資料４

NISC National Information Security Center

２０１３年度　重要インフラにおける「補完調査」について

２０１４年３月１１日
内閣官房情報セキュリティセンター（NISC）

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」見直しの取り組みに反映させる。

・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

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	認証ＩＤ・パスワードの外部漏えい	サイバー攻撃をはじめとする意図的要因
事例２	複数Ｗｅｂサイトの改ざん	サイバー攻撃をはじめとする意図的要因
事例３	複数回にわたるＷｅｂサイト遅延障害	サイバー攻撃をはじめとする意図的要因

事例１（認証ＩＤ・パスワードの外部漏えい）　１／４

【概　要】

- 事業者が管理する会員制サイトのサーバに対する不正アクセスにより、当該サイトへログインするための認証ＩＤと暗号化されたパスワードが外部に漏えいした。
- 監視強化中に再び不正アクセスを検知したため、関連する全システムの稼働を停止するとともに当該会員制サイトのサービス提供を停止。サーバを再構築したうえでサービスを再開した。

＜１回目の不正アクセス＞

当該サーバで利用しているミドルウェアにおける脆弱性について、情報セキュリティ関係機関が注意喚起を実施。

それを受けた当該事業者は、パッチの適用について検討を開始するとともに、暫定的なセキュリティ対策を実施したうえで、当該対策を実施するまでの間に不正アクセス等がなかったかについてログ等の確認作業を実施。

