

FUJIFILM Holdings Corporation  
情報セキュリティ報告書



トップメッセージ .....	3	お客様への安全のご提案 .....	11
情報セキュリティ体制 .....	4	社内の情報セキュリティ .....	12
製品・サービスの情報セキュリティ .....	8	第三者評価・認証／富士フィルムグループの概要 ..	18

## グループパーパス

企業理念：富士フィルムグループの社会における存在意義

地球上の笑顔の回数を増やしていく。

わたしたちは、多様な「人・知恵・技術」の融合と独創的な発想のもと、  
様々なステークホルダーと共にイノベーションを生み出し、世界をひとつずつ変えていきます。

## DXビジョン

富士フィルムグループは、AI・IoTを活用した企業変革を目的として積極的にDXの実現に取り組んできました。2021年にはDXのさらなる推進により、これまで以上に優れた製品・サービスを提供し、社会課題の解決に向けた挑戦を続けることをコミットするべく、「DXビジョン」を策定しました。

富士フィルムグループの「DXビジョン」

わたしたちは、デジタルを活用することで、一人一人が飛躍的に生産性を高め、そこから生み出される優れた製品・サービスを通じて、イノベティブなお客さま体験の創出と社会課題の解決に貢献し続けます。

## 情報セキュリティ基本方針

わたしたち富士フィルムグループは、「オープン、フェア、クリア」の精神で、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、お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・お取引先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、お客様やお取引先様等との契約を遵守します。

## 社会課題解決への挑戦を支える基盤として、 情報セキュリティ強化に取り組む

富士フィルムグループは、2024年1月20日に創業90周年を迎え、グループパーパス「地球上の笑顔の回数を増やしていく。」を新たに制定しました。当社が持つ多様な「人・知恵・技術」を生かしてイノベーションを生み出し、社会課題の解決に貢献することで、より多くの「笑顔」を創り出せる会社を目指していきます。

また当社は2021年に「DXビジョン」を策定・公開し、DXのさらなる推進により、これまで以上に優れた製品・サービスを提供し、社会課題の解決に向けた挑戦を続けることをコミットしています。しかしながら、近年、世の中の地政学的緊張の高まり、社会・産業のデジタル変革などのさまざまな背景により、サイバー攻撃による情報漏えいなどのリスクが増しており、情報セキュリティの重要性がますます高まっています。DX推進には、富士フィルムグループ全体での強固な情報セキュリティが必要不可欠となっています。

そのため当社では情報セキュリティを企業価値に直結する極めて重要な経営課題と位置付け、取締役会や、ESG委員会（“ESG=環境、社会、ガバナンス”活動を審議する社内の重要会議）での審議を重ねています。その上で、情報セキュリティガバナンスのさらなる強化、お客さまに安心・安全をお届けするための製品・サービスの開発など、グループ全体で情報セキュリティ対策に力を注いでいます。

例えば情報セキュリティ対策の一つであるサイバー攻撃対策として、攻撃の予兆を早期に検知するFUJIFILM SOC (Security Operation Center) や、インシデントが発生した場合の影響・被害を最小限にとどめる対応体制であるFUJIFILM CERT (FUJIFILM Cybersecurity Emergency Response/Readiness Team) をグローバルで強化しています。さらに、日々、高度化・巧妙化するサイバー攻撃に対する継続的な強化策として、セキュリティソリューションの活用、従業員教育や訓練を行っています。また、ヒューマンエラー、内部不正、情報セキュリティの各種法規制への対応など、総合的なセキュリティ強化を図っています。加えて、富士フィルムグループのみならず、パートナー企業と連携して、サプライチェーン全体のセキュリティ対策も行っています。このような取り組みが評価され、当社は2023年12月に「Cyber Index Awards 2023」大賞<sup>\*</sup>を受賞しました。

富士フィルムグループは、今後も社会課題の解決に向けた挑戦を続けていきます。本報告書では、この挑戦を支える基盤である情報セキュリティの取り組みを紹介しています。本報告書が少しでも皆さまのご参考になれば幸いです。



富士フィルムホールディングス  
代表取締役社長・CEO

後藤 禎一

<sup>\*</sup>詳細はP. 19「Topics」をご覧ください。

# 1

## 情報セキュリティ体制

### 情報セキュリティガバナンス

富士フィルムグループは持株会社である「富士フィ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ィルム株式会社および富士フィルムビジネスイノベーション株式会社ならびに関係会社などで構成されています（詳細はP.19「富士フィルムグループの概要」をご覧ください）。

富士フィルムグループでは、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り組みを行っています。本章では、富士フィ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。

#### 富士フィルムグループにおける情報セキュリティの考え方

富士フィルムグループはESG（環境、社会、ガバナンス）を重要な経営課題として位置づけ、その中の重要な活動として情報セキュリティ強化の取り組みを行っています。

富士フィルムグループは、創業以来、時代の変化や社会のニーズに合致したイノベーションを創出し、事業ポートフォリオを変革させてきました。これらの変革によって、当社の技術情報のみならず、メディカルシステムやバイオ医薬品の生産受託などのヘルスケア領域、ITを活用したソリューション・サービスに軸足を置いたビジネスイノベーション領域などお客様の重要な情報をお預かりする機会が増え、情報セキュリティの重要性がますます高まっています。

また各事業でグローバル化を進め、全世界での販売が拡大しているため、グローバルでの情報セキュリティガバナンス強化が必

要となっています。

#### 情報セキュリティの推進体制

富士フィ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ガバナンス責任者、富士フィルムホールディングスのICT推進部門の担当役員を全社ICTセキュリティ責任者とし、配下に全社情報セキュリティガバナンス統括組織、全社ICTセキュリティ統括組織を配置しています。全社情報セキュリティを統括する組織には、情報処理安全確保支援士などの資格を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などの外部の脅威、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に関する法対応へのリスクを低減する取り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当たっては、ISO/IEC 27001 (ISMS) を参考にした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などのグローバルスタンダードも活用し、特定・防御・検知・対応・復旧の各フェーズの対応力の強化に取り組んでいます。

またサイバーセキュリティ対応は、攻撃を受けることを前提に、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<sup>※1</sup>）を設置し、「FUJIFILM CERT<sup>※2</sup>」の名称で、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。

※1 Computer Security Incident Response Team

※2 FUJIFILM Cybersecurity Incident Response/Readiness Team

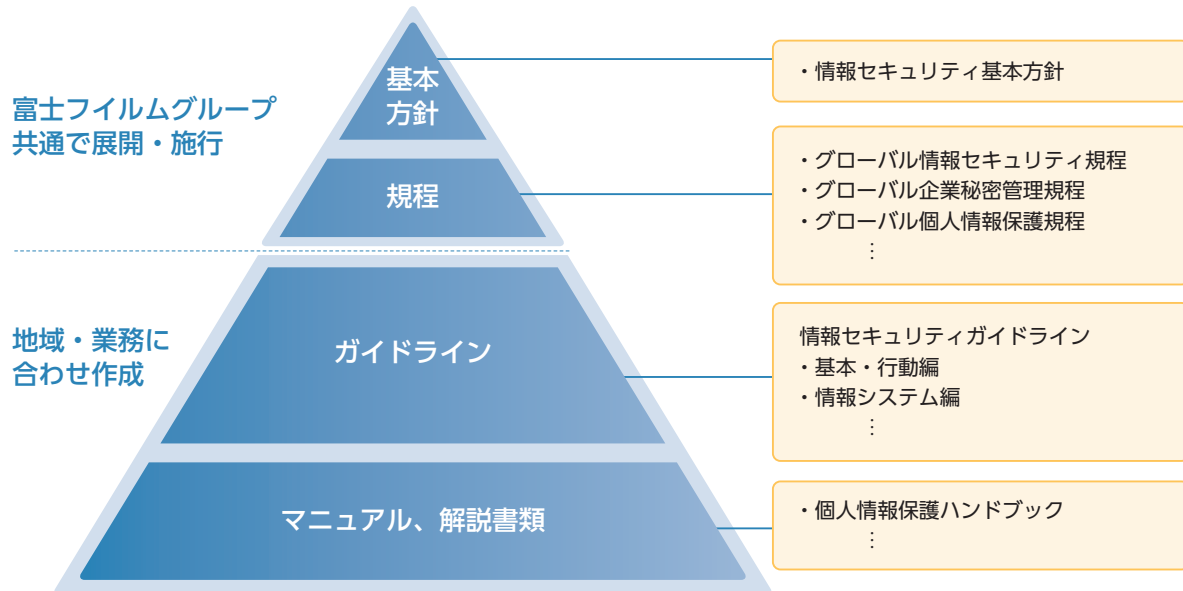
#### 富士フィルムグループの情報セキュリティ体制図



## 情報セキュリティに関わるルール体系

富士フィルムグループは、情報倫理、コンプライアンス、機密区分など、さまざまな観点から情報セキュリティに関わるルールを制定しています。ルールの構成としては、情報セキュリティに対する富士フィルムグループの姿勢を示し社内外に宣言している「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」となっています。「基本方針」「規程」は、海外各地域を含めたグループ全体で共通のものを展開しており、「ガイドライン」以下は地域ごとの環境や業務に合わせた独自のものを展開しています。また、いずれも、状況に合わせて見直しを行っています。



