

Trusted Value Chain

セキュリティやデータプライバシーを守り、安心安全でレジリエントな企業活動を実現する

企業活動がグローバルに拡大する中、情報セキュリティや災害、コンプライアンス等の企業活動で生じるリスクも多様化しています。当社はそうしたリスクをバリューチェーン全体で正しく捉え、管理し、適切に対応することで、信頼できるバリューチェーンを構築し、安心安全でレジリエントな企業活動を実現します。

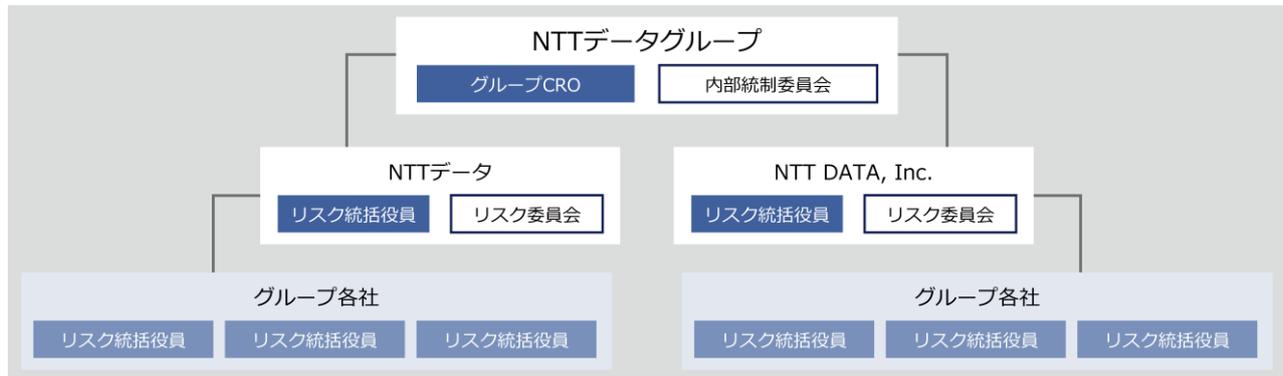
強靱なリスクガバナンスの推進

◆ 基本方針と推進体制

当社は、グループ全体の健全な成長、リスクの経営への影響の抑制・低減を図るため、グループ全体としてめざすべきリスクマネジメントのあり方を体系化し、グローバルレベルで標準的に対応すべき事項を定めたリスクマネジメントポリシーを制定しています。これに基づきグループのリスクマネジメントを統括・推進する役員及びリスクマネジメント部門を置くとともに、主要なグループ会社にリスクマネジメントを統括する役員を選任し、グループで連携してリスクマネジメント体制を整備しています。

なお、グループにおけるリスクマネジメントに係る体制として、危機発生時をはじめ、グループ経営に重大な影響を及ぼす事項についてはグループ会社から当社に迅速に報告する体制を整備し、リスク発生時の迅速な対応を行っています。

▶ リスクマネジメント体制



◆ 重要なリスクへの対応

重要リスクの選定とリスク統制

当社の事業計画の達成、存立基盤に重大な影響を与える可能性のあるリスクを「重要リスク」として取締役会において選定し、更に「重要リスク」のうち、平時の統制に加え迅速な有事対応を必要とするリスクについては「特に重要なリスク」と定義しています。

各「重要リスク」については、グループ全体として重点的な統制活動を推進し、内部統制委員会において、その統制状況について定期的なモニタリングやその有効性の確認、改善事項の提言等を実施するとともに、その他リスクマネジメントの浸透・徹底に必要な事項の審議・決定を行っています。

また、グループ全体としての「重要リスク」の統制に加え、各事業会社や海外統括会社においても、それぞれの事業特性に応じた「重要リスク」を選定し、その統制やモニタリングを行っています。グループ全体としてのリスク統制活動と、各事業会社・海外統括会社でのリスク統制活動は、各社のリスクマネジメント統括役員間の連携体制の下で相互連携しながら実施しており、これらの活動全体を内部統制委員会でモニタリングすることで、グループ一體的なリスクマネジメント活動の推進を図っています。

2023年度 重要リスク

当社では、2023年度の重要リスクとして以下の(1)から(16)のリスクを選定しています。このうち、(1)から(8)を平時の統制に加え、迅速な有事対応を必要とするリスクである「特に重要なリスク」として定め、有事発生時の対応を含め、特に重点的に統制活動を行っています。

区分		リスク
重要リスク 当社グループの事業計画の達成、存立基盤に重大な影響を与えるリスク	特に重要なリスク 平時の統制に加え、迅速な有事対応を必要とするリスク	(1) システム開発リスク
		(2) 出資・M&A・設備投資に関するリスク
		(3) 情報セキュリティに関するリスク
		(4) コンプライアンスに関するリスク
		(5) システム・サービス運用リスク
		(6) 大規模災害や重大な伝染病等に関するリスク
		(7) 人権対応に関するリスク
		(8) 地政学に関するリスク
		(9) 気候変動に関するリスク
		(10) 人財確保に関するリスク
		(11) 技術革新に関するリスク
		(12) 知的財産権に関するリスク
		(13) 競争激化に関するリスク
		(14) 規制対応に関するリスク
		(15) 為替・金利の変動やインフレーションの進行に関するリスク
		(16) 親会社の影響力

2023年度重要リスクに関する詳細は有価証券報告書をご参照ください。

<https://www.nttdata.com/global/ja/investors/library/asr/>

◆ リスクマネジメント教育

当社では、グループ全体でリスクマネジメントの徹底を図るため、当社及びグループ会社の新任取締役(監査等委員を含む)、新任監査役を対象として法的役割等に関する研修を継続的に実施しています。

2022年度は、8月に国内グループ会社の新任取締役・新任監査役向けの研修を実施しました。今後も各種研修を継続的に実施することで、リスクマネジメントへの意識向上や対応能力の強化を推進していきます。

情報セキュリティの徹底/データプライバシーの保護

当社は、「情報の安全性の確保」と「情報の積極的な活用・共有」を適正なバランスで両立させることが重要と考え、ルール策定や情報セキュリティ教育・啓発活動等の「管理的対策」、情報漏えい対策ソリューションやゼロトラストアーキテクチャの導入といった「技術的対策」の両軸から、様々な対策を実施しています。

