資料９－１

電気通信事業ガバナンス強化に向けた検討状況の整理

令　和　３　年　10　月　４　日

電気通信事業ガバナンス検討会

事　　務　　局

ガバナンス強化に係る検討の背景、現状の課題と検討の方向性

1. 検討の背景

（1）電気通信事業を取り巻く状況の変化とリスクの高まり

- 情報通信技術の進展・サービス構造の変化等、通信サービスの提供環境の変化によるリスクの高まり（情報の漏えい・不適正な取扱い等のリスク、通信サービス停止のリスク）
- 情報の漏えい・不適正な取扱い等や通信サービスの停止は、多様な個人的法益・社会的法益・国家的法益の侵害につながるおそれ

（2）電気通信事業におけるガバナンス強化の必要性

- リスク管理を適切に機能させるための体制の整備、ユーザへの説明・情報開示などによるアカウンタビリティ・透明性の確保などを通じて、「電気通信事業ガバナンス」の在り方を検討することが必要

2. 電気通信事業を巡る現状

（1）国内の電気通信事業におけるガバナンスの現状

- 電気通信役務の円滑な提供を確保する観点からの回線設置事業者への設備規律
  （損壊・故障対策、通信の秘密の保持等）

（2）ガバナンスに関する諸外国の制度・国際標準等

- 米NISTによるサイバーセキュリティに係る規格
- 欧州における電気通信関連制度の改正
- 国際標準（ISO27000シリーズ）に基づく情報セキュリティ対策

3. 電気通信事業ガバナンスの在り方

（1）基本的な考え方、検討の方向性

- 「事業者の内部統制によるガバナンス」を「社会全体の仕組みによるガバナンス」によって促進していくという構造を基本的な考え方として、その在り方を検討
- 多様な個人的法益、社会的法益、国家的法益の侵害を防止する観点から、情報の漏えい・不適正な取扱い等や通信サービスの停止のリスクを低減するため、設備に加え、新たに情報を対象とした対策が必要
- 多様な法益侵害につながるおそれへの対処が単独の事業者では困難になってきていることから、政府による規制・ガイドライン等の新たな枠組みを構築し、政府も関与する共同規制等の仕組みによって、事業者自らによる取組を促進

（2）電気通信事業ガバナンスの強化に向けた方策

①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策

- 適正な管理が必要な電気通信事業に係る情報と当該情報の適正な管理が求められる者
- 情報の漏えい・不適正な取扱い等を防止するための新たな規律（情報の取得・収集・保管等に関する管理規程の策定、統括責任者の選任、安全管理措置等）

②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策

- 設備のクラウド化・多様化を踏まえた対策
- 単独の事業者では対応が困難なリスクへの対策（事業者間連携によるサイバー攻撃対策等）
- 情報の漏えい・不適正な取扱い等や事故への迅速かつ適切な対応に必要な措置（兆候段階からの報告義務等）

③情報の適正な取扱いや通信サービスの提供等に関する利用者等への情報提供

１．検討の背景

（１）電気通信事業を取り巻く状況の変化とリスクの高まり
（２）電気通信事業におけるガバナンス強化の必要性

電気通信事業を取り巻く状況の変化とリスクの高まり

● 情報通信技術の進展・サービス構造の変化等、通信サービスの提供環境の変化により、情報の漏えい・不適正な取扱い等(※)のリスク、通信サービス停止のリスクが高まりつつある。社会における通信サービスの重要度が向上している中で、情報の漏えい・不適正な取扱い等や通信サービスの停止は、多様な個人的法益・社会的法益・国家的法益の侵害につながるおそれ。

(※)提供先に対するリスク評価が不十分な状態で情報を不適切に外部提供する場合、通信の秘密やプライバシー性の高い情報を不適正に取り扱う場合等

通信サービスの提供環境の変化

・情報通信分野における**技術の進展**(ネットワークの仮想化(ソフトウェア化)等)
・**サービス構造の変化**(クラウドの活用によるネットワーク構築、関与するステークホルダーの増加・複雑化等)
・**サイバー攻撃の複雑化・巧妙化**(DDoS攻撃、不正アクセス等)
・**経済活動のグローバル化**(国外への開発委託(ｵﾌｼｮｱﾘﾝｸﾞ)、多様なﾍﾞﾝﾀﾞｰ製品の使用、国外のﾃﾞｰﾀｾﾝﾀｰの活用等)の進展
→ サプライチェーンリスクや外国の法的環境による影響等のリスク

情報の漏えい・不適正な取扱い等のリスク・通信サービス停止のリスクの高まり

通信サービスの重要度の向上

①**通信サービス利用の一層の浸透**(大量のデータの収集・蓄積による利用者情報の重要性の向上)
②**通信サービスの社会経済活動・国民生活の基盤としての役割の高まり**
③**通信サービスの自由な情報発信や多様な情報収集手段としての役割の高まり**(健全な民主主義社会を実現するための基盤化)
④**通信サービスの国家安全保障上の役割の高まり**(グローバルレベルでの国家間・企業間等における対立や競争激化)

情報の漏えい・不適正な取扱い等や通信サービスの停止が生じた際の影響は大きくなっており、

個人的法益・社会的法益・国家的法益の侵害につながるおそれ

①**ユーザのプライバシー侵害の深刻化のおそれ、要人に関する情報の悪用等による国家安全保障上の脅威**
②**多様な社会経済活動や国民生活の確保に大きな支障を生じるおそれ、ひいては、デジタル社会の実現が停滞するおそれ**
③**ユーザの自由な情報発信や知る権利の侵害のおそれ、健全な民主主義システムに影響を与えるおそれ**
④**機密データ等の窃取による国家安全保障上の脅威、サイバー攻撃による政府機関や重要インフラの機能停止**

電気通信事業におけるガバナンス強化の必要性

- 電気通信事業を取り巻く状況の変化に伴い、**情報の漏えい・不適正な取扱い等や通信サービスの停止**が生じた場合には、多様な個人的法益・社会的法益・国家的法益の侵害につながるおそれ。

1. 個人的法益

- ✓ 情報漏えい等の防止によるユーザのプライバシーの保護
- ✓ 通信サービスの円滑な提供を通じた、ユーザの利便性の確保
- ✓ ユーザによる自由な情報発信や知る権利の保障

2. 社会的法益

- ✓ 多様な社会経済活動や国民生活の確保、ひいてはデジタル社会の実現
- ✓ サイバー犯罪による経済的損失の防止
- ✓ 健全な言論環境の確保（社会の分断の回避）
- ✓ 通信サービスに係る制度そのものに対する信頼の維持

3. 国家的法益

- ✓ 健全な民主主義システムの確保
- ✓ 要人に関する情報の悪用の防止
- ✓ 機密データ等の窃取の防止
- ✓ サイバー攻撃による政府機関や重要インフラの機能停止の防止

- 上記の保護法益を確保するためには、**情報の漏えい・不適正な取扱い等や通信サービス停止のリスクに適切に対処することが急務**。

  ⇒ 情報の漏えい・不適正な取扱い等や通信サービス停止のリスクに適切に対処するために、**リスク管理(※)を強化することが必要。**

(※)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

- また、これらのリスクに対するユーザの不安・懸念等も高まっており、**事業者によるリスクへの対処状況等について、ユーザからの情報開示や説明への期待**に向けた対応も求められる。

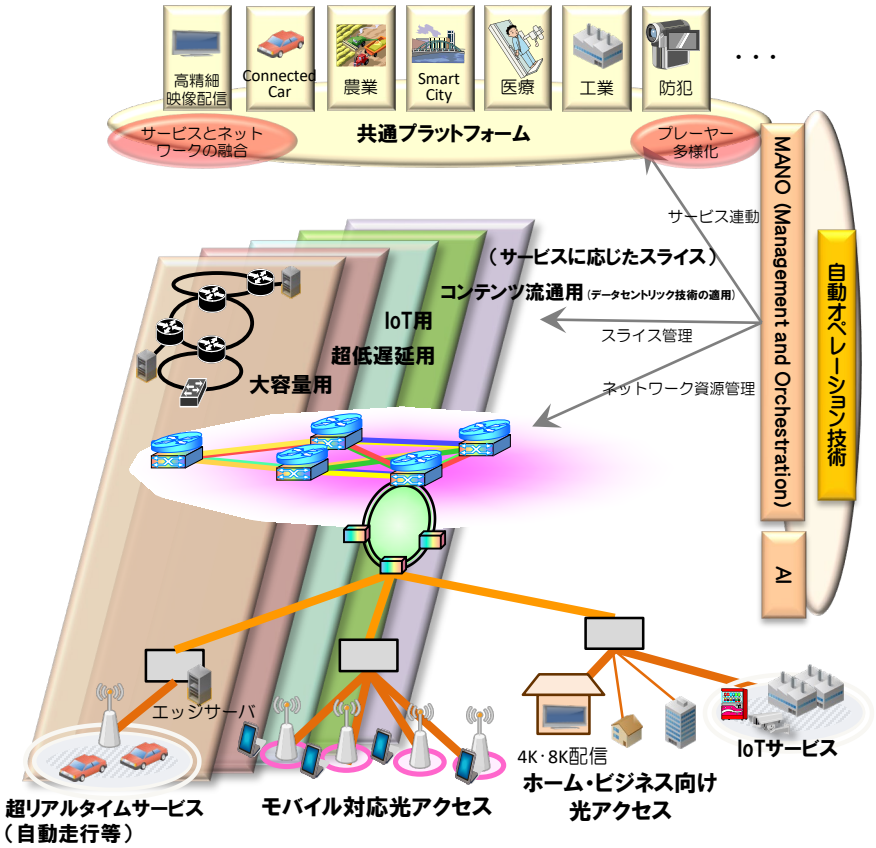
  ⇒ **利用者利益を保護する観点から、**情報の漏えい・不適正な取扱い等や通信サービス停止のリスクへの**対処状況についてのユーザへの説明・情報開示の推進が必要。**

- **リスク管理を適切に機能させるための体制の整備、ユーザへの説明・情報開示などによるアカウンタビリティ・透明性の確保**などを通じて、**情報の漏えい・不適正な取扱い等や通信サービス停止のリスクを低減**させ、**上記保護法益の確保を実現**する観点から、**「電気通信事業ガバナンス」の在り方を検討する必要**がある。

