富士通グループ
情報セキュリティ報告書
2013

FUJITSU

shaping tomorrow with you

社会とお客様の豊かな未来のために

情報セキュリティ報告書 2013

CONTENTS

富士通が考える情報セキュリティ 3

Number 1 富士通グループの情報セキュリティ 4

Number 2 ITセキュリティへの取り組み 7

Number 3 クラウドサービスにおけるセキュリティ対策 11

Number 4 ソリューションビジネスグループの取り組み 13

Number 5 製品のセキュリティ 16

Number 6 安全な暮らしを支えるセキュリティ技術の研究開発 18

Number 7 お取引先と連携した情報セキュリティ向上策 20

Number 8 第三者評価・認証 22

Number 9 富士通の安心安全ソリューション 23

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2013年3月時点に於ける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、2013年5月に発行しました。

本報告書に記載されている会社名、商品名は、各社が商標または登録商標として使用している場合があります。

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

情報通信技術（ICT）の進歩は、人々の夢を実現してきました。この進歩は、とどまるところを知らず、グローバルな規模のネットワーク社会を形成して、ビジネスを変え、生活を変え、社会を大きく変えてきました。そして現在、スマートデバイスやクラウドの普及によってICTの利用は再び新しい時代を迎えようとしています。富士通グループはICTインフラを支える企業として、常にヒューマンセントリックなICTの可能性を追求し、新しい価値を創造し続けることにより、人が安心して暮らせる豊かな社会、「ヒューマンセントリック・インテリジェントソサエティ」の実現をめざしています。

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ともに、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に関する五つの関連規定を整備し、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 2013」は富士通グループの情報セキュリティに関する活動を紹介するものです。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、社内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

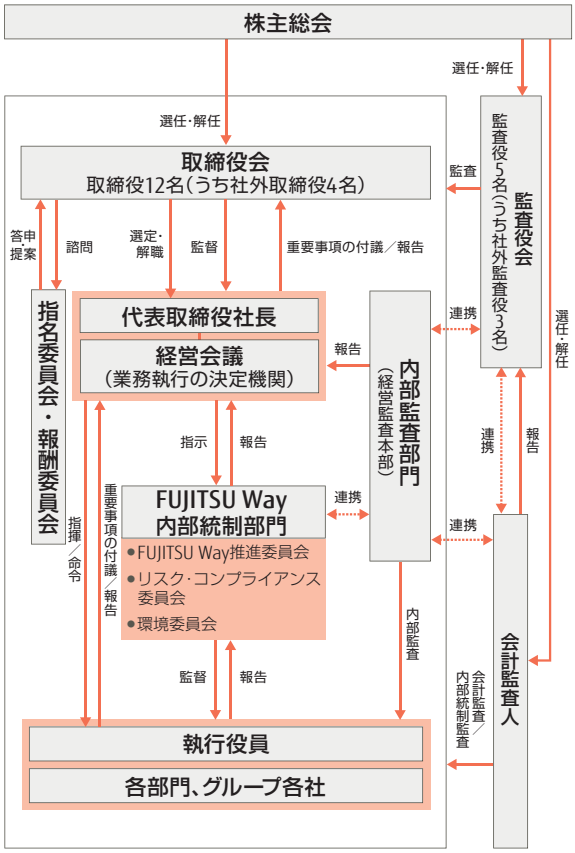
コーポレートガバナンス

企業価値の持続的向上を実現するためには、経営の効率性を追求するとともに、事業活動より生じるリスクをコントロールすることが必要であり、そのためにはコーポレート・ガバナンスの強化が不可欠です。この基本的な考え方のもと、当社の取締役会において「内部統制体制の整備に関する基本方針」を定め、継続的に施策を実施しています。

また、富士通では、経営の監督機能と執行機能を分離することで意思決定の迅速化を図るとともに、経営責任を明確にすることに努めています。監督と執行の2つの機能間での緊張感を高めるとともに、社外役員を積極的に任用することにより、経営の透明性と効率性を一層向上させています。

グループ会社については、富士通グループとしての全体最適を追求するため、グループ全体の価値創出プロセスにおけるそれぞれの役割・位置づけを明確にしています。これによって、富士通グループの企業価値の持続的向上をめざしたグループ運営を行っています。

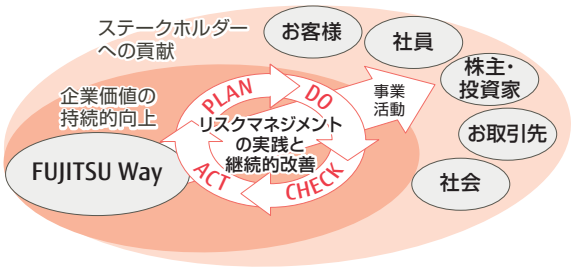
▼ コーポレートガバナンス体制



リスクマネジメント

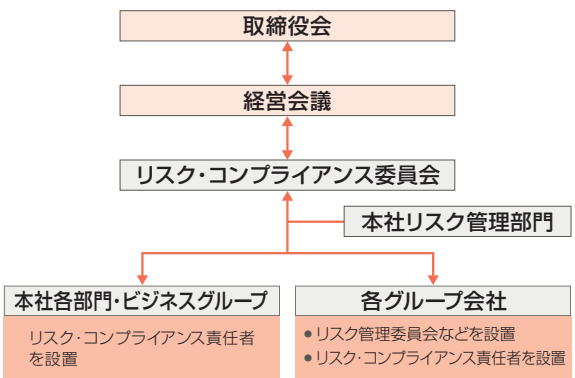
富士通グループは、グローバルなICT事業活動を通じて、企業価値を持続的に向上し、お客様や地域社会をはじめすべてのステークホルダーの皆様に貢献することをめざしています。この目的の達成に影響を及ぼすリスクを適切に把握し、対応することを経営における重要な課題と位置づけ、FUJITSU Wayに基づくグループ全体のリスクマネジメント体制を構築し、また、様々なリスクについて、未然防止および発生時の影響の最小化に向けた活動を推進し、グループ全体でのリスクマネジメントの実践と継続的改善を行っています。

▼ リスクマネジメントの実践と継続的改善



また、2012年7月、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体制の一元化と強化のため、従来の「リスク管理委員会」と「行動規範推進委員会」を統合し、「リスク・コンプライアンス委員会」を新設しました。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体制



情報セキュリティについて

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、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。

また、「富士通グループ情報セキュリティ基本方針」のもとに五つの関連規定を整備し、情報セキュリティ対策を実施しています。

富士通グループ 情報セキュリティ基本方針

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。

- 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。
- 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。
- 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。

取組みの原則

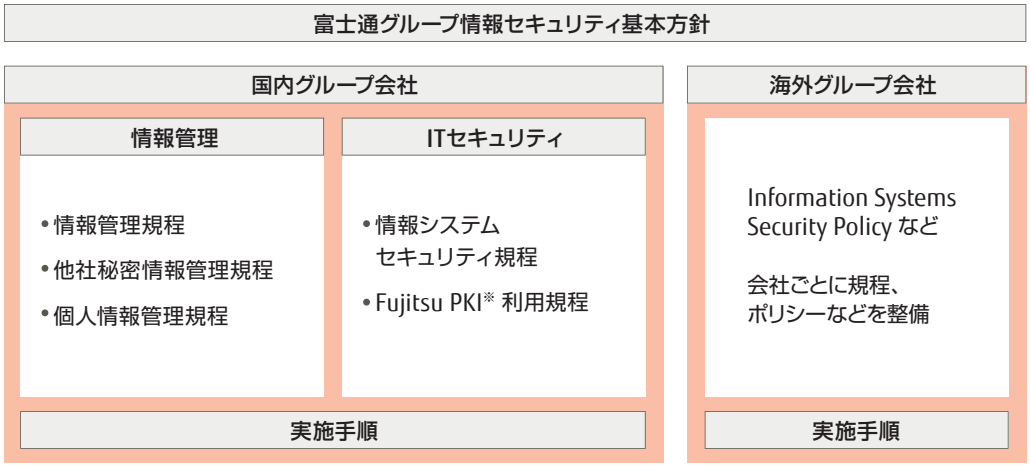
富士通グループは、次の事項を情報セキュリティへの取組みの原則とします。

- 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。
- 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。
- 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。
- 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。
- 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。

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。

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ともに、役員を含む全社員を対象としたeラーニングを毎年実施しています。

▼ eラーニング画面

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、富士通および国内グループ会社の各事業所にポスターを掲示するとともに、全社員の業務用PCにシールを貼付することで、情報セキュリティに対する、社員一人ひとりの意識の高揚を図っています。

また、社内において有効な情報セキュリティ対策を実施している部門の活動状況を参考事例としてイントラネットで公開し、各部門における自主的なセキュリティ推進活動を促進しています。

さらに、電子メールの社外誤送信対策ツール（メールチェッカー）を全社で導入するなど、ICTの活用の推進と併せて、社員一人ひとりの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

昨今、一般的に情報漏えい・紛失事故が多発していることから、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

