

NEC キャピタルソリューショングループ 情報セキュリティ報告書

2023 年 3 月 31 日

NEC キャピタルソリューション株式会社

<お問合せ先>

NEC キャピタルソリューション株式会社 法務部

〒108-6219

東京都港区港南二丁目 15 番 3 号

品川インターシティ C 棟 19 階

1. 情報セキュリティ基本方針

当社グループは、情報セキュリティの確保を経営上の重要事項と位置づけ、情報セキュリティに関する基本方針を以下の通り定めています。本基本方針は、当社グループの情報システムならびに当社グループが独自に所有する情報および当社グループのお客様・取引先等から提供を受けた情報等について適切なセキュリティ対策を講じることにより、正常な企業活動および組織運営を維持し、お客様・取引先等からの信頼を得ることを目的としています。

1. 当社グループは、情報セキュリティ管理体制を確立し、情報資産の適切な管理に努めます。
2. 当社グループは、情報セキュリティに関する社内規程を整備、実施します。
3. 当社グループは、情報セキュリティの確保に必要な教育を継続的に実施します。
4. 当社グループは、適切な人的・組織的・技術的施策を講じ、情報システムおよび情報資産に対する不正侵入、情報漏えい、改ざん、紛失・盗難、破壊、利用妨害等が発生しないよう努めます。
5. 当社グループは、万一情報セキュリティ上の問題が発生した場合には、すみやかにその原因を究明し、その被害を最小限に止めるとともに再発防止に努めます。
6. 当社グループは、情報セキュリティに関係する法令、その他の社会的規範を遵守します。
7. 当社グループは、情報資産管理の基本方針として、以下の項目を定めます。
 - ① 業務上必要な情報のみ取得し保有します。
 - ② 情報は、業務上必要な者に対してのみ開示します。
 - ③ 情報を利用できる権限の付与は、業務上必要最低限にとどめます。
8. 当社グループは、前各号の活動を継続的に見直し、改善に努めます。

制定 2005 年 2 月 21 日

最近の改正 2019 年 10 月 1 日

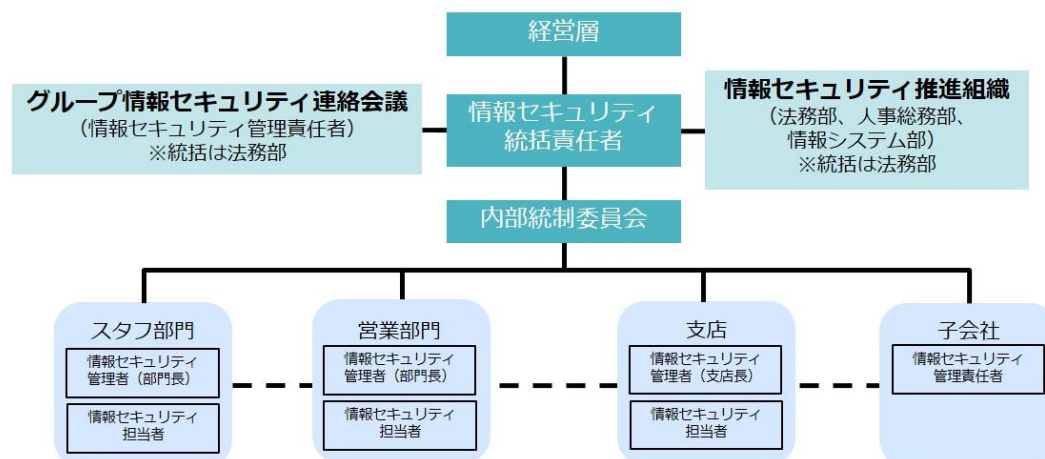
NEC キャピタルソリューション株式会社

代表取締役社長 菅沼 正明

2. 情報セキュリティ管理体制

当社グループは、情報セキュリティレベルの更なる向上を目指し、以下の管理体制を整備しています。情報セキュリティ統括責任者のもと、情報セキュリティ推進組織が中心となり、情報セキュリティ目標を設定し、施策を推進するとともに、内部統制委員会およびグループ情報セキュリティ連絡会議で情報セキュリティ活動状況や重点課題等を審議し、経営層へ報告等を行っています。

情報セキュリティ管理体制図



3. 情報セキュリティ人材

当社は、当社グループ各社の役員および社員一人ひとりのセキュリティ意識を高めると同時に、セキュリティスキルの向上やセキュリティプロ育成の施策を推進し、情報セキュリティに関する豊富な人材を確保しています。

