プライバシー保護とサイバーセキュリティの法的対応

2025年11月13日

光和総合法律事務所
弁護士　渡邊　涼介

講師　渡邊涼介　プロフィール

光和総合法律事務所（パートナー）
弁護士・情報処理安全確保支援士

2007年弁護士登録。2014年～2016年総務省総合通信基盤局消費者行政課専門職、2016年～2017年総務省総合通信基盤局消費者行政第一課、消費者行政第二課専門職（併任）。2019年～2020年、内閣サイバーセキュリティセンター（NISC）サイバーセキュリティ関連法令の調査検討等を目的としたサブワーキンググループ タスクフォース構成員。

総務省では、個人情報保護法の改正に関わる他、ＩｏＴやカメラ画像など、ＩＣＴ（情報通信技術）分野におけるデータ保護に関する施策を担当した。弁護士業務では、データの利活用・管理を中心とした法的助言をしている。

・主な著作

『プライバシー保護・サイバーセキュリティの法的対応』（ぎょうせい、2025）
（山岡裕明弁護士との共著）

『データ利活用とプライバシー・個人情報保護〔第２版〕』（青林書院、2023）

『人事労務管理とプライバシー・個人情報保護』（青林書院、2022）

プログラム

1．プライバシー保護とサイバーセキュリティの関係
（1）最近の動向
（2）プライバシー保護とは
（3）サイバーセキュリティとは
（4）プライバシー保護とサイバーセキュリティの相違点

2．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（1）「社労夢」ランサムウエア攻撃事件
（2）NTT西日本子会社不正持出し事件

3．サイバー対処能力強化法の概要

1．プライバシー保護とサイバーセキュリティの関係
（1）最近の動向

◢ 情報セキュリティ10大脅威 2025 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

出典：IPAホームページ
情報セキュリティ10 大脅威 2025
https://www.ipa.go.jp/security/10threats/10threats2025.html

1．プライバシー保護とサイバーセキュリティの関係
（1）最近の動向

1位 ランサム攻撃による被害

ランサムウェアとは、PC やサーバーに感染後、端末のロックやデータの窃取、暗号化を行い、これらを取引材料とした様々な脅迫により金銭を要求するマルウェアの一種である。ランサムウェアを用いた攻撃をランサム攻撃と呼び、攻撃者は複数の脅迫を組み合わせて、被害組織が金銭の支払いを検討せざるを得ない状況を作り出そうとする。また、近年では RaaS（Ransomware as a Service）という、サービスとして開発・提供されたランサムウェアを利用して攻撃を実行する形態も確認されるほか、ランサムウェアによる暗号化を行わず、窃取した機密情報を公開すると脅迫して金銭を要求する「ノーウェアランサム」による攻撃も確認されている[1]。

出典：IPAホームページ　情報セキュリティ10 大脅威 2025
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf

1．プライバシー保護とサイバーセキュリティの関係
（1）最近の動向

（抜粋）
＜脅威と影響＞
攻撃者は PC やサーバーをランサムウェアに感染させ、金銭要求を伴う以下のような脅迫を行う。
① PC やサーバーのデータを暗号化し、業務の継続を困難にさせた後、データの復元と引き換えに金銭要求に応じるよう脅迫する。
② 機密情報を窃取し、リークサイト等に公開すると脅迫する。
③ DDoS 攻撃（Distributed Denial of Service Attack：分散型サービス妨害攻撃）を仕掛けると脅迫する。
④ ランサムウェアに感染したことを被害者の利害関係者等に連絡すると脅迫する。
また、これらを組み合わせた「二重脅迫」や「四重脅迫」も確認されている。ランサム攻撃を受けると、その調査や復旧に多くの費用と時間がかかり、業務やサービス提供の停止による損失や、取引先からの信頼失墜等につながるおそれもある。
近年では、ランサムウェアを用いない金銭要求を行う攻撃として、「ノーウェアランサム」による攻撃や、DDoS 攻撃を仕掛けると脅迫するランサムDDoS攻撃も確認されている。

出典：IPAホームページ　情報セキュリティ10 大脅威 2025
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf

⑤　漏えい等元及び漏えい等原因

（期間：令和６年４月１日～令和７年３月 31 日）

	漏えい等元	件数（割合）	原因							
			誤交付	誤送付	誤廃棄	紛失	盗難	内部不正	不正アクセス	その他
個人情報取扱事業者等	報告者	9,494件（66.9%）	5,329件（37.5%）	2,527件（17.8%）	67件（0.5%）	453件（3.2%）	36件（0.3%）	39件（0.3%）	431件（3.0%）	612件（4.3%）
	委託先	2,248件（15.8%）	210件（1.5%）	355件（2.5%）	6件（0.0%）	76件（0.5%）	7件（0.0%）	20件（0.1%）	1,429件（10.1%）	145件（1.0%）
	不明	2,456件（17.3%）	137件（1.0%）	72件（0.5%）	3件（0.0%）	36件（0.3%）	4件（0.0%）	5件（0.0%）	2,018件（14.2%）	181件（1.3%）

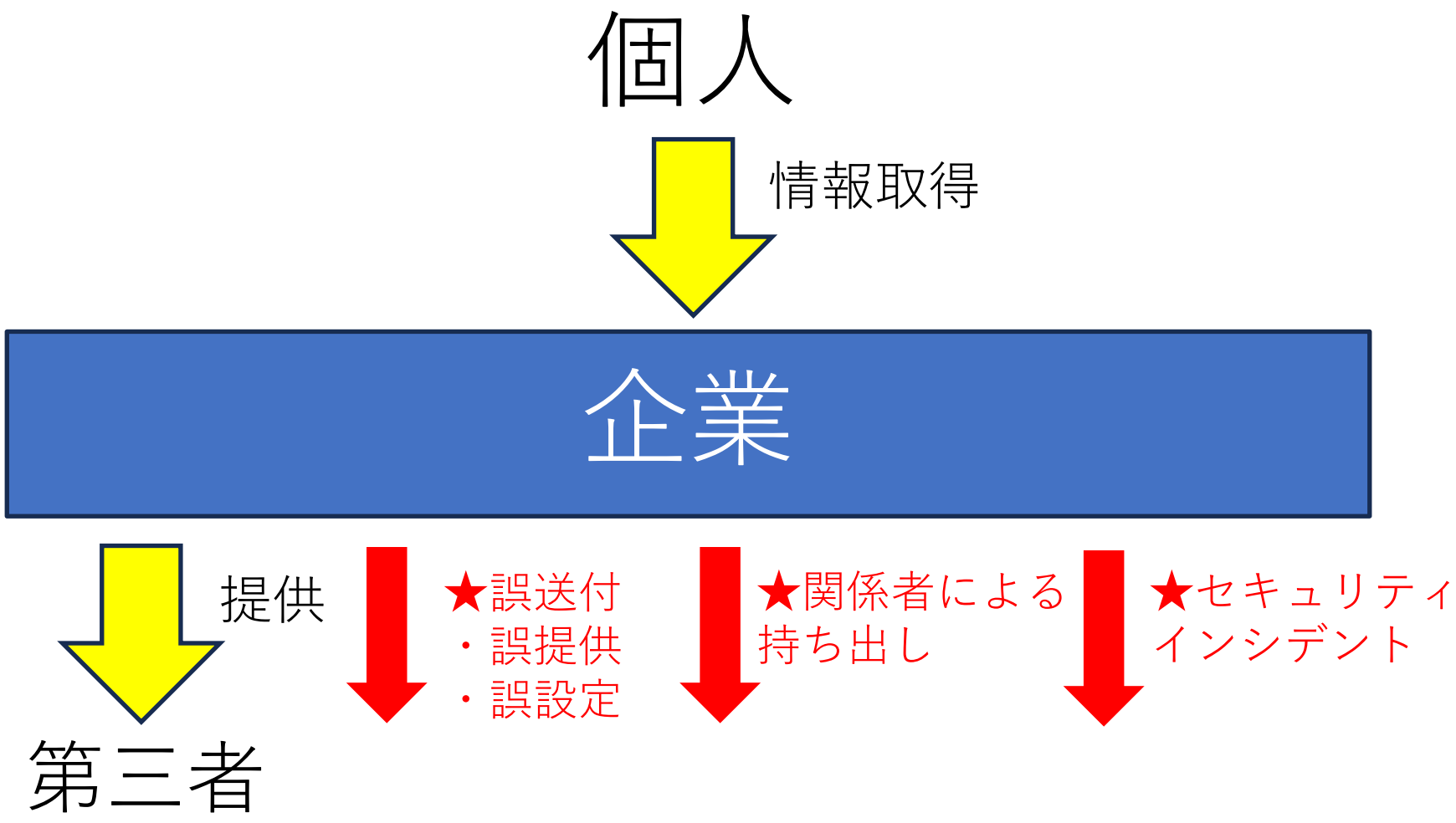
出典：令和６年度 個人情報保護委員会 年次報告
https://www.ppc.go.jp/files/pdf/070610_annual_report.pdf

1．プライバシー保護とサイバーセキュリティの関係
（1）最近の動向

Ⅱ その他の権限行使　１ 個人情報保護法（1）指導・助言（第147条又は第157条） 計166件[1]
① 民間事業者 計127件
・不正アクセスを原因とする漏えい等事案を中心に、安全管理措置の不備等について指導を行った。
・不正アクセスによる漏えい等の原因として、①VPN（Virtual Private Network）機器の脆弱性やECサイトを構築するためのアプリケーション等の脆弱性が公開され、対応方法がリリースされていたにもかかわらず、事業者が放置していたこと、②ID・パスワードが容易に推測されやすいものとされていたこと、③設定ミスによりデータベースへのアクセス制御が不適切な状態になっていたことなど、安全管理措置に不備があったケースが多くみられている。
・攻撃種類としては、ブルートフォース攻撃[2]やECサイトのクロスサイトスクリプティング攻撃[3]などがみられているほか、ランサムウェア攻撃[4]も、30件みられている。
・不正アクセス以外の漏えい等事案では、個人データが保存されたPCやUSBメモリの入ったかばんの盗難などがみられている。
・このほか、不適正な個人情報の利用（個人情報保護法第19条違反）や、本人の同意を得ていない個人データの第三者提供（同法第27 条第１項違反）といった事案もみられた。
・指導等の内容としては、特に技術的安全管理措置に関し、外部からの不正アクセス等の防止の不備が最も多く（42件）、次いで、アクセス者の識別と認証の不備（26件）が多かった。このほか、組織的安全管理措置の不備（９件）、委託先に対する監督の不備（件）などに対して指導を行った。
・下表ア及びイの事案対応のほか、漏えい等報告の提出の遅延に関し、39件の指導を行った。