確認作業の結果、不正アクセスにより認証ＩＤと暗号化されたパスワードが収集された痕跡を確認。

＜２回目の不正アクセス＞

数日後、セキュリティ監視を強化しているなかで、新たな不正アクセスを検知。

当該不正アクセスは、１回目の不正アクセス時に設置されたバックドアプログラムに起因する不正アクセスと判明。

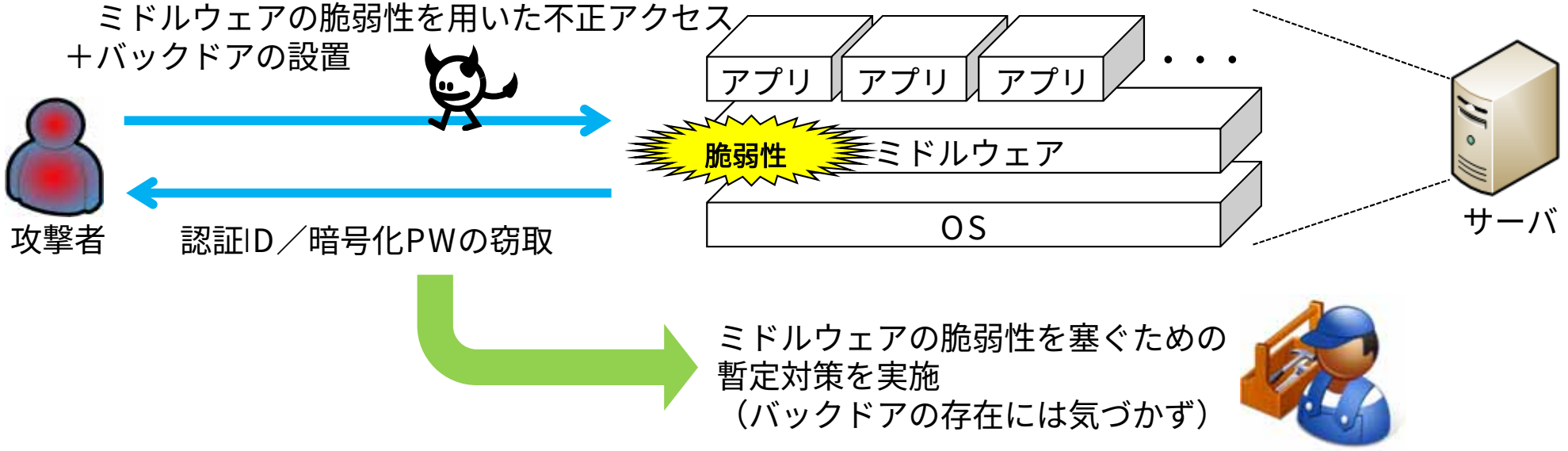
関連する全てのシステムの稼働を直ちに停止させ、新たな情報漏えいを未然に防止。

その後、サーバを再構築（当該ミドルウェアのパッチは適用済）し、新たなセキュリティ監視装置（ＷＡＦ）を導入したうえでサービスを再開。

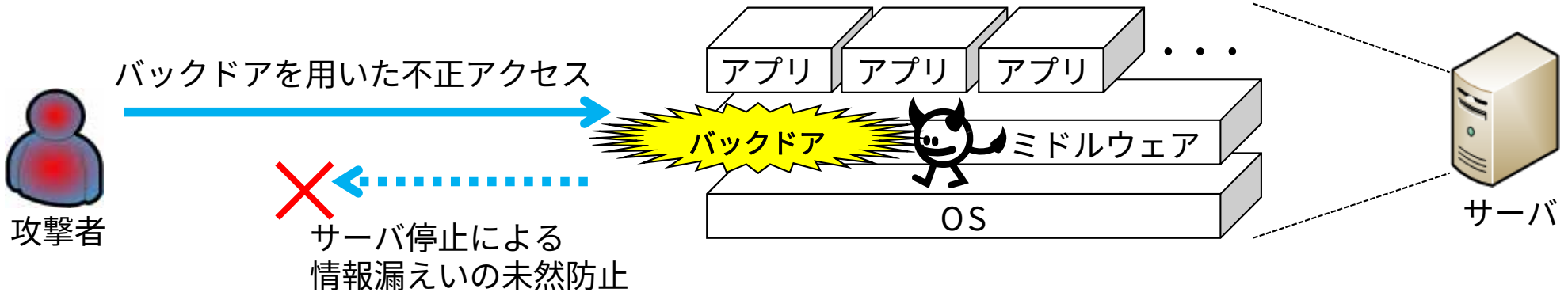
事例１（認証ＩＤ・パスワードの外部漏えい）　２／４

【事象のイメージ】

＜１回目の不正アクセス＞



＜２回目の不正アクセス＞



事例１（認証ＩＤ・パスワードの外部漏えい）　３／４

【原　因】

＜１回目の不正アクセス＞

- 当該サーバで利用しているミドルウェアにおける脆弱性を悪用した不正アクセスであったが、開発元が当該脆弱性のパッチを公開し、情報セキュリティ関係機関が注意喚起を行うまでの間に攻撃が発生した。
- 脆弱性に対するパッチについて、当該ミドルウェア上で動作する各種アプリケーションの動作を確認する必要があるため、直ちにパッチを適用できない状況であった。

＜２回目の不正アクセス＞

- １回目の不正アクセスの際に、サーバ上の、通常では発見しづらい箇所にバックドアプログラムが設置されていた。

事例１（認証ＩＤ・パスワードの外部漏えい）　４／４

【再発防止】

- 高度な攻撃を検知・自動ブロックするためのセキュリティ監視装置を導入。
- ユーザに対し、認証パスワードの再設定の必要性を周知。
- 社内のシステムを洗い出し、脆弱性対応を一元化できる仕組みを導入。
- 脆弱性の重要度に対する対応目安日数を設定し、対応状況をシステムで管理。
- 情報セキュリティ事案に対する全社的な緊急対応体制※を新たに整備し、その体制に基づく訓練を実施。

※ ＩＴ障害発生時に、社内の対策本部を立ち上げる基準や手順等

【得られた気づき・教訓】

- パッチ適用など根本対処が直ちにできない場合は、不正アクセスの監視強化などの暫定対処を行う。
- 脆弱性への対応を迅速に行うために、平時からシステムで利用されているソフトウェアを把握する。
- 脆弱性情報を重要度に応じて、その対応状況を含めて管理し組織内で迅速に情報共有を行う。
- 情報セキュリティ事案に対する緊急対応体制を平時から準備し、その対応を訓練する。
- 不正アクセスされた場合は、情報漏えいの可能性だけでなく、2次被害としてバックドアプログラムの設置の可能性を想定し、隠しファイルの確認を含めた対応を行う。

事例２（複数Ｗｅｂサイトの改ざん）　１／４

【概　要】

- 本事業者は複数のWebサイトを有しており、その一部はIT担当部署以外の担当部署が管理をしている。
- ある担当部署が管理する一部のWebサイトに対する不正アクセスにより、当該Webサイトが書き替えられ外部のWebサイトへの不正な誘導（リダイレクト）が発生。
- さらに、上記のインシデント対応中に別の担当部署が管理するWebサイトに対しても不正アクセスにより、当該Webサイトが書き替えられるインシデントが発生した。

＜１件目のインシデント案件＞

事業者の職員が利用している端末に導入されているウィルス対策ソフトがウィルスを検知。ウィルスについて調査したところ、IT担当部署以外の担当部署で管理しているWebサイトにアクセスしたことによるものと特定。

