



安心・安全でレジリエントな社会の実現

Building a Safe and Resilient Society

88 ネットワークサービスの提供

91 NTTドコモの災害対策

96 電波の安全性

97 情報セキュリティ・プライバシー保護

103 AIへの対応





マテリアリティ

安心・安全でレジリエントな社会の実現

めざすゴール

いつでも、どこでもお使いいただける通信環境の提供を使命とし、お客さまの安心・安全で快適なコミュニケーションを提供します。

サステナビリティ課題

- ・サービス等安全性・安定提供
- ・情報セキュリティ・プライバシー保護

リスク

ネットワークの高度化・サービスの安定供給への対応遅れ、激甚化・頻発化する自然災害により、安心・安全なサービス提供の障害となる場合があります。またサイバー攻撃、情報流出、金融・決済サービスの不正取引などの情報セキュリティの脅威は、信頼低下につながる可能性があります。

戦略

NTTドコモグループは、24時間365日つながるためのネットワークの安定供給や高度化、電波の安全性への配慮、セキュリティ脅威への対応など、常にお客さまに信頼されるネットワークの提供に取り組んでいます。

機会

技術動向、顧客ニーズ、市場動向、自然災害リスクの増大、DX化の進展を背景に、ネットワークの強靱化や迅速な復旧対応、情報セキュリティの確保を強化することで、お客さまの生活基盤を支え、顧客満足度やブランドイメージの向上につなげていきます。

2025年度の取組み

- ・通信サービスの品質向上として、5G基地局を2026年3月末までに約5.9万局(4G周波数+Sub6+ミリ波)整備しました。またAIを活用した通信品質指標「CNX指数」を導入し、全国約8,000万人規模のデータを日々分析することで体感品質の向上をめざしています。
- ・2025年度の電波状況の問い合わせは11.2万件で、基地局の増設に加え、屋内エリアに「ドコモレピータ」「フェムトセル」を導入し、改善を図っています。
- ・「ネットワーク保守業務向けAIエージェントシステム」の商用利用を2026年2月に開始し、故障原因の特定や対処方法の提示を通じて、復旧時間の短縮と

トラブルの未然防止を実現。通信サービスの安定提供を支えるレジリエンスの強化につなげています。

- ・災害時の通信確保に向け、通信事業者間の連携を強化し、「つなぐ×かえる」プロジェクトによる支援情報の共有に加え、非常時の代替通信手段として「JAPANローミング™」を開始しました。
- ・セキュリティ人材の中級・上級認定者を2025年度に1,991名まで拡大し、セキュリティ人材の育成・強化を進めました。
- ・「ドコモグループAIリスクマネジメントガイドライン」を制定するとともに、ガイドラインに沿った運用を実施し、安全かつ適切なAI活用を推進しています。

主な2025年度実績

重大事故
発生件数

1件

生活基盤システム
事故発生件数

0件

サイバー攻撃に伴う
重大なインシデント
発生件数

0件

重大な
情報漏洩件数

0件

P.25 指標と目標



ネットワークサービスの提供

基本的な考え方

NTTドコモは、お客さまに常に信頼していただける、よりよいネットワークの提供に取り組んでいます。基地局の整備などを通じた「サービスエリアの拡大」により、都市部・地下鉄・過疎地・遠隔地など、「どこでも」つながる状態をめざしています。また、24時間365日体制で、平時のみならずイベント開催時も、「いつでも」つながる状況を確保するよう取り組んでいます。

さらに、仮想化技術を適用したネットワークの提供により、通信混雑時におけるつながりやすさや故障時の通信サービスの確保など、信頼性の向上に取り組んでいます。

NTTドコモが提供するネットワークの全体像

NTTドコモは通信ネットワークを、無線アクセスネットワーク、コアネットワーク、サービスプラットフォーム、各種基幹システムおよびオペレーションシステムにより構成しています。

サービスエリアの拡大

NTTドコモは「エリア構築基本方針」を定め、過疎地、遠隔地における計画的な基地局整備を進めています。日本国内におけるサービスエリアは、「LTE 4G方式」で人口カバー率が約100%に到達しています。

■ 基地局の整備

NTTドコモは通話・通信品質のさらなる向上とサービスエリアの拡大をめざし、基地局の整備を積極的に進めています。第5世代移動通信方式(5G)の基地局については、2020年3月25日に商用サービスの提供を開始しました。5G基地局は2026年3月末までに約5.9万局(4G周波数+Sub6+ミリ波)を整備し、いっそうの通信環境の充実に取り組んでいます。

通信サービス品質向上を最重要課題の一つとし、2024年度は高速・大容量通信が可能なSub6基地局数を前年度比1.2倍に増強しました。東京ビッグサイトやベルーナドーム、鈴鹿サーキットといった大規模施設に加え、全国の主要都市中心部や鉄道動線においても設備容量・基地局数を強化し、すべての通信改善目標を達成しました。

□ ドコモの通信改善 取組み宣言 2025年度

■ 基地局建設時の姿勢

基地局の新設の際、近隣の方々のなかには電波に対して不安を感じる方や、基地局の建設に関して違和感を覚える方もいらっしゃると思います。NTTドコモは、関連法令に規定がある場合はそれに則り、ない場合は社内規程で定めた範囲で地域住民のみなさまに向けて事前の説明会や公聴会を開催しています。そして住民のみなさまの意見や懸念をしっかりと受け止め、環境への配慮はもちろんのこと、地域社会に不利益をもたらさないようにした上で建設に着手しています。

真摯な説明を心がけ、地域住民のみなさまの生活に配慮した作業スケジュールを組むなど、可能な限り迷惑をかけないように努め、施工の際には住民のみなさまの安心・安全を最優先して工事を行っています。そして、地域の緊急通信体制

の向上なども実現しつつ、社会インフラとしての役割を果たしていきます。

■ 電波状況の調査・改善活動

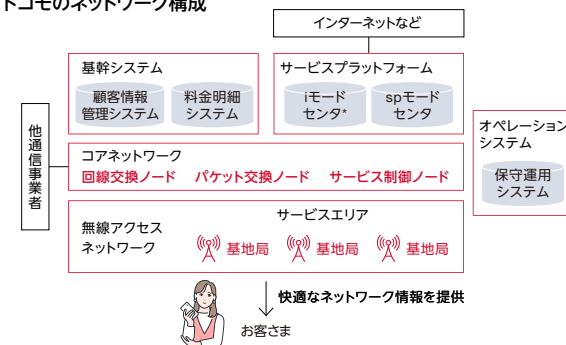
NTTドコモは通信品質の確保や通信エリアの拡大を図るために、広くお客さまから電波状況に関する声をいただいています。2025年度には、約11.2万件のお問い合わせをいただきました。

お客さまからのご意見に誠実に応えるため、お客さまからのご意見の他、トラヒックデータ、アプリデータ、AIによる体感品質推定などを組み合わせ、総合的に通信品質の把握、評価を行っています。

それらの取組みにより通信品質をさらに改善していくとともに、安定的な通信確保のために基地局の増設も行っています。

なお、ご希望のお客さまには電波状況に応じて改善策を提案しています。具体的には、電波を増幅する「ドコモレピータ」、電波を発信する「フェムトセル」を用いて屋内エリアの電波状況の改善を図っています。

ドコモのネットワーク構成



* 2026年3月31日をもってサービスは終了しました



■ 通信の体感品質の改善

ドコモはAIを活用し「お客さまの体感」を基準とした新たな通信品質指標である「CNX指数」を導入しています。基地局設備の正常性だけでは把握できない通信の使い心地を数値化し、見えない通信ストレスを可視化することで、迅速な品質改善につなげています。全国約8,000万人規模のデータを日々分析し、お客さま一人ひとりの体感に寄り添った品質向上を実現し、QoE（体感品質）の継続的な向上をめざしています。

■ 大規模イベント時の通信品質の確保

大規模イベントの開催などで特定の場所にお客さまが集中した際には、基地局の処理能力を超える膨大な通信が発生し、携帯電話がつながりにくくなる場合があります。NTTドコモは想定される通信の突発的な集中に備え、さまざまな対策を講じています。また、お客さまのご利用状況を踏まえたネットワークの設備容量拡大についても計画的に行っています。

対策例	内容
花火大会やコンサートなどのイベント	- 臨時基地局車やWi-Fiの設置による通信の分散処理 - イベント会場をカバーする基地局設備の増設や、設備を制御するソフトウェアの設定変更による通信容量の確保
EXPO2025 大阪・関西万博	- キャリア4社共同のシェアリング基地局により限られた設置スペースで通信容量を最大化 - スマートポールを活用した人が集中する場所のピンポイント対策や、ガラスアンテナを導入し、景観を損なわずに通信エリアを拡大 - 開幕後の混雑対策として臨時基地局車の追加設置による対策、エリアチューニングによるトラフィック分散を実施 - 会場までの動線や周辺エリアについても設備増強し通信容量を確保

