富士通グループ
情報セキュリティ報告書
2014

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 2014

CONTENTS

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2014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、2014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」を中期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 2014」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

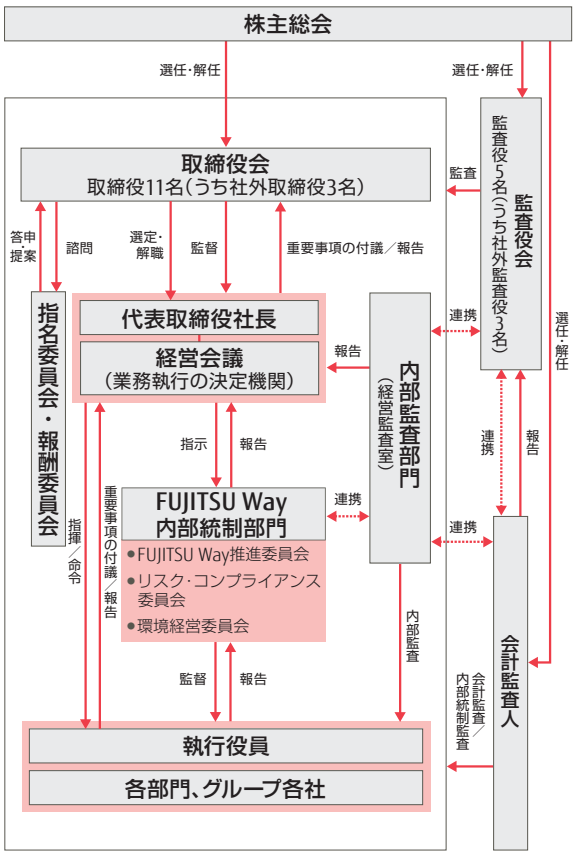
コーポレートガバナンス

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共に、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下、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共に、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共に、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・位置付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目指したグループ運営を行っています。

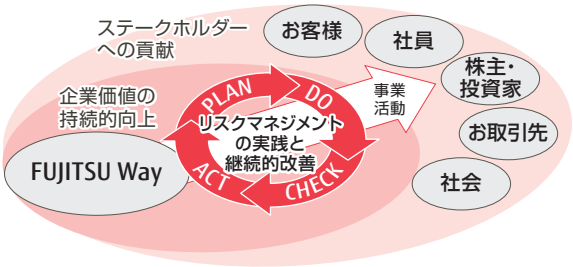
▼ コーポレートガバナンス体制図



リスクマネジメント

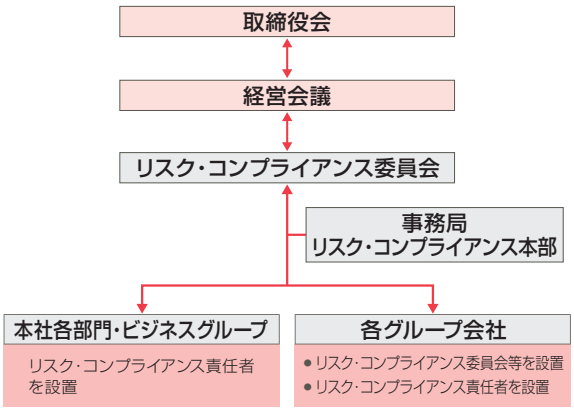
富士通グループは、グローバルなICT事業活動を通じて、企業価値を持続的に向上させ、お客様や地域社会をはじめとするすべてのステークホルダーの皆様に貢献することを目指しています。この目的の達成に影響を及ぼす様々なリスクを適切に把握し、その未然防止および発生時の影響最小化と再発防止を、経営における重要な課題と位置付けています。そのうえで、グループ全体のリスクマネジメントおよびコンプライアンスの体制を構築し、その実践を推進すると共に継続的に改善しています。

▼ 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。

また、富士通グループ各社は、「富士通グループ情報セキュリティ基本方針」の下に関連規定を整備し、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

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

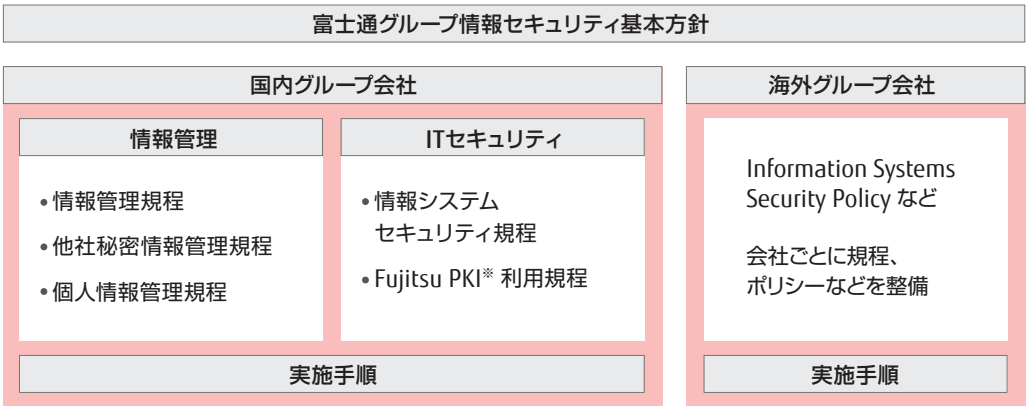
富士通グループは、次の事項を情報セキュリティへの取組みの原則とします。

(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2008年度から、「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PC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、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

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

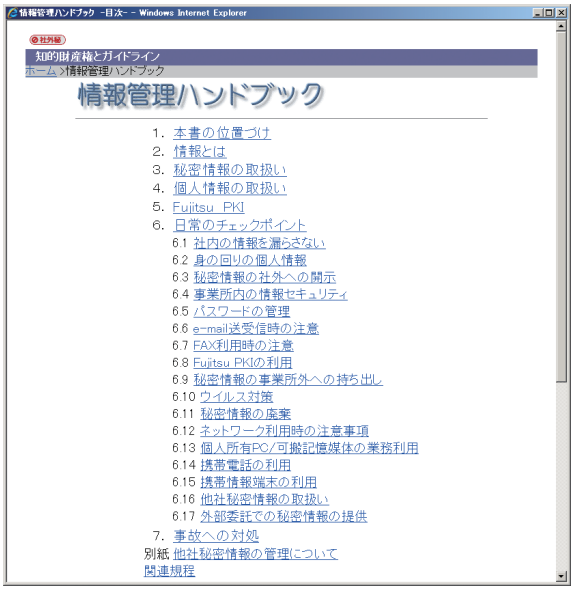
富士通では、「個人情報保護ポリシー」と「個人情報管理規程」を定めています。この規程に基づき、毎年、個人情報の取り扱いに関する教育や監査を実施するなど、継続的に個人情報保護体制の強化を図っています。

