FUJITSU

富士通グループ
情報セキュリティ報告書
2017

shaping tomorrow with you

社会とお客様の豊かな未来のために

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強化を図ることを重要な社会的責任と捉え、さまざまな施策を展開しています。

「情報セキュリティ報告書」では、富士通グループが推進するさまざまな情報セキュリティの取り組みについて報告しています。2009 年より制作を開始し、今回で 9 冊目となりました。

本報告書は、今までの内容を一新し、富士通グループ内の情報セキュリティに焦点をあて、各種施策について掲載しています。

本報告書を通じて、安心・安全なデジタル社会の実現を支える富士通グループについてご理解いただけると幸いです。

■ 報告対象期間

2016 年度（2016 年 4 月 1 日～ 2017 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 514 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：2017 年 6 月
- 英語版　：2017 年 9 月

目次

より快適で安心できるネットワーク社会づくりを目指して情報セキュリティのさらなる強化を図っていきます。

ICT は、世界の人々をつなぎ、さまざま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。国境を越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、さまざま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、安心・安全で、情報が新たな価値を生み出し、豊かで持続可能な社会「ヒューマンセントリック・インテリジェントソサエティ」をビジョンに掲げています。そして、ICT の力によって、持続可能な地球と社会の実現に貢献することと、デジタル社会の安心・安全を維持・強化していくことをグローバル ICT 企業としての社会的責任と考えています。

このビジョンの下、富士通グループでは、FUJITSU Way※「行動規範」に基づく社内規定を遵守し、情報の適正な管理および活用を行っています。それと共に、FUJITSU Way に掲げる企業理念を実践するために、経済産業省および独立行政法人情報処理推進機構が公表した「サイバーセキュリティ経営ガイドライン」に準拠した国内外共通の「富士通グループ情報セキュリティ基本方針」を新たに定め、情報セキュリティの確保・向上に積極的に努めます。

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整備しています。

今回お届けする「情報セキュリティ報告書 2017」は富士通グループの情報セキュリティに関する活動をご紹介するものです。是非、ご覧いただきますようお願い申し上げます。

富士通株式会社
最高情報セキュリティ責任者 (CISO)
髙 綱 直 良

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

富士通グループ内の情報セキュリティ

日々高度化、巧妙化するサイバー攻撃への対策は、
企業にとって大きな課題となっています。
社会問題化するサイバー攻撃に迅速・確実に対応するためには、
現状の可視化を踏まえて対策・組織・プロセスの強化を図り、
情報セキュリティの高度化とその運用を継続的に
実施する必要があります。
ICT を事業の根幹とする富士通グループは、情報セキュリティに対する
基本方針や規定、グループ共通で利用する ICT インフラおよび
セキュリティ施策などの多様な取り組みを通じて、
富士通グループ内の情報セキュリティの確保・向上を推進しています。

基本方針

富士通グループは、グループの理念指針であるFUJITSU Wayで掲げる「快適で安心できるネットワーク社会づくり」を実現するため、グローバルなセキュリティポリシー「富士通グループ情報セキュリティ基本方針」に基づき、情報セキュリティの確保・向上に取り組んでいます。

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。

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「サイバーセキュリティ経営ガイドライン」を公表したことを受け、取締役会に直属するリスク・コンプライアンス委員会において、グループ全体をカバーするグローバルなセキュリティポリシーの検討を行い、2016年4月に「富士通グループ情報セキュリティ基本方針」を策定しました。

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）
http://www.fujitsu.com/jp/documents/about/csr/management/security/security-2016-04.pdf

マネジメント体制

富士通グループは、リスク・コンプライアンス委員会の下に最高情報責任者（CIO）から独立した最高情報セキュリティ責任者（CISO）を設置し、グローバル ICT 企業としての情報セキュリティガバナンスの強化を図っています。

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グローバルな 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の強化を図っています。

■ 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。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。

