富士通グループ
情報セキュリティ報告書
2015

FUJITSU

shaping tomorrow with you

社会とお客様の豊かな未来のために

CONTENTS

情報セキュリティ報告書 2015

本報告書の概要

報告対象期間・範囲

本報告書は、富士通グループの2015年3月末までの情報セキュリティに関する取り組みを対象としています。

報告書の発行時期

本報告書は、2015年5月に発行しました。

富士通が考える情報セキュリティ

「快適で安心できるネットワーク社会づくり」と情報セキュリティ

富士通グループは、グループの理念・指針として「FUJITSU Way」を制定しています。
ここでは、“社会における企業の責任と役割の変化”を強く意識しており、
社会における富士通グループの存在意義を示す企業理念を以下のように定めています。

企業理念

富士通グループは、常に変革に挑戦し続け
快適で安心できるネットワーク社会づくりに貢献し
豊かで夢のある未来を世界中の人々に提供します

ICT（Information and Communication Technology）は、世界の人々をつなぎ、様々なアイデアと機会を生み出しました。その一方で、私たちはICTの急速な普及によって新たな課題にも直面しています。国境を超えて増加し続けるサイバー攻撃への備え、個人情報や機密情報などの確実な保護は、あらゆる企業や団体において早急に対応すべき事項となってきています。富士通グループでは、自社のシステム運用で培ったテクノロジーの活用を基本に、様々な関連機関と協働してこれらの問題に対応しています。

富士通グループは、誰もがICTにより最大限に可能性を引き出し、社会が持続的に成長していく世界「ヒューマンセントリック・インテリジェントソサエティ」をビジョンに掲げています。そして、ICTの力によって、持続可能な地球と社会の実現に貢献することと、デジタル社会の安心安全を維持・強化していくことをグローバルICT企業としての社会的責任と考えています。

このビジョンのもと、富士通グループはこれからのインテリジェントな社会を支えていくための様々な情報セキュリティ施策を推進しています。「FUJITSU Way」において、社員として厳守すべきことを示した行動規範として機密保持を要求すると共に、国内外共通の「富士通グループ情報セキュリティ基本方針」を定めています。この基本方針に基づいて情報セキュリティ関連規定を整備し、富士通グループ全体に適用しその遵守に努めています。

また、富士通グループでは、情報管理を徹底し、情報セキュリティの強化を図るために、統一的な情報セキュリティ管理体制を構築しています。一方で、幅広い分野にわたってビジネスを展開していることから、個々のビジネスの特性によって求められる情報管理や情報セキュリティ上の異なる課題に迅速に対応できるよう、部門単位での情報セキュリティ管理体制も合わせて敷いています。

今回お届けする「情報セキュリティ報告書 2015」は富士通グループの情報セキュリティに関する活動をご紹介するものです。是非、ご覧いただきますようお願い申し上げます。

富士通株式会社
代表取締役社長
山本 正已

富士通グループの情報セキュリティ

富士通グループではコーポレート・ガバナンス体制のもと、リスクマネジメントの一環として、グループ規定に従い適正な情報管理と情報の活用を推進しています。

» コーポレート・ガバナンスとリスクマネジメント

コーポレート・ガバナンス

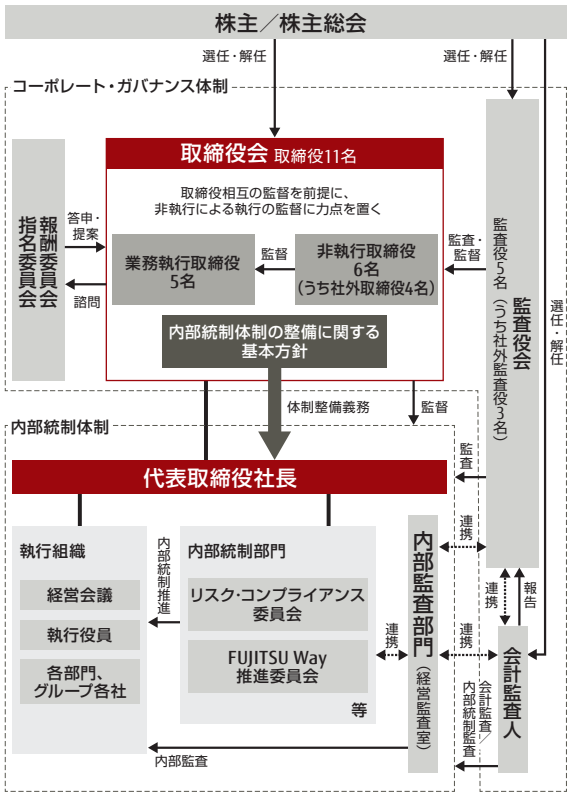
富士通のコーポレート・ガバナンスに関する基本的な考え方は、監査役設置会社制度を採用しつつ、取締役会において「非執行取締役による業務執行取締役の業務執行に対する監督と助言」に力点を置くというものです。

具体的には、取締役相互の監視と取締役会による取締役の監督を前提としつつ、執行と監督の役割分担を明確にし、業務執行を担う「業務執行取締役」に対し、業務執行の監督機能を担う「非執行取締役」を同数以上確保することで、監督の実効性を高めています。

また、非執行取締役候補者の選定にあたり、出身の属性と当社事業への見識を考慮することで、多様な視点から実効性のある助言が得られるよう配慮しています。

さらに、監査役による取締役会の外からの監査・監督と、任意に設置している指名委員会、報酬委員会により取締役会を補完することで、全体としてコーポレート・ガバナンスの整備を通じた株主価値の向上を目指します。

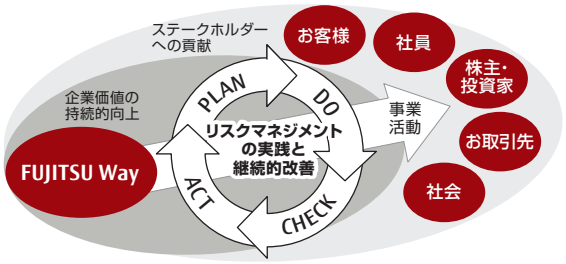
↓コーポレート・ガバナンス体制図



リスクマネジメント

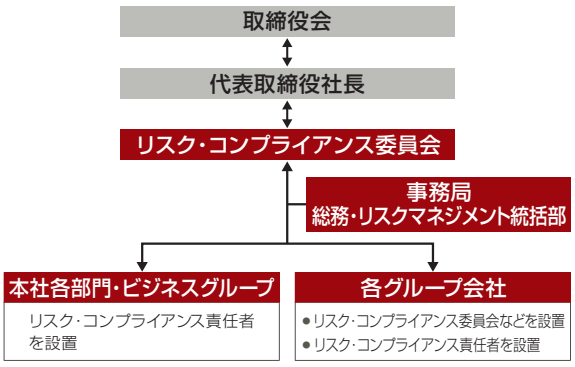
富士通グループは、グローバルなICT事業活動を通じて、企業価値を持続的に向上させ、お客様や地域社会をはじめとするすべてのステークホルダーの皆様に貢献することを目指しています。この目的の達成に影響を及ぼす様々なリスクを適切に把握し、その未然防止および発生時の影響最小化と再発防止を、経営における重要な課題と位置付けています。そのうえで、グループ全体のリスクマネジメントおよびコンプライアンスの体制を構築し、その実践を推進すると共に継続的に改善しています。

↓リスクマネジメントの実践と継続的改善



富士通グループでは、グローバルなリスクマネジメントとコンプライアンスの推進のため、経営トップ直属の内部統制部門の一委員会として、「リスク・コンプライアンス委員会」を設けています。リスク・コンプライアンス委員会は、国内外の富士通の各部門および各グループ会社にリスク・コンプライアンス責任者を配置し、相互に連携を図りながら、潜在リスクの発生予防と顕在化したリスクへの対応の両側面から、富士通グループ全体でリスクマネジメントおよびコンプライアンスを推進する体制を構築しています。

↓リスクマネジメント・コンプライアンス体制



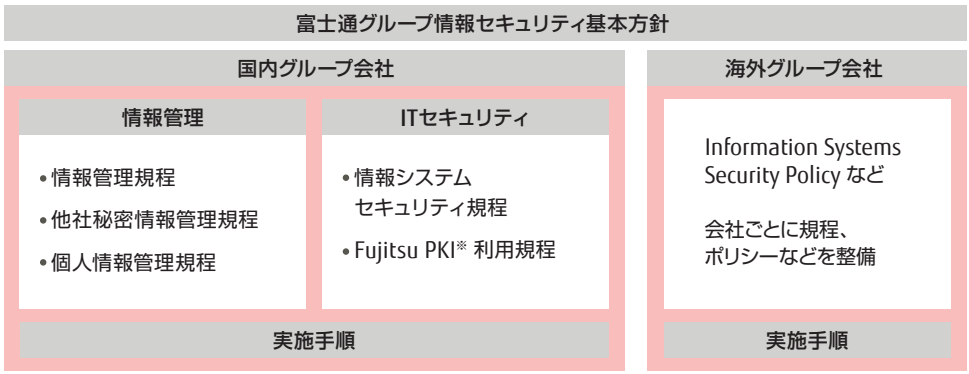
≫ 情報セキュリティの推進

情報セキュリティ基本方針と関連規定

富士通グループは、「お客様のかけがえのないパートナーとなり、お取引先と共存共栄の関係を築く」との企業指針を実現し、社会的責任の重要な側面としての「機密保持」を実践するため、国内外共通の「富士通グループ情報セキュリティ基本方針」を定め、情報セキュリティの推進に取り組んでいます。

富士通グループ各社は、情報セキュリティ関連規定体系に沿って「情報セキュリティポリシー策定指針」を使い、各国の制度・法律などを考慮しつつ、各社におけるポリシーの整合性を確保します。また「グローバル情報セキュリティ管理策フレームワーク」を用いて、情報セキュリティ対策を選択・決定・実施すると共に、評価・改善を行っています。

↓情報セキュリティ関連規定体系



〔※〕PKI：Public Key Infrastructure の略。本人認証や暗号化の仕組みの利用に関する規程。

富士通グループ 情報セキュリティ基本方針

1. 目的

富士通グループは、事業の遂行において情報が基礎となること、また、情報の取扱いにおけるリスクを深く認識し、次の事項を目的として情報セキュリティに取り組むことにより、FUJITSU Wayに示す「お客様のかけがえのないパートナーとなり、お取引先と共存共栄の関係を築く」との企業指針を実現し、社会的責任の重要な側面として、行動規範で定める「機密保持」を実践いたします。

(1) 富士通グループは、その事業において、お客様およびお取引先の個人や組織から提供を受けた情報を適切に取り扱い、当該個人および組織の権利および利益を保護します。
(2) 富士通グループは、その事業において、営業秘密、技術情報その他の価値ある情報を適切に取り扱い、富士通グループの権利および利益を保護します。
(3) 富士通グループは、その事業において、情報を適切に管理し、製品およびサービスを適時にかつ安定的に提供することによりその社会的機能を維持します。

2. 取組みの原則

富士通グループは、次の事項を情報セキュリティへの取組みの原則とします。

(1) 取り扱う情報について、機密性、完全性、可用性の維持を情報セキュリティの目的とし、これを達成するための情報セキュリティ対策を立案します。
(2) 情報セキュリティ対策を適切かつ確実に実施するため、体制と責任を明確にします。
(3) 情報セキュリティ対策を適切に実施するため、情報の取扱いに伴うリスクおよび対策のための投資を勘案します。
(4) 情報セキュリティ対策を維持するため、計画、実施、評価および改善の各段階のプロセスを整備し、情報セキュリティの水準を維持・向上させます。
(5) 情報セキュリティ対策を適切かつ確実に実施するため、役員および従業員に対し情報セキュリティに関する啓発と教育を行い、その重要性を認識させ、行動させます。

