安心・安全

私たちのアプローチ

すべての人が安心・安全に暮らせる、ICTに守られた社会へ

NTTコムウェアのありたい姿

今日も、明日も、見守り、支える

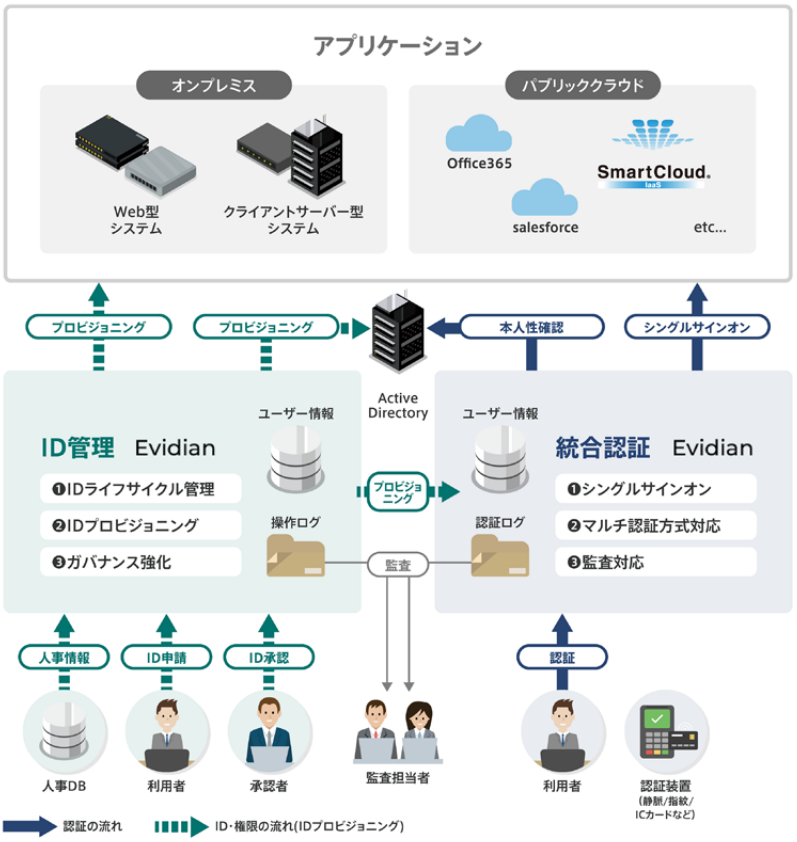
ICT技術の進化にともない、経済性にとどまらず、「安心・安全」を実現するための責任も増しています。NTTコムウェアグループは、情報インフラを提供するNTTグループの一員として、その円滑な運用・保守を実現する品質維持・事業継続体制を整備し続けます。また、日々生まれる新たなセキュリティリスクに対しても信頼性の高い技術を積極的に取り入れ、AIの適切な利用にも留意し、社会に責任を果たします。

アクションハイライト：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。

●統合された、柔軟かつ強固なID管理・統合認証の仕組み



主に貢献するSDGs

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。引き続き、「安心・安全なICTサービス」を徹底することで、お客さまはもちろん、社会の皆さまの信頼を得られるよう、日々、取り組んでいきます。

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

2022年度　成果の総括

●2022年度の主な成果

マテリアリティ	2022年度サステナビリティ定量指標(KPI)	2022年度目標	実績
社会インフラ品質の向上	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	サイバー攻撃を起因とした意図しないサービス停止の件数	0件	0件
	重大な個人データ流出ゼロ(個人情報の漏えい件数)	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。

具体的には「社会インフラ品質の向上」では、「重大故障発生件数」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、災害発生時の対応のさらなる強化をめざし、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、個人情報の漏えいゼロという継続的な目標に加え、サイバー攻撃を起因とした意図しないサービス停止件数も新たにKPIに定め、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。

社会インフラ品質の向上

システムの「品質」と「信頼性」は、NTTコムウェアグループが最も重視している価値です。
システムをつくり上げるための「ソフトウェア」、システムを安定してご提供するための「サービス業務」について、とも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、全社に展開するとともに、2007年にはITサービス業務に特有なISO20000の認証も取得して、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	ITサービス業務
登録番号	JQA-1997	JQA-IT0044
取得日	1997/11/28	2007/1/10
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	情報・通信システム(①)、データセンターサービス(②)の運用・保守およびそれに付随する戦略立案、企画、設計・構築のサービス事業に関わるITサービスマネジメントシステム 【関連事業所】 ▶ ネットワーククラウド事業本部プラットフォームサービス部 MPS−BU Assurance Platform担当(一般、NTTグループ) MPS−BU Service Integration and Management 担当(一般) 〔活動範囲:❶〕 ▶ 地域事業本部 北海道支店 BS部門　サービス担当 (ハウジングサービス・ホスティングサービス) 〔活動範囲:❷〕

ITサービス業務の品質向上

NTTコムウェアは、IT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IT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。

