SaaS 型セキュリティ対策サービス

サーバセキュリティ あんしんプラス

ユーザーズガイド

Version 2.13

日本事務器株式会社

改版履歴

Version	日付	変更内容
2.13	2024/11/14	注意事項の URL リンク修正。
2.12	2024/08/23	注意事項の URL リンク修正。
2.11	2023/11/27	注意事項の「TLSトラフィックの検査」追加。
2.10	2021/07/03	Ver20 対応。
2.03	2020/05/25	Ver12 対応。URL リンク修正。
2.02	2020/01/20	Ver11 対応。注意事項追加。
2.01	2019/04/18	注意事項の追加(サポート対象の Docker バージョン)。
2.00	2018/10/06	Ver10対応。不正プログラム対策強化、
		アプリケーションコントロール、Docker 環境の保護機能の追加。
1.11	2018/07/30	注意事項の追加。
1.10	2018/04/13	注意事項の修正。
1.09	2018/01/25	不正プログラム(ウイルス)で隔離されたファイルの復元手順追加。
1.08	2017/10/20	文言、画像修正。
1.07	2017/07/12	インストールスクリプト作成手順および誤記修正。
1.06	2016/07/15	インストールスクリプト作成手順修正。
		変更監視(カスタム設定)テンプレートによる設定手順修正。
		リアルタイム検索手順修正。
1.05	2015/07/15	インストールスクリプト作成手順修正、注意事項追加。
		Windows 手動インストール手順修正。
1.04	2015/04/07	変更監視運用手順および注意事項の修正。
1.03	2014/10/09	エージェントインストール注意事項追加。
1.00	2014/08/01	新規作成。

目次

1.	はじ	めにお読みください <注意事項>	. 6
1	.1.	注意事項	. 6
1	.2.	システム構成イメージ	. 8
2.	導入	、手順	. 9
2	.1.	管理 WEB コンソールについて <ログオン>	. 9
2	.2.	利用ライセンスの登録 <アクティベーションコード登録>	12
2	.3.	エージェントインストール方法	14
2	.4.	エージェントインストール用スクリプト作成	15
2	.5.	LINUX エージェントインストール	16
2	.6.	WINDOWS エージェントインストール(POWERSHELLを使用)	17
2	.7.	WINDOWS エージェント手動インストール (POWERSHELL を使えない場合)	18
2	.8.	エージェントインストール後の確認	21
2	.9.	LINUX エージェントアンインストール	22
2	.10.	WINDOWS エージェントアンインストール	22
2	.11.	管理 WEB コンソールからサーバの削除	22
3.	サー	-バ設定概要	23
3	.1.	サーバ毎に設定する	23
3	.2.	ポリシーを作成してサーバに割り当て	23
3	.3.	ポリシー概念	26
4.	ウイ	ルス対策『不正プログラム対策』	27
4	.1.	不正プログラム対策の有効化	27
4	.2.	不正プログラム対策設定	28
4	.3.	リアルタイム検索	31
	(1)	特定のディレクトリをリアルタイム検索から除外する場合	31
	(2)	特定のファイルをリアルタイム検索から除外する場合	33
	(3)	特定の拡張子をリアルタイム検索から除外する場合	34
4	.4.	予約検索	35
4	.5.	不正プログラム対策イベント	35
4	.6.	不正プログラム対策アラート通知	36
4	.7.	隔離ファイルの復元方法	37
	隔離	ジァイルを復元する前の準備	37
	隔離	ジァイル復元手順	40
5.	不正	E WEB サイトブロック 『WEB レピュテーション』	43

5.1.	WEBレピュテーションの有効化	
5.2.	WEBレピュテーション設定	
5.3.	WEBレビュテーションイベント	
5.4.	WEBレビュテーションアラート通知	
5.5.	WEB レピュテーションブロック画面	
6. 不	正な通信を防御『ファイアウォール』	
6.1.	ファイアウォールの有効化	
6.2.	ファイアウォールルール概要	
6.3.	ファイアウォールルール設定	
6.4.	あんしんプラス運用に必要なルール	
6.5.	攻撃の予兆	59
6.6.	ファイアウォールイベント	
6.7.	ファイアウォールアラート通知	60
7. 脆	弱性・WEB アプリケーション保護 『侵入防御(仮想パッチ)』	61
7.1.	侵入防御の有効化	61
7.2.	侵入防御(推奨設定)	
7.3.	侵入防御(カスタム設定)	
7.4.	侵入防御ルール割り当て状況の確認	
7.5.	侵入防御イベント	
7.6.	侵入防御アラート通知	
8. 改	ざん検知『変更監視』	
8.1.	変更監視の有効化	
8.2.	変更監視(推奨設定)	
8.3.	変更監視(カスタム設定)テンプレートによる設定	
8.4.	変更の検索	
8.5.	変更監視イベント	
8.6.	変更監視アラート通知	
9. 不	正アクセス検知『セキュリティログ監視』	
9.1.	セキュリティログ監視の有効化	
9.2.	セキュリティログ監視(推奨設定)	
9.3.	セキュリティログ監視(カスタム設定)テンプレートによる設定(LINUX例)	
9.4.	セキュリティログ監視(カスタム設定)XMLよる設定(WINDOWS例)	
9.5.	セキュリティログ監視イベント	
9.6.	セキュリティログ監視アラート通知	
10. 未	許可のアプリケーションを監視『アプリケーションコントロール』	
10.1.	アプリケーションコントロールの有効化	

10.2.	アプリケーションコントロール機能の確認	
10.3.	メンテナンスモード	
10.4.	アプリケーションコントロールアラート通知	
11. 共通	重オブジェクト	105
11.1.	共通オブジェクトリスト	
12. 予新	りタスク(スケジュール設定)	
12.1.	予約タスク概要	
12.2.	予約タスクの設定例 ①セキュリティアップデートのダウンロード	
12.3.	予約タスクの設定例 ②コンピュータの推奨設定を検索	
13. 管理	里者へのメール通知設定	110
13. 管理 13.1.	里者へのメール通知設定 アラート通知メールの受信設定	110 110
13. 管理 13.1. 14. 管理	里者へのメール通知設定 アラート通知メールの受信設定 里 WEB コンソール	110 110 112
 13. 管理 13.1. 14. 管理 14.1. 	里者へのメール通知設定 アラート通知メールの受信設定 里 WEB コンソール ダッシュボード	110 110 112 11 2
 13. 管理 13.1. 14. 管理 14.1. 14.2. 	里者へのメール通知設定 アラート通知メールの受信設定 WEB コンソール ダッシュボード アラート.	
 13. 管理 13.1. 14. 管理 14.1. 14.2. 14.3. 	里者へのメール通知設定 アラート通知メールの受信設定 WEB コンソール ダッシュボード アラート イベントとレポート	
 13. 管理 13.1. 14. 管理 14.1. 14.2. 14.3. 14.4. 	里者へのメール通知設定 アラート通知メールの受信設定 里WEBコンソール ダッシュボード アラート イベントとレポート コンピュータ.	
 13. 管理 13.1. 14. 管理 14.1. 14.2. 14.3. 14.4. 14.5. 	里者へのメール通知設定 アラート通知メールの受信設定 型WEBコンソール ダッシュボード アラート イベントとレポート コンピュータ ポリシー	

1. はじめにお読みください <注意事項>

本ユーザーズガイドは、サーバセキュリティあんしんプラス(以下「本サービス」と称す)」のインストールおよび管理 運用設定について記載いたします。

各機能の詳細な設定については Deep Security 管理コンソールのヘルプをご確認ください。

Deep Security システム要件

https://www.trendmicro.com/ja_jp/business/products/hybrid-cloud/deep-security.html#requirement-tm -anchor

お客様システムヘインストールする Agent のシステム要件は「Deep Security Agent のシステム要件」をご確 認ください。

※Deep Security Manager のバージョンは現在 20.0 となります。

1.1. 注意事項

(1)本サービスご利用する全ての保護対象サーバがインターネットへ接続できる必要があります。

接続には ポート80、443、4120、4122を使用します(Agent からインターネット側へのアウトバウンド通信のみ) ※プロキシサーバ経由はサポートされません。

(2) OS によってサポートされる機能が異なります。

例えば不正プログラム対策 (Anti-Malware)機能で Windows や Red Hat Enterprise Linux、CentOS などはリアルタイム 検索 (Realtime Scan) に対応していますが、Oracle Linux など一部バージョンではリアルタイム検索 (Realtime Scan) に対応していません。

OSごとの各機能サポート詳細については以下サイトの表をご確認ください。

https://help.deepsecurity.trendmicro.com/20_0/on-premise/ja-jp/supported-features-by-platform.html

(3)エージェントをインストール・アンインストールする際に再起動は必要ありませんが、ネットワークの一時的な切断や OSのネットワークドライバーが他のプログラムによってロックされてしまっている場合は、OSの再起動が求められる場合 があります。

(4)Linux 環境で日本語および文字コードが Unicode/UTF-8 ではない場合、新規作成するルールやカスタムルールでは日本語(2 バイト文字)は使わないでください。 日本語文字コードの扱い

https://success.trendmicro.com/ja-JP/solution/KA-0003639

(5)エージェントから管理サーバへの通信は5分間隔に行っています。そのため管理 Web コンソールで設定を行った場合、設定が反映されるまでに数分から10分程度かかります。

(6) エージェントと管理サーバ間の通信は ipv4 となり ipv6 は未対応となります。

(7)ウイルス対策(不正プログラム対策)利用時

データベース領域やアーカイブログデータなど、ディスク I/O が頻繁に発生するフォルダやファイルはリアルタイム検索の除外設定が必要になる場合があります。例)データベースフォルダ。

アプリケーションが遅くなるなどの事象が起こります。

ご利用になっているアプリケーションでリアルタイム検索除外が必要なファイルやフォルダを確認ください。

(8)エージェントのプログラムアップデートは、お客様で実施していただく必要があります。新しいエージェントプログラムが利用可能になった場合は警告としてアラート「Agent/Applianceのアップグレード推奨(新しいバージョンが使用可

能)」が表示されます。※メール通知を設定していればメール通知もされます。

Agent プログラムアップデート手順は以下サイトをご確認ください。

https://usersguide.anshinplus.jp/ →Agent アップグレード手順

(9) Web サーバで HTTPS 通信が使用されている場合の浸入防御保護について

侵入防御機能で HTTPS 通信を検査するためには、「TLSトラフィックの検査」を有効化する必要があります。 詳細は以下サイトをご確認ください。

<u>TLSトラフィックの検査</u>

各プラットフォームでサポートされている機能

【注意】

・高度な TLS トラフィック検査の有効化(Advanced TLS Traffic Inspection)

高度なTLSトラフィック検査でサポートされていないTLSトラフィック、または他のオペレーティングシステムのTLSトラフィックを検査する必要がある場合は、代わりに従来のSSL検査を設定できます。

高度なTLSトラフィック検査を使用すると、侵入防御モジュールは、追加の設定を行わなくても、PFS暗号で暗号化されたトラフィックを分析できます。

・SSL インスペクションを設定する(レガシー) (SSL Encrypted Traffic) 資格情報ファイルには、秘密鍵が含まれている必要があります。 ※資格情報は1つの NIC に対して1つの資格情報しかインポートできません。

(10) Docker 環境の保護については以下サイトをご確認ください。 Docker コンテナの保護

サポート対象の Docker バージョンは以下サイトをご確認ください。 Docker support

(11)Deep Security Agent の停止、起動方法

Agent を一時的に停止する場合の手順は下記 URL の Deep Security Agent 再起動/停止/開始方法をご確認ください。 https://success.trendmicro.com/ja-JP/solution/KA-0006584

1.2. システム構成イメージ





2. 導入手順

本サービス利用開始 ~ インストールについて説明いたします。

2.1. 管理 Web コンソールについて <ログオン>

本サービス契約、または評価版のお申込み完了後、「アカウント通知」、「パスワード通知」および「あんしんプラス アカ ウント登録完了のお知らせ」、「あんしんプラス ライセンス登録完了のお知らせ」のメール4通がお客様担当者へ送付さ れます。管理Webコンソールに接続するためにはアカウント通知メールに記載されているURL、アカウント名、ユーザ名、 およびパスワード通知メールに記載されているパスワードが必要になり、利用する機能ごとにライセンスの登録が必要に なります。

「あんしんプラス アカウント登録完了のお知らせ」に記載されているURL、ユーザ名、パスワード(初回変更の必要あり) にてお客様の保有しているライセンス情報をいつでも確認することができます。

(1)通知メール

<件名>アカウント通知

<件名>パスワード通知

<件名>[通知] あんしんプラス アカウント登録完了のお知らせ

<件名>[通知] あんしんプラス ライセンス登録完了のお知らせ

センス情報確認用

管理 Web コンソールアクセス用

アカウント通知メール

Deep Security へようこそ。新しいアカウントが作成されました。パスワードは別のメールでお知らせします。

アカウント名: ss_user001

ユーザ名: ss_user001

Deep Security の管理 Web コンソールは次の URL からアクセスできます:

https://ss.anshinplus.jp:443/SignIn.screen?tenantAccount=ss_user001&username=ss_user001

パスワード通知メール

Deep Security アカウント用に自動生成されたパスワードをお知らせします。アカウント名とユーザ名、Deep Security の管理 コンソールにアクセスするためのリンクを別のメールでお知らせします。

パスワード: SaNSrJ6OCtaA

※上記アカウント通知メールとパスワード通知メールはサンプルです。お客様へ送信されたアカウント通知メールに記載されている URL からログオンしてください。

[通知] あんしんプラス アカウント登録完了のお知らせメール

アカウントの登録が完了しました。すぐにサービスをご利用できます。
【ログイン ID】
Anshinplus
【パスワード】
はじめに次の URL をクリックし、パスワード発行の手続きを行ってください。
https://Forgetpwd.trendmicro.com/ForgetPassword/ResetPassword?T=zv0Xv&v=15cb45b7-60e2-40fb-b319-6c48
b987556f
※この URL は7 日間のみ有効です。
サービスを利用するには、下記の URL からログインしてください。
* ログイン URL:https://clp.trendmicro.com/Dashboard?T=zv0Xv

[通知] あんしんプラス ライセンス登録完了のお知らせメール

製品/サービスのライセンス登録が完了しました。

ライセンス情報

* サービスプラン:SSDA あんしんプラス

* ライセンス数:1

*アクティベーションコード: Deep Security Advance (JP)

Deep Security: DX-BPM5-V3H67-S7QYQ-XZLMJ-3ZAHZ-587LE

※上記ライセンス登録完了メールおよびアカウント登録完了メールはサンプルです。お客様へ送信されたライセンス登録完了のお知らせメールに記載されているアクティベーションコードを使用してください。

(2)ログオン

アカウント通知メールの URL リンクをクリックすると認証画面が開きます。

アカウント通知メールに記載されているアカウント名、ユーザ名およびパスワード通知に記載されているパスワードを入 カしてログオンをクリックしてください。

	🤋 🛛 Deep Security	◎ サポート情報
	ログオン	
	アカウンド名 SS-USEr0001	
å	೨-	
٩	パス ワード	
	◎ 参要素認証を使用する	パスワードを忘れた場合

ログオンに成功するとダッシュボード(関連情報をまとめて表示)が表示されます。

この画面がお客様専用の管理画面で、各種設定やセキュリティ状態を確認するための管理 Web コンソールになります。



(3) ログオンパスワードの変更

管理 Web コンソール右上のユーザ名をクリックし、パスワードを変更することができます。

njotech001 ss-use	r0001 - ⑦ へルt	ブ 🔘 サポート情報 🗕
ユーザプロパティ		
バスワードの変更		
ログオフ		

(4) ユーザプロパティの変更

管理Webコンソール右上のユーザ名をクリックし、ユーザ情報(メールアドレス等)の連絡先情報を変更することができます。



2.2. 利用ライセンスの登録 <アクティベーションコード登録>

(1)ライセンス登録

本サービスを利用開始するために、初めにライセンス登録を行います。

管理 Web コンソールの「管理」より、「ライセンス」を選択し、「新しいアクティベーションコードの入力」をクリックします。

ダッシュボード アラート	・ イベントとレポート コンビュータ ポリシ	/~ 管理			
🔹 システム設定	ライセンス				
🐻 予約タスク					
🔡 イベントベースタスク		ステータス	種類	有効期限	
🚦 ライセンス		/ / -			
、 ぬ フーザ管理	不止プログラム対策とWebレビュテーション	● ライセンスなし	なし	Tail.	詳細の表示…
	ファイアウォールと侵入防御	● ライセンスなし	なし	なし	詳細の表示…
> 🌒 //yファート	変更監視とアプリケーションコントロール	ライセンスなし	なし	なし	詳細の表示…
	セキュリティログ監視	 ライセンスなし 	なし	なし	詳細の表示…
	Deep Security Scanner	ライセンスなし	なし	なし	詳細の表示…
	新しいアクティベーションコードの入力…				

(2)アクティベーションコード登録

「あんしんプラス ライセンス登録完了のお知らせ」に記載されているアクティベーションコードを入力して「次へ」をクリックします。

※利用する機能ごとに入力する場所が異なります。SSDA あんしんプラスの場合のみ、すべてのモジュール欄に1行だ け入力してください。

・SSDA あんしんプラス(Deep Security)

- ・変更監視(Integrity Monitoring)
- ・セキュリティログ監視(Log Inspection)
- •侵入防御(Virtual Patch)

保護モジュール

۲	複数のモジュール用の単一アクティベーション	コード						
	すべてのモジュール	-	-	-	-	-	-	
•	各モジュール用の個別アクティベーションコー	e						
	ファイアウォールと侵入防御	-	-	-	-	-	-	
	変更監視とアプリケーションコントロール	-	-	-	-	-	-	
	不正プログラム対策とWebレビュテーション	-	-	-	-	-	-	
	セキュリティログ監視	-	-	-	-	-	-	

正しく入力が完了すると登録したライセンスが有効になります。

※有効期限は、解約されるまで自動的に更新されます。「完了」をクリックしてください。

入力したアクティベーションコード	で次のライセンスが有効になります。
7070/C/2741 V 2424 T	CNW/JTC//A/H/M/OB/Ja/J.

	ステータス	種類	有効期限	
ファイアウォールと侵入防御	😑 有効なライセンス	製品版	2015-04-02	
売了をクリックして、入力したアクラ	ティベーションコードを適用しま	ます。		
			<戻る	完了 キャンセル

「閉じる」をクリックしてください。

これでライセンスを登録した機能が利用できるようになります。



2.3. エージェントインストール方法

エージェントインストールには以下の方法があります。

Linux

インストールスクリプト

Windows

PowerShell を使ったインストールスクリプト
 Windows PowerShell 2.0 以降が必要。(Windows2008R2 以降は標準)
 ※Windows2003、2008 は PowerShell および Net Framework をインストールする必要があります。

※スクリプトが実行禁止になっている場合、RemoteSigned(ローカルに保存されているスクリプトは実行可能)または、 Unrestricted(全てのスクリプトが実行可能)へ実行ポリシーを変更する必要があります。

※他のアンチウイルスソフトを併用する場合、手動インストールを行ってください。 手動インストール時に「Anti-Malware」を選択せずにインストールを行います。

▶ 手動インストール ※PowerShell が使えない場合

2.4. エージェントインストール用スクリプト作成

エージェントをインストールするためのインストールスクリプトを作成し、スクリプトをサーバで実行します。

(1)インストールスクリプトの作成

管理 Web コンソール右上のサポート情報をクリックし、インストールスクリプトを選択します。



(2)パラメータの設定

エージェントをインストールするプラットフォームを選択します。

※Linux 環境かWindows 環境を選択してください。

インストールスクリプト



エージェントを自動的に有効化にチェックを入れます。

ポリシー:Base Policyを選択します。(ポリシーは後で変更可能です。)

インストールスクリプト

Deep Security Agentは、Righ 使用して、必要なスクリプトを生り	tScale、Chef、Puppet、SSHなどのツ 成できます。	ールを使用して配信できる	ます。このインストールスクリプトジェネレータを
WindowsとLinux以外のブラットフォ	ームについては、インストールガイドを参照し	してください。	
ブラットフォーム:	Linux版Agentのインストール	-	
 インストールスクリプトに 行する前に、Deep Secu す。追加ソフトウェアのイ インストール後にAgentを自 	ま、Deep Security ManaserからAsentソフト ity ManaserIこAsentソフトウェアをインボー ンボート 動的に有効化(セキュリティボリシーを割り	ウェアをダウンロードする月 トしておく必要があります。 当てる場合は必ず有効化し	F順が含まれています。インストールスクリフトを実 スクリプトは管理者権限で実行する必要がありま ってください)
セキュリティボリシー:	Base Policy	•	
コンピュータグル ープ:	コンビュータ	-	
Relayグループ:	初期設定のRelayグルー	ブ -	
Deep Security Manager^ 用するプロキシ:	の接続に使 プロキシを選択…	-	
Relayへの接続に使用する	ジロキシ: プロキシを選択	•	
備考 Asentからのリモ ヘルプのコマン	Eート有効化では、ホスト名、説明、一意の ドラインの手順ページを参照してください。	₪、およびその他のプロパき	ティも設定できます。詳細については、オンライン

(3) インストールスクリプトの保存

パラメータ設定により作成されたインストールスクリプトがウィンドウの下に表示されます。

全てのコマンドを選択するか「クリップボードにコピー」をクリックし、ファイルとして保存します。

Linux の場合:(例)install.sh ※保存する際に1 行目が #!/bin/bash であることを確認します。

Windows の場合:(例)install.ps1 ※保存する際に1 行目および最終行の</powershell>を削除してください。

インストールスクリプト

	コンビューダクルーフ:	コンビュータ	¥		
	Relayグループ:	初期設定のRelayグループ	•		
	Deep Security Managerとの接続に使用す るプロキシ:	プロキシを選択	•		
	Relayとの接続に使用するプロキシ:	プロキシを選択	•		
	GG考 Agentからのリモート有効化では、オ ヘルプのコマンドラインの手順ペー:	ー スト名、説明、一意のID、およびその他の、 ジを参照してください。	プロパティも設定できます。詳細については、オンライン		
	Deep Security ManagerのTLS証明書を確認す	る。詳細を表示			
#//bin/bash #//bin/bash # This script detects platform and architecture, then downloads and installs the matching Deep Security Agent package if [[\$(/usr/bin/id -u) -ne 0]]; then echo You are not running as the root user. Please try again with root privileges; logger -t You are not running as the root user. Please try again with root privileges; exit 1; fi, if you can be called a scheme try again with root privileges; exit 1; fi, SOURCEURL=Inttps://dsm.anshinolus.jp.443° curl \$SOURCEURLSoftware/deploymentscript/platform/linux/ -o /tmp/DownloadInstallAgentPackage —insecure —silent					
if [-=s	if [s_/tmp/DownloadInstallAgentPackage]; then				

2.5. Linux エージェントインストール

エージェントをインストールするサーバで、インストールスクリプトを実行します。

(例)[root@cent65 /]#. /home/install.sh

エージェントのダウンロード後、インストールが実行され初期設定が行われます。

最後に「Command session completed.」が表示されればインストール完了となります。

[root@cent65 /]# . /home/install.sh

Preparing	****	[100%]
1:ds_agent	****	[100%]
Loaded dsa_filter module ve	rsion 2.6.32-358.2.1.el6.x86_64 [OK]	
Starting ds_agent: [OK]		
Sending the command to the	agent on the local machine	
~~ 中略 ~~		
Received a 'GetAgentEvents'	command from the manager.	
Received a 'GetAgentStatus'	command from the manager.	
Command session completed.		
[root@cent65 /]#		

2.6. Windows エージェントインストール (PowerShell を使用)

(1)実行環境の確認
Windows PowerShell を起動し実行ポリシーを確認します。
コマンドラインより Get-ExecutionPolicy を実行してください。
PS C:¥Users¥Administrator> Get-ExecutionPolicy
Restricted
現在の実行ポリシーが表示されます。
Restricted はすべてのスクリプトが実行禁止。※Restricted 以外であればインストール実行に進んでください。

(2)実行ポリシーの変更

ローカルに保存されているスクリプトは実行可能なポリシーに変更します。 コマンドラインより Set-ExecutionPolicy RemoteSigned を実行してください。

実行ポリシーを変更しますか?の確認には[Y]はいとします。

再度実行ポリシーの確認をしてください。

PS C:¥Users¥Administrator> Get-ExecutionPolicy

RemoteSigned

RemoteSigned となっていれば変更完了です。

(3) インストール実行

エージェントをインストールするサーバで、インストールスクリプトを実行します。

(例)PS C:¥Users¥Administrator> C:¥install.ps1

インストールが完了するまで約1~2分かかります。

エージェントのダウンロード後、インストールが実行され初期設定が行われます。

最後に「Command session completed.」が表示されればインストール完了となります。

PS C:¥Users¥Administrator> C:¥install.ps1

Sending the command to the agent on the local machine...

~~ 中略 ~~

Received a 'GetAgentStatus' command from the manager.

Command session completed.

