

Connected Threat Defense 連携動作確認ガイド(IMSVA)

トレンドマイクロ株式会社



TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScan Web Manager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro Mobile Security、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro InterScan Web Manager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンアップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おまかせバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンアップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Airサポート、Connected Threat Defense、フライトフリーザー、Trend Micro Policy Manager、メールダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、およびTrend Micro Policy-based Security Orchestrationは、トレンドマイクロ株式会社の登録商標です。

Copyright © 2018 Trend Micro Incorporated. All rights reserved.

製品名の表記について

本ドキュメントにおいては製品名等は以下のように表記します。

- Connected Threat Defense ... 「CTD」
- Trend Micro Deep Discovery Analyzer ... 「DDAN」
- Trend Micro Control Manager ... 「TMCM」
- InterScan Messaging Security Virtual Appliance ... 「IMSVA」
- Smart Protection Server ... 「SPS」
- Trend Micro Deep Discovery Inspector ... 「DDI」
- 不審オブジェクト[Suspicious Object] ... 「SO」

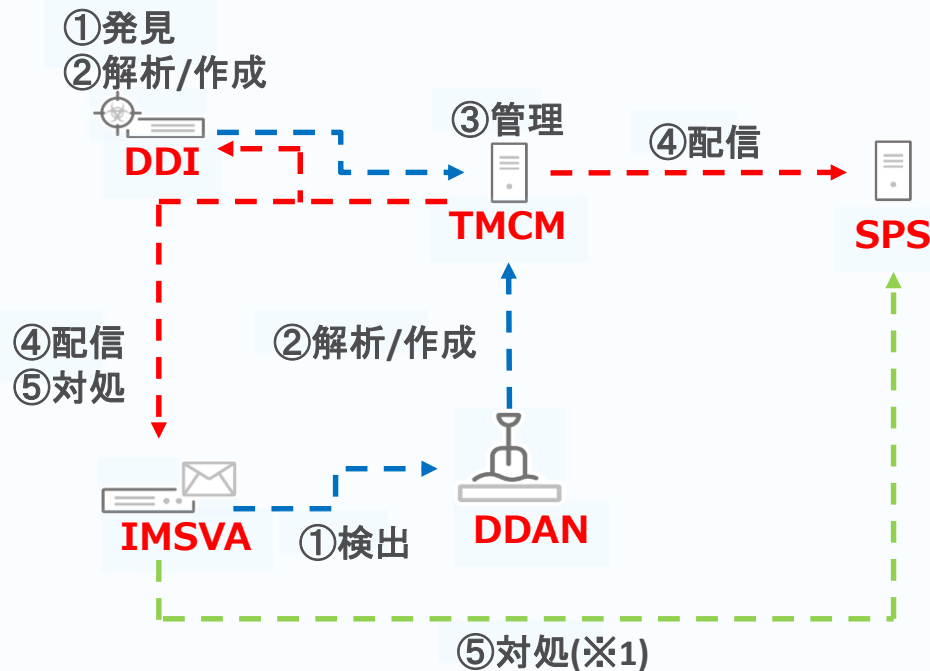
本ドキュメントの目的

本ドキュメントはIMSVAを中心としたCTDの設定に特化した資料となります。

CTDの製品間連携の設定後、その設定が正常に機能しているかのテスト方法について記載しています。

また、各テストに利用してるサンプルの検体の提供については担当営業またはエンジニアへお問い合わせください。

連携構成図



※1 不審オブジェクト(URL)の検出には、統合SPSまたはスタンドアロンSPSを参照します。

※2 DDIは必須コンポーネントで無いため、利用されていない環境では以降の設定は割愛ください。

目次

STEP1 IMSVA-DDAN連携で検出する	P6-P13
STEP2 SOを使いIMSVAで隔離する	P14-P22
STEP3 DDIで生成したSOを使いIMSVAで隔離する	P23-P32
STEP4 SPSと連携し URL SOをIMSVAで隔離する	P33-P37

STEP1 IMSVA-DDAN連携で検出する


STEP1-1 ATSEを有効にする

1. IMSVAのWEBコンソールへアクセスする
[https://\[IMSSVA IP or FQDN\]:8445/console.imss](https://[IMSSVA IP or FQDN]:8445/console.imss)
2. ログインします
3. [ポリシー] – [検索エンジン] をクリックします
4. 以下のパラメータを入力し、保存をクリックします

チェックする

ウイルス検索エンジン

高度な脅威検索エンジン

☒ 高度な脅威検索エンジンを有効にする 

注意: 潜在的な脅威を含むメッセージは、仮想アナライザに送信して詳しく分析することをお勧めします。仮想アナライザは個別にライセンスを取得してアクティベートする必要がある製品です。仮想アナライザを設定するには、[管理]→[IMSSVA設定]→[仮想アナライザの設定] の順に選択します。

保存

キャンセル

STEP1-2 DDANに送信するポリシーを作成する

1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)

2. ログインします

3. [ポリシー] – [ポリシーリスト] をクリックします

4. [追加 > その他] をクリックします

5. [送信者]、[受信者] を設定し、次へ をクリックします。

6. 実ファイルタイプ のチェックボックスをチェックします。

7. 実ファイルタイプ をクリックします。

STEP1-2 DDANに送信するポリシーを作成する

8. 以下のパラメータを入力し、保存をクリックします。

新規ルール > 添付ファイルの実際のファイルタイプ

保存

キャンセル

チェックする

実際のファイルタイプの選択

選択: 選択された添付ファイルタイプ ▼

☒ 実行可能ファイル▼

☐ 文書▼

☐ 画像▼

☐ メディア▼

☐ 圧縮ファイル▼

☐ Microsoft Windowsのショートカット

仮想アライザの検索

☒ ファイルを仮想アライザに送信 ⓘ

保存

キャンセル

チェックする

STEP1-2 DDANに送信するポリシーを作成する

9. 次へ をクリックします
10. 次の場所に隔離 を選択します
11. 次へをクリックします
12. 右のパラメータを入力し、完了を
クリックします。

チェックする

ポリシーの参照順序を入力します。
※今回はウイルス検索ルール
の後にDDANへ送信するように
2を設定します。

ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> 手順3 >>> 手順4: 名前と順序

< 戻る 完了 キャンセル

ルール 備考

☒ 有効

ルール名:

