資料１－３

現状と課題等について

令　和　３　年　５　月　12　日

電気通信事業ガバナンス検討会

事　　務　　局

目次

1. 現状

１－１．データの取扱い等

構成員限り
（P４～P20）

電気通信事故の発生概況

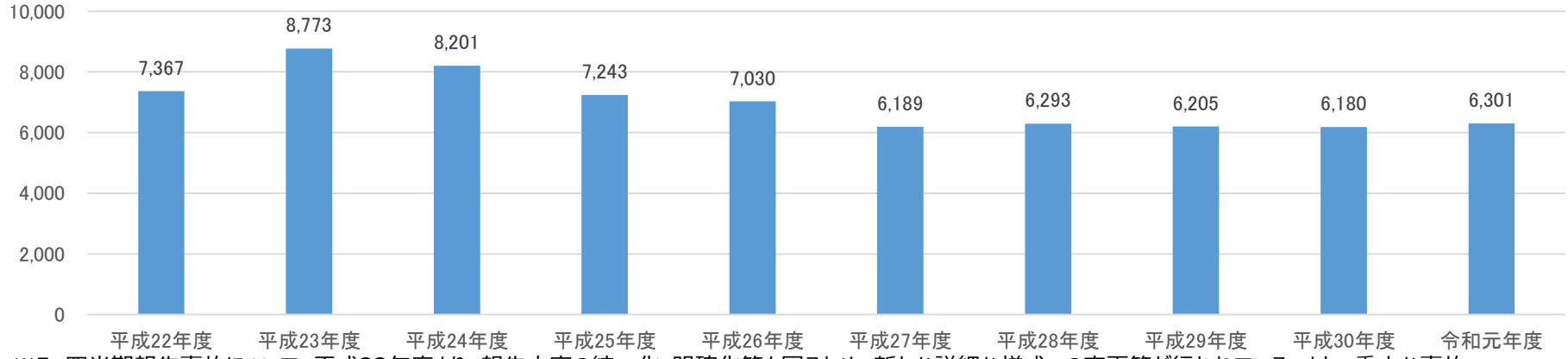
■令和元年度に報告された電気通信事故

（括弧内は前年度（平成30年度）の数値）

	報告事業者数	報告件数
重大な事故	5社※1 （6社※1）	3件 （4件）
四半期報告事故		
詳細な様式による報告※3	111社 （132社）	6,301件※2（6,180件※2）
簡易な様式による報告※4	24社 （27社）	58,211件 （62,240件）

※1 卸役務に関する事故については、報告事業者数として卸提供元事業者及び卸提供先事業者の両方が含まれているため、報告事業者数が報告件数よりも多くなっている。
※2 卸役務に関する事故については、当該事故における卸提供元事業者及び卸提供先事業者の両方からの報告件数が含まれている。
※3 重大な事故については、施行規則様式第50の3に加え、電気通信事業報告規則様式第27により報告することとされているため、詳細な様式による報告に含まれている。
※4 ①無線基地局、②局設置遠隔収容装置又はき線点遠隔収容装置及び③デジタル加入者回線アクセス多重化装置の故障による事故については、簡易な様式による報告が認められている。

■事故発生件数（詳細な様式による報告分）の年度ごとの推移※5



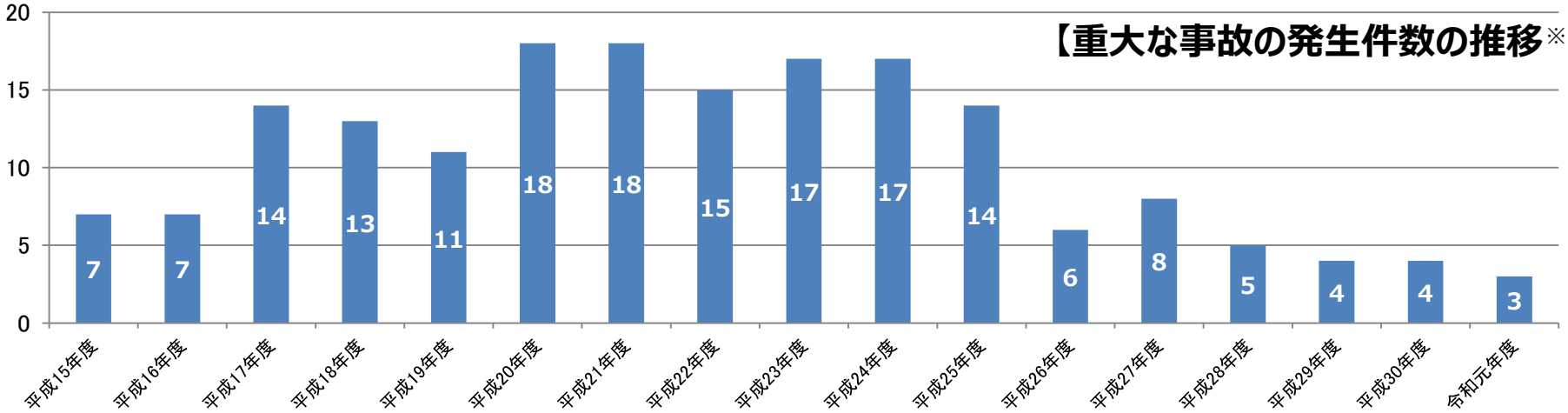
※5 四半期報告事故について、平成22年度より、報告内容の統一化・明確化等を図るため、新たな詳細な様式への変更等が行われている。また、重大な事故について、電気通信サービスの多様化・高度化・複雑化等に伴い、それまでのサービス一律の報告基準（影響利用者数３万以上かつ継続時間２時間以上）から見直しが行われ、平成27年度からはサービス区分別の基準に基づき報告が行われている。

重大な事故等の発生状況

■ 令和元年度において、**重大な事故は３件**発生。サービス区分別の報告基準に改正された平成27年度以降で発生件数は最少。なお、サービス一律の報告基準であった時期も含め、平成15年以降で**最少**。

■ 令和元年度の重大な事故等は、主に**データ通信サービス（MVNO）**等、**新たな技術・ビジネスモデルや携帯事業への新規参入**等に関するもの。**ベンダ等含め国内外の多様な事業者の連携**という点で特徴的。

