【WAF】
クラウドWAF運用の課題と
ベストプラクティスとは？
～WideAngleにおけるWAAPの取り組み～

久保田 雄
マネージド&セキュリティサービス部
セキュリティサービス部門
担当課長
NTTコミュニケーションズ株式会社

F5 AppWorld 2024 TOKYO

クラウドWAF運用の課題と ベストプラクティスとは？ ～WideAngleにおけるWAAPの取り組み～

2024年9月4日

NTTコミュニケーションズ株式会社

自己紹介

NTTコミュニケーションズ
　マネージド&セキュリティサービス部　セキュリティサービス部門

久保田　雄（くぼた　ゆう）

主な経歴

NTTコミュニケーションズ　法人営業部（関西のアカウント営業）
同社　クラウドサービス部（クラウドサービスの企画・運営）
NTTコミュニケーションズ　マネージド&セキュリティサービス部
**　セキュリティサービス（WideAngle）の戦略・企画を主導**

本日の流れ

1．WAFの重要性とWAF運用の課題
　　～これまでの取り組み～

2．Webセキュリティのトレンドとクラウドwaf
　　～これからの取り組み～

3．クラウドWAF運用のベストプラクティスとは？

１．WAFの重要性とWAF運用の課題 ～これまでの取り組み～

Webサービスに関わるサイバー攻撃の動向 ～インシデントの大半はWebサービス～

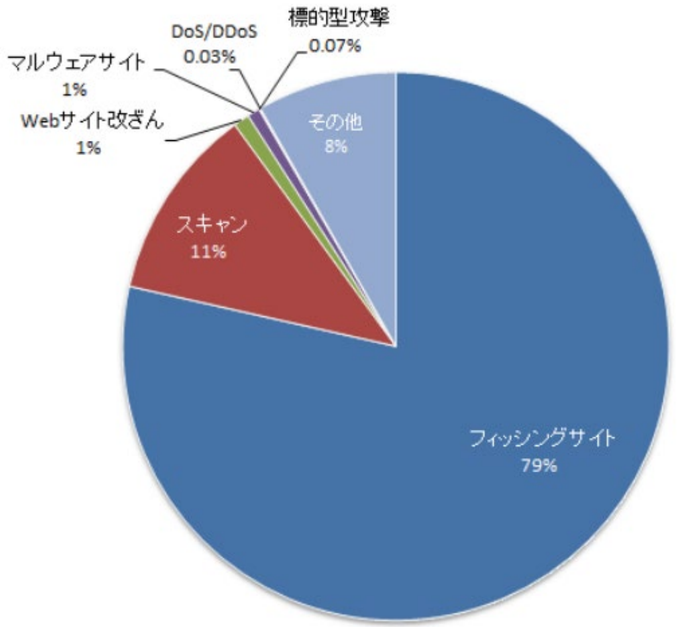
・世の中で発生しているインシデントは、Webサービスに関するものが大半
・Webセキュリティ（Webサイトに対する攻撃への対策）は重要となっている

インシデント報告件数のカテゴリー別内訳（2024年1月～2024年3月）

インシデント	1月	2月	3月	合計	前四半期合計
フィッシングサイト	1,539	1,534	1,708	4,781	4,473
Webサイト改ざん	20	18	19	57	72
マルウェアサイト	11	14	20	45	53
スキャン	280	240	177	697	1,393
DoS/DDoS	0	1	1	2	1
標的型攻撃	2	0	2	4	1
その他	136	149	218	503	455

JPCERTインシデント報告対応レポート
https://www.jpcert.or.jp/ir/report.html

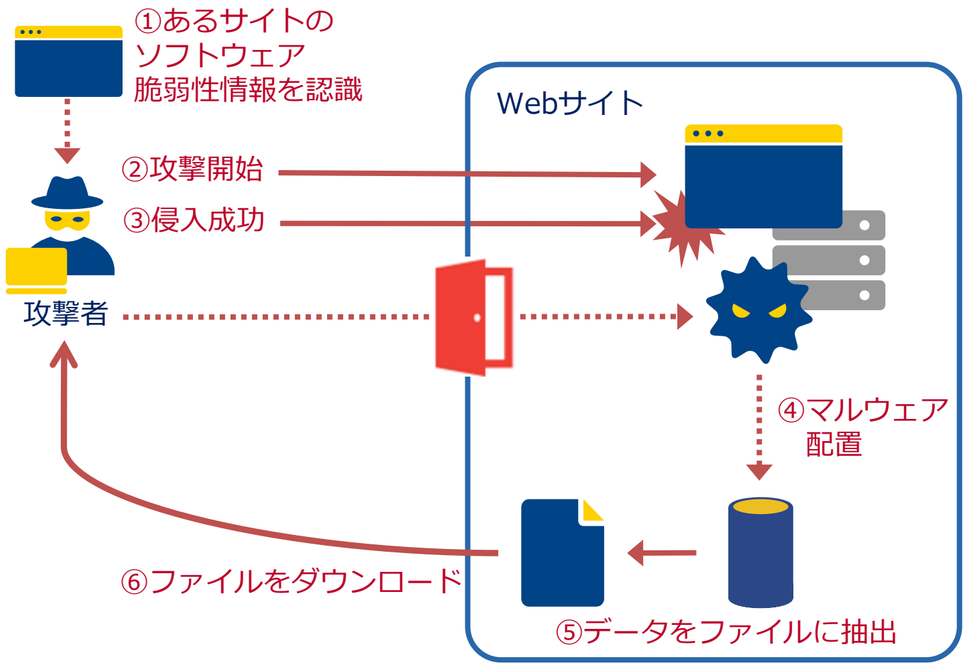
インシデントのカテゴリー別割合



セキュリティ事故の発端となる脆弱性の動向

公開サーバの脆弱性を突いた攻撃による情報漏洩

公開サーバーは外部に対して解放されているため、
攻撃対象になりやすく、脆弱性を残しておくことは非常に危険です。
脆弱性を突いた攻撃は増加しており、
報告される脆弱性の件数も増加しています。



