FUJIFILM
Value from Innovation

FUJIFILM HOLDINGS CORPORATION

情報セキュリティ報告書

基本情報

本報告書を発行している目的と対象期間、対象範囲などは、以下のとおりです。

本報告書の目的

本報告書は、富士フイルムグループの情報セキュリティへの取り組みをステークホルダー[1)]の皆様に説明し、事業への信頼性を高めていただくことを目的として発行しています。本報告書の内容は、情報セキュリティの効果を阻害しない範囲で、ステークホルダーの皆様に開示することが適当であると判断した情報を記載しています。

本報告書の対象期間

本報告書が対象とする期間は、2019年4月1日～2021年3月31日です。(期間外を対象とする場合は、日付を記載しています。)

本報告書の対象範囲

本報告書が対象とする組織は、富士フイルムグループ(富士フイルムホールディングス、及び傘下の全連結対象会社。以下、全社)とします。連結対象会社は下記URLに記載しています。

https://holdings.fujifilm.com/ja/about/affiliates

本報告書の責任部署・お問い合わせ先

〒107-0052
東京都港区赤坂九丁目7番3号
富士フイルムホールディングス株式会社
ESG推進部
コンプライアンス&リスク管理G

TEL: 03-6271-2069

1) 本報告書における「ステークホルダー」とは、お客様、従業員、パートナー企業、株主、地域住民、そのほかの利害関係者とします。

Contents

トップメッセージ 3
情報セキュリティ体制 4
製品・サービスの情報セキュリティ 8
お客様への安全のご提案 11
社内の情報セキュリティ 13
第三者評価・認証 18
今後の計画について 19

情報セキュリティ基本方針

わたしたち富士フイルムグループは、オープン、フェア、クリアな企業風土のもと、信頼される企業であり続け、社会への責任を果たすため、事業活動における重要課題の一つである情報セキュリティの維持向上に向け、情報セキュリティ基本方針を定めます。

1. 情報セキュリティに関する各種ルールの整備と遵守

当基本方針に従うため、ならびに業務を遂行している地域で適用されるすべての法令や規制等を遵守するために、規程やガイドライン等のルールを整備し、遵守徹底を図ります。

2. 情報セキュリティ管理体制の確立

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。情報セキュリティ管理体制のもと、社会の一員として、社外の情報セキュリティ関係組織との間で、適切な情報提供と積極的な情報収集をします。

3. 情報セキュリティに関する教育

情報セキュリティ対策を適切かつ確実に実施するため、啓発と教育・訓練による意識向上に努めます。

4. 情報セキュリティ対策の継続的改善

法令や規制の要求事項の変化やサイバー攻撃などにおける新たな情報セキュリティリスクに対応するため、リスクアセスメントをもとに各種施策を必要に応じて見直し、継続的な改善に努めます。また、取引先様などサプライチェーンのセキュリティの維持・向上を図ります。

5. 情報資産の保全・保護

社員行動規範にもとづき、お客様・お取引様の情報や自社の技術情報等、重要な情報を漏えい・改ざん・滅失などにつながる脅威から守ります。お客様の情報を守るために製品・サービスのセキュリティ確保に努めます。万一、事故が発生した場合には、被害拡大防止等の初動対応を迅速に実施することで影響を最小限に抑えるとともに、再発防止に努めます。

6. 法令等の遵守

業務を遂行している地域で適用される情報セキュリティに関する法令、お客様や取引先様等との契約を遵守します。

富士フイルムグループは、先進・独自の技術で人々の生活の質の更なる向上に寄与していくため、すべての事業活動の基盤となる情報セキュリティの継続的な強化に取り組んでいます

富士フイルムグループは、社会の文化・科学・技術・産業の発展、健康増進、環境保持に貢献し、人々の生活の質のさらなる向上に寄与することを企業理念としています。

当社はこの企業理念に則り、これまで多岐にわたる事業分野で培ってきた先進・独自の技術を駆使し、新たな価値を生み出すことで、人々の暮らしにおけるさらなる快適さ、便利さの提供と社会が直面するさまざまな課題への解決に取り組んでいます。

これらの取り組みを加速していくには、生産性の向上や既存ビジネスの変革、新規ビジネスの創出をもたらすAI/IoTの活用、デジタルトランスフォーメーション(DX)が欠かせません。当社では全社横断的にDXを推進しており、例えば①AI活用による既存製品・サービスの強化および社内業務の効率化、②IoT活用による、機器のリモート保守、③さまざまなマーケティングデータの収集・分析による、顧客ニーズやセグメントに応じたきめ細やかな提案を行うデジタルマーケティングなど、戦略的に重要度の高いテーマを掲げ課題解決に向け取り組んでいます。

そして、DXの推進においては、当社の機密情報のみならず、お客様の個人情報などの重要な情報資産を処理するため、サイバー攻撃などの脅威から確実に保護できる環境(情報セキュリティ)を整備し、お客様をはじめとしたステークホルダーの皆様が、当社の製品・サービスを安心してご利用いただけるようにすることが不可欠です。それゆえ当社は、情報セキュリティを極めて重要な経営のテーマと位置付け、社内IT基盤強化、製品・サービス開発、生産というそれぞれの切り口から、情報セキュリティ対策に力を注いでいます。

具体的には、社内IT基盤をはじめとした各種情報システムに対しては、ますます高度に巧妙化したサイバー攻撃の脅威に対応するため、組織横断的なサイバーセキュリティ対応チーム「FUJIFILM CERT※」を立上げました。FUJIFILM CERTは、監視や情報収集活動で発見されたインシデントに迅速に対応し、被害を未然に防ぐ活動に力をいれています。

製品・サービスの開発においては、製品のライフサイクルを通じたセキュリティマネジメントを推進しており、製品の企画・設計段階から情報セキュリティ対策を盛り込み、また製品化後もセキュリティ上の課題 が発見された際に速やかに対応できる体制整備を進めています。

さらに生産分野では、生産効率向上を目的にしたIoT機器の利用推進やあらゆる現象をデータ化して解析を行うためのネットワーク化拡大によりサイバー攻撃の脅威が高まる中で、製品供給を止める事態を発生させないよう、生産システムのセキュリティ強化に取り組んでいます。

本報告書では、こうした我々富士フイルムグループが日々推進している情報セキュリティの活動についてご紹介しています。是非ご覧いただければと思います。

※FUJIFILM CERT(FUJIFILM Cybersecurity Emergency Response/Readiness Team):サイバー攻撃対応などの脅威に対応するため、インシデント対応、脆弱性対応、セキュリティ課題対応をおこなう社内対応体制

代表取締役社長・COO
助野健児

情報セキュリティガバナンス

富士フイルムグループは持ち株会社である「富士フイルムホールディングス株式会社」を中心とするグループ経営を展開し、事業会社である富士フイルム株式会社および富士フイルムビジネスイノベーション株式会社(以下富士フイルムBI)ならびに関係会社などで構成されています。(詳細はP.19富士フイルムグループの概要をご覧ください。)

富士フイルムグループでは、お客様に安心して当社の製品・サービスをご利用いただけるように、さまざまな情報セキュリティの取組みをおこなっています。本章では、富士フイルムグループにおける情報セキュリティの考え方、ガバナンス体制についてご紹介します。

富士フイルムグループの情報セキュリティの考え方

富士フイルムグループはESG(環境、社会、ガバナンス)を経営の重要なテーマとして捉え、情報セキュリティをその中の重要な活動として、取り組んでおります。

富士フイルムグループはこれまで、銀塩写真技術によるイメージング事業と、ゼログラフィ技術によるドキュメント事業が中心でした。現在は、業態を大きく変革し、医薬やメディカルシステムなどのヘルスケア事業や、ドキュメント事業はITを活用したソリューション・サービスに変化しつつあります。

これらの事業変革によって、当社の技術情報のみならず、お客様の重要な情報をお預かりし、処理する機会が増え、情報セキュリティの重要性が益々高まっております。

また、各事業でグローバル化が急速に進展しています。ドキュメント事業は、従来、日本国内とアジアオセアニア地域を中心に販売・サポートをしてきました。2021年4月以降は、米国・欧州など全世界に販売を拡大します。情報セキュリティはグローバルでのガバナンスの強化が必要となっております。

情報セキュリティの推進体制

富士フイルムグループでは、富士フイルムホールディングスのESG推進部門の担当役員を全社情報セキュリティ統括責任者(CISO)として、その配下に全社情報セキュリティ統括組織を配置し、グループ全体の情報セキュリティガバナンスを実施しています。

全社情報セキュリティ統括組織には、情報セキュリティ安全確保支援士やCISSP (Certified Information Systems Security Professional) などの資格を保有する専門性の高いメンバーを配置し、サイバーセキュリティ等の外部の脅威、エラーや不正などの内部の脅威、そして、個人情報保護法対応などの情報セキュリティ法対応など様々なリスクを低減する取組みを実施しています。