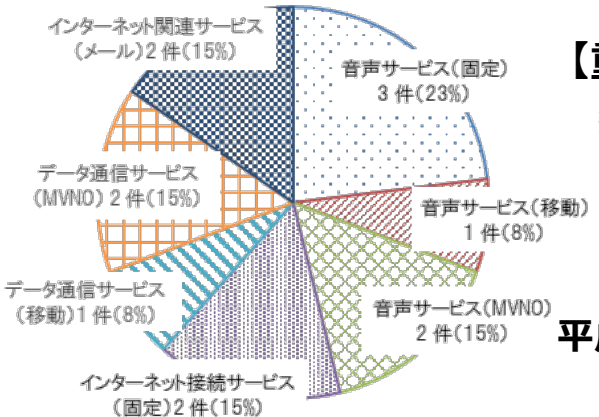
【重大な事故の発生件数の推移※】



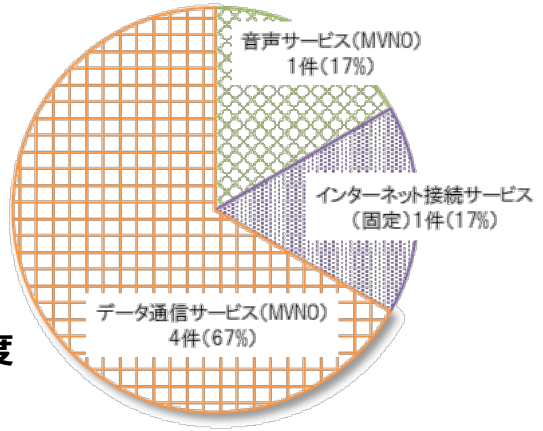
※　報告件数。なお、重大な事故について、平成20年度から、電気通信役務の品質が低下した場合も重大な事故に該当することとなり、さらに、平成27年度から、電気通信サービス一律から電気通信サービスの区分別に重大な事故に該当する基準が定められており、年度ごとの推移は単純には比較できない。

【重大な事故のサービス別内訳※】

※　報告のあった１件の事故について、複数のサービスに同時に影響している場合があるため、それらの場合を含めたものとなっている。



平成30年度



令和元年度

「企業のリスクマネジメントおよびクライシスマネジメント実態調査2020」

- デロイトトーマツグループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査2020年版」（令和年3月）において、「サイバー攻撃・ウイルス感染等による情報漏えい」が国内第3位・海外第5位となり、ともに順位が上昇。
- また、「グループガバナンスの不全」については、国内第8位で上昇し、前回同様で海外第2位になるとともに、新たな選択肢である「事業に影響するテクノロジーの変革」が国内第7位、海外第9位。

2020年はCOVID-19の影響に加え、気候変動・サイバー攻撃等の外部環境変化への対応やDX対応・グループガバナンス等の内部変革が上場企業の課題として浮き彫りになった

日本国内と海外拠点それぞれにおける、優先して着手が必要と思われるリスク（Q2、Q4のサマリー）

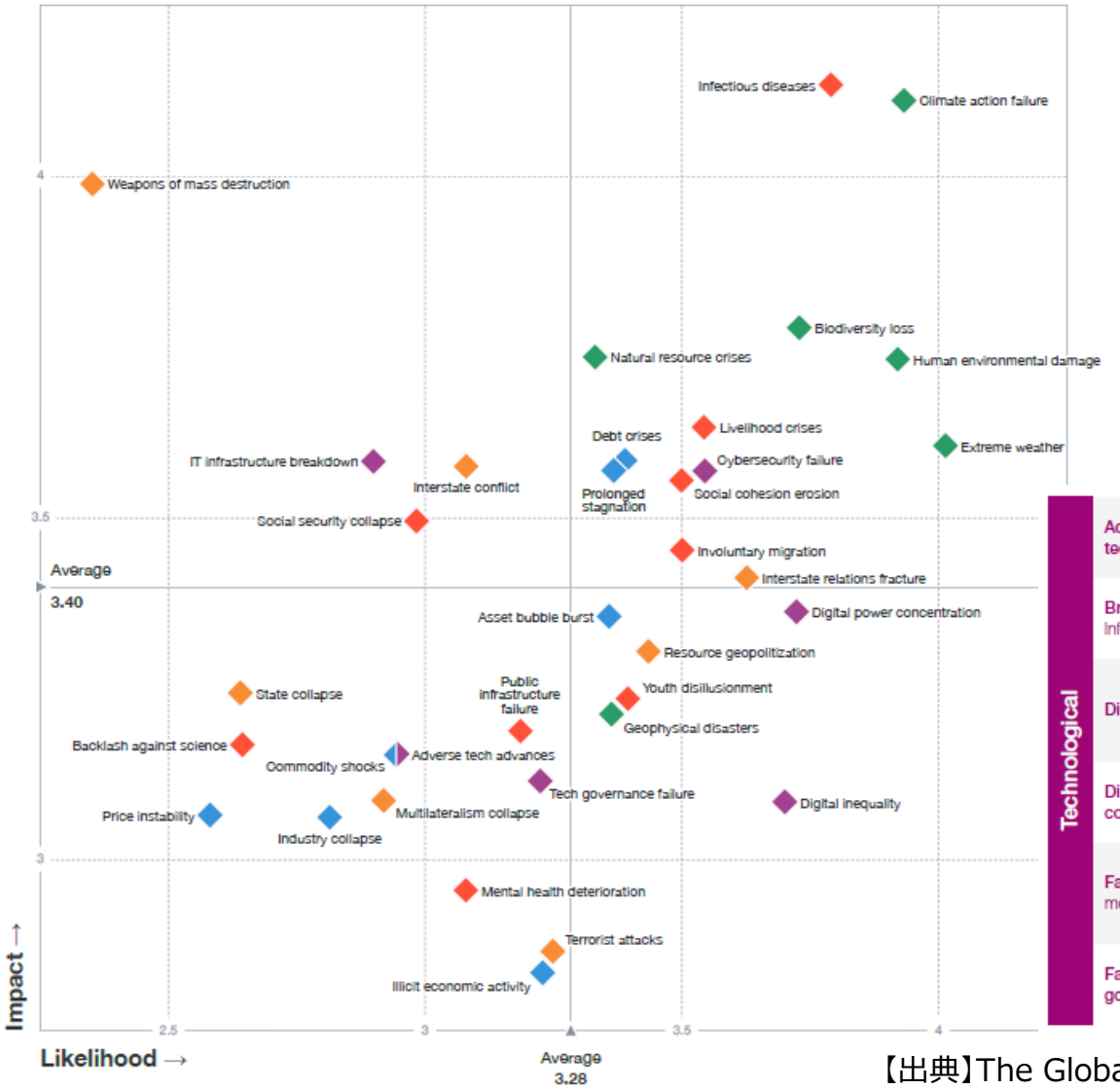
日本国内			海外拠点	
疫病の蔓延（パンデミック）等の発生（②）	34.4%（24）	第1位	疫病の蔓延（パンデミック）等の発生（②）	39.6%（27）
異常気象（洪水・暴風など）、大規模な自然災害（地震・津波・火山爆発・地磁気嵐）（②）	30.9%（1）	第2位	グループガバナンスの不全（⑦）	18.5%（2）
サイバー攻撃・ウイルス感染等による情報漏えい（⑩）	21.3%（5）	第3位	異常気象（洪水・暴風など）、大規模な自然災害（地震・津波・火山爆発・地磁気嵐）（②）	13.5%（5）
人材流失、人材獲得の困難による人材不足（⑪）	19.5%（2）	第4位/第3位	製品/サービスの品質チェック体制の不備（⑨）	13.5%（3）
製品/サービスの品質チェック体制の不備（⑨）	15.7%（4）	第5位	サイバー攻撃・ウイルス感染等による情報漏えい（⑩）	11.7%（10）
長時間労働、過労死、メンタルヘルス、ハラスメント等労務問題の発生（⑪）	12.5%（11）	第6位/第5位	人材流失、人材獲得の困難による人材不足（⑪）	11.7%（6）
事業に影響するテクノロジーの変革（⑤）	11.7%（-）	第7位	為替変動（③）	10.4%（8）
グループガバナンスの不全（⑦）	11.4%（9）	第8位	市場における価格競争（③）	9.5%（11）
市場における価格競争（③）	10.8%（7）	第9位	事業に影響するテクノロジーの変革（⑤）	9.0%（-）
サイバー攻撃・ウイルス感染等による大規模システムダウン（⑩）	10.8%（12）	第9位/第10位	従業員の不正・贈収賄等（⑧）	8.6%（4）

