ガバナンス

コーポレートガバナンス

コーポレートガバナンスの基本的な考え方

富士通は、2015 年12 月の取締役会決議によって、コーポレートガバナンスに関する当社の考え方を整理した基本方針（「コーポレートガバナンス基本方針」）を制定しました。2023年9月に改訂した当基本方針は、現在の富士通にとって最善のものと考えて作成していますが、硬直化し、形骸化することのないよう不断に見直し、適宜取締役会で議論するなどして、常に最善のコーポレートガバナンス体制を維持できるよう努めています。

- コーポレートガバナンス基本方針

コーポレートガバナンス体制（2024年6月24日現在）

富士通は、コーポレートガバナンス基本方針に則り、監査役会設置会社制度の長所を生かしつつ、取締役会における非執行取締役（独立社外取締役および社内出身の業務を執行しない取締役をいう。以下、同じ）による業務執行取締役の業務執行に対する監督の実効性と多様な視点からの助言の確保を実現しています。

＜取締役会＞
富士通は、経営の重要な事項の決定と監督を行う機関として取締役会を設置しています。取締役会は、法令および定款に反せず、妥当と考える最大限の範囲で、業務執行に関する意思決定権限を代表取締役およびその配下の執行役員以下に委譲し、取締役会はその監督および助言を中心に活動を行います。また、取締役会は、業務執行の誤り、不足、暴走等の是正、修正を可能とするよう非執行取締役を中心に構成し、独立社外取締役の員数を取締役会の員数の過半数とすることで監督機能および助言機能を強化しています。なお、取締役の経営責任をより明確化するため、2006年6月23日開催の株主総会決議により、取締役の任期を2年から1年に短縮しました。

取締役会は、2024年6月24日現在において、業務執行取締役3名、非執行取締役6名（内、社外取締役5名）の合計9名で構成しています。

2023年度においては、取締役会を18 回（内、臨時取締役会6回）開催し、会社法および当社取締役会規則に定める取締役会において取り扱うべき事項につき、機動的に決議および報告を行いました。特に、富士通グループの事業環境を踏まえて取締役会としてフォーカスすべきテーマとして、①新中期経営計画、②ビジネスポートフォリオ・トランスフォーメーション、③海外ビジネスの収益性改善、④品質・セキュリティ事案、⑤取締役等のサクセッションプランニング、⑥各テーマの効率的なモニタリング方法の6テーマを設定し、これらについて集中的に議論を行うとともに、継続的な監督を行いました。

さらに、株主還元、政策保有株式の検証、内部統制システムの整備・運用状況の報告、株主および投資家との対話のフィードバック等を議題として取り上げました。また、取締役会全体の実効性評価については、2023年度より、アンケート回答に基づき取締役会事務局が回答役員ごとに個別インタビューを行い、分析・評価を実施しました。これにより、正確な回答の理解に基づく的確な改善施策を取締役会において議論することが可能となり、社外役員への情報共有の充実を含め、取締役会の実効性のさらなる実質的向上を図りました。富士通グループ全体のリスクマネジメントを統括するリスク・コンプライアンス委員会は、各施策実行の迅速性と実効性を担保する目的で2023年度から毎月開催しており、取締役会は、同委員会から任務遂行状況の報告を毎回受け、また、個別の品質・セキュリティ事案についても再発防止を含めた対応について、議論、監督を行いました。

＜監査役（会）＞
富士通は、監査機能および監督機能として監査役（会）を設置しています。監査役は、取締役会等の重要な会議に出席し、取締役会および業務執行機能の監査・監督を行います。監査役会は、2024年6月24日現在において、監査役5名（内、常勤監査役2名、社外監査役3名）で構成しています。

2023年度においては、監査役会を11 回開催（内、臨時監査役会2回）し、主に、監査役監査の方針および監査計画の立案と決議、会計監査人の監査計画、監査方法の確認、結果の相当性および監査上の主要な検討事項等の検討を行うとともに、内部監査部門からの報告聴取、常勤監査役から社外監査役への重要な事項の報告および検討等を行いました。
2023年度における監査役の活動としては、決議した監査の方針および計画に従い、内部統制システムの構築・運用と経営課題への対応を重点に以下を行いました。

- 取締役会、独立役員会議その他重要な会議への出席と意見表明
- 重要な決裁書類の閲覧
- 代表取締役との意見交換
- 本社各部門・子会社の業務等のヒアリング
- 子会社監査役からの報告聴取
- 会計監査人からの報告聴取

- 内部監査部門からの監査状況および結果の聴取
- コンプライアンス部門からの内部通報の状況の聴取
- リスク管理や品質管理の状況の聴取 等

なお、監査上の主要な検討事項に関しては、連結財務諸表における潜在的な重要な虚偽表示のリスク並びに2023年度に発生した重要な事象等の影響および変化等について、会計監査人と十分な議論、検討を行いました。

＜独立役員会議＞
富士通は、独立役員の活用を促すコーポレートガバナンス・コードの要請に応えつつ、取締役会において中長期の会社の方向性に関する議論を活発化させるためには、業務の執行と一定の距離を置く独立役員が恒常的に当社事業への理解を深めることのできる仕組みが不可欠と考え、独立役員会議を設置しています。独立役員会議は、すべての独立役員（独立社外取締役5名、独立社外監査役3名）で構成し、中長期の当社の方向性の議論を行うとともに、独立役員の情報共有と意見交換を踏まえた各独立役員の意見形成を図ります。

2023年度においては、独立役員会議を8回開催し、経営方針、M&Aを含む富士通および富士通グループの事業再編に伴う経営上の重要な事項などについて、継続的に議論するとともに、情報共有と意見交換を行いました。

＜指名委員会・報酬委員会＞
富士通は、役員選任プロセスおよび役員報酬決定プロセスの透明性および客観性を確保し、効率的かつ実質的な議論を行うこと並びに役員報酬の体系および水準の妥当性の確保などを目的として、取締役会の諮問機関である指名委員会および報酬委員会を設置しています。

指名委員会は、当社の「コーポレートガバナンス基本方針」に定めた「コーポレートガバナンス体制の枠組み」と「役員の選解任手続きと方針」に基づき、役員候補者について審議し、取締役会に答申または提案しています。また、報酬委員会は、当社の「コーポレートガバナンス基本方針」に定めた「役員報酬の決定手続きと方針」に基づき、基本報酬の水準と、業績連動報酬の算定方法を取締役会に答申または提案しています。

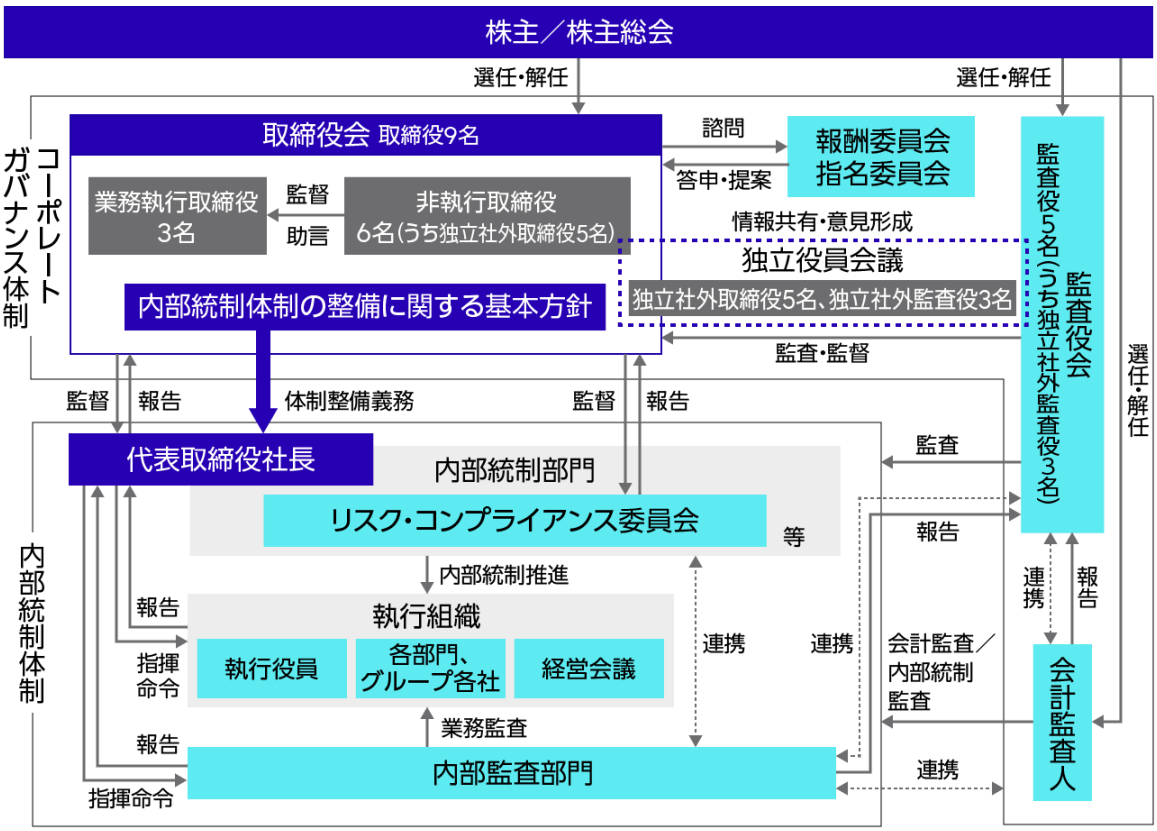
2024年6月に選任された両委員会の委員は以下のとおりであり、指名委員会については非執行役員3名（内、独立社外取締役2名）、報酬委員会については独立社外取締役3名で構成されています。また両委員会の事務局は、当社の人事部門および法務部門が担当しています。

- 指名委員会
  委員長：向井 千秋（独立社外取締役）
  委員：古城 佳子（独立社外取締役）、古田 英範（非執行取締役、会長）

- 報酬委員会
  委員長：バイロン ギル（独立社外取締役）
  委員：佐々江 賢一郎（独立社外取締役）、平野 拓也（独立社外取締役）

なお、2023年度は、指名委員会を9回、報酬委員会を7回開催しました。指名委員会においては、CEOを含む代表取締役の選定案、取締役および監査役候補者並びに取締役会議長候補者の選任案等について、報酬委員会においては、取締役の報酬水準の改定、業務執行取締役の業績連動報酬の内容に関する改定、および非執行取締役に対する株式報酬の導入等について検討を行い、2023年度末までにそれぞれ取締役会に答申しました。また、指名委員会においては、CEO等のサクセッションプランや社外役員候補者の選定の検討、および非執行取締役の相互評価を実施し、報酬委員会においては、2023年度における業務執行取締役の個人別報酬支給額についても検討を行いました。

富士通のコーポレートガバナンス体制の模式図は次のとおりです。（2024年6月24日現在）



コーポレートガバナンス体制の模式図

現状のコーポレートガバナンス体制を選択している理由

富士通は、非執行取締役による業務執行に対する直接的な監督と、業務の決定に関与しない監査役による、より独立した立場からの監督の両方が機能することで、より充実した監督機能が確保されるものと考えています。このような考え方から、独任制の監査役で構成される監査役会を設置する「監査役会設置会社」を採用しています。

また、業務執行の誤り、不足、暴走等の是正、修正を可能とするよう、取締役会は、非執行取締役を中心に構成するものとし、独立社外取締役の員数を取締役会の員数の過半数としています。非執行取締役の中心は独立性が高く、多様な視点を有する社外取締役とし、さらに、富士通の事業分野、企業文化等に関する知見不足を補完するために社内出身の非執行取締役を1名以上置くことで、非執行取締役による監督、助言の実効性を高めています。