脆弱性（CVE)の報告件数

6,484件
（2015年）

12,174件
（2019年）

1.9
倍

出典：https://www.cvedetails.com/browse-by-date.php

闇市場のビットコイン流入額

$357M
（2015年）

$790M
（2019年）

2.2
倍

企業秘密が
闇市場で売買されている
Zoomの弱点は数億円
出典：日本経済新聞2020/7/20

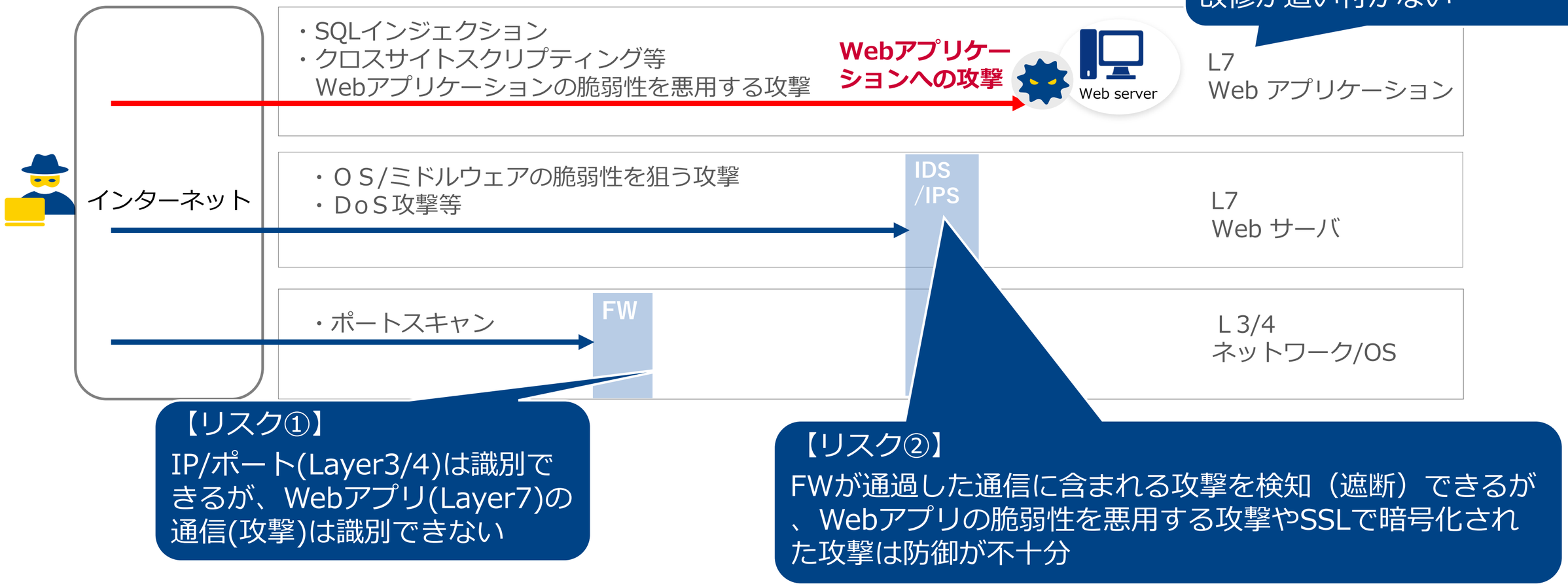
出典：Chainalysis

製品側は報奨金制度で闇市場に対抗！

Webサイトに対する攻撃と従来の対策の課題 ～FWやIPSでは防御しきれない～

Webサイトに対する攻撃はFWやIPSなどの対策では防御しきれません。

・FWやIDS／IPSでは正常な通信と区別がつきません。



WAF（Webアプリケーションファイアウォール）による対策

WAF（Webアプリケーションファイアウォール）を用いて、
従来のFWやIDS/IPSで防ぎきれなかった攻撃に対応します。

・Webアプリケーションの脆弱性を悪用した攻撃を検知・防御します。
・Webアプリケーションへの通信を可視化し、攻撃の頻度や手法、攻撃元を明らかにします。

	FW	IDS/IPS	WAF
ポートスキャン	○	○	×
ＯＳの脆弱性を狙う攻撃	×	○	○
ミドルウェアの脆弱性を狙う攻撃	×	○	○
ＤｏＳ攻撃	×	○	○
Webアプリケーションの脆弱性を悪用する攻撃	×	×	○
SQLインジェクション	×	×	○
クロスサイトスクリプティング	×	×	○

WAF運用の課題

・WAF導入後の**シグネチャ更新やチューニング等の運用がセキュリティ確保の最大の課題**
・シグネチャによる検査は、IPSと同様に、**過検知、非検知の可能性**があるため、
サービスやシステムの特徴、利用形態に応じた、**シグネチャのチューニングが必要**
・ブラックリストによる検査は基本的に既知の攻撃パターンにのみ有効であるため、
ブラックリストの品質維持（シグネチャ更新）が重要

「運用におけるポイント」（出典）WAF読本 改訂第2版（独立行政法人情報処理推進機構）

1

通常運用：WAFを効果的に活用するために以下の運用を行うことが重要
・WAFのアップデートや検出パターンの更新
・定期的なログの確認

2

緊急対応：以下事象の発生を前提として、定期的な訓練が推奨される
・WAF自身の障がい
・過検知の発生

3

保守：商用WAF を導入した場合は、必ず保守契約が必要
・ハードウェア保守
・ソフトウェア保守

WAF運用の課題

・WAF導入後の**シグネチャ更新やチューニング等の運用がセキュリティ確保の最大の課題**
・シグネチャによる検査は、IPSと同様に、**過検知、非検知の可能性**があるため、
サービスやシステムの特徴、利用形態に応じた、**シグネチャのチューニングが必要**
・ブラックリストによる検査は基本的に既知の攻撃パターンにのみ有効であるため、
ブラックリストの品質維持（シグネチャ更新）が重要

