資料４

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

2020年度　重要インフラにおける補完調査について

2021年5月31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、令和２年１月30日サイバーセキュリティ戦略本部改定）

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、2020年1月1日～2020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

No	事例	事例の概要
システム故障に起因した重要インフラサービス障害		
1	ハードウエア故障に伴う 重要インフラサービスの停止	ハードウエア障害が発生、予備系への自動切り替えも失敗し、定められた時間にサービスを開始できなかった。 復旧に向け、サービス再開時期を調整。記者会見を開催し、経営層が停止に至った経緯等を説明した。
2	クラウドでのシステム障害に伴う サービスの停止	クラウドサービス基盤でシステム障害が発生、同基盤上に構築した複数の重要インフラサービスが停止した。 クラウド事業者と連携しつつ、予め定めた優先順位に基づき復旧することで、業務影響を最小限に抑えることができた。
3	システム障害に伴う重要インフ ラサービスの業務遅延	業務システムのストレージがロックされたことでデータが閲覧できなくなり、重要インフラサービスの業務が遅延した。 事業継続計画に基づき、対応することで、業務を継続できた。
外部からのサイバー攻撃		
4	連携サービス間の脆弱性を 突いたサービスの不正利用	重要インフラ事業者は、利用者から身に覚えのないサービスの利用履歴があるとの問合せを短期間に複数受領した。 問合せが相次いだことを不審に思い、役員まで報告、被害を抑えるため、サービスの停止を迅速に判断した。
5	重要インフラ事業者における 2度のランサムウエア感染	重要インフラ事業者のサーバーがランサムウエアに感染、デスクトップ上のファイルが暗号化された。 端末・サーバーの迅速な使用禁止、保全指示により、ログ等から攻撃者の侵入経路を特定、さらなる再発を防止。
6	重要インフラ事業者における 「WannaCry」の感染	マルウエア感染した端末がネットワークに接続されたことで、パッチ未適用のサーバーを経由して感染が拡大した。 事象を特定し、封じ込めを行う等の対応により、業務を継続しながら、感染を収束させた。
7	重要インフラ事業者の 偽サイトの確認	偽サイト確認の連絡を受け、調査及び迅速な注意喚起等を実施した。 その後、同事業者のWebサイトが有害サイトと判定されたが、経営層と迅速に連携する等して、対応を実施した。
8	問合せシステムを悪用した 不正なメールの送信	第三者が重要インフラ事業者の問合せシステムを悪用し、不正なメールを送信した。 被害防止のため、Webサイト等で注意喚起を実施した。
9	業務用PCにおける サポート詐欺	業務用PCでWeb閲覧時に、警告音と有償サービス契約画面が表示された。その後、サポート詐欺と判明。 PCの迅速な使用中止判断により被害拡大を防止。また、迅速な代替PCの手配により、業務を継続できた。

補完調査の結果（総括）

事象

システム故障に起因した重要インフラサービス障害

外部からのサイバー攻撃

主な教訓等

○リスクマネジメント及び障害対応体制の強化が重要

- ✓ システム切替・業務再開に関する手順の関係者間合意と訓練が重要
- ✓ 定期的に情報共有できる体制の強化
- ✓ 外部委託先を含むコミュニケーションによるリスク共有及び緊急連絡体制の整備
- ✓ バックアップの重要性
- ✓ 脆弱性対応を含めた変更管理・資産管理の厳格化

○組織全体のマネジメントが重要（サイバー部門だけで閉じていない。）

- ✓ 事前に、サービスの復旧優先順位を経営層も含めて合意
- ✓ 事後に、サービス停止や公表時期等の組織的な判断

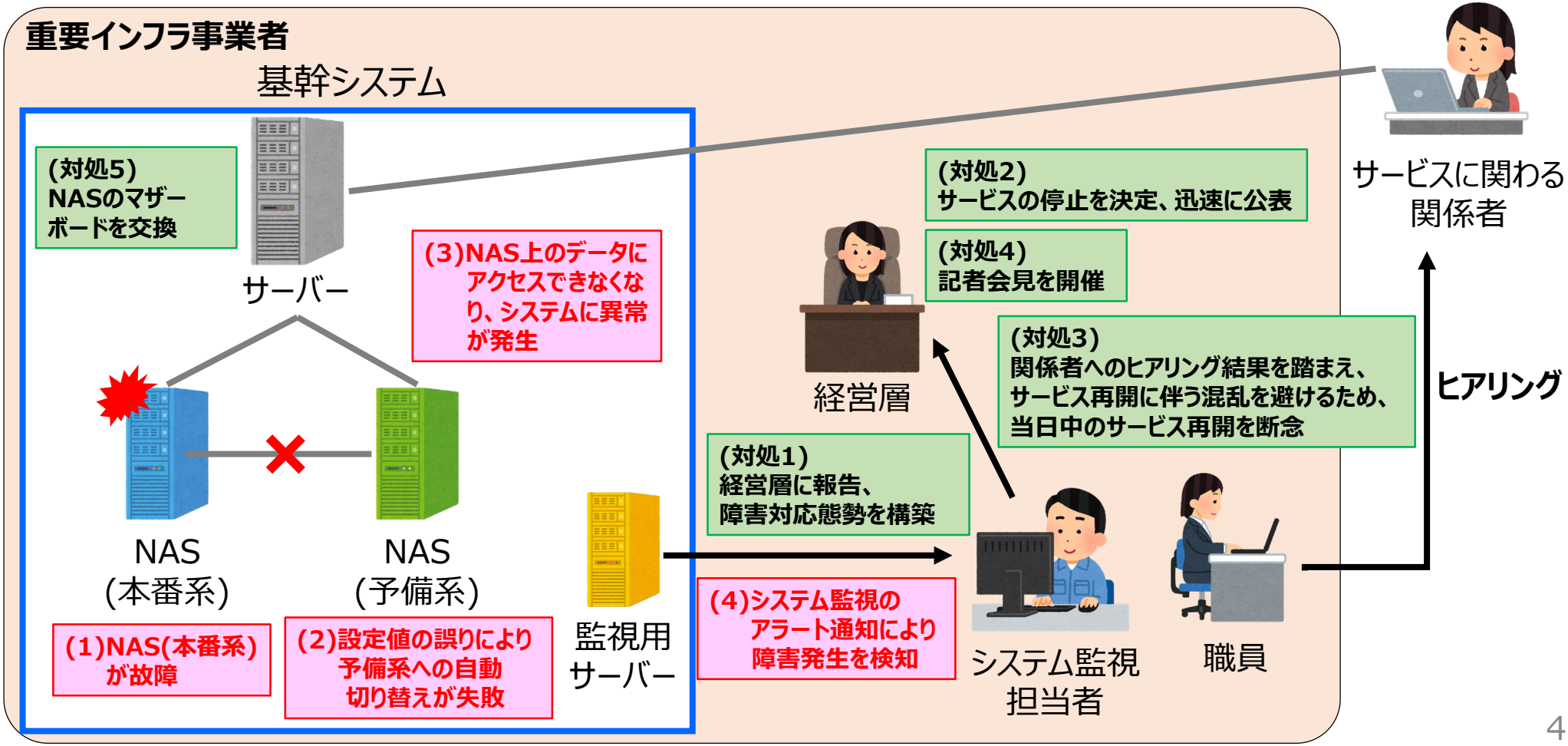
総括

いずれの良好事案に共通して、重要インフラ事業者の使命である持続的なサービス提供に対して、経営者の積極的な関与のもと、事業継続計画（IT-BCP）が策定され、事案発生時に組織全体で適時的確な行動がなされていたことが判明した

※個別事例ごとの気付き・教訓については、各事例スライドを参照。

事例1　ハードウエア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の基幹システムで使用しているNAS(ネットワークストレージ)に障害が発生、当該システムは冗長化していたが、設定値の誤りにより、予備系への自動切り替えに失敗、NAS上のデータにアクセスできなくなり、事業者のルールに基づき、重要インフラサービス(以下「サービス」という)の停止を決定した。
- システムの再立ち上げによる当日中のサービス再開も検討したが、事前にサービスに関わる関係者との取り決めなく、再開することが混乱を招くと重要インフラ事業者が判断、当日中のサービス再開を断念した。