## 情報セキュリティインシデント対応と未然防止活動

富士フィルムグループでは情報セキュリティルールの徹底およびさまざまな管理策によって、インシデント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たとしても、情報セキュリティインシデントの発生を想定しないわけにはいきません。

そのためサイバー攻撃などの情報セキュリティインシデント報告を受け付けるための窓口を設置しています。グループ内の各部門で情報セキュリティインシデントを発見した際は、発見した部門の担当者が情報を把握し、セキュリティを統括する組織に情報が集約されます。その情報を内容に応じて関係組織と共有し、直ちに初動対応を実施することで影響を極小化するとともに、再発防止を検討・実施します。

発生した情報セキュリティインシデントが緊急かつ重要な案件の場合は、直ちに社長／全社情報セキュリティガバナンス責任者

／全社ICTセキュリティ責任者に報告します。その上で、全社での対応が必要な場合は、ESG委員会の分科会の位置付けで、社長を委員長とした総合危機管理委員会を開催し、被害の最小化に向けた対策を講じます。

このような対応を行った情報セキュリティインシデントの情報は、定期的にESG委員会、取締役会に報告しています。

また、組織ごとに1年に一度、リスクの抽出活動を実施しています。この活動の中では、情報セキュリティインシデントの発生状況を踏まえ、情報セキュリティに関わるリスクも抽出しています。その結果をESG推進部門が集約・評価して、全社で取り組むべき重要なリスクテーマを決め、対策を実行することで、情報セキュリティインシデントの再発防止、未然防止に努めています。



## 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ィルムグループの活動

富士フィルムグループは、グローバルで事業活動を行っています。そのため、サイバー攻撃への対応を、グローバルでの重要な経営課題の一つと捉えています。製品・サービスの安全なお客様への提供と、安定した事業継続のため、サイバー攻撃の早期検知と、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FUJIFILM CERTを設置・運用しています。

### FUJIFILM CERTの体制

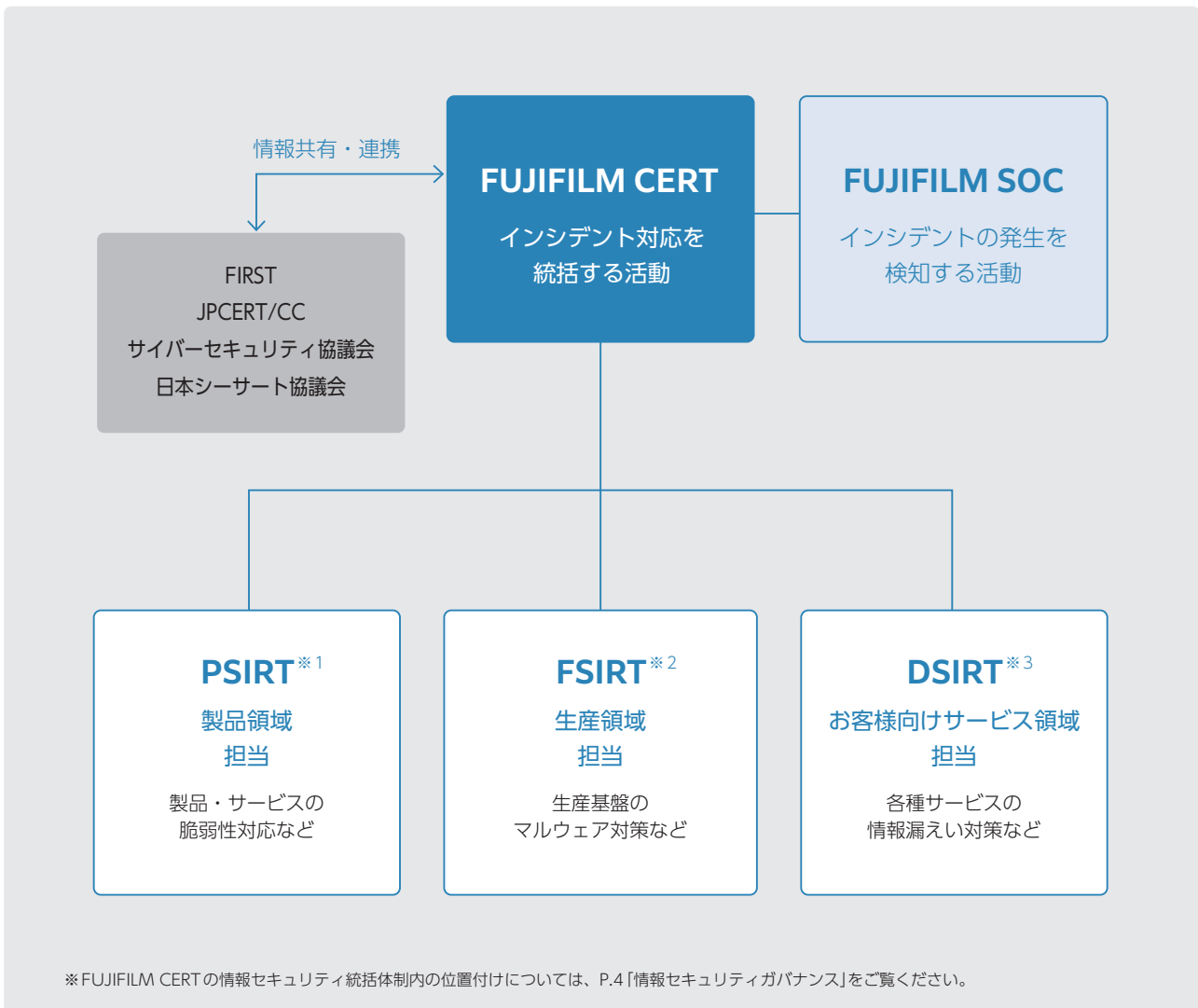
FUJIFILM CERTは、富士フィルムグループ傘下の関係会社／関連組織を横断する組織として運営されています。FUJIFILM CERTの運営事務局は、富士フィルムホールディングスの全社情報セキュリティ統括体制の一組織として置かれ、富士フィル

ムグループ傘下の各企業(海外拠点を含む)の製品領域を担当するPSIRT<sup>※1</sup>、生産領域を担当するFSIRT<sup>※2</sup>、お客様向けサービス領域を担当するDSIRT<sup>※3</sup>が連携して活動しています。また、富士フィ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24時間365日、グローバルで監視するFUJIFILM SOC(Security Operation Center)とも連携し、インシデントの発生を早期に検知するとともに、検知した場合は迅速に対応しています。

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、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](mailto:fujifilm-cert@fujifilm.com) (FUJIFILM CERT)

### FUJIFILM CERTの体制図



※ FUJIFILM CERT の情報セキュリティ統括体制内の位置付けについては、P.4「情報セキュリティガバナンス」をご覧ください。

※1 Product Security Incident Response Team ※2 Factory Security Incident Response Team ※3 Digital service Security Incident Response Team

## FUJIFILM CERTにおける活動

FUJIFILM CERTが対象にしているのは、富士フイルムグループ傘下の全ての関係会社であり、以下の表に示すような活動をしています。また、FUJIFILM CERTでは、CSIRT 記述書にて定義した体制・役割分担の下、定例会でメンバーとの情報共有を行いながら、日々のインシデント対応ならびに継続的な改善を行っています。

