umv

WARSS

Website **A**ttack **R**estoration
Security **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

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？

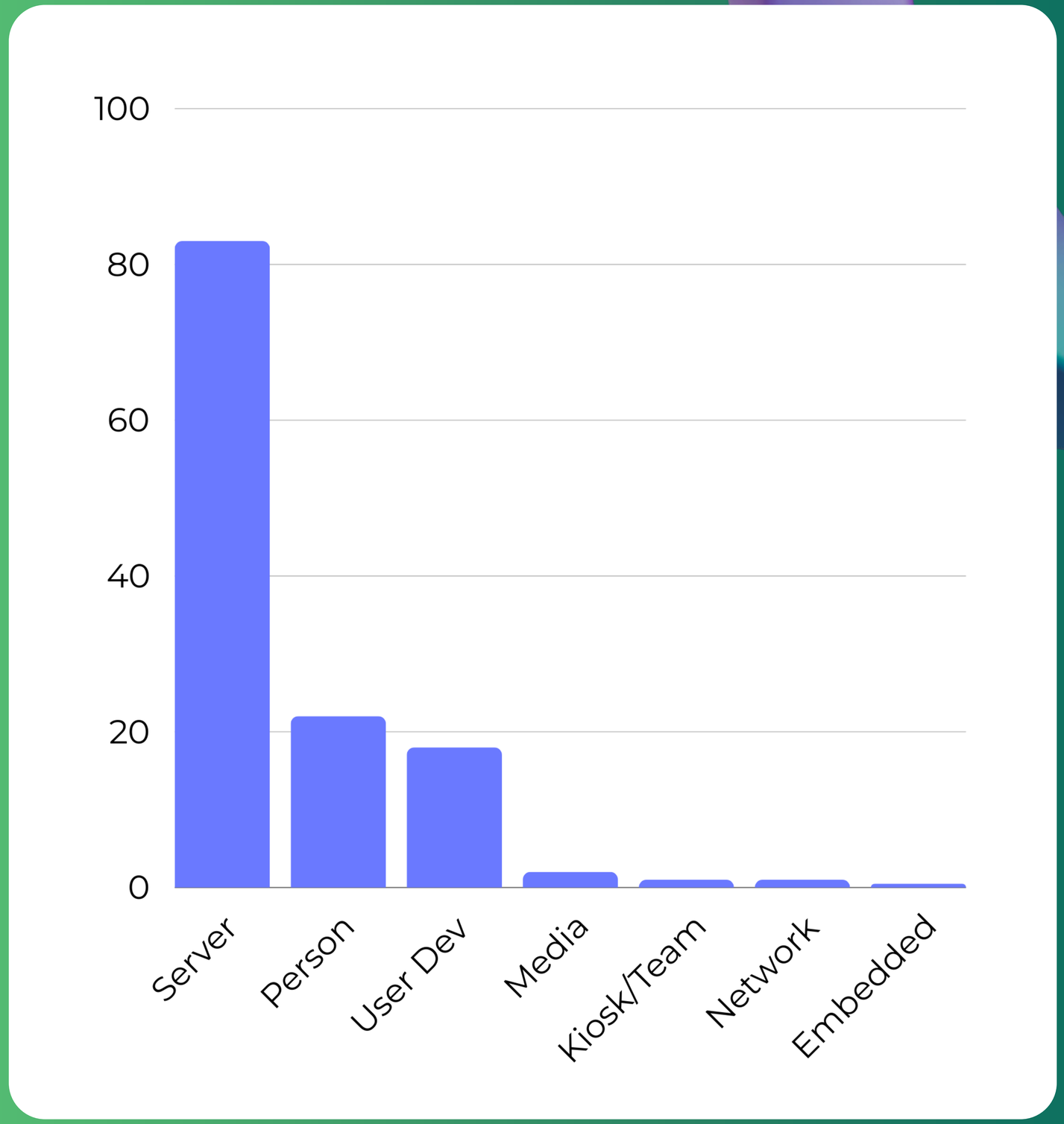
増加するウェブハッキング

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。

2024 Verizon データ侵害調査レポート

侵害の影響を受ける資産

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

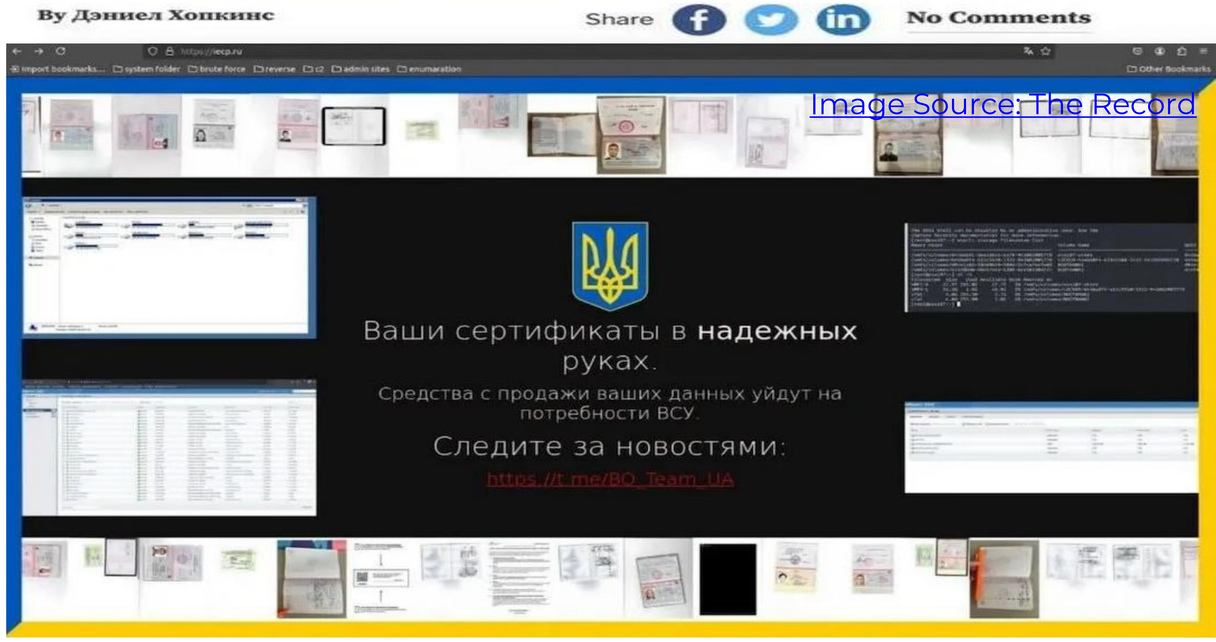


Image Source: The Record

- https://therecord.media/ukrainian-news-outlets-attacked-by-russian-hackers
- https://therecord.media/russia-osnavanie-digital-signatures-cyberattack-ukraine

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

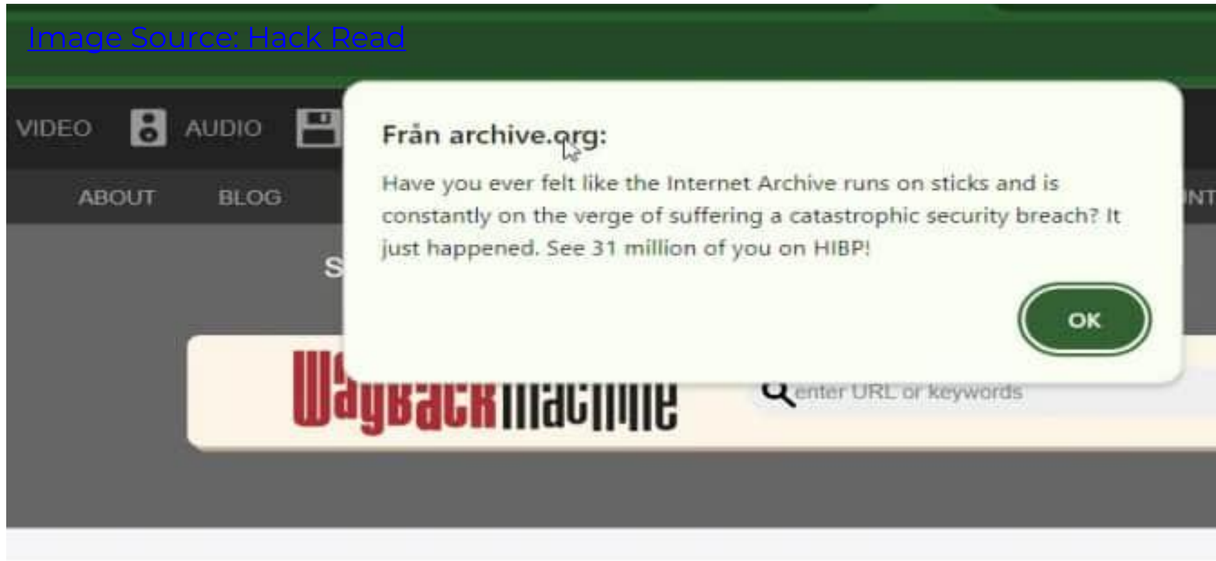
2024 年 10 月 9 日 : DDoS 攻撃によりサイトがダウン、Web サイトが JavaScript アラートで改ざんされる。3100万件のユーザーアカウントのユーザー名、メールアドレスなどが漏洩