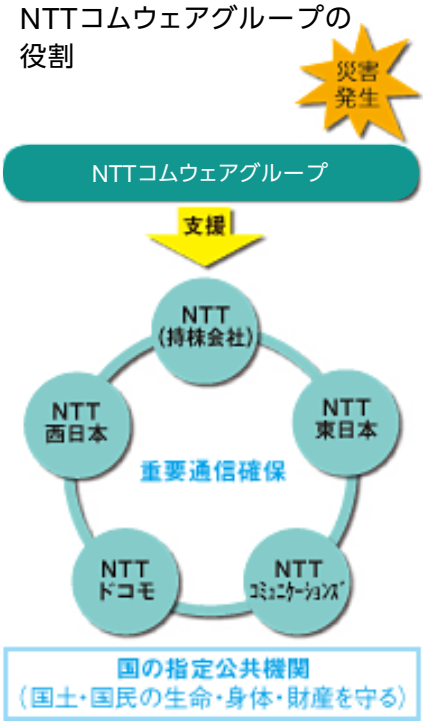
災害対策の取り組み

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

●FSC24®の監視コックピット

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®(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。

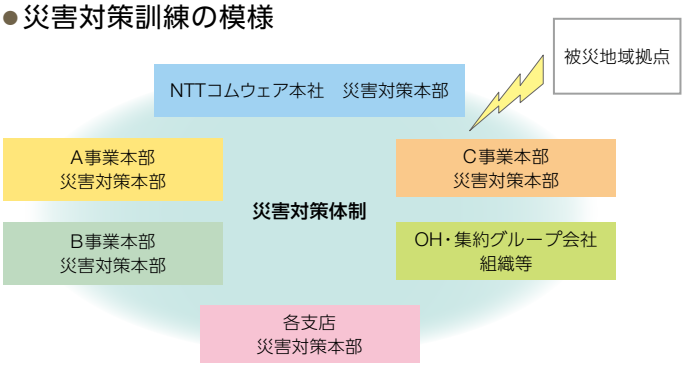
災害発生に備えた具体的な取り組み

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



●2022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	2023年2月

2022年度の災害対策訓練は、切迫性が指摘され広範囲で大規模の被災を受ける南海トラフ地震を想定し、西日本エリア被災時にリモートツールなどを活用した初期態勢の構築と、本社・支店間の情報連携方法、災害対策本部のスムースな態勢変更の確認などに取り組みました。

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。

2022年度は、新たな働き方への適応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

  リモートワークや休日などで社員が出勤していない状況を考慮した、ロケーションフリーによる災害対策訓練を実施することで、勤務状況に応じた災害時の基本行動の定着を図りました。
- 自然災害への早期対応

  豪雨・台風など被害等が予測される災害の情報収集を行い社員へ展開を図ることで、人的被害の抑止に向けた早期行動を促しました。また、最大震度5強以上の地震等発生時には、迅速に社員・家族の安否確認などを実施し、的確な対応をとることができました。
- 社員安否システムの更改

  アプリでの即時通知による早期安否登録やUI向上による誤投入防止などを狙い、老朽化した社員安否システムを最新のクラウドサービスである新システムへ2022年5月に切り替えました。

  システム切り替え前後の新システムを利用した社員安否登録訓練の実施、新システムの内容に最新化した携帯用サイズの行動マニュアルを配布することで、利用の習熟・定着を図り、円滑な運用につなげることができました。

堅牢なセキュリティ環境

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、適切なセキュリティ管理を実践し、安全な情報流通基盤を築く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、「個人情報保護方針」「情報セキュリティポリシー」を制定し、それに基づく仕組み「情報セキュリティマネジメントシステム(ISMS)」を確立させ、「プライバシーマーク」および「ISMS認証」を取得しています。また、毎年全従業員に「自覚研修」を行い、社員一人ひとりのセキュリティ意識を高め、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。今後とも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、取締役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、全組織の実効的な情報セキュリティ、個人情報保護活動を推進するため、「セキュリティガバナンスオフィス」を設置し、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、全従業員(正社員および協働者)を対象に、WBTを活用した情報セキュリティ研修(「自覚研修」)を実施しています。WBTには、セキュリティに関する最新の話題をトピックスとして盛り込み、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、以下のセキュリティ研修施策を実施しました。

- 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。

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冊子の作成、セキュリティ事件や事故事例などの周知を通じた注意喚起など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

電子メール利用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を導入調整し、運用を開始しています。

さらに、標的型攻撃対策として、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など、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、監視運用を開始しています。

また、近年、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、または万一つくり込んでしまった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。

また、2021年に延期された東京2020大会は、開催中にサイバー被害を受けることなく終了しましたが、未だ世界的に深刻視されているサイバー脅威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、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。

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、お客さまの要求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、ゼロトラスト・セキュリティモデルの実現をめざしていきます。

プライバシーマーク・ISMS認証取得状況

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行うため、「プライバシーマーク」と「ISMS」の認証をグループ会社で取得しています。

●NTTコムウェアグループのプライバシーマーク、ISMS認証取得状況

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

●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

なお、当社では「個人情報保護方針」を制定し、これに従い個人情報（個人番号および特定個人情報を含む）の重要性を認識し全社において個人情報保護活動を推進しています。

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/