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

2021年度　重要インフラにおける補完調査について

2022年5月30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、平成30年7月25日・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、2021年1月1日～2021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	システムの不具合に伴う重要インフラサービスの停止	店舗端末に組み込まれたプログラムが誤動作し、各地の店舗端末が停止、重要インフラサービスの提供が停止した。各部門が連携し、迅速に利用者への周知や復旧方法の確認・実施をしたことで、大きな混乱なく事態を収拾した。
2	ソフトウエア障害に伴う重要インフラサービスの停止	基幹系システムでソフトウエア障害が発生し、重要インフラサービスの提供が停止した。迅速に情報連携を行い、サービスを提供しているすべての設備に職員を派遣し、対応することで顧客への影響を最小限に抑えた。
3	ハードウエア故障に伴う重要インフラサービスの一部制限	基盤システムでハードウエア故障が発生し、始業前の復旧が困難。サービス提供に一部制約がつくが迅速にバックアップシステムへの切替えを判断、バックアップシステムでの運用を組織内に周知し、重要インフラサービスの提供を継続した。
サプライチェーンに起因した重要インフラサービス障害		
4	外部委託先のランサムウエア被害	外部委託先がランサムウエアに感染し、重要インフラ事業者の情報が漏えいした可能性が発覚。システム部門、法務部門等、関係部門間で連携し、早期に情報公開を判断。迅速に対象者への連絡やWebサイトへの情報公開等を実施した。
5	子会社から親会社へネットワークを経由したマルウエア感染	子会社のサーバーがマルウエア感染、グループ間ネットワークを経由し、重要インフラ事業者のサーバーが感染。迅速に不審な通信や感染端末を特定し、隔離することで被害の拡大を防止し、重要インフラサービスの提供を継続できた。
6	VPNルーターの脆弱性を悪用したランサムウエア感染	委託先事業者が設置したVPNルーターの脆弱性を悪用され、侵入後、ランサムウエアにより暗号化された。対象端末の隔離等の対処、平行して代替サーバーの構築等を行い、一部制約があるが、重要インフラサービスの提供を継続できた。
7	外部Webサービスの仕様変更による情報漏えい	外部事業者が提供するWebサービスを利用していたが、Webサービス側のアクセス権限の仕様変更により、外部から意図しない情報へのアクセスが可能となっていた。第3者からの連絡を受け、即日サービスを停止し、同サービスを利用している他の重要インフラ事業者にも情報提供を実施した。

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	サプライチェーンに起因した 重要インフラサービス障害

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

- ✓ 障害発生に備え、IT部門だけでなく、組織全体の役割分担や連絡先を整備
- ✓ ランサムウエア感染時もバックアップデータが保護される仕組み作り

○外部委託先等を含めたサプライチェーン全体のセキュリティ確保が重要

- ✓ 脆弱性対応を含めた変更管理・IT資産管理の実施
- ✓ 関係者間でセキュリティリスクと対応内容を共有
- ✓ 外部サービス利用のリスクを認識し、障害時の代替策整備やセキュリティ診断を実施

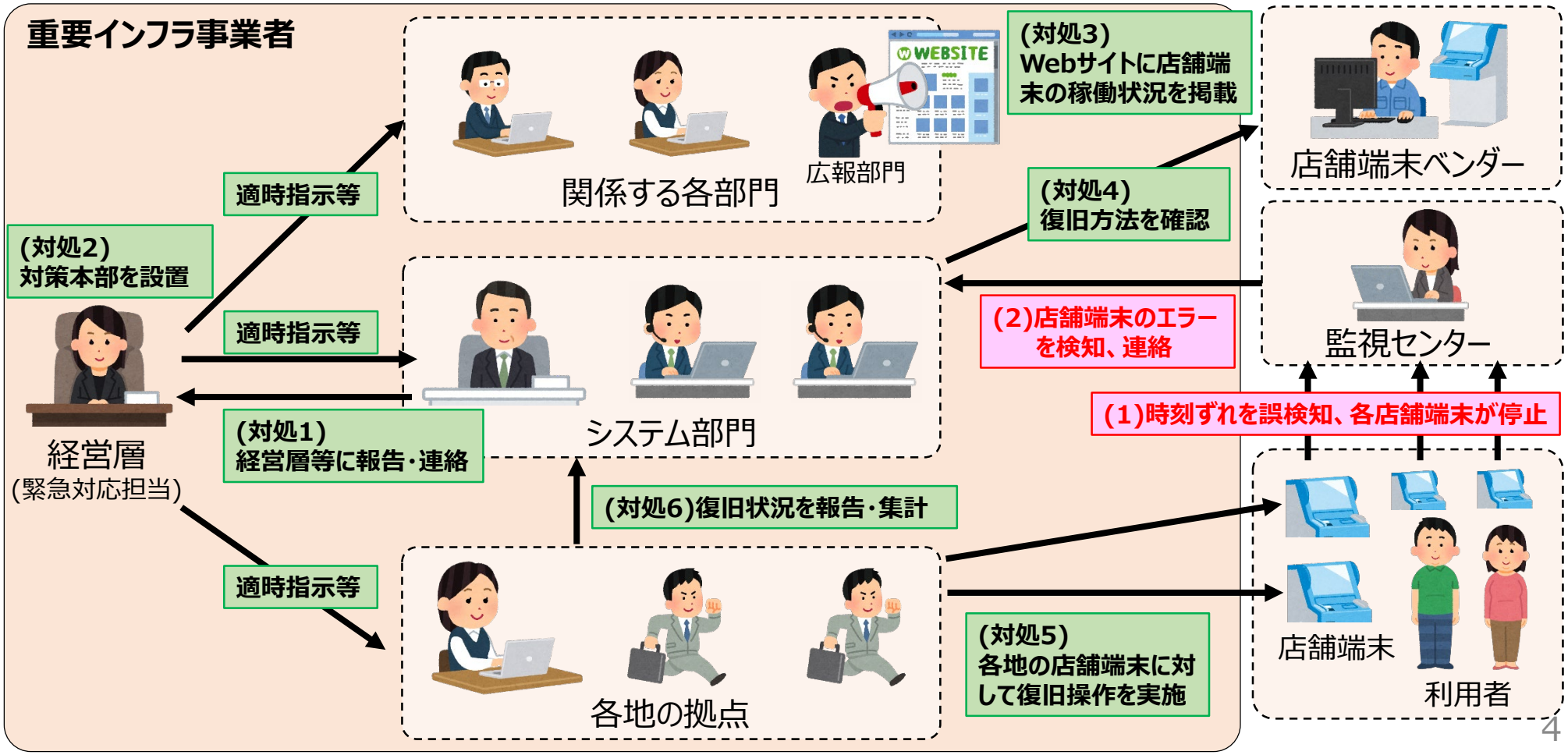
総括

いずれの良好事例に共通して、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、事前に策定した連絡体制に基づき、事案発生時に迅速に情報共有を行い、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。また、外部からの脅威に対して、脆弱性対応を含めたIT資産管理を行い、サプライチェーン全体でサイバーセキュリティを確保することが重要。

