資料６

内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

2023年度　重要インフラにおける補完調査について

2024年6月7日

内閣官房　内閣サイバーセキュリティセンター(NISC)

補完調査の概要

調査の目的

補完調査とは、行動計画※の取組の評価に当たって、個別施策の結果・成果だけでは把握しきれない状況についても適切に把握することが重要であることから、個別施策の指標では捉えられない側面を補完的に調査することを目的として毎年度実施する調査です。

※重要インフラのサイバーセキュリティに係る行動計画（令和４年６月１７日サイバーセキュリティ戦略本部決定）

調査の運営

重要インフラサービス障害等の事例について、重要インフラ事業者等の協力を得て、現地調査（ヒアリング等）を実施します。重要インフラ事業者等における今後の取組にも資するよう、原因、対応、得られた気付き・教訓等をとりまとめ、可能な範囲で調査結果を公表します。

調査対象事例の選定基準

本報告書の調査対象事例は、2023年1月1日～2023年12月31日の間に、重要インフラ事業者等から内閣サイバーセキュリティセンターに提出された情報連絡の事例の中から、主に以下の選定基準により選定しました。

- 重要インフラサービス及びその周辺サービスへの実害の有無
- 事案の重大さ・社会的影響（関心）の大きさ
- 類似事例の発生状況や今後発生する可能性
- 攻撃手口や被害の目新しさ
- 世の中のトレンド
- 他分野への波及の可能性
- 得られる気付き・教訓の有用性等