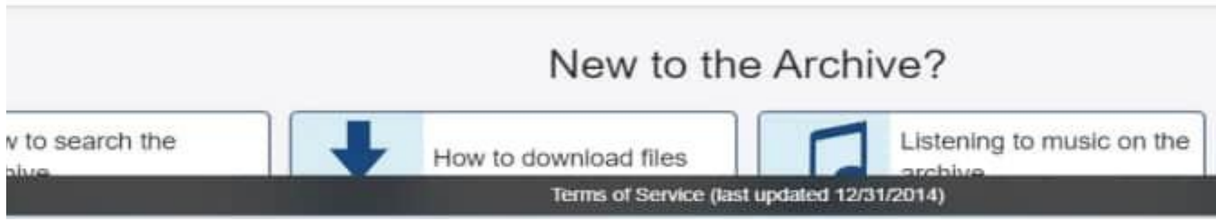
通常に戻る

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

- https://unicri.it/sites/default/files/2024-06/DW.pdf

umv

ウェブサイト改ざん

ウェブサイト改ざん 方法

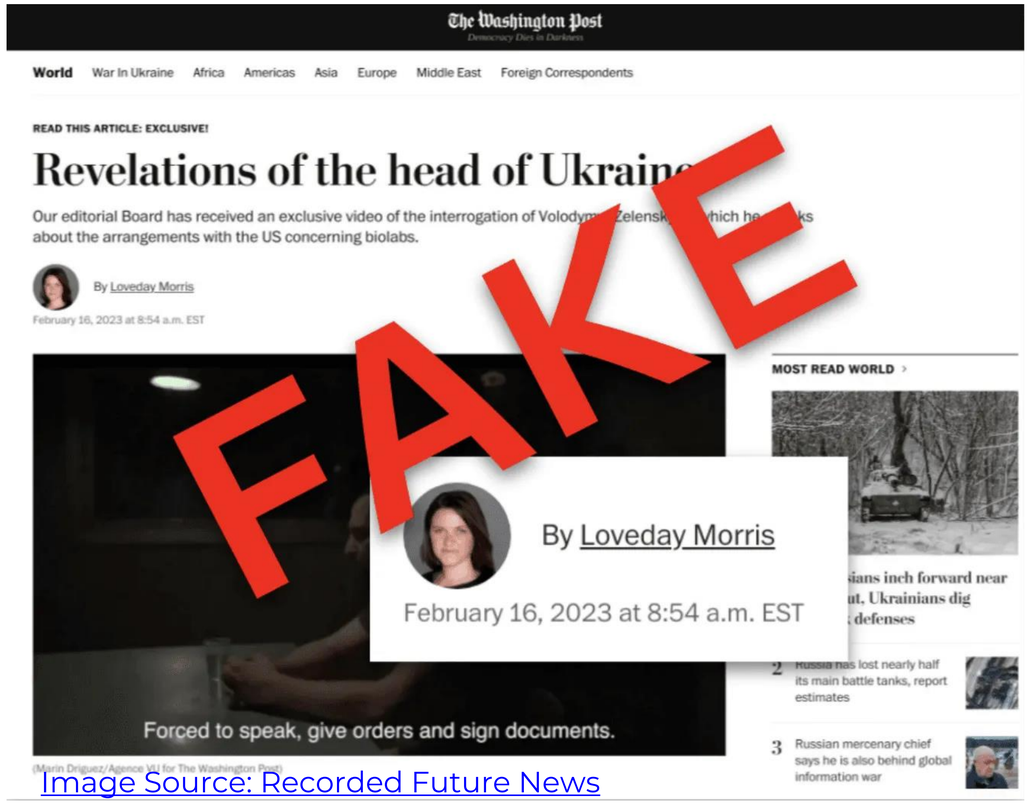
1. ソースコードの修正

Image Source: alphavilleherald.com

Image Source: 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



[Image Source: Recorded Future News]

[Image Source: National Post]

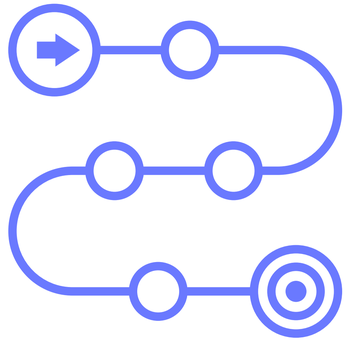
なぜディフェイス（**Defacement**）攻撃が行われるのか？

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

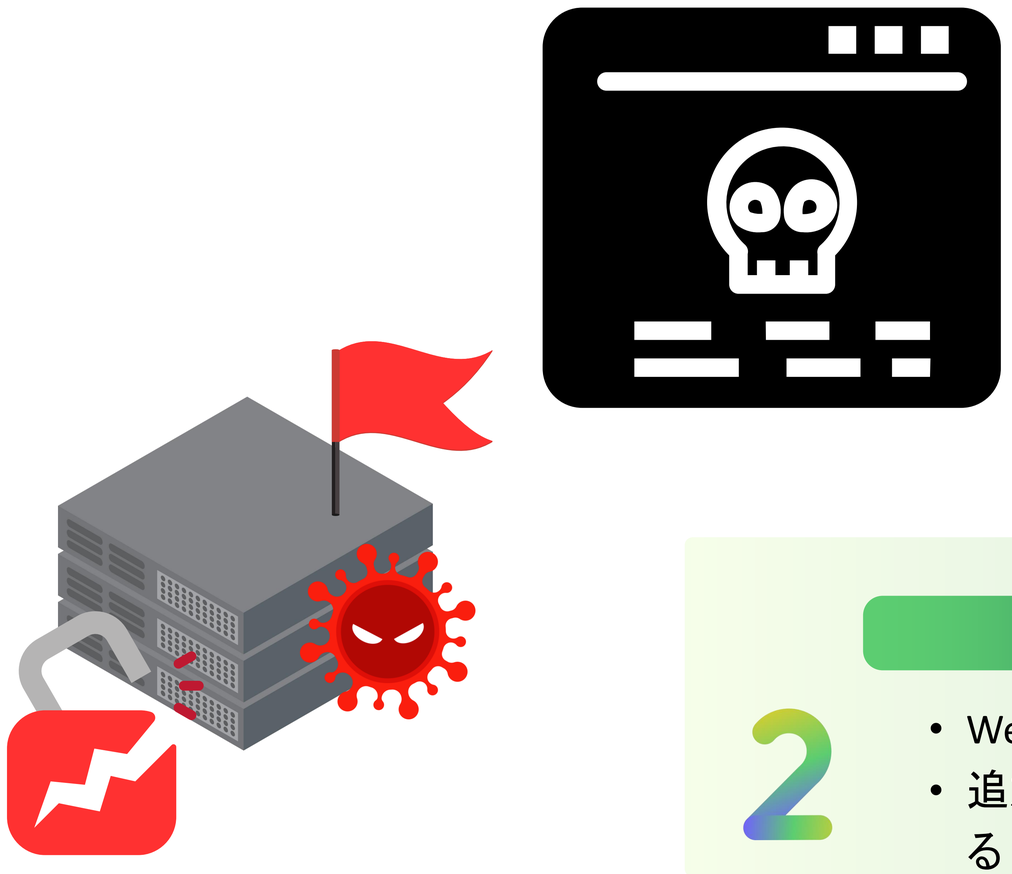


方法

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



3 ダメージ

- 変調(Defacement)
- ソースコード及びコンテンツ偽造・変調

2 高度化

- 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

1 浸透

- 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

外部ネットワーク

Network Firewall

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

IPS/IDS

- Worm
- Rule Match

Web Application Firewall (WAF)