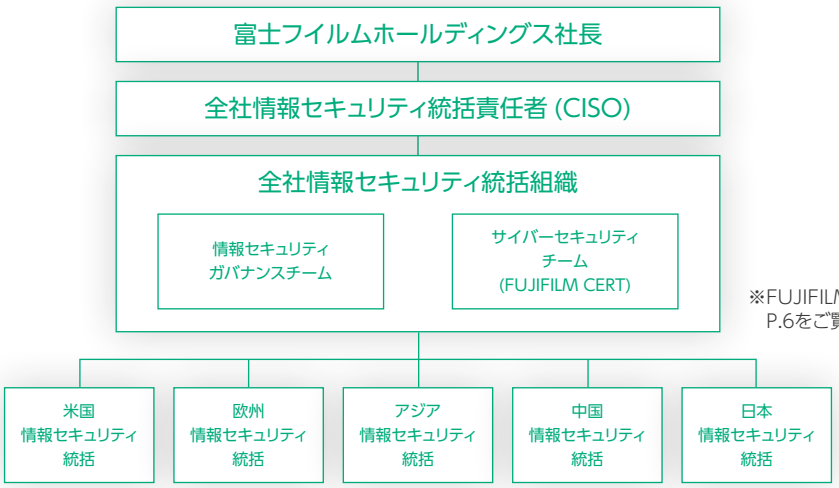
情報セキュリティガバナンスの実行にあたっては、ISO27001(ISMS)による情報セキュリティマネジメントに加え、サイバー攻撃の脅威への対応を高めるため、NISTサイバーセキュリティフレームワーク、NIST SP800-171等、グローバルスタンダードを盛り込むことで、防御・検知・対応・復旧の各フェーズの管理策対応力の強化に取り組んでおります。

またサイバーセキュリティ対応は攻撃に遭うことを前提に、サイバーセキュリティに対するインシデント対応組織(CSIRT)を設置し、「FUJIFULM CERT」の名称で活動しています。

FUJIFILM CERTは、社内ITインフラ、製品・サービス、工場の情報システムのリスクを対象に活動しています。

全社情報セキュリティ統括組織が事務局を務め、情報システム部門(情報システム子会社を含む)、品質保証部門、生産企画部門、事業部門から構成されるメンバーが役割分担をして、各領域のサイバーセキュリティリスクの低減をはかっています。

富士フイルムホールディングス情報セキュリティ体制図



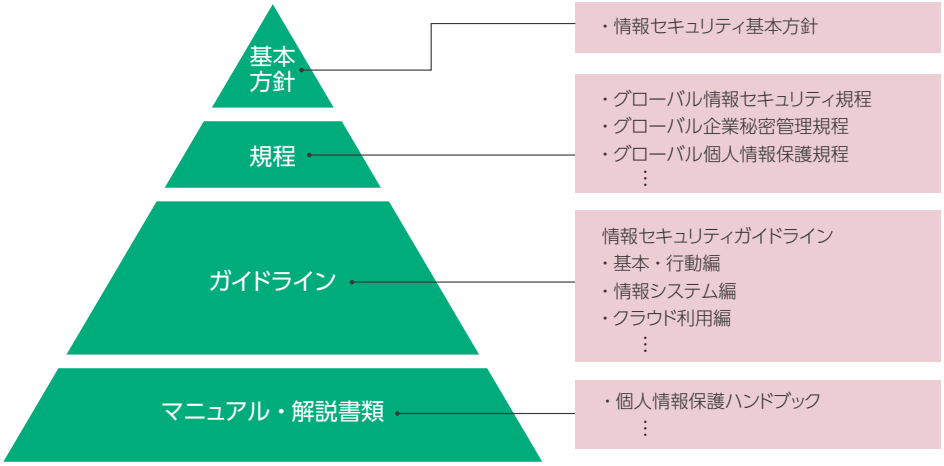
※FUJIFILM CERTの詳細は P.6をご覧ください。

情報セキュリティに関わるルール体系

富士フイルムは、情報の機密区分、コンプライアンス、情報倫理など、さまざまな観点から情報セキュリティに関わる全社共通ルールを制定しています。

具体的には、情報セキュリティに対する全社共通の考え方を示した「基本方針」、基本的なルールを定めた「規程」、具体的な管理策を定めた「ガイドライン」、および「マニュアル・解説書類」から構成されています。

いずれも、定期的に見直しを行い、最新の状況を取り入れ、更新しています。



情報セキュリティ事故が発生した際の対応

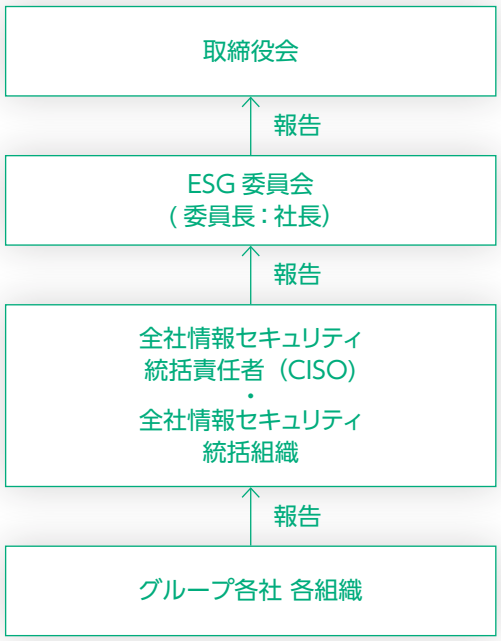
富士フイルムグループでは情報セキュリティルールの徹底をはじめとした様々な管理策によって、事故の未然防止に努めています。しかし最善の未然防止策を実施していても、情報セキュリティ事故の想定を怠り、事故が発生しない前提でいるわけにはいきません。

そのため情報セキュリティ事故または疑わしい事象を発見した際のエスカレーションプロセスを右図のように定め、適切な事故対応を行い、被害や損失を最小限に抑えるように努めています。

グループ内の各社、各組織で情報セキュリティ事故が発生した際は、直ちに部門の担当者が状況を把握し、全社情報セキュリティ統括部門に報告されることになっております。事故情報は、内容に応じて経営や関係組織と共有し、初動対応を実施し、影響を極小化と共に、再発防止策を講じております。

また事故情報は、ESG委員会、取締役会に報告しております。

なお、富士フイルムグループでは2019・2020年度ともに情報セキュリティに関連し、第三者もしくは規制当局から指摘され、社外に公開すべきと判断した深刻な事案はありませんでした。



※緊急かつ重要な案件は、直ちに社長/CISOに報告

サイバーセキュリティ

サイバー攻撃に対応するための富士フイルムグループの活動

富士フイルムグループは、日本および世界各国に商品・サービスを提供しており、サイバー攻撃への対応は、グローバルに取り組むべき重要な経営課題のひとつと捉えています。このため、商品・サービスを安全にお客様に提供し、安定した事業継続を図るためのサイバー攻撃の早期検知と、万が一サイバー攻撃を受けた場合の被害の最小化を担う、サイバーセキュリティ専門組織としてCSIRT(Computer Security Incident Response Team)を設置・運用しています。

FUJIFILM CERT – 従来のCSIRT機能の統合と強化

富士フイルムグループでは、これまで、現富士フイルムビジネスイノベーション株式会社のCSIRT 機能であるFuji Xerox CERT(2013年設立)、富士フイルム株式会社のCSIRT 機能であるFF-CSIRT(2016年設立)をそれぞれ、設置・運用してきました。

2021年4月からは、これら従来のCSIRT機能を、持株会社である富士フイルムホールディングス株式会社に集結し、富士フイルムグループ全体を網羅する、より強化されたFUJIFILM CERTとして活動を開始しています。