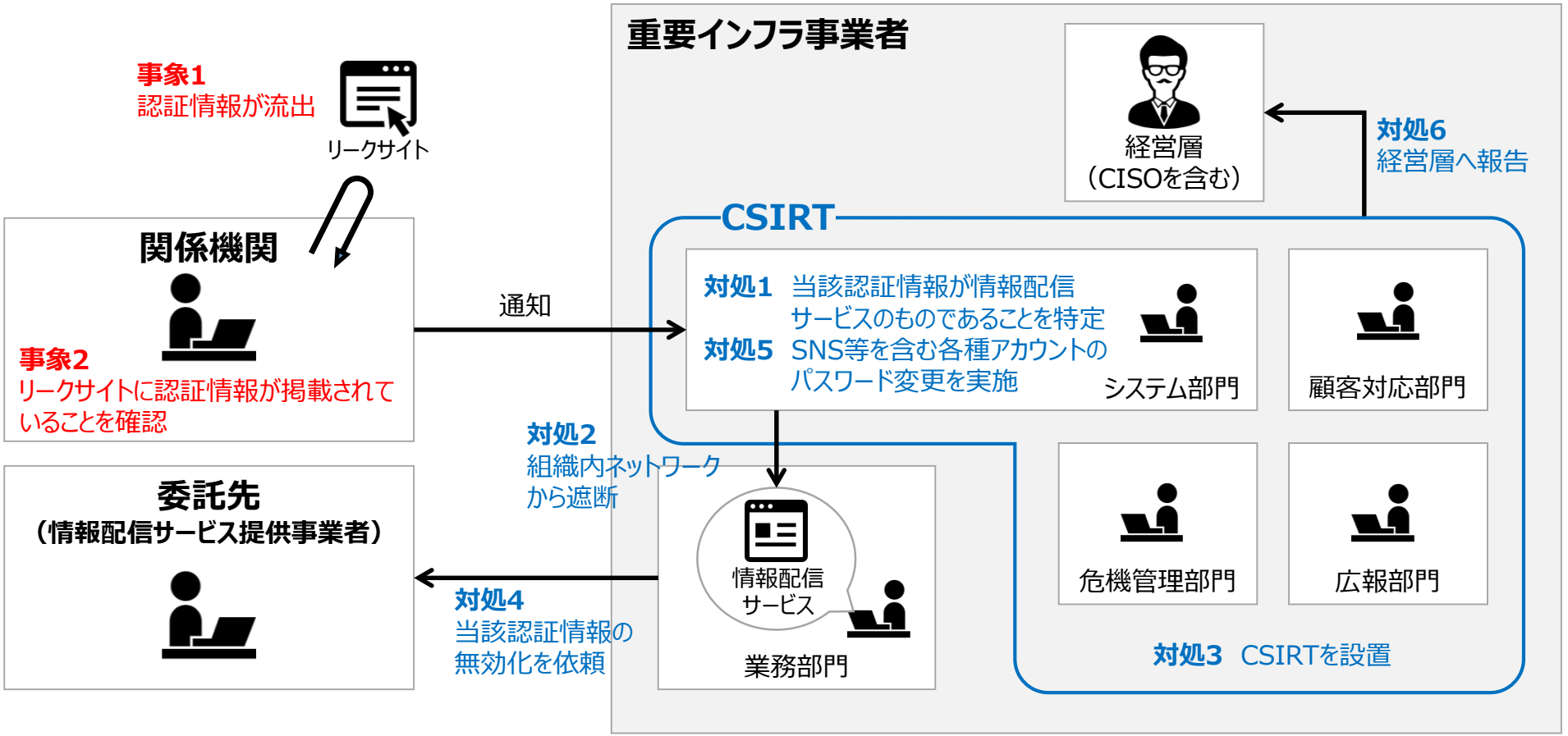
※その他、事案の対応の優劣、分野のバランスも考慮

補完調査の対象事例一覧

	事例の概要	主な気付き・教訓
サイバー攻撃の影響を低減した事例		
1	• 外部サービス利用のための**認証情報がリークサイトに掲載**。 • **当該サービスの利用停止**、**漏えいした認証情報の使用禁止**等を速やかに実施。	• **定期的なインシデント対応訓練**の結果、インシデント発生時の対処を円滑に進められた。 • 認証情報の悪用によるリスクを踏まえて、**調査や対処する範囲を適切に定める**ことが重要。
2	• DNSサーバーに対して**DDoS攻撃**が発生。 • **DNSサーバーの設定変更**や**関係者連絡先リストの見直し・周知**を行い、後日の攻撃では影響を抑制。	• 緊急時には、夜間休日を問わず迅速な情報伝達や意思決定が求められるため、**緊急連絡先の周知徹底**が重要。 • 現状のセキュリティ対策の課題を**定期的に確認し改善し続ける**ことが重要。
委託先・グループ子会社へのサイバー攻撃に起因する事例		
3	• Webサイト運用業務の**再委託先がランサムウェアに感染**し、Webサイトが停止。CSIRT構成員が組織を跨いで円滑に連携して対応。 • **再委託先の再選定**及び**サイト移行**を実施。	• CSIRTが実際に機能するように、**定期的に訓練を行う**ことが重要。 • **委託先のセキュリティ対策状況を見極めた上で**、委託先を選定することが重要。
4	• 再委託先のシステムが不正アクセスを受け、**個人情報がリークサイトに掲載**。 • 再委託先のシステムから**当該情報を削除**、委託先における**情報管理体制の実態を点検**。	• 委託先や再委託先の情報管理等に関する**実運用を把握**し、**確実に管理・検証する**ことが重要。 • **経営層を含む対処体制**について危機レベルに応じて設置することを定めていたことが円滑な初動対応に繋がった。
5	• グループ子会社の社員が**サポート詐欺**を受け、遠隔操作ソフトウェアをインストール、同社内ネットワーク内の**一部ファイルが削除**。 • 感染端末のネットワーク遮断やフォレンジック調査による情報漏えい有無の確認を実施。	• 情報システムへの技術的対策のみならず**社員への教育**が不可欠。 • サプライチェーンを狙ったサイバー攻撃の脅威が高まる中、**グループ全体でのセキュリティガバナンスを実現する仕組み**が必要。
システム故障に起因した障害の事例		
6	• 稼働系システムにおいてソフトウェア障害が発生。 • 速やかに**待機系システムへの切替え**を行い、**重要インフラサービスの提供に大きな影響は生じなかった**。	• 待機系システムへの**切替手順の周知**や**定期的な切替訓練**を実施していたことから、システム障害発生時にも混乱なく業務を継続できた。 • システム障害発生時の**対応体制が情報セキュリティポリシーで定められて**おり、インシデント発生時の対応においても迅速に連絡や報告、対処ができた。
7	• 権威DNSサーバー移行に際して、**旧登録情報の有効期限を関係者間で共有**されず、**名前解決が実行不可**に。 • 原因を特定し、**速やかに適切な設定変更**を実施。	• 情報システムの変更時に発生し得る障害とその防止策及び対応策を事前に検討し、**関係者間で共通認識を持つ**ことが重要。 • 関係者が一堂に会して打合せする機会を設けることも一案。

事例１：認証情報のリークサイトへの投稿 1／2

- 重要インフラ事業者は、外部の情報配信サービスを利用しており、職員ごとにID及びパスワードを設定していた。
- 関係機関より、重要インフラ事業者が管理するドメインのメールアドレスを含む認証情報がリークサイトに掲載されているとの連絡を受けた。
- 重要インフラ事業者は、掲載された認証情報が登録されていたサービスの特定、当該サービスの遮断及び当該認証情報の無効化等の対応を、年に一度実施していたインシデント対応訓練における対応体制にもとづき速やかに実施した。



事例１：認証情報のリークサイトへの投稿 2／2

1. 背景

- 重要インフラ事業者は外部の情報配信サービスを利用しており、職員ごとにID及びパスワードを設定していた。
- CSIRT要員によるインシデント対応訓練を、年に一度の頻度で実施していた。

2. 検知

- 重要インフラ事業者のIT部門が、関係機関より、重要インフラ事業者が管理するドメインのメールアドレスを含む認証情報がリークサイトに掲載されているとの連絡を受けた。

3. 対処

- リークサイトに掲載された認証情報が情報配信サービスのものであることを特定し、組織内ネットワークと当該サービスとの接続を遮断した。
- 組織内の各部門へ注意喚起を実施した。
- システム部門や危機管理部門、広報部門、顧客対応部門からなるCSIRTを設置し、対応方針を協議した。
- システム部門が情報配信サービスを利用している業務部門に対するヒアリングを実施した。
- 業務部門より情報配信サービスの提供事業者に対し、リークサイトに掲載されたアカウントの削除及び情報漏えいに係る事実確認を依頼した。
- 掲載された認証情報を永久に使用禁止とした。
- 当該サービス以外からも認証情報が漏えいしている可能性を考慮し、認証情報の悪用による影響が大きいSNS等の対外広報ツールのアカウントのIDとパスワードを、掲載を検知した翌日までに変更した。その後、対象システムを拡大し各種アカウントのパスワードを変更した。
- 適宜経営層に対して対応状況を共有した。

4. 原因

- 認証情報漏えいの直接原因の特定には至らなかった。
- 認証情報が掲載されたリークサイトは、掲載を検知した数日後には閉鎖されており、追跡が不可能であった。

5. 再発に備えた対策

- 組織内の各部門に対して認証情報の窃取に関する注意喚起を実施した。
- 他の認証情報の漏えい有無を確認するための調査を実施した。
- 認証情報が漏えいした際の影響範囲を小さくするため、悪用による影響が大きいSNS等の対外広報のためのツールや顧客対応のためのシステムに登録するアカウントのIDと、組織内システムに登録するアカウントのIDに同一のメールアドレス等を利用しないといった対策を検討している。

6. 得られた気付き・教訓

- **CSIRTの整備と定期的な訓練**

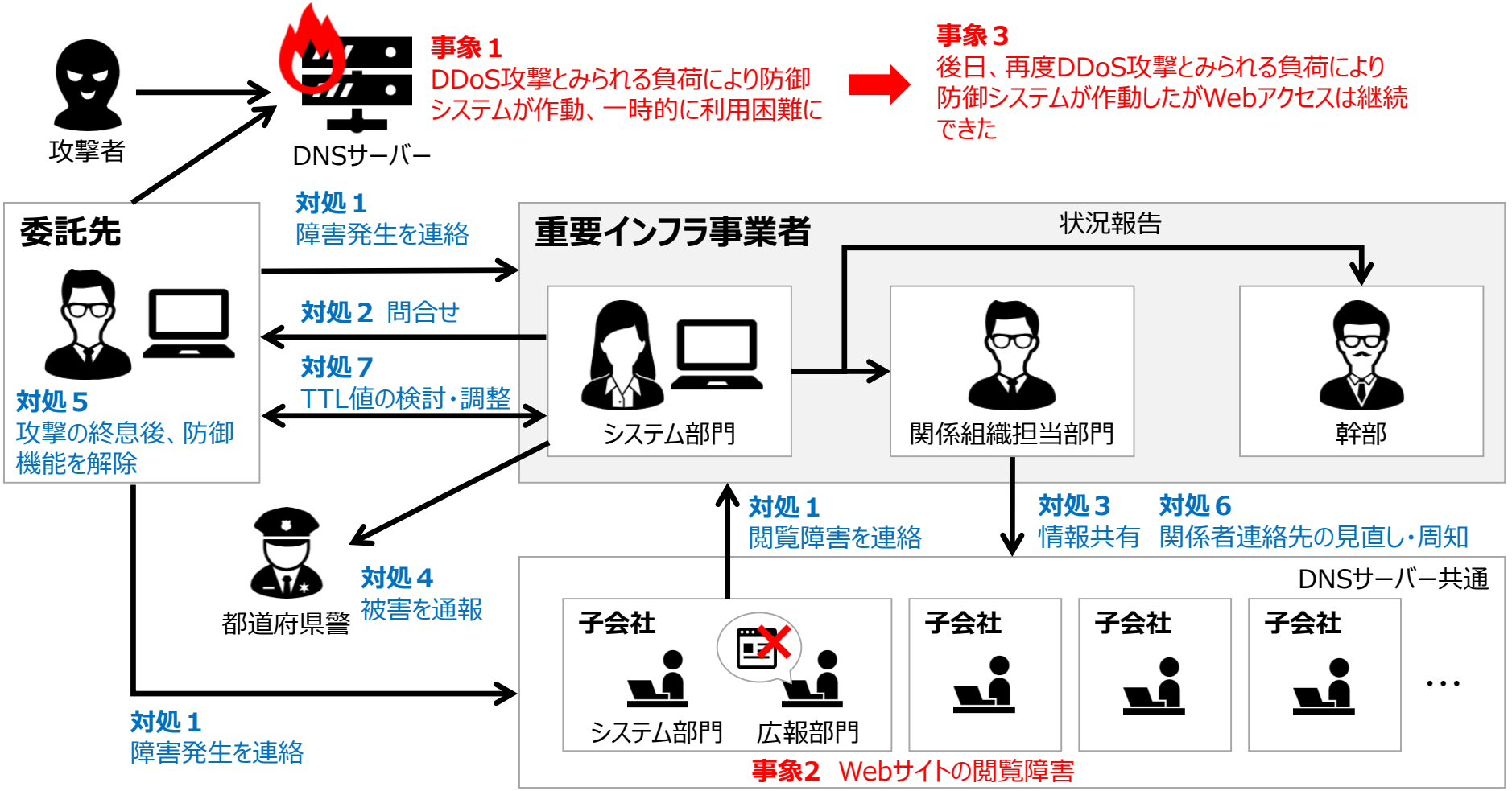
  システム部門や危機管理部門、広報部門、顧客対応部門からなるCSIRTにおいて年に一度のインシデント対応訓練を実施していたことにより、実対応を経験しているCSIRT要員がいなかったものの役割分担や対処を円滑に進められた。また、CISOを含む経営層への連絡や会議体における報告、指示命令の伝達等についても適切に実施することができた。人事異動等による要員の変更を考慮し、インシデント対応に係る経験や知識を継承することが重要。