■ 過疎地、遠隔地におけるエリア整備

NTTドコモは、過疎地や山間部、離島などにおいても、誰もが安心して利用できる通信環境の整備を進めています。時期によって通信が急増する観光地などの一時的な回線増大に対応しています。対策を講じることで、登山中のけがや遭難時の救助要請を可能にしており、命が救われた事例も多くなっています。

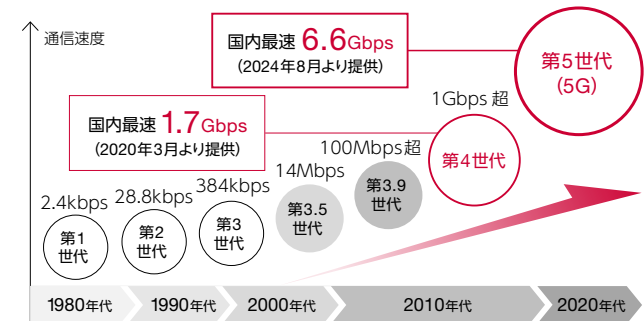
対策例	内容
富士山の山開き期間	山頂などに臨時的基地局を設置し、安定的で快適な通信サービスを提供
地形や植生の影響で電波が届きにくい登山道	登山道対策専用アンテナや山小屋の屋根への小型基地局などの設置
新幹線のトンネル内での携帯電話利用	国内新幹線全トンネルエリアでの携帯電話サービスを提供

■ 海外でのご利用

NTTドコモは、海外でも安心・快適に通信サービスをご利用いただけるよう国際ローミングサービス「WORLD WING」を提供しています。5Gネットワークによる高速データ通信や、VoLTEによる高音質通話の利用可能国・地域の拡大も進めており、NTTドコモでご契約の携帯電話は2026年6月末現在で、200以上の国・地域で使用可能です。

高速・大容量の実現

NTTドコモは移動通信システムの世代を1980年代のアナログ方式の第1世代（1G）から約10年に1度のペースで進化させてきました。その間、通信速度の飛躍的な高速化とネットワークの大容量化を図り、より快適な通信を実現するための取組みに注力してきました。



※ 一部エリアに限ります。通信速度は送受信時の技術規格上の最大値であり、実際の通信速度を示すものではありません。ベストエフォート方式による提供となり、実際の通信速度は通信環境やネットワークの混雑状況に応じて変化します

■ 実効速度計測結果

	受信	送信
Android™	56Mbps～351Mbps	10Mbps～32Mbps
iOS	75Mbps～373Mbps	10Mbps～31Mbps

※ 「実効速度計測結果」は、総務省が定めた「実効速度に関するガイドライン（略称）」にもとづき2026年1月～3月に全国10都市で計測し、その結果、中央値に近い半数がこの範囲内の速度であったことを示すものです。全国10都市での計測結果のため、お客さまの利用場所・時間・通信環境により、実効速度は異なります

■ PREMIUM 4G

NTTドコモはLTEAdvancedを使用した通信サービス「PREMIUM 4G」を提供しています。最大受信速度は「キャリアアグリゲーション」や「256QAM4×4MIMO」などの高速化技術を導入し、2020年3月、1.7Gbpsに達しています。

また、お客さまのトラフィック量を分析し、通信が集中する全国主要都市を中心にエリア展開を進めています。お客さま一人ひとりのニーズにあわせて、今後も動画や音楽、SNSなどのさまざまなコンテンツを快適にご利用いただけるネッ



ネットワークサービスの提供

NTTドコモの災害対策

電波の安全性

情報セキュリティ・プライバシー保護

AIへの対応

トワークの提供をめざしていきます。

■ 5Gの導入による高速・大容量通信の実現

NTTドコモは2020年3月に5Gの商用サービスを開始しました。本サービスでは、5G専用の広帯域な3つの新しい周波数帯域 (3.7GHz・4.5GHz・28GHz) を用いることで、高速・大容量な通信を提供しています。さらに「低遅延」「多数端末接続」といった5Gの特徴を最大限活用するとともに、20年以上にわたって蓄積したネットワーク運用ノウハウと最先端技術の開発力を発揮して、今後もさらなる高速化を実現し、通信における世界のイノベーションをけん引していきます。

■ SA (Standalone) 方式による 5G通信サービスの提供

NTTドコモは2021年12月より、5G専用のコアネットワーク装置である5GC (5G-Core) を導入したSA (Standalone) 方式による5G通信サービス「5G SA」を法人のお客さま向けに提供しています。「5G SA」は通常の5Gよりもさらに高速・大容量な通信を利用できるサービスで、さまざまな業種・業態のソリューション創出による産業の発展をめざしています。

2022年8月にはNTTドコモの5G対応料金プランを契約中のお客さま向けオプションサービスとして「5G SA」を提供開始しました。提供箇所は2022年度までに主要駅や商業施設を中心に拡大し、2023年度はスタジアムや大学、空港など人が多く集まる施設にも拡大しました。「5G SA」はスマートフォンのご利用に対応し、通信速度*1は受信時最大6.6Gbps、送信時最大1.1Gbpsを実現しています。「5G SA」により可能となるネットワークスライシング*2の導入に先駆け、2024年4月に無線区間の優先制御機能を導入し、一般ユーザーと比べ優先的にパケットを割り当てることで混

雑エリアや時間帯においても安定した通信を実現するサービスを開始しました。今後、ネットワークスライシングの導入によって用途やサービスに合わせた、5Gならではの柔軟なネットワークの提供をめざしています。

*1 通信速度は技術規格上の最大値であり、実際の通信速度を示すものではありません。ベストエフォート方式による提供となり、実際の通信速度は、通信環境やネットワークの混雑状況に応じて変化します。

*2 ネットワークスライシング：5Gネットワークを運用する上でユースケースやビジネスモデルなどのサービス単位でコアネットワークを分割して最適化する技術

通信速度のさらなる高速化

5Gの商用サービス化を受け、NTTドコモは今後のさらなる高速化に向けた取組みとして5Gの高度化 (5G Evolution) ならびに2030年代の6G導入に向けた技術企画の検討および研究開発を行っています。5G Evolution & 6Gの実現に向け、5Gが可能にする高速大容量、高信頼・低遅延、多数接続のさらなる進化 (超高速・大容量、超高信頼・低遅延、超多接続) をめざしているほか、陸上、空、海への超カバレッジ拡張、カーボンニュートラル実現に寄与する超低消費電力の開発など、新たな領域への挑戦も行っています。

安定したネットワークの提供

NTTドコモは、お客さまに「いつでもどこでも」ご利用いただけるネットワークを提供するために、トラブル発生時のお客さまサービスへの影響を極力発生させない仕組みづくりに取組んでいます。

■ 24時間365日体制でのネットワーク設備の監視と措置

NTTドコモは東京・大阪の2拠点にネットワークオペレーションセンターを設置し、基地局などのネットワーク設備の

装置やお客さまへのサービス提供状況といった全国の通信状況を24時間365日体制で監視し、ネットワーク設備が故障し、サービス停止状態に陥らないように、未然に対処する仕組みづくりに取組んでいます。

たとえば、ネットワーク設備の正常稼働時の情報を日々収集・分析し、異常の疑いを察知した際は故障前兆か否かを解析して事前に対処しています。また複雑化するネットワーク故障に対応するため、世界最大級規模のデータを用いた「ネットワーク保守業務向けAIエージェントシステム」を開発し、2026年2月に商用利用を開始しました。100万台以上の装置データを統合し、熟練エンジニアの経験知をAIに反映することで、故障原因の特定や対処方法の提示を可能としています。これにより、復旧時間の短縮やトラブルの未然防止を実現し、通信サービスの安定提供を支えるレジリエンスの強化につなげています。

オペレーターに異常が知らされた際には、遠隔操作でネットワーク設備やトラフィックの経路などをコントロールし、お客様サービスへの支障を防ぐため速やかに対処しています。また、トラブルの原因を究明し、設備の物理的な修理が必要な場合は、設備保守のプロフェッショナルが現地にて、迅速にネットワーク設備を交換・修理しています。

なお、電気通信事業法に則り、電気通信サービスの事故件数を、サステナビリティに関する指標として管理しています。

電気通信サービスの重大事故発生件数

(件)

