Expand - Collapse

- Sec01-05
  サイバーセキュリティ対策普及啓発教材
  【素材】
  - 【2017年8月9日】
  - 情報セキュリティ
    - サイバーセキュリティ
      - 標的型メール
      - 攻撃者ウェブサイト
    - 物理セキュリティ
      - セキュリティ区画
      - PC、媒体の紛失、盗難
  - 攻撃方法
    - 無差別攻撃
    - 標的型攻撃
      - 標的型メール
      - 攻撃者ウェブサイトへ誘導
    - マルウェアに感染
  - 攻撃手順
    - 標的の探索
      - 無差別探索
    - 標的へのアプローチ
      - 標的型メール
      - 攻撃者ウェブサイトへ誘導
    - 標的への攻撃準備
      - バックドア設置
      - マル不正プログラム設置
      - 感染先拡大
    - 標的への攻撃
      - 情報搾取
      - 情報破壊
  - ケース
  - フィッシングページによる情報搾取
    - ユーザ
    - 改ざんされたWebサイト
    - 犯罪者サイト
    - 犯罪者
  - 脆弱性攻撃サイトへの誘導
    - ユーザ
    - 改ざんされたWebサイト
    - 犯罪者サイト
    - 犯罪者
  - CMSの脆弱性を狙ったサイバー攻撃
    - 初期侵入

