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。

- **[PDF] 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（2025年6月23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、2025年6月23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。

2024年度においては、取締役会を15回（内、臨時取締役会３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、毎月の定例取締役会に加え、必要な場合には臨時取締役会を開催して、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取締役会で決議した中期経営計画の進捗、②マテリアリティをビジネスに結び付ける取組み、③内部統制体制の整備・運用及びリスクマネジメントの監督、④重要なM&Aや再編事案のモニタリング、⑤取締役等のサクセッションプランニングの5テーマを設定し、これらに重点を置いて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、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るとともに、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からは、任務遂行状況に関する毎月の報告及び当事業年度に発生した個別のリスク事案への対応等についてタイムリーな報告を受け、継続的な監督を行いました。また、富士通は、取締役会の実効性を高め、企業価値の向上を図るため、取締役会の実効性評価を毎年実施しています。2024年度は、2023年度に引き続き、全ての取締役・監査役を対象とするアンケートおよびアンケート回答に基づく各役員への個別インタビューを実施

し、分析・評価を行ったうえで、取締役会において具体的な対応施策を議論しました。これらを通じて認識された課題の解決策として、①中期経営計画の達成に向けた課題を確認し重要な経営テーマを集中的に議論する「集中討議」の枠組みを新設し、②取締役会を効率的に運用する取り組みとして、録画映像を使って付議議案を事前に説明する仕組みを導入するなどの施策を実行することで、取締役会の実効性の更なる向上を図りました。

＜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。

2024年度においては、監査役会を９回開催し、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を行いました。また、常勤監査役から社外監査役への重要な事項の報告及び検討等を行いました。
2024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2024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。

2024年度においては、独立役員会議を12回開催し、経営方針の進捗や、M&Aを含む富士通および富士通グループの事業再編などの経営上の重要な事項を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。また、取締役会決議を要する重要案件の事前説明を議題とする場合は、会議体を「案件事前説明会」と構成して常勤監査役もオブザーバー参加する枠組みを新設し、当事業年度において2回開催しました。

＜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

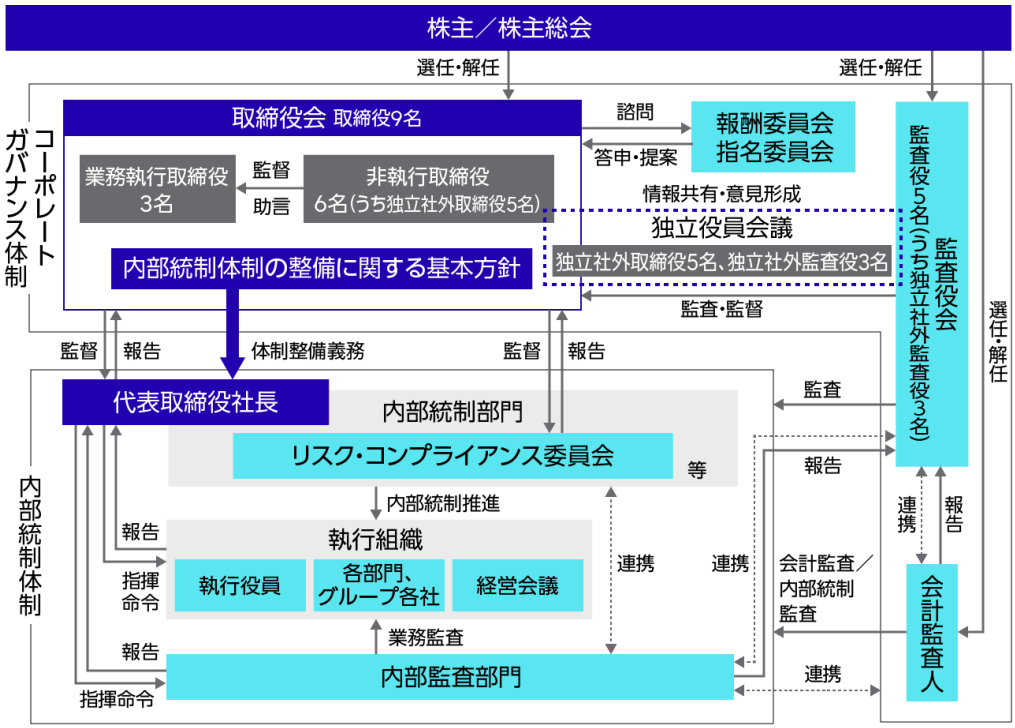
手続きと方針」に基づき、役員候補者について審議し、取締役会に答申または提案しています。また、報酬委員会は、当社の「コーポレートガバナンス基本方針」に定めた「役員報酬の決定手続きと方針」に基づき、基本報酬の水準と、業績連動報酬の算定方法を取締役会に答申または提案しています。

2025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。なお、両委員会は、「コーポレートガバナンス基本方針」において、非執行役員で構成し、そのうち過半数を独立社外取締役とすることとし、また、両委員会の委員長は独立社外取締役が務めるものとしています。なお、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：古城 佳子（独立社外取締役）
  委員：佐々江 賢一郎（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：平野 拓也（独立社外取締役）、小林 いずみ（独立社外取締役）

なお、2024年度は、指名委員会を10回、報酬委員会を６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、取締役の報酬水準及び業務執行取締役の業績連動報酬における評価指標の内容等について検討を行い、2024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、スキルマトリックス、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、役員報酬の開示範囲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。（2025年6月23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。

- **[PDF] 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 P13」

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。

- **[PDF] 第125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（2025年6月23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	執行役員専務、CHRO		
非執行	古田 英範	会長		
	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			○
	小林 いずみ			○

- [PDF] 取締役（2025年6月23日）

2024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	15回	100%
監査役会	9回	97.8%

- [PDF] 2024年度 取締役会・監査役会の出席状況

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。なお、各取締役・監査役が有するスキルのうち、当社の取締役会が特に期待するスキルに「○」を記載しています。

取締役（2025年6月23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
取締役会長	古田 英範		男性	日本	○		○	○	
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	古城 佳子	○	女性	日本			○		○
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	○		○	○	
取締役	小林 いずみ	○	女性	日本		○	○		○

- **[PDF] スキルマトリックス（取締役）**

監査役（2025年6月23日現在）

監査役 氏名	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	小関 雄一		男性	日本		○	○
常勤監査役	湯浅 一生		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	○		