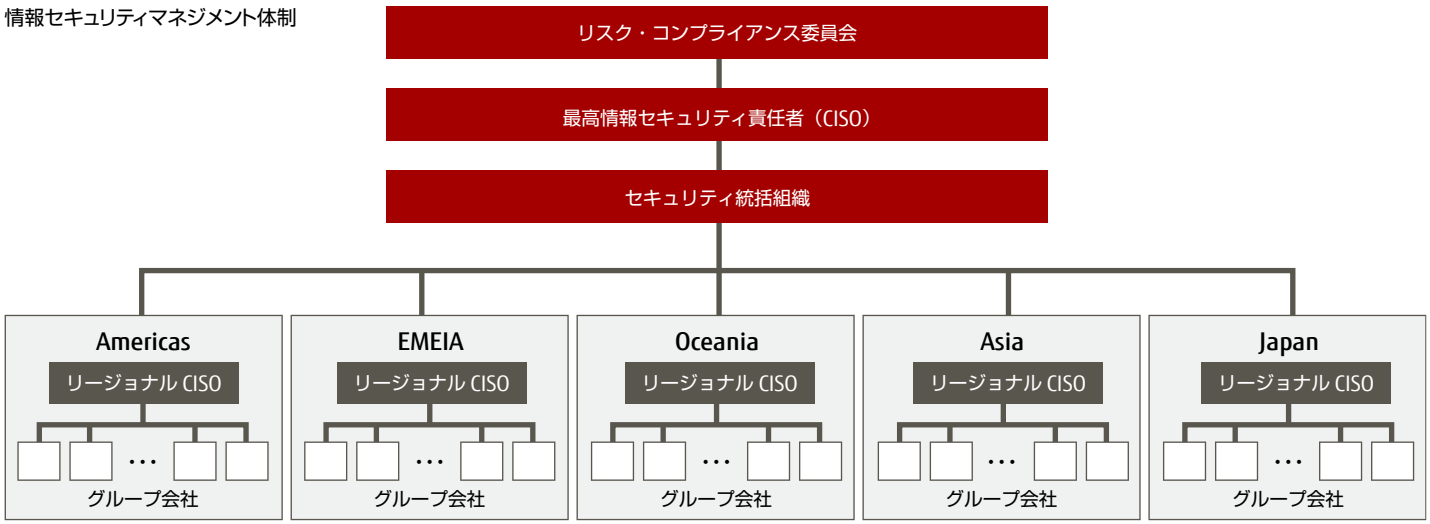
■ 最高情報セキュリティ責任者（CISO）

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。

■ 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。

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

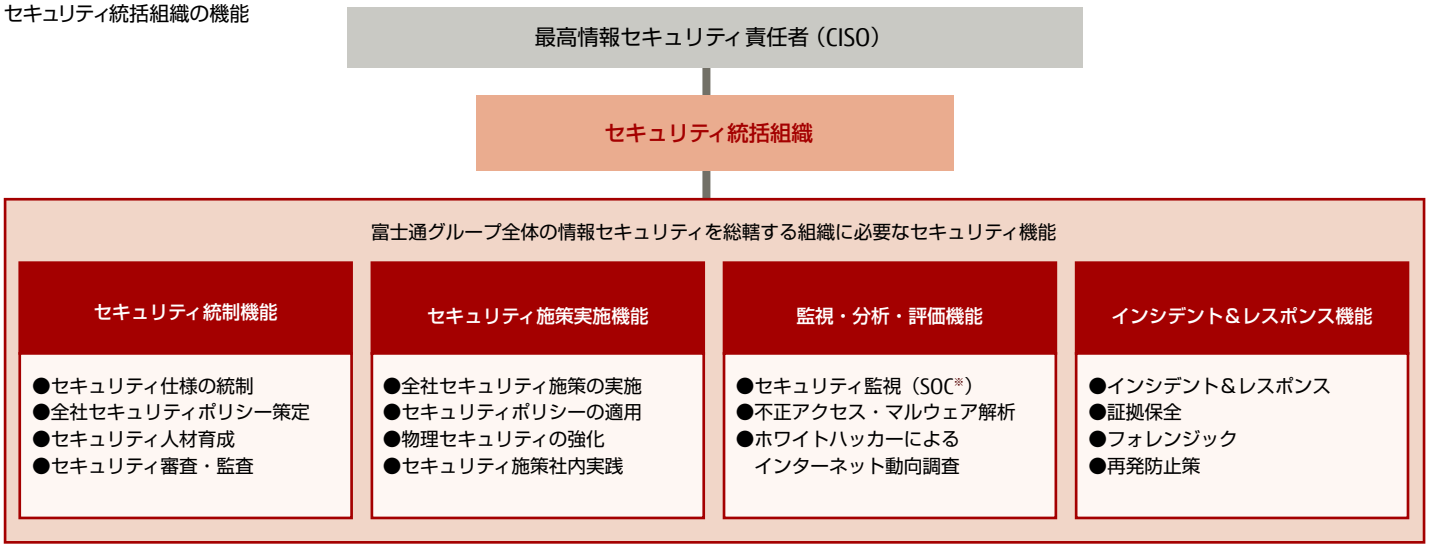
セキュリティ統括組織は富士通グループの情報セキュリティ対策を強化するため、CISO 直轄の組織として設立され、グループ共通のルールや施策の企画立案を行い、一元管理するマネジメントを推進しています。