活動項目	実施内容の概要
脅威インテリジェンス	<ul style="list-style-type: none"> <li>●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</li> <li>●外部情報ソース (FIRST、JPCERT/CC、サイバーセキュリティ協議会など)やFUJIFILM SOCからの脅威情報の収集と分析</li> </ul>
インシデントハンドリング	<ul style="list-style-type: none"> <li>●サイバー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</li> </ul>
脆弱性ハンドリング	<ul style="list-style-type: none"> <li>●富士フイルムグループが提供する製品・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)</li> <li>●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</li> </ul>
未然防止活動	<ul style="list-style-type: none"> <li>●生産拠点ネットワークのセキュリティ強化 (FSIRT)</li> <li>●社外向けサイトの脆弱性検査 (PSIRT、DSIRT)</li> <li>●セキュア設計開発プロセスの運用 (PSIRT)</li> <li>●クラウドサービス商品全般のセキュリティ対策 (DSIRT)</li> <li>●FUJIFILM SOCの監視活動と連携した、情報持ち出しなどの内部不正に対する未然防止活動</li> </ul>
啓発・教育・訓練	<ul style="list-style-type: none"> <li>●FUJIFILM CERT内での定期的な活動状況報告</li> <li>●全社員を対象にした不審メール対応訓練</li> <li>●経営層を含めたインシデント発生時の初動対応訓練</li> <li>●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</li> </ul>

## 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へ所属、または連携し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年に加盟しました。

### JPCERT/CC (JPCERT コーディネーションセンター)

JPCERT/CCは、インターネットを介して発生する侵入やサービス妨害などのコンピューターセキュリティインシデントに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを技術的な立場から行う組織です。FUJIFILM CERTでも、当組織が提供する早期警戒情報を活用し、サイバーセキュリティ対応に当たっています。

### 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が運営するコミュニティです。情報セキュリティ上の脅威や攻撃に対し、少しでも早い段階でサイバーセキュリティの確保に必要な情報を迅速に共有することが目的であり、当社は2019年より参加しています。

### 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、同協議会の活動(サイバー演習に関するワーキンググループなど)に積極的に参加し、貢献しています。

# 2

## 製品・サービスの情報セキュリティ

### メディカル製品のセキュリティ

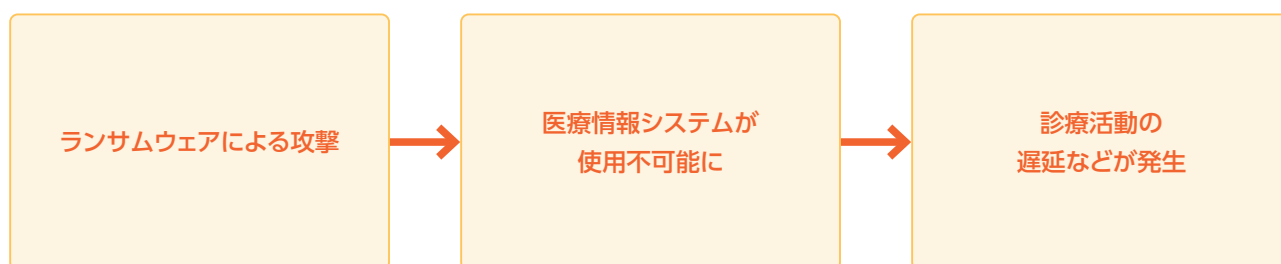
#### 医療情報システムのサイバーリスク

データを不正に暗号化し、復号を条件に身代金を要求するランサムウェアの攻撃が、2020年以降、増加傾向にあり、それに伴い医療機関を標的にした攻撃も増加しています。ランサムウェアに感染した医療機関では、医療情報システム(医療機器を含む)が使用できなくなることで、医療処置や検査に遅れが生じたり、他施設に患者の移送を余儀なくされたりといった深刻な被害に発展するリスクがあります。中には、システム復旧に数カ月を要する場合もあります。

医療機関がランサムウェアの標的となる理由としては、①患者の個人情報や医療記録といった機微な情報を大量に保有しており、身代金の要求につながりやすいこと、②医療情報システムは、そのシステムが使用しているOSなどのサポート期限を超えて長期にわたって使用される傾向があり、脆弱性を抱えている場合があること、などが挙げられます。

特に日本では、ランサムウェアの侵入経路のうち、7割以上がVPN機器に起因するとされています。<sup>\*1</sup>

#### ランサムウェアが医療機関にもたらすリスク



#### 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、早くから米国食品医薬品局(FDA)が積極的取り組み、製品の設計から市販後の管理まで、包括的なセキュリティ対策を求めるガイダンスを発行。2022年末にはFD&C(Federal Food, Drug, and Cosmetic)法<sup>\*2</sup>を改正し、医療機器のサイバーセキュリティの確保が規制要求となりました。

欧州では、医療機器規制MDR(Medical Device Regulation)、体外診断用医療機器規制IVDR(In Vitro Diagnostic Medical Device Regulation)にサイバーセキュリティ要求が盛り込まれたほか、2019年に欧州医療機器調整グループMDCG(Medical Device Coordination Group)が「医療機器のサイバーセキュリティガイダンス」を発行し、規制要求を補足しています。

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IMDRF(International Medical Device Regulators Forum)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など関係者間における遅滞のない製品セキュリティに関する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の考慮事項を記載しています。日本を含めた各国の規制当局が、このIMDRFのガイダンスを自国に導入するためのガイダンスを発行しています。

2021年12月には、医療機器を含むヘルスケアソフトウェアのサイバーセキュリティに関する国際規格「IEC 81001-5-1」が発行されました。この規格は、製品の設計から市販後、製品廃棄までの製品ライフサイクルを通して製造事業者が行うべき活動を規定しており、米国や欧州の規制要求とも多くの共通事項を含みます。日本では、薬機法における医療機器の基本要件基準にサイバーセキュリティ要求を追加し、その適合性確認として「JIS T 81001-5-1」に基づく対応を求めています。

<sup>\*1</sup> 参考：警察庁広報資料「令和5年上半年におけるサイバー空間をめぐる脅威の情勢等について」

<sup>\*2</sup> 連邦食品・医薬品・化粧品法



## 富士フィ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機器について、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) を発足させました。

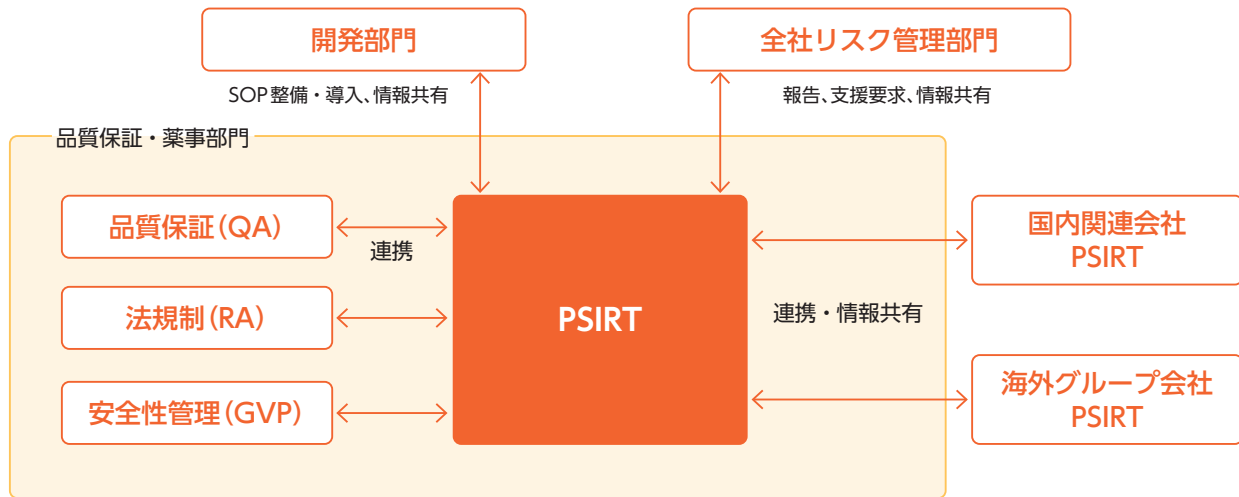
PSIRTの主な役割としては、以下の5つがあります。

- 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
- ⑤ ISO/IEC 27001 認証取得の維持・拡大の推進

PSIRTは発足当初より、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に必要な開発・管理プロセス(SOP)の整備・導入に取り組んできました。現在も継続して、最新規制動向を見据えた対応やプロセス改善に取り組んでいます。

また、2021年6月に情報セキュリティマネジメントシステムに関する国際規格「ISO/IEC 27001」の認証を取得し、対象領域の拡大に継続的に取り組んでいます。

## 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



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。

<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、さまざまな環境で複合機をお使いいただく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、データへの不正アクセスや複合機への侵入をいかに早く検知して、対応と復旧につなげることができるかがお客様の事業継続に重要だと考えます。

