



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

資料 6

重要インフラにおける補完調査について (2018年度)

2019年4月18日

内閣官房 内閣サイバーセキュリティセンター(NISC)

補完調査とは

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。

※重要インフラの情報セキュリティ対策に係る第4次行動計画（平成29年4月18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・教訓等を取りまとめ、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、2018年1月1日～2018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
- 世の中のトレンド
- 事案の重大さ・社会的影響（関心）の大きさ
- 他分野への波及の可能性
- 類似事例の発生状況や今後発生する可能性
- 得られる気付き・教訓の有用性等
- 攻撃手口や被害の目新しさ

※その他、事案の対応の優劣、地域性や分野のバランスも考慮

2018年度 調査対象事例 概要

- ・ **“外部事業者のサービス障害に起因した重要インフラサービス障害”**が複数分野の重要インフラ事業者等で発生したことから、各事業者における対応事例を調査。
- ・ **“外部からのサイバー攻撃”**や**“重要インフラ事業者内でのインシデント”**等、例年発生頻度の高い脅威は2018年も一定数発生しているが、対応を実際に経験したことで重要インフラ事業者が新たに気づいた課題や教訓等について調査。

No.	事例	影響	原因
外部事業者のサービス障害に起因した重要インフラサービス障害			
1	インターネットサービス利用時の認証の障害	インターネットを通じて提供される重要インフラサービスで、利用者を認証する機能に障害が発生し、一部サービスが使用できなくなった。	外部サービス（クラウド型認証サービス）の障害
2	重要インフラ事業者間での映像データ送受信の中断	重要インフラサービスとして提供する予定の映像を予定時刻に送受信できず、利用者に提供できなくなった。	外部サービス（通信回線）の障害
3	重要インフラサービスの受付業務の遅延	利用者の受付業務に支障が発生し、重要インフラサービスの提供が遅延した。	外部サービス（顧客受付システムを共同利用するための共通ネットワーク）の障害
外部からのサイバー攻撃			
4	IoTデバイスへの不正侵入及び改ざん	第三者にネットワークカメラ等に不正に侵入・改ざんされ、施設等の監視に支障が発生した。	第三者が類推可能な認証情報（ID/パスワード）の悪用
5	脆弱性を悪用した攻撃	クラウド基盤のネットワーク機器が機能停止し、基盤上の業務システムが使用できなくなった。	ネットワーク機器の脆弱性を悪用した攻撃
6	広域DoS攻撃によるWebサイト閲覧障害	ある分野の複数の重要インフラ事業者等のWebサイトが閲覧できなくなった。	Webサイトに対するDoS攻撃
重要インフラ事業者内でのインシデント			
7	商用ネットワークの高負荷による通信障害	商用ネットワーク全体が高負荷となり、特にDNSサーバからの応答が滞ったことで、顧客のインターネット接続に支障が発生した。	商用ネットワーク内のネットワーク機器の不具合によるトラフィックの異常増加
8	他人の認証情報の悪用による情報の不正取得	本来、閲覧権限のない機微情報を不正に利用された。	従業員による他人の認証情報（ID/パスワード）の不正利用

得られた気付き・教訓 概要（各事案に共通する事項）

外部事業者に起因した重要インフラサービス障害事例（No. 1, 2, 3）から

- セキュリティ対策やリスクマネジメントに日々積極的に取り組んでいる先導的な重要インフラ事業者であっても、外部事業者のサービス障害に起因したサービス障害への対応を経て、**重要インフラ設備の一部を外部事業者に依存してサービスを提供する際のリスク**が再認識されている。重要インフラ事業者側で取り得る対策としては以下が挙げられる。他事業者においても参考とすることが期待される。
 - 外部事業者のサービスが中断した場合の、自組織への影響を再度評価する。
 - 特定の外部事業者のみに依存しない、多様性のある設備を自組織側で確保する。
 - （事業上の制約で多様性のある設備が確保できない場合、）重要な業務については、外部事業者のサービスの復旧までの間、自組織側で実行可能なコンティンジェンシープランの整備や更なる効率化を図る。
 - 外部事業者との緊急連絡体制の整備は必須であるが、外部事業者側の現場の対応状況を直接確認できる連絡体制がより望まれる。緊急時の連絡の場合は、中継のみのために介在する組織/担当者をできる限り減らすなど、連絡体制を効率化する。
 - 自組織内の各部署/各担当者が有事における自身の役割を理解し、能動的に動けるレベルを目指して訓練を行う。

外部からのサイバー攻撃への対応事例（No. 4, 5, 6）から

- 情報セキュリティの専任の担当者がいない/少ない事業者においては、担当者の稼働やスキルの不足、予算の不足等により、既知のリスクへの対策が十分に行うことができず、事案への対応の進め方にも窮する場合がある。この際、**事業上の関係がある組織や情報セキュリティ関係機関等からの助言により事態が好転したケース**が複数の重要インフラ事業者で確認されている。しかしながら、事案に対応した多くの担当者によれば、「緊急時には、平時から関係のある信頼できる組織や担当者に対してでなければ、そもそも相談しようという発想が出てこない」という。情報共有の体制や訓練への参加は重要であるが、参加するだけでなく、**平時からの実体のあるコミュニケーション**が有事の際に重要となる。