（参考）通信サービスの提供環境の変化

- 情報通信技術の進展（ネットワークの仮想化（ソフトウェア化）等）やサービス構造の変化（クラウドの活用によるネットワーク構築、多様なステークホルダーの増加等）等により、通信サービスの提供環境が変化してきている。
- また、経済活動のグローバル化（国外への開発委託（オフショアリング）、多様なベンダー製品の使用、国外のデータセンターの活用等）の進展によって、外国の法的環境による影響等のリスクも高まりつつある。

ネットワークの仮想化イメージ



出典：総務省「将来のネットワークインフラに関する研究会」報告書

外国の法的環境による影響のリスクの例

- LINE社が提供するメッセージングサービス「LINE」は、国内で約8,600万ユーザが利用するとともに、一部公共サービスにも利用されている。
- 同サービスの日本ユーザーの個人情報（通報されたメッセージの内容を含む。）が、中国法人でありLINE社の業務再委託先であるLINE China社からアクセス可能であった。

➢ 2021年3月、LINE社はメッセージングサービス「LINE」の中国における開発及び保守を終了。

➢ なお、中国法人からのアクセスは、開発及び保守プロセスにおける正規の作業であったことが確認されている。

出典：Zホールディングス(株)「グローバルなデータガバナンスに関する特別委員会」第一次報告書（2021年6月11日）及び第二次報告書（2021年8月4日）より作成

（参考）中国における法的環境

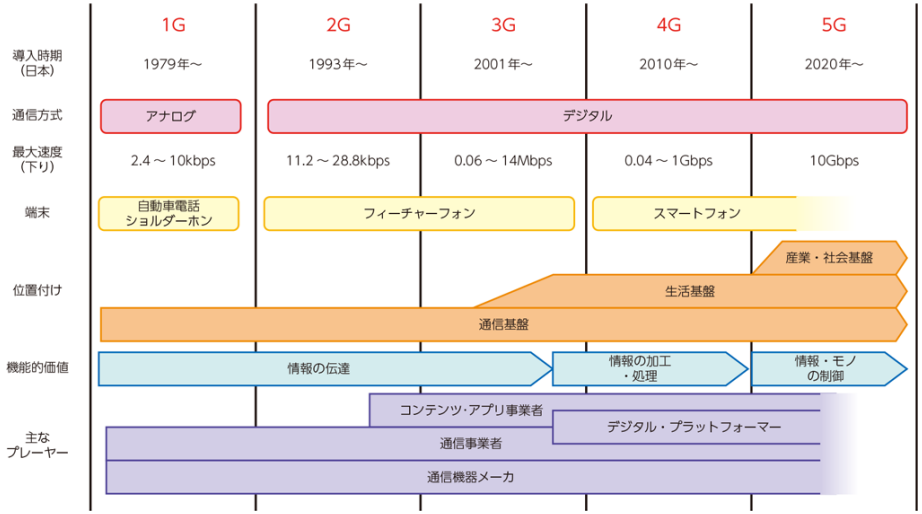
国家情報法（2017年6月27日制定）

➢ 国民と組織は、法に基づいて国の情報活動に協力し、国の情報活動の秘密を守らなければならず、国は、そのような国民及び組織を保護する。

（参考）通信サービスの重要度の向上

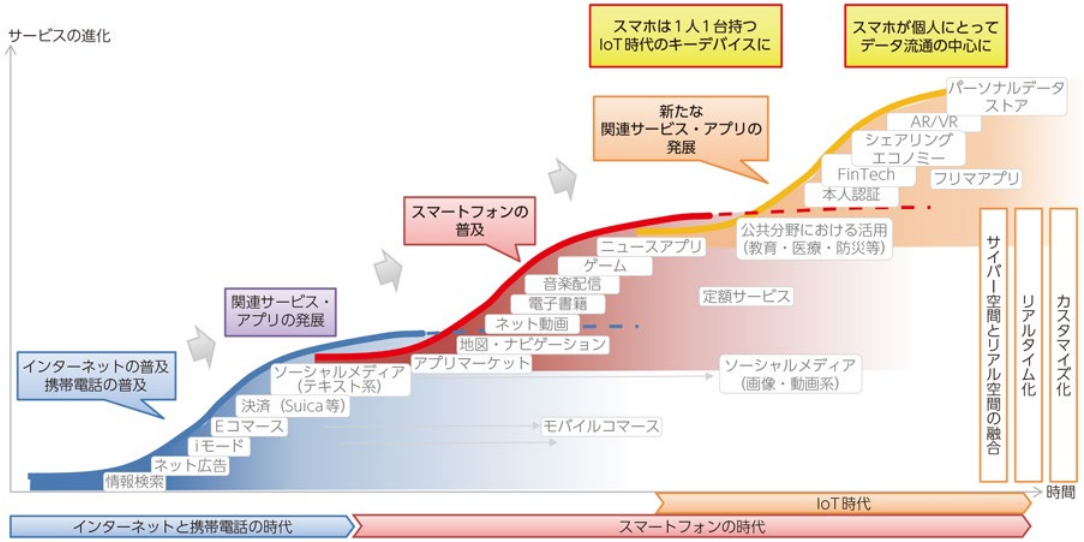
- 移動通信システムの進展とともに、スマートフォンを中心に、FinTech、シェアリング・エコノミー、AR/VR等の新たなサービスが普及するなど、通信サービスは国民に一層浸透してきている。
- 通信サービスについては、社会経済活動・国民生活の基盤としての役割や、自由な情報発信や多様な情報収集手段としての役割が高まってきており、重要度が向上してきている。
- また、グローバルレベルでの国家間・企業間等における対立や競争激化等を背景として、通信サービスの国家安全保障上の役割も高まりつつある。

移動通信システムの進展



出典：総務省「令和2年 情報通信に関する現状報告」

スマホ関連サービス・アプリ変遷の概念図



出典：総務省「平成29年 情報通信に関する現状報告」

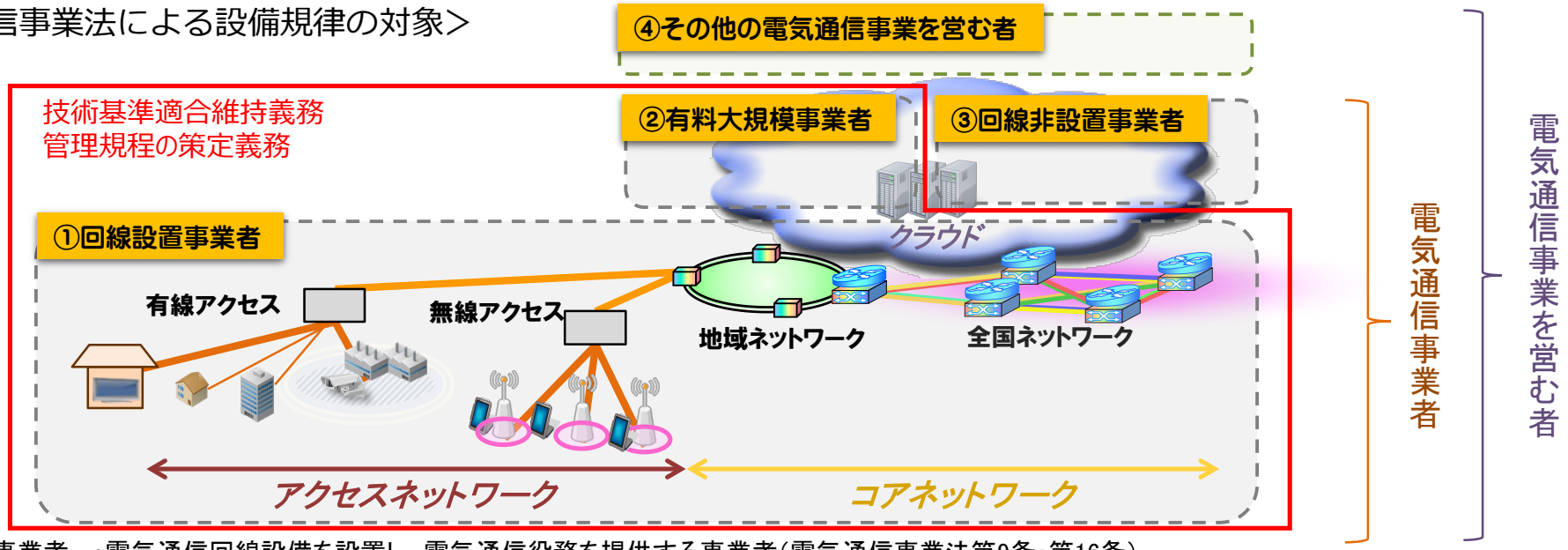
２．電気通信事業を巡る現状

（１）国内の電気通信事業におけるガバナンスの現状
（２）ガバナンスに関する諸外国の制度・国際標準等

電気通信事業におけるガバナンスの現状（設備規律）

- 電気通信事業法は、**電気通信役務の円滑な提供を確保する**（送信側から受信側に情報を確実に伝える）**ことが利用者の利益の保護に直結する**という考え方を基本として、伝送路設備を有する「回線設置事業者」及び有料で利用者100万人以上のサービスを提供している「有料大規模事業者」に対し、電気通信設備の安全・信頼性を確保するための規律（技術基準への適合維持義務、管理規程の策定義務等）を課している。
- 通信ネットワーク全体の中で情報を伝送する役割を担う回線設置事業者に対し、予備機器の設置、故障検出機能の具備、大規模災害対策、異常ふくそう対策等を求めることで、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し、電気通信役務の円滑な提供の確保に努めている。

＜電気通信事業法による設備規律の対象＞



①回線設置事業者　：電気通信回線設備を設置し、電気通信役務を提供する事業者（電気通信事業法第9条・第16条）
②有料大規模事業者：電気通信回線設備を設置せず、有料かつ利用者100万人以上の電気通信役務を提供する事業者（電気通信事業法第16条・第41条）
③回線非設置事業者：電気通信回線設備を設置せず、有料かつ利用者100万人未満又は無料の電気通信役務を提供する事業者（電気通信事業法第16条）
④その他の電気通信事業を営む者：電気通信回線設備を設置せず、他人の通信を媒介しない電気通信役務を提供する電気通信事業を営む者など、①、②及び③以外の電気通信事業を営む者。（電気通信事業法第164条第1項第1号から第3号まで）