「運用におけるポイント」（出典）WAF読本 改訂第2版（独立行政法人情報処理推進機構）

1 **通常運用**：WAFを効果的に活用するために以下の運用を行うことが重要
・WAFのアップデートや検出パターンの更新
・定期的なログの確認

2 **緊急対応**：以下事象の発生を前提として、定期的な訓練が推奨される
・WAF自身の障がい
・過検知の発生

3 **保守**：商用WAF を導入した場合は、必ず保守契約が必要
・ハードウェア保守
・ソフトウェア保守

WideAngleにおまかせ！

WideAngleとは

「WideAngle」 はNTT Comが提供する 総合セキュリティサービスブランドです

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

- プロフェッショナルサービス
- マネージドセキュリティサービス

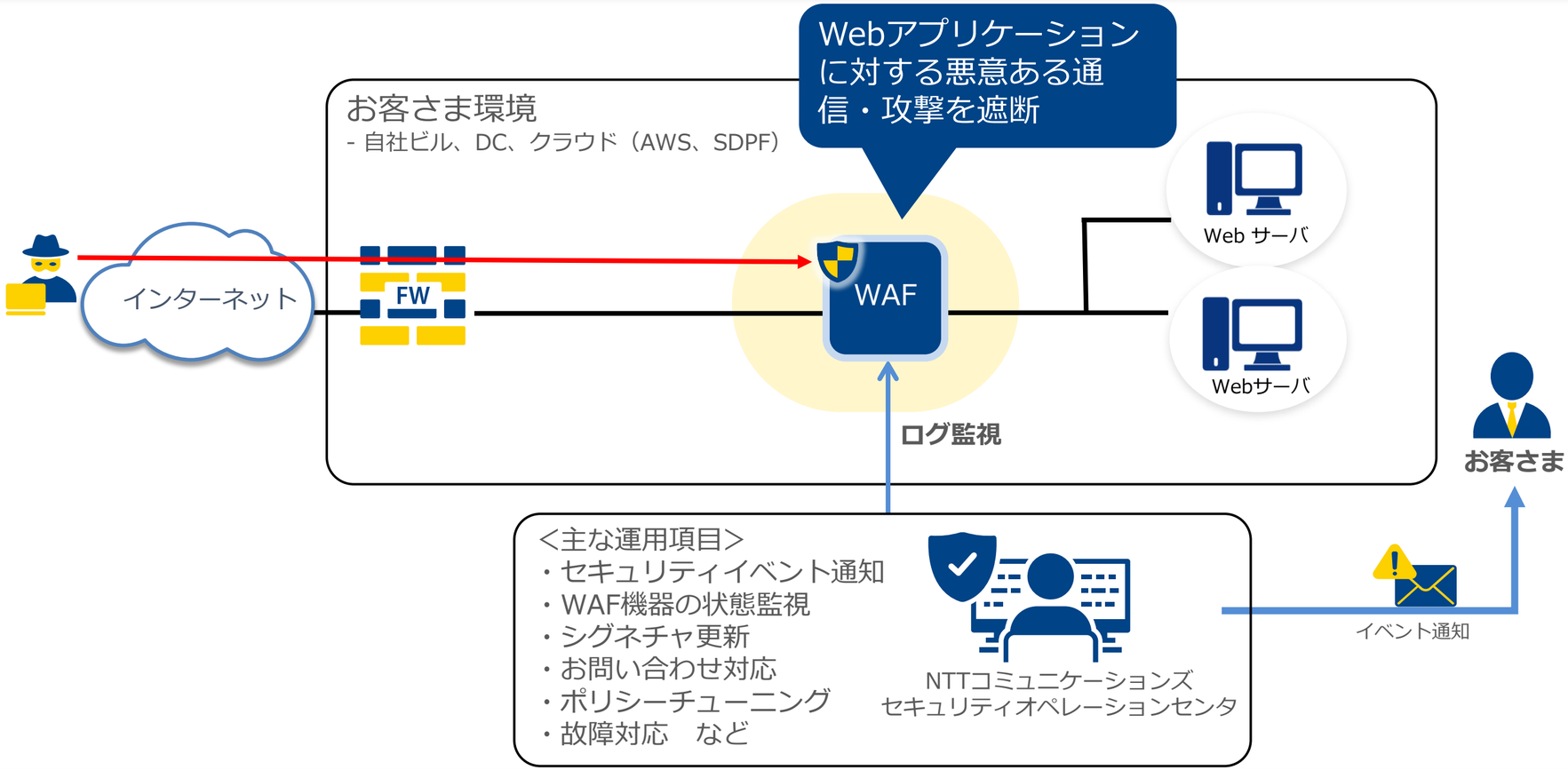
WideAngleという名称には、標的型攻撃など未知の脅威に世界がさらされる中、
広い視野でリスクを見通し、より安心・安全な社会を志す開拓者でありたいという思いを込めています。
NTT Comは、WideAngleブランドのもと総合リスク マネジメント サービスを積極的に展開し、
マネージド セキュリティ サービス プロバイダー（以下MSSP）のトップ プレイヤーを目指します。

WideAngle WAFサービスによるWAF運用

WAFを効果的に運用するために必要となる設定・監視・改善提案など、セキュリティのエキスパートが対応

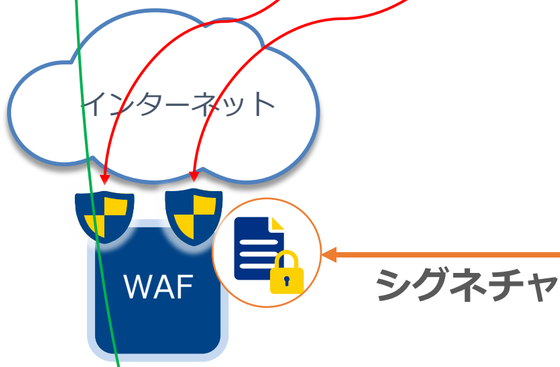
【WideAngle WAFサービスによる運用】

- WAFに熟練したアナリストがお客さまのWebアプリケーションに最適なポリシーチューニングを提案（導入時）
- SOCエンジニアが24時間365日、Webアプリケーションに対する攻撃や機器の正常性を監視
- イベント検知時にメール通知、検知内容に関するお問合せサポート、チューニング方法に対するアドバイス



WideAngle WAFサービスにおける脆弱性対応事例

2021年12月9日、Apache Log4jログ出力ライブラリの複数のバージョンに影響を与える深刻なゼロデイ脆弱性情報が公開されました。翌々日にLog4jの脆弱性に対応したシグネチャーが緊急配信され、脆弱性によるリスク低減に貢献します。



シグネチャー自動更新・適用

※1 Threat Campaigns Signatureサブスクリプションを追加導入した場合に使用可能な機能です。
WideAngleのSOC監視費用と別にサブスクリプションライセンスが別途必要になります。

