IPA Better Life with IT

ウェブサイトの安全な運用について

2022年 10月 27日

独立行政法人情報処理推進機構
セキュリティセンター セキュリティ対策推進部
脆弱性対策グループ

本講演の概要

- 講演内容
  - 「脆弱性」とはなにか、実際に被害が発生した事例を交えつつ解説
  - ウェブサイト運営者が実施するべき基本的な対策について解説
  - 運用しているウェブサイトで、脆弱性が発見された際の対応方法を解説

※**注意事項**
本セミナーでは、実際に攻撃に使用できる文字列を複数紹介しております。こちらを、第三者のウェブサイト等に対して試してみる等の行為は、絶対に行わないでください。

目次

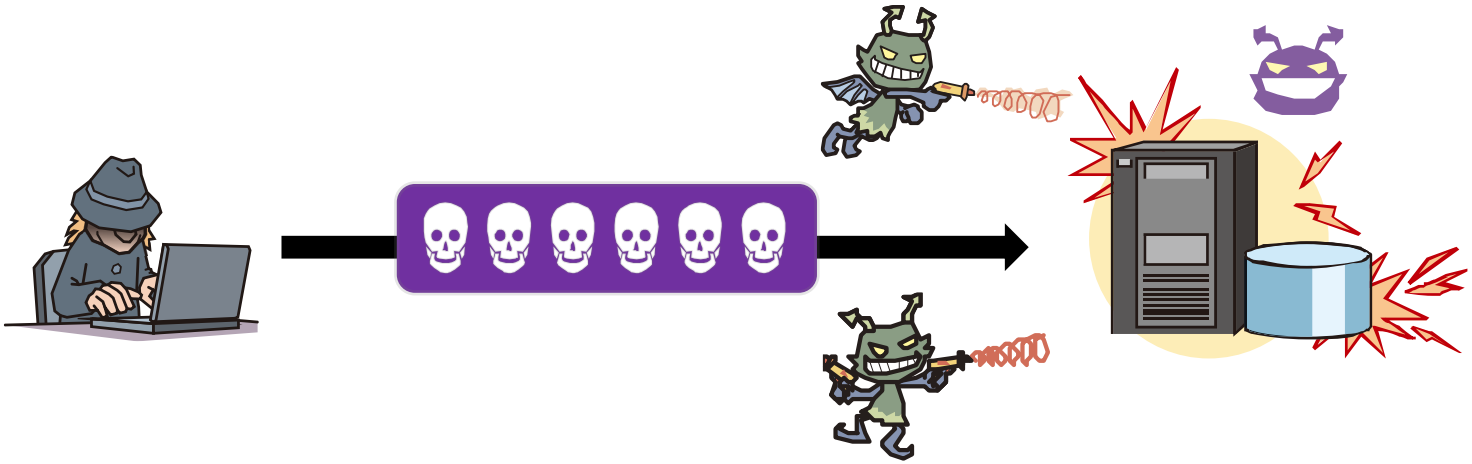
第一章 脆弱性について

1.1 脆弱性とはどんなものか？

1.2 脆弱性による被害の事例

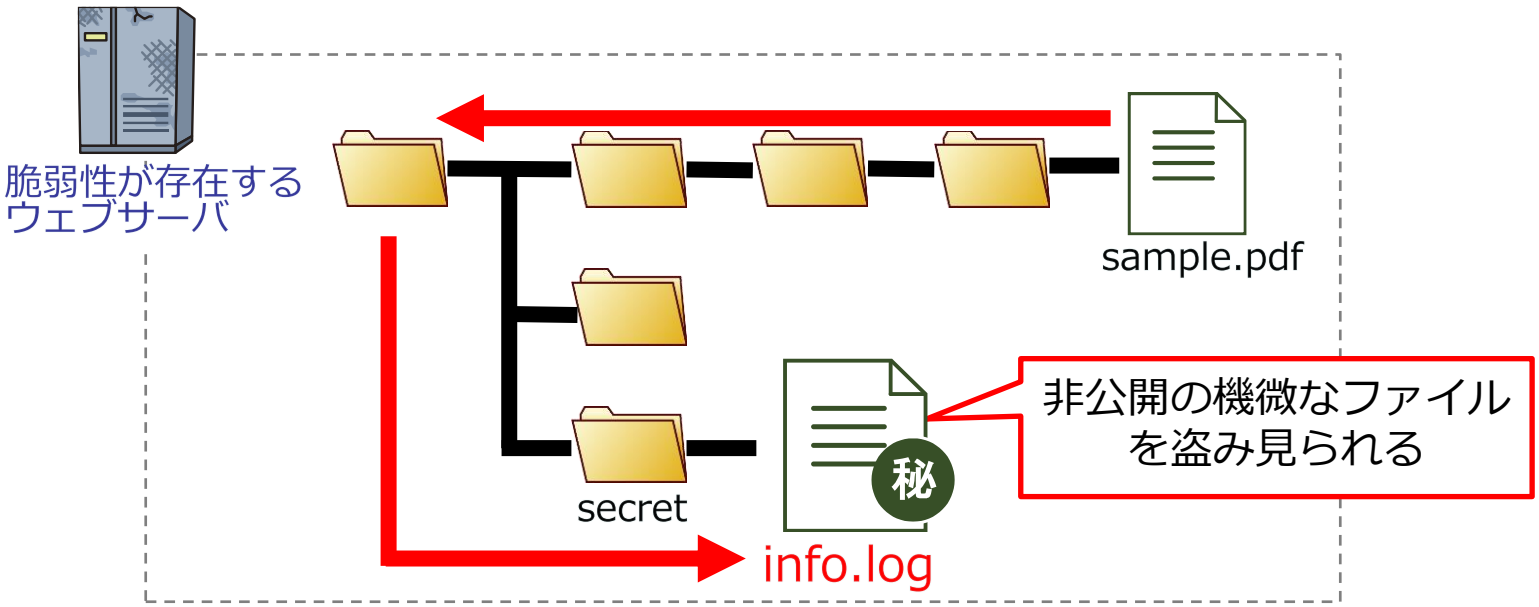
機能や性能を損なう脆弱性(1)

- 脆弱性とは
  - ウェブサイトやソフトウェア製品の機能や性能を損なう問題個所
  - 放置されると、ウイルスの感染活動やウェブサイトの乗っ取り、情報漏洩等の被害につながる可能性がある
  - ウェブサーバの設定不備についても脆弱性とみなされる



機能や性能を損なう脆弱性(2)

- 脆弱性を悪用した攻撃手法の一例
  - 正常時のURL
    http://example.com/a/b-01.php?down=sample.pdf
  - 攻撃時のURL
    http://example.com/a/b-01.php?down=**../../../secret/info.log%00**



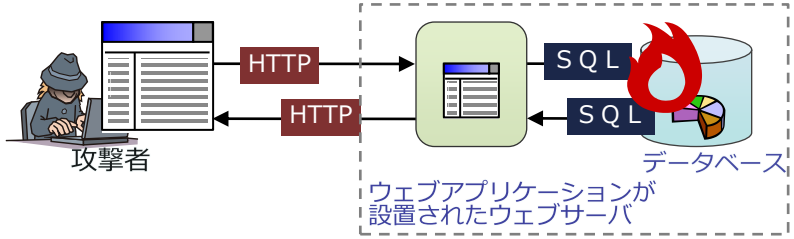
機能や性能を損なう脆弱性(3)

- 脆弱性の例

① 攻撃者が、細工したリクエストを送信する
例：専用のソフトで通信データを直接細工する

② 動作が停止してしまう

① 攻撃者が、細工したリクエストを送信する
例：通常の入力　・・・パスワード
細工した入力・・・SQLクエリ等



② 使用しているデータベースを不正に操作されてしまう

- アプリケーションが利用できなくなる
- データベースに保存している個人情報が漏洩する

セキュリティ上の弱点として「脆弱性」と呼ばれる

第一章 脆弱性について

1.1 脆弱性とはどんなものか？

1.2 脆弱性による被害の事例

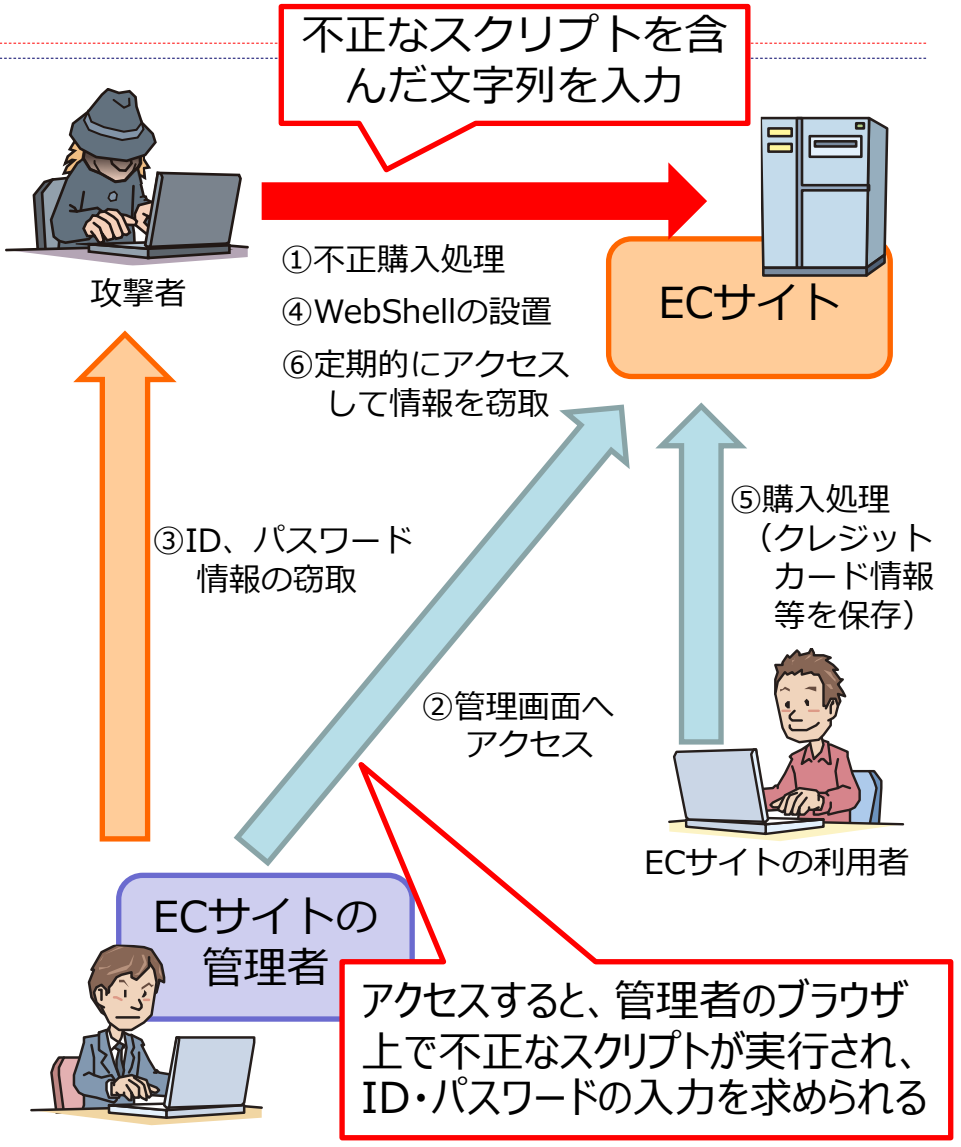
SQLインジェクション攻撃による被害の状況

- SQLインジェクション攻撃によって発生した被害
  - 大手玩具メーカーが運営する会員制のウェブサイトより、サイト会員のメールアドレス4万6,421件が流出した可能性（2021年6月）
  - クレジットカード決済基盤提供会社のウェブサイトより、クレジットカードの番号、有効期限、セキュリティコードなど最大46万395件が流出（2022年2月）
  - アウトドア用品企画会社のウェブサイトより、顧客および取引先のメールアドレス2万3,435件が流出した可能性（2022年2月）