役員報酬の決定方針

取締役および監査役の報酬は、報酬委員会の答申を受けて取締役会で決定した「取締役の個人別の報酬等の内容についての決定に関する方針（役員報酬決定方針）」に基づき決定しています。

- コーポレートガバナンス報告書
  「取締役へのインセンティブ付与に関する施策の実施状況 P11 / 報酬の額又はその算定方法の決定方針の有無 P12 」

内部統制体制の基本的な考え方

富士通グループの企業価値の持続的向上を図るためには、経営の効率性を追求するとともに、事業活動により生じるリスクをコントロールすることが必要です。このような認識の下、富士通では、富士通グループの行動の原理原則である「Fujitsu Way」の実践・浸透を図るとともに、経営の効率性の追求と事業活動により生じるリスクのコントロールのための体制整備の方針として、取締役会において「内部統制体制の整備に関する基本方針」を定めています。

「内部統制体制の整備に関する基本方針」の全文ならびに業務の適正を確保するための体制の運用状況の概要については、以下をご覧ください。

- 第124 回定時株主総会電子提供措置事項（交付書面非記載事項）

コーポレートガバナンスに関する開示事項

取締役（2024年6月24日）

	氏名	役位および担当	代表権	独立社外役員
業務執行	時田 隆仁	社長、CEO、リスク・コンプライアンス委員会委員長	○	
	磯部 武司	副社長、CFO	○	
	平松 浩樹	執行役員SEVP、CHRO		
非執行	古田 英範	会長		
	向井 千秋			○
	古城 佳子	取締役会議長		○
	佐々江 賢一郎			○
	バイロン ギル			○
	平野 拓也			○

2023年度 取締役会・監査役会の出席状況

会議体	開催回数	出席率
取締役会	18 回	97.5%
監査役会	11 回	98.2%

取締役および監査役のスキル

富士通は、イノベーションによって社会に信頼をもたらし、 世界をより持続可能にしていくグローバル企業として、取締役および監査役が業務執行、助言または監督機能を有効に発揮するのに必要と考えられる多様性およびスキルをそれぞれ特定し、スキルマトリックスとして開示しています。

取締役（2024年6月24日現在）

	取締役氏名	独立社外	多様性		スキルマトリックス				
			ジェンダー	国籍	企業経営	財務・投資	グローバル	テクノロジー	ESG・学識・政策
代表取締役社長	時田 隆仁		男性	日本	○		○	○	
代表取締役副社長	磯部 武司		男性	日本	○	○	○		
取締役執行役員	平松 浩樹		男性	日本	○		○		○
取締役会長	古田 英範		男性	日本	○		○	○	
取締役	向井 千秋	○	女性	日本			○	○	○
取締役	古城 佳子	○	女性	日本			○		○

	取締役氏名	独立社外	多様性		スキルマトリックス				
			ジェンダー	国籍	企業経営	財務・投資	グローバル	テクノロジー	ESG・学識・政策
取締役	佐々江賢一郎	○	男性	日本			○		○
取締役	バイロン ギル	○	男性	米国		○	○		
取締役	平野拓也	○	男性	日本	○		○	○	

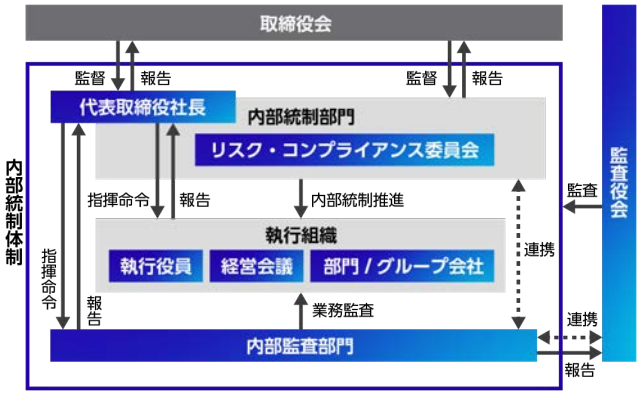
監査役（2024年6月24日現在）

	監査役氏名	独立社外	多様性		スキルマトリックス		
			ジェンダー	国籍	法務・コンプライアンス	財務会計	業務プロセス
常勤監査役	広瀬陽一		男性	日本		○	○
常勤監査役	小関雄一		男性	日本		○	○
監査役	初川浩司	○	男性	日本		○	○
監査役	幕田英雄	○	男性	日本	○	○	
監査役	キャサリン オーコネル	○	女性	ニュージーランド	○		

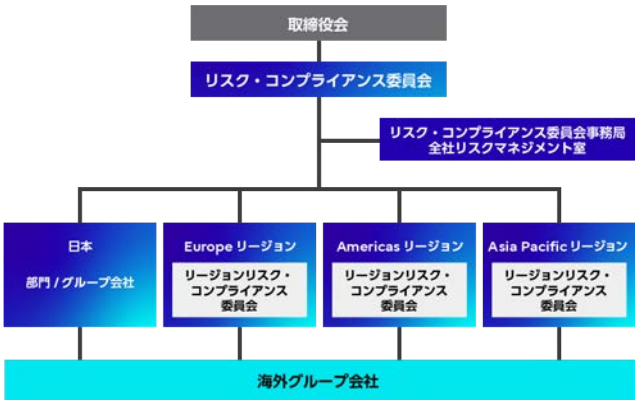
リスクマネジメント

方針・推進体制

富士通グループは、事業継続性、企業価値の向上、企業活動の持続的発展を実現することを目標とし、その実現に影響を及ぼす不確実性をリスクと捉え、これらのリスクに対処するために、取締役会が決定した「内部統制体制の整備に関する基本方針」に基づき、取締役会に直属し、グループ全体のリスクマネジメントおよびコンプライアンスを統括する「リスク・コンプライアンス委員会」を設置しています。
リスク・コンプライアンス委員会は、代表取締役社長（CEO）を委員長として業務執行取締役などで構成しており、富士通グループに損失を与えるリスクを常に評価、検証し、認識された事業遂行上のリスクについて、未然防止策の策定などリスクコントロールを行うとともに（潜在リスクマネジメント）、リスクの顕在化により発生する損失を最小限に留めるため、顕在化したリスクを定期的に分析し、取締役会等へ報告を行い、再発防止に努めています（顕在化したリスクのマネジメント）。
また、リスク・コンプライアンス委員会はグローバルな地域に基づく業務執行体制の区分であるリージョンごとに、下部委員会としてリージョンリスク・コンプライアンス委員会を設置し、国内外の部門（第1線）やグループ会社、リージョンにリスク・コンプライアンス責任者を配置するとともに、これらの組織が相互に連携を図りながら、グループ全体でリスクマネジメントおよびコンプライアンスを推進する体制を構築しています。
さらに、グループ全体のリスク管理機能強化のため、事業部門から独立した代表取締役社長直下の組織である全社リスクマネジメント室（第2線）にリスク・コンプライアンス委員会の事務局機能を設置し、CRMO（Chief Risk Management O icer）の下、リスク情報全般を把握するとともに、迅速・適切に対応しています。そして、2023年6月にCQO（Chief Quality O icer）を新たに選任し、情報セキュリティ、システム品質に関する全社的な施策および対応を実施しています。代表取締役社長主導によるリスクマネジメント経営を徹底するとともに、リスク・コンプライアンス委員会を毎月開催することで、施策実行の迅速性と実効性を担保するよう努めています。
なお、リスクマネジメント・コンプライアンス体制について、毎年、監査役監査、監査部門（第3線）による内部監査、監査法人による外部監査を行い、体制が正常に機能していることを確認しております。



内部統制体制におけるリスク・コンプライアンス委員会の位置づけ



リスクマネジメント・コンプライアンス体制

プロセス

【潜在リスクマネジメントプロセス】

- グループにおける重要リスクの抽出・見直し
  リスク・コンプライアンス委員会事務局（全社リスクマネジメント室、第2線）にて、当社グループを取り巻く環境変化を踏まえたグループにおける重要リスク（16 項目）の抽出・見直しを実施。重要リスクごとにリスクシナリオを定義。
  純粋リスクと経営リスクに区分。

- リスク管理部門（第2線）の選出
  重要リスクごとに当該重要リスクにおける責任を持ち統制を行う所管部門であるリスク管理部門を選出。

- グループにおけるリスク評価
  リスク管理部門/部門/グループ会社において、各重要リスクの影響度、発生可能性、対策状況などを評価。
  当社グループの事業戦略およびビジネス目標達成の観点から積極的に取るべきリスクと回避すべきリスクを選別。

- 重要リスクのランキング化・マップ化
  グループにおける評価内容を踏まえ、重要リスクのランキング化・リスクマップの作成を行い、重要度を可視化。
  重要度をふまえて重点対策リスクを決定。

- リスク・コンプライアンス委員会報告
  グループにおける評価結果を踏まえた分析を実施、重要リスクの対策方針などを議論・決定。

- 部門・グループ会社への是正指導
  グループにおける評価結果をふまえ、部門・グループ会社にフィードバックを実施し、改善を指示。

- 部門・グループ会社におけるリスクモニタリング
  部門・グループ会社において定常的にリスクモニタリングを実施し、リスク対策の状況確認と低減を実施。

【顕在化したリスクへの対応】

- リスクマネジメントに関する規程に基づき、リスク・コンプライアンス委員会への迅速なエスカレーションの実施などのルールを義務化し、従業員に周知。

- リスクマネジメントに関する基準やリスク・コンプライアンス委員会へのエスカレーションルールを基に、部門・グループ会社におけるエスカレーションルールを定め、迅速な対応を実施。

- リスクの分析・横展開を行うとともに必要に応じて取締役会報告等を行い、再発防止に努める。

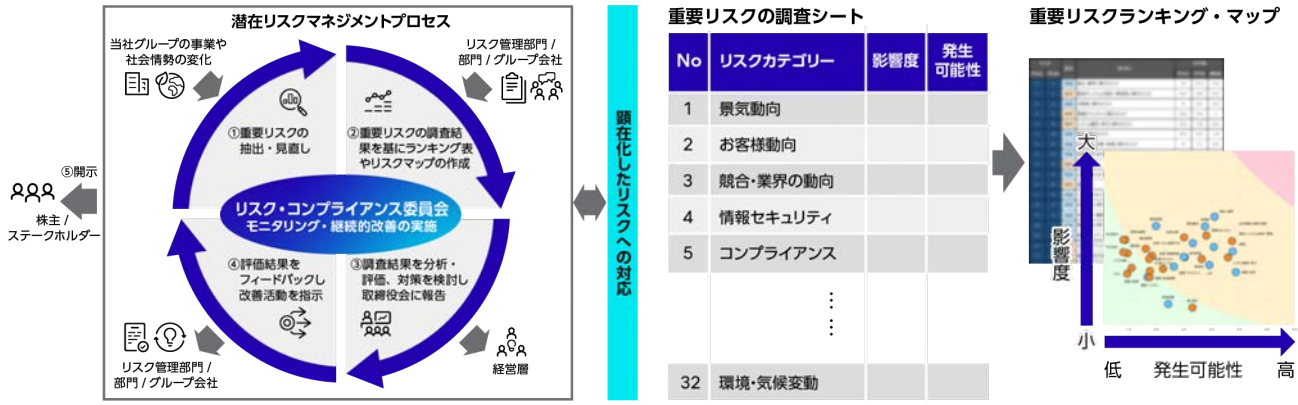
このようなプロセスを繰り返し実行するとともに半期ごとにリスク管理部門による確認を行うことで、グループ全体のリスクの低減と顕在化した際の影響の極小化に努めています。

【重点対策リスク】

潜在リスクマネジメントにおける評価結果に加えて、顕在化したリスクの状況を踏まえたうえで、当社グループの事業戦略およびビジネス目標達成への影響を鑑み、重点的に取り組むリスクを「重点対策リスク」として選定しています。2023年度、2024年度における重点対策リスクは以下2つを定めています。

