RICOH
imagine. change.

情報セキュリティ報告書 2023

トップメッセージ

株式会社リコー
セキュリティ統括センター 所長

手島 裕之

昨今情報セキュリティに対するリスクは、さらに急増しております。サイバー攻撃の頻発、不正技術の多様化・高度化（ランサムウェア等）、各国規制の強化・多様化、地政学リスクの顕在化など、企業の対応範囲も拡大しております。また、デジタルサービスカンパニーへの変遷を経営目標とする当社においては、デジタルサービスにおける地政学的リスクの軽減のみならず、既存事業における収益性をより盤石なものとするため、「セキュリティ」を企業価値に据える必要があります。

デジタルサービスの会社への変革を目指すリコーにおいては、デジタルサービスにおける地政学リスクの軽減のみならず、既存事業における収益性をより盤石なものとするため、「セキュリティ」を企業価値の一つとしてとらえています。その一例として、2021 年に独自の自然言語処理 AI（人工知能）などを活用して業務支援を図る新サービス「仕事のAI」[1]シリーズを発売し、データビジネスに本格参入しました。

また、全社情報セキュリティに対する素早い経営判断と各国法規制への対応戦略を明確にし、セキュリティを企業価値向上につなげることを目的として「情報セキュリティ統括センター」を新たに創設しました（2023年6月 に「セキュリティ統括センター」に変更）。 官民挙げてのセキュリティ水準強化などの外部環境の変化を常に注視しながら、デジタルサービスの会社として柔軟に対応できるよう、継続的にセキュリティの取り組みを強化・改善し、それを実現するための情報セキュリティ体制を強化していきます。

本報告書では、リコーグループの情報セキュリティの取り組みの全体像をご紹介しておりますので、ぜひご一読くださいますようお願い申し上げます。

情報セキュリティ委員会の新設

「情報セキュリティ委員会」は、リコーグループのセキュリティに関する審議および意思決定を行うために当社の社長執行役員のもとに設置される機関として、2022 年度下期に新設しました。当委員会は、一定の資格要件を満たす執行役員で構成されており、2023年度から原則四半期ごとに開催します。 当委員会では、主に、リコーグループのセキュリティ戦略、セキュリティガバナンス、セキュリティオペレーションについて審議を行います。 昨今、情報セキュリティに対するリスクは急速に高まっています。サイバー攻撃の頻発、不正技術の多様化・高度化（ランサムウェアなど）、各国法規制の強化・多様化、地政学リスクの顕在化など、企業の対応範囲も拡大しています。

また、デジタルサービスの会社への変革を目指す上で、既存事業における収益性をより盤石なものとするため、デジタルサービスにおけるセキュリティリスクの軽減のみならず、事業成長に向けた投資としてとらえ、取り組む必要があります。 近年、企業がDX化による企業競争力の向上を狙う一方で、解決すべきセキュリティの課題も生じています。このため、2022年度からセキュリティ統括担当であるCEOの直轄に、リコーグループ全体のセキュリティ戦略およびプライバシー保護戦略の立案・推進を担うセキュリティ推進部門を設置しました。当該部門は、セキュリティに対する素早い経営判断や、各国法規制への対応戦略の明確化など、当委員会の運営を支えています。

セキュリティ強化へ具体的な取り組み

●プロダクトセキュリティ

■ セキュリティ・バイ・デザイン：商品・サービスのセキュリティを企画・設計段階から確保するセキュリティ・バイ・デザインの実践に取り組んでいます。セキュア開発の国際標準ISO/IEC27034-1 に基く社内規定を制定し、順次適用を進めています。
■ セキュリティリスクへの取り組み：脆弱性対策については国際基準 ISO/IEC 29147/30111 に基づき脆弱性への早期対応を図っています。高いサイバー攻撃リスクに対する対応状況・注意喚起、セキュリティ研究者からの脆弱性報告の受付窓口の設置、脆弱性対策情報を提供しています。

●コーポレートセキュリティ

ランサムウェアなど企業を標的としたサイバー攻撃が高度化、複雑化する中、リコーグループはサイバーセキュリティ対策をグローバルで推進しています。
■ CSIRT の設置と運用：2013 年度より RICOH-CSIRT (Computer Security Incident Response Team) を組織し、SOC（Security Operation Center）からのインシデント報告、社外 CSIRT 組織からの情報、セキュリティ情報サイトからの情報をもとに脅威を分析し、特定された脅威に対して迅速かつ最適な対応（証拠保全、攻撃解析、原因究明、拡散防止、事態収束）を主導しています。
■ SOC の設置と運用：リコーグループの保有する IT システムを常時監視することで、外部からの不正侵入、内部からの不正利用をいち早く検知し、CSIRTと連携することによりインシデントの早期対応を実現しています。

●ファクトリーセキュリティ

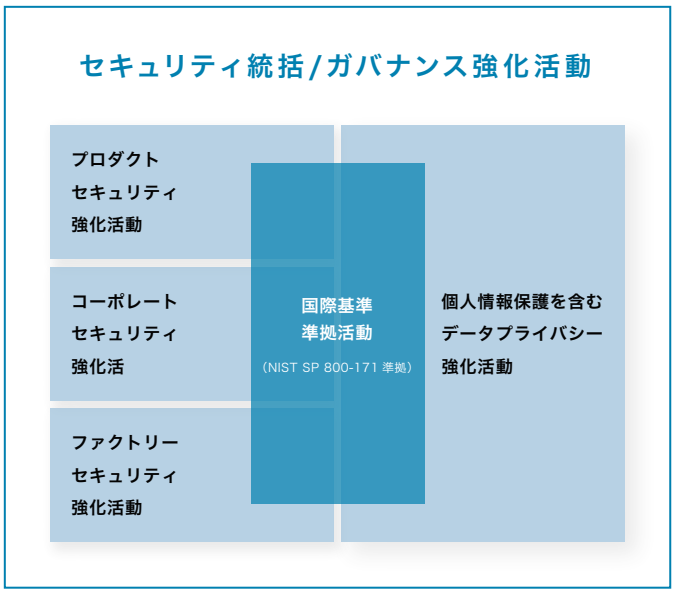
工場ネットワークOT（Operational Technology）を対象とするセキュリティ強化を推進しています。一般的に攻撃者は強度の低い箇所から侵入を試みるため、オフィスの IT と比較して強度の低い工場のセキュリティ強化は喫緊の課題です。 リコーグループでは、各工場が活動の主体となり、セルフアセスメントや第三者アセスメントによる状況把握、課題に対する対策強化活動を実施するとともに、組織によるガバナンスを強化する取り組みを継続的に実施しています。

●データプライバシーポリシー

デジタル化の進展やビッグデータの利活用の広がりを背景に、データプライバシーや個人情報を含むパーソナルデータの保護への関心が高まっています。一方、パーソナルデータの利活用におけるルールはまだ明確ではなく、その活用がどの程度であれば適正かの線引きはされていません。さらにお客様の視点では、自分のパーソナルデータが適正に取り扱われているかやプライバシーが保護されているかが不明確であることは、懸念材料となっています。 リコーグループは、個人情報保護法等の法令に則り、お客様のパーソナルデータ全般に対してデータプライバシーポリシーを定義して情報管理に取り組んでいます。さらに、データビジネス事業を本格始動させ、AI 活用による新たな価値を創出し、お客様の成長と課題の解決に貢献していきます。

国際的なセキュリティ基準準拠に向けて

サイバー攻撃の増加と高度化に伴い、その標的は業種を問わず、無差別かつあらゆる産業に拡大しています。リコーグループでは、お客様の情報資産を守ることを第一に配慮したセキュリティ活動を行い、国際的な基準・ガイドラインである、NIST SP 800-171 への準拠[2]を目指します。この活動は「コーポレート」「プロダクト」「ファクトリー」「データプライバシー」を包括したセキュリティ強化の一環です。
リコーグループの「製品・サービス」は、セキュアな「事業環境」を目指しているお客様、またNIST SP 800-171 に準拠した「事業環境」を目指しているお客様を想定し、NIST SP 800-171 に必要な機能を搭載した製品を提供していきます。　また、リコーグループの「事業環境」においても、お客様の守るべき情報資産を厳格に管理し、保護するため、NIST SP 800-171 に準拠した施策を継続的に行っていきます。 これらセキュリティ強化への取り組みは、リコーグループの「製品・サービス」の導入を検討されるお客様のセキュリティニーズに対応、情報資産を守ることに貢献し、お客様のビジネスリスクを低減します。



