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、グループ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

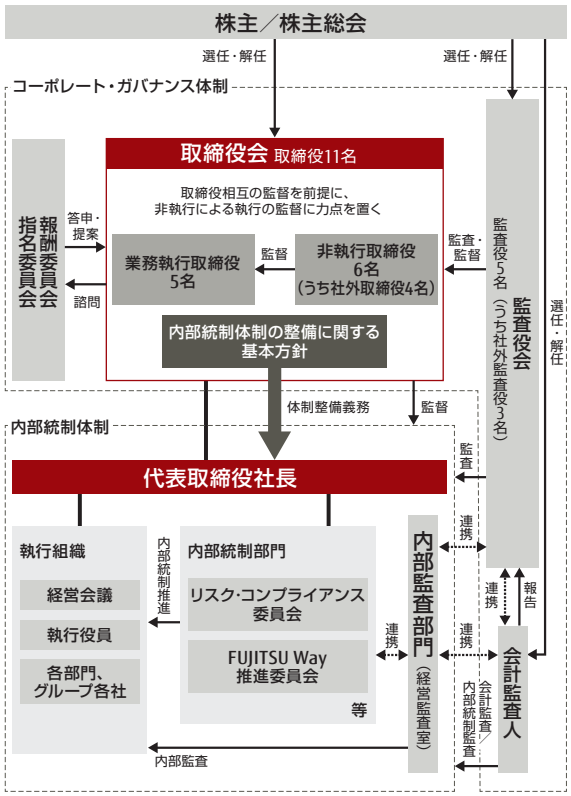
富士通のコーポレート・ガバナンスに関する基本的な考え方は、監査役設置会社制度を採用しつつ、取締役会において「非執行取締役による業務執行取締役の業務執行に対する監督と助言」に力点を置くというものです。

具体的には、取締役相互の監視と取締役会による取締役の監督を前提としつつ、執行と監督の役割分担を明確にし、業務執行を担う「業務執行取締役」に対し、業務執行の監督機能を担う「非執行取締役」を同数以上確保することで、監督の実効性を高めています。

また、非執行取締役候補者の選定にあたり、出身の属性と当社事業への見識を考慮することで、多様な視点から実効性のある助言が得られるよう配慮しています。

さらに、監査役による取締役会の外からの監査・監督と、任意に設置している指名委員会、報酬委員会により取締役会を補完することで、全体としてコーポレート・ガバナンスの整備を通じた株主価値の向上を目指します。

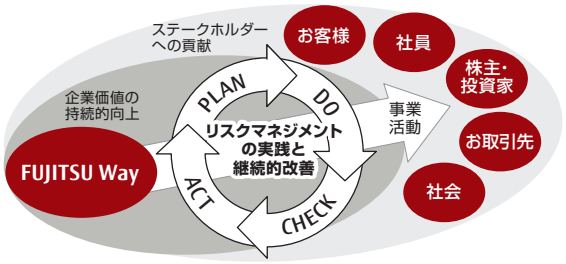
↓コーポレート・ガバナンス体制図



リスクマネジメント

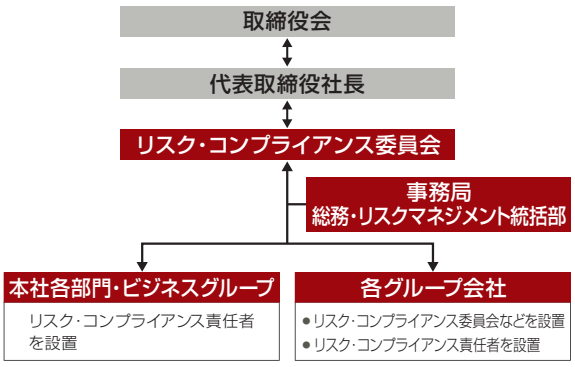
富士通グループは、グローバルなICT事業活動を通じて、企業価値を持続的に向上させ、お客様や地域社会をはじめとするすべてのステークホルダーの皆様に貢献することを目指しています。この目的の達成に影響を及ぼす様々なリスクを適切に把握し、その未然防止および発生時の影響最小化と再発防止を、経営における重要な課題と位置付けています。そのうえで、グループ全体のリスクマネジメントおよびコンプライアンスの体制を構築し、その実践を推進すると共に継続的に改善しています。

