資料４－３

「電気通信事業ガバナンス」の強化に関する検討に当たっての基本的な考え方

（たたき台）

令　和　３　年　６　月　18　日

電気通信事業ガバナンス検討会

事　　務　　局

「ガバナンス」とは

① 「ガバナンス」とは、一般的に、「内部統制（統治・支配・管理）」、又は、「内部統制（同左）のための機構や方法」を意味する。

この他、「健全な企業経営を目指す、企業自身による管理体制」、「ステークホルダー（顧客、株主等）が企業活動を監視する仕組み」、「企業経営者が自らの企業をどのように規律するか、という問題」、「企業が説明責任（アカウンタビリティ）を果たすための仕組み」等の考え方もある。

⇒「情報の安全管理や通信設備の安全・信頼性確保等の対策を有効に機能させるための各電気通信事業者による内部統制の仕組み」

［参考1］「DX時代における企業のプライバシーガバナンスガイドブックVer1.0」（令和2年8月28日、総務省及び経済産業省）

「企業のプライバシーガバナンスとは、プライバシー問題の適切な*リスク管理*と*信頼の確保*による企業価値の向上に向け、*経営者が積極的にプライバシー問題への取組にコミットし、組織全体でプライバシー問題に取り組むための体制を構築し、それを機能させること*が、基本的な考え方となる。」

［参考2］ ISO/IEC27014:2020（情報セキュリティガバナンス）～ Information security, cybersecurity and privacy protection – Governance of information security～

＜4つのガバナンスプロセス＞

- *「評価（Evaluate）」*:将来の目標を実現するために調整が必要な個所を決定するガバナンスプロセスになっているか。
- *「指示（Direct）」*:経営陣が事業体の目標及び戦略を指示するガバナンスプロセスになっているか。
- *「監視（Monitor）」*:経営陣が、戦略的目標の達成度を評価することができるガバナンスプロセスがあるか。
- *「伝達（Communicate）」*:経営陣と利害関係者が、特定のニーズに応じた情報を交換する双方向のガバナンスプロセスがあるか。

② 「ガバナンス」は、必ずしも「内部」統制には限られない。社会システムを円滑・適切に確保するための仕組みとする考え方もある。

⇒「電気通信事業における情報の安全管理や通信設備の安全・信頼性確保等の対策を有効に機能させるための、政府による規制を含む、制度・ルール等の社会全体の仕組み」

［参考3］「The Global Risks Report 2021」（WEF: World Economic Report））

「Failure of technology governance：Lack of globally accepted frameworks, institutions or regulations for the use of critical digital networks and technology, as a result of different states or groups of states adopting incompatible digital infrastructure, protocols and/or standards. テクノロジーガバナンスの失敗：互換性のないデジタルインフラ、プロトコル及び/又は標準を採用している様々な国家又は国家のグープの結果として、重要なデジタルネットワーク及びテクノロジーの利用に関する世界的に認められたフレームワーク、制度又は規制の欠如（事務局仮訳）」

［参考4］「Governance: A Very Short Introduction」（Mark Bevir）

「Governance refers, therefore, to all processes of governing, whether undertaken by a government, market, or network, whether over a family, tribe, formal or informal organization, or territory, and whether through laws, norms, power or language.ガバナンスとは、家族・部族・公式または非公式の組織・領土に対して、政府や市場やネットワークによって、*法律や規範や権力や言葉を通じて行われる統治に関する全てのプロセス*。（事務局仮訳）」

「電気通信事業ガバナンス」の強化の必要性について

＜電気通信事業をめぐる環境変化に伴うリスクの高まり＞（第1回会合資料より）

- ・委託等の増加
- ・外国の法的環境による影響

⇒ 外部の委託先等における情報漏えい・滅失・き損や通信設備の故障等のリスク

- ・システムのソフトウェア化
- ・開発プロセスの多様化
- ・関与するステークホルダーの増加や複雑化

⇒ 内部の設定ミス等による情報漏えい・滅失・き損や通信設備の故障等のリスク

- ・情報の付加価値の高まり
- ・不正アクセスやDDoS攻撃等の巧妙化

⇒ サイバー攻撃による情報漏えい・滅失・き損や通信設備の故障等のリスク

これら上記リスクに適切に対処するため、各企業自ら、次の対応が必要。

① 企業自らによるガバナンス確保

1. 経営者のリーダーシップ及びコミットメントによる、適正なリスク管理（※）のための体制構築やモニタリング・レビュー
2. マルチステークホルダー（利用者や株主等）に対するアカウンタビリティや透明性の確保・向上

（※）リスク管理：リスクを把握・評価・分析することにより、情報の安全管理や通信設備の安全・信頼性確保等のための具体的な対策を措置

しかし、各企業が単独でリスクに適切に対処することが困難な状況。

⇒ 他の通信サービス・ネットワークにおける情報の漏えい・滅失・き損や通信設備の故障等のリスク

（通信事業者間で通信サービス・ネットワークが相互に連携・接続しているため、一企業にとってのリスクにとどまらず、他にも波及）

⇒ 通信サービス・ネットワークに対する安心・安全・信頼性が低下し、デジタル社会が停滞するリスク

（通信サービス・ネットワークがデジタル社会の神経網であるため、国民生活、社会経済及び危機管理・安全保障等に対する脅威）

以下について、国による規律等の在り方検討が必要。

② 社会全体によるガバナンス確保

1. 通信事業者自らによるガバナンス確保の推進（第三者認証の活用や国によるモニタリング・レビュー等の共同規制等）
2. 電気通信事業者間の連携・協力の推進（サイバー攻撃事態発生時の対応等）

【目的】デジタル社会における通信サービス・ネットワークの円滑な提供の確保及び利用者利益の保護

国による規律等の在り方検討に当たっての基本的な考え方①

1. 現状

- 各通信事業者は、マルチステークホルダー（利用者等）からの信頼を得る観点から、通信サービスの提供停止や利用者利益への支障の発生を回避するため、情報の漏えい・滅失・き損や通信設備の故障等のリスクへの対策を自ら講じるなど、**通信事業者自らによるガバナンスの確保に取り組んでいる**。
- また、以上のガバナンス確保のための具体的な取組（例：リスク管理の具体的な手法・組織体制・アカウンタビリティの確保策・安全管理措置等）については、**通信事業者が、各々直面しているリスク等に応じ、適切と考える方法により取り組んでいる**。
- **国による規律**については、電気通信事業が、イノベーション等により市場競争が激しく、通信サービス・ネットワークがそれを提供する通信事業者ごとに異なる特性を持ち、それを熟知する通信事業者の主体的な取組が有効かつ重要であるため、各通信事業者の自主的な取組を基本とし、そのための**必要最小限の環境整備**として、**行為義務等が法律上義務づけ**られている。