ウェブサーバー関連のOS脆弱が発覚された場合は
「緊急シグネチャー」※1が配信されます。

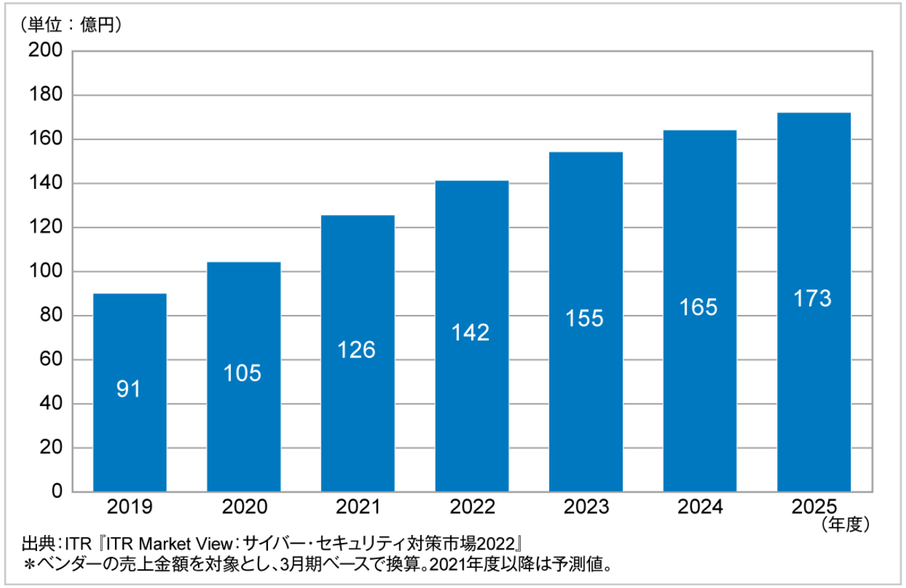
Log4j脆弱性に対応したシグネチャー配信例

日付	種別	説明	動作
2021/12/11	緊急シグネチャーA	Log4j2 'Log4Shell'によるリモードコード実行防御	追加
2021/12/12	緊急シグネチャーB	Log4j2 'Log4Shell'によるリモードコード実行防御	修正
2021/12/12	WAFシグネチャーA	JNDI インジェクション防御 (Content)	追加
2021/12/12	WAFシグネチャーB	JNDIインジェクション防御 (Parameter)	修正
2021/12/14	緊急シグネチャーC	Log4j2 'Log4Shell'によるリモードコード実行防御	修正
・・・・	・・・・		
2021/12/17	緊急シグネチャーD	Log4j2 'Log4Shell' Remote Code Execution	追加

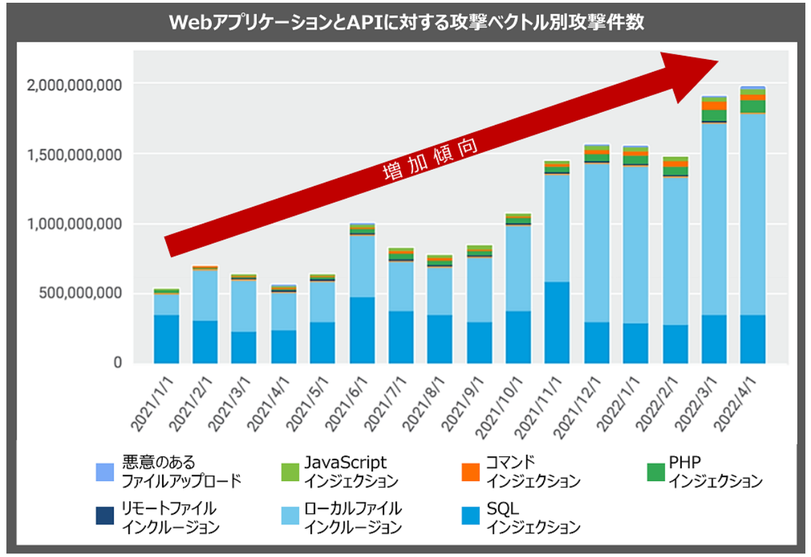
２．Webセキュリティの
トレンドとクラウドWAF
～これからの取り組み～

Webセキュリティのトレンド
～WAF市場は増加傾向＆APIセキュリティの高まり～

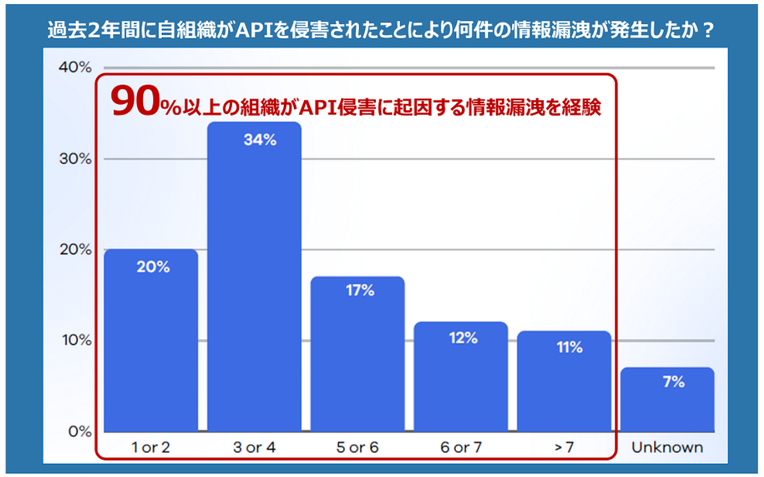
- コロナ以降、オンラインショップ、インターネットバンキングなど、Webサービスへの依存度が高まったことで、Webセキュリティ対策として、**WAF市場は増加傾向（CAGR 10.5%）**
- WAF市場成長と同じく、**WebアプリケーションやAPIに対する攻撃は増加傾向**
- 90%以上の組織がAPI侵害に起因する情報漏えいを経験しているというアンケート調査もあり、APIの普及とともに、Webセキュリティにおける**APIのセキュリティ対策が高まっている**



出典：ITR『ITR Market View：サイバー・セキュリティ対策市場2022』
＊ベンダーの売上金額を対象とし、3月期ベースで換算。2021年度以降は予測値。



Akamai Technologies, Inc.「Akamai Web Application and API Threat Report H1 2022」
https://www.akamai.com/resources/research-paper/akamai-web-application-and-api-threat-report



Traceable Inc.「2023 State of API Security: A Global Study on the Reality of API Risk」https://www.traceable.ai/2023-state-of-api-security

Webセキュリティのトレンド
～次世代Webセキュリティの概念「WAAP」～

WAAP（Web Application and API Protection）

・APIファースト時代における「クラウド型WAFサービス」の進化形として、 Gartner社が提唱
・F5社では、Gartner社の提唱を踏まえ、従来のWAF機能に３要素を加えた、
以下の４機能をWAAPサービスとして提供

（参考）F5社のWAAPの紹介

Gartnerにより提唱されたAPIファースト時代の次世代Webセキュリティ概念。
APIはWeb・モバイルアプリケーションで急速に発達し、データ侵害の最大の攻撃ベクトル。
WAAPをWAF市場の進化として定義し、以下の機能を必須とする。

DDoS対策	ネットワーク及びアプリケーションレベルのリソース保護。
次世代WAF	アタックシグネチャ自動更新、クライアントの振舞い学習。
Bot防御	Bot及びツールの検証。振舞いを把握し悪意のあるBotを検知。
API保護	APIディスカバリと機械学習によるリクエスト毎の異常確認。

※Gartnerは４項目の細かい機能を明示していません。上記一部はF5の実装です。

F5 XC WAAP
（F5 Distributed Cloud Web Application and API Protection）

DDoS対策

DDoS対策 | 次世代WAF | Bot防御 | API保護

L3-L7 DDoS 軽減
重要なアプリケーションとネットワークリソースの確保。

ボリューム攻撃を検知・緩和。
VIPに対するL3/4レートリミット。特定のIPアドレスやASN等をブロック。
Javascript/Captchaチャレンジによるブラウザー利用、ツール/Bot判別。
MLでユーザの挙動を学習しBlock/Javascript/Captchaチャレンジを適用。
IPアドレスやASN等の送信元、Domainやパス等の宛先毎にレートリミット。

