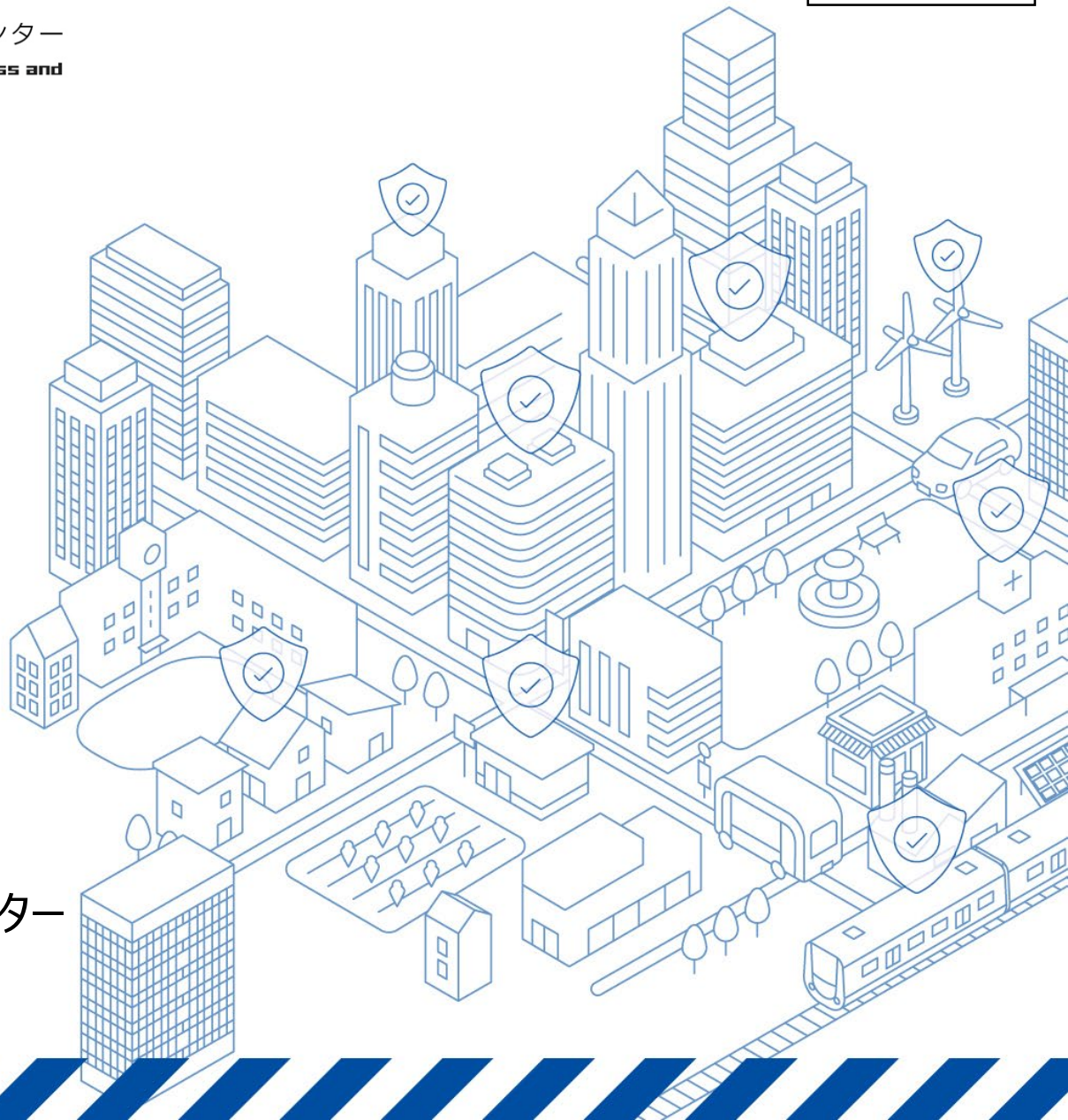
資料６

NISC 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



サイバーセキュリティ戦略本部
重要インフラ専門調査会（第39回）

重要インフラにおける補完調査について [2024年度]

2025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

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、2024年1月1日～2024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

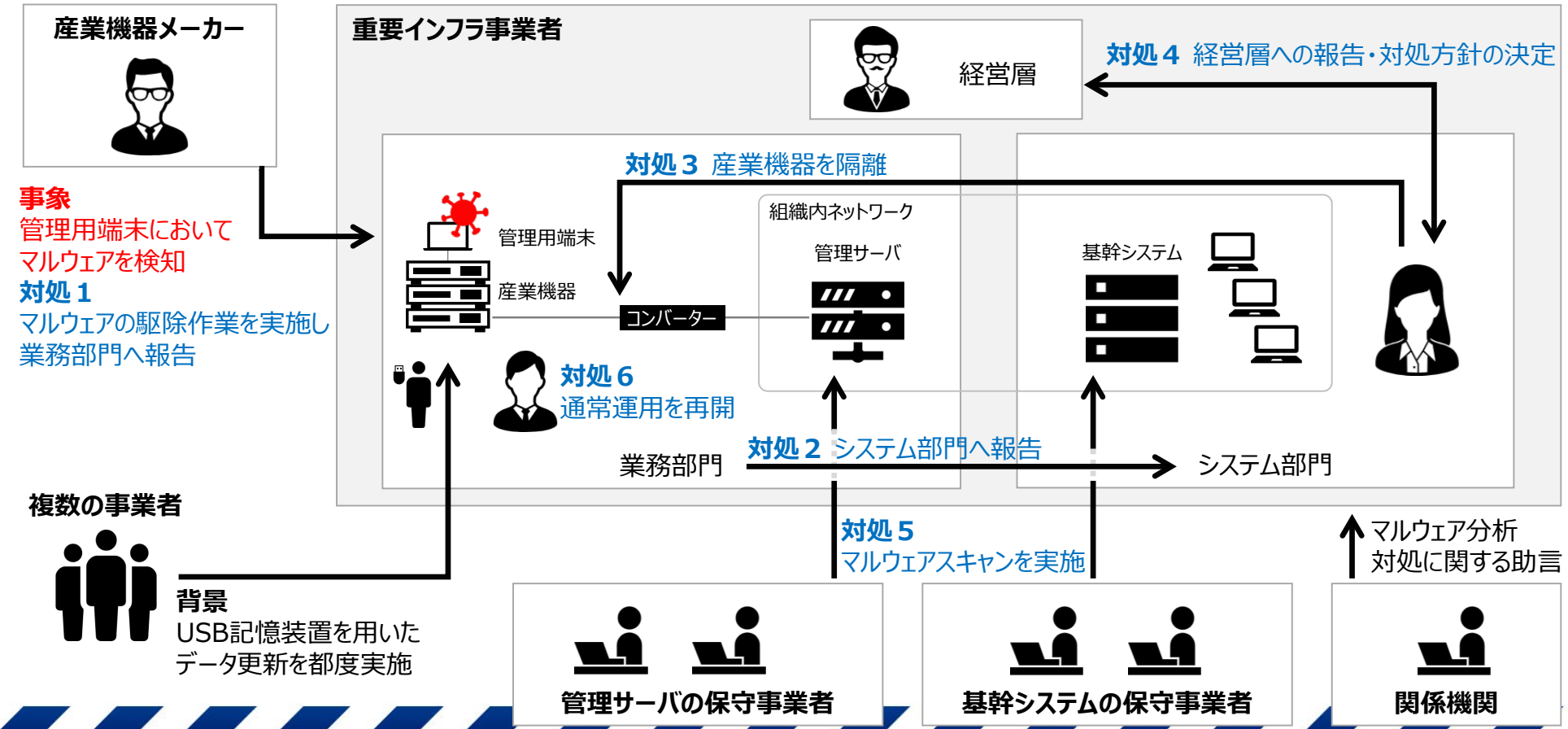
	事例の概要	主な気づき・教訓
サイバー攻撃に起因した重要インフラ関連サービスの障害		
1	• 管理が行き届いていないUSB記憶装置を用いたデータ更新を行っていた**産業機器においてマルウェアを検知**し、当該機器を隔離。 • 関係機関の助言を受けながら**周辺システムの健全性を確認**した後に、通常運用を再開。	• システムへのUSB接続を黙認していたことは**管理不足**と言わざるを得ない。USB接続をなくせない場合であっても、**都度ウイルススキャンを実施したUSBでメーカーに作業を実施させる**等の管理が必要。 • 産業機器において**サイバーインシデントが発生した際の影響**等について、重要インフラ事業者と機器メーカーとの間の**認識に違い**があった。平時から関係者と共通理解を持つことが重要。
2	• 基幹システムが**ランサムウェア感染**により停止したことを受け、BCP用端末及び人的対応により重要インフラサービスの提供を継続。 • **マルウェアの残留やバックドア設置の可能性**があったため、**基幹システムを新規構築**。その際、オフラインバックアップではなく他システムに蓄積していたデータを基に実施。	• **脆弱性情報の入手やその評価**、また、**脆弱性の修正を管理する台帳**を作成し都度、**評価やソフトウェア更新を行う体制を整える**ことが重要。 • **オフラインバックアップ取得を保守事業者に委託**していたものの、**作業不備**により本事例の対処に用いることができなかった。**作業手順の整備や確認**が重要。 • ランサムウェア感染以前より、特定サーバーの障害が複数発生。攻撃の兆候であった可能性も考えられ、**障害対応においてサイバー攻撃の可能性も考慮しつつ原因を究明**することが重要。
3	• 重要インフラサービスに組み込んでいた認証サービスが**DDoS攻撃**を受け、**認証機能が一時停止**。 • あらかじめ定めていた**対応手順や判断基準に基づいて対応、連携**。事象の重大性を鑑みて、経営層レベルで働きかけをし、認証サービス提供事業者と**直接コミュニケーションを取る体制を構築**。	• **組織を超えたリアルタイムな情報共有を行うこと**は、スピード感のある対応に繋げられる意味で有用と思われる。 • 被害発生の際に、**誰が何をどのように行うか事前に想定し、明文化しておくこと**が重要。併せて平時から訓練を実施し、関係者の理解を深め、**インシデント発生時に役員含めた関係者すべてが集まる文化を醸成する**ことも重要。
4	• クラウド上に構築された**Webサイト**が**DDoS攻撃**を受け、**閲覧障害**が発生。 • **緊急時の連絡体制表を用いて**経営層を含めた各部門責任者に報告・連絡。**システムの優先度を勘案して**、システム部門を中心に各種対処を実施。	• 被害を受けたことで既存のセキュリティ対策を見直し、その後発生した攻撃での被害を抑えることができた。**既存の対策を見直して継続的に改善すること**が重要。 • リソースが不足する中で、人材を増やす、高度なセキュリティ製品を導入するといったリソースを必要とする施策の他に、サイバー保険への加入といった**限られたリソースで実施可能な施策がないか検討すること**が重要。
5	• 開発/運用を委託していたWebサイトにおいて、**アプリケーションの作り込みの際に生じた脆弱性をついたサイバー攻撃**が発生し、**個人情報を含む情報が流出**。 • **CSIRT体制を持つ情報管理部門**を中心に、対応の協議、委託先への指示、被害公表等の**各種対処**を実施。	• システム開発にあたって開発委託元が実施できる方策としては、**委託契約時の仕様書に盛り込むセキュリティ要件を充実させる**こと、**外部認証の取得有無等の基準を設定して開発委託先組織のセキュリティ対策状況を評価する**ことが考えられる。