また、グループ全体で知識・ノウハウを共有するために、国内グループ会社とは情報セキュリティ推進者フォーラム、NTT DATA, Inc.及び海外グループ会社とは Global CISO Conference 等を通じてグループ内のナレッジの流通を促進し、グループ一体となった情報セキュリティガバナンスの確立に取り組んでいます。

◆ 基本方針

当社は、「NTT データグループセキュリティポリシー（GSP）」をはじめとする規程類を制定し、情報漏えいや情報の不正利用等の深刻なセキュリティ侵害から情報資産を守る行動基準、情報の積極的な活用・共有を図る行動基準を定めています。個人情報保護（データプライバシーの保護）についても各社のプライバシーポリシー（個人情報保護方針）等のガイドラインを定め、そのルールにしたがって適切に取り扱うことを求めており、当社全体で個人情報は適切に保護されます。これらの行動基準には、業務を委託するパートナー企業も範囲に含め、情報資産の適切な取り扱いを実現しています。

また、国内グループ会社には、改正個人情報保護法等に対応する「NTT データグループ日本地域個人情報保護規程（JPP）」、「NTT データグループ日本地域個人情報管理方法ガイドライン（JPG）」を制定し、適切に個人情報を取り扱うために遵守すべき項目と実践するための手順を定めています。さらに、「EU一般データ保護規則（GDPR : General Data Protection Regulation）」が適用される個人データを扱う場合には、GDPR に基づき通知が求められる事項を文書化するなど、GDPR の遵守を国内グループ会社に求めています。

◆ 推進体制

グローバルガバナンス

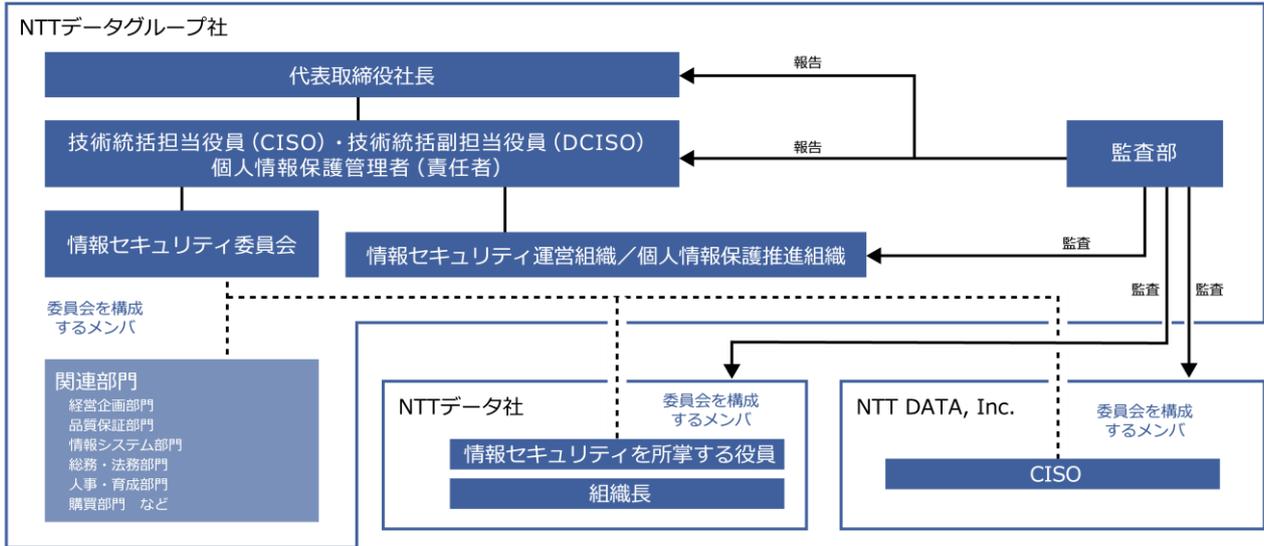
当社では、2006 年度から NTT データグループセキュリティポリシー（GSP）に基づく情報セキュリティの徹底を図っています。当社の海外拠点に対しても GSP を適用しており、2012 年度からは 5 つの地域（北米（NDS）、EMEAL 地域（EMEAL）、APAC 地域（NDAP）、Business Solutions、NTT Ltd.、2023 年度 10 月時点）の統括会社を軸とした情報セキュリティ推進体制を構築し、ベースラインの統一と地域別の柔軟性を両立した運営を行っています。

グローバルセキュリティを支える連携

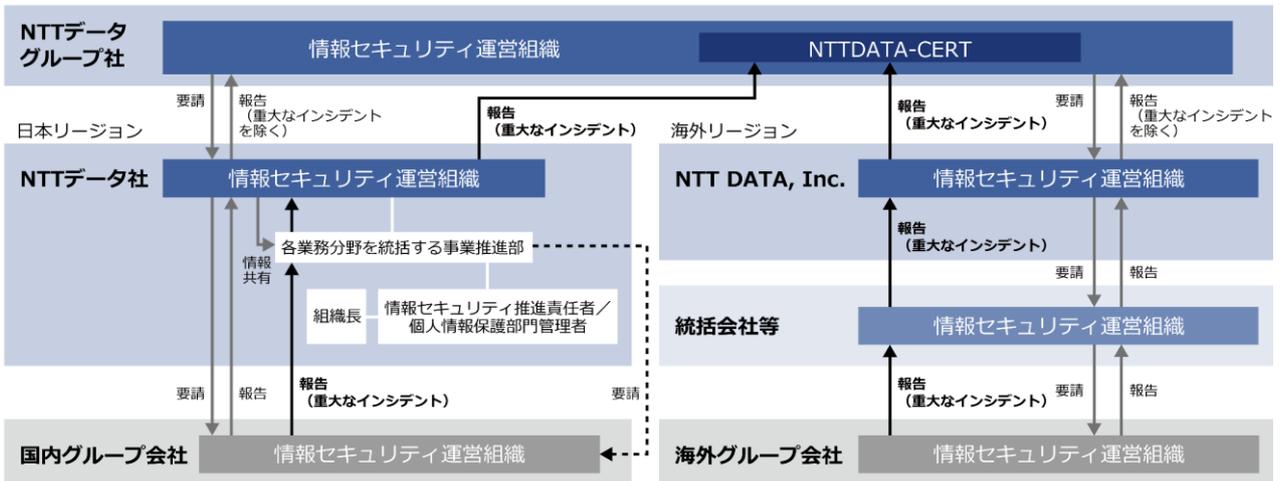
情報セキュリティのグローバルガバナンスを徹底するために、NTT データグループ社、NTT データ社、NTT DATA, Inc.、統括会社等、各グループ会社に配置される情報セキュリティ運営組織の階層からなる情報セキュリティガバナンス体制を整えています。

