ITセキュリティへの取り組み

ICTを活用する場面では、業務に関する大量の情報を集積してこれを容易に扱える状態に置くことになり、情報の漏えい、毀損、利用不能その他の様々な脅威が伴います。
このため、富士通グループでは、グループ全体の共通課題としてICTの活用において情報の安全管理を確保するITセキュリティに取り組んでいます。

業務を支援するITセキュリティの追求

富士通グループでは、ITセキュリティは、業務の利便性や効率を妨げるものとせず、むしろ、業務を支援するものとすることを目指しています。
情報セキュリティ対策のために規制を過剰なものにすると、従業員にとって規則の理解や遵守が負担になり、ともすると現実には守れないものになりかねません。
富士通グループのITセキュリティでは、対策をできる限り業務環境や業務手順に組み込んで実現します。こうして、従業員が本来の業務に専念できるようにすることが重要だと考えています。
また、ICTの進歩と共に脅威も変容する中で有効な対策を維持するためには、技術的な対策を開発・実装し、問題を解析して対応するための先端技術が必要であると考え、ITセキュリティのための専門の部署を置いています。
加えて、開発・実装された技術的な対策は、お客様に提供する前に自ら実践し、その効果や実用性の確認も行い、製品※にフィードバックを行っております。
〔※〕製品：FENICSⅡユニバーサルコネクトサービスなど

ITセキュリティの枠組み

富士通グループにおけるITセキュリティの施策は、ITセキュリティ関連規定に基づいて実施しています。情報を取り扱う場面に応じた施策に「業務システムにおける情報管理」、「クライアントセキュリティ統制」、「利用者の一元管理を実現する認証システム」と「ネットワークセキュリティ統制」があり「資産管理」がこれらの基礎になります。また、「ITセキュリティ監査」を行い、施策の定着と改善を進めています。

ITセキュリティの枠組み

ITセキュリティ関連規定			
●場面の設定　●役割と責任　●PDCAサイクルの確立			
業務システムにおける情報管理	**クライアントセキュリティ統制**	**利用者の一元管理を実現する認証システム**	**ネットワークセキュリティ統制**
業務・情報・利用者の分析に基づく ●アクセス制御機能 ●信頼性維持機能	●対策の自動化 ●電子メール誤送信対策 ●社内標準パソコン	セキュリティカードによる ●入室管理 ●認証 ●文書の決裁	●ネットワークの統制 ●電子メールの統制 ●ネットワークサービス利用の統制
ITセキュリティの基礎となる資産管理			
●財産としての現物管理　●セキュリティ対策管理　●ライセンス管理			
ITセキュリティ監査			
●実施状況の確認			

ITセキュリティ関連規定

富士通グループのITセキュリティ関連規定は、1.～3.に示す3つの特長があります。

1. 場面の設定
ICT活用の主要な場面には、次のものがあります。ITセキュリティ関連規定では、それぞれの場面において実施すべきITセキュリティ対策を定めています。
- サーバを中心に業務情報を蓄積し取り扱う業務システム
- パソコンなどを活用する事務所その他の職場
- 職場をつなぐ事業所内や事業所間のネットワーク

2. 役割と責任
ITセキュリティ対策の実施について役割と責任を定め、業務システムや職場ごとに、ITセキュリティ対策の実施に責任を負う者を指名させます。また、対策の実施を統制する部門の権限を定めています。

3. PDCAサイクルの確立
ITセキュリティ対策の実施、啓発と教育、周知、事故への対応、評価と改善を含む、PDCAサイクルを構成するそれぞれの要素について規定し、施策の定着と改善を図っています。

業務システムにおける情報管理

富士通グループでは財務・経理、人事・総務、営業、購買、SE業務、生産・物流、製品開発管理をはじめとする様々な業務にICTを活用しています。そこに保有し、取り扱う様々な情報について、業務や職責に応じたセキュリティ要件があります。この要件を分析し、利用者の立場や資格に応じて情報へのアクセスを制御するアクセス制御機能や、業務の重要性や継続性要件を満たす信頼性維持機能を装備し、運用しています。

クライアントセキュリティ統制

情報セキュリティの重要な課題は、ヒューマンエラーへの対策です。ICTを活用する人の行為において、注意力に頼るだけでは情報セキュリティ事故は防ぎきれません。対策として教育を充実し、啓発活動により注意を喚起することは当然ですが、それでもなお、情報漏えいその他の事故がICTでの対策の及ばないところで発生します。

この事実を踏まえて、人の行為が係わるクライアントの業務プロセスに着目し、注意力に依存する対策をICTによる対策に置き換えることの可能性を検討し、具体化してきました。