富士フイルムビジネスイノベーションは、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だけでなく、サプライチェーン全体でセキュリティリスクの低減に努めています。またセキュリティ認証を取得し、全世界のお客様に、安心してお使いいただける製品を提供します。

### サプライチェーンセキュリティの取り組みと ISO/IEC 20243 認証取得

近年、製品の開発・生産工程においてマルウェアなどが混入した不正な部品やプログラムを仕込むことで、標的となる企業の情報システムを攻撃する「サプライチェーン攻撃」が増加しています。富士フイルムビジネスイノベーションは、サプライチェーンの透明性を確保し、製品の信頼性と安全性を向上させる活動に取り組み、開発生産工程全体で偽造品混入防止に努めています。

また、2024年7月には国際規格であるISO/IEC 20243の第三者認証を取得しました。この認証は、サプライチェーン(サプライヤー・委託先・自社における開発、調達、製造、販売、流通、保守、廃

棄)における、不正な部品やプログラムの差し替え・混入、偽造品混入のリスクに対する規格であり、本規格の認証により、製品のサプライチェーン全体にわたるセキュリティリスクに対する対策を確認できます。こうした取り組みにより、私たちの製品を、製品のライフサイクルを通じ安心して安全にお使いいただけることを保証します。

### 複合機のセキュリティ対策方針

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、米国国立標準技術研究所(NIST)が定めているSP800-171/SP800-172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、防衛調達をはじめとして導入の検討が進んでいます。

富士フイルムビジネスイノベーションでは、「特定」「防御」「検知」「対応」「復旧」の5つの観点で複合機のセキュリティ対策を実施することでSP800-171/SP800-172対応を進め、その準拠性について情報セキュリティ格付け機関から最高評価の「AAAIis」を取得しています。

### 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される脅威に対しては、「起動時改ざん検知機能」(起動時にソフトウェアの完全性をチェックし、改ざん検知時は修復を実施)と「稼働時改ざん防止機能」(ホワイトリストに基づいて、不正なアプリケーションの実行を防止)により対策しています。

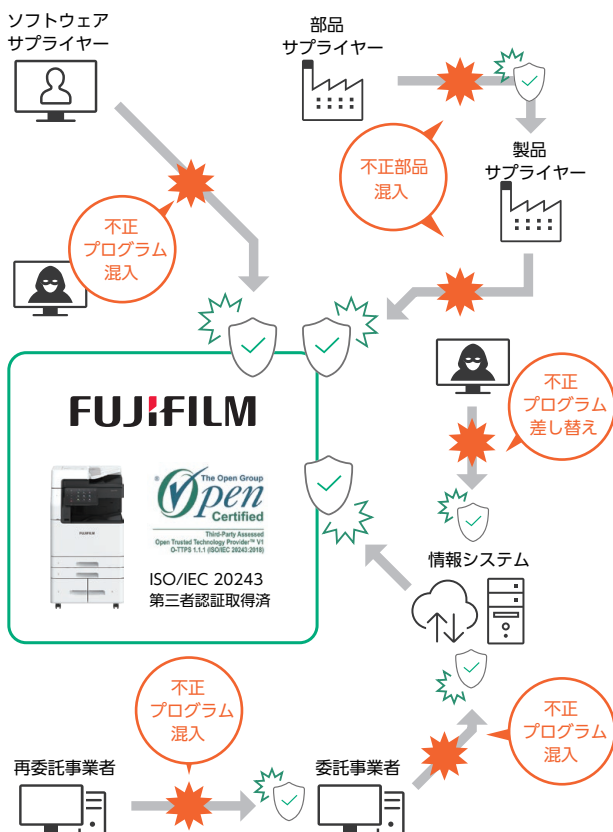
### セキュリティ脅威の早期検知

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、ジョブ実行などの事象は監査ログとして、リアルタイムに外部のサーバーに転送できます。複合機をSIEM<sup>※</sup>製品と連携させることで、複合機の監査ログを一元管理・分析することができ、セキュリティ脅威となる事象の早期検知が可能となります。

※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

富士フイルムビジネスイノベーションの複合機は、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 プロテクトプロファイルv1.0」(HCD PP v1.0)に適合した国際セキュリティ標準ISO/IEC 15408 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。



# 3

## お客様への安全のご提案

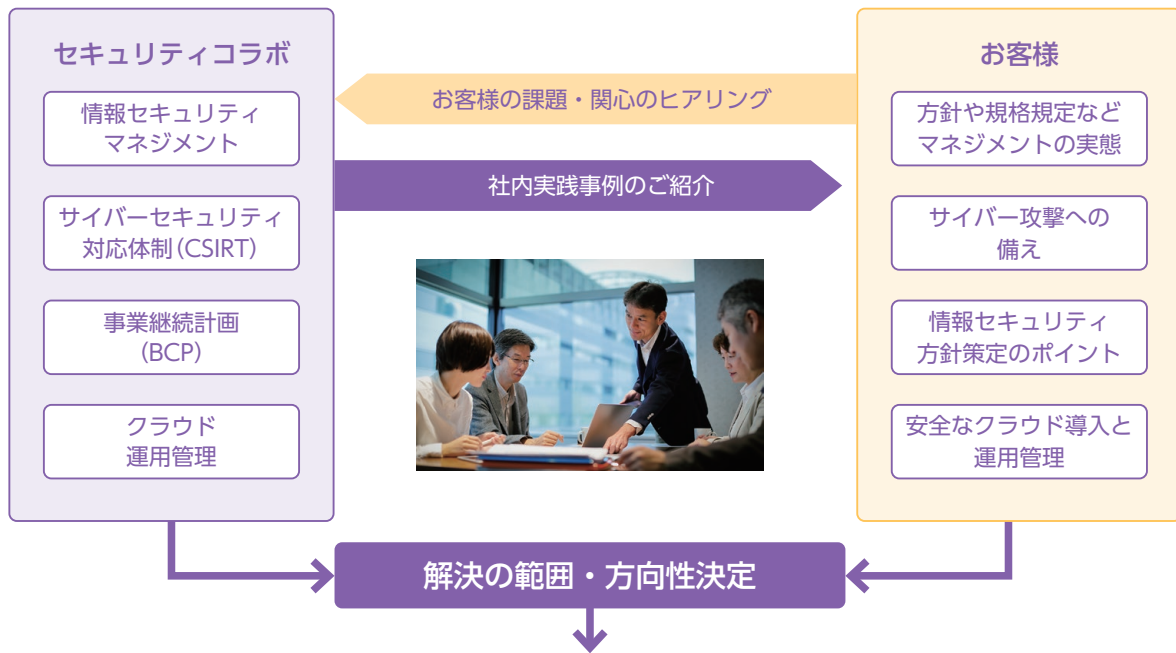
### 社内実践事例コラボによる情報セキュリティの課題解決

富士フイルムビジネスイノベーションは、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ISO/IEC 27001を取得し、運用しています。さらにNIST SP800-171も参照し、情報セキュリティの取り組みを行っています。こうした取り組みを通じて直面した課題やその是正方法などに関するノウハウを数多く蓄積しており、それらを社内で活用するだけでなく、お客様の課題に応じた解決の方向性を具体的に紹介する「社内実践事例コラボ」を開催しています。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するとともに、企業によって規模感や深さが異なる課題

の現状を個別に調査・分析しながら、共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最高責任者である経営者の皆様にマッチした内容となっています。

さらに豊洲ショールーム(東京都江東区)に常設した情報セキュリティブースでは、刻々と変化する情報セキュリティの脅威を踏まえ、マルウェアなどのリスクや、最新のソリューションを体感できる機能を備え、お客様に具体的な課題解決のイメージを提供しています。

#### ■ 社内実践事例コラボの概要



### 情報セキュリティの脅威と最新ソリューションの体感

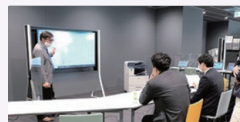
#### 豊洲ショールーム

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

- ① 最新セキュリティに関する情報を紹介。
- ② お客様の課題に応じた、解決のヒントを提示。
- ③ 視覚的、体感的に理解しやすい展示内容。



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あります。

# 4

## 社内の情報セキュリティ

### 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

※写真はイメージです。実際の対策シーンとは異なります。



#### 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／維持
- 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リスクマネージャー／情報セキュリティ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時の速やかな社内報告の徹底
- 経営層およびFUJIFILM CERTを対象としたサイバーセキュリティ訓練の実施
- 従業員を対象とした不審メール訓練の実施
- サプライヤー／業務委託先に対する情報セキュリティ調査
- 有事を想定した初動対応マニュアルの整備