※（）カッコ内は前回順位
※各項目名に続く（）内の番号は、本調査において設けたリスクおよびクライシスの種類上の分類

【出典】デロイト トーマツ グループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020年版」(2021年３月)

「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））

電気通信事業者におけるデータの取扱い等に関する実態把握・自己点検

■現在、総務省において、関係業界団体の協力を得て、当該団体に加盟する電気通信事業者へアンケートを送付し、セキュリティ対策やデータの取扱いの実態について回答を求めるとともに、自身の制度及びその運用が適切なものになっているかに関する自己点検を依頼中。

対象団体

- 一般社団法人ICT-ISAC
- 一般社団法人テレコムサービス協会
- 一般社団法人電気通信事業者協会
- 一般社団法人日本インターネットプロバイダー協会
- 一般社団法人日本ケーブルテレビ連盟

結果の取扱い

個社名を伏せ、内容を一般化の上、
本検討会における検討資料として活用予定。

調査内容分類	質問項目（例）	自己点検内容（例）
サイバーセキュリティやデータの取扱いに関する社内規程	情報セキュリティポリシー及び危機管理計画の策定状況	左記の文書は、情報通信ネットワーク安全・信頼性基準に照らして適切なものになっているか？
サイバーセキュリティやデータの取扱いに関する社内体制	CISO（最高情報セキュリティ責任者）等の配置状況	サイバーセキュリティに関する体制（CSIRT、CISO等）は、適切なものになっているか？
情報通信NWのセキュリティ対策	情報通信NWで使用しているソフトウェア及びハードウェアの資産管理状況	電気通信事業用NW及びそれ以外の情報通信NW（社内LAN等）のセキュリティ対策は適切か？
情報通信NWへの不正な侵入の防止	情報通信NWへのアクセスに必要な本人認証	電気通信事業用NW及びそれ以外の情報通信NWに適切なアクセス制御をかけているか？
パーソナルデータの取扱いに係るガバナンスの確保	国内外におけるパーソナルデータの保管、委託状況	保管先/委託先での個人情報や通秘対象情報の適切な取扱いのために必要な措置を施しているか？
設備データの取扱いに係るガバナンスの確保	国内外における設備データの保管、委託状況	保管先/委託先での設備情報の適切な取扱いのために必要な措置を施しているか？
サイバーセキュリティに関するフレームワーク	ISMS認証ほか第三者認証の取得状況	―

１－２．安全・信頼性対策に関する制度

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3月31日現在）

登録 332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)】

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】

事業用電気通信設備の技術基準

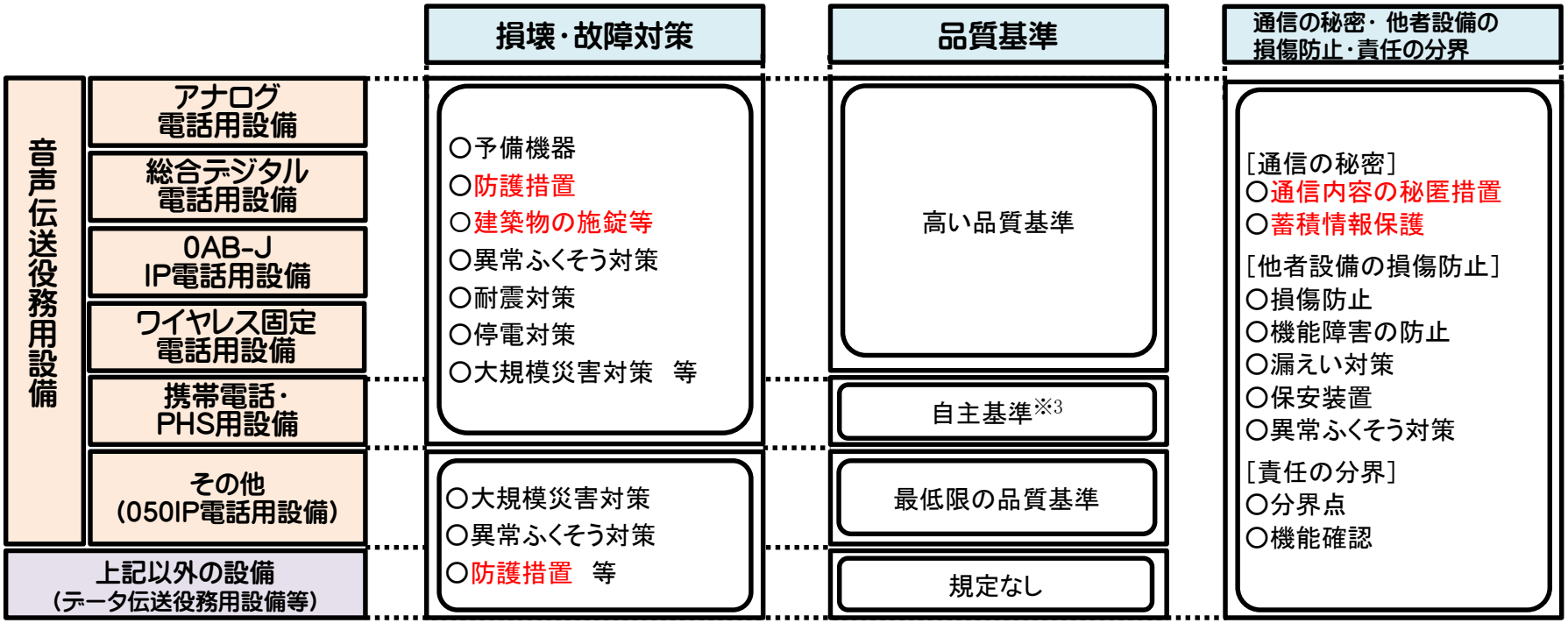
- 「電気通信回線設備(送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備)を設置する電気通信事業者」及び「内容、利用者の範囲等からみて利用者の利益に及ぼす影響が大きいものとして総務省令で定める電気通信役務を提供する電気通信事業者※1」等は、事業用電気通信設備を総務省令で定める技術基準※2に適合するように維持しなければならない。[電気通信事業法(以下「法」という。)第41条]