2021年度	2022年度	2023年度	2024年度	2025年度
1	3	4	1	1

対象範囲：ドコモ・ドコモビジネス



NTTドコモの災害対策

「災害対策3原則」に基づき、災害時における通信の確保に注力

災害発生時に、人命救助や復旧活動、安否確認に不可欠な役割を果たすのが携帯電話です。NTTドコモは非常時に備え、会社設立当初より「システムとしての信頼性向上」「重要通信の確保」「通信サービスの早期復旧」を柱とする「災害対策3原則」を定め、災害時における通信の確保に継続的に取り組んでいます。

東日本大震災の教訓から「新たな災害対策」を策定し、2012年2月末までに対策を完了しています。また、2018年には多発する自然災害への対策強化のために、2年間にわたる200億円規模の追加対策を発表、対応しました。今後も予見される多様な自然災害に対応するために、さらなる災害対策に取り組んでいきます。

ドコモの災害対策3原則

災害対策の3原則

システムとしての 信頼性向上

- ・設備構造の強化
 - ・耐震対策(震度7にも耐える設計 など)
 - ・風水害防護対策(防水扉、防潮板の設置 など)
 - ・火災防護対策(防火シャッター、扉の設置 など)



基地局 中継局

重要通信の確保

- ・110、119、118の緊急通報
- ・災害時に重要通信を扱う機関に対する災害時優先電話制度
- ・音声通話とパケット通信を分けたコントロール

通信サービスの 早期復旧

- ・災害対策機器によるエリア復旧
 - ・移動基地局車
 - ・衛星エントランス基地局
 - ・移動電源車・発電発電機 など



災害対策の取組み

発災時の事象など

サービス中断による
重要通信の確保への支障

長時間停電による
バッテリーの枯渇

地震・豪雨による伝送路断
(光ファイバなど)

災害対策の取組み

大ゾーン基地局(激甚災害に備えた非常用基地局)

全国105か所(都道府県庁 など)

- ・無停電化(エンジン) ・伝送路冗長化

平成30年北海道胆振東部地震にて初運用



中ゾーン基地局(自然災害に備えた基地局)

全国2,000か所(災害拠点病院、役場 など)

- ・停電時24時間以上運用 ・伝送路冗長化

令和2年7月豪雨にて62局を運用



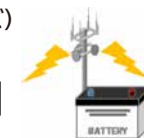
予備電源の強化

全国14,000か所(主要公共機関、避難所 など)

- ・停電時6時間以上運用可能

令和2年台風第10号にて1,000か所をバッテリー運用

※ 6時間以上運用可能局以外も含む

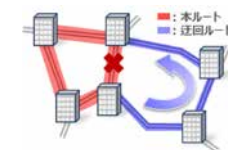


伝送路の多ルート化

全国1,200ビル

- ・伝送路の多ルート確保
- ・伝送路の自動迂回

令和2年7月豪雨にて自動迂回運用



▶ 東日本大震災以降の災害対策投資額 累計 **1,000** 億円以上



災害時のマネジメント体制

NTTドコモグループは「NTTグループ防災業務計画」に基づき、災害発生時に初期動作がスムーズに行えるように、災害の規模、復旧活動の規模などに応じた態勢がとれるようにしています。この態勢は部門横断的な編成にしており、混乱時にも円滑な災害対応ができるようにしています。

災害時の社内態勢

規模	社内態勢	発令者	過去の災害 及び 目安
大 小 災害発生前	第一非常態勢	社長	・ 東日本大震災
	第二非常態勢	副社長	・ 令和6年 能登半島地震 ・ 平成30年 台風21号 北海道胆振東部地震(複合災害)
	第三非常態勢	NW本部長	・ 令和2年 台風10号 ・ 令和元年 台風15号 ・ 南海トラフ地震臨時情報「巨大地震注意」 ・ 北海道・三陸沖後発地震注意情報
	情報連絡態勢	災害対策室長	・ 台風の接近や、影響の少ない地震 等 ・ 災害等の発生が予測される場合 等

状況に応じた災害対策基地局の活用

NTTドコモは、災害時のネットワーク確保のために災害対策用基地局を設置しています。被害状況に応じて、臨時基地局の設営や、既存の基地局の電波の発射角度を遠隔で変更するなどの対応を行っています。

ドコモの災害対策基地局

	移動基地局車可搬型基地局	中ゾーン基地局	大ゾーン基地局
ポイント	多様な自然災害に対応 スポット的な エリア救済を目的とした、 移動式の基地局(車両、可搬)	多様な自然災害に対応 既存基地局の基盤を強化し、 災害時に周辺をカバーする ことが可能な基地局	激甚災害専用 周辺局のほとんどが 中断となる場合に限り、 広域をカバーする
利用イメージ	通常時 	通常時 [運用] 	通常時 [停止]
	災害時 	災害時 [運用(エリア拡大)] 	災害時 [運用]
広さ(エリアの 半径)	小 (~1km程度)	小 (1km程度)	中 (3~5km程度) 大 (7km程度)
災害時 運用	移動・設置の時間が必要	遠隔で即時運用が可能	遠隔で即時運用が可能



■大ゾーン基地局

大ゾーン基地局は、広域災害・停電時に、人口密集地の通信を確保するため、通常の基地局とは別に、より広範なエリアをカバー（半径約7km、360度）する災害時専用の基地局です。NTTドコモは2011年度以降、全国に105か所の大ゾーン基地局を設置しています。2018年9月に発生した北海道胆振東部地震の際にはじめて大ゾーン基地局による運用を図り、釧路市内で広範囲の通信回復に貢献しました。



災害時に人口密集エリアの通信を確保する大ゾーン基地局

■中ゾーン基地局

中ゾーン基地局は、通常の基地局の基盤を強化した基地局で、平時は通常の基地局として運用し、災害時に周辺基地局がサービス中断に陥った際には、遠隔操作で通信エリアを拡大し、周辺エリアをカバーできる基地局です。ハザードマップを参考に被害が想定されるエリアをカバーすることを想定し、全国で2,000局以上の中ゾーン基地局を整備しました。また、中都市郊外や災害拠点病院、沿岸部、山間部などの通信確保を目的とした「中ゾーン基地局の全国展開」を実施しています。令和2年7月豪雨では、62局を運用しました。

■駆けつけ困難地域の対応

災害時の応急復旧手段の多様化に対応するため、NTTドコモは保守拠点から駆けつけまでに時間がかかる駆けつけ困難地域などのエリアの災害時救済に向け、船上基地局や有線ドローン中継基地局の整備、関係機関との連携強化を図っています。

2024年の元日に発生した能登半島地震では、NTTドコモとしてはじめて船上基地局を運用しました。KDDI株式会社と共同で運用し、被害の大きかった輪島市の2つのエリアを救済しました。また、関係機関との連携については、陸路が閉ざされた地域の復旧に向けて、自衛隊にご協力いただき、海路でのアプローチを実施しました。

ドローン中継局の運用により、上空の電波を増幅することで通信エリアの確保が可能になり、応急復旧活動の体制強化につながりました。



ドローン中継局

被災地における通信の確保

■Starlinkの導入

NTTドコモは2024年1月1日の能登半島地震を契機に、基地局のバックホールとしてStarlinkを導入しました。地震などで基地局向けの光回線が切断しても、Starlink衛星を活用して上空から基地局への臨時回線を確保できるため、災害時に有効です。Starlinkは高度約550kmの低軌道に位置しており、従来の静止軌道衛星に比べ地球からの距離が短いため、低遅延で高速な通信が可能です。2024年5月の総合防災訓練で実用化し、その後は2024年8～9月の台風10号や奥能登豪雨、2025年2～3月の大船渡の山火事など、複数の災害で活用しています。

□ Starlinkで変わる災害対策 迅速な復旧で被災地をつなげる

■docomo Starlink Direct

「docomo Starlink Direct」は、「いつでも、どこでもつながる」ネットワークの実現に向けて、SpaceX社が提供する衛星通信サービス「Starlink Mobile」を活用した、衛星とスマートフォンの直接通信サービスです。

本サービスは、山間部や離島、海上などこれまで通信提供が困難だったエリアや、災害により地上通信設備が被災したエリアにおいて、テキストメッセージの送受信や対応アプリでのデータ通信、緊急地震速報の受信を可能にすることで、非常時における通信手段の確保に貢献します。

■JAPANローミング™

「JAPANローミング™」は、非常時における通信手段の確保のため、国内の携帯電話事業者*が共同で取組むサービスです。

ご契約中の携帯電話事業者のネットワークが災害などで利用できなくなった場合に、ほかの携帯電話事業者のネットワークに切り替えることで、通信が可能になります。

* KDDI株式会社／沖縄セルラー電話株式会社、ソフトバンク株式会社、楽天モバイル株式会社、株式会社NTTドコモをさします。

■JAPANローミングの仕組み



ネットワークサービスの提供

NTTドコモの災害対策

電波の安全性

情報セキュリティ・プライバシー保護

AIへの対応

■ つなぐ×かえるプロジェクト

「つなぐ×かえるプロジェクト」は、国内の通信事業者各社が協力して、社会貢献をめざすプロジェクトで、2020年9月にNTTとKDDIが主体となってスタートしました、2024年12月にはソフトバンクおよび楽天モバイルも参画して枠組みを強化しています。その中でも災害対策においては大規模災害時の通信インフラをいち早く復旧し、被災地支援を迅速に実施していきます。

