参考資料

（第1回　資料1－2）

総務省

特定利用者情報の取扱いに関する規律の詳細における検討事項

令和4年6月

事務局

電気通信事業法の一部を改正する法律の概要
（利用者に関する情報の適正な取扱いに係る制度整備）

大量の情報を取得・管理等する電気通信事業者を中心に、諸外国における規制等との整合を図りつつ、利用者に関する情報の適正な取扱いを促進するための新たな規律を整備。

	【 現状・課題 】	【 規律の内容 】
利用者情報の適正な取扱い	➢ **デジタル変革時代のイノベーションを促進**するため**安心・安全な電気通信サービスの確保**が不可欠 ➢ **諸外国の法的環境の変化、サイバー攻撃の複雑化**により、利用者が安心して利用できる電気通信サービスの提供の確保が急務 ➢ 特に、**大量の利用者情報を取り扱う事業者**には一層の高い信頼性の確保が必要	**1. 利用者の利益に及ぼす影響が大きい電気通信事業者**(例：利用者数1000万人以上)**に対する義務** 利用者情報を守るための必要最小限の規律 → 効果 ・利用者情報※の取扱いに関する**社内ルール**(取扱規程)**の策定**、利用者情報の**取扱方針の公表等**（記載事項例：安全管理の方法等） → **電気通信サービスの高い信頼性を保持**するとともに、**利用者自らが安心して利用できるサービスを選択**することが**可能となる** ・利用者情報の取扱いに関する**自己評価**、取扱規程・取扱方針への反映 → **自ら PDCAを実施して、各事業者の実態を踏まえた情報の適正な取扱い体制を確保** ・利用者情報の**統括責任者**の選任等 → **全体的観点からの適切な判断や、情報漏えい時の迅速な対応が可能となる** ※ 利用者に関する情報のうち、通信の秘密に該当する情報、役務契約を締結又はID等により利用登録をした利用者の情報を想定。 **大規模な検索サービス**または**SNS**を提供する事業についても規律の対象とする。
利用者の情報の外部送信	➢ 利用者がアプリやwebサイトを利用する際、タグ等により、**利用者の意思によらず第三者に自身の情報が送信**されている場合がある	**2. 電気通信事業者※に対する義務** ・利用者に電気通信サービスを提供する際に、**情報を外部送信**する指令を与える電気通信を送信する場合、**確認の機会を付与** → 利用者が意図しない情報の外部送信がなくなり、**利用者が安心して電気通信サービスを利用することが可能となる** ※ 電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務を電気通信回線設備を設置することなく提供する電気通信事業（電気通信事業法第164条第1項第3号）を営む者を含む。利用の状況からみて利用者に与える影響が少なくない者に限る。

（参考）利用者に関する情報 の 適正な取扱い に係る 規律

電気通信事業 を営む者（＝ 電気通信事業法の対象範囲）

電気通信事業者（登録・届出 要）

利用者の利益に及ぼす影響が大きい **大規模な 電気通信事業者**
※ 要件を満たす**大規模な「検索」及び「SNS」を新たに電気通信事業者とする**

左記以外の
電気通信事業者

その他の電気通信事業（第三号事業）を営む者（登録・届出 不要）

※ 検索、 SNS、オンラインショッピングモール、掲示板、オンラインオークション 等が含まれる。

利用者情報の適正な取扱い

取扱規程

- **利用者情報(※1)の取扱いに係る取扱規程の策定・届出**
  - ✓ 安全管理、委託先の監督、取扱方針、自己評価に関する事項等を記載

  担保措置：変更命令・遵守命令等

取扱方針

- **利用者情報の取扱いに係る取扱方針の策定・公表**
  - ✓ 取得する利用者情報、利用の目的、安全管理の方法、営業所の連絡先等を記載

  担保措置：業務改善命令等

自己評価・反映

- **毎事業年度 情報の取扱状況を自己評価、取扱規程・方針に反映**

  担保措置：業務改善命令等

統括責任者

- **上記事項の統括責任者の選任・届出、職務遂行義務**
  - ✓ 管理的地位にあり実務経験のある者から選任、誠実な職務遂行義務等

  担保措置：業務改善命令等

※1 利用者に関する情報のうち、①**通信の秘密**に該当する情報、②**役務契約を締結**又は**ID等により利用登録をした利用者**の情報を想定。

なし
（自主的な取組のみ）

外部送信

- **利用者に関する情報(※2)を外部送信させる場合に確認の機会を付与**（※利用の状況からみて利用者に与える影響が少なくない者に限る）
  - ✓ 送信先等を当該利用者に通知又は公表、同意取得、オプトアウト措置のいずれかを実施

  担保措置：業務改善命令等

※2 **利用者の端末に記録**された当該利用者に関する情報(**氏名などの個人情報**、**閲覧履歴などの利用者の行動履歴に関する情報**などが該当、ただし、電気通信サービス利用に必要な情報（OS情報など)を除く。)

参考（既存規律）

○ **通信の秘密の保護、検閲の禁止**

利用の公平、事業の登録・届出、提供条件の説明、業務休廃止の周知、事故の報告義務等

特定利用者情報の取扱いに関する規律に係る検討事項（全体）①

令和４年電気通信事業法の一部を改正する法律における特定利用者情報の取扱いに関する規律の詳細に係る検討事項は以下のとおり。

※　赤字は特に検討を要し、本WGで検討することが必要と考えられる事項。

規律の対象者

検討事項①

■　内容、利用者の範囲及び利用状況を勘案し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）として、**総務省令で定めるところにより、**総務大臣が指定した電気通信事業者

※１　電気通信回線設備を設置することなく、次の電気通信役務を提供する者として、総務大臣が**総務省令で定めるところにより**指定する者により提供される電気通信事業を含む。

・　検索情報電気通信役務：入力された検索情報（検索により求める情報をいう。以下この号において同じ。）に対応して当該検索情報が記録されたウェブページのドメイン名その他の所在に関する情報を出力する機能を有する電気通信設備を他人の通信の用に供する電気通信役務のうち、その内容、利用者の範囲及び利用状況を勘案して**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**　検討事項②

・　媒介相当電気通信役務：その記録媒体（当該記録媒体に記録された情報が不特定の者に送信されるものに限る。）に情報を記録し、又はその送信装置（当該送信装置に入力された情報が不特定の者に送信されるものに限る。）に情報を入力する電気通信を不特定の者から受信し、これにより当該記録媒体に記録され、又は当該送信装置に入力された情報を不特定の者の求めに応じて送信する機能を有する電気通信設備を他人の通信の用に供する電気通信役務のうち、その内容、利用者の範囲及び利用状況を勘案して**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**　検討事項③

対象者の指定に際して報告を求める情報

■　総務大臣は、この法律の施行に必要な限度において、電気通信事業者、第三号事業を営む者に対し、その事業に関し報告をさせることができる。（**報告内容は省令である電気通信事業報告規則で規定**）　検討事項④

規律の対象となる情報（特定利用者情報）

■　利用者（※２）に関する情報のうち、①通信の秘密に該当する情報、②契約等する利用者を識別することができる情報であって**総務省令で定めるもの**。　検討事項⑤

※２　電気通信役務の提供を受ける契約を締結する者その他**これに準ずる者として総務省令で定める者**

特定利用者情報の取扱いに関する規律に係る検討事項（全体）②

規律の内容

(1)情報取扱規程

- **総務省令で定めるところにより**、特定利用者情報の取扱いに係る「情報取扱規程」（※３）を定め、届け出なければならない。

  ※３ 安全管理、委託先の監督、情報取扱方針、評価に関する事項、**その他総務省令で定める事項**を記載。 検討事項⑥

(2)情報取扱方針

- **総務省令で定めるところにより**、特定利用者情報の取扱いに係る「情報取扱方針」（※４）を定め、公表しなければならない。

  ※４ 取得する特定利用者情報の内容、利用の目的・方法、安全管理の方法、苦情等の連絡先、**その他総務省令で定める事項**を記載。 検討事項⑦

(3)評価・反映

- **総務省令で定めるところにより**、毎事業年度、特定利用者情報の取扱状況の自己評価を行うとともに、その結果を「情報取扱規程」や「情報取扱方針」に反映しなければならない。 検討事項⑧

(4)情報統括管理者

- **総務省令で定めるところにより**、「特定利用者情報統括管理者」（※５）の選任をしなければならない。

  ※５ 管理的地位にあり、**利用者に関する情報の取扱い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**を備える者から選任 検討事項⑨

- 選任し、又は解任したときは、**総務省令で定めるところにより**、遅滞なく、その旨を総務大臣に届け出なければならない。

(5)事故報告

- 通信の秘密の漏えい及び**特定利用者情報であって総務省令で定めるものの漏えい**時には、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告しなければならない。 検討事項⑩

規律の対象者

（検討事項①～③）

規律の対象となる電気通信事業者(役務)の基準(新法※第27条の5関係)

※　令和４年電気通信事業法の一部を改正する法律による改正後の電気通信事業法を「新法」という。

検討事項①

- 特定利用者情報の適正な取扱いの**規律の対象となる**（総務大臣が指定する）**電気通信事業者が提供する電気通信役務**（「内容、利用者の範囲及び利用状況を勘案し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」）**の対象基準について、検討が必要。**

検討の視点

- 利用者への影響が限定的な電気通信事業者に対する配慮も必要であるため、「電気通信事業ガバナンス検討会報告書（令和４年２月）」では「例えば、**国内総人口の約１割程度の1000万人以上」との基準が示された。**

※　なお、ＥＵのデジタルサービス法案では、超巨大プラットフォームの定義として、サービス受信者数が欧州人口の10%以上（4,500万人以上）に相当するサービスを指すとされている。
また、米国のプラットフォーム競争及び機会法案等では、5000万人以上の利用者数を有する等のプラットフォームを規制対象としている。
ドイツのネットワーク執行法では、200万人以上の登録利用者数を有するプラットフォーム事業者を規制対象としている。

- また、**参議院における**改正電気通信事業法案に対する**附帯決議として、「本法の趣旨を踏まえ、義務付けの対象外となる事業者においても特定利用者情報の適正な取扱いが行われるよう検討すること。」とされている。**

ご議論頂きたい事項

- 対象となる電気通信役務の基準として、例えば、以下が考えられるのではないか。

✓　利用者（契約締結者又は利用登録によりアカウントを有する者）数1000万人以上を有する電気通信役務

※「利用者数」は、前年度末(３月末)時点における(月に少なくとも一度利用した)**月間アクティブ利用者数の年平均値と**してはどうか。なお、検索サービスの利用者数は、スマートフォンにおいてはログインをした状態で検索サービスを使用することが一般的であるため、登録アカウント数を代替的に用いてはどうか。

- その他考慮すべき事項はあるか。
- なお、対象外となる電気通信事業を営む者にも、ガイドライン等で利用者情報の適正な取扱いの推奨が必要か。

（参考）規模要件に関する諸外国の事例

EU デジタルサービス法案　等 	■ **デジタルサービス法案**　※4億4,732万人（2020年） ✓ 規制対象である「超巨大プラットフォーム」について、**欧州域内の月間平均アクティブユーザー数が4500万人以上**であることが要件の１つとして挙げられている。 ■ **デジタル市場法案** ✓ 規制対象である「ゲートキーパー」について、**欧州域内の月間平均アクティブユーザー数が4500万人以上**であることが要件の１つとして挙げられている。
アメリカ　プラットフォーム競争・機会法案 	■ **プラットフォーム競争・機会法案**　※人口3億2,950万人（2020年） ✓ 規制対象である「対象プラットフォーム」について、**月間ユーザー数が5000万人以上**であることが要件の１つとして挙げられている。（Sec.3 (d)(2)） ■ **米国イノベーション・選択オンライン法案** ✓ 規制対象である「対象プラットフォーム」について、**月間ユーザー数が5000万人以上**であることが要件の１つとして挙げられている。（Sec.2 (h)(4)(B)(ｉ)（Ｉ）） ■ **ネットワーク執行法（NetzDG）**　※人口8,324万（2020年）
ドイツ ネットワーク執行法　等 	✓ ドイツ国内の**登録利用者数が 200 万人以上**のプラットフォーム事業者は、苦情処理に関する報告義務や、申告のあった違法コンテンツへの対応義務を負う。 ■ **セキュリティ要件カタログ** ✓ **10万人以上**の利用者数を有する場合には、重要性の高い事業者（standard criticality, elevated criticality, increased criticalityのうち後者２つの分類）としてより高いリスク対策を求められる。（5.3.1 重要性の分類）

「電気通信事業ガバナンス検討会」における第三号事業に係る検討

電気通信事業（第三号事業）に対する規制の現状

- 電気通信回線設備を設置せずかつ他人の通信を媒介しない電気通信事業（電気通信事業法第164条第１項第3号に該当する事業。以下「第三号事業」という。）については、電気通信事業法創設当時の技術等に鑑みれば、小規模なものしか想定されないか、特殊な形態のサービスであって、法の規律を課す社会的必要性が乏しいと考えられ、通信の秘密の保護と検閲の禁止を除き、電気通信事業法の規律の適用を除外されてきた。

