

5. オープンソースWAF「ModSecurity」導入事例 ～ IPA はこう考えた ～

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

1. 背景・目的

2. JVN iPedia へのWAF導入

1. 事前検討

2. 導入

3. 運用

3. まとめ



背景

IPAでは、脆弱性対策の一つとして「WAF」が有効であると考えている。しかし……

■ 「WAF」の認知度が低い

理由: WAFについて、日本語で紹介している文献があまりない



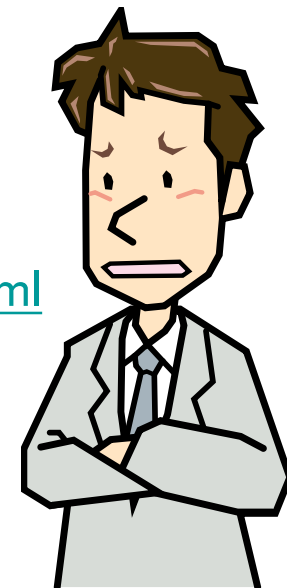
施策: WAF の理解を手助けする情報として、

「Web Application Firewall(WAF)読本」を公開

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

■ 「WAF」の活用事例が少ない

理由: WAFの導入実績を、日本語で紹介している文献があまりない



目的

JVN iPedia へ

オープンソースWAF「ModSecurity」導入

- IPA自らWAFを導入・運用
- WAFができる事できない事、導入・運用における注意点などをノウハウとして蓄積

導入・運用事例として公開することで
WAF活用を推進

本講演の内容はWAF 読本 改訂第二版にて掲載予定(来春公開予定)



[補足] JVN iPedia、ModSecurity

■ JVN iPedia <http://jvndb.jvn.jp/>

国内で利用されている製品を対象にした脆弱性対策情報を網羅し蓄積したデータベース

JVN iPedia

- アクセス数 月間 100 万件
- 登録数 2010年9月末 9,027件



■ ModSecurity <http://www.modsecurity.org/>

TrustWave社がGPLv2 ライセンスのもと提供しているオープンソースの Web Application Firewall (WAF)

■ OWASP Core Rule Set

http://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

OWASP (Open Web Application Security Project) が GPLv2 ライセンスのもと提供しているオープンソース WAF ModSecurity のルール (シグネチャ)

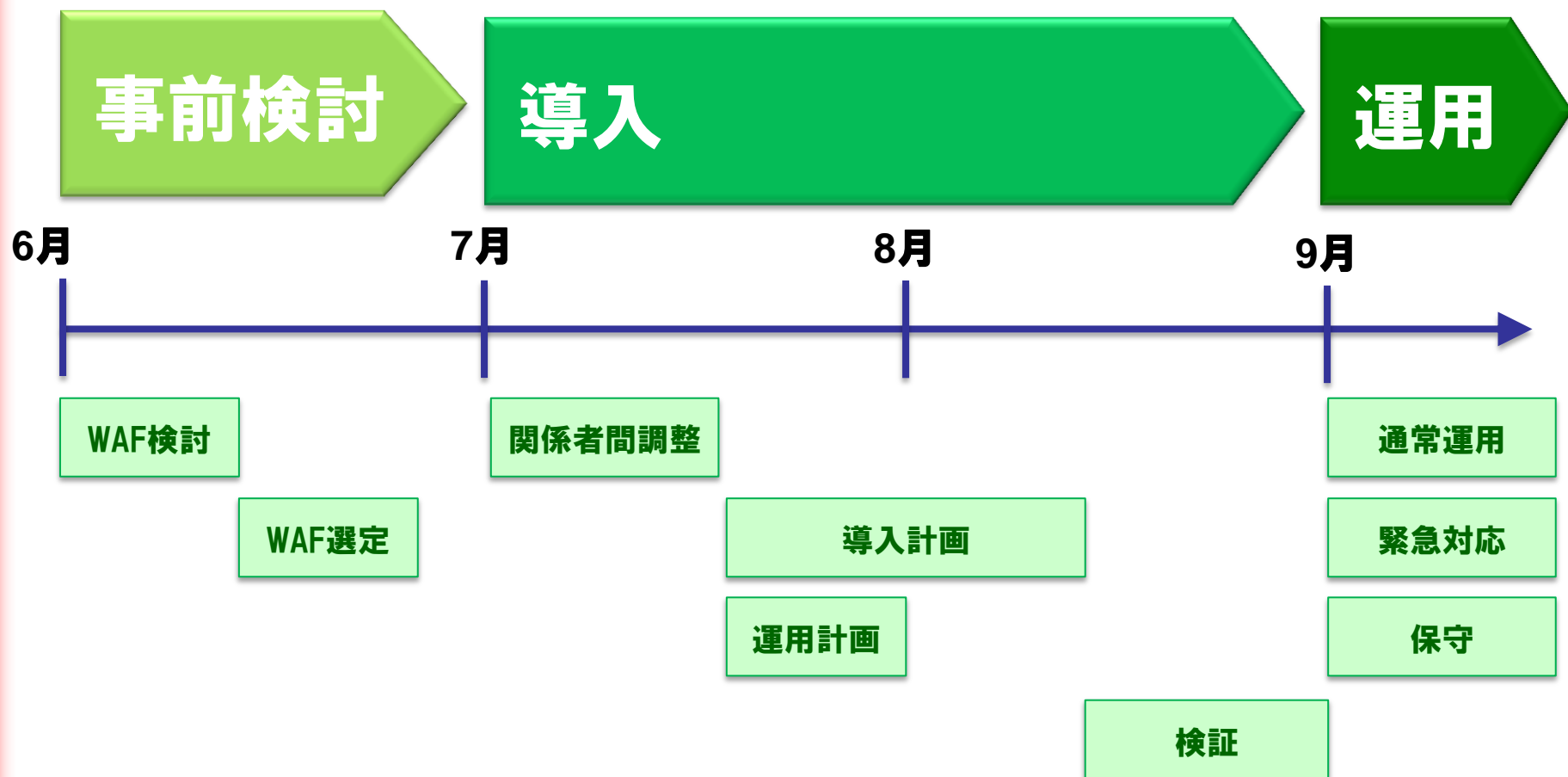
1. 背景・目的
2. JVN iPedia へのWAF導入
 1. 事前検討
 2. 導入
 3. 運用
3. まとめ



