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

2022年度　重要インフラにおける補完調査について

2023年6月2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、2022年1月1日～2022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

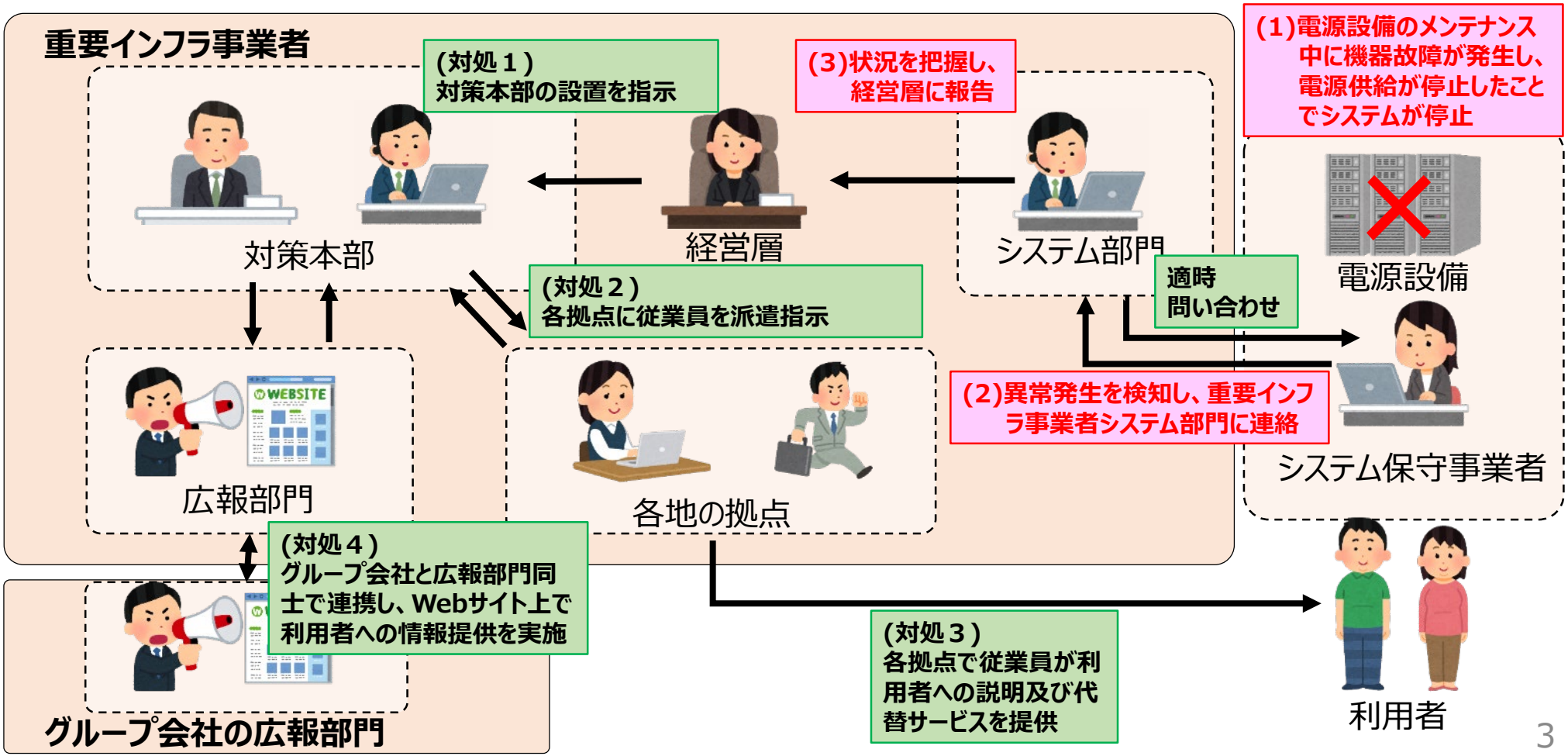
※その他、事案の対応の優劣、分野のバランスも考慮

補完調査の対象事例一覧

	事例の概要	主な気づき・教訓
システム故障に起因した重要インフラサービス障害		
1	• **外部サービスの電源設備メンテナンス中に故障が発生**し、同サービスを利用した重要インフラ**サービスの提供が停止** • 各部門が連携し、利用者へ周知や代替策を案内	• 外部サービスでインシデントが発生した場合の**連絡体制を、通常時から関係者間で議論して確認**しておく。 • **実績のある作業においても**、故障が発生した際のサービスへの影響を考慮し**作業リスクを判定する**。
サイバー攻撃に起因した重要インフラ関連サービス障害		
2	• 海外子会社のネットワークが侵害され、**工業製品（OT）の制御PCや古いOSのサーバー等がランサムウエアに感染** • システムを再構築し、速やかに業務を再開	• OT関連機器は事業者が**自由にパッチ適用出来ないため**、**ベンダー及び販売代理店を含めて**素早く対応出来るような**協力体制を整える必要**がある。 • 発生した事案の内容に応じた緊急時の連絡先を把握しておくことが重要。
3	• コーポレートサイト等の**WebサイトにDDoS攻撃を受けた** • 攻撃元IPアドレスを遮断し、正常化したことを確認	• **組織内規定を事前に整備**し、対応訓練を実施していたことから、インシデント発生時に迅速に対応できた。 • 事象の検知から原因の特定までを迅速に行うために、**IT資産や構成図の適切な管理が重要**。
4	• 重要インフラ関連サービスの**WebサイトにDDoS攻撃を受けた** • 攻撃元IPアドレスを遮断後もIPアドレスを変えて攻撃が継続したため、Webサイトを一時停止し、メール等による代替業務を実施	• ファイアウォール等による外部からの不正侵入対策だけではなく、サービスの重要性に応じて、CDNやWAF等の**DDoSに特化した対策が重要**。 • インターネットに公開している機器については**誰でも狙われるという危機意識を醸成**し、適切に対策を行うことが重要。
サイバー攻撃の影響を低減した事例		
5	• 重要インフラ関連サービスの**Webサイトに投稿フォーム**があり、短時間に**大量の投稿を受信** • 攻撃元IPアドレスを遮断し、Webアプリケーションを改修	• **想定される事案毎に連絡先を整理**し、緊急時に迅速な対応ができた。 • システム**保守事業者任せでは無く、職員がシステム構成を十分把握**していたことで、検知後の対処を迅速に判断することができた。
6	• **委託先のサーバーがランサムウエアに感染**し、一部業務が停止 • 委託先との接続経路を特定し、迅速に遮断を実施し、代替手段で業務を再開	• CSIRTが通常時から**サイバーセキュリティの情報収集を行い、CISOに頻繁に共有**していたことで、インシデント発生時の対処方法を迅速に決定できた。 • **外部組織との接続経路を管理**していたことで、迅速に遮断することができた。
7	• 職員が**マルウェアが添付されたEメールを受信し、感染** • CSIRTが感染端末を隔離し、代替端末にデータを移行し、業務への影響を最小限に抑えた	• サイバーセキュリティ**教育だけではインシデントを防げないため、システム面での対応**を並行して実施することが重要。 • 不審なメールを開封した際の対応手順書により、円滑な対処ができた。

事例１ 外部サービスの電源設備故障に伴う重要インフラサービスの停止 1／2

- 重要インフラ事業者は他事業者と共同で外部サービスを利用し、重要インフラサービスを提供していた。
- 外部サービスのシステム保守事業者による電源設備のメンテナンス中に故障が発生、同サービスを利用した重要インフラサービスの提供が一時停止した。
- 重要インフラ事業者は、あらかじめ定めていたシステム障害時の対応計画に従い、各部門が連携し、利用者への説明や代替策の案内を実施した。



