情報セキュリティ
Information Security

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。
NTTドコモでは情報セキュリティ対策を徹底し、
お客さまの情報資産を保護することに努めています。

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

● 情報セキュリティポリシー・マネジメント

ドコモでは、情報の適切な管理が重要な経営課題であることを認識し、お客さまに安心して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ドコモグループの取組み方針として「情報セキュリティポリシー」を宣言し、「情報セキュリティポリシー」および「プライバシーポリシー」の順守を徹底しています。情報セキュリティポリシーで対象としている情報資産は、企業活動において入手および知り得た情報、ならびに当社が業務上保有するすべての情報としています。

マネジメントについては、「情報セキュリティ管理責任者（CISO）」と「個人情報保護管理者（CPO）」を兼任する副社長を委員長とした情報管理委員会を設置し、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、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っています。

情報インシデントが起きた際は、インシデントの内容や影響度を把握し、本社情報セキュリティ部や総務部へエスカレーションする流れとなっています。影響度により代表取締役社長を委員長とする委員会が設置され、対応が行われます。

また、通信の秘密および職務上知ることができた秘密・個人情報を正当な理由なく使用し、漏らしたまたは漏らそうとした場合は、社内規定により懲戒処分の対象となります。

● 具体的なセキュリティ対策

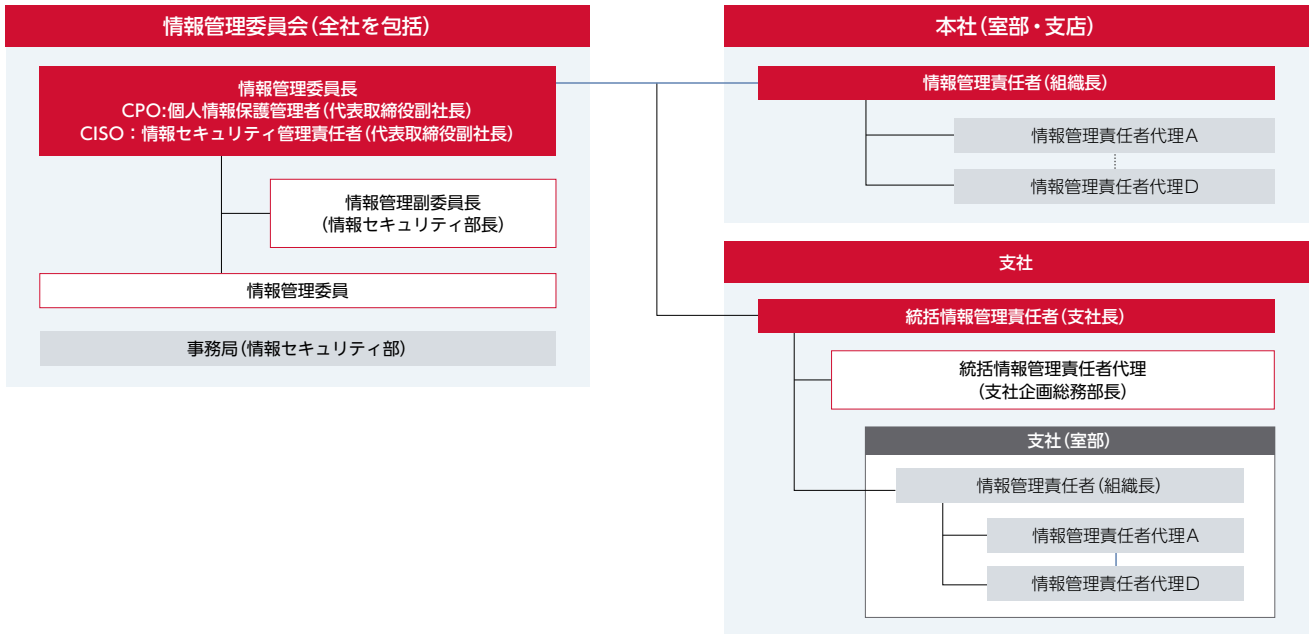
［脆弱性分析］

システム構築から運用に至るシステムライフサイクルの主要段階において、社内システム脆弱性に対する主なセキュリティ対策を社内規程に基づいて実施しています。システム保有部門およびセキュリティ統括部門が、それぞれ脆弱性情報に対して必要な対策の実施状況をチェックすることで、情報資産に係る不正アクセス・破壊・情報漏えい・改ざんなどの発生を予防するとともに発生した場合の被害最小化を図っています。