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、管理職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



2 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。

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

• 場面の設定　• 役割と責任の定義　• PDCAサイクルの確立

利用者の一元管理を実現する認証システム	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	ネットワークセキュリティ統制
セキュリティカードによる • 入室管理 • 認証 • 文書の決裁	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	• 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

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。

■ クライアント機器の社外での安全な使用

パソコ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、社外での機器の使用における注意事項の周知徹底は、毎月の「セキュリティチェックデー」や毎年行う情報セキュリティ教育の重要なテーマです。この場面でも、ICTによる追加の施策として、情報を持ち出さずに社外でクライアント機器を活用できる「仮想デスクトップサービス」という仕組みも導入して、重要な情報の保護に活用しています。

仮想デスクトップサービスでは、社外でクライアント機器を使用する場合、社内のネットワークにインターネットなどを通して接続し、社内のサーバにある情報や電子メールを、独立したクライアント機器を利用する場合と同じ操作で使用できます。また、クライアント機器に表示する社内の情報は、クライアント機器には保存できない仕組みにしています。自宅にある個人の機器からこの仕組みを使う場合にも、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しているため、業務情報の安全な管理が確保されています。

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

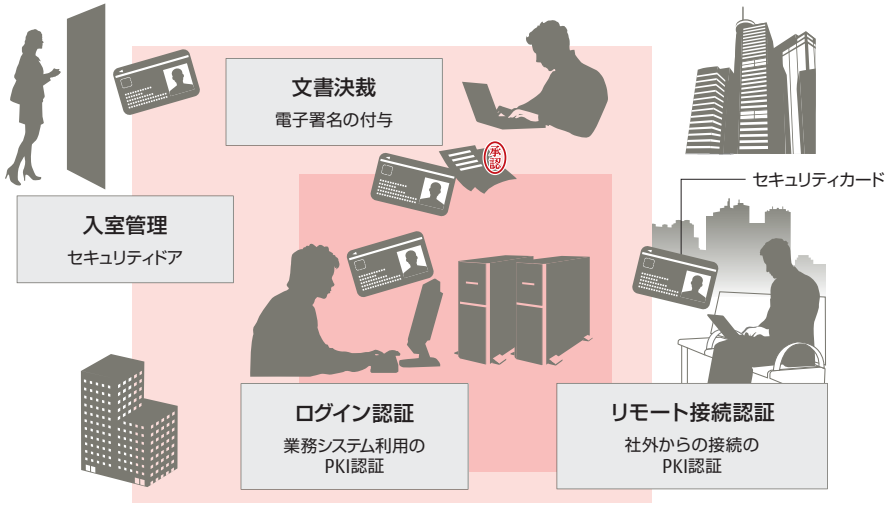
業務システムの利用にセキュリティカードが必要です。業務システムへのログインでPKIによる認証を行っているため、従業員の識別と認証が確実に行われ、しかも操作は容易です。

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ー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）
- 安定稼働のための性能管理、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
- 安定稼働のための性能管理、信頼性設計

ネットワークサービス利用の統制

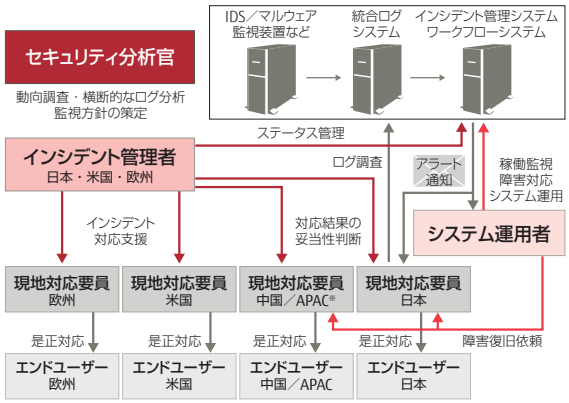
社外のインターネット環境にはファイル転送やオンライン会議などの様々なネットワークサービスがあります。これらについて、業務上の利便性や必要性と、クライアントセキュリティ統制が向上した現状を勘案して、制限を設けながら利用を認めています。他方では、情報漏えいにつながる恐れのある特定のネットワークサービスは、利用を禁止しています。また、誤使用を防止するために、このような通信を常時監視しています。

イントラネット利用の統制

富士通グループでは、「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。富士通グループでは、グループ会社をつなぐ一つのイントラネットを持っています。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ています。

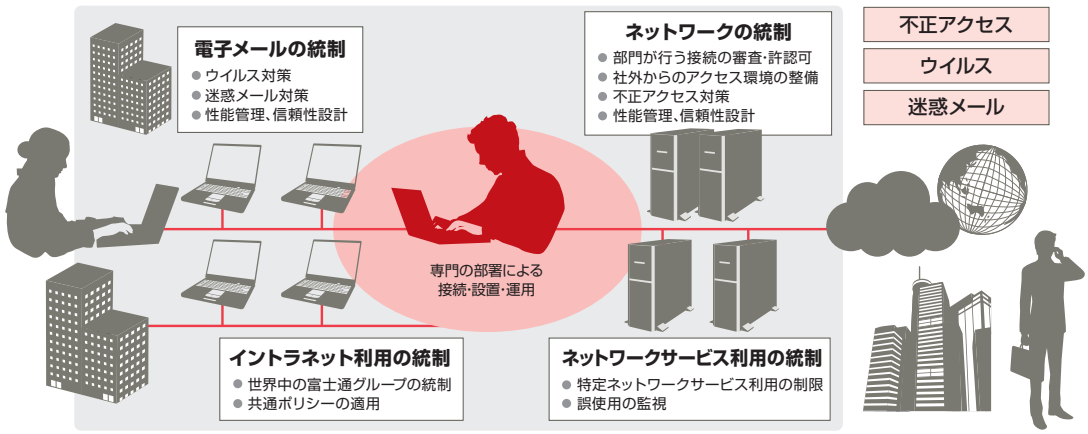
グローバルに一つのイントラネットを持っていることに対応して、ネットワークのインシデント対応も、専門組織であるSOC（Security Operation Center）によるグローバルな統制の下で行っています。一日に世界中のグループ会社で検知されるネットワークのアラートは、数億件にのぼります。これらのリスクレベルを判定し、インシデントとして扱う事象を特定し、これに迅速に対応します。その特徴は、次のとおりです。
- グローバルに統一したリスク基準と対応プロセス
- 大量の事象およびログの自動での判定
- 各地域に配置したSOC要員による、時差を活用した24時間の対応
- インシデント管理者やシス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。