  ※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。

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

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……○

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

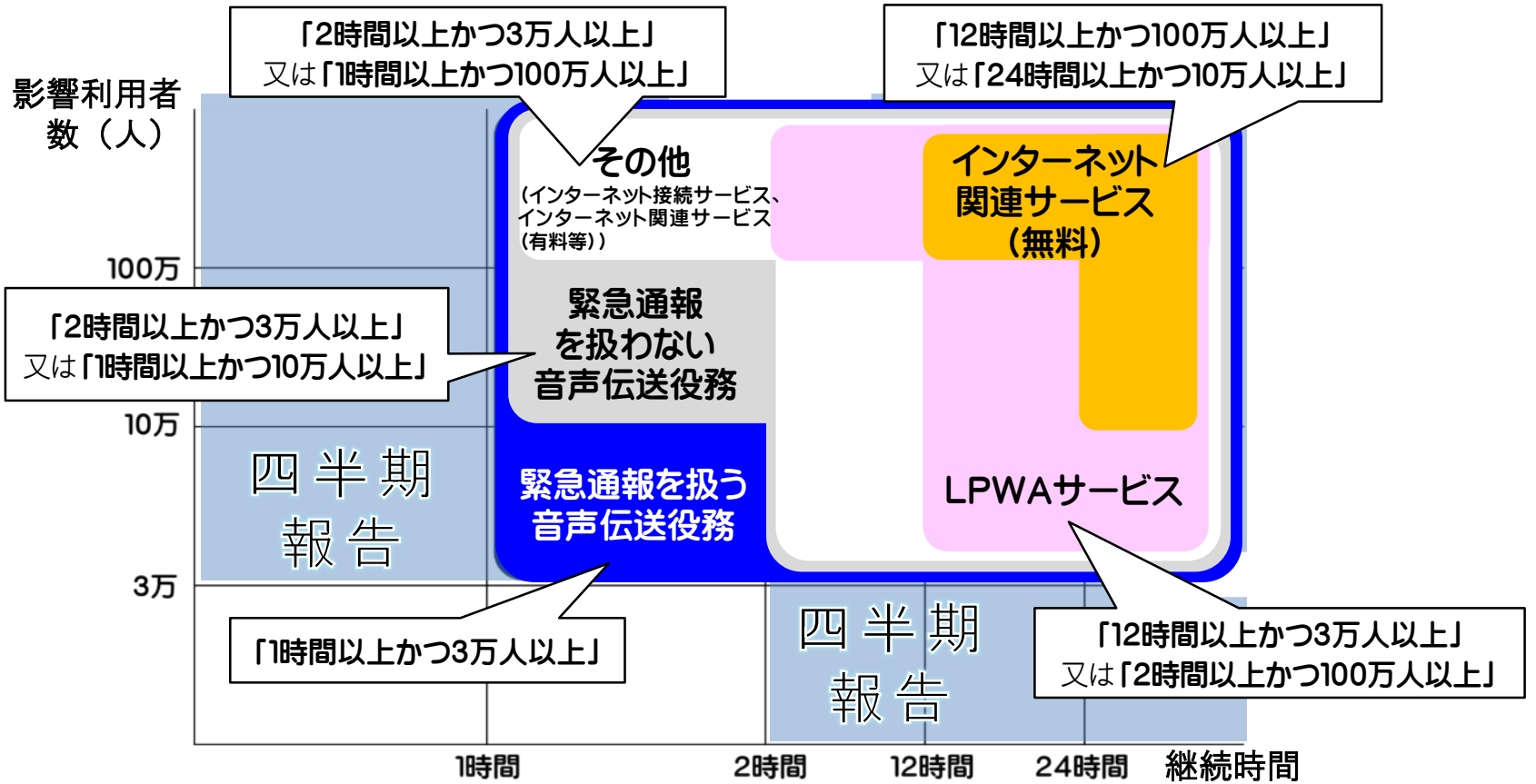
電気通信事故の報告制度の概要

● 通信事業者において、電気通信事業法※に基づき、総務大臣に対する報告を要する電気通信事故（電気通信設備の故障による電気通信役務の提供の停止又は品質の低下等）は、次の２つに大別。

①「重大な事故」：サービス毎の影響利用者数・継続時間の基準（下図参照）に該当、又は、
重要電気通信設備（衛星・海底ケーブル等）の故障により、全ての通信の疎通が２時間以上不能
（→ 事故後、速やかに一報、30日以内に報告書を提出）

②「四半期報告事故」：影響利用者数３万人以上又は継続時間２時間以上の事故（電気通信設備以外の設備の故障により電気通信役務の提供に支障を来した事故を含む）、又は、
電気通信役務の提供に支障を及ぼすおそれのある電気通信設備に関する情報の漏えい（インシデント）
（→ 四半期ごとに報告）