各層の情報セキュリティ運営組織は、情報セキュリティポリシーの維持・整備、施策のモニタリング、インシデント防止のための予防措置活動及び緊急時の司令塔の役割を担い、緊密に連携を図っています。

➤ NTT DATA グループ全体のセキュリティガバナンス体制



➤ NTT DATA グループ全体のセキュリティマネジメント体制



➤ NTT データグループ社の情報セキュリティガバナンスにおける役割

技術総括担当役員・ 技術総括副担当役員	<p>情報セキュリティマネジメントを推進する役員により、グループ全体の視点で情報セキュリティガバナンスを確立する</p> <p>※技術総括担当役員は、技術開発・研究 (CTO)、品質保証、及びセキュリティ (CISO) を総括する分掌です。</p> <p>※技術総括副担当役員は、技術開発・研究 (DCTO)、品質保証、及びセキュリティ (DCISO) を総括する分掌です。</p>
個人情報保護管理者 (責任者)	<p>個人情報保護マネジメントシステムの計画及び運用に関する責任と権限を有する役員により、グループ全体の視点で、個人情報の取り組みを指揮する</p>

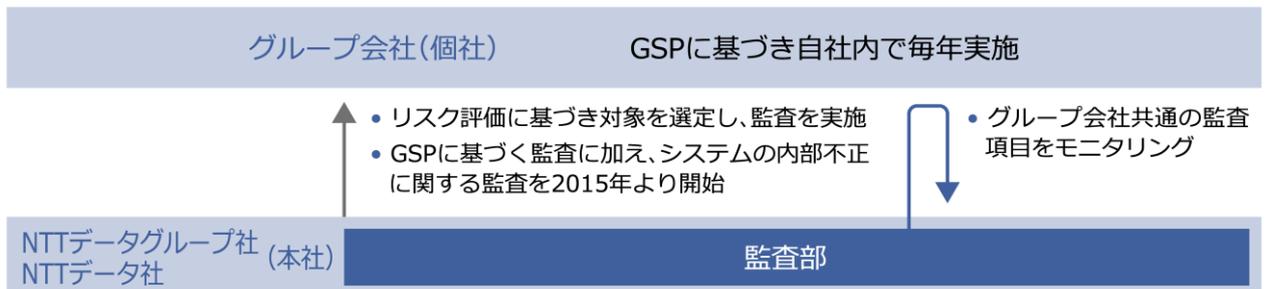
➤ NTT DATA グループ全体の情報セキュリティガバナンス・情報セキュリティマネジメントにおける主な体制と取り組み

<p>情報セキュリティガバナンスに関する会議体及び組織</p>	<p>【会議体】[評価・方向付け]</p> <ul style="list-style-type: none"> ・情報セキュリティ委員会（NTT データグループ社） NTT データグループ社の技術総括副担当役員を委員長とし、NTT データグループ社の各関連部門長、NTT データ社の情報セキュリティを所掌する役員、NTT DATA, Inc.の CISO、NTT データ社の各事業部門の組織長で構成。当社全体の活動状況と課題点を把握・評価し、当社全体の情報セキュリティ戦略を決定 <p>【組織】[推進・モニタリング]</p> <ul style="list-style-type: none"> ・情報セキュリティ運営組織（NTT データグループ社） NTT データグループ社の情報セキュリティ委員会事務局として会議体を運営 NTT データ社・NTT DATA, Inc.・各統括会社と連携し、グループ全体の情報セキュリティ方針及び施策推進計画に関する情報共有を行うとともに、NTT データ社・NTT DATA, Inc.・各統括会社の統制状況を定期的にモニタリングにて把握し、統制レベルの維持及び向上に向けた支援を実施
<p>情報セキュリティマネジメント組織</p>	<p>NTT データ社・NTT DATA, Inc.・各統括会社・各グループ会社に設置される情報セキュリティ運営組織は、NTT データグループ社から展開されたグループ全体の情報セキュリティ方針及び施策推進計画をもとに、各地域の特性や事情を考慮したマネジメント体制を構築し、情報セキュリティ施策を運用する</p>
<p>グループ会社間の情報共有</p>	<ul style="list-style-type: none"> ・Global CISO Conference 当社が主催し、各統括会社の CISO を含むキーパーソンが参加。各統括会社及び本社間の情報共有及び連携を強化 ・情報セキュリティ推進者フォーラム 当社が主催し、国内グループ会社の CISO・情報セキュリティ推進責任者が参加。グループの情報セキュリティ戦略と施策方針を共有

➤ NTT DATA の監査・モニタリング体制

<p>監査・モニタリング体制</p>	<ul style="list-style-type: none"> ・NTT データグループセキュリティポリシー（GSP）に基づく情報セキュリティの徹底による国内外のグループ会社を含めた監査・モニタリングの体制の確立（2006 年度～） ・3 つの視点によるセキュリティ監査の推進。リスクベース監査により、リスクの高い領域に重点的かつ効率的な監査を実施 <ol style="list-style-type: none"> 1. 基本動作の徹底：GSP に基づく組織の安全管理状況及び個人情報扱うシステムの安全管理状況を確認 2. 外部からの不正への対応：高度化するサイバー攻撃を踏まえ、脆弱性に対する防御、攻撃の検知/遮断等、システム的な対策の有効性を確認 3. 内部不正による情報漏えい防止のため、アクセス制御、持出管理等のシステムの及物理的な対策に加え、委託先管理を含めた対策の有効性を確認
--------------------	---

➤ 内部監査体制



◆ セキュリティインシデントの防止、検知、対応

当社では、平時の活動を通じて情報セキュリティインシデント*の発生を未然に防止するとともに、インシデントを早期に検知し、緊急対応を迅速かつ正確に行うための組織内 CSIRT として「NTTDATA-CERT」を運営しています。