報道発表を行うとともに、当該Webサイトを閉鎖し、IT担当部署が管理をしているメインのWebサイトにおいて利用者への周知を実施。

その後、コンテンツの見直しを行い、メインのWebサイトに統合済。

＜２件目のインシデント案件＞

1件目のインシデント案件と同じ週に、別の担当部署が管理するWebサイトの一部を閲覧出来ない事象を職員が発見。当該Webサイトの保守業者に連絡を取り調査を行ったが、ウィルス対策ソフトでは検知されず、原因の特定に至らなかった。

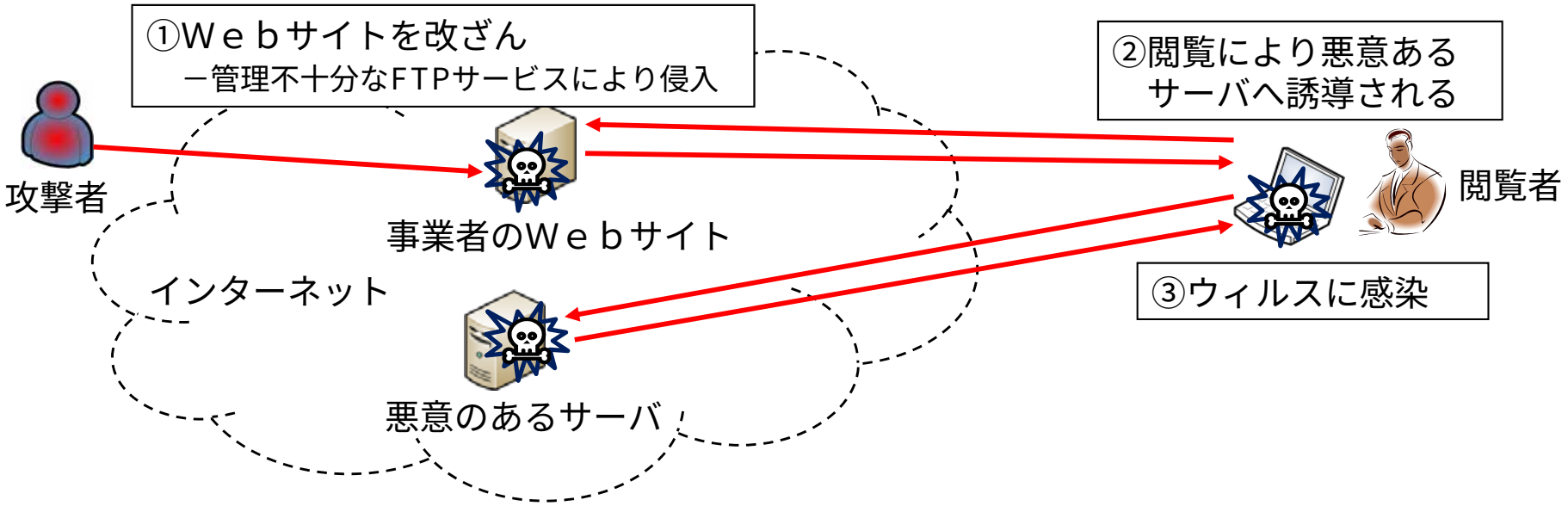
しかし、不正アクセスによる改ざんを疑い担当部署の判断で当該Webサイトを閉鎖。ウィルス対策ベンダに調査を依頼したところ新種のウィルスであり、 Webサイトへの不正アクセスによりウィルスを混入されていたことが確認できたため、報道発表を行うともに、IT担当部署が管理をしているメインのWebサイトにおいて利用者への周知を実施。

