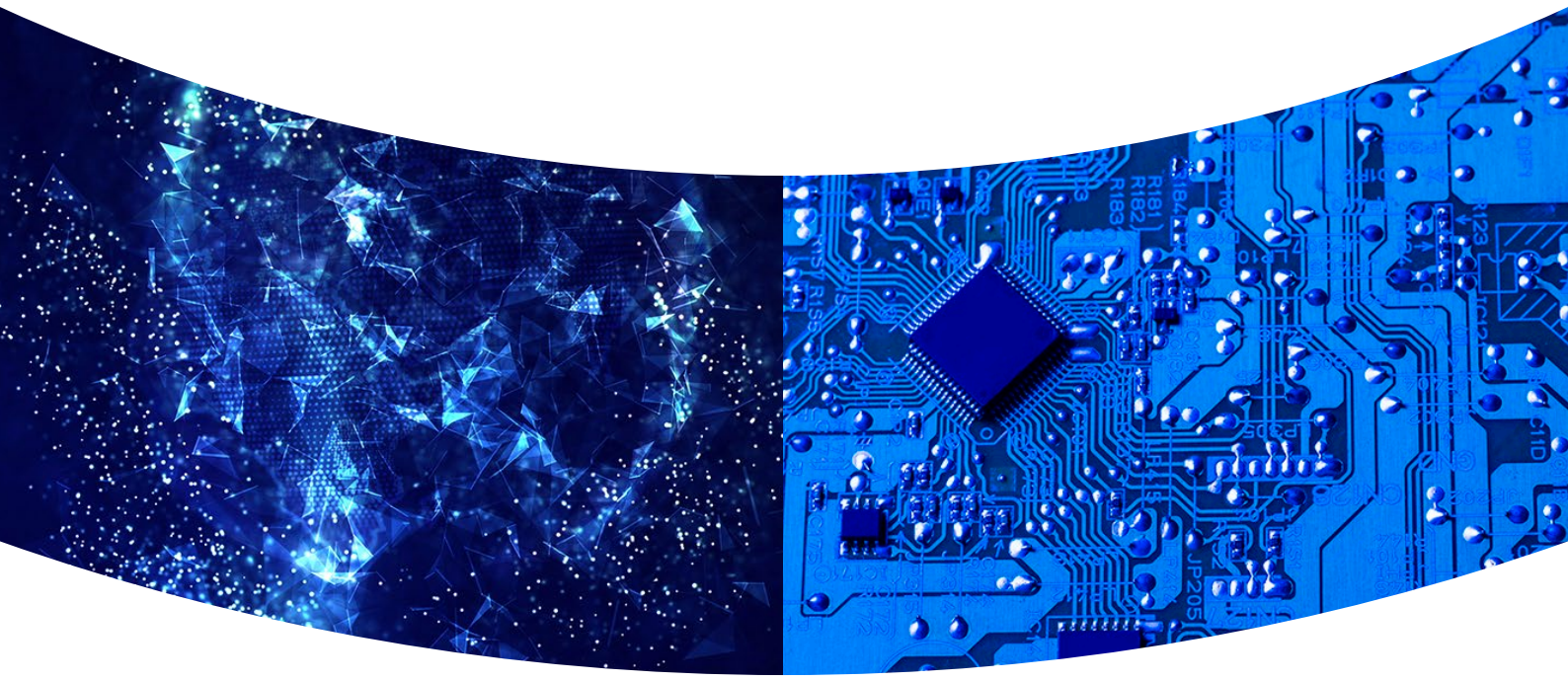
Panasonic
CONNECT

情報セキュリティ報告書



パナソニック コネクト株式会社

CONTENTS

発行について

パナソニック コネクト株式会社は、企業としての存在意義であるパーパスを、「現場から　社会を動かし　未来へつなぐ」と掲げています。
この想いの実現のために、日々取り組んでいる情報セキュリティへの取り組みについてステークホルダーの皆様に報告することを目的としています。

報告内容

範囲　主に、2022年度のパナソニック コネクト株式会社の情報セキュリティへの取り組みについて

お問い合わせ先

〒104-0061
東京都中央区銀座８丁目２１番１号
汐留浜離宮ビル

IT・デジタル推進本部
サービスデリバリー部
情報・ITセキュリティ課
（情報セキュリティ事務局）

CIOメッセージ

河野 昭彦
Akihiko Kawano

執行役員
チーフ・インフォメーション・
オフィサー（CIO）
（兼）IT・デジタル推進本部長

パナソニック コネクトの情報セキュリティについて

パナソニック コネクトは、
情報セキュリティを経営の重要戦略の一つと位置付け、
お客様の満足と信頼の獲得、健全なる情報化社会の実現を目指しています

■ サイバーセキュリティリスクへの対応

近年のサイバー攻撃はますます巧妙化し、高度化しています。当社は、顧客企業の機密情報や個人情報を扱ったIoTソリューションやAI技術を提供しています。この状況を踏まえた適切なセキュリティ対策が不可欠です。そのため、当社では製品やサービスの設計初期段階から、ライフサイクル（企画・設計・実装・検証診断・運用保守）の視点でリスク評価を行い、暗号化やアクセス制御などの技術対策を導入しています。また、日々発生する新たな脅威に対応するため、定期的なセキュリティ監査や脆弱性評価を実施しています。さらに、サイバー攻撃に対する予防・検知・対応のため、サイバーセキュリティインシデント対応体制を整備しています。