- **[PDF] スキルマトリックス（監査役）**

スキル項目の定義

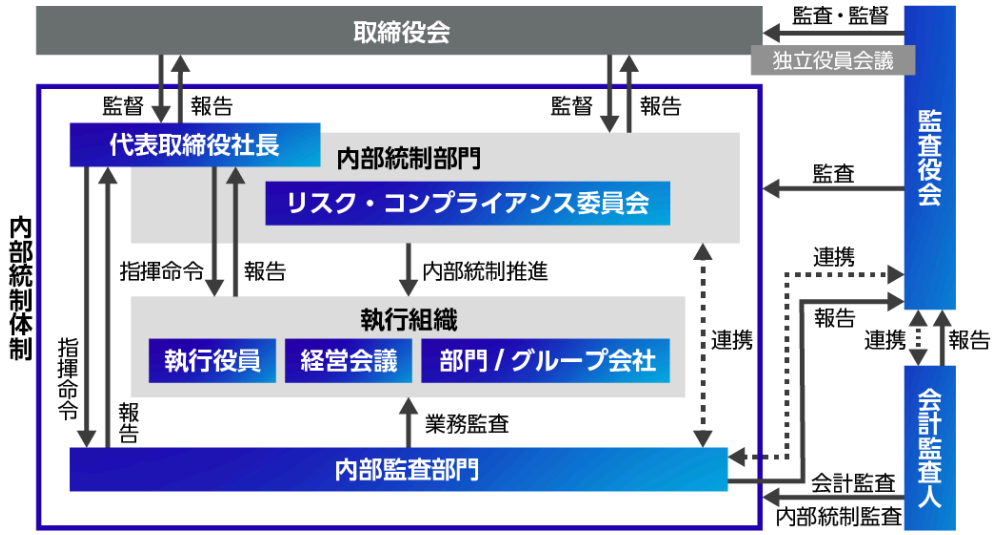
	項目	定義
取締役	企業経営	経営トップまたは経営幹部として培った企業経営に関する経験
	財務・投資	企業における財務、資本または投資の戦略立案・実行の経験あるいは金融業界や投資業務における経験
	グローバル	企業における海外ビジネス担当経験、海外拠点マネジメント経験、海外企業勤務経験または国際的な団体での活動・リード経験
	テクノロジー	テクノロジー企業・団体における技術戦略立案または研究開発に関する経験あるいは先端科学技術分野における経験
	ESG・学識・政策	行政機関、業界団体、大学・研究機関等における代表者または研究に従事した経験あるいはESG・学識・政策に関連する対外発信の経験
監査役	法務・コンプライアンス	法曹、法律学者または企業法務・コンプライアンスの責任者等の経験
	財務会計	公認会計士、税理士等の専門資格保有者または財務会計・ファイナンス全般の経験
	業務プロセス	企業の業務プロセス全般の統括管理に関する経験

- **[PDF] スキル項目の定義**

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（独立役員会議含む）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 Officer）の下、リスク情報全般の把握と迅速かつ適切な対応を行うとともに、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し、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）による内部監査を行い、体制が正常に機能していることを確認しています。



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

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、富士通グループを取り巻く環境変化をふ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
- 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ふまえ、重要リスクのランキング化およびリスクマップの作成を実施。リスクマップでは4象限にプロットすることで重要リスクの選好度を4段階に評価（回避/移転/低減/保有）。評価結果および顕在化したリスクの状況から、重要度を評価し重点対策リスクを選出。
- 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ふまえた分析を実施、重点対策リスクや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

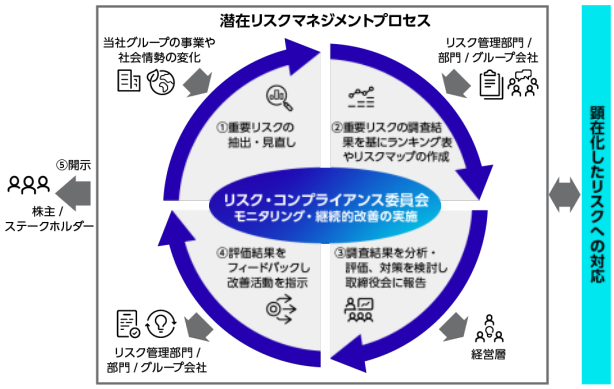
【顕在化したリスクへの対応】

- 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

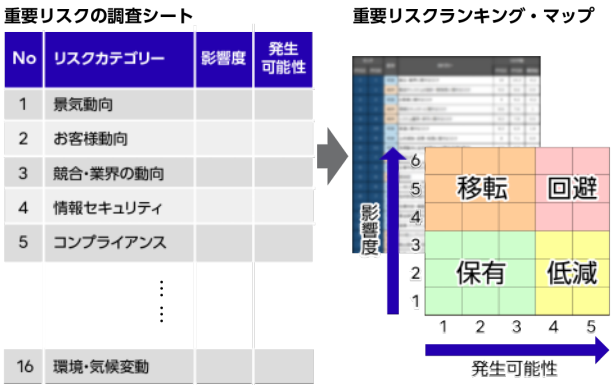
このようなプロセスを繰り返し実行するとともに1年を通してリスク管理部門による定期的な確認を行うことで、グループ全体のリスクの低減と顕在化した際の影響の極小化に努めています。

【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ふまえたうえで、富士通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。2025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）

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

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。
2024年度の教育実績については、「2024年度実績」をご参照ください。

全社防災

富士通および国内外グループ会社は、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」を構築しています。
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、2024年度の活動実績は、「2024年度実績」をご参照ください。

- **[PDF] 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います。 富士通および国内外グループ会社は、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。
富士通グループでは、災害や感染症への対応においてお客様、お取引先、社員およびその家族の安全や健康の確保を最優先としつつ、お客様への製品・サービス提供の継続および災害や感染症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、2024年度の活動実績は「2024年度実績」をご参照ください。

- **[PDF] BCM活動の取り組みや感染症対策、サプライチェーンのBCM**

2024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：38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ラーニングを提供。

富士通グループ新任幹部社員向け研修：1,012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ラーニングにて実施。

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ラーニングを実施。

防災フォーラム：357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・事業継続担当者および全従業員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

重大インシデント対応訓練（2024/4 Europeリージョン：143名、2025/1 Uvanceビジネス：88名）：合計231名 —

重大インシデントが発生した際の対応（暫定対処、原因究明、現場・リージョンとHQとの連携、顧客対応、個人情報漏洩対応、メディア対応等）の強化として現場対象部門および経営層での対策会議形式の二段階で訓練を実施し、インシデント対応プロセスの検証を行った。
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：2024年度のテーマ「中四国地方広域地震」 —

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、危機事象発生による人的リソースの損失を想定したアウェアネス訓練を実施した。また、各組織のBCPに沿ってオペレーションや複数組織間連携をシミュレーションすることにより課題を洗い出し、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