［情報セキュリティ研修・意識醸成］

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継続的な教育・訓練を実施しています。「ドコモセキュリティ教育全体図」における学習プログラムの枠組みに基づき、eラーニング等による情報セキュリティ／サイ

情報管理体制図



（2021年7月1日現在）

バーセキュリティの認識向上の教育を提供しています。これらの教育プログラムは経営層、管理者、社員にわたり、受講を必須としています。2020年度は、情報管理ルール、関連法令の対応、情報セキュリティのリスク動向と対策などについて、研修・啓発活動を実施しました。

また毎年11月を「情報セキュリティ強化月間」に定め、さまざまな取組みを実施することで社員の意識向上を図っています。

[項目別セキュリティ対策]

❶ 組織的セキュリティ

1. 情報セキュリティポリシーの制定
2. 情報管理に関する組織体制の整備
3. 情報セキュリティ基本方針の策定、規程・マニュアルの整備・運用
4. 情報資産の把握と運用管理
5. 監査・セキュリティチェックの実施・運用
6. 事故、違反への対応

❷ 人的セキュリティ

1. 誓約書による秘密保持の義務付け
2. 業務委託契約先へのセキュリティ対策および情報管理遵守の義務付け
3. 従業者、業務委託先、販売代理店に対する研修・啓発の実施
4. ハンドブック、動画配信など研修ツールの作成と配布

❸ 物理的セキュリティ

1. 情報管理端末の台数制限、設置場所および権限付与者の継続的適正化
2. 可搬型機器の貸与、持ち出し管理の徹底
3. 大量顧客データ抽出端末の集約化と特別監視
4. お客さま申込書など帳票類のペーパーレス化
5. 情報を取扱う場所への入退室管理

❹ 技術的セキュリティ

1. アクセス制御、アクセスログ保存と定期的調査
2. システム利用に対する生体認証の導入
3. 顧客情報検索条件の厳格化
4. 情報システム端末、通信路の暗号化
5. 不正持ち出し監視
6. サイバー攻撃対策、システム監視

Web 情報セキュリティポリシー

● 2020年度の主な取組み

情報管理については、「個人情報保護法」や各省庁等の定めるガイドライン等に則り、当社における情報管理規程・細則・マニュアル類を定めて、個人情報の取扱いも含め、厳格に運用（委託先、パートナーも含む）しています。

あわせて、「EU一般データ保護規制（GDPR）」、「改正割賦販売法（PCI-DSS）」等、情報セキュリティを取り巻く環境の変化に対応した取組みについても推進しています。

サイバー攻撃については、必要なセキュリティ対策を行うことができる専門組織を設置しており、攻撃の監視等や社内外との連絡対応を含め、インシデント対応発生時に備えています。2020年度は東京2020大会に向けて、サイバー攻撃を警戒した社内外の体制構築、および社内外のセキュリティ関連組織との連携体制を構築し、情報伝達訓練を実施しました。

2020年度の情報セキュリティ強化月間では、情報セキュリティ管理責任者（CISO）である副社長および情報セキュリティ部長からの注意喚起メッセージを発信したほか、経営幹部に向けて、サイバーセキュリティの最新動向についてセミナーを開催しました。また役職・社員区分に応じた情報セキュリティに関するeラーニングを年3回開講しました。毎年実施する標的型攻撃メール訓練については、訓練メールのバリエーションを増やし、警戒心を持続させる取組みを実施しました。

こうした取組みにより、情報セキュリティに関する知識を、年間を通じて社員一人ひとりに理解・浸透させるとともにルールを順守する意識の醸成を図ることでドコモグループ全体の情報セキュリティ強化に努めています。

データプライバシーの保護

● 個人情報保護方針と体制の整備

ドコモは、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考えています。

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、グループ全社にこの方針を適用することで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、ドコモグループで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けるお客さま情報の収集に際しては、電気通信事業の契約に必要な情報および利用目的を明示してお客さまに同意を得た範囲の情報のみを収集・保有しています。第三者への情報提供についても、必ずお客さまから同意を得た範囲の情報に限定しています。

また、EUの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たGDPRに関しては、2018年度に制定した「GDPR対応マニュアル」に続き、2019年4月にEU個人情報の取扱い等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。

2020年度、ドコモグループ内においては規制当局による指導や法令違反になる情報漏えい・苦情などはありませんでした。

個人情報の漏えいやデータの盗難・紛失の件数については、以下の表のとおりでした。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。

