資料４

NISC National Information Security Center

2012年度　重要インフラにおける「補完調査」について

2013年6月20日

内閣官房情報セキュリティセンター（NISC）

１．　補完調査の目的・観点

目的・スタンス

○第２次行動計画で期待される結果（アウトカム）の評価をより実態に即するようにするためには、指標では捉えられない側面を補完的に調査することが必要であり、IT障害等の事例を調査し、評価の材料を得る。

○検証にあたり、所管省庁及び重要インフラ事業者等の協力（情報提供・ヒアリングの実施等）を得るに当たっては、検証に協力した事業者等に不利益が生じないよう必要な配慮を行う。

検証の観点

○目的・スタンスに照らして、以下の点について検証を行う。なお、重要インフラ事業者等が「安全基準等」により具体的に対応することが望まれる課題については、「指針及び対策編」見直しの取組に反映させる。

・ＩＴ障害の未然防止、拡大防止、早期復旧のために実際にどのような対処が行われたか。
・安全基準等は、被害の発生防止、拡大防止に関し、十分なものであったか。
・官民の情報共有体制、セプター等による事業者間での情報共有が、具体的にどのように機能したか。
・他の事業者等から受けた影響、あるいは他の事業者等へ与えた影響はあったか。
・その他、被害の未然防止、拡大防止、早期復旧の観点から得られた教訓はあるか。

２．今年度の補完調査対象事例

検証の対象とする事例

実際に発生した「ＩＴ障害」及びＩＴ障害の要因となり得る「脅威」について、類似事例の発生状況（可能性）や社会的影響（関心）の大きさを考慮して以下の事例を選定した。

No.	事　例	脅　威
事例1	政府機関職員を詐称した不審メールの大量送付	①サイバー攻撃をはじめとする意図的要因
事例2	閲覧者へのウィルス感染を意図したWebサイトの改ざん	①サイバー攻撃をはじめとする意図的要因
事例3	閲覧者へのウィルス感染を意図したWebサイトの改ざん	①サイバー攻撃をはじめとする意図的要因
事例4	通信会社における国際通話のシステム障害	②非意図的要因

3. 事例１（政府機関職員を詐称した不審メールの大量送付）

事例１
政府機関職員を詐称した不審メールが大量に送信された事例を検証。

事象の概要

（１）政府機関職員のメールアドレスを詐称した不審メール（２種類）が大量に送信。

（２）不審メールの総数は、３９，８４２通（※１）
うち、政府機関　　：８，０５０通（２０．１％）
地方自治体　　：　６１８通（　１．５％）
重要インフラ事業者　：　２７８通（　０．７％）（※２）

（※１）ドメインベースで送信が確認されたもの。送信先アドレスの実在の有無及び当該ドメインの存続の有無は未確認。
（※２）すべての重要インフラ事業者を網羅しているとは限らない。