26 ©2022 F5

次世代WAF

DDoS対策 | 次世代WAF | Bot防御 | API保護

シグネチャベースの識別
複数シグネチャを用いて悪意あるリクエストを検知

既知のアタックシグネチャだけでなく常に更新されるライブシグネチャに対応。
特定の製品を狙った高度なシグネチャに対応。MLによる誤検知の削減。

- F5 WAFで実装されているシグネチャを適応
- F5 Labが収集した実攻撃情報をもとに作成した高精度シグネチャ（Threat campaings）を無償バンドル
- 機械学習による誤検知抑制機能を実装
- シグネチャ検出以外の各種回避テクニックの検出にも対応
- Botシグネチャを標準実装。BotをGood/Suspicious/Maliciousに自動的に分類

脅威と誤検知の把握
クライアントを識別し振舞いを学習

異常なユーザー行動を分析・特定し、悪意のある攻撃をブロック。
潜在的に有害な人間以外の自動化されたリクエストを認識。
時系列で過去の行動履歴を確認可能（レトロスペクティブ分析）

28 ©2022 F5

Bot防御(Bot Defense)

DDoS対策 | 次世代WAF | Bot防御 | API保護

クライアントのメタデータをBot Defenseサービスへ送信

Bot検知と脅威の軽減
自動化された人間以外の攻撃を特定

既知の検索エンジンの振る舞いを把握。
Botシグネチャ、ブラウザ検証テスト、脆弱性スキャナー等のツールを検知。
JavaScriptやSDKで振舞いデータを収集、悪意あるBotか判断。

- 従来のBot検出技術を回避する高度なBot （Captchaバイパスや、ブラウザ偽装ツール等を利用したBot）を、独自に開発した人工知能と機械学習モデルを用いて高精度に判定
- ログイン、サインアップ画面などの重要なフローを保護し、以下に対応
  - OAT-019 Account Creation
  - OAT-001 Carding
  - OAT-008 Credential Stuffin

32 ©2022 F5

API 保護

DDoS対策 | 次世代WAF | Bot防御 | API保護

APIのDiscovery & Security
新規APIの発見と異常アクセス対策

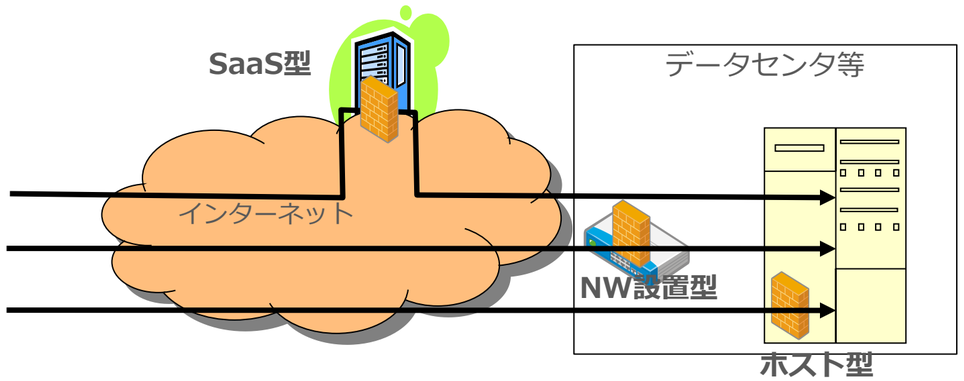
エンドポイントパスの自動把握とリクエストレートの可視化。
リクエストやエラーレートを学習し疑わしい挙動を検知。
APIスキーマとSwaggerファイルを生成、APIの手動追跡を最小限に抑制。
不審なリクエストをブロックし、データ漏洩を防止。
APIセキュリティポリシーの設定・導入にかかる時間を短縮。

38 ©2022 F5

WAFの分類

・WAFの利用形態は、大きく分けて3種類が存在
・WideAngleではNW設置型に対応してきたが、WAAPの高まりにより、クラウド型（クラウドWAF）にも対応予定

	分類		構成	WideAngleサポートデバイス
従来提供	**NW設置型**	**単体機能型**	WAF専用のアプライアンスとして設置。利用形態として透過型とプロキシ型がある。	Imperva WAF Gatewayシリーズ（Imperva）
		統合型、モジュール型	UTMやロードバランサなどの一機能（またはモジュール）として設置。利用形態として透過型とプロキシ型がある。	F5 BIG-IPシリーズ（F5）
		仮想アプライアンス型	仮想サーバのゲストOSの下で動作するソフトウェアとして設置。	Imperva WAF Gateway 仮想アプライアンス（Imperva） F5 BIG-IP 仮想アプライアンス（F5）
	ホスト型		Webサーバで動作するソフトウェアとして設置。	—
クラウドWAF提供（新規追加）	**クラウド型（SaaS型）**		インターネット上のクラウドサービスとして提供。	F5 XC WAAP（F5）（予定）



クラウドWAFの運用上の課題

- NW設置型WAFと比べ、WAAP（クラウドWAF）は**製品自体のアップデートや保守は不要**
- 最新の攻撃パターンへの対応のための**シグネチャ更新も不要（自動適用）**
- 一方、 NW設置型WAF同様、検知状況（過検知、非検知）を踏まえた**シグネチャのチューニングは必要**
- 加えて、**F5 XC WAAPの問い合わせは英語のみ**

「運用におけるポイント」（出典）WAF読本 改訂第2版（独立行政法人情報処理推進機構）

1

通常運用：WAFを効果的に活用するために以下の運用を行うことが重要
- WAFのアップデートや検出パターンの更新、**シグネチャのチューニング**
- 定期的なログの確認

2

緊急対応：以下事象の発生を前提として、定期的な訓練が推奨される
- WAF自身の障がい
- **過検知の発生**

3

保守：商用WAF を導入した場合は、必ず保守契約が必要
- ハードウェア保守
- ソフトウェア保守

問い合わせ（F5 XC WAAPは英語）

クラウドWAFの運用上の課題

・NW設置型WAFと比べ、WAAP（クラウドWAF）は**製品自体のアップデートや保守は不要**
・最新の攻撃パターンへの対応のための**シグネチャ更新も不要（自動適用）**
・一方、 NW設置型WAF同様、検知状況（過検知、非検知）を踏まえた**シグネチャのチューニングは必要**
・加えて、**F5 XC WAAPの問い合わせは英語のみ**

