Safety and Security

安心・安全なコミュニケーション

安心・安全なコミュニケーション

CSR 重点活動項目	中期目標	CSR 定量指標	目標値	目標達成年度	実績（年度）		
					2017	2018	2019
情報セキュリティの強化	外部からのサイバー攻撃に伴う電気通信サービスのサービス停止件数※1	サービス停止件数	0 件	2020 年	―	―	0 件
	外部からのサイバー攻撃に伴う個人情報流出件数※1	個人情報流出件数	0 件	2020 年	―	―	1 件
個人情報保護	個人情報の流出・漏えいを発生させない	個人情報の漏えい件数	0 件	―	2 件	1 件	1 件
通信サービスの安定性と信頼性の確保※4	通信サービスを安定的に提供し、重大通信災害を発生させない	安定サービス提供率※2	99.99%	―	100%	100%	100%
		重大事故発生件数※3	0 件	―	0 件	0 件	0 件

※1　2020 年度より新設

※2　〔1－重大事故総影響時間（影響ご利用者様数×重大事故対象時間）／主要サービス提供総時間（ご利用者様数×24 時間×365 日）〕×100%

※3　電気通信役務の提供を停止または品質を低下させた、以下の条件を満たす事故の件数

- 緊急通報（110、119 など）を扱う音声サービス：1 時間以上かつ 3 万人以上
- 緊急通報を扱わない音声サービス：2 時間以上かつ 3 万人以上、または 1 時間以上かつ 10 万人以上
- インターネット関連サービス（無料）：12 時間以上かつ 100 万人以上、または 24 時間以上かつ 10 万人以上
- その他の役務：2 時間以上かつ 3 万人以上、または 1 時間以上かつ 100 万人以上

※4　集計範囲：通信 4 社（NTT 東日本、NTT 西日本、NTT コミュニケーションズ、NTT ドコモ）

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

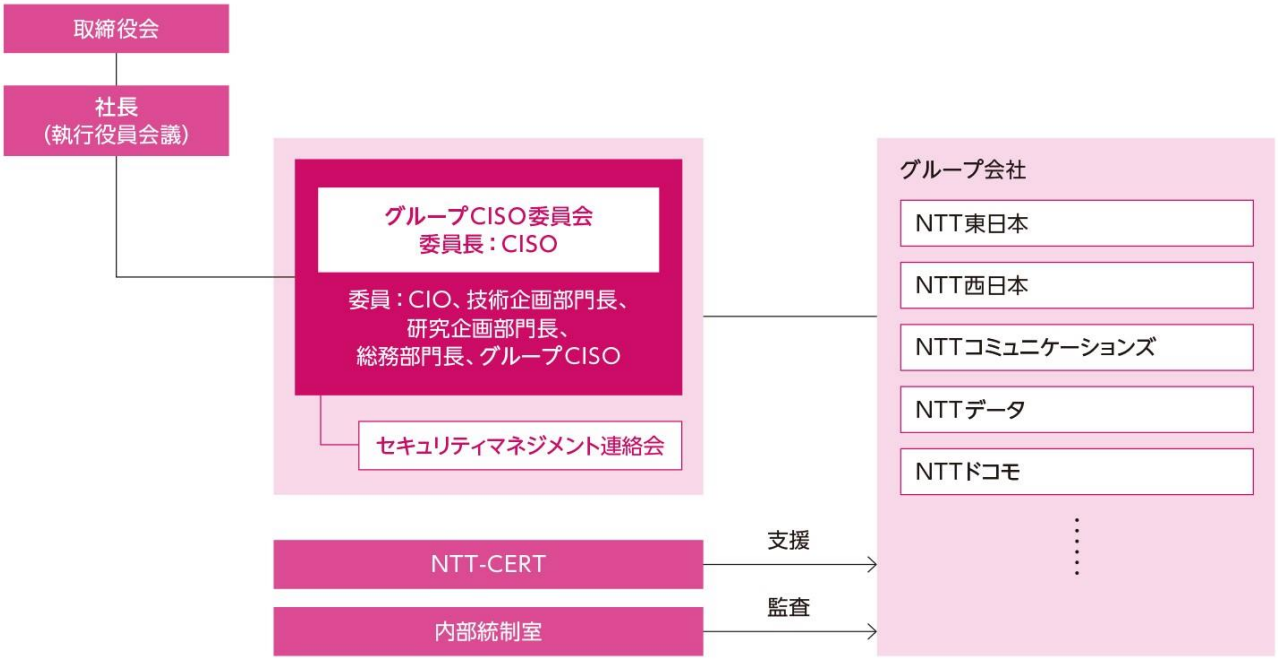
私たち NTT グループは常に安心・安全なサービスを提供し続け、いつまでも皆様に信頼される企業でありつづけたいとの考え方のもと、情報通信産業の責任ある担い手として、以下の方針に従い、情報セキュリティの確保に努めブロードバンド・ユビキタス社会の健全な発展に貢献してまいります。