このような対策により、当社は、ビジネスの持続性や成長を支える信頼性の高い製品/サービスを提供していきます。

■ 個人情報保護の重要性について

国内外を問わず、個人情報の取り扱いやデータプライバシーに対する関心が高まっています。当社でも、従業員全員が個人情報の重要性を理解し、適切に管理することが必要だと認識しています。そのため、個人情報保護の取り組みを情報セキュリティ基本活動に組み込んでいます。当社が提供するサービスにおいて個人情報を取り扱う場合は、社内の専門職員が、個人情報取扱いスキームやコンプライアンス適合性を事前に精査し、法令に適合した対応を行っています。

当社は、お客様からお預かりした個人情報をしっかりと保護し、信頼を築くことが大切だと考えています。

■ 情報セキュリティの取り組みについて

当社は、情報セキュリティガバナンスの強化策として、情報セキュリティ体制の構築、ルールの制定、教育、サプライチェーン情報セキュリティ対応、内部監査・ISO/IEC 27001認証取得等包括的に取り組んでいます。これにより、情報セキュリティに関するリスクを最小限に抑えることができています。しかしながら、技術革新によりセキュリティに関するリスクは常に変化しています。当社は、新たな脅威に対応するため、今後も情報セキュリティ活動をアップデートし続けていきます。

本書では、当社の情報セキュリティの取り組みをご紹介しています。是非、ご一読いただき、私たちの情報セキュリティに対する取り組みと姿勢をご理解いただけますようお願いいたします。

情報セキュリティガバナンス

情報セキュリティ推進体制の確立

セキュリティに対する脅威に適切な対応を行うには、体制構築が重要です。パナソニック コネクトでは、情報セキュリティ基本方針に基づき、推進体制を整備・確立しています。

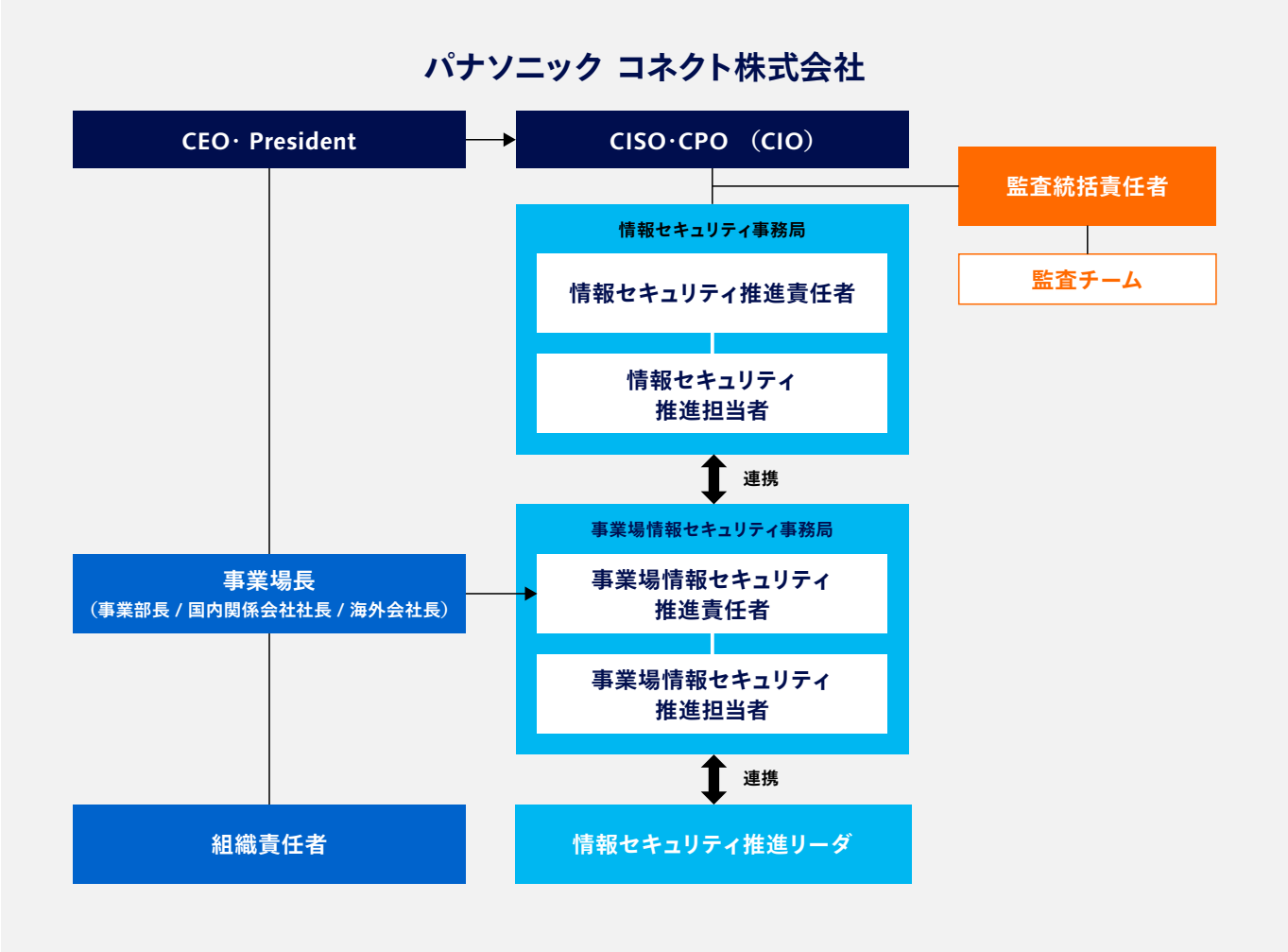
具体的には、CISO(Chief Information Security Officer※)直轄に、情報セキュリティ推進責任者を任命し、専任部隊として情報セキュリティ事務局を設置しています。