順序番号:

順序	既存のルール	処理	変更日	ステータス
	グローバルDKIM適用ルール	隔離	2018/06/11	✖
1	グローバルウイルス対策ルール	トレンドマイクロの推奨処理	2018/06/11	✔
2	初期設定のスパムメール対策ルール	隔離	2018/06/11	✔
3	復号化できないメッセージの初期設定ルール	隔離...	2018/06/11	✔
4	パスワードで保護された添付ファイルの初期設定ルール	スタンプ	2018/06/11	✔
5	コンプライアンスー医療情報	隔離...	2018/06/11	✖
6	コンプライアンスー金融および銀行取引	隔離...	2018/06/11	✖
7	コンプライアンスー個人識別番号	隔離...	2018/06/11	✖
8	コンプライアンスークレジットカード名義人情報	隔離...	2018/06/11	✖

受信者と送信者

受信
宛先 すべてのユーザ
および
差出人 すべてのユーザ

検索条件
添付ファイルの実際のファイルタイプが ...

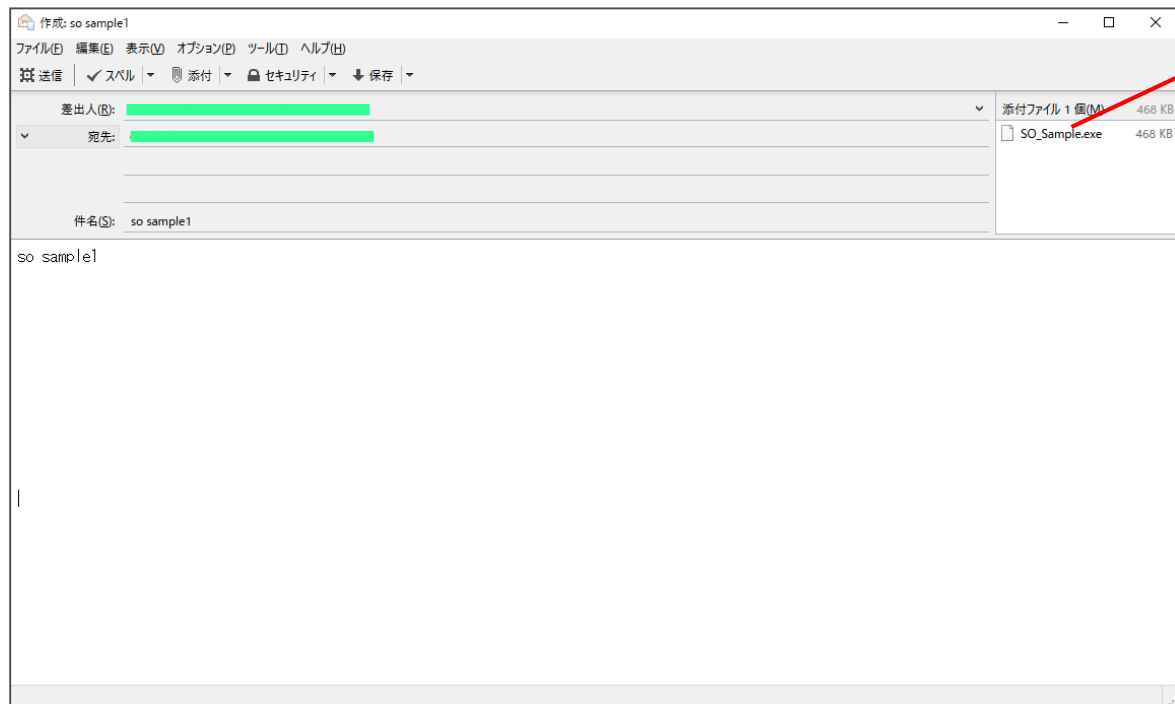
処理
メッセージを隔離

< 戻る 完了 キャンセル

ルール名を入力する(任意)

STEP1-3 DDANと連携して隔離する

1. Sample SOファイルを添付してメールをIMSVaへ送信します



添付する

STEP1-3 DDANと連携して隔離する

2. IMSVAのWEBコンソールへアクセスします

[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)

3. ログインします

4. [ログ] – [ログクエリ] をクリックします

5. [種類] > 隔離イベント を選択します

6. 日付範囲を調整し、ルールにStep1-2で設定したルール名を入力後、
ログ表示をクリックします

STEP1-3 DDANと連携して隔離する

ログクエリ

基準

種類: 隔離イベント

日付: 2018/06/14 10 ~ 2018/06/15 14
年月日 (yyyy/mm/dd) 時 (hh) 年月日 (yyyy/mm/dd) 時 (hh)

ルール: ddan-submit

[ルール] フィールドで、検索項目の区切りにはセミコロンを使用します。
完全一致で検索するには、キーワードを入力します。部分一致で検索するには、アスタリスク(*)を使用します。たとえば、「*username」を指定すると、「username」で終わるすべての文字列が一致します。

