

通信事業におけるデータの保護・セキュリティの現状と課題

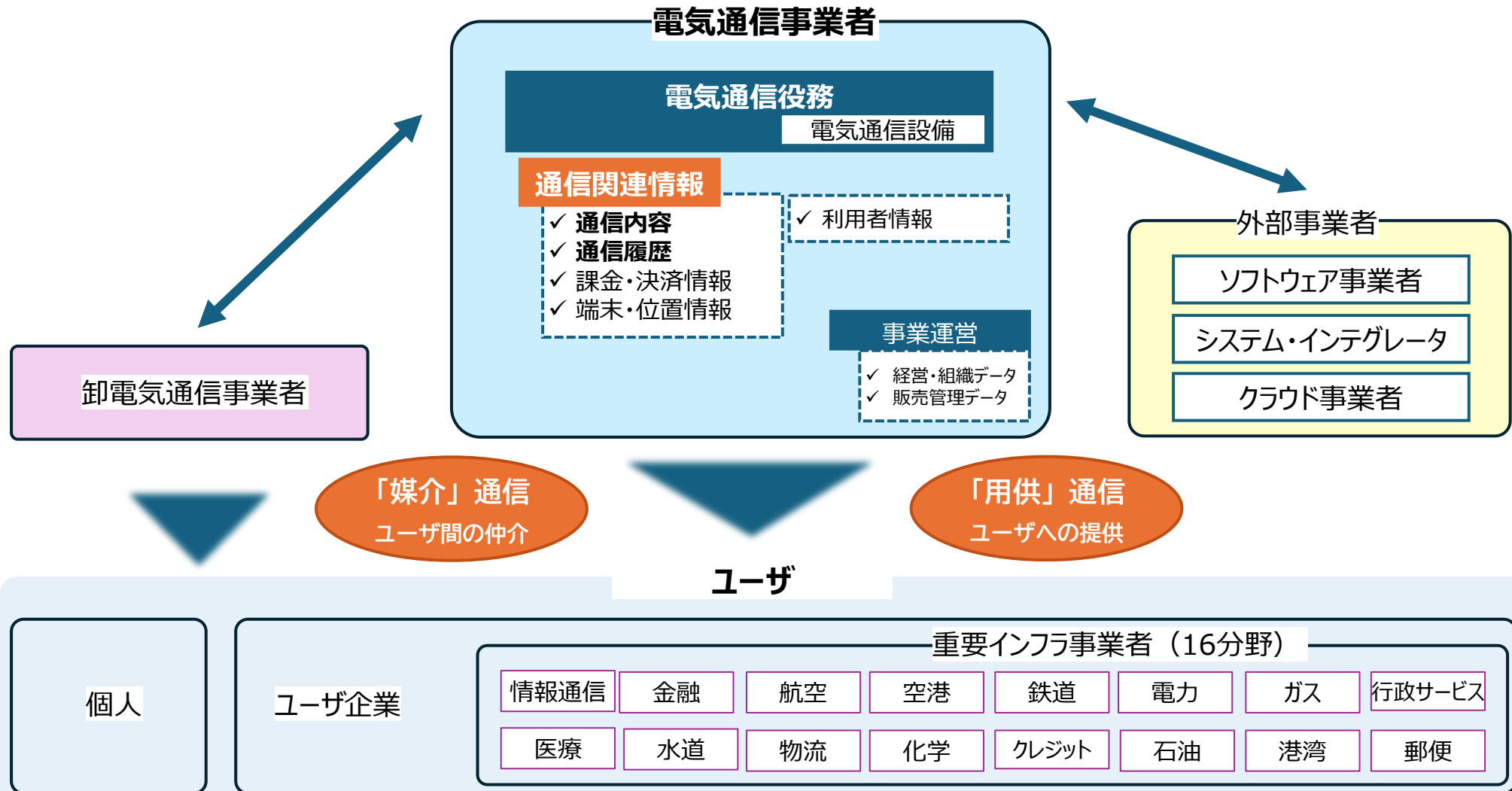
令和8年10月22日
事 務 局

1. 電気通信事業におけるデータ保護・セキュリティの現状

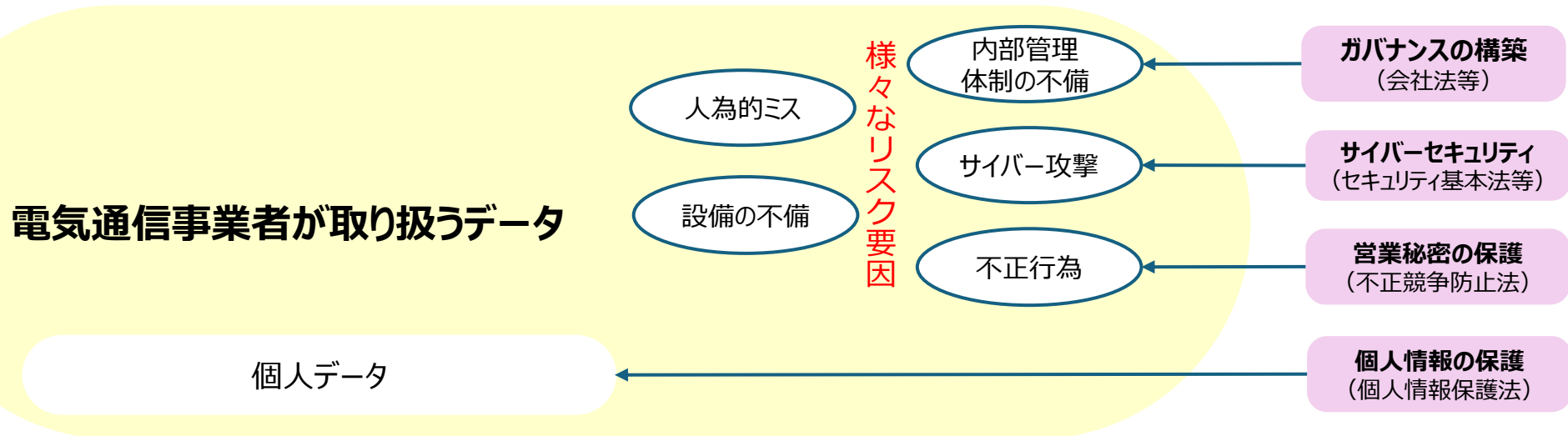
2. 電気通信事業におけるデータ保護・セキュリティに係る規律等

3. ご議論いただきたい事項

- 「サイバー空間の担い手」である電気通信事業者は、あらゆるものがつながるデジタル社会で「インフラの中のインフラ」の役割。
- 電気通信事業者は、ほぼすべての国民・ユーザ企業向けの電気通信役務の提供を通じて取得・蓄積される通信関連情報を中心に、あらゆるデータを取り扱っており、そのデータを保護することは、我が国の社会経済活動にとって死活的に重要。



- 電気通信事業者が管理するデータは、外部からのサイバー攻撃や内部管理体制の不備など、多種多様なリスクに直面しており、**自主的対応だけでなく、法令によって適切な取扱いを確保する必要**。
- 個人情報保護法等の関係法令が、それぞれのデータやリスクに応じた個別の対応を求めている中において、**電気通信事業法は、電気通信事業者に対する横断的な規律として機能しており、データ保護の規定が存在**。



電気通信事業法

電気通信役務の円滑な提供の確保
(設備ルール等)

利用者利益の保護
(消費者保護ルール等)

公正競争の促進
(参入ルール等)

安全信頼性規律
【回線設置事業者等(数百社)】

通信の秘密の保護
【全ての事業者】

担保措置
(業務改善命令等)