※電気通信事業法28条・166条、同法施行規則58条、電気通信事業報告規則7条の3



１－３．リスクマネジメント及び情報セキュリティに関する規格等

通信分野の安全・信頼性対策における「リスクマネジメント」の考え方

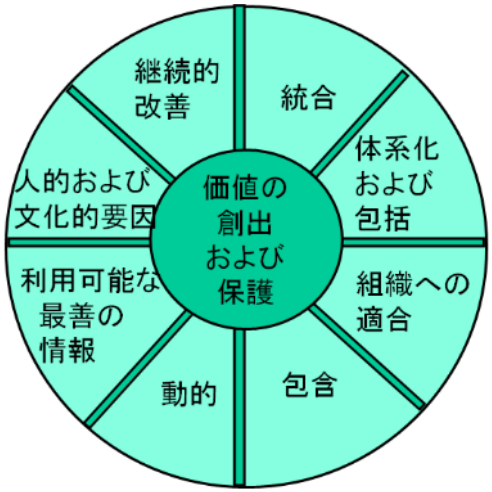
- 「リスクマネジメント」については、国内外で統一的な定義等がないため、関係者間における共通的な考え方や用語等を踏まえた取組が重要。
- 通信分野における安全・信頼性対策においては、「重要インフラの情報セキュリティ対策に係る第4次行動計画※」及び「重要インフラにおける機能保証に基づくリスクアセスメント手引書（第1版）※※」で参照する「ISO31000:2018」等における考え方等を基本的に活用し検討。

※令和2年1月サイバーセキュリティ戦略本部改定等

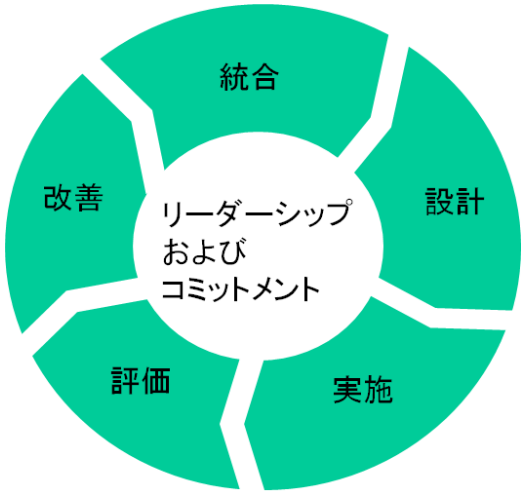
※※令和元年5月サイバーセキュリティ戦略本部重要インフラ専門調査会改定等

ISO31000:2018 リスクマネジメント-指針

- リスクマネジメント：リスク（目的に対する不確かさの影響）について組織を指揮統制するための調整された活動
- 2018年改正により、PDCAサイクルによるリスクマネジメントの継続的改善について、組織活動へのリスクマネジメントの統合及びそのためのトップマネジメントによるリーダーシップが必要であること等が新たに規定



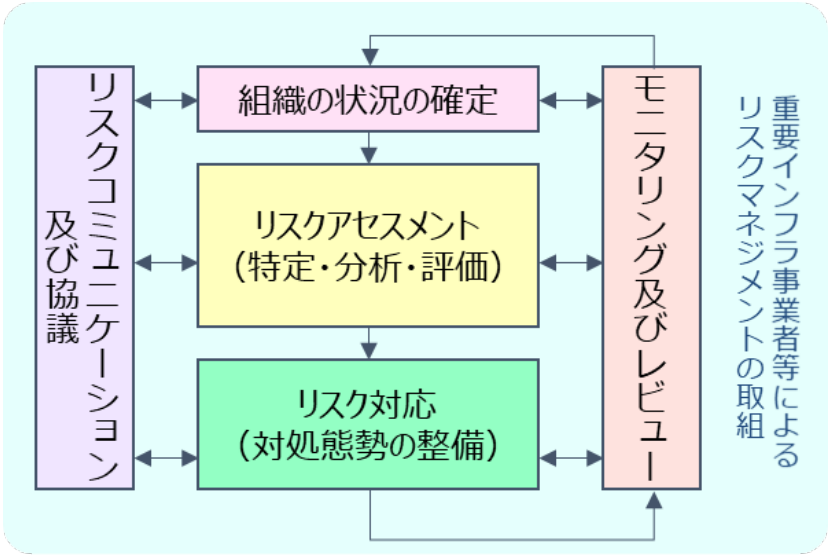
【原則　4章】



【枠組み　5章】

重要インフラにおける機能保証に基づくリスクアセスメント手引書（第1版）

- 経営戦略上の目的：社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスの提供を維持・継続すること
- リスク：目的に対する不確かさの影響。負の影響（好ましくない結果をもたらすリスク）に限定。



【出典】指田朝久（立教大学大学院21世紀社会デザイン研究科客員教授等）「リスクマネジメントと危機管理～想定内と想定外：原点に戻って考える～」（2020年4月26日事故報告・検証制度等TF第5回）等

ISO/IEC27000ファミリー

●ISO/IEC27000シリーズは、情報技術を扱うISO（国際標準化機構）及びIEC（国際電気標準会議）による国際規格。各組織において**情報セキュリティを確保するためのマネジメントを平時から運用・改善するための要求事項や管理策等を規定**。

JIS Q 27001
（国内規格）
JIS Q 27001に準拠した運用を認証する制度として、「ISMS認証※1」がある。

参照（同内容）

ISO/IEC27001
組織の業態を問わず、情報セキュリティ管理システム(ISMS)を構築・運用・改善するための要求事項を規定。

対応関係を整理

NIST SP800-53
NIST SP800-171

ISMSのための関連規格

JIS Q 27002
（国内規格）

参照（同内容）

ISO/IEC27002
ISO/IEC27001附属書Aに記載の管理策について、ベストプラクティスを整理。

セクターに特化

ISO/IEC27011
電気通信業界でのISO/IEC27002に基づく情報セキュリティ管理の実践のための規格。

共通規格（同内容）

ITU-T X.1051
ITU-Tにおけるセキュリティの Lead Study Groupである SG17による規格。

翻訳

JT X-1051
国内の情報通信ネットワークに関する標準化を扱う一般社団法人情報通信技術委員会(TTC)による規格。

用語の整理

JIS Q 27000
（国内規格）

ISO/IEC27000
ISO/IEC27000ファミリー規格の概要、用語等について規定。

ISO/IEC27005
情報セキュリティにおけるリスクマネジメント実施のための方法論をガイドライン化。

ISO/IEC27017
クラウドサービスでのISO/IEC27002に基づく情報セキュリティ管理の実践のための規格。

サイバーセキュリティに特化

ISO/IEC TS 27100
サイバーセキュリティの概念及びその情報セキュリティとの関連について整理※3。

JIS Q 27006
（国内規格）

参照（同内容）

ISO/IEC27006
ISMS認証を希望する組織の審査・認証を行う認証機関に対する要求事項を規定した規格。

JIS Q 27014
（国内規格）

参照（同内容）

ISO/IEC27014
ISO/IEC27001に規定するISMS内外の情報セキュリティガバナンスの目標と運用プロセスについて整理。

ISO/IEC27000ファミリー（抜粋）

参照（同内容）

JIS Q 27017
（国内規格）
JIS Q 27011に加えてJIS Q 27017に準拠した運用を認証する制度として、「ISMSクラウドセキュリティ認証※2」がある。