※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　システムの不具合による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、各地に点在する店舗端末で重要インフラサービスを提供していたが、各店舗端末に予防的に組み込んだプログラムが特定時刻で時刻ずれを誤検知したことにより、各地の店舗端末が停止し、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、迅速に利用者への周知や復旧方法の確認・実施をしたことで、大きな混乱なく事態を収拾。



事例1　システムの不具合による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、各地に拠点を持っており、各地に点在する店舗端末により重要インフラサービスを提供していた。
- 古い店舗端末で時刻ずれが発生したことから、時刻ずれを検知・補正するプログラムを予防的に各店舗端末に組み込んでいた。
- 利用者が店舗端末を使用中に店舗端末が停止し大きな混乱を招いた同業他社の事案を参考に、同プログラムは、利用者が店舗端末を使用中の場合、使用終了後に店舗端末を停止する仕様としていた。

【2　検知】

- 監視センターが各地の店舗端末からエラーが発せられたことを検知、重要インフラサービス事業者のシステム部門がその旨連絡を受けた。

【3　対処】

- システム部門は、緊急対応担当の経営層、各部門等に報告・連絡。経営層は対策本部を設置し、適時指示等を実施。
- Webサイトに店舗端末の稼働状況を掲載。
- システム部門は、エラーコードから復旧方法を推定。店舗端末ベンダーに確認。
- 対策本部は、各地の拠点に対して、各店舗端末に復旧操作を行うように指示。各拠点は各地に点在する店舗端末に対し、従業員を向かわせ、復旧操作を実施。

【4　原因】

- 予防的に組み込んだプログラムが特定時刻で時刻ずれを誤検知したことで、各地の店舗端末全てが停止した。

【5　再発に備えた対策】

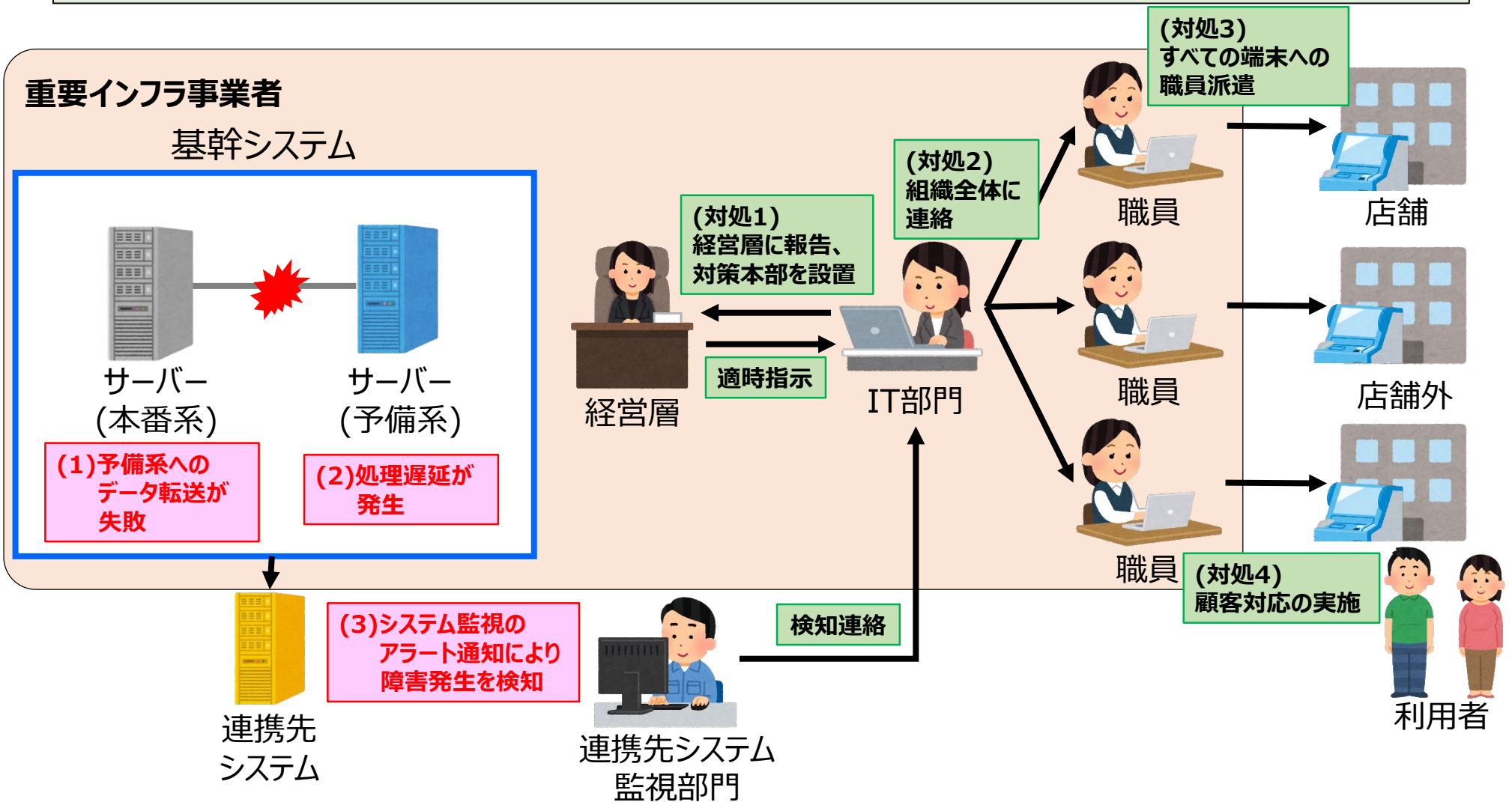
- 時刻ずれが発生する可能性のある古い店舗端末は、遠隔で復旧できるように改修。時刻ずれの心配のない店舗端末は、該当プログラムを停止。

