

**umv**

# WARSS

Website **A**ttack **R**estoration  
**S**ecurity **S**olution

リアルタイムウェブサイトのセキュリティ



# コンテンツ

01

会社紹介

02

Webハッキング動向

03

改ざん

04

WARSS

05

構築事例

06

QnA

# umv



# UMV Inc.

**2008年設立**

本社：ソウルヤンジェドン

## Webセキュリティソリューション

リアルタイムWebサーバーセキュリティ

**防ぐ**

盗まれたデータ、中断されたWebサービス、ウェブサイト  
の破損、APT攻撃

**モットー**

「セキュリティチェーンの強さは、最も弱い部  
分の強さによって決まります。」

# なぜWARSなのか？

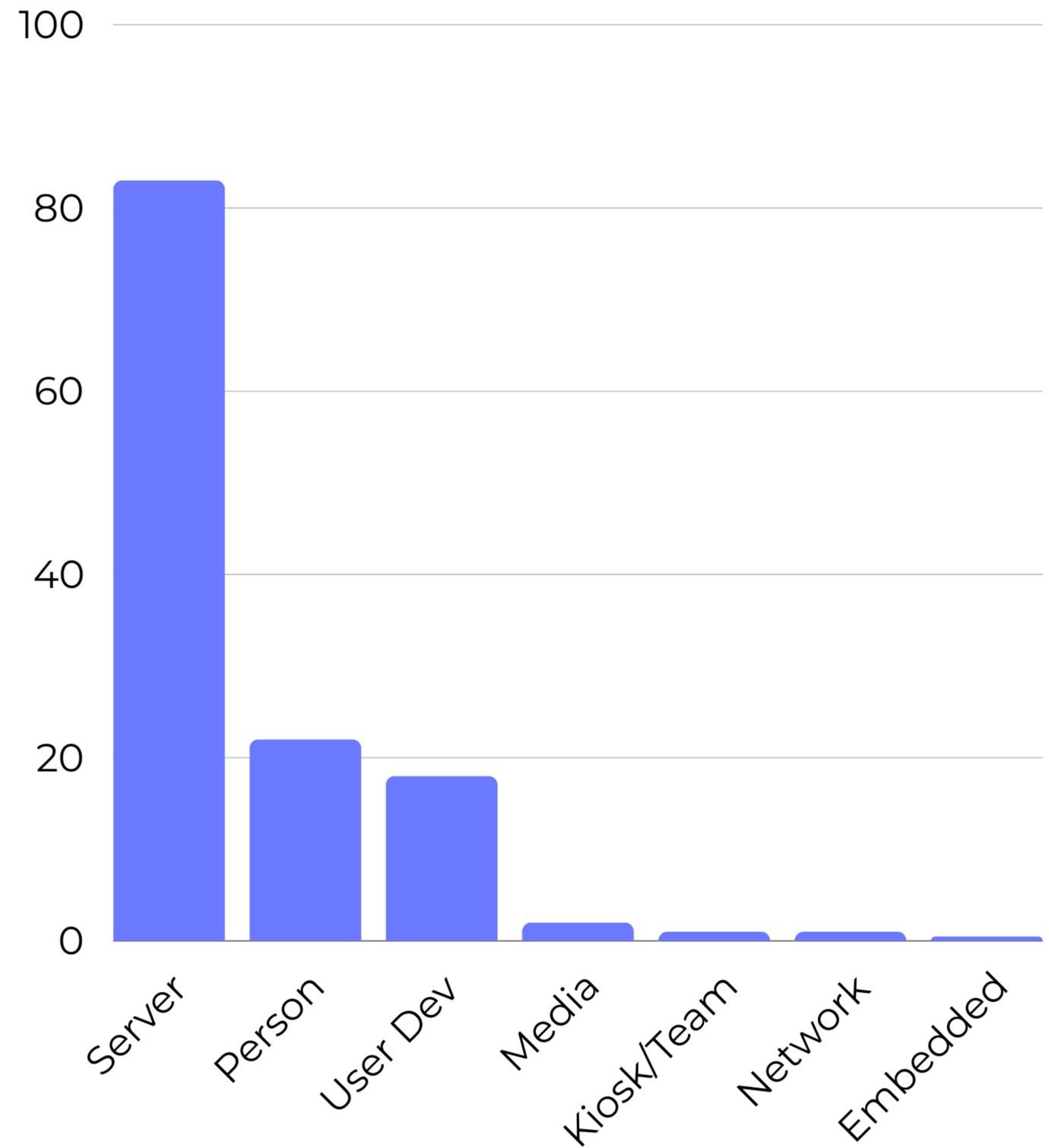


# 増加するウェブハッキング

Verizonは、2022年から2023年の間に検証されたセキュリティ侵害の件数が過去最高の2倍に増加したと分析しました。

# 影響を受ける資産の侵害を産

2023 Verizon DBIR



# ウクライナとロシアの Web サイトが改ざんされる

## フェイクニュース

2024年2月現在：ロシアとウクライナの戦争は、互いと同盟国に対する継続的なサイバー攻撃を伴う

## 誤報とデータ収集

ターゲットには、中小企業、メディア、政府機関、OT、および個人情報や機密情報を保有するその他の組織が含まれます

## 不信：サイバー戦争の鍵

ハッキング攻撃を公表すると、民間人の間で恐怖、当局への不信、誤情報が生まれます

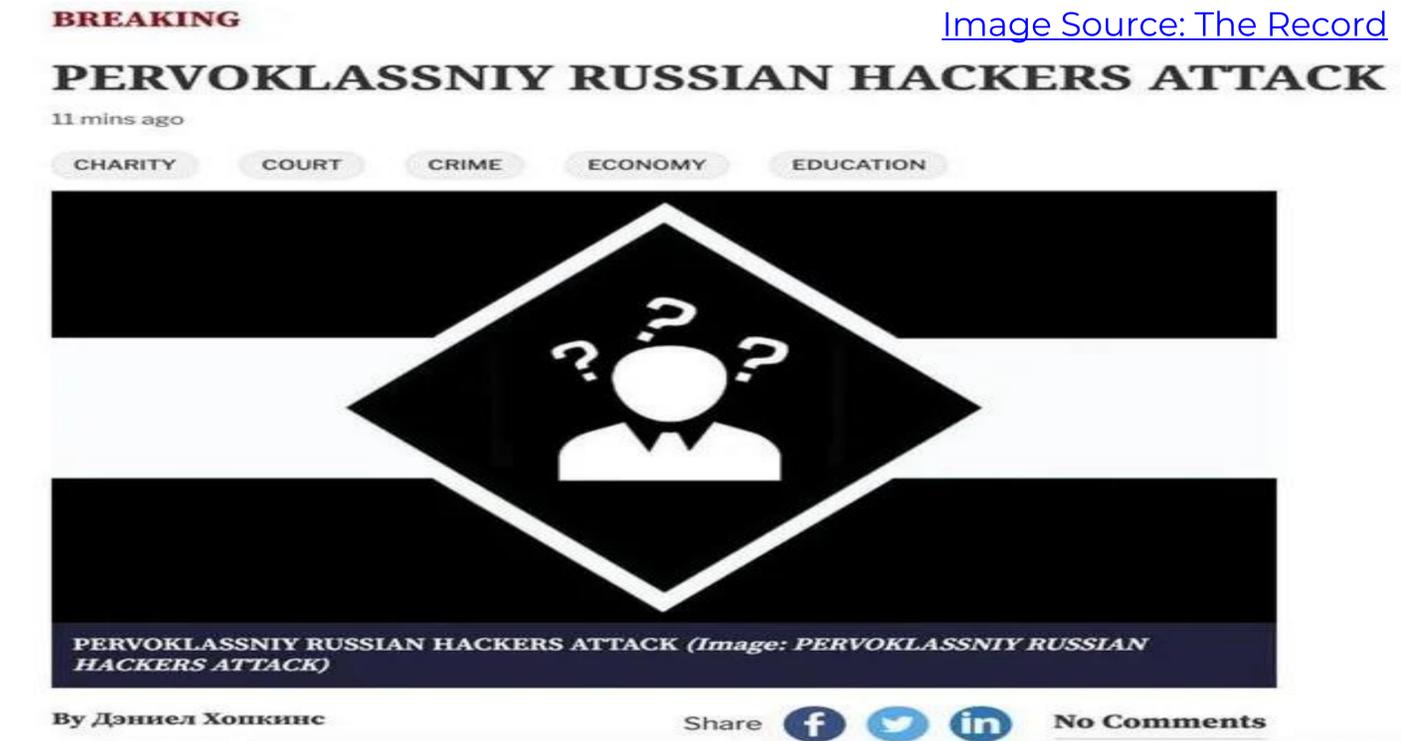


Image Source: The Record

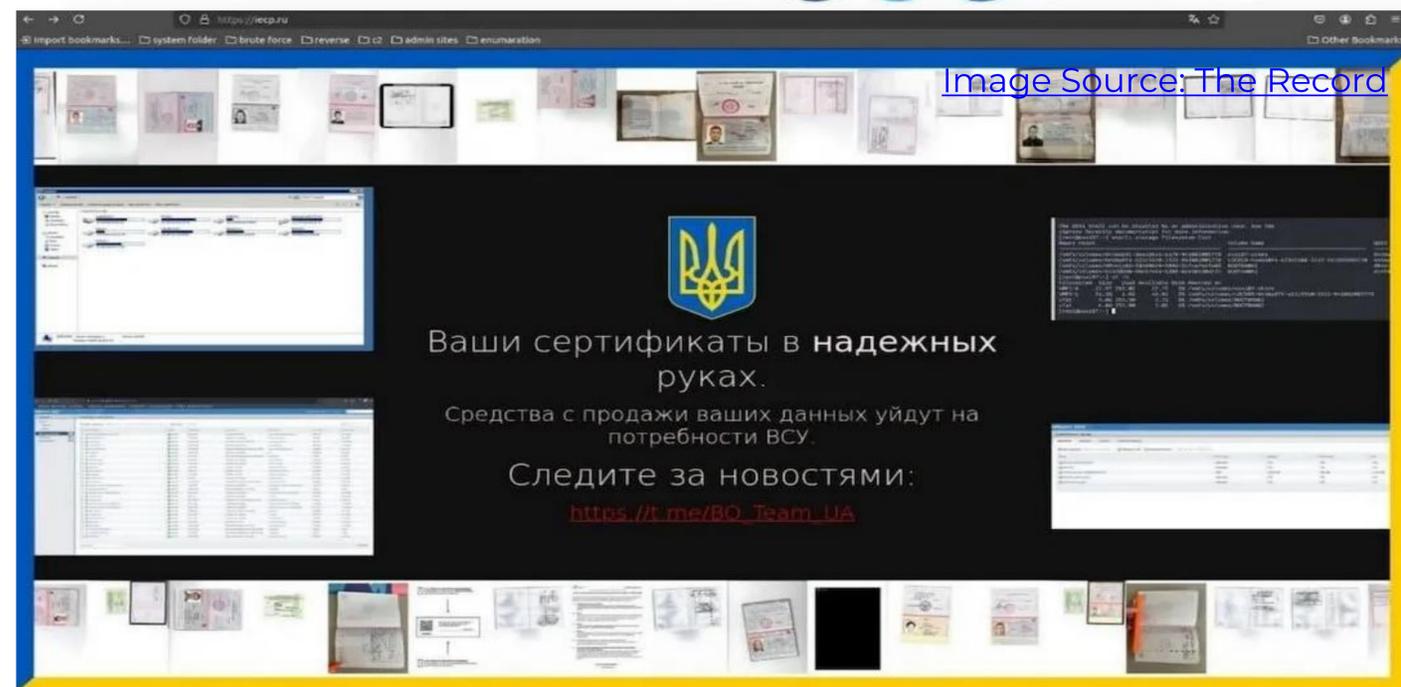


Image Source: The Record



# インターネットアーカイブ攻撃

## 第1ラウンド: DDoS、改ざん、データ盗難

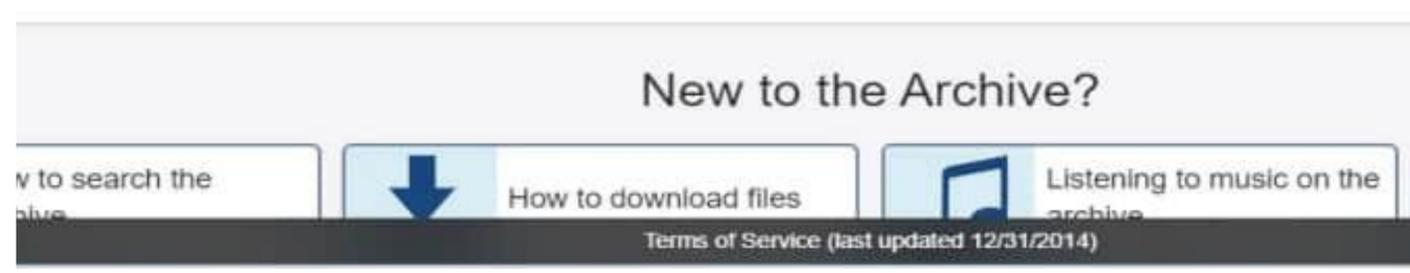
**2024年10月9日**: DDoS 攻撃によりサイトがダウン、Web サイトが JavaScript アラートで改ざんされる。3100万件のユーザーアカウントのユーザー名、メールアドレスなどが漏洩

## 通常に戻る

**2024年10月18日**: IA はデータが安全であり、サービスが復旧したことを確認

## 第2ラウンド: 保護されていないデジタルキー

**2024年10月20日**: ローテーションされていないアクセス トークンを悪用して、インターネットアーカイブの Zendesk サポート プラットフォームにアクセスします。2018年まで遡って80万件以上のサポートチケットにアクセスしました



- <https://www.cbc.ca/radio/asithappens/internet-archive-hack-1.7359959>
- <https://therecord.media/internet-archive-data-breach-ddos-defacement>
- <https://hackread.com/internet-archive-archive-org-hacked-accounts-compromised/>

