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

資料７

2015年度　重要インフラにおける補完調査について

２０１６年３月２５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　DDoS攻撃によるサービス障害
事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い
事例３　USBメモリを介したマルウェア感染　※マルウェア･･･コンピュータウィルスなどの不正・悪質なソフトウェアの総称
事例４　Webサイトへの不正アクセス

事例１　DDoS攻撃によるサービス障害　　１／４

【事例の概要】

- サービス提供WebサイトがDDoS攻撃を受け利用者がアクセスできない状態となった。
- データセンター事業者にてトラフィック制限を行う等の対応を実施した。
- 分野内での情報共有を行うとともに、利用者への周知を実施した。

【背景】

- サービス提供Webサイトを外部のクラウドサービスを利用して構築。
- 告知用Webサイトは災害対応等を考慮し、別のデータセンターでも運用していた。

【検知】

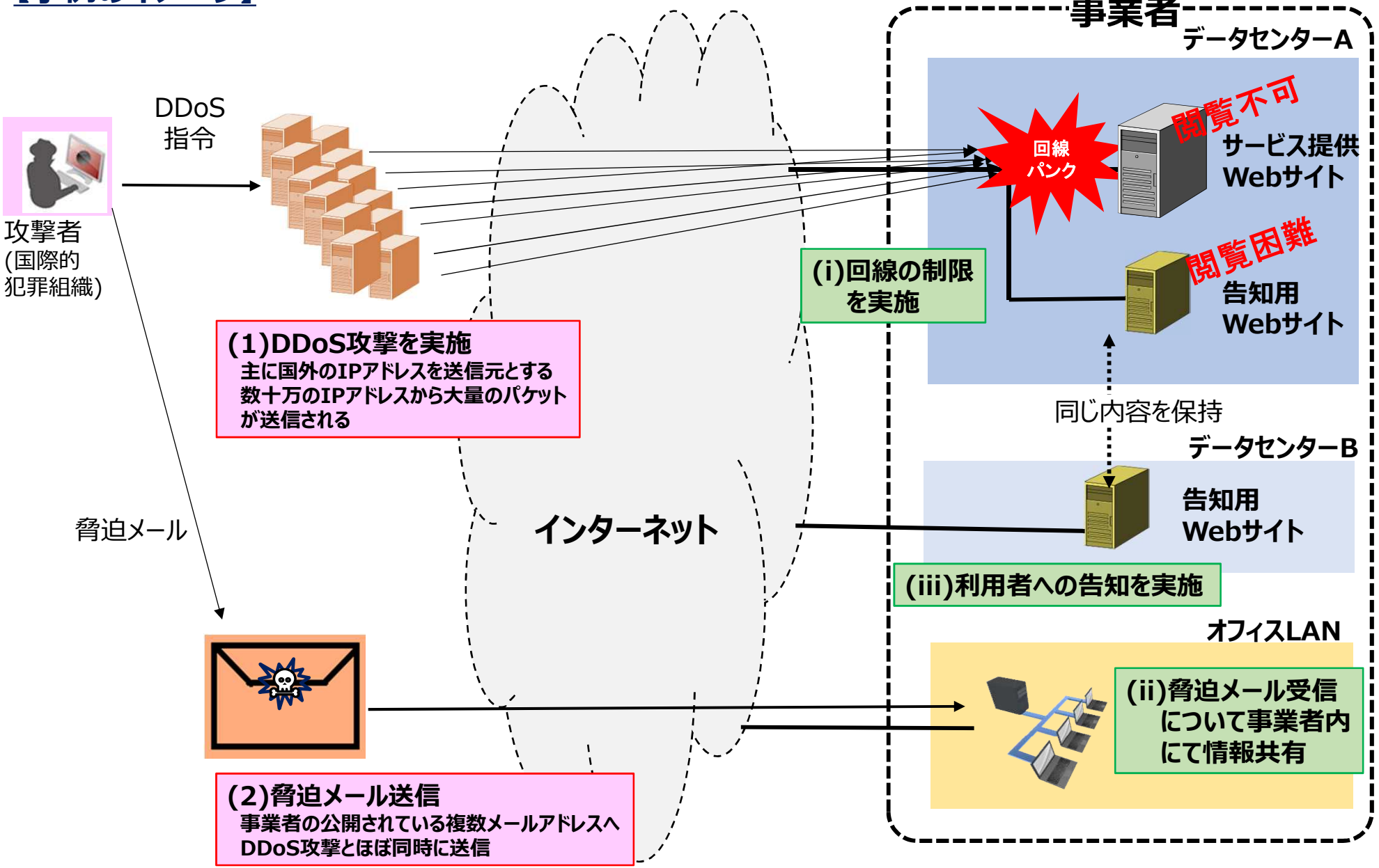
- 監視担当部署でサービス提供Webサイトの異常を検知しDDoS攻撃と判断。
- 同時にインターネット上に公開されているメールアドレス宛に金銭を要求する脅迫メールが届き、その情報が事業者内で共有された。