↓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・コンプライアンス体制



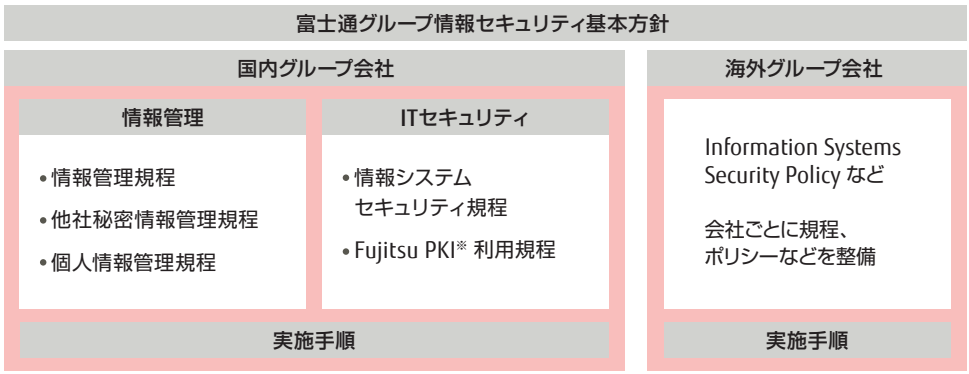
≫ 情報セキュリティの推進

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。

富士通グループ各社は、情報セキュリティ関連規定体系に沿って「情報セキュリティポリシー策定指針」を使い、各国の制度・法律などを考慮しつつ、各社におけるポリシーの整合性を確保します。また「グローバル情報セキュリティ管理策フレームワーク」を用いて、情報セキュリティ対策を選択・決定・実施すると共に、評価・改善を行っています。

↓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。

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、「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、全社員の業務用パソコン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

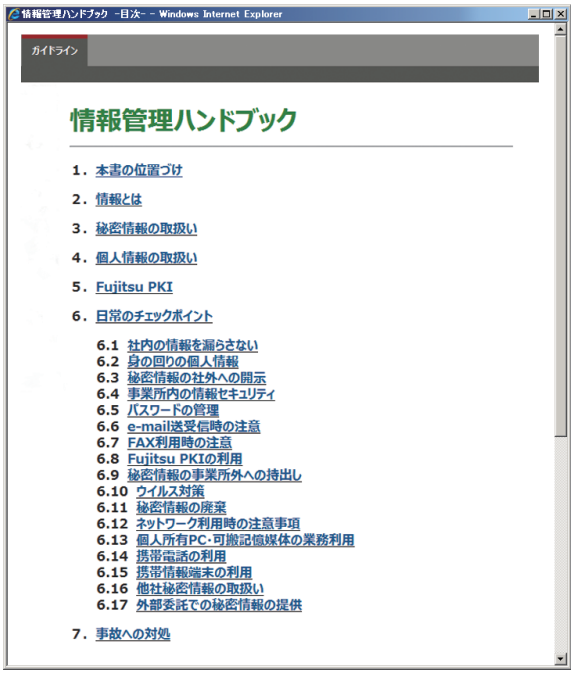
富士通では、「個人情報保護ポリシー」と「個人情報管理規程」を定めています。この規程に基づき、毎年、個人情報の取り扱いに関する教育や監査を実施するなど、継続的に個人情報保護体制の強化を図っています。

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、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」画面



≫ 情報セキュリティ人材の育成 ―セキュリティマイスター認定制度の取り組み―

サイバー攻撃が、社会問題化しています。今後は、マイナンバー（社会保障・税番号）制度導入、さらには500億のデバイスがインターネットにつながるIoT（Internet of Things）時代をむかえ増々攻撃が高度化、巧妙化していくことが予想されます。富士通は、システムインテグレーションおよびサービス運用の最前線で、セキュリティ品質の向上を実践し、堅牢なセキュリティ品質を持つソリューションを実現する情報セキュリティ人材の育成に取り組んでいます。