（３）１組織に複数（数通から千通程度まで）の不審メールが送信されるケースあり。

（４）ある組織のサーバが攻撃者に乗っ取られ、海外のサーバ経由で、当該サーバを踏み台にして不審メールが送信。

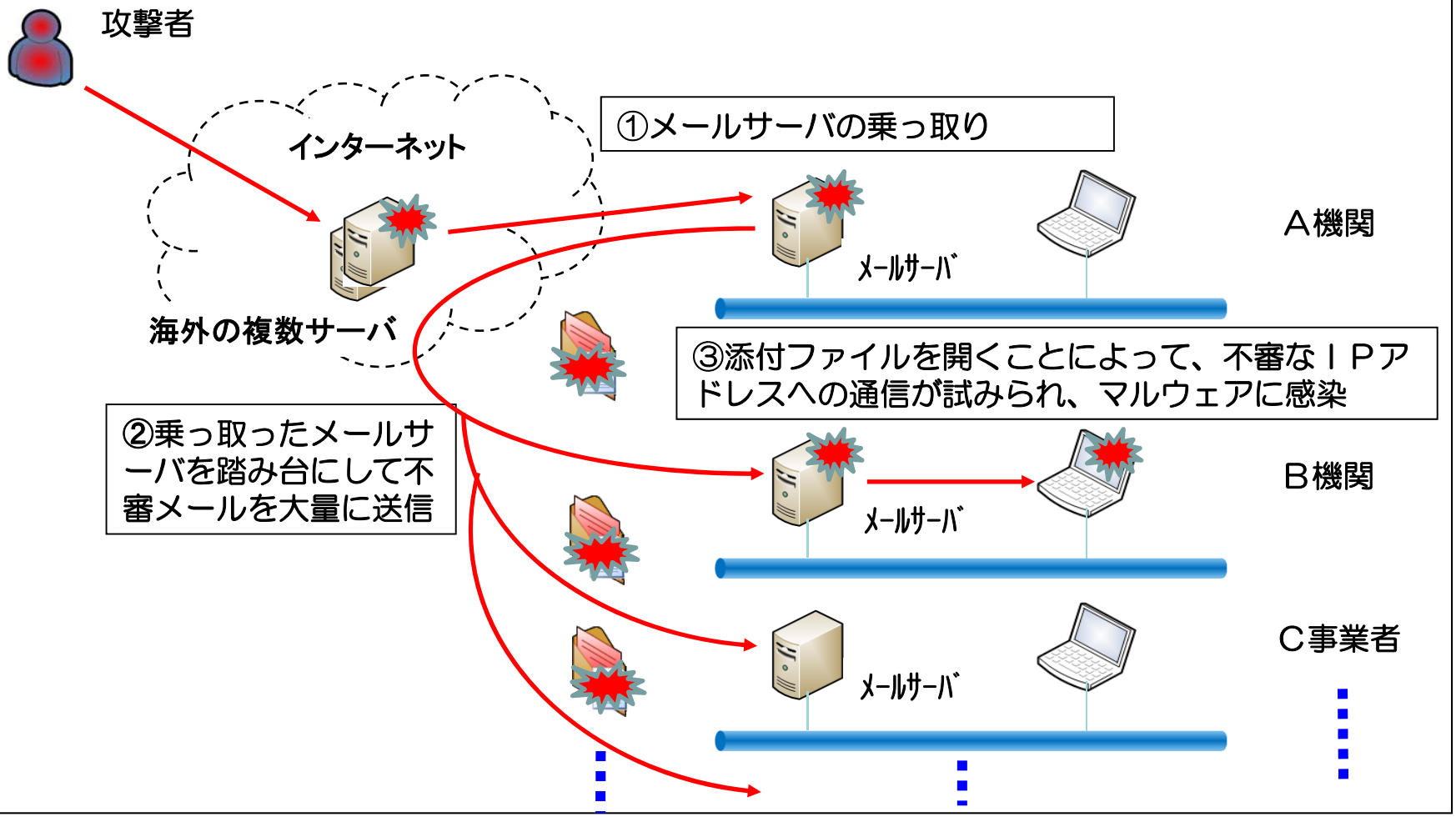
（５）メールに添付されたファイルを開くと不審なＩＰアドレスへの通信が試みられ、マルウェアに感染。