ログ表示

隔離イベント

1ページあたりの結果数: 15

現在のページを印刷 CSV形式にエクスポート

1-1 / 1

結果 2018/06/15 10:37:51

ルール	隔離	隔離解除	隔離解除の割合
ddan-submit	1	0	0.00

STEP2 SOを使いIMSVAで隔離する

STEP2-1 DDAN上のSO生成を確認します

0. STEP1が正しく出来ていることが前提条件です。

1. DDANのWEBコンソールへアクセスします

[https://\[DDAN IP or FQDN\]/pages/login.php](https://[DDAN IP or FQDN]/pages/login.php)

2. ログインします

3. [仮想アナライザ] - [不審オブジェクト] をクリックします

4. 以下のようにSOが生成されていることを確認します

後の隔離テストではこちらを利用します

前回の検出	▲ 失効日	リスクレベル	種類	オブジェクト	最新の関連サンプル
2018年06月15日 10:20:01	2018年07月15日 10:19:57	高	ファイル	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3
2018年06月15日 10:20:01	2018年07月15日 10:19:57	高	URL	http://ms21.winshipway.com:80/	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3
2018年06月15日 10:20:01	2018年07月15日 10:19:57	高	ドメイン	ms21.winshipway.com	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3
2018年06月15日 10:20:01	2018年07月15日 10:19:57	中	ドメイン	ms74.winshipway.com	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3
2018年06月15日 10:20:01	2018年07月15日 10:19:57	高	IPアドレス	159.78.102.115:80	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3

STEP2-2 TMCM上でSOの同期を確認します

1. TMCMのWEBコンソールへアクセスする

[https://\[TMCM IP or FQDN\]/webapp/login.aspx](https://[TMCM IP or FQDN]/webapp/login.aspx)

2. ログインします

3. [運用管理] – [不審オブジェクト] – [仮想アナライザオブジェクト]をクリックします

4. 以下のようにSOがDDANから同期されていることを確認します

すべてをエクスポート

除外リストに追加

期限なし

今すぐ期限切れにする

処理を設定

影響の診断

<input type="checkbox"/>	オブジェクト	リスクレベル	種類	有効期限	危険性の高いエンドポイント	検出時の処理	処理プロセス
<input type="checkbox"/>	1FB5AF2228410D2F824CB87E174EE7A890CBC3	高	ファイル	2018/07/15 10:19:57	まだ診断されていません	ログ	表示
<input type="checkbox"/>	http://lure21.winchinsaw.com:80/	高	URL	2018/07/15 10:19:57	まだ診断されていません	ログ	表示
<input type="checkbox"/>		高	ドメイン	2018/07/15 10:19:57	まだ診断されていません	なし	表示
<input type="checkbox"/>		中	ドメイン	2018/07/15 10:19:57	まだ診断されていません	なし	表示
<input type="checkbox"/>		高	IPアドレス	2018/07/15 10:19:57	まだ診断されていません	ログ	表示

STEP2-3 TMCM上でSOの検出時の処理を変更します

1. 以下の画面のように対象SOをチェックし、「処理を設定」をクリックします

すべてエクスポート

除外リストに追加

期限なし

今すぐ期限切れにする

処理を設定

影響の診断

<input type="checkbox"/>	オブジェクト	リスクレベル	種類	有効期限 ▼	危険性の高いエンドポイント	検出時の処理	処理プロセス
<input checked="" type="checkbox"/>	▶ 1FB5AF2228410D2F824CB2B87E174EE7A890CBC3	高	ファイル	2018/07/15 10:19:57	まだ診断されていません	ログ	表示
<input type="checkbox"/>	▶ [redacted]	高	URL	2018/07/15 10:19:57	まだ診断されていません	ログ	表示
<input type="checkbox"/>	[redacted]	高	ドメイン	2018/07/15 10:19:57	まだ診断されていません	なし	表示
<input type="checkbox"/>	[redacted]	中	ドメイン	2018/07/15 10:19:57	まだ診断されていません	なし	表示
<input type="checkbox"/>	▶ [redacted]	高	IPアドレス	2018/07/15 10:19:57	まだ診断されていません	ログ	表示

2. 以下の画面のようにブロックに設定し、適用をクリックします

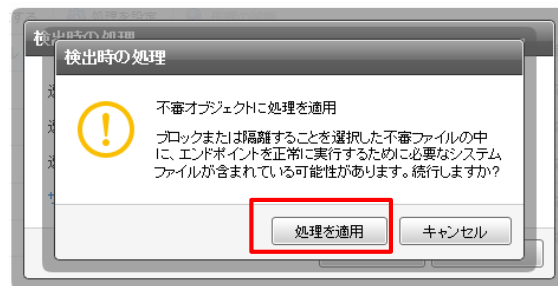


※ご注意！

ログ : IMSVA上で「隔離」せず、「放置」します
ブロック: IMSVA上で「隔離」します

STEP2-3 TMCM上でSOの検出時の処理を変更します

3. 以下の画面の処理を適用をクリックします



4. 以下の画面のようにブロックとなっていることを確認します

<input type="checkbox"/>	オブジェクト	リスクレベル	種類	有効期限 ▼	危険性の高いエンドポイント	検出時の処理	処理プロセス
<input type="checkbox"/>	▷ 1FB5AF2228410D2F824CB2B87E174EE7A890CBC3	高	ファイル	2018/07/15 10:19:57	まだ診断されていません	ブロック	表示
<input type="checkbox"/>	▷ [REDACTED]	高	URL	2018/07/15 10:19:57	まだ診断されていません	ログ	表示
<input type="checkbox"/>	▷ [REDACTED]	高	ドメイン	2018/07/15 10:19:57	まだ診断されていません	なし	表示
<input type="checkbox"/>	▷ [REDACTED]	中	ドメイン	2018/07/15 10:19:57	まだ診断されていません	なし	表示
<input type="checkbox"/>	▷ [REDACTED]	高	IPアドレス	2018/07/15 10:19:57	まだ診断されていません	ログ	表示

