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。

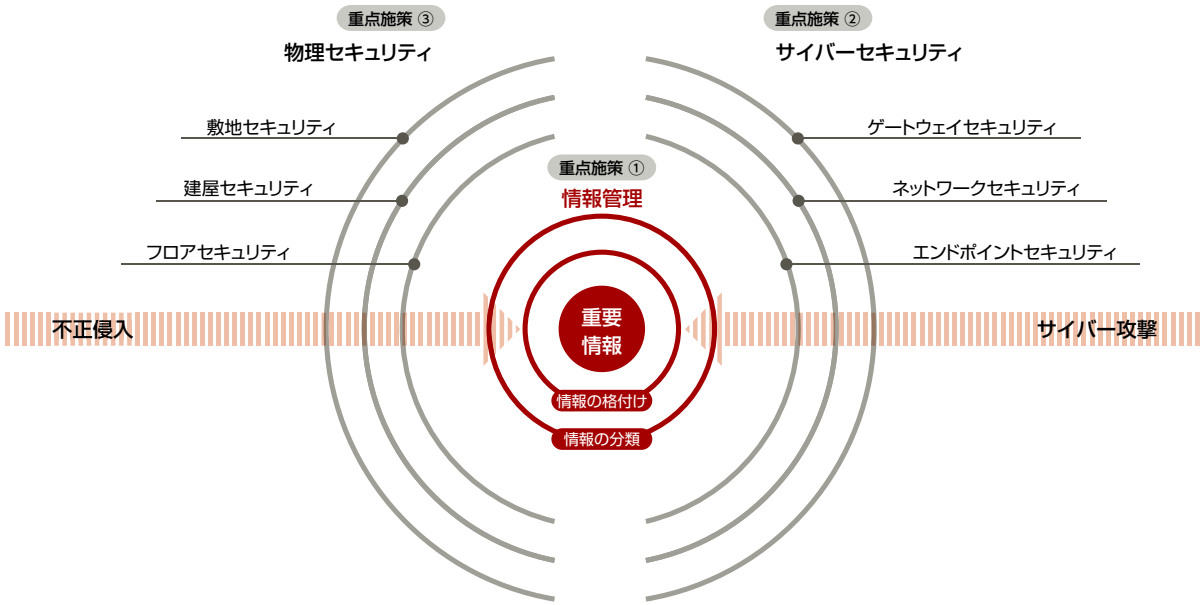
重点施策 ①：「情報管理」のセキュリティ

■ 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。

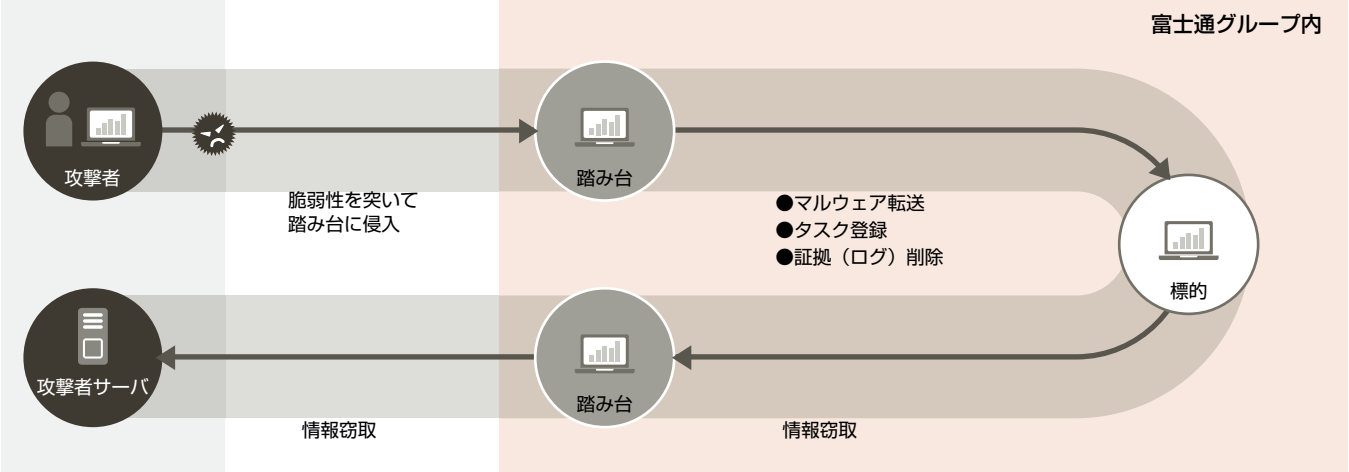
■ エンドポイントセキュリティ施策

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。

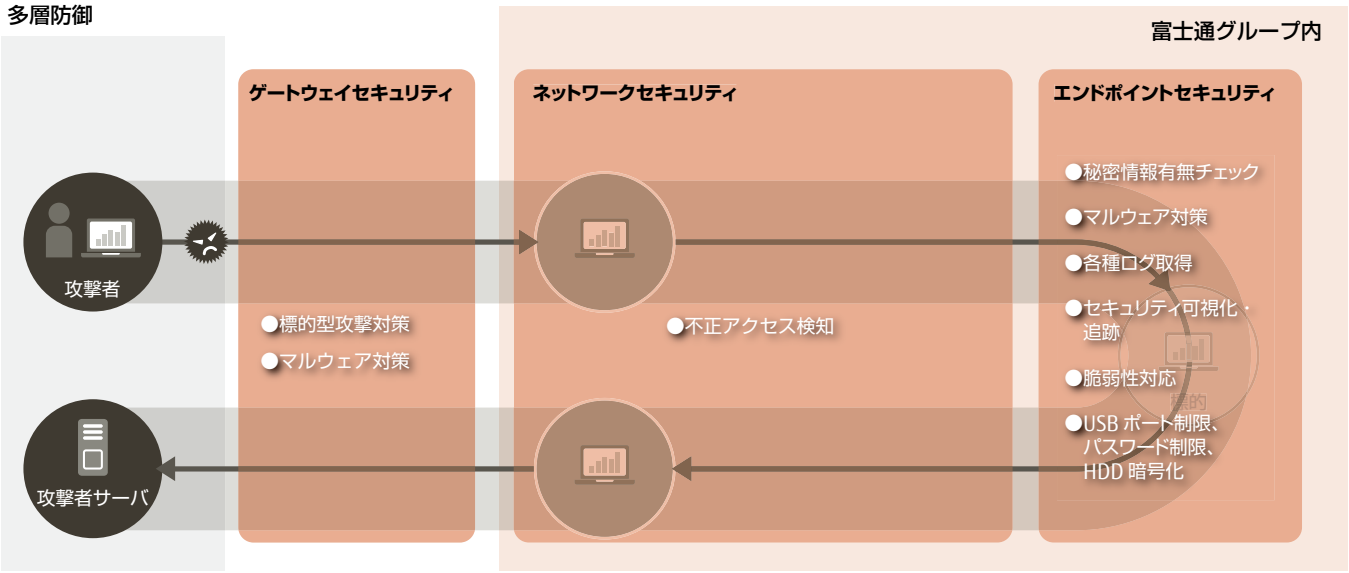
富士通グループでは、従業員のパソコンやモバイル端末など、エンドポイントにおけるセキュリティ施策においても「多層防

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）