＜参考：現状の電気通信事業法等による規律＞

（1）情報の安全管理・適正な取扱い関係

- *通信の秘密*について、*利用者利益の保護の観点*から、*漏えいの防止*に加え、*技術基準により、「通信の秘密が侵されないようにすること」を確保するため、通信内容の秘匿措置及び蓄積情報保護*を義務づけ。また、*通信の秘密や個人情報の保護*の観点から、*「電気通信事業における個人情報保護に関するガイドライン」（告示）*を定め、通信事業者による対策を支援・促進。なお、個人情報の保護については、個人情報保護法に基づく権限が委任。
- *接続業務に関する情報*について、*適正な競争関係の確保の観点*から、第一種指定電気通信設備を設置する通信事業者に対し、*接続業務に関して知り得た情報の適正な管理*を義務づけ。

⇒ 規律の対象となる情報については、上記の通り一部のみ。
⇒ 行為義務等の規律の内容ついては、企業自ら及び社会全体によるガバナンス確保に関する規定は一部のみ。

（2）通信設備の安全・信頼性の確保関係

- *特定の通信サービスの提供の用に供する通信設備（事業用電気通信設備）*について、*サービスの円滑な提供の確保*の観点から、公共性の高さや社会的影響の大きさ等に鑑み、*電気通信回線設備を設置する通信事業者、利用者の利益に及ぼす影響が大きいサービス等を提供する通信事業者のみを対象*として、強制基準としての*技術基準*の遵守・自己確認、自主基準としての*管理規程*の策定・届出、実効性確保のための体制（担当役員）としての*電気通信設備統括管理者*の選任を義務づけ。また、具体策に関する推奨基準としての*「情報通信ネットワーク安全・信頼性基準」（告示）*を定め、通信事業者における対策を支援・促進。

⇒ 規律の対象となる通信サービス等については、上記の通り一部のみ。
⇒ 行為義務等の規律の内容については、企業自ら及び社会全体によるガバナンス確保に関する規定は一部のみ。

国による規律等の在り方検討に当たっての基本的な考え方②

2. 課題

① 近年、電気通信事業を取巻く、次の環境変化により、情報の漏えい・滅失・き損（以下「漏えい等」）や通信設備の故障等のリスクが高まっている。

1. 委託等の増加 ⇒ 委託先等におけるリスクの高まり
2. システムのソフトウェア化 ⇒ 設定ミス等による内部からのリスクの高まり
3. マルチステークホルダー化 ⇒ 連携不足等によるリスクの高まり
4. サイバー攻撃の巧妙化・悪質化 ⇒ 外部からの侵入によるリスクの高まり

② また、上記のようなリスクに適切に対処できなかったために、実際に、次の事案が発生し、通信サービスの円滑な提供の確保及び利用者利益の保護が図られないケースが頻発している。

1. 通信サービス提供のためのアプリ・システムの不具合により、利用者の個人情報や通信の秘密の漏えい事案
2. 利用者情報について海外の委託先等がアクセス可能な状態にあることにより、通信サービスに対する利用者の信頼が損ねられ、通信サービスと連携した公共サービスの提供が停滞する事案
3. 通信事業者間における情報共有等の連携不足により、長期間、クラウドWiFiサービスの提供停止等が頻発した事案
4. サイバー攻撃により窃取された恐れのある通信設備に関する情報が悪用され、通信サービスの提供先である重要インフラ関係事業者が緊急時の事業継続等のために利用する当該サービスの提供が停止する恐れのある事案
5. サイバー攻撃により通信サービスの提供停止に至る事案

③ 以上のとおり、現状の各通信事業者による自主的な取組、そして、そのための必要最小限の環境整備としての現行の国による規律では、リスクへの対処が困難となってきている。他方で、CPS（Cyber Physical System）におけるサイバー空間を構成する中核であるとともに、同空間とフィジカル空間を繋ぐ神経網として、今後、デジタル社会の中枢基盤となる通信サービス・ネットワークを提供する通信事業者が、引続きイノベーションの牽引等、主導的な役割を果たす環境整備も必要となっている。

④ そこで、デジタル社会における通信サービス・ネットワークの円滑な提供の確保や利用者利益の保護という目的を実現するための「電気通信事業ガバナンス」を強化する観点から、通信事業者の自主的な取組を基本とした、現行の国による規律の在り方について、自主性と実効性とのバランスに配慮しつつ、次の点に関する基本的な考え方を整理することが課題となっている。

1. 各通信事業者自らによるガバナンスや通信事業者間の連携・協力を推進するための環境整備の在り方
2. 上記1にあたっての自主規制、法的規制、共同規制の在り方

対策の検討に当たっての基本的な考え方③

3. 基本的な考え方の整理

① 情報の漏えい等や設備の故障等のリスクへの対応については、各企業で直面しているリスクの把握・評価・分析を行った上で必要な具体策を講じるなど、**通信事業者自らがリスク管理に取り組むことを基本とすべき**ではないか。

② また、**経営陣の主体的な関与により**、リスク管理のしくみを適切に機能させるための組織体制の構築や、リスク管理状況の対外的な公表等によりアカウンタビリティの確保を図るなど、**通信事業者自らのガバナンスを強化することが必要**ではないか。

③ 従って、**通信事業者の自主性を基本**とし、**イノベーションが進展する中で、通信事業者が引続き主導的な役割を果たす**ため、**国は**、特に**公共性が高く、社会的な影響が大きいと考えられる場合を対象として**、例えば、現行の規律では明確ではないリスク管理等について、通信事業者自らによるガバナンス確保のための必要最小限の規律を課すとともに、具体的な対策を指針等において示すなどにより、引続き、**通信事業者によるこれらの取組を推進すべき**ではないか。

④ 一方、**一通信事業者による取組のみに委ねるのではリスクへの対応が十分といえないと考えられる場合**には、**通信事業者間の連携・協力の在り方や国によるモニタリング・レビューの在り方を検討することが適当**ではないか。

（※）VUCA：：Volatility：変動性, Uncertainty：不確実性, Complexity：複雑性, Ambiguity：曖昧性

⑤ この点、VUCA（※）と言われる環境変化に伴う**リスクの複雑化・多様化を背景として、一通信事業者において確実にリスクの把握・評価・分析を行うことが益々難しく**なっている。当該一事業者による取組のみに委ねるのでは**通信サービス・ネットワーク全般に対する安心・安全・信頼性を低下させ、その利用によるデジタル社会の停滞を及ぼす重大なリスクを生じさせる**ことから、これに対応するため、通信事業者自らによるガバナンス確保が機能しているかについて、**規律の実効性を確保**するため、第三者認証の活用や国による**モニタリング・レビュー等の共同規制の在り方を検討することが必要**ではないか。

⑥ 次に、**他の通信事業者の通信サービス・ネットワークと連携・接続して自らの通信サービス・ネットワークを提供している通信事業者において、当該他事業者におけるリスクへの対処が適切でないことにより重大なリスクが発生する場合**には、当該一事業者による取組のみに委ねるのでは不十分であり、サイバー攻撃事態発生時の対応等、**通信事業者間の連携・協力による対応が図られるようにするための規律の在り方を検討することが必要**ではないか。

