Orchestrating a brighter world NEC

Webアプリケーションファイアウォール

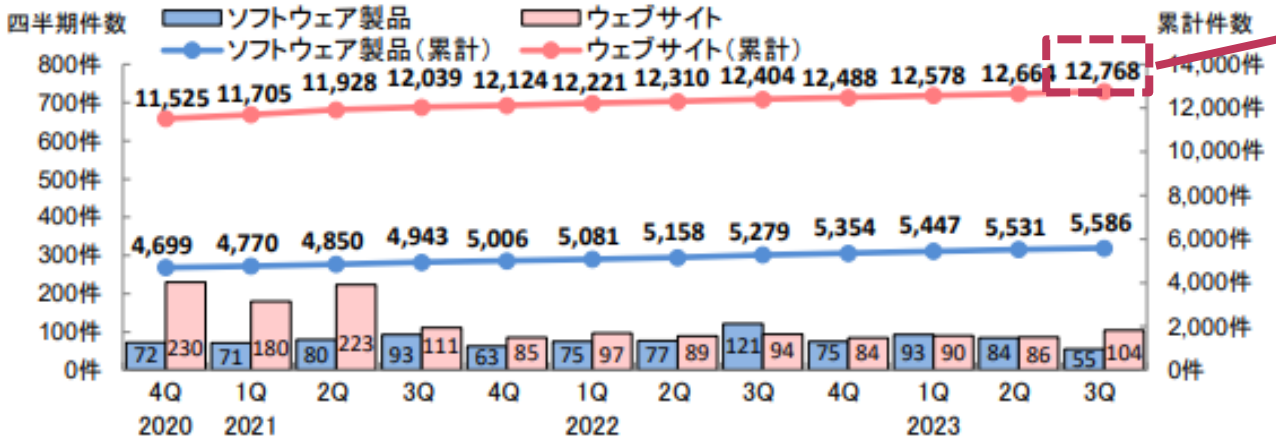
InfoCage SiteShell ご紹介資料

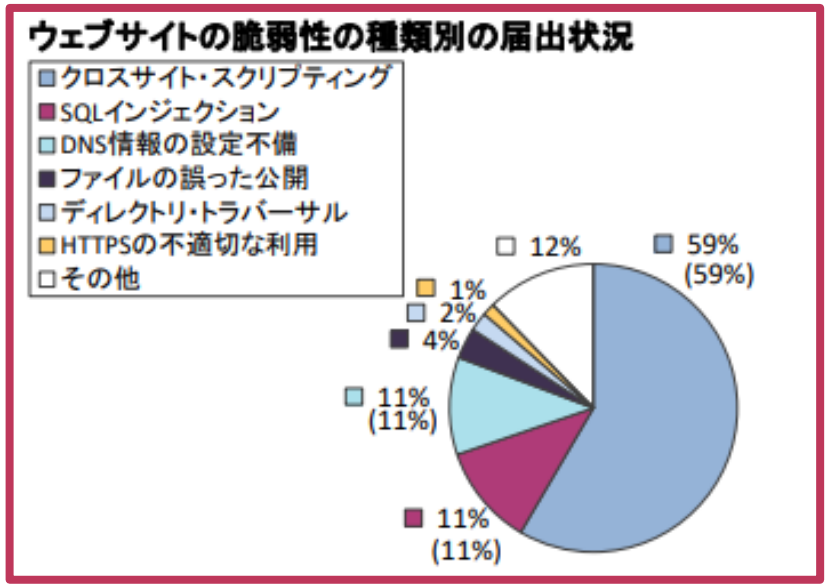
日本電気株式会社
セキュリティ事業統括部

Webサイトの脆弱性届出状況

- IPAおよびJPCERTが2023年10月19日に発表した「ソフトウェア等の脆弱性関連情報に関する届出状況（2023年第3四半期（7月~9月））」によると、**Webサイトの脆弱性に関する届出が全体の約7割**と、依然として高い比率を占めています。

極めて多いWebサイトの脆弱性





（出典）
IPA「ソフトウェア等の脆弱性関連情報に関する届出状況（2023年第3四半期（7月~9月））」

Webサイトの3大被害

① 機微な情報の流出

■顧客、取引先、従業員などの個人情報（名前、住所、生年月日、性別、血液型、メールアドレス、電話番号、クレジットカード情報　etc）など機微な情報が漏洩すると、**プライバシー権侵害にあたり、損害賠償責任を問われる加害者**となり得ます。

② Webサイトの改ざん

■官公庁、自治体、企業など情報発信サイトの静的コンテンツ、ECサイトのクレジットカード決済プログラムのような動的コンテンツが改ざん被害の対象です。**改ざん被害によって個人情報を漏洩させてしまうと、一転して加害者**となり得ます。

■プログラムが改ざんされると、ウィルスメールやスパムメールを送信したり、他のWebサイトへ大量のリクエストを送信する**「DoS攻撃」に利用され、加害者となり得ます**。