詳しくはWEBへ

[1]仕事のAI
[2]NIST SP 800-171 準拠活動への取り組み

目次

基本情報

本報告書の目的

本報告書は、ステークホルダーの皆様に向けてリコーグループの
情報セキュリティに関する活動を解説することを目的としております。

報告対象期間

2021/7/1~2023/9/30

報告範囲

リコーグループの情報セキュリティの取り組みについて

お問い合わせ先

株式会社リコー

セキュリティ統括センター
〒143-8555　東京都大田区中馬込1-3-6
Tel: 03-3777-8111（代表）

1　はじめに

1-1　取り組みの背景、重要性

2020年にリコーは「デジタルサービスの会社への変革」を宣言しました。ワークプレイス（オフィス／現場＋ホーム）のITインフラを構築し、ワークフローをデジタル化してつなぎ、新しい働き方をサポートします。デジタルサービスの会社として、国や地域、業種など、お客様ごとに異なる課題をくみ上げ、リコーの技術力とデジタルの力を掛け合わせて、それぞれのお客様に最適な解決策を提供することで、はたらく人の創造力を支え、ワークプレイスを変えていきます。

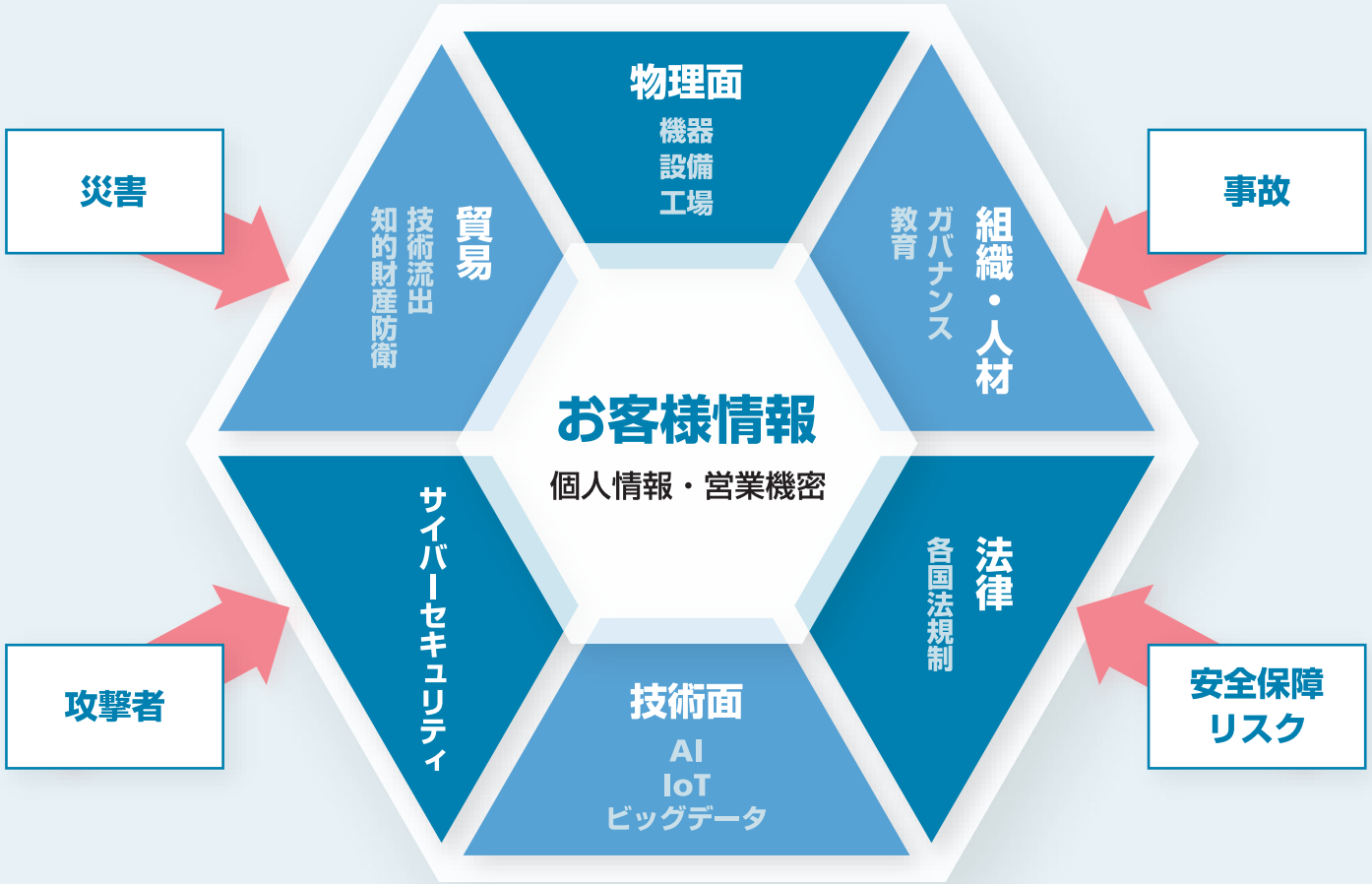
デジタル化されたワークフローではお客様情報[1]のデジタルデータをさまざまな形で利活用させていただき価値を提供していきますが、その過程で重要になるのはこのお客様情報を安心・安全に守ることです。紙媒体などアナログデータとは異なりデジタルデータはオリジナルをコピーすることが容易なため、安心・安全を担保するために関与する範囲がデジタルサービスのワークフロー処理過程にとどまらず、ワークフローを実施する環境、商品・サービスを製造・開発する現場の環境、製造に必要な部品調達などのサプライチェーン、関連企業、業界、地域、国家までにも広がっており、サービスの高度化・複雑化により更なる広がりを見せています。

ランサムウェアやマルウェアなどを用いた悪意ある攻撃者との攻防は後を絶ちません。国際的セキュリティ標準活動にみられるように、1企業にとどまらず、国家レベルで連携することで一定水準以上のセキュリティを維持していくことが重要となります。

そのためには、攻撃者との攻防にみられるサイバーセキュリティのみならず、個人情報の保護や各国法規制・貿易などの分野と連携して進めていく必要があります。

リコーでは「お客様情報を脅威から安心・安全に守る」ために必要な活動範囲を「情報セキュリティ」と捉え、さまざまな施策を実施しております。本報告書ではリコーの情報セキュリティをご紹介いたします。

[1] お客様情報とは、リコーの製品・サービスが収集するお客様の個人情報、お客様の秘密情報、お客様環境に設置している製品の動作情報、お客様の問い合わせ情報などを指します。