【対処】

- データセンター事業者側にてアクセス制限を実施した。
- 告知用Webサイトには影響がなかったため、そちらを通じて利用者にサービス利用不可の状況と代替サービスの提供方法の案内を実施した。
- 分野内での情報共有を実施。同じような攻撃を受けたケースを参考に対応を検討した。

事例１　DDoS攻撃によるサービス障害　２／４

【事例のイメージ】



事例１　DDoS攻撃によるサービス障害　３／４

【原因】

- 国際的な犯罪組織によるDDoS攻撃により、平時の1000倍以上もの通信がありデータセンターの回線がパンクした。

（DDoS攻撃解除のために金銭を要求※。）

※要求通り金銭を支払っても攻撃がやまない場合が多い。

【再発防止策】

＜短期的対策＞

- データセンター事業者にてサービス提供に用いていない通信を遮断※した。

※攻撃に利用された通信がUDPパケットのみだったため、UDPパケットがサービス提供に利用されていないことを確認の上、データセンター事業者側でUDPパケットをカットすることにより通信を維持させた。

＜中長期的対策＞

- CDN※サービスを利用することにより大量の通信を処理できる環境を検討。

※ Contents Delivery Network:ウェブコンテンツの大量配信に最適化されたネットワーク。負荷分散以外にも不要な通信を遮断し、必要な通信のみを正規サイトに流すオプションメニューもある。

- DDoS攻撃対策を含むセキュリティに関する社内規程を追加準備中。
- 今後不審な通信を遮断できるよう、送信元の国単位やIPアドレスの範囲を指定した遮断など柔軟な通信遮断手順を検討。

事例１　DDoS攻撃によるサービス障害　４／４

【得られた気付き・教訓】

- データセンター事業者と連絡が取れるような体制の構築
  （DDoS攻撃ではサーバーの負荷上昇に止まらず、データセンター事業者の回線をパンクさせる場合もあるため、データセンター事業者との連携体制を構築しておくことが重要。）
- 外部との積極的な情報共有
  - ✓ 外部との情報共有窓口の明確化
    （分野内の情報共有により、攻撃者の傾向を知り迅速に対策を打つことができた。）
  - ✓ 周囲から情報を得るため、まずは自らの情報を発信
    （事象発生時の情報発信について、予め経営層を含めたコンセンサスを得ておく。）
- サービス利用者への周知方法の確保
  - ✓ 告知手段の冗長化
    （告知用Webサイトを複数データセンターで構築していたため、事象発生時も告知手段を確保できた。この他、電子メールやtwitter等も検討されていた。）
  - ✓ インシデント対応における広報担当者との連携
    （対応チーム内に広報担当がいたおかげで、状況に応じ適切な告知手段を選択するなど、対外的な対応もスムースに行うことができた。）

事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い　１／４

【事例の概要】

- 改ざんされたWebサイトにアクセスした事業者に対して、NISCから注意喚起を実施。
- 端末を特定し隔離するとともに、事業者全体のインターネット接続を遮断。
- 事業者のIT担当部署が調べたところ、Adobe Flash Playerが最新だったため感染はなかった。