PS C:¥Users¥Administrator>

2.7. Windows エージェント手動インストール (PowerShell を使えない場合)

(1)インストール準備

エージェントインストールプログラムをダウンロードします。ファイル名:agent.msi

【32ビット】https://ss.anshinplus.jp/software/agent/Windows/i386/

【64ビット】https://ss.anshinplus.jp/software/agent/Windows/x86_64/

(2)インストールプログラムを実行

agent.msiを実行します。セキュリティの警告が表示された場合は「実行」をクリックしてください。

闇いているファイル - セキュリティの警告			
20771	「ルを実行しますか?		
17	名前 C¥agent.msi 発行元 <u>Trend Micro, Inc.</u> 種類 Windows インストーラー バッケージ 発信元 C¥agent.msi		
™ 2007	実行(B) キャンセル アイル間に第に警告する(W)		
インターネットのファイルは役に立ちますが、このファイルの種類はコンピューターに問 置を起こす可能性があります。信頼する発行元のソフトウェアのみ、実行してくださ い、危険性の説明			

(3) インストールウイザード

インストールを続ける場合は「次へ」をクリックします。



「使用許諾契約書に同意します」にチェックを入れ、「次へ」をクリックします。

謝 Trend Micro Deep Security Agent セットアップ ローロ	X
使用許諾契約書 以下の使用許諾契約書をよくお読みください。	0
使用許諾契約書について	-
本製品の使用許諾契約の内容につきましては、製品インストールメディア内 に格納されている使用許諾契約書をご確認ください。	E
格納されている使用許諾契約書と当社webサイトに掲載している使用許諾契 約書に異なる定めがあった場合には、当社webサイトに掲載されている使用 許諾契約書が優先されます。	
また、CD-ROMなどのインストールメディアのない製品やサービスにつきましては、当社webサイトに掲載している契約書をご確認くださいますようお願い	÷
☑ 使用許諾契約書(二同意します(A)	
印刷(2) 戻5(8) 次へ(1) キャン	211

インストールフォルダを指定します。フォルダを指定し「次へ」をクリックします。

謝 Trend Micro Deep Security Agent セットアップ 📃 📼
インストール先フォルダ 既定のフォルダにインストールするには [次へ] をクリックし、別のフォルダを選択する には [変更]をグリックします。
Trend Micro Deep Security Agent のインストール先:
C:#Program Files#Trend Micro#Deep Security Agent¥
& E Com
戻る(8) 次へ(1) キャンセル

「インストール」をクリックするとインストールを開始します。

🖶 Trend Micro Deep Security Agent セットアップ
Trend Micro Deep Security Agent のインストール準備完了
インストールを開始するには「インストール」をクリックしてください。インストール設定を確認また は変更するには【戻る】をクリックしてください。ウィザードを終了するには【キャンセル】をクリック してください。
戻る(8) インストール(1) キャンセル

「完了」をクリックします。



(4)エージェント有効化の準備

インストールスクリプトの一部コマンドを実行するため管理 Web コンソールよりインストールスクリプト作成画面を開きます。

プラットフォーム:Windows を選択

エージェントを自動的に有効化にチェックを入れます。

ポリシー:Base Policyを選択します。(ポリシーは後で変更可能です。)

パラメータ設定により作成されたインストールスクリプトがウィンドウの下に表示されます。

インストールスクリプト

Deep Security Agentは、RightScale、Chef、Puppet、SSHなどのツールを使用して配信できます。このインストールスクリプトジェネレータを 使用して、必要なスクリプトを生成できます。 WindowsとLinux以外のブラットフォームについては、インストールガイドを参照してください。 Windows版Agentのインストール プラットフォーム: -(通考) インストールスクリプトには、Deep Security ManagerからAgentソフトウェアをダウンロードする手順が含まれています。インストールスクリプトを実 行する前に、Deep Security ManagerにAgentソフトウェアをインボートしておく必要があります。スクリプトは管理者権限で実行する必要がありま す。追加ソフトウェアのインボート ✓ インストール後にAgentを自動的に有効化(セキュリティポリシーを割り当てる場合は必ず有効化してください) セキュリティポリシー: Base Policy Ŧ コンビュータグルーブ: Ŧ コンビュータ Relayグループ: 初期設定のRelayグループ Deep Security Managerへの接続に使 ブロキシを選択.. Ŧ 用するプロキシ: Relavへの接続に使用するプロキシ: プロキシを選択 * <powershell> #requires -version 4.0 # PowerShell 4 or up is required to run this script # This script detects platform and architecture. It then downloads and installs the relevant Deep Security Agent package if (-NOT ([Security Principal,WindowsPrincipal] [Security Principal,WindowsIdentity]::GetCurrent()).IsInRole([Security Principal,WindowsBuiltInRole] 'Administrator'')) { Write-Warning "You are not running as an Administrator. Please try again with admin privileges." exit 1

(5)エージェント有効化の実行

インストールスクリプトの dsa_control 以降 -a dsm: から policyid:1" までのコマンドをコピーします。

~~ 省略 ~~

Start-Sleep -s 60

& \$Env:ProgramFiles"¥Trend Micro¥Deep Security Agent¥dsa_control" -a dsm://ss.anshinplus.jp:4120/ "tenantID:B10705AE-6DA9-BDBA-726E-8C3E5369A85F"

"tenantPassword:3D2DE82C-3DE3-E0A2-E2B8-C1EE7ED29975" "policyid:1"

コマンドプロンプトよりエージェントがインストールされているフォルタに移動します。

C:
 ¥Program Files ¥Trend Micro ¥Deep Security Agent

dsa_control コマンドと合わせてコピーしたコマンドを張り付けて実行します。

(例)

dsa_control -a dsm://ss.anshinplus.jp:4120/ "tenantID:B10705AE-6DA9-BDBA-726E-8C3E5369A85F" "tenantPassword:3D2DE82C-3DE3-E0A2-E2B8-C1EE7ED29975" "policyid:1"

最後に「Command session completed.」が表示されればインストール完了となります。	
--	--

C:¥Program Files¥Trend Micro¥Deep Security Agent>dsa_control –a dsm://ss.anshinplus.jp:4120/
"tenantID:B10705AE-6DA9-BDBA-726E-8C3E5369A85F" "tenantPassword:
3D2DE82C-3DE3-E0A2-E2B8-C1EE7ED29975" "policyid:1"
Sending the command to the agent on the local machine
$\sim \sim$ 中略 $\sim \sim$
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Received a 'UpdateComponent' command from the manager.
Command session completed.

2.8. エージェントインストール後の確認

エージェントインストール後、管理 Web コンソールのコンピュータより対象のサーバが表示され、管理対象(オンライン) となっていることを確認します。



以上でエージェント導入は完了です。

各機能の設定は管理 Web コンソールより行ってください。

2.9. Linux エージェントアンインストール

(1)アンインストール実行
エージェントをアンインストールするサーバで、アンインストールコマンドを実行します。
[root@cent65[~]]# rpm -ev ds_agent
Stopping ds_agent: [OK]
Unloading dsa_filter module... [OK]

Unloading dsa_filter module...[OK]と表示されたらアンインストールは完了です。

2.10. Windows エージェントアンインストール

(1)アンインストール実行

コントロールパネルのプログラムと機能より「Trend Micro¥Deep Security Agent」を選択しアンインストールを実行してください。



2.11. 管理 Web コンソールからサーバの削除

エージェントをアンインストールしても管理 Web コンソールにサーバ情報が残るため、アンインストールしたサーバを削除します。

エージェントをアンインストールしたサーバを選択し、削除してください。

 スマートフォルダ コンピュータ 	コンピュータ サブグループを	を含む ▼ グループ別 ▼	(
	+ 追加 -	詳細 🕈 処理 🔹 📋 イベント 🔹	■ エクスポート 💌 🖽 列
	名前	明 プラットフォー	・・ ポリシー ステータス *
	♥ コンピュータ(6)		
	📑 test1206.localdomain	Red Hat Enter	Base Policy 🛛 ● オフライン
	ip-10-0-2-11 awa	s-justice AM-Linux Amazon Linux	···· Base Policy 😑 セキュリティログ監視ル…

3. サーバ設定概要

各機能設定方法の概要を説明します。

3.1. サーバ毎に設定する

管理 Web コンソールに登録されているサーバ毎に設定を行います。 1 台のサーバを設定する場合や、各サーバの設定が異なる場合にはサーバ毎に設定してください。

3.2. ポリシーを作成してサーバに割り当て

ポリシーでは、ルールや設定をまとめて保存し、複数のサーバに簡単に割り当てることができます。 例えば、侵入防御(仮想パッチ)の設定を複数サーバに割り当てる場合や、Linux サーバ用、Windows サーバ用のポリ シーを作成しておき、サーバを追加した時にポリシーを選ぶだけというような運用ができます。 ポリシーをサーバに割り当てても個々に修正(オーバーライド)することができます。

※ポリシーカスタマイズ時の注意事項

侵入防御、変更監視、セキュリティログ監視で推奨設定を利用する場合は Base Policy の利用を推奨します。 Linux 用や Windows 用のポリシーが用意されていますが、割り当てると侵入防御や変更監視のすべてのルールが割り 当てられ個別にルールをカスタマイズする必要があります。

Linux サーバ用ポリシー設定例

(1)ポリシー「Linux Server」をダブルクリックします。

■ポリシー設定画面



(2)侵入防御や変更監視、セキュリティログ監視の設定を行います。

■ポリシー内容設定画面

4	概要	一般	このポリシーを使用	しているコンピュータ	1/2/
Ø	不正プログラム対策	名前:		Linux Server	
۲	Webレビュテーション	1说6月:		An example policy for	r Linux servers.
۲	ファイアウォール				
θ	侵入防御				
0	変更監視				
0	セキュリティログ監視	継承	আছি বিভি		
۲	アブリケーションコントロー	親ポリシー:		✓ ≧ Base Polic	cy
	インタフェースの種類			> 🎽 Deep S	Seaurity
	設定			🖄 Solaris	is Server
Х;	オーバーライド	モジュー	-JL		
		😵 不	正プログラム対策:	オン	▼ ● リアルタイム

(3)コンピューター覧よりポリシーを割り当てるサーバをダブルクリックします。

ダッシュボード 処理 アラート イベン	トとレポート コンピュータ	ポリシー 管理		
🔁 スマートフォルダ	コンピュータ サブグル	ーブを含む ▼ グループ別 ▼		Q このページを検察
コンピュータ	+ 追加 - 💼 削除	■詳細 ★ 処理 ▼ 首	イベト・ 🖪 エクスポート・	睥,列
	名前	說明	プラットフォー・・ ポリシー :	ステータス 👻
	✓ コンピュータ(6)			
	ip-10-0-2-15	aws-justice F	Red Hat Enter… Base Policy 🛛 🌒 🛱	理対象(オンライン)
	makino2012F2std	tech-sv M	Microsoft Win… Base Policy 🛛 🕚 🖺	理対象(オンライン)

(4)サーバに適切なポリシーを割り当てます。

- 概要	一般 処理 システム・	
😵 不正プログラム対策	ホスト名:	ip-10-0-2-15
💿 Webレビュテーション	表示名:	
😑 ファイアウォール	説明:	aws-justice
😌 侵入防御		1
◎ 変更監視	プラットフォーム:	Red Hat Enterprise 7 (64 bit) (3.10.0– 123.81.el7.centos.plus.x86 <u>.</u> 64)
❷ セキュリティログ監視	グループ:	コンピュータ ・
🥺 アプリケーションコントロー	ポリシー:	Base Policy 🔹
- インタフェース	資産の重要度	7au 🗸

(5)個別設定例

■サーバ設定画面

割り当てたポリシー「Linux server」では変更監視が継承(オフ)になっているとします。

😵 不正プログラム対策	変更監視
💼 Webレビュテーション	設定: 継承(オフ) ▼
🖶 ファイアウォール	ステータス: 🌒 オフ, インストールされています, 22 ルール
😌 侵入防御	リアルタイム検索の有効化
◎ 変更監視	
セキュリティログ監視	変更の検索

このサーバで変更監視を有効に設定したい場合、継承(オフ)からオンに変更することにより設定が修正(オーバーライドされ 亦更監視が 有効に たります

ドされ変更監視が有効になります。

😵 不正プログラム対策	変更監視
🕝 Webレビュテーション	設定: オン 🗸
🖶 ファイアウォール	ステータス: オフ, インストールされています, 22 ルール
😌 侵入防御	リアルタイム検索の有効化
◎ 変更監視	リアルタイム
マキュリティログ監視	変更の検索

※このようにサーバで個別に設定変更する場合には継承を外して設定します。

3.3. ポリシー概念



ポリシーを設定しサーバへ割り当てた場合、設定を継承する形になります。ポリシーと異なる設定にする場合は、各サーバで継承を外して設定します。機能のオン、オフだけでなくルール設定も継承、継承しないで設定することができます。

※Base Policy ではファイアウォール機能を除き、全ての機能が有効(オン)になっていますが、機能毎のライセンスが ない場合は利用できません。

4. ウイルス対策『不正プログラム対策』

不正プログラム対策設定について説明いたします。

4.1. 不正プログラム対策の有効化

(1)管理 Web コンソールにログオンしてください。

コンピュータより、不正プログラム対策を設定するサーバをダブルクリックします。

ダッシュボード	7 5 -ト	イベントとレポート	コンピュータ	ポリシー	管理			
		ュータ サブグループを含む	む マ グループ別 、	·			Q 検索	•
		新規 🖌 💼 削除 📰	詳細 処理 -	イベント 🖌 🔂 エ	クスポート 🔹	1 列		
		名前 🔻 説明	ブラッ	トフォーム ポリシ	-	ステータス	前回の通信	前回成功したアップデート
	E =	ビュータ (2)						
		cent65	Red I	Hat Enter Linux	Server 😑	管理対象 (オンライン)	3 分 前	37分前
		2008r2	Micro	soft Wind Base I	Policy 😑) 管理対象 (オンライン)	1分前	17 時間 前
	~~							

(2)サーバの設定画面が表示されます。

「不正プログラム対策」をクリックします。

■ 概要	一般処理イベント				
😨 不正プログラム対策	[→般		_		^
💿 Webレビュテーション	不人作名: 表示名:	2008r2	×	(前回使用されたIP: 61.120.61.62)	
🎯 ファイアウォール	説明:				
📀 侵入防御					
🔘 変更監視					
http://www.intelligible.com/ http://wwww.intelligible.com/ http://wwww.intelligible.com/ http://wwwwwwwwwwwwww	プラットフォーム:	Microsoft Windows Server 2008 R2 (64 bit) Build 7600			
C 1200 HE DER	グループ:	コンピュータ	-		
📟 インタフェース	ポリシー:	Base Policy	-	編集	
🎲 設定 🧠	資産の重要度:	ねし	~	編集	
アップデート	セキュリティアップデートのダウンロード テ・	トレンドマイクロアップデートサーバ	~	羅集	
<u>∳</u> オーバーライド	「ステータスーーーーーー				

(3)不正プログラム対策のステータスを「オン」にして「保存」をクリックしてください。

これで不正プログラム対策が有効になります。継承(オン)になっている場合は既に有効になっています。

※OS によってリアルタイム検索可否が異なります。リアルタイム検索に対応していない OS の場合は予約タスクにより定期的に検索を行う設定が必要です。詳細は本マニュアルの注意事項を確認ください。

📃 概要	- 設 Smart Protection 詳細 隔離ファイル イベント
😵 不正プログラム対策	「不正プログラム対策」 不正プログラム対策のステータス: 継承(オン)
● Webレビュテーション ◎ ファイアウォール	「Uアルタイム検索
侵入防御	☑ 搬承 設定: Default Real-Time Scan Conflouration
	スケジュール: Every Day All Day 🗸 庸集
 セキュリティロク監視 インタフェース 	「手動検索」 「「「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」「」」」
()) 設定	 ● 相對// ● 相對// ● Default Manual Scan Configuration ● 福集
■ アップデート	- 予約除業
5 4-N-24K	

4.2. 不正プログラム対策設定

不正プログラム対策モジュールには、不正プログラム、ウイルス、トロイの木馬、スパイウェアなどのファイルベースの脅 威からリアルタイムに保護する機能と、必要に応じて保護する機能があります。脅威を特定するために、サーバにホスト されている、またはアップデート可能なパターンとしてローカルに保管されている包括的な脅威データベースに対して、 ファイルを照合します。また、圧縮や既知の攻撃コードなど、特定の特性がないかについても確認します。

(1)「一般タブ」

手動検索、予約検索、リアルタイム検索には、それぞれ異なるプロパティを設定できます。 前回の不正プログラムの手動検索および予約検索の日時を表示し、不正プログラムのクイック検索またはフル検索を実 行または中止できます。



検索の種類ごとに、検索されるオブジェクトと検索の順序

対象	フル検索	クイック検索
ドライバ	1	1
トロイの木馬	2	2
プロセスイメージ	3	3
メモリ	4	4
ブートセクタ	5	_
ファイル	6	5
スパイウェア	7	6

(2)「Smart Protection タブ」

スマートスキャンでは、トレンドマイクロのサーバに保存されている脅威シグネチャが参照されます。スマートスキャンを 有効にすると、まず、ローカルで保持している情報を元にセキュリティ上の危険が検索されます。その検索中にファイル の危険を評価できなかった場合は、トレンドマイクロのグローバルスマートスキャンサーバに接続します。

スマートスキャンには、次の機能と利点があります。

・脅威からの保護にかかる合計時間を削減

・パターンのアップデート時に使用されるネットワーク帯域幅を削減。パターン定義のアップデートの大半は、クラウドで 保持され、多数のエンドポイントへの配信は不要

・企業全体へのパターン展開に関連するコストとオーバーヘッドを削減

・エンドポイントにおけるカーネルのメモリ消費を削減。メモリ消費量の増加を最小限に抑制

・クラウドで、高速でリアルタイムのセキュリティステータス検索機能を実現



※スマートスキャンをオフにすると従来型スキャンになります。通常はスマートスキャン利用を推奨します。

(3)「Connected Threat Defense タブ」本サービスでは使用しません。

(4)「詳細タブ」

隔離ファイルの保存に使用される最大ディスク容量、検索するファイルの最大サイズなどが設定できます。

通常は初期値のままで問題ありません。

概要	-般 Smart Protection 詳細 隔離ファイル イベント
	「隔離ファイルー
> Webレビュテーション	□ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
) ファイアウォール	
侵入防御	- 「検索の制限
変更監視	検索するファイルの最大サイズ: 0 MB
セキュリティログ監視	「不下ブログラム検索用のルソース事ド当て
インタフェース	不正プログラム検索でマルチスレッド処理を使用(利用可能な場合): (批承(しいえ)
設定 アップデート オーバーライド	≪ ■ マルチスレッド接通を使用すると、コビュータ上で東ド午の他の処理に利用す数なリノースが低下する可能性があります。この設定を有 化するはえ、マルチスレッド接通を有効にしたコビュータを再転換する必要があります。 (計可するス) ビウェア/ジレーウェアー
	スパイウェアグレーウェアとして認識された特定のアプリケーションを一部のシステムで残すことができます。追加削除オブションを使用して、許可 るスパイウェアグレーウェアのリストを管理できます
	18.10
	Rife
	このリスクのエントリオ大文字とリ文字が区別はれます。追加、た刀ドグウェアグレーウェアがすむこ不正プログラム対策イベンドに表示 でいる場合は、ドイベト)をおクリックして「DJ ドクシュアグリーウェアを発展リストに追加」を提供します。

(5)「検出ファイル」

コンピュータで隔離されたファイルが表示されます。

復元させたい場合には「隔離ファイルの復元方法」を参照ください。



4.3. リアルタイム検索

検索除外設定について説明します。

ヒント:

不正プログラム対策保護を有効にするとパフォーマンスが低下する場合、検索除外を使用して特定のフォルダやファイ ルを検索対象から除外すると改善できることがあります。

不正プログラム対策の「一般タブ」を開きます。設定の「編集」をクリックします。

	概要	一般	Smart Protection	Connected Threat Defense	副補	検出ファイル	不正プログ	ラム対策イベント
8	不正プログラム対策	不正プロ	コグラム対策					
٦	Webレビュテーション	設定:	継承 (オン)	~				
۲	ファイアウォール	ステータ	ג: 🔍 אין דע	レタイム				
θ	侵入防御	リアルタ	イム検索					
0	変更監視	اللہ اللہ اللہ اللہ اللہ اللہ اللہ اللہ	承					
0	セキュリティログ監視	不正プロ	コグラム検索設定:	Default Real-Time Sc	an Configur	ation	~	編集
	アプリケーションコントロー	スケジョ	r−µ:	Every Day All Day				編集

(1)特定のディレクトリをリアルタイム検索から除外する場合

「検索除外タブ」のディレクトリリストにチェックを入れ新規を選びます。

※一度作成したリストは保存され以後、選択できるようになります。



名前:リスト名を入力します。 ディレクトリ:除外ディレクトリをフルパスで入力します。(複数指定可) 例)d:¥oracle フォルダを除外する場合 d:¥oracle¥ 決定は「OK」をクリックしてください。 一般割り当て対象

┌─般情報───	
名前:	DBサーバフォルダ除外
見8月:	oracleフォルダ
- デオンクトリン(1/5)	あたり1つのディックトロン
diloracie)	0(201207) 40219)
u.ioraciei	
「サポートされてい	5形式:
デルクリ	例: c:\Program Files\
ディレクトリバ	C:\Program Files*\
ディレクトリ*\	C:\Program Files\サブディレクトリ名*\
WILLIAM STREET	
いなり見ると説で、 S(ENV VAR)	(b): S(windir)
VILLION VILLI	173. #[minimi]
	ント 199. C.Wemp #TEIMPナイレクトリを味外します

ディレクトリリストに作成したリストが表示されます。

「OK」をクリックして完了します。



(2)特定のファイルをリアルタイム検索から除外する場合

「検索除外タブ」のファイルリストにチェックを入れ新規を選びます。 ※一度作成したリストは保存され以後、選択できるようになります。



名前:リスト名を入力します。

ファイル:ファイル名を入力します。(複数指定可)

例) document.txt ファイルを除外

決定は「OK」をクリックしてください。

一般	削り当て対象
「一般情報─	
名前:	fileサーバ除外
見8月:	Document.txt
ファイル: (1	行あたり1つのファイル)
document	

ファイルリストに作成したリストが表示されます。

「OK」をクリックして完了します。

è索除· □ デ	外 ―――― イレクトリリスト	:						
7	ー イレクトリリスト	の選択	×	编集				
v 7	ァイルリスト:							
fil	leサーバ除外		\ \	編集				
7	ァイル拡張子し	자:						
7	ファイル拡張子!	リストの選択	×	编集				
🖌 プ	ロセスイメージ	ファイルリス	.F:					
P 猫考	rocess Image 「プロセスイ>	Files (Win	dows) 🕓 レリストコ設分	・ 編集 目はDeep Se	ecurity Ager	ntで検索	が行われる場	合のみ適用され
P 猫考	rocess Image 「ブロセスイ> ます。この読	Files (Win ージファイ) 包よ、Deep	dows) レリストJ設元 Security V	2 編集 記JDeep Se irtual Applia	ecurity Ager nceでは無初	ntで検索 見されま	が行われる場 す。	合のみ適用され

(3)特定の拡張子をリアルタイム検索から除外する場合

「検索除外タブ」のファイル拡張子リストにチェックを入れ新規を選びます。

※一度作成したリストは保存され以後、選択できるようになります。



名前:リスト名を入力します。

ファイル拡張子:拡張子を入力します。(複数指定可)

例) 拡張子 log ファイルを除外

決定は「OK」をクリックしてください。

一般	割り当て対象
┌──般情報	
名前:	Logファイル除外
[見 ¹ 月:	logファイル除外
「ファイル拡	張子: (1行あたり1つのファイル拡張子)
log	
-	

ファイルリストに作成したリストが表示されます。

「OK」をクリックして完了します。

	検索除外	処理	オプション	/ 割り当	て対象			
検索除	外———							
ロデ	ーレクトリリスト							
7	ディレクトリリスト	の選択	[✓ 編集				
ロ フ	ァイルリスト:							
-	ファイルリストの	選択	[✓ 編集				
⊻ ⊇	アイル拡張子り	자:						
L	.ogファイル除タ	`	[✔ 編集				
V 7	ロセスイメージ	ファイルリス	ՀԻ:					
				_				
P 備考	Process Image 「プロセスイ> ます。この設	Files (Wir ニジファイ. 定は、Dee	ndows) ルリスト」設 p Security	✓ 編集 定はDeep Virtual App	Security	Agentで利 は無視され	検索が行われる: はます。	場合のみ適用さ
(備考)	Process Image 「ブロセスイ> ます。この設	Files (Wir ージファイ. 記よ、Dee	ndows) ルリストJ設 p Security	▼ 編集 定はDeep Virtual App	Securit) liance c	r Agentで批	検索が行われる5 ます。	場合のみ適用さ

4.4. 予約検索

予約検索は予約タスクにて実行します。 予約タスク(スケジュール設定)を参照してください。

4.5. 不正プログラム対策イベント

ウイルスを検出した場合、不正プログラム対策イベントとして記録します。

ダッシュボード 処理 こ	アラート イベントとレポー	- N コンピュー	-タ ポリシー 管理			
> 曽 イベント	不正プログラム対象	ほイベント す	オベて 🗸 グループ化した	alı 💌		
	期間: 過去1時間		•			
	コンビュータ: コンビュータ	:	▼ 2008R2aws-	justi	Ŧ	
	■ 表示 📑 エクスポー	-ト 👻 🔒 自重	助タグ付け 田. 列			
	時刻 -	コンピュータ	感染ファイル	タグ	不正プログラム	実行された…
	2018-10-05 15:2554	2008R2aws-justi	C¥Users¥Administrator¥Ap	р …	Eicar_test_file	削除
	2018-10-05 15:25:47	2008R2aws-justi	C¥Users¥Administrator¥Ap	p	Eicar_test_file	削除

イベントをダブルクリックすると詳細が表示されます。

一般タグ							
一般情報							
コンピュータ:	2008R2aws-justi						
送信元:	Agent						
不正プログラム	"報						
検出時刻:	2018-10-05 15:25 54						
不正プログラム:	Eicar_test_file						
感染ファイル:	$\label{eq:constraint} C \\ \texttt{W} Users \\ \texttt{A} dministrator \\ \texttt{A} \\ \texttt{A} \\ \texttt{A} \\ \texttt{A} \\ \texttt{D} \\ \texttt{D} \\ \texttt{a} \\ \texttt{a}$						
検索の種類:	リアルタイム						
実行された処理	削除						
理由:	Default Real-Time Scan Configuration						
主要なウイルス	重類: ウイルス						
く戻る	次へ > 開じる						

4.6. 不正プログラム対策アラート通知

不正プログラム対策イベントに記録された中から、アラートを発するように設定されている場合にアラートとして記録され、 指定された管理者宛てにメール通知します。

リアルタイム検索、手動検索、予約検索にて設定可能で初期値ではアラート通知を行う様に設定されています。

■リアルタイム検索「オプションタブ」

一般	検索対象 検索除外 詳細 割り当て対象							
1	ドキュメントの脆弱性を突いた攻撃コードを検索する 🕕							
	💿 既知の脆弱性に対する攻撃コードのみを検索する 🟮							
	◎ 既知の脆弱性に対する攻撃に加え、未知の攻撃コードも積極的に検索する 🚺							
挙動	会視 📲 🖲 							
1	不審なアクティビティ/不正な変更(ランサムウェアを含む)を検出する 🛛							
	□ ランサムウェアによって暗号化されたファイルをバックアップおよび復元する							
スパイ	りェア/クレーフェア							
1	スパイウェア/グレーウェア対策を有効にする 🙃							
Intelli	Ггар							
1	IntelliTrapの有効化 🕕							
プロセ	スメモリ検索 💶 💿							
1	ブロセスメモリ内の不正ブログラムを検索する 🕕							
7=.								
79-	7							
	この不正ブログラム検索設定でイベントが記録されたときにアラートを発令する							
備考	「挙動監視」または「ブロセスメモリ検索」のブロキシオブションを設定するには、「コンピュータの詳細)→「設定」→「一般] タブに移動し ます。							

記録された不正プログラム対策アラートは、消去するまで同イベントが発生してもアラート記録及び通知は行われません。

	ダッシュボード 処理	アラート	イベントとレポート	コンビュータ	ポリシー	管理
アラート リストビュー マ グループ化しない マ						
	コンビュータ すべてのコンビュータ ・					
	■ 表示 💼 消去 🌆 アラートの設定					
	時刻 ▼	重要度	アラート	対象	対象	箇所
•	2018-10-05 15:30	警告	不正プログラム対策アラート	2008R2aws	≔justi Defaul	t Real-Time Scan Configuration
•	2018-06-25 11:01	警告	不正プログラム対策アラート	test1206.lo	cal… Defaul	t Real-Time Scan Configuration

※消去とは、発生したイベントの対応や確認が完了したことを意味します。消去するとアラート解決メールが通知されます。
4.7. 隔離ファイルの復元方法

不正プログラムとして検知、隔離されているため、通常はバックアップやインストールメディアからの復旧をおこないます が、誤検知などでファイルを復旧しても再度隔離されてしまう場合や、隔離されたファイルを復元させたい場合は本手順 で復元させます。

誤検知か不正プログラムか判断できない場合にはサポートセンターまでお問い合わせください。

隔離ファイルを復元する前の準備

ファイルがリストアされた後に、再び同ファイルに対する隔離を繰り返してしまわないように、ファイルを元の場所にリスト アする前に検索除外の設定をしてください。コンピュータのエディタにおいて、該当ファイルの検索除外を設定する手 順を以下に示します。

同じ設定をポリシーのエディタで設定することも可能です。

(1)コンピュータのエディタを開き、[不正プログラム対策]→[検出ファイル]タブに進み、該当の隔離ファイルをダブルクリ ックしてプロパティ画面を開きます。期間は初期値1時間となっているため、検出期間を含む7日間やカスタム範囲を指 定します。