- セキュリティに関するリスク

- 製品やサービスの欠陥や瑕疵に関するリスク



リスクマネジメントプロセス　　重要リスクの可視化

当社グループにおける重要リスク（注1）

項	区分	重要リスクカテゴリー
1	純粋リスク	セキュリティに関するリスク
2	純粋リスク	自然災害や突発的事象発生のリスク
3	純粋リスク	コンプライアンスに関するリスク
4	経営リスク	財務に関するリスク
5	経営リスク	知的財産に関するリスク
6	純粋リスク	環境・気候変動に関するリスク
7	経営リスク	調達先・提携等に関するリスク
8	経営リスク	お客様に関するリスク
9	経営リスク	競合・業界に関するリスク
10	純粋リスク	製品やサービスの欠陥や瑕疵に関するリスク
11	経営リスク	公的規制・政策・税務に関するリスク
12	経営リスク	人材に関するリスク
13	純粋リスク	人権に関するリスク
14	経営リスク	経済や金融市場の動向に関するリスク
15	経営リスク	投資判断、事業再編に関するリスク
16	純粋リスク	当社グループの施設・システムに関するリスク

（注1） 事業活動に伴うリスクの例：記載例は一部であり、有価証券報告書などに掲載。

- 有価証券報告書・半期報告書・四半期報告書 >

TCFD（気候関連財務情報開示タスクフォース）提言に沿ったリスク関連情報の詳細は、以下のWebサイトもご参照ください。

- 環境リスクへの対応 >

リスクマネジメント教育等

富士通グループ全体でリスクマネジメントを徹底するため、階層別に各種教育・研修を実施しています。

具体的には、新任役員、新任幹部社員などを対象に、リスクマネジメントの基本的な考え方やリスク・コンプライアンス委員会への迅速なエスカレーションなどのルールの周知、製品・サービス、情報セキュリティに関する事案を共有し、継続的なリスクマネジメントの意識向上と対応能力の強化を推進しています。

また、リスクマネジメント部門においては、従業員の評価指標にリスクマネジメントの要素を取り入れることで、評価が金銭的インセンティブに結び付くとともに、組織としてのリスクマネジメントスキルの向上を図り、対応力強化に努めています。

2023年度の教育実績については、「2023年度実績」をご参照ください。

全社防災

富士通および国内グループ会社は、災害発生時の安全確保、被害の最小化と二次災害の防止に努め、操業の早期再開とお客様・お取引先の復旧支援の推進を基本方針として、社内組織の強固な連携体制の構築と事業継続対応能力の強化を図っています。

各事業部やグループ各社の職制系統によるお客様への対応に加えて、地域ごとに富士通グループとして、協力し対応する「エリア防災体制」を構築しております。

また、防災体制の実効性を検証し、対応力を強化するために、全社、対策本部、事業所、従業員など各階層に応じた訓練を行うとともに、被害の最小化、事故の未然防止のため自主点検や検証活動を行っています。これにより課題を把握し、改善に向けた検討・施策を推進することで継続的な防災・事業継続能力の向上を図っています。

全社防災体制と合同防災訓練、検証活動については以下のPDFを、2023年度の活動実績は、「2023年度実績」をご参照ください。

- 全社防災体制と合同防災訓練、検証活動

事業継続マネジメント

近年、地震や水害などの大規模な自然災害、事件・事故、感染症の流行など、経済・社会活動の継続を脅かすリスクが多種多様となっております。 富士通およびグループ会社は、不測の事態発生時にも、お客様が必要とする高性能・高品質の製品やサービスを安定的に供給するため、事業継続計画（BCP：Business Continuity Plan）を策定しています。また、このBCPを継続的に見直し、改善していくために事業継続マネジメント（BCM：Business Continuity Management）を推進しています。

新型コロナウイルス感染症について、富士通グループでは、お客様、お取引先、社員およびその家族の安全確保と感染拡大の防止を最優先としつつ、お客様への製品・サービス提供の継続および感染拡大により生じる様々な社会課題の解決に資する取り組みを進めました。

BCM活動の取り組みや感染症対策、サプライチェーンのBCMについては以下のPDFを、2023年度の活動実績は「2023年度実績」をご参照ください。

- BCM活動の取り組みや感染症対策、サプライチェーンのBCM

2023年度実績

リスクマネジメント教育

— 富士通グループ新任役員向け研修：45名

リスクマネジメントに関する事項のほか、内部統制体制、コンプライアンスに関する事項など、新任役員として留意すべき点について具体的な事例の紹介を交えて実施。

— 取締役向け研修：9名（うち、非執行取締役6名）

非執行/執行の取締役を対象に、リスクマネジメントを含む様々な分野のe-Learningを提供。加えてリスクマネジメントに関する非執行取締役向けの個別セッションを担当執行役員より実施。

— 富士通グループ新任幹部社員向け研修：1,033名

リスクマネジメントに関する基本的な考え方や幹部社員としてのリスクマネジメントにおける役割などについて、e-Learningにて実施。

— リスクマネジメントに関する教育：富士通グループ12万名

リスクマネジメント全般（情報セキュリティ、コンプライアンスなど）に関するe-Learningを実施。

— 防災フォーラム：314名

大規模災害に向けた現場の対応力向上を目的に、富士通グループの防災・事業継続担当者を対象とした知見共有のためのフォーラムを開催。

重大インシデント対応訓練

— 海外リージョンにおける情報セキュリティインシデント対応訓練（Asia Pacific：90名、Americas：75名）：合計165名

情報セキュリティインシデント発生時の初動対応の一連の流れを日本と海外リージョンとをリアルタイムで繋いで実践し、リージョン内や本社との連携/情報共有や顧客対応、個人情報漏洩対応、メディア対応等を含むインシデント対応プロセスの確認・検証を行う。
訓練を通じて課題を抽出し、継続的改善を図ることにより、海外リージョンにおけるインシデント対応力と組織間連携を強化する。

防災・BCM訓練

— 合同防災訓練：2023年度のテーマ「首都直下地震」

年に1回、災害模擬演習を取り入れた全国一斉防災訓練を実施。富士通および国内グループ会社が連携して大規模災害（「首都直下型地震」、「南海トラフ巨大地震」などを想定）に対処するための要領の習熟とその検証を行う。

— パンデミックなどを想定したBCP確認訓練

業務継続に関わる従業員一人ひとりの意識向上を促し、組織全体の事業継続能力を図ることを目標にグローバル全従業員を対象に、パンデミックを想定した在宅リモートワーク勤務を実施した。また、BCPに関するサーベイを実施し、その分析結果をフィードバックすることにより、富士通グループのBCP改善に繋げる。

情報セキュリティ

基本方針

富士通グループでは、専任のCISO（Chief Information Security O.ficer：最高情報セキュリティ責任者）を設置し、情報セキュリティマネジメント体制を強化するとともに、グローバルで一貫したセキュリティポリシーおよび施策を展開することで、グループ全体の情報セキュリティを確保しながら、製品およびサービスを通じてお客様の情報セキュリティの確保・向上に努めています。

マネジメント体制

＜経営者主導による情報セキュリティマネジメント＞

より高度化・巧妙化したサイバー攻撃が急増する中、情報セキュリティの強化が、国の経済安全保障や企業の経済活動における喫緊の課題となっています。富士通では、さらなる情報セキュリティの施策強化と実効性担保を図るため、これまで以上に経営者主導による迅速かつ適切な対応が必要と考え、富士通グループに関する重要なリスク・コンプライアンスについての審議の場であり、CEO（Chief Executive Officer：最高経営責任者）が委員長を務めるリスク・コンプライアンス委員会の体制・機能を拡充し、恒常的・全社的な対応を実現する体制に強化しました。

また、同委員会によるマネジメントと並行し、CEO、CISO、CRMO（Chief Risk Management Officer：最高リスクマネジメント責任者）、CQO（Chief Quality Officer：最高品質責任者）および、各事業責任者を交えた対策協議の場として、月次開催の品質・セキュリティ対策定例会議を新設し、情報セキュリティの状況確認と状況に応じた対策強化を図ることで、CEO主導によるリスクマネジメント経営を徹底しています。

＜CISOによるガバナンス体制の強化＞

CISOによるガバナンス体制として、日本および海外の3リージョン（Americas、Europe、Asia Pacific）にそれぞれリージョンCISOを設置し、本社方針と各国特有のセキュリティ要件をアラインメントすることで、グローバル体制による情報セキュリティ強化を図っています。
また、富士通本社および日本・海外リージョンのグループ会社については、各部門の自律的な情報セキュリティ強化を担うセキュリティ責任者を配置し、CISOによる統率を強化するための体制を構築しています。

具体的なセキュリティ責任者体制については、情報の管理・保護を統率する「情報管理責任者」、情報システムセキュリティの維持・管理を統率する「情報セキュリティ責任者」、製品に関する脆弱性管理を統率する「PSIRT（注1）責任者」を各部門に配置し、CISOと連携して情報セキュリティの各施策を推進しています。

（注1） PSIRT：Product Security Incident Response Team
企業内の製品（Product）を対象としてインシデント対応を行う組織や体制です。

CISOと情報セキュリティ責任者による情報セキュリティマネジメント体制

情報セキュリティの取り組み

情報セキュリティの目指す姿

富士通では、セキュリティ・ライフサイクル・マネジメントを見据えた、プロアクティブな戦略・施策を計画・実行することで、**適切なリスクコントロールによる安心してお客様へサービス提供できる情報セキュリティの実現**を目指しています。

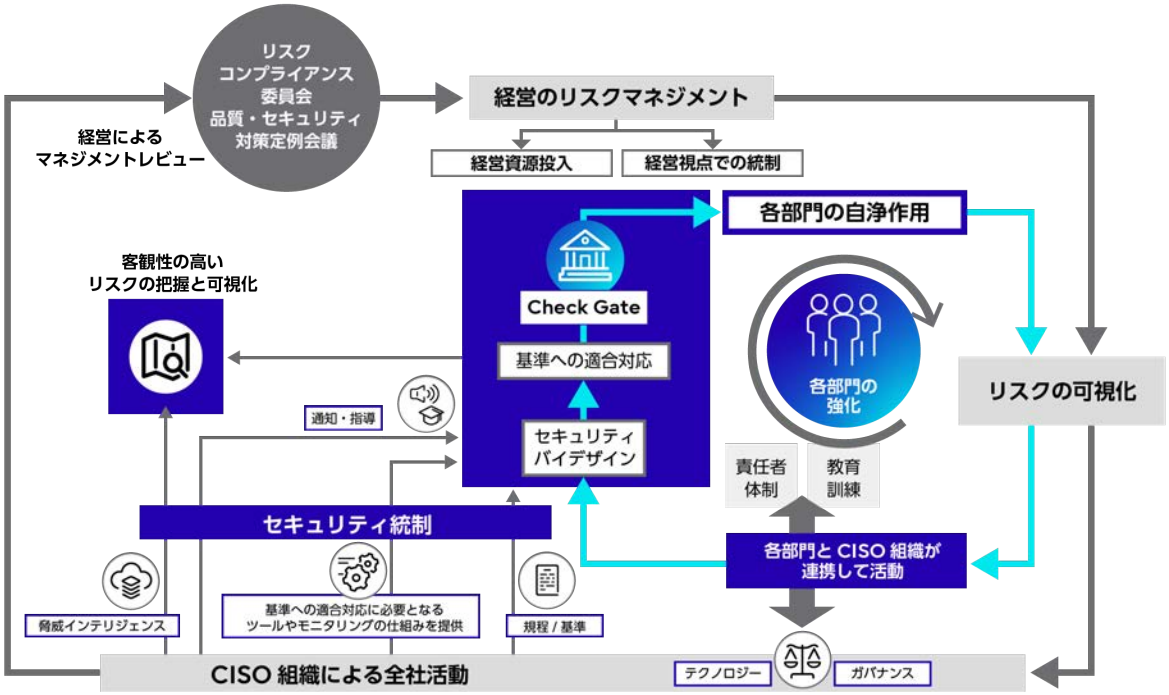
この目指す姿を実現するため、「進化し続ける高度な情報セキュリティによるサイバー攻撃への対応」とともに、成功の鍵となる「従業員一人ひとりの意識改革や組織の風土改革」を進め、全社一丸となって、情報セキュリティ対応のプロセス・ルール・推進体制を整備し、お客様やパートナー企業との安全なビジネス環境および、富士通グループ全体の情報セキュリティ強化に取り組んでいます。