事例1　ハードウエア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では、従前からシステム障害発生時にサービスを停止する条件を定めていた。

【2　検知】

- システム監視のアラート通知により、障害発生を検知。

【3　対処】

- システム障害の対策本部を迅速に設置、あわせて、経営層が参加するリスク管理にかかる会議体を開催。
- 事業者のルールに基づき、サービスの停止を決定、迅速に公表。
- 事前にサービスに関わる関係者との取り決めなく、障害発生当日中にサービスを再開することが、サービスの混乱を招くと判断し、当日中のサービス再開を断念。
- サービス停止の謝罪及び停止に至った経緯等を説明する記者会見を開催。
- NAS(ネットワークストレージ)のマザーボード交換を実施、翌日には、サービスを再開できるようにした。

【4　原因】

- 本番系システムで利用していたNASが故障、それに伴い、システム障害が発生。
- 本来、予備系システムに自動で切り替わる設計だったが、NASの設置値の誤りにより、自動切り替えに失敗。
- NASの設定値は、システム構築時は正しいもの(自動切り替えされるもの)だったが、NASの製品仕様の変更により、誤ったもの(自動切り替えされないもの)に変わってしまった。

【5　再発に備えた対策】

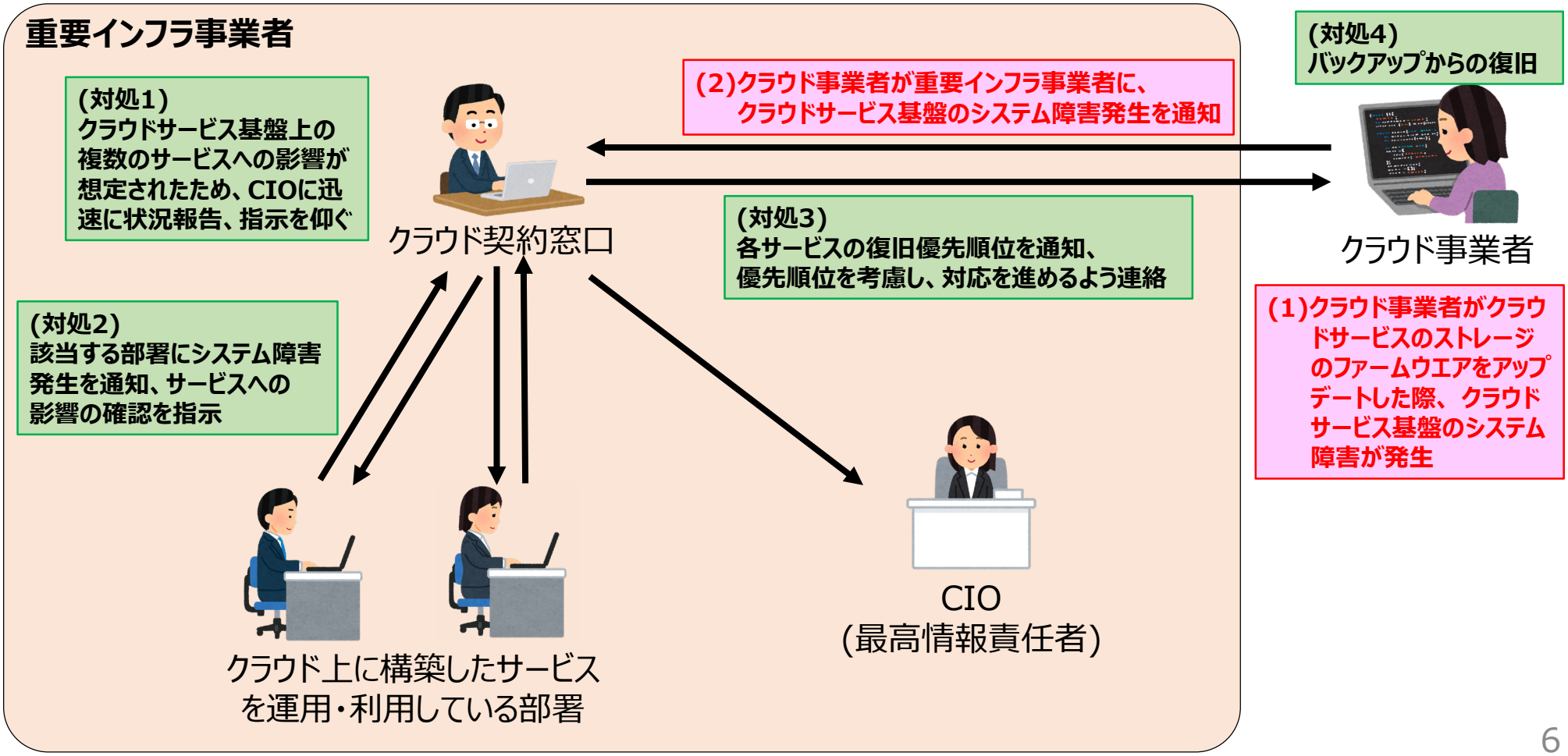
- システム障害時の予備系システムへの自動切り替えにかかる設定値の総点検を実施、自動切り替えが成功するかを確認。
- 障害発生当日にサービスを再開するための手続き、手順を関係者と検討し、今後は、サービスを迅速に再開できるようにした。

【6　得られた気付き・教訓】

- **設定どおりの稼働確保の重要性**
  冗長化したシステムに関して、システム障害発生時に自動で予備系システムに切り替わるか事前に確認することが重要。また、自動で切り替わらなかった場合に備えて、強制的な切り替え手順の事前確認とその訓練の実施(BCPの確保)があわせて必要。
- **レジリエンス(障害回復力)の強化**
  システム障害の防止に十分務めることは必要であるが、これに加えて、レジリエンス(障害回復力)の強化に資する取組も必要。サービスの復旧に際しては、サービスに関わる関係者全体で適切な手順を検討・合意し、それに従い復旧を進めることが重要。
- **経営層の適切な関与**
  サイバーセキュリティを考慮したリスク管理及び危機管理体制等について、経営層と対応組織が適宜コミュニケーションをとり、経営層指示の元、関係者全体で取り組むことが重要であることを再認識。
- **システム障害発生時の対応の明確化**
  障害発生時の対応を迅速に進めるため、障害発生時の対応、対応態勢、判断権者を明確化・マニュアル化しておくことが重要であることを再認識。

事例2　クラウドでのシステム障害に伴うサービスの停止　1／2

- クラウド事業者のクラウドサービス基盤でシステム障害が発生し、重要インフラ事業者のクラウドサービス基盤上に構築した複数の顧客向け重要インフラサービス(以下「サービス」という)が一時停止した。
- 重要インフラ事業者では、複数のサービスへの影響が想定されたことから、迅速にCIOに状況を報告し判断を仰ぎ、さらに、事前に定めていた各サービスの復旧優先順位に基づき、クラウド事業者と連携して、各サービスの復旧を進め、重要インフラサービスの障害による影響を最小限に抑えた。



事例2　クラウドでのシステム障害に伴うサービスの停止　2／2

【1　背景】

- 重要インフラ事業者とクラウド事業者は、クラウドサービス基盤の利用契約を締結、各部署は、クラウド基盤上に構築した重要インフラサービス(以下「サービス」という)を提供している。
- 重要インフラ事業者は、過去にも本事案と同一のクラウドサービス基盤でのシステム障害を経験していた。
- 上記事案対応時の反省から、重要インフラ事業者は、クラウド上のサービス一覧、各部署の緊急連絡先を事前に収集、サービスの復旧優先順位を定めていた。