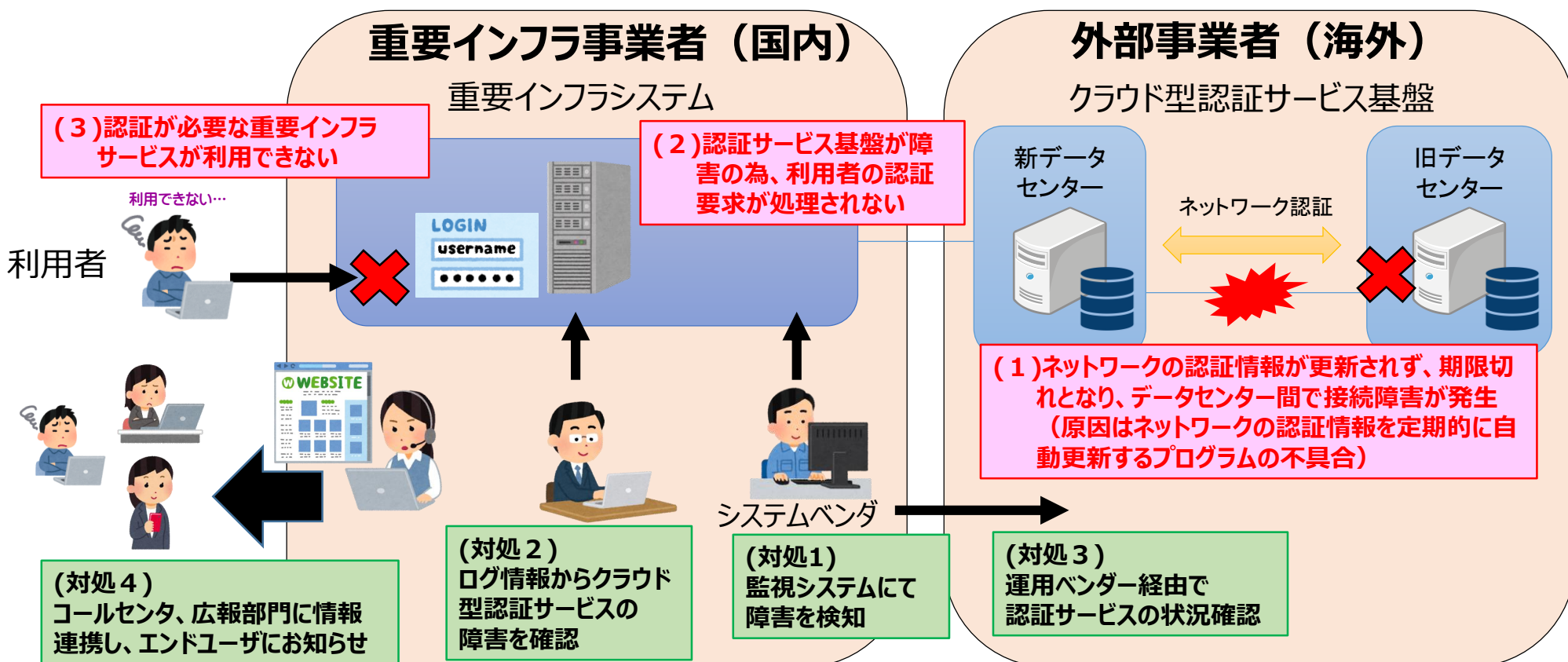
重要インフラ事業者内で発生した事案への対応事例（No. 7, 8）から

- 機器の故障等、偶発的な要因で発生する障害は、完全に防止することは困難であるが、事業上重要なシステム/サービスについては、各分野の安全指針等を参考に、迅速に対処・復旧するための対策を**設計段階から検討する**必要がある。
- 従業員による不正等、人為的に発生する要因は、自組織で扱う情報の重要性等も考慮し、セキュリティリスクについて、システム面、運用面のアプローチで低減するとともに、**実行動機の抑止に繋がる対策**についても従業員への研修等、教育面のアプローチを検討する必要がある。

※ 個々の事例ごとの他の気付き・教訓については、各事例の項を参照。

事例 1 インターネットサービス利用時の認証の障害 1/2

- インターネットを通じて提供される重要インフラサービスにおいて、利用時に認証が必要な一部のサービスが利用できなくなる事象が発生。
- 原因は、利用者の認証に使用している外部事業者のクラウド型認証サービスの障害。当該外部事業者では、データセンターの移行のために新旧データセンターを暫定のネットワークで接続しており、そのセキュリティ強化のためにネットワーク認証を導入していたが、認証情報の有効期限が切れたことにより、通信断が発生。
- 恒久対策として、特定の外部事業者 1 社のサービスに依存しないよう、複数の認証方法の導入を検討。



事例 1 インターネットサービス利用時の認証の障害 2 / 2

【1 背景】

- インターネットを通じて提供される重要インフラサービスにおいて、利用者の認証に外部事業者（海外）のクラウド型認証サービスを採用していた。
- 外部事業者では、クラウド認証サービスの基盤があるデータセンターの移行を進めており、新旧データセンター間を暫定ネットワークで接続し、セキュリティ強化の為にネットワーク認証を導入していた。

【2 検知】

- 監視システムにてクラウド型認証サービスの異常を検知。
- 障害発生直後からコールセンターに多数の問い合わせ。

【3 対処】

- 重要インフラシステム側のログのエラー情報から、クラウド型認証サービスでの障害であることを特定。
- システムベンダ経由で、外部事業者から障害に関する調査・対応状況を収集し、テレビ会議で利用者対応部門（広報、コールセンター等）にリアルタイムに共有。
- 外部事業者による復旧までの間、ホームページとコールセンターを通じて、復旧状況を利用者に逐一提供。

【4 原因】

- ネットワーク認証の認証情報の有効期限切れにより、新旧データセンター間の接続に障害が発生した結果、旧データセンター側のシステムに登録されていた利用者情報との照合ができなくなった。
- ネットワーク認証の認証情報は自動で更新される仕組みであったがプログラムの不具合により更新されなかった。

【5 再発に備えた対策】

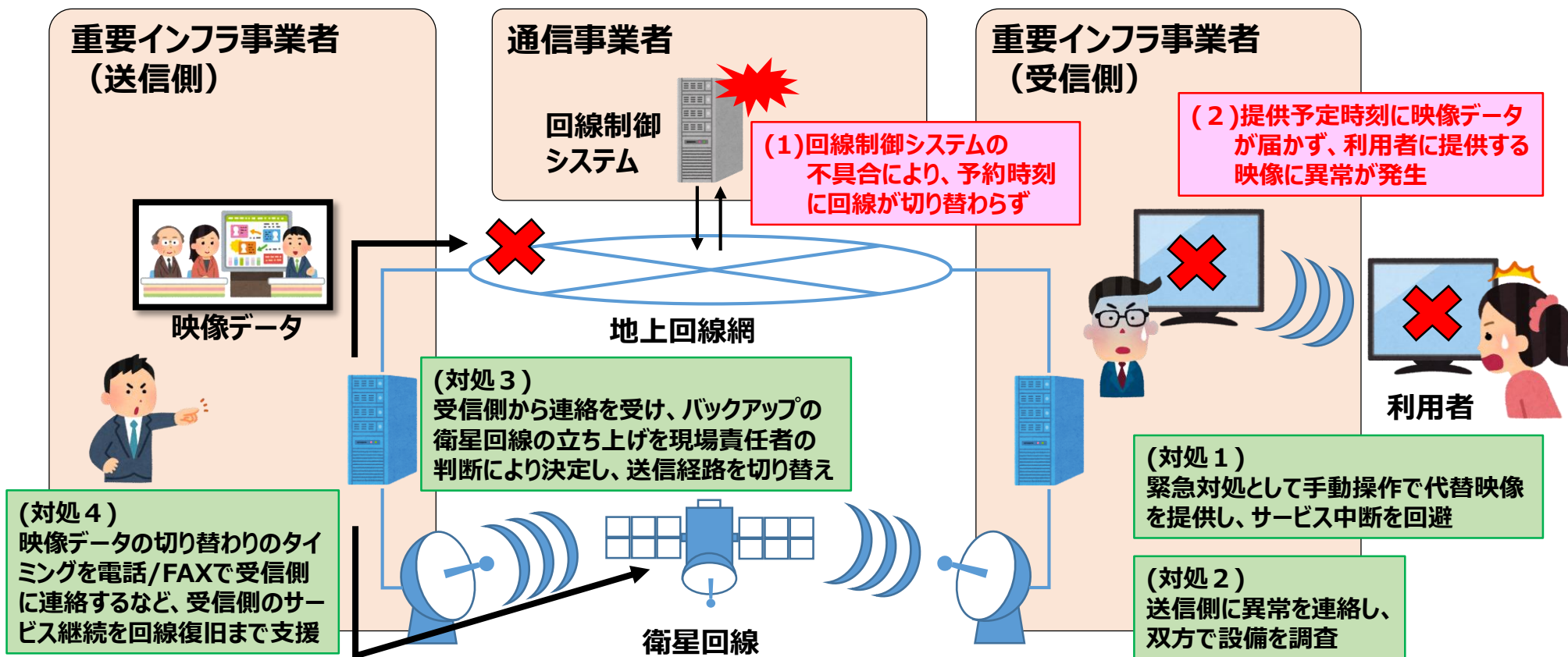
- 重要インフラサービス側の認証機能の多様化や代替手段の導入を検討し、特定 1 社への依存を解消。
- 外部事業者の現地の運用者とのホットラインを構築し、日本人を経由する連絡体制で生じる時間ロスを解消。

