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

2017年度　重要インフラにおける補完調査について

２０１８年３月２０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

補完調査として、重要インフラサービス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

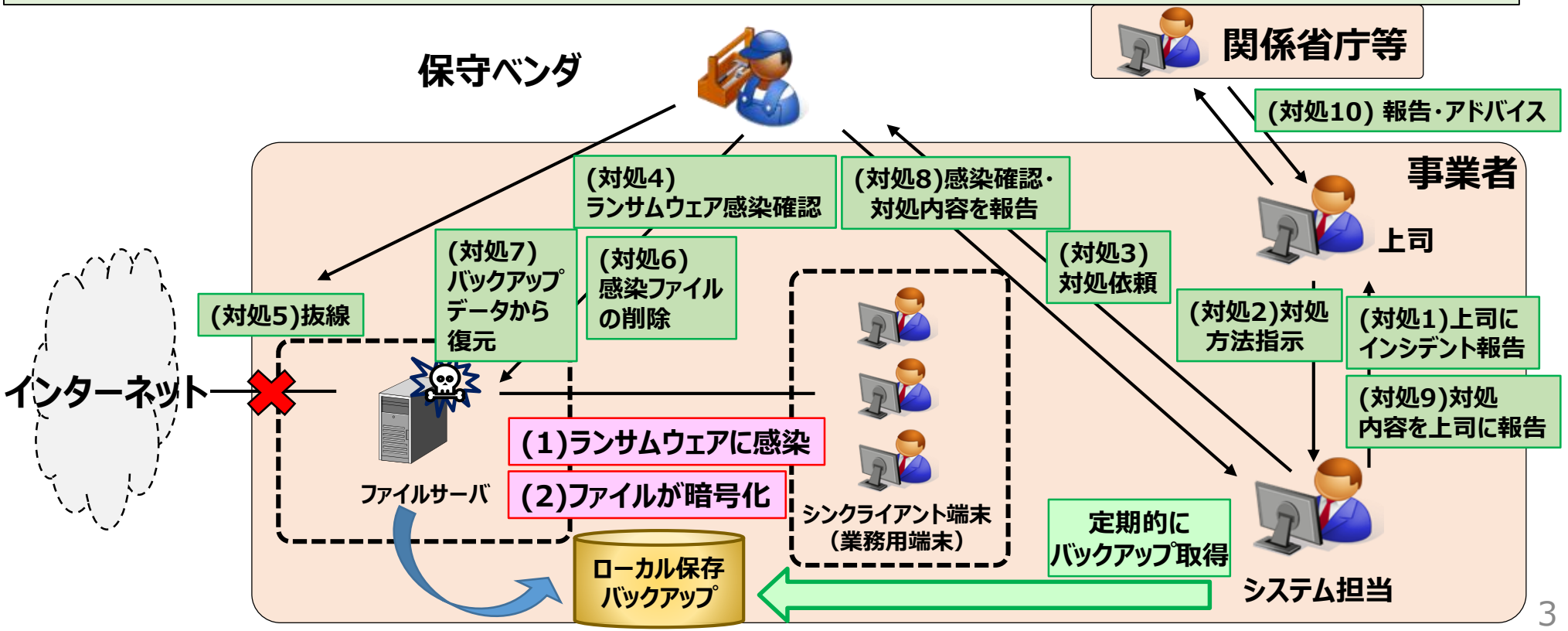
調査対象は、実際に発生した重要インフラサービス障害等について、類似事例の発生状況（可能性）や社会的影響（関心）の大きさ、及び得られる気付き・教訓の有用性等を考慮して、以下の事例を選定しました。

事例１　WannaCryによるサイバー攻撃
事例２　認証の脆弱なIoT機器への第三者アクセス
事例３　コインマイナー
事例４　SNSアカウント乗っ取り
事例５　世界中で広く利用されているフリーソフトウェアに由来したサプライチェーン攻撃
事例６　送信元詐称メールに対する備え
事例７　DDoS攻撃
事例８　リスト型の不正ログイン攻撃
事例９　SQLインジェクションによる個人情報流出

事例１　WannaCryによるサイバー攻撃　　１／２

【事例の概要】

- シンクライアント端末からファイルサーバにアクセスした際、「.WCRY」拡張子のファイルがあることに気づいたが、該当するファイルは開くことができなかった。
- 保守ベンダにて、ファイルサーバのLANケーブルを抜線してネットワークから隔離し、ファイルサーバがランサムウェアに感染していることをウイルス対策ソフトにて確認した。
- ランサムウェア感染していると考えられるファイルをすべて消去し、バックアップデータから復元した。
- 再度、感染がないことを確認した上で、ファイルサーバをネットワークに接続し、元の状態に戻した。



事例１　WannaCryによるサイバー攻撃　２／２

【１　背景】

- 業務都合上、シンクライアント端末上でUSBメモリを利用していたが、許可されたUSBメモリのみ使用可としていた。
- インターネットからダウンロードするものは全てウイルスチェックを徹底していた。
- シンクライアント端末は環境復元ソフトが入っており、再起動の度に設定された状態に復元される仕様になっていた。

【２　検知】

- シンクライアント端末からファイルサーバにアクセスした際、「.WCRY」拡張子のファイルがあることに気づいた。
- 関係省庁から、WannaCryに関する注意喚起があり、内容が酷似していることを確認した。

【３　対処】

- ファイルが開けない状態であったため、上司に報告し、システム担当が保守ベンダに対処を依頼した。
- 保守ベンダがランサムウェアの感染を確認し、インターネット接続用のLANケーブルを抜線した。さらにファイルサーバ内の感染していると考えられるファイルを削除した。
- 保守ベンダにより、システム担当が事前に取得し、ローカルに保存していたバックアップデータから、ファイルを復元した。
- 再度感染がないか確認した上で、ファイルサーバをネットワークに接続し、元の状態に戻した。
- 状況を上司に報告し、関係省庁等と連携をとった。

【４　原因】

- 感染原因は特定できておらず、おそらくUSBメモリ経由ではないかと思われる。

【５　再発に備えた対策】

- シンクライアント端末は、環境復元ソフトにより、セキュリティアップデートも無効化されてしまうため、セキュリティアップデートが有効化されるよう検討した。
- USBメモリの使用方法に関しては、再度周知徹底を行った。
- ローカルへのバックアップの定期的な取得を検討した。
- システム担当の一時対応強化のため、外部のセキュリティ研修に参加した。