③ Webサイトの閲覧不可

■短時間に大量のリクエストを受け、Webサイトが高負荷でリソースが枯渇した状態になることで、通常の利用者がWebサイトを閲覧できなくなります。

脆弱性対策が不十分なまま放置していると被害者になるだけでなく、意図せず加害者になる可能性があります

Webサイトの被害をどう防ぐ？

① 機微な情報の流出
② Webサイトの改ざん

■Webサイト上で動作するアプリケーションの脆弱性への対策

WAF（WebApplicationFirewall）の導入

クロスサイトリクエストフォージェリ、SQLインジェクションといった攻撃に有効

■Webサイトのネットワークやプラットフォームの脆弱性への対策

FWやIPS/IDSの導入

OSやCMS（Contents Management System）、サーバ運用のためのソフトウェアの脆弱性を狙った攻撃に有効

■社員・パートナーへの教育によるセキュリティ意識向上による対策

啓蒙・意識改革、教育

簡単なID/PW、PW使いまわしの禁止、内部犯行などに有効

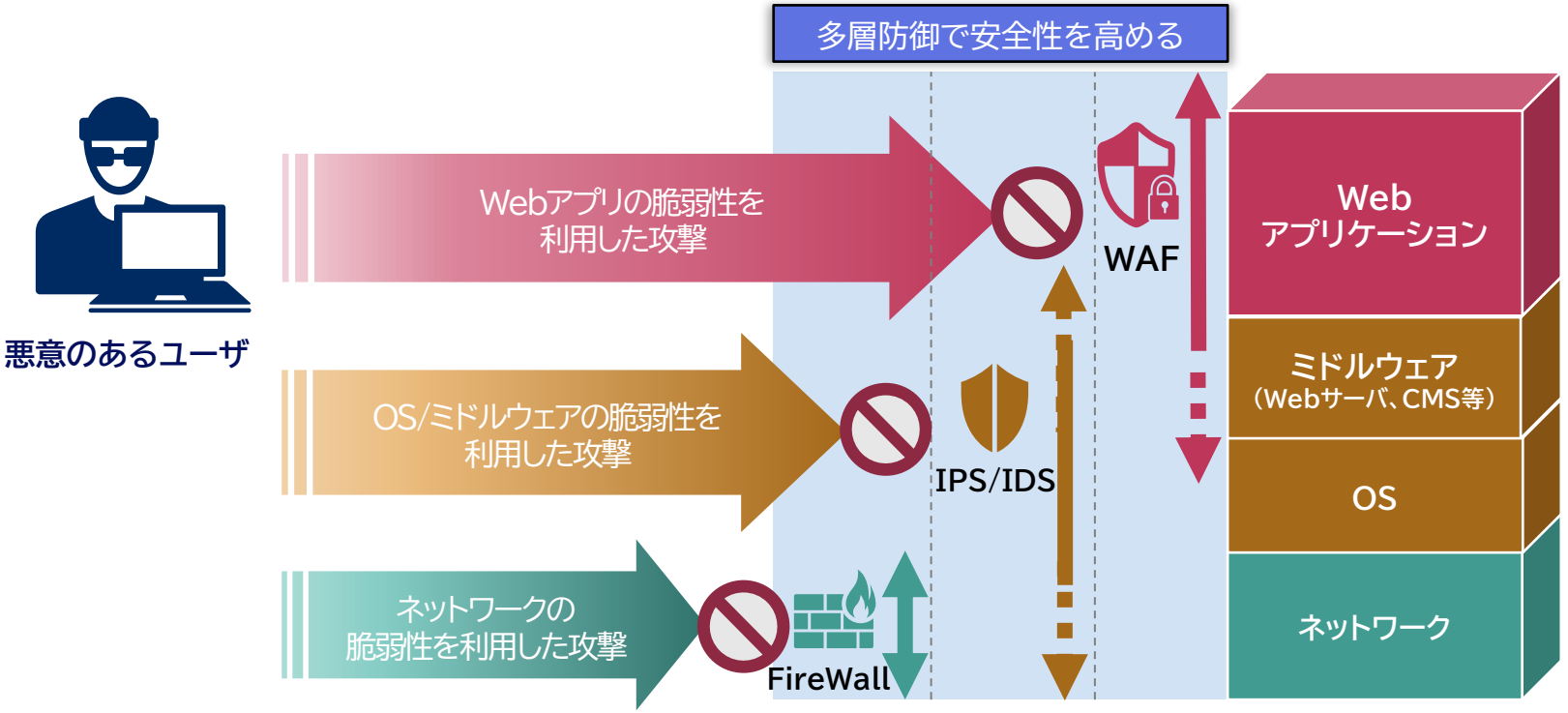
③ Webサイトの閲覧不可

■DoS/DDoS攻撃への対策

UTMやIPS/IDSの導入

WAF（WebApplicationFirewall）とは？

- WAFはインターネットからの不正アクセスを防ぐためのセキュリティツールです。FWやIPS/IDSでは防ぎきれない、Webアプリケーションへの攻撃を防御します。
- ネットワーク、OS・ミドルウェア、Webアプリケーション、抜け目のない各層防御がWebサイト全体のセキュリティを高めます。

