安心・安全

すべての人が安心・安全に暮らせる、ICTに守られた社会へ

マテリアリティ（重要課題）

社会インフラ品質の向上

堅牢なセキュリティ環境

社会の期待

ICTによるインフラの発展は、同時に新しい課題も生み続けています。悪意ある攻撃で社会システムがダウンする、災害で通信ネットワークが遮断する、不慮の事故でお客さまや社会の財産を損なうなど、さまざまな事態を想定した柔軟・強靭・安定したインフラづくりは今や不可欠であり、ICT企業の使命は重みを増しています。

今日も、明日も、見守り、支える

ICT技術の進化にともない、経済性にとどまらず、「安心・安全」を実現するための責任も増しています。NTTドコモソリューションズグループは、情報インフラを提供するNTTグループの一員として、その円滑な運用・保守を実現する品質維持・事業継続体制を整備し続けます。また、日々生まれる新たなセキュリティリスクに対しても信頼性の高い技術を積極的に取り入れ、社会に責任を果たします。

ビジネス環境や働き方の変化を見据えた「SmartCloud®IAMソリューション」

ビジネス環境のDXや、テレワークを中心とした新しい働き方が急速に広まる現在、セキュリティやガバナンスの在り方も大きな変化を迫られています。新たな時代のリスクに適切に対応するため、「誰に・どのような権限で」アクセスさせるか、「どのような手段で」アクセスさせるかを適切に管理する「ID管理&アクセス管理(IAM)」が以前にも増して重要になりつつあります。

「IAMソリューション」は、クラウド、オンプレミス双方に対応可能なハイブリッド型のID管理、統合認証を提供し、監査を含めた内部統制強化への対応と利用アプリケーションを選ばない柔軟なシングルサインオン(SSO)環境の実現を両立しています。

また、ID管理から統合認証へのプロビジョニング機能をコーディング不要で設定できる「プロビジョニング設定の容易さ」、トラブル発生時の迅速な解析・対策をトータルでコーディネートする「保守サポートのしやすさ」、親和性の高い製品の採用による「段階導入のしやすさ」を提供することで、変化の激しいビジネス環境や働き方に俊敏に対応します。

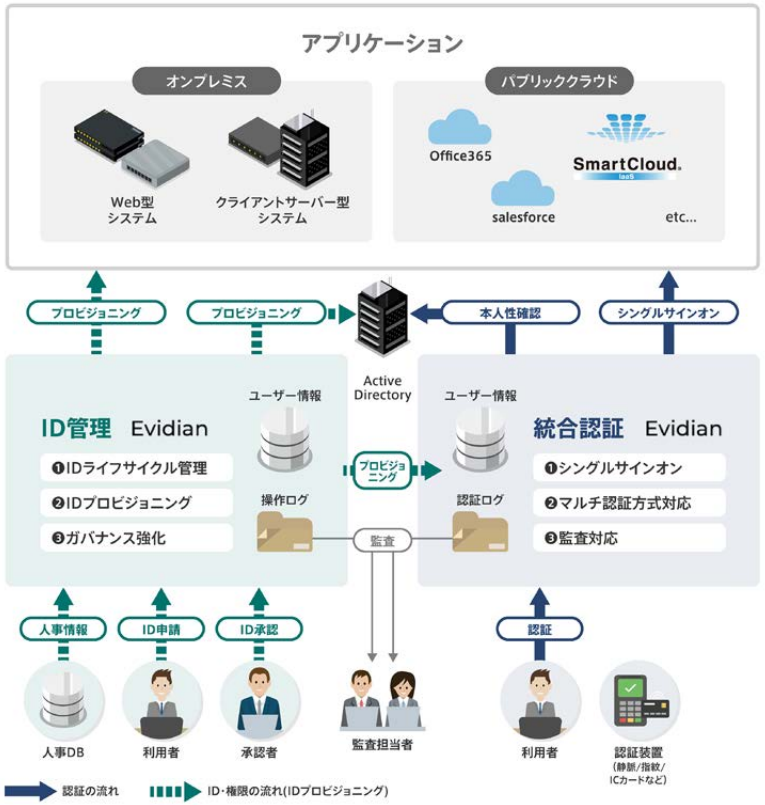
インパクト

セキュリティと柔軟性

新しい働き方への貢献

主に貢献するSDGs

» 統合された、柔軟かつ強固なID管理・統合認証の仕組み



＊「SmartCloud(スマートクラウド)」「SmartCloud」ロゴは、NTTドコモソリューションズ株式会社の登録商標です。
＊ Evidianは、NTTドコモソリューションズと戦略的協業契約を締結しているEviden社の製品です。
＊ Active Directory、Office 365は、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。
＊ Salesforceは、Salesforce, Inc.の商標または登録商標です。
＊ その他、記載されている社名、商品名などは、各社の商標または登録商標である場合があります。