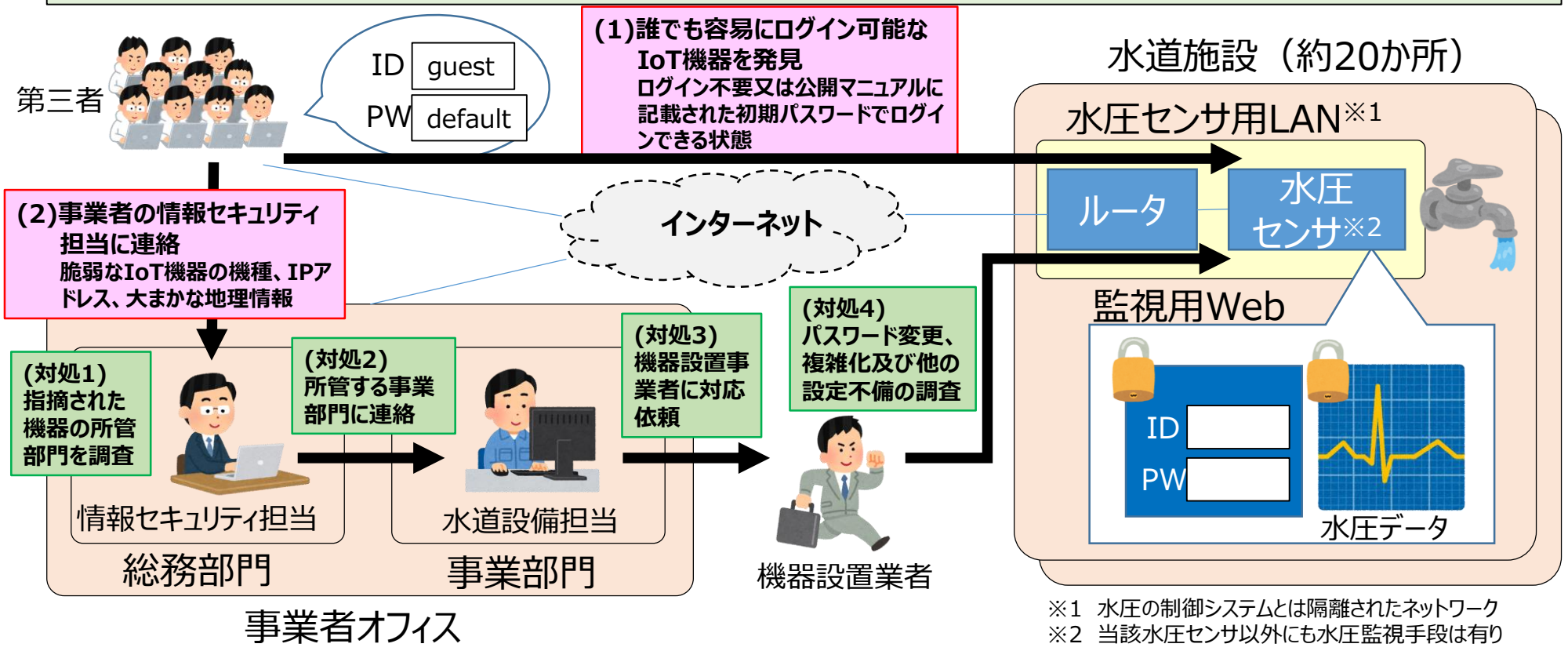
【６　得られた気付き・教訓】

- **重要データの定期的なバックアップ取得**
  システム担当者が定期的にバックアップを取得していたため、復号できないファイルに対しても、バックアップデータから復元することができた。ランサムウェア対策においては、定期的なバックアップを取ることが重要である。
- **関係省庁・団体との情報共有**
  今回の初動対応時、ウイルス対策ソフトでは感染が検知できない状況ではあったが、情報提供を受けていた内容と酷似していたことから状況を把握できたものであり、日頃からシステム担当者まで情報共有されていたことが役立った。

事例２　認証の脆弱なIoT機器への第三者アクセス　１／２

【事例の概要】

- 水圧監視用のIoT機器（以下、水圧センサ）数十台が、インターネット経由で第三者が容易にログインでき、監視情報を閲覧できる状態になっていることが、外部からの指摘により発覚した。
- 水圧センサに内蔵された監視用Webの認証が不要又はマニュアルから入手できるID/初期パスワードが使われており、接続可能なIPアドレスや端末も制限されていなかった。
- 情報セキュリティ担当とIoT機器所管の事業部門（水道設備部門）で連携して設置場所を特定し、機器設置業者の協力の下、対象の全てのIoT機器のパスワードを複雑なものに変更した。



※1　水圧の制御システムとは隔離されたネットワーク
※2　当該水圧センサ以外にも水圧監視手段は有り

事例２　認証の脆弱なIoT機器への第三者アクセス　２／２

【１　背景】

- 水道施設の水圧監視のため、水圧データを閲覧できる簡易Webサーバ機能（パスワード認証）を持つIoT機器（水圧センサ）を水道施設 約20か所に設置した。
- 導入は、各種設定の検討も含め、機器設置業者に委託していた。
- 当該IoT機器以外にも水圧監視の手段を有していた。

【２　検知】

- 事業者の情報セキュリティ担当が、第三者から、「脆弱なIoT機器を発見した」との連絡があり、対象の機器のIPアドレス、大まかな地理情報、問題点等を受領した。

【３　対処】

- 情報セキュリティ担当にて、受領したIPアドレスが割り当てられた機器の所管の事業部門を特定するため、調査を開始した。IoTデバイスは資産管理台帳の対象に含めていなかったため難航したが、最終的に水圧センサであることを特定し、事業部門（水道設備部門）に連絡した。
- 水道設備部門から機器設置業者に対して、該当機器のパスワードを複雑なものに変更するよう指示した。
- 機器設置業者にて、全ての水圧センサのパスワードを複雑なものに変更した。また、水圧センサの不正操作の痕跡、機微情報の漏えい、他の設定不備及び水圧の制御システムへの影響がないことも確認した。
- 情報セキュリティ担当にて、他の事業部門に対して、IoT機器が脆弱な状態で運用されていないか、確認を依頼した。結果、他に問題のある機器は発見されなかった。

【４　原因】

- 事業部門及び機器設置業者において、IoT機器のセキュリティ対策の必要性の認識が浅く、認証の設定についても導入時の検討事項に挙がらず、初期パスワードのまま導入されていた。
- 業務上、モバイル端末でのアクセスが必要であるため、インターネット経由でアクセスできる環境に水圧センサを接続していたが、水圧センサ及びルータへのアクセス元のIPアドレスや端末の制限は行っておらず、誰でもアクセス可能な状態で稼働していた。

【５　再発に備えた対策】

- IoT機器の設置に関して、資産管理やセキュリティ対策のルールを策定し、事業部門及び機器設置業者に展開した。

【6　得られた気付き・教訓】

- **IoT機器の管理とセキュリティ対策のルール化**

  IoT機器は、組織によっては事業部門が導入し、情報システム部門の管理外であるケースもあり、資産管理方法やセキュリティ対策、有事の際の対応について、双方協議の上、ルール化することが望ましい。

