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

当社は、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」）を制定いたしました。2023 年 9 月に改訂した当基本方針は、現在の当社にとって最善のものと考えて作られていますが、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（2023 年 6 月 26 日現在）

当社は、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おります。

＜取締役会＞

当社は、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おります。取締役会は、法令及び定款に反せず、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及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及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及び助言機能を強化しております。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、2023 年 6 月 26 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 名で構成されております。

2022 年度においては、取締役会を 13 回（内　臨時取締役会 1 回）開催し、経営方針の策定やその実現に向けた施策について議論し、指名委員会の答申に基づく新経営体制等について決議しました。

＜監査役（会）＞

当社は、監査機能及び監督機能として監査役（会）を設置しております。監査役は、取締役会等の重要な会議に出席し、取締役会及び業務執行機能の監査・監督を行います。監査役会は、2023 年 6 月 26 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）で構成されております。2022 年度においては、監査役会を 10 回開催（内臨時監査役会 1 回）し、主に、監査の方針及び監査計画、会計監査人の監査の方法及び結果の相当性並びに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及び検討等を行いました。また、全ての回において全監査役が出席しております。

＜独立役員会議＞

当社は、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係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、全ての独立役員（独立社外取締役 5 名、独立社外監査役 3 名）で構成する独立役員会議を設置しております。同会議では、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役員の意見形成を図ります。2022 年度においては、独立役員会議を 12 回開催し、経営方針、M&A を含む当社及び当社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、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＞

当社は、役員選任プロセス及び役員報酬決定プロセスの透明性及び客観性を確保し、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及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及び報酬委員会を設置しております。

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おります。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することとしております。

2023 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、指名委員会につきましては非執行役員 3 名（内、独立社外取締役 2 名）、報酬委員会につきましては独立社外取締役 3 名で構成されております。また両委員会の事務局は、当社の人事部門及び法務部門が担当しております。

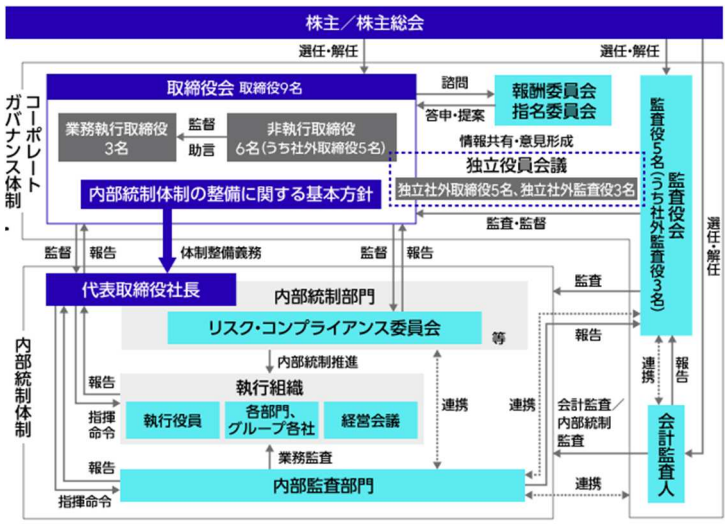
- ●指名委員会
  - 委員長　：阿部　敦（独立社外取締役）
  - 委員　　：古城　佳子（独立社外取締役）、山本　正已（取締役シニアアドバイザー）
- ●報酬委員会
  - 委員長　：向井　千秋（独立社外取締役）
  - 委員　　：佐々江　賢一郎（独立社外取締役）、バイロン・ギル（独立社外取締役）

なお、2022 年度は、指名委員会を 8 回、報酬委員会を 6 回開催し、指名委員会においては社長を含む代表取締役の選定案、取締役候補者の選任案及び役員のスキルマトリックス等、報酬委員会においては役員報酬の内容改訂や個人別報酬決定プロセスの変更等について検討し、それぞれ取締役会に答申しました。

- ●コーポレートガバナンス報告書
  業務執行、監査・監督、指名、報酬決定等の機能に係る事項（現状のコーポレートガバナンス体制の概要）

当社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。（2023 年 6 月 26 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

当社は、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おります。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」を採用しております。

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おります。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、さらに当社の事業分野、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の実効性を高めております。

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）」に基づき決定されています。

- 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 P10 / 報酬の額又はその算定方法の決定方針の有無 P11」

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 123 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（2023 年 6 月 26 日現在）

	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	○	
	古田　英範	副社長、COO	○	
	磯部　武司	執行役員 SEVP、CFO		
非執行	山本　正已	シニアアドバイザー		
	向井　千秋			○
	阿部　　敦	取締役会議長		○
	古城　佳子			○
	佐々江　賢一郎			○
	バイロン ギル			○

2022 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	13 回	99.1%
監査役会	10 回	100%

* 取締役 9 名のうち、8 名は 100%

取締役および監査役のスキル

当社は、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（2023 年 6 月 26 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	古田　英範		男性	日本	○		○	○	
取締役執行役員	磯部　武司		男性	日本	○	○	○		

取締役シニアアドバイザー	山本　正已		男性	日本	○		○	○	
取締役	向井　千秋	○	女性	日本			○	○	○
取締役	阿部　敦	○	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		○	○		

監査役（2023 年 6 月 26 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	山室　恵		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	○		

