

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8月6日公開

目次

1. はじめに

1.1 本セミナーで扱う範囲

1.2 WAFとは

2. ウェブサイトを取り巻く状況

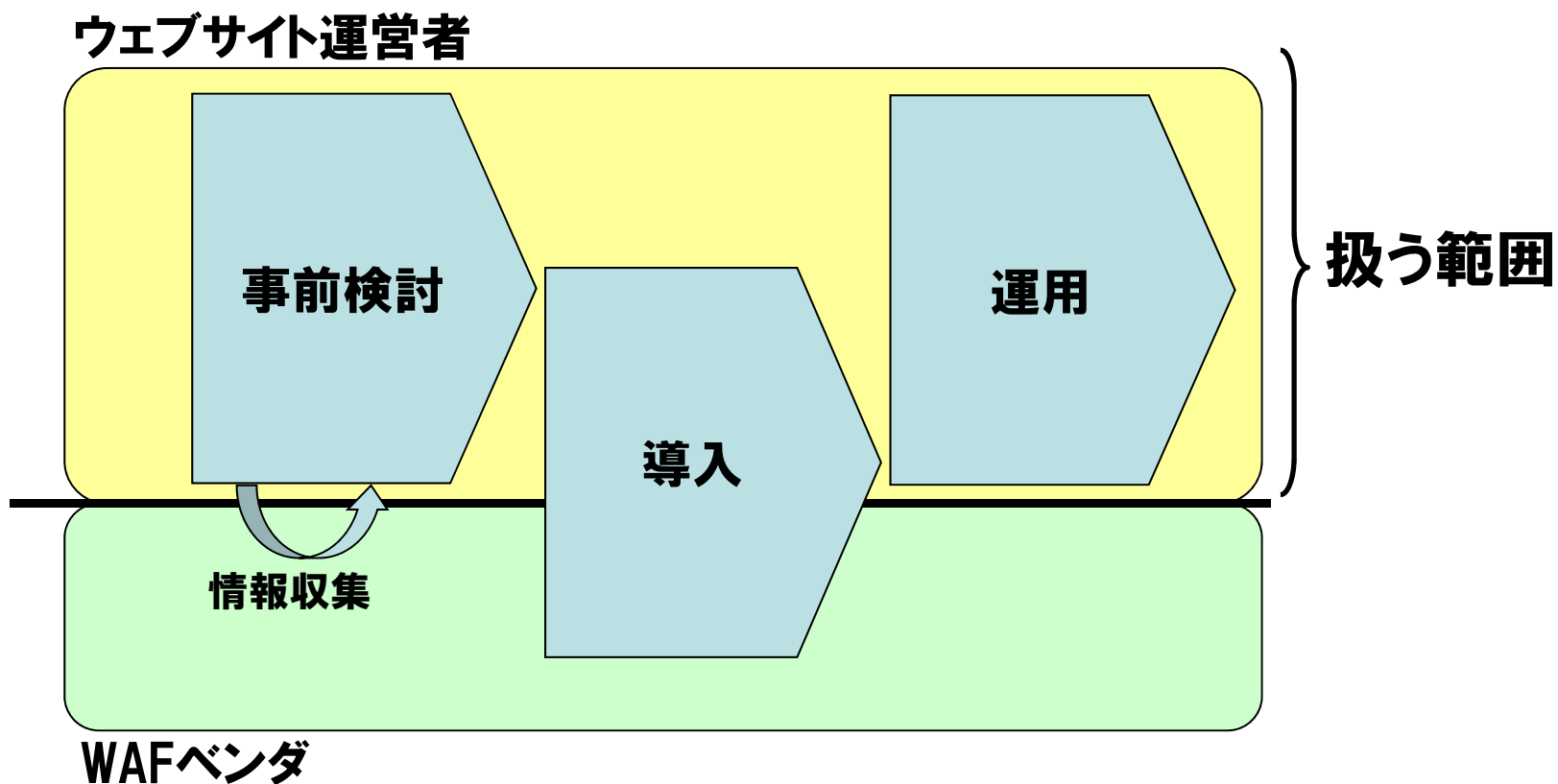
3. IPAのWAFに関する取り組み

4. WAFの導入におけるポイント

5. まとめ