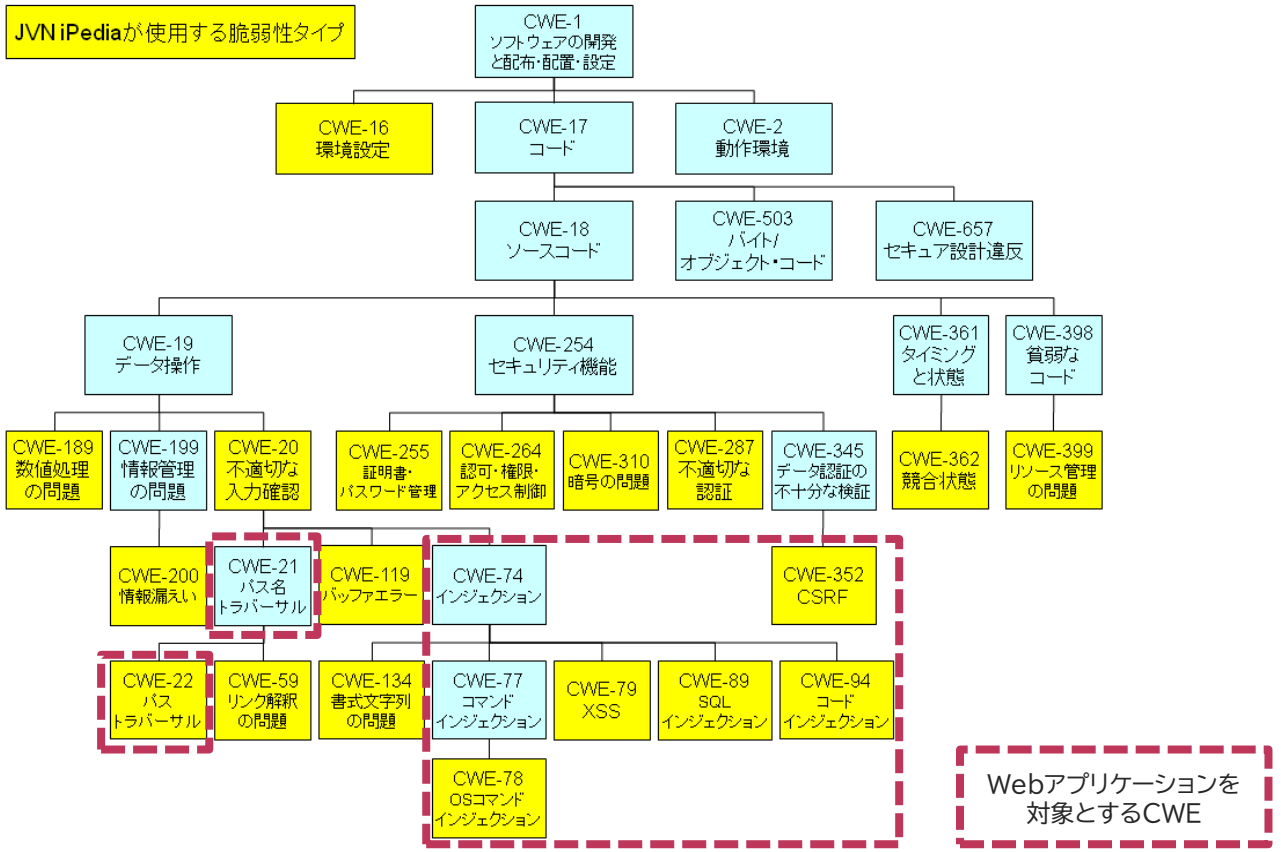


WAFが担う役割の重要性

- 危険な脆弱性タイプのトップ25において、Webアプリケーションを対象とするものが多数ランクインしており、WAFが担う役割の重要性がわかります。

第1位:Out-of-bounds Write(CWE-787)
第2位:Cross-site Scripting(CWE-79)
第3位:SQL Injection(CWE-89)
第4位:Use After Free(CWE-416)
第5位:OS Command Injection(CWE-78)
第6位:Improper Input Validation(CWE-20)
第7位:Out-of-bounds Read(CWE-125)
第8位:Path Traversal(CWE-22)
第9位:Cross-Site Request Forgery(CWE-352)
第10位:Unrestricted Upload of File with Dangerous Type(CWE-434)
:

(出典)2023MITREの危険な脆弱性タイプのトップ25



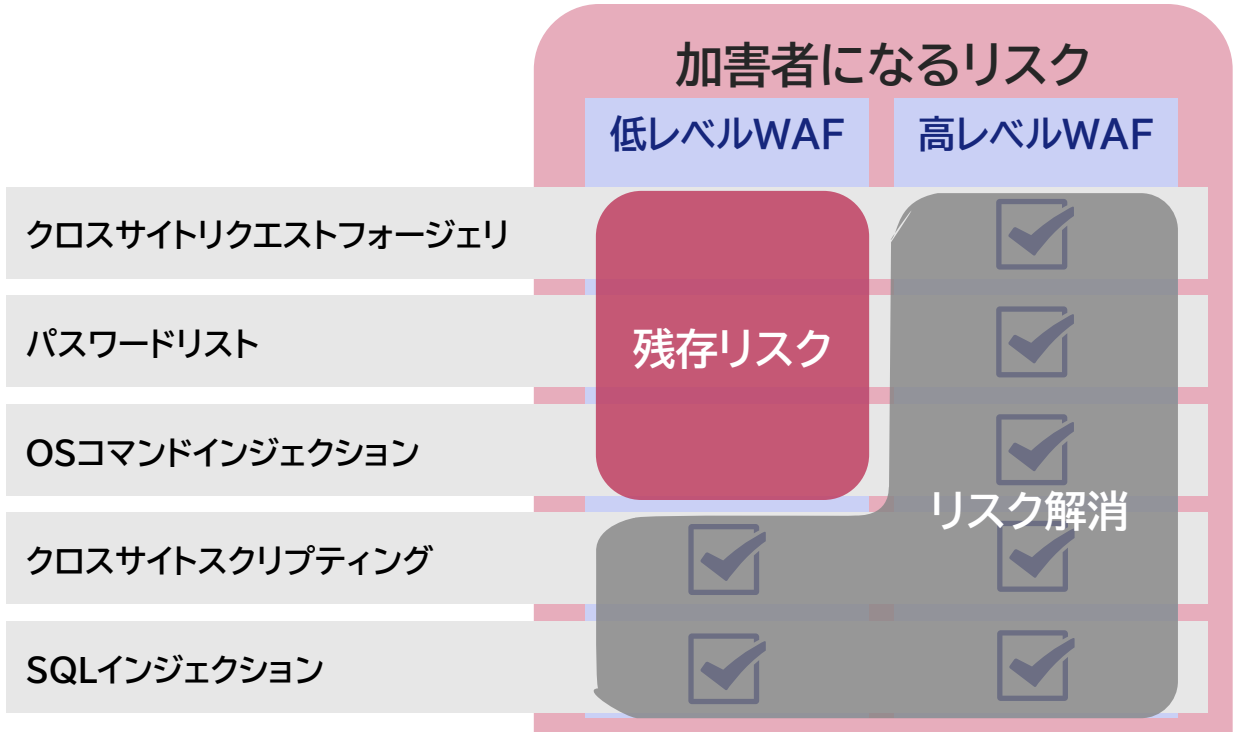
(出典)IPA「共通脆弱性タイプ一覧CWE概説」

どんな攻撃を防御できるのか？

◆ Webアプリケーションの脆弱性を利用した下記のような攻撃が防御可能です。

- SQLインジェクション
- クロスサイトスクリプティング
- セッションハイジャック/リプレイ
- OSコマンドインジェクション
- パストラバーサル
- バッファオーバーフロー
- パラメータ改ざん
- クロスサイトリクエストフォージェリ
- 強制的ブラウズ
- エラーコード
- パスワードリスト型攻撃
- Cookieの脆弱性攻撃
- 既知の攻撃元IPからのアクセス

WAF製品・サービスは多数ありますが、
防御機能差があり、概ね価格も比例します



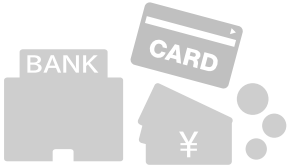
WAFを導入すべきWebサイトは？

- 機微な情報を扱うWebサイト、機会損失を嫌うWebサイトはもちろんですが、
  脆弱性被害によって加害者となるリスクを軽減するためには、
  全てのWebサイトにWAFを導入すべきです。

ECサイト

会員登録サイト

メーカー直販サイト



オンライントレード

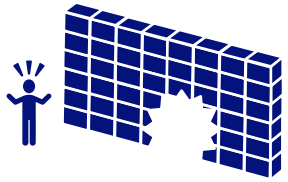
地方特産・名産品販売サイト

自社サーバのWebサイト

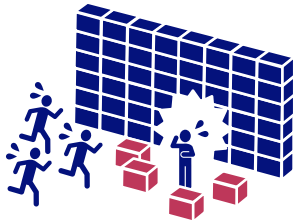
どうしてWAFが必要なのか？

◆ 脆弱性被害を受けないためには、Webアプリの脆弱性を改修できればいいわけですが、次々と発生する攻撃に追いつけません。WAFは本格対処（Webアプリ改修）までの暫定対処として、素早く攻撃被害からWebサイトを守ります。