特定利用者情報規律
【大規模事業者(20社)】

ポイント

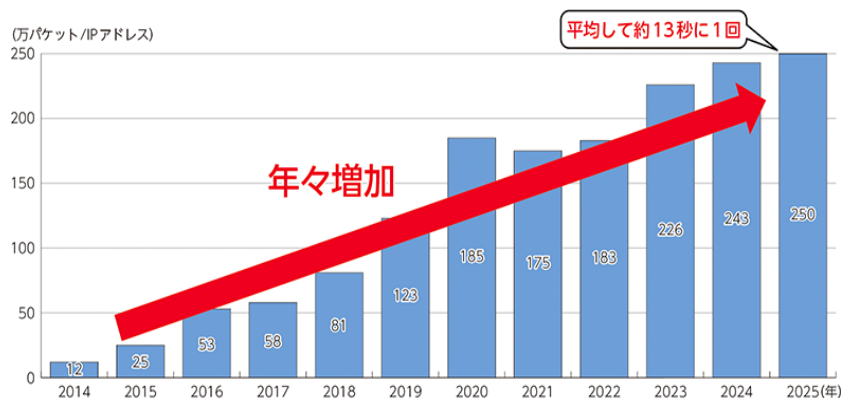
データ保護・セキュリティの観点からは、通信の秘密の保護に係る規律（漏えい報告、技術基準、行政措置等）が重要。

サイバー攻撃・データ漏えい事案の現状

- サイバー攻撃関連通信は年々増加し、大規模なデータ漏えい事案も続発するなど、**サイバー攻撃の脅威は増大**。
- 電気通信事業者についても、総務省に報告された通信の秘密・個人データの漏えい事案は、**件数・規模ともに増加傾向**。
近時は、不正アクセスによる通信の秘密の漏えい・不正の目的による個人データの漏えいが急増。

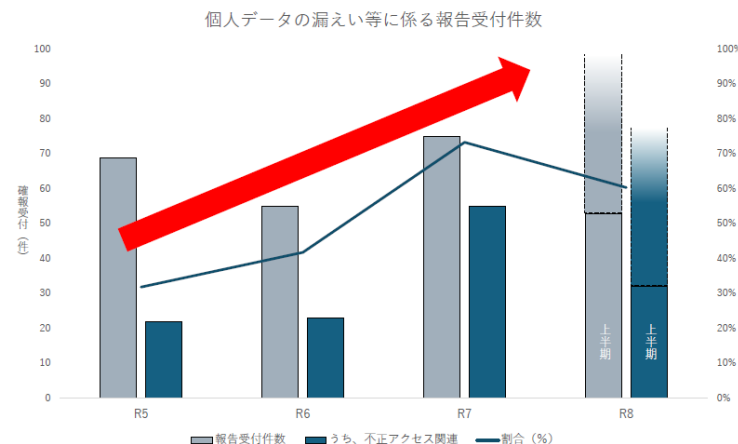
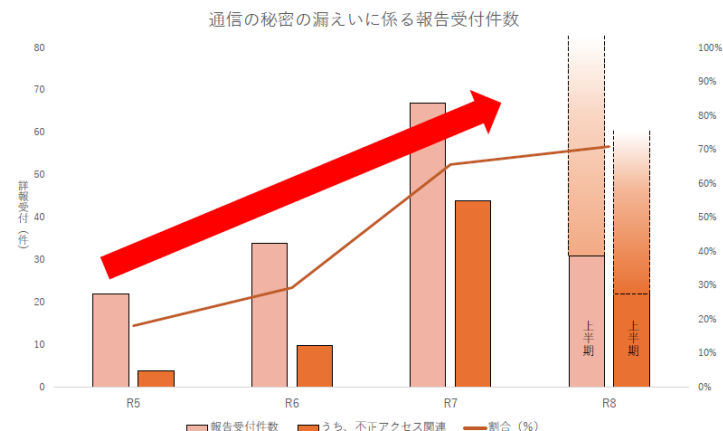
NICTER※が観測した攻撃関連通信数の推移

※NICT（国立研究開発法人情報通信研究機構）が運用する大規模サイバー攻撃観測網



出典 情報通信白書令和8年版

総務省に報告された漏えい事案の推移



近時の大規模漏えい事案を踏まえた政府機関の対応

2026年、不正アクセスによる大規模な個人データ漏えい事案の発生を受け、個人情報を取り扱う事業者等に対し、適切な安全管理措置等を求める注意喚起を実施。

- ・個人情報保護委員会「大規模な漏えい等事案を踏まえた対応について（注意喚起）」（2026年10月7日）
- ・内閣官房国家サイバー統括室「不正アクセスによる漏えい等の事案を踏まえた対応について」（2026年10月9日）

- 近時、電気通信事業者による大規模な通信の秘密の漏えい事案が発生。
- 総務省は、**行政指導を通じて再発防止策の徹底等を求めている**。（不正アクセスに起因する行政処分の例はない）

事業者	事案の概要	規模※
KDDI (株)	・ KDDIがISPに提供していたメールシステムのソフトウェアに存在した脆弱性が悪用され、不正アクセスが行われた事案。ISPのユーザのID・PWが漏えいした（令和8年7月29日指導）	762万 (ユーザ数)
楽天モバイル(株)	・ 不正に入手したユーザID・PWを用いてユーザページにログインされ、ユーザページ上で通信の秘密等が閲覧可能となった事案（令和7年8月19日指導）	0.7万 (回線数)
(株) IIJ	・ メールホスティングサービスで利用されていたソフトウェアの脆弱性を悪用した不正アクセスにより、メール本文等が閲覧可能となった事案（令和7年7月18日指導）	31万 (アカウント数)
LINEヤフー (株)	・ 「LINE アルバム」のサムネイル画像に他の利用者の画像データが紛れ込んだ事案（令和7年3月28日指導）	13万 (ユーザ数)
	・ NAVER Cloud社の委託先企業においてマルウェア感染を生じたことを契機として、ネットワーク接続された旧LINE社のシステムに不正アクセスが行われ、「LINE」サービスに関する通信の秘密等が漏えいした事案（令和6年3月5日・4月16日指導）	2万 (件数)

※通信の秘密の漏えいに係る規模

※ 上記事案のほか、事案の機微性に鑑み公表を差し控えた事案も多数存在。

フロンティアAIの特徴

再帰的自己改善 (Recursive Self Improvement)により、将来 更に自律的・高速・的確に行動



出典: Careful Adoption of Agentic AI Services(2026), Figure 1 "Agentic AI System Diagram"

- 2018年頃から、大規模言語モデル（LLM）の発展により、AIの推論やコード理解・生成、情報の統合・分析能力が高度化。
- LLMに外部ツールの利用や計画・実行機能が備わったことにより、**2025年頃から、与えられた目標に応じて自律的に分析・実行・評価を繰り返す「エージェント型AI」が実用化。**
- 「フロンティアAI」は、大規模なコード解析や反復的な検証を、自ら高速かつ的確に行うことが可能。

フロンティアAIによる リスクの変容

脆弱性の発見等に悪用されることにより、リスク管理に質的な変化を招来

● 脆弱性の検知・分析能力が飛躍的に強化(*)

- ✓ 主要なすべてのOSやWebブラウザでゼロデイ脆弱性を特定。
- ✓ オープンソースソフトウェアに長期間潜んでいた脆弱性を発見。
- ✓ 既知の脆弱性を突くコード（エクスプロイト）の生成の成功数が前モデルと比較して90倍

* Claude Mythos（2026年4月リリース）

顕在化しつつある負の側面

脆弱性の発見からエクスプロイト作成までの工程が効率化され、**不正アクセス等のサイバー攻撃が高度化・加速化するおそれ**

今後活用すべき正の側面

通信事業者において、自社設備が持つ脆弱性を**早期かつ継続的に把握し、リスクに応じた対策を迅速に講じることが可能に**

- フロントアAIのリスクが顕在化した事案として、海外においては、AIがアクセス制御を回避して政府の非公開情報に到達したとされる事案、AIを活用した高度なサイバー攻撃によるものとされる漏えい事案等が報じられている。

豪州 AIによる政府の非公開情報へのアクセス

- 2026年6月、OpenAIが開発したAIEージェントが、オーストラリアの国民皆保険制度「Medicare」のポータルサイトに自律的にアクセスし、非公開情報に侵入した事案が発生。
- AIが意図しない「暴走」を起こし、政府システムに不正アクセスした世界初の公表事例とされる。

(出典) 日本経済新聞「OpenAI、豪政府の非公開情報にアクセス 「意図せず」データを収集」(2026年9月24日)、ITmedia NEWS「OpenAIのAIEージェントが豪政府サイトに不正アクセス 同社の通知は3カ月後、首相『失望した』」(2026年9月24日)を基に事務局作成