【6 得られた気付き・教訓】

- 自力でのサービス継続のための代替手段の必要性**
外部事業者による利用者認証サービスを利用していたが、その障害時に自組織側で発動できる代替手段がなく、外部事業者による復旧を待たざるを得なかった。自力でのサービス継続のため、利用者への代替の認証手段を用意しておくべきであった。
- 有事を想定した利用者対応訓練の効果**
重要インフラサービスの障害では利用者からの問い合わせが急増するが、有事の情報公開についてシステム部門と利用者対応部門で定期的に訓練を実施しており、混乱なく対応できた。
- 外部事業者との緊急時の連絡体制整備**
海外の外部事業者という事もあり、連絡ルートにシステムベンダや日本法人が介在しているため、復旧状況の把握に時間がかかった。本件を受け、経営幹部が主体的に交渉に動き、現地の運用者と直接連絡が取れるホットラインを構築した。
- 海外サービス利用時の現地時差**
海外のサービスを利用する場合、メンテナンス等が相手国の深夜時間帯に実施されると日本時間で業務時間帯にあたることもあることから、サービス提供側の国と利用者側の国との時差によるリスクの見直しを行った。

事例 2 重要インフラ事業者間での映像データ送受信の中断 1 / 2

- 重要インフラ事業者間で映像データの送受信に使用している回線が、予約日時に切り替わらず、接続障害が発生し、受信側の重要インフラ事業者では予定の映像を利用者に提供できなくなった。
- 回線が切り替わらなかった原因は、回線を提供している通信事業者の回線制御システムの不具合。
- 通信事業者の回線網は冗長化されているため、回線起因の障害は当該重要インフラ事業者では前例が無かったが、「サービス（映像の提供）の継続を最優先に行動」という共通の対応方針の下、衛星回線経由のルートに切り替え、迅速に復旧。



【1 背景】

- ・ 重要インフラ事業者間で、サービスに使用する映像データを送受信する際、通信事業者の回線を利用している。
- ・ 回線は、通信事業者の回線制御システムに使用時間帯を予約設定することで時間帯毎に切り替わる仕組み。

【2 検知】

- ・ 受信側の重要インフラ事業者のオペレーターが、映像提供予定時刻に映像データが届いていないことを発見。同時に、受信側の重要インフラ事業者では利用者に提供する映像に異常が発生。
- ・ 送信側の重要インフラ事業者は、受信側からの連絡により、映像データが正常に届いていないことを認識。

【3 対処】

- ・ 回線制御システムの予約含め、重要インフラ事業者側の操作ミスや設備不具合を調査したが、該当無し。
- ・ 重要インフラ事業者から通信事業者に問い合わせたが、原因・復旧共に不明との回答。
- ・ 送信側で、別の通信事業者が提供するバックアップ用の衛星回線への切り替えを決定し、送信のタイミング等を連絡。
- ・ 受信側は、通信事業者の回線の復旧までの約30分間、手動操作によりサービスを継続。

【4 原因】

- ・ 通信事業者の回線制御システムのソフトウェア不具合。（通信事業者内でも回線は冗長化されていたが、制御するソフトウェア側の不具合のため機能せず）

【5 再発に備えた対策】

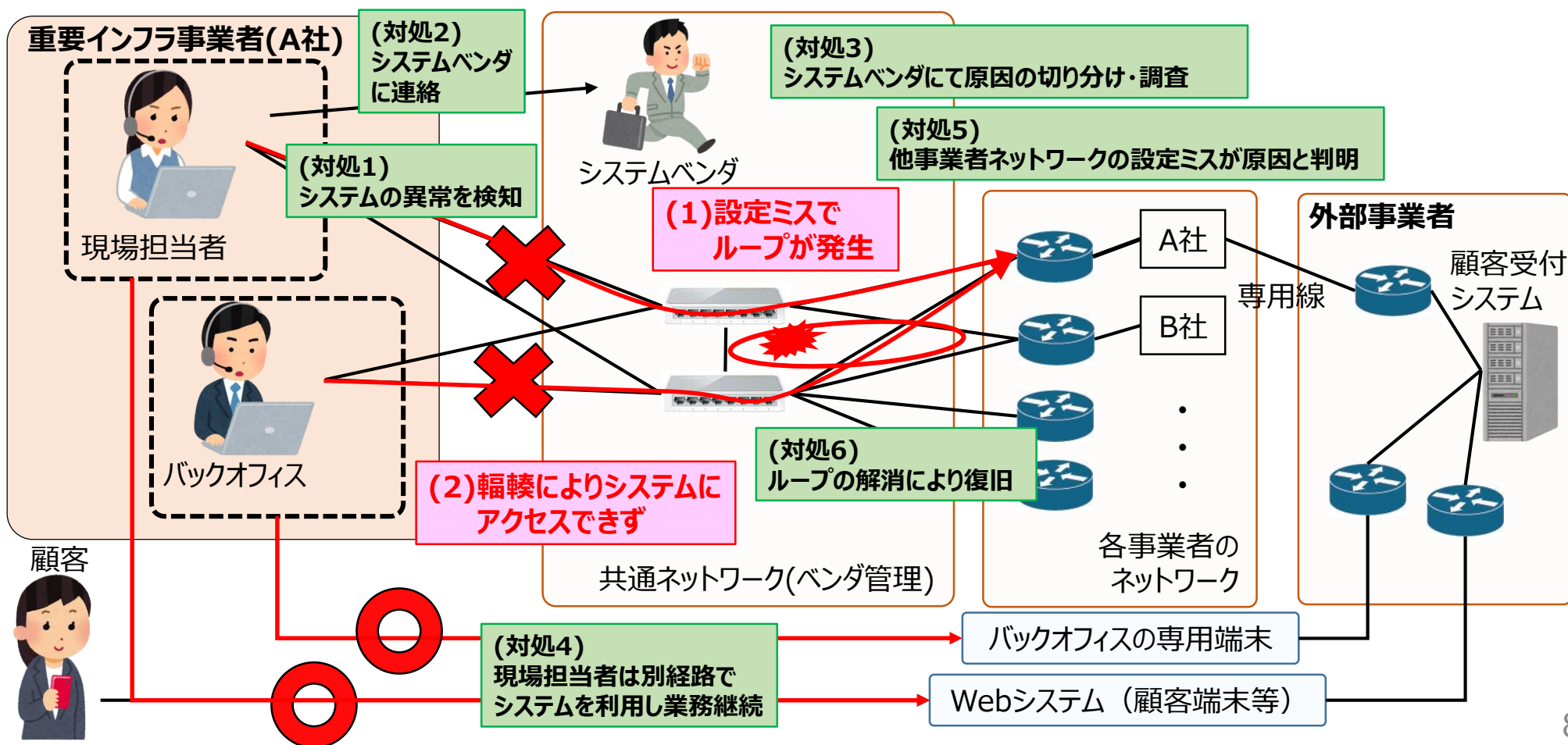
- ・ 回線制御システムの不具合の解消（通信事業者にて実施）。
- ・ 通信事業者に対する、異常発生時の迅速な情報提供の依頼。
- ・ 緊急時対応プロセスの更なる効率化による有事の切り替え時間短縮、及びオペレーター全員への定期訓練等による手順の浸透。
- ・ 自組織全体、及び同じ分野の重要インフラ事業者への事例共有による、分野内での類似事案への対処能力の強化。