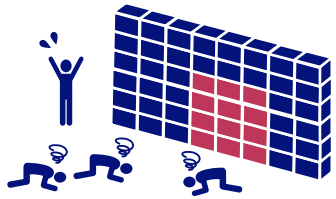
本格対応（Webアプリ改修）イメージ



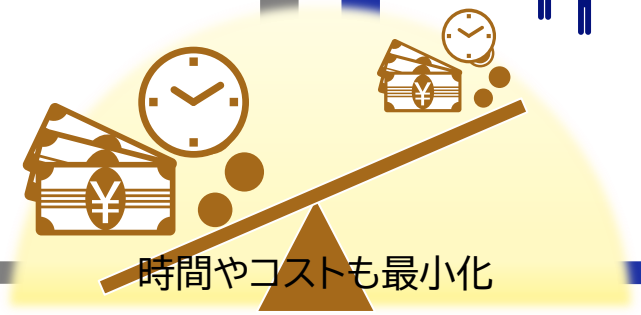
穴（脆弱性）を発見



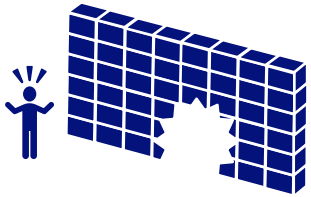
穴を塞ぐ方法を検討し
工事（Webアプリ改修）を人手をかけ
急ピッチで実行



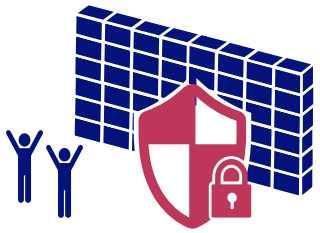
穴を塞いで対応完了



WAFによる対応イメージ



穴（脆弱性）を発見



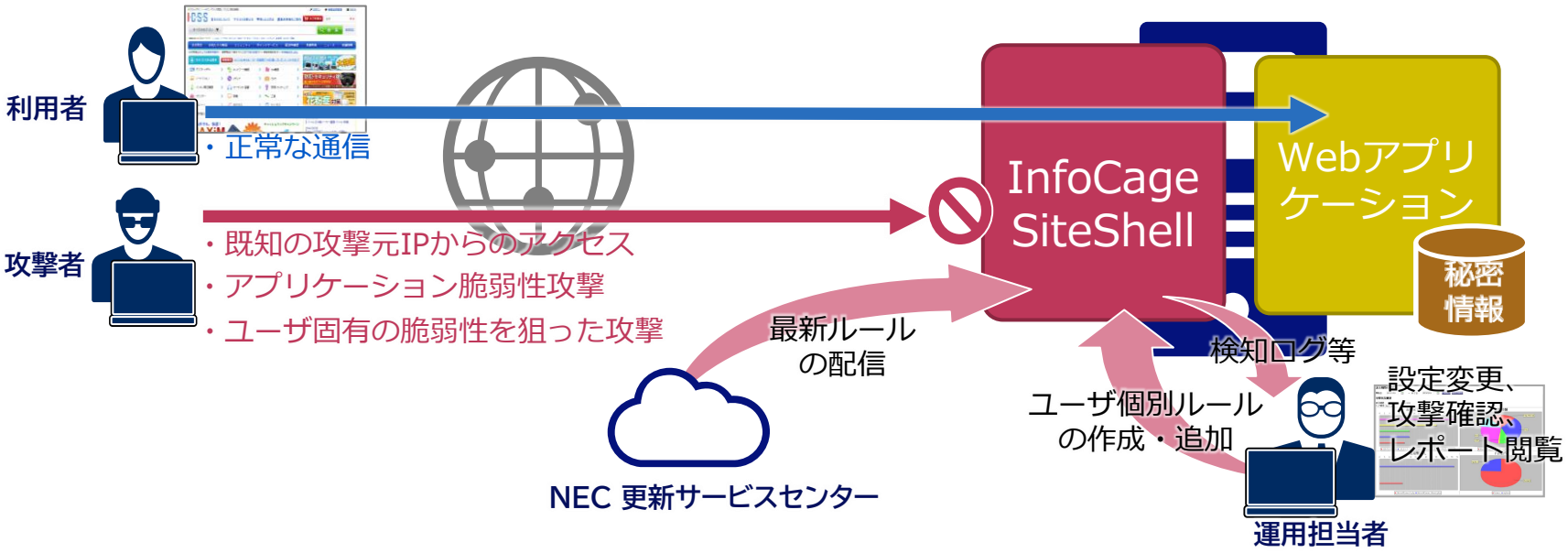
即座にWebアプリの
前段に盾（WAF）を
設置して対応完了

本格対処とすることも
可能です

NECのWAF製品「InfoCage SiteShell」

InfoCage SiteShell 利用イメージ

- Webアプリケーションの前段にインストールした InfoCage SiteShell は、WAFプログラムと「シグニチャ」と呼ばれる攻撃対策ルールで構成されます。
  次々発生する新しい攻撃に対抗する攻撃対策ルールをNECから配信しており、これが自動適用されることで、常に攻撃から守られた状態を保ちます。



最新ルール＋個別ルールによる攻撃防御

InfoCage SiteShell 機能一覧

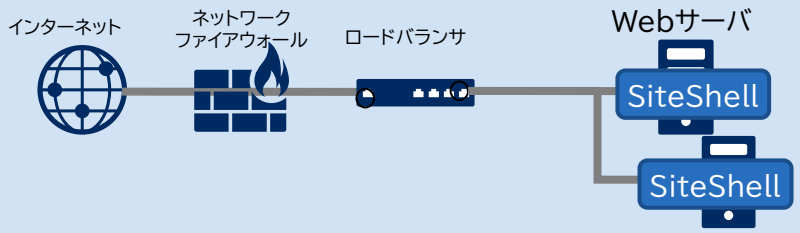
機能	概要	デフォルト設定
攻撃対策機能	SQLインジェクション対策	ON
	クロスサイトスクリプティング対策	ON
	セッションハイジャック対策	ON
	OSコマンドインジェクション対策	ON
	パストラバーサル対策	ON
	HTTPプロトコルのメソッド対策	ON
	バッファオーバーフロー対策	OFF
	クロスサイトリクエストフォージェリ対策	OFF
	パラメータ改ざん対策	OFF
	強制的ブラウズ対策	OFF
	エラーコード対策	OFF
	Cookieに関する脆弱性攻撃対策	OFF
	パスワードリスト攻撃対策	OFF
	ユーザ個別の攻撃対策　※ユーザ個別ルール	OFF
	ユーザ個別の攻撃元IPリスト	OFF
予兆検知機能	攻撃予備動作となる文字列のリスト	OFF
運用管理機能	専用管理コンソールによる、GUIでの攻撃状況確認、設定変更	ON
	メール、syslog、SNMPトラップによる攻撃検出時の通知	OFF
	脆弱性対策PKGのオンライン自動更新(オフライン手動更新も可能)	ON
オプション機能(別売り)	Webコンテンツ改ざん検知/自動復旧　※Windows版のみ	ー