3. 富士通グループの施策

上記目的および取組みの原則に基づく情報セキュリティ対策を確実に実施するため、富士通グループは、関連規定を整備し、これを実施します。

情報セキュリティ教育の推進

情報漏えいを防ぐためには、規程類を社員に周知するだけでなく、従業員一人ひとりのセキュリティに対する意識とスキルを向上させることが重要と考えています。そこで、富士通および国内グループ会社の社員を対象とした新入社員研修や昇格・昇級時研修の際に、情報セキュリティ教育を実施すると共に、役員を含む全社員を対象としたe-Learningを毎年実施しています。

↓e-Learning画面

情報セキュリティに対する意識啓発

富士通グループでは、「情報管理徹底宣言！～情報管理は富士通グループの生命線」を共通のスローガンとして掲げています。そして、富士通および国内グループ会社の各事業所に啓発ポスターを掲示するほか、全社員の業務用パソコンにシールを貼付するなどの施策を行い、社員一人ひとりの情報セキュリティに対する意識の高揚を図っています。

また、電子メールの社外誤送信対策ツールを全社で導入するなど、ICTの活用の推進と併せて情報セキュリティに対する意識を高めています。

↓情報管理 徹底宣言のシール

お取引先に対する情報セキュリティ研修会を開催

近年のICT環境の急激な変化に伴い、これまで以上に情報漏えいリスクが高くなっていることから、富士通グループでは、グループの社員だけではなく、ソフトウェア開発・サービスを委託したお取引先に対しても情報セキュリティ研修会を開催しています。

個人情報保護体制の強化

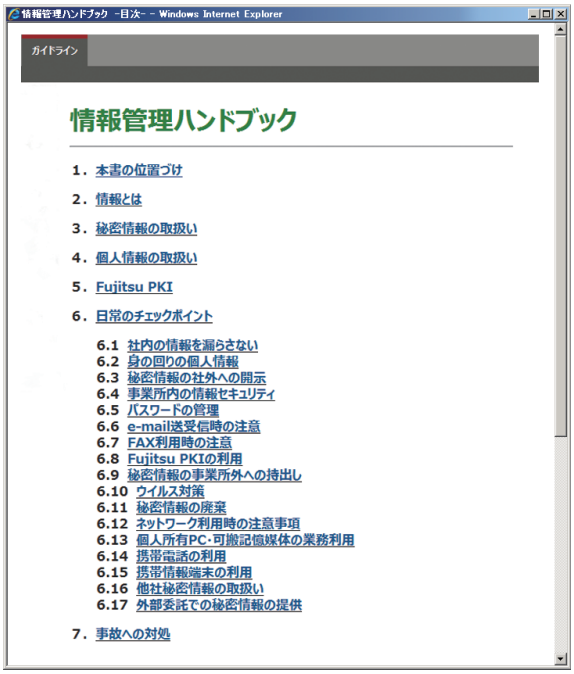
富士通では、「個人情報保護ポリシー」と「個人情報管理規程」を定めています。この規程に基づき、毎年、個人情報の取り扱いに関する教育や監査を実施するなど、継続的に個人情報保護体制の強化を図っています。

また、2007年8月に富士通全社でプライバシーマークを取得し、2年ごとに更新しています。国内グループ会社も、必要に応じて各社でプライバシーマークを取得し、個人情報管理の徹底を図っています。海外グループ会社の主な公開サイトにおいては、各国の法律や社会的な要請に応じたプライバシーポリシーを掲載しています。

その他の支援

情報管理に関する社内規定の理解を深めることを目的とした「情報管理ハンドブック」を発行しています。さらに、イントラネット上でも参照できるようになっており、情報管理に関して疑問点がある場合はすぐに確認することができるようになっています。これ以外にも、イントラネットを利用し、世の中で多発している情報漏えい事件を紹介することによる注意喚起や、毎月1回のセキュリティチェックデーを設け、幹部社員が自部門のセキュリティ対策状況を確認する活動を行っています。

↓「情報管理ハンドブック」画面



≫ 情報セキュリティ人材の育成 ―セキュリティマイスター認定制度の取り組み―

サイバー攻撃が、社会問題化しています。今後は、マイナンバー（社会保障・税番号）制度導入、さらには500億のデバイスがインターネットにつながるIoT（Internet of Things）時代をむかえ増々攻撃が高度化、巧妙化していくことが予想されます。富士通は、システムインテグレーションおよびサービス運用の最前線で、セキュリティ品質の向上を実践し、堅牢なセキュリティ品質を持つソリューションを実現する情報セキュリティ人材の育成に取り組んでいます。

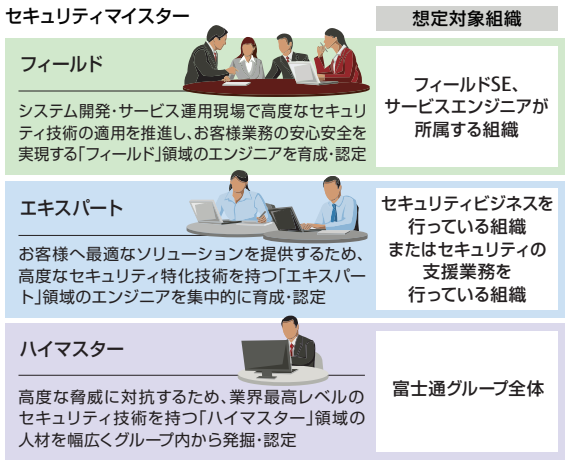
プロフェッショナルな情報セキュリティ人材育成の必要性

昨今の企業や組織を対象とした標的型攻撃による被害が深刻化するなど、サイバー攻撃に関する脅威が多様化・高度化しています。そこで、富士通では、これらの脅威からお客様の情報資産を守る取り組みの一つとして、高いレベルのセキュリティ技術を持つ技術者をグループ内から発掘、認定し、フィールドに配置する仕組みをつくりました。

セキュリティマイスター認定制度

サイバー攻撃から情報システムを守るセキュリティを実践できるスペシャリストを「セキュリティマイスター」という位置付けで、系統的、計画的、継続的に育成し、認定していきます。この制度は、活動領域により「フィールド」、「エキスパート」、「ハイマスター」の3つの領域で区分し定義しています。2016年度末までに700名の技術者の育成・認定を計画しています。

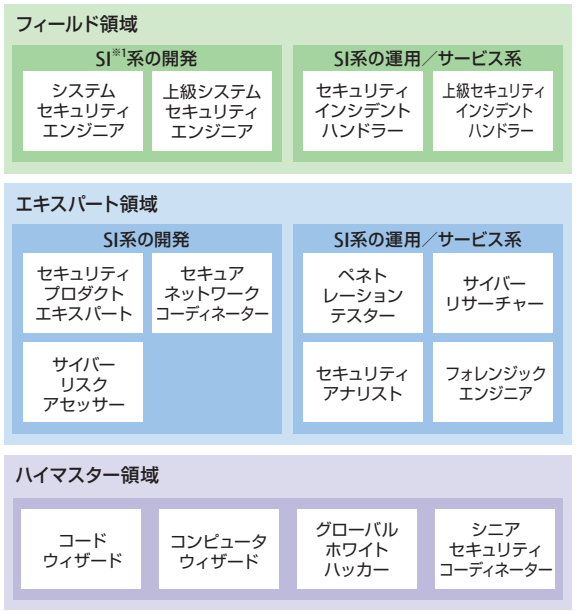
セキュリティマイスターの３つの領域



セキュリティ技術者の人材像を明確化

「セキュリティマイスター認定制度」では、今日のICT開発・ICT運用の現場ニーズに適合したセキュリティ技術者の人材像を定義しています。人材像モデルはICT開発・ICT運用の各場面で求められるセキュリティ技術を、次の3領域15種類の人材像モデルとして具体化しています。

セキュリティ技術者の人材像モデル



具体化にあたっては、日本のITスキル標準、海外の各種セキュリティ技術者人材モデルとの整合性を考慮しています。さらに、ホワイトハットハッカー※2やトップガン人材※3に相当する「ハイマスター」人材像も定義しました。

〔※1〕SI：システムインテグレーション
〔※2〕ホワイトハットハッカー（white hat hacker）：善玉ハッカーのこと。
〔※3〕トップガン（Top Gun）人材：先鋭的な技術者のこと。

以下に定義の例を示します。フィールド領域の「システムセキュリティエンジニア」は、システム開発部門に籍を置き、現場のセキュリティ設計と、技術的なセキュリティ対策の実施を担当する位置付けとしています。

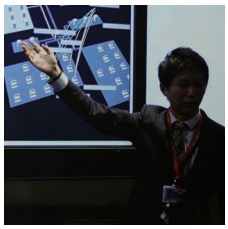
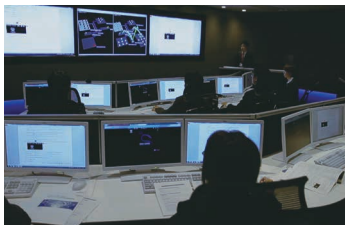
「セキュリティインシデントハンドラー」は、システム運用部門に籍を置き、システムのセキュリティ運用設計と、現場で発生した情報セキュリティインシデントに関してのセキュリティ対策の実施などを担当します。

ハイマスター領域の「コンピュータウィザード」は、組み込み系など開発部門に籍を置き、技術力を活かして独自の研究・情報発信活動を行う人材です。セキュリティにおける最先端の技術を体現する人材と位置付け、自ら積極的にモチベーションをもって、外部団体の活動（研究活動および国内の技術者向けセキュリティセミナーなど）へ参加し、発表を行うことを期待しています。

育成プログラムの整備

実践力を重視したセキュリティ技術者育成プログラムの整備の一環として、人材モデルの類型ごとの専門教育コースを開設しています。また、サイバーレンジ（仮想演習場）を採用した技術者育成教育を新規に開発しました。この技術者育成教育は、広くお客様にもご利用いただける教育コースとして、ご提供しています。

育成教育の風景

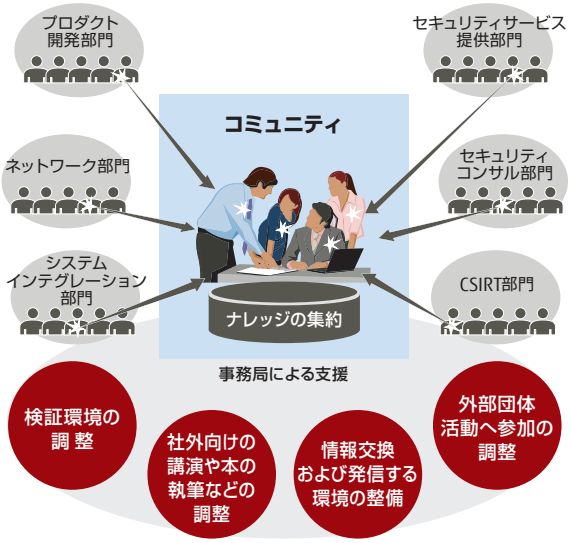
セキュリティ人材の発掘と人口拡大

セキュリティ人材の発掘とセキュリティ技術者人口の拡大を促進しています。社内の各部門に点在しているナレッジの集約化を図り、有効活用するためのセキュリティマイスター・コミュニティを形成しています。このコミュニティでは、有識者同士のナレッジ共有により、認定後のスキル向上にもつながっています。

さらに、ハッキング技術を含むセキュリティコンテストを社内で開催しています。セキュリティコンテストでもサイバーレンジを活用し、同時に40名が技術力を競い合うことが可能です。

このように、富士通では、積極的なセキュリティ人材育成によって、お客様に安心安全をご提供していきます。

セキュリティマイスター・コミュニティ



富士通初のセキュリティコンテストを開催

富士通グループセキュリティ人材の技術力向上、人材交流の一環として、2014年12月に「富士通サイバーセキュリティワークショップ2014」を開催しました（160名参加）。