- 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

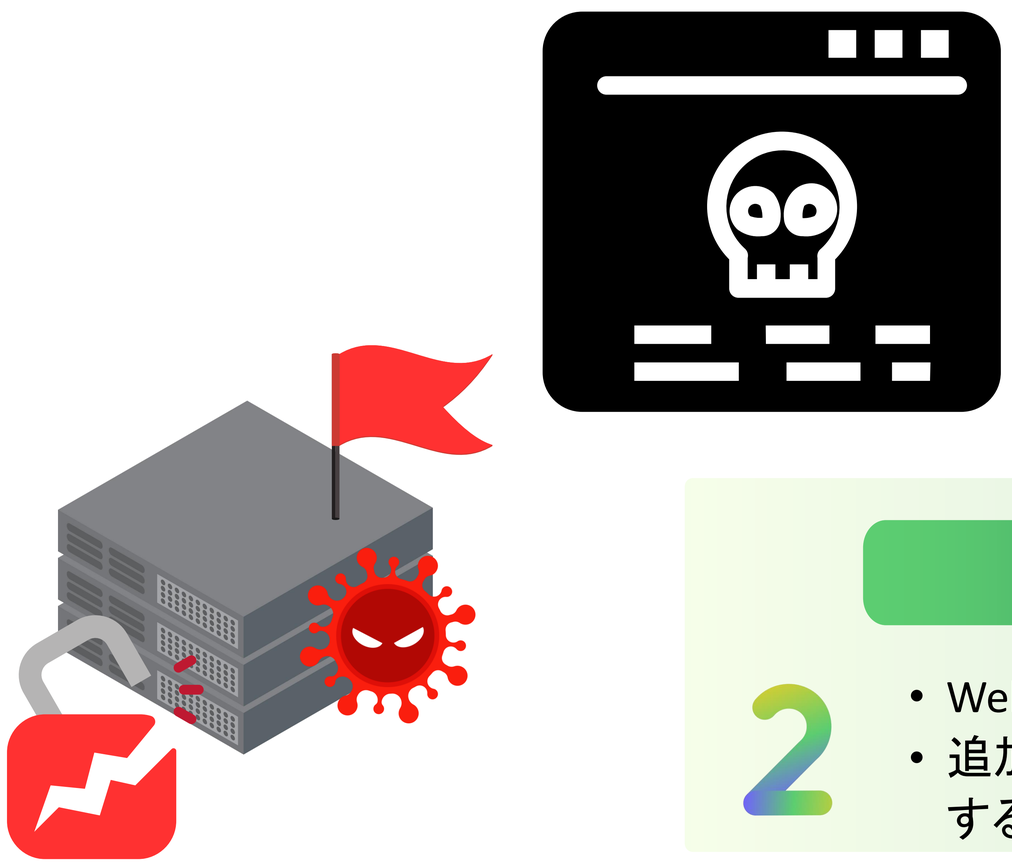
本番サーバー

DTA サーバー

- 外部の共同作業者
- 社内従業員

ポート 80

Web攻撃の段階



3 ダメージ

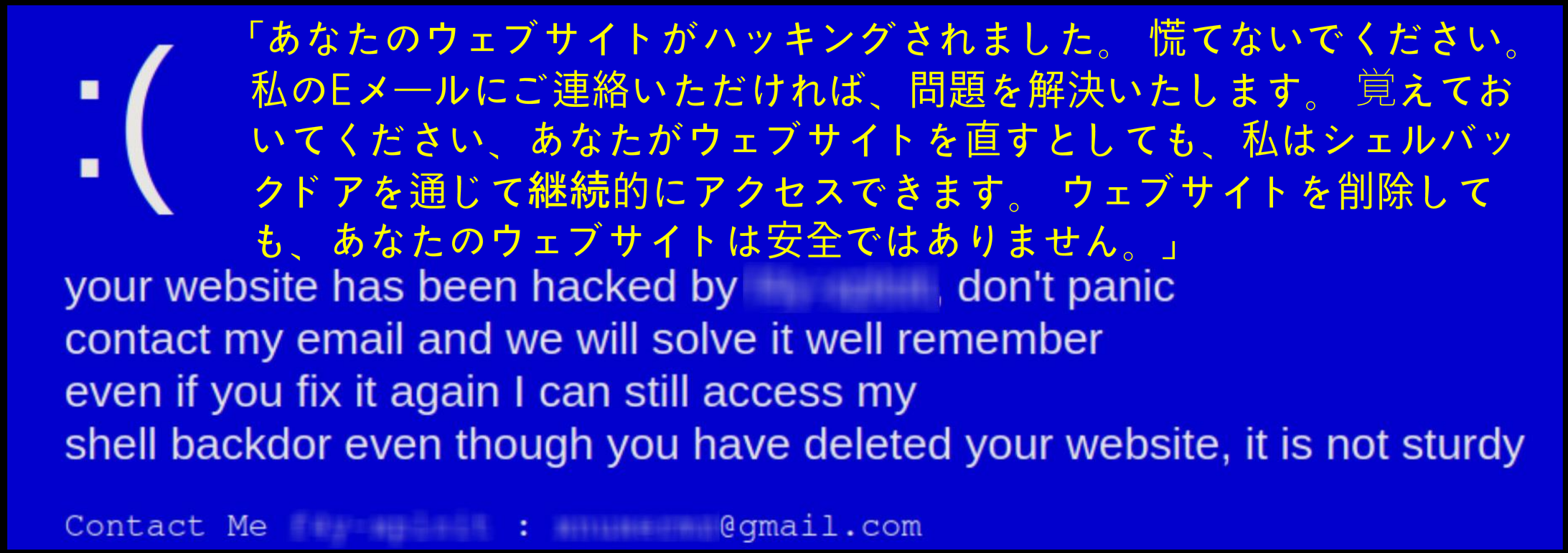
- 変調(Defacement)
- ソースコード及びコンテンツ偽造・変調

2 高度化

- 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

1 浸透

- 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)