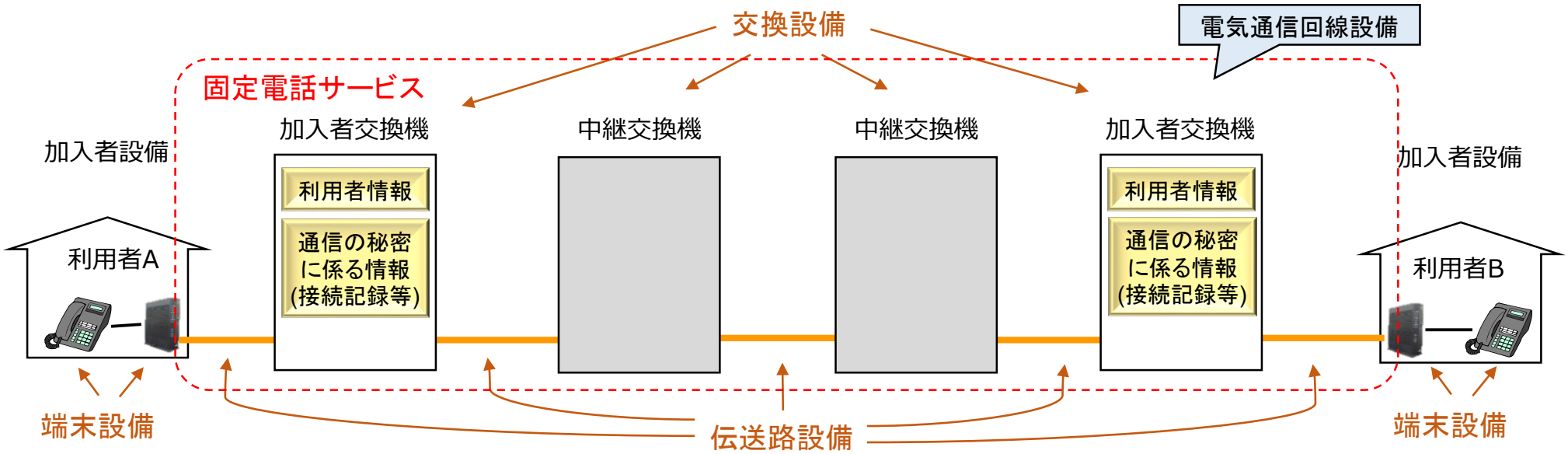
※ 電気通信事業法による規律対象を模式的に表したイメージであり、実際のネットワークのレイヤ構造を正確に表したものではない。

※ 電気通信事業については、電気通信設備の仮想化（ソフトウェア化）・クラウド化等が進展し、電気通信事業者以外の事業者を含む様々な事業者の集合体によってサービスが提供されることもあるため、このイメージに当てはまらないケースも存在する。

電気通信事業におけるガバナンスの現状（情報（通信の秘密））

- 電気通信事業法では、「電気通信事業者の取扱中に係る通信の秘密は侵してはならない」（電気通信事業法第4条）とされている。
- 特に、伝送路設備を含む設備（電気通信回線設備）を設置する電気通信事業者に対しては、通信内容の秘匿措置、蓄積情報の保護措置等を求めており、こうした措置を通じて「通信の秘密が侵されないようにすること」（電気通信事業法第41条第6項第3号）を確保。
- 一方、回線非設置事業者を含む電気通信事業を営む者に対しては、通信の秘密の保護に関し罰則以外の規定はなく、大量の情報を取得・収集・保管等する場合も含め、その適正管理は自主的な取組に委ねられている。

＜設備規律を通じた情報の適正管理のイメージ（固定電話サービスの場合）＞



* 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

（参考） 電気通信事業法上の電気通信設備に関する技術基準

- 「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(株)の4者が指定されている。

- 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。

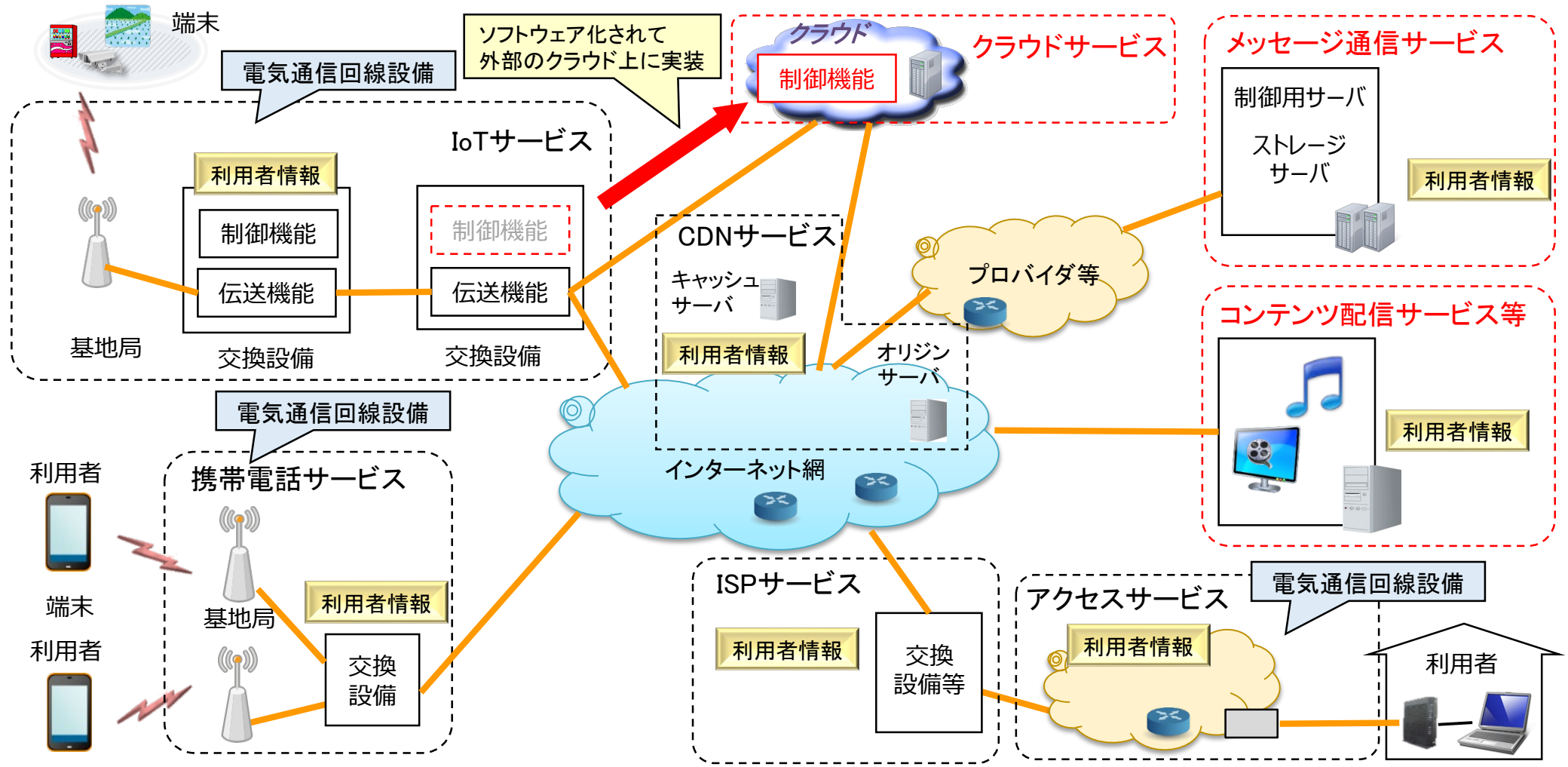
＜電気通信役務の種類に応じた事業用電気通信設備の技術基準＞

		損壊・故障対策	品質基準	通信の秘密・他者設備の損傷防止・責任の分界
音声伝送役務用設備	アナログ電話用設備	○予備機器 ○防護措置 ○建築物の施錠等 ○異常ふくそう対策 ○耐震対策 ○停電対策 ○大規模災害対策　等	高い品質基準	[通信の秘密] ○通信内容の秘匿措置 ○蓄積情報保護 [他者設備の損傷防止] ○損傷防止 ○機能障害の防止 ○漏えい対策 ○保安装置 ○異常ふくそう対策 [責任の分界] ○分界点 ○機能確認
	総合デジタル電話用設備			
	0AB-J IP電話用設備			
	携帯電話・PHS用設備		自主基準※3	
	その他(050IP電話用設備)	○大規模災害対策 ○異常ふくそう対策 ○防護措置　等	最低限の品質基準	
上記以外の設備(データ伝送役務用設備等)			規定なし	

※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）通信サービスの提供構造

- 通信サービスを提供するネットワークは、ソフトウェア化等の技術の進展やクラウドの活用等によって多様化が進み、その提供構造が複雑化している。
- また、通信ネットワークは、電気通信回線設備等を設置して情報を伝送する役割を担う「通信インフラ提供者」と、自ら又は他者の通信インフラを使用してサービスを利用者に提供する「通信サービス提供者」が複雑に組み合わさる形で構成されている。



電気通信事業におけるガバナンスの現状（事業者の自主的な取組）

(注) 事業者における一般的な取組を記載したものであり、全ての事業者において同様の措置が取られていることを保証するものではない。

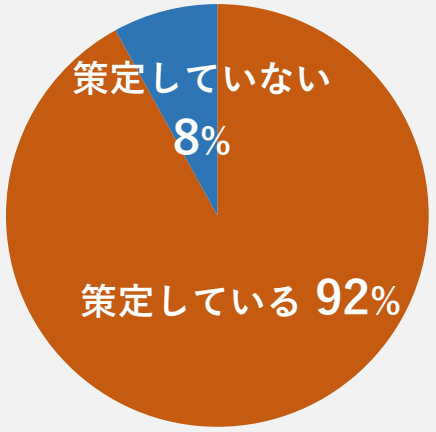
- 電気通信事業者においては、情報セキュリティに関する規程を策定するとともに、CISO（最高情報セキュリティ責任者）やCDO（最高デジタル責任者）等を責任者とする情報セキュリティマネジメント体制を整備。
- 利用者データ、通信の秘密に係るデータなど、取り扱うデータの種別に応じた管理を実施。
- 必要に応じ、ISMS（情報セキュリティマネジメントシステム）等の認証を取得することで、機密性(Confidentiality)、完全性(Integrity)及び可用性(Availability)を考慮した情報資産のリスク管理体制を構築。

CISO: Chief Information Security Officer　CDO: Chief Digital Officer　ISMS: Information Security Management System