	概要	一般	Smart Protection	Connected Threat Defense	詳細	検出ファイル	不正プログラム対	策イベント			
•	不正プログラム対策	±2÷4					0	- /	+0.45		
	Webレビュテーション	1921		->160/a(1 +			Ч.	このヘーンを	(作用)并6		•
۲	ファイアウォール		期間: 過去1時間	*							~
θ	侵入防御	コンビ	ュータ: コンビュータ:		2008R2aws	-justi	•				G
0	変更監視										
0	セキュリティログ監視	面削	除	🖥 エクスポート 👻 🤗 復元	: 🕀 ś	ジウンロード	Q. 分析				
	アプリケーションコントロー	時刻	*	感染ファイル			不正プログ	די ⊐ <i>י</i> צ	(9	実行され	n <i>t</i> e
	インタフェース	2018-1	10-05 15:25:54	C¥Users¥Administrator¥A	kppData¥Lo	cal¥Temp¥2¥rdd∪a	azXq.••• Eicar_test_fi	le 2008R	2aws-justi	削除	
•	設定	2018-1	10-05 15:25:47	C¥Users¥Administrator¥A	kppData¥Lo	cal¥Temp¥2¥_LLwv	vJ6… Eicar_test_fi	le 2008R	2aws-justi	削除	
¢	アップデート										
х;	オーバーライド										

(2)「感染ファイル」でファイルが元々あった OS 上のファイル名とパスを確認しておきます。

一般		
不正プログラム情報		
検出時刻:	2018-01-19 14:53:53	
感染ファイル:	C:¥Documents and Settings¥Administrator¥デスクトップ¥新規テキストドキュメント.txt	
不正プログラム:	Eicar_test_1	
検索の種類:	リアルタイム	
実行された処理:	削除	

(3)引き続きコンピュータのエディタで、[不正プログラム対策]→[一般]タブに進み、それぞれの[不正プログラム検索設定]の[編集] ボタンをクリックし、不正プログラム検索設定のプロパティ画面を開きます。

※「リアルタイム検索」、「手動検索」、「予約検索」それぞれ必要に応じて検索設定を行います。

- 概要	一般 Smart Protection 詳細 隔離ファイル イベント					
😨 不正プログラム対策	不正プログラム対策 ▲ 設定: 継承(オン) ▼					
💮 Webレビュテーション	ステータス: 🎧 オン, リアルタイム					
🛞 ファイアウォール						
📀 侵入防御	リアルダイム検米					
● 変更監視	不正プログラム検索設定: Default Real-Time Scan Configuration ▼ 編集					
セキュリティログ監視 セキュリティログ監視	スケジュール: Every Day All Day 🔻					
🕮 インタフェース	≪ 「手動検索					
🛞 設定	□ 総承					
📮 アップデート	不正プログラム検索設定: Default Manual Scan Configuration ▼ 編集					
サーバーライド	予約検索					
	□ 総承					
	不正プログラム検索設定: Default Manual Scan Configuration ▼ 編集					
	「不正プログラム検索					
	不正プログラムの前回の手動検索: 2016-07-07 14:31					
	不正プログラムの前回の予約検索: なし					
	不正プログラムのクイック検索 不正プログラムのフル検索 ▼					

(4)検索設定のプロパティ画面で、[検索除外]タブをクリックします。

一般	検索除外	処理	オプション	割り当て対象	
検索除タ	۱ <u> </u>				
🔲 ディ	ィレクトリリ	スト:			
デ	んクトリリス	トの選択	Ŧ	編集	
27	ァイルリスト	÷			
7:	ァイルリストの	選択	Ŧ	編集	
27	マイル拡張子	リスト:			
7:	ァイル拡張子	リストの選択	• 5	福集	
✓ プロ	コセスイメー	・ジファイル	リスト:		
Pr	ocess Image	Files (Windo	ows) 🔻	編集	
備考	「プロセス・ み適用され	イメージフ ます。この	ァイルリスト 設定は、Dee	」設定はDeep Se p Security Virtual	ecurity Agentで検索が行われる場合の Applianceでは無視されます。

(5)検索除外タブで、[ファイルリスト] のチェックボックスを選択します。すでにファイルリストが選択されている場合は [編集] ボタンをクリック、またはプルダウンメニューから[新規…]を選択して新しいファイルリストを作成します。

💿 新規ファイルリン	ストのプロパティ - Google Chr 🗖 🖻 🗾 🌌
● 保護された通信	https://ss.anshinplus.jp/com.trendmic…
一般割り当て	対象
一般情報	
名前:	新規ファイルリスト
説明:	
トロマイル: (1行あた	- わ1つのファイル
サポートされてい	る形式:
懂書 「フロセス のみで、 :	イメージファイルリスト] で認識されるのはフルパス それ以外の形式は無視されます。
ファイル:	
ファイル	例: testfile.doc
ファイルパス	例: C:¥Documents¥testfile.doc
ワイルドカード (*)付きファイル:
ファイル*	1例:MyApp*.vApp
ノアイル:拡張子*	туј: МУАрр.v^
環境変数: \${ENV VAR}	例: S{myDBFile}
	an et al and
コメント: ファイルパス #コ	メント 例: C:¥temp¥file.txt #除外します
	<u>ОК</u> キャンセル

(6)ファイルリストのプロパティ画面で、リストアしようとしているファイルの場所とファイル名を、サポートされている形式に 従って[ファイル]欄に入力します。OK をクリックし、ファイルリストのプロパティ画面を閉じます。 ※ファイル名またはファイルのフルパスを指定します。

(7) OK をクリックし、不正プログラム検索設定のプロパティ画面を閉じます。

(8)コンピュータのエディタで、すべての[不正プログラム検索設定]の編集を終えたら、[保存] ボタンをクリックします。

これでファイルをリストアする準備は完了です。

隔離ファイル復元手順

◆Windows の場合

(1) 感染ファイルが元々あった OS 上のパスと日時を確認しておきます。

管理コンソールからコンピュータのエディタを開き、[不正プログラム対策]→[検出ファイル]を開き、該当の隔離ファイル のエントリをダブルクリックします。

一般	
「不正プログラム情報	
検出時刻:	2018-01-19 14:53:53
感染ファイル:	C:¥Documents and Settings¥Administrator¥デスクトップ¥新規テキストドキュメント.txt
不正プログラム:	Eicar_test_1
検索の種類:	リアルタイム
実行された処理:	削除

(2)復元ツールのダウンロード

ダウンロード URL

http://usersguide.anshinplus.jp/SS/QFAdminUtil.zip

ダウンロードした QFAdminUtil.zip を解凍します。※3 つのファイルが展開されます。

★隔離フォルダの場所

※隠しフォルダのためエクスプローラの設定で「すべてのファイルとフォルダを表示する」に設定します。

Windows Server 2003 の場合

Windows Server 2012R2 の場合

□ ファイルとフォルダの表示
 ③ すべてのファイルとフォルダを表示する
 ○ 隠しファイルおよび隠しフォルダを表示しない

>WindowsXP、2003

C:\Program Files\Trend Micro\AMSP\quarantine

または

 $C: {\tt \baselines} {\tt \baselines} C: {\tt \baselines} {\tt \baselines$

>Windows Vista、2008 以降

 $C: \ensuremath{\texttt{P}} rogram Data \ensuremath{\texttt{F}} Trend\ Micro \ensuremath{\texttt{A}} AMSP \ensuremath{\texttt{q}} uarantine$

解凍した「QDecrypt.exe」を実行します

暗号化された隔離ファイル(復元させたいファイル)を隔離フォルダから選択して「開く」を押します。

Quarantined file to decrypt								
ファイルの場所型:	🗁 quarantine	•	G 🤌 📂 🖽					
	名前 ▲	サイズ 種類	更新日時	属性				
	🖬 AK3BQ4P0.1 J8	1 KB 1J8 ファイル	2018/01/18 15:03	A				
最近使ったファイル	🖬 AK36SHQ0.1 JG	1 KB 1JG ファイル	2018/01/18 15:00	A				
	🖬 AK376MH0.1 JK	1 KB 1JK ファイル	2018/01/18 15:00	A				
	🖬 AMHQEKP0.1 J4	1 KB 1J4 ファイル	2018/01/19 13:53	A				
デスクトップ	🖬 AMHTEK20.1 J8	1 KB 1J8 ファイル	2018/01/19 13:55	A				
<u> </u>	🖬 AMIP5570.1 JC	1 KB 1JC ファイル	2018/01/19 14:10	A				
	amjrkvv0.1 jk	1 KB 1JK ファイル	2018/01/19 14:29	A				
マイ ドキュメント	🖬 AMJTLT40.1 JG	1 KB 1JG ファイル	2018/01/19 14:30	A				
	AML6PQV0.1 JC	1 KB 1JC ファイル	2018/01/19 14:53	A				
	🖬 AML88PT0.1 JK	1 KB 1JK ファイル	2018/01/19 14:53	A				
マイ コンピュータ	KU3mLSR_zip.RB0	1 KB RB0 ファイル	2018/01/18 15:03	A				
	┃ 🗟 Ku9wvgyc.zip.RB0 ┃ 種類: 1 Jk ● 単新日時	ファイル 2018/01/19 14:53 RB0 ファイル	2018/01/18 15:00	А				
	一 年代末:26	97X7F						
マイ ネットワーク								
	ファイル名(N): AML88PT0.1	JK	-	開((_)				
	ファイルの種類(T): All files (**)		キャンセル				
	All thes (*.*.	, ,		11207				

復元するファイルの保存先を指定して[保存]を押します。

File to save decry	ile to save decrypted data to ?							
保存する場所①:	🞯 デスクトップ		•	G 🖄 📂 🎰				
最近使ったファイル び デスクトップ マイ ドキュメント マイ コンピュータ	 マイ ドキュメント マイ コンピュータ マイ ネットワーク desktop.ini Mozilla Firefox Symantec Backu bk Debug View Crystal Disk Mark QFAdminUtil への ドキュメントrtf 	p Exec 10d for Windows Servers)ショートカット						
マイ ネットワーク) ファイル名(<u>N</u>): ファイルの種類(<u>T</u>):	新規テキスト ドキュメント.txt All files (*.*)		•	保存(S) キャンセル			

「Decryption successful!」と表示され、指定したファイル名で元のファイルが復元されます。

◆Linux の場合

復元ツールは Windows 版のみのため、Windows の場合の手順を参照ください。

★隔離ディレクトリ

/var/opt/ds_agent/guests/0000-0000-0000/quarantined/

5. 不正 WEB サイトブロック 『Web レピュテーション』

Web レピュテーション設定について説明いたします。

5.1. Web レピュテーションの有効化

(1)管理 Web コンソールにログオンしてください。

コンピュータより、Web レピュテーションを設定するサーバをダブルクリックします。

ダッシュボード	7 5 -ŀ	イベントとレポート	コンピュータ	ポリシー	管理			
	コノビ	ュータ サブグループを含	む ▼ グループ別 ▼	-			♀ 検索	•
		新規 🖌 💼 削除 🥅	詳細 処理 -	イベント 🛛 🖾 エ	クスポート 🗸	📑 列		
		名前▼ 説明	l プラッ	トフォーム ポリシ	-	ステータス	前回の通信	前回成功したアップデート
	E =2	ビュータ (2)						
		cent65	Red I	Hat Enter Linux	Server 😑	管理対象 (オンライン)	3分前	37分前
		2008r2	Micro	soft Wind Base I	Policy 😑) 管理対象 (オンライン)	1分前	17 時間 前
	~							

(2)サーバの設定画面が表示されます。

「Web レピュテーション」をクリックします。

- 概要	一般処理イベント				
📀 不正プログラム対策	龄		_		~
💿 Webレビュテーション	ホスト名:	2008r2	×	(前回使用されたIP: 61.120.61.62)	
🎯 ファイアウォール	30.1-m. 1说明:				
🧐 侵入防御					
🔘 変更監視					
またまっしティログ監視	プラットフォーム:	Microsoft Windows Server 2008 R2 (64 bit) Build 7600			
CIESSIASI	グループ:	コンピュータ	-		
📟 インタフェース	ポリシー:	Base Policy	-	編集	
💮 設定 🤐	資産の重要度:	tal.	~	編集	
見 アップデート	セキュリティアップデートのダウンロード 元:	トレンドマイクロアップデートサーバ	~	羅集	
<u>∯</u> オーバーライド	Г.Х.F-92				

(3)Web レピュテーションのステータスを「オン」にして「保存」をクリックしてください。

これで Web レピュテーションが有効になります。継承(オン)になっている場合は既に有効になっています。



5.2. Web レピュテーション設定

Web レピュテーションモジュールはレピュテーションの評価に基づいて Web ページをブロックします。これらの評価は Web ページのリンク、ドメインと IP アドレスの関係、スパムの送信元、スパムメッセージ内のリンクなど、複数の評価項目 の合計で、トレンドマイクロのサーバに問い合わせて使用します。Web レピュテーションはトレンドマイクロから評価を取 得することで、利用可能な最新情報を使用して有害ページをブロックします。

(1)「一般タブ」

初期値では(低)危険と認識される Web サイト接続をブロックします。

セキュリティレベルを変更する場合は継承のチェックを外してローカルのコンピュータに設定するか、ポリシーを設定することも可能です。

設定の決定は「保存」をクリックしてください。

※セキュリティレベルを中・高に設定するとWebサイトへの接続安全性は高まりますが、危険ではないサイトをブロックしてしまう可能性も高まります。



■セキュリティレベル

Web レピュテーション評価システムでは、URL に次のリスクレベルを割り当てます。

- ・危険:不正、または脅威の既知の発信源であると確認された URL
- ・非常に不審:不正または脅威の発信源である可能性が疑われた URL
- ・不審:スパムメールに関連付けられている、または感染している可能性のある URL
- ・安全: リスクのない URL

高: 次のリスクレベルのページをブロックします。

- ・危険
- ・非常に不審
- •不審

中: 次のリスクレベルのページをブロックします。

- ・危険
- ・非常に不審

低: 次のリスクレベルのページをブロックします。

・危険

トレンドマイクロでテストしていないページをブロック:次のリスクレベルのページをブロックします。 ・トレンドマイクロで規定していないレベル

(2)「除外タブ」

許可およびブロックサイトを設定することができます。

[許可] リストに含まれているURLは、安全性の評価に関係なくアクセスできます。一度に複数のURLを追加できますが、 その場合は改行で区切る必要があります。[許可] リストにURLを追加する場合は、同じドメインを持つすべてのURLを 許可するのか、それとも特定のURLを許可するのかを選択します。

[ブロック] リストに含まれているURL、およびこのリストで指定したキーワードを含むURLは、常にブロックされます。ただし、[許可] リストに優先エントリが存在する場合は除きます。一度に複数のURLまたはキーワードを追加できますが、その場合は改行で区切る必要があります。URLをブロックする場合は、ドメイン内のすべてのURLをブロックするのか、特定のURLをブロックするのか、それとも特定のキーワードを含むURLをブロックするのかを選択します。

決定は「保存」をクリックしてください。

- 概要	一般 除外 Smart Protection 詳細 イベント	
😨 不正プログラム対策	「許可 —	
💮 Webレビュテーション	許可リストに追加するURL (1行に1つずつ):	(注前除) エクスポート
🐵 ファイアウォール		許可するURL▲ 範囲
🛞 侵入防御		
🔘 変更監視	iu 3) الم عاد () () () () () () () () () () () () ()	
🔇 セキュリティログ監視		
🎟 インタフェース	●ドメイン内すべてのURLを許可する	
🎲 設定 .	< ORL変計する	
🗐 アップデート		
碞 オーバーライド		
	イフレック ブロックリストに追加するURL(1行に1つずつ)	
		プロックするURL▲ 範囲
	iu 200 مار غاز () بار غ	
	●ドメイン内すべてのURLをブロックする	
	○ URLをブロックする	
	○ このキーワードを含むURLをブロックする	
		保存 閉じる

5.3. Web レピュテーションイベント

危険サイト接続をブロックした場合、Web レピュテーションイベントとして記録します。

概要	- 般 除外 Smart Protection 詳細 イベント	
🦁 不正プログラム対策	Webレビュテーションイベント すべて マ グループ化しない マ Q 検索	
💮 Webレビュテーション	期間: 過去18時間	
圆 ファイアウォール	⊐ℋュータ: ⊐ℋュータ: ♥ 2008/2 ♥	· ·
📀 侵入防御	■ 表示 🚯 エクスポート 🔹 省 自動タグ付け 🔢 列	
◎ 変更監視	■ 時刻 ▼ コンピュータ URL タグ	リスク
🔇 セキュリティログ監視	2014-07-16 17:40:40 2008r2 http://wrs21.winshipway.com/favicon.ico	危険
● インタフェース	2014-07-16 17:40:39 2008r2 http://wrs21.winshipway.com/	危険
🛞 設定	<	

イベントをダブルクリックすると詳細が表示されます。

ſ	一般 タグ	
Г-	一般情報	
8	時刻:	2014-07-16 17:40:39
:	コンピュータ:	2008r2
;	送信元:	Agent
	URL:	http://wrs21.winshipway.com/
		再評価
-	ランク:	100 = 資産評価×重要度 = 1 × 100
!	リスク:	危険
		許可リストに追加

5.4. Web レピュテーションアラート通知

アラートを発するように設定されている場合にアラートとして記録され、指定された管理者宛てにメール通知します。

	一般 路外 Smart Protection 詳細 イベナ
💿 不正プログラム対策	ブロックページー
🥌 Webレビュテーション	ピ 総承 ゴロックされているページの再評価をユーザが依頼できるようにするため、ブロックページに表示するリンクを指定します。
🐵 ファイアウォール	
📀 侵入防御	997- Inttp://sitesafety.trendmicro.com 例: http://intranet.supportdesk.example.com法たばmailto:administrator@example.com
🍈 変更監視	「「「」 なかいシンを使用すると、エンド フーザが特定のWebth-ひとの認備を解明、評価が開始っていると思われるサイトの面評価を要求できる、Trend Micro Site Safety
🔇 セキュリティログ監視	Centerl :移動します。http://sitesafety.trendmicro.com/
🔲 インタフェース	۲۶۶-۱۰
	(マラート: れ)

■「詳細タブ」 アラートを「はい」に設定してください。「継承(はい)」の場合は有効になっています。

記録されたれた Web レピュテーションアラートは、消去するまで同イベントが発生してもアラート記録及び通知は行われません。

	ダッシュボード	アラート	イベントとレポート ニ	ひピュータ	ポリシー	管理					
7	アラート リストビューマ グルーガヒしないマ										
	コンビュータ: すべてのコンピュータ										
	コブロバティ <u> </u> 消去	🕵 アラート	の設定								
	時刻 🔻	重要度	アラート	対象	件名:						
Δ	2014-07-17 11:29	警告	Webレビュテーションイベントアラート	2008r2							

※消去とは、発生したイベントの対応や確認が完了したことを意味します。消去するとアラート解決メールが通知されます。

5.5. Web レピュテーションブロック画面

■Web ブラウザによるブロック画面

🧭ブロックされたページ - Windows Internet Explorer		_ 🗆 🗵
Co o la http://wrs21winshipway.com/	💌 🗟 🐓 🗙 🔁 Bing	₽ •
😭 お気に入り 👍 🕘 おすすめサイト・ 🧶 Web スライス ギャラリー・		
🏉 ブロックされたページ	🏠 • 🔊 • 🖃 🌧 • ページ(P)・ セーフ	アティ(S)▼ ツール(O)▼ @▼
Trend Micro Deep Security		<u> </u>
このページは安全ではありません。		
URL: wrs21.winshipway.com/		
リスクレベル: 危険		
安全のため、このページは管理者によってブロックされました。		
┌ 実行できる操作		
 前のページに戻る この判定についてフィードバックする 		
	ィョンによるブロック、Trend Micro Deep Securi	ty Agent 9.0.0.3500
Copyright © 2013 Trend Micro Inc. All rights reserved.		-
・ ページが表示されました	💊 インターネット 保護モード: 無効	🐴 🔹 🔍 100% 🔹 🎢

6. 不正な通信を防御『ファイアウォール』

ファイアウォール設定について説明いたします。

6.1. ファイアウォールの有効化

(1)管理 Web コンソールにログオンしてください。

コンピュータより、ファイアウォールを設定するサーバをダブルクリックします。

ダッシュボード	7 5 -ŀ	イベントとレポート	コンピュータ	ポリシ	- 管理				
コンピュータ	שיר	ニータ サブグループを含	は ▼ グループ	181 -				Q 検索	•
		新規 🖌 <u> </u> 削除 🔲	詳細 処理 -		🔄 エクスポート	•	王 列		
		名前 🔻	A :	ブラットフォーム	ポリシー		ステータス	前回の通信	前回成功したアップデート
	E	ビュータ (2)							
		cent65	í	Red Hat Enter	Linux Server	0	管理対象 (オンライン)	3分前	37分前
		2008r2	1	Microsoft Wind	Base Policy	0	管理対象 <mark>(</mark> オンライン)	1分前	17 時間 前
	~~								

(2)サーバの設定画面が表示されます。

「ファイアウォール」をクリックします。

コンピュータ: cent65				0 ^
板要		一般 処理 イベント		
😨 不正プログラム対策		一般		
💿 Webレビュテーション		ホスト名: 	cent65 ×	(前回使用されたIP: 54.95.118.236)
🐵 ファイアウォール		1.0.1.0L.		
⑧ 侵入防御				
🌍 変更監視				
🔇 セキュリティログ監視		プラットフォーム:	Red Hat Enterprise 6 (64 bit) (2.6.32- 431.11.2.el6.centos.plus.x86_64)	
📟 インタフェース		グループ:	⊐2ta-9]
🎲 設定	~	ポリシー:	Base Policy	編集
	-	資産の重要度:	tal. 🗸	編集
□ , 1921 – F	- 11	セキュリティアップデートのダウンロード	プライマリテナントのRelayグループ	福集
🕂 🕂 オーバーライド		元:		

(3)ファイアウォールのステータスを「オン」にして「保存」をクリックしてください。

ファイアウォールが有効になります。継承(オン)になっている場合は既に有効になっています。

	概要	一般 インタフェース制限 攻撃の予兆 詳細 イベント	
0	不正プログラム対策		
	Webレビュテーション	ファイアワオールステータス: オン	
8	ファイアウォール	ファイアウォールステートフル設定	
8	侵入防御	グローバル (オペてのインタフェース) 継承 (Enable Stateful Inspection)	編集
0	変更監視	etnu - 22:00:0A7/E:11.5F (DHCP) 総承 (Enable Stateful Inspection)	編集
8	セキュリティログ監視	ボート検索	
	インタフェース	前回のホートの検索: なし 検索されたボート: なし	
-	設定	親いているポート: なし	
E.	アップデート	オープンボートの検索 ボート検索のキャンセル	
+ 4	オーバーライド	削当てられたファイアウォールルール	
		割り当て唐り当て離除 📰 プロパティ… 🔂 エクスポート 🔹 🏭 列…	
		名前▲ 処理の種類 優先度 方向 フレームの… ブロトコ… 送信元P	送信元M/
		Ballow solicited ICMP replies 許可 0-最低 受信 IP ICMP 任意	任意
		◎ Allow solicited TCP/UDP replies 許可 0-最低 受信 IP TCP+UDP 任意	任意
		◎ ARP 許可 0-最低 受信 ARP なし なし	任意
		DHCP Server 建制的に許可 2 - 標準 受信 IP UDP 任意	任意

6.2. ファイアウォールルール概要

Agent は双方向のステートフルなファイアウォール保護を提供します。DoS 攻撃を阻止し、すべての IP ベースのプロトコルとフレームタイプに対応するほか、ポート(L4)、IP アドレス(L3)、および MAC アドレス(L2)をフィルタリングできます。

ファイアウォールでは、次の条件を使用して、トラフィックの送信元と送信先を判断できます。

- ・IP アドレス
- ・MAC アドレス
- ・ポート

①IP アドレス

IP アドレスの定義には、次のオプションを使用できます。

- ・任意:アドレスの指定がないので、送信元または送信先として任意のホストが対象
- ・単一 IP: IP アドレスを使用してコンピュータを特定
- ・マスクされている IP: 同じサブネットマスクを使用するすべてのコンピュータにルールを適用
- ・範囲: IP アドレスが特定の範囲内にあるすべてのコンピュータにルールを適用
- ・IP: IP アドレスが連続しない複数のコンピュータにルールを適用する場合に使用
- ・IP リスト: IP アドレスのコンポーネントリストを使用してホストを定義

②MAC アドレス

- MAC アドレスの定義には、次のオプションを使用できます。
- ・任意: MAC アドレスの指定がないので、すべてのアドレスにルールを適用
- ・単一 MAC: 特定の MAC アドレスにルールを適用
- ・MAC: ここで指定された複数の MAC アドレスにルールを適用
- ・MAC リスト: MAC リスト内の MAC アドレスにルールを適用

③ポート

- ポートの定義には、次のオプションを使用できます。
- ・任意: 単一のポートにルールを適用
- ・ポート: ここで指定された複数のポートにルールを適用
- ・ポートリスト: ポートリストにルールを適用

④トランスポートプロトコル

ルールがインターネットプロトコル (IP) のフレームの種類を対象としている場合、プロトコルフィールドが有効になり、管理者は分析するトランスポートプロトコルの指定を求められます。使用できるプロトコルオプションは次のとおりです。 ・任意 (ファイアウォールはプロトコルで区別しない)

- •ICMP
- •ICMPV6

- •IGMP
- •GGP
- •TCP
- PUP
- •UDP
- •IDP
- •ND
- •RAW
- •TCP+UDP
- ・その他 (プロトコル番号の指定が必要)

⑤方向

ファイアウォールは双方向のファイアウォールです。ホストへのトラフィック(受信)とホストからネットワークへのトラフィック(送信)の両方にルールを適用できます。

注意:1つのファイアウォールルールは一方向にのみ適用されます。このため、特定の種類のトラフィックを対象とする ファイアウォールルールはペアにしてください。

⑥TCP ヘッダフラグ

TCPトラフィックについては、ルールを適用するTCPフラグを選択できます。すべてのフラグにルールを適用するのでない場合、次のいずれかを選択できます。

・任意のフラグ

- •URG
- •ACK
- •PSH
- •RST
- •SYN
- $\bullet \text{FIN}$

⑦フレームの種類

「フレーム」とはイーサネットフレームを指し、フレームで送信されるデータは、使用可能なプロトコルによって指定されます。

インターネットプロトコル (IP)、アドレス解決プロトコル (ARP)、および逆アドレス解決プロトコル (RARP) が、現在のイー サネットネットワークで使用されている最も一般的なプロトコルですが、リストから [その他] を選択することで、その他の 任意のフレームの種類を「フレーム番号」で指定できます。

⑧ファイアウォールルールの処理

ファイアウォールルールでは、次の処理が可能です。

・許可: ルールと一致するトラフィックの通過を明示的に許可し、その他のトラフィックは黙示的に拒否します。
・バイパス: ファイアウォールと侵入防御分析の両方のバイパスをトラフィックに許可します。この設定は、ネットワーク負荷の高いプロトコルにのみ使用します。この処理では、ポート、方向、およびプロトコルのみを設定できます。
・拒否: ルールと一致するトラフィックを明示的にブロックします。

・強制的に許可:他のルールで拒否されるトラフィックを強制的に許可します。

注意:強制的に許可ルールで許可されるトラフィックは、侵入防御モジュールによる分析の対象となります。 ・ログのみ:トラフィックはログに記録されるだけです。その他の処理は実行されません。

⑨「バイパス」ルールの詳細

バイパスルールはネットワーク負荷の高いプロトコルを対象に設計されています。ネットワーク負荷の高いプロトコルでは、 ファイアウォールや侵入防御モジュールによるフィルタリングが必要とされず、望まれてもいないためです。バイパスル ールには、次の特徴があります。