https://blog.sucuri.net/wp-content/uploads/2023/03/image-1.jpg

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

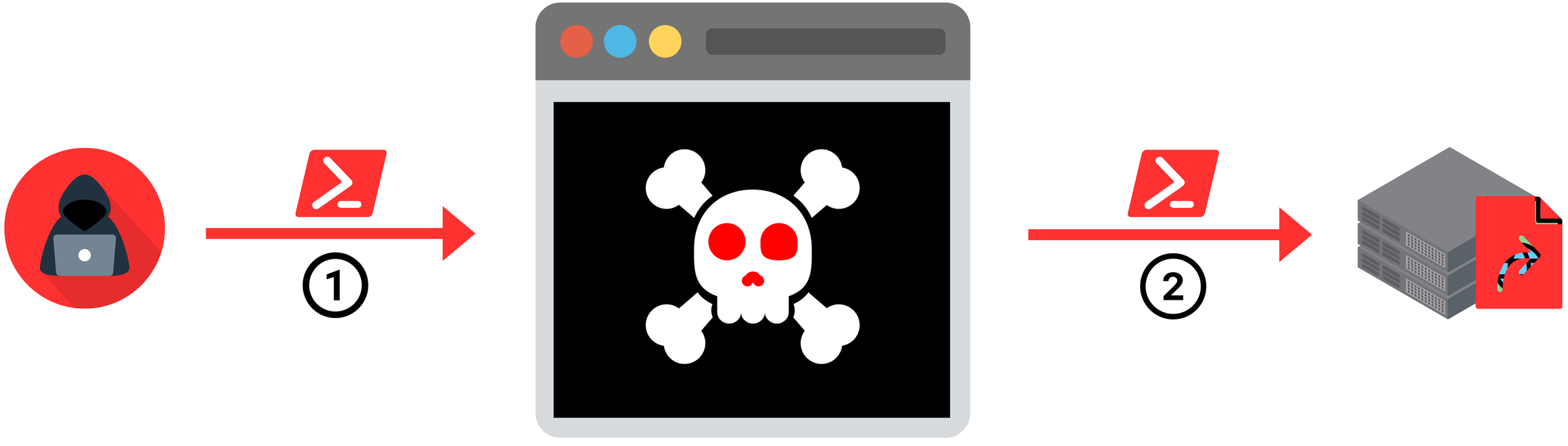
3
ファイル削除

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

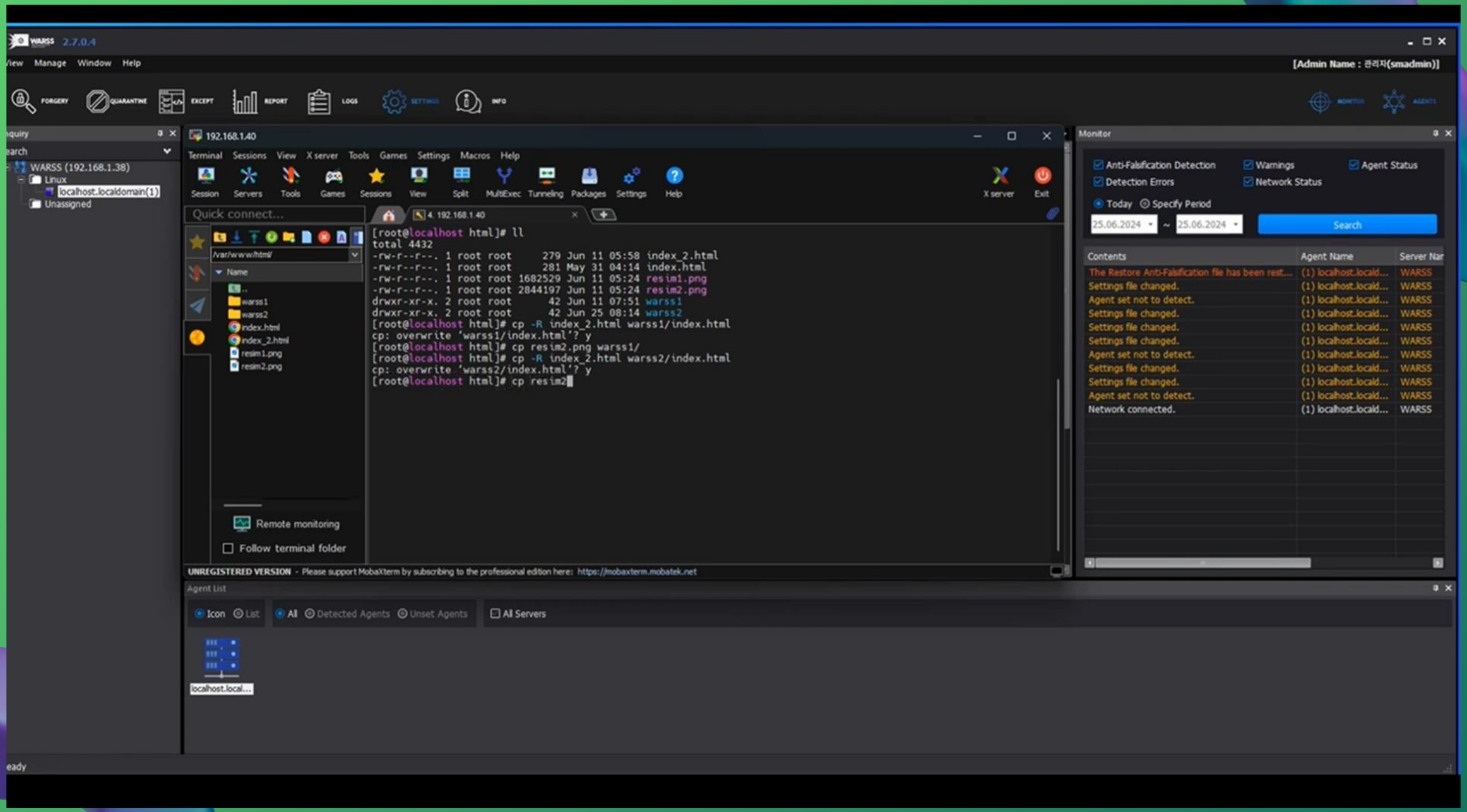


WARSSはどのように機能しますか？

ウェブサイトの脆弱性

Webサーバー

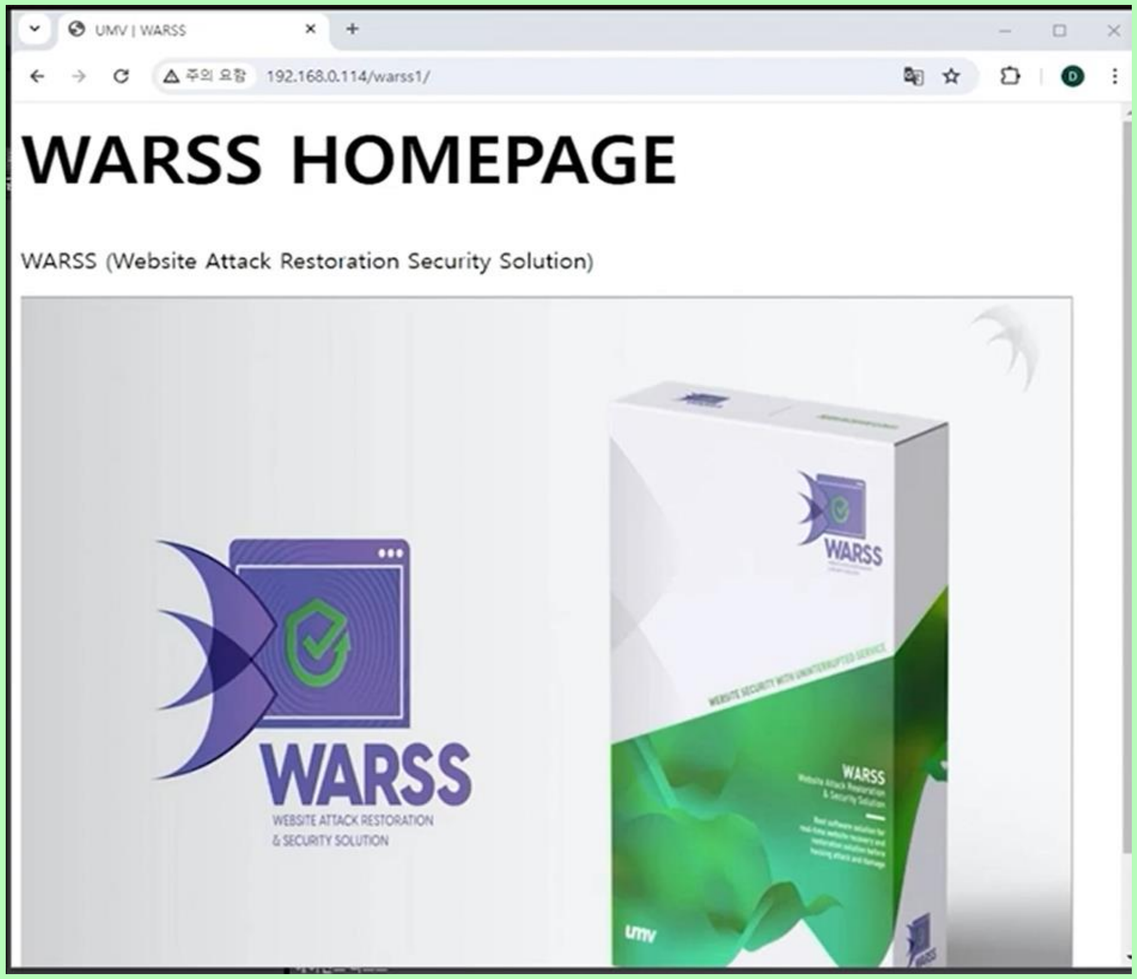
デモ



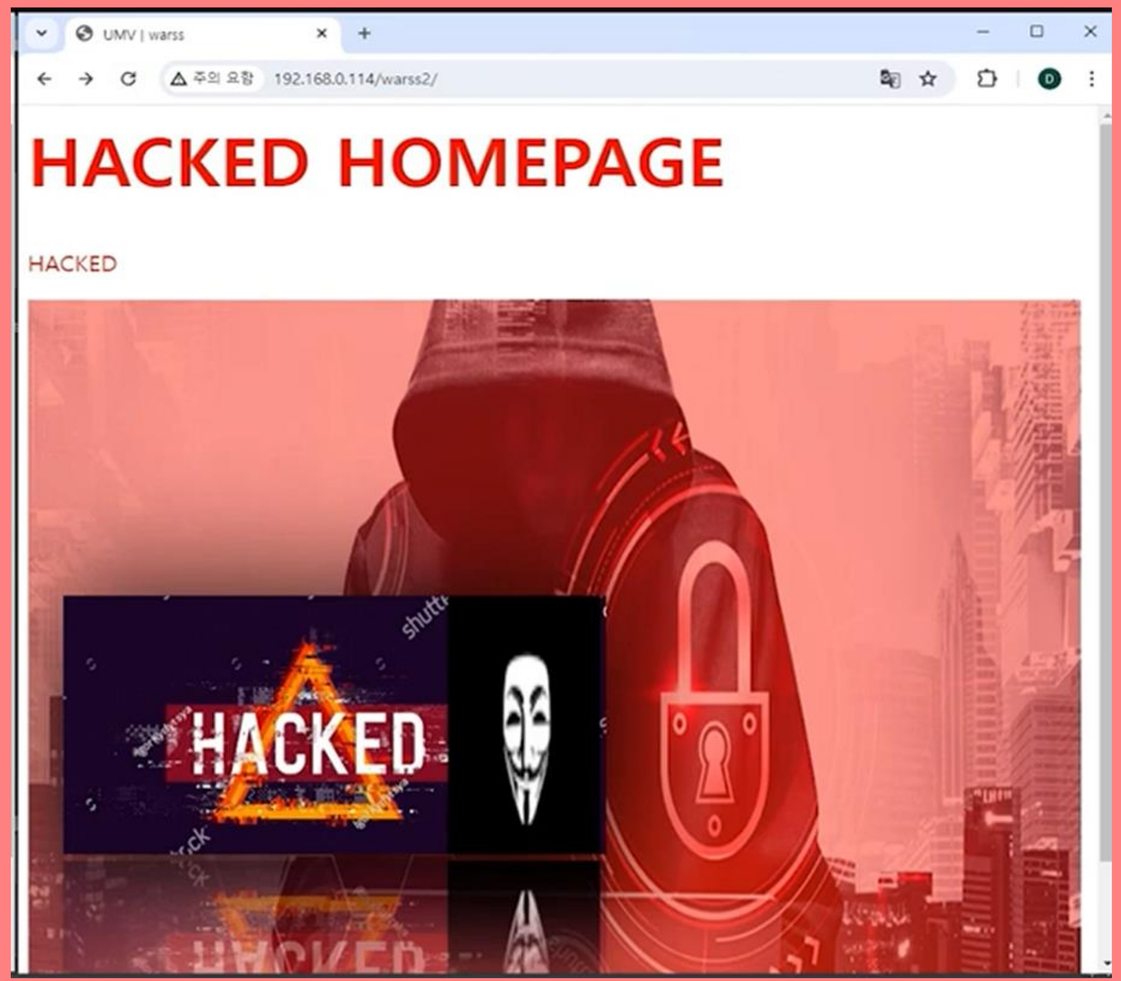
https://www.youtube.com/watch?v=B20LDk0iAJQ

実際の操作画面

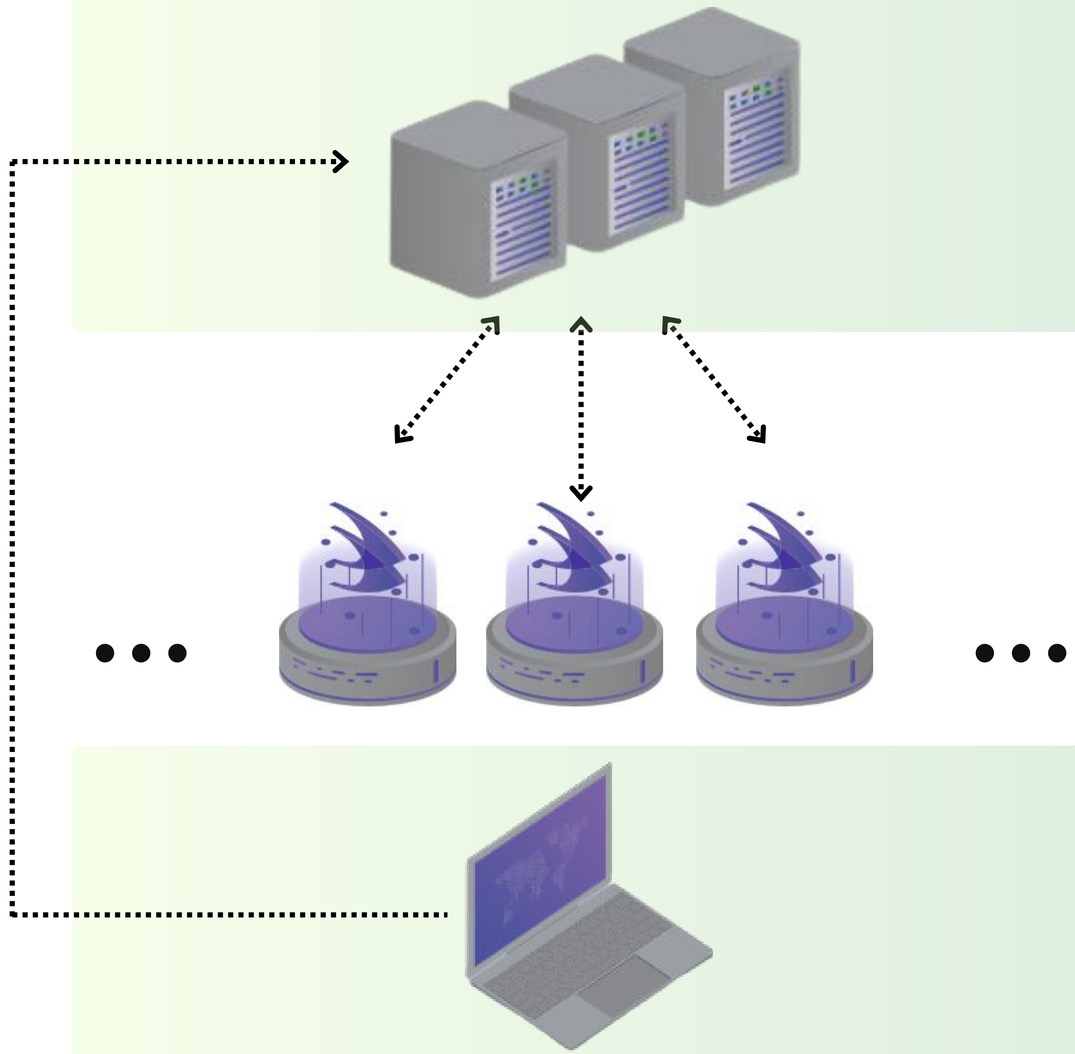
WARSSを導入したWebページ



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

リアルタイムの
ファイル監視

効率的な管理

リアルタイムのア
ラートとレポート

迅速な対応

自動復元と回復

GS (Good Software)
レベル 1 認定

- テスト標準：

  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
  - 信頼性
  - 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