その後、Webサイトの脆弱性調査を行い、多数の脆弱性を確認し、対応後にWebサイトを再開。

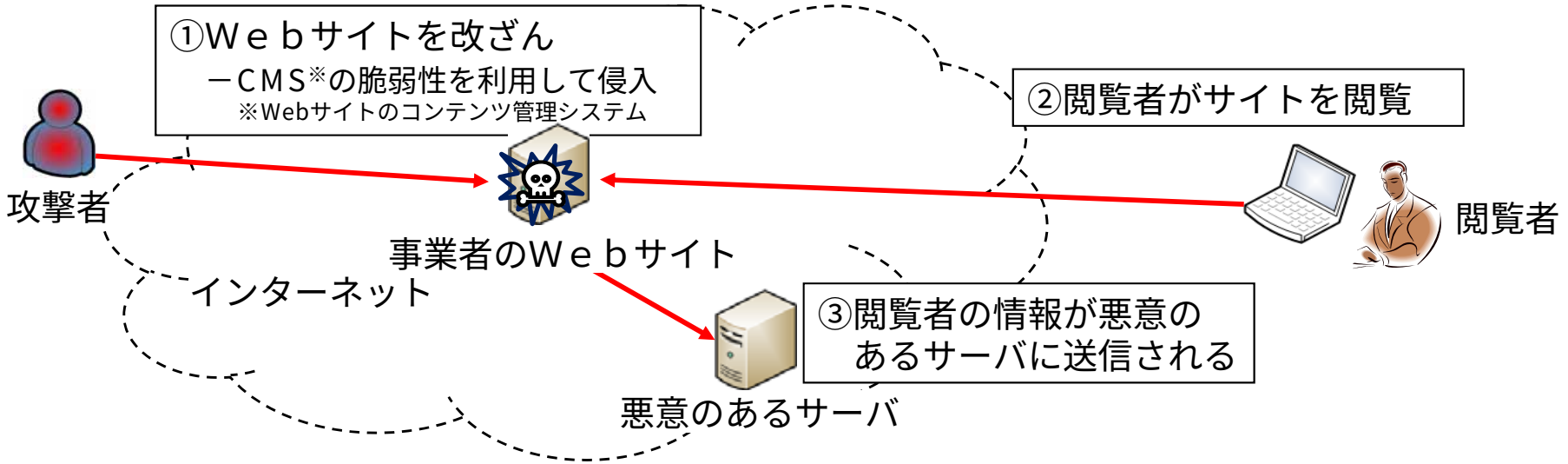
事例２（複数Ｗｅｂサイトの改ざん）　２／４

【事象のイメージ】

＜１件目のインシデント案件＞



＜２件目のインシデント案件＞



事例２（複数Ｗｅｂサイトの改ざん）　３／４

【原　因】

＜１件目のインシデント案件＞

- 初期構築時にのみFTPを利用し、その後はＣＭＳを利用した更新を行っていた。現在の担当者がFTPサービスが提供されている事を知らなかったため、FTPのID・パスワードは初期構築時より変更されていなかった。
- 不正なFTP接続によって、外部のWebサイトよりウィルスをダウンロードさせるプログラムがWebサイトに挿入された。

＜２件目のインシデント案件＞

- 同一Webサイト上にバージョンが異なる（脆弱性を有するバージョンを含む）ＣＭＳが存在していた。脆弱性の存在を認識していたものの運用中のWebサイトへの影響を考慮し、更新及び統一化が出来ていなかった。また、担当部署に加え外部事業者等の複数者がWebサイトの内容変更が可能な権限を有していた。
- 改ざんの約１ヶ月前に当該Webサイトに対して総当たり攻撃が行われていた。

事例２（複数Ｗｅｂサイトの改ざん）　４／４

【再発防止・課題等】

- Webサイトの必要性の見直しを行い、可能な限りIT担当部署が管理するWebサイト等に統合することにより管理の効率化等を図った。
- ファイアウォール等の設定を見直し、Webサイト利用における最小限の通信のみとした。
- 管理ページを含めたWebサイトのログを取得し、適切な期間（例えば1年間）保存するとともに、定期的に確認を行うこととした。
- ＣＭＳを１つに統合し一元的に管理すると共に、Webサイトの内容変更ができる権限を持つ者を限定した。
- 事業者内のWeb管理者向け研修において、事例を共有することにより他の担当部署が管理するWebサイトで同様の事象が起こらないように注意を促した。
- 幹部会議において事例を紹介し、担当者任せにせず幹部主導の下、組織として改善を行って欲しい旨の周知を行った。

【得られた気づき・教訓】

- ２件目の案件において、担当部署の判断により詳細が判明する前にWebサイトを停止することにより被害の拡大が防止された。現場で素早い判断を行うための体制や運用ルールの明確化または、現場で判断が出来ない場合であっても、速やかに判断できる者に報告できる体制構築が望ましい。
- Webサイトのアクセスログについて、事業者全体のルールでは保存期間を決めていなかったため、今回の2件ともに1ヶ月の保存期間であった。そのためログの解析が十分に出来なかった。今回の教訓を踏まえ、全体ルールとして適切な期間のログの保存を義務付けた。
- Webサイトの担当部署が複数に分かれるためITに詳しくない担当者もいる。ITに詳しくない担当者に対してもインシデント内容の重大性を理解してもらうための分かりやすい説明が必要である。また、何か不明な点があればIT担当部署に問い合わせを行うべきである。
- 普段からWebサイトの挙動に気を配り、通常と違う挙動が見られた場合に調査を行う、いわゆる予兆を見逃さない心構えが重要である。