事例１ 外部サービスの電源設備故障に伴う重要インフラサービスの停止 2／2

【１　背景】

- 重要インフラ事業者は、他事業者と共同で外部サービスを利用し、重要インフラサービスを提供していた。
- 外部サービスのシステム保守事業者（以下「保守事業者」という）のデータセンター内に複数のシステムが構築してあり、毎年設備のメンテナンスを行い正常性を確認していた。
- 電源設備はUPS経由と商用電源の2系統接続しており、故障時に無停電で切り替えられる設計となっていた。

【２　検知】

- 保守事業者がデータセンター内の複数システム停止を検知。
- 重要インフラ事業者のシステム部門が保守事業者から報告を受け、本事象を認識した。

【３　対処】

- システム部門は、経営層含めた各部門責任者に報告・連絡。経営層は対策本部を設置し、適時指示を実施。
- 対策本部からの指示を受け、従業員は各拠点に向かい、利用者に対して説明及び代替サービスを提供。遠隔地の拠点に対しては到着に時間を要した。
- 広報部門はグループ会社の広報担当者と連携し、Webサイト上で利用者への情報提供を実施。
- システム部門は保守事業者に復旧状況を都度問い合わせたが、保守事業者側の体制が不十分であり、復旧完了まで時間を要した。

【４　原因】

- 電源設備の年次メンテナンス中に故障が発生し、電源が遮断されたことで、データセンター内の電子機器が停止した。
- 電源設備は本来UPS経由のみ接続が許可されており、商用電源を直接接続することは電源設備機器メーカーは保証しておらず、メンテナンスや異常による接続切り替えの度に故障が発生しうる状況だった。
- 保守事業者は影響を受ける全ての事業者に対してサービスの復旧対応をする必要があったが、有識者が限られていたため、復旧に時間を要した。

【５　再発に備えた対策】

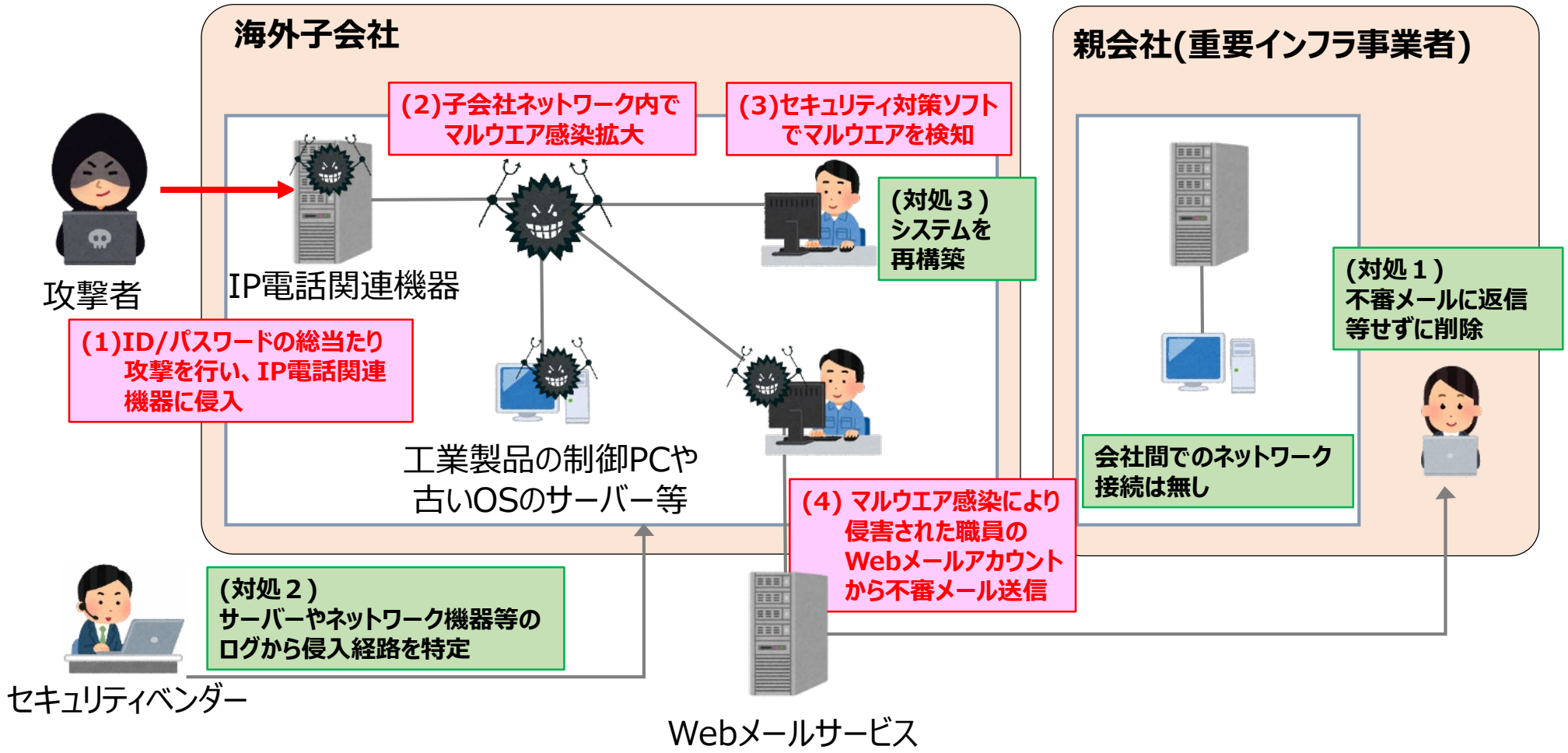
- 速やかに利用者対応するために、各拠点への到着時間などを基準に定め、訓練を通じて実効性を確認。
- 保守事業者に対して、同様の障害が発生した際に速やかに復旧対応できるように要請。
- 電源設備の接続系統についてメーカー推奨の構成に変更。

【6　得られた気付き・教訓】

- **外部サービスにおける緊急時の連絡体制**
  外部サービスでインシデントが発生した場合、利用している各事業者から保守事業者に問い合わせが殺到し、連絡に時間を要することがあった。どのような体制でインシデントをハンドリングしていくのか通常時に保守事業者や他事業者と議論して確認しておくべき。
- **作業リスクの判定基準の見直し**
  実績を重視した判断基準になっており、保守事業者は毎年実施しているメンテナンス作業であることからリスク低と判断した。結果、日中帯に作業を実施したことで故障時のサービス影響が大きくなった。データセンターの作業の主体は保守事業者だが、同作業がサービス提供に影響を及ぼす可能性について、重要インフラ事業者も十分に確認すべきであった。

事例２ OTの制御PC等のランサムウエア感染 １／２

- 重要インフラ事業者の海外子会社の職員が、セキュリティ対策ソフトでマルウエアを検知。
- 侵入されたIP電話関連機器（VoIPゲートウェイ装置）は、撤去予定だったがコロナ禍による出社自粛により撤去作業を延期していた。結果、ID/パスワードの総当たり攻撃による被害を受けた。
- 現地セキュリティベンダーと協力し、攻撃を受けた経路を特定、侵害されたシステムを1週間程度で再構築し、速やかに業務を再開した。



