富士通グループ
情報セキュリティ報告書
2019

shaping tomorrow with you

社会とお客様の豊かな未来のために

目次
編集方針

編集方針

富士通グループは、グローバル ICT（Information and Communication Technology）企業として安心・安全なデジタル社会を実現するために、情報セキュリティの維持とさらなる強化をしていくことを重要な社会的責任と捉えております。

2009 年より制作を開始し、今回で 11 冊目となりました。従来からの施策に加え、社会の動向に合わせたさまざまな施策を展開しております。

富士通グループのセキュリティに対する取り組みをご理解していただき、さらに皆様のセキュリティ向上につながればと願っております。

ぜひご一読いただけると幸いです。

■ 報告対象期間

2018 年度（2018 年 4 月 1 日 ～ 2019 年 3 月 31 日）の活動を基本的な報告対象期間としています。ただし、それ以外の期間の活動も一部含みます。

■ 報告対象組織

富士通株式会社および連結子会社 411 社（海外を含む）を報告対象組織としています。

■ 参照した資料

経済産業省「情報セキュリティ報告書モデル」

■ 報告書発行時期

・日本語版：2019 年 6 月
・英語版　：2019 年 8 月

私たちはこれまでの経験と ICT の力で、お客様とともに「豊かで夢のある未来」の実現を目指しています

富士通株式会社
最高情報セキュリティ責任者（CISO）
安井三也

富士通グループは、人々がテクノロジーやデータを活用することにより、豊かで持続可能な社会の実現を目指しています。現在の複雑化したデジタル社会において、私たちが掲げている未来の社会ビジョン「ヒューマンセントリック・インテリジェントソサエティ」はますます重要性が増してきています。

デジタル技術の進歩により、あらゆるモノやデータがつながり数多くのイノベーションが生み出された結果、私たちの日々の生活は豊かで便利になりました。しかし、その一方で、日々高度化、巧妙化するサイバー攻撃は深刻な脅威となっています。また、個人情報の漏えい不正利用のリスクも高まる中、データやテクノロジーならびにそれらを使ってビジネスを行う企業に対する信頼は大きく揺らいでいます。ビジネスや社会の信頼をどのように再構築するかという事が、より良い未来を導くための最重要課題となっています。

富士通グループは「Human Centric Innovation: Driving a Trusted Future」をテーマに掲げ、デジタル社会におけるデータの信頼性を保ちながら、情報の保護に努めています。さらに情報漏えいを防止するため、情報セキュリティを一層強化し誰もが安心・安全に暮らせるトラステッドな（信頼性のある）未来を築いていきます。

富士通グループのセキュリティに対する具体的な取り組みとしては、最高情報セキュリティ責任者（CISO）を設置し、迅速かつ的確な情報セキュリティにおけるマネジメント体制を整え強固なものにしています。情報セキュリティ対策では、サイバー攻撃の脅威を最小化するために多層防御による仕組みを強化するとともに、セキュリティを維持するための適正な運用管理を継続しています。さらに、ネットワーク・情報機器の監視については、インテリジェントなセキュリティ技術の強化を進めており、独自の AI 技術「Deep Tensor」を使った分析による取り組みを行っています。

この「情報セキュリティ報告書 2019」では富士通グループにおける情報セキュリティについて紹介しています。また特集では、より安全なセキュリティと利便性を向上するための手のひら静脈認証を活用した入退出管理について掲載しています。

私どもの情報セキュリティの取り組みについてご理解いただき、皆様のお役に立てれば幸いです。今後も、グループの理念である FUJITSU Way に則り、強いデジタル技術をベースとする「サービスオリエンテッド・カンパニー」として、トラステッドな未来をお客様と共創していきます。

ぜひ、ご覧いただきますようお願い申し上げます。

※富士通グループの理念・指針「FUJITSU Way」: https://www.fujitsu.com/jp/about/philosophy/

基本方針

富士通グループ情報セキュリティ基本方針

ICT を基幹事業とする富士通グループでは、「快適で安心できるネットワーク社会づくり」への貢献を企業理念に掲げ、グループ全体の情報セキュリティを確保しながら、ICT 製品およびサービスの提供を通じたお客様の情報セキュリティの確保とそのレベルアップに努めています。

2016 年 4 月には、こうした考えを富士通グループ全体で共有し、従業員一人ひとりが行動していくことを目指し、「富士通グループ情報セキュリティ基本方針」を取締役会に直属するリスク・コンプライアンス委員会の先導の下策定しました。この基本方針は、2015 年 12 月に経済産業省および独立行政法人情報処理推進機構（IPA）が策定した「サイバーセキュリティ経営ガイドライン」に準拠しています。

また、一般社団法人日本経済団体連合会（以下：経団連）が 2018 年 3 月に公表した「経団連サイバーセキュリティ経営宣言」※ について、「富士通サイバーセキュリティ宣言」(2016 年 11 月公表) と理念を同じくするものとして、富士通グループはこの経団連の宣言を支持しています。

富士通グループは ICT のリーディングカンパニーとして、積極的な研究開発によって最新のテクノロジーを育み、それらが組み込まれたさまざまな ICT ソリューションの提供を通じて、お客様のみならず社会全体のサイバーセキュリティの確保に貢献します。

※ 経団連サイバーセキュリティ経営宣言（経団連ホームページへのリンク）
http://www.keidanren.or.jp/policy/2018/018.pdf

富士通グループ情報セキュリティ基本方針（抜粋※）

（グローバルセキュリティポリシー）

I. 目的

本情報セキュリティ基本方針（以下、「本基本方針」）は、経済産業省が策定した「サイバーセキュリティ経営ガイドライン」を踏まえ、富士通グループにおける情報セキュリティを確保するための対策、体制等の基本事項を定めるとともに、富士通グループが、ICT を事業の根幹としていることに鑑み、グループ全体の情報セキュリティを確保しながら、製品およびサービスを通じてお客様の情報セキュリティの確保・向上に積極的に努めることを内外に宣言し、もって FUJITSU Way に掲げる企業理念を実践することを目的とします。