〈出典：電気通信事業法逐条解説等〉

規律の必要性

- 近年、第三号事業であっても、以下の観点から、**利用者利益を保護する社会的要請**が高まってきている。

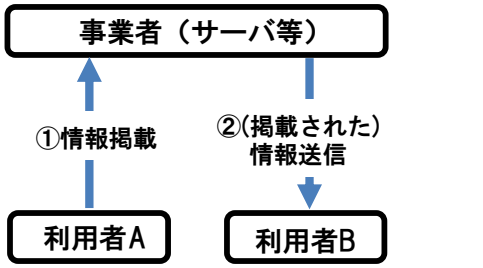
①【取り扱う利用者の情報量の膨大化】
インターネットの発展等に伴い、第三号事業であるにもかかわらず著しく利用者数が多く、登録や届出の対象となっている電気通信事業と同等又はそれ以上に電気通信役務の利用者に関する情報を取得・蓄積し得る電気通信事業が出現

②【社会経済活動における不可欠性の高まり】
インターネットにおいて他人間の通信の案内を行い多くの利用者が様々な電気通信役務にアクセスすることを助ける第三号事業等、社会経済活動における不可欠性が高く、様々な電気通信役務に係る基盤的な役割を担う第三号業事業が出現

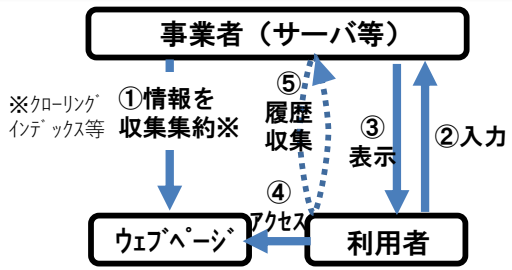
③【社会的・経済的影響力の高まり】
インターネットの発展等により、不特定多数の者がコミュニケーション等を行うプラットフォームを提供するような実質的に他人の通信を媒介する第三号事業や、利用者が様々な電気通信役務に接続するための基盤的な役割を担う第三号事業等、法の目的でもある電気通信の健全な発展にも大きな影響を与えるほど社会的・経済的影響が大きい第三号事業が出現

➡ **他人の通信を実質的に媒介する電気通信役務（媒介相当電気通信役務）**又は**検索サービス（検索情報電気通信役務）**であって、**利用者の利益に及ぼす影響が大きい場合に限り、第三号事業者についても規律の対象**とすることが適当。

媒介相当電気通信役務のイメージ



検索情報電気通信役務のイメージ



検索情報電気通信役務の詳細（新法第164条関係）

検討事項②

- **検索情報電気通信役務**（入力された検索情報（検索により求める情報をいう。）に対応して当該検索情報が記録されたウェブページのドメイン名その他の所在に関する情報を出力する機能を有する電気通信設備を他人の通信の用に供する電気通信役務のうち、その内容、利用者の範囲及び利用状況を勘案し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）**の詳細について、検討が必要。**

検討の視点

- 「電気通信事業ガバナンス検討会報告書（令和４年２月）」では、特に影響が大きい役務に対象を限定する観点から、（レストラン、商品等、特定分野のみの検索サービスは対象外とし）分野横断的な検索サービスを提供する電気通信役務であって、利用者数が非常に多いものに限って法の規律の対象とすることが適当である旨示された。
- なお、検索エンジンを規制対象としているEUの「ネットワークおよび情報システム（Network and Information Systems：NIS）指令」においては、「オンライン検索エンジン」の定義として、あらゆる主題の問い合わせに対応し、全てのウェブサイトの検索が可能であるもの等とされている。

【参考】EU ネットワークおよび情報システム（Network and Information Systems：NIS）指令 第4条(18))
「オンライン検索エンジン」とは、利用者が、キーワード、フレーズ、またはその他の入力によるあらゆる主題の問い合わせにより、原則として、すべてのWebサイトまたは特定の言語のWebサイトの検索を実行でき、要求されたコンテンツに関連する情報を見つけることができるリンクを返すデジタルサービスを意味する。

ご議論頂きたい事項

- 検索情報電気通信役務の詳細として、特に影響が大きい役務に対象を限定する観点から、以下の**どちらにも該当する役務**が考えられるのではないか。

1．利用者（契約締結者又は利用登録によりアカウントを有する者）数1000万人以上を有する電気通信役務

※利用者数は、前年度末(３月末)時点における**年平均月間アクティブ利用者数**としてはどうか。
検索サービスの利用者数は登録アカウント数で代替してはどうか。

2．(利用者に公開されている全てのウェブサイトの検索が可能な)分野横断的な検索サービスを提供する電気通信役務

媒介相当電気通信役務の詳細（新法第164条関係）

検討事項③

- **媒介相当電気通信役務**（その記録媒体に情報を記録し、又はその送信装置に情報を入力する電気通信を不特定の者から受信し、これにより当該記録媒体に記録され、又は当該送信装置に入力された情報を不特定の者の求めに応じて送信する機能を有する電気通信設備を他人の通信の用に供する電気通信役務のうち、その内容、利用者の範囲及び利用状況を勘案し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）**の詳細について、検討が必要。**

検討の視点

- 「電気通信事業ガバナンス検討会報告書（令和４年２月）」では、特に影響が大きい役務に限定する観点から、利用者数が非常に多く、コミュニケーションを実質的に媒介することを主として行うサービスであるものに限って規律の対象とすることが適切（付随的な実質的媒介や商取引に関する情報を扱う場合は対象外）である旨示された。※

（※）他人の通信の実質的媒介を行う電気通信役務について、①SNS、②レビュー機能やコメント機能等を付随的に有するサイト、③ネット・オークション、オンライン・フリーマーケット等が想定される。このうち、①SNSに関しては、利用者から送信されたコミュニケーションに係る情報を他の利用者が閲覧しうる状態にすることで、実質的にコミュニケーションに係る情報の媒介を行うことから、非常に多くの利用者を有する者に限り、規律の対象とすることが考えられる。また、②利用者からのレビュー機能やコメント機能等を付随的に有するサイトは、コミュニケーションに係る情報を実質的に媒介するものではあるが、役務全体における当該機能の不可欠性や利用者に与える影響等に鑑み、**あくまで付随的に実質的媒介の機能を提供する場合は、対象外とすることが考えられる**。なお、**付随性の判断基準としては、当該機能がなくても電気通信役務が成り立つか否かで判断することが考えられる**。③ネット・オークション、オンライン・フリーマーケット等は、利用者から送信（投稿）された出品物等に関する情報を他の利用者が閲覧しうる状態にすることで、実質的に通信の媒介を行うものではあるが、**取り扱う情報は、出品物の特徴や価格に関するものであり、主としてコミュニケーションに係る情報ではないことから、対象外とすることが考えられる**。（「電気通信事業ガバナンス検討会報告書（令和4年2月）」抜粋）

ご議論頂きたい事項

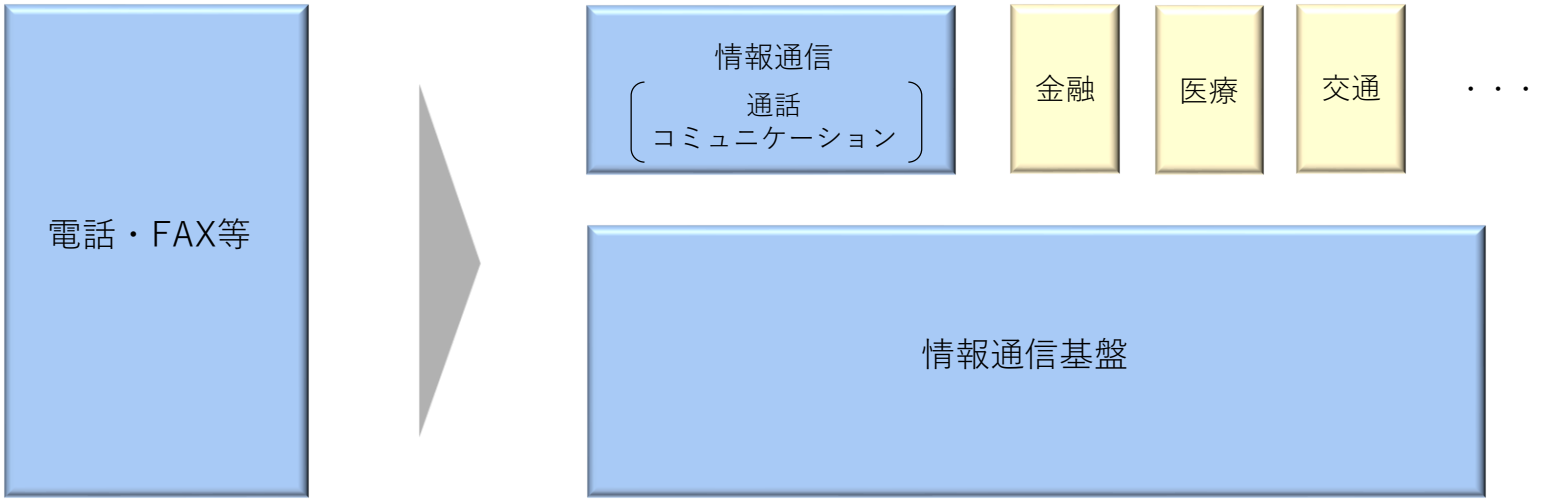
- 媒介相当電気通信役務の詳細として、必要最小限とするとともに、これまでの電気通信事業法の規律対象事業との近似性・連続性にも配慮し、**以下に該当する役務**が考えられるのではないか。

1．利用者（契約締結者又は利用登録によりアカウントを有する者）数1000万人以上を有する電気通信役務

※　利用者数は、前年度末(３月末)時点における**年平均月間アクティブ利用者数**としてはどうか。

2．ただし、付随的に媒介相当電気通信役務の機能を提供する電気通信役務及び特定の商取引に関する情報のみを扱う電気通信役務は、対象外とする

- 電気通信事業は、公益事業としての公共性を有するとともに、国家機能の維持及び国民の生命・財産の安全にとって不可欠な重要通信の確保など、国のインフラとして中枢神経的な機能を果たすもの。
- 国民の誰もが安心して利用でき、信頼性の高い電気通信サービスの提供が確保され、我が国の社会全体のイノベーション促進、デジタル化・DX推進を支える基盤として貢献することを通じて、電気通信事業の中長期的な発展が確保されるものと考えられる。
- 電気通信事業法の適用対象は、引き続き、電気通信インフラとしての情報通信基盤と情報通信分野の通話・コミュニケーション等のサービスとなることが基本。



出典：中村構成員提出資料より作成

規律対象者の指定に際して報告を求める内容

（検討事項④）

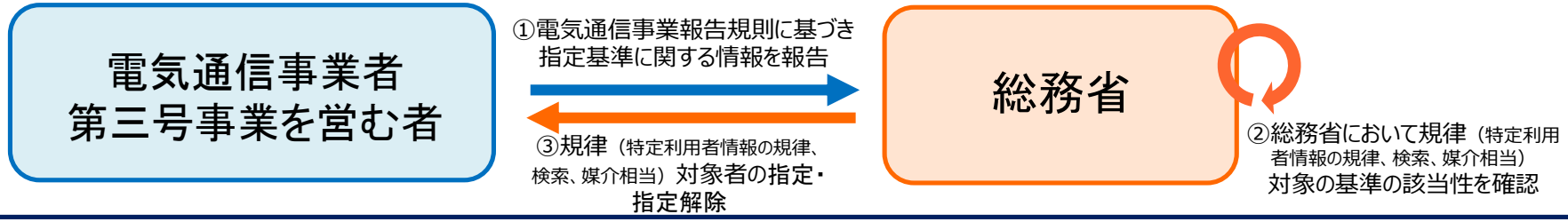
規律対象者の指定に際して報告を求める内容(新法第166条関係)

検討事項④

- 総務大臣は、この法律の施行に必要な限度において、電気通信事業者、第三号事業を営む者等に対し、その事業に関し報告をさせることができるとされているが、**規律対象者の指定に際して、報告を求める内容の詳細について、検討が必要。**

検討の視点

- 規律対象者の指定手続きとしては、まず電気通信事業法第166条及び電気通信事業報告規則に基づき、電気通信事業者及び第三号事業を営む者から一定の情報を報告いただき、当該情報に基づき、総務省において基準の該当性を確認の上、規律対象者の指定を行うことが想定される。このため、電気通信事業者及び第三号事業を営む者からの**報告を求める内容**は、基本的に**検討事項①～③で検討された基準に係る情報が想定**される。ただし、事業者側の準備も必要なため、利用者数の報告は基準を少し下回る段階からの報告が望まれるのではないか。