午前のセミナーは、経営層、幹部社員、現場エンジニアがそれぞれの視点から最前線のサイバーセキュリティをテーマに、二つの会場でセミナーを実施しました。

午後は、富士通グループで初となるハッキング技術やセキュリティ知識を競う「セキュリティコンテスト」が行われ、20組40名の技術者が参加しました。

セキュリティコンテストでは、通常のCTF（Capture The Flag）大会とは異なり、様々な工夫を行いました。

まず、約70問の問題は全て運営事務局が、高度なセキュリティスキルを有する「ハイマスター」の協力を得て独自に作成しました。Webサーバやネットワーク上のパケットデータのどこに答え（Flag）があるのかなどを問う実践的なセキュリティ技術が求められる問題に加え、セキュリティの幅広い知識を問うクイズ問題を出題しました。

また、巧みな話術や覗き見などにより攻撃ターゲットから必要な情報を入手する「ソーシャルハッキング」技術を競う問題も用意しました。

さらに、コンテスト用に構築されたダッシュボードにより競技の模様を可視化することによって、出場者の腕試しだけに留まらず、同時並行で別室の見学者向けにコンテスト中の問題解説をライブで行い、参加者全員のセキュリティ技術向上を狙いました。

参加者からは、「実際に手を動かすことが少なくなっているので、出場者として参加できて良かった」、「自分の実力が分かった」、「問題のアーカイブが欲しい」、「部門間対戦をやりたい」、「Write-up（問題の解説）サイトを開設して欲しい」などの感想やコメントが出ていました。

これからも、富士通グループのセキュリティ人材の技術力向上、人材交流の一環として、コンテストを継続的に開催していきます。

セキュリティコンテストの風景

ITセキュリティへの取り組み

ICTを活用する場面では、業務に関する大量の情報を集積してこれを容易に扱える状態に置くことになり、情報の漏えい、毀損、利用不能その他の様々な脅威が伴います。
このため、富士通グループでは、グループ全体の共通課題としてICTの活用において情報の安全管理を確保するITセキュリティに取り組んでいます。

業務を支援するITセキュリティの追求

富士通グループでは、ITセキュリティは、業務の利便性や効率を妨げるものとせず、むしろ、業務を支援するものとすることを目指しています。
情報セキュリティ対策のために規制を過剰なものにすると、従業員にとって規則の理解や遵守が負担になり、ともすると現実には守れないものになりかねません。
富士通グループのITセキュリティでは、対策をできる限り業務環境や業務手順に組み込んで実現します。こうして、従業員が本来の業務に専念できるようにすることが重要だと考えています。

また、ICTの進歩と共に脅威も変容する中で有効な対策を維持するためには、技術的な対策を開発・実装し、問題を解析して対応するための先端技術が必要であると考え、ITセキュリティのための専門の部署を置いています。
加えて、開発・実装された技術的な対策は、お客様に提供する前に自ら実践し、その効果や実用性の確認も行い、製品※にフィードバックを行っております。
〔※〕製品：FENICSⅡユニバーサルコネクトサービスなど

ITセキュリティの枠組み

富士通グループにおけるITセキュリティの施策は、ITセキュリティ関連規定に基づいて実施しています。情報を取り扱う場面に応じた施策に「業務システムにおける情報管理」、「クライアントセキュリティ統制」、「利用者の一元管理を実現する認証システム」と「ネットワークセキュリティ統制」があり「資産管理」がこれらの基礎になります。また、「ITセキュリティ監査」を行い、施策の定着と改善を進めています。

ITセキュリティの枠組み

ITセキュリティ関連規定			
●場面の設定　●役割と責任　●PDCAサイクルの確立			
業務システムにおける情報管理	**クライアントセキュリティ統制**	**利用者の一元管理を実現する認証システム**	**ネットワークセキュリティ統制**
業務・情報・利用者の分析に基づく ●アクセス制御機能 ●信頼性維持機能	●対策の自動化 ●電子メール誤送信対策 ●社内標準パソコン	セキュリティカードによる ●入室管理 ●認証 ●文書の決裁	●ネットワークの統制 ●電子メールの統制 ●ネットワークサービス利用の統制
ITセキュリティの基礎となる資産管理			
●財産としての現物管理　●セキュリティ対策管理　●ライセンス管理			
ITセキュリティ監査			
●実施状況の確認			

ITセキュリティ関連規定

富士通グループのITセキュリティ関連規定は、1.～3.に示す3つの特長があります。

1. 場面の設定

ICT活用の主要な場面には、次のものがあります。ITセキュリティ関連規定では、それぞれの場面において実施すべきITセキュリティ対策を定めています。

- ●サーバを中心に業務情報を蓄積し取り扱う業務システム
- ●パソコンなどを活用する事務所その他の職場
- ●職場をつなぐ事業所内や事業所間のネットワーク

2. 役割と責任

ITセキュリティ対策の実施について役割と責任を定め、業務システムや職場ごとに、ITセキュリティ対策の実施に責任を負う者を指名させます。また、対策の実施を統制する部門の権限を定めています。

3. PDCAサイクルの確立

ITセキュリティ対策の実施、啓発と教育、周知、事故への対応、評価と改善を含む、PDCAサイクルを構成するそれぞれの要素について規定し、施策の定着と改善を図っています。

業務システムにおける情報管理

富士通グループでは財務・経理、人事・総務、営業、購買、SE業務、生産・物流、製品開発管理をはじめとする様々な業務にICTを活用しています。そこに保有し、取り扱う様々な情報について、業務や職責に応じたセキュリティ要件があります。この要件を分析し、利用者の立場や資格に応じて情報へのアクセスを制御するアクセス制御機能や、業務の重要性や継続性要件を満たす信頼性維持機能を装備し、運用しています。

クライアントセキュリティ統制

情報セキュリティの重要な課題は、ヒューマンエラーへの対策です。ICTを活用する人の行為において、注意力に頼るだけでは情報セキュリティ事故は防ぎきれません。対策として教育を充実し、啓発活動により注意を喚起することは当然ですが、それでもなお、情報漏えいその他の事故がICTでの対策の及ばないところで発生します。

この事実を踏まえて、人の行為が係わるクライアントの業務プロセスに着目し、注意力に依存する対策をICTによる対策に置き換えることの可能性を検討し、具体化してきました。

■パソコンにおける対策の自動化

パソコンにおいては、OSやアプリケーションのセキュリティ修正の適用とウイルス定義ファイルの更新を自動化しています。

■電子メール誤送信対策

電子メールは、宛先や添付ファイルを間違うと容易に情報が漏えいしてしまいます。そこで、電子メールの宛先を自動的に識別して、外部への送信について送信者に再確認の操作をさせるなどにより、誤送信を削減しています。

■富士通標準パソコンの導入

富士通標準パソコンとは、社内利用向けに標準に定めた機種と仕様のパソコンです。暗号化ハードディスクの使用、BIOSパスワードおよびスクリーンセーバーの設定、資産管理ソフトウェアおよびウイルス対策ソフトウェアの搭載などのセキュリティ対策済のものを配布します。これにより、利用者を各種セキュリティ対策の実施から解放し、対策の確実な実施を実現します。加えて、パソコンの選定・導入・運用を定型化し、費用の削減をおこないます。

■クライアント機器の社外での安全な使用

パソコンやスマートフォンなどのクライアント機器は、自宅や出張先などの社外でも業務に使います。このとき、機器の盗難・紛失の恐れや、機器からの情報流出の恐れがあるため、機器のセキュリティ対策実施状況を確認するセキュリティチェックデー（毎月実施）や、注意事項を周知徹底するための情報セキュリティ教育（年一回実施）を行っています。

また、ICTによる技術的な施策として、情報を持ち出さず社外でクライアント機能を活用できる「仮想デスクトップサービス」やモバイル機器で利用できる「専用アプリケーション」を導入し、重要な情報の保護に活用しています。

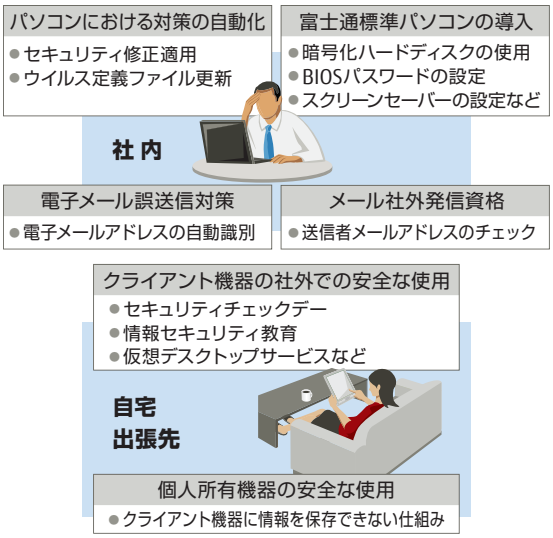
■個人所有機器（パソコン、スマートフォンなど）の安全な使用

個人が所有するパソコンやスマートフォンなどを使用して電子メールや社内の業務システムを安全に利用するために、「仮想デスクトップサービス」や「FENICSⅡユニバーサルコネクト」を活用しています。これらのサービスでは、利用者の不注意による秘密情報の保存・漏えいを回避するため、クライアント機器に情報を保存できない仕組みにしています。私的な情報と社内のネットワークへの接続は機器の中で隔離され、業務情報の安全な管理が確保されています。

■社外への電子メール発信の管理

電子メールを社外に発信する資格の有無を確認します。これにより、業務上不要な利用者による社外へのメール発信・情報漏えいを防止します。

↓クライアントセキュリティ統制



ITセキュリティの基礎となる資産管理

サーバ、パソコンなどに関する資産を管理するIT資産管理は、財産管理の役割だけでなく、ICT活用やITセキュリティの基礎になります。富士通グループでは、「ITリソース管理システム」と呼ぶ業務システムでIT資産管理を行っています。

ITリソース管理システムには、以下の情報を保有しています。

■ハードウェア資産：サーバ、パソコンの機種、仕様

■ソフトウェア資産：サーバ、パソコンごとに使用しているソフトウェアとその版数

■セキュリティ修正の適用状況

ソフトウェアとその版数を管理することにより、ライセンス契約に合致したソフトウェアの導入を自動化しています。また、ソフトウェア資産やセキュリティ修正適用の進捗状況を管理者が把握し、対処を指示します。

このITリソース管理システムは、統合運用管理ソフトウェアSystemwalkerのセキュリティ管理製品であるSystemwalker Desktop Patrolで構築し、IT資産とセキュリティの状態や、ソフトウェアライセンスを一元的に管理しています。

利用者の一元管理を実現する認証システム

富士通グループでは、従業員の認証その他の用途に「セキュリティカード」と呼ぶICカードを導入しています。

セキュリティカードの表面には氏名と顔写真を印刷しています。また、ICチップには氏名、従業員番号、従業員のPKI（Public Key Infrastructure）証明書と鍵を格納しています。これらの情報は、富士通グループ内で一元的に管理されたその従業員に固有の情報です。

セキュリティカードは、人事部門の管理の下で、従業員の入社時に交付し退社時に返却させるため、その使用者が正当な従業員であることが保証されています。また、紛失時には失効させて、悪用を防ぎます。

セキュリティカードの主な用途は次のとおりです。

入室管理

富士通グループの事業所では、建屋や事務所の入口にセキュリティドアを設置しており、出社した従業員は、セキュリティカードを使って入室します。

認証

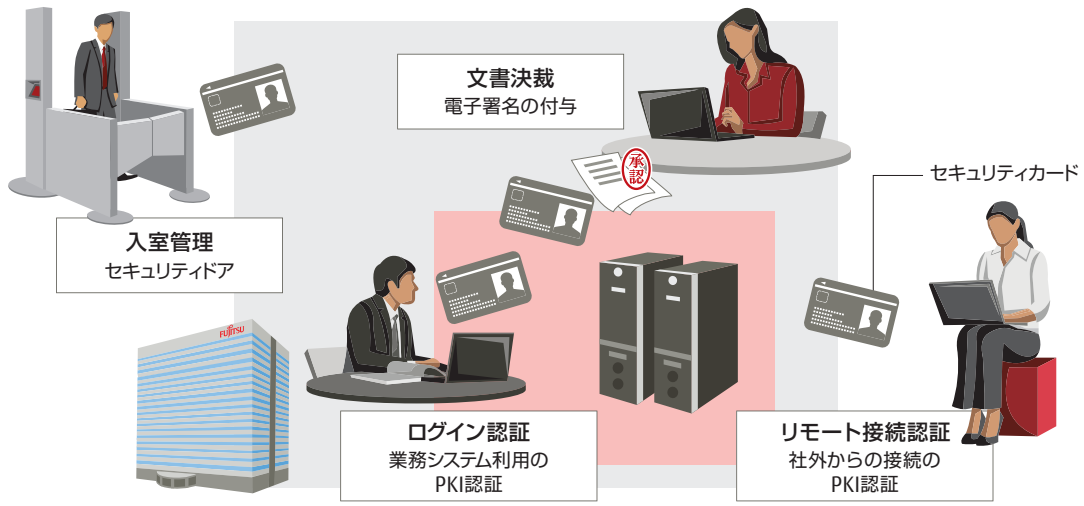
業務システムの利用にセキュリティカードが必要です。業務システムへのログインでPKIによる認証を行っているため、従業員の識別と認証が確実に行われ、しかも操作は容易です。