バイパスルールの条件と一致するパケットは、次のように処理されます。

・ステートフル設定の条件の対象にならない

・ファイアウォールと侵入防御分析の両方をバイパスする

バイパスされるトラフィックにはステートフルインスペクションが適用されないので、一方向のトラフィックがバイパスされて も、逆方向の応答は自動的にはバイパスされません。したがって、受信トラフィック用と送信トラフィック用のバイパスル ールは、必ずペアで作成および適用します。

⑩「強制的に許可」ルールの詳細

「強制的に許可」オプションでは、拒否処理の対象となるトラフィックの一部を除外します。他の処理との関係を下に示します。強制的に許可ルールは、バイパスルールと同じ効果があります。ただし、バイパスルールとは異なり、この処理によってファイアウォールを通過するトラフィックは侵入防御モジュールによる監視の対象となります。一般に有効にする強制的に許可ルールの初期設定は、次のとおりです。

·許可

·拒否

·強制的に許可

(1)ファイアウォールルールのシーケンス

コンピュータに届くパケットは、ファイアウォールルール、ファイアウォールステートフル設定条件、および侵入防御ルールの順に処理されます。

受信および送信でファイアウォールルールが適用される順序は次のとおりです。

1.優先度4(最高)のファイアウォールルール

1.バイパス

2.ログのみ(ログのみルールは優先度4(最高)にのみ割り当て可能)

3.強制的に許可4.拒否

2.優先度3(高)のファイアウォールルール
 1.バイパス
 2.強制的に許可
 3.拒否

3.優先度2(標準)のファイアウォールルール
1.バイパス
2.強制的に許可
3.拒否

4.優先度1(低)のファイアウォールルール 1.バイパス

- 2.強制的に許可
- 3.拒否

5.優先度0(最低)のファイアウォールルール

1.バイパス

2.強制的に許可

3.拒否

4.許可(許可ルールは優先度0(最低)にのみ割り当て可能)

【注意】コンピュータに有効な許可ルールがない場合、拒否ルールでブロックされていないかぎり、すべてのトラフィック が許可されます。許可ルールを1つ作成したら、許可ルールの条件を満たしていないかぎり、その他すべてのトラフィッ クがブロックされます。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールでブロックされていないかぎ り、常に許可されます。

迎各ファイアウォールルールの関係

Deep Security ファイアウォールルールには、ルール処理とルール優先度があります。この2つのプロパティを同時に使用することによって、非常に柔軟で強力なルール設定を作成できます。他のファイアウォールで使用されているルール 設定では実行順にルールを定義する必要がありますが、それとは異なり、Deep Security ファイアウォールルールは、ル ール処理とルール優先度に基づいて決定論的な順序で実行されます。これは、定義された順序や割り当てられた順序 とは無関係です。 13ルール処理

各ルールには、以下の4つのルール処理のいずれかを設定できます。

1.バイパス: パケットがバイパスルールに一致した場合は、同じ優先度の他のルールにかかわらずファイアウォールと侵入防御エンジンを通過します。

2.ログのみ:パケットがログのみルールに一致した場合は、通過してイベントがログ記録されます。

3.強制的に許可: パケットが強制的に許可ルールに一致した場合は、同じ優先度の他のルールにかかわらず通過します。

4.拒否:パケットが拒否ルールに一致した場合は、破棄されます。

5.許可: パケットが許可ルールに一致した場合は、通過します。許可ルールのいずれにも一致していないトラフィックは すべて拒否されます。

■許可ルールを実装すると、許可ルールに一致しないその他すべてのトラフィックが拒否されます。



■拒否ルールを許可ルールに実装して、特定の種類のトラフィックをブロックすることができます。



■強制的に許可ルールを拒否トラフィックに適用すると、例外のみ通過させることができます。



6.3. ファイアウォールルール設定

多数の一般的なOSおよびアプリケーション用のファイアウォールルールが用意されていますが、独自のカスタムルール を作成することもできます。カスタムルールを作成する場合は、新しいファイアウォールルールを作成します。ルールを ポリシーで作成することによりポリシーを割り当てているコンピュータ全てにルールを割り当てることもできます。

(1)ファイアウォールルールを設定するには、「割り当て/割り当て解除」をクリックします。

_ 100 .20		一般	インタフェース制限	攻撃の予測	L I¥#B	イベント					
🤇 不正プログラム対策	E	[7747	ウォール								
🎐 Webレビュテーション	,	7747	ウォールステータス: [:	オン		~	副オフ,23)	ルール			
 ファイアウォール 侵入防御 変更監視 		ファイア <i> 「ファイア</i> グロ ・ ・	ウォールステートフル& コーバル (すべてのイン eth0 - 22:00:0A:7E:1	設定 - タフェース) 11:5F (DHCP)			継承 (Enable State 継承 (Enable State	ful Inspection	n) V #	集
セキュリティログ監絡	R	「ポート検	·索	ta.							
インタフェース		検索され	n = 1:00根本: したポート:	ねし							
設定	~<	聞いてい	いるボート:	なし							
アップデート	_		オープンボートの検索		ボート検索の	キンセル					
オーバーライド		▶ 割り当て 割り	られたファイアウォーノ 当て唐り当て解除。	レルール	जिन 🚯	Eクスポート •	14 列				
		名龍	й ^		処理の種類	優先度	方向	フレームの	プロトコ	送信元IP	送信元M/
		🙆 Alk	ow solicited ICMP rep	olies	許可	0-最低	受信	IP	ICMP	任意	任意
		🛞 Alk	ow solicited TCP/UDP	P replies	許可	0 - 最低	受信	IP	TCP+UDP	任意	任意
		🔞 AR	P		許可	0 - 最低	創愛	ARP	なし	ねし	任意
		🛞 DH	ICP Server		強制的に許可	2 - 標準	受信	IP	UDP	任意	任意
		💿 DN	IS Server		強制的に許可	2 - 標準	受信	IP	TCP+UDP	任意	任意
		0.0	main Official (TOD)		10.77	0.是任	∰{\$	ID.	TOP	Demois Ore	/ri ete
		00 00	main Client (TCP)		8+"J	0 - 100155	~18		101	Domain Con	1T.S

(2)表示フィルタにより「割り当てあり」や「割り当てなし」、「処理の種類別」や「優先度別」などで表示させることができま す。「すべて」を選ぶと定義済みのすべてのルールが表示されます。チェックボックスにチェックを入れ「OK」をクリックす ることで、選択したルールが割り当てされます。規定で複数アプリケーションの許可ルールが割り当てされていますが、 不必要なルールはチェックを外して割り当て解除することができます。

ファイアウェ	ォールルール	ব্≺ব্দ্	処理の種類別、	r				Q #	i索		-
新規 ·	• 🏦 前版紀	== ブロバテ	イ 门 複製	 「 」 エクスポー	۰ - ا	列					
	名前 ▲				優先度	方向	フレームの	プロトコ	送信元IP	送信元MAC	送们
■ 強制的に調	许可 (42)										- 1
🛞 🗆 1	DHCP Client				2 - 標準	受信	IP	UDP	任意	任意	DH
🛞 🗹 🖬	DHCP Server				2 - 標準	受信	IP	UDP	任意	任意	DH
🛞 🗹 🖬	DNS Server				2 - 標準	受信	IP	TCP+UDP	任意	任意	任馬
🛞 🗆 🛙	Domain Client (UDP)			2 - 標準	受信	IP	UDP	Domain Con	任意	Dor
🛞 🗆 🛙	Domain Control	ler (UDP)			2 - 標準	受信	IP	UDP	任意	任意	任意
🛞 🗹 B	ICMP Echo Req	quest			2 - 標準	受信	IP	ICMP	任意	任意	なし
🛞 🗹 B	Microsoft SQL S	Server			2 - 標準	受信	IP	TCP+UDP	任意	任意	任意
🛞 🗹 B	MySQL Server				2 - 標準	受信	IP	TCP+UDP	任意	任意	任尨
🛞 🗹 🖬	NetBios Name S	Service			2 - 標準	受信	IP	UDP	任意	任意	Net
🛞 🗆 B	Network Time P	rotocol			2 - 標準	受信	IP	UDP	任意	任意	任意
🛞 🗆 6	Off Domain Exc	eptions - ARP			2 - 標準	送信	ARP	なし	なし	任意	なし
🛞 🗆 🛙	Off Domain Exc	eptions - DHCF	P Client		2 - 標準	送信	IP	UDP	任意	任意	DH
🛞 🗆 B	Off Domain Exc	eptions - DNS			2 - 標準	送信	IP	TCP+UDP	任意	任意	任馬
🛞 🗆 6	Off Domain Exc	eptions - Doma	in Client (TCP)		2 - 標準	送信	IP	TCP	任意	任意	任意
🛞 🗆 🛙	Off Domain Exc	eptions - Doma	in Client (UDP)		2 - 標準	送信	IP	UDP	任意	任意	任加
🛞 🗆 🖬	Off Domain Exc	eptions - GRE			2 - 標準	送信	IP	その他: 47	任意	任意	ねし
🛞 🗆 6	Off Domain Exc	eptions - HTTP	(S)		2 - 標準	送信	IP	TCP	任意	任意	任意
<											>
									ок	*	ャンセル

(3)ファイアウォールルールの変更

ルールをコンピュータに対して編集するには、ルールを右クリックして [プロパティ...] をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)...]をクリックします。

※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が 適用されます。

例) ftp サーバへの接続送信元を IP アドレス 1.1.1.1 からのみ制限

ファイアウォールルール 割り当てあり マ 処理の種類別 マ				Q 8	ί¢		
📑 新規 🔹 🏦 削除 📰 プロパティ 📑 複製 🔂 エクスポー	-t • 🏢	列					
名前 🔺	優先度	方向	フレームの	プロトコ	送信元IP	送信元MAC	送伯
e — –	2 - 標準	受信	IP	TCP+UDP	任意	任意	任意
■ 詩町 (15)							
	0-最低	受信	IP	ICMP	任意	任意	なし
	0-最低	受信	IP	TCP+UDP	任意	任意	任意
🛞 🗹 🗷 ARP	0-最低	受信	ARP	なし	ねし	任意	なし
🛞 🗹 🖬 Domain Client (TCP)	0-最低	受信	IP	TCP	Domain Con	任意	Dor
B Domain Controller (TCP)	0-最低	受信	IP	TCP	任意	任意	任意
🛞 🗹 🖻 FTP Server	0-最低	受信	IP	TCP	任意	任意	任意
	0-最低	受信	IP	TCP	任意	任意	任意
IMAP Server	0-最低	受信	IP	TCP	任意	任意	任意
🔞 🗹 🖻 Microsoft Exchange Server	0-最低	受信	IP	TCP	任意	任意	任意
🛞 🗹 💌 POP3 Server	0-最低	受信	IP	TCP	任意	任意	任意
😁 🗹 🖻 Remote Access RDP	0-最低	受信	IP	TCP	任意	任意	任焉
Remote Access SSH SH SH	0-最低	受信	IP	TCP	任意	任意	任意
SMTP Server	0-最低	受信	IP	TCP	任意	任意	任意
😁 🗹 🖻 VMware vCenter Server	0-最低	受信	IP	TCP+UDP	任意	任意	任焉
🧐 🗹 💌 Web Server	0-最低	受信	IP	TCP	任意	任意	任意。
<							>
					ОК	\$ \$73	ノセル

「ファイアウォールルールプロパティタブ」

パケット送信元:コンピュータに対して設定する場合は継承のチェックを外し、単一 IP を選択します。

入力欄に IP アドレスを入力します。「OK」クリックすることで設定が有効になります。

. <u></u>		
名前:	FTP Server	
≣党¤月:	Allow incoming traffic to an FTP Server	
処理:	ifir可	
優先度:	0-最低	
バケット方向:	受信	
フレームの種類:	IP 🗸	🗌 選択以外
プロトコル:	TCP	🗌 選択以外
パケット送信元 ―		
パケット送信元 — IP: 🗌 維承	₩-IP: V 1.1.1.1 ×	🗌 🗌 選択以外
『ケット送信元 — IP: 維承 MAC:	単一IP: ♥ [1.1.1.1] × 任意 ♥	□ 選択以外
パケット送信元── IP: □ 維承 MAC: ポート: ☑ 維承	単−IP: V [1.1.1.1] × 任意 V 任意 V	 選択以外 選択以外 選択以外 選択以外
『ケット送信元── IP: □ 維承 MAC: ポート: ☑ 継承	単-IP: ▼ 1.1.1.1 × 任意 ▼ 任意 ▼	 選択以外 選択以外 選択以外
『ケット送信元 ── IP: □ 継承 MAC: ポート: ☑ 継承 『ケット送信先 ── IP: ☑ 継承	 単-IP: 【1.1.1.1] X 任意 ✓ 	□ 選択以外 □ 選択以外 □ 選択以外 □ 選択以外
ドケット送信元 ── IP: □ 継承 MAC: ボート: ☑ 継承 ドケット送信先 ── IP: ☑ 継承 MAC:	 単-IP: ▼ 1.1.1.1 X 任意 ✓ 任意 ✓ 任意 ✓ 	□ 選択以外 □ 選択以外 □ 選択以外 □ 選択以外 □ 選択以外

FTP Server ルールの送信元 IP アドレスが「任意」」から 1.1.1.1 へ変更されました。

ファイアウォールルール 割り当てあり ▼ 処理の種類別 ▼		♀ 検索						
	۶ - 👪	il]						
名前 🔺	優先度	方向	フレームの	プロトコ	送信元IP	送信元MAC	送伯	
	- 08-1-	216			17.22	17722	11.2	
🌐 🗹 🖻 Windows File Sharing	2 - 標準	受信	IP	TCP+UDP	任意	任意	任意	
■ 許可 (15)	<mark>0</mark> - 最低	受信	IP	ICMP	任意	任意	なし	
	<mark>0</mark> - 最低	受信	IP	TCP+UDP	任意	任意	任意	
🥮 🗹 🖬 ARP	<mark>0</mark> - 最低	受信	ARP	なし	なし	任意	なし	
	<mark>0</mark> - 最低	受信	IP	TCP	Domain Con	任意	Dor	
🛞 🗹 🖻 Domain Controller (TCP)	0-最低	受信	IP	TCP	任意	任意	任意	
🛞 🗹 ■ FTP Server	0-最低	受信	IP	TCP	1.1.1.1	任意	任	

(4)ファイアウォールルールの作成

既定のルールがない場合は、独自にルールを作成できます。

新規から「新しいセキュリティログ監視ルール」を選択します。

1	ファイアウォールルール 割り当	てあり 👻 処理の種業	♀ 検索							,	
	📑 新規 🖌 🏦 削除 📰 プロ	コパティ 📋 複製	🔂 エクスボー	+ • 🔛	5IJ						
	📑 新規ファイアウォールルール			優先度	方向	フレームの	プロトコ	送信元IP	送信元MAC	送伯	,
1	🗉 🔄 ファイルからインボート										
	🛞 🗹 🖻 DHCP Server	1		2 - 標準	受信	IP	UDP	任意	任意	DH	
	🛞 🗹 🖻 DNS Server			2 - 標準	受信	IP	TCP+UDP	任意	任意	任意	

「一般タブ」一般情報:ルールの名前、処理、優先度、パケット方向、フレームの種類

パケット送信元、パケット送信先を設定後、OK をクリックすることでルールが作成され割り当てされます。

一般 オラシ	ョン 割り当て対象	
一般情報		
名前:	新規ファイアウォールルール	
兑明:		
処理:	許可 🖌	
優先度:	0 - 最低	
パケット方向:	受信・	
フレームの種類	IP V	□ 選択以外
プロトコル:	TCP V	□ 選択以外
「ケット送信元-		
IP:	意	□ 選択以外
MAC:		□ 選択以外
шары, ро Парадор		_
π-r. f	意	□ 道択以外
《ケット送信告-		
IP:	意	□ 選択以外
MAC: D		1994mis Loi
1	I I I I I I I I I I I I I I I I I I I	□ 嗟扒以外
ポート:	<u>主意</u>	□ 選択以外
7	トーr. ポートリスト:	
皆定フラグ — ^上		
A 100 million and 100 million	7	

(5)ファイアウォールルールの確認/変更

新しく作成したルールにチェックがついていれば割り当てされ有効になっています。

ルールをコンピュータに対して編集するには、ルールを右クリックして [プロパティ...]をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)...]をクリックします。

※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が 適用されます。

設定を終了するには、「OK」をクリックしてください。

ファイアウォールルール 割り当てあり 💌 処	ファイアウォールルール 割川当てあり ▼ 処理の種類別 ▼									
📑 新規 🖌 👔 削除 🥅 ブロパティ [] 複製 🛛 🔂	エクスポー	÷ •	🌆 列						
名前 🔺	優先度	方向	7 7	カトコ	送信元IP	送信元	送信元ポート	送信	送信	送信先ポート
		218		0. 00.	11.35	11.30	17.20	11722	11.35	
■ 許可 (16)										
	0-最低	受信	IP I	CMP	任意	任意	なし	任意	任意	なし
Image: Allow solicited TCP/UDP replies	0-最低	受信	IP T	CP+UDP	任意	任意	任意	任意	任意	任意
🛞 🗹 🖬 ARP	<mark>0-</mark> 最低	受信	A t _e	il.	なし	任意	なし	なし	任意	なし
🞯 🗹 🖬 Domain Client (TCP)	<mark>0 - 最低</mark>	受信	IP T	CP	Domain	任意	Domain Co	任意	任意	任意
🛞 🗹 🖬 Domain Controller (TCP)	<mark>0-</mark> 最低	受信	IP T	CP	任意	任意	任意	任意	任意	Domain Cont
🔞 🗹 🖻 FTP Server	0-最低	受信	IP T	CP	1.1.1.1	任意	任意	任意	任意	FTP (20, 21)
🎯 🗹 🖻 IDENT	<mark>0</mark> - 最低	受信	IP T	CP	任意	任意	任意	任意	任意	IDENT (113)
🞯 🗹 🖻 IMAP Server	<mark>0</mark> - 最低	受信	IP T	CP	任意	任意	任意	任意	任意	IMAP (143, 5
🎯 🗹 🖻 Microsoft Exchange Server	<mark>0</mark> - 最低	受信	IP T	CP	任意	任意	任意	任意	任意	Exchange Se
🎯 🗹 💌 POP3 Server	<mark>0</mark> -最低	受信	IP T	CP	任意	任意	任意	任意	任意	POP3 (110)
🎯 🗹 🖻 Remote Access RDP	<mark>0</mark> -最低	受信	IP T	CP	任意	任意	任意	任意	任意	Remote Desi
🎯 🗹 🖻 Remote Access SSH	<mark>0</mark> - 最低	受信	IP T	СР	任意	任意	任意	任意	任意	SSH (22)
🛞 🗹 💌 SMTP Server	<mark>0</mark> - 最低	受信	IP T	CP	任意	任意	任意	任意	任意	SMTP (25)
🎯 🗹 🖻 VMware vCenter Server	<mark>0</mark> -最低	受信	IP T	CP+UDP	任意	任意	任意	任意	任意	VMware vCe
🎯 🗹 💌 Web Server	0-最低	受信	IP T	CP	任意	任意	任意	任意	任意	HTTP(S) (80
🤓 🗹 🖻 新規ファイアウォールルール	0-最低	受信	IP T	СР	任意	任意	任意	任意	任意	3776 🗸
<										>
									ОК	キャンセル

6.4. あんしんプラス運用に必要なルール

ファイアウォール機能を利用し、必要最低限のルール設定を行う場合、以下表のルールはあんしんプラス運用に必要 なため、必ず追加および有効にしてください。

※新規ルールは作成する必要があります。

- ・ARP 送信ルール
- ・dns リゾルバ (クライアント)
- ・あんしんプラス運用ポート

名前	処理の		フレー	プロト	送信元	送信元	送信元	送信先	送信先	
(任意)	種類	方向	ムの	コル	IP	MAC	ポート	IP	MAC	送信先ポート
			種類							
ARP	許可	受信	ARP	なし	なし	任意	なし	なし	任意	なし
receive										
arp send	許可	送信	ARP	なし	なし	任意	なし	なし	任意	なし
新規ルール										
dns client	許可	送信	IP	UDP	任意	任意	任意	任意	任意	53
新規ルール										
anshinplus	許可	送信	IP	TCP	任意	任意	任意	任意	任意	80, 443, 4120, 4122
新規ルール										

6.5. 攻撃の予兆

攻撃が検出されると、一時的に送信元 IP からのトラフィックを Agent でブロックするように設定できます。[トラフィックのブロック] リストを使用して分数(最大 30 分)を設定できます。

[攻撃の予兆] 画面では、すべてまたは選択したコンピュータのトラフィック分析を有効にしたり、設定したりすることができます。

・攻撃の予兆の検出の有効化: 攻撃の予兆の検出のオン/オフを切り替えできます。

・検出を実行するコンピュータ/ネットワーク:保護する IP をリストから選択します。既存の IP リストから選択します。(この IP リストは、[ポリシー]→[共通オブジェクト]→[リスト]→[IP リスト] 画面を使用して作成できます。)

・検出を実行しない IP リスト: 無視するコンピュータとネットワークを IP リストセットから選択します。(上で述べたのと同様 に、この IP リストは、[ポリシー]→[共通オブジェクト]→[リスト]→[IP リスト] 画面を使用して作成できます。)

攻撃の種類ごとに、アラートがトリガされる Deep Security Manager に情報を送信するよう Agent を設定できます。また、 アラートのトリガ時にメール通知を送信するように Manager を設定できます([管理]→[システム設定]→[アラート] を参 照してください)。アラートは、「ネットワークまたはポートの検索」、「OS のフィンガープリント調査」、「TCP Null 検索」、 「TCP FIN 検索」、および「TCP Xmas 検索」です。) このオプションには [DSM にただちに通知] を選択してください。

ファイアウォール「攻撃の予兆タブ」

概要	一般 インタフェース制限 攻撃の	予兆 詳細 イ	~>+			
🦻 不正プログラム対策	□ 攻撃の予兆検索					
> Webレビュテーション	攻撃の予兆の検出の有効化:	Itti		\sim		
ファイアウォール	☑ OSのフィンガーブリント調査	✓ DSMICただちは	に通知 トラフィックのブロッ ク:	uluž 💙		
侵入防御	☑ ネットワークまたはボートの検索	☑ DSMにただちは	:通知 トラフィックのブロッ (ク:	ເມເນີ 🗸		
	☑ TCP Null検索	☑ DSMIこただちは	ご通知 トラフィックのブロッ ク:	30分 🗸		
ビーエリティロン 証視 	☑ TCP SYNFIN検索	☑ DSMにただちに	: 通知 トラフィックのブロッ ク:	uuz ∨		
設定 《	☑ TCP Xmas検索	☑ DSMIこただちは	:通知 トラフィックのブロッ ク:	ເທເນີ 🗸		
アップデート	検出を実行するコンピュータネットワー	ク: 維承 (す	(7.>-	~		
オーバーライド	検出を実行しないIPリスト:	維承 (lo	維承 (Ignore Reconnaissance)			

攻撃の予兆の保護を機能させるには、ステートフルインスペクションをオンにして、TCPおよびUDPのログを有効にする 必要があります。ステートフルインスペクションは、ポリシーまたはコンピュータのエディタの [ファイアウォール]→[一般] タブで有効化できます。ログは、ポリシーまたはコンピュータのエディタの [ファイアウォール]→[詳細] タブで有効化で きます。

6.6. ファイアウォールイベント

ファイアウォールの明示的に設定している拒否ルールに合致した場合、ファイアウォールイベントとして記録します。

概要	一般 インタフェース制限 攻撃の	の予兆 詳細 イベント			
🦁 不正プログラム対策	ファイアウォールイベント すべ	て マ グループ化しない マ	へ 検知	索	•
💮 Webレビュテーション	期間: 過去1時間	~			
圆 ファイアウォール	コンピュータ: コンピュータ:	✓ 2008r2		\checkmark	`
📀 侵入防御	📰 表示 🔂 エクスポート 🔹	省 自動タグ付け 🛛 🌉 列			
◎ 変更監視	時刻	ゴンビュータ 理由 ▲	タヴ	処理 ランク	方向
セキュリティログ監視	2014-07-15 10:10:14	2008r2 icmp拒否		拒否 100	受信
	2014-07-15 10:09:14	2008r2 icmp拒否		拒否 100	受信
🥮 インタフェース	2014-07-15 10:08:04	2008r2 icmp拒否		拒否 100	受信

イベントをダブルクリックすると詳細が表示されます。

一般	タグ	ヘッダ							
┌──般"情報 [
時刻:		2014-07-15 10:10:14							
ביצעב	ータ:	2008r2							
イベンド	送信元:	Agent							
理由:		icmp拒否							
処理:		拒否							
方向:		受信							
ランク:		100 = 資産評価×重要度 = 1 × 100							
インタフ:	ェース:	00:15:5D:41:0B:00							
	の種類一								
70-4	の種類:	IP							
ブロトコ/	V:	ICMP							
755:		Type:8 Code:0							
┌送信元-									

6.7. ファイアウォールアラート通知

ファイアウォールイベントに記録された中から、アラートを発するように設定されているファイアウォールルールに合致した場合にアラートとして記録され、指定された管理者宛てにメール通知します。

■ファイアウォールルール「オプションタブ」

ファイアウォールルールプロパティ	オプション
「アラート アラート: 継承 (オン)	

記録されたファイアウォールアラートは、消去するまで同イベントが発生してもアラート記録及び通知は行われません。

ダッシュボー	-F	アラート	イベントとレポート	コンピュータ	ポリシー	管理			
アラート リストビュー マ グループ化しない マ									
⊐ンピュータ: すべてのコンピュータ									
🔟 プロパティ	<u> î</u> 消去	🌆 アラート	の設定						
時刻 ▼ 重要度 アラート 対象 件名:									
▲ 2014-07-15 10:00 警告 ファイアウォールルールアラート				2008r2	icmp拒否				

※消去とは、発生したイベントの対応や確認が完了したことを意味します。消去するとアラート解決メールが通知されます。

7. 脆弱性・WEB アプリケーション保護『侵入防御(仮想パッチ)』

侵入防御設定について説明いたします。

7.1. 侵入防御の有効化

(1)管理 Web コンソールにログオンしてください。

コンピュータより、侵入防御を設定するサーバをダブルクリックします。

ダッシュボード 処理 アラート イベン	トとレポート コンピュータ	ポリシー 管理		
🛐 スマートフォルダ	コンピュータ サブク		•	Q このページを検索
= コンピュータ				
	+ 追加 > 💼 削除	■ 詳細 🔸 処理 👻	首 イベナ ▼ ■ エクスポート	▼ 毘.列
	名前 ▲	説明	プラットフォー・・ ポリシー	ステータス
	マ コンピュータ(6)			
	2008R2aws-justi	aws-justice	Microsoft Win Base Policy	● 設定のアップデートの…
	ip-10-0-2-11	aws-justice AM-Linux	Amazon Linux Base Policy	● セキュリティログ監視ル…

(2)サーバの設定画面が表示されます。

「侵入防御」をクリックします。

=.	概要	一般	処理	システムイベント	
8	不正プログラム対策	ホスト名	1:		2008R2aws-justi
	Webレビュテーション	表示名:			
۲	ファイアウォール	説明:			aws-justice
θ	侵入防御				
0	変更監視	プラット	フォーム:		Microsoft Windows Server 2008 R2 (64 bit) Service Pack 1 Build 7601
0	セキュリティログ監視	グルーフ	1:		コンピュータ ▼

(3) 侵入防御のステータスを「オン」にして「保存」をクリックしてください。

これで侵入防御が有効になります。継承(オン)になっている場合は既に有効になっています。

- 概要	一般	詳細	侵入防御イベント	
😵 不正プログラム対策	侵入防後	卸		
💿 Webレビュテーション	設定	継承	た(オン)	-
🖶 ファイアウォール	ステーダ	7ス: ●	オン, 防御, 207 ルール	L
😌 侵入防御	侵入防	卸の動作		
◎ 変更監視	● 103 ● 検	ゴロリ 注出		
Q セキュリティログ監視	現在割	山当てらわ	ていス侵入防御ル・	- 11,
😕 アプリケーションコントロー				
	9	~(•		