1.1 本セミナーで扱う範囲

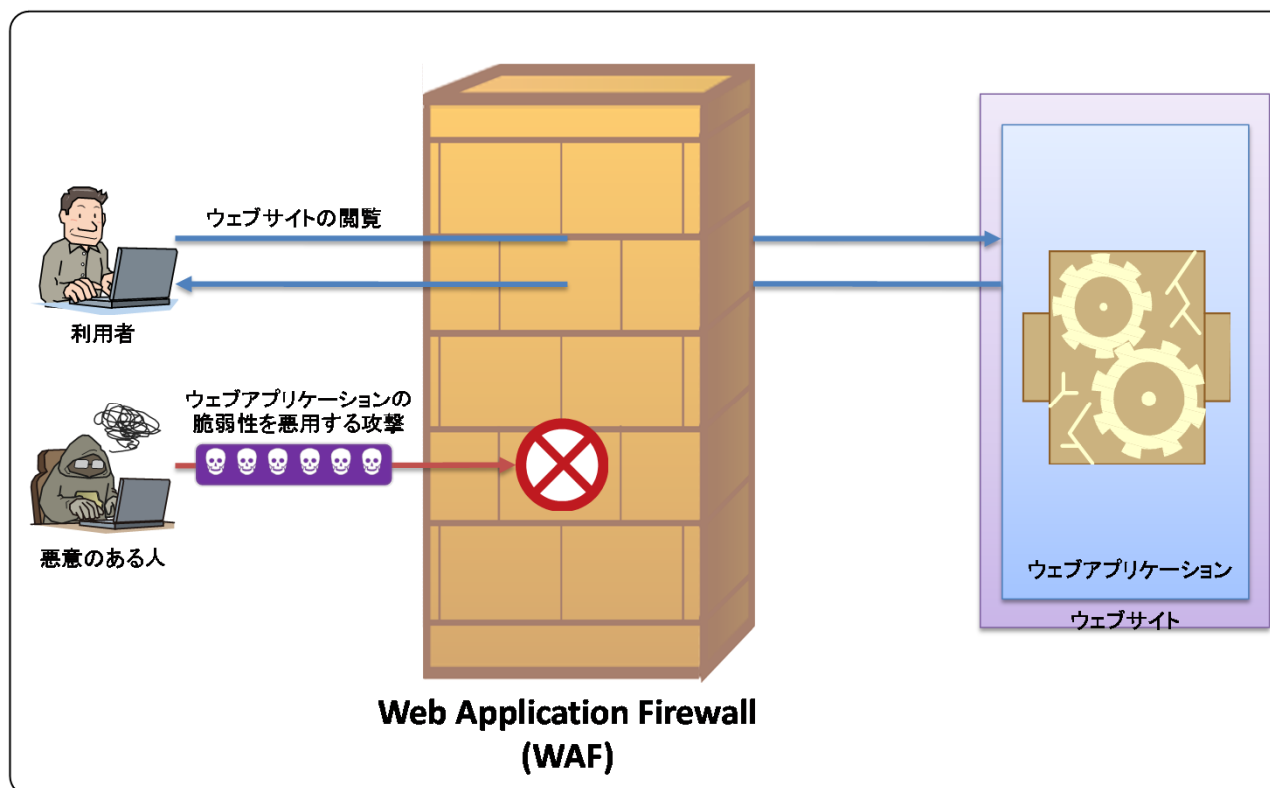


※ 上記は、WAF導入の流れの一例

1.2 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

ウェブサイトのセキュリティ対策の1つとしてWAFは有効

1. はじめに
2. ウェブサイトを取り巻く状況
3. IPAのWAFに関する取り組み
