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３

2016年度　重要インフラにおける補完調査について

２０１７年3月１６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

補完調査の目的

補完調査とは、行動計画※の枠組みの評価に当たって、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とら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3次行動計画（平成27年5月25日サイバーセキュリティ戦略本部改訂）

調査の運営

補完調査として、IT障害等の事例についての現地調査（ヒアリング等）を行い、調査結果については、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、事例の概要・原因とともに得られた気付き・教訓等をとりまとめ、公表するものです。

調査対象

調査対象は、実際に発生したＩＴ障害等について、類似事例の発生状況（可能性）や社会的影響（関心）の大きさ、及び得られる気付き・教訓の有用性等を考慮して以下の事例を選定しました。

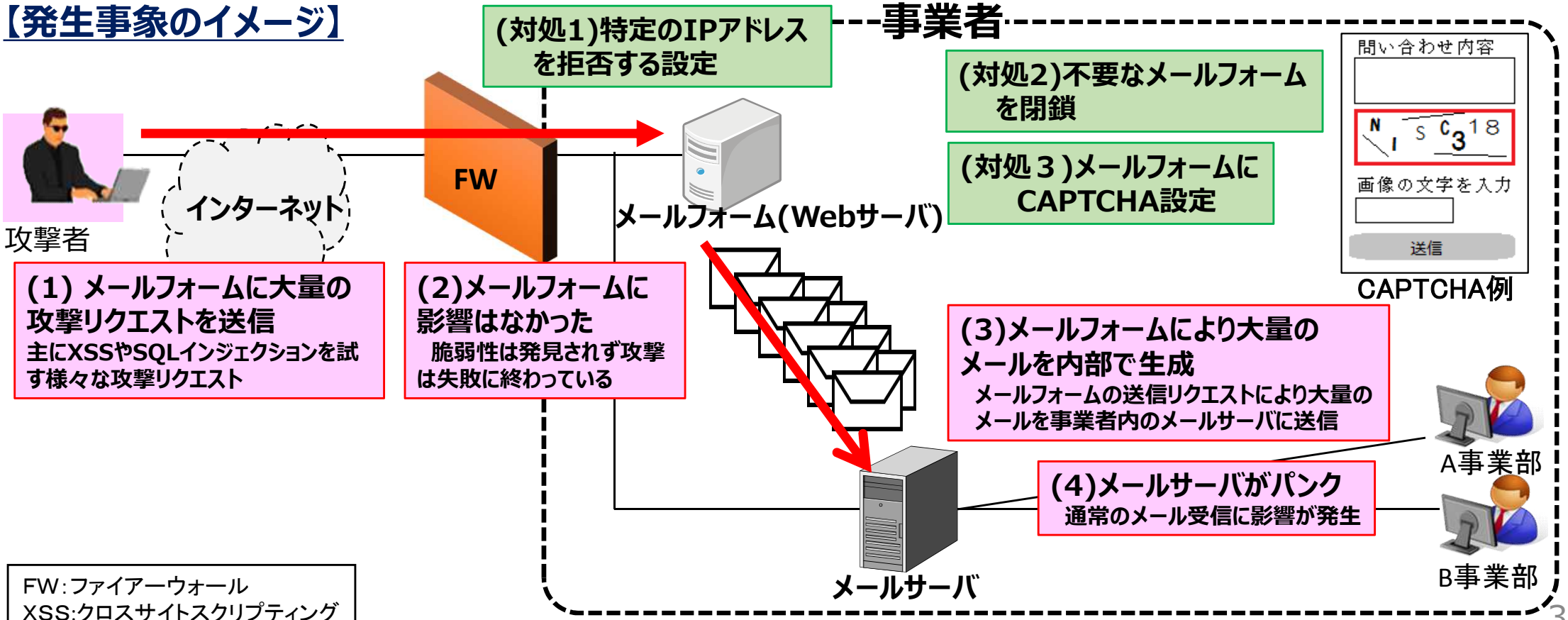
事例１　メールフォームへの攻撃
事例２　アクセス制限の不備
事例３　ランサムウェア被害
事例４　管理サーバへの不正アクセス
事例５　ソフトウェアの継続的なセキュリティ対策
事例６　システムの不具合によるサービス障害

事例１　メールフォームへの攻撃　　１／３

【事例の概要】

- Webサイトに設置した複数のメールフォームに、脆弱性を狙った大量のリクエストがあった。
- メールフォームに脆弱性はなく、メールフォームやWebサイトに影響はなかった。
- メールフォームから大量のメールが事業者内に送信され、事業者内のメールが約1日受信できない状態になった。
- メールを利用した一部の業務について、手順を変更して実施した。