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。

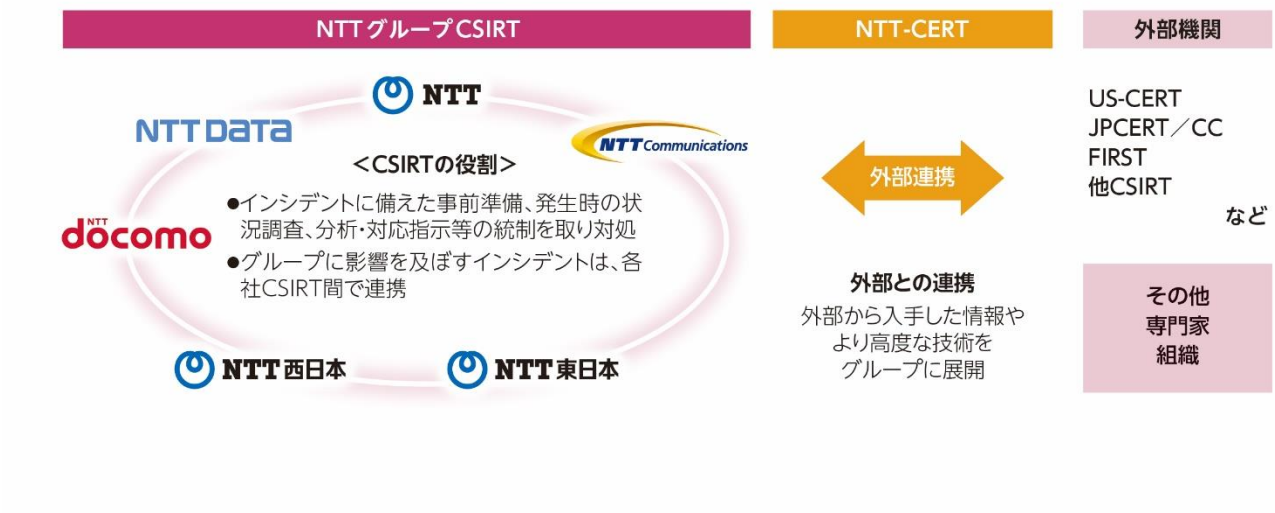
NTT-CERT は、US-CERT※1 や JPCERT コーディネーションセンター※2 と連携するとともに、FIRST や日本シーサート協議会※3 への加盟などにより国内外の CSIRT 組織と連携し、動向や対策法などの情報共有を図っています。また、内閣サイバーセキュリティセンター（NISC）が主催する分野横断的演習にも参加し、ノウハウ共有・情報収集に努めています。加えて、NTT-CERT はグループ各社の CSIRT 構築を推進し、対応能力の向上にも努めています。

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



個人情報保護

関連する GRI スタンダード：103-2

方針・考え方

NTT グループは、個人のお客さまから法人のお客さまに至るまで、多数の個人情報をお預かりしています。近年、お客さまからの個人情報保護への関心は高まる一方です。また、2017 年の個人情報保護法の改正や 2018 年の EU（欧州連合）の一般データ保護規則（GDPR）の施行など、法規制の面からも個人情報保護や情報管理の徹底の重要性がますます高まっています。

このような中、個人情報の漏えいは、NTT グループの企業価値のき損やお客さまの流出など、事業運営にさまざまな影響を及ぼす可能性があり、最重要事項として個人情報の管理を徹底していく必要があります。

推進体制

NTT グループは、「NTT グループ情報セキュリティポリシー」のもと、お客さまや株主の皆さまの個人情報保護に関する方針や、マイナンバー制度にともなう特定個人情報の保護に関する方針などを Web サイト上で公開しています。これらの方針では、NTT グループがお預かりしている個人情報の開示・訂正・利用停止などのお申し出に対応するための手続きについても定めています。また、セキュリティマネジメント体制としては、NTT において情報セキュリティの最高責任者として CISO（Chief Information Security Officer）を設置し、NTT グループとしての情報セキュリティを徹底しています。（P054 参照）