ご議論頂きたい事項

- 規律対象者の指定に際して、書面により報告を求める内容としては、以下が考えられるのではないか。

✓ **電気通信事業者**並びに検索情報電気通信役務及び媒介相当電気通信役務の（利用者数を除く）役務内容の要件に該当する役務を提供する**第三号事業を営む者**は、**毎年度**、**毎報告年度経過後１月以内**に、**当該報告年度の年平均月間アクティブ利用者**（契約締結者又は利用登録によりアカウントを有する者）**の数が900万以上である電気通信役務を提供している場合**は、**その利用者の状況（該当する電気通信役務と利用者数）**（正確な利用者数の算出が困難な場合は、10万単位等での報告も可能とすることが考えられるのではないか。）

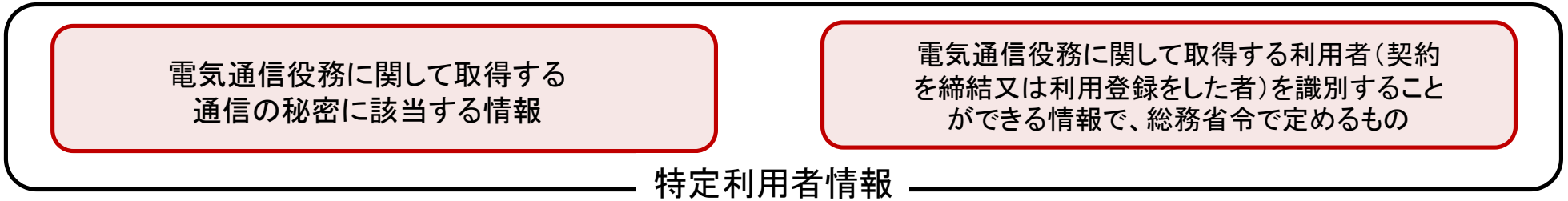
規律の対象となる情報

（検討事項⑤）

規律対象となる特定利用者情報の詳細（新法第27条の５関係）

検討事項⑤

- **規律対象となる特定利用者情報**（規律対象の電気通信役務に関して取得する利用者に関する情報のうち、通信の秘密に加え、利用者（契約を締結又はID等で利用登録をした者）を識別することができる情報であつて総務省令で定めるもの）**の詳細について、検討が必要。**



検討の視点

- 「電気通信事業ガバナンス検討会報告書（令和４年２月）」では、規律対象となる特定利用者情報は、**データベース化されているものに範囲を限定することが適当**である旨示されている。
- **個人情報保護法**において**安全管理措置等の対象とされているのは、個人情報データベース等を構成する個人情報**である個人データとされている（個人情報保護法第16条第３項、第22条等）。

※「個人データ」とは、個人情報データベース等を構成する個人情報をいう。(個人情報保護法第16条第３項)
※「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。(個人情報保護法第16条第１項)
一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

ご議論頂きたい事項

- 特定利用者情報は、通信の秘密に加え、利用者（契約締結又は利用登録によりアカウントを有する者）を識別できる情報であって、**「データベース等を構成する利用者（契約締結又は利用登録した者）の情報」**が考えられるのではないか。その他考慮すべき事項はあるか。

規律の内容
（検討事項⑥～⑩）

情報取扱規程の詳細①（新法第27条の６関係）

検討事項⑥

- **情報取扱規程に記載すべき事項**（法律では①安全管理に関する事項、②委託先の監督に関する事項、③情報取扱方針の策定・公表に関する事項、④評価に関する事項、⑤その他総務省令で定める事項を規定）**の詳細について、検討が必要。**

検討の視点

- 情報取扱規程は、電気通信事業者による自主的かつ実行的なガバナンスを確保することを目的とするものであり、「電気通信事業ガバナンス検討会報告書（令和４年２月）」では、**安全管理や委託先の監督等の方針、体制、方法を記載することが想定される旨、示されている。**

- **「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」**第12条では、安全管理措置が求められており、同ガイドラインの解説において、具体的に、**組織的・人的・物理的・技術的安全管理措置と外的環境の把握**が挙げられている。また、同ガイドライン第13条では、情報の管理に関する事項として、**従業者及び委託先の監督**が規定されている。

- 他国法令では、例えば、**ドイツの電気通信事業者法では**、暗号化の措置、可用性を確保する措置等の**技術的組織的防護措置等を内部規程において定めることとされている**（第166条）。また、**英国の電子コミュニケーション（セキュリティ対策）規制案**では、**セキュリティ侵害のリスクに関するビジネス手順等を定め**、定期的に見直すこととされている（第9条）。

- なお、日本産業規格の一つであるJIS Q 15001では、組織の各部門及び階層における個人情報を保護するための権限及び責任に関する規定、個人情報の適正管理に関する規定、個人情報保護リスクアセスメント及び個人情報保護リスク対応の手順に関する規定等を含む内部規程を文書化することとされている（ 附属書A.3.3.5 ）。

情報取扱規程の詳細②（新法第27条の６関係）

ご議論頂きたい事項

- 電気通信事業者による自主的かつ実効的なガバナンスを確保する観点から、情報取扱規程に記載すべき事項として、例えば、以下が考えられるのではないか。

1. 特定利用者情報の安全管理に関する体制及び方法に関する事項
   - 組織的安全管理措置（例：責任者の設置、漏えい等事案に対応する体制等報告連絡体制、マニュアル整備、自己点検・監査等）
   - 人的安全管理措置（例：研修の実施、誓約書の提出等）
   - 物理的安全管理措置（例：入退室管理、機器の持ち込み制限、盗難・紛失防止措置等）
   - 技術的安全管理措置（例：アクセス管理、不正アクセスやDDoS攻撃等サイバー攻撃への対策等）
   - 外的環境の把握体制（例：諸外国の法的環境の把握体制等）
2. 特定利用者情報の委託先の監督に係る体制及び方法に関する事項
   - 委託先の選定方法（例：自らが講ずべき安全管理措置と同等の措置が確実に実施されることの確認方法等）
   - 委託契約において記載する特定利用者情報の取扱いに関する事項（例：安全管理措置、秘密保持、再委託の条件、委託契約終了時の利用者情報の取扱い、契約内容が遵守されなかった場合の措置、その他の利用者情報の取扱いに関する事項等）
   - 委託先（再委託先、再々委託先等含む）における特定利用者情報の取扱状況の把握に関する体制及び方法（例：定期的監査、監査結果を踏まえた委託契約の見直し、再委託先における情報の取扱状況の把握方法等）
3. 情報取扱方針の策定及び公表に係る体制に関する事項（例：方針の策定組織等）
4. 特定利用者情報の取扱状況の評価に係る体制及び方法に関する事項
   - 評価実施体制及び評価結果の反映体制
   - 評価事項、評価頻度及び評価方法
5. 従業者の監督に係る体制及び方法に関する事項（例：アクセス管理の体制、教育研修等の内容・頻度等）

- なお、グローバル企業において、日本の利用者情報に限定した情報取扱規程を策定することが困難な場合も想定され、上記が含まれる前提で企業集団全体で情報取扱規程の策定を行うことも問題ないのではないか。

（安全管理措置）
第十二条 **電気通信事業者は、その取り扱う個人データ又は通信の秘密に係る個人情報**（以下「個人データ等」という。）の漏えい、滅失又は毀損の防止その他の個人データ等の**安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講じなければならない。**

■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解説（令和4年3月31日版）
7　講ずべき安全管理措置の内容
7-2 個人データ等の取扱いに係る規律等の整備
電気通信事業者は、その取り扱う個人データ等の漏えい等の防止その他の個人データ等の安全管理のために、個人データ等の具体的な取扱いに係る規律を整備しなければならない。

講じなければならない措置	手法の例示
○個人データ等の取扱いに係る規律の整備	取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データ等の取扱規程を策定することが考えられる。なお、具体的に定める事項については、以降に記述する**組織的安全管理措置**、**人的安全管理措置**及び**物理的安全管理措置**の内容並びに情報システム（パソコン等の機器を含む。）を使用して個人データ等を取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）は**技術的安全管理措置の内容を織り込むことが重要**である

7-7 **外的環境の把握**
電気通信事業者が、外国において個人データを取り扱う場合、**当該外国の個人情報の保護に関する制度等を把握した上**で、個人データの安全管理のために必要かつ適切な措置を講じなければならない。

（従業者及び委託先の監督）
第十三条 電気通信事業者は、その従業者（派遣労働者を含む。以下同じ。）に個人データ等を取り扱わせるに当たっては、当該個人データ等の安全管理が図られるよう、当該**従業者に対する必要かつ適切な監督**を行わなければならない。
2 電気通信事業者は、安全管理措置の実施その他の個人データ等の適正な取扱いの確保のため、その従業者に対し、必要な教育研修を実施するよう努めなければならない。
3 電気通信事業者は、個人データ等の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データ等の安全管理が図られるよう、**委託を受けた者に対する必要かつ適切な監督**を行わなければならない。

■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解説（令和4年3月31日版）

3-4-6　委託先の監督（第 13 条第 3 項関係）

電気通信事業者は、個人データ等の取扱いの全部又は一部を委託する場合は、委託を受けた者（以下「委託先」という。）において当該個人データ等について安全管理措置が適切に講ぜられるよう、委託先に対し必要かつ適切な監督をしなければならない。**具体的には、電気通信事業者は、第 12 条に基づき自らが講ずべき安全管理措置と同等の措置が講ぜられるよう、監督を行うものとする**（※2）。

その際、(中略)委託する事業の規模及び性質、個人データ等の取扱状況（取り扱う個人データ等の性質及び量を含む。）等に起因するリスクに応じて、**次の（1）から（3）までに掲げる必要かつ適切な措置を講じなければならない**（※3）。なお、通信の秘密に係る個人情報については、通信当事者の同意又は違法性阻却事由がなければ提供してはならないことに留意する必要がある（3-7-4（第三者に該当しない場合）参照）

（1）適切な委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第 23 条及び本ガイドラインで委託元に求められるものと同等であることを確認するため、「7（別添）講ずべき安全管理措置の内容」に定める各項目が、委託する業務内容に沿って、**確実に実施されることについて、委託先の体制や規程等の確認に加え、必要に応じて個人データ等を取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行う等により、あらかじめ確認しなければならない。**（略）

（2）委託契約の締結

委託契約には、安全管理措置（委託先において個人データ等を取り扱う者（委託先の作業者以外の者を含む。）を明確にすること、委託先において講ずべき安全管理措置の内容等）、**秘密保持、再委託の条件**（再委託を許すかどうか並びに再委託先を許す場合は再委託先に個人データ等を適正に取り扱っていると認められる者を選定すること、再委託を行うに当たっての電気通信事業者への文書による事前報告又は承認及び再委託先の監督に関する事項等。なお、二段階以上の委託を許す場合は同様に再々委託先等の選定、監督に関する事項等を定める必要がある。）、**委託契約終了時の個人データ等の取扱い**（個人データ等の返却、消去等）、**契約内容が遵守されなかった場合の措置**（例えば、安全管理に関する事項が遵守されずに個人データ等が漏えいした場合の損害賠償に関する事項、安全管理措置の不備が発見された場合の解約等）**その他の個人データ等の取扱いに関する事項を適正に定めることが適当である。**（略）

（3）委託先における個人データ等取扱状況の把握

委託先における委託された個人データ等の取扱状況を把握するためには、**定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価する**ことが望ましい。また、**委託先が再委託を行おうとする場合は、委託を行う場合と同様**、委託元は、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データ等の取扱方法等について、委託先から事前報告を受け、又は承認を行うこと、及び委託先を通じて、又は必要に応じて自らが、定期的に監査を実施すること等により、**委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が第 12 条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様である。**

（参考）規程に係る諸外国の事例

ドイツ 電気通信事業者法

✓ 公共の電気通信ネットワークを運営する、または一般にアクセス可能な電気通信サービスを提供する者は、**以下の事項を含めたセキュリティコンセプトを作成しなければならない。**（第166条(1)3.）

(a) **どのような電気通信サービスを提供しているのか**
(b) **予想されるリスク**
(c) **セキュリティ要件カタログに具体化されている義務を果たすために講じられた又は予定されている技術的防護措置またはその他の保護措置**