補完調査の対象事例一覧

	事例の概要	主な気づき・教訓
システム不具合に起因した重要インフラ関連サービスの障害		
6	• **セキュリティ製品パッチに不具合**があり、当該パッチが配信された機器が異常停止したことで**複数システムが機能を停止**。 • **体制/対応手順/システム一覧に沿って**対策本部を立ち上げ、各種対処を実施。サーバーについては**障害発生日中に復旧**させ、**重要インフラサービスへの影響を最小限に抑えた**。	• **資産管理が適切に行われて**おり、事業継続の観点から、どのシステムを優先的に復旧させるべきなのか、**速やかな対応優先度の判断が可能**となった。 • **平時から**システム障害を見据えた**対応体制や手順を整備し、訓練すること**により**「対応の型」というべきものを醸成しておくこと**が重要。
7	• **SSL証明書の更新**の際、**未把握の仕様に起因してエラーを発生させてしまう不備**があり、重要インフラ事業者を含む**複数事業者のWebサービスへのアクセス障害**が発生。 • **障害対応フローに従って**緊急時の対応体制を整え、**情報共有及び復旧作業**を実施。	• システムの要件定義・基本設計の段階から**稼働に影響の大きい仕様を把握する**とともに、不測の事態が発生しても早急に対応・復旧できる**対応手順の明文化**が必要。 • **平時から緊急時の障害対応フローを整備**し、**定期的に訓練を実施**することで緊急時の対応に備えておくことが重要。
8	• 想定外の大量データを受付け、それに対応するデータベースの検索結果が全件エラーとなったことに伴い、データベースの過負荷が発生。 • **事前に定められた手順に則り対処**し、過負荷の原因となった処理の改修によって重要インフラサービスの処理遅延を解消。	• 本事例の対処の際、特定の人員に対応が集中してしまった。**役割分担の明確化**や**人員毎の作業負荷の均等化**を予め検討することが重要。 • **システム障害対応訓練の実施**を通じて、各部門やシステム保守事業者の**役割分担の確認**や障害発生時の**要員を想定どおり確保可能であるか**等を平時より確認することが重要。
9	• ホストと産業機器の通信を中継するサーバーの障害により、**各拠点に設置された産業機器の一部が使用不能**。 • 当該サーバーをネットワークから切り離し、使用不能となった産業機器を再起動したことにより復旧。	• 過去のシステム障害における教訓等に基づき、**平日日中や夜間、休日のそれぞれの連絡・報告体制を整備**していたことにより、円滑に対処。 • **システム障害の規模等に応じた報告基準や、各種報告内容のテンプレート**を整備していたことにより、組織内の関係部門等と円滑に情報を共有。 • **経営層を含む対応訓練を定期的に実施**していたことにより、本事例の対処においても経営層が現場で指揮。

事例１：USB記憶装置経由と考えられる産業機器のマルウェア感染 1／2

- 重要インフラ事業者は産業機器を運用しており、データ更新のため複数の事業者がUSB記憶装置を当該機器の管理端末へ都度接続していた。
- 産業機器の定期メンテナンス時に、当該機器に接続された管理用端末においてマルウェアが検知された。
- 重要インフラ事業者は直ちに産業機器を隔離し、周辺システムの保守事業者やサイバーインシデント対応に関する知見のある関係機関と共に対処にあたり、マルウェアの拡散の可能性が極めて低いことを確認した上で通常運用を再開した。



事例１：USB記憶装置経由と考えられる産業機器のマルウェア感染 2／2

１．背景

- 重要インフラ事業者の業務部門は産業機器を運用しており、当該機器はコンバーターを介して管理サーバへ接続されていた。
- 産業機器の定期メンテナンスを当該機器のメーカーが実施していた。
- USB記憶装置を用いた当該機器のデータ更新を複数の事業者が都度実施していた。
- 業務部門が運用する機器等について、外部記憶装置の接続に関する管理が行き届いていなかった。

２．検知

- 産業機器のメーカーが実施する定期メンテナンスにおいて、当該機器に接続された管理用端末のマルウェアスキャンを実行したところ、マルウェアを検知した。

３．対処

- 産業機器のメーカーは、マルウェアの検知後、マルウェア駆除作業を実施した。その後、重要インフラ事業者の業務部門へ本事象を報告した。
- 業務部門はシステム部門へ本事象を報告し、報告を受けたシステム部門は、産業機器を物理的に隔離した。
- システム部門は事前に定められたCSIRT体制に基づいて経営層へ本事象を報告し、産業機器をオフラインで稼働させる方針を決定した。
- 管理サーバと基幹システムの各保守事業者は、全てのサーバー及び端末のマルウェアスキャンを実施し、マルウェアは検出されなかった。
- システム部門、管理サーバの保守事業者、基幹システムの保守事業者及び知見のある関係機関の４者による協議を実施した。前述のマルウェアスキャン結果や産業機器がコンバーターを介して管理サーバへ接続されていることを踏まえ、管理サーバー等のマルウェア感染の可能性は極めて低いと判断した。
- システム部門が主導して、業務部門との調整や関係機関の協力を得て迅速な対応を行ったことにより、マルウェア検知の翌日には、産業機器を管理サーバーへ接続し通常運用を再開することができた。

４．原因

- 産業機器に接続された管理用端末のUSB接続が有効であったこと、データ更新の際にUSB記憶装置が接続されていたこと及び関係機関によって分析されたマルウェアの特徴から、USB記憶装置が感染経路であった可能性が高い。

５．再発に備えた対策

- 産業機器に接続された管理用端末において、USB接続ポートを物理的に閉塞した。
- システム部門が運用するシステムについては外部記憶装置の接続に関する管理がなされていたものの、業務部門が運用する機器等については管理が行き届いていなかった。運用上やむを得ず機器等に外部記憶装置を接続する場合にはマルウェアスキャンを徹底することとした。

6. 得られた気付き・教訓

- **システムへのUSB接続に関する管理不足**

  マルウェア感染のリスクが容易に想定できるシステムへのUSB接続を黙認していたことは管理不足と言わざるを得ない。システムの仕様上、USB接続をなくせない場合であっても、都度ウイルススキャンを実施したUSBでメーカーに作業を実施させる等のリスクを軽減させるための管理が必要。