※1 一般社団法人情報マネジメントシステム認定センター(ISMS-AC)が認証機関の認定を行い、認証機関が各組織を審査の上、認証登録する制度。
認証取得組織数：6384（2021年4月19日現在）。
なお、電気通信事業者が同認証を取得する際には、ISO/IEC 27011（ITU-T X.1051）が参照される。

※2 制度の仕組みはISMS認証に同じ。
認証取得組織数：226（2021年4月21日現在）。

※3 本年、サイバーセキュリティのフレームワーク策定を支援するISO/IECTS 27110が策定されたが、この中では「識別、防御、検知、対応、復旧」の概念が用いられている。

NISTによるサイバーセキュリティに係る各種文書

● 米国NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は、政府機関や重要インフラ事業者におけるセキュリティ対策のために**サイバーセキュリティフレームワーク及びSP800シリーズを発行**。内容はリスク管理やセキュリティ技術に留まらず、**インシデント対応等の ISO/IEC27001に含まれないレジリエンスの観点も含む幅広いもの**となっている。

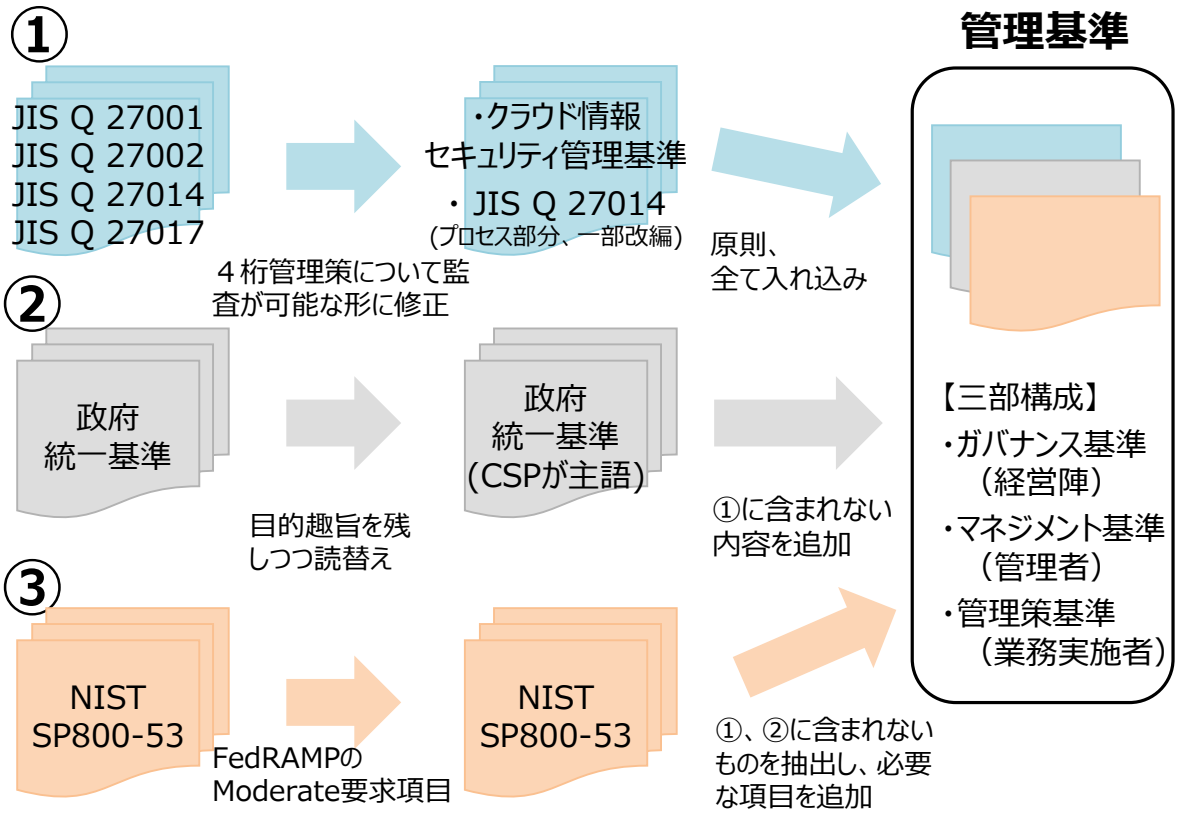
具体化

文書名	サイバーセキュリティフレームワーク （Framewrok for Improving Critical Infrastructure Cybersecurity: CSF）	情報システムと組織のための セキュリティとプライバシー管理 （NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations）	連邦政府外のシステムと組織における 管理対象の非機密情報の保護 （NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations）
最新版の発行年月	2018.4（version 1.1） 【変更ポイント】サプライチェーンリスク管理の説明等を追加	2020.12（revision 5） 【変更ポイント】セキュリティとプライバシーの統合カタログ化	必要な要件を抽出 2020.2（revision 2） 【変更ポイント】サプライチェーンリスク管理対策等の充実化
想定読者	重要インフラ事業者	• 米国の政府機関のシステム関係者、契約担当者、監査人等 • IT製品や情報セキュリティ関連企業	米国の政府機関及び（政府機関から委託を受ける）民間企業のシステム関係者、契約担当者、監査人等
管理対象となる情報	指定なし	機密情報 （Classified Information, CI）	管理対象非機密情報 （Controlled Unclassified Information, CUI）
内容	組織がサイバーセキュリティ対策を開始/改善する際の概念（識別、防御、検知、対応、復旧）及び手順を整理。 優先順位・範囲決定 → 方向付け → プロファイル作成 → リスク評価 目標プロファイル作成 → ギャップ分析 → 行動計画実施 ※ プロファイルの作成にあたっては、組織の対策状況を数値化したティア(Tier)を考慮	• サイバーセキュリティ対策とプライバシー管理の取組カタログ集。 • 組織の責務等を踏まえたサイバーセキュリティ及びプライバシー管理策の策定・調整プロセスを整理。	CUIが政府機関外に置かれる際、その保護のために要求する、14の具体的なセキュリティ要件（※）を整理。 ※ システムと通信の保護、監査と責任追跡性、インシデント対応等
本文書をベースとした認証制度	―	**FedRAMP認証** （Federal Risk and Authorization Management Program：連邦リスク・認証管理プログラム） • NIST SP 800-53 rev.4に基づく、クラウド製品・サービスに対する第三者によるセキュリティ評価と継続的なモニタリング制度（現在rev.5を踏まえた改訂中）。 • 自社のクラウドサービスを米国政府機関に提供しようとする事業者は、認証を取得し、継続的にモニタリングを受けることが必要。	**CMMC認証** （Cybersecurity Maturity Model Certification：サイバーセキュリティ成熟度モデル認証） • 防衛関連の調達に関して、米国政府機関が調達先組織のCUI及び連邦契約情報（FCI）の管理水準を評価するための第三者による認証制度。 • NIST SP 800-171 rev.1等のセキュリティ基準を組み合わせ、ベストプラクティスとプロセスを5段階の成熟度レベル別にマッピングするもの。