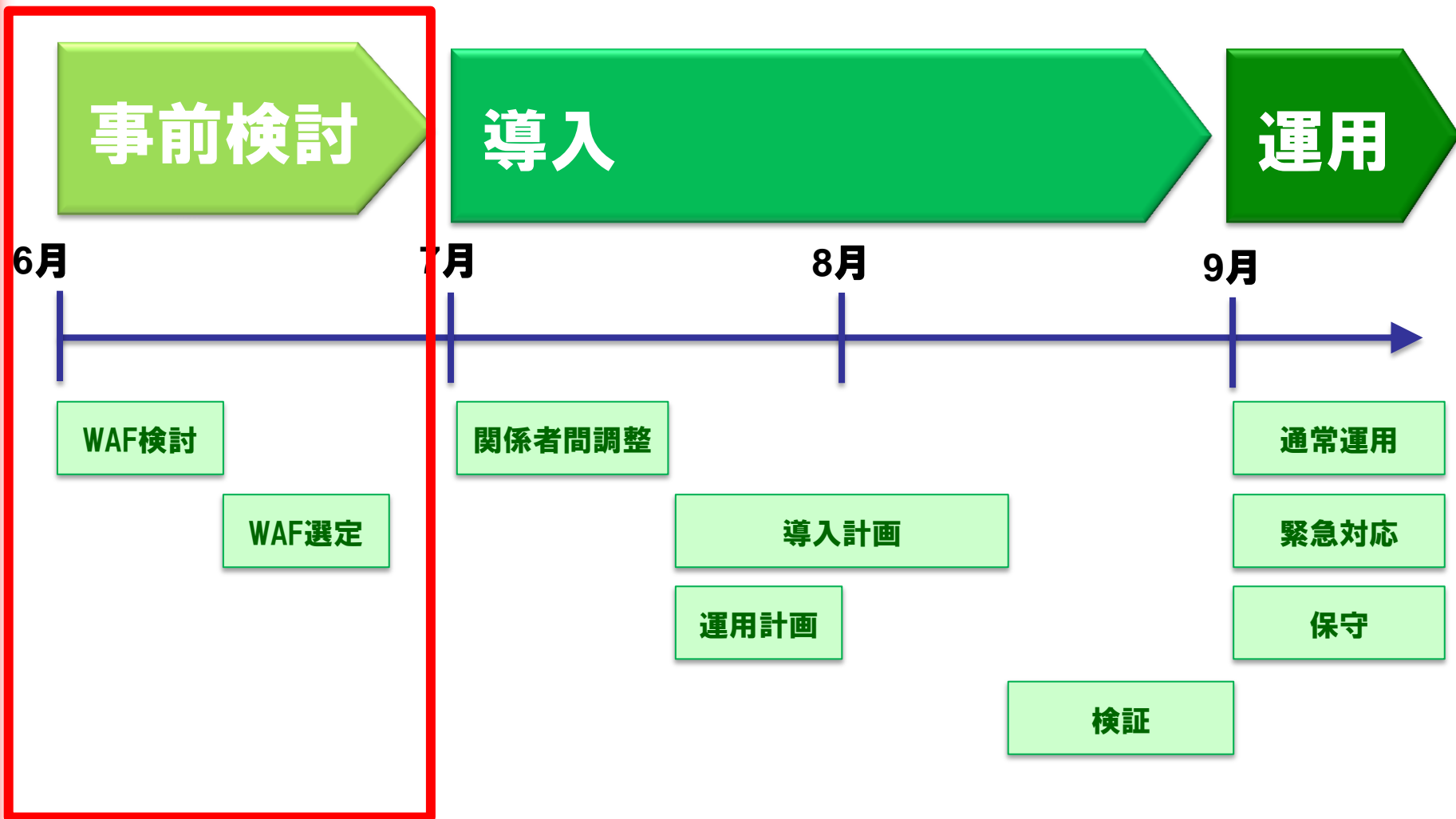
WAFの導入の流れ



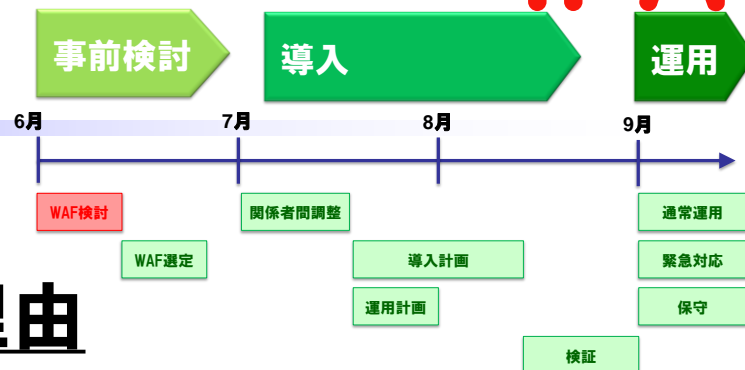
IPAのWAF導入の実情



事前検討



WAF検討



■ IPAがWAFの導入を検討した理由

自らWAFを導入・運用し、WAFができる事できない事、運用における注意点などをノウハウとして蓄積するため

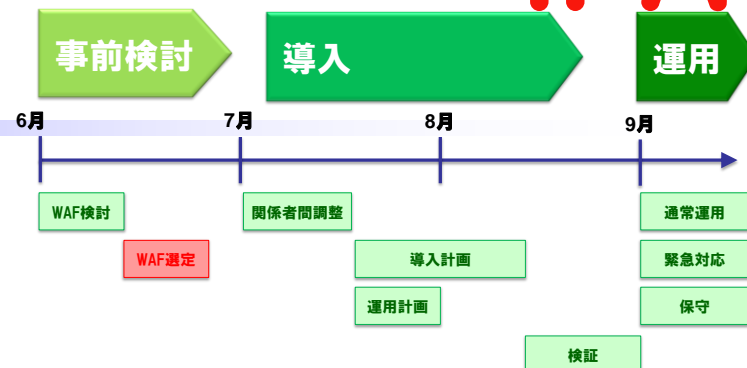
■ 一般的にWAF導入の際想定される理由

- 開発者にウェブアプリケーションの改修依頼ができない
- 改修できないウェブアプリケーションに脆弱性が発見された
- その他



(注) JVN iPedia に脆弱性は確認されていません

WAF選定(1)



■ WAFの選定方法

- 予算・人材から選択(商用 WAF ? オープンソフトWAF?)
- 構成から選択(ネットワーク型? サーバインストール型?)
- その他
 - サーバの種類など
 - 機能や性能など

検討課題(1)

WAF の種類はたくさんあるけど、
どれを選べばいいのだろう？



WAF選定(2)



IPAはこう考えた(1)