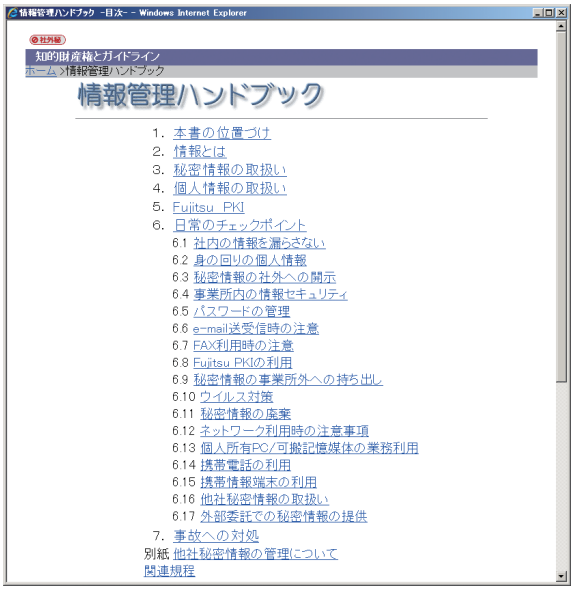
富士通では、個人情報保護法に準拠した「個人情報保護ポリシー」と「個人情報管理規程」を定めています。この規程に基づき、毎年、個人情報の取り扱いに関する教育や監査を実施するなど、継続的に個人情報保護体制の強化を図っています。

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では、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、管理職自ら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



Number 2

ITセキュリティへの取り組み

ICT（情報通信技術）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リスクが伴います。

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。

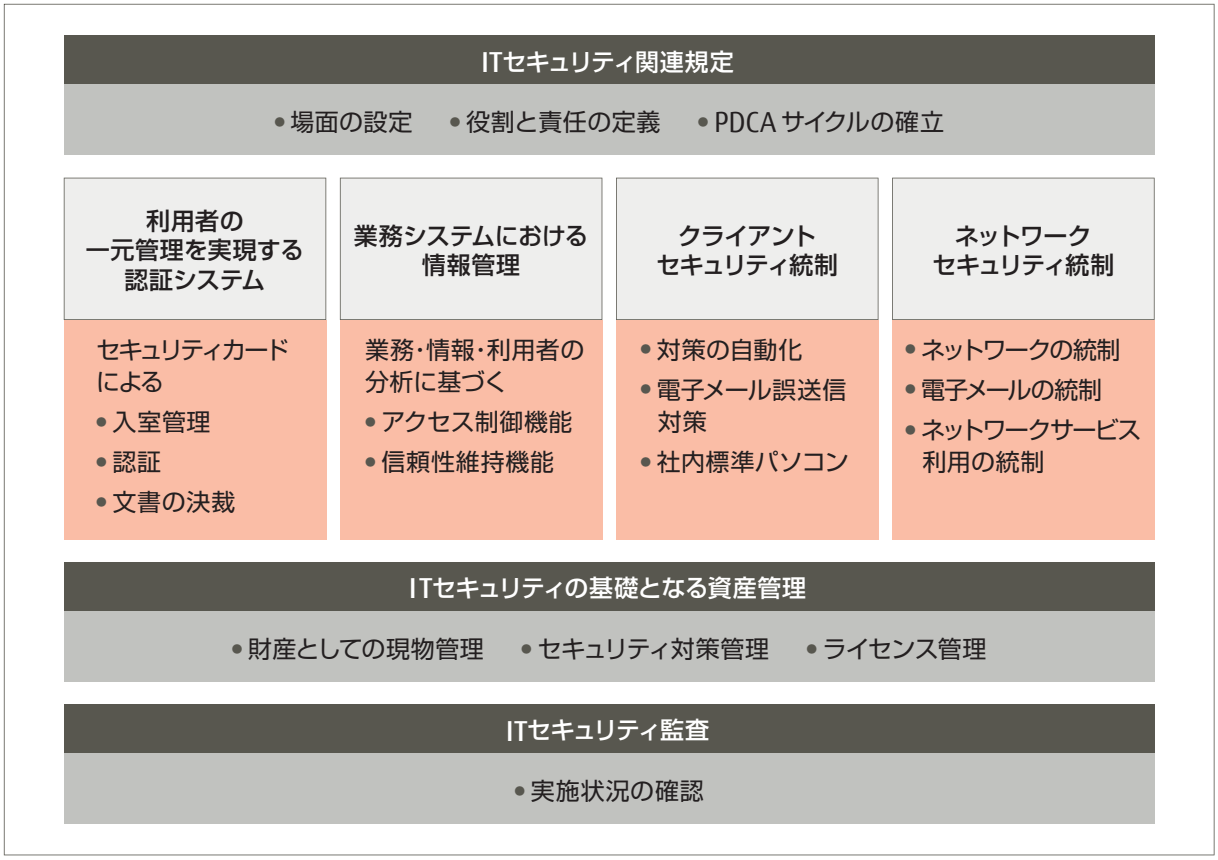
富士通グループのITセキュリティでは、対策をできる限り業務環境や業務手順に組み込んで実現します。こうして、従業員が本来の業務に専念できるようにすることが重要だと考えています。

また、ICTの進歩ととも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。

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「認証システム」「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」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

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

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

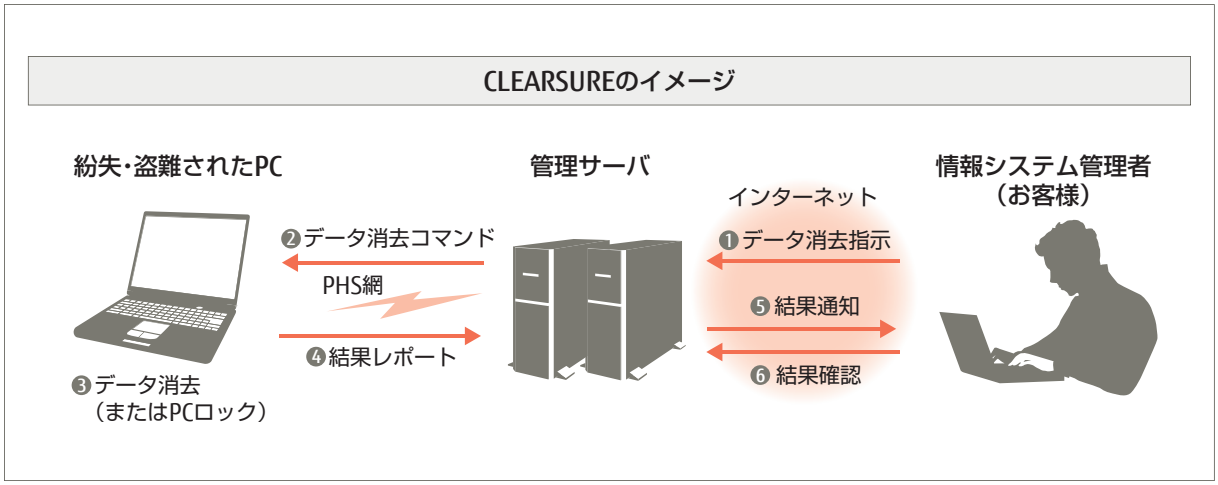
電子メールは、宛先を誤ると容易に情報が漏えいしてしまいます。そこで、電子メールの宛先を自動的に識別して、外部への送信について送信者に再確認の操作をさせるなどにより、誤送信を削減しています。

■社内標準パソコンの導入

富士通グループでは、「社内標準パソコン」の導入を進めています。社内標準パソコンとは、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、パソコンの選定・導入・運用を定型化し、費用の削減とセキュリティ対策の確実な実施を実現しています。

さらに、ノートパソコンの紛失・盗難対策として、遠隔指示によってノートパソコンのデータを無効化する仕組みを社内標準パソコンに装備しました。これにより、仮にパソコンの紛失・盗難が発生しても情報漏えいに至る可能性を格段に下げることができます。この機能は、情報漏洩対策ソリューションの一つの「CLEARSURE（クリアシュア）」としてお客様に提供しています。