- **サイバーインシデント対応に関する知見をもつ関係機関との連携**

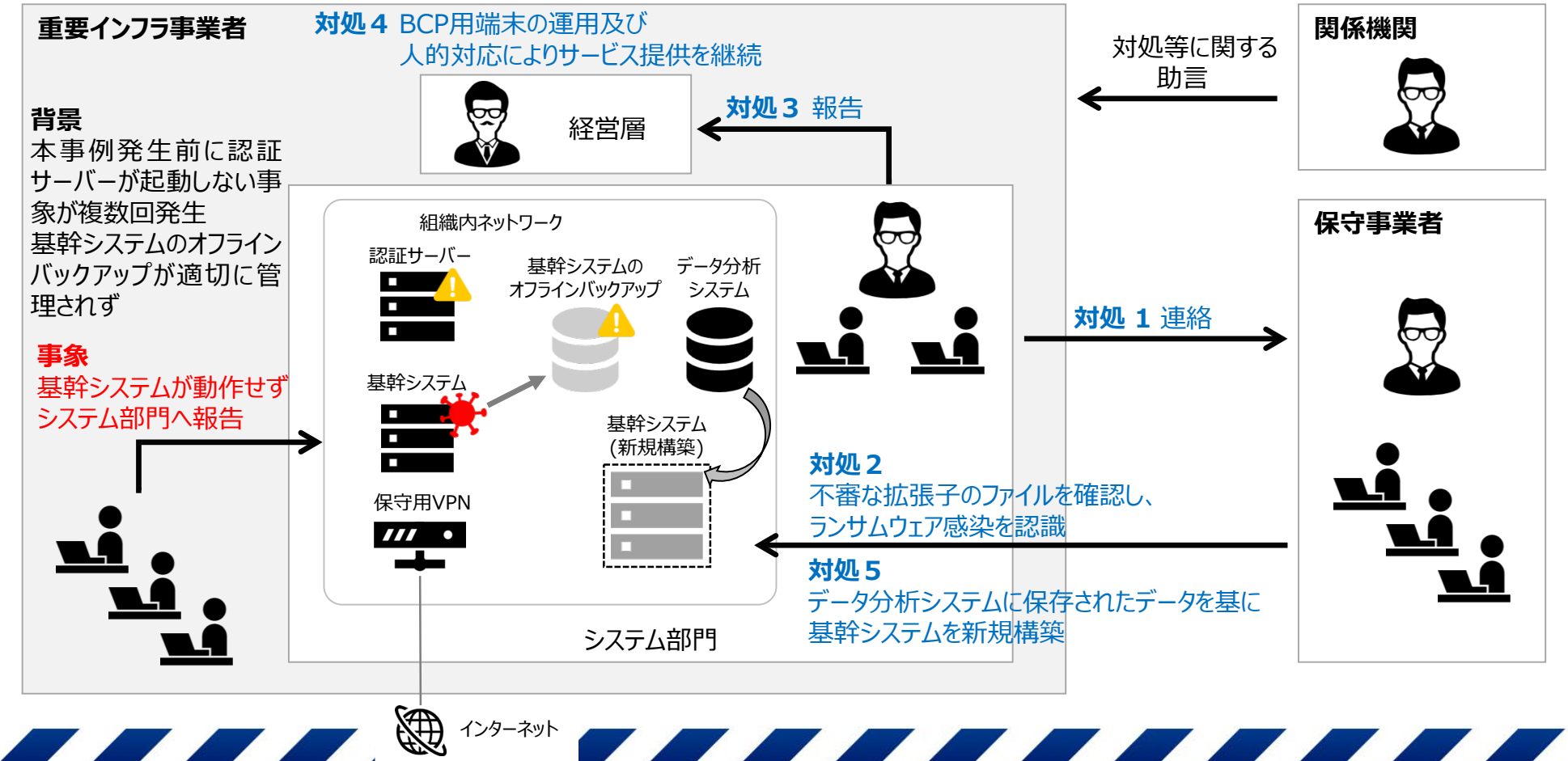
  本事例の対処において、サイバーインシデント対応に関する知見のある関係機関が初動段階から参画したことが、迅速な対処に繋がった。特に通常運用再開の判断に際しては、マルウェアが検知された産業機器のみならず基幹システムを含む周辺システムの健全性を確認する必要があり、インシデントレスポンスの経験をもつ有識者による助言は重要。

- **システム構成等に関する関係者との共通理解**

  本事例では、最初にマルウェア感染を認識した産業機器のメーカーは、マルウェア検知の段階においては重要インフラ事業者へ報告せず、マルウェア駆除作業の完了後に報告した。対して、重要インフラ事業者は当該機器が管理サーバへ接続され間接的に基幹システムへもつながっていることから、メーカーからの報告後に直ちに当該機器を隔離しており、当該機器においてサイバーインシデントが発生した際の影響等の認識に違いがあった。システム構成や各機器等の重要性について、平時から関係者と共通理解をもつことが重要。

事例２：基幹システムのランサムウェア感染 1／2

- 重要インフラサービスの提供のため運用する基幹システムがランサムウェアに感染し停止した。
- 調査の結果、基幹システムの復旧には時間を要すると判断し、災害発生時の運用を想定して整備されていたBCP用端末及び人的対応により重要インフラサービスの提供を継続した。
- 基幹システムの復旧にあたり、マルウェアの残留やバックドア設置の可能性があったため、新たに基幹システムを構築した。その際、オフラインバックアップではなく、基幹システムのデータを定期的に蓄積していたデータ分析システムに保存されていたデータを利用した。



事例２：基幹システムのランサムウェア感染 2／2

１．背景

- 本事例の発生前、認証サーバーが起動しない事象が複数回発生していた。
- 定期的に差分バックアップ（以降、オフラインバックアップ）を取得していたことに加えて、基幹システムのデータを集計・分析する「データ分析システム」が、基幹システムのデータを蓄積していた。
- 災害発生時の運用を想定したBCP用端末を整備していた。

２．検知

- 従業員が、基幹システムが動作しないことを認識し、システム部門へ報告した。

３．対処

- システム部門は直ちに保守事業者へ連絡し、調査を開始した。
- 認証サーバーが起動しない事象が発生していたことから、保守事業者が認証サーバーの障害を疑い調査を進めたものの原因は判明せず、基幹システムの復旧に時間を要すると判断し、BCP用端末による運用を準備した。
- 保守事業者が基幹システム内の大多数のサーバーに不審な拡張子のファイルが存在することを確認し、ランサムウェア感染によるシステム障害であることを認識した。
- システム部門は経営層へ事態を報告し、経営層はBCP用端末の運用及び人的対応により重要インフラサービスを継続する方針を決定した。また、以後の対処においてサイバーインシデント対応に関する知見のある関係機関による支援を依頼した。
- 基幹システム内のサーバーのマルウェアスキャン等を実施したが、後述の原因により、これらのマルウェア等を駆除した場合でもマルウェアの残留やバックドアが設置されている可能性があった。オフラインバックアップでは初回フルバックアップのデータを管理しておらずシステムの復元が出来なかったものの、データ分析システムについてはランサムウェアによるデータ暗号化を免れたことから、当該システムに保存されたデータを基に新たな基幹システムを新規構築し、通常運用を再開した。

４．原因

- ランサムウェアの感染経路は明らかでないが、次の事柄が考えられる。
  - 保守用VPN機器、サーバー及び端末のID及びパスワードが推測可能な同一の文字列であったこと
  - 保守用VPN機器のソフトウェア更新がなされておらず、ランサムウェア攻撃における悪用が確認されていた脆弱性が存在していたこと
  - サーバー及び端末の全てのユーザに管理者権限が付与されていたこと

５．再発に備えた対策

- インターネットから基幹システムへのアクセスには多要素認証やアクセス制御を導入した。
- 基幹システムにおいて動作するアプリケーションが管理者権限を必要とする仕様であったため、標準ユーザーで運用可能となるよう改修し、管理者権限付与の見直しを行った。

6. 得られた気付き・教訓

- **資産管理及び脆弱性管理**

  本事例のランサムウェア感染経路は明らかでないものの、特にインターネット境界にあるファイアウォールやVPN機器の脆弱性情報の入手やその評価、また、脆弱性の修正を管理する台帳を作成し都度、評価やソフトウェア更新を行う体制を整えることが重要。

- **データバックアップ等の作業手順の整備・確認**

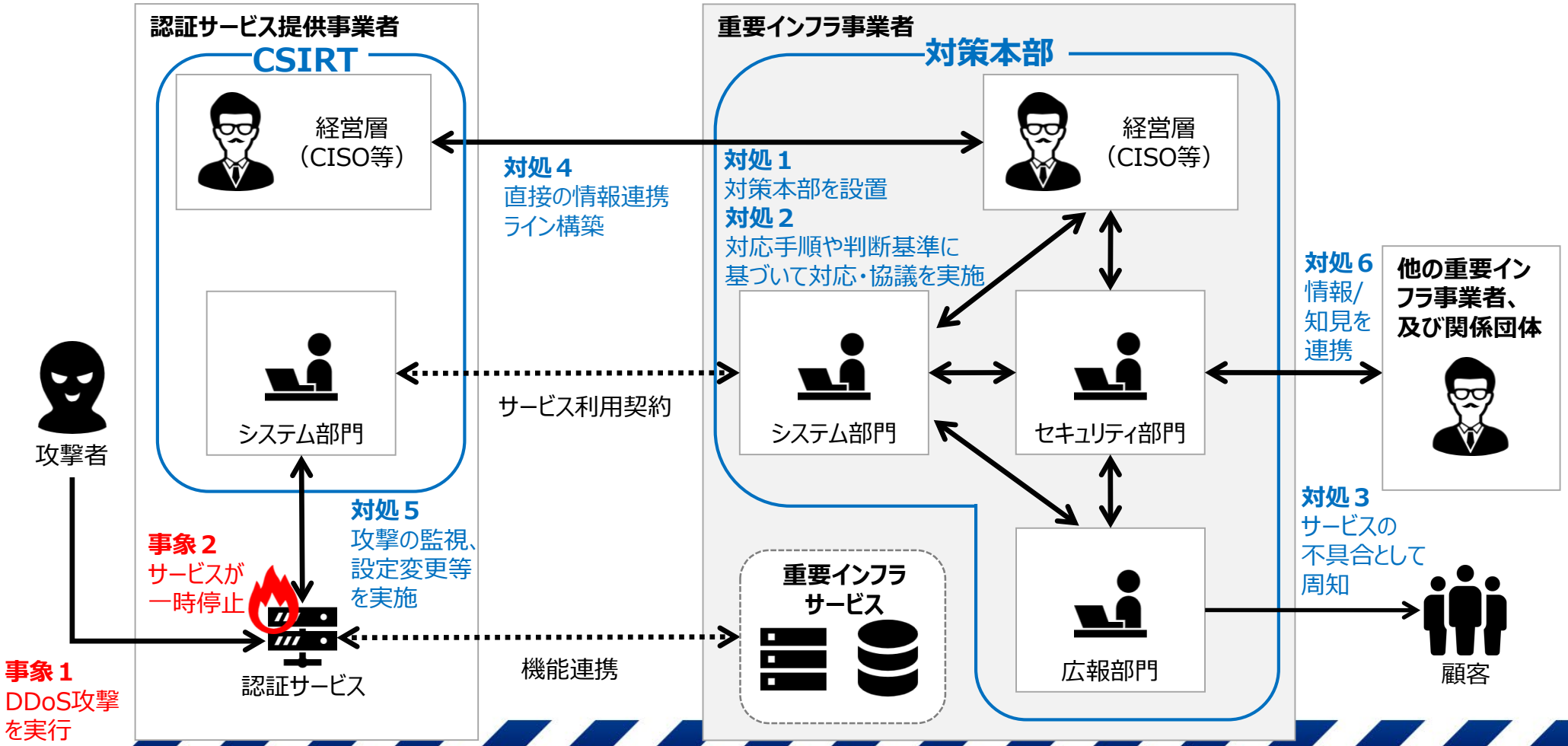
  重要インフラ事業者は保守事業者へ基幹システムのオフラインバックアップを委託していた。保守事業者は差分バックアップを実施していたものの、データ復旧に必要な初回フルバックアップのデータを管理していなかったことから、本事例の対処において本オフラインバックアップを使用できなかった。オフラインバックアップに限らないが、作業手順の整備や確認が重要。