» 2024年度の主な実績

マテリアリティ	サステナビリティ定量指標	2024年度目標	2024年度実績
●社会インフラ品質の向上	S級重大故障発生件数	0件	0件
	IP相互接続切り替えにおける全通信キャリアとの重要課題未解決件数	0件	0件
●堅牢なセキュリティ環境	◇サイバー攻撃にともなう重大なインシデント発生件数	0件	0件
	◇重大な情報漏えい件数	0件	0件

◇：グループKPI

何故重要か

ICT技術の進化にともない、経済性にとどまらず、「安心・安全」を実現するための責任も増しています。例えばネットワーク社会のグローバルな浸透の結果、ICTを悪用した「サイバー犯罪」の巧妙化や国際犯罪化が、新たな社会リスクとして顕在化しています。加えて、世界各地において自然災害や気象現象の激甚化なども深刻化しています。このように、レジリエント(強靭)でサステナブルなICTインフラを実現し、安心・安全かつ先進的な生活環境へと貢献することに、社会の期待が一層高まっています。

NTTドコモソリューションズグループは、情報インフラに従事するNTTグループの一員として、提供する各種ICTサービスの品質を高め続けることに加え、その円滑な運用・保守を実現する事業体制を整備しています。また、セキュリティリスクに対しても信頼性の高い技術を積極的に開発・展開しています。さらには、情報漏えいの防止はもちろん、AIなど新たな技術の活用に際し、社員の法令違反や権利侵害を予防する仕組みも重要であり、その強化に取り組んでいます。

発揮をめざす社会・環境インパクトの例

- 堅牢性、セキュリティに優れたデータセンターサービス
- 安定性・効率性に優れた、高品質なシステム・クラウドソリューション
- 公共や企業ネットワークのセキュリティ、保守サービス
- 自社のBCP、セキュリティの徹底、情報漏えいの防止、他者の権利の適切な取り扱い

2024年度　総括

2022年度から、サステナビリティテーマ「安心・安全」は、「社会インフラ品質の向上」「堅牢なセキュリティ環境」をマテリアリティに掲げ、従前からの各種活動のさらなる進化に挑んでいます。

「社会インフラ品質の向上」では、重大な影響を及ぼす故障の管理および再発防止、未然防止活動を継続的に実施するとともに、発生した故障に対しては「社会・顧客への影響度」に重点を置き、提供者目線ではなくお客さま目線を重視した評価を行うなど、通信サービスの安定性と信頼性の確保に努めています。さらに、災害発生時の対応強化に向けリスク要素の見直しやBCP体制の強化、有事訓練などを継続的に実施し、「もしも」に日々備える仕組みを一層強固にしました。

「堅牢なセキュリティ環境」では、NTTグループKPIであるサイバー攻撃にともなう重大なインシデント発生件数と重大な情報漏えい件数を重視し、適切な防衛・有事対応体制を強化しています。またこれらを継続的に実践するため、社員の能力向上および情報管理意識の啓発も、引き続き徹底していきます。

社会インフラ品質の向上

システムの「品質」と「信頼性」は、日本の社会インフラを支えてきたNTTドコモソリューションズが重視している価値であり、強みでもあります。
システムを安定して提供するために国際的な規格や指標などを導入し、多角的な視点から、品質向上への継続的な取り組みを行っています。

品質マネジメントシステムの取り組み

NTTドコモソリューションズは、1997年9月の創業直後に品質マネジメントシステムの国際規格であるISO9001の認証を取得して顧客要求事項に基づく活動を展開し、品質向上に役立てています。

» 品質マネジメントシステムの認証取得状況

対象業務	ソフトウェア開発およびサービス業務
登録番号	JQA-1997
取得日	1997/11/28
審査登録範囲	顧客要求事項に基づく ❶ 情報通信システムおよびソフトウェアの設計・開発、構築、運用および保守 ❷ 情報処理サービスの提供