【6　得られた気付き・教訓】

- **緊急時の対応の明確化**
  緊急時の対応として、災害時の対応と同じく、システム障害への対応を定めていたため、迅速に対応を行えた。各地に点在する端末への個別対応等、対応に人手が多く必要な場合は、人的リソースや移動時間等まで考慮した対応計画をあらかじめ定めておくことが重要。
- **緊急時の対応の訓練の重要性**
  緊急時の連絡体制を定めていたが、連絡体制上の該当者が出張や外出等で一時的に不在であったり、ツールを用いた緊急時の連絡で一部漏れや遅延が発生する等、定めた通りに動く難しさを実感。新型コロナウィルス対応等での要領更新時には尚更、考慮漏れをなくし、対応をスムーズに行うために、緊急時を想定した訓練が重要であることを再認識した。
- **同業他社の教訓の取り入れ**
  同業他社の事案を参考に、エラー発生時に利用者が店舗端末を使用中の場合、使用終了後に店舗端末を停止する仕様としていたため、大きな混乱なく事態を収拾できた。
- **適時適切な情報公開**
  障害発生時に、Webサイトだけでなく、現場にお知らせのポスターを掲示する等、適時適切な周知を行うことが重要。

事例2　ソフトウエア障害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、ソフトウエア障害により本番系から予備系へのデータ転送が失敗し、処理遅延が発生、重要インフラサービス（以下「サービス」という）が停止。
- 顧客保護のため、迅速に組織全体に情報共有を行い、すべての店舗端末及び店舗外端末に職員を派遣し、説明や代替策の案内を実施。



事例2　ソフトウエア障害に伴う重要インフラサービスの停止　2／2

【1　背景】

- 基幹系システム障害の対策マニュアルがあり、定期的に教育や訓練を行っていた。
- 顧客第一の考え方が組織内に浸透しており、規定にない事象が発生した場合も、すべての職員が顧客保護を最優先として動く意識を持っていた。

【2　検知】

- 連携先システムの監視アラートにより、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。
  ※経営トップは出張中だったため、WEB会議で参加
- 組織全体に周知を行い、顧客保護のためにサービスを提供しているすべての設備に職員を派遣。
- インターネット向けのサービスについてWebページに障害発生状況を公開。
- ベンダーと協力して原因を特定し、原因箇所の切り離しを実施し、復旧。
- 原因となったソフトウエア不具合を修正。

【4　原因】

- 本番系と予備系のデータ同期処理に不具合があり、処理量の上限を超えたことで、処理遅延が発生し、重要インフラサービスが停止。
- 数日前に発生した基幹系システムのハードウエア故障を起因として、関連したデータ同期処理のソフトウエア不具合が顕在化。

【5　再発に備えた対策】

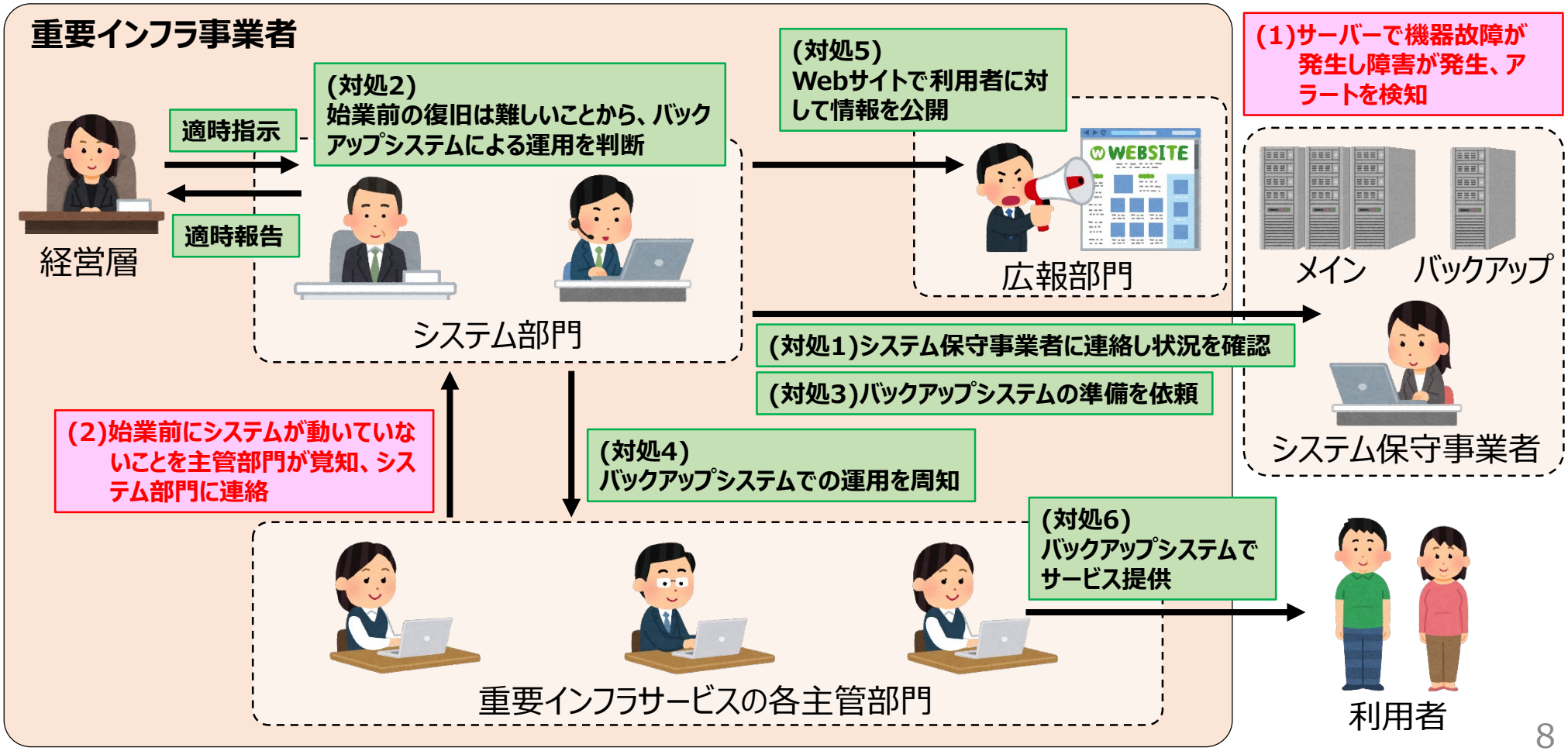
- 障害発生時の役割分担を再確認。
- 故障箇所を迅速に特定するため、システム基盤の全体構成や、各種機器の動作と故障時の影響を確認。
- 情報収集ツールの再整備と周知。
- 実際に発生する可能性の高いシナリオの訓練を実施。
- 遠方の店舗外端末にどこの職員を派遣するのか分担の見直し。