大きく 4 つの機能を持っており、セキュリティ統制機能、セキュリティ施策実施機能、監視·分析·評価機能、インシデント＆レスポンス機能を担い、富士通グループを統制しています。

セキュリティ統制機能

■ 全社セキュリティポリシー策定

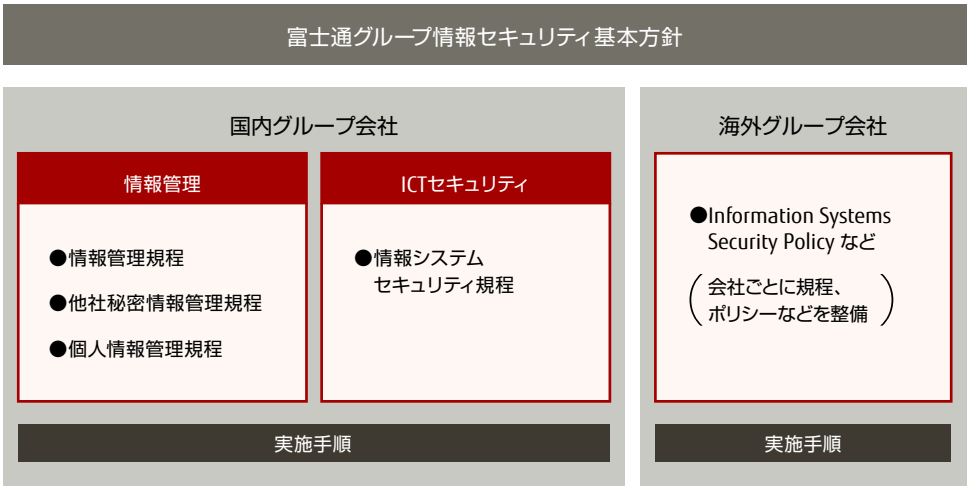
富士通グループ各社は、「富士通グループ情報セキュリティ基本方針」に基づき、国内外のグループ会社において情報管理や ICT セキュリティに関する社内規定を整備し、情報セキュリティ対策を実施しています。グローバル共通の富士通グループ情報セキュリティ基本方針の下、グループ会社向けの情報管理関連規定と情報セキュリティ規定を用意しています。