【背景】

- 事業者内LAN及びインターネット接続の管理をIT担当部署が実施。
- 職員が業務上よく利用するWebサイトが改ざんされた。

【検知】

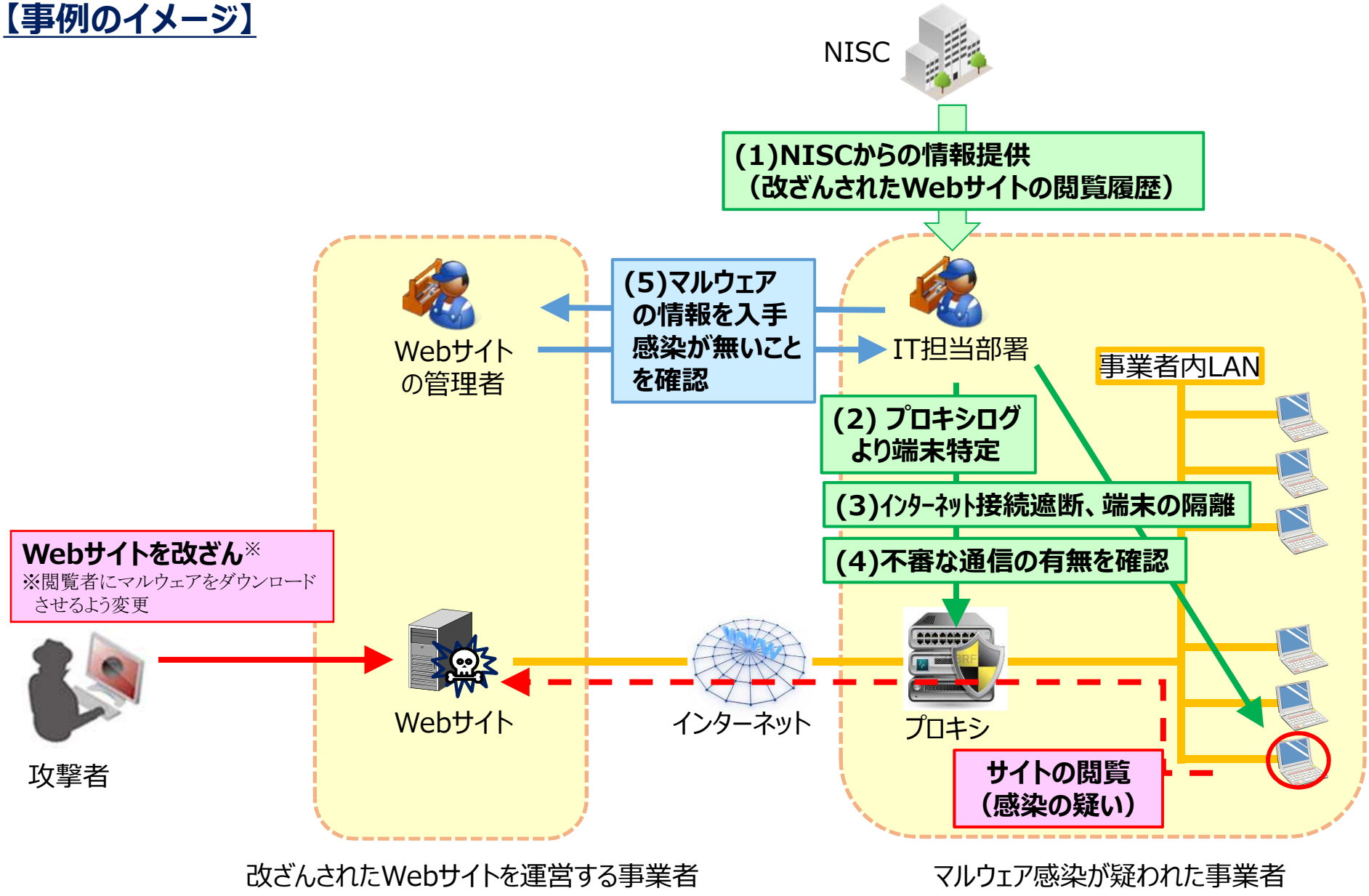
- NISCからの所管省庁を通じた情報提供により、IT担当部署がマルウェア感染の疑いを認知。

【対処】

- 保守ベンダー※と連携し、情報提供の内容を元にプロキシログから感染の疑いがある端末を特定。
  ※事業者内LAN管理業務の委託先。契約時間外であったが、緊急時対応として対処。
- 該当端末を隔離するとともに、プロキシの停止によりインターネット接続を遮断※。
  ※インターネット接続の遮断についての権限はIT担当部署にあることが、規程に定められていた。
- プロキシログから該当端末が外部へ不審な通信をしていないことを確認。
- 改ざんされたWebサイトの管理者からマルウェアに関する情報※を入手し、マルウェア感染がないことを確認。
  ※マルウェアのファイル名、保存先、通信先情報等

事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い　２／４

【事例のイメージ】



事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い　３／４

【原因】

- 事業者内LANに接続された端末が、改ざん※されたWebサイトにアクセスした。
  ※ブラウザのプラグイン（Adobe Flash Player）の脆弱性を利用しマルウェアに感染させる仕掛けが埋め込まれた。
- 端末のブラウザのプラグインは更新済みであったため、マルウェア感染はなかった。

【再発防止策】

＜短期的対策＞

- 業務上必要な場合を除き、該当のプラグインを原則使用禁止とした。
- やむを得ず使用する場合は常に最新版にアップデートするよう注意喚起を実施。

＜中長期的対策＞

- ネットワーク機器のログ監視・分析能力の強化策を検討。

事例２　改ざんされたWebサイトの閲覧によるマルウェア感染の疑い　４／４

【得られた気付き・教訓】

- 不要なブラウザのプラグインの使用禁止
  （一律禁止できない場合は、実行を制限するブラウザ設定等の導入も検討すべき。）
- 緊急時を考慮した規程類や判断基準等の事前確認・見直し
  （社内規程に従いIT担当部署の判断でインターネットを遮断できた。）
- 緊急時を考慮した保守体制の整備
  （事象発生直後から保守ベンダーと連携し迅速に対応できた。）
- プロキシログ等の調査手順の確認
  （プロキシログの調査手順を知っていたため、端末を迅速に特定できた。）
- インターネット接続の遮断等についての具体的手順の確認
  （プロキシを停止したことにより必要な通信も遮断されてしまった。）
- 能動的な情報収集と対策への活用
  （配信されたマルウェアの情報を入手することで、感染がないことを確認できた。）

事例３　USBメモリを介したマルウェア感染　１／４

【事例の概要】

- スタンドアローン※で運用中のPCにおけるマルウェア感染が発覚。
- PC間のデータ交換のために、USBメモリを日常的に使用しており、それを介して感染が拡大した。
- USBメモリを使用した全PCを特定し、ウイルス対策ソフトを用いて駆除。

※LAN等のネットワークに接続していない状態をいう。

【背景】

- 事業所内のほとんどのPCがスタンドアローンによる運用で、外部の事業者とのデータ交換、PC間のデータ交換、PCのソフトウェア更新に、それぞれ特定のUSBメモリを使用。
- USBメモリの使用は管理され、許可されていないUSBメモリの使用は許されていない。
- 業務要件によりウイルス対策ソフト等が導入できないPCも存在。

【検知】

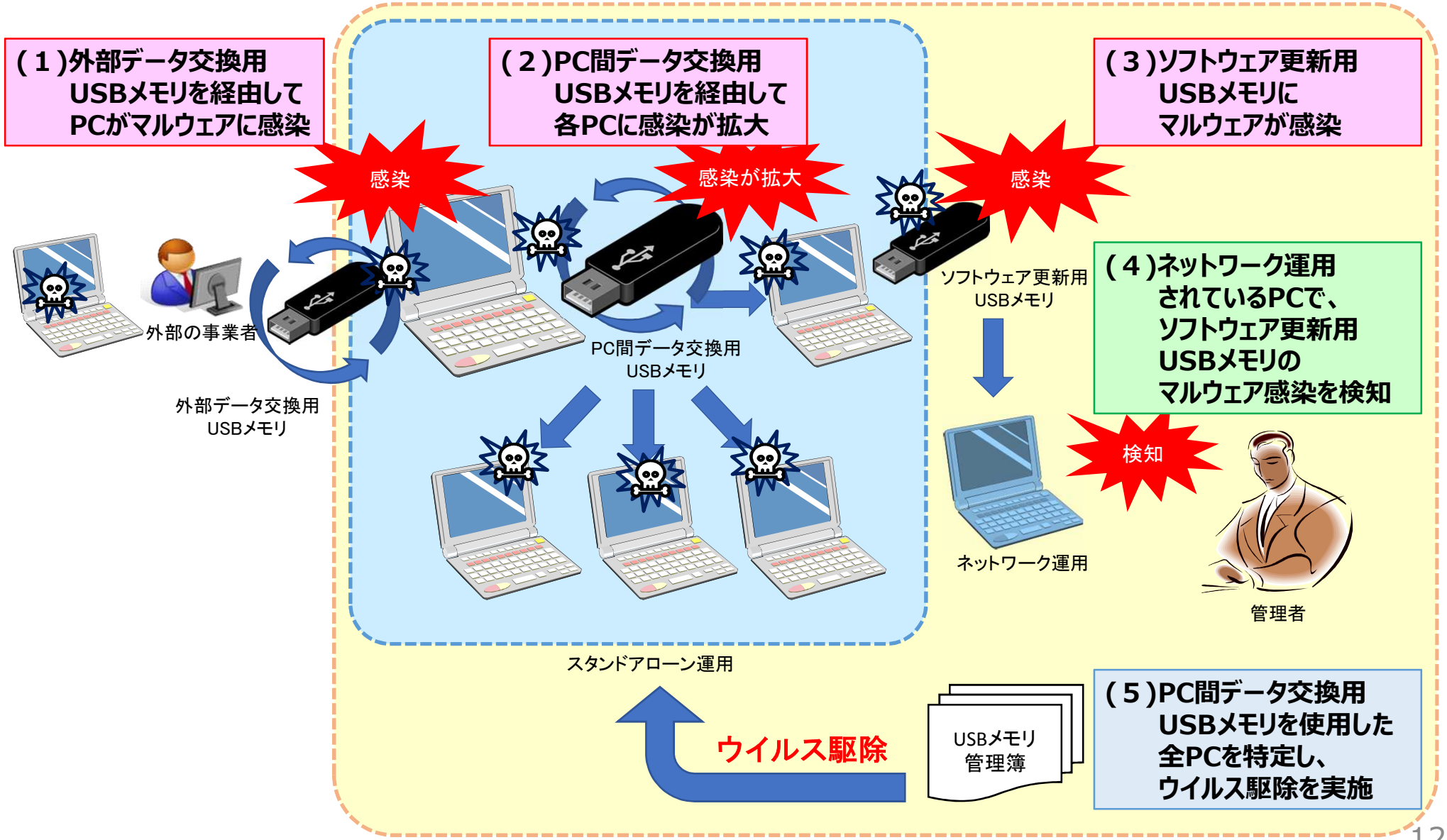
- ソフトウェアの更新に用いていたUSBメモリをネットワーク運用されているPCに挿入した際、マルウェアを検知。

【対処】

- PC間のデータ交換用USBメモリを使用した全てのPCを特定。
- ウイルス対策ソフトが導入できるPCは、ウイルス対策ソフトを最新の状態にし、ウイルス駆除を実施。
- ウイルス対策ソフトが導入できないPCは、USBメモリ型のウイルス対策ソフトでウイルス駆除を実施。

事例３　USBメモリを介したマルウェア感染　２／４

【事例のイメージ】



事例３　USBメモリを介したマルウェア感染　３／４

【原因】

- 過去に外部の事業者とUSBメモリを用いてデータ交換していたことから、そのUSBメモリを介してPCがマルウェア感染していたものと思われる。
- 上記PCから、組織内PC間のデータ交換に用いるUSBメモリを介して、他のPCへ更に感染が拡大したものと考えられる。

【再発防止策】

＜短期的対策＞

- ウイルス対策ソフトを導入できるPC

  USBメモリ等を用いて、定期的にウイルス定義ファイル等の更新を実施する。

- ウイルス対策ソフトを導入できないPC

  USBメモリ型のウイルス対策ソフトを用いて、定期的にウイルスチェックを実施する。

  USBメモリを用いて外部とデータ交換をする際は、事前に別のPCでウイルスチェックを実施する。

＜中長期的対策＞

- PCのネットワーク化及び管理サーバーの導入による手動更新の負担軽減などを検討している。

事例３　USBメモリを介したマルウェア感染　４／４

【得られた気付き・教訓】

- スタンドアローンで運用しているPCの把握と適切なセキュリティ対策の実施
  （スタンドアローンのPCもUSBメモリ等を介して、マルウェアに感染する可能性がある。）
- スタンドアローンで運用しているPCにおけるウイルス対策ソフト等のソフトウェアの最新化
  - ✓ ソフトウェア更新作業の組織的な運用計画の整備
    （人手を介した更新作業は運用負担が大きいため、場当たり的な対応では、作業の実施漏れや引継ぎ漏れ等により、更新されない状態が長く続いてしまう可能性がある。）
  - ✓ 業務要件によりウイルス対策ソフト等をインストールできないPCへの対策
    （USBメモリ型のウイルス対策ソフトを用いた対応も可能だが、運用負担軽減のための対策を別途検討する必要がある。）
- USBメモリ等外部記憶媒体の使用履歴の保持
  （履歴を元に感染の疑いのあるPCを特定し、調査対象範囲を絞ることができる。）

事例４　Webサイトへの不正アクセス　　１／４

【事例の概要】

- Webサイトへの不正アクセスにより、Web管理者情報の窃取やWebサイトの改ざんが発生。
- 事案の発生がNISC等から事業者に対して速やかに伝達され、被害を最小限に。
- Webサイトを一時閉鎖後、CMS※やレンタルサーバの脆弱性対策等を実施。

※Content Management System：Webサイト上のコンテンツを管理・編集するためのソフトウェア。

【背景】

- Webサイトのコンテンツ制作は外部業者に委託。
- Webサーバは外部のレンタルサーバを利用するが、日々の保守・運用は事業者自らが対応。

【検知】（事案2は事案1から約半年後に発生）

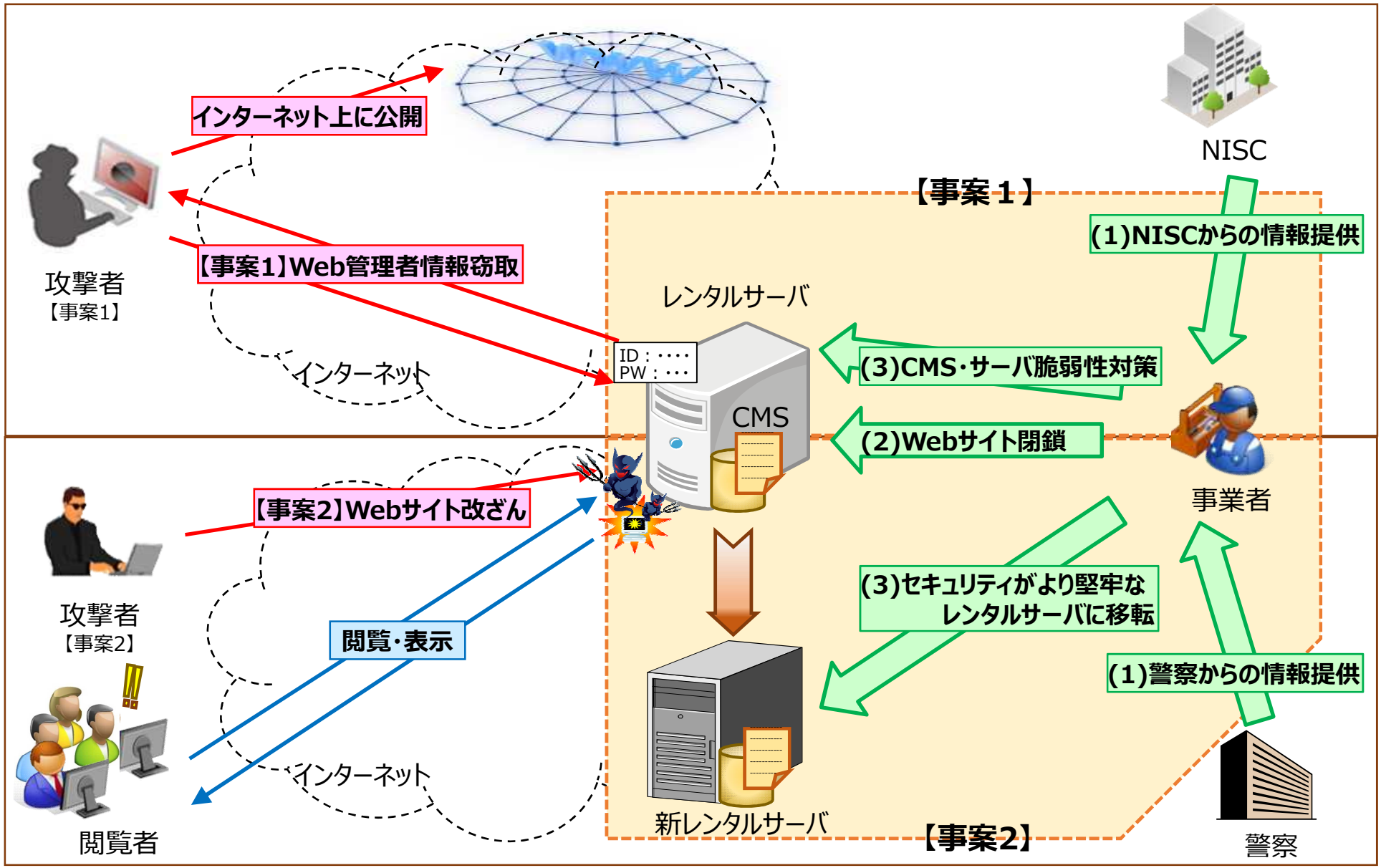
- 【事案１】NISC等からの情報提供により、IT担当部署の担当者がWeb管理者情報の窃取を認知。
- 【事案２】NISC等からの情報提供により、IT担当部署の担当者がWebサイトの改ざんを認知。