（６）送信先となっているメールアドレスの中には、ホームページ等での意見募集や問い合わせの際の宛先が用いられていると推測される例が存在。

（７）今回の事例で判明した送信先リストの他に、同様のリストが他にも存在する可能性高し。

4. 事例１（政府機関職員を詐称した不審メールの大量送付）

事象のイメージ図



5. 事例１（政府機関職員を詐称した不審メールの大量送付）

対応状況

（１）政府機関のホームページにおいて、国民に対して注意喚起を行うとともに、報道関係者にも周知。

（２）詐称されたメールアドレスを拒否設定するとともに、内閣官房情報セキュリティセンターにも報告。

再発防止策・課題等

（１）メールアドレスを掲載しているホームページを差し替え。

（２）メールアドレスの詐称防止のために、各組織のＷｅｂ掲載担当者に対して、ホームページにおいてはメールアドレス掲載を禁止していることを再周知。

（３）各組織のWeb掲載担当者を含む職員全員に、基本的な情報セキュリティ対策に関する注意喚起を繰り返し実施していくことが重要であることを、再認識。

6. 事例１（政府機関職員を詐称した不審メールの大量送付）

得られた気づき・教訓

（１）送信先となっているメールアドレスの中には、意見募集や問い合わせの際の宛先が用いられていると推測される例が存在。外部からのメールを受信する職員だけでなく、システム管理者も公表しているメールアドレスを認識し、外部から不審メールが送信されてくることを前提として情報セキュリティ対策を講じる必要があるのではないか。

（２）今回の事例で判明したリストは送信先リストの一例に過ぎないが、このようなリストが他にも存在する可能性は高く、またこれらのリストが攻撃者の間で繰り返し用いられている可能性も否定できない。
　一度、不審メールを受信した経験のある機関・事業者等には、今後も他の不審メールが到来する可能性があることを認識して、「もう来ないだろう」などと高をくくらないで、常に情報セキュリティ対策をチェックする必要があるのではないか。

（３）今回の事例のように同時に大量の不審メールが送信されるケースに対しては、不審メールが来ていることに気づいた人・組織がいち早く他の人・組織にも連携するなどして、不審メール情報を共有し、被害の拡大を止めることが対策として有効ではないか。