# トレンド: ハクティビズム (Hacktivism) とサイバーテロリズム (Cyber Terrorism)

- 政治的または宗教的信念を促進するためのハッキング
- 暗号化された通信プラットフォーム (**Telegram**、**Rocket Chat**、**Discord** など) と暗号通貨の利用可能性の向上
  - 2021年以降、TRONはテロ資金調達に関連する資金の約90%を占めています (INTERPOL New Technologies Forum、2023年10月、Merkle Science)
- サービスとしてのサイバー犯罪 (**DDoS**、ランサムウェア、認証情報、データなど)

- 表面下のレポート (2024年6月)  
国連テロ対策センター (UNCCT)

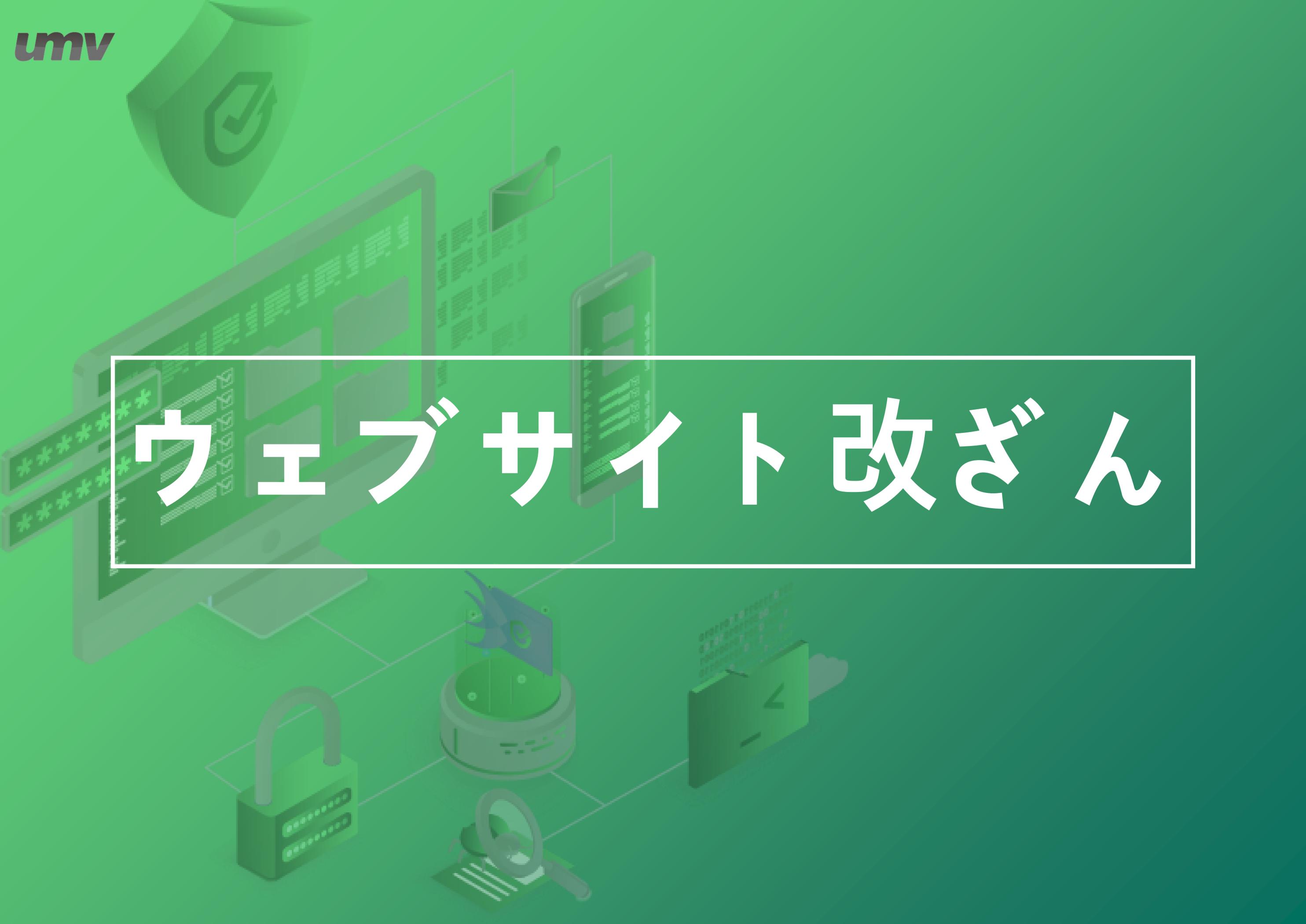


[Image Source: Malcontent News](#)



[Image Source: POLITICO](#)

# ウェブサイト改ざん



# ウェブサイト改ざん方法

## 1. ソースコードの修正

Bitcoin, eh? Never heard of it. But perchance you would like to try something better. Something with more "zing". Something named CosbyCoin!

Continue =>

|  |             |    |      |   |
|--|-------------|----|------|---|
| crash.. Holding my Cosbycoin..           | bitjet      | 2  | 333  | Today at 07:33:43 pm<br>by kjj                |
|  | WiseOldOwl  | 9  | 402  | Today at 07:32:21 pm<br>by ShadowOfHarbringer |
| iform to Mt Gox. Anybody interested? < 1 | 4xCoder     | 24 | 1564 | Today at 07:32:20 pm<br>by AlexZ              |
|  | mizerydeana | 17 | 562  | Today at 07:19:34 pm<br>by ssaCEO             |
| pydun<br>butcoins.org                    |             | 17 | 1501 | Today at 06:58:32 pm<br>by enmaku             |

Image Source: [alphavilleherald.com](http://alphavilleherald.com)



**FUCK! KOREA**

Deploy the Sade missile system is ignorant  
Lotte group is too naive!  
Cherish peace, stay away from war!  
Boycott lotte, resisit Sade!  
lotte,get out of China! Korea sticks fuckyou!