格納型クロスサイト・スクリプティング

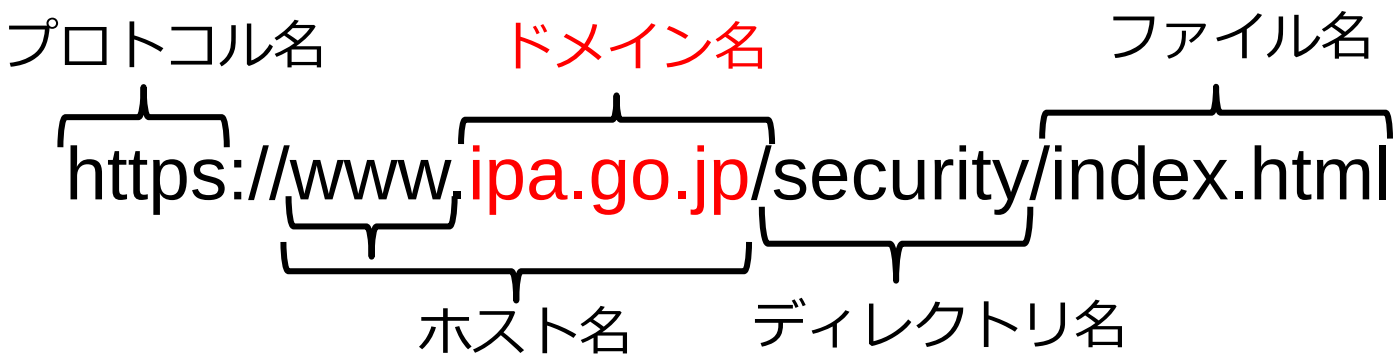
不正購入処理を利用した攻撃

- ECサイトで被害報告
  - 「不正購入処理」でECサイトを侵害する攻撃キャンペーン(Water Pamola)
  - 非保持化を実現していたとしても、カード情報やセキュリティコードが漏えいする
- ECサイトの管理画面上の脆弱性を悪用
  - 管理画面上にクロスサイト・スクリプティングの脆弱性が存在した場合に影響
  - WebShellを設置され、継続的に情報を窃取される



ドメイン名ハイジャック(1)

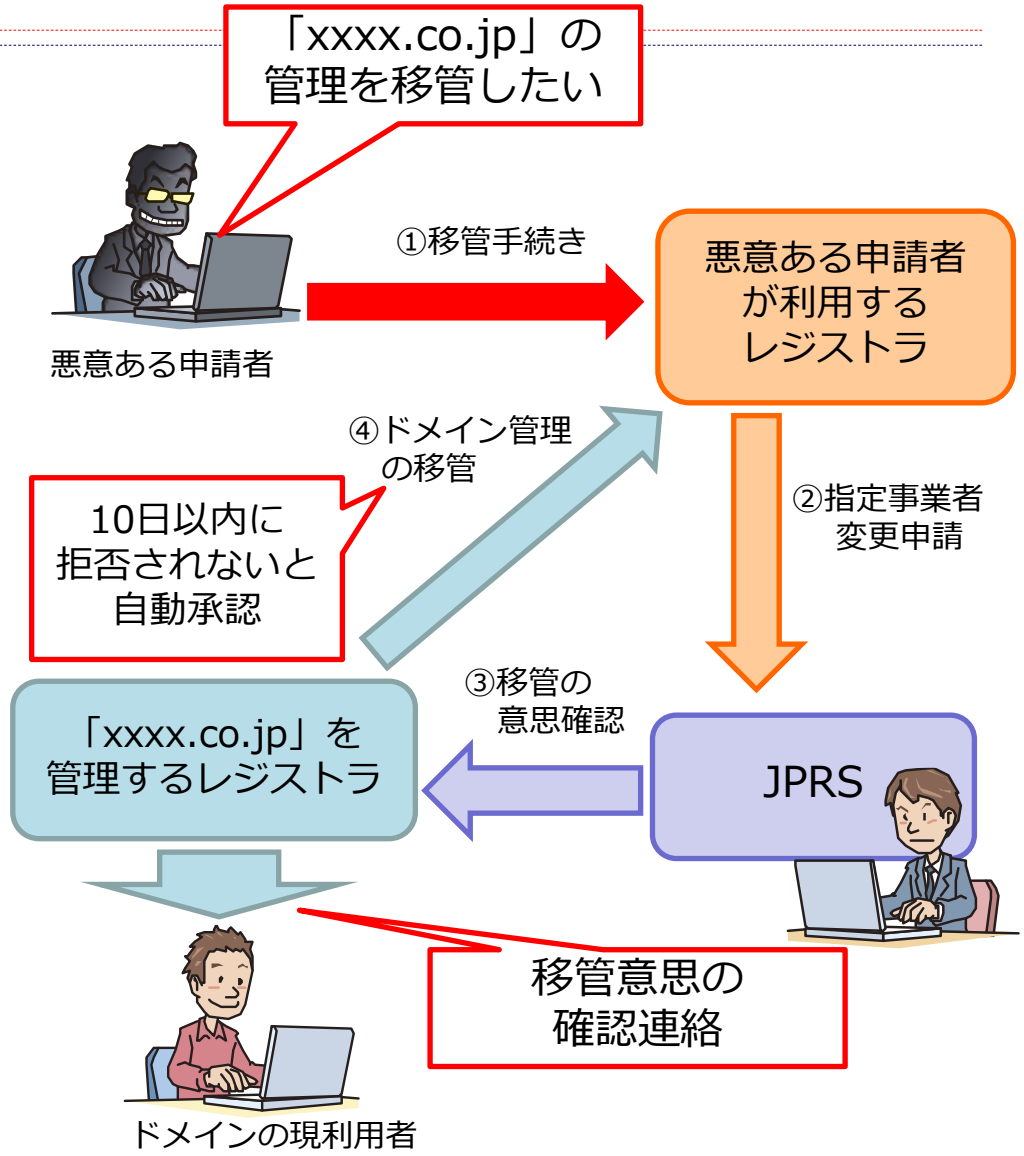
- ドメイン名とは
  - インターネット上のネットワークを識別するための名前



ドメイン名が第三者によって、意図せず乗っ取られる事件が発生！

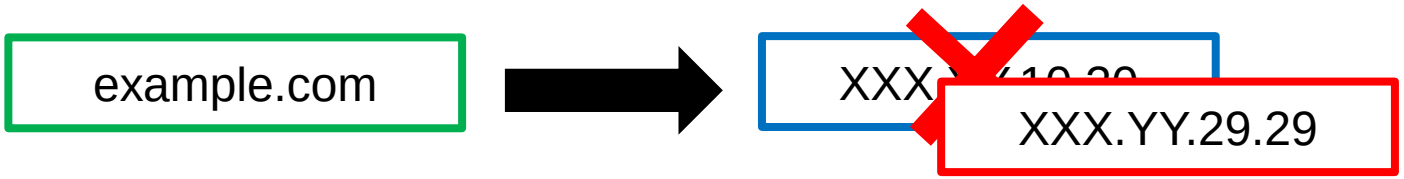
ドメイン名ハイジャック(2)

- 有名アニメサイトが意図しないコンテンツを表示
  - 突然アニメサイトに無関係な情報が表示される事態
  - 当初はウェブサイトの改ざんが疑われた
- ドメイン不正移管が原因
  - 悪意ある申請者により、ドメイン移管の申請をされる
  - ドメインの移管手続きは正規の手順であった
  - 10日以内に現利用者の移管意思の回答がない場合、自動的に移管手続きが完了する



ドメイン名ハイジャック(3)

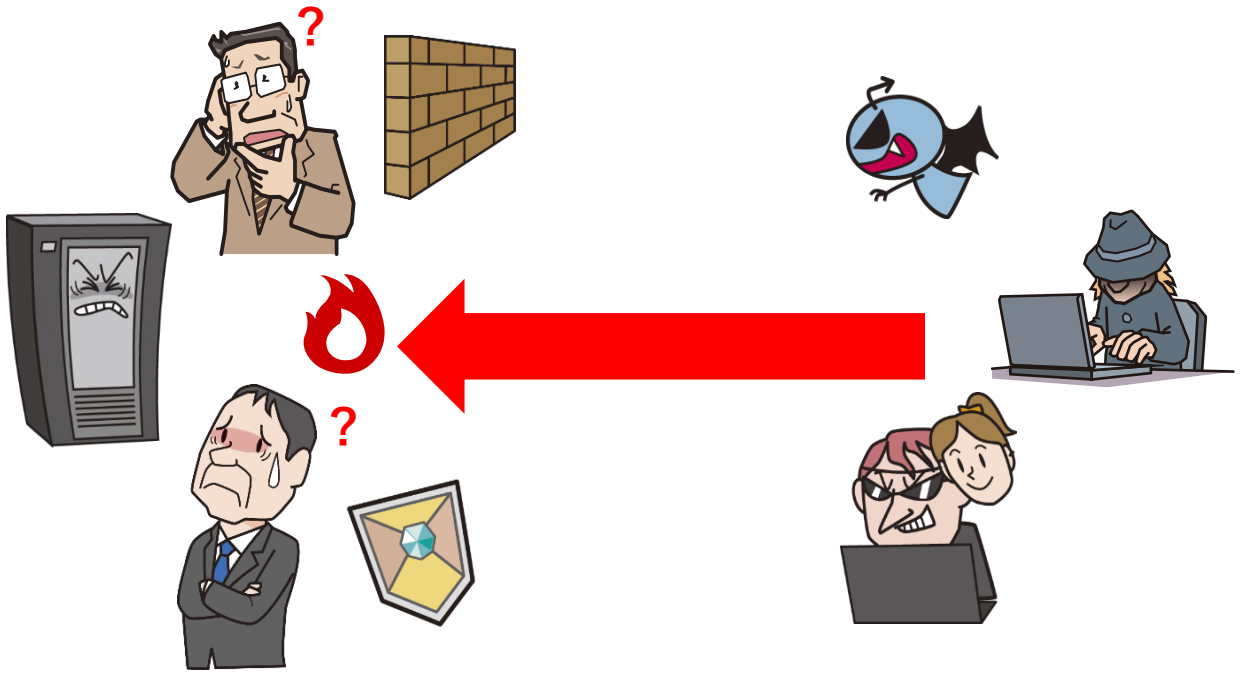
- ドメイン登録事業者のアカウントを乗っ取り
  - 登録事業者(レジストラ)のウェブサイトの脆弱性を悪用
  - 登録メールアドレスを変更し、アカウントを乗っ取り
- 登録事業者の登録情報を改ざん
  - ドメイン名の問い合わせ先サーバ情報を変更
  - 攻撃者が用意したサーバに問い合わせを誘導