FUJIFILM CERTの体制

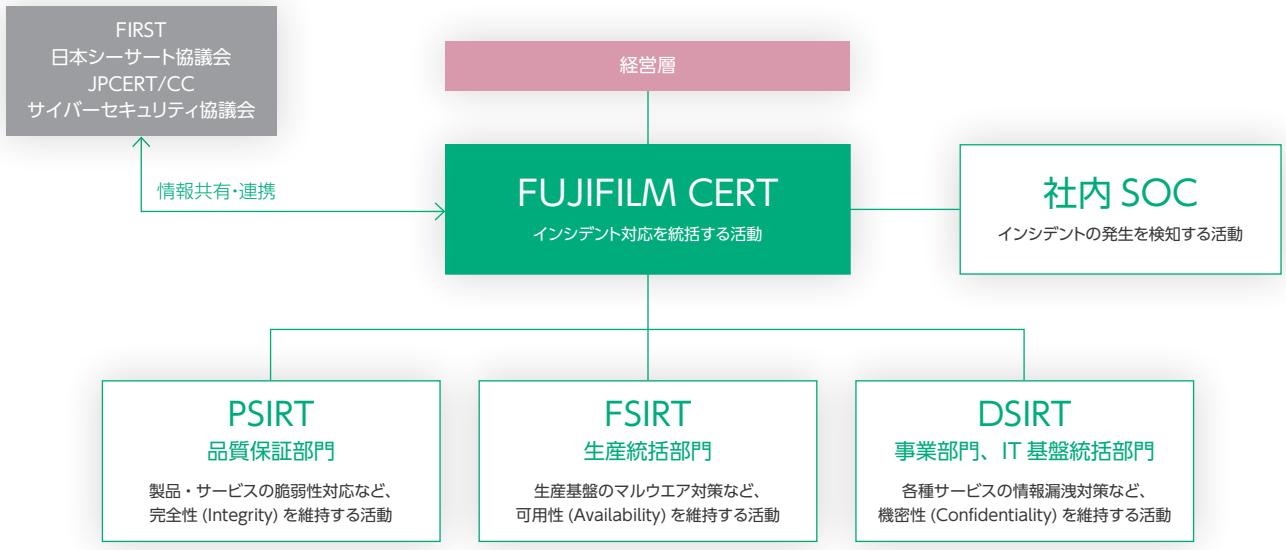
FUJIFILM CERTは、富士フイルムグループ傘下の関連会社/関連組織を横断するバーチャル・チームとして運営されています。FUJIFILM CERTの運営事務局は、富士フイルムホールディングス株式会社の情報セキュリティ統括部門に置かれ、富士フイルムグループ傘下の各企業(海外拠点を含む)の品質保証統括部門のPSIRT(Product SIRT)、生産統括部門のFSIRT(Factory SIRT)、お客様向けサービス提供部門やIT基盤統括部門のDSIRT(Digital service SIRT)が連携し、活動しています。

また、富士フイルムグループ全体のIT基盤に対するサイバー攻撃や内部不正を監視する社内SOC(Security Operation Center)と連携し、インシデントの発生を早期に察知し、迅速に対応できるようにしています。

さらに、FUJIFILM CERTは、社内のインシデント連絡窓口に加え、対外的な連絡窓口(下記)を設置し、外部のセキュリティ関連機関、CSIRT、善意の通報者から、脆弱性情報や脅威情報などを受け付けています。

連絡窓口: fujifilm-cert@fujifilm.com (FUJIFILM CERT)

FUJIFILM CERTの組織体制



FUJIFILM CERTにおける活動

FUJIFILM CERTのサービス対象は、富士フイルムグループ傘下のすべての関連会社であり、以下に示すような活動をしています。

また、FUJIFILM CERTでは、CSIRTの評価指標である成熟度モデルSIM3(Security Incident Management Maturity Model)を活用して活動内容を定期的にアセスメントし、継続的な改善をおこなっています。

FUJIFILM CERTの活動

種別	実施内容の概要
脅威インテリジェンス	● 富士フイルムグループ全体を対象にした、サイバーセキュリティアセスメント(自社のネットワーク構成、社外向けサイト、外部クラウド基盤の利用状況の調査に基づく脅威分析・リスク分析)の実施 ● 外部情報ソース(サイバーセキュリティ協議会、JPCERT/CC、FIRST等)や社内SOCからの脅威情報の収集と分析
インシデントハンドリング	● コンピュータセキュリティインシデントが発生した場合を想定したエスカレーション体制の整備と、インシデント発生時の対応支援 ● 社内SOCの監視活動と連携した、情報持ち出し等の内部不正に対する未然防止活動
脆弱性ハンドリング	● 富士フイルムグループが提供する商品・サービスに関する情報セキュリティ上の脆弱性への対応(JPCERT/CC製品開発者登録、PSIRTを中心とした情報セキュリティ早期警戒パートナーシップに基づく対応) ● 脅威情報や脆弱性情報に基づく業務ITインフラへの影響調査と対応
未然防止活動	● 生産拠点ネットワークのセキュリティ強化(FSIRT) ● 社外向けサイトに対する脆弱性検査の実施(PSIRT、CSIRT、DSIRT) ● セキュア設計開発プロセスの運用(PSIRT) ● クラウドサービス商品全般のセキュリティ対策(DSIRT)
啓蒙・教育・訓練	● FUJIFILM CERT活動報告書の発行(半期毎) ● 全社員を対象にした標的型メール攻撃対応訓練 ● CSIRTや社外向けWebサイト管理者を対象にしたサイバー演習

外部セキュリティ関連団体との連携

FUJIFILM CERTは、以下のような外部のセキュリティ関連団体のメンバーとして加盟して活動を進めています。

FIRST

FIRST(Forum of Incident Response and Security Teams)は、世界各国の企業や団体が加盟しているCSIRTの国際コミュニティです。FUJIFILM CERTは、グローバルな事業展開を推進する上で、CSIRT間での国際的な信頼関係を構築し、情報共有や相互協力を円滑に図れるようにするため、2015年にFIRSTに加盟しました(Fuji Xerox CERTとして加盟)。

日本シーサート協議会

一般社団法人 日本シーサート協議会(日本コンピュータセキュリティインシデント対応チーム協議会)は、400以上の国内企業や団体が加盟しているCSIRTコミュニティです。現在、FUJIFILM CERTは、同協議会の幹事会員として、同協議会における活動(サイバー演習に関するワーキンググループなど)を積極的に推進し、貢献しています。

サイバーセキュリティ協議会

サイバーセキュリティ協議会は、サイバーセキュリティ基本法を受けて設立された、NISC(内閣サイバーセキュリティセンター)とJPCERT/CC(JPCERTコーディネーションセンター)が運営するコミュニティです。FUJIFILM CERTは、同協議会の設立当初から加盟しています。

メディカル製品のセキュリティ

1. 医療システムのサイバーリスク

医療システムのサイバーリスクが注目されるようになったのは、2011年にインスリンポンプの脆弱性をついたハッキング実験にて、投与量の変更など患者の生死に関わる攻撃が可能なことが示されたことがきっかけと言われています。その後もインスリンポンプや心臓ペースメーカ、その他様々な医療機器の脆弱性が報告されています。

Windows等の汎用OS上で動作する医療システムの場合は、頻繁に公開されるセキュリティパッチに対し、製造販売業者での評価を終えないと適用ができないこともあり、適切なタイミングでパッチが適用されているとは言えないのが現状です。また、医療システムは長期に渡って使用されることが多く、OSのサポートが終了した後も継続して使用しているケースが少なくありません。近年、問題となっているランサムウェアなどによる被害は、こうした脆弱性対策が放置された汎用OSベースのシステムで多く見受けられます。

今後、ネットワークに接続される医療システムが増えていくのは明らかであり、サイバーセキュリティの強化がより重要になると考えられます。

医療システムの脆弱性やインシデントの一例

2013.6	脆弱性	ICS-CERT(The Industrial Control Systems Cyber Emergency Response Team)により、40ベンダ300種の医療機器でパスワードがハードコーディングされていることが報告された。
2017.5	インシデント	ランサムウェアWannaCryにより世界中の医療施設で約20万台のWindowsベースのコンピュータに影響を与えたと推定されている。英国の医療施設では手術のキャンセルや救急車の行先変更を余儀なくされる事態となった。
2017.8	脆弱性	アメリカ食品医薬品局(FDA)が米国で約46万5000人に埋め込まれている心臓ペースメーカについて、脆弱性をついたプログラム修正の可能性を指摘し、脆弱性によるものとしては初めてのリコールを発表した。
2017.10	インシデント	国内の公立病院にて電子カルテシステムがランサムウェアGandCrabに感染。バックアップが適切にとられていない運用上の問題が重なり、2日間電子カルテが使用できず、また、完全普及には数か月を要した。同病院の報告書によると感染経路は特定されていない。

2. 医療機器のサイバーセキュリティ規制動向

医療機器のサイバーセキュリティに関しては、アメリカ食品医薬品局(FDA)が積極的に取り組んでいます。製品寿命の長い医療機器の特徴を踏まえ、設計・開発フェーズにて必要なセキュリティ対策を組み込み、市販後も継続的に監視して必要な対応を求めるガイダンスを発行しています。

日本においても、厚生労働省が医療機器のサイバーセキュリティの確保を求める通知やその具体的なガイダンスを公開しています。この通知やガイダンスは、医療機器のサイバーリスクに対する適切なリスクマネジメントの実施や、市販後のサイバーリスクに基づく不具合等の情報について、GVP省令[1)]における安全性情報として取り扱うことなどを求めています。