□ つなぐ×かえるプロジェクト

一 通信事業者間の協力体制

大規模災害発生時、各通信事業者は避難所への通信サービスの提供などを通して被災地を支援していますが、これまでは各社が個別に支援活動を行うことで、支援の重複や地域的な偏りが発生することがありました。それらを解消し、被災地の通信ネットワークの早期復旧を行うため、「つなぐ×かえるプロジェクト」の一環として、2025年7月より通信業者8社*で「通信業者間の被災地支援に関する情報連携」を開始しました。この情報連携により、各社が協力し、被災地のみなさまに通信サービスの提供をはじめとした支援を速やかに実施していきます。

今後は情報連携に加えて、避難所支援に関する分担を図るなど、通信事業者間の協力体制をさらに強化することで、被災地における避難所への支援を広域かつ速やかに行い、持続可能な社会の実現にさらに寄与することをめざします。

* NTTグループ（NTT株式会社、NTT東日本株式会社、NTT西日本株式会社、株式会社NTTドコモ、NTTドコモビジネス株式会社）、KDDI株式会社、ソフトバンク株式会社、楽天モバイル株式会社の8社

支援・取組み内容

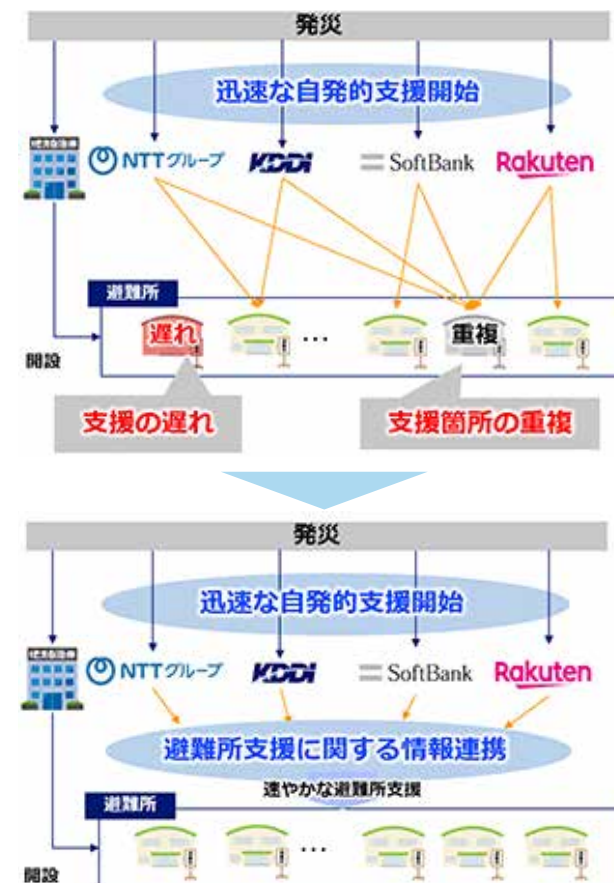
支援内容

- 通信サービス（無料Wi-Fiサービスなど）
- 充電サービス
- 問い合わせ先の掲示など

取組み内容

- 支援する避難所の情報共有（通信サービスおよび充電サービスの提供状況など）
- 各通信事業者のサービスに関する問い合わせ先の掲示
- 各自治体、各通信事業者が実施する防災訓練、防災イベントでの各社の情報連携による取組みの展示

各社の連携による速やかな避難所支援のイメージ





災害時の対応状況

2024年元日に発災した能登半島地震では、停電や伝送路断の影響により、最大260局の基地局でサービスが中断し、被災した6市町村（七尾市、珠洲市、輪島市、志賀町、穴水町、能登町）の通常エリアと比較して、サービスエリアが30%まで落ち込みました。NTTドコモは、発災直後より社内体制を確立し、翌日より復旧活動を進め、延べ1万人が対応に従事しました。

半島という限られた交通路による渋滞や長距離移動に加え、余震や積雪により現地アクセスに障壁が発生するなかで、全国から駆けつけた社員による復旧作業により、計200サイト以上を応急復旧させました。加えて、船上基地局の運用や関係機関との連携にも取組んだ結果、1月17日には立入困難地域を除く応急復旧、3月21日にはエリア復旧が完了しました（輪島市の舩倉島を除く）。

また、指定／指定外合わせたほぼすべての避難所（約300か所）へ直接訪問し、避難者のみなさまへ無料充電サービスや無料Wi-Fiサービス（d Wi-Fi／Starlink Wi-Fi）、ドコモ公衆ケータイの無料貸し出しを行いました。さらには長期化する避難所生活への支援として、オンライン診療および動画サービスの提供による心と体のケアを実施しました。なお、ドコモ公衆ケータイ、オンライン再診、動画サービスの支援はNTTドコモとしては初めての試みです。

災害救助法適用地域を対象とした主な支援

主な支援	具体的な支援内容
お客さま	・災害時データ無制限モードの実施 ・付属品の無償提供 ・携帯電話機購入時における特別割引の実施 ・一部手数料の無料化 ・故障修理代金の一部減額 ・ケータイ補償サービスの対応 ・ケータイデータ復旧サービスの無料化 ・代替機賠償金の無料化 ・受付手続きの緩和 ・「ドコモ光」の基本料金などを無料化 ・「ドコモ光」などに関する一部機器の無償提供 ・「ひかりTV for docomo」基本料金などの返還 ・料金支払い期限の延長 ・失効したdポイントの返還
自治体など	・携帯電話、衛星携帯電話の貸出 ・避難所におけるマルチチャージャの設置、Wi-Fiの設置

行政や自治体との連携

NTTドコモグループは、災害対策基本法に基づく指定公共機関として、防災措置の円滑かつ適切な遂行を視野に「NTTグループ防災業務計画」に則り、平時の防災対策および災害発生時の対処活動に努めています。災害時には行政機関などと連携し、自治体への携帯電話の貸し出しをはじめとした「重要通信の確保」に関する対応を図っています。

☐ 防災業務計画

災害時に役立つサービス

大規模災害発生時に電話が集中し、携帯電話がつながりにくくなった被災地の方の安否確認ができる「災害用伝言板」を提供しています。いざというときにスムーズにご利用いただけるよう、毎月1日と15日に体験サービスを実施しています。また、遠隔地のエリアメール配信情報をSMSで受信できる「どこでも災害・避難情報」の提供も行っています。

災害用伝言板の特徴

被災者の方が自分の安否状況を登録することで、簡潔にその情報が伝えられ、インターネットを通じて全世界から確認が可能。入力方法は2種類あります。

① 以下の4つの定型メッセージから選択

無事です。 被害があります。 自宅にいます。 避難所にいます。

② コメント入力（全角100文字、半角200文字以内）

「どこでも災害・避難情報」の特徴

- ・あらかじめ登録した地域にエリアメールが配信された際にSMSでお知らせが届きます。
- ・過去3日間に配信された全国の災害・避難情報などがWebページで確認できます。

☐ どこでも災害・避難情報



電波の安全性

基本的な考え方

NTTドコモは携帯電話基地局ならびに端末を、電波法令を順守して運用・提供しており、発射される電波の強さは電波防護指針の基準値以下です。電波防護指針の基準値以下の強さの電波は、健康に悪影響をおよぼすおそれはないと世界的に認識されています。従ってNTTドコモの携帯電話は安心してご利用になれます。

電波の安全性への配慮

■ 電波防護指針

電波が人体に与える影響については60年以上にわたって国内外で調査研究が行われています。電波の人体に対する安全基準として、世界保健機関 (WHO) と協力関係にある国際非電離放射線防護委員会 (ICNIRP) による指針および米国電気電子学会の国際電磁界安全委員会 (IEEE/ICES) による指針が定められており、いずれも国際的な指針として多くの国で採用されています。日本では、これらの国際的な指針に整合した「電波防護指針」が定められており、最新の知見を反映するために適宜見直されています。2018年および2024年には5Gの安全な電波利用を確保するための改定が実施され、法規制にも反映されています。NTTドコモは法規制の順守を徹底しており、携帯電話基地局および端末が発する電波の強さは基準値以下です。さらに、NTTドコモの各携帯電話端末について、安心してご利用いただけるよう、人体に吸収される電波のエネルギー量を示すSAR (比吸収