最終的に企業宛のメールを盗み見られる被害が発生

ウェブサイトへの攻撃に対して

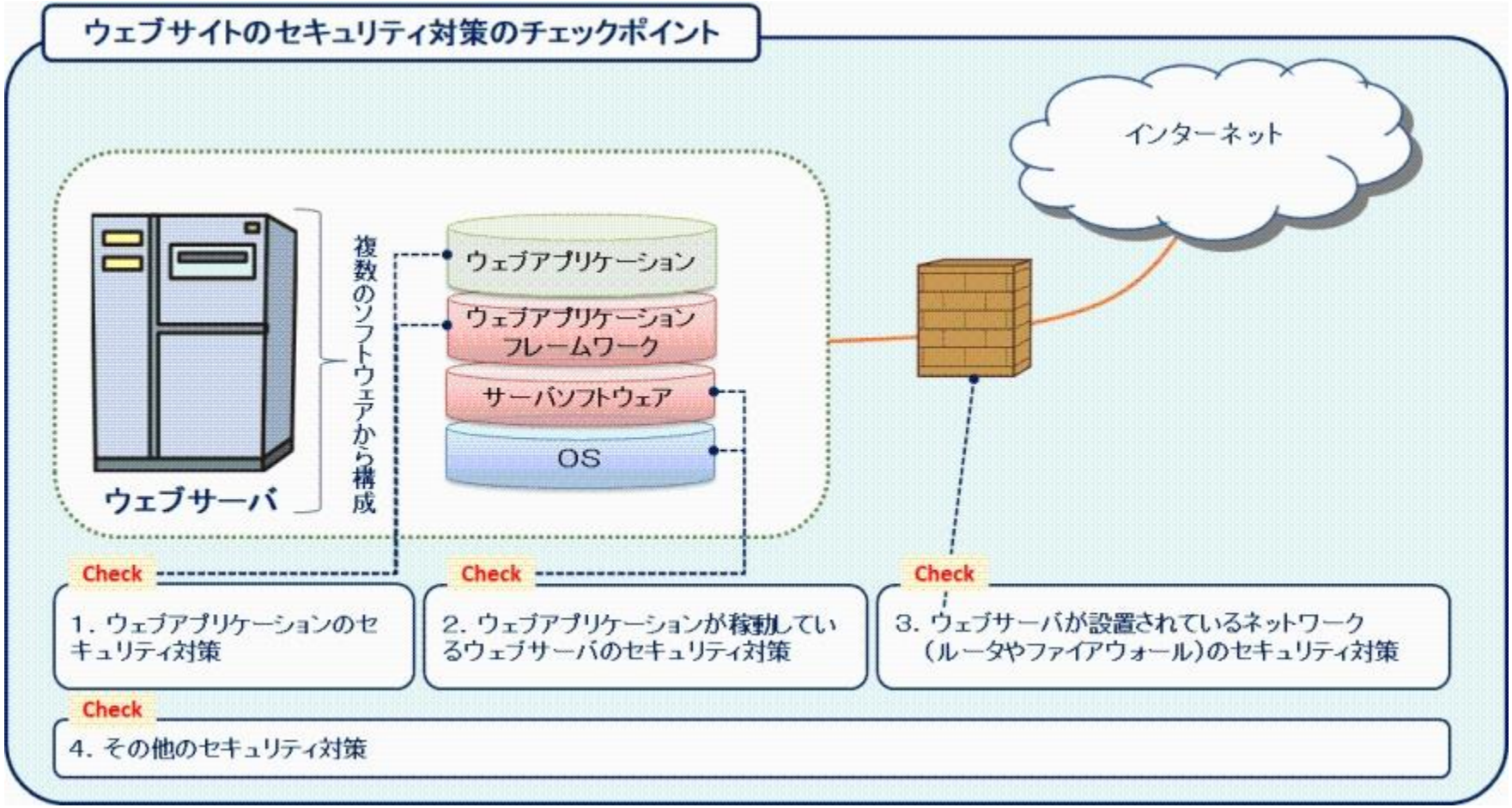
- 何に注意すればいいの？
- どのような対策が必要になるの？



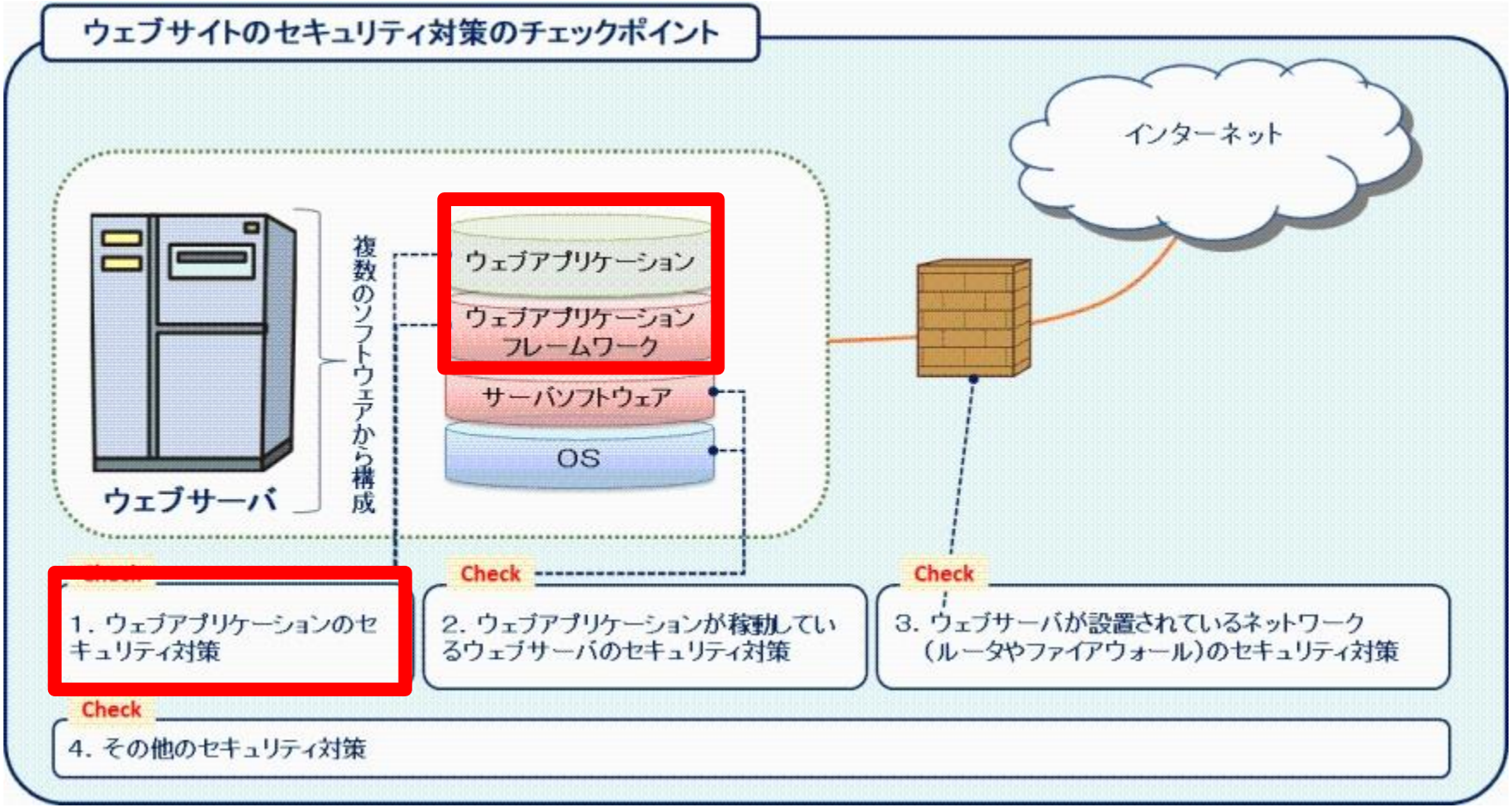
第二章 対策方針について

第一章 脆弱性について
第二章 対策方針について
第三章 脆弱性が発見されたら
第四章 まとめ

第二章 対策方針について

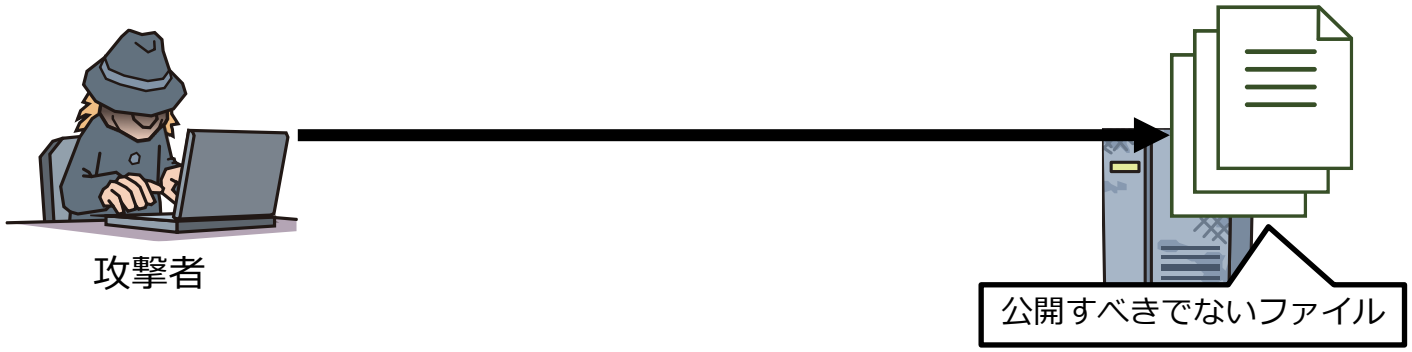


1．ウェブアプリケーションのセキュリティ対策



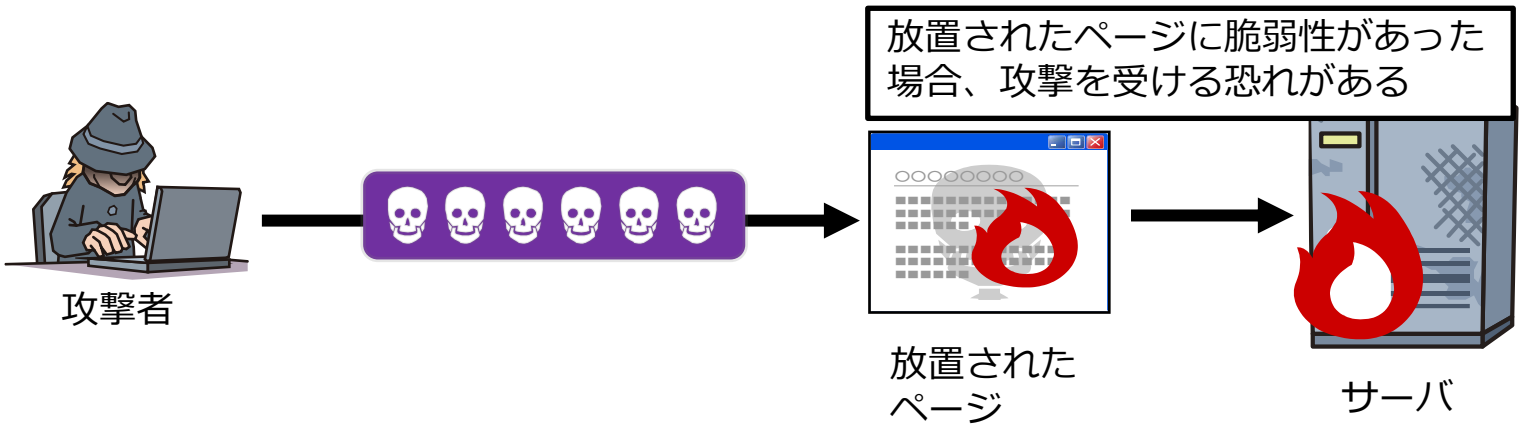
1-1.
公開しているファイルの確認(1)

- 公開すべきでないファイルを公開していませんか？
  - **個人情報**や**機密情報の記載されたファイル**、.htaccessなどの**システムファイル**などが該当します。
  - これらのファイルを誤って公開してしまっていた場合、**非公開にする**と同時に、キャッシュの削除を検索エンジンを提供している企業などに依頼することをご検討ください。



1-1.
公開しているファイルの確認(2)

- 不要になったページやウェブサイトを公開していませんか？
  - 不要となったページを残しておくと管理が及ばず、脆弱性が発覚した際に影響を受ける可能性があります。
  - そのため、公開期間が終了になった際や、不要となったタイミングで**非公開**とすることを推奨いたします。



1-2.
脆弱性対策の実施と更新(1)

- ウェブアプリケーションの脆弱性への対策をしていますか？
  - 「**安全なウェブサイトの作り方**」には、一般的に多くみられるウェブアプリケーションの脆弱性に対する対策を記載しています。
  - これらの対策が出来ているか今一度ご確認ください。

    安全なウェブサイトの作り方
    https://www.ipa.go.jp/files/000017316.pdf

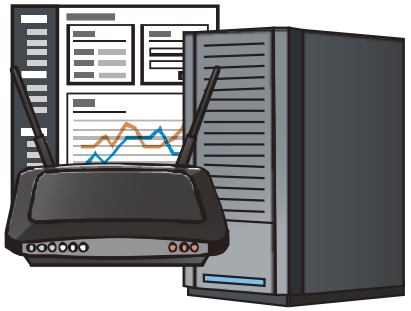
SQLインジェクション
OSコマンド・インジェクション
ディレクトリ・トラバーサル
セッション管理の不備
クロスサイト・スクリプティング　…など
11種類の脆弱性の概要と対策について記載

1-2.
脆弱性対策の実施と更新(2)

- プラットフォーム並びに、ウェブアプリケーションを構成しているソフトウェアの脆弱性対策を定期的にしていますか？
  - プラットフォーム等に脆弱性が見つかった場合、**アップデートを行う**必要があります。
    - OSやサーバソフトウェア、ミドルウェア
    - ウェブアプリケーションを構築する各種ソフトウェアやフレームワーク
    - CMS（コンテンツ・マネジメント・システム）
  - その為にも、自組織で使用している**ソフトウェアや機器を把握**し、脆弱性があるバージョンでないか、定期的に確認する必要があります。
  - JVN iPediaで公開しているので、情報収集の手段の一つとして活用してください。
    - https://jvndb.jvn.jp/