- **システム障害発生時の原因究明の重要性**

  本事例の発生前、認証サーバーが起動しない事象が複数回発生したが、当時は速やかに復旧したことから詳細な調査を行わなかった。関連は明らかでないものの、この事象が本事例の兆候であった可能性も考えられる。システム障害の対応時にはサイバー攻撃の可能性も考慮しつつ原因を究明することが重要。

事例３：DDoS攻撃による重要インフラサービスの一部機能停止 1／2

- 重要インフラ事業者は、複数の事業者が提供するサービスを組み込んで重要インフラサービスを提供していた。
- 組み込んだサービスのうち、認証サービスがDDoS攻撃を受け、重要インフラサービスの認証機能が一時停止した。
- 重要インフラ事業者は、関係各所へ連絡して対策本部を設置した上で、あらかじめ定めていたサイバー攻撃に対する対応手順や判断基準に基づいて各種対応や連携を実施した。



事例３：DDoS攻撃による重要インフラサービスの一部機能停止 2／2

１．背景

- 重要インフラ事業者は、複数の事業者が提供するサービスを機能として組み込んで重要インフラサービスを提供していた。
- 組み込んだ機能のうち、認証サービスの運用については、認証サービス提供事業者となっていた。
- 認証サービス提供事業者はDDoS攻撃への対策として、WAFやロードバランサー等のDDoS攻撃対策製品を導入し運用していた。

２．検知

- 認証サービス提供事業者はDDoS攻撃対策製品の動作からDDoS攻撃を検知した。
- 重要インフラ事業者のセキュリティ部門は、認証サービス提供事業者から報告を受けて本事象を認識した。
- 重要インフラ事業者は、重要インフラサービスの認証機能が一時停止していることを確認するとともに、複合攻撃もあり得るとの認識を持った。

３．対処

- セキュリティ部門は、経営層含めた各部門責任者に報告・連絡して対策本部を設置し、適時意思決定を実施した。
- セキュリティ部門は、あらかじめ定めていたサイバー攻撃に対する対応手順や判断基準に基づいて、各種対応や関係者との連携を実施した。特に認証サービス提供事業者とは、事象の重大性を鑑みて、経営層レベルで働きかけをし、直接コミュニケーションを取る体制を構築した。
- 認証サービス提供事業者は、セキュリティ部門と情報を共有しながら攻撃状況の監視とDDoS攻撃対策製品の設定変更、再起動等を実施した。
- DDoS攻撃によるサービス影響を受けた事実自体が攻撃者のメリットとなる可能性があるため、サイバー攻撃の情報は公表せず、顧客に限定してサービスの不具合が発生していると周知を実施した。
- 一部の他事業者に対して情報を提供した上で、類似事例の知見提供を依頼するとともに、関係団体への連携も行った。

４．原因

- 認証サービス提供事業者の認証サービスに対してDDoS攻撃対策製品の許容量を超える攻撃を受けたことで、認証サービスが一時的に利用不可となった。
- 断続的に攻撃が続いたことによって、長期間にわたって対応を余儀なくされた。

５．再発に備えた対策

- これまでシステムに導入していた対策に加えて、IPアドレスの変更や通信回線の増強、クラウドCDNの導入等を実施した。
- 重要インフラ事業者側で認証機能の応答状況を直接監視・異常を検知できる仕組みを構築した。

6. 得られた気付き・教訓

- **他事業者との相互連絡によるリアルタイムな情報共有の有用性**

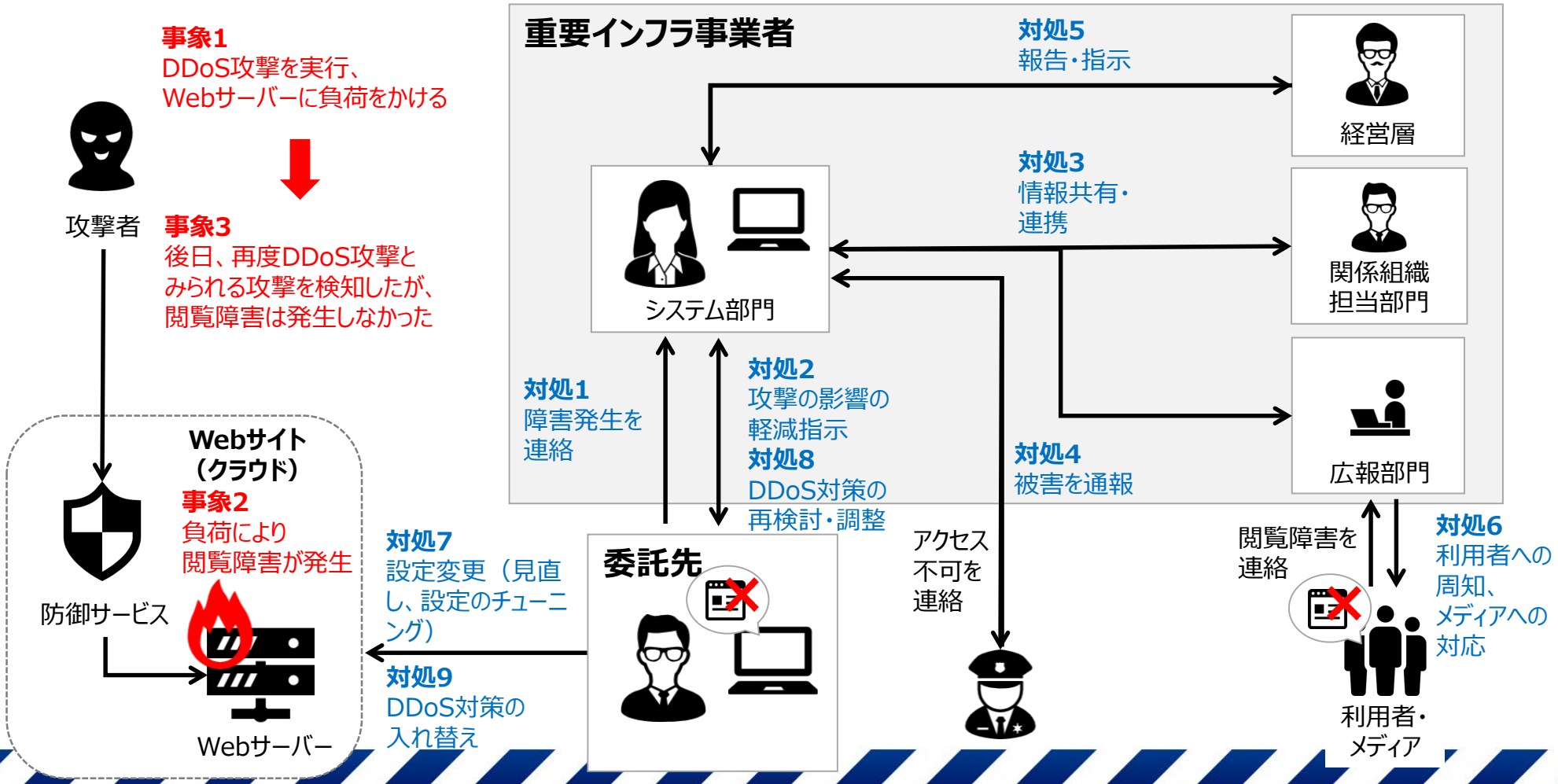
  本事例における認証サービス提供事業者との関係構築のように、組織を超えて他事業者とリアルタイムな情報共有を行うことは、スピード感のある対応に繋げられる意味で有用と思われる。DDoS攻撃が大規模に発生していた時には、認証サービス提供事業者はもちろん、DDoS攻撃を受けていた他の重要インフラ事業者とも相互に連絡を取り合って攻撃の傾向やIoC情報等をリアルタイムにやり取りしていた。