2020年3月には、各国の医療機器規制の調和を目的に活動する国際医療機器規制当局フォーラム(International Medical Device Regulators Forum:IMDRF)が「医療機器サイバーセキュリティの原則及び実践」を公開しました。このガイダンスは、行政、医療機器製造販売業者、医療機関および医療従事者等のステークホルダー間における遅滞のない情報共有の重要性を言及しており、市販前と市販後のベストプラクティスとして考慮事項を記載しています。

市販前の考慮事項

セキュリティを考慮したアーキテクチャ設計、リスクマネジメント、セキュリティ試験、製品ライフサイクルを通したリスクマネジメント計画、ラベリングやユーザー向けセキュリティ文書、規制当局への申請書類

市販後の考慮事項

意図する使用環境における医療機器の運用、関係者間における情報共有、協調的な脆弱性の開示、脆弱性の対策、インシデントへの対応

このIMDRFのガイダンスの作成と並行し、各国の規制当局がガイダンスを発行しており、医療機器申請時の規制要件とする国も出てきています。日本においても、厚生労働省が今後3年程度を目処にこのガイダンスを導入すべく、検討を開始しています。

1) GVP省令(医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令):医薬品等の品質、有効性及び安全性に関する事項その他適正な使用のために必要な情報の収集、検討及びその結果に基づく必要な措置の方法を定めたもの

3. 富士フイルムの医療機器の製品セキュリティへの取り組み

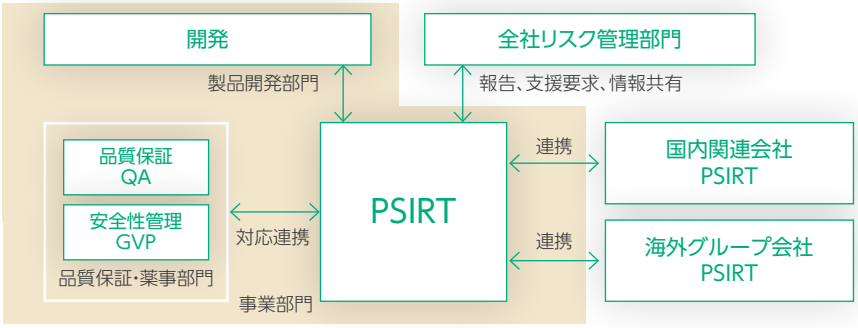
お客様に提供する医療システムについて、各国規制当局のセキュリティ規制強化の動きに適切に対応し、製品・サービスのセキュリティを確実にするために、2019年4月に、PSIRT(Product Security Incident Response Teams PSIRT)が発足しました。

PSIRTの主な役割としては、以下の4つがあります。

① 各国法規・規格対応の推進
② 製品脆弱性への対応推進
③ 製品情報セキュリティインシデントの対応推進
④ 対外的な情報開示

組織発足より1年半、PSIRTは製品脆弱性への対応、対外的な情報開示など段階的に運用を開始しつつ、規格や各国法規制要求に対応するための開発・管理プロセス(SOP)の整備に取り組んできました。必要なSOPの整備と教育を終え、現在、当社の医療機器の設計・開発、および、保守への導入を開始しています。

PSIRTを中心とした組織連携の概念図



PSIRTの主なタスクと当社医療機器のセキュリティリスクマネジメントプロセス

役割① 各国法規・規格対応の推進
製品情報セキュリティ対策技術や国内外の関連規格・法規動向の監視と企画・開発部門への情報展開
規格や法規制に対応するための開発・管理プロセス (SOP) の整備と教育
リスク評価手法の検討、脆弱性分析・セキュリティテストツール等の評価・選定、導入

セキュリティリスクマネジメントプロセス

1	2	3	4	5	6	7
トレーニング	要件	設計	実装	検証	リリース	対応
開発・管理プロセス (SOP) の作成と基本的教育	セキュリティ要件の作成 セキュリティとプライバシーのリスク評価	設計要件策定 脅威モデリングによる脆弱性分析と対応策の策定	静的解析ツールによる安全でない機能や構造の検出と削除	動的解析ツールによる攻撃への弱点検出と対応	脆弱性やインシデント発生時の対応計画策定 SBOM 登録	脆弱性やインシデント発生時の対応 脆弱性情報の自動抽出 製品情報セキュリティの情報開示

役割② 製品脆弱性への対応推進
脆弱性情報発信サイト JPCERT/CC 等より脆弱性情報を取得し、深刻度を考慮の上、
各製品の SBOM(ソフトウェア部品表) との突き合わせによる懸念ある製品・脆弱性の抽出、
製品開発部門による対策検討を指示

役割③ 製品情報セキュリティインシデントの対応推進
個人情報漏えいやその他情報セキュリティインシデント発生時に製品対応の実施
全社リスク管理部門や海外・国内のグループ会社・関連会社との連携・情報共有

役割④ 対外的な情報開示
製品情報セキュリティポリシー、製品に関連する脆弱性情報、脆弱性対応状況等の情報開示

製品セキュリティ情報については、公式サイトにて情報開示しています(2020年2月 運用開始)。
https://www.fujifilm.com/jp/ja/healthcare/security-information

複合機のセキュリティ

複合機はお客様の重要な情報資産であるデータを扱う情報機器であり、電子媒体と共に紙媒体に対してお客様のデータを保護することは重要課題です。さらに、サイバー攻撃が、日々、高度化かつ巧妙化している状況においては、お客様のデータや複合機への不正アクセスや侵入をいかに早く検知して、対応と復旧につなげるかがお客様の事業継続に重要だと考えます。

富士フイルムBIは、お客様のセキュリティ課題を解決するため、各種セキュリティ機能の提供、脆弱性評価や対応、そして、外部認証機関によるセキュリティ認証の取得など、セキュリティに重点をおき、商品開発に取組んでいます。

NIST SP800-171対応と準拠性の格付けAAAisの取得

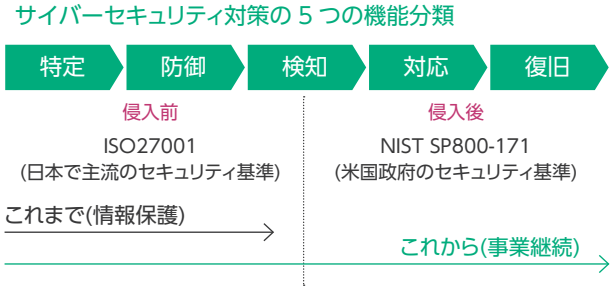
米国では、防衛調達や政府調達のセキュリティガイドラインとして、NIST(米国国立標準技術研究所)が定めているSP800-171が適用され、自動車などの産業にもその適用範囲が拡大しつつあります。また、日本においても、防衛調達を始めとして導入の検討が進んでいます。

これまでのセキュリティ対策基準は、ISO/IEC 27001が主流ですが、これは侵入されないための事前対応である「特定」と「防御」の観点からの対策基準です。

一方、NIST SP800-171では、「特定」「防御」の他に、サイバー攻撃により万一侵入されてしまった場合の事後対応である「検知」「対応」「復旧」を含むセキュリティ対策を求めています。

富士フイルムBIでは、複合機のNIST SP800-171対応を進め、その準拠性について、情報セキュリティ格付会社の評価で、2020年8月に販売開始したデジタルカラー複合機・プリンターの「ApeosPort」シリーズで最高ランクの AAAis を取得しています。

サイバーセキュリティ対策の 5 つの機能分類



複合機のウイルス対策

複合機に侵入したウイルスや脆弱性を利用した不正アクセスにより、複合機の正当なソフトウェアが改ざん・破損される脅威に対しては、以下の機能により複合機のソフトウェアを保護しています。

- 稼働時改ざん防止機能:複合機のソフトウェアへの不正アクセスや不審なアプリケーションの実行を、ホワイトリストに基づいて監視し、ソフトウェアの改ざんや不正な動作を防止します。
- 起動時改ざん検知機能:複合機が起動する時にソフトウェアが改ざんされていないかをチェックし、ソフトウェアが改ざんされていることを検知した場合は起動を停止します。

セキュリティ脅威の早期検知

複合機のセキュリティ設定、証明書の変更、ユーザーのログインやログアウト、ジョブ終了などの事象は複合機の監査ログとして、リアルタイムに外部のサーバーに転送されます。複合機をSIEM※製品と連携させることで、複合機の監査ログを一元管理・分析することが可能となり、以下のようなセキュリティ脅威の事象の早期検知・分析が可能となります。

- 内部不正:深夜や休日の大量のジョブ実行、禁止宛先への文書のFAX送信やメール送信による不正な情報持ち出し。
- 外部攻撃:複合機に対する不正なログインやセキュリティ設定の変更によるセキュリティ機能の停止など。

※:SIEM(=Security Information and Event Management)とは、機器やソフトウェアの動作状況の記録(ログ)を一元的に 蓄積・管理し、セキュリティ上の脅威となる事象をいち早く検知・分析するセキュリティーソフト/サービス。