II. 基本原則

(1) 富士通グループは、その事業において、お客様またはお取引先である個人および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、研究開発および人材育成に努め、お客様の情報セキュリティの確保・向上に資する製品およびサービスを適時かつ安定的に提供することにより、お客様、ひいては社会の持続的発展に寄与します。

※ 富士通グループ情報セキュリティ基本方針（全文） https://www.fujitsu.com/jp/imagesgig5/InformationSecurityPolicy.pdf

マネジメント体制

情報セキュリティマネジメント体制

富士通グループでは、昨今のサイバー攻撃の増加を受けて、2015 年 8 月にリスク・コンプライアンス委員会の下に最高情報セキュリティ責任者（CISO: Chief Information Security Officer）を設置しました。従来、最高情報責任者（CIO: Chief Information Officer）が担っていた情報セキュリティにおけるマネジメント責任を分離し独立させ、情報セキュリティ管理に専任･特化した責任者を置くことで、増加･巧妙化するサイバー攻撃へのリスク対策を迅速かつ的確にマネジメントする体制を整えました。

また、グローバルな情報セキュリティマネジメント体制の強化を目指して、CISO の傘下に世界各リージョン最高情報セキュリティ責任者（リージョナル CISO）を設置しました。米州・EMEIA・オセアニア・アジア・日本の 5 つのリージョンにおいて ICT ビジネスを支えるグローバルな情報セキュリティガバナンスを強化しています。

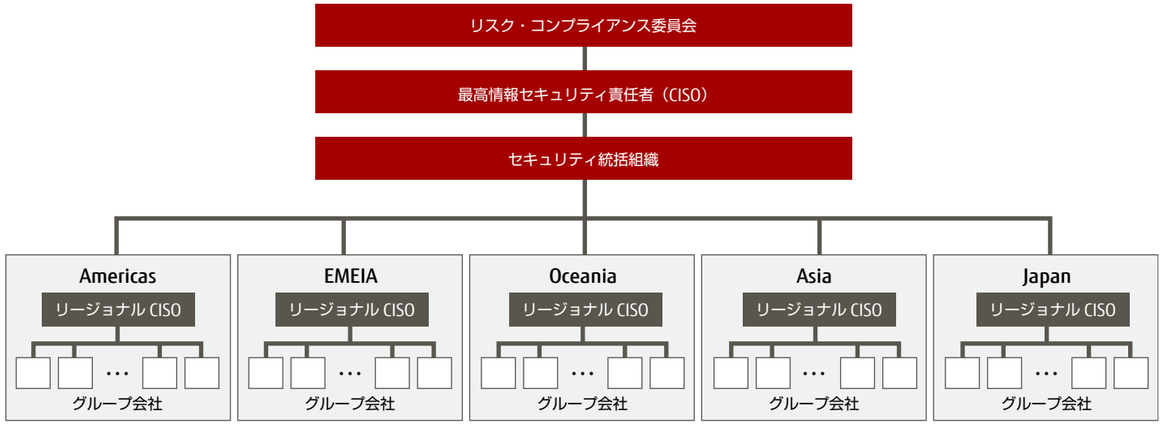
■ リスク・コンプライアンス委員会

リスク・コンプライアンス委員会は、グローバルにビジネスを展開する富士通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を統括する取締役会直属の組織です。富士通株式会社の代表取締役社長と業務執行取締役およびリスクマネジメント担当役員で構成されています。また重要なリスクの 1 つである情報セキュリティリスクも統括する役割を担います。

■ 最高情報セキュリティ責任者（CISO）

最高情報セキュリティ責任者（CISO）は、リスク・コンプライアンス委員会から任命され、富士通グループにおけるグローバルな情報セキュリティ対策に関する責任と権限を付与されています。CISO は、セキュリティ施策の執行状況についてリスク・コンプライアンス委員会に定期的に報告するほか、必要に応じて随時報告を行います。