7.2. 侵入防御(推奨設定)

サーバのパッチ適用状況を検索し、侵入防御ルールの割り当て/解除を自動的に行わせることができます。

(1)侵入防御の推奨設定を自動的に適用(可能な場合):を「はい」にします。

「保存」をクリックして設定を保存します。継承(はい)になっている場合は既に有効になっています。

まだ侵入防御ルールは割り当てられていません。推奨設定の検索を行うことによりルールが自動的に割り当てされま

す	0											
	概要	一般	5关注册	侵入防御イベン	-							
Ø	不正プログラム対策											
O	Webレビュテーション	現在割	り当てられ	ている侵入防御	ルール —							
٢	ファイアウォール	I G	t									
θ	侵入防御		9~(*									
0	変更監視	割	り当て/割り	当て解除 🗐 🗆	プロパティ	🗈 エクスボート 🔹	6 アブ	リケーション	の種類	毘 列		
0	セキュリティログ監視	名i	前 *		アプリケー	ションの種類	優先度	重要度	モード		種類	カテゴリ
۲	アプリケーションコントロー	() 100	0128 – HTTR	Protocol Deco····	Web Server	Common	1-低	● 重大	防御		スマート	Webアプリケーション・
	インタフェース	 1 00	4360 – Multi	ple Browser Deni…	Web Client (Sommon	2 - 標準	高	防御		攻撃⊐∹	胞弱性と攻撃コード
ä	段定 (1 00	4715 – HTTR	⊃Web Client De…	Web Client (Sommon	1-低	● 重大	防御		スマート	絶弱性と攻撃コード
	アップデート	<mark>⊖</mark> 100	4790 – Ident	ified Diginotar C…	Web Client S	SL	2 - 標準	● 重大	防御		スマート	聴弱性と攻撃コード
~	オーバーライド	< アイテ.	41 -	100/207						Ŀ,		K < >
		推奨設	定									
		現在の	ステータス		207	個の侵入防御ルールが	割り当てられ	ています				
		前回の	推奨設定の	検索:	なし							
		1 推	運設定の検	素結果なし								
		侵入	防御の推奨	空定を 自動的に適用	1(可能な場合): (tl.		•				
			推奨197	色の検索	18	挺設定の検索のキャンセ			推奨設定をク			
												保存

(2) 推奨設定の検索

「推奨設定の検索」をクリックするとサーバに指示が出され検索を実行します。

検索が終了するまで数分から数十分かかります。

※推奨設定の検索は「予約タスク」機能によって定期的に自動で行うことができます。アプリケーションが追加/削除された場合や、パッチ適用、アプリケーションの設定変更などを行った場合に、自動的にルールを追加/削除するよう に予約タスクを設定します。(推奨設定の検索は1週間に1回を推奨します。)

	概要	一般 詳細 侵入防御-イベント	
•	不正プログラム対策	● 検出	
•	Webレビュテーション	現在割り当てられている侵入防御ルール	
۲	ファイアウォール		
θ	侵入防御	9. XC +	
0	変更監視	割り当て/割り当て解除 国 プロパティ 臣 エクスポート * ⑥ アプリケーションの)種類
0	セキュリティログ監視	名前 ▲ アプリケーションの種類 優先度 重要度	モード 種類
	アプリケーションコントロー	😌 1000128 - HTTP Protocol Deco… Web Server Common 1 - 低 🛛 ● 重大	防御 スマート
	インタフェース	😝 1004360 - Multiple Browser Deni™ Web Client Common 2 - 標準 🔸 高	防御 攻撃コード
\$	設定	⊖ 1004715 - HTTP Web Client De… Web Client Common 1 - 低 ● 重大	防御 スマート
	アップデート	➡ 1004790 - Identified Diginotar C···· Web Client SSL 2 - 標準 ● 重大	防御 スマート
∞,	オーバーライド	アイテム 1 -100/207	
		推契設定	
		現在のステータス: 207個の侵入防御ルールが割り当てられています	
		前回の推奨設定の検索:なし	
		1 推奨設定の検索結果なし	
		侵入防御の推奨設定を自動的に適用(可能な場合): 継承(はい) 🔹	
		推奨設定の検索 推奨設定の検索のキャンセル 推	鮮奨設定をクリア

(3) 推奨設定の検索が完了すると侵入防御ルールがサーバに割り当てされます。

例では67個のルールが割り当てられています。

しかし、未解決の推奨設定警告(1個)が出ています。一部ルールによっては自動的に割り当てして良いかの判断ができず手動で割り当て/割り当て解除の設定が必要となります。

	不正プログラム対策	 所知 					
	Webレビュテーション	● 検出					
۲	ファイアウォール	現在割り当てられている侵入防	御ルール				
θ	侵入防御	すべて マ					
0	変更監視						_
0	セキュリティログ監視	割り当て/割り当て解除 [■ プロパティ 📑 エクスポート 🕚	• ⑥ アプ!	リケーションの	D種類	11. 列
	アプリケーションコントロー	名前 ▲	アプリケーションの種類	優先度	重要度	モード	種類
	インタフェース	🥰 1000128 – HTTP Protocol Decc	•••• Web Server Common	1-低	● 重大	防御	スマート
	现中	😌 1004715 – HTTP Web Client De	···· Web Client Common	1-低	● 重大	防御	スマート
	axie	😝 1004790 – Identified Diginotar C)··· Web Client SSL	2-標準	● 重大	防御	スマート
	アップデート	🥰 1005040 – Identified Revoked C	≽··· Web Client SSL	2-標準	● 重大	防御	スマート
\;	オーバーライド	😔 1005307 – Identified Fraudulent	···· Web Client SSL	2 - 標準	● 重大	防御	スマート
		4					
		推奨設定					
		現在のステータス:	67個の侵入防御ルールた	割り当てられて	こいます		
		前回の推奨設定の検索	2018-10-04 15:07				
		⚠️ 未解決の推奨設定:	現在割り当てられている1	個のルールの製	削り当て解除		
		侵入防御の推奨設定を自動的に	適用(可能な場合): 継承(はい)		Ŧ		—

(4)未解決の推奨設定

未解決の推奨設定を確認、設定するためには「割り当て/割り当て解除」をクリックします。

•	不正プログラム対策	⑥ 防御					
	Webレビュテーション	◎ 検出					
•	ファイアウォール	現在割り当てられている侵入防御	1ルール				
θ	侵入防御	すべて 💌					
0	変更監視						_
0	セキュリティログ監視	割り当て/割り当て解除	プロパティ 📑 エクスポート 🔻	· 6 アラ	リケーション	の種類	围,列
	アプリケーションコントロー	名前 ▲	アプリケーションの種類	優先度	重要度	モード	種類
	インタフェース	🥰 1000128 – HTTP Protocol Deco···	Web Server Common	1-低	● 重大	防御	スマート
-	30字	😌 1004715 – HTTP Web Client De…	Web Client Common	1-低	● 重大	防御	スマート
*	ax/L	😝 1004790 – Identified Diginotar C…	Web Client SSL	2-標準	● 重大	防御	スマート
C.	アップデート	🥰 1005040 – Identified Revoked Cerr	•• Web Client SSL	2-標準	● 重大	防御	スマート
	オーバーライド	😔 1005307 – Identified Fraudulent …	• Web Client SSL	2-標準	● 重大	防御	スマート
		•					
		推奨設定					
		現在のステータス:	67個の侵入防御ルールが	割り当てられ	ています		
		前回の推奨設定の検索	2018-10-04 15:07				
		⚠️ 未解決の推奨設定:	現在割り当てられている11	個のルールの	割り当て解除	ŧ	
		侵入防御の推奨設定を自動的に適	用 (可能な場合): 継承 (はい)		•		

(5) IPS ルールの「割り当てを推奨」または「割り当て解除を推奨」を選択します。 推奨設定検索によって割り当てまたは解除を推奨するルール一覧が表示されます。

・割り当て解除を推奨の場合

ルールを解除する場合はチェックボックスのチェックを外し入れ「OK」をクリックしてください。選択したルールが解除されます。

侵入防御ルール すべて ▼ 割り	Q このぺー:	ジを検索								
🎦 新規 🔹 💼 削除 🗐 プロパティ	∎ 複製	■ エクス	マポート 🔹	C アプリケー:	ションの種類 田, 羽	آآ <u>]</u>				
名前 🔺	優先度	重要度	モード	種類	カテゴリ	CVE	CVSSスコア			
 ✓ Ø ● ▶ Web Client Common (1) ポートリスト 										
⊖ 🗹 💽 🛛 1006444 – Adobe Flash Player B·	・ 2 – 標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	CVE-2014	10.0			

・割り当てを推奨の場合

旗マークが推奨設定により検索されたルールで、アイコンに歯車がついているルールは、オプション設定ができるもの や設定が必要となるルールです。自動割り当てされない理由は、誤検知により通信をブロックしてしまう可能性があるた めです。ルール割り当て後、業務など動作確認を行える場合は、チェックボックスにチェックを入れ「OK」をクリックしてく ださい。選択したルールが割り当てされます。

(手動で割り当てたルールは後で解除する場合を考慮し、控えておいてください。CSV エクスポートも可能です。) 動作確認ができない、分からない場合はそのままにしておきます。

※問題が起きた場合はルール割り当てを解除してください。

IPSルール 身へて ▼ 割り当てを推奨 ▼ アラリクーションの推奨時日 ▼	-										
「 新規 ▼											
名前 優先度 重要度 モード	種類										
E 🛛 🖓 🚩 Database MySQL (2)											
🥰 🗖 🖬 📭 📭 1005063 - Restrict MySQL Database Access 2 - 標準 🛑 中 防御	スマート										
🎯 🗌 🗊 🏴 1004901 - Identified Suspicious Remote Login To MySQL Server Without Password 2 - 標準 🚥 重大 検出のみ	スマート										
DNS Client (1)											
🎯 🗌 💵 🏴 1005020 - Detected Too Many DNS Responses With 'No Such Name' Error 2 - 標準 🛑 中 検出のみ	スマート										
□ 🖉 🐨 🚩 Mail Server Common (1)											
🎯 🗌 🖬 🏴 1005344 - POP3 Mail Server Possible Brute Force Attempt 2 - 標準 🚥 重大 防御	スマート										
Cracle MySQL InnoDB Memcached Plugin (1)											
🧐 🗌 💵 🏴 1005511 - Oracle MySQL Server InnoDB MemCached Remote Denial Of Service Vulnerability 🛛 2 - 標準 📰 💼 中 防御	攻撃コード										
E ☑											
🧐 🗌 💵 🏴 1000511 - CVS Annotate Command Long Revision String Buffer Overflow 2 - 標準 🛛 💼 防御	脆弱性										
E 🛛 🖉 Veb Client Common (1)											
🧐 🗍 💵 🏴 1005290 - Identified Suspicious JavaScript iframe Object 2 - 標準 🗰 防御	スマート										

<	>
	OK キャンセル

7.3. 侵入防御(カスタム設定)

侵入防御ルールの割り当てを手動で行う方法です。推奨設定とカスタム設定を合わせて使うこともできます。 ※全てのルールから必要な侵入防御ルールを設定、メンテナンスすることは非常に困難だと思われるため、推奨設定 (自動)による運用をおすすめします。

(1)手動で設定する場合、「割り当て/割り当て解除」をクリックします。

全て手動で割り当てを行い、自動でルールを適用させない場合は「侵入防御の推奨設定を自動的に適用(可能な 場合):」を「いいえ」に設定してください。



(2)サーバに割り当てるルールを選択して「OK」をクリックします。

※キーワードにより検索することも可能です。

侵入防御	ルール すべて 🔹 すべて	Q このページを検索								
旝 新規 👻	削除	💼 複製	■ エクス	スポート 👻 🖪	5] アプリケー:	ソョンの種類 巴列				
,	名前 🔺	優先度	重要度	モード	種類	カテゴリ	CVE	CVSSZ37	前回のアップ…	-
🗸 🔲 🗷 Advanc	ed Message Queuing Protocol (AM	ąp) (1)							ポート:5672	
0	1009126 - Pivotal Spring AMQP …	2-標準	高	防御	攻撃コード	脆弱性と攻撃コード	CVE-2017	75	2018-07-25	
🗸 🔲 🖻 Apache	OpenMeetings (1)								ポート: 5080,5443	
0	1008267 - Apache OpenMeeting…	2 - 標準	• 中	防御	攻撃コード	脆弱性と攻撃コード	CVE-2016	4.0	2017-07-12	
🗸 🔲 🖻 Ancserv	ve Unified Data Protection (1)								ボート:8015	
⊖ ■	1008711 - Arcserve Unified Dat…	2 - 標準	商	防御	脆弱性	脆弱性と攻撃コード	CVE-2015	78	2018-01-31	
🗸 🔲 🖻 Asteris	k Manager Interface (AMI) HTTP (3))							ボート:8088	
0	1005348 – Asterisk Management…	2-標準	• 中	防御	脆弱性	脆弱性と攻撃コード	CVE-2012	5.0	2013-05-15	
😝 🗆 🖬	1005445 – Digium Asterisk HTT…	2-標準	• 中	防御	脆弱性	脆弱性と攻撃コード	CVE-2013	5.0	2013-06-19	
0	1006203 – Disium Asterisk Mana…	2-標準	ө 高	防御	脆弱性	脆弱性と攻撃コード	CVE-2014	75	2014-12-10	
🗸 🔲 🖻 Asteris	k RTP Protocol (1)								ポート: 1024-65535	-
ページ 1 /65	5								< <	> >
									0K キャン・	セル

(3) 現在割り当てられている侵入防御ルールを確認します。

サーバセキュリティあんしんプラス

例では5個の侵入防御ルールが割り当てられています。

 概要 不正プログラム対策 「億 Webレビュテーション 	 一般 詳細 イベント 見入防御 					
 不正ブログラム対策 修 Webレビュテーション 	受入防御					
Webレビュテーション						
	侵入防御のステータス: オン	🗸 🏹 防御,5ルー,	ŀ			
ファイアウォール 15	使人隊方御の動作 ● Rt☆n					
侵入防御						
変更監視	現在割り当てられている侵入防御ルール・					
● セキュリティログ監視	すべて マ					
	割り当て創り当て解除… 📃 プロ	パティ 😰 エクスポート 🔹 🐻 アコ	リケーションの種	類 🔢 3	列	
	名前	アブリケーションの種類	優先度	重要度	モード	種類
	😳 1005692 - Identified Apache Struts	Dy Web Server Miscellaneous	2 - 標準	● 重大	検出のみ	スマート
, ////////////////////////////////////	😳 1005604 - Apache Struts Multiple F	Re Web Server Miscellaneous	2 - 標準	💶 重大	防御	攻撃コー
オーバーライド	🧐 1000128 - HTTP Protocol Decodin	g Web Server Common	1-低	🚥 重大	防御	スマート
	🧐 1000931 - Multiple Vendor BSD ftp	od gl FTP Server Linux	2 - 標準	🚥 重大	防御	攻撃コー
	1000834 - SMTP Decoding	Mail Server Common	<mark>4</mark> - 最高	🚥 重大	防御	スマート
	(
「指	推奨設定		_			
J	現在のステータス: く	5個の侵入防御ルールが割り当てられていま	:ज			
前	前回の推奨設定の検索:	なし				
	 推奨設定の検索結果なし 					
6	侵入防御の推奨設定を自動的に適用(可	(能な場合): (はい	~			

7.4. 侵入防御ルール割り当て状況の確認

現在割り当てられている侵入防御ルールに、どのようなルールが割り当てられているか一覧及びキーワード検索にて 確認できます。

(1)侵入防御ルール一覧表示

現在割り当てられている侵入防御ルールです。「割り当て/割り当て解除を」をクリックすると一覧が開き、キーワード 検索やサーバに割り当てられていない全てのルールなどを表示させることができます。

コンピュータ: 2008R2a	ws-justi											
■ 概要	一般 詳細 最入防御イベント											
😵 不正プログラム対策	ステータス: ● オン,防御, 207 ルール											
👩 Webレビュテーション	表入防御の動作											
😑 ファイアウォール	 防御 +>u 											
😔 侵入防御	* 18出 在割り当でられている侵入防御ルール											
◎ 変更監視												
 セキュリティログ監視 	すべて ▼											
🥺 アプリケーションコントロー	割り当て/割り当て/割り当て/割り当て/割り当て/割り当て/割り当て/割り当て/											
🔜 インタフェース	ノ 2前 アブリケーションの種類 偽牛度 香要度 モード 種類 カテブリ	CVE 🚖										
✿ 設定	→ 1006224 - Microsoft Windows S ⁺⁺ DCERPC Services 2 - 標準 ● 重大 防御 施弱性 施弱性と攻撃コード	OVE-2017-**										
⑦ アップデート	⊖ 1009031 - Microsoft Windows Cr···· Remote Desktop Protocol Client 2 - 標準 ● 高 防御 攻撃コード 脆弱性と攻撃コード	CVE-2018-**										
ン\$ オーバーライド	😔 1009135 - Microsoft Windows D ··· DNS Client 2 - 標準 ● 重大 防御 攻撃コード 脆弱性と攻撃コード	CVE-2018-**										
	⊖ 1009182 - Microsoft Internet Ex···· Web Client Internet Explorer/Edge 2 - 標準 ● 高 防御 攻撃コード 脆弱性と攻撃コード	CVE-2018-** 💌										
	《 74元4 1 -100/907											
	推奖設定											
	現在のステータス: 207個の侵入防御ルールが割り当てられています											
		-										

表示フィルタにより「割り当てあり」や「割り当てなし」、「優先度」や「CVSS スコア別」に表示させることができます。

	侵入防御	ルール すべて 🔹 割り当	当てあり マ	アプリケ	アブリケーションの種類別 🔻				Q 201-3	-	
	旝 新規 👻	削除	💼 複製	E ±27	マポート -	1 アプリケー:	ションの種類 囲. 列				
		名前	優先度	重要度	モード	種類	カテゴリ	CVE	CVSSZ37	前回のアップ・・・	^
~	DCERF	PC Services (14)								動的	
	⊖ ⊻ •	1008224 - Microsoft Windows S…	2 - 標準	● 重大	防御	脆弱性	脆弱性と攻撃コード	CVE-2017	9.3	2018-10-02	
	0	1008327 - Identified Server Sus…	2-標準	● 重大	検出のみ	スマート	脆弱性と攻撃コード	CVE-2017	9.3	2018-09-26	
	0	1008225 - Microsoft Windows S…	2-標準	● 重大	防御	脆弱性	脆弱性と攻撃コード	CVE-2017	93	2018-09-26	
	⊖ ⊻ ∎	1008227 - Microsoft Windows S…	2-標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	CVE-2017	9.3	2018-09-26	
	⊖ 💌 🖬	1008306 - Microsoft Windows S…	2-標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	CVE-2017	9.3	2018-09-26	
	⊖ 💌 🖬	1008228 - Microsoft Windows S…	2-標準	● 重大	防御	脆弱性	脆弱性と攻撃コード	CVE-2017	9.3	2018-09-26	
	⊖ 💌 🖬	1008560 - Microsoft Windows S…	2-標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	CVE-2017	9.3	2018-08-29	
	⊖ 💌 🖬	1008713 - Microsoft Windows S…	2-標準	● 低	検出のみ	脆弱性	脆弱性と攻撃コード	CVE-2017	35	2018-08-29	
	⊖ 💌 🖬	1008468 - Microsoft Windows S…	2-標準	• 中	検出のみ	脆弱性	脆弱性と攻撃コード	CVE-2017	4.3	2018-08-29	
	⊖ 💌 🖬	1008432 - Microsoft Windows S…	2-標準	- 中	防御	脆弱性	脆弱性と攻撃コード	CVE-2017	4.3	2018-08-29	
	⊖ 💌 🗉	1008717 - Microsoft Windows S…	2 - 標準	● 重大	防御	脆弱性	脆弱性と攻撃コード	CVE-2017	10.0	2018-08-29	-
~-	ジ 1 /3									K	$\langle \rangle \rangle$
										ОК 🕇	ャンセル

(2)キーワード検索

脆弱性に対して実際に侵入防御ルールがあるか確認してみます。

例)OpenSSL の脆弱性(CVE-2014-0160)

表示フィルタは「すべて」を選択し、検索キーワードを入力しエンターキーを押してください。

CVE-2014-0160 を検索してみます。

IPSルール	すべて 👻 すべて 👻 アブリケーションの種類的 👻		<mark>익</mark> 検索			-
新規 →	□ 削除 □ ブロバティ □ 複製 🗗 エクスポート 🔹 🐻 アプリケーションの種類.	📑 列				
	名前 🔺	優先度	重要度	モード	種類	,
E 🗌 🖬 Adobe	ColdFusion Solr Service (1)					
📀 🗆 🖻	1003966 - Adobe ColdFusion Solr Collections Information Disclosure	2 - 標準	中口	検出のみ	スマート	
E 🗌 🖬 Applic	ation Control For Download Manager (1)					
🥶 🗆 🖻	1004902 - Application Control For JDownloader	2 - 標準	■ 高	検出のみ	スマート	
E 🗌 🖬 Applic	ation Control For File Sharing (18)					
۲ 🕑 🧐	1001109 - Application Control For BitTorrent	2 - 標準	■ 商	検出のみ	スマート	
۲ 🕑	1002471 - Application Control For Emule	2 - 標準	💼 高	検出のみ	スマート	
🧐 🗆 🖬	1002472 - Application Control For FTP Client	2 - 標準	💶 重大	検出のみ	スマート	
🥶 🗆 🖬	1002473 - Application Control For TFTP Client	2 - 標準	💼 高	検出のみ	スマート	
🧐 🗆 🖬	1003368 - Application Control For Gnutella	2 - 標準	■ 高	検出のみ	スマート	
۲ 🕑	1003647 - Application Control For Manolito	2 - 標準	💶 商	検出のみ	スマート	
🥶 🗆 🗉	1003651 - Application Control For Windows Live FolderShare	2 - 標準	■ 高	検出のみ	スマート	
۲ 🕑	1003652 - Application Control For DC++	2 - 標準	💶 商	検出のみ	スマート	
۲ 🕑	1003655 - Application Control For Share NT5	2 - 標準	💼 高	検出のみ	スマート	
۲ 🕑 🥵	1003656 - Application Control For Kazaa	2 - 標準	💶 高	検出のみ	スマート	
۲ 🕑 🥹	1003665 - Application Control For Soulseek	2 - 標準	💶 重大	検出のみ	スマート	`
<					>	
ページ1 / 23						×
				ок	キャンセ	ı.

検索結果表示より、5件のルールでそれぞれ2014/5/14、2014/5/28にアップデートされていることが分かります。

実際にOpenSSLアプリケーションを利用していて脆弱性が存在していた場合、推奨設定を自動割り当てすることで侵入防御ルールが自動的に適用されます。

IPS/L-/L	すべて マ	すべて マ	アブリケーション	の種類別	-				CVE-201	4-0160	×	-
新規 →	<u>前</u> 前除	= プロパテ	-r 📋 複製	[] I:	ウスボート	・ • 💽 アブレ	ケーション	の種類	14 列			
	名前 ▲				優先度	重要度	モード	種類	CVE	CVSSス⊐ア	前回のア	ップ
🗉 🖌 💌 OpenS	SL (3)									*		366,44
🧐 🗆 🖬	1006010 - R	estrict OpenS	SL TLS/DTLS He	artbe	2 - 標準	: 一 中	防御	スマート	CVE-2014-0160	5.0	2014-05-	-14
🛞 🗆 🖬	1006011 - 0	penSSL TLS/I	DTLS Heartbeat I	nform	2 - 標準	· • 中	防御	脆弱性	CVE-2014-0160	5.0	2014-05-	-14
🛞 🗆 🖬	1006012 - Id	entified Suspi	cious OpenSSL T	LS/D	<mark>2</mark> - 標準	· • 中	防御	スマート	CVE-2014-0160	5.0	2014-05-	-14
E De OpenS	SL Client (2)									ボ		366,44
📀 🗆 🖬	1006016 - O	penSSL TLS/	DTLS Heartbeat N	Messa	2 - 標準	с Ф	防御	脆弱性	CVE-2014-0160	5.0	2014-05-	-28
۵ 🕒 🧐	1006017 - R	estrict OpenS	SL TLS/DTLS He	artbe	2 - 標準	- 中	6方御	スマート	CVE-2014-0160	5.0	2014-05-	-28
<												>
										ок	キャンセル	ŀ

(3)IPS ルール表示補足

CVE

CVE(Common Vulnerabilities and Exposures)は、個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利 団体の MITRE 社が採番している識別子です。脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利 用しています。CVE の書式は、「CVE-西暦-連番」の形式で構成。

共通脆弱性識別子と言われています。

脆弱性対策情報データベース検索

https://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja

■CVSS スコア

脆弱性対策情報データベースでは、共通脆弱性評価システム CVSS(Common Vulnerability Scoring System)を用いて、 評価結果および CVSS 基本値の評価内容を記載し、脆弱性の固有の深刻度を表しています。

■種類

・攻撃コード / セキュリティホール / Exploit
 特定の脆弱性を攻撃する "特定の攻撃" を検知するためのルール

•脆弱性 / Vulnerability

1 つ以上のエクスプロイトが存在する "特定の脆弱性" への攻撃を検知するためのルール

・スマート / Smart

1つ以上の既知、または未確認(ゼロデイ攻撃の可能性のある)攻撃を検知するためのルール



7.5. 侵入防御イベント

侵入防御ルールに合致した場合、侵入防御イベントとして記録します。

🧒 概要	一般詳細イベント					
😨 不正プログラム対策	侵入防御イベント すべて▼	入防御イベント すべて▼ グループ化しない ▼ Q 検索 ▼				
🥯 Webレビュテーション	期間: 過去1時間	\checkmark				
圆 ファイアウォール	コンピュータ: コンピュータ:	dss.securityplus.jp	\checkmark			
📀 侵入防御	📰 表示 🔛 エクスポート 🔹	省 自動タグ付け 🛛 🏭 列				
🔘 変更監視	時刻	コンピュータ タグ	アプリケーションの種類	処理 ランク		
🗨 セキュリティログ監視	2014-07-14 20:00:57	dss.securityplus.jp ,	tal	リセット 100		

イベントをダブルクリックすると詳細が表示されます。

→般 タグ	データ			
┌一般情報───				
時刻:	2014-07-14 20:00:57			
コンピュータ:	dss.securityplus.jp			
イベント送信元:	Agent			
理由:	ハンドシェーク内の不正なパラメータ			
処理:	リセット			
方向:	送信			
70-:	リバースフロー			
ランク:	100 = 資産評価 × 重要度 = 1 × 100			
インタフェース:	06:54:43:12:1D:6F			
プロトコル:	TCP			
フラグ:	ACK PSH DF=1			

7.6. 侵入防御アラート通知

侵入防御イベントに記録された中から、アラートを発するように設定されている侵入防御ルールに合致した場合にアラートとして記録され、指定された管理者宛てにメール通知します。

■侵入防御ルール「オプションタブ」

侵入防御ルール	ブロバティ 脆弱性	設定	オプション	
「アラートーーー アラート:	オン		~	

記録された侵入防御アラートは、消去するまで同イベントが発生してもアラート記録及び通知は行われません。

ダッシュボード		イベントとレポート	コンピュータ	ポリシー 管	理	
アラート リストビュー マ グループ化しない マ						
コンピュータ: すべてのコンピュータ 🗸 🗸						
🛄 ブロパティ 📋 消去	ゴロパティ… 1 消去 場 アラートの設定…					
時刻 🔻	重要度	アラート	対象	件名:		
19:02 2014-07-14	警告	変更監視ルールアラート	cent65	wwwコンテンツ監視(c	ent65)	