参考資料

（参考）企業自らによるガバナンスの確保の具体的な実施事項の例

企業自らによるガバナンスの確保

（例）○経営者のリーダーシップ及びコミットメント

- 対応方針の策定・公表（情報・設備に関する管理規程やセキュリティポリシーの公表等）
- 組織内のリスク管理（リスクの把握・評価・分析及び具体策の実施管理（右枠内参照））を機能させるための体制構築（担当役員等）
- モニタリングレビュー・当該評価踏まえた重大なリスクへの適時適切な対処のためのしくみ（監査や役員会、第三者委員会の活用等）
- 組織内へのセキュリティ意識・文化の浸透（役員や従業員に対する研修や訓練等）

○アカウンタビリティ・透明性の向上

- 積極的な取組の公表
- 第三者認証の取得

技術的措置等の具体的な対策

（例）

- 委託先の監督
- 内部からの情報漏えいの防止策
- 外部からの不正侵入防止策
- アクセス管理の強化
- データの安全管理措置
- 他事業者との連携体制の構築 等

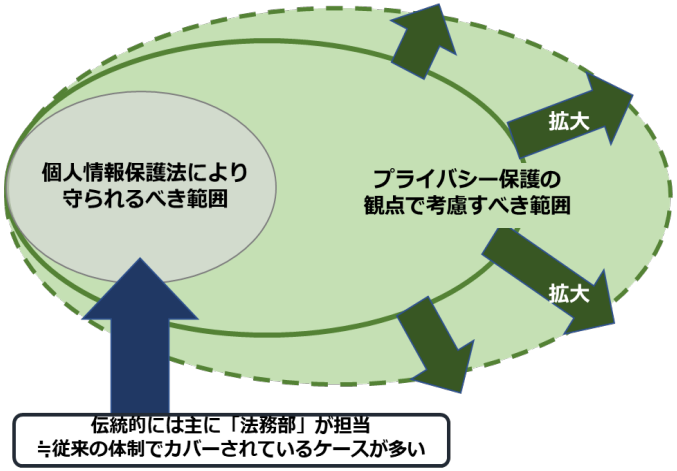
（参考）DX時代における企業のプライバシーガバナンスガイドブックVer1.0の背景

＜「DX時代における企業のプライバシーガバナンスガイドブックVer1.0」概要（令和2年8月28日総務省及び経済産業省プレスリリース）より抜粋＞

- 昨今ビジネスモデルの変革や技術革新が著しく、イノベーションの中心的役割を担うDX企業は、**イノベーションから生じる様々なリスクの低減を、自ら図っていかなければならない。**
- プライバシーに関する問題について、個人情報保護法を遵守しているか否か（コンプライアンス）の点を中心に検討されることが多かった。しかし法令を遵守していても、本人への差別、不利益、不安を与えるとの点から、**批判を避けきれず炎上し、企業の存続に関わるような問題として顕在化**するケースも見られる。
- 企業は、**プライバシーに関する問題について能動的に対応し**、消費者やステークホルダーに対して、積極的に説明責任を果たし、**社会からの信頼を獲得する**ことが必要である。経営者は、プライバシー問題の向き合い方について、経営戦略として捉えることで、企業価値向上につながるといえる。

プライバシー保護の観点で考慮すべき範囲と体制構築

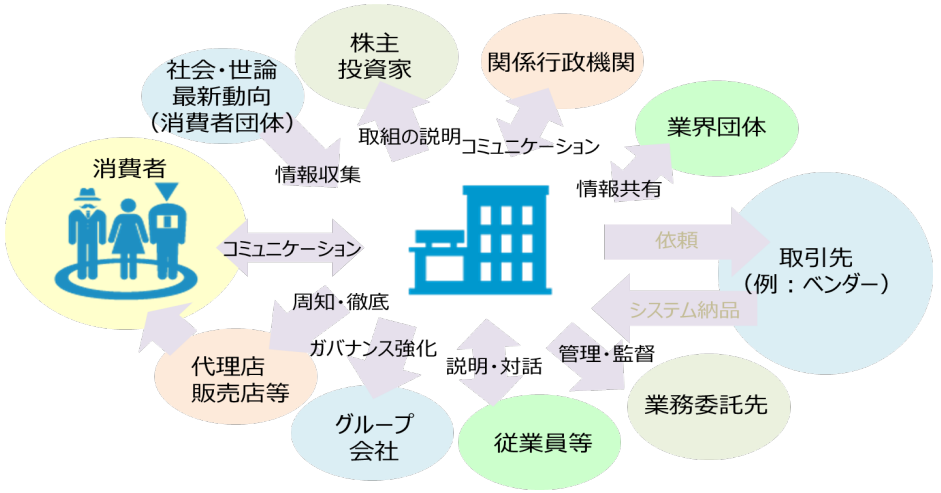
プライバシーは取り扱う情報や技術、取り巻く環境によって変化する



イノベーション（技術革新）と比例して
プライバシー保護の観点で考慮すべき
範囲（プライバシー問題）が拡大

プライバシー問題全体を考えられる
体制の構築が必要

ステークホルダーとのコミュニケーション



企業が社会からの信頼の獲得するためのプライバシーガバナンスの構築に向けて、
まずは取り組むべきことをガイドブックとして取りまとめた

（参考）DX時代における企業のプライバシーガバナンスガイドブックVer1.0の概要

＜「DX時代における企業のプライバシーガバナンスガイドブックVer1.0」概要（令和2年8月28日総務省及び経済産業省プレスリリース）より抜粋＞

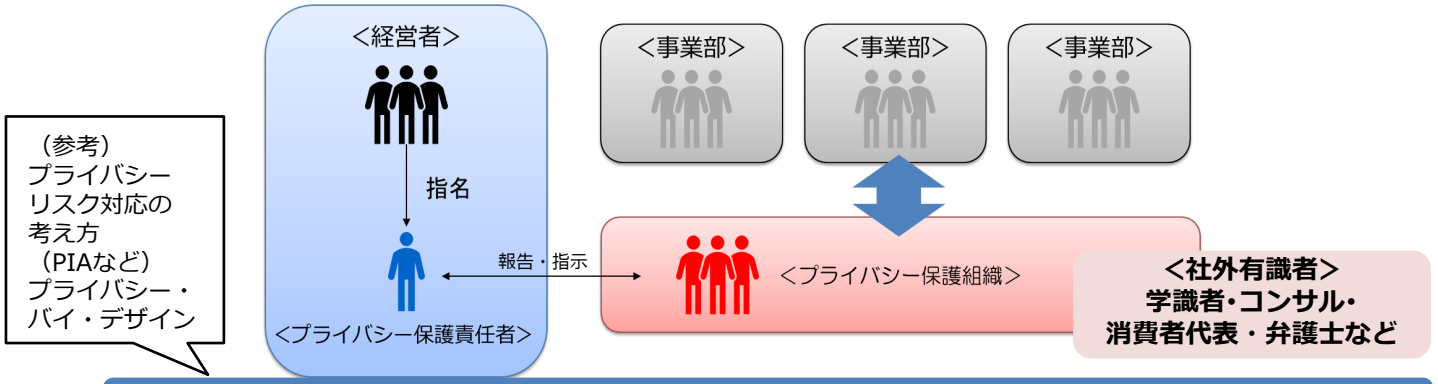
【対象読者】パーソナルデータを利活用した製品・サービスを提供し、消費者のプライバシーへの配慮を迫られることが想定される企業や、そのような企業と取引をしているベンダー企業等であって、
①**企業の経営陣**または**経営者へ提案できるポジションにいる管理職**等
②データの利活用や保護に係る事柄を総合的に管理する部門の責任者・担当者　など