情報セキュリティマネジメント体制



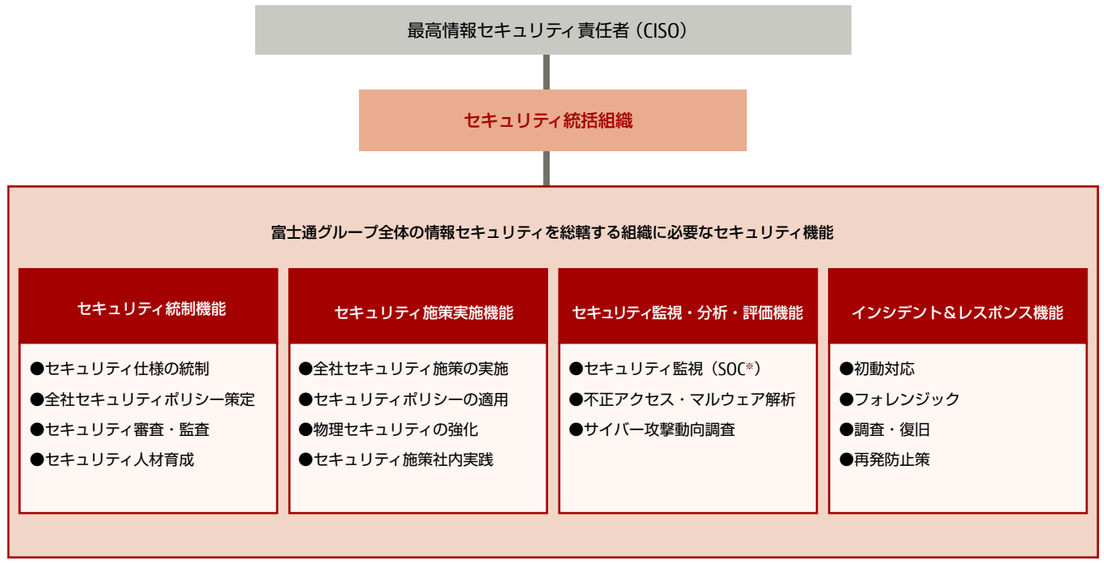
■ セキュリティ統括組織

セキュリティ統括組織は、富士通グループの情報セキュリティ対策を強化するための CISO 直轄の組織です。情報セキュリティに関するグループ共通のルールや施策の企画立案を行い、一元管理するマネジメントを担います。具体的にはセキュリティ統制機能、セキュリティ施策実施機能、セキュリティ監視・分析・評価機能、インシデント&レスポンス機能を担い、富士通グループを統制しています。

■ リージョナル CISO

リージョナル CISO は 5 つのリージョンごとに配置された最高情報セキュリティ責任者で、管掌するリージョン内の情報セキュリティについて最高の権限と責任が付与されています。配下のリージョンにおける情報セキュリティ施策を策定するとともに、グループ各社のセキュリティチームが実施する情報セキュリティ施策の確実な実行とその報告を推進しています。

セキュリティ統括組織の機能



※ SOC: セキュリティオペレーションセンター

セキュリティ統制

セキュリティポリシー策定

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」に基づき、国内外のグループ会社において情報管理や ICT セキュリティに関する社内規定を整備し、情報セキュリティ対策を実施しています。グローバル共通の富士通グループ情報セキュリティ基本方針の下、グループ会社向けの情報管理関連規定と情報セキュリティ規定を用意しています。

また海外では、その国の制約に合わせて、会社ごとに規定、ポリシーを独自に作成・整備しています。

セキュリティ審査

富士通グループでは、新会社設立時などイントラネットを敷設する際にセキュリティ審査を実施しています。具体的には、ISO27001 で規定されたセキュリティ要件に従い、現地調査を実施し、セキュリティリスクの有無を確認しています。

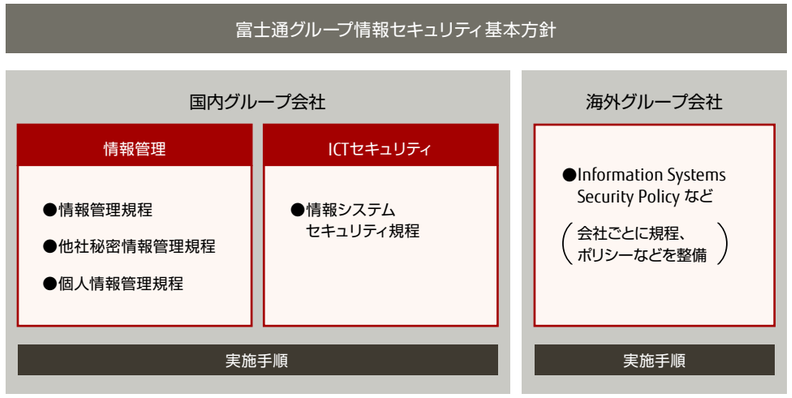
また、サーバをインターネットに公開する際にもセキュリティの脆弱性を審査するほか、サーバを公開した後も定期的に脆弱性を確認し、安全な状態を維持しています。

セキュリティ監査

富士通グループでは、国内外の事業部門を対象に情報セキュリティ監査を実施しています。この監査は、事業部門から独立した監査部門が行い、具体的には情報管理の運用状況や ISMS への適合性を監査しています。

監査の結果は各事業部門にフィードバックされ、情報セキュリティの向上に役立てられます。

情報セキュリティ関連規定体系



情報管理規程：
業務上取り扱う情報を適切に扱うためのルール

他社秘密情報管理規程：
他社の秘密情報を適切に取り扱うためのルール

個人情報管理規程：
個人情報保護ポリシーの理念に基づき、個人情報を適切に取り扱うためのルール

情報システムセキュリティ規程 / Information Systems Security Policy：
情報機器や情報システムおよびネットワークを使ううえで機密性、完全性、可用性を維持するための管理ルール

セキュリティ人材育成

■ 情報管理教育

情報漏えいを防ぐためには、規程類を従業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です。そこで、富士通および国内グループ会社では、従業員を対象とする情報管理教育を実施しています。具体的には、毎年、役員を含む全従業員を対象とした e-Learning を実施し、さらに新入社員や昇格・昇級者にはそれぞれの研修の際に情報セキュリティ教育を実施しています。

海外グループ会社では、従業員に対する情報セキュリティ教育を毎年実施し、また、情報セキュリティ管理者には、管理者向けのセキュリティ教育も実施しています。

■ 情報管理に対する意識啓発

国内富士通グループでは、2007 年に「情報管理 徹底宣言！ ～情報管理は富士通グループの生命線」という国内富士通グループ共通のスローガンを策定し、情報管理に対する意識啓発を図っています。具体的には、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、全従業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っています。

また、イントラネット上のウェブサイトを利用して、世の中で多発している情報漏えい事件を紹介し、情報管理への注意喚起を促しています。さらに、毎月、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」の発行

情報を適切に取り扱うことは、富士通グループの企業活動の基本であり、生命線でもあります。

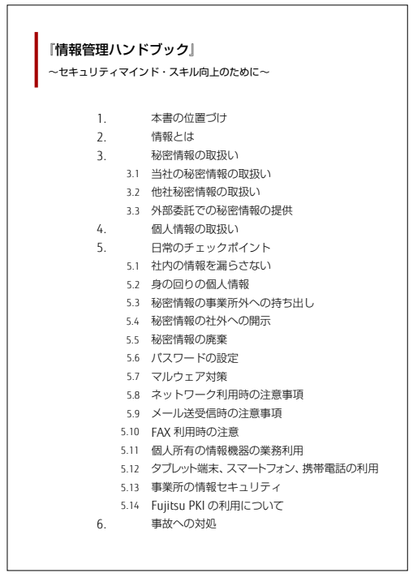
富士通グループでは、情報漏えいによるトラブルを未然に防ぐために、情報セキュリティに関する規定を整備し、セキュリティ対策を実施しています。