- **セキュリティ対策機能を備えたIoT機器の選定**

  IoT機器を選定する際、セキュリティ対策機能についても仕様を調べ、IoT機器で扱う情報や用途に相応であるかを確認すると良い。

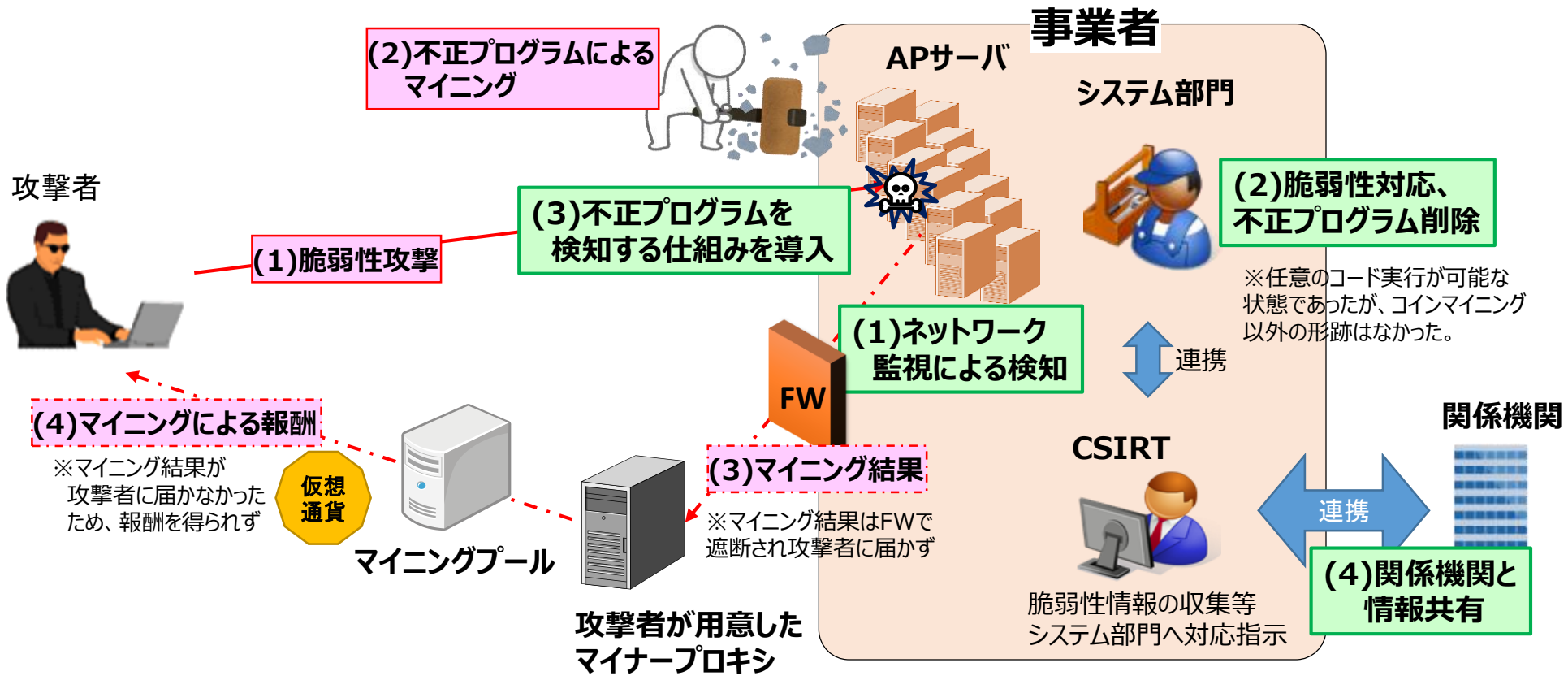
- **IoT機器のセキュリティ対策についての当事者意識**

  IoT機器への被害が進行すると、ボット化して外部への攻撃に使用されるおそれもあるため、セキュリティ対策は事業者がその必要性を理解して要件を定めることが望ましい。また、ベンダに導入を委託する場合も、どのような対策が必要かを事業者自身が理解し、チェックすると良い。

事例３　コインマイナー　1／2

【事例の概要】

- 攻撃者は、アプリケーションサーバ（APサーバ）の脆弱性をつき、仮想通貨をマイニングする不正なプログラムを埋め込み、マイニングさせた（結果は通信遮断により、攻撃者に届かず）。
- 大量のトラフィック（UDPパケット）の発生により、利用者がサービスにアクセスしづらいなどの影響が発生した。
- 大量のトラフィックの発生をネットワーク監視により検知し、調査後、本事案が発覚した。
- APサーバの脆弱性対応を行った上で、不正プログラムを削除し、検知する仕組みを導入した。



事例３　コインマイナー　２／２

【１　背景】

- CSIRT部門は、関係機関等を通じて、日々脆弱性情報等を収集し、サーバに保有する情報の重要度に応じて対策を行っていた。
- CSIRT部門からシステム部門に対して脆弱性対策を指示していたが、長期間対応を行っていなかった。

【２　検知】

- ネットワーク監視により、海外のIPアドレスへの大量トラフィック（UDPパケット）を検知（通常の３倍程度まで徐々に増大。CPU負荷も上昇）。

【３　対処】

- システム部門は、脆弱性対応を行った上、不正プログラムを削除した（任意のコード実行が可能な状態であり、他のサイバー攻撃を受けるおそれがあったが、コインマイニング以外の形跡がないことを確認した）。
- 不正プログラム（cronの改ざん）を検知する仕組みを導入した。
- インシデント内容について、関係機関と情報共有を行った。

【４　原因】

- 任意のコード実行が可能な緊急度の高い脆弱性を突かれ、不正プログラムを埋め込まれた。
- 過度にCPU負荷を与えないようなマイニングにより、検知するまでに時間を要した。

【５　再発に備えた対策】

- 事業者内で、脆弱性情報の重要度・緊急度の認識を統一し、CSIRT部門は、システム部門から定期的に対応状況の報告を受けることとした。
- 任意のコード実行が可能な脆弱性等が、マイニングに利用されたため、脆弱性対応に漏れがないよう、情報システムの構成管理方法を検討した。

【６　得られた気付き・教訓】

仮想通貨のマイニングを目的とした攻撃が増加しており、HPへのアクセスが困難になるなど、サービス提供に影響が発生するおそれがあることから、攻撃手法を認識し、事前に対策をとることが重要である。