- **認証情報の漏えい事象における対処範囲の検討**

  本事例では、認証情報漏えいの直接原因の特定には至らなかったことから、リークサイトへの掲載が確認された認証情報を扱っていたサービスのみならず、その他のサービスのパスワードの変更等の対処を合わせて実施した。認証情報の悪用によるリスクを踏まえて、調査や対処の範囲を適切に定めることが重要。

事例２：DNSサーバーに対するDDoS攻撃 1／2

- 重要インフラ事業者は、複数の重要インフラ事業者と共通のDNSサーバーを使用していた。
- 重要インフラ事業者は、DDoS攻撃（事象１）を受けて関係組織や都道府県警との連携等の必要な対処によって事態を収拾し、DNSサーバーへの設定変更や関係者連絡先リストの見直し・周知などによって今後の攻撃に備えた。
- 後日発生したDDoS攻撃（事象３）ではサービスへの影響を抑えることができた。



事例２：DNSサーバーに対するDDoS攻撃 2／2

１．背景

- 重要インフラ事業者は、複数の重要インフラ事業者と共通のDNSサーバーを使用していた。
- 当該DNSサーバーは、Webサイトやメール等のインターネット接続システム用で、重要インフラサービスへの影響は限定的。
- DDoS攻撃によるDNSサーバーの停止を防ぐため、攻撃時に通信流量を制限する防御システムを設置していた。

２．検知

- 防御システムがDNSサーバーの高負荷を検知し、通信流量を制限した。
- 子会社から、Webサイトが閲覧できない旨連絡を受けた。（通信流量制限の影響）
- 重要インフラ事業者とDNSサーバーを共同利用する子会社は、 DNSサーバーの運用委託先から障害発生の連絡を受けた。

３．対処

- DNSサーバーの運用委託先に状況を問い合わせ、防御システムが作動中である旨を確認した。
- DNSサーバーを共通で使用している他の重要インフラ事業者に情報共有した。その際、当該DNSサーバーを使用しない外部メールサービス等の代替手段を用いた。
- 都道府県警へDDoS攻撃被害を受けたことを通報した。
- 幹部へ状況を報告した。

４．原因

- DDoS攻撃によるDNSサーバーの過負荷。

５．再発に備えた対策

- DNSサーバーのキャッシュ生存時間（TTL値）を適度に延長する調整をベンダに提案し、ベンダの技術的知見を踏まえて設定を変更したことで、DNSへのDDoS発生時もキャッシュの利用が期待できる一般利用者からはWebアクセスしやすくなるようにした。
- DNSサーバーを共同利用する一部子会社に対して緊急連絡先の共有が不十分であったため、緊急連絡先を周知徹底した。
- すでに作成済みであった自然災害やシステム障害を想定したIT-BCPをもとに、サイバー攻撃を想定したIT-BCPを検討している。