Expand - Collapse

- •サイバー犯罪者はCMSに発覚した脆弱性を狙って攻撃を仕掛ける

⊟ バックドア設置
- •脆弱性を悪用してバックドアをWebサーバの特定ディレクトリに設置する

⊟ 侵入拡大
- •サイバー犯罪者は設置したバックドアを利用して、Webサーバ上で任意のコマンドを実行する

⊟ 踏み台
- •Webサーバから外部のアドレスにスパムメールを大量送信する

⊟ CMS プラグインの脆弱性を狙ったサイバー攻撃

⊟ 初期侵入
- •Movable Typeのプラグイン「ケータイキット for Movable Type」のゼロデイ脆弱性を狙って攻撃を仕掛ける

⊟ バックドア設置
- •OSコマンドインジェクション攻撃を試みて、バックドアをWebサーバに設置する

⊟ 侵入拡大
- •サイバー犯罪者は設置したバックドアを利用して、Webサーバ上でコマンドを実行する

⊟ 踏み台
- •システム内部のデータを探索し、コピー・圧縮したデータを外部のサイバー犯罪者が管理するサーバに送信する

⊟ FW をすり抜けてWeb サイトの脆弱性が狙われる
-

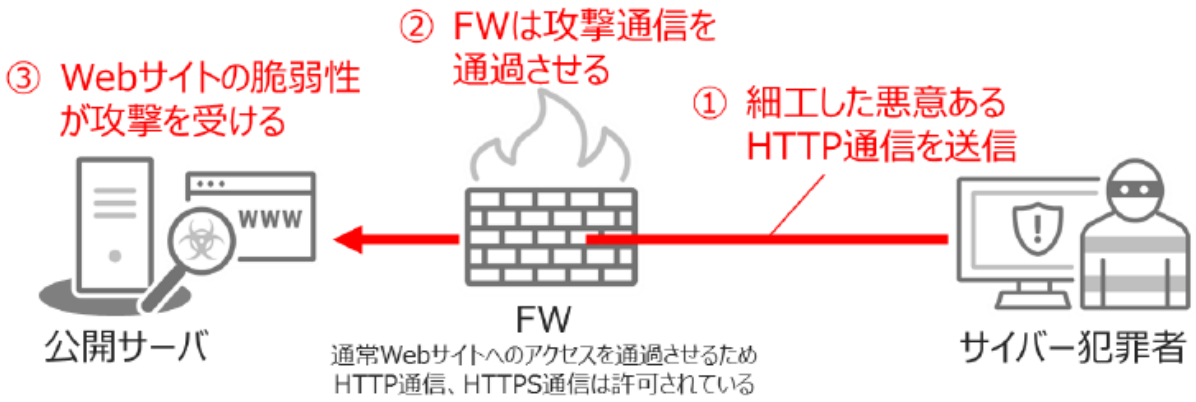

図６：FW をすり抜けて Web サイトの脆弱性が狙われる

⊟ 複数のセキュリティ対策をすり抜けて不正アクセスの被害に

Expand - Collapse

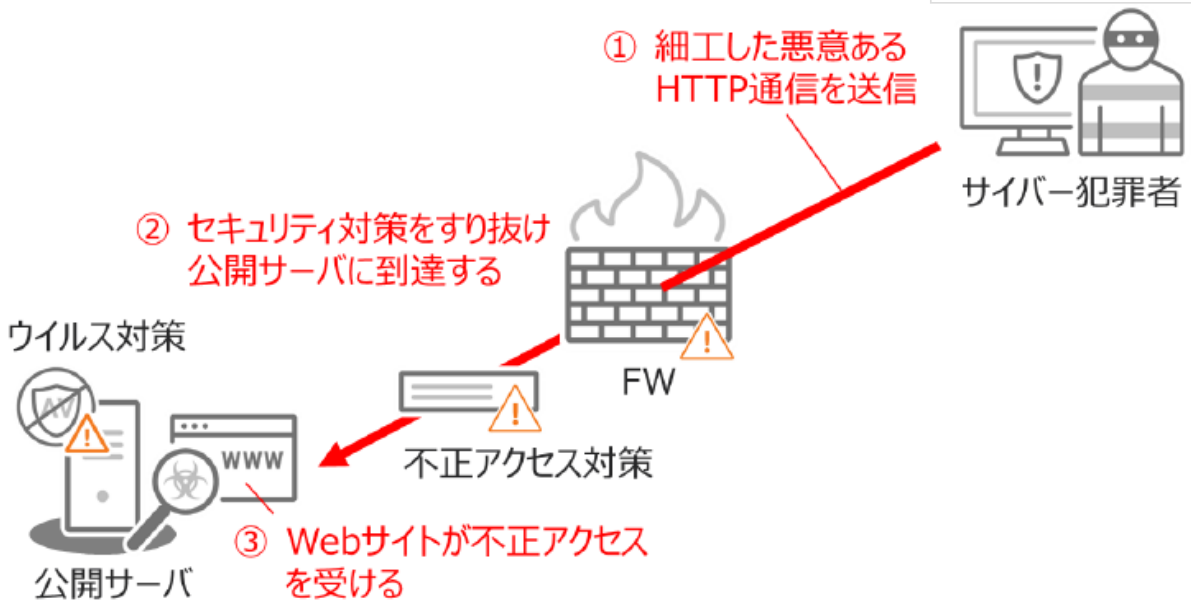

図７：複数のセキュリティ対策をすり抜けて不正アクセスの被害に

- SQL インジェクションの攻撃
  - 標的探索
    - サイバー犯罪者は、ツールなどを用いて脆弱性が存在する可能性があるWeb サイトを探索する
  - 調査行為
    - 標的のWebサイトを定め、入力データを細工したHTTPリクエストを送信し、サーバからのレスポンスをもとにSQLインジェクションの攻撃が可能かを判断する
  - 情報搾取
    - 本格的にSQLインジェクションの攻撃を仕掛け、データベース（DB）内の情報窃取を試みる
  - DB破壊
    - 最後にSQLインジェクションの攻撃によって、データベース内のデータ書換えやデータ削除といった破壊活動を実施する
- インジェクション攻撃による情報漏えい
  - 標的探索
    - サイバー犯罪者は、ツール等を用いて脆弱性が存在する可能性があるWebサイトを探索する
  - 調査行為
    - 標的のWebサイトを定め、入力データを細工したHTTPリクエストを送信し、サーバからのレスポンスをもとにインジェクション攻撃が可能かを判断する
  - バックドア
    - 本格的に脆弱性を悪用したインジェクション攻撃を仕掛け、バックドアを公開サーバ内に設置する
  - 侵入拡大
    - サイバー犯罪者はバックドアを利用し、サーバ内の情報を探索、収集する
  - 情報搾取
    - 収集した情報を圧縮し、外部のサイバー犯罪者が準備したサーバに送信する