STEP2-4 IMSVAへSOが同期されたことを確認します

1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSSVA IP or FQDN\]:8445/console.imss](https://[IMSSVA IP or FQDN]:8445/console.imss)

2. ログインします

3. [管理] - [IMSSVA設定] - [接続] - [Control Managerサーバ]をクリックします

4. 以下の同期時刻を確認します

不審オブジェクトリストの設定

☒ 不審ファイルリスト ⓘ

同期間隔: 分

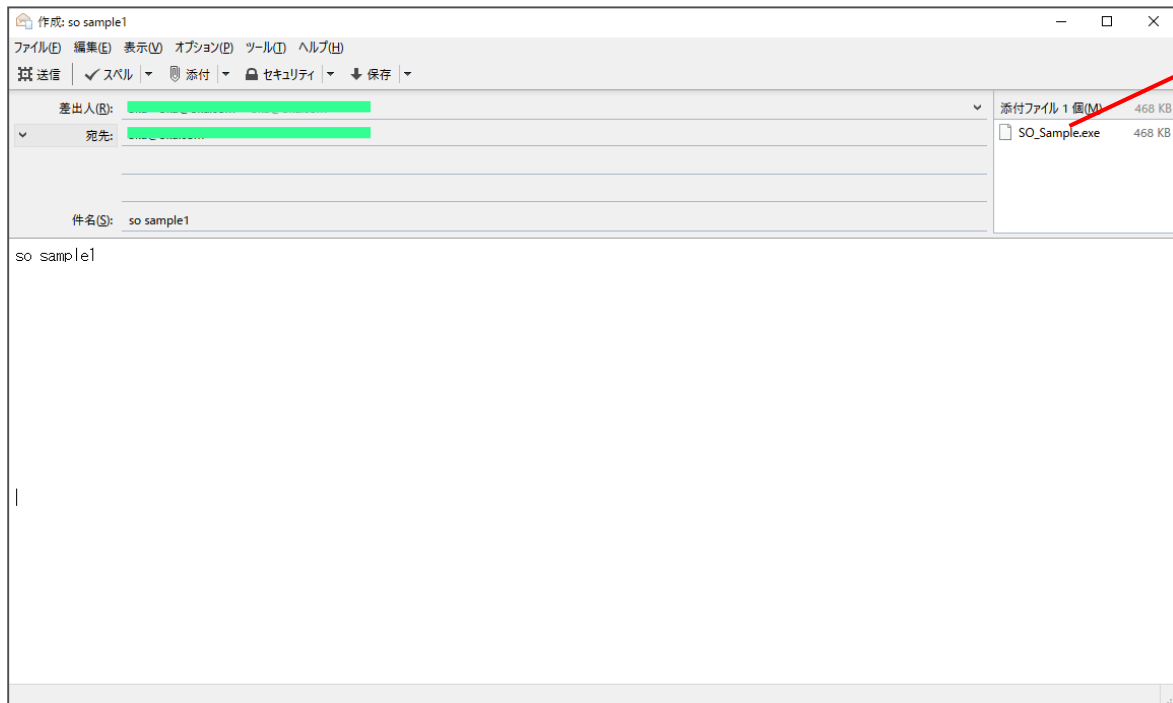
前回の同期:

2018/06/15 14:57:03

STEP1-3の設定完了後、この時刻が更新されるまでお待ちください

STEP2-5 IMSVAでメールを隔離します

1. Sample SOファイルを添付してメールをIMSVAへ送信します



添付する

STEP2-5 IMSVAでメールを隔離します

1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)

2. ログインします

3. [ログ] – [ログクエリ] をクリックします

4. [種類] > ポリシーイベント を選択します

5. 日付を調整し、ログ表示をクリックします

STEP2-5 IMSVAでメールを隔離します

7. 以下のように隔離されていることを確認します

ログクエリ

基準

種類: ポリシーイベント すべて

日付: 2018/06/15 14:08 ~ 2018/06/15 15:08
年月日 (yyyy/mm/dd) 時 (hh) 分 (mm)

送信者: 件名: 違反する添付ファイル: メッセージID:

受信者: 完全一致で検索するには、キーワードを入力します。部分一致で検索するには、アスタリスク(*)を使用します。たとえば、「*username」を指定すると、「username」で終わるすべての文字列が一致します。

ルール:

ログ表示

ポリシーイベント 1ページあたりの結果数: 15

現在のページを印刷 CSV形式にエクスポート 1-1 / 1

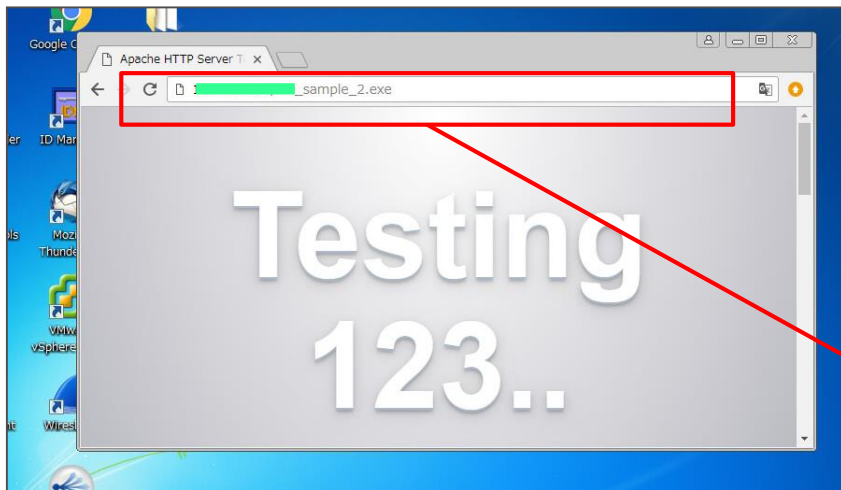
日時	処理	ルール	メッセージID
2018/06/15 15:04:41	隔離	TMCM_不審ファイルの検出	8.....13013c7279 4.....