1 （略）
2 ブルートフォース攻撃とは、考えられる全てのパスワードを使って、総当たりでログインを試みる攻撃手法である。
3 クロスサイトスクリプティング攻撃とは、ウェブサイトの脆弱性を悪用して、攻撃者が用意した悪意のあるスクリプトを利用者の元に送り込んで実行させる攻撃手法であり、典型的には、ECサイト上に不正なファイルを作成し、そこに利用者が入力したクレジットカード情報を含む個人データを蓄積の上、外部へ転送する形で窃取するというものである。
4 ランサムウェア攻撃とは、感染すると PC 等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラムを用いた攻撃手法である。

出典：令和７年９月24日 個人情報保護委員会
令和７年度第１四半期における監視・監督権限の行使状況の概要
https://www.ppc.go.jp/files/pdf/250924quarter-report_kengenkoushi.pdf



※赤字は、漏えい等（漏えい、滅失、毀損）に該当

プライバシー保護に関連する主な法律

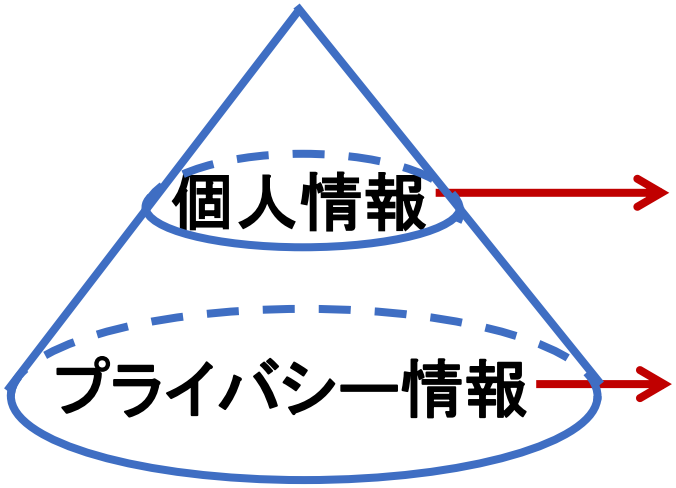
★民法（不法行為、債務不履行：プライバシー侵害に基づく損害賠償請求）

★個人情報保護法（情報の性質に着目した規制）

★独占禁止法・優越的地位の濫用（取扱主体及び取扱態様に着目した規制）

★不正競争防止法（営業秘密・刑事）（取扱態様に着目した規制）

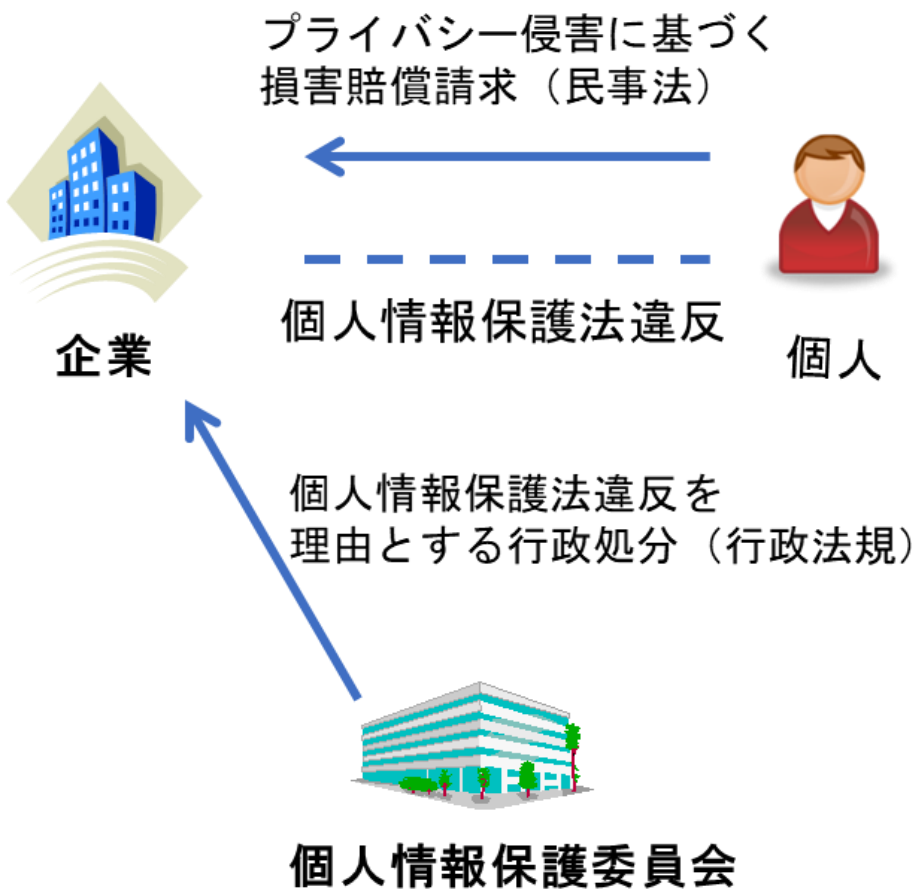
★業法（金融、医療、通信分野（電気通信事業法）等）（取扱主体に注目した規制）



プライバシー情報 ⊃ 個人情報

・個人情報保護法による規律で特に保護
⇒違反すると、指導（個情法147条）などの対象となる

・民事法による規律が適用される
⇒受忍すべき限度を超えて侵害すると、不法行為（民法709条）が成立する


プライバシー侵害に基づく
損害賠償請求（民事法）
個人情報保護法違反
企業
個人
個人情報保護法違反を
理由とする行政処分（行政法規）
個人情報保護委員会

サイバーセキュリティ基本法２条

「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

（３）サイバーセキュリティとは

情報セキュリティ
企業の情報システムを取り巻く様々な脅威から、情報の機密性・完全性・可用性の３要素を確保・維持すること

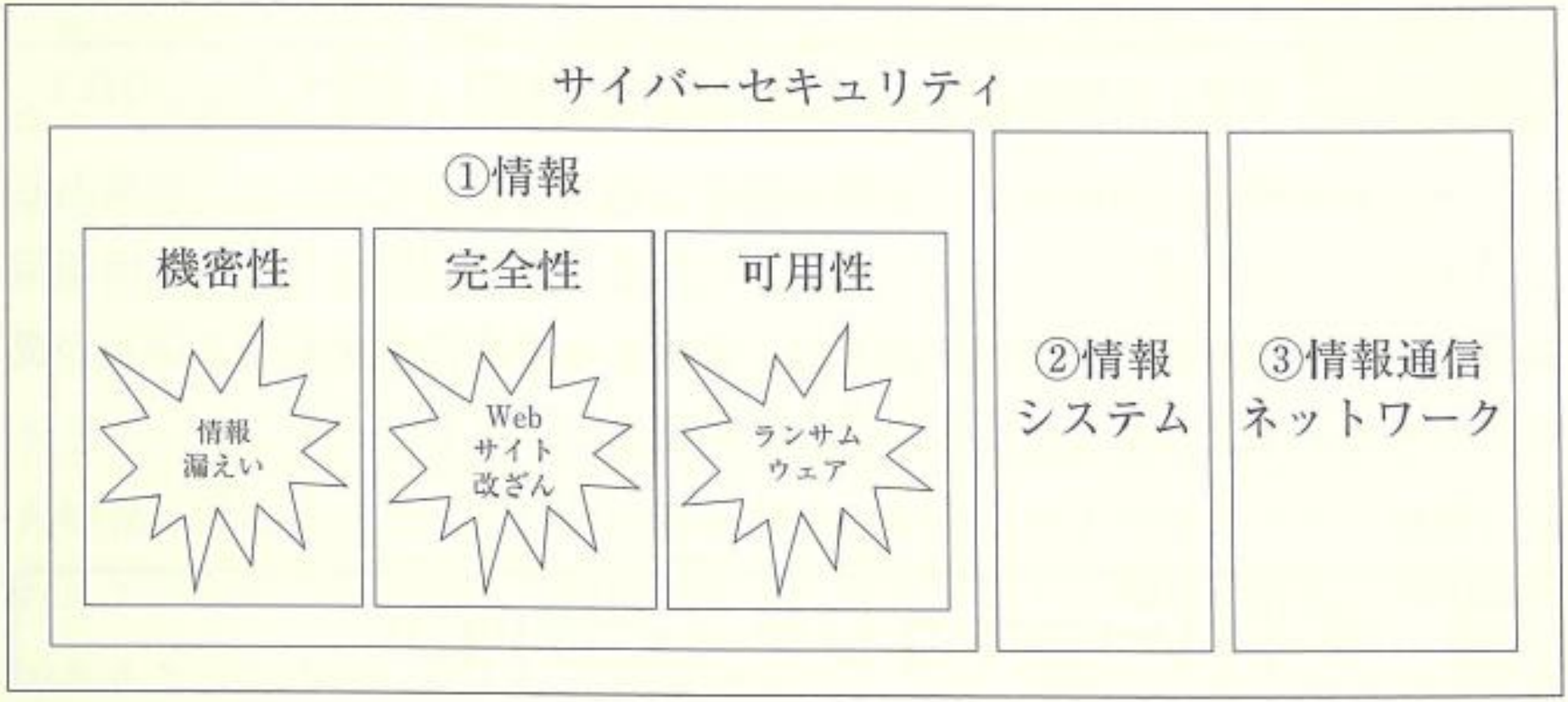
★機密性：認可されていない人に情報を使用させず、開示しないこと
（侵害例：情報の漏えい、通信（電子メール）の盗聴）