事例２ OTの制御PC等のランサムウエア感染 ２／２

【１ 背景】

- 重要インフラ事業者の海外子会社（以下「海外子会社」という）では、IP電話関連機器（VoIPゲートウェイ装置）を導入していた。
- IP電話関連機器は当初撤去予定だったが、コロナ禍による出社自粛により撤去作業を延期していた。
- 社内システムは工場設備含めてインターネット接続されていたが、工場設備（制御PC含む）は、セキュリティ対策が未実施だった。
- 社員の大半はテレワーク勤務しており、社内システムの大半はクラウド上に構成していた。
- 重要インフラ事業者と海外子会社間は直接ネットワーク接続されていなかった。
- 重要インフラ事業者は事業分野が広いため、様々な法令に対応する必要があり、連携先が多数ある。

【２ 検知】

- 海外子会社の職員が、社内サーバー上のセキュリティ対策ソフトでウィルスを検知し、調査したところ社内の複数機器がランサムウェアに感染していることを確認。
- 海外子会社の職員のアカウントから同社内および重要インフラ事業者宛に不審メールが送信されたことを確認。

【３ 対処】

- 侵害されたサーバー、PCをネットワークから隔離。
- セキュリティベンダーに調査を依頼し、サーバーやネットワーク機器等のログから侵入経路を特定。
- 不審メールは返信等せずに削除。
- システムを再構築し、業務を再開。

【４ 原因】

- IP電話関連機器にID/パスワード総当たり攻撃を受け、外部から不正アクセスされた。
- 組織内のほとんどの機器が同一ネットワークに接続しており、工業製品の制御PC等の製品仕様上セキュリティ対策ソフトが導入できない機器や古いOSで動作していたサーバーにマルウエアが感染拡大した。

【５ 再発に備えた対策】

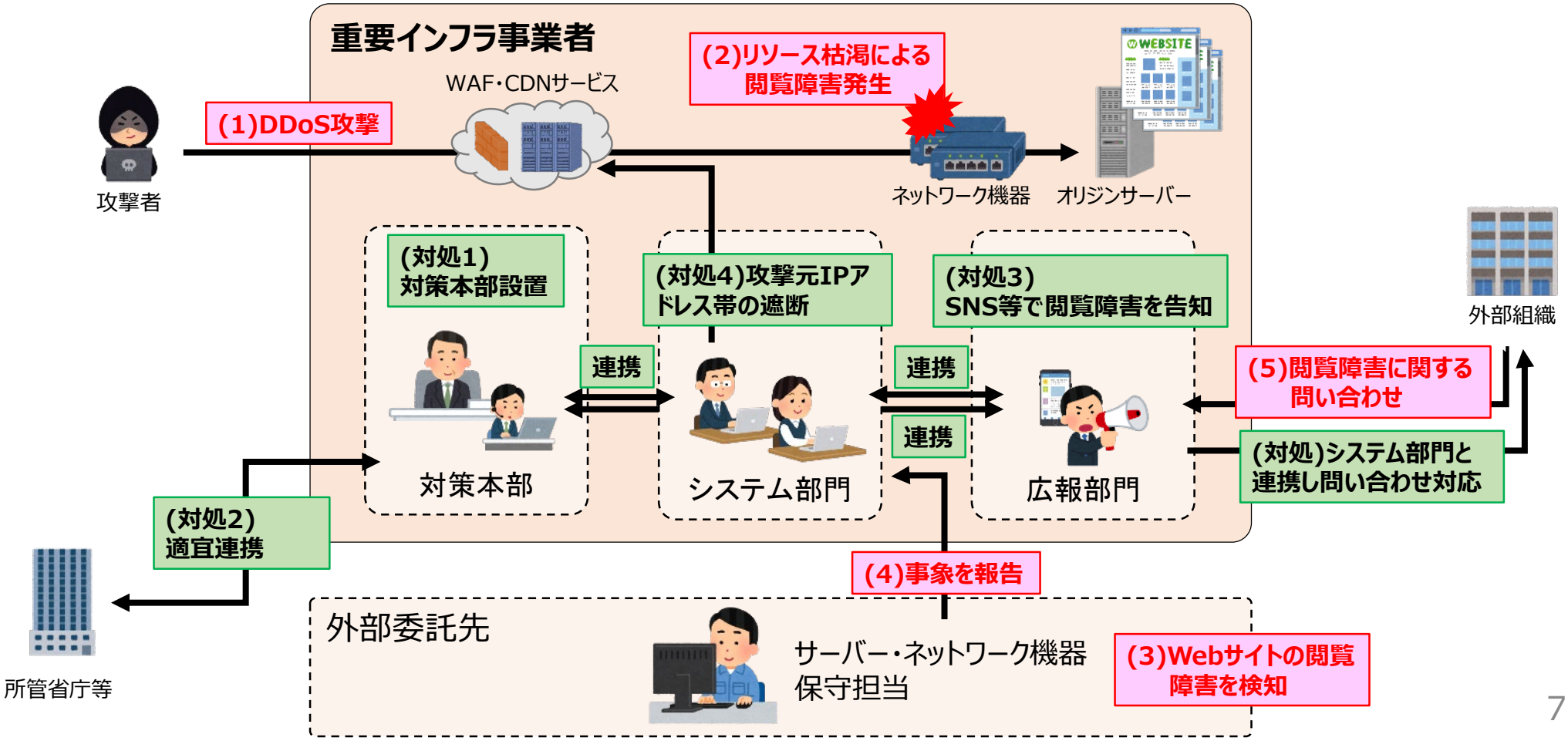
- システムを再構築し、外部からの侵入対策を実施。
- 重要インフラ事業者のグループ全体を統括するセキュリティ対策組織を構築。
- 国内外のグループ全体でOT関連機器含めたセキュリティ対策を強化。

【6 得られた気付き・教訓】

- **OT関連機器のセキュリティ対策強化**
  OT関連機器は事業者が勝手にパッチ適用できない（販売代理店のサポート対象外となってしまうことがある）ため、ベンダー及び**OT製品の販売代理店を含めて**素早く対応出来るよう協力体制を整える必要がある。
- **緊急時の連絡先の把握**
  各会社の事業内容や発生した事案に応じて報告先が異なるため、通常時に連絡先を整理し、把握しておくことが重要。
- **国や土地の文化に応じた対応**
  国外連携する際は、事象の表現や価値観の差異を考慮し、真意が伝わっているか話を掘り下げて確認する必要がある。

事例３ コーポレートサイト等へのDDoS攻撃による閲覧障害 1／2

- 重要インフラ事業者は、コーポレートサイトや重要インフラ関連サービスのためのWebサイトに対するDDoS攻撃を受けた。
- 重要インフラ事業者は、外部委託先から連絡を受け、社内規定に沿って迅速に対策本部を設置。システム部門や広報部門が連携し、SNS等の広報手段を活用した閲覧障害の告知や問い合わせ対応を実施した。
- 攻撃元IPアドレスの遮断によりWebサイトの閲覧が正常化したことを確認した。



事例３ コーポレートサイト等へのDDoS攻撃による閲覧障害 2／2

【１　背景】

- サイバー攻撃に備えたBCP等の組織内規定を整備していた。
- DDoS等のサイバー攻撃に備え、WAFやCDNを導入していた。

【２　検知】

- Webサーバーやネットワークの保守を担当する外部委託先において、コーポレートサイトや重要インフラ関連サービスのWebサイトに接続しづらい事象を検知した。
- 外部からWebサイトに繋がらないとの問い合わせを受けた。