【6　得られた気付き・教訓】

- **障害発生時の対応の明確化**
  障害発生時の役割分担、対応内容、判断権者を明確にし、マニュアル化しておくことが重要であることを再認識。
- **顧客への影響を最小限にするための取り組みの強化**
  顧客への影響等の情報収集に時間を要したため、情報共有のツールや使い方の再整備が必要。
- **平時からの関係者間の連携強化**
  システム障害発生時にシステムベンダー含めて機動的に調査を行うことで、原因を特定することができた。自組織内外の関係者と定期的に情報交換を行う等、平時から連携を行うことにより、有事の際に迅速に連携することができた。

事例3　ハードウエア故障に伴う重要インフラサービスの一部制限　1／2

- 重要インフラ事業者が基幹システムに使用している仮想基盤のハードウエア故障により障害が発生、始業前に重要インフラサービス(以下「サービス」という)の提供に使用するアプリケーション(以下「システム」という)が動作していないことが発覚した。
- 重要インフラ事業者は、始業前の復旧が困難であることから、サービス提供に一部制約がつくが迅速にバックアップシステムへの切替えを判断、同運用を組織内に周知し、重要インフラサービスの提供を継続した。



事例3　ハードウエア故障に伴う重要インフラサービスの一部制限　2／2

【1　背景】

- 重要インフラ事業者は、基幹システムとして、仮想基盤上で動作するアプリケーションの提供を受け、各種の重要インフラサービスを各主管部門が提供していた。
- 仮想基盤の一部機器のハードウエア故障は、仮想基盤上で復旧できる想定だった。
- システムは、2系統(メインとバックアップ)用意しており、バックアップは、制約事項の下、サービスを提供できるものだった。

【2　検知】

- 始業前に、主管部門から、システムが起動していない旨、システム部門に連絡があり、本事象を認識した。
- システム部門からシステム保守事業者(以下「保守事業者」という)に連絡したところ、早朝にシステムエラーのアラートがあり、確認中と回答があった。

【3　対処】

- 始業前の復旧は難しいことから、バックアップシステムを使用しサービス提供を行うことを判断。
- 保守事業者へ準備の依頼、各主管部門へ周知、広報部門へ連絡しWebサイトで利用者に対して情報を公開。
- 始業時刻から、バックアップシステムでサービス(一部制約事項があり)を提供した。

【4　原因】

- 仮想基盤の一部機器のハードウエア故障により障害が発生、仮想基盤上での復旧が想定通りに発動しなかった。

【5　再発に備えた対策】

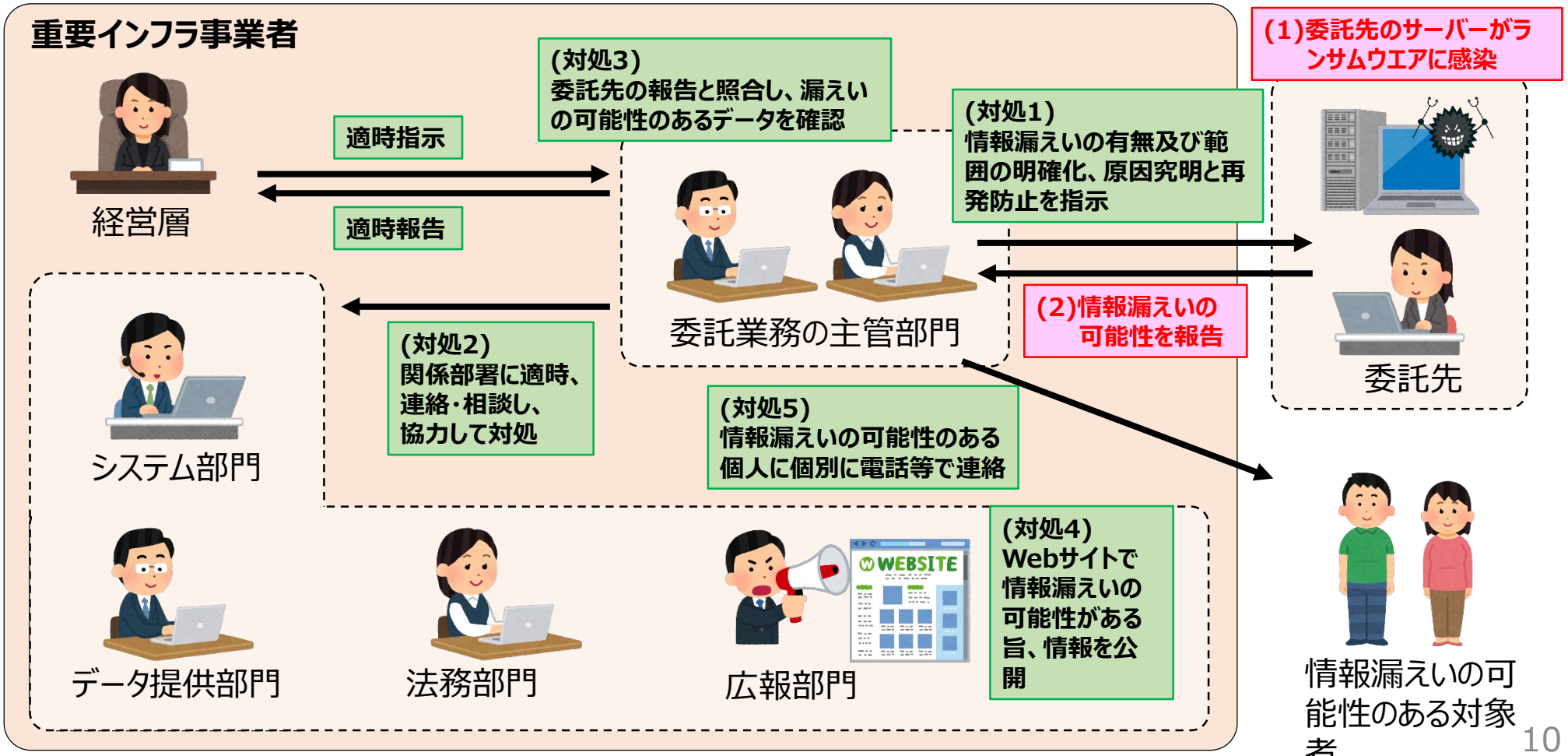
- 仮想基盤のハードウエア故障時に可用性を担保できるように、設定や復旧手順を検討、修正した。