4. WAFの導入におけるポイント
5. まとめ



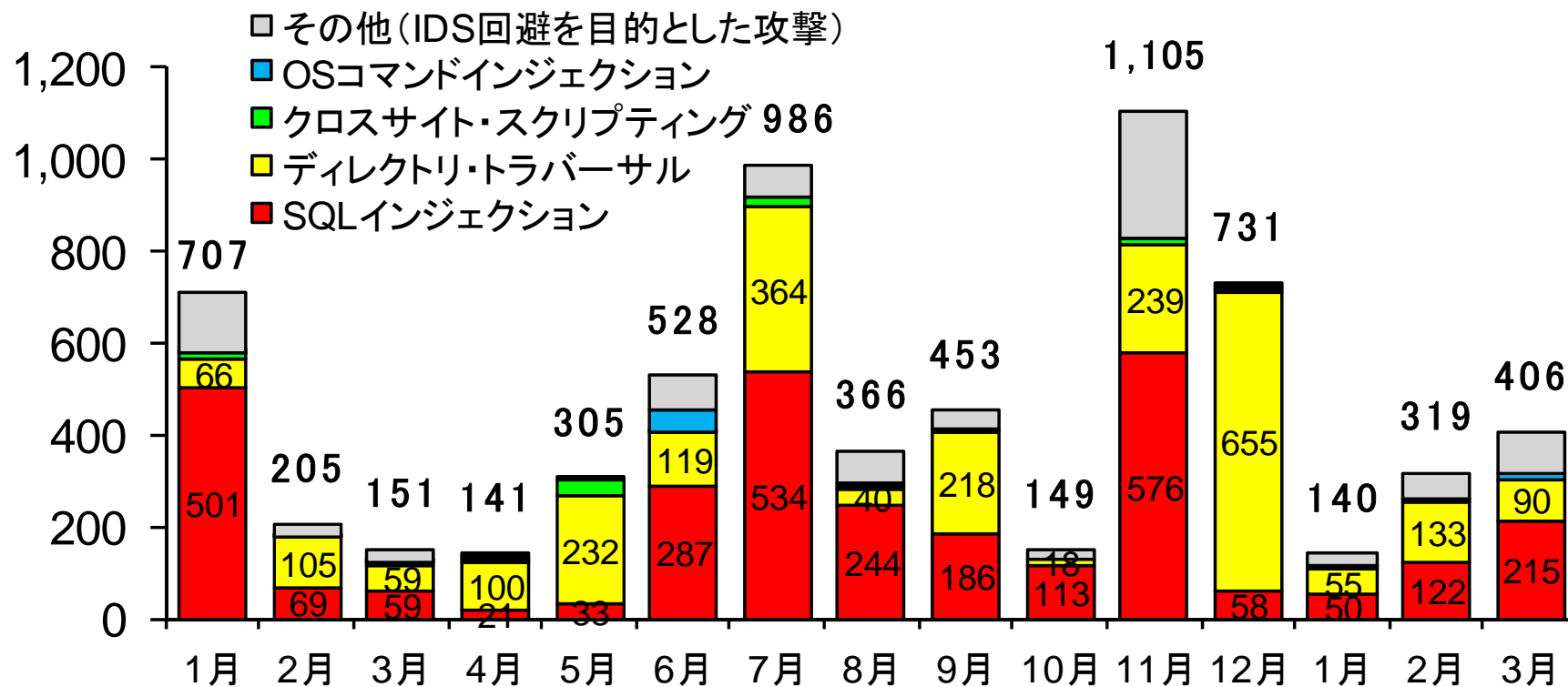
望ましい脆弱性対策

- 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、あれば修正するのが第一！

実情は(攻撃)

● ウェブサイト(JVN iPedia)への攻撃事例



ウェブサイトの規模に関係なく攻撃は行われる！

実情は(脆弱性)