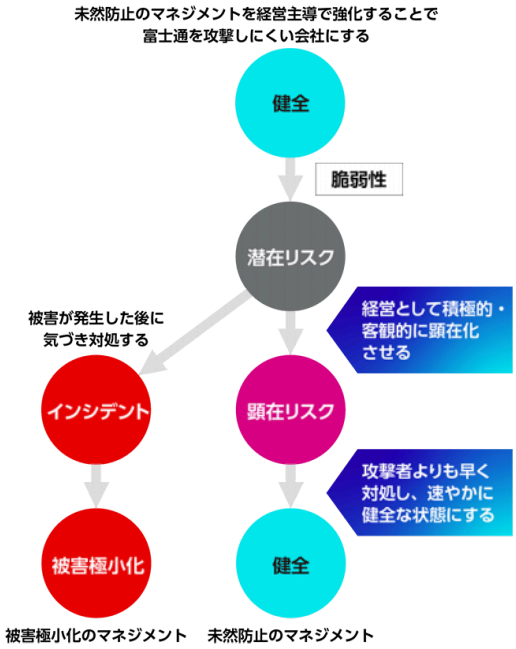
世界は、以前にも増して多くの深刻なサイバー攻撃にさらされ様々な被害を受けています。インターネットに公開されたシステムを見つけ出す技術が進歩し誰もが弱点を容易に見つけ攻撃することが可能になっており、未知の脆弱性を悪用した攻撃や脆弱性公表から数日以内での攻撃など、想定すべき脅威や攻撃手法はますます高度になっています。
そういった環境において、富士通グループは、イノベーションを通じて社会に信頼をもたらし、世界をより持続可能にしていくことをパーパスに掲げ活動しています。富士通は多くのお客様とともに社会に対する価値創造を行っており、富士通が一度被害を受ければその影響は自社全体に留まらず、お客様・社会にまで影響を及ぼすものと理解しています。そのため、セキュリティ対策は富士通における重要な経営課題であり、経営層から現場部門まで全社一体となって取り組んでいます。また、そのための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ています。

<セキュリティリスクマネジメントの考え方>

富士通は、2021年以降、複数の重大なセキュリティインシデントに見舞われ、その対応に追われる現場では社内の様々な問題に直面しました。これらの問題を解決していく中で、富士通を攻撃者にとって「攻撃しにくい会社」にしそれを維持していくことが必要であると認識しました。「攻撃しにくい」とは、富士通への攻撃が容易ではない、すなわち攻撃が成功しにくいと攻撃者に思わせる状態を意味します。
「攻撃しにくい会社」を実現するためには、特に、インターネットに面したアセットの脆弱性など、外部からの攻撃の起点となるセキュリティリスクを徹底的に排除します。これにより、攻撃者は攻撃口を発見すること自体が困難になり、仮に攻撃口を発見できたとしても、その後の攻撃実行も極めて困難となる状態を目指しています。

<攻撃しにくい会社を実現するセキュリティリスクマネジメント>

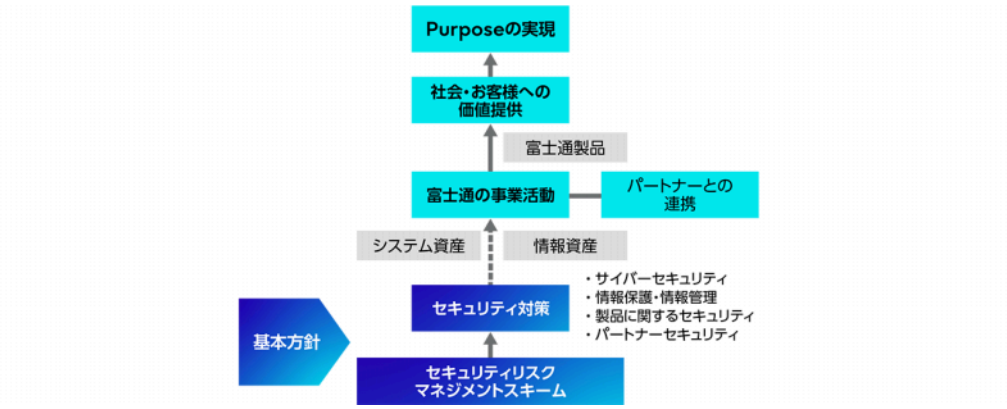
富士通の従来のセキュリティリスクマネジメントでは、一般的なリスクマネジメントの考え方に基づき、インシデント発生後の事後対応による被害最小化を重視していました。その結果、現場部門が認識しないまま潜在的なリスクが徐々に拡大し、インシデント発生後に初めてその深刻さが露呈するという事態が起こりました。
このような状況を踏まえ、攻撃者の視点でより早い段階で潜在的なリスクを自ら顕在化させ、攻撃者よりも先に対応することで被害を抑制することが必要であるという考えに至りました。特に、昨今のサイバー攻撃におけるリスク発見から攻撃までの時間が極めて短くなっていることを考えると、潜在的なリスクの早期顕在化と迅速な対応を実現するマネジメントが不可欠です。
潜在するリスクの様々なケースを想定しそれに対応する顕在化の仕組みを構築することで、潜在的なリスクを網羅的に特定しリスクに対応すべき現場部門を把握できるようになっています。リスクの対応にあたっては、特定されたリスクを分析（攻撃難易度等）・評価（発生確率と被害規模）することで対応方針・優先度などを決定しています。優先度の高いリスクについては、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）の下で全社セキュリティ統制を担う組織（以下、CISO組織）が直接現場に対して対応を指導することも行っています。



顕在化によるリスクマネジメント

<セキュリティ対策のスコープ>

パーパスの実現を支えるために、攻撃者が富士通自身だけでなく、パートナー企業あるいは富士通のクラウド基盤上のSaaSなど、サプライチェーン全体を通じて、国内外問わずお客様の情報を狙っているものと想定したセキュリティ対策に取り組んでいます。富士通のお客様への価値提供のためのシステム（ビジネスシステム）や事業活動をささえるシステム（社内システム）に対するサイバーセキュリティ対策はもちろん、適切に情報を扱う・保護するための情報管理、富士通の提供する製品そのものやサプライチェーンを担うパートナー企業に対するセキュリティ対策もスコープとして活動しています。