【6　得られた気付き・教訓】

- **バックアップシステム利用の適切な判断**
  適切なタイミングにおけるバックアップシステムの使用判断等、障害発生時の対応を迅速に進めるため、障害発生時の切り替え・切り戻し等の判断タイミング、判断権者を含めて明確化しておくことが重要。
- **緊急時の連絡体制の再確認**
  多数の部門が使用するシステムであり、障害時にはサービスの継続に大きな影響を及ぼすことが想定されるため、システムを利用するサービスの一覧、各部門への連絡先、経営層や広報担当等の緊急連絡先を事前に把握、定期的に更新を行い、インシデント発生時に迅速に対応できるようにすることが重要。また、エラー検知時等の連絡について、保守事業者と事前に取り決めをしておくことが重要。
- **バックアップシステムの利用の周知**
  障害時のバックアップシステムの利用について、組織内に周知済みであったが、職員の異動等も発生するため、定期的に周知、訓練しておくことが重要であると再認識。
- **想定通りの稼働確保の重要性**
  冗長化したシステムについて、想定通りに動作をするか事前に確認しておくことが重要。

事例4　外部委託先のランサムウエア被害　1／2

- 重要インフラ事業者は、業務を外部の事業者に委託、個人情報を含むデータを提供していたが、委託先のサーバーがランサムウエアに感染、情報漏えいの可能性が発覚した。
- 重要インフラ事業者は、委託業務の主管部門やシステム部門、法務部門等、関係部門間で連携し、早期に情報公開を判断。Webサイトで情報公開、情報漏えいの可能性のある対象者に個別に電話するなど、対応を迅速に実施した。



事例4　外部委託先のランサムウエア被害　2／2

【1　背景】

- 重要インフラ事業者は、一部業務を外部の事業者に委託しており、個人情報を含むデータを提供していた。
- 重要インフラ事業者で公表が遅かった過去事例があった。

【2　検知】

- 委託先が、自社のサーバーがランサムウエアに感染したことを公表し、情報漏えいの可能性があることを重要インフラ事業者に報告した。

【3　対処】

- 委託業務の主管部門からシステム部門や法務部門等、関係する各部門に連絡、相談。
- 委託先に情報漏えいの有無及び範囲の明確化、原因究明と再発防止を指示。
- 委託先に提供していたデータを再確認、委託先の報告と照合し、個人情報を含むデータの漏えいの可能性を確認。
- 公表が遅かった過去事例を踏まえ、早期に情報公開を判断。情報漏えいの可能性がある旨を Webサイトで公表。情報漏えいの可能性のある対象者に個別に電話等で連絡。

【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エアに感染した。

【5　再発に備えた対策】

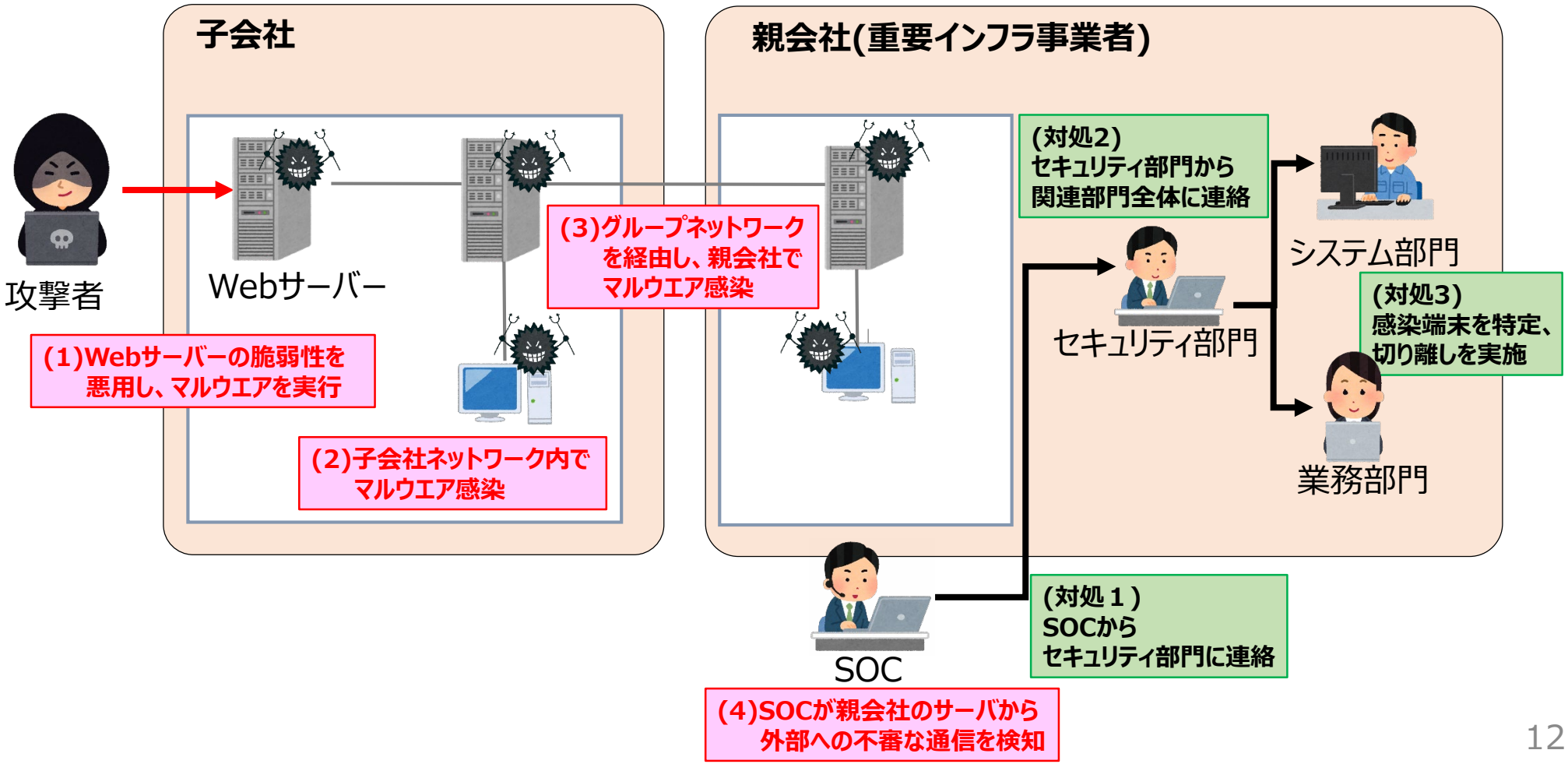
- 委託先の情報セキュリティに関するレベルを担保するため、委託先の選定時や契約時に使用するセキュリティに係る仕様書例を作成し、業務を委託する際に使用するようにした。