個人情報の漏えい・データの盗難・紛失件数

(件)

	2017年	2018年	2019年	2020年
件数	0	0	0	0

Web プライバシーポリシー

● 個人情報の管理と社員に対する教育・啓発

お客さま情報を管理するシステムは、使用できる社員を最小限とし、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、利用履歴のチェックも定期的に実施しています。さらに、情報を暗号化して管理することで、無断で持ち出されても意味をなさないものとしているなど、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安全性を確保しています。

そうした対策とともに、安全管理措置の実施その他の個人情報の適正な取扱いの確保のため、派遣社員を含むすべての社員・役員に年1回以上の研修と階層別のeラーニングを実施しています。

※ 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

● パーソナルデータに対する対応について

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。ドコモにおいても、「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て、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くことをめざしています。

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、法令を順守することはもちろん、お客さまのプライバシーを保護し、お客さまへの配慮を実践することも重要な使命と考えています。ドコモでは、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。

ドコモでは、「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。

● NTTドコモ パーソナルデータ憲章

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—

私たち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て、イノベーションの創出に挑戦し続けています。生活にかかわるあらゆるモノやコトをつないで、お客さまにとっての快適や感動を実現すること、そして社会が直面するさまざまな課題に対する新しい解決策を見出すことにより、国や地域、世代を超えたすべての人々が豊かで快適に生活できる未来を創ることが、私たちの考えるイノベーションです。安心・安全、健康、学び、そして暮らしの中のさまざまな楽しみまで、お客さま一人ひとりにとって最適な情報と一歩先の喜びを提供し、また、それらを実現するさまざまなビジネスの革新や社会課題の解決に向けた取組みを支えます。

私たちは、現状に満足することなく、社会との調和を図りながら、このような未来をお客さまとともに創っていきたいと考えています。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することをめざします。

一方で、私たちNTTドコモがお客さまの大切なパーソナルデータを活用させていただくにあたっては、法令を順守することはもちろん、お客さまのプライバシーを保護し、お客さまへの配慮を実践することも重要な使命です。パーソナルデータの活用について、不安や懸念を感じるお客さまもいらっしゃるかもしれません。しかしながら、私たちは、これまでと変わらずこれからも、お客さまに安心・安全を実感していただき、お客さまからの信頼にこたえ続けるという強い信念のもと、責任をもってパーソナルデータを取扱います。そして、これまで以上にお客さまとの“絆”を大切にし、お客さまのお声に真摯に耳を傾けながら、データの活用によりお客さまや社会にもたらすことができる新たな価値と、一人ひとりのお客さまにとって最適なプライバシー保護のあり方を考え続け、お客さまにお伝えし続けることこそが、最も重要であると考えています。

私たちは、「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、以下に掲げる行動原則を、企業活動のあらゆる場面において、お客さまのパーソナルデータを取扱う際の意思決定の基準とします。

● NTTドコモ パーソナルデータ憲章　6つの行動原則

行動原則

お客さまとのコミュニケーションを大切にし、透明性を確保します
- パーソナルデータをどのように取得・利用しているのかをお客さまにご理解いただけるように、透明性を確保します。
- パーソナルデータの取得・利用にあたっては、平易な表現、要約、映像などを用いたわかりやすい説明を通じてお客さまにご理解いただけるよう取組みます。
- お客さまが感じられた不安、疑問を解消し、ご安心いただくためのコミュニケーションの充実に努めます。

お客さまの利益や社会への貢献を考えます
- パーソナルデータの利用を通じて、お客さまや社会に新たな価値を提供します。
- パーソナルデータの利用に際しては、お客さまの利益になるか、社会への貢献につながるかを意識し、お客さまの信頼を損なうような利用は行いません。
- パーソナルデータの取得・利用は、お客さまのお気持ちに配慮し、適切かつ適法な方法により実施します。

お客さま一人ひとりの意思を尊重します
- パーソナルデータの利用に対する感じ方は、お客さまによっても異なることを踏まえ、利用するパーソナルデータの性質や利用態様などに応じて、パーソナルデータの利用についてお客さまご自身により選択いただける手段（オプトアウト手段など）を提供します。
- 選択手段は、簡便かつわかりやすいものとなるよう努めます。

