安心・安全なコミュニケーション

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

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、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ー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。これらを通じ「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、取り組んでいます。

SDGsとの関わり

社会のすべての人が、安心して先進的な生活環境の恩恵を受ける仕組みをつくること。これは、最先端のICTでインフラを支えるNTTコムウェアグループの事業特性が活きるテーマです。国連SDGsの目標11「住み続けられるまちづくりを」を踏まえつつ、安定的で信頼性の高いサービス、そして自社のセキュリティーの両面から取り組みを推進します。

SDG11に貢献しうる、私たちの取り組みの例

- 堅牢性、セキュリティーに優れたデータセンターサービス
- 都市防災計画へ貢献するソリューション
- 公共や企業ネットワークのセキュリティー、保守サービス
- 自社のBCP、セキュリティーの徹底

2020年度　成果のハイライト

●2020年度の主な成果

重点活動項目	CSR定量指標（KPI）	2020年度目標	実 績
個人情報保護	●個人情報の漏えい件数	0件	0件
情報セキュリティーの強化	★セキュリティー人材の確保	実績把握	上級：1人 中級：311人 初級：5,942人
通信サービスの安定性と信頼性の確保	★コムウェア災害対策訓練の実施	1回	1回

●＝NTTグループCSR重点活動項目と同一
★＝コムウェア独自のCSR重点活動目標

2017年度より開始した新・重点活動項目に即し、2020年度も、「個人情報保護」「情報セキュリティーの強化」「通信サービスの安定性と信頼性の確保」それぞれの領域で具体的な目標に即したPDCAの徹底および各種施策の強化を継続しました。

具体的には、「個人情報保護」では、個人情報の漏えいゼロの継続を目標に定め、各種認証の継続的取得など個人情報保護体制の継続的強化や社員への情報管理意識の啓発により情報漏えいの防止を徹底しました。一方「情報セキュリティーの強化」ではNTTグループが推進する「セキュリティー人材」の育成へと引き続き積極的に取り組み、昨年度以上の成果を挙げています。また「通信サービスの安定性と信頼性の確保」に向けた取り組みとしては、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。なお新型コロナウイルス（COVID-19）の国内感染拡大および緊急事態宣言発出にともなう事業継続施策に関しては、CSRマネジメント章に記載しましたのであわせてご覧ください。

災害対策

早期発見・早期復旧を可能にする体制を整備
NTTグループの通信システムを一元的に監視する体制を核に、通信サービスの安定的な提供に向けた徹底的な取り組みを行っています。

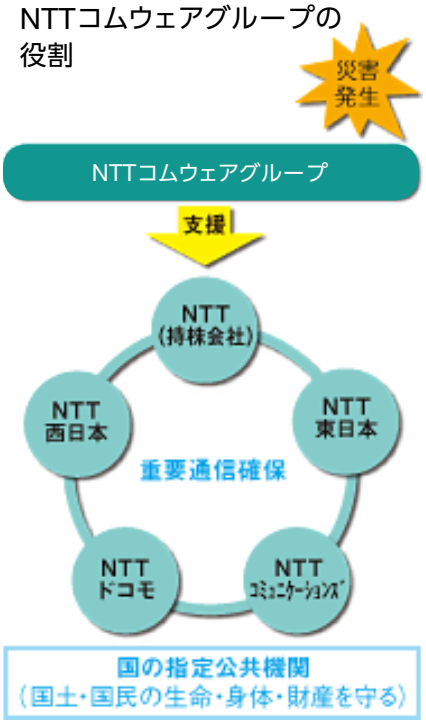
災害対策の取り組み

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、災害発生時においても迅速な対応を行っています。

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程度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。