率) やPD (電力密度) をNTTドコモのホームページ上で開示しています。

□ 携帯電話の電波防護への適合性について

■ 業界各社との電波の安全性を確認する研究を推進

NTTドコモは、2002年からKDDI株式会社、ソフトバンク株式会社と共同で人体の細胞・遺伝子への電波の影響を調べる実験を実施し、2007年に「影響は確認されなかった」と最終報告をしています。これは、電波が細胞の構造や機能に影響を与えてがん化するという主張を否定する科学的証拠の一つであり、携帯電話の電波の安全性を改めて示したものです。総務省も電波の安全性に関する研究を継続的に実施しています。

また現在、一般社団法人電波産業会 (ARIB) 電磁環境委員会では、電波利用における公共の福祉の増進活動の一環として、携帯電話の電波の安全性に関する調査・研究活動などが行われています。NTTドコモもこの活動に賛同し、正会員として積極的に関与しています。

□ 電波の安全性について

■ 5Gに関する電波の安全性の説明

NTTドコモは、2020年3月から日本でも商用サービスが開始された5Gに関して、電波の安全性についてステークホルダーのみなさまへ説明することの重要性を認識しています。ホームページにて、電波の安全性に対する国内外の関係機関の評価や見解、5G帯域を含む電波の人体に対する安全基準を定めた国際的な指針に関する情報を紹介しています。さらに、電波の安全性に対するNTTドコモの考えや、よくあげられる質問について回答を公開するなど、5Gの利用にあたり、利用者のみなさまがより安心して利用できるよう情

報公開を行っています。

□ 電波による人体への影響と、安全利用のための基準・制度

□ 電波の安全性に関するドコモや主要機関の見解

■ 医用電気機器への影響と対策

総務省および電波環境協議会は、携帯電話やほかの無線機器からの電波が心臓ペースメーカーなどを含む、医用電気機器の動作に影響をおよぼす場合があることを確認しており、安全に利用できるようガイドラインを作成して、一般に周知しています。当社においても、同ガイドラインに対応した注意を携帯電話端末の取扱説明書やNTTドコモのホームページで案内するなど、利用者が携帯電話を使用する際の注意点を十分認識できるよう取り組んでいます。



情報セキュリティ・プライバシー保護

情報セキュリティの確保

■ 基本的な考え方

NTTドコモでは、情報セキュリティの強化／情報管理の徹底を重要な経営課題として取組んでおり、お客さまに安心してNTTドコモのサービスをご利用いただくために、情報セキュリティに関する取組み方針として「情報セキュリティポリシー」と「プライバシーポリシー」を宣言し、順守を徹底しています。これらの方針に則り、情報管理体制を構築し、重大なインシデント発生件数ゼロをめざしています。

なお、情報セキュリティポリシーで対象としている情報管理資産は、企業活動において入手および知り得た情報、ならびにNTTドコモが業務上保有するすべての情報としています。

■ 情報セキュリティ・プライバシー保護の指標(ドコモグループ)

(件)

指標	目標	2023年度	2024年度	2025年度
サイバー攻撃に伴う重大なインシデント発生件数*	0	0	0	0
重大な情報漏えい件数	0	0	0	0

*2023年からKPI指標に追加

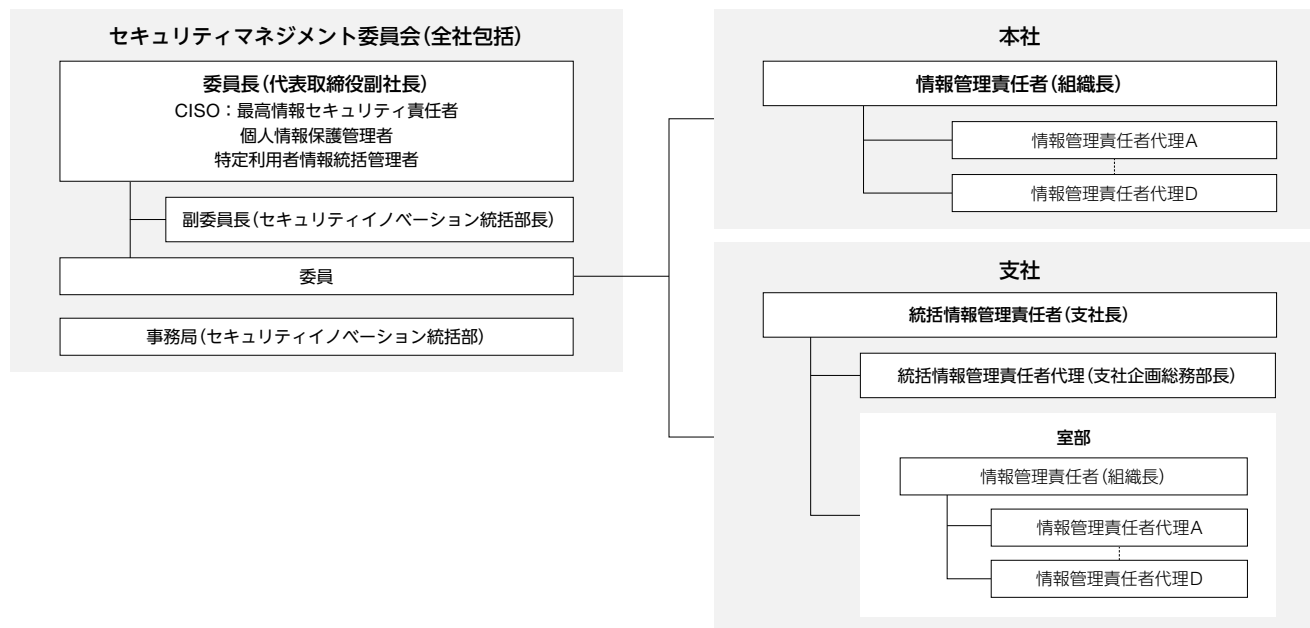
□ [情報セキュリティポリシー](#)

□ [NTTドコモ プライバシーポリシー](#)

■ NTTドコモ情報管理体制

NTTドコモは、保有するすべての情報資産の保護および適切な管理を行うことを目的に、「最高情報セキュリティ責任者(CISO)」と「個人情報保護管理者」「特定利用者情報統括管理者」を兼任する代表取締役副社長を委員長としたセキュリティマネジメント委員会を設置し、各組織に情報管理責任者を配置することで、情報セキュリティ対策を速やかに実施できる体制を構築しています。セキュリティマネジメント委員会は年2回開催し、主に次の3つに対応する役割を担っています。

■ 情報管理体制図(ドコモ)



(2026年7月現在)



■ 情報セキュリティルールの徹底

「電気通信事業法」や「個人情報保護法」をはじめとする関連法令、各省庁などが定めるガイドラインなどに則り、NTTドコモにおける情報管理規程・細則・マニュアル類を定めており、社員、委託先、パートナーは、個人情報の取扱いも含め、厳格に運用しています。

なお、通信の秘密および職務上知り得た秘密・個人情報を正当な理由なく使用し、漏えいしたまたは漏えいしようとした場合は、社内規程により懲戒処分の対象としています。

■ グループ会社における情報セキュリティガバナンス

グループ会社における情報管理の徹底／インシデントの未然防止を図るため、NTTドコモ情報管理規程に基づく「ドコモグループセキュリティ対策マニュアル」を制定し、グループ各社は適正なセキュリティ管理に必要な体制を構築し、ルール順守を実現しています。

さらに、NTTドコモの情報セキュリティ部にはグループ会社を統括する部署を設置し、グループ各社における情報セキュリティ業務運営のモニタリング・セキュリティ教育および訓練の実施・サイバーセキュリティに関する脅威やその対策についての情報共有・インシデント発生時の対応連携などを行っています。

また、グループ会社の中でもNTTドコモビジネス、NTTドコモソリューションズ、NTTドコモ・グローバルとは各社CISOによるNTTドコモグループCISO会議を設置し、情報セキュリティ戦略・重要な施策の方針決定を行っています。それらの決定に基づき、情報セキュリティ対策・セキュリティ人材強化を一体的に運営しています。

情報セキュリティ対策

■ 情報セキュリティリスク管理

NTTドコモグループおよびNTTグループで発生したインシデントや、最新のサイバー攻撃動向や世界情勢・法制度整備状況・技術動向などを踏まえて情報セキュリティリスクを抽出し、評価分析および対策対応を行っています。

■ システムセキュリティ対策

NTTドコモグループのシステムは、米国国立標準技術研究所 (NIST) が発行するSP800-37のリスクマネジメントフレームワークなどをベースとして、約200項目のセキュリティ対策を実施することを求められており、開発時のセキュリティ審査・脆弱性診断などを実施しています。