なお、非執行の取締役の中で、企業での業務経験者である山本取締役シニアアドバイザー、阿部取締役の 2 名については、リスクマネジメントの専門知識を有している。

リスクマネジメント

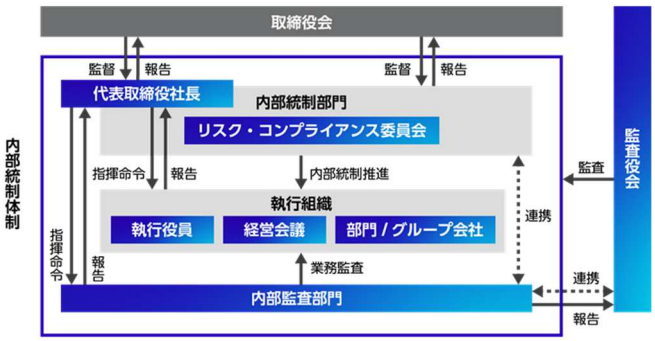
方針・推進体制

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。

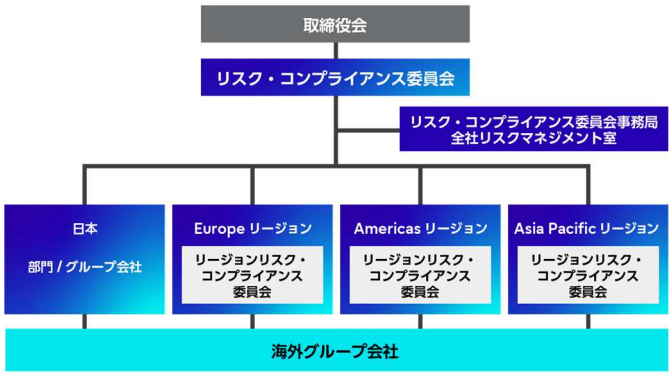
リスク・コンプライアンス委員会は、代表取締役社長（CEO）を委員長として業務執行取締役等で構成しており、富士通グループに損失を与えるリスクを常に評価、検証し、認識された事業遂行上のリスクについて、未然防止策の策定等リスクコントロールを行うとともに、リスクの顕在化により発生する損失を最小限に留めるため、顕在化したリスクを定期的に分析し、取締役会等へ報告を行い、再発防止に努めています。

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。

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



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にリスク･コンプライアンス委員会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っています。

これまでの取り組みを踏まえ、さらなる施策強化と実効性の担保を図るためには、これまで以上に経営者主導による全社的、組織横断的な対応が必須であると考え、富士通グループ全体の品質責任者として最高品質責任者（Chief Quality Officer：CQO）を新たに任命しました。さらに、CEO 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。

具体的には、これまで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った同委員会のメンバーに新たに任命した CQO を加えるとともに、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個別事象への対応も含め、具体策まで踏み込んで決定し、迅速に実行する体制としています。こうした体制を構築することで、CISO・CQO に対してこれまで以上に強化した権限を付与し、人事制度や投資リソース等その他の各

CxO の領域を含む全体を統括する、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。また、施策実行の迅速性と実効性を担保するため、同委員会を毎月開催しています。

事業活動に伴う主なリスク（注 1）	
・ 経済や金融市場の動向に関するリスク ・ お客様に関するリスク ・ 競合・業界に関するリスク ・ 投資判断・事業再編に関するリスク ・ 調達先・提携等に関するリスク ・ 公的規制・政策・税務に関するリスク ・ 自然災害や突発的事象発生のリスク ・ 財務に関するリスク	・ 製品やサービスの欠陥や瑕疵に関するリスク ・ コンプライアンスに関するリスク（人権に関するリスク含む） ・ 知的財産に関するリスク ・ セキュリティに関するリスク ・ 人材に関するリスク ・ 当社グループの施設・システムに関するリスク ・ 環境・気候変動に関するリスク

(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。
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」

プロセス

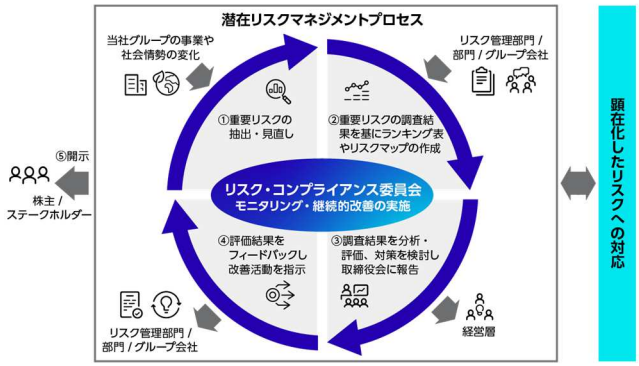
富士通グループを取り巻く様々なリスクから、事業活動に伴う重要リスクの抽出・見直しをしたうえで、毎年、重要リスクの発生可能性・影響度・対策状況等について調査・分析・評価し、可視化を行っています。

評価結果を基に、リスク・コンプライアンス委員会において重要リスクを確認し、さらなる対策等を指示するとともに、取締役会に報告しています。リスク・コンプライアンス委員会が決定した方針、対策等をグループ全体にフィードバックし、重要リスクごとに定めたリスク管理部門がグループにおける対策等を適切に管理することでリスクの低減を図っています。

なお、潜在リスクマネジメントプロセスにおいて得られた情報は、ステークホルダーに開示する有価証券報告書やサステナビリティデータブック等に反映しています。 また、リスクが顕在化した際には、リスクマネジメントに関する規程に基づき、迅速にリスク・コンプライアンス委員会へエスカレーションを実施するなどのルールを義務化し、従業員に周知することにより、リスクマネジメントの意識向上を図っています。

このようなプロセスを回すとともに四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。

リスクマネジメントプロセス

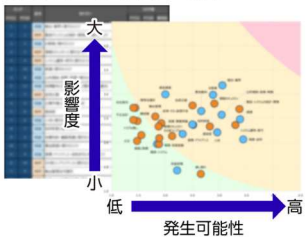


重要リスクの可視化

重要リスクの調査シート

No	リスクカテゴリー	影響度	発生可能性
1	景気動向		
2	お客様動向		
3	競合・業界の動向		
4	情報セキュリティ		
5	コンプライアンス		
⋮			
32	環境・気候変動		

重要リスクランキング・マップ



リスクマネジメント教育の実施

富士通グループ全体でリスクマネジメントの徹底を図るため、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。