#### 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
- 情報の不正持ち出し監視
- 紛失・盗難時のPC内ファイルの遠隔削除
- 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
- PCのディスク全体暗号化
- アクセス禁止カテゴリや悪性サイトに対するWebアクセスのフィルタリング
- プリント時のICカード認証
- 機密文書プリント時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
- ネットワークの脆弱性に関する情報管理
- 文書ファイルの暗号化
- 侵入を前提とした検知・監視・駆除対策



#### 物理的対策

- 主要拠点での従業員証(ICカード)による入退管理
- ワイヤロックによるPCの固定、PCの施錠保管
- 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)
- 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
- 情報機器利用終了時のサニタイズ処理(安全な廃棄処理)



## サプライチェーンのセキュリティ対策

昨今のサイバー攻撃の高度化、巧妙化により、サプライチェーン全体にその影響範囲が拡大しています。もはや企業における情報セキュリティは、自社のセキュリティ強化のみに注力するフェーズを過ぎ、サプライチェーン全体を意識した情報セキュリティ体制の構築・強化が求められています。

富士フィルムグループでは、製品の製造に必要な部品や原材料などを供給・納入するサプライヤー、商品開発や基幹業務をはじめとした業務の委託先など、多くのパートナー企業に支えられて事業活動を行っています。サプライチェーンを構成するパートナー企業がサイバー攻撃を受けた場合、当社の生産・供給リスクや預託していた機密情報・個人情報の流出リスクにつながることから、パートナー企業と緊密に連携を行い、情報セキュリティについても品質の一部と捉えて、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、業務委託時には、委託先のみならず、その先に関与する事業者についても富士フィルムグループ各社の管理範囲と見なし、サプライチェーン全体の情報セキュリティの確保・強化を行っています。

### サプライヤーへの情報セキュリティ強化の取り組み

富士フィルムグループでは、サプライヤーに対する情報セキュリティ要求事項の策定を行い、所定のプロセスに基づいた情報セキュリティ調査を行うことでサプライヤーの基本的な情報セキュリティ対応状況を確認しています。

サプライヤーへの情報セキュリティ調査はWebシステムなどを活用して実施しており、結果を報告書としてフィードバックすることにより、サプライヤー各社は自社・他社の対策状況を自ら確認することができます。

また、情報セキュリティ調査の結果、十分に対策ができていないセキュリティ上の問題については、未対策のまま運用を続けることで生じるリスクと、その対策方法を報告書の中で解説しています。さらに、サイバーセキュリティ対策についての勉強会を開催するなど、サプライヤーとのコミュニケーションを通して、サプライチェーン全体でセキュリティに対する意識を底上げする啓発活動を進めています。

### 業務委託先への監査強化の取り組み

他社の業務委託先での大規模な個人情報漏えい事故をきっかけに、富士フィルムビジネスイノベーションでは重要な情報を預託している業務委託先へのセキュリティ調査を行っています。以前より業務委託先にお客様や当社の重要な情報を預ける際のガイドラインを整備・運用していましたが、セキュリティを担当する情報セキュリティ統括組織・品質保証部門だけでなく、購買部門も加わったタスク活動で、案件に応じて適切なパートナー企業を

選定するためのプロセスの効率化とガバナンスを強化するとともに、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ラインを修正しました。

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業務委託先に依頼しています。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を確認する設問で構成されており、それらに対する回答結果を購買部門に集約し一元管理しています。また、個人情報が含まれる場合には、管理方法など取り扱いに関する覚書を取り交わして、法令を遵守し富士フィ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。

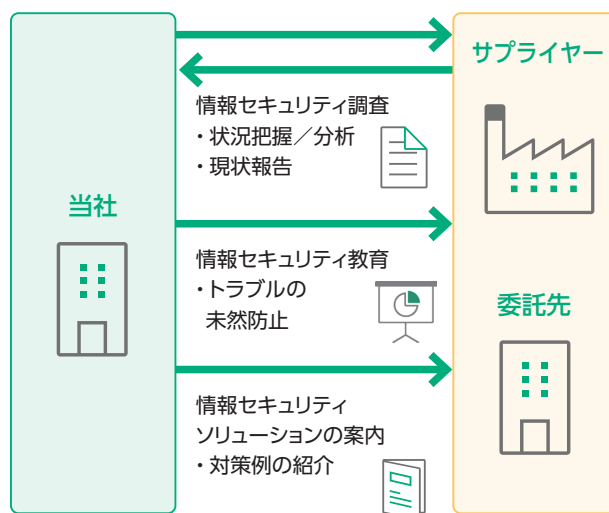
現在、同様にグループ内での取り組みを拡大しています。

### 具体例：委託先の委託業務従事者からの誓約書の取得

富士フィルムビジネスイノベーションでは、社員以外の従業員、派遣社員、および当社事業所内で勤務する委託業務事業者から、「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、具体的には下記の内容を目的としています。

1. 秘密保持契約に基づく情報漏えいの防止
2. 富士フィルムビジネスイノベーションとその関連会社の施設、設備などの適正利用
3. 情報資産を含む当社資産の保全
4. 富士フィルムビジネスイノベーションとその関連会社の事業所における入退管理ルール of 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. 入退館カードの適正利用

### ■ パートナー企業に対する情報セキュリティ強化の取り組み

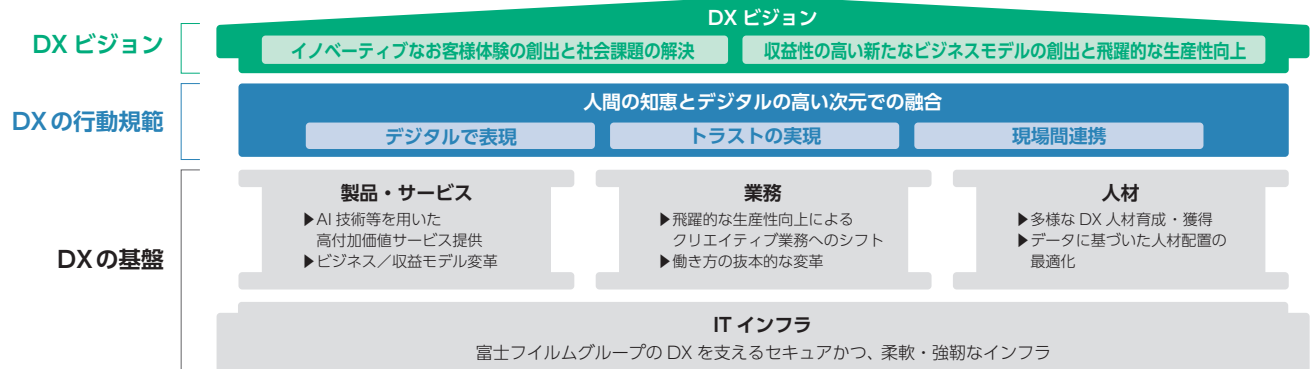


## DXの推進とリスク対応

### 富士フィルムグループが目指すDXとAIの活用

現在、富士フィルムグループでは、ロボティクス・AI技術を製品・サービスに応用してお客様のDX加速を支援する「製品DX」、ソフトウェアなどの活用により業務プロセスを抜本的に変革し生産性を飛躍的に高める「業務DX」、DX人材の育成やデータに基づいた人材配置の最適化を推進する「人材DX」に取り組んでいます。さらにはこれらの取り組みを支える基盤として、強固な情報セキュリティの下、柔軟かつ強靱なITインフラを構築しています。