■ パソコンにおける対策の自動化

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ウイルス定義ファイルの更新を自動化しています。

■ 電子メール誤送信対策

電子メールは、宛先や添付ファイルを間違うと容易に情報が漏えいしてしまいます。そこで、電子メールの宛先を自動的に識別して、外部への送信について送信者に再確認の操作をさせるなどにより、誤送信を削減しています。

■ 富士通標準パソコンの導入

富士通標準パソコンとは、社内利用向けに標準に定めた機種と仕様のパソコンです。暗号化ハードディスクの使用、BIOSパスワードおよびスクリーンセーバーの設定、資産管理ソフトウェアおよびウイルス対策ソフトウェアの搭載などのセキュリティ対策済のものを配布します。これにより、利用者を各種セキュリティ対策の実施から解放し、対策の確実な実施を実現します。加えて、パソコンの選定・導入・運用を定型化し、費用の削減を行います。

■ クライアント機器の社外での安全な使用

パソコンやスマートフォンなどのクライアント機器は、自宅や出張先などの社外でも業務に使います。このとき、機器の盗難・紛失の恐れや、機器からの情報流出の恐れがあるため、機器のセキュリティ対策実施状況を確認するセキュリティチェックデー（毎月実施）や、注意事項を周知徹底するための情報セキュリティ教育（年一回実施）を行っています。

また、ICTによる技術的な施策として、情報を持ち出さず社外でクライアント機能を活用できる「仮想デスクトップサービス」やモバイル機器で利用できる「専用アプリケーション」を導入し、重要な情報の保護に活用しています。

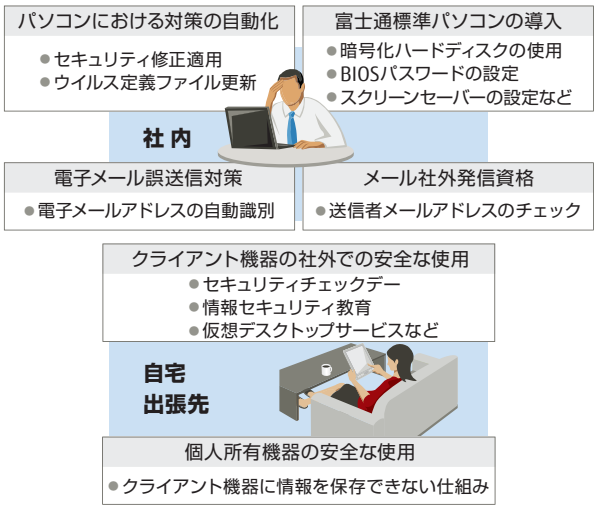
■ 個人所有機器（パソコン、スマートフォンなど）の安全な使用

個人が所有するパソコンやスマートフォンなどを使用して電子メールや社内の業務システムを安全に利用するために、「仮想デスクトップサービス」や「FENICSⅡユニバーサルコネクト」を活用しています。これらのサービスでは、利用者の不注意による秘密情報の保存・漏えいを回避するため、クライアント機器に情報を保存できない仕組みにしています。私的な情報と社内のネットワークへの接続は機器の中で隔離され、業務情報の安全な管理が確保されています。

■ 社外への電子メール発信の管理

電子メールを社外に発信する資格の有無を確認します。これにより、業務上不要な利用者による社外へのメール発信・情報漏えいを防止します。

■ クライアントセキュリティ統制



ITセキュリティの基礎となる資産管理

サーバ、パソコンなどに関する資産を管理するIT資産管理は、財産管理の役割だけでなく、ICT活用やITセキュリティの基礎になります。富士通グループでは、「ITリソース管理システム」と呼ぶ業務システムでIT資産管理を行っています。

ITリソース管理システムには、以下の情報を保有しています。

■ ハードウェア資産：サーバ、パソコンの機種、仕様

■ ソフトウェア資産：サーバ、パソコンごとに使用しているソフトウェアとその版数

■ セキュリティ修正の適用状況

ソフトウェアとその版数を管理することにより、ライセンス契約に合致したソフトウェアの導入を自動化しています。また、ソフトウェア資産やセキュリティ修正適用の進捗状況を管理者が把握し、対処を指示します。

このITリソース管理システムは、統合運用管理ソフトウェアSystemwalkerのセキュリティ管理製品であるSystemwalker Desktop Patrolで構築し、IT資産とセキュリティの状態や、ソフトウェアライセンスを一元的に管理しています。

利用者の一元管理を実現する認証システム

富士通グループでは、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ています。また、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。これらの情報は、富士通グループ内で一元的に管理されたその従業員に固有の情報です。

