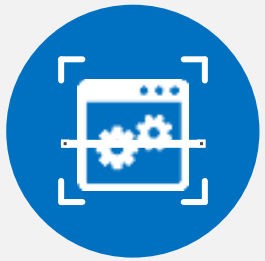
# FFRI yarai バージョン3.4 新機能のご紹介

Ver2.00.02

# 検知精度の向上

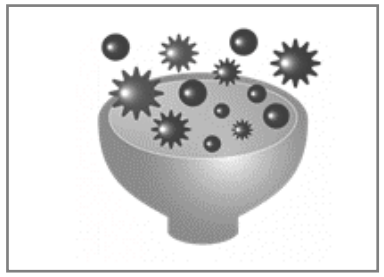
# 検出精度の向上 1



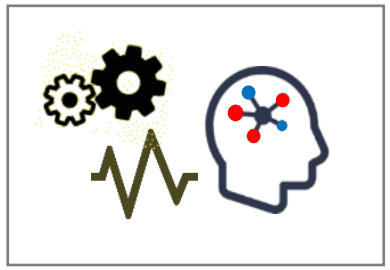
Static分析
エンジン

## Static機械学習機能を搭載

ＦＦＲＩセキュリティが独自に収集したマルウェア及び正常系ソフトウェアのデータから学習した特徴をもとに静的にファイル構造を解析



マルウェア及び正常系
ソフトウェアのデータ
を解析システムに投入



ファイル構造特性や
振る舞いの特性を抽出

Static分析
エンジン

**Static機械学習機能　New！**

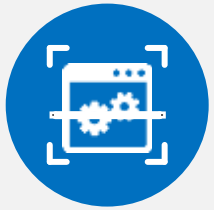
機械学習から得た統計的な特徴データによるファイル構造の解析

機械学習
エンジン

機械学習から得た統計的な特徴データによる挙動の監視

**独自の機械学習を静的解析・動的監視 両方に反映**

# 検出精度の向上 2



Static分析
エンジン

HIPS
エンジン

## ATT&CK Matrix 対応

MITRE社が提唱するセキュリティフレームワークATT&CK Matrixのカバレッジを強化

ATT&CK Matrix for Enterprise の「Tactics」12カテゴリー

Initial Access(初期アクセス)　Execution(実行)　Persistence(永続化)
Privilege Escalation(権限昇格)　Defense Evasion(防衛回避)　Credential Access(認証情報アクセス)
Discovery(探索)　Lateral Movement(横展開)　Collection(収集)
Exfiltration(持ち出し)　Command and Control(指令＆制御)　Impact(影響)

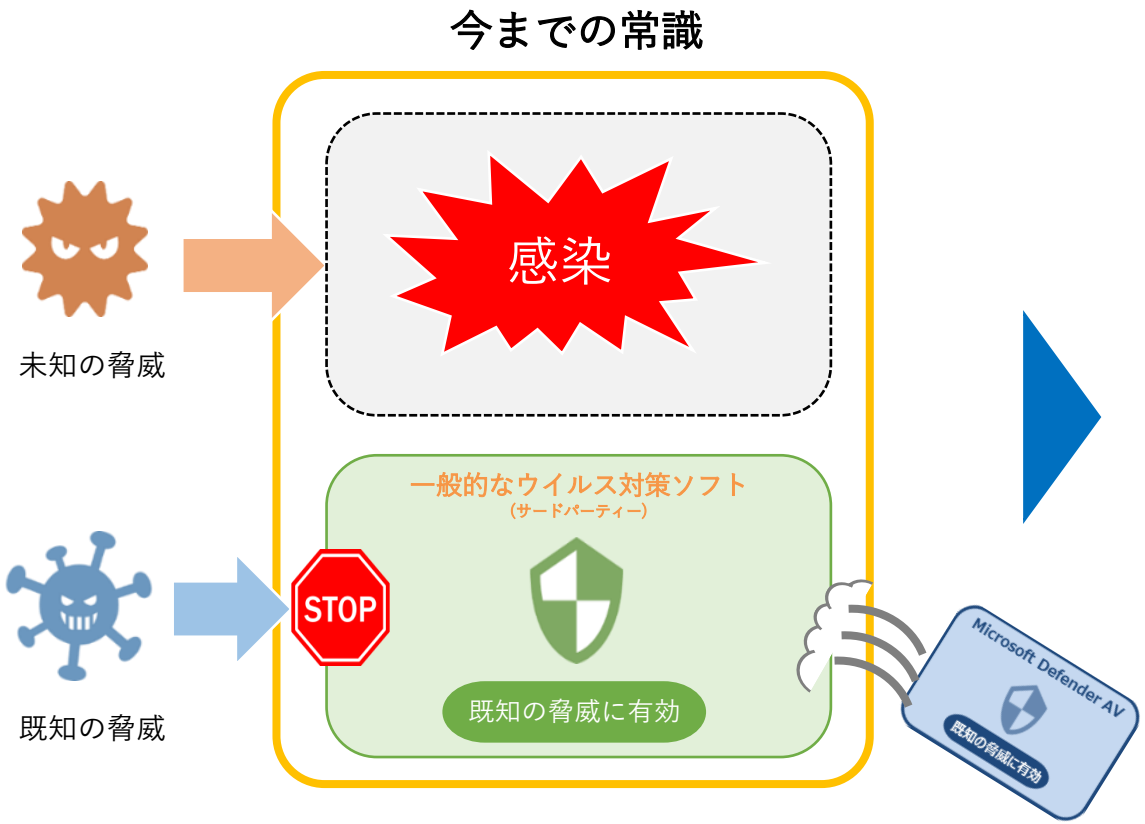
※ 出典：https://attack.mitre.org/　https://www.socyeti.jp/posts/4873582/

**ATT&CK Matrix「Tactics」の12カテゴリー全てをカバー**

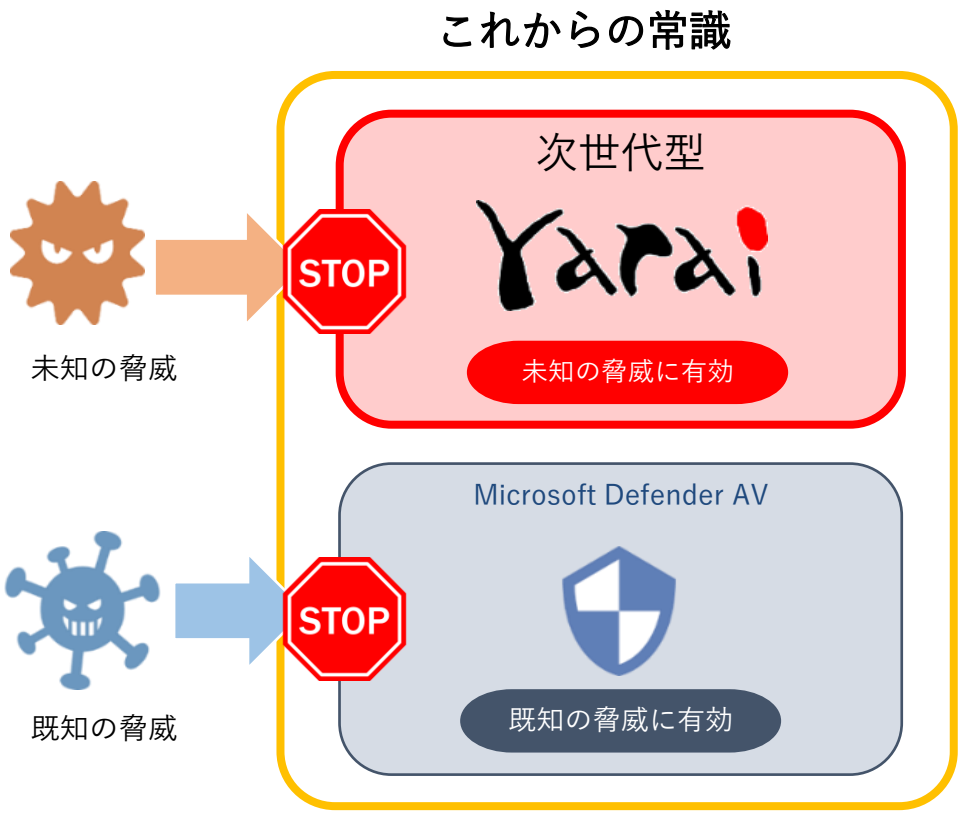
※各カテゴリーにおいて、「Technique」のいずれかをカバー

# Microsoft Defender連携機能強化

# 一般的なウイルス対策ソフトとの組み合わせ運用




Microsoft Defender AVではなく市販のウイルス対策ソフトに
置き換えても防御範囲は同じなため
未知の脅威は防げず、更新料も必要




市販のウイルス対策ソフトと検知力の変わらない
Microsoft Defender AVとFFRI yaraiを
導入することで既知・未知の脅威を防御

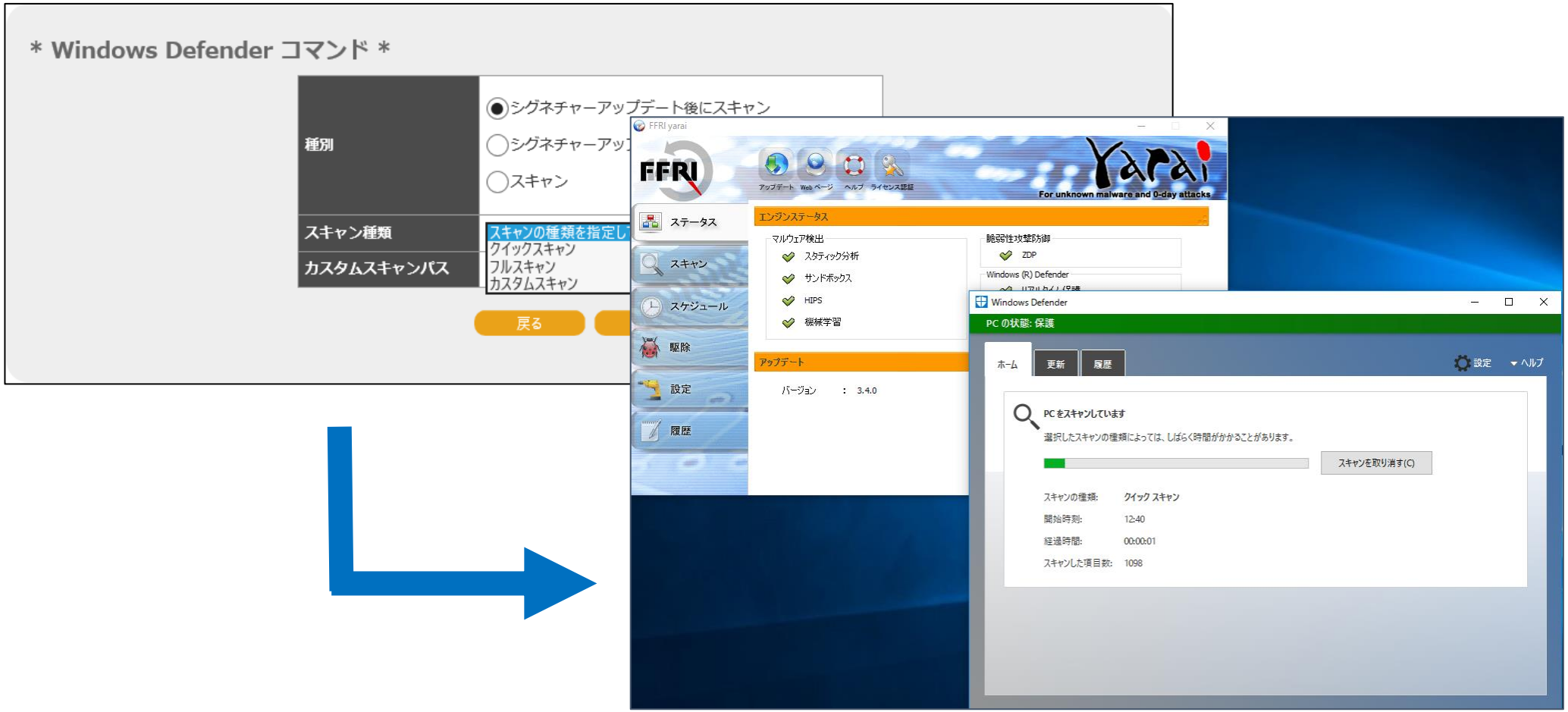
**既存対策と組み合わせることで未知の脅威への防御力が大幅に向上します！**

# Microsoft Defender 連携強化

FFRI AMCより Microsoft Defender の動作状況の確認、
スキャンや例外リストの配布、シグネチャ更新を実施

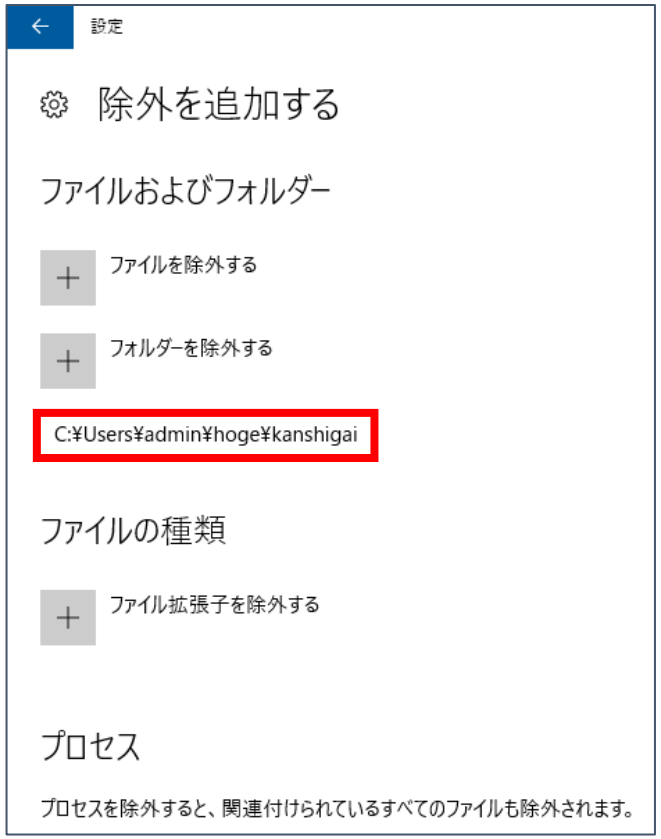
**Microsoft Defender 運用にかかる 負荷やコストを軽減**

# Microsoft Defender配布イメージ




**FFRI AMCからシグネチャアップデートやスキャンの配布が可能**

# Microsoft Defender除外リスト連携



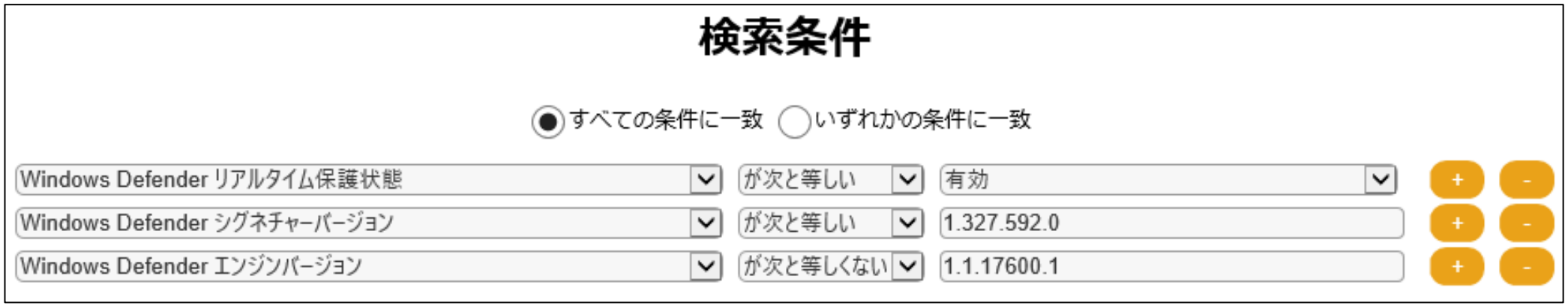

**FFRI AMCからMicrosoft Defender除外リストの配布も可能**

# Microsoft Defenderイベント監視

| イベントタイプ | プロセス名 | 検出機構 | 詳細 |
|---|---|---|---|
| スキャン完了 | クイックスキャン | Windows Defender | 詳細情報 |
| スキャン完了 | クイックスキャン | Windows Defender | 詳細情報 |
| スキャン完了 | クイックスキャン | Windows Defender | 詳細情報 |
| 駆除成功 | C:¥Users¥[redacted]¥eicar.exe | Windows Defender | 詳細情報 |
| シグネチャーアップデート | 1.327.592.0 | Windows Defender | 詳細情報 |
| シグネチャーアップデート | 1.327.592.0 | Windows Defender | 詳細情報 |
| 保護操作完了 | C:¥Users¥admin¥[redacted]Test.exe | Windows Defender | 不審なファイルが検疫されました。(Trojan:Win32/Dynamer!ac) |
| マルウェアを検出しました | C:¥Users¥admin¥[redacted]Test.exe | Windows Defender | 不審なファイルが検出されました。(Trojan:Win32/Dynamer!ac) |
| マルウェアを検出しました | C:¥Users¥admin¥[redacted]Test.exe | Windows Defender | 不審なファイルが検出されました。(Trojan:Win32/Dynamer!ac) |

**Microsoft Defenderのイベント監視も可能**

# Microsoft Defenderクライアント管理画面




| Windows Defender リアルタイム保護状態 | Windows Defender シグネチャーバージョン | Windows Defender シグネチャーの最終更新日時 | Windows Defender エンジンバージョン | Windows Defender スキャン最終終了日時 | Windows Defender スキャン最終種類 | Windows Defender 除外リスト | Windows Defender オンデマンドスキャン実施結果 | Windows Defende オンデマンドスキャン実施結果 |
|---|---|---|---|---|---|---|---|---|
| 有効 | 1.327.592.0 | 2020-11-09 12:29:49 | 1.1.17600.5 | 2020-11-13 12:40:32 | クイックスキャン | あり | 正常 | 2020-11-09 14:30: |

**Microsoft Defenderの管理状況の確認や複数条件による検索も可能**

# EDR機能追加（STIX/TAXII対応）

# EDR機能の機能追加（STIX/TAXII対応）

## 脅威情報インポート/自動検索機能追加

STIX/TAXII にて取り込んだ脅威を自動検索する機能を追加

| FFRI yarai 3.4 EDR機能拡張内容 |
| --- |
| TAXII（Ver.1.1）と、それに準拠したバージョンのSTIX形式の脅威情報の取り込み機能（STIXはVer.1.0系/1.1系を検証済み） |
| 取り込んだ脅威情報の自動検索機能 |
| 検出した端末の自動ネットワーク隔離機能（※） |
| 検出アラートのSyslog（CEF形式に対応）出力機能 |

※EDR機能以外で検出した場合は自動隔離対象外

**脅威情報のインポート自動検索機能を追加し脅威検索の自動化を実現**

# STIX/TAXII連携運用イメージ

・配信する脅威情報（STIX）の生成
・作成した脅威情報に関する問い合わせ窓口

TAXII/STIX サーバー

※ファイルサーバーへの
アップロードは 別ツールを提供

ファイル サーバー

レポート
（pdf）

検出アラートの
Syslog 出力

脅威情報
ソース

STIX

管理コンソール
（FFRI AMC）

ハッシュの検索

クライアントPC
（FFRI yarai）

システム管理者

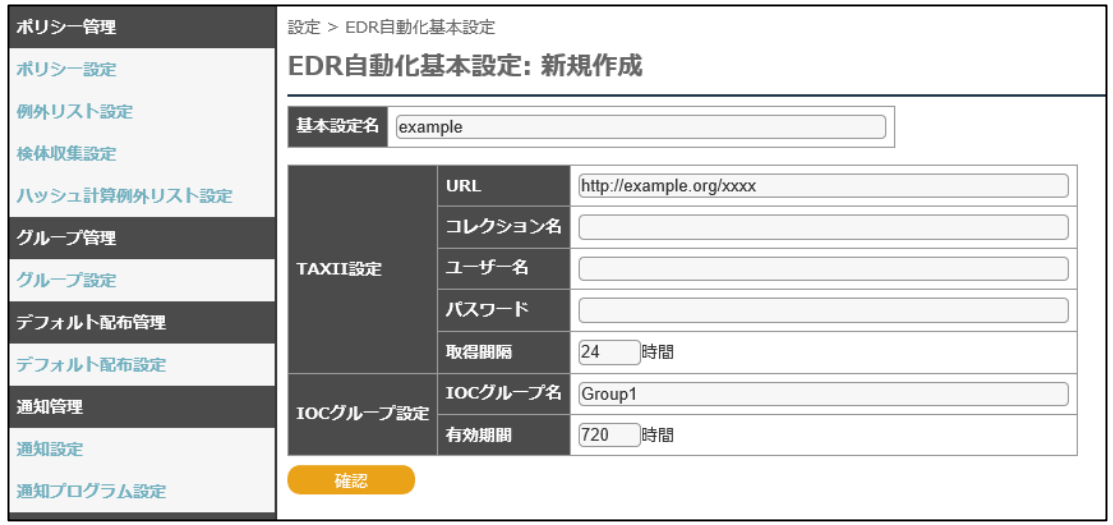
省庁/独法等

配信された脅威情報に対する
検索結果のみ
フィードバックします。

※図は当社の想定イメージです

# 脅威情報インポート/自動検索機能 画面イメージ

## 自動取得設定画面




## レポート