政府情報システムのためのセキュリティ評価制度」（ISMAP）

- 「政府情報システムのためのセキュリティ評価制度」(ISMAP：Information system Security Management and Assessment Program) を令和2年6月に立上げ。
- 国際標準等を踏まえて策定した基準に基づき、各基準が適切に実施されているか監査するプロセスを経て、基準を満たすクラウドサービスを登録する制度。
- 各政府機関は、原則、安全性が評価され「登録簿」に掲載されたサービスから調達。
- 令和3年3月10日、第1弾として10サービスを登録・公表。

ISMAP管理基準の構成



現在登録されているサービス

No.	サービス名	申請者
1	OpenCanvas (IaaS)	株式会社エヌ・ティ・ティ・データ
2	FUJITSU Hybrid IT Service FJcloud	富士通株式会社
3	Apigee Edge	Google LLC
4	Google Cloud Platform	Google LLC
5	Google Workspace	Google LLC
6	Salesforce Services	株式会社セールスフォース・ドットコム
7	Heroku Services	株式会社セールスフォース・ドットコム
8	Amazon Web Services	Amazon Web Services Inc.
9	NEC Cloud IaaS	日本電気株式会社
10	KDDIクラウドプラットフォームサービス	KDDI株式会社

２．主な検討課題(案)

（１）電気通信事業法の目的・関連規定

① **電気通信事業法**は、**「電気通信サービスの円滑な提供を確保」するとともに、「利用者の利益を保護」**し、もって**電気通信の健全な発達と国民の利便性の確保**を図ることとしている（電気通信事業法第1条）。

② 以上のための具体的な措置として、1）**通信の秘密に係る情報の漏えいの防止**（通信の秘密の保護）、2）**通信設備の故障等によるサービス提供への支障の防止**（確実かつ安定的なサービス提供の確保）のための規定を定めている。

③ 具体的には、

1. **通信の秘密に係る情報の漏えいの防止**に関しては、通信設備の技術基準等の他、**通信の秘密を侵した者に対する罰則**を定めている。
2. **通信設備の故障等によるサービス提供への支障の防止**に関しては、一部の電気通信事業者（回線設備を設置する事業者等）に対し、1）**通信設備について、技術基準に適合するよう維持・自己確認しなければならない旨**、2）**管理規程の作成・届出**、3）**電気通信設備統括管理者の選任**等を**義務づけ**ている。
3. **これらの規律の実施を確保するための規定**として、1）電気通信事業者による業務の方法に関し**通信の秘密の確保に支障がある場合や事故によるサービス提供への支障を除去するために必要な措置を速やかに行わない場合の業務改善命令**、2）通信設備が技術基準に適合していないと認める場合における**技術基準適合命令**、3）**管理規程の変更・遵守命令**、4）**電気通信設備統括管理者の解任命令**等を、**総務大臣が発することができる旨**を定めている。

序：検討の背景等②

（１）電気通信事業法の目的・関連規定［続き］

④ このほか、1）**通信の秘密の漏えい**や、2）**通信設備の故障によるサービスの提供停止等の重大事故**が発生した場合には、**総務大臣への速やかな報告義務**を課すことにより、サービスの円滑な提供及び利用者の利益を確保するため、早期の対処や被害拡大の防止等を図ることとしている。

⑤ また、1）**通信設備に関する情報の漏えいによりサービス提供に支障を及ぼすおそれ（インシデント）**、2）**通信設備以外の設備の故障によるサービス提供への支障等が発生した場合**には、**総務大臣への定期的（四半期毎）な報告義務**を課することにより、事故発生状況の統計分析等による必要な政策の立案等を図ることとしている。

⑥ しかしながら、昨今、電気通信事業者において、**取扱うデータ（通信の秘密に係る情報や通信設備に関する情報等）の漏えい等のデータ管理に関するリスク**や、**通信設備の故障によるサービスの提供停止等のリスク**が高まっており、**現状の制度では、電気通信サービスの円滑な提供を確保するとともに、利用者の利益を保護することが困難になってきている面もあるのではないか**と考えられる。

（２）データ管理に関するリスクの高まり

① 電気通信事業者が取扱う**データの管理に関するリスクの高まりの背景**として、以下のような状況変化があるのではないか。

1. **業務委託**のほか、他事業者との連携、データセンターの分散やクラウド化の進展など、**情報の処理方法や保管場所の多様化**

   （⇒*【検討課題A】委託先等における情報漏えい等のおそれ*）

2. 電気通信サービスを提供する**システムのソフトウェア化や多様化**

   （⇒*【検討課題B】設定ミスによる内部からの情報漏えいやネットワーク情報の誤入力等のおそれ*）

3. **サイバー攻撃の巧妙化・多様化・悪質化**

   （⇒*【検討課題C】サイバー攻撃による情報漏えいや改ざん等のおそれ*）

序：検討の背景等③

（３）通信設備の故障によるサービスの提供停止等のリスクの高まり

① **通信設備の故障によるサービスの提供停止等のリスクの高まりの背景**として、以下のような状況変化があるのではないか。

1. 電気通信サービスに関する**システムの高度化・マルチステークホルダー化**

（⇒*【検討課題A】委託先等における設備の故障等のおそれ*）

（⇒*【検討課題B】設定ミスや委託先等関係者の連携不足等による設備の故障等のおそれ*）

2. **サイバー攻撃の巧妙化・多様化・悪質化**

（⇒*【検討課題C】サイバー攻撃による設備の故障等のおそれ*）

（４）リスクマネジメント等によるガバナンス確保の必要性の高まり

① このほか、電気通信事業者において、取扱うデータの漏えい等のデータ管理に関するリスクや、通信設備の故障によるサービスの提供停止等のリスク等に対して、**定期的なリスク評価等により対策の実施を確保するリスクマネジメントやガバナンス確保の必要性の高まりの背景**として、以下のような状況変化があるのではないか。