★完全性：情報が改ざんされることなく正確な情報を保つこと
（侵害例：ウェブサイトのコンテンツの改ざん）

★可用性：認可された人が要求したときに、情報が使用可能であること
（侵害例：Webサーバの停止、ランサムウェア感染）

（３）サイバーセキュリティとは

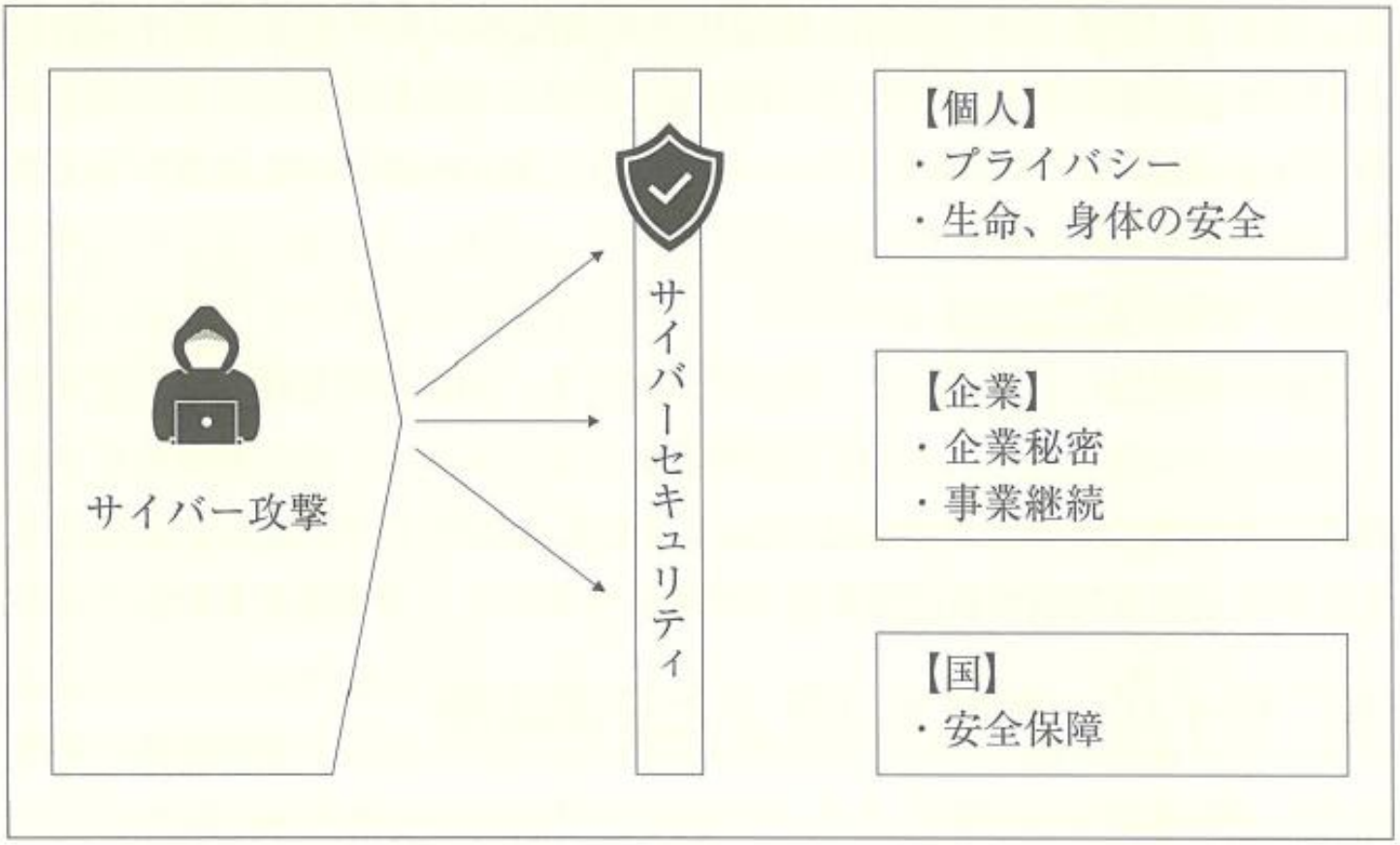
〈図表２〉　保護すべき客体の観点から整理したサイバーセキュリティの概念図



出典：プライバシー保護・サイバーセキュリティの法的対応』8頁

（３）サイバーセキュリティとは

〈図表３〉　保護法益の観点から整理したサイバーセキュリティの概念図



出典：プライバシー保護・サイバーセキュリティの法的対応』11頁

サイバーセキュリティに関連する主な法律等

★国のサイバーセキュリティに関する施策について
- サイバーセキュリティ基本法

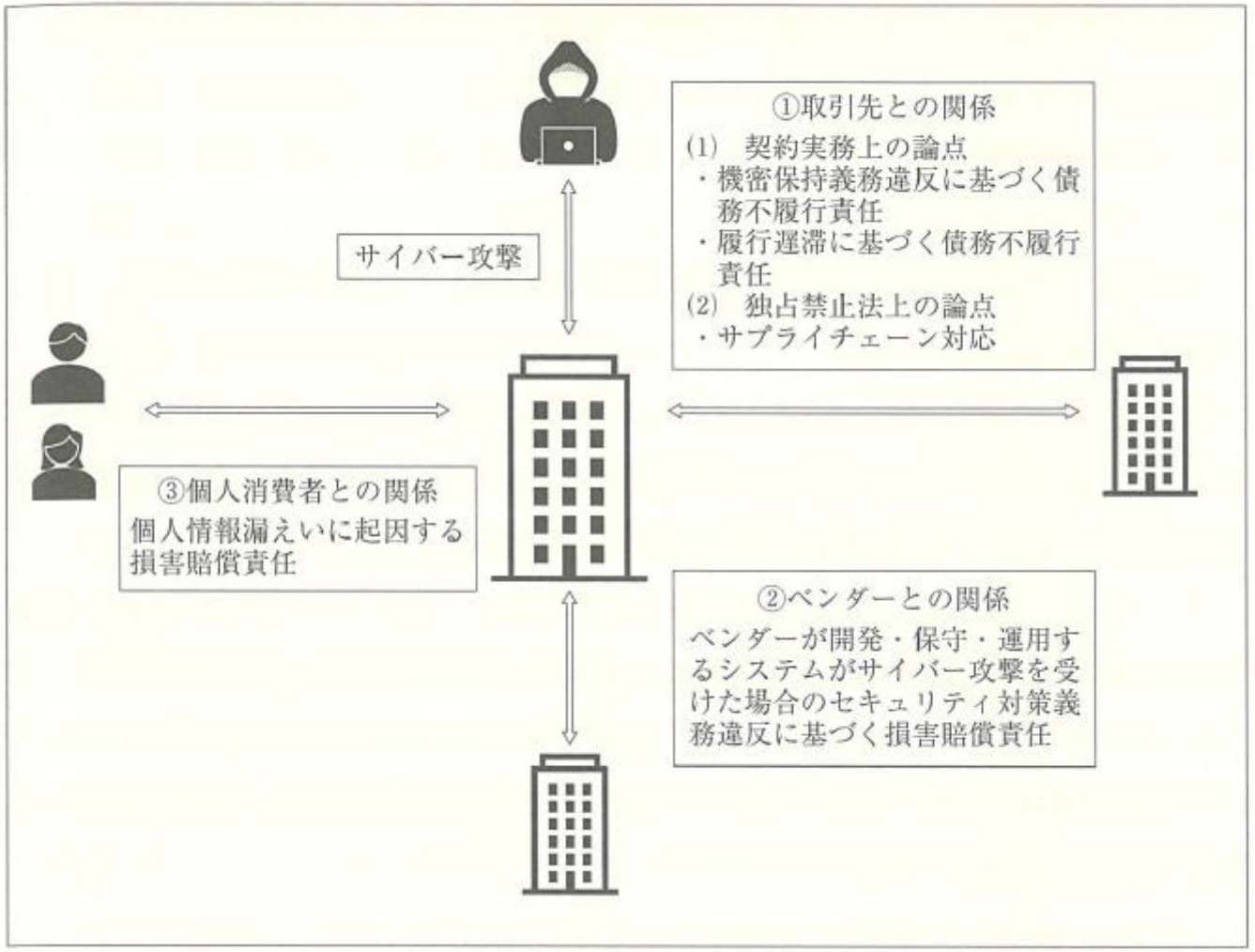
★対象となる情報の保護について
- 個人情報保護法
- 秘密情報（秘密保持契約）
- 不正競争防止法（営業秘密）
- 各種業法

★サイバー攻撃に関する犯罪、刑罰について
- 刑法（不正指令電磁的記録作成等罪等）、不正アクセス禁止法

★損害賠償責任について
- 民法（不法行為、債務不履行）
- 会社法（取締役による内部統制システムの構築義務違反）

1．プライバシー保護とサイバーセキュリティの関係
（3）サイバーセキュリティとは

〈図表18〉　サイバー攻撃を受けた際に生じる各ステークホルダーとの責任関係



出典：プライバシー保護・サイバーセキュリティの法的対応』83頁

（３）サイバーセキュリティとは

「サイバーセキュリティ関係法令Q&Aハンドブック Ver2.0」（NISC、令和5年9月）
https://security-portal.nisc.go.jp/guidance/law_handbook.html

Q&Aで取り上げている主なトピックスについて

1. サイバーセキュリティ基本法関連
2. 会社法関連（内部統制システム等）
3. インシデント対応関連総論（当局等対応、関係者対応）
4. 個人情報保護法関連
5. 不正競争防止法関連
6. 労働法関連（秘密保持・競業避止等）
7. 情報通信ネットワーク関連（IoT関連等を含む）
8. 契約関連（電子署名、システム開発、クラウド等）
9. 資格等（情報処理安全確保支援士等）
10. その他各論（リバースエンジニアリング、暗号、情報共有、脅威インテリジェンス、データ消去等）
11. インシデント対応関連（事後的対応等）（ランサムウェア対応、デジタル・フォレンジック、サイバー保険等を含む）
12. 民事訴訟手続
13. 刑事法（サイバー犯罪等）
14. 海外法令（GDPR等）