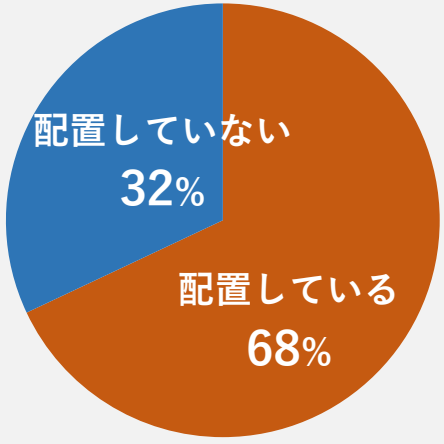
＜総務省「情報通信ネットワークのセキュリティ対策及び各種データの取扱いに関する調査」アンケート結果の例＞

総務省において、令和3年4月下旬から5月下旬の間、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（電気通信回線設備を設置する者が大宗を占める）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たもの。（回答数：130事業者）

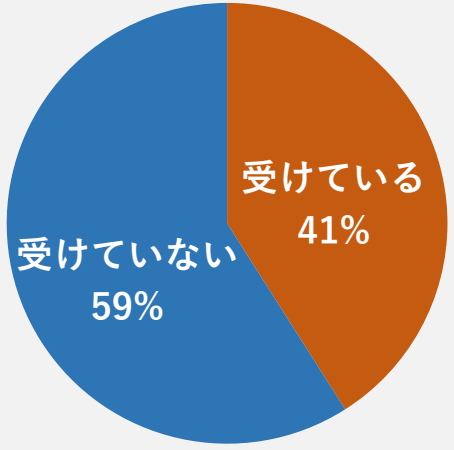
● 情報セキュリティポリシーに当たる社内規程を策定しているか。



● 組織内にCISOを配置しているか。



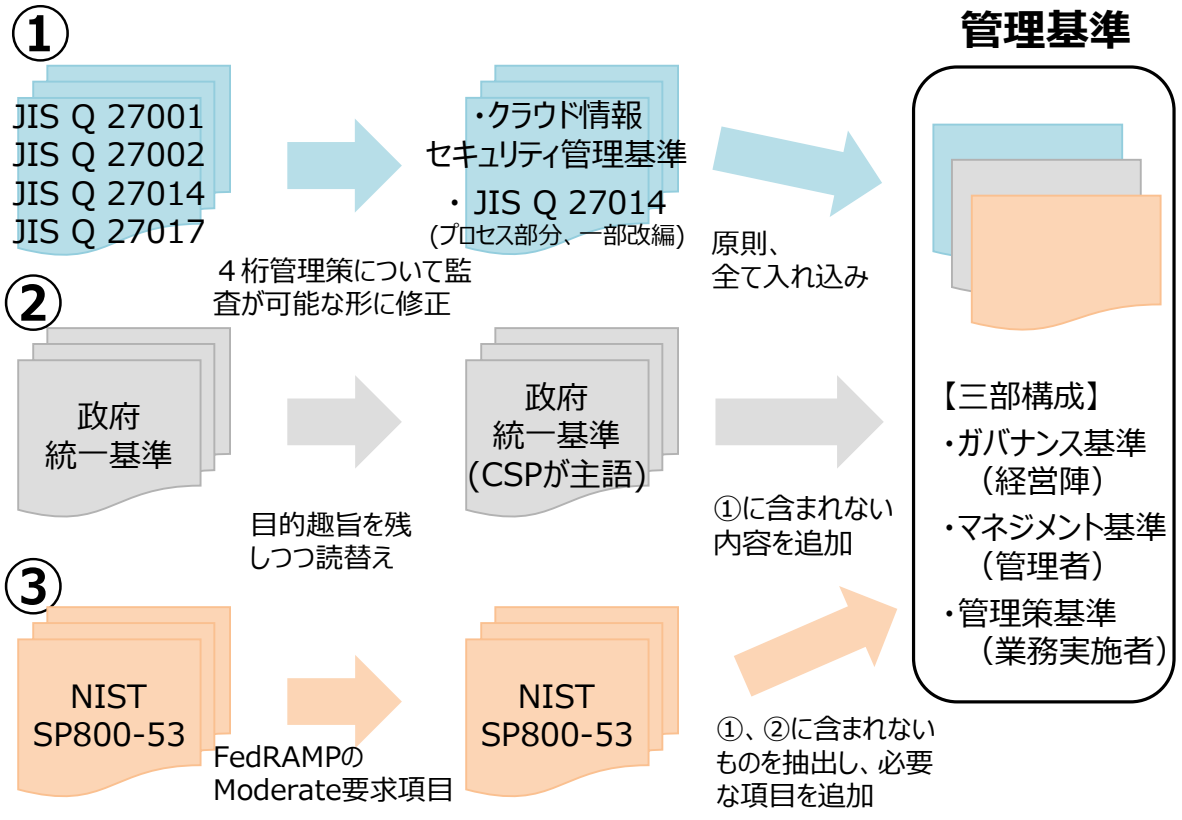
●組織における情報資産のセキュリティを管理するため、ISO/IEC 27001の情報セキュリティマネジメントシステム(ISMS)等のフレームワークに基づく第三者による認証や定期的なリスクアセスメントを受けているか。



（参考）「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12日、第1弾として10サービスを登録・公表。同年9月13日時点で、20サービスが登録済み。

ISMAP管理基準の構成



現在登録されているサービス（令和３年９月13日時点）

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
11	Oracle Cloud Infrastructure	Oracle Corporation
12	Microsoft Azure, Dynamics 365, and Other Online Services	日本マイクロソフト株式会社
13	Microsoft Office 365	日本マイクロソフト株式会社
14	エンタープライズクラウドサービス／エンタープライズクラウドサービ ス G２／フェデレーテッドポータルサービス	株式会社日立製作所
15	Cisco Webex	Cisco Systems, Inc.
16	クラウドサービス運用基盤cybozu.com 並びにcybozu.com 上で提供するGaroon及びkintone	サイボウズ株式会社
17	Box	Box, Inc.
18	Smart Data Platform サービス	エヌ・ティ・ティ・コミュニケーションズ株式会社
19	Oracle Cloud Infrastructure Platform as a Service	Oracle Corporation
20	Oracle Exadata Cloud@Customer	Oracle Corporation

情報セキュリティに関する規格等（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。 • 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。

諸外国におけるセキュリティ対策

- 英国においては、Telecom Security Bill(2021年9月時点において審議中)の中で、通信事業者・サービス事業者に対し、経営レベルのセキュリティ管理の責任者の任命や、外国の法的環境を考慮した措置を義務として課している。
- 独国においては、Telecommunications Modernization ACT(2021年5月成立)の中で、通信事業者に対し、セキュリティ責任者の指名義務や、通信ネットワークサービスのリスクマネジメント義務を課している。

英国

【規制の名称】
Telecom Security Bill(2021年9月時点において上院審議中)

【規制の対象】
通信事業者、サービス事業者

【セキュリティ対策の例】
通信事業者またはサービス事業者は、第105A条第1項に記載された目的のために、提供者のために措置を講じる責任を与えられた者の適切な管理を確保しなければならない。特に以下の義務が含まれる。

(a) セキュリティをビジネスの本質的な機能として扱い、明確なセキュリティポリシーの公布や適切な人材の確保など、効果的なセキュリティ管理を確保する責任を、取締役レベル（又はそれに相当するレベル）の人物又は委員会に与えること。

(b) 公衆電子通信ネットワークまたは公衆電子通信サービスの提供に関与する人物による不正行為によって生じるセキュリティ侵害のリスクを特定し、それを低減するためのあらゆる妥当な措置を講じること。これには、居住国を理由とするか否かにかかわらず、それらの人物が不適切な影響を受けやすいことを考慮した措置も含まれる。

独国

【規制の名称】
Telecommunications Modernization ACT(2021年5月成立)

【規制の対象】
通信事業者

【セキュリティ要件の例】
165条　技術・組織的防御：
- 最新の技術を用いて通信の秘密・個人情報を守る方策の導入義務
- 外部からの攻撃や災害により生じる大規模ネットワーク障害を防ぐ方策の導入義務
- 通信ネットワークサービスのリスクマネジメント義務
- ネットワークへの攻撃を検知するシステムの導入義務

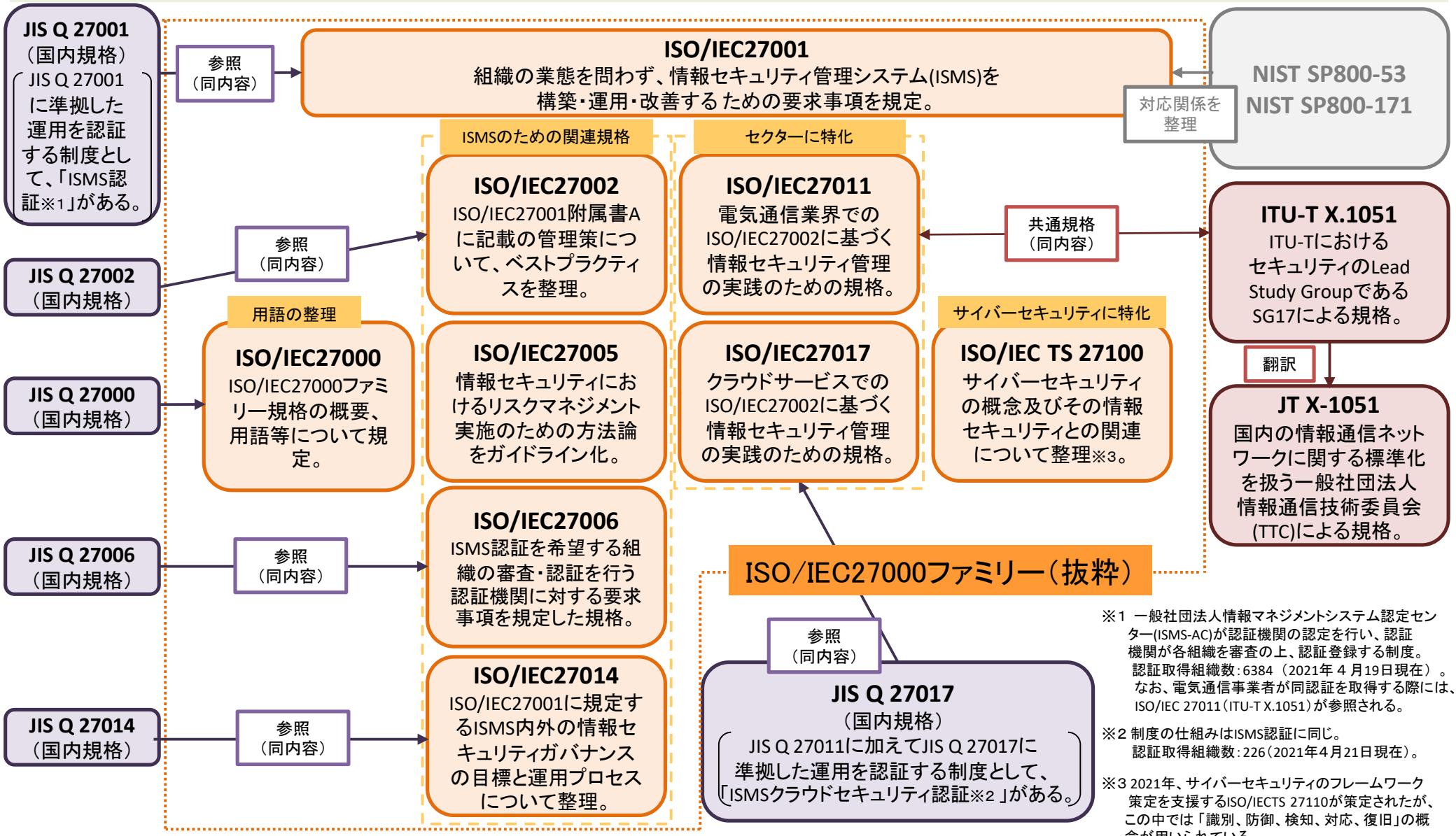
166条　セキュリティ責任者とセキュリティポリシー：
- セキュリティ責任者の指名義務
- EU内連絡先担当者の任命義務

