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、情報セキュリティ施策推進会議事務局は、情報セキュリティマネジメントの礎となる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ています。組織・グループ会社ではセキュリティマネジメントフレームワークを適用し、施策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

昨今、高度化、多様化するサイバー攻撃の脅威、グローバルにおける各種ビジネス規制が課題となっています。その対策・対応方針を検討するために、富士通は、2013年にサイバーセキュリティに関する情報共有、当社ビジネス方針の討議を行う目的で「セキュリティ委員会」を発足させました。

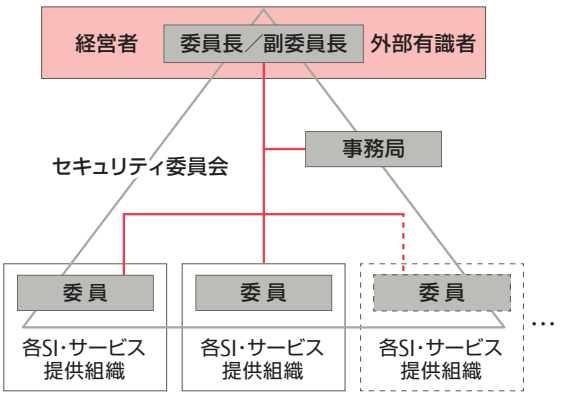
セキュリティ委員会は次のメンバーで構成しています。システムインテグレーション・サービスビジネス各事業を統轄する役員、国内営業・マーケティング・海外ビジネス各部門を担当する役員、第三者性確保のために招へいした外部有識者です。

富士通は、「Fujitsu Technology and Service Vision」を理念として掲げています。ヒューマンセントリック・インテリジェントソサエティでは情報の信頼性が重要であり、情報の利活用を続けられる仕組みづくり、事故を前提とした備えを必須としています。サイバーテロの脅威と対策、各国クラウドセンターが遵守すべき法、個人情報の取り扱いなど、グローバルレベルで対応が必要な案件をセキュリティ委員会で方針を討議し、承認しています。

セキュリティ委員会では、当社のシステムインテグレーションおよびサービスのセキュリティ品質向上活動をうたっています。セキュリティ委員会の下部組織である情報セキュリティ施策推進会議（以下、推進会議と略す）にて社内のセキュリティ活動の方向付けを行い、情報セキュリティ施策推進会議参加組織（以下、参加組織と略す）へ展開しています。

そのほかに、富士通グループ全体のシステムインテグレーションおよびサービスのセキュリティ人材育成を推進しています。

セキュリティ委員会体制

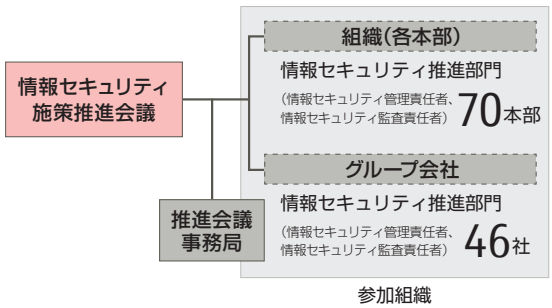


セキュリティガバナンスの構築・実践

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、経営の観点でリスクマネジメントが求められています。富士通は、情報セキュリティガバナンスの下、情報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推進会議に参加しています。セキュリティマネジメントフレームワーク（SMF：詳細は次ページ参照）を基礎として、セキュリティ計画の立案、セキュリティ対策の導入、参加組織で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・評価して、マネジメントの仕組み、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、秘密情報を取り扱っています。そこで、お客様の情報を含めた情報を適切に保護することを目的として、推進会議は「情報セキュリティ施策推進会議　活動方針」を定めました。この活動方針に基づいて、参加組織は情報セキュリティの維持・推進を図っています。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は、四半期ごとに開催される推進会議の会議体に参加し、セキュリティ施策にかかわる情報交換・意見交換の場としています。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。

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）は、参加組織に対して、効果的なセキュリティ対策の支援、改善策の助言などを必要に応じて行い、情報提供・サービス提供をしています。これにより、参加組織は情報セキュリティ活動を継続的に推進しています。

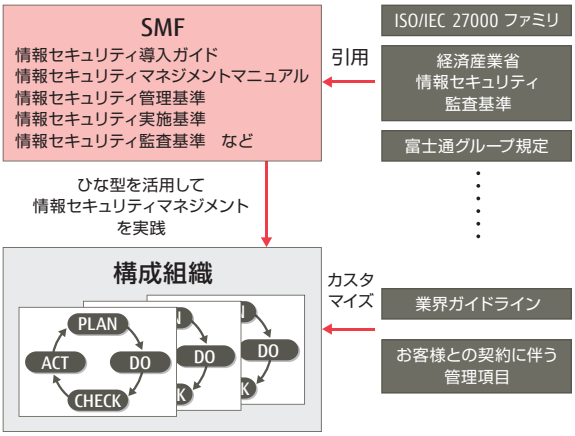
一方、参加組織は、推進会議から要求される情報セキュリティ活動を推進することで、組織としての情報セキュリティのレベルを維持しています。