品質マネジメントシステム推進体制

NTTドコモソリューションズは、社長をトップマネジメントとし、各事業本部のPMO（Project Management Office）、SMO（Service Management Office）などで構成した品質マネジメントシステムの運営体制を確立しており、品質管理プロセスの継続的な改善を推進しています。

品質マネジメントシステムの教育・浸透

NTTドコモソリューションズの品質マネジメントシステムに関する理解と浸透を目的として、以下の施策を実施しています。

- 新入社員の導入研修および経験者採用時のウェルカム研修において、NTTドコモソリューションズの品質マネジメントシステムを構成する品質管理プロセスの講話を実施しています。
- 品質マネジメントシステムの変更について、全社周知するとともに各事業本部のPMOとSMOへの説明・展開により品質管理プロセスの浸透を実施しています。

品質方針の徹底

NTTドコモソリューションズは、全社的に定めた「品質方針」のもと、お客さまに満足していただけるシステムとサービスの提供に取り組んでいます。品質目標を設定し、達成に向けて取り組むとともに、品質マネジメントシステムの継続的改善に努めています。

NTTドコモソリューションズ 品質方針

NTTドコモソリューションズは、お客さまから信頼され、満足されるシステム及びサービスを提供するために次の事項を行います。

❶ 品質目標を設定し、目標達成に向けて改善をします。
❷ 品質マネジメントシステムの有効性を評価し、マネジメントレビューを定期的に実施し、継続的改善に努めます。
❸ 関係する法律、規制等の要求事項を遵守します。

システム開発業務の品質向上

NTTドコモソリューションズは、ISO9001に基づく管理プロセス・体制を構築し、開発工程ごとにきめ細かなチェックを実施しています。それによって、社会インフラに求められる厳しい品質水準をクリアしています。

サービス業務の品質向上

NTTドコモソリューションズは、サービス業務の品質向上を目的に、ITサービスマネジメントのベストプラクティス集として国際的に利用されている「ITIL®(Information Technology Infrastructure Library)*」をベースに、NTTドコモソリューションズが提供する運用プロセスを標準化した「サービス標準」を制定しています。この「サービス標準」をもとにした営みの中で業務改善・品質改善を実践し、着実にサービス業務の品質向上に取り組んでいます。

*「ITIL」は、AXELOS Limitedの登録商標です。

品質管理の取り組み

NTTドコモソリューションズは、社会インフラのシステム管理を担う企業として、重大な影響を及ぼす故障の管理および再発防止、未然防止活動を継続的に実施しています。

この故障管理においては、発生した故障に対して「社会・顧客への影響度」に重点を置き、提供者目線ではなくお客さま目線を重視した評価をしています。特に、著しく影響度の大きい重大故障については「S級重大故障」と位置づけるとともに、KPIとして「年間発生件数：0件」を目標に設定しています。2024年度は、「S級重大故障」に該当する故障は0件でした。今後もさらなる品質向上に努めていきます。

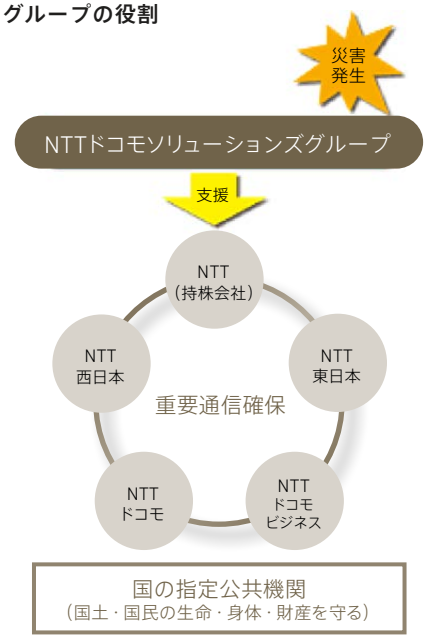
災害対策の取り組み

NTTグループは、国の指定公共機関として、「サービスの早期復旧」「重要通信の確保」「ネットワークの信頼性向上」を災害対策の3つの柱としています。避難所への非常用電話機の設置、「災害用伝言ダイヤル(171)」の提供など、災害時における通信手段を確保するとともに、通信設備の早期復旧に向けた幅広い取り組みを行っています。