▼ ノートパソコン紛失・盗難対策



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通りです。

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

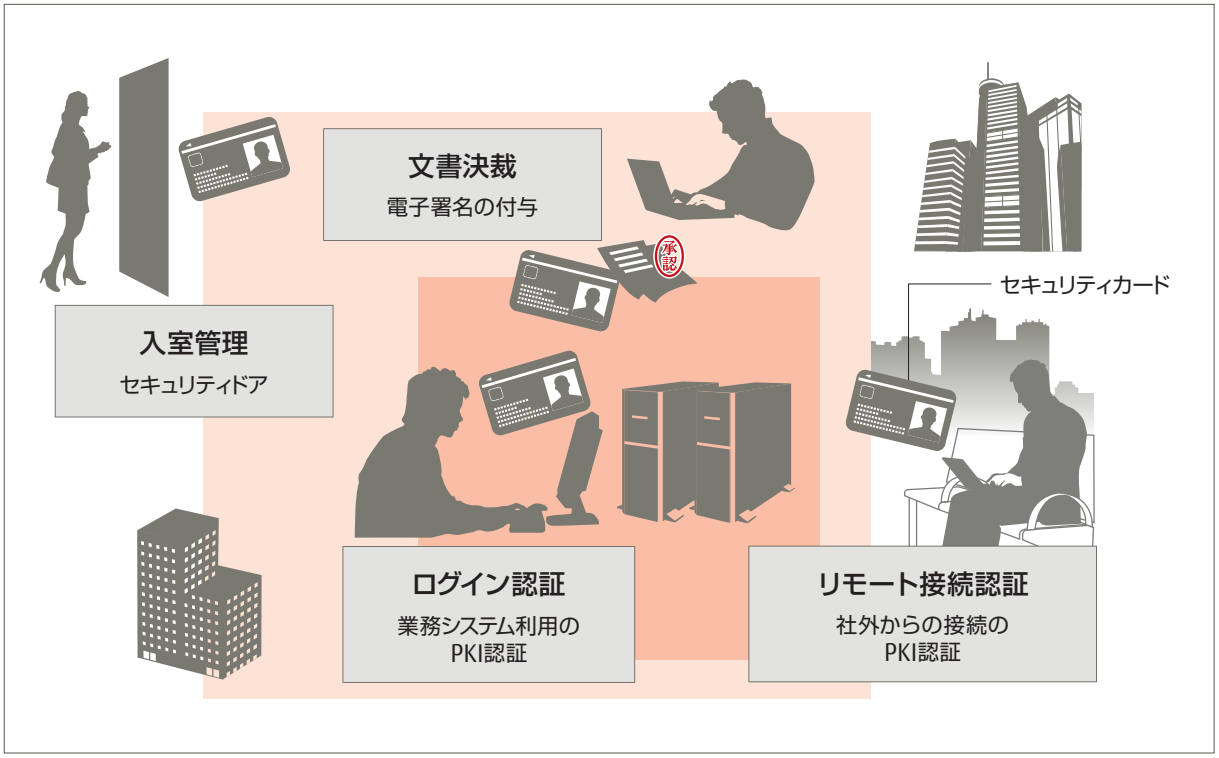
業務システムの利用にセキュリティカードが必要です。業務システムへのログインでPKIによる認証を行っているため、従業員の識別と認証が確実に行われ、しかも操作は容易です。

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。

文書の決裁

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り、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、富士通グループ外とのやり取りについても、業務で必要である限り使用を認めています。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

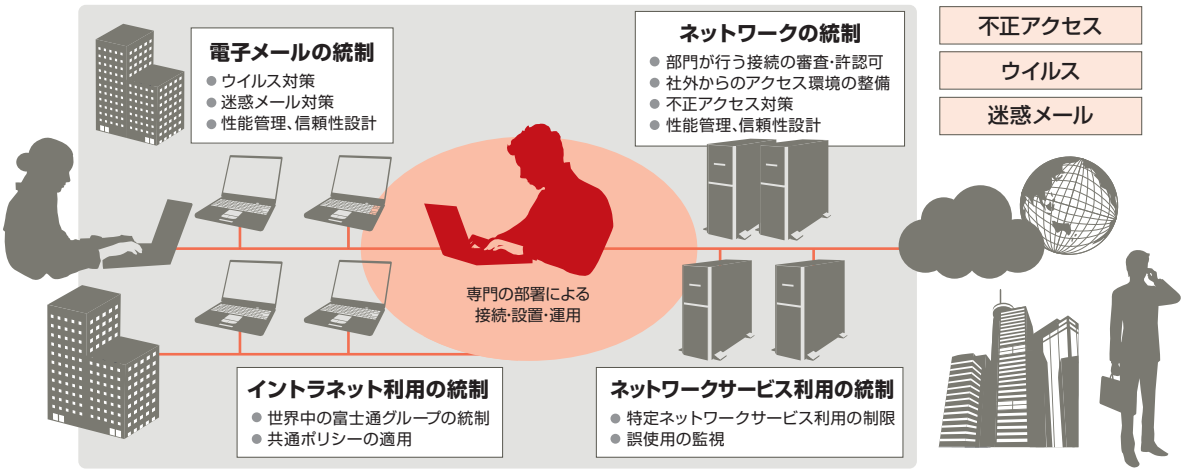
ネットワークサービス利用の統制

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、イントラネット利用の統制を進めています。「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施策として、世界中のグループ会社におけるイントラネットの構築と利用を共通のポリシーおよび管理施策に基づき統制します。

▼ 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。

クラウドサービスにおけるセキュリティ対策

クラウド・コンピューティングは、従来のシステムでは実現できなかった、コンピューティングの柔軟性、俊敏性などを実現する新しいスキームです。しかし、クラウド化することで、安全性や信頼性への不安など利用者は新たなセキュリティの問題に直面することにもなります。本報告書では、富士通がクラウド・コンピューティングサービスで実現しているセキュリティの取り組みをご紹介します。

クラウド・コンピューティングの課題

クラウドは、経営のスピードアップや新事業におけるICT導入のしやすさなどビジネスに恩恵をもたらす一方で、そのサービス形態ゆえに発生する脅威に対応しなければなりません。例えば、クラウドでは多くの利用者アカウントや複数の利用者のデータが同一のITリソースに存在するため、セキュリティ事故の影響が大きくなる可能性があります。またクラウドで用いられる仮想化技術の脆弱性を利用した攻撃やクラウドのリソースを悪用して第三者への攻撃が行われる可能性、さらにクラウドの基盤を支える事業者内部の不正行為も懸念されます。

これらの脅威に対して、ネットワークやサーバ、Webアプリケーションにおいて、境界防御・多層防御を施す従来のセキュリティの考え方はもちろん大切です。一方で、仮想化技術に関連するリスクへの対応や、ITリソースに対する責任範囲が変化することによる運用およびマネジメントの対応など、クラウドの特徴を考慮したセキュリティの考え方も必要となります。

富士通はクラウドサービスを提供するにあたり、組織面と技術面の両面からセキュリティの確保に取り組んでいます。

Fujitsu Global Cloud Platform（FGCP）の取り組み

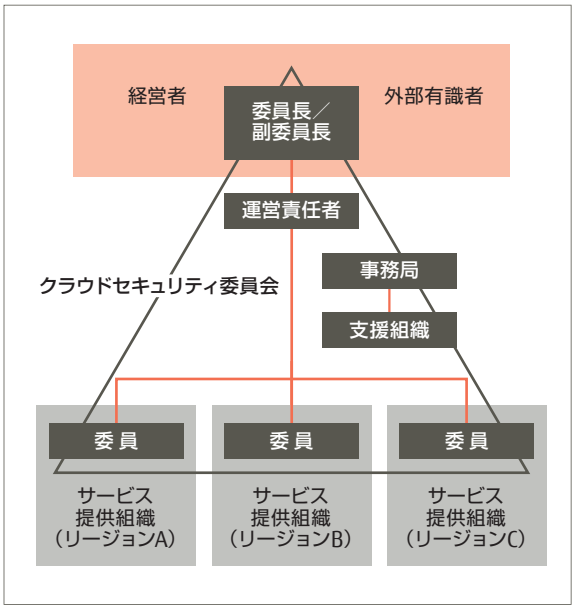
富士通はInfrastructure as a ServiceであるFGCP/S5と、Platform as a ServiceであるFGCP/A5という2つのパブリック型クラウドサービスを提供しています。これら2つのサービスを提供する際に、サービス基盤を支えるセキュリティ対策として下図に示す8つの視点があります。このうち、セキュリティのための組織と情報セキュリティインシデントの管理についてご紹介します。

▼ FGCPサービス基盤を支えるセキュリティ対策 8つの視点

情報セキュリティ基本方針	セキュリティのための組織	人的資源のセキュリティ
物理的および環境的セキュリティ	情報システムの取得、開発および保守	情報セキュリティインシデントの管理
事業継続管理	順 守	資産の管理
アクセス制御	通信および運用管理	

富士通では、クラウドサービスを提供するにあたり2011年に社内委員会として「クラウドセキュリティ委員会」を設置しました。委員会は、右図に示す通り、経営層を委員長に、第三者性を確保するための外部有識者と各サービスを提供する組織の責任者で構成されます。この委員会では、サイバーテロ、不正利用などの脅威の他、各国クラウドセンターの準拠法や個人情報の取り扱いなどグローバルレベルでの対応が必要な案件について方針を討議し、承認しています。

▼ クラウドセキュリティ委員会



また、クラウドにおいてセキュリティのインシデントが発生した際には、影響範囲を最小限にするための判断と対処が重要です。富士通では、海外を含めたインシデントレスポンス体制を整備し、訓練を実施しています。

これらサービス共通で実施するセキュリティ対策については、クラウドのセキュリティを専門的に扱う専門組織「富士通クラウドCERT」が重要な役割を果たしています。富士通クラウドCERTについては次頁で説明します。

各サービスにおける取り組み

FGCP/S5とFGCP/A5は、そのサービス特性に応じたセキュリティ対策を実装しています。これら2つのサービスが提供しているセキュリティ機能には、下図に示す3つの視点があります。利用者はこの機能によりクラウドサービスを用いてセキュアなシステム開発と運用が実現できます。