- **コインマイニングの早期検知**

  ①　コインマイニングの検知に時間を要したことから、トラフィック量やCPU使用率（特に、Webサーバ等の権限によるプロセス起動）の上昇などシステム監視を徹底する。

  ②　さらに、システム監視では検知できない場合、不正な外部通信（マイニング結果の送信）や改ざん（cronの改ざん）を検知することが効果的である。

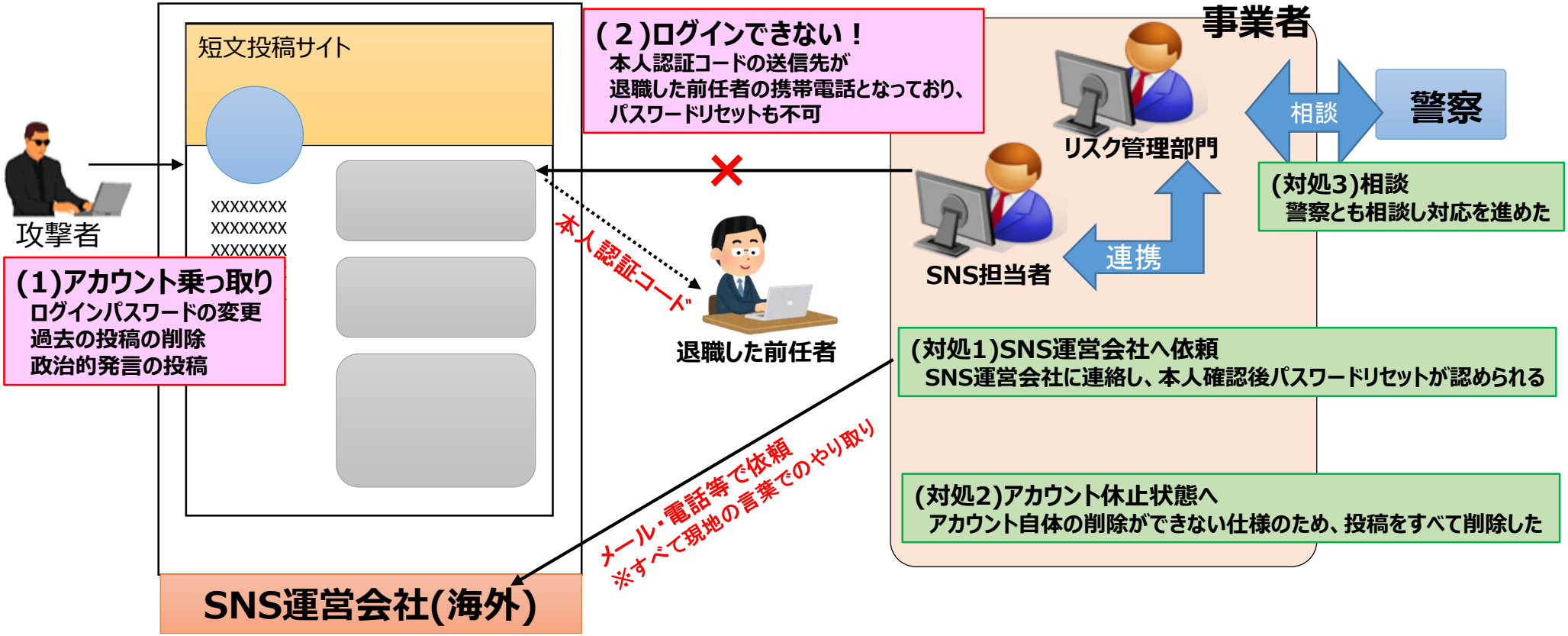
- **コインマイニングに関する情報共有**

  攻撃元IPアドレス等に加え、コインマイナー特有の情報（ウォレットアドレス、仮想通貨名等）の共有を行い、対策に活用することが重要である。

事例４　SNSアカウント乗っ取り　　１／３

【事例の概要】

- 海外へのPRのため、５年以上前から海外の短文投稿サイトを使用して情報発信を実施していた。
- 短文投稿サイト(SNS)のアカウントが乗っ取られ、パスワードが変更されるとともに、過去の投稿がほとんど削除され、政治的な発言が投稿された。
- SNS運営会社を通じてパスワードをリセットするとともに、SNSアカウント管理について見直し、周知を行った。



事例４　SNSアカウント乗っ取り　　２／３

【１　背景】

- 事業者は、海外へのPRを積極的に行うために、海外の短文投稿サイト(SNS)にアカウントを作成し、定期的に情報を発信していた。
- 事業者は、SNS担当者として現地出身の人を1年ごとに雇用し、現地文化を踏まえた表現を用いて、現地の言葉で発信していた。フォロワー数は順調に伸びており、クレーム等は発生していなかった。

【２　検知】

- SNS担当者が情報発信しようとしたところ、短文投稿サイトのログインができないことから本事案が判明した。
- 攻撃者にパスワードが変更されていたこと、及び本人認証コードの送信先が退職した前任者の携帯電話となっていたことから、パスワードリセットも不可であった。
- 投稿内容を見ると、ほとんどの投稿が削除されており、政治的な発言が投稿されていた。

【３　対処】

- 短文投稿サイトのSNS運営会社に連絡し、本人確認後、パスワードリセットが認められた。しかし、これ以上の対応(過去の投稿の復元、ログの解析や提供)はできないとの回答があった。

※やり取りはすべて現地の言葉で行われた

- 短文投稿サイトは、アカウントを退会(削除)できない仕様となっていたため、投稿内容及び登録していた画像をすべて削除した。
- 警察とも相談して対応したが、過去の投稿が削除されているため、被害を証明することが難しいことに加え、SNS運営会社が日本にはないため、対応が難しい案件となった。
- SNS運営会社の日本の代理店を通じて、有料の公式アカウントを申請した。新しいアカウントができ次第、新アカウントへ旧ユーザーを誘導する予定。

【４　原因】

- 攻撃者がID/パスワードの認証を突破し、短文投稿サイトのアカウントを乗っ取ったものと思われる。

【５　再発に備えた対策】

- ２段階認証を有効化し、不審なログイン試行(通常と異なる環境からのログインや連続パスワード試行等)が発生した際に、認証コードを入力させるようにする。
- 担当者の異動等によりアカウントを引き継ぐ際には、
  ・ログインパスワードの変更
  ・2段階認証に用いるメールアドレス(携帯電話番号等)の変更

  を確実に実施する。

事例４　SNSアカウント乗っ取り　　３／３

【6　得られた気付き・教訓】

・SNSアカウントの管理における対策

①不正アクセスの検知（2段階認証/不審なログインへのアラート設定）

不審なログイン試行が発生した際に、普段利用しているものとは異なる端末や環境からのログイン試行に早期に気付けるようにするため、あらかじめ登録した通知先にアラートを送信するように設定しておく。また、SNS担当者の異動の際は、２段階認証に用いるメールアドレス及び携帯電話番号の変更を着実に実施する必要がある。

②公式アカウントの作成における有料アカウントの検討

一般アカウントと有料アカウントでは、公式マークの表示や提供される機能など、サービス内容も異なる。リスクと得られるメリットを検討し、状況によっては有料アカウントも検討すると良い。

・SNSへのコンテンツ投稿における留意事項

①標的となるリスクの軽減

目的、発信方針(内容・表現)等を定めたソーシャルメディアポリシー(※)を策定し、SNS担当者と理解を共有しておくと良い。特に、海外の利用者を対象として情報発信する場合は、今回のように現地の文化的・政治的な背景をよく理解した上で、内容・表現に留意して発信することが望ましい。

※参考例　NISC　SNS運用ポリシー(https://www.nisc.go.jp/security-site/SNSpolicy.html)