こうした中、NTTドコモソリューションズグループは、NTTグループの一員として、ライフラインである通信ネットワークの早期復旧に向けた技術的支援などさまざまな災害復旧活動を行い、通信サービスの確保に貢献しています。東日本大震災をはじめ、近年頻発する豪雨災害などにおいても、被害を受けたNTTグループの通信設備の復旧をさまざまな形で支援しました。

また、NTTグループの通信インフラ設備の構築・保守・運用で培った技術・ノウハウをもとに、災害時の迅速な復旧を可能にする態勢の構築や耐災性の高いデータセンターの整備などを進め、お客さまの通信システムの安定的な運転を確保しています。

» 災害復旧におけるNTTドコモソリューションズグループの役割



災害発生に備える体制

NTTドコモソリューションズでは、統合監視センター「FSC24®(Field Service Cockpit 24)*」により、24時間365日、提供システムを一元的に監視・保守する体制を構築しています。NTTグループの通信インフラ設備の構築・保守・運用で培った技術・ノウハウをもとにした高度なスキルにより、近年の自然災害・システム障害対応では同センターが司令塔となり早期復旧に大きく貢献しています。また、首都直下地震のような大規模災害発生時には、社長を本部長とした災害対策本部を設置し、NTTグループ各社やお客さまと緊密な連携を図りながら、サービスの安定的な提供に向けて活動します。直近の能登半島地震の発生直後には、「FSC24®」の速やかな初期態勢構築により、関連組織へ迅速かつ的確な情報配信を行うことができました。

*「FSC24®(Field Service Cockpit 24)」は、NTTドコモソリューションズ株式会社の登録商標です。

「FSC24®」の信頼性を確かなものとするために

「FSC24®」には、高度な専門技術を有する技術者を配置しており、トラブル発生時に関連組織や協力会社を含めて指揮統制し、早期復旧に努めています。また、「FSC24®」は予備エンジンの配備などによりデータセンターと同等の耐災性を備えています。

NTTドコモソリューションズは、「FSC24®」の危機管理体制と信頼性を確かにすることを通じて、皆さまの生活や事業活動を支えています。

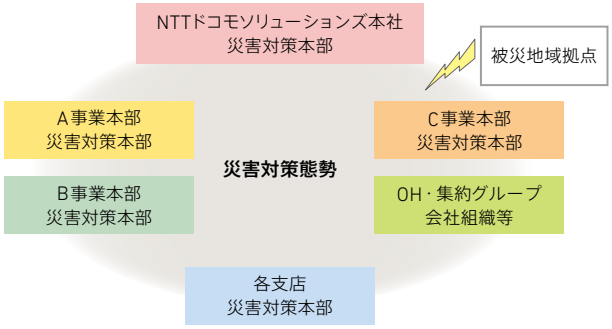
災害発生に備えた具体的な取り組み

災害対策訓練の実施

NTTドコモソリューションズグループでは、首都圏や東海、関西での地震による被災など、さまざまな災害を想定した訓練を毎年実施し、大規模災害発生時においても迅速な対応ができるように日頃から備えています。特に昨今では東日本大震災の経験を踏まえNTTドコモソリューションズ組織(ロケーション)ごとの災害対策態勢強化に取り組んでいます。

また、NTTグループの一員として、NTTグループ各社の災害対策訓練などにも参加し、災害時における連携体制を再確認しています。

» 災害対策訓練の模様



» 2024年度主な災害対策訓練実施状況

災害対策訓練実施時期	実施時期
NTTドコモソリューションズ 災害対策訓練	2025年3月

2024年度の災害対策訓練は、東北エリアを想定被災地として選定し、機能改善したリモートツールなどを活用した初期態勢の構築および本社・支店・グループ各社との連携方法の再確認などに並行して取り組み、確認を行いました。

信頼性の高いデータセンターの提供

NTTドコモソリューションズが提供するデータセンタービルでは、震度7の地震が発生した場合にも甚大な被害を受けない水準の信頼性を確保するとともに、大規模停電時にも予備エンジンによる電力供給を行えるようにし、通信システムの安定的な提供に努めています。