▼ FGCPが提供するセキュリティ機能3つの視点

情報セキュリティ基本方針	セキュリティのための組織	人的資源のセキュリティ
物理的および環境的セキュリティ	情報システムの取得、開発および保守	情報セキュリティインシデントの管理
事業継続管理	順 守	**資産の管理**
アクセス制御	**通信および運用管理**	

富士通のクラウドサービスでは、利用者はサービスのポータルサイトで仮想システムの配備や実行環境の操作を行います。ポータルサイトでは、稼働しているシステムやリソースの一覧表示など資産管理を支援する機能を利用することができます。

また、アクセス制御で重要な権限管理において、利用者は組織に応じた柔軟な権限設定が可能です。例えば、FGCP/S5ではリソース管理者への権限付与をカスタマイズする機能が利用できます。利用者は、IDごとに資源の追加や削除を行う権限の設定ができます。

利用者はインターネットを経由してシステムの開発や運用を行うため、暗号化機能などにより通信を保護する必要があります。また、FGCP/S5では、Web、アプリケーション、データベースの三階層からなるセキュアなシステム構築が可能です。これによりオンプレミス環境と同様の安全性の高いシステムを実現できます。

富士通クラウドCERTの取り組み

今日のビジネスに求められる「トラステッド(高信頼)」なクラウドを実現するために、富士通はクラウドのセキュリティを専門的に扱う「富士通クラウドCERT」を2010年に設立しました。CERTは、Computer Emergency Response Teamの略であり、コンピュータ環境で発生する緊急事態に迅速かつ的確に対応するための専門チームを意味します。富士通クラウドCERTは、米カーネギーメロン大学によって公式にCERTの名称使用を許諾された、世界で最初のクラウドCERT組織です。

富士通クラウドCERT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、クラウドサービス基盤に対する脆弱性診断やモニタリングなどの情報セキュリティ対策を実施し、24時間365日体制で運用します。

2. 緊急対応

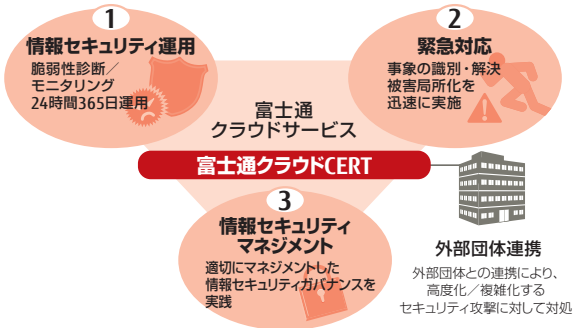
予期できないセキュリティインシデントに対して適切に対処するために、インシデント発生時のプロセスを定め、万が一のインシデント発生時には、事象の識別・解決・被害局所化を迅速かつ確実に実施します。

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。

▼ 富士通クラウドCERTの活動



第三者評価と情報公開の取り組み

富士通は、クラウドセキュリティに関する情報を公開しています。第三者評価もその取り組みの一つです。例えば、FGCP/S5ではグローバルなサービスを提供するにあたり、お客様の一次対応やデータセンターの運用など主要な役割を担う部門でISMSの認証を取得しています。また、ホワイトペーパー「クラウドセキュリティに関する富士通の取り組み」を公開しています。

Number 4

ソリューションビジネスグループの取り組み

富士通のソリューションビジネスグループ（SBG）では、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、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、SBGは情報セキュリティマネジメント体制の下にセキュリティマネジメントフレームワークを各部門・グループ会社に提供し、セキュリティ施策の推進に取り組んでいます。

ソリューションビジネスグループの特徴

ソリューションビジネスグループは、ITシステムのコンサルティング、構築などを行うソリューション・SIと、アウトソーシングなどを中心とするインフラサービスを提供しています。

富士通のサービスビジネスは、国内No.1、グローバルNo.3のシェアを持ち、欧州、米州、アジア、オセアニアまで幅広い国・地域でサービスを展開しています。

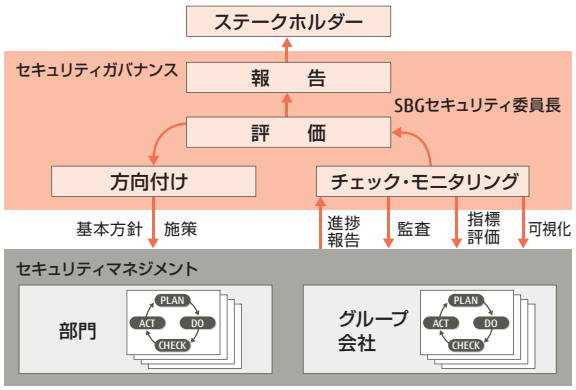
特にアウトソーシング分野では、日本、欧州を中心に、世界16ヵ国、約100拠点にデータセンターを配し、お客様のICTにかかる運用負担の軽減や環境対応など、様々なニーズに応えるサービスを提供しています。

SBG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、経営的な観点でリスクマネジメントが求められています。そのため、情報セキュリティガバナンス体制を確立しセキュリティ活動を推進しています。

ソリューションビジネスグループを構成する、営業・SE業務の各部門・グループ会社はSBGセキュリティ委員会に参加しており、SBGセキュリティ委員会の委員長は情報セキュリティ活動の方向付けをしています。これに従い各部門・グループ会社は、セキュリティマネジメントフレームワーク（SMF：詳細は次頁参照）に基づいて、セキュリティ計画の立案やセキュリティ対策の導入、各部門・グループ会社での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・評価することで、マネジメントの仕組みやセキュリティ対策の改善に取り組んでいます。

▼ SBG情報セキュリティガバナンス



SBG情報セキュリティマネジメント推進体制

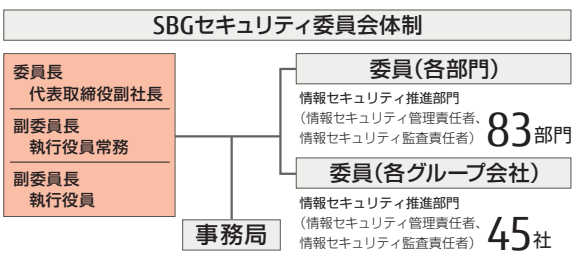
SBGは、お客様の情報資産や秘密情報を取り扱うため、お客様の情報および自社情報の適切な保護を目的として「ソリューションビジネスグループ情報セキュリティ基本方針」を定めています。この基本方針に基づいて「SBGセキュリティ委員会」を設置し、情報セキュリティの維持・推進を図っています。また、四半期毎にSBGセキュリティ委員長、各部門・グループ会社の情報セキュリティ管理責任者、情報セキュリティ監査責任者が参加する委員会総会を開催しています。

各部門の部門長・グループ会社の社長は、SMFの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。

また、各部門・グループ会社が円滑に適切な情報セキュリティ活動を行うことができるよう、SBGセキュリティ委員会事務局が情報セキュリティ活動を推進する上で有効な対策の支援や改善策の助言などを必要に応じて行っています。

これらSBGセキュリティ委員会活動を通じ、各部門・グループ会社は情報セキュリティに関する情報提供・サービスを受けています。その一方で、委員会から要求される情報セキュリティ活動を推進し、SBGで定める情報セキュリティのレベルを維持しています。

▼ SBGセキュリティ委員会組織図

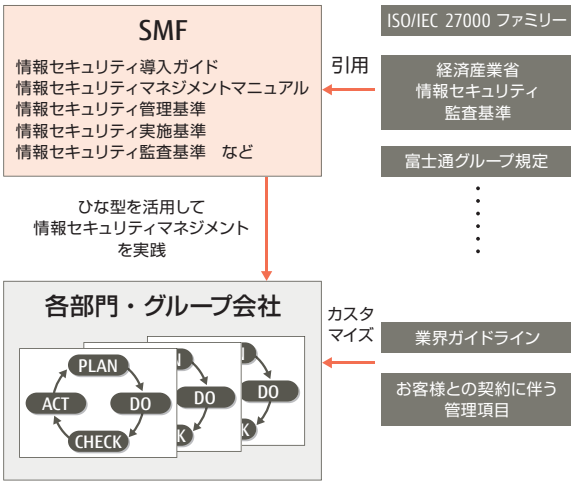


SMF（セキュリティマネジメントフレームワーク）

SBGでは、情報セキュリティマネジメントを実践するためのひな型としてSMFを提供しています。SMFは、富士通グループ規定に加え、ISO/IEC 27000ファミリー、経済産業省の情報セキュリティ監査基準、さらに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。各部門・グループ会社は、業務上関係があるお客様の業界ガイドラインやお客様との契約に関わる管理項目などを考慮し遵守する必要があります。これらを取り入れて最適化した、自部門の情報セキュリティ管理基準、情報セキュリティ監査基準などの情報セキュリティ関連文書を規定し、それに従った運用を行っています。

2012年度は富士通グループ規程の改版があり、これに伴いSMF文書とその監査チェックリストを改訂しました。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