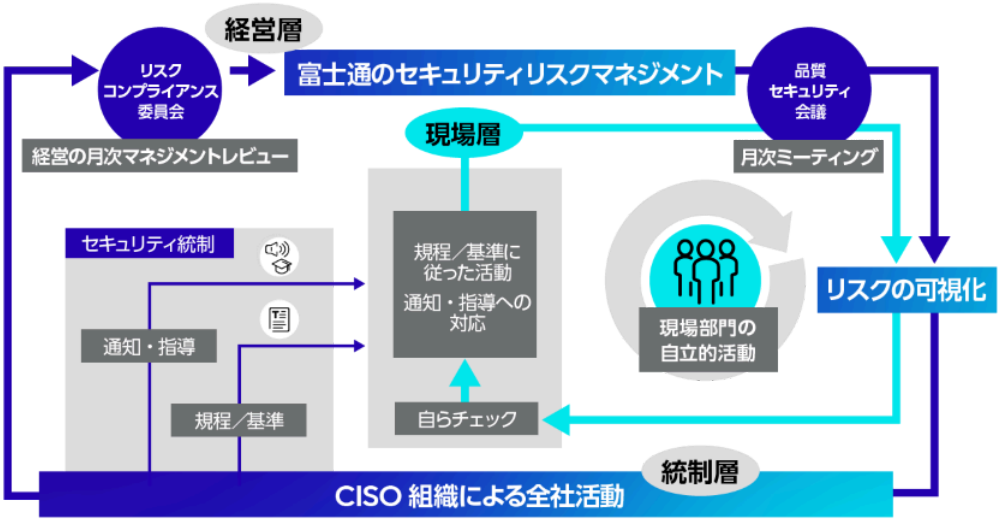
Purposeの実現に向けたセキュリティリスクマネジメント

全社セキュリティリスクマネジメントスキーム

富士通は、過去の事案への対応経験・その分析を通して、現場の一部門のセキュリティインシデントが自社全体に留まらずお客様・社会に影響を及ぼす可能性があること、潜在リスクの早期顕在化と迅速な対応を実現する現場実行力を高めるには経営の関与が必須であることを認識しています。この認識のもと、経営層・現場層・CISO組織（統制層）が一体となって経営課題としてセキュリティ対策に取り組むための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ています。

<スキームの概要>

このスキームは、経営層・現場層・CISO組織（統制層）が一体となってセキュリティ対策に取り組んでいくためのものであり、リスクの可視化とその共通認識化が各層の連携した取り組みを生む鍵となっています。
CISOは、セキュリティリスクを経営層に適切に開示し、経営層と現場層の共通認識を形成させることでトップダウンの統制（外側ループ）とボトムアップの改善（内側ループ）を促します。また、CISO組織では、現場層で自立的に取り組むべき活動の規程／基準の確立、重大かつ緊急性の高い脆弱性が顕在化した際には現場部門に対する直接的なセキュリティ統制を実施することで、富士通グループ全体で統一的な活動によるセキュア化を推進しています。
経営層は、可視化されたリスク情報をもとに意思決定を行う役割を担います。現場層でリスク対応を行う場合に、現場層が業務効率化やコスト削減、お客様要求の実現といったセキュリティ対応と相反する要求のために板挟みとなり、対応のスピード感が損なわれる場合があります。このため、経営層が可視化されたリスクをもとに意思決定を行い、現場層では解決できない・実行したくともできない環境の改善を行います。
現場層は、平時においてはCISO組織が定めた全社規程／基準に沿って活動を行います。リスクが顕在化した有事の際には、自部門内で暫定対処を行いつつCISO組織からの通知・指導に従って対策を実施しています。また、可視化されたリスクに基づいて自立的に自部門を改善する活動に取り組んでいます。



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

- 外側ループ（濃い青色の矢印）
  セキュリティリスクを可視化し経営層が把握できるようにすることで経営層の関与を強めるとともに、CISO組織によるセキュリティガバナンスを効かせてリスクマネジメントを行うためのループ
- 内側ループ（薄い青色の矢印）
  可視化されたリスク情報に基づき、現場部門が自らリスクを評価し、自主的にリスク対応を行うためのループ

<スキームに沿った全社レベルのセキュリティリスクマネジメント>

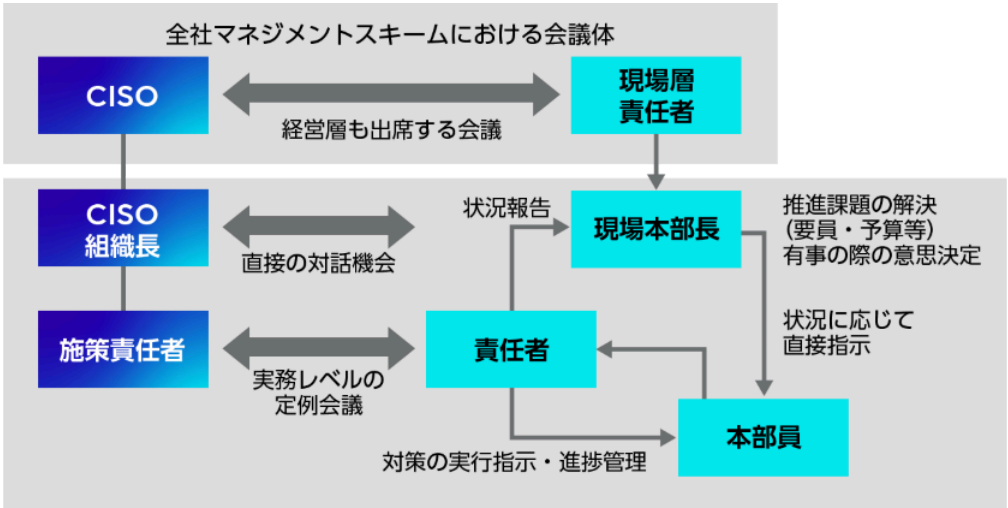
本スキームでは、CEOを委員長とするリスク・コンプライアンス委員会とCEO、CRMO（Chief Risk Management Officer：最高リスクマネジメント責任者）、CISO、CQO（Chief Quality Officer：最高品質責任者）、各現場層責任者による品質セキュリティ会議の2つの会議を通して、経営層と統制層、経営層・統制層と現場層の間でリスクの状況とセキュリティ対策の進捗状況について共通認識をもち、全社のセキュア化を推進しています。
例えば、セキュリティ対応を行うことを現場層責任者の責務に含めることもこれらの会議を通して決定されました。また、緊急性の高い脆弱性への対応が遅れている部門を特定し、必要に応じてCISOがトップダウンで現場部門責任者に働きかける対応も実施しています。このようなコミュニケーションは、現場層責任者がセキュリティ対応を担当者任せにするのではなく、自ら主体的に

セキュリティ強化を推進することにもつながっています。
リスクの状況やセキュリティ対策の進捗状況は継続してモニタリングされており、経営層と現場層は自部門の対応状況を定量的に把握できるようになっています。このモニタリングの結果は、対応が遅れている場合にその緊張感を高め、危機意識を醸成する役割を果たしています。セキュリティ対策の遅延や不備が発生するとCISOからの直接的な指導が行われる場合もあり、現場層責任者は、セキュリティ対策の遂行における自身の責任の重さを改めて認識し、現場レベルでの対策実施が徹底されるようになりました。