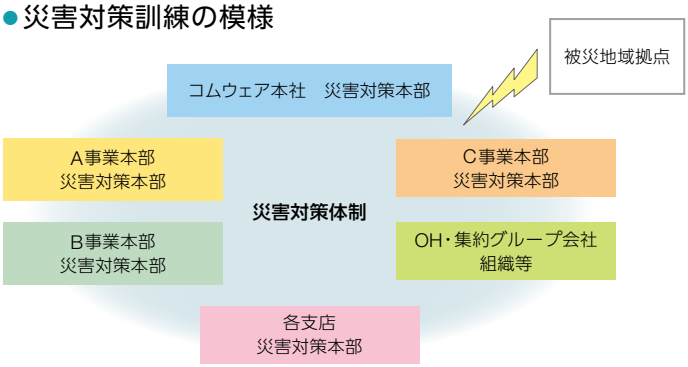
災害発生に備えた具体的な取り組み

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



●2020年度の主な災害対策訓練実施状況

災害対策訓練	実施時期
コムウェア災害対策訓練	2020年11月

2019年度に引き続き、地域エリアにおける災害発生時の迅速な体制確立と大規模停電等を想定したBCP(事業継続計画)の検証に取り組みました。

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。

2020年度は、新たな働き方への適応や社員の安全を確保するために直近の災害状況や過去の災害時の対応を踏まえた以下の取り組みを実施しました。

- 災害シミュレーションの拡大
  リモートワークのさらなる推進や休日等で社員が出勤していない状況においても、ロケーションフリーによる対応を想定した訓練を実施することで、自宅等から柔軟に基本動作が守れる訓練を実施しました。
- 自然災害への早期対応
  発生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、九州地方集中豪雨をはじめ自然災害発生時には、迅速に社員・家族の安否確認等を実施し、的確な対応をすることができました。
- 円滑な情報連携網の整備
  ロケーションフリーの実現には、複数の情報連絡網を用いることが必要であり、社内コミュニケーションツールを積極的に活用した情報連絡手段の検討を行うとともに、他情報連絡班との輻輳を回避した円滑な連絡網の整備を図りました。

情報セキュリティーの確保と個人情報の保護

体系的な情報セキュリティー対策を着実に推進

情報セキュリティー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。

情報セキュリティー推進体制

NTTコムウェアは、情報セキュリティー活動(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情報セキュリティー活動全般の戦略的計画の決定、②セキュリティー基本方針の制改定の審議、③セキュリティー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ー、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連絡会」を設置し、情報セキュリティー活動を展開しています。

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ーの重要性を認識し、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	有効期間	登録番号	有効期間
NTTコムウェア 株式会社	11820039 (12)	2021.5.11-2023.5.10	JUSE-IR-006	2023/6/21 (R5)
NTTインターネット 株式会社	21000009 (09)	2021.4.27-2023.4.26	JQA-IM0034	2022.11.30 (R4)
コムウェア・ファイナンシャル・システムズ株式会社*	17000980 (05)	2020.1.11-2022.1.10	—	—

＊ISMS認証は取得していません

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。

●情報セキュリティー認証類の取得歴

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	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 5月	NTTコムウェア「ISMS」更新(JUSE-IR-006)
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
2015年 5月	NTTコムウェア「プライバシーマーク」更新
2015年 6月	新規格対応「ISMS」定期兼移行(JUSE-IR-006)

情報セキュリティーの教育・啓発

情報セキュリティー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(Web Based Training)を活用した情報セキュリティー研修(「自覚研修」)を実施しています。WBTには、セキュリティー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ーに関する意識を啓発しています。これらの結果、NTTグループ内の認定制度において、セキュリティー人材と認定された人数は、上級レベル1名、中級レベル311名、初級レベル5,942名となっています。

また、各階層におけるセキュリティー活動の意識向上、レベルアップを目的として、以下のセキュリティー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、セキュリティーの重要性を認識する機会としてセキュリティー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ー活動の持つ意味と重要性を認識し、セキュリティー活動上の役割および責任について意識向上するため、セキュリティー講話を実施しています。

その他、「情報セキュリティーポリシー」「個人情報保護方針」を浸透させるためのポスターの掲示や社員向け冊子の作成、セキュリティー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ー対策の構築・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FW・迷惑メールフィルタリングなどに加え、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ー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、脆弱性を作り込まない、または万一作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ー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大会開催中に懸念され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ー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。

情報セキュリティー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ーサービス・ソリューションを幅広く提供しています。

現場の対策状況を見える化し、セキュリティールールの見直しや現場浸透のPDCAサイクル策定を支援するセキュリティーガバナンスサポート(コンサルティング)、NTTグループの通信インフラや基幹システムの構築・運用で培ったノウハウに基づき、エンタープライズレベルの要求に応えるセキュリティー対策を実現する「SmartCloud*」セキュリティーソリューション、セキュリティー専門家が監視・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、IT資産情報や脆弱性に関する情報をリアルタイムで見える化する「SmartPIER*」など、コンサルティングから開発構築、維持管理、監視運用までを含めトータルにセキュリティーサービス・ソリューションを提供しています。

*「SmartCloud」「SmartPIER」は、NTTコムウェア株式会社の登録商標です。