- **緊急時の対応手順、対応体制等をあらかじめ策定**

  あらかじめ定めていたサイバー攻撃に対する対応手順や判断基準、対応体制に沿って対応を実施できたため、状況が変化しても迅速に対処が可能であった。被害が発生した際に、誰が何をどのように行うか事前に想定し、明文化しておくことが重要。併せて平時から緊急時に備えた訓練を実施し、関係者の理解を深め、インシデント発生時には、役員含めた関係者すべてが集まる文化を醸成することも重要。

事例４： Webサイトに対するDDoS攻撃 1／2

- 重要インフラ事業者はクラウド上に構築されたWebサイトを利用しており、構築・運用を委託先に委託していた。
- 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、攻撃の影響の軽減を狙って設定変更等の対応を実施。その後、WebサイトへDDoS対策製品の追加導入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）では閲覧障害の発生を抑えることができた。



事例４： Webサイトに対するDDoS攻撃 2／2

1．背景

- 重要インフラ事業者は、クラウド上に構築されたWebサイトを利用しており、構築・運用を委託先に委託していた。
- 当該Webサイトは利用者からの閲覧を想定したものであり、重要インフラサービスへの影響は限定的だった。
- 重要インフラ事業者は、サイバー保険に加入することでセキュリティの専門家と相談が出来る体制を確立していた。
- WebサイトへのDDoS攻撃対策として、DDoS防御サービスとWebサイトの監視システムを導入していた。

2．検知

- 監視システムが攻撃を検知したことを受けて、委託先からの連絡によりシステム部門は本事象を認識した。
- 利用者からWebサイトが閲覧できない旨連絡を受けた。
- 都道府県警より、Webサイトのアクセス不可について連絡を受けた。

3．対処

- システム部門は、緊急時の連絡体制表を用いて経営層を含めた各部門責任者に報告・連絡した。
- システム部門は、都道府県警へDDoS攻撃被害を受けたことを通報した。
- 経営層は、Webシステムの優先度を勘案してシステム部門を中心に対処するよう指示を実施した。
- 委託先は、攻撃の影響の軽減を狙ってDDoS防御サービスの設定変更を実施したが効果が得られなかった。
- 広報部門は、利用者やメディアからの電話による問い合わせに応対。
- DDoS攻撃が収束したことにより復旧した。

4．原因

- DDoS攻撃によるWebサーバーの過負荷。
- DDoS防御サービスが通常の通信と認識してしまう通信を大量に送りつける攻撃を受けていた。

5．再発に備えた対策

- これまで使用していた防御サービスに代わり、DDoS攻撃の特徴を捉える振る舞い検知が可能なDDoS対策製品を導入した。
- 作成済みであった自然災害やシステム障害を想定したBCPをもとに、サイバー攻撃を想定したBCPを新たに作成することを検討している。

6. 得られた気付き・教訓

- **既存対策の継続的改善**

  本事例では、被害を受けたことで既存のセキュリティ対策を見直し、その後発生した攻撃での被害を抑えることができた。既存の対策を見直して継続的に改善することが重要。

- **セキュリティ体制の不足を補う施策の重要性**

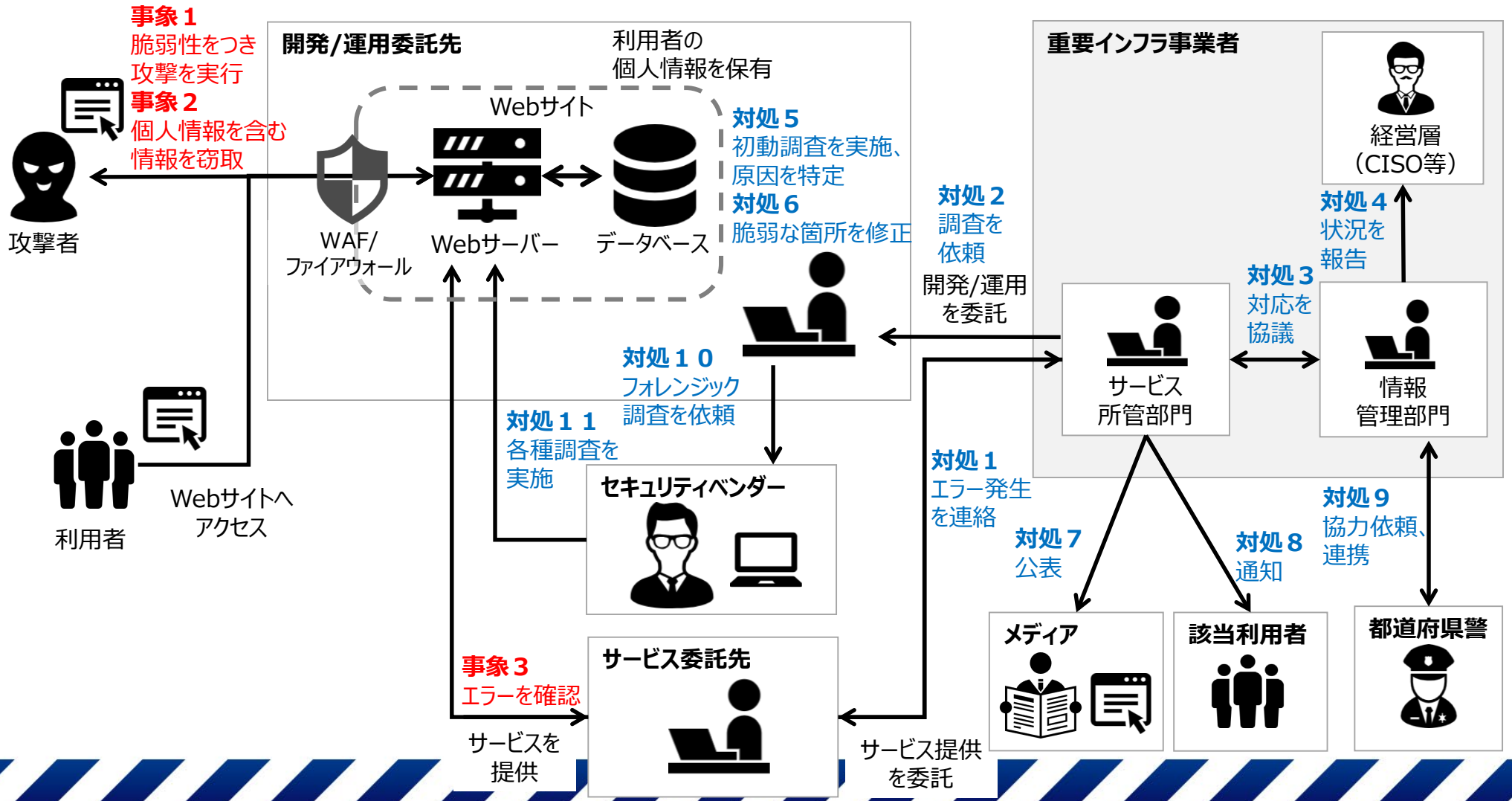
  予算や人材の制約によって、セキュリティ体制に割り当てるリソースが不足していると考える組織は多い。人材を増やす、高度なセキュリティ製品を導入するといったリソースを必要とする施策の他に、限られたリソースで実施可能な施策がないか検討することが重要。例えば、本事例ではサイバー攻撃を想定したBCPを新たに作成することによるインシデント対応の効率化に加えて、サイバー保険に加入していることでセキュリティの専門家と相談が出来る体制を確立し、人材不足を補おうとしている。

- **緊急時の対応体制の事前策定**

  本事例では、あらかじめ連絡体制をまとめた表を作成していたため、攻撃発生時の関係各所への連絡・連携を速やかに実施できた。被害が発生する前に連絡体制表等をあらかじめ策定することが重要。

事例５：Webサイトの脆弱性をついたサイバー攻撃による個人情報の流出 1／2

- 重要インフラ事業者は、外部事業者への委託によりWebサイトを構築してサービスを提供していた。
- Webサイトの脆弱性をついたサイバー攻撃が発生し、個人情報を含む情報が流出した。
- 重要インフラ事業者は、CSIRT体制を持つ情報管理部門を中心に各種対処を実施した。



事例５：Webサイトの脆弱性をついたサイバー攻撃による個人情報の流出 2／2

１．背景

- 重要インフラ事業者は、Webサイトの開発及び運用を外部事業者（以降、開発/運用委託先という）に委託し、Webサイトを用いたサービス提供を別の外部事業者（以降、サービス委託先）に委託していた。
- 当該Webサイトは、Webサーバー上に開発/運用委託先が作成したアプリケーションを格納し、データベース上に格納したデータを適宜呼び出すことで稼働していた。
- 当該Webサイトは、サイバー攻撃に備えてWAFやファイアウォールの設置、サーバーのリソース監視製品の利用、各種ログやアラートの監視等のセキュリティ対策を実施していた。

２．検知

- サービス委託先がシステムの操作に際して、エラーが発生する旨を重要インフラ事業者に連絡し、重要インフラ事業者は開発/運用委託先へ調査を依頼した。
- 開発/運用委託先が調査したところ、サイバー攻撃と思われる不正なアクセスの痕跡を発見したことで本事例を認識した。