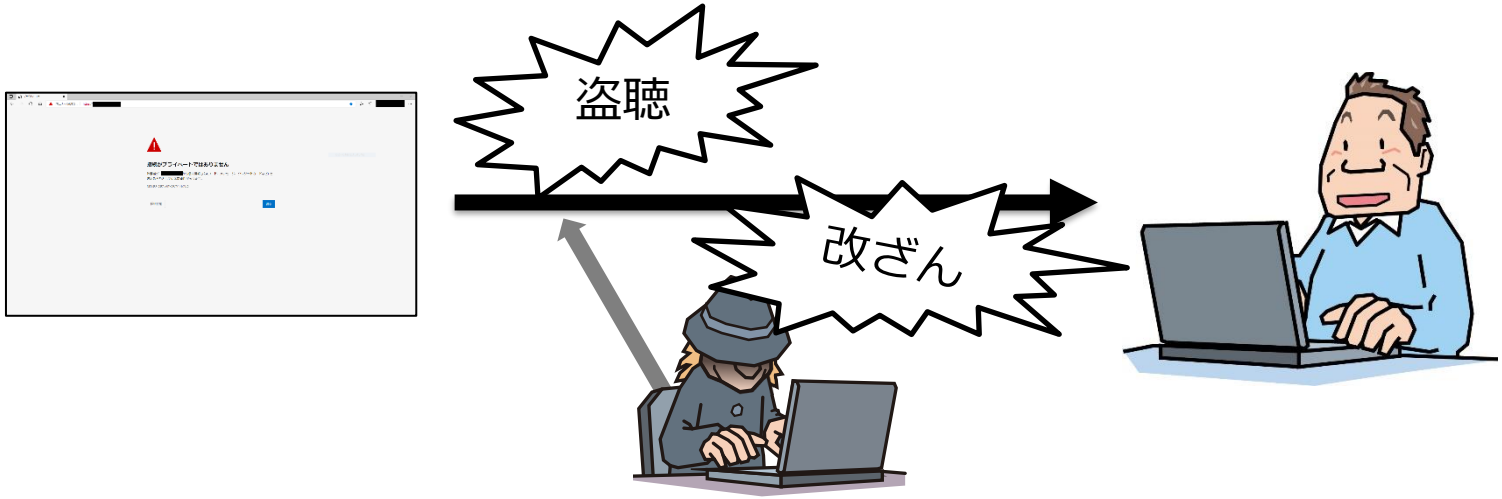
1-3.定期的なログの確認

- ウェブアプリケーション
- ウェブサーバ
- ネットワーク機器
- 上記のログを保管し、定期的に確認していますか？
  - 定期的に各種ログを確認する事で、攻撃の兆候に気付いたり、**故障**に気付くことができます。
  - 適切に取得・保管し、定期的に確認してください。

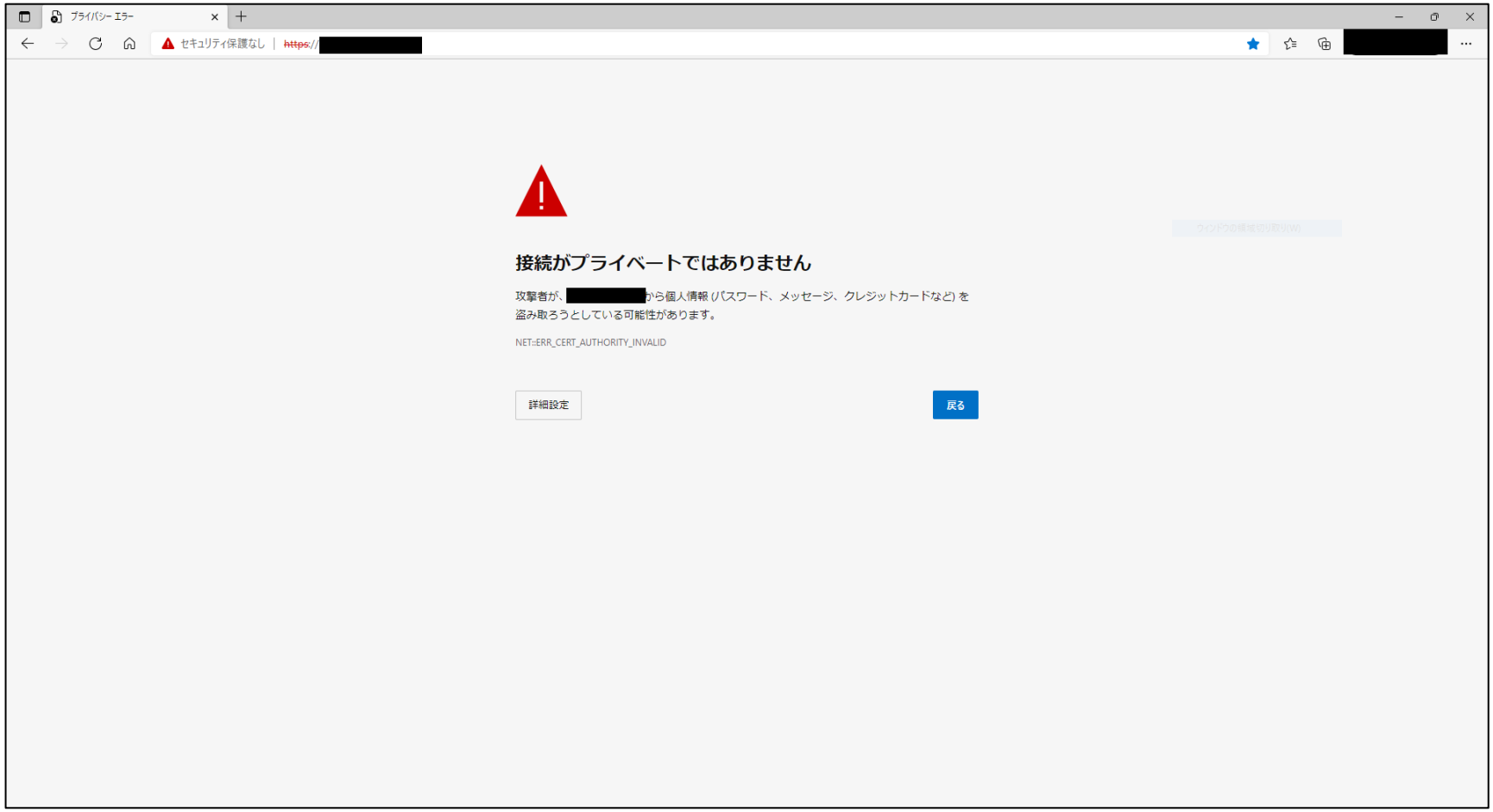


1-4.暗号化の実施

- インターネットを介して送受信する通信内容の暗号化はできていますか？
  - ウェブアプリケーションと利用者間の通信は、盗聴や改ざん・なりすましの恐れがあります。
  - HTTPS化することで、情報が不正に窃取されることを防止できます。**暗号化**がされていない場合は、導入をご検討ください。

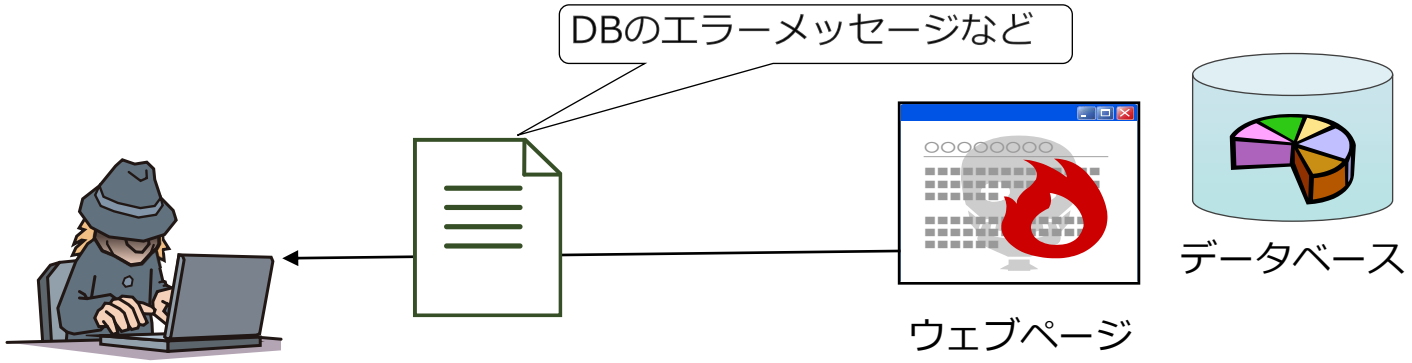


1-4.暗号化の実施

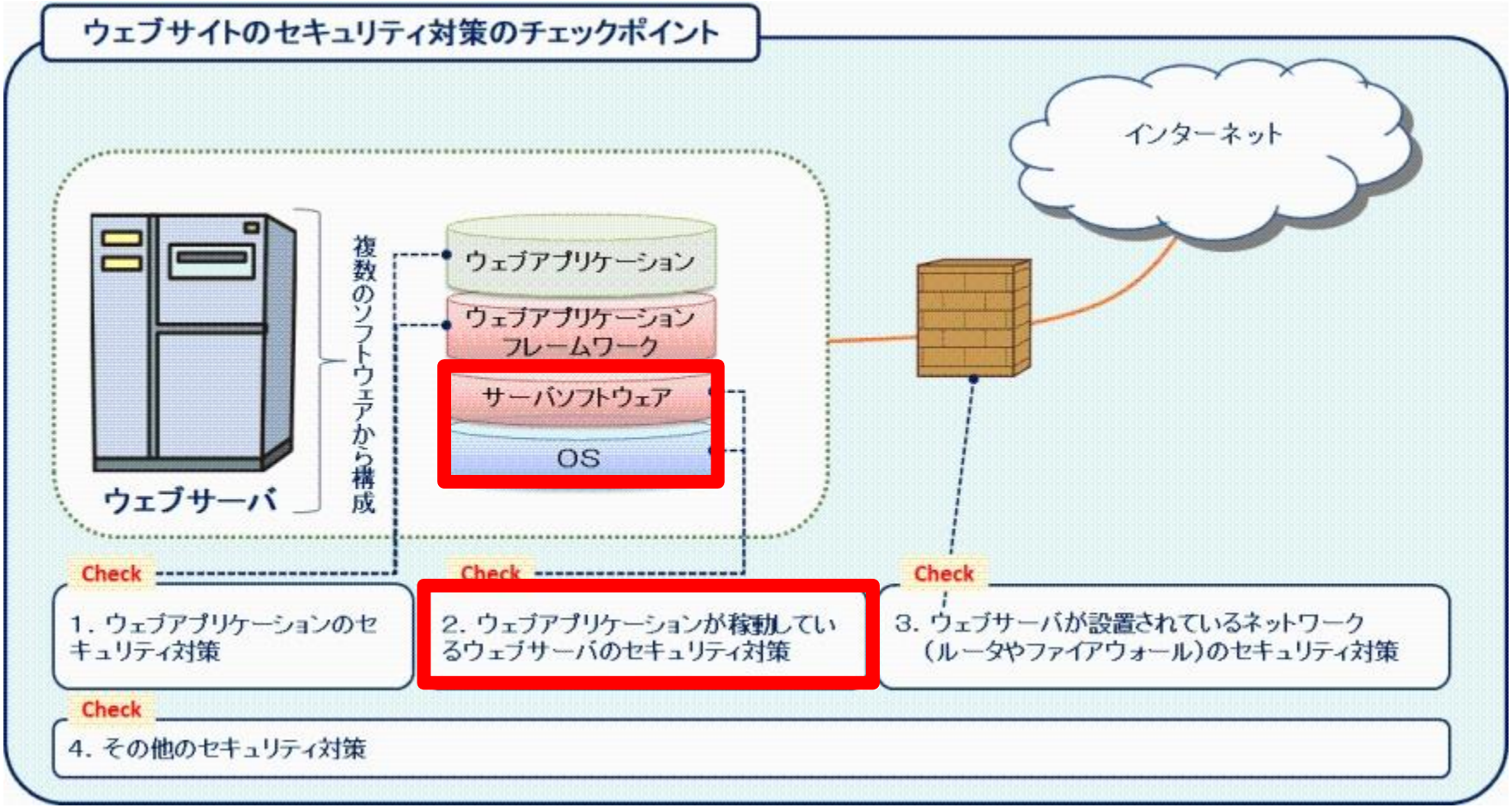


1-5.エラーメッセージの確認

- 不必要なエラーメッセージを返していませんか？
  - アプリケーションやDBのエラーメッセージをそのまま返しているケースがあります。
  - エラーメッセージは**必要最低限**とすることを推奨いたします。