【３　対処】

- 事象の検知後速やかに、組織内規定に沿って対策本部を設置し、経営層へ報告した。
- 所管省庁などに対し、適宜状況を報告した。
- 広報部門において、SNS等を通じてWebサイトにアクセスしづらい状況であることを発信した。また、外部からの問い合わせについてもシステム部門と連携して対応した。
- システム部門において、DDoS攻撃の送信元IPアドレスの多くを占める国からのアクセスを遮断した。
- Webサイトの閲覧が正常化したことを確認した。

【４　原因】

- CDNでは応答できない更新頻度の高いコンテンツへのアクセスにより、オリジンサーバーへの問い合わせが増大し、経路中のネットワーク機器のリソース枯渇が発生した。

【５　再発に備えた対策】

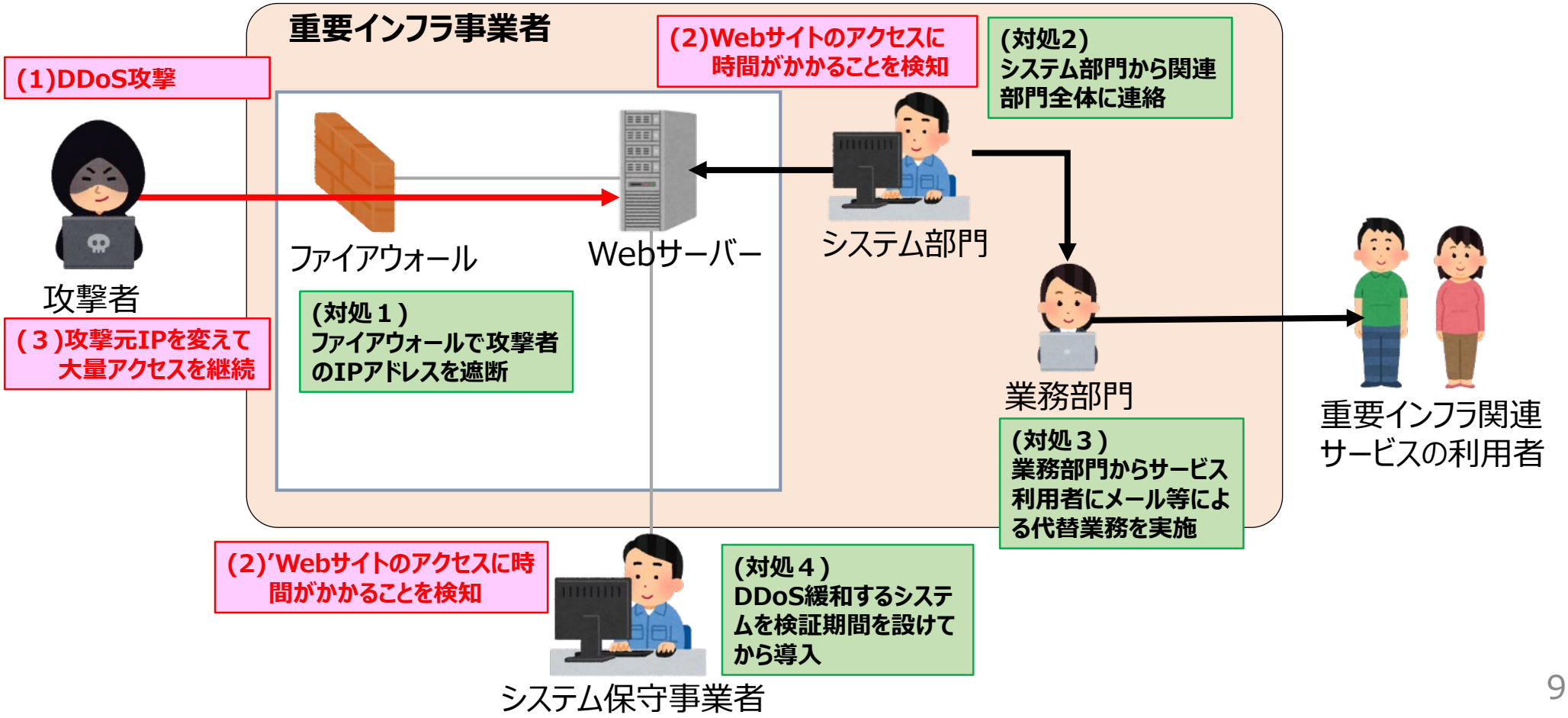
- インシデント発生時の速やかな初動対応体制や情報連携を強化する。
- 以前から実施しているサイバー攻撃に備えた訓練について、今回の対処内容を踏まえ、部門を横断してシナリオを再確認した。

【６　得られた気付き・教訓】

- **組織内規定の整備や事前準備の重要性**
  インシデント発生時やサイバー攻撃被害の恐れを検知した時の体制は組織内規定として明文化されており、指揮命令系統が明確であったため、迅速に判断を行うことができた。また、意思決定者や事案時系列共有のためのフォーマットを整備していたことが円滑な対処に繋がった。
- **インシデント対応訓練の重要性**
  サイバー攻撃による被害を想定した訓練を実施していたことから、組織内や所管省庁等との連携を含めインシデント発生時の対処を速やかに行えた。
- **障害発生時の広報手段の確保の重要性**
  閲覧障害の発生したコーポレートサイト以外にもSNS等の広報手段を準備していたことにより、顧客等を含む関係者への周知を行えた。
- **IT資産の適切な管理の重要性**
  事象の検知から原因の特定までをより迅速に実施するため、IT資産や構成図等の管理を適切に行うことが重要。適切な管理により、効率的な対処を実施できる。
- **対処に伴う作業の属人化防止**
  CDNやWAFサービスでWebサイトへのアクセス量等を閲覧できる人員が限られるアカウント運用となっていた。非常時には適宜アカウントを付与する等、複数人が対応できるよう運用とすべき。

事例４ 利用者向けWebサイトへのDDoS攻撃によるスローダウン １／２

- 重要インフラ関連サービスのWebサイトに大量のアクセスが発生し、一時スローダウンした。
- 重要インフラ事業者の職員がWebサイトへのアクセスに通常より時間がかかることに気づいたため、システム保守事業者に調査を依頼したところ、国外から大量のアクセスを受信していることが判明。
- 攻撃元IPアドレスを特定して遮断したが、IPアドレスを変えて攻撃が継続したため、Webサイトを一部停止。メール等による代替業務を行いながら、DDoSを緩和するためのシステム的な対処を行うことで、後日全面復旧することができた。



事例４ 利用者向けWebサイトへのDDoS攻撃によるスローダウン １／２

【１　背景】

- 重要インフラ事業者は重要インフラ関連サービスのWebサイトを運営しており、法人及び個人の利用者が利用していた。

【２　検知】

- 重要インフラ事業者の職員が、Webサイトにアクセスする際に通常よりも時間がかかることに気づき、システム不具合の可能性を考慮して、システム保守事業者に連絡した。
- 同時タイミングでシステム保守事業者もWebサーバーのスローダウンを検知した。

【３　対処】

- システム保守事業者によりWebサーバーの状態を確認したところ、国外から大量のアクセスを受信したことで、リソース不足となりスローダウンが発生していることを確認。
- システム部門からシステム保守事業者に対して、当該IPアドレスの遮断を依頼。
- システム部門から業務部門に連絡し、Webサイトを使わないメール等による代替業務を実施。
- Webサーバーに対して、接続元IPアドレスを変えた攻撃が継続したため、Webサーバーを停止。
- DDoS以外にフィッシングメール等の複合攻撃が発生する可能性があるため社内に注意喚起。