３．対処

- 重要インフラ事業者は、CSIRT体制を持つ情報管理部門を中心に対応を協議し、経営層へ適宜状況を報告した。
- 開発/運用委託先は、各種ログやアラートを調査してサイバー攻撃の原因や経路を推定し、個人情報の流出の恐れがあることを把握した。
- 開発/運用委託先は、アプリケーションの脆弱な箇所を速やかに修正した。
- サービス所管部門は、個人情報流出の可能性があることを踏まえてサイバー攻撃被害を公表し、該当する利用者に通知した。
- 情報管理部門は、都道府県警に協力を依頼し、情報を連携した。
- セキュリティベンダーは、開発/運用委託先の依頼を受けて、フォレンジック調査による被害範囲の特定と原因究明、ペネトレーションテストによるセキュリティレベルの現状把握と必要な対策の提言、及びダークウェブ調査による窃取情報の公開有無の確認を実施した。

４．原因

- アプリケーションに脆弱性があり、SQLインジェクションを実行すればデータベースに格納されている個人情報を含む情報を窃取可能だった。
- 異常を検知するログやアラートが大量のデータに埋もれてしまい、攻撃をすぐに認知できなかった。

５．再発に備えた対策

- 重要インフラ事業者は、委託先選定時のセキュリティ対策の調査及び契約後のセキュリティに関する取り組み状況の確認を強化することとした。
- システムの監視体制を強化するために、ログ容量の監視機能やシステム監視サービスを導入した。

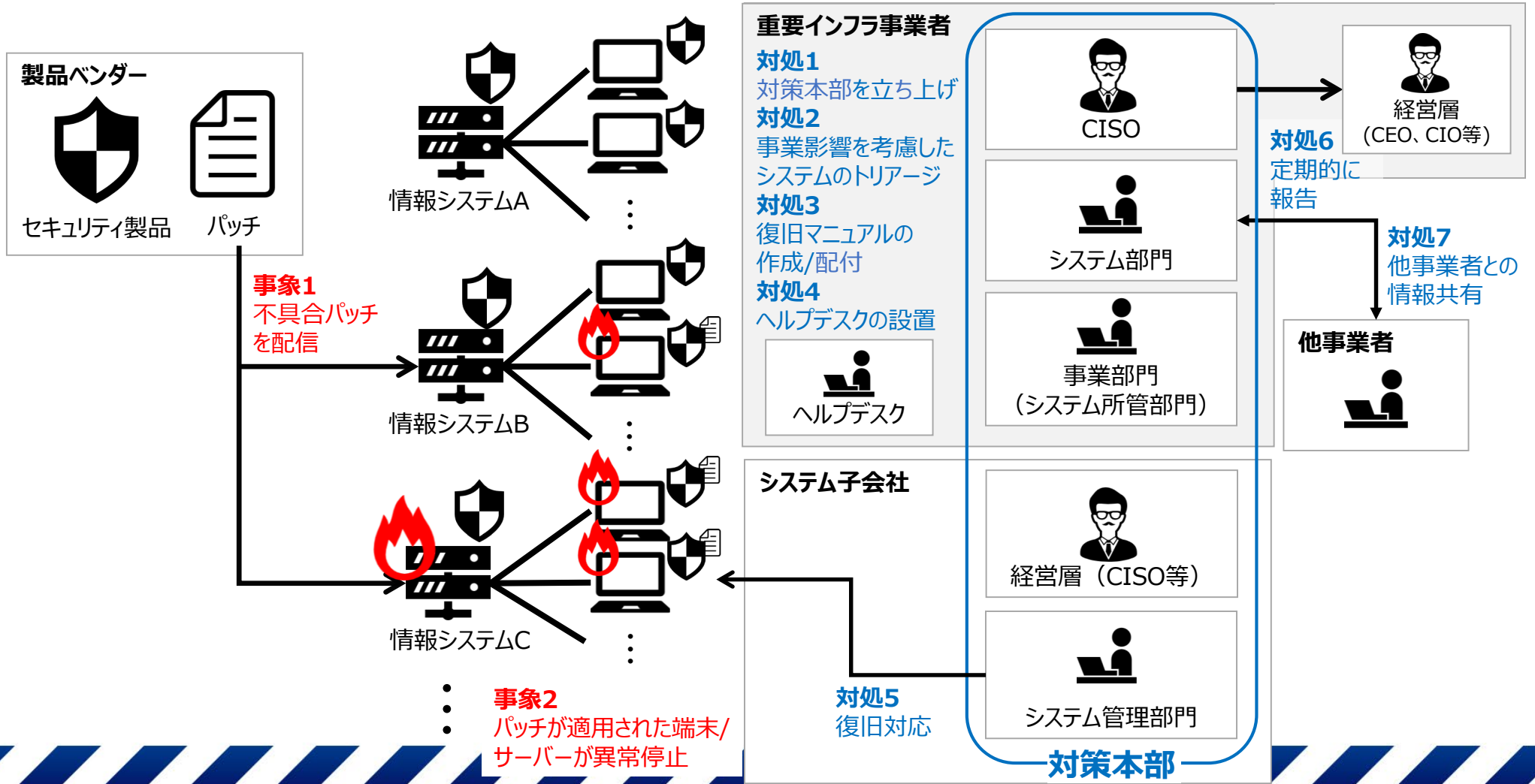
6. 得られた気付き・教訓

- **システム開発委託において必要なセキュリティ対策の確認**

  システム開発の委託に際しては、システム自体のセキュリティ要件・設計の確認に加えて、開発委託先のセキュリティ対策状況も確認することが重要。システム開発にあたって開発委託元が実施できる方策としては、委託契約時の仕様書に盛り込むセキュリティ要件を充実させること、外部認証の取得有無等の基準を設定して開発委託先組織のセキュリティ対策状況を評価することが考えられる。

事例６：セキュリティ製品の不具合に伴う複数システムへの復旧対応 １／２

- 重要インフラ事業者の各システムに順次導入していたセキュリティ製品パッチに不具合があり、当該パッチが配信された端末/サーバーが異常停止したことにより、複数のシステムが機能を停止した。
- 重要インフラ事業者は、対策本部の立ち上げ、情報システムのトリアージ、あらかじめ定めていたシステム大規模停止時の対応手順に基づいた必要な対処等により、重要インフラサービスへの影響を最小限に抑えた。



事例６：セキュリティ製品の不具合に伴う複数システムへの復旧対応 2／2

1．背景

- 重要インフラ事業者は、グループ全体のセキュリティを向上させるために各社の情報システムに対してセキュリティ製品を順次導入していた。
- 重要インフラ事業者のシステム部門が導入を推進し、グループ60社（サーバー約1,000台、端末約35,000台）に対して導入を完了していた。
- システム部門は、事前にCSIRT体制/システム大規模停止時の対応手順/システム一覧を作成しており、経営層やグループ各社関係者が参加する全社インシデント対応訓練を実施していた。上記の事前対応により、インシデントへの「対応の型」が既に醸成されていた。

2．検知

- セキュリティ製品パッチに不具合があり、当該パッチが配信された端末/サーバーが異常停止したことで複数のシステムが機能を停止した。
- 重要インフラ事業者のシステム部門は、監視システムのアラートやシステム利用者の問合せから本事象を認識した。

3．対処

- システム部門は、システム大規模停止時の対応手順に沿って対策本部を立ち上げ、対応状況の整理とCISOを含めた意思決定を実施した。
- システム部門は、システム一覧から障害による事業影響を考慮したトリアージを行い、優先度の高いシステムからグループ会社と連携して復旧作業を実施した。トリアージに際しては、システムの所管部門責任者とも連携し事業影響を判断した。
- システム部門は、ベンダー提示の復旧手順に基づいて社内向け復旧マニュアルを作成し、システム所管部門や利用者へ展開した。
- 他の事業者と障害について情報交換を行い、対処に活用した。
- 事業部門は、停止したシステム間で連携していた情報を、IT化の際に代替手段として残していたFAX等を用いて各所と連携した。
- CISOは、経営会議において社長を含めた全役員に対して定期的に復旧状況の報告を実施した。
- 停止したサーバーについては障害発生日中に復旧させ、重要インフラサービスへの影響を最小限に抑えた。一方で復旧できなかった端末への対応のために、24時間対応可能なヘルプデスクを立ち上げて2週間で全台を復旧させた。

4．原因

- セキュリティ製品のパッチに含まれていた不具合により、特定OSのサーバーや端末が異常終了した。

5．再発に備えた対策

- 同様の事例に備えて速やかにグループ各社へ情報連携をするために、セキュリティ製品の管理画面の閲覧権限を各社担当部門へ付与した。
- 本事例を通して経営層を含めたインシデント対応訓練は非常に効果的であったことが確認できたため、様々なシナリオを用い、今後も継続して訓練を実施する。