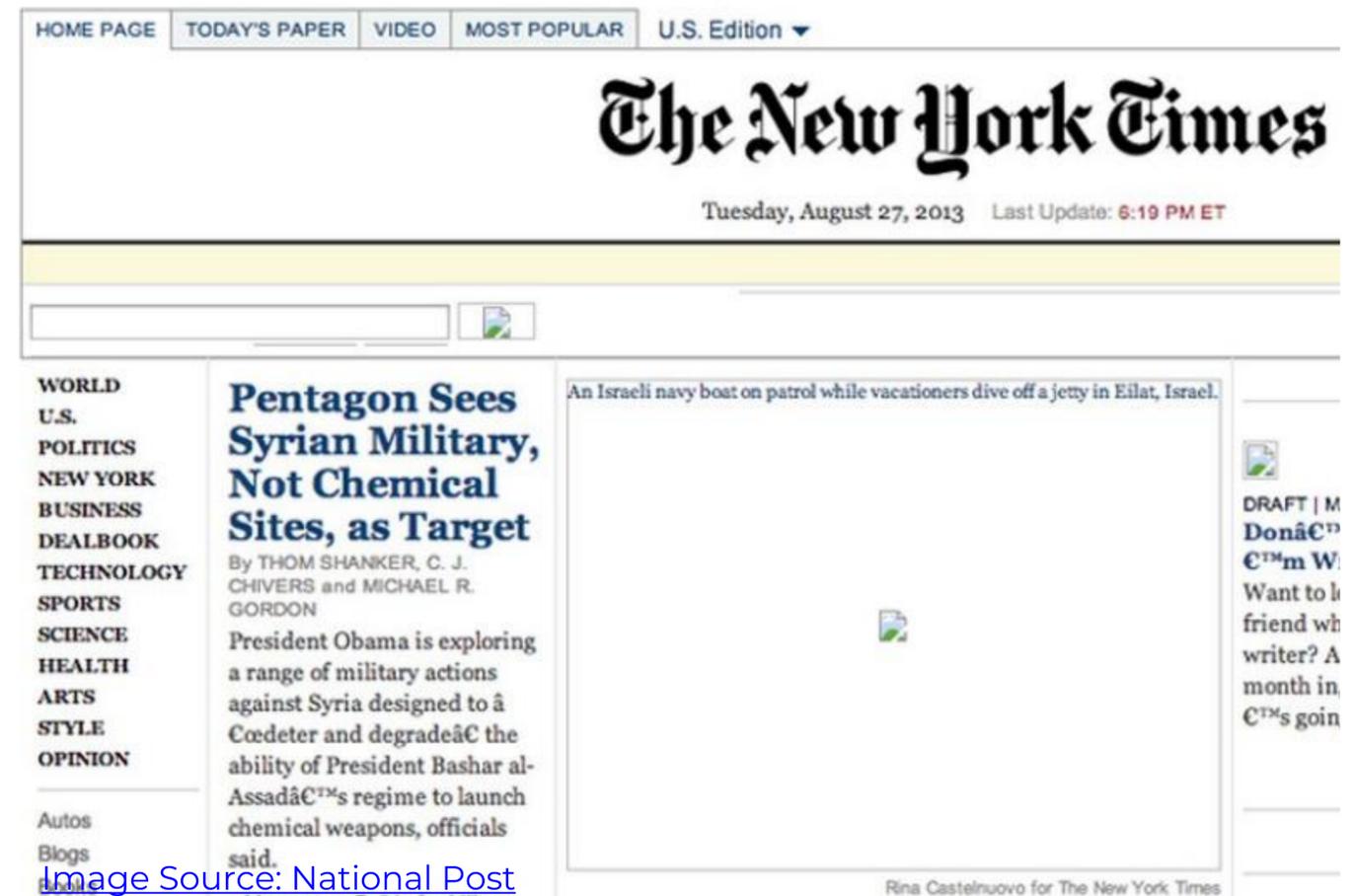
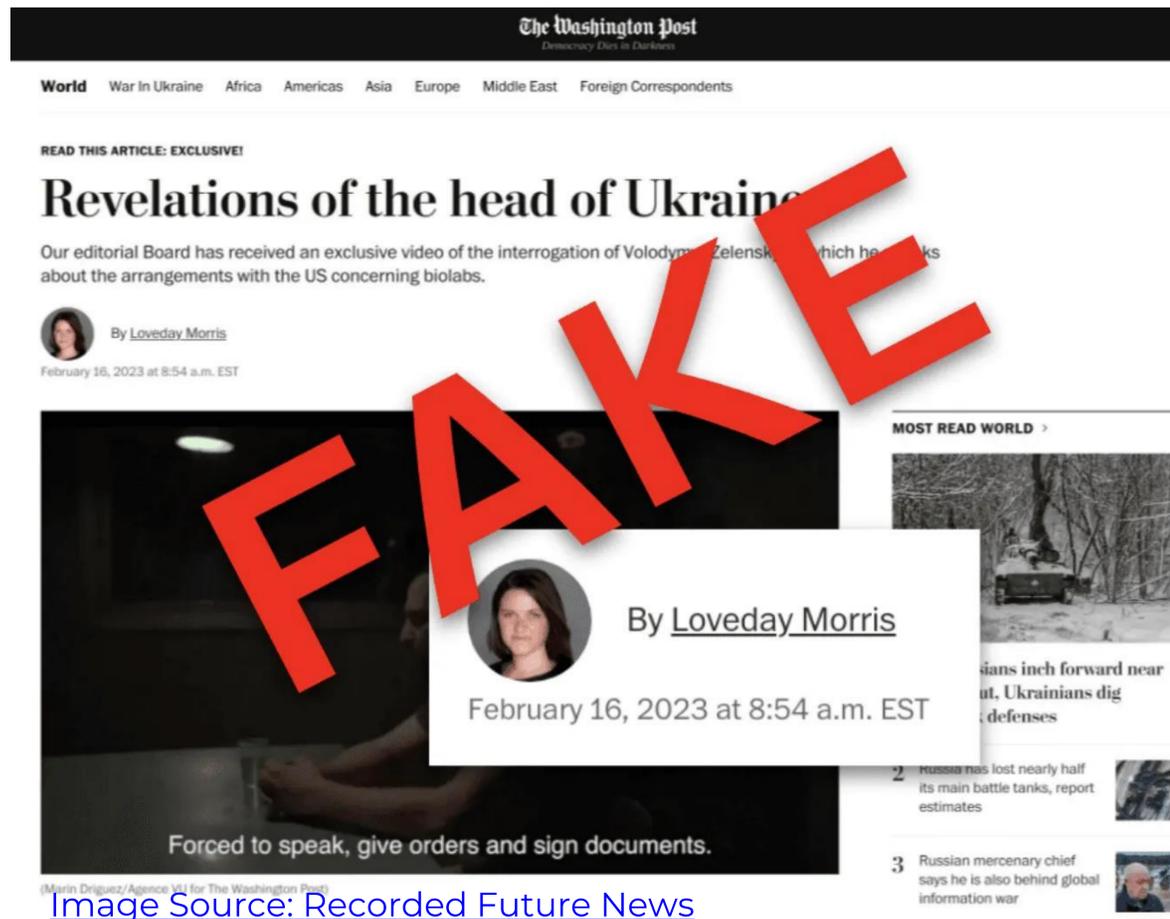
犯我中华者虽远必诛!

Py. China, Heck **보안뉴스** Intelligence Bureau

Image Source: [boannews.com](http://boannews.com)

# ウェブサイト改ざん方法

## 2. コンテンツなりすまし/インジェクション



# なぜディフェイス (Defacement) 攻撃が行われるのか？



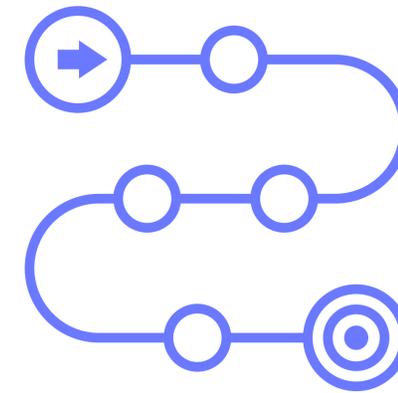
## 動機

- ハクティビズム
- 屈辱
- 名声/認定
- サイバーテロリズム



## 目標

- 政府機関
- 医療機関
- 大企業
- 利便性のために選択されたターゲット

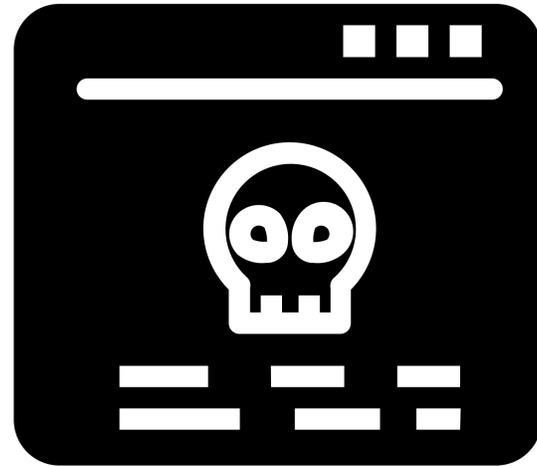
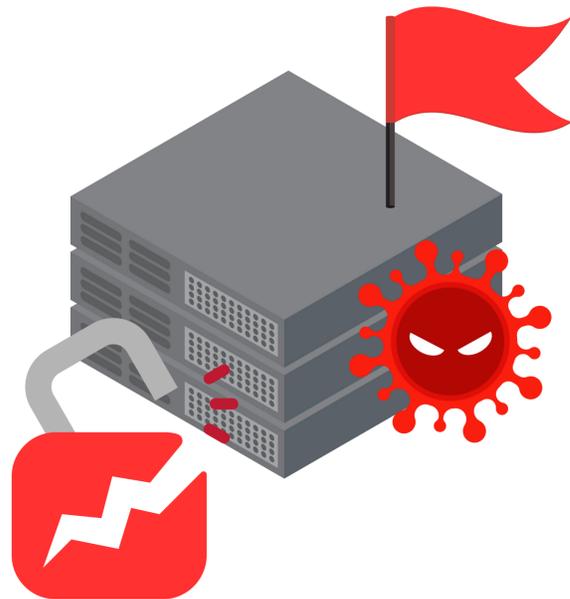