* マルウェア感染や不正アクセス、情報漏えい等、情報管理やシステム運用に関してセキュリティ上の脅威となる現象

新たなセキュリティリスクに備えた活動

最新の攻撃手法やインシデントの発生状況等、セキュリティに関する広範な情報収集・情報分析・情報発信をはじめ、通信監視、緊急対応、研究開発、外部連携を実施しています。

内外と連携した幅広い活動

当社の活動にとどまらず、グローバルな CSIRT のコミュニティである「FIRST*」に加盟し、JPCERT コーディネーションセンター（JPCERT/CC）や日本シーサート協議会（NCA）に加盟している各社の CSIRT 等、外部のセキュリティ組織と幅広く連携することにより、迅速なセキュリティ関連情報の共有を行い、情報セキュリティ事案の早期検知・早期対応を実現しています。

* Forum of Incident Response and Security Teams の略。政府機関、教育機関、企業等の 635 の CSIRT チームから構成されるグローバルなコミュニティ（2022 年 7 月 29 日時点）

OSINT を活用した CSIRT 運営

政府の公式発表やマスメディアによる報道、論文・技術資料等、合法的に入手できる情報を積極的に活用するオープン・ソース・インテリジェンス（OSINT）のアプローチを NTTDATA-CERT の運営に採用しています。日々収集した情報は NTTDATA-CERT の情報分析専門家がセキュリティ動向を分析、予測して、当社各社へニュースや四半期レポートとして報告されるほか、サイバー攻撃監視の強化や当社のセキュリティ戦略・対策に活用しています。

インシデント対応ワークショップの実施

情報セキュリティインシデントが発生した場合に、組織的で速やかな対応を行い、影響を最小限に抑えてインシデントを終息できるよう、国内グループ会社に対してワークショップを実施しています。「NTT データグループ日本地域における情報セキュリティインシデント対応基準」をもとに、インシデント発生から終息までに行うべき行動の学習と、当社で過去に発生したインシデント事例を使った演習を通して、サイバー攻撃の適切な対応方法を習得しています。

◆ セキュリティガバナンスの取り組み強化

当社では、グローバルで直面するセキュリティリスクを把握し確実に対応するため、セキュリティガバナンスの取り組みを強化しています。

2022 年度は「グローバルガバナンス成熟度向上」に向けた取り組み、「グローバルセキュリティ基盤」の安定運用、「重大なインシデント発生時の確実なエスカレーション」への取り組みを行いました。

グローバルガバナンス成熟度向上

当社では、各統括会社が直面するセキュリティリスクの状況を集約し、グローバルのグループ会社全体で重点的に取り組むべきセキュリティ対策を決定するプロセスを確立し、運用しています。また、各統括会社の CISO を含むキーパーソンが一堂に会する Global CISO Conference を定期的に開催し、各統括会社及び本社間の情報共有及び連携を強化しています。

グローバルセキュリティ基盤

多様化する働き方に対応するため、また高度化するサイバー攻撃に対抗するため、当社共通の第一期グローバルセキュリティ基盤を構築・運用しています。このセキュリティ基盤によりメールやクラウドサービス利用時のセキュリティを強化、更にユーザーが使用するデバイス及びインターネット接続点を集中管理し、当社全体で高いセキュリティレベルを保っています。また、万一外部からネットワークに侵入された場合にもほかの地域への拡散を防ぐため、当社の国内及び海外拠点間の遮断も可能です。更に、高度なサイバー攻撃を検知可能とするための高度なログ分析システムで日々監視しています。

2020 年度からは第二期グローバルセキュリティ基盤として、メールセキュリティ強化とゼロトラストアーキテクチャを取り入れたユーザーの IT 環境の強化を行いました。

重大なインシデント発生時の早期エスカレーション

重大なインシデント発生時の早期検知と報告対応を確実に実施するため、当社の国内及び海外拠点のインシデント対応組織を階層的に整備し、現場による即応力と、高難度インシデントへの対応力を確保しています。また、グループ内のルールで役割・責任、報告基準を明確に定め、重大なインシデント発生時には、当社の国内及び海外のグループ会社から統括会社等を介し、本社へ速やかな報告が確実に行われる体制を維持しています。なお、2022年度、「(株) NTT データ お客様情報対応窓口」で受け付けた顧客プライバシーの侵害及び顧客データの紛失に関して具体化した不服申し立てはありませんでした。

◆ 具体的な取り組み

HQ

ND

国内G

Inc.

安全・安心な商用システムのセキュリティを確保

サイバー攻撃は、対処方法が知られた「既知の攻撃」に加え、ソフトウェア開発者やシステム開発ベンダですら気づいていない脆弱性を悪用した攻撃も増加しており、このような「未知の攻撃」についても考慮したセキュリティ対策をシステム全体にわたって抜け漏れなく行うことが求められています。

当社では、最新のセキュリティ技術動向、脆弱性情報をグループ内で迅速に共有するとともに、システム構築や運用において、必要なセキュリティレベルを確保するためのプロセスを組み込み、システムが必要なセキュリティレベルを確保できる仕組みを整備しています。構築したシステムは、セキュリティ専門家によるセキュリティ診断を定期的に行い、新たに発見される脆弱性に適切に対応するなど、継続的に安全・安心なシステム・サービスの提供に努めています。

総合的なセキュリティ管理により安全・安心なシステム環境を提供

当社は、豊富な経験と実績から得たセキュリティノウハウを結集し、お客様のビジネス構造の変化に合わせた最適な解決策を提案しています。

例えば、グローバル拠点も含めたセキュリティガバナンスの構築、重要な情報を取り扱うシステムに必要とされる高レベルなセキュリティ技術、新しい働き方を促進するための安全なリモートワーク環境を実現するゼロトラストセキュリティを提供します。

また、近年、日々高度化する標的型攻撃や内部不正による情報漏えい等、「防御」のセキュリティ対策をすり抜けるリスクが発生する前提での備えが重要になっています。被害を局所化するためには、攻撃の確実な「検知」と速やかな「対応・復旧」が求められます。セキュリティコンサルティングによってリスクを「特定」し、リスクを「抑止」「防御」するために必要なソリューションやサービスを提供、更には「検知」「対応・復旧」のために、UEBA^{*1}、EDR^{*2}、サンドボックス^{*3}、SIEM^{*4}、SOC^{*5}、CSIRT^{*6}等の構築サービスや運用監視サービスを提供することにより、お客様のセキュリティ対策支援サービスを強化しています。