※CIO(Chief Information Officer)が、CISO並びにCPO(Chief Privacy Officer)を兼務

情報セキュリティ事務局は、情報セキュリティ活動やルールの策定と展開、日々の活動のサポート、社内コンサルティング、インシデント発生時の対応など、グループ全体における情報セキュリティガバナンスを統括しています。

各事業場及び関係各社においても、当該事業場内を統制する情報セキュリティ事務局を設置し、末端まですべての組織に速やかに情報セキュリティ活動の展開ができるように、推進体制を確立しています。2022年度は、国内外で事業場情報セキュリティ事務局約250名、組織の推進リーダ600名体制で推進しています。

一方、ガバナンスが適切に働いているかをチェックする機能として、監査統括責任者を任命し、毎年、百部門以上に対し内部監査を実施し、情報セキュリティ活動の適切性を確認しています。監査結果は、CISOへ報告され、改善の取り組みへつなげています。



情報セキュリティマネジメント

情報セキュリティ年間活動計画

各組織で情報管理が適切に行われるように、年度初頭に情報セキュリティ事務局が、情報セキュリティ年間活動計画を策定、展開しています。各組織は、本活動計画に従って、リスク低減に努めます。

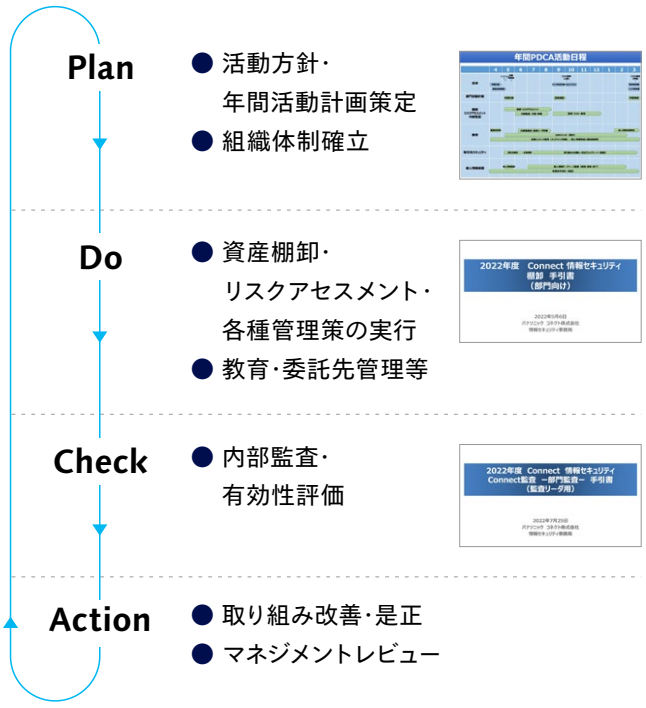
情報セキュリティマネジメントサイクル（PDCA）

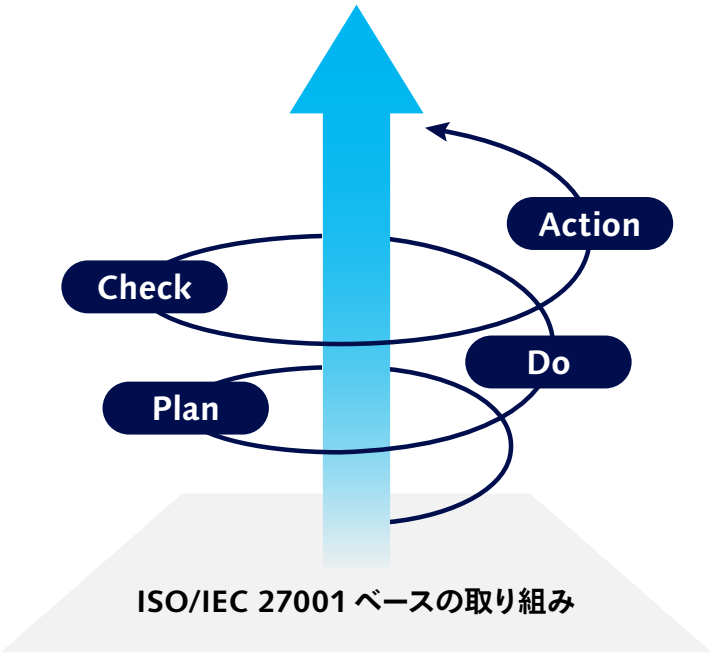
基礎活動として、部門単位での体制の構築、お客様からお預かり・管理している各種情報資産の特定（棚卸）や分類、導入している管理施策の実施状況確認、リスクアセスメントなど、PDCA（Plan-Do-Check-Action）サイクルに基づいて取組むように年間計画を定めています。また、これら活動は全員取り組みという観点から、どの組織でも、誰もがスムーズに進めることができるように、活動別に標準手引書を準備し、各組織へ周知徹底しています。

基礎活動以外に、委託先への情報セキュリティへの取り組み依頼や、個人情報保護活動、教育も年間活動に組み入れ、全方位で漏れの無いように取り組んでいます。特に、資産を取り扱うのは"人"であるという観点から、情報セキュリティ教育を重要視し、複数のカテゴリーの教育を提供・実施しています。

チェックフェーズでの内部監査は、監査人としてパナソニックグループ社内資格認定を受け、十分に力量が備わった人材が各組織を定期的に監査しています。

これらの活動は、ISO/IEC 27001（情報セキュリティマネジメントシステム）に照らし合わせ、内部及び外部の課題、利害関係者からの要望等の結果を含めてCISOへ報告され、今後の方向性についての指示を受けています。そして翌年の情報セキュリティマネジメントをサイクルとして回すことにより、年々変化する脅威に対する継続的な改善活動につなげて、スパイラルアップを図っています。