「情報管理ハンドブック」は、これらの規定の情報管理に関する理解を深めることを目的に発行しており、情報管理に関して疑問がある場合はすぐに確認することができます。

e-Learning 画面

情報管理徹底宣言のシール

情報管理ハンドブック


『情報管理ハンドブック』
～セキュリティマインド・スキル向上のために～

セキュリティ施策

セキュリティ施策 ～「多層防御」の考え方を取り入れた 3 つの重点施策

「標的型攻撃」に代表される近年のサイバー攻撃は、これまで以上に巧妙化・多様化・複雑化しており、従来型の単一のセキュリティ対策では防御しきれない状況になっています。

富士通グループでは情報セキュリティ対策の基本コンセプトとして、1 つの施策で防ぐのではなく、複数の異なる施策で多層化して防御する、「多層防御」の考え方を取り入れています。多層防御には「防御壁を多重に配置し攻撃を防ぐ」「多重に検知機能を配置し攻撃を早期に発見する」「侵入されたとしても被害を最小限に抑える」という 3 つの目的があります。このように組み合わせて防御することで攻撃を未然に防ぎ、被害を最小限にすることが可能となります。

富士通グループでは、情報の保護を目的とする「情報管理」、サイバー攻撃に対するシステムの防御施策を中心とする「サイバーセキュリティ」、そしてオフィス・工場などのファシリティにおける不正アクセスを予防する「物理セキュリティ」の 3 つを情報セキュリティにおける重点施策として社内の情報セキュリティ対策に取り組んでいます。

セキュリティ施策 ①：情報管理

■ 情報の分類

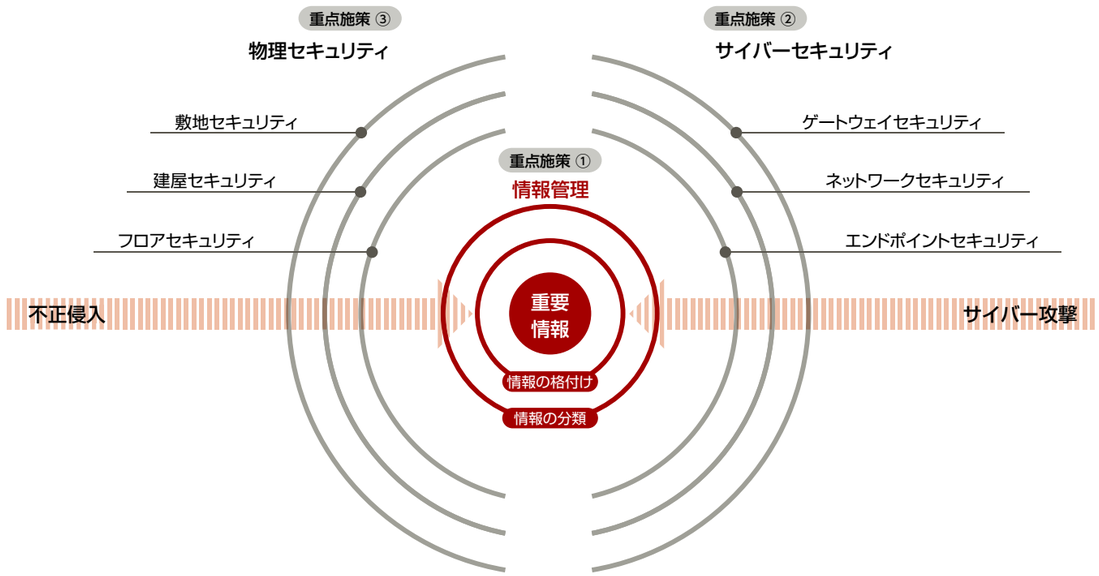
国内富士通グループでは、社内に流通する情報に関する取り扱いのルールとして「情報管理規程」を定め、社内に流通する情報を分類し、適切に管理、運用しています。

また、海外グループ会社においても各国の事情に合わせて同様の情報分類を行い、管理を行っています。なお、社外秘情報と関係者外秘情報は「情報管理規程」に、他社秘密情報は「他社秘密情報管理規程」に従って管理しています。

■ 情報の格付け（公開情報・秘密情報の分類）

富士通グループでは、分類された情報を、法的な要求事項、価値、重要性など取り扱いをどの程度慎重に行うのかの観点から格付けを行い、格付けに応じたセキュリティ対策を講じて情報を保護しています。

多層防御のコンセプトイメージ



■ 情報保護マネジメントシステムによる情報の保護

国内グループ会社においては、他社秘密情報および当社秘密情報を適切に保護するために、現場での自律した情報保護活動、具体的には、業種・業態による規制等、お客様、取引先に応じた適切な管理を設定し情報を保護する取り組みと、社内第三者組織による監査の実施により、取り組み状況を確認する「情報保護マネジメントシステム」を構築し、情報保護の改善に努めています。

■ 個人情報の保護

グローバルなデータの流通がますます進展していく中で、個人情報の保護をより安全に、より円滑にしていくために、富士通グループは各社の個人情報保護の強化に取り組んでいます。

富士通では、2007 年 8 月にプライバシーマークを取得し、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強化を図っています。