全社セキュリティリスクマネジメントスキーム

富士通では、客観性の高いセキュリティリスクの把握と可視化および的確な是正を軸とした、「全社セキュリティリスクマネジメントスキーム」を構築し、情報セキュリティの目指す姿の実現に取り組んでいます。
「全社セキュリティリスクマネジメントスキーム」は以下のような二重ループ構造となっており、セキュリティリスクの可視化により明らかになるそれぞれの問題に対してセキュリティ施策を組み合わせることで、経営層と各部門、そしてCISO組織を有機的な活動の中でつなげ、連携して対応するスキームを構築しています。
このスキームのループの中で、リスク・コンプライアンス委員会や品質・セキュリティ対策定例会議といった経営層が直接関与する毎月のマネジメントレビューによるモニタリングを行います。そうすることで、CISOが管轄するセキュリティ施策についても、経営課題として経営層と同じ目線で推進することができ、全社一丸となったリスクマネジメントサイクルを実現しています。

- **外側のループ（グレーの矢印にて表現）**
  可視化されたリスクを経営層が把握できるようにすることによって経営層の関与を強めるとともに、CISOによるセキュリティガバナンスを効かせたリスクマネジメントを行うための**統制ループ**

- **内側のループ（ブルーの矢印にて表現）**
  客観性の高いリスク可視化により、自部門の状況を正しく把握することで、各部門の自浄作用（原理原則に基づいた自律的な是正活動）を促進するための**自律ループ**



二重ループによる全社セキュリティリスクマネジメントスキーム

<全社セキュリティリスクマネジメントスキームによって実現すること>

「全社セキュリティリスクマネジメントスキーム」の二重ループは、「セキュリティリスクの可視化」が外側のループと内側のループの共通のチェックポイントとなっており、このチェックポイントを起点に二重ループを回すことで情報セキュリティの継続的な維持・改善・強化を図ります。また継続による定着化を図ることで組織風土の改革を実現します。

<テクノロジーを活用したセキュリティリスクの可視化>

「セキュリティリスクの可視化」 については、CMDB（注2）や、情報管理ダッシュボード（注3）を導入することで、情報システムの残存脆弱性や情報の不適切な管理状態などのリスクをデジタル（機械的）に可視化します。例えば、CMDBに登録されている情報システムの構成情報と脆弱性データベース（注4）を突合し、脆弱性を検知した場合は、是正タスクのチケットを発行することで、システム管理部門に対して是正を指示します。是正指示後の状況についても、脆弱性の残存状況をダッシュボードで可視化することにより、確実な是正完了をモニターします。
なお、リスクの可視化において、特に危険度が高いリスクが検出された場合は、経営層やCISOが関与した統制を行い、より迅速かつ適切な対処を実行します。

（注2） CMDB：Con.iguration Management Database / 構成管理データベース
情報システムの構成情報（ハードウェア、ソフトウェア、ネットワークなどの構成情報）を収集し一元管理するためのデータベースです。収集した構成情報は、セキュリティ点検・監査、脆弱性対応、セキュリティインシデント対応に活用されます。

（注3） 情報管理ダッシュボード：デジタル化された情報管理台帳
富士通グループでは情報管理台帳（秘密情報の管理者、管理場所、共有範囲などを管理する台帳）をデジタル化し管理運用しています。さらに実際の情報管理の状態（ストレージサービスの監査ログなど）と整合性チェックを行い、不備などを検出した場合は、管理部門へアラート通知を行うことで早急な対応を可能としています。

（注4） 脆弱性データベース：
既知の製品脆弱性などを収集し一元管理しているデータベースです。

また、各部門についても、リスク可視化を基に自浄作用が働く組織風土を醸成します。
最初のステップとして、従業員自身や組織の情報管理リテラシーの状態（内的要因）、サイバーリスクの実態（外的要因）について可視化し共有します。（見える化）
続いて、従業員一人ひとりが可視化されたリスクの状態を正しく理解・共感（自分ごと化）することにより、各部門の自律的な情報セキュリティ対応（行動化）を促し、これを改善しながら繰り返し定着させることで、自浄作用が働く組織風土を醸成します。

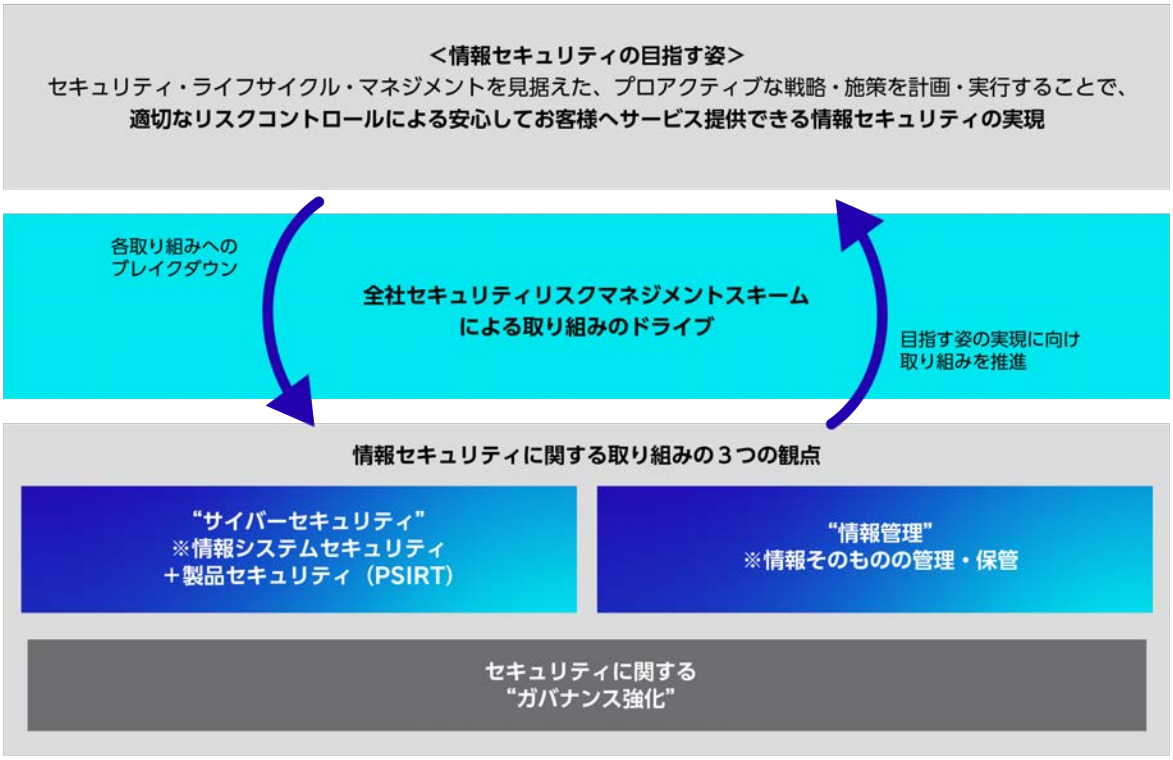
取り組み

「全社セキュリティリスクマネジメントスキーム」の中で実行されている主な取り組みについて、以下3つの観点で紹介します。

- **サイバーセキュリティ**
  情報システムセキュリティ（情報システムおよびネットワークに対する安全性・信頼性の確保・維持）に加え、富士通製品・サービスのセキュリティ維持活動に関する施策の紹介

- **情報管理**
  重要情報（秘密情報、個人情報）を含む情報そのものの機密性・完全性・可用性の維持管理に関する施策の紹介

- **ガバナンス強化**
  各セキュリティ施策を浸透・定着化させ、組織全体のセキュリティ強化を図るための、ガバナンス強化施策の紹介



情報セキュリティに関する取り組みの3つの観点

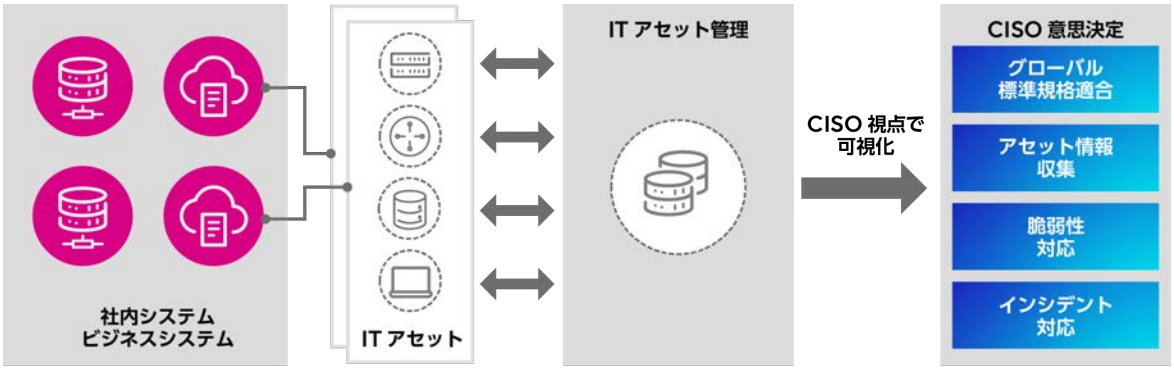
サイバーセキュリティ

富士通の所有するシステムのITアセット管理情報を基軸に、攻撃者からの侵入の防御に加え、侵入された際の検知・防御の両面にて、境界防御とゼロトラストセキュリティを具備していくことで、セキュリティ侵害を未然に防ぐ対応を強化していきます。

ITアセットの一元管理と連動した施策

＜ITアセット一元管理・可視化による自律的な是正＞

富士通では、お客様の安心安全でサステナブルな事業活動を支えるため、グローバルに展開しているお客様向けのITシステムおよび、社内ITシステムのITアセット管理を一元化し可視化することで、グループ全体のセキュリティリスクの特定と是正を速やかに実施しています。平時からのリスク管理を強化するとともに、CISO直轄組織によるリスク監査と結果を見える化し、各部門における適切な現状把握と自律的な是正を促進しています。