【6 得られた気付き・教訓】

- ・ **事業継続を最優先として動く組織のマインド**
事業継続のために優先すべき対応がオペレーションの現場まで浸透し、かつ判断の権限を持っていることが、迷いのない迅速な対処に繋がった。
- ・ **日常的な障害対応訓練**
コンティンジェンシープラン等を整備するだけでなく、日常的に障害対応訓練を行っており、誰が対応することになっても判断し対応できるレベルまで緊急時のオペレーションが成熟していた。
- ・ **依存度の高い外部サービスの障害に備えた対策**
経営上重要な事業に使用している外部事業者のサービスで障害が発生する事態に備え、代替の外部サービスを確保していたことが、復旧時間の短縮に大きく寄与した。
- ・ **他事業者任せにしない再発防止**
障害の直接原因は他事業者であったが、そのような場合に備えた自組織側の対応プロセスについても見直した。

事例3 重要インフラサービスの受付業務の遅延 1/2

- 複数の事業者が利用する顧客受付システムを接続する共通ネットワークにおいて、ある事業者の設定ミスによりループが発生。ネットワーク全体が輻輳し、複数の事業者が当該システムを利用できなくなった。
- 現場担当者は、別の経路を利用して顧客受付システムに接続し、業務を継続。
- 恒久対策として、システムベンダでネットワーク機器の交換および障害検知のためのログ監視ツールを導入。



事例3 重要インフラサービスの受付業務の遅延 2/2

【1 背景】

- 複数事業者が利用する顧客受付システムのネットワークに、個々の重要インフラ事業者が管理する部分と、複数事業者が利用する部分（共通ネットワーク）がある。
- 共通ネットワークについては、システムベンダに保守を委託している。

【2 検知】

- 重要インフラ事業者の現場担当者が、当該システムが利用できなくなっている状態を検知した。

【3 対処】

- 現場担当者は、まずシステムベンダに連絡し、ネットワークベンダにて原因の切り分け作業を行った。
- 切り分け作業の結果を元に、システムベンダにて調査を開始した。
- 経路のループの箇所を特定し、設定を修正することでネットワークを正常化した。
- 顧客受付システムは別のネットワーク上に設置されていたため、現場担当者はインターネット経由、もしくはバックオフィスの専用端末で当該システムに接続することで顧客の受付業務を継続した。

【4 原因】

- 共通ネットワークに接続する他事業者の作業ミスで、当該事業者と共通ネットワークとの間でループが発生した。
- 共通ネットワークが輻輳し、接続された複数の事業者において、顧客受付システムが利用不可となった。

【5 再発に備えた対策】

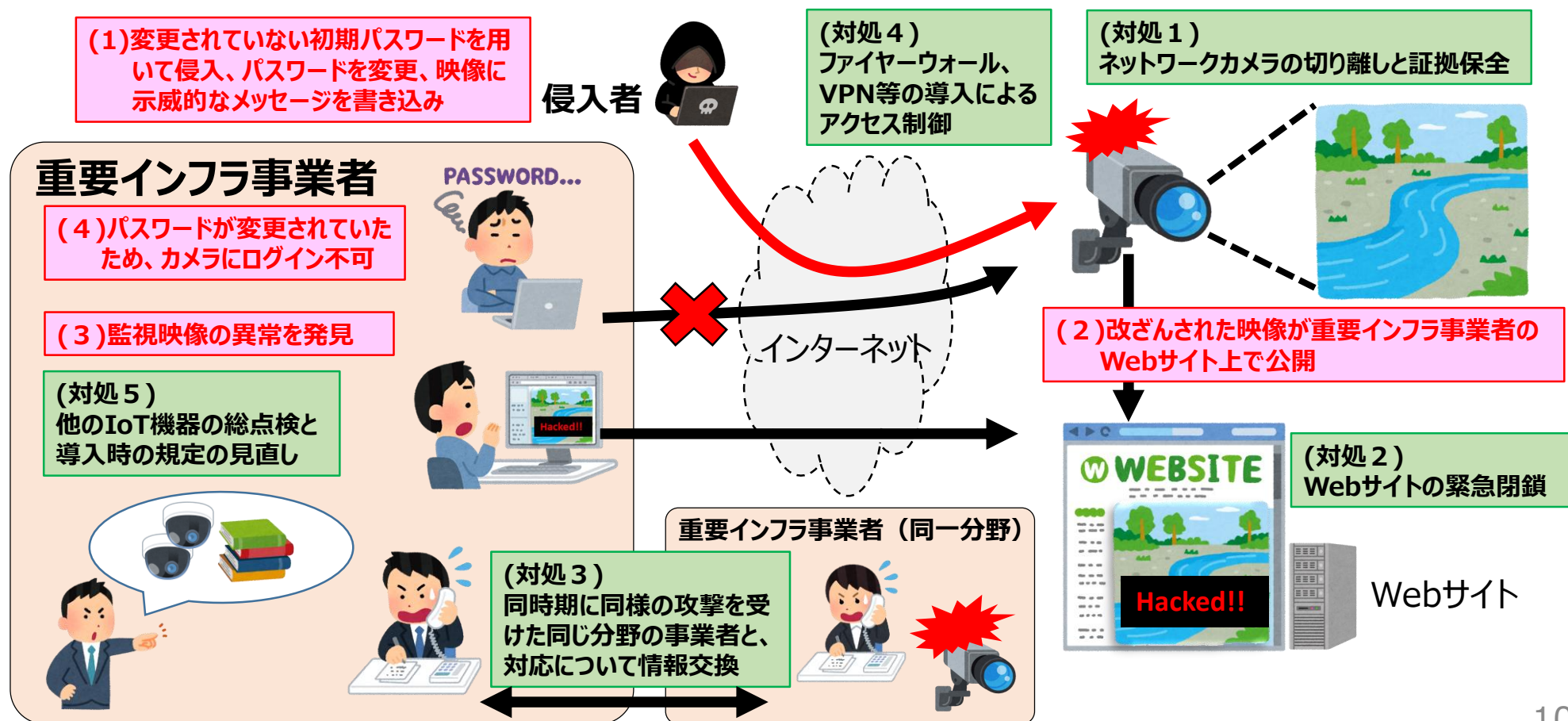
- システムベンダにおいてループが発生しないネットワーク機器および障害検知のためのログ監視ツールを導入。
- 対処に時間がかかったことへの対策として、委託先のシステムベンダの保守体制（緊急時の情報伝達経路等）の見直しを依頼。
- 顧客受付システムを利用する事業者間で事例を共有。