【４　原因】

- 外部からの攻撃に備えてファイアウォールは設置していたが、DDoSに特化した対策はしていなかった。

【５　再発に備えた対策】

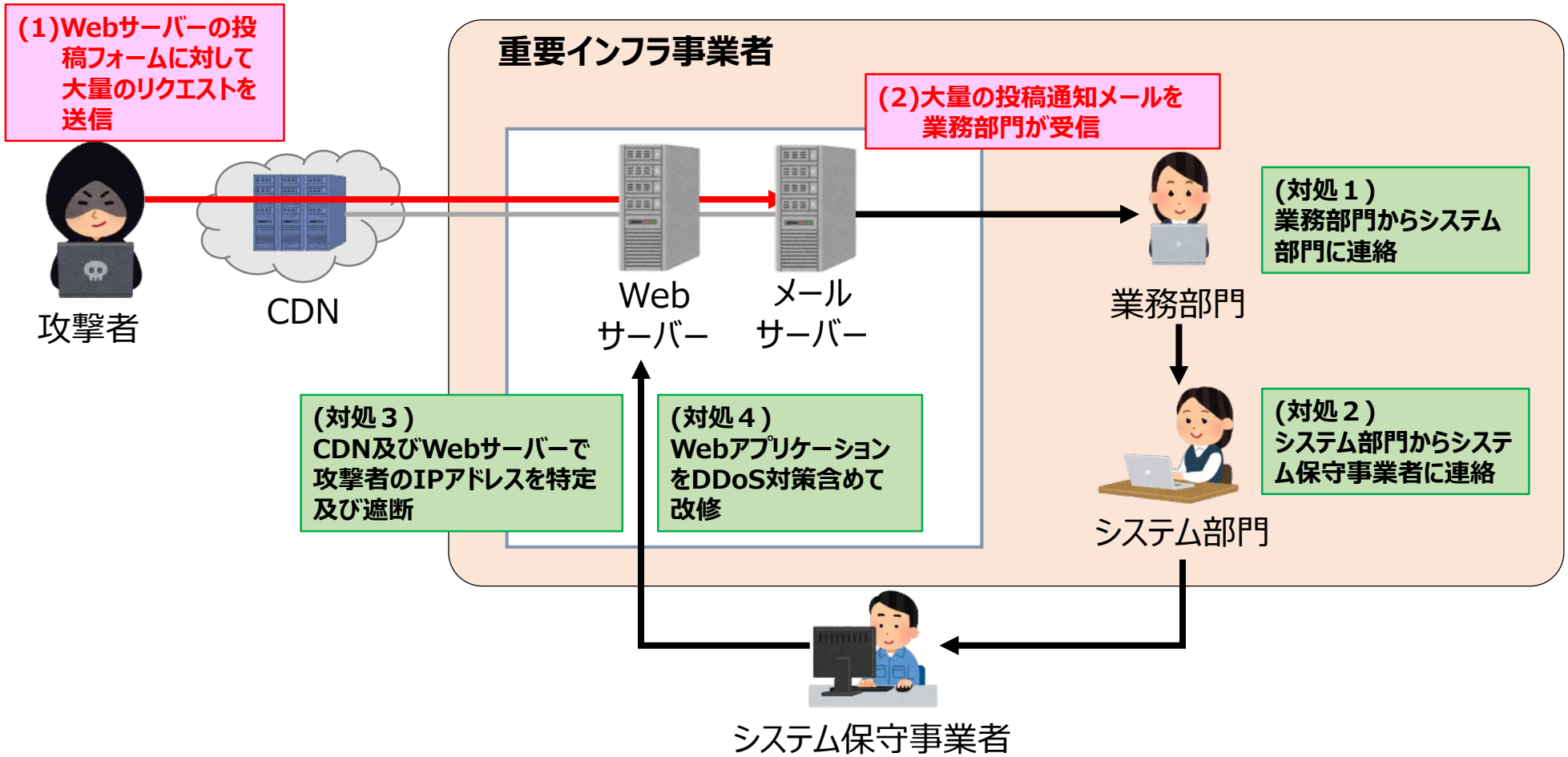
- クラウド型のWAFを導入。
- Webサイト上の投稿フォームにCAPCHA機能を追加し、機械的なアクセスをブロック。

【6　得られた気付き・教訓】

- **DDoSに特化した対策の必要性**
  Webサーバーについては外部からの不正侵入を防ぐためにファイアウォールを設置していたが、業種及び規模から、DDoSのターゲットとして自組織が狙われるという意識が低く、CDNやWAF等のDDoSに特化した対策はしていなかった。
- **職員へのサイバー攻撃に関する教育**
  不審メール等の職員を狙った攻撃の訓練や教育は定期的に行っていたが、DDoS等のシステムへのサイバー攻撃に関しては職員向けの教育はしていなかった。本件ではDDoS対策が全て完了するまでに時間を要したが、組織内においてはDDoS対策の重要性や後から導入することの難易度の高さについて認識が無かったため、組織内の協力を得やすくするためにも攻撃事例等を学習する機会を設けると良い。
- **サイバー攻撃に対する危機意識の醸成**
  システム更改時にDDoS対策を含めることを元々予定していたが、ベンダー都合により延期していた。サイバー攻撃に関する危機意識が高ければ、システム更改時以外での攻撃に備えた準備等を行うことができたと考えらえる。業種及び規模から、狙われやすい分野だけが攻撃を受けるのではなく、インターネットに公開している機器については誰でも狙われるという意識を持つことが重要。

事例５ Webサイトの問い合わせフォームへのDoS攻撃 1／2

- 重要インフラ関連サービスの利用者向けWebサイトには投稿フォームがあり、利用者が投稿すると業務部門の職員にメールで通知される仕組みとなっていた。
- ある日、短時間に大量の通知メールを受信したことで、異常が発生していることを検知。
- 攻撃元IPアドレスを特定し、CDN及びWebサーバーで遮断し、後日Webアプリケーションの改修をすることで、同様の攻撃への対策を行った。



事例５ Webサイトの問い合わせフォームへのDoS攻撃 1／2

【１　背景】

- 重要インフラ関連サービスの利用者向けWebサイトに投稿フォームがあり、利用者が投稿すると業務部門の職員にメールで通知される仕組みとなっていた。

【２　検知】

- 重要インフラ事業者の職員が、大量の投稿通知メールを受信していることに気づき、投稿内容も不審なものだったため、業務部門の情報セキュリティ管理者に報告。

【３　対処】

- 業務部門の情報セキュリティの管理者がシステム部門の責任者に連絡したが、業務時間外で不在だったため、システム部門の職員と連携し、システム保守事業者に連絡を実施。
- Webサーバーの状態を確認したところ、国外の単一IPアドレスから大量のアクセスを受信していることが判明。
- システム部門からシステム保守事業者に対して、CDN及びWebサーバーでの当該IPアドレスの遮断を依頼。
- 検知から対処完了まで1時間程度で対応を完了しており、スローダウンやサーバー停止は発生していない。
- 対処後に、警察や所管省庁への連絡実施。

【４　原因】

- 通常、利用者はWebサイト上の投稿フォームに情報を入力して送信するが、投稿フォームのURLに直接アクセスすることで、Webサイト上の投稿フォームを介さずに投稿することが可能となっていた。そのため、 投稿を連続で受け付けやすい状態となっていた。