1　はじめに

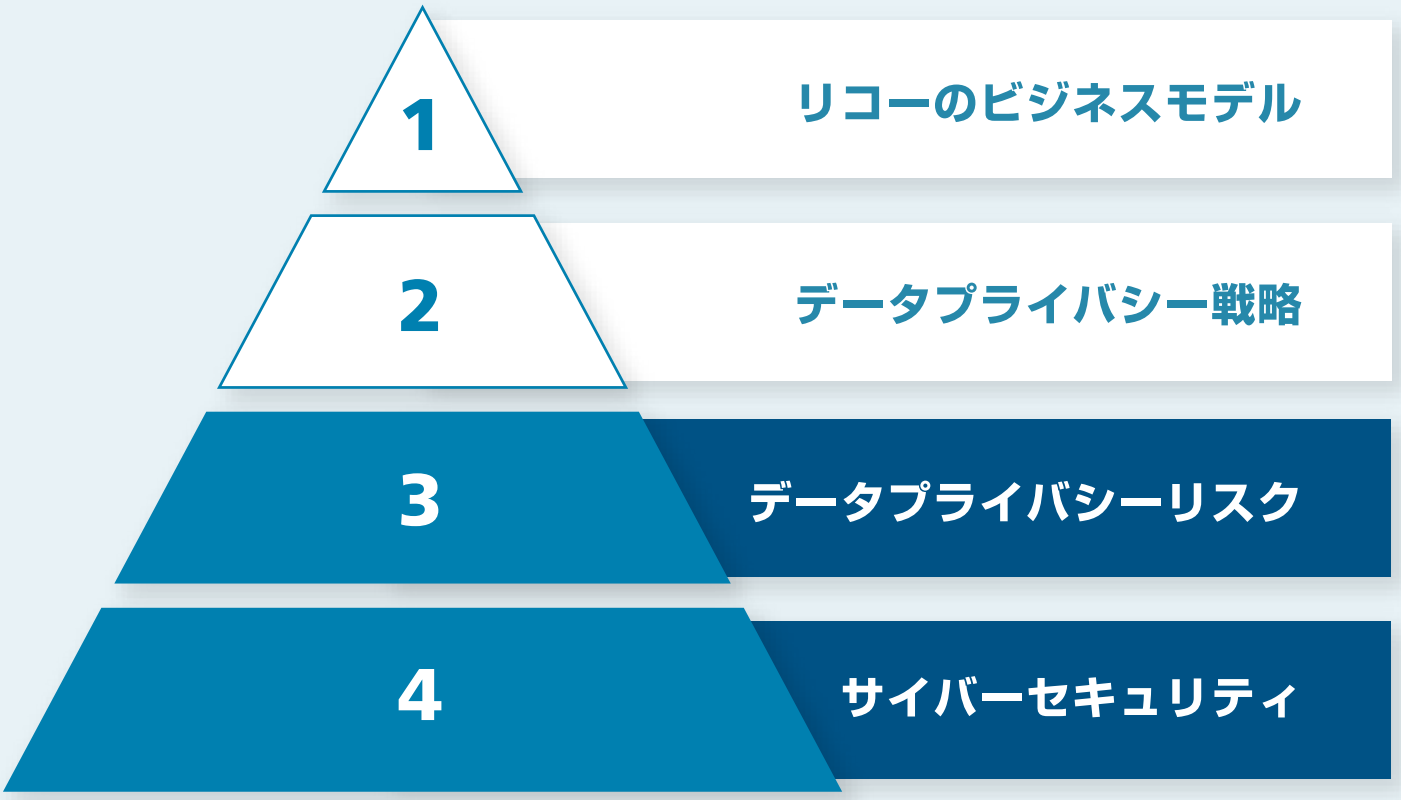
1-2　経営における情報セキュリティの位置づけ

リコーグループ経営会議のグループマネジメントコミッティ（以下、GMC）とリスクマネジメント委員会は、経営理念や事業目的などに照らし、利害関係者への影響を含めて、経営に大きな影響を及ぼすリスクを網羅的に識別した上で、“重点経営リスク”を決定し、その対応活動に積極的に関与しております。

リコーグループでは、情報セキュリティに関して各国、国策レベルで対策が求められてきている中、変化し続ける情報セキュリティ情勢を常に把握した上で、グローバルに活動拠点のある当社グループにとって適切な対策を検討・推進していくことを、“重点経営リスク”の中でも最重要課題の一つと位置づけております。

国際社会の動向や持続可能な開発目標（SDGs）、ステークホルダーからの期待、リコーの経営理念、中期経営計画、社外有識者の意見を踏まえてマテリアリティを特定し、定期的に見直しをかけています。「事業を通じた社会課題解決」とそれを支える「経営基盤の強化」の２つの領域で７つのマテリアリティを特定するとともに、各マテリアリティに紐づく17のESG目標を設定しています。目標の１つであるステークホルダーエンゲージメントでは、国際的セキュリティ標準に基づくセキュリティ強化を掲げております。

リコーの情報セキュリティは、ワークフローやデータプライバシーなど多岐に済当社のデジタルサービスの活動を支え（下図③④）、価値創造プロセス（下図①②）を実施するために必要とされる活動と位置づけています。



2　リコーの情報セキュリティの取り組み

2-1　情報セキュリティに関する考え

リコーグループは経営理念の中に『人と情報のかかわりの中で、世の中の役に立つ新しい価値を生み出し、提供しつづける』という私たちの使命を掲げています。企業市民として社会的責任を果たすことを経営の基本と認識し、経済的価値の創出と社会的責任の達成を同時に実現することで企業価値の向上を目指しています。

デジタルサービスを事業領域とするリコーグループにとって、情報セキュリティへの取り組みはお客様に安心してご利用いただける商品・サービスを提供していくための不可欠の要素と認識しています。

この考えに基づき、「リコーグループ情報セキュリティ基本方針」および「商品・サービスの情報セキュリティ基本方針」を定め、内外に周知するとともに、国際的なセキュリティ標準に基づき、情報セキュリティに関わる取り組みを強化しています。これらの取り組みをリコーに所属する役員・従業員含む全員参加の活動と位置付け、現場・第一線での日々の管理と継続的改善を進めるとともに、それらを基盤としてリコーの製品・サービスをお客様へ提供します。

2-2　情報セキュリティの基本方針/基本ポリシー

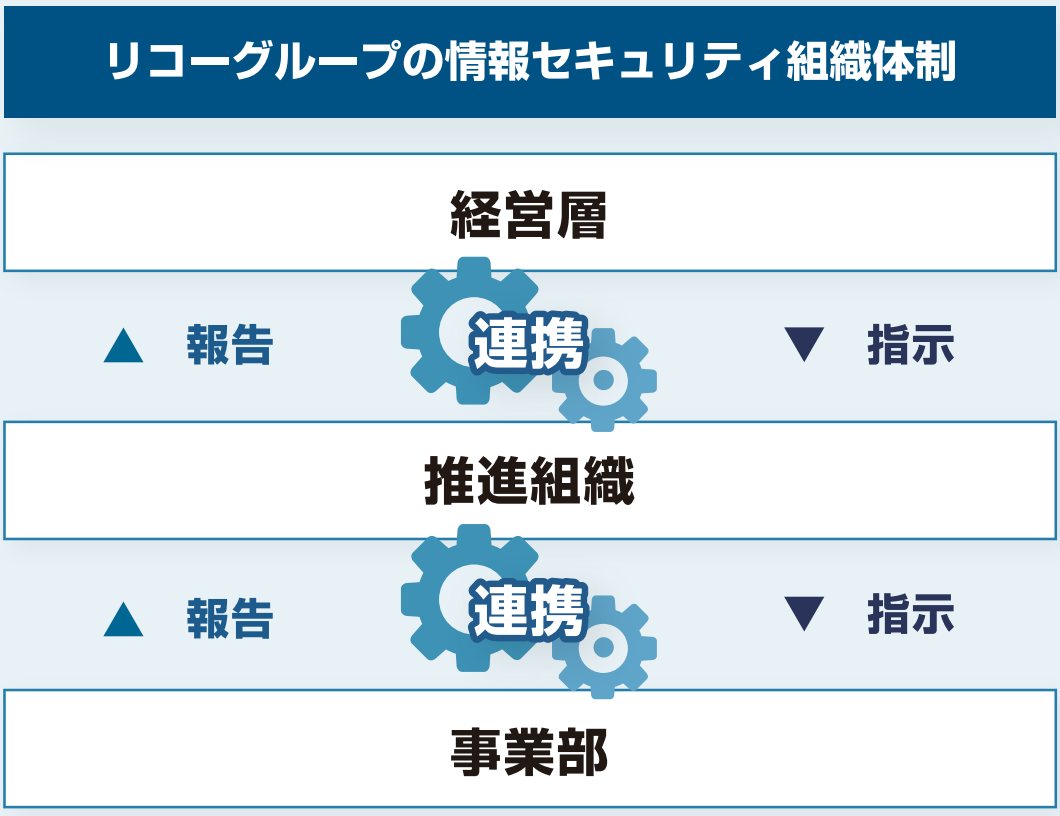
継続的に成長する企業価値向上のため、リコーグループとしてお客様への安心・安全な製品/サービスの提供のため、および、自社の事業基盤のための情報セキュリティに関する/方針/ポリシーを策定しております。

- 商品・サービスの情報セキュリティ
- リコーグループ情報セキュリティ基本方針
- リコーグループデータプライバシーポリシー
- リコーグループAI活用基本方針