TMCM_不審ファイル検出
ルールで隔離されている
ことを確認

STEP3 DDIで生成したSOを使い IMSVAで隔離する

STEP3-1 DDIでSOを生成する

1. DDI監視下のPCでSample SO2ファイルをキャプチャします



ブラウザ経由でSample
SO2ファイルをダウンロードする

STEP3-1 DDIでSOを生成する

2. DDIのWEBコンソールへアクセスする

[https://\[DDI IP or FQDN\]/](https://[DDI IP or FQDN]/)

3. ログインします

4. 検出 > 不審オブジェクト をクリックします。

SOの生成を確認します

不審オブジェクトの検出

表示:

すべて

IPアドレス、SHA-1、ドメインまたはURLの指定

Q

1-6/6 |

◀

▶

 ページ:

1

 /1

▶

25

 /ページ

拒否リストに移動

許可リストに移動

削除

<input type="checkbox"/>	不審オブジェクトの検出	リスク	種類	有効期限
<input type="checkbox"/>	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3	高	ファイル	2018/07/15 10:19:57
<input type="checkbox"/>	http://www2.winamp.org/...	高	URL	2018/07/18 13:29:47
<input type="checkbox"/>	www21.winamp.org	高	ドメイン	2018/07/18 13:29:47
<input type="checkbox"/>	www1.winamp.org	中	ドメイン	2018/07/18 13:29:47
<input type="checkbox"/>	192.168.1.1	高	IPアドレス	2018/07/18 13:29:47
<input type="checkbox"/>	28BDFD6BDD82EF5B1B2260FA816E46D42778E316	高	ファイル	2018/07/18 13:29:47

1-6/6 |

◀

▶

 ページ:

1

 /1

▶

25

 /ページ

STEP3-2 SOの同期を確認する

1. TCMのWEBコンソールへアクセスする

[https://\[TCM IP or FQDN\]/webapp/login.aspx](https://[TCM IP or FQDN]/webapp/login.aspx)

2. ログインします

3. [運用管理] - [不審オブジェクト] - [仮想アナライザオブジェクト]
をクリックします

4. 以下のようにSOがDDIから同期されていることを確認します

オブジェクト

除外

表示

すべて

すべてエクスポート

除外リストに追加

期限なし

今すぐ期限切れにする

処理を設定

影響の診断

<input type="checkbox"/>	オブジェクト	リスクレベル	種類	有効期限	危険性の高いエンドポイント	検出時の処理	処理プロセス
<input type="checkbox"/>	▶ [REDACTED]	高	URL	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input type="checkbox"/>	▶ [REDACTED]	高	ドメイン	2018/07/18 01:29:47	まだ診断されていません	なし	表示
<input type="checkbox"/>	▶ [REDACTED]	中	ドメイン	2018/07/18 01:29:47	まだ診断されていません	なし	表示
<input type="checkbox"/>	▶ [REDACTED]	高	IPアドレス	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input type="checkbox"/>	▶ 28BDFD6BDD82EF5B1B2260FA816E46D42778E3...	高	ファイル	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input type="checkbox"/>	▶ 1FB5AF2228410D2F824CB2B87E174EE7A890CBC3	高	ファイル	2018/07/15 10:19:57	まだ診断されていません	ブロック	表示

レコード: 1 - 6 / 6

ページ: 1 / 1

20

ページ

レコード: 1 - 6 / 6 | ページ: 1 / 1 | 20 / ページ

STEP3-3 TCMCM上でSOの検出時の処理を変更します

1. 以下の画面のように対象SOをチェックし、「処理を設定」をクリックします

オブジェクト

除外

表示

すべて

すべてをエクスポート

除外リストに追加

期限なし

今すぐ期限切れにする

処理を設定

診断の診断

<input type="checkbox"/>	オブジェクト	リスクレベル	種類	有効期限	危険性の高いエンドポイント	検出時の処理	処理プロセス
<input type="checkbox"/>	ト	高	URL	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input type="checkbox"/>	ト	高	ドメイン	2018/07/18 01:29:47	まだ診断されていません	なし	表示
<input type="checkbox"/>	ト	中	ドメイン	2018/07/18 01:29:47	まだ診断されていません	なし	表示
<input type="checkbox"/>	ト	高	IPアドレス	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input checked="" type="checkbox"/>	ト 28BDFD6BDD82EF5B1B2260FA816E46D42778E3...	高	ファイル	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input type="checkbox"/>	ト 1FB5AF2228410D2F824CB2B87E174EE7A890CBC3	高	ファイル	2018/07/15 10:19:57	まだ診断されていません	ブロック	表示

2. 以下の画面のようにブロックに設定し、適用をクリックします

検出時の処理

選択したファイル:

ブロック

選択したIPアドレス:

ログ

選択したURL:

ログ

サポートされる製品の表示

適用

キャンセル

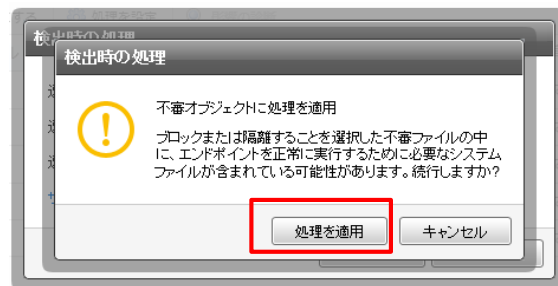
※ご注意！

ログ：IMSV A上で「隔離」しません

ブロック：IMSV A上で「隔離」します

STEP3-3 TMCM上でSOの検出時の処理を変更します

3. 以下の画面の処理を適用をクリックします



4. 以下の画面のようにブロックとなっていることを確認します

<input type="checkbox"/>	オブジェクト	リスクレベル	種類	有効期限 ▼	危険性の高いエンドポイント	検出時の処理	処理プロセス
<input type="checkbox"/>	[REDACTED]	高	URL	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input type="checkbox"/>	www24.winchincorp.com	高	ドメイン	2018/07/18 01:29:47	まだ診断されていません	なし	表示
<input type="checkbox"/>	www74.winchincorp.com	中	ドメイン	2018/07/18 01:29:47	まだ診断されていません	なし	表示
<input type="checkbox"/>	[REDACTED]	高	IPアドレス	2018/07/18 01:29:47	まだ診断されていません	ログ	表示
<input checked="" type="checkbox"/>	28BDFD6BDD82EF5B1B2260FA816E46D42778E316	高	ファイル	2018/07/18 01:29:47	まだ診断されていません	ブロック	表示
<input type="checkbox"/>	1FB5AF2228410D2F824CB2B87E174EE7A890CBC3	高	ファイル	2018/07/15 10:19:57	まだ診断されていません	ブロック	表示

STEP3-4 IMSVAへSOが同期されたことを確認します


1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSSVA IP or FQDN\]:8445/console.imss](https://[IMSSVA IP or FQDN]:8445/console.imss)

2. ログインします

3. [管理] - [IMSSVA設定] - [接続] - [Control Managerサーバ]をクリックします

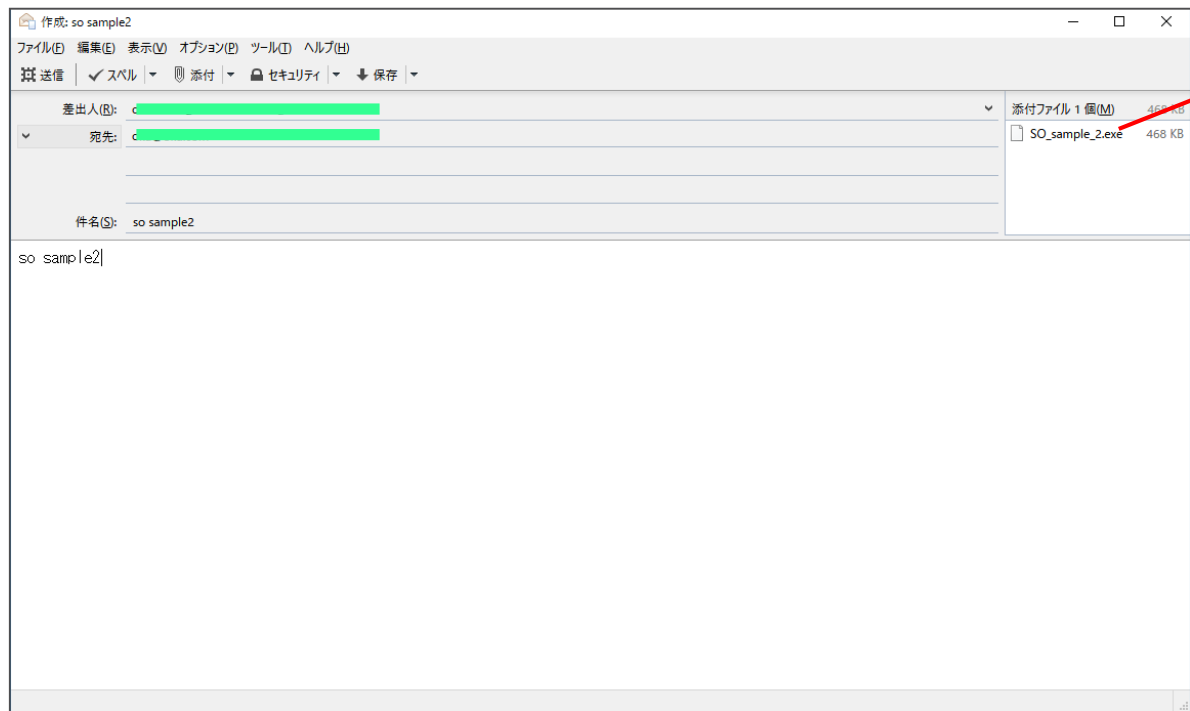
4. 以下の同期時刻を確認します

不審オブジェクトリストの設定	
<input checked="" type="checkbox"/> 不審ファイルリスト 	
同期間隔:	<input type="text" value="5"/> 分
前回の同期:	<div>2018/06/18 13:49:41</div>

STEP3-3の設定完了後、この時刻が更新されるまでお待ちください

STEP3-5 IMSVAでメールを隔離します

1. Sample SOファイルを添付してメールをIMSVAへ送信します



STEP3-5 IMSVAでメールを隔離します

1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)

2. ログインします

4. [ログ] – [ログクエリ] をクリックします

5. [種類] > ポリシーイベント を選択します

6. 日付を調整し、ログ表示をクリックします

STEP4 SPSと連携し URL SOをIMSVA で隔離する

STEP4-1 Webレピュテーション用ポリシーを作成します

1. IMSVAのWEBコンソールへアクセスする

[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)