6. 得られた気付き・教訓

- **適切な資産管理をベースとした各システムの復旧の優先順位付け**

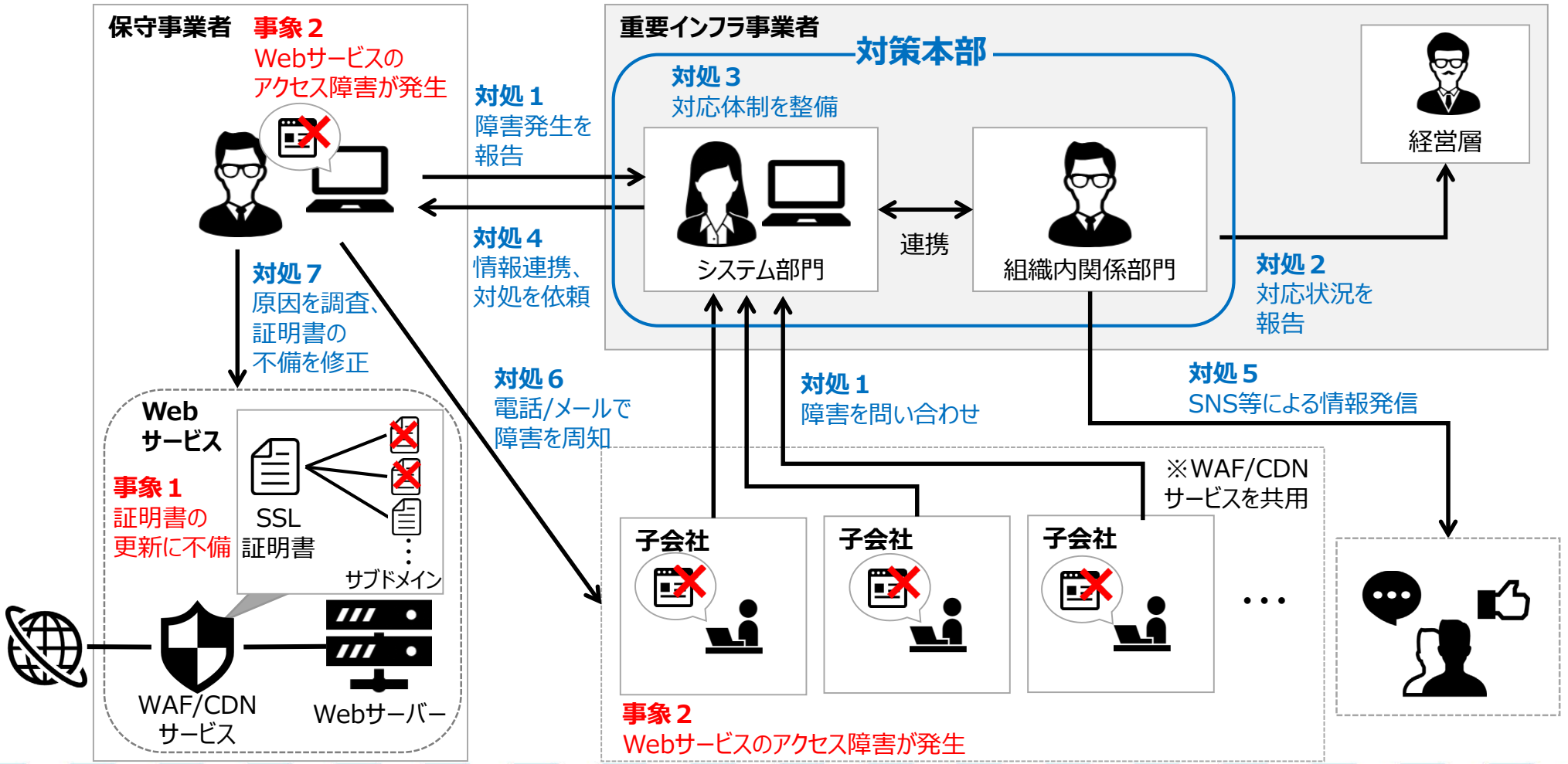
  本事例では、資産管理が適切に行われており、事業継続の観点から、どのシステムを優先的に復旧させるべきなのか、速やかな対応優先度の判断が可能となった。
- **対応手順の整備と訓練の実施**

  経営層を含めたインシデント対応訓練を実施していたことで、経営層/部門/グループ会社間の情報共有や連携を速やかに実施できた。平時からシステム障害を見据えた対応体制や手順を整備し、訓練することにより「対応の型」というべきものを醸成しておくことが重要。
- **速やかな対応の結果生み出した余剰リソースの活用**

  本事例では、上記の対策によって組織全体でのインシデント対応を効率的に行えた結果、余剰リソースを生み出し、ヘルプデスクのようなリソースを大量に必要とする対応を実施可能にした。平時の対策実施が、緊急時のリソースを生み出すという副次的効果を発揮した。

事例７：SSL証明書更新不備によるWebサービスへのアクセス障害 1／2

- 重要インフラ事業者は、グループ子会社とWAF/CDNサービスを共用して利用者向けにWebサービスを提供していた。
- SSL証明書の更新に不備があり、重要インフラ事業者を含む複数事業者のWebサービスへのアクセス障害が発生した。
- 重要インフラ事業者は、障害対応フローに従い緊急時の対応体制を整え、保守事業者と情報共有及び復旧作業を実施した。



事例７：SSL証明書更新不備によるWebサービスへのアクセス障害 2／2

1．背景

- 重要インフラ事業者は、グループ子会社と共同でWAF/CDNサービスを利用し、サービス利用者向けにWebサービスを提供していた。
- Webサーバーはマルチドメイン運用されており、グループ子会社は重要インフラ事業者ドメインのサブドメインにてWebサービスを公開していた。
- Webサービスのシステム構築・保守を委託する事業者（以下「保守事業者」という）のデータセンター内にシステムが構築されていた。
- 新たにWebサービスを利用するグループ子会社（以降、新規子会社）の追加に伴い、SSL証明書の更新が行われた。
- 過去に発生したインシデントを踏まえ、障害対応フローを整備していた。

2．検知

- 従来からWebサービスを利用するグループ子会社（以降、既存子会社）は、Webサービスにアクセスできないことを確認した。
- 保守事業者は監視システムによりWebサービスへのアクセス障害を検知。
- システム部門は、既存子会社からの問い合わせ及び保守事業者からの報告によって本事象を認識した。

3．対処

- システム部門は、経営層を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。障害対応フローに従い緊急時の対応体制を整え、保守事業者と適宜情報共有を実施。
- システム部門は、広報担当者と連携し、Webサービス障害についてSNS等の別チャネル上で利用者へ情報提供を実施。
- 既存子会社への障害通知は、障害対応フローに基づき、保守事業者がメールおよび電話を用いて実施。
- 保守事業者は、 Webサーバーを調査してSSL証明書の更新不備が障害の原因であると予想し、証明書の更新を実施して障害発生から約6時間で復旧。

4．原因

- 新規子会社のサブドメイン追加により、WAF/CDNサービス内のSSL証明書自体の有効期限とサブドメイン（SAN）の有効期限に差分が生じた。
- WAF/CDNサービスの仕様上、SSL証明書とSANの有効期限の差分が90日未満の場合、両者を手動更新する必要があったが、更新を行わなかったために信頼されない証明書としてWeb表示が無効化された。
- 保守事業者は、上記仕様を把握できておらず、また事象発生以前には両者の同時更新のみ実施していたため、問題が顕在化していなかった。

5．再発に備えた対策

- 証明書の更新タイミングを見直し、許容範囲外となる事が無くなる作業日程に調整。また、有効期限を迎える前に自動でアラートメールを送信する設定を実施。
- 保守事業者の内部調査が長期化しないよう、障害原因の切り分けの時限的タイミングを設けてWAF/CDNサービス開発元へ問い合わせを行う運用ルールを追加。
- 保守事業者を含めて年に1回実施していた大規模インシデントを想定した訓練を、今後も継続して実施予定。

6. 得られた気付き・教訓

- **システムを構成する各製品の仕様を完全に把握する難しさ**

  システム障害の原因となりうるサービスの仕様を網羅的に把握しておくことが重要である一方で、完全な把握は難しい。システムの要件定義・基本設計の段階から稼働に影響の大きい仕様を把握するとともに、不測の事態が発生しても早急に対応・復旧できる対応手順の明文化が必要。

- **緊急時に備えた障害対応フローの整備と訓練**

  本事例では、過去のインシデントを受けて整備していた障害対応フローに基づいて対応を進めたことによって、早急な障害への対処や関係組織との連携が可能となった。平時から緊急時の障害対応フローを整備し、定期的に訓練を実施することで緊急時の対応に備えておくことが重要。

事例８：データベースの過負荷による重要インフラサービスの処理遅延 １／２

- 重要インフラ事業者は、過去のシステム障害における教訓等に基づき、対策本部の設置基準及び組織内関係者や顧客への周知に関する手順を事前に定めていた。
- 通常発生しないパターン（想定外）の大量データを受付け、それに対応するデータベースの検索結果が全件エラーとなったことに伴い、データベースの過負荷が発生した。
- 重要インフラ事業者は、事前に定められた手順に則り対処を行い、過負荷の原因となった処理プログラムの改修によって重要インフラサービスの処理遅延を解消させた。

事例８：データベースの過負荷による重要インフラサービスの処理遅延 2／2

1．背景

- 過去のシステム障害における教訓等に基づき、システム障害発生時の報告や各種会議体（対策本部等）の設置、組織内の関係部門及び顧客への周知に関する手順が事前に定められていた。

2．検知

- 重要インフラ事業者のシステム部門（システム監視担当）が処理のタイムアウトを含む多数のエラーを検知した。

3．対処

- システム責任者を含む会議において対応方針を決定し、原因及び影響の調査を開始した。
- 調査により、エラー発生件数が大量であること等から復旧に想定以上の時間を要することが判明したため、経営層をトップとする対策本部を設置した。
- システム部門は重要インフラサービスの処理遅延が発生している旨を顧客対応部門や広報部門等の組織内関係部門へ周知し、その後、広報部門が対外公表を実施した。
- システム部門及びシステム保守事業者において、データベースへの負荷を抑制するため、データベースへのアクセスの一部をスキップする暫定的なプログラム改修を検討し、対策本部において改修内容を承認した。
- システム保守事業者による改修プログラムの適用作業を実施し、処理遅延が解消した。
- 重要インフラサービスの処理遅延が解消した旨を組織内関係部門へ周知し、その後、対外公表を実施した。