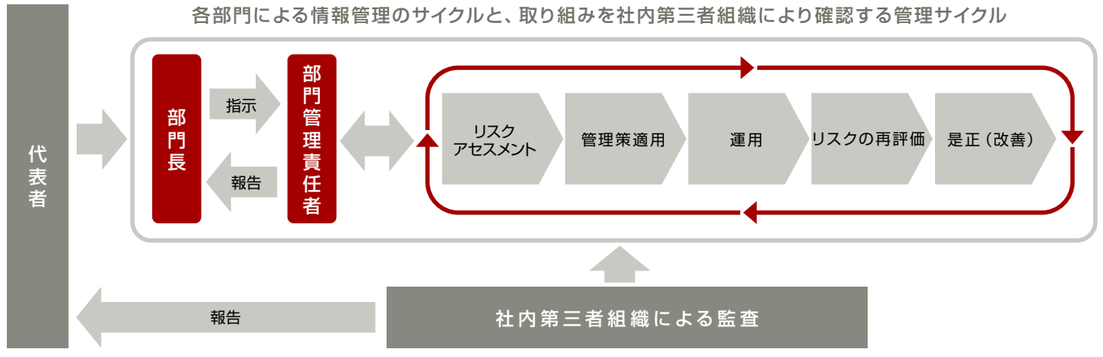
国内グループ会社も、必要に応じて各社でプライバシーマークを取得し、個人情報管理の徹底を図っています。海外グループ会社の公開サイトにおいては、各国の法律や社会的な要請に応じたプライバシーポリシーを掲載しています。

情報の分類

情報の分類			例	個人情報の例
公開情報			カタログ、マニュアル、ニュースリリース、公開ウェブなど	公開ウェブに掲載された役員の情報など
秘密情報	当社の秘密情報	社外秘情報	関係者外秘情報以外の情報 ・社内ルールなど	職制表など
		関係者外秘情報	関係者以外に開示してはいけない情報 ・研究中の技術情報	人事情報、顧客リストなど
	他社秘密情報			受託業務に伴い受領した個人情報

公開情報	公開ウェブ、カタログ、マニュアル等、一般に公開されているものをいいます。
秘密情報	「当社の秘密情報」と「当社以外の秘密情報」に分類し、さらに当社の秘密情報を「社外秘情報」と「関係者外秘情報」に分類しています。
社外秘情報	社外に開示してはならない情報のことをいい、社内ルール、社内報等がこれにあたります。
関係者外秘情報	「人事情報」「研究中の技術情報」「顧客リスト」等、知る必要のない人には知られてはならない情報をいいます。
他社秘密情報	受託契約や秘密保持契約、ライセンス契約等によりお客様や他社から入手した秘密情報など、契約による守秘義務が課されている情報です。
個人情報	当社が自ら取得した個人情報と、受託開発などお客様から業務を受託するに伴い、お客様が保有している個人情報を受領し、アクセスを許された個人情報があります。個人情報には、マイナンバー（個人番号）も含まれます。

情報保護マネジメントシステム



■ プライバシーマークについて

当社は、一般財団法人日本情報経済社会推進協会よりプライバシーマークの付与認定を受けています。プライバシーマークは、JIS Q 15001：2006 に適合した個人情報保護マネジメントシステムの下で個人情報を適切に取り扱っている事業者に付与されるものです。

プライバシーマーク

■ GDPR 対応

富士通グループでは、2018 年 5 月に施行された欧州の一般データ保護規則（GDPR）について、主に以下の取り組みを実施しています。今後は、GDPR を始めとする各国の個人情報保護法についてグループ全体で取り組んでいきます。

グローバルな体制構築

取締役会に直属するリスクマネジメントおよびコンプライアンスにかかる最高決定機関であるリスク・コンプライアンス委員会の承認の下、GDPR に基づくグローバルでの個人情報保護体制を構築しました。なお、域外適用を認める法制度の新設・改正の動きやサイバーセキュリティの脅威の高まり等に鑑み、GDPR だけでなく世界各国の個人情報保護法についても、本体制を富士通グループの個人情報保護体制として活用するように拡張しました。

社内ルール等の整備と周知

CISO 組織と法務部門主導の下、EMEIA リージョン等と連携して整備した各種社内規定・チェックシート等について、GDPR に対応するため継続的に調査を行い、適宜ルール・チェックシート・運用プロセスの見直しや従業員教育のアップデート等を実施しています。

域外移転規制への対応

個人データの EU 域外移転規制への対応として、お客様から処理の委託を受けた個人データの取り扱いに関するグループの共通ルールを定めた個人データ処理者のための拘束的企業準則（Binding Corporate Rules for Processors: BCR-P）を 2017 年 12 月にオランダの欧州データ保護機関に申請しています。また、欧州委員会によって日本と EU 間の十分性認定が 2019 年 1 月 23 日に発効されましたので、当該十分性認定に基づき域外移転を行った個人情報の取り扱いに関する社内ルール等を整備・周知しました。

※一般データ保護規則（General Data Protection Regulation：GDPR）について：GDPR とは、2018 年 5 月 25 日に施行された個人データ保護を企業や組織・団体に義務付ける欧州の規則で、個人データの欧州経済領域外への移転規制や、データ漏えい時の 72 時間以内の報告義務などが規定されている。違反した企業や組織・団体には、グループ全体の年間売上の 4% または 2,000 万ユーロのうち、いずれか大きい方を上限とする罰金が課せられる可能性がある。

セキュリティ施策 ②：サイバーセキュリティ

富士通グループでは、サイバー攻撃に備えて、ネットワークの特性に合わせて対策を複数層に分けて実施しています。ファイアウォールや標的型攻撃対策などの「ゲートウェイセキュリティ施策」、不正アクセス検知などの「ネットワークセキュリティ施策」、マルウェア対策やセキュリティパッチ管理などの「エンドポイントセキュリティ施策」を組み合わせた多層防御により、巧妙化・多様化・複雑化するサイバー攻撃への対策を講じています。