NTTドコモにおいては個人情報などの重要な情報を扱うシステムについて、顧客情報検索時のルール厳格化、システム利用に対する多要素認証の導入、情報システム端末・通信路の暗号化、不正持ち出し監視といった対策を必須化しています。

■ ソフトウェア脆弱性の撲滅

外部からの攻撃の足掛かりとなる大きな要因としてソフトウェアの脆弱性があげられます。その対策としてシステムは稼働前の脆弱性診断をパスすることを必須化しており、稼働後も定期的に脆弱性診断を実施しています。

新たに危険度が高いソフトウェアの脆弱性が発見された場合は、速やかに必要な対策を実施し、情報資産にかかる不正アクセス・破壊・情報漏えい・改ざんなどの発生を予防、被害最小化を図っています。

ーパブリック・クラウド利用におけるセキュリティ対策

自由度が高いIaaS/PaaSの設定不備や管理者IDの漏えいなどによる攻撃の対策として、管理者アカウント払出の一元化と、クラウド環境ごとに定められたセキュリティポリシーを常時監視して維持することを必須化しています。

セキュリティポリシーに違反した場合はアラート発生後、速やかな対処を義務化しています。

ー高度化するDDoS攻撃への対応

DDoS攻撃はインターネットを利用する以上不可避で、攻撃手法の高度化が著しい脅威です。NTTドコモではこれまでに受けたDDoS攻撃から、同様な攻撃に対する対策を講じて被害抑止に努めています。

攻撃を検知した際には、グループ各社間で攻撃手法などの情報を共有し、各システムの監視を強化し攻撃に対応します。攻撃の規模によっては、事後の詳細な分析結果も含めてNTTグループ内での情報共有、また業界他社やセキュリティベンダとの情報連携を行います。

■ サービス不正利用の抑止

被害が拡大しているフィッシング詐欺をはじめ、個人向けサービスを狙った攻撃は年々高度化・増加しており、NTTドコモではCISO配下に「不正アクセス対策委員会」を設置し、不正アクセス被害に遭う前の予見・予防、被害発生状況のモニタリング、また被害にあった後の迅速なインシデントレスポンスを総合的に強化しています。

また、新たにサービスを提供する際には、各サービスの特性を踏まえてアカウント乗っ取りによる不正利用・情報漏えいなどのセキュリティリスクを抽出し、対策が講じられているか審査しています。



■ セキュリティ監視

セキュリティ監視の専門組織であるSOC (Security Operation Center) を設置し、サイバー攻撃やサービスの不正利用の兆候を24時間監視しています。SIEM (Security Information and Event Management) と呼ばれるセキュリティ情報管理の仕組みにより、サーバーやネットワーク機器などのログを集約し、相関分析による攻撃の早期検知やAIを活用した高度ログ分析による異常検知を実現しています。

また、攻撃に関するさまざまな情報を日々収集し、検知手法の改善や予防も含め対応を実施しています。

■ パートナー企業などに対する情報セキュリティの取組み

NTTドコモはスマートライフ事業の拡大の柱の一つとして社会課題解決に向けた他産業との協働を進めています。パートナー企業との情報の連携・共有が増加することから、パートナー企業に対しても、個人情報保護法令および各省庁や公的機関の定めるガイドラインの順守を要求するなど、適切な管理を実施しています。なお、個人情報を共有する場合は、お客さまの同意を得た上で提供しています。

— 個人情報を取扱う委託先企業の選定基準

事業を運営していくなかで個人情報を扱う業務を外部にお願いすることがあります。当社はこれらの委託先企業においても当社と同水準の情報管理措置を実現すべきと考え、NTTドコモが定める会社選定基準を満たした企業とのみ契約を締結しています。本基準は、独立行政法人情報処理推進機構 (IPA) や個人情報の保護に関する法律についてのガイドライン (通則編) なども参考に策定しています。

契約時には安全管理措置・秘密保持・再委託の条件・その他の個人情報の取扱いに関する事項について適正に定め、ま

た契約期間中は現地訪問などによる実際のセキュリティ対策実施状況のチェックやルール順守状況のモニタリングを行い、万一、監督ならびに体制・業務運用が不適切だった場合には是正措置を徹底しています。

— ドコモショップにおけるセキュリティ意識向上と情報管理の徹底

販売代理店であるドコモショップに対しても、情報セキュリティに特化した研修をスタッフ全員に年1回以上実施するとともに、店頭で起こりやすいセキュリティ事例をまとめた「セキュリティNews」を四半期毎に発行し、啓発活動を行っています。

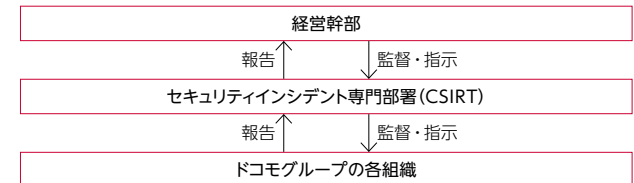
また、販売現場ではお客さまの情報をお預かりすることも多く、情報漏えいのリスクが高いことから、毎月の自主点検に加えて各支社の情報管理担当が徹底した業務監査を3か月に1回実施し、情報管理が適切に行われているかを確認しています。

■ セキュリティインシデントの対応

NTTドコモグループではインシデント発生時に対応する専門部署としてCSIRT (Computer Security Incident Response Team) を設置しており、重大なインシデント発生時には対応マニュアルに従い、CSIRTを中心として社内外の関係組織や経営幹部と密に連携をとり、対応にあたります。

平時には、自社設備への攻撃の監視や国内外の攻撃動向の収集を行い、インシデント発生に備えています。

■ セキュリティインシデント対応体制図



— 外部連携

NTTドコモは、一般社団法人日本シーサート協議会、Forum of Incident Response and Security Teams、一般社団法人ICT-ISAC JAPAN、一般社団法人JPCERT コーディネーションセンター、一般財団法人日本サイバー犯罪対策センターなどのセキュリティ団体に加盟し、外部組織との連携を通じて国内外のセキュリティ動向を情報収集しています。収集した情報はセキュリティ対策や社員向け訓練、実際のセキュリティインシデントの対応に反映しています。

また、NTTドコモグループで起こったインシデントとその対策などの取組みを団体などに情報発信・共有し、他企業など社会への貢献も行っています。

— 脅威情報分析

NTTドコモは、外部セキュリティベンダと連携し、高度化するサイバー攻撃の種別・動向・手法などの脅威情報を収集しています。その中でも通信事業など重要インフラ事業を対象としている攻撃トレンドを主として分析を行い、次なる攻撃対象となりえるNTTドコモのサイバー攻撃の予見に役立てています。

— インシデント対応訓練

NTTドコモでは、提供しているサービスでのインシデン



ト発生を想定した社内訓練を毎年実施し、経営幹部、サービス部門、お客さま対応部門、広報部門を含めた対応体制構築および対応手順の確認を行っています。

脅威動向を踏まえ、2025年度はランサムウェア攻撃を想定した社内訓練を行いました。経営幹部も参加しながら、事業部門・コーポレート部門を含めた感染発生時のサービス復旧までの手順、法令・コンプライアンス上の観点を踏まえた対応方針を確認し、被害発生時に速やかな対処が行えることを検証しました。

また、監督官庁や公的機関主催の演習、NTTグループ内演習にも積極的に参加し、インシデント発生時の実践力を高めています。

さらに、NTTドコモグループの役員、社員、パートナー社員（派遣社員など）を対象に、標的型攻撃メール訓練を毎年実施し、警戒意識の維持・向上を図るとともに、全員がインシデント発生時の報告手順を確認する取組を毎年継続的に実施しています。

—情報セキュリティ研修・意識醸成

NTTドコモでは全社員に対して情報セキュリティリテラシーの向上を図るとともに、情報資産の適切な管理を実行するために、定期的・継続的な教育・訓練を実施しています。「情報管理研修ガイドライン」で示す学習プログラムの枠組みに基づき、eラーニングなどによる情報セキュリティ／サイバーセキュリティの認識向上に向けた教育を提供しています。これらの教育プログラムは役員、社員、パートナー社員（派遣社員など）に受講を義務付けています。

さらに、グループ各社の社長は就任時に、NTTグループ共通の社長向けセキュリティ研修を、またシステム管理責任者にはシステムセキュリティ研修を毎年受講し試験をパスす

ることを必須化するなど、それぞれの役割に応じた研修も拡充しています。

セキュリティ人材強化

国内のサイバーセキュリティ人材は11万人以上不足しているとされており、サイバー攻撃の高度化やデジタル化の進展に伴い、今後さらに深刻化するとされています。NTTドコモグループは、高度な専門スキルを有するセキュリティ人材の拡充と、安心・安全なサービスの提供に関わるすべての人材に対するセキュリティスキルの底上げに取り組んでいます。