経営者が取り組むべき3要件

要件１：プライバシーガバナンスに係る姿勢の明文化
経営戦略上の重要課題として、プライバシーに係る基本的考え方や姿勢を明文化し、組織内外へ知らしめる。経営者には、明文化した内容に基づいた実施についてアカウンタビリティを確保することが求められる。

要件２：プライバシー保護責任者の指名
組織全体のプライバシー問題への対応の責任者を指名し、権限と責任の両方を与える。

要件３：プライバシーへの取組に対するリソースの投入
必要十分な経営資源（ヒト・モノ・カネ）を漸次投入し、体制の構築、人材の配置・育成・確保等を行う。



プライバシーガバナンスの重要項目

1. **体制の構築**（内部統制、プライバシー保護組織の設置、社外有識者との連携）
2. **運用ルールの策定と周知**（運用を徹底するためのルールを策定、組織内への周知）
3. **企業内のプライバシーに係る文化の醸成**（個々の従業員がプライバシー意識を持つよう企業文化を醸成）
4. **消費者とのコミュニケーション**（組織の取組について普及・広報、消費者と継続的にコミュニケーション）
5. **その他のステークホルダーとのコミュニケーション**
（ビジネスパートナー、グループ企業等、投資家・株主、行政機関、業界団体、従業員等とのコミュニケーション）

企業価値の向上・ビジネス上の優位性

社会からの信頼獲得

消費者・その他のステークホルダー

（参考）プライバシーガバナンスに係る取組の例

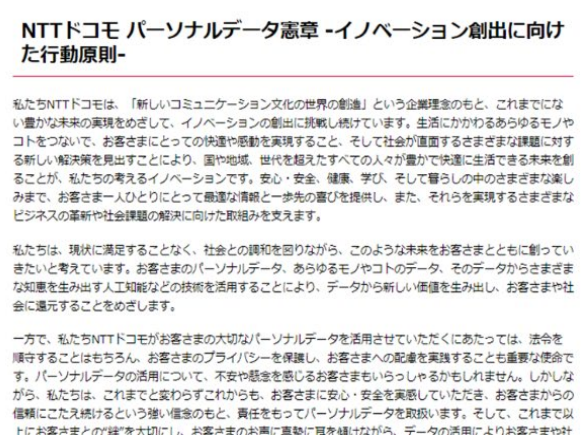
＜「DX時代における企業のプライバシーガバナンスガイドブックVer1.0」概要(令和2年8月28日。総務省及び経済産業省プレスリリース)より抜粋＞

○プライバシーガバナンスに係る姿勢の明文化

明文化の具体的な形としては、宣言の形をとったプライバシーステートメントや、組織全体での行動原則を策定するケースもある。

事例：NTTドコモ パーソナルデータ憲章の公表

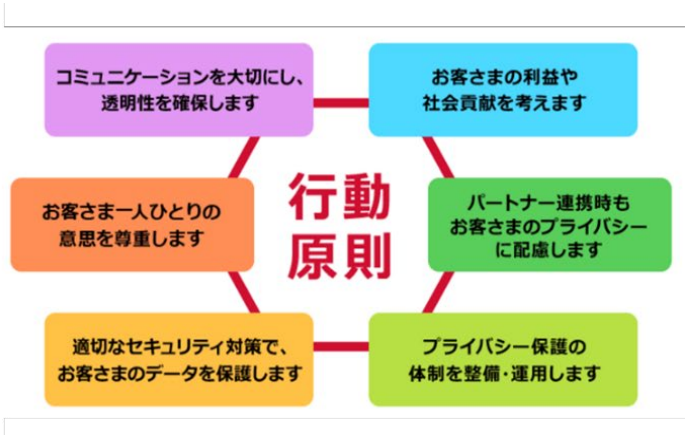
株式会社NTTドコモでは、「パーソナルデータ憲章―イノベーション創出に向けた行動原則―」を作成し、公表している。このパーソナルデータ憲章は、NTTドコモが「新しいコミュニケーション文化の世界の創造」という企業理念の下、これまでにない豊かな未来の実現をめざして、イノベーション創造に挑戦し続けていること、社会との調和を図りながら、未来をお客様と共に創っていきたいと考えていること、パーソナルデータの活用に当たり法令順守はもちろん、お客様のプライバシーを保護し、配慮を実践することも重要な使命であることなどを宣言し、行動原則として6つの原則を提示している。


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



○消費者とのコミュニケーション（組織の取組の公表、広報）

透明性レポート（transparency report）のように、消費者が特に懸念する項目等を、積極的に分かりやすく公表していく方法は有効である。データの高度な利活用が進むほど、新しいプライバシーリスクが発生する。消費者が懸念点を解消できるよう、取組の情報を定期的に取りまとめて発信することで、消費者も安心してサービスを利用することができる。

