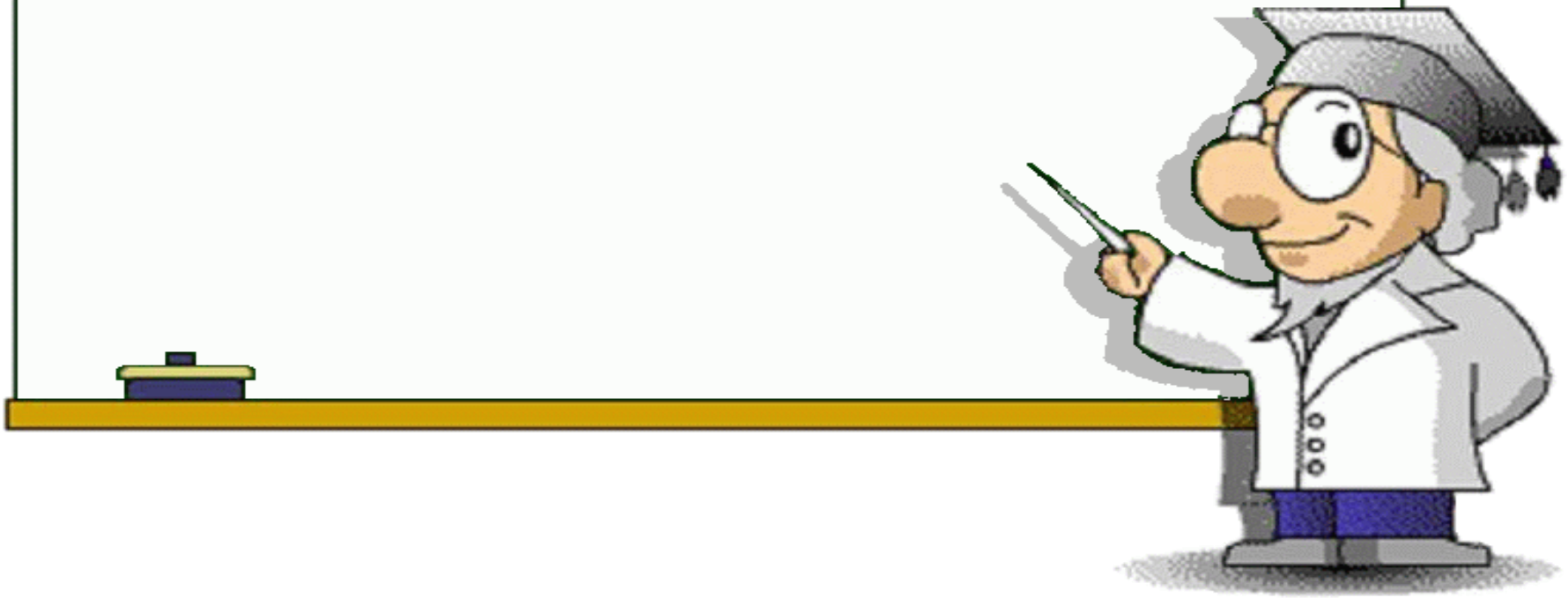
IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