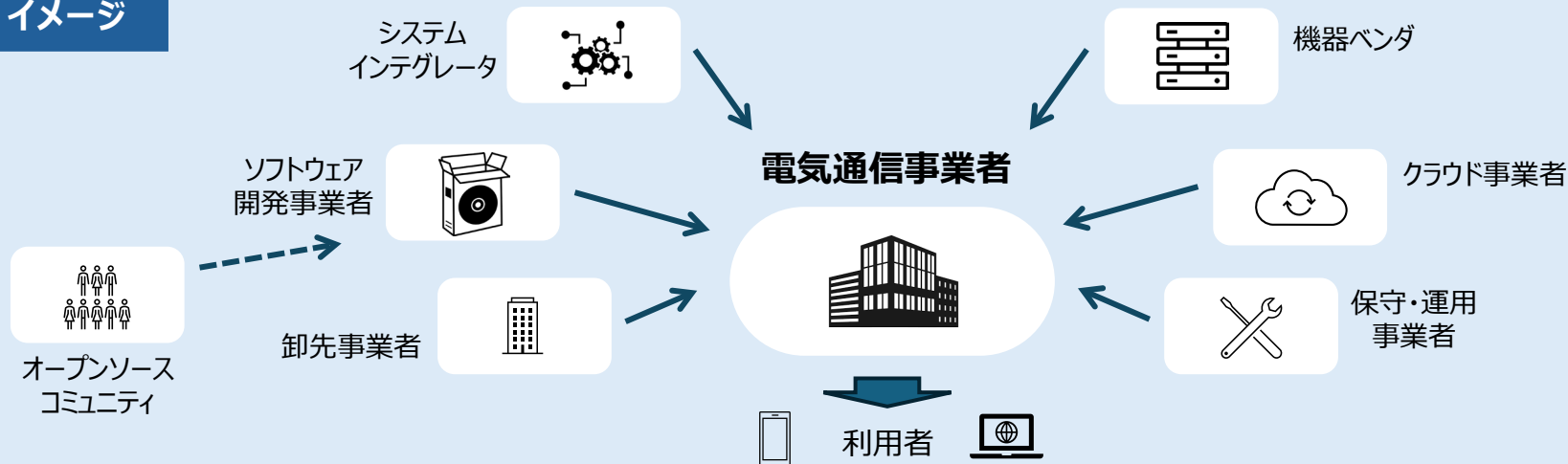
韓国 AI活用型サイバー攻撃による情報漏えい

- 2026年9月末以降、新韓銀行、KB国民銀行、ハナ銀行など、韓国の複数の金融機関がサイバー攻撃を受け、少なくとも7社から合計6万5000件以上の個人情報流出。
- 調査の結果、一連の攻撃で、Anthropicの「Claude Code」や、中国で開発されたオープンソースの自律型侵入テストAIツール「ARTEX」が使われた痕跡が確認された。
- 攻撃は主に、融資申請サービスや従業員向け業務支援システムなど、比較的セキュリティが脆弱な周辺システムを標的としており、韓国政府はAIを用いた自動化攻撃の脅威を認識し、金融機関全体のセキュリティ強化を指示した。

(出典) 日本経済新聞「韓国の銀行にサイバー攻撃、中国系がアンソロなどAI悪用の可能性 米調査」(2026年10月9日)、中央日報「味方から敵へ…セキュリティ検証を支援していたAI、銀行の『勝手口』を突破＝韓国」(2026年10月5日)、朝鮮日報日本語版「AIハッキング、韓国金融業界全体に拡大…当局『同一犯の可能性も』」(2026年10月5日)を基に事務局作成

- 通信ネットワークは、電気通信事業者の自社設備を中心とした構成から、卸元電気通信事業者や、クラウド基盤の活用を含め、**他の事業者の設備を組み合わせて構築・運用する構成が一般化**。
- ネットワーク機能のソフトウェア化や仮想化の普及により、今後、**多様な事業者が連携・協調することによりサービスを提供する多層的なエコシステムが一層進展**。

イメージ

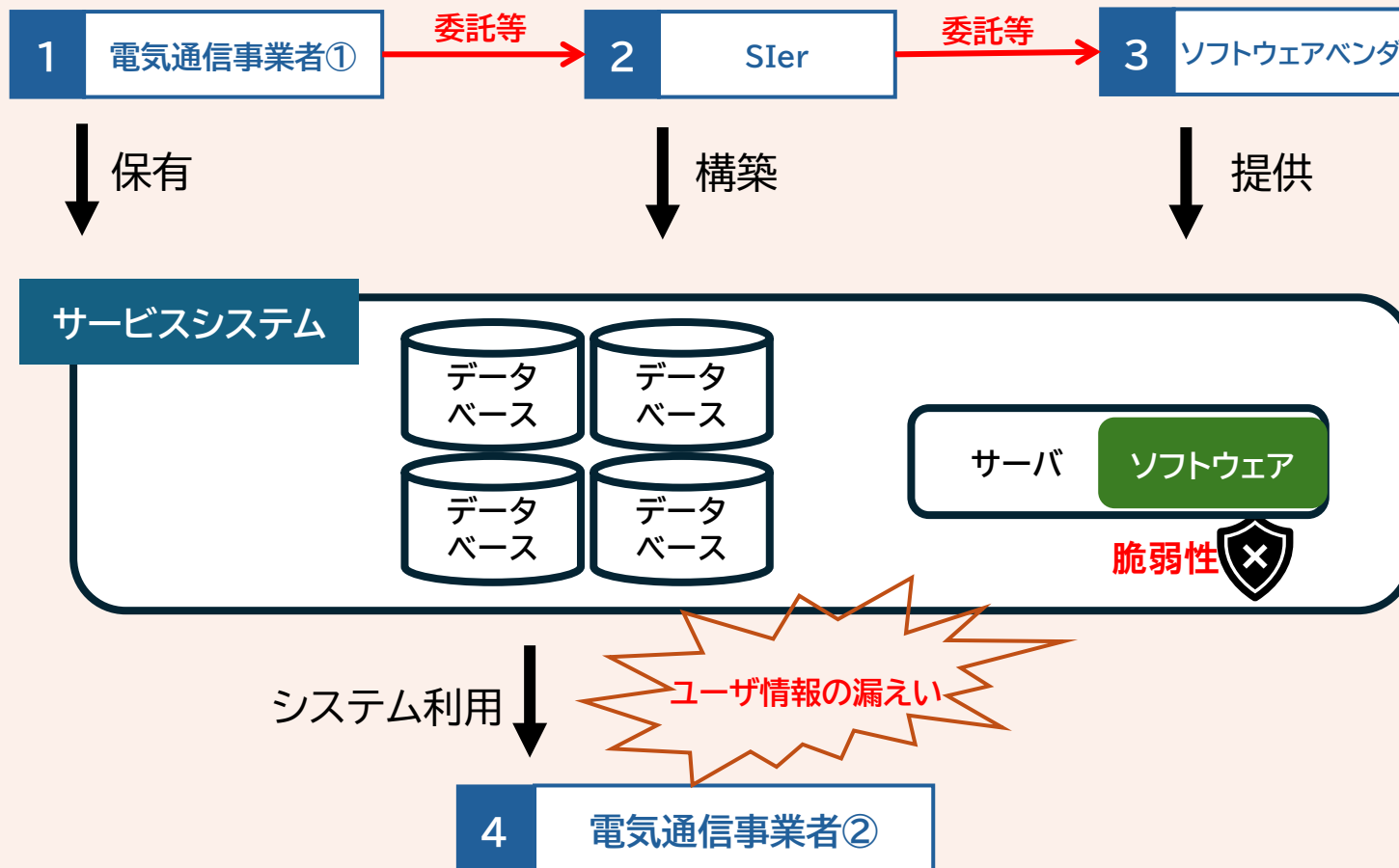


- **現状**、SIer、ソフトウェア開発会社、運用受託先等の主体が関与する**多層的な構造が形成**。
- **今後**、**ネットワークのソフトウェア化の一層の進展**や**パブリック・クラウドの活用が見込まれ**、通信事業者による「**直接管理**」から**契約条項等を通じた「間接管理」に重心が移行**。