業務システムを出張先など社外から利用することもできます。その場合には、リモート接続についてPKIによる認証を行い、確実な本人確認を行います。

文書決裁

セキュリティカードは、電子文書の決裁にも利用します。決裁者は、PKI機能を利用して、電子文書に電子署名を付与します。これは、決裁者本人がその文書を確認して決裁したことを示す点で、紙の文書への決裁印の押印と同じ効果があります。

↓セキュリティカードの利用



ネットワークセキュリティ統制

インターネットは、業務連絡手段として、また、広報・情報提供の手段として、あるいは外部の膨大な情報の活用手段として業務に欠かせません。その反面、インターネットのオープン性や仕組みに由来する深刻な脅威も無視できません。富士通グループでは、先端技術を持つ専門の部署が脅威への対策にあたると共に、全世界でインターネットの出入り口を統合管理し、従業員の負担を最小限に留めて安全を確保しています。

ネットワークの統制

ネットワークに関して、以下の対策を行っています。

■インターネット接続およびイントラネット構築・運用の統制
- ●専門の部署によるファイアウォールなどのゲートウェイシステムの設置・運用
- ●部門が行う接続の審査・許認可

■運用時のセキュリティ維持
- ●不正アクセス対策（サーバの設定、機器管理状況の確認、不正通信の監視・阻止）
- ●安定稼動のための性能管理、信頼性設計

■モバイル機器への対応
- ●パソコンやスマートデバイス※を使って、社外からイントラネットへ接続して安全に業務を行う環境の整備と運用

〔※〕スマートデバイス：スマートフォンやタブレット端末のこと。

■変容する脅威への対応
- ●標的型メール攻撃やAPT（Advanced Persistent Threat）などの従来の対策手法では対応が困難な新たな脅威について、その動向分析・情報収集および対策
- ●攻撃手法と対応の研究
- ●利用者への啓発・教育活動

電子メールの統制

電子メールは、現在の業務遂行に無くてはならないものとなっています。その安全管理のために、以下の対策を行っています。

■ 電子メールの統制
- 専門の部署による電子メールサーバの設置・運用

■ 運用時のセキュリティ維持
- ウイルス対策
- 迷惑メール対策
- 安定稼動のための性能管理、信頼性設計

ネットワークサービス利用の統制

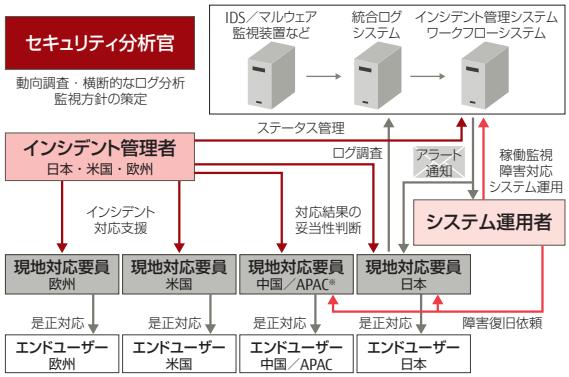
社外のインターネット環境にはファイル転送やオンライン会議などの様々なネットワークサービスがあります。これらについて、業務上の利便性や必要性と、クライアントセキュリティ統制が向上した現状を勘案して、制限を設けながら利用を認めています。他方では、情報漏えいにつながる恐れのある特定のネットワークサービスは、利用を禁止しています。また、誤使用を防止するために、このような通信を常時監視しています。

イントラネット利用の統制

富士通グループ全体で、「富士通グループ情報セキュリティ基本方針」を基礎とするグローバルな統制の重要な要素として、イントラネット利用の統制を行っています。その情報セキュリティ対策は、国や地域によらず共通の水準を達成し、維持する必要があります。このため、世界中のグループ会社におけるイントラネットの構築や利用におけるセキュリティ対策を、共通のポリシーおよび管理施策に基づき統制します。

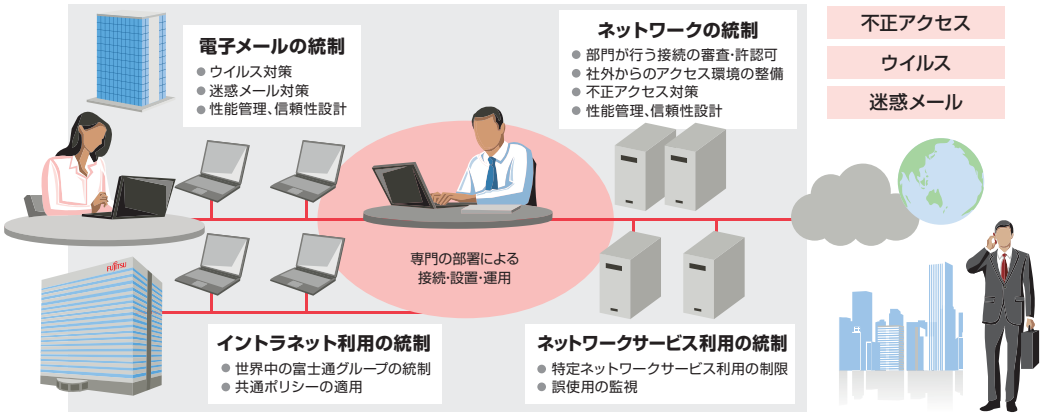
グローバルに一つのイントラネットを持っていることに対応して、ネットワークのインシデント対応も、専門組織であるSOC（Security Operation Center）によるグローバルな統制の下で行っています。一日に世界中のグループ会社で検知されるネットワークのアラートは、数億件にのぼります。これらのリスクレベルを判定し、インシデントとして扱う事象を特定し、これに迅速に対応します。その特徴は、次のとおりです。
- グローバルに統一したリスク基準と対応プロセス
- 大量の事象およびログの自動での判定
- 各地域に配置したSOC要員による、時差を活用した24時間の対応
- インシデント管理者やシステム運用者の連携を支援するワークフローシステムによる対応時間の短縮
- 専門のセキュリティ分析官による脅威状況の把握と新規施策の立案

ネットワークのインシデント対応　－SOC－



〔※〕APAC：Asia-Pacific

ネットワークセキュリティ統制



ITセキュリティ監査

これらのITセキュリティ施策を対象に、被監査部門である実施部門から独立した監査部門が監査の年度計画を策定し、これを実行しています。監査は、その対象に適した方法で行います。監査人が現場に出向いて機器の管理状態や設定を目視で確認する方法、実施部門による点検の結果を査閲する方法、ネットワークを通して技術的に脆弱性を検査する方法などがあります。被監査部門は、監査結果を活用してITセキュリティ対策の実施を改善します。

お客様の情報資産を守るための富士通グループの取り組み

富士通グループのシステムインテグレーション・サービスを提供する組織とグループ会社は、お客様の情報資産や個人情報を取り扱う機会が多いため、富士通グループ内でもより高いレベルの情報管理が求められています。そこで、情報セキュリティ施策推進会議事務局は、情報セキュリティマネジメントの礎となるセキュリティマネジメントフレームワークを関係組織とグループ会社に提供しています。組織・グループ会社ではセキュリティマネジメントフレームワークを適用し、施策推進に取り組んでいます。

情報セキュリティ推進組織設立の考え方

昨今、高度化、多様化するサイバー攻撃の脅威、グローバルにおける各種ビジネス規制が課題となっています。その対策・対応方針を検討するために、富士通は、2013年にサイバーセキュリティに関する情報共有、当社ビジネス方針の討議を行う目的で「セキュリティ委員会」を発足させました。

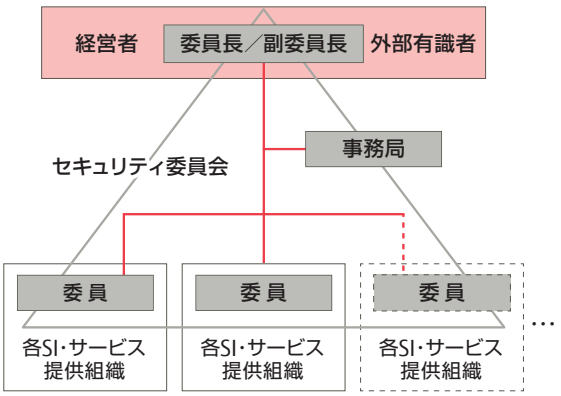
セキュリティ委員会は次のメンバーで構成しています。システムインテグレーション・サービスビジネス各事業を統轄する役員、国内営業・マーケティング・海外ビジネス各部門を担当する役員、第三者性確保のために招へいした外部有識者です。

富士通は、「Fujitsu Technology and Service Vision」を理念として掲げています。ヒューマンセントリック・インテリジェントソサエティでは情報の信頼性が重要であり、情報の利活用を続けられる仕組みづくり、事故を前提とした備えを必須としています。サイバーテロの脅威と対策、各国クラウドセンターが遵守すべき法、個人情報の取り扱いなど、グローバルレベルで対応が必要な案件をセキュリティ委員会で方針を討議し、承認しています。

セキュリティ委員会では、当社のシステムインテグレーションおよびサービスのセキュリティ品質向上活動をうたっています。セキュリティ委員会の下部組織である情報セキュリティ施策推進会議（以下、推進会議と略す）にて社内のセキュリティ活動の方向付けを行い、情報セキュリティ施策推進会議参加組織（以下、参加組織と略す）へ展開しています。

そのほかに、富士通グループ全体のシステムインテグレーションおよびサービスのセキュリティ人材育成を推進しています。

セキュリティ委員会体制

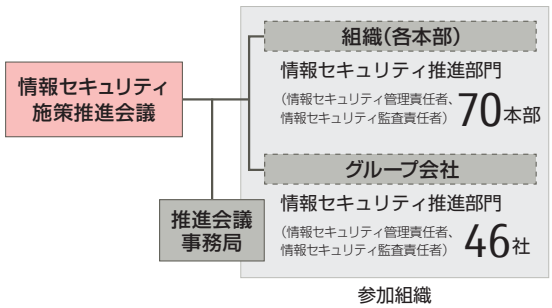


セキュリティガバナンスの構築・実践

近年ますます企業・団体への標的型攻撃、ウェブサイト攻撃、個人情報の漏えいなど情報セキュリティの脅威が増加しており、経営の観点でリスクマネジメントが求められています。富士通は、情報セキュリティガバナンスの下、情報セキュリティ活動を推進しています。

システムインテグレーション・サービスを提供する組織とグループ会社は推進会議に参加しています。セキュリティマネジメントフレームワーク（SMF：詳細は次ページ参照）を基礎として、セキュリティ計画の立案、セキュリティ対策の導入、参加組織で情報セキュリティ活動の推進、内部監査などを推進しています。また、日々の情報セキュリティ活動状況やセキュリティ事件・事故の状況を確認・評価して、マネジメントの仕組み、セキュリティ対策の改善に取り組んでいます。