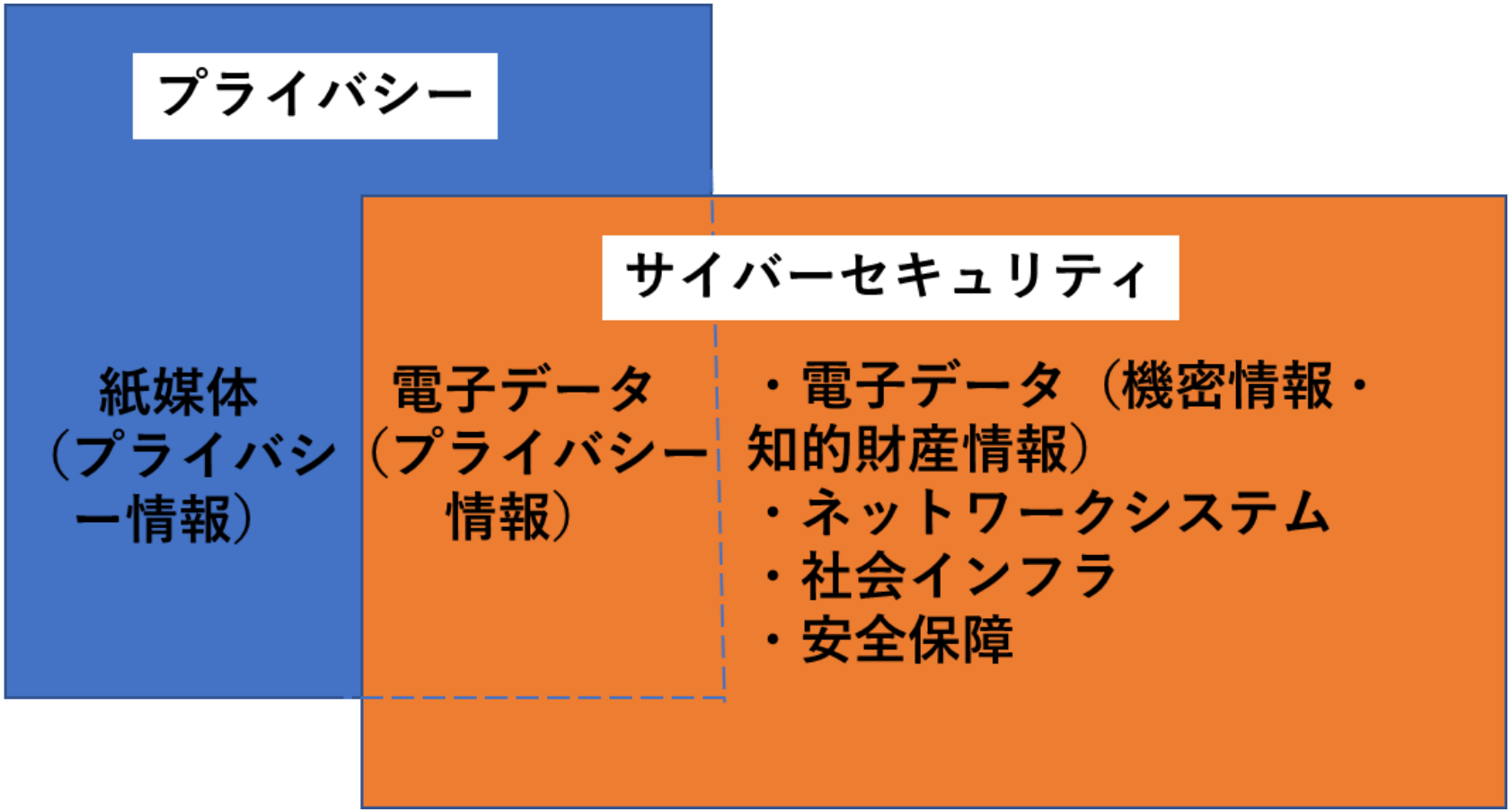
（３）サイバーセキュリティとは

「サイバーセキュリティ関係法令Q&Aハンドブック Ver2.0」（NISC、令和5年9月）
https://security-portal.nisc.go.jp/guidance/law_handbook.html

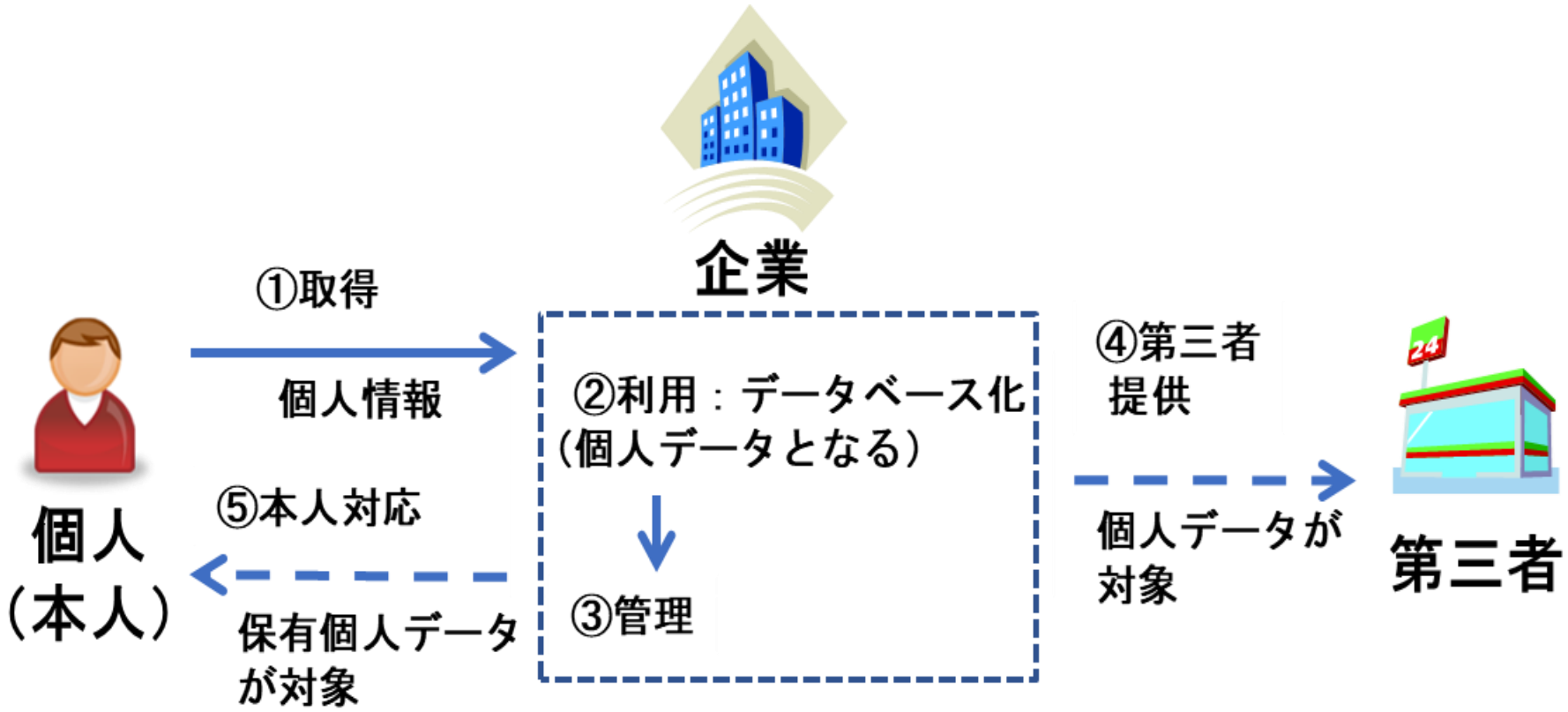
Ver2.0で追加されたQの一覧

- サイバーセキュリティインシデント発生時の当局等対応
- インシデントレスポンスと関係者への対応
- 5G促進法（特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律）
- ドローンとサイバーセキュリティ
- 重要インフラ分野における規律
- モビリティとサイバーセキュリティ
- DX認定・DX銘柄とサイバーセキュリティ
- サイバーセキュリティに関する規格等とNIST SP800シリーズ
- 認証/本人確認に関する法令について
- サイバーセキュリティ事業者への投資
- 脅威インテリジェンスサービス
- データの消去、データが記録された機器・電子媒体の廃棄
- ランサムウェア対応
- インシデント対応における費用負担及びサイバー保険
- 越境リモートアクセス
- 海外における主なサイバーセキュリティ法令
- 国際捜査共助・協力に関する条約・協定

（４）プライバシー保護とサイバーセキュリティの相違点



（４）プライバシー保護とサイバーセキュリティの相違点



１．プライバシー保護とサイバーセキュリティの関係
（４）プライバシー保護とサイバーセキュリティの相違点

個人情報保護法

（安全管理措置）
第２３条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の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。
（従業者の監督）
第２４条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データ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。
（委託先の監督）
第２５条　個人情報取扱事業者は、個人データ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。

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）3-4-4
・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、「10（（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、あらかじめ確認しなければならない。
・委託契約の締結
委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むことが望ましい。
・委託先における個人データ取扱状況の把握
　委託先における委託された個人データ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、及び再委託先が法第23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（※4）。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。