6. 得られた気付き・教訓

- **障害発生時の緊急連絡先の周知徹底**

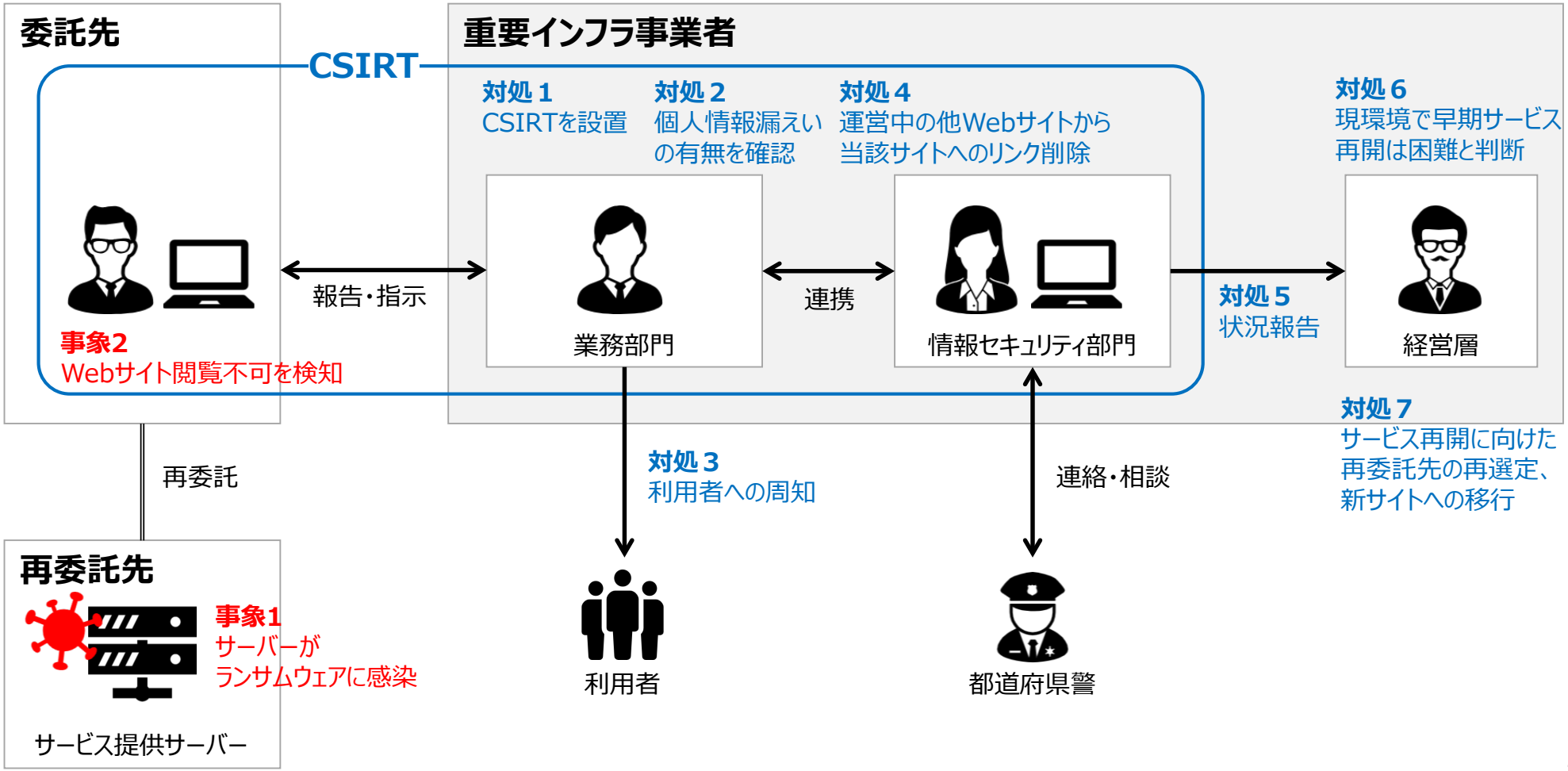
  本事例では、DNSサーバーを共同利用する一部子会社に緊急連絡先の共有漏れがあり、更に夜間休日に障害が発生したことも重なったため、最初に障害を認識した部門は、重要インフラ事業者への出向者を通して連絡することになった。緊急時には、夜間休日を問わず迅速な情報伝達や意思決定が求められるため、緊急連絡先の周知徹底が重要であることを再認識。

- **セキュリティ対策の定期的な見直し、改善**

  現状のセキュリティ対策に課題がないかを定期的に確認し、改善することが重要。本事例では、サイバー攻撃を受けたことを起点として、システムの設定を変更したことで、再度サイバー攻撃を受けた際の影響を抑えることができた。

事例３：再委託先のランサムウェア感染によるWebサイト停止 1／2

- 重要インフラ事業者は委託先にWebサイト運用を委託し、委託先は再委託先が提供するクラウドサービス上でWebサイトを運用していた。
- 情報セキュリティ部門は、委託先や業務部門等を招集してCSIRTを設置し、各部門が連携して個人情報漏えい有無の確認や再委託先の再選定及びサイト移行を実施したことで事態を収拾、サービスを再開させた。



事例３：再委託先のランサムウェア感染によるWebサイト停止 2／2

1．背景

- 重要インフラ事業者は、Webサイトを運営していた。
- 重要インフラ事業者は、Webサイトの運用を外部事業者(以降、委託先)に委託していた。
- 委託先は、Webサイトを公開するためのサーバーの運用をクラウドサービス事業者(以降、再委託先)に再委託していた。

2．検知

- 委託先は、Webサイトが閲覧できないことを検知し、重要インフラ事業者に報告した。
- 重要インフラ事業者は、再委託先がランサムウエア攻撃を受けクラウドサービスが停止していることを再委託先のWebサイトで確認した。

3．対処

- 情報セキュリティ部門、業務部門、委託先からなるCSIRTを設置した。
- 被害にあったWebサイトでは、個人情報の漏えいがなかったことを確認した。
- 二次被害防止のため、運営している他のWebサイトから当該Webサイトへのリンクを削除した。
- 利用者に対してシステム障害が発生している旨を、運営している他のWebサイト上で周知した。
- 経営層へ対応状況を報告。再委託先のクラウドサービス上でのWebサイト早期再開は困難と判断し、再委託先の変更を決定した。
- Webサイト再開に向けた再委託先の選定、Webサイトの移行を実施した。

4．原因

- 再委託先のサーバーがランサムウェアに感染した。

5．再発に備えた対策

- 再委託先の選定にあたり、サイバー攻撃対策に関する外部認定を受けた事業者であることを条件に加えた。
- 脆弱性診断サービスを導入し、Webサイト自体のサイバー攻撃対策を強化した。
- 個人情報漏えいのリスクを一層低減させるために、問い合わせフォームとメールマガジンを廃止した。

6. 得られた気付き・教訓

- **平時からの関係者間の連携強化**

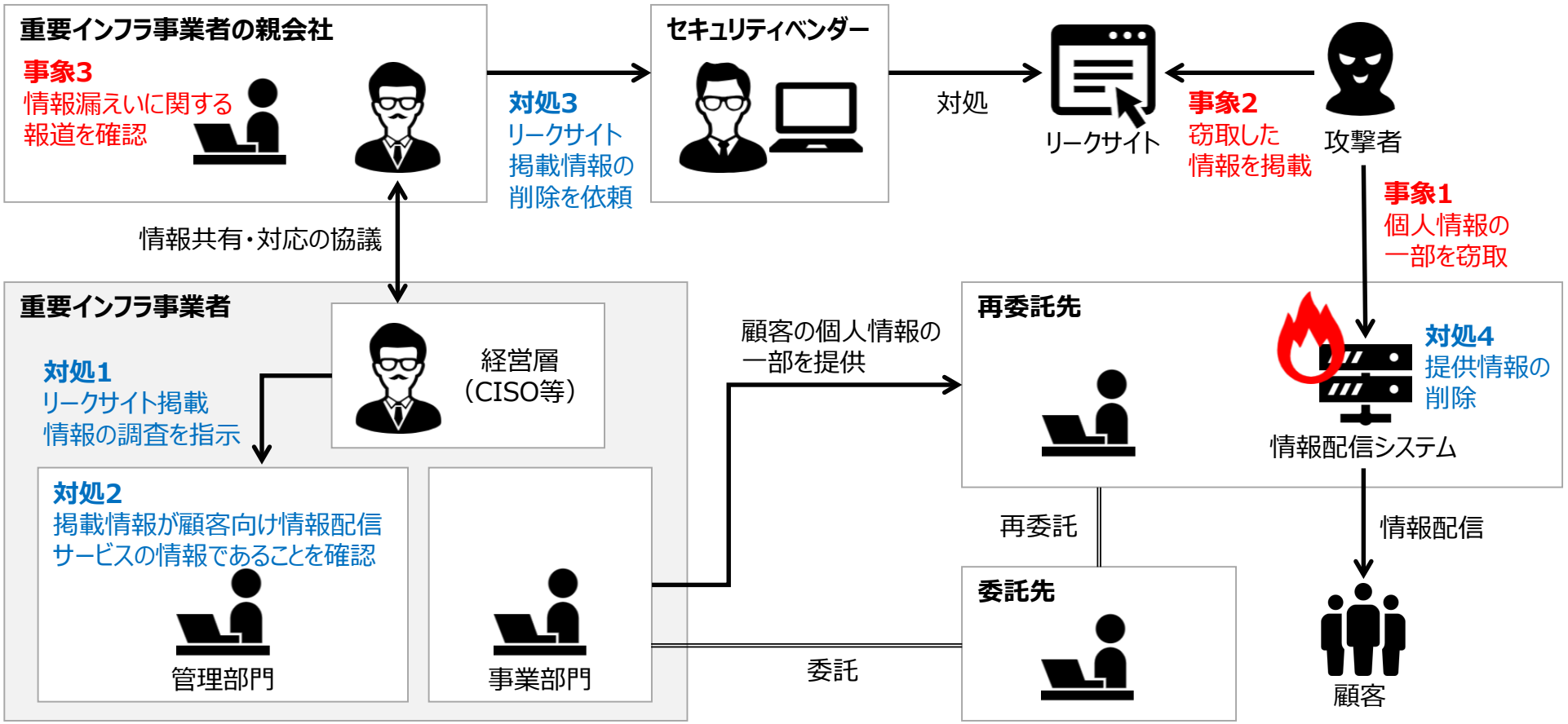
  CSIRT体制を制度上定めるだけではなく、有事の際に実際に機能するように、平時から訓練を行うことが重要。本事例では、CSIRTの主たる構成組織で定期的にインシデント対応訓練や研修会を実施し、平時から連携を行っていたため、障害発生時には各組織が円滑に対応できた。また、都道府県警や他の重要インフラ事業者とも定期的に会議を開いており、技術支援の要請等、円滑に連携することができた。

