提として考えることがICT運用を最適化させ，サービスを継続できる社会構造を形成することにつながる。

本稿では，富士通が目指すセキュリティに対する考え方を紹介する。更に，体系を強化するために必要な領域として「セキュリティインテリジェンス」「プライバシー保護」「認証基盤の充実」の三つを設定し，業務継続の運用を支える考え方について論述する。

サイバー攻撃の現状

21世紀の初め，パソコンやインターネットの普及によって情報の拡散が非常に容易になり，情報の利活用は従来以上に進化した。この時代は「ウイルス」という迷惑型の攻撃に対するセキュリティ対策が中心であり，そのための投資が場当たり的に行われていた。

2005年に制定された個人情報保護法により，企業は様々な予防対策を施したが，漏えい事故はとどまることなく経営陣を悩ませる結果となった。新たに発生する漏えい事故の事例分析から，コンプライアンスの観点で内部統制システムの構築が要請された。また，コーポレートガバナンスの仕組みの多くはセキュリティマネジメントと共通する部分も多いことから，セキュリティ対策にはコストがかかるという認識が根付いてきたと考えられる。

日本の組織では，内部のリスクに関しては「従業員，人間は性善である」ことを前提にしており，外部からの脅威に関しては法律で守られていると考えている場合が多い。しかし，ICTの高度化と進展の早さにより，内部のリスクの変化や外部からのリスクへの対応が困難な状況になっている。更に，内部不正を阻止できず，サイバー攻撃の被害も拡大していることから，従来の対策の限界を迎えていると考えられる。

2010年6月に発見されたマルウェア「Stuxnet」は，サイバー攻撃がインターネット社会における新たな脅威として認識されるべき起点となった。以降，国家間での攻撃のみならず，営利を目的とした組織犯罪も拡大しており，日本国内においても多くの事件が外部からの攻撃により引き起こされている。このように，日々，事件・事故は起こっているものの，自分の組織は大丈夫といった楽観的な感覚を持つ経営者が多いこと，また，完全にこのサイバー攻撃を阻止する技術は存在しないことが，ICTが抱える課題である。

ICTに関係するリスクはコーポレートガバナンスとして扱われ，適正な投資の中で厳正な運用を実現することが極めて重要な問題であると認識すべきである。

新たな考え方

ICTの使命は，業務を継続させるための運営を支え，新たな価値を創造することである。しかし，ICTに依存する限り日々変化するセキュリティ問題から解放されることはない。つまり，セキュリティは一時的な対策投資ではなく，継続すべき運用であることを再認識し，組織の特性に応じたリスク認識によって運用をイノベーションする必要がある。

サイバー攻撃に対応するための事業継続観点での考え方を**図-1**に示す。危機発生後の事業復帰曲線を，事前対策によって最低限の事業レベルを確保するための事前準備や，早期に通常レベルに復帰するための危機管理対応の必要性は，自然災害，機器障害などのリスク対応と同じである。しかし，サイバー攻撃リスクは危機発生前にその兆候に気づくことができる機会が存在するため，この兆候をインシデントとして的確に対応することで危機の発生を未然に防ぐことができる。ここにイノベーションのポイントが存在し，挑戦すべき課題であると考えた。