2-3　情報セキュリティの体制/組織

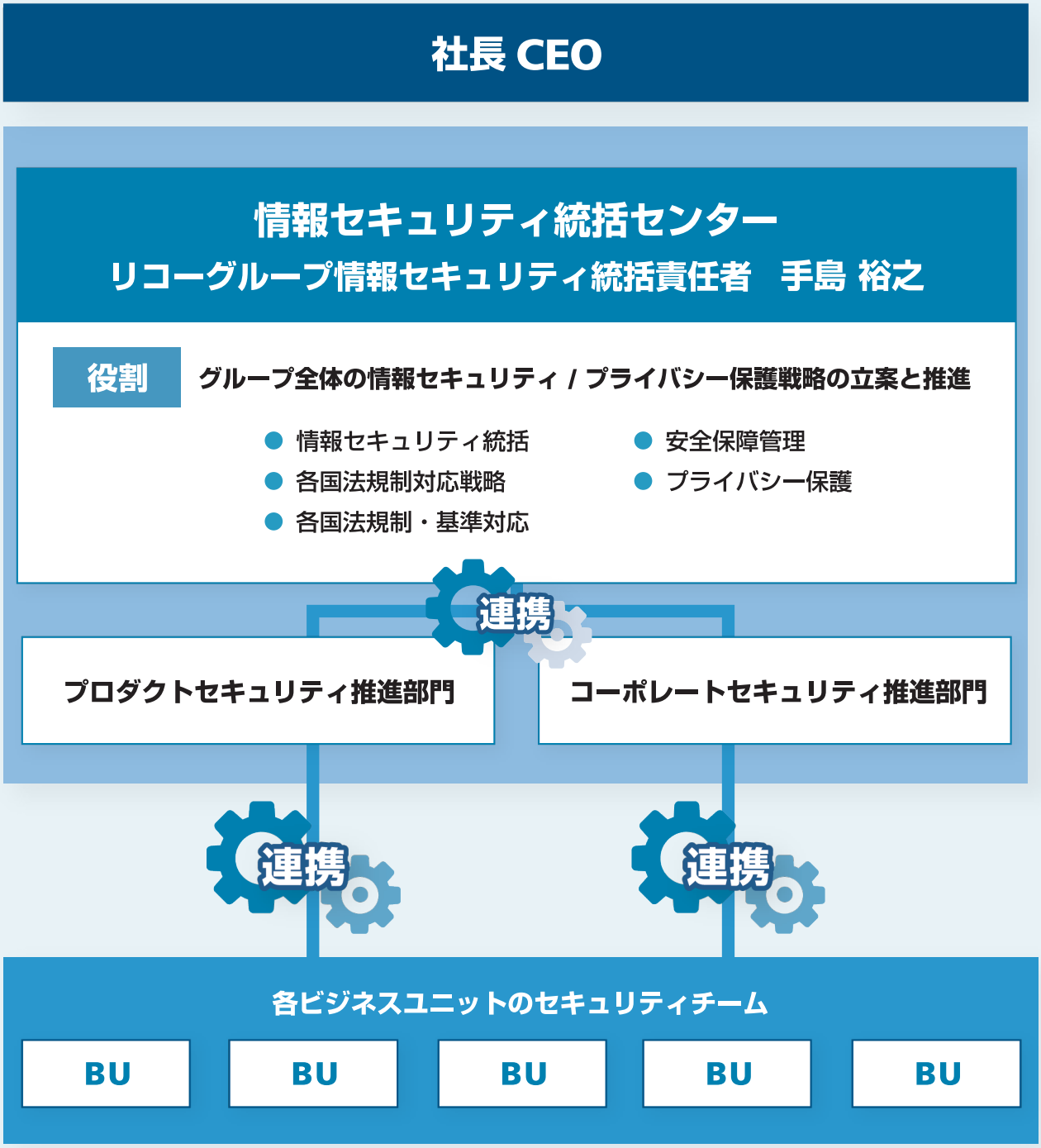
企業を取り巻く環境が複雑かつ多様化する中、リコーグループでは「リスクマネジメント」を事業に関する社内外の様々な不確実性を適切に管理し、経営戦略や事業目的を遂行していく上で不可欠のものと位置づけています。

リスクマネジメント項目の中でも情報セキュリティは重点経営リスク管理項目の1つに位置づけられ、統括責任者が評価者として取り組み状況の確認を行っています。経営層・推進組織・事業部に所属するリコーグループの全員が継続的な情報セキュリティ強化に向けて取組んでいます。



2-3 情報セキュリティの体制/組織

また、CEOの直轄に、グループ全体の情報セキュリティの戦略の立案・推進およびプライバシー保護に戦略の立案・推進を担う「情報セキュリティ統括センター」を設置しています。情報セキュリティ統括センターでは、製品のセキュリティを担うプロダクトセキュリティ推進部門と事業全体の情報セキュリティを担うコーポレートセキュリティ推進部門や、各ビジネスユニットに設置されたセキュリティチームと連携しながら、グループ全体の活動の強化に取り組んでいます。



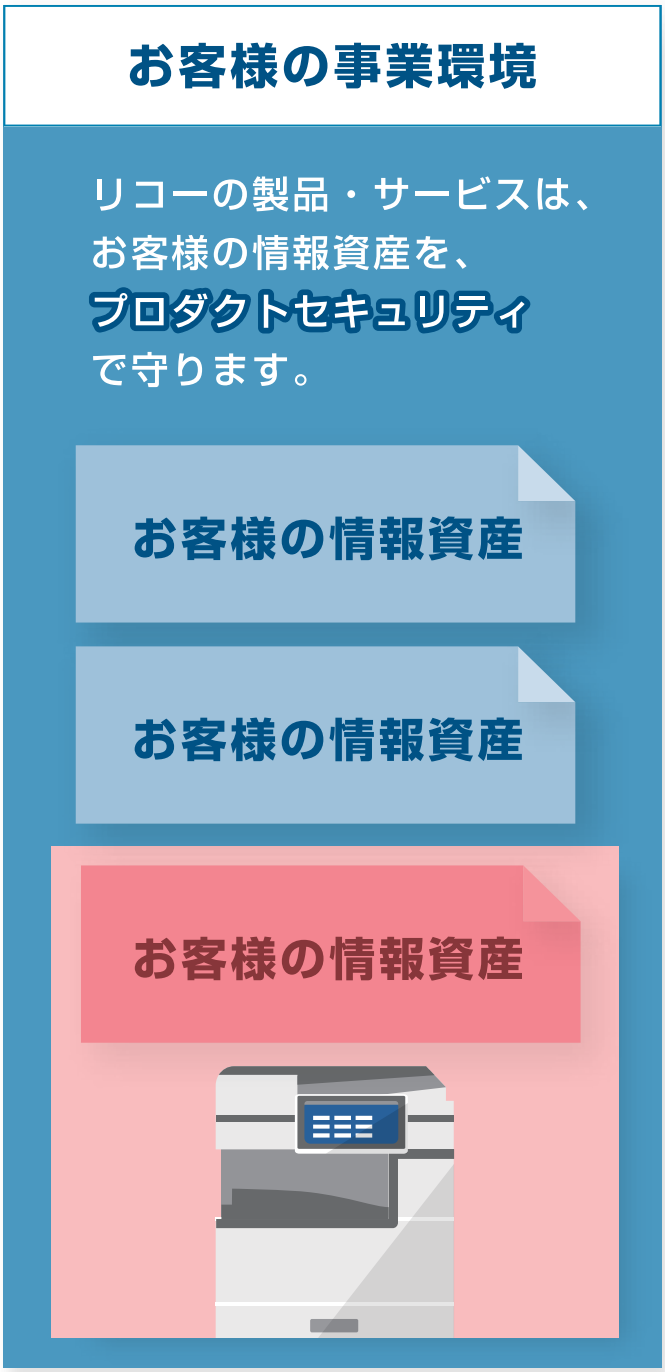
仕事のAI

2-4　情報セキュリティの適用範囲

適用範囲は大きく2つあります。「製品・サービス」と「事業環境」。

1-1で記載の通り、お客様からお預かりするお客様情報の安心・安全を守るためには、ご利用いただく製品・サービスが堅牢なものであることはもとより、それらを開発・生産するメーカーであるリコーの事業環境そのものも堅牢でなければなりません。事業環境には、商品の企画から販売・保守に至るバリューチェーン、各過程で用いられる情報管理システムや、生産/開発/販売システム、それらの運用ルール/プロセスが含まれています。近年、製品・サービスへの直接的な攻撃だけではなく、この事業環境を対象としたサイバーセキュリティリスクが増加しています。