【6 得られた気付き・教訓】

- **外部サービスでの障害に備えた自組織側での対応訓練**
SLAを厳しくする、抜け漏れがないようにRFPに記載する等の対策を行っていても、外部サービスの障害を完全に防ぐことは困難である。外部サービスが利用不可となったことを想定し、日頃から訓練を行っていると、システムが利用できなくても業務を継続できると考えられる。
- **委託先との連絡体制整備**
対処に時間がかかった原因の一つとして、「委託先の情報伝達がしっかりしていなかった」、「対処方針を示す指示役（旗振り役）がいなかった」といった点が挙げられる。緊急時における委託先との情報伝達経路を整備するとともに、委託先における体制についても把握しておくことが重要である。
- **同一システムを利用する間での事例の共有**
本事案は、ある事業者の設定ミスが他事業者に波及したという事例であり、利用者側でシステムや対応の改善のみで完全に防ぐことは困難である。同様の事案を起こさないように、関係する事業者間で事例の共有を行うと良い。

事例4 IoTデバイスへの不正侵入及び改ざん 1 / 2

- 重要インフラ事業者が管理する施設情報の監視に使用していたネットワークカメラが外部から侵入され、管理ログインができなくなる、映像が改ざんされる、などの被害が複数の分野で発生した。
- 侵入された原因は、第三者が容易に類推できるパスワードや、アクセス制御の不備。
- 今回の件を受け、ネットワークに接続するIoT機器のパスワード設定やファイヤーウォール等でのアクセス制御の総点検を行ったほか、導入時のセキュリティ上の考慮事項を内規に盛り込んだ。



事例 4 IoTデバイスへの不正侵入及び改ざん 2 / 2

【1 背景】

- 重要インフラ事業者の施設情報の監視・公開を目的として、ネットワークカメラを設置し、映像をWebサイトで公開。

【2 検知】

- 施設の映像を確認するためにアクセスした従業員が、複数のカメラの映像内に不審なメッセージを発見。
- ネットワークカメラのパスワードが侵入者により変更され、管理画面にログインできなくなっていた。
- 他の事業者でもネットワークカメラに対し、同様の不正侵入が確認され、メーカーから注意喚起が発出された。

【3 対処】

- Webサイトでの監視映像の公開を停止し、当該カメラに対する外部からの直接アクセスも制限。
- 当該重要インフラ事業者が保有している全てのIoT機器の状況を調査。念のためパスワードを全て変更。
- 対応方針について、同時期に同様の攻撃を受けた同じ分野の事業者と情報交換、外部の調査機関にも相談。
- 侵入された機器をネットワークから切り離れたうえで、ログ等の痕跡を保全するため電源は維持し、外部の調査機関立ち合いのもと、調査。1日分のログしか残らない設定となっていたため、侵入元特定には至らず。
- Webサイト閉鎖中の代替措置として、従業員による目視で施設の監視を行い、状況をWebサイトやTwitterを通じて利用者に逐一伝達。
- 代替機器を手配し、監視映像の公開を再開。

【4 原因】

- ネットワークカメラのパスワード設定は、導入時、事業者と機器設置業者のいずれでも検討されず、初期設定のまま運用されていた。
- ネットワークカメラへの直接アクセスによる閲覧は許可する予定はなかったが、特にアクセス制限を行っていなかった。

【5 再発に備えた対策】

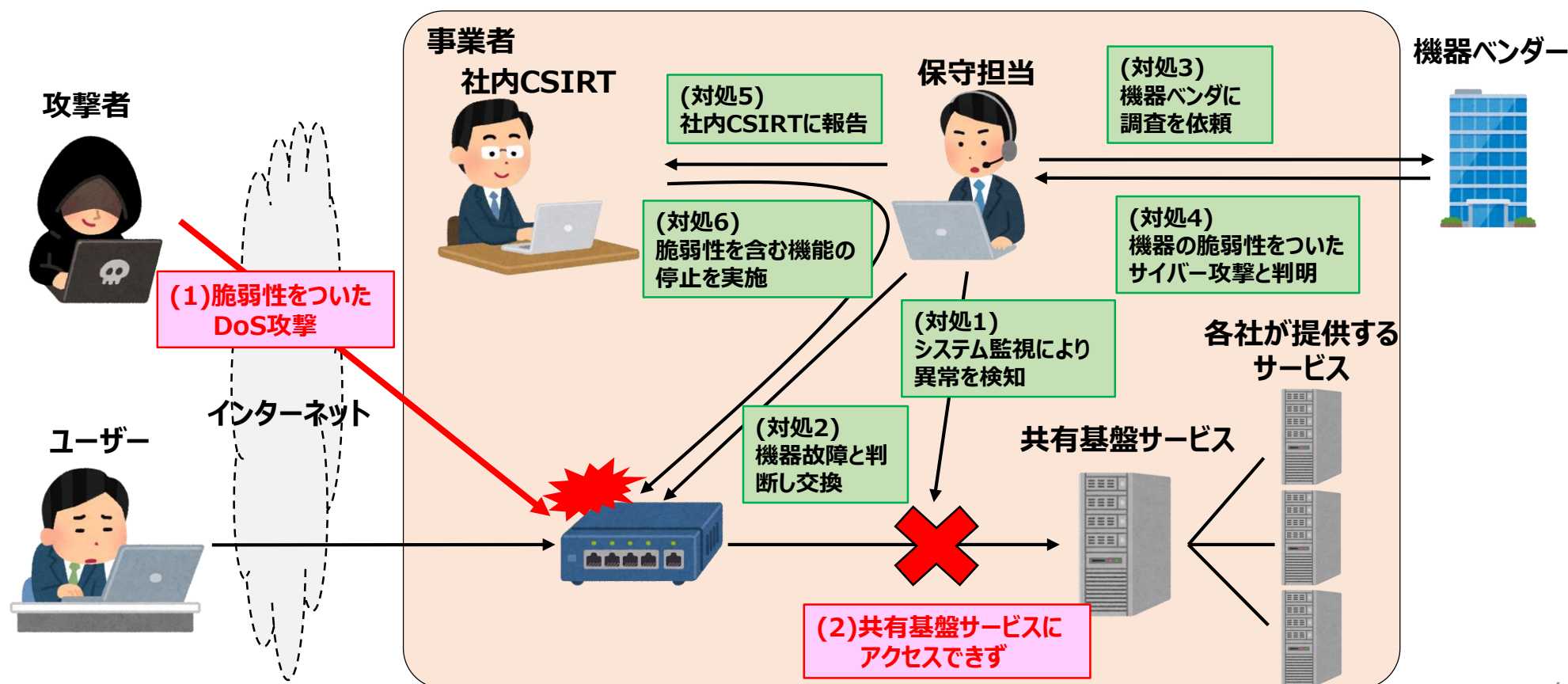
- IoT機器のセキュリティ設定やログの取得・保存期間に関して、導入時および運用時の手順を見直し、利用部門への研修も企画。
- IoT機器を調達する際の検討事項として、認証やアクセス制御等のセキュリティ機能の観点を追加。
- ネットワークカメラへのアクセスはVPN経由のもののみ許可するようにし、外部からアクセスできないようにネットワークを構成変更。