✓ **セキュリティコンセプトは連邦ネットワーク庁に届出なければならない。**

● 独セキュリティ要件カタログ
セキュリティ要件として以下の項目について規定。

3.1 組織
3.1.1 組織的リスクマネジメント
3.1.2 役割と責任
3.1.3 サプライヤーマネジメント
3.2 人的マネジメントにおけるセキュリティ
3.2.1 セキュリティチェック
3.2.2 専門性と知識
3.2.3 人事異動
3.2.4 規則違反への対応
3.3 データ、システム及び施設のセキュリティ
3.3.1 機微データと情報の安全な取扱い
3.3.2 物理的防御要件
3.3.3 サプライのセキュリティ（全体システムの可用性）
3.3.4 ネットワークと情報システムへのアクセスコントロール
3.3.5 ネットワークと情報システムの完全性と可用性
3.3.6 コミュニケーションの機密性
3.4 マネジメント
3.4.1 運用手順
3.4.2 マネジメントの変更
3.4.3 アセットマネジメント
3.5 セキュリティインシデント
3.5.1 セキュリティインシデントの検知
3.5.2 セキュリティインシデントへの対応
3.5.3 セキュリティインシデントの報告
3.6 緊急対応
3.6.1 通信インフラとサービスの継続性（事業継続マネジメント）
3.6.2 復旧（災害復旧マネジメント）
3.7 監視とテストの手続き
3.7.1 監視とログ取得の手続き
3.7.2 緊急訓練
3.7.3 ネットワークとITシステムのテスト
3.8 セキュリティ手法の評価
3.9 法律事項のコンプライアンス

イギリス 電子コミュニケーション(セキュリティ対策）規制案

✓ ネットワーク提供者又はサービス提供者は、提供者を代表して措置を執る責任が与えられた、適切なマネジメント者を確保しなければならない。（第9条）
✓ 特に以下の義務を含む。
● 様々な深刻レベルのセキュリティインシデントへの対応手順等、**セキュリティ侵害のリスクに関するビジネス手順を確立**し、定期的に見直さなければならない。
● ビジネス手順は、インシデント報告の際も含めた、明確に確立された役割及び責任、コミュニケーション及び高まるリスクと課題に対応するためのチャネルを準備しなければならない。

（参考）JIS Q 15001:2017

附属書A.3.3.5 内部規程
組織は，**次の事項を含む内部規程を文書化し，かつ，維持しなければならない。**
a) **個人情報を特定する手順**に関する規定
b) 法令，国が定める指針その他の規範の特定，参照及び維持に関する規定
c) 個人情報保護**リスクアセスメント**及び個人情報保護**リスク対応の手順**に関する規定
d) 組織の各部門及び階層における個人情報を保護するための**権限及び責任**に関する規定
e) **緊急事態への準備及び対応**に関する規定
f) 個人情報の**取得，利用及び提供**に関する規定
g) 個人情報の**適正管理(※)** に関する規定
h) 本人からの**開示等の請求等への対応**に関する規定
i) **教育**などに関する規定
j) **文書化した情報の管理**に関する規定
k) **苦情及び相談への対応**に関する規定
l) **点検**に関する規定
m)**是正処置**に関する規定
n) **マネジメントレビュー**に関する規定
o) **内部規程の違反に関する罰則**の規定

組織は，事業の内容に応じて，個人情報保護マネジメントシステムが確実に適用されるように**内部規程を改正しなければならない。**

（※）2022年改正案においては、適正管理の内容として、データ内容の正確性の確保等，安全管理措置，従業員の監督，委託先の監督が規定されている。

情報取扱方針の詳細①（新法第27条の８関係）

検討事項⑦

- **情報取扱方針の記載事項**（法律では①取得する特定利用者情報の内容、②特定利用者情報の利用の目的及び方法、③特定利用者情報の安全管理の方法、④利用者からの苦情等に応ずる営業所の連絡先、⑤その他総務省令で定める事項を規定）**や記載方法等の詳細について、検討が必要。**

検討の視点

- 「電気通信事業ガバナンス検討会報告書（令和４年２月）」では、安全管理の方法として、利用者情報を保管する電気通信設備の所在国や当該情報を取り扱う業務を委託した第三者の所在国を公表すること等が考えられるとされている。
- 「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」第15条では、取得される情報の項目、取得方法、利用目的の特定・明示、第三者提供の有無、委託に係る事項等を定めるべき事項としてプライバシーポリシーを定め、公表することが適切であるとされている。
- 他国法令では、例えば、EUのGDPRにおいては、情報が直接データ主体から取得される場合、及び情報がデータ主体以外から取得される場合の双方において、管理者の連絡先、取扱目的、関連する個人データの種類、第３国への移転の詳細、保管期間等について、利用者への情報提供が規定されている（第13条、第14条）。
- また、衆議院及び参議院における本法案に対する附帯決議として、「**特定利用者情報の取扱方針に係る総務省令を定めるに当たっては、利用者保護の重要性を十分に踏まえ、特定利用者情報を保管するサーバーの所在国や特定利用者情報を取り扱う業務を委託した第三者の所在国を公表することを定めること**」とされている。
- 国際標準であるISO/IEC 27017 でも、クラウドサービスプロバイダの組織の地理的所在地，及びクラウドサービスカスタマデータを保存する可能性のある国をクラウドサービスカスタマに通知することが推奨されている。
- 日本産業規格の一つであるJIS Q 15001では、個人情報保護方針において、安全管理、苦情等の対応に関すること等が記載事項として規定されている（附属書A.3.2.2）。

情報取扱方針の詳細②（新法第27条の８関係）

ご議論頂きたい事項

- 公表する情報が多くなるほど、利用者にとってわかりにくくなりかねないという事情も考慮し、利用者が安心で信頼できる電気通信サービスを確保する観点から、必要最低限の事項として、**ホームページにおいて**、利用者が理解しやすい**わかりやすい記載**により、例えば、以下を記載した情報取扱方針を策定頂くことが考えられるのではないか。
  （なお、既にプライバシーポリシーを定めている場合は、既存のものに必要事項を付け加えることで問題ないのではないか。）

1. 取得する特定利用者情報の内容に関する事項
   - 直接取得する特定利用者情報の項目
   - 特定利用者情報の取得方法
2. 特定利用者情報の利用の目的及び方法に関する事項（※）
   - 特定利用者情報の利用目的（具体的利用例含む）
3. 特定利用者情報の安全管理の方法に関する事項（※）
   - 安全管理措置の概要
   - 外国に所在する第三者に特定利用者情報の取扱いを委託する場合、委託先（再委託先を含む）の所在国の名称
   - 外国に所在するサーバに特定利用者情報を保存する場合、サーバの所在国の名称（保存する可能性がある国の名称を含む）
4. 利用者からの相談等に応ずる営業所等の連絡先（※）

（※）個人情報保護法第32条第1項においては、保有個人データの利用目的、保有個人データの安全管理のために講じた措置、保有個人データの取扱いに関する苦情の申出先等を本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む）に置かなければならないとされている。

- その他考慮すべき事項はあるか。

第15条（第1項、第2項）
1　電気通信事業者は、プライバシーポリシー（当該電気通信事業者が個人データ等の適切な取扱いを確保する上での考え方や方針をいう。）を定め、公表することが適切である。
2　前項に定めるプライバシーポリシーにおいて、次に掲げる事項について定め、利用者にとって分かりやすく示すことが適切である。
(1)　電気通信事業者の氏名又は名称
(2)　取得される情報の項目
(3)　取得方法
(4)　利用目的の特定・明示
(5)　通知・公表又は同意取得の方法及び利用者関与の方法
(6)　第三者提供の有無
(7)　問合せ窓口・苦情の申出先
(8)　プライバシーポリシーの変更を行う場合の手続
(9)　利用者の選択の機会の内容、データポータビリティに係る事項
(10)　委託に係る事項

■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解説（令和4年3月31日版）

3-5-1　プライバシーポリシーの策定・公表（第 15 条第 1 項、第 2 項関係）
電気通信事業者の個人データ等の適切な取扱いについての社会的信頼を確保するため、電気通信事業者は自らの個人データ等の適切な取扱いを確保する上での考え方や方針についての宣言をプライバシーポリシーとして定め、公表することが適切である。

【プライバシーポリシーに示すことが適切である項目】
プライバシーポリシーは、それぞれの電気通信事業者が、当該電気通信事業者の利用者において、当該電気通信事業者による個人データ等の取扱いを理解できるように、分かりやすい表現で記載すべきものであるが、プライバシーポリシーに記載すべき事項としては、次のようなものが考えられる。
① 法及び通信の秘密に係る電気通信事業法の規定その他の関係法令の遵守
② 本ガイドラインの遵守
③ 第15条に定める事項
（ⅰ）電気通信事業者の氏名又は名称
（ⅱ）取得される情報の項目
（ⅲ）取得方法
（ⅳ）利用目的の特定・明示
（ⅴ）通知・公表又は同意取得の方法及び利用者関与の方法
　利用目的の通知又は開示若しくは訂正等の本人からの請求に応じる手続
（ⅵ）第三者提供の有無
（ⅶ）問合せ窓口・苦情の申出先
　認定個人情報保護団体の名称及び苦情の解決の申出先を含む。

（viii）プライバシーポリシーの変更を行う場合の手続
（ix）利用者の選択の機会の内容（※）、データポータビリティに係る事項
（x）委託に関する事項
委託の有無、委託する事務の内容を明らかにするなど、委託処理の透明化を進めること。
④ 第12条の安全管理措置に関する方針
⑤ その他利用者の権利利益の保護に関する事項
（ⅰ）保有個人データについて本人から求めがあった場合には、ダイレクトメールの発送停止など、自主的に利用停止等に応じること
（ⅱ）電気通信事業者がその事業内容を勘案して利用者の種類ごとに利用目的を限定して示したり、電気通信事業者が本人の選択による利用目的の限定に自主的に取り組むなど、本人にとって利用目的がより明確になるようにすること
（ⅲ）個人情報の取得方法（取得元の種類等）を、可能な限り具体的に明記すること

（※）(ア)電気通信事業者が（任意の取組として）利用者の求めに応じて自主的に個人データ等の取得・利用を停止しているか（利用者はこれを求めることができるか）、(イ)利用者において個人データ等の取得・利用の停止を求めることができる場合には、利用者がこれを求める方法、及び、利用者がこれを求めた場合にも電気通信サービスが利用可能か等

なお、取得に際しての利用目的（第9条第1項、第3項）、オプトアウトによる個人データの第三者提供を行う場合の個人データの項目等（第17条第2項、第3項、第9項）、共同利用における共同利用される個人データの項目等（第17条第10項第3号、第11項）、匿名加工情報に含まれる情報の項目等（第33条第3項、第4項、第5項、第7項、第34条）、保有個人データに関する公表すべき事項（第19条第1項）、匿名加工情報取扱事業者における匿名加工情報の安全管理措置等（第36条）については、通知し、又はプライバシーポリシー等において公表し若しくは本人が容易に知り得る状態に置かなければならないことに留意する必要がある。
以下、略

（参考）EU GDPR第13条・14条に基づきデータ主体に提供しなければならない情報の概要

必要となる情報の種類	情報が直接データ主体から取得される場合（第13条）	情報がデータ主体以外から取得される場合（第14条）	補足 （情報に関する要件に関する旧第29条作業部会※のコメント概要） ※独立の諮問機関で、加盟国のデータ保護監督機関の代表者、欧州委員会の代表者などから構成され、個人データ保護についてEUの執行機関である欧州委員会に対して意見を提供する役割を負う
管理者の身元及び連絡先	法第13条1(a)項	法第14条1(a)項	この情報により、管理者の容易な識別が可能になるはずであり、また望ましくは、データ管理者とのさまざまな方法での通知（例えば電話番号、電子メールアドレス、郵送先など）が可能になる。
データ保護オフィサーの連絡情報	法第13条1(b)項	法第14条1(b)項	（略）
取扱目的及び法的根拠	法第13条1(c)項	法第14条1(c)項	特別な種類の個人データの場合、関連規定（及び関連する場合には、データの取扱いを規律するEU法又は加盟国の適用法）を明記するべきである。
正当な利益が取扱いの法的根拠とされている場合には、当該正当な利益	法第13条1(d)項	法第14条1(d)項	慣行の観点から、管理者は、バランシングテストから得た情報をデータ主体に提供してもよいが、それは取扱いの合法的な根拠として、データ主体の個人データを収集する前に実施しなければならない。いずれにせよ、請求すればバランシングテストに関する情報を取得できることをデータ主体に提供する情報に明示すべき。
関連する個人データの種類	非該当	法第14条1(d)項	第14条の場合では、**個人データをデータ主体から取得しておらず、データ管理者がどの種類の個人データを取得しているかについてデータ主体が意識していないため、この情報が必要である。**
個人データの受領者	法第13条1(e)項	法第14条1(e)項	**データの移転又は開示を受ける他のデータ管理者、共同管理者及び処理者は「取得者」という用語の範囲に含まれ、そのような取得者に関する情報が提供されるべきである。**個人データの実際の取得者又は取得者の種類を提示しなければならない。
第三国への移転の詳細、関連する保護措置の詳細等	法第13条1(f)項	法第14条1(f)項	移転及び対応する仕組みを可能にするGDPRの関連条文（例えば、第45条に基づく十分性決定／第47条に基づく拘束的企業準則／第46条(2)に基づく標準的なデータ保護条項／第49条に基づく例外及び保護措置等）を明示すべきである。
保存期間	法第13条2(a)項	法第14条2(a)項	データ主体が、それぞれのデータ／目的に応じ、自分の状況に基づいて適切な保存期間を評価できるような方法で表現するべき。個人データの種類及び又はそれぞれの取扱いの目的に応じた異なる保存期間を定めるべきである。
データ主体の権利	法第13条2(b)項	法第14条2(c)項	特に、**取扱いに異議を述べる権利は、データ主体にはっきりとした形で知らされなければならない。**
処理が同意に基づく場合、同意を撤回する権利	法第13条2(c)項	法第14条2(d)項	この情報には同意を撤回する方法を含めるべきであり、データ主体にとって同意を撤回することが同意するのと同程度に容易なものとなるよう配慮する。
監督機関に異議を申し立てる権利	法第13条2(d)項	法第14条2(d)項	特に職場、又は問題とされる違反の発生場所の加盟国の監督機関に不服申立てを行う権利がデータ主体にあることを説明するべき。
個人データ提供のための法制上もしくは契約上の要件等	法第13条2(e)項	非該当	例えばオンラインフォームでは、どのフィールドが「必須」であり、また必須ではないか、及び必須フィールドに入力しなかった場合の結果を明示すべきである。
個人データの発信元、公開されている情報からのものか否か等	非該当	法第14条2(f)項	データの情報源を明示することが不可能でない限り、明示するべき。情報源を明記しない場合には、情報源の性質（公的／私的に保有されている情報源）及び組織／業界／産業部門のタイプ）を含めるべき。