複合機のセキュリティ認証

富士フイルムBI の複合機は、セキュリティ機能の適切性・確実性を保証すべく、デジタル複合機のセキュリティ要件である「ハードコピーデバイス プロテクションプロファイル v1.0」(HCD PP v1.0)に適合した国際セキュリティ標準ISO/IEC15408認証(Common Criteria認証)を取得しています。また、米国のKeypoint Intelligence社のBLI Security 認定テスト(デバイス侵入評価)に合格しています。

複合機内のデータ保護や設定・操作ミス抑制機能など詳しいセキュリティ機能についてさらに知りたい方は富士フイルムBI公式サイト内「デジタル複合機のセキュリティ白書」もぜひご覧ください。

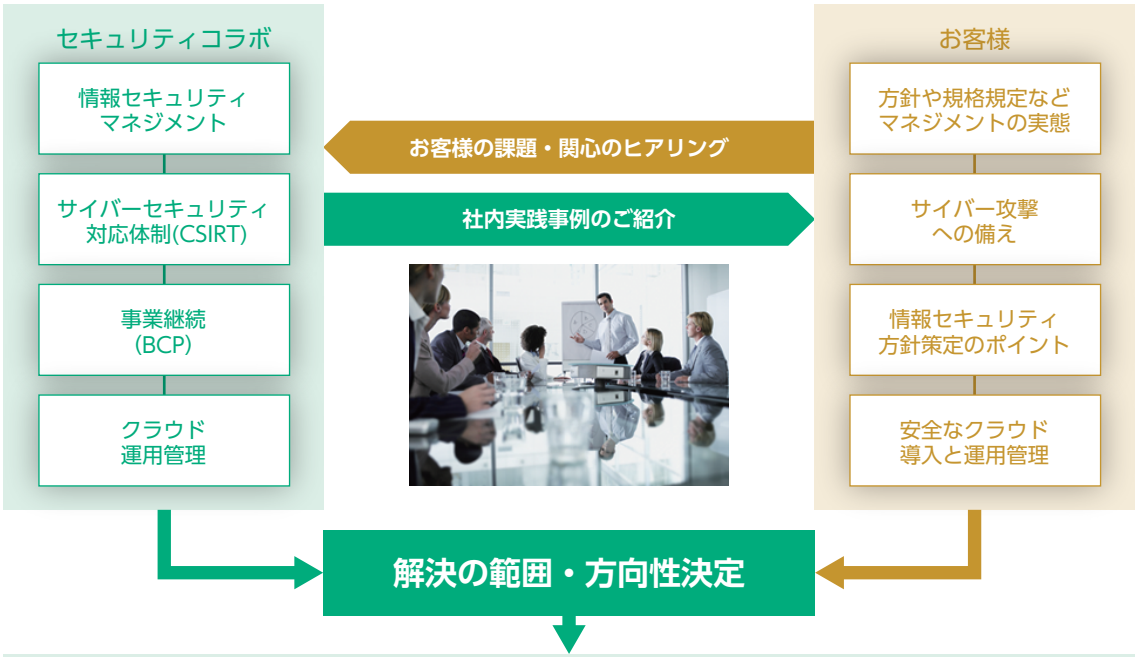
https://www.fujifilm.co.jp/fb/product/multifunction/promotion/security_measure

社内実践事例コラボによる情報セキュリティの課題解決

富士フイルムBIは、情報セキュリティマネジメントシステムの国際規格である(ISO27001)を取得し、NIST SP800-171を社内ルールなどの運用にいち早く取り入れ実践しています。実際の取組みで直面した課題や是正方法など多くのノウハウを蓄積しており、そのノウハウを社内にとどめるだけでなく、お客様の課題に応じた解決の方向性を具体的にご紹介する「社内実践事例コラボ」をご用意いたしました。企業が抱える主な情報セキュリティ対策上の課題をメニュー化し、範囲や深さが異なる課題に対し現状をお伺いしながら、ともに解決の方向性を探っていきます。特に情報セキュリティにおける責任者である経営者の皆様にご参加いただきたい内容となっています。

さらに豊洲ショウルームに情報セキュリティブースを常設しました。変化の激しい情報セキュリティの脅威に対し、最新ソリューションやマルウェア感染など、具体的な対策手法を体感いただき課題解決のイメージをお持ちいただけます。

社内実践事例コラボの概要



豊洲ショウルーム　体感

Bridge for Innovation

Live Security Tokyo
(新たな時代の情報セキュリティがここに)

主な特徴

・視覚的、体感的にセキュリティをご理解いただけます。
・お客様の課題に応じた、解決のヒントをご提示致します。
・豊洲から最新セキュリティに関する情報を発信致します。



・マルチポイントセキュリティソリューション
・ランサムウェア感染体感コーナー
・パスワードクラック体感コーナーなど

＊展示内容は都度変更となる場合がございます。

ファイルの安全・安心な送受信環境を提供するクラウドサービス「SECURE DELIVER」

テレワーク・在宅勤務の急速な普及に伴い、ファイルを送受信する機会が増加しております。そのような中で、デジタル改革担当相が中央省庁におけるパスワード付きZipファイルを廃止する方針を明らかにしたことや、セキュリティ強化を目的にパスワード付きZipを受信拒否する運用が広がっていることなどからファイル送受信に関するセキュリティ対策に関心が高まっております。

富士フイルムホールディングスでは、e-mailの添付ファイルからの情報漏えい対策として、グループ会社が提供しているクラウドサービス【SECURE DELIVER:セキュアデリバー】を使い、情報漏えいの防止に努めております。

富士フイルムイメージングシステムズが提供するクラウドサービス「SECURE DELIVER」とは

SECURE DELIVERは、インターネットを経由し企業間で安心・安全にファイルの送受信を行うことが出来るクラウドサービスです。送受信されるファイルはユーザーが意識することなく暗号化された状態でインターネットを通過するため、ユーザーは送信のたびにパスワード付きZipを作成する等の手間を省くことが出来ます。また、1回の送信あたり60GBまでのファイル容量送信に対応しているため、送信可能容量の制限により無料転送サービスを利用されてしまうことを防止できます。

SSO(シングルサインオン)によるログインアカウントの一元管理や上長承認機能(上長の確認/承認までファイル転送が保留される機能)などを利用することで、より強固に重要データの漏えい防止対策を行うことが出来ます。

SECURE DELIVER運用イメージ

お客様に安心して御利用いただくために

富士フイルムイメージングシステムズではお客様に安心してSECURE DELIVERのサービスをご利用いただくために、セキュリティへの配慮を重視しております。また、テロ等に伴う海外政府の介入によるサーバー停止を防止する為、お客様の重要な情報を保管するサーバーは日本国内の堅牢なデータセンター (Tier3レベル)に設置しております。また、クラウドサービスを比較・評価・検討いただく為の情報として、総務省が推進する「ASP・SaaS 安全・信頼性情報開示認定制度 」を取得し、安全・信頼性にかかる情報を適切に開示しております。

メールへのファイル添付が危険な理由

- メールの宛先を間違えると、情報がそのまま漏えいしてしまう
- メール経路上で添付ファイルが傍受・盗聴できるリスクがある
- ファイルがウイルス感染していると、送信先も感染してしまうリスクがある
- ファイルを取得後に総当たり攻撃によりパスワードが解析されてしまうリスクがある

SECURE DELIVERのセキュリティメリット

- 誤送信時にファイル取得が出来ないように、送信後のファイル削除ができる
- メールにファイルが添付されないので、メールが傍受されても搾取される危険がない
- 送信時にウイルスを自動検出し、ウイルスが検出された場合には送信を停止できる
- パスワードの試行回数制限があるため、総当たり攻撃によるパスワード解析が困難

社内の情報セキュリティ施策

富士フイルムグループは、情報セキュリティ基本方針の考え方に基づき、人的・組織的対策、物理的対策、技術的対策の観点で、さまざまな情報セキュリティ対策を行い、情報資産の適切な保護・管理に努めています。

情報セキュリティ対策の3つの側面

人的・組織的対策

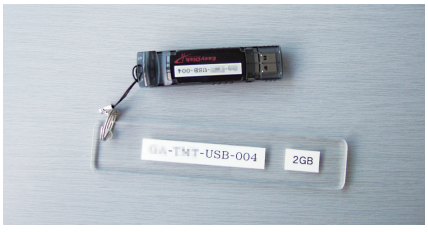
- 情報セキュリティに関する規程、ガイドラインの整備
- ルールを解説したハンドブック、事故事例教材の展開
- 各社、各部門から選出された情報セキュリティの管理者による情報セキュリティガバナンス
- 情報セキュリティ、個人情報保護に関する教育の定期的な実施
- 新入社員教育、管理職教育などの階層別情報セキュリティ教育の実施
- 情報セキュリティ事故発見から即日、速やかな報告(第一報)の徹底
- サイバーセキュリティ訓練の実施
- 不審メール訓練の実施