2022 年度の教育実績については、「2022 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。

特に、各事業部やグループ各社の職制系統による対応に加えて、地域ごとに所在するグループ各事業所が協力する「エリア防災体制」の構築を進めています。

また、防災体制の実効性を検証し、対応力強化を図るために、全社、対策本部、事業所、個人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、2022 年度の活動実績は、「2022 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、各種感染症の流行など、経済・社会活動の継続を脅かす不測のリスクが増大しています。 富士通および国内グループ会社は、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 の継続的な見直し、改善を実施する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ています。

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、2022 年度の活動実績は「2022 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

2022 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：26 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。

- **富士通グループ新任幹部社員向け研修： 1,257 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。

- **防災フォーラム： 450 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

- **情報セキュリティインシデント対応訓練：70 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実践し、検証することでインシデント対応の迅速化を図る。

- **製品・サービストラブル対応訓練：95 名**

  製品・サービストラブルが発生した際の影響の把握や社外向けの対応を模擬的に実施し、組織間の連携プロセスの確認および検証を行い、課題を抽出、継続的改善を図る。

防災・BCM 訓練

- **合同防災訓練： 2022 年度のテーマ「南海トラフ巨大地震」**

  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。

情報セキュリティ

基本方針

富士通グループでは、2021 年 10 月に専任の CISO（Chief Information Security Officer：最高情報セキュリティ責任者）を任命し、新たな情報セキュリティ体制の下で、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

CISO の下、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、グローバルに一貫したセキュリティポリシーおよび施策を展開しています。リージョン CISO は、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し、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、情報セキュリティのあるべき姿の実現に向け、CISO による関連部門の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(※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。

(※1)　PSIRT : Product Security Incident Response Team

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

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。当社では、＜情報セキュリティの目指す姿＞ を以下のように考え、これを実現するため “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、社内関連部門や従業員とともに、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。

＜情報セキュリティの目指す姿＞

- ●攻めの情報セキュリティ
  - **DX** 時代の多様な働き方を支える情報セキュリティの継続的な進化
  - 従業員や組織の自律的な情報セキュリティ対応
- ●守りの情報セキュリティ
  - 脆弱性対応によるサイバー攻撃の未然防止
  - 監視強化による有事のサイバーリスク極小化

取り組み

＜再発防止策の横展開とセキュリティリスクの可視化＞

当社では、専任 CISO 体制の下、プロジェクト情報共有ツール「ProjectWEB」およびクラウドサービス「FJcloud-V／ニフクラ」の情報セキュリティ事案を受け、再発防止策の横展開を推進しています。2022 年には、主な再発防止策

の一つである “WEB システムの多要素認証化” について、国内展開を完遂しています。さらに、全社セキュリティ点検によって、セキュリティリスクの可視化を実施し、継続して是正対策を推進しています。

2023 年も引き続き ＜情報セキュリティの目指す姿＞ の実現に向け、下記の主要テーマに基づき、セキュリティリスクの可視化による適切な是正とともに、情報セキュリティの進化に取り組んでいきます。

＜セキュリティリスクの可視化によって実現すること＞

- 社内関連部門が自律的にリスクをコントロール

  情報管理や情報システムセキュリティに関するリスクを客観的に可視化します。社内関連部門は可視化された自部門のリスクを確認し、スピーディーに対応しています。重要なシステムや情報に関しては **CISO** 直轄組織による直接検査を実施し、対応内容の客観的な確認により精度を高めています。
  また、従業員自身や組織の情報管理リテラシー（内的要因）、サイバーリスクの実態（外的要因）についても可視化し共有します。（見える化）
  従業員一人ひとりがこれを理解・共感することで（自分ごと化）、自律的な情報セキュリティ対応（行動化）を促し、組織の風土を醸成します。

- デジタル化したリスクを的確に是正

  CMDB（注 **1**）や、情報管理ダッシュボード（注 **2**）を導入し、情報システムの脆弱性や情報管理不備などのリスクをデジタルに可視化します。可視化されたリスクを人手に頼らず機械的に是正することで、的確かつスピーディーにセキュリティリスクを極小化します。

(注1) CMDB：Configuration 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）を自動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2) 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、是正をチケット化（ワークフロー化）し早急な対応を可能としています。

- テクノロジーを活用した情報セキュリティの進化

  2023 年からの取り組みとして、認証基盤の統一による、利用者 **ID**・認可情報・証跡ログの集中管理と見える化を推進します。
  この認証基盤では、証跡ログを利用した行動解析や、解析結果と連動した認可情報の最適化などにもチャレンジしていきます。

＜主な施策について＞

各テーマに紐づく主な施策について、以下 3 つの観点で紹介します。

- サイバーセキュリティ

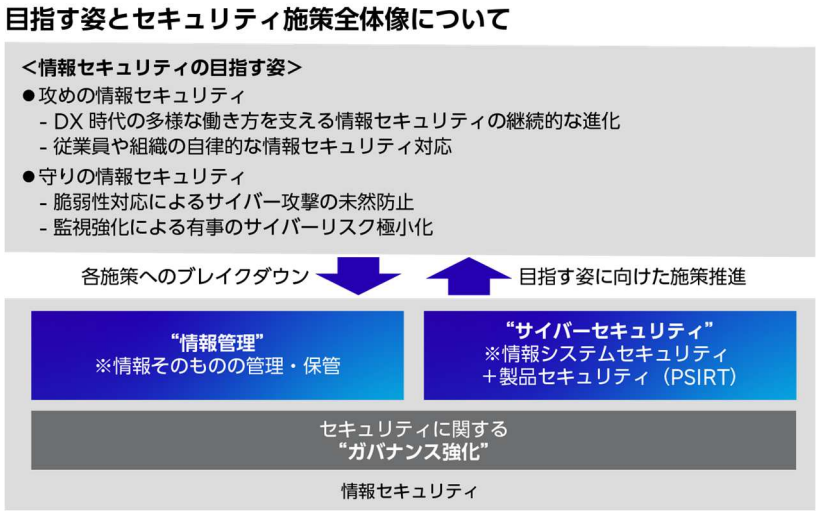
  情報システムセキュリティ（情報システムおよびネットワークに対する安全性・信頼性の確保・維持）に加え、当社製品・サービスのセキュリティ維持活動に関する施策の紹介