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

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

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・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ます。監査は、事業部門の特性や事業戦略、推進中の情報セキュリティ施策などを踏まえた方法で行われます。例えば、国内においてはイントラネット敷設時に規定通りに設置されているかの現地調査を実施し審査しているほか、インターネット公開しているサーバは開設時の監査と定期的な脆弱性監査を実施しています。

また、海外では ISO27001 準拠のセキュリティ要件に従い、管理状況についてアセスメントツールを使用して監査しています。

監査を受けた事業部門は、この監査結果を踏まえて、情報セキュリティ対策の改善に努めます。

■ 情報セキュリティ教育

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従業員 10 万人を対象として、新入社員研修や昇格・昇級時研修の際に、併せて情報セキュリティ教育を実施するとともに、役員を含む全従業員を対象とした e-Learning を日本語と英語で毎年実施しています。

海外グループ会社の従業員に対しても、年 1 回のセキュリティ教育を約 10 か国語で実施しています。また、海外の情報セキュリティ管理者には、管理者として必要なセキュリティ教育も実施しています。

e-Learning 画面

■ 情報セキュリティに対する意識啓発

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」という国内グループ共通のスローガンを策定して掲げています。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い、従業員一人ひとりの情報セキュリティに対する意識の向上を図っています。

これ以外にも、イントラネットを利用し、世の中で多発している情報漏えい事件を紹介することによる注意喚起や、毎月 1 回のセキュリティチェックデーを設け、幹部社員が自部門のセキュリティ対策状況を確認する活動を行っています。

情報管理徹底宣言のシール

■ 「情報管理ハンドブック」の発行

国内では、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。これは、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がある場合はすぐに確認することができます。

『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～

■ お取引先との連携

[お取引先の情報セキュリティ管理（選定・状況評価・確認）]

新規のお取引先選定においては、情報セキュリティ状況を確認するとともに、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などにつき、契約で合意を得られるお取引先に限定しています。

既存のお取引先についても、情報セキュリティ対策状況の書面調査を毎年実施しており、個人情報保護法などの要求事項に基づいて委託先を選定しています。なお、この書面調査の結果は、全体状況と評価ツールをお取引先にフィードバックし、自社で改善への取り組みが実施できるようにしています。

さらに、毎年お取引先を選定のうえ、情報セキュリティ監査を実施しています。お取引先を訪問し、契約に基づいた情報セキュリティの遵守状況を点検しています。点検の結果、是正が必要な場合には、是正計画の立案・実施指導を行っています。

情報セキュリティ監査実績（2016 年度） 約 190 社

[情報セキュリティ研修会の実施]

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、グループの従業員だけではなく、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。

2016 年度は、お取引先においても標的型攻撃に備えるなど、サイバーセキュリティの確保は急務であることから、「セキュリティリスクへの対応」を主要テーマとして研修会を開催しました。

また、お取引先からの要請で講師を派遣する出前研修会を実施しました。このほかリーダークラスのスキルアップを希望するお取引先には、リスク対応スキルの向上を目的として、グループ演習と講義を行う出前ワークショップを実施しました。ワークショップ型研修については、多くのお取引先に参加いただけるよう、１名から申込可能な集合ワークショップを企画・実施しました。

情報セキュリティ研修会開催実績（2016 年度）

約 900 社／約 1,200 名受講
（仙台、東京、川崎、千葉、名古屋、大阪、高松、福岡、沖縄）

- 出前研修会：約 80 社／約 1,300 名受講
- 出前ワークショップ：約 10 社／約 180 名受講
- 集合ワークショップ：約 20 社／約 30 名受講

[情報共有・現場支援ツールの提供]

情報セキュリティに関する最新情報の共有・啓発を目的とし、2009 年より「情報セキュリティの広場」「啓発ポスター」をお取引先に提供しています。

また、各プロジェクトの情報セキュリティ要求事項を、開始時に合意し、従事者全員で共有するため、「プロジェクト情報セキュリティ計画書」を提供し、課題の早期発見、対応を図っています。そのほかにも、自主点検ツールとして「遵守状況チェックシート」を提供しています。