【発生事象のイメージ】



FW：ファイアーウォール
XSS:クロスサイトスクリプティング

事例１　メールフォームへの攻撃　　２／３

【１　背景】

- アンケートや各種イベントの申込受付のために、Webサイトに20か所程度メールフォームを設置していた。
- メールフォームに入力されたメッセージは、事業者内の特定のメールアドレス宛に送信される仕組みだった。
- メールフォームは定期的にメンテナンスされており、未対応の脆弱性などはなかった。

【２　検知】

- 他事業部の担当者からシステム担当者へメールが届いていないとの連絡があった。

【３　対処】

- 攻撃元IPアドレスを特定し、該当IPアドレスからの接続を拒否した。
- 現在使用されていないメールフォームを閉鎖した。
- メールフォームにCAPTCHAを設定した。

【４　原因】

- 攻撃者が、複数のメールフォームに対してWebサイトの脆弱性を探る多数の攻撃リクエストを送信したため。

※WebサイトにXSSやSQLインジェクションなどの脆弱性はなく、攻撃者の意図は失敗に終わったと思われる。

【５　再発防止策】

＜システム面＞

- 特定の送信元IPアドレスをFWで接続拒否する設定を追加。
- 特定の送信元IPアドレスをメールフォームのプログラムで拒否する設定を追加。
- すべてのメールフォームにCAPTCHAを設定し、自動化された大量アクセスへの対策を実施。

＜運用面＞

- 大量アクセスがあった場合に、送信元IPアドレスを特定する方法の共有。
- 特定の送信元IPアドレスを拒否する設定方法の共有。
- 利用していないメールフォームの閉鎖。

※今回は単一IPアドレスからの大量アクセスだったが、今後、不特定多数のIPアドレスからアクセスされた場合の対応体制については。継続して検討を進めている。

事例１　メールフォームへの攻撃　　３／３

【６　得られた気付き・教訓】

- **メールフォーム運用時に考慮する点**

① 大量のメールが生成・送信される可能性がある。

WEBサイトの負荷以外にも、送信先のメールサーバの負荷も考慮に入れる必要がある。

② CAPTCHAを利用することにより、自動化された大量のリクエストを軽減できる。

大量のリクエストは自動化されたものが多いため、CAPTCHAを利用することにより軽減を図ることができる。ただし、解析技術の進歩などにより、CAPTCHAの有効性については定期的な見直しが必要。