- 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



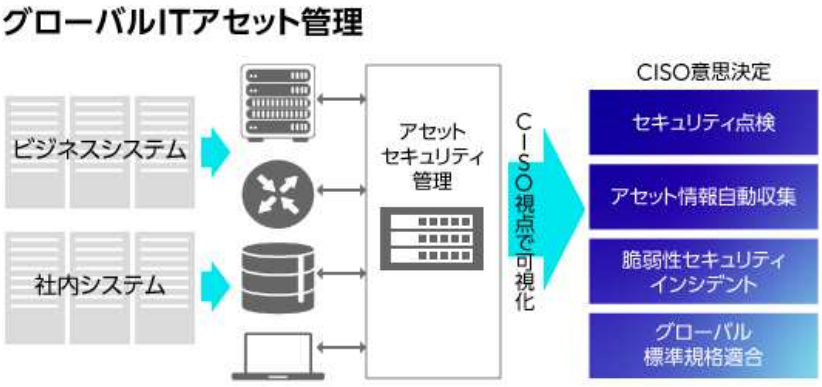
サイバーセキュリティ

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>

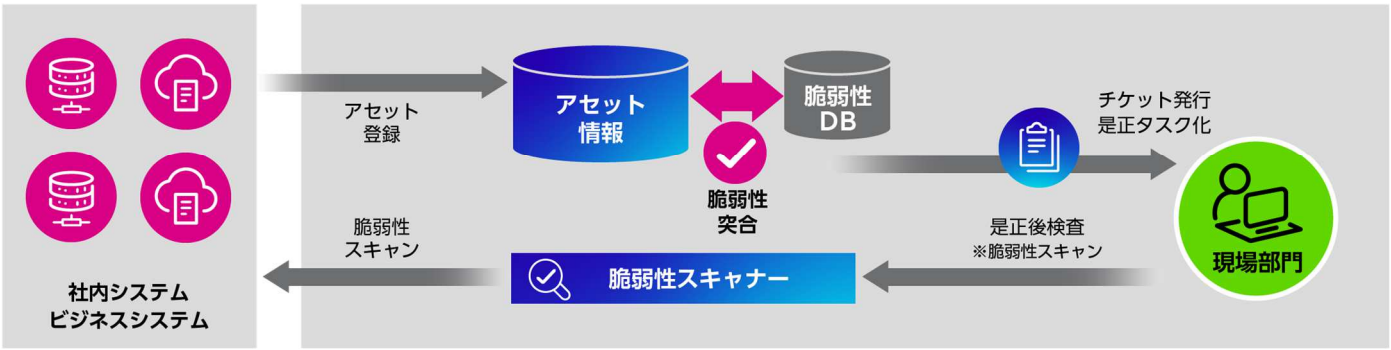
当社では、お客様の安心安全でサステナブルな事業活動を支えるため、グローバルに展開しているお客様向けの IT システムおよび、社内 IT システムの IT アセット管理を一元化し可視化することで、グループ全体のセキュリティリスクの特定と是正を速やかに実施しています。平時からのリスク管理を強化するとともに、CISO 直轄組織によるリスク監査と結果を見える化し、社内関連部門における適切な現状把握と自律的な是正を促進しています。



＜インターネット表出システムの脆弱性スキャン＞

IT アセット管理情報を基軸に、外部からインターネット表出のシステムに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社内関連部門による、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、さらに重要システムに関しては、CISO 直轄組織による第三者監査で精度を高めています。2023 年は、このプロセスの自動化・機械化についても実現に向け推進していきます。
なお、インターネットに表出していないシステムの脆弱性についても、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、重要な脆弱性について、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。

インターネット表出システムの脆弱性スキャン



＜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は 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。

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。そのために、有事が起こることを前提としたインシデント対応プロセスを策定し、有事の際には組織としてエスカレーション・対応・復旧・通知という一連のプロセスを迅速に実施できるよう取り組んでいます。

①エスカレーションプロセス

インシデントによるリスクインパクトを算出し、その結果に応じてエスカレーションを実施するプロセスを標準化し、継続的に改善することで、有事の際の組織としての対応力を強化しています。

②インシデント対応・システム復旧プロセス

攻撃情報や脆弱性情報を入手後、該当する製品・システムに対して、適切なインシデントハンドリングに加え、パッチ適用計画や BCP を含めたシステム復旧計画を策定し、迅速な復旧に向けた対応を行います。

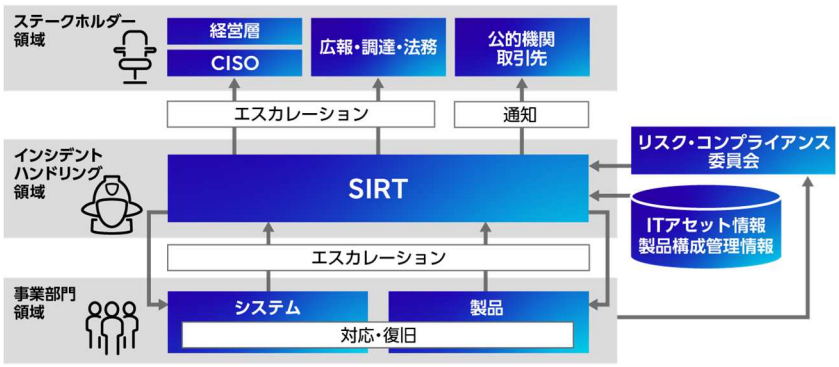
③通知プロセス

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・報告の適切な実施に努めています。

④プロセス定着化活動

富士通グループでは、インシデント対応に関する定期的な教育・訓練を実施することで、社員への啓発と意識徹底を図り、インシデント対応プロセスの定着化に向けた活動を実施しています。