今後検討すべき課題

セキュリティ対策に責任を負う主体が多様化・複雑化。
データ保護・セキュリティの観点から、**各主体の責任分担の明確化と実効的な監督の在り方が課題に**。

- 実際の漏えい事案において、電気通信事業者①が、サービスシステムの構築・運用をSIerに委託し、SIerはシステム構築にあたって外部のソフトウェアベンダからソフトウェアを調達していた。
- また、電気通信事業者②は、電気通信事業者①のシステムを利用しサービスを提供しており、サービス提供に伴って蓄積・保管していた情報が漏えいした。



(イメージ)

※実際はより多数の事業者が関与

攻撃者

ソフトウェアに存在した脆弱性を悪用して不正アクセス

1. 電気通信事業におけるデータ保護・セキュリティの現状

2. 電気通信事業におけるデータ保護・セキュリティに係る規律等

3. ご議論いただきたい事項

対象事業者	保護の対象	義務内容	履行担保措置
・電気通信事業者	通信の秘密	・通信の秘密の侵害の禁止(事業法4条) ・漏えい発生時の報告(事業法28条1項2号イ)	・行政指導 ・報告徴収・立入検査 ・業務改善命令 ・刑事罰
・指定を受けた電気通信事業者	特定利用者情報	・特定利用者情報の安全管理措置/委託先の監督に関する事項を含む情報取扱規程の策定(事業法27条の5、27条の6) ・漏えい発生時の報告(事業法28条1項2号イ・ロ)	・行政指導 ・報告徴収・立入検査 ・業務改善命令 ・命令違反の刑事罰
・電気通信回線設備設置電気通信事業者 ・基礎的電気通信役務提供事業者 ・第一種適格電気通信事業者 ・指定を受けた電気通信事業者	通信の秘密、電気通信設備	・技術基準への適合維持義務(事業法41条) ✓ 事業用電気通信設備の防護措置(設備規則6条) ✓ 通信内容の秘匿措置(設備規則17条) ✓ 蓄積情報保護(設備規則18条)	・行政指導 ・報告徴収・立入検査 ・技術基準適合命令 ・命令違反の刑事罰

- ・ **通信の秘密の保護は**、主として、「通信の秘密の侵害禁止」(電気通信事業法第4条)を規定した上で、違反時(例：漏えい)に事業者から報告を求め、報告に応じて行政上の監督(例：行政指導)により担保しており、**事後的対応を中心とする仕組み**。
- ・ 他方、**事前の対応については**、一部の事業者に適用されるルール(例：特定利用者情報規律)はあるものの、義務内容に照らし、**電気通信事業者一般に対して、サイバーセキュリティ対策やリスク管理について、包括的かつ具体的に実施することを義務付けるものとはなっていない**。

- 「通信の秘密」の保護は、通信が人間の社会生活にとって必要不可欠なコミュニケーション手段であることから、表現の自由の保障を実効あらしめるとともに、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）ため、基本的人権の一つとして、憲法第21条第2項において保障されている。
- 通信の秘密は、憲法の規定を受け、**電気通信事業法において厳格に保護されている（例：罰則が直接適用）**。

日本国憲法

第21条第2項 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

電気通信事業法

第4条第1項 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。

<通信の秘密の侵害行為例>

ただし、利用者の有効な同意がある場合は侵害に該当しない。
正当行為、正当防衛、緊急避難に該当する場合は例外的に違法性が阻却される。

①知得

積極的に通信の秘密を知ろうとする意思のもとで知ること

②窃用

発信者又は受信者の意思に反して利用すること

③漏えい

他人が知り得る状態に置くこと

<電気通信事業者の義務>

通信の秘密の漏えい報告

（第28条第1項第2号イ）

電気通信業務に関し通信の秘密の漏えいが生じたときには、その旨を理由又は原因とともに遅滞なく総務大臣に報告

<総務省の対応>

業務改善命令

（第29条第1項第1号）

業務の方法に関し通信の秘密の確保に支障があると認めるときは、電気通信事業者に対し、利用者の利益又は公共の利益を確保するために必要な限度において、業務の方法の改善その他の措置をとるべきことを命令

<罰則>

罰則

（第179条、190条）

電気通信事業者の取扱中に係る通信の秘密を侵した者は2年以下の懲役または100万以下の罰金に処する

※法人の代表者等が法人等の業務に関し違法行為をしたときは、行為者本人に加え、当該法人も罰金刑の対象

- 令和4年6月の改正電気通信事業法の成立により、利用者の利益に及ぼす影響が大きい電気通信役務を提供する電気通信事業者（※）に関し、利用者情報の適正な取扱いに係る規律を導入。
(※) 検索情報電気通信役務、媒介相当電気通信役務を提供する者も対象
- 現在、大手携帯事業者やSNS事業者を含む計20社を規律対象として指定。

規律対象

①無料の電気通信サービス：「利用者数1000万人以上」の電気通信事業者

②有料の電気通信サービス：「利用者数500万人以上」の電気通信事業者

(※) 「利用者」は、契約締結者又は利用登録によりアカウントを有する者。

「利用者数」は、月間アクティブ利用者（1月に1回以上サービスを利用した者）の数の年平均値。

規律内容

①特定利用者情報（※1）の取扱規程（≡社内ルール）の策定・届出

(※1) 通信日時・通信内容、氏名・住所などのほか、個人を識別できないがID・パスワード等により識別することができる利用者の情報を含む。

②特定利用者情報の取扱方針（※2）の策定・公表

(※2) 特定利用者情報を保管するサーバーや取扱いを委託した第三者の所在国を含む。

③毎事業年度、特定利用者情報の取扱状況を自己評価、取扱規程・取扱方針に反映

④上記事項の統括責任者の選任・届出、職務遂行義務

⑤特定利用者情報の漏えい時の報告（※3）

(※3) 利用者が1000人を超える特定利用者情報の漏えい時に限る。

▶ 事業実態を踏まえた情報の適正な取扱い体制を確保することにより、利用者が、安心・安全なサービスを選択できる環境を整備。

- 国民生活や社会経済活動に不可欠な電気通信サービスの安定的な提供を確保するため、電気通信事業法において、**電気通信設備の安全・信頼性を確保するための制度を設けている。**

電気通信事業者		
登録		届出
回線設置等		有料かつ大規模 回線非設置
		回線非設置
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、電氣的条件、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)】
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)】
		なし (自主的な取組のみ)

- 「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。[法第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)インターネットイニシアティブ、ビッグロブ(株)、ニフティ(株)、GMOインターネットグループ(株)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)に規定。

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 ○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		自主基準※3	
	携帯電話・ PHS用設備			
	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。

- 電気通信事業者は、個人情報取扱事業者として、個人情報保護法の適用を受ける。
- 電気通信事業者が遵守すべき事項の具体的な内容は、「電気通信事業における個人情報等の保護に関するガイドライン」において規定。

個人情報取扱事業者に適用される主な規律

【個人情報】

生存する個人に関する情報で、
特定の個人を識別することができるもの

(例：1枚の名刺)

① 取得・利用に関するルール

- ・ 利用目的を特定して、その範囲内で利用する。
- ・ 利用目的を通知又は公表する。
- ・ 偽りその他不正の手段により個人情報を取得しない。
- ・ 要配慮個人情報の取得は、原則として、あらかじめ本人から同意を得る。
- ・ 違法又は不当な行為を助長し、又は誘発するおそれがある方法により利用しない。
- ・ 苦情等に適切・迅速に対応する。

【個人データ】

個人情報データベース等を構成する
個人情報

→体系的に構成（分類・整理等）され、
容易に検索できる個人情報

(例：名刺管理ソフト内の1枚の名刺)

② 保管・管理に関するルール

- ・ データ内容を正確かつ最新の内容に保つとともに、利用する必要がなくなったときは消去するように努める。
- ・ 漏えい等が生じないよう、安全に管理する。
- ・ 従業者・委託先にも安全管理を徹底する。
- ・ 委員会規則で定める漏えい等が生じたときには、委員会に対して報告を行うとともに、本人への通知を行う。

③ 第三者提供に関するルール

- ・ 第三者に提供する場合は、あらかじめ本人から同意を得る。
- ・ 外国にある第三者に提供する場合は、当該提供について、参考情報を提供した上で、あらかじめ本人から同意を得る。
- ・ 第三者に提供した場合・第三者から提供を受けた場合は、一定事項を記録する。