非常災害時における対応

NTTドコモソリューションズでは、新たな感染症パンデミック発生時において想定される被害を考慮しつつ、社会的機能の維持、お客さまとの関係維持や会社経営の維持・存続の観点から、①人命最優先、②お客さまの意向を踏まえた業務の優先順位づけ、③グループ・委託先との連携、を基本的な考え方に事業継続計画を策定してきました。2011年の東日本大震災を受け、パンデミック発生時を想定して策定した事業継続計画を基本に、大規模災害発生時の事業継続計画も策定し、有事には災害対策本部などとも連携し、柔軟に対応していきます。

2024年度は、社員安否確認等のさらなるガバナンス強化や社員の安全の確保および環境整備のために以下の取り組みを実施しました。

災害シミュレーションによる災害時基本行動の定着

リモート勤務が定着し常態化している中、遠隔での災対態勢の確立や情報を速やかに提供・把握するため、災害ポータルサイトのUI改善や通知機能の追加などのシステム改善を行い、仕組みを充実させるとともに訓練を通じて確認手順などの定着化を図っています。

自然災害等への早期対応

台風等の被害が予想される場合の出退勤等における厳重な警戒や服務の扱いについて、年度初めに周知を実施するとともに、実際に台風等の被害が予測された場合には、情報収集を行い社員へ展開を図っています。また、豪雨による土砂災害や、北朝鮮ミサイル発射によるJアラート発動にも、迅速に情報収集・判断・報告を行い、これら社会的な不測事態発生時においても社員への情報展開を図り、人的被害の抑止に向けた早期行動を促しました。

その他、最大震度5強以上の地震発生時には、迅速に社員・家族の安否確認などを実施し、的確な対応を行っています。

大規模災害対応の連絡体制強化

2024年1月1日に発生した能登半島地震の対応の振り返りを踏まえたNTTドコモ、NTTドコモビジネスとの災害時における社員安否確認等の連携体制の整理を図るとともに、社内における災害時のエスカレーションルールも明瞭化しました。

南海トラフ地震臨時情報への対応

2024年8月に南海トラフ地震臨時情報（巨大地震注意）が、2019年の制度開始後初めて発表された際、迅速に情報収集を図るとともに、NTTグループの対応方針を速やかに社内へ展開し、有事に備えた統制を行いました。また、「南海トラフ地震臨時情報」発表時の態勢明確化のため、2025年1月に災害対策等規程の改訂を行いました。

堅牢なセキュリティ環境

国際標準の情報セキュリティ規格に準拠したルールと仕組みを整備するとともに、社員の意識向上や技術的対策に注力し、着実な管理水準の向上に努めています。また、情報漏えいの防止や他者情報の適切な管理など、法令遵守を徹底しています。

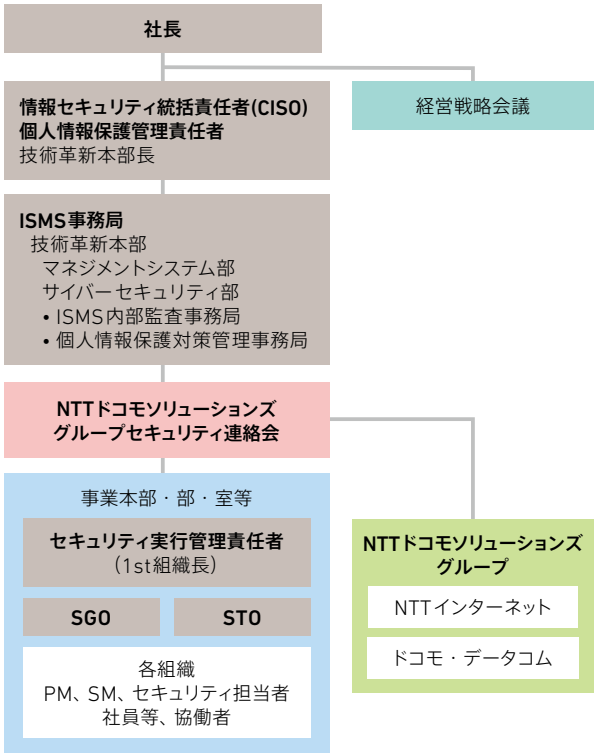
情報セキュリティ

NTTドコモソリューションズは、情報セキュリティ管理を適切に実践することを企業責任のひとつと認識しています。その基盤として、「情報セキュリティポリシー」「個人情報保護方針」を制定し、ISO27001に基づく仕組み「情報セキュリティマネジメントシステム(ISMS)」を確立しています。また、個人情報・情報資産を保護することの重要性を認識し、日常の事業活動を通してお客さまの信頼に応えるべく、情報セキュリティ対策を徹底しています。さらに、情報システム分野の最新技術を活用し、情報セキュリティ水準の維持・向上に努めていきます。