2.ウェブサーバのセキュリティ対策

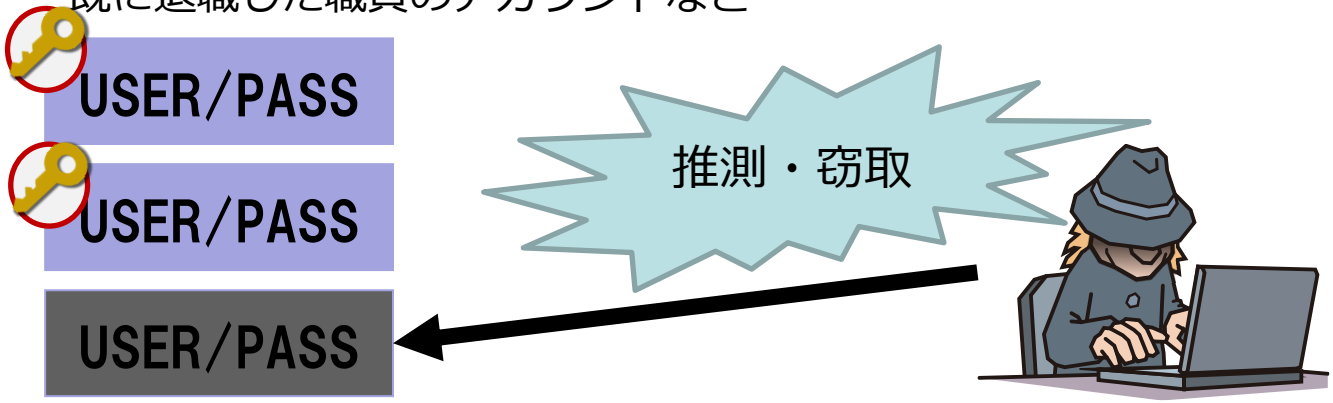


2-1.定期的なサービスの確認

- 不要なサービスやアプリケーションがありませんか？
  - ウェブサーバ上で不要なサービスが稼働している場合、そのサービスを踏み台にするなどして攻撃を受ける可能性があります。
  - 起動するサービスは**必要最低限**とし、不要となったアプリケーションは**削除**してください。

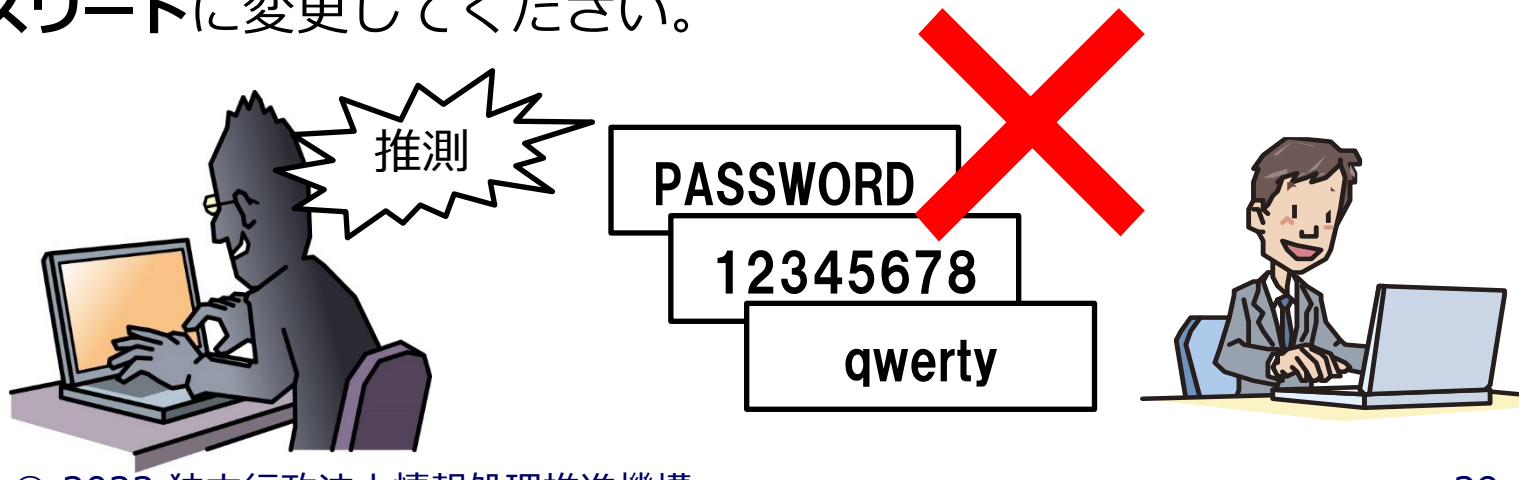
2-2.アカウント管理の徹底(1)

- 運営者のサーバや端末に不要なアカウントが登録されていませんか？
  - ウェブサーバや、それを管理する端末上で不要なアカウントが登録されている場合、**悪用**される恐れがあります。
  - 不要なアカウントが残存している場合、**削除**してください。
    - 開発段階やテスト段階で使用されていたアカウント
    - デフォルトで用意されているアカウント
    - 既に退職した職員のアカウントなど



2-2.アカウント管理の徹底(2)

- 運営者のサーバや端末に推測されやすい単純なパスワードを使用していませんか？
  - 推測されやすいパスワード（password、adminなど）を使用している場合、アカウントを乗っ取られ、**悪用**される可能性が非常に高まります。
  - 特に、管理者権限を持ったアカウントや、リモートアクセスを行うアプリケーションなどの場合、被害が大きくなります。
  - 安易なパスワードを使用している場合、**推測されにくい複雑なパスワード**に変更してください。

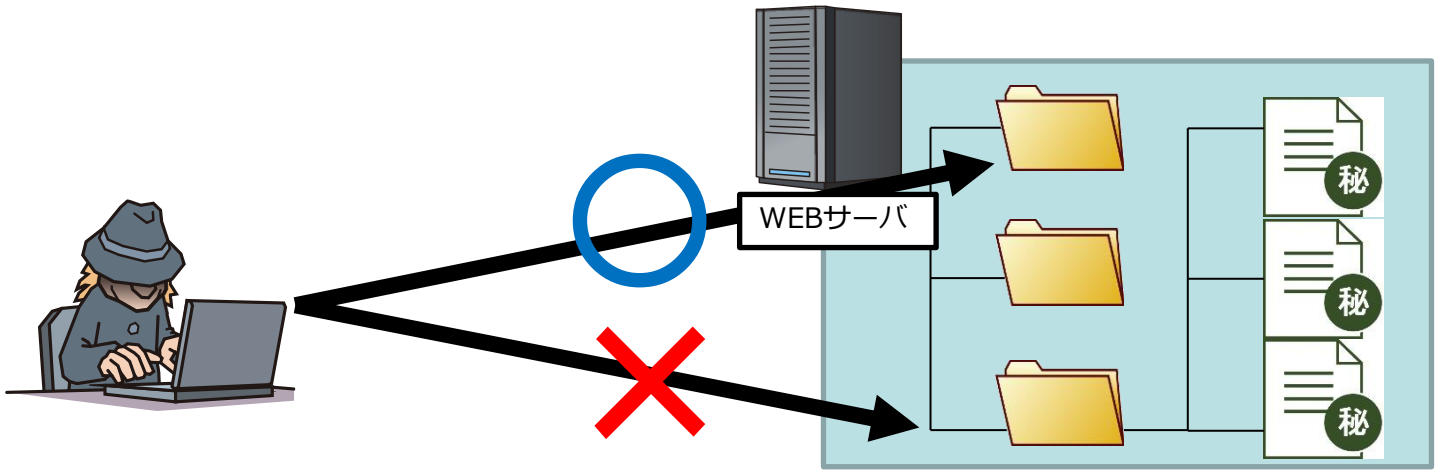


2-2.アカウント管理の徹底(3)

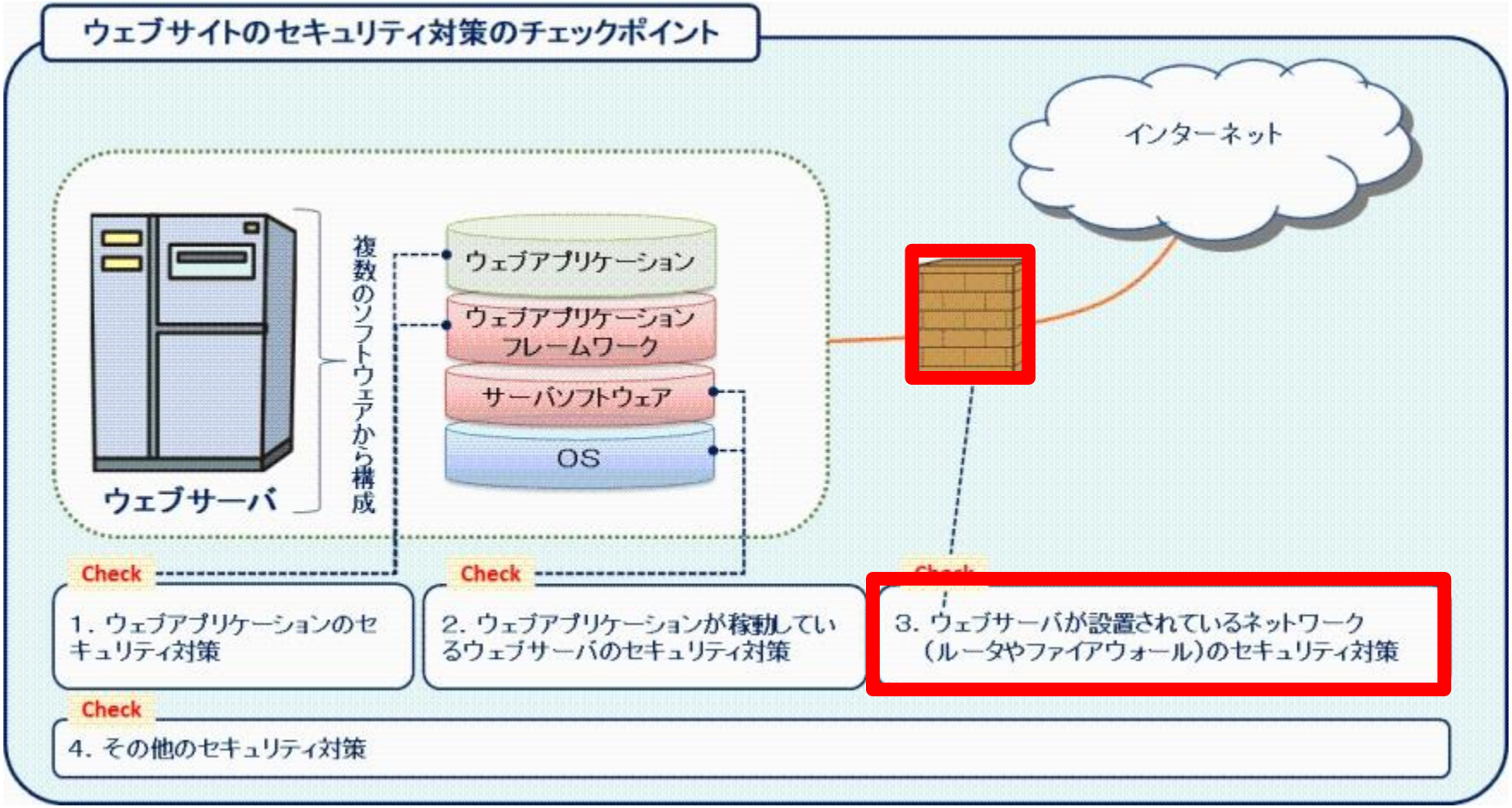
- ユーザのアカウントに対する不正ログインの対策はできていますか？
  - 別のウェブサイトやサービスから漏洩したIDやパスワードによる不正ログインによって、**利用者が**情報漏洩などの被害を受ける恐れがあります。
  - 利用者に対して**アナウンス**をするとともに、不正ログインを検知、防止するための**システムの導入**を検討してください。

2-3.アクセス制御の実施

- ファイル、ディレクトリへの適切なアクセス制御をしていますか？
  - サーバ上に配置されているファイル、ディレクトリに**適切なアクセス制限**がされていない場合、第三者に非公開のファイルを見られたり、不正にプログラムを設置され、実行される恐れがあります。
  - 非公開のファイル・ディレクトリは適切にアクセス制限を施してください