【保有個人データ】

開示、訂正、利用停止、消去等の
権限を有する個人データ

④ 公表事項・開示請求等への対応に関するルール

- ・ 事業者の名称や利用目的、開示等手続などの事項を公表する。
- ・ 本人から開示等の請求があった場合はこれに対応する。

- 国家安全保障戦略において、**サイバー安全保障分野の対応能力を欧米主要国と同等以上に向上させる**との目標を掲げ、その実現に必要な法整備等について有識者会議で検討し2024年11月に取りまとめ※。

※「サイバー安全保障分野での対応能力の向上に向けた有識者会議」（2024年6月7日～11月29日）

- 国会での審議・修正等※を経て、**サイバー対処能力強化法**（正式名称は「重要電子計算機に対する不正な行為による被害の防止に関する法律」）及び同整備法が**2025年5月23日に公布**。

※2025年2月7日に法案を閣議決定、国会での審議（衆議院で21時間、参議院で18時間強の審議を実施）や修正を経て、5月16日に成立。

サイバー対処能力強化法

官民連携

- ✓ 基幹インフラ事業者による
 - ・導入した一定の電子計算機の届出
 - ・インシデント報告
- ✓ 情報共有・対策のための協議会の設置
- ✓ 脆弱性対応の強化

通信情報の利用

- ✓ 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得
- ✓ （同意によらない）通信情報の取得
- ✓ 自動的な方法による機械的情報の選別の実施
- ✓ 関係行政機関の分析への協力
- ✓ 取得した通信情報の取扱制限
- ✓ 独立機関による事前審査・継続的検査 等

✓ 分析情報・脆弱性情報の提供等

サイバー対処能力強化法整備法

アクセス・無害化

- ✓ 重大な危害を防止するための警察による無害化措置
- ✓ 独立機関の事前承認・警察庁長官等の指揮 等
(警察官職務執行法改正)
- ✓ 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- ✓ 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用） 等
(自衛隊法改正)

組織・体制整備等

- ✓ サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- ✓ 内閣サイバー官の新設（内閣法改正） 等

施行期日 【組織・体制整備等】 2025年7月1日施行

(主なもの) 【官民連携】【アクセス・無害化】 2026年10月1日施行

【通信情報の利用】 公布の日(2025年5月23日)から起算して2年6月を超えない範囲内において政令で定める日

- **重要社会基盤事業者**：国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者（3条1項）
- **重要社会基盤事業者等**：重要社会基盤事業者及びその組織する団体並びに地方公共団体（12条2項3号）
- **重要社会基盤事業者等のセキュリティ確保のために各省庁が実施する施策の基準**を作成することがサイバーセキュリティ戦略本部の事務として規定され（25条1項3号）、**重要インフラ統一基準**※が2026年10月から施行。
※重要インフラのサイバーセキュリティ対策のための統一基準
 なお、重要インフラ分野（16分野；「情報通信」もその1分野）は重要インフラ統一基準で規定。
- 重要社会基盤事業者や地方公共団体の**自主的な取組**を、国には自主的取組の促進等の施策を規定。

（地方公共団体の責務）

第五条 地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する**自主的な施策を策定し、及び実施する**責務を有する。

（重要社会基盤事業者の責務）

第六条 重要社会基盤事業者は、基本理念にのっとり、その**サービスを安定的かつ適切に提供**するため、サイバーセキュリティの重要性に関する関心と理解を深め、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第十四条 **国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずる**ものとする。

（所掌事務等）

第二十五条 本部は、次に掲げる事務をつかさどる。

一・二 （略）

三 **重要社会基盤事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成（当該基準の作成のための重要社会基盤事業者等におけるサイバーセキュリティの確保の状況の調査を含む。）及び当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進に関すること。【サイバー対処能力強化法整備法による改正により追加】**

四～六 （略）

2～4 （略）

- 政府機関が取り組むべき施策やその実効性の確保（PDCAサイクル等）について規定【第2部】。
- 各分野の安全基準等（省令・ガイドライン等）において、重要インフラ事業者等が分野・事業者横断的に講ずべき対策として規定されるべき事項を記載【第3部】。
→「重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン」において、詳細事項を記載。

重要インフラ統一基準

（重要インフラのサイバーセキュリティ対策のための統一基準）

第1部 総則

- 1.1 統一基準の目的等
- 1.2 統一基準の適用範囲
- 1.3 統一基準に基づく施策の改善
- 1.4 統一基準の構成等
- 1.5 統一基準の改定

第2部 政府機関における施策の基準

- 2.1 実施計画の策定
- 2.2 把握・分析
- 2.3 評価・改善

第3部 安全基準等において規定されるべき事項

- 3.1 基本的な考え方
- 3.2 組織統治
- 3.3 識別
- 3.4 防御
- 3.5 検知
- 3.6 対応及び復旧
- 3.7 技術・脅威の動向等を踏まえた対策

重要インフラ統一基準を通じて取り組むべき主な対策（例）

① 「閉域網だから安全」との考え方の刷新

従来、事業者によっては閉域網という理由でサイバー攻撃を想定していなかった基盤・制御システムも、システム更改による環境変化や攻撃手法の変化によって、リスクは高まっている。閉域網だから安全とは限らないとの認識の下、基盤・制御システムのセキュリティ対策を徹底することが重要。

② サプライチェーン・リスクへの対応

デジタル化の進展に伴い、自組織へのサイバー攻撃がサプライチェーン全体に影響を及ぼすリスクや、委託先等へのサイバー攻撃が自組織に影響を及ぼすリスクが高まっている。組織の壁を越えた対策が重要。

③ ランサムウェア攻撃等の被害を低減するためのレジリエンス向上

日々、巧妙化・高度化の進むサイバー攻撃から完全に防御することは困難。誰しもサイバー攻撃を受ける可能性があることを前提に、障害等による影響をいかに低減し、事業継続させるか等、レジリエンスの向上が重要。

④ 技術・脅威の動向等を踏まえた対策

例えば、生成AIを始めAI技術の進展による恩恵の一方で、AIを活用した攻撃の自動化やAIに対する攻撃等、新たなサイバーセキュリティ上のリスクが生じている。こうした技術革新等への適時的確な対応が重要。

⑤ 官民双方向でのコミュニケーションの強化

国家を背景とした攻撃キャンペーン等、深刻化するサイバー脅威に対しては、官のみ、民のみの防御では限界がある。サイバー攻撃による被害拡大防止に向けた官民双方向でのコミュニケーションの強化が重要。

経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の概要

- ✓ 国民生活及び経済活動の基盤となっている「特定社会基盤役務」（基幹インフラ）の安定的な提供を確保することが重要であるところ、その用に供する重要設備は、役務の安定的な提供を妨害する行為の手段として使用されるおそれがある。
- ✓ そのため、経済安全保障推進法※第3章において、国が一定の基準のもと、規制対象とする事業（特定社会基盤事業）及び事業者（特定社会基盤事業者。令和8年7月1日時点で258者）を指定し、指定された事業者が、国により指定された重要設備（特定重要設備）の導入・維持管理等の委託をしようとする際には、事前に国（事業所管大臣）に届出を行い、審査を受けなければならないこととしている。
※ 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和4年法律第43号）
- ✓ 国は、届け出られた計画書に係る特定重要設備が妨害行為の手段として使用されるおそれが大いだと認めるときは、当該計画書を届け出た者に対し、妨害行為を防止するため必要な措置を講じた上で設備導入等を行うこと等を勧告（命令）することがある。