## 方法

Webベースのコンポーネントの脆弱性を悪用する：

- Webサーバー
- Webアプリケーション
- ウェブサイト

# Web攻撃の段階



## ダメージ

3

- 変調(Defacement)
- ソースコード及びコンテンツ偽造・変調

## 高度化

2

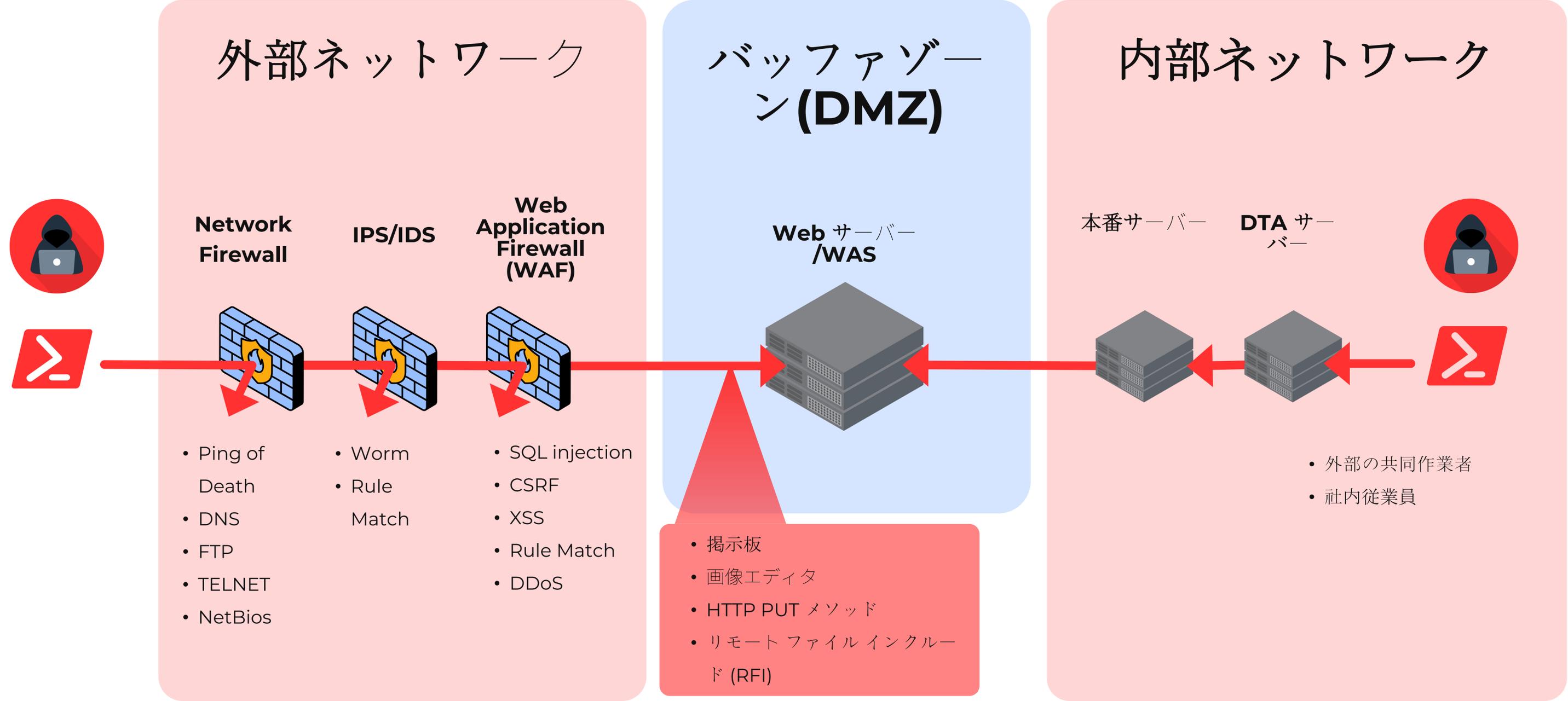
- Webサーバーにマルウェア(Malware)をアップロードして基盤を築く
- 追加のマルウェア(Payload)を実行してWebサーバーファイルを変更する

## 浸透

1

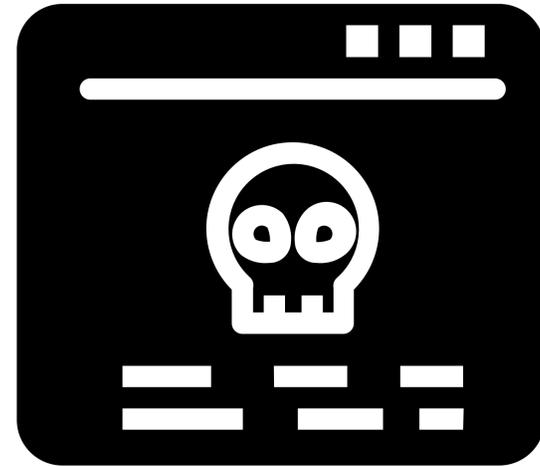
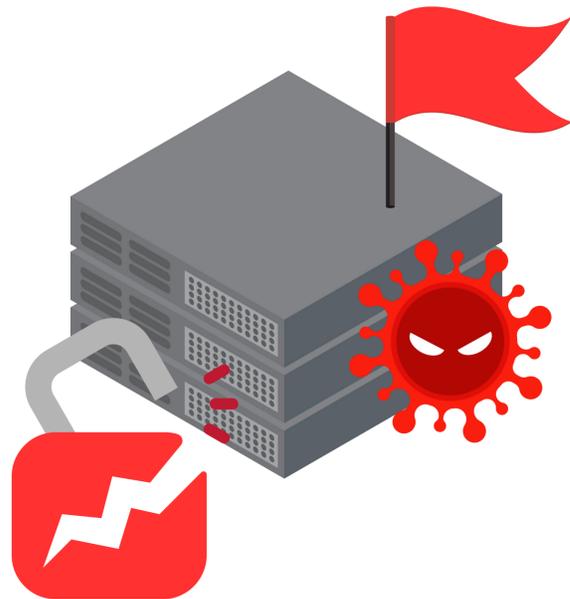
- Webサーバー(Web Server)またはWAS(Web Application Server)の脆弱性を悪用して初期アクセス権を取得する
- 例: SQL Injection、権限の奪取、フィッシング(Phishing)

# 現状維持



ポート 80

# Web攻撃の段階



## ダメージ

3

- 変調(Defacement)
- ソースコード及びコンテンツ偽造・変調

## 高度化

2

- Webサーバーにマルウェア(Malware)をアップロードして基盤を築く
- 追加のマルウェア(Payload)を実行してWebサーバーファイルを変更する

## 浸透

1

- Webサーバー(Web Server)またはWAS(Web Application Server)の脆弱性を悪用して初期アクセス権を取得する
- 例: SQL Injection、権限の奪取、フィッシング(Phishing)

- 「あなたのウェブサイトがハッキングされました。慌てないでください。私のEメールにご連絡いただければ、問題を解決いたします。覚えておいてください、あなたがウェブサイトを直すとしても、私はシェルバックドアを通じて継続的にアクセスできます。ウェブサイトを削除しても、あなたのウェブサイトは安全ではありません。」

your website has been hacked by [REDACTED], don't panic  
contact my email and we will solve it well remember  
even if you fix it again I can still access my  
shell backdor even though you have deleted your website, it is not sturdy

Contact Me [REDACTED] : [REDACTED]@gmail.com

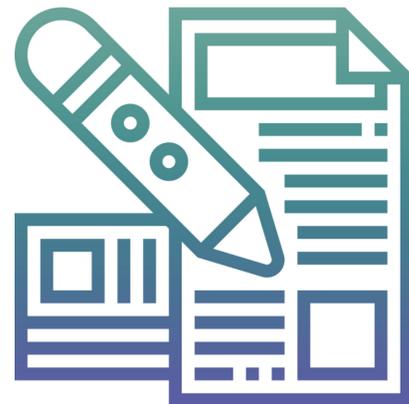
鍵:

# リアルタイムの検出と対応

すべての攻撃は3つの変化のうちの1つから始まります。



1  
ファイル生成



2  
ファイルの修正



3  
ファイル削除

# Website Attack Restoration & Security Solution (WARSS)

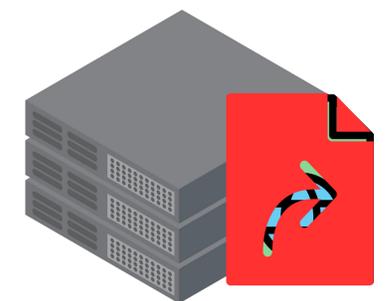
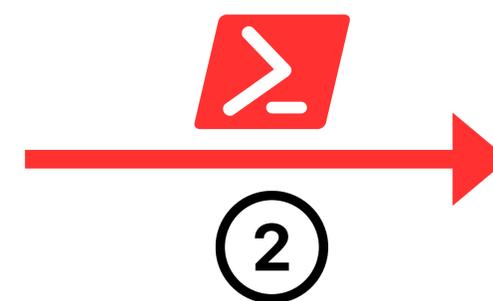
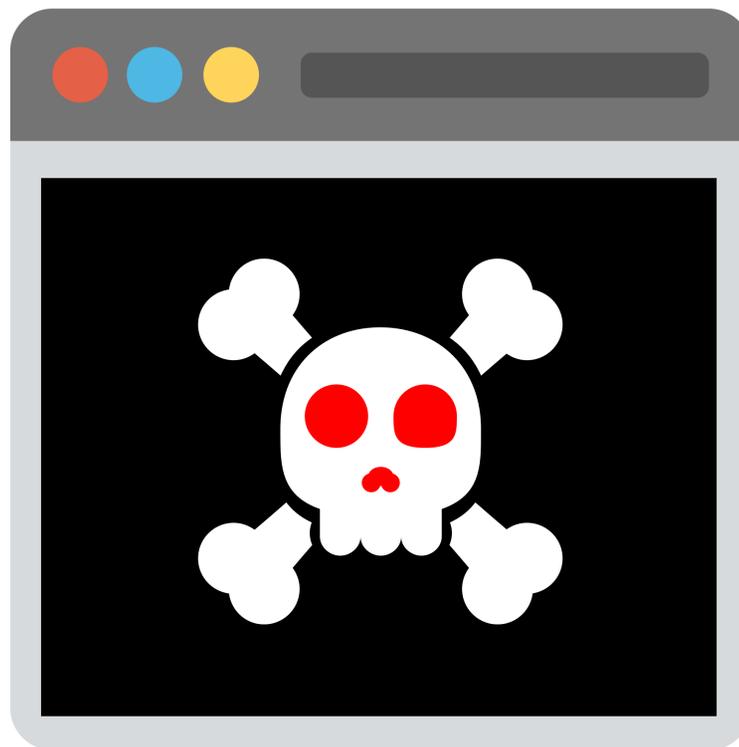
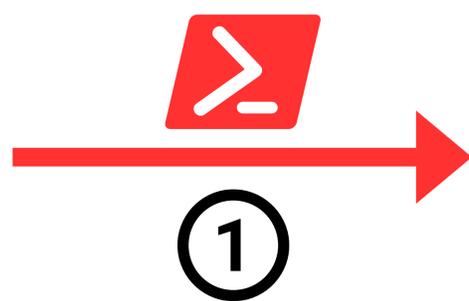
Webサーバーセキュリティソリューションは、ウェブサイトへの不正な変更を検出し、リアルタイムで復元します。