7. 事例2（閲覧者へのウィルス感染を意図したWebサイトの改ざん）

事例２
閲覧者へのウィルス感染を意図したWebサイトの改ざん事例を検証。

事象の概要

（１）事業者のWebサイトにおいて、第三者による改ざんがなされていることが判明。

（２）当該にWebサイトにアクセスし、ある箇所にカーソルを合わせると、悪意あるWebサイトに誘導され、ウイルスがダウンロード。

（３）改ざんされた当該Webサイトへの総アクセス件数は約７千件。ウイルスに感染したとの報告なし。

原因・対応状況

（１）改ざんされた原因は以下と考えられる。

①ＣＭＳ（Contents Management System）そのものに脆弱性が存在し、バージョンアップも行っていなかったこと

②編集者ＩＤのパスワードが推測されやすいものであったこと

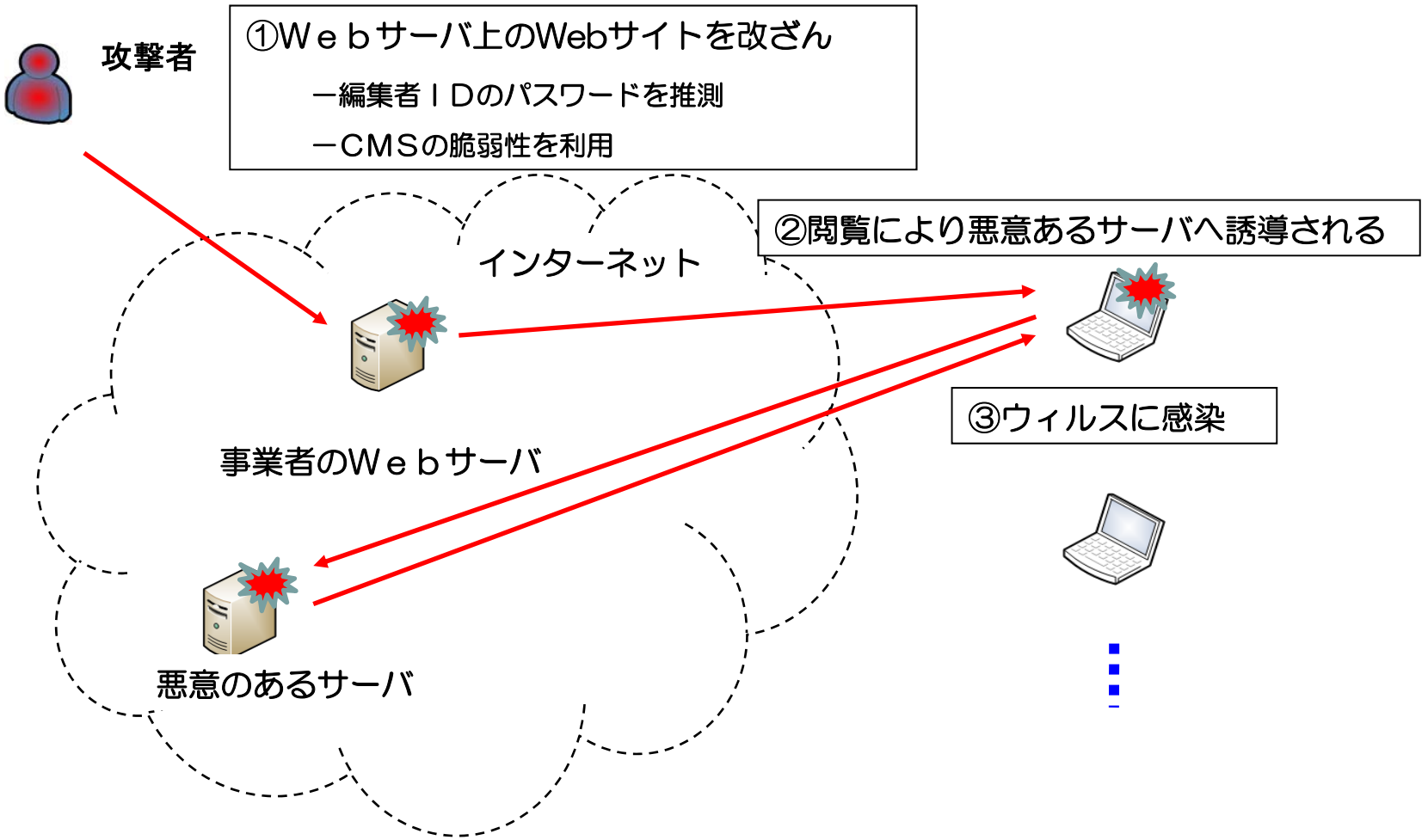
（２）不正プログラムの削除、ＣＭＳのバージョンアップ、編集者ＩＤのパスワード変更の後、Webサイトを一旦再開したが、警察の指導により閉鎖。

（３）Webサイトを開くと、表面上は全く分からないが、見えない形で悪意のあるWebサイトに誘導され、そのWebサイトからウィルス感染する恐れがあること、また、Webサイトにアクセスしてしまった場合は、ＯＳや各種プログラム、ウィルス対策ソフトのバージョンが最新であるかを確認した上で、ウィルスチェック行う必要があることを公表。

（４）事業者が独自で管理・運用するサーバに、 Webサイトを新規構築して再開。

8. 事例2（閲覧者へのウィルス感染を意図したWebサイトの改ざん）

事象のイメージ図



9. 事例2（閲覧者へのウィルス感染を意図したWebサイトの改ざん）

再発防止策・課題等

当該Webサイトは、事象発生まで、ホスティングサービス会社に委託して運用していたが、事業者が独自で管理・運用するサーバにWebサイトを新規構築し、速やかにソフトウェアのバージョンアップができる体制にした。

得られた気づき・教訓

（１）委託先(大手通信会社)のホスティングサービスについては、最低限のセキュリティ対策しか提供されていないため、セキュリティ対策を高めるためにはオプション契約を結ぶ必要があったが、事業者は大手通信会社の名前を過信してしまったことにより、基本契約のみとしたこと、セキュリティ対策不足のみが事象の原因ではないが、システム導入時の業者選定基準が低かったこと等から、外部委託契約の内容等をあらかじめ確認すること。