情報セキュリティ施策推進会議体制



情報セキュリティマネジメント推進体制

参加組織は、お客様の情報資産、秘密情報を取り扱っています。そこで、お客様の情報を含めた情報を適切に保護することを目的として、推進会議は「情報セキュリティ施策推進会議　活動方針」を定めました。この活動方針に基づいて、参加組織は情報セキュリティの維持・推進を図っています。参加組織の情報セキュリティ管理責任者、情報セキュリティ監査責任者は、四半期ごとに開催される推進会議の会議体に参加し、セキュリティ施策にかかわる情報交換・意見交換の場としています。参加組織の長は、責任者として情報セキュリティマネジメントを推進しています。

情報セキュリティ施策推進会議事務局（以下、推進会議事務局と略す）は、参加組織に対して、効果的なセキュリティ対策の支援、改善策の助言などを必要に応じて行い、情報提供・サービス提供をしています。これにより、参加組織は情報セキュリティ活動を継続的に推進しています。

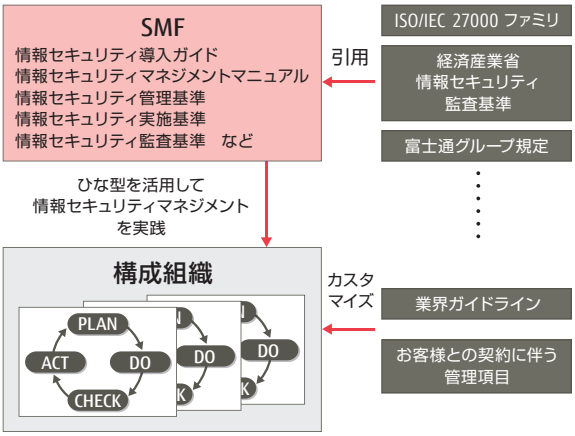
一方、参加組織は、推進会議から要求される情報セキュリティ活動を推進することで、組織としての情報セキュリティのレベルを維持しています。

SMF（セキュリティマネジメントフレームワーク）

参加組織が情報セキュリティマネジメントを実践するために、推進会議事務局はSMFのひな型を提供しています。SMFは、富士通グループ規定を基準とし、ISO/IEC 27000ファミリ、経済産業省の情報セキュリティ監査基準など国内外の基準を取り入れています。SMFは、情報セキュリティ管理系と情報セキュリティ監査系の文書で構成されています。参加組織は、お客様の業界ガイドライン、お客様との契約に関わる管理項目などのセキュリティ要求事項を満たす必要があります。このため参加組織は、SMFひな型を基に情報セキュリティ関連文書を規定し、運用を行います。

SMFと富士通グループ規定類、国際標準、業界ガイドラインなどとの関係を右図に示します。

SMFと富士通グループ規定・国際標準・業界ガイドラインなどとの関係



セキュリティ向上への取り組み

人材教育

参加組織の情報セキュリティの推進・管理を行う情報セキュリティ管理責任者や情報セキュリティ推進者を対象として「情報セキュリティ管理者教育」を開講しています。2012年度から、管理責任者を対象に継続的な自己研鑽促進のため、e-Learning教育を開講しています。内部監査人向けの教育として、「情報セキュリティ監査人教育」を開講しています。

施策推進会議では、内部監査の質向上と監査人のキャリアパスを目的として、日本セキュリティ監査協会（JASA）が認定する監査人資格の取得を積極的に推進しています。2014年度までに141名が認定を受けて、内部・外部監査で活躍しています。

そのほかに、情報セキュリティ教育の教材を提供し、各組織で活用されています。

教育受講者数

教育コース名	受講者数
情報セキュリティ管理者教育（集合形式）	648名
情報セキュリティ管理者教育（e-Learning版）	652名
情報セキュリティ監査人教育	1,252名

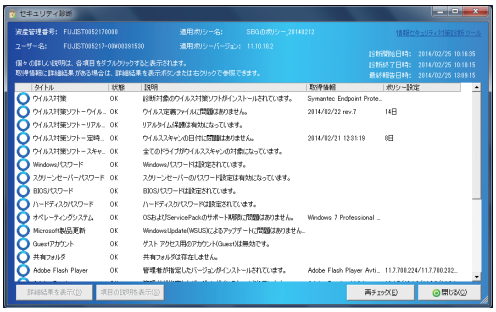
定期的なセキュリティチェック活動

富士通グループでは毎月「セキュリティチェックデー」活動を行っています。この施策で、パソコンやスマートデバイスのセキュリティ設定や可搬記憶媒体の管理状態の確認を行っています。推進会議では情報セキュリティ対策診断ツール（IT Policy N@vi）をパソコンに導入することを義務付けて、各パソコンのセキュリティ対策・運用状態を診断しています。このツールは、パソコン起動時に診断項目※を自動的に診断し、診断結果をパソコン画面に表示します。各組織の情報セキュリティ管理責任者は、すべてのパソコンについて診断結果を容易に確認し、セキュリティ対策の浸透を維持しています。

スマートデバイスについては、社内規程に準拠したセキュリティチェックシートを提供し、各参加組織で活用しています。

〔※〕診断項目：OS、ウイルス関連、パスワード関連、暗号化、設定禁止事項など19項目があります。

情報セキュリティ対策診断の結果の画面



情報セキュリティ監査

推進会議では、情報セキュリティ監査として内部監査と外部監査を実施しています。内部監査は、参加組織が自組織を対象に実施する監査です。外部監査は、推進会議事務局が第三者の観点で実施する監査を意味します。

参加組織は定期的に内部監査・外部監査を受けることで、情報セキュリティマネジメントの浸透・定着度と情報セキュリティ対策の運用状況・定着度を確認し、改善の指針としています。

外部監査は推進会議事務局が毎年テーマを定めて、監査計画を立案しています。監査チームは、推進会議事務局を中心としたJASA監査人資格を保有する監査人で構成します。この監査チームが、情報セキュリティのマネジメント推進状況を確認し、不備事項の指摘や、改善事項の提案など行い、参加組織全体のセキュリティ維持・向上を図っています。また、被監査組織の優れた施策を推進会議会議体で事例として紹介し、参加組織全体のセキュリティレベルの底上げに活用しています。

そのほか、参加組織から個別の要望、業務上の必要性に応えるために、推進会議事務局の専門家が特定プロジェクトや組織・グループ会社を対象とした特別監査を実施しています。

ソーシャルメディア教育

昨今、情報通信手段としてSNS※が私たちの生活に浸透しています。一方で、業務利用、私的利用問わずに、利用機会の増加に伴い、企業責任が問われる事案が発生しています。

そこで、富士通では、ソーシャルメディアを利用する場合のルールとマナーをガイドラインとして定めています。これに基づき、推進会議事務局は、参加組織向けに「情報セキュリティ実践講座（ソーシャルメディア利用編）」を作成し、提供しています。

SNSを利用するリスクについて事例を通して解説し、SNSの正しい利活用のために啓発を行っています。

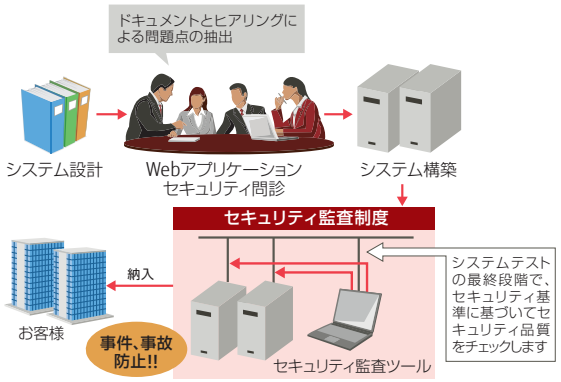
〔※〕SNS：Social Networking Service

お客様納入システムのセキュリティ監査

富士通グループでは、お客様に納入するインターネット接続システム（お客様納入システム）が満たすべきセキュリティ基準を定めています。

また、お客様納入システムを納入する前に、品質検査の一環としてセキュリティ監査を受けることが義務付けられており、セキュリティ基準を満たしていることをセキュリティ専門の部署が客観的な観点で確認しています。

お客様納入システムのセキュリティ監査



お客様納入システムのセキュリティ監査は、インフラ（OS・ミドルウェア）部分の「インフラ納入前セキュリティ監査制度」とWebアプリケーション部分の「Webアプリケーションセキュリティ監査制度」に分けて運用しています。

特にWebアプリケーションセキュリティ監査では、セキュリティに関する問題点を早期に抽出し、解決するため、システム構築の設計段階でセキュリティ問診を実施しています。

これにより、お客様納入システムが、富士通グループで定めた均質のセキュリティレベルを確保されていることを確認し、外部からの不正アクセスによるセキュリティ事故防止に貢献しています。お客様納入システムのセキュリティ監査の運用開始後、システム構築におけるセキュリティ対策の不備に起因する事故が激減していることを確認しています。

クラウドをはじめとするサービスにおける セキュリティ品質向上への取り組み

クラウドサービスをはじめとしたお客様に提供するサービスを安心安全にご利用いただくために、サービスプロバイダーは、常に変化するセキュリティ脅威に対応していく必要があります。富士通は、サービスプロバイダーとして実施すべきセキュリティ対応事項を明確化し、ガイドラインや対策基準を策定し監査しています。また、インシデントの対応を専門に実施する組織の整備、第三者評価、および情報公開にも取り組んでいます。

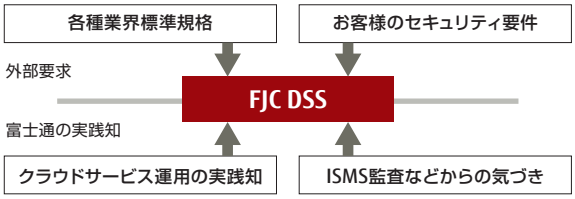
クラウドサービスへの対策基準による取り組み

日本国内のデータセンターにおいて稼働するクラウドサービスが増加するに従い、セキュリティ面の不安やレイテンシ（遅延）問題は低減され、コスト削減・可視化、業務継続性の期待により、パブリッククラウドを第一の選択肢とする「クラウドファースト」の時代が到来しています。

経済産業省、CSA、ENISA などの様々な団体がクラウドセキュリティガイドラインを公開しています。また、その経済産業省のガイドラインをベースとして、2015年度にISO/IEC27017がクラウドセキュリティの国際標準化される見込みです。しかしこれらのガイドラインにおける要求事項は、クラウドサービスを活用する側が、どのセキュリティ強度の対策をとるか自由に選択できるようになっているため、クラウドサービス提供者ごとに対応レベルのばらつきが出てしまいます。

そこで富士通では、これらの外部セキュリティ要求事項と、お客様のセキュリティ要件、さらに、富士通社内の実践知から独自のセキュリティ基準である「富士通クラウドデータセキュリティスタンダード」（FJC DSS※）を策定し、2015年度中にサービス提供を開始する予定の“次世代クラウド基盤”も含めて実践していきます。これにより、富士通が提供するクラウドサービスがばらつきなく、一定のセキュリティ品質を満たしているかを明らかにすることが可能となります。

FJC DSSの策定方針



〔※〕FJC DSS : Fujitsu Cloud Data Security Standard

ガイドラインや監査による取り組み

富士通では、お客様に提供するサービスのセキュリティ品質を確保するため、サービス開発工程とサービス運用工程で実施すべき事項を「サービスセキュリティ対応ガイドライン」としてまとめています。

各サービスを提供する部門は、このガイドラインで示した内容に基づき、セキュリティ対策を実践します。サービス開始の前には、監査部門がセキュリティ対策の実施状況を監査し、セキュリティ品質確保を担保しています。

サービス運用時には、監査部門によるセキュリティ定期監査を実施します。必要に応じて是正対応を行うことで、セキュリティ品質の確保と向上を継続的に実現しています。

富士通クラウドCERTの取り組み

クラウドをはじめとするサービスのセキュリティを専門的に扱う「富士通クラウドCERT（Computer Emergency Response Team）」は、クラウド環境を各種のセキュリティ脅威から守り、お客様のビジネスを支えるために、グローバル規模で以下のような活動を行っています。