# ホームページ偽造変調はどのように発生 しますか？

ウェブサイトの脆弱性

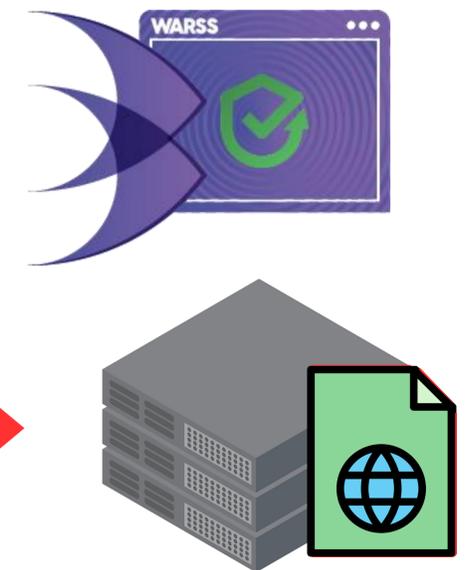
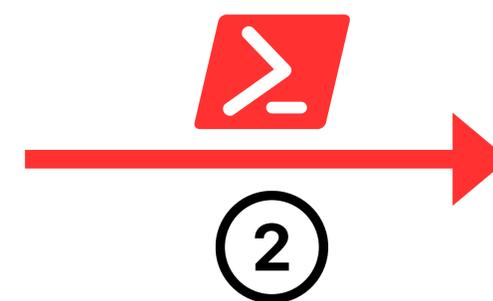
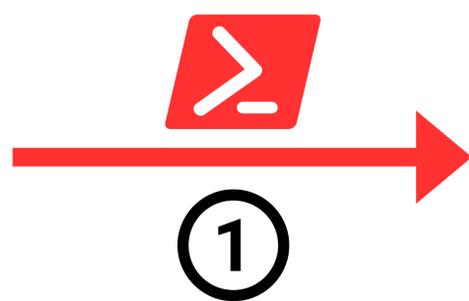
Webサーバー



# WARSSはどのように機能しますか？

ウェブサイトの脆弱性

Webサーバー



# デモ

The screenshot displays the WARSS 2.7.0.4 interface. The main window is a terminal session on a Linux system (localhost.localdomain) connected to 192.168.1.40. The terminal shows the following commands and output:

```
[root@localhost html]# ll
total 4432
-rw-r--r--. 1 root root 279 Jun 11 05:58 index_2.html
-rw-r--r--. 1 root root 281 May 31 04:14 index.html
-rw-r--r--. 1 root root 1682529 Jun 11 05:24 resim1.png
-rw-r--r--. 1 root root 2844197 Jun 11 05:24 resim2.png
drwxr-xr-x. 2 root root 42 Jun 11 07:51 warss1
drwxr-xr-x. 2 root root 42 Jun 25 08:14 warss2
[root@localhost html]# cp -R index_2.html warss1/index.html
cp: overwrite 'warss1/index.html'? y
[root@localhost html]# cp resim2.png warss1/
[root@localhost html]# cp -R index_2.html warss2/index.html
cp: overwrite 'warss2/index.html'? y
[root@localhost html]# cp resim2
```

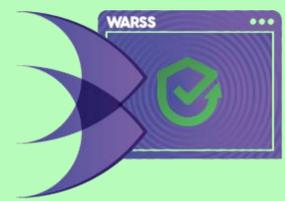
The interface also features a 'Monitor' window on the right, which displays a list of events and their corresponding agent names and server names. The events include:

- Anti-Falsification Detection
- Detection Errors
- Warnings
- Network Status
- Agent Status

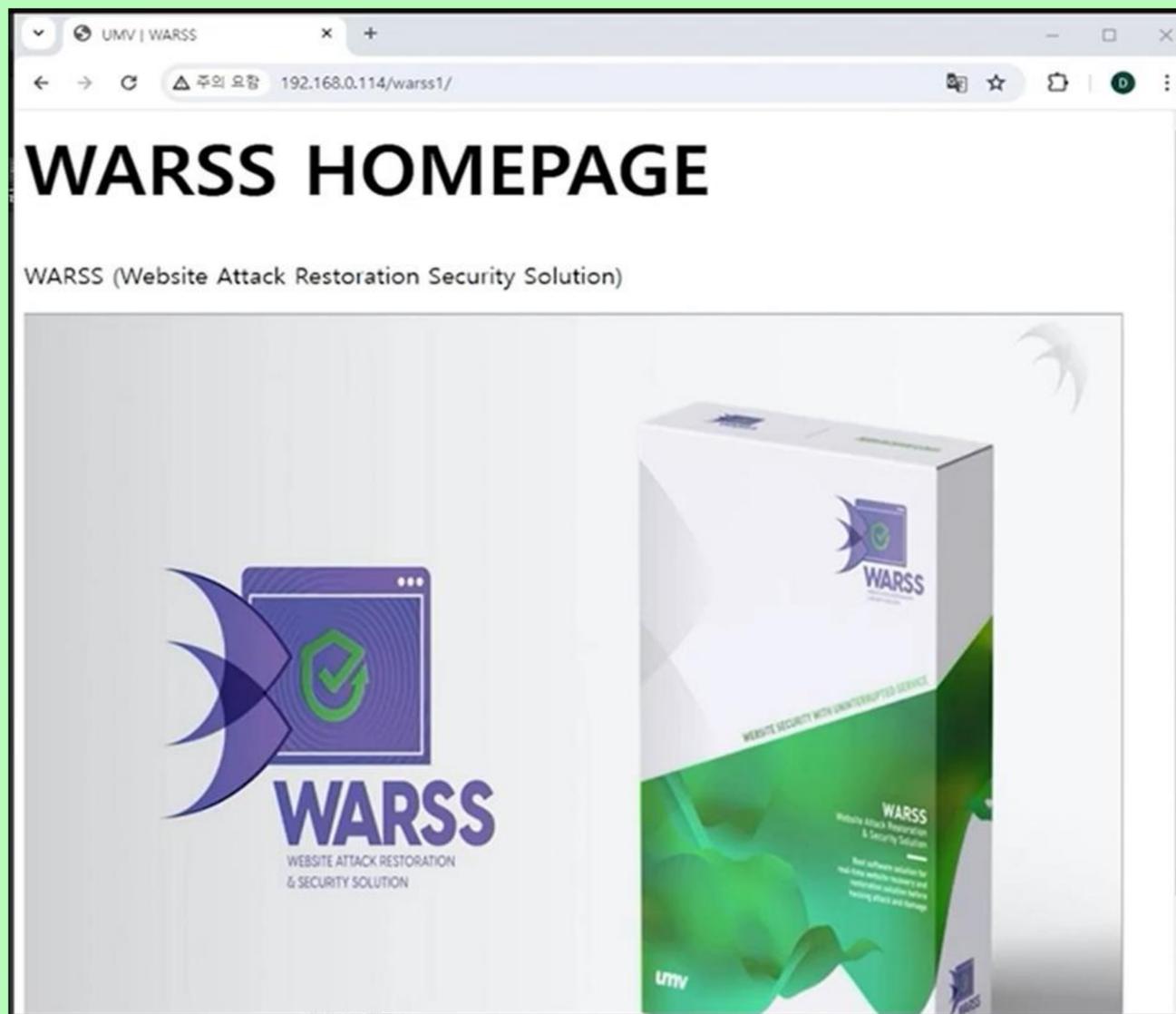
The 'Monitor' window also includes a search bar and a table with columns for 'Contents', 'Agent Name', and 'Server Name'. The table shows several entries, including 'The Restore Anti-Falsification file has been rest...', 'Settings file changed.', and 'Agent set not to detect.'.