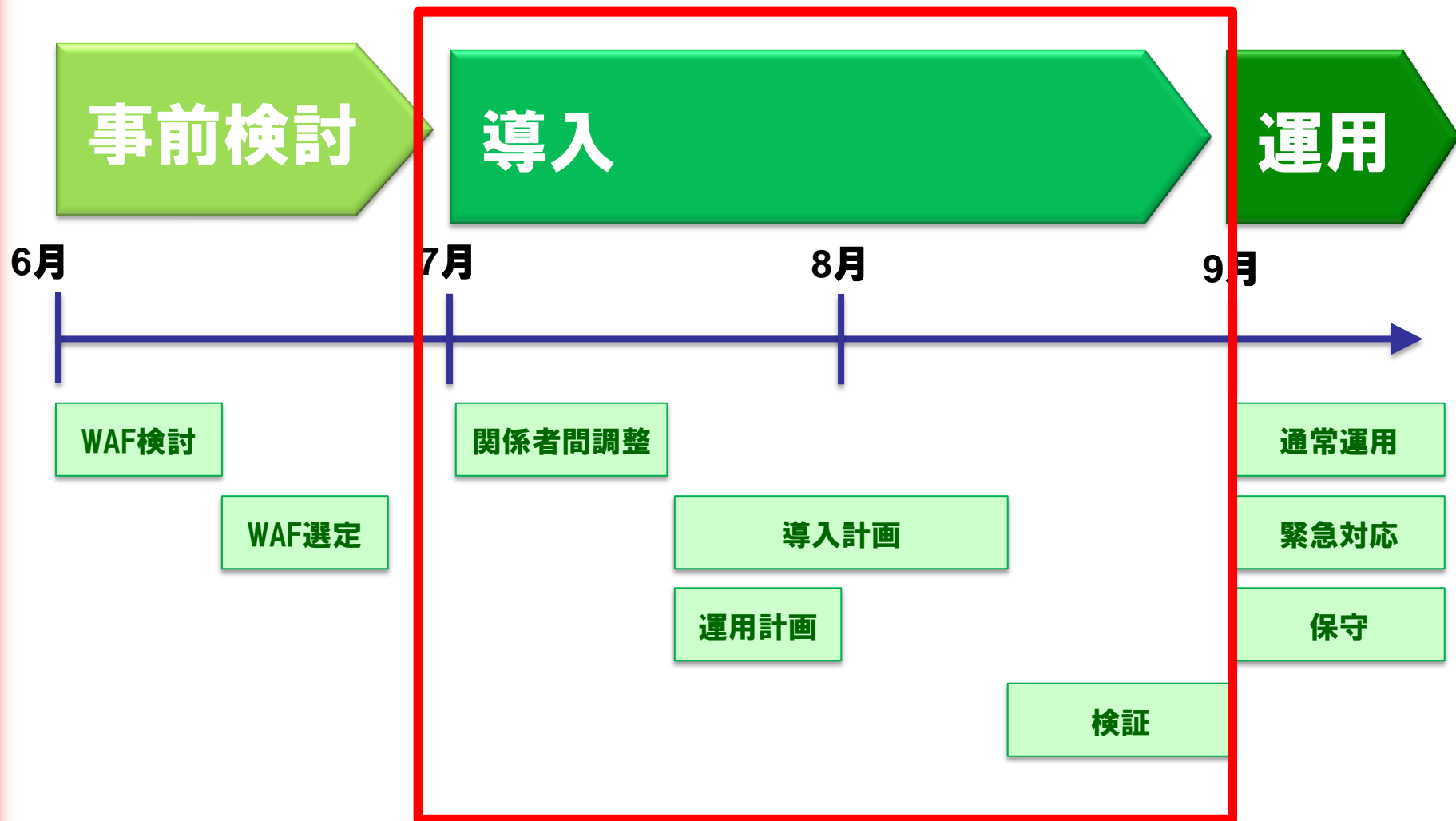
- 新たにNW機器の導入は想定していないため サーバインストール型
- 予算・人材から オープンソースWAF を選択
- Apache で動作する必要がある

選定結果:

ModSecurity



導入

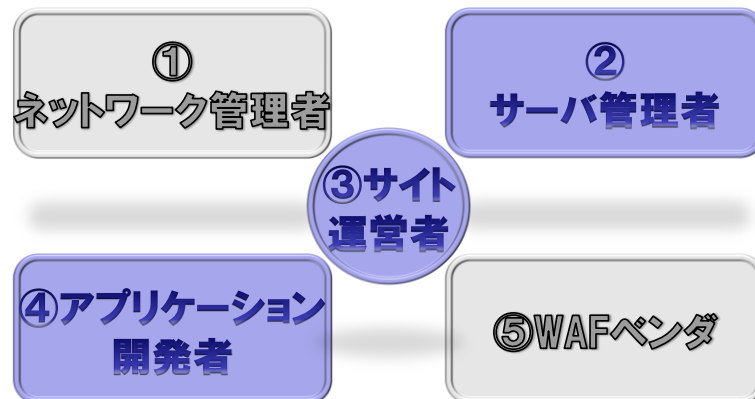


関係者間調整①

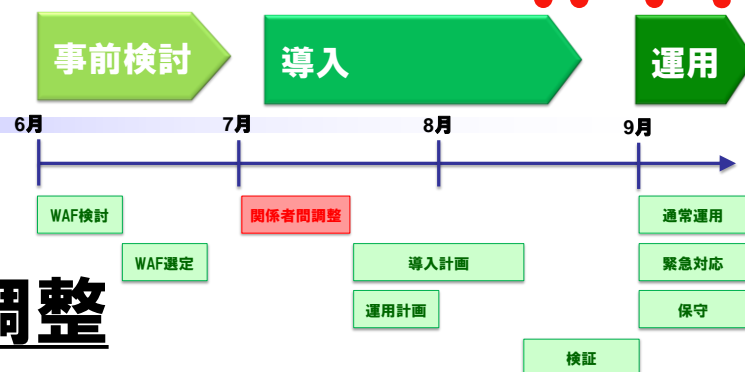


関係者の洗い出し

- ① (IPAのネットワーク管理者)
- ② JVN iPedia のサーバ管理者
- ③ JVN iPedia のサイト運営者
- ④ JVN iPedia のアプリケーション開発者
- ⑤ (WAFベンダ)