「運用におけるポイント」（出典）WAF読本 改訂第2版（独立行政法人情報処理推進機構）

1
通常運用：WAFを効果的に活用するために以下の運用を行うことが重要
・WAFのアップデートや検出パターンの更新、**シグネチャのチューニング**
・定期的なログの確認

2
緊急対応：以下事象の発生を前提として、定期的な訓練が推奨される
・WAF自身の障がい
・**過検知の発生**

3
保守：商用WAF を導入した場合は、必ず保守契約が必要
・ハードウェア保守
・ソフトウェア保守

＋ 問い合わせ（F5 XC WAAPは英語）

➡ WideAngleで提供予定！

WideAngle クラウドWAF（F5 XC WAAP）の特長

多くのWAFの運用経験と実績に基づいたノウハウを活かし、最適なWAAPのチューニングをサポート

WideAngle独自の初期ポリシー（シグネチャ、バイオレーション等の検知ルール）

- お客さま環境へのWAAP導入に当たり、多くの運用経験および蓄積されたノウハウに基づいて作成されたWideAngle独自の初期ポリシー（検知精度の低い検知ルールを除外したポリシーのテンプレート）を適用

イニシャルチューニング（オプションで設定依頼が可能）

- 導入効果を最大化するため、WideAngle WAAPではブロッキングモードによる運用を基本としています。正常通信を誤って遮断してしまう誤検知を減らすため、ブロッキング移行前に行うイニシャルチューニングの精度がポイントになります。

運用中のチューニングもエキスパートがサポート（オプションで設定依頼が可能）

- シグネチャの追加、Webアプリケーションの変更などにより、WAAPの導入後も誤検知が発生しチューニングが必要になることがあります。WideAngle WAAPでは、攻撃と誤検知によるリスクを最小化するため、アナリストが最適なチューニングをアドバイス、代行設定いたします。

お客さまサポート

- 検知ログに関するお問合せやチューニングのご相談など、セキュリティのエキスパートによるサポートを提供いたします。
- F5 XC WAAPの製品サポートは英語となりますが、WideAngle WAAPではお客さまより、日本語でのお問い合わせを受け付け、必要に応じて、F5社へ英語で確認を行い、日本語でのサポートを提供いたします。

※現時点（開発中）での予定となるため、実際の提供内容は一部変更となる可能性がございます

3．クラウドWAF運用の
ベストプラクティスとは？

NW設置型WAFとクラウドWAFの違い

NW設置型WAF

きめ細かいWebセキュリティ対策！

- 細かい設定、チューニングの**カスタマイズ性**に強み
- 詳細のログ取得が可能で、**ログから高度な分析**が可能
- クラウドWAFに比べ、運用負荷は高い（導入設計、ソフトウェアやハードの更新等）

クラウドWAF

手軽にWebセキュリティ対策！

- **導入しやすい**（DNSの名前解決先を変更することで利用可能）
- **APIセキュリティ**、**Bot防御**、**DDoS対策**に強み
- ソフトウェアアップデートが不要
- わかりやすいGUI
- NW設置型に比べ、ログは限られる可能性あり（ログからの高度な分析には不向き）

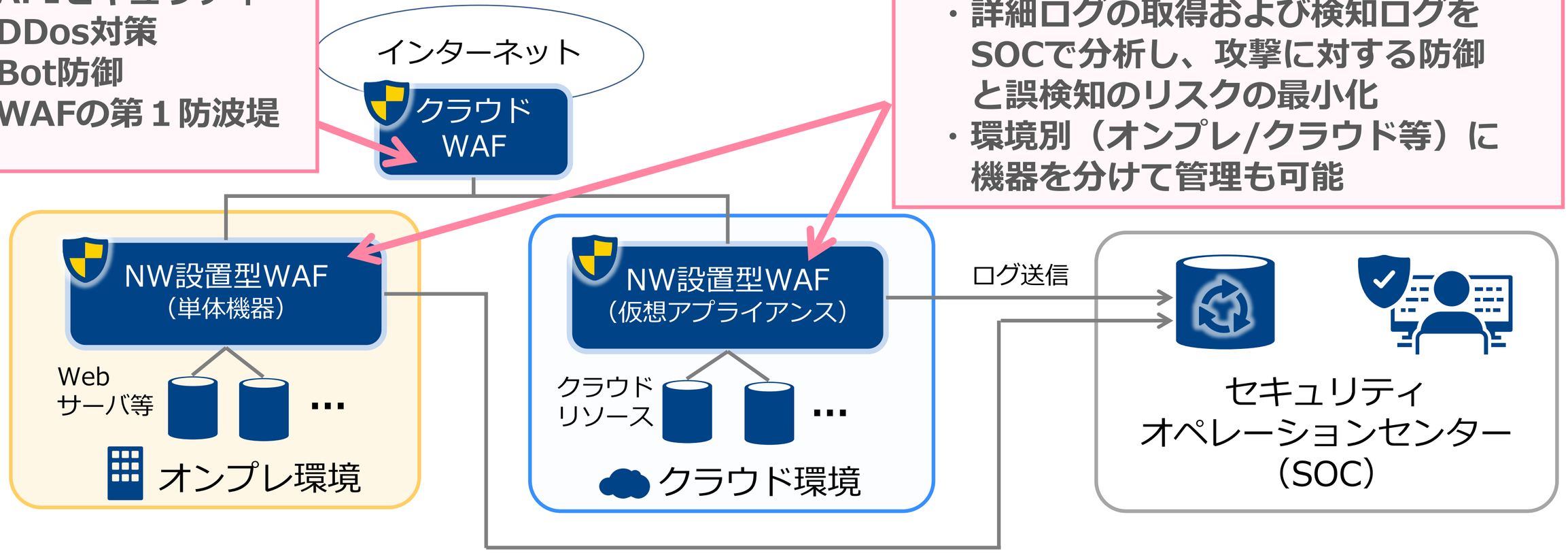
➡ **お互いの特長を踏まえた使い分けが必要**

NW設置型WAFとクラウドWAFのハイブリット構成

高度なWebセキュリティ対策を求めるお客さまは、NW設置型WAFとクラウドWAFの互いの特長を活かしたハイブリット構成もベストプラクティス

クラウドWAF
- APIセキュリティ
- DDos対策
- Bot防御
- WAFの第１防波堤

NW設置型WAF
- WAFの第２防波堤
- きめ細かいルールによる高度な制御
- 詳細ログの取得および検知ログをSOCで分析し、攻撃に対する防御と誤検知のリスクの最小化
- 環境別（オンプレ/クラウド等）に機器を分けて管理も可能