3 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関係組織と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。

情報セキュリティ推進組織設立の考え方

高度化、多様化するサイバー攻撃の脅威やグローバルにおける各種ビジネス規制に対し、富士通グループ全体でその対策や対応方針を検討する必要が出てきました。

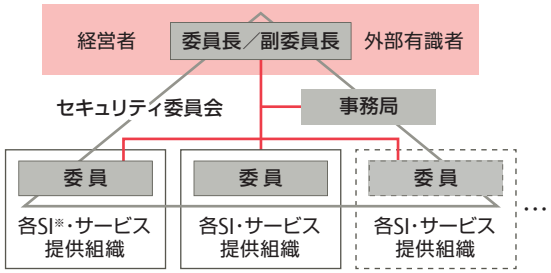
そこで、2013年にサイバーセキュリティに関する情報共有と当社ビジネス方針の討議を行うことを目的に、「セキュリティ委員会」を発足させました。

セキュリティ委員会は、システムインテグレーション・サービスビジネスの各事業を統轄する役員と、国内営業・マーケティング・海外ビジネス各部門の担当役員、第三者性を確保するため招聘した外部有識者とで構成しています。

サイバーテロの脅威と対策を始め、各国クラウドセンターが遵守すべき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。

また、セキュリティ委員会は、下部組織として富士通グループのセキュリティ活動の方向付けを行う、「情報セキュリティ施策推進会議」を持ちます。

▼ セキュリティ委員会体制



〔※〕SI：システムインテグレーション

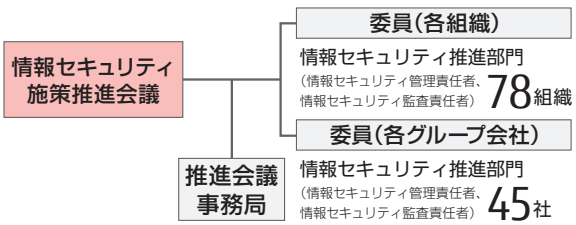
情報セキュリティ施策推進会議

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の下で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「情報セキュリティ施策推進会議」（以下、推進会議と略す）に参加しています。この参加組織は、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）を基礎として、セキュリティ計画の立案やセキュリティ対策の導入、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。

▼ 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「情報セキュリティ施策推進会議活動方針」を定めています。この活動方針に基づいて推進会議を設置し、情報セキュリティの維持・推進を図っています。また、四半期ごとに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が参加する推進会議の定例会と連絡会を開催しています。

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。

また、参加組織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、「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）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。

これら推進会議活動を通じ、参加組織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、活動方針に従い情報セキュリティ活動を推進し続け、参加組織自ら定める管理ルールに従い情報セキュリティのレベルを維持しています。

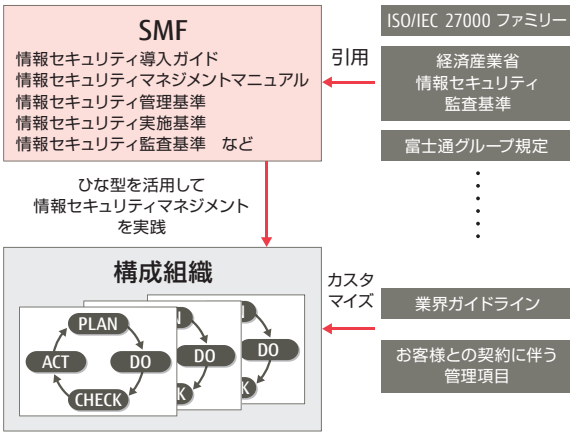
SMF（セキュリティマネジメントフレームワーク）

推進会議では、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。参加組織は、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、自組織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。

2013年度にISO/IEC 27001と27002が改版されました。これを受けて、国際標準と整合性を維持するためSMFを改版する予定です。

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」を実施しています。今までに管理者教育の受講者は614名となり、各組織・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に役立てています。また、2012年度からは管理責任者への継続的な自己研鑽と教育受講を促すため、e-Learning形式で開催し、既に588名が受講しています。

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1200名がこの教育を受講し修了しています。

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パスを推進するために、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。昨年までに137名が監査人資格の認定を受け、内部・外部監査で活躍しています。

管理者、監査人向け教育以外にも参加組織共通の情報セキュリティ教育の教材を提供し、各組織で活用しています。

ITインフラ標準運用サービスによるセキュリティ維持

推進会議では、情報セキュリティ対策実施の確実性・継続性向上のために「社内標準パソコン」を導入しています。

推進会議事務局内のインフラ運用サービス組織では、社員へパソコンの配布から、導入支援、日常運用、廃却まで、一連の機器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組織へ展開しています。

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組織の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

富士通グループでは、毎月「セキュリティチェックデー」活動をしています。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を確認しています。推進会議では、パソコンに情報セキュリティ対策診断ツール導入を義務付けて、セキュリティ対策の運用状態を診断しています。パソコン起動時に19の診断項目（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）を自動的に診断し、結果をパソコン画面に表示させています。また、各組織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ています。

スマートデバイスについては、グループ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、各参加組織で活用しています。

▼ 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

情報セキュリティ監査には、参加組織が自身で行う内部監査と推進会議事務局が参加組織に対して実施する外部監査があります。毎年実施している内部監査・外部監査を通して、参加組織は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、参加組織内で前述の「情報セキュリティ監査人教育」を修了した監査人が中心となり実施しています。外部監査は、推進会議内における外部監査と位置付け、毎年サンプリングで選定した被監査組織を第三者の観点で実施しています。

外部監査は、JASA監査人資格を有する、推進会議事務局と被監査組織に所属しない監査人で構成する監査チームが行います。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います。優れた施策(ストロングポイント)は参加組織のノウハウとして、前述の推進会議定例会と連絡会の場で事例紹介を行い、水平展開を行っています。