2. ログインします

3. [ポリシー] – [ポリシーリスト] をクリックします

4. [追加] – [その他]をクリックします。

STEP4-1 Webレピュテーション用ポリシーを作成します

5. 以下の右画面の[受信者]をクリックします。

その後、以下左画面の[すべてのユーザ]をチェックし、保存をクリックします。

ポリシーリスト > 新規ルール

手順1: 受信者と送信者の選択 >>> 手順2 >>> 手順3 >>> 手順4

このルールの適用対象 受信メッセージ ▼

< 戻る 次へ > キャンセル

宛先	受信者
差出人	送信者
除外設定	送信者から受信者

次の宛先への受信メッセージ

ルールの追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☒ すべてのユーザ

☐ 選択したアドレスのいずれか

メールアドレスの入力 ▼

追加 >

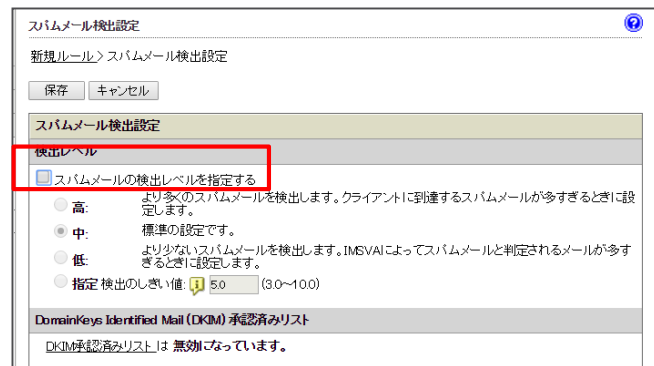
選択済み

6. [次へ]をクリックします。

STEP4-1 Webレピュテーション用ポリシーを作成します

7. 以下の左画面の[Webレピュテーション設定]をチェックします。
また、チェック後[スパムメール検出設定]のリンクをクリックします。

自動的にチェックされます



8. 上記右画面の[スパムメールの検出レベルを設定する]のチェック外し、保存をクリックします。

※本設定はスパムメール検出を無効化するために実施します。

9. [次へ]をクリックします。

STEP4-1 Webレピュテーション用ポリシーを作成します

10. [次の場所に隔離]をチェックし、[次へ]をクリックします。

このスクリーンショットは、Webレピュテーションポリシーの「インターセプト」設定画面を示しています。画面の上部には「戻る」、「次へ」、「キャンセル」のボタンがあります。中央には「ルール条件に一致するメッセージがすべてログに記録されます。」というメッセージがあります。下部には「インターセプト」のセクションがあり、いくつかのオプションがリストアップされています。その中で、「次の場所に隔離」が選択されており、このオプションが赤い枠で囲まれています。他のオプションには「メッセージをインターセプトしない」、「メッセージ全体を削除」、「次の受信者に変更」、「中継」があります。また、「初期設定の隔離」のドロップダウンメニューと「編集」ボタンも表示されています。

11. 以下の設定をし、[完了]をクリックします。

このスクリーンショットは、Webレピュテーションポリシーの「ルール」設定画面を示しています。画面の上部には「戻る」、「完了」、「キャンセル」のボタンがあります。中央には「ルール」のタブがあり、「有効」のチェックボックスがチェックされています。下部には「ルール名」と「順序番号」の入力欄があります。この画面では、「ルール名」に「wfs」と入力されており、「順序番号」に「2」と入力されています。両方の入力欄が赤い枠で囲まれています。

ルール名(任意)を入力

ルールの照会順序番号を入力

STEP4-2 DDANでURL SOを生成します

1. DDAN用の手動ファイルサブミッションツールを準備します

※法人カスタマーサイトよりダウンロードください

2. ダウンロードしたzipを解凍し、生成されたディレクトリ以下の[config.ini]をテキストエディタで開き、以下のパラメータにDDANのIPとAPIキーを設定します

[DTAS]

Host = [DDAN IPアドレス]

ApiKey = [DDAN Api Key]

※DDAN管理コンソール [ヘルプ] - [バージョン] - [APIキー:] から確認ください

3. work¥indir ディレクトリ以下へ、送信するテストファイルを配置します

STEP4-2 DDANでURL SOを生成します

4. コマンドプロンプトを開き[dtascli.exe -b]コマンドを実行します

```
C:\Users\Administrator\Desktop\submission_v1.2.7>dtascli.exe -b
2018-07-28 01:09:00,197 INFO **** welcome to use submission tool v1.2.7 ****
2018-07-28 01:09:00,197 INFO indir: C:\Users\Administrator\Desktop\submission_v1.2.7\work\indir
2018-07-28 01:09:00,213 INFO outdir: C:\Users\Administrator\Desktop\submission_v1.2.7\work\outdir
2018-07-28 01:09:00,213 INFO DDA Server: 10.3.180.14
2018-07-28 01:09:00,213 INFO API Key: 9D8BCED7-9736-41F0-8A16-CA77E5B547D0
2018-07-28 01:09:01,322 INFO Register is success
2018-07-28 01:09:01,540 INFO Find sample: VA-URL-SO_testSample.xls
2018-07-28 01:09:02,401 INFO 4DE40DEE20114ED4C8F4AD7C70245C95BCCBC502 (FileName:VA-URL-SO_testSample.xls) is processing
2018-07-28 01:09:02,602 INFO Unregister is success
C:\Users\Administrator\Desktop\submission_v1.2.7>_
```

5. DDANのWEBコンソールへアクセスします

[https://\[DDAN IP or FQDN\]/pages/login.php](https://[DDAN IP or FQDN]/pages/login.php)

6.[仮想アナライザ] – [不審オブジェクト]をクリックします

7. 以下のように、URL不審オブジェクトが生成されたことを確認します

<input type="checkbox"/> 前回の検出	失効日	リスクリ...	種類	オブジェクト
<input type="checkbox"/> 2018年07月28日 01:04:41	2018年08月27日 01:04:36	中	URL	https://[redacted].com/1028/submittingcommander.cgi?cf=cf&cf=cf&cf=cf