（参考）JIS Q 15001･ISO/IEC

● JIS Q 15001　附属書A.3.2.2 外部向け個人情報保護方針

トップマネジメントは，外部向け個人情報保護方針を文書化した情報には，A.3.2.1に規定する内部向け個人情報保護方針の事項に加え，**次の事項も明記しなければならない**。

a) 制定年月日及び最終改正年月日

b) 内部向け個人情報保護方針の内容についての問合せ先

トップマネジメントは，外部向け個人情報保護方針を文書化した情報について，一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない。

・ 附属書A.3.2.1 内部向け個人情報保護方針

トップマネジメントは，5.2.1 e)に規定する内部向け個人情報保護方針を文書化した情報には**次の事項を含めなければならない**。

a) 事業の内容及び規模を考慮した適切な個人情報の取得，利用及び提供に関すること[特定された利用目的の達成に必要な範囲を超えた個人情報の取扱いを行わないこと及びそのための措置を講じることを含む。]。

b) 個人情報の取扱いに関する法令，国が定める指針その他の規範を遵守すること。

c) 個人情報の漏えい，滅失又はき損の防止及び是正に関すること。

d) 苦情及び相談への対応に関すること。

e) 個人情報保護マネジメントシステムの適用範囲及び継続的改善に関すること。

f) トップマネジメントの氏名

● ISO/IEC 29100 4.6 プライバシーポリシー

外部プライバシーポリシーによって，組織のプライバシー慣行，並びに，PII（※１）管理者の識別要素（※）及び公式な住所，PII主体が追加の情報を取得することができる連絡先などの他の関連する情報を，組織に属さない者へ公表又は通知する。

（※１）情報通信技術システムにおける個人識別可能情報

（※２）PII管理者の氏名，職名などを指す。

● ISO/IEC 27017 6.1.3 関係当局との連絡

クラウドサービスプロバイダは，クラウドサービスカスタマに，クラウドサービスプロバイダの組織の地理的所在地，及び**クラウドサービスプロバイダが，**クラウドサービスカスタマに**データを保存する可能性のある国を通知することが望ましい**。

特定利用者情報の取扱状況の評価の詳細（新法第27条の９関係）

検討事項⑧

- 毎事業年度実施が求められている特定利用者情報の**取扱状況に関する評価の詳細について、検討が必要。**

検討の視点

- 「電気通信事業ガバナンス検討会報告書（令和４年２月）」では、評価の観点として、外国の法制度が適正な取扱いに与える影響等の観点について含むことが考えられる旨示されている。
- 他国法令では、例えば、EUのGDPRにおいては、データ主体に及ぼすリスク等のデータ保護影響評価（第35条）を行うこととされている。また、英国の電子コミュニケーション（セキュリティ対策）規制案では、年に１度、ネットワーク等がさらされる可能性があるリスク、サプライチェーンリスク、セキュリティ侵害のリスクに関連する変化、サービスの提供等に関与する者によるリスク等を考慮して、セキュリティ侵害のリスクに関する評価を書面で行うこととされている。

ご議論頂きたい事項

- 特定利用者情報の取扱状況に関する評価については、以下の事項・観点が考えられるのではないか。

1. 前事業年度における情報取扱規程及び情報取扱方針の遵守状況
2. 前事業年度における、社会情勢、技術革新、外国の法的環境の変化、サイバー攻撃のリスク、その他の**外部環境の変化による影響**
3. 前事業年度における、事故その他の**内部環境の変化による影響**

- なお、グローバル企業において、日本の利用者情報に限定した評価の実施の困難さも想定され、企業集団全体で評価を行うことも問題ないのではないか。

（参考）評価に係る諸外国の事例

EU 一般データ保護規則(GDPR) 	✓ **データ保護影響評価は、少なくとも以下の事項を含める**ものとする。(第35条) (a) 予定されている取扱業務及び取扱いの目的の体系的な記述（管理者の求める正当な利益を含む） (b) その目的に関する取扱業務の必要性及び比例性の評価 (c) 第１項で定める**データ主体の権利及び自由に対するリスクの評価** (d) データ主体及び他の関係者の権利及び正当な利益を考慮に入れた上で、個人データの保護を確保するための、及び、本規則の遵守を立証するための、保護措置、安全管理措置及び仕組みを含め、**リスクに対処するために予定されている手段**
イギリス 電子ｺﾐｭﾆｹｰｼｮﾝ(ｾｷｭﾘﾃｨ対策)規制案 	✓ 少なくとも12ヶ月に１度のセキュリティ侵害のリスクを見直し、**以下を考慮に入れて、セキュリティ侵害の全体のリスクの程度に関する書面による評価を行う。**（第９条） （ｉ）ネットワーク提供者の場合、機微なデータを含んでいるか、セキュリティの重要な機能か等を考慮し、特定された**ネットワーク全体及び個々の機能又はネットワークがさらされる可能性のあるリスク** （ii）**サプライチェーンに起因するセキュリティ侵害のリスク**に基づき特定されたリスク （iii）**セキュリティ侵害のリスクに関連する変化を考慮した上でのセキュリティ措置**の定期的なレビュー結果 （iv）公共の電子コミュニケーションネットワーク又は公共の電子コミュニケーションサービスの**提供に関与する者による不正な行いに起因するセキュリティ侵害のリスク**で特定されたリスク （ｖ）その他の関係情報
ドイツ 電気通信事業者法等 	✓ **連邦ネットワーク庁**は、セキュリティコンセプトの実施状況を**定期的に監査しなければならない。**監査は少なくとも2年ごとに実施しなければならない。（第166条） ■ 独セキュリティ要件カタログ　※自己で行うことが求められているもの。 ✓ セキュリティ手法は定期的に再評価されなければならない。（3.8 セキュリティ対策の評価） ✓ 特定の数値（誤動作の回数、ダウンタイムなど）による定期的なリスク分析及び調査はセキュリティ手法の評価に活用し得る。 ✓ 定期的かつ現実的なストレステストは、新たなリスク要因を潜在的に特定し得る。

特定利用者情報統括管理者の要件（新法第27条の10関係）

検討事項⑨

- 特定利用者情報の取扱い責任者である**特定利用者情報統括管理者**（管理的地位にあり、かつ、利用者に関する情報の取扱い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を備える者）**の要件について、検討が必要。**

検討の視点

- 電気通信設備統括管理者については、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を備える者（**電気通信設備の設計、工事、維持又は運用に関する業務やこれを監督する業務に通算して３年以上従事した経験を有すること又は同等以上の能力を有すると認められること**）とされている。
- 「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」第14条においては、個人データ等（個人データ又は通信の秘密に係る個人情報）の取扱いに関する責任者として個人情報保護管理者を設置し、内部規程の策定、監査体制の整備、個人データ等の取扱いの監督を行わせるよう努めなければならない、とされている。
- 他国法令では、（具体的な職務経験の年数等に言及はないものの、）例えば、英国の電子コミュニケーション（セキュリティ対策）規制案では、セキュリティ管理の責任を取締役会(board)レベルの者に付与し、要件として**情報システムのセキュリティの適切な知識・技能を有すること**等とされている（第9,10条）。
- 国際的なｾｷｭﾘﾃｨ関連の資格（CISSP、CCSP、CISM）では、試験の合格に加え５年以上の業務経験が必要とされている。

ご議論頂きたい事項

- 特定利用者情報の取扱い責任者である特定利用者情報統括管理者の要件としては、事業運営上の重要な決定に参画する管理的地位にあることに加え、以下を要件とすることが考えられるのではないか。（なお、CIO、CISO、個人情報保護管理者等を設置している場合は、必要となる任務を追加して対応することも問題ないのではないか。）

✓ 利用者に関する情報の取扱いに関する**安全管理**又は**法令等に関する業務**、若しくは**これらの業務を監督する業務に一定期間従事した経験（他業種含む。）**を有すること又は**同等以上の能力**を有すると認められること。

第14条
電気通信事業者は、個人情報保護管理者（当該電気通信事業者の個人データ等の取扱いに関する責任者をいう。）を置き、本ガイドラインを遵守するための内部規程の策定、監査体制の整備及び当該電気通信事業者の個人データ等の取扱いの監督を行わせるよう努めなければならない。

■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解説（令和4年3月31日版）

3-4-7　個人情報保護管理者（第 14条関係）

個人データ等保護措置の実施に関する責任の所在を明確にし、第12条の安全管理措置の実施その他の個人データ等の適正な取扱いについて電気通信事業者の内部における責任体制を確保するため、電気通信事業者は、当該電気通信事業者の個人データ等の適正な取扱いの確保について必要な権限を有する役員などの組織横断的に監督することのできる者（個人情報保護管理者）を置いて、個人情報保護管理者において責任をもって必要な個人データ等の取扱いの監督等を行わせるよう努めなければならない。

なお、個人情報保護管理者の設置は、特に、電気通信事業者の内部又は外部からの不正行為による個人データ等の漏えい等を防止するため、また責任の所在を明確化する上でも重要であり、個人情報保護管理者の設置を通じて、あらかじめ個人データ等の漏えい等を防止するための体制を整備し、また、漏えい等事案の発生時に、被害拡大防止措置の実施及び監督官庁等への報告等の対応を行うための体制を整備することが望ましい。

また、個人情報保護管理者は、内部規程の策定や監査体制の整備に当たっては、「7（別添）講ずべき安全管理措置の内容」に規定された措置を盛り込むことが望ましい。この際、監査体制の整備の一環として、委託先の監査を含む監査体制を整備し監査結果を踏まえた個人データ等の取扱方法に関する見直し・改善を行うことが望ましい。

なお、電気通信事業者の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られる場合における総務大臣による電気通信事業法第29条第1項第１号の規定に基づく業務の改善命令の発動に係る指針として「通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針」（https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000111.html）が定められている。

（参考）責任者の要件等に係る諸外国の事例

EU 一般データ保護規則(GDPR) 	✓ データ保護オフィサーは、**専門家としての資質、及び、特に、データ保護の法令及び実務に関する専門知識並びに次の職務を充足するための能力に基づいて指定**される。管理者又は処理者は、データ保護オフィサーの連絡先の詳細を公表し、かつ、監督機関に対し、それを連絡しなければならない。（第37条） a. 管理者又は処理者及び取扱いを行う従業者に対し、本規則及びそれ以外のEU 若しくは加盟国のデータ保護条項による義務を通知し、かつ、助言すること； b. 取扱業務に関与する職員の責任の割当て、意識向上及び訓練、並びに、関連する監査を含め、本規則の遵守、それ以外のEU 又は加盟国の個人データ保護条項遵守、並びに、個人データ保護と関連する管理者又は処理者の保護方針の遵守を監視すること； c. 要請があった場合、第35 条によるデータ保護影響評価に関して助言を提供し、その遂行を監視すること； d. 監督機関と協力すること； e. 取扱いと関連する問題に関し、監督機関の連絡先として行動すること。第36条に規定する事前協議、適切な場合、それ以外の関連事項について協議することを含む。
イギリス 電子ｺﾐｭﾆｹｰｼｮﾝ(ｾｷｭﾘﾃｨ対策)規制案 	✓ ネットワーク提供者又はサービス提供者は、**提供者を代表して措置を執る責任が与えられた者**（以下「責任者」という。）及びセキュリティの重要な機能の運用をサポートする者が、責任を果たし、セキュリティの重要な機能の運用をサポートするに足る能力を有すること、及び職務の遂行にあたり適切な権限及びリソースが与えられていることを確保しなければならない。また特に以下の義務を含まなければならない。（第10条） (a) セキュリティ上重要な機能の運用を支えるネットワーク及び情報システムのセキュリティに関し、組織上の役割を効率的に果たすことができる適切な知識・技能を有すること。 (b) セキュリティの重要な機能の運用をサポートする者は、セキュリティ措置に関し適切に訓練をされていること。 (c) 責任者について、**モニタリング及び監査の義務を果たすことができる能力を有し**、そのために適切なリソースを与えられていること。
ドイツ 電気通信事業者法等 	✓ 公共の電気通信ネットワークを運営する、または一般にアクセス可能な電気通信サービスを提供する者は、セキュリティ管理者を指名しなければならない。（第166条） ■ 独セキュリティ要件カタログ ✓ セキュリティ管理者は一定の調整、管理、専門家としての権限が与えられなければならない。セキュリティ管理者等は連邦ネットワーク庁のコンタクトパーソンでなければならない。（５．１．８ セキュリティ管理者の指名）