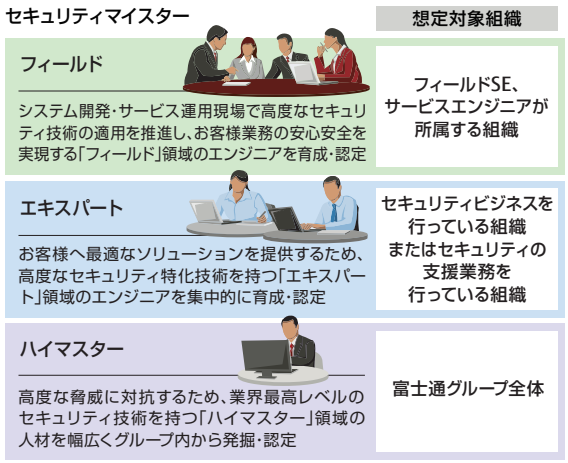
プロフェッショナルな情報セキュリティ人材育成の必要性

昨今の企業や組織を対象とした標的型攻撃による被害が深刻化するなど、サイバー攻撃に関する脅威が多様化・高度化しています。そこで、富士通では、これらの脅威からお客様の情報資産を守る取り組みの一つとして、高いレベルのセキュリティ技術を持つ技術者をグループ内から発掘、認定し、フィールドに配置する仕組みをつくりました。

セキュリティマイスター認定制度

サイバー攻撃から情報システムを守るセキュリティを実践できるスペシャリストを「セキュリティマイスター」という位置付けで、系統的、計画的、継続的に育成し、認定していきます。この制度は、活動領域により「フィールド」、「エキスパート」、「ハイマスター」の3つの領域で区分し定義しています。2016年度末までに700名の技術者の育成・認定を計画しています。

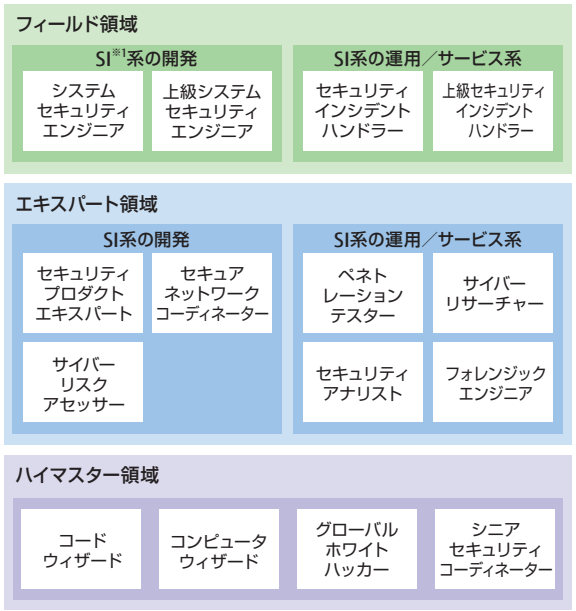
セキュリティマイスターの３つの領域



セキュリティ技術者の人材像を明確化

「セキュリティマイスター認定制度」では、今日のICT開発・ICT運用の現場ニーズに適合したセキュリティ技術者の人材像を定義しています。人材像モデルはICT開発・ICT運用の各場面で求められるセキュリティ技術を、次の3領域15種類の人材像モデルとして具体化しています。

セキュリティ技術者の人材像モデル



具体化にあたっては、日本のITスキル標準、海外の各種セキュリティ技術者人材モデルとの整合性を考慮しています。さらに、ホワイトハットハッカー※2やトップガン人材※3に相当する「ハイマスター」人材像も定義しました。

〔※1〕SI：システムインテグレーション
〔※2〕ホワイトハットハッカー（white hat hacker）：善玉ハッカーのこと。
〔※3〕トップガン（Top Gun）人材：先鋭的な技術者のこと。

以下に定義の例を示します。フィールド領域の「システムセキュリティエンジニア」は、システム開発部門に籍を置き、現場のセキュリティ設計と、技術的なセキュリティ対策の実施を担当する位置付けとしています。

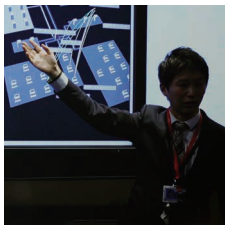
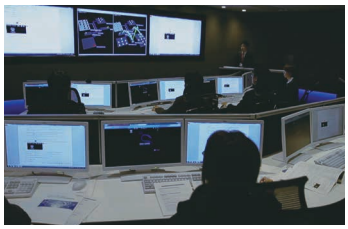
「セキュリティインシデントハンドラー」は、システム運用部門に籍を置き、システムのセキュリティ運用設計と、現場で発生した情報セキュリティインシデントに関してのセキュリティ対策の実施などを担当します。