InfoCage SiteShell 導入形態

◆ インストールしてご利用頂く「ソフトウェア型WAF」ですが、お客様環境・要件に合わせて、様々な導入形態を用意しています。
ソフトウェア型WAFとしては、業界No.1製品です。

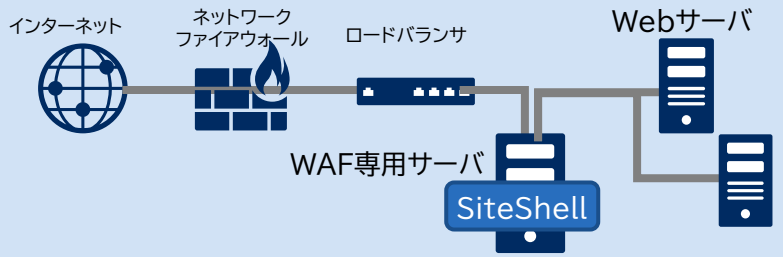
※出典：富士キメラ『2021ネットワークセキュリティビジネス調査総覧（市場編）』

ホスト型



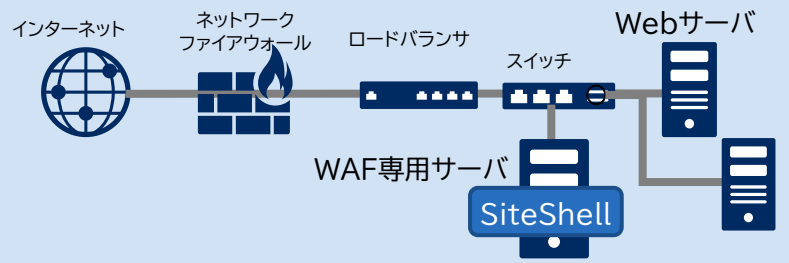
Webサーバにインストール
※Apache、IIS、WebOTX ASに対応
※1ライセンスで防御可能なFQDN数は2まで

ネットワーク型



Webサーバ前段に設置した
WAF専用サーバにインストール
※1ライセンスで防御可能なFQDN数に制限なし

スニファ型（検知専用）



スイッチのミラーポートに接続したWAF
専用サーバにインストール
キャプチャしたリクエストパケットのみを対象とした
攻撃検知のみ可能

InfoCage SiteShell 導入までの流れ

◆ 約1～2週間程度で安全に導入可能です。

■ インストールは数分ですが、過剰検知が出ないための評価・調整に約1～2週間を要します。

①インストール
数分で完了します。

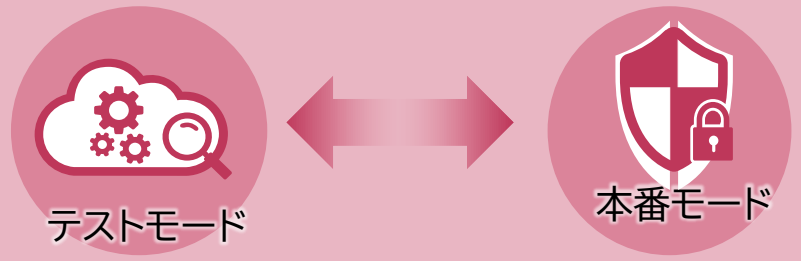
②初期設定
デフォルトでも多くの脆弱性に対応していますが、適宜脆弱性対応設定を変更します。

③評価・調整（過剰検知防止）
通常1～2週間程度

お客様Webサイトでの正常な通信を標準の攻撃対策ルールが攻撃と判断してしまう可能性があります。（過剰検知）
お客様Webサイトが正常に利用できることを評価し、過剰検知発生の場合、該当ルールを除外するなどの調整を行います。

④本番移行
防御を開始します。

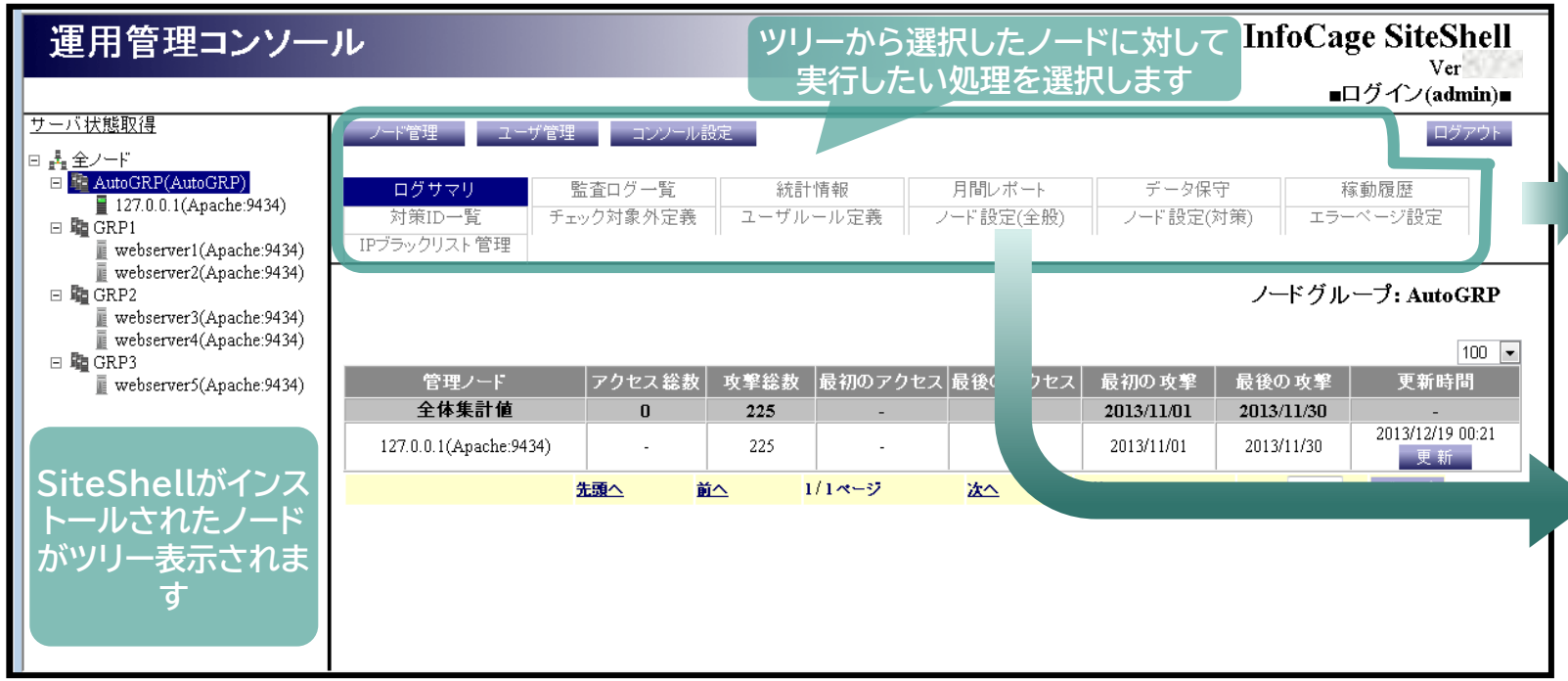
対応脆弱性一覧	SiteShell	他社WAF（例）
クロスサイトスクリプティング対策 SQLインジェクション対策	デフォルトで有効 インストールするだけで 対応完了	既定
セッションハイジャック/リプレイ対策 OSコマンドインジェクション対策 パストラバーサル対策 HTTPプロトコルのメソッド対策		個別設定が必要