4. 安全なウェブサイト運営のためのWAF
～ 脆弱性を悪用する攻撃を防ぐために ～

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
情報セキュリティ技術ラボラトリー

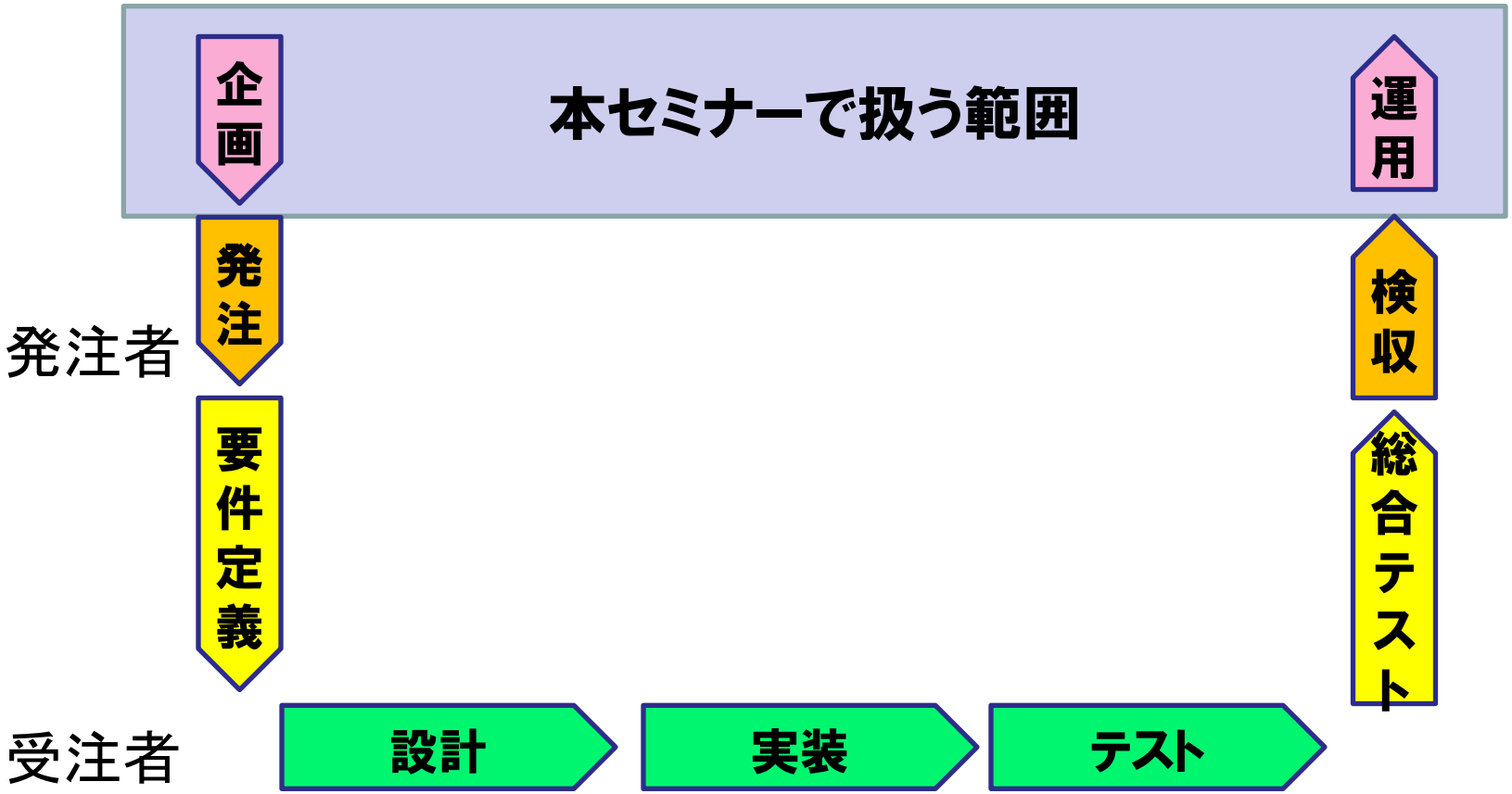
2010年12月6日公開

目次

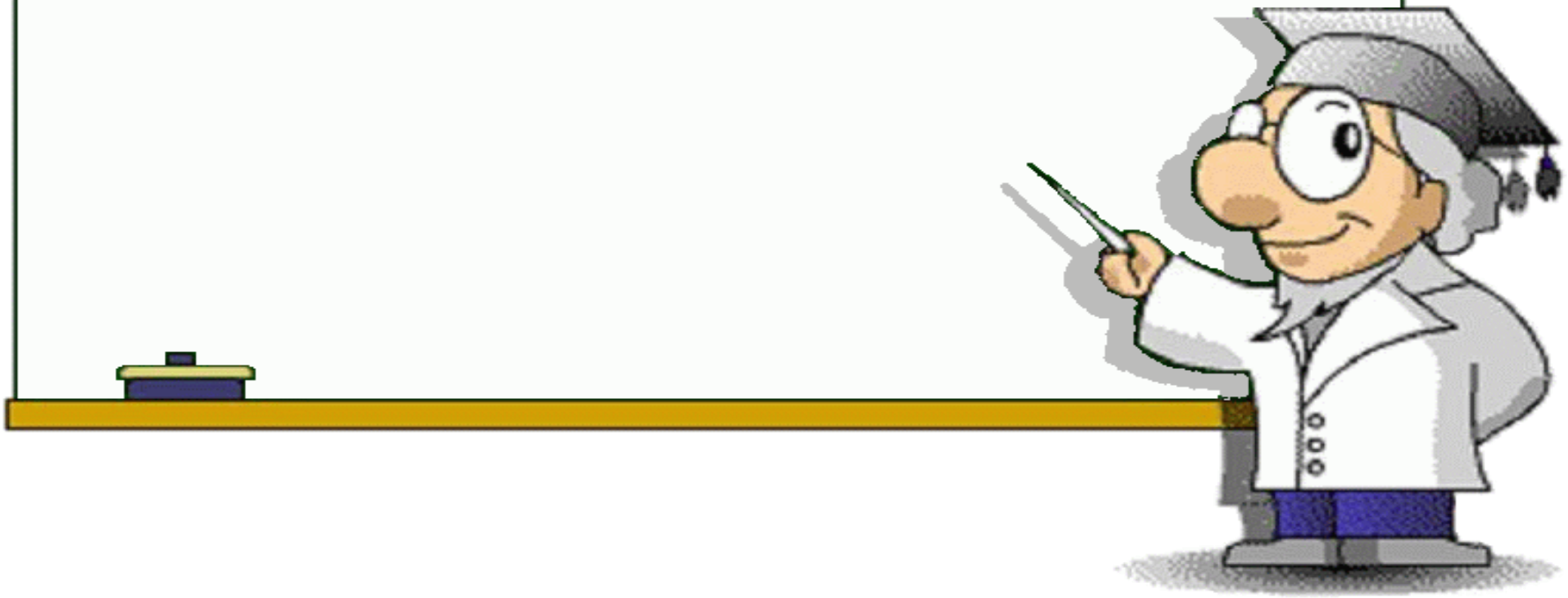


はじめに：本セミナーで扱う範囲

ウェブサイト開発の流れ



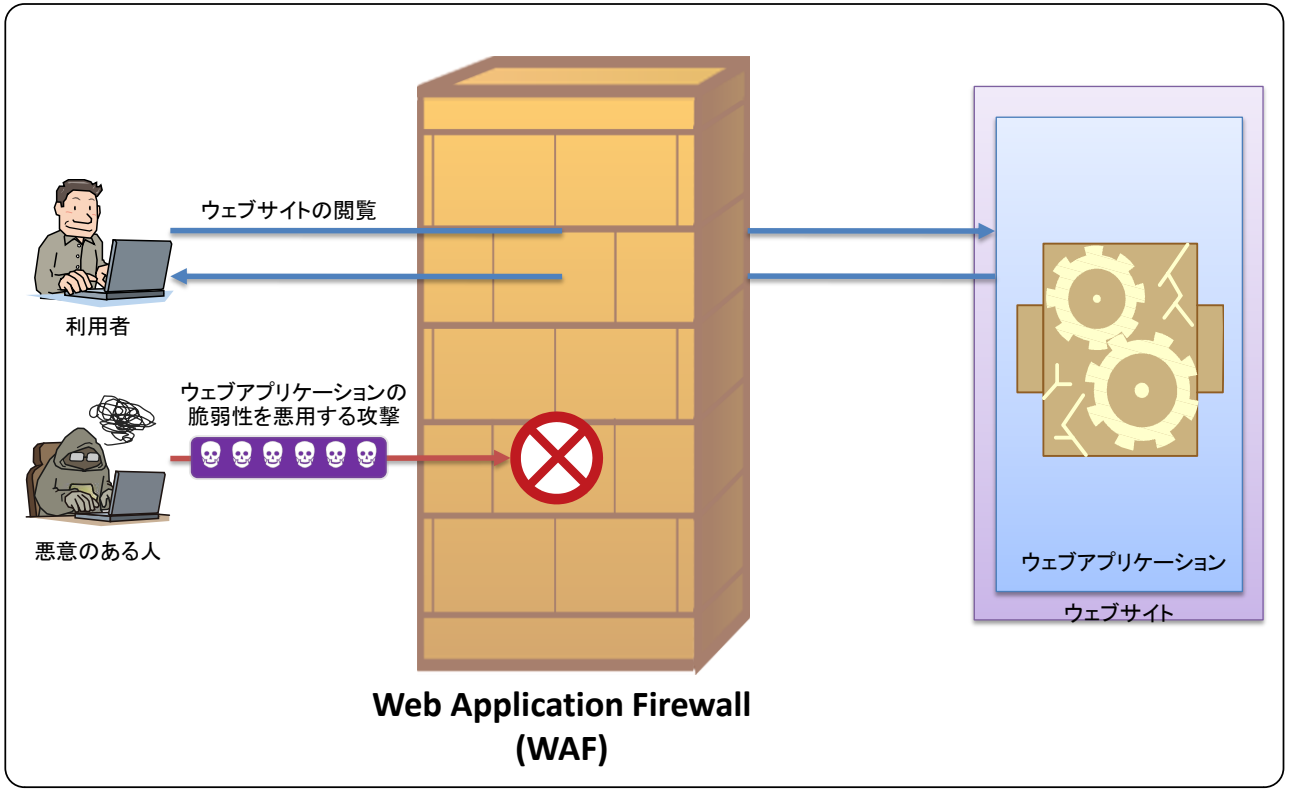
1. はじめに：本セミナーで扱う範囲
2. WAFとは
3. WAFの導入におけるポイント
4. まとめ