情報セキュリティ推進体制

NTTドコモソリューションズは、個人情報保護を含む情報セキュリティ活動について、社長、副社長、執行役員をメンバーとして構成される「経営戦略会議」で、①情報セキュリティ活動全般の戦略的計画の決定、②セキュリティ基本方針の制改定の審議、③セキュリティ対策案件に対する審議と決定を実施しています。また、セキュリティに関する最高責任者であるCISOの統括の下に、全組織に情報セキュリティおよび個人情報保護活動を推進するための「セキュリティガバナンスオフィス(SGO)」「セキュリティ技術オフィス(STO)」を設置し、実効性の高い情報セキュリティ活動を展開しています。

» NTTドコモソリューションズの情報セキュリティ推進体制



情報セキュリティの教育・啓発

情報セキュリティを徹底するためには、社員一人ひとりの意識を高めることが不可欠です。NTTドコモソリューションズでは毎年、社員および協働者等を対象に、WBTを活用した「情報セキュリティ研修」を実施し、社員一人ひとりのセキュリティ意識を高めています。情報セキュリティ研修には、セキュリティに関する最新の話題を盛り込み、常に社員のセキュリティに関する意識を向上させ、基本動作の徹底を啓発しています。

また、各階層におけるセキュリティ活動の意識向上、レベルアップを目的として、さまざまな施策を実施しています。

- 毎年、新入社員の導入研修において、学生から社会人になり、セキュリティの重要性を認識する機会としてセキュリティ講話を実施しています。
- 毎年、新任課長研修において、管理職が自らセキュリティ活動の持つ意味と重要性を認識し、セキュリティ活動上の役割および責任について意識向上するため、セキュリティ講話を実施しています。
- 2024年度から、新たに昇級、昇格したリーダー層に対して、求めるセキュリティ上の行動を明確化し、セキュリティ対応力を向上させるため、階層別に研修を企画・実施しました。その他、「情報セキュリティポリシー」「個人情報保護方針」を浸透させるための社員向け情報セキュリティガイドの改訂、セキュリティインシデント事例などの周知を通じた注意喚起なども随時実施しています。

セキュリティレベル高度化の取り組み

昨今の国内外のセキュリティ動向や他社の個人情報漏えいインシデントを踏まえ、NTTドコモソリューションズでは「技術的対策（端末、ネットワーク、サーバー、クラウドなど）」「物理的対策（運用管理を含む）」「人的・組織的対策（制度・ルール、研修、内部監査、体制・組織）」の各観点でセキュリティレベルの向上に取り組んでおり、特にゼロトラストに基づくシステム利用環境の高度化、および内部不正対策の強化を行っています。

さらには、子会社も含めた一体的な情報漏えい対策を実行するために、NTTドコモソリューションズグループとしてのガバナンス強化にも取り組んでいます。

徹底した情報セキュリティ対策の構築・運用

日常的に利用する電子メールによる情報漏えいのリスク低減を目的に、協力会社社員単独で社外へメール送信できない仕組み、および協力会社社員がプライベートアドレス宛へのメール送信を規制する仕組みの運用を行っています。

さらに、外部からの標的型攻撃メール対策として、従来のウイルス対策やファイアウォール・迷惑メールフィルタリングに加えて、社内から社外へ不審な通信が発生していないかを検知するシステムも導入し、監視運用を実施しています。

また近年、システムやネットワークの脆弱性を悪用したセキュリティ事故が発生している現状を踏まえて、お客さまに安心・安全にNTTドコモソリューションズの開発システムやサービスをご利用いただけるように、社内のPSIRT（ピーサート）組織が、脆弱性をつくり込まない、または万一、脆弱性をつくり込んでしまったときにも、脆弱性をリリース前に検知・修正することを目的としたセキュリティ脆弱性対策に取り組んでいます。

なお、未だ世界的に深刻視されているサイバー攻撃への対応を強化するため、NTTドコモソリューションズでは社内のCSIRT（シーサート）組織がNTTグループ各社セキュリティ組織と連携し、常に最新動向を収集しつつ、お客さまおよび自社のネットワークシステムにセキュリティインシデントが発生した際には、全社的な統制や指示を担い 、被害の特定と軽減、原因解析、再発防止などを実施します。