■ ゲートウェイセキュリティ施策

サイバー攻撃を防御するうえで、外部からの侵入を防ぐことが重要です。富士通グループでは、外部インターネット空間と富士通グループ内情報ネットワークとの境界部分にゲートウェイを設置し、外部からの不要な通信を阻止することでセキュリティの確保に努めています。具体的には、インターネット層との境界部分には不正アクセスを防御する「ファイアウォール」や、標的型攻撃対策として未知マルウェア検知システムを導入し、メールやウェブの通信を監視し「入口 / 出口対策」を実施しています。

メールセキュリティ

外部からの脅威に対して、メールゲートウェイでは IP レピュテーションや送信ドメイン認証などの迷惑メール対策およびマルウェア（ウイルス）対策を実施しています。また、メール宛先の自動識別による社外への送信に関する再確認操作や社外に発信する資格有無について自動的に確認を行い、業務上不要な利用者による社外へのメール発信や情報漏えいを防止しています。

ウェブアクセスセキュリティ

インターネットへのウェブアクセスに対し、必ずプロキシサーバを経由させ、マルウェアチェックや URL フィルタを実施し、悪意あるウェブサイトへのアクセスから守り、安全なアクセス手段を提供しています。また、プロキシ利用はユーザー認証による制限を行っており、意図しないアクセスを防ぐとともに、利用者のアクセスログを記録しています。

リモートアクセス

パソコンやスマートデバイスを使用して、社外からイントラネットへ接続して安全に業務を行うリモートアクセス環境を提供しています。アクセス経路として通信を暗号化し、アクセスするために 2 要素認証を用いて、不正なアクセスを防止しています。また、働き方改革の取り組みとして、仮想デスクトップを活用し、パソコンにデータが残らないよう、セキュリティを確保しながら仕事を実施できる環境を提供しています。

■ ネットワークセキュリティ施策

従来のサイバー攻撃対策は外部からの侵入を防御するゲートウェイ（入口）対策が中心でしたが、近年、標的型攻撃をはじめサイバー攻撃が高度化するなか、サイバー空間からの侵入を完全に防御することが困難になりつつあります。社内ネットワークにおける脅威を素早く検知するための内部対策が重要です。

富士通グループでは、内部対策として内部不正通信の検知機器を導入し、社内ネットワーク内の不審な通信の検知に努めており、研究中の新しい技術についても、製品化や実運用に向けて社内実践の場を通じて検証を行っています。

■ エンドポイントセキュリティ施策

近年、「標的型攻撃メール」をはじめ、パソコンやモバイル端末などのエンドポイントをターゲットとしたサイバー攻撃が増加しており、その対策がこれまで以上に求められています。

富士通グループでは、従業員が利用するエンドポイントにおけるセキュリティ施策においても「多層防御」の考え方を取り入れ、マルウェア対策、ログ取得や HDD 暗号化など、エンドポイントを各レイヤー（層）に分けて必要なセキュリティ施策を実施しています。

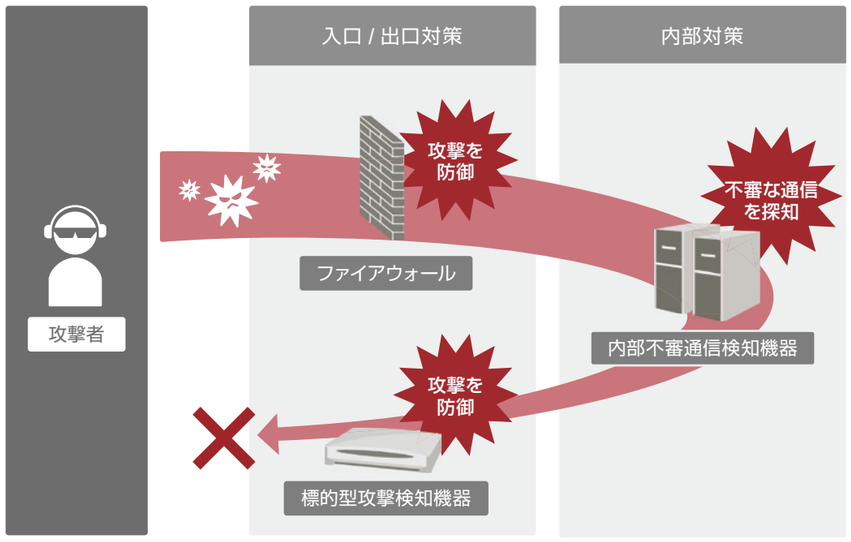
情報漏えい対策として、データが保存できないシンクライアント端末と仮想デスクトップを組み合わせて使用し、これまで従業員個々のパソコン内に保存していたデータを部門用・個人用ストレージ内で一元的に集中管理し、セキュリティを強化しています。

なお、シンクライアント端末以外のパソコンについても、データをパソコン内に保存させない対策に加え、IT Policy N@vi を導入し、業務で使用する USB メモリやポータブルハードディスク等の USB 機器を制限し情報の持ち出しを防止しています。

その他、サポートを終了した OS やソウトウェアを使用しているパソコンについては、ネットワークから強制的に遮断する処置を行い、セキュリティリスクを低減しています。

これらのエンドポイントセキュリティ施策を施したパソコン、シンクライアント端末を利用することにより、これまで従業員一人ひとりが行っていたパソコンの各種セキュリティ対策の負担を軽減するとともに、組織内に標準化されたエンドポイントセキュリティを一元管理のもとで実施することで、セキュリティの向上を図っています。