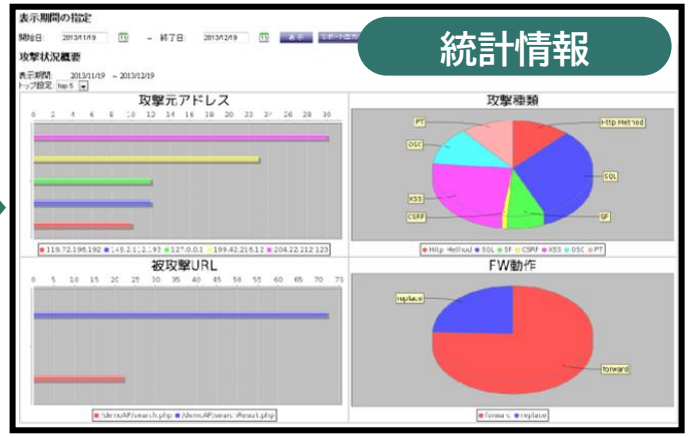


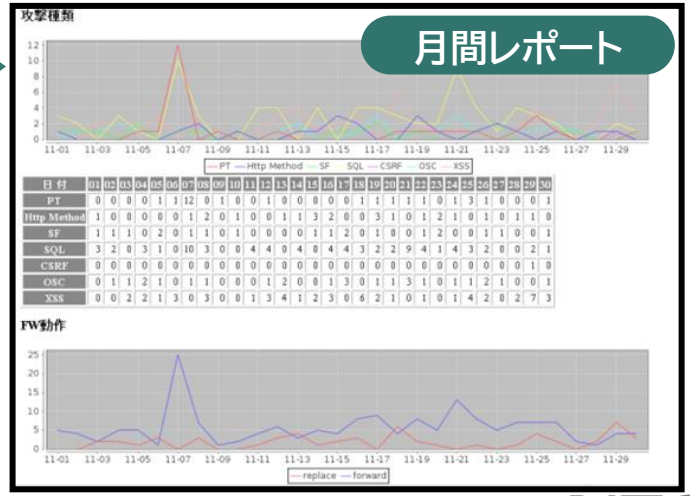
テストモードは、攻撃の有無のみ行い、その結果を監査ログに出力するものです。SiteShellを既存Webサイトに導入するケースでは、「③評価・調査」をテストモードで行い、「④本番移行」のタイミングで本番モードに切り替えることが可能です。