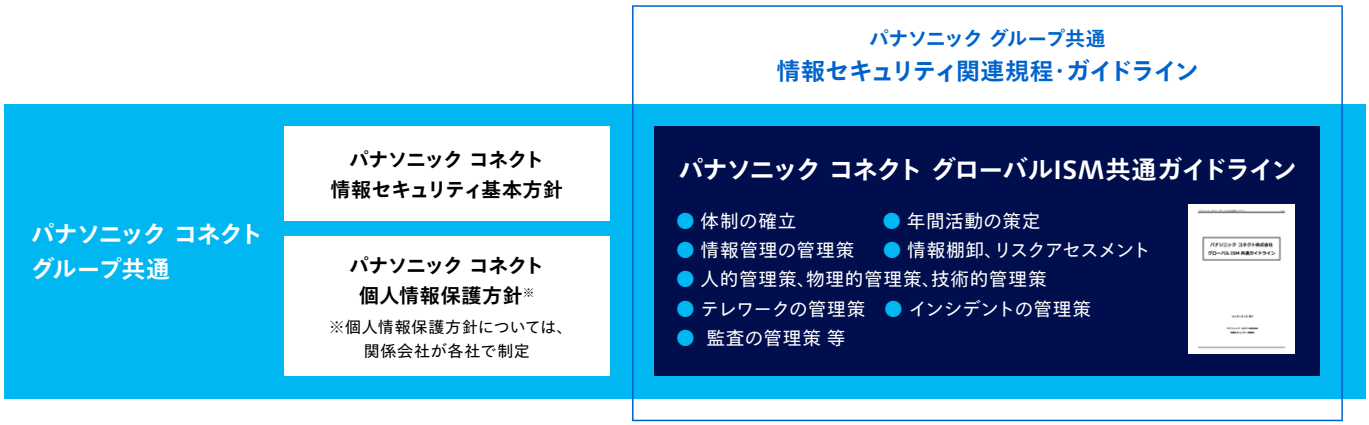
各種セキュリティリスクへの対応

情報セキュリティのルール

パナソニック コネクトでは、運用骨格となる情報セキュリティの基本方針に基づき、パナソニックグループで順守されるべき上位規程に準拠した"パナソニック コネクト グローバルISM(Information Security Management)共通ガイドライン"を発刊しています。本ガイドラインには、事業場長・情報セキュリティ事務局・組織責任者等の情報セキュリティ推進に対する役割と責任を、組織的視点から明確に定めています。また、組織及び個人で、日常的に順守すべき様々なルール・管理施策・インシデント対応、委託先管理等を規定しています。

本ガイドラインの適用は、パナソニック コネクトならびに関係会社の従業員および取締役、役員、ならびに、雇用契約や派遣契約を通じた嘱託、顧問、雇員および派遣社員を対象としています。

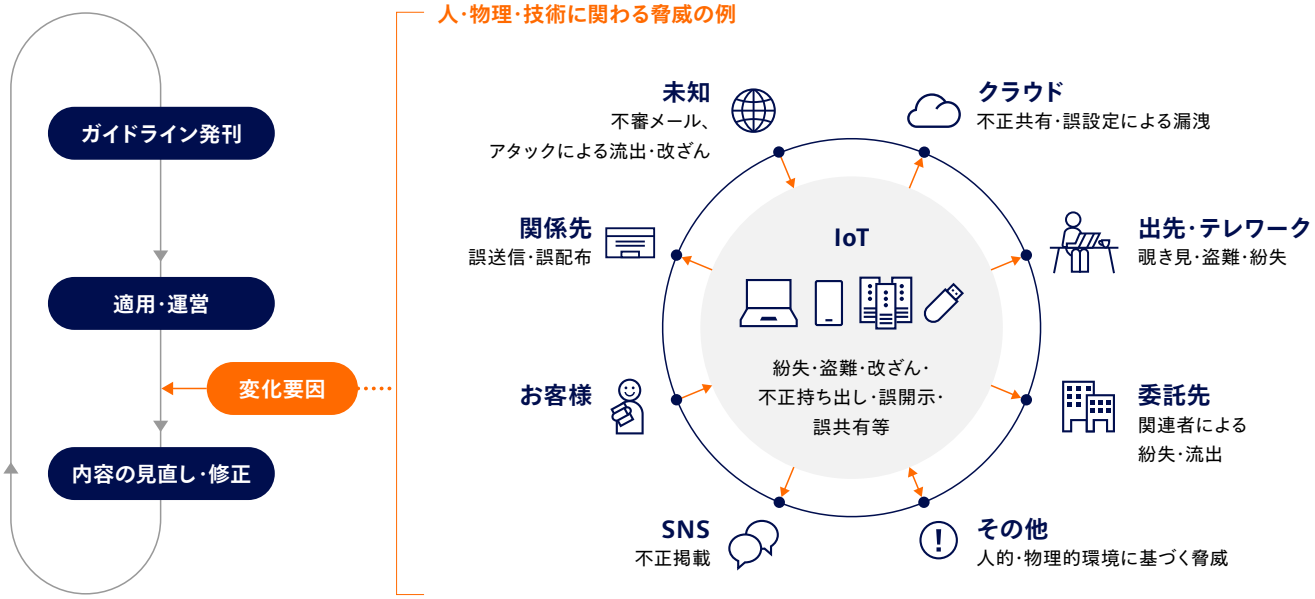
本ガイドラインを含む関連規程一式は、社内イントラネット上の情報セキュリティポータルに掲載されており、適用対象者は常に閲覧可能な状態を維持し、いつでも誰でもが迷うことなく情報セキュリティを順守できる環境を提供しています。