本書では、製品・サービスで取り扱うお客様情報を攻撃者から守る活動を「プロダクトセキュリティ」、当社事業環境の中で取り扱うお客様情報を攻撃者から守る活動を「コーポレートセキュリティ」と呼びます。



2　リコーの情報セキュリティの取り組み

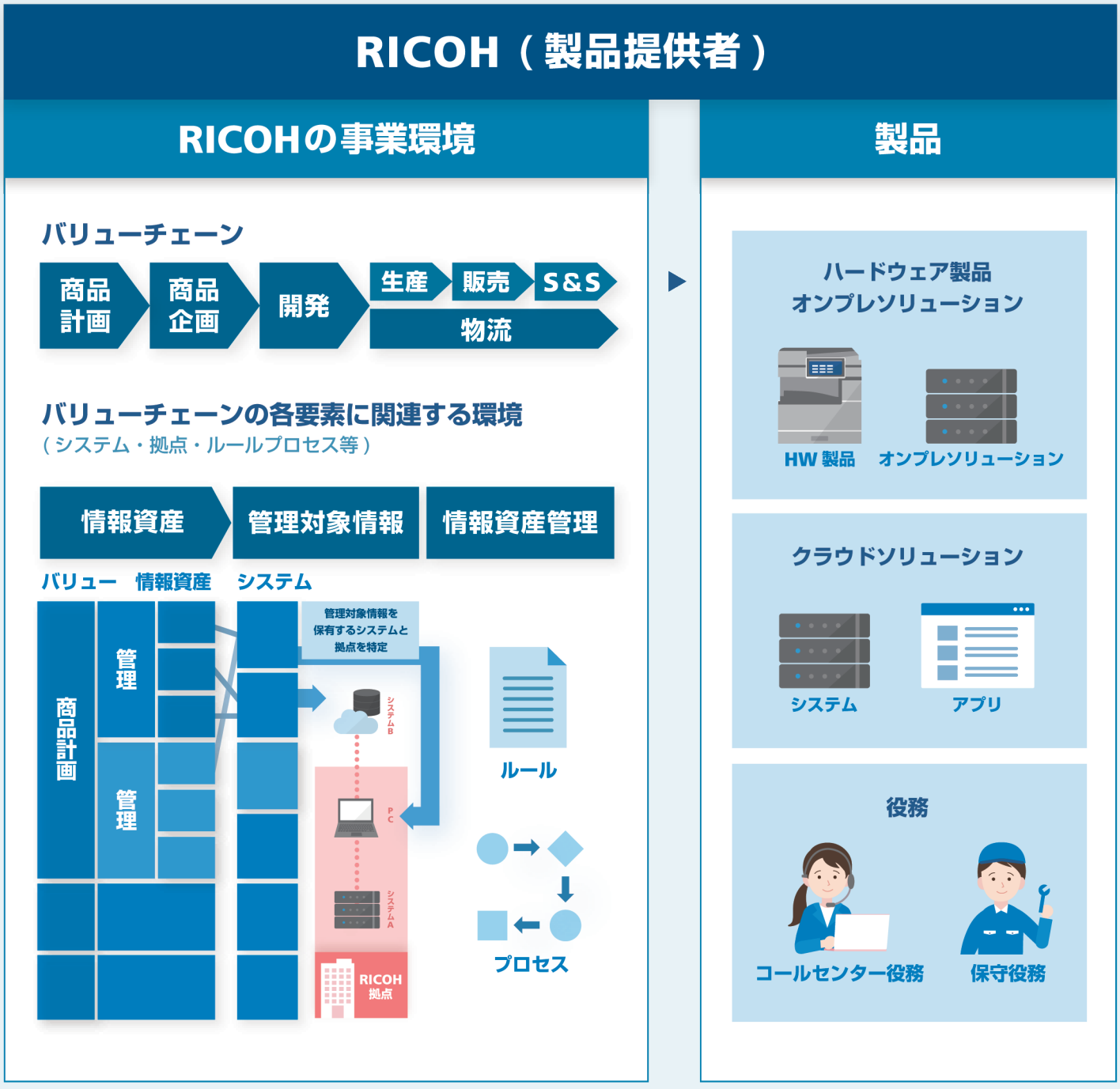
2-4　情報セキュリティの適用範囲

国際的な情報セキュリティ標準（ISO/IEC（*1）、NIST（*2）など）に基づき、当社グループのサプライチェーン全体の情報セキュリティを意識した体制を構築/強化するとともに、企画・設計・購買・生産・販売・サポートの各過程の業務システムに関わるセキュリティリスクを適宜想定し、継続的に対策検討及び実施を行っております。

「製品・サービス」の情報セキュリティ活動であるプロダクトセキュリティに関しては３章でご紹介いたします。

「事業環境」の情報セキュリティ活動であるコーポレートセキュリティに関しては４章でご紹介いたします。

*1 ISO/IEC：International Organization of Standardization/International Electrotechnical Commission　*2 NIST：National Institute of Standards and Technology



3　プロダクトセキュリティ

3-1　商品・サービスの情報セキュリティ基本方針

リコープロダクトのセキュリティ方針は、以下の通り、「商品・サービスの情報セキュリティ基本方針」として定め、リコーのホームページにも公開しております。

基本方針

リコーグループは、お客様の情報資産を守り、お客様が情報資産を最大限活用できるよう、お客様のワークプレイスや情報セキュリティポリシーと調和し、安心してご使用いただける商品・サービスを提供します。

基本原則

第１原則　法令遵守

法令遵守を基本とし、第２原則と第３原則に優先します。

第２原則　情報資産の保護

第１原則を満たすことを前提に、各商品・サービスでお客様の情報資産を保護し、第３原則に優先します。

第３原則　提供価値の最大化

第１原則、第２原則を満たすことを前提に、各商品・サービスによってお客様に提供する価値の最大化を図ります。
（ここでいう価値は、“ 商品 ” の価値全般であり、情報セキュリティに関するものに限定しません。）

行動指針

1　法令遵守

リコーグループは、商品・サービスを提供する各国の情報セキュリティに関係する法令や指針、契約上の義務を遵守します。

2　お客様起点

リコーグループは、お客様の情報セキュリティニーズを把握し、対応した商品・サービスを提供することに努めます。

3　環境変化の把握と対応

リコーグループは、情報セキュリティの環境変化を把握し、対応した商品・サービスを提供することに努めます。

4　情報セキュリティリスクへの対応

リコーグループは、商品・サービスの情報セキュリティリスクを定期的に分析し、低減することに努めます。

5　情報セキュリティマネジメント

リコーグループは、商品・サービスの情報セキュリティ体制を構築し、継続的な改善を行います。

6　お客様価値の最大化

リコーグループは、利便性と安全性を両立した商品・サービスを提供します。

2018年1月

株式会社リコー
代表取締役 社長執行役員
山下 良則

3-2　安心・安全な製品の追求

3-2-1　セキュリティ・バイ・デザイン

お客様に安心して製品やサービスを利用していただくために、情報セキュリティを企画・設計段階から確保するセキュリティ・バイ・デザインの実践に取り組んでいます。セキュア開発の国際標準ISO/IEC27034-1 に基づく社内規定を制定し、順次適用を進めています。

3-2-2　セキュリティリスクへの注意喚起

情報化社会の発展と共に、コンピュータウィルスや個人情報の漏えい、外部からの不正アクセスなど様々な脅威が我々の周りを取り囲んでいます。多様化する脅威に対し、お客様にとってセキュリティ対策の取り組みが、最も重要な課題のひとつとして取り上げられています。

このようなセキュリティの脅威は、パソコンやサーバー、ネットワークに限られた話ではありません。当社の製品・サービスについても、適切な設定・運用をすることによりセキュリティの脅威を軽減することが可能です。