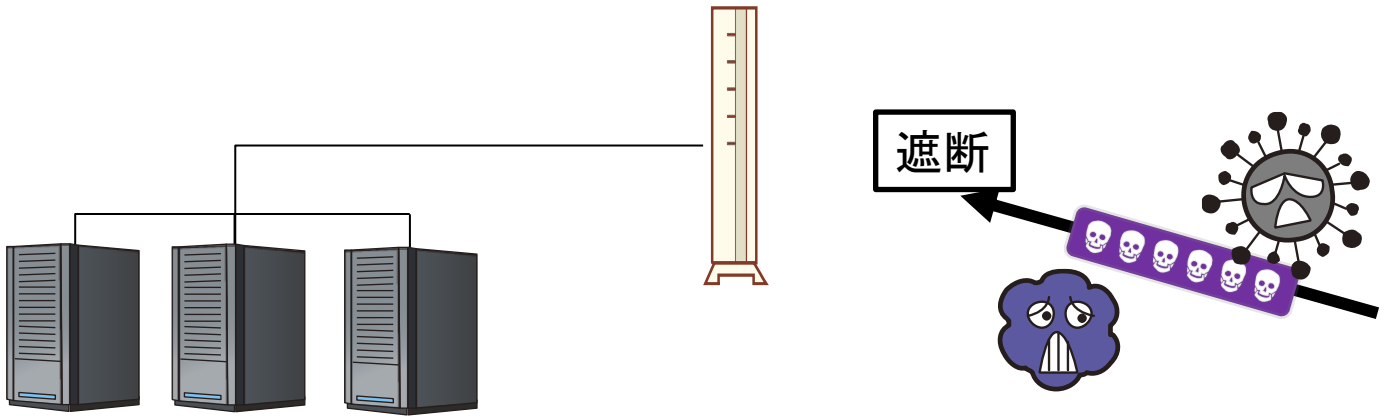


3.ネットワークのセキュリティ対策



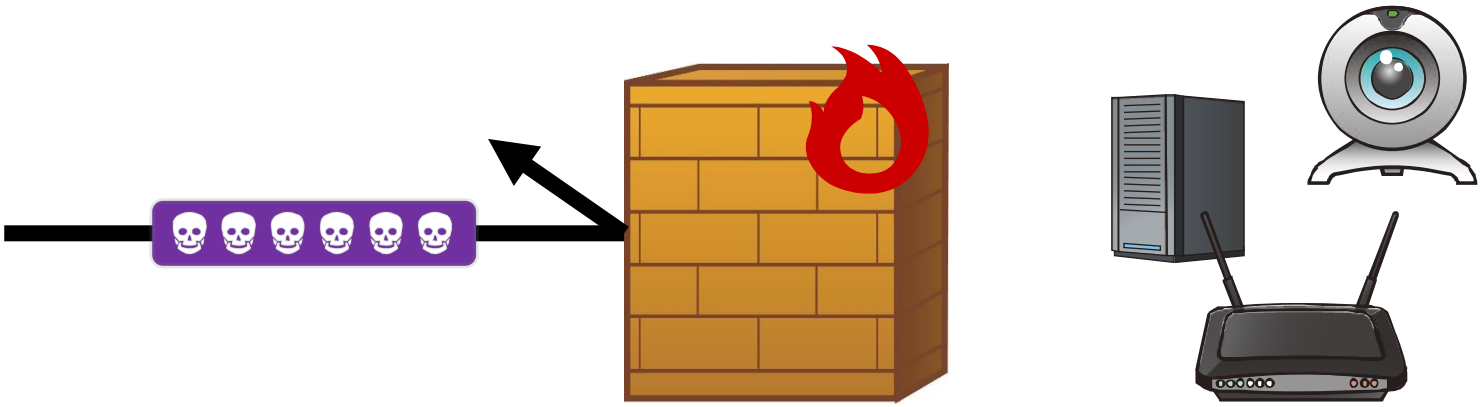
3-1.ネットワーク機器での対策

- ルータなどを使用してネットワークの境界で不要な通信を遮断していますか？
  - 境界ルータなどのネットワーク機器を使用して、**不要な通信を遮断**することで、攻撃の糸口を減らすことができます。
  - 内部の通信の場合でも、**不要な通信を遮断**することで、万が一侵入された場合の被害を軽減できる可能性があります。



3-2.フィルタリングによる攻撃の遮断(1)

- ファイアウォールを使用して、適切に通信をフィルタリングしていますか？
  - 適切なフィルタリング設定がなされていない場合、ファイアウォールを設置していても防御することができません。
  - 送受信の規則を把握し、今一度設定を見直すことをご検討ください。

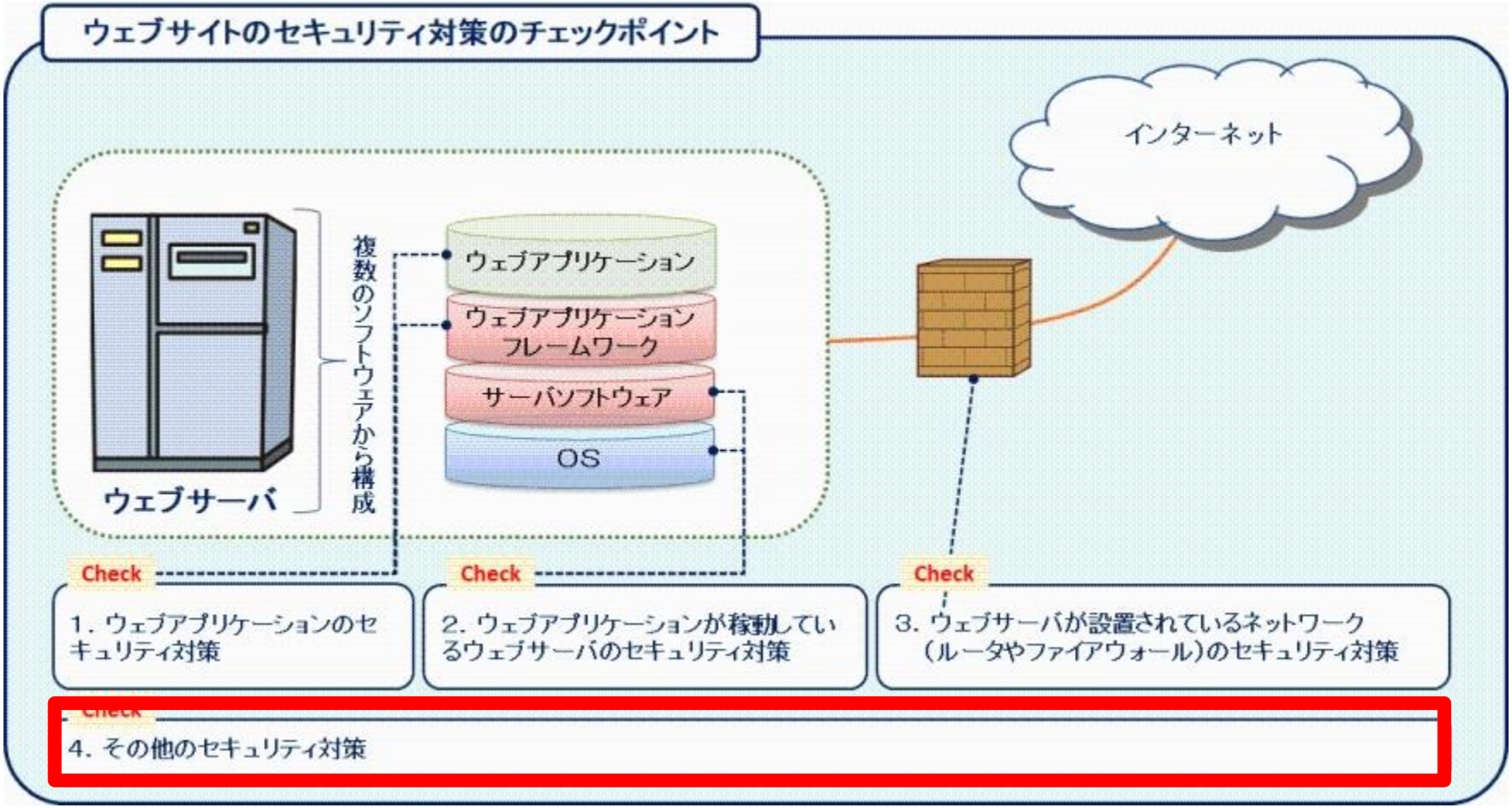


3-2.フィルタリングによる攻撃の遮断(2)

- ウェブサーバ（ウェブアプリケーション）への不正な通信を検知または、遮断していますか？
  - IDSやIPS、WAFなどを導入することで、ウェブサイトと利用者の間の通信を検査し、**自動的に検知、遮断**をすることが出来ます。
  - 攻撃の影響を低減するのに有効な手段の一つとして、導入をご検討ください。
  - IPAではWAFの導入を検討する際の参考となる資料を公開しておりますので、ご活用ください。

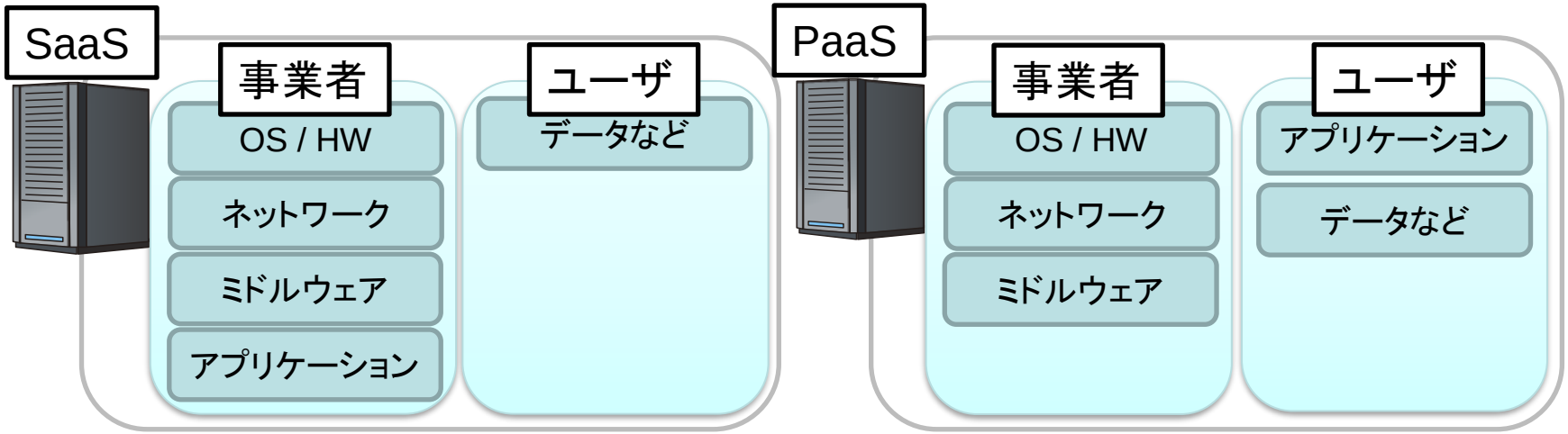
    ウェブアプリケーションファイアウォール読本
    https://www.ipa.go.jp/security/vuln/waf.html

4.その他のセキュリティ対策



4-1.サービス利用時における責任範囲の把握

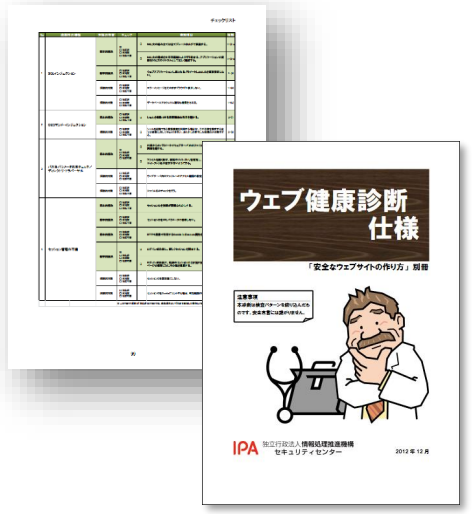
- クラウドなどのサービス利用において、自組織の責任範囲を把握していますか？
  - クラウドやホスティングサービスを利用している場合、これ以前のスライドで記載したセキュリティ対策をサービス事業者側が提供している場合があります。
  - クラウドなどのサービスを利用する場合、サービス事業者側の**作業範囲とセキュリティ対策を把握**したうえで、不足している部分は自組織で対応してください。



4-2.セキュリティ診断サービスの活用

- 定期的にセキュリティ検査（診断）、監査していますか？
  - 対策の洩れや不足が無いか確認するために、セキュリティ診断は効果的な手段となります。
  - **定期的**なセキュリティ診断・監査を**運用に組み込む**事で、新たな脆弱性や運用上の問題を洗い出すことができます。

安全なウェブサイトの作り方 チェックリスト
https://www.ipa.go.jp/files/000044465.pdf
「ウェブ健康診断 仕様」
https://www.ipa.go.jp/files/000017319.pdf



参考資料

安全なウェブサイト運営にむけて
～ 企業ウェブサイトのための脆弱性対応ガイド ～
https://www.ipa.go.jp/files/000089537.pdf

安全なウェブサイトの運用管理に向けての20ヶ条
～セキュリティ対策のチェックポイント～
https://www.ipa.go.jp/security/vuln/websitecheck.html