- **セキュリティ対策状況を踏まえた委託先の選定**

  業務委託先におけるサイバー攻撃被害のリスクを低減するためには、外部認定の取得を参考にしつつ、クラウドサービスの内容やサービスプロバイダとの契約内容を確認し、セキュリティ対策状況を見極めたうえで選定することが重要。本事例では、サイバー攻撃対策に関する外部認定を受けた事業者を委託先の選定条件に加えることで、業務委託先のセキュリティ対策レベルの担保を図っている。

事例４：再委託先へのサイバー攻撃による情報漏えい 1／2

- 重要インフラ事業者は顧客向け情報配信サービスを外部事業者へ委託し、再委託先が運営するシステムで個人情報の一部を取り扱わせていた。
- 再委託先が重要インフラ事業者の基準に基づいた情報管理を適切に行っていなかったこと等が一因となり、再委託先が運営するシステムへの不正アクセスが発生し、個人情報の一部が窃取されリークサイトに掲載された。
- 重要インフラ事業者は再委託先システムからの情報の削除やリークサイト掲載情報の削除を依頼すると共に、業務委託先における情報管理体制やその実態の点検を実施した。



事例４：再委託先へのサイバー攻撃による情報漏えい 2／2

1. 背景

- 重要インフラ事業者は、顧客向け情報配信サービスを外部事業者へ委託しており、委託先は情報配信システムを運営する外部事業者へ当該サービスを再委託していた。
- 顧客向け情報配信サービスは顧客情報と連動したコンテンツを配信するものであり、重要インフラ事業者は当該サービスの運用にあたり、再委託先へ個人情報の一部を提供していた。
- 重要インフラ事業者は、委託先や再委託先に対して、個人情報の取扱いやシステム運用体制、サイバーセキュリティ体制等を事前に確認していた。また、再委託先はシステム運用に関する第三者認証を取得していた。
- 重要インフラ事業者は、サイバーセキュリティインシデント等の危機レベルに応じた対処体制や連絡・報告体制を定めていた。

2. 検知

- 重要インフラ事業者の親会社が、重要インフラ事業者の顧客情報がリークサイトに掲載されている旨、セキュリティ専門のニュースサイト運営会社が報じたことを確認した。

3. 対処

- 重要インフラ事業者のCISOの指示によりリークサイトに掲載された情報について調査したところ、当該情報が再委託先へ提供した情報であることが判明した。
- 事前に定められた規定等に基づき、経営層や事業部門、管理部門等からなる対処体制を設置するとともに、親会社及び重要インフラ事業者の経営層が対応方針を協議した。
- 個人情報の一部の漏えいに関する対外公表を実施した。
- 親会社はセキュリティベンダーに対して掲載情報の削除を依頼し、掲載情報は削除された。
- 重要インフラ事業者が再委託先へ提供した個人情報の一部を、情報配信システムから全て削除した。

4. 原因

- 再委託先が運用する情報配信システムが不正アクセスを受け、複数の認証情報が窃取された。当該認証情報の悪用により、重要インフラ事業者が再委託先へ提供した個人情報の一部を格納する領域への侵入及び当該情報の窃取が行われた。
- 再委託先において、重要インフラ事業者が事前に確認し、かつ第三者認証を取得していたシステム運用体制等が適切に運用されていなかった。また、重要インフラ事業者との取り決めによる期間を超えた削除すべき情報が情報配信システムに残存していた。