● なくなるにウェブサイトの脆弱性

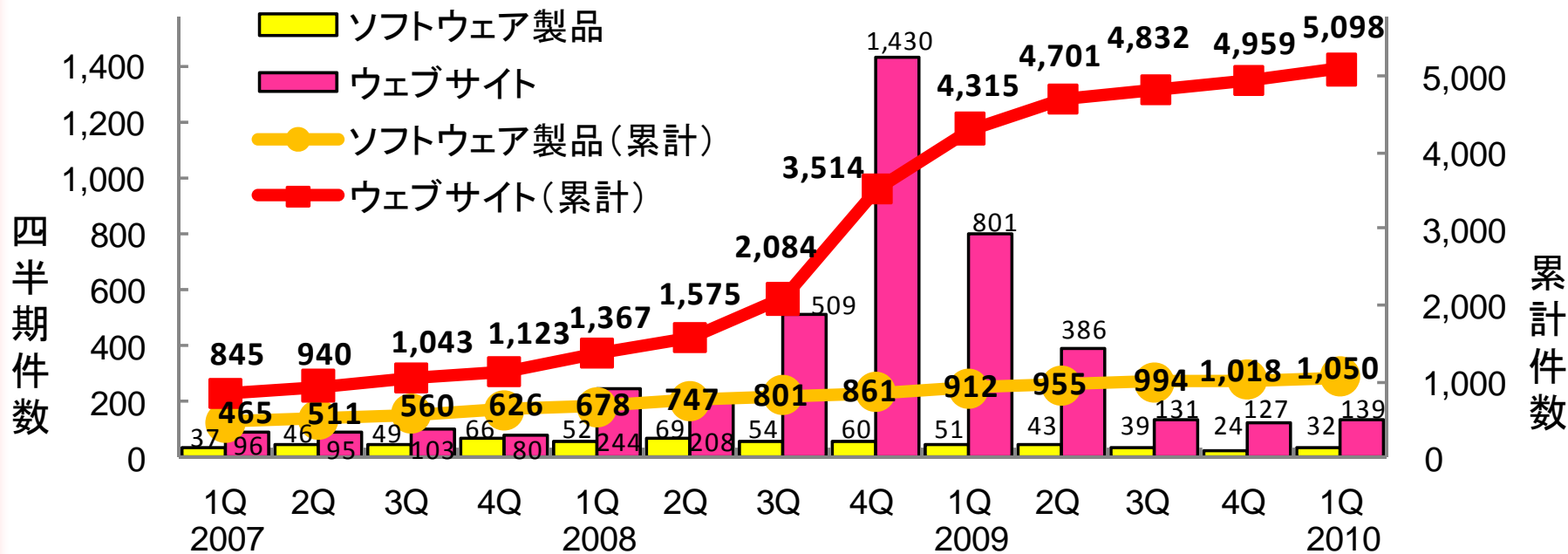
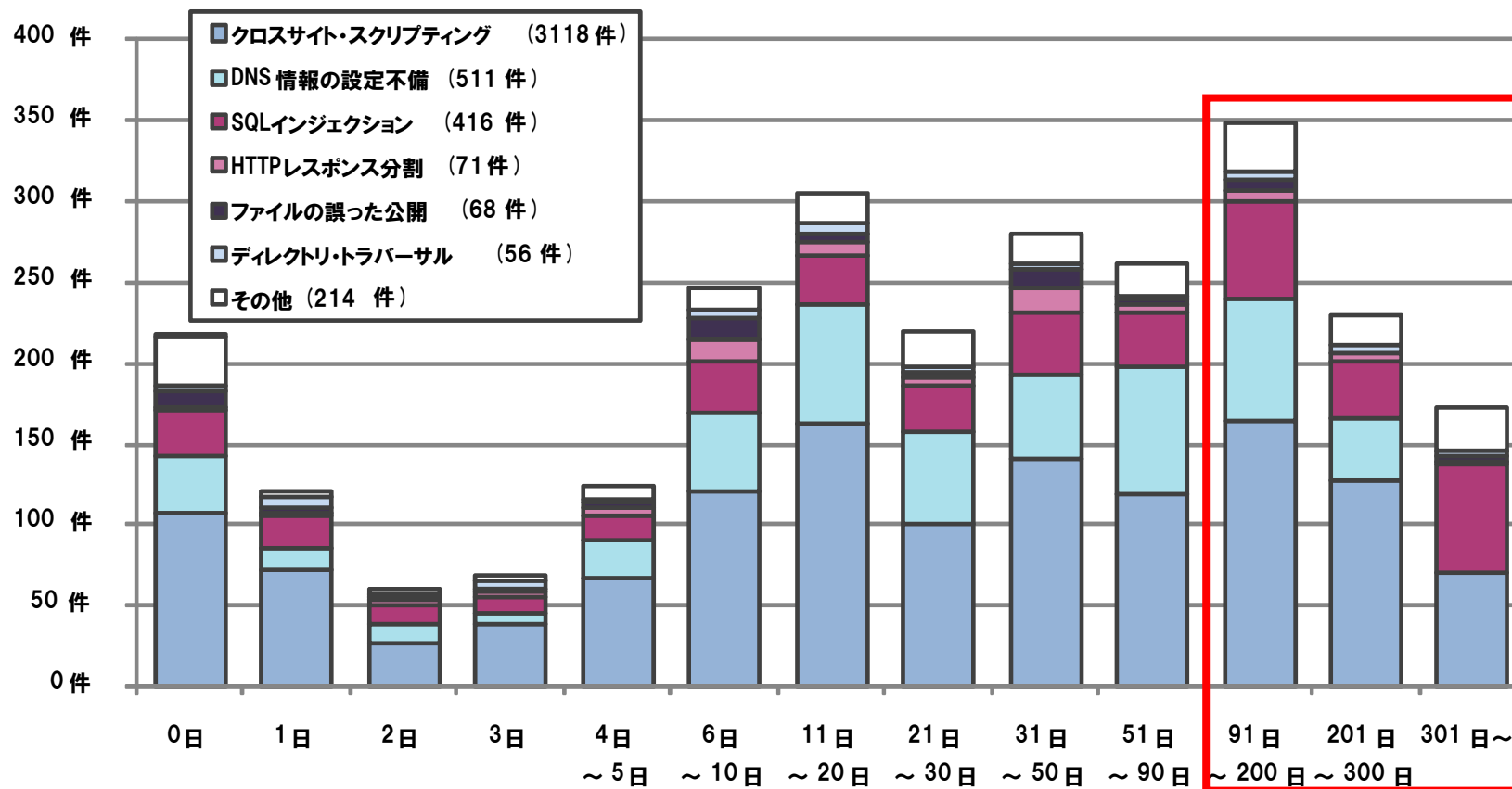


