IPA Better Life with IT

2019 暗号と情報セキュリティシンポジウム
MWS/CWS合同企画セッション(1)

脆弱性届出制度における受付窓口対応

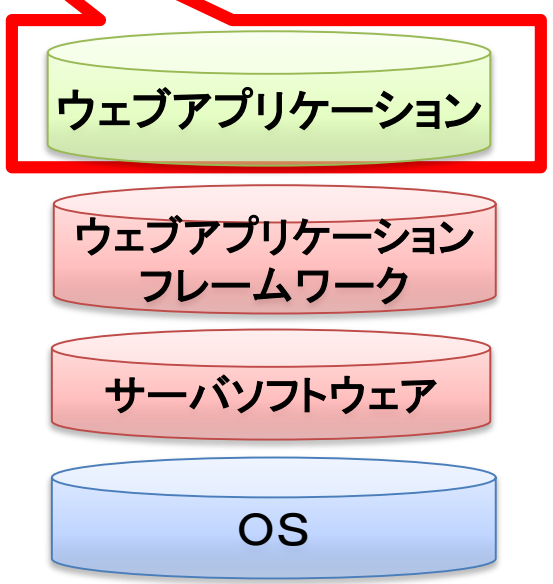
2019年1月24日

独立行政法人情報処理推進機構（IPA）
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リーダー　渡辺 貴仁

届出の範囲（ウェブアプリケーションの届出）

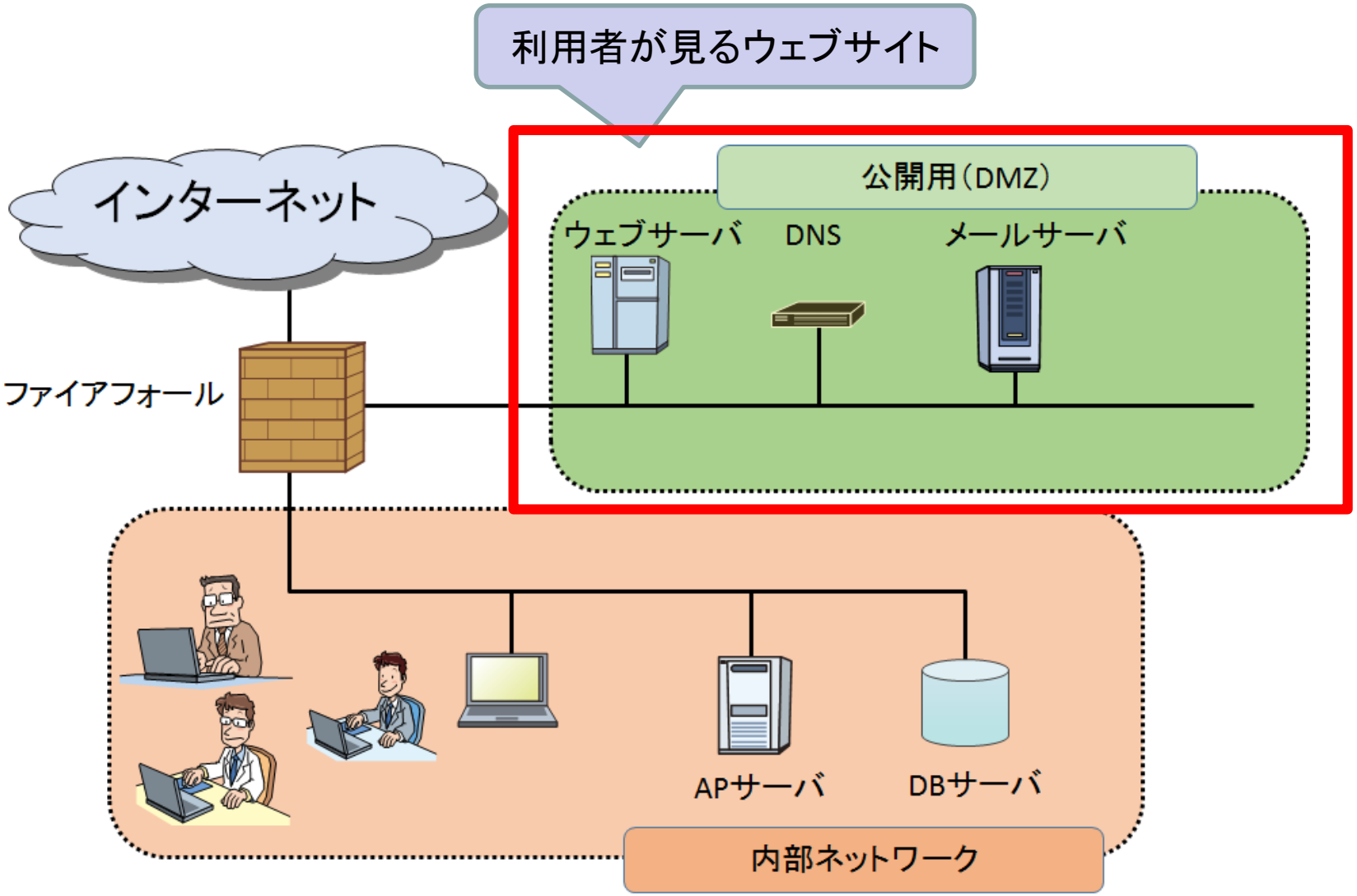
- イメージは**ウェブサイト**に存在する脆弱性
  - ウェブサイトにおけるウェブアプリケーションの脆弱性
    （例）XSS、SQLインジェクションなど
  - ウェブサイトの不適切な運用
    （例）
    - 脆弱性なソフトウェアを使用
    - アクセス制御が不適切
    - DNSまわり