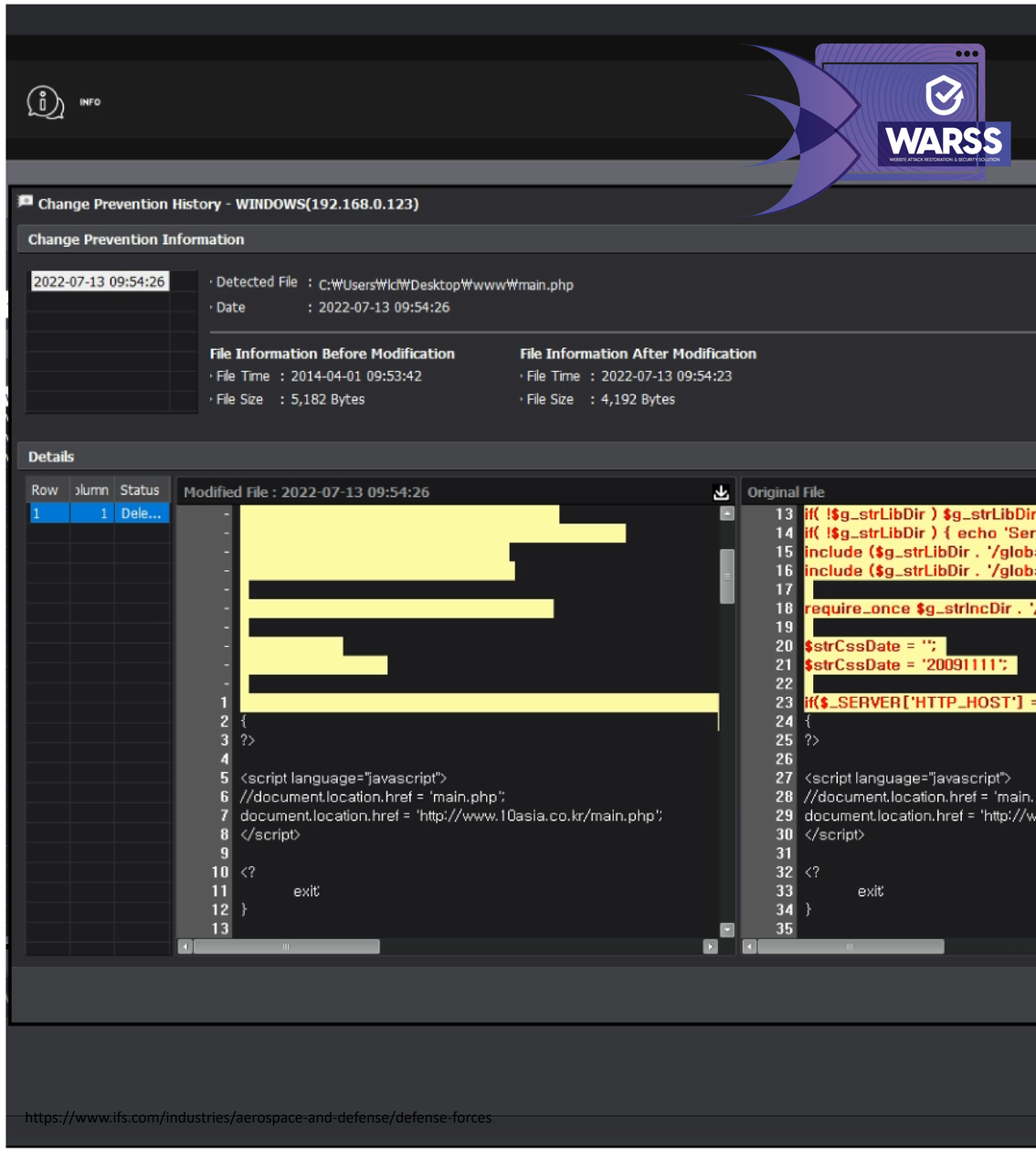
自動復元と効率的な管理を提供するエージェントベースのソリューションを特に探していた

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



https://www.ifs.com/industries/aerospace-and-defense/defense-forces

umv

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?

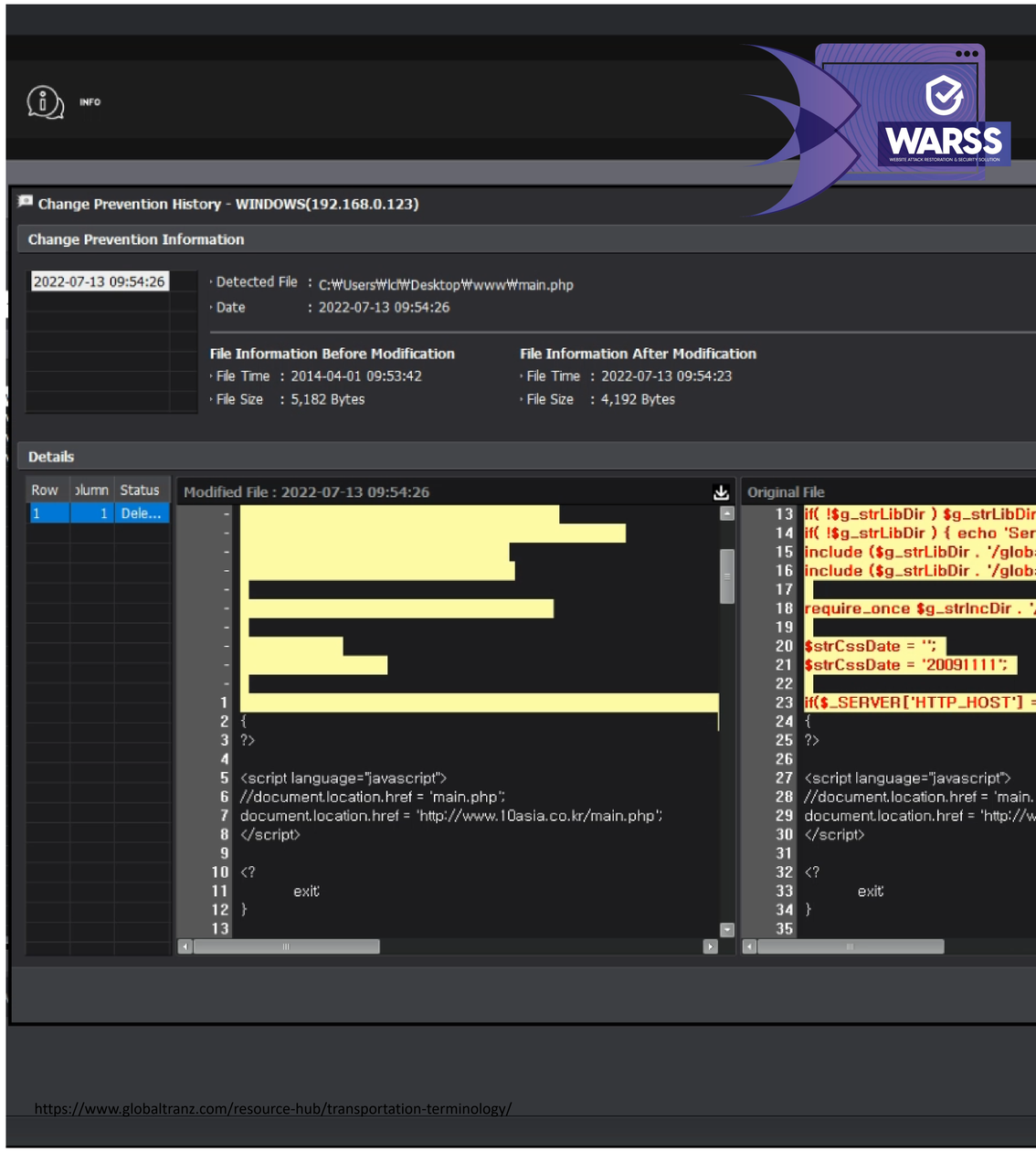
テストした他の偽造防止ソリューションと比較して、WARSSはソースコード、画像、およびビデオ偽造防止機能を提供する唯一のソリューションでした。