- *1 User and Entity Behavior Analytics の略。平常時の人やものの振る舞いを機械学習し、通常と異なる動作と判断された処理をアラートとして通知するソリューション
- *2 Endpoint Detection and Response の略。パソコンやサーバ等エンドポイントを監視し、インシデントの検知やその後の対応プロセスを統合的に管理できるソリューション
- *3 保護された仮想領域内でプログラムを動作させることで、マルウェアの検知を行うソリューション
- *4 Security Information and Event Management の略。セキュリティ機器単体では発見困難な不正アクセスの痕跡や兆候を検知・分析・可視化するソリューション
- *5 Security Operation Center IDS/IPS の略。ファイアウォール、DB ファイアウォール、WAF 等を総合的に監視・運用する拠点や体制
- *6 Computer Security Incident Response Team の略。セキュリティ専門家から構成されるインシデント対応を行うための組織。セキュリティインシデント、セキュリティ関連技術、脆弱性等の情報を収集・分析し、有効な対策や訓練の実施等の活動を行う

情報セキュリティ教育・啓発

当社では、社員やビジネスパートナー、協働者に対して、個人情報保護の方針や「NTT データグループセキュリティポリシー」に記載されたルールの理解、情報セキュリティを意識した行動の理解を促すために、e-ラーニングや座学教育等の情報セキュリティ教育を実施しています。2022年度も社員一人ひとりに情報セキュリティの基本行動を徹底させるため、各種施策を継続して実施しました。更に、NTT データグループ社、NTT データ社、NTT DATA, Inc.の全社員・協働者が標的型攻撃メールやばらまき型攻撃メールを見分け、正しい対応が取れるかを確認する訓練を、毎年実施しています。

➤ 2022年度にNTTデータ（現NTTデータグループ社・NTTデータ社・NTT DATA, Inc.）で実施した情報セキュリティ教育
（単位：人）

対象者	実施形態	受講者数	
全社員	情報セキュリティ・個人情報保護教育 （e-ラーニング）	目標	対象者 12,788（100%修了）
		実績	対象者 12,788（100%修了）
各階層	情報セキュリティ講話（座学教育）	人事本部で実施（階層研修プログラムとして組み込み）	
	セキュリティ社内資格者向け教育（e-ラーニング）	対象者に教材をオンライン提供	
協働者	個人情報保護導入教育/ 情報セキュリティ教育（e-ラーニング）	目標	当社システム登録者 47,775（100%修了）
		実績	当社システム登録者 47,775（100%修了）
	情報セキュリティ教育ハンドブック	新規協働者にダウンロード提供	
全社員・協働者	標的型メール対応訓練	全社員・協働者（約5.3万人）に訓練メールを送付し、見分け・初動対応演習を実施	

➤ 2022年度に実施した主なグループ会社の情報セキュリティ教育

（単位：人）

対象者	実施形態	受講者数
国内グループ会社社員・協働者	GSPセキュリティ教育・個人情報保護教育（e-ラーニング）（3言語）	35,637（国内グループ会社 66社）

※上記のほか、海外リージョンのグループ会社向けには各統括会社の配下で情報セキュリティ教育を実施

➤ 認証取得状況（2023年3月31日現在）

認証取得	<ul style="list-style-type: none"> 情報セキュリティマネジメントシステム（ISMS）認証取得 日本国内でNTTデータを含め43社（71社中43社 約60%） ISO/IEC27001認証取得 欧州、中国、インド等の海外の複数のグループ会社で取得 一般財団法人日本情報経済社会推進協会（JIPDEC）からのプライバシーマークの使用許諾 日本国内でNTTデータを含む40社（71社中40社 約56%）
------	--

➤ セキュリティ人材

当社ではセキュリティ人材の育成とスキル向上に積極的に取り組み、2023年4月時点で、NTTグループが推進する「セキュリティ人材認定」を有する990名が国内外で活躍しています。

人材レベル		認定者数
セキュリティマスター	業界屈指の実績、発信力を持つ第一人者	2
セキュリティプリンシパル	経営陣にセキュリティ戦略を提言するスペシャリスト	7
セキュリティプロフェッショナル	深い経験と判断力を備えたスペシャリスト	981

人材タイプ
セキュリティマネジメント/セキュリティコンサルティング
セキュリティ運用
セキュリティ開発

AI ガバナンス

人工知能（AI）は、今後ますます社会に浸透し、人々の行動や意思決定にも影響を与えるようになります。特に昨年から急速に普及をしている生成 AI は、人の能力に迫る精度を持ち、一般ユーザーでも気軽に利用できますが、その利用にあたっては、不正確な回答に基づく誤判断、情報漏えい、他者の権利侵害等、様々なリスクに対処する必要があります。NTT データグループ社では、AI を活用してお客様の業務改革を実現するため、推進と統制の両輪でビジネス拡大に取り組んでいます。

統制の取り組みとして、NTT データグループ社では、AI の研究、開発、運用、利活用等を推進する立場として、AI による差別・人権侵害や偽情報の発信等の問題に代表されるような、「倫理・社会受容性」のリスクを軽減し、真に人間と AI が共生する人間中心の社会を実現するため、2019 年 5 月に「NTT データグループ AI 指針」を策定しました。

<https://www.nttdata.com/global/ja/news/release/2019/052900/>

その後、2020 年 7 月に「AI 開発プロセス」の策定、AI 案件への適用を開始し、2020 年 10 月には「AI 品質アセスメントサービス」を試行開始するなど、AI ガバナンスに関する取り組みを拡大・継続してきました。

<https://www.nttdata.com/global/ja/news/release/2020/063000/>

加えて、AI に関わるガバナンスの強化を目的として、2021 年 4 月より社外有識者で構成される「AI アドバイザリーボード」を設置し、2023 年度も活動を継続しています。AI 利活用に関する技術動向、法令・規制、市民社会の認識についてアドバイザリーボードメンバーと当社の AI プロジェクトに関わる現場最前線のメンバーが議論をし、その結果を AI ガバナンスの具体的な手段に取り入れています。2022 年度はアドバイザリーボードでいただいた指摘を踏まえ、AI リスクの具体化、AI プロジェクト開始前のリスクチェックの仕組化等、普及展開を進めています。また、AI の不適切な利用によって生じるリスクを実効的にマネジメントし、AI の適正活用を推進するための専門組織として、AI ガバナンス室を 2023 年 4 月 1 日に設置しました。