    など



そもそも公開設定が不適切なケースも多い

届出の範囲（ウェブアプリケーションの届出）



届出の範囲（ソフトウェア製品の届出）

- 有償製品、無償製品。工場等で使用される製品も
  - クライアント上のソフト
    - OS、ブラウザ、メーラー等
  - サーバ上のソフト
    - CMS、PHP、Apache 等
  - ハードウェア（組み込み）
    - ルーター、プリンタ等
  - 制御システム用製品

CMS関連の製品や家庭用ルータの届出も増えている

届出の記載の注意点

1. 対応する人間は皆が技術者とは限らない
   - 脆弱性の報告を受ける人と開発者が別の可能性がある
     - 知識に差がある
     - 発見者の当たり前は相手の当たり前ではない
2. 再現手順をわかりやすく記載
   - ウェブサイト運営者・製品開発者が再現検証や脆弱性とするか判断をするために大事なこと
     - 調査をすると、脆弱性を悪用しても攻撃者に付与された権限以上操作ができない場合がある
   - 攻撃者および被害者の操作を明確にして具体的な攻撃手順を書く
     - 特に製品のSQLインジェクションやバッファオーバーフローの脆弱性は、実際に情報の漏洩や任意コードの実行が可能となることを確認する

届出の記載の注意点

3. 脆弱性と判断した理由
   - 特に、マニュアル等の明確な根拠が良い
4. 脆弱性により発生しうる脅威
   - 脆弱性が悪用されてしまうと、機密性・完全性・可用性に対して、どのような影響が出ることが予想されるか、分かる範囲で具体的に記載し、脅威を明確にする

ウェブサイトの脆弱性発見する際の注意点

1. 他人のアカウントでアクセスすることはしない
   - たとえ、認証回避の脆弱性があっても実践しない
2. SQLインジェクションを試さない
   - 場合によってはウェブサイトの大事なデータを削除してしまう可能性
3. ツールを使用して勝手に脆弱性検査をしない
   - 場合によってはウェブサイトが停止してしまう可能性
4. インターネット上に公開されていないファイルにはアクセスしない
   - ディレクトリ・トラバーサル

危険な調査をやり過ぎてしまうことがある

ソフトウェア製品の脆弱性発見する際の注意点

1. インターネット上で発見しない
   - 仮想環境など安全な環境で検証する
   - 誤ってインターネットへ出て行かぬよう十分な配慮を
2. ソフトウェア利用許諾契約違反とならぬよう
   - 利用許諾されているソフトウェアを対象に
   - 利用条件を守るように
     - 複製禁止
     - リバースエンジニアリング禁止