１．プライバシー保護とサイバーセキュリティの関係
（４）プライバシー保護とサイバーセキュリティの相違点

個人情報保護法（安全管理措置）通則GL10（別添）講ずべき安全管理措置の内容（2023年9月現在）

講じなければならない措置	手法の例示
①基本方針の策定	（略）
②個人データの取扱いに係る規定の整備	企業は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために、個人データ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。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の取扱規程を策定することが考えられる。
③組織的安全管理措置	ア 組織体制の整備 イ 個人データの取扱いに係る規律に従った運用 ウ 個人データの取扱状況を確認する手段の整備 エ 漏えい等の事案に対応する体制の整備 オ 取扱状況の把握及び安全管理措置の見直し
④人的安全管理措置	企業は、従業者の教育をしなければならない。手法の例として、個人データの取り扱いに関する留意事項について、従業者に定期的な研修等を行うこと、個人データの秘密保持に関する事項を就業規則等に盛り込むことがあげられる。
⑤物理的安全管理措置	**ア 個人データを取り扱う区域の管理** **イ 機器および電子媒体等の盗難等の防止** **ウ 電子媒体等を持ち運ぶ場合の漏えい等の防止** **エ 個人データの削除および機器、電子媒体等の廃棄**
⑥技術的安全管理措置	**ア アクセス制御** **イ アクセス者の識別と認証** **ウ 外部からの不正アクセス等の防止** **エ 情報システムの使用に伴う漏えい等の防止**
⑦外的環境の把握	企業は、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。

（４）プライバシー保護とサイバーセキュリティの相違点

通則GL10-6　技術的安全管理措置

　個人情報取扱事業者は、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。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。

（1）アクセス制御

担当者及び取り扱う個人情報データベース等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従業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。

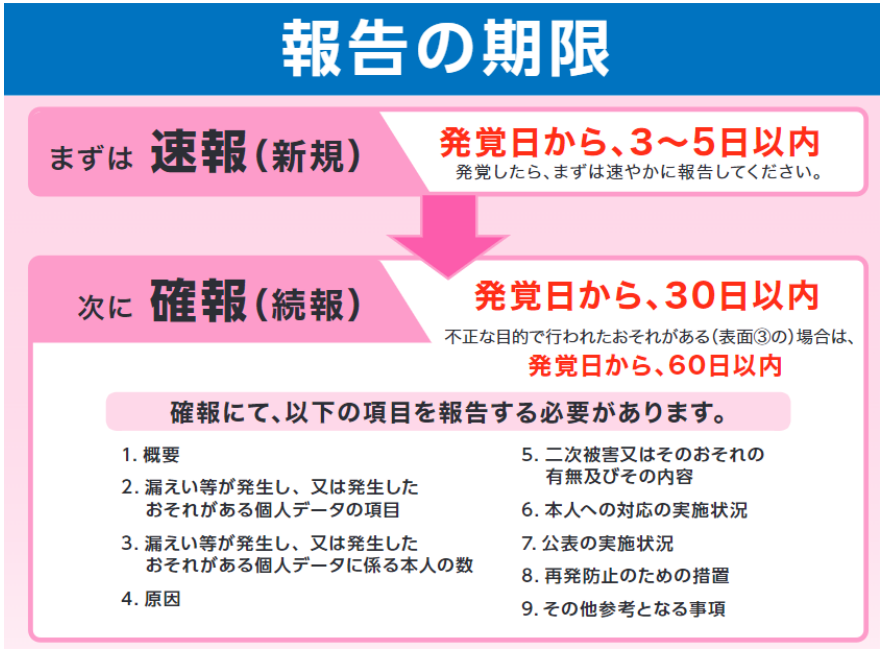
個人情報保護法

（漏えい等の報告等）

第２６条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

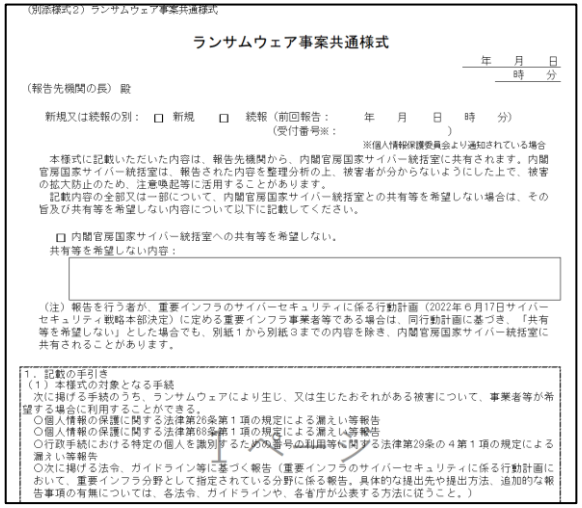
２　前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

1．プライバシー保護とサイバーセキュリティの関係
（4）プライバシー保護とサイバーセキュリティの相違点



出典：個人情報保護委員会ホームページ　漏えい等報告リーフレット
https://www.ppc.go.jp/files/pdf/roueihoukoku_leaflet_2023.pdf

参考　令和7年10月1日以降、ランサムウェア事案による個人データの漏えい等（又はそのおそれ）が発生した場合は、統一様式により報告を行うことができるようになった。


（別添様式2）ランサムウェア事案共通様式

ランサムウェア事案共通様式

年　月　日
時　分

（報告先機関の長）殿

新規又は続報の別：□ 新規　□ 続報（前回報告：　年　月　日　時　分）
（受付番号※：　）
※個人情報保護委員会より通知されている場合

本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。内閣官房国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります。
記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び共有等を希望しない内容について以下に記載してください。

□ 内閣官房国家サイバー統括室への共有等を希望しない。
共有等を希望しない内容：

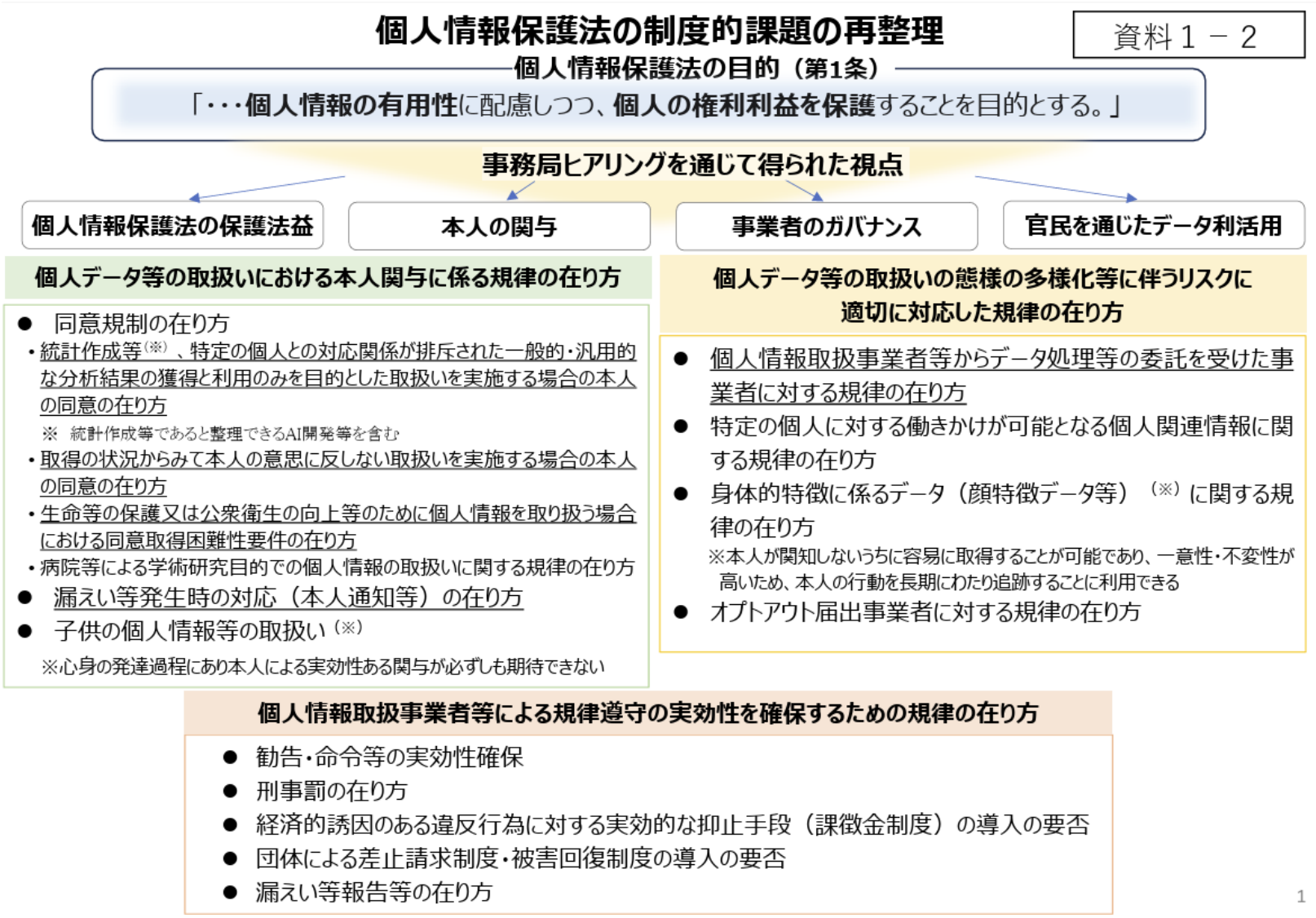
（注）報告を行う者が、重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等である場合は、同行動計画に基づき、「共有等を希望しない」とした場合でも、別紙１から別紙３までの内容を除き、内閣官房国家サイバー統括室に共有されることがあります。

1．記載の手引き
（1）本様式の対象となる手続
次に掲げる手続のうち、ランサムウェアにより生じ、又は生じたおそれがある被害について、事業者等が希望する場合に利用することができる。
○個人情報の保護に関する法律第26条第１項の規定による漏えい等報告
○個人情報の保護に関する法律第68条第１項の規定による漏えい等報告
○行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項の規定による漏えい等報告
○次に掲げる法令、ガイドライン等に基づく報告（重要インフラのサイバーセキュリティに係る行動計画において、重要インフラ分野として指定されている分野に係る報告。具体的な提出先や提出方法、追加的な報告事項の有無については、各法令、ガイドラインや、各省庁が公表する方法に従うこと。）

出典：個人情報保護委員会ホームページ漏えい等の対応とお役立ち資料
https://www.ppc.go.jp/personalinfo/legal/leakAction/