関係者間調整②



①IPAのネットワーク管理者と調整

- ネットワークの変更が必要ではなく、調整不要であった（サーバインストール型WAFを導入するため）

②JVN iPediaの管理者と調整

③JVN iPediaのサイト運営者と調整

- 導入時にサービス停止が必要となるなど導入におけるリスクを説明し、WAFを導入することの了承を得た
- 偽陽性(誤検知)が発生した場合、運用に影響を及ぼす可能性が存在するなど運用におけるリスクを説明し、WAFを導入することの了承を得た

関係者間調整③



■ ④アプリケーション開発者

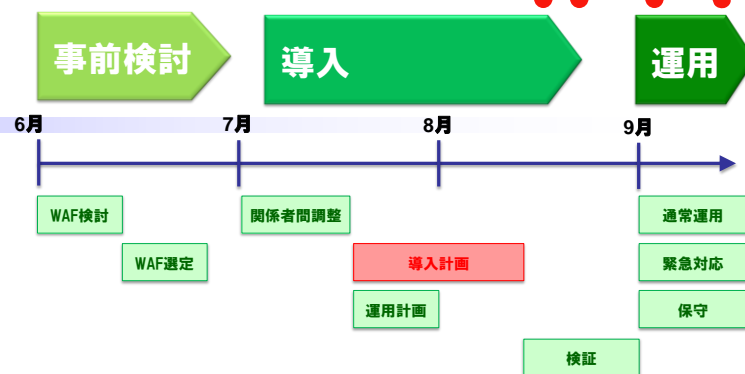
【開発元企業】と調整

- ウェブサーバやウェブアプリケーションの保守・サポートの契約について確認し、WAFを導入により、サポート範囲外にならないことを確認した

■ ⑤WAFベンダと調整

- オープンソースWAFを利用するため、調整不要であった

導入計画(1)



■ 導入前の事前確認

- サーバ環境の詳細な確認
 - ハードウェア構成、必須ソフトウェアのインストール状況など

■ 初期設定決定

- ログ出力設定の決定
- 有効にするルール(シグネチャ)の選定

検討課題(2)

全てのルールを有効にしてよいのだろうか？



導入計画(2)

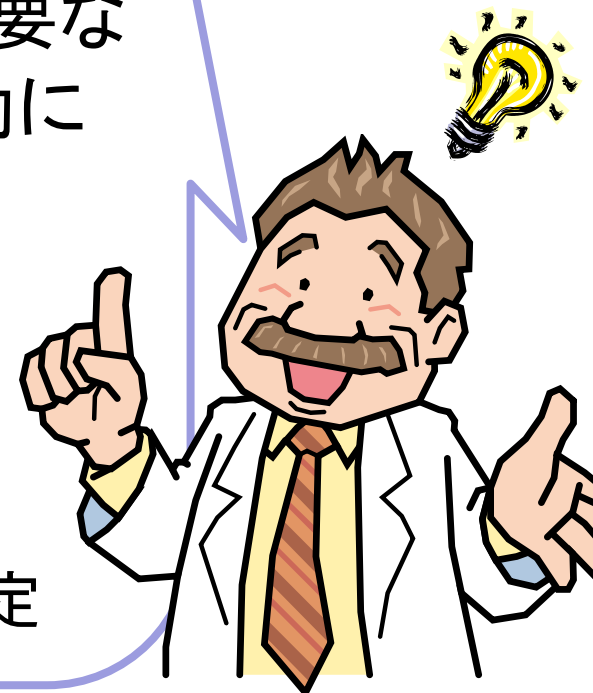


IPAはこう考えた(2)

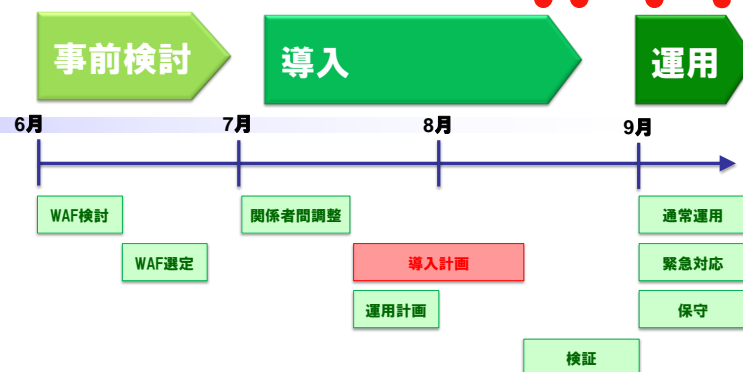
全てのルールを有効にすると偽陽性の発生確率が高くなる。対策が必要な脆弱性に関するルールだけを有効にしよう！

➔ IPAではまず、影響が深刻な脆弱性である「SQL インジェクション」のみを有効にした

今後、順次ルールを有効にする予定



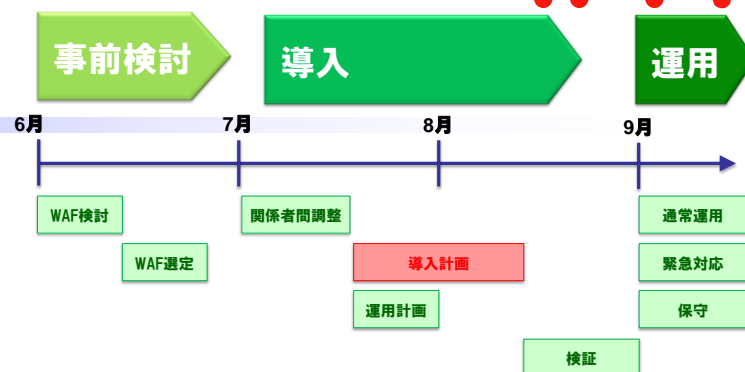
導入計画(3)



■ 導入手順書の作成

- 導入前の事前確認、初期設定決定に伴い、導入手順書を作成しました。
- IPAの手順書には以下の内容が記載されています
 - ModSecurity 導入手順
 - ModSecurityの動作に必要なソフトウェアのインストール手順
 - ModSecurityのインストール手順
 - ModSecurity 設定変更手順
 - ログファイルの管理設定変更手順
 - ルール(シグネチャ)の変更手順
 - ModSecurityのアップデート手順

導入計画(4)



■ 検証内容の検討

- WAFの運用を開始する前に検証を行わないと、偽陽性の発生等の理由によりサービスが停止してしまうなど、通常
のサービスに影響が発生してしまう可能性があります

検討課題(3)

でもまてよ……

検証するためとはいえ、いきなり運用しているサーバに導入してしまっ
て大丈夫なのだろうか？



導入計画(5)



IPAはこう考えた(3)