物理的対策

- 主要拠点での従業員証(ICカード)による入退室管理
- ワイヤーロックによるPCの固定
- 携帯電話やUSBメモリーへのストラップの取り付け
- 高セキュリティエリアへの対策(ゾーニングの設定/カメラによる監視/私物機器持ち込みの禁止および抜き打ち点検)
- 機密文書のキャビネットにおける施錠管理および鍵管理

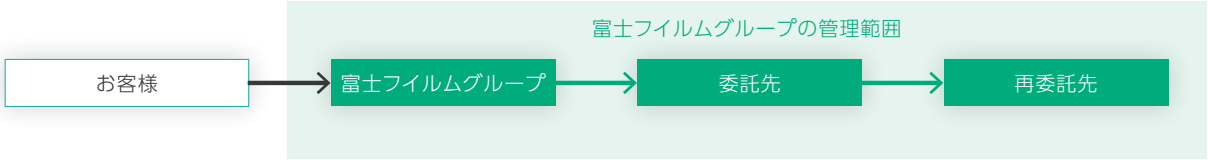
技術的対策

- サーバー、システムへのユーザー単位でのアクセス制御
- 従業員のPC操作ログの取得・管理
- 私物などの未登録デバイスへの書き出し制御、ログ管理
- 不正持ち出し対策(フリーアドレスへの送信監視、複合機の利用状況監視、クラウドストレージの利用監視)
- PC持ち出し前のデータ削除ツール(富士フイルムBI)
- スマートフォン利用管理
- インターネット通信(Webアクセス、メール送受信)の監視
- 社外持出しPCのディスク全体暗号化
- PC管理ツールによる使用ソフトの適正利用監視
- アクセス禁止カテゴリーや悪性サイトに対するWebアクセスのフィルタリング
- 文書(紙)出力時のICカード認証
- 機密文書(紙)への複製禁止コードの埋め込み
- 不正通信のモニタリング、遮断



パートナー企業と連携した情報セキュリティ

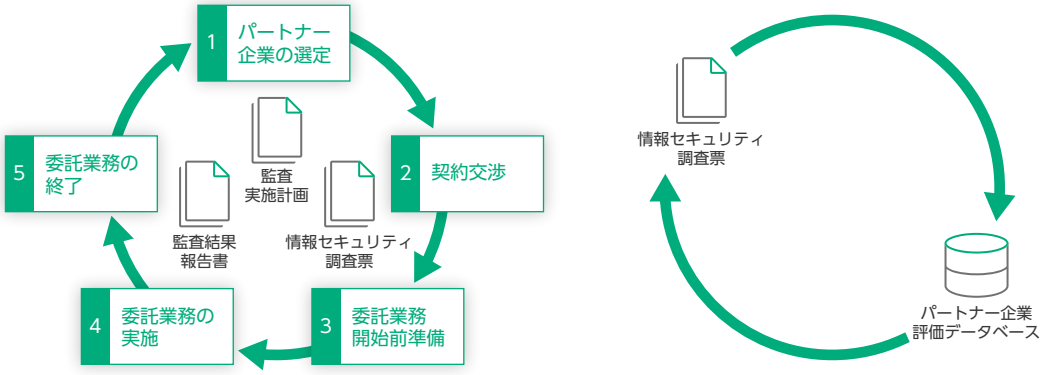
富士フイルムグループでは、商品開発や社内の基幹業務など、さまざまなパートナー企業(業務の委託先)に支えられて事業活動を行っています。業務内容によっては、お客様からお預かりする大切な情報をパートナー企業が扱うことがありますので、パートナー企業と緊密に連携して情報セキュリティを確保することにより、品質の一部として、お客様に安全・安心をお届けできるよう努めています。また、パートナー企業よりさらに業務の委託を行う場合には、再委託先まで富士フイルムグループ各社の管理範囲とみなし、活動をおこなっています。



パートナー企業監査強化の取り組み (富士フイルムBI)

他社での大規模な個人情報漏えい事故をきっかけに、重要な情報をグループ外に委託している業務に関する調査を行いました。以前よりパートナー企業にお客様や自社の重要な情報を預けるガイドラインを整備し運用していましたが、セキュリティを担当する総務・品質保証部門だけでなく、購買部門も加わったタスクにて案件に応じた適切なパートナー企業選定プロセスの効率化とガバナンスを強化、調査と改善依頼のプロセスが正しく行われるようガイドを修正しました。

パートナー企業の管理監督強化プロセス



業務を委託する際には、業務委託の内容に応じた3種類の調査票への回答をお願いしています。それぞれ「組織的安全措置」「人的安全措置」「物理的安全管理措置」「技術的安全措置」の観点からセキュリティ状況についての設問を構成しており、その結果を購買部門に集約して情報を一元管理しております。

また、個人情報が含まれる場合には、管理策等の取扱いに関する覚書を取り交わして、法令を遵守し富士フイルムグループの個人情報方針を満たした適切な扱いを求めています。

取組事例

パートナー企業の委託業務従事者からの誓約書取得

富士フイルムBIでは、社員外従業員、派遣社員、およびパートナー企業の社員(委託業務従事者)から、「情報資産、設備等の適正利用についての誓約書」を取得しています。この誓約書は全社におけるセキュリティの維持徹底を狙いとしており、具体的には右の内容を目的としています。

1. 秘密保持契約としての位置づけによる情報漏えいの防止
2. 当社グループの施設、設備等の適正利用
3. 情報資産を含む当社資産の保全
4. 当社グループ事業所における入退管理ルールの徹底
5. 社内ネットワークおよび社内情報システムの適正利用
6. 入退館カードの貸与

海外グループ会社における情報セキュリティ

富士フイルムグループでは、地域ごとや機能組織ごとに海外ガバナンスを展開しています。現在は富士フイルム・富士フイルムBIそれぞれで行っていたルール・手順などの共通化を順次進めております。

海外の情報セキュリティ情報の共有とガバナンス体制

富士フイルムグループでは、欧州・米国・中国・アジアパシフィック等地域ごとにそれぞれの状況にあわせた海外ガバナンスを展開しており、日本で作成したルールをもとに一部地域にあわせてカスタマイズした運用を行っております。

情報セキュリティもグローバル共通で遵守すべき基本事項を展開し、各地域の法令などに合わせた対応を行っています。また情報セキュリティ事故が発生した際はそれぞれの地域で初動対応を行い、リスクレベルや影響が大きな案件については日本への報告を行ったうえで経営への情報共有と再発防止策の徹底を行っています。

各地域の情報セキュリティ担当者とは定期的な情報交換会を開催し、各地域で共通する課題や本社で集約すべき施策の情報交換、そしてグローバルに展開する必要のある情報について確認を行っています。

グローバルで共通した施策の推進

富士フイルムグループでは『グローバル共通ルール』をつくり、グローバルで導入するウイルス対策ソフトを始めとしたセキュリティ製品の共通化を進めています。セキュリティ製品を共通化することで、管理コンソールを通じて世界各国での使用状況を把握、またポリシーも統一化することができています。これまで現地法人ごとにレベルが異なっていた部分も多かったセキュリティ対策を均一にすることにより、セキュリティ事故の未然防止に役立っています。

2021年度には、グローバルのネットワークやデバイスを24時間365日体制で監視するグローバルSOC(Security Operation Center/p.6をご覧ください)の構築を行い、サイバー攻撃の検知・対応能力を格段に強化します。

生産拠点における事故情報の共有と再発防止策

生産系の国内関連会社や生産拠点では、リスク情報の共有のために定期的に生産拠点リスクマネジメント会議を実施しており、労務管理上の安全衛生や環境リスクなどと同様に情報セキュリティもリスクマネジメント会議内で事故の概要報告と再発防止策の共有を行っています。

当会議において、各拠点の推進者のコミュニケーションを促進することで、リスク対策施策やリスクマネジメント活動運営施策のベストプラクティスを水平展開し、富士フイルムグループ生産全体のリスクマネジメントレベルの向上も行っています。

アジアパシフィックの情報セキュリティ（富士フイルムBI）

情報セキュリティマネジメントシステム（ISMS）とその継続的改善

現在、情報は個人、組織にとって、またビジネスを行う上で必要となる最も重要な資産だと考えることができ、自組織内だけではなく、お客様や業務に関わる方々の情報を確実に保護することが非常に重要です。富士フイルムBI アジアパシフィックのトップマネジメントは、お客様や自社の情報を保護するために地域全体で情報セキュリティマネジメントシステム（ISMS）プログラムを導入するという大きな決断を下し、毎年変化するリスクに効果的に対応することをコミットしました。