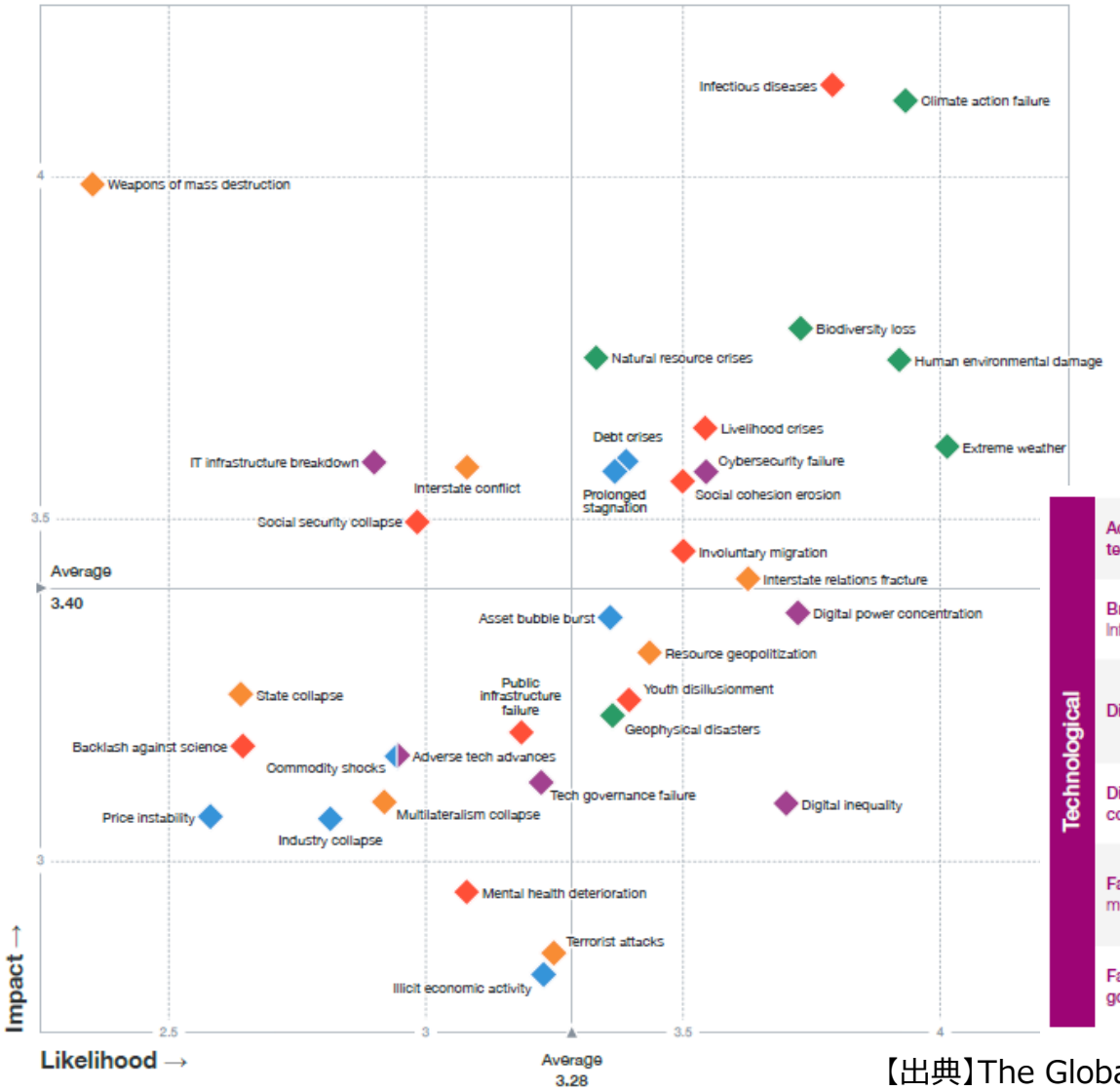
事例：LINE
TRANSPARENCY REPORTの公表

LINE株式会社の「TRANSPARENCY REPORT」では、消費者から預かるデータをどのように取り扱っていたかを定期的に報告し、プラットフォーム運営に当たっての考え方を公表している。

（出典）https://linecorp.com/ja/security/transparency/top

（参考）「グローバルリスク報告書2021」

- 世界経済フォーラム（World Economic Forum）「グローバルリスク報告書2021」（令和3年1月）において、今後10年間における最も可能性や影響の大きいリスクが公表。
- デジタル関係では、「Cybersecurity failure」、「IT Infra breakdown」や「Digital power concentration」等に加え、今回より、新たに「Tech governance failure」が追加。



Top Risks by likelihood

1. Extreme weather
2. Climate action failure
3. Human environmental damage
4. Infectious diseases
5. Biodiversity loss
6. Digital power concentration
7. Digital inequality
8. Interstate relations fracture
9. Cybersecurity failure
10. Livelihood crises

Top Risks by impact

1. Infectious diseases
2. Climate action failure
3. Weapons of mass destruction
4. Biodiversity loss
5. Natural resource crises
6. Human environmental damage
7. Livelihood crises
8. Extreme weather
9. Debt crises
10. IT infrastructure breakdown

Technological

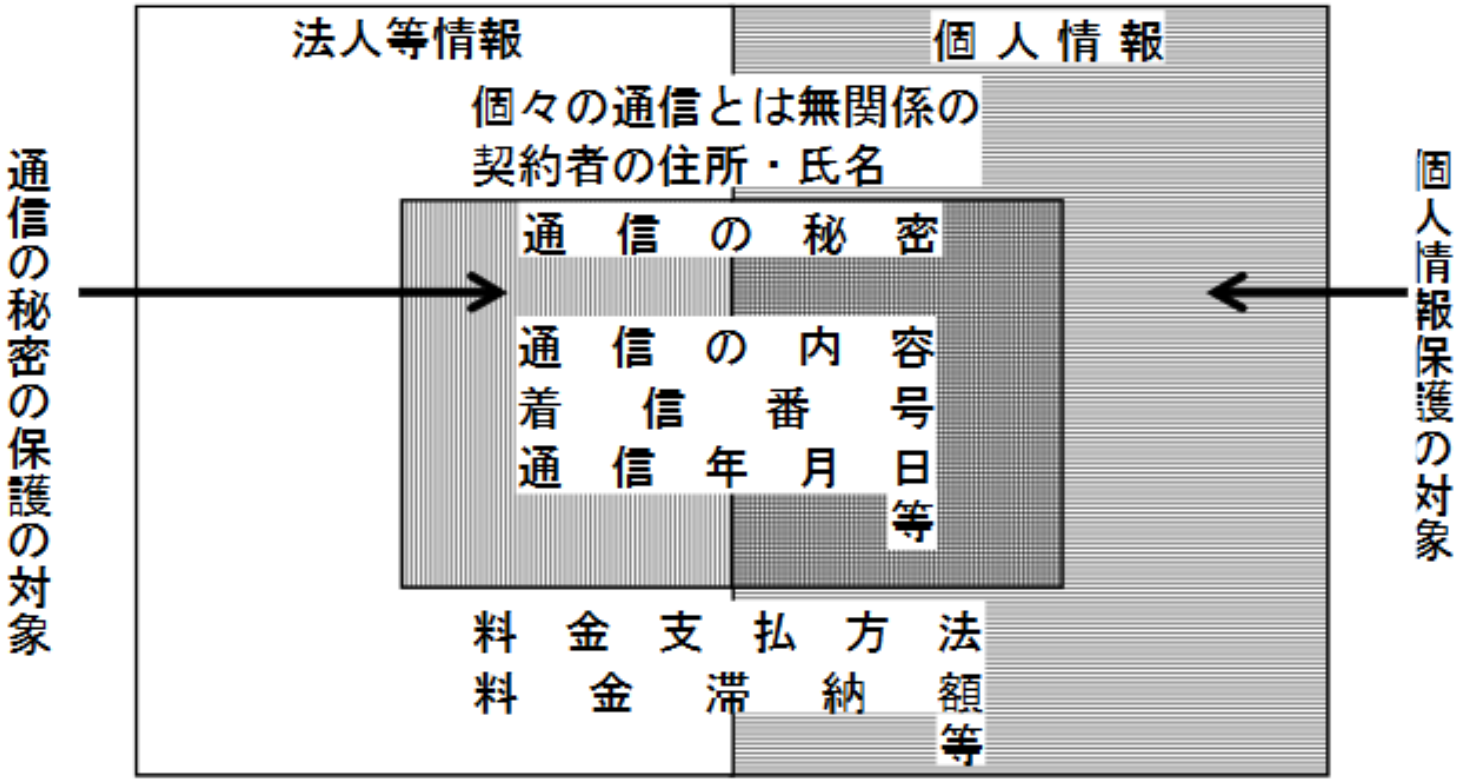
Adverse outcomes of technological advances	Intended or unintended negative consequences of technological advances on individuals, businesses, ecosystems and/or economies: AI, brain-computer interfaces, biotechnology, geo-engineering, quantum computing etc.
Breakdown of critical information infrastructure	Deterioration, saturation or shutdown of critical physical and digital infrastructure or services as a result of a systemic dependency on cyber networks and/or technology: AI-intensive systems, internet, hand-held devices, public utilities, satellites, etc.
Digital inequality	Fractured and/or unequal access to critical digital networks and technology, between and within countries, as a result of unequal investment capabilities, lack of necessary skills in the workforce, insufficient purchase power, government restrictions and/or cultural differences
Digital power concentration	Concentration of critical digital assets, capabilities and/or knowledge by a reduced number of individuals, businesses or states, resulting in discretionary pricing mechanisms, lack of impartial oversight, unequal private and/or public access etc.
Failure of cybersecurity measures	Business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability
Failure of technology governance	Lack of globally accepted frameworks, institutions or regulations for the use of critical digital networks and technology, as a result of different states or groups of states adopting incompatible digital infrastructure, protocols and/or standards