5. 再発に備えた対策

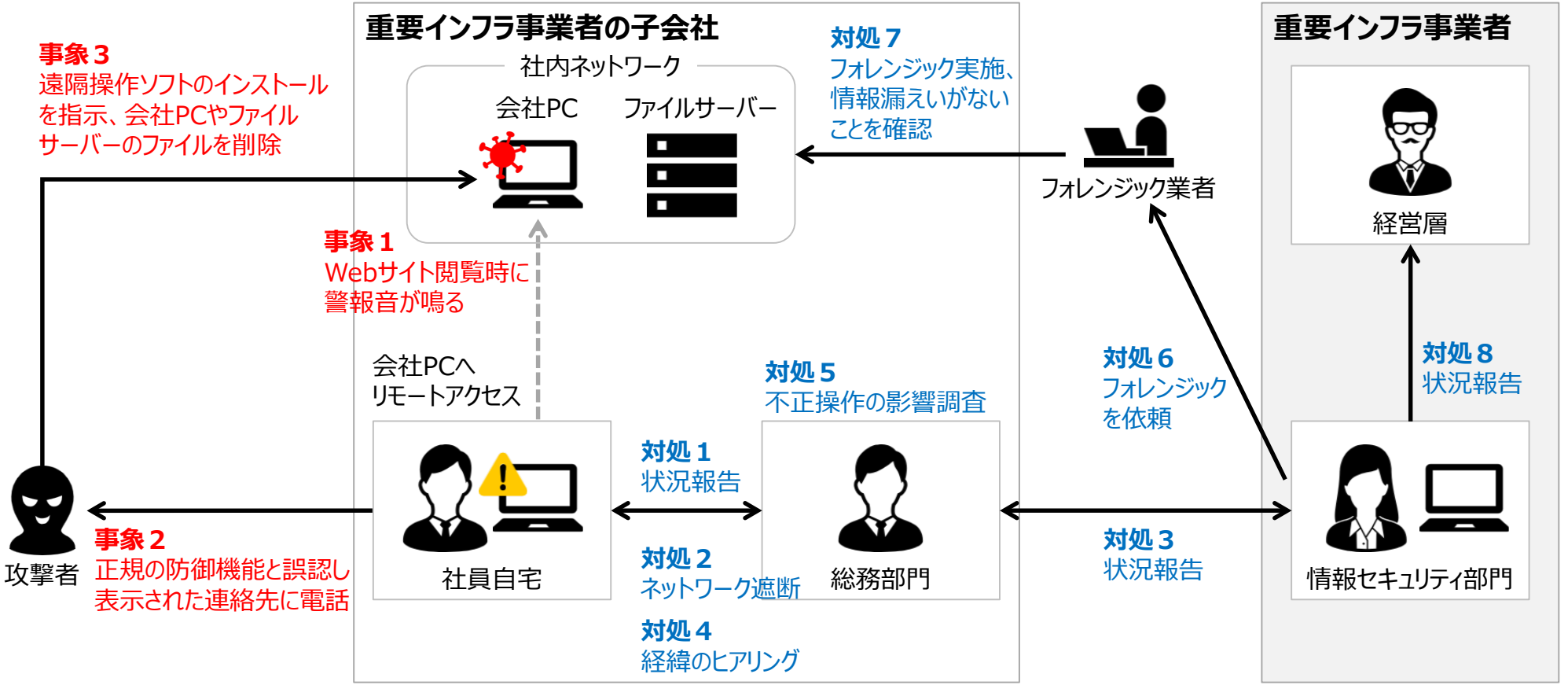
- 委託先における個人情報の取扱いを必要最小限とし、使用後の速やかな削除を徹底するため、事業部門による委託先の情報管理に対する監督を徹底し、加えて管理部門により事業部門の監督状況を定期的に検証する。
- 個人情報を含む情報を取り扱う業務の外部事業者への委託について、委託開始前及び委託期間中の審査項目を詳細化し、証跡確認を合わせて実施することで委託先管理を強化する。

6. 得られた気付き・教訓

- **委託先における情報管理等の実態把握の重要性**
  業務の委託に際する情報管理等に関する確認では、委託先や再委託先の実運用を把握し、これを確実に管理・検証することが重要。
- **事業継続計画等の事前の定めや定期的な見直しの重要性**
  経営層を含む対処体制について、危機レベルに応じて事前に定めていたこと等が円滑な初動対応に繋がった。リスクシナリオの検討、事業に与える影響の分析、それらを踏まえた事前の対策や訓練を平時から実施することが重要。

事例５：グループ子会社におけるサポート詐欺 1／2

- 重要インフラ事業者のグループ子会社は、グループ全体の共通ネットワークとは独立した社内ネットワークシステムを使用していた。
- 重要インフラ事業者は、子会社の総務部門等と連携してサポート詐欺により遠隔操作ソフトをインストールした社員へのヒアリング、ネットワーク遮断やフォレンジック調査による情報漏えい有無の確認等の必要な対処を行い、事態を収拾した。



事例５：グループ子会社におけるサポート詐欺 2／2

1．背景

- 重要インフラ事業者のグループ子会社は、社員の個人PCから会社PC(以降、当該端末)にリモートアクセスができる社内ネットワークシステム(以降、当該システム)を使用していた。
- 当該システムは、重要インフラ事業者のグループ会社全体の共通ネットワークに接続しない独立したシステムである。

2．検知

- 当該システムを利用し、自宅にてリモートワークを実施していた子会社の社員(以降、当該社員)が、(リモート越しに操作していた)当該端末上でWebサイトを閲覧していたところ、偽セキュリティ警告による警報音が鳴った。
- 当該社員は当該端末の正規のセキュリティ対策ソフトが動作したと誤認し、画面に表示された連絡先に電話をかけ、通話相手の指示通り当該端末に遠隔操作ソフトウェアをインストールした。
- その後、デスクトップから複数ファイルが削除されていることに気づき、不審に思い、子会社の総務部門へ連絡した。また、当該端末の操作もできなくなっていた。

3．対処

- 子会社は、社内ネットワークがマルウェアに感染したことを重要インフラ事業者の情報セキュリティ部門に報告した。
- 子会社は、当該端末を社内ネットワークから速やかに遮断した。
- 当該社員へのヒアリングを行い、不正操作に至るまでの経緯を確認した。
- 子会社は、社内ネットワーク内で不正操作が行われていないかを確認し、ファイルサーバー上の一部フォルダが削除されたことが分かった。
- 重要インフラ事業者は、フォレンジック業者に当該端末と子会社の社内ネットワークのフォレンジック調査を依頼した。調査の結果、情報漏えいの痕跡は確認されなかった。
- 経営層へ対応状況を報告した。