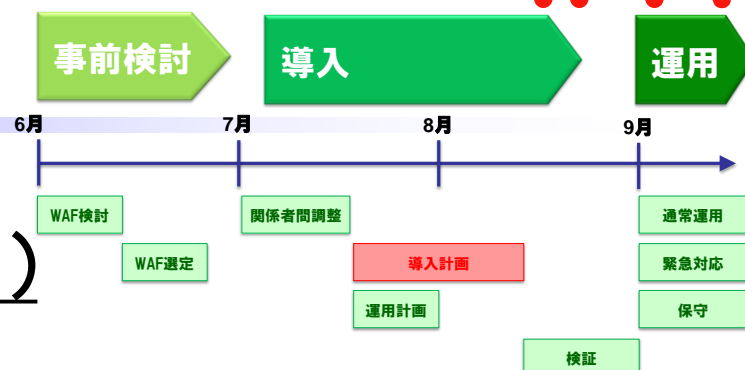
導入に失敗してサービスを停止しては大変！

導入手順書にそって、テスト環境（仮想環境等）でテストを実施する

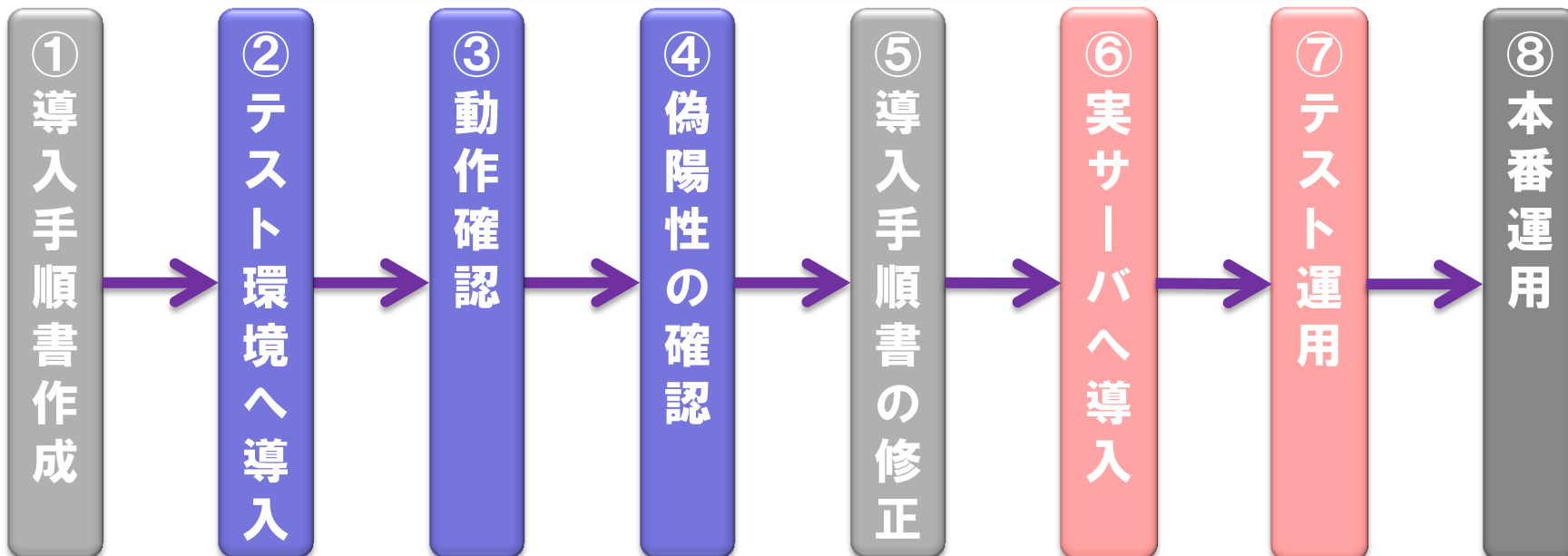
- ModSecurityのインストールテスト
- 導入手順書の妥当性テスト



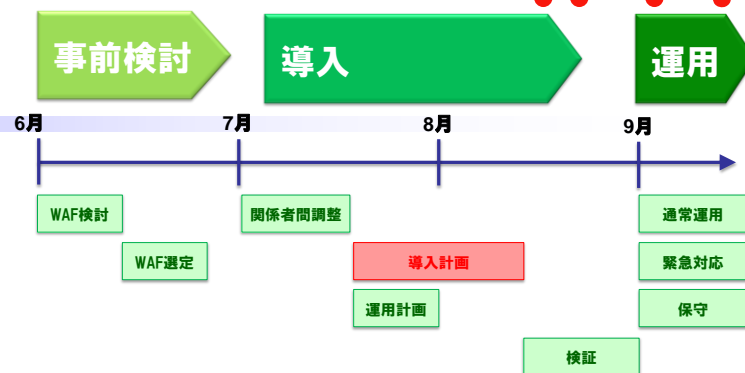
導入計画(6)



■ IPAが行った検証(詳細は後述)



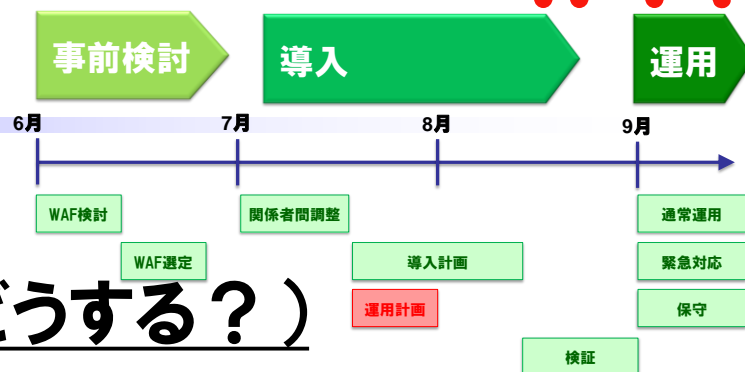
導入計画(7)



■ その他導入に向けた計画

- 導入日時調整
 - JVN iPediaが動作していないと困る事情がないことを確認
- 利用者への通知
 - 1週間前にメンテナンスを告知
- 導入対応要員の確保
 - 作業員及び確認者一名ずつ準備する
- 導入時の連絡体制の整備
 - 担当 → 現場責任者 → 統括責任者

運用計画(1)



■ 運用ポリシー(誰が?いつ?どうする?)

- ModSecurityのアップデート
- OWASP Core Rule Set(シグネチャ)のアップデート
- 攻撃検知時、偽陽性発生時の対応
- 障害発生時の対応

検討課題(4)

でもまてよ...