WAFとは

- **WAF（Web Application Firewall）**

  ウェブアプリケーションの脆弱性を悪用した攻撃などからウェブアプリケーションを保護するソフトウェア、またはハードウェア



WAFで攻撃を防御する
～検出パターンに基づいた検査～

- **ブラックリスト**

  ―ブラックリストとは
  - **「不正な値、またはパターン」をブラックリストとして定義**
  - **ブラックリストに合致したときに、不正な通信として検出**

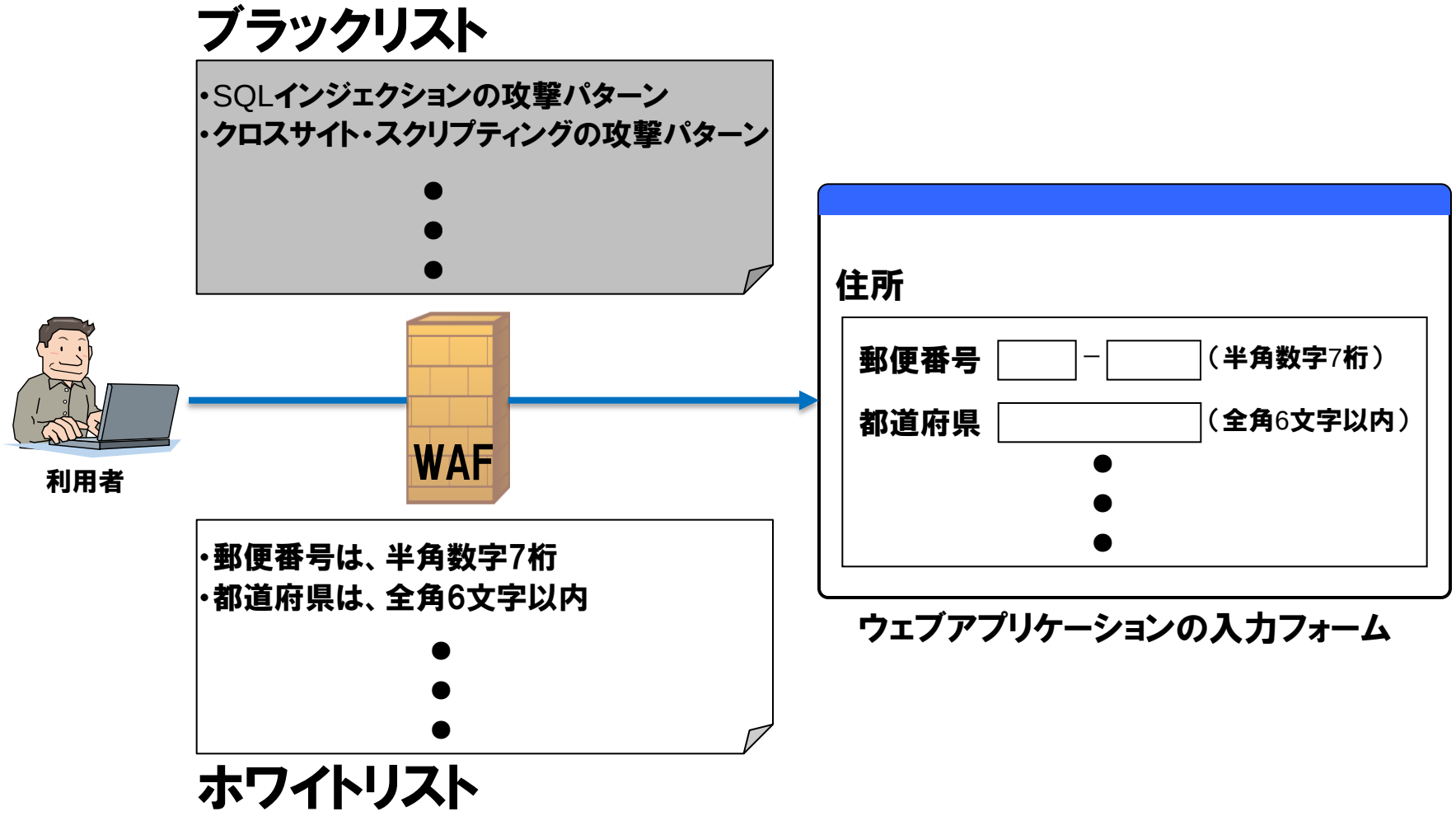
  ―特徴
  - **検査の性能はブラックリストの精度に依存**
  - **攻撃側の視点で作成されるため、ウェブアプリケーションの作りに依存なし**

- **ホワイトリスト**

  ―ホワイトリストとは
  - **「正しい値、またはパターン」をホワイトリストとして定義**
  - **ホワイトリストに合致しないときに、不正な通信として検出**

  ―特徴
  - **ホワイトリストを定義しているパラメータは未知の攻撃にも対応可能**
  - **ウェブアプリケーションの作りに依存**

WAFで攻撃を防御する
～ブラックリスト、ホワイトリストの違い～



WAFが有効な場面

- **多層防御**

  ウェブサイト全体のセキュリティ強化

  - **各ウェブアプリケーションの品質に依存しない均一的なセキュリティの確保**
  - **最新の攻撃パターンへの対応**

- **脆弱性を悪用した攻撃への対応**

  ウェブアプリケーションに脆弱性があった場合、その脆弱性を悪用した攻撃への対応

  - **ウェブアプリケーションの開発者がいない場合でも対策を検討する時間ができる**
  - **オープンソースソフトウェアの脆弱性等、独自に対応が難しい状況でもパッチ提供を待つことができる**