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、全体の対象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。
当社では、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対応インシデントの振り返りを行い、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。

当社製品・サービスにおけるリスクの未然防止

＜PSIRT 責任者体制＞

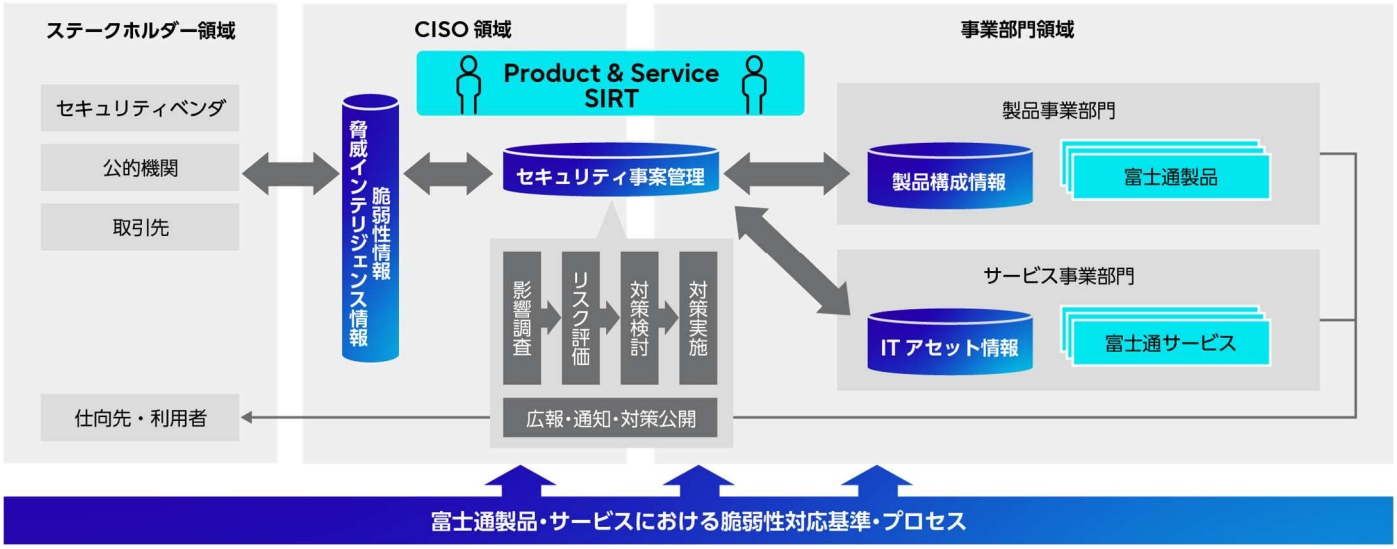
当社の製品やサービスをご利用いただくお客様を守るため、製品構成情報、IT アセット情報、および脆弱性情報を含む脅威インテリジェンス情報の一元的な管理に加え、社内関連部門において脆弱性対応を担当する PSIRT 責任者を配置することにより、製品やサービスの脆弱性に起因するリスクに対してスピーディーでプロアクティブな対応が可能となる体制を構築しています。

＜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、データサイエンティストによる統計解析や対応実績を基に、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最小限にすることができます。

富士通製品・サービスにおける脆弱性対応体制



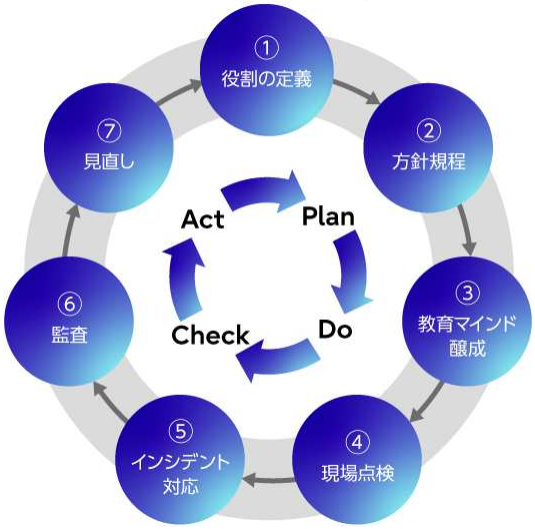
情報管理

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（7ポイント）



①役割の定義

代表取締役社長の下、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-Learning）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。
※2022 年受講者実績：37,343 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。

情報保護管理体制および役割

個人情報の保護

当社では、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 3) 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3)　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 4）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。2022 年度は全部門にて内部監査を実施しています。

(注4) 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 2022 年度、当社に設置した「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）