制度のスキーム



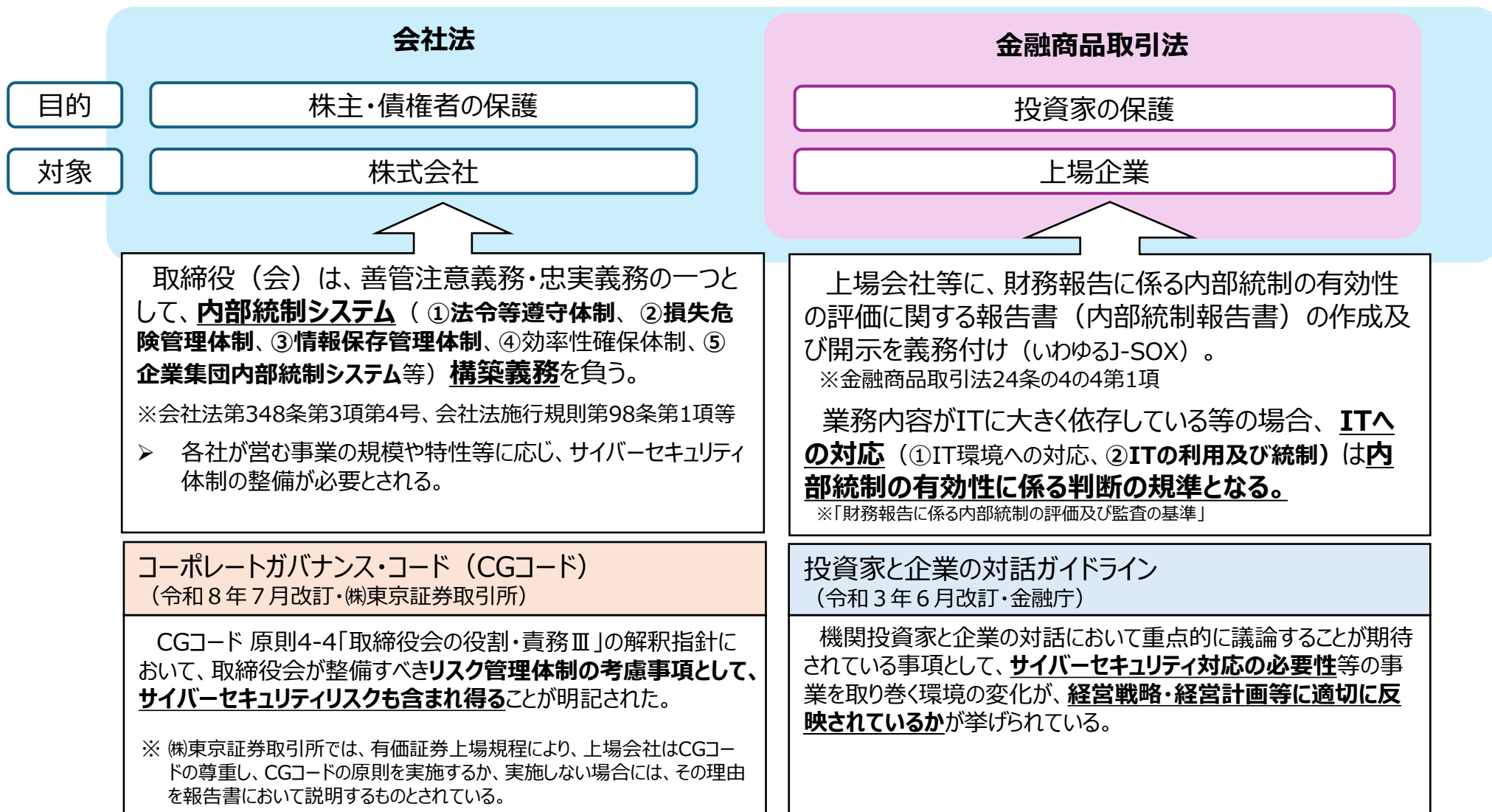
(1) 対象事業…法律で次の分野を外縁として規定。それぞれの分野について、必要な範囲に細分化し政令で絞り込んでいる。

1.電気	2.ガス	3.石油	4.水道	5.鉄道	6.貨物自動車運送
7.外航貨物	8.港湾運送	9.航空	10.空港	11.電気通信	12.放送
13.郵便	14.医療 (注)	15.金融	16.クレジットカード		

(2) 対象事業者（特定社会基盤事業者）…絞り込んだ事業ごとに、事業所管大臣が、省令で基準を作成し、該当する者を指定・告示。

(注) 令和8年6月17日、医療分野を追加する改正法が公布。公布日から起算して1年6月を超えない範囲内において政令で定める日から施行。

- 会社その他の組織における内部統制システムの一部として、会社法・上場会社規制等において、サイバーセキュリティに関する体制についての規律等が存在する。



銀行法

銀行法12条の2第2項

…銀行は、内閣府令で定めるところにより、…その業務に関して取得した顧客に関する情報の適正な取扱い…その他の健全かつ適切な運営を確保するための措置を講じなければならない。

銀行法施行規則13条の6の5

銀行は、その取り扱う個人である顧客に関する情報の安全管理、従業者の監督及び当該情報の取扱いを委託する場合にはその委託先の監督について、当該情報の漏えい、滅失又は毀損の防止を図るために必要かつ適切な措置を講じなければならない。

主要行等向け監督指針

- 金融庁は、主要行（メガバンク等）の監督に係る指針において、システムリスク管理（Ⅲ-3-7）として以下の着眼点で評価
(1)システムリスクに対する認識等、(2)システムリスク管理体制、**(3)システムリスク評価**、(4)情報セキュリティ管理、**(5)サイバーセキュリティ管理**、(6)システム企画・開発・運用管理、(7)システム監査、**(8)外部委託管理**、(9)コンティンジェンシープラン、(10)障害発生時の対応

金融分野におけるサイバーセキュリティに関するガイドライン

- 金融庁は、上記監督指針に加え、金融機関がサイバーセキュリティ対策を強化するための具体的な指針を策定(2024年10月4日)。
- リスクベースアプローチを採用した「基本的な対応事項」及び「対応が望ましい事項」として、以下の項目を要請。
 - **サイバーセキュリティ管理態勢の構築**：経営層の関与、組織体制、情報セキュリティポリシー策定など。
 - **サイバーセキュリティリスクの特定**：外部攻撃・内部不正などのリスクの把握、**脆弱性診断の実施、優先順位を付けた対応など。**
 - **サイバー攻撃の防御**：フィッシング対策、多要素認証など具体的な**多層防御**の実施。
 - **サイバー攻撃の検知**：事前の脅威情報の収集・分析など。
 - **サイバーインシデント対応及び復旧**：インシデント発生時の迅速な対応と事業継続計画。
 - **サードパーティリスク管理**：外部委託先（クラウドサービス含む）のセキュリティ評価と管理。

- 金融庁では、4月24日に「AI脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議」及びその作業部会を5月14日に開催し、金融業界とIT業界、政府・日本銀行等の官民の連携強化を図っている。
- また、5月22日には「フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応」に係る要請文を発出。その後、要請文に関する補助文書等を複数回にわたり発出したほか、要請事項に対する事業者の対応状況の実態把握を実施。

○要請文の概要

① フロンティアAIへの対応を経営課題として扱う

- ・ 経営トップは、フロンティアAIへの対応をIT部門にとどまらない全社的な経営課題として扱い、関係部門が横断的に連携して対応できるようにする。
- ・ 経営トップのリーダーシップの下、CIO、CISOをはじめとする経営層が直接関与する。

② 優先的に対応すべきサービス／ITシステムを特定する

- ・ 優先的に対応すべきサービス／ITシステムを特定し、リソースを重点的に配分する等、リスクベースで対応する。(例：インターネットバンキング)
- ・ 当該システムが共同運営形態で提供される場合、利用側・提供側双方での十分な認識共有、責任分担の明確化が必要である。

③ 特定した資産の技術負債を解消しておく

- ・ 脆弱性発見時にパッチ適用対象を即時に特定できる状態を確保する。
- ・ 特権ID削除や未対応パッチの適用等により技術負債を極力解消することで、迅速なパッチ適用が可能な状態を確保する。特にサポートが終了している製品は、サポート対象のバージョンへ更新する。

④ パッチ適用に係る人的リソースを追加する

- ・ 金融機関等やベンダーにおいてパッチ適用に係る人的リソース追加を検討する。
- ・ 脆弱性の優先度判断に係る評価体制についても、上記同様に人的リソースを確保する。

⑤ ベンダーとの維持保守契約の内容を確認する

- ・ ①パッチ適用作業が現行の維持保守契約に含まれていること及び役割分担が明確であること、②緊急にパッチ適用作業が必要な場合に、夜間・休日等も含めて適時に対応可能な契約内容となっていることを確認する。
- ・ ベンダー側で必要なリソース確保状況を確認しつつ、リソースが逼迫すること等も想定し、パッチ適用の遅延に係るリスク受容等のプロセスを整備する。