等

出典：総務省「電気通信ネットワーク技術の進展に伴う国内外調査等」（令和3年度）

情報セキュリティに関する規格等（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**。



※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 2021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。

３．電気通信事業ガバナンスの在り方

（１）基本的な考え方、検討の方向性

（２）電気通信事業ガバナンスの強化に向けた方策

①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策

②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策

③情報の適正な取扱いや通信サービスの提供等に関する利用者等への情報提供

電気通信事業におけるガバナンス強化に向けた基本的な考え方

- 電気通信事業は、デジタル社会における基幹的・中枢的なインフラを構成しているところ、サービスの提供構造の多様化、グローバル化の進展等の事業を取り巻く状況の変化により、情報の漏えい・不適正な取扱い等や通信サービス停止が生じた場合には、多様な個人的法益・社会的法益・国家的法益の侵害につながるおそれがある。
- 従って、電気通信事業の円滑・適切な運営を確保することが一層重要になっており、「電気通信事業ガバナンス」（電気通信事業の円滑・適切な運営を確保するための管理の仕組み）の在り方について検討を行うことが必要。
- 「電気通信事業ガバナンス」については、前述の状況変化により、単独の事業者による適切な確保が困難になってきていると考えられることから、「①事業者の内部統制によるガバナンス」を「②社会全体の仕組みによるガバナンス」によって促進していくという構造を基本的な考え方として、その在り方の検討を進める。

①事業者の内部統制によるガバナンス・・・電気通信事業の運営に当たっての、経営者による組織の規律・管理体制やマルチステークホルダー（利用者、株主や政府等）に対する説明責任（アカウンタビリティ）等、事業者の内部統制による規律

②社会全体の仕組みによるガバナンス・・・上記①の事業者における内部統制の自律的な発揮を確保・促進するための、政府による規制を含む指針・ルール等の社会全体の仕組みによる規律

【参考】

- 「**ガバナンス**」とは、一般的に、企業等の組織体における「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。また、「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。

  （出典）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18日、総務省及び経済産業省）、Governance: A Very Short Introduction（Mark Bevir） 等
- 2021年5月に成立した**デジタル社会形成基本法**において、次のとおり規定されている。
  - 「デジタル社会の形成に関する施策の策定に当たっては、**サイバーセキュリティ**（サイバーセキュリティ基本法（平成26年法律第104号）第2条に規定するサイバーセキュリティをいう。第37条第2項第14号において同じ。）の確保、情報通信技術を用いた犯罪の防止、情報通信技術を用いた本人確認の信頼性の確保、情報の改変の防止、高度情報通信ネットワークの災害対策、個人情報の保護その他の**国民が安心して高度情報通信ネットワークの利用及び情報通信技術を用いた情報の活用を行うことができるようにするために必要な措置**が講じられなければならない」（第33条）

「電気通信事業ガバナンス」確保のための検討の方向性

検討の方向性(案)

Ⅰ　電気通信事業ガバナンスの強化

- 電気通信事業を取り巻く環境が著しく変化するとともに同事業の重要性が高まりつつある中、電気通信事業法第1条の目的である「電気通信の健全な発達及び国民の利便の確保」を引き続き実現していくためには、電気通信事業を営む者が、デジタル社会の形成等におけるイノベーションの牽引や利用者の権利・利益の保護に向けて、主導的な役割を果たすことができるような環境整備を目指すことが必要。
- そのため、デジタル社会における基幹的・中枢的なインフラである電気通信事業の円滑・適切な運営を確保するための管理の仕組みを「電気通信事業ガバナンス」として定義し、①事業者の内部統制によるガバナンスと②社会全体の仕組みによるガバナンスの両方の側面から、その強化に向けて取り組むべき対策に関する検討を進めていくべきではないか。

Ⅱ　対策を講じるべき対象

- 情報の漏えい・不適正な取扱い等や通信サービス※の停止のリスクを低減するためには、設備を対象とした対策に加え、新たに情報を対象とした対策が必要ではないか。
- 対策を講じるべき情報として、通信の秘密や利用者に関する情報(これらの情報の漏えい・不適正な取扱いによって、多様な個人的法益・社会的法益・国家的法益の侵害につながるおそれが高まることから)のほか、電気通信設備に関する情報であって漏えい時には電気通信役務の提供に支障を及ぼすおそれのある情報についても、対象とすることが適当ではないか。
- 対策を講じるべき設備としては、従来対象としていた電気通信事業者自身が設置する伝送路を含む設備のほか、他の事業者等の設備を組み合わせて通信サービスが提供される場合等、ネットワークを構成する設備の多様化を踏まえ、設備の全体像を整理した上で、対象を決めていくことが適当ではないか。

※ 通信サービス:
電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること(電気通信事業法上の電気通信役務の定義と同じ。)

「電気通信事業ガバナンス」確保のための検討の方向性（続き）

検討の方向性（案）

Ⅲ 対策の実施主体

- 情報の漏えい・不適正な取扱い等や通信サービス停止のリスクへの対策の実施主体は、通信サービス提供に当たって利用者に対する一義的な責任を有する通信サービス提供者※1とすることが適当ではないか。なお、設備を対象とした対策については、他の事業者等の設備を組み合わせて通信サービスが提供される場合等においては、ネットワークを構成する設備の全体像を整理した上で、適切な実施体制を構築することが必要ではないか。
- 社会的な影響が大きい又は公共性が高いと考えられる通信サービス提供者を中心として、リスクに応じて対策の実施主体を考えるべきではないか。

Ⅳ 電気通信事業ガバナンス確保の促進

- Ⅱ、Ⅲの対策を適切に実施するに当たり、①事業者の内部統制によるガバナンス、②社会全体の仕組みによるガバナンスの強化に向けた取組として、以下のような検討を進めていくべきではないか。

①事業者の内部統制によるガバナンス

- 電気通信事業は、技術の進展が著しいことから、その進展を阻害しないという観点への配慮が必要。そのため、「電気通信事業ガバナンス」の強化に向けた仕組みについては、電気通信事業を取り巻く環境の変化によって顕在化した新たなリスクへの対応として内部統制の強化を通じた事業者自らによる取組の向上を基本とすべきではないか。

②社会全体の仕組みによるガバナンス

- グローバルプレーヤーを含む様々な事業者等の集合体によって通信サービスが提供される環境下においては、多様な個人的法益、社会的法益、国家的法益の侵害につながるおそれに対処することが単独の事業者では困難になってきていると考えられることから、政府による規制・ガイドライン等の新たな枠組みを構築し、各事業者の取組や事業者間の連携・協力を推進していくなど、政府も関与する共同規制※2等の仕組みによって、①の事業者自らによる取組を促進していくという方向を目指すべきではないか。

※1 通信サービス提供者：利用者と通信サービスの利用に係る契約を締結するなど、通信サービス提供に当たって利用者に対する一義的な責任を有する者

※2 共同規制：「立法機関によって定義された目的の達成を、その分野で活動する主体（経済的主体や社会的パートナー、NGOや共同体などを含む）に委ねる法的措置のメカニズム」と定義され、民間の自主規制とそれに対する一定の政府補強措置により問題の解決や抑止を図る規制手法（出典：内閣府「平成25年度諸外国における有害環境への法規制及び非行防止対策等に関する実態調査研究報告書」）

電気通信事業ガバナンスの強化に向けた方策

①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策

利用者の利益の保護を確保する観点から、大量の情報を所有する者による電気通信事業に係る情報の漏えい・不適正な取扱い等を原因として、利用者やサービス提供に影響を及ぼすおそれがあることを踏まえ、新たに利用者情報の適正管理等を促進するための規律を検討。

政府による規制・ガイドライン等の新たな枠組みを構築し、情報の適正管理等に関する事業者自らの取組を促進する方策を検討。

- 対象となる情報・者の整理
- 利用者情報の管理方法等
- 設備関連情報に係る対策

②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策

電気通信役務の円滑な提供を確保する観点から、ネットワークを構成する設備の多様化を踏まえ、クラウド事業者等の設備やサービスを使用して提供される多様な通信サービスを前提とした設備規律を検討。

また、単独の事業者では対応が困難なリスクに対応するため、事業者間連携によるサイバー攻撃対策等を検討。あわせて、情報の不適正な取扱いや事故による多様な法益侵害を最小化する観点から、それらの未然防止や被害軽減を図るため、兆候段階における事態の速やかな報告や対策を検討。