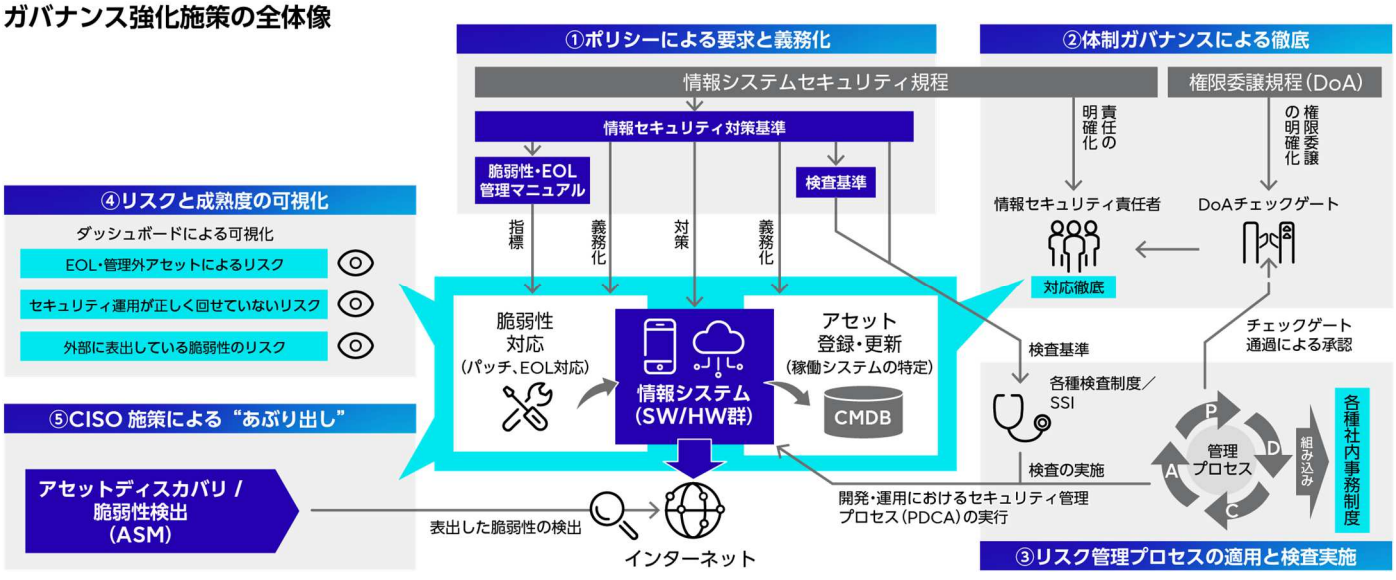
ガバナンス強化

当社では、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



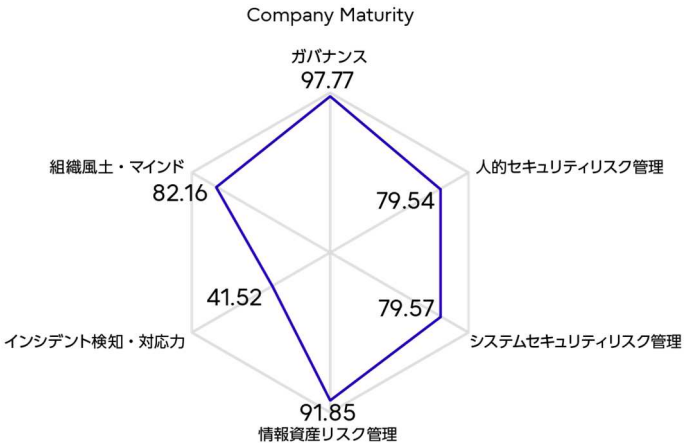
セキュリティ成熟度のメータリング

当社では、組織におけるセキュリティの成熟度をインフラの設定値やセキュリティログ、監査データなどを自動収集してスコアリングすることで、セキュリティ成熟度の評価を実施しています。富士通本社、各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。

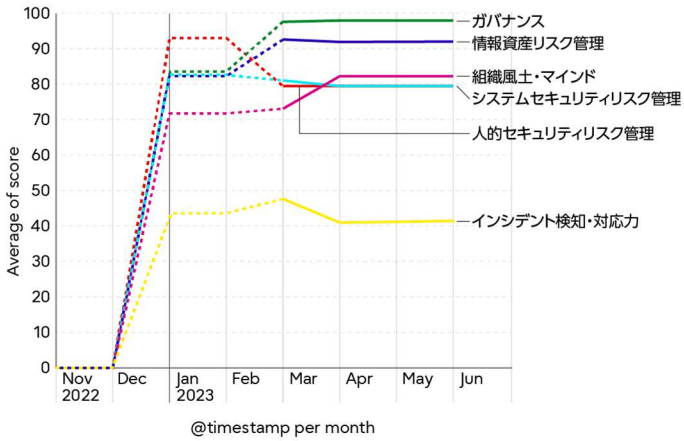
セキュリティ成熟度評価の指標は、国内外で実績のあるサイバーセキュリティ能力成熟度モデル C2M2（注 5）や、セキュリティインシデントマネジメントの成熟度モデル SIM3（注 6）を参考にした上で、成熟度スコアをセキュリティ施策におけるデータから機械的にスコアリングする方法を独自に取り入れて評価しています。評価スコアは 100 点を上限とし、ガバナンス、人的セキュリティリスク管理、システムセキュリティリスク管理、情報資産リスク管理、インシデント検知・対応力、組織風土・マインドのカテゴリ別に 6 軸で成熟度をスコアリングしています。2023 年は対外組織連携およびサプライチェーンリスク管理を加え 8 軸で評価を行います。

(注5)　C2M2：Cybersecurity Capability Maturity Model
(注6)　SIM3：Security Incident Management Maturity Model

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

当社では、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 7）の「CSF」（注 8）、「SP800-53」（注 9）および「ISO/IEC27002」を参考に 200 以上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 10）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。

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7)　NIST : National Institute of Standards and Technology
(注8)　CSF：Cybersecurity Framework
(注9)　SP800-53：NIST SP800-53 Rev.2 Security and Privacy Controls for Information Systems and Organizations
(注10)　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。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。
また、CISO および CISO 直轄組織による定期的な社内への情報発信やセキュリティ責任者コミュニティの活性化により、富士通グループ全体における情報管理やセキュリティ施策が、業務上の利便性やコスト削減に劣後しない風土づくりを目標として、下記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」に見直し、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・社員を対象にしたインシデント対応訓練を年 2 回実施しています。具体的には、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インシデントの発生を想定して、実践的な訓練を年 1 回実施しています。また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、迅速な対応と影響を最小限にする目的で、役員や社内関連部門が参加するインシデント訓練を年 1 回実施しています（合計年 2 回）。
2022 年度にはさらに標的型メール訓練も 2 回実施し、従業員一人ひとりのセキュリティマインドの醸成を促進しています。こちらも年 1 回以上継続的に行っていきます。