※消去とは、発生したイベントの対応や確認が完了したことを意味します。消去するとアラート解決メールが通知されます。

8. 改ざん検知『変更監視』

変更監視設定について説明いたします。

8.1. 変更監視の有効化

(1)管理 Web コンソールにログオンしてください。

コンピュータより、変更監視を設定するサーバをダブルクリックします。

ダッシュボード	7 5 -ŀ	イベントとレポート	コンピュータ	ポリシー	管理			
コンピュータ	コノセ	ニータ サブグループを含	む マ グループ別	J -			Q 検索	-
		新規 🖌 <u> </u> 削除 📃	詳細 処理 🗸	イベント 🔹 🔝	エクスポート ・	1		
		名前▼ 説明	月 プ	ラットフォーム ポリ	≥-	ステータス	前回の通信	前回成功したアップデート
	E	ピュータ (2)						
		cent65	R	ed Hat Enter Linu	ix Server) 管理対象 (オンライン)	3分前	37分前
		2008r2	Mi	icrosoft Wind Bas	e Policy 🛛 🌔	🌖 管理対象 (オンライン)	1分前	17 時間 前
	«							

(2)サーバの設定画面が表示されます。

「変更監視」をクリックします。

コンピュータ: cent65			0 ^
- 概要			
😨 不正プログラム対策	「一般		
💿 Webレビュテーション	ホスト名: 表示名:	cent65 ×	(前回使用されたIP: 54.95.118.236)
🛞 ファイアウォール	说明:		
🛞 変更監視			
🕙 セキュリティログ監視	ブラットフォーム:	Red Hat Enterprise 6 (64 bit) (2.6.32- 431.11.2.el6.centos.plus.x86_64)	
🎟 インタフェース	グループ:	コンピュータ]
	ポリシー:	Base Policy	編集
	資産の重要度:	tau 🗸	編集
	セキュリティアップデートのダウンロード	プライマリテナントのRelayグループ	福集
🕂 オーバーライド	元:		

(3)変更監視のステータスを「オン」にして「保存」をクリックしてください。

これで変更監視が有効になります。継承(オン)になっている場合は既に有効になっています。

- 概要					
📀 不正プログラム対策	反更監視				
🐵 Webレビュテーション	変更監視のステータス: 維承 (オン)				
圆 ファイアウォール					
🧐 侵入防御	- 本面の始本				
🚷 麦更監視	またの状況 前回の変更のフル検索: なし 変更の検索				
🕙 セキュリティログ監視					
🎟 インタフェース	「ペースラインー				
🌼 設定	作成された最新の整合性ペースライン: なし				
📮 アップデート	ベースラインの再構築 ベースラインの表示				
🕂 オーバーライド	「現在割り当てられている変更監視ルール				
	割り当て削り当て解除 🔟 プロバティ 🗗 エクスポート 🗸 🏗 列				
	26前▲ 重要度 種類 前回のアップ				
	(リストにアイテムがありません)				

8.2. 変更監視(推奨設定)

さまざまな OS とアプリケーションに対応した、定義済みの多数のルールにより、検索対象のサーバに対して、変更監視 ルール (Windows の変更監視ルールや Linux の変更監視ルールなど)をコンピュータに自動で割り当てることができま す。変更監視対象は、インストール済みのソフトウェア、実行中のサービス、プロセス、ファイル、ディレクトリ、待機中の ポート、レジストリキー、およびレジストリ値です。

推奨設定では定義済みの多数のルールが用意されているため、多数のイベント記録及びアラート通知が発生する可能 性があります。必要に応じて検索対象を変更するか、監視対象ディレクトリやファイルが明確である場合、手動ルール設 定を行ってください。

(1)変更監視ルールの推奨設定を自動的に適用(可能な場合):を「はい」にします。

「保存」をクリックして設定を保存します。継承(はい)になっている場合は既に有効になっています。

📃 概要		→般 詳細 イベント							
💿 不正プログラム	刘策	前回の変更のフル検索: なし							^
Seburgar-	ション	変更の検索							
🎯 ファイアウォー	V	「ペースライン							
🤨 侵入防御		作成された最新の整合性ペースラー	(ン:なし	()					
🌒 安更監視		ペースノイノの何情報	~~~~	1,200,8645					
セキュリティロ	「監視	現在割り当てられている変更監視ル							
📟 インタフェース		割り当て信り当て解除] ブロバティ	コエクスポート 1525	• 國列				
🌐 ikc	~~	活動▲	重要度	權規	前回のアッフ				
📑 アップデート				リストにアイ	テムがありません)				
🕂 オーバーライド									
		- 単初時空							
		確認もれた 現在のステータス:	0個の変更監護	現ルールが割り着	行られています				
		前回の推奨設定の検索	ねし						
		 推奨設定の検索結果なし 							
		変更監視ルールの推奨設定を自動	的に適用(可能な対	湯合): 継承 (は	, 1)	~			
		推調設定の検索	推奨設	定をクリア					~
							保存	ह्याह्य	

(2)推奨設定の検索

「推奨設定の検索」をクリックするとサーバに指示が出され検索を実行します。

検索が終了するまで数分から数十分かかります。

※推奨設定の検索は「予約タスク」機能によって定期的に自動で行うことができます。新しいアプリケーションが追加された場合など、自動的にルールを追加するように日単位、週単位などのスケジュールを予約タスクで設定することもできます。

Γ	推奨設定				
	現在のステータス:	0個の変更監視ルールが割り当てられています			
	前回の推奨設定の検索:	なし			
	🚯 推奨設定の検索結果なし				
	変更監視ルールの推奨設定を自動的に適用(可能な場合): 維承(はい)				
	推奨設定の検索	推奨設定をクリア			
(3) 推奨設定の検索が完了すると変更監視ルールがサーバに割り当てされます。

例では22個のルールが割り当てられています。

概要		
🦁 不正プログラム対策	「パースライン」 作成された最新の整合性ペースライン: 2014-07-11 11:43	,
💿 Webレビュテーション	ペースラインの再構築 ペースラインの表示	
圆 ファイアウォール	「現在書作」当てられている変更整視ルール	
	割り当て/割り当て/割り当て/割り当て/割り当て/割り プロパティ (2) エクスポート ・ (1) 列	
🌒 麦更監視	名前▲ 重要度 種類 前回のアップ	^
🕙 セキュリティログ監視	🥞 1002766 - Unix - Directory attribu 🐽 高 定義済み 2009-07-29	
- 	🎯 1002770 - Unix - File attributes c 💶 高 定義済み 2009-06-24	
	🧉 🔘 1002771 - Unix - Permissions of I 💼 高 定義済み 2011-10-12	
🔅 設定	🚱 1002875 - Unix - Added or Remo 💼 高 定義済み 2011-02-16	
・ アップデート	🎯 1003000 - Database Server - My 💼 中 定義済み 2011-10-12	~
▲ オーバーライド	● 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒 〒	
<u> </u>		
	現在のステータス: 22個の変更監視ルールが割り当てられています	
	前回の推奨設定の検索: 2014-07-11 12:07	
	✔ 未解決の推奨設定はありません	
	推奨設定の検索 推奨設定をクリア	
	保存	閉じる

(4)変更監視ルールの確認/変更

コンピュータに割り当てられているルールの内容を確認、変更する場合は「割り当て/割り当て解除」をクリックします。

- 概要	一般 詳細 イベント	
😨 不正プログラム対策	「変更の検索 前回の変更のフル検索: ない	
😁 Webレビュテーション	変更の検索	
🛞 ファイアウォール		
🤨 侵入防御	作成された最新の整合性ペースライン: 2014-07-11 11:43	
🌔 変更監視	ペースラインの再構築 ペースラインの表示	
🕙 セキュリティログ監視	「現在書り当てられている変更監視ルール	
🎟 インタフェース	割り当て傷り当て解除 🗐 プロパティ 🕒 エクスポート 🗸 🏭 列	
🍪 設定	名前▲ 重要度 種類 前回のアップ 300000700 1000 2000007.00 2000007.00	^
見 アップデート	- Canada Canad	
碞 オーバーライド	🍯 1002771 - Unix - Permissions of I 💼 高 定義済み 2011-10-12	
	🚭 1002875 - Unix - Added or Remo 🐽 定義済み 2011-02-16	
	● 1003000 - Database Server - My	
	● 1003019 - Trend Micro Deep Sec < 中 定義済み 2013-10-23	~

変更監視ルール一覧が表示されます。

表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。旗マークが推奨設定により検索されたルールで、アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックのオン/オフでルールの割り当て/割り当て解除を行えます。決定は「OK」をクリックしてください。

変更監視	2ルール すべて ▼ グループ化しない ▼				Q 検索	-
📑 新規	. • 🗊 削除 🔲 プロパティ 门 複	製 🔹 エク	スポート 🗸	🏭 列		
	名前 🔺	重要度	種類	前回のアップ		^
🥶 🗹 🏴	1002766 - Unix - Directory attributes chang	🚥 高	定義済み	2009-07-29		
8	1002767 - Microsoft Windows - System dire	高	定義済み	2009-07-29		
🎯 🗹 🏴	1002770 - Unix - File attributes changed in /	━□ 高	定義済み	2009-06-24		
🎯 🗹 🏴	1002771 - Unix - Permissions of log files ch	━□ 高	定義済み	2011-10-12		
())	1002773 - Microsoft Windows - 'Hosts' file	高	定義済み	2010-05-26		
	1002774 - Microsoft Windows - Microsoft H	中	定義済み	2009-06-24		
68	1002775 - Microsoft Windows - Network co	高	定義済み	2009-07-15		

(5) 推奨設定されたルールの割り当て変更

例)/etc ディレクトリを監視対象から外す場合

推奨設定で割り当てされたルールのチェックボックスを外すことで、/etc ディレクトリを監視対象から外すことができます。

変更監視ルール 割り当てあり ▼ 重要度別 ▼		Q 検索	•
□ 新規 ・ 👔 削除 🔲 ブロバティ [複製 🔂 エクスポート	• 🚛 列		
名前一	種類 前回のアップ		^
🎯 🗹 🟴 1003370 - Application - OpenSSL	定義済み 2011-10-12		
🎯 🗹 🟴 1003375 - Application - Postfix	定義済み 2011-10-12		
🎯 🗹 🏴 1003379 - Application - Gzip	定義済み 2011-10-12		
🎯 🗹 🟴 1003385 - Application - Xorg-x / XFree86 / Xfree86 / Xorg-x11	定義済み 2011-10-12		
🎯 🗹 🏴 1003533 - Application - OpenSSH	定義済み 2011-10-12		
🎯 🗹 🏴 1003587 - Unix - Directory attributes changed for /bin	定義済み 2009-07-29		
🎯 🗹 🏴 1006076 - Task Scheduler Entries Modified	定義済み 2014-06-07		
■ 斎 (10)			
🎯 🗹 🟴 1002766 - Unix - Directory attributes changed for /sbin	定義済み 2009-07-29		
🎯 🗹 🟴 1002770 - Unix - File attributes changed in /usr location	定義済み 2009-06-24		
🍈 🗹 🏴 1002771 - Unix - Permissions of log files changed	定義済み 2011-10-12		
🎯 🗹 🏴 1002875 - Unix - Added or Removed Software	定義済み 2011-02-16		
🎯 🗹 🟴 1003168 - Unix - Open Port Monitor	定義済み 2009-07-15		
🎯 🗹 🏴 1003169 - Unix - Process Monitor	定義済み 2011-10-12		
🎯 🗹 🏴 1003513 - Unix - File attributes changed in /etc location	定義済み 2009-06-24		
🎯 🗹 🟴 1003514 - Unix - File attributes changed in /lib location	定義済み 2009-06-24		
🎯 🗹 🟴 1003573 - Unix - File attributes changed in /bin location	定義済み 2009-06-24		
🎯 🗹 🏴 1003574 - Unix - File attributes changed in /sbin location	定義済み 2009-06-24		~
		ОК	キャンセル

(6)変更監視ルールの変更

例)/etc ディレクトリ内のファイルが更新された場合のみを監視する場合、attributes(属性)による監視を設定します。 ※LastModified(最終更新日)のみ監視にしても、仕様によりファイル作成、削除も検知します。

ルールをコンピュータに対して編集するには、ルールを右クリックして [プロパティ...]をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)...]をクリックします。

※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が 適用されます。

変更監視ルールのプロパティが開きます。

設定タブを選択します。



コンピュータに対して割り当てる場合は「継承」のチェックを外します。

変更監視ルールプロパティ 設定 オプション	
- 設定オブション	^
File attributes to monitor:	
Created	
☑ LastModified	
Permissions	
☑ Owner	
Group	
Size	
Contents	
SymLinkPath	
File path to be ignored under '/etc' path (e.g., /etc/log/* is used to ignore monitoring all file under /etc/log/ path): Note: A single asterisk * can be used as a wildcard for a name, a double asterisk ** is a wildcard for any path depth.	
Add	~
 OK キャンセル 適用	

LastModified(最終更新日)以外のチェックを外し、「OK」をクリックします。これでルールが変更されました。 監視ディレクトリ配下のサブディレクトリなどを監視対象外(例)/etc/log/* に設定することも可能です。

変更監視ルールブロバティ 設定 オプション		変更監視ルールブロバティ 設定 オブション	
_ 設定オブション	~	File attributes to monitor:	~
		Created	
		☑ LastModified	
		Permissions	
		Owner	
LastModified		Group	
L. Permissions		□ Size	
U Owner		Contents	
Group		SymLinkPath	
□ Size			
Contents		File path to be ignored under '/etc' path (e.g., /etc/log/* is used to ignore monitoring all file under /etc/log/ path):	
SymLinkPath		Note: A single asterisk * can be used as a wildcard for a name, a double	
File path to be ignored under '/etc' path (e.g., /etc/log/* is used to ignore		asterisk ** is a wildcard for any path depth.	
monitoring all file under /etc/log/ path):		Add	
Note: A single asterisk * can be used as a wildcard for a name, a double		/etc/log/* Remove	
asterisk " is a wildcard for any path depth.			
Add	~		~
OK キャンセル 適用		OK キャンセル 適用	

(7)ベースラインの再構築【重要】

ベースラインは、変更の検索結果の比較対象となる元の状態です。変更監視対象が構築したベースラインと異なった 場合にイベント記録及びアラート通知を行います。

※OS やアプリケーションの環境変更や Web コンテンツを修正した場合には、都度ベースラインの再構築が必要です。 ※変更監視をリアルタイムで行っている場合、コンテンツ変更などでイベント記録及びアラート通知が発生します。 「ベースラインの再構築」をクリックします。

 Webレビュテーション アップアウォール アップアウォール アップア・ト アップア・ト デップア・ト アップア・ト アップア・ト アップア・ト アップア・ト アップア・ト アップア・ト アンプア・ト アングア・ト アンプア・ト アンプロッシッシュ アンプロッシュ アンプロッシュ アンプロッシュ アングア・シー アンジェ アングア・シー 	
 ③ ファイアウォール ③ クァイアウォール ③ 使入防御 ③ 支型監視 ③ 支型監視 ③ セキュリティログ監視 ※更の検索 前回の変更のフル検索: 2014-07-11 17:59 ※ 世史 ※ レックフェース ※ 防定 ペースライン 作成された最新の整合性ペースライン: 2014-07-11 17:47 ペースラインの再構築 ペースラインの画構築 ペースラインの表示 ・ペースラインの画構築 ペースラインの画構築 ペースラインの表示 ・ペースラインの画構築 ・ペースラインの表示 ・ペースラインの画構築 ・ペースラインの表示 ・ペースラインの画構築 ・ペースラインの画構築 ・ペースラインの表示 ・ペースラインの画構築 ・ペースラインの表示 ・ペースラインの画構築 ・ペースラインの表示 ・ペースラインの画構築 ・ペースラインの表示 ・ペースラインの画構築 ・ペースラインの表示 ・ペースラインの画構築 ・ペースラインの表示 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
 ③ 良久防御 ③ 支更監視 ※更の検索 前回の変更のフル検索: 2014-07-11 17:59 ※ セキュリティログ監視 ペースライン ※ 防定 ペースライン 作成された最新の整合性ペースライン: 2014-07-11 17:47 ペースラインの展示 ・ペースラインの展示 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの展示 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースラインの目的 ・ペースの ・ペースの ・ペースの ・ペースの	
 ま更監視 ま更の検索 前回の変更のフル検索: 2014-07-11 17:59 変更の検索 変更の検索 でもコリティログ監視 変更の検索 で、スライン 作成された最新の整合性ペースライン: 2014-07-11 17:47 ペースラインの表示 ペースラインの表示 ポースラインの表示 ポースラインの表示 ポースラインの表示 ポースラインの表示 ポースラインの表示 ポースラインの表示 ポースラインの表示 パーン ポープジディト ポースラインの表示 ポースラインの表示 ポースラインの表示 ポースラインの表示 パー	
 ③ セキュリティログ監視 変更の検索 ※ セキュリティログ監視 変更の検索 ペースライン 作成された最新の整合性ペースライン: 2014-07-11 17:47 ペースラインの高示 ※ オーパーライド 調り当て合れている変更監視ルール 期り当て確則当て合れている変更監視ルール 第り当てなり当て留称: 回 プロパティ ③ エクスポート ・ 113 列 名前 ▲ 重要度 種類 前回のアップ ※ 1002760 - Unix - Directory attributes changed for /sbin ← 高 種類高谷 2009-07-29 ④ 1002760 - Unix - Directory attributes changed for /sbin ← 高 種類高谷 ● 定義高谷 2009-07-29 ● 1002760 - Unix - Directory attributes changed for /sbin ← 高 種類高谷 ● 二、 二、	
 マンダフェース ※ ペースライン ※ マップデート ダ オーバーライド (株式内広最新の整合性ペースライン: 2014-07-11 17:47 マースラインの画様為 ペースラインのあ示 (現在部)当てられている変更監視ルール 部)当て信引当て解除 ゴロパティ エクスポート ・ 取列 名前 ▲ 重要度 種類 前回のアップ ② 1002766 - Unix - Directory attributes changed for /sbin ● 正務済み 2009-07-29 (1002766 - Unix - Directory attributes changed in /bits loration 	
 	
・ アップデート ペースラインの表示 ・ オーパーライド ・ ・ ・	
ダ オーバーライド 「現在割り当て谷れている次更監視ルール 割り当てなり当て谷和吹加、 回 プロパティ ②エクスボート ・ 国 列 名前 ▲ 重要度 種類 前回のアップ 20102766 - Unix - Directory attributes changed for /sbin ← 定義済み 2009-07-29 「ついつての。」Unix - Elle attributes changed for /sbin ← 定義済み 2009-07-29	
割川当て(南州)当で(南)(当て前除 団) プロパティ (ユ) エクスポート ↓ 田 列 名前 ▲ 重要度 種類 前回のアップ 1002766 - Unix - Directory attributes changed for /sbin ← 高 定義済み 2009-07-29 1002770 - Unix - Directory attributes changed in /srs loration 一 高 定義済み 2009-07-29	
名前▲ 重要度 種類 前回のアッブ ジ 1002766 - Unix - Directory attributes changed for /sbin 高 定義済み 2009-07-29 ジ 1002760 - Unix - Directory attributes changed for /sbin 高 定義済み 2009-07-29	
 2002766 - Unix - Directory attributes changed for /sbin 高定義済み 2009-07-29 2002770 - Link - Elle attributes changed in //sc location 一方定英楽社 2000-06-24 	~
🚳 1002770 - Linix - File attributes changed in /usr location	
Total 10 - On A - The automotics changed in fush location - Liss rate 2005-00-24	
🕘 1002771 - Unix - Permissions of log files changed 🛛 💼 定義済み 2011-10-12	
🌍 1002875 - Unix - Added or Removed Software 🛛 💼 商 定義済み 2011-02-16	
💕 1003000 - Database Server - MySQL 🛛 🕞 中 定義済み 2011-10-12	
⑥ 1003019 - Trend Micro Deep Security Agent	
推奨設定	•
現在のステータス: 22個の変更監護ルレールが重い当てられています	

ベースラインが作成されると、作成された日時が更新され以後監視対象に変更があった場合にイベントとして記録され ます。「ベースラインの表示」をクリックすると保持されているベースラインの一覧を表示できます。

Г	-ベースライン		
	作成された最新の整合性ベースライン	: 2014-07-11 18:30	
	ベースラインの再構築	ペースラインの	表示

· //// X/	ベー	・スラィ	インヨ	長示
-----------	----	------	-----	----

ベースライン	ノ表示ツール グループ化しない ▼		♀ 検索	-
☶ 表示				
種類▲	+-	フィンガープリント	ルール名	_
Directory	/opt/ds_agent	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/opt/ds_agent/lib	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/opt/ds_agent/2.6.32-358.0.1.el6.x86_64-x	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/opt/ds_agent/Licenses	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/opt/ds_agent/2.6.32-71.el6.x86_64-x86_64	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/opt/ds_agent/2.6.32-358.2.1.el6.x86_64-x	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/opt/ds_agent/lib/iaucore	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/opt/ds_agent/lib/iaucore/libs	2014-07-11 11:42:01	1003019 - Trend Micro Deep Security Agent	
Directory	/var/log/ds_agent	2014-07-11 11:42:02	1003019 - Trend Micro Deep Security Agent	
Directory	/bin	2014-07-11 11:42:01	1003587 - Unix - Directory attributes changed for /bin	
Directory	/usr/libexec/openssh	2014-07-11 11:42:01	1003533 - Application - OpenSSH	
Directory	/etc/ssh	2014-07-11 11:42:01	1003533 - Application - OpenSSH	
Directory	/sbin	2014-07-11 11:42:01	1002766 - Unix - Directory attributes changed for /sbin	
File	/etc/gshadow-	2014-07-11 18:30:27	1003513 - Unix - File attributes changed in /etc location	
File	/etc/rc	2014-07-11 18:30:27	1003513 - Unix - File attributes changed in /etc location	
File	/etc/my.cnf	2014-07-11 18:30:27	1003513 - Unix - File attributes changed in /etc location	
File	/etc/.swp	2014-07-11 18:30:27	1003513 - Unix - File attributes changed in /etc location	
File	/etc/hosts.denv	2014-07-11 18:30:27	1003513 - Unix - File attributes changed in /etc location	
アイテム 1	59,676の100まで		14 4	► H

8.3. 変更監視(カスタム設定)テンプレートによる設定

変更監視ルールの割り当てを手動で行う方法です。推奨設定とカスタム設定を合わせて使うこともできます。

多数の一般的なOSおよびアプリケーション用の変更監視ルールが用意されていますが、独自のカスタムルールを作成 することもできます。カスタムルールを作成する場合は、「基本ルール」テンプレートを使用するか、新しいルールをXML で記述できます。ルールをポリシーで作成することによりポリシーを割り当てているコンピュータ全てにルールを割り当て ることもできます。

※定義済みルールに加えて、Webサーバとして変更監視を適用しておくべきルールをカスタムルールとして作成することを推奨します。

■カスタムルールにてカバーすることを推奨する監視対象

Web サーバに関する以下のファイルの属性変更

- ・コンテンツファイルが格納されるディレクトリ配下 (例:/var/www/html/*)
- ・動的コンテンツ (例:/var/www/cgi-bin/*)
- ・Apache ロードモジュール (例:/etc/httpd/modules/*)

(1)手動で設定する場合、「割り当て/割り当て解除」をクリックします。

全て手動で割り当てを行い、自動でルールを適用させない場合は「侵入防御の推奨設定を自動的に適用(可能な場合):」を「いいえ」に設定してください。

	概要		
0	不正プログラム対策	前回の変更のフル検索: なし	
	Webレビュテーション	変更 の 検索	
0	ファイアウォール	「ペースライン	
0	侵入防御	作成された最新の整合性ペースライン: 2016-06-22 15:52	
	変更監視	ペースラインの再構築 ペースラインの表示	
0	セキュリティロ分野調	「現在割り当てられている変更監視ルール	
	(()) () () () () () () () ()	割り当て唐り当て解除… 📰 プロパティ… 🔂 エクスポート 🖌 🏢 列…	
	1/9/1-7	名前▲ 重要度 種類 前回のアップ	^
203	設定。	🔮 1002766 - Unix - Directory attribu 🍋 高 定義済み 2009-07-29	
	アップデート	🚭 1002770 - Unix - File attributes c 💶 高 定義済み 2009-06-24	
-9	オーバーライド	🌍 1002771 - Unix - Permissions of I 💶 高 定義済み 2011-10-12	
-		🚭 1002851 - HTTP Server - Apache 🐑 中 定義済み 2013-05-07	
		🍯 1002875 - Unix - Added or Remo 💶 商 定義済み 2011-02-16	
		lefen 1003019 - Trend Micro Deep Sec cつ中 定義済み 2016-02-24	Ť
		 「#認識定 現在のステータス: 23個の変更監視ルールが割り当てられています 約回の准規設定の検索: 2016-07-07 11:40 ✓ 未解決の准規設定を自動的に適用(可能な場合) しては、 推奨設定の検索 指奨設定の休奈のキャンセル 推奨設定のりア 	

(2)表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックスにチェックを入れ「OK」をクリックすることで、選択したルールが割り当てされます。

変更監視	現ルール すべて ▼ グループ化しない ▼			Q 検索	-
📑 新規	見 🔹 💼 削除 📰 プロパティ 🛄 複製	10 エクス	ボート 🖌 🌆 列		
*	名前 重要度	種類	前回のアップ		
🔮 🗖	1002781 - Microsoft Windows - A 💼 中	定義済み	2009-06-24		
90	1002778 - Microsoft Windows - S 💼 高	定義済み	2009-06-24		
🔋 🗆	1003517 - Microsoft Windows - S 💶 高	定義済み	2009-06-24		
	1002774 - Microsoft Windows - M e_中	定義済み	2009-06-24		
	1002783 - Microsoft Windows - D 💼 中	定義済み	2009-06-24		
	1002788 - Microsoft Windows - 'A 💼 🕈	定義済み	2009-06-24		
	1002790 - Microsoft Windows - In • 四中	定義済み	2009-06-24		
	1002860 - Microsoft Windows - S 💼 高	定義済み	2009-06-24		
😁 🗆	1002787 - Microsoft Windows - E 💼 中	定義済み	2009-07-15		
	1002784 - Microsoft Windows - I e 中	定義済み	2009-06-24		
🕒 🗆	1002786 - Microsoft Windows - M ඟ 中	定義済み	2009-07-15		
🕲 🗆	1002775 - Microsoft Windows - N 💼 高	定義済み	2009-07-15		
🔮 🗆 👘	1002777 - Microsoft Windows - S 💼 高	定義済み	2015-01-14		
S 🗆 🖸	1003138 - Microsoft Windows - A 💼 中	定義済み	2009-07-15		
9	1002767 - Microsoft Windows - S 💼 高	定義済み	2009-07-29		
8 🗆	1002914 - FTP Server - NettermF ඟ 中	定義済み	2009-09-09		
69 🗆	1002898 - FTP Server - WS_FTP 000000000000000000000000000000000000	定義済み	2009-09-09		
🕒 🗆	1002910 - HTTP Server - IIS 0000000000000000000000000000000	定義済み	2009-09-09		~
アイテム 1	- 100/140			н	<►
				ОК +-	アンセル