■セキュリティ人材CoE (Center of Excellence)

情報セキュリティ部門と人事部門による「セキュリティ人材CoE」体制を構築し、セキュリティ専門人材の採用・育成・配置に戦略的に取り組んでいます。高度な専門スキルを有するセキュリティ人材を計画的かつ継続的に輩出し、NTTドコモの情報セキュリティ強化だけでなく、個人のお客さま向けサービスの安全性向上、法人のお客さまのセキュリティ上の課題解決への貢献といったさまざまな分野でセキュリティ人材が活躍することをめざしています。

—新卒採用と高度なセキュリティ育成プログラム

NTTドコモでは、セキュリティフィールドでの活躍が期待される新卒者を一定数採用しています。採用者は入社後、NTTドコモビジネスのセキュリティ人材育成子会社であるN.F. Laboratories社で3か月から最大12か月のセキュリティ技術に関するトレーニングを受けた後、1～2年間セキュリティ関連業務に従事することで、業務に必要な情報セキュリティ上のナレッジやノウハウを高水準かつ均質的に習

得します。

これらのカリキュラム修了後、個人の希望や適性に合致したポジションに配属され、即戦力として活躍しています。採用数は、2024年度35名、2025年度52名、2026年度59名と推移しており、今後も拡大していく予定です。

■セキュリティ社内認定制度

NTTドコモグループは、安心・安全・安定的なサービスの提供におけるセキュリティ専門知識や、IT活用・DX化の推進に必要なセキュリティスキルを習得するにあたり、有用な国家・民間資格の取得を奨励・支援しています。

またIPAの情報処理安全確保支援士・情報セキュリティスペシャリスト、ISC2のCertified Cloud Security Professional (CCSP) / Certified Information Systems Security Professional (CISSP)、ISMS審査員などの特定の資格・業務スキルを有する人材をセキュリティ中級・上級人材として認定しており、セキュリティ中級以上の人材は、あらゆる組織・業務におけるセキュリティ強化・維持に寄与することから、中期的な目標を定めて認定者数拡大を推進しています。

■主な認定制度と認定者数(ドコモグループ)

(名)

認定制度	目標	2023年度	2024年度	2025年度
セキュリティ中級・上級認定	2,160	1,715	1,755	1,991

情報セキュリティ監査

NTTドコモは、情報セキュリティ監査を「情報システムの開発運用にかかわるシステムセキュリティ監査」と、「情報システムやサービスの利用にかかわる業務セキュリティ



監査」の2軸で行っています。どちらの監査においても、セキュリティ対策が適正に実施・運用されていることを継続的に確認するため、内部監査部門が業務執行から独立した立場で、全組織を対象に情報セキュリティ監査を実施しています。監査結果を踏まえて、セキュリティ対策の是正や助言を行い、必要に応じて情報セキュリティ部門にセキュリティ対策の改善提案を行います。

監査計画については、社内外における情報セキュリティインシデントの発生状況やグループで要求するセキュリティ対策の変更などの環境変化を注視しながら、内部監査部門が培ってきたノウハウを活用して監査対象のリスクを評価し、策定しています。

■ システムセキュリティ監査

システムセキュリティ監査は、NTTドコモグループが保有しているシステムを対象にリスクベース評価でリスクの大きなシステムを開発・運用する部門に対して、技術的セキュリティ対策の実施状況を確認するもので、最低年に1回実施しています。2025年度は技術的セキュリティ対策全般の項目について、合計8件の監査を行い、是正すべき点の指摘と助言を行いました。是正すべき点は、内部監査部門が必要に応じて指導し、是正完了まで証跡をもって確認しています。

■ 業務セキュリティ監査

業務セキュリティ監査は、各組織のリスク評価によって合理的に監査対象を決定し、組織的セキュリティ、人的セキュリティ、物理的セキュリティの実施状況を確認するもので、最低年に1回実施しています。

2025年度は委託先との個人情報の授受に関する項目や情報機器の取扱いに関する項目について合計42件の監査を行

い、是正すべき点を発見し是正を指導しました。是正すべき点は内部監査部門が是正完了していることを確認しています。

■ 監査人の独立性

内部監査部門が取締役会に直接付議することで内部監査計画を承認しており、監査結果も同様に代表取締役や取締役会へ直接報告しています。これらにより業務執行から独立した立場で監査できる体制を確保しています。

また、各監査人は一定期間以内に所属した部門の監査をしてはならないと定め、監査人の独立性を確保しています。

データプライバシーの保護

■ 個人情報保護に関する方針・ガイドライン

事業を運営していく上で、個人情報の重要性を認識し、保護の徹底を図ることが最大の責務と捉え、お客さまへ安心・信頼を提供するための方針を明文化した「プライバシーポリシー」を策定・公表しています。

2019年12月には、NTTドコモパーソナルデータ憲章に掲げる行動原則に基づいて再編し、これまでのパーソナルデータの取扱い範囲を変更することなく、シンプルでわかりやすい構成・表現に改めました。また、2023年度にも個人情報保護法の改正に伴う改定など、随時方針の見直しを行い、個人情報の保護に努めています。

個人情報の取得、利用・提供、匿名化した情報の取扱いについては、個人情報保護法などの法令の順守および改正への対応を速やかに行い、個人情報保護のための管理体制を確立するとともに、社内規程などに従い適切かつ慎重に取扱っています。お客さまに対しては、取扱う個人情報の内容、情報の利用に関するお客さまの同意に関する事項、第三者提供な

どについて、プライバシーポリシーにて公表しています。またドコモショップにおいて、利用目的を明示のうえ、契約に必要な情報などを取得しています。第三者への個人データ提供についても、法令により認められる範囲もしくはお客さまから同意を得た範囲の範囲に限定しています。

また、2018年5月にEUで新たな個人情報の枠組みとして個人データに関するルールを定め、施行された一般データ保護規則 (General Data Protection Regulation (GDPR)) に関しては、「GDPR対応マニュアル」を制定しました。2019年4月には、EU個人情報の取扱いなどを定めた社内規程として「情報管理細則 (EU個人データ取扱い編)」を制定しました。

重大な個人情報の漏えいやデータの盗難・紛失が発生した場合にはホームページ上でお知らせしています。

□ NTTドコモ パーソナルデータ憲章 -イノベーション創出に向けた行動原則-

■ 個人情報の管理

NTTドコモはお客さま情報を管理するシステムのアクセス権限を必要最小限の社員とし、担当者ごとに取扱う情報を設定および制限しています。その上で、システムの使用時には都度、生体認証*を必須とし、利用履歴の確認も定期的実施しています。個人情報への不正なアクセス、個人情報の漏えい、滅失またはき損などのリスクに対し合理的な措置を講じ、個人情報の正確性および機密性を確保しています。

* 生体認証：指紋、顔、声などの身体的特徴によって、利用者本人であるかどうかを確認する仕組み

■ パーソナルデータの活用

AIやIoTの進展により、ビッグデータを活用した多様な製品・サービスが生み出され、これまでにない新しい価値の創出に向けた取組みが社会全体で加速しています。NTTドコモ



は「新しいコミュニケーション文化の世界の創造」という企業理念のもと、これまでにない豊かな未来の実現をめざし、イノベーションの創出に挑戦し続けています。今後も、お客さまのパーソナルデータ、あらゆるモノやコトのデータ、そのデータからさまざまな知恵を生み出す人工知能などの技術を活用することにより、データから新しい価値を生み出し、お客さまや社会に還元していきます。一方で、お客さまの大切なパーソナルデータの活用にあたっては、法令順守はもちろん、お客さまのプライバシーを保護し、お客さまへ配慮することも重要な使命と考えています。NTTドコモは、これまでと変わらずこれからも、お客さまの信頼に応え続けるという強い信念のもと、責任を持ってパーソナルデータを取扱います。

NTTドコモは「データ活用によるお客さまや社会への新たな価値の継続的な提供」とともに、「お客さまにとって最適なプライバシー保護」を実現すべく、データ活用に関する会社方針として「パーソナルデータ憲章」を制定し、2019年8月に公表しました。同憲章において6つの行動原則を定め、これらに則ったデータ活用を行っています。2024年4月には、パーソナルデータを取り巻く環境の変化を踏まえ、以下3つの観点で一部憲章の見直しを実施しました。

- 子どもやシニア層のプライバシーへの配慮
- NTTドコモグループ各社でのプライバシー配慮
- 委託先におけるセキュリティ対策

パーソナルデータの活用について、イラストなどを用いてわかりやすく解説した「知ってナットク!ドコモのパーソナルデータ活用」を公開するとともに、お客さまご自身がパーソナルデータの取扱いについて同意していただいた主な内容を確認