NTT の個人情報保護に関する方針

- **お客様個人情報の保護に関する方針** https://www.ntt.co.jp/kojinjo/okyaku.html
- **株主様個人情報の保護に関する方針** https://www.ntt.co.jp/kojinjo/kabu.html
- **お取引先等特定個人情報等の保護に関する方針** https://www.ntt.co.jp/kojinjo/okyaku-m.html
- **株主様特定個人情報等の保護に関する方針** https://www.ntt.co.jp/kojinjo/kabu-m.html

主な取り組み

NTT では、お客様個人情報の取り扱いにあたり、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置を講じています。

（1） 組織的安全管理措置
委員会や各組織の管理責任者などの管理体制の構築、社内規程の整備、管理台帳やプロセス管理表などのステートメントの作成、さらに継続的な改善など組織的な管理体制を構築しています。

（2） 人的安全管理措置
役員、社員、派遣社員を問わず、お客様個人情報を取り扱う全ての従業者に、お客様個人情報保護の重要性を周知・啓発し、守秘義務契約の締結とともに必要な監査・監督を行い、その実効性を担保します。

（3） 物理的安全管理措置
お客様個人情報を取り扱う建物やフロアの入退室管理、盗難等の防止、火災・落雷等によるお客様個人情報のき損に対する対策、システムや文書の持ち出し・移送・保管時における施錠などの諸対策を講じます。

（4） 技術的安全管理措置
個人データにアクセスする場合の認証・権限管理・制御・記録などのアクセス管理、システムへの不正ソフトウェア対策やウィルス対策、暗号化や責任の明確化などによる移送・送受信時の対策、情報システムの監視などの技術的安全管理措置を講じます。

国内グループ各社では、改正個人情報保護法に基づき、それぞれの事業に合わせた個人情報保護体制を確立し、物理面、システム面での厳格なセキュリティ対策を講じ、委託先への適切な監督など、情報保護に向けた取り組みを継続的に実施しています。

国内グループ各社の主な取り組み

- 規程・規則として各種社内ルールを制定
- 上記社内ルールの適切な運用に向けた社員研修の実施
- 情報セキュリティ管理を推進する組織の設置
- 情報への不正なアクセス、情報の紛失・改ざん・漏えいの防止、ウィルス対策や外部への情報持ち出しなどを管理するセキュリティ対策システムの導入

また、グローバルに事業を展開しているNTTグループ各社においては各国の法規制にしたがって対応しています。2018年5月に施行されたEUの一般データ保護規則（GDPR）への対応にあたっては、NTTグループ間で議論し規則の遵守を推進するとともに、NTTグループ各社において、個人情報の取得時やEU域外への移転にともなう必要な措置を行い、国内外のNTTグループ会社間での社員情報の共有についても、同規則や各国の法規制を踏まえた対応を進めています。

個人情報対応窓口の設置

NTTにおいて「お客様個人情報対応窓口」を設けるとともに、NTTグループ各社において各種サービスなどの個人情報に関するお問い合わせ窓口を設けています。なお、NTTは持株会社のため電気通信サービスの提供を行っておらず、サービスの提供などに係る個人情報に関するお問い合わせについてはサービスを提供している各事業会社の窓口にお問い合わせいただいています。

また、法令等に基づく個人情報に関する照会などがあった場合の対応についても、各事業会社の情報セキュリティの責任者の責任のもと実施しています。

日本電信電話株式会社 お客様個人情報対応窓口

電子メール：ntt.kojin.uz@hco.ntt.co.jp

https://www.ntt.co.jp/kojinjo/okyaku.html

通信サービスの安定性と信頼性の確保

関連する GRI スタンダード：103-2/203-1/413-1

方針・考え方

NTT グループは、平常時から社会の通信インフラを支えることを使命とする企業グループとして、いつでもどこでもつながる信頼性の高い通信ネットワークの構築に尽力しています。災害時には通信の重要性が高まることから、災害に対する救助・復旧活動をはじめ、公共秩序の維持に必要な重要通信、110 番・119 番・118 番といった緊急通信の確保、に努めております。とくに日本は地震や台風といった自然災害が多く、甚大な被害をもたらした東日本大震災では、通信の重要性があらためて認識されました。首都直下型地震や南海トラフ地震などの発生も想定される中、こうした起こりうる災害に備え、通信の安定性と信頼性を確保することがますます求められています。

NTT グループは、「重要通信の確保」「サービスの早期復旧」「ネットワークの信頼性向上」を災害対策の基本と位置づけ、東日本大震災以降はこれらをさらに強化しています。また、中期経営戦略に「災害対策の取り組み」を掲げ、更なる通信インフラの強化、初動対応の強化（プロアクティブな災害対応）、被災した方々への情報発信力の強化にも注力しています。