(3)変更監視ルールの作成

新規から「新しい変更監視ルール」を選択します。

セキュリティログ監視ルール 割り当て	あり 🔻 グル	ープ化しない 👻			♀ 検索	•
📑 新規 👻 💼 削除 🔲 プロパティ	自複製	🛐 エクスポート	 ■デコーダ 	🏭 列		
■ 新しいセキュリティログ監視ルール	種類	前回のアップ				
😓 ファイルからインポート		(リスト)こ				

(4)新しい変更監視のプロパティ設定

「一般タブ」ルールの名前を設定します。

→般 コンテンツ オプション 暑	明当て対象
┌──般情報	
名前:	wwwコンテンツ監視(cent65)
≣兑B月:	htmlディレクトリ
最小Agent/Applianceバージョン:	6.0.0.0
最小Managerバージョン:	6.0.0
=¥¢m.	
a开加. 香車度·	±
	+

「コンテンツタブ」

テンプレート:ファイル

基本ディレクトリ:例)/var/www/html ディレクトリ

属性:STANDARD

一般 コンテンツ オプション 割り当て対象	
「デンプレート ○ レジストリ値 ● ファイル ● カスタム (XML)	^
「基本ディレクトリー 基本ディレクトリ /var/www/html ☑ サブディレクトリも含む	
- ファイル名 、次のような名前のファイルを含む(1行に1つずつ) 、次のような名前のファイルを含まない(1行に1つずつ)	
?1文字と一致 *0文字以上と一致	
「屑性 「監視する屑性 (1行に1つずつ) STANDARD	-
OK キャンセ	π

※属性について

FileSet において STANDARD にマッピングされる属性は、以下の通りです。

Created、LastModified、Permissions、Owner、Group、Size、Contents、Flags (Windows のみ)、SymLinkPath (Linux の

属性	説明
Created	ファイルの作成日時のタイムスタンプ
LastModified	ファイルの最終更新日時のタイムスタンプ
LastAccessed	ファイルの最終アクセス日時のタイムスタンプ
Permissions	Windows の場合は、ファイルのセキュリティ記述子 (SDDL 形式)。 ACL をサポートする UNIX
	システムの場合は、Posix スタイルの ACL。それ以外の場合は、数値(8 進数)形式の UNIX ス
	タイルの rwxrwxrwx のファイル権限
Owner	ファイル所有者のユーザ ID。通常、UNIX では「UID」と呼ばれます
Group	ファイル所有者のグループ ID。通常、UNIX では「GID」と呼ばれます
Size	ファイルのサイズ
Sha1	SHA-1 ハッシュ
Sha256	SHA-256 八ッシュ
Md5	MD5 八ッシュ

ユーザーズガイド **version** 2.13

Flags	Windows のみ。GetFileAttributes() Win32 API から返されるフラグ。Windows エクスプロ
	ーラでは、これらをファイルの「属性」(読み取り専用、アーカイブ、圧縮など) とみなします
SymLink Path (UNIXのみ)	ファイルがシンボリックリンクである場合は、そのリンクのパスがここに格納されます。
	Windows NTFS では、UNIX ライクなシンボリックリンクをサポートしますが、ファイルでは
	なくディレクトリ専用です。Windows のショートカットオブジェクトは OS では処理されない
	ため、本当の意味でのシンボリックリンクではありません。Windows エクスプローラはショー
	トカットファイル
InodeNumber	ファイルの inode 番号
(UNIX のみ)	
DeviceNumber	ファイルに関連付けられている inode が格納されるディスクのデバイス番号
(UNIX のみ)	
BlocksAllocated	ファイルを格納するために割り当てられるブロック数
(UNIX のみ)	

「オプションタブ」

アラート:このルールによってイベントが記録された場合にアラートにチェックすることでアラート通知を行えます。 リアルタイム監視を許可:リアルタイム監視を許可する場合はチェックを入れてください。 設定後「OK」をクリックすることで新しいルールが作成されます。

一般 コンテンツ オブション 割り当て対象	
□ このルールによって1ペントか記録された場合にアラート	
「リアルタイム監視を許可	
◎ リアルタイム監視を計す	
0	K キャンセル 適用

(5)変更監視ルールの確認/変更

新しく作成したルールにチェックがついていれば割り当てされ有効になっています。

ルールをコンピュータに対して編集するには、ルールを右クリックして [プロパティ...]をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)…] をクリックします。

※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が 適用されます。

設定を終了するには、「OK」をクリックしてください。



(6)ベースラインの再構築【重要】

ベースラインは、変更の検索結果の比較対象となる元の状態です。変更監視対象が構築したベースラインと異なった場合にイベント 記録及びアラート通知を行います。

※OS やアプリケーションの環境変更や Web コンテンツを修正した場合には、都度ベースラインの再構築が必要です。

※変更監視をリアルタイムで行っている場合、コンテンツ変更などでイベント記録及びアラート通知が発生します。

「ベースラインの再構築」をクリックします。

📙 概要	一般詳細イベント
◎ 不正プログラム対策	
💿 Webレビュテーション	変更監視の人ナータス: 批承 (オン)
🞯 ファイアウォール	
(③) 侵入防御	- 李重介始帝
🌍 変更監視	前回の変更のフル検索: 2014-07-14 10:06
🕙 セキュリティログ監視	変更の検索
📟 インタフェース	r<-25/2
🌼 設定 🔍	作成された最新の整合性ペースライン: 2014-07-11 18:30
📮 アップデート	ベースラインの画構築 ベースラインの表示
ಈ オーバーライド	「現在割り当てられている変更監視ルールー
	割り当て割り当て解除 📰 ブロバティ 🚯 エクスポート 🗸 🏭 列
	名前 ▼ 重要度 種類 前回のアップ
	🥘 wwwコンテンツ監視(cent65) (画中 力スタム なし

ベースラインが作成されると、作成された日時が更新され以後監視対象に変更があった場合にイベントとして記録され ます。「ベースラインの表示」をクリックすると保持されているベースラインの一覧を表示できます。

「ベースライン ―――		
作成された最新の整合性ベースライン	2014-07-11 18:30	
ベースラインの再構築	ペースラインの表示	

ベースライン表示

同志示				< 検索	•
1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.		フィンガープリント	ルール名		
ile /var/wwv	w/html/index.html	2014-07-14 11:23:15	wwwコンテンツ監視(cent65)		

8.4. 変更の検索

変更の検索は、「リアルタイム検索」、「予約検索」、「手動検索」に対応しています。

ファイル監視について、Linux ではリアルタイム監視には対応していません。(Windows はリアルタイム監視可) 手動検索または予約検索でのみ検知します。定期的な監視を実行するためには、予約タスクを設定する必要がありま す。

■変更監視の検知動作

エンティティ (監視対象)	Windows	Linux
ファイル (File Set)	0	×
ディレクトリ (DirectorySet)	0	×
インストール済みソフトウェア (InstalledSoftwareSet)	0	0
プロセス (ProcessSet)	0	0
ポート (PortSet)	0	0
ユーザ (UserSet)	0	0
グループ (GroupSet)	0	0
サービス (ServiceSet)	0	
レジストリキー (RegistryKeySet)	×	_
レジストリ値 (RegistryValueSet)	×	_
Windows Management Instrumentation (WQLSet)	0	_

8.5. 変更監視イベント

変更監視設定ルールに合致した場合、変更監視イベントとして記録します。

概要	- 12 I	細イベント					
😨 不正プログラム対策	変更監視イ	ベント すべて 🔹	グループ化しない 👻]	Q 検索		-
💮 Webレビュテーション	期間:	過去1時間	×	•			
🎯 ファイアウォール	コンピュータ:	コンピュータ:	N	cent65	\checkmark		
🛞 侵入防御	🔜 表示	🔄 エクスポート 🔹	省 自動タグ付け	114 死]			
🌔 変更監視	時刻 👻		コンピュータ	理由	タヴ	変更	ラン
セキュリティログ監視	2014-07-	14 19:02:28	cent65	wwwコンテンツ監視(cent65)		アップデート	25
💷 インタフェース							
🎲 設定 🔍							

イベントをダブルクリックすると詳細が表示されます。

→設 55			
一般指導展			
B寺茨川:	2014-07-14 19:02:28		
コンピュータ:	cent65		
イベント送信元:	Agent		
理由:	www.mンテンツ監視(cent65)		
変更: アップデート			
ランク:	25 = 資産評価×重要度 = 1×25		
重要度	ф		
種類	ファイル		
+-:	/var/www/html/index.html		
ユーザ:	ねし		
プロセス:	fal.		
1488			
検索時に次の変〕	Eが検出されました:		
最終更新日·		^	
古山市: 2014	-07-14 10:26:42		
新しい値: 2014	-07-14 19:02:21		
SHA-1:		\sim	
<戻る	次へ >	閉じる	

8.6. 変更監視アラート通知

変更監視イベントに記録された中から、アラートを発するように設定されている変更監視ルールに合致した場合にアラートとして記録され、指定された管理者宛てにメール通知します。

■変更監視ルール「オプションタブ」

変更監視ルールプロパティ	コンテンツ	オプション		
[7ラート				
アラート:	オン			

記録された変更監視アラートは、消去するまで同イベントが発生してもアラート記録及び通知は行われません。

ダッシュボー	-۴	アラート	イベントとレポート	コンピュータ	ポリシー 管理	l		
77-1 UZE		グループ化した	at) 🔻				Q 検索	•
コンピュータ: すべてのコンピュータ 🗸 🗸								
🔟 プロバティ	デブロパティ… 1 消法 1 アラートの設定…							
時刻 👻		重要度	アラート	対象	件名:			
A 2014-07-14 19:0	2	警告	変更監視ルールアラート	cent65	wwwコンテンツ監視(cen	t65)		

※消去とは、発生したイベントの対応や確認が完了したことを意味します。消去するとアラート解決メールが通知されます。

9. 不正アクセス検知 『セキュリティログ監視』

セキュリティログ監視設定について説明いたします。

9.1. セキュリティログ監視の有効化

(1)管理 Web コンソールにログオンしてください。

コンピュータより、セキュリティログ監視を設定するサーバをダブルクリックします。

ダッシュボード	7 7 -ŀ	イベントとレポート	⊐H-+	ターポリシ	~ 管理	!			
コンピュータ	٦L	ビュータ サブグループを	含む ▼ グルー:	プ別 マ				Q 検索	•
		* 新規 🖌 💼 削除… [詳細 処理	 イベント・ 	😰 エクスポート	-	🏭 列		
		名前 🔻 🚦	見 印月	ブラットフォーム	ポリシー		ステータス	前回の通信	前回成功したアップデート
	E	コンピュータ (2)							
		cent65		Red Hat Enter	Linux Server	θ	管理対象 (オンライン)	3分前	37分前
		2008r2		Microsoft Wind	Base Policy	0	管理対象 (オンライン)	1分前	17 時間 前
	«								

(2)サーバの設定画面が表示されます。

「セキュリティログ監視」をクリックします。

コンピュータ: cent65			@ ^
🧱 概要	一般 処理 イベント		
🦁 不正プログラム対策	□ →設		
💿 Webレビュテーション	ホスト名:	cent65	× (前回便用されたIP: 54.95.118.236)
圆 ファイアウォール	1000-10-10-10-10-10-10-10-10-10-10-10-10		
📀 侵入防御			
🔘 変更監視			
🔇 セキュリティログ監視	プラットフォーム:	Red Hat Enterprise 6 (64 bit) (2.6.32- 431.11.2.el6.centos.plus.x86_64)	
📟 インタフェース	グループ:	コンピュータ	•
🎂 設定 🐰	ポリシー:	Base Policy	▼ 編集
	資産の重要度:	tal	✔ 編集
Et 1921-1	セキュリティアップデートのダウンロード	プライマリテナントのRelayグループ	✔ 編集
会 オーバーライド	π.		

(3) セキュリティログ監視のステータスを「オン」にして「保存」をクリックしてください。

これでセキュリティログ監視が有効になります。継承(オン)になっている場合は既に有効になっています。

- 概要							
🦁 不正プログラム対策							
💿 Webレビュテーション	セキュリティロク監視のステータス: 継承 (オン)						
🛞 ファイアウォール	「現在割り当てられているセキュリティログ監視ルール						
③ 侵入防御	割り当て創り当て解除 📰 プロパティ 😰 エクスポート 🔹 🚅 デコーダ 🌆 列						
◎ 変更監視	名前▲ 種類 前回のアップ						
④ セキュリティログ監視	(リストにアイテムがありません)						
🎟 インタフェース							
一 設定	"						
見 アップデート							
碞 オーバーライド							

9.2. セキュリティログ監視(推奨設定)

さまざまな OS とアプリケーションに対応した、定義済みの多数のルールにより、検索対象のサーバに対して、セキュリティログ監視ルール (Windows のセキュリティログ監視ルールや Linux のセキュリティログ監視ルールなど)をコンピュータ に自動で割り当てることができます。一部のセキュリティログ監視ルールは、正常に機能するために、ローカルでの設定 を必要とします。このようなルールをコンピュータに割り当てるか、ルールが自動的に割り当てられると、設定が必要であ ることを通知するアラートが発令されます。

また、推奨設定では定義済みの多数のルールが用意されているため、多数のイベント記録及びアラート通知が発生する可能性があります。必要に応じて重要度レベルを変更するか、監視ログ内容が明確である場合、手動ルール設定を行ってください。

(1)セキュリティログ監視ルールの推奨設定を自動的に適用(可能な場合):を「はい」にします。 「保存」をクリックして設定を保存します。継承(はい)になっている場合は既に有効になっています。

・ ・ ・ ・ ・	
 文支配約< 支配約 42約▲< 43約▲ 43約▲ 43007vj U2NE7454がありません) U2NE7454がありません) U2NE7454がありません) 	
 ○ セキュリティロク監測 (リストにアイテムがありません) ● インタフェース ● 設定 ● アップデート 	
 ● インタフェース ● 設定 ● アップブート 	
※ 設定 ペ □ アップブート	
🛃 アップデート	
<u>∳</u> オーバーライド	
44/2810-	
「推発設定 現在のステータス: 0個のセキュリティログ監視ルールが準制当でられています	
前回の推奨設定の検索: なし	
 ・ ・ ・/> ・ ・ ・ ・	
セキュリティログ監視ルールの推奨設定を自動的に適用(可能な場合)・総承(はい)	
推奨設定の検索 推奨設定をクリア	`
	_

(2) 推奨設定の検索

「推奨設定の検索」をクリックするとサーバに指示が出され検索を実行します。

検索が終了するまで数分から数十分かかります。

※推奨設定の検索は「予約タスク」機能によって定期的に自動で行うことができます。新しいアプリケーションが追加さ れた場合など、自動的にルールを追加するように日単位、週単位などのスケジュールを予約タスクで設定することも できます。

「推奨設定」	
現在のステータス:	O個の侵入防御ルールが割り当てられています
前回の推奨設定の検索:	tal.
 推奨設定の検索結果なし 	
侵入防御の推奨設定を自動的に適用(可能な場合): Iはい V
推奨設定の検索	推奨設定をクリア

(3) 推奨設定の検索が完了するとセキュリティログ監視ルールがサーバに割り当てされます。

例では7個のルールが割り当てられています。

しかし、未解決の推奨設定警告(3個)が出ています。一部ルールによっては自動設定ができず、ログファイルの指定が 必要となります。

慨要			
不正プログラム対策			
Webレビュテーション	セキュリティロラ監視のステージス:オン	· · · · · · · · · · · · · · · · · · ·	
ファイアウォール	「現在割り当てられているセキュリティログ監視ルールー		
受入防御	割り当て割り当て解除 📰 プロパティ 😰 エクスボート 🗸	🖷 デコーダ 🏢 列	
京 面 転加	名前 🔺	種類 前回のアップ	
	State 1002792 - Default Rules Configuration	定義済み 2010-03-19	
2キュリティロク監視	1002797 - Database Server - MySQL	定義済み 2010-07-14	
レタフェース	1002798 - Database Server - PostgreSQL	定義済み 2009-12-23	
	1002823 - Application - Samba	定義済み 2010-09-15	
UE .	1002831 - Unix - Syslog 1002831 - Unix - Syslo	定義済み 2011-07-13	
ップデート	1003443 - Mail Server - Postfix	定義済み 2010-08-25	
ナーバーライド	😵 1003447 - Web Server - Apache	定義済み 2011-03-23	
	「推奨設定」 「推奨設定」 現在のステータス: 7個のセキュリティログ監視ルールだ 前回の推奨設定の検索: 2014-07-10 03.08	増別当てられています	
	▲ 未解決の推奨設定: 3個の追加ルールの割り当て		
	セキュリティログ監視ルールの推奨設定を自動的に適用(可能な場合): は	L1 🗸	
	推旗設定の検索 推旗設定をクリア		
		保存	- Pai

(4)未解決の推奨設定

未解決の推奨設定を確認、設定するためには「割り当て/割り当て解除」をクリックします。

概要	
不正プログラム対策	
Webレビュテーション	
) ファイアウォール	「現在割り当てられているセキュリティログ監視ルールー
侵入防御	割り当て割り当て解除 🗐 プロパティ 😰 エクスポート 🗸 🖷 デコーダ 🏢 列
変更監視	名前▲ 種類 前回のアップ
	😤 1002792 - Default Rules Configuration 定義済み 2010-03-19
セキュリティロク監視	🕙 1002797 - Database Server - MySQL 定義済み 2010-07-14
インタフェース	🕙 1002798 - Database Server - PostgreSQL 定義済み 2009-12-23
10	🔇 1002823 - Application - Samba 定義済み 2010-09-15
88.AE «	🔇 1002831 - Unix - Syslog 定義済み 2011-07-13
アップデート	🕙 1003443 - Mail Server - Postfix 定義済み 2010-08-25
オーバーライド	😵 1003447 - Web Server - Apache 定義済み 2011-03-23
	「推奨設定 現在のステータス: 7個のセキュリティログ監視ルールが書り当てられています 前回の推奨設定の検索: 2014-07-10 03:08
	🔔 未解決の推奨設定: 3個の追加ルールの割り当て
	セキュリティログ監視ルールの推奨設定を自動的に適用(可能な場合): はい
	推調設定の検索 推調設定をクリア
	-

(5) セキュリティログ監視ルールの「割り当てを推奨」を選択します。 推奨設定検索によって割り当てを推奨するルール一覧が表示されます。 旗マークが推奨設定により検索されたルールで、アイコンに歯車がついているルールは、オプション設定ができるもの や設定が必要となるルールです。自動割り当てされない理由は、システム環境によってログファイルの指定場所が異な る場合があるためです。チェックボックのオン/オフでルールの割り当て/割り当て解除を行えます。決定は「OK」をクリ ックしてください。

セキュリティロク監視ルール 割り当てを推奨 マ グルーブ化しない マ			♀ 検索	
📑 新規 ▾ 💼 削除 🔲 ブロパティ 📋 複製 🔹 エクスポート ▾	🖷 デコーダ	. 🏭 列		
名前 🔺	種类與	前回のアップ		
😤 🗖 🏴 1002815 - Authentication Module - Unix Pluggable Authentication Module	定義済み	2013-01-09		
🚳 🗌 🏴 1002828 - Application - Secure Shell Daemon (SSHD)	定義済み	2013-01-09		
🕞 🗌 🏴 1003455 - Application - Telnetd	定義済み	2009-12-23		
			ОК	キャンセル

(6) ルールの設定を行います。

ルールをコンピュータに対して編集するには、ルールを右クリックして [プロパティ...]をクリックします。 ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)...]をクリックします。 ※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が 適用されます。

セキュリティログ監視ルールのプロパティが開きます。

設定タブを選択します。

このセキュリティログ監視ルール にのみ適用されます: Redmine	の遊訳されたラロバティはオーバーライドが可能です。この変更はコンピュータ 🙀 -AWS3.njc.co.jp
セキュリティログ監視ルールプロパティ	設定オプション
一般情報	
名前:	Authentication Module - Unix Pluggable Authentication Module
1938年1	Inspect Pluggable Authentication Modules for events.
	Platform: Non Windows
最小Agent/Applianceパージョン:	6.0.0.0
最小Managerバージョン:	6.0.0
r ID-	
種類:	定義済み
前回のアップデート:	2013-01-09
識別子:	Trend Micro - 1002815
	OK キャンセル 適用

(7)コンピュータに対して設定する場合は継承のチェックを外し、ログファイルを指定します。

例)/var/log/auth.log

ログファイルを指定したら add をクリックしてください。

このセキュリティログ監視ルールの選択されたプロバー にのみ適用されます: Redmine-AWS3.njc.co.jp	ティはオーバーライドが可能です。この変更はコンピュータ	×
セキュリティログ監視ルールブロパティ	Add Remove	
Type of Log File(s): syslog		
5500 - Grouping of the pam_unix rules	初期設定 - 無視 💙	
5501 - Login session opened	初期設定 - 低 (3) 💙	
5502 - Login session closed	初期設定 - 低 (3)	\sim
	OK キャンセル 適用	

(8)監視を行うログファイルが指定されました。必要に応じてログファイルのタイプを選択します。

設定完了は「OK」をクリックしてください。

このセキュリティログ監視ルールの選択されたプロバティはオーバーライドが可能で にのみ適用されます: Redmine-AWS3.njc.co.jp	です。この変更はコンビュータ 🗙
セキュリティログ監視ルールプロバティ 設定 オブション	
Log Files to monitor:	^
Add /var/log/auth.log Remove	
Type of Log File(s): syslog	
This rule matches events decoded as: pam	
5500 - Grouping of the pam_unix rules 初期設定 - 無視	✓
5501 - Login session opened 初期設定 - 低 (3)	~
5502 - Login session closed 初期設定 - 低 (3)	~
5503 - User login failed 初期設定 - 中 (5)	✓
5551 - Multiple failed logins in a small period of time 初期設定 - 高 (10)	✓
ок	キャンセル 適用

(9)セキュリティログ監視ルールの重要度レベル

推奨設定の検索では、下記表の定義に基づき重要度レベルが設定されます。

セキュリティログ監視イベント発生時に設定された重要度レベルにより、イベント記録及びアラート通知を行います。 ※推奨設定では定義済みの多数のルールが用意されているため、多数のイベント記録及びアラート通知が発生する可 能性がありますが、必要に応じて重要度レベルを変更できます。

■セキュリティログ監視ルールの重要度レベルと推奨される使用法

レベル	説明	備考
レベル 0	無視され、処理は行われない	主に誤判定を回避するために使用されます。これらのルールは、他のすべてのルールより先に検索され、セキュリティとは無関係のイベ ントが含まれます。
レベル 1	事前定義された使用法はなし	
レベル 2	システムの優先度の低い通知	セキュリティとは無関係のシステム通知またはステータスメッセージ。
レベル 3	成功した/承認されたイベント	成功したログイン試行、ファイアウォールで許可されたイベントなど。
レベル 4	システムの優先度の低いエラー	不正な設定または未使用のデバイス/アプリケーションに関連するエラー。セキュリティとは無関係であり、通常は初期設定のインストール またはソフトウェアのテストが原因で発生します。
レベル 5	ユーザによって生成されたエラー	パスワードの誤り、処理の拒否など。通常、これらのメッセージはセキュリティとは関係ありません。
レベル 6	関連性の低い攻撃	システムに脅威を及ぼさないワームまたはウイルスを示します(Linux サーバを攻撃する Windows ワームなど)。また、頻繁にトリガされる IDS イベントおよび一般的なエラーイベントも含まれます。
レベル 7	事前定義された使用法はなし	
レベル 8	事前定義された使用法はなし	
レベル 9	無効なソースからのエラー	不明なユーザとしてのログインの試行または無効なソースからのログインの試行が含まれます。特にこのメッセージが繰り返される場合 は、セキュリティとの関連性がある可能性があります。また、admin または root アカウントに関するエラーも含まれます。
レベル 10	ューザによって生成された複数の エラー	複数回の不正なパスワードの指定、複数回のログインの失敗などが含まれます。攻撃を示す場合や、単にユーザが資格情報を忘れた可 能性もあります。
レベル 11	事前定義された使用法はなし	
レベル 12	重要度の高いイベント	システムやカーネルなどからのエラーまたは警告のメッセージが含まれます。特定のアプリケーションに対する攻撃を示す場合もありま す。
レベル 13	通常と異なるエラー(重要度:高)	バッファオーバーフローの試行などの一般的な攻撃パターン、通常の Syslog メッセージ長の超過、または通常の URL 文字列長の超過。
レベル 14	 重要度の高いセキュリティイベント	通常は、複数の攻撃ルールと攻撃の兆候の相関関係の結果。
レベル 15	攻撃の成功	誤判定の可能性はほとんどありません。すぐに対処が必要です。

①セキュリティログ監視ルールの重要度レベル設定

②セキュリティログ監視イベントの発生頻度設定

特定の時間内に発生するイベント回数のしきい値設定が可能です。

例ではログイン失敗やログインセッションオープンなどが180秒以内に6回発生した場合に重要度高(10)としてイベントに記録されます。

※初期値では重要度中(6)以上の場合にイベントに記録されます。

参考ルール名:1002815-Authentication Module - Unix Pluggable Authentication Module (Linux)

このセキュリティロク監視ルールの選択されたプロバティはオーバーライドが可能です。この変更はコンピュータ にのみ適用されます: Redmine-AWS3.njc.co.jp	×
セキュリティログ監視ルールプロバティ 設定 オブション	
	^
Type of Log File(s): syslog	
This rule matches events decoded as: pam	
5500 - Grouping of the pam_unix rules 初期設定 - 無視	
5501 - Login session opened 初期設定 - 低 (3)	
5502 - Login session closed 初期設定 - 低 (3)	
5503 - User login failed	
5551 - Multiple failed logins in a small period of time 初期設定 - 高 (10)	
Frequency (1 to 128): 6	
Time Frame (1 to 86400): 180 secs	
5504 - Attempt to login with an invalid user 初期設定 - 中 (5)	
	. ~
OK キャンセル 適用	

参考ルール名:1002795-Maicrosoft Windows Events (Windows)

	セキュリティログ監視ルールブロバティ 設定 オブション		
	Type of Log File(s): eventlog		^
	18100 - Group of windows rules	初期設定 - 無視 🛛 💙	
	18101 - Windows informational events	初期設定 - 無視 🛛 💙	
	18126 - Remote access login success	初期設定 - 低 (3) 💙	
	18145 - Service startup type was changed	初期設定 - 低 (3) 💙	
	18146 - Application Uninstalled	初期設定 - 中 (4) 💙	
	18147 - Application Installed	初期設定 - 中 (4) 💙	
	18174 - Windows System.ArgumentsOutOfRange Error	初期設定 - 高 (10) 🛛 💙	
	18179 - Log file is cleared	初期設定 - 中 (6) 🛛 💙	
	18193 - The computer has rebooted from a bugcheck. This may be a possible attack (CVE-2012-0180)		
Î	18102 - Windows warning events	初期設定 - 無視 🛛 💙	
5	18125 - Remote access login failure	(See Below)	
Ì	18155 - Multiple Windows warning events) 初期設定 - 高 (10) 🛛 🖌	
	Erequency (1 to 128): 6		
A DESCRIPTION OF	Time Frame (1 to 86400): 120 secs		~
Committee of	ОК	キャンセル 適用	

9.3. セキュリティログ監視(カスタム設定)テンプレートによる設定(Linux 例)

セキュリティログ監視ルールの割り当てを手動で行う方法です。推奨設定とカスタム設定を合わせて使うこともできます。 多数の一般的な OS およびアプリケーション用のセキュリティログ監視ルールが用意されていますが、独自のカスタムル ールを作成することもできます。カスタムルールを作成する場合は、「基本ルール」テンプレートを使用するか、新しいル ールを XML で記述できます。

ルールをポリシーで作成することによりポリシーを割り当てているコンピュータ全てにルールを割り当てることもできます。

(1)手動で設定する場合、「割り当て/割り当て解除」をクリックします。

全て手動で割り当てを行い、自動でルールを適用させない場合は「侵入防御の推奨設定を自動的に適用(可能な場合):」を「いいえ」に設定してください。



(2)表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックスにチェックを入れ「OK」をクリックすることで、選択したルールが割り当てされます。

セキュリラ	ティログ監視ルール すべて マ	グループ化	Utali 👻			Q 検索	-
📑 新規	・ 💼 削除 🔝 プロパティ	📋 複製	🔂 エクスポート	・ 🖷 デコーダ	🌉 列		
	名前 ▲	種類	前回のアップ				~
<u> –</u>	1002792 - Default Rules Configur	定義済み	2010-03-19				
	1002793 - Mail Server - Microsoft	定義済み	2010-09-15				
S 🗆	1002794 - FTP Server - Microsoft	定義済み	2010-07-14				
	1002795 - Microsoft Windows Ev	定義済み	2013-11-07				
۵	1002797 - Database Server - My	定義済み	2010-07-14				
S 🗆	1002798 - Database Server - Pos	定義済み	2009-12-23				
S 🗆	1002799 - Network Monitoring To	定義済み	2010-08-25				
🕙 🗆	1002800 - PBX Server - Asterisk	定義済み	2009-12-23				
S 🗆	1002804 - Mail Server - Courier	定義済み	2009-12-23				
S 🗆	1002807 - Webmail Client - Hord	定義済み	2010-01-14				
🕙 🗆	1002809 - Mail Server - IMAPD	定義済み	2009-12-23				
S 🗆	1002815 - Authentication Module	定義済み	2013-01-09				
🕙 🗆	1002817 - Authentication Tracking	定義済み	2010-02-24				
S 🗆	1002819 - FTP Server - ProFTPD.	定義済み	2010-01-14				
S 🗆	1002823 - Application - Samba	定義済み	2010-09-15				
S 🗆	1002824 - Solaris Auditing - Basi	定義済み	2009-12-23				
S 🗆	1002828 - Application - Secure S	定義済み	2013-01-09				
S 🗆	1002831 - Unix - Syslog	定義済み	2011-07-13				
	1002835 - Web Server - Web Acc	定義済み	2014-02-12				~
						ov	
						OK 4492	v .