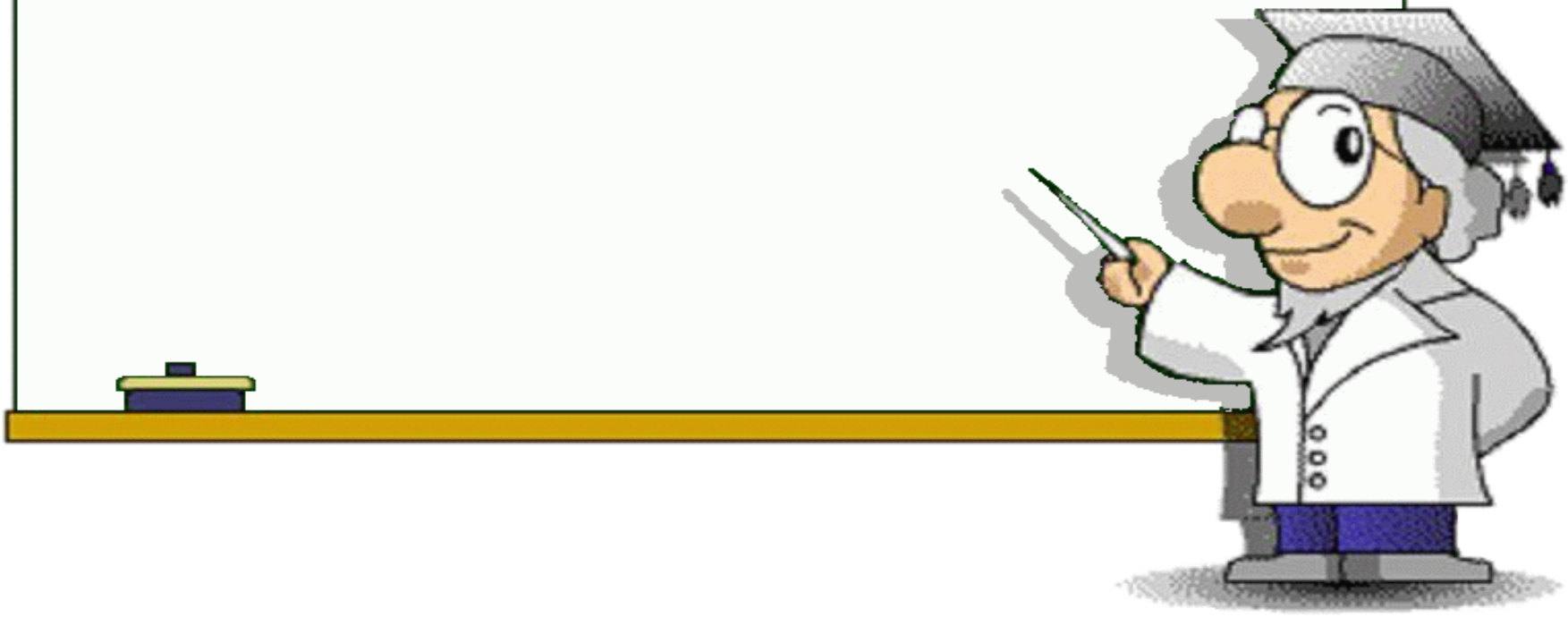
第三章 脆弱性が発見されたら

第一章 脆弱性について
第二章 対策方針について
第三章 脆弱性が発見されたら
第四章 まとめ

第三章 脆弱性が発見されたら

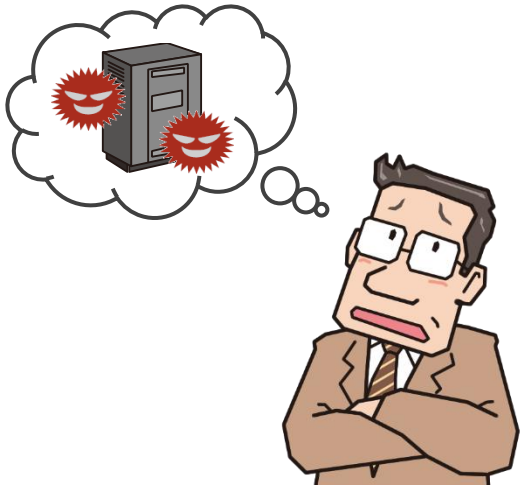
3.1 脆弱性が見つかったら？

3.2 届出制度について



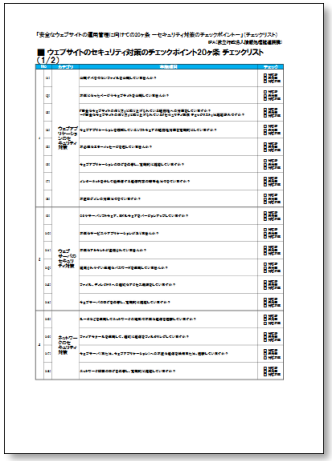
ウェブサイトに脆弱性が見つかったら？

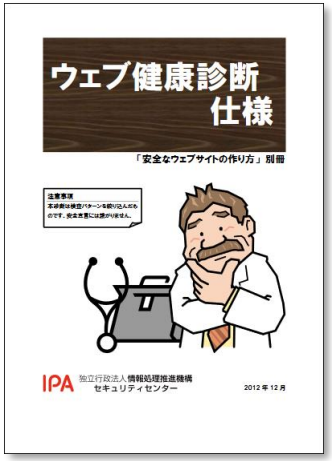
- 発見者が自社（ウェブサイト運営者）の場合
  - 自社で気づき、脆弱性を修正
- 発見者が第三者の場合
  - 第三者から直接連絡があって気づき、脆弱性を修正
  - 第三者が IPA に報告し、IPA から連絡があって気づき、脆弱性を修正



発見者が自社の場合（１）
自社で調査

- IPA の資料や診断サービスの結果をもとに、脆弱性の有無を確認
  - 「ウェブサイトのセキュリティ対策のチェックポイント 20 ヶ条」
    https://www.ipa.go.jp/files/000070296.xlsx
  - 「ウェブ健康診断 仕様」
    https://www.ipa.go.jp/files/000017319.pdf
  - 「5 分でできる！情報セキュリティ自社診断」
    https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html



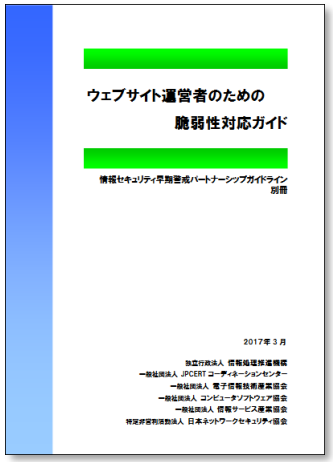


発見者が自社の場合（１）
自社で修正・対応

- 脆弱性を発見した場合は、以下の資料を参考に修正
  - 「安全なウェブサイトの作り方」
    https://www.ipa.go.jp/security/vuln/websecurity.html

    脆弱性を修正する方法や開発時に注意すべきセキュリティ対策など、
    代表的な 11 の脆弱性を解説
  - 「ウェブサイト運営者のための脆弱性対応ガイド」
    https://www.ipa.go.jp/files/000058492.pdf

    ウェブサイトの脆弱性を扱う上で、組織としてどう対応するか解説

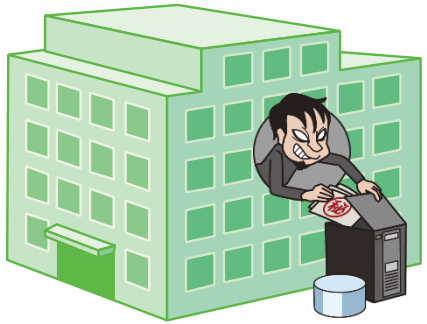


発見者が自社の場合（２）
外部からの攻撃について、調査・対応

- 状況を確認
  - 攻撃による損害の有無
    ネットワークを流れる通信を確認（現在の状況の把握）
    ログに蓄積したデータを確認　　（過去の状況の把握）
  - 利用者への影響の有無とその範囲

↓

- 攻撃が継続している または 修正に時間を要する場合
  - 一時的な緩和策を実施（不正な通信の遮断，WAF や IDS の導入など）
- 実害に発展している場合
  - 利用者や関係各所への連絡
  - システムの復旧 または サービスの一時停止
  - 利用者への対応の検討



発見者が自社の場合（２）
外部からの攻撃について、相談

- 自社で対処することが難しい場合は、専門家に相談
  - セキュリティベンダー
    情報セキュリティサービス基準適合サービスリストの公開
    https://www.ipa.go.jp/security/it-service/service_list.html
  - IPA
    情報セキュリティ対策支援サイト
    https://security-shien.ipa.go.jp/
    情報セキュリティ安心相談窓口
    https://www.ipa.go.jp/security/anshin/
  - JPCERT/CC
    インシデント対応依頼
    https://www.jpcert.or.jp/form/

発見者が第三者の場合
第三者からの連絡をもとに、修正・対応

- 届出の内容を把握
  - 脆弱性情報を確認

↓

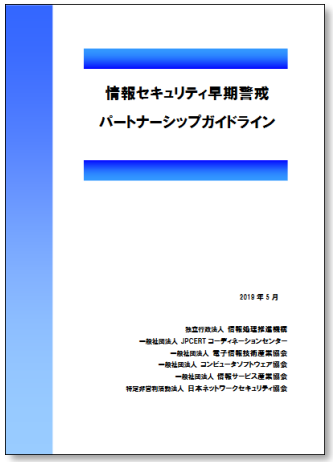
- 脆弱性が再現するか確認
  - 再現手順を把握
  - テスト環境で確認

↓

- 再現する場合は、IPA の資料を参考に修正・対応
  - 「安全なウェブサイトの作り方」
  - 「ウェブサイト運営者のための脆弱性対応ガイド」

IPA がおすすめする対応

- 「情報セキュリティ早期警戒パートナーシップ」の枠組みを活用
  - 「情報セキュリティ早期警戒パートナーシップガイドライン」
    https://www.ipa.go.jp/files/000073901.pdf



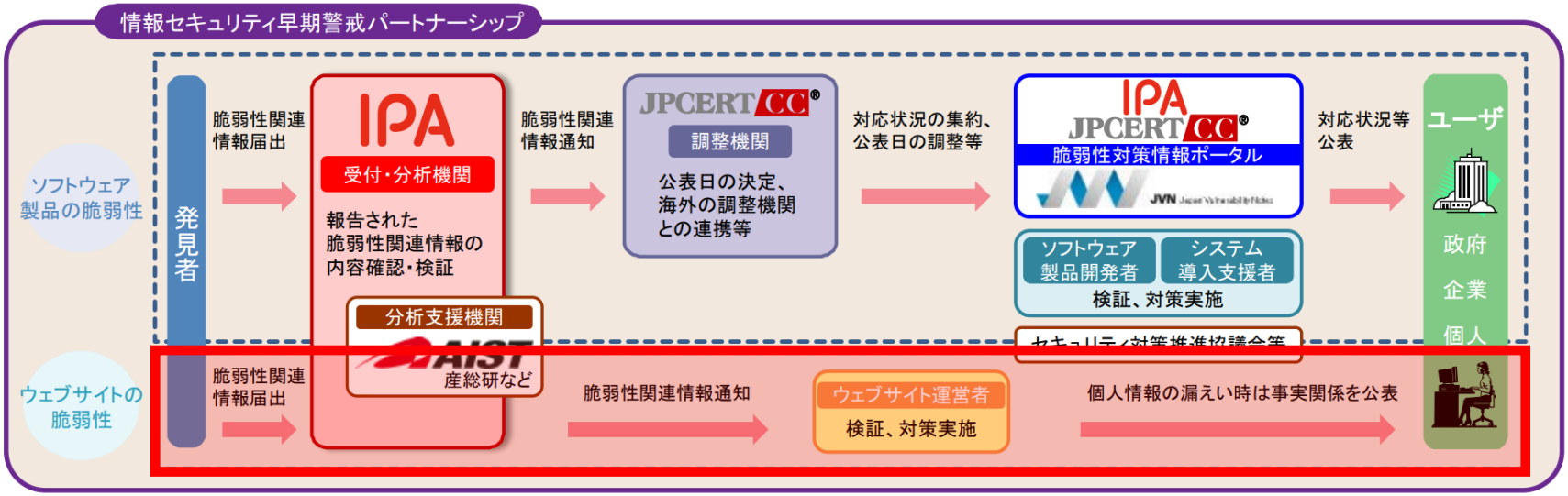
第三章 脆弱性が発見されたら

3.1 脆弱性が見つかったら？

3.2 届出制度について

「情報セキュリティ早期警戒パートナーシップ」の紹介

- 脆弱性の発見から対策までを当事者間で相互に連携して対応
  - 「情報セキュリティ早期警戒パートナーシップガイドライン」
    https://www.ipa.go.jp/security/ciadr/partnership_guide.html
  - 「平成 29 年経済産業省告示第 19 号」
    http://www.meti.go.jp/policy/netsecurity/vul_notification.pdf