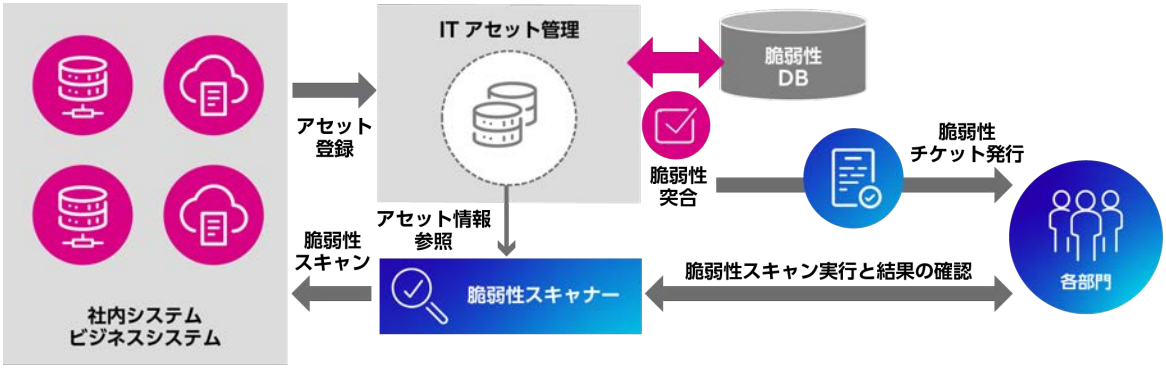


グローバルITアセット管理

＜脆弱性の検出と是正＞

ITアセット管理情報を基軸に、インターネットから直接アクセス可能となっているシステム（アセット）に対して脆弱性スキャンをかける仕組みを提供することで、システムを管理する各部門による、自律的な定期スキャンと脆弱性の検知をトリガーとした是正対応を可能としています。この仕組みを利用した定期的検査を毎年１回行うことで、脆弱性対応が確実に実施されていることを確認し、さらにリスクの高い脆弱性を検知した際は、CISO直轄組織の関与により、迅速で確実な是正対応を行います。
また、ITアセット管理情報を定期的に最新化し、脆弱性データベースと突合することにより検出した脆弱性について、対象部門へチケット（是正タスク）を発行し、確実な対処を徹底する仕組みを実現しています。この仕組みでは、インターネットから直接アクセスができないシステム（アセット）の脆弱性の検出も可能となっています。
なお、本取り組みによって検知した優先して対処すべき脆弱性（注5）に関して、国内のシステムについては2023年度末時点で対策を完了しています。海外リージョンについては2024年度中に対策を完了する予定です。

（注5） 優先して対処すべき脆弱性：
インターネットから直接アクセス可能かつ個人情報などの重要情報を保持しているシステム（アセット）に残存するリスクの高い脆弱性を指しています。



脆弱性の検出と是正

<脅威インテリジェンスの活用とアタックサーフェスマネジメント>

インターネット表出システムの脆弱性検知と対応を迅速化するため、脅威インテリジェンスの活用を積極的に進めています。脅威インテリジェンスでは、世の中の脅威動向や脆弱性に関する情報、富士通グループの表出システムにおける脆弱性の情報など、攻撃者の視点に立って実際に攻撃を行う初期段階の情報収集を行うことが可能であり、入手した脅威インテリジェンスに対し、インパクトを分析し、迅速な是正対応を実現しています。
さらに、ITアセット管理情報を基軸とした、インターネット表出システムの脆弱性スキャンと組み合わせ、攻撃者の視点からシステムの脆弱性をモニタリングする、アタックサーフェスマネジメントを実施しています。

監視の徹底

サイバーセキュリティを取り巻く環境は常に変化し、攻撃の手口は複雑かつ巧妙化の一途を辿っています。富士通グループではこのような状況下においても、「サイバー攻撃による侵入を100%防ぐことはできない」というゼロトラストな考え方を前提としたセキュリティ監視の強化に取り組んでいます。
セキュリティ監視に対する社内のガイドラインを整備し、定期的なシステム点検を行うことで現状把握と可視化を行うとともに、サイバー攻撃に対する検知能力向上と早期対処に向けた監視の健全化に取り組んでいきます。さらに重要システムに関しては、CISO直轄組織による第三者点検を実施することで監視を徹底するように進めています。
なお、国内の重要システムについては、2023年度末時点でサイバー攻撃に対する検知能力の強化・整備を完了しました。海外リージョンについては、2023年度末に整備計画の策定を完了しており、2024年度中に計画に沿った整備を予定しています。

インシデント対応

お客様の安心安全な事業活動を支える企業として、巧妙化・高度化していくサイバー攻撃に対して即応していく必要があります。そのため、平時においてセキュリティインシデントの発生を前提としたインシデント対応のポリシーや体制および対応手順を予め整備し、有事の際には組織としてエスカレーション・対応・復旧・通知という一連の対応を迅速に実施できるよう取り組んでいます。

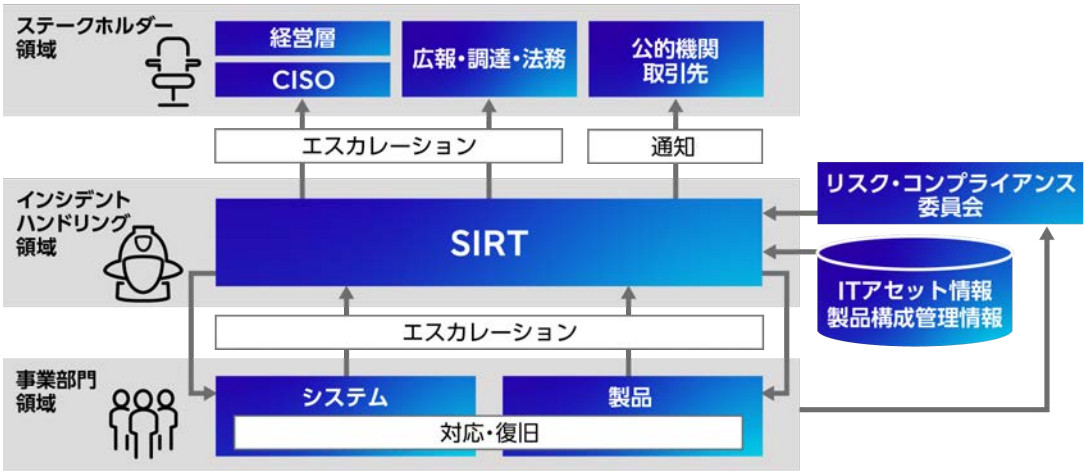
①エスカレーション
各部門で管理しているシステムや個人用端末においてセキュリティインシデントによる被害の発生を確認した場合、予め準備された手順に従い事象や被害範囲を確認し、すぐに実施可能な応急処置を行うとともに、被害が発生した旨のエスカレーションを行います。エスカレーション後は、セキュリティ統制部門からインシデント対応を支援するセキュリティ統制部門（支援担当）がアサインされ、連携してインシデント対応を行います。

②インシデント対応
インシデント対応では、セキュリティ統制部門とシステムを管理する部門が連携し、被害の拡大を防止するための対応として、インシデントが発生したシステムの停止や特定機能の無効化などを行った後、インシデントの発生原因を調査し根絶（一例として脆弱性に対する修正パッチ適用など）を行います。

③復旧
インシデント発生原因の根絶の後、システムや業務関連のデータを正常な状態に戻し、システムや業務を復旧します。

④通知
公的機関、被害を受けたお客様やお取引先などのステークホルダーに対する説明責任を果たすべく、インシデント情報の共有・報告を行います。

なお、上記のインシデント対応ポリシーや対応手順などを定義したインシデント対応ハンドブック・ガイドラインの策定、および国内への展開は2023年度に完了しており、海外リージョンについては、各国特有の要件などアラインメントを行い、2024年度に展開する予定です。



インシデント対応プロセス

＜インシデント対応の高度化＞

セキュリティインシデントに対応するには、ログ分析・マルウェア解析・ディスクフォレンジックなど技術的観点で事象を正確に理解する必要があります。加えて迅速かつ適切に対応するにあたり、全体の方針を決め社内外関係者と連携し、インシデント対応を行う必要があります。
富士通では、技術的な専門家と、解決までの道筋をリードするメンバーが連携し、エスカレーションプロセスなど各種プロセスに則り、セキュリティインシデントに対応しています。
さらに、攻撃者のツール、プロセス、アクセス手法などの情報を蓄積するとともに、継続的な対応メンバーのトレーニングにより技術的な知識やスキルを向上させています。また、グローバルを含めたインシデント対応の振り返りを行い、体制・ルール・プロセスの改善やノウハウ蓄積を含め、インシデント対応力を継続的に改善していくことで、迅速な対応と影響の極小化ができるよう取り組んでいます。

富士通製品・サービスにおけるリスクの未然防止

＜xSIRT体制＞

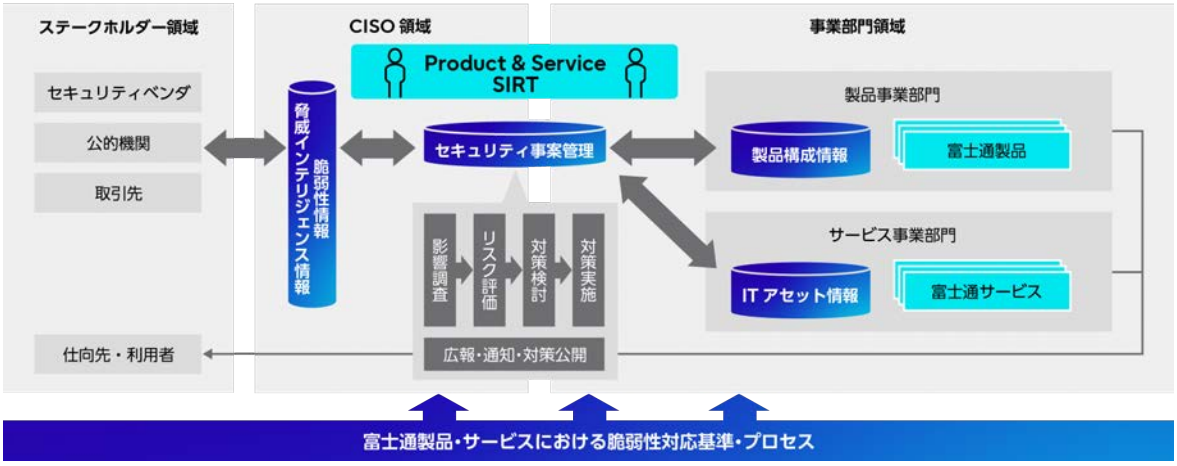
富士通の製品やサービスをご利用いただくお客様を守るため、製品構成情報、ITアセット情報、および脆弱性情報を含む脅威インテリジェンス情報の一元的な管理に加え、各部門において脆弱性対応を担当する情報セキュリティ責任者やPSIRT責任者の配置による xSIRT（注6）体制を整備し、製品やサービスの脆弱性に起因するリスクに対してスピーディーでプロアクティブな対応を可能としています。

（注6） xSIRT：Security Incident Response Team
企業内の製品・サービスを対象としてインシデント対応を行う組織や体制です。
PSIRTと同じような役割を担いますが、xSIRTはより広い範囲での対応を行う体制です。

＜プロセス策定＞

製品やサービスに与えるリスクの見積り、および製品やサービスに対するリスクを踏まえた脆弱性への対策検討・実行を迅速に遂行するために、脆弱性を起因とするリスクに対する対応基準やプロセスを策定し、統計解析や実際の対応実績を基に、プロセスの継続的な改善を実施しています。
これらの体制やプロセスに基づいて、迅速な脆弱性対応を実現することにより、脆弱性対応に係る期間を短縮し早期解決を図ることで、お客様における二次被害を防止し、お客様の事業継続への影響を極小化します。
なお、本施策による成果の一例となりますが、世界中で被害や影響が拡大し、CISA（注7）から重大リスク警告が発せられた脆弱性起因のサイバー攻撃発生の際に、富士通では該当システム特定と対処を迅速に実施し、情報搾取被害を回避しました。