毎回アップデートを行うと、
サーバ停止など運用に影響が
あるのでは...



運用計画(2)



IPAはこう考えた(4)

IPAでは、次の場合のみアップデートすることにしました。

ModSecurity

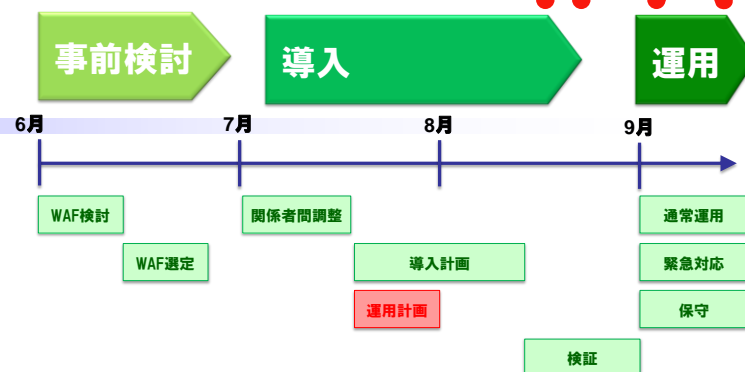
➡ 運用に影響を与える致命的なバグが修正されている場合

Core Rule Set

➡ 有効としたルールが更新された場合
(今回は SQL インジェクションのみが対象)



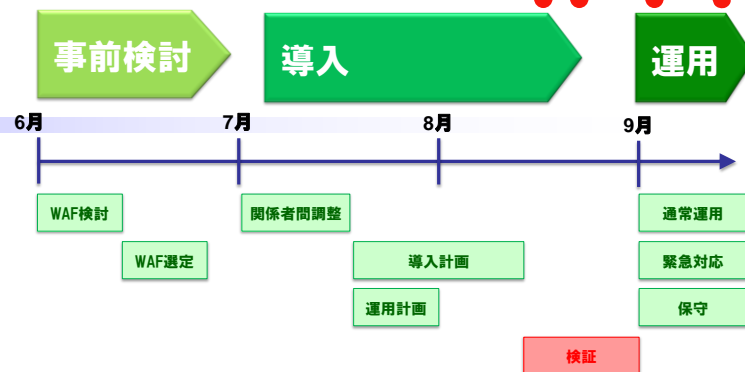
運用計画(3)



■ 運用手順書の作成

- 運用ポリシーの決定に伴い、運用手順書を作成しました。
- IPAの手順書には以下の内容が記載されています
 - 運用ポリシー
 - ModSecurity / Core Rule Setアップデートポリシー
 - 遮断時(偽陽性発生時)の対応ポリシー
 - 作業手順
 - ModSecurity/Core Rule Set アップデート時の対応手順書
 - 遮断時(偽陽性発生時)の対応手順書

検証(1)



■ 計画した検証内容及び結果

②テスト環境へ導入

内容: 手順書に従いModSecurityをインストールし、正常起動を確認

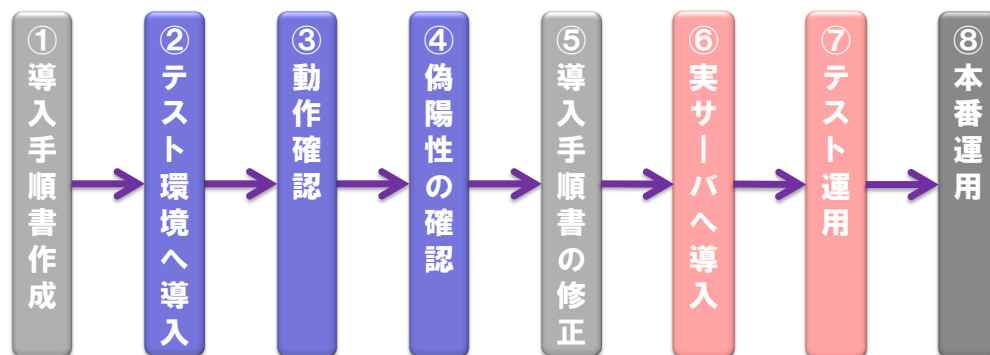
結果: インストールは完了するも、ウェブサーバが起動しない現象が発生

対処: ModSecurityのメーリングリスト等を調査した結果、コンパイルオプションを変更することで同じ事象が解決していたため、コンパイルオプションの変更し対処。

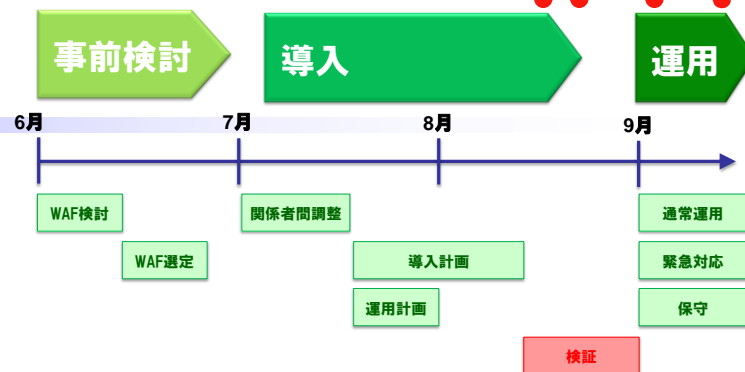
③動作確認

内容: テストデータを入力し、ModSecurityがログを出力するか確認

結果: ログが出力されることを確認できた。



検証(2)



■ 計画した検証内容及び結果

④ 偽陽性の確認

内容: JVN iPediaの最新過去1ヶ月のログから、利用者の通信を作成し、その通信をModSecurityがブロックしないことを確認

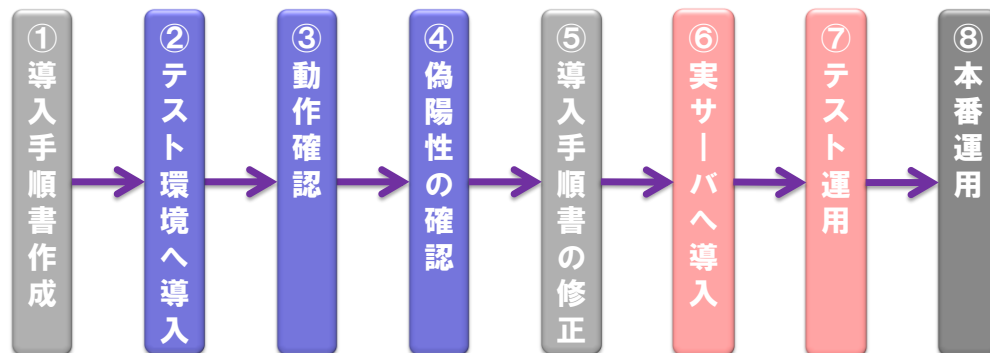
結果: 偽陽性の発生は、**0件**であった

尚、iLogScannerで「SQL インジェクション」と判定した通信のうち、ModSecurity (CoreRulset v2.0.7)で検出できなかったのは、**4件**(ユニーク)であった