1．プライバシー保護とサイバーセキュリティの関係
（4）プライバシー保護とサイバーセキュリティの相違点

参考：個人情報保護法改正（検討）との関係



出典：https://www.ppc.go.jp/files/pdf/250305_shiryou-1-2.pdf

プライバシー保護とサイバーセキュリティの主な相違点

★サイバーセキュリティ対策における通信の秘密の侵害
- 電気通信事業法における通信の秘密との関係は、これまで総務省の研究会等で検討
- 令和7年5月、サイバー対処能力強化法が成立

★サイバーセキュリティ対策導入時における、従業員のプライバシー保護

プログラム

1．プライバシー保護とサイバーセキュリティの関係
（1）最近の動向
（2）プライバシー保護とは
（3）サイバーセキュリティとは
（4）プライバシー保護とサイバーセキュリティの相違点

2．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（1）「社労夢」ランサムウエア攻撃事件
（2）NTT西日本子会社不正持出し事件

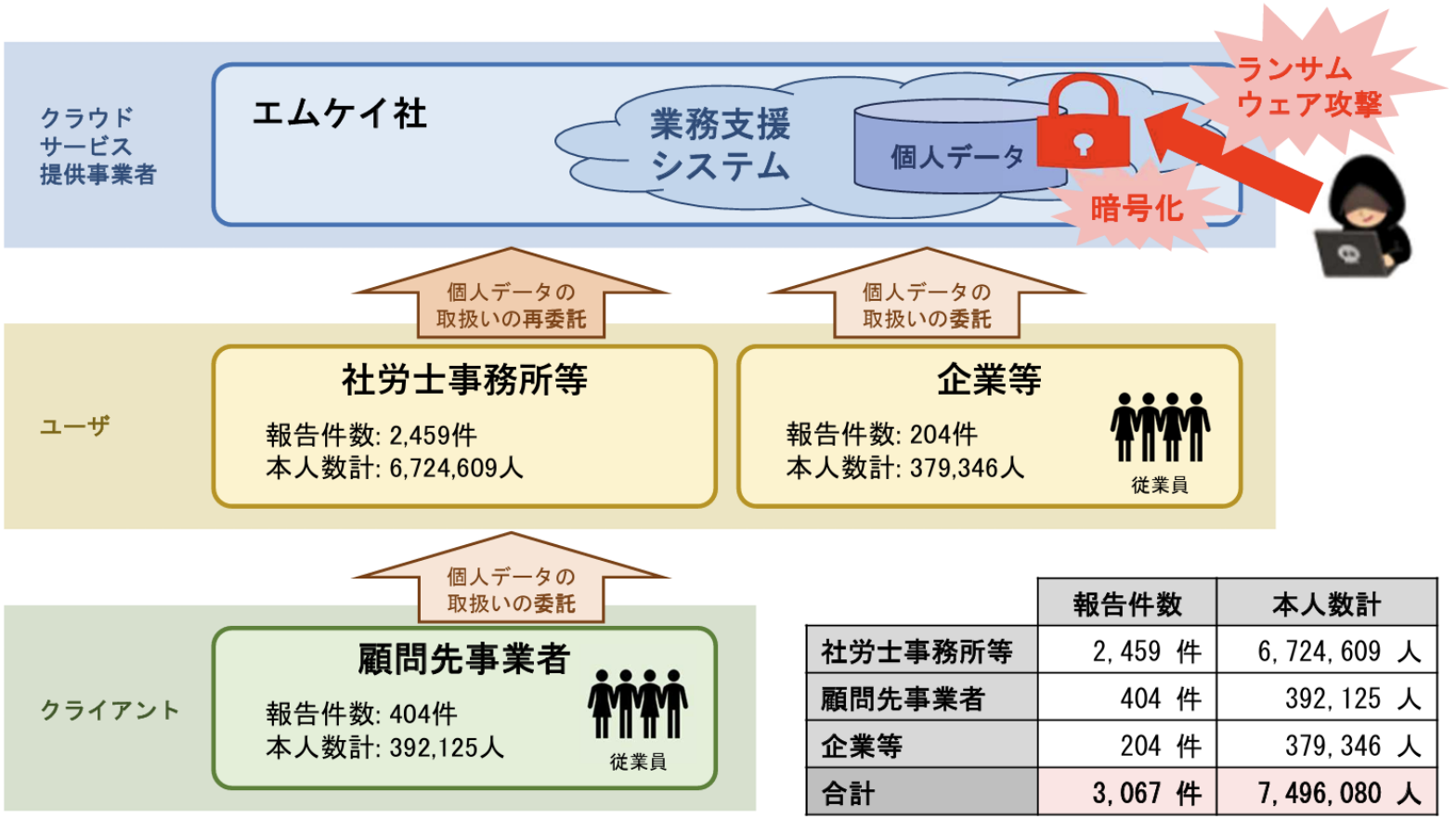
3．サイバー対処能力強化法の概要

２．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（１）「社労夢」ランサムウエア攻撃事件

資料１－２

公表資料

本事案の概要



	報告件数	本人数計
社労士事務所等	2,459 件	6,724,609 人
顧問先事業者	404 件	392,125 人
企業等	204 件	379,346 人
合計	3,067 件	7,496,080 人

※図中の本人数計は、個人情報保護委員会に提出された漏えい等報告のうち、令和６年３月８日時点のものである（本人数不明として報告されているものを除く）。また、本人数は、社労士事務所等と顧問先事業者とで重複して報告している可能性がある。
※エムケイ社からの情報によると、本件システムで管理する本人数は、令和５年６月５日時点で、最大約2,242万人とのことである。

出典：個人情報保護委員会：株式会社エムケイシステムに対する 個人情報の保護に関する法律に基づく行政上の対応について　https://www.ppc.go.jp/files/pdf/240325_houdou.pdf

２．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（１）「社労夢」ランサムウエア攻撃事件

本事案の対応経緯

日付	対応状況
2023/6/5（月）6:00 頃	システムやサービスにアクセスできない状況を確認、システム異常を検知
2023/6/5（月）7:00 頃	弊社内での調査開始。ランサムウェアによる感染を認知
2023/6/5（月）	ランサムウェア被害対策本部設置
2023/6/5（月）午後	外部の情報セキュリティ専門会社へ対応要請 ～状況ヒアリングや初動対応及び原因調査のためのデータ保全等を実施
2023/6/6（火）	大阪府警（捜査当局）へ本事案について連絡、事情聴取に対応
2023/6/6（火）	「第三者によるランサムウェア感染被害のお知らせ」適時開示
2023/6/8（木）	個人情報保護委員会へ報告
2023/6/9（金）	「第三者によるランサムウェア感染被害への対応状況のお知らせ」適時開示
事案発生直後～現在	システム復旧に向けた再構築（継続対応中）
2023/6/21（水）	「第三者によるランサムウェア感染被害への対応状況のお知らせ（第２報）」適時開示
2023/6 月中旬～現在	再発防止策及び対策強化（継続対応中）
2023/6/30（金）0 時	一部サービスの再開：社労夢 V5.0（社労夢シリーズ、ネット de 顧問、ネット de 事務組合）、DirectHR
2023/7/7（金）9 時	一部サービスの再開：社労夢 V3.4（社労夢シリーズ、ネット de 顧問、ネット de 事務組合）、MYNABOX、MYNABOX CL
2023/7/11（火）0 時	一部サービスの再開：一般企業向け社労夢 CompanyEdition V5.0、DirectHR、MYNABOX
2023/7/19（水）	個人情報保護委員会へ確報を提出
2023/7/19（水）	当社サーバへの不正アクセスに関するお知らせと調査結果のご報告（本報告）

出典：株式会社エムケイシステム　当社サーバへの不正アクセスに関する調査結果のご報告（第３報）

２．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（１）「社労夢」ランサムウエア攻撃事件

（略）当社は、2023年６月６日付「第三者によるランサムウェア感染被害のお知らせ」にて公表しました通り、当社サービスを提供しているデータセンター内のサーバーがランサムウェアによる第三者からの不正アクセスを受けました。結果としてシステムが停止し、正常にサービスを提供できない状況となったことから、影響を受けた対象ユーザー様に対する６月ご利用分及び７月ご利用分の一部について請求を停止することになりました。

　またシステムの復旧に当たり、新たにクラウド基盤でのサービスを提供することとなったため、ランサムウェアに感染したデータセンター内のサーバを撤去いたしました。更にシステム復旧及びサービス再開に当たり外部専門機関への調査委託費用、インフラ整備の再構築費用、セキュリティ強化のための費用などが発生しました。これに伴い、当連結会計年度において固定資産除却損として129,831千円、システム障害対応費用として132,106千円を特別損失として計上しました。

出典：株式会社エムケイシステム　有価証券報告書ー第36期（2023/4/1-2024/3/31）から抜粋

2．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（1）「社労夢」ランサムウエア攻撃事件

株式会社エムケイシステムにおける再発防止策の実施状況及び今後の対応について

資料２
公表資料

- 株式会社エムケイシステム（以下「エムケイ社」という。）が社会保険労務士事務所等を対象に提供する社会保険／人事労務業務支援システム（以下「本件システム」という。）のサーバが不正アクセスを受け、ランサムウェアにより、本件システム上で管理されていた個人データが暗号化され、漏えい等のおそれが発生した事案について、個人情報保護委員会（以下「当委員会」という。）はエムケイ社に対し、令和６年３月25日、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）第147条の規定により指導を行い、同法第146条第１項の規定により再発防止策の実施状況を報告するよう求めていた。
- エムケイ社から報告のあった再発防止策の実施状況に関して確認したところ、現時点において当委員会の指導事項を踏まえた一定の取組が認められた。当委員会としては、エムケイ社が再発防止策を確実に実施すること等を引き続き注視していく。
- 一方、ユーザ等のエムケイ社に対する監督の実施状況等については調査中であり、今後、権限行使を含めた必要な対応を検討する。エムケイ社においては、本件システムにおける個人データの取扱いを継続するか否かを検討中であるとのことであり、かかる検討結果についても引き続き注視していく。