各部門・グループ会社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」を実施しています。これまでに管理者教育の受講者は596名となり、各部門・グループ会社における情報セキュリティマネジメントの推進を行っています。

2012年度は管理責任者に継続的な自己研鑽と新規に教育受講を促すため、e-learning形式でも実施し397名が受講しました。

内部監査に携わる情報セキュリティ監査責任者、監査を実施する内部監査人向けには、「情報セキュリティ監査人教育」を実施しています。これまでに監査人教育の受講者数は1,100名となり各部門・グループ会社の内部監査で活躍しています。

また、監査人向けの教育を検討する上で、セキュリティ監査の品質向上と監査人のキャリアアップを推進するために、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。これまでに127名が監査人資格の認定を受け、内部監査、委員会監査で活躍しています。

管理者、監査人向け教育以外にもSBG共通の情報セキュリティ教育の教材を提供し、各部門で活用しています。

「ITインフラ標準運用サービス」によるセキュリティ維持

SBGでは、情報セキュリティ対策を確実に、継続的に実施するために「SBG標準パソコン」を導入しています。

SBGインフラ運用サービス部門では、社員へのパソコン配布から、導入支援、日常運用、廃却まで、一連のライフサイクルにおいて、情報セキュリティ維持に主眼をおいた総合的なサービスを各部門へ展開しています。

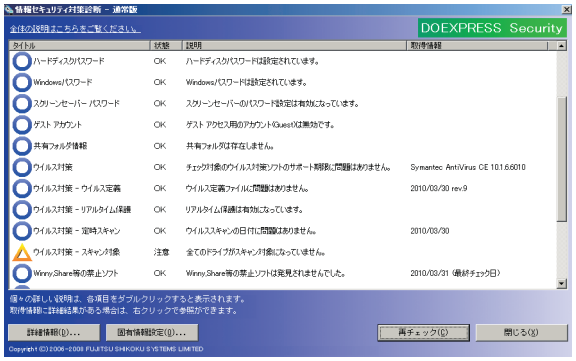
このサービスでは、セキュリティ対策が不十分なパソコンや長期非稼働パソコン、禁止されているファイル交換ソフトのインストールなどの状況を監視し、不備が発見された場合には部門管理者や利用者へ注意を喚起しています。さらに、転用廃却代行サービスを請負うことで、パソコン廃棄時のデータ消去の一括処理を担っています。これによりセキュリティ施策に係る現場負荷を軽減させながらセキュリティリスクの低減に貢献しています。

定期的なセキュリティチェック活動

毎月、全社的な「セキュリティチェックデー」の活動に従い、パソコンやスマートデバイスのセキュリティ設定状況や可搬記憶媒体の管理状況を確認しています。SBGでは情報セキュリティ対策診断ツール（DOEXPRESS Security）を全てのパソコンに導入し、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。パソコン起動時に診断項目（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21項目）を自動的に診断し、診断結果をパソコン画面に表示させています。また、各部門の情報セキュリティ管理責任者は、全てのパソコンの診断結果を確認することで、セキュリティ対策の浸透に効果を上げています。これにより、パソコンのセキュリティ対策状況を確認する責任者の負荷を軽減させました。

スマートデバイスについては、全社方針に準拠したスマートデバイスのセキュリティチェックシートを提供し、各部門で活用しています。

▼ 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

各部門・グループ会社が自身で行う内部監査とSBGセキュリティ委員会が各部門・グループ会社に対して行う監査（委員会監査）があります。毎年実施している内部監査・委員会監査を通して、SBG内の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・定着度を確認しています。

内部監査は、各部門・グループ会社内で前述の「情報セキュリティ監査人教育」を修了した監査人を中心に実施しています。委員会監査は、富士通グループ内における外部監査と位置づけ、毎年サンプリングで選定した被監査部門を第三者の観点で実施しています。

委員会監査はJASA監査人資格を保有する監査人が実施しています。その際、SBGセキュリティ委員会事務局と被監査部門に所属しない監査人で監査チームを構成し、情報セキュリティの推進状況の確認、不備事項の指摘、改善事項の提案などを行っています。さらに、優れた施策（ストロングポイント）はSBG内のノウハウとして、前述のSBGセキュリティ委員会総会の場で事例紹介を行い、SBG内で水平展開を行っています。

また、委員会監査では従来から実施している現地監査に加えて、昨年度からはSBG全部門・グループ会社を対象とした文書監査を併せて実施しています。これは内部監査の実施状況を定期的に把握し、各部門・グループ会社へフィードバックすることで内部監査の質を向上させることを目的としています。

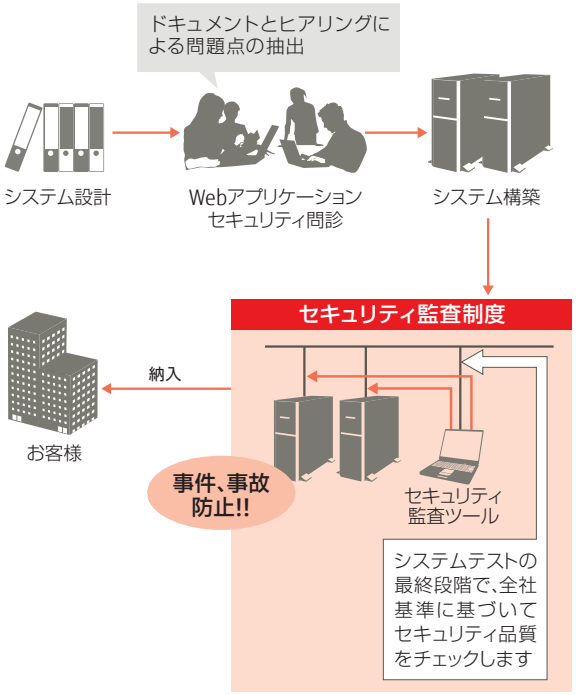
このように異なる観点の監査を組み合わせて毎年継続的に実施することにより、SBG全体の情報セキュリティ維持・向上を図っています。

その他に、各部門・グループ会社から個別の要望、業務上の必要性に応えるために、特定プロジェクトや各部門・グループ会社を対象とした特別監査を実施しています。特別監査はSBGセキュリティ委員会総会事務局の専門家が、その背景に応じた個別の監査テーマを設定して、個別の情報セキュリティ監査を実施しています。

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）のセキュリティ対策として「お客様インターネット接続システムにおけるセキュリティ必須要件」（セキュリティ必須要件）を定めています。システム構築者は、お客様にシステムを納入する前にセキュリティ必須要件を満たすことが義務付けられています。システムの要件確認を行う際には、セキュリティ専門の部署が客観的な観点で行っています。

▼ 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アプリケーションに関しては、上流工程でセキュリティ問題を事前に解決するため、システム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を富士通で定めた均質のセキュリティレベルを確保し、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。

製品のセキュリティ

富士通のソフトウェア製品開発部門では、出荷するソフトウェア製品が一定水準以上のセキュリティ品質を確保できるように標準化による品質向上の取り組みを行っています。

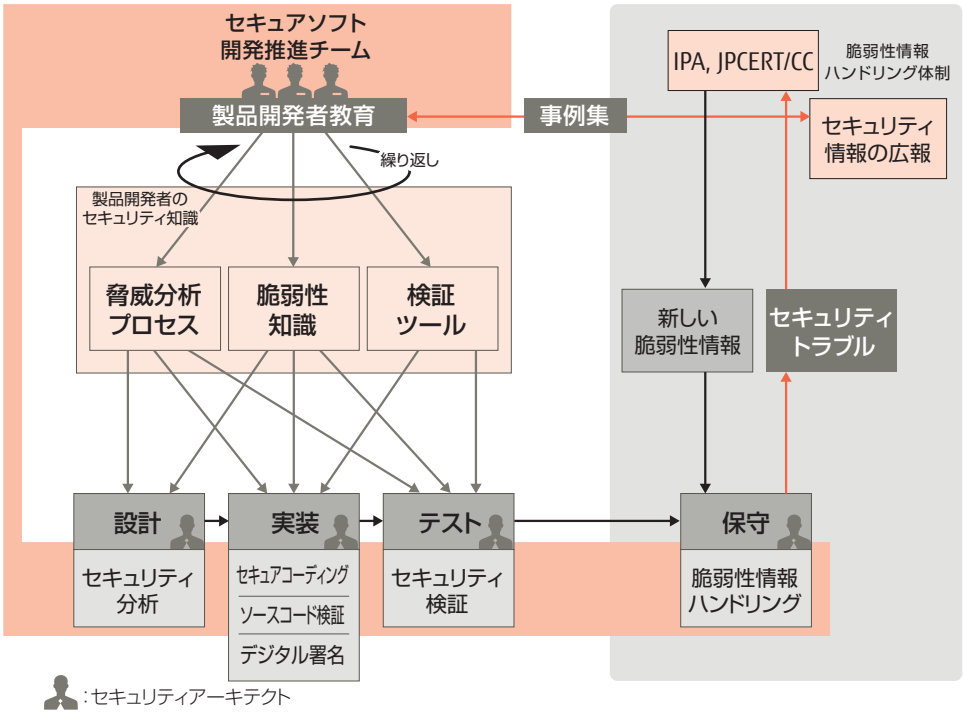
ソフトウェア製品のセキュリティ品質活動

富士通では、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、セキュアソフト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広報を行います。