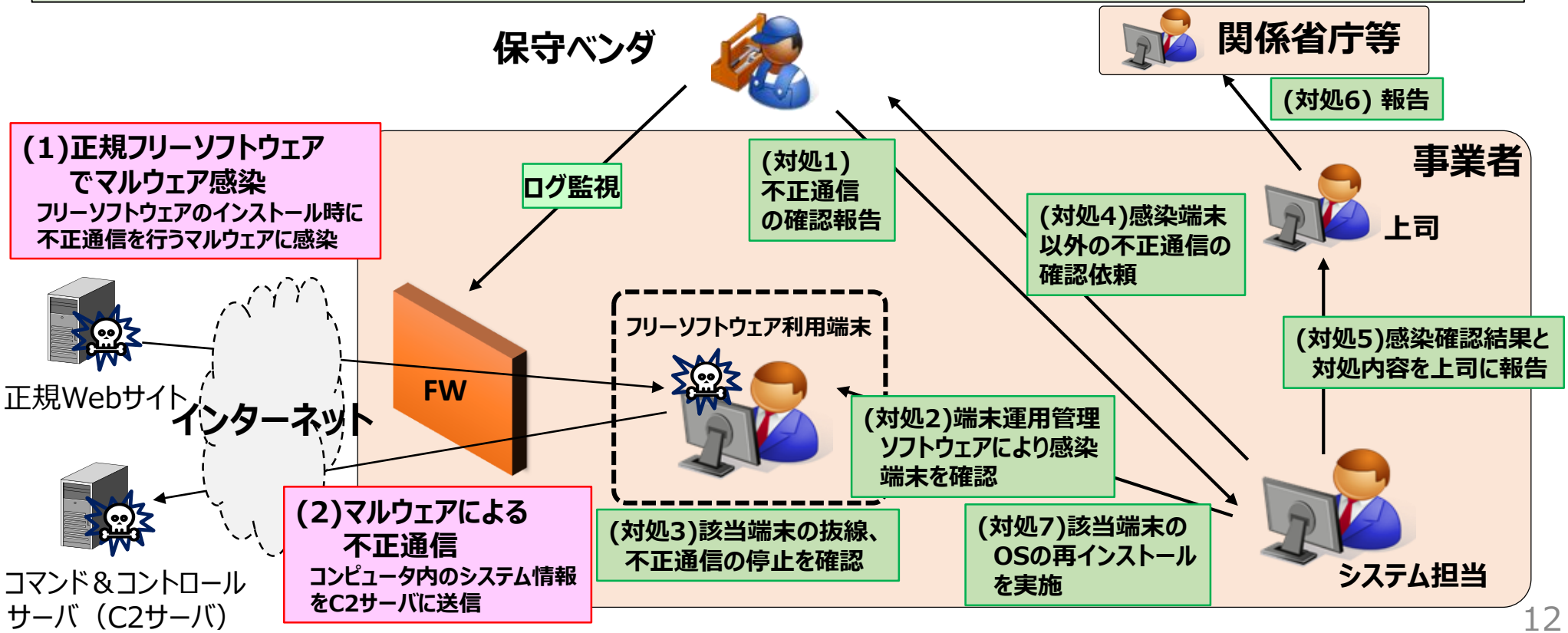
②投稿コンテンツのバックアップ

SNSで発信される情報は、その手軽さや重要度の低さなどからバックアップの考慮対象外となることが多い。しかし、投稿コンテンツが削除されてしまった場合、SNS運営会社側でも復元対応が困難なケースがある。被害の証明や復元のために、投稿内容のバックアップを取っておくと良い。

事例５　世界中で広く利用されているフリーソフトウェアに由来したサプライチェーン攻撃　１／２

【事例の概要】

- 保守ベンダから、マルウェアに感染したフリーソフトウェアに由来する不正通信が検出されたとの報告があった。
- システム担当が導入していた端末運用管理ソフトウェアにより、フリーソフトウェアをインストールした端末を特定し、早急に端末をネットワーク（インターネットに接続）から切り離した。
- 不正通信は、正規のフリーソフトウェアに埋め込まれたマルウェアによるものであり、フリーソフトウェアを利用していた感染端末以外からの不正通信等はないことを確認した。



事例５　世界中で広く利用されているフリーソフトウェアに由来したサプライチェーン攻撃　２／２

【１　背景】

- インターネット接続用にファイアウォールを構築していた。
- 端末へのソフトウェアのインストールは許可制(要申請)になっており、その旨は定期的な研修等で伝えていた。

【２　検知】

- 所管省庁から、広く利用されているフリーソフトウェアのマルウェア感染の可能性について注意喚起があった。
- 保守ベンダからシステム担当に対して、不正通信を行っている端末があることが報告された。

【３　対処】

- システム担当が端末運用管理ソフトウェアを利用し、当該ソフトウェアを使用している端末を探り当て、当該端末がマルウェアに感染して不正通信が行われていたことを確認した。
- ネットワークケーブルの抜線により、不正通信が停止したことを確認した。
- 保守ベンダに調査を依頼し、感染端末以外から不正通信が行われていないことを確認した。
- 状況を上司に報告し、関係省庁等と連携をとった。
- 保守ベンダの調査報告後に、該当端末のOSの再インストールを実施した。

【４　原因】

- 信頼できると考えられるフリーソフトウェアの正規インストーラにマルウェアが埋め込まれていた。
- 許可を取らずにフリーソフトウェアをインストールした。
  ※ただし、今回の場合は申請しても許可されていた可能性あり

【５　再発に備えた対策】

サプライチェーン攻撃に対して、決定的な対策を取ることは困難ではあるが、効果があるものと考え、以下の対策を実施した。

- インストールするソフトウェアの管理・把握を強化した。
- マルウェア感染事例として注意喚起を実施した。
- 全従業員向けに研修を実施し、セキュリティ意識の高揚を図った。
- サイバー攻撃に起因した事業継続計画（ICT-BCP）が策定されていないため、策定を検討した。

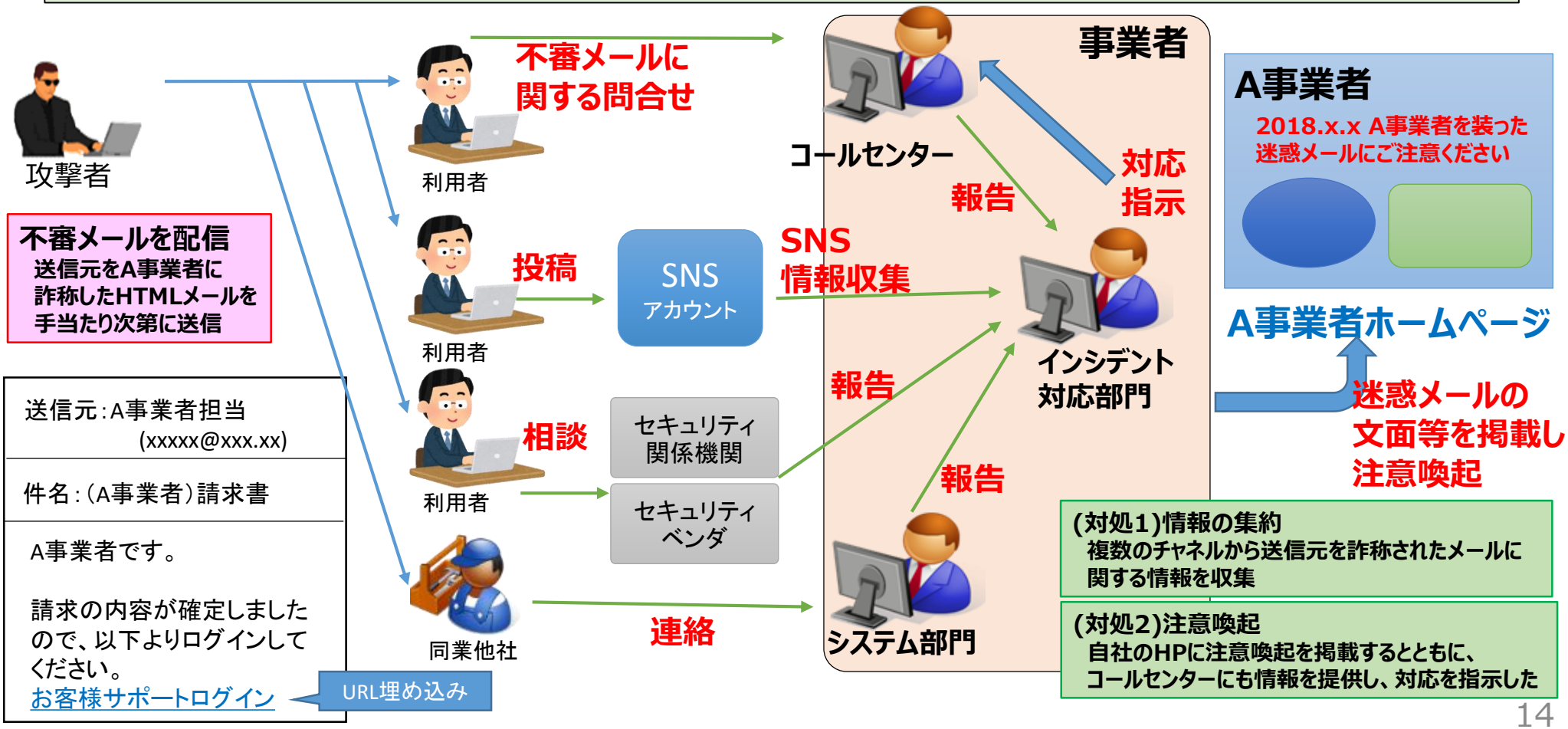
【6　得られた気付き・教訓】

- **資産管理の重要性（端末運用管理ソフトウェアの導入等）**
  本事案では、ファイアウォールを導入していたが、セキュリティポリシーが適用される前は不正通信が行われていた。感染端末の検索や許可されていないソフトウェアの検索のために、端末運用管理ソフトウェアを導入していたことが感染端末の早期発見に役立った。
- **ネットワーク監視の重要性**
  保守ベンダが早期に不正通信を検出したことが、本事案での被害抑止につながった。平時から、事業者内の端末からの通信を監視しておくことで、サプライチェーン攻撃のような予期せぬ感染の拡大防止に役立つと考えられる。
- **保守ベンダとの日常的な情報交換の大切さ**
  保守ベンダと良好な関係が構築できていたため、対応を必要とする情報が得られ、対応などについての相談もできたため、早期に原状回復することができた。