【6　得られた気付き・教訓】

- **委託先の管理の重要性の再認識**
  重要インフラ事業者の内部からの情報漏えいだけでなく、外部の委託先からの情報漏えいが、重要インフラ事業者の責任となることを再認識した。委託先のセキュリティはコントロールできない範囲が大きいため、情報漏えい等が発生しないように、契約等により委託先のセキュリティを担保することが重要。
- **委託先へ提供するデータの適正な管理**
  委託先に対し、必要最小限の情報のみを渡すようにし、委託業務に不要な個人情報等を渡さないようにすることが重要。また提供したデータを一覧化するなどして管理し、性質等を把握しておくことで、緊急時の対応を適切・迅速に行える。
- **関係各部門間の連携と迅速な対応**
  各部門の専門性を活かした役割分担で、関係部門間で連携しつつ対応に当たることで、公表が遅かった過去事例の反省を活かし早期に情報公開を行うなど、迅速に適切な対応が実施できた。
- **バックアップの重要性**
  委託先がデータをバックアップしていたため、ランサムウエアによるデータ暗号化の業務への影響はなかった。

事例5　子会社から親会社へネットワークを経由したマルウエア感染　1／2

- 子会社のサーバーがマルウエア感染、グループ間ネットワークを経由し、重要インフラ事業者のサーバーが感染。
- 重要インフラ事業者のネットワークを監視していたSOCが感染を検知し、感染元を調査したところ子会社のサーバーを起点にして侵入されていたことが判明。
- 攻撃者のサーバーとの通信や不審な挙動を特定し、感染端末を隔離することで、重要インフラサービスを継続できた。



事例5　子会社から親会社へネットワークを経由したマルウエア感染　2／2

【1　背景】

- 親会社(重要インフラ事業者)は複数のグループ会社を保有しており、グループ間でネットワーク接続していた。

【2　検知】

- 親会社のネットワークから不審なサーバー宛ての通信をSOCが検知した。

【3　対処】

- 親会社のネットワークから不審なサーバー宛ての通信を遮断。
- IT部門と連携し、ネットワークの通信ログや端末のイベントログ等から感染源を辿り、子会社の端末から親会社のネットワークに侵害したことを特定。
- 子会社と連携し感染源を調査したところ、最初に攻撃を受けたWebサーバーを特定。
- 親会社と子会社の感染端末を特定し、ネットワークから隔離。
- 感染端末のフォレンジックを実施。
- 全ユーザのパスワード変更、不審ファイルの有無等を全台調査。

【4　原因】

- 子会社の社外向けWebサーバについて、システム稼働を優先し、セキュリティパッチが未適用だった。
- システム管理用の特権アカウントに平易なID／パスワードが設定されており、Webサーバ侵害後に同ネットワーク内の端末を経由して、親会社のネットワークまで感染拡大した。

