富士通グループ情報セキュリティ基本方針
（グローバルセキュリティポリシー）

I. 目的

本情報セキュリティ基本方針（以下、「本基本方針」）は、経済産業省が策定した「サイバーセキュリティ経営ガイドライン」を踏まえ、富士通グループにおける情報セキュリティを確保するための対策、体制等の基本事項を定めるとともに、富士通グループが、ICT を事業の根幹としていることに鑑み、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・向上に積極的に努めることを内外に宣言し、もって FUJITSU Way に掲げる企業理念を実践することを目的とします。

II. 基本原則

(1) 富士通グループは、その事業において、お客様またはお取引先である個人および組織から提供を受けた情報を適切に取り扱い、当該個人および組織の権利および利益を保護します。

(2) 富士通グループは、その事業において、営業秘密、技術情報その他の価値ある情報を適切に取り扱い、富士通グループの権利および利益を保護します。

(3) 富士通グループは、研究開発および人材育成に努め、お客様の情報セキュリティの確保・向上に資する製品およびサービスを適時かつ安定的に提供することにより、お客様、ひいては社会の持続的発展に寄与します。

III. 情報セキュリティの定義

本基本方針において、次に掲げる用語の定義は、次に定めるところによるものとします。

(1) **「情報」**とは、富士通グループのものであるか否か、またネットワーク、書類その他流通形態を問わず、富士通グループが業務上取り扱う情報として関連社内規定に定めるものをいい、公開情報、秘密情報および個人情報を含むものとします。

(2) **「情報セキュリティ」**とは、情報の機密性、完全性、可用性(*)を維持することを意味し、情報管理、物理セキュリティ、サイバーセキュリティを含むものとします。

(3) **「サイバーセキュリティ」**とは、①データの漏えい、滅失、毀損の防止その他当該データの安全管理のために必要な措置、ならびに②IT システムおよびネットワークの安全性および信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていることを意味します。

IV. 情報セキュリティ体制

富士通グループは、「内部統制体制の整備に関する基本方針」に基づき、富士通グループの情報セキュリティを脅かす様々な要因を事業遂行上のリスクとして認識し、以下の内容の情報セキュリティ体制を整備します。

(1) 富士通株式会社の代表取締役社長と業務執行取締役およびリスクマネジメント担当役員で構成される取締役会直属のリスク・コンプライアンス委員会が、当該リスクのグローバルなマネジメントを統括するものとします。

(2) リスク・コンプライアンス委員会は、最高情報セキュリティ責任者（CISO: Chief Information Security

---

(*) 「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいいます。
「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいいます。
「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報および関連資産にアクセスできる状態を確保することをいいます。

Officer）を任命し、富士通グループにおけるグローバルな情報セキュリティ対策の実行に関し、責任と権限を付与するものとします。なお、最高情報セキュリティ責任者は、情報セキュリティ部門や法務部門等のコーポレート部門担当役員が担うものとします。

(3) CISO は、職務の執行状況につき、リスク・コンプライアンス委員会に定期的に報告するほか、必要に応じて随時報告を行うものとします。

(4) リスク・コンプライアンス委員会は、専門的見地から富士通グループのサイバーセキュリティに関する戦略全体の検討を行うサイバーセキュリティ委員会を、下部委員会として設置します。

V. 情報セキュリティ対策

1. 情報セキュリティ対策フレームワークの構築

(1) 富士通グループは、グループ内において守るべき資産を特定し、その所在や内容を把握するとともに、IT システムやネットワークの構成などを踏まえ、情報セキュリティ上のリスクを分析し、当該リスクに応じたグローバルな情報セキュリティ対策を講じます。

(2) 富士通グループは、グローバルな情報セキュリティ対策を着実に実施するための計画を策定し、その実行を評価および継続的に改善するためのプロセス（PDCA サイクル）を整備します。

2. 関連規定の整備および法令等の遵守

(1) 富士通グループは、情報セキュリティ対策を適切に実施するための関連社内規定をグローバルに整備し、役員および従業員に周知徹底させます。

(2) 富士通グループは、情報セキュリティに関連する法令または社内規定の違反に対して、厳しく対処します。

3. リソースの確保

(1) 富士通グループは、グローバルに情報セキュリティ対策を適切に実施するために必要な経営資源を確保・投入します。

(2) 富士通グループは、高度なセキュリティ技術を保有する人材を、計画的かつ継続的に育成・確保します。

(3) 富士通グループは、役員および従業員に対し、情報セキュリティに関する啓発と教育を行い、その重要性を認識させ、行動させます。

(4) 富士通グループは、外部の情報共有活動に積極的に参加し、情報セキュリティ対策に反映します。

4. サプライチェーンや外部委託先等における情報セキュリティ

富士通グループは、サプライチェーンにおけるお取引先および IT システムやネットワークの運用・管理に関する外部委託先に対して、富士通グループの情報セキュリティに関する指針等を周知するとともに、当該指針等に基づく適切な情報セキュリティの確保を求めます。

5. 情報開示

富士通グループは、情報セキュリティへの取り組みに関して、「情報セキュリティ報告書」等を通じて、情報セキュリティの確保に支障が生じない範囲で、開示します。

VI. お客様の情報セキュリティ

(1) 富士通グループは、情報セキュリティに関する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・向上に積極的に努めます。

(2) 富士通グループは、製品およびサービスの開発段階において、セキュリティ品質の確保に努めます。

(3) 富士通グループは、情報セキュリティに関する研究開発を積極的に行い、常に技術・ノウハウの更新に努めます。

VII. 情報セキュリティインシデント対応

富士通グループは、情報セキュリティリスクの顕在化（「情報セキュリティインシデント」という）に備え、以下の内容の体制・対応方針を整備します。

(1) 報告体制や初動対応マニュアルを整備し、関係者に周知徹底させるとともに、定期的かつ実践的な訓練を行います。

(2) 情報セキュリティインシデントに対応するために、CISO の指揮の下、専門チーム（CERT: Computer Emergency Response Team / CSIRT: Computer Security Incident Response Team 等）を組織します。

(3) CISO は、重大な情報セキュリティインシデントが発生した場合には、リスク・コンプライアンス委員会に報告するものとします。

(4) リスク・コンプライアンス委員会は、前項の報告があった場合、当該情報セキュリティインシデントの対応方針を決定するとともに、再発防止を指示し、必要に応じて取締役会に報告するものとします。

(5) 情報セキュリティインシデントに関して、官公庁への届けや関係者への通知を、状況に応じて適切に行います。

VIII. 本基本方針の改廃

本基本方針の改廃は、リスク・コンプライアンス委員会の決定によるものとします。
但し、軽微な改定は、CISO の裁量により、行うことができるものとします。

以　上

制定日：2016 年 4 月 15 日
改定日：2019 年 1 月 31 日