<セキュリティ対策実行レベルの体制とコミュニケーション>

CISO組織の統制する規程／基準やセキュリティ対策を現場レベルに浸透させるためのガバナンス体制の構築も行っています。
CISO組織からの指示に基づいて、現場の各本部において本部長の指名する「情報セキュリティ責任者」「情報管理責任者」「PSIRT責任者」（注1）を配置し、現場の自立的な活動を推進しています。これらの現場体制に対し、CISO組織の本部長・施策責任者が対峙する形で本部長レベル・責任者レベルでのコミュニケーションを実施しています。
具体的には、本部長の一人ひとりに対し、事案の情報を含む「富士通が置かれている現実」とその「組織のリスク状況の現実」を伝え、危機感を共有するとともに自組織のセキュリティ対応を自分事とするための対話を集中的に実施しています。また、CISO組織のセキュリティ施策責任者と現場層における各責任者の対話の場として責任者会議やその分科会を定期的に開催し、全社の規程／基準やセキュリティ対策の現場浸透を行っています。これらにより、セキュリティ対応に関わる本部長のリーダーシップと各責任者による現場への展開を確かなものとし、現場におけるセキュリティ対応の実行性を高めています。なお、海外については、本社方針と各国固有のセキュリティ要件をアラインメントする必要があり、リージョンごとにリージョンCISOを配置する体制を整えています。

注1：
- 情報セキュリティ責任者：情報システムセキュリティの維持・管理を統率する責任者
- 情報管理責任者：情報の管理・保護を統率する責任者
- PSIRT責任者：製品に関する脆弱性管理を統率する責任者



ガバナンス体制と各層のコミュニケーション

＜規程／基準＞

富士通では、グローバルスタンダードであるNIST（注2）の「SP800-37」（注3）を参考に、富士通グループを対象とす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」を策定し、組織および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を規定しています。これにより、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、これらのプロセス群を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。
また、NISTの「CSF」（注4）、「SP800-53」（注5）および「ISO/IEC27002」を参考に、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」を策定しています。この対策基準は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。更に、これら管理策の適用を推進するため、マニュアルおよびガイドラインを整備し全社に展開しています。

注2：NIST : National Institute of Standards and Technology
注3：SP800-37：NIST SP800-37 Rev.2 Risk Management Framework
注4：CSF：Cybersecurity Framework
注5：SP800-53：NIST SP800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations

＜セキュリティリスクの可視化＞

富士通では、リスクモニターや情報管理ダッシュボード等の各種ダッシュボードを構築し、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）に可視化しています。
「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。
「情報管理ダッシュボード」は、デジタル化された情報管理台帳です。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視ログなど）との整合性をチェックし、不備などを検出した場合は管理部門へアラート通知し早期是正を可能にしています。
これらのダッシュボードは、経営層・統制層と現場層で共有され現場部門への統制ツールとして機能するとともに、現場部門で自組織の状態を把握し自立的に改善するためのツールとしても活用しています。

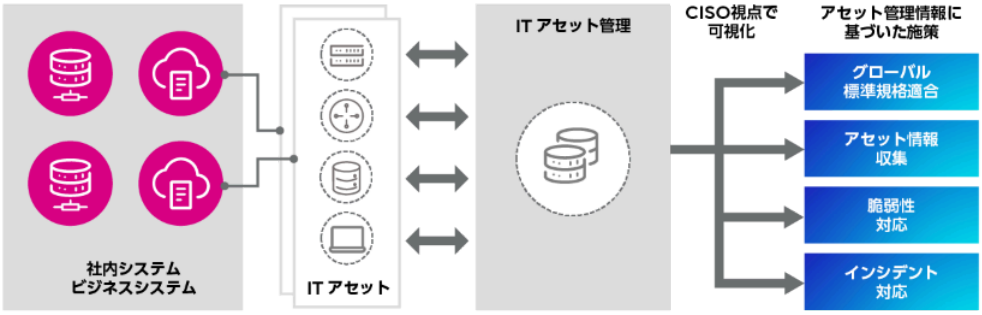
サイバーセキュリティ対策

富士通では多層防御によるサイバーセキュリティ対策を導入しています。侵入に対する防御として所有するシステムのITアセット管理情報を基軸に脆弱性のマネジメントを実施しています。また、侵入された場合に備えて監視の徹底を実施しています。さらに、万が一情報が搾取された際の対応として、重要情報の暗号化を実施しています。

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＞

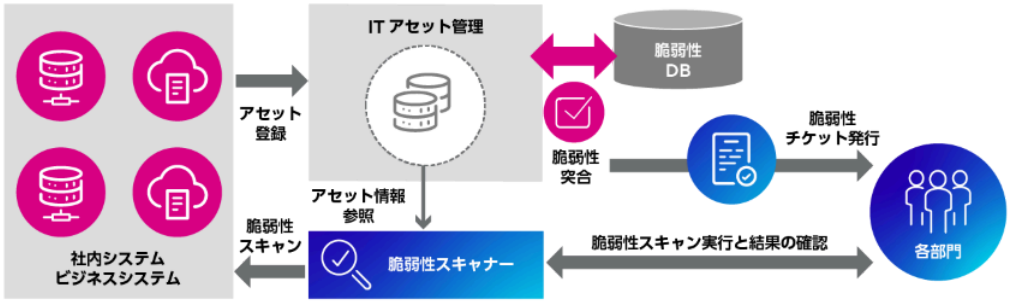
富士通では、お客様の安心安全でサステナブルな事業活動を支えるため、グローバルに展開しているお客様向けITシステム（ビジネスシステム）および社内ITシステムのITアセット管理情報を一元化し可視化することで、グループ全体のセキュリティリスクの特定と是正を速やかに実施しています。平時からのリスク管理を強化するとともに、CISO組織によるリスク監査と結果の可視化により、各部門における適切な現状把握と自律的な是正を促進しています。



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に対して脆弱性スキャンをかける仕組みを構築することで、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、インターネットから直接アクセスできないシステムであっても、インターネット表出システム経由でのラテラルムーブメントにより侵害を受け、被害が拡大する可能性があります。これに対応するため、脆弱性検知ならびに管理手段として、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で脆弱性の検知と是正を行っています。
本取り組みを富士通グループ全体で実施し管理されたアセットに対する脆弱性の早期潰し込みを徹底することで、外部に表出した脆弱性の新規検知数は大幅に減少しています。その中でも、ポート開放などの高リスクの脆弱性検知は数件程度までに削減しています。



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、富士通グループのインターネット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います。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。