セキュリティカードは、人事部門の管理の下で、従業員の入社時に交付し退社時に返却させるため、その使用者が正当な従業員であることが保証されています。また、紛失時には失効させて、悪用を防ぎます。

セキュリティカードの主な用途は次のとおりです。

入室管理

富士通グループの事業所では、建屋や事務所の入口にセキュリティドアを設置しており、出社した従業員は、セキュリティカードを使って入室します。

認証

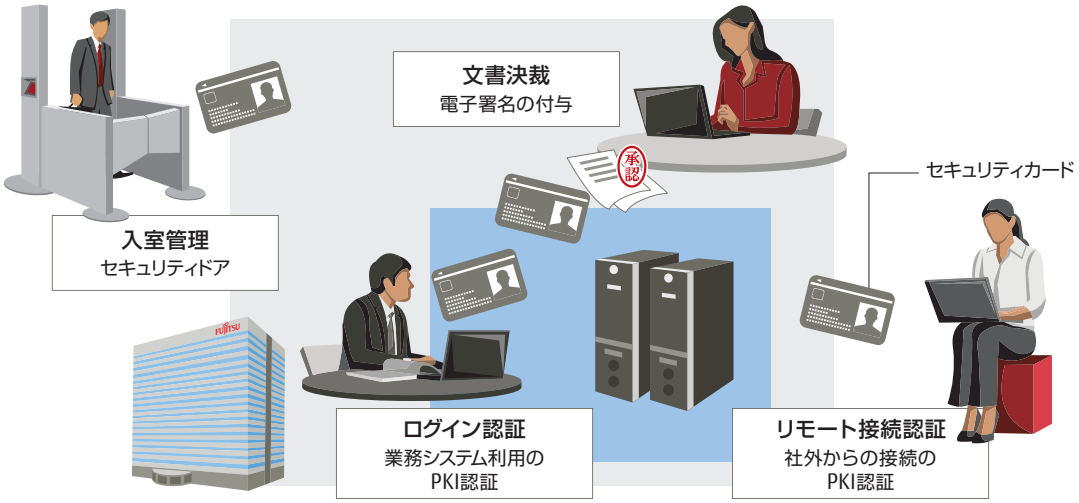
業務システムの利用にセキュリティカードが必要です。業務システムへのログインでPKIによる認証を行っているため、従業員の識別と認証が確実に行われ、しかも操作は容易です。

業務システムを出張先など社外から利用することもできます。その場合には、リモート接続についてPKIによる認証を行い、確実な本人確認を行います。

文書決裁

セキュリティカードは、電子文書の決裁にも利用します。決裁者は、PKI機能を利用して、電子文書に電子署名を付与します。これは、決裁者本人がその文書を確認して決裁したことを示す点で、紙の文書への決裁印の押印と同じ効果があります。

セキュリティカードの利用



ネットワークセキュリティ統制

インターネットは、業務連絡手段として、また、広報・情報提供の手段として、あるいは外部の膨大な情報の活用手段として業務に欠かせません。その反面、インターネットのオープン性や仕組みに由来する深刻な脅威も無視できません。富士通グループでは、先端技術を持つ専門の部署が脅威への対策にあたると共に、全世界でインターネットの出入り口を統合管理し、従業員の負担を最小限に留めて安全を確保しています。

ネットワークの統制

ネットワークに関して、以下の対策を行っています。

■ インターネット接続およびイントラネット構築・運用の統制
- 専門の部署によるファイアーウォールなどのゲートウェイシステムの設置・運用
- 部門が行う接続の審査・許認可

■ 運用時のセキュリティ維持
- 不正アクセス対策（サーバの設定、機器管理状況の確認、不正通信の監視・阻止）
- 安定稼働のための性能管理、信頼性設計

■ モバイル機器への対応
- パソコンやスマートデバイス※を使って、社外からイントラネットへ接続して安全に業務を行う環境の整備と運用

〔※〕スマートデバイス：スマートフォンやタブレット端末のこと。

■ 変容する脅威への対応
- 標的型メール攻撃やAPT（Advanced Persistent Threat）などの従来の対策手法では対応が困難な新たな脅威について、その動向分析・情報収集および対策
- 攻撃手法と対応の研究
- 利用者への啓発・教育活動