【2　検知】

- クラウド事業者から、重要インフラ事業者のクラウド契約窓口に、クラウドサービス基盤のシステム障害発生にかかる連絡があり、本事象を認識。

【3　対処】

- CIO(最高情報責任者)に、システム障害発生を連絡、クラウド上の複数サービスへの影響が想定されたことから、状況を報告し、指示を仰いだ。
- クラウド契約窓口から該当する部署に、システム障害発生を通知、サービス影響の確認及び報告を指示。
- クラウド契約窓口から、クラウド事業者に対して、クラウド上の各サービスの復旧優先順位を通知、優先順位を考慮し、対応を進めるよう連絡。
- クラウドサービス基盤のバックアップから各サービスを復旧。

【4　原因】

- クラウド事業者が、クラウドサービスのストレージのファームウエアをアップデートした際、クラウドサービス基盤の障害が発生。

【5　再発に備えた対策】

- 重要インフラ事業者とクラウド事業者でサービスレベルの合意(SLA(Service Level Agreement)の締結)を実施。

【6　得られた気付き・教訓】

- **クラウド事業者とのサービスレベルの合意(SLAの締結)**
  重要インフラ事業者がシステムに求められるサービスレベルを十分に考慮した上、クラウド事業者とサービスレベルを事前に合意(SLA(Service Level Agreement)を締結)、そのサービスレベルを踏まえ、重要インフラ事業者がシステム障害発生時の対応を検討することが重要。
- **バックアップの確実な取得**
  クラウドサービス利用時は、クラウド事業者と締結したSLAを踏まえ、クラウドでのシステム障害時にもサービスが安定的に供給できるよう、システム基盤や各サービスのバックアップを定期的かつ確実に取得する。
- **システム障害発生時の迅速な対応**
  特に、クラウド等の影響が多岐に渡るシステム障害では、サービスの継続に大きな影響を及ぼすことも想定されるため、クラウドを利用するサービスの一覧、各部署への連絡先、経営層や広報担当等の緊急連絡先を事前に把握し、迅速に対応できるようにすることが重要。
- **サービスの復旧優先順位の決定**
  重要インフラ事業者が複数のサービスを実施しており、並行でシステム復旧を進めることが難しい場合は、経営層の指示に基づき、復旧優先順位を定め、対応するアプローチが有効。

事例3　システム障害に伴う重要インフラサービスの業務遅延　1／2

- 業務システム(以下「システム」)で、ハードウエア障害が発生したと誤認識した結果、ストレージがロックされ、データが閲覧できなくなり、重要インフラサービスの業務が一時的に遅延、サービス利用者がサービスを受けられない等の事象が発生
- 事業継続計画に基づき、システム担当部署の職員がシステム上の情報を紙に印刷し、各部署の職員に配布。職員は、紙による事務処理等を行うことで、業務を継続。

重要インフラ事業者

(1)ハードウエア障害と誤認識した結果、ストレージがロックされ、データが閲覧できなくなった

(2)ハードウエア故障でなかったため、システム(予備系)に自動切替されず、影響が長期化

業務システム(本番系)

業務システム(予備系)

(対処5)
システム(本番系)を起動

(対処4)
システム(予備系)への手動切替を実施

(3)システムがフリーズし、情報が閲覧できない旨、システム担当部署に報告

システム担当部署

(対処1)
施設内にいるサービス利用者に、サービスを提供できないこと等を連絡、代替手段の実施にかかる協力を要請

サービス利用者

(対処2)
事業継続計画に基づき、システム上の情報を紙に印刷し、各部署に配布

各部署の職員

(対処3)
各部署の職員は、紙により業務を継続

事例3　システム障害に伴う重要インフラサービスの業務遅延　2／2

【1　背景】

- 重要インフラ事業者では、業務システム(以下「システム」)上で表示される情報をもとに、サービス利用者にサービス提供や受付業務等を実施していた。
- システムは、2系統(本番系と予備系)にしており、ハードウエア故障時には、予備系に自動切替されるようになっていた。

【2　検知】

- 重要インフラ事業者の各部署の職員が、業務システムがフリーズし、情報が閲覧できない旨、システム担当部署に報告したことで、事象が判明。

【3　対処】

- 施設内にいるサービス利用者に対して、サービスを提供できないこと等を連絡し、代替手段の実施にかかる協力を要請。
- 事業継続計画に基づき、システムの情報を紙に印刷し、各部署に配布し、重要インフラサービスが継続できるようにした。
- 故障の原因が、ハードウエア故障でなかったことから、予備系に自動切替しなかったため、手動切替を実施。
- 別途、本番系を起動し、完全に復旧。

【4　原因】

- SAN(Storage Area Network)インターフェースの障害により、ハードウエア障害が発生したと誤認識し、ストレージがロックされ、データを読み取ることができなくなった。

【5　再発に備えた対策】

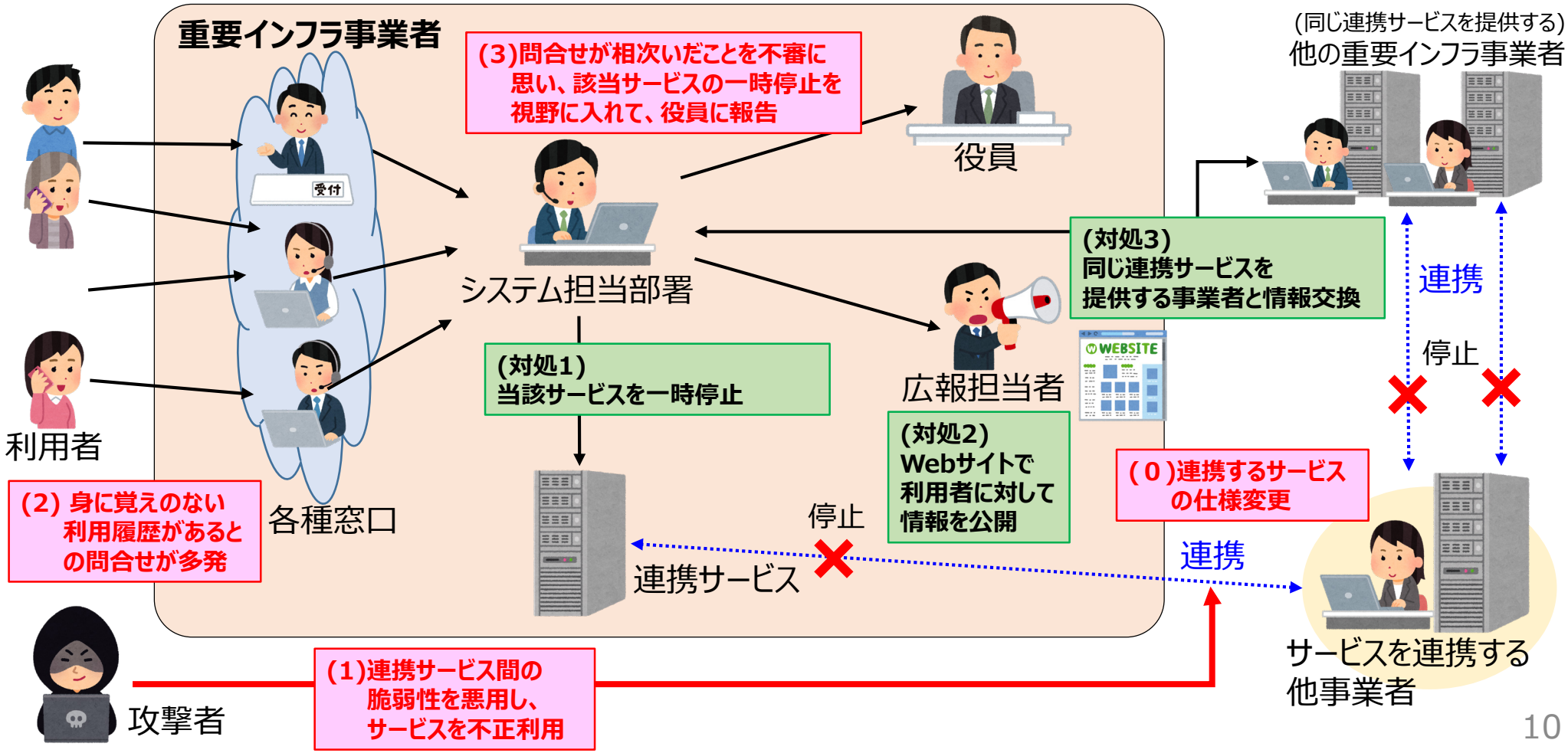
- システム(本番系と予備系)の独立性が担保されているか確認した。
- 本番系と予備系で同じストレージを参照していた部分は、障害時に当該ストレージを参照しない形で運用できるよう変更した。
- ストレージのロックを検知するプログラムを作成、当該プログラムを用いた定期的な監視により、障害を早期に検知できるようにした。
- 紙による業務継続手段は、緊急マニュアルに記載し、周知していたが、職員の定期的な異動等の理由により、運用が浸透せず、事象発生当日、職員に混乱が生じ、業務が遅延したことから、緊急時はシステム担当部署の職員を派遣する形に変更。