【出典】The Global Risks Report 2021（2021年1月世界経済フォーラム（WEF））

（参考）個人情報と通信の秘密の関係

- 通信の秘密は、「個々の通信」を保護するものであり、主体が法人その他の団体の情報であっても保護対象となる点で、個人情報よりも対象範囲が広い。
- 「個々の通信」とは無関係の契約者の住所・氏名などは保護対象とならない点で、個人情報よりも対象範囲が狭い。
- 通信の秘密は「知られない」、「漏えいされない」、「窃用されない」という消極的な自由権を保護するものであるのに対して、個人情報保護が自己に関する情報をコントロールする権利利益としての積極的な性格を有する（郵政省電気通信局「電気通信とプライバシー保護」）。

●個人情報と通信の秘密との関係



※「電気通信事業における個人情報保護に関するガイドラインの解説」

（参考）電気通信分野における安全・信頼性対策に関する制度

- 電気通信設備は事業者ごとに異なる特性を持ち、それを熟知する事業者の主体的な取組が有効かつ重要であることから、安全・信頼性の確保は、事業者の自主的な取組（自律的・継続的なPDCAサイクル）が基本。国は、そのための環境を整備。
- 具体的には、「事業用電気通信設備」のライフサイクル（設置・設計、工事、維持・運用）を念頭に、事業者ごとの特性に応じた自主基準「管理規程」をPDCAサイクルの基盤とし、事業者共通の強制基準「技術基準」や監督責任者の設置を義務付け。

電気通信事業者 （2021年4月1日現在）

登録 333者	届出 21,581者	
回線設置等 約450者	有料かつ大規模 回線非設置 4者	回線非設置 約2.15万者

監督責任

電気通信設備統括管理者

●経営レベルの事業用電気通信設備の統括管理
電気通信事業者が経営陣で実務経験のある者から選任、事故防止対策に主体的に関与。
【法第44条の3等、電気通信事業法施行規則(省令)】

電気通信主任技術者

●事業用電気通信設備の工事・維持・運用を監督
電気通信事業者が資格者を選任して事業用電気通信設備を監督。電気通信主任技術者に登録講習機関による講習を受けさせる義務。【法第45条等、電気通信主任技術者規則(省令)】

工事担任者

●端末設備等の接続の工事を実施等
資格者が利用者の端末設備等の接続の工事を実施・実地監督。
【法第71条・第74条等、工事担任者規則(省令)】

強制基準

技術基準

●電気通信事業者の事業用電気通信設備の技術基準
予備機器、停電対策、耐震対策、防護措置、通話品質等を規定。
【法第41条・第42条等、事業用電気通信設備規則(省令)】

●利用者の端末設備等の接続の技術基準
安全性、電気的条件、責任の分界、セキュリティ対策等を規定。登録認定機関等が技術基準適合認定等を実施。登録修理業者は修理された端末機器の技術基準適合性を確保義務。
【法第52条・第86条等、端末設備等規則(省令)、技術基準適合認定等に関する規則(省令)】

自主基準

管理規程

●事業用電気通信設備の管理に係る事業者毎の特性に応じた自主基準
部門横断的な設備管理の方針、電気通信主任技術者等の職務、組織内外の連携、事故対応等を定める義務。
【法第44条等、電気通信事業法施行規則(省令)】

なし
（自主的な取組のみ）

推奨基準

安全・信頼性基準

●情報通信ネットワーク全体の安全・信頼性対策に関する基本的・総合的な指標を整理した推奨基準（ガイドライン）
設備等に関する「設備等基準」と、設計・施工・運用等に関する「管理基準」に区分。大規模インターネット障害対策、ソフトウェア信頼性向上、災害対策、事故状況の情報公開等を規定。自営情報通信ネットワークやユーザネットワークも対象。
【情報通信ネットワーク安全・信頼性基準(告示)】