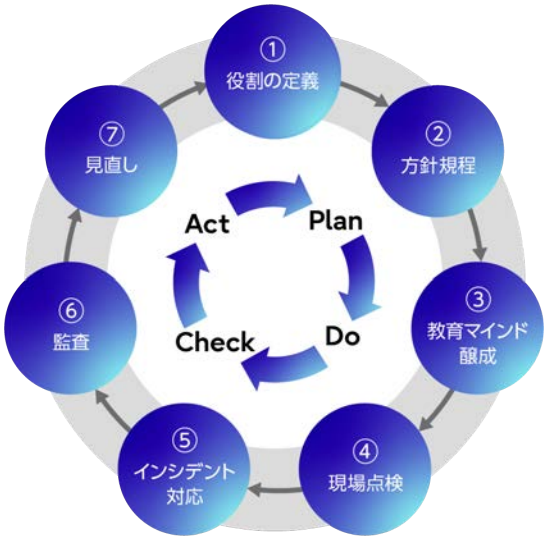
（注7） CISA：Cybersecurity and Infrastructure Security Agency
アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁



富士通製品・サービスにおける脆弱性対応体制

情報管理

富士通および国内グループ会社では、個人情報を含む他社秘密情報および、当社秘密情報を適切に保護するため、情報保護マネジメントシステムによる運用を行うとともに、「①役割の定義」から「⑦見直し」に至るPDCAを回しています。守るべき情報資産を明確にするために、情報の分類をグローバルで統一しつつ、部門ごとの自律した情報保護活動（業種・業態による規制等）において、お客様、お取引先の状況に応じた適切な管理を設定し、情報を保護する取り組みを実施しています。
また、適切な情報管理を支援するため、情報管理ダッシュボードなどを活用した様々な自動化支援ツールを提供し、実効性と安全性を兼ね備えた運用の実現に向け、改善も随時行っています。



情報保護マネジメントシステム

情報保護マネジメントシステムにおける主な活動内容は以下の通りです。

①役割の定義

CEOの下、CISOを中心としたグローバルなネットワークで、情報を管理保護する体制を構築し、各部門においては、部門ごとの管理責任者を任命するとともに役割を明確化し、適切な情報の取り扱いを推進しています。

②方針・規定

情報を正しく取り扱うため、必要な規程や手順を定め、年間の活動計画を立てています。
また、法改正への対応を含めた方針・規程の見直しを定期的に行っています。

③教育・マインド醸成

社員一人ひとりの意識とスキル向上のため、立場や役割に応じて必要な情報を提供するとともに、テレワーク等の環境変化に応じた様々な教育や情報発信を行っています。
毎年、役員を含む全社員を対象とした情報管理教育（eラーニング）の実施と、いつでも受講可能な情報管理の教材を社内に公開しています。
※2023年受講者実績：38,603名

④現場点検

保有している情報資産を特定、分類し、さらにリスク分析を行い、定期的な棚卸しを行っています。

情報保護管理体制および役割

情報セキュリティ講座 2023-2024

⑤情報管理インシデント対応

情報管理インシデントへの対応を迅速かつ適切に行うための体制や、エスカレーションルート、手順等をグローバルで整備しています。

⑥監査

部門ごとの情報管理の状態を情報管理推進部門が第三者観点で確認し、是正や改善の指示・提案を行っています。

⑦見直し

監査結果・インシデント・苦情を含む外部からの意見、法改正、環境の変化等を考慮し、情報保護マネジメントシステムの改善・見直しを図っています。

個人情報の保護

富士通では、グローバルでの個人情報保護体制を構築し、個人データ保護の強化を図っています。CISO直轄組織と法務部門主導の下、各リージョンおよびグループ会社と連携し、GDPR（注8）を含む各国の法令に準ずる対応を行っています。個人情報の取り扱いに関しては各国の公開サイトにてプライバシーポリシーを掲載し公表しています。

プライバシーマーク

（注8） GDPR：General Data Protection Regulation / 一般データ保護規則
2018 年5月25日に施行された個人データ保護を企業や組織･団体に義務づける欧州の規則で、個人データの欧州経済領域外への移転規制やデータ漏えい時の72 時間以内の報告義務などが規定されています。

日本では個人情報の保護を目的とし、2007年8月に一般財団法人日本情報経済社会推進協会よりプライバシーマーク（注9）の付与認定を受け、現在も継続的に更新し、個人情報保護体制の強化を図っています。国内グループ会社でも、必要に応じて各社でプライバシーマークを取得し、個人情報管理の徹底を図っています。また、部門ごとの情報管理の状態を情報管理推進部門が第三者観点で確認し、是正や改善の指示・提案を行っています。2023年度は全部門にて内部監査を実施しています。

（注9） プライバシーマーク
JIS Q 15001 ：2017 に適合した個人情報保護マネジメントシステムの下で、個人情報を適切に取り扱っている事業者に付与されるものです。

なお2023年度、富士通社内に設置した「富士通お客様相談センター個人情報保護総合窓口」へ寄せられたお客様プライバシーに関する相談・苦情はありませんでした。また、個人情報保護法令に基づいた政府や行政機関へのお客様情報の提供実績もありませんでした。

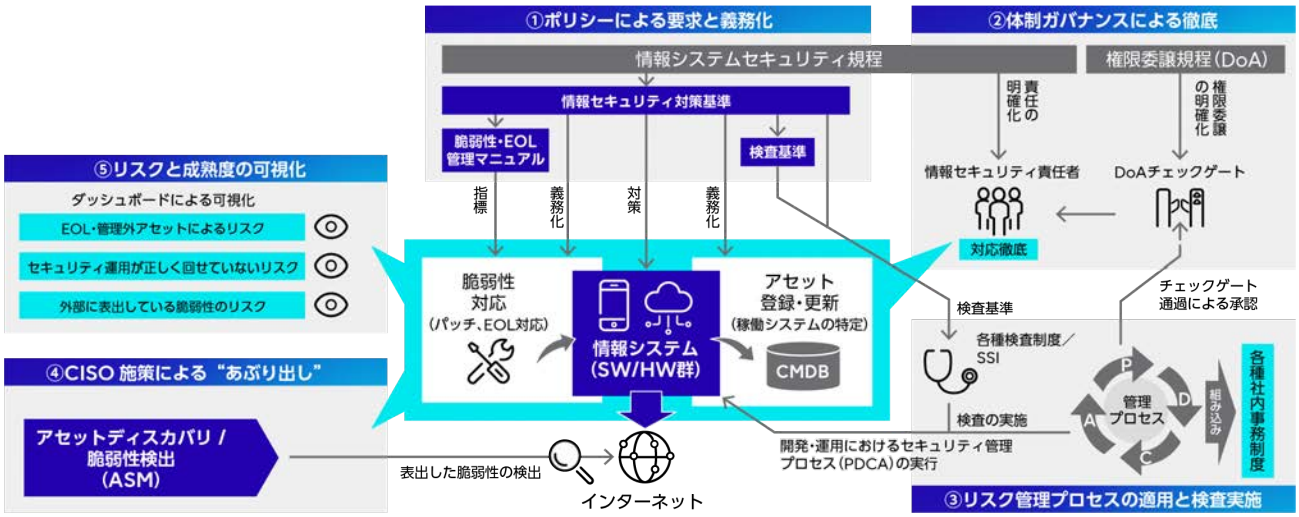
情報システムの認証取得

富士通グループは、情報セキュリティの取り組みにおいて、第三者による評価・認証の取得を積極的に進めています。

- 第三者評価・認証監査結果（リンク）

ガバナンス強化

富士通では、グローバルでセキュリティガバナンスを強化するため、複合的なアプローチによりセキュリティリスクの極小化に取り組んでいます。
グローバル共通でのガバナンスを徹底させるため、「①ポリシーによる要求を義務化」することで対応すべきことを明確化し、さらに、情報セキュリティ責任者体制による「②体制ガバナンスによる徹底」で対応を徹底、冒頭の「サイバーセキュリティ」に関する対策である「③検査と監査の実施」「④ASMによる"あぶり出し"」を有機的に組み合わせることで、各部門が自律的に行う確実なセキュリティ対策を実現しています。
また、次項「セキュリティ成熟度のメータリング」などの施策も加え「⑤リスクと成熟度の可視化」をすることで、自律的にセキュリティ対策を講じる風土を醸成し、サイバーセキュリティ対応の自浄作用を促進しています。



ガバナンス強化施策の全体像

セキュリティ成熟度のメータリング

富士通では、「全社セキュリティリスクマネジメントスキーム」による組織ガバナンス強化を円滑に推進するための仕組み（両ループの共通接点）として、各種セキュリティ対策の状況を把握するための「セキュリティリスク・成熟度モニター」を活用しています。
リスクを可視化する「リスクモニター」と、成熟度を可視化する「成熟度モニター」の2つの機能を持っており、経営層、各部門の双方で同一の尺度による「リスクの把握」および「成熟度のチェック」が可能となっています。

<リスクモニター>

「リスクモニター」では、富士通本社およびグループ会社の各部門を俯瞰して、リスクに関する数値を可視化しています。前述の脆弱性スキャンなどの施策により検出したリスクについて、重要度別の是正残数をヒートマップやグラフで表示しており、重要度の高いリスクを優先した対応が可能となっています。

＜成熟度モニター＞

「成熟度モニター」では、脆弱性の発生状況や、脆弱性を是正するまでの対応速度、といった要素をデジタルにスコアリングしています。富士通本社およびグループ会社の各部門の成熟度を月単位で可視化することで、現在の状態や目標との差異の把握による、具体的な施策や是正対応を自律的に講じる風土を醸成し、各部門のサイバーセキュリティ対応の自浄作用の促進を図ります。

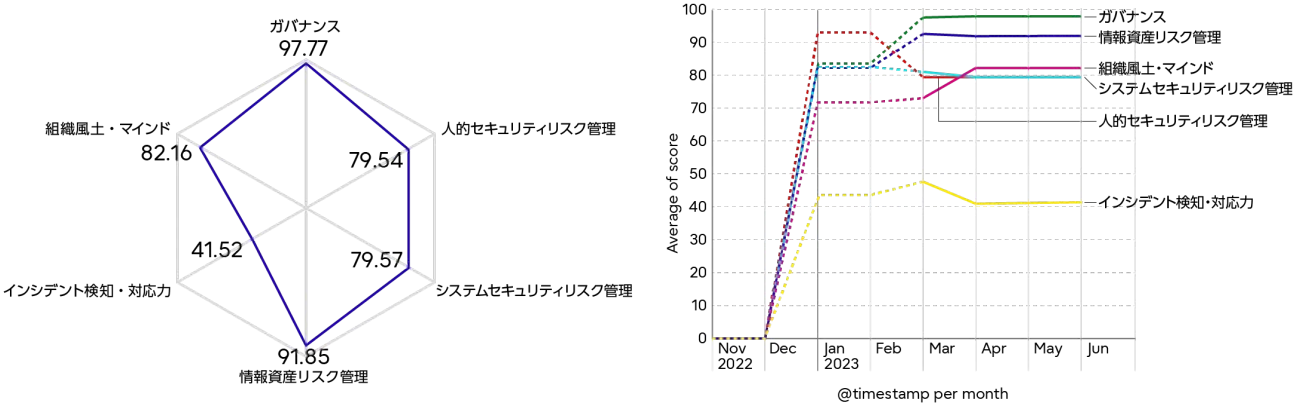
セキュリティ成熟度評価の指標は、国内外で実績のあるサイバーセキュリティ能力成熟度モデルC2M2（注10）や、セキュリティインシデントマネジメントの成熟度モデルSIM3（注11）を参考にした上で、成熟度スコアをセキュリティ施策におけるデータから機械的にスコアリングする方法を独自に取り入れて評価しています。評価の内容については、ガバナンス、人的セキュリティリスク管理、システムセキュリティリスク管理、情報資産リスク管理、インシデント検知・対応力、組織風土・マインドのカテゴリー別に6軸で成熟度をスコアリングしています。

なお、上記富士通内部のメータリングに加え、社外のセキュリティレイティングサービスなども利用しており、第三者から見た客観性の高い富士通のセキュリティ対応状況のスコアリングについて継続的に確認し、サイバーセキュリティ対応力強化を図っています。