2012年度から外部監査は、現地監査に加えて、文書監査を併せて実施しています。推進会議事務局が毎年監査テーマを選定し、各組織の実施状況を確認することで、参加組織全体のセキュリティ向上を図っています。

このように異なる観点の監査を組み合わせ、毎年継続的に実施することにより、推進会議参加組織全体に対し情報セキュリティ維持・向上を図っています。

その他、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、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。特別監査は推進会議事務局の専門家が、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。

タブレット運用管理の社内実践

富士通グループでは、営業の新たなビジネスシーンの発掘と新しい拡販モデルを模索するために、「ワークスタイル変革」としてタブレットの利用促進を図っています。

タブレットは従来のノートパソコンなどに比べてセキュリティ上のリスクが高く、利用者には一段高いセキュリティ意識が求められます。そこで、セキュリティを維持しつつ利便性を損なわないよう個別の運用ルールを策定し、認定制度の施行を特定組織にて開始しました。

利用者は、情報セキュリティルールに留まらず、タブレット保有の主旨・目的、ICTスキル、知的財産、SNS※活用方法など運用に必要な知識やスキルの取得を求められます。そこで、教育とテストを受講させて、一定レベル以上のスキルが担保できた者を対象にタブレット利用を認めています。利用者には、一年ごとに上記スキルを確認し続けることで、継続的なセキュリティ維持・向上を求めています。万一、セキュリティ事故を発生させた利用者には、適切な教育とテストを課し、再度セキュリティ意識を持って運用できるよう指導を行います。

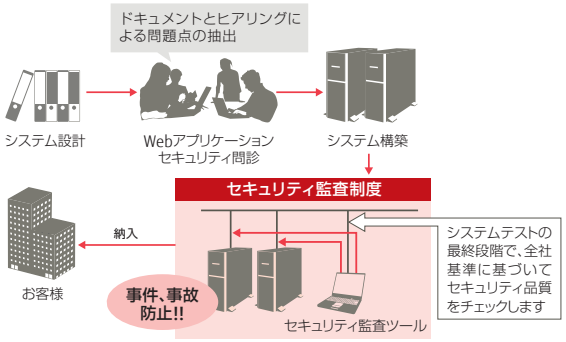
また、モバイルデバイス管理ツールを活用し、タブレット運用事務局が全タブレットのセキュリティ対策の最新状態を確認しています。

〔※〕SNS : Social Networking Service

お客様納入システムのセキュリティ監査

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」および「セキュアWebガイド」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、この2つのガイドライン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グループ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。

4 サービスにおけるセキュリティ品質向上への取り組み

インターネット上でご提供するサービスをはじめとして、お客様にサービスを安心・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積極的に取り組んでいます。

ガイドラインと対策基準の整備、監査への取り組み

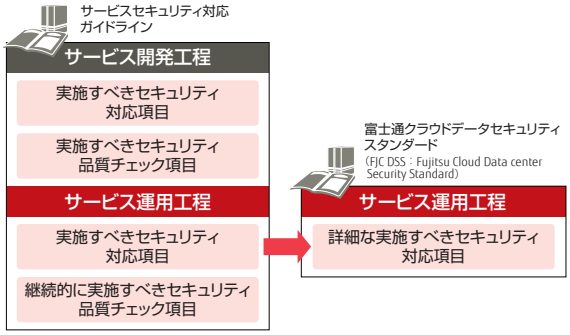
富士通では、お客様にご提供するサービスのセキュリティ品質を確保するため、サービス開発工程とサービス運用工程で実施すべき事項を、「サービスセキュリティ対応ガイドライン」としてまとめています。各サービスを提供する部門では、このガイドラインで示した内容に基づき、右図に示すセキュリティ対策を実践することで、セキュリティ品質を確保しています。

また、サービスを開始する前に、監査部門がセキュリティ対策の実施状況を監査することで、セキュリティ品質が確保されていることを担保しています。

サービス運用においては、セキュリティ対策事項をより詳細に記載したクラウドをはじめとするサービス向けのセキュリティ対策基準である「富士通クラウドデータセキュリティスタンダード」（FJC DSS）を定め、遵守するようにしています。このFJC DSSは、国際的なセキュリティスタンダードと、お客様のセキュリティ要件、さらに、富士通のクラウドプラットフォーム運用の経験で培った技術を加味して富士通が独自に策定し、社内実践しているセキュリティ対策基準です。

また、セキュリティ品質が確保できているか継続的にチェックするために、セキュリティ監査部門によるセキュリティ定期監査を実施し、必要があれば是正することで一定のセキュリティ品質の確保、向上を継続的に実現しています。

▼ ガイドラインと対策基準の整備



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）」なサービスを継続的に提供するために、富士通は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」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。

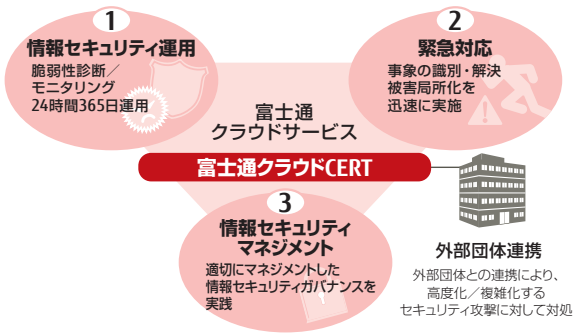
富士通クラウドCERTは、クラウド環境を各種のセキュリティ脅威から守り、お客様のビジネスを支えるために、グローバル規模で以下のような活動を行っています。

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、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。

また、現在は既知の脆弱性が存在しない環境であっても、新たな脆弱性が日々発見されています。そこで、定期的なセキュリティ脆弱性診断を実施することにより、脆弱性を客観的に発見し、対処しています。さらに、継続的な脆弱性情報監視と、タイムリーなパッチ適用などでインシデント発生の予防に注力し、リスクコントロールを実施していることが、この活動の大きな特長です。こうしたトータルなセキュリティ対策の継続的な実施により、セキュリティ品質向上に取り組んでいます。

▼ 富士通クラウドCERTの活動



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。

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、「FUJITSU Cloud IaaS Trusted Public 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「富士通クラウドセキュリティ対策基準による富士通の取り組み」を公開しています。