まとめ

- WebセキュリティにWAFは必須（FWやIPSでは防御しきれない）
- **WebアプリケーションやAPIに対する攻撃は増加傾向**であり、「クラウド型WAFサービス」の進化形として、 WAAPが生まれ、コロナ以降のWebサービスへの依存度が高まったことから**クラウドWAF（WAAP）のニーズは高まっている**
- WAFもクラウドWAFも利用にあたり、**有スキル者による一定の運用が必要**
  （初期ポリシー設定、シグネチャのチューニング、シグネチャの最新化…）
- 有スキル者の運用サービスとして、WideAngleではWAFのマネージドサービスを提供中
  さらに、クラウドWAFとして、**「F5 XC WAAP」のマネージドサービスを提供予定**
- **WAFとクラウドWAFの特長を踏まえた使い分け**が必要。高度なセキュリティ対策を実現したいお客さまは**WAFとクラウドWAFのハイブリット構成**がベストプラクティス

ご清聴ありがとうございました


App
World
2024

以下、参考資料

（参考）プロフェッショナルサービス

「WideAngle プロフェッショナルサービス」は、
お客さま企業のセキュリティ管理体制の整備や運用に対して、セキュリティ専門家の知見を提供するサービスです。

国内外で8,000件以上の実績を誇る**「総合コンサルティング」**、
セキュリティインシデント発生時のレスキュー対応を行う**インシデントレスポンス**や
ICT環境の弱点を可視化する**脆弱性診断**など、
お客さまの「CSIRT運用を支援するソリューション」から構成されている専門性の高いセキュリティサービスです。

セキュリティ プロフェッショナル

セキュリティ・コンサルタント
セキュリティ・リサーチャー
フォレンジック・エンジニア
脆弱性診断・エンジニア

総合コンサルティング

・事業戦略レベルのセキュリティ対策の立ち上げ
・CSIRTやSOCなど専門管理体制の構築支援
・現状のセキュリティ体制への評価

CSIRT 運用支援ソリューション

・CSIRTの幅広い管理、
運用業務に対する専門性と高度化を備えた
サポートサービスの提供

（参考）マネージドセキュリティサービス・SOCサービス

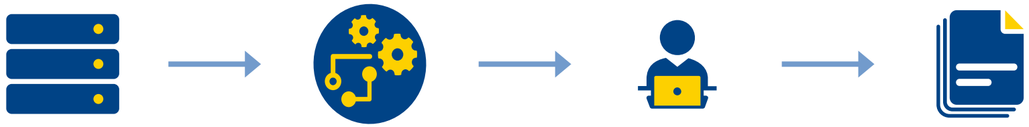
マネージド セキュリティ サービス（MSS）とは、
アナリストが**セキュリティ監視センター（SOC）**から、
セキュリティ機器の設定や運用、**高度なセキュリティ監視**を**24時間365日**行うサービスです。

サイバー攻撃などのリスクを最小化するとともに、お客さまの日々の運用負担を軽減いたします。

（参考） SOCサービスの３分類

WideAngleの高度分析サービスは分析型に該当

	即時性	正確性	対応コスト※
直接型：セキュリティ機器のアラートを直接受け取る	高	低	高
処理型：SIEM等で機械処理された情報を受け取る	中	中	中
分析型：アナリストが分析した結果を受け取る	低	高	低



※インシデントレポート受領後のインシデント対応稼働コスト

日本セキュリティオペレーション事業者協議会（ISOG-J）　『マネージドセキュリティサービス(MSS)選定ガイドライン Ver.2.0』より

（参考）リアルタイム分析の全体像と仕組み

日々SOCで観測される検知ログやマルウェア検体など
リサーチで入手した様々なインテリジェンスを活用し
分析システムにフィードバックすることでシステムを高度化

セキュリティアナリストが
独自ポータルでお客さまと
直接コミュニケーション

カスタムシグネチャー / チューニング
アナリストが脅威情報を
独自シグネチャーとして作成し
セキュリティ機器へ適用

独自ロジック / ブラックリスト
SOCが独自に所有する
検知ロジック・脅威情報を
SIEMエンジンへ随時投入

アナリストによる外部脅威情報の収集

✓ **SOC独自インテリジェンスをフル活用**

- 脆弱性情報／攻撃手法
- マルウェア解析情報
- グローバルでの検知状況
- 実際のアラート解析結果
- Sandbox／ハニーポットで捕捉したマルウェアの解析情報