情報セキュリティ、個人情報保護教育

当社は、毎年、情報セキュリティおよび個人情報保護教育を実施し、当社グループ各社の役員および社員（派遣社員、構内作業員含む）全員が受講しています。また教育内容につきましても、新しい脅威への対応や意識啓発、情報の取り扱い、テレワーク時のセキュリティ対策等、セキュリティ脅威のトレンドを考慮したうえで毎年更新し、情報セキュリティの知識やスキルの継続的な向上を図っています。

教育実績 <https://www.necap.co.jp/csv/governance/compliance.html>

知識と経験を兼ね備えた情報セキュリティ組織の運営

当社は、情報処理安全確保支援士を含むメンバーで構成した情報セキュリティ推進組織が中心となり、全営業部店および子会社の情報セキュリティ管理責任者等と連携し、各種施策を展開しながら情報セキュリティの維持向上に努めています。また、毎年、教育による知識レベルの向上を図りつつ、実務レベルでの情報セキュリティに関する取組の検討と実行を通じて、情報資産管理や個人情報保護の対応力を強化しています。

情報セキュリティの遵守事項への誓約

当社は、お客様・取引先等の情報や個人情報、企業秘密を扱う際に遵守すべき事項について、役員および社員から誓約書を取得しています。

4. 情報セキュリティ対策

当社グループは、情報セキュリティに関するリスクを把握・管理するために、グループ情報セキュリティ連絡会議等を通じてリスク対策の遂行状況をモニタリングしています。また、リスク対策の有効性評価および改善を行うことにより、当社グループ全体における情報セキュリティインシデント発生の未然防止や、影響の最小化を目指しています。

サイバー攻撃対策

一例として、以下の対策を実施しています。

- ・未知の攻撃に対応したエンドポイントセキュリティ対策
- ・ランサムウェア等の世界的な脅威に備えた標的型攻撃対策
- ・稼働サーバの定期的な脆弱性対策

インシデント対応体制

当社グループは、情報セキュリティインシデント発生時において、被害を最小限に抑えるため迅速かつ適切な対応および業務の適正化をはかるための体制を整備しています。また、近年のランサムウェア等の世界的な脅威に備え、役員および社員に対して標的型攻撃メール訓練や業務停止等を想定した模擬訓練を実施しています。

サプライチェーンセキュリティ対策

当社グループは、お客様の大切な情報を守るため、ビジネスパートナーや委託先等を含めたサプライチェーンに対し、情報セキュリティ管理体制や対策状況の確認・審査を実施しています。

第三者認証の効率的な活用

当社は、ISO/IEC27001 やプライバシーマークの認証を取得し、第三者認証の基準規格に基づいた運用を構築しています。また、教育、監査、マネジメントレビュー等の共通事項をまとめて行い、効率的な運用を実施しています。

・ISO/IEC27001 の認証取得

当社は、2006 年に情報セキュリティマネジメントシステムの国際規格である ISO/IEC27001 の認証を全営業部店で取得しています。ISO/IEC27001 は、組織が保有する情報に関わる様々なリスクを適切に管理し、組織の価値向上をもたらす ISMS の国際規格です。



・プライバシーマークの認証取得

当社は、2020 年に「JISQ 15001（個人情報保護マネジメントシステム-要求事項）」に準拠した個人情報保護マネジメントシステムを確立し、プライバシーマークを取得しています。



個人情報およびプライバシー保護

・個人情報保護について

当社は、お客様の個人情報を適切に保護するため、「個人情報保護方針」を制定し、この方針に従い個人情報を取り扱っています。また、当社は、個人情報の漏えい等の事故への対応手順を定めているほか、個人情報の取扱いを外部へ委託する場合は、適正な委託先の選定、委託契約の締結、委託先における個人情報の取扱い状況の把握を行い、安全管理に努めています。

個人情報保護方針 <https://www.necap.co.jp/policy/index.html>

個人情報のお取扱いについて <https://www.necap.co.jp/policy/index.html#anc-p0401>

・プライバシーについて

当社グループは、「NEC キャピタルソリューショングループ人権方針」において、職場や業務を通じて知り得た個人のプライバシーを尊重し、事業活動がプライバシーの侵害等を含めた人権問題を引き起こさないために最善の注意を払うよう定めています。また、当社は、口座番号等の経済的な影響を与える情報や、出生地等の機微（センシティブ）情報、携帯電話番号等のプライバシー性の高い情報について、本人の同意を得ない取得を原則禁止としています。

NEC キャピタルソリューショングループ人権方針 <https://www.necap.co.jp/csv/humanrights.html>

専門家の活用

当社は、情報セキュリティに関する専門家の助言や指導を通じて、当社グループ全体の情報セキュリティレベル向上を推進しています。