（参考）年数要件の事例

【情報セキュリティに関する国際的な資格】

■CISSP（Certified Information Systems Security Professional))

認定のためには、試験合格に加えて**５年以上**の関連する業務経験があることが要件とされている。

■CCSP(Certified Cloud Security Professional)

認定のためには、試験合格に加えて**５年以上**の関連する業務経験があることが要件とされている。

■公認情報セキュリティマネージャー（CISM）（Certified Information Security Manager）

認定のためには、試験合格に加えて、**５年以上**の関連する業務経験があることが要件とされている。

【安全統括管理者の年数要件】

<table>
<tr><th></th><th>貨物自動車運送事業法</th><th>鉄道事業法</th><th>海上運送法</th><th>内航海運業法</th><th>航空法</th></tr>
<tr><td>業務</td><td colspan="5">・輸送の安全を確保するための事業の運営の方針に関する事項
・輸送の安全を確保するための事業の実施及びその管理の体制に関する事項
・輸送の安全を確保するための事業の実施及びその管理の方法に関する事項
に掲げる事項に関する業務を統括管理</td></tr>
<tr><td>要件（地位）</td><td colspan="5">事業運営上の重要な決定に参画する管理的地位にあること。</td></tr>
<tr><td rowspan="2">要件（実務経験）
【省令】</td><td>①事業用自動車の運行の安全の確保に関する業務、②点検及び整備の管理に関する業務、③その他の輸送の安全の確保に関する業務に<u>通算三年以上</u></td><td>鉄道事業の安全に関する業務の経験の期間が<u>通算して十年以上</u></td><td>一般旅客定期航路事業の安全に関する業務の経験の期間が<u>通算して三年以上</u></td><td>内航海運業の安全に関する業務の経験の期間が<u>通算して三年以上</u></td><td>航空運送事業の実施又は管理の総括に関する業務の経験が<u>通算して三年以上</u></td></tr>
<tr><td colspan="5">上記と同等以上の能力と認める者</td></tr>
</table>

事故報告の対象となる特定利用者情報の詳細（新法第28条関係）

検討事項⑩

- 特定利用者情報のうち、①通信の秘密、②通信の秘密以外の総務省令で定める情報の漏えい時には、総務大臣に報告が必要となるが、当該②**通信の秘密以外の情報の詳細について、検討が必要。**

検討の視点

- **個人情報保護法は、一定の個人データの漏えい等事案について報告義務を課している。**電気通信業については漏えい等報告の受領権限が総務大臣に委任されており、**電気通信業において個人データの漏えい等事案が生じた場合には、総務省宛てに漏えい等報告がされる。**
- **個人情報保護法施行規則（第７条）は、以下の事態について、報告義務の対象と定めている。**
  一　要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第一項において同じ。）の漏えい、滅失若しくは毀損（以下この条及び次条第一項において「漏えい等」という。）が発生し、又は発生したおそれがある事態
  二　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
  三　不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
  四　**個人データに係る本人の数が千人を超える漏えい等が発生**し、又は発生したおそれがある事態

ご議論頂きたい事項

- 特定利用者情報のうち、通信の秘密以外の情報については、以下の場合に報告を求めることが考えられるのではないか。

✓ データベース等を構成する利用者の数が**千人を超える**特定利用者情報の漏えいが発生した場合

- なお、当該特定利用者情報の漏えい報告と、個人情報保護法に基づく個人データの漏えい報告の双方に該当する事態の場合、**双方の法に基づく報告を一の報告書で行う**ことも可能とすべきではないか。

参考資料
（参考条文）

（参考）ドイツ電気通信事業者法（仮訳）

第166条　セキュリティ管理者及びセキュリティコンセプト

（１）３．公共の電気通信ネットワークを運営する、または一般にアクセス可能な電気通信サービスを提供する者は**以下の事項を含めたセキュリティコンセプトを作成しなければならない。**

(a) **どのようなサービスを提供しているのか**

(b) **予想されるリスク**

(c) 第165条（１）～（７）から第167条について**セキュリティ要件カタログに具体化されている義務を果たすために講じられた又は予定されている技術的防護措置またはその他の保護措置**（カタログにセキュリティ目標のみが指定されている場合は、それぞれのセキュリティ目標が講じられた対策で完全に達成されていることを示さなければならない。）

（2）公共の電気通信ネットワークを運営する者は、ネットワーク運用の開始直後に、**セキュリティコンセプトを連邦ネットワーク庁に届出しなければならない。**一般にアクセス可能な電気通信サービスを提供する者は、セキュリティコンセプトを提出するように連邦ネットワーク庁から求められることがある。

● 独セキュリティ要件カタログ

セキュリティ要件として以下の項目について規定。

3.1 組織
- 3.1.1 組織的リスクマネジメント
- 3.1.2 役割と責任
- 3.1.3 サプライヤーマネジメント

3.2 人的マネジメントにおけるセキュリティ
- 3.2.1 セキュリティチェック
- 3.2.2 専門性と知識
- 3.2.3 人事異動
- 3.2.4 規則違反への対応

3.3 データ、システム及び施設のセキュリティ
- 3.3.1 機微データと情報の安全な取扱い
- 3.3.2 物理的防御要件
- 3.3.3 サプライのセキュリティ（全体システムの可用性）
- 3.3.4 ネットワークと情報システムへのアクセスコントロール
- 3.3.5 ネットワークと情報システムの完全性と可用性
- 3.3.6 コミュニケーションの機密性

3.4 マネジメント
- 3.4.1 運用手順
- 3.4.2 マネジメントの変更
- 3.4.3 アセットマネジメント

3.5 セキュリティインシデント
- 3.5.1 セキュリティインシデントの検知
- 3.5.2 セキュリティインシデントへの対応
- 3.5.3 セキュリティインシデントの報告

3.6 緊急対応
- 3.6.1 通信インフラとサービスの継続性（事業継続マネジメント）
- 3.6.2 復旧（災害復旧マネジメント）

3.7 監視とテストの手続き
- 3.7.1 監視とログ取得の手続き
- 3.7.2 緊急訓練
- 3.7.3 ネットワークとITシステムのテスト

3.8 セキュリティ手法の評価

3.9 法律事項のコンプライアンス

（参考）ドイツ電気通信事業者法（仮訳）

第165条　技術的・組織的防御措置

(1) 電気通信サービスを提供する者、または電気通信サービスに参加する者は、以下のために適切な技術的予防措置およびその他の措置を講じなければならない。

1.電気通信の秘密を守るための措置

2.個人データの保護に対する違反を防止する措置

その際、最新の技術を考慮しなければならない。

(2)公共の電気通信ネットワークを運営する、または一般にアクセス可能な電気通信サービスを提供する者は、以下の目的のために運営される電気通信システムおよびデータ処理システムにおいて、技術的・組織的に適切な予防措置及びその他の措置を講じなければならない。

1.電気通信ネットワークおよびサービスの重大な障害につながる混乱を、外部からの攻撃や災害の影響によって引き起こされる場合も含めて、防止すること。

2.電気通信ネットワークおよびサービスのセキュリティに対するリスクを管理すること。

特に、電気通信およびデータ処理システムを不正アクセスから保護し、セキュリティ違反がユーザーや他の電気通信ネットワーク及びサービスに与える影響を最小限に抑えるために、適切な場合には暗号化などの措置を含む対策を講じなければならない。

これらの措置は、最新の技術を考慮したものでなければならない。

(3)　(2)に規定される適切な措置として、公共の電気通信ネットワークの運営者および一般にアクセス可能な電気通信サービスの提供者は、BSI法第2条(9b)に規定する攻撃検知のためのシステムを使用することができる。潜在的リスクが高い公共の電気通信ネットワークの運営者及びおよび一般に利用可能な電気通信サービスの提供者は、攻撃検知のための適切なシステムを使用しなければならない。使用する攻撃検知システムは、継続的かつ自動的な記録と評価により、危険または脅威を検知できなければならない。また、特定された危険または脅威を回避し、発生した混乱に対して適切な救済措置を提供する能力を有していなければならない。連邦ネットワーク庁は、第167条に基づくセキュリティ要件のカタログにおいて、さらなる詳細を規定することができる。

(4) BSI法第2条第13項に規定する重要部品は、最初に使用する前に公認の認証機関によってチェックされ、認証された場合に限り、潜在的リスクが高い公共の通信ネットワークの運営者が使用することができる。

(5) 公共の電気通信ネットワークの運営者は、そのネットワークの適切な運用を確保し、それにより当該ネットワーク上で提供されるサービスの継続的な可用性を確保するための措置を講じなければならない。

(6) 技術的予防措置およびその他の保護措置は、そのために必要とされる技術的および経済的努力が、保護されるべき電気通信ネットワークまたはサービスの重要性に不釣り合いでない場合には、適切とされる。連邦データ保護法第62条(1)が適宜適用される。

(7) 場所又は技術設備の共同利用の場合、特定の義務を特定の当事者に割り当てることができない限り、各当事者は、(1)から(5)までの義務を履行しなければならない。

(8)～(11)　略

（参考）ドイツ電気通信事業者法（仮訳）

第166条　セキュリティ管理者及びセキュリティコンセプト

（1）公共の電気通信ネットワークを運営する者、または一般にアクセス可能な電気通信サービスを提供する者は、以下を行う。

1.セキュリティ管理者の指名

2.欧州連合に拠点を置く連絡担当者の指定。

3.以下の事項を含むセキュリティコンセプトの策定

a）どの公共通信ネットワークが運営され、どの利用可能な電気通信サービスが提供されているか

b）予想される危険

c）第165条（１）～（７）から第167条についてセキュリティ要件カタログに具体化されている義務を果たすために講じられた又は予定されている技術的防御措置またはその他の保護措置（カタログにセキュリティ目標のみが指定されている場合は、それぞれのセキュリティ目標が講じられた対策で完全に達成されていることを示さなければならない。）

（2）公共の電気通信ネットワークを運営する者は、ネットワーク運用の開始直後に、セキュリティコンセプトを連邦ネットワーク庁に届出しなければならない。一般にアクセス可能な電気通信サービスを提供する者は、セキュリティコンセプトを提出するように連邦ネットワーク庁から求められることがある。

（3）セキュリティコンセプトとともに、セキュリティコンセプトに概説されている技術的防御措置およびその他の保護措置が実施されている、または直ちに実施されるという宣言を届出しなければならない。

（4）連邦ネットワーク庁は、セキュリティコンセプトまたはその実装にセキュリティ上の欠陥を発見した場合、これらの欠陥の即時の排除を要求することができる。セキュリティコンセプトの基礎となる状況が変化した場合、(2)に基づいて義務付けられた人は、変更の直後にセキュリティコンセプトを変更し、変更箇所がわかるように、変更後速やかに連邦ネットワーク庁に届出しなければならない。

(5) 連邦ネットワーク庁は、セキュリティコンセプトの実施状況を定期的に監査しなければならない。監査は少なくとも2年ごとに実施しなければならない。

第167条　セキュリティ要件カタログ

（1）連邦ネットワーク庁は、情報セキュリティ連邦局及びデータ保護および情報の自由に関する連邦委員会と合意の上で、電気通信およびデータ処理システムの運用及び個人情報の処理のためのセキュリティ要件のカタログにおいて、以下の事項について、具体化する。

1．公共電気通信ネットワークおよび一般にアクセス可能な電気通信サービスのさまざまなリスクの可能性を考慮した上での、第165条（1）から（7）に従って取られるべき技術的防御措置およびその他の措置の詳細