【6　得られた気付き・教訓】

- **システム(本番系と予備系)の独立性の確保**
  システムの冗長化を過信せず、システム(本番系)の各箇所が故障した場合に、システム(予備系)が支障なく起動できるかを事前に確認しておくことが必要。
- **各部署の実態に即した業務継続計画の策定**
  システム障害は発生するという前提の下、各部署の業務継続計画の策定が必要。あわせて、業務継続計画を実行するための準備(職員への定期教育、現場への有識者の派遣等)も必要。
- **システム(予備系)への自動切替処理の検証**
  システム(本番系)の障害時に、システム(予備系)に自動切替されるかを検証することが必要。運用開始後、仕様追加や変更を行った際は、特に留意する。システム(本番系)の停止による検証が望ましいが、難しい場合は、机上での確認等を行う。

事例4　連携サービス間の脆弱性を突いたサービスの不正利用　1／2

- 重要インフラ事業者は、他事業者が提供するサービスと連携するサービスを提供していたが、利用者から身に覚えのないサービスの利用履歴があるとの問合せを短期間に複数受領。
- システム担当部署は、問合せが短期間に相次いだことを不審に思い、役員まで報告、該当サービスを一時停止。原因は、サービスを連携する他事業者の仕様変更により生じた連携サービス間の脆弱性の悪用と判明。
- 再発防止策として、他事業者と連携する際のリスク評価に関する規定・要領を見直し、契約も変更。



事例4　連携サービス間の脆弱性を突いたサービスの不正利用　2／2

【1　背景】

- 重要インフラ事業者では、他事業者が提供するサービスと連携するサービス(以下「連携サービス」という)を提供していた。
- 連携サービス開始後、連携する他事業者が仕様を変更したが、重要インフラ事業者では把握していなかった。
- 利用者から、身に覚えのないサービス利用履歴があるという問合せを受領することは平時からあったが、そのほとんどは利用者の勘違いによるものであった。
- 利用者から、自身のサービス利用履歴を確認したところ、身に覚えのないサービスの利用履歴があるとの問合せを短期間に複数受領した。

【2　検知】

- システム担当部署は、同様の問合せが短期間に相次いだことを不審に思い、該当サービスの一時停止を視野に入れて、役員まで報告した。

【3　対処】

- 同日中にサービスを一時停止した。
- 同日中に事業者内及び関係機関等へ情報を共有し、Webサイトで利用者に対して情報を公開した。
- 同じ連携サービスを提供する他の重要インフラ事業者とも情報交換した。

【4　原因】

- サービスを連携する他事業者の仕様変更により生じた連携サービス間の脆弱性が悪用された。

【5　再発に備えた対策】

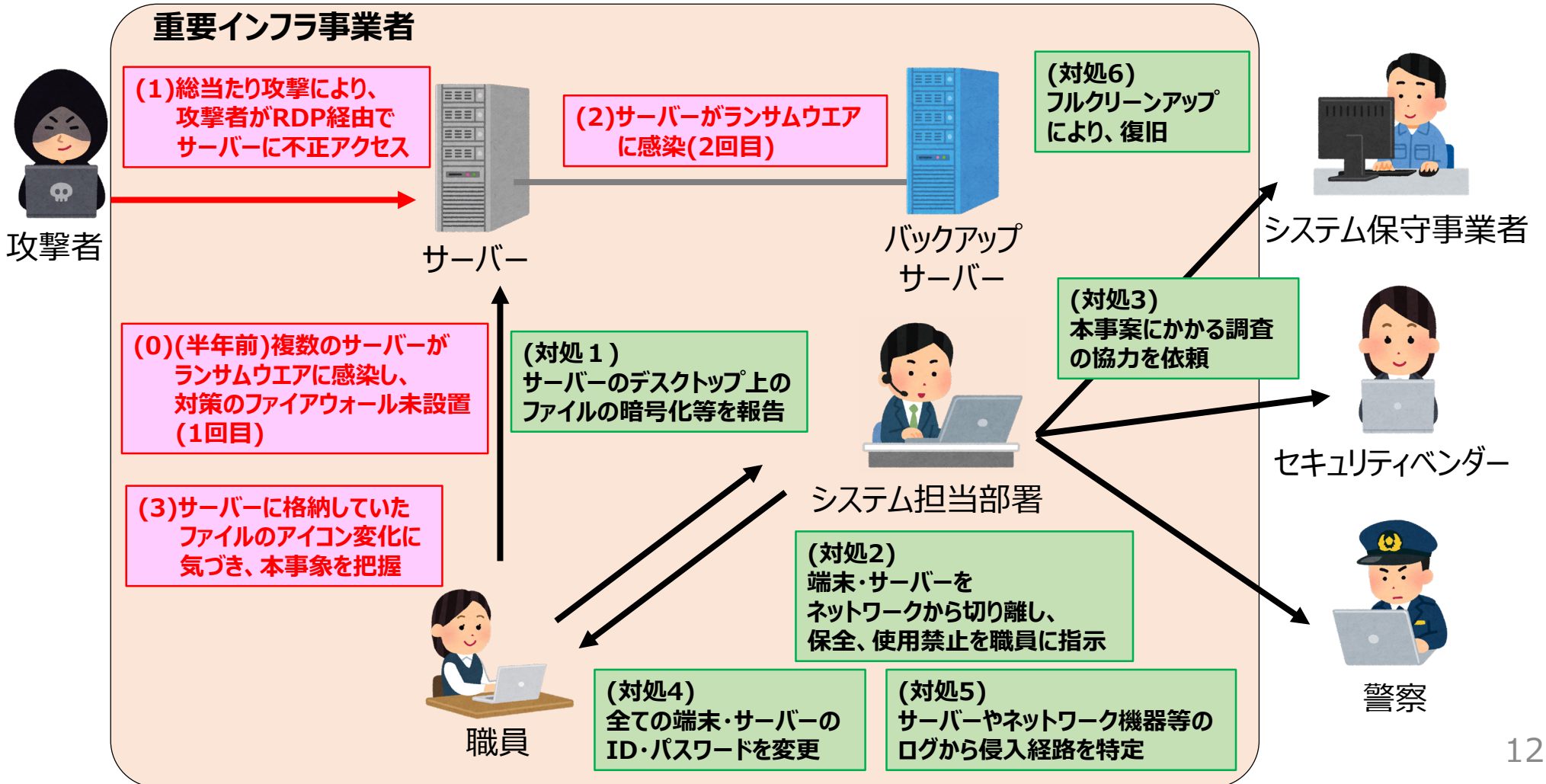
- 他事業者の仕様変更により生じた脆弱性を塞ぐよう、連携サービスを修正した。合わせて、他事業者でも、連携するサービスを修正した。
- 他事業者と連携する際のリスク評価に関する事業者内の規定・要領を見直し、これに合わせ、他事業者との契約を変更した。