STEP4-3 TMCMへURL SOが同期されたことを確認します

1. TMCMのWEBコンソールへアクセスする

[https://\[TMCM IP or FQDN\]/webapp/login.aspx](https://[TMCM IP or FQDN]/webapp/login.aspx)

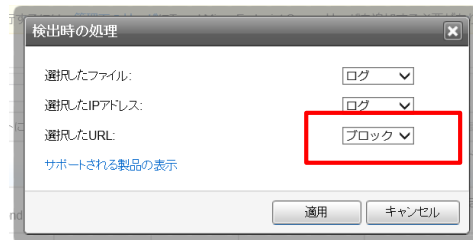
2. ログインします

3. [運用管理] - [不審オブジェクト] - [仮想アナライザオブジェクト]をクリックします

4. 以下のようにURL SOがDDANから同期されていることを確認します
その後、再左列をチェックし、[処理を設定]をクリックします。

すべてエクスポート 除外リストに追加 期限なし 今すぐ期限切れにする 処理を設定 影響の診断							
<input type="checkbox"/>	オブジェクト	リスクレベル	種類	有効期限 ▼	危険性の高いエンドポイント	検出時の処理	処理プロセス
<input checked="" type="checkbox"/>	https://[redacted].com:443/danmang...	中	URL	2018/08/27 01:04:36	まだ診断されていません	ログ	表示

5. 以下の画面のようにブロックに設定し、適用をクリックします。その後、上記画面[検出時の処理]が[ブロック]へ変更されたことを確認します



※ご注意！

ログ : IMSVA上で「隔離」せず、「放置」します

ブロック: IMSVA上で「隔離」します

STEP4-4 SPSへURL SOが同期されたことを確認します

1. TMCMのWEBコンソールへアクセスする

[https://\[SPS IP or FQDN\]/](https://[SPS IP or FQDN]/)

2. ログインします

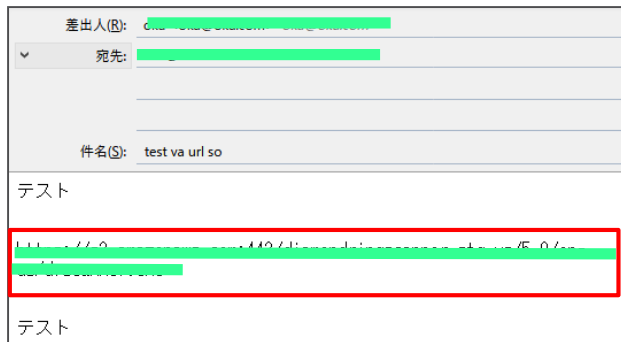
3. [Smart Protection] – [不審オブジェクト] をクリックします

4. 同期された時刻を確認します、また[今すぐ同期]をクリックすると即座に同期が実行されます。

The screenshot displays the Trend Micro console interface. At the top, a blue notification banner with a green checkmark icon states: 「不審オブジェクトのソースと同期しました。」 (Synchronized suspicious object sources). Below this, the '設定' (Settings) section is visible, containing the instruction: 「Control Managerなどのサポートされているソースに登録して、不審オブジェクトを同期します。」 (Register with supported sources like Control Manager to synchronize suspicious objects). The 'ソース' (Source) field is populated with 'https://10.2.2.123/WinApp'. The 'APIキー' (API Key) field contains a masked key. Below these fields are buttons for '登録解除' (Unregister) and '接続テスト' (Test Connection). At the bottom, the checkbox '不審オブジェクトを同期して有効化' (Enable synchronization of suspicious objects) is checked. The text '前回の同期: 2018年07月28日 01時38分47秒 (同期間隔: 10分)' (Last sync: 2018/07/28 01:38:47 (Sync interval: 10 min)) is shown. A red box highlights the '今すぐ同期' (Sync Now) button.

STEP4-5 IMSVAでURL SOを隔離します

1. IMSVAへメールを送信します



差出人(E): [redacted]

宛先: [redacted]

件名(S): test va url so

テスト

[redacted]

テスト

2. IMSVAのWEBコンソールへアクセスする

[https://\[IMSVA IP or FQDN\]/](https://[IMSVA IP or FQDN]/)

2. ログインします

3. [ログ] – [ログクエリ] をクリックします

4. [種類] > ポリシーイベント を選択します

5. 日付を調整し、ログ表示をクリックします

STEP4-5 IMSVAでURL SO隔離します

6. 以下のように隔離されていることを確認します

ログケリ

基準

種類: ポリシーイベント ▼ すべて ▼

日付: 2018/07/28 00:50 ~ 2018/07/28 01:50
年月日 (yyyy/mm/dd) 時 (hh) 分 (mm) 年月日 (yyyy/mm/dd) 時 (hh) 分 (mm)

送信者: 件名:

受信者: 違反する添付ファイル:

ルール: メッセージID:

[受信者] フィールドと [添付ファイル] フィールドで、検索項目の区切りにはセミコロンを使用します。
完全一致で検索するには、キーワードを入力します。部分一致で検索するには、アスタリスク(*)を使用します。たとえば、「*username」を指定すると、「username」で終わるすべての文字列が一致します。

ログ表示

ポリシーイベント 1ページあたりの結果数: 15 ▼

現在のページを印刷 CSV形式にエクスポート 1-1 / 1

日時 ▼	処理	ルール	メッセージID
2018/07/28 1:45:23	隔離	TMCM_不審URLの検出	[REDACTED]

TMCM_不審URL検出ルールで隔離されていることを確認