事例６　送信元詐称メールに対する備え　　１／２

【事例の概要】

- 近年、知名度の高い事業者名を使用した不審メールが出回る事例が多く、送信元を詐称された事業者はどのような対応を行っているのか好事例を調査した。
- 送信元詐称メールの情報は、複数のチャネルから寄せられていた。
- 情報はインシデント対応部門に集約され、迅速な対応がなされていた。



事例６　送信元詐称メールに対する備え　　２／２

【１　背景】

- 知名度の高い金融機関や物流事業者、テーマパーク等の事業者名を送信元に詐称する不審メールが増えている。
- 特に、重要インフラ事業者は、顧客からの信頼も厚いため、攻撃者に社名が利用されやすいと考えられる。
- 利用者からの信頼を維持するために、どのような対応が望ましいのか好事例を調査した。

【２　検知】

- 送信元詐称メールを認知する経路は、複数のチャネルにわたっていた。具体的には、利用者からの問合せ(コールセンター)、SNSによる投稿、セキュリティ関係機関やセキュリティベンダーからの報告、同業他社からの連絡等により、本事案を把握した。
- 大規模なものだと、コールセンターへの問合せ量が通常時の15倍近くになることもあった。

【３　対処】

- 複数の検知経路から受領した情報について、最終的にはインシデント対応部門に集約していた。
- インシデント対応部門は、HPに迷惑メールの文面等を掲載して注意喚起を行い、さらにコールセンターへの情報提供及び対応の指示を行うなど、対応を迅速に行うための連絡ルートを確立していた。

【４　得られた気付き・教訓】

- **巧妙に詐称されたメール文面やWebページの特徴**
  送信元詐称メールの文面は、普段事業者が定型的に送信する文章がほぼそのまま利用されているケースが多い。また、リンク先のURLについても、実際のWebページを模倣しているものもあるため、気付きにくい。
  しかし、事業者が送信するメールはテキスト形式であったが、送信元詐称メールはURLを隠すためHTMLメールになっていたり、ファイルが添付されていたり、ショートメッセージサービス(SMS)を利用していたりするなど、多少異なる点があった。
- **どの事業者にも存在するリスク**
  Webシステム等を堅牢に構築していたとしても、攻撃者が送信元を詐称してばらまくメールは防ぎようがない。そのため、どの事業者にも発生しうるインシデントであると言える。
  利用者からの信頼を失わないためにも、このようなリスクがあることを認識して対応できるよう、情報収集・情報集約・周知に関する連絡ルートを確認しておく必要がある。
- **顧客への注意喚起方法**

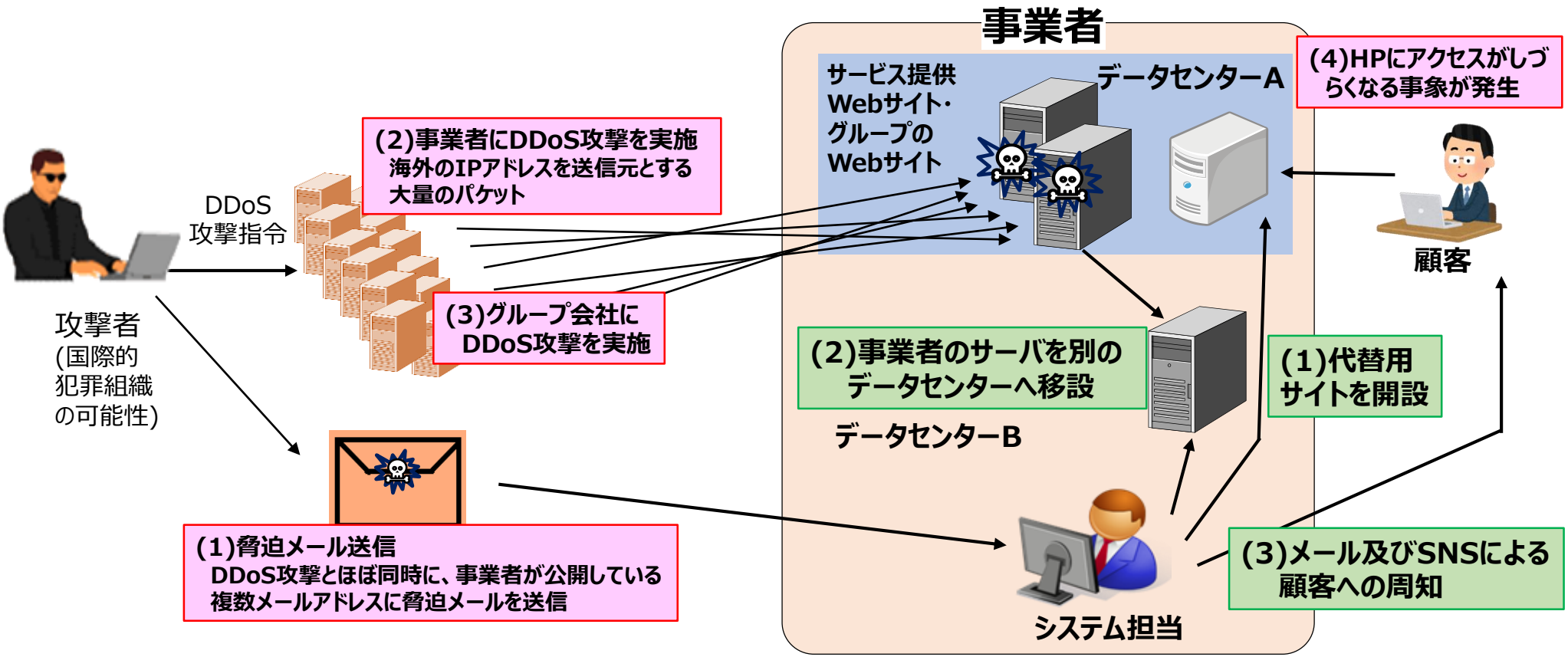
①広報方法
　詐称メールへの注意を促すために、自社のHPは良い広報ツールとなる。トップページのお知らせ欄や、アクセス数が多いページの上部等に表示することが効果的である。

②広報内容
　不審メールの文面が入手できる場合は、その文面をHP等に掲載すると効果的である(ただし、個人情報を掲載しないように注意する必要がある)。

事例７　DDoS攻撃　1／2

【事例の概要】

- DDoS攻撃の数日前から、HPへの軽微なDoS攻撃が行われていた（攻撃者による偵察の可能性あり）。
- その後、匿名の脅迫メールを受信し、ほぼ同時に海外からのDDoS攻撃が発生し、HPにアクセスしづらくなった。（同日中に複数回（グループ会社にも攻撃）、数日後にもDDoS攻撃が発生した）
- 当該HPの代替用サイトを開設するとともに、Webサーバの移設等を行い、影響を緩和した。
- HPにアクセスしづらくなっている事象について、メールやSNSにより顧客に周知した。