【6　得られた気付き・教訓】

- **ヒヤリハット情報の迅速な共有体制の整備**
  普段あまり問題にならない報告でも、漏らさずに事業者内で素早く共有する体制が整っていたことで、事案を早期に覚知できた。
- **緊急時の統一した対応体制の構築**
  サイバー攻撃等の事案に対しても、災害時と同様に、緊急時の統一した対応体制の中で対応したことで、事案の覚知後、迅速にサービス停止の判断を実施、被害の拡大防止へつながった。
- **適時・的確な情報発信**
  緊急時対処マニュアルに基づき、迅速に第一報を公表し、その後も適宜必要なタイミングで情報を公表したことで、被害の早期発見へつながった。また、同じ連携サービスを提供していた他の重要インフラ事業者の対応にも貢献した。
- **他事業者と連携するサービスの仕様変更時のリスク評価**
  他事業者と連携するサービスを提供する際には、それぞれのサービスの仕様変更が脆弱性を生む可能性があることを認識し、双方で情報共有を密に行い、都度必要に応じてリスク評価等を実施することが重要である。

事例5　重要インフラ事業者における2度のランサムウエア感染　1／2

- 重要インフラ事業者の職員が、サーバーのデスクトップ上のファイルが暗号化されていることを認識。
  原因は、ランサムウエアの感染で、当該ランサムウエアは機密情報の窃取を伴うものではなかった。
- 重要インフラ事業者は、本事案の半年前にも、サーバーがランサムウエアに感染。その対策で、ファイアウォールを導入予定だったが、新型コロナ禍に伴い調達できず、2度目のランサムウエア感染が発生。



事例5　重要インフラ事業者における2度のランサムウエア感染　2／2

【1　背景】

- 重要インフラ事業者では、本事案の半年前に、サーバー等がランサムウエアに感染(1回目)。
- その対策で、ファイアウォールを導入予定だったが、新型コロナ禍に伴い調達できず未設置。
- 事案1回目では、端末やログの保全が遅れたため、調査に必要な情報が揃っておらず、不正アクセスの原因を特定できなかった。

【2　検知】

- 重要インフラ事業者の職員が、サーバーのデスクトップ上のファイルの暗号化に気づき、事象を把握。

【3　対処】

- システム担当部署が、端末・サーバーを、ネットワークから切り離し、保全、使用禁止を迅速に指示。
- システム担当部署が、システム保守事業者、セキュリティベンダー、警察に連絡、当該事案の調査にかかる協力を依頼。
- サーバーやネットワーク機器のログ等から、侵入経路を特定。
- 全ての端末・サーバーのID・パスワードの変更。
- サーバーのフルクリーンアップにより復旧。

【4　原因】

- サーバーがリモートメンテナンスのため、インターネット経由でリモートデスクトップ(RDP)接続可能であり、ID・パスワードも推測可能なものであったため、総当たり攻撃により、RDP経由で組織内に侵入された。

【5　再発に備えた対策】

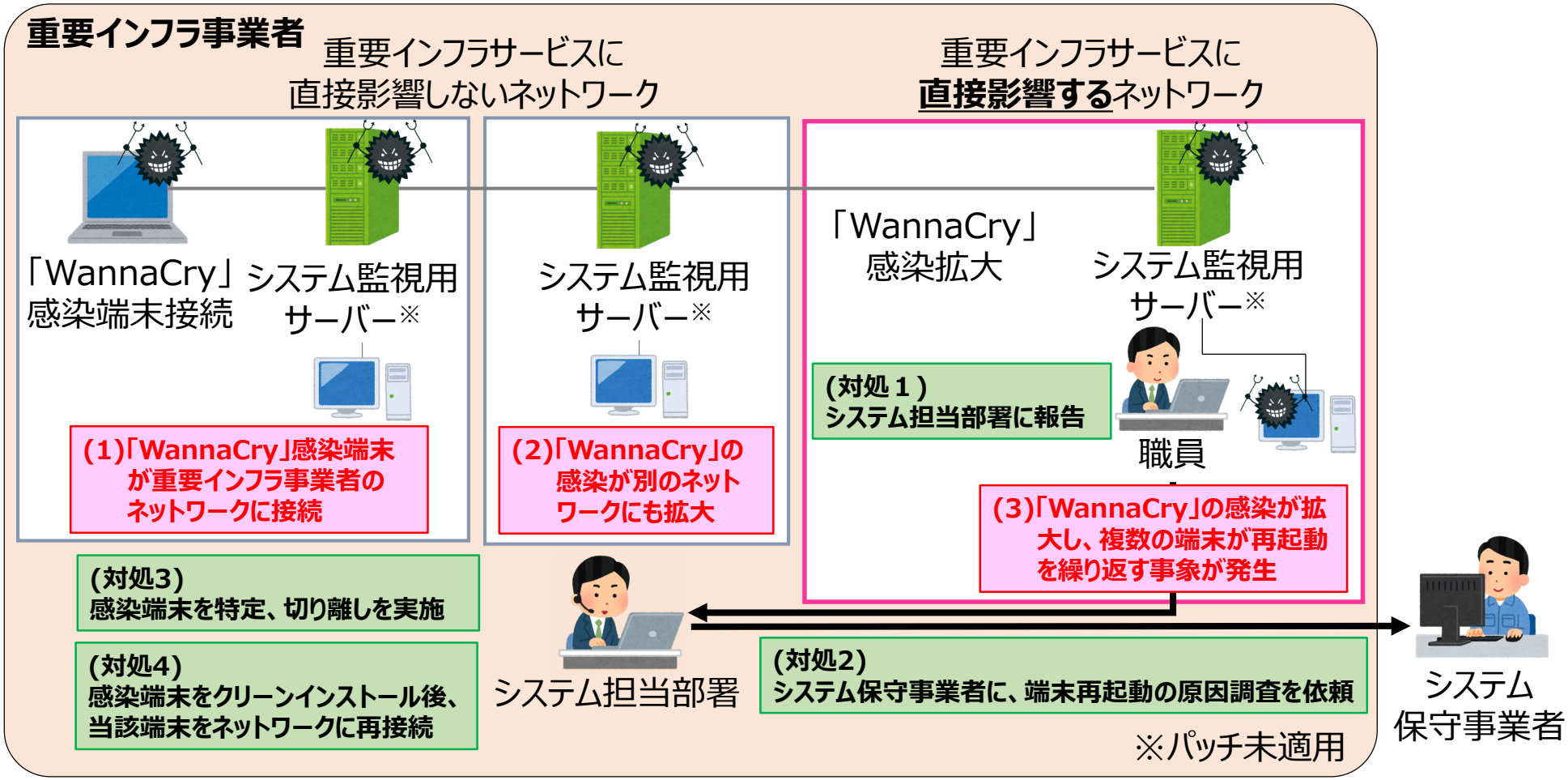
- ファイアウォールの設置、適切な通信制御の実施。
- リモートメンテナンスの廃止。
- 全ての端末・サーバーのID・パスワードを推測が困難なものに変更。

【6　得られた気付き・教訓】

- **インターネット公開サーバーに対する適切なアクセス制御**
  インターネット公開の必要性を適切に判断し、リモートメンテナンス等で必要な場合、必要最小限のポートのみの開放、アクセス元IPアドレスの制限等のアクセス制御を講じることが重要。
- **適切なパスワードの設定**
  パスワードは、十分な長さと複雑さを持たせた容易に推測されないものを設定し、パスワードの使い回しをしないことが重要。
- **端末やネットワーク機器等のログの迅速な保全**
  マルウエア感染端末やネットワーク機器のログの保全が遅れた場合、感染原因、感染拡大経路、被害状況を調査できないことが多いため、端末やログの迅速な保全が重要。ランサムウエアによる暗号化を考慮し、ログのバックアップの必要性も検討する。
- **バックアップデータの適切な取得**
  重要なデータは、バックアップを取得する。バックアップの検討に当たっては、ランサムウエア感染時でもバックアップが保護されるように留意する。また、バックアップで取得したデータをもとに、実際に復旧できるかを確認することも重要。

事例6　重要インフラ事業者における「WannaCry」の感染　1／2

- 重要インフラ事業者のネットワークに、マルウエア「WannaCry」に感染した端末が接続、各ネットワークに設置しているパッチ未適用のシステム監視用サーバーを経由して、「WannaCry」の感染が拡大
- 本事案においては、すべての端末において、「WannaCry」によるファイルの暗号化は発生しなかった
- 重要インフラ事業者のシステム担当部署の職員が、感染端末のイベントログや端末上に攻撃者が作成したファイルの特徴等から、本事象は「WannaCry」の感染によるものと判断、ネットワークからの切り離しを実施