③ 使用していないメールフォームは閉鎖する。

入力フォームがあるページは攻撃の対象になりやすい。

④ 定期的な脆弱性チェック・ソフトウェアのアップデート対応が必要。

今回の攻撃は、主にXSSやSQLインジェクションを狙った内容であったため、日常的な情報収集・対応がなければ、業務への深刻な影響が出た可能性がある。

⑤ メールフォームから送信されるメールは、メールサーバからも社外発信できない設定にする。

メールフォームに未知の脆弱性があったとしても、外部へメール送信の踏み台として利用されるリスクを減らせるため、多層防御の観点から有効な設計であった。

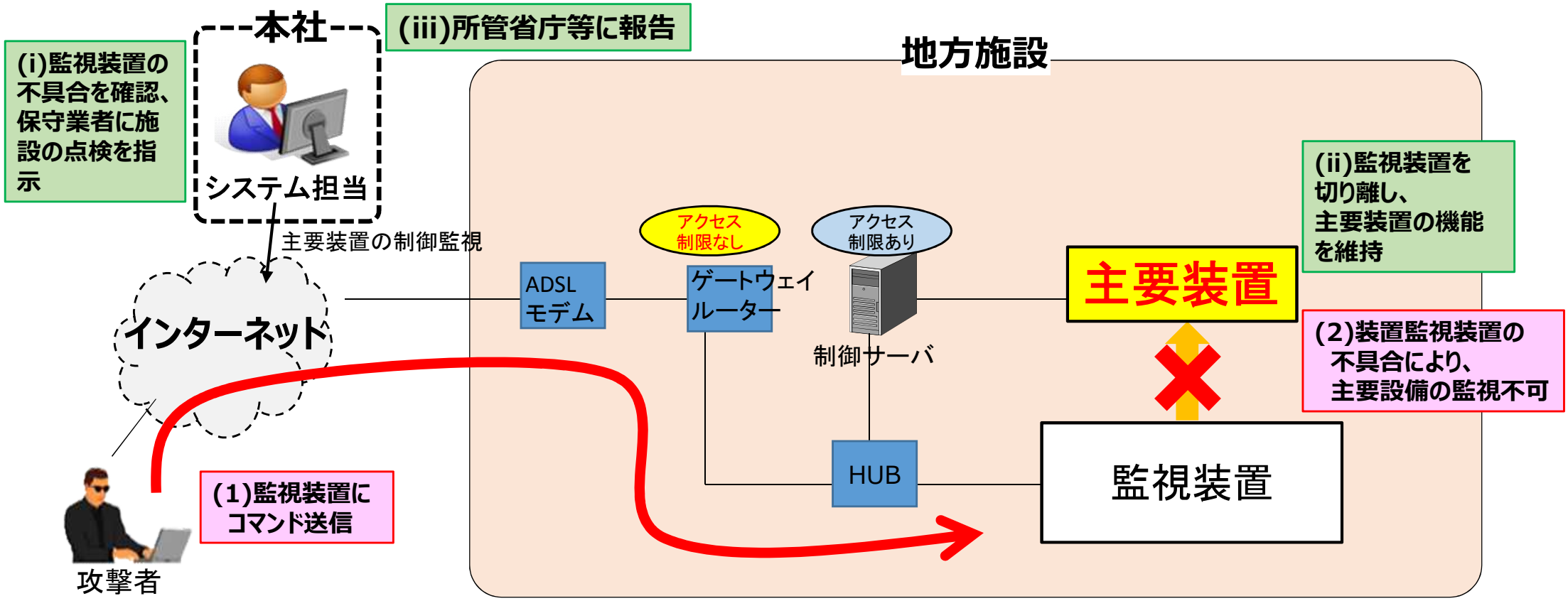
⑥ 必要に応じて、迷惑メール対策を実施する。

意図に反した内容も送られてくるため、頻繁に送られてくるようなら対応が必要になる場合もある。

事例２　アクセス制限の不備　　１／２

【事例の概要】

- 主要装置へのアクセス制限には対応していたものの、監視装置へのアクセス制限に不備があった。
- 監視装置への不正アクセスにより、機能が停止された。なお、主要装置の基本的な動作には影響はなく、重要インフラサービス自体への影響はなかった。
- 監視装置を切り離し、主要装置の機能を維持した。



事例２　アクセス制限の不備　　２／２

【１　背景】

- インターネットを経由して、アクセス制限をしていないゲートウェイルータを介して、監視装置をつないでいた。
- 地方施設のシステムの保守・点検については、保守ベンダーに委託していた。

【２　検知】

- 本社では、毎日定時に監視装置の管理画面にアクセスし、機器が正常に動作しているか確認していたが、その日は監視ができなかった。また同日、システムの保守ベンダーから、当該施設で使用していたものと同型の機器で構成されている他の施設で、監視装置に不具合が発生しているとの連絡があり、発覚した。

【３　対処】

- 現地でサービス提供が維持できているかを現地業者に確認。
- 保守ベンダーに施設の対応を依頼。
- 監視装置へのアクセスに問題があることが分かったため、同装置をシステムから切り離した。
- 所管省庁等へ連絡。

【４　原因】

- ゲートウェイルーターの設定で、ポートにアクセス制限がかけられておらず、また、監視装置で不要なポートが開いていたため、悪意を持った第三者から送信されたコマンドが送られてしまったもの

【５　再発防止策】

- ゲートウェイルーターのポート制限を実施（通常操作は可能）
- 悪意あるコマンドを受け付けないよう、プログラムを改修

【6　得られた気付き・教訓】

- **積極的な情報共有**

  当該事業者は、同型の機器を使用している他事業者への参考になるだろう、との考えで所管省庁へ自主的に報告を上げた。このように積極的に情報共有していただくことにより、他事業者の参考となり、重要インフラサービスの面的な防護にもつながる。
- **機器の設定確認**