（２）ソフトウェアのバージョンアップは速やかに実施し、少なくとも既知の脆弱性がない状態を保つこと。
　ホスティング環境などで直接サーバの管理ができない場合は、ホスティング事業者にサーバの脆弱性への対処ポリシーをあらかじめ確認しておくこと。

（３）編集者ＩＤのパスワードは容易に推測されにくいものにすること。

（４）編集権限でサーバにアクセスできる端末を制限するために、ＩＰアドレスによるアクセス制限を行うこと。

10. 事例3(閲覧者へのウィルス感染を意図したWebサイトの改ざん)

事例3

閲覧者へのウィルス感染を意図したWebサイトの改ざん事例を検証

【概　要】

○　事業者が管理するCMS型Webサイトのサーバにおいて不正侵入による改ざんが発生、当該サーバは20超の団体等のWebサイトで利用されていたため、傘下のWebサイト全体で意図しないURLへ誘導されるなどの障害が発生。

○　所要の対策を講じ、Webサイトを再開したが約３週間後に再び改ざんが発生。

【１回目の改ざん】

Webページで利用しているJavaScriptが改ざんされ、トップページにアクセスすると、不正サイトへ誘導される事象が発生。警察本部との現状報告会議を設置。

以下の作業を実施し、復旧までの対応を実施。

・サーバの再構築
・ペネトレーションテスト(侵入)用サーバの構築
・CMSのバージョンアップ
・改ざん前のデータ移行
・ペネトレーションテスト
・侵入検知機能の有効化

作業終了後、問題ないことを確認し、事業者内の関係者の会議を設置し、現状を報告。

11．事例3(閲覧者へのウィルス感染を意図したWebサイトの改ざん)

事例３

閲覧者へのウィルス感染を意図したWebサイトの改ざん事例を検証

【２回目の改ざん】

１回目と同様に、トップページに接続すると、不正サイトへ誘導される事象が発生。

以下の作業を実施し、復旧までの対応を行った。

・以前より埋め込まれていたバックドアプログラムの削除
・サーバ構成を再検討し、新サーバを構築（外部サーバ、内部サーバに分けた複数台構成）
・最新パッチの適用
・コンテンツの移行及び確認
・アクセス権限の修正（外部からは閲覧専用）
・ペネストレーションテスト
・侵入検知機能の有効化
・監視機能の有効化

作業終了後、問題ないことを確認し、Webサイトを再開。

12. 事例3(閲覧者へのウィルス感染を意図したWebサイトの改ざん)

事例３

閲覧者へのウィルス感染を意図したWebサイトの改ざん事例を検証

【原　因】

【１回目の改ざん】

CMSが脆弱性のあるバージョンだったため、脆弱性を突かれバックドアプログラムがWebサイトに埋め込まれたため。これにより、バックドアプログラムが実行されJavaScriptが書き換えられ、Webサイトが改ざんされることとなった。

【２回目の改ざん】

初回対応時に改ざん前のデータを移行する際に、ウイルススキャンを実行したが、ウイルスとして検知されなかった。さらに不可視ファイルとなっており、巧妙に隠されていたため、バックドアプログラムも戻されてしまった。これにより、バックドアプログラムが実行されJavaScriptが書き換えられ、Webサイトが改ざんされることとなった。

※補足説明※

バックドアプログラムは、不可視ファイル（「.(ドット)」から始まるファイル名）となっており、巧妙に隠されていたため、１回目の改ざんでの対処では見落としてしまった。

13. 事例3(閲覧者へのウィルス感染を意図したWebサイトの改ざん)