【6 得られた気付き・教訓】

- **IoT機器を悪用されるリスクの認識**
IoT機器の初期パスワードは、公開されているマニュアル等を通じて誰でも容易に知り得ることを認識し、悪用されないように導入時に必ずパスワードを変更する。メーカーが発信する脅威情報にも注意し、注意喚起等が行われた場合は、自組織の利用形態におけるリスクを点検し対応の要否を検討する。
- **同様の攻撃を受けた事業者との情報交換の有用性**
同時期に他の事業者でも同様の攻撃を受けたことを知っていたため、攻撃手口や対応方法等について当該事業者と情報交換しながら対応を進めることができ、平時から互いに相談できる関係作りの重要性を認識した。

事例5 脆弱性を悪用した攻撃 1 / 2

- ネットワーク機器の脆弱性をついたDoS攻撃により、複数のWeb上のサービスが停止した。
- 当初はシステム障害として対応したが、ベンダに調査を依頼したところ、ネットワーク機器の特定の機能に含まれる脆弱性をついたサイバー攻撃が原因だと判明し、社内CSIRT部門に報告した。
- 脆弱性を含む機能の停止、及びファームウェアのバージョンアップを実施した。



事例 5 脆弱性を悪用した攻撃 2 / 2

【1 背景】

- ・ 事案発生の数日前、当該脆弱性を利用した攻撃があったという情報をつかんだ。
- ・ 該当機器には、情報をつかんだ10日後の、月次メンテナンスの日にパッチを適用する予定であった。

【2 検知】

- ・ システム監視にて検知し、保守担当にて確認した。
- ・ ネットワーク機器のステータスランプが点滅状態（正常時は点灯）になっていたため、ハード故障と判断し対応した。

【3 対処】

- ・ ネットワークから該当機器を切り離しバックアップ用の機器で運用し、翌日には該当機器を交換した。
- ・ ベンダーにて該当機器のログ等を調査したところ、ネットワーク機器の特定の機能の脆弱性をついたサイバー攻撃が原因と報告があり、社内CSIRTに報告した。
- ・ 脆弱性を含む機能を停止し、ファームウェアをバージョンアップした。

【4 原因】

- ・ ネットワーク機器の特定の機能の脆弱性をついた攻撃が原因であった。
- ・ 該当機器では、アクセス制限を使用機能に応じたプロトコルとIPアドレスで実施していたが、本脆弱性がある機能に気がつかず、アクセスが可能な状態になっていた。

【5 再発に備えた対策】

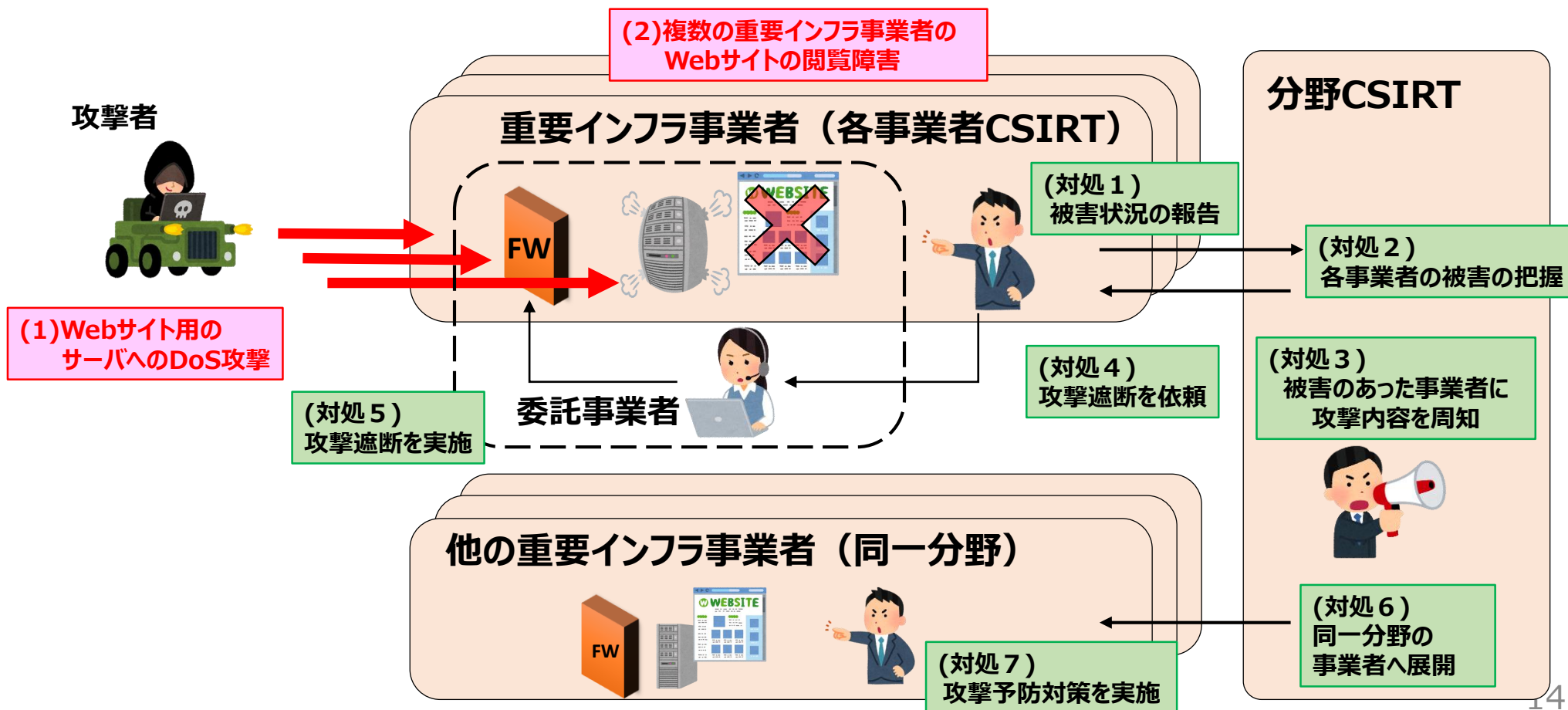
- ・ 本内容を社内、グループ会社で共有した。
- ・ 普段使用しない機能の脆弱性をついた攻撃であったことから、他にも各ネットワーク機器で動作中の機能を確認し、不要な機能を停止した。
- ・ ネットワーク機器への脆弱性が出た場合は、検証環境にて対象かどうかの確認を行う、診断ツールが利用できる場合は使用する等、社内ルールを変更した。
- ・ サイバー攻撃に関する勉強会を定期的実施することとした。

