情報セキュリティの強化

関連する GRI スタンダード：102-12/103-2/203-2

方針・考え方

社会経済のデジタル化の進展や国際情勢の変化を受け、サイバー攻撃をはじめとするセキュリティ脅威はますます高度化・深刻化しています。このような中、ICT サービスインフラとお客さまの基本的な権利および自由、そして情報資産を守り、デジタル経済の成長に向けた健全な基盤を提供することは NTT グループの責務です。

2018 年に策定した中期経営戦略を受け、セキュリティにおいても、デジタル経済のインフラを支え、自由、オープン、安全な ICT 基盤の構築と発展に貢献することをミッションと定義し、お客さまと NTT 自身のデジタルトランスフォーメーションを実現すること、またお客さまから NTT グループを選んでいただける理由となることをビジョンとして掲げました。

これらの実現に向け、自らのスケールを活かした研究開発に取り組むこと、早期検知と迅速な対応能力に優れること、誠実さと高度な技能という価値を共有する人材群の育成に努めること、利益主義を超え社会に対して先導的な知見を発信することを柱に取り組んでいきます。

世界的にますます関心の高まる個人情報の適切な取り扱いや、国際的なイベントなどに合わせた大規模で高度なサイバー攻撃に対する対策も重要です。NTT グループは、デジタル社会を創造するグローバルなコミュニティの一員として、セキュリティ事業を通じて社会的課題の解決に貢献していきます。

NTT グループ情報セキュリティポリシー

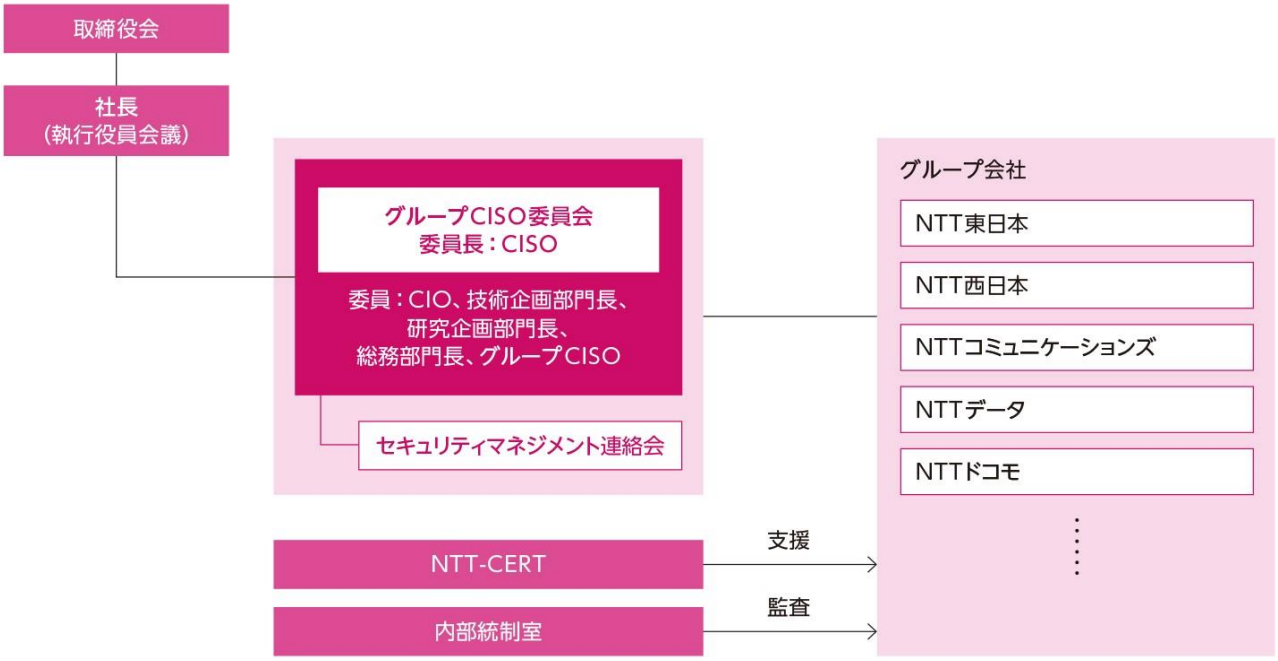
私たち NTT グループは常に安心・安全なサービスを提供し続け、いつまでも皆様に信頼される企業でありつづけたいとの考え方のもと、情報通信産業の責任ある担い手として、以下の方針に従い、情報セキュリティの確保に努めブロードバンド・ユビキタス社会の健全な発展に貢献してまいります。

1. ブロードバンド・ユビキタス社会における情報セキュリティの重要性を深く認識し、安心・安全で便利なコミュニケーションネットワーク環境の構築に努め、情報セキュリティの確保に取り組んでまいります。
2. 情報を保護することは、NTT グループの事業活動の基本であり、企業としての重要な社会的責任であることを NTT グループ会社の役員・従業員が十分に認識し、通信の秘密の厳守はもとより個人情報保護法等の関連法令等を遵守してまいります。
3. 情報セキュリティの管理体制を整備し、情報への不正なアクセス、情報の紛失・改ざん・漏洩の防止等に向けた物理面、システム面での厳格なセキュリティ対策の実施、社員教育の徹底、委託先への適切な監督等、情報の保護に向けた必要な取り組みを継続的に実施してまいります。