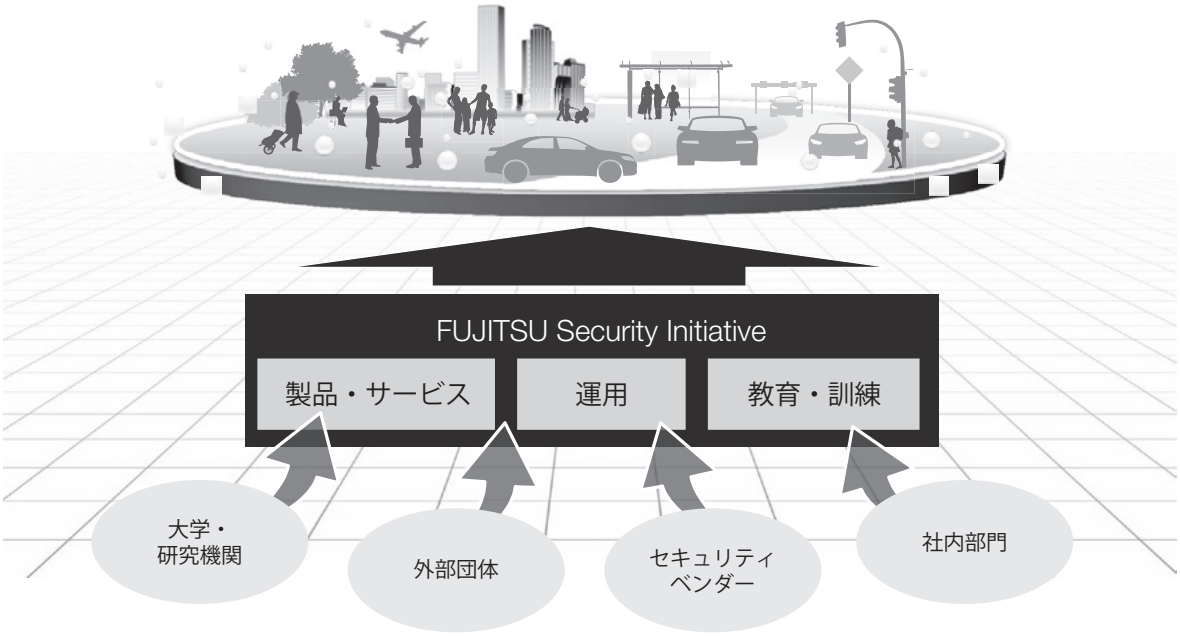

図-2　FUJITSU Security Initiativeの概念

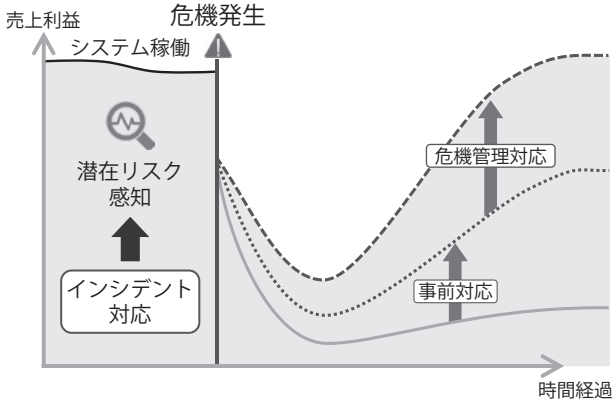

図-1　事業継続観点の考え方

富士通はこの問題解決に当たり，ICTベンダーとしてリファレンスを確立する手法により運用の最適化がいかに有益であるかを証明し，更にその運用に必要となる技術を開発するプロセスを提言することで，この社会問題の解決に挑むことにした。

FUJITSU Security Initiativeの概念を**図-2**に示す。これは，富士通がお客様のイノベーションを支えるために，お客様基点でICTの安心・安全を実現する継続的な取組みであり，お客様と創造するインテリジェントソサエティを三つの要素でセキュアにする考え方である。考え方の中心は「運用」であり，組織に最適な運用を作り上げる必要性を表している。この運用を実現するために必要となる「製品やサービス」を選別して，完全性・機密性・可用性を満たしていくことを提言している。また，製品やサービスを導入するだけではリスクマネジメントや緊急対応は実現できない。適切な運用のためには，最低限の知識と経験を備えた人材が必要になる。そのため，人材育成のための「教育・訓練」も継続的に実施し，危機管理能力を組織として高めることが重要であると考えている。富士通は，この考え方に基づいた運用のイノベーションを継続的に実施しており，その内容については本誌で紹介する。

目指す技術戦略

いつでも，どこでも，誰でも，どのようなことにもICTが活用されるIoT（Internet of Things）時代が進展している。2020年には，500億個以上の物がインターネットに接続され，相互利用される時代になる。様々なデバイスやセンサーがつながり，データが価値を生み出す中で，いかに安心・安全にICTを利用できるようにするのか，サイバー攻撃への対応を併せて考える必要がある。