（略）

（参考）イギリス電子コミュニケーション（セキュリティ対策）規制案（仮訳）

9. ガバナンスと説明責任

(1)ネットワーク提供者又はサービス提供者は、法第105条Ａ（１）の目的を達成するため、
提供者を代表して措置を執る責任が与えられた、適切なマネジメント者を確保しなければならない。

(2) (1)の義務は、特に以下の義務を含む。

(d) 様々な深刻レベルのセキュリティインシデントへの対応手順等、
セキュリティ侵害のリスクに関するビジネス手順を確立し、定期的に見直す。

(e)ビジネス手順は、インシデント報告の際も含めた、**明確に確立された役割及び責任、コミュニケーション及び高まるリスクと課題に対応するためのチャネルを準備**しなければならない。

（参考）ISO/IEC27002

5.1.1 情報セキュリティのための方針群

情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知することが望ましい。

情報セキュリティ方針には，**次の事項に関する記載を含めることが望ましい**。

a) 情報セキュリティに関する全ての活動の指針となる，情報セキュリティの定義，目的及び原則
b) 情報セキュリティマネジメントに関する一般的な責任及び特定の責任の，定められた役割への割当て
c) 逸脱及び例外を取り扱うプロセス

方針群のより低いレベルでは，情報セキュリティ方針は，トピック固有の個別方針によって支持されることが望ましい。このトピック固有の個別方針は，情報セキュリティ管理策の実施を更に求めるもので，一般に組織内の対象となる特定のグループの要求に対処するように，又は特定のトピックを対象とするように構成されている。このような**個別方針のトピックの例**を，次に示す。

a) アクセス制御
b) 情報分類（及び取扱い）
c) 物理的及び環境的セキュリティ
d) 次のような，エンドユーザ関連のトピック
    1) 資産利用の許容範囲
    2) クリアデスク・クリアスクリーン
    3) 情報転送
    4) モバイル機器及びテレワーキング
    5) ソフトウェアのインストール及び使用の制限
e) バックアップ
f) 情報の転送
g) マルウェアからの保護
h) 技術的ぜい弱性の管理
i) 暗号による管理策
j) 通信のセキュリティ
k) プライバシー及び個人を特定できる情報の保護
l) 供給者関係

（参考）アメリカ国立標準技術研究所(NIST) SP800-53

3.12 計画　PL-2 システムセキュリティおよびプライバシー計画

a 以下のような**システムセキュリティおよびプライバシー計画を策定する**。

1 組織のエンタープライズアーキテクチャと整合している。
2 構成するシステムコンポーネントを明示的に定める。
3 システムの運用状況を、ミッションおよび事業プロセスの観点から記述する。
4 システムの役割と責任を果たす個人を特定する。
5 システムによって処理、保存、および伝送される情報タイプを特定する。
6 システムのセキュリティ分類化を、根拠を含めて、提供する。
7 組織が懸念するシステムに対する特定の脅威を記述する。
8 個人情報を取扱うシステムのプライバシーリスクアセスメントの所見を提供する。
9 システム、および他のシステムまたはシステムコンポーネントへの依存関係または接続に関するシステムの運用環境について記述する。
10 システムのセキュリティおよびプライバシー要件の概要を提供する。
11 該当する場合、関連する管理策ベースラインまたはオーバーレイを特定する。
12 セキュリティおよびプライバシーの要件を満たすために導入または計画されている管理策を、テーラリング判断の根拠を含め、記述する。
13 セキュリティおよびプライバシーのアーキテクチャおよび設計上の判断に関するリスクの決定を含める。
14 組織が定める個人またはグループとの計画策定および調整を必要とする、システムに影響を与えるセキュリティおよびプライバシー関連の措置を含める。
15 計画の実装前に、認可権限のある担当者または指定された代理人によってレビューされ、承認されている。

b 計画のコピーを配布し、計画に対するその後の変更を組織が定める職員または役割に通知する。

c 組織が定める頻度で計画をレビューする。

d システムおよび運用環境の変更、または計画の実装または管理策アセスメント中に特定された問題に対応するために計画を更新する。

e 計画を認可されていない開示や変更から保護する。

（参考）EU GDPR(13条：データ主体から情報が取得される場合)

出典： https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

第13 条 データ主体から個人データが取得される場合において提供される情報

1. データ主体と関連する個人データがそのデータ主体から収集される場合、管理者は、その個人データを取得する時点において、そのデータ主体に対し、**以下の全ての情報を提供**する：
(a) 管理者の身元及び連絡先、及び、該当する場合は、管理者の代理人の身元及び連絡先。
(b) 該当する場合は、データ保護オフィサーの連絡先。
(c) 予定されている個人データの取扱いの目的及びその取扱いの法的根拠。
(d) その取扱いが第6 条第1 項(f)を根拠とする場合、管理者又は第三者が求める正当な利益。
(e) もしあれば、個人データの取得者又は取得者の類型。
(f) 該当する場合は、管理者が個人データを第三国又は国際機関に移転することを予定しているという事実、及び、欧州委員会による十分性認定の存否、又は、第46 条若しくは第47 条に定める移転の場合又は第 49 条第 1 項第 2 項後段に定める移転の場合、適切又は適合する保護措置、及び、その複製物を取得するための方法、又は、どこでそれらが利用可能とされたかについての情報。

2. 第 1 項に定める情報に加え、管理者は、個人データを取得する時点において、データ主体に対し、公正かつ透明性のある取扱いを確保するために必要な**以下の付加的な情報を提供**する。
(a) その個人データが記録保存される期間、又は、それが不可能なときは、その期間を決定するために用いられる基準。
(b) 個人データへのアクセス、個人データの訂正又は消去、又は、データ主体と関係する取扱いの制限を管理者から得ることを要求する権利、又は、取扱いに対して異議を述べる権利、並びに、データポータビリティの権利が存在すること。
(c) その取扱いが第6 条第1 項(a)又は第9 条第2 項(a)に基づく場合、その撤回前の同意に基づく取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利が存在すること。
(d) 監督機関に異議を申立てる権利。
(e) その個人データの提供が制定法上若しくは契約上の要件であるか否か、又は、契約を締結する際に必要な要件であるか否か、並びに、データ主体がその個人データの提供の義務を負うか否か、及び、そのデータの提供をしない場合に生じうる結果について。
(f) プロファイリングを含め、第22 条第1 項及び第4 項に定める自動的な決定が存在すること、また、これが存在する場合、その決定に含まれている論理、並びに、当該取扱いのデータ主体への重要性及びデータ主体に生ずると想定される結果に関する意味のある情報。

3. 当該個人データが収集された際の目的とは別の目的による個人データの追加的取扱いを管理者が予定している場合、その管理者は、データ主体に対し、当該追加的取扱いの開始前に、当該別の目的に関する情報及び第2 項に定める関連する付加的情報を提供する。

4. 第1 項、第2 項及び第3 項は、データ主体が既にその情報をもっている場合、その範囲内では、適用されない。

（参考）EU GDPR(14条：データ主体以外から情報が取得される場合)

第14 条 個人データがデータ主体から取得されたものではない場合において提供される情報

1. 個人データがデータ主体から取得されたものではない場合、管理者は、データ主体に対し、以下の情報を提供する：
 (a) 管理者の身元及び連絡先、及び、該当する場合は、管理者の代理人の身元及び連絡先。
 (b) 該当する場合は、データ保護オフィサーの連絡先。
 (c) 予定されている個人データの取扱いの目的及びその取扱いの法的根拠。
 (d) 関係する個人データの種類。
 (e) もしあれば、個人データの取得者又は取得者の類型。
 (f) 該当する場合は、管理者が個人データを第三国又は国際機関の取得者に対して移転することを予定しているという事実、及び、欧州委員会による十分性認定の存否、又は、第46 条若しくは第47 条に定める移転の場合又は第 49 条第 1 項第 2 項後段に定める移転の場合、適切又は適合する保護措置、及び、その複製物を取得するための方法、又は、どこでそれらが利用可能とされたかについての情報。

2. 第1 項に定める情報に加え、管理者は、データ主体に対し、データ主体に関して公正かつ透明性のある取扱いを確保するために必要な以下の情報を提供する。
 (a) その個人データが記録保存される期間、又は、それが不可能なときは、その期間を決定するために用いられる基準。
 (b) その取扱いが第6 条第1 項(f)を根拠とする場合、管理者又は第三者が求める正当な利益。
 (c) 個人データへのアクセス、個人データの訂正又は消去、又は、データ主体と関係する取扱いの制限を管理者から得ることを要求する権利、又は、取扱いに対して異議を述べる権利、並びに、データポータビリティの権利が存在すること。
 (d) その取扱いが第6 条第1 項(a)又は第9 条第2 項(a)に基づく場合、その撤回前の同意に基づく取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利が存在すること。
 (e) 監督機関に異議を申立てる権利。
 (f) どの情報源からその個人データが生じたか、及び、該当する場合は、公衆がアクセス可能な情報源からその個人データが来たものかどうか。
 (g) プロファイリングを含め、第22 条第1 項及び第4 項に定める自動的な決定が存在すること、また、それが存在する場合、その決定に含まれている論理、並びに、当該取扱いのデータ主体への重要性及びデータ主体に生ずると想定される結果に関する意味のある情報。

3. 管理者は、以下のとおりに、第 1 項及び第 2 項に定める情報を提供する。
 (a) その個人データが取扱われる具体的な状況を考慮に入れ、個人データ取得後の合理的な期間内。ただし、遅くとも1 か月以内。
 (b) その個人データがデータ主体との間の連絡のために用いられる場合、遅くとも、当該データ主体に対して最初の連絡がなされる時点において。又は、
 (c) 他の取得者に対する開示が予定される場合、遅くともその個人データが最初に開示される時点において。

4， 5 （略）

（参考）CCPA第1798.130条（仮訳）

出典：https://www.ppc.go.jp/files/pdf/ccpa-provisions-ja.pdf

第1798.130条

(5)事業者が、オンライン・プライバシー・ポリシーを有している場合にはそのオンライン・プライバシー・ポリシー、及び、消費者プライバシー権についてのカリフォルニア固有の記述において、プライバシー・ポリシーを持たない場合には、その事業者のインターネット・ウェブサイトにおいて、**以下の情報を開示し、少なくとも12か月に１回その情報をアップデートする**。

(A)第1798.100条、第1798.105条、第1798.110条、第1798.115条及び第1798.125条による消費者の権利の記述、及び、一つ又はそれ以上の要求の提出の指定された方法。

(B) 第1798.110条第（c）項の目的のために、収集された個人情報を最も厳密に記述する第（c）項に列挙された類型を参照した、過去12か月に事業者が収集した消費者の個人情報の類型の一覧。

(C)第1798.115条第（c）項（1）号及び（2）号のために、二つの別々の一覧:

(i)販売された個人情報を最も厳密に記述する第（c）項に列挙された類型を参照した、過去12か月間に販売された消費者の個人情報の類型の一覧。
もし事業者が過去12か月間に消費者の個人情報を販売していなかった場合には、事業者はその事実を開示する.

(ii) 開示された個人情報を最も厳密に記述する第（c）項に列挙された類型を参照した、過去12か月間に事業目的のために開示された消費者に関する個人情報の類型の一覧。もし事業者が過去12か月間に事業目的のために消費者の個人情報を開示していなかった場合には、事業者はその事実を開示する。

（参考）個人情報保護法（平成十五年法律第五十七号）

（保有個人データに関する事項の公表等）
第三十二条　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
一　当該個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
二　全ての保有個人データの利用目的（第二十一条第四項第一号から第三号までに該当する場合を除く。）
三　次項の規定による求め又は次条第一項（同条第五項において準用する場合を含む。）、第三十四条第一項若しくは第三十五条第一項、第三項若しくは第五項の規定による請求に応じる手続（第三十八条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）
四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの
２・３　（略）

● 個人情報の保護に関する法律施行令（平成十五年政令第五百七号）
（保有個人データの適正な取扱いの確保に関し必要な事項）
第十条　法第三十二条第一項第四号の政令で定めるものは、次に掲げるものとする。
一　法第二十三条の規定により保有個人データの安全管理のために講じた措置（本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）
二　当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
三　当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

（参考）EU GDPR第35条（仮訳）

出典： https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

第35条　データ保護影響評価

1. 取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならない。類似の高度のリスクを示す一連の類似する取扱業務は、単一の評価の対象とすることができる。

2. 管理者は、データ保護影響評価を行う場合、その指定をしているときは、データ保護オフィサーに対して助言を求めなければならない。

3. 第1 項に規定するデータ保護影響評価は、とりわけ、以下の場合に求められる：

(a) プロファイリングを含め、自動的な取扱いに基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価の場合；