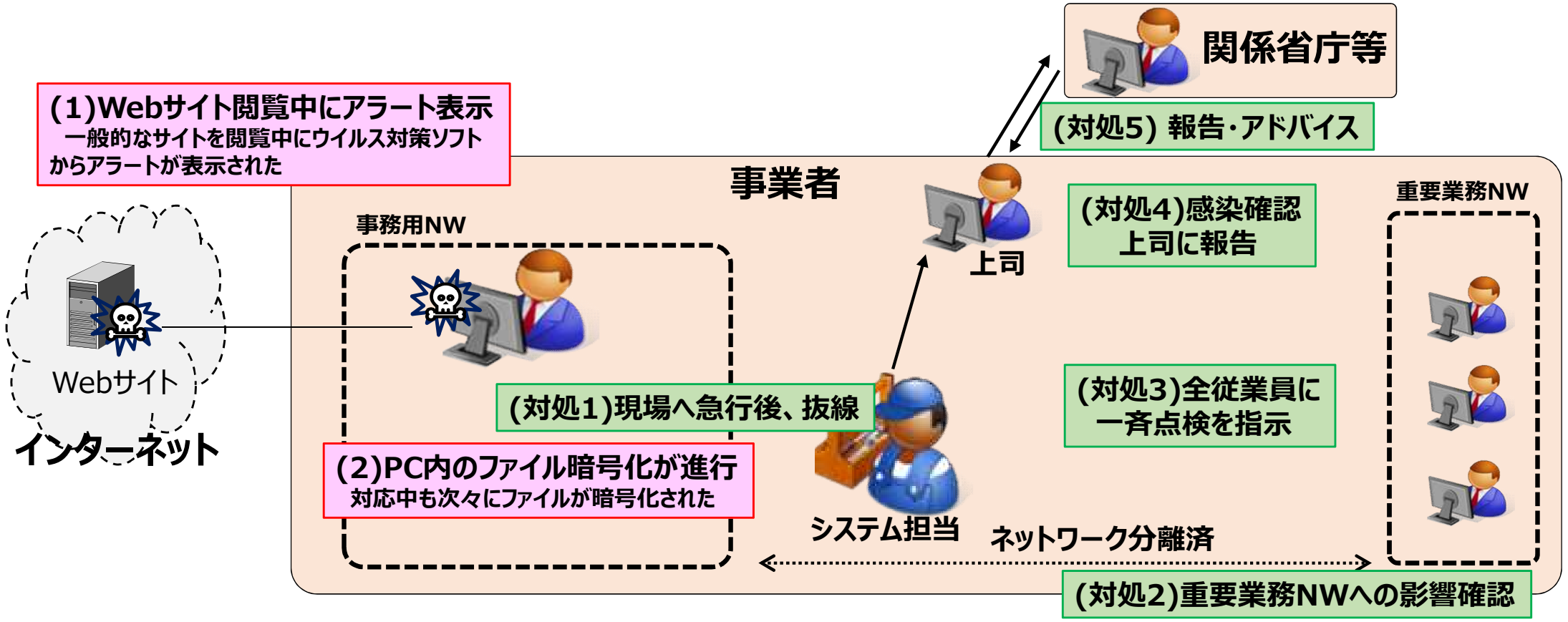
  機器の設定がほぼ初期設定だったことが不正アクセスを受けた要因になったので、本当に必要なポート以外は閉じるなどして、攻撃を受ける可能性を最小限に抑える努力が必要。
- **保守ベンダーとの情報共有等**

  インターネットに接続している機器については、サイバーセキュリティ対策がどのように行われているか保守ベンダーと情報を共有するとともに、必要に応じてセキュリティ対策を第三者に監査してもらうなど検討すると良い。

事例３　ランサムウェア被害　　１／２

【事例の概要】

- Webサイトの閲覧中に、ウイルス対策ソフトからアラートが表示された。
- システム担当に連絡し、早急にPCをネットワーク（インターネットに接続）から切り離した。
- ランサムウェアに感染したものであり、インシデント対応中もPC内で次々にファイルが暗号化され、最終的には数百のファイルが暗号化されていた。
- 重要業務ネットワークは、事務用ネットワークとは切り離されていたため、重要業務ネットワークへの感染はなかった。



事例３　ランサムウェア被害　　２／２

【１　背景】

- 重要業務ネットワーク(クローズドなネットワーク)と事務用ネットワーク(インターネットに接続されているネットワーク) を分けて構築していた。
- 事務用PCの管理は利用者各自に任せられており、セキュリティアップデートがなされていないものもあった。

【２　検知】

- Webサイトの閲覧中にウイルス対策ソフトのアラートが表示され、利用者がシステム担当へ連絡した。

【３　対処】

- システム担当が現場に急行し、ネットワークケーブルを抜線した。
- 当該PCがランサムウェアに感染していること、及び重要業務ネットワークへの影響がないことを確認した。
- 全従業員にウイルスチェックを依頼し、報告させた。
- 状況を上司に報告し、関係省庁等と連携をとった。
- 関係省庁等から助言をもらい、復号ツール(ウイルス対策ベンダー提供)を試した。

【４　原因】

- Webブラウザやソフトウェアの脆弱性を悪用したドライブバイダウンロード攻撃によるランサムウェア感染

【５　再発防止策】

- OSのセキュリティパッチやソフトウェアのバージョンを管理する仕組みの検討を始めた。
- ウイルス対策ソフトの管理サーバを導入し、定期的なパターンファイルの更新管理を検討した。
- 個人が作成したデータを保存するファイルサーバの導入を進めていたが、ランサムウェア対策として、
  - ・世代管理できること
  - ・PCから書込みができないドライブにバックアップが取れること