InfoCage SiteShell 運用管理機能

◆ 標準添付の「運用管理コンソール」を使えば、ブラウザ操作で簡単に運用可能です。
レポートは経営層向けの報告に活用可能です





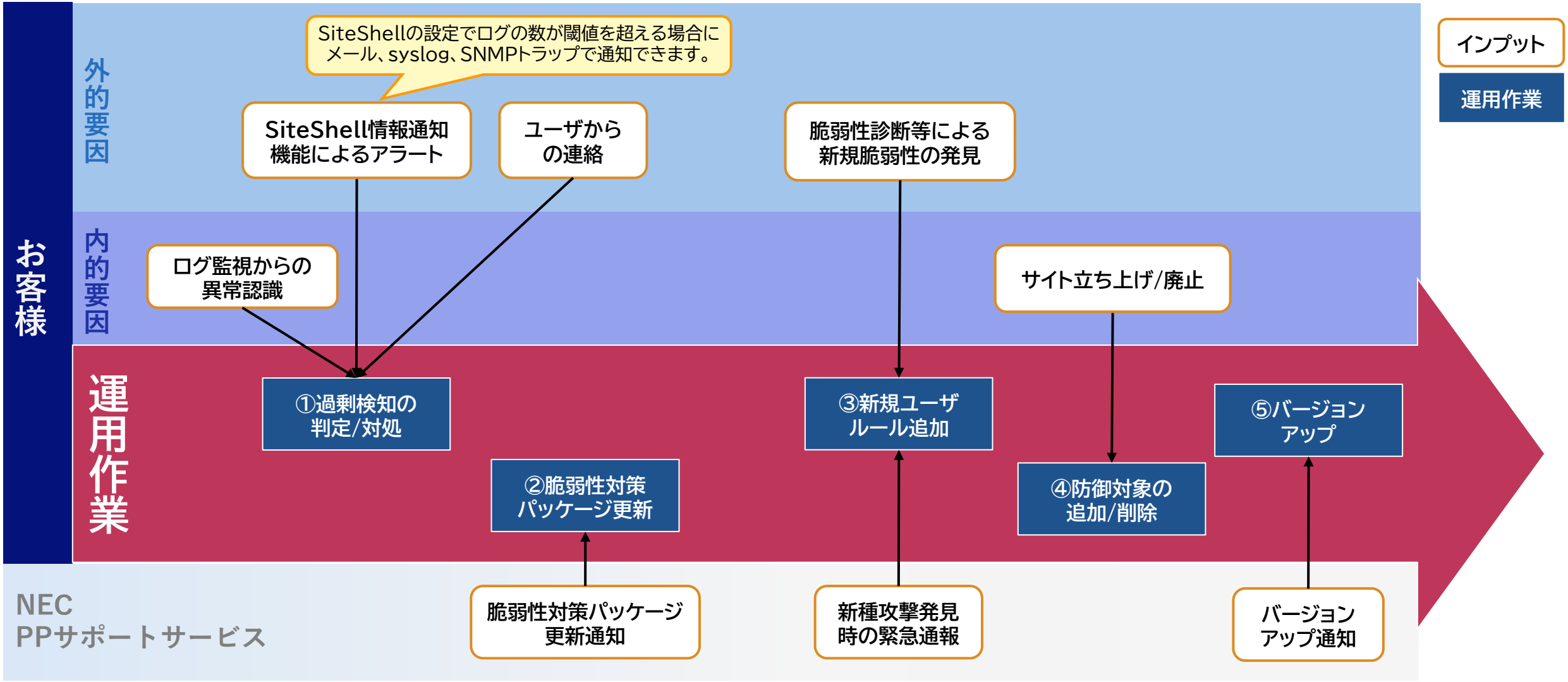


ログやレポートの確認 監査ログの閲覧、統計情報や月間レポートの確認などが可能です。

SiteShellの設定変更 過剰検知時の除外設定、ユーザ個別ルールの適用などが可能です。

複数ノードの一元管理 セキュリティポリシーを同一とする「管理グループ」毎に一括アクションが可能です。

InfoCage SiteShell 運用作業



InfoCage SiteShell NECから提供するルール

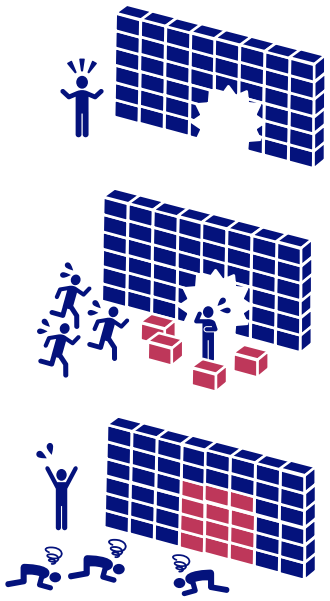
- NECの更新サービスセンターにて、多様な情報源から最新攻撃情報を収集/分析し、サイバーセキュリティの知見とWebサーバ開発により培った技術を基に、各攻撃対策に必要なルールを適宜提供しています。

ルール	配信内容	配信タイミング
脆弱性対策パッケージ	どのお客様にも適用すべき対策ルール群	定期
個別ルール	緊急性の高い脆弱性への対策ルール 特定条件を満たすお客様のみ適用すべき対策ルール	随時

InfoCage SiteShell 自動適用可能な脆弱性対策パッケージ

◆ 定期配信される脆弱性対策パッケージは自動適用され、新たな攻撃への防御が強化されます。(脆弱性対策パッケージは手動適用することも可能です。)

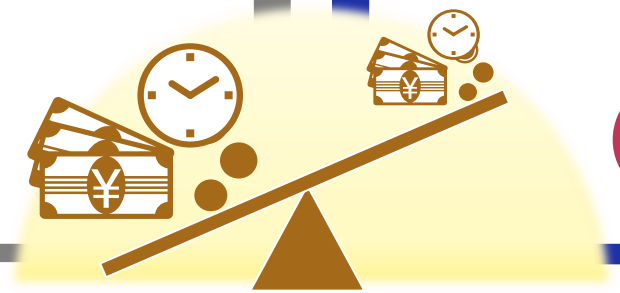
Webアプリ改修による対応イメージ



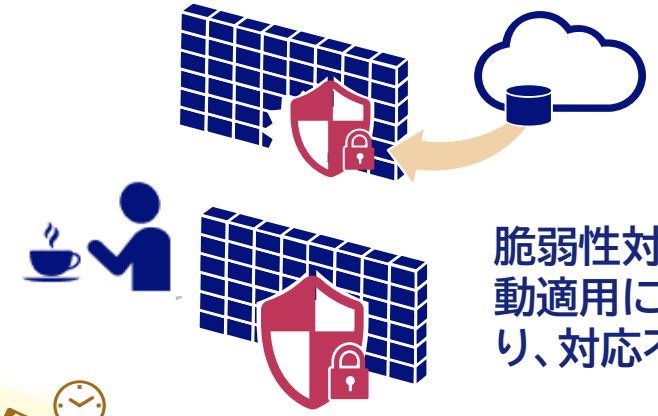
穴(脆弱性)を発見

穴を塞ぐ方法を検討し
工事(Webアプリ改修)を人手をかけ
急ピッチで実行

穴を塞いで対応完了



WAFによる対応イメージ



脆弱性対策パッケージの自動適用によって、穴が塞がり、対応不要

時間やコストが最小化

【参考事例】Apache Log4j 脆弱性(CVE-2021-44228)