<https://www.youtube.com/watch?v=B20LDk0iAJQ>

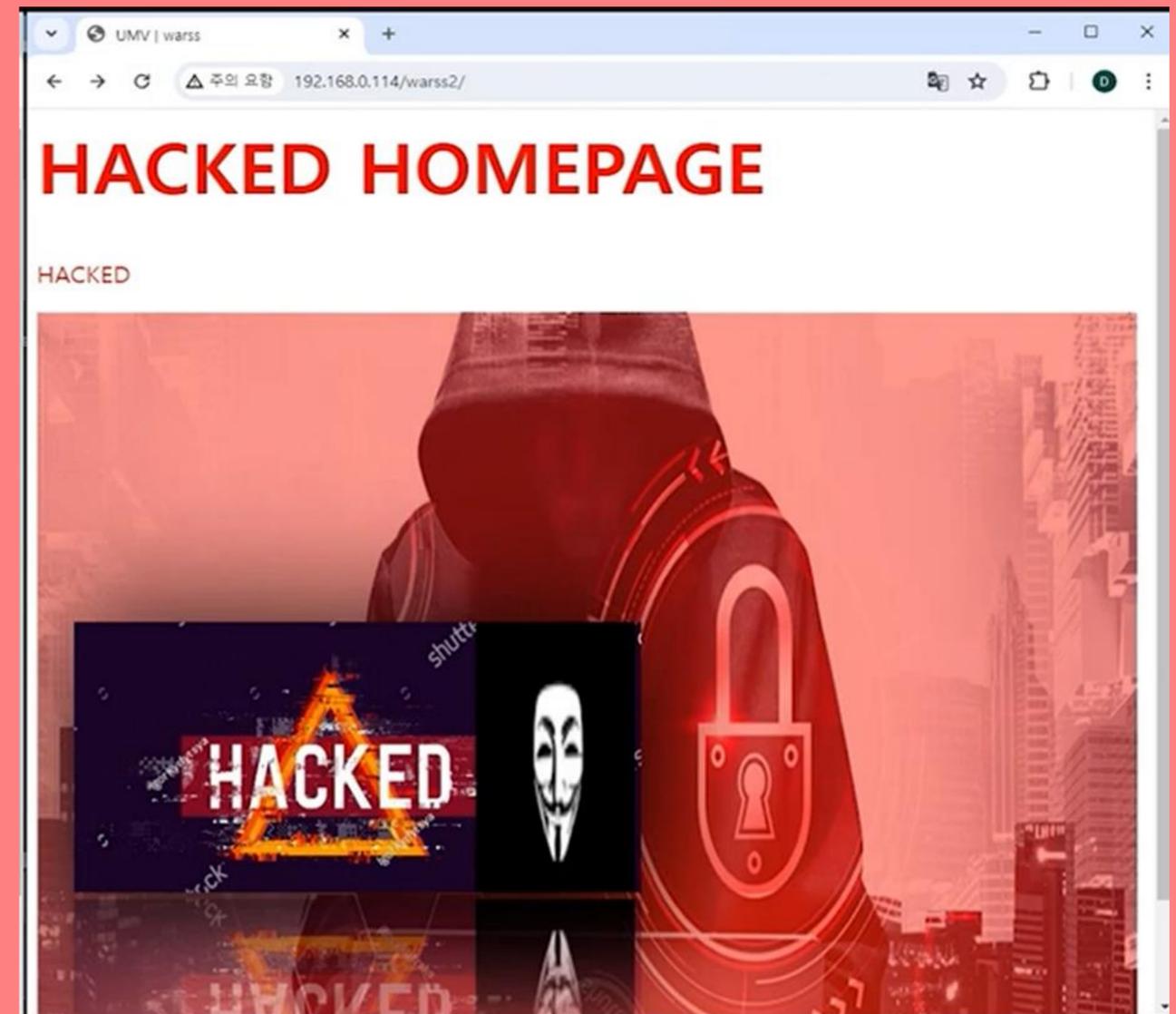
# 実際の操作画面



WARSSを導入したWebページ



導入していないWebページ



# WARSS 構成



## WARSS Management Server(s)

- HW/VMにインストールされたサーバーソフトウェア
- エージェントをリモートで管理および制御
- 検出履歴の保存
- エージェントへの更新と設定変更のデプロイ



## WARSS Agent(s)

- Webサーバー/WASにインストールされたプログラム
- ソースコードとサーバー内のファイル、データの変化を検出
- Unix、Linux、Windows NT O/Sと互換性(JDK 1.5以上サポート必須)



## WARSS Manager Program

- 管理者PCにインストールされたプログラム
- 検出、リモートアクション、環境設定、レポート設定の管理
- アクセス管理、統計、レポートの設定

# WARSS の違い

## WARSS



## Web Crawlers



検出方法:

リアルタイム、パターンベース

定期的な検出

負荷:

最適化されたリソース使用率 (CPU の約 1%)

エージェントレス

検出対象:

サーバー ファイル (ソース コード、データ、コンテンツ)

コンパイルされた URL ユニットとデータ ファイル

対策:

リアルタイムの自動復元

侵害時の手動緩和

# リアルタイム検出

ソースコード  
とコンテンツ  
を保護



軽量

# 即時の復元と回復

# ZERO TRUST

1. “決して信頼せず、常に検証”
2. 最小権限のアクセス
3. 侵害を想定

# ZERO TRUST

## 3. 侵害を前提とした設計



リアルタイム検出

効率的な管理

迅速な対応

リアルタイムの  
ファイル監視

リアルタイムのア  
ラートとレポート

自動復元と回復



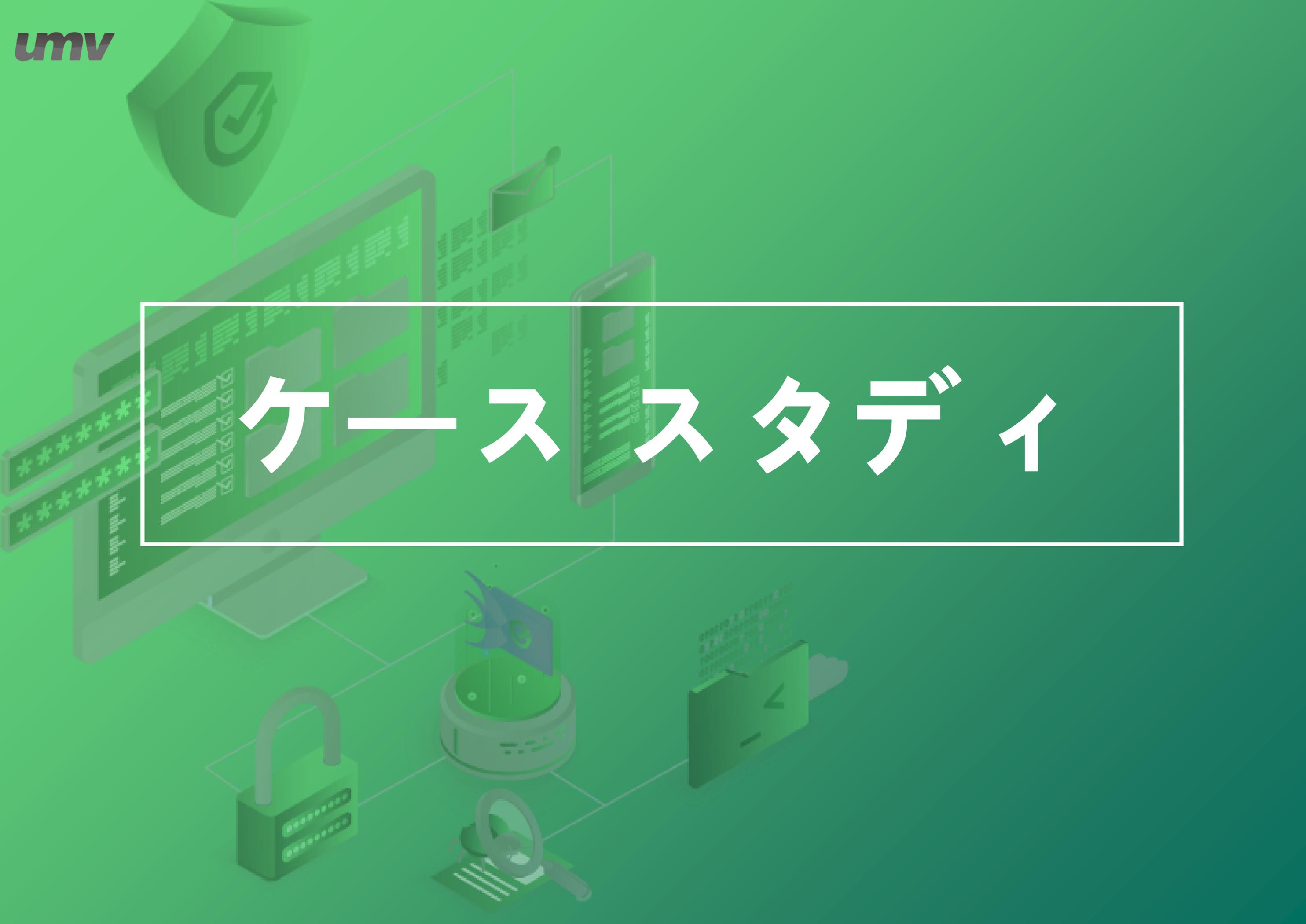
# GS (Good Software)

## 레벨 1 認定

- 테스트 標準 :  
ISO/IEC 25023, 25051, 2504
- ~ 向けに 検証 された :
  - 機能 適合 性
  - 性能 効率 性
  - 互換 性
  - 使用 性
  - 信賴 性
  - セキュリティ
  - メンテナンス
  - モビリティ



# ケーススタディ



# 政府防衛機関

## セキュリティの欠陥

「W」 Web ベースの偽造検出ソフトウェアのパフォーマンスと管理のしやすさに不満

## チェックリスト

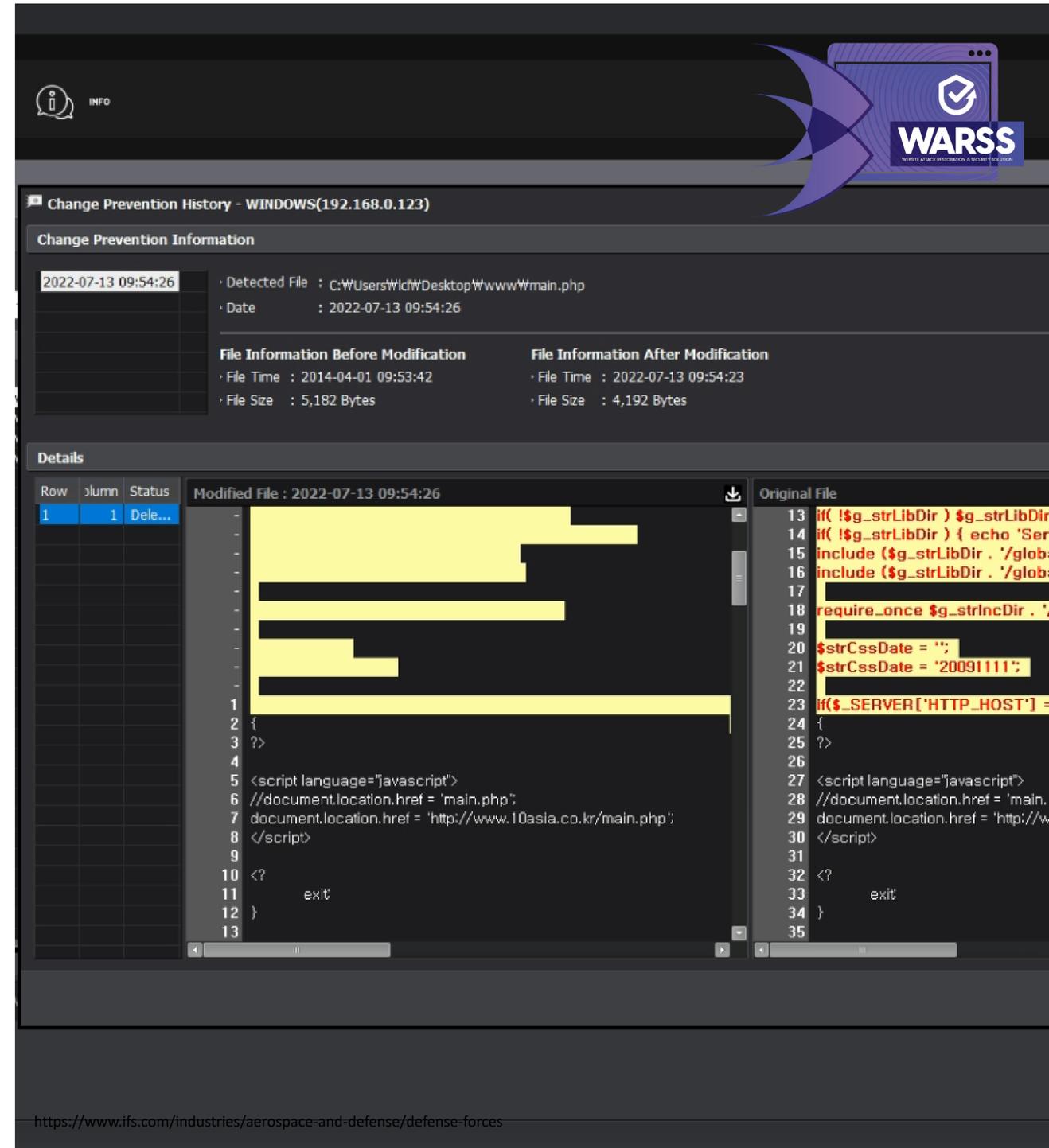
自動復元と効率的な管理を提供するエージェントベースのソリューションを特に探していた