4．原因

- サポート詐欺により、遠隔操作ソフトウェアをインストールした。

5．再発に備えた対策

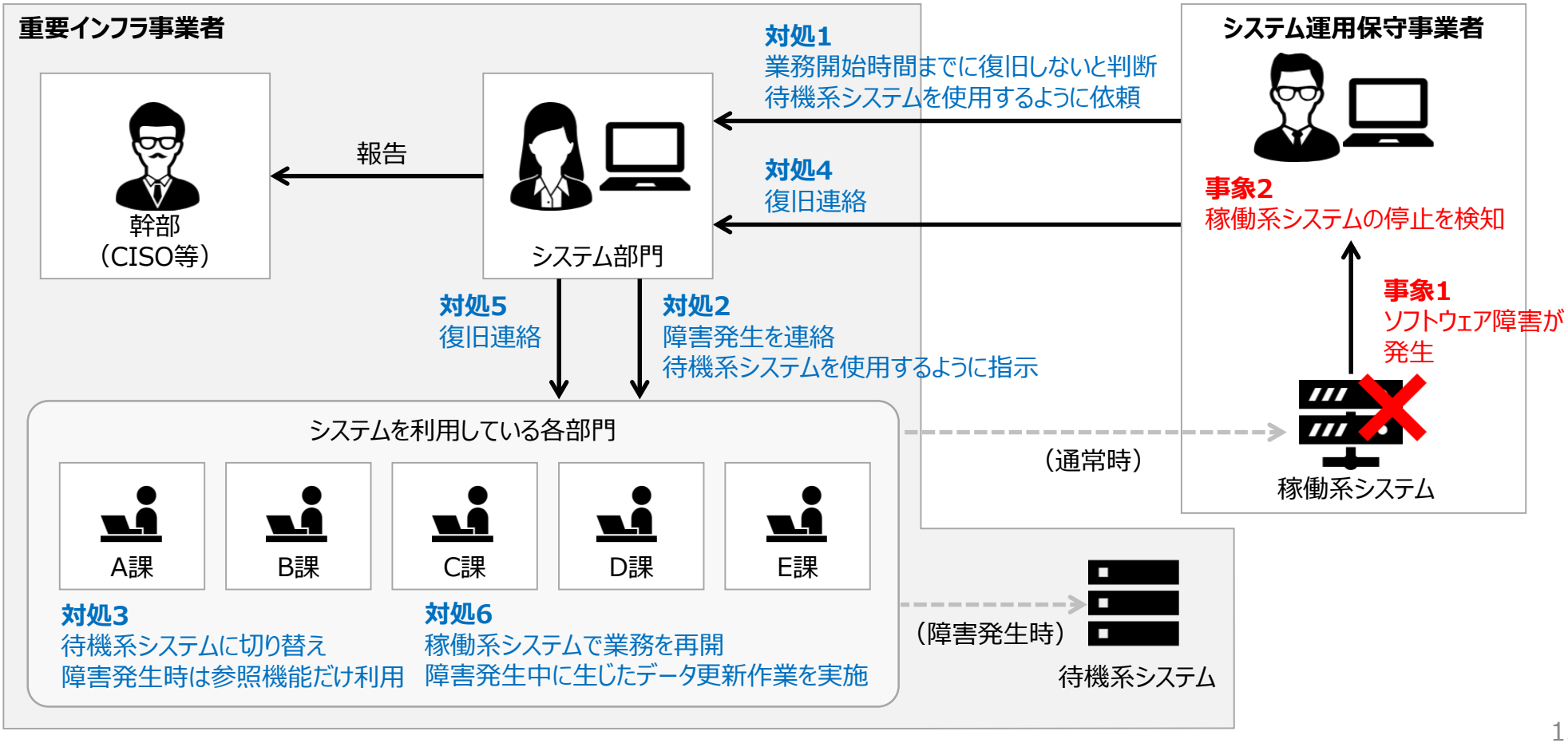
- グループ各社社員向けにリモートワーク時の注意事項やサイバー攻撃を受けた際の対処方針を周知した。
- グループ各社社員向けに情報セキュリティに関するe-Learningを実施する。
- グループ各社が使用するシステムの構成やシステム間の接続状況を一覧化し、セキュリティ対策の検討や改善に活用できる情報を整理する。

6. 得られた気付き･教訓

- **グループ全体での社員の情報セキュリティレベルの向上**
  子会社を含めたグループ全体での情報セキュリティレベルの向上には、情報システムへの技術的対策のみならず社員に対する教育が不可欠。e-Learningやハンズオンなどを活用して、多数の組織･社員に対して一定水準以上のリテラシーを身に付けさせることが必要。
- **グループ各社全体でのセキュリティガバナンスの実現**
  サプライチェーンを狙ったサイバー攻撃の脅威が高まる中、グループ全体でセキュリティガバナンスを実現するための仕組みが必要。所在地（国間の時差、文化及び商流の違い等）、リモートワークなどの業務環境の多様化や情報セキュリティ体制、資本力が各社異なる中で、グループ各社のセキュリティポリシーの整合性やCSIRT組織の連携強化等が求められる。本事例では、重大な被害は発生しなかったものの、全社経営会議まで事例を報告することでグループ全体で問題意識の共有を図るとともに、グループ全体を守備範囲とするグループCSIRTを構築しガバナンス強化を図っている。

事例６：ソフトウェア障害に伴う稼働系システムの停止 1／2

- 重要インフラ事業者は冗長性確保のため稼働系と待機系の２系統からなるシステムにより重要インフラサービスを提供していた。
- 稼働系システムにおいてソフトウェア障害によるシステム停止を検知したため、待機系システムのデータ参照機能を使用した運用へ切替えた。システムを利用する各部門に対して切替手順が周知されていたこと等により重要インフラサービスの提供に大きな影響は生じなかった。
- 稼働系システムの復旧後、システム障害発生中に生じたデータ更新作業を実施した。



事例６：ソフトウェア障害に伴う稼働系システムの停止 2／2

1. 背景

- 重要インフラ事業者は、重要インフラサービスを提供するためのシステムの冗長性確保のため、委託先が提供するクラウドシステムを稼働系として、同委託先が保守を行うオンプレミスシステムを待機系として、２系統を運用していた。
- 待機系システムは１日に一度、重要インフラ事業者の業務時間外に稼働系システムとデータを同期していた。
- 待機系システムへの切替手順はシステムを利用する各部門へ周知されており、また、切替訓練は年に一度実施していた。

2. 検知

- 重要インフラ事業者の業務開始前の時間帯に、委託先が稼働系システムの仮想マシン停止を検知した。

3. 対処

- 委託先において稼働系システムの復旧作業を実施した。
- 委託先は復旧作業が重要インフラ事業者の業務開始時間までに完了しないと判断し、重要インフラ事業者のシステム部門に対して待機系システムへの切り替えを依頼した。
- システム部門はシステムを利用する各部門に対して、待機系システムへの切替えを指示した。ただし、稼働系システムとのデータ不整合を防ぐため、データ更新機能は使用せず参照及び出力機能のみを使用することとした。
- 事前に定められたシステム障害対応体制に基づき、CISOに対して状況を報告した。以後、CISOを含む経営層に対し状況報告を適時行った。
- システムを利用する各部門は切替手順に従って待機系システムに接続し業務を開始した。
- 委託先において稼働系システムの復旧作業を完了し、システム部門に対して稼働系システムが復旧した旨を連絡した。
- システム部門において稼働系システムの正常動作を確認し、システムを利用する各部門に対して稼働系システムでの業務再開を指示した。
- システムを利用する各部門は稼働系システムでの業務を再開し、システム障害発生中に生じたデータ更新作業を実施した。