啓発ポスター

[海外のお取引先対応]

お客様のグローバル化対応や開発コスト削減および人材確保などを目的として、海外のお取引先と連携したビジネスが増加しています。

出前ワークショップ

インドでの情報セキュリティ教育

富士通では、国内と同様に海外のお取引先に対しても、その国の事情に合わせて受託情報の取り扱いを規定した「受託者用情報管理要領」を締結し、定期的に情報セキュリティ監査、情報セキュリティ教育を実施しています。

■ 個人情報の保護

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体制の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。 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体制の強化に取り組んでいきます。

セキュリティ施策実施機能

富士通グループでは、全社セキュリティポリシーに則り、以下のような全社セキュリティ施策をグループ全体で実施しています。

■ ネットワークセキュリティ

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不正アクセスを防御するファイアウォールや不正侵入検知システムを導入し、イントラネットを安全に維持しています。検知情報はセキュリティオペレーションセンター（SOC）が 24 時間 365 日体制で監視しています〔P.12 参照〕。

■ 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。

■ エンドポイントセキュリティ

従業員のパソコンにおいては、OS やアプリケーションのセキュリティ修正の適用とマルウェア定義ファイルの更新を自動化しています。加えて、端末にデータを保存できないシンクライアントを展開し、情報漏えい防止対策を強化しています。また、これらのエンドポイントセキュリティ施策を施した標準パソコン・シンクライアントを順次導入しています。これにより、そ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、組織的に平準化されたエンドポイントセキュリティを一元管理の下で実施することで、セキュリティレベルの向上を図っています。

■ 認証セキュリティ

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、および紙の文書への決裁印の押印と同じ効果がある電子文書決済などに利用しています。

監視・分析・評価機能

■ 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、そこからログ自動化・管理ツール「Systemwalker Security Control」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。

■ ホワイトハッカーによるインターネット動向調査

変容するサイバー攻撃の脅威に対応するため、ホワイトハッカーによる世の中のインシデントや脆弱性を調査、またサイバーインテリジェンスを駆使し不正アクセスやマルウェアを解析した結果のリスク情報を基にログを調査し、新しい脅威からの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。

インシデント&レスポンス機能

■ インシデント&レスポンス

富士通グループでは、インシデント＆レスポンスの専門部隊を配置しています。インシデント発生時には SOC などと連携し、発生場所や被害端末を特定のうえ、専用の機器を使い証拠保全※を適切に行います。また、二次被害の発生を防ぐための施策を展開し、被害の拡大を抑止します。