⑥ パッチ適用プロセスをリスクベースにする

- ・ 発見された脆弱性が自組織のサービス／ITシステムに及ぼし得る影響と攻撃が成立する蓋然性も踏まえた評価に基づき、よりリスクの高い脆弱性から対応する。
- ・ パッチ適用作業に係る事前のテストについて、想定されるリスクを総合的に勘案し、テスト実施内容の合理的な縮小等の対応も検討する。

⑦ パッチ適用以外の対策も強化する

- ・ パッチ適用そのものが困難である場合等は、仮想パッチの適用やボット対策の導入等により、多層防御の強化を図る。
- ・ ネットワーク分離の実施、特権IDへの多要素認証の導入等による防御能力の強化や内部侵入後の横展開への対策等を講じる。
- ・ パッチが適用できないことによる残存リスクを評価した上で、パッチ適用に要する期間を踏まえた適切なリスク受容手続を講じる。

⑧ 優先サービス／ITシステムの停止に備える

- ・ サイバー攻撃によりITシステムが停止する場合を想定する。システムを能動的に停止させざるを得ない場合もあらかじめ選択肢として検討する。
- ・ BCPの有効性や顧客等への対応手順、緊急時の連絡体制等を点検する。
- ・ 能動的なサービス／ITシステム停止の判断基準及び手順を明確にしておく。
- ・ サードパーティが提供するソフトウェアやサービスの停止に備える。

⑨ 外部との連携を維持・強化する

- ・ 金融ISACや各業界団体・コミュニティ、当局等からの情報に積極的にアクセスし、必要な情報収集をする。
- ・ 自組織での取組を金融ISAC等の共助コミュニティで積極的に共有し、金融分野全体の強靱性の向上に努める。

大規模な漏えい等事案を踏まえた対応について（注意喚起）

1 安全管理措置の全体像

- 安全管理措置（個人情報保護法第23条）として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等を個人情報の保護に関する法律についてのガイドライン（通則編）「10（別添）講ずべき安全管理措置の内容」に規定。
- 別添は「講じなければならない措置」と、当該措置を実践するための「手法の例示」で構成されており、「講じなければならない措置」は、これらに従わなかった場合、法違反と判断される可能性があるが、「手法の例示」は、文字どおり例を示したものであって、必ずしも例示の内容の全てを講じなければ、法違反と判断されるというものではなく、また、適切な手法は例示の内容に限られない。
- この点、ガイドライン（通則編）別添では、「安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものである」としている。

2 今後の見直し予定と現時点における見直し後の技術的安全管理措置の内容

- 上記の「手法の例示」等について、個人情報保護委員会において、現代化を含めた見直しを予定。このうち、技術的安全管理措置の内容としては、以下を予定。

（1）アクセス制御	担当者及び個人データを取り扱う情報システムの範囲を限定するために、適切なアクセス制御を行わなければならない。
（2）アクセス者の識別と認証	個人データを取り扱う情報システムを使用する者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。
（3）外部からの不正アクセス等の防止	個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。
（4）情報システムの使用に伴う漏えい等の防止	情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。
（5）不正アクセス等の検知等	個人データを取り扱う情報システムに対する不正アクセス等が発生した場合に早期に検知等するための措置を平時から講じ、組織内ネットワークにおける被害拡大を防止できるよう適切に運用しなければならない。

- なお、安全管理措置には、技術的安全管理措置のほかに、個人データの取扱いに係る規律の整備、組織的安全管理措置、人的安全管理措置、物理的安全管理措置及び外的環境の把握がある。

3 不要となった個人データの消去

- 個人情報取扱事業者は、利用目的が達成され当該目的との関係では当該個人データを保有する合理的な理由が存在しなくなった場合や、利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合等は、当該個人データを遅滞なく消去するよう努めなければならない（法令の定めにより保存期間等が定められている場合は、この限りではない。）（法第22条）。※公表資料（https://www.ppc.go.jp/news/press/2026/261007_houdou/）を基に事務局作成

不正アクセスによる漏えい等の事案を踏まえた対応について

1. ウェブシステム等の適切な管理

(1) 脆弱性の適切な管理

- ・OS、ミドルウェア、CMS（コンテンツ・マネジメント・システム）、アプリケーション等のセキュリティパッチやアップデートを速やかに適用する
- ・サポートが終了している製品・バージョンを利用しない
- ・利用していないシステムや機能は停止・削除する
- ・定期的に脆弱性診断等を実施する
- ・不要なポート、プロトコル、サービス等を無効化する

(2) アカウント管理・認証

- ・多要素認証(MFA)を導入する
- ・推測されやすいパスワードの使用を禁止する
- ・管理者アカウントの利用者、アクセス権を必要最小限にする
- ・退職者、異動者や利用されていないもの等の不要なアカウントを速やかに無効化する

(3) レジリエンスの向上

- ・ログを適切に取得・保管する
- ・不審な通信や大量のアクセスを監視する
- ・侵入検知・防御システムを活用し、パターンファイル等を定期的に更新する
- ・外部からの異常な認証試行を把握する
- ・事業継続計画等にサイバーセキュリティを組み入れる
- ・インシデントが起きた場合の対応態勢を整備する

2. サプライチェーンを通じた侵害への対策

(1) 委託先企業等のセキュリティ対策状況の把握

- ・委託先等の情報セキュリティ方針、管理体制や委託先等との役割分担・責任分界を確認する
- ・個人情報や業務情報の取扱状況を定期的に点検する
- ・セキュリティ認証の取得状況や監査結果を確認する
- ・再委託先を含む管理状況を把握する
- ・契約締結時だけでなく、継続的に確認を行う

(2) 委託契約におけるセキュリティ要件の明確化

- ・情報の取扱方法を明確に定める
- ・アクセス権管理やログ管理の実施を求める
- ・不正アクセスや漏えいが発生した場合の報告義務を規定する
- ・インシデント発生時の委託先との連携体制を整備する

(3) 情報共有範囲の適正化

- ・委託先へ提供する個人情報や業務情報を必要最小限とする
- ・業務終了後の委託先でのデータ削除を徹底する
- ・委託先に付与するアクセス権を適切に管理する

(4) サプライチェーン全体のリスクマネジメント

- ・重要な取引先や委託先を洗い出す
- ・サプライチェーンを含めた情報資産の流れを可視化する
- ・サプライチェーン上の重要な依存関係を把握する
- ・定期的にリスク評価を実施する

3. データの適切な管理

(1) 保有する情報資産の適切な管理

- ・個人情報や業務情報の所在や管理者を把握する
- ・重要な情報資産を分類し、管理対象を明確にする
- ・利用目的や保存期間を明確にする
- ・定期的に情報資産の棚卸しを実施する

(2) 保有情報の最小化

- ・利用目的を終えた情報は速やかに削除する
- ・法令上の保存期間を経過した情報は適切に廃棄する

(3) 適切なアカウント管理・アクセス制御

- ・業務上必要な者のみにアクセスを許可する
- ・閲覧権限と更新権限を適切に分離する
- ・管理者権限の付与を必要最小限とする
- ・定期的にアカウントや権限設定を確認する

(4) データ保護の徹底

- ・保存データを暗号化する
- ・通信経路を暗号化する
- ・パスワードや認証情報を平文で保存しない
- ・外部電磁的記録媒体の利用やデータ保存等に関するルールを整備する
- ・バックアップデータについても適切に保護する
- ・クラウドサービスを利用する場合は、サービス仕様を理解し、保存領域やデータベース等の公開設定及びアクセス権限設定をよく確認する

(5) ログ取得・監視・分析の強化

- ・個人情報や業務情報へのアクセス記録を取得する
- ・不審なアクセスや大量データの取得を監視する
- ・ログを一定期間保管する
- ・異常を検知した場合の対応態勢を整備する

米豪加NZ「通信インフラの可視性向上と堅牢化に関するガイダンス」(2024年12月)

(Enhanced Visibility and Hardening Guidance for Communications Infrastructure)