人材面では、各部門に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育成し、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。2012年12月現在、このセキュリティアーキテクトには、313名が認定されています。

▼ ソフトウェア製品のセキュリティ対応プロセス



作業項目標準化の取り組み

セキュリティ対応活動の属人化による品質のバラツキ

従来の開発活動では、活動の内容や質について製品開発部門の主体性を尊重することにより、製品の特性に応じた柔軟なセキュリティ対応活動を推進してきました。しかし、この進め方では、各製品間のセキュリティ品質にバラツキが生じるリスクが発生してしまいます。例えば、Webアプリケーション開発では、攻撃者やマルウェアなどの攻撃に耐えられる堅牢なプログラムを書く必要がありますが、細部の判断や対応を開発現場任せにすると対策や措置が属人化する傾向があります。さらにこれを放置すると対策漏れや実装ミスを起こしやすくなり製品のセキュリティを一定の品質に維持することが難しくなります。

品質のバラツキを防止するための標準化

そこで、各開発工程で考慮すべき観点や実施すべき作業項目の標準化によって、セキュリティ対策が属人化してしまうことを防止します。標準化にあたっては、脆弱性対策の解説や、実施したセキュリティ対策の標準化対応の評価方法も合わせて整理します。

項目を標準化することにより、開発者が実施するセキュリティ対策に関して、標準への対応の度合いを測定することができるようになります。また、開発者が実施すべき作業項目の選別をしやすくするよう、項目のグループ分けを行い、標準化のメニューとして定義します。

標準化のメニューには、必須項目と任意項目を設定します。必須項目は、ソフトウェア製品の機能として相応しない場合を除き、必ず対応しなければならない項目です。必須項目を設定することにより、一定以上のセキュリティ品質を確保できるようになります。このことから必須項目をベースライン項目としています。任意項目は、製品の位置づけなどに基づいて必要と判断した場合に追加で対応するもので、例えば、よりセキュアな対応が求められるセキュリティ製品などの開発で選択します。下表は標準化メニューとベースライン項目、および任意項目のイメージを示しています。

▼ 標準化メニューと項目のイメージ

メニュー	ベースライン項目	任意項目
識別と認証	ID／パスワードによる認証 …	電子証明書／PINによる認証 …
アクセス制御	ロールベースアクセス制御（RBAC） …	強制アクセス制御（MAC） …
暗号化	電子政府推奨暗号PKCS#5による鍵生成 …	HSMによる鍵管理乱数による鍵生成 …

〔※〕項目は、抽象化しています。

標準化項目を用いた現場でのセキュリティ品質活動

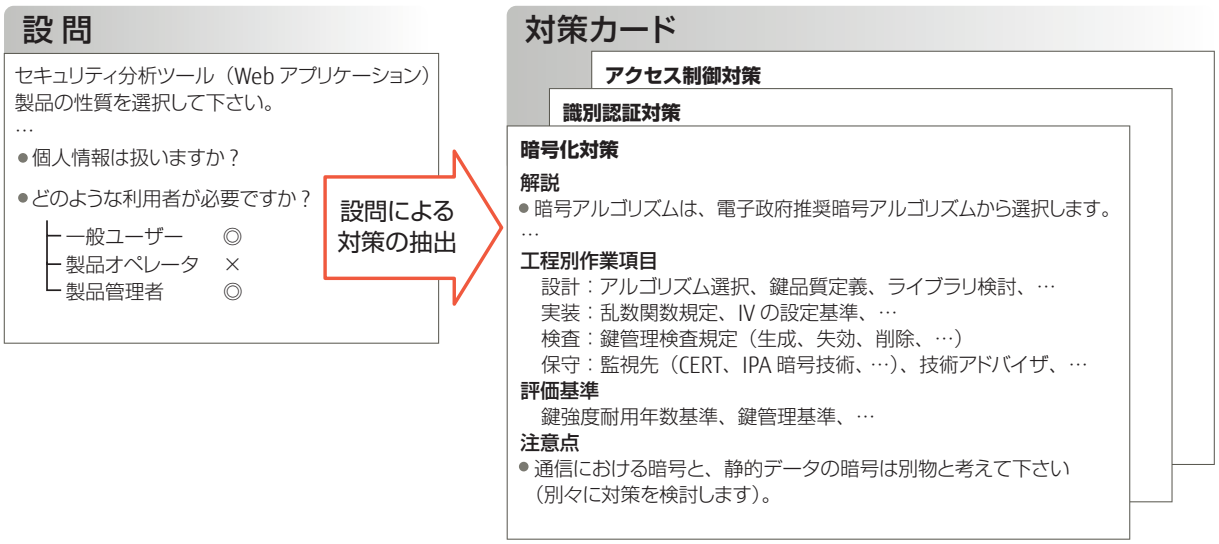
標準化項目を用いた現場でのセキュリティ品質活動の具体的な取り組みを以下に紹介します。セキュアソフト開発推進チームは開発者にセキュリティ分析に必要な専門的知識がなくてもセキュリティ品質を確保できるよう、セキュリティ対策抽出ツールを開発しました。下図は、このツールの適用イメージです。このツールは、設問に答えることにより、製品の特性に応じたセキュリティ対策項目を自動で抽出することができます。この例では、個人情報を扱うかを問う設問から暗号化対策の項目を抽出しています。また、利用者に関する設問から利用者の識別認証に関する要件、役割が複数存在する場合にはアクセス制御に関する要件の抽出を行っています。

セキュアソフト開発推進チームは、標準化項目の継続的改善も行います。開発現場で活動を行っているセキュリティアーキテクトと連携し、標準化項目に開発現場で発生する新しい作業項目を反映するようにしています。

標準化に向けた取り組みは、要件が明確になっている点と需要が多いことを考慮して、先ずWebアプリケーションを中心に進めていきます。その後、ソフトウェア製品一般に拡張していく予定です。

以上のように、ソフトウェア製品に関するセキュリティ対応プロセスを標準化することによる属人化の排除、およびベースラインの定義による一定水準以上のセキュリティ品質の確保を行っていきます。

▼ 設問による対策の抽出イメージ



安全な暮らしを支えるセキュリティ技術の研究開発

スマートフォンの業務利用が浸透し、サイバー攻撃が高度化するなか、企業でのプライバシー情報や秘匿情報の漏えいを引き起こす脅威が増大してきています。これらの新しい脅威に対応するために、新しいセキュリティ技術が求められています。富士通研究所では、新しい技術の要請に応え、最先端技術の開発に取り組んでいます。

富士通研究所でのセキュリティ技術の取り組み

富士通研究所では、企業で活用する情報を様々な脅威から守るための研究を行っています。その範囲は、安心で安全な社会を支えるシステムセキュリティから、様々な要素技術まで広範囲にわたっています。例えば、システムや製品の脆弱性をなくすためのセキュアな開発プロセス、サイバー攻撃対策、最新の暗号や秘匿技術を活用したプライバシー保護技術、生体認証技術などで、当社が提供するシステムや製品のセキュリティ向上に大きく貢献しています。

特に、生体認証では、手のひらの静脈パターンを非接触で認証する技術を世界で初めて開発しました。また、タブレットPCやスマートフォン向けの超小型・高精度の指紋認証技術も開発しています。

本報告書では、先端技術への取り組みとしてセンサーデータを保護して流通・利活用するための技術と、サイバー攻撃による情報漏えいを防ぐための標的型攻撃の出口対策技術を紹介します。

センサーデータの機密を守って流通・利活用

プライバシーや機密情報の扱いは、ビッグデータの利活用において大きな課題となっています。最近では、情報家電やスマートメータ、スマートフォンなど身の回りのセンサーから得られるデータも増えており、そこにはユーザーIDなどの個人を特定する情報や、移動経路や不在情報といったプライバシー情報が含まれています。これらのデータが紐づくと、個人の生活パターンが明らかになり、例えば、留守宅を狙われるなどの危険につながる可能性があります。また、欧州における個人情報保護規制の強化や、日本再生加速プログラム（匿名化ガイドライン）など、プライバシーの安全利用に向けた規制が世界的に見直されつつあり、今後こうしたデータの保護と利活用を両立する技術が必須になってきます。