図1.脆弱性関連情報の届出件数の四半期別推移

今なお脆弱性の潜在しているウェブサイトが多い！

実情は(修正期間)

● ウェブサイトの修正作業の長期化



危険な脆弱性においても修正作業は長期化！

何故修正が進まないのか？

- 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

ウェブアプリケーションを修正することが困難な場合がある

1. はじめに
2. ウェブサイトを取り巻く状況
- 3. IPAのWAFに関する取り組み**
4. WAFの導入におけるポイント
5. まとめ



IPAのWAFに関する取り組み

- ウェブサイトのセキュリティ対策の1つとして
WAF が有効である
 - 継続するウェブサイトへの攻撃
 - 脆弱性の修正が長期化する事例

韓国でも効果が挙げられた事例あり

WAFの導入促進を目的とした施策の実施

IPAのWAFに関する取り組み①

● 安全なウェブサイトの作り方

安全なウェブサイトの作り方

改訂第4版

ウェブアプリケーションのセキュリティ実装とウェブサイトの安全性向上のための取り組み

独立行政法人 情報処理推進機構
 セキュリティセンター

2010年1月

2.6 WAFによるウェブアプリケーションの保護

2.6 WAFによるウェブアプリケーションの保護

ウェブアプリケーションの安全を確保するには、脆弱性を作り込まないことや、脆弱性が発見されたら早期に該当箇所を修正することが重要です。一方、そのようなウェブアプリケーションの実装面での対策とは別に、ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護する運用面での対策として、WAF (Web Application Firewall) の使用があります。

WAF は、ウェブアプリケーションを含むウェブサイトと利用者との間で交わされる HTTP (HTTPS 通信を含む²⁾) を検査し、攻撃などの不正な通信を自動的に遮断するソフトウェア、もしくはハードウェアです。WAF を使用することで以下の効果を期待できます。

- 脆弱性を悪用した攻撃からウェブアプリケーションを防御する
- 脆弱性を悪用した攻撃を検出する
- 複数のウェブアプリケーションへの攻撃をまとめて防御する

WAFの動作イメージ

Web Application Firewall (WAF)

WAFの動作イメージ

ウェブアプリケーションの開発状況や運用状況によっては、ウェブアプリケーションの実装面での対策よりも、WAFの使用が有効な場合があります。

改訂第4版で安全性向上のためWAFによる保護に言及

IPAのWAFに関する取り組み②

- Web Application Firewall読本



ウェブサイト運営者に向けた読本

1. はじめに
2. ウェブサイトを取り巻く状況
3. IPAのWAFに関する取り組み
4. **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
5. まとめ



WAFの導入におけるポイント



1. はじめに
2. ウェブサイトを取り巻く状況
3. IPAのWAFに関する取り組み
4. **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
5. 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

(初期費用+ランニングコスト)と(ウェブアプリケーション修正費用)