【５　再発に備えた対策】

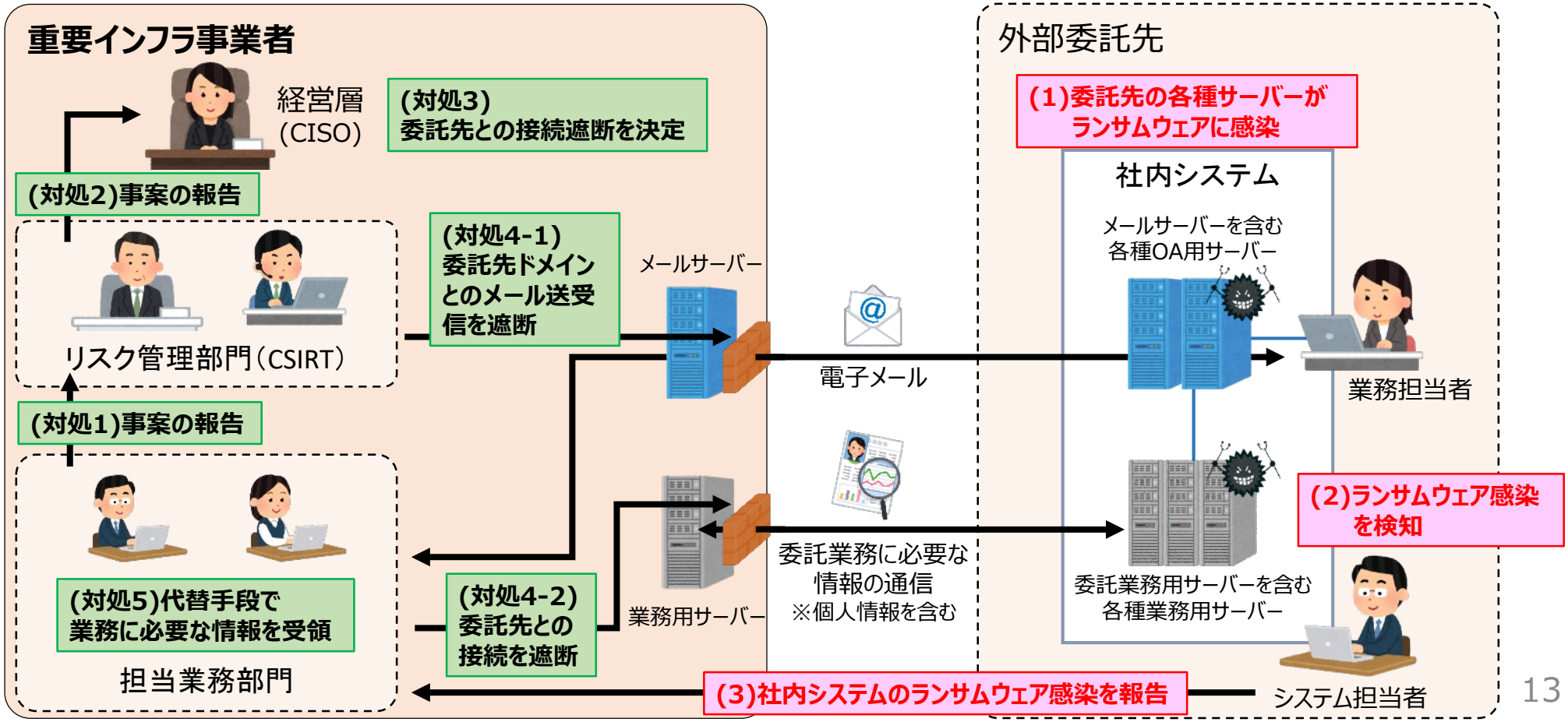
- Webサーバーに対して直接リクエストを送信できないようにWebアプリケーションを改修。
- WAFを導入。（本事案以前より導入を計画していたもの）

【6　得られた気付き・教訓】

- **緊急連絡体制の確認の重要性**
  システム保守事業者でしか対応出来ない作業があるため、有事の際の緊急連絡体制の確認が重要。今回は業務時間外に発生したため、責任者が不在だったが、連絡先を事前に整理していたために電話でやりとりをして対処することができた。想定される事案毎に連絡先を整理することで、即座に対応できた。
- **システム構成の理解の重要性**
  職員がシステム構成を把握していたため、攻撃を検知後にどのように対処すべきか迅速に判断することができた。複数名で同じ業務を行ったり、ドキュメントを作成して引き継ぎすることで、属人化を防いでいる。
- **DDoSに特化した対策の重要性**
  本事案では攻撃者の接続元が単一のIPアドレスだったため、遮断することができたが、多数のIPアドレスから同時に攻撃が来た場合に防げたかどうかは不明であった。そのため、後日WAFを導入することで、DDoS対策を強化している。
- **サイバーセキュリティ関連業務の人材育成**
  現在はWAF等の機器について、システム保守事業者に依頼して設定変更等を行っているが、システム保守事業者不在時に備えて職員でも操作できるようにするために人材育成が必要。

事例６ 外部委託先サーバーのランサムウェア感染 1／2

- 重要インフラ事業者は、業務の一部を外部の事業者に委託していたが、委託先のサーバーがランサムウェアに感染し、当該業務が停止した。
- 重要インフラ事業者は、委託先との接続経路を特定し、迅速に遮断を実施。遮断後、重要インフラ事業者側の二次感染がないことを確認した。
- 重要インフラ事業者は、委託先による原因調査結果および再発防止策を確認後、委託先のシステム上の接続を再開した。



事例６ 外部委託先サーバーのランサムウェア感染 2／2

【１　背景】

- 重要インフラ事業者は業務の一部を外部の事業者に委託しており、業務上必要な顧客の個人情報を含む情報を当該委託先へ提供していた。
- 経営層（CISO）とリスク管理部門（CSIRT）が定期的に情報共有を行っていた。

【２　検知】

- 委託先が社内システムのランサムウェア感染を検知し、重要インフラ事業者の担当業務部門へ報告した。

【３　対処】

- 担当業務部門がCSIRTへ、CSIRTがCISOへ、それぞれ事案を報告した。
- 重要インフラ事業者側システムへの感染を防ぐため、CISOが委託先との接続経路の全ての遮断を迅速に決定した。
- 委託先との接続経路を遮断するため以下の対応を実施した。
  - 社内CSIRTが委託先ドメインのメールアドレスとのメール送受信を遮断
  - 委託先ネットワークとの接続を有し個人情報を扱うシステムについて、担当業務部門が委託先との接続を遮断
  - 重要インフラ事業者側システムへの二次感染の有無を調査
- 委託先との接続遮断の間、電話等の代替手段で業務を継続した。
- 委託先による復旧作業や調査結果の受領、再発防止策の受領の後、重要インフラ事業者が接続経路の遮断を復旧した。