人間の知恵とデジタルの高い次元での融合を追求し、当社DXビジョン実現を加速させる

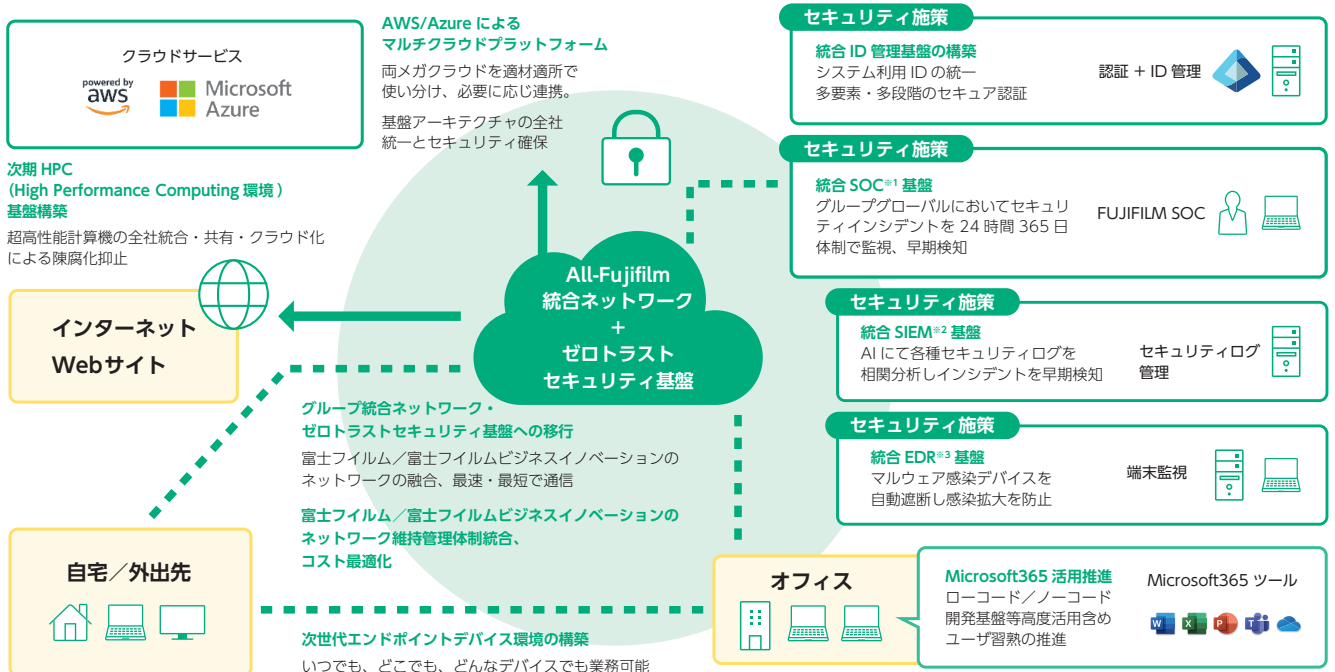


なお、DXを推進する国内外のありとあらゆる現場でAIを積極活用し、製品・サービスの強化、業務の飛躍的な生産性向上、多様な人材の活躍の実現をより一層加速させていく上では、AI利活用におけるリスク対応も重要な要素です。

富士フィルムグループでは、サイバーセキュリティの面だけではなく著作権・プライバシー権など関連する各国の法令や新たな規制対応など、AIの適正利用に向けて、社内の関連する組織でリスクに対応しています。

### インフラ・セキュリティ主要施策

最新技術・サービスの活用ならびに国内外のグループ会社共通の施策導入により、高い生産性と安全な執務環境を両立しています。



※ 1 SOC…Security Operation Center：サイバー攻撃の監視・検知・分析を行う専門組織

※ 2 SIEM…Security Information and Event Management：ファイアウォールなどから出力されるログやデータを一元的に集約し、それらのデータを組み合わせて相関分析を行うことでサイバー攻撃やマルウェア感染などのインシデントを検知することを目的とした仕組み

※ 3 EDR…Endpoint Detection and Response：ネットワークに接続されたコンピューターやサーバーを監視し、不審な挙動を検出するセキュリティ対策ソフトウェア

また、DX推進のロードマップを掲げ、さまざまなステークホルダーとの協働による新たなエコシステムの形成を通じて、当社の製品・サービスを「持続可能な社会を支える基盤」として定着させ、社会課題の解決に貢献し続けることを目指しています。そのためには、全てのステークホルダーに対する安心・安全な環境の提供が不可欠であり、サイバーセキュリティを欠かせない要素であると位置付けています。

## サイバーセキュリティ対策強化の取り組み

当社では、米国国立標準技術研究所(NIST)が発行する、グローバル標準のサイバーセキュリティフレームワークを活用し、下記のとおり技術・運用の両面から漏れない対策を進めています。

フェーズ	対応項目	対策の例
特定	資産・重要情報の特定	<ul style="list-style-type: none"> <li>●従来国内外のグループ会社で現場個別管理となっていた端末に対し、セキュリティ対策ならびに重要情報の所在についての調査を実施</li> <li>●ネットワーク機器構成情報の把握ならびに脆弱性対策の強化のため、国内外のグループ会社共通のネットワーク機器管理を開始</li> </ul>
	漏えい防止策	<ul style="list-style-type: none"> <li>●私用外部ストレージなどを用いた会社情報の持ち出し防止強化策として、SASE<sup>*4</sup>による外部サービスへのアクセス制限を開始</li> <li>●重要な情報を安全に保管するため、国内外のグループ会社共通のストレージを展開中</li> <li>●万が一、重要な情報が持ち出されても会社支給端末以外では閲覧できないようにするため、IRM<sup>*5</sup>による暗号化設定を活用中</li> </ul>
防御	基盤対策	<ul style="list-style-type: none"> <li>●クラウド環境のセキュリティを国内外のグループ会社全体で確保するため、共通のセキュリティ設計に基づくマルチクラウドプラットフォームの利用を開始</li> <li>●攻撃者侵入後の横展開による被害を最小化するため、マイクロセグメンテーション<sup>*6</sup>によるデータセンターネットワークセキュリティ強化を実施</li> </ul>
	早期発見	<ul style="list-style-type: none"> <li>●サイバー攻撃の兆候を早期に検知・対応するため、国内外のグループ会社全体でのEDR、SOC運用などにより24時間365日、異常を監視・対応する仕組みと体制を運用中</li> <li>●FUJIFILM SOCの監視精度の高度化や運用品質の向上を目的として、Red Teamテスト<sup>*7</sup>などを通じた課題の洗い出しや改善を行い、継続的に検知・対応力の強化を実施中</li> </ul>
対応	通報	<ul style="list-style-type: none"> <li>●従業員が夜間・休日でも緊急連絡を直ちに行える緊急連絡受付体制を整備し運用中</li> </ul>
	緊急指示・対応	<ul style="list-style-type: none"> <li>●会社支給端末を使わず従業員に緊急指示ができるよう、個人端末から利用可能な災害用緊急連絡システム、館内放送、館内掲示板の活用ルールを運用中</li> </ul>
	対策会議	<ul style="list-style-type: none"> <li>●経営層による迅速かつ的確な意思決定のため、重大なサイバー攻撃発生時にはESG委員会にて対策を検討するプロセスを運用中</li> </ul>
	影響と原因調査	<ul style="list-style-type: none"> <li>●端末のフォレンジック<sup>*8</sup>による原因調査を速やかに実施するため、あらかじめ依頼する外部ベンダー候補を決定し有事を想定した準備を実施</li> </ul>
復旧	関係機関報告	<ul style="list-style-type: none"> <li>●個人情報保護法を遵守するため、個人情報保護委員会やその他報告先候補への報告手順をまとめ運用中</li> </ul>
	事業継続	<ul style="list-style-type: none"> <li>●システム停止で甚大な影響が想定される業務について、有事に備えPCを使わない業務などへの代替策(BCP：事業継続計画)を準備し、運用中</li> </ul>
復旧	復旧	<ul style="list-style-type: none"> <li>●優先して復旧させるシステムを決めるとともに、システムの利用不能時に備えて重要な情報は確実にバックアップを取ることに付いて、定期的に周知活動を実施</li> </ul>

※4 SASE…Secure Access Service Edge：ゼロトラストネットワークを実現するネットワークセキュリティモデルの一つ。全ての通信をインターネット上の仮想セキュリティ基盤に経由させ、外部サービスへのアクセスを制限するなど、クラウドセントリックな環境下でも安全な環境を実現

※5 IRM…Information Rights Management：文書ファイルを暗号化し、閲覧や編集を管理・制限することのできるソフトウェア

※6 マイクロセグメンテーション：ネットワークセグメントを細分化し、トラフィックの可視化と制御を細かく行うことでセキュリティを高める設計技術

※7 Red Teamテスト：セキュリティ専門家が顧客企業に対して現実に近い各種攻撃を仕掛け、企業のセキュリティ対策の実効性を検証するテスト

※8 フォレンジック：すでに消えてしまったデータや管理情報を対象に精細に情報を取り出し、実際にどのような操作が行われたのかをデータから解明する作業

## 個人情報保護への取り組み

### 基本方針

富士フィルムグループでは、国内外の全従業員がどのよう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、富士フィルムグループ各社が個人情報保護方針、またはプライバシーポリシーを定め、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、富士フィ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。\*