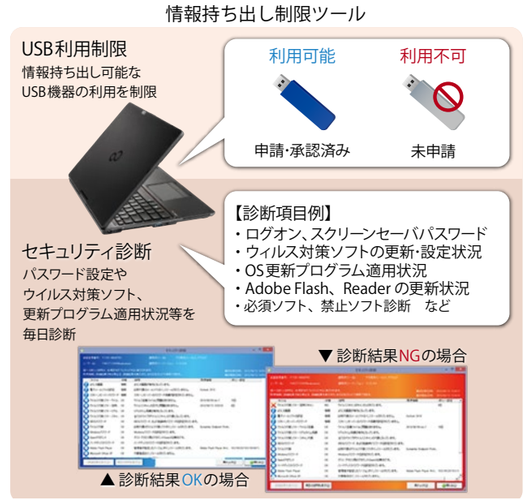
サイバー攻撃と多層防御によるサイバーセキュリティ施策



主なエンドポイントセキュリティ施策

レイヤー	セキュリティ施策
データ	秘密情報有無チェック
セキュリティツール	マルウェア対策
ログ	各種ログ取得
セキュリティパッチ	セキュリティ可視化・追跡
OS	脆弱性対応
デバイス	USB ポート制限、パスワード制限、HDD 暗号化

情報持ち出し制限ツールの概要



■ 認証セキュリティ施策

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、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。人事部門が管理しており、カードの使用者が正当な従業員であることを保証します。このカードを用いることで確実な本人確認によるシステムへのログイン認証、および紙の文章への決裁印の押印と同じ効果がある電子決裁などに利用しています。

その他、静脈認証やOTP（One Time Password）を利用シーンに応じて導入しています。

セキュリティ施策 ③：物理セキュリティ

情報管理、サイバーセキュリティに続く3点目の重点施策である物理セキュリティについても、多層防御の考え方に沿った対策を行っており、具体的には、敷地・建物・フロアの3層において、「人的警備」と「機械警備」を組み合わせた物理セキュリティ環境を構築しています。

これにより、物理的な不正侵入から、重要情報を保護しています。また、海外においても、その国々の状況に合わせて、類似の物理セキュリティ対策を実施しています。

■ 物理セキュリティポリシー

「人的警備」「入退場管理機器（セキュリティゲート・カードリーダー）」「監視カメラ」を組み合わせ、物理セキュリティ強化を実現する

1	身元不詳の不審者の侵入を防ぐ
2	悪意ある者の正面突破を防ぐ（テロ行為含む）
3	従業員、来訪者の確実な入退場管理
4	従業員の不正な持ち出しの証跡を残す
5	ICTによる高セキュリティ環境の実現

■ 先端技術の導入

より高度な物理セキュリティ環境を構築するために、昨年度実施した、なりすましを防ぐことが可能な静脈認証装置を組み合わせたセキュリティゲートの実証実験を経て、実証実験で得たノウハウを活用し、新型のトビラ用リーダーが完成しました。既に社内展開されており、実用化に至っています。

手のひら静脈認証入退室装置（富士通 Security Initiative Center）

セキュリティ監視・分析・評価

セキュリティ監視

全世界に配備したセキュリティ監視機器から1日約10億件のログが集められます。情報セキュリティマネジメントを行ううえでこのログを効率的・効果的に管理することが重要です。

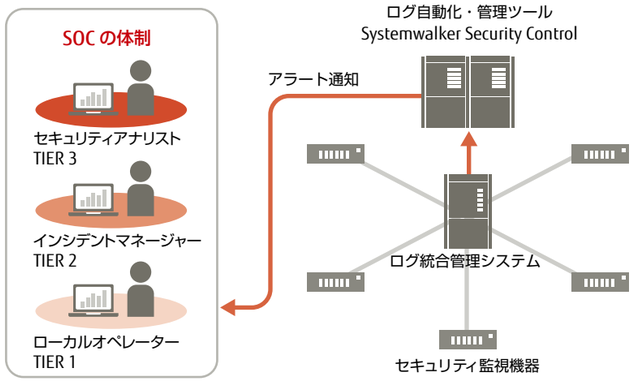
富士通グループでは、24時間365日体制のセキュリティオペレーションセンター（SOC）を設置し、迅速・的確なインシデント対応、セキュリティアラート対応を可能にする仕組みを構築しています。社内ネットワークの各所に組み込まれた「セキュリティ監視機器」で生成されたログは、「ログ統合管理システム」に集約・一元管理され、そこからインシデント管理システムに送られ、脅威が確認された場合、アラート通知メールがSOCに送られる仕組みになっています。

SOCは「ローカルオペレーター」「インシデントマネージャー」「セキュリティアナリスト」というスタッフで構成され、受信したアラート通知メールの内容を分析し、脅威の質・範囲・重度を見極め、対応優先順序を付けて、迅速・的確に対処します。

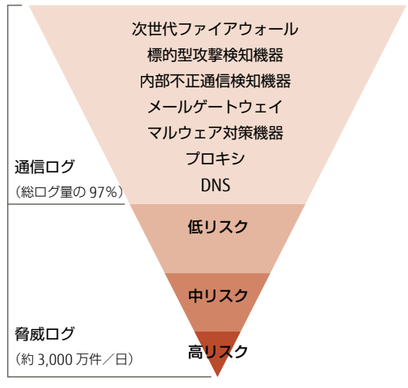
■ 外部機関との連携によるサイバー攻撃動向調査

変容するサイバー攻撃の脅威に対応するため、外部機関と情報共有を行い、サイバー攻撃の予兆を検出、実際の攻撃情報を基に脅威に対処し、リスクを最小限に抑えてインシデントの発生を防ぎます。

セキュリティ監視（SOC）体制



セキュリティアラートの分類



インシデント＆レスポンス

初動対応

富士通グループでは、CISO 配下にサイバーセキュリティに関するインシデントレスポンスの専門部隊を設けています。インシデント発生時には SOC と連携して被害機器を特定し、速やかにネットワークから切断・隔離することで、被害を最小限にとどめます。また、関連部門へ連絡し、対応するための体制を構築します。さまざまな可能性を検討し、二次被害を防ぐ施策を展開し、被害の拡大を抑止します。