WAFを導入すれば、脆弱性対策はばっちり！

WAFが有効な場面
～望ましい脆弱性対策との関連～

- **ウェブアプリケーションに脆弱性を作りこまない**

  開発段階でプログラムに脆弱性を作りこまないよう、開発者向けの資料を公開

  - **「安全なウェブサイトの作り方」、「安全なSQLの呼び出し方」**
  - **「セキュア・プログラミング講座」**

- **脆弱性の修正**

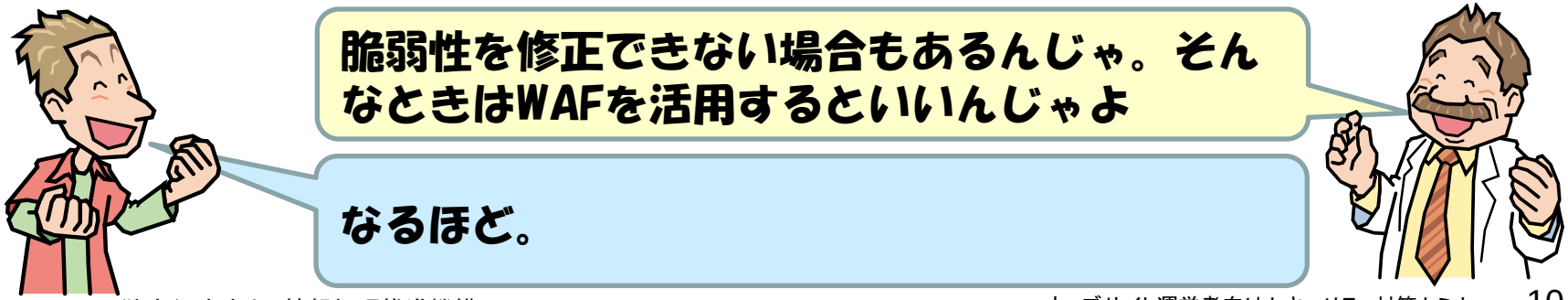
  『情報セキュリティ早期警戒パートナーシップ』による脆弱性関連情報の円滑な流通、及び対策の普及

  - **「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」**
  - **「ウェブサイト運営者のための脆弱性対応ガイド」**

脆弱性は作らない、あれば修正するが第一！

WAFが有効な場面
～脆弱性を修正できない場面～

- 脆弱性を修正できない要因
  - 開発者がいない
  - 修正方法が分からない
  - 長期間サービスをとめることができない
  - 修正するための予算がない



【参考】Web Application Firewall（WAF）読本

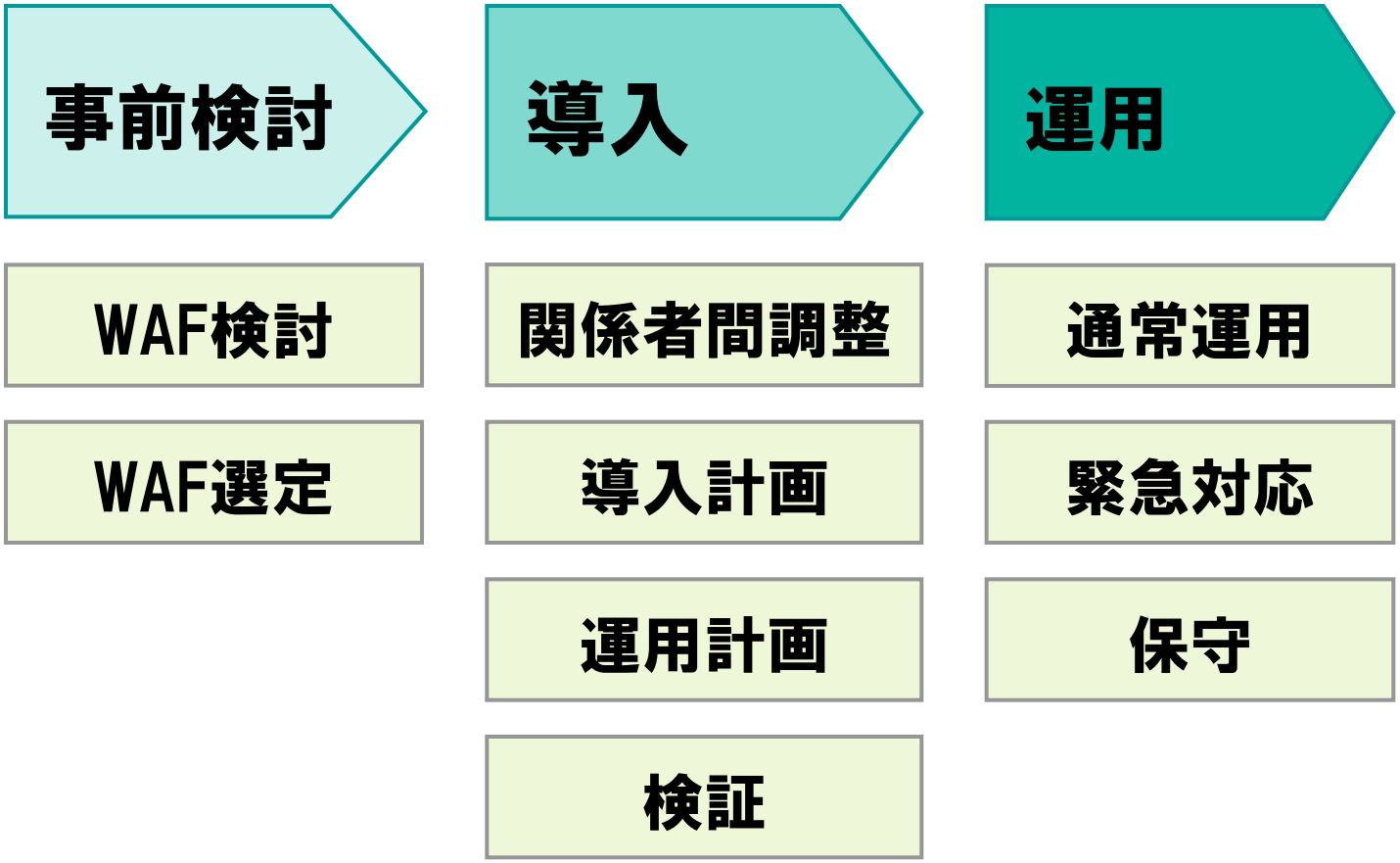
http://www.ipa.go.jp/security/vuln/waf.html

