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コムウェアグループは、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、情報セキュリティソリューション「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。

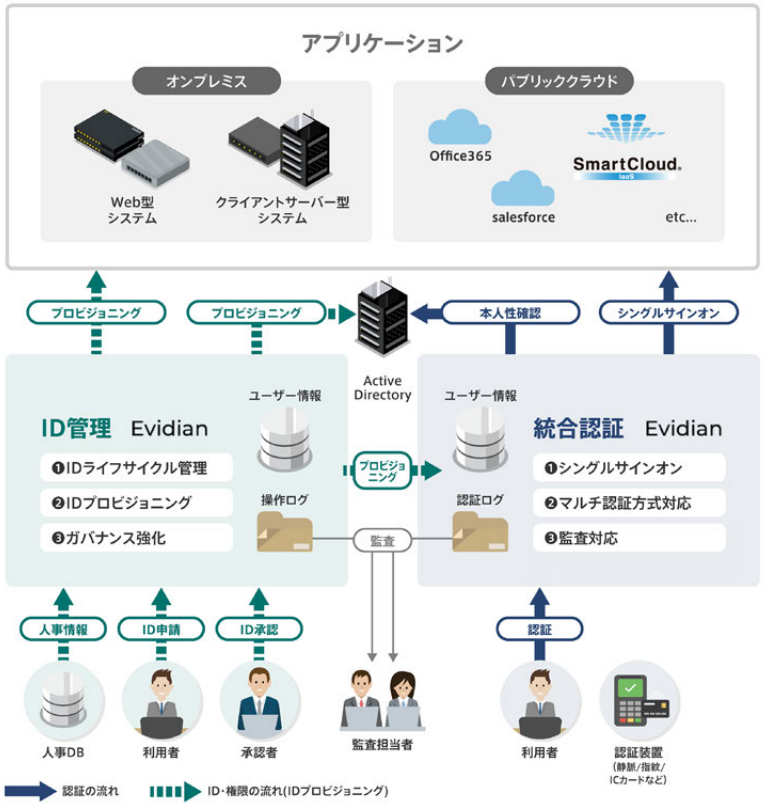
インパクト

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



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、世界各地において高頻度で続く自然災害や、地球温暖化などを要因とする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。

これらの社会の潮流を踏まえ、NTTコムウェアグループは、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、ネットワーク技術の進化にともない発生し続け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開発・展開しています。これらの取り組みは、ビジネスならびに一般の皆さまが日常的に利用される各種通信・クラウドサービスを提供するドコモグループの一員となった現在、一層重要度を増しています。

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

2023年度　総括

●2023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(KPI)	2023年度目標	2023年度実績
●社会インフラ品質の向上	社会インフラへの影響を加味した品質定義の改訂検討	品質定義の確立	品質定義を確立
	重大故障発生件数 (総務省が規定する、電気通信役務の「重大な事故」に該当する重大故障を対象とする)	0件	0件
●堅牢なセキュリティ環境	開発・保守職域におけるセキュリティ課題解決によるリモートワーク導入状況のモデル運用を通じた評価方法の検討	評価方法の確立	検討を実施*
	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

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、重大故障発生件数に加え、社会インフラへの影響を加味した品質定義の改訂をKPIに定め、通信サービスの安定性と信頼性の確保を図りつつ、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、2023年度よりサイバー攻撃にともなう重大なインシデント発生件数に加えリモートワーク導入への評価手法開発もKPIに定め、時代に即した防衛・有事対応体制を強化しつつあります。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ます。

＊ 詳細な検討経過はP.29「開発・保守職域におけるリモートワーク導入に向けた、セキュリティ課題の把握」を参照ください

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コムウェアグループ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コムウェアは、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コムウェアは、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コムウェア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コムウェア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。
- 標準的な開発手順の理解度向上と浸透を目的としたWBT（Web-Based Training：インターネットやイントラネットを使用した学習システム）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コムウェアは、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コムウェア品質方針

NTTコムウェアは、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コムウェアは、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コムウェアは、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コムウェア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コムウェアは、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。2023年度も大きな施策強化を実施しました。

具体的には、従来は「社会・顧客への影響度」を考慮しつつ「故障の影響範囲、影響時間、発生原因」などの定量情報に重点を置いた評価方法でしたが、「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故障の評価方法に改善しました。

さらに著しく影響度の大きい重大故障の管理を目的に2024年度から「S級重大故障」を新設し、KPIとして「年間0件」を目標に設定することとしました。2023年度はS級重大故障に該当する故障は0件であり、さらなる品質向上に努めてまいります。

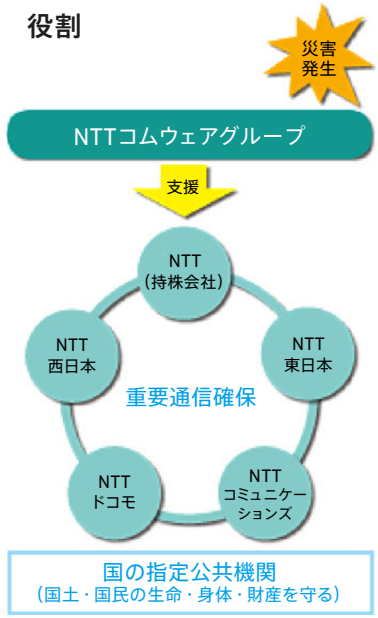
災害対策の取り組み

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。

その中でNTTコムウェアグループは、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体制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コムウェアグループの 役割