ガイドラインを含む関連ルール詳細は、社外公開しておりません。

脅威への対応と見直し

ガイドラインは、一度取り決めしたらそれで終わりというものではなく、各種活動の課題や有効性評価結果、内外からの要求事項、セキュリティを保つべき領域の変化に伴うリスクの変化等に柔軟に対応するため、毎年内容を見直してます。



サイバーセキュリティ

サイバーセキュリティ

ITを駆使するパナソニック コネクトにおいて、情報セキュリティにおけるサイバーセキュリティの位置づけはますます重要になっています。

■ 体制

パナソニック コネクトに配置されたCSIRT※1は、サイバー攻撃や脆弱性の検出・分析・対策などを行うことで、製品やサービス、社内環境のセキュリティを向上させる役割を果たしています。パナソニック コネクトのCSIRTは、パナソニックホールディングスのCSIRTや、事業部・各職場との縦の連携はもちろん、PSIRT※2、FSIRT※3とも横連携し、各種の予防・防御や各種検査の対策を通じて、サイバーセキュリティリスクを極小化する取り組みを行っています。また、パナソニックグループとして「日本シーサート協議会（一般社団法人 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）」に加盟し外部機関の組織と連携しています。

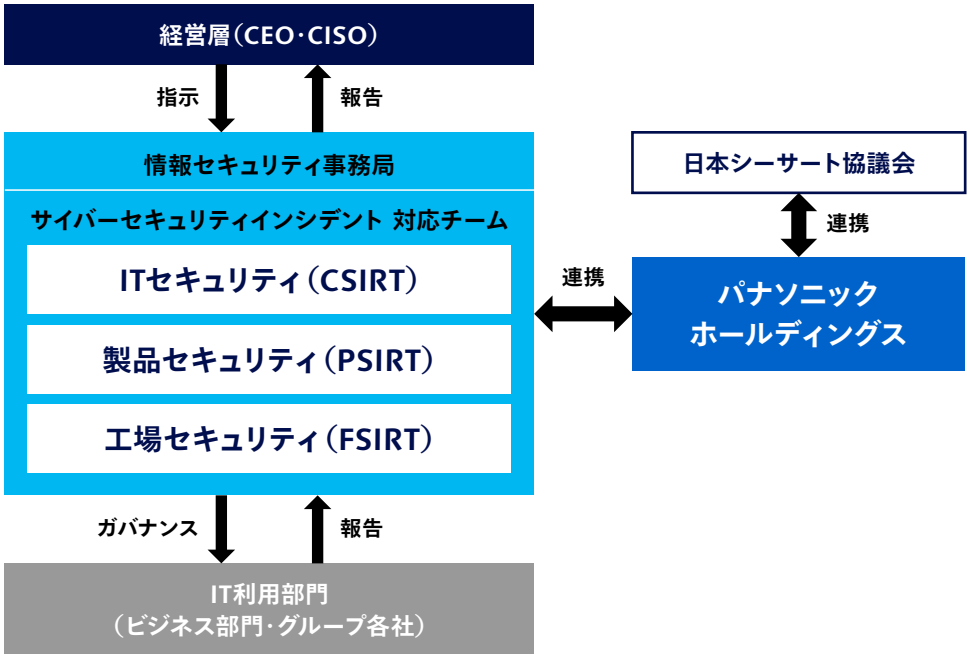
■ 技術的対策

従来の境界型防御の考え方に、ゼロトラストの考え方も加え、多層防御の仕組みを導入しています。具体的には、PC・サーバにはEPP※4やEDR※5、ネットワーク上のアクセスには多要素認証、WebサイトにはWAF※6を導入するなどして、サイバー攻撃からの防御策を講じています。実装すべき防御策を定義すると同時に、定期的なセキュリティ監査や脆弱性評価を実施し、新たな脅威へも対応しています。また、拡大するクラウド等の技術の利用に応じて、事前の安全確認体制を充実させ、ビジネス部門を含めた社内の安全なIT利用環境の構築を支援しています。

■ サイバー教育・訓練

定期的にサイバー教育コンテンツを用いた従業員教育や、標的型メール攻撃を装った疑似メールを用いた訓練を実施し、サイバーセキュリティの周知・啓蒙活動に取り組んでいます。

サイバーセキュリティ インシデント対応体制



※1 CSIRT…Computer Security Incident Response Teamの略で、コンピュータやネットワークに関するセキュリティインシデントに対応する組織のこと。
※2 PSIRT…Product Security Incident Response Teamの略で、製品に関するセキュリティインシデントに対応する組織のこと。
※3 FSIRT…Factory Security Incident Response Teamの略で、工場や生産設備に関するセキュリティインシデントに対応する組織のこと。
※4 EPP…Endpoint Protection Platformの略で、アンチウイルスソフトのような、マルウェアの感染を防ぐソフトウェアのこと。
※5 EDR…Endpoint Detection and Responseの略で、マルウェア感染後の対応を支援するソフトウェアのこと。
※6 WAF…Web Application Firewallの略で、Webアプリケーションの脆弱性を悪用した攻撃からの防御を行うツールのこと。

製品セキュリティ

製品セキュリティ 開発・運用のプロセス整備と取り組み

サイバー攻撃による影響の拡大により、製品およびサービスのセキュリティ確保に対する社会的要請が高まってきています。また、攻撃手法の高度化などにより、インシデントが発生するリスクも日々厳しいものとなってきています。加えて、製品/サービスにおけるサプライチェーンでのセキュリティ確保も必要となっています。