### 推進体制

富士フィルムグループでは、ESG推進部門担当役員を管理統括者として個人情報保護体制の構築・維持を行っています。

グループ全体における個人情報に関する方針は、富士フィルムホールディングスの社長を委員長とするESG委員会でご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担っており、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が担保されています。ESG委員会の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ESG推進部門から、方針・目標がグループ内に展開されます。また、ESG推進部門は、方針・目標の遂行状況の把握や個人情報を取り扱う各組織長に対する指導・助言、規程内容の従業員への周知徹底などを行っています。さらに、社会での個人情報保護に関する意識向上に伴い、個人情報の保護は会社の重大なリスク課題であると捉え、毎年実施しているリスク抽出の中でもアクションプランを策定し、グループ全体のリスクマネジメントの体制の中で活動の確認をしています。

グループ各社・各組織にて個人情報保護に取り組む体制としては、個人情報実務管理責任者を選任しています。また、一部の事業組織では製品単位ではなく、組織横断で適切な法令対応が実施できるように事業組織の品質部門に個人情報保護の対応を推進する役割を据え付けています。なお、ISMS / プライバシーマークを取得しているグループ会社では、ISMSの推進活動と一体化して定期的な外部審査の受審とその審査結果を基にした改善活動を行っています。

### 従業員教育

富士フィルムグループでは、個人情報の取り扱いに関する事故・違反の発生防止のためには、従業員一人ひとりが必要とされる知識を身に付け、高い意識を持つことが重要だと考えています。そのため、全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。特に大量の個人情報を取り扱う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」を配布し従業員の啓発に役立てています。

また、国内では就業規則において、許可を得ない個人情報の持ち出しに対して懲戒処分を含めた対応を行うことを定め、海外に付

いても同様の対応を進めています。さらに、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ち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。

### 個人情報の適切な取り扱い

富士フィルムグループでは、個人情報の取り扱いに関する内部規程（グローバル個人情報保護規程、個人情報管理規程、各種ガイドラインなど）と個人情報保護方針 / プライバシーポリシーを定め、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Web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、政府機関から個人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。

### 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・見直しが進んでいるため、それらに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。

2023年には欧州、米国、アジアパシフィック地域などの一部のグループ会社で共通の個人情報の棚卸システムを導入し、これらの地域の個人情報の取り扱い状況を一元管理できるようにしました。年1回の棚卸しにより、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などを行っています。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。

### 個人情報の取り扱いに関する事故・違反

2023年度は、個人情報の外部への漏えいや目的外利用などの不適切な取り扱いに対する第三者もしくは規制当局からの指摘、ならびに社外に公開すべき重要な事案はありませんでした。なお、軽微な事案についても全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関係者などに情報を開示し、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。

\* 調達先・業務委託先との連携についての詳細は、P.13「サプライチェーンのセキュリティ対策」を参照ください。



## 重要情報管理

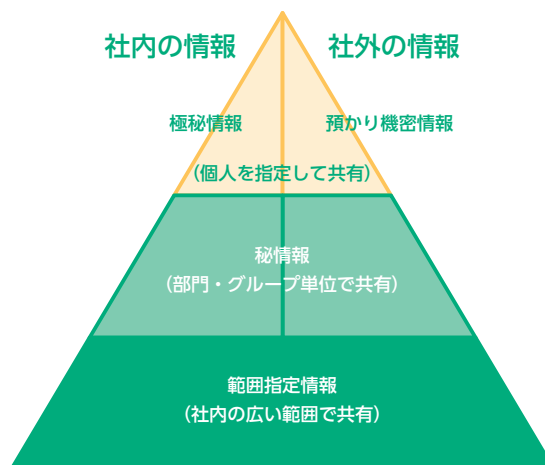
近年高まる情報セキュリティリスクに対し、前述のサイバーセキュリティ対策やセキュリティ監視に加え、社内の機密情報、お客様やお取引先様からお預かりしている情報や個人情報の管理強化も同時に進めています。

富士フィルムグループでは、日々社内で作成される情報や社外から預かる情報は、右図のとおり重要性に基づいた4つの区分で分類しています。社内で使用する文書にはその区分が分かるように表示を付け、社外持ち出しや複製・社外とのやり取りにおいてその区分に応じた取り扱いをするよう社内ルールで定めています。

会社にとって非常に重要な情報(右図の黄色枠内)については、IRM (Information Rights Management) を利用し、外部への漏えいが発生した際であっても第三者は閲覧することができないよう、文書の暗号化とアクセス制御を同時に実施することで、組織が保護すべき重要情報を不正なアクセスから保護しています。また、国内外の各組織では、個人情報を含め重要な情報の台帳管理を進めることで、守るべき情報資産の特定を行い、適切な対策を講じています。

このような施策を進める中で、従業員に対し、作成中の文書における重要性の判断基準を分かりやすく示し、容易に暗号化設定を行うことができるよう、国内のグループ会社では社内開発した「区分支援ツール」を導入しました。

### ■ 富士フィルムグループにおける文書情報区分



### ■ 区分支援ツール

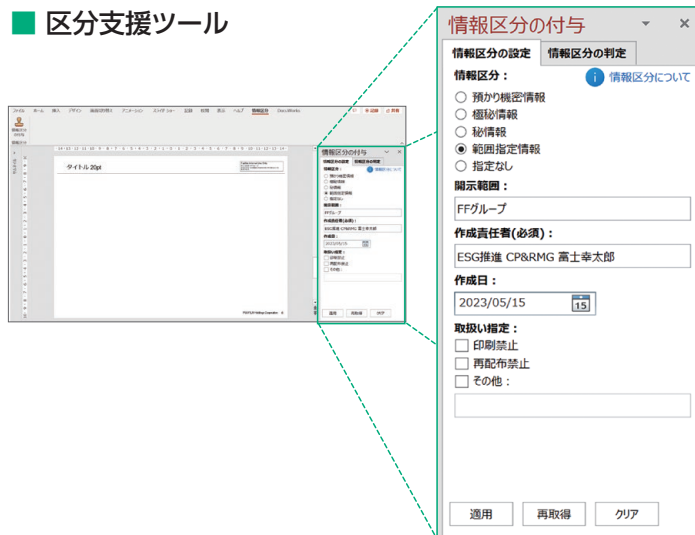
区分支援ツール(右図)は、作成中のOffice文書(Power Point / Word)に情報区分の表示を付与し、同時に暗号化設定を行うOfficeアプリケーションのアドイン(追加機能)です。

区分支援ツールには「情報区分の判定」と「情報区分の設定」の2つの機能があります。「情報区分の判定」は、その文書がどのような情報を含むかを選択肢から選ぶことで、上図に示した4つの情報区分のどれに相当するかを判別し、作成者が情報区分の判断に迷う際の支援となる機能です。また「情報区分の設定」では、情報区分と「開示範囲・作成責任者・作成日・取扱い指定」の区分表示を作成します。さらに、社内ユーザーのみが開くことのできる暗号化設定を行います。

なお海外ではマイクロソフト社の秘密度ラベルを活用し、同じく重要な情報の暗号化とアクセス制御を進めています。

このように万が一、不正なアクセスによる被害を受けた際にも被害を最小限に抑える管理を行うとともに、被害にあった情報の重要性に応じて社外への公表や監督官庁への報告など、必要とされる対応を迅速に実施できる体制と手順を整備しています。

### ■ 区分支援ツール



### ■ 技術情報等の重要情報の保護

技術情報など、漏えいすると甚大な影響が生じる重要情報を特定して、情報漏えい対策を強化する活動を実施しています。サイバー攻撃などの外部脅威、および内部者による不正な情報持ち出しなどの内部脅威に対応するためです。

主な強化策としては、①サイバー攻撃や権限者による不正持ち出しに対応するための頑強なITインフラ/情報管理システムの構築、②技術的な情報持ち出しの禁止措置、③情報持ち出しの監視措置を導入しています。これらの実施に当たっては、棚卸しにより重要な情報資産を特定し、どこにリスクが潜んでいるかを把握するためのリスクアセスメントを実施しています。

# 5

## 第三者評価・認証／ 富士フィルムグループの概要

### 富士フィルムグループにおけるプライバシーマークとISMS認証の取得状況(2024年4月時点)

#### プライバシーマーク<sup>※1</sup>

プライバシーマネジメントシステム(PMS)の規格JIS Q 15001の認証を取得し、一般財団法人日本情報経済社会推進協会(JIPDEC)のプライバシーマークの使用を認められた認定会社は、以下のとおりです。