NTT グループ情報セキュリティポリシー　https://www.ntt.co.jp/g-policy/index.html

推進体制

NTT グループは、CISO（Chief Information Security Officer）を最高責任者とする情報セキュリティマネジメント体制を整備し、情報セキュリティの管理を徹底しています。また、「グループ CISO 委員会」を設置し、グループにおける情報セキュリティマネジメント戦略の策定や各種対策の計画・実施、人材の育成など、グループ各社と連携しながら取り組んでいます。



主な取り組み

サービスセキュリティの強化

重要な社会インフラであり、社会経済のデジタル化の基盤となる、安心・安全な情報通信サービスを提供するため、電気通信設備、IT サービス環境、およびスマートシティやスマートビルディングなどのサービスの全てにおいて、セキュリティの強化に取り組んでいます。

NTT グループにおけるグローバル連携

グローバル事業の統合を受け、セキュリティにおいてもグローバル連携を進めています。多様な事業や地域を含む NTT グループの連携にあたっては、リスクベースマネジメントの考え方と、共通言語となるフレームワークを導入し、「特定」「防御」「検知」「対応」「復旧」の観点から、グループ共通の満たすべき基準を定めています。

グローバルコミュニティへの参画と貢献

米欧を中心に、各国政府や産業界のサイバーセキュリティ強化の取り組みに参画し、セキュリティ脅威情報やベストプラクティスの共有と、互いに信頼し合える企業と組織によるコミュニティの形成に取り組んでいます。

NTT グループのセキュリティ人材の育成

グループ内のセキュリティ人材育成強化として、セキュリティ人材を、質・量ともに充実させることを目標に、人材タイプや人材レベルに応じた人材育成施策をグループ各社で推進しています。

NTT グループのセキュリティ人材体系

		呼称	人材タイプ		
			セキュリティマネジメント・コンサル	セキュリティ運用	セキュリティ開発・研究
人材レベル	上級	セキュリティマスター セキュリティプリンシパル	業界屈指の実績を持つ第一人者		
	中級	セキュリティプロフェッショナル	深い経験と判断力を備えたスペシャリスト		
	初級	セキュリティエキスパート	必須知識を持ち担当業務を遂行できる実務者		

情報セキュリティ研修

各グループ会社にて、全従業員および協力会社社員に対し、情報セキュリティリテラシー向上を目的とした研修を実施しています。研修はｅラーニング形式で実施し、受講者は年１回の受講が義務づけられています。今後は、グループ全体で業務に必要な情報セキュリティ知識の同一水準化を目指し、研修コンテンツの統一化を検討しています。これにより、NTT グループのセキュリティケーパビリティを向上させ、お客さまや社会に安全安心な事業を提供するための人材力を強化することを目指します。

研究開発の取り組み

サービスセキュリティのための技術開発に加え、セキュリティ要素技術の開発にも力を入れています。新たに、世界レベルの先駆的研究者を中心として、サイバーセキュリティと暗号技術に取り組むグローバル研究所を 2019 年に設立しました。

CSIRT の運営

NTT グループは、コンピュータセキュリティに係るインシデントに対応する組織（CSIRT：Computer Security Incident Response Team）として、2004 年に「NTT-CERT」を立ち上げ、グループに関連するセキュリティインシデント情報の受け付け、対応支援、再発防止策の検討、トレーニングプログラムの開発およびセキュリティ関連情報の提供などに取り組んでいます。さらに、NTT グループのセキュリティ分野における取り組みの中核として、情報セキュリティに関する信頼できる相談窓口を提供し、NTT グループ内外の組織や専門家と協力して、セキュリティインシデントの検知、解決、被害極小化および発生の予防を支援することにより、NTT グループおよび情報ネットワーク社会のセキュリティ向上に貢献しています。

NTT-CERT は、US-CERT※1 や JPCERT コーディネーションセンター※2 と連携するとともに、FIRST や日本シーサート協議会※3 への加盟などにより国内外の CSIRT 組織と連携し、動向や対策法などの情報共有を図っています。また、内閣サイバーセキュリティセンター（NISC）が主催する分野横断的演習にも参加し、ノウハウ共有・情報収集に努めています。加えて、NTT-CERT はグループ各社の CSIRT 構築を推進し、対応能力の向上にも努めています。

今後も、NTT-CERT は脆弱性や攻撃情報などの収集範囲を DarkWeb などにまで広げ、情報分析プラットフォームの強化、サイバー脅威対応のさらなる自動化・高度化など、変化する脅威に継続的に対応していきます。

※1 US-CERT：米国国土安全保障省（DHS）配下の情報セキュリティ対策組織
※2 JPCERT コーディネーションセンター：インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデントについて、日本国内に関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている組織
※3 NTT-CERT は日本シーサート協議会の発起人

NTT-CERT　https://www.ntt-cert.org/
日本シーサート協議会　https://www.nca.gr.jp/
FIRST Forum of Incident Response and Security Teams　https://www.first.org/

NTT グループにおける CSIRT の取り組み