パナソニック コネクトでは、製品/サービスのライフサイクル(企画・設計・実装・検証診断・運用保守)全体を通して、お客様が受けるセキュリティに対する脅威から保護するために、各種ガイドラインを整備・運用し、それを定期的に見直すことにより、全社で一丸となってセキュリティの確保に取り組んでいます。

製品/サービスの開発段階においては、リスクの最小化のために、守るべき資産・機能やそれらに対する攻撃の可能性を検討し、適切なセキュリティ対策が施されるように開発を行います。また、出荷前には、専門家によるセキュリティ診断を行い、検出された脆弱性を修正して取り除いています。

さらに、製品/サービスのセキュリティに関する情報(脆弱性情報など)を入手したときは、関連部門と協力し、直ちに事実確認を行います。確認の結果、問題があることが判明したときには、アップデート等によって製品セキュリティの確保を行うとともに、チェック体制の整備などの再発防止に向けた取組みを行います。

製品/サービスのライフサイクルにおける取り組み

※OSS:Open Source Softwareのこと

教育・人材育成

人材育成の基本

パナソニック コネクトでは、お客様からお預かりした情報や個人情報を適切に取り扱うための情報セキュリティ教育を推進しています。組織的に情報を取り扱うことが多いため、入社時・昇格時など組織の役割に応じた階層別研修も開催しており、日ごろから教育を受けることができる仕組みを提供しています。

個人情報保護に関する教育

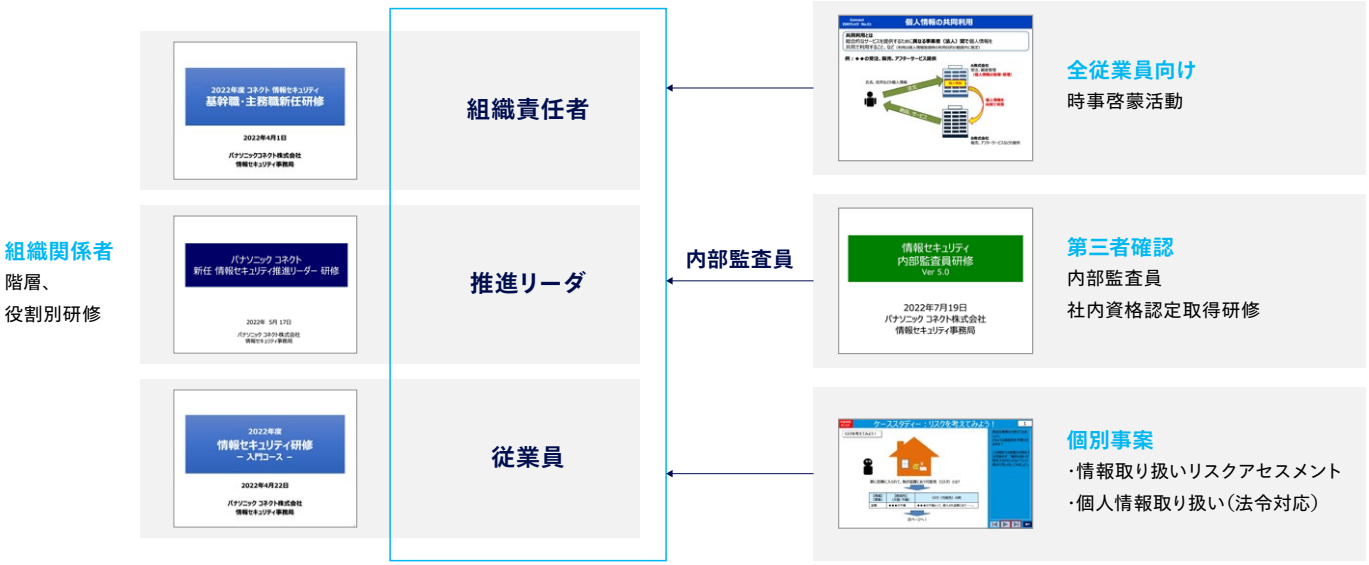
BtoBソリューションビジネスにおける、個人情報の取り扱いには特に配慮が必要です。パナソニック コネクトでは、個人情報を取り扱う従業員に対し、取り扱いの開始前、ならびに定期的に、特別な教育を実施しています。お預かりした情報の取り扱いに関するリスクアセスメントとして、業務フロー分析教材などを独自開発し、使用しています。

環境変化に応じた教育

コロナ禍において、テレワークが飛躍的に進みましたが、そうした環境においても、業務を滞りなく進めることのできるような教材も提供しています。また、定期的に役員を含む全従業員を対象とした「標的型攻撃メール訓練」も実施しており、不審メールに対する予防に努めています。

日々活動に対応した教育

PDCAの一環として、力量確保のための専門研修を実施しています。具体的には、内部監査資格（社内認定制度）やリスクアセスメント教材を提供し、職場におけるリスク対応を図っています。



過去の教育事例

● 組織
- ・組織責任者研修
- ・新入社員研修
- ・新任情報セキュリティ推進リーダ研修
- ・新任事業場情報セキュリティ事務局研修
- ・働き方改革における情報セキュリティ説明会

● 個人情報
- ・個人情報の取扱い者の教育
- ・グローバルBtoBソリューション ビジネスにおける個人情報概論

● PDCA
- ・内部監査員研修
- ・リスクアセスメント 業務フロー分析

● その他
- ・ISMナレッジ （情報セキュリティに関する時事啓蒙）
- ・全従業員教育「インシデント事例に学ぶ」
- ・全従業員教育「パスワードを強化するヒント」
- ・標的型攻撃メール訓練