富士通研究所ではセンサーデータの収集から分析結果の利活用まで、プライバシーを保護する次に示す2つの技術を開発しました。

1. 部分復号技術

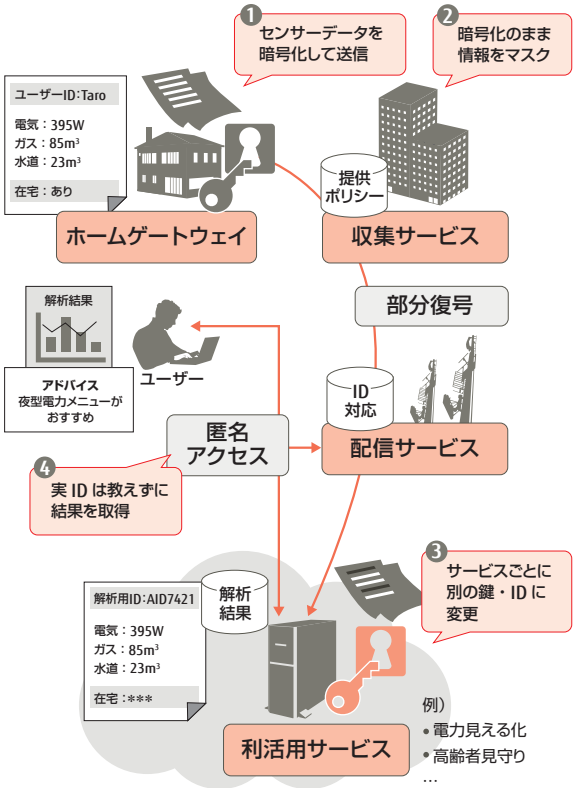
センサーデータを暗号化したまま、利活用サービスごとにユーザーIDを仮IDに変更したり、データをマスキングしたり、異なる暗号鍵に変更することを可能とする技術。

2. 匿名アクセス技術

ユーザーが利活用先に自分の実IDを知らせずに、仮IDのみでデータの分析を行い、その分析結果を取得できる技術。

これらにより例えば、ユーザーが一括してホームゲートウェイなどのセンサーデータを収集サービスに預け（❶）、エネルギー見える化や高齢者見守りといったサービスごとに必要なデータを安全に提供することができるようになります。センサーデータは、収集・配信サービスが連携して、暗号のまま加工して各利活用サービスに送ります（❷、❸）。利活用サービスではマスクされたデータに対し仮IDのまま分析を行い、その結果を利用者は匿名のまま取得することができます（❹）。

▼ 部分復号技術と匿名アクセス技術による安全なセンサーデータ利活用の例



標的型攻撃の出口対策技術

1. 出口対策が求められる背景

特定の組織や個人に対して、特別に作成したウイルスを添付し、興味を持ちそうな内容のメールを送りつける標的型攻撃と呼ばれるサイバー攻撃が脅威となっています。特に、アンチウイルスソフトなどのセキュリティ製品で検知されにくい巧妙な手口が用いられるため、侵入被害が長期間気づかれずに被害が拡大してしまったケースも報告されています。

これまでサイバー攻撃には、公開サーバへの対策が中心でしたが、今後は安全な領域とされていたイントラネット内部についてもセキュリティ対策が求められてきます。「攻撃者を決して侵入させない」ことも大切ですが、さらに「侵入されることを前提に、脅威はできる限り早期に検知して被害を最小限に抑える」という考え方が必要になります。これは、侵入されたコンピュータから外部への不審な通信リクエストを統制する出口対策の考え方です。

これまでの検知技術は、シグネチャとして登録された特徴的なキーワードでの識別や、有害サイトをブロックするWebフィルタリング技術（URLフィルタリング技術）を基に行っていました。しかし、利用形態の多様化と攻撃手口の巧妙化により、このようなやり方では正常通信との区別が困難になってきました。

特に、組織内に侵入した後、外部にあるサーバとの制御通信路を確立する新しいタイプのウイルスが日々多数出現してきています。URLや特徴的なキーワードによる対策では後追いとなってしまいます。さらに、ウイルスを特定するための情報が限定的なため、業務アプリケーションによる通信をウイルスによるものと誤検知してしまう問題があります。

そこで富士通研究所では、外部サーバとの通信が許可されているHTTP/HTTPSプロトコルを対象として、通信セッションの特徴に着目することで、従来の検知技術の問題を解決する3つの技術で「不正HTTP通信監視システム」の開発を行いました。

2. 不正HTTP通信監視システム

「不正HTTP通信監視システム」は、以下の3つの技術から構成されます。

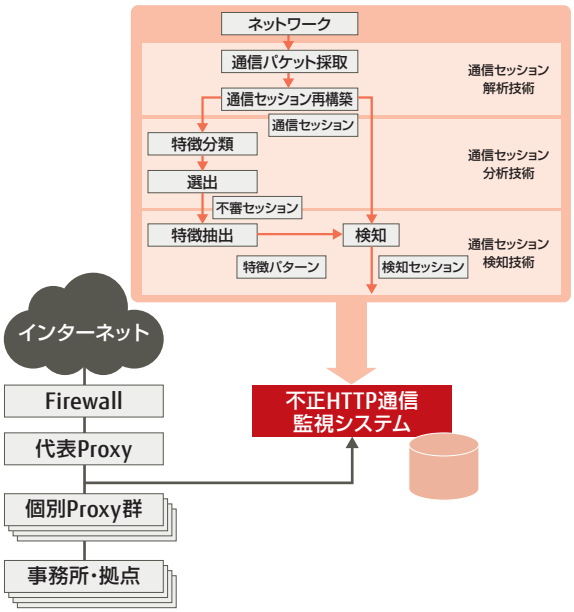
- 通信セッション解析技術
- 通信セッション分析技術
- 通信セッション検知技術

一つ目は、代表Proxyの前段で外部への通信パケットを収集し、サーバとクライアント間の一連の処理を通信セッションとして再構築する「通信セッション解析技術」です。

二つ目は、収集した通信セッションにおけるデータの流れ方の特徴を様々な指標で数値化する「通信セッション分析技術」です。これらの技術を用いて、組織内部から外部サイトへの通信状況を数か月以上にわたり観測し、その特徴の分析を行いました。

その結果、通常のWebサイトへのアクセスや特定の通信アプリケーションなどで、通信セッションにおける振る舞いにいくつかの異なる特徴があることを確認しました。この数値化された通信状況を統計的に処理することで、複合的な指標による相関関係を得ることができ、また、それをいくつかのグループに分類できることがわかりました。一方で、このような相関関係やグループから外れる不審な通信セッション群の存在を確認しています。これらのことから偽装により、一見通常の業務通信と区別がつかないような不正な通信であっても、通信セッションの一連の流れの振る舞いに着目することで、正規の業務通信とは異なる特徴を見つけられることがわかりました。

▼ 不正HTTP通信監視システムの概要



これらの独自の調査研究の成果を基に、三つ目の「通信セッション検知技術」を開発し、不正HTTP通信監視システムの試作を行いました。組織内ネットワークを模した仮想的な環境での検知実験を経て、現在は実環境にて試行稼働を行っています。

本研究により、従来は識別が困難であったウイルスによる外部サーバとの不正な制御通信を特定することが可能となりました。この監視システムは、従来の方式と比べて正常な通信を不正な通信と見誤る誤検知率を300分の1程度に向上することができます。

さらに、この監視システムを応用することで、ウイルスによる通信だけでなく、様々なアプリケーションによる通信をも検知することができるようになります。例えば、業務上許可されていないアプリケーション使用の有無が分かるので、組織内ネットワークにおけるコンプライアンスの遵守状況の監視にも有効な技術となります。

今後、組織内ネットワークを管理するセキュリティ管理者には、脅威が内部に侵入した形跡がないかの確認作業が求められてきます。この検知システムは、この確認作業に対する一つの有効な手段になり得ると考えています。

お取引先と連携した情報セキュリティ向上策

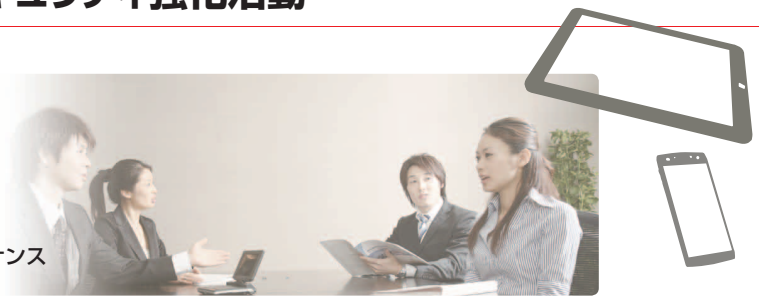
富士通グループの事業活動は、その付加価値の基となる様々なソフトウェア、サービス、物品、部材などを提供していただいているお取引先に支えられています。

この中にあって、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により長期的な信頼関係を構築し、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、ともに繁栄・存続していく共存共栄の関係を築いています。

富士通グループは、お取引先とともにサプライチェーン全体で「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の予防・再発防止策に関して教育、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。

2012年度の情報セキュリティ強化活動

1. お取引先選定
2. 教育・啓発
3. 状況確認
4. 事故対応支援
5. 状況評価
6. 情報の共有
7. 富士通グループのガバナンス
8. 海外のお取引先対応



お取引先における情報セキュリティ事故は、情報セキュリティルールの浸透、また、継続的なPDCAサイクルに基づく施策推進により、減少傾向にあります。

しかしながら近年、事業継続マネジメント（BCM）を契機とした外部サービス（クラウドサービスなど）、情報共有を目的としたソーシャル・ネットワーキング・サービス（SNS）の業務利用が増加し、また、そのインフラとしてスマートデバイスの急激な増加、ネットワークの多様化／高度化など、急激な技術変化、環境変化によって、情報漏えいのリスクが高くなってきています。