1. 情報セキュリティ運用

お客様に安心して富士通のクラウドサービスを利用していただくために、外部からの様々な攻撃を水際で検知するモニタリングなどのセキュリティ対策を実施し、24時間365日体制で運用しています。

2. 緊急対応

インシデント発生時のプロセスを定め、万が一のインシデント発生時には、事象の識別・解決・被害局所化を迅速かつ確実に実施します。

3. 情報セキュリティマネジメント

お客様の大切な情報を守るために、富士通クラウドサービスにおける「人」、「モノ」、「情報」を適切にマネジメントします。さらに、日本シーサート協議会、FIRST※などのセキュリティ関連団体に加盟し、グローバルなクラウドセキュリティの向上のために活動しています。

〔※〕FIRST : Forum of Incident Response and Security Teams

富士通クラウドCERTの活動

製品のセキュリティ

富士通の製品開発部門でのセキュリティ向上への取り組みの中から、オープンソースソフトウェアの脆弱性対応と人材育成に関する活動をご紹介します。

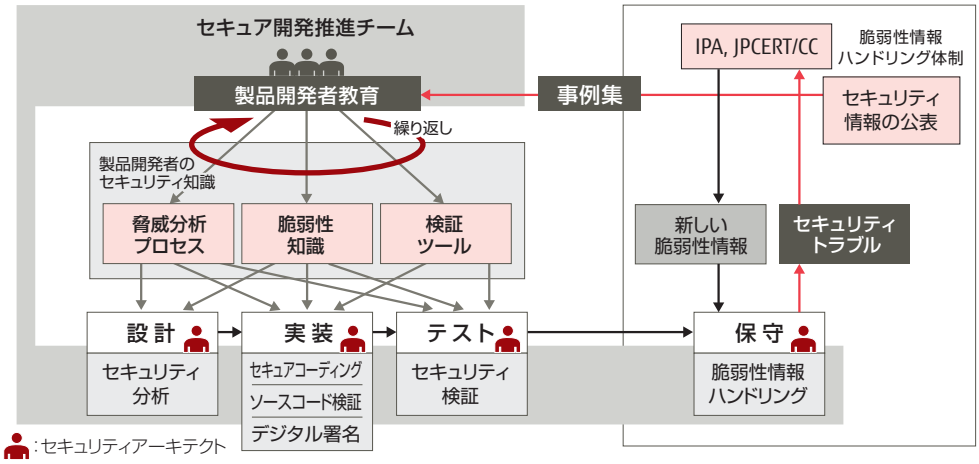
≫ ソフトウェア製品のセキュリティ品質向上への取り組み

富士通では、ファームウェアを含めたソフトウェア製品のセキュリティ品質を向上させるため、セキュア開発推進チームを中心に、下図に示す取り組みを行っています。具体的には、開発プロセスに次の1.から4.に示すセキュリティ品質を確保する活動を組み込んでいます。

1. 設計工程では、セキュリティ分析（脅威分析）と設計への反映を行います。
2. 実装工程では、脆弱性を作り込まないコーディング（セキュアコーディング）、ツールによるソースコード検証、必要に応じてプログラムへのデジタル署名を行います。
3. テスト工程では、ツールによるセキュリティ検証と、セキュリティ観点でのテストを行います。
4. 保守工程では、IPAやJPCERT/CCと連携して、セキュリティ脆弱性監視、迅速なセキュリティ修正パッチの提供、およびセキュリティ情報の公表を行います。

各工程においては、セキュリティ対応の専門知識を有したセキュリティアーキテクトを各部門に配置し、開発活動における適切なセキュリティ対応の浸透を図っています。開発者全体の1割の人材を確保しています。

ソフトウェア製品のセキュリティ対応プロセス



≫ オープンソースソフトウェアを利用した出荷済製品のセキュリティ確保の活動

「4.保守工程」の一環として行っているオープンソースソフトウェア（Open Source Software：OSS）を利用した製品のセキュリティ確保の活動をご紹介します。昨今のソフトウェア製品のニーズの多様化に伴い、当社製品で利用するOSSの種類も増えています。このため、それぞれのOSSの脆弱性に迅速に対応することが重要になってきています。そこで、OSSの脆弱性への対処を網羅的、効率化するための「OSS脆弱性対応システム」を社内のSE部門と共同で構築し、対応漏れの防止と迅速な対応に努めています。

OSS脆弱性対応システムの概要

1. OSS脆弱性情報の情報源にJVN iPedia脆弱性対策情報データベース※1を採用しています。これにより、NVD（National Vulnerability Database）※2番号が割り当てられた脆弱性を網羅しています。
2. 製品リポジトリに格納されている情報を基に、脆弱性情報の収集対象OSSを設定しています。これにより、製品で利用している全てのOSSを、脆弱性調査の対象とすることができます。
3. OSS脆弱性対応システムに収集された脆弱性情報は、製品リポジトリに格納されている製品別OSS情報と照合の上、即座に製品開発者に通知されて、脆弱性対応が始まります。

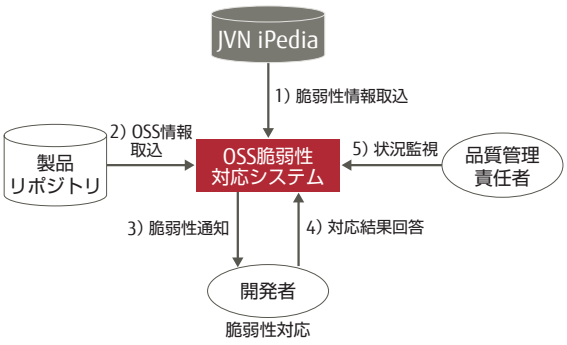
4. セキュリティは優先度の高い問題と位置付けられており、OSS脆弱性も優先度を上げて調査を実施します。対応状況は製品開発部門の品質管理責任者がチェックしており、対応が停滞していた場合は指導が行われます。

なお、情報源として、各種のインターネット公開情報も利用します。

〔※1〕JVN iPedia脆弱性対策情報データベース：JPCERT/CCと情報処理推進機構（IPA）が共同で管理している脆弱性情報データベース。2007年以降にNVDに登録された脆弱性情報を網羅している。

〔※2〕NVD（National Vulnerability Database）：米国NIST（National Institute of Standard and Technology）が管理している脆弱性データベース。

OSS脆弱性対応システムの概要



製品開発者教育

ソフトウェア製品開発部門のセキュリティ教育には、プロフェッショナル人材に向けた「セキュリティアーキテクト教育」と、一般の製品開発者・製品検査担当者に向けた「一般教育」の2系統があります。

セキュリティアーキテクト認定制度

セキュリティアーキテクトとは、ソフトウェア製品のセキュリティ品質を向上させるための、セキュリティ対応活動の推進役となる社内プロフェッショナル資格であり、ソフトウェア製品開発部門では育成プログラムを含むセキュリティアーキテクト認定制度を運用しています。

セキュリティアーキテクトの育成プログラムは、各開発担当部署から推進された候補者に対して数ヶ月かけて4つのフェーズにより実施されるカリキュラムであり、①事前学習と課題作成、②集合教育（演習形式）、③脅威分析レポートの作成、④認定ヒアリングで構成されます。

セキュリティアーキテクトとして認定された後は、スキルアッププログラムとして、下図に示す以下の内容の研修会を年1～2回の頻度で、定期的に開催しています。

- 他部署のセキュリティ活動紹介
- 社内障害事例紹介
- 専門組織の研究報告
- セキュアなソフトウェアの開発プロセス（最新情報）

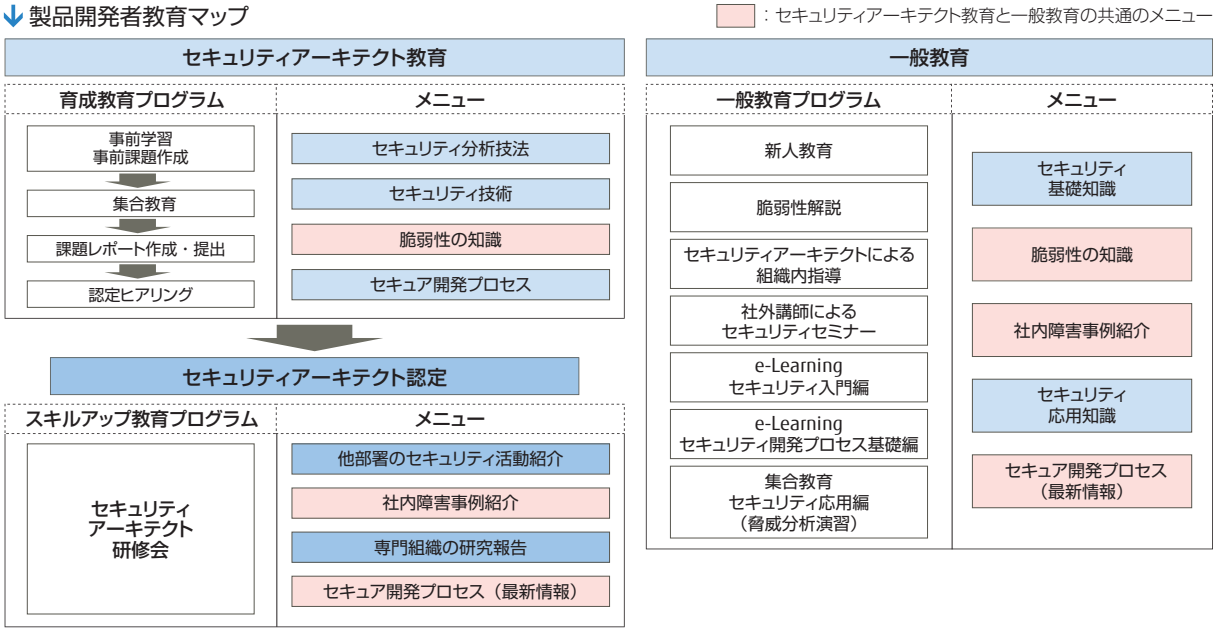
研修会を通して、個々のスキルアップや知識の更新を図ると共に、意見交換や情報交換が行われることにより、セキュリティアーキテクト同士の意識啓発を図っています。

一般教育

一般教育は、新人教育をはじめとするe-Learningや集合教育のほかに各部門内での教育、社外講師を招いてのセミナーなど、様々なメニューを用意して、セキュリティ対応能力の向上を図っています。

脆弱性やセキュア開発プロセスなど重要な事項は、開発者にも必要な知識となることから、セキュリティアーキテクト教育と共通で一般教育でも提供しています。

製品開発者教育マップ



安全な暮らしを支える セキュリティ技術の研究開発

サイバー攻撃が日々激化、巧妙化を続け、企業システムの安全が脅かされています。一方で、様々な機器がネットワークに接続される IoT時代をむかえ、パーソナル情報をはじめとする様々な機器からの情報を安全に利活用することが望まれています。これらの課題の解決のために、富士通研究所では、最先端の技術開発に取り組んでいます。本報告書では、最近猛威を振るっている標的型攻撃を早期に検知する技術と、IoT機器同士の軽量かつ高セキュアな相互認証技術をご紹介します。

≫ 標的型サイバー攻撃の新しい検知技術

巧妙化するサイバー攻撃

近年、特定組織や個人を標的として情報窃取を行うことを目的とした標的型攻撃が急増しており、その攻撃の方法は、より巧妙になってきています。標的型攻撃では、マルウェアと呼ばれる悪意あるプログラムが用いられます。

最新のマルウェアは、通常の業務で発生するメール送受信やウェブアクセスなどの通信に紛れて、攻撃者が組織外から内部の感染パソコンを遠隔操作し、内部情報を取集するRAT（Remote Access Trojan）というタイプが主流になってきています。RATが攻撃する際の通信内容にはマルウェア自体が含まれず、遠隔操作の通信自体も暗号化されていることがほとんどで、従来のアンチウイルスソフトウェアや不正侵入検知システムなどの対策では発見が困難でした。