※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。

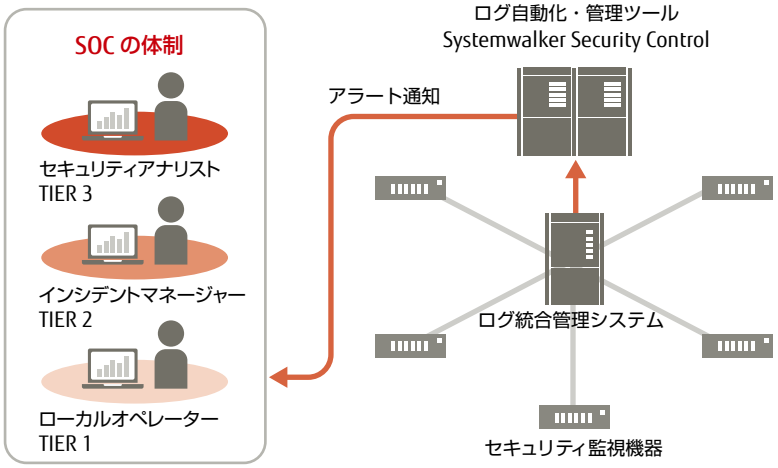
■ フォレンジック

保全した証跡、および SOC で取得したアラートやログを解析します。被害および原因や影響範囲を特定し、迅速に事態の収束を行います。

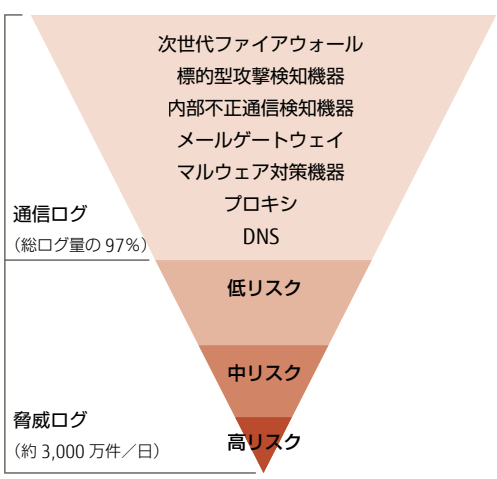
■ 再発防止策

調査によって判明したリスクをリスク・コンプライアンス委員会へ報告し、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。

セキュリティ監視（SOC）体制



セキュリティアラートの分類



重点施策

富士通グループは、多層防御の視点から情報セキュリティ対策の重点分野を絞り込み、「情報管理」「サイバーセキュリティ」「物理セキュリティ」の 3 つを重点施策として強力に推進しています。

「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。これを適切に展開していく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。

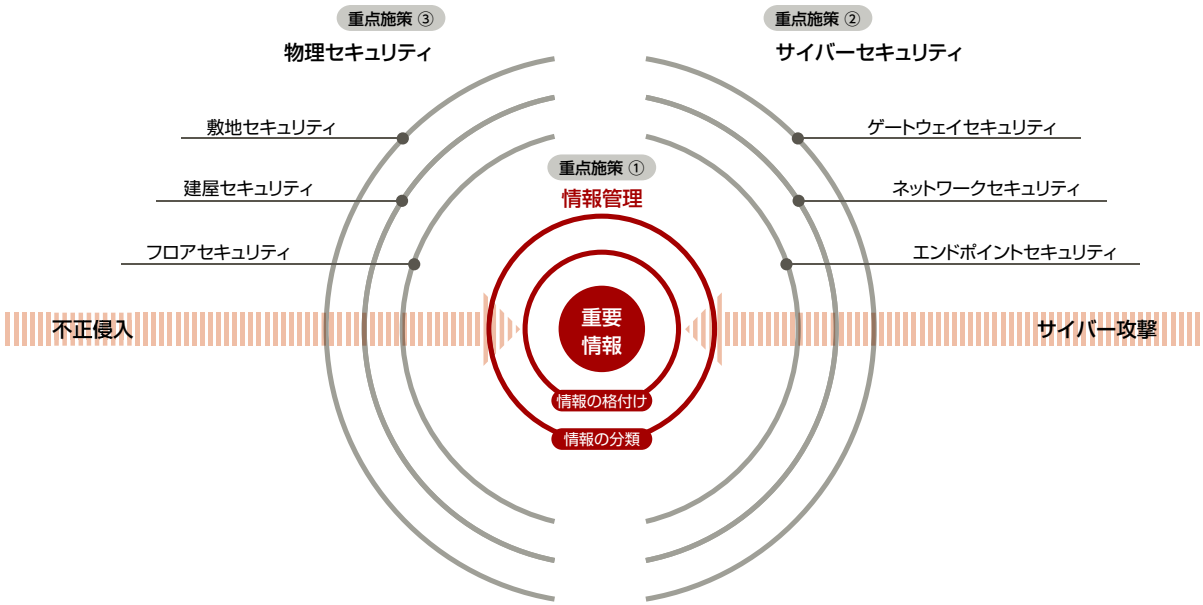
重点施策 ①：「情報管理」のセキュリティ

■ 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。海外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。