指導の原因となる事実	指導の内容	策定した再発防止策の実施状況
【アクセス者の識別と認証】 エムケイ社においては、本件システムのユーザのパスワードルールが脆弱であり、また、管理者権限のパスワードも脆弱であり類推可能なものであった。	1. 法第23条及び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）に基づき、必要かつ適切な措置を講ずること。 2. エムケイ社において策定された再発防止策を確実に実施すること。	① 令和５年６月、パスワードポリシーを強化した。 ② 令和５年６～７月、全ユーザが新ルールに基づくパスワードを設定した。 ③ 令和５年６月、不要アカウントの削除を実施し、削除ルールを整備した。 ・ 社内の未使用アカウントを削除した。 ・ 契約解除したユーザ及びトライアル利用期間が終了したユーザについては、解約及び終了の翌営業日にアカウントを削除する運用に変更した。 ④ 令和６年２月、デバイス認証を導入した。 ・ ID及びパスワード認証に加え、電子証明書導入済のデバイスからのみ本件システムの利用を許可するデバイス認証を導入した。
【外部からの不正アクセス等の防止】 エムケイ社においては、ソフトウェアのセキュリティ更新が適切に行われておらず、深刻な脆弱性が残存していただけでなく、ログの保管、管理及び監視が適切に実施されておらず、不正アクセスを迅速に検知できなかった。		セキュアなプラットフォーム上で本件システムを再構築の上、以下を実施した。 ① 安全な環境における長期のログ保管 ・ 令和５年６月、ログの発生源と保管先を分離し、安全な環境で１年間以上のログが保管できるようにした。 ② ペネトレーションテストの定期的実施 ・ 令和５年６月以降、外部機関により年２回実施する。直近では令和６年５月に実施。 ③ 令和５年７月、ふるまい検知EDR(※1)の導入と外部のSOC(※2)による常時監視を開始した。 ④ ソフトウェアの更新・管理の徹底 ・ 令和５年７月、パッチ適用ツールの利用により、漏れなく迅速にソフトウェアを更新する仕組みを導入し、適用結果を日次で確認している。 ⑤ WAF(※3)ルールの最適化ツールの導入 ・ 令和５年８月、ビッグデータとAIを活用した最適なWAFルールを自動適用するツールを導入した。 ⑥ その他 ・ 令和５年７月、セキュリティ専門会社とアドバイザリー契約を締結。 ・ 令和６年４月、社内のセキュリティ啓発活動の強化と拡充。

※1 EDR(Endpoint Detection and Response:PC等のエンドポイントの不審な挙動を検知・防御する仕組み)
※2 SOC(Security Operation Center:セキュリティ・サービス及び監視を提供する組織)
※3 WAF(Web Application Firewall:Webサイトへのアクセス内容を監視し、攻撃パターンを検知・遮断する仕組み)

出典：個人情報保護委員会ホームページ
https://www.ppc.go.jp/files/pdf/240717_shiryou-2.pdf

2．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
参考　ランサムウェアに関する対応

ランサムウェアでは、復旧と引き換えに金銭を要求される（恐喝罪）。
→ 金銭を支払うことに関し、法的問題が生じる。

●善管注意義務（会社法第 330 条、民法第 644 条）違反に基づく損害賠償責任（会社法第 423 条第 1 項、第 429 条第 1 項）
・経営判断原則　「その決定の過程、内容に著しく不合理な点がない限り、取締役としての善管注意義務に違反するものではない」とされている（最判平成 22 年 7 月 15 日判タ1332 号 50 頁参照）
取締役が、反社会的勢力等である株主からの株主の地位を濫用した不当な要求に応じて金銭的利益の供与を行った事案において、取締役は「暴力団関係者等会社にとって好ましくないと判断される者…（中略）…から、株主の地位を濫用した不当な要求がされた場合には、法令に従った適切な対応をすべき義務を有する」とした判例（最判平成 18 年 4 月 10 日民集 60 巻 4 号 1273 頁）
・経産省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」令和 2 年 12 月
身代金への対応が「経営者が判断すべき経営問題そのものであるということを強く認識する必要がある」と、対応が経営問題であることを強調しつつ、身代金の支払いは、「犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。」
●適時開示
要求された身代金の金額次第では、身代金を支払うこと又は支払わないことを決定した事実は、「投資者の投資判断に著しい影響を及ぼすもの」（有価証券上場規程（東京証券取引所）第 402 条第 1 項 ar）として適時開示が必要となり得る。

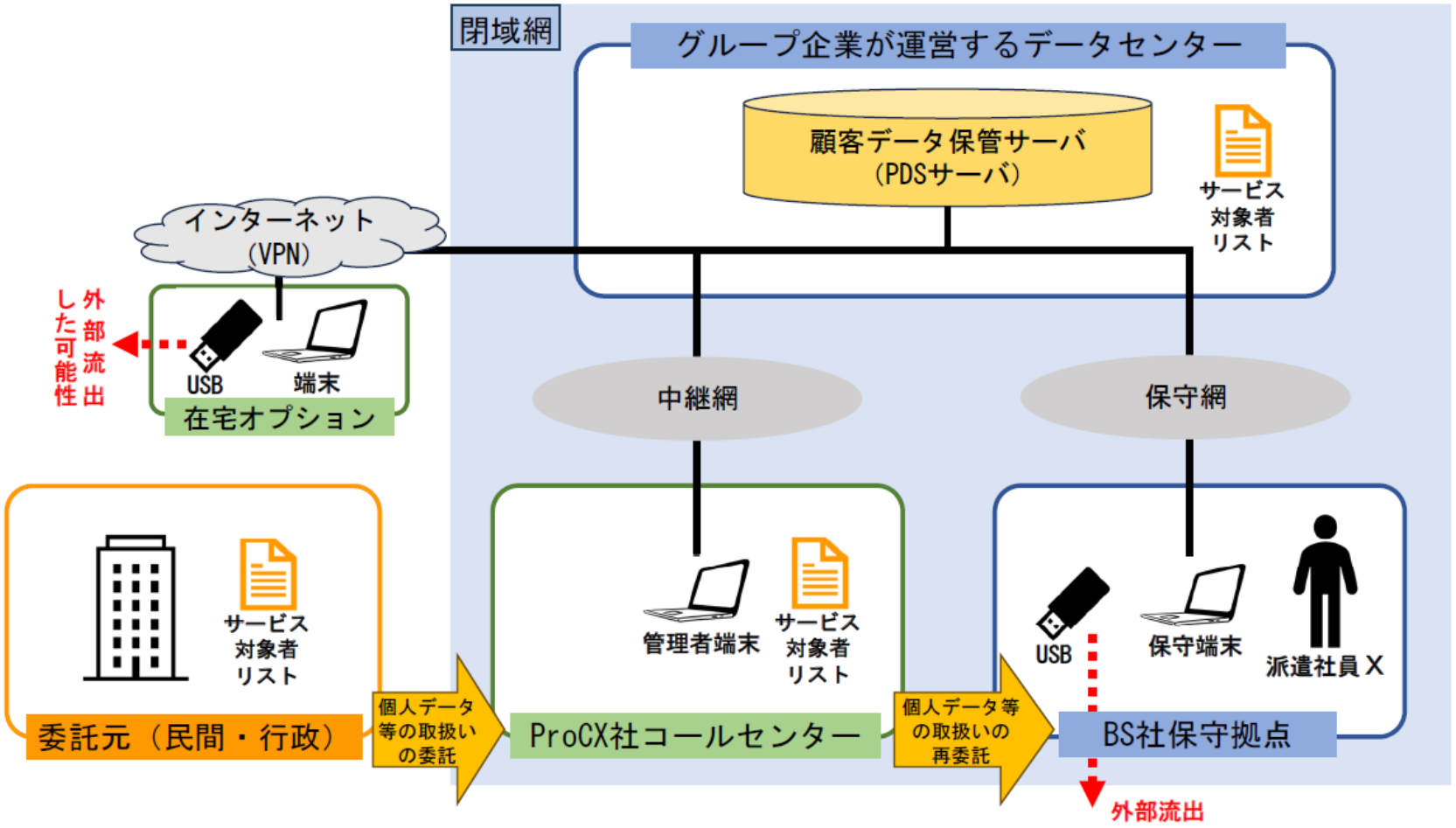
サイバーセキュリティ関係法令 Q&Aハンドブック Ver2.0　Q64　ランサムウェア対応　参照

・身代金を支払っても、データが復元されるかはわからない。
・再被害に遭う可能性がある。

2．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（2）NTT西日本子会社不正持出し事件

資料１－３

委託元、株式会社NTTマーケティングアクトProCX（ProCX社）
及びNTTビジネスソリューションズ株式会社（BS社）関係図



※サービス対象者リストは、管理者端末から顧客データ保管サーバにアップロードして格納される。

出典：個人情報保護委員会：株式会社NTTマーケティングアクトProCX等における 不正持ち出し事案に対する個人情報の保護に関する法律に基づく行政上の対応について　https://www.ppc.go.jp/files/pdf/240911_houdou.pdf

（2）時系列

2013年7月～	BSに派遣されていた元派遣社員によるお客さま情報の不正持ち出し（2023年2月頃まで）
2022年4月	クライアントさま一社からProCXに対し、「自社のお客さま情報が流出している可能性があるので、社内調査を実施いただきたい」旨の依頼を受け、ProCX及びBSにおいて調査を実施 当時の不適切な調査により、漏えいに関する事実を把握することができず、流出の問題がない旨、当該クライアントさまへご報告 （以降、当時の不適切な調査を**「過去調査」**と記載）
2023年7月13日	元派遣社員の勤務先（BS拠点）に対し、警察が捜査を実施
10月17日	ProCX、BS「クライアントさまのお客さま情報の流出について」公表
	NTT西日本 「当社のお客さま情報の流出について」公表
12月19日	ProCX、BS「クライアントさまのお客さま情報の流出について」続報公表 （クライアントさまへの紐づけ作業の結果）
2024年1月24日	（個人情報保護委員会）ProCX、BSに対する勧告および指導
1月31日	BSに派遣されていた元派遣社員の逮捕 （2024年2月21日起訴）
2月 9日	（総務省）NTT西日本に対する行政指導
2月29日	ProCX、BS 個人情報保護委員会の勧告に対する報告