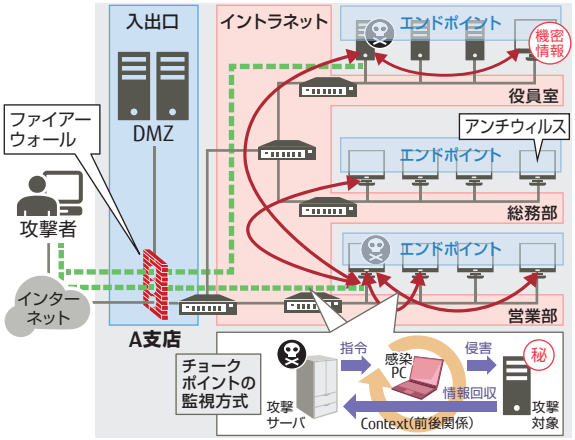
組織内に侵入したマルウェアの新しい検知技術

今回、RATの社内潜伏活動をイントラネットで検知する技術を開発しました。

1. チョークポイントの監視方式

多様な攻撃の手口に共通する通信の特徴的なパターンをチョークポイントと呼びます。この通信パターンに着目し、イントラネットを流れている通信の種類と、関連する通信の前後関係を解析することで、RATによる社内潜伏活動を検知します。通信の種類と前後関係のみを見るので、通信にマルウェアが含まれていなかったり、暗号化されていたりしても高い検出率を実現します。

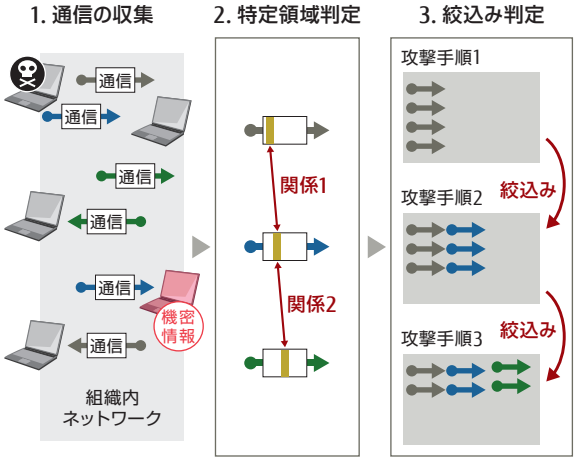
チョークポイントの監視方式のイメージ



2. RATの通信パターンの効率的な判定技術

チョークポイントの監視方式において、攻撃通信の判定を、二つの技術で効率的に行います。一つは、一般に通信内容の詳細解析が必要な攻撃通信の判定を、複数通信の特定領域の情報と通信順序の関係のみを使用し、検知精度を下げることなく解析処理量を削減しながら攻撃通信を判定する「特定領域判定」技術です。もう一つは、大量の通信の中から複数通信で構成された攻撃を抽出する時間がかかる処理を、攻撃手順の段階ごとに解析すべき通信情報の候補を狭めて管理することで、効率的に複数の不審な通信を判定する「絞込み判定」技術です。

RATの通信パターンの効率的な判定技術の概要



開発技術を、2,000台規模の端末が接続された大量の業務通信が流れているギガビットのネットワーク環境で、RATの潜伏活動を再現しながら実証評価し、全通信パケット量の0.0001%に当たるRATの攻撃通信をすべて検知すると共に、業務通信を攻撃通信と誤検知しないことを確認しています。

新しい検知技術の効果

本技術を搭載したネットワーク装置を組織内ネットワークへ配備することにより、組織内のイントラネットを流れる不正な通信を監視することができます。ファイアーウォールやアンチウイルスソフトウェアでは検知困難な標的型攻撃のマルウェアを、情報漏えい前に検出することに効果を発揮します。今後は、攻撃検知後の対処技術の研究開発も目指して行きます。

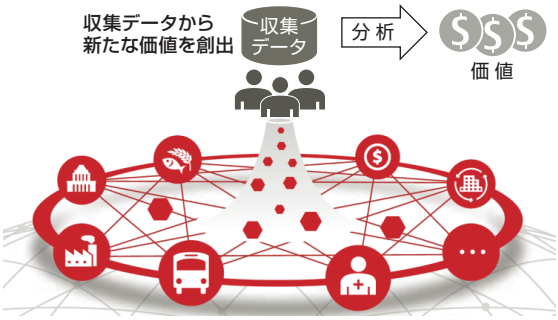
» IoT時代の機器間相互認証技術

IoTのセキュリティ確保のために

汎用PCに加えて、エアコン、照明、自動車など、多様な機器がインターネットに接続されるIoT時代をむかえ、機器が得た情報を収集し、その分析結果を利活用する新たなビジネスに注目が集まっています。こうした用途では、収集した情報が正しいか、機器が不正に操作されていないかを保証するセキュリティ技術が必須となります。一方で、2020年には接続されるデバイスが約500億個になると予想されており、そこで使用されるセキュリティ技術にも高い効率性が求められます。富士通研究所では、IoTの世界で効率的に機器同士の相互認証が可能な技術の研究開発を行っています。

現在のインターネットでは、TLS（Transport Layer Security）と呼ばれる認証・暗号通信技術が広く利用されています。TLSでは、通信相手が正しいことを認証するために、公開鍵暗号を利用します。一般に公開鍵暗号では、ユーザーや機器と使用する鍵との紐付けを保証する証明書が必要です。通信相手の認証には、証明書を互いに送信し、証明書検証などの負荷の高い暗号処理が必要となります。それを機器数の膨大なIoTの世界で行うと、全機器に証明書を準備・管理する膨大な手間がかかること、また、証明書検証のための暗号処理と通信量の爆発的増加が課題となります。そこで、富士通研究所では、証明書を利用しない相互認証技術を開発しました。

↓IoT利用イメージ



機微情報も通信されるためセキュリティ確保は必須

開発した技術

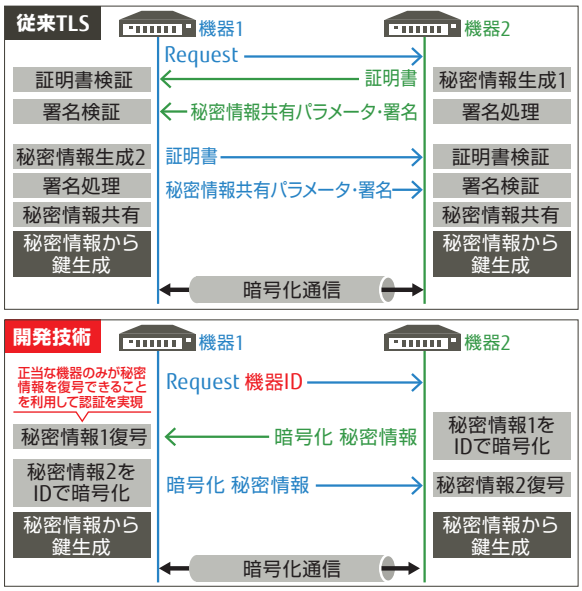
開発技術では、IDベース暗号と呼ばれる、IDを鍵に使える公開鍵暗号を活用しています。TLSで使われている公開鍵暗号、RSA暗号や楕円曲線暗号では、ユーザーとは無関係の乱数を鍵に使います。そのため、暗号化を行うには、事前に通信相手の証明書を入手し、その鍵（乱数）の正当性を検証する必要がありました。これに対し、IDベース暗号では、相手のIDが鍵のため、証明書の事前入手や、証明書を使った鍵の確認をすることなく、暗号化を行うことが可能です。

開発した相互認証技術では、この性質を利用して、相手の機器IDで暗号化した秘密の情報を互いに送りあいます。次に、入手した暗号化秘密情報を復号し、その秘密情報から暗号通信用の一時鍵を生成します。暗号化に使用したIDに対応する正当な機器のみが秘密情報を復号可能なため、この一時鍵でその後の通信を行うことで、相互認証と暗号通信を同時に実現できます。

また、TLSを拡張して、開発した相互認証方式の適用技術を開発しました。適用技術では、既存のTLSプロトコルに適合するように、IDベース暗号による秘密情報の交換を整形・最適化しました。特にこれまでのTLSでは、証明書の交換なしには、機器IDとしてIPアドレスやドメイン名などしか利用できない制約があったのですが、送信者の情報を通信開始時に効率的に伝達する拡張を行うことで、任意の情報を機器IDとして利用可能となりました。

この適用技術により、従来のTLS利用と同等の簡便さで、機器IDによる相互認証技術の利用が可能となります。

↓従来TLSと開発技術との比較



[開発技術の効果]

開発技術を小型のワンボードマイコンに実装したところ、TLSと比較して通信量を1/4、処理性能を2.5倍にすることに成功しました。開発技術により、軽量に機器間の相互認証が可能となり、膨大な機器が接続されるIoTの世界におけるセキュリティ確保を効率的に実現できます。

[相互接続性確保に向けた取り組み]

本研究で開発している認証は、IoTの基盤部分で利用される技術です。今後、数百億個の機器がネットワークでつながるIoTの世界で相互接続性を確保するためには、独自ではなく、他社との協力も重要となります。そのため現在、東大グリーンICTプロジェクトと共同でBEMS（Building Energy Management System）向け通信規格IEEE1888への適用開発を進めています。今後は、本プロジェクトでのIEEE標準化を目指しています。

お取引先と連携した情報セキュリティ向上策

富士通グループの事業活動は、その付加価値の基となる様々なソフトウェア、サービス、物品、部材などを提供していただいているお取引先に支えられています。

富士通グループとお取引先とは、FUJITSU Way企業指針に基づき、相互に切磋琢磨を積み重ねることで長期にわたる信頼関係を構築してまいりました。良きパートナーとして、お互いが自己の力をより一層発揮し、共に存続・繁栄できるような関係を築いています。

富士通グループは、お取引先と共に「情報セキュリティ事故撲滅」を掲げ、情報セキュリティ事故を抑止するために、サプライチェーン全体で、教育、啓発、監査、情報共有などの施策を継続的に実施し、情報セキュリティの維持に配慮した事業活動を推進しています。

2014年度の主な情報セキュリティ強化活動

教育・啓発活動

■ お取引先向け情報セキュリティ研修会

2014年は、実際に発生した盗難・紛失、メール誤送信、ウイルス感染、内部犯行事故を題材に、「うっかり」、「知らないうちに」、「故意」に分類し、情報セキュリティ撲滅・抑止する対策と、今後危惧される新たな脅威（IoT、サイバー攻撃など）について研修会を実施いたしました。

- 2014年度 約950社／約1,200名受講（仙台、東京、川崎、千葉、名古屋、大阪、高松、福岡、沖縄）

■ お取引先向け出前研修会

2014年も、お取引先からの要請で講師を派遣し、お取引先従業員向け研修会を実施いたしました。

- 2014年度 約45社／約1,600名受講

■ お取引先リーダ向けワークショップ

主要なお取引先のリーダクラスを対象に、リーダとしての役割を再認識し、また情報セキュリティ事故の防止スキルを向上いただくため、情報セキュリティ事故の疑似体験（報告書作成、要因分析、是正策の策定など）のワークショップを実施いたしました。

- 2014年度 約20社／約70名（東京、大阪）

お取引先選定、状況評価

新規のお取引先選定においては、情報セキュリティ状況を事前確認すると共に、業務委託時の情報セキュリティ管理、個人情報保護取扱に関する要求事項などにつき、契約で合意を得られるお取引先に限定させていただいております。

さらに、関連情報一式をCD-ROMで提供し、富士通の情報セキュリティレベルへの早期立ち上げを推進しています。

既存のお取引先についても、「個人情報の保護に関する一般法」、「社会保障・税番号制度」などに基づいて委託先を選定しています。お取引先を定期的に直接訪問して「情報セキュリティ点検」を実施し、情報セキュリティ状況を確認しています。また、必要書類の提出による「情報セキュリティ書類点検」など、お取引先に情報セキュリティ施策を自主的に推進させる施策も実施しています。

情報セキュリティ書類点検

情報共有・現場支援ツールの提供

各プロジェクトの情報セキュリティ要求事項を、プロジェクト開始時に的確に合意を支援する「プロジェクト情報セキュリティ計画書」を提供し、課題の早期発見、対応を図っています。