- 設備のクラウド化・多様化への対応
- 事業者間連携によるサイバー攻撃対策等
- 事故の兆候段階からの報告義務

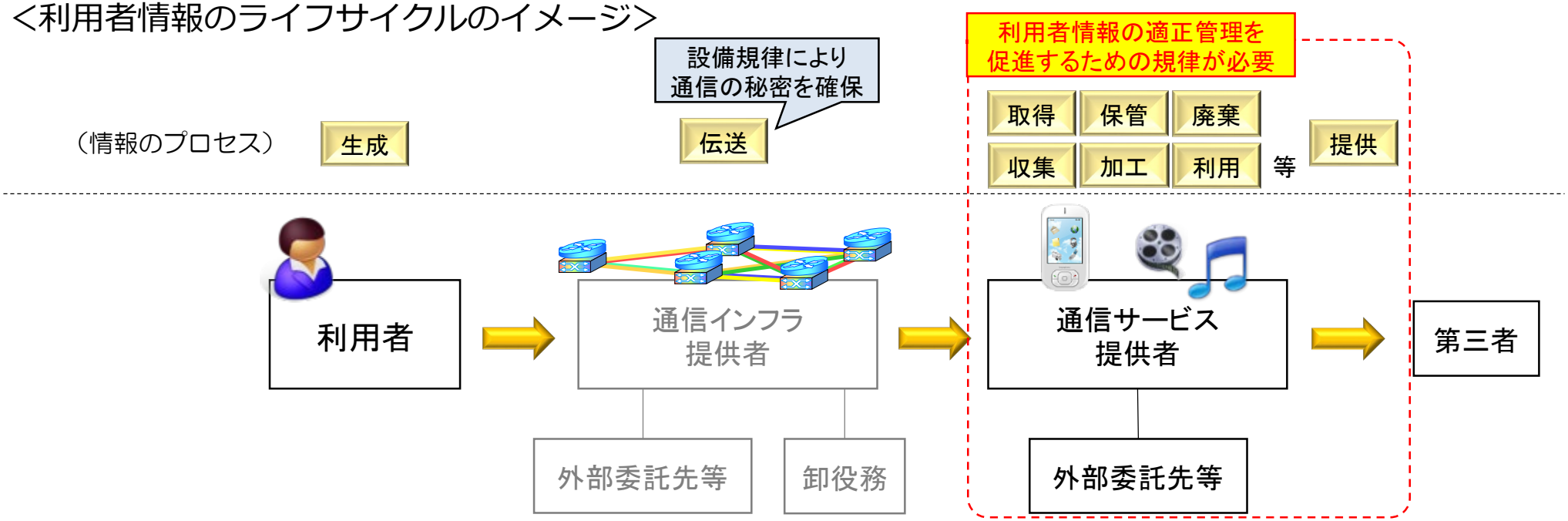
③情報の適正な取扱いや通信サービスの提供等に関する利用者等への情報提供

利用者に対しては、平常時から、情報の適正な取扱いや通信サービスの提供に関する情報、情報の漏えい・不適正な取扱い等や事故が生じた際の対処方策等について利用者に理解しやすい形での周知広報に努め、非常時においても、電気通信事業者等は、適時に適切な方法で情報提供を行い、利用者が適切な対応ができるような方策を検討。

情報の適正管理を促進する必要性の高まり

- 電気通信回線設備は、他人の通信を媒介するために必要となる設備の基本単位であり、これを設置する事業者のみならず他の事業者にとっても通信サービスを提供する上での基盤となっていることを踏まえ、現在、通信内容の秘匿措置等の通信の秘密に係る規定は、電気通信回線設備を設置する事業者についてのみ課せられている。
- 他方、多数の利用者に対し通信サービスを提供する回線非設置事業者は、大量の利用者情報を抱えていることから、情報の漏えいや不適正な取扱い等が発生した場合の影響は甚大なものと考えられ、回線設置の有無と利用者への影響の大きさとが必ずしもリンクしなくなってきている。
- 利用者情報の生成から廃棄に至るライフサイクルの中で、通信インフラ提供者による「伝送」のプロセスにおいては設備規律が機能しているものと考えられることから、通信サービス提供者による「伝送」以外のプロセスにおいて、特に、情報の「取得」、「利用」等、情報の第三者への「提供」のプロセスを中心に情報の適正管理を促進していくことの必要性が高まっている。

＜利用者情報のライフサイクルのイメージ＞



①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策（対象となる情報・者）

- 適正管理を行うべき情報については、情報通信が我が国の経済・社会活動、国民生活の基盤として重要な役割を果たすようになりつつあることから、電気通信事業法の目的の一つである利用者利益の保護の観点を重視し、情報の漏えい・不適正な取扱い等が利用者に及ぼす影響の大きさなどを踏まえ、通信の秘密に係る情報を含む電気通信事業に係る利用者情報等に着目した規律とすることが適当ではないか。
- 情報の適正管理については、社会的な影響が大きい又は公共性が高いと考えられる電気通信事業者を中心とするなど、情報の漏えい・不適正な取扱い等により生じ得るリスクに応じた基準とすることが適当ではないか。なお、電気通信事業を営む者が保有する多様かつ大量の情報のリスクについても留意が必要ではないか。
- 具体的には、利用者情報を多く取得、収集等して利用する電気通信事業を営む者ほど利用者への影響度が大きく、結果として社会的影響も大きくなり得ると考えられることから、利用者数を中心とした基準を定め、これに応じた規律を検討することが適当ではないか。なお、利用者数が基準以下の場合も一定の規律を検討すべきではないか。
- 利用者情報の取得時においては、利用者数に関わらず広く電気通信事業を営む者を対象として、情報の適正な取扱いを確保する観点から、必要な規律を検討することが適当ではないか。

対象となる情報

情報の種類		例
通信サービスの利用者に関する情報	通信の秘密に係る情報	通信内容、通信の日時・場所、通信当事者の氏名・住所・電話番号　等
	利用者の識別に係る情報	氏名、住所等の契約者情報、ログインに必要な識別情報、クッキー技術を用いて生成された識別情報、契約者・端末固有ID　等
	通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴、ウェブページ上の行動履歴、アプリケーションの利用履歴、位置情報、写真、動画、システム利用ログ　等
電気通信設備に関する情報		アカウント情報、認証情報、ネットワーク情報、設備・システム情報　等

①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策（利用者情報の管理方法等）

- 各事業者における情報の漏えい・不適正な取扱い等や通信サービスの停止のリスクへの適切な対処を促進する観点から、情報の適正な管理を促進するため、ISO/IEC 27000ファミリー等の国際標準や業界団体ガイドライン等を踏まえ、情報の取得・保管・廃棄等の管理に係る方法や体制の明確化を図っていくことが適当ではないか。
- 具体的には、情報の適正管理を行うべき事業者に対し、情報管理プロセスを定めた上でのリスクアセスメントの実施を求めるとともに、情報管理規程の策定、統括責任者の選任等の規律を設けることで、事業者自らによる取組を促進することが適当ではないか。また、情報の適正管理の実効性確保の観点から、情報管理規程の行政による確認、利用者への開示等について規律を設けることが適当ではないか。
- あわせて、外部に情報の取扱いの一部又は全部を委託等する場合には、外部委託先の適正な管理に関する規律を設けることが適当ではないか。
- 利用者数を中心とした基準に応じた規律とするとともに、基準以下の場合であっても、努力義務等の規律を設けることが適当ではないか。
- また、利用者情報の取得時においては、利用者に確認の機会を適切な方法で与える規律を設けることが適当ではないか。

情報セキュリティ管理策の項目例

- 情報セキュリティのための方針 Security Policy Management
- 情報セキュリティのための組織 Corporate Security Management
- 人的資源のセキュリティ Personnel Security Management
- 運用のセキュリティ Operational Security Management
- 通信のセキュリティ Network Security Management
- システムの取得、開発及び保守 System Security Management
- 情報セキュリティインシデント管理 Security Incident Management

出典：ISO/IEC 27001附属書A 管理目的 / 管理策

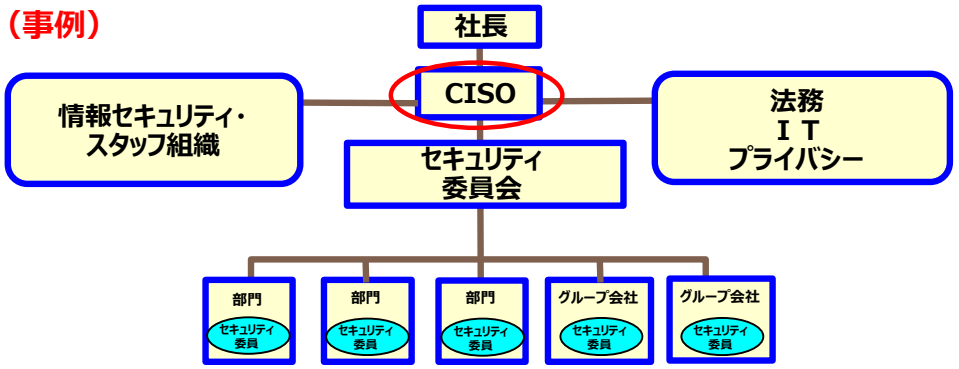
外部委託先管理に当たって留意すべきポイントの例

- 目的、範囲等を明確化。
- 外部委託先選定の手続きを明確化。
- 外部委託先と安全対策に関する項目を盛り込んだ契約を締結。
- 外部委託先の要員に対しセキュリティポリシー等の遵守を義務づけ、その遵守状況を確認。

出典：（公財）金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書」

＜統括責任者(CISO等)の設置＞

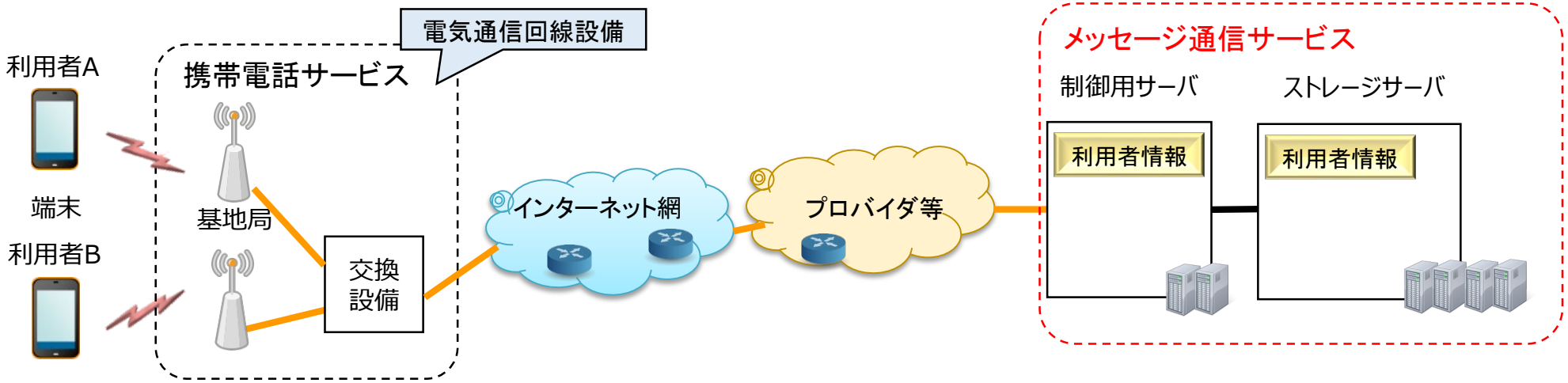
■情報セキュリティを統括するトップマネジメント（ＣＩＳＯ）の設置
トップマネジメント：最高位(highest level)で組織（Organization）を指揮（Direct）し、管理（Control）する個人又は人々の集まり