SMF（セキュリティマネジメントフレームワーク）

参加組織が情報セキュリティマネジメントを実践するために、推進会議事務局はSMFのひな型を提供しています。SMFは、富士通グループ規定を基準とし、ISO/IEC 27000ファミリ、経済産業省の情報セキュリティ監査基準など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、お客様の業界ガイドライン、お客様との契約に関わる管理項目などのセキュリティ要求事項を満たす必要があります。このため参加組織は、SMFひな型を基に情報セキュリティ関連文書を規定し、運用を行います。

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」を開講しています。2012年度から、管理責任者を対象に継続的な自己研鑽促進のため、e-Learning教育を開講しています。内部監査人向けの教育として、「情報セキュリティ監査人教育」を開講しています。

施策推進会議では、内部監査の質向上と監査人のキャリアパスを目的として、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。2014年度までに141名が認定を受けて、内部・外部監査で活躍しています。

そのほかに、情報セキュリティ教育の教材を提供し、各組織で活用されています。

教育受講者数

教育コース名	受講者数
情報セキュリティ管理者教育（集合形式）	648名
情報セキュリティ管理者教育（e-Learning版）	652名
情報セキュリティ監査人教育	1,252名

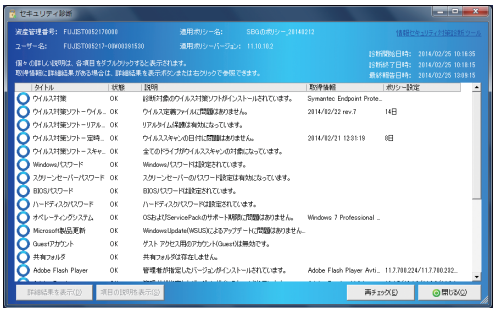
定期的なセキュリティチェック活動

富士通グループでは毎月「セキュリティチェックデー」活動を行っています。この施策で、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状態の確認を行っています。推進会議では情報セキュリティ対策診断ツール（IT Policy N@vi）をパソコンに導入することを義務付けて、各パソコンのセキュリティ対策・運用状態を診断しています。このツールは、パソコン起動時に診断項目※を自動的に診断し、診断結果をパソコン画面に表示します。各組織の情報セキュリティ管理責任者は、すべてのパソコンについて診断結果を容易に確認し、セキュリティ対策の浸透を維持しています。

スマートデバイスについては、社内規程に準拠した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。

〔※〕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19項目があります。

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

推進会議では、情報セキュリティ監査として内部監査と外部監査を実施しています。内部監査は、参加組織が自組織を対象に実施する監査です。外部監査は、推進会議事務局が第三者の観点で実施する監査を意味します。

参加組織は定期的に内部監査・外部監査を受けることで、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、改善の指針としています。

外部監査は推進会議事務局が毎年テーマを定めて、監査計画を立案しています。監査チームは、推進会議事務局を中心としたJASA監査人資格を保有する監査人で構成します。この監査チームが、情報セキュリティのマネジメント推進状況を確認し、不備事項の指摘や、改善事項の提案など行い、参加組織全体のセキュリティ維持・向上を図っています。また、被監査組織の優れた施策を推進会議会議体で事例として紹介し、参加組織全体のセキュリティレベルの底上げに活用しています。

そのほか、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、推進会議事務局の専門家が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。

ソーシャルメディア教育

昨今、情報通信手段としてSNS※が私たちの生活に浸透しています。一方で、業務利用、私的利用問わずに、利用機会の増加に伴い、企業責任が問われる事案が発生しています。

そこで、富士通では、ソーシャルメディアを利用する場合のルールとマナーをガイドラインとして定めています。これに基づき、推進会議事務局は、参加組織向けに「情報セキュリティ実践講座（ソーシャルメディア利用編）」を作成し、提供しています。

SNSを利用するリスクについて事例を通して解説し、SNSの正しい利活用のために啓発を行っています。

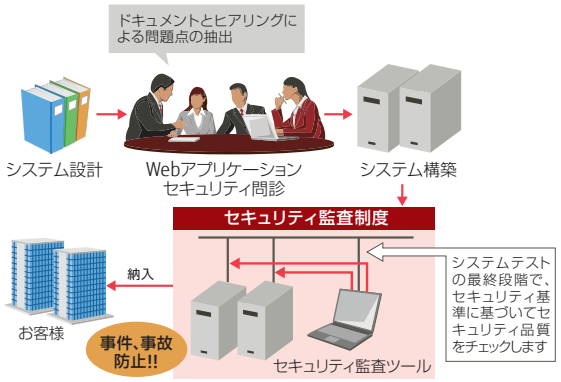
〔※〕SNS：Social Networking Service

お客様納入システムのセキュリティ監査

富士通グループでは、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）が満たすべきセキュリティ基準を定めています。

また、お客様納入システムを納入する前に、品質検査の一環としてセキュリティ監査を受けることが義務付けられており、セキュリティ基準を満たしていることをセキュリティ専門の部署が客観的な観点で確認しています。

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アプリケーションセキュリティ監査では、セキュリティに関する問題点を早期に抽出し、解決するため、システム構築の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が、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されていることを確認し、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。