＜緊急時の脆弱性対応プロセスの整備＞

緊急時に限らず平時から脆弱性対応を迅速に実行できる状態を整備しておくことが必要であり、国内においては、サービス停止を判断する責任者の明確化、緊急時の脆弱性対応プロセスについての整備を完了しています。
また、昨今では、ソフトウェアの脆弱性に対するサイバー攻撃が脆弱性発見後極めて短時間に行われており、日々、サイバー攻撃のスピードは加速しています。このような状況下、富士通はお客様の大切なデータを守るとともにお客様に安定したサービスを継続提供することを目的に、特に緊急性の高い脆弱性に対して富士通の判断でサービス中断を行う場合があります。お客様や富士通の情報資産を守るためにサービス停止を伴う対処を迅速に判断・実行する必要がある場合に行う措置であり、 結果的にセキュリティリスクだけでなくビジネス影響の最小化にもつながると考えています。

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。

重要情報の保護

富士通では、お客様との契約を伴う開発／運用等の秘密情報を取り扱う活動について、情報セキュリティ対策の強化およびシステム品質確保を目的にFujitsu Developers Platformの適用を原則としています。
Fujitsu Developers Platformは情報管理の不備を抜本的に改善する機能を実装しており、プロジェクトメンバー限定での情報共有機能による複数プロジェクト間のデータ混在防止、利用期限の強制機能によるプロジェクト終了後の不適切な情報保有の抑止を実現しています。これに加え、ファイルの秘密度ラベルに対して格納先フォルダが不適切な場合にアラート通知を行うことで、機密度に応じた適切な情報管理も実現しています。さらに、ダウンロードなど情報持ち出しを監視する機能により、侵入後の情報流出を早期に検知し被害拡大を防ぎます。
Fujitsu Developers Platform上の重要情報は暗号化することをルールとしており、非暗号化状態の情報がある場合はダッシュボードに可視化することで是正を促します。様々なビジネス活動における大切な情報資産をセキュリティリスクから守り、安心・安全な業務遂行を実現します。

インシデント対応

セキュリティインシデントの発生を未然に防ぐ取り組みは行っていますが、万が一インシデントが発生した場合にはすぐさま対応し被害を最小限に抑える必要があります。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体制および対応手順を予め整備し、有事の際に組織としてエスカレーション・対応・復旧・通知という一連の活動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

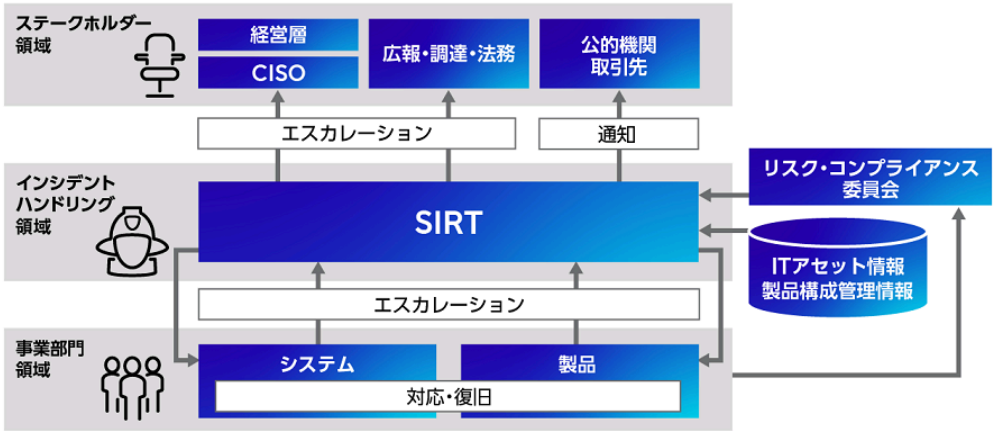
ます。エスカレーション後は、セキュリティ統制部門からインシデント対応を支援する専門チームがアサインされ、連携してインシデント対応を行います。

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、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・ガイドラインを策定し、富士通および国内グループ会社に展開しています。また、海外グループ会社については、各国特有の要件などアラインメントを行っています。



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、メンバーの継続的な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

＜SIRT体制＞

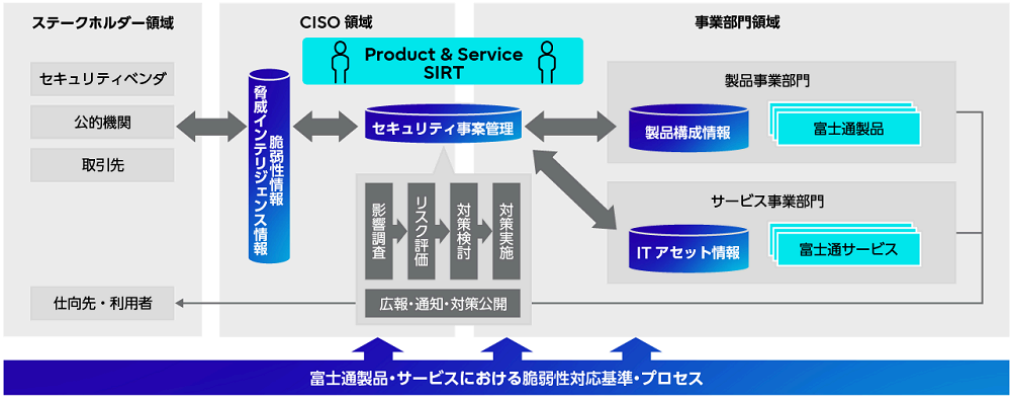
富士通の製品やサービスをご利用いただくお客様を守るため、製品構成情報、ITアセット情報、および脆弱性情報を含む脅威インテリジェンス情報の一元的な管理に加え、各部門において脆弱性対応を担当する情報セキュリティ責任者やPSIRT責任者の配置による xSIRT（注6）体制を整備し、製品やサービスの脆弱性に起因するリスクに対してスピーディーでプロアクティブな対応を可能としています。

注6：SIRT：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

＜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ています。また、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、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の特定と対処を迅速に実施した結果、情報搾取被害を回避しています。

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、個人情報を含む当社秘密情報および他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の運用として、「①役割の定義」から「⑦見直し」に至るまでのPDCAサイクルを回しています。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。なお、社内の一部の組織ではISMS認証を取得しています。情報保護マネジメントシステム運用における主な活動内容は以下の通りです。

情報保護マネジメントシステム

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、秘密情報・個人情報を管理・保護する体制を構築し、各部門においては、部門ごとの情報管理責任者を任命するとともに役割を明確化し、適切な秘密情報・個人情報の取り扱いを推進しています。

情報管理体制および役割

②方針・規程
秘密情報・個人情報を正しく取り扱うため、必要な規程（情報管理規程・他社秘密情報管理規程・個人情報管理規程）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。
年に一回以上、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。
（参考）受講者実績37,234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。