＜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、各部門を支援するため、セキュリティ責任者体制を任命しセキュリティ責任者コミュニティの活性化を行い、各部門のセキュリテ

ィに関する考え方、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、特に現場の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。現場の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現場組織のセキュリティ体制を強化しています。
なお、セキュリティに関する経験が不足している部門に対しては、組織のセキュリティ成熟度向上を前述の「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を通じた定期的コミュニケーション実施などを通じて、各部門とともに改善に取り組んでいます。

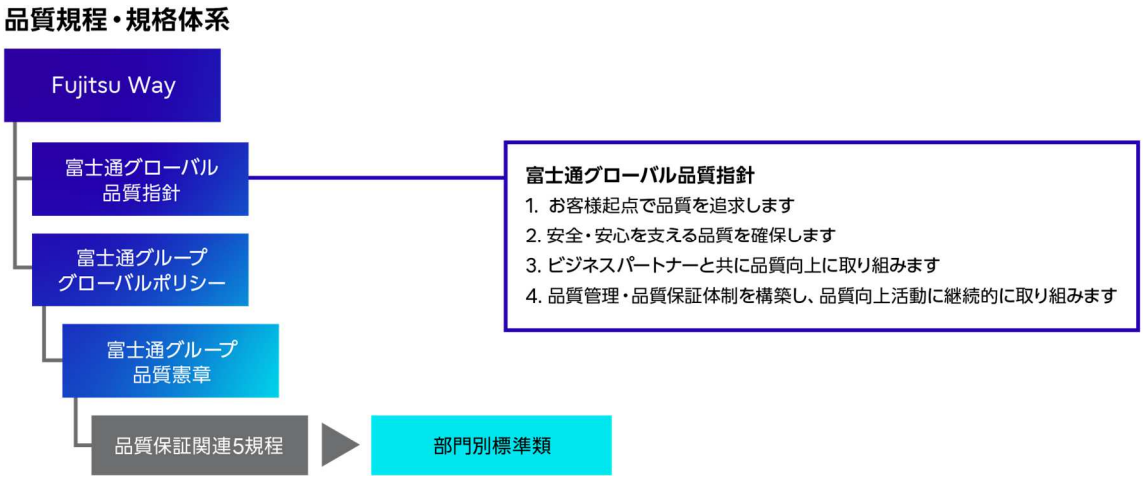
品質への取り組み

方針

富士通グループでは、Fujitsu Way の下に、どの製品・サービスであっても共通して守る指針・憲章と、製品・サービスの特性やお客様の要求事項、法令・規制などに合わせて守る規程・標準類を整備しています。これにより、富士通グループの各事業において、安心・安全な製品・サービスを提供し、発展する社会の基盤をはじめ、多様なお客様の事業や生活を支えています。

「富士通グローバル品質指針」は、Fujitsu Way の大切にする価値観「信頼：テクノロジーを活用し、信頼ある社会づくりに貢献します」を実践するための富士通グループ共通の考え方を示したものです。

お客様に安心してお使いいただける製品・サービスを提供し続けるためにも、「品質」を我々の根幹として捉え、グローバルでの共通認識を持てるよう、本指針を定めています。



「富士通グローバル品質指針」を実践するために、富士通グループグローバルポリシーの下、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・リリース規程や、安全推進規程等）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。

各事業部門・リージョン・グループ会社に品質管理責任者を設置し、CQO のもとグループ全体で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、品質管理責任者を通して展開・適用することで、世界中のお客様に一貫性のある最適な品質の製品・サービス提供に努めています。

また、個々の部門や地域での品質保証活動に加えて、組織の枠を超えたノウハウや情報の共有、利活用や共通課題の解決を図る全社連携活動にも取り組んでいます。

これによりトラブルの再発防止や未然防止、効果的な品質活動の共有により富士通の品質レベルの底上げを図っています。

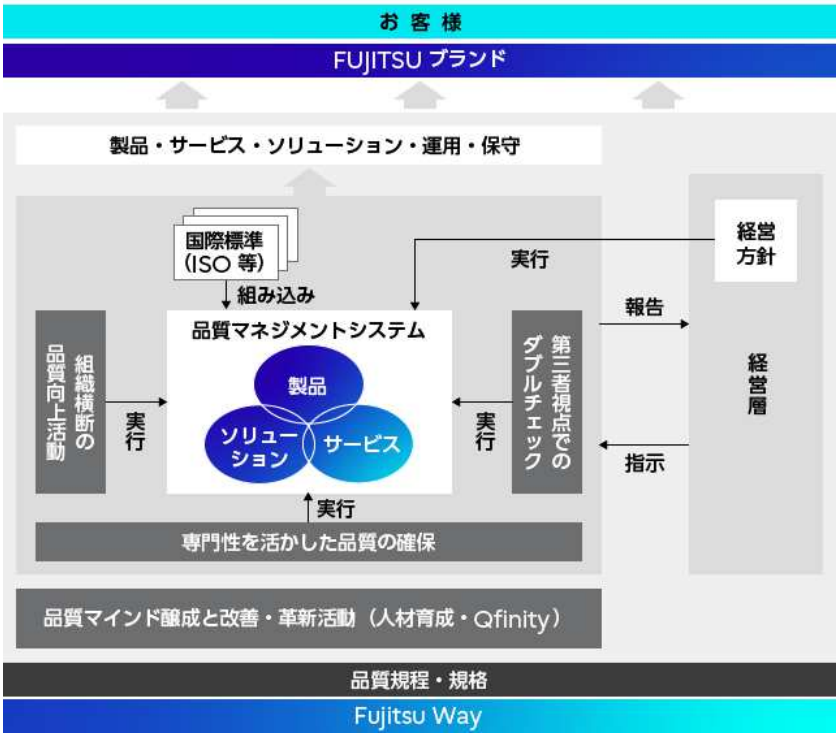
品質マネジメント体制

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・保守までに事業部門、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・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