（参考）事業用電気通信設備の技術基準

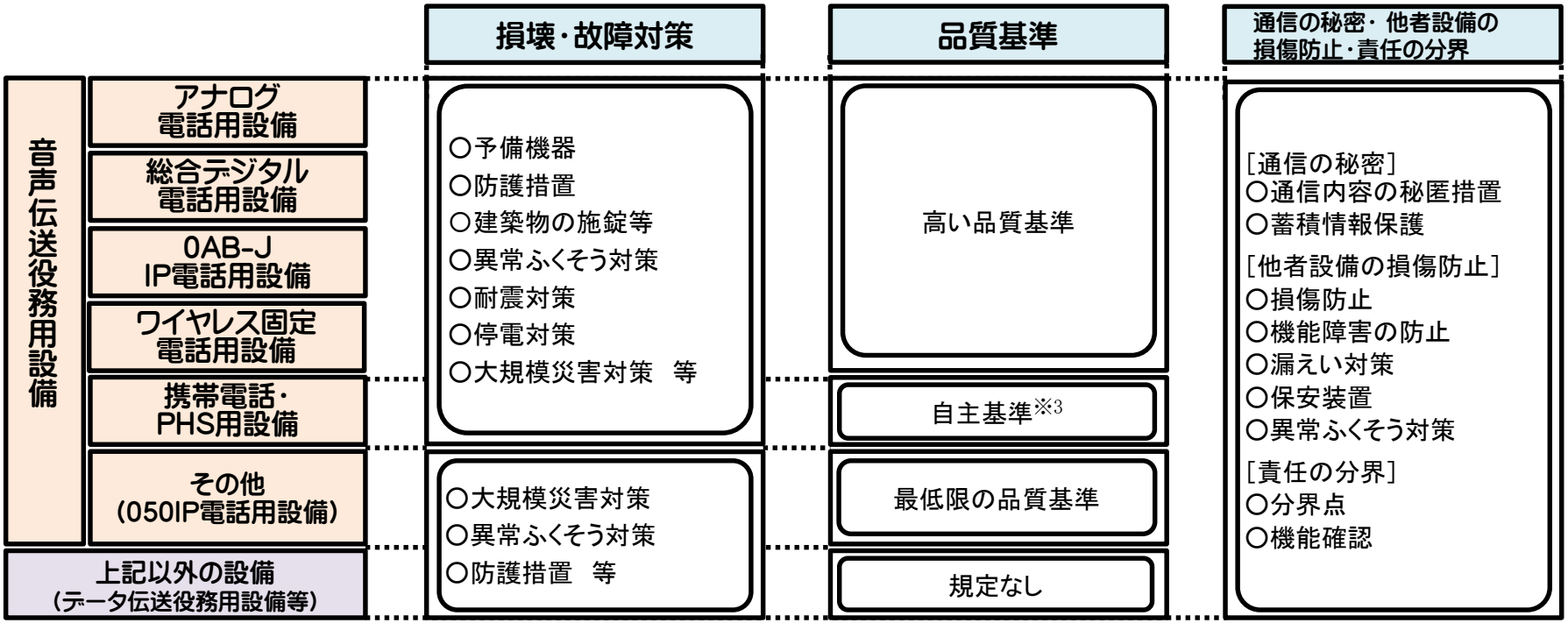
- **「電気通信回線設備（送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備）を設置する電気通信事業者」**及び**「内容、利用者の範囲等からみて利用者の利益に及ぼす影響が大きいものとして総務省令で定める電気通信役務を提供する電気通信事業者※1」**等は、**電気通信事業の用に供する「事業用電気通信設備」**を総務省令で定める技術基準※2に適合するように維持しなければならない。［電気通信事業法（以下「法」という。）第41条］

※1　有料で利用者100万人以上のサービスを提供する電気通信事業者を、電気通信設備を適正に管理すべき電気通信事業者として総務大臣が指定。
現在、（株）NTTぷらら、ニフティ（株）、ビッグローブ（株）、GMOインターネット㈱の4社が指定されている。

- 上記事業者は、事業用電気通信設備の使用を開始しようとするときは、技術基準※2に適合することを自ら確認し、その結果を当該設備の使用開始前に総務大臣に届け出なければならない。［法第42条］

※2　①電気通信設備の損壊又は故障により、電気通信役務の提供に著しい支障を及ぼさないようにすること、②電気通信役務の品質が適正であるようにすること、③通信の秘密が侵されないようにすること、④利用者又は他の電気通信事業者の接続する電気通信設備を損傷し、又はその機能に障害を与えないようにすること、⑤他の電気通信事業者の接続する電気通信設備との責任の分界が明確であるようにすること、が確保されるものとされ、詳細は事業用電気通信設備規則（総務省令）で規定。

＜電気通信役務の種類に応じた事業用電気通信設備の技術基準＞



※3 携帯電話の品質基準は、電波の伝搬状態に応じて通話品質が影響を受けることを考慮し、基準を一律に定めるのではなく、自主基準としている。

（参考）事業用電気通信設備の技術基準と自己確認届出（携帯電話用設備の例）

○事業用電気通信設備の技術基準

（事業用電気通信設備規則(省令)第2章）

第1節 電気通信設備の損壊又は故障の対策
（予備機器等、故障検出、設備の防護措置、試験機器・応急復旧機材の配備、異常ふくそう対策等、耐震対策、電源設備、停電対策、誘導対策、防火対策、屋外設備の防護措置、建築物等の防護措置、大規模災害対策）

第2節 秘密の保持
（通信内容の秘匿措置、蓄積情報保護）

第3節 他の電気通信設備の損傷又は機能の障害の防止
（損傷防止、機能障害の防止、保安装置、異常ふくそう対策）

第4節 他の電気通信設備との責任の分界
（分界点、機能確認）

第5節 音声伝送役務の提供の用に供する電気通信設備
（基本機能、通話品質、接続品質、総合品質、緊急通報の機能、災害時優先通信の優先的取扱い、異なる電気通信番号の送信の防止等）

○技術基準適合自己確認の届出書類

（電気通信事業法施行規則(省令)(以下「施行規則」という。)第27条の5）

(全般)

① 交換設備、伝送路設備及びこれらの附属設備の設備構成図（これらの設備の全部又は一部の機能をソフトウェアが制御することにより仮想化した当該機能を論理的に構成する場合にあつては、当該機能に係る論理的な構成を具体的に示した設備構成図を含む）並びにこれらの接続構成図