（注10） C2M2：Cybersecurity Capability Maturity Model

（注11） SIM3：Security Incident Management Maturity Model

以下は、成熟度モニターの表示例となります。



会社成熟度　　成熟度スコア推移（会社全体）

セキュリティ成熟度の可視化グラフ（サンプル）

フレームワーク・ルール・プロセスの周知・浸透

富士通では、グローバルでセキュリティ対策レベルを統一し、底上げするため、主に 2 つの取り組みを行っています。

＜富士通グループ情報セキュリティ対策基準＞

1つ目は、富士通グループにおけるセキュリティ対策の基準となる「富士通グループ情報セキュリティ対策基準」の策定です。グローバルスタンダードであるNIST（注12）の「CSF」（注13）、「SP800-53」（注14）および「ISO/IEC27002」を参考に165 の管理策から構成されており、情報システムの重要度等に応じた管理策の適用がルール化されています。また、これら管理策の適用を支援するマニュアルまたはガイドラインといった資材を整備しています。

＜リスクマネジメントフレームワーク＞

2つ目は、富士通グループにおけるセキュリティリスク管理の枠組みである「リスクマネジメントフレームワーク」の策定です。グローバルスタンダードであるNISTの「SP800-37」（注15）を参考に、各組織および各情報システムが持つセキュリティリスクを識別し、組織的かつ適切に管理するためのプロセス群が規定されており、各組織における定期的なリスクマネジメントと、各情報システムの開発フェーズおよび運用フェーズにおけるリスクマネジメントをルール化するとともに、これらプロセス群を富士通グループの各種業務プロセスに組み込むことで周知・浸透を図っています。
なお、国内は、2023年度より「リスクマネジメントフレームワーク」の運用を開始しており、2024年度は海外リージョンへ運用を拡大する予定です。

これら2つの取り組みを富士通グループ内に展開し、「リスクマネジメントフレームワーク」プロセス群の実行を通じて、「富士通グループ情報セキュリティ対策基準」に基づく管理策を各組織および各情報システムに適用するとともに、継続的な改善プロセスを回していくことにより、セキュリティ対策の効果的な実装とセキュリティ・バイ・デザインの実現に努めています。

（注12） NIST : National Institute of Standards and Technology

（注13） CSF：Cybersecurity Framework

（注14） SP800-53：NIST SP800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations

（注15） SP800-37：NIST SP800-37 Rev.2 Risk Management Framework

セキュリティ訓練・マインド醸成・人材育成・責任者成熟化

上記で述べたセキュリティ成熟度の向上を下支えする施策の1つとして、セキュリティ教育・訓練に取り組んでいます。中でも近年発生したインシデントの再発防止にとりわけ注力しています。具体的には全社必修教育としている情報セキュリティ教育において、最新のセキュリティ脅威の動向やインシデント事例を共有するとともに、事案対応から学んだ教訓と必要とされる施策の周知徹底を行い、従業員一人ひとりのセキュリティマインドの醸成とスキル強化に取り組んでいます。

＜セキュリティ教育、訓練＞

情報管理およびサイバーセキュリティに関する基本的な教育に加え、最新動向や事案対応から学んだ教訓を周知徹底しています。また、システム管理者向けにはシステム監視のガイドラインを発行するなどして、専門人材のスキルアップにも取り組んでいます。インシデントを完全に防ぐことは難しいため、「有事を起こさないための取り組み」から「有事が起こることを前提とした取り組み」へ見直し、全社のインシデント対応力強化に取り組んでいます。その1つとして、富士通グループでは、役員・社員を対象にした全社訓練を半年に1回の頻度で実施しています。具体的には、社会的インパクトのあるインシデントが発生した際にも、迅速な対応と影響の極小化を目的に、役員や各部門が参加するインシデント訓練、ビジネスや社内業務に携わるSE・ビジネスプロデューサーを対象に実践的なシナリオを想定した訓練を実施しています。訓練での気づきは、「インシデント対応」の項目でご紹介した「インシデント対応ハンドブック・ガイドライン」に適宜反映し、各部門と共有しています。さらに、従業員一人ひとりのセキュリティマインドの醸成を目的とした標的型メール訓練も継続的に実施しています。
※2023年度の訓練実施回数：全社訓練2回、標的型メール訓練1回

＜セキュリティ体制強化と人材育成＞

富士通グループとして、CISOおよびCISO直轄組織からの定期的な社内への情報発信を行うとともに、各部門に配置したセキュリティ責任者を通じてセキュリティ施策を展開し、セキュリティに関する考え方や行動の変革に取り組んでいます。
また、2023年より、セキュリティ人材像、特に各部門に配置しているセキュリティ責任者の人材像を再定義し、プロフェッショナル認定制度の見直しを行いました。セキュリティ責任者の役割と責任を明確化したうえで報酬制度を含めた見直しを行い、2023年1月より先行して国内から各部門のセキュリティ体制を強化しています。
なお、前述の「セキュリティ成熟度のメータリング」による可視化によって各部門の実態を共有するとともに、セキュリティ責任者コミュニティやセキュリティ責任者会議・分科会などによる定期的コミュニケーションを通じ、各部門とともに組織のセキュリティ成熟度向上に取り組んでいます。

品質への取り組み

方針

富士通グループは、様々な製品・サービスを提供することを通して、社会の発展のみならず、多様なお客様の事業や生活を支えるという重要な責任を担っています。私たちは「信頼ある社会づくり」に貢献するため、テクノロジーを活用し、富士通グループ一丸となって、お客様システムの安定稼働と品質向上に取り組んでいます。

富士通グループでは、Fujitsu Wayの大切にする価値観である「信頼」を実践するため、「富士通グローバル品質指針」を定めています。この指針は、「品質」を私たちの根幹として捉え、グローバルに安全・安心な製品・サービスを提供し続けるための取り組み方を示しています。
Fujitsu Wayおよび品質指針に則り、グループ共通で守るべきルールとしてのFujitsu Group Global Policyに Quality Policy（Standard Policy for Quality Management）とGlobal QualityfRulesを定めています。また、FujitsufGroupfGlobalfPolicyの下、国や製品・サービスの特性、お客様の要求事項、法令・規制などに応じた規程・標準類を整備しています。

富士通グローバル品質指針と品質規格体系

例えば、国内では、「富士通グループ品質憲章」および品質保証関連5規程（出荷・登録・リリース規程、安全推進規程など）を定めています。企画・計画、設計から検証、生産、販売、サポートまでのすべての過程で、これら憲章・規程に基づいた活動を展開し、お客様およびお客様を取り巻く事業環境の変化を先取りした製品・サービスを提供し続けています。

製品・サービスの安全に関する実践方針

富士通グループは、安全・安心な社会を構築するという社会的責任を認識し、事業活動のあらゆる面において製品・サービスの安全性を常に考慮し、次の方針の下で実践しています。

1. 法令等の遵守
   製品・サービスの安全に関する法令を遵守します。

2. 安全確保のための取り組み
   製品・サービスの安全を確保するため、さまざまな利用態様を踏まえて製品・サービスの安全化を図り、必要に応じた対策を行います。さらに法令で定められた安全基準に加え自主安全基準を整備、遵守し、継続的な製品・サービスの安全性向上に努めます。

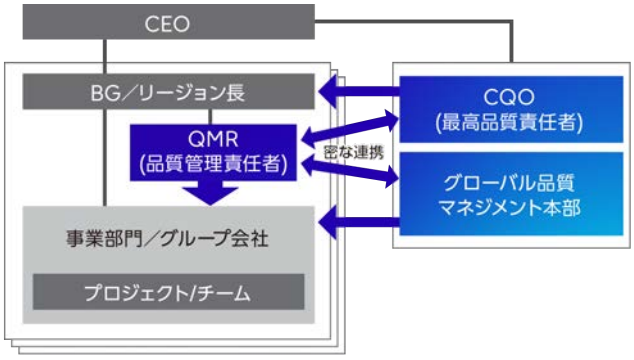
3. 誤使用等による事故防止
   お客様に製品・サービスを安全に利用いただくため、取扱説明書、製品本体等に誤使用や不注意による事故防止に役立つ注意喚起や警告表示を適切に実施します。

4. 事故情報等の収集
   製品・サービスの事故情報および事故につながり得る情報等の安全性に関する情報をお客様等から積極的に収集します。

5. 事故への対応
   製品・サービスに関して事故が発生した場合、直ちに事実確認と原因究明を行い適切に対応します。製品・サービスの安全性に問題がある場合、お客様等に情報提供を行うとともに、製品回収、サービスの修復、その他の危害の発生・拡大の防止等の適切な措置を講じます。富士通グループは、重大製品事故が発生したときは、法令に基づき、迅速に所轄官庁に報告を行います。

品質マネジメント体制

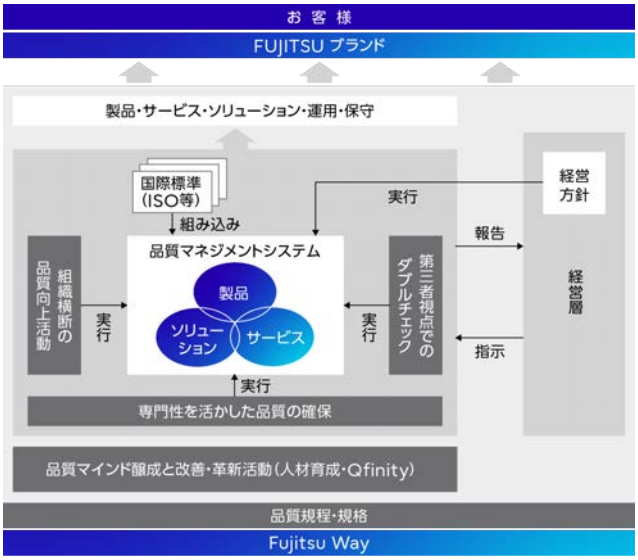
富士通グループでは、2023年6月に専任のCQO（Chief Quality Officer：最高品質責任者）を任命し、グループ全体で製品・サービスの品質強化を図っています。
各BG（ビジネスグループ）・リージョンにQMR（Quality Management Representative：品質管理責任者）を設置し、CQOのもとグループ全体の品質管理を統制しています。CQOの意思決定に従い、ヘッドクォーターとしてグローバル品質マネジメント本部がグループ共通の活動方針や標準化・品質向上施策を策定し、それらを各組織のQMRと共有、密に連携することで、より現場に即した展開・適用、品質管理を行い、お客様に一貫性のある最適な品質の製品・サービスを提供するよう努めています。



品質マネジメント体制

品質を支えるフレームワーク

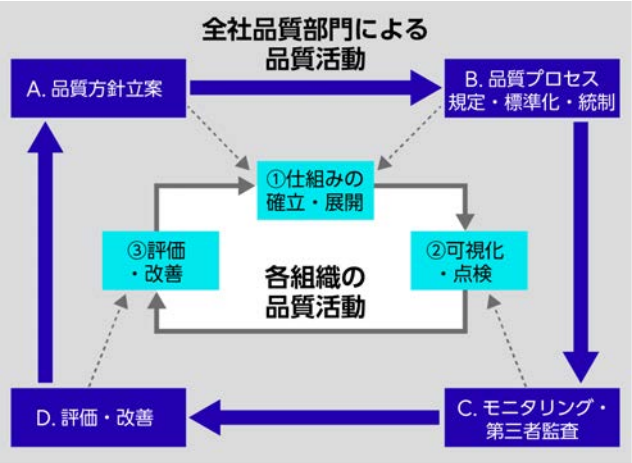
お客様のニーズや期待に応えられる製品・サービスの品質を一貫して提供するためには、企画・計画から開発、製造、試験、販売、運用・保守に至るまで、事業部門、共通部門、ビジネスパートナーなど社内外の様々な組織との連携が必要であり、これら組織が一体となる体制や仕組みが基盤として必要不可欠です。
そのため富士通は、製品・サービスに応じ、これら関連部門と連携しながら品質マネジメントシステム（QMS：Quality Management System）を構築し、運用しています。QMSの運用にあたっては、ISOなどの国際的な認証規格にも照らして進捗を定期的に検証し、より良い品質の実現を目指してプロセスの改善を図っています。