富士通グループでは、各組織にて品質マネジメントシステムの整備・実践を行うとともに、全社共通の方針・施策の策定から評価・判断に至るサイクルを回すことで、グループ全体で戦略的に品質向上に取り組んでいます。

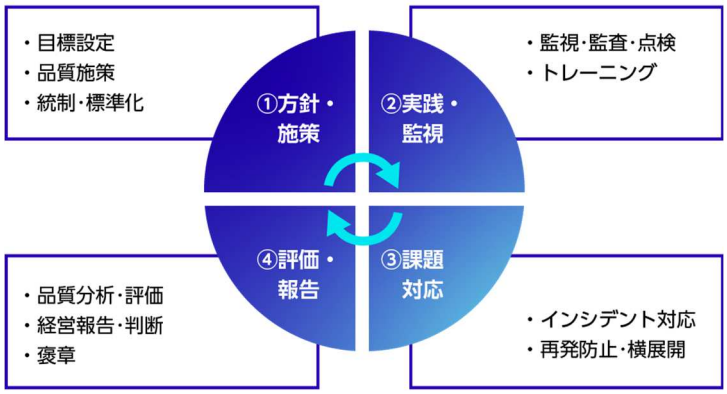
① 方針・施策

目標の設定・見直しを行い、その実現のための品質施策を立案し、富士通グループ全体に展開しています。また、規程やルール等での統制のほか、品質プロセスの標準化を行い、安定した品質の確保を図っています。

② 実践・監視

品質施策やルール、標準プロセスに従い事業を遂行するよう、各事業のプロジェクトを監視し、品質懸念がある場合は監査や点検を通して、是正・改善しています。また、トレーニングにより、人材のスキルアップを図っています。

全社品質向上サイクル



③ 課題対応

製品・サービスに品質問題が発生した場合は、インシデントとして管理し、迅速に対応・対策を行います。重大な品質問題の場合、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への対応と再発防止策を検討します。立案した再発防止策は品質管理責任者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。

④ 評価・報告

定期的に品質状況を整理・分析し、必要に応じて追加の施策を検討します。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。当サイクルを短い単位で繰り返し、経営層や事業部門長も含め、全社一丸となり、品質改善に努めています。

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

新たに任命した CQO の下、富士通グループ全体に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みます。

品質ガバナンスの強化にあたっては、リスク評価の基盤や意思決定モデル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。

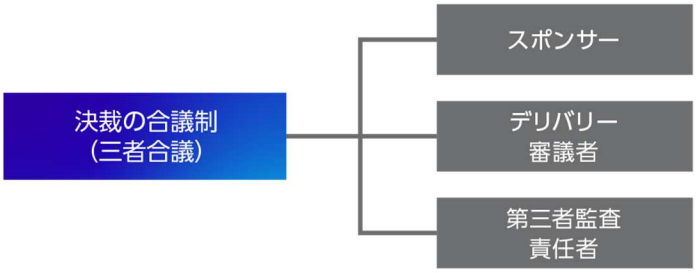
品質統制・リスクモニタリングを支える設計・運用基盤の強化

開発プロジェクトの進捗やテスト密度・不具合検出率等、開発現場で発生す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 上に乗せて 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ます。

意思決定モデル

商談・プロジェクトの推進にあたっては、ステークホルダーによる合議制を取り入れています。従来の BG／リージョン（スポンサー）の判断に加えて、開発部門（デリバリー審議者）、グローバル品質マネジメント本部（第三者監査責任者）による、複数の目で審議を行います。この三者での合議により、ビジネス観点だけでなく、品質・テクノロジー・リソースの観点も踏まえ、多角的に判断しています。

合議による意思決定モデル



商談や開発のフェーズごとにチェックゲートを設け、三者合議で意思決定することで、誤ったプロジェクトの推進や品質問題の発生を抑止し、お客様によりよい提案ができるよう努めています。

日本や世界のつながりがより拡大・発展する中、富士通グループへの期待も大きく変わりつつあります。初めての事業や取り組みに挑戦することが増える中で、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。

2022 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：0 件

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

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。

また、お客様の適用をサポートするため、ご相談窓口をご用意しています。

製品の安全性に関する法令以外の違反、情報とラベリングの違反

- 製品の情報とラベリングの違反：0 件

- 製品の電波法違反に関する不具合：1件
- 欧州電磁界曝露規制に対する不具合：1件

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。

- ISO 9001： 22 本部 認証
- ISO 20000：9 本部 認証

お客様とともに

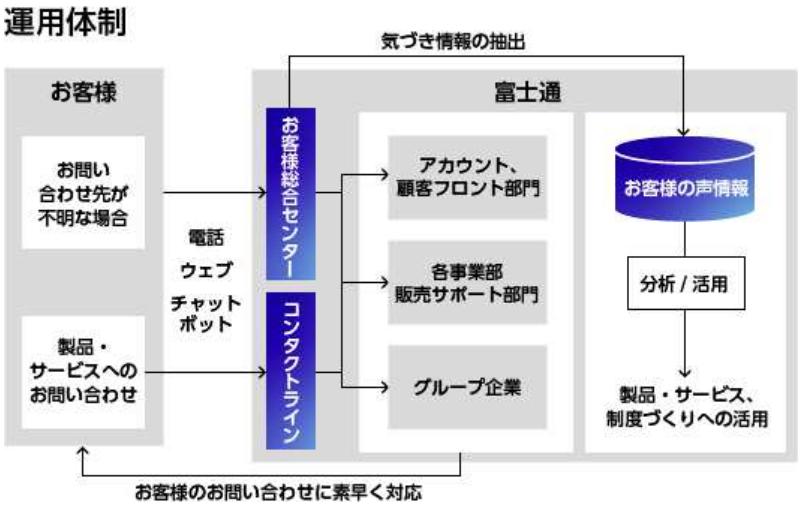
お客様の満足度向上のために

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、年間約 4 万件の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



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。2022 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