(b) 第9 条第1 項に規定する特別な種類のデータ又は第10 条に規定する有罪判決及び犯罪行為と関連する個人データの大規模な取扱いの場合；又は、

(c) 公衆がアクセス可能な場所の、システムによる監視が大規模に行われる場合。

4~6　（略）

7. 評価は、**少なくとも以下の事項を含めるものとする**：

(a) 予定されている取扱業務及び取扱いの目的の体系的な記述。該当する場合、管理者の求める正当な利益を含む；

(b) その目的に関する取扱業務の必要性及び比例性の評価；

(c) 第1項で定めるデータ主体の権利及び自由に対するリスクの評価；並びに、

(d) データ主体及び他の関係者の権利及び正当な利益を考慮に入れた上で、個人データの保護を確保するための、及び、本規則の遵守を立証するための、保護措置、安全管理措置及び仕組みを含め、リスクに対処するために予定されている手段。

8~10　（略）

11. 必要があるときは、管理者は、少なくとも、取扱業務によって示されるリスクの変化が存在する時点において、データ保護影響評価に従って取扱いが遂行されているか否かの評価を見直しを実行しなければならない。

（参考）イギリス　電子コミュニケーション（セキュリティ対策）規制案（仮訳）

9. ガバナンスと説明責任

(1)ネットワーク提供者又はサービス提供者は、法第105条Ａ（１）の目的を達成するため、
提供者を代表して措置を執る責任が与えられた、適切なマネジメント者を確保しなければならない。

(2) (1)の義務は、特に以下の義務を含む。

(b) 公共の電子コミュニケーションネットワーク又は公共の電子コミュニケーションサービスの**提供に関与する者による不正な行いに起因するセキュリティ侵害のリスク**を低減するため、
居住国等により不適切な影響の受けやすさを考慮した措置等、全ての適切な措置を特定し、執ること。

(c) 少なくとも12ヶ月に１度のセキュリティ侵害のリスクを見直し、以下を考慮に入れて、セキュリティ侵害の全体のリスクの程度に関する書面による評価を行う。

（ｉ）ネットワーク提供者の場合、3(3)(a)(b)（※）に基づき特定されたリスク
※ **全体ネットワーク及び個々の機能又はネットワークがさらされた場合のリスク。（機微なデータを含んでいるか、セキュリティの重要な機能か等を考慮。）**

（ii）6(2)(a)（※）に基づき特定されたリスク　※ **サプライチェーンに起因するセキュリティ侵害のリスク**

（iii）7(2)(ｉ)（※）に基づき行われたレビューの結果
※ **セキュリティ侵害のリスクに関連する変化を考慮した上でのセキュリティ措置の定期的なレビュー**

（iv）(b)（※）で特定されたリスク
※ 公共の電子コミュニケーションネットワーク又は公共の電子コミュニケーションサービスの**提供に関与する者による不正な行いに起因するセキュリティ侵害のリスク**

（ｖ）その他の関係情報

(d) 様々な深刻レベルのセキュリティインシデントへの対応手順等、
セキュリティ侵害のリスクに関する**ビジネス手順を確立し、定期的に見直す**。

（参考）ドイツ電気通信事業者法（仮訳）

● 独電機通信事業者法第166条

（5）連邦ネットワーク庁は、**セキュリティコンセプトの実施状況を定期的に監査**しなければならない。
監査は少なくとも2年ごとに実施しなければならない。

● 独セキュリティ要件カタログ　※自己で行うことが求められているもの。

3.8 セキュリティ対策の評価

（略）**セキュリティ手法は定期的に再評価**されなければならない。（略）

- 特定の数値（誤動作の回数、ダウンタイムなど）による**定期的なリスク分析及び調査はセキュリティ手法の評価に活用**し得る。
- 定期的かつ現実的なストレステストは、新たなリスク要因を潜在的に特定し得る。

（参考）JIS Q 15001:2017

9.3 マネジメントレビュー

トップマネジメントは、トップマネジメントは，組織の個人情報保護マネジメントシステムが，引き続き，適切，妥当かつ有効であることを確実にするために，あらかじめ定めた間隔で，個人情報保護マネジメントシステムをレビューしなければならない。マネジメントレビューは，**次の事項を考慮しなければならない。**

a) 前回までのマネジメントレビューの結果、とった処置の状況
b) 個人情報保護マネジメントシステムに関連する外部及び内部の課題の変化
c) 次に示す傾向を含めた、個人情報保護パフォーマンスに関するフィードバック
  1) 不適合及び是正処置
  2) 監視及び測定の結果
  3) 監査結果
  4) 個人情報保護目的の達成
d) 利害関係者からのフィードバック
e) リスクアセスメントの結果及びリスク対応計画の状況
f) 継続的改善の機会

マネジメントレビューからのアウトプットには，継続的改善の機会，及び個人情報保護マネジメントシステムのあらゆる**変更の必要性に関する決定を含めなければならない。**

（参考）ISO/IEC･NIST

● ISO/IEC 27001 9.3 マネジメントレビュー

トップマネジメントは，組織のISMSが，引き続き，適切，妥当かつ有効であることを確実にするために，あらかじめ定めた間隔で，ISMSをレビューしなければならない。マネジメントレビューは，**次の事項を考慮しなければならない**。

a) 前回までのマネジメントレビューの結果とった処置の状況
b) ISMSに関連する外部及び内部の課題の変化
c) 次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック
　1)不適合及び是正処置
　2) 監視及び測定の結果
　3) 監査結果
　4) 情報セキュリティ目的の達成
d) 利害関係者からのフィードバック
e) リスクアセスメントの結果及びリスク対応計画の状況
f) 継続的改善の機会

マネジメントレビューからのアウトプットには，継続的改善の機会，及びISMSのあらゆる**変更の必要性に関する決定を含めなければならない**。 組織は，マネジメントレビューの結果の証拠として，文書化した情報を保持しなければならない。

● NIST SP800-171 3.11 リスク評価

基本セキュリティ要件
　3.11.1 組織のシステム運用、および CUI に関連する処理、格納、または伝送から生ずる、組織運営（ミッション、機能、イメージ、評判を含む）、組織資産、および個人に対するリスクを定期的に評価する。
派生セキュリティ要件
　3.11.2 システムおよびアプリケーションの脆弱性スキャンを定期的に、かつ、それらのシステムおよびアプリケーションに影響する新たな脆弱性が特定された場合に実施する。
　3.11.3 リスク評価に従って、脆弱性を取り除く。
　3.12 セキュリティ評価
基本セキュリティ要件
　3.12.1 組織のシステムのセキュリティ管理策を定期的に評価し、その管理策の適用が有効かどうかを判断する。
　3.12.2 組織のシステムの欠陥を修正し、脆弱性を軽減・排除することを意図した実施計画書を作成し、実施する。
　3.12.3 システムのセキュリティ管理策が継続的に有効であることを確実にするため、その管理策を継続的に確認する。
　3.12.4 システムの境界、運用環境、セキュリティ要件の実装方法、および他のシステムとの関係または他のシステムへの接続について記述したシステムセキュリティ計画書を作成し、文書化し、定期的に更新する。

（参考）EU GDPR第37･39条（仮訳）

出典： https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

第37条 データ保護オフィサーの指名

1. （略）

2. 企業グループは、データ保護オフィサーが各拠点から容易にアクセス可能な場合に限り、1 名のデータ保護オフィサーを指名できる。

3･4 （略）

5.データ保護オフィサーは、**専門家としての資質、及び、特に、データ保護の法令及び実務に関する専門知識並びに第39条で定める職務を充足するための能力**に基づいて指定される。

6 （略）

7. 管理者又は処理者は、データ保護オフィサーの連絡先の詳細を公表し、かつ、監督機関に対し、それを連絡しなければならない。

第39条 データ保護オフィサーの職務

1. データ保護オフィサーは、**少なくとも、以下の職務を行わなければならない**：

(a) 管理者又は処理者及び取扱いを行う従業者に対し、本規則及びそれ以外のEU 若しくは加盟国のデータ保護条項による義務を通知し、かつ、助言すること；

(b) 取扱業務に関与する職員の責任の割当て、意識向上及び訓練、並びに、関連する監査を含め、本規則の遵守、それ以外のEU 又は加盟国の個人データ保護条項遵守、並びに、個人データ保護と関連する管理者又は処理者の保護方針の遵守を監視すること；

(c) 要請があった場合、第35 条によるデータ保護影響評価に関して助言を提供し、その遂行を監視すること；

(d) 監督機関と協力すること；

(e) 取扱いと関連する問題に関し、監督機関の連絡先として行動すること。第36条に規定する事前協議、適切な場合、それ以外の関連事項について協議することを含む。

2. データ保護オフィサーは、その職務を遂行する際、取扱いの性質、範囲、過程及び目的を考慮に入れた上で、取扱業務と関係するリスクに関し、適正に注意を払う。

（参考）イギリス・ドイツ関連法令（仮訳）

■ 英電子コミュニケーション（セキュリティ対策）規制案

9. ガバナンスと説明責任

(1)ネットワーク提供者又はサービス提供者は、法第105条Ａ（１）の目的を達成するため、提供者を**代表して措置を執る責任が与えられた者の適切なマネジメント**を確保しなければならない。

(2) (1)の義務は、特に以下の義務を含む。

(a) セキュリティを重要なビジネス機能として扱い、明確なセキュリティ方針及び適切なリソースの確保等を通じて、**効率的なセキュリティマネジメントを行う責任を取締役会レベルの者又は委員会に与える**こと。

10. コンピテンシー

(1)法第105条Ａ（１）の目的を達成するため、以下のとおり、**提供者を代表して措置を執る責任が与えられた者（**以下「責任者」という。）及びセキュリティの重要な機能の運用をサポートする者**を確保しなければならない。**

(a) **責任を果たし、こうした機能の運用をサポートするに足る能力を有する**こと。

(b) 職務の遂行にあたり適切な権限及びリソースが与えられていること。

(2) (1)の義務は、特に以下の義務を含む。

(a) **セキュリティ上重要な機能の運用を支えるネットワーク及び情報システムのセキュリティに関し、組織上の役割を効率的に果たすことができる適切な知識・技能を有する**こと。

(b) セキュリティの重要な機能の運用をサポートする者は、**セキュリティ措置に関し適切に訓練をされていること。**

(c) 責任者について、regulation 5に基づく**モニタリング及び監査の義務を果たすことができる能力を有し**、そのために適切なリソースを与えられていること。

(d)(e) （略）

(3) （略）

■ 独電気通信事業者法

第166条　セキュリティ管理者及びセキュリティコンセプト

（１）公共の電気通信ネットワークを運営する、または一般にアクセス可能な電気通信サービスを提供する者は、セキュリティ管理者を指名しなければならない。（略）

■ 独セキュリティ要件カタログ

５．１．８　セキュリティ管理者の指名

（略）セキュリティ管理者は**一定の調整、管理、専門家としての権限が与えられなければならない。**セキュリティ管理者等は連邦ネットワーク庁のコンタクトパーソンでなければならない。

（参考）JIS Q 15001･ISO/IEC･NIST

● JIS Q 15001　附属書A.3.3.4 資源，役割，責任及び権限の割当て

トップマネジメントは，少なくとも，次の責任及び権限を割り当てなければならない。

a) 個人情報保護管理者

b) 個人情報保護監査責任者

トップマネジメントは，この規格の内容を理解し実践する能力のある個人情報保護管理者を組織内部に属する者の中から指名し，個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え，業務を行わせなければならない。

トップマネジメントは，次の事項により個人情報保護管理者を指名することができる。

c) 社外に責任をもつことができる者（例えば，経営層）を個人情報保護管理者に指名すること。

d) 複数の者を指名し，責任が不明確になることを避けること。

e) 業務部が複数あり個人情報保護管理者を複数名指名する場合，当該者間での役割分担を明確にすること。

個人情報保護管理者は，個人情報保護マネジメントシステムの見直し及び改善の基礎として，トップマネジメントに個人情報保護マネジメントシステムの運用状況を報告しなければならない。個人情報保護管理者は，運用の手順を実施する担当者を兼任しても差し支えない。

トップマネジメントは，公平，かつ，客観的な立場にある個人情報保護監査責任者を組織内部に属する者の中から指名し，監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え，業務を行わせなければならない。

個人情報保護監査責任者は，監査を指揮し，監査報告書を作成し，トップマネジメントに報告しなければならない。監査員の選定及び監査の実施においては，監査の客観性及び公平性を確保しなければならない。

● ISO/IEC 27001 5.3 組織の役割，責任及び権限

トップマネジメントは，次の事項に対して，責任及び権限を割り当てなければならない。

a) ISMSが，この規格の要求事項に適合することを確実にする。

b) ISMSのパフォーマンスをトップマネジメントに報告する。

注記 トップマネジメントは，ISMSのパフォーマンスを組織内に報告する責任及び権限を割り当ててもよい

● NIST SP800-53

3.13 プログラムマネジメント　PM-2 情報セキュリティプログラムの責任者の役割

組織全体の情報セキュリティプログラムを調整、策定、実装、維持するためのミッションとリソースを有する政府機関の情報セキュリティ責任者を任命する。