<https://www.nttdata.com/global/ja/news/release/2023/032301/>

これにより、多様な観点で AI プロジェクトにおける問題発生を抑制するとともに、提供する AI ソリューションの品質／信頼性を向上させることにより、社会とお客様が AI 活用によるベネフィットを最大限に享受し、サステナブルな社会を実現できる環境を整備していきます。

開催頻度	AI に関する幹部層との意見交換：年 1 回 AI に関する実務層（マネージャーレベル）との勉強会：年 2 回 AI に関する案件相談(AI ガバナンス室)：最大年 4 回
構成メンバー (敬称略／五十音順)	座長 ・森川 博之 東京大学 大学院 工学系研究科 教授 メンバー ・石川 冬樹 国立情報学研究所 アーキテクチャ科学研究系 准教授 ・梅津 光弘 梅津総合研究所(株) 代表取締役 ・奈良 由美子 放送大学 教養学部 教授、SOLVE for SDGs プログラム総括補佐 ・西村 友海 九州大学 法学研究院 准教授

※2023 年 6 月現在

災害リスクへの対応

◆ 基本方針と推進体制

当社は、社会基盤を支える情報システムやサービスを数多く提供しており、災害時にシステムダウンやサービス中断が発生すると、社会や人々の生活に甚大な影響を及ぼします。そのため「災害時 Business Continuity Plan (BCP)」や、社会インフラにかかわるシステム・サービスの「コンティンジェンシー・プラン」の整備と継続的な改善に努めています。

直近では、テレワークでの働き方が主になるなかで大規模震災等があった場合や感染症拡大防止策等の対応等を進めています。

マネジメント推進責任者	社長
マネジメント体制	<ul style="list-style-type: none"> ・執行責任者の社長は災害対策の方針及び災害対策施策を決定 ・運営責任者及び運営責任者補助者のグローバルガバナンス本部長及び災害対策室長は、災害対策に必要なプロセスの確立、実施及び維持を確実にし、本社災害対策本部における災害対策プロセスの計画、実施、評価及び継続的改善を行う ・事業本部等においては、主管責任者である責任組織単位の長がその権限及び業務の範囲内で責任を負い、各事業本部等の災害対策本部等における災害対策プロセスの計画、実施、評価及び継続的改善を行う
計画・体制	<ul style="list-style-type: none"> ・「災害時 BCP」や「コンティンジェンシー・プラン」を整備 ・災害リスクの最小化に向けた各種訓練の実施：全社員向けの安否確認訓練や本社災害対策本部の設置等全社レベルの訓練にとどまらず、各組織等が業務に沿った個別訓練を実施
認証取得 2021年3月末時点実施	<ul style="list-style-type: none"> ・国際規格 ISO22301：2019 による BCMS 認証を取得 ・データセンタの建物、電力、空調、セキュリティ等のファシリティ保全業務は情報システム運用に重要な基盤業務であることから、全自社ビルにおいて事業継続マネジメントの認証を取得し、大規模地震や広域停電発生時等のインシデントに対応できる体制を整備

◆ 具体的な取り組み

当社は、ITIL (Information Technology Infrastructure Library)・ISO20000 等を参考にした網羅的な観点での点検や、障害発生時の対応ノウハウの展開及びそれらを通じた IT サービスマネージャーの育成等、徹底したシステム障害対策を進めています。災害時において当社及び当社グループの事業を継続させるためには、各組織ができるだけ早く業務復旧に着手し、短時間で目標レベルまで業務を回復させる必要があるため、事業継続計画を定め、教育・訓練及び災害時事業継続計画書の定期的な見直しを実施しています。

責任あるサプライチェーンの推進

◆ 基本方針

当社は、健全で透明な経営を実践しながら、新しい「しくみ」や「価値」の創造によって、お客様や社会の発展に寄与し、自ら成長するとともに豊かで調和のとれた安全・安心な社会の実現に貢献することを、企業として果たすべき使命・責任と考え、調達活動においてもその責任を全うし、社会へ貢献していくために、調達に関する基本方針を定めています。

調達に関する基本方針

1. 広く国内外のサプライヤの皆様に対し、公正に競争機会を提供するとともに、相互理解と信頼関係の構築に努めます。
2. 品質・価格・納期・安定供給を総合的に判断し、ビジネスニーズに即した競争力ある製品・サービスを、経済合理性に基づき調達します。
3. 法令や社会規範を遵守するとともに、人権・環境・安全等を重視した調達を行うことで、持続可能な社会の実現に貢献します。

<https://www.nttdata.com/global/ja/about-us/proc/procurement/>

「調達に関する基本方針」の浸透

NTT データグループ社は、購買取引に関する基本的事項を定めた「調達に関する基本方針」を Web サイト上に公開しています。また、購買取引を適正に実施する手続き方法等の社内規程や、お客様やサプライヤとの取引・契約に関して遵守すべき法令やルール、行動指針等をまとめた「公正取引規程」を設けて、公正な取引の徹底及び浸透を図っています。

◆ 具体的な取り組み

ガイドラインの策定と浸透

HQ

ND

海外G

当社は、サプライチェーン全体におけるサステナビリティ・ESG 関連の取り組みを推進するため、サプライヤの皆様にご遵守いただきたい事項を明確化したサプライヤ行動規範を 2022 年 10 月に改訂し、「NTT データグループ サプライチェーンサステナビリティ推進ガイドライン」を制定しました。これは、これまでの「NTT データグループ サプライチェーン CSR 推進ガイドライン」を再構成したものです。本ガイドラインは、海外グループ会社を含めた全社へ展開しています。

本ガイドラインをもとに、サステナビリティに関する 7 つの領域（人権・労働、安全衛生、環境、公正取引・倫理、品質・安全性、情報セキュリティ、事業継続計画の策定）で遵守すべき項目についてサプライヤの皆様にご周知するとともに、当社の施策への理解を促進していただくための働きかけを継続的に行ってまいります。

<https://www.nttdata.com/global/ja/about-us/proc/procurement/>

本ガイドラインについて、既存取引関係のあるサプライヤに対しては同意書の取得や取引契約書への条件追加、新規に取引を開始するサプライヤに対しては取引前提条件としての同意取得、等の対応により遵守要請をおこなっています。特にビジネスパートナー（BP）会社*については、2022 年度末時点で全 44 社のうち 41 社から同意書を取得しています。