し、一定の範囲で設定・変更することができる「パーソナルデータダッシュボード」をホームページ上で提供しています。

今後も、個人情報保護はもちろんのこと、パーソナルデータを適切に取扱うなど、データプライバシーの保護に努めていきます。

□ 知ってナットク!ドコモのパーソナルデータ活用

□ パーソナルデータダッシュボード

■ プライバシー影響評価(PIA)制度

NTTドコモはお客さまの大切なパーソナルデータの活用にあたり、法令順守や安全管理のための体制や制度、そして「NTTドコモパーソナルデータ憲章」に掲げる行動原則に基づき、プライバシー影響評価(Privacy Impact Assessment (PIA))制度を整備し、運用しています。当制度のもと、パーソナルデータを利用した施策やサービスの企画段階から、お客さまのプライバシーに配慮しているかを評価し、お客さまのプライバシーの保護に力を入れて取組んでいます。

具体的には、パーソナルデータを利用した施策・サービスを実施するにあたり、プライバシー観点の評価項目について施策・サービス実施部門において評価します。利用するパーソナルデータの性質や利用方法など一定の基準に当てはまる場合には、専門的な諮問機関として社内を設置した「PIA会議」での評価を実施しています。評価する際には、「NTTドコモパーソナルデータ憲章」の行動原則に反していないか、お客さまや社会から受容されるかという観点を中心に実施しています。「PIA会議」ではこれまで650件以上のパーソナルデータを利用した施策・サービスの評価し、評価結果を踏まえて必要に応じて見直しや改善などを図っています。2025年度は、合計62件の評価を行いました。

過去事例 1

お客さまの位置情報や決済履歴、サービス利用状況などのパーソナルデータをAIが横断的に活用し、お客さま一人ひとりの趣味嗜好や生活パターンを理解したうえで最適な情報や提案を提供するサービス「SyncMe」の提供に際して、評価を実施しました。具体的には、データ利用についてわかりやすく説明ができているか、不安や不快に感じないかといった観点から評価を行いました。

過去事例 2

「d ticket」の提供に際して、チケット購買データや顧客基盤を利用するため、データ利用についてわかりやすく説明できているか、お客さまにメリットを感じていただけるかなどの観点で評価を実施しました。

□ プライバシー対策はどうなっているの?

PIA会議付議件数

(件)

2023年度	2024年度	2025年度
76	85	62

■ パーソナルデータ憲章・PIAに関する社員への研修・啓発

NTTドコモでは、すべての社員・役員を対象に、パーソナルデータ憲章およびプライバシー影響評価(PIA)に関する研修・啓発を年1回以上行っています。また、NTTドコモグループ各社でもお客さまのパーソナルデータを取扱う社員を対象に同様の取組みを実施しています。



AIへの対応

AIガバナンスの背景

NTTドコモは、AIを活用した業務のDX推進や付加価値サービスの提供に向けた取り組みを進めています。AIには、テキスト生成や画像・動画生成、画像解析などさまざまな種類があり、それぞれの特性に適した活用方法を選択することで、これまで人手で行っていた作業の大幅な効率化や、新たなアイデア創出を実現することが可能になります。一方で、AIの利用による思わぬ差別、不当な行動制約や誘導、知的財産権の侵害や偽情報、誤情報の生成・拡散などの新たなリスクも発生し、AIがもたらす社会的リスクは多様化・増大の傾向にあります。

NTTグループでは、AIに対する不安を払拭し、競争力強化と安全性向上を両立するため、「NTTグループAI憲章」をはじめとするAI活用の基本方針や規程類を整備しています。NTTドコモにおいても、これらの方針・規程類に基づき、「ドコモグループAIリスクマネジメントガイドライン」を制定するとともに、ガイドラインに沿った運用を実施し、安全かつ適切なAIの活用を推進しています。

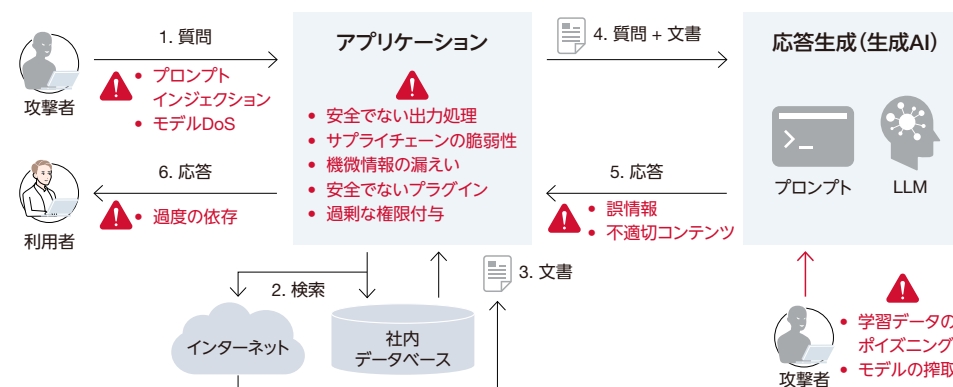
□ NTTグループ AIガバナンス

ドコモグループAIリスクマネジメントガイドラインの位置付け

ドコモグループAIリスクマネジメントガイドラインの目的は、AI利用リスクを適切に評価し、リスクの発生を防止または発生した場合の事業への影響を軽減するとともに、積極的なAI利用と価値創出を推進することです。

AI利用のリスクは図の通り、AIのモデル自体だけでなくアプリケーションや利用者も含めたリスク管理が重要となっています。AIリスクマネジメントガイドラインでは、AIモデル開発者・AIサービス提供者・AI利用者の3つのロールでそれぞれのリスクに対する対策を規定しています。

AI利用のリスク例(生成AIの場合)

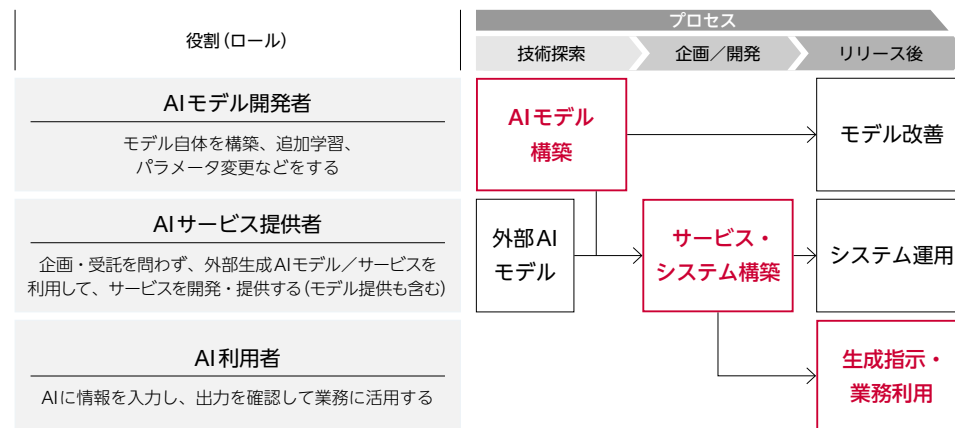




■ドコモグループAIリスクマネジメントガイドラインにおけるロールと対策基準

本ガイドラインでは、AIの活用形態に応じて3つのロールを定義し、それぞれの責任範囲やリスク特性に応じた対策基準を定めています。これにより、AIモデルの開発からサービス提供、利用に至るまで一貫したリスク管理を実現するとともに、適切なガバナンスの下でAIの活用と価値創出を推進しています。具体的には、AI利用者に対しては情報管理や著作権・誤情報への対応などの基本的な対策を、AIサービス提供者やAIモデル開発者に対しては、学習データやモデル品質の管理、独自データの活用に伴うリスク管理など、より高度な対策を求めています。

各ロールの関係性



■ドコモグループAIリスクマネジメントガイドラインの社内審査プロセス

NTTドコモは各ロールごとに定められた対策基準に沿って運用を行い、品質の安定化を図るための社内審査プロセスを設けています。

また、リスクを5つの項目に分類し、それぞれについてリスク管理部門が審査を実施しています。

5つのリスク対策

●AIモデル/サービスの選定

学習データの改ざんによる不正アクセスを起因とした第三者からの攻撃などのリスクを低減できる技術選定

●管理情報の保護

管理情報のLLM (Large language Models) 学習による、第三者のLLM利用時における管理情報混入の防止

●パーソナルデータの保護

個人情報保護法などの法令順守にかかわる確認、プライバシー影響評価制度の運用

●知的財産権の保護

LLM学習や生成物利用における第三者の知的財産権侵害の対処

●誤情報・倫理等のレピュテーションリスクの防止

LLMの不適切な回答などが拡散されることによるレピュテーションリスクを踏まえたチューニング、運用体制

社内審査プロセス