  をファイルサーバーの要件に加えた。

【6　得られた気付き・教訓】

- 日常的に連絡体制を周知することの大切さ

  （社内）システム担当への連絡先が周知され、各利用者もきちんと認識しており、日ごろから活用されていた

  （社外）関係する組織のシステム担当者と定期的に情報交換をしており、事例を共有でき、助言をもらうことができた。
- ファイルバックアップの重要性

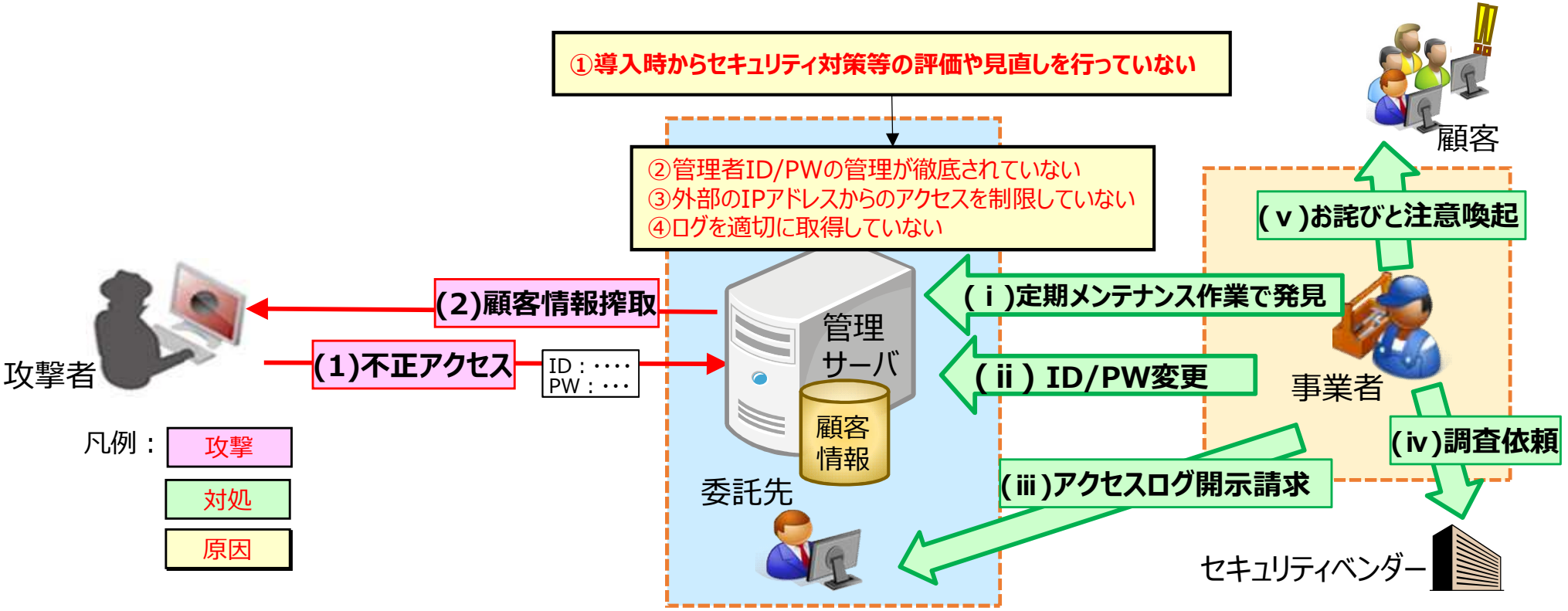
  ウイルス対策ベンダーが提供している復号ツールをいくつか試してみたが、処理にかなりの時間がかかり、今回のケースでは最終的には復号できなかった。バックアップ等の事前の対策が有効である。
- ネットワーク分離の大切さ

  重要業務ネットワークを事務用ネットワークと分離していたため、重要業務ネットワークへの影響はなかった。

事例4　管理サーバへの不正アクセス　1／2

【事例の概要】

- 攻撃者は、管理者ID/PWを取得し（経緯不明）、当該ID/PWで管理サーバへ不正アクセスを行った。
- 事業者は、管理サーバへの不正アクセスを定期メンテナンスで発見、顧客情報漏えいが判明。
- 委託先でログを取得する契約となっていないものの、委託先へ開示請求を行い、アクセスログを入手。
- アクセスログを基に、セキュリティベンダーに調査を依頼し、HPで顧客へお詫びと注意喚起。
- 継続的な評価・改善、ID/PWの管理徹底、アクセスの制限、ログによる早期検知などの対策を講じた。



事例4　管理サーバへの不正アクセス　２／２

【１　背景】

- 委託先のサーバを利用し、顧客情報のやり取りを行っており、外部のIPアドレスからのアクセスが可能。更に、アクセスログを取得する契約となっていない。
- 管理者ID/PWを定期的に変更していない。

【２　検知】

- 管理サーバへの不正アクセスを定期メンテナンスで発見し、委託先へログの開示請求を行った。
- セキュリティベンダーによる調査を行ったものの、管理者ID/PW漏えいの原因特定に至らず。