事例３（複数回にわたるＷｅｂサイト遅延障害）　１／４

【概　要】

- 事業者が管理するWebサイトに複数回にわたり、海外の複数地域より大量の接続要求があり、表示が著しく遅くなった。
- ４回目の事象発生時に、DNSサーバへの接続要求も多数確認した。当該事象を情報共有した結果、DNSサーバがオープンリゾルバ状態※1であることが判明したため、対策を実施した。

※1 応答する必要のない外部からの問い合わせに応答する状態。攻撃の踏み台として利用される危険が高い。

＜１～３回目のインシデント案件＞

最初の２回については、Webサイトの表示が著しく遅くなったものの、短時間で通常状態となったため、監視強化を行った上で様子見とした。

３回目については、それまでに２回発生していたこと、比較的影響が長時間続いたこともあり、ファイアウォールにて発信元IPの遮断を実施した。しかしながら遮断後においても、IPアドレスを変えて引き続きアクセスされる状況であったため、Webサーバの処理能力に余裕があったことから、厳しめに設定していたファイアウォール側での同時接続数を増加させることで対応した。

＜４回目のインシデント案件＞

３回目と同様の措置を実施して対処した。またDNSサーバへの接続要求も多数確認※2した。

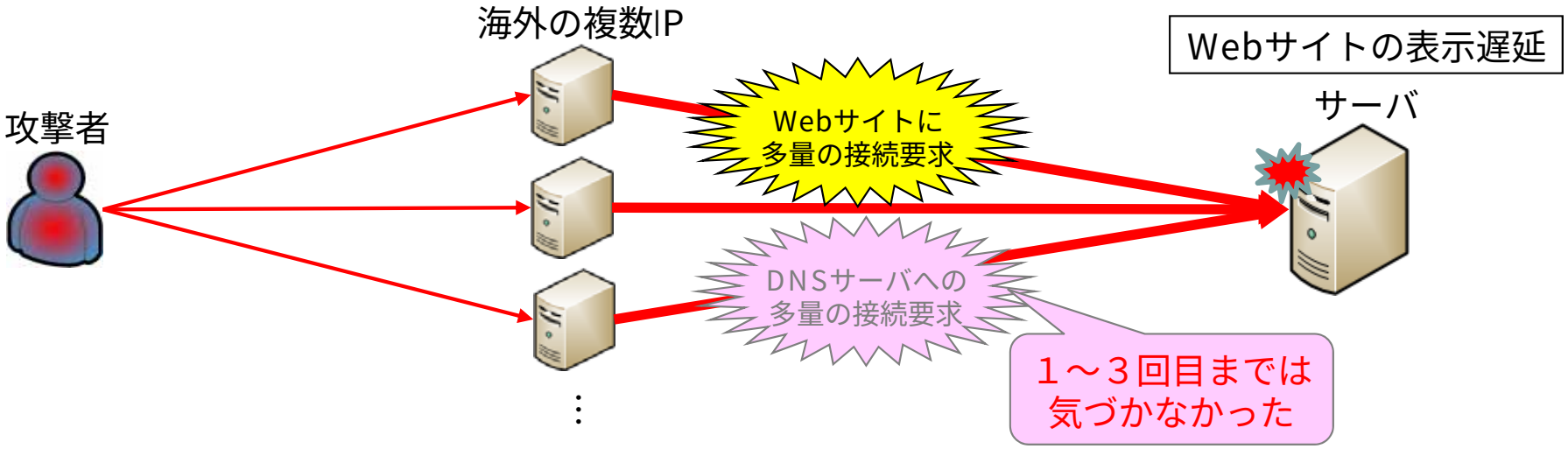
本事案を情報連絡により情報共有したところ、NISCより、DNSサーバがオープンリゾルバ状態である旨の指摘を受け、対策を行い解消した。その後は、同様の事象は発生していない。