個人情報保護

個人情報保護の取り組み

パナソニック グループで規程されているルールに準拠し、同水準の保護体制を確立しています。

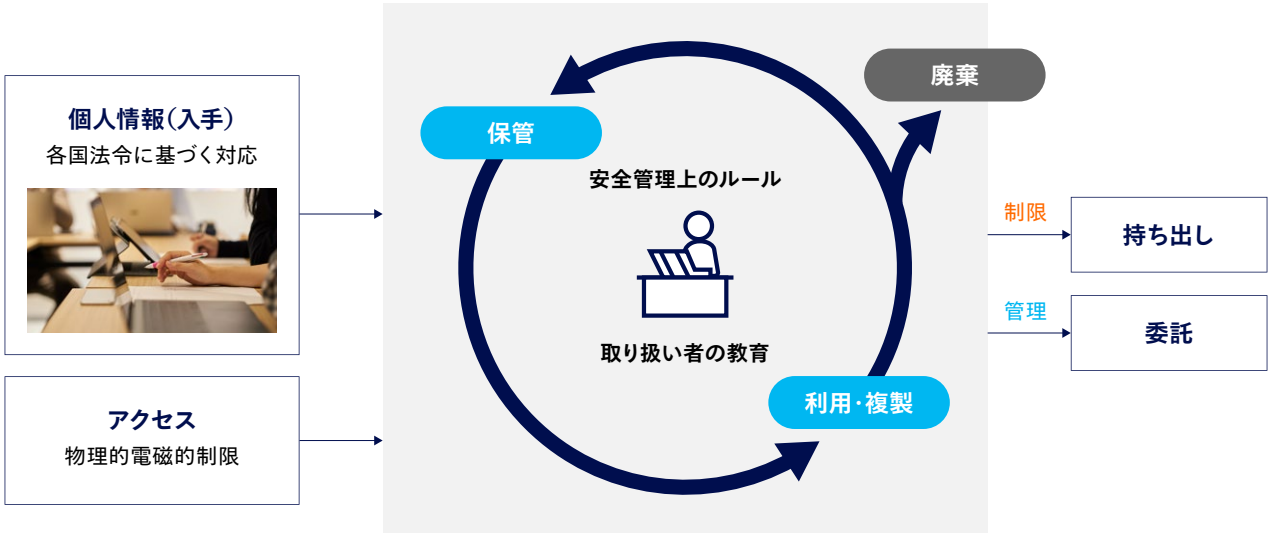
パナソニック コネクトは、個人情報保護法に基づき、お預かりする個人情報は、利用目的を明示したうえで、その範囲内で利用し、適切に管理しています。また、サービス利用ごとに窓口を設置し、開示等に対する対応を速やかに行っています。

パナソニック コネクトの個人情報保護方針は、こちら（https://connect.panasonic.com/jp-ja/privacy-policy）
（個人情報保護方針については、関係会社が各社で制定）

安全管理の側面では、保管、アクセス、持ち出し、委託先管理などライフサイクルの視点でルールを強化し、事故抑制に努めています。さらに個人情報の取り扱い者には、取り扱い開始前ならびに定期的教育を実施し、力量を確保しています。

グローバル個人情報保護の取り組み

海外各国でも個人情報の取り扱いに関する法令・規制が整備、強化されてきました。その多くは、EU一般データ保護規則（GDPR：General Data Protection Regulation ）を意識したものが多くなってきており、今後もその傾向が続くことが予測されます。パナソニック コネクト内で、グローバル展開している事業においては、原則各国の法令に基づき、それぞれサービス特有の事情を勘案して、対応方針を定め対応しています。



物理的セキュリティ

安心安全な物理的環境の整備

パナソニックグループの基準に則り、すべての活動拠点で物理的セキュリティ境界（ゾーン管理）を定め、執務ゾーンへの入退室管理を行っています。具体的には、顔認証/IDカード入退室管理システム、監視カメラシステム等を個別のリスク事情を勘案して設置し、不正なアクセスからの保護を図っています。

ゾーン別セキュリティ

作業できるゾーンは区分けされており、ゾーン事に取り合う情報資産のランクが異なりゾーンに応じたルールを規定しています。お客様との打ち合わせを行う際は、原則、事業場ゾーンで行います。通常業務を行う際は、事務ゾーン以上で行います。このゾーンは、原則従業員のみがアクセス可能です。特に重要な情報や個人情報を取り扱う場合は、特定者のみがアクセス可能なゾーンを使用します。

配送物の授受においても適切に行うためルール化し、また外部（社外からの派遣者、構内請負業者、訪問者等）からの情報機器などの持ち込み制限や、定められたゾーンからの持ち出しに関する制限（指定の情報資産の持ち出し不可など）を行っています。