個人情報保護に関する取り組み

NTTドコモソリューションズではパーソナルデータの取り扱いルールを独自に定め、社内各組織のシステム開発やサービス提供案件に対し、個人情報保護法に基づく適切な個人情報の取り扱いを組織的に行うため、「個人情報取り扱い社内審査」の仕組みを導入しています。また、個人情報保護法など関連法令の改正や、個人情報保護に関するコンプライアンス事案をもとに、全社員に対して、個人情報保護に関する研修を実施しています。こうした取り組みを通じて個人情報保護活動を推進しています。

NTTドコモソリューションズにおける個人情報の取り扱いの詳細について
https://www.nttcom.co.jp/privacypolicy/

NTTドコモソリューションズグループにおけるISMS認証・プライバシー取得状況

NTTドコモソリューションズグループは、社員が情報セキュリティの重要性を認識し、日常の業務活動を通じてお客さまの信頼に応えるとともに、個人情報保護法に基づいた個人情報の適切な取り扱いを徹底するため、「ISMS認証」と「プライバシーマーク」をすべてのグループ会社で取得しています。

» NTTドコモソリューションズグループのISMS、プライバシーマーク認証取得状況

NTTドコモソリューションズグループ会社	ISMS		プライバシーマーク	
	登録番号	有効期限	登録番号	有効期限
NTTドコモソリューションズ株式会社	JUSE-IR-006	2026.6.21	11820039(14)	2027.5.10
NTTインターネット株式会社	JQA-IM0034	2025.11.30	21000009(11)	2027.4.26
ドコモ・データコム株式会社	JQA-IM0218	2026.3.3	11820328(10)	2025.4.6

» NTTドコモソリューションズグループの情報セキュリティ認証類の取得歴

1999年5月	NTTコムウェア「プライバシーマーク」取得
2003年4月	NTTコムウェア「ISMS」認証取得（JUSE-IR-006）
2005年9月	NTTコムウェアグループ全社「プライバシーマーク」取得完了
2014年8月	地域会社合併にともなう「ISMS認証」統合（JUSE-IR-006）
2014年9月	地域会社合併にともなう「プライバシーマーク」継続

サイバー攻撃にともなう重大なインシデントの抑制

NTTドコモソリューションズでは、2024年度に「サイバー攻撃にともなう重大インシデント0件」をKPIに定め、経営陣の統括のもと、技術革新本部が中心となり、その抑止を徹底していく対策を実施しています。

2024年度は、アラート等インシデントの予兆に対して迅速な対応を行うことで重大インシデントを回避し、「サイバー攻撃にともなう重大インシデント」は0件でした。また、サイバー攻撃にともなうインシデント以外についても管理しており、内部不正への対応を高度化する取り組みを実施しました。

引き続き、外部脅威への対応を高度化する取り組みとして、外部攻撃リスクの低減や訓練等を実施し、重大なセキュリティインシデント抑止に注力していきます。

開発・保守職域におけるリモートワーク導入に向けた取り組み

開発・保守職域でリモートワークを可能とする範囲を拡大していくことは、新しい働き方の模索の観点でも、またIOWN構想に即したシステム管理の省人化・リモート化を拡大していく観点でも、重要なテーマであり、リモートワーク環境におけるセキュリティ確保に向けて取り組んでいます。

開発職域においては、開発環境等におけるセキュリティレベル向上の必要性が高まっていることを受け、2024年度からNTTドコモソリューションズにおいても開発環境に対して各種セキュリティソリューションの導入を進めています。

また、保守職域においては、物理的・技術的・人的セキュリティ対策を講じ、社内審査を経た上で安心・安全にリモートワークを可能とするセキュリティ制度を整備し、その範囲を徐々に拡大しています。

今後もお客さまに提供するセキュリティ品質を維持・強化しつつ、社員のリモートワーク環境整備に資する施策・仕組みの積極的な検討を続けていきます。

情報セキュリティソリューションの提供

NTTドコモソリューションズでは、各種法令の遵守やITガバナンス強化など、お客さまのご要望に適合するセキュリティサービス・ソリューションを幅広く提供し、お客さまのゼロトラスト・セキュリティモデルの実現に貢献しています。