事例6　重要インフラ事業者における「WannaCry」の感染　2／2

【1　背景】

- 2017年に登場したマルウエア「WannaCry」は、ファイル共有等で利用されるプロトコルSMBに関する脆弱性(MS17-010)を悪用し、感染を拡大する。
- 「WannaCry」には、感染端末上のファイルを暗号化するもの(ランサムウエア)と、暗号化を伴わないものが存在。

【2　検知】

- 重要インフラサービスに直接影響するネットワークで使用している複数の端末が、再起動を繰り返したことで、異常を把握。

【3　対処】

- システム保守事業者に端末再起動の原因調査を依頼。
- システム担当部署の職員が、端末のイベントログや端末上に攻撃者が作成したファイルの特徴等から、本事象は「WannaCry」の感染によるものと判断。
- 感染端末を特定し、ネットワークからの切り離しを実施。
- 感染端末は、クリーンインストール後にセキュリティアップデートを実施したうえでネットワークに再接続。

【4　原因】

- グローバルIPアドレスを割り当てた端末をインターネットに接続した際、適切な対策を講じていなかったことから、脆弱性を悪用され、「WannaCry」に感染。
- 「WannaCry」に感染した端末を、重要インフラ事業者のネットワークに接続、同ネットワーク内のパッチ未適用のシステム監視用サーバーを経由して、別のネットワークの端末に「WannaCry」の感染が拡大した。

【5　再発に備えた対策】

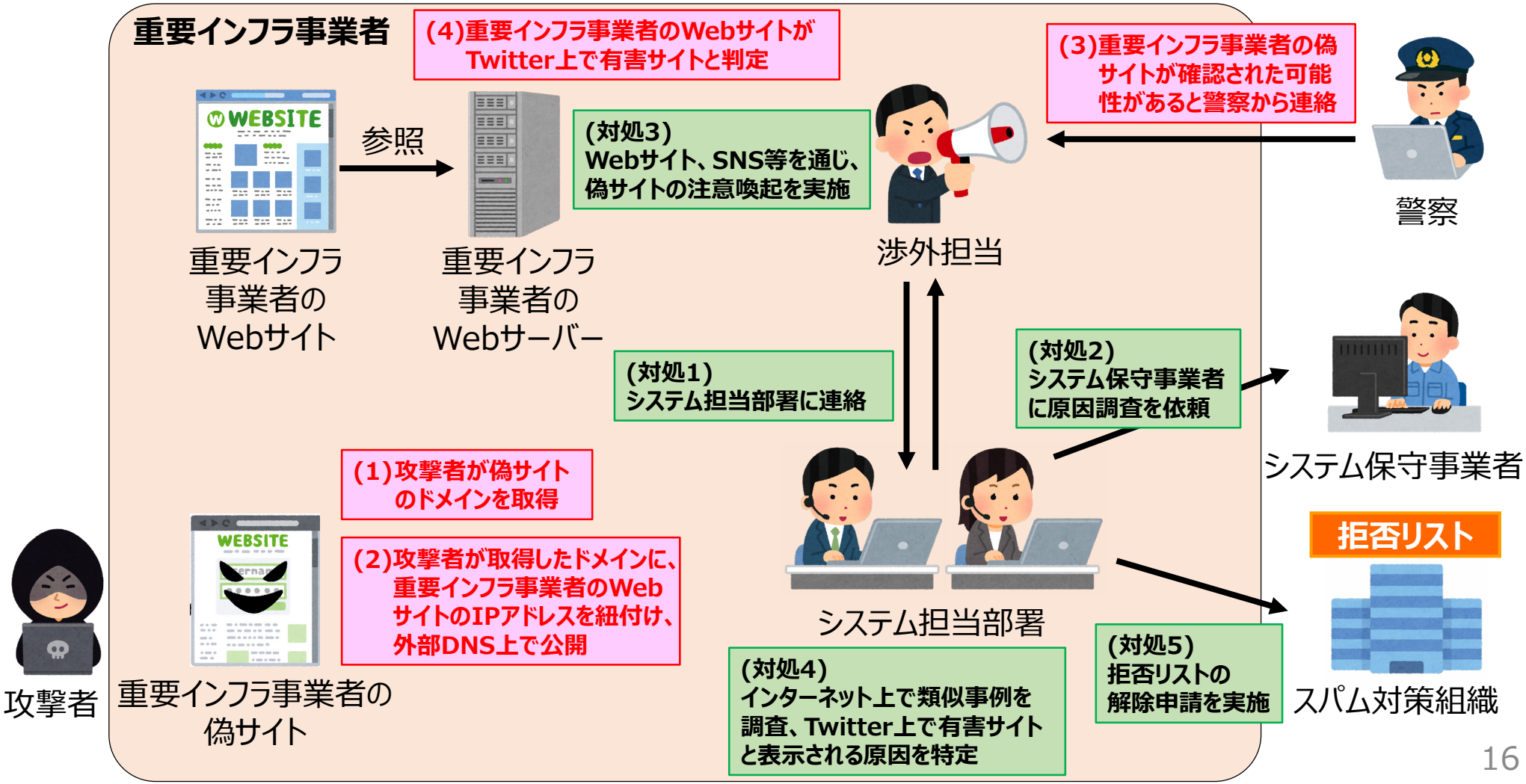
- 各ネットワークの境界点にファイアウォールを設置し、必要最小限の通信のみ通過させるように設定。
- 利用が終了した端末はクリーンインストールを必ず実施し、端末をネットワークに再接続する際には、ウイルス対策ソフトによるスキャンを必須とするように組織内のルールを変更。

【6　得られた気付き・教訓】

- **パッチ適用が困難な端末等に対する適切な管理策の検討**
  システムの制約上、迅速なセキュリティパッチ適用が困難な端末等について、不必要な通信の遮断、異常を早期に検知・対処できる仕組みの導入、定期的なバックアップの取得などの適切な管理策を検討し、対策を講じることが重要。
- **ネットワークに感染の恐れのある端末を接続する仕組みの検討**
  職場のネットワークに感染の恐れのある端末が接続されないようにするためには、検疫システムの導入を検討することが重要。システムの導入が難しい場合は、端末再利用時のルール(端末再利用時には、クリーンインストールやウイルス対策ソフトによるスキャンを必須化すること)を検討し、実施することが重要。
- **ネットワークの境界点における適切な通信制御**
  サイバー攻撃による侵害範囲の拡大を防ぐためには、ネットワークの境界点にファイアウォールを設置し、必要最小限の通信のみ通過させるように制御することが重要。
- **迅速に感染端末を特定する仕組みの検討**
  事案発生時に早期に影響範囲を特定し、対処するためには、EDR等の迅速に感染端末を特定する仕組みが重要。

事例7　重要インフラ事業者の偽サイトの確認　1／2

- 重要インフラ事業者のWebサイトをコピーしたサイトが確認された可能性がある旨、警察から連絡があり、調査したところ、偽サイトであることが判明したため、Webサイト、SNS等で利用者に注意喚起を実施。
- 後日、上記の件が影響し、重要インフラ事業者のWebサイトがスパム対策組織により有害サイトと判定されたことから、重要インフラ事業者は、同組織が管理する拒否リストの解除申請を実施。



事例7　重要インフラ事業者の偽サイトの確認　2／2

【1　背景】

- 本事案発生当時、国内外の事業者等のWebサイトをコピーした偽サイトが相次いで発見される事象が発生。

【2　検知】

【事象①：偽サイトが作成された事案】

- 重要インフラ事業者が、同事業者の偽サイトが確認された可能性があると警察から連絡を受け、事案が判明。

【事象②：Webサイトが有害サイトと判定された事案】

- 重要インフラ事業者の職員が、同事業者のTwitterを確認した際、ツイート内の同事業者のWebサイトへのリンクが有害サイトに判定されていたことで、事案が判明。