将来へ向けてICT運用のイノベーションを進める中で，今後強化すべき三つの技術領域について述べる（**図-3**）。

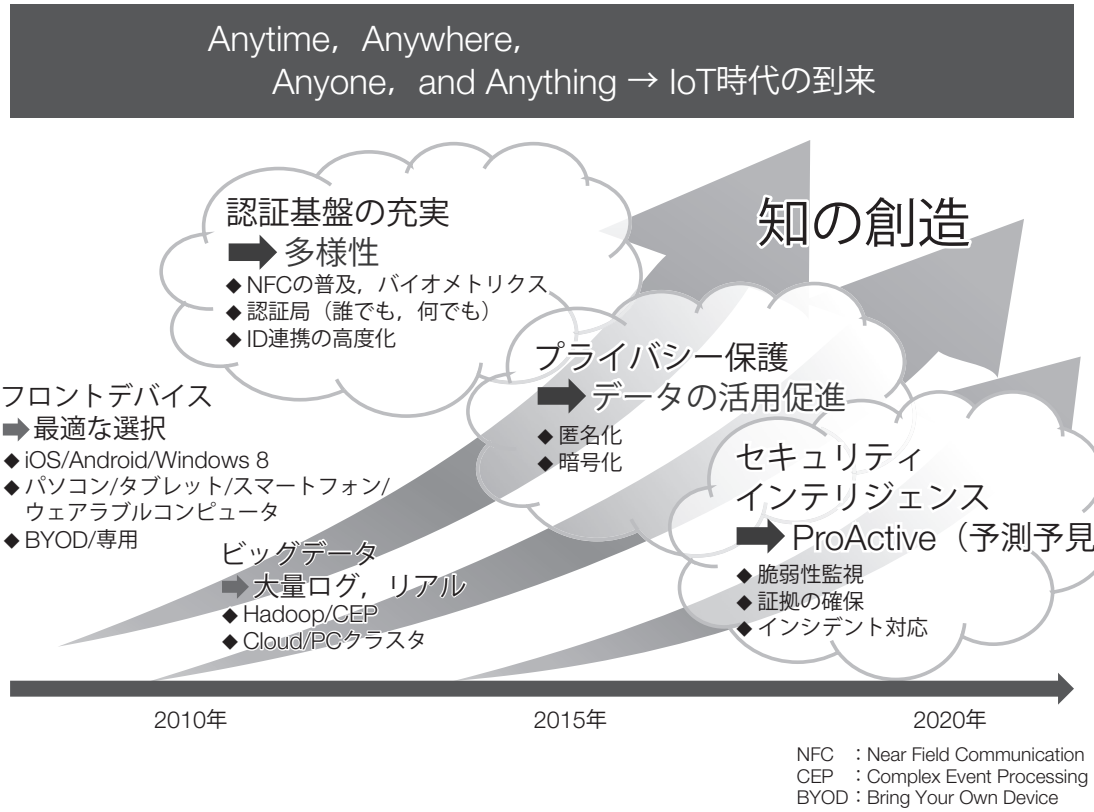

図-3　これからのセキュリティ強化ポイント

（1）セキュリティインテリジェンス

現在，大きな社会課題となっているサイバー攻撃の脅威に対抗するための新たな技術領域である。知見の集約と活用により，攻撃直後の迅速な対応の実現と，最新の社会情勢に応じて変化できるセキュリティ運用を実現する。

（2）プライバシー保護

情報漏えいが発生した際に，被害を極小化・無害化する暗号化・匿名化技術である。犯罪者の行為を無力化するのではなく，攻撃の結果を無効化すると同時に，情報の活用も可能にする技術領域である。

（3）認証基盤の充実

実世界とサイバー空間をつなぐ認証・認可基盤を確実に構築することにより，的確なアクセスコントロールが可能となり，サービス提供レベルの最適化や不正利用の発見・阻止を迅速に行える。これにより，内部不正の阻止やサイバー攻撃の発見，効果的なフォレンジック（証拠）情報としての活用が可能になり，正確な状況把握と的確で迅速な危機対応ができる。

富士通は，自社のICTのセキュリティ運用をリファレンスとした改善の継続により得た経験や知見を，社会に還元することを決めた。更に，前述の三つの技術領域において，より効果的な改善を進めるための技術開発と製品の提供を継続することで，IoT時代のICT運用のリーダーシップを目指していく。