【再発防止含めた対応策】

・サーバの書き換えを防ぐために、公開系サーバと更新系サーバを分け、外部からの接続は、参照用の公開系サーバのみの接続に変更。

・監視用サーバを設置し、更新ファイルを検知する改ざん検知システムを導入。

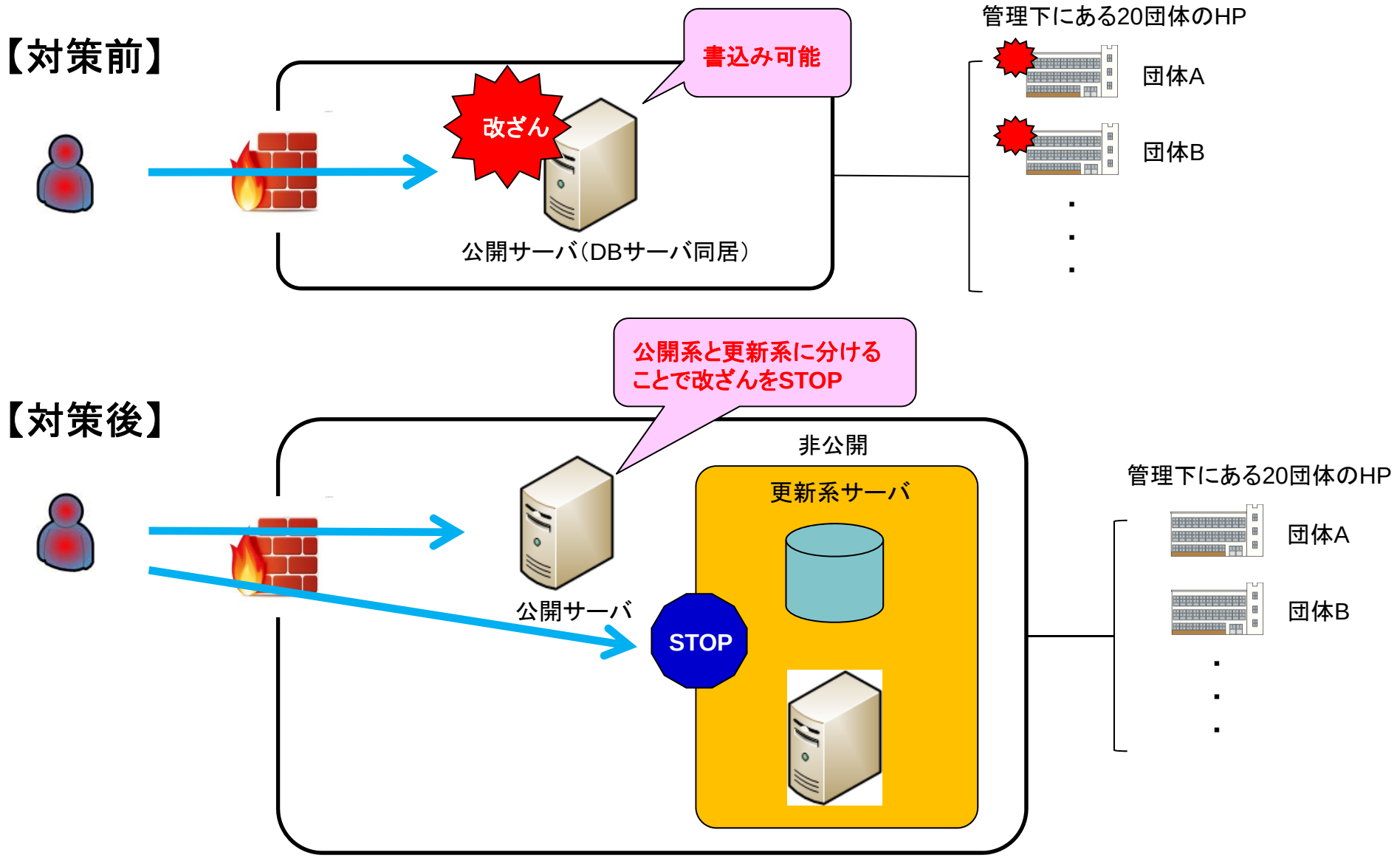
・Webページの編集権限を、内部からの特定端末のみに限定。

・サーバへのパッチ適用を即時対応可能な体制に変更。

・セキュリティ意識向上のため、定期的なセキュリティ研修の実施。

14. 事例３(閲覧者へのウィルス感染を意図したWebサイトの改ざん)