出典：中尾構成員説明資料（第7回）より

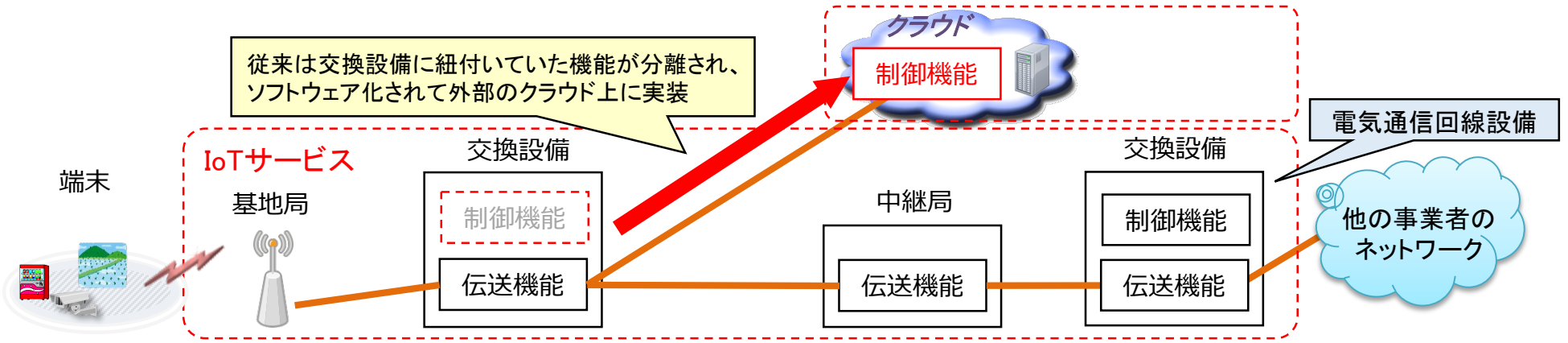
- 通信サービスやその提供者等の多様化とともに、ネットワークを構成する設備についても多様化が進んでおり、特定の通信サービスを提供するためのサーバ等の電気通信設備を使用して様々な通信サービスが提供されているところ。
- 当該設備は、通信サービス提供者自らが設置する場合、クラウド事業者等の他者の設備やサービスを利用する場合等の様々な形態があることや利用者情報を始めとする大量の情報の適正管理の必要性等を考慮して、電気通信設備に関する情報等について安全措置等の規律を設けることが適当ではないか。

他者の電気通信回線設備を使用して、特定の通信サービスを提供するための電気通信設備を用いて通信サービスを提供する形態（メッセージ通信サービス等）



- 設備のソフトウェア化の高度化やクラウド技術等の進展により、クラウド事業者のサービスやインフラを利用して通信サービスを提供することが現実のものとなっている。
- 電気通信事業法上、電気通信事業者が他者のクラウド設備を電気通信回線設備の一部として使用する場合には、そのクラウド設備にも設備規律が課せられることとなるが、規律はクラウド設備の設置者ではなく、クラウド設備を使用する電気通信事業者に課せられている。また、音声役務の提供に係る設備や有料大規模の電気通信役務の提供に係る設備を除き、電気通信設備の一部に他者が設置する設備を使用する場合、当該他者の設備については、利用者への影響が軽微なものとして、技術基準への適合維持義務が除外されている。
- 通信サービスの提供に係るネットワークの多様化に対応していくため、その損壊又は故障時には通信サービス停止に至るリスクが大きいと考えられる設備については、他者設備であっても技術基準への適合維持義務を課していくことが適当ではないか。
- 電気通信回線設備と一体として使用されるものであって交換設備の機能の一部（制御機能等）を担う電気通信設備に対しては、損壊又は故障による利用者への影響が大きいと考えられることから、実効性のある技術基準を定めるなど、設備規律による適正な管理を行っていくことが適当ではないか。

＜通信サービスを提供する設備のクラウド化のイメージ＞

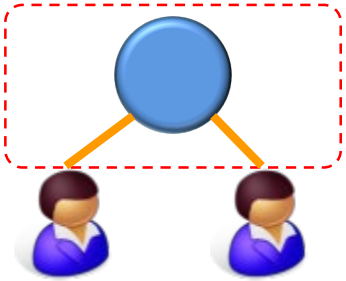


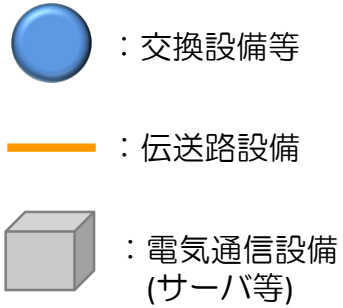
（参考）電気通信事業のサービス提供形態のモデル化

＜通信インフラ提供者の例＞

(A) 自己完結モデル

送信側から受信側に情報を伝達するための電気通信回線設備を自ら設置して、通信サービスを提供する形態（固定電話サービス等）

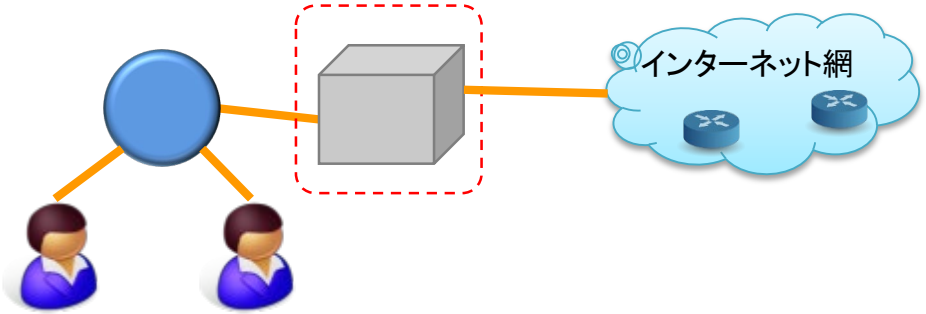




* サーバ等の電気通信設備は、自ら設置するほか、他者の設備を利用する場合がある
** 赤枠は、各モデルにおける通信サービス提供者が通常支配・管理している設備の範囲

(B) 情報伝達モデル

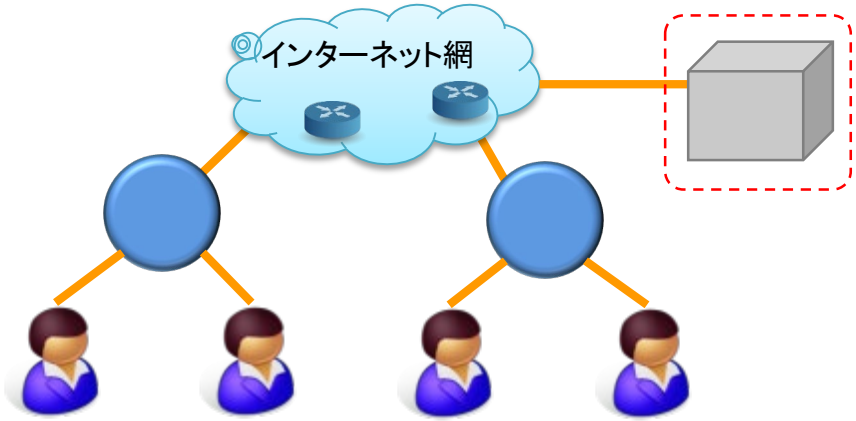
自ら伝送路設備は設置しないが、送信側から受信側に情報を伝達する役割の一部を担う通信サービスを提供する形態（ISPサービス、MVNOサービス、CDNサービス等）



＜通信サービス提供者の例＞

(C) サービス専従モデル

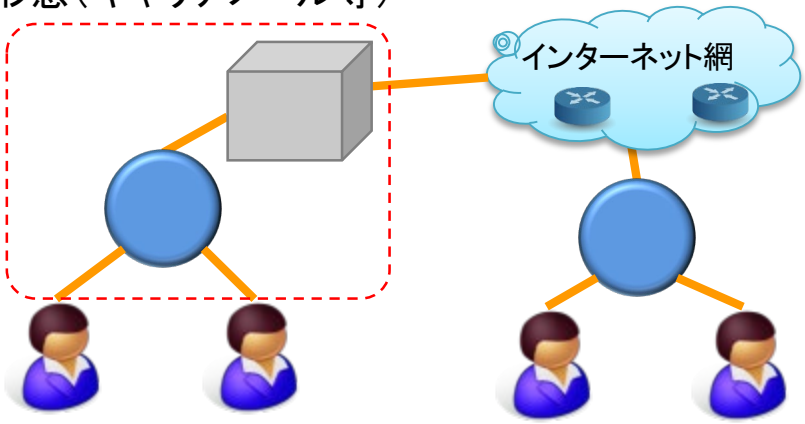
他者の電気通信回線設備を使用して、特定の通信サービスを提供するための電気通信設備を用いて通信サービスを提供する形態（メッセージ通信サービス等）



＜通信インフラ提供者かつ通信サービス提供者の例＞

(D) インフラ・サービス複合モデル

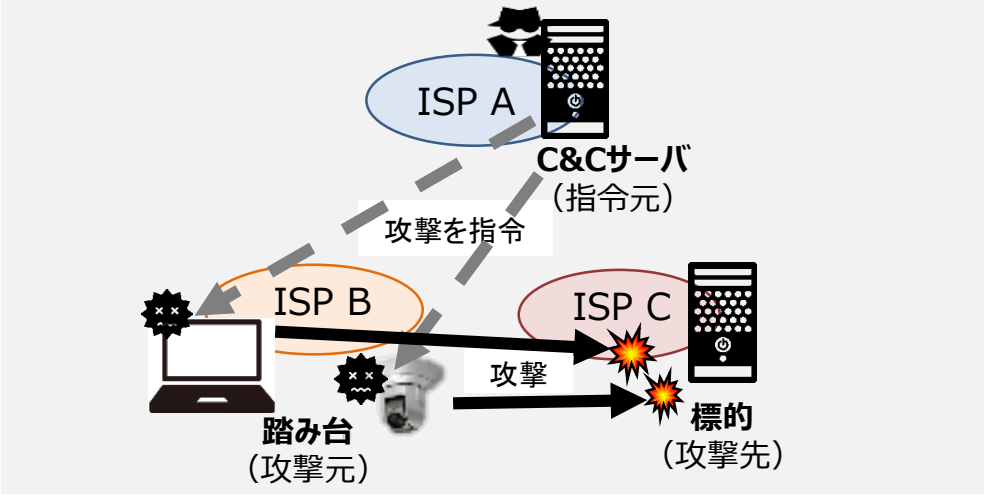
自ら電気通信回線設備を設置するとともに、特定の通信サービスを提供するための電気通信設備を設置して、インターネット網を介した通信サービス提供も可能な形態（キャリアメール等）