【３　対処】

- 管理者ID/PWを変更。
- HPで顧客情報漏えいについてお詫びと注意喚起。

【４　原因】

① 導入時からセキュリティ対策等の評価や見直しを行っていない。

② 管理者ID/PWの管理が徹底されていない。

③ 外部のIPアドレスからのアクセスを制限していない。

④ ログを適切に取得していない。

【５　再発防止策】

① 定期的にシステムの安全性を評価・改善するため、情報セキュリティ委員会（社長が委員長）を設置。

② 社内システム全てのID/PWを変更し、ID管理規程を整備し、PW変更管理を徹底。

③ 管理サーバへのアクセスを事業者のIPアドレスに制限。

④ ログ管理に関する規程を定め、ログを適切に取得。

【６　得られた気付き・教訓】

- **不正アクセスの未然防止**

① システム導入時から情報セキュリティ対策等の評価や見直しを行っていないことから、環境変化に伴う継続的な評価・改善を経営者主導で、全社的に取り組むことが重要。

② ID/PWの漏えいにより不正アクセスされたことから、ID/PWの変更を定期的に行い、漏えい防止の対策を講じるなど、適切に管理することが重要。

③ 外部から不正アクセスされたことから、外部のIPアドレスからのアクセスを制限することが重要。

- **不正アクセスの早期検知**

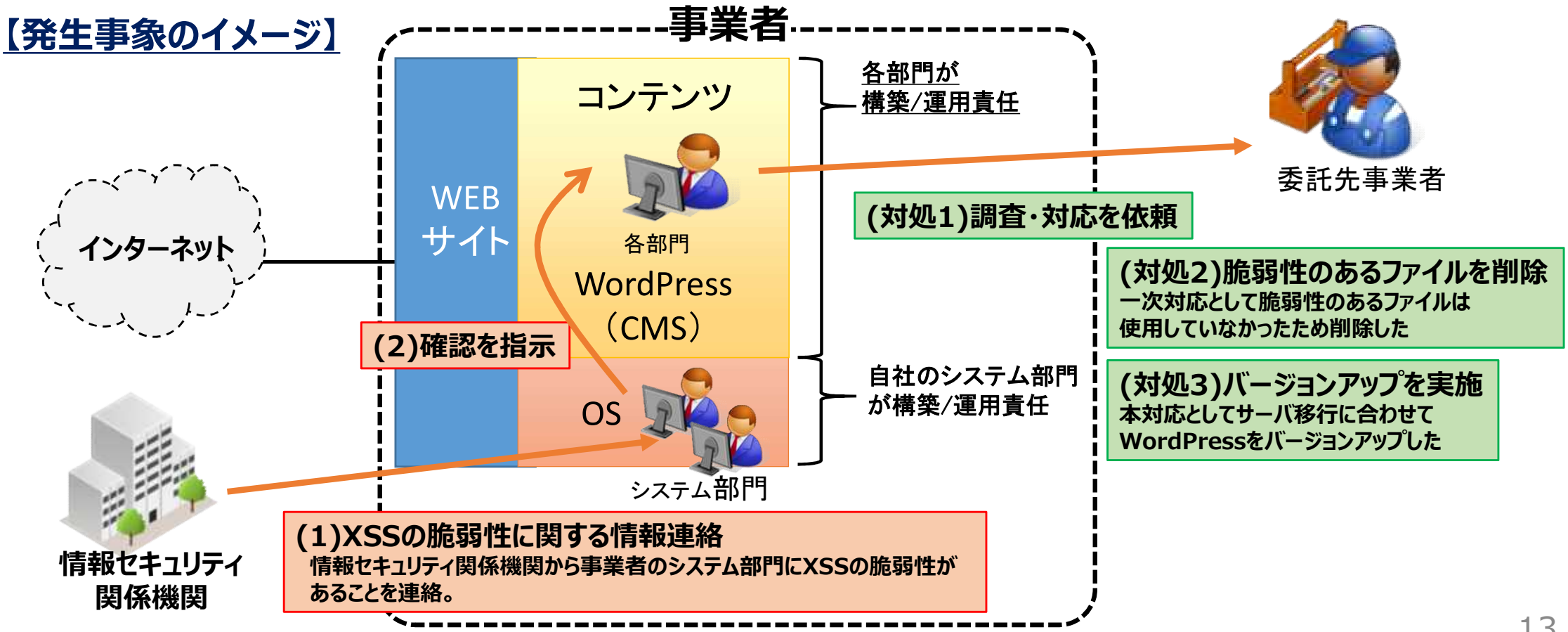
不正アクセスに気付くのに時間を要したことから、ログの取得を委託先との契約で明確化し、早期に検知することが重要。

事例５　ソフトウェアの継続的なセキュリティ対策　　１／３

【事例の概要】

- WordPressにXSS(クロスサイトスクリプティング)の脆弱性が発見され、セキュリティアップデートが公式HPにおいて公開された。
- 該当Webサイトはメンテナンス契約などを結んでおらず、担当者が脆弱性に気づかないままだった。
- 情報セキュリティ関係機関から、XSSの脆弱性に関する連絡を受け、委託先事業者に調査・対応を依頼した。