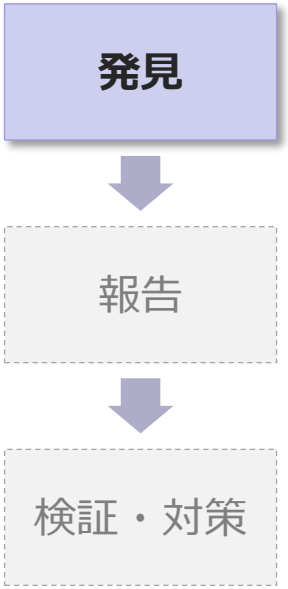
※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

ウェブサイトの脆弱性に関する対応

- **発見**：発見者（第三者）
  ↓
- **報告**：発見者 → IPA → ウェブサイト運営者
  ↓
- **検証・対策**：ウェブサイト運営者
  ↓
- **報告**：ウェブサイト運営者 → IPA → 発見者

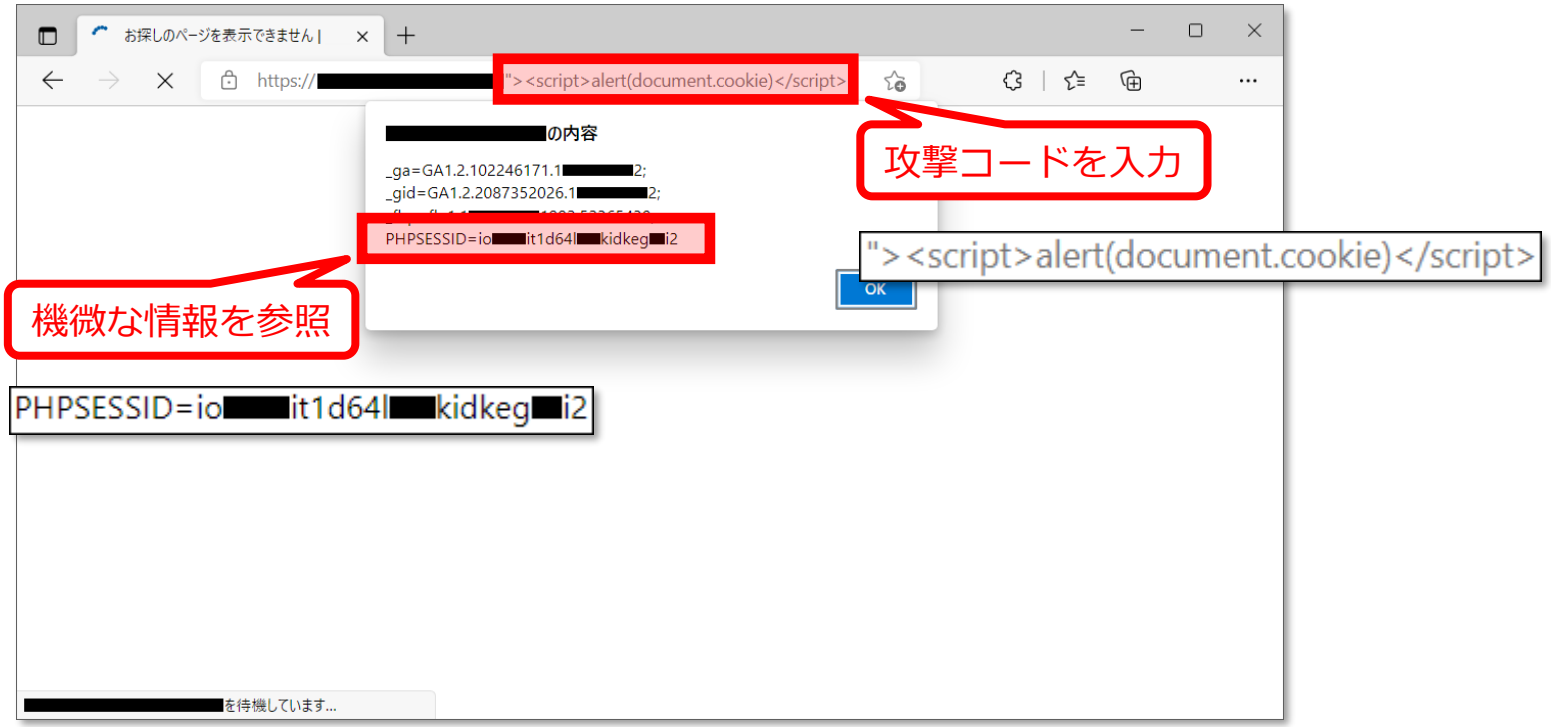
※ウェブサイト運営者が対策を実施することで、届出の取扱が完了します。
ただし、情報漏洩などの実害が発生した場合は、別途対応が必要です。

「発見」の段階で実施すること

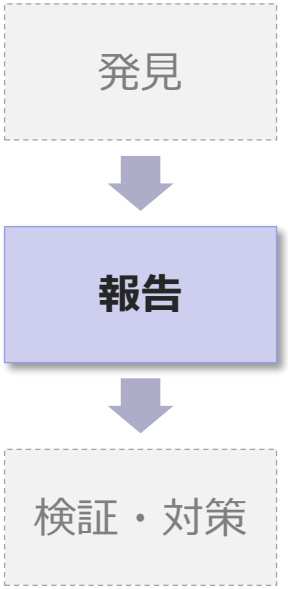


- だれが？
  - 発見者
- どうする？
  - 脆弱性情報を入手・整理
    - 脆弱性の種類を特定
      クロスサイト・スクリプティング（XSS）
      SQL インジェクション
      など
    - 脆弱性による影響を判断
    - 脆弱性を再現させるための条件や手順を確認
    - 検証コード，証跡，ログファイルを取得
      攻撃コード（攻撃用のスクリプトやコマンド）
      画像 および 動画
      など

(参考)
XSS の証跡の例



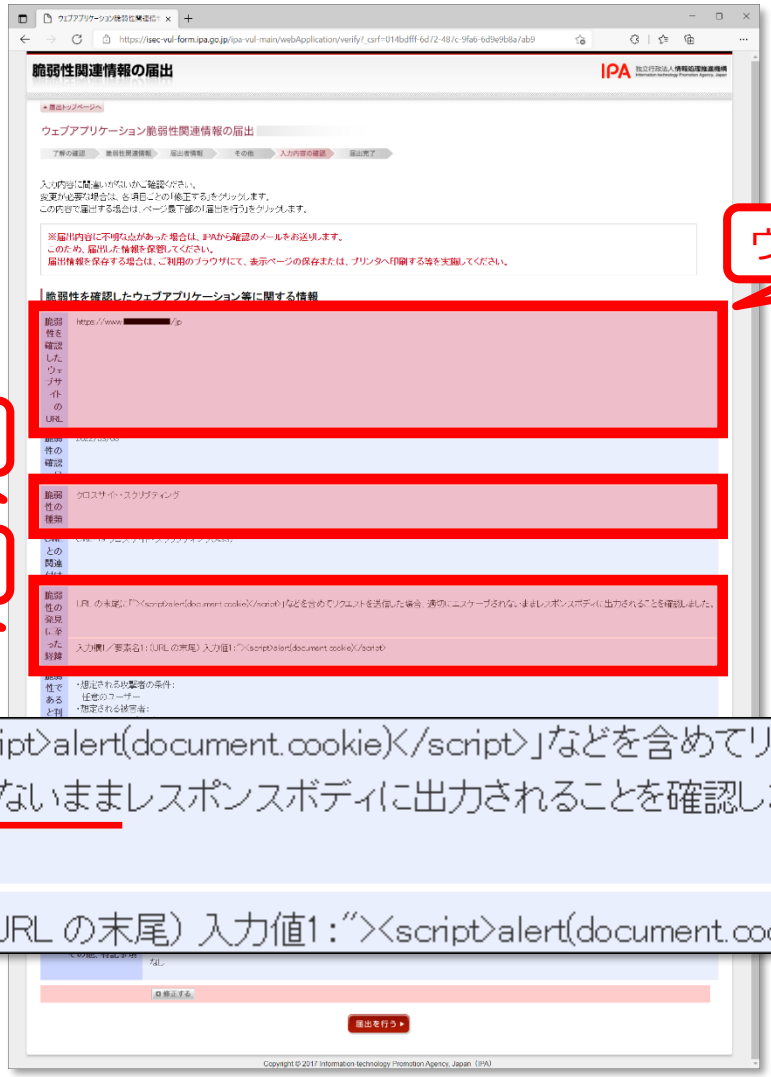
「報告」の段階で実施すること



- だれが？
  - 発見者
  - 第三者機関（IPA）
  - ウェブサイト運営者
- どうする？
  - 脆弱性情報を報告
    - 脆弱性を検証するために必要な情報を送付
      攻撃コード，画像・動画，ログファイルなど
    - 届出フォーム／電子メールから報告
      ウェブアプリケーション脆弱性関連情報の届出
      https://isec-vul-form.ipa.go.jp/ipa-vul-main/index.html
      ※電子メールから報告する場合は、届出の様式（テンプレート）に従って記入・送付します。
    - IPA 経由で脆弱性情報を受領

（参考）
脆弱性関連情報の届出

（参考）
脆弱性関連情報の届出の記入例



ウェブサイトの URL

脆弱性の種類

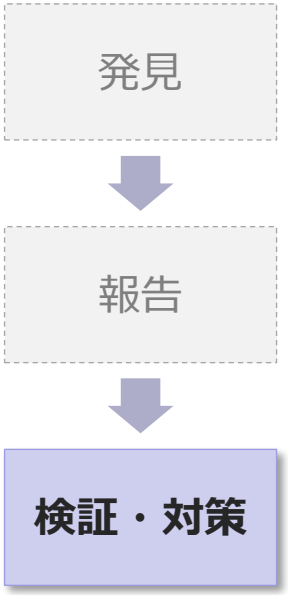
脆弱性の再現手順

URL の末尾に「"><script>alert(document.cookie)</script>」などを含めてリクエストを送信した場合、適切にエスケープされないままレスポンスボディに出力されることを確認しました。

入力欄1／要素名1：(URL の末尾) 入力値1："><script>alert(document.cookie)</script>

脆弱性の原因

「検証・対策」の段階で実施すること



- だれが？
  - ウェブサイト運営者
- どうする？
  - 脆弱性情報をもとに検証
    - 脆弱性が再現することを確認

      ※再現が確認できない または 適切な対策が策定できない場合は、発見者に確認する必要があります。
    - 脆弱性に関する対策を検討

      根本的解決

      保険的対策・回避策

ウェブサイト運営者の役割

- 利用者や利害関係者に対する被害を発生させない
- 脆弱性が見つかった場合は、当事者間で相互に連携し、速やかに対応する
- 脆弱性情報の取扱には十分に注意する
- 脆弱性を修正する際は、新たな脆弱性を埋め込まない

参考資料

- PDF
  - ウェブサイト運営のファーストステップ
    ～ ウェブサイト運営者がまず知っておくべき脅威と責任 ～
    https://www.ipa.go.jp/files/000071949.pdf
  - ウェブサイト運営者向け「セキュリティ問い合わせ窓口設置」の手引き
    https://www.ipa.go.jp/files/000096758.pdf
- 動画
  - 脆弱性の発見から対策実施までの流れ
    「脆弱性発見・報告のみちしるべ」動画シリーズ
    https://www.youtube.com/watch?v=sjbVlQPpEuw
  - 被害にあわないウェブサイト運営に向けて（前編）
    - ウェブサイトを取り巻く脅威
    https://www.youtube.com/watch?v=jjY0EcuST8M
  - 被害にあわないウェブサイト運営に向けて（後編）
    - ウェブサイトで実施すべき対策
    https://www.youtube.com/watch?v=ipBqS4C4KUU

第四章 まとめ

第一章 脆弱性について
第二章 対策方針について
第三章 脆弱性が発見されたら
第四章 まとめ

まとめ

- 「脆弱性」とはなにか、実際に被害が発生した事例を交えつつ解説
- ウェブサイト運営者が実施するべき基本的な対策について解説
- 運用しているウェブサイトで、脆弱性が発見された際の対応方法を解説

isec-labsemi-vul@ipa.go.jp

- 本セミナーに関するお問い合わせは、上記までご連絡ください。