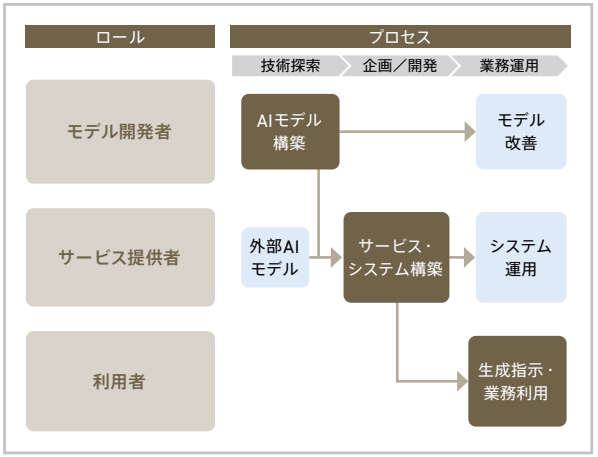
» 提供する情報セキュリティソリューションの例

ソリューション	概要
セキュリティ診断サービス	OSやミドルウェアの既知の脆弱性とWebアプリケーション固有の脆弱性を診断
サイバー保険付き脆弱性診断サービス	診断対象システムに起因して発生した情報漏えいなどの損害リスクをサイバー保険で補償
クラウドWAFオペレーションサービス	セキュリティ専門家が監視・運用を行うクラウドベースのWebアプリケーション・ファイアウォールを提供
s-WorkProtector®	インターネットの入口・出口対策とリアルタイム監視・保護
ゼロトラスト型セキュリティサービス	ユーザーがどこにいても安心・安全なテレワーク環境を提供
セキュリティリスクレポート	お客さまのセキュリティリスクを可視化
SmartCloud®IAMソリューション	企業のID管理を適正化し、セキュリティやガバナンスを強化するとともにアプリケーションごとの認証を統合したシングルサインオン環境を実現

AI利用に関する社内ルールと社員教育

NTTドコモソリューションズでは、NTTグループ共通のAI憲章およびAIガバナンスポリシーを上位文書とし、その下位に位置づけられる実務指針としての「AI利用ガイドライン」を策定しています。その中で、NTTドコモソリューションズとして認識すべき具体的なリスクと対策、社内審査プロセスおよび手続きを全社員向けに周知徹底しています。AI利用に関する一連のプロセスを明示することで、業務現場における判断基準の統一と、法令・倫理・社会的受容性への適合を図っています。また、本ガイドラインでは、AI利用者を「モデル開発者」「サービス提供者」「利用者」の3つのロールに分類し、それぞれの役割とリスクを明確にしています。ロールに応じた対策を整理することで、透明性と実効性のあるガバナンスを実現しています。

» 各ロールとプロセス



ガイドラインの実践事例として、NTTドコモソリューションズではAI技術の業務活用にともなうリスクを適切に管理するため、AI利用ガイドラインに基づいた社内審査制度を設けています。審査では、知的財産権の侵害、個人情報の取り扱い、機密情報の漏えい、倫理的な懸念など、幅広い観点からリスクを包括的に評価しています。具体的には、AIが生成・処理するデータや成果物が第三者の知的財産権への侵害をしていないか、個人情報が不適切に扱われていないか、また誤った判断や偏見が含まれていないかなどを慎重に確認します。これらのリスク評価は、専門領域ごとに担当チームが分担して実施する体制が整備されており、AI利用に関するリスクを漏れなく、かつ実効性のある方法で管理しています。過去の審査結果は社員が閲覧できるようになっており、社内審査の判断の透明性向上および対策内容の有効性強化に寄与しています。

また、システム開発およびサービス提供におけるAIリスクに対応するため、AIガバナンスとシステム開発における品質保証活動を連携させ、リスク評価および審査を一体的に行う仕組みを整備しています。これにより、審査結果の相互活用と重複作業の削減を実現し、品質および安全性の観点から整合性のある運用を可能にしています。

社員教育については、社内におけるAI活用のリスクへの理解を深めることを目的に、全社員を対象とした教育や啓発活動を実施しています。単なる利用ルールの周知にとどまらず、具体的な活用事例、リスクや留意点などを体系的に学べる内容となっており、社員一人ひとりのAIリテラシー向上をめざしています。