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



https://www.globaltranz.com/resource-hub/transportation-terminology/

顧客会社

대한민국 청와대

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

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

...そしてより多くの会社**!**

あ り が と う

UMV Inc.
韓国、ソウル

+82 2 448-3435
sales@umvglobal.com
www.umvglobal.com

付録

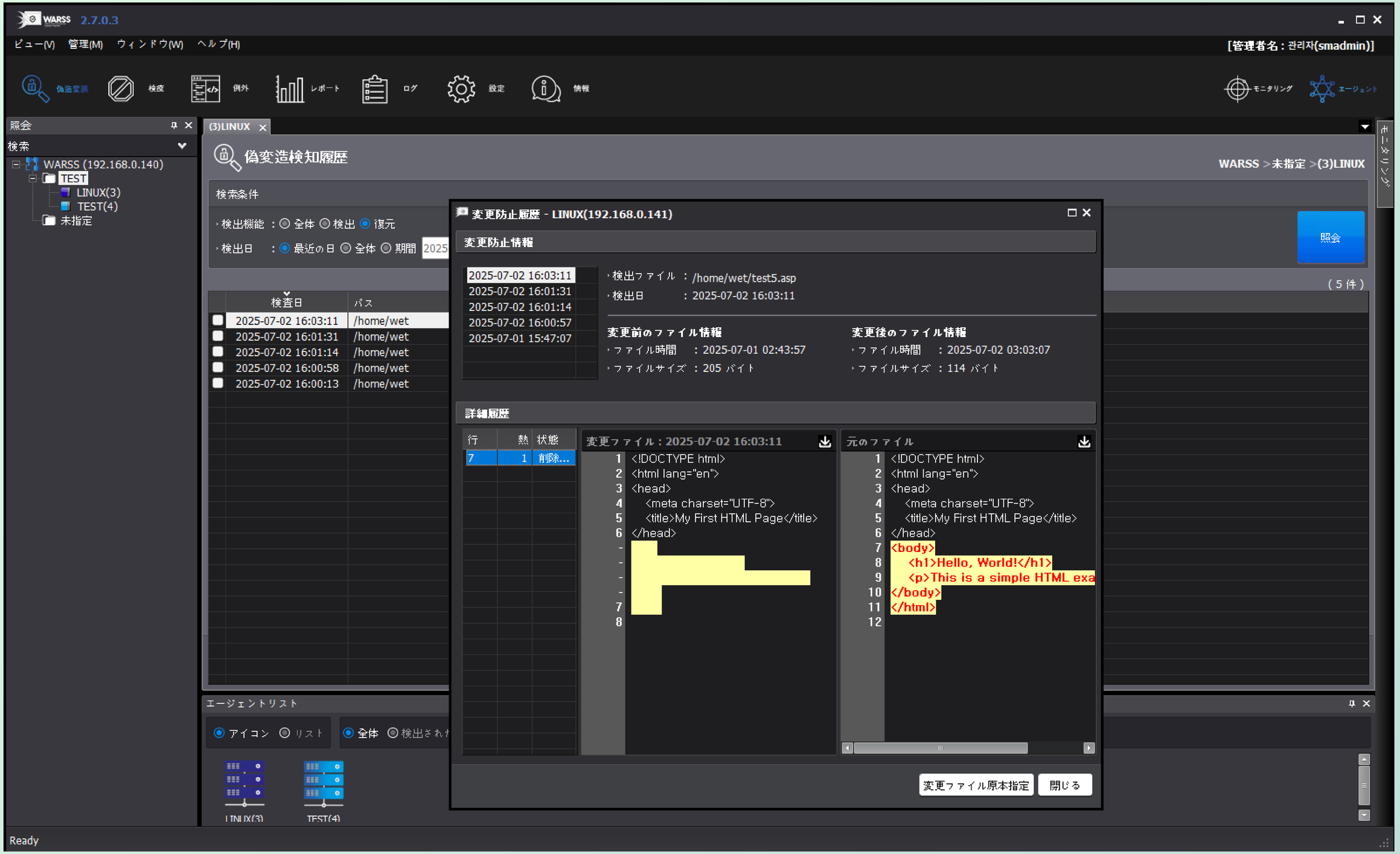
WARSS の機能

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



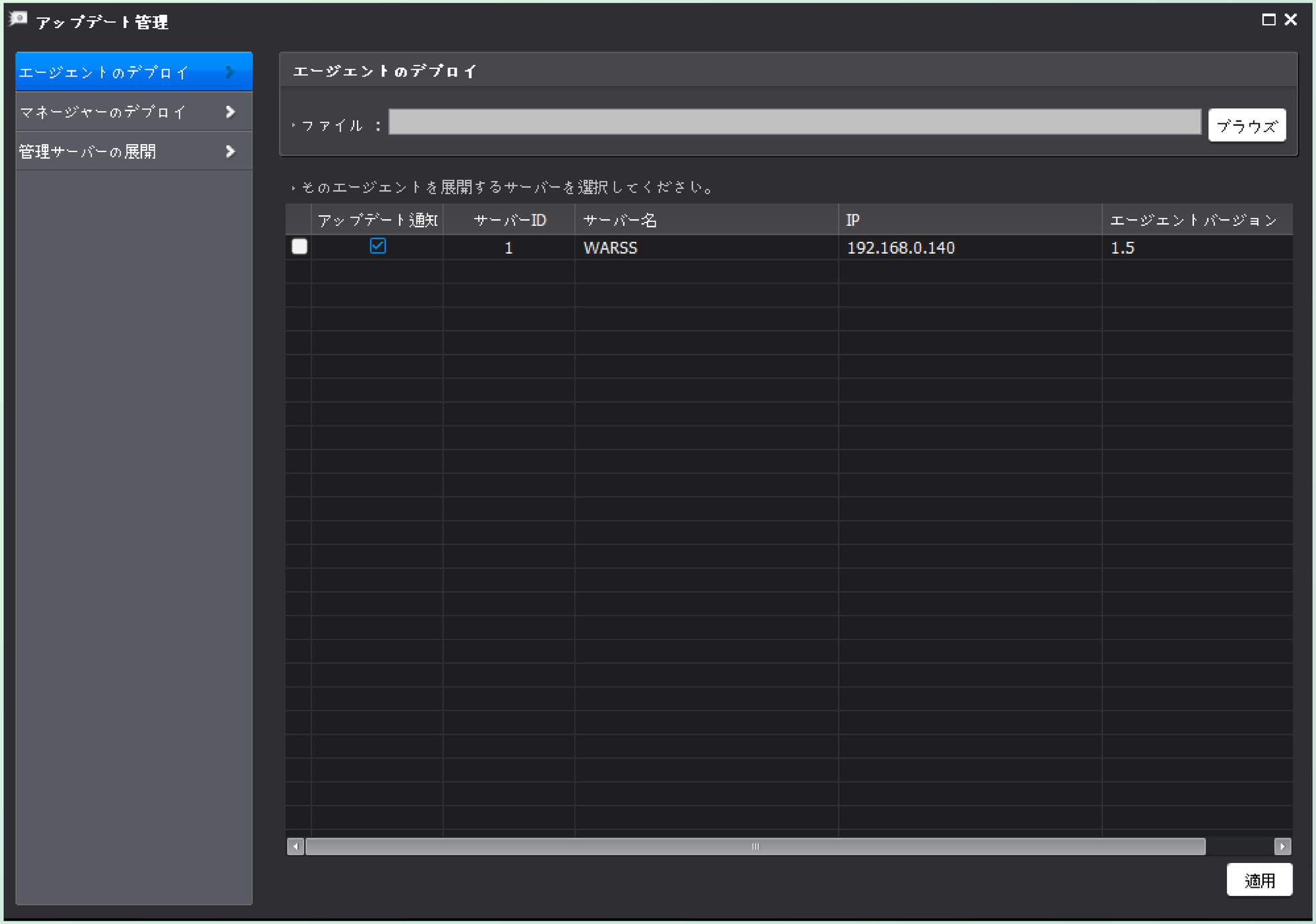
WARSS 機能

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	• アカウントとユーザー固有の権限の管理 • 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 • レポートと統計
安定性	• リソース使用制御 • サーバー環境に合わせたカスタマイズ
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	• 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 • 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

管理ビュー

更新管理


アップデート管理
エージェントのデプロイ
マネージャーのデプロイ
管理サーバーの展開
エージェントのデプロイ
ファイル：
ブラウズ
そのエージェントを展開するサーバーを選択してください。
アップデート通知
サーバーID
サーバー名
IP
エージェントバージョン
1
WARSS
192.168.0.140
1.5
適用