## 2023 WARSS 実装

すべての Web サーバーに 50 個の WARSS エージェントをインストール

## フィードバック

WARSSの自動ホームディレクトリ検出機能に満足、URLを手動で入力しなくても簡単に検出設定可能



# 交通機関

## コンテンツ偽造の懸念

教育コンテンツ(画像、動画)を含むウェブサイトを運営しており、独自の偽造防止ソリューションの開発を外注しようとしたが失敗した。

## なぜ WARSS なのか?

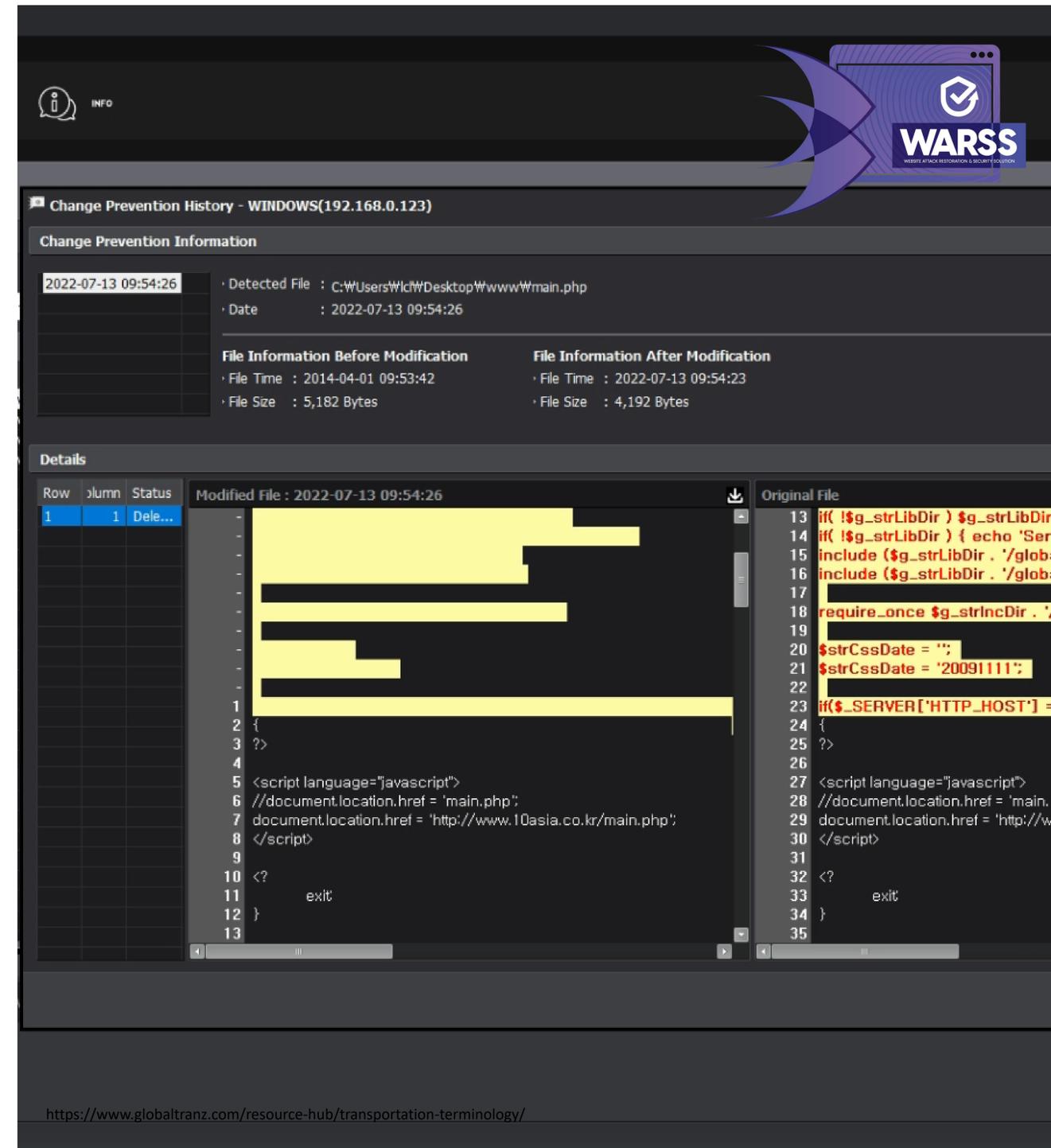
テストした他の偽造防止ソリューションと比較して、WARSSはソースコード、画像、およびビデオ偽造防止機能を提供する唯一のソリューションでした。

## WARSS を選んだ理由

すべての Web サーバーに 100 個の WARSS エージェントをインストール

## 継続的な保護

WARSS はそれ以来、偽造事件を防止してきました。  
お客様はシステムにサーバーを追加するたびにエージェントを購入し続けています



# 顧客会社



대한민국육군  
Republic of Korea Army



한국지역난방공사  
KOREA DISTRICT HEATING CORP.



국방과학연구소  
Agency for Defense Development

ETRI  
한국전자통신연구원  
Electronics and Telecommunications Research Institute

서울특별시  
SEOUL METROPOLITAN GOVERNMENT



영남대학교  
Yeungnam University

LS ELECTRIC



한전원자력연료  
KEPCO NUCLEAR FUEL

한국도로교통공단  
KOROAD

...そしてより多くの会社！

# 何百ものお客様



13+ years



13+



7-8



Hanwha

13+



10+



13+



TOYOTA



STARBUCKS



SUPREME COURT OF KOREA



Ministry of National Defense  
Republic of Korea

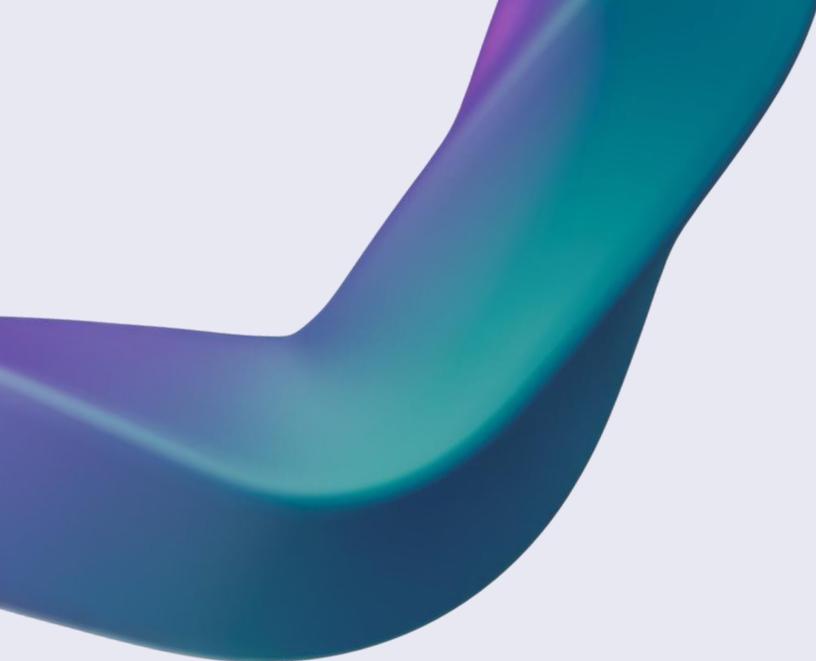


HYUNDAI

Deloitte.

iMBC

...そしてより多くの会社!



**umv**

ありがとう

**UMV Inc.**

韓国、ソウル

 +82 2 448-3435

 [sales@umvglobal.com](mailto:sales@umvglobal.com)

 [www.umvglobal.com](http://www.umvglobal.com)

# 付録

# WARSS の機能

## 偽造の検出と復元

| 機能名   | 説明                               |
|-------|----------------------------------|
| 偽造の検出 | Web サイトのソース ファイルとデータの偽造と変更の検出と通知 |
| 偽造の復元 | 偽造が検出されると、元のファイルをリアルタイムで復元       |
| 元の再指定 | 適法な変更が必要な場合は、基準/原本ファイルを再指定します。   |

# 偽造検出ビュー

偽造の検出とリアルタイム復元

The screenshot shows the WARSS 2.7.0.3 interface. The main window displays a search for tampering history (偽変造検知履歴) for the host (3)LINUX. The search results table shows several entries with timestamps and file paths. A modal window titled '変更防止履歴 - LINUX(192.168.0.141)' is open, showing details for a file change on 2025-07-02 at 16:03:11. The modal displays the original file information (205 bytes) and the modified file information (114 bytes). Below this, a comparison of the file content is shown, with the modified content highlighted in yellow.