⑤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監査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。

情報セキュリティ講座 2024-2025

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。

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監査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。2024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2024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。

情報セキュリティ／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。

- **[PDF] 第三者評価・認証監査結果**

現場層の自立化に向けた取り組み

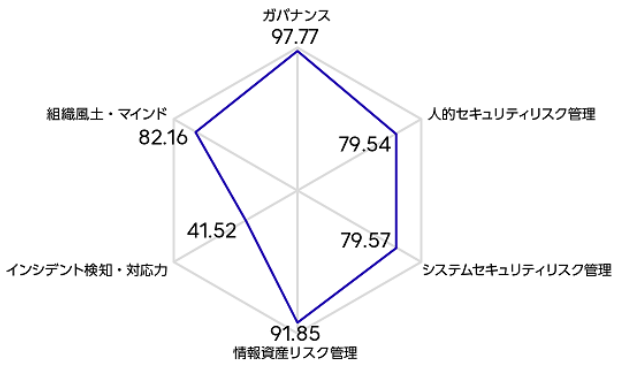
全社セキュリティリスクマネジメントスキームに従い、統制層を中心により「攻撃しにくい会社」を実現する取り組みを推進していますが、統制層からの通知・指導をきっかけに現場層で対応を開始するのでは攻撃者のスピードに遅れてしまう可能性があります。攻撃者より先にリスクを顕在化し攻撃されるより前に是正を完了させることを確実にしていくためには、組織が自立的にセキュリティ基準を遵守し迅速にセキュリティ対応を実行していくことが必要になります。

組織成熟度の可視化

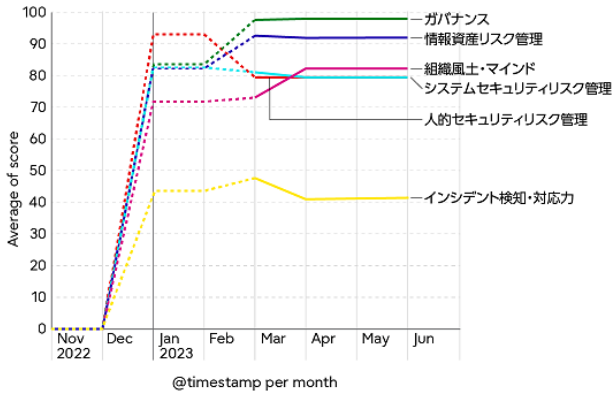
＜成熟度モニター＞

富士通では、組織における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、組織の成熟度として可視化しています。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を把握し具体的な施策や是正対応を現場部門自ら実行する風土の醸成を目指しています。
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、これら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ーティングなども利用しており、第三者から見た客観性のある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



組織成熟度



成熟度スコア推移

＜第三者評価＞

グローバルにITサービスを提供する企業として、富士通グループではセキュリティ対策の継続的な実施とステークホルダーの皆様へのセキュリティ健全性に関する説明責任を重視しています。その一環として、客観的なセキュリティ評価を可能とするセキュリティレーティングSecurityScorecard およびBitsightを導入しています。これらのサービスでは攻撃者視点でのリスク評価や公表されたセキュリティインシデントを加味したセキュリティの健全性をスコアとして表しています。セキュリティレーティングを活用したセキュリティ対策を行うことで、SecurityScorecardおよびBitsightにおいていずれも高水準の達成・維持を実現しております。

SecurityScorecard：Aランク、　Bitsight：Advancedランク（2025年5月時点）

富士通グループでは、今後もセキュリティレーティングを通じた客観的な評価に基づき、セキュリティ対策の継続的な改善に努めていきます。これらの取り組みを通して、ステークホルダーの皆様からの信頼を獲得し、パートナーシップの強化やお取引先の拡大などのビジネス面での好影響にもつなげていきたいと考えています。

セキュリティに関わる人材の育成

現場層の自立化に向けて、最新のセキュリティ脅威の動向だけでなく富士通で発生したインシデントの実態とその対応から学んだ教訓を活かした教育・訓練を実施し、役員・社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＞

サイバーセキュリティおよび情報管理に関する基本的な教育に加え、最新動向や富士通の事案対応から学んだ実態と教訓を周知徹底しています。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、専門人材のスキルアップにも取り組んでいます。また、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の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・セールス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。これらの訓練での気づきは、「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、全社で共有しています。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。

注：2024年度の訓練実施回数：全社訓練1回、標的型メール訓練2回

＜セキュリティ体制強化と人材育成＞

富士通グループに向けてCISOおよびCISO組織から定期的に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。
2023年には富士通グループとしてのセキュリティ人材像を再定義し、セキュリティに関わるプロフェッショナル認定制度の見直しを行いました。全社・各部門のセキュリティ向上に貢献する人材としての姿を明確にしたうえで、プロフェッショナルとなる教育の実施とプロフェッショナルに見合った報酬制度の整備を行っています。これらの取り組みでセキュリティ人材を拡充し、各部門のセキュリティ体制の強化を推進しています。

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 Quality Rulesを定めています。また、Fujitsu Group Global Policy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。

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。

富士通グローバル品質指針と品質規格体系

製品・サービスの安全に関する実践方針

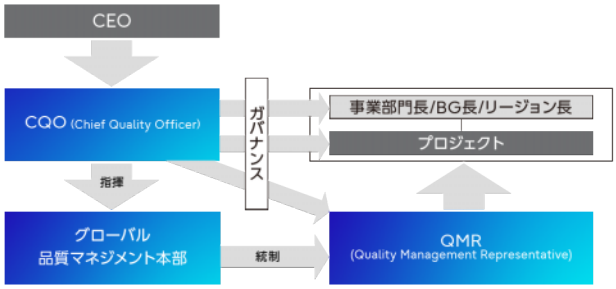
富士通グループは、安全・安心な社会を構築するという社会的責任を認識し、事業活動のあらゆる面において製品・サービスの安全性を常に考慮し、次の方針の下で実践しています。

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、様々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