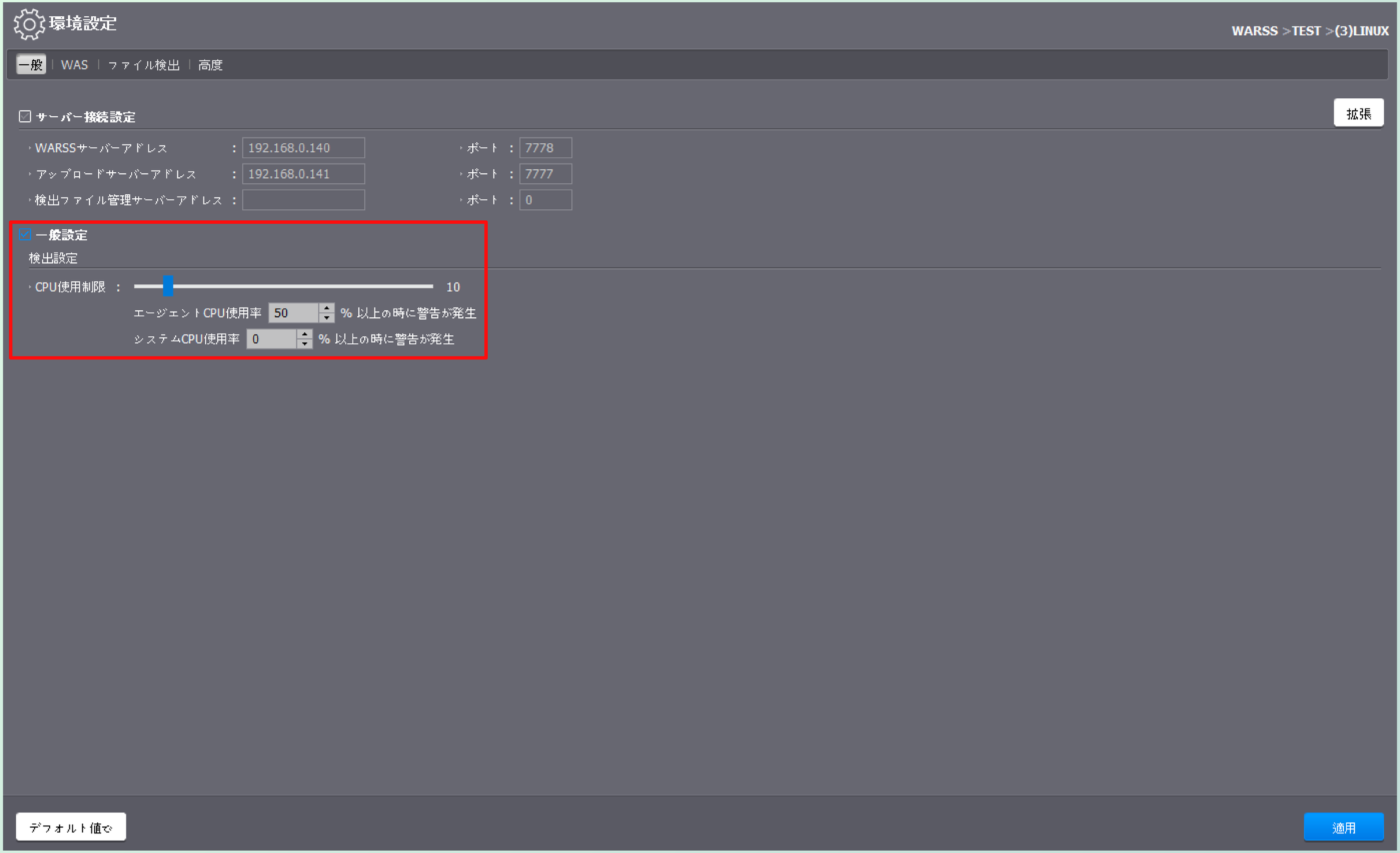
管理ビュー

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

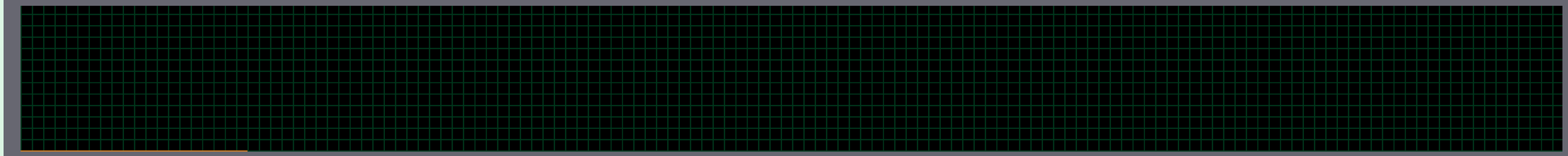
リソース ステータスの監視

情報

WARSS >TEST >(3)LINUX

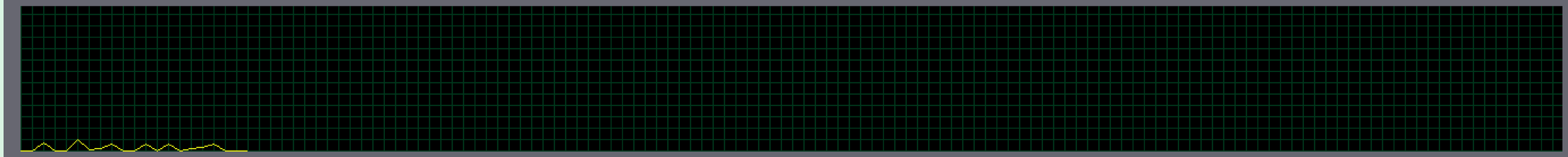
エージェント情報 | システム情報 | 資源状況

エージェントCPU使用率



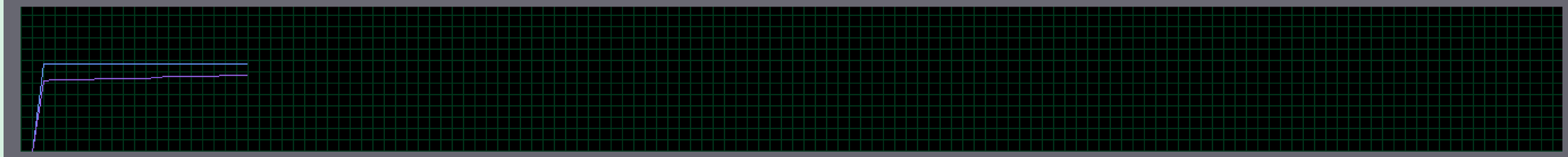
エージェントCPU使用率 ： **0.1%**

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

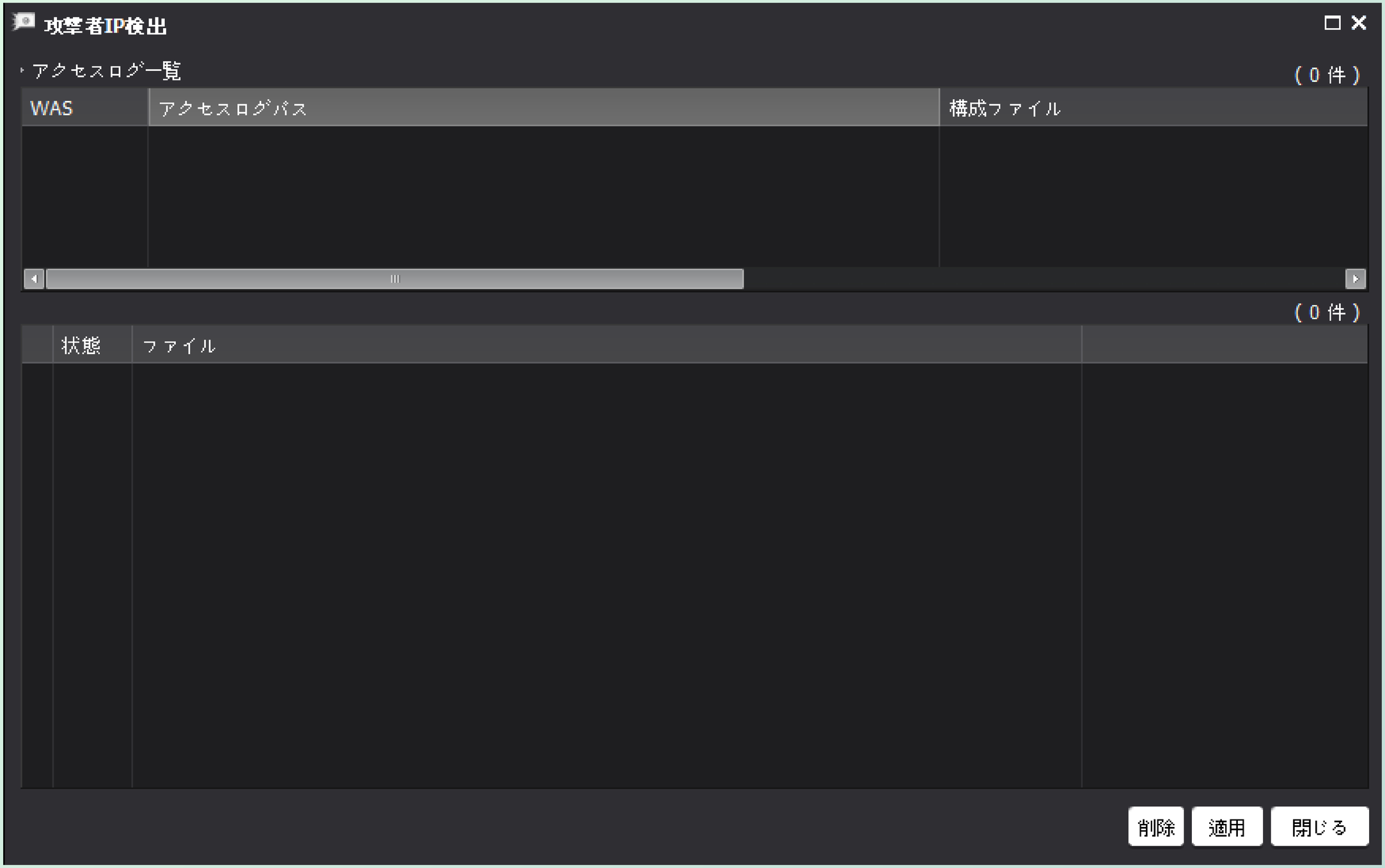
- 使用率 ： 53.4%
- 全体 ： 41.0MB
- 使用 ： 21.9MB
- 使用可能 ： 19.1MB

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



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

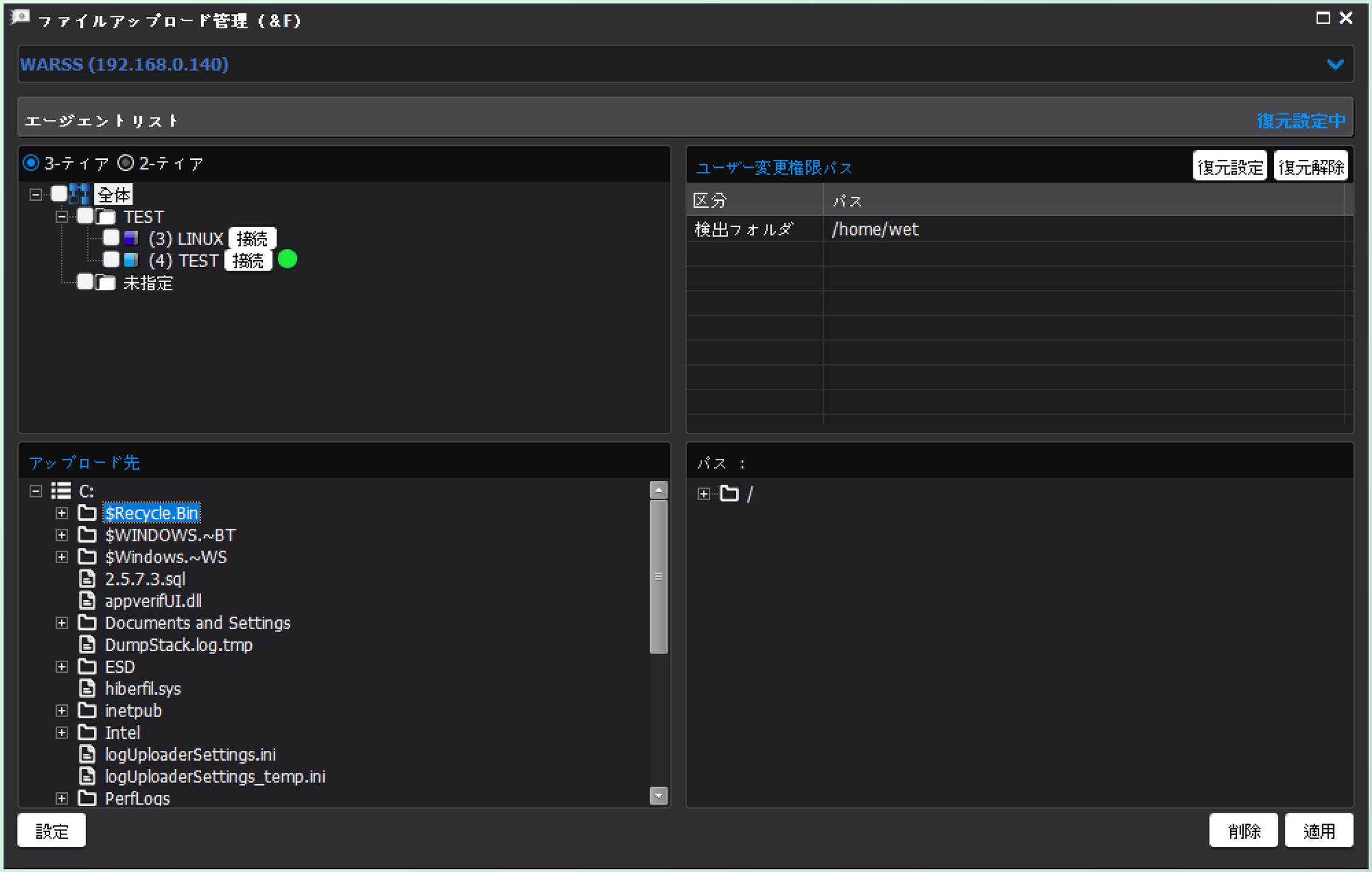
(1 件)