検索条件

- 検出機能 :  全体  検出  復元
- 検出日 :  最近の日  全体  期間 2025

| 検査日  | パス        |
|--|-----------|
| <input type="checkbox"/> 2025-07-02 16:03:11 | /home/wet |
| <input type="checkbox"/> 2025-07-02 16:01:31 | /home/wet |
| <input type="checkbox"/> 2025-07-02 16:01:14 | /home/wet |
| <input type="checkbox"/> 2025-07-02 16:00:58 | /home/wet |
| <input type="checkbox"/> 2025-07-02 16:00:13 | /home/wet |

変更防止情報

2025-07-02 16:03:11  
2025-07-02 16:01:31  
2025-07-02 16:01:14  
2025-07-02 16:00:57  
2025-07-01 15:47:07

検出ファイル : /home/wet/test5.asp  
検出日 : 2025-07-02 16:03:11

変更前のファイル情報  
ファイル時間 : 2025-07-01 02:43:57  
ファイルサイズ : 205 バイト

変更後のファイル情報  
ファイル時間 : 2025-07-02 03:03:07  
ファイルサイズ : 114 バイト

詳細履歴

| 行 | 熱 | 状態    | 変更ファイル : 2025-07-02 16:03:11  | 元のファイル  |
|---|---|-------|---|---|
| 7 | 1 | 削除... | 1 <!DOCTYPE html><br>2 <html lang="en"><br>3 <head><br>4 <meta charset="UTF-8"><br>5 <title>My First HTML Page</title><br>6 </head><br>7 [Redacted] | 1 <!DOCTYPE html><br>2 <html lang="en"><br>3 <head><br>4 <meta charset="UTF-8"><br>5 <title>My First HTML Page</title><br>6 </head><br>7 <body><br>8 <h1>Hello, World!</h1><br>9 <p>This is a simple HTML example</p><br>10 </body><br>11 </html><br>12 |

エージェントリスト

- アイコン  リスト  全体  検出された

LINUX(3) TEST(4)

# WARSS 機能

## 管理機能

| 機能名           | 説明  |
|---------------|---|
| 更新管理          | エージェントとマネージャーの更新、バージョン管理  |
| 権限とレポート管理     | <ul style="list-style-type: none"><li>• アカウントとユーザー固有の権限の管理</li><li>• 外部システム (ESM、SMS、電子メールなど) とのインターフェイス</li><li>• レポートと統計</li></ul>      |
| 安定性           | <ul style="list-style-type: none"><li>• リソース使用制御</li><li>• サーバー環境に合わせたカスタマイズ</li></ul>  |
| 攻撃者の IP 検出    | 偽造ファイルの実行IPレポート (検出機能のみが有効な場合は利用可能)   |
| 設定管理          | Web / WAS構成ファイルの管理と変更検出の設定  |
| 専用の安全なアップローダー | <ul style="list-style-type: none"><li>• ユーザー アカウントごとに安全なアップロード先ディレクトリを指定</li><li>• 安全アップローダを使用してアップロードされたファイルにマルウェアがあるかどうかを確認する</li></ul> |



# 管理ビュー

管理者権限

管理者の管理

WARSS (192.168.0.140)

管理者リスト

- 管理者権限
- エージェント権限 (管理者)
- エージェント権限 (エージェント)
- アップロード属性
- メッセージ設定

権限グレードのリスト

| 権限レベル                                | 権限  |
|--------------------------------------|---|
| <input type="checkbox"/> 上級管理者       | <input type="checkbox"/> エージェント - 検出履歴処理        |
| <input type="checkbox"/> 中級管理者       | <input type="checkbox"/> エージェント - 環境設定 (一般、WAS) |
| <input type="checkbox"/> 一般管理者       | <input type="checkbox"/> エージェント - 環境設定 (検出規則)   |
| <input type="checkbox"/> 管理要員 - マルチ  | <input type="checkbox"/> エージェント - 一時停止/再開       |
| <input type="checkbox"/> 管理要員 - シングル | <input type="checkbox"/> サーバー - マルチサーバーの使用      |
|                                      | <input type="checkbox"/> サーバー - 環境設定            |
|                                      | <input type="checkbox"/> 管理者アカウントの作成            |
|                                      | <input type="checkbox"/> エージェントの割り当て、グループの作成    |
|                                      | <input type="checkbox"/> ファイルのアップロード            |
|                                      | <input type="checkbox"/> メッセージ設定                |
|                                      | <input type="checkbox"/> エージェントの削除              |

追加 削除 適用

# 管理ビュー

安定性

環境設定

WARSS > TEST > (3)LINUX

一般 | WAS | ファイル検出 | 高度

サーバー接続設定

拡張

・ WARSSサーバーアドレス : 192.168.0.140      ・ポート : 7778  
・ アップロードサーバーアドレス : 192.168.0.141      ・ポート : 7777  
・ 検出ファイル管理サーバーアドレス :      ・ポート : 0

一般設定

検出設定

・ CPU使用制限 :  10  
エージェントCPU使用率 50 % 以上の時に警告が発生  
システムCPU使用率 0 % 以上の時に警告が発生

デフォルト値で

適用

# 管理ビュー

リソースステータスの監視

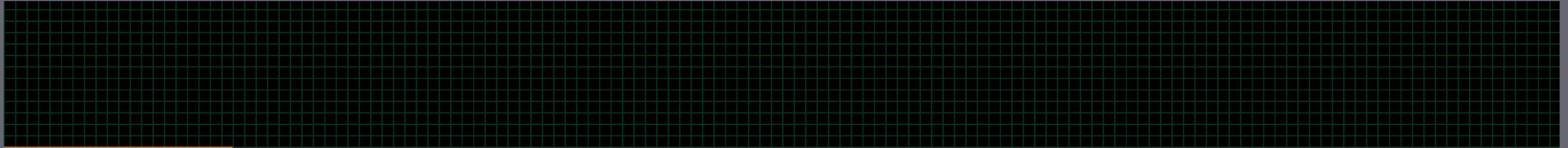


情報

WARSS > TEST > (3)LINUX

エージェント情報 | システム情報 | **資源状況**

## エージェントCPU使用率



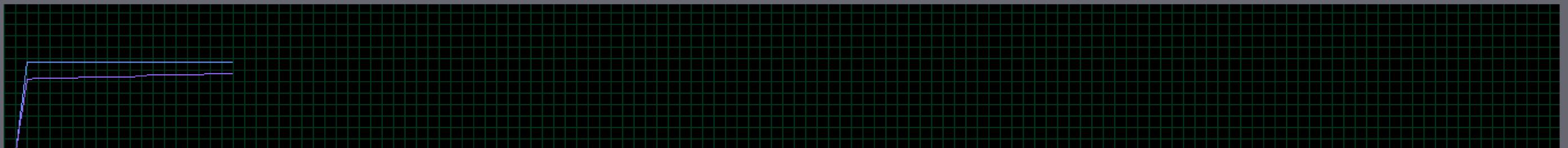
■ エージェントCPU使用率 : 0.1%

## システムCPU使用率



■ システムCPU使用率 : 0.0%

## メモリ使用率



### ■ 実メモリ

・使用率 : 61.3%  
・全体 : 770.5MB  
・使用 : 472.4MB  
・使用可能 : 298.1MB

### ■ 仮想メモリ

・使用率 : 53.4%  
・全体 : 41.0MB  
・使用 : 21.9MB  
・使用可能 : 19.1MB

### ■ ハードディスク

・使用率 : 0.8%  
・全体 : 92.9GB  
・使用 : 0.8GB  
・使用可能 : 92.1GB

# 管理ビュー

攻撃者の IP 検出

攻撃者IP検出 □ ×

・アクセスログ一覧 (0件)

| WAS | アクセスログパス | 構成ファイル |
|-----|----------|--------|
|     |          |        |

◀ | | ▶

(0件)

| 状態 | ファイル |
|----|------|
|    |      |

削除 適用 閉じる

# 管理ビュー

## 設定管理

環境設定 WARSS > TEST > (3)LINUX

一般 | WAS | **ファイル検出** | 高度

検出の基本設定 一般

リアルタイム監視 :  使用

実行周期 : なし

再検出 :  使用 CPU使用制限 :  10

偽造変調ファイル最小サイズ : 0 バイト 偽造変調の復元 :  使用

検出ファイルのバックアップ数 : 2 個 検出ファイル数超過通知 : 0 個

検出ファイルのバックアップの削除 :  設定された期間を過ぎたバックアップファイルの自動削除 90 日

拡張子バイパス検出 :  使用

検出ファイル数確認経過時間通知 : 10 時間

偽造変調ファイル最大サイズ : 5120 KByte(s) 全体メモリ使用量が95%を超えると一時停止 :  使用

検出ディレクトリの設定 ( 1 件 )

| 使用                                  | ディレクトリ    | 状態 | 読む | 書く | 設定 | コード                                 | 偽造変調                                | 復元                                  | 拡張子   | URL | ログパス情報 |
|-------------------------------------|-----------|----|----|----|----|-------------------------------------|-------------------------------------|-------------------------------------|---|-----|--------|
| <input checked="" type="checkbox"/> | /home/wet | 含む | ✓  | ✓  | 手動 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | asp,aspx,asa,cer,cdx,hta,ascx,asax,ashx,soap,r... |     |        |

デフォルト値で ディレクトリ設定 WASディレクトリ 削除

偽造変調検出ディレクトリの設定 適用



# WARSS 機能

クラウドコンピューティングサポート

| 機能名          | 説明  |
|--------------|---|
| スケール イン/アウト  | <ul style="list-style-type: none"><li>スケール アウト時に新しい検出ターゲットを自動登録し、検出を自動的に開始します</li><li>スケール イン時に削除されたエージェントの検出/変更/削除ログを管理サーバーに自動バックアップ</li></ul> |
| ホーム ディレクトリ検索 | <ul style="list-style-type: none"><li>Web/WAS ホーム ディレクトリへの変更/追加を見つけるための検出をスケジュールします</li><li>ホーム ディレクトリの追加/変更履歴の表示</li></ul>                     |
| 履歴管理         | エージェントの動作状況と履歴管理 (インストール、削除、開始/停止など)  |
| イベント重複防止     | ホーム ディレクトリが NAS 領域に含まれている場合、冗長システムで重複検出イベントが発生しないようにします   |



# クラウド設定ビュー

ログ記録/履歴管理

モニタリング 🔍 ✕

偽造変調検出     警告     エージェントの状態  
 検出エラー     ネットワークステータス

今日     期間指定

2025-07-02 ▾ ~ 2025-07-02 ▾ 照会

| 内容                  | エージェント名   | サーバー名 |
|---------------------|-----------|-------|
| 環境設定ファイルが変更されました。   | (3) LINUX | WARSS |
| 環境設定ファイルが変更されました。   | (3) LINUX | WARSS |
| 偽造変調復元ファイルが修復されました。 | (3) LINUX | WARSS |
| ネットワークが接続されました。     | (4) TEST  | WARSS |
| ネットワークが接続されました。     | (3) LINUX | WARSS |
|                     |           |       |
|                     |           |       |
|                     |           |       |
|                     |           |       |
|                     |           |       |
|                     |           |       |
|                     |           |       |
|                     |           |       |

# WARSS オンプレミス構成図