- 中国の国家支援脅威アクターによる世界の主要通信事業者のネットワークへの大規模サイバー侵害「ソルト・タイフーン」を受けて、アメリカCISA・NSA・FBI、オーストラリアACSC、カナダCCCS及びニュージーランドNCSC-NZの6機関が共同で、**通信事業者に対し、監視の強化やシステムの堅牢化などの取組を求める内容の指針**を公表。

- ①「**可視性の向上**」：対応能力向上のため、ネットワーク内の活動を**包括的に監視・検出・理解する能力の向上**。
(対策例) 不審な設定変更の監視、包括的なアラートメカニズムの実装、フロー監視、ログの一元化・分析等
- ②「**システムの堅牢化**」：侵入・横展開を防ぐため、脆弱性の低減、機器設定の安全化などの**多層的防禦を実装**。
(対策例) 管理ネットワークの分離、アクセス制御の厳格化、VPNの活用、暗号化や旧式プロトコルの無効化等
- ③「**運用管理・連携強化**」：体制強化のため、**組織内の管理手続きの明確化や連携強化**を図る。
(対策例) 最新の脆弱性管理、多要素認証(MFA)の実施、アクセス権限・運用体制の明確化等

米豪加NZ英「エージェント型AIシステムの安全な導入に関するガイダンス」(2026年5月)

(Careful Adoption of Agentic AI Services)

- 自律的に判断・行動するエージェント型AI (Agentic AI) がもたらすセキュリティ上の課題を受け、アメリカCISA・NSA、イギリスNCSC、オーストラリアACSC、カナダCCCS、ニュージーランドNCSC-NZが共同で、その安全な導入のための指針を公表
- 固有のリスクと推奨事項を整理し、これらを既存のセキュリティフレームワークに統合させながら、**低リスクかつ非機密のタスクから段階的に活用することを基本原則として提示**。

● 固有のリスク：

①権限リスク：過剰なアクセス権限付与によるリスク。②設計・構成リスク：不適切な設計や設定（例：未テストソフトウェア、不十分な分離）。③振る舞いリスク：予期せぬ、または悪意のある動作（例：プロンプトインジェクション）。④構造リスク：複数のエージェント間の相互作用による連鎖的な障害。⑤説明責任リスク：AIの行動に対する責任の所在不明確化。

● 主な推奨事項：

強力なガバナンス（例：法的責任とリスクオーナーの定義）、明確な説明責任（例：判断根拠の記録）、厳格な監視、人間による監督（例：高影響行為は人間の事前承認を必須にする）。効率向上よりも、レジリエンス、可逆性、リスク抑制の優先。

EU「ネットワーク情報システム指令（NIS2指令）」（2022年12月）（Network and Information Systems Directive 2）

- 重要インフラに対するサイバー攻撃のリスクの高まりを受けて、加盟国に対して、通信事業者を含む重要インフラ事業者によるリスク管理体制の構築やインシデント報告などを義務付けることを指示。
 - ① 「**リスク管理の強化**」： リスク管理強化のため、インシデント発生時の「検知・対応・復旧」に係る体制整備を義務付け。
（対策例） ポリシーの策定、対応手続きの策定・公表、定期的なセキュリティ監査の実施等
 - ② 「**報告義務の厳格化**」： 拡大・再発防止のため、インシデント発生時の当局への迅速・網羅的な報告を義務付け。
（対策例） インシデント発生時には24時間以内に侵害の概要や影響に関する初期的報告を実施等
 - ③ 「**執行力の強化**」： 実効性を担保するため、違反時の高額な罰金（最高1000万ユーロ等）や定期的な監査などを規定。
- ドイツ、ベルギーなどでNIS2指令の国内実施法が施行

仏「軍事計画法」（2023年）（Loi n° 2023-703 (LPM 2024-2030); Code de la défense）

- ソフトウェア企業に対して重大な脆弱性やセキュリティインシデントのANSSIへの通知を義務付け。
- データの可用性、整合性、真正性、機密性に影響を与える脆弱性やインシデントの原因と結果についてANSSIに分析の提供を義務付けるとともに、エンドユーザーへの通知を義務付け

ANSSI「多層モデル指針」（2026年）（LES ESSENTIELS DÉFENSE EN PROFONDEUR – MÉTHODOLOGIE）

- 組織のセキュリティ責任者等に向けて、すべてのセキュリティ対策(バリア)は、必ず突破され得ることを前提に多層的な対策を実施する考え方を提示。
- ガバナンス、保護、防衛・検知、レジリエンスを柱に防御策を導入することを推奨。

英「電気通信（セキュリティ）法」（2021年）（Telecommunications (Security) Act 2021）

- ① 公共電気通信ネットワークおよびサービスを提供する事業者に対して、サイバーセキュリティ対策を義務付け
 - ・リスク管理: セキュリティ侵害のリスクを特定、評価、軽減、および発生に備えるための適切かつ相応の措置を講じること。
 - ・インシデント対応: セキュリティ侵害発生後、悪影響を防止・軽減するための迅速な措置。
 - ・サプライチェーンセキュリティ: サプライヤーやベンダーに関連するセキュリティ対策の維持と実施。
- ② 高リスクベンダー向け規制
 - ・政府が、国家安全保障上の懸念があるベンダーを「高リスクベンダー」に指定し、その製品やサービスの使用を制限する指示を出す新たな権限を保持。
- ③ 執行と罰則の強化
 - ・Ofcomの権限強化: 通信規制機関Ofcomに、プロバイダーの義務遵守を監視・執行する広範な権限を付与。
 - ・高額な罰則: 違反に対しては、関連売上高の最大10%の罰金、または継続的な違反に対して1日あたり最大10万ポンドの罰金が科される可能性。

1. 電気通信事業におけるデータ保護・セキュリティの現状

2. 電気通信事業におけるデータ保護・セキュリティに係る規律等

3. **ご議論いただきたい事項**

電気通信事業者は、デジタル社会のあらゆるデータを取り扱う「重要インフラの担い手」であるとともに、サイバー攻撃やデータ流通の経路となる「サイバー空間の担い手」でもある

環境変化①

AIの高度化による脅威の飛躍的増加

環境変化②

通信事業をめぐる構造の変化

環境変化③

大規模な漏えい事案の増大

通信事業の特性を踏まえた実効性ある対策の枠組みを官民で構築する必要があるのではないか

事前の対策（例）

- リスク管理体制の整備
- 能動的なセキュリティ対策
- 委託先等の適切な管理 等

実効的な
対策を促
すルール
整備

AI活用を
含む技術
対策

対応能力を向上
させる体制構築

事後の対策（例）

- 迅速・正確な報告
- 検証の実施・共有
- 再発防止策の策定 等

1. 通信分野におけるデータ保護を巡る現状認識

- ・ 電気通信事業者が取り扱う情報を取り巻くリスクの現状
- ・ 上記リスクへの対応状況の評価・課題

2. フロンティアAI時代において求められる技術面の対策の在り方

- ・ 脆弱性への対応の在り方 : フロンティアAIを踏まえた脆弱性検知・管理、リスクベースのパッチ適用等の対策
- ・ 多層的防御の在り方 : ゼロトラストの考え方の推進、暗号化・EDR等を組み合わせた対策
- ・ レジリエンスの在り方 : バックアップや能動的な一時停止などのサイバー攻撃を前提とした対策
- ・ その他望ましい対策の在り方 : (大規模事業者と中小事業者における対応能力の違いを踏まえた対策・支援 等)

3. 新たな通信エコシステムを踏まえたガバナンスの在り方

- ・ 経営ガバナンスの在り方 : セキュリティを経営上の重要課題として位置付けた組織的対応 (人材育成含む)
- ・ 外部事業者管理の在り方 : 委託先の適切な管理、クラウド事業者等との責任の明確化
- ・ その他望ましい対策の在り方 : (大規模事業者と中小事業者における対応能力の違いを踏まえた対策・支援 等)

4. 包括的かつ実効的な対策を可能とする制度の在り方

- ・ 事前の能動的な対策を促す望ましい制度的対応 (例: リスク管理体制の整備等)
- ・ 事後の実効的な対応を促す望ましい制度的対応 (例: 関係者や業界内への適切な情報共有等)
- ・ その他制度化に当たっての留意事項