【3　対処】

【事象①：偽サイトが作成された事案】

- Webサイトの保守事業者に原因調査を依頼。
- 事業者のWebサイト、SNS等を通じて、偽サイトの確認に関する注意喚起を実施。

【事象②：Webサイトが有害サイトと判定された事案】

- 過去の他事業者の類似事案をインターネットで調査。
- スパム対策組織に対し、拒否リストの解除申請を実施。

【4　原因】

【事象①：偽サイトが作成された事案】

- 攻撃者が、自身で取得したドメインに、重要インフラ事業者のWebサイトのIPアドレスを紐付け、外部DNS上で公開したことにより、偽サイトが作成された。

【4　原因】

【事象②：Webサイトが有害サイトと判定された事案】

- 重要インフラ事業者のドメインが、スパム対策組織が管理する拒否リストに登録されたことで、そのリストを参照していると思われるTwitterが、同ドメインを有害サイトに判定した。

【5　再発に備えた対策】

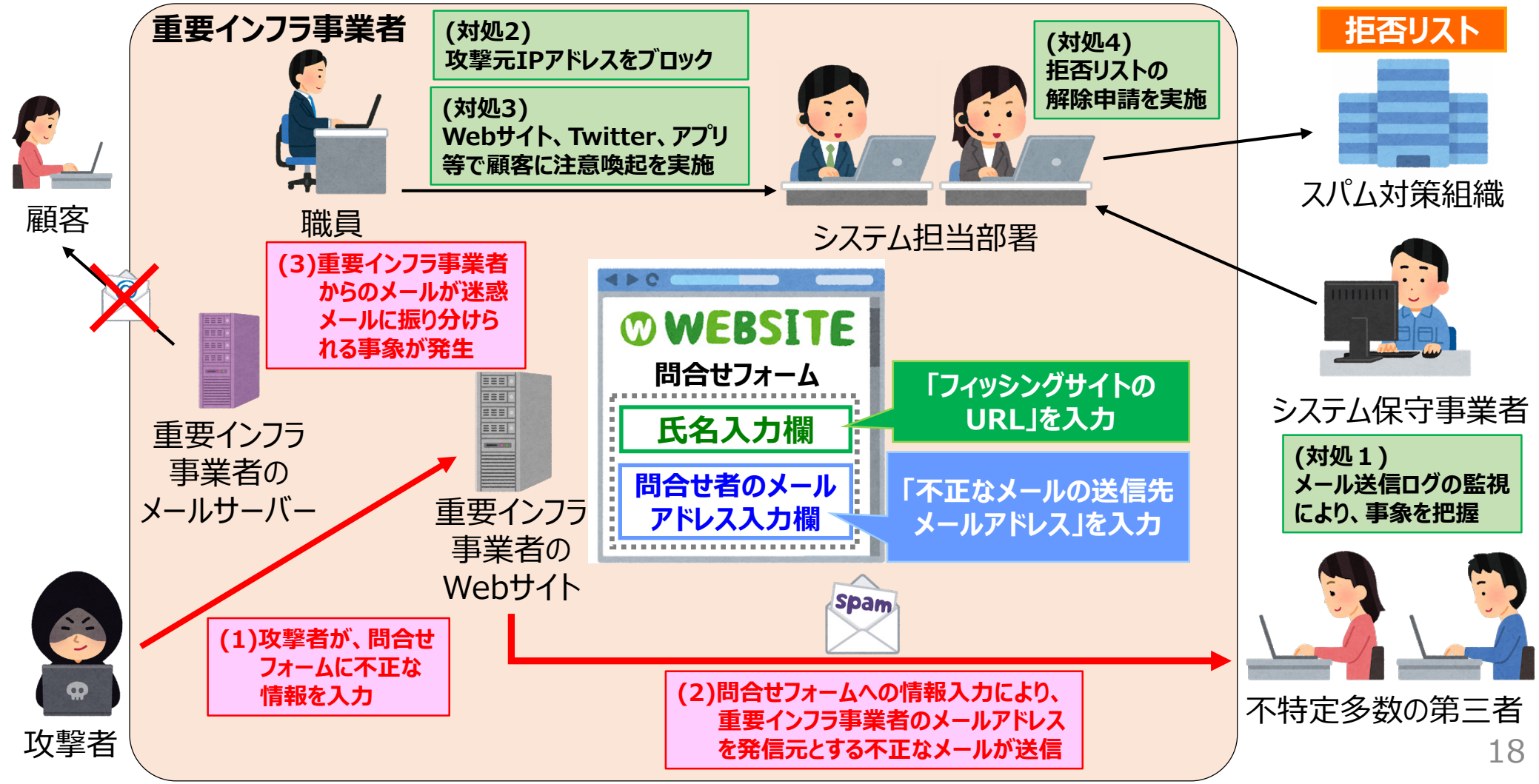
- 重要インフラ事業者の正規のURL以外からは、同事業者のWebサイトにアクセスできないように設定を実施した。

【6　得られた気付き・教訓】

- **サイバー攻撃事案にかかる情報の定期的な収集**
  サイバー攻撃にかかる対応では、過去の類似事案が参考になることも多いため、情報共有体制への参画等を含めた日頃から定期的に情報を収集・入手できる体制の確保が必要。
- **スパム対策組織の拒否リストの迅速な確認**
  自組織のWebサイトが有害サイトと判定された場合は、原因を特定、取り除いた後に、スパム対策組織の拒否リストに自組織のドメインが追加されていないか迅速に確認することが必要。
- **アクセス制御の適切な実施**
  自組織が管理するサーバー、ネットワーク機器等について、正規の経路以外からはアクセスできないようにする等、適切にアクセス制御を講ずることが必要。

事例8　問合せシステムを悪用した不正なメールの送信　1／2

- 重要インフラ事業者のWebサイトに設置していた問合せフォームが踏み台として利用され、同事業者のメールアドレスから、不特定多数の第三者に不正なメール(フィッシングメール)が送信された。
- 後日、同事業者のドメインがスパム対策組織の拒否リストに追加されたことを契機に、同事業者が送信したメールが迷惑メールに振り分けられ、重要インフラ事業者の顧客に正しく届かない事象が発生。



事例8　問合せシステムを悪用した不正なメールの送信　2／2

【1　背景】

- 重要インフラ事業者では、同事業者のWebサイト上に、顧客からの問合せを受け付ける問合せフォームを設置。
- 重要インフラ事業者では、システム監視の一環で、メール送信ログを監視していた。

【2　検知】

【事象①：不正なメールが多数送信された事象】

- メール送信ログの監視により、同事業者のメールアドレスから、大量のメールが送信される事象を検知。

【事象②：同事業者のメールが正しく届かない事象】

- 職員が作業中に、同事業者のドメインから送信したメールが、迷惑メールフォルダに振り分けられることを確認。

【3　対処】

【事象①：不正なメールが多数送信された事象】

- 攻撃元IPアドレスをブロックした。
- 事業者のWebサイト、Twitter、アプリ等を通じて、本事象に関する注意喚起を実施。

【事象②：同事業者のメールが正しく届かない事象】

- スパム対策組織に対し、拒否リストの解除申請を実施。

【4　原因】

【事象①：不正なメールが多数送信された事象】

- 攻撃者が、問合せフォームの氏名入力欄に「フィッシングサイトのURL」を、問合せ者のメールアドレス入力欄に「不正なメールの送信先メールアドレス」を入力したため、問合せ受付メール(不正なメール)が第三者に届いた。

【4　原因】

【事象②：同事業者のメールが正しく届かない事象】

- 重要インフラ事業者のドメインが、スパム対策組織が管理する拒否リストに登録されたことで、同事業者が外部に送信した一部のメールが正しく届かない等の事象が発生した。