新しい脅威に素早く構えられる InfoCage SiteShell の対応力

2021年12月10日(金)午後の公開後、契約ユーザ向けに即日ユーザルール定義を公開

NECのWAF管理センターでは、Webアプリケーションの脅威となる**脆弱性ニュースを日々ウォッチ**しています。

公開された攻撃手法を基に、定義作成、過剰検知確認を含めた評価を実施後、ユーザルール定義の公開に至りますが、この後も攻撃手法の変化に監視を続けています。

12/10(金)夜にユーザルール定義を公開後、週明けにかけて、これをバイパスする攻撃手法が次々発見されており、

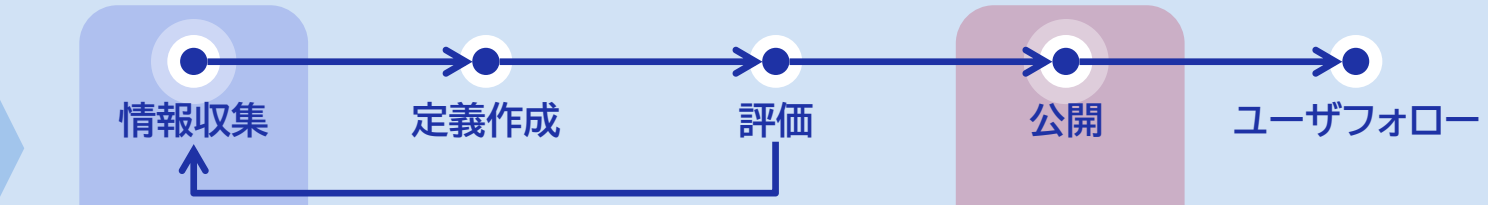
12/13(月)までに、2回のアップデート版を公開しました。

リスクに晒された状態から、平常状態に戻すまでの時間は重要

社外Webサイト

NECサポートポータル

ユーザルール定義公開までのステップ

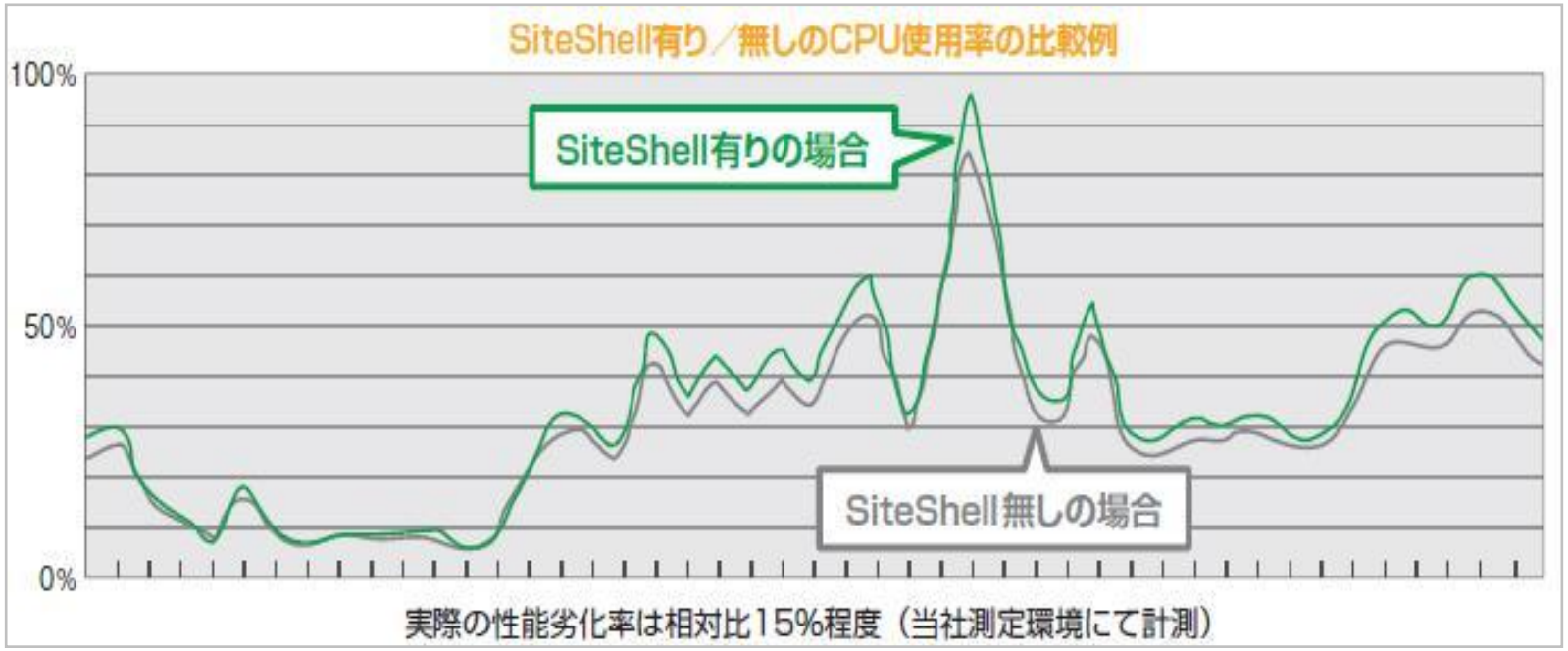


ここが最もスキルと手間を要するステップ

次回の定期配信便「脆弱性対策パッケージ」への取込検討対象となる

InfoCage SiteShell 導入による影響

- SiteShell は、インストールしたサーバ性能に大きな影響を与えません。
  下記グラフは SiteShell 有り／無しでのWebサーバのCPU使用率を示すものですが、性能劣化率は相対比15%程度と小さく、一般的なWebサーバの運用状況では影響ないレベルです。



当社測定環境でのレスポンスは、1アクセスで平均12～20msec程度の遅れであり、体感できる遅延ではありませんでした。

この計測値はWebサーバ（IIS、Apache）とaspやphpを組み合わせて、Webアプリを動作させたものです。
従って、計測条件が異なる場合、必ずしもこれに近い数値とはならない場合があります。
例えば、極めて軽いWebアプリ処理であったり、単純にAPサーバへのリクエスト転送を行うWebアプリ処理の場合は、相対的にSiteShellの処理の方が重たくなり、この数値よりも悪くなり得ます。

InfoCage SiteShell 価格

導入形態	製品名	最小構成価格	備考
ホスト型	InfoCage SiteShell ホスト型・1年間ライセンス	年額　約600,000円～	• インストール可能なサーバは1台です • SW使用権と保守をセットにした1年間サブスクライセンスです
ネットワーク型	InfoCage SiteShell NW型・4コア・1年間保守付き	初期費用　約4,550,000円～ 次年度以降保守年額　約1,050,000円～	• インストール可能なサーバは1台です • インストール可能なサーバのCPUコア数は4までです • SW使用権は買取となります • 初年度の保守費用を含みます（次年度以降、別途保守のみの手配が必要です） • インストール先サーバ費用は含みません

■ 上記は最小構成を示した一例です。
詳細なお見積りをご要望の際は、下記情報を添えて、NEC営業までお問合わせください。

- 導入形態、通常保守（5d8h）｜延長保守（7d24h）、ご利用想定年数
- インストール先サーバ台数、CPUコア数（ネットワーク型の場合のみ）
  - CPUコア数は論理プロセッサ数となります。
  - ネットワーク型SiteShellをインストールするWAF専用サーバを冗長構成にする場合、冗長形態（両現用｜現用/予備）も必要です。
  - ネットワーク流量を基にしたWAF専用サーバの選定はお客様にてお願いいたします。

InfoCage SiteShell 動作環境

ホスト型

OS(x64)	Windows Server 2012 、2012R2、2016、2019、2022
	RedHat Enterprise Linux v.6、v.7、v.8、v.9
	Rocky Linux v.8、v.9
	CentOS v.6、v.7、v.8、CentOS Stream8
	Amazon Linux 、Amazon Linux2、Amazon Linux2023
Webサーバ	Internet Information Services 8.0、8.5、10.0
	Apache HTTP Server 2.4
	WebOTX Application Server V10.2、10.3、10.4、11.1

＊コンテナの作成および動作確認は、CentOS v.7、Rocky Linux v.8、v.9のコンテナイメージを使用しております。
詳細は『InfoCage SiteShell コンテナイメージ作成ガイド』をご参照下さい
＊Apache Windows版のマルチプロセッシングモジュール（mpm）は、「mpm_winnt」(Windows版のデフォルトモジュール)にのみ対応しています。

ネットワーク型

OS(x64)	RedHat Enterprise Linux v.6、v.7、v.8、v.9
	Rocky Linux v.8、v.9
	CentOS v.6、v.7、v.8、CentOS Stream8
	Amazon Linux 、Amazon Linux2 、Amazon Linux2023

＊リバースプロキシ方式のみ IPv6 にも対応しています。
ルータ方式、ブリッジ方式、スニッフィング方式(スニファ型)は IPv4 のみの対応となります。

詳細は下記サイトをご確認下さい。
InfoCage SiteShell 動作環境 https://jpn.nec.com/infocage/siteshell/requirement.html

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC