不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点

令和８年１月16日

個人情報保護法サイバーセキュリティ連絡会

目次

はじめに（１／４）

- 個人情報保護委員会は、令和６年12月から、関係省庁等と「個人情報保護法サイバーセキュリティ連絡会」を開催し、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」といいます。）上求められる各種の安全管理措置として講じ得る方策等について検討・把握するとともに、個人情報取扱事業者や行政機関等に対する効果的な普及啓発の在り方等を検討しています。

【個人情報保護法サイバーセキュリティ連絡会　参加機関】

・内閣官房　国家サイバー統括室（ＮＣＯ）

・警察庁サイバー警察局

・独立行政法人情報処理推進機構（ＩＰＡ）

・国立研究開発法人情報通信研究機構（ＮＩＣＴ）

・一般社団法人ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）

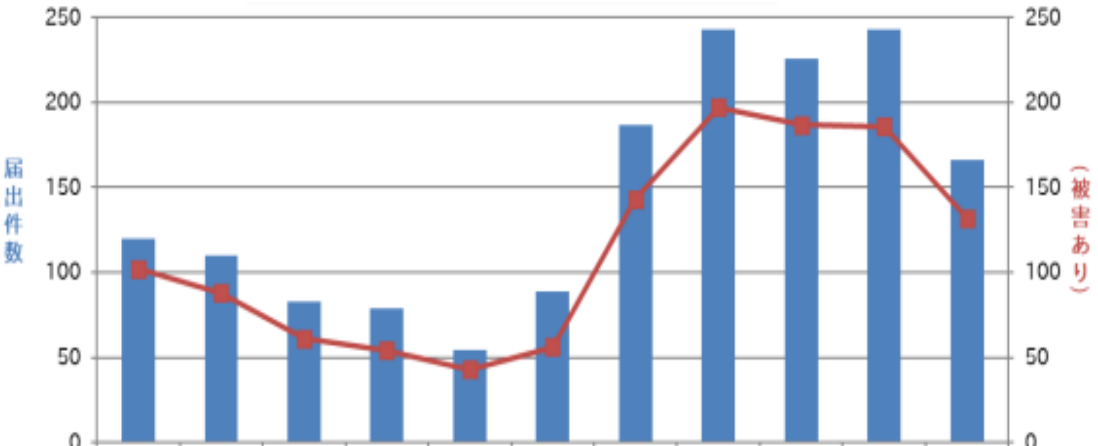
・個人情報保護委員会事務局

- 本資料は、同連絡会における取組の一環として、不正アクセス被害への対応とフォレンジック調査に関する議論を踏まえ、参考資料として取りまとめたものです。

はじめに（２／４）

- 不正アクセス被害は近年多発しており、個人情報保護委員会が受け付ける不正アクセスによる漏えい等報告件数も増加しています。

ＩＰＡへのコンピュータ不正アクセス届出件数の推移



	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	2022年	2023年	2024年
届出件数	120	110	83	79	54	89	187	243	226	243	166
(内:被害あり)	102	88	61	54	43	56	143	197	187	186	132

【ＩＰＡ「コンピュータウイルス・不正アクセスの届出状況　［2024年（1月～12月）］」（令和７年２月26日）Ｐ７】

個人情報取扱事業者及び行政機関等からの不正アクセスによる漏えい等報告件数

	報告件数（個人情報保護委員会直接受付分）	うち不正アクセスによるものの報告件数
令和４年度	4,331件	370件
令和５年度	8,234件	472件
令和６年度※	16,149件	4,024件

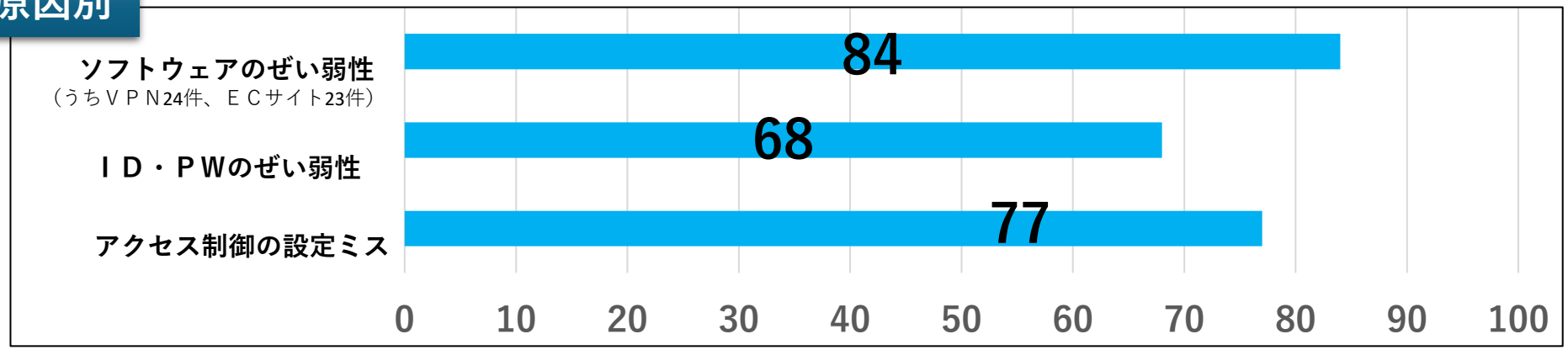
【個人情報保護委員会作成の「令和４年度年次報告」、「令和５年度年次報告」及び「令和６年度年次報告」を元に作成しました。】

（※）上記の件数には、ＳａａＳを提供する事業者のサーバが不正アクセスを受けたことにより、同社ＳａａＳを利用していた多数の個人情報取扱事業者に影響が及んだ事案に係る漏えい等報告2,745件が含まれています。

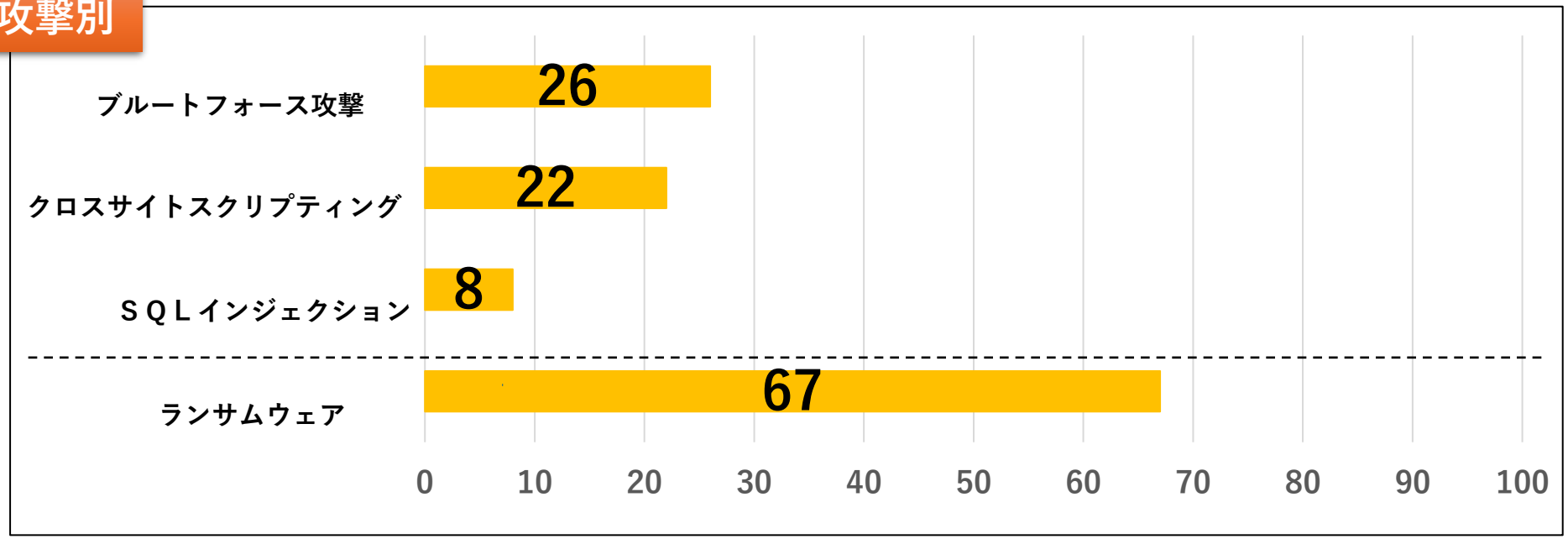
参考１：令和６年度指導･助言案件の要因分析※1※2

（全体件数　198）

原因別



攻撃別



（※1）個人情報保護委員会における民間事業者に対する指導案件のうち、不正アクセスが原因となっている事案（198件）を抽出して分析したもの。なお、原因別･攻撃別の項目は、主なものに限り記載しています。

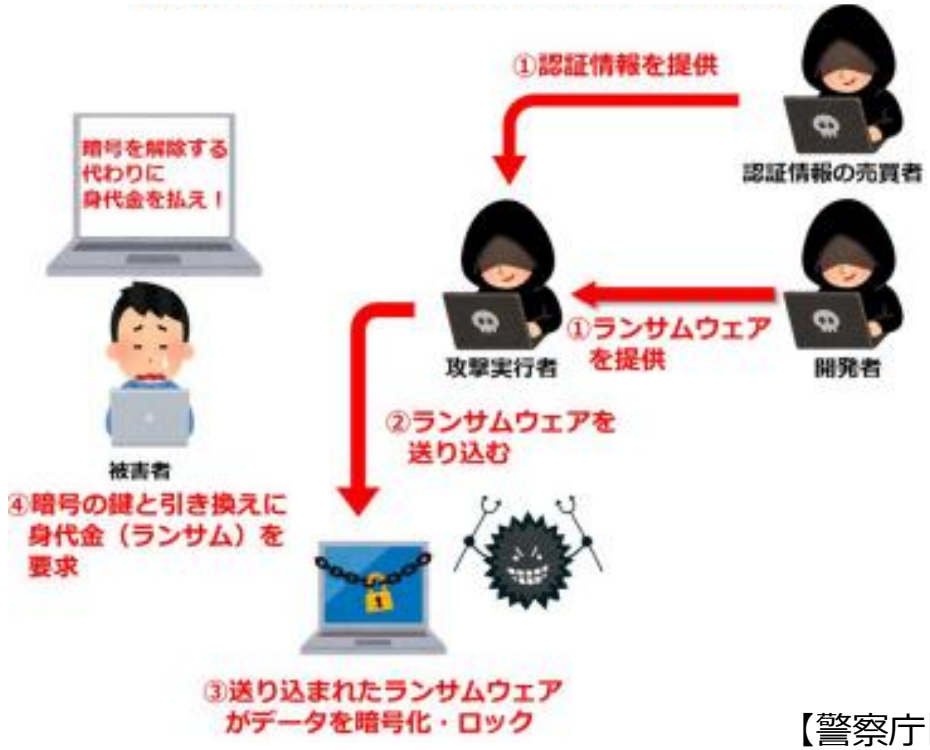
（※2）一つの事態で複数の原因別･攻撃別の項目に該当する場合には全てに計上しているため、原因別･攻撃別の各項目の件数の合計は、全体件数を超えることがあります。

参考２：ランサムウェアとは

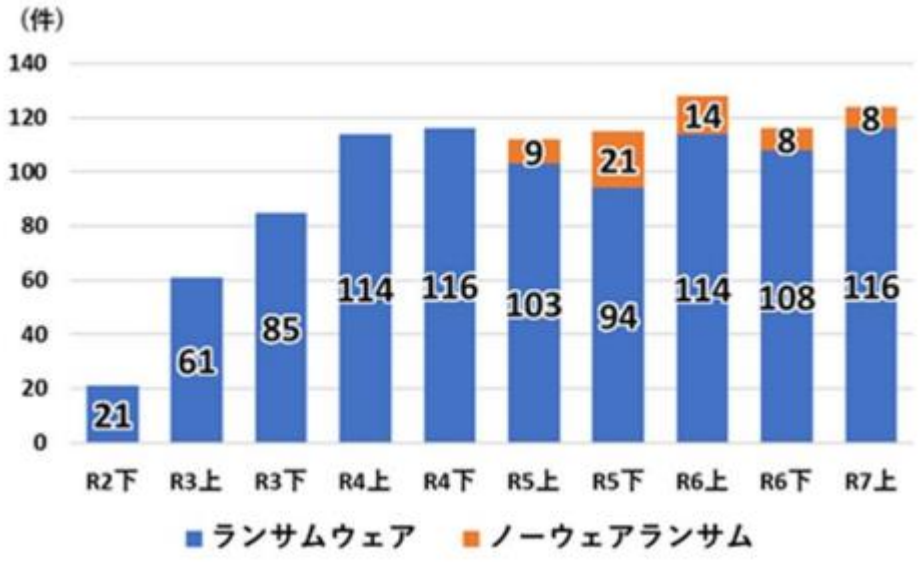
- **ランサムウェア**とは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラムです※。

（※）近時では、暗号化することなくデータを窃取した上で対価を要求する**ノーウェアランサム**という手口も確認されています。

ランサムウェア攻撃の流れ



警察庁の把握するランサムウェア被害の報告件数



【警察庁「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和７年９月） P８】

はじめに（３／４）

- 個人情報取扱事業者や行政機関等においては不正アクセス被害を防止するために**平時から組織として備えておくことが重要**ですが、サイバー攻撃が巧妙化・多様化する中で、あらかじめ一定の備えをしておいたとしても**不正アクセスを完全に防ぐことは困難**になってきています。
- 万一不正アクセス被害を受けた際には、**必要な調査**を行い、**不正アクセスの原因・被害範囲を把握**して適切に対応した上で、**再発防止策**を講ずる必要があります。
- 不正アクセスの発生原因・被害範囲の把握や効果的な再発防止策の実施のために必要とされる調査について、自ら実施することが困難である場合には、**専門の調査会社にフォレンジック調査を依頼しながら対応することも有用**であり、実際に活用される事案も多く見受けられます。
- 調査会社にフォレンジック調査を依頼することにより、以下のようなメリットが期待できます。
  - ①　不正アクセスの発生原因・被害範囲が明らかになり、**効果的な再発防止策の実施**に繋がります。
  - ②　専門家による客観的な分析が記載された調査報告書を活用することで、内外の関係者（経営層（幹部）、取引先、顧客、監督官庁等）との**コミュニケーションが円滑**になります。
  - ③　証拠となり得る情報（ログ等）を収集・保全し、**訴訟手続に備える**ことができます。

はじめに（４／４）

- 一方で、**フォレンジック調査の成否は、組織における平時からの備えや、初期対応の内容により大きく左右されます。**そのため、平時の備えが不十分であったり、初期対応を誤った場合には、期待されるメリットが得られなくなるおそれがあります。
- 本資料は、このようなフォレンジック調査の性質を踏まえ、**平時から備えておくと効果的な事項**、**不正アクセス被害を受けた場合に注意すべき事項**、及び**フォレンジック調査の活用に関する事項**を**参考資料**として整理したものです※1※2

（※1）本資料においては、「フォレンジック調査」という語句を、**発生した不正アクセスの侵入原因・被害範囲を特定するために実施される詳細な調査活動**を指すものとして用います。本資料は不正アクセス対策や、いわゆるインシデント対応に関する推奨事項を網羅的に整理するものではありません。

（※2）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（以下「サイバー対処能力強化法」といいます。）、個人情報保護法等に基づく報告を提出する場面において、**専門の調査会社によるフォレンジック調査が義務付けられているものではありません。**

１　平時から備えるべき事項

１（１）平時からの備えの重要性

- 特に個人データ及び保有個人情報（以下合わせて「個人データ等」といいます。）を守る上では、**個人情報保護法第23条及び第66条が定める安全管理措置**が適切に実施されていることが前提となります。不正アクセス被害に円滑に対応する上では、以下が特に重要です。

① **情報資産の把握**：各種サーバ、ＰＣ、個人データ等を含む各種情報等、守るべき情報資産がどの程度存在し、それがどのように管理されているのかを把握しておくことが重要です。

関連する安全管理措置の項目：ガイドライン（通則編）※1：10-3 組織的安全管理措置⑶ 個人データの取扱状況を確認する手段の整備

事務対応ガイド※2：4-8-5⑼ 保有個人情報の取扱状況の記録

② **ログの保管**：特にフォレンジック調査を依頼する場合には、適切な範囲のログが保管されていることが必要不可欠です。

関連する安全管理措置の項目：ガイドライン（通則編）※1：10-３ 組織的安全管理措置⑵ 個人データの取扱いに係る規律に従った運用

10-６ 技術的安全管理措置⑶ 外部からの不正アクセス等の防止

事務対応ガイド※2：4-8-6⑶及び⑷ アクセス記録

③ **不正アクセス発生時の対応フローの整理**：組織内外の関係者に、適時に必要な情報が連携されるような対応フローを整理することが重要です。

関連する安全管理措置の項目：ガイドライン（通則編）※1：10-3 組織的安全管理措置⑷ 漏えい等事案に対応する体制の整備

事務対応ガイド※2：4-8-11⑴から⑸ 事案の報告及び再発防止措置、同⑹ 法に基づく報告及び通知、同⑺ 公表等

（※1）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）を指します。以下同じです。
（※2）個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）を指します。

１（２）情報資産の把握

- **日々取り扱っている情報や、情報を取り扱うネットワーク、システムの全体像を適切に把握すること**は、守るべき情報資産の範囲・状態を明らかにする上で重要です。これにより、平時の管理漏れを防ぎ、不正アクセス発生時には、初期対応や調査会社との連携をスムーズに行うことが期待できます。

- 例えば、Ｐ12のような**情報資産管理台帳等**や、Ｐ13のような**ネットワーク構成図**を作成・更新することが有効です。

例１：情報資産管理台帳・データマッピング表

- 情報資産をリスト化することは、不正アクセス発生時の**影響範囲の特定**に役立ちます。リスト化に当たっては、**個々の情報資産を識別・特定可能なＩＤ・名称**を設定し、取扱状況を把握しやすくなるようにしましょう。**個人情報の保管の有無を明記**することで、不正アクセス発生時に、個人情報への影響範囲の特定も容易になります。
- 情報資産のリスト化に当たっては、**ネットワーク機器（ＶＰＮ装置、ルータ等）**も漏れなく含め、平時の情報資産管理の対象から漏らさないように注意しましょう。

【参考例】

① 独立行政法人情報処理推進機構（ＩＰＡ）作成の情報資産管理台帳※1

② 個人情報保護委員会事務局作成のデータマッピング表※2

【情報資産管理台帳（①抜粋）】

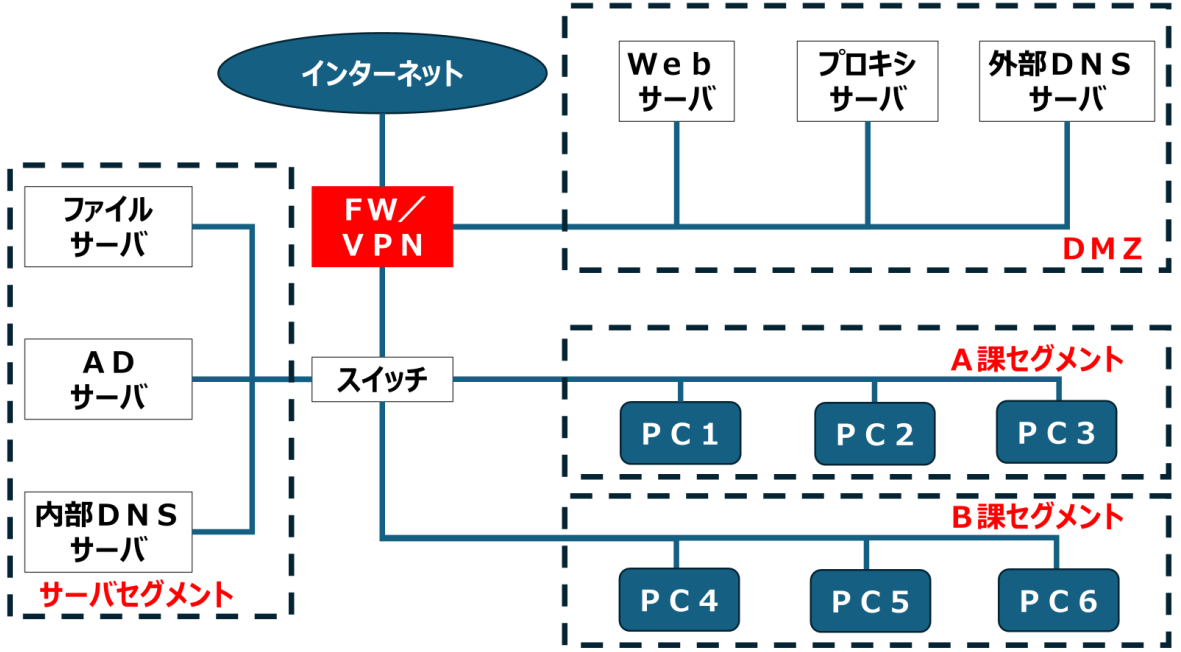
業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類		
						個人情報	要配慮個人情報	特定個人情報

（※1）https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx
（※2）https://www.ppc.go.jp/personalinfo/independent_effort/

例２：ネットワーク構成図

- ネットワーク構成図は、主に、**物理構成図**※1と**論理構成図**※2に分けられます。
- 不正アクセスへの対応との関係では、**簡易な構成図**であっても、漏えい等発生の**影響範囲の特定**に役立ちます。
- ランサムウェア攻撃の事案では、**ＶＰＮ装置**から侵入される事案が多く報告されています。

【簡易な構成図の例】



（※1）組織内に存在するＰＣ、各種サーバ、ネットワーク機器等の配置・物理的な接続関係を明らかにするために作成される構成図を指し、各種機器の設置場所や配線状態等が記載されます。

（※2）組織内ネットワーク内の通信経路やネットワークの目に見えない（論理的な）接続関係を明らかにするために作成される構成図を指し、ＩＰアドレスや各種サーバの役割等が記載されます。

１（３）ログの保管（１／２）

- フォレンジック調査を効果的に行うためには、**適切な範囲のログの保管が不可欠**です。ログは、自身が操作するＰＣ上のみではなく、運用する各種サーバ、通信経路上に設置されているネットワーク機器及びクラウドサービス上にも存在します。
- 不正アクセスは長期間に及ぶこともあるため、調査に必要となるログについては**少なくとも１年程度保管することが望ましい**です※。

（※）**法令上保管が許容される期間を超えてログを保管することを推奨するものではありません。**特に、電気通信事業者においては、通信の秘密との関係で通信履歴について慎重な取扱いが求められるため、関連するガイドラインを確認の上で適切に通信履歴を保管してください。

「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（令和４年個人情報保護委員会・総務省告示第４号（最終改正令和７年個人情報保護委員会・総務省告示第２号））の解説」（令和４年３月（令和７年12月更新））Ｐ202及びＰ203

「いったん記録した通信履歴は、記録目的の達成に必要最小限の範囲内で保存期間を設定し、保存期間が経過したときは速やかに通信履歴を消去（通信の秘密に該当する情報を消去することに加え、該当しない部分について個人情報の本人が識別できなくすることを含む。）しなければならない。また、保存期間を設定していない場合であっても、記録目的を達成後は速やかに消去しなければならない。

保存期間については、提供するサービスの種類、課金方法等により電気通信事業者ごとに（※1）、また通信履歴の種類ごとに（※2）異なり得るが、業務の遂行上の必要性や保存を行った場合の影響、社会環境の変化（※3）等も勘案し、その趣旨を没却しないように限定的に設定すべきである。

（中略）

（※2）例えば、ＡＰが保有する通信履歴のうち、インターネット接続サービスにおける接続認証ログ（利用者を認証し、インターネット接続に必要となるＩＰアドレスを割り当てた記録）の保存については、利用者からの契約、利用状況等に関する問合せへの対応やセキュリティ対策への利用など業務上の必要性が高いと考えられる一方、利用者の表現行為やプライバシーへの関わりは比較的小さいと考えられることから、電気通信事業者がこれらの業務の遂行に必要とする場合、一般に６か月程度の保存は認められ、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など、より長期の保存をする業務上の必要性がある場合には、１年程度保存することも許容される。」

１（３）ログの保管（２／２）

- ログ管理サーバやＳＩＥＭを導入し、**ログを一元管理することも有効**です。

- ログを効率的に保管する上では、その全てを、いつでもすぐに利用できる状態に置いておく必要はなく、**保管期間・用途に応じて、古いログを外部記憶媒体（例：ＵＳＢメモリ、外付けＨＤＤ）・クラウドストレージ等に保管する**ことも有効です。

【保管対象となり得るログの例】

ネットワーク関連のログ	システム・サーバ関連のログ	アプリケーション関連のログ
ＦＷ（ファイアウォール）ログ、ＶＰＮ接続ログ、ＩＤＳ／ＩＰＳログ	ＯＳのイベントログ（Windowsイベントログ、Linux /var/log/配下のログ）、認証ログ（ＡＤサーバのログ、ＲＡＤＩＵＳサーバのログ）、データベースログ（接続ログ、クエリログ）、Ｗｅｂサーバログ、クラウドサービスのログ、プロキシサーバログ	各種アプリケーション上のログ（ユーザーの操作ログ、アプリケーションの動作ログ等）

１（３）に関する用語説明

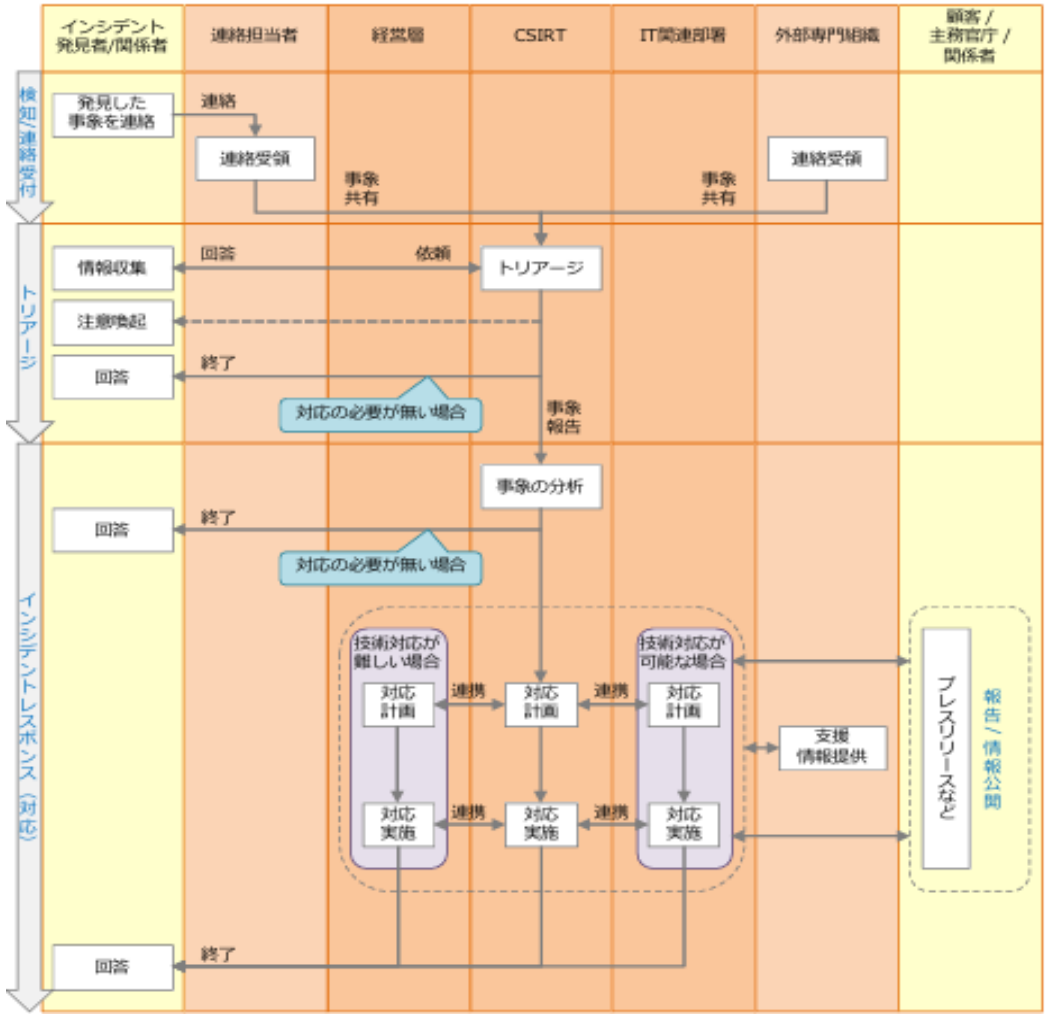
用語	説明
ＩＤＳ	Intrusion Detection Systemの略。通信経路を監視し、ネットワーク上の不審な通信を検知するシステム。
ＩＰＳ	Intrusion Prevention Systemの略。ＩＤＳの機能に加え、検知した不審な通信を遮断する機能を持つシステム。
ＲＡＤＩＵＳ	Remote Authentication Dial-In User Serviceの略。ネットワーク接続の際に用いられるユーザ認証プロトコル。ＲＡＤＩＵＳを用いて認証サービスを提供するサーバを、一般的にＲＡＤＩＵＳサーバと呼ぶ。
ＳＩＥＭ	Security Information and Event Managementの略。ファイアウォールやＩＤＳ／ＩＰＳ、プロキシサーバ等から出力されるログやデータを一元的に集約し、それらを分析することでネットワーク監視・サイバー攻撃等を検知することを目的とする仕組み。
/var/log/	Linux（ＯＳの一種）環境におけるログの保管場所。
クエリログ	データベースを操作するために入力されるコマンド（クエリ）のログ。
プロキシサーバ	インターネットへのアクセスをＰＣに代わって（代理して）行うサーバ。

１（４）不正アクセス発生時の対応フローの整理（１／２）

- 組織内外の関係者に適時に情報が連携されるような対応フローを整理することが重要です。

【内部関係者との情報連携】

- **不正アクセスの端緒を認識した際のエスカレーション先（責任者・担当部署）**などを整理した対応フローを作成・周知し、早期に情報を共有することが重要です。
- エスカレーション先として、情報セキュリティ問題を専門で扱う**ＣＳＩＲＴ（Computer Security Incident Response Team）**を設置することも有効です。
- 情報システム担当部署のほかに**個人情報保護の担当部署が別に存在する場合には、当該部署にも早期に情報を共有し**、漏えい等報告の要否を早期に判断できるようにしましょう。



【対応フローの例】
ＪＰＣＥＲＴ／ＣＣ「インシデントハンドリングマニュアル」（令和３年11月30日）Ｐ２より抜粋

１（４）不正アクセス発生時の対応フローの整理（２／２）

【外部関係者との情報連携】

- **警察組織**：不正アクセス被害に遭った際は、**速やかに**通報・相談することが望ましいです。
- **調査会社・専門機関**※1：自組織での対応が困難である場合や、対応について相談したい場合には、**速やかに**連絡することが望ましいです。その際、マルウェア・不正な通信先などの攻撃技術情報等を共有することが有効です※2 。
- **取引先・顧客等**：法令等に基づき本人通知・公表が必要となる場合には、定められた内容につき、適時に行う必要があります。例えば、個人情報保護法第26条第２項及び第68条第２項に基づく本人通知は、**当該事態の状況に応じて速やかに**行う必要があります。
- **監督官庁**：法令等に基づき、定められた内容を、適時に報告等する必要があります。例えば、個人情報保護法第26条第１項及び第68条第１項に基づく漏えい等報告（速報）は、**報告対象事態を知った後、速やかに（概ね３～5日以内）**行う必要があります※3 。

（※1）国の法令／制度等に基づき、非営利でインシデント対応相談や分析、情報共有活動を行う組織です。
例）ＪＰＣＥＲＴ／ＣＣ、ＩＰＡ

（※2）特にＩＳＡＣ（Information Sharing and Analysis Center）等の情報共有活動を行う組織に攻撃技術情報等を共有することで、参考となる情報が得られる可能性があります。詳細は、サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月８日）も御参照ください。

（※3）政府全体の取組として、「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」に基づき、報告様式の一元化・窓口一元化等に向けた取組が進められています。

参考３：調査会社・専門機関間の情報連携について

- 現在、サイバー攻撃の全容解明やサイバー攻撃による被害拡大の防止の観点から、**調査会社・専門機関間でのサイバー攻撃に関する情報共有の促進に向けた取組**が行われています※。この取組は、被害組織においても、サイバー攻撃の全体像の解明に資する等のメリットがあります。なお、この取組との関係で、調査会社との契約書類に、以下のような条項が含まれることがあります。

（※）詳細は、サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局「攻撃技術情報の取扱い・活用手引き」（令和６年３月11日）を御参照ください。

【調査会社・専門機関間でのサイバー攻撃に関する情報共有の促進の観点から追加される条項例】

※甲：被害組織、乙：調査会社

1．乙は、本サービスの遂行過程において、乙の知見により得られたサイバー攻撃に関する通信先、マルウェア、脆弱性その他の情報（以下この条において「攻撃技術情報」という。）について、甲の被害に対する迅速な調査、被害拡大の防止及び甲乙以外の組織に対するサイバー攻撃の未然防止を目的としてこれを保有又は利用し、また、甲を識別及び特定できないように加工した攻撃技術情報（以下この条において「攻撃技術情報」及び「甲を識別及び特定できないように加工した攻撃技術情報」を合わせて「攻撃技術情報等」という。）を作成、保有、利用又はサイバーセキュリティに関する専門組織に対して開示することができる。

（以下略）

参考４：「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」に基づく報告様式一元化・窓口一元化

「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和７年５月28日関係省庁申合せ。同年9月25日一部改正。）により、今後、以下の運用が予定されています。

（１） ＤＤｏＳ攻撃事案・ランサムウェア事案に係る報告様式の一元化

個人情報保護法第26条第１項の規定による個人データの漏えい等に係る報告等、都道府県警察への相談その他の共通様式に記載の手続に関する官公署への報告等に際して、被害組織が「ＤＤｏＳ攻撃事案共通様式」又は「ランサムウェア事案共通様式」を用い、又は別途法令等で定める様式に添付する形で報告等を行うことを可能とする。具体的な提出先及び提出方法については、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とする。

その際、内閣官房国家サイバー統括室において国内で発生しているこれら事案の情報集約を行うため、被害報告を行う者の同意がある場合は、各様式に基づいて報告を受けた官公署は、当該内容を内閣官房国家サイバー統括室に共有するものとする。

➡令和７年10月１日より運用開始

また、サイバー対処能力強化法第５条の施行に併せ、官民連携基盤の整備により、共通様式により報告が行われる場合における窓口を一元化するよう所要の調整を進める。

➡サイバー対処能力強化法公布の日から1年６月を超えない範囲内で政令で定める日から施行

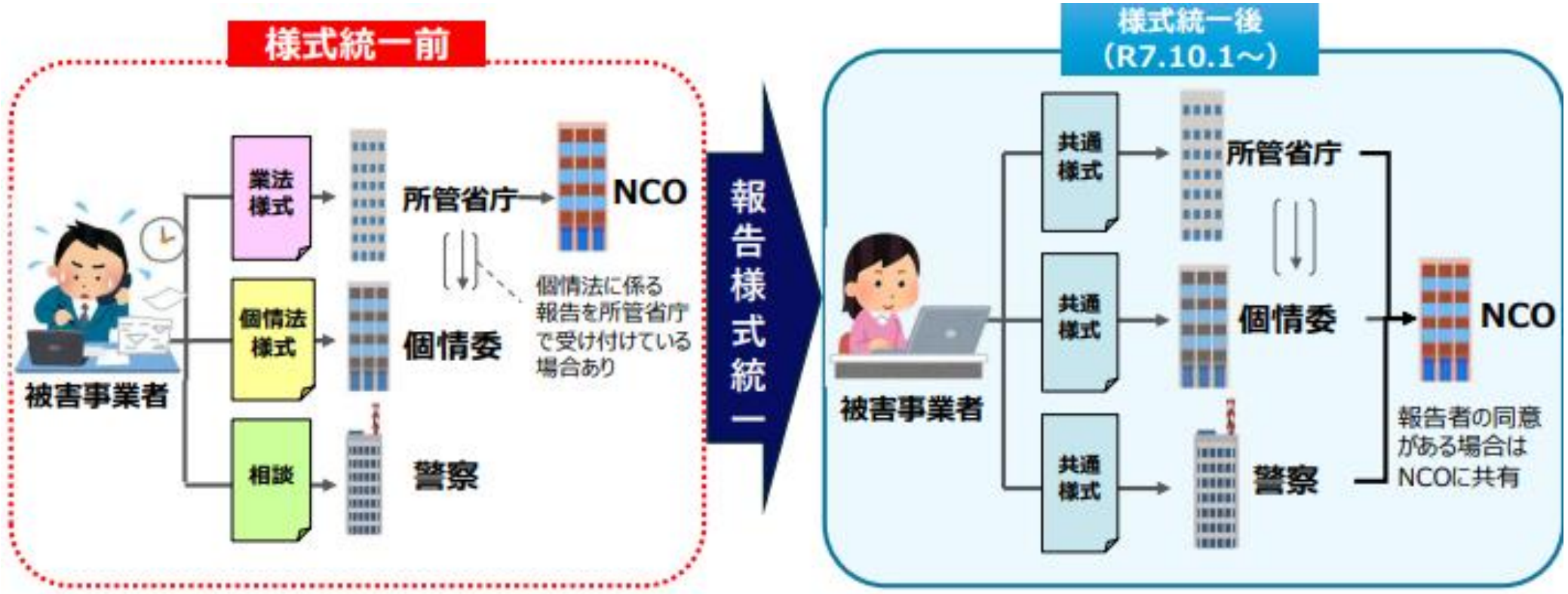
（２）サイバー対処能力強化法に基づく報告

特別社会基盤事業者は、特定侵害事象等の発生を認知した場合、サイバー対処能力強化法第５条の規定に基づき、特別社会基盤事業所管大臣及び内閣総理大臣に報告しなければならないとされているところ、当該規定に基づく報告及び（１）に掲げる報告等について、当該規定の施行に併せ、官公署への報告等に際して利用できる共通様式を整備し、さらに官民連携基盤の整備により、これらの報告の窓口を一元化するよう所要の調整を進める。

➡サイバー対処能力強化法公布の日から1年６月を超えない範囲内で政令で定める日から施行

参考５：サイバー攻撃時の報告様式の統一について(ＤＤｏＳ攻撃、ランサムウェア事案)※

サイバー攻撃の被害組織の初動対応段階における負担軽減のため、**特に件数の多いＤＤｏＳ攻撃・ランサムウェア事案について**、政府関係機関申合せにより関係政府機関に対する報告様式を統一します。
これにより、**共通様式**を用いて、官公署への報告を行うことが可能となります。（令和7年10月1日～）



（※）https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html

参考６：専門機関等への相談・報告

- 不正アクセスを受けた場合等は、その内容に応じて、以下の機関に相談や報告を行ってください※1。

不正アクセス・マルウェア感染・サイバー攻撃等を受けたとき	ＩＰＡ	サイバーセキュリティ 相談・届出窓口一覧 https://www.ipa.go.jp/security/support/soudan.html
	ＪＰＣＥＲＴ／ＣＣ※2	インシデント対応相談、情報共有依頼、テイクダウン（停止措置）依頼等 https://form.jpcert.or.jp/
	警察庁	サイバー事案に関する通報等のオンライン受付窓口 https://www.npa.go.jp/bureau/cyber/soudan.html
個人データ等の漏えい等又はそのおそれが生じたとき	個人情報保護委員会	漏えい等報告※3 https://www.ppc.go.jp/personalinfo/legal/leakAction/

（※1）上記のほか、所管省庁へのインシデント報告等が必要となる場合があります。
（※2）このほか、ＪＰＣＥＲＴ／ＣＣでは、調査会社向けのインシデント対応に関する相談・情報提供も受け付けています。
https://www.jpcert.or.jp/ir/consult.html
（※3）所定の要件を満たす漏えい等又はそのおそれは、その報告が法律上義務付けられていますので、御注意ください。

２　不正アクセスが発生した際に注意すべき事項

２（１）エスカレーション・被害の封じ込め

【エスカレーション】

- あらかじめ定めた不正アクセス発生時の対応フローに基づき、担当者（担当部署）にエスカレーションしましょう。その際、必要に応じ、経営層（幹部）へ報告することも重要です。

【被害の封じ込め】

- 不正アクセスが発生した際の初期対応としては、早期の**封じ込め対応**が重要です。影響が及んだ可能性がある機器については、被害拡大を防止するため、**速やかにネットワーク隔離**を実施する必要があります。
- 特にランサムウェア攻撃の事案では、「今現在進行形で発生している事案への対応」が必要となるため、スピーディーな対応が求められます。そのため、必要に応じて速やかに**調査会社・専門機関等**に相談し、適切に対応しましょう。

２（２）証拠保全

- 初期対応を誤ると、**ログの消失等により、原因の特定・復旧作業に悪影響が生じ得るため、**適切に**証拠保全**を行うことも重要です。そのため、必要に応じて速やかに**調査会社・専門機関等に相談**し、フォレンジック調査を予定している機器※の取扱いに注意しながら対応しましょう。
- 被害機器の保守等をほかの組織に委託している場合には、**委託先と連携しながら**慎重に対応しましょう。

（※）例えば、ファイル暗号化が実行されたり、通常行われない通信を行ったりしている機器など、不審な兆候が確認された機器が考えられます。

フォレンジック調査を予定している機器に対して 実施してもよい措置	フォレンジック調査を予定している機器に対して 実施してはいけない措置
・ネットワーク隔離（有線／無線接続の切断）	・電源オフ、再起動 ・ウイルススキャン ・初期化、ソフトウェアの更新

２（３）調査会社への依頼内容の明確化

- 調査会社に調査を依頼する場合、その目的に応じて、**何を依頼するのか**を明確に意識する必要があります。
- 調査会社は、**フォレンジック調査**以外にも、ダークウェブモニタリング、（広義の）ぜい弱性診断といったほかの調査サービスや、被害の封じ込め対応といった初期対応サービスを提供していることがあります。
- **事実関係の調査及び原因の究明との関係では、フォレンジック調査が重要です。**
  調査会社に封じ込め対応まで相談・依頼したい場合には、あらかじめその旨を伝えておく必要があります。

【各サービスの主な利用目的】

封じ込め対応	フォレンジック調査	ダークウェブモニタリング	（広義の）ぜい弱性診断
当該不正アクセスの被害拡大を防止すること	**当該不正アクセスについて、侵入原因・被害範囲を特定すること**	ダークウェブ※上に当該不正アクセスに関連して自組織が取り扱う機密情報（個人情報を含む。）が流通していないかを監視すること	（不正アクセスの発生を前提とせず）システム環境に存在するぜい弱性を特定・評価し、対策を講ずること

（※）専用のウェブブラウザ等を利用しないとアクセスできないウェブを指します。

3　フォレンジック調査の活用

３（１）調査会社の選び方

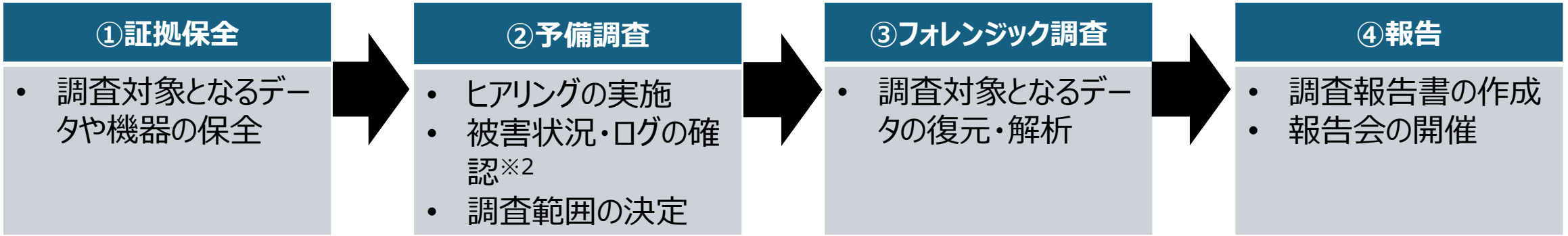
- ＩＰＡでは、経済産業省が策定した「情報セキュリティサービス基準」※1に適合する情報セキュリティサービスの提供状況について調査を行い、基準に適合するサービスを、**情報セキュリティサービス基準適合サービスリスト**※2として公開しています。この中には、**デジタルフォレンジックサービス**も含まれています。

（※1）https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html
（※2）https://www.ipa.go.jp/security/service_list.html

3（2）フォレンジック調査のスケジュール

- フォレンジック調査は、以下のような流れで進むことが一般的ですが、調査報告書の受領までに**1か月以上**要する例が多いです※1。そのため、調査会社に依頼する可能性があるときは、早めに調査会社に相談しましょう。

【フォレンジック調査の流れ】



（※1）調査に要する期間・コストを踏まえ、必ずしも一度に全ての機器のフォレンジック調査を依頼する必要はなく、段階的にフォレンジック調査を依頼することも有効です。
（※2）確認対象となり得るログについては、スライドＰ15を御参照ください。

３（３）調査報告書に盛り込むことが推奨される事項

- 発生した不正アクセスの詳細を適切に理解・評価し、再発防止策を効果的に実施する等の観点から、調査会社にフォレンジック調査を依頼する場合には、以下の事項を含めて調査報告書を作成してもらうように相談しましょう。

ア　フォレンジック調査の前提に関する事項

①調査対象・範囲、②調査範囲の設定根拠、③ログの範囲

イ　フォレンジック調査の結果に関する事項

①調査結果の概要、②不正アクセスの概要、③初期侵入の詳細、

④被害拡大の詳細、⑤情報漏えいの詳細

ウ　再発防止に関する事項

（※）調査報告書における項目分け・記載の様式は問わず、また、以上の項目以外の内容を含めることを妨げるものではありません。

ア①　調査対象・範囲

- 調査対象を明確にするため、**データ保全・調査の対象としたＰＣ・サーバ（物理／仮想）の詳細**や**その業務上の役割**を明らかにすることが重要です。
- 保全の対象となるデータ（イメージファイル、ログファイル等）については、フォレンジック調査のために複製されたデータと複製元のデータの同一性を担保するために**ハッシュ値※（２種類）を取得し、**調査報告書にも記載しておくことが望ましいです。

【記載例】

項目	対象	備考
対象機器・名称	ＡＤＳＶ－０１	ＡＤサーバとして利用
ファイル名	×××××.××	
ファイルサイズ	○○○.○○ＧＢ	
ハッシュ値（ＳＨＡ－２５６）	587cff1ada623bad4cb9fa0ad2837c0d06b1e67b25cf7ef09c00bfcc34244db5	
ハッシュ値（ＳＨＡ－５１２）	・・・	

（※）ハッシュ関数（ＳＨＡ－２５６、ＳＨＡ－５１２等）により、ファイルごとに作成されるランダムの文字列を指します。
異なるデータから同じハッシュ値は生成されにくいことから、ハッシュ値を照合することでデータの同一性を担保することができます。

ア②　調査範囲の設定根拠

- **当該機器を調査対象として選定した理由及び選定しなかった理由**※1など、調査範囲の設定根拠を明らかにすることが重要です。

【設定根拠の例】

例１：簡易調査により、不正アクセスの影響範囲が特定された。

例２：全機器の調査には多大なコストがかかるため、重要と思われる機器に限定した※2。

例３：ログが保存されておらず、調査対象以外に有益な情報が得られなかった※2 。

（※1）例えば、**不正アクセスの展開過程で一定の役割を果たしているが、調査対象としなかった機器**については、その理由を明らかにすることが重要です。

（※2）**不正アクセスによる被害（情報漏えいの可能性を含む。）が発生した範囲が調査範囲に限定されていない場合**は、影響範囲の特定のためにもその旨を明らかにすることが重要です。

ア③　ログの範囲

- **調査報告書の証拠価値は、調査の前提となったログの状況により大きく左右されます。**そのため、調査報告書では、**フォレンジック調査の前提となったログの詳細**を明らかにし、フォレンジック調査を実施する上で**重要性が高いログが保存されない設定となっていたり、不正アクセスの影響により消失等していたりした場合には、その旨**を明らかにすることが重要です。

【記載例】

ログ分類	保存期間	備考
ＶＰＮ接続ログ	2024年●月●日●時●分●秒～ 2025年〇月〇日〇時〇分〇秒	ただし、接続成功ログのみ。
ファイアウォールログ	なし	保存しない設定となっていた。
Windowsイベントログ	不明	暗号化されており、復元不可能だった。／攻撃者により消去されたため、確認できなかった。
・・・	・・・	・・・

イ①　調査結果の概要

- 事案の全体像を把握するため、詳細な調査結果を示す前に**調査結果の概要**を明らかにすることが重要です※。

【記載項目の例】
・初期侵入（標的となるネットワークへの最初の侵入）の概要とその原因
・初期侵入後の活動の概要とその原因
・情報漏えい等の可能性の有無・程度、漏えいが確認されたファイル名一覧

（※）**フォレンジック調査で明らかにならなかった点については、その理由**を明らかにすることが重要です。
また、被害状況から考えられる攻撃手法がある場合は、推測であること及びその根拠を明示した上で説明されていることが望ましいです。

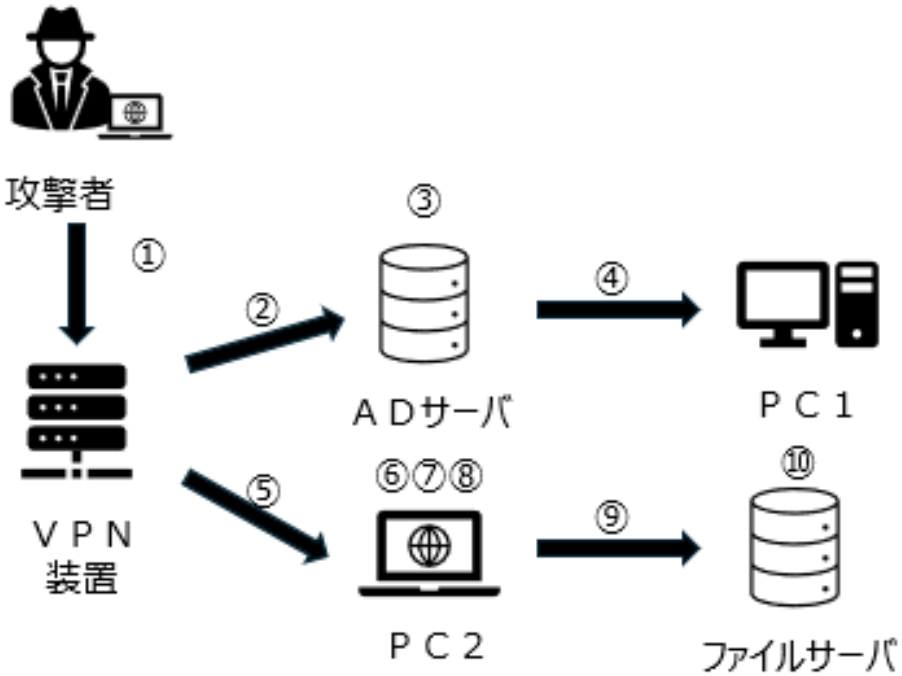
イ②　不正アクセスの概要

- **根拠資料（ログ等）に基づき**、フォレンジック調査の結果確認された事象を**時系列表・不正アクセスの概要図等を用いて整理し、**当該不正アクセスの全体像を明らかにすることが重要です。