【対処】

- 【事案１/２】不正アクセスを認知後、事業者内セキュリティポリシーを踏まえ速やかに責任者に報告し、当日中にWebサイトを閉鎖。
- 【事案１】Web管理者情報を変更した上で、CMSやレンタルサーバの脆弱性対策を実施。
- 【事案２】Web管理者情報を変更した上で、セキュリティ向上を図るため別会社のレンタルサーバに移転。
- 【事案１/２】事案発生１週間以内にWebサイトを再開。

事例４　Webサイトへの不正アクセス　２／４

【事例のイメージ】



事例４　Webサイトへの不正アクセス　３／４

【原因】

- 【事案１】使用していたCMSが汎用的なものでなく独自仕様なので安全といった誤解もあり、脆弱性対策が不十分であった。
- 【事案２】CMS管理外のWebサイトが改ざんされており、レンタルサーバのセキュリティに問題ありと推定。
- 【事案１/２】IT担当部署の職員数の不足もあり事案対応に追われ、対外機関との間での情報共有が必ずしも十分でなかった。

【再発防止策】

＜短期的対策＞

- 【事案１】CMSやレンタルサーバの脆弱性情報を常に把握し、速やかに更新。
- 【事案１】レンタルサーバのアクセスログを定期的に確認し、不正アクセスを速やかに検知。
  ※（独）情報処理推進機構が提供するWebサイトの攻撃兆候検出ツール”iLogScanner”を使用。
- 【事案２】Webサイトの更新作業に際して、送信元を特定のIPアドレスに限定するなどセキュリティ対策を柔軟に適用できるレンタルサーバを利用。

＜中長期的対策＞

- 【事案１/２】事業者単独では対応できない事案も想定して、事案発生時におけるグループ会社のセキュリティ担当者間での連携を強化。
- 【事案１/２】平時から対外機関との間のセキュリティ情報に係る共有体制を把握。

事例４　Webサイトへの不正アクセス　　４／４

【得られた気付き・教訓】

- 外部委託契約におけるセキュリティ対策についての責任分界の確認
  （外部業者が対策してくれるという思い込みはせず、あらかじめ契約内容等を確認すべき。）
- 不正アクセス検出を目的としたサーバアクセスログ調査手順の確認
  （情報セキュリティ関係機関から検出ツールが公開されている。）
- Webサイト閉鎖を想定したサービス利用者向け情報伝達手段の確保
  （Webサイトの閉鎖期間が長期間に及ぶ場合、サービス利用者に対してどのように事業者発の情報を伝達するか、代替手段をあらかじめ決めておくことも有効。）
- 対外機関との情報共有体制の確認
  （平時から対外機関との間での情報共有体制を理解しておくことで、事案発生時における初動対応でも慌てずに連携を図ることができる。）
- 事業者内のIT担当部署におけるセキュリティ人材の育成・確保
  （平時から事業者内全体のセキュリティ意識の向上を図り、事案発生時に対応可能な人材の育成に努めるとともに、必要に応じ、例えばグループ会社のセキュリティ担当者間で相互協力が図れるよう取り決め等を結んでおくことも有効。）