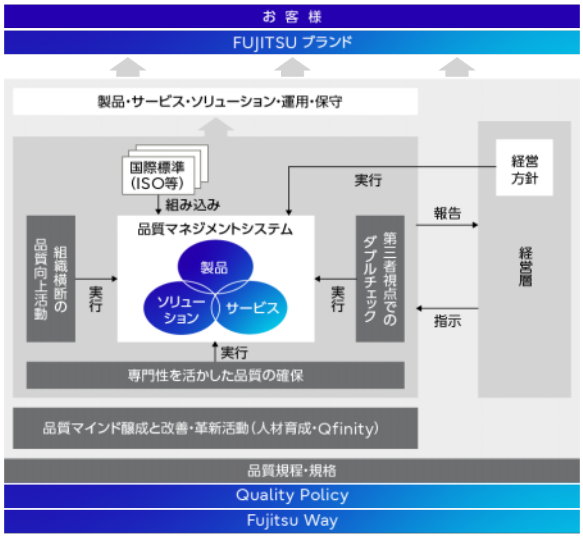
富士通グループでは、CQO（Chief Quality Officer：最高品質責任者）を任命し、グループ全体で製品・サービスの品質マネジメント体制を構築しています。具体的には、CQOの指揮の下、全社ヘッドクォータとして、グローバル品質マネジメント本部が全社の品質方針・戦略を策定し、その実行状況について第三者視点での確認を通して評価、改善を行うことで、富士通グループ全体の品質活動を推進・実行しています。また、各事業部門・BG（ビジネスグループ）・リージョンに自部門の品質管理を実行するQMR（Quality Management Representative：品質管理責任者）を設置することで、グループ全体の品質管理を統制しています。
品質ガバナンス徹底に向けて、CQO・QMR・グローバル品質マネジメント本部で、現場の課題や対策、実行状況を定期的に協議する会議体を設置し、現場に即した品質活動を行い、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

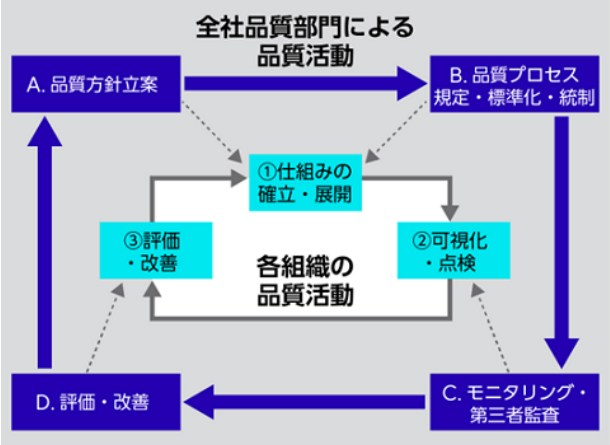
お客様のニーズや期待に応えられる製品・サービスの品質を一貫して提供するためには、企画・計画から開発、製造、試験、販売、運用・保守に至るまで、事業部門、共通部門、ビジネスパートナーなど社内外の様々な組織との連携が必要であり、これら組織が一体となる体制や仕組みが基盤として必要不可欠です。
そのため富士通は、製品・サービスに応じ、これら関連部門と連携しながら品質マネジメントシステム（QMS：Quality Management System）を構築し、運用しています。QMSの運用にあたっては、ISOなどの国際的な認証規格にも照らして進捗を定期的に検証し、より良い品質の実現を目指してプロセスの改善を図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



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。

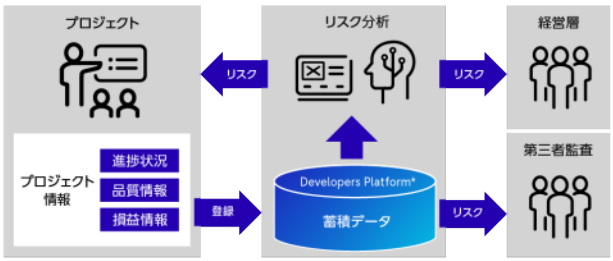
Qfinityは、2001年度から富士通グループ全体で開始した「社員一人ひとりが主役となり、製品やサービスの品質を向上し続ける改善・革新活動」です。Qfinityを通して、各職場での品質向上活動を推進するとともに、優れたナレッジの抽出、共有を促進することで、製品・サービスの品質向上に取り組んでいます。

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、様々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＞

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に集約しています。これらの蓄積されたデータをAIで分析し、将来起こり得るリスクを予見して対策を促すことで、プロジェクト成功率の向上を目指しています。
また、日々の活動で得られる品質データからリスクを抽出・可視化することで、現場プロジェクトが自らリスクに気づき、自律的に改善することにつなげています。



* Developers Platform :富士通全社で利用可能なデリバリ変革を支える新たな標準開発基盤

リスク予見型品質マネジメントのための仕組み

＜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」への変革を進めてきました。「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っています。

「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。
この「One Delivery品質保証プロセス」により、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しています。

One Delivery品質保証プロセス

2024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：輸入事業者表示内容の誤り（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**
- ノートパソコンのバッテリ発火の未然防止策
  富士通では、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、富士通では、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
- 第三者認証における違反：1件（認証書類の不正（是正済み））

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、2024年9月時点）。

- ISO 9001：20本部 認証
- ISO 20000：9本部 認証

お客様とともに

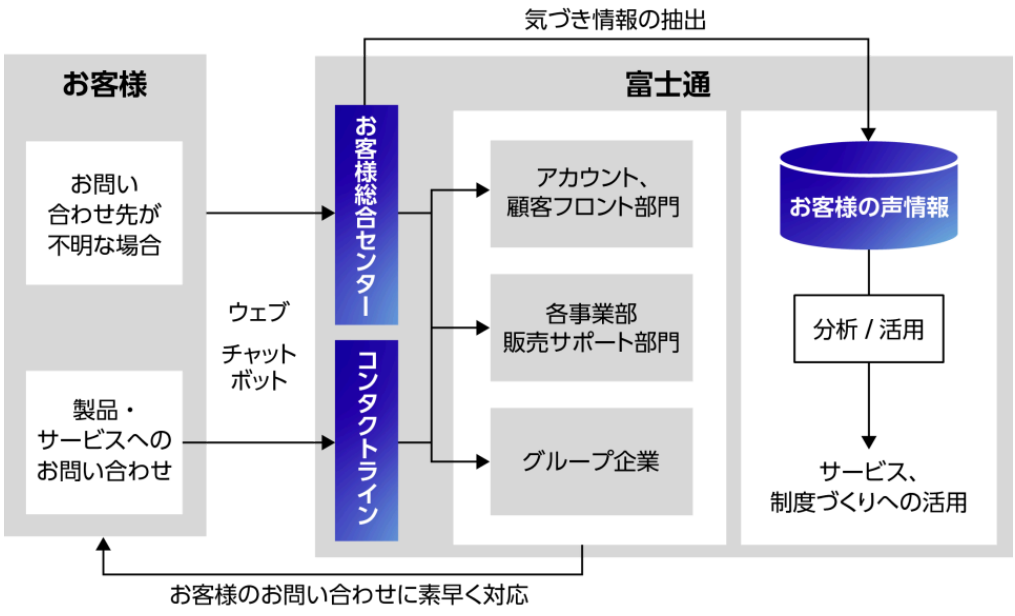
お客様の満足度向上のために

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**



運用体制

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。2025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」というパーパスに基づいた富士通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。
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**