【時系列表の例】

Ｎｏ	日時	概要	根拠	攻撃戦略
①	○年○月○日○時○分○秒	ＩＰアドレスＡ（Ａ国）からＶＰＮアカウント「user1」を用いたＶＰＮ接続成功	ＶＰＮ装置のＶＰＮ接続ログ	初期侵入
②	○年○月○日○時×分×秒	ＩＰアドレスＢから、アカウントＢを使用しＡＤサーバへのＲＤＰ※接続	ＡＤサーバのＲＤＰ接続ログ	水平展開
③	・・・	・・・（攻撃終了まで記載）…	・・・	・・・

【概要図の例】



（※）Remote Desktop Protocolの略であり、別の場所にあるＰＣ・サーバを遠隔で操作する際に用いるプロトコルです。

イ③　初期侵入の詳細

- **根拠資料（ログ等※1）に基づき**、初期侵入の経路、手口及びそれが可能となった原因の詳細を明らかにすることが重要です※2。
- 詳細の記載に当たっては、確認された事実関係を列挙するのみではなく、**当該不正アクセスの過程でどのような意味を持つか**も説明されていることが望ましいです。

【初期侵入の例（ランサムウェア攻撃）】

活動概要	具体例	根拠資料
初期侵入（標的ネットワークへの最初の侵入手法）	ＶＰＮ装置経由の不正アクセス（ぜい弱性の悪用、既に漏えいしていた認証情報の悪用、総当たり攻撃等）、ＲＤＰ経由の不正アクセス（既に漏えいしていた認証情報の悪用、総当たり攻撃等）等	各種ログ、被害機器のＯＳバージョン、ポートの設定状況、ダークウェブ上での認証情報流通の有無、パスワードの設定ルール（桁数・文字種別等）等

（※1）スクリーンショット等を活用し、**視覚的に分かりやすく**示されていることが望ましいです。
（※2）**フォレンジック調査で明らかにならなかった点については、その理由**を明らかにすることが重要です。
また、被害状況から考えられる攻撃手法がある場合は、推測であること及びその根拠を明示した上で活動の詳細が説明されていることが望ましいです。

イ④　被害拡大の詳細

- **根拠資料（ログ等※1）に基づき**、初期侵入後の活動の詳細及びそれが可能となった原因の詳細を明らかにすることが重要です※2。
- 詳細の記載に当たっては、確認された事実関係を列挙するのみではなく、**当該不正アクセスの過程でどのような意味を持つか**も説明されていることが望ましいです。

【初期侵入後の活動の例（ランサムウェア攻撃）】

活動概要	具体例	根拠資料
水平展開（侵入済みのシステムから、ほかのシステムへと不正アクセスの範囲を広げる手法）	ＲＤＰ・遠隔実行ツール（PsExec※3等）・脆弱性の悪用によるほかのＰＣ／サーバへの不正アクセス等	各種ログ等
権限昇格（システムを操作する上でより強力な権限を取得する手法）	認証情報収集ツールの実行・ぜい弱性の悪用等による管理者権限の窃取等	各種ログ等

（※1）スクリーンショット等を活用し、**視覚的に分かりやすく**示されていることが望ましいです。
（※2）**フォレンジック調査で明らかにならなかった点については、その理由**を明らかにすることが重要です。
また、被害状況から考えられる攻撃手法がある場合は、推測であること及びその根拠を明示した上で活動の詳細が説明されていることが望ましいです。
（※3）Windows ＰＣに対して遠隔でコマンドを実行するための正規ツールです。

イ⑤　情報漏えいの詳細

- **根拠資料（ログ等※）に基づき、以下の二つの経路**を考慮の上で、不正アクセスによる情報漏えいの可能性の有無・程度を明らかにすることが重要です。特に、攻撃者による**ログの消去活動**が確認された場合、それがどのように影響するかを明らかにすることも重要です。

①外部送信の可能性

【検討視点の例】

- マルウェアの機能や攻撃者の特性(攻撃者グループの過去の行動など)
- ツールの使用履歴(データの窃取や圧縮痕跡の有無)
- ファイル共有サービスへの接続の有無
- 外部との通信状況(通信先や通信量)

②閲覧の可能性

【検討視点の例】

- 実際にファイルにアクセスされた(閲覧された)かどうか
- ファイルが保存されている場所への不正アクセスの有無・設定状況を踏まえた技術的なアクセス可能性の有無
- 悪用されたアカウントの権限(不正アクセスの展開状況も含めて評価)

（※）スクリーンショット等を活用し、**視覚的に分かりやすく**示されていることが望ましいです。

ウ　再発防止に関する事項

- 当該不正アクセスにおいて、**初期侵入や被害拡大を防ぐことができなかった原因を踏まえた再発防止策**を明らかにすることが重要です。その際、**どのような観点から当該再発防止策が有効であるのか、実施の優先度等**が明らかにされていることが望ましいです。
- その他、当該不正アクセスとは直接関わりがない場合であっても、セキュリティ上好ましくない事象が確認された場合には、参考情報としてその改善策が記載されていることが望ましいです。

【記載項目の例】

- 短期的な再発防止策（発生した不正アクセスと結びつく対策のうち、実施の容易性・重要度等の観点から、即時に実施すべきもの）
- 長期的な再発防止策（発生した不正アクセスと結びつく対策のうち、実施の容易性・重要度等の観点から、長期的には実施することが望ましいもの）
- その他好ましい取組（発生した不正アクセスとは結びつかないものの、実施することが望ましいもの）

参考７：フォレンジック調査に伴う個人データの提供等

Q．個人情報データベース等が記録されたサーバが不正アクセス被害を受け、個人データの漏えいのおそれが生じました。フォレンジック調査のために、当該サーバ上のデータのコピーを調査会社に提供したいのですが、本人の同意を得ずに提供しても問題ないでしょうか？要配慮個人情報が含まれている場合はどうですか？

A．個人情報取扱事業者は、漏えい等又はそのおそれのある事案（以下「漏えい等事案」といいます。）が発覚した場合は、漏えい等事案の内容等に応じて、事実関係の調査及び原因の究明等について必要な措置を講じなければなりません※１。上記措置を講ずるための具体的な手法については、漏えい等事案の内容等に応じて個別の事例ごとに判断することになりますが、必要に応じて調査会社にフォレンジック調査を依頼することも有効です。

フォレンジック調査を依頼する会社は、例えば、フォレンジック調査業務を調査会社に「委託」（個人情報保護法第27条第５項第１号）する場合※２や、「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」（同条第１項第２号）に該当する場合※３には、調査に必要な個人データを本人の同意を得ずに当該調査会社に提供することができます。

また、上記の場合には、調査会社は、あらかじめ本人の同意を得ずとも、要配慮個人情報※４を取得することができます※５。

（※１）ガイドライン（通則編）3-5-2を御参照ください。
（※２）委託者は、委託先を監督する義務があります（個人情報保護法第25条）。
（※３）ガイドライン（通則編）3-1-5(2)では、本例外に該当する事例として「不正送金等の金融犯罪被害の事実に関する情報を、関連する犯罪被害の防止のために、他の事業者に提供する場合」などを挙げています。
（※４）「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他不当な差別や偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして個人情報保護法施行令で定める記述等が含まれる個人情報をいいます（個人情報保護法第２条第３項。ガイドライン（通則編）2-3も御参照ください。）。
（※５）「委託」（個人情報保護法第27条第５項第１号）の場合について個人情報保護法第20条第２項第８号、同施行令第９条第２号を、「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」（個人情報保護法第27条第1項第2号）に該当する場合について個人情報保護法第20条第２項第２号を御参照ください。