【5　再発に備えた対策】

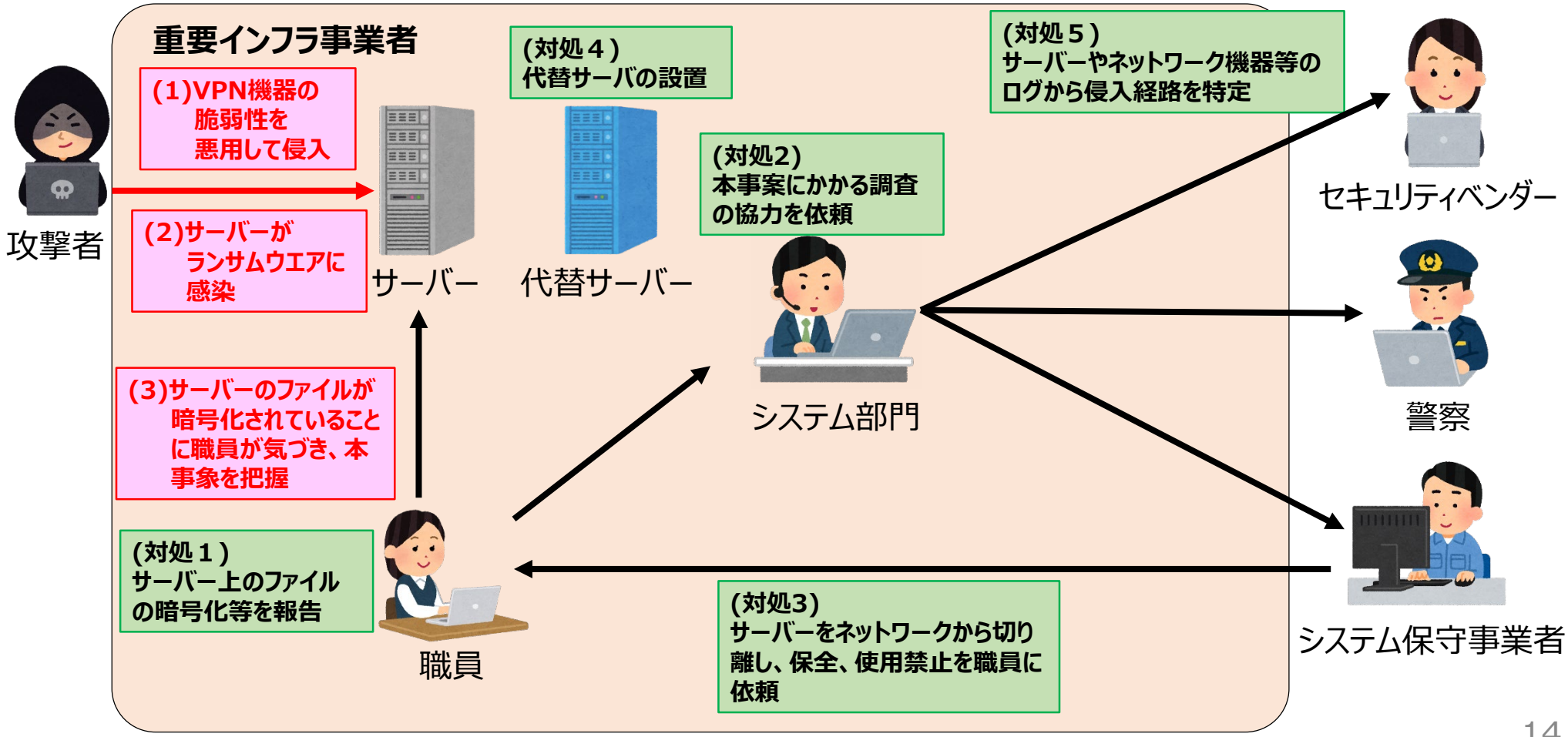
- 特権アカウントの管理システム導入。
- 通信を監視し、不正検知する新たな仕組みの検討。
- 新たな攻撃に備えて訓練等によるセキュリティ意識の向上。

【6　得られた気付き・教訓】

- **業務委託先やグループ会社含めたIT資産管理の徹底**
  自組織だけではなく、業務委託先やグループ会社含めてIT資産管理を徹底し、最新のパッチ適用等を適切に運用できているか確認することが重要。
- **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、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。
- **社内での不正な通信を検知する仕組みの強化**
  親会社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、グループ内の通信については防御・検知が不十分だったため、SOCが検知するまでに多数の端末に感染した。外部からの侵入だけではなく、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。
- **迅速に組織間で連携し、感染端末を隔離**
  事案発生時はグループ会社や業務部門含めて関係組織間で迅速に連携することで、感染端末を特定し、隔離する動きが出来た。

事例6　VPNルーターの脆弱性を悪用したランサムウエア感染　1／2

- 重要インフラ事業者の職員が、サーバー上の業務データが暗号化されていることを認識。
- 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、代替サーバーを設置し、重要インフラサービスを継続した。
- 侵入されたVPNルーターは、重要インフラ職員向けの外部接続サービスを提供するために委託先業者が設置した機器であり、重要インフラ事業者は管理していなかった。



事例6　VPNルーターの脆弱性を悪用した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、緊急時に外部から接続するためのシステムを導入していた。
- 当該システム導入時にVPNルーターが設置されたが、重要インフラ事業者は機器を認識しておらず、管理はシステム保守事業者が行っていた。

【2　検知】

- 重要インフラ事業者の職員が、サーバー上のファイルの暗号化に気づき、事象を把握し、システム保守事業者に連絡した。

【3　対処】

- 事象からウイルスによるものと判断し、サーバーをネットワークから隔離。
- ネットワーク内のすべての端末のウイルスチェックを実施。
- サーバーを使用しない運用方法を検討し、業務を継続。
- システム保守事業者、セキュリティベンダーや警察に連絡し、当該事案の調査にかかる協力を依頼。
- 翌日、代替サーバーを設置し、環境を再構築。
- 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。

【4　原因】

- VPNルーターについてファームウエアが更新されておらず、脆弱性がある状態のまま使用していたため、当該脆弱性を悪用され、外部から不正アクセスされた。
- バックアップを同一サーバー内に保存していたため、ランサムウエア感染時にバックアップデータも暗号化された。