当社の製品・サービスをより安全にご利用いただくために、いくつかのご対応を推奨しております。

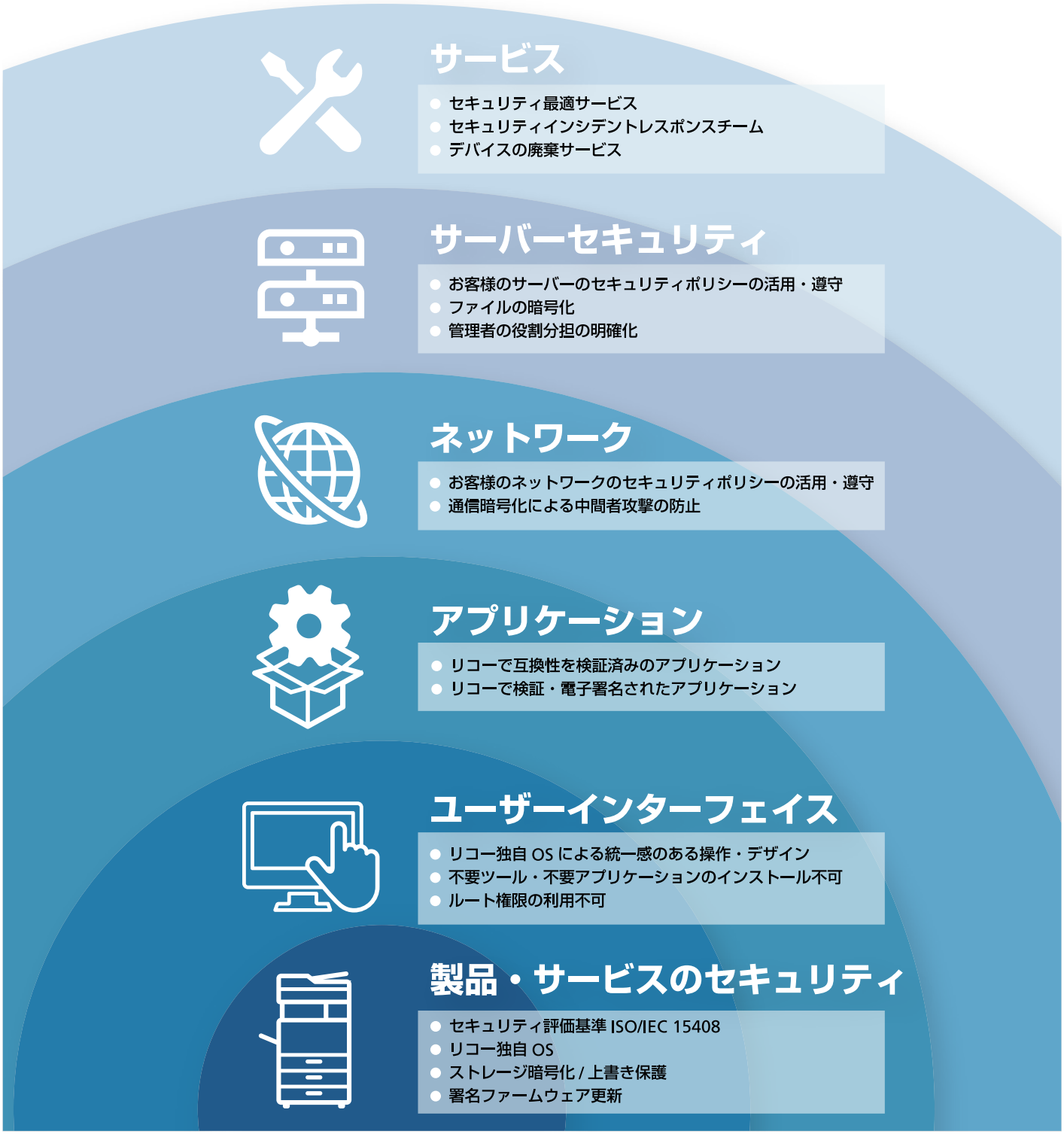
詳しくは https://jp.ricoh.com/security/products/ を参照ください。

加えて、サイバー攻撃リスクの高い脆弱性に対する対応状況・注意喚起、セキュリティ研究者からの脆弱性報告の受付窓口の設置、脆弱性対策情報の提供など、脆弱性対策の国際標準であるISO/IEC29147/30111に基づく脆弱性への早期対応にも取り組んでいます。

3-3 リコーのセキュリティレイヤーアプローチ

当社のセキュリティモデルの中心にあるのは、お客様にご利用いただく製品やサービスそのものです。製品やサービスのセキュリティを確保するにあたり、オペレーティングシステム、ユーザーインターフェース、アプリケーション、ネットワーク、サーバー、保守・サービスなど、取り巻くテクノロジーすべてのレイヤーに対してセキュリティの配慮を行っております。

当社の製品・サービスは、セキュリティに関する様々な脅威からお客様データを保護するために、常に最新の国際セキュリティ標準を参照し、暗号化・OSS脆弱性管理・データ権限管理・セキュア開発プロセス等様々な技術動向に追従します。



4　コーポレートセキュリティ

リコーグループでは、2007年3月に共通基準を策定し、2007年4月から本格的にグループ各社への共通基準の展開・定着を推進しています。この共通基準により、各社の情報セキュリティ対応レベルの継続的向上を図り、お客様に新しい価値を提供するためのさらなる基盤強化を目指しています。

リコーグループが、情報セキュリティへの取り組みを通じて企業の社会的責任を果たし、企業価値の向上を図るためには、グループ会社間の垣根を越え、各社の情報セキュリティを一定以上に引き上げるセキュリティレベルの「共通化」が重要です。同じグループ会社といえども、規模や企業文化にはさまざまな違いがあり、その業務も、会社によって研究・開発・設計・生産・販売・サービス等多岐にわたります。また、個別に取り組む情報セキュリティのレベルにも差が生まれがちです。

リコーグループでは、こうしたさまざまな問題を解決し、情報セキュリティ活動の基盤となるグループISMS（Information Security Management System）をさらに有効なものにするためには、グループ全体の統一したセキュリティポリシーとなる共通基準が必要であると考えました。また、国際規格ISO/IEC27001では、個別の安全対策についてどこまで実施すべきかまでは規定していないため、具体的な実施基準が必要でした。そこで、この国際規格の要求に合わせ、リスクの大きさに応じた実施基準の検討を2005年12月から始め、2007年3月に「リコーグループ共通基準」として策定し、2007年4月から本格的にグループ会社への展開・定着を推進しています。

詳しくは https://jp.ricoh.com/security/management/activity/standard.html を参照ください。

また、近年サイバー攻撃手法がますます複雑化・巧妙化しており、『未然防止』に重点を置いたISMSの考え方だけでは対応が困難になっています。

このような状況より、攻撃 / 侵入を前提とした『早期発見・迅速対応』にも重点を置いた米国国立標準技術研究所（NIST）より発行されたCSF（Cyber Security Framework）の考え方や、刻一刻と変化する攻撃の即応性に優れた手法である“OODA”を採用してサイバーセキュリティ対応を実施しています。

4　コーポレートセキュリティ

4-1　リコーのコーポレートセキュリティ戦略

ランサムウェアなど企業を標的としたサイバー攻撃が複雑化・巧妙化する中、
リコーは戦略的かつグローバルでサイバーセキュリティ対策を推進しています。

セキュリティ戦略

対策状況の可視化と計画
(NIST CSF対応、リスクベース計画)

昨今、世間を騒がせているランサムウェアなどのサイバー攻撃などの脅威に対し、『未然防止』に重点を置いた従来の ISMS の情報セキュリティ対策のための要求事項(以下、要求事項)への対応だけでは対策が不十分となっています。

このような背景を受け、サイバーセキュリティ対策を改善するためのフレームワーク(CSF)の要求事項も参照し、セキュリティ脅威に対する対応状況のヒートマップによる可視化及び、アセスメント、セキュリティ強化のためのリスクベースの計画を策定し、実施しています。