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

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

【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

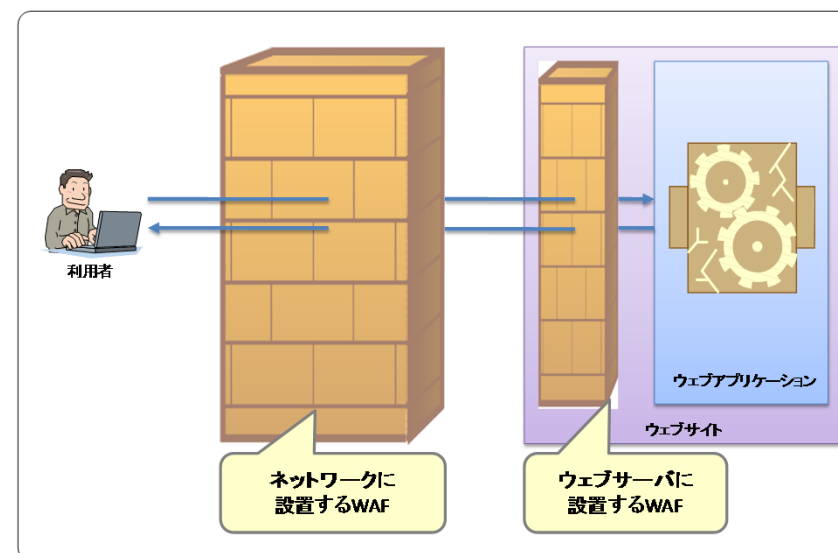
ネットワークに設置するタイプのWAFには以下の特徴がある。

- ・ 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

サーバに設定するタイプの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



【参考】WAFの検査機能

● ブラックリスト

ー ブラックリストとは

HTTP/HTTPS通信における「不正な値、またはパターン」をブラックリストとして定義し、ブラックリストに合致したときに、そのHTTP/HTTPS通信を不正な通信として検出

ー 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は依存しない

【参考】WAFの検査機能

● ホワイトリスト

ー ホワイトリストとは

HTTP/HTTPS通信における「正しい値、またはパターン」をホワイトリストとして定義し、ホワイトリストに合致しないときに、そのHTTP/HTTPS通信を不正な通信として検出

ー 特徴

- ホワイトリストを定義しているパラメータについては未知の攻撃にも対応できる
- ウェブアプリケーションの視点で作成されるため、ウェブアプリケーション毎に「ホワイトリスト」を作成する必要がある

1. はじめに
2. ウェブサイトを取り巻く状況
3. IPAのWAFに関する取り組み
4. **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
5. まとめ

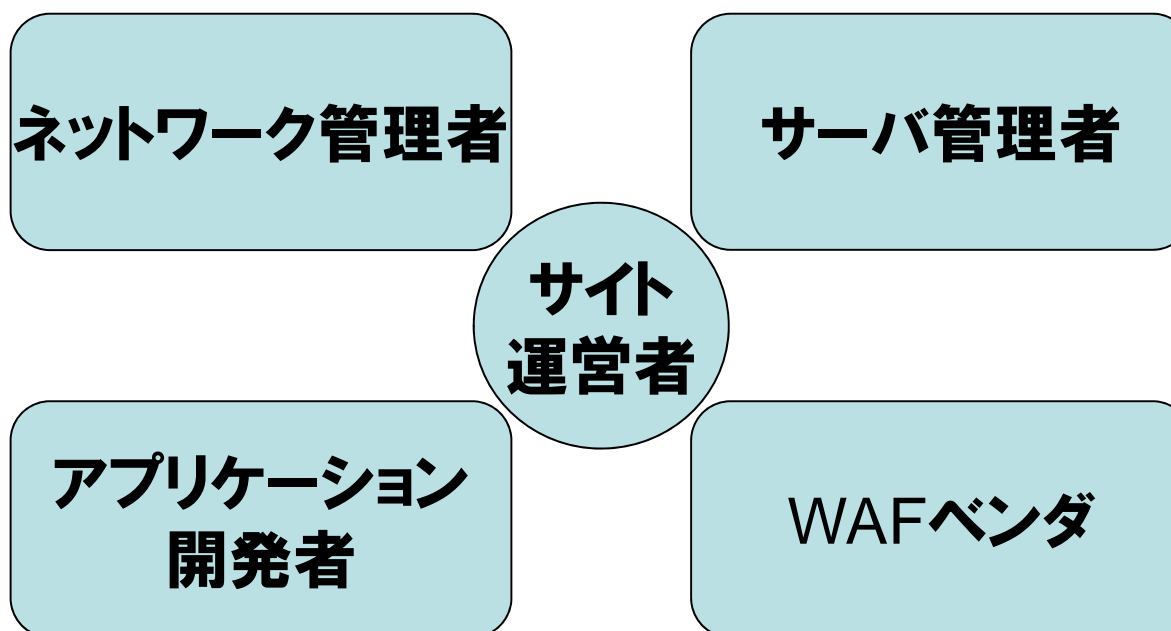


導入：関係者間調整



● 関係者間調整

導入をスムーズに進めるためにも、事前にステークホルダ間の調整を行なっておく必要がある。以下は一例。



導入：導入計画

IPA®



● 導入計画

一 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

一 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

一 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

一 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

一 運用方法

運用の体制、運用方法を検討

導入:運用計画



● WAF障害時の運用確認

WAF自体の障害発生時のシステムへの影響を確認しておく

－ WAF本体の物理的障害(電源異常等)