品質を支えるフレームワーク

全社品質向上サイクル

富士通グループの品質活動には、全社品質部門による品質方針を起点とした品質活動（図［全社品質向上サイクル］の“全社品質部門による品質活動”部分）と、各組織にて品質マネジメントシステムの整備・実践を行う活動（図［全社品質向上サイクル］の“各組織の品質活動”部分）があります。それぞれがサイクルを回し、連携することで、グループ全体で戦略的に品質向上に取り組んでいます。



全社品質向上サイクル

A. 品質方針立案

品質目標の設定・見直しを行い、その実現のための品質戦略・方針を立案し、富士通グループ全体に展開しています。また、品質方針に沿った活動が行われるよう、監視・コントロールを行います。

B. 品質プロセス規定・標準化・統制

品質方針を踏まえ、強化すべきポイントに対して、具体的なプロセスや手法などの標準化を進め、現場への展開・統制を行っています。また、品質方針に沿って、組織横断での品質向上活動を推進しています。

さらに、品質に関する標準化の周知・展開に加えて、プロジェクトの良い実践事例から他のプロジェクトでも広く活用できるように汎用化・形式知化したベストプラクティスを提供したり、プロジェクトの失敗事例から教訓を整理し誰でも活用できるかたちで提供するなど、ナレッジの共有をすすめ、プロジェクトの標準化を推進しています。

C. モニタリング・第三者監査

各組織のプロジェクトを監視し、品質リスクの予兆を捉え、エスカレーションするとともに対策を行います。品質懸念がある場合は、第三者が現物確認や監査・点検を行い、是正・改善します。

<お客様に提供している製品・サービスに重大な品質問題が発生した場合>

リスクマネジメント規程に従い、現場から直ちに本社リスク・コンプライアンス委員会へ報告が行われ、当委員会からの指示の下で、関連部門が共同で品質問題に対応、再発防止策を検討します。立案した再発防止策はQMRを通じて他部門へも横展開し、富士通グループ全社で品質問題の再発防止に努めています。

D.評価・改善

定期的に品質状況を整理・分析し、必要に応じて追加施策を検討し、各組織のビジネス特性を踏まえてQMRへ改善を指示します。経営層にも定期的に報告のうえ、経営層の判断・指示に従い、対応を実施します。
また、Qfinity（注1）の活動を通して、優れた成果を出した活動を表彰するとともに、富士通グループ全体に横展開し、グループ全体の品質向上につなげています。

（注1） Qfinity
「Qfinity」とは、Quality（質）とInfinity（無限）を合体させた造語（インナーブランド）で、「一人ひとりが無限にクオリティを追求する」という富士通グループのDNAを表しています。
Qfinityは、2001年度から富士通グループ全体で開始した「社員一人ひとりが主役となり、製品やサービスの品質を向上し続ける改善・革新活動」です。Qfinityを通して、各職場での品質向上活動を推進し、製品・サービスの品質向上に取り組んでいます。

品質ガバナンス

CQOの下、富士通グループ全体の品質ガバナンスを強化し、重大インシデントの再発防止と製品・サービスの品質強化に取り組んでいます。
品質ガバナンスの強化にあたっては、品質リスクを評価するための共通基盤やサービスデリバリーを支える品質保証プロセスを富士通グループ内に展開することで、リスクを正しく評価し、対策を徹底します。
初めての事業への挑戦が増え、情報システムが複雑化する中で、これらの仕組みをベースに、素早く適切な判断を行い、さまざまなリスクに備えています。

品質統制・リスクモニタリングを支える設計・運用基盤の強化

開発プロジェクトの進捗やテスト密度・不具合検出率など、開発現場で得られる品質に関わる情報を共通プラットフォームであるFujitsu Developers Platformに集約し、EVM（Earned Value Management）や品質指標と組み合わせてタイムリーに解析することにより、開発現場の品質や出荷の判定を、より客観的に評価する仕組みを構築しています。

現場の判断を客観的に評価する仕組み

サービスデリバリーを支える品質保証プロセス

富士通グループでは、お客様へのこれまで以上の高い価値提供とシステムの安定稼働を目指し、新たなサービスデリバリーの型として、組織に依存しないプロジェクト体制「One Delivery」への変革を進めています。One Deliveryでは、共通の「One Delivery品質保証プロセス」に則ってプロジェクト運営を行い、一元的にリスクマネジメントを行えるようにしています。

「One Delivery品質保証プロセス」には、これまでの品質問題の傾向を踏まえた4つのポイントがあります。まずは「リソース統制」で、スキルアンマッチなどの問題を抑止します。次に「決裁の合議制」に基づき、商談・プロジェクトの推進を客観的・多角的な視点で判断します。そして、「テクノロジー統制」で採用する技術の適正化と実現可能性の向上を目指します。最後に、「商談・品質統制」により、問題予兆プロジェクトを早期に検出します。
富士通グループ全体でより高品質で安定したサービスを提供できるよう、この「One Delivery品質保証プロセス」の適用をすすめるとともにプロセスの改善を図っています。

One Delivery品質保証プロセス

2023年度実績

製品の安全性に関する法令違反

- 製品の安全性に関する法令違反：1件（電気用品安全法：安全設計要求の不適合（改修済み））

製品安全に関する情報の開示

- 情報開示件数：0件の重大製品事故
- 製品安全に関する重要なお知らせ
  https://www.fujitsu.com/jp/support/safety/

- ノートパソコンのバッテリ発火の未然防止策
  当社は、バッテリパック製造過程におけるバッテリ内部への異物混入に起因した発火事故の拡大防止のため、これまで3回にわたり、バッテリパックの交換・回収のお願いをしています。しかしながら、すでに交換・回収を実施しているバッテリパック以外にも、発生率は非常に低いものの発火事故が発生しています。
  これらの発火事故に対する未然防止策として、バッテリの内圧が上昇する現象を抑制することが効果的であると判明しており、当社では、2017 年2月9日より、2010 年から2016 年に販売開始したノートパソコンを対象にバッテリ充電制御機能のアップデートを当社webサイトにて提供させていただいています。
  さらに、アップデート対象のパソコンをご使用いただいているすべてのお客様に適用していただくため、「バッテリ充電制御機能アップデート」を、Microsoft社のWindows Updateにより対象の皆様のノートパソコンに配信させていただく施策を2018 年11 月より実施しています。

製品の安全性に関する法令以外の違反

- 製品の情報とラベリングの違反：0件
- 外国為替及び外国貿易法の違反：1件（該否判定時の書類記載誤り（修正済み））

ISO9001／ISO20000認証取得状況

富士通は、QMSの下で継続的なプロセス改善に取り組んでいます（以下、2023年9月時点）。

- ISO 9001：21 本部 認証
- ISO 20000：5本部 認証

お客様とともに

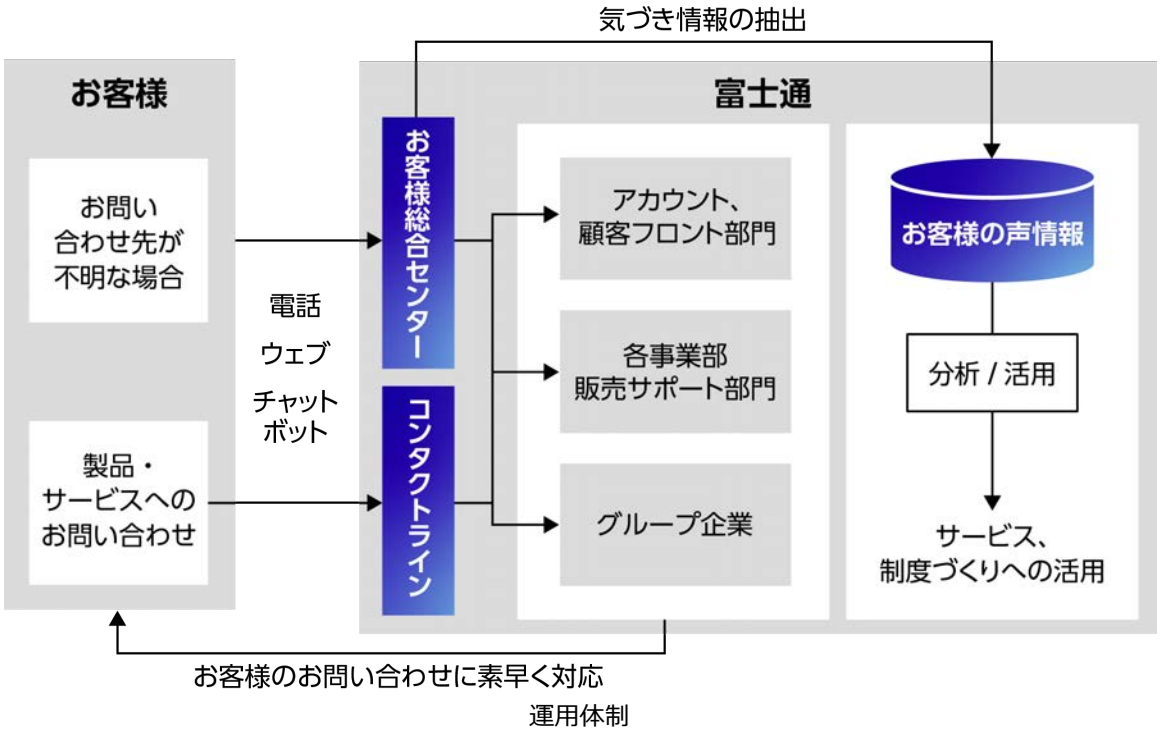
お客様の満足度向上のために

社会や経済の環境がめまぐるしく変化し将来の予測が困難な時代においては、お客様の要望や利用シーンの変化を素早く的確に捉え、“お客様起点”で発想・行動しながら自らを変革していくことが求められます。

富士通お客様総合センター／富士通コンタクトラインの運営

「富士通お客様総合センター」と「富士通コンタクトライン」では、お客様からのお問い合わせに対して迅速かつ的確にご回答できるよう、複数の部門との連携やAI、チャットボットを活用し対応に当たっています。さらに、対応状況の監視による回答漏れ・回答遅延の防止の役割も果たしています。迅速な回答によってお客様満足度を高めるだけでなく「お客様の声情報」を分析し、製品・サービスの開発や品質向上に活用しています。

- 富士通お客様総合センター／富士通コンタクトライン
  https://www.fujitsu.com/jp/about/resources/contact/others/customer/



宣伝・広告の方針

富士通のあらゆる宣伝・広告活動は、法令や社内規程を遵守し、公正かつ適切な表示・表現を用いるよう努めています。2024年度も、イノベーションによって社会に信頼をもたらし、世界をより持続可能にしていく当社の取り組みについて、広く認知いただける活動を推進していきます。宣伝方針ならびに費用対効果に関しては、目標（KPI）を設定するとともにPDCAサイクルを回して、KPIを達成しているかを検証しています。

なお、富士通はビジネスモデルの変更により、景品表示法の対象となる製品・サービスは2018 年度以降保有していません。

また、富士通で導入しているお問い合わせ対応システムにて、随時広告に対するご意見を承っています。いただいたご意見は真摯に受け止め、対応すべき件に関しては丁寧にお応えするなど、さらなるコミュニケーションを図っています。

- 広告宣伝
  https://jad.fujitsu.com/