また、情報共有、啓発を目的とした「情報セキュリティの広場」、「啓発ポスター」を継続して提供しています。

プロジェクト情報セキュリティ計画書

海外のお取引先対応

お客様の海外進出支援、開発リソースの確保、国内のお客様の開発費抑制やグローバル製品への対応などを目的とし、海外のお取引先と連携したビジネスが増加しています。

富士通では、国内のお取引先と同様、海外のお取引先に対しても、お取引先の国事情に合わせて受託情報の取扱を規定した「受託者用情報管理要領」を締結し、「情報セキュリティ状況調査」を実施しています。また、「情報セキュリティ監査」、「情報セキュリティ教育」などの支援を行い、健全なパートナーシップを強化、維持しています。

中国での情報セキュリティ教育

第三者評価・認証

富士通グループでは、情報セキュリティの取り組みにおいて第三者による評価・認証の取得を積極的に進めています。

プライバシーマーク登録状況

富士通およびグループ会社における、一般財団法人日本情報経済社会推進協会（JIPDEC）からのプライバシーマーク登録状況は、以下のとおりです。

富士通株式会社
株式会社富士通アドバンストエンジニアリング
株式会社富士通アドバンストクオリティ
株式会社富士通アドバンストシステムズ
富士通アプリケーションズ株式会社
富士通アプリコ株式会社
株式会社富士通 HR プロフェショナルズ
株式会社 AB システムソリューション
富士通エフ・アイ・ピー株式会社
富士通エフ・オー・エム株式会社
株式会社富士通エフサス
株式会社沖縄富士通システムエンジニアリング
株式会社富士通鹿児島インフォネット
株式会社富士通九州システムズ
富士通コミュニケーションサービス株式会社
富士通コワーコ株式会社
富士通 CIT 株式会社
株式会社ジー・サーチ
株式会社富士通四国インフォテック
株式会社富士通システムズ・イースト
株式会社富士通システムズ・ウエスト
株式会社富士通総研
株式会社富士通ソーシアルサイエンスラボラトリ
株式会社富士通ソフトウェアテクノロジーズ
トータリゼータエンジニアリング株式会社
株式会社富山富士通
富士通トラベランス株式会社
株式会社富士通新潟システムズ
株式会社富士通パーソナルズ
株式会社富士通パブリックソリューションズ
株式会社富士通バンキングインフォテクノ
株式会社富士通ビー・エス・シー
株式会社 PFU
富士通フロンテック株式会社
株式会社富士通フロンテックシステムズ
株式会社ベストライフ・プロモーション
株式会社富士通北陸システムズ
株式会社富士通マーケティング
株式会社富士通ミッションクリティカルシステムズ
株式会社富士通山口情報
株式会社ユーコット・インフォテクノ
株式会社富士通ラーニングメディア
株式会社ライフメディア
株式会社富士通ワイエフシー

ISMS 認証取得状況

富士通およびグループ会社において、情報セキュリティマネジメントシステムを定めた国際規格ISO/IEC 27001に基づくISMS認証を取得した部門を持つ会社は、以下のとおりです。

富士通株式会社
株式会社富士通アドバンストエンジニアリング
富士通エフ・アイ・ピー株式会社
株式会社富士通エフサス
株式会社富士通鹿児島インフォネット
富士通関西中部ネットテック株式会社
株式会社富士通九州システムズ
株式会社富士通四国インフォテック
ジスインフォテクノ株式会社
株式会社富士通システムズ・イースト
株式会社富士通システムズ・ウエスト
株式会社富士通ゼネラル
株式会社富士通総研
株式会社富士通ソーシアルサイエンスラボラトリ
株式会社富士通ディフェンスシステムエンジニアリング
株式会社富山富士通
ニフティ株式会社
富士通ネットワークソリューションズ株式会社
株式会社富士通パブリックソリューションズ
株式会社富士通ビー・エス・シー
株式会社 PFU
富士通フロンテック株式会社
株式会社富士通マーケティング
株式会社富士通ミッションクリティカルシステムズ
富士通ミドルウェア株式会社
富士通リース株式会社
株式会社富士通ワイエフシー

情報セキュリティ格付けの取得状況

情報セキュリティ格付けとは、企業や組織が取り扱う技術情報、営業機密、個人情報について、主として漏えい事故などが起きないかどうか、そのセキュリティのレベルを示す指標です。

株式会社アイ・エス・レーティングより付与された、富士通グループの情報セキュリティ格付けの取得状況は、右のとおりです。

会社名	格付スコープ	格付符号
富士通株式会社	館林システムセンター	AAA_{is}
	明石システムセンター	AAA_{is}
富士通エフ・アイ・ピー株式会社	横浜データセンター	AAA_{is}
	中部データセンター	AAA_{is}
	九州データセンター	AA^{+}_{is}
株式会社 富士通エフサス	東京 LCM サービスセンター	AA^{+}_{is}

ISMS 資格取得状況

一般財団法人日本情報経済社会推進協会（JIPDEC）が国内で2002年より情報セキュリティマネジメントシステム（ISMS）適合性評価制度の本格運用を始めました。国内では、審査員の評価登録を行っている要員認証機関として、一般財団法人日本規格協会（JRCA）とIRCAジャパン（国際審査員登録機構）があります。

審査員の資格区分には、「ISMS主任審査員」、「ISMS審査員」、「ISMS審査員補」などがあります。富士通およびグループ会社のISMSの監査人資格を有する人数は、次のとおりです。

〈153名〉

JASA 監査人資格取得状況

特定非営利活動法人日本セキュリティ監査協会（JASA）は、経済産業省が2003年4月に施行した「情報セキュリティ監査制度」に基づいた情報セキュリティ監査を実施する監査人を認定する団体です。資格区分としては、「公認情報セキュリティ主任監査人」、「公認情報セキュリティ監査人」、「情報セキュリティ監査人補」、「情報セキュリティ監査アソシエイト」があります。

富士通およびグループ会社のJASAの監査人資格を有する人数は、次のとおりで国内で最も多い資格者を有しています。

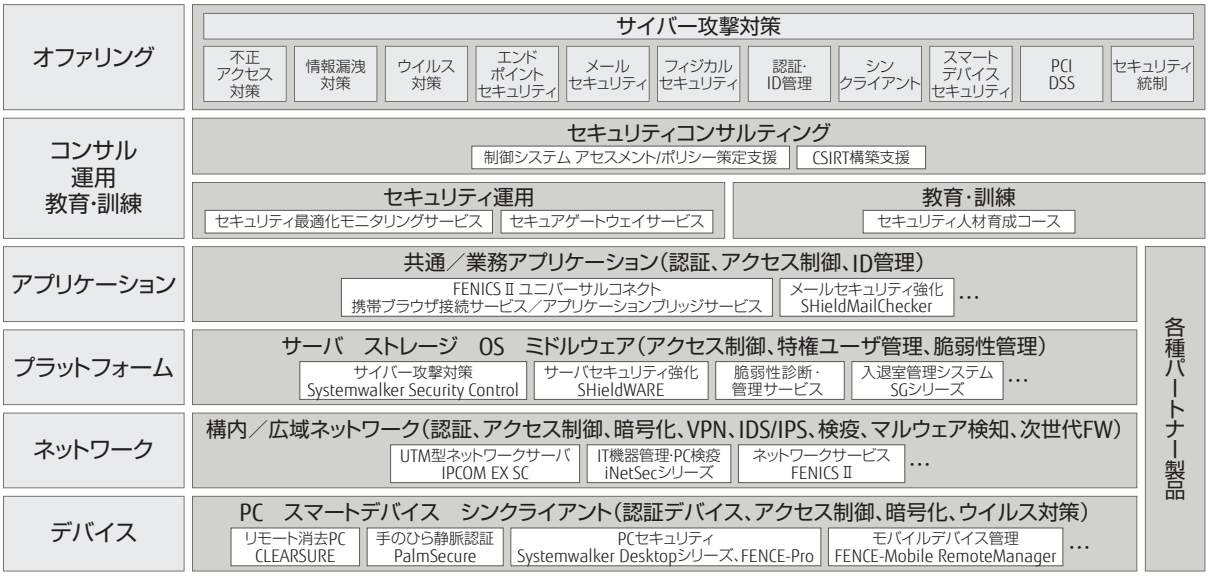
〈141名〉

FUJITSU Security Initiative

お客様と社会の事業継続を支え続けるため、ICTにおける安心安全の実現に継続的に取り組みます。

クラウドコンピューティングやスマートデバイスの普及によりICT活用領域が広がる一方、日々高度化、巧妙化するサイバー攻撃への対策は、ICTの安心安全な活用において大きな課題となっています。当社は世界約300社に広がるイントラネットで起こる一日数億件に及ぶイベントを、適切な対策と運用で対処しています。富士通はこれらのノウハウをお客様のセキュリティ対策に展開します。システムや運用の強化および教育・訓練の統合的な実現に向け、「FUJITSU Security Initiative」として製品・サービスを体系化し、お客様と社会の事業継続を支え続けます。

FUJITSU Security Initiative



セキュリティソリューション

昨今、情報セキュリティを取り巻く環境は、ウイルスや不正アクセスなどをはじめとする外部からの脅威、さらには、サイバー攻撃や、スマートデバイスの利用拡大に伴う情報漏えい事故など、様々なセキュリティリスクにさらされています。当社では、富士通の実践ノウハウを蓄積した「富士通エンタプライズセキュリティアーキテクチャー（ESA）」と「セキュリティマネジメントフレームワーク（SMF）」による一貫したセキュリティの考え方と徹底した社内実践に基づき、セキュリティソリューションを提供しています。ソリューション提供にあたっては情報システムに必要なセキュリティソリューションを体系化し、「富士通エンタープライズセキュリティアーキテクチャー（ESA）」に準拠することで、企業内の効率的な投資を機能面から支援します。社内実践に基づくリファレンスモデルの提案により、お客様は実績ある信頼性の高いソリューションを導入することができます。

主なオファリングモデル 詳しくはこちら ▶ http://jp.fujitsu.com/solutions/safety/secure/

セキュリティ統制	ICTを含む企業活動全体の視点から継続的なセキュリティ対策を捉え、組織の「情報セキュリティガバナンス」の実現を支援。
サイバー攻撃対策	従来の対策を活かしつつ、新たな攻撃手法に最適な対策を提供。
スマートデバイスセキュリティ	お客様のスマートデバイスの業務活用時におけるセキュリティ懸念を解消するためのソリューションを提供。
不正アクセス対策	24時間365日のセキュリティ監視をはじめ、企画・策定／対策実施／監査／監視などのセキュリティサイクルを実現。
情報漏洩対策	個人情報保護・情報漏洩防止のため、情報管理のポリシー作成や策定／暗号化機能などを提供。
ウイルス対策	コンピュータウイルス対策のため、防御／駆除／監視／復旧支援などを提供。
エンドポイントセキュリティ	エンドポイント（クライアントが接続されるシステムの末端）における機密情報の漏洩やウイルス被害といった脅威から、お客様のシステムを守る環境を実現。
メールセキュリティ	ウイルス対策や証跡保全など、電子メールを安全に利用できるようにするためのセキュリティ対策をトータルに提供。
認証・ID管理	情報セキュリティの基盤となる認証および利用者情報管理の運用を、生体認証、電子証明書、ディレクトリなど各種製品／サービスの提供により支援。
PCI DSS	PCI DSS（Payment Card Industry Data Security Standard、ペイメントカード業界データセキュリティ基準）のクリアを支援するセキュリティ対策ソリューション。
シンクライアント	最新端末や安全なネットワークでクライアント仮想化をトータルに提供。豊富な利用端末でのモバイル活用でワークスタイル変革も支援。
フィジカルセキュリティ	オフィスにおけるセキュリティ上の課題を総合的に解決。

富士通株式会社
セキュリティテクノロジーセンター

〒144-8588 東京都大田区新蒲田1-17-25 富士通ソリューションスクエア
TEL：03-6810-6682
http://jp.fujitsu.com/