出典：お客さま情報の不正持ち出しを踏まえたNTT西日本グループの情報セキュリティ強化に向けた取組みについて
2024年2月29日 西日本電信電話株式会社
株式会社ＮＴＴマーケティングアクトＰｒｏＣＸ、ＮＴＴビジネスソリューションズ株式会社

NTT西日本グループ全体の再発防止の取組み

- 抽出された課題への対処に向けて、セキュリティのフレームワーク(NIST CSF※1、3ラインモデル※2)に基づき、NTT西日本グループ全体で以下４点を再発防止の柱として取組む
- これらの実施にあたって、約１００億円規模の予算を割り付けるとともに、約１００名規模の新たな推進組織を設立し、情報セキュリティ強化に取組む

※1：米国国立標準研究所（National Institute of Standards and Technology, NIST）が策定したサイバーセキュリティに関する世界標準的なフレームワーク
※2：内部監査人協会(The Institute of Internal Auditors, IIA)が提唱している監査モデル

出典：お客さま情報の不正持ち出しを踏まえたNTT西日本グループの情報セキュリティ強化に向けた取組みについて
2024年2月29日　西日本電信電話株式会社、株式会社ＮＴＴマーケティングアクトＰｒｏＣＸ、
ＮＴＴビジネスソリューションズ株式会社

ProCX 再発防止の取組み

➢ **NTT西日本グループ全体の再発防止内容を踏まえてProCXの再発防止策を講じることで、クライアントさまに安心・信頼をおいていただけるコールセンタ業務の適切な運営の実現に向け取組む**

クライアントさま

業務委託

ProCX

リスクマネジメント

NTT西日本グループの取組みに即した本格対処を実施

- **（1）リスクの視える化**
- **（2）リスク箇所の最小化**

　業務毎のリスクの洗い出しによる頻度／影響度を加味した業務フローの策定と定期的なアップデート

- **（3）点検の徹底**　業務実態に合わせた点検内容の具体化と点検基準の明確化
- **監視の高度化**　セキュリティ管理システムの導入による全社員・全端末の不審なふるまいの検知

体制強化・意識改革

- ✓ **「顧客起点」と「情報セキュリティ」が経営の最重要課題であることをトップ自らコミット**
- ✓ **コールセンタ運営の各役割（ スーパーバイザー／オペレーター等）を踏まえた研修**の実施
- ✓ NTT西日本と連携した情報セキュリティ推進体制の強化

委託先管理

- ✓ **個人情報の取扱いを再委託する場合における委託先の管理監督の徹底** ※
  委託先の管理監督に関わる実務フローの確立（安全管理措置内容等についての契約内容の明確化、定期点検の実施徹底）

※ 個人データの取扱いを再委託する場合

出典：お客さま情報の不正持ち出しを踏まえたNTT西日本グループの情報セキュリティ強化に向けた取組みについて
2024年2月29日　西日本電信電話株式会社、株式会社ＮＴＴマーケティングアクトＰｒｏＣＸ、
ＮＴＴビジネスソリューションズ株式会社

BS 再発防止の取組み

➢ **サービスを提供する事業者として、NTT西日本と連携して、情報セキュリティの取組みを強化するとともに、改めて、事業を支える社員一人一人に顧客起点のマインドを浸透させ、顧客の立場に立った組織となるため、経営トップ自ら率先して以下の取組みを進める**

これまで実施してきたこと	①**当該システムについて、暫定対処を完了** ②お客さま情報を保有する**全システムの総点検**を実施。発見された**不備箇所について、暫定対処を完了**（運用対処を含む）

本格対処として実施すること

技術的な対処	**（1）リスクの視える化** **（2）リスク箇所の最小化** **（3）監視の高度化・点検の徹底** **NTT西日本グループの取組みに即した本格対処を実施**
体制強化・教育	✓ 西日本と連携した**情報セキュリティ推進体制の強化** ✓ 顧客情報を扱う全社員に対し、**実運用を踏まえたセキュリティリスクに関する集中教育**実施 ✓ 顧客情報を扱うシステム従事者の**長期配置見直し**
意識改革	✓ **「顧客起点」と「情報セキュリティ」が経営の最重要課題であることをトップ自らコミット** ・日常のマネジメントにおける社員とのコミュニケーションの中で浸透・定着化 ✓ 心理的安全性が高く、**なんでも言い合える組織風土への変革推進** ・タウンホールミーティングでの対話を通じた課題把握と改革策の展開 ・社員が問題であると思うことを吸い上げる仕組み　等

出典：お客さま情報の不正持ち出しを踏まえたNTT西日本グループの情報セキュリティ強化に向けた取組みについて
2024年2月29日　西日本電信電話株式会社、株式会社ＮＴＴマーケティングアクトＰｒｏＣＸ、
ＮＴＴビジネスソリューションズ株式会社

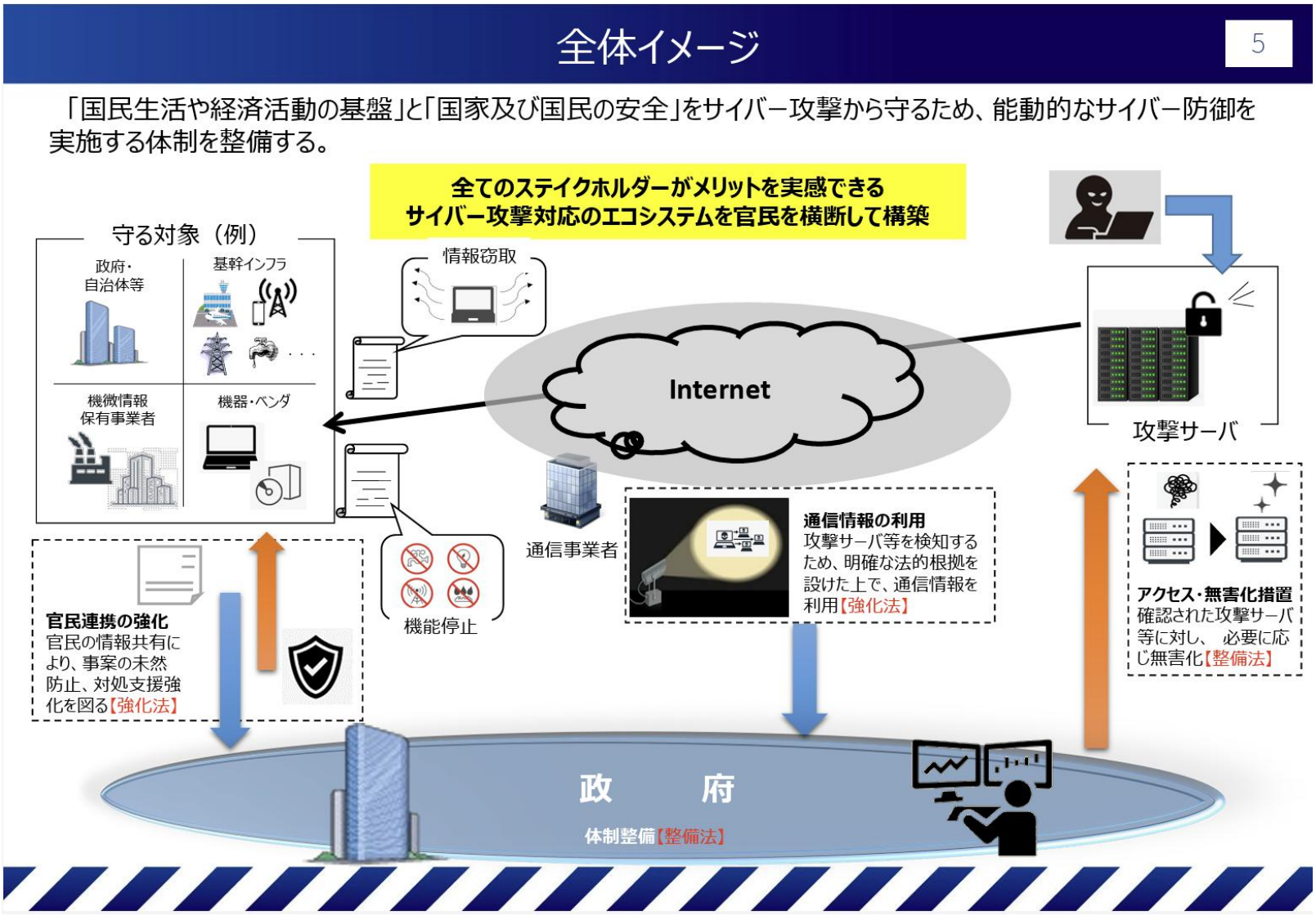
プログラム

1．プライバシー保護とサイバーセキュリティの関係
（1）最近の動向
（2）プライバシー保護とは
（3）サイバーセキュリティとは
（4）プライバシー保護とサイバーセキュリティの相違点

2．プライバシー保護とサイバーセキュリティが交錯する事案の紹介
（1）「社労夢」ランサムウエア攻撃事件
（2）NTT西日本子会社不正持出し事件

3．サイバー対処能力強化法の概要

3．サイバー対処能力強化法の概要



出典：令和７年９月内閣官房国家サイバー統括室
サイバー対処能力強化法及び同整備法について
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

3．サイバー対処能力強化法の概要

法の全体像

6

- 国家安全保障戦略（令和4年12月16日閣議決定）では、サイバー安全保障分野で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、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置**等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和6年6月7日から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を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

P7　総　則
- 目的規定、基本方針等（第１章）

P8　官民連携（強化法）
- 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（第２章）
  - インシデント報告
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

P11　通信情報の利用（強化法）
- 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（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

P16 → 分析情報・脆弱性情報の提供等 ← （第８章）

P18　アクセス・無害化措置（整備法）
- 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）

P21　組織・体制整備等（整備法）
- 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　P24　公布の日（令和7年5月23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　等

出典：令和７年９月内閣官房国家サイバー統括室
サイバー対処能力強化法及び同整備法について
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

3．サイバー対処能力強化法の概要

重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針（案）

パブリック・コメント
重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針（案）に関する意見の募集について
https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000301883

プログラム

ご清聴いただきまして、ありがとうございました。