〔※〕富士通のパブリック型（IaaS）のクラウドサービス。

●●コラム●●

サイバー攻撃に対応する“対症療法”と“原因療法”、そして“予防対策”とは

最近、インターネット公開サーバを、高度化するサイバー攻撃から守るにはどうしたら良いかという相談を受けることが数多くあります。公開サーバの管理を怠ると、気付かないうちに情報を窃取されたり、ウェブサイトを改ざんされたりするほか、サーバがサイバー犯罪の「踏み台」にされ、攻撃に加担させられることがあります。こうなると、企業としての評判を落とし、信頼の失墜につながってしまいます。公開サーバは、世界中の誰とも知らない者からの攻撃を、いつ受けるかわからないということを考慮しておかなければなりません。では、公開サーバに必要なセキュリティ対策とは何でしょうか。

まず、多くの方が真っ先に挙げられるのは、ファイアーウォールやIPS※1、WAF※2の導入です。また、最近では通信データ内のアプリケーションを識別し制御する「次世代ファイアーウォール」もあるでしょう。こうした、攻撃そのものを水際で防御する手法は、即効性があり、限定的な範囲では、とても効果的な対策といえます。しかし、これらはあくまで“対症療法”※3と位置付けられ、中長期的観点で考えると良策にはなり得ません。

次に考えられる対策は、“原因療法”※4です。アプリケーション・レイヤーにおけるWeb脆弱性診断（ブラックボックス・テスト）、およびWebアプリケーションのソースコードを直接チェックするソースコード・レビュー（ホワイトボックス・テスト）により、脆弱性が存在する箇所を突き止め、その脆弱性を改修することが、原因療法です。短期的には工数や対処費用が増大しますが、中長期の観点で見れば効率的な対処と言えます。

最後に、サイバー攻撃の対応で肝心なのは予防対策です。Webアプリケーション開発を例にとると、開発者がセキュアな設計やコーディングを徹底することです。これを、「脆弱性の作り込み防止」といいます。開発の上流工程でセキュアな設計からはじめることが、トータルコスト低減につなげられます。予防対策の重要性は最近特に着目され、取り組みの優先順位も上がってきています。

■ 対策別の特長

	即効性	効果	トータルコスト パフォーマンス
対症療法	高	中	低
原因療法	中	高	中
予防対策	低	高	高

サイバー攻撃に対応する現場では、新たな脅威や脆弱性が日々発生するため、継続的な活動が必要です。また、攻撃手法が日々高度化する中で、当初は脆弱では無かった設計でも後々脆弱だと指摘されることもあります。公開サーバに対するセキュリティ対策とは、まず、開発の上流工程からスタートさせる「脆弱性の作り込み防止」（予防対策）を確実に実施することです。そして、公開後の運用工程では、継続的な脆弱性情報監視など（予防対策）に加え、IPSやWAFのリアルタイムでの脆弱性コントロール（対症療法）と定期的な脆弱性診断・対処（原因療法）を組み合わせ、継続的に実施することです。予防を実施した上で、現実に起きている攻撃を防御しつつ、真の原因解消を並行して進める、短期と中長期の観点をバランスよく持つことが重要となります。

〔※1〕IPS：Intrusion Prevention System
〔※2〕WAF：Web Application Firewall
〔※3〕対症療法とは、通常は医療の現場で使用される言葉であり、対処すべき病気などにおける症状を緩和や、回避する為の治療方法であるとされています。
〔※4〕原因療法とは、表面的な症状に対応するのでは無く、根本的な原因を究明し取り除く治療方法とされています。