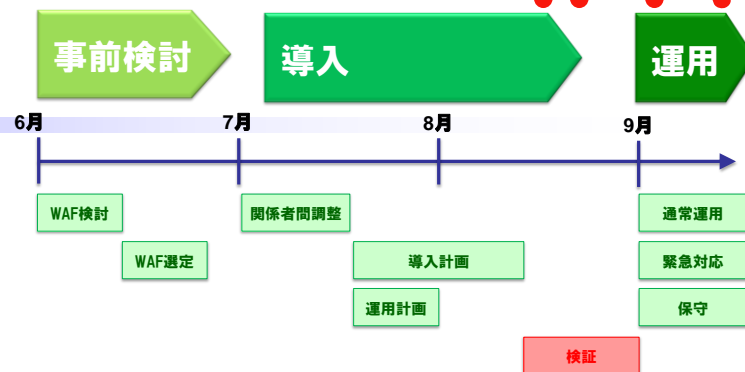


⑤ 導入手順書の修正

テスト環境での検証(②~④)をもとに手順書を修正



検証(3)



■ 計画した検証内容及び結果

⑥実サーバへの導入

内容: 手順書に従いModSecurityをインストールし、正常起動を確認

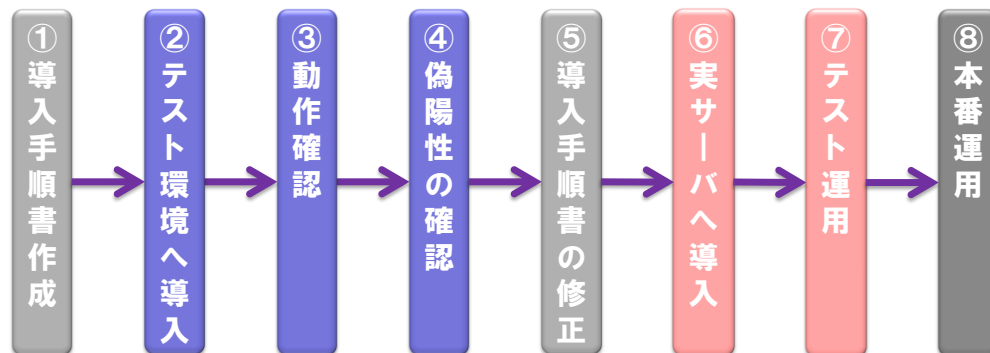
結果: 正常に起動することが確認できた

⑦テスト運用(約 2 週間程度)

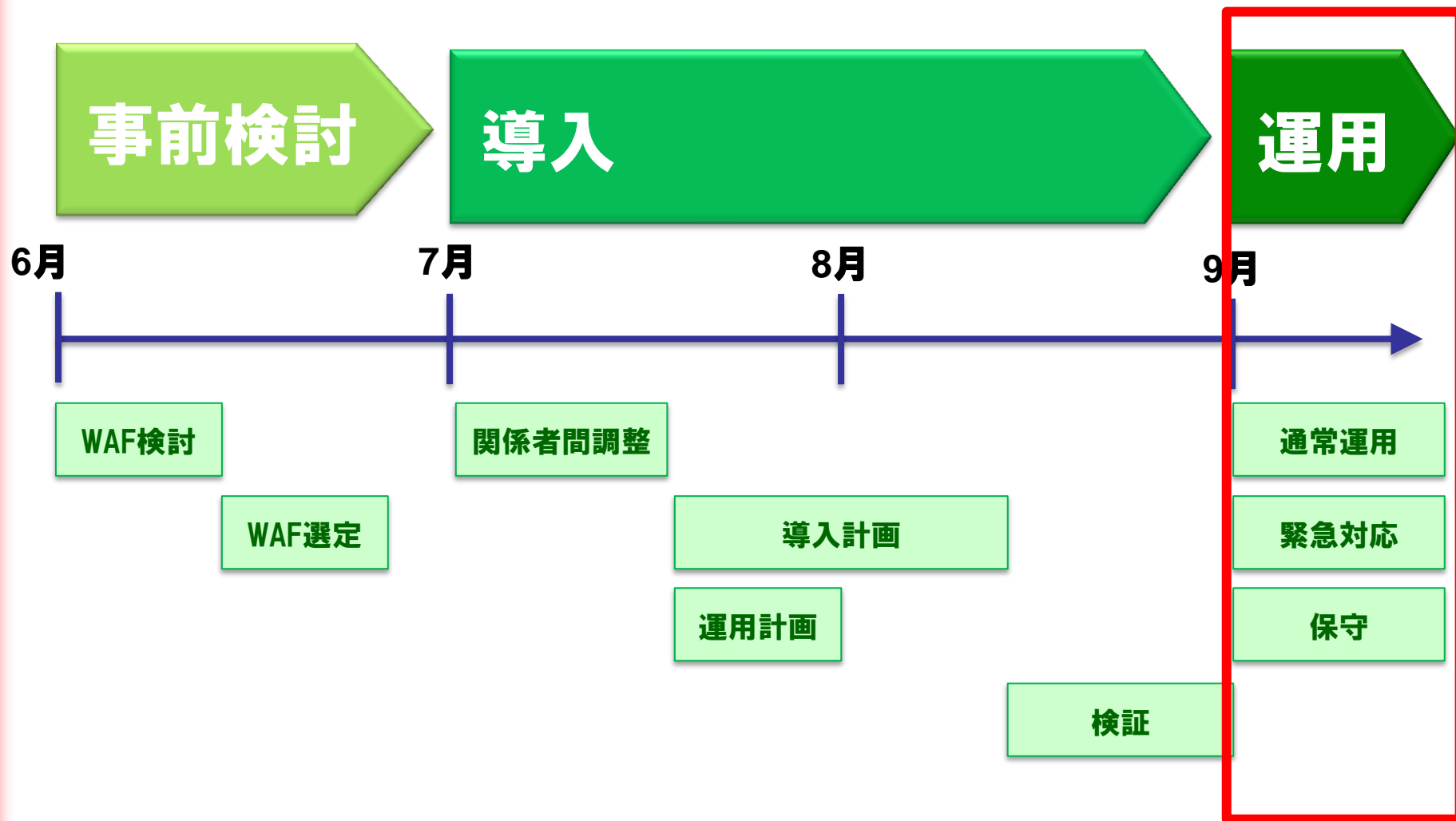
内容: 遮断はしない検知モード(通過処理)で、テスト運用を行い日々ログから、偽陽性の発生を確認