また取引契約書については、NTT データグループ社、NTT データ社及び国内グループ会社共通の契約書雛形に本ガイドラインの遵守要請を盛り込んだほか、海外グループ会社においても地域の特性や商慣習に合った形で、同様に取引契約書でのガイドライン遵守要請を実施しています。

* NTT データグループ社では、お客様への品質保証活動を共同して推進するため、将来にわたり当社の事業展開への継続的な協力が期待できる日本国内の委託先をビジネスパートナーとして選定しています。

サプライヤに対する調査等の実施

HQ

ND

サプライヤに対し、NTT グループ共同でのアンケート調査や、フランスの評価機関である EcoVadis 社によるサステナビリティ調査等 Self-Assessment Questionnaire (SAQ) によるアセスメントを実施し、サプライヤのサステナビリティリスクを評価しています。まずは国内における調達額上位サプライヤから取り組みをはじめ、2022 年度は調達額のうち 66.1%を占めるサプライヤから回答をいただきました。調査の結果、サステナビリティに関する取り組みが不十分と判断された項目については、後述の実地調査等を通じサプライヤとともに改善策の検討を行っています。

サステナビリティ取り組みの強化

HQ

ND

IT業界ではサステナビリティへの取り組みが十分に成熟しておらず、評価機関による調査等への対応がすぐにはできないサプライヤも存在するため、そうしたサプライヤに対するサステナビリティリスクアセスメント支援を目的として、当社独自のSelf-Assessment Questionnaire (SAQ)を開始する予定です。2023年度はEcoVadis社によるサステナビリティ調査と合わせて約200社のサプライヤからご回答いただくことを目標としています。また、実地調査の実施対象を拡大していくとともに、サプライヤの状況に応じた課題の解消や協働についても強化していく予定です。

当社では、これらの取り組みにより、サプライチェーンにおけるリスクを可視化し、その改善を実施することで、持続可能な社会の実現に向けたサプライチェーンの構築・維持に努めていきます。

モニタリングの実施

HQ

ND

重要サプライヤに対するサステナビリティリスクのモニタリングとして、企業訪問等の直接対話による実地調査を実施しています。実地調査では、サプライヤとの対話を通じてサステナビリティに関するマネジメントシステムの構築を要請するとともに、Self-Assessment Questionnaire (SAQ)によって検出されたリスク項目を確認することを目的としています。2022年度はNTTグループにおける調達額上位のサプライヤ約40社に対して、NTTグループ共同で実地調査を実施した結果、人権をはじめとした顕著なサステナビリティリスクは発見されませんでした。

また実地調査では、同時に各サプライヤの取り組み状況の確認や課題としている事項の把握、ガイドラインの浸透を図っています。

サプライヤとのコミュニケーション

HQ

ND

国内G

2023年度はBP会社を中心とした重要なサプライヤを対象に、サステナビリティの取り組みに関する交流会を開催し、環境や人権をはじめとしたサプライチェーン全体におけるサステナビリティに対する意識向上と、取り組みの推進を図る予定です。

また、サプライヤからの相談・申告を受ける、NTTデータグループ社、NTTデータ社及び国内グループ会社共通の内部通報制度を設置しており、当窓口に通報したことを理由とした不利益な取り扱いを行わないことを「グループ内部通報ポリシー」に定めています。

【参照ページ】「内部通報制度」

コンプライアンスの徹底

◆ 基本方針と推進体制

当社では、法令違反等のコンプライアンスリスクの低減・未然防止のため、コンプライアンスリスクをグローバル全体で見えていく重要リスクとして設定し、全社的な対策の実施とモニタリングを実施しています。また、コンプライアンスリスクについて、抑止し、探知し、対応するためのコンプライアンスプログラムをグローバルで構築し、同プログラムを継続的に評価・改善することにより、コンプライアンス強化に努めています。具体的には、リスク抑止の仕組みとしてグループの役員及び社員が遵守すべき「NTT DATA 行動規範」を制定して日々の活動における規範を明確化し、行動規範に沿って、必要な規程類を整備し、研修等の教育啓発を行っています。また、リスク探知の仕組みとして内部通報制度を導入して社員からの通報を促す仕組み等をグローバルで整備しています。リスクが顕在化した際には、影響最小化に向けた対応、再発防止に向けたプログラムの改善等の対応を行っています。

◆ 具体的な取り組み

NTT DATA 行動規範

当社は、企業倫理・コンプライアンス意識の醸成及び昨今の経営環境の変化に対応することを目的とし、当社社員一人ひとりの日々の活動における基本的な規範として「NTT DATA 行動規範」を制定しています。

[NTT DATA 行動規範](#)

コンプライアンスリスクアセスメントの実施

当社は、コンプライアンス体制の定着状況の検証や意識向上を目的に、コンプライアンス・アセスメントを全海外グループ会社に実施しています。

このコンプライアンス・アセスメントは、贈収賄等に関する設問に回答する形式で実施され、そのうち、リスクが高いと見込まれるグループ会社に対しては個別インタビューを実施し、より詳細な統制状況を把握し、次年度のコンプライアンスプログラム強化へとつなげています。

役員・社員を対象にした理解浸透の取り組み

当社は、国内グループ会社社員約 43,000 人・海外グループ会社社員約 159,000 人を対象としたコンプライアンス研修（e-ラーニング等）を実施しているほか、昇格の節目に受講する階層別研修のプログラムとして企業倫理の講義を組み込むなど、組織やグループ会社のビジネス特性に応じたコンプライアンス関連の研修を実施し、社員のコンプライアンス意識の着実な向上に努めています。

また、事業活動のグローバル化を踏まえ、国際社会における汚職・贈賄の規制強化に対する意識の向上や、競争法法規等の法改正を踏まえた委託契約の注意喚起等も加え、教育の充実を図っています。更に、「NTT DATA 行動規範」の更なる理解浸透を目的に、日常の業務における判断に迷いや事例等を解説した「身近なケースに学ぶコンプライアンス NTT データグループ 倫理ガイド」も作成し、社員へ周知するとともに、社内ホームページに掲載し、いつでも参照・活用できるようにしています。

➤ 2022 年度の主なコンプライアンス関連研修

(単位：人 (%))

