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。

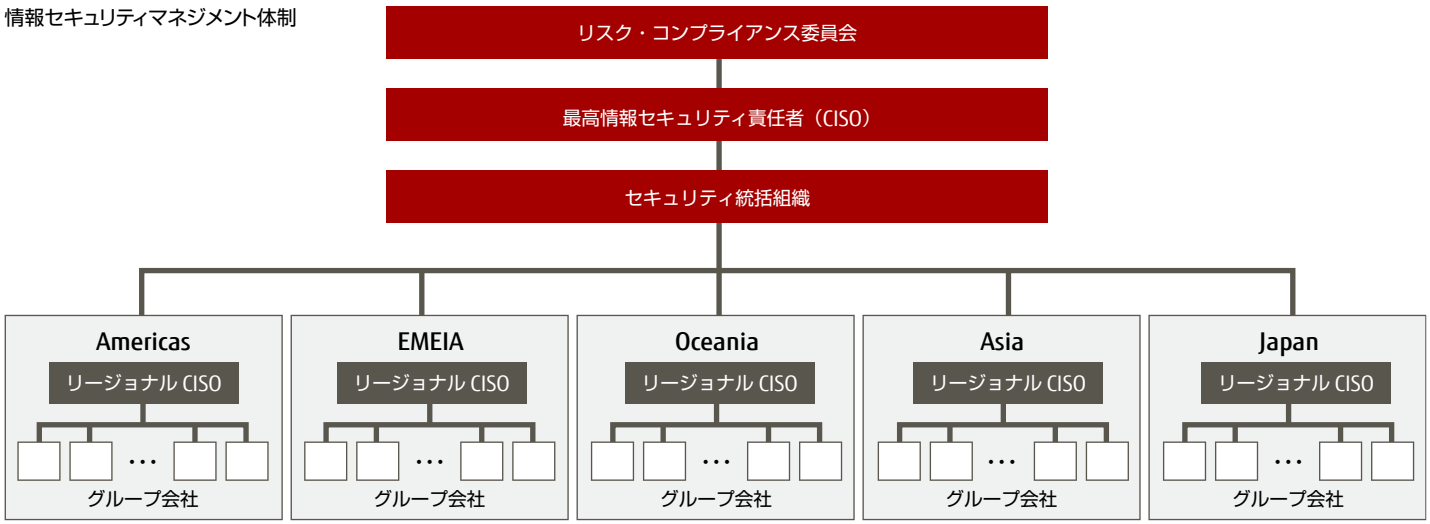
■ 最高情報セキュリティ責任者（CISO）

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

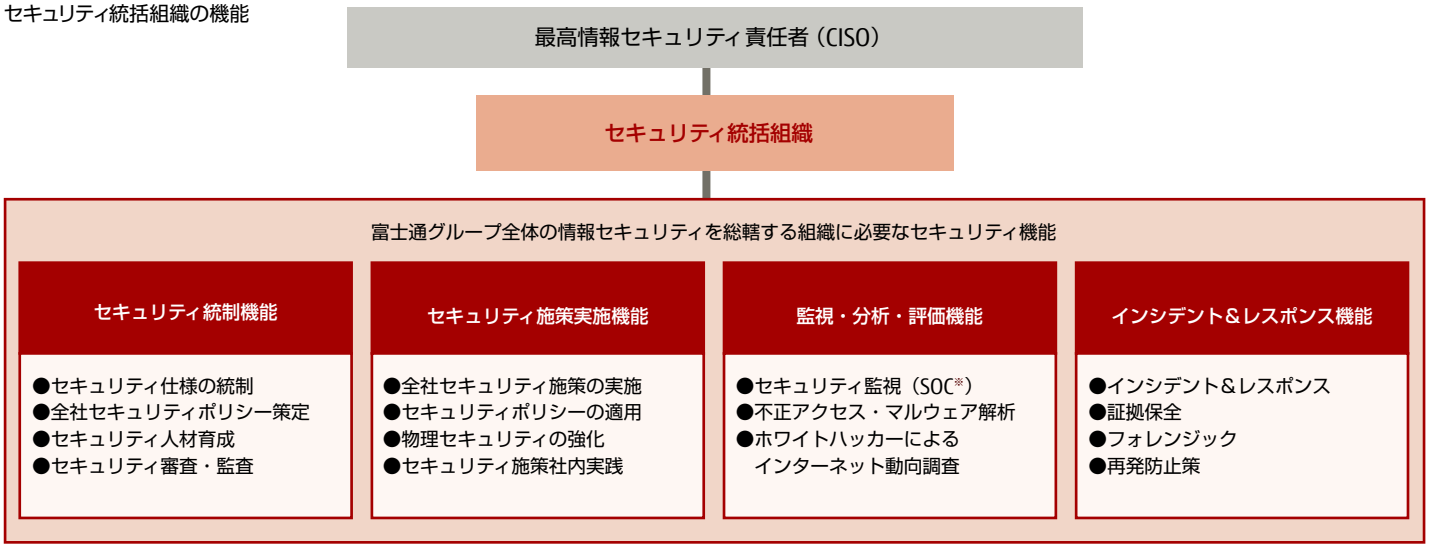
セキュリティ統括組織は富士通グループの情報セキュリティ対策を強化するため、CISO 直轄の組織として設立され、グループ共通のルールや施策の企画立案を行い、一元管理するマネジメントを推進しています。大きく 4 つの機能を持っており、セキュリティ統制機能、セキュリティ施策実施機能、監視·分析·評価機能、インシデント＆レスポンス機能を担い、富士通グループを統制しています。