OODA 採用

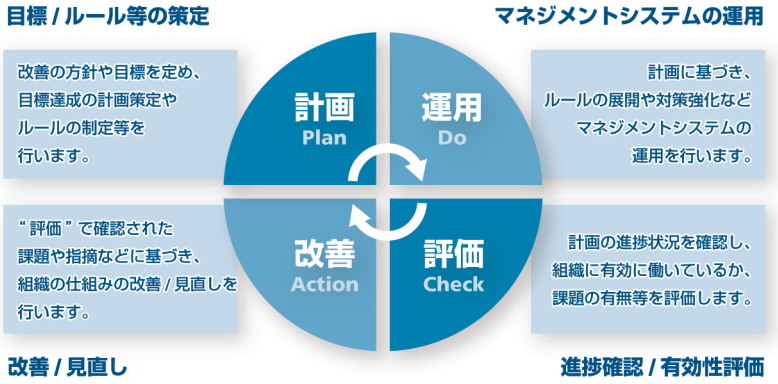
ISMS 活動では PDCA サイクルを回すことでセキュリティレベルの向上を図っていました。
“PDCA” は明確な目的を達成するための活動を行うことに適した手法です。

一方で、サイバー攻撃のようなコントロール不可能な外部要因が多い事象への対応には適していません。

そこで、刻一刻と状況が変化するサイバー攻撃などの事象への即応性に優れた手法である“OODA” を併用することで、目的達成のための活動（PDCA）と状況が変化する事象に対応するための活動（OODA）を適宜使い分けてセキュリティ管理態勢の強化を図っています。

特定・防御（ ISMS活動 ）

組織にとって重要な情報資産を守るために、組織内外の状況把握、確認された課題解決の優先順位付け、課題解決するための計画策定 / 実行、このサイクルを継続することで、情報セキュリティ対策レベルの向上を図ります。

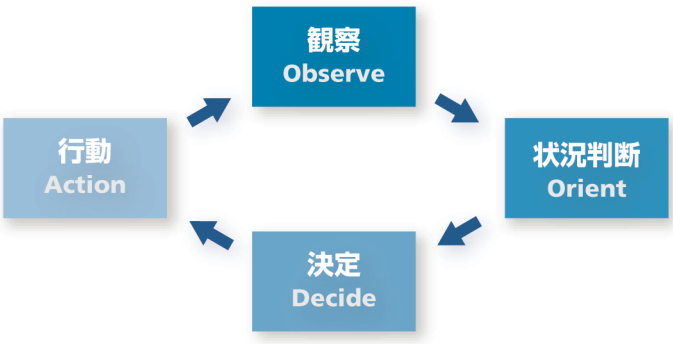


検知・対応・復旧（ サイバー攻撃対応活動 ）

サイバー攻撃の領域においては、SOC※1/CSIRT※2 体制をグローバル各地域毎に設定し、適時状況を監視 / 判断し、適切な決定のもと迅速に行動 / 対応を行い、影響を最小限に抑える。

※1 **SOC** : Security Operation Center
※2 **CSIRT** : Computer Security Incident Response Team

運用の１つであるサイバー攻撃対応活動では、刻一刻と変化する攻撃の状況に合わせた対応が求められるため、即応対に優れた手法である“OODA” を採用します。



4　コーポレートセキュリティ

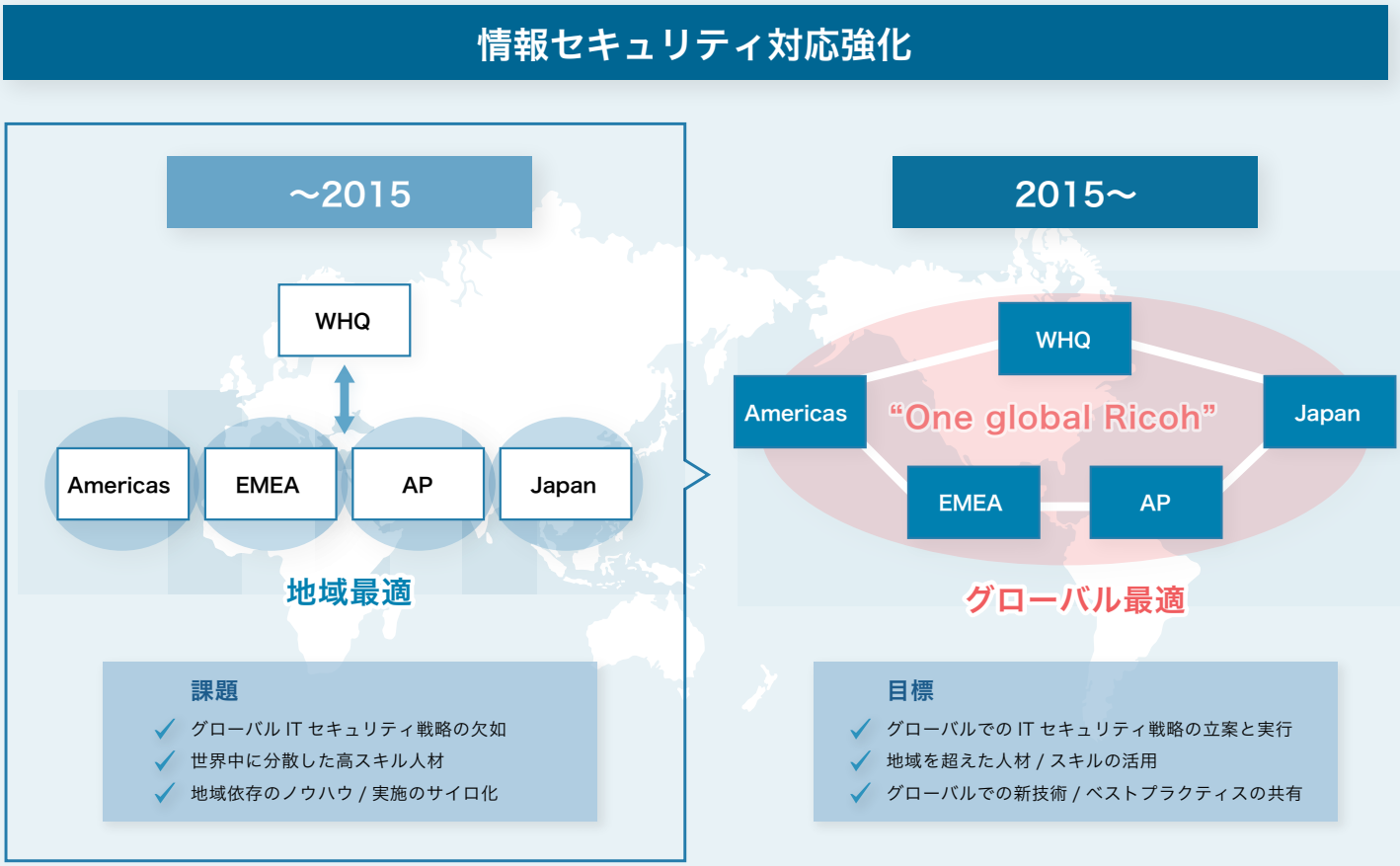
4-1　リコーのコーポレートセキュリティ戦略

グローバルな事業展開を行うリコーでは、セキュリティ対策においてもグローバルに一貫性のある対応が必要と考えています。リコーでは、グローバルでのセキュリティ強度の均質な向上、グローバルでのセキュリティ担当者間の連携加速を目的とし、VOIT（Virtual One IT）を2015年より組織し、活動を続けてきました。

VOITの狙い

- グローバルの情報セキュリティとリスク管理プログラムの推進
- グループ情報セキュリティポリシー、スタンダード、プロシージャの制定
- グローバルレベルのセキュリティアウェアネス向上
- グローバル横断のセキュリティ実装計画のレビュー
- 確認された脆弱性に関する情報共有／相互対応支援

VOIT体制図



4　コーポレートセキュリティ

4-2　セキュリティインシデント対応強化

昨今のサイバー攻撃に迅速に対応できるように、CSIRT/SOC 体制を構築し日々強化に取り組んでいます。

CSIRTの設置と運用

2013 年度より RICOH-CSIRT（Computer Security Incident Response Team）を組織し、SOC（Security Operation Center）からのインシデント報告、社外CSIRT組織からの情報、セキュリティ情報サイトからの情報をもとに脅威を分析しています。さらに特定された脅威に対して迅速かつ最適な対応（証拠保全、攻撃解析、原因究明、拡散防止、事態収束）を主導してします。