②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策（事業者間連携によるサイバー攻撃対策）

- サイバー攻撃の複雑化・巧妙化、グローバルプレーヤーを含む電気通信事業に関与するステークホルダーの増加や電気通信事業の提供構造の複雑化等により、情報漏えいや通信サービスの停止のリスクに対して単独の事業者のみでの対処が困難なケースが拡大しており、これに適切に対処するために、事業者間の連携協力を促進する仕組みが必要ではないか。
- 特に、サイバー攻撃の複雑化・巧妙化が進み、例えば、Mirai(マルウェア)によるDDoS攻撃に見られるように、他の事業者に接続されたIoT端末が踏み台となり、自らの事業用サーバが集中攻撃を受けてダウンするなどの事例が国内外で発生している。
- サイバー攻撃は、C&Cサーバ（指令元）、踏み台（攻撃元）、標的（攻撃先）となる機器の所在が複数のISPにまたがるケースが多く、これに対処するためには、指令元や攻撃元となり得るISPが、攻撃先となり得るISPと積極的に連携協力することが必要ではないか。
- 現在も、（一社）ICT-ISAC等の枠組み等を活用してISP間の連携が行われているが、法律上規定されているのは、事業者自身又は事業者の利用者がサイバー攻撃の送信先であることが特定された場合の認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）を介した連携に限られている。サイバー攻撃に予め備えるためには、平時における認定協会を介した連携協力についても対象に含めていくこととともに、ISP間における更なる連携協力の必要性について今後検討を深めることが適当ではないか。

＜指令元、攻撃元、攻撃先が複数のISPにまたがるサイバー攻撃の例＞



- ✓ DDoS: 攻撃：分散型サービス妨害（Distributed Denial of Service）攻撃の略。複数ネットワークに分散するコンピュータが特定のサーバへ一斉にパケットを送出し、通信路を溢れさせたり、大量の処理を実施させることによって機能を停止させる攻撃。
- ✓ C&Cサーバ: Command and Controlサーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に指令を送って制御するサーバコンピュータのこと。

②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策（事故の兆候段階からの報告義務）

- 電気通信事業法では、電気通信事業者に対し、電気通信業務に関し通信の秘密を漏えいしたとき、重大な事故が生じたとき等について、理由又は原因とともに遅滞なく報告することを求めている。
- なりすまし端末による不正アクセスなど、電気通信事業の事故原因が多様化する中で、ひとたび情報の漏えい等が生じた場合には回復が困難であること、通信サービスの停止による社会的な影響が大きくなってきていることから、事故の未然防止や被害軽減のための仕組みを構築することが適当ではないか。
- 具体的には、重大な事故等の兆候段階の事態についても遅滞なく報告を受け、実態把握や原因分析等を行い、当事者である電気通信事業者や関係省庁等と連携しつつ、適切な指導、助言等を行う仕組みが考えられるのではないか。
- 事故の兆候段階としては、①通信サービスの自らの提供環境に係る異常な変化、②電気通信設備そのものに係る異常な変化、③外部環境に係る異常な変化等を捉えていくことが適当ではないか。
- 具体的には、①通常の通信サービスの提供に際して発生することが想定されない事態（異常なトラフィックの増加、情報のアクセス権限の誤設定等）、②電気通信設備が正常に機能することを妨げる事態（認証情報の漏えい、不正アクセスの痕跡、広範に影響を及ぼすソフトウェア脆弱性の発見等）、③自らの通信サービスの提供に影響を及ぼす他者の電気通信設備、通信サービスに支障が生じる事態等が考えられるのではないか。
- 併せて、重大な事故等へとつながる兆候を整理し、得られた教訓等を電気通信事業者等において共有し、当該事故等の未然防止等につなげていくことが適当ではないか。

②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策（事故の兆候段階からの報告義務）

(1)鉄道事業法の例（鉄道事故等報告規則第4条第1項）

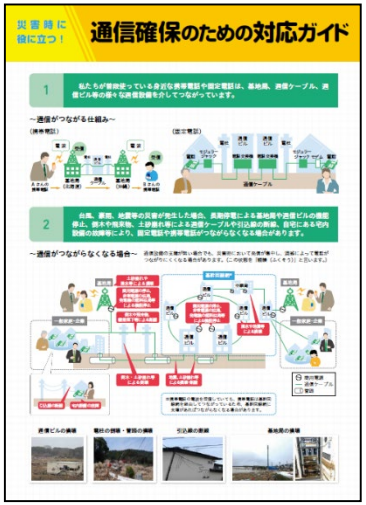
一　閉そくの取扱いを完了しないうちに、当該閉そく区間を運転する目的で列車が走行した事態
二　列車の進路に支障があるにもかかわらず、当該列車に進行を指示する信号が現示された事態又は列車に進行を指示する信号を現示中に当該列車の進路が支障された事態
三　列車が停止信号を冒進し、当該列車が本線における他の列車又は車両の進路を支障した事態
四　列車又は車両が停車場間の本線を逸走した事態
五　列車の運転を停止して行うべき工事又は保守の作業中に、列車が当該作業をしている区間を走行した事態
六　車両が脱線した事態であって次に掲げるもの
　イ　本線において車両が脱線したもの
　ロ　側線において車両が脱線し、本線を支障したもの
　ハ　側線において車両が脱線したものであって、側線に特有の設備又は取扱い以外に原因があると認められるもの
七　鉄道線路、運転保安設備等に列車の運転の安全に支障を及ぼす故障、損傷、破壊等が生じた事態
八　車両の走行装置、ブレーキ装置、電気装置、連結装置、運転保安設備等に列車の運転の安全に支障を及ぼす故障、損傷、破壊等が生じた事態
九　列車又は車両から危険品、火薬類等が著しく漏えいした事態
十　前各号に掲げる事態に準ずる事態

(2)航空法の例（航空法施行規則第166条の4）

一　次に掲げる場所からの離陸又はその中止
　イ　閉鎖中の滑走路、ロ　他の航空機等が使用中の滑走路
　ハ　法第九十六条第一項の規定により国土交通大臣から指示された滑走路とは異なる滑走路、ニ　誘導路
二　前号に掲げる場所又は道路その他の航空機が通常着陸することが想定されない場所への着陸又はその試み
三　着陸時において発動機覆い、翼端その他の航空機の脚以外の部分が地表面に接触した事態
四　オーバーラン、アンダーシュート及び滑走路からの逸脱（航空機が自ら地上走行できなくなつた場合に限る。）
五　非常脱出スライドを使用して非常脱出を行つた事態
六　飛行中において地表面又は水面への衝突又は接触を回避するため航空機乗組員が緊急の操作を行つた事態
七　発動機の破損（破片が当該発動機のケースを貫通した場合に限る。）
八　飛行中における発動機（多発機の場合は、二以上の発動機）の継続的な停止又は出力若しくは推力の損失（動力滑空機の発動機を意図して停止した場合を除く。）
九　航空機のプロペラ、回転翼、脚、方向舵、昇降舵、補助翼又はフラップが損傷し、当該航空機の航行が継続できなくなつた事態
十　航空機に装備された一又は二以上のシステムにおける航空機の航行の安全に障害となる複数の故障
十一　航空機内における火炎又は煙の発生及び発動機防火区域内における火炎の発生
十二　航空機内の気圧の異常な低下
十三　緊急の措置を講ずる必要が生じた燃料の欠乏
十四　気流の擾乱その他の異常な気象状態との遭遇、航空機に装備された装置の故障又は対気速度限界、制限荷重倍数限界若しくは運用高度限界を超えた飛行により航空機の操縦に障害が発生した事態
十五　航空機乗組員が負傷又は疾病により運航中に正常に業務を行うことができなかつた事態
十六　物件を機体の外に装着し、つり下げ、又は曳航している航空機から、当該物件が意図せず落下し、又は緊急の操作として投下された事態
十七　航空機から脱落した部品が人と衝突した事態
十八　前各号に掲げる事態に準ずる事態

③情報の適正な取扱いや通信サービスの提供等に関する利用者等への情報提供

- 電気通信事業法では、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法に関する事項の一部として、ふくそう、事故、災害等の場合の報告、記録、措置及び周知に関すること、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に関することを定めることとしている。
- 具体的には、安全・信頼性基準において、電気通信事業者は、情報通信ネットワークの安全・信頼性の確保の取組状況を適切な方法により利用者に対して公開すること、災害時においては、不要不急の電話を控えること及び通話時間をできるだけ短くすることについて周知・要請し、災害用伝言サービスを含めた音声通話以外の通信手段の利用等を平常時から呼びかけることとしている。
- また、事故・ふくそうが発生した場合又は利用者の混乱が懸念される障害が発生した場合には、事故・障害の状況を適切な方法により速やかに利用者に対して理解しやすいように工夫して公開することとしている。
- さらに、情報提供の手段を多様化するとともに、利用者と直接対応する販売代理店、MVNO等に事故の情報を周知することとしている。
- 情報の取扱い等についても、電気通信事業者は、利用者に対して、情報の適正な管理に係る取組を適切な方法で公開することが適当ではないか。また、情報の漏えい・不適切な取扱い等が発生した場合には、その状況を適切な方法により速やかに利用者に対して理解しやすいように工夫して公開することが適当ではないか。



＜電気通信事業者による情報提供の例＞

- 災害時に役立つサービス（災害用伝言サービス、緊急速報、SMS等）の紹介
- 被災エリアでのWi-FiスポットSSID「00000JAPAN」の提供
- 復旧エリアマップの提供
- SNS等を活用した情報提供
- ハンドブックの作成、配布　等

＜総務省による情報提供の例＞

- 災害時に役立つ！通信確保のための対応ガイドの作成、配布
  - 電話がつながらなくなる場合に想定される原因とそれに対する一般利用者による対応策、通信事業者等が提供する被災者向けサービス等に関するリーフレット