	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
	☑	/home/wet	含む	✓	✓	手動	☑	☑	☑	asp,aspx,asa,cer,cdx,hta,ascx,asax,ashx,soap,r...		

ディレクトリ設定 | WASディレクトリ | 削除

デフォルト値で | 偽造変調検出ディレクトリの設定 | 適用

管理ビュー
専用安全アップローダ



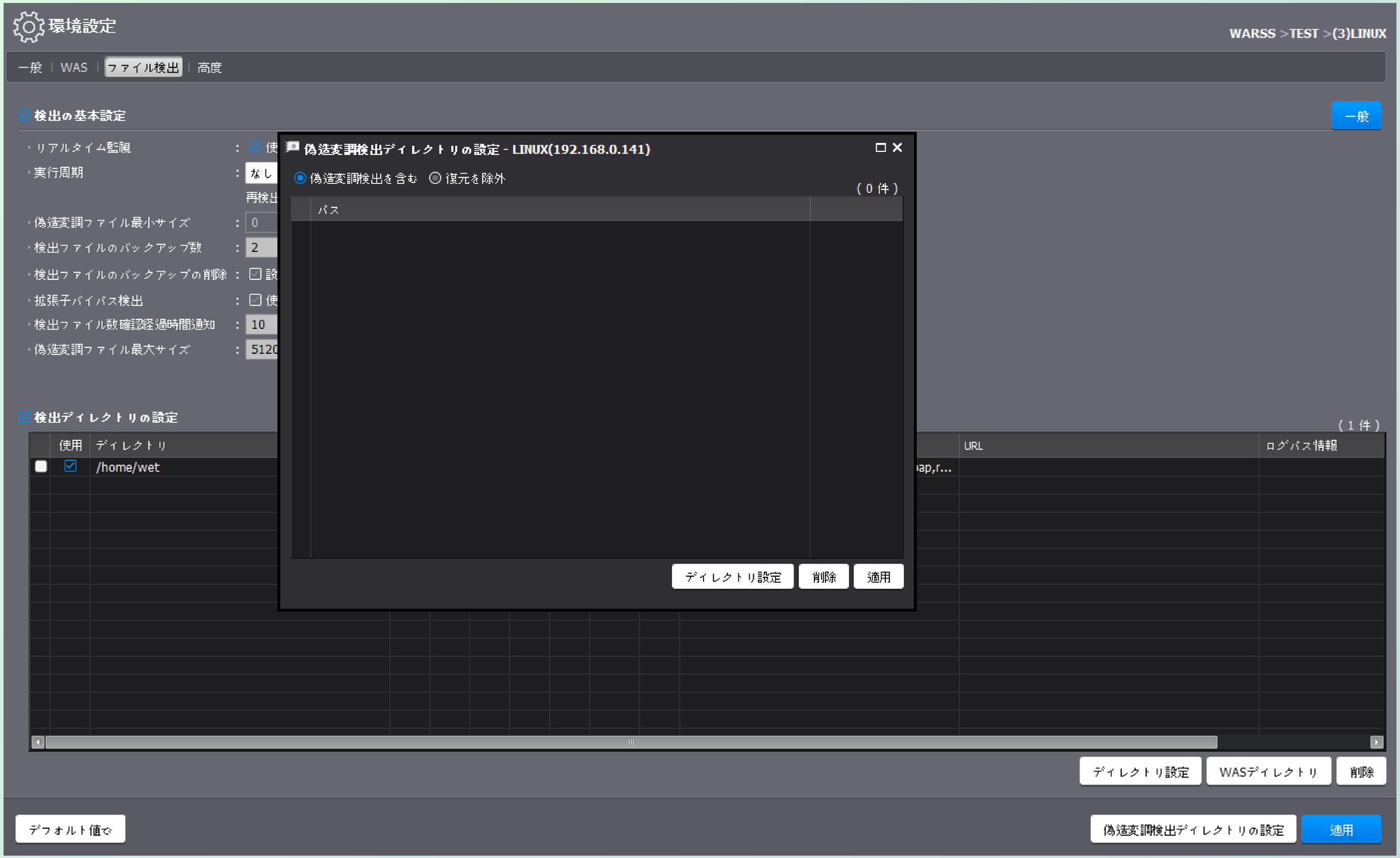
WARSS 機能

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	• 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 • 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
ホーム ディレクトリ検索	• 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 • ホーム ディレクトリの追加/変更履歴の表示
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

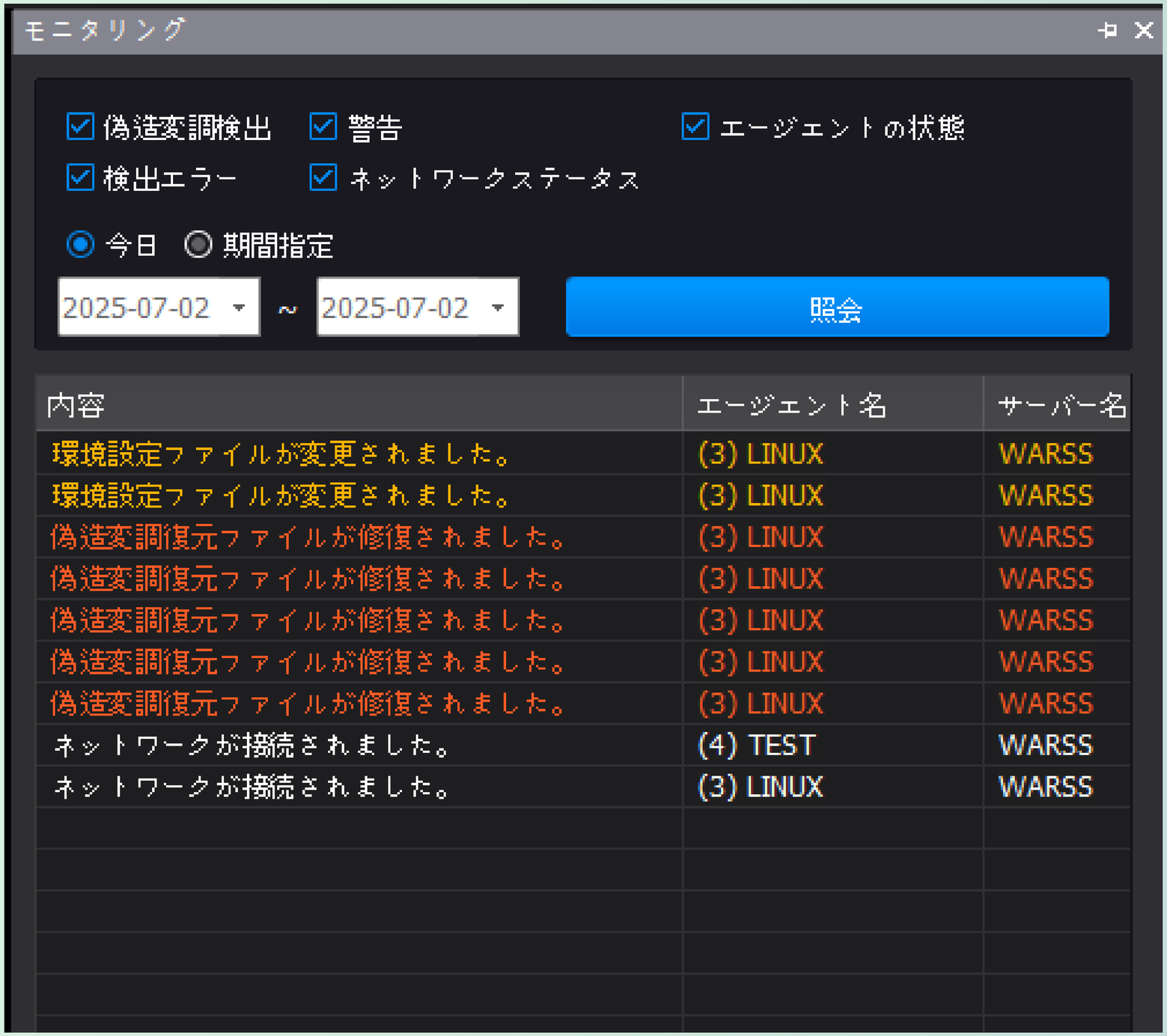
クラウド設定ビュー

ホームディレクトリ検索



クラウド設定ビュー

ログ記録/履歴管理



WARSS オンプレミス構成図