5 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。

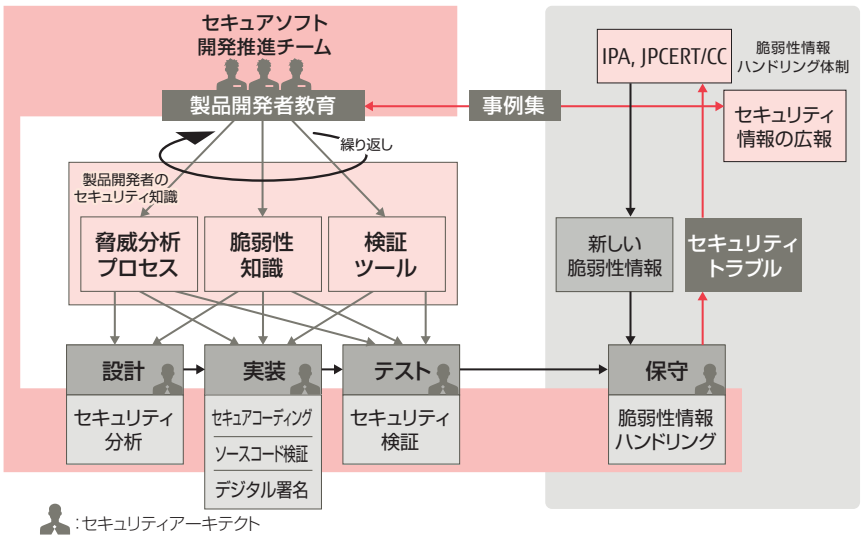
ソフトウェア製品のセキュリティ品質向上への取り組み

富士通では、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。

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



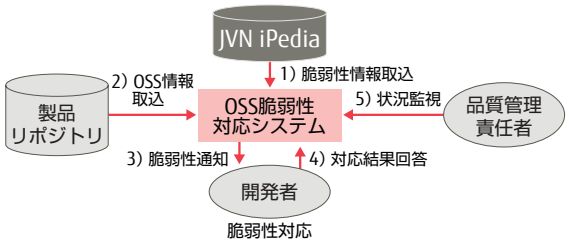
オープンソースソフトウェアを利用した出荷済製品のセキュリティ確保の活動

「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。

▼ OSS脆弱性対応システムの概要



〔※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。

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）

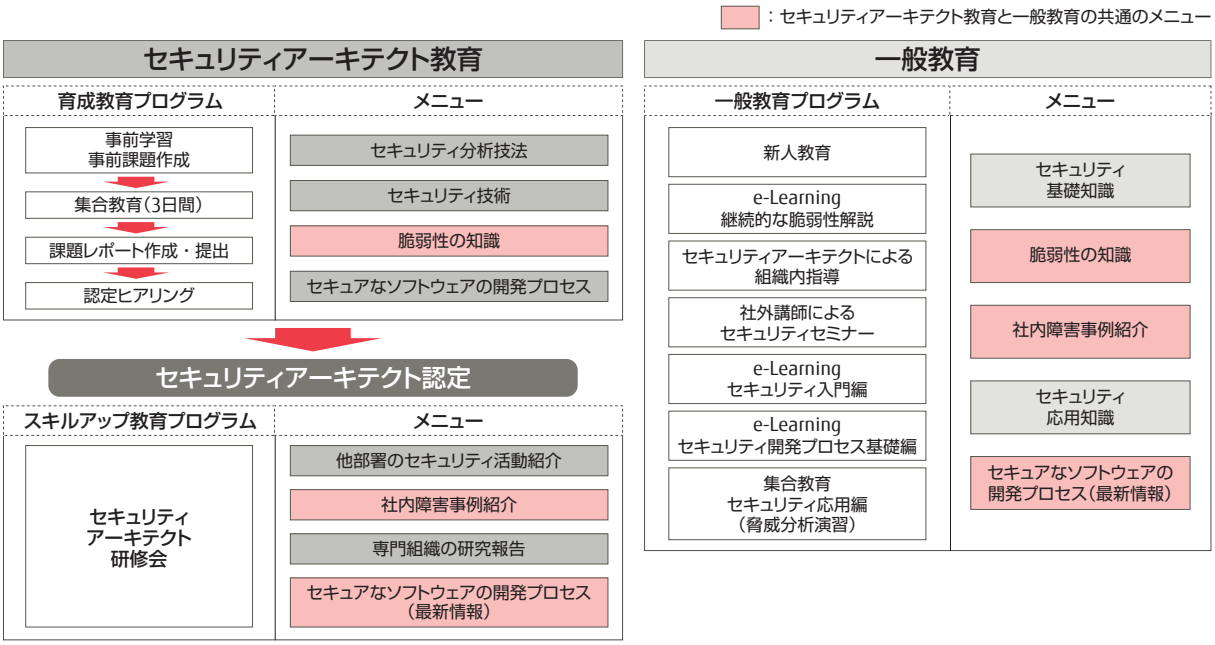
研修会を通して、個々のスキルアップや知識の更新を図ると共に、意見交換や情報交換が行われることにより、セキュリティアーキテクト同士の意識啓発を図っています。

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。

脆弱性やセキュアなソフトウェ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



6 安全な暮らしを支えるセキュリティ技術の研究開発

複雑化、高度化するサイバー攻撃に的確に対処しながらパーソナル情報をはじめとする様々な情報の保護と利活用を同時に実現できる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、最先端の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、セキュリティ研究を推進しています。その範囲は、例えば、暗号化したまま演算処理や検索ができる準同型暗号や静脈認証などの要素技術から、プライバシー保護やサイバー攻撃対策などのシステムセキュリティまで広く、研究成果は、当社が提供する製品やサービスのセキュリティ向上に大きく貢献しています。

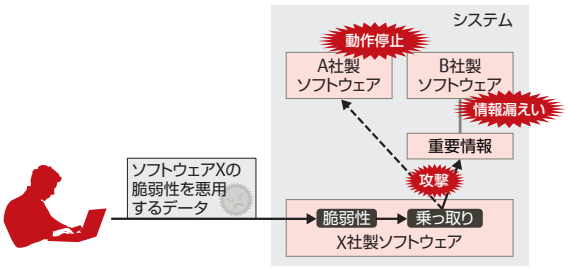
本報告書では、製品やシステムの脆弱性をなくすためのファジングを用いた新しい検査手法と、生体認証において必要に応じて生体情報をキャンセルできる新しいバイオコード技術をご紹介します。

システムに潜む未知脆弱性の評価・検出技術

安心できるICTシステムを実現するために

現代の企業においてサイバー攻撃は、経営上の大きな課題となっています。多くのサイバー攻撃は、ソフトウェアの脆弱性を悪用して攻撃を仕掛けてきます。そこで、富士通研究所では、ソフトウェアに含まれる未知の脆弱性を効率よく検出し、対策可能にする技術について研究開発を行っています。

▼ ソフトウェアの脆弱性を悪用する攻撃の例



ファジング手法による未知脆弱性評価技術

ファームウェアからWebアプリケーションまで多層なソフトウェアで構成されるシステムは、脆弱性対策が不十分なソフトウェアを組み込んでしまったり、システムを長期運用すると、開発時点では想定していなかった新たな技術により脆弱性が発現してしまうことがあります。

現在、このようなシステムの脆弱性を検出する技術として、攻撃者の「攻撃」を製品開発時に「評価」として実施する「ファジング手法」が注目されています。

ファジング手法は、ブラックボックステストの一種で、「ファズ（fuzz）データ」と呼ばれる開発者が想定しない評価データを評価対象に入力し、状態変化を監視することにより脆弱性を検出する手法です。

ファジング手法では十分にテストケースを考慮しておかないと評価データ数が無限になり、現実的な時間で評価できないという課題がありました。

そこで、富士通研究所では以下の技術を開発しました。

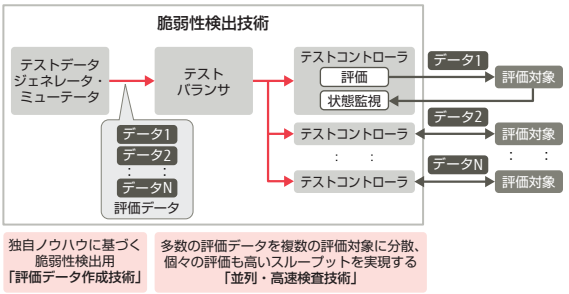
1. 評価データ作成技術

評価対象に通常運用時に入力されるデータの構造を自動解析、分割した複数のパートに対しバッファオーバーフローや整数オーバーフローといった脆弱性を発現する可能性の高い評価データを作成します。富士通研究所が従来から脆弱性を多数検出してきた独自ノウハウを活かした評価データを作成することにより、評価データ数を現実的な時間で評価可能なレベルにまで削減することを可能にしました。

2. 並列・高速検査技術

多数の評価データを複数の評価対象に分散して同時に検査、さらに高いスループットの検査処理を実現する実装により、限られた開発期間内での脆弱性検出を可能にします。

▼ ファジング手法による未知脆弱性検出技術の概要



本研究を採用したファジングテストツールはすでに稼働しており、富士通で開発中の複数の製品の脆弱性を検出し製品出荷前の対策を実現しました。 さらに現在のICTシステムでは他社のネットワーク製品を含む場合があることから、他社製品についても評価しており、複数製品で未知脆弱性を検出、開発元へ改善のための報告を実施しています。