1. 電気通信事業者が取扱うデータの漏えい等のデータ管理に関するリスクや、通信設備の故障によるサービスの提供停止等に関するリスク等、**電気通信事業を取巻くリスクの急速な多様化・深刻化・拡散と特定困難なリスクの増加**

（⇒*【検討課題D】リスク対策の実施の確保（ガバナンス）*）

主な検討課題（案）①

【A】委託先等における情報漏えいや設備の故障等のおそれへの対策

① 委託先等（業務提携先、通信設備等の保守管理・運用先やクラウド等外部のデータ保管場所を含む。以下同じ。）を通じて電気通信事業者が取扱うデータが外部に流出するリスク等が生じていることから、そのリスクを最小限にするために、電気通信事業者において、データの適切な取扱い等を確保するための**委託先等の監督の在り方**について、どう考えるか。

② 電気通信事業者における委託先等の選定に当たって、**リスクを十分に評価**することが必要ではないか。特に、外国の事業者を委託先等に選定する場合には、**外国の法的環境による影響等を含めたリスク評価の在り方**について、どう考えるか。

③ 電気通信事業者が取扱うデータについて、**海外における委託先等の場合**は、利用者による電気通信サービスの選択に資する観点から、どの委託先等にどのような目的でデータの提供等をしているか等、**委託先等に係る利用者への情報開示や説明の在り方**について、どう考えるか。

主な検討課題（案）②

【B】設定ミスによる自社内からの情報漏えい、ネットワーク情報の誤入力や委託先等関係者の連携不足等による設備の故障等のおそれへの対策

① 電気通信事業者の内部からの情報漏えいにつながる設定ミス等のおそれの高まりの背景として、具体的には、通信設備やその他の設備（社内業務用システム等）において、情報を閲覧・処理等するための**システムのソフトウェア化・多様化**の進展のほか、それに伴う**システムの開発プロセスの複雑化**や**関与するステークホルダーの増加や関係の複雑化**があるのではないか。

② 通信設備やその他の設備（社内業務用システム等）におけるシステムの**ソフトウェア化・多様化の進展に対応したセキュリティ対策の強化の在り方**について、どう考えるか。例えば、開発プロセスにおける権限分離・アクセス管理強化・セキュリティチェックの徹底など、開発プロセスに対するガバナンスの強化等について、どう考えるか。

③ そのほか、**他の事業者によるネットワーク情報の誤入力**や**委託先等関係者の連携不足**等に起因して、通信設備の故障等が発生するケースに対処するため、**電気通信事業者間による連携・協力の確保の在り方**について、どう考えるか。

主な検討課題（案）③

【C】サイバー攻撃による情報漏えいや改ざんや設備の故障等のおそれへの対策

① サイバー攻撃については、**攻撃手法の巧妙化のみならず、目的・狙いも多様化・悪質化**しているのではないか。

1. **従業員やユーザになりすまして侵入するケース**や、ログが消去されるなど、**侵入した痕跡を残さない**ように努めたと推測されるケースも発生し、不正なアクセスがあったと気づくのに時間がかかる、又は、気づくのが困難なケースが顕在化している。更に、実際に気づいていないケースも少なからずある可能性も考えられる。

2. 社内業務用システムなど、**通信設備以外の設備におけるシステムに侵入し、又は、それを経由して通信設備に侵入**するケースや、サービスの提供停止に至らない侵入・攻撃によるケースも発生している。これらの狙いは、**通信設備やその他の設備等の機微情報に関するデータの窃取**、又は、大規模通信障害を引き起こす準備等も想定される。

3. 前述の検討課題Ａ及びＢによる脆弱性が、サイバー攻撃リスクの拡大に輪をかけている側面も考えられる。

② 電気通信事業者における**基本的なサイバーセキュリティ対策やマインドの醸成の在り方**について、どう考えるか。例えば、定期的なデータや資産の管理、ユーザ認証の強化、定期的なアップデート、社員研修等が適切に実施されていないのではないか。

③ 社員の認証情報が漏えいすることを前提として、電気通信事業者における**外部からのなりすましによる侵入を防ぐための対策の在り方**について、どう考えるか。例えば、振る舞い検知、エンドポイントセキュリティ、従業員の認証強化・アクセス管理、社内システムへのアクセスログの保存・監査等を講じる必要があるのではないか。

主な検討課題（案）④

【C】サイバー攻撃による情報漏えいや改ざんや設備の故障等のおそれへの対策［続き］

④ **通信設備やその他の設備（社内業務用システム等）におけるシステムに関する機微情報**など、通信の秘密に係る情報以外のデータについて、電気通信事業者における保護対策の在り方について、どう考えるか。

⑤ **通信設備以外の設備（社内業務用システム等）**について、電気通信事業者における安全・信頼性対策の確保の在り方について、どう考えるか。

⑥ そのほか、一事業者のみでは迅速・効果的な対処に限界があるサイバー攻撃への対応のため、例えば、攻撃元情報の共有など、**電気通信事業者間による連携・協力の確保の在り方**について、どう考えるか。

主な検討課題（案）⑤

【D】電気通信事業者における各種対策の実施の確保（ガバナンス）

① データ管理やサイバーセキュリティ対策の実施状況の定期的なチェックなど、電気通信事業者による**リスク評価などリスクマネジメントの在り方**について、どう考えるか。

② 電気通信事業者内における組織全体で対策の実施を確保するための**責任者の設置等の社内体制の在り方**について、どう考えるか。

③ リスクマネジメント等によるガバナンスの確保について、例えば、**ISMS規格等に関する第三者認証やNISTによる関連文書の活用の在り方**について、どう考えるか。

④ 利用者の多寡等に関わらず、電気通信事業法におけるガバナンスに関する規律（技術基準への適合維持義務、管理規程の策定や電気通信設備統括管理者の選任等）の対象外となっている、1）**電気通信回線設備を設置せずに、無料の通信サービスを提供する電気通信事業者**、2）**いわゆる「用供事業者」（クラウドサービス事業者等）における対策の確保の在り方**について、どう考えるか。

⑤ データ管理やサイバーセキュリティ対策について、電気通信事業者におけるガバナンスの実効性や信頼性を確保するため、対策に関する定期報告等による**モニタリングなどの国の関与の在り方**について、どう考えるか。