4．原因

- 通常発生しないパターン（想定外）の大量データを受付けた場合、検索結果としてエラーを応答する仕組みであるが、全件エラーとなったため、データベースの過負荷が発生した。
- データベースの過負荷に伴い、当該利用者のみならず他の利用者による重要インフラサービスの利用にも影響が生じた。

5．再発に備えた対策

- 大量のエラーが発生しないよう、検索条件の追加により、データベースへの過負荷を抑制した。
- 処理遅延の原因となった処理以外においても、同様の処理遅延が発生する可能性がないか点検を実施し、一部処理の見直しを計画した。
- システム障害発生時におけるエラーの内容や件数の確認といった原因究明に向けた対応手順や役割分担が不十分であったことから、対応フローを整備した。

6. 得られた気付き･教訓

- **役割分担の明確化と人員毎の作業負荷の均等化**

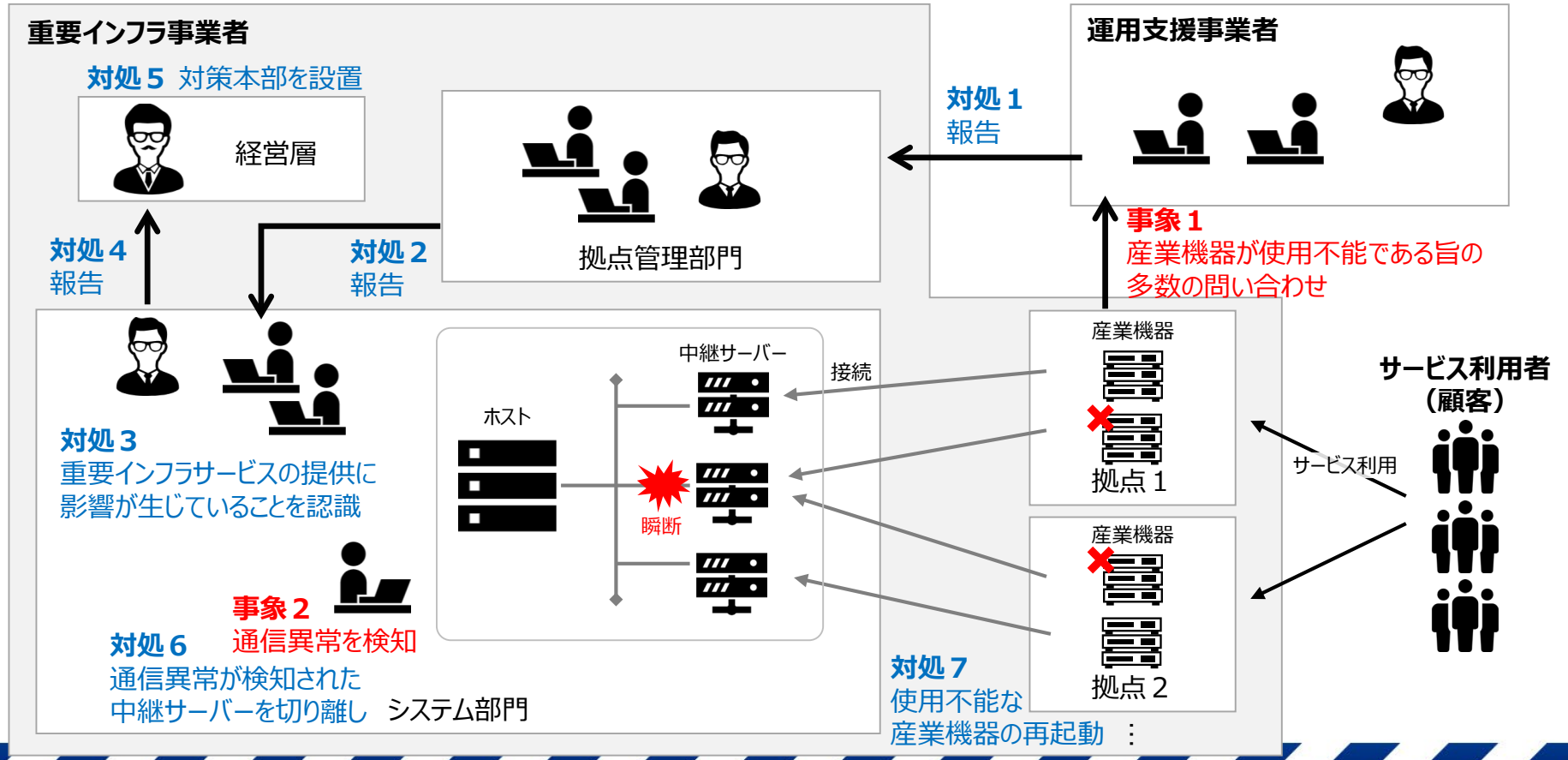
  システム障害の対処においては、目下の対応に集中するほど後続の対応が後手に回ってしまう。本事例においては、システム保守事業者のリーダーが重要インフラ事業者との窓口と現場の管理を兼ねていたことから、当該リーダーに対応が集中してしまった。対処における役割分担の明確化や人員毎の作業負荷の均等化を予め検討することが重要。

- **システム障害対応訓練の実施**

  本事例では対策本部の設置及び組織内関係者や顧客への周知が事前に定められた手順に則って行われ、また、システム障害対応訓練を定期的に実施していた。当該訓練の実施を通じて、各部門やシステム保守事業者の役割分担の確認や障害発生時の要員を想定どおり確保可能であるか等を平時より確認することが重要。

事例９：ネットワークの瞬断に起因する重要インフラサービスの一部停止 1／2

- 重要インフラサービスの提供にあたり、重要インフラ事業者の各拠点に産業機器が設置されており、当該機器は複数ある中継サーバーの内、１台を経由してホストと通信していた。
- ネットワーク機器を原因とする瞬断が発生し、これにより特定の中継サーバーに接続する産業機器が使用不能となった。
- 事前に用意された連絡・報告体制に基づき速やかに情報共有を行い、対策本部を設置した。
- 通信異常を検知した中継サーバーをネットワークから切り離し、その後、各拠点において使用不能となった産業機器の再起動を実施し、産業機器全台を復旧させた。



事例９：ネットワークの瞬断に起因する重要インフラサービスの一部停止 2／2

1．背景

- 重要インフラサービスの提供にあたり、重要インフラ事業者の各拠点に産業機器が設置されており、当該機器は複数ある中継サーバーの内、１台を経由してホストと通信していた。
- 重要インフラ事業者はシステム障害等発生時の連絡・報告体制や組織内の関係部門等への報告事項等を定めていた。さらに、数年前に同重要インフラ事業者において発生した大規模なシステム障害における教訓等に基づいて、円滑に対応できるよう改定していた。

2．検知

- 各拠点に設置された産業機器の運用支援事業者が、当該機器が使用不能である旨の多数の問い合わせを受け、重要インフラ事業者の拠点管理部門へ報告した。
- 重要インフラ事業者のシステム部門が、特定の中継サーバーの通信異常を検知した。

3．対処

- 拠点管理部門は、運用支援事業者において多数の問い合わせを受けている旨をシステム部門へ報告した。
- システム部門は、当該報告と通信異常の検知を踏まえ、重要インフラサービスの提供に影響が生じていることを認識し、経営層及び組織内関係部門に即座に報告した。併せて、検知の5分後には対策本部を設置した。
- 調査の結果、各拠点に設置された産業機器の内、通信異常が検知された中継サーバーを経由してホストへの通信を試みている産業機器が使用不能であることが判明した。
- 接続異常が検知された中継サーバーをネットワークから切り離し、これにより使用不能となる産業機器が増加しないことを確認した。
- 各拠点において、使用不能となった産業機器の再起動を実施し、障害発生から約7時間後に産業機器全台の復旧を確認した。

4．原因

- 特定の中継サーバーとホスト間の通信において、接続するネットワーク機器を原因とする瞬断が発生した。
- システムの構成上、中継サーバーとホスト間で確立された通信においてホストからの応答パケットが上記の瞬断により損失した場合、通信のリトライを実行することになるが、両者の通信のリトライ間隔が長く設定されていたために、瞬断後も当該中継サーバーとホスト間の通信が直ちに復旧せず、産業機器の使用不能につながった。

5．再発に備えた対策

- 中継サーバーとホスト間の通信のリトライ間隔を短く修正した。

6. 得られた気付き・教訓

- **連絡・報告体制等の整備**

  数年前に同重要インフラ事業者において発生した大規模なシステム障害における教訓等に基づき、システム障害やサイバー攻撃、自然災害時における連絡・報告体制について、平日日中や夜間、休日のそれぞれのフローを改定していた。また、各拠点でシステム障害が発生した際の対応者を予め定めていたことにより、円滑な対処に繋がった。

- **報告基準の整備や報告内容の様式化による円滑な情報共有**

  前述のフローとともに、システム障害の規模等に応じた報告基準や、各種報告内容のテンプレートを整備していたことで、組織内の関係部門等と円滑に情報を共有することができた。システム障害の対処時に原因調査や復旧作業に注力するためにも、これらのフローや報告基準、テンプレート等を事前に整備しておくことが重要。

- **経営層を含む対応訓練の定期的な実施**

  経営層を含む対応訓練を定期的に実施していたことにより、本事例の対処においても経営層が現場で陣頭指揮を執ることができた。