概要イメージ



15. 事例3(閲覧者へのウィルス感染を意図したWebサイトの改ざん)

【得られた気づき・教訓】

・バックドアプログラムは、１回目の改ざんが発見される約１か月前に仕掛けられたものであり、しかも１か月間何も動作していなかった。当該プログラムは、初回対応時にデータ移行を行う際に、一緒に移行されてしまったものであり、ウィルスチェックでも検出されていないことなどから、改ざんされた後に、データを戻す際は、バックドアプログラムが仕掛けられていないかの確認、ファイル形式の変換を行うなど、適切な対策を講じることが必要。

＊バックドアプログラムへの接続には、パスワードが求められるようになっているが、攻撃者以外は接続できないものとなっていた。

・サーバのOS、アプリケーションを常に最新のバージョンにしておくこと。
個別開発のアプリケーションがある場合は、最新のバージョンで動作するか確認を行うこと。

・ウィルス対策ソフトを常に最新にし、コンテンツが感染していないかどうか全ファイルのチェックを行うこと。

・定期的に、勉強会などを通して、セキュリティ意識の向上を図ること。

・被害が発生した際の復旧手順及び緊急連絡体制を確立しておくこと。

16. 事例４(通信会社における国際通話のシステム障害)

事例4

通信会社における国際通話のシステム障害事例を検証

【概　要】

　国内の携帯電話網と海外の携帯電話網を繋ぐ共通信号中継装置と国際交換機の間で、輻輳が発生したため国際共通線網を経由した国際ローミングサービスが利用しづらい事象に陥った。
　また国内の携帯電話網内のサービス制御装置が故障したことにより、共通信号中継装置からの要求信号が滞りやすくなり、信号処理を行う機能が大幅に低下し、国内の携帯電話の通信サービスが利用しづらい事象に陥った。