【6 得られた気付き・教訓】

- ・ **脆弱性へのパッチ適用の判断**
月次メンテナンスでパッチを適用するまでの間に攻撃を受けた。ネットワーク機器の脆弱性が公表された場合に、対応要否を迅速に見極めるために、検証環境にて影響有無の確認を行う、診断ツールが利用できる場合は利用するなど、運用を見直した。
- ・ **報告用フォーマットの改善**
最初からサイバー攻撃である可能性も視野に入れて対応できるよう、責任者への報告用フォーマットにサイバー攻撃が疑われる場合のチェックポイントを組み込んだ。
- ・ **セキュリティリテラシーの底上げ**
一部のセクションでは診断ツールでチェックができていたなど、部署ごとの対応にばらつきがあった。サイバー攻撃に関する勉強会等によりセキュリティリテラシーの底上げを図った。

事例6 広域DoS攻撃によるWebサイト閲覧障害 1 / 2

- ある分野の広範囲の重要インフラ事業者にDoS攻撃があり、運営しているWebサイトが閲覧できなくなった。
- 異常を察知した重要インフラ事業者が、当該分野の全体調整を行っている分野CSIRTに報告した。
- 報告により得られた内容から原因を特定し、被害を受けている事業者に攻撃元等の情報を展開することで、事態の収束を図った。また、被害を受けていなかった同一分野の重要インフラ事業者にも攻撃元等の情報を共有し、セキュリティインシデントの抑止に繋げた。



【1 背景】

- 複数の重要インフラ事業者において、Webサイトの運用を同一の事業者へ委託していた。

【2 検知】

- Webサイト運用担当者が、Webサイトの表示が不安定であることに気づいた。
- 外部機関からも「攻撃を受けているのではないか」、という指摘があった。

【3 対処】

- インシデントハンドリングを実施することとなっている事業者へ状況を報告し、関係する事業者全体の被害状況を把握した。
- 取りまとめられた状況から、攻撃元IPアドレス等の詳細な攻撃情報を関係事業者全体に周知した。
- 委託事業者へWebサイト運用サーバへの攻撃を遮断するよう指示した。

【4 原因】

- 委託先運用のサーバへのDoS攻撃

【5 再発に備えた対策】

- 委託先事業者へ指示し、関係事業者を防護しているファイアウォールに攻撃元と考えられるIPアドレスをリスト登録した。
- 早期に情報共有できる体制を構築し、サイバー攻撃があった際、関係する事業者へ素早く展開できるよう、共有体制の見直しを行った。

【6 得られた気付き・教訓】

・ 組織間の情報共有体制の構築

平時から関係する組織間で情報を共有し、連絡先を認識(顔の見える関係の構築)しておくことで、広範囲にわたるサイバー攻撃が発生した際に、スムーズな情報連携が確立でき、早期に事態を収束することが可能となると考えられる。

・ 自組織でのサイバーセキュリティの専門人材の登用・育成

システムやセキュリティの運用を外部委託している場合でも、有事の際に状況の正確な認識、事態への円滑な対処等を統制しながら進めることのできるサイバーセキュリティの専門人材は、自組織側でも確保する必要があることを認識した。専門人材の採用や自組織内での育成を、費用面等の制約条件も考慮して検討する。また、希望すれば専門人材としてのキャリアパスが選択できるような仕組みも検討する。

・ サイバー攻撃への対応ノウハウの定着

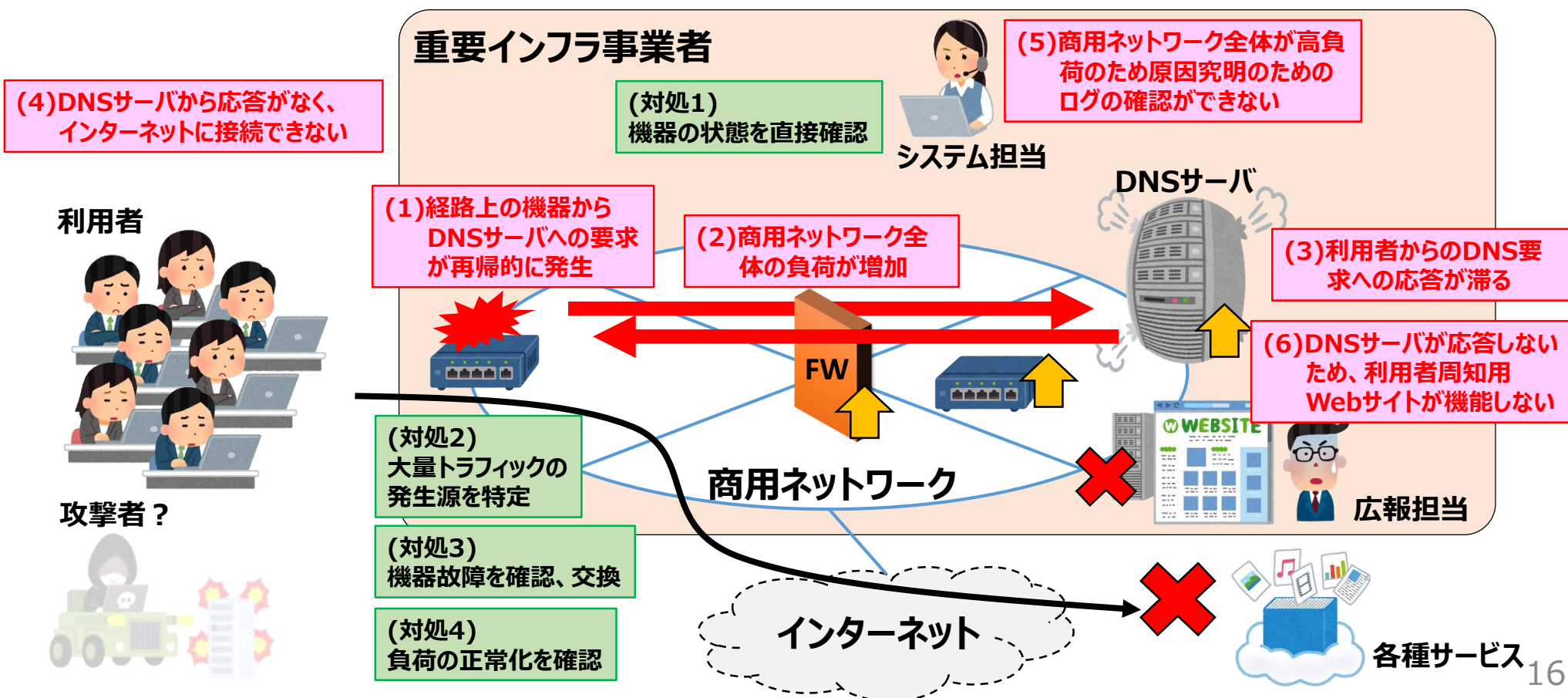
今回のサイバー攻撃への対応において、専用のマニュアルは存在していなかったが、攻撃を受けたシステムの運用監視を長期間行っていた、スキルのある担当者により、苦慮しつつも対応を行うことができた。今後はこの対応を組織として形式知化し他の担当者にも展開し、組織的に対応できるよう対策を行う。