結果: 偽陽性の発生は**0件**であった。一方、SQLインジェクション攻撃を**152件**検知

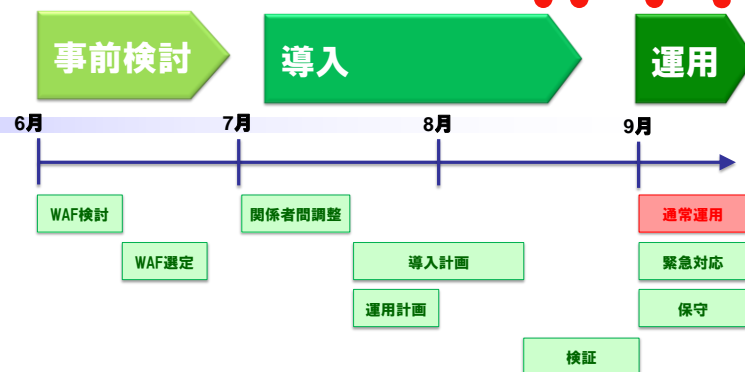
⑧本番運用



運用



通常運用(1)



通常運用における作業①

- 定期的に検知ログを確認
 - 攻撃の状況を確認
 - 偽陽性の発生を確認



ウェブサイト攻撃の検出ツールiLogScanner(*)

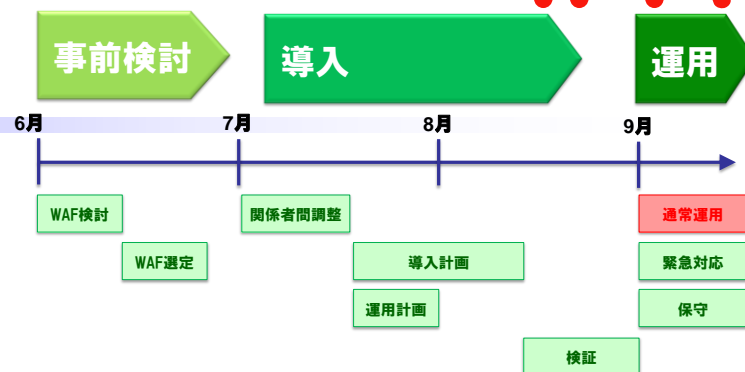
専門的なスキルが必要だったウェブサーバのログ解析が誰でも簡単に行うことができます。

ログ解析などの攻撃状況の把握は、対策を立てる上での指針の一つになります。**日頃からログを分析する習慣をつけることを推奨**します。IPAでもiLogScanner利用して、日々ログ解析をおこなっています。



(*)<http://www.ipa.go.jp/security/vuln/iLogScanner/index.html>

通常運用(2)



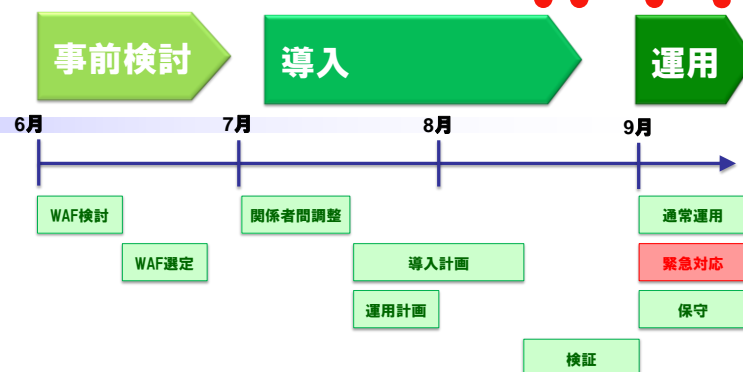
■ 通常運用における作業②

- ModSecurity、Core Rule Setのアップデート
 - バグFixやセキュリティFix等の対応

アップデートする際は、導入時と同じく必ず、検証をおこないましょう。



緊急対応



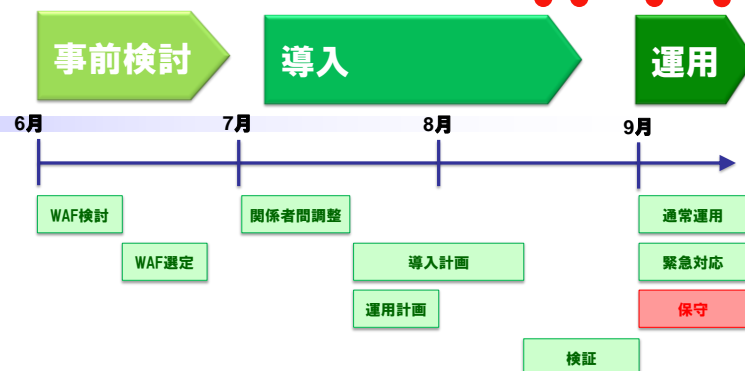
緊急対応作業

- IPAは、緊急対応作業として次の内容を想定しています。
 - ModSecurity障害時の対応
 - 偽陽性発生時の対応



- ① JVN iPediaの運用が停止する時間を最低限に抑えるため、ModSecurityを停止
- ② 障害の原因をログなどから調査
- ③ 対応策検討
- ④ 障害復旧

保守



■ 保守作業

ModSecurityは、オープンソースWAFです。

基本的に保守契約はなく、運営者自ら保守していく必要があります。

IPAは、保守作業として次の様な内容を想定しており、運用に組み込んでいます。

- ModSecurityのアップデート確認作業
- OWSP Core Rule Setのアップデート確認作業

1. 背景・目的
2. JVN iPedia へのWAF導入
 1. 事前検討
 2. 導入
 3. 運用
3. まとめ



まとめ

- オープンソースWAF「ModSecurity」を実際にIPAで導入・運用を継続しています。
- 本発表では、主にWAFを導入・運用する上で、実際にIPAで検討した内容・結果などを紹介しました。
 - 導入時の作業内容・検討内容
 - 運用時の作業内容・検討内容
など
- 本発表が、WAF 導入における一助になれば幸いです。