電子メールの統制

電子メールは、現在の業務遂行に無くてはならないものとなっています。その安全管理のために、以下の対策を行っています。

■ 電子メールの統制
- ●専門の部署による電子メールサーバの設置・運用

■ 運用時のセキュリティ維持
- ●ウイルス対策
- ●迷惑メール対策
- ●安定稼働のための性能管理、信頼性設計

ネットワークサービス利用の統制

社外のインターネット環境にはファイル転送やオンライン会議などの様々なネットワークサービスがあります。これらについて、業務上の利便性や必要性と、クライアントセキュリティ統制が向上した現状を勘案して、制限を設けながら利用を認めています。他方では、情報漏えいにつながる恐れのある特定のネットワークサービスは、利用を禁止しています。また、誤使用を防止するために、このような通信を常時監視しています。

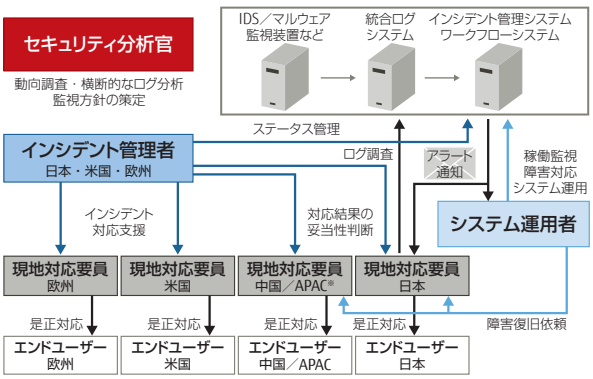
イントラネット利用の統制

富士通グループ全体で、「富士通グループ情報セキュリティ基本方針」を基礎とするグローバルな統制の重要な要素として、イントラネット利用の統制を行っています。その情報セキュリティ対策は、国や地域によらず共通の水準を達成し、維持する必要があります。このため、世界中のグループ会社におけるイントラネットの構築や利用におけるセキュリティ対策を、共通のポリシーおよび管理施策に基づき統制します。

グローバルに一つのイントラネットを持っていることに対応して、ネットワークのインシデント対応も、専門組織であるSOC（Security Operation Center）によるグローバルな統制の下で行っています。一日に世界中のグループ会社で検知されるネットワークのアラートは、数億件にのぼります。これらのリスクレベルを判定し、インシデントとして扱う事象を特定し、これに迅速に対応します。その特徴は、次のとおりです。

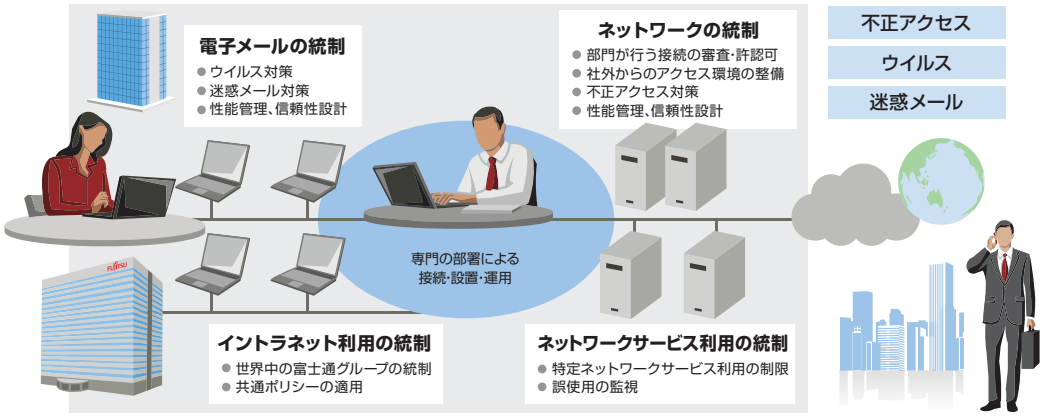
- ●グローバルに統一したリスク基準と対応プロセス
- ●大量の事象およびログの自動での判定
- ●各地域に配置したSOC要員による、時差を活用した24時間の対応
- ●インシデント管理者やシステム運用者の連携を支援するワークフローシステムによる対応時間の短縮
- ●専門のセキュリティ分析官による脅威状況の把握と新規施策の立案

ネットワークのインシデント対応　－SOC－



〔※〕APAC：Asia-Pacific

ネットワークセキュリティ統制



ITセキュリティ監査

これらのITセキュリティ施策を対象に、被監査部門である実施部門から独立した監査部門が監査の年度計画を策定し、これを実行しています。監査は、その対象に適した方法で行います。監査人が現場に出向いて機器の管理状態や設定を目視で確認する方法、実施部門による点検の結果を査閲する方法、ネットワークを通して技術的に脆弱性を検査する方法などがあります。被監査部門は、監査結果を活用してITセキュリティ対策の実施を改善します。