攻撃による影響を低減。

- WAFの動作概要、機能詳細、導入におけるポイントをまとめた手引書
- 各機関におけるWAFの取り組みの紹介を記載
- 「WAF」がどのような物であるかについて概要を記載
- 「WAF」の機能説明、機能の留意点を記載
- 「WAF」導入の際の各フェーズにおけるポイントを記載

1. はじめに：本セミナーで扱う範囲
2. WAFとは
3. WAFの導入におけるポイント
    3.1. 事前検討
    3.2. 導入
    3.3. 運用
4. まとめ

WAFの導入におけるポイント



1. はじめに：本セミナーで扱う範囲
2. WAFとは
3. WAFの導入におけるポイント
    3.1. 事前検討
    3.2. 導入
    3.3. 運用
4. まとめ

事前検討：WAF検討

- **WAFを導入すべきか？**

ーウェブアプリケーションの修正は可能か？

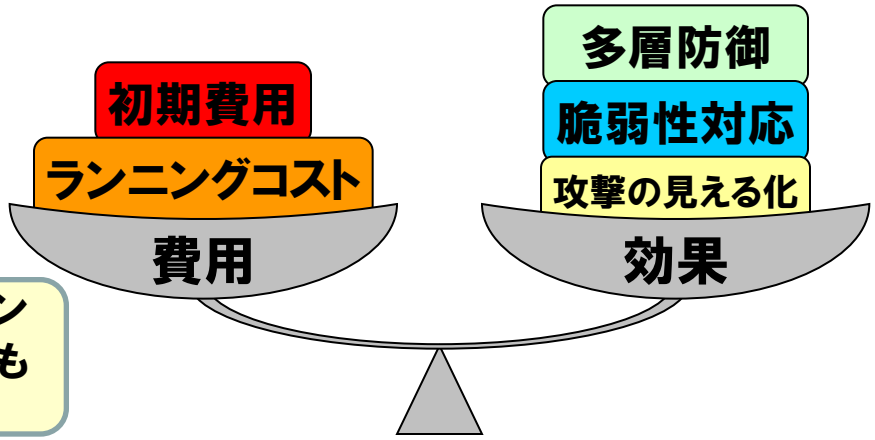
万一脆弱性が発見された場合、開発者の不在などによるウェブアプリケーションの修正が不可能な状況はないか

ーどんな攻撃をWAFで防御したいのか？

防御したい攻撃をWAFで防御できるのか

ーコストは？

WAFを導入した場合の
費用対効果



WAFを導入せずに、ウェブアプリケーションを修正した場合の費用とリスクについても検討が必要

攻撃による影響を低減するためにWAFを導入するのがベスト

【参考】WAFで防御できない攻撃

- **ウェブアプリケーションにおける認可制御の欠落**

  例えば、ウェブアプリケーションにおける認可制御に問題があり、特定の利用者だけ許可する機能がそれ以外の利用者にも使用できるというような脆弱性については対応できない

論理設計上のバグは基本的にWAFでは防御できない！

事前検討：WAF選定

- どのWAFを導入するか？
  - ー予算
  - ーウェブサイトの構成
    - 自社にウェブサイトを設置
    - ハウジングを利用
    - ホスティングを利用
    - etc
  - ーウェブサイトの性能
    - 単位時間当たりのパケット数
    - CPUやメモリの使用量
  - ーWAFの機能・性能
    - 検査機能
    - 管理機能（ユーザインタフェース）
    - 防御対象
    - 耐障害性
    - etc

導入するWAFの導入形態の決定

導入するWAF製品の決定

運用まで意識したWAFの選定が重要

【参考】WAFの種類

- **「オープンソースソフトウェア」のWAF**

  オープンソースソフトウェアのWAFには以下の特徴がある。

  - **ライセンスに従えば無償で利用可能**
  - **サポートサービスがない（ウェブサイト運営者自らがWAFの導入から運用まで行なう必要がある）**
  - **マニュアルが充実していない（WAFに関する深い知識が要求される）**