② 交換設備、伝送路設備及びこれらの附属設備における予備設備の設置等に関する説明書

③ 交換設備、伝送路設備及びこれらの附属設備における故障等の検出方式及び通知方式に関する説明書

④ 電気通信設備における利用者又は他の電気通信事業者の電気通信設備から受信するプログラムの機能制限等の防護措置に関する説明書

⑤ 電気通信設備の工事、維持及び運用を行う事業場に配備している主要試験機器の一覧

⑥ 電気通信設備の工事、維持及び運用を行う事業場に配備している主要応急復旧機材の一覧

⑦ 交換設備における異常ふくそう検出方式及びその対策方式に関する説明書

⑧ トラヒックの瞬間的かつ急激な増加及び制御信号の増加の対策措置に関する説明書

⑨ 交換設備、伝送路設備及びこれらの附属設備における耐震措置に関する説明書

⑩ 停電対策措置に関する説明書

⑪ 線路設備における誘導対策措置に関する説明書

⑫ 電気通信設備を設置している通信機械室等における自動火災報知設備及び消火設備の設置状況に関する説明書

⑬ 屋外設備の設置に関する説明書

⑭ 電気通信設備を設置する建築物等における自然災害等の対策措置及び不法侵入防止措置に関する説明書

⑮ 通信内容の秘匿措置に関する説明書

⑯ 電気通信設備に蓄積する利用者の通信に係る情報の保護措置に関する説明書

⑰ 電気通信設備と利用者又は他の電気通信事業者の事業用電気通信設備との間における保安装置の設置に関する説明書

⑱ 電気通信設備と利用者又は他の電気通信事業者との間における分界点の場所に関する説明書

⑲ 分界点における電気通信設備の正常性確認方式に関する説明書

⑳ 音声伝送用設備における端末設備等の接続条件に関する書類及び試験結果

㉑ 接続品質に関する設計値及びその根拠に関する説明書

㉒ 緊急通報を扱う事業用電気通信設備に関する説明書

㉓ 災害時優先通信を優先的に取り扱う事業用電気通信設備に関する説明書

㉔ 異なる電気通信番号の送信の防止措置に関する説明書

(参考)事業用電気通信設備の管理規程

- 事業用電気通信設備の技術基準適合維持義務が適用される電気通信事業者は、電気通信役務の確実かつ安定的な提供を確保するため、電気通信事故の事前防止や発生時に必要な取組のうち、**技術基準等で画一的に定めることが必ずしも適当でなく、電気通信事業者ごとの特性に応じた自主的な取組により確保すべき事項を「管理規程」**として定め、総務大臣に届け出なければならない。[法第44条]

管理規程に定める事項(法第44条)

電気通信事業者が定める管理規程
(施行規則第29条(一部は告示も含む)に基づく内容)

○○株式会社　事業用電気通信設備管理規程

○事業用電気通信設備の管理の方針に関する事項

- 組織の全体的かつ部門横断的な設備の管理の方針……○
- 関係法令、管理規程その他の規定の遵守……○
- 通信需要、相互接続等を考慮した設備の管理の方針……○
- 災害を考慮した設備の管理の方針……○
- 情報セキュリティの確保のための方針……○

○事業用電気通信設備の管理の体制に関する事項

- 経営の責任者の職務……○
- 電気通信設備統括管理者の職務……○
- 電気通信主任技術者の職務及び代行……○
- 各部門の責任者の職務に関すること……○
- 各従事者の職務……○
- 組織内の連携体制の確保……○
- 組織外の関係者との連携及び責任分担……○

○事業用電気通信設備の管理の方法に関する事項

- 基本的な取組……○
- 設備の設計、工事、維持及び運用に従事する者に対する教育及び訓練等の実施……○
- 設備の設計、工事、維持及び運用……○
- 通信量の変動を踏まえた適切な設備容量の確保……○
- 情報セキュリティ対策……○
- ソフトウェアの信頼性の確保……○
- 重要通信の確保及びふくそう対策……○
- 緊急通報の確保……○
- 防犯対策……○
- 取組の実施状況等現状の調査、分析及び改善……○
- ふくそう、事故、災害その他非常の場合の報告、記録、措置及び周知……○
- 利用者の利益の保護の観点から行う利用者に対する情報提供……○
- 事故の再発防止のための対策……○

○電気通信設備統括管理者の選任に関する事項

- 電気通信設備統括管理者の選任及び解任……○

- 管理規程の見直し……○
- その他……○

（参考）電気通信設備統括管理者の制度

- 事業用電気通信設備の技術基準適合維持義務が適用される電気通信事業者は、**経営陣の事故防止の取組に関する認識の向上や関与の強化を図るため、経営レベルの設備管理の責任者として、「電気通信設備統括管理者」**の選任が義務付けられている。
- これにより、設備管理の専門化・細分化や外部委託等が進む中で、社内・社外の全体調整を含め、**事故防止の方針・体制・方法への経営陣の主体的関与を強化し、「管理規程」等に基づく事故防止の取組の実効性を確保**。

電気通信事業者による選任義務等

- 電気通信事業者は、電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の方針・体制・方法に関する事項に関する業務を統括管理させるため、事業運営上の重要な決定に参画する管理的地位にあり、かつ、電気通信設備の管理に関する一定の実務の経験その他の総務省令で定める要件※1を備える者のうちから、電気通信設備統括管理者を選任※2しなければならない。【法第44条の3】

※1　電気通信事業の用に供する電気通信設備の設計、工事、維持又は運用に関する業務又はこれらの業務を監督する業務に三年以上従事した経験を有すること等。【施行規則第29条の2第1項】

※2　管理規程に定める「電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の方針・体制・方法に関する事項」に関する業務を開始する前に、電気通信設備統括管理者を選任しなければならない。【施行規則第29条の2第2項】

- 電気通信事業者は、電気通信役務の確実かつ安定的な提供の確保に関し、電気通信設備統括管理者のその職務を行う上での意見を尊重しなければならない。【法第44条の4第2項】

総務大臣による解任命令

- 電気通信設備統括管理者の事故防止に果たす重要性に鑑み、その職務を怠ることによって事故防止が適切に図られていないと認める場合は、総務大臣が、解任を命じることができる。【法第44条の5】

（参考）情報通信ネットワーク安全・信頼性基準（昭和62年2月14日郵政省告示第73号）

- 情報通信ネットワーク全体から見た対策項目につき網羅的に整理・検討を行い、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持・運用等を総合的に取入れた安全・信頼性に関する**推奨基準（ガイドライン）**として策定
- 技術基準等の対象となるネットワーク（回線設置事業者、ユニバーサルサービス提供事業者、有料で利用者100万以上のサービス提供する回線非設置事業者のもの）に加え、自営情報通信ネットワークやユーザネットワークも対象
- 全国5Gの特定基地局の開設指針等において、サプライチェーンリスクを考慮した機器調達（基地局、ネットワーク設備）を申請者に促すため、認定の条件として、本基準に留意することを規定

1.設備等基準 … 情報通信ネットワークを構成する設備及び情報通信ネットワークを構成する設備を設置する環境の基準（65項目171対策）

第1 設備基準 47項目121対策	1.一般基準（15項目67対策）	2.屋外設備（17項目22対策）	3.屋内設備（8項目13対策）	4.電源設備（7項目19対策）
第2 環境基準 18項目50対策	1.センタの建築（4項目13対策）	2.通信機器室等（6項目22対策）	3.空気調和設備（8項目15対策）	

2.管理基準 … 情報通信ネットワークの設計、施工、維持及び運用の管理の基準（43項目178対策）

第1 方針 9項目9対策	1.全体的・部門横断的な設備管理（3項目3対策）	2.関係法令等の遵守（1項目1対策）	3.設備の設計・管理（2項目2対策）	4.情報セキュリティ管理（3項目3対策）
第2 体制 18項目46対策	1.情報通信ネットワークの管理体制（2項目8対策）	2.各段階における体制（16項目38対策）		
第3 方法 16項目123対策	1.平常時の取組（13項目100対策）	2.事故発生時の取組（2項目17対策）	3.事故収束後の取組（1項目6対策）	

指針 … 管理基準に基づく指針　**情報セキュリティポリシー策定のための指針**　**危機管理計画策定のための指針**

解説 … 全ての対策項目に関する措置例等について参考として解説