4. 原因

- ソフトウェア障害により稼働系システムが停止した。

5. 再発に備えた対策

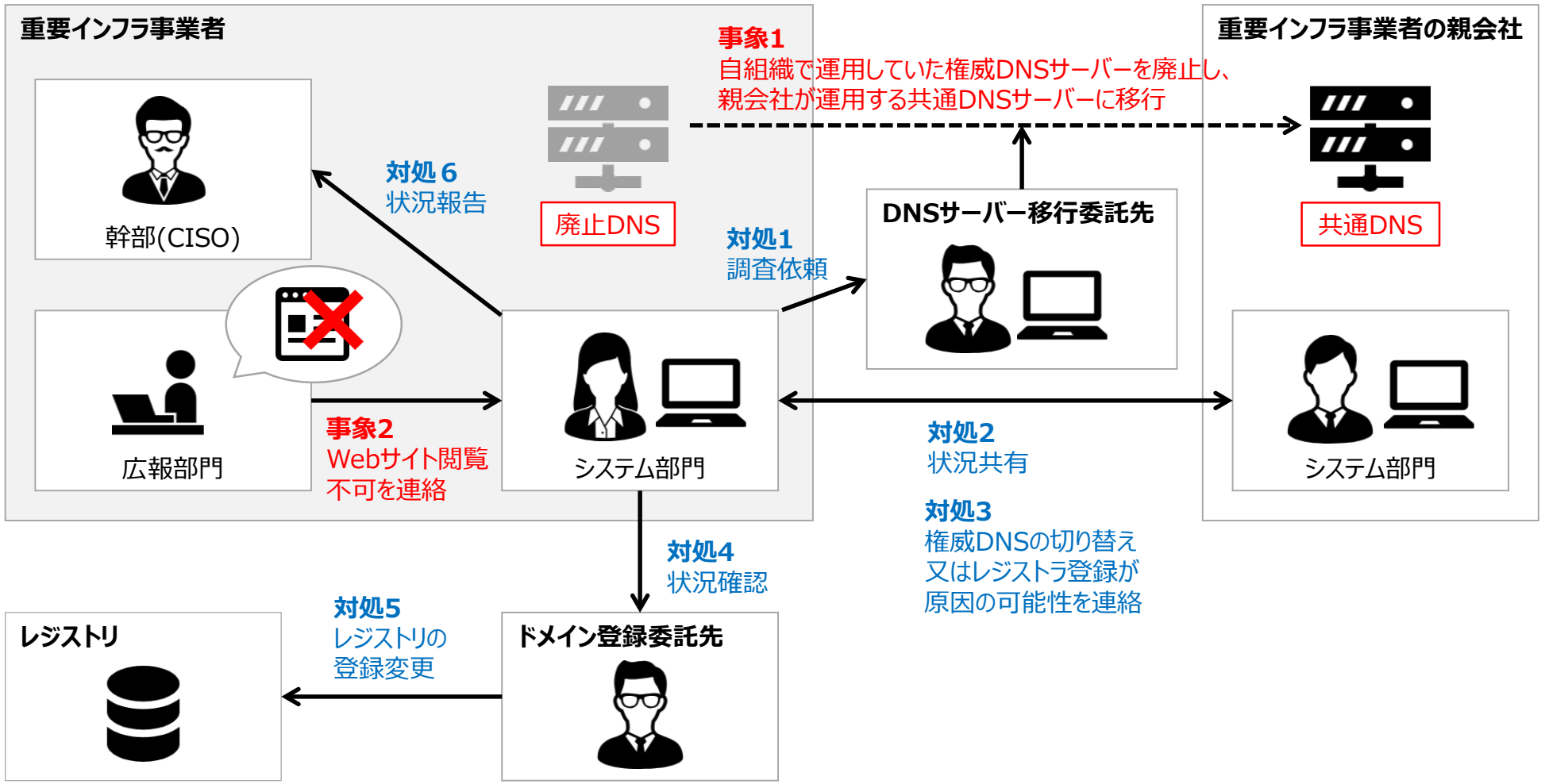
- 同様のソフトウェア障害が発生しないよう、原因となったソフトウェアの改修を実施した。
- システム障害発生時の重要インフラ事業者と委託先の連絡先を明確化した。
- 業務継続計画(BCP)は災害を前提としたものであったため、システム障害を踏まえたICT-BCPの策定を検討しており、組織内で利用している情報システムの把握、業務の重要度やシステム依存度などを整理している。

6. 得られた気付き・教訓

- **システム障害発生に備えた対応訓練の重要性**
  待機系システムへの切替手順がシステムを利用する各部門に適切に周知されていたことや、定期的に切替訓練を実施していたことから、システム障害発生時にも混乱なく業務を継続できた。
- **システム障害発生時の対応体制整備の重要性**
  CISOや各部門の担当者を含むシステム障害発生時の対応体制が情報セキュリティポリシーにおいて定められており、実対応においても迅速に連絡や報告、対処を実施できた。

事例７：権威DNSサーバー移行時のサービス障害 1／2

- 重要インフラ事業者は、権威DNSサーバーの移行を実施した。
- 権威DNSサーバー移行に際して、ドメイン登録事業者へ登録変更を依頼していたが、旧登録情報の有効期限を共有しなかったため、期限切れ時点で登録変更が未実施となっていた。
- 重要インフラ事業者は、関係各所と連携して原因を特定し、登録作業を実施したことで事態を収拾した。



事例７：権威DNSサーバー移行時のサービス障害 2／2

1．背景

- 重要インフラ事業者は、自組織のみで運用していた権威DNSサーバーを廃止し、親会社が運用する権威DNSサーバーを利用することとした。
- 重要インフラ事業者は、サーバー移行業務をDNSサーバー移行委託先に委託し、サーバーの移行は完了していた。
- 重要インフラ事業者は、ドメイン登録事業者へ登録変更を依頼したが、旧登録情報の有効期限を共有しなかったため、期限切れ時点で登録変更が未実施となっていた。

2．検知

- 重要インフラ事業者の広報部門が、自組織のWebサイトが閲覧できないことを検知し、システム部門に報告した。

3．対処

- システム部門は、DNSサーバー移行委託先に調査を依頼した。
- 幹部(CISO)及び親会社のシステム部門に状況を共有した。
- システム部門は、サーバーの移行、又はレジストリへの登録変更失敗/未実施に原因可能性を絞り込んだ。親会社からも、原因の可能性について同様の助言を受けた。
- ドメイン登録事業者に、レジストリへの登録変更状況を確認した。
- レジストリへの登録変更が未実施だったため、ドメイン登録事業者が直ちに登録を実施した。

4．原因

- 移行前の旧登録情報がキャッシュから消失し、DNSサーバーの名前解決ができなくなった。
- 関係者間での作業スケジュールの確認不足。

5．再発に備えた対策

- 情報システムを変更する際には、その作業によって発生しうる障害とその防止策及び対応策を事前に検討することにした。
- 情報システム関係者の緊急連絡先を再確認した。
- 業務全体に対する助言等、仕様書上で明確にしにくい作業について、どのように委託先と調整していくのが良いかを検討している。

6. 得られた気付き･教訓

- **情報システム変更時の障害想定と対策の共有**

  情報システムを変更する際には、その作業によって発生しうる障害とその防止策及び対応策を事前に検討した上で、関係者間で共通認識を持つことが重要。 本事例のようなDNSサーバーや基幹ネットワークの切り替え等、影響範囲が大きい作業では、優先度を上げて実施したい。

- **業務全体を俯瞰したタスク管理と複数関係者間での連携**

  個々の作業単位だけでなく、業務全体として見落としがないかを確認することの重要性を実感。本事例では、ドメインの登録変更が必要なことは認識していたが、その実施期限の確認が不十分であった。ドメインの登録変更とサーバー移行の実施順の認識齟齬、他の類似作業と合わせて効率的な実施計画を立てていたこと、キャッシュの残存期間を意識していなかったことが重なった。

  １対１では十分に連携できていたとしても、関係者が３者以上いる場合は、関係者全員が一同に会して打合せをする機会を設けることで、認識齟齬や見落としに気づける可能性が考えられる。