- **「商用製品」のWAF**

  商用製品のWAFには以下の特徴がある。

  - **WAF製品自身に対して費用が発生する**
  - **サポートサービスが充実している**
  - **WAFに関する深い知識を必ずしも要求されない**

【参考】WAFの設置

●ネットワークに設置

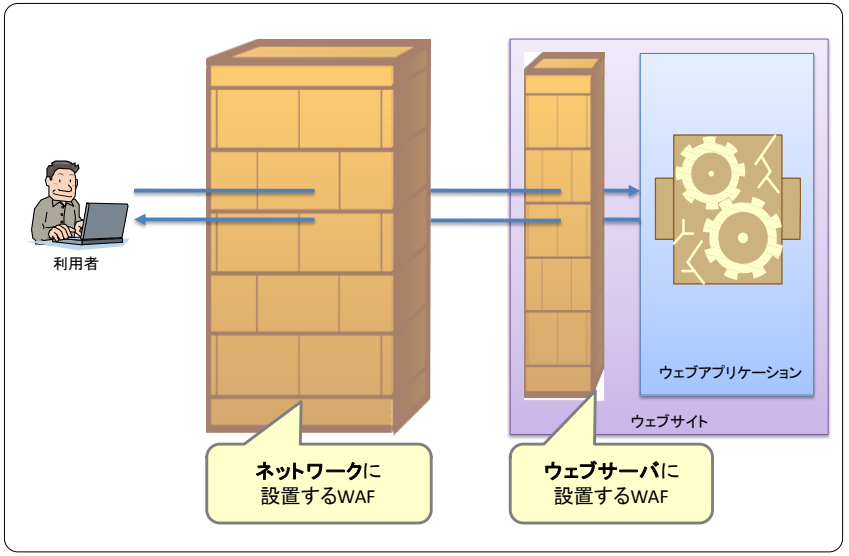
ネットワークに設置するタイプのWAFには以下の特徴がある。

- **ウェブサイトの動作環境、ウェブサーバの台数に依存しない**
- **ネットワーク構成を見直す必要がある**
- **可用性低下の可能性がある**

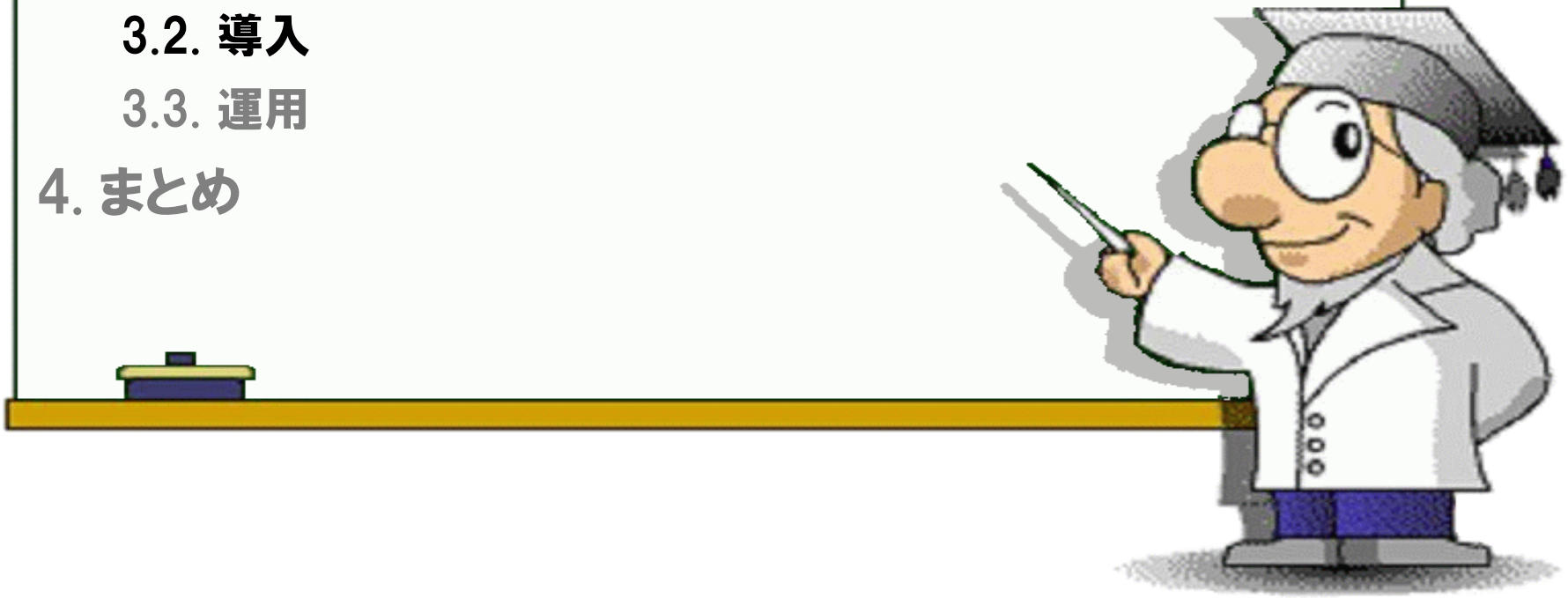
●サーバに設置

サーバに設置するタイプのWAFには以下の特徴がある。

- **ウェブサイトの動作環境、サーバ台数に依存する**
- **ネットワーク構成に影響しない**
- **可用性低下の可能性がある**



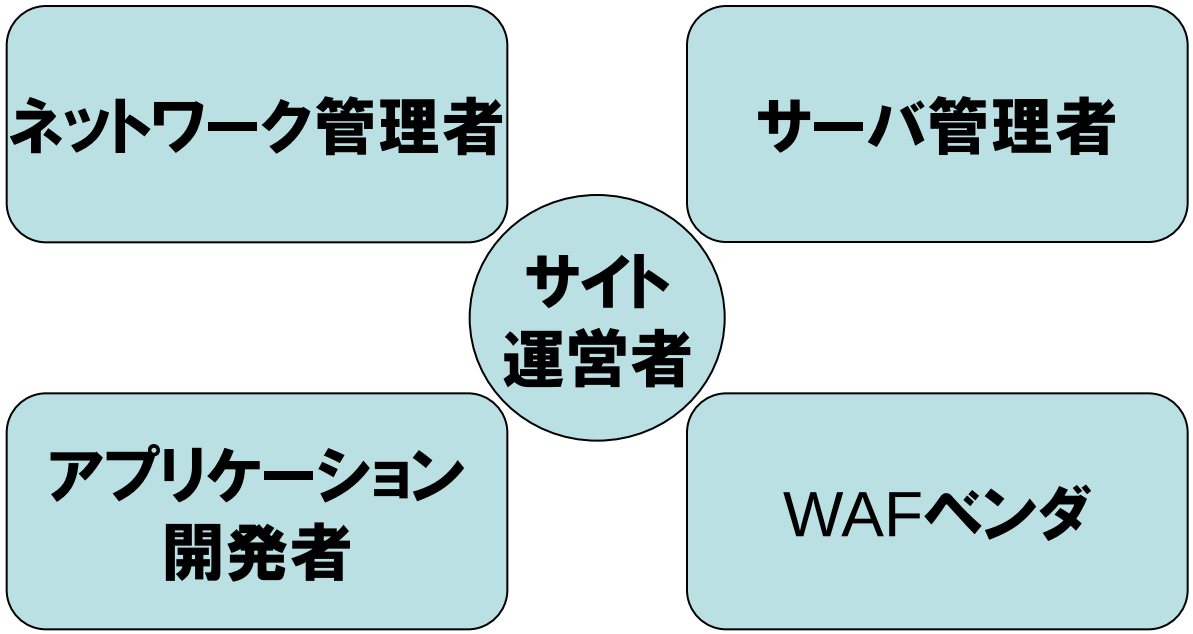
1. はじめに：本セミナーで扱う範囲
2. WAFとは
3. WAFの導入におけるポイント
    3.1. 事前検討
    3.2. 導入
    3.3. 運用
4. まとめ