【発生事象のイメージ】



事例５　ソフトウェアの継続的なセキュリティ対策　２／３

【１　背景】

- 自部門のプロジェクトに関するWebサイトの構築を外部に委託し、システム部門が運用する共用サーバに配置した。
- 共用サーバにおけるOSのセキュリティ対策は、自社のシステム部門で一括して行われるが、CMS(コンテンツマネジメントシステム)等のセキュリティ対策は、各部門において管理する運用となっている。
- 該当WebサイトはCMS(コンテンツマネジメントシステム)のWordPressを用いて構築している。

【２　検知】

- 情報セキュリティ関係機関からWebサイトにXSSの脆弱性がある旨、システム部門に情報連絡があった。
- WordPressに関する脆弱性であり、セキュリティアップデートが10カ月前にリリースされていた。
- 調査の結果、脆弱性を利用したサイバー攻撃を受けた形跡はなかった。

【３　対処】

- 委託先事業者に連絡し、調査・対応を依頼した。
- 一次対応：脆弱性のあるファイルは、当該Webサイトでは使用していなかったため、削除した。
- 本対応：サーバ移行にあわせて、WordPressを最新のセキュリティアップデートにバージョンアップした。

【４　原因】

- 継続的に脆弱性情報をチェックする体制が定められておらず、該当Webサイトが脆弱性のある状態で放置されてしまった。

当時の体制

委託先事業者	・・・Webサイト構築までの契約(保守契約等なし)
自社システム部門	・・・共用サーバのOSのセキュリティ対策
各部門	・・・CMS等のセキュリティ対策

※各部門は当時セキュリティアップデートを確認しなければいけない認識がなかった

【５　再発防止策】

＜短期的対策＞

- 担当部門がWebサイトに関する定期的な脆弱性に関する情報を収集することとした。
- 保守契約があり、保守期間が残っているWebサイトについて、委託先事業者と脆弱性対応に関する取決めの確認を実施した。