パートナーとの連携にあたってもお客さまのプライバシーに配慮します
- お客さまや社会に新たな価値を提供するためのパートナーとの連携によるオープンイノベーションの取組みなどにおいて、パーソナルデータやこれを匿名化・統計化した情報をパートナーに提供する場合、法令を順守するだけでなく、お客さまのプライバシーにも配慮します。
- パートナーへの情報の提供にあたっては、提供する情報の性質などに応じて、提供先の信頼性を確認する、提供先による情報の利用・提供を制限するなど、適切な方法により実施します。

適切なセキュリティ対策により、お客さまのパーソナルデータを保護します
- お客さまの大切な情報を、漏えいや盗難、改ざんなどの事故を防止するために適切な組織的・人的・物理的・技術的手段を用いて保護します。
- 定期的に情報セキュリティに関する評価を実施し、セキュリティリスクの軽減策を講じます。

お客さまのプライバシー保護のための体制を整備し、運用します
- プライバシー・バイ・デザインの思想をもとに、新たな商品やサービスを開発する際には、お客さまのプライバシーに配慮して開発します。
- プライバシーへの配慮を徹底するため、お客さまのパーソナルデータを取扱う者に対する社内での研修など教育・啓発および情報共有を継続して実施します。
- プライバシーへの影響を評価する専門的な諮問機関を社内に設置するなど、パーソナルデータの利用に伴うお客さまのプライバシーへの影響を評価する仕組みを整備し、運用します。

※ 行動原則の内容およびその運用については、お客さまの信頼にこたえ続けるために、継続的に検証し、適宜見直しを行うこととします。

Web NTTドコモ パーソナルデータ憲章

ステークホルダーの対応

標的型攻撃と呼ばれるマルウェアによる内部侵入や、インターネットを介した不正アクセスの発生など、情報セキュリティに対する脅威は年々高まっています。ドコモではスマートライフ事業の拡大の柱の一つとして+dによる社会課題解決に向けた他産業との協働を進めており、+dのパートナー企業との顧客情報の共有が増加する中で、パートナー企業に対するサイバー攻撃もドコモの情報セキュリティリスクとなり得ます。高度化、深刻化する情報セキュリティに対してドコモでは高度な情報セキュリティ体制の構築とともに、サイバー攻撃を想定した訓練や、情報セキュリティ教育の実施など情報セキュリティのさらなる強化を行っています。

また、個人情報を含むデータプライバシーの取扱いは時代とともに、より複雑性を増しています。2018年5月に施行されたGDPRについては、対応マニュアルの策定や研修の実施、プライバシー影響評価の実施等の具体的施策を展開しています。2019年12月には、パーソナルデータ憲章に掲げる行動原則に基づき、「NTTドコモ プライバシーポリシー」を再編し、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・表現にあらためました。これらの取組みについて、イラストなどを用いてわかりやすく解説する「知ってナットク！ドコモのパーソナルデータ活用」も公開しています。

また、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いただいた内容を確認したり、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Webサイト上で提供しています。ドコモでは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。

● ドコモショップや業務委託先におけるセキュリティ管理

ドコモショップに対しては、情報セキュリティに特化した研修を年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」を発行して啓発活動を支援しています。また、販売現場が最も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3か月に1回の業務監査を実施するなど徹底した監査で情報管理が適切になされているかを確認しています。業務委託先に関しても、個人情報を適正に取扱うと認められるものを選定し、委託契約において、安全管理措置、秘密保持、再委託の条件そのほかの個人情報の取扱いに関する事項について適正に定め、必要かつ適切な監督を実施しています。

● +dパートナーにおけるセキュリティ管理

+dのパートナー企業に対しては、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。また個人情報をパートナー企業と共有する場合は、お客さまの同意を取得した上で提供するなど、個人情報保護に取り組んでいます。

「ドコモ口座」を利用した不正利用について

2020年9月、ドコモが展開する「ドコモ口座®」を通じて金融機関から預貯金が不正に引き出される問題が発生しました。ドコモはこれまで不正アクセスに対する二段階認証やアカウントロックなど、さまざまなセキュリティ対策を講じてきましたが、問題を受けeKYC（オンライン本人確認システム）や「dアカウント®」の連絡先携帯電話番号登録、専門スタッフによる24時間365日監視体制などを導入しました。加えて金融サービス関連のリスク管理専門部署や問い合わせ専用電話窓口を新設することで安心・安全にサービスをご利用いただける体制を整えました。併せて補償制度に関する新たな規約を制定し、不正被害の補償について明確化しました。万が一ドコモ口座に関連する被害が生じた場合は被害額を全額補償します。今後はこれまで以上に徹底したセキュリティ対策のもと、お客さまの信頼回復に努めます。