セキュリティ統制機能

■ 全社セキュリティポリシー策定

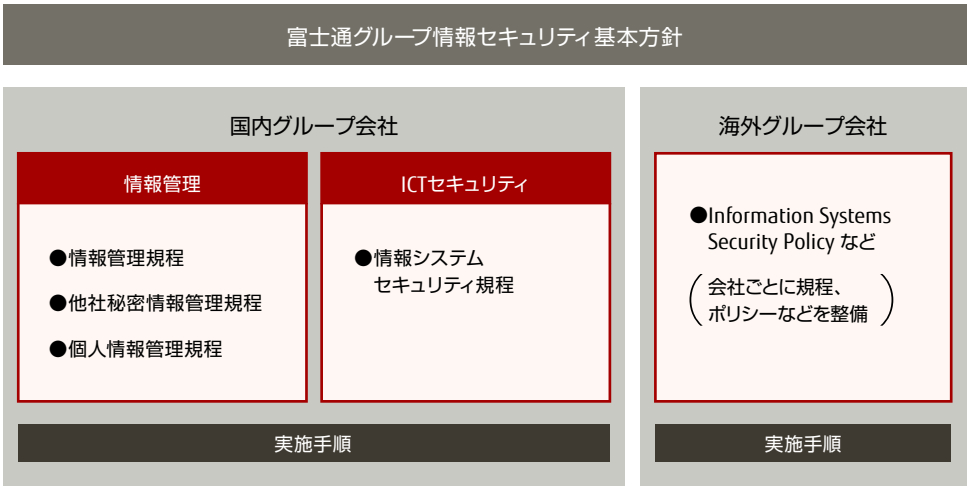
富士通グループ各社は、「富士通グループ情報セキュリティ基本方針」に基づき、国内外のグループ会社において情報管理や ICT セキュリティに関する社内規定を整備し、情報セキュリティ対策を実施しています。グローバル共通の富士通グループ情報セキュリティ基本方針の下、グループ会社向けの情報管理関連規定と情報セキュリティ規定を用意しています。

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。

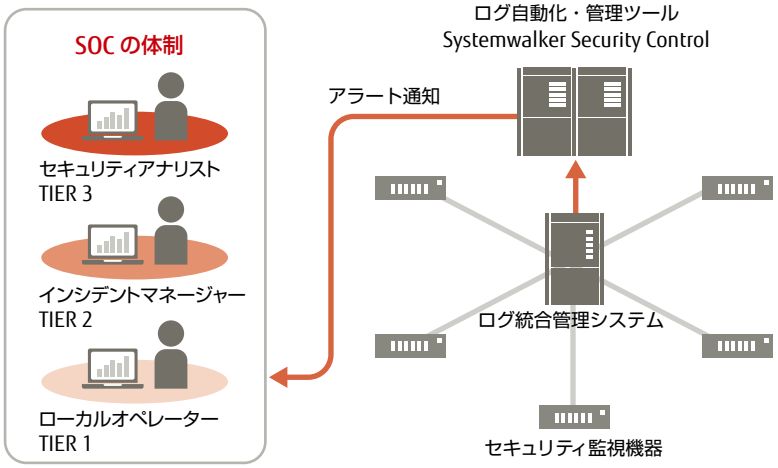
■ フォレンジック

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