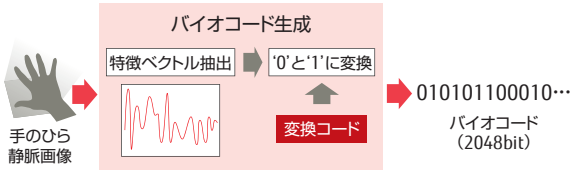
バイオコードによる生体認証技術

バイオコード技術と開発の背景

近年、本人を確認する技術として、生体認証技術の普及が進んでいます。生体認証は、身一つで本人認証が行える一方で、認証に用いる生体情報は変えられないため、より慎重に取り扱う必要があります。生体認証の利用をさらに拡大するために、認証システムで生体情報をより簡単に取り扱える技術が求められていました。

富士通研究所は、手のひら静脈画像から特徴を2048bitのバイオメトリック・コード（以下、バイオコードと記す）として抽出して高精度に照合する技術を開発しました。従来適用していた静脈特徴パターンを比較する照合処理の代わりに、静脈画像から'0'と'1'で表されるバイオコードを生成して比較計算による高速な照合を実現しています。

▼ 生体情報からの特徴コードの抽出



この技術では変換コードを変えて1つの生体情報から複数のバイオコードを生成することが可能です。例えば登録したバイオコード情報が漏えいした場合でも、新しいバイオコードを生成して再登録して利用することができます。このバイオコードは他人受入率1/10万レベルの識別性能を持っています。バイオコード間の照合時間はPCで従来技術の数ミリ秒から約1μ秒に短縮可能であり、データサイズはICカードやQRコードでの利用を考慮して2048bitとしました。データサイズは、識別性能に合わせて変更することも可能です。

このような1つの生体情報から複数の生体特徴情報を生成する技術は、「キャンセラブルバイオメトリクス」あるいは「リニューアブルバイオメトリクス」と呼ばれ、プライバシー保護が先行するEUを中心として研究が行われてきました。しかし、センサで取得される生体情報が毎回全く同じではなく、撮影条件や入力条件により変動することから、識別性能は他人受入率1/1000程度と、従来のパターンマッチングや画像特徴を用いた場合の他人受入率1/10万～1/100万程度と大きな差がありました。

開発した技術

今回、「手のひら静脈画像を正規化する技術」と「バイオコード抽出技術」の2つの技術を開発し、手のひら静脈認証における登録処理と照合処理で適用しました。

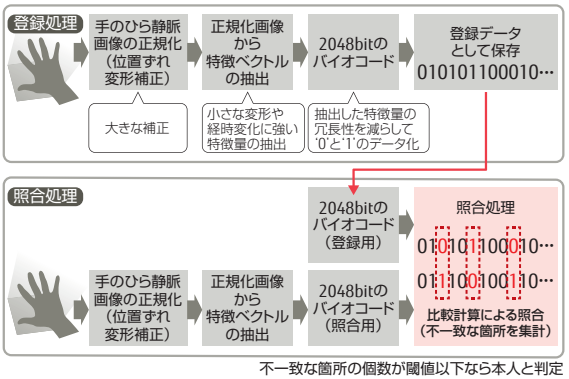
1. 手のひら静脈画像を正規化する技術

手のひら静脈画像の画像正規化では、手の輪郭情報を用いて手のひら静脈画像の位置補正や形状補正を行い、センサで取得された手のひら静脈画像を一定の位置と形に置かれた静脈画像のように変換します。

2. バイオコードの抽出技術

バイオコードの抽出処理では、手のひら静脈画像を分割し、分割した各領域から静脈パターンの特徴ベクトルを抽出します。抽出した特徴ベクトルから情報量削減の技術を用いて最終的に2048bitのバイオコードを生成します。また、抽出されたバイオコードから元の画像を類推することは困難です。

▼ バイオコードによる手のひら静脈認証の概要

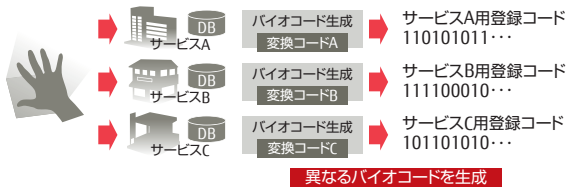


不一致な箇所の個数が閾値以下なら本人と判定

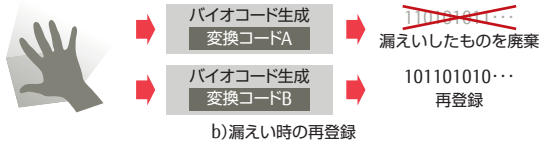
効果と想定適用例

バイオコード生成時の変換コードを変えることにより、1つの手のひら静脈画像から多数のバイオコードを生成できるため、あたかもパスワードを変えるように利用することができます。サービスごとに別々のバイオコードを登録することができるため、利用者は、より安心して手のひら静脈認証を利用することが可能です。バイオコード技術を用いての生体認証システムのさらなる利用拡大先として、インターネットアクセス、店舗決済など様々なサービスや場所での利用を想定しています。

▼ 本技術を利用した生体認証サービスの適用イメージ



a）サービスごとに異なるバイオコードを登録して利用可能



b）漏えい時の再登録

今後は実用化を目指して、画像正規化技術の強化とバイオコード抽出技術の高精度化を進め、実証実験などを行いつつ生体認証の利用シーンへの適用を検討していきます。

7 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で長期的な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の予防・再発防止策に関して、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。

2013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、情報リテラシーが低い利用者や脆弱な機器・サービスを狙い、情報を窃取するなどの新たな脅威が懸念されています。

富士通グループでは、ICT環境の変化を的確にとらえ、スマートデバイス／外部サービス／サーバに対する標的型攻撃など、新たな情報漏えいリスクを未然に抑止するため、教育・啓発活動などを通じ、新たな情報セキュリティ施策の企画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、個人情報保護法に基づいた個人情報委託先の選定を行い、情報セキュリティの管理監督を定期的に実施しています。