組織全体のガバナンスとコンプライアンスを強化するために、日本本社の協力を得ながら、地域全体で情報セキュリティのルールが統一され順守されています。今日、サイバー攻撃や情報セキュリティインシデントは世界的に日々増加しています。セキュリティガバナンスを強化するために、私たち富士フイルムBIは継続的に監査等の点検評価を行い、その他のベストプラクティスを参考にしながら全体の設計と計画、そして確実な実施を通して情報セキュリティレベルの向上に努めています。

またISMSの取り組みに加えて、個人情報保護の法令要件は国ごとに頻繁に変更されています。富士フイルムBIは従業員、お客様、ビジネスパートナー、そして事業を通じて取り扱うすべての個人データの保護に努めています。

サイバーセキュリティ、クラウドサービスおよび業務委託における安全性について

富士フイルムBIは、クラウドサービスプロバイダーやサプライヤーとの最新技術を駆使して、お客様にサービスを提供しています。お客様の情報を始めとして、今やほとんどの情報が外部のクラウドシステムを活用して業務上の様々な処理や保存が行われる可能性があるため、富士フイルムBIはクラウドシステムや業務委託先に対するセキュリティ基準や期待値を設定し、リスクを最小限に抑えるよう努めています。弊社の求める基準に達しない場合は是正いただくよう求め、それが難しい場合にはトップマネジメントの承認を必要とするルールとしています。

個人情報保護への取組み

1. 基本方針

富士フイルムグループでは、国内外の全従業員がいかに行動するかを定めた行動規範の中で、人権尊重の一項目として個人情報保護について定めています。また、富士フイルムグループで共通の内容を含む個人情報保護方針またはプライバシーポリシーを各グループ会社で定めており、グループ共通の考え方で個人情報を取り扱っています。

これらの方針は、富士フイルムグループの調達先・業務委託先にも展開されており、サプライチェーン全体に適用されています。(調達先・業務委託先との連携についての詳細は、P.15「パートナー企業と連携した情報セキュリティ」をご参照ください。)

2. 推進体制

富士フイルムグループでは、富士フイルムホールディングスのESG推進部門(以下、単にESG推進部門といいます)担当役員を管理統括者として個人情報保護体制の構築・維持にあたっています。

グループ全体における個人情報に関する方針や目標は、富士フイルムホールディングスの社長を委員長とするESG委員会で意思決定されるとともに、ESG委員会から取締役会にも定期的に報告されています。取締役会はグループ全体のコンプライアンスとリスクマネジメントを監督する責任を持っており、個人情報保護もその中の重要項目として、そのプロセスの有効性は担保されています。個人情報保護に関する取り組みはESG委員会で方針の決定がなされた後、個人情報保護の統括部門である富士フイルムホールディングスのESG推進部門から、方針・目標を展開するとともに、その遂行や管理状況の調査・把握、規程内容の従業員への周知徹底、個人情報を取り扱う各組織長に対する指導・助言等を行っています。

特に、社会での個人情報保護に関する意識向上に伴い、リスク管理の視点から個人情報保護については、毎年グループ全体で実施しているリスク抽出とアクションプラン策定の中で確認しており、グループ全体としてリスクマネジメントの体制を構築しています。

なお、ISMSを取得している会社では、ISMSの推進活動と一体化して個人情報保護に取り組んでいます。また、機微な個人情報を取扱っている会社ではプライバシーマークを取得しており、どちらも定期的な外部審査の受審とその審査結果をもとにした改善活動を行っています。

3. 従業員教育

富士フイルムグループでは、個人情報の取り扱いに関する事故・違反の発生防止には、日々の情報を扱う際に、従業員一人ひとりが必要とされる知識を身につけ、高い意識をもつことが重要だと考えています。そのため、すべての従業員を対象に、個人情報保護について、eラーニングによる教育を毎年実施しています。

また、就業規則において、許可を得ない情報の持ち出しに違反した従業員には懲戒処分を科すことを定めるとともに、他社事例を含めたヒヤリハット事例の共有を通じた注意喚起や不正な情報持出しの検知活動などを実施しており、個人情報の保護に万全を期しています。

BtoBビジネスにおいて大量の個人情報の取扱いを受託する機会が多いグループ会社には、「個人情報保護ハンドブック」を作成・配布し従業員の啓発に役立てています。

4. 個人情報の適切な取り扱い

富士フイルムグループでは、個人情報保護方針／プライバシーポリシーに基づき個人情報の取扱いに関する内部規則(個人情報管理規程、各種ガイドライン等)を定め、適切な安全管理策を施し、保有する個人情報の保護に努めています。個人情報保護方針／プライバシーポリシーの変更の際はウェブサイト上で公表し、法令上本人の同意が必要な場合には適切に取得します。

また年に一度は、部門ごとに保有している個人情報の棚卸しを専用システムで行い取扱い状況を一覧できるようにするとともに、安全管理措置の確認・是正や保有の必要がない個人情報の削除対応等を行っています。棚卸の実施状況については、ESG推進部門が各組織の監査を実施しています。

また、政府機関から情報の開示を求められた場合は、要求内容と適用される法律を確認の上、適切に判断を行います。

5. グローバルコンプライアンスへの対応

昨今、EUのGDPR(General Data Protection Regulation:一般データ保護規則)をはじめとして、世界各国で個人情報保護法令の整備・見直しが急速に進んでいるため、それらをキャッチアップし確実に遵守していく必要があります。

そのための主要な実務対応は各地域統括会社および各国現地法人が行っていますが、ESG推進部門においても世界各国の個人情報保護法令の整備・見直し状況を把握し、各地域統括会社および各国現地法人の対応状況を確認しています。

6. 個人情報の取り扱いに関する事故・違反

2020年度は顧客・取引先の個人情報に関連し、外部への漏えいや目的外利用などの不適切な取り扱いを第三者もしくは規制当局から指摘され、社外に公開すべきと判断した深刻な事案はありませんでした。

なお、軽微な事案についてもすべて情報セキュリティ事故として取り扱い、事故の内容に応じてご本人などへ情報を開示し、詳細な要因分析と再発防止策の策定・展開を行っています。

トピックス

コロナ禍での働き方の変化と情報セキュリティ

2020年初頭から始まった新型コロナウイルスの感染拡大に伴い、富士フイルムグループでは国内外で様々なコロナ対応を行ってきました。

在宅勤務・リモートワーク拡大に伴うセキュリティ施策

富士フイルムグループでは以前より営業担当の従業員を中心に、会社のオフィス以外での勤務を認めるリモートワークを行っていました。緊急事態宣言が発令された2020年3月より、通常では社外への持ち出しを認めていない組織もある、ラップトップPC・デスクトップPCも特別にグループ全体で在宅勤務の使用に認め、グループ内の多くの従業員が在宅勤務を行いました。解除後も妊娠中や基礎疾患のある従業員は在宅勤務を継続し、政府の要請などコロナウイルスの感染状況に応じ、リモートワークや在宅勤務などの柔軟な働き方を、セキュリティに配慮したルールのもとで実施しています。

- 社内イントラ情報として「新型コロナ対応」ページを新設し、ITの利用ルール、その他一般的な情報セキュリティルールとマナーを周知徹底した。
- 在宅勤務者が増加しネットワーク環境が不安定になったため、快適で安全な在宅勤務環境を提供するためにネットワークの増強を行った。
- 従業員が安全にweb会議を実施できるように、会社契約のweb会議ツールを展開し、web会議実施時の注意事項(データやり取りに関する注意や録音の禁止など)の周知を行った。
- VPNの脆弱性指摘に対する安全確認を行った。

情報機器廃棄時の情報漏えい未然防止策強化

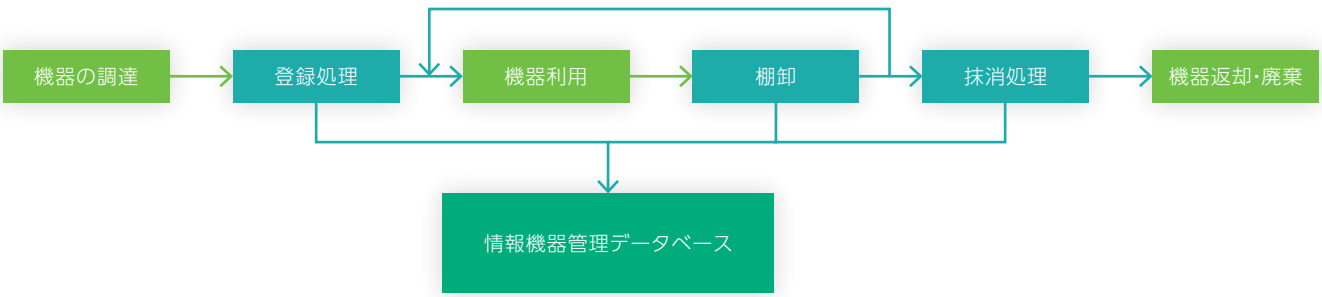
2019年、ハードディスクのデータ消去作業を請け負った企業の従業員が、作業前の複数のハードディスクを盗み出し、ネットオークションで転売した結果、ハードディスクに保存されていた自治体の内部情報が流出する事件がありました。この事件をきっかけに、富士フイルムグループ全体でPCなどの情報機器の管理を見直し、下記のような管理策を導入し進めております。