・ DoS攻撃への対策

自組織の事業上、重要なサーバについては、ある程度の瞬発的なアクセス増加に耐え得るサーバリソースの設計や、通信量のモニタリング、特定IPからのアクセスの制限方法の導入等の対策を講じる。

事例7 商用ネットワークの高負荷による通信障害 1/2

- DNSサーバに通常の数十倍以上の大量のアクセスがあり、DNSサーバからの応答ができなくなったことで、利用者がインターネットに接続できなくなった。DNSサーバへのDoS攻撃の可能性も視野に入れ、調査を実施。
- 原因は、経路上のネットワーク機器とDNSサーバ間で大量のトラフィックが発生し、DNSサーバにアクセスしづらいなどの影響が発生したことによるもの。当該DNSサーバと同一セグメントにあるメールサーバ等への接続にも影響が出たほか、機器監視も同一セグメントで行っていたため、ログが追えない状態となった。
- 今後に備えた対策として、監視用の専用ネットワークの整備や帯域制御などの設計の見直しを行った。



事例 7 商用ネットワークの高負荷による通信障害 2 / 2

【1 背景】

- 利用者にインターネット接続サービスを提供していた。
- 機器の監視は、商用ネットワークで実施していた。
- 商用ネットワークは帯域制御しておらず、異常トラフィックを考慮した設計となっていなかった。

【2 検知】

- 利用者から、「インターネットに接続できない」という問い合わせがあった。
- 商用ネットワークの状況を確認するために、機器にアクセスしたが、輻輳が発生しており、確認できなかった。

【3 対処】

- 現地で直接各ネットワーク機器の通信状況を確認した。
- 通信内容から、特定の機器間で通信が再送され続けていることを確認。サイバー攻撃の可能性も考慮し、対応を実施した。
- 当該機器を再起動し、輻輳が正常化したことを確認後、機器を交換した。

【4 原因】

- 当該機器の一部ポートにおけるソフトウェアエラーにより、再帰的にリクエストが発生した。

【5 再発に備えた対策】

- 輻輳によるネットワーク機器のリソース逼迫も誘発していたため、帯域制御を実施した。

- 商用ネットワークの障害時にも状態把握が可能となるよう、監視専用のネットワークを別途構築し、監視方法を変更した。
- 利用者への周知方法として、自組織のWebサイトを利用する以外に、SNSの公式アカウントを取得し、周知方法を増やした。

【6 得られた気付き・教訓】

• 障害に強いネットワーク設計の重要性

ネットワーク機器の監視用のネットワークと、商用ネットワークを分離して整備することで、商用ネットワークで障害が発生してもネットワーク機器の状態をリアルタイムに確認でき、原因の切り分けがより迅速になる。監視用ネットワークと商用ネットワークを分けておくことが重要である。

DNSサーバ等、サービス提供上重要なサーバは、経路の異なる別セグメントに分散して配置するなどを設計段階で検討しておくことで、サービス提供の強靱性を向上できる。設計段階からの障害対策が重要である。

• 通信帯域の制限

通信帯域の制限により、ネットワーク機器のリソース逼迫を回避できることに加え、閾値超過時の早期異常検知にも役立つ。

• 周知方法の多様化

オンプレミスのみでWebサイトを構築している際、自組織のネットワークに異常があった場合、利用者への広報手段として機能しなくなる場合がある。外部のSNSで公式アカウントを運用する等、周知方法の多様化を考慮する必要がある。

事例 8 他人の認証情報の悪用による情報の不正取得 1/2

- ある重要インフラ事業者では、業務用データは部署ごとにアクセスを制限しており、他部署の従業員のIDによるアクセスは、通常であれば利用できない状態であった。
- 不正を行った従業員は、他部署の従業員（被害者）のIDからパスワードを類推し、本来アクセス権の無い他部署の業務用データにアクセスし、機密情報を印刷した上、私的利用していた。
- 複合機の印刷ログから不正を行った従業員を特定するとともに、全システムのパスワードを、より複雑性を高めた上で変更を行った。また、全従業員向けに研修を行うことで内部不正の抑止に関する意識向上を図った。



事例 8 他人の認証情報の悪用による情報の不正取得 2 / 2

【1 背景】

- 重要データ（顧客の個人情報等）と業務用データ（その他の情報）が別のシステムで管理されていた。
- 業務用データを取り扱うシステムへのログインは、部署ごとにアクセス制御を実施しており、関係する従業員のみ利用可能となっていた。

【2 検知】

- 該当部署で閲覧不可能な業務用データの資料が印刷され、プリンターに放置されていた。

【3 対処】

- プリンターのログを確認し、印刷した端末を特定した。
- 該当する端末を利用している職員に聞き込みを実施し、職員の特定に至った。
- サーバのアクセスログから、業務用データへの不正なアクセスを開始した時期を特定した。

【4 原因】

- 業務用データへのアクセスに使用するID・パスワードは、使用頻度が高いことから、類推しやすい平易なものになっていた。

【5 再発に備えた対策】

- パスワードの桁数を増やし、ランダムなものに設定しなおした。また、類推しやすい平易なものを設定不可とした。
- アクセスログを取得していることを含めて、全従業員向けに研修を実施し、内部不正の抑止に関して意識向上を図った。

【6 得られた気付き・教訓】

• 組織内での意識醸成と抑止

組織内で内部不正・不正アクセスに関する周知・教育を研修等を通じて徹底しておく必要がある。それと同時に、万が一不正アクセスが行われた際には、早期に検知できるよう、各システムのアクセスログを収集し、定期的に不審な点が無いか確認しておくことが肝要であると考えられる。

• 生体認証を含めた二要素認証の採用

重要なデータへのアクセスについては、ID・パスワードのような、代替しやすい手段だけではなく、第三者が不正利用しにくい生体情報を含めた二要素認証を採用することが望まれる。

• （参考）パスワード設定の重要性

パスワードの定期的な変更の要否については、議論の残すところではあるが、システムログインにおけるパスワードは、英数・記号・大文字小文字を含めた推察されにくいランダムな文字列で10桁以上で設定しておくことが望まれる。

NISCとしての見解は、パスワードの定期変更は基本は必要なしと考えている。ただし、万が一パスワードが流出した場合は速やかに変更すべきであると考えている。また、ZIPファイルのようなものの暗号キーである場合は、英数・記号・大文字小文字を含めた推察されにくいランダムな文字列で15桁以上で設定することが望まれる。

※参考資料：インターネットの安全・安心ハンドブックVer.4.00（NISC）

(<https://www.nisc.go.jp/security-site/files/handbook-all.pdf>)