多層防御のコンセプトイメージ



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。

■ 情報の格付け（公開情報・秘密情報の分類）

社内で取り扱う情報は、上図の通りに分類されています。さらに、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、国内では公開情報と社外秘情報、関係者外秘情報、他社秘密情報の 4 段階に格付けしています。

格付けごとにその情報をどのように取り扱い、どのように保護するかについて規定で定めています。国内グループ会社においては、年 1 回、重要な情報を規則通り管理するための PDCA サイクルを回しているかの現場監査を行っています。海外グループ会社においても、国内と同様に情報の格付けを行っています。

重点施策 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。

■ 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になります。

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。

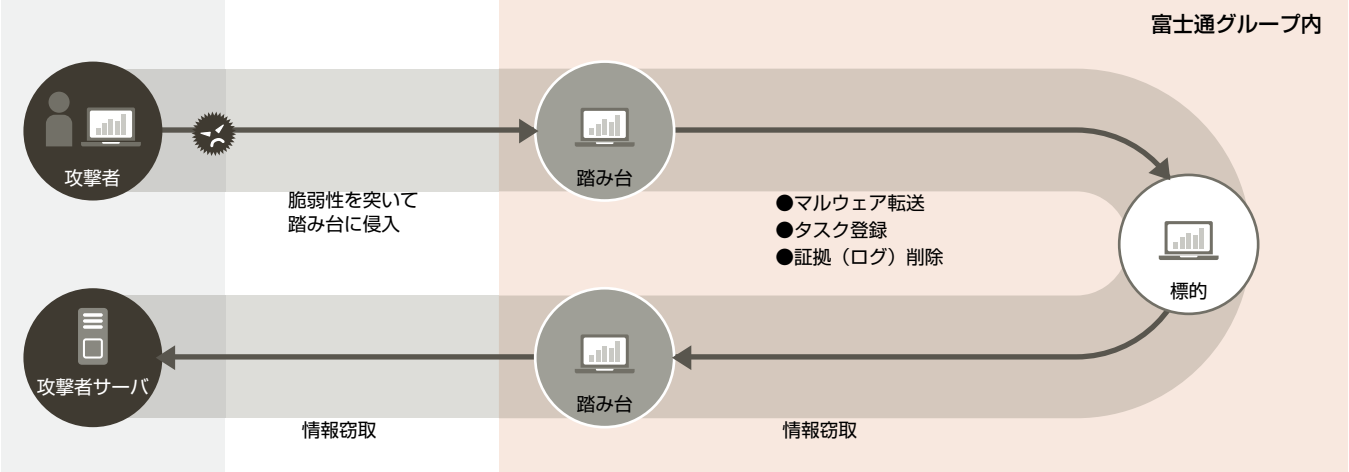
■ エンドポイントセキュリティ施策

近年、「標的型攻撃メール」をはじめ、個人の情報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。

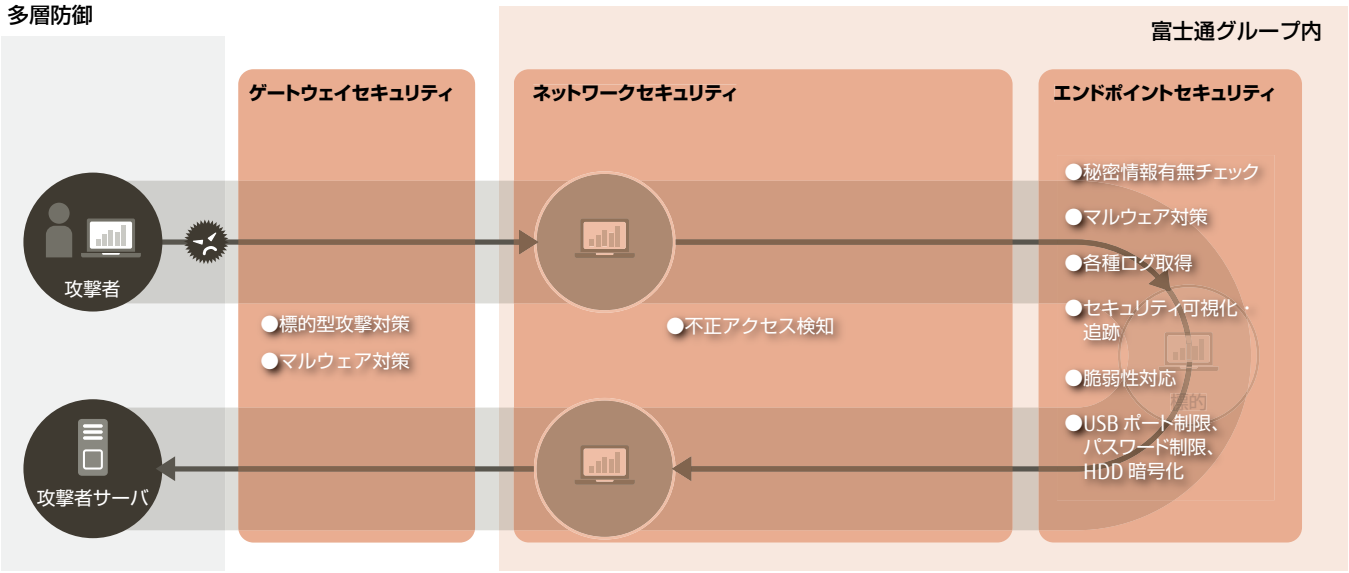
富士通グループでは、従業員のパソコンやモバイル端末など、エンドポイントにおけるセキュリティ施策においても「多層防

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

サイバー攻撃のパターン



多層防御



御」の考え方を取り入れ実践しています。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に分けて必要なセキュリティ施策を実施しています。国内外の富士通グループ共通の情報セキュリティ規定に則り、サポート切れ OS 等のパソコンについてネットワークアクセスの制限を実施し、セキュリティ統制を行っています。