事例７　DDoS攻撃　　２／２

【１　背景】

- 事業者は、メインとなるサービスをHPで提供しており、当該サービスを継続的に提供することが最も重要であると位置づけていた。
- DDoS攻撃が発生する数日前から、HPへの軽微なDoS攻撃が行われていた(攻撃者による偵察の可能性あり)。また、関係機関からも同様の情報を得ていた。

【２　検知】

- 匿名の脅迫メールを受信し(DDoS攻撃解除のためにビットコインを要求するもの)、ほぼ同時に、海外からのDDoS攻撃が発生し、HPへアクセスがしづらくなった。

  ※同日中に複数回（グループ会社にも攻撃）、数日後にもDDoS攻撃が発生した。
- 脅迫メールの受信とほぼ同時にDDoS攻撃が行われたため、攻撃を事前に気づくことはできなかった。

【３　対処】

- 代替用サイトを開設するとともに、攻撃対象となったグループのWebサイトのサーバー分離等の対応を行った。
- 顧客対応については、HPで対応することができなかったため、メール及びSNSにより顧客に周知した。

【４　原因】

- 事業者は、これまでDDoS攻撃を受けたことがなく、特段の技術的対策や対応マニュアル等が整備されていなかった。

【５　再発に備えた対策】

- 早期検知や未然防止の観点から、クラウド型のDDoS攻撃対策サービスを速やかに導入した。
- 不審メールの受信時やサイバー攻撃を受けた際における情報連絡体制を整備した。
- DDoS攻撃等のサイバー攻撃を踏まえたBCPを策定し、業務継続体制を構築することを検討した。

【６　得られた気付き・教訓】

- **事業継続計画(BCP)の整備**

  DDoS攻撃への技術的な対策の準備がない場合は、即時対応が困難であるため、サービスの継続性が求められるものは、技術的対策やBCPを検討しておくことが重要（本事案では、代替用サイトを開設した）。

- **連絡体制の整備**

  同時多発的にサイバー攻撃が行われる可能性があることから、自社だけではなくグループ会社やサプライヤーなど内外の関係者を含めた複数の連絡体制の備えが重要である。

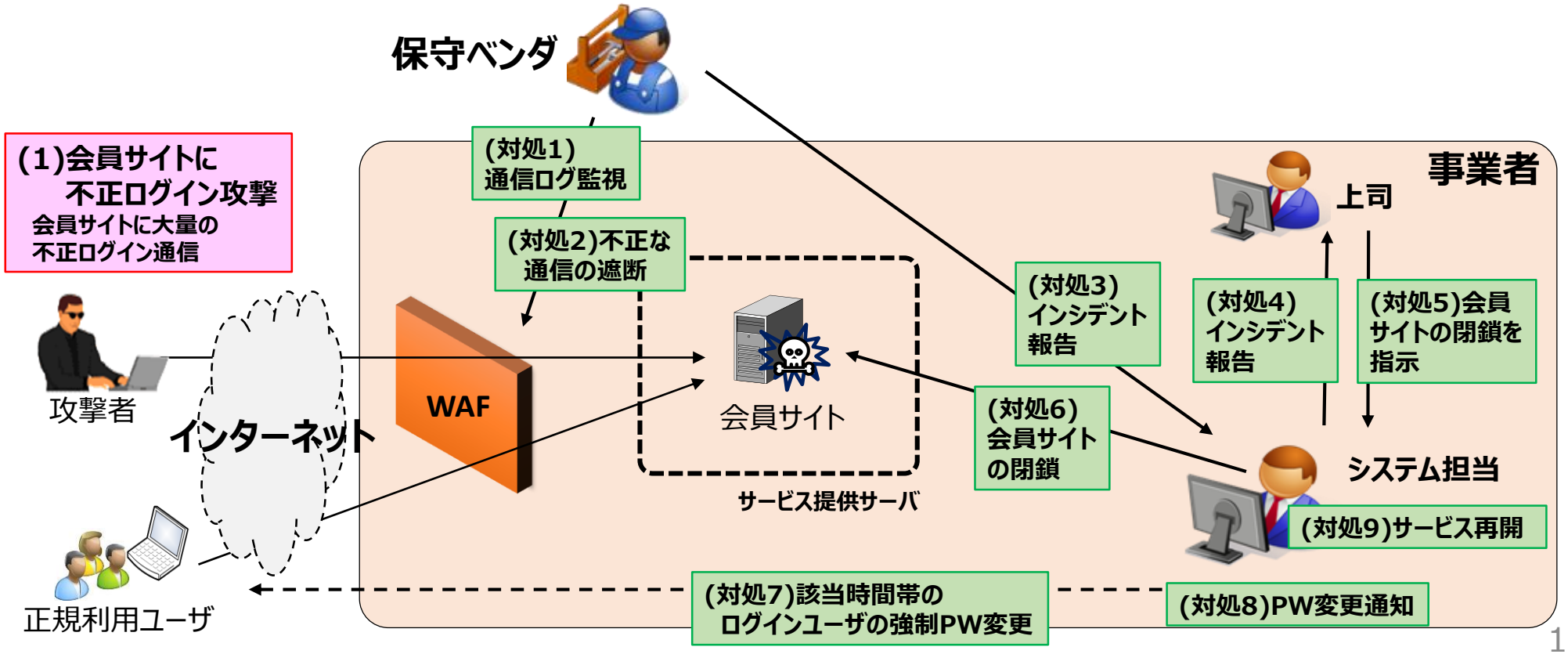
- **事後の検討**

  目的を達成するまで執拗なサイバー攻撃が行われる可能性があることから、復旧をもって対応を完了するのではなく、事後に攻撃内容を検証し、対策を検討することが重要である。

事例８　リスト型の不正ログイン攻撃　　１／２

【事例の概要】

- 事業者が運営している会員サイトに、ログインエラーが急増した。
- 保守ベンダがWAFを用いて、攻撃元のIPアドレスからの通信を遮断した。
- 攻撃者が別のIPアドレスから攻撃を行うことによって、サービスへの影響が出ることを懸念し、会員サイトを一時閉鎖した。
- 攻撃があった時間帯にログインのあったユーザに対して、パスワードを強制変更した。



事例８　リスト型の不正ログイン攻撃　　２／２

【１　背景】

- 会員サイトのセキュリティ対策として、WAF (Web Application Firewall)を構築していた。
- 会員サイトへのログインにはID/パスワードが必要であり、同一IDによるログイン試行が複数回失敗した場合、一定時間アクセスができなくなる設定としていた。

【２　検知】

- WAFにより、会員サイトへのログイン試行が増えていることを検知し、保守ベンダが攻撃元IPアドレスからの通信を遮断した後、事業者に報告した。
- ログの状況から、第三者によるリスト型攻撃と判断した。(数件の不正ログインが成功した形跡があり、氏名やメールアドレス等の情報が盗み見られた可能性がある)

【３　対処】

- 保守ベンダが、大量のログイン試行を行ったIPアドレスを特定し、WAFにて当該IPアドレスからの通信を遮断した。
- 上司に相談し、攻撃者が別のIPアドレスから攻撃するおそれがあったため、会員サイトを一時閉鎖した。
- 攻撃時間帯にログインのあったユーザのパスワードを強制変更した。
- パスワードを強制変更したIDのユーザに対して、メールや電話等により、パスワードの変更を通知した上で、会員サイトを再開した。