【４　原因】

- 委託先のサーバーが第三者からのサイバー攻撃によりランサムウェアに感染した。

【５　再発に備えた対策】

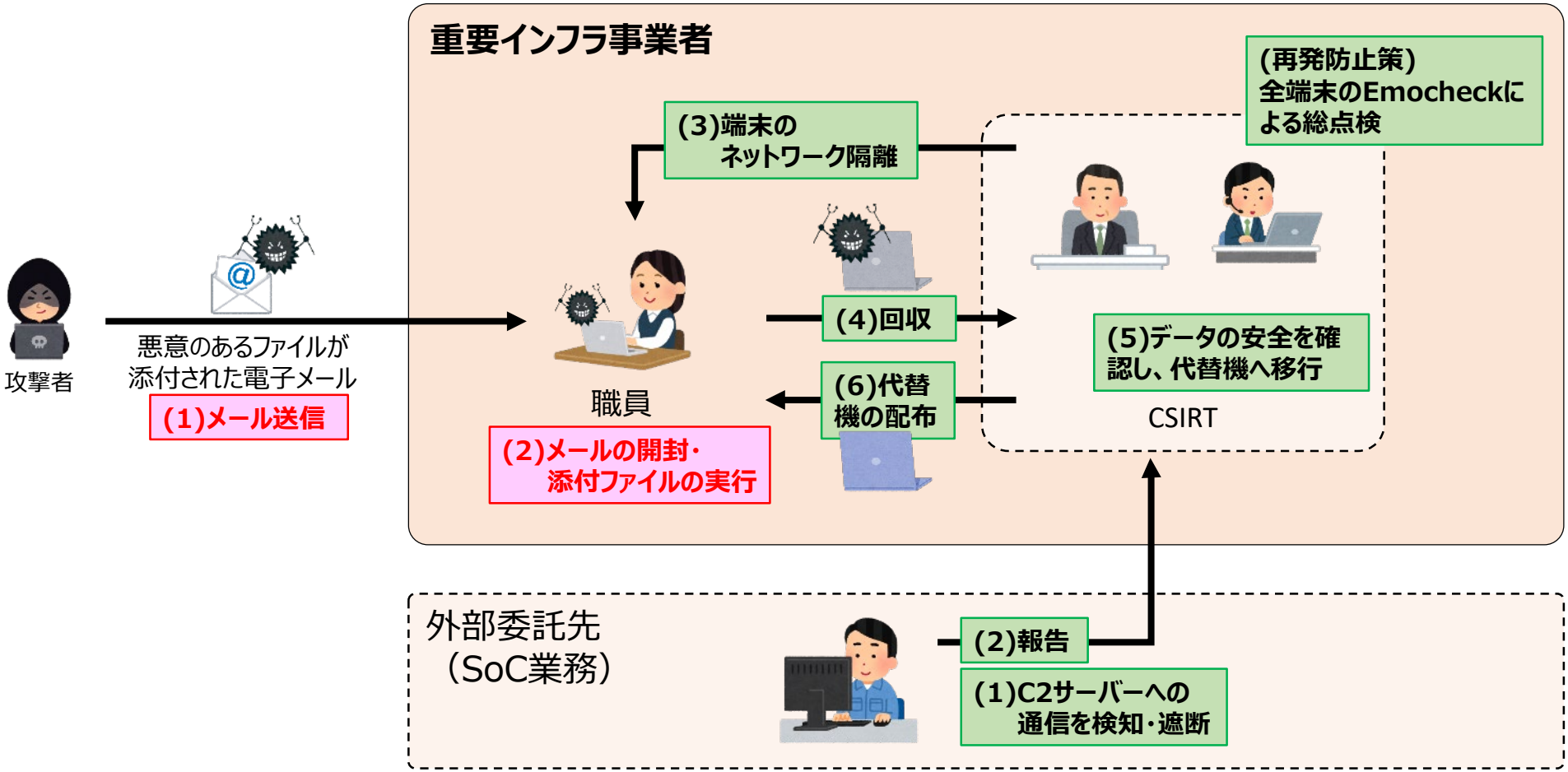
- 事案以前から実施している委託先の定期的な調査について、データの暗号化や取扱管理、入退出管理等のサイバーセキュリティに関する項目を調査項目として新たに追加した。
- 事業継続計画（BCP）について、サイバー攻撃に関する項目（バックアップの取得等）を新たに追加した。

【6　得られた気付き・教訓】

- **情報収集とCISOとの情報共有**
  CSIRTは、サイバーセキュリティに関する情勢の把握やその対処方法、社内のサイバー攻撃被害状況（不審メールの受信数等）等について情報収集を実施していた。これらの情報を本事例発生前から頻繁にCISOと共有していたことにより、本事例発生時の対処方法を迅速に決定できた。
- **外部組織との接続経路の管理**
  外部組織との接続経路を管理していたことにより、委託先との接続経路の遮断を、CSIRTと担当業務部門が連携し、迅速に不足なく実施できた。
- **緊急時の連絡先の把握**
  委託先との接続経路を遮断した後、委託先との連絡手段が限られた。連絡先の把握や定期的な更新が重要である。

事例７ Eメール添付ファイルの実行によるマルウェア感染 1／2

- 重要インフラ事業者の職員が悪意のあるファイル（Emotet）が添付されたEメールを受信し、添付ファイルを開きマクロを実行した。
- SoC委託事業者において、マルウェアによるC2サーバー宛の通信を検知し、通信を遮断するとともに重要インフラ事業者へ報告した。
- 重要インフラ事業者はマルウェアが実行された端末を隔離し、業務に必要なデータを代替端末へ移行した。



事例７ Eメール添付ファイルの実行によるマルウェア感染 2／2

【１　背景】

- 受信メールの監視システムを活用し、悪意のあるメールを自動判別して職員に届かないよう対策を講じていた。
- 組織内にCSIRTを常設し、職員からの問い合わせの受け付けや不審な通信を検知する体制を構築していた。
- 職員がEメールに添付された悪意のあるファイル（Emotet）を開き、マクロを実行した。

【２　検知】

- SoC業務の委託事業者において、マルウェアによるC2サーバー宛の通信を検知・遮断し、CSIRTへ報告した。

【３　対処】

- CSIRTから当該職員へ連絡し、被疑端末をネットワークから隔離するとともに、当該端末を回収した。
- CSIRTが被疑端末で感染確認ツール（EmoCheck※）を実行し、マルウェアへの感染が判明した。
- CSIRTにおいて、感染端末にある業務に必要なデータを抽出し、サンドボックス環境においてデータの安全を確認した。
- CSIRTにおいて、代替端末に業務に必要なデータを移行し、当該職員へ配布し迅速に業務を再開した。

【４　原因】

- Eメールに添付された悪意のあるファイルがパスワード付きZIP形式で暗号化されていたことで受信メール監視システムにおいてメールの判別や遮断を実施できなかった。
- 注意喚起を実施していたものの、職員が添付ファイルを開きマクロを実行した。

【５　再発に備えた対策】

- 職員向けポータルサイト等を通してEメールを媒介としたマルウェアに関する注意喚起を実施した。
- 全端末でEmoCheckを実行し、感染がないことを確認した。
- 全職員向けに定期的に実施しているサイバーセキュリティ研修において、本事例の紹介を内容に含めた。