【5　再発に備えた対策】

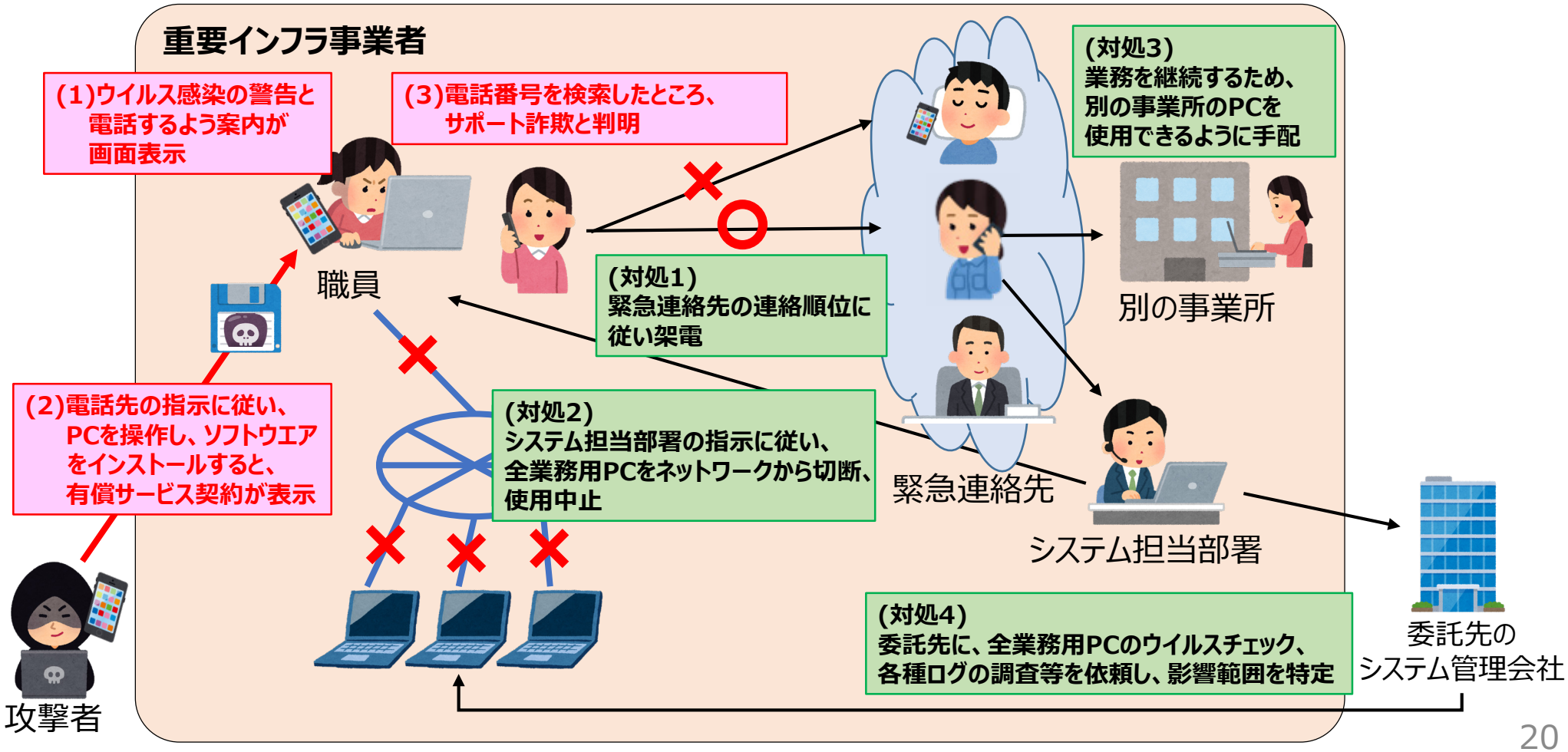
- 問合せフォームへの投稿が人間によるものか機械によるものかを判定する技術(CAPCHA)の導入。
- 連続投稿を防止する機能の追加等、一部プログラムを改修。

【6　得られた気付き・教訓】

- **平時におけるインシデント対処要員の育成**
  インシデント対処に関わる全要員に対して、CYDER等のサイバー防御演習の受講を義務付けていたことで、対処時における行動イメージが明確になり、当該事案でも各要員が迅速に情報を整理、関係者に対応状況を正確かつわかりやすく報告できた。
- **複数経路での情報発信**
  重要インフラ事業者が、複数経路(Webサイト、Twitter、アプリ等)で注意喚起情報を発信したことで、顧客に迅速に正確な情報を伝えることができ、大きな混乱も生じなかった。
- **スパム対策組織への迅速な拒否リスト解除申請**
  自組織のメール環境が悪用された場合、スパム対策組織の拒否リストに、自組織のドメインが追加される可能性があるという認識の下、先回りして拒否リストへの追加有無を確認することで、迅速に解除申請を実施でき、業務影響を抑えることが可能。

事例9　業務用PCにおけるサポート詐欺　1／2

- 被害組織の職員が、夜間、業務用PCでWeb閲覧した際、警告音が鳴り、ウイルス感染の警告と指定の電話番号へ連絡するよう案内が画面表示された。表示の電話番号へ連絡し、電話先の指示に従いPC操作を行うと、有償のサービス契約の情報が画面表示。
- 職員が不審に思い、同僚に相談、電話番号を検索したところ、サポート詐欺と判明。
- 再発防止として業務用PCを使う全職員に対し、最新の攻撃事例を交えたセキュリティ教育を定期的に実施。



事例9　業務用PCにおけるサポート詐欺　2／2

【1　背景】

- Web閲覧時、偽のセキュリティ警告を画面表示等し、電話をかけさせ、PC遠隔操作等のソフトウエアのインストールを促し、対応費用としてプリペイドカード等を搾取する事案(サポート詐欺)が相次ぎ発生している。
- 被害組織の職員が、夜間、業務用PCでWeb閲覧した際、ウイルス感染の警告画面が表示され、警告音が鳴り、指定の電話番号へ連絡するよう画面表示された。
- 指定の電話番号へ連絡し、電話先の指示に従いPC操作を行うと、有償サービス契約が画面表示された。

【2　検知】

- 職員が不審に思い、同僚に相談し、指定の電話番号を検索したところ、サポート詐欺であることが判明した。

【3　対処】

- 職員は緊急時の連絡体制の連絡順位に従い、緊急連絡先に架電し、その後、システム担当部署の指示に従い、職員らは該当PCを含む被害組織内の全業務用PCをネットワークから切断、同PCを使用中止にした。
- システム担当部署は、委託先のシステム管理会社に、全業務用PCについて、ウィルスチェック、各種ログ調査等を依頼し、影響範囲を特定した。
- 業務用PCが使用中止になり、職員らは業務影響を抑えるべく、代替手段として別の事業所のPCを使用した。

【4　原因】

- 職員がWeb閲覧の際、画面表示に従いサポート詐欺の電話番号に連絡した。

【5　再発に備えた対策】

- 業務用PCを使う全職員に対し、最新のサイバー攻撃事例を交えたセキュリティ教育を月1回程度、実施することとした。
- 夜間や休日でも緊急時に対応できるように、連絡体制を見直し、委託先のシステム管理会社を含む緊急時の連絡体制を再確認し、事業者内でも全職員に再周知した。

【6　得られた気付き・教訓】

- **全職員に対する最新事例を交えた定期的なセキュリティ教育**
  最新の事例を交えたセキュリティ教育を全職員に対し定期的に実施することで、職員のセキュリティ知識や意識を底上げしたうえで、サイバー攻撃被害の未然防止を図った。
- **緊急時の連絡体制の浸透**
  職員が緊急時の連絡体制を把握しており、速やかに連絡できたことで、夜間にも関わらず対応がスムーズに行えた。夜間や休日は連絡が取れないこと等を考慮し、委託先等も含めて、迅速な連絡体制を構築、浸透させておくことが重要。
- **ソフトウエアのインストール権限の最小化**
  サポート詐欺等のサイバー攻撃による被害の拡大を防ぐため、職員にソフトウエアのインストール権限を原則与えず、インストールする場合は業務上必要最小限のものをシステム担当者が確認、許可とすることが重要。
- **業務を継続するため迅速な代替手段の確保**
  インシデント対応等により業務用PCが使用中止となり、早急に代替手段を確保したことで、必要最低限のPC作業を実施でき、影響を抑えて業務を継続できた。業務継続の観点から、事前に代替手段を検討することが重要。