研修名	受講者数
コンプライアンス研修	国内社員 約 42,000 (99.7)
コンプライアンス研修	海外社員 約 159,000 (98.7)
階層別集合研修（講話：企業倫理とリスクマネジメント）	約 3,300 (96.6)

内部通報制度

当社では、法令・企業倫理等の違反行為を早期に発見し、速やかに是正することで健全な経営を維持するため、社員・協働者等、当社グループで働くすべての人や取引先から相談・申告を受ける内部通報制度を設け、下記のとおり運用しています。当窓口に通報したことを理由に通報者に対して不利益な取り扱いを行わないことを「NTT データグループ内部通報ポリシー」において規定しています。

内部通報制度の運用

- ・ 本社及びすべての海外統括会社ごとに、「NTT データグループ内部通報ポリシー」に準拠した内部通報窓口・制度を整備・運用
- ・ 通報者は、各統括会社単位に設置された窓口、もしくは本社の通報窓口に通報することが可能
- ・ 内部通報への対応は各社 CRO（Chief Risk Officer）の責任の下で行われ、法令や「NTT DATA 行動規範」及び各種規定への違反が認められた場合は、グループ各社が定める懲戒規程等に基づき減給や出勤停止等の懲戒処分の他、状況に応じて査定（評価）や人事異動に反映

➤ 本社通報窓口への通報件数とその内訳

2022年度の通報件数は147件であり、2件の懲戒処分を行いました。

(単位：件)

	2020年度			2021年度			2022年度		
	通報件数	懲戒 処分 件数		通報件数	懲戒 処分 件数		通報件数	懲戒 処分 件数	
		厳重 注意 件数	懲戒 処分 件数		厳重 注意 件数	懲戒 処分 件数			
全体通報件数	78	2	34	100	1	42	147	2	35
ハラスメント通報件数	54	1	22	78	0	36	109	2	35
コンプライアンス違反	23	1	22	36	0	36	37	2	35
社内ルール違反	23	1	22	36	0	36	37	2	35
法令違反 【人権侵害等】	0	0	0	0	0	0	0	0	0
違反なし	31	-	-	42	-	-	72	-	-
不適切な業務処理通報件数	17	1	7	14	1	5	22	0	0
コンプライアンス違反	8	1	7	6	1	5	0	0	0
社内ルール違反	8	1	7	6	1	5	0	0	0
法令違反【贈収賄、不正会計、偽装請負等】	0	0	0	0	0	0	0	0	0
違反なし	9	-	-	8	-	-	22	-	-
会社経費の私的使用通報件数	2	0	1	2	0	0	8	0	0
コンプライアンス違反	1	0	1	0	0	0	0	0	0
社内ルール違反	1	0	1	0	0	0	0	0	0
法令違反	0	0	0	0	0	0	0	0	0
違反なし	1	-	-	2	-	-	8	-	-
その他 通報件数	5	0	4	6	0	1	8	0	0
コンプライアンス違反	4	0	4	1	0	1	0	0	0
社内ルール違反	1	0	1	1	0	1	0	0	0
法令違反	3	0	3	0	0	0	0	0	0
違反なし	1	-	-	5	-	-	8	-	-

倫理的で責任ある活動の推進

当社は、「NTT DATA 行動規範」に基づき、事業において参照すべき倫理やコンプライアンスについての考え方を示しています。

◆ 税の透明性

税務に関する基本方針

当社では、海外グループ会社も含めたグループ全体で税務に関連する法規制等を遵守し、グループ会社の多国籍化や国際取引の増加によるグローバルな観点での税務リスクへの適切な対応及び管理の重要性の高まりに応じていくため、税務実務に関する基本指針を定めています。基本指針は地域統括会社等を含む国内外グループ会社への展開を図ることにより、グループ全体への税務コンプライアンスの維持向上や税負担の適正化をめざしています。

社員への浸透

実務においては、社内規程を整備し社員に対して適切な税務処理に関する指導を行っています。当社（連結子会社）に対しては税務に関する基本指針を定め、社員の教育、指導及び業務改善により、法令遵守の徹底と税務リスクの低減に努めています。

税務当局との関係

適時適切な情報提供や財務処理に関する照会等を通じて、税務当局との信頼関係を築いています。問題点の指摘等を受けた場合には、税務当局の措置・見解に対する異議申し立て・訴訟等を行う場合を除き、直ちに問題点の原因を解明し、適切な是正及び改善措置を講じて再発を防止しています。

➤ 収益額（2021年度）

(単位：億円)

収益額	約33,712	
	日本	20,310
	アメリカ	4,832
	スペイン	2,042
	ドイツ	1,224
	イタリア	761
	インド	715
	イギリス	655
	その他の国	3,191

➤ 税引前利益額（2021年度）

(単位：億円)

税引前利益額	約3,081	
	日本	2,742
	アメリカ	54
	その他の国	285

➤ 発生税額（2021年度）

（単位：億円）

発生税額	約1,288	
	日本	1,138
	インド	31
	その他の国	119

➤ 納付税額（2021年度）

（単位：億円）

納付税額	約1,141	
	日本	1,007
	インド	25
	その他の国	109

上記金額については、日本税務当局へ提出した「国別報告事項」に基づくものであり、連結財務諸表との直接的な関連はありません。

◆ 贈収賄・腐敗防止の禁止

当社では、腐敗防止に関して「NTT DATA 行動規範」に基づき対応するとともに、各国法令の遵守を徹底しています。2022年度における汚職と贈賄の事例や係争案件は確認されていません。

◆ 政治政策への対応

国内では政治献金に関して「NTT DATA 行動規範」に基づき対応するとともに、政治資金規正法の遵守を徹底しています。2022年度の国内の政治献金額は、750万円でした。

◆ 不正競争防止への対応

当社では、反トラスト/反競争的慣行に関して「NTT DATA 行動規範」に基づき対応するとともに、各国法令の遵守を徹底しています。国内においては社内規程として「公正取引規程」を制定し社内への浸透を図るとともに、海外においても現地法令に基づく取り組みを行っており、2022年度は国内、海外いずれも違反事例や係争案件は確認されていません。

◆ 適切なコーポレートブランディングへの対応

当社では、グローバルな事業展開にあたり、各国・各地域における適切なコーポレートブランドの認知をめざして活動を進め、各国・各地域の法令を遵守した宣伝・広告活動を進めています。2022年度において、違反事例や係争案件は確認されていません。