独自ポータルにてご提供

- SOCアナリストへの問い合わせ
- 通知チケット
- レポートの閲覧

（参考） SOCの歴史

2020 4月

2016 11月　東京セキュリティオペレーションセンタを拡充し、現在の拠点に移設

2016 8月　NTTセキュリティ社をNTT持株配下に設立し、グループのリソースを統合

2013　NTTコムセキュリティ設立　協力　NTTセキュア　プラットフォーム　研究所

2012　運用基盤統合

2011　INTEGRALIS、SECODE会社統合

2010　SECODE　買収

2009　INTEGRALIS　買収

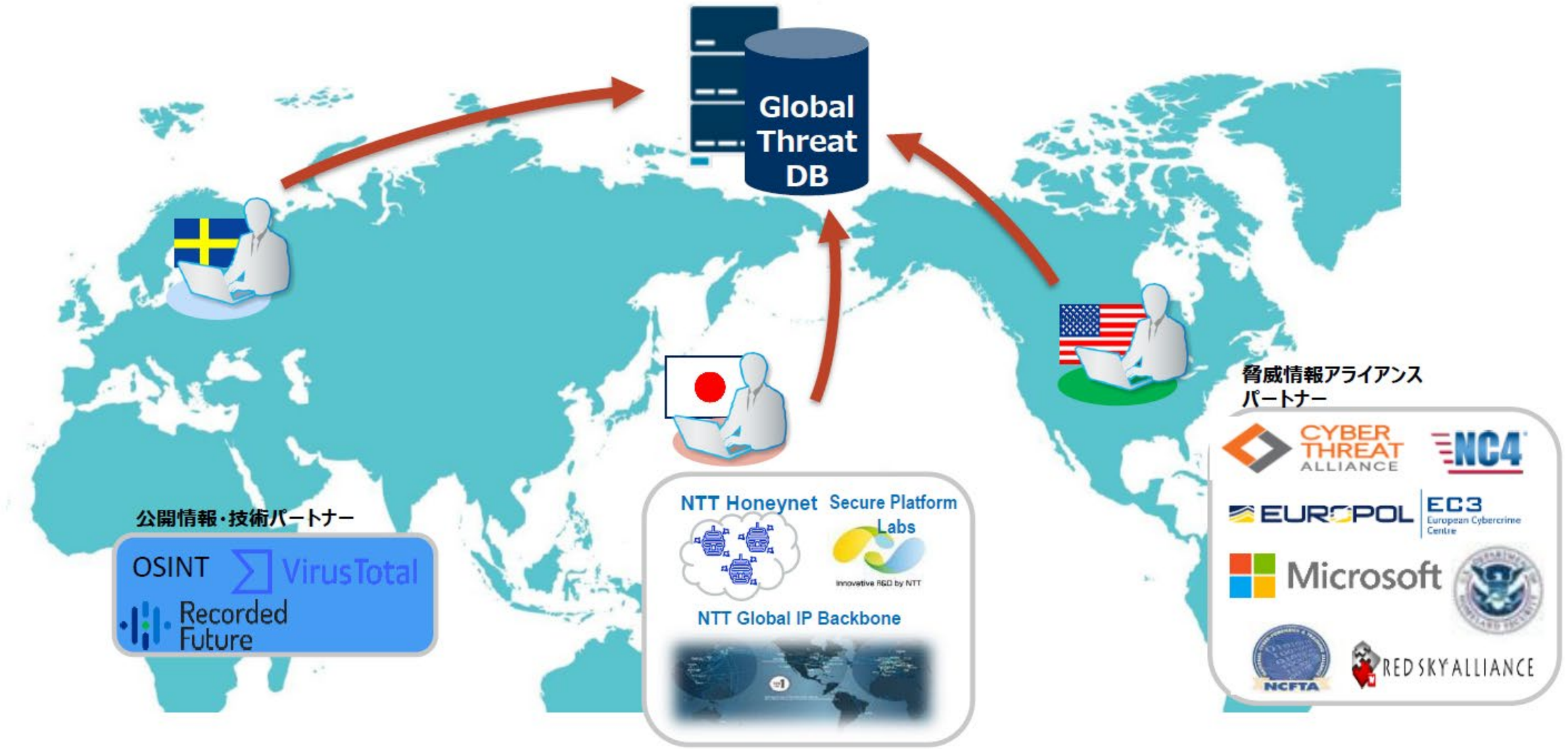
2003　NTTコミュニケーションズ セキュリティオペレーションセンター　設立

設立：1988年
（事業内容）フルレイヤーセキュリティ サービスの構築・運用
（実績）　欧米を中心に、業種を問わない豊富な実績

設立：1986年
（事業内容）セキュリティコンサル及び、MSSの提供
（実績）　官公庁及び金融業を中心に豊富な実績

34

（参考）サイバー攻撃監視・検知におけるグローバル体制



（参考）WideAngleが選ばれる理由

NTT Com は、セキュリティ対策の導入/運用実績が豊富で、専門家集団を有しており、国家的なプロジェクトの担い手です。

SOCによるサイバー攻撃監視

- 2003年に東京SOC（セキュリティオペレーションセンター）を開業
- 国内外でサイバー脅威を収集
- 250のセキュリティ監視案件

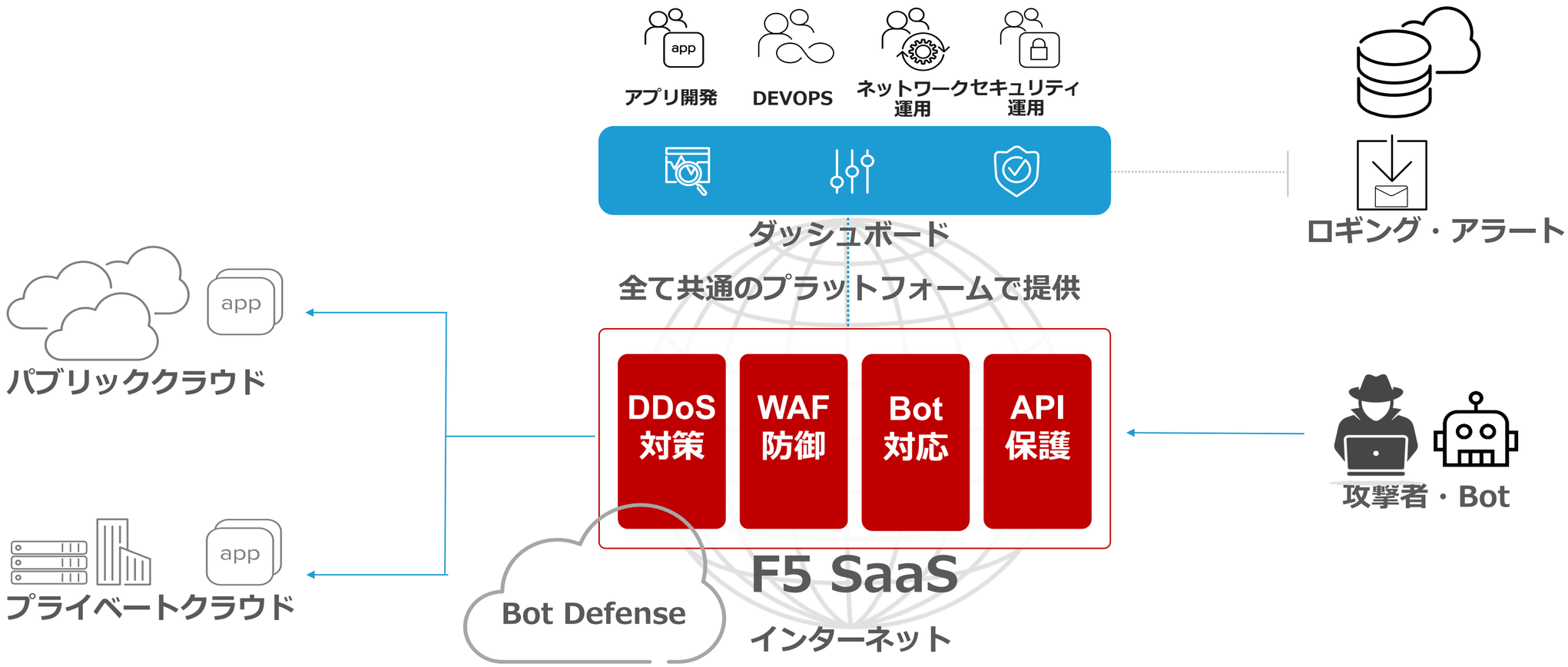
セキュリティの専門家集団

- セキュリティ大会（CTF）でフォレンジック部門世界3位
- セキュリティ事故担当者全員が難関資格GCFAホルダー

国家的プロジェクトを担う実力

- 2021年東京の国際的スポーツイベントにおいてサイバー被害ゼロ
- 大阪万博にてICT-PF サービス提供業務を受託

（参考）次世代セキュリティスタックをSaaSで提供



- 実績豊富なBIG-IP AWAFエンジンを搭載。特定製品を狙った高度シグネチャに対応。MLによる誤検知の削減
- Bot Defenseでブラウザとモバイルアプリからのアカウント乗取りを防止
- 様々な業界で実績豊富な最新セキュリティをサブスクリプションで提供