【原　因】

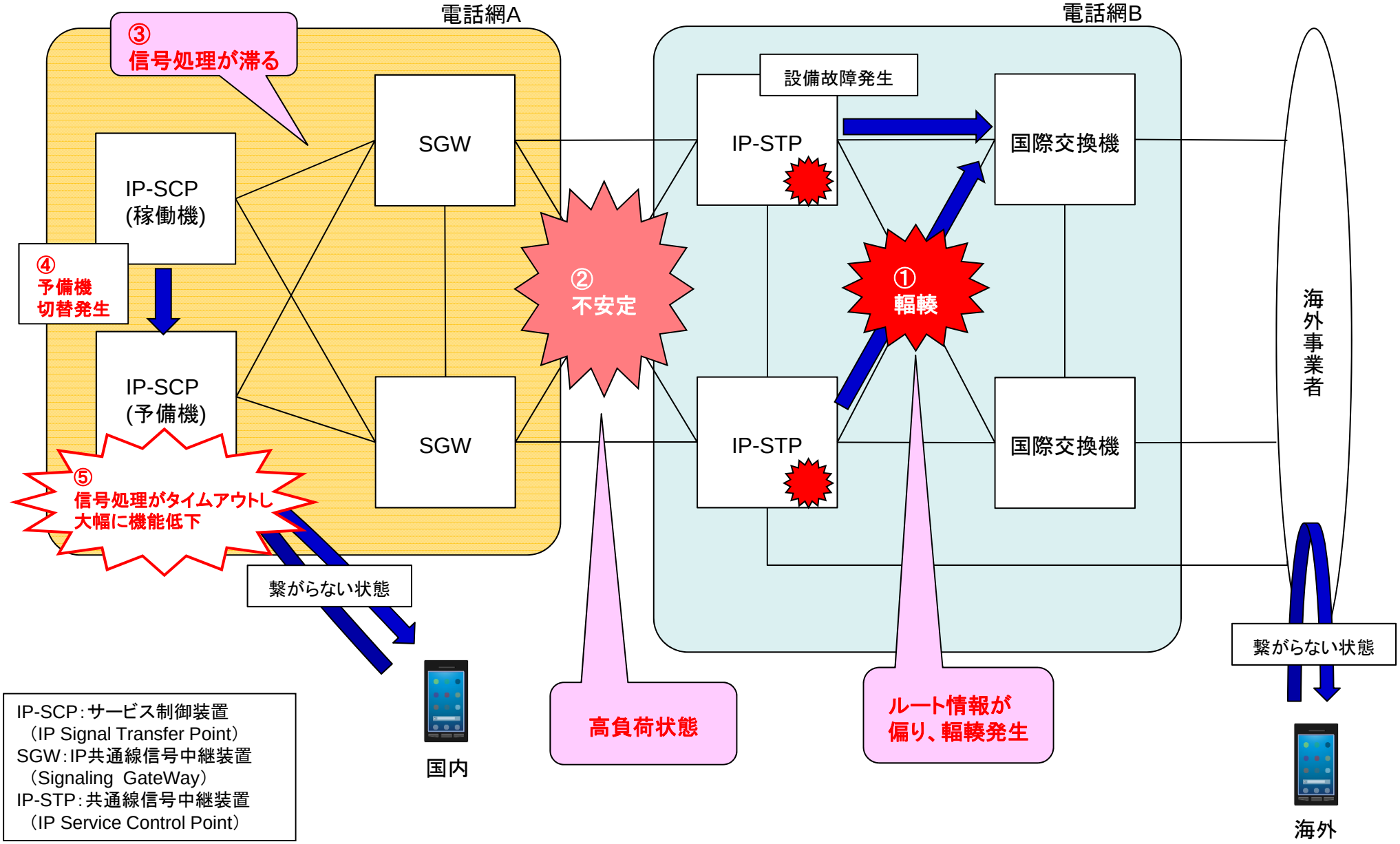
　国内と海外を結ぶルート情報の設定に誤りがあり、共通信号中継装置が故障した際に、トラヒックが偏ってしまい、輻輳が発生したため。これにより国際ローミングが利用しづらい状況となった。
　また国内の携帯電話網内のサービス制御装置が故障し、要求信号がタイムアウトした際に解放処理に時間がかかり、信号処理に間に合わなかったため。これにより国内の携帯電話も利用しづらい状況となった。

【対　応】

暫定対処として、データのトラヒック制限を実施し、順次トラフィック制限を解除することで、サービスを回復した。根本対処として、以下を実施。
・ルート情報の設定変更を実施し、トラヒック流用の平準化
・要求信号がタイムアウトした際、即時に解放処理できるよう見直し

17．事例４(通信会社における国際通話のシステム障害)

概要イメージ



18. 事例４(通信会社における国際通話のシステム障害)

【再発防止策・課題等】

- 携帯電話網の事業者が分かれているため、相互連携、情報共有、定期会合を実施。
- 緊急時における容量拡大に向けた対策を実施。
- 使用率を監視し、閾値を超えた場合の緊急体制の確立。

【得られた気づき・教訓】

- 複数の事業者がサービスの運用に係る場合、責任境界線及び作業範囲を明確にしておくこと。
- 通常時におけるデータの流れ、障害時におけるデータの流れを相互に各事業者が理解するとともに、ルート情報含めた各種情報を設定するに至る業務フローの手順書を整備する。
- 各種設定変更作業を実施する場合は、事前検証を行い、何かあった場合に備えて復旧手順を確立しておくこと。また作業終了後は、手順書の見直しを行うこと。
- サービスを提供する事業者は、全体のとりまとめを行うとともに、緊急時における体制を確立しておくこと。