PC廃棄時の情報漏えい防止の仕組みを含め、グループで保有するPC、USBメモリなど、情報を記録するための情報機器を対象に、一括して管理する仕組みを導入しました。具体的には、情報機器の利用開始と同時に、その機器情報をデータベースに登録し、最後に適切に廃棄されるまでのライフサイクルを管理するものです。

この仕組みにより、情報機器の使用期間中の管理状況を確認し、情報機器の紛失・盗難を早期に発見することができます。

また、情報機器の廃棄時の情報漏えい対策として、国際的な基準であるNIST-SP800を参考にして、廃棄前に何を実施すれば、安全に廃棄可能かの対策基準(サニタイズ基準)を定め、この基準に沿った手順を実施する運用を決定しました。そして、廃棄の際には実施記録を残すことで、後に機器の紛失・盗難が発覚した場合でも、該当する情報機器から情報漏えいすることはないことを確認できます。

このように、情報機器の使用開始から、使用中の管理、廃棄までのライフサイクル全般を通した管理を実現しています。



第三者評価・認証

富士フイルムグループでは、情報セキュリティに関する第三者評価・認証の取得に積極的に取り組んでいます。

富士フイルムグループにおけるプライバシーマークとISMSの取得状況

2021年2月[1)]

種類	取得済みの関係会社	
Pマーク[2)]	富士フイルムメディカル 富士フイルムイメージングシステムズ 富士フイルムメディアクレスト	富士フイルムテクノサービス 富士フイルムイメージングプロテック 富士フイルムシステムサービス
ISMS[3)]	富士フイルムイメージングシステムズ 富士フイルムイメージングプロテック 富士フイルムメディカル	富士フイルムソフトウエア 富士フイルム記録メディア事業部 富士フイルム和光純薬
	富士フイルムビジネスイノベーション 富士フイルムビジネスイノベーションジャパン 富士フイルムマニュファクチュアリング 富士フイルムプリンティングシステムズ	富士フイルムシステムサービス 富士フイルムサービスリンク 富士フイルムサービスクリエイティブ
	FUJIFILM Business Equipment Shanghai FUJIFILM Manufacturing Shenzhen	FUJIFILM Eco-Manufacturing (Suzhou) FUJIFILM Manufacturing Hai Phong
	FUJIFILM Business Innovation Australia FUJIFILM Business Innovation Asia Pacific FUJIFILM Business Innovation New Zealand FUJIFILM Business Innovation Malaysia Sdn Bnd FUJIFILM Business Innovation Philippines FUJIFILM Business Innovation Singapore FUJIFILM Business Innovation China FUJIFILM Data Management Solutions	FUJIFILM Business Innovation Korea FUJIFILM Business Innovation Malaysia FUJIFILM Business Innovation Thailand FUJIFILM Business Innovation Taiwan FUJIFILM Business Innovation Vietnam FUJIFILM Business Innovation Hong Kong

1) 2021年2月時点の取得企業ですが、社名については2021年4月時点のものを掲載しております。
2) プライバシーマーク:(一財)日本情報経済社会推進協会(JIPDEC)より、個人情報について適切な取り扱いが行われている企業に与えられるマーク
3) ISMS:情報セキュリティマネジメントシステム国際規格(ISO/IEC27001)。個人情報をはじめとする情報全般の管理体制に関する認証

ISO/IEC15408[4)]認証の取得状況

富士フイルムBIおよび関連会社は、2007年より、複合機、プリンターなどの製品において、ISO/IEC 15408の認証を取得しています。2018年12月から2020年12月までの認証取得した当社製品は、以下のとおりです。

製品名	認証年月日
Fuji Xerox ApeosPort-VII C7773/C6673/C5573/C4473/C3373/C2273 DocuCentre-VII C7773/C6673/C5573/C4473/C3373/C2273 スキャナー、ファクス機能標準搭載モデル +データ上書き消去機能 ApeosPort-VII C7773/C6673/C5573/C4473/C3373/C3372/C2273 DocuCentre-VII C7773/C6673/C5573/C4473 スキャナー、データ上書き消去機能標準搭載モデル +ファクス機能 DocuCentre-VII C3373/C2273 スキャナー、ファクス機能標準未搭載モデル+データ上書き消去、スキャナー、ファクス機能 DocuCentre-VII C3373/C3372/C2273 データ上書き消去機能標準搭載モデル+スキャナー、ファクス機能	2019/12/27
Fuji Xerox ApeosPort-VII C7788/C6688/C5588 DocuCentre-VII C7788/C6688/C5588 データ上書き消去機能、ファクス機能付きモデル	2020/2/20
Fuji Xerox ApeosPort-VII　C7773/C6673/C5573/C4473/C3373/C3372/C2273 DocuCentre-VII　C7773/C6673/C5573/C4473/C3373/C3372/C2273 ハードディスクの上書き消去、コピー、プリント、ファクス、スキャン機能付きモデル	2020/9/15
Fuji Xerox ApeosPort 5570/4570/3570/5570 G/4570 G コピー、プリント、ファクス、スキャン機能搭載、ストレージの上書き消去機能非搭載モデル	2020/11/2

4)ISO/IEC15408:情報セキュリティの観点から、情報技術に関連した商品およびシステムが適切に設計され、かつその設計が正しく実装されているかどうかを評価するための国際的なセキュリティ基準。

情報セキュリティの今後の計画

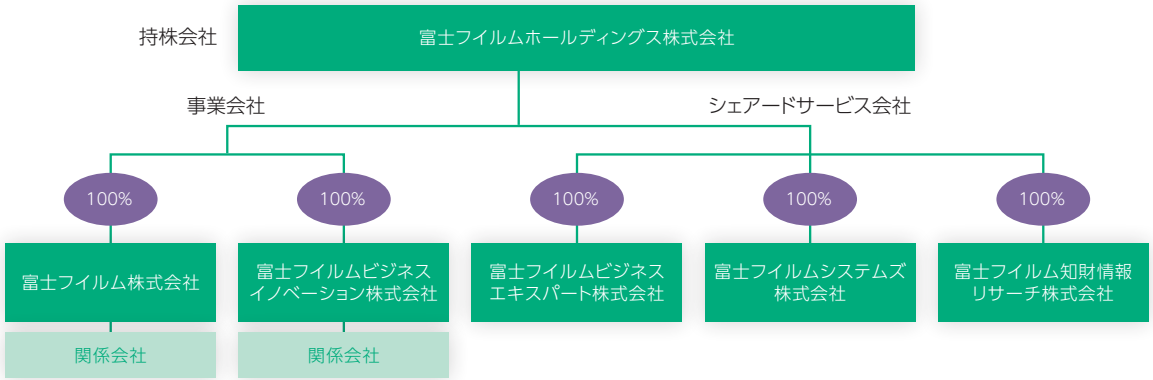
今後も富士フイルムグループでは情報セキュリティの継続的な強化に取り組み、主に次の活動を実施する予定です。

- 巧妙化するサイバー攻撃などの脅威に対応するため、防御中心の対策に加え、侵入を前提にした対策をグローバルで導入します。
- 製品や生産拠点の情報セキュリティに対し、各事業部中心の対応から本社主導によるグループ全体での施策導入をすすめ、ガバナンスを強化します。
- 個人情報を適切に管理し、各国の法令や規則を遵守するために、規程やガイドライン等のルールを再整備します。
- 内部不正、ヒューマンエラーなどによる従業員や業務委託先からの情報流出を防ぐための対策を一層強化します。
- 情報セキュリティに関する全社対象の教育・訓練を継続実施するとともに、専門性の高い人材を育成し、組織全体での情報セキュリティ強化を図ります。

富士フイルムグループの概要

会社名　：富士フイルムホールディングス株式会社
本社　：東京都港区赤坂9丁目7番3号(東京ミッドタウン)
設立　：1934年1月20日

富士フイルムグループの組織構造



事業領域

イメージングソリューション	ヘルスケア&マテリアルズソリューション	ドキュメントソリューション
「撮影」から「出力」に至る、写真に関わる製品・サービスを提供	重点事業分野である「ヘルスケア」「高機能材料」をはじめ、BtoB中心に多彩な事業を展開	オフィス向けに複合機やサービスなど、ドキュメントに関わる事業を展開

■ 本報告書についてのお問い合わせ先

富士フイルム ホールディングス株式会社

ESG推進部
〒107-0052　東京都港区赤坂9丁目7番3号（東京ミッドタウン）
TEL: 03-6271-2069