- フェイルオープン、フェイルクローズ
- 復旧方法

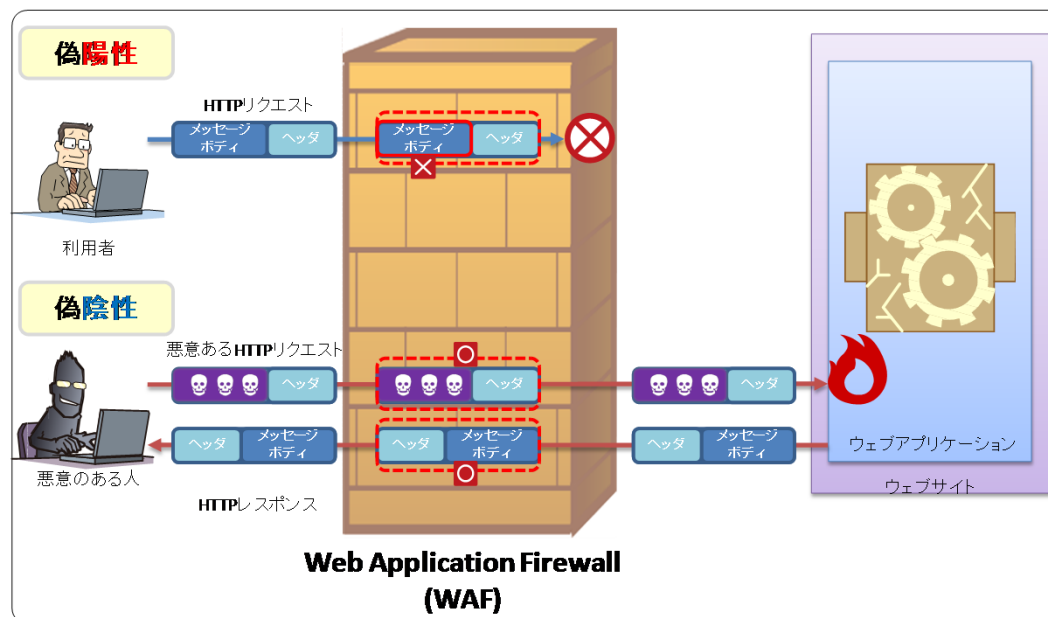
－ WAFモジュールの異常

- フェイルオープン、フェイルクローズ
- 復旧方法

導入: 検証

事前検討	導入	運用
WAF検討	関係者間調整	通常運用
WAF選定	導入計画	緊急対応
	運用計画	保守
	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する

導入: 検証

IPA[®]



● 性能測定

WAF適用時の性能への影響を測定

ー TAT(ターンアラウンドタイム)

システムに処理を送ってから、結果の出力が終了するまでの時間

ー スループット

単位時間当たり転送量

ー リソース消費

CPU、メモリ容量、HDD容量

1. はじめに
2. ウェブサイトを取り巻く状況
3. IPAのWAFに関する取り組み
4. **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
5. まとめ



運用:通常運用



● 通常時の運用

ー「ブラックリスト」の更新

- ・ 更新手順、更新のタイミング、影響の確認手順の確立

ー「ホワイトリスト」の更新

- ・ 更新手順、更新のタイミング、影響の確認手順の確立

ー WAFのバージョンアップや修正プログラムの適用

- ・ 更新手順、更新のタイミング、影響の確認手順の確立

ー 定期的なログの確認

- ・ ログの確認手順の確立

運用: 緊急対応

IPA®



● 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

- － インシデントの発生
- － 偽陽性判定の発生
- － WAF自体の障害
 - ・ ハードウェア障害
 - ・ ソフトウェアの異常終了

運用:保守



● 保守契約の更新

ー 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

ー 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
2. ウェブサイトを取り巻く状況
3. IPAのWAFに関する取り組み
4. WAFの導入におけるポイント
5. まとめ



まとめ

- WAFはウェブサイトのセキュリティ対策の1つ
 - －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
 - －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
 - －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