導入：関係者間調整

- **関係者間調整**

  事前にステークホルダ間の調整を実施。以下は一例。



WAFの導入、運用におけるトラブル回避には事前の調整が大切

導入:導入計画

- **導入計画**
  - **ー初期設定**

    導入時に必須の設定と検証期間で確認する設定を検討し、必要な設定を投入
  - **ー検証方法・期間**

    検証期間に確認および設定する内容を決定し、その期間内に終わるようにスケジュールを検討
  - **ー体制**

    導入がスムーズに進行するように、問題発生時のエスカレーション先とエスカレーション方法を検討
  - **ー本番稼動**

    本番稼動の時期とそれまでに終わらせておく必須項目を検討

WAFでどこまで対応させるのか明確な計画が必要

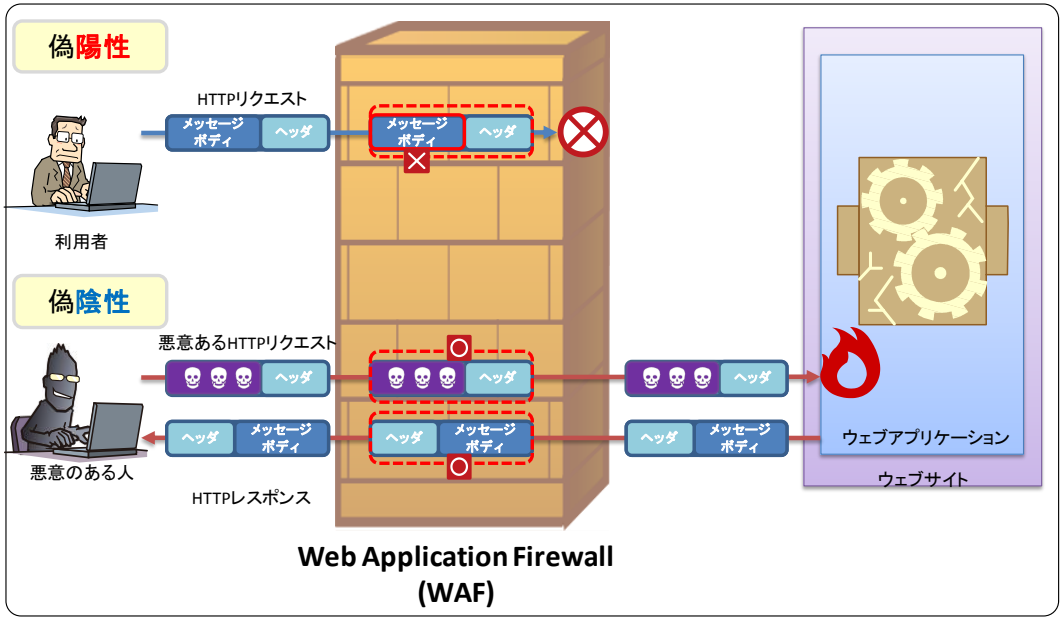
導入:運用計画

- **運用体制**
- **運用ポリシー**
  - **WAFのメンテナンス**
    - ブラックリスト／ホワイトリストの更新方法
    - WAF自身の更新方法(アップデート、修正プログラム)
    - ログのローテーション
  - **WAF自身の障害発生時の対応**
    - フェイルオープン、フェイルクローズ
    - 回避方法、復旧方法

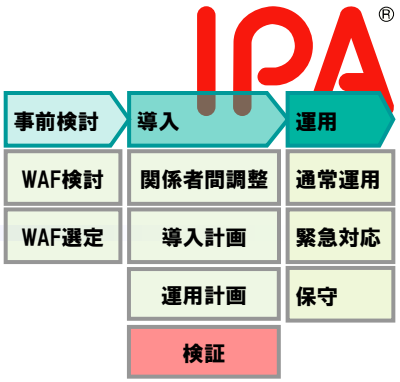
進化する攻撃に対応するにはWAFの運用計画も重要

導入：検証

- **偽陽性（false positive）とは**
  本来「正常なHTTP通信」を「不正なHTTP通信」と判定するエラー
- **偽陰性（false negative）とは**
  本来「不正なHTTP通信」を「正常なHTTP通信」と判定するエラー