災害発生に備える体制

NTTコムウェアでは、統合監視センター「FSC24®(Field Service Cockpit 24)*」により、24時間365日、通信システムを一元的に監視・保守する体制を構築し、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で災害発生時をはじめ、近年の大規模災害・障害対応でも同センターが司令塔となった復旧支援活動でも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。東日本大震災の発生直後には、「FSC24®」の速やかな初期体制構築により、災害対策本部ほか関連組織へ的確な情報配信を行うことができました。

●FSC24®の監視コックピット

＊「FSC24®(Field Service Cockpit 24)」は、NTTコムウェア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「オフィサ」と呼ばれる技術者を配置しています。オフィサは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が、万が一被災した場合に備えて、西日本の拠点に代替センターを用意しています。NTTコムウェアは、「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。

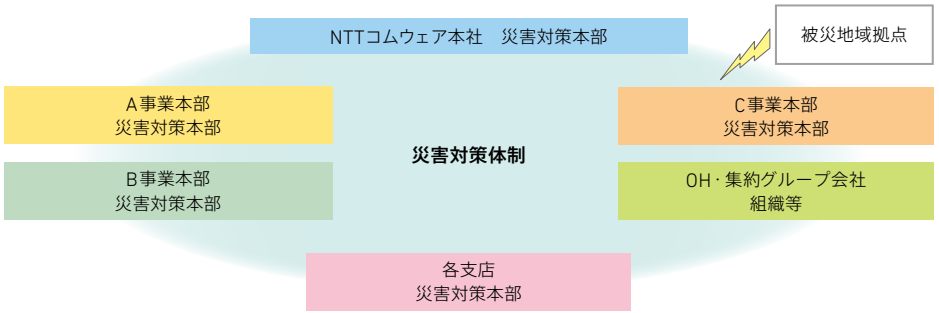
災害発生に備えた具体的な取り組み

災害対策訓練の実施

NTTコムウェアグループでは、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。とくに昨今では東日本大震災の経験を踏まえNTTコムウェア各組織(ロケーション)ごとの災害対策体制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



●2023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
コムウェア災害対策訓練	2024年2月

2023年度の災害対策訓練は、2023年度訓練直前に発生した「能登半島地震(2024年1月1日発生)」の復旧対応を行いつつ、最適化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コムウェア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。東日本大震災の発生時も、NTTコムウェアのデータセンターは運転を継続しました。

非常災害時における対応

NTTコムウェアでは、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たところですが、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。

2023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きた中、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改善や自動連絡ツール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「情報伝達訓練（年一回）」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。

- **大規模災害対応の教訓の活用および連絡体制強化に向けた議論**

  2024年1月1日に発生した能登半島地震の影響を踏まえた対応の振り返りおよびNTTドコモ、NTTコミュニケーションズとの災害時における社員安否確認等の連携体制強化に向けた議論を開始しました。

- **社員安否システムの統一**

  2022年7月のドコモ・システムズ株式会社との統合後、社内で2つの社員安否システムを運用していましたが、2023年12月に統一を図り、一元管理による効率的な社員安否確認およびガバナンス強化を実現しました。

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。

情報セキュリティ

NTTコムウェアは、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コムウェアは、情報セキュリティ活動(個人情報保護を含む)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、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。

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コムウェアでは毎年、社員等および協業者を対象に、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、以下の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。

さらに2023年度は、NTTグループにおける個人情報漏えいを受け、全社をあげての緊急点検、および全社員に対するセキュリティ研修、セキュリティセミナーなどを通じて、基本動作の徹底を改めて啓発しました。

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コムウェアでは「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、とく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コムウェア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、および社員・協力会社社員ともに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開始しています。

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コムウェアの開発システムやサービスをご利用いただけるように、CW-PSIRT（コムウェア・ピーサート）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、2025年日本国際博覧会を見据え、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コムウェアではCW-CSIRT（コムウェア・シーサート）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。

サイバー攻撃にともなう重大なインシデントの抑制

NTTコムウェアでは、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、コーポレート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。

2023年度、サイバー攻撃は複数件観測されましたが、いずれも初動対応で被害を抑制し、重大なセキュリティインシデントに至る事例はありませんでした。

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、セキュリティ課題の把握

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、重要なテーマといえます。この観点に立ち、NTTコムウェアは、同職域のリモートワーク拡大に向けての技術的ならびにセキュリティ上の課題の把握を進めています。調査の結果、目標としていたリモートワークの導入率や状況把握については、現時点では手段を十分講じていることからKGIに基づく目標管理からいったん取り下げました。

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コムウェアでは、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ています。

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する「セキュリティ診断サービス」、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する「サイバー保険付き脆弱性診断サービス」、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する「クラウドWAFオペレーションサービス」、インターネットの入口・出口対策とリアルタイム監視・保護を行う「s-WorkProtector」、ユーザがどこにいても安心・安全なテレワーク環境を提供する「ゼロトラスト型セキュリティサービス」、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する「SmartCloud® IAMソリューション」など、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。

NTTコムウェアグループにおけるISMS認証・プライバシーマーク取得状況

NTTコムウェアグループは、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。

さらに先述の「個人情報保護方針」に基づく、個人情報保護活動を推進しています。

●NTTコムウェアグループのISMS、プライバシーマーク認証取得状況

NTTコムウェアグループ会社	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コムウェア株式会社	JUSE-IR-006	2026.6.21	11820039(13)	2025.5.10
NTTインターネット株式会社	JQA-IM0034	2025.11.30	21000009(10)	2025.4.26
ドコモ・データコム株式会社	JQA-IM0218	2026.3.3	11820328(10)	2025.4.6

●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

NTTコムウェアにおける個人情報の取り扱いの詳細については、こちらをご覧ください。
http://www.nttcom.co.jp/privacypolicy/