※2 DNSサーバへの接続要求は１回目からあったが、Webサイトの遅延のみに注意を向けていたため、４回目になって初めて気づいた。

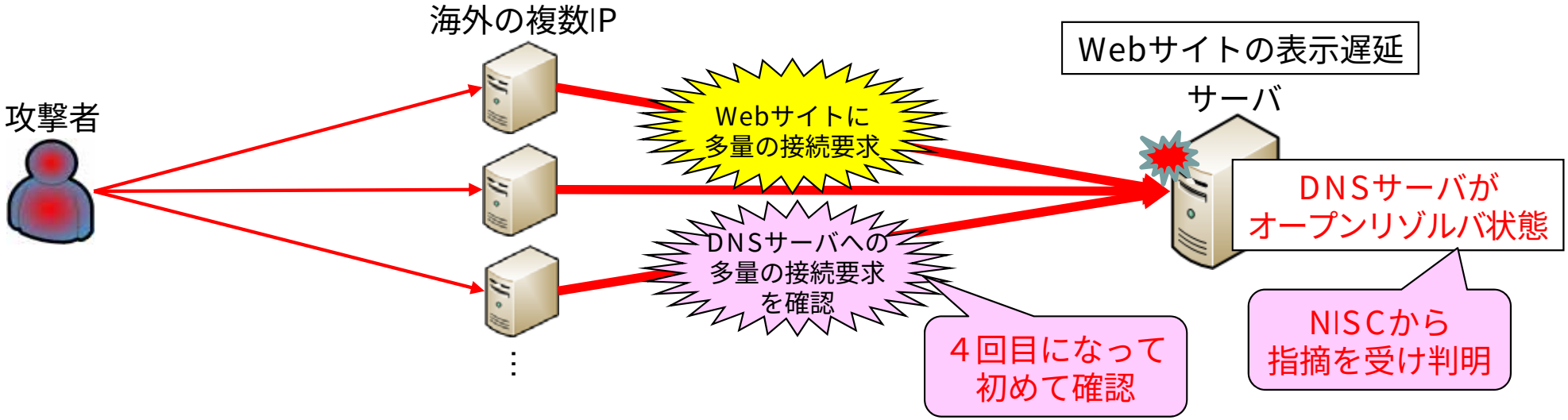
事例３（複数回にわたるＷｅｂサイト遅延障害）　２／４

【事象のイメージ】

＜１～３回目のインシデント案件＞



＜４回目のインシデント案件＞



事例３（複数回にわたるＷｅｂサイト遅延障害）　３／４

【原　因】

＜１～３回目のインシデント案件＞

- 根本原因については不明。
- 他事業者で同様の事象が発生していないかどうかの確認を行い、他事業者で発生していないことを確認。

＜４回目のインシデント案件＞

- 根本原因については不明だが、ＤＮＳサーバがオープンリゾルバ状態であったことが判明。
- 運用保守は業務委託し、常駐保守となっていることもあり、セキュリティ対策は十分に実施しているとの思い込みがあった。
- 公開サーバ系を中心としたパッチ適用等は実施していたため、脆弱性は問題ないとの認識があった。
- セキュリティ監査については、予算の関係もありしばらく実施できていない状態であった。

事例３（複数回にわたるＷｅｂサイト遅延障害）　４／４

【再発防止】

- 監視強化の一環として、ログ確認を毎日定期的に実施。
- 不正アクセス対策として、高度な攻撃を検知・自動ブロックするためのIPS装置※１を導入。
- セキュリティ注意喚起に関する連絡を確実に実施※２。
- ファイアウォール等（IPS含む）のログは、アクセス数が多いと一杯になってしまうため、ログサーバで保存する等の管理を徹底。

※１　不正侵入防止システム
※２　ネットワーク構成が２つに分かれており端末も別々のため、セキュリティ注意喚起に関する連絡については、確認が十分に行えていない状態であった。

【得られた気づき・教訓】

- 障害等が発生した場合には、把握をしている範囲で関係機関に情報連絡を行うとともに、関係機関から提供された情報について、適切に対応する。
- 公開サーバ系については、パッチ適用等の脆弱性対策を行うだけでなく、設定情報等のチェックを含めたセキュリティ監査についても、定期的に実施する。
- 運用保守を委託先に全て任せるのではなく、セキュリティ対策は事業者自身が責任を負うということを再度認識するとともに、連絡体制を整えておく。
- 障害発生時は、事業者内だけでなく、他事業者とも連携をとるとともに、Webサイト応答時間計測システム※3等の仕組みについても活用することにより、横の情報共有を行う。

※３　DDoS攻撃やアクセス集中時等のWebサイトのレスポンス変化を観測し、情報共有を行うセプターカウンシルにおける取組み。