＜中長期的対策＞

- システム部門にて、運用保守契約の中に、定型的に盛り込むべき継続的な脆弱性対応に関する項目を検討している。

事例５　ソフトウェアの継続的なセキュリティ対策　３／３

【６　得られた気付き・教訓】

- **各部門の役割の明確化**

① 「システム部門」と「各部門」それぞれが実施するセキュリティ対策の明確化

Webサイトの運用について、複数の部門が関係する組織体制の場合、どのような運用をする必要があるか留意点をまとめた社内共通の規程があると良い。

② メンテナンス契約の必要性

各部門に専門的な知識を持つ人が少なく、日常的にセキュリティに関する情報収集が難しい場合は、メンテナンス契約などにより運用を委託する方法もある。

- **脆弱性に関する情報収集の必要性**

① WordPressをはじめとするCMSソフトについても、オフィスのPCで使用しているソフトと同様に脆弱性の情報収集やセキュリティアップデートが必要

サーバで使用するソフトについても、脆弱性が発見され、修正プログラムが配布される。契約によっては、バージョンアップなどを行う場合は有償になるケースもある。

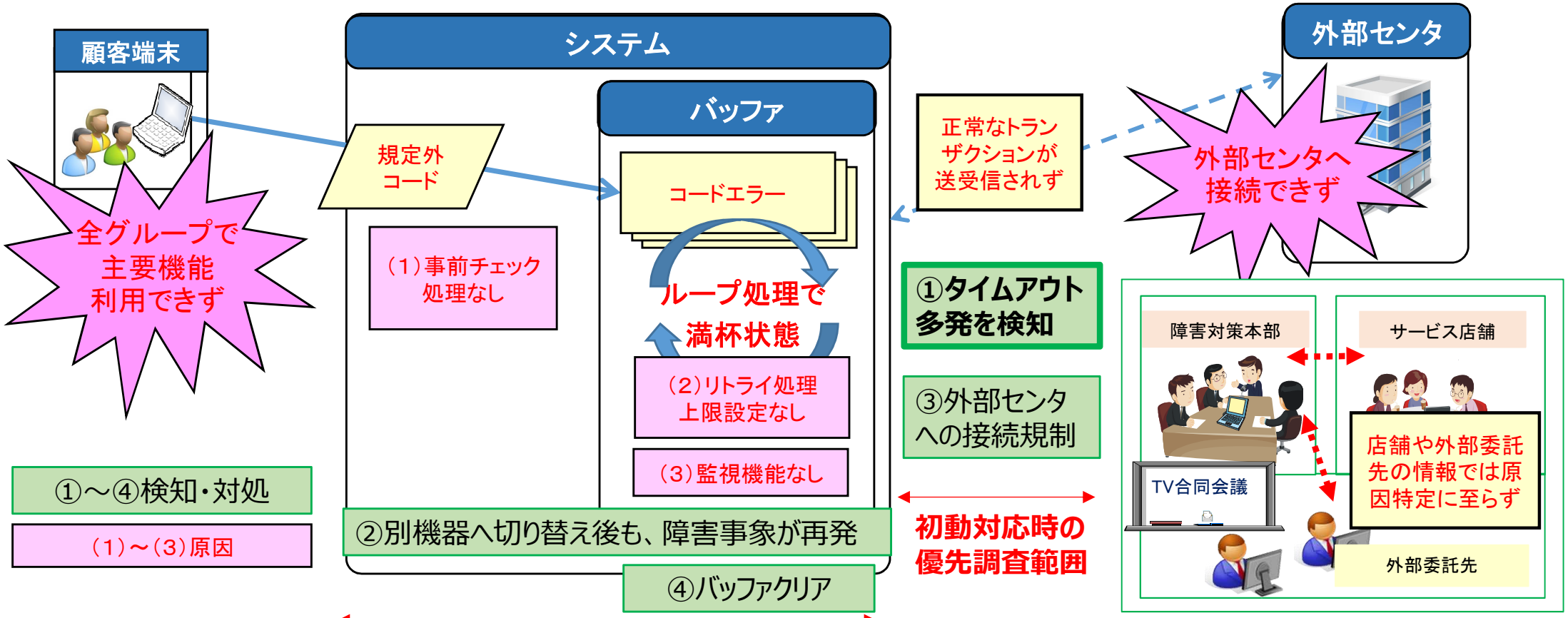
② 定期的な情報収集

情報収集先として、該当ソフトウェアの公式ホームページ、IPA、JPCERT/CC、NISCからのニュースレター等がある。事業者によっては、ISACやセプターに加入している場合があり、そこから得られる情報も有効である。

事例6　システムの不具合によるサービス障害　1／2

【事例の概要】

- 顧客が、端末にデータに異常があるカードを挿して操作を行ったところ、全グループ会社において、端末で他社との取引ができなくなった（複数の外部センタ間の接続も不可）。
- 過去に例のない障害のため、障害範囲の切り分けに手間取り、原因究明や復旧に時間を要した。
- 障害原因となったプログラムを改修。他の類似ロジックの総点検を実施した。
- システム監視設計強化、組織間情報共有の円滑化、想定外事態への対処を迅速化する対策を講じた。



事例6　システムの不具合によるサービス障害　　2／2

【1　背景】

- グループ会社とともにシステム運用を外部委託（システムは複数の外部センタと接続してサービスを提供）。
- 機器の切り替えなどのシステム障害対応訓練を、外部委託ベンダやグループ会社と定期的に実施。
- カードの不良によって、偶発的に、端末から規定外コードがシステムに送信。

【2　検知】

- システムと外部センタとの連携を要する特定の処理でタイムアウトを検知。
- 外部委託先から全グループ会社に自動通報。

【3　対処】

- 店舗や外部委託先のサービス影響情報では原因特定に至らず、タイムアウト多発したことを受け、過去障害事例を参考にネットワークの障害状況を確認・解析。
- 機器の切り替えや外部センタとの接続規制を実施するも同事象が再発。
- 共通バッファ領域※が枯渇していることを究明し、該当機器の再立ち上げ（バッファクリア）を実施し、復旧。

※バッファ領域は、外部センタとの共通バッファ領域であったため、関連する全ての外部センタで障害が発生。

【4　原因】

- 特定業務においてカードの事前チェック処理が一部漏れており、規定外コードがシステムに送信され、特定の処理が異常終了。
- 規定外コードのエラー処理がループ化されており、共通バッファ領域が枯渇し、当該領域を使用する処理にも影響が波及。
- バッファ領域の異常をリアルタイムに検知する仕組の不備。

【5　再発防止策】

- エラー処理ロジックの適正化（事前チェック処理の実装、リトライ処理の上限設定など）
- その他の業務に関連する類似ロジックの総点検を実施
- 現状把握・対処の迅速化に向けた手順の見直し及びマニュアル・ツール類の整備。
- 早期検知を可能とする監視設計の見直し（バッファ領域の状態の常時監視など）

【6　得られた気付き・教訓】

早期復旧体制の整備

① 重要リソースの異常をリアルタイムに検知していなかったことから、システム監視設計を強化し、障害を未然に防止することが重要。

② 想定外事態への原因究明に時間を要したことから、業務部門や外部委託先との間で、情報共有の更なる円滑化が重要。

③ 機器の切り替えでは復旧できなかったことから、想定外の事態を前提とした関係組織全てを巻き込んだ訓練が重要。