【４　原因】

- WAFによる不正ログインの検知は行っていたが、自動遮断機能は設定していなかった。
- ユーザが他サイトと同じパスワードを利用していた。

【５　再発に備えた対策】

- 大量のログイン試行による攻撃を検知した際、WAFにて自動的にアクセスを遮断する設定を行った。
- 他サイトと同じパスワードを利用しないこと、パスワードを定期的に変更することをユーザに周知（メール、ログイン画面）した。

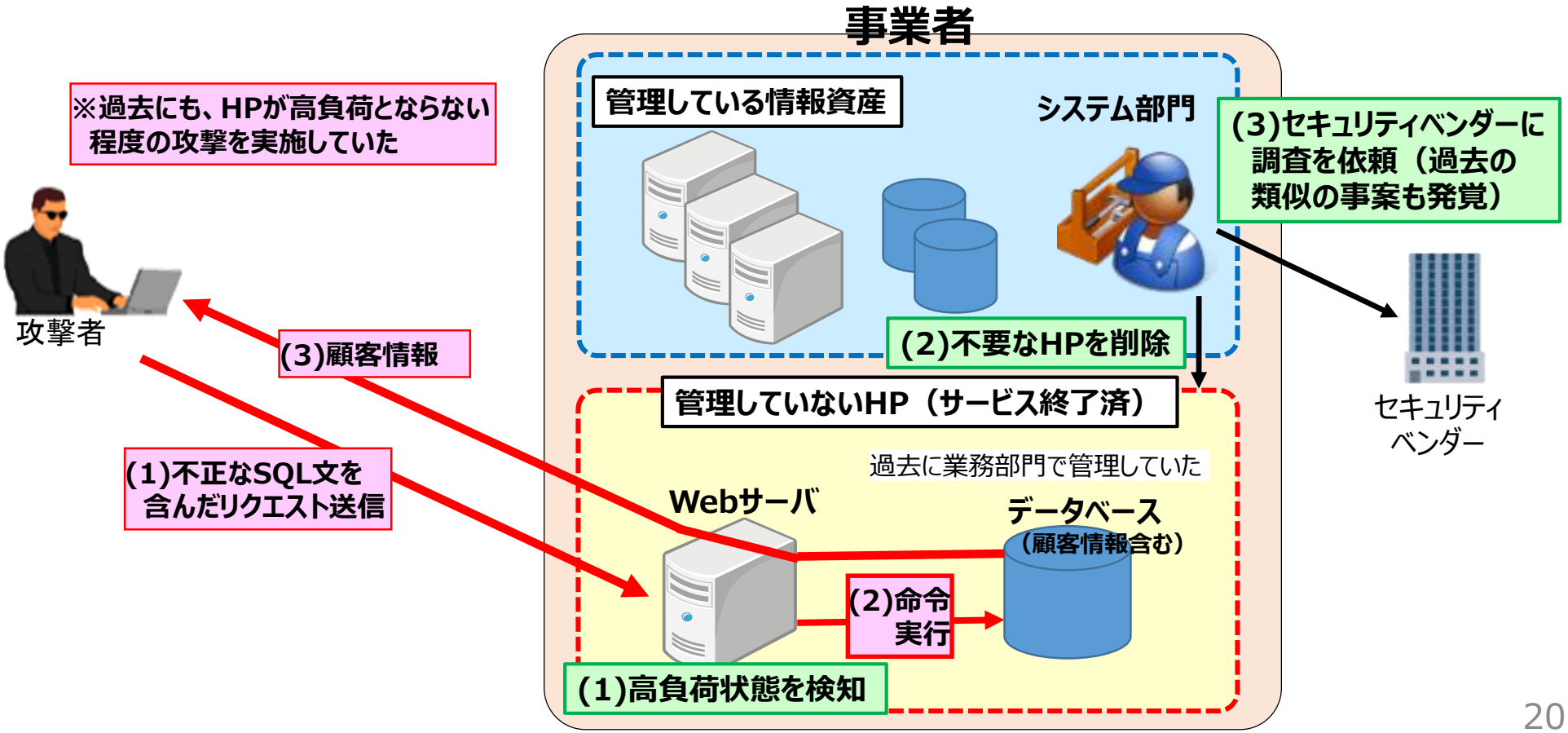
【6　得られた気付き・教訓】

- **システムログの分析**
  システムログの傾向分析を定期的に実施することで、平常時とは異なる状況にいち早く気づくことが大切である。また、分析した結果を踏まえ、WAFの自動遮断設定に生かすことが可能となる。
- **サイバー攻撃を考慮したサービスの継続や停止の判断の明確化**
  意思決定するためのルール（サービス継続・停止判断基準）を明確化・明示しておくことで、いざという時の判断や対応を迅速に行うことが可能となる。
- **ユーザへの継続的な注意喚起**
  他サイトと同じパスワードを利用しない等、ユーザに注意喚起し続けることが重要である。

事例９　SQLインジェクションによる個人情報流出　１／２

【事例の概要】

- 業務部門は、個人情報を含むHPのコンテンツのサービス終了に伴い、管理しなくなった。
- 攻撃者は、SQLインジェクションにより、サービス終了済みで管理していないHPから顧客情報を取得した。
- HPの高負荷状態の検知により、本事案が発覚した。さらにセキュリティベンダーの調査により、過去の類似の事案も発覚した。
- 攻撃対象となった不要なHPを削除し、不正アクセスの検知機能を強化した。



事例９　SQLインジェクションによる個人情報流出　２／２

【１　背景】

- 業務部門は、個人情報を含むHPのコンテンツを管理していたが、システム部門で一括管理することとなった。
- 一部のサービス終了済みHPのコンテンツは、業務部門からシステム部門に引き継がれないまま、管理されない状態となっていた。
- システム部門で管理しているHP等については、脆弱性アセスメントやペネトレーションテスト等を実施し、適切に対応していた。

【２　検知】

- HPの高負荷状態を検知し、SQLインジェクションによる顧客情報の漏えいが発覚した。
- セキュリティベンダーの調査により、過去にもSQLインジェクションによって顧客情報が漏えいしていたことも発覚した。

【３　対処】

- 攻撃対象となった、管理していない不要なHPを削除した。
- SQLインジェクション等の不正アクセスの検知機能を強化した。

【４　原因】

- 攻撃対象となったHPは、既に存在自体が認識されておらず、管理や対策が行われていなかった。
- 資産管理台帳が整備されていないことから、担当者がコンテンツを作成・削除・更新した場合に、管理者が認識できる仕組みになっておらず、オリジナルデータのコピー等も複数箇所に散在していた。

【５　再発に備えた対策】

- 業務部門の情報資産管理が不十分であったため、システム部門は、必要な情報資産以外を削除し、Webサーバを再構築した。
- 検知機能の強化の観点から、導入が容易なWAFのクラウドサービスの利用を開始した。
- 情報共有強化の観点から、経営層が関与するリスク管理委員会を設置した。
- 対策の実効性の観点から、各種関連規程・マニュアルを策定した。

【６　得られた気付き・教訓】

- **情報資産管理の徹底**

情報資産を洗い出した上で、管理台帳への登録を適切に行い、情報資産を網羅的に管理・対策することが重要である。（特に、使用しなくなった情報資産を放置しないことが重要）

- **SQLインジェクション等の未然防止**

脆弱性アセスメント等の結果を踏まえ、攻撃対象とならないよう、セキュアプログラミングによる安全なウェブサイトを作ることが重要である。（ただし、認識していない情報資産がある場合は、脆弱性が残存している可能性があるため、注意が必要）