富士通グループでは、これらの最新のICT環境の変化を的確にとらえ、外部サービス／サーバ、スマートデバイスなどの新たな情報漏えいリスクを抑止するために、富士通グループとお取引先間の情報セキュリティに関する取り決めである「受託者用情報管理要領ガイドライン」を2012年10月に改定、適用し、継続的に情報セキュリティ強化施策の推進を図っています。

1. お取引先選定

新規のお取引先選定においては、候補会社の情報セキュリティ状況を確認とともに、業務委託時の情報セキュリティ管理、個人情報の取り扱いに関する要求事項について、契約で合意を得られるお取引先に限定しています。

また、既存のお取引先についても、定期的に個人情報保護法に基づき、個人情報委託先の選定を行っており、お取引先の情報セキュリティの管理監督を実施しています。

2. 教育・啓発

お取引先向け、情報セキュリティ研修会

2012年は、「受託業務の現場に即した、情報セキュリティ強化について」と題し、情報セキュリティインシデント事例の紹介と、常駐型プロジェクトやオフショア時の情報セキュリティ対策を中心に研修会を実施しました。

また、お取引先社内の啓発ツールとして当研修会資料を活用していただくことを目的に、合成音声によるナレーションを付加し提供しました。

- 2012年10月　約1,000社／約1,250名
  アンケートでは、約99%が有効と回答

お取引先向け、出前研修会

「情報セキュリティの最新動向と対策」と題し、お取引先よりの要請にて講師を派遣し、お取引先従業員向けの研修会を実施しました。

- 2012年度　約50社／約1,000名受講

お取引先新卒者向けワークショップ

主要なお取引先の新卒者向けに、社会人、企業人としての情報リテラシーの育成、および、ビジネスにおける情報セキュリティに関する基礎知識教育をワークショップ形式で実施しました。

- 2012年度　約40社／約150名

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として、情報セキュリティ事故時の報告書作成、また、情報セキュリティ事故が発生した要因分析、是正策の策定などをワークショップ形式で実施しました。

- 2012年度　約30社／約50名

3. 状況確認

富士通グループとお取引先間の基本契約に則し、定期的に、情報セキュリティ対策の状況確認を実施し、確認結果に基づいた是正計画の立案と、実施の指導および、是正結果の確認を行っています。

また、情報セキュリティ事故発生お取引先に対しては、是正勧告、是正の確認を実施しています。

さらに、依頼元などの要請にて、お取引先、プロジェクトなどの情報のセキュリティ要求事項を含めた点検を実施し、全てのお取引先に対して、１回／年、個人情報保護状況を含めた情報セキュリティ状況調査を実施しています。

- 2012年度監査　約140社

4. 事故対応支援

情報セキュリティ事故発生時に、お取引先を含む現場部門と連携し、漏えい情報の影響度調査などの初動調査および、是正対応支援を行っています。

5. 状況評価

情報セキュリティ状況確認、情報セキュリティ事故対応などの状況を基に、お取引先の情報セキュリティの状況を評価しています。

また、重大な問題が発覚した場合や、改善が見られない場合は、取引の見直しや新規発注停止なども必要に応じて実施しています。

6. 情報の共有

お取引先に情報セキュリティ管理責任者を設置し、また、富士通グループを含め、情報セキュリティに関する最新情報の共有をタイムリーに行っています。

- 最新の情報セキュリティ情報の共有を目的に2009年4月より「情報セキュリティの広場」と啓発ポスターを隔月に発刊し、2012年12月号では、年末年始の飲酒などに起因する盗難、紛失を抑止する啓発ポスターを提供しました。
- 「受託者用情報管理要領ガイドライン」の改定に伴い、「情報セキュリティハンドブック」「情報セキュリティ遵守状況チェックシート」「情報セキュリティ教育教材」を改版し、お取引先へ提供しました。

▼ 啓発ポスター

7. 富士通グループのガバナンス

富士通グループでは、お取引先の情報セキュリティ強化施策をグループ全体で推進しています。

各施策についてグループ内で連携し、また、情報セキュリティ事故事例などの情報を共有することにより、より効果的な予防施策を策定、共有し、お取引先に対して推進しています。

8. 海外のお取引先対応

開発費抑制／グローバル製品対応を目的とし、近年、海外取引先と連携したオフショア開発の機会が増加しています。

富士通では国内のお取引先と同様に、海外のお取引先とも、受託情報の取り扱いを規定した「受託者用情報管理要領」を取り交わし、情報セキュリティ維持に取り組んでいます。

2012年10月に、日本国内のお取引先向けの「受託者用情報管理要領ガイドライン」改定に合わせて、海外のお取引先向けに英語翻訳版を提供しました。また、中国のお取引先向けに「受托方情报管理规定指南」を改定し、適用しています。

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、以下の通りです。

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ソリューションズ
株式会社富士通アドバンストソリューションズ東海
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、以下の通りです。

富士通株式会社
株式会社富士通ITプロダクツ
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ソリューションズ
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
富士通コミュニケーションサービス株式会社
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
株式会社富士通ソーシアルサイエンスラボラトリ
株式会社富士通総研
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
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
富士通モバイルフォンプロダクツ株式会社
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、右の通りです。

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	AAAis
	明石システムセンター	AAAis
富士通エフ・アイ・ピー株式会社	横浜データセンター	AAAis
	中部データセンター	AAAis
	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

ITセキュリティ評価認証の取得状況

セキュリティ評価基準の国際標準であるISO/IEC 15408に基づいて、評価認証された代表的な製品は、以下の通りです。

- Systemwalker Centric Manager Enterprise Edition
- Systemwalker Operation Manager Enterprise Edition
- Symfoware Server Enterprise Extended Edition
- Interstage Application Server Enterprise Edition
- Interstage Security Director
- OS IV/MSPセキュアAF2
- IPCOM EXシリーズ ファームウェアセキュリティコンポーネント
- Si-R Security Software（ルータ、スイッチ）
- SR-S Security Software（ルータ、スイッチ）
- SafetyDomain（認証制御ソフトウェア）
- PalmSecure（手のひら静脈認証装置）

〔注〕詳細については、別途お問い合わせ願います。

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、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、右の通りです。

145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、右の通りで国内で最も多い資格者を有しています。

127名

富士通の安心安全ソリューション

富士通の安心安全ソリューション　SafetyValue

近年、企業は新たなリスクマネジメントの構築が求められています。その実現には、「選択と集中」を追い求める経営から「分散と共有」により事業の継続性を高め、同時に「効率性」を確保する経営への変革が必要です。富士通は、“サステナブルな経営へ”を理念に、ICTによりお客様の経営を支え続ける安心安全ソリューション「SafetyValue（セーフティバリュー）」を提供します。

富士通の「安心安全とは」

SafetyValueの特長

- お客様起点
  お客様の課題に対して、事業継続、セキュリティ、エネルギーの3つの観点で最適な解決策を提案します。
- 利便性向上
  お客様の資産を大切に守ると同時に、情報資産を効率的に活用できる環境を実現します。
- 環境貢献
  エネルギーの最適利用に向けて、多様なワークスタイルと効率的なマネジメントを実現するオフィス環境の構築を支援します。

SafetyValueのソリューション体系

SafetyValueはお客様の経営課題を起点に「事業継続」「セキュリティ」「エネルギー」の3分野を柱に構成されています。これにより、情報資産を安全かつ効率的に活用するための利便性向上、エネルギー最適利用と多様なワークスタイルを両立させるオフィス環境の構築を推進していきます。本報告書では、「セキュリティ」についてのソリューションをご紹介いたします。

▼ サステナブルな経営を実現する3つの柱

● 事業継続	事業継続計画の策定と対策、継続的改善活動を支援する運用管理まで含めた一貫したサービスを提供し、強力な事業継続対策を実現します。自社実践のノウハウと最新のクラウド・コンピューティング技術を活用し、お客様の事業継続の取り組みを強力に支援します。
● セキュリティ	仮想化やクラウド化などにより顕在化する新たなセキュリティリスクへの対応だけでなく、ICTによる業務改善・生産性向上など、ワークスタイルの変革を支える最適なソリューションを提案します。
● エネルギー	企業活動において事業継続やセキュリティとともに考慮が必要なエネルギー利用の効率化を、計画立案から見える化、ICTの改善までトータルな解決策を提案します。

ソリューションメニュー

▼ 情報セキュリティ14分野のソリューション（2013年4月）

セキュリティ	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。
セキュリティコンサルティング	情報セキュリティ基本方針の策定からマネジメントの定着まで、組織の情報セキュリティマネジメントの確立を総合的に支援。
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。
ピンポイントセキュリティ	特定目的のセキュリティ対策を簡単に導入いただくためのセキュリティ商品。

富士通株式会社
情報セキュリティセンター

〒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/

このカタログには、FSC®森林認証紙、植物油インキ、有害な廃液を出さない水なし印刷方式を採用しています。
©FUJITSU LIMITED 2013