　加えて、情報漏えい対策として、パソコンへのお客様データ等を含む秘密情報の保存や外部媒体への書き出しができないよう制限しています。

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

重点施策

重点施策 ③：物理セキュリティ

オフィスの入り口に限らず、工場などの敷地およびオフィス内のフロアのセキュリティについて、対策を行っています。こちらも多層防御の考え方に沿って、「従業員」と「来訪者」の動線を明確に分離し、確実な入退室管理が行えるセキュリティ施策を適用しています。また、セキュリティカードや監視カメラにより、入退場の詳細な情報を把握するとともに、有事の際の追跡力を強化しています。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。

ポリシー

- 敷地内／建屋内／フロア内には認められた人しか入れない
- 社内外問わず、人員の入退室を明確に把握・記録する

■ 敷地セキュリティ

入退場門でのセキュリティゲート、立哨による入場・退場チェックに加え、外柵センサー・監視カメラによる侵入検知を行い、認められた人しか入れないよう厳正に管理しています。

■ 建屋セキュリティ

セキュリティゲート、セキュリティカードによる建屋入り口での入退室管理を実施し、不正な侵入を防いでいます。

■ フロアセキュリティ

社内ネットワークが敷設された執務エリアは、その他のエリアと分離するとともに、入退室を強化し権限を持たない者が重要な情報にアクセスすることを防止しています。また、たとえ付き添いの従業員がいても富士通グループ従業員以外の入室を禁止し、セキュリティの確保を行っています。具体的には、入退室の際にセキュリティカードによる認証を行い、さらにセキュリティレベルを上げる必要がある場合には、手のひらによる認証を行っています。

手のひら認証を使ったセキュリティゲート（欧州オフィス）

［発行者］

富士通株式会社

総務・リスクマネジメント本部

〒105-7123 東京都港区東新橋 1-5-2 汐留シティセンター

TEL：03-6252-2198