■ フォレンジック

初動対応にて隔離した機器を、専用機器などを用いて証拠保全※を行います。保全した証跡のコピー、および SOC で取得したアラートやログを解析し、被害および原因や影響範囲を特定します。

※証拠保全：インシデント発生の原因や被害を特定するためには、サイバー攻撃の痕跡を迅速に収集し、分析をすることが必要です。その痕跡が失われないよう、インシデントに関連する機器の電磁的証拠（ハードディスク、ログ等）の保全（複製作成等）を行います。

調査・復旧

フォレンジックや不正プログラム解析などにより判明した情報を基に影響を特定し、リスクに応じた対応を行います。また、並行して原因究明、および脅威の除去を行い、安全が確認されたところから復旧を進めます。

再発防止策の展開

判明した事象をリスク・コンプライアンス委員会へ報告します。さらに、CISO の下、同様のインシデントが発生していないかの調査、監査を行い、関連部署と連携して再発防止策を全社展開します。

特 集

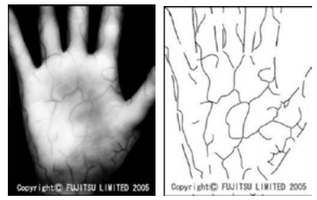
手のひら静脈認証の社内適用拡大による セキュリティと利便性の向上

富士通グループは、仮想デスクトップのログイン認証を手のひら静脈認証方式へと切り替えを進めていますが、今後は入退室管理などを含め、手のひら静脈認証の適用範囲を拡大していきます。

手のひら静脈認証の特長

富士通の手のひら静脈認証は、体内にある通常では目に見えない静脈パターンを読み取って照合し、本人確認または個人を特定できる独自技術です。精度が高く、「手をかざす」という直感的で自然な動作で認証できることから、国内だけでなく海外でも広く採用されています。

手のひら静脈を始めとする生体認証は、盗難や漏えいによる不正使用のリスクが極めて低く、忘却や紛失によって本人が認証できなくなってしまうことも無いため、今後ますます適用範囲の拡大が見込まれています。



静脈パターン画像

手のひら静脈認証適用拡大

現在、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 カードを使用しています。セキュリティカードの IC チップには従業員番号や PKI（Public Key Infrastructure）証明書と鍵を格納しており、業務システムへログインする際には、セキュリティカード（所有物）と PIN（Personal Identification Number）入力（知識）の正しい組合せにより本人認証を行っています。

一方で手のひら静脈認証を適用した仮想デスクトップサービスは、2019 年度内には全従業員への展開が完了する見込みで、今後はこれまでセキュリティカードで実現していた業務システムへのログインにも段階的に手のひら静脈認証の適用を開始する予定です。

入退室管理への手のひら静脈認証適用

同様に、セキュリティカードで認証している入退室管理についても、2017 年度から実施してきた「大規模事務所での入退室ゲートの手のひら静脈認証 PoC（Proof of Concept）」を経て、他の事業所のゲートや扉の認証への適用拡大が可能になりました。アンケート調査から、利用者は利便性の向上を実感しており、社内の認証をすべて手のひら静脈にしたいという声も上がっています。

2018 年 11 月、手のひら静脈認証入退室装置（PalmSecure AuthGate）を製品化し、SIC（Security Initiative Center）やセキュリティを強化したい事業所への導入を進めており、今後、全国事業所への展開も計画しています。


入退場ゲートの手のひら認証 PoC

AuthGate の導入例

手のひら静脈認証入退室装置（PalmSecure AuthGate）

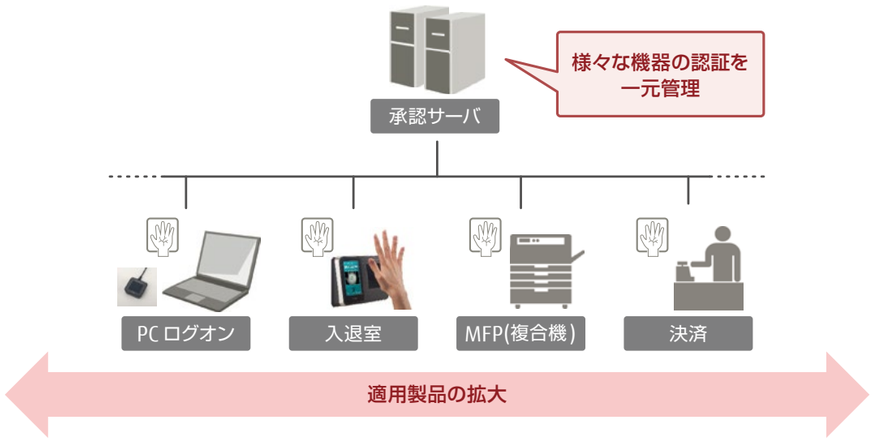
PalmSecure AuthGate は、最新の静脈センサーと認証ライブラリーの採用で、手かざしだけの 1 対 N 認証でも精度の高い本人認証が可能になり、設置環境耐力の向上によって準屋外環境への設置も実現しています。また、手かざし部分に触れることなく認証できることから利用者の抵抗感が少なく、衛生面にも配慮した操作性になっています。

PalmSecure AuthGate
https://pr.fujitsu.com/jp/news/2018/11/8-1.html

簡単でセキュアにつながる世界を目指して

ここまで記した仮想デスクトップや業務システム、入退室管理以外にも、より多くのシステム（例えば複合機）への手のひら静脈認証適用を目指し、継続的に取り組んでいく予定です。

つながる手のひら静脈認証システム



［発行者］

富士通株式会社

法務・コンプライアンス・知的財産本部

〒 105-7123 東京都港区東新橋 1-5-2 汐留シティセンター

TEL：03-6252-2220（代表）