資料10

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

2014年度 重要インフラにおける補完調査結果について

２０１５年３月２６日

内閣官房　内閣サイバーセキュリティセンター(NISC)

補完調査の目的・観点

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26年5月19日情報セキュリティ政策会議決定）

調査の実施方法

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。

調査対象の選定

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　Webサイト（トップページ）の改ざん
事例２　会員制サービスの不正ログイン
事例３　端末へのマルウェア感染　※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１　Webサイト（トップページ）の改ざん　　１／４

【発生事象の概要】

- Webサイトに対する不正アクセスにより、トップページが改ざんされた。
- 閲覧すると、攻撃者の主義主張を表す画像が表示され、更に別のWebサイトに誘導される。
- Webサイトを一時閉鎖後、改ざん箇所の修正と他への影響有無確認を実施して復旧。

【背景】

- Webサーバは外部の共用サーバ（ホスティングサービス）を利用。
- Webサイト自体の運用は事業者の広報担当者（IT担当部署ではない）が実施。
  （Webサイトの構築は外部委託したが、日々の運用・保守は外部委託せずに広報担当者が実施。）

【検知】

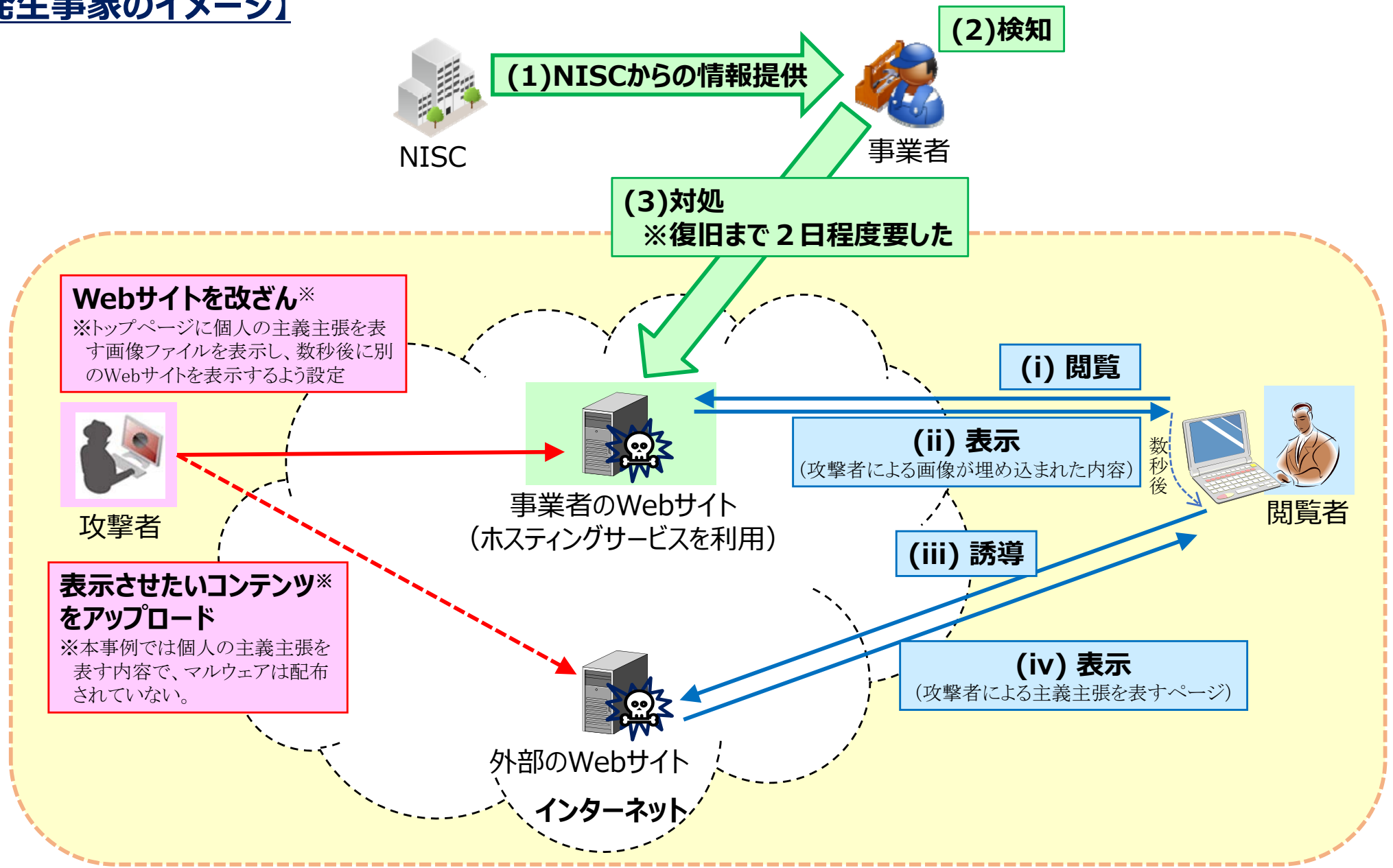
- NISCからの所管省庁を通じた情報提供により、IT担当部署の担当者がWebサイトの改ざんを認知。

【対処】

- 検知が深夜であり、また、ホスティングサービスの業者の応対時間外だったため、IT担当部署の担当者判断により、翌朝から対処を行った。
- 広報担当者がWebサイトの一時閉鎖作業に着手したが、トップページのみではなく、Webサイト全体を閉鎖する方法が容易に判明せず、作業に時間を要した（約半日）。
- 危機管理の責任者の指示により、Webサイトの一時閉鎖について報道発表を閉鎖当日中に実施。
- 危機管理の責任者の指示により、費用発生の如何に関わらず早期復旧すべき方針が示され、Webサイト構築時の業者と協力して復旧作業（作業用に一時閉鎖を部分解除／改ざん箇所を修正）を実施。
- その後、トップページ以外の全ページを目視により検査・確認し、Webサイトを再公開。

事例１　Webサイト（トップページ）の改ざん　２／４

【発生事象のイメージ】



事例１　Webサイト（トップページ）の改ざん　３／４

【原因】

- ホスティングサービスの契約内容にログ採取が含まれておらず、改ざん原因は特定できなかった。
- なお、状況から推測される原因は次のとおり。
  - ✓ 使用していたCMS※について、数年間更新しておらず、脆弱性があるバージョンを使用していた。
    ※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。
  - ✓ Webサイトを更新するためのソフトウェア（FTPクライアント）に脆弱性があるバージョンを使用していた。（パスワードを保持する設定としていたが、パスワード漏えいの脆弱性があった。）
  - ✓ パスワード（FTPパスワード）を運用開始以来、一度も変更していなかった。

【再発防止策】

- FTPパスワードを変更（推測されにくいようランダムな文字列を使用。）。
- 使用しているソフトウェアについては、パッチ適用等の脆弱性対策を実施。
- 専門知識を持った外部業者への運用委託を含めた、Webサイトの全面更改を検討・計画。
- Webサイト更改に当たり、情報セキュリティ対策の検討などに外部専門家（コンサルティング会社）を活用。

事例１　Webサイト（トップページ）の改ざん　　４／４

【得られた気づき・教訓】

- 夜間・休日対応のため、組織内外との連絡ルール、連絡手段及び役割分担の整理が重要。
  （担当者自身がどこまで判断してよいかを明確にしておく必要。）
- ホスティングサービス等の外部サービス利用時は、夜間・休日を含めた対応体制や、ログの取得といった障害発生時の対応の可否について確認が必要。
  （事業者自身が提供するサービスに照らして、それが十分であるかを併せて確認する。）
- Webサイトの改ざんに備えた、閉鎖のための判断基準や操作手順の整備が必要。
  （マルウェアが埋め込まれていた場合、閲覧者へのマルウェア感染拡大を防止する必要。）
- 復旧・稼働を優先する重要な業務・システムを整理し、それを組織内に定着しておくことが重要。
  （時間外勤務や外部委託等の費用発生をしてでも迅速に対応すべきものを確認。）
- 環境変化や時間経過に応じ、適切な予算措置や人材確保により情報セキュリティ対策を継続的に実施していくことが必要。
  （Webサイトの構築時だけではなく、維持するためにも、専門知識を持つ人材や費用が必要であり、IT担当部署だけでなく、経営層を含めた共通認識とする必要。）
- 情報セキュリティ事象について、報道発表を行う基準やその判断者を事前に決めておくことが必要。
  （不特定多数に影響のある事象については、迅速かつ正確な情報発信が重要。）

事例２　会員制サービスの不正ログイン　　１／４

【発生事象の概要】

- 複数の会員制サービスのサーバに対し、大量のログイン試行が行われた。
- 一部のログイン試行が成功し、個人情報を含む会員情報が閲覧された。
- サービスを一時停止し、不正ログインされたアカウントの凍結や監視強化等を措置。

【背景】

- 攻撃を受けた事業者は会員制サービスを複数運用。
- 各会員制サービスは、各担当部署（IT担当部署ではない）が原則として管理。
- 会員制サービスのログイン状況の監視は、一定時間ごとのログ監視により実施。

【検知】

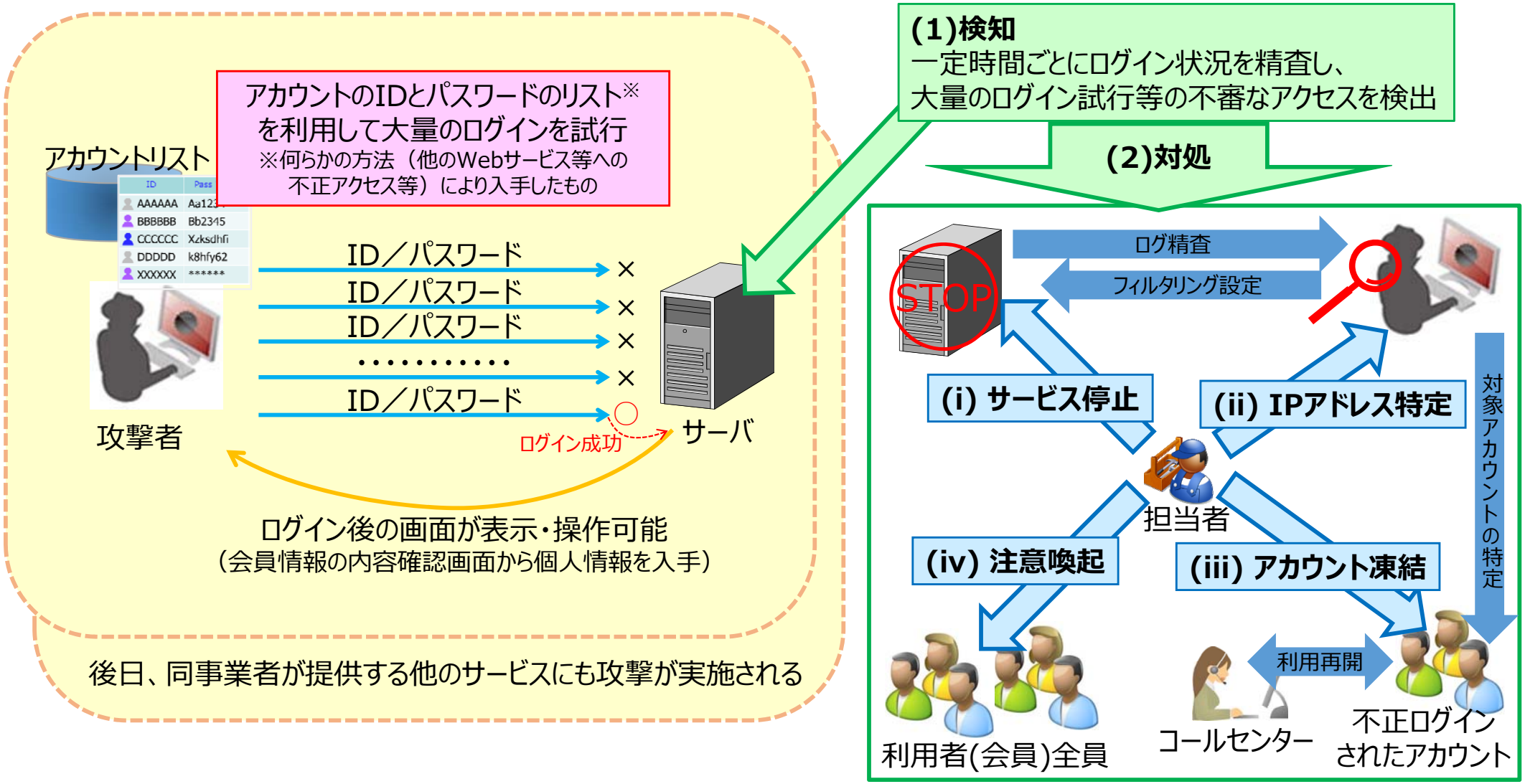
- 短時間に大量のログイン試行が行われたことが、ログ監視により検出され、担当部署へ通知。
- その後も、大量のログイン試行が、同一サービスだけでなく、他のサービスにおいても行われたことを確認。
  （管理状況の異なる他のサービスの監視体制を強化する前にログイン試行を受けた。）

【対処】

- 会員制サービスを一時停止。深夜であり担当者が駆けつけるまでに数時間を要した。
  （その後、24時間対応を実施している別の部署に停止作業を移管することで改善。）
- 一時停止中に、不審なIPアドレスを特定。通信の遮断（フィルタリング）等を実施後、サービス再開。
- 不正ログインされたアカウントを凍結し、電子メールにて連絡。再開手続きはコールセンターにより実施。
- サービスの会員全員に対して、電子メールでパスワード管理に関する注意喚起を行った。

事例２　会員制サービスの不正ログイン　２／４

【発生事象のイメージ】



事例２　会員制サービスの不正ログイン　３／４

【原因】

- 第三者によるアカウントリスト攻撃※と推定される

※アカウントリスト攻撃・・・IDとパスワードがセットになった「アカウントリスト」を元に不正ログインを試行する攻撃。アカウントリストは、何らかの方法（例：他のオンラインサービスへの不正アクセス）により事前に入手しておく。利用者がIDとパスワードをオンラインサービス間で使い回していると、攻撃が成功してしまう。

【再発防止策】

＜早期対策＞

- 大量アクセスに対する監視間隔の短縮による早期検知。　（例：日時→毎時、毎時→15分ごと）
- 大量ログイン試行の検知後、通信を遮断するまでのプロセスを自動化。

＜中長期対策＞

- ログイン画面に画像認証（CAPTCHA※）を追加。
  ※歪んだり崩れた文字列を表示させ、それを利用者に入力させることで、機械的な自動アクセスを防ぐ方法。
- ログイン後の画面や会員情報照会画面に個人情報を表示させず、閲覧・変更時は二重認証※を実施。
  ※本事例の場合においては、ID・パスワード以外に、個人情報の一部を認証項目として入力させることとしている。
- リスクベース認証※を実施。
  ※利用者のログイン環境（IPアドレス、使用パソコン、使用ブラウザ等）を総合的に分析し、普段と異なる環境からのアクセスと判断した場合に、追加的な認証を要求する方式。

事例２　会員制サービスの不正ログイン　４／４

【得られた気づき・教訓】

- 提供サービスのログを定期的に確認するとともに、異常となる閾値を決めておくことが重要。
  （確認するスキームがなければそもそも不正アクセスに気付くことすらできない。）
- 他事業者で発生した攻撃について、自サービスでの発生に備えた対応を実施することが重要。
  （アカウントリスト攻撃が発生しているのであれば、監視間隔を短くする等の措置が有効。）
- 攻撃情報や情報セキュリティ対策について、部署間やグループ会社間での情報共有が必要。
  （利用者から見れば一つの事業者として捉えられ、再発防止を全社的に取り組む必要。）
- 不正ログインの疑いがある場合の、サービス停止の判断基準の整備が必要。
  （不正ログインが続けば、個人情報の漏えいが拡大してしまうため迅速な対応が必要。）
- 夜間・休日における迅速なサービス停止のため、事業者内連携も含めた体制の確認が必要。
  （担当者が駆けつけるだけでなく、停止作業を他部署の担当者に移管する方法も有効。）

【得られた気づき・教訓（事業者による取組以外のもの）】

- 攻撃元の通信遮断に資するため、被攻撃事業者とISP事業者との情報共有枠組みが必要。
- 攻撃手法の事業者間での情報共有について、既存の各種法令の整理が必要。
  （アカウントリスト攻撃のアカウントリストの個人情報への該当性に留意が必要。）
- 利用者自身が、IDやパスワードを使いまわさないように心掛けることも必要。

事例３　端末へのマルウェア感染　　１／４

【発生事象の概要】

- マルウェア感染によるものと疑われる通信について、NISCから該当事業者へ情報提供を行った。
- 情報提供した内容を元に、事業者のIT管理部署が調査を実施。
- 感染の疑いがある端末を特定し、端末の初期化を行うとともに、部署内で情報共有を行った。

【背景】

- 部署ごとに別の業務システムを有しており、それぞれ別のファイヤーウォールを通してインターネットに接続。
- マルウェア感染が疑われた業務システムは、複数の下部組織が使用。下部組織ごとに管理者がおり、独立した管理が行われている。また、外部から下部組織内への接続は行えない設定※となっている。
  ※NAT変換（ネットワークアドレス変換）を行い下部組織内のネットワークが当該下部組織の外からは隠蔽されている。

【検知】

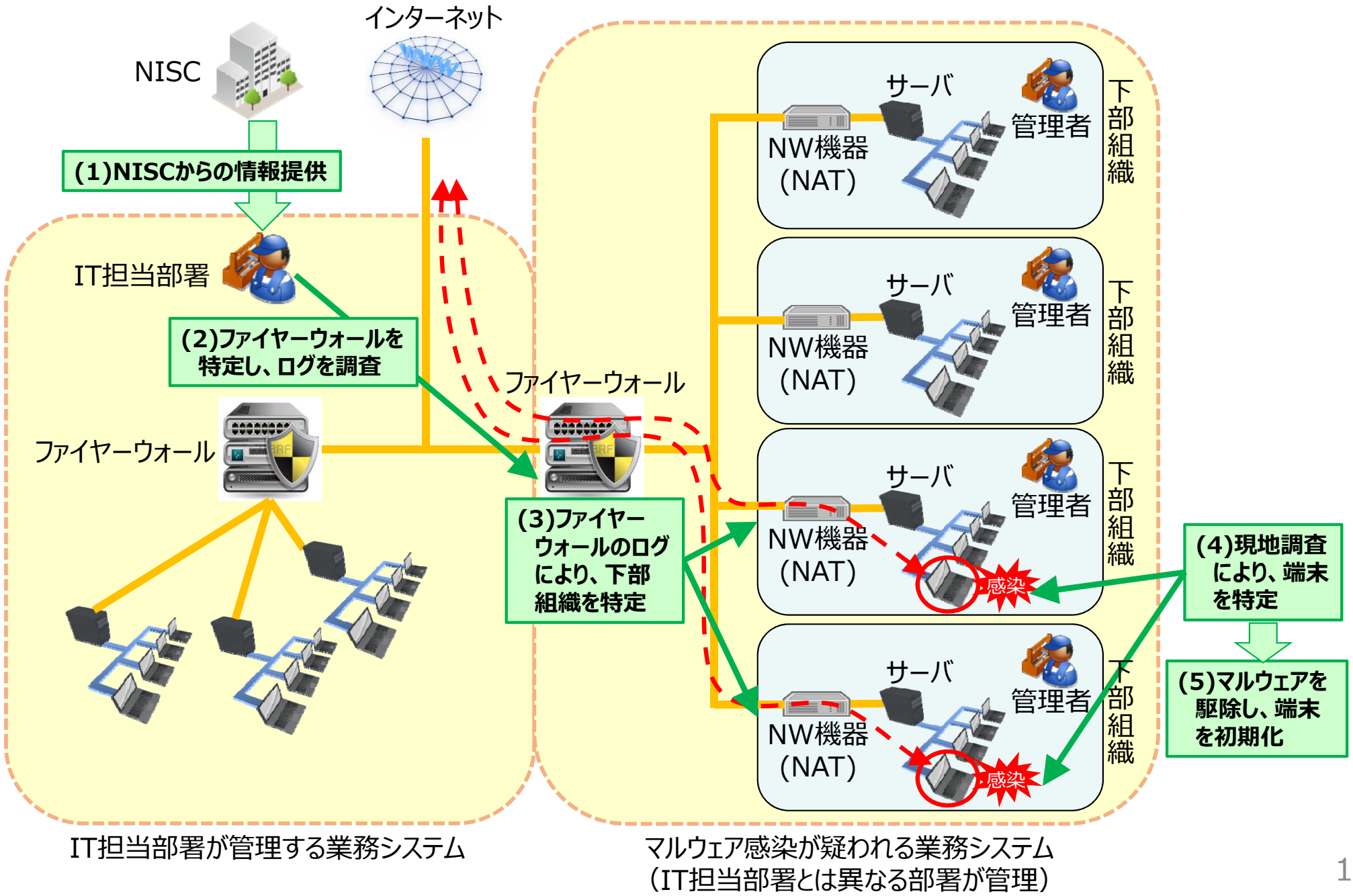
- NISCからの所管省庁を通じた情報提供により、IT担当部署の担当者がマルウェア感染の疑いを認知。

【対処】

- 情報提供の内容（IPアドレス）から、該当のファイヤーウォールを特定し、該当部署に連絡を実施。
- IT担当部署でファイアウォールのログを調査し、マルウェア感染の疑いのある複数の下部組織を特定した。
- 該当の下部組織に対してそれぞれ連絡を行い、現地にて端末の調査を実施。
- マルウェア駆除ツールを使用し、マルウェアによるものと疑われる通信の停止を確認。端末の初期化も実施。
- 各部署の責任者間、各下部組織の責任者間、及び各下部組織の管理者間において、情報を共有した。

事例３　端末へのマルウェア感染　２／４

【発生事象のイメージ】



事例３　端末へのマルウェア感染　３／４

【原因】

- ウィルス対策ソフトの設定について、調達時の仕様書に十分な内容が記載されていない等の理由により、定義ファイルの更新や定期的なスキャンが行われていない端末が存在した。
- マルウェア感染が疑われた業務システムは、下部組織ごとの管理者が管理しているものの、業務システム全体としての管理状況の把握が十分に行われていなかった。
- 端末利用者に対して情報セキュリティ研修を行っていないなど、情報セキュリティ意識が不十分であった。

【再発防止策】

＜早期対策＞

- 該当業務システム配下の全端末について、定義ファイルの更新と定期的なスキャンの設定※を実施。
  ※定期スキャンの設定時刻経過後に電源を入れた場合には、電源投入時に定期スキャンを実施するよう確実な設定を実施。
- ウィルス対策ソフトがマルウェアを検知した場合、IT担当部署の管理者に、電子メールで通知するよう設定。

＜中長期対策＞

- 業務システム内のネットワーク管理については、下部組織ごとではなく、部署として統一的な管理を実施。
- 調達仕様書のひな形の作成や運用手順等の明確化を行い、部署内での調達・運用管理を統一化。
- 情報セキュリティに関する従業員・職員研修を定期的に実施。
- IT担当部署（情報セキュリティ担当）の増強を実施。

事例３　端末へのマルウェア感染　　４／４

【得られた気づき・教訓】

- 事業者全体の情報セキュリティ意識の向上のためには、経営層から意識付けを始める必要。
- 情報セキュリティ対策を、事業者内、部署内で統一することが重要。
  （下部組織ごとに責任者が管理している場合でも横串を通して管理することが重要。）
- 運用ルールの統一には、調達仕様書のひな形作成や、運用手順のマニュアル化が有効。
- 統一的な管理には、情報セキュリティ教育を受けた者を管理者とし、上位の組織から横串を通して行うことが必要。
  （情報セキュリティを確保するためには一定の専門知識が必要で、人数も限られる。）、
- 端末利用者の情報セキュリティ意識向上のために、定期的な情報セキュリティ教育が必要。
- 事後的な原因調査のため、ファイヤーウォール等のネットワーク機器でのログ取得が重要。