【5　再発に備えた対策】

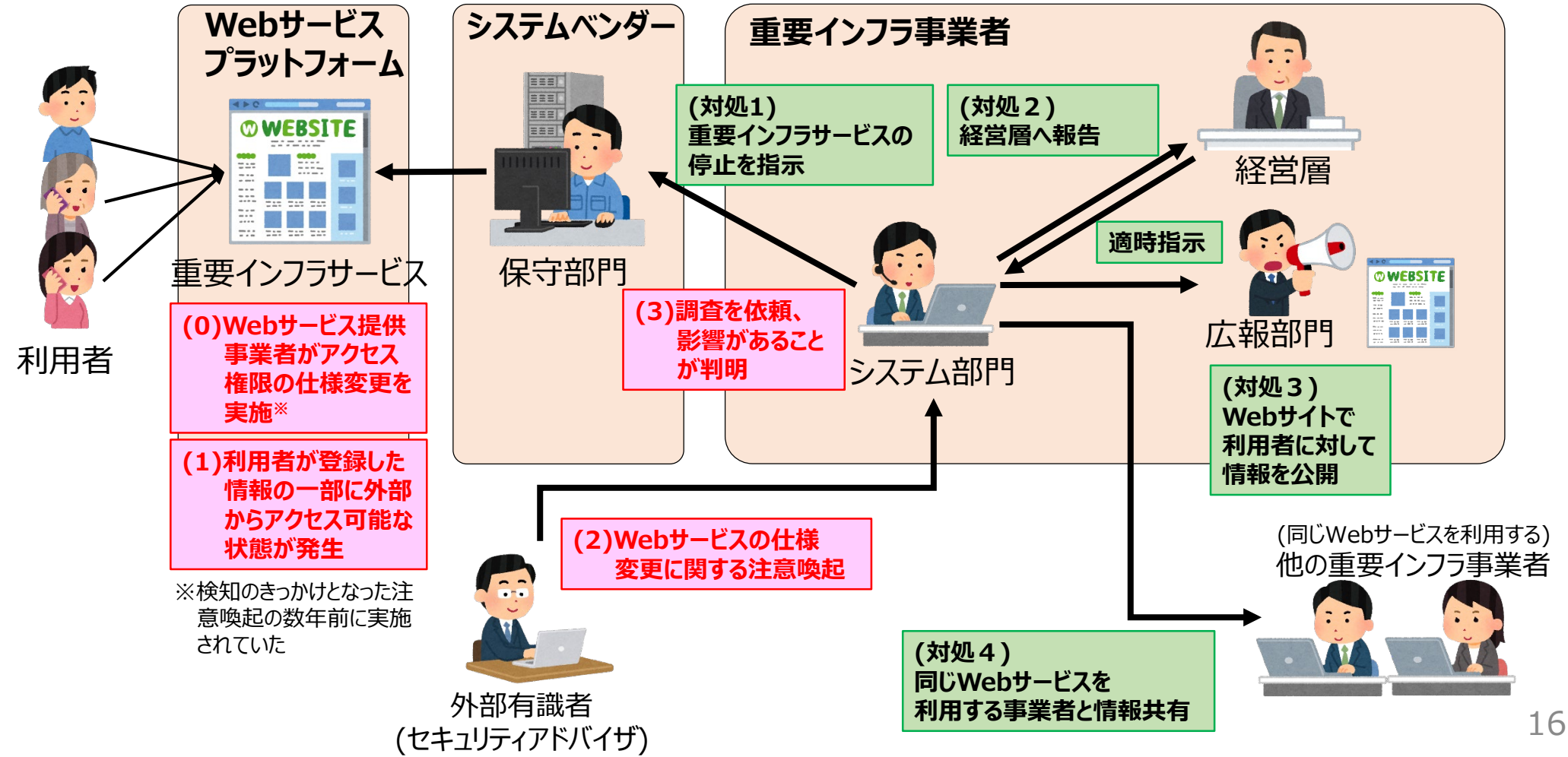
- すべてのルーターのファームウエアを確認し、更新や機器を買い換え。
- システム保守事業者と新規契約する際に、保守作業としてセキュリティパッチ適用等のアップデートを含めるように変更。
- 緊急時の連絡先の整理。
- ランサムウエア感染時もバックアップデータが保護されるように、バックアップの管理方法を改善。

【6　得られた気付き・教訓】

- **構成図等の定期的なメンテナンス**
  機器導入時のまま更新されていない資料や、システム保守事業者ごとに様式が異なる資料が混在していたため、構成図等を定期的にメンテナンスし、機器やソフトウエアのバージョンを管理することが重要。
- **脆弱性情報の収集と評価**
  使用しているソフトウエアや機器に脆弱性が無いか確認し、内容に応じてセキュリティパッチや緩和策の適用等を行うことが重要。
- **緊急時の連絡先の把握**
  サイバー攻撃を受けた際に迅速に対応するため、セキュリティベンダーや所管省庁等の連絡先をあらかじめ把握しておくことが重要。
- **バックアップデータの適切な管理**
  ランサムウエア感染時でもバックアップデータが保護されるように、ネットワークから分離した環境で保存する。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7　外部Webサービスの仕様変更による情報漏えい　1／2

- 重要インフラ事業者は、他事業者が提供するWebサービス(以下「Webサービス」という)のプラットフォーム上で重要インフラサービスを提供していた。
- 外部有識者(セキュリティアドバイザ)からWebサービスの仕様変更に関する注意喚起があり、ベンダーに調査を依頼したところ、情報の一部に外部からアクセス可能であることが判明したため、重要インフラサービスを停止。
- 利用者に対して情報提供を実施、同じWebサービスを利用する他の重要インフラ事業者と情報共有を実施。



事例7　外部Webサービスの仕様変更による情報漏えい　2／2

【1　背景】

- 重要インフラ事業者は、顧客から予約を受け付ける重要インフラサービスの開発をシステムベンダーに依頼。
- システムベンダーは他事業者が提供する外部Webサービス(以下「Webサービス」という)上にシステムを開発。

【2　検知】

- 外部有識者(セキュリティアドバイザ)からWebサービスの仕様変更に関する注意喚起を受領。
- システムベンダーに調査を依頼し、利用者が登録した情報の一部に外部からアクセス可能であることが判明。

【3　対処】

- 同日中に重要インフラサービスを停止。
- 電話やFAX等の代替手段による重要インフラサービスを再開。
- セキュリティベンダー等と連携し、外部からアクセスされた可能性のある情報の調査を実施。
- 重要インフラ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。
- ベンダー経由で同じWebサービスを提供する他の重要インフラ事業者に情報共有。

【4　原因】

- Webサービス提供事業者がWebサービスのアクセス権限の仕様を変更したため、情報の一部に外部からアクセス可能となった。
- 重要インフラ事業者はシステムベンダーに問い合わせるまでWebサービスのセキュリティ設定の認識を過誤していたため、検知に時間がかかった。

【5　再発に備えた対策】

- Webサービスのアクセス権限を見直し、外部から情報を参照出来ないように修正。
- 調査の際にログの取得に時間を要したため、円滑に情報取得できるよう手続きを整備。

【6　得られた気付き・教訓】

- **サプライチェーンを含めたIT資産管理の重要性**
  重要インフラ事業者はシステムベンダーに開発を委託しており、Webサービスのセキュリティ設定の認識を過誤していたため、検知するまで時間がかかった。自組織だけではなく、業務委託先を含めて変更管理やIT資産管理を実施し、仕様変更等による影響を確認することが重要。
- **関係者間でのセキュリティリスクの共有**
  外部サービスを利用することによるセキュリティリスクと対応内容について、ベンダと共有することが重要。
- **情報取得手続きの確認**
  外部サービスはログの取得に制限がある場合や、手続きに時間を要する場合があるため、調査のために必要な手続きを事前に把握することが重要。
- **外部有識者の活用**
  サイバーセキュリティを確保するために、セキュリティアドバイザといった外部有識者を活用することが有用であることを本件で認識。