2. 教育・啓発

■ お取引先向け情報セキュリティ研修会

2013年は、「最新の情報セキュリティ事情と対策」と題し、以下のように、最新ICTにおける脅威と対策を中心とした研修会を実施いたしました。

- スマートデバイス
- ソーシャル・ネットワーキング・サービス（SNS）
- 外部サービス／サーバ
- オフショア開発
- 標的型攻撃
- BYOD（Bring Your Own Devices）など

● 2013年度　約1,000社／約1,200名受講
（東京、大阪、名古屋、福岡など）

また、お取引先社内の啓発ツールとして活用していただくため、合成音声によるナレーションを付加した資料を配布し、好評を博しました。

■ お取引先向け出前研修会

2013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。

● 2013年度　約40社／約1,200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、社会人としての情報リテラシーを高めるため、身近なスマートフォンにまつわる情報セキュリティ事故を例にあげ、情報セキュリティに関する基礎教育のワークショップを実施いたしました。

● 2013年度　約40社／約200名（東京、大阪）

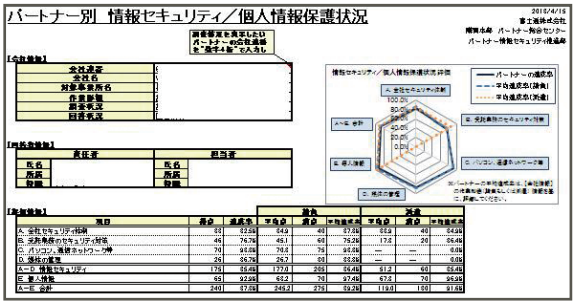
■ お取引先リーダ向けワークショップ

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。

- 2013年度　約50社／約60名（東京、大阪）

3. 状況確認

お取引先に対し、富士通グループとの基本契約に則し、情報セキュリティ対策の状況確認を定期的に実施しています。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。


パートナー別　情報セキュリティ／個人情報保護状況

また、情報セキュリティ事故が発生したお取引先に対する是正勧告、是正確認も実施しています。

さらに、全てのお取引先に対し、年1回、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。

- 2013年度監査　約130社
- 2013年度状況調査　約1,500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を基に、お取引先の情報セキュリティ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いただき、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、ご相談対応などをタイムリーに実施しています。

- 2009年4月より、「情報セキュリティの広場」と「啓発ポスター」を隔月で発行し、情報セキュリティに関する最新情報の共有・啓発を、お取引先に対して実施しています。

▼ 2013年11月発行

「情報セキュリティの広場」「啓発ポスター」

7. 富士通グループのガバナンス

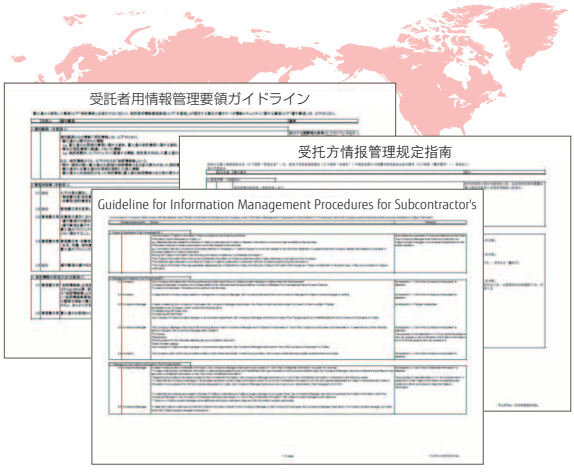
富士通グループ全体で、お取引先に対する情報セキュリティ強化施策を推進しています。

グループ内で、情報セキュリティ連絡会などを四半期ごとに開催し、情報セキュリティ事故の事例などを共有、より効果的な予防施策を策定・推進しています。

8. 海外のお取引先対応

近年、開発費の抑制やグローバル製品への対応を目的とし、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、海外のお取引先（英語圏、中国）に対しても、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、国内と同レベルの情報セキュリティ施策を推進すると共に、カントリーリスクの把握と対応に取り組んでいます。



8 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
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
バンキングチャネルソリューションズ株式会社
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。

〈148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。

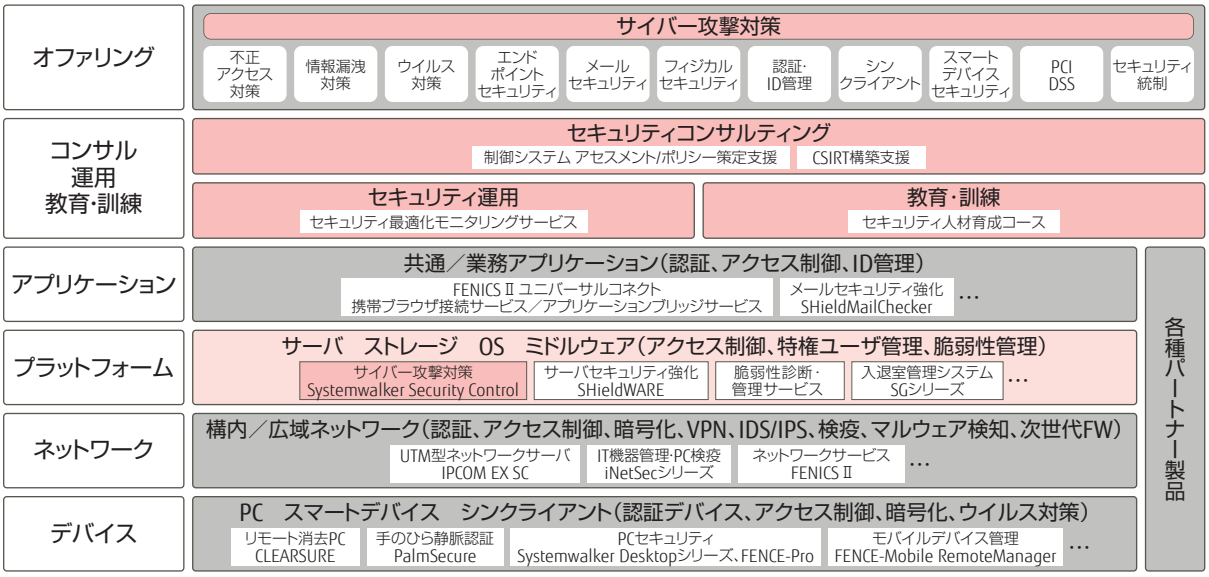
〈137名〉

9 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、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/