NTT グループの「災害対策に関わる基本方針」

推進体制

NTT、NTT 東日本、NTT 西日本、NTT コミュニケーションズ、NTT ドコモの 5 社は災害基本法における指定公共機関として、防災に関して取るべき措置を定め、円滑かつ適切な災害対策を遂行するために、「防災業務計画」を定めています。各社は防災業務計画に基づき、あらかじめ災害対策組織を編成し、災害発生時はその規模・状況に応じた態勢を取るとともに、関係政府機関とも緊密な連携を図り、円滑かつ適切な災害復旧と重要通信の確保に努めています。

また、日頃より通信サービスが途絶えないよう、通信伝送路の多ルート化や通信ビル・通信基地局の停電対策、通信ビルの耐震性強化などを図り、通信の信頼性向上に努めるとともに移動電源車などの災害対策機器の全国配備を充実させ、大規模災害を想定した訓練も繰り返し実施し、緊急通信や重要通信を確保できるよう、日々対策に取り組んでいます。

NTT グループ「防災業務計画」　https://www.ntt.co.jp/saitai/plan.html

主な取り組み

重要通信の確保

NTT グループは、災害時に必要な通信を確保するため、被災地での特設公衆電話の設置や携帯電話などの貸し出し、被災地の方の安否を確認するための手段の提供など、さまざまな取り組みを実施しています。あわせて、110 番・119 番・118 番などの緊急通報回線の被災に備え、警察本部・消防本部・海上保安本部などの指令台まで複数ルートの回線を設置するなどの対策を行っています。

さらに、大規模災害が発生した際、交通機関遮断などの社会的混乱が予想されます。その際、各通信事業者における携帯電話および固定電話の通話規制状況などを総合的に勘案し、必要と判断される場合には、公衆電話から発信する際の通話料などを無料化※しています。

※ 通話料を設定している事業者においては通話料を無料とし、接続料を設定している事業者においては接続料を事業者間で精算しない扱いとしています。具体的な事業者名などについては下記 Web サイトをご確認ください。

- **NTT 東日本エリアの公衆電話の無料化措置について** http://www.ntt-east.co.jp/info-st/saigai/index.html
- **NTT 西日本エリアの公衆電話の無料化措置について** https://www.ntt-west.co.jp/ptd/basis/disaster.html

災害発生時の安否確認や情報収集を容易にするサービスの提供

大規模な災害が発生し、被災地への電話がつながりにくい状況が発生した場合などには、安否確認手段として下記のようなサービスを開設・提供しています。

主なサービス

災害用伝言ダイヤル（171）	被災地との安否確認手段として、電話により音声の伝言をお預かり
災害用伝言板（web171）	インターネット経由でテキストによる伝言をお預かり
災害用音声お届けサービス（i モード/sp モード/mopera U）	携帯電話から音声メッセージで安否情報をお届け
災害用伝言板（i モード/sp モード）	携帯電話から文字による伝言をお預かり

災害発生時などに、これらの安否確認手段を開設した場合には、速やかに報道機関や Web サイトなどを通じて、お客さまへお知らせしています。

「災害用伝言板（web171）」と「災害用伝言板（i モード/sp モード）」は、検索機能を連携させることで、当該サービスを提供する各社に登録された内容を、いずれの提供事業者のサービスからも参照することが可能になったほか、安否情報登録時に指定された通知先へメールや音声で通知を行う機能があります。また、「災害用伝言板（web171）」は英語・中国語・韓国語、「災害用伝言板（i モード/sp モード）」は英語に対応し、登録可能な伝言数や保存期間を拡大するなど、利便性向上を図っています。

なお、災害用伝言板（web171）は 2019 年 8 月よりおよび株式会社 NTT ドコモ、KDDI 株式会社、ソフトバンク株式会社提供の「災害用伝言板」との連携により、それぞれで登録された伝言内容を、相互に確認が可能となりました。

通信サービスの安定性と信頼性確保

NTT グループは、移動電源車やポータブル衛星装置などの機動性のある機器の配備や機能の高度化、各地域での防災訓練に参加するなど、通信サービスの早期復旧に努めています。また、災害に強い通信設備の構築に取り組むとともに、通信ネットワークが常に正常に機能するよう、定期的な安全パトロールや予防保全的な装置交換など保守・運用にも万全な体制で臨むことで、災害に強い通信ネットワーク・設備づくりに努めています。