挑戦する領域

本章では，「サイバー攻撃の現状」の章で論じた問題点を解決するための手法と，それを実現する新たな技術について，本誌で掲載する順に紹介する。

（1）認証技術

ICT活用の現場は，パソコンからスマートフォン，タブレットへと一気にシフトしている。しかし，その利用におけるセキュリティは，ID，パスワード程度で強度が極めて低い。この強度を高めるため，最低でも二要素認証や生体認証を取り入れる組織・サービス分野も出始めている。富士通は，様々な制約（時間，場所，利用デバイス，組織ロール）を自由に組み合わせ，経済的で安全な認証基盤を

構築する挑戦を開始した。いつでも，誰でも，様々なサービスにアクセスでき，更に正しく認証する基盤として手のひら静脈認証を採用し，利便性と安全性を両立させる取組みである。

また，2016年1月から始まるマイナンバーカードの配布に伴い，様々な認証基盤の基礎になる公的身分証明証とひも付けた本人認証基盤の普及に向けた準備が完了している。

(2) プライバシー保護，暗号技術

クラウドコンピューティングにより，データの活用はICTの大きな役割となった。しかし，そのデータに関してプライバシー保護や機密情報の保全の観点から新たな技術が求められている。マイナンバー制度や個人情報保護法，EUデータ保護規則案の観点から，富士通では個人情報やプライバシー情報を含むパーソナルデータを安全化して取り扱うk-匿名化や準同型暗号の活用を可能にする技術を確立し，ソリューションの提供を開始した。また，サイバー攻撃などで窃取されたデータを犯罪者が有益な情報にするために多大なコストが必要となる，最先端の暗号化技術の成果についても本誌掲載の「暗号技術の最先端」で紹介する。

(3) セキュリティインテリジェンス

サイバー攻撃は圧倒的に攻撃者優位の状況にあり，技術の進展が犯罪や反社会的な行為に利用されている。このため，社会全体から多くの脅威情報を収集し，新たな攻撃に対して準備を進めなくてはならない。また，自らが利用するICTの中で何が起こっているのかを常に把握し，脅威への対応の妥当性を検証しつつ，現状から将来のリスクを想定し攻撃に備える運用や体制構築が極めて有効であり，必要な解である。

現在，情報収集の考え方として，インターネットの入り口と出口で攻撃と侵略を感知する仕組みが多く用いられている。また，多くのICT運用ログを活用した相関分析から脅威を発見し，その後の対応を的確に実施するセキュリティインテリジェンスが普及し始めている。これにより，攻撃のパターンや侵略の手法を分析するとともに，防御や侵略状況を把握する技術を高め，有効なインテリジェンスを作り上げてきた。サイバー攻撃を的確に阻止することができない中で，その後の内部侵略を発見し，拡大を防ぐことが可能となってきており，今後多くのICT運用に適用することで更なるインテリジェンスの高度化が図れると期待している。

これら三つの技術要素への挑戦を行いつつ，開発，運営における人材の育成についても取組みを開始した。経済産業省の試算では，2020年に約8万人のセキュリティエンジニアが不足すると予測されるように，今後のICTの開発・運用におけるセキュリティ人材育成は重要度が増す。新たな人材をいかに発見・確保するかが大きな社会課題となる中で，富士通が保有するエンジニアの育成を支援するためのセキュリティマイスター認定制度を2014年度より開始している。お金でのリクルートや新卒人材の確保など多くの施策がある中で，社内人材の育成に重きを置いた考え方を取った。ICTのある限り存在し続けるサイバー攻撃の脅威と運用課題に対して，永続的なお客様との協調を実現するための最適な解であり，その教育・訓練内容をお客様にも提供し，社会全体の人材強化に貢献したいと考えている。

むすび

不確実性の時代にICTを安心・安全に活用するために，社内の実践を通じて高めてきた技術やノウハウを多くの場面でお客様に活用していただける準備が整った。しかし，どのような事件・事故が発生するのか予測できない時代においては，技術を進化させ続ける必要がある。

セキュリティ運用のインテリジェンスをお客様と共創・共有し，社会全体のエコシステム形成を通じて，運用の実践と技術の探究を大切にしていく。また，次世代のセキュリティ関連エンジニアの育成を含め，お客様のセキュリティ環境のイノベーションを推進することをお約束し，むすびとしたい。

著者紹介

太田大州（おおた　たいしゅう）

統合商品戦略本部 所属

現在，セキュリティ・エバンジェリストとしてお客様への価値訴求と社会課題の社内フィードバックに従事。