導入：検証



- **通過処理での検証**

  偽陽性・偽陰性の検証を行う際は、WAFが通信の検査により不正と判断した場合でも、そのまま利用者またはウェブサイトに送信する状態で検証することが多い。

- **偽陽性の検証**

  ウェブサイト内を網羅的にアクセスして、正常なアクセスを遮断しないことを確認する

- **偽陰性の検証**

  WAFが防御すべき不正なアクセスを行い、実際にWAFがそのアクセスを検知することを確認する

WAFがきちんと設定されているか確認

本番稼動でのトラブル回避に検証フェーズは必要

導入：検証

- **性能測定**

  WAF導入時の性能への影響を測定

  - **ターンアラウンドタイム、レスポンスタイム**

    処理速度への影響を評価

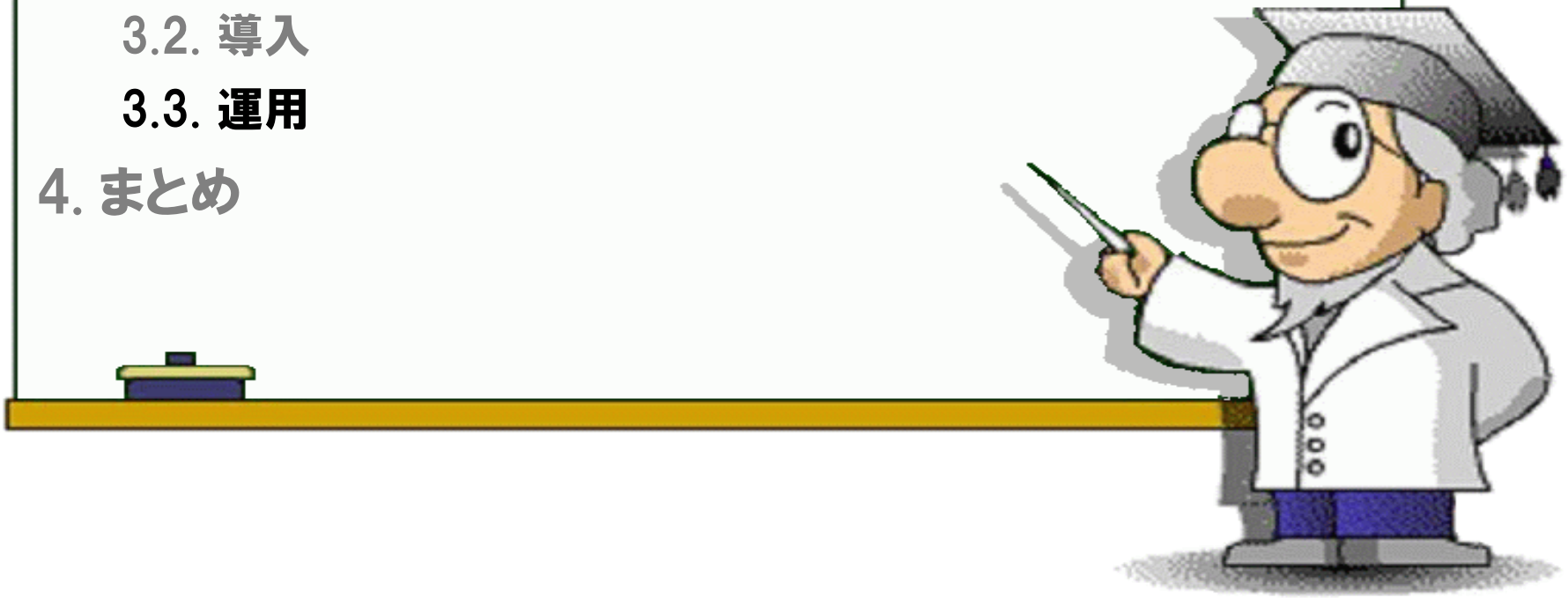
  - **スループット**

    単位時間当たりの転送量への影響を評価

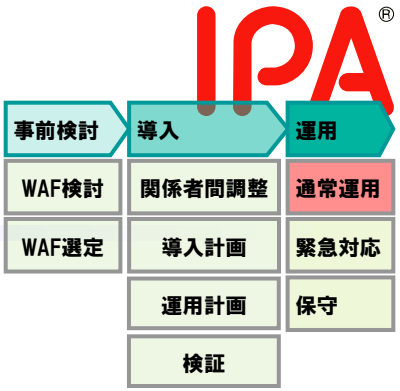
  - **リソース消費**

    CPU使用率や、メモリ使用量、HDD容量への影響を評価

1. はじめに：本セミナーで扱う範囲
2. WAFとは
3. WAFの導入におけるポイント
    3.1. 事前検討
    3.2. 導入
    3.3. 運用
4. まとめ

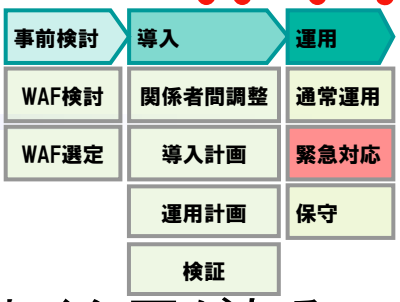


運用：通常運用



- **通常時の運用**
  - **―「ブラックリスト」の更新**
    - 影響の確認、更新タイミング
  - **―「ホワイトリスト」の更新**
    - 影響の確認、更新タイミング
  - **― WAFのバージョンアップや修正プログラムの適用**
    - 影響の確認、適用タイミング
  - **―定期的なログの確認**
    - 攻撃の確認、障害発生の予兆、偽陽性の確認

運用：緊急対応



● 障害発生時の運用

WAFを運用する上で、以下の事象を想定して、準備をしておく必要がある

ー インシデントの発生

- エスカレーション
- WAFでの対応方法

ー 偽陽性判定の発生

- WAFへの設定反映方法、回避方法

ー WAF自体の障害（ハードウェア障害、ソフトウェア異常）

- エスカレーション
- 回避方法
- 復旧方法
- 代替品の準備

運用：保守

- **保守契約の更新**
  - **ハードウェア保守**

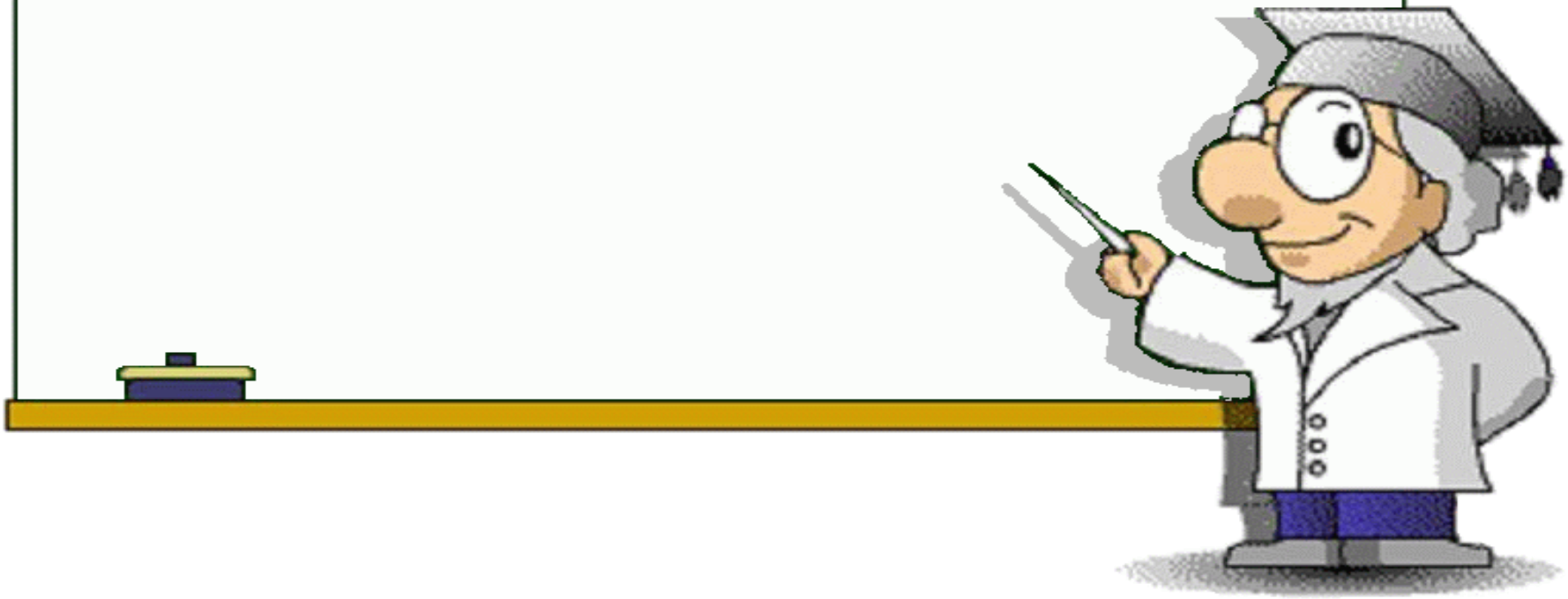
    ハードウェア保守契約を更新しないと・・・

    - **ハードウェア故障時にウェブサイトが無防備状態になる**
  - **ソフトウェア保守**

    ソフトウェア保守契約を更新しないと・・・

    - **「ブラックリスト」の更新ができず、新しい攻撃手法に対応できない**

1. はじめに：本セミナーで扱う範囲
2. WAFとは
3. WAF導入におけるポイント
4. まとめ



まとめ

- **WAFはウェブサイトの脆弱性対策の1つ**
  - ーWAFでできること・できないことを理解した上で、セキュリティ対策の1つと理解して導入すること
  - ーウェブアプリケーションに脆弱性が発見された場合は、最終的にウェブアプリケーション自身の修正まで検討すること
- **目的にあったWAFを選ぶ**
  - ー導入したけど使えないということがないように、運用することまで考慮してWAFを選定すること