SOCの設置と運用

SOC（Security Operation Center）を組織し、リコーグループの保有する IT システムを常に監視し、不審な事象の詳細な内容分析を実施しています。これにより、外部からの不正侵入、内部からの不正利用をいち早く検知、必要に応じて対応チームに連携することによりインシデントの早期発見を実現しています。

社外セキュリティエキスパートの活用

サイバー攻撃の高度化複雑化が著しい今日では、セキュリティ対応のすべてを社内で完結することは困難となっています。そこでリコーでは、セキュリティエキスパートのパートナーによる MSS（Managed Security Service）の導入や各種セキュリティ団体と連携を図り、常に最先端のセキュリティ技術を活用しています。

4-3　セキュリティ教育

情報資産を脅威から守るためには、ルールの制定・周知やシステムの導入だけでなく、従業員一人ひとりのセキュリティに対して高い意識とスキルを持つことが必要不可欠です。リコーでは、定期的なセキュリティ教育、啓蒙活動を実施、人財を育成しています。

セキュリティ教育

移動中やリモート業務での注意点、クラウドサービスの利用方法、ウィルス対策等、日常の業務の中で注意すべきセキュリティリスクに対する意識の向上と、その正しい対応方法について理解し、セキュリティを保った業務遂行ができるよう教育を進めています。

標的型攻撃メール訓練

標的型攻撃メール訓練サイバー攻撃が疑われる不正なメールの見分け方や、受信した場合の対処方法を周知するとともに、サイバー攻撃を模したメールの受信と対処を体験させ、実際の攻撃メールによる被害の抑止を図っています。

インシデント対応机上訓練

サイバー攻撃の脅威に対しては被害が発生しないように防止するだけでなく、万が一発生しても被害拡大を防止、早い復旧を行えるようにすることも重要です。そのために、定期的にサイバー攻撃の発生を想定した模擬訓練を実施しています。

セキュリティ通信

サイバーセキュリティでは従業員の基礎的な知識だけでなく、常に最新の動向を把握することも大切です。そのために全社従業員向けに定期的にセキュリティ動向やそれを受けた社内セキュリティの対応を「セキュリティ通信」として情報発信・共有しています。

5　データプライバシー

デジタル化の急速な進展やビッグデータ利活用を背景として、データプライバシーや個人情報保護への関心は、グローバル規模で日々高まってきています。GDPR をはじめとするデータプライバシーに関する各国の法規制対応は、企業の競争力を維持するうえで優先的な課題の一つです。

我が国における個人情報保護は、2005 年の個人情報保護法施行以来、技術の発展や、ビジネスのグローバル化などの社会状況の変化によって、改正法が施行されてきました。

リコーでは、デジタルサービスの会社への変革を進め、2021 年に独自の自然言語処理 AI（人工知能）などを活用して業務支援を図る新サービス「仕事の AI」シリーズをリリースして、データビジネス事業を本格始動いたしました。

一方、パーソナルデータの利活用におけるルールがまだ明確ではないことや、企業にとってのパーソナルデータの活用が、どの程度であれば適正であるのか判断するのが困難であることがあげられます。さらにお客様の観点からは、自分のパーソナルデータが適正に取り扱われていて、プライバシーもしっかりと保護されているのかどうか不明確であることも懸念材料の一つとなっております。

このためリコーではお客様からの情報に関する法令全般を遵守することを目的に、お客様の個人情報を含むパーソナルデータ全般に対してデータプライバシーポリシーを定義して情報の管理を行っております。

5-1　個人情報保護について

リコーグループは、グローバル情報社会における個人情報[2]（個人番号および特定個人情報を含む）の有用性と、個人の権利利益の保護の重要性を認識し、業務上取り扱うすべての個人情報が適正かつ効果的に活用されるよう、関係法令およびその他規範を遵守いたします。

また、リコーグループでは、2005 年の個人情報保護法施行以後、個人情報保護に関する国際的な動向にも配慮した自主規程の策定ならびに運用・管理を行い、これらを全従業者およびその他関係者に周知徹底するとともに、継続的に維持改善しており、2022 年 4 月施行の改正法にも対応を行っております。

リスクマネジメント項目の中でも情報セキュリティは重点経営リスク管理項目の 1 つに位置づけられ、統括責任者が評価者として取り組み状況の確認を行っています。経営層・推進組織・事業部に所属するリコーグループの全員が継続的な情報セキュリティ強化に向けて取り組んでいます。

[2]個人情報とは個人を識別できる情報です。※パーソナルデータとは個人が識別できるかどうかによらない、個人に関する情報全般をさす名称です。

5-2　リコーグループのデータプライバシーポリシーについて

リコーグループでは、目指すべき持続可能な社会の姿を、経済（Prosperity）、社会（People）、地球環境（Planet）の 3 つの P のバランスが保たれている社会「Three Ps Balance」として表しています。この目指すべき社会の実現に向け、社会課題解決と社会貢献に取り組んでいます。上記の取り組みに則り、以下の基本方針のもと、お客様情報、すなわち、リコーの製品・サービスが収集するお客様の個人情報、お客様の秘密情報、お客様環境に設置している製品の動作情報、お客様の問い合わせ情報などを適法に、またお客様指示のもとに扱うことで、人々の生活のあらゆるシーンに効率性と利便性を提供するだけでなく、人々に歓びを提供することに努めます。

1　個人情報についての基本方針

リコーグループは、個人情報保護基本方針に基づき、関係法令およびその他規範を遵守いたします。また、リコーグループ各社では、個人情報保護基本方針に加え、各事業に適した個別の個人情報保護方針を提示し、その方針に従い商品・サービスを展開する場合があります。

2　プライバシーおよびセキュリティ

リコーグループは、当社の個人情報保護基本方針に従って、お客様情報を適切に取り扱うとともに、お客様情報を保護するために、適切な安全管理策を施します。さらに、リコーグループ情報セキュリティ基本方針及び商品・サービスの情報セキュリティ基本方針に基づき、収集されたコンテンツの機密性、完全性および可用性が確保されるよう努めます。

3　リコーグループが取り扱う情報について

リコーグループは、当社の製品・サービスの提供、製品・サービスの質向上、新しい製品・サービスの検討のために、お客様情報を取り扱います。

4　透明性と説明責任

お客様情報の活用について、その適切性の担保に努めるとともに、用途や状況に応じた説明を行います。

5　データプライバシー

5-3　リコーグループのAI活用基本方針

リコーグループは、創業者・市村清による「人を愛し、国を愛し、勤めを愛す」という創業の精神（三愛精神）を企業活動の原点に据え、「世の中の役に立つ新しい価値を生み出し、生活の質の向上と持続可能な社会づくりに責任を果たす」ことを使命としています。

この使命に則り、以下の基本方針のもと、これまでに培ってきた先端技術と AI を融合して活用することで、人々の生活のあらゆるシーンに効率性と利便性を提供するだけでなく、人々に歓びを提供することに努めます。

1　個人情報についての基本方針

リコーグループでは、人権方針に基づき、AIを活用してまいります。

2　データプライバシーポリシー

リコーグループでは、データプライバシーポリシーに基づき、データを取り扱います。

3　公平性

リコーグループは、AI の活用において、判断結果に偏りが生じる可能性を認識し、そのような偏りが生じないよう、努めてまいります。

4　新しい価値の創出

リコーグループは、お客様に寄り添い、信頼を得ながら、AI 活用による新たな価値を創出し、お客様の成長と課題の解決に貢献していきます。

6　おわりに

セキュリティブランドの確立を目指して

世界的なサイバー攻撃の増加による情報保護のニーズの高まりはいまや普遍なものであり常識となりつつあります。攻撃者とのいたちごっこはこれからも続き、今後もそれが緩むことはないでしょう。リコーグループは、各業界、国を挙げてのセキュリティ水準強化などの外部環境の変化を常に注視しながら、デジタルサービス会社として柔軟に対応できるよう、継続的にセキュリティの取り組みを強化・改善し、それを実現するための情報セキュリティ体制の強化を継続的に実施していきます。

RICOH
imagine. change.

株式会社 リコー
東京都大田区中馬込1-3-6 〒143-8555

http://jp.ricoh.com/

●お問い合わせ・ご用命は・・・

2023年3月発行