富士フィルムイメージングシステムズ 富士フィルムイメージングプロテック 富士フィルム医療ソリューションズ	富士フィルムテクノサービス 富士フィルムヘルスケアシステムズ 富士フィルムヘルスケアラボラトリー	富士フィルムメディアクレスト 富士フィルムメディカル 富士フィルムシステムサービス
--	--	---

#### ISMS(情報セキュリティマネジメントシステム)

国際規格ISMS(ISO/IEC 27001)認証<sup>※2</sup>を取得した組織を持つ会社は、以下のとおりです。

富士フィルム <sup>※3</sup> 富士フィルムイメージングシステムズ <sup>※3</sup> 富士フィルムイメージングプロテック <sup>※3</sup> 富士フィルムソフトウェア <sup>※3</sup> 富士フィルムメディカル <sup>※3</sup> 富士フィルム和光純薬 <sup>※3</sup> 富士フィルムビジネスイノベーション 富士フィルムビジネスイノベーションジャパン 富士フィルムシステムサービス 富士フィルムプリンティングシステムズ 富士フィルムマニュファクチャリング	富士フィルムサービスクリエイティブ 富士フィルムサービスリンク 富士フィルムデジタルソリューションズ 富士フィルムRIPCORDER FUJIFILM Eco-Manufacturing (Suzhou) FUJIFILM Manufacturing Hai Phong FUJIFILM Manufacturing Shenzhen FUJIFILM Business Innovation Asia Pacific FUJIFILM Business Innovation Asia Pacific (Malaysia Operations) FUJIFILM Business Innovation Australia	FUJIFILM Business Innovation (China) FUJIFILM Business Innovation Hong Kong FUJIFILM Business Innovation Korea FUJIFILM Business Innovation Malaysia Sdn. Bhd. FUJIFILM Business Innovation New Zealand FUJIFILM Business Innovation Philippines FUJIFILM Business Innovation Singapore FUJIFILM Business Innovation Taiwan FUJIFILM Business Innovation (Thailand) FUJIFILM Business Innovation Vietnam FUJIFILM Data Management Solutions
--	---	---

#### ISMS-PIMS(プライバシー情報セキュリティマネジメントシステム)

ISMS-PIMS(ISO/IEC 27701)認証<sup>※4</sup>を取得した組織を持つ会社は、以下のとおりです。

富士フィルムシステムサービス <sup>※3</sup>	FUJIFILM Business Innovation Korea	FUJIFILM Business Innovation Taiwan
------------------------------	------------------------------------	-------------------------------------

※1 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です。

※2 情報セキュリティリスクを管理する仕組みの構築・運用方法を定めた国際規格の認証です。適用範囲が限定される場合がありますので、詳細は各会社へお問い合わせください。

※3 国内適用範囲および組織部門名称は、「情報システムマネジメントシステム認定センター」の「登録組織検索」にてご確認ください。

※4 ISMS認証を前提としたプライバシー保護に関する認証です。P.19「Topics」もご確認ください。

### ISO/IEC 15408<sup>※5</sup>認証の取得状況

富士フィルムビジネスイノベーションおよび関連会社は、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。2022年4月から2024年3月まで新規に認証取得した製品は、以下のとおりです。

製品名	認証年月日
FUJIFILM Apeos C3060 / C2560 / C2360 / C2060 / C3060 GK / C2560 GK / C2060 GK コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2022年5月9日
FUJIFILM Apeos 5570 / 4570 / 3570 / 5570 GK / 4570 GK コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2022年5月9日
FUJIFILM Apeos 3560 / 3060 / 2560 / 3560 GK / 3060 GK / 2560 GK コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2022年5月9日
FUJIFILM Apeos C5240 コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2022年6月2日
FUJIFILM Apeos 6340 コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2022年6月2日
FUJIFILM Revoria Press E1136 / E1125 / E1110 / E1100 コピー、プリント、スキャン、ストレージの上書き消去、PostScript 機能搭載モデル	2022年7月8日
FUJIFILM Apeos 7580 / 6580 / 5580 コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2023年3月5日
FUJIFILM Apeos 5330 / 4830 コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2023年3月20日
FUJIFILM Apeos C4030 / C3530 コピー、プリント、ファクス、スキャン、ストレージの上書き消去機能搭載モデル	2023年3月20日

※5 情報セキュリティの観点から、情報技術に関連した製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。

## Topics

### 富士フィルムシステムサービスが富士フィルムグループで初となる ISMS-PIMS 認証を取得しました

2023年10月27日、富士フィルムシステムサービスが提供する「戸籍総合システム・ブックレス クラウドサービス」に対し、プライバシー保護の国際規格である ISMS-PIMS 認証 (ISO/IEC 27701) の初回登録が承認されました。ISMS-PIMS 認証は、広く情報セキュリティ管理基盤として認知されている ISO/IEC 27001 (ISMS) およびその実践規範である ISO/IEC 27002 のアドオン規格であり、富士フィルムグループでは初の取得となります。

### 富士フィルムホールディングスが「Cyber Index Awards 2023」大賞を受賞しました

2023年12月8日、富士フィルムホールディングスは、日本経済新聞社が主催する「Cyber Index Awards 2023」において、最上位賞である大賞を受賞しました。「Cyber Index Awards」は、経済・社会のデジタルトランスフォーメーション (DX) を大きく前進させる上で重要なサイバーセキュリティで優れた成果を上げた企業や取り組みを表彰するものです。



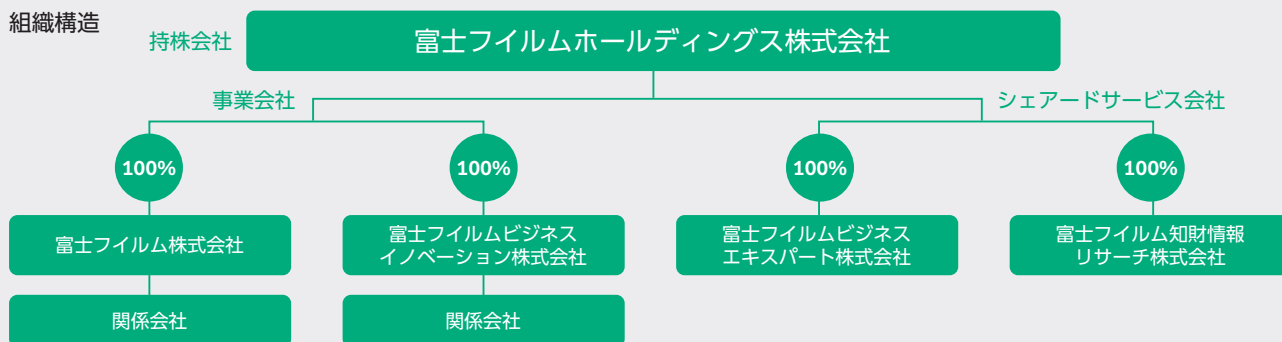
大賞受賞に際し、特に高く評価された取り組みは以下のとおりです。

- デジタルを活用することで、一人ひとりが飛躍的に生産性を高め、そこから生み出される優れた製品・サービスを通じて、イノベティブなお客様体験の創出と社会課題の解決に貢献し続けるという「DXビジョン」を策定し、最高経営責任者 (CEO) 自らが中心となってグループ全体のDXを推進している。
- DXとサイバーセキュリティを、持続的な自社グループの成長と社会発展に貢献し続けるのに欠かせない要素と位置付けている。
- 社会、経済、環境、人権などを考慮したグループ企業全体のサステナビリティの観点から、サイバーインシデントの報告ルールや統括的な対応体制などグループ全体のガバナンス体制を構築。それらの取り組みを統合報告書やサステナビリティレポートなどで社内外に発信している。
- 社会的意義が大きい医療分野においてDXを推進し、サイバーセキュリティ強化に取り組んでいる。

## 富士フィルムグループの概要

会社名：富士フィ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

### 組織構造



### 事業領域

ヘルスケア	エレクトロニクス	ビジネスイノベーション	イメージング
トータルヘルスケアカンパニーとして「予防」「診断」「治療」の3領域で幅広い事業を展開	デジタル時代を支える半導体や次世代ディスプレイなどに向けた高機能材料、データ保存用の記録メディアなどを提供	新しい働き方や生産性向上、創造性の発揮をもたらす製品やソリューションサービス、グラフィックコミュニケーションを展開	「撮影」から「出力」に至る、写真に関わる製品・サービスを提供



■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 : 03-6271-1111 (代表)

2024年9月発行