ハイマスター領域の「コンピュータウィザード」は、組み込み系など開発部門に籍を置き、技術力を活かして独自の研究・情報発信活動を行う人材です。セキュリティにおける最先端の技術を体現する人材と位置付け、自ら積極的にモチベーションをもって、外部団体の活動（研究活動および国内の技術者向けセキュリティセミナーなど）へ参加し、発表を行うことを期待しています。

育成プログラムの整備

実践力を重視したセキュリティ技術者育成プログラムの整備の一環として、人材モデルの類型ごとの専門教育コースを開設しています。また、サイバーレンジ（仮想演習場）を採用した技術者育成教育を新規に開発しました。この技術者育成教育は、広くお客様にもご利用いただける教育コースとして、ご提供しています。

育成教育の風景

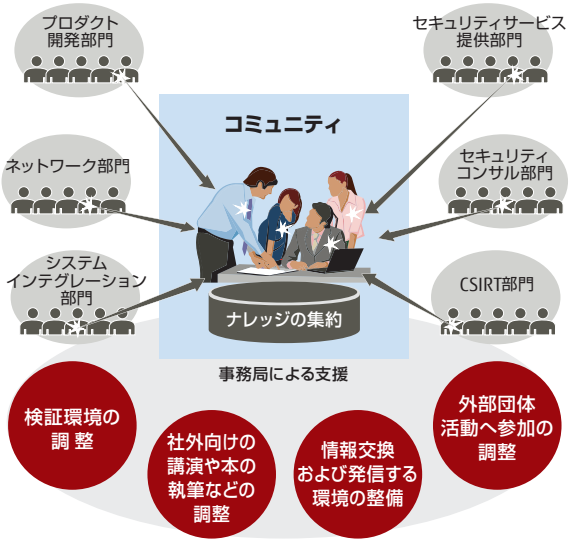
セキュリティ人材の発掘と人口拡大

セキュリティ人材の発掘とセキュリティ技術者人口の拡大を促進しています。社内の各部門に点在しているナレッジの集約化を図り、有効活用するためのセキュリティマイスター・コミュニティを形成しています。このコミュニティでは、有識者同士のナレッジ共有により、認定後のスキル向上にもつながっています。

さらに、ハッキング技術を含むセキュリティコンテストを社内で開催しています。セキュリティコンテストでもサイバーレンジを活用し、同時に40名が技術力を競い合うことが可能です。

このように、富士通では、積極的なセキュリティ人材育成によって、お客様に安心安全をご提供していきます。

セキュリティマイスター・コミュニティ



富士通初のセキュリティコンテストを開催

富士通グループセキュリティ人材の技術力向上、人材交流の一環として、2014年12月に「富士通サイバーセキュリティワークショップ2014」を開催しました（160名参加）。

午前のセミナーは、経営層、幹部社員、現場エンジニアがそれぞれの視点から最前線のサイバーセキュリティをテーマに、二つの会場でセミナーを実施しました。

午後は、富士通グループで初となるハッキング技術やセキュリティ知識を競う「セキュリティコンテスト」が行われ、20組40名の技術者が参加しました。

セキュリティコンテストでは、通常のCTF（Capture The Flag）大会とは異なり、様々な工夫を行いました。

まず、約70問の問題は全て運営事務局が、高度なセキュリティスキルを有する「ハイマスター」の協力を得て独自に作成しました。Webサーバやネットワーク上のパケットデータのどこに答え（Flag）があるのかなどを問う実践的なセキュリティ技術が求められる問題に加え、セキュリティの幅広い知識を問うクイズ問題を出題しました。

また、巧みな話術や覗き見などにより攻撃ターゲットから必要な情報を入手する「ソーシャルハッキング」技術を競う問題も用意しました。

さらに、コンテスト用に構築されたダッシュボードにより競技の模様を可視化することによって、出場者の腕試しだけに留まらず、同時並行で別室の見学者向けにコンテスト中の問題解説をライブで行い、参加者全員のセキュリティ技術向上を狙いました。

参加者からは、「実際に手を動かすことが少なくなっているので、出場者として参加できて良かった」、「自分の実力が分かった」、「問題のアーカイブが欲しい」、「部門間対戦をやりたい」、「Write-up（問題の解説）サイトを開設して欲しい」などの感想やコメントが出ていました。

これからも、富士通グループのセキュリティ人材の技術力向上、人材交流の一環として、コンテストを継続的に開催していきます。

セキュリティコンテストの風景