取引先(委託先)セキュリティ

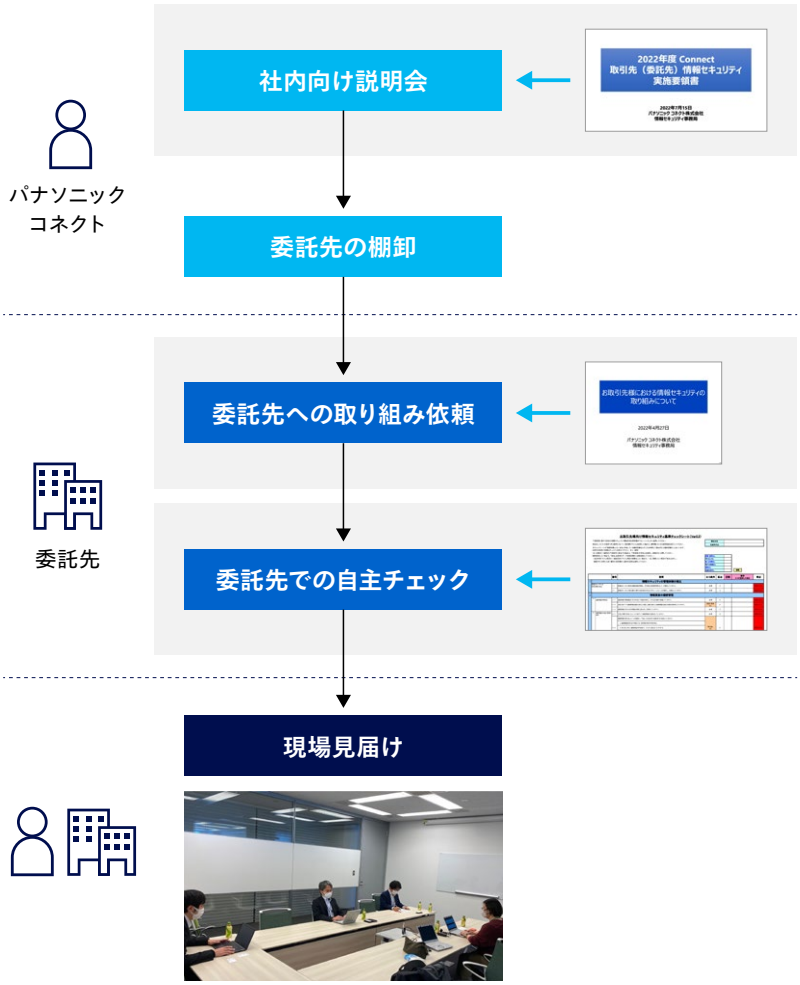
委託先の重要性の認識

パナソニック コネクトでは、委託先の情報セキュリティレベルが重要事項の1つであると認識しています。従って、委託先を選定する際の基準や情報セキュリティの状態を確認できる体制を整備しています。

機密情報を取り扱う委託先への管理、監督の取り組み

委託先の管理を徹底するために、詳細手引書を準備、展開しています。具体的には、社内関連部門へ取り組み説明会を開催し、各部門で機密情報を開示している委託先の洗い出しを行います。その後、書面による情報セキュリティ事項の確認を定期的に行っています。点検結果は数値化され、一定基準に満たない場合は、改善要望を行い、フォローしています。状況に応じて委託先の協力を得た上で現場の見届けまで実施しています。また、機密情報を共有する再委託先については、事前に文書で伝えることを確認しています。

必要な委託先には、情報セキュリティ構築のための参考資料を提供し、委託先のセキュリティレベル向上を図っています。



事故対応

事故対応

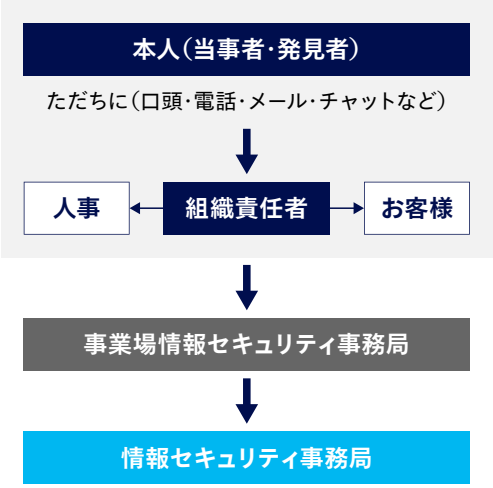
事故が予見される事象が発生した場合は、組織責任者を通じて情報セキュリティ事務局に報告されます。情報セキュリティ事務局は、直ちに被害拡大防止・証拠保全などの初動対策を実施します。また事故の根本原因の究明および再発防止など恒久対策を実施します。

業務委託する取引先で事故が発生した場合は、取引先と協議・連携しながら対応を行います。海外会社においても同様のプロセスで報告されます。

万が一お客様関連の事象が発覚した際には、対応について第一に取り組みます。法令等で定められた事象に該当する場合は、関連する省庁・機関へ報告します。事故に至らなかった事象を含めて受付結果はすべて分析し、事故抑制に努めています。必要な場合は、リスク発生の経過と原因、予防策などの事例を全従業員に教育します。

また、社内諸規則に違反をしているケースにおいては、人事懲罰の対象になります。

情報セキュリティ　事故報告ルート



ISO/IEC 27001

第三者認証　ISO/IEC 27001

パナソニック コネクトグループでは、情報セキュリティマネジメントシステム（Information Security Management System：以下ISMS）の国際認証規格であるISO/IEC 27001認証を取得しています。

ISMSを通して、情報のCIA（「機密性：Confidentiality」、「完全性：Integrity」、可用性：Availability」）を保護する体系的な仕組みを構築しています。

認証基準	ISO/IEC 27001:2013 / JIS Q 27001:2014
登　録　日	2007年12月26日
登録番号	IC07J021
認証機関	株式会社日本環境認証機構　(ISR007)
登録範囲	サプライチェーン」「公共サービス」「生活インフラ」「エンターテインメント」分野向け機器・ソフトウェアの開発／製造／販売、並びに、システムインテグレーション／施工／保守・メンテナンス、およびサービスを含むソリューションの提供
適用範囲	・パナソニック コネクト株式会社 IT・デジタル推進本部　情報・ＩＴセキュリティ課、 メディアエンターテインメント事業部、アビオニクスビジネスユニット、モバイルソリューションズ事業部、 マーケティング本部 モバイルソリューションズマーケティング部、佐賀工場、プロセスオートメーション事業部、現場ソリューションカンパニー ・パナソニック SSサービス株式会社 ・パナソニック システムデザイン株式会社 ・株式会社パナソニック システムネットワークス開発研究所

Panasonic
CONNECT