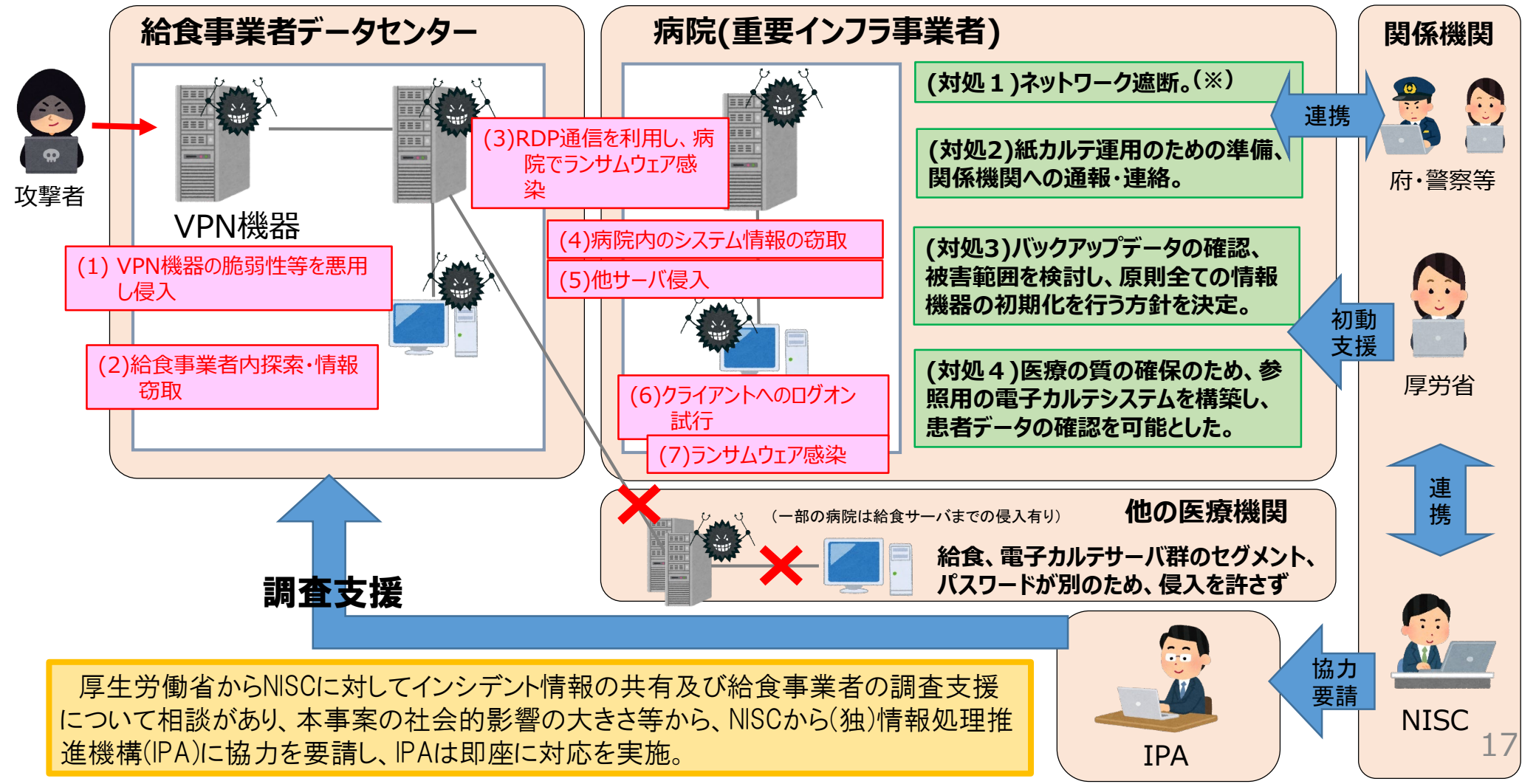
【6　得られた気付き・教訓】

- **サイバーセキュリティ教育とシステムにおける対策**
  サイバーセキュリティに関する研修や訓練を定期的に実施しているが、セキュリティ意識には個人の差が生まれてしまい全職員の水準を均一に向上させることが難しい。このため、迅速なセキュリティパッチ適用などのシステム面での対応を並行して実施する。
- **インシデント発生時の連絡体制整備の重要性**
  職員が不審なメールを受信した際や開封した際の連絡先を含め、対応手順書を整備していたことにより、円滑な対処を行えた。
- **組織内ネットワークの一元管理**
  CSIRTの所属する部門が組織内ネットワークを管理しており、組織内のネットワーク構成を一元的に確認できた。これにより、C2サーバー宛通信の検知や遮断、不審な通信の有無の確認を迅速に実施できた。

※JPCERTコーディネーションセンター「EmoCheck」
https://github.com/JPCERTCC/EmoCheck

（参考） 大阪急性期・総合医療センターのランサムウェア感染事案 1／2

- サプライチェーンの給食事業者のVPN機器の脆弱性等を悪用され、給食事業者データセンターに侵入、リモートデスクトップ（RDP）通信を経由し、大阪急性期・総合医療センター（以下「病院」）のサーバがランサムウェア感染。
- 病院は速やかに紙カルテ運用の準備を進め、関係各所に連絡、厚生労働省の初動対応支援の専門家チームを加えたシステム復旧会議を開催し復旧方針を決定。医療の質の確保のため、参照用の電子カルテシステムを構築し、患者データの確認を可能とした。
- 同様に給食事業者とネットワーク接続していた他の医療機関では、不正アクセスの痕跡等はあったが、大事には至らなかった。



厚生労働省からNISCに対してインシデント情報の共有及び給食事業者の調査支援について相談があり、本事案の社会的影響の大きさ等から、NISCから(独)情報処理推進機構(IPA)に協力を要請し、IPAは即座に対応を実施。

（※）地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター情報セキュリティインシデント調査委員会調査報告書(2023年3月28日)より、NISCがインシデント対処のポイントとなると考えた箇所から作成。

（参考） 大阪急性期・総合医療センターのランサムウェア感染事案 2／2

【1 背景】

- 病院は給食提供委託契約を締結していた給食事業者とRDP通信で常時接続していた。

【2 検知】

- ランサムノート表示、暗号化に職員が気づき、システムベンダーの調査により感染を把握。

【3 対処】

- ネットワーク遮断。
- 紙カルテ運用のための準備、関係機関への通報・連絡
- バックアップデータの確認、被害範囲を検討し、原則全ての情報機器の初期化を行う方針を決定。
- 医療の質の確保のため、参照用の電子カルテシステムを構築し、患者データの確認を可能とした。

【4 原因】

- サプライチェーンのVPN機器の脆弱性が放置されていた。
- リモートデスクトップ通信(RDP)接続が常時接続となっていた。
- ユーザー全てに管理者権限を与えていたため、攻撃者に管理者権限を利用された。
- Windowsのパスワードが、サーバ、端末毎に全て共通であった。
- アカウントロックアウトの設定が無く、パスワード総当たり攻撃や辞書攻撃によりパスワードを数多く試行されログオンが成功した。
- 電子カルテシステムの一部サーバにウィルス対策ソフトが未設定。

【5 再発に備えた対策】

- ユーザーは管理者権限のない標準ユーザーに変更、ID・パスワードの共用を禁止、強力なパスワードに変更、アカウントロックの設定有効化、ウィルス対策ソフト設定。

【6 得られた気付き・教訓】（甚大な被害に至らなかった医療機関との差を中心に）

- **情報機器のパスワード、セグメントの個別化**
  侵入されたサーバと電カルシステムのパスワード、セグメントが共通であったため、容易に攻撃者の横展開を許した。これらは個別化することが重要。
- **IT資産管理の徹底**
  外部と接続する機器について、自組織が設置した機器のみならず業務委託先が設置する機器を含めてネットワーク構成図等を作成し、定期的に棚卸しすることで、全ての機器を漏れなく管理出来ているか、業務委託先との責任分界点・役割分担も含めて確認することが重要。また、OSのサポート期限やライセンス等が切れる前に機器を更改し、常に最新のパッチ適用等を適切に運用できているか確認し必要な対応をとることが重要。
- **組織内での不正な通信を検知する仕組みの強化**
  病院のネットワークセキュリティは境界防御を基本としており、外部からの侵入に対しては防御・検知する仕組みを構築していた。しかし、病院ネットワーク内の通信については防御・検知が不十分だったため、内部に入られた後の動きについても防御・検知する仕組みが重要。
- **関係機関との連携**
  NISC及び厚労省が連携し、IPAに給食事業者の調査支援に係る協力要請をして被害拡大防止に努めた。所管省庁、NISC、関係機関の協力・連携をより進めていくことが重要。