通信設備の耐災性確保

通信設備や建物、鉄塔などは、地震・風水害・火災・停電などさまざまな災害を想定した設計基準を定め、耐災性を確保しています。

主な対策例

- NTT の通信ビルや鉄塔を震度 7 クラスの地震や風速 60m/s の大型台風にも耐えられるように設計
- 津波や洪水などによる通信設備への浸水防止のため立地条件に合わせて水防扉などを設置
- 通信機械室への防火シャッターや防火扉を設置
- 突然の停電時に電力を長時間確保できるよう通信ビルや通信基地局に予備電源を設置
  万一の際は移動電源車から配電・給電
- 他通信サービスが途絶えないよう中継伝送路の多ルート化を実施
- 災害時などにひとつの基地局で大きなエリアをカバーできる大ゾーン携帯基地局を設置
- 非常用電源の燃料タンクの設置

更なる設備の強靭化・復旧対応の迅速化

近年、災害エネルギーの増大により、大規模な災害影響が多発しています。通信設備やサービスへの影響の増大や復旧の長期化を踏まえ、設備の強靭化や復旧対応の迅速化等に対する更なる取り組みも推進しています。

設備の強靭化に関する主な取り組み

- 停電対策など、災害に対する備えを持たせた中ゾーン基地局の拡大
- EV を活用した基地局の停電対策
- NTT グループが保有する移動電源車（約 400 台）の一元管理、運用
- 災害影響などを考慮したケーブルの地中化やワイヤレス固定電話などの検討

復旧対応の迅速化に関する主な取り組み

- AI を活用した被害想定による復旧体制（全国広域支援体制など）の事前立上げ
- 当社 OB 社員の活用などを含めた、復旧体制の増強、人員確保

被災されたお客さま支援の強化

- 避難等を支えるための、リアルでわかり易い情報発信（通信被災状況、復旧状況、充電スポット、災害時公衆電話等の開設状況、訪日／在留外国人対応など）
- 被災地での出張 113 開設などを通じた、通信に関わるお困りごと相談の受付
- 自治体等と連携した、公衆電話 BOX への Wi-Fi・蓄電池設置による災害時の通信確保

平常時における安定した通信サービスの提供

常に安心して通信サービスをご利用いただくことができるよう、通信ネットワークの監視システムの運用、事故や故障の未然防止対策、ネットワークの保守・運用に携わる人材のスキル向上に取り組んでいます。

安定した通信サービスに関する主な取り組み

- 24 時間 365 日リアルタイムでネットワーク運行状況を監視・制御するオペレーション体制
- 正常稼働時における通信装置のパフォーマンス情報収集・分析を通じた故障の予兆把握と対処
- 予期せぬトラブルが発生した際の迅速かつ的確な回復措置を可能とする体制の構築及び手順の見直し
- 過去のトラブルから得た教訓の水平展開や重大事故につながる可能性のある事例分析による基本動作の徹底強化
- ネットワークの保守・運用に携わる人材を育成するための研修・訓練の実施やしくみの構築

新型コロナウイルス感染拡大による通信需要増加に対する安定した通信サービス提供

当社および通信事業を営む主要子会社は、指定公共機関としての責務の遂行および人命尊重の視点から感染防止に資することを目的とし、業務計画を定めています。感染症の流行拡大に伴い、インターネットの利用やテレワークの需要などが高まっている中、主に固定通信において、特に平日昼間帯のデータトラフィック量（通信量）が大幅に増加していますが、NTT グループ各社は、これまで夜間帯のピークトラフィックを踏まえたネットワーク設計をしており、現時点では昼間帯はネットワーク容量を確保できております。今後も、通信サービスの安定的な提供のため、状況に応じて設備を増強していきます。

携帯電話基地局・端末の運用（NTT ドコモ）

電波の人体への影響については、これまで 60 年以上にわたり世界各国で研究が行われ、日本をはじめ世界では、電波を安全に利用するための基準や制度が設けられています。

日本では 1990 年に郵政省（現在の総務省）が過去 40 年にわたる国内外の研究結果に基づいて、電波の人体に対する安全性基準を「電波防護指針」として定めています。同指針の基準値は世界保健機関（WHO）が推奨する国際的な指針と同等で、この基準値以下の強さの電波は健康に悪影響を及ぼすおそれはないと世界的にも認識されています。

NTT ドコモの携帯電話基地局ならびに端末は、同指針の基準値を下回るレベルで運用しています。電波防護指針のもとで制定された関係法令を遵守し、サービスを提供しており、安心して携帯電話をご利用いただけます。

NTT ドコモ「電波の安全性について」 https://www.nttdocomo.co.jp/corporate/csr/network/radio/safe.html