株式会社ルネッサ情報セキュリティ基本方針

制定 2023 年 4 月 3 日
株式会社ルネッサ
代表取締役　青木　皇

（目的）

第 1 条　株式会社ルネッサ（以下「ルネッサ」という。）の情報システムが取り扱う情報には、顧客情報、重要技術情報及び社員の個人情報など、部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

従って、これらの情報資産を様々な脅威から防御することは、ルネッサ及び顧客の財産、並びに従業員のプライバシーの保護や、業務の安定的な運営のためにも必要不可欠であり、このことは、ルネッサに対する社会らの信頼維持向上に寄与するものである。

ルネッサが保有する情報資産の機密性、完全性及び可用性を維持するため、ルネッサが実施する情報セキュリティ対策の基本的な方針を定めることを目的とする。

（定義）

第 2 条　本基本方針の用語の定義は、次のとおりとする。

(1)　ネットワーク

ルネッサ本社及び工場並びに外部と相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）及び電磁的記録媒体で構成され、通信処理を行う仕組みをいう。

(2)　情報システム

ネットワーク、ハードウェア、ソフトウェア及び電磁的記録媒体で構成され、業務処理を行う仕組みをいう。

(3)　情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク、情報システム及びそれらで取り扱う全てのデータ（紙媒等を含む。）をいう。

(4)　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(5)　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(6)　機密性

情報にアクセスすることが許可された者だけがアクセスできることを確保することをいう。

(7)　完全性

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う。

(8)　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(9)　インターネット接続系

インターネットメール、大容量ファイル送受信システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(対象とする脅威)

第3条　情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

(1)　不正アクセス、ウイルス攻撃、サービス不要攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2)　情報資産の悪意ある持出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3)　地震、落雷、火災等の災害によるサービス及び業務の停止等

(4)　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

(適用範囲)

第4条　本基本方針の適用範囲は、次に定めるところによる。

(1)　適用対象者

社員、非正規雇用労働者、及び出向社員並びに委託事業者とする。

(2)　適用資産

ルネッサが管理する全ての情報資産とする。

(情報セキュリティポリシーの位置付けと社員等の遵守義務)

第5条　情報セキュリティポリシーは、ルネッサが所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最上位に位置するものである。

従って、代表取締役をはじめとしてルネッサが所掌する情報資産に関する業務に携わる全ての社員等及び委託事業者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

(情報セキュリティ管理体制)

第6条　情報資産の統一的な情報セキュリティを確保するため、情報セキュリティ対策を推進・管理するための組織体制を確立するものとする。

(情報資産の分類)

第７条　情報資産については、機密性、完全性及び可用性に応じての分類を行い、当該分類に応じ適切な情報セキュリティ対策を実施するものとする。

（情報システム全体の強靭性の向上）

第８条　情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の３段階の対策を講じるものとする。

(1)　端末からの情報持出し不可設定や端末への多要素認証の導入等により、情報の漏洩を防ぐ。

(2)　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（情報セキュリティ対策）

第９条　第３条で示した脅威から情報資産を保護するために、次の情報セキュリティ対策を講ずるものとする。

(1)　物理的セキュリティ対策

情報システムの設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(2)　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、社員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(3)　技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。

(4)　運用におけるセキュリティ対策

システム開発等の委託、ネットワークや情報システムの監視、情報セキュリティポリシー厳守状況の確認等運用面の対策を講ずる。

(5)　緊急時におけるセキュリティ対策

緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

(6)　業務委託と外部サービスの利用時におけるセキュリティ対策

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した仕様書により契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて措置を講ずる。

外部サービスを利用する場合には、利用に係る規定を整備し対策を講ずる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（情報セキュリティ監査等の実施）

第 10 条　情報セキュリティポリシーが厳守されていることを検証するために、定期的に又は必要に応じて監査を実施する。

（見直しの実施）

第 11 条　情報セキュリティ監査の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するために新たに対策が必要となった場合には、適宜情報セキュリティポリシーの見直しを実施する。

（情報セキュリティ対策基準の策定）

第 12 条　ルネッサの様々な情報資産について、前 3 条の情報セキュリティ対策を講ずるに当たっては、厳守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を別途、策定するものとする。

（情報セキュリティ実施手順の策定）

第 13 条　情報セキュリティ対策基準を厳守して情報セキュリティ対策を実施するために、情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、別途、情報資産の情報セキュリティ実施手順を策定するものとする。

（情報セキュリティ対策基準及び実施手順の扱い）

第 14 条　情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることによりルネッサの会社運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

（罰則）

第 15 条　この基本方針に定められた情報セキュリティ対策に違反した社員等及び委託事業者は、関連法令等に基づき、懲戒処分、損害賠償請求等の対象となることがある。

附　　則

この基本方針は、2023 年 4 月 3 日から運用開始する。