(3) セキュリティログ監視ルールの作成

新規から「新しいセキュリティログ監視ルール」を選択します。

セキュリティログ監視ルール 割り当て	あり 👻 グル	/一プ化しない ▼			ヘ 検索	•
前第 → 👔 前除 🗐 プロバティ	自複製	🛐 エクスポート 🔸	🖷 デコーダ	🌉 列		
➡️新しいセキュリティログ監視ルール	種類	前回のアップ				
🔄 ファイルからインポート		(リストニアイラ	テムがありません)			

(4)新しいセキュリティログ監視のプロパティ設定

「一般タブ」ルールの名前を設定します。

一般 コンテンツ ファイル オ:	ブション 割り当て対象
┌→般情報────	
名前:	sshログイン失敗監視
[見 ⁸ 月:	
最小Agent/Applianceバージョン:	6.0.0.0
最小Managerバージョン:	6.0.0

「コンテンツタブ」

テンプレート:基本ルール

ルール ID:自動的に採番されます。

レベル:重要度を設定します。

グループ(カンマ区切り):例) authentication_failed

ルールの説明:ルールの説明を入力してください。

照合するパターン:ログ内で照合する文字パターンです。例) Connection closed

100000	
高 (10)	
authentication_failed	
ssh接続失敗	
	-
Connection closed	
文字列リジョーン	
	-
イベントをトリガ:	
ルールのトリガ時にイベントをトリガ:	
	7
	100000 高 (10) authentication_failed ssh据続失敗 Connection closed 文字ヂリ パターン (ペントをトリガ: ルールのトリガ時にイベントをトリガ: 周 (秒単位) 内に指定の頻度で依存ルールと一致した場合のみ、トリガされます。

「ファイルタブ」

ファイルの追加をクリックして監視対象ファイルを指定します。 ファイル:例)/var/log/secure ※複数ファイルを登録できます。 必要に応じてファイルタイプを設定します。

ファイル: /var/log/secure 新聞 ファイルの追加 「 「	一般 コンテンツ ファイル	オプション割り当て対象	
/var/log/secure syslog 当時 ファイルの追加			
ファイルの追加	/var/log/secure	syslog	▶ 削除
	ファイルの追加		

「オプションタブ」

アラート:このルールによってイベントが記録された場合にアラートにチェックすることでアラート通知を行えます。 最少のアラート重要度:アラート通知が行われる重要度を設定します。

設定後「OK」をクリックすることで新しいルールが作成されます。

ー般 コンテンツ ファイル オプション 割り当て対象

「アラート	
☑ このルールによってイベントが記録された場合にアラート	7
最小のアラート重要度: 中(4)	
	-

(5)セキュリティログ監視ルールの確認/変更

新しく作成したルールにチェックがついていれば割り当てされ有効になっています。

ルールをコンピュータに対して編集するには、ルールを右クリックして [プロパティ...] をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)...]をクリックします。

※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が 適用されます。

設定を終了するには、「OK」をクリックしてください。

セキュリティログ監視ルール 割当てあり ▼ グルーブ化しない ▼			Q 検索	•
📑 新規 🗸 💼 削除 📰 プロパティ 📑 複製 🔂 エクスポート 🔹	 デコータ	第 🏭 列		
名前 ▲	種類	前回のアップ		
S I Linuxログイン失敗監視	カスタム	<i>t</i> ಚட		
			ОК	キャンセル

9.4. セキュリティログ監視(カスタム設定) XML よる設定(Windows 例)

セキュリティログ監視ルールの割り当てを手動で行う方法です。推奨設定とカスタム設定を合わせて使うこともできます。 多数の一般的な OS およびアプリケーション用のセキュリティログ監視ルールが用意されていますが、独自のカスタムル ールを作成することもできます。カスタムルールを作成する場合は、「基本ルール」テンプレートを使用するか、新しいル ールを XML で記述できます。

ルールをポリシーで作成することによりポリシーを割り当てているコンピュータ全てにルールを割り当てることもできます。

(1)手動で設定する場合、「割り当て/割り当て解除」をクリックします。

全て手動で割り当てを行い、自動でルールを適用させない場合は「侵入防御の推奨設定を自動的に適用(可能な場合):」を「いいえ」に設定してください。



(2)表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックスにチェックを入れ「OK」をクリックすることで、選択したルールが割り当てされます。

セキュリラ	ティログ監視ルール すべて マ	グループ化	Utali 👻			Q 検索	-
📑 新規	・ 💼 削除 🔝 プロパティ	📋 複製	🔂 エクスポート	・ 🖷 デコーダ	🌉 列		
	名前 ▲	種類	前回のアップ				~
<u> –</u>	1002792 - Default Rules Configur	定義済み	2010-03-19				
	1002793 - Mail Server - Microsoft	定義済み	2010-09-15				
S 🗆	1002794 - FTP Server - Microsoft	定義済み	2010-07-14				
	1002795 - Microsoft Windows Ev	定義済み	2013-11-07				
۵	1002797 - Database Server - My	定義済み	2010-07-14				
S 🗆	1002798 - Database Server - Pos	定義済み	2009-12-23				
S 🗆	1002799 - Network Monitoring To	定義済み	2010-08-25				
S 🗆	1002800 - PBX Server - Asterisk	定義済み	2009-12-23				
S 🗆	1002804 - Mail Server - Courier	定義済み	2009-12-23				
S 🗆	1002807 - Webmail Client - Hord	定義済み	2010-01-14				
🕙 🗆	1002809 - Mail Server - IMAPD	定義済み	2009-12-23				
S 🗆	1002815 - Authentication Module	定義済み	2013-01-09				
🕙 🗆	1002817 - Authentication Tracking	定義済み	2010-02-24				
S 🗆	1002819 - FTP Server - ProFTPD.	定義済み	2010-01-14				
S 🗆	1002823 - Application - Samba	定義済み	2010-09-15				
S 🗆	1002824 - Solaris Auditing - Basi	定義済み	2009-12-23				
S 🗆	1002828 - Application - Secure S	定義済み	2013-01-09				
S 🗆	1002831 - Unix - Syslog	定義済み	2011-07-13				
	1002835 - Web Server - Web Acc	定義済み	2014-02-12				~
						ov	
						OK 4492	v .

(3) セキュリティログ監視ルールの作成

新規から「新しいセキュリティログ監視ルール」を選択します。

セキュリティログ監視ルール 割り当て	あり マ グループ化しない マ	🔍 検索	•
前規 - □ 前除 □ プロバティ	📋 複製 🚯 エクスポート 🗸 📲 デコーダ	🏭 列	
➡️新しいセキュリティログ監視ルール	種類 前回のアップ		
🔄 ファイルからインポート	(リストにアイテムがありません)		-

(4)新しいセキュリティログ監視のプロパティ設定

「一般タブ」ルールの名前を設定します。

一般 コンテンツ ファイ	レ オプション 割り当て対象
┌一般情報 名前:	windowsログオン失敗監視(ID4265)
』· 見知明:	
最小Agent/Applianceバージ 最小Managerバージョン:	a)/: 6.0.00 6.0.0

「コンテンツタブ」

例) Windows セキュリティイベントでイベント ID4625 が発生した場合に検知させます。

※ID4625 検知は既定のセキュリティログ監視ルール「1002795-Maicrosoft Windows Events」に含まれています。

テンプレート:カスタム(XML) コンテンツ:XML にて記述します。 詳しくはヘルプを参照ください。

記述例

```
<group name="eventid">
```

```
<rule id="100000" level="10">
```

 $<\!\!\text{category}\!\!>\!\!\text{windows}\!<\!\!/\text{category}\!>$

 ${\rm \langle id \rangle}4625 {\rm \langle /id \rangle}$

<description>ログオン失敗</description>

 $\langle /rule \rangle$

```
\langle /group \rangle
```

🥥 windowsログオン失敗監視(ID4265)のプロパティ - Internet Explorer
🖻 https://dss. securityplus.jp /com.trendmicro.ds.loginspectionLogInspectionRulePropertie 😵 証明書のエラー
一般 コンデンツ ファイル オブション 割り当て対象
● 77.2.3.4. (XML)
「コンテンツ:
<pre><group name="eventid"></group></pre>
<category>windows</category>
<id>4d25</id>
() groups
OK キャンセル 適用

「ファイルタブ」

ファイルの追加をクリックして監視対象ファイルを指定します。

ファイル:例)Security ※複数ファイルを登録できます。

必要に応じてファイルタイプを設定します。

	一般 :	コンテンツ	ファイル	オブション	割り当て対象						
Γ											
l	Security				eventlog 🗸			削除			
l	ファイル	の追加									

「オプションタブ」

アラート:このルールによってイベントが記録された場合にアラートにチェックすることでアラート通知を行えます。 最少のアラート重要度:アラート通知が行われる重要度を設定します。

設定後「OK」をクリックすることで新しいルールが作成されます。

ー般 コンテンツ ファイル オブション 割り当て対象									
۲۶-۱									
☑ このルールによってイベントが記録された場合にアラート									
最小のアラート重要度: 中(4)									

(5)セキュリティログ監視ルールの確認/変更

新しく作成したルールにチェックがついていれば割り当てされ有効になっています。

ルールをコンピュータに対して編集するには、ルールを右クリックして [プロパティ...] をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ (グローバル)...]をクリックします。

※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が 適用されます。

設定を終了するには、「OK」をクリックしてください。

9.5. セキュリティログ監視イベント

セキュリティログ監視ルール及び、重要度レベルに合致した場合、セキュリティログ監視イベントとして記録します。

セキュリティログ監視「詳細タブ」

初期値では重要度中(6)以上の場合にイベントとして記録します。

	一般	詳細	イベント				
1	重要度の	ウリッピン:					
	Agent/A 送信:	ppliance	ベントが次の	り重要度以上の場合に、	イベントをSyslogiこ	維承 (中 (6))	\checkmark
	Agent/A	ppliance√ ×/÷	ベントが次の	り重要度以上の場合に、	イベントを記録して	維承 (中 (6))	\checkmark
	DSIVILLY	조1름.					

変更監視イベント

📃 概要	一般 詳細 イベント		
🦁 不正プログラム対策	セキュリティログ監視イベント すべて ▼ グループ化しない	▼	-
📟 Webレビュテーション	期間: 過去24時間		
圆 ファイアウォール	コンピュータ: コンピュータ:	2	
📀 侵入防御	📰 表示 🚯 エクスポート 🔹 省 自動タグ付け 🏭 列		
🔘 変更監視	時刻▼ コンピュータ 理由	タグ 説明 ラ	シク
🔍 セキュリティログ監視	2014-07-15 09:32:03 2008r2 100279	95 - Microsoft Wi Multiple Windows Logo 50	0
	2014-07-15 09:31:59 2008r2 100279	95 - Microsoft Wi Multiple Windows Logo 50	0
🎟 インタフェース	2014-07-15 09:31:51 2008r2 100279	95 - Microsoft Wi Multiple Windows Logo 50	0

イベントをダブルクリックすると詳細が表示されます。

	一般	タグ		
ĺ	一般情報	8		
	時刻:		2014-07-15 08:58:08	
	コンピュ・	ータ:	2008r2	
	イベントう	送信元:	Agent	
	理由:		1002795 - Microsoft Windows Events	
	I兑8月:		Multiple Windows Logon Failures	
	ランク:		50 = 資産評価 × 重要度 = 1 × 50	
	重要度:		高 (10)	
	グルーコ	9:	windows,authentication_failures,	
	プログラ	ム名:		
	イベント: 		WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows-Security-Auditing: (no user):	

9.6. セキュリティログ監視アラート通知

セキュリティログ監視イベントに記録された中から、アラートを発するように設定されているセキュリティログ監視ルールの 重要度レベルを超えた場合にアラートとして記録され、指定された管理者宛てにメール通知します。

■セキュリティログ監視ルール「オプションタブ」

初期値では重要度中(4)以上がアラートの対象になります。

※イベントに記録される重要度が中(6)に設定されている場合、重要度中(6)以上よりイベントに記録されるため、アラート通知の対象になります。

例えば、最少のアラート重要度を高(10)に設定することで重要度中(6)以上はイベントに記録、重要度高(10)以上の 場合のみアラート通知させる設定が可能です。

セキュリティログ監視ルール	カバティ 設定 オブション	
「アラートーーーーー		1
アラート:	オン 🔽	
最小のアラート重要度:	維承 (4)	

記録されたセキュリティログ監視アラートは、消去するまで同イベントが発生してもアラート記録及び通知は行われません。

	ダッシュボー	-۴	アラート	イベントとレポート	コンピュータ	ポリシー	管理			
7	アラート リストビュー ▼ グループ化しない ▼									
=	コンピュータ: すべてのコンピュータ									
III プロパティ 1 消去 🎝 アラートの設定										
	時刻▼ 重要度 アラート			対象		件名:	_			
1014-06-10 18:49		警告	セキュリティログ監視ルールア	dss.security	dss.securityplus.jp (DSM) 1002795 - Microsoft Windows E					

※消去とは、発生したイベントの対応や確認が完了したことを意味します。消去するとアラート解決メールが通知されます。

10. 未許可のアプリケーションを監視『アプリケーションコントロール』

アプリケーションコントロール設定について説明いたします。 アプリケーションコントロールの詳細については以下をご確認ください。 アプリケーションコントロールの設定

10.1.アプリケーションコントロールの有効化

アプリケーションコントロールは、保護対象サーバのソフトウェア変更を継続的に監視し、次のような実行可能ファイルに 対する変更が検出されます。

- ・ユーザによる不要なソフトウェアのインストール
- ・PHP ページ、Python スクリプト、または Java アプリケーションの追加
- ・予定されていない自動アップデート
- ・ゼロデイのランサムウェア

(1)管理 Web コンソールにログオンしてください。

コンピュータより、アプリケーションコントロールを設定するサーバをダブルクリックします。

ŝ	『ッシュボード 処理			コンピュータ	ポリシー 管理				
Ā	スマートフォルダ		リンピュータ サブ	Q. このページを検索					
-	コンピュータ								
	2012	1	▶ 追加 ▼ 💼 削除		◆ 処理 ▼ 首 イベント ▼	・ こうスポ	─▶ ▼ 問列		
>	🖿 ハウジング		名前 ▲	説明	プラットフォーム	ポリシー	ステータス		メンテナンス…
		× :	コンピュータ(4)						
			2012R2AWS		Microsoft Windows Server 201…	Base Policy	● 管理対象(オンライン)		tal.
			ip-10-0-0-123		Amazon Linux 2 (64 bit)	Base Policy	● 管理対象 (オンライン)		なし

(2)サーバの設定画面が表示されます。

「アプリケーションコントロール」をクリックします。



(3)アプリケーションコントロールのステータスを「オン」にして「保存」をクリックしてください。

これでセアプリケーションコントロールが有効になります。継承(オン)になっている場合は既に有効になっています。

	概要	一般 アプリケーションコントロールイベント 判定ログ								
•	不正プログラム対策	アプリケーションコントロール								
•	Webレビュテーション	設定 オン マ								
۲	ファイアウォール	ステータス: 🔍 オフ, インストールされていません								
θ	侵入防御	施行								
0	変更監視	 承認されてしなし、ソフトウェアを明示的に許可するまでブロック 承認されてしなし、ソフトウェアを明示的にブロックするまで許可 								
0	セキュリティログ監視									
D	アプリケーションコントロール	メンテナンスモードでは、新規または変更されたソフトウェアが見つかると、現在有効になっているルールセットの許可さ								
	インタフェース	れるソフトウェアのリストに自動的に追加されます。								
•	設定	ステータス: なし								
	アップデート									

アプリケーションコントロールを有効にするとAgent により検索が実行され、コンピュータにインストールされているすべてのソフトウェアのインベントリが生成されて、検出されたすべてのソフトウェアを許可するルール(許可リスト)が作成されます。環境に応じて、この初期インベントリには15分以上かかることがあります。

アプリケーションコントロールが有効化され、最初のソフトウェアインベントリ検索が完了すると、次の状態になります。 [コンピュータ]の [ステータス] が「アプリケーションコントロールルールセットの構築中」から「管理対象(オンライン)」 に変わります。

[イベントとレポート]→[イベント]→[システムイベント] に、「アプリケーションコントロールルールセットの作成開始」および「アプリケーションコントロールルールセットの作成完了」が記録されます。

アプリケーションコントロールルールセットの作成完了イベントサンプル イベント: アプリケーションコントロールインベントリ検索の完了 説明: アプリケーションコントロールのインベントリ検索が完了しました。 アプリケーションコントロールインベントリに追加されたアイテム数:10,555 検索されたアイテム数: 39,408 アプリケーションコントロールインベントリの検索時間: 11 秒

10.2.アプリケーションコントロール機能の確認

アプリケーションコントロールが機能していることを確認するために、コンピュータに実行可能ファイルをコピーするか、プレーンテキストファイルに実行権限を追加して、そのファイルを実行、またはアプリケーションをインストールしてみます。

承認されていないソフトウェアに対する設定に応じて、ファイルがブロックまたは許可されます。アプリケーションコントロ ールで初期許可ルールの構築または共有ルールセットのダウンロードが完了している場合、変更が検出されると [処 理] タブに表示され、このタブで許可ルールとブロックルールを作成できます。また、アラートを設定していれば、承認さ れていないソフトウェアが検出されたときやアプリケーションコントロールによってソフトウェアの起動がブロックされたとき にアラートも表示されます。ソフトウェアの変更が存在しなくなるまで、または最も古いデータがデータベースから削除さ れるまで、イベントは保持されます。



10.3. メンテナンスモード

コンピュータへのパッチ適用、ゴールデンイメージのアップデート、実稼働環境へのプッシュなどの際は、必ずメンテナンスモードを有効にして、新規または変更されたソフトウェアをルールセットに追加してください。 期間を選択してオンにします。

予定されているメンテナンス期間が終了した時点で、メンテナンスモードは自動的に無効になります。または、アップデ ートの完了時に手動でメンテナンスモードを無効にする場合は、[無期限]を選択します。



メンテナンスモードをオンにするとメンテナンスモードが「開始を要求」に変更され、

	コンピュータ	Q このページを検索				
	+ 追加 👻 💼	削除 🔳 詳細	↓ 処理 ・	■ エクスポ・	-▶ ▼ ■ ■ 列	
	名前	説明	プラットフォーム	ポリシー	ステータス 💌	メンテナンスモード
~	コンピュータ(4)					
	ip-10-0-0-123	0	Amazon Linux 2 (64 bit)	Base Policy	● 管理対象(オンライン)	開始を要求

オンに代わります。オンにしている間にソフトウェアをインストールまたはアップグレードします。

コンピュータ サブグループを含む、	グループ別 🔻		Q このページを検索
+ 追加 ▼ 💼 削除 🗐 詳細	★ 処理 ▼	・ Eエクスポート ・ 思列…	
名前 説明	プラットフォーム	ポリシー ステータス *	メンテナンスモード
✓ コンピュータ(4)			
ip-10-0-0-123	Amazon Linux 2 (64 bit)	Base Policy 🛛 🌔 管理対象 (オンライン)) オン, 無期限

メンテナンスモードを無効するにはメンテナンスモードのステータスを「オフ」にします。

10.4.アプリケーションコントロールアラート通知

ソフトウェア変更が検出された場合アラートとして記録され、指定された管理者宛てにメール通知します。

ダッシュボード 処理	アラート イベントとレポート コンピュータ ポリシー 管理
アラート 概要ビュー 、	▼ 時間別 ▼
コンピュータ: すべてのコンピ	' <u>-</u> -タ ▼
 1台のコンピュータで ソフトウェア変更が検ば 詳細非表示 	ジ フトウェア変更が検出されました。 出されました。詳細は、「処理] 画面の [ソフトウェア変更] を参照してください。
時刻: 前回のアップデート・	2018-10-11 20:48 2018-10-11 20:48
重要度:	활범
コンピュータ:	ip-10-0-0-123

11. 共通オブジェクト

共通オブジェクトの基本的な使用方法について説明いたします。

11.1.共通オブジェクトリスト

ポリシーやルールなどの多くの構造体で共有できるオブジェクトとなります。ポリシーエディタとコンピュータエディタの画面にも同じオブジェクトー覧が表示され、多数の一般的な IP リストやポートリストが用意されており、独自のカスタムリストを作成することもできます。カスタムリストを作成する場合は、ポリシー共通オブジェクトのリストより作成します。

■リスト 主にファイアウォールで使用 IPリスト MACリスト ポートリスト

主に不正プログラム対策の除外設定などで利用 ディレクトリリスト ファイルリスト ファイル拡張子リスト

■ポートリスト

ダッシュオ	ベード 処理 アラート	イベン	ト とレボー	-ト コンビュ	ータ	ボリシー	- 管理	ŧ			
魯 型	シー	ポー	トリスト								
、 ♥ 井シ	通オブジェクト	-	_	-			-				_
> 🖶	ルール	1 兼	f規 ▼	面削除	I	パティ	● 複製		エクスポート	*	围.列
~ 🗎	リスト	名前	•		詳細	I					
	■ ₽リスト	🗎 Alt-N	WebAdmin	Server	1000						
	MACUZE	🗎 Answe	rBook2		8888						
	■ デルクトリリスト	🗎 Arkeia	Server		617						
	ファイルリスト	🗎 Back (Back Orifice		1337,	1387, 31337					
	■ ファイル拡張子リスト	🗎 Backd	oor TCP		3241	3, 30029, 79	9, 48, 6789, :	2343			
		🗎 Backd	oors UDP		2718	4, 1183, 666	5				
	팀 사·トリスト	🗎 Badku	p Server C	A BrightStor A…	• 6070,	6071,6050)				
> 🌍	その他	🗎 Backu	p Server El	viC Dantz Retr••	• 497						
		🗎 BakBo	ne NetVau	lt Server	2003	1					
		🗎 CA Ar	CA Antivirus Console Server		1216	12168					
		🗎 CA Br	CA BrightStor ARCServe		4152	41524, 41523					
		🗎 CA Ur	icenter		4105	4105					
		🗎 CFEna) CFEngine		5308	5308					
		🗎 Cisco	Cisco Collaboration Server		80						
		🗎 Olient	Client to Domain Controller (TCP)			3, 135, 139,	445, 3268,	3269			
		-		,							

12. 予約タスク(スケジュール設定)

予約タスクの基本的な使用方法について説明いたします。

12.1. 予約タスク概要

[予約タスク] 画面では、特定の共通タスクを自動化または予約できます。 時間単位、日単位、週単位、月単位、1回のみでのスケジュール設定が可能です。

■予約タスクの種類

①セキュリティアップデートのダウンロード: 定期的にセキュリティアップデートを確認し、使用可能なアップデートがある場合、ダウンロードしたり、オプションでインストールしたりします。
 ※ルールやパターン更新に必須のため、初期値で1日1回実行する予約がされています。(1時間毎を推奨)

②コンピュータの推奨設定を検索: Deep Security Manager によって、コンピュータ上の一般的なアプリケーションが検索 され、検出結果に基づいた推奨設定が作成されます。 侵入防御、セキュリティログ監視、変更監視ルールの推奨設定を自動化できます。 アプリケーションの追加や削除を自動的に検出させるために1週間に1回程度の実行を推奨します。

- ③コンピュータの不正プログラムを検索:不正プログラム検索の予定を作成します。検索の設定は、各コンピュータの ポリシーまたはコンピュータのエディタの [不正プログラム対策] 画面で指定したものと同じです。 不正プログラム対策の予約検索機能に相当します。
- ④コンピュータの変更を検索: Deep Security Manager によって、コンピュータの現在の状態とベースラインを比較するための変更の検索が実行されます。

⑤レポートの生成: レポートを自動生成し、オプションでユーザのリストへ送信します。

⑥未解決アラートの概要: すべての未解決アラートをリストしたメールを生成します。

⑦コンピュータのオープンポートを検索:1つ以上のコンピュータに対して定期的なポート検索を予約します。検索は、 特定のコンピュータグループに所属する個別のコンピュータまたは全コンピュータを指定できます。検索するポートは、 ポリシーまたはコンピュータのエディタの[設定] 画面の[検索] タブで定義されたものです。

⑧コンピュータの検出:使用しません。

⑨ポリシーの送信:使用しません。

12.2. 予約タスクの設定例 ①セキュリティアップデートのダウンロード

(1)管理 Web コンソールにログオンしてください。

管理より、予約タスクを選択します。

コンポーネントアップデートタスクをクリックします。

ダッシュボード	7 7 -ŀ	イベントとレポート	コンピュータ	ポリシー	管理			
🎆 システム設定	予約ら	なり				-	🔍 検;	*
▶ 予約タスク	:	所規 📋 削除 🔟 コ	プロバティ [] 複製	▶ 今すぐタスク	を実行			
	名前	Ĵ ▲	種類	スケジュール		前回の実行日時	次回の実行日時	詳細
■ 🎾 ユーザ管理	ど コン	ボーネントアップデートタスク	セキュリティアップデ	ー 毎日14:00)	2014-07-16 14:55	2014-07-17 14:00	選択したセキュリティアップデートの取得
📑 アップデート								

(2)コンポーネントアップデートタスクのプロパティが開きます。

コンポーネントアップデートタスクは1日に1回となっていますが、時間単位(毎時)を推奨します。 決定は「OK」をクリックしてください。

6	コンポーネントフ https://dss. sec	?ップデートタスクのプロパティ 💶 💷 💳 💳
	 一般 タスク詳 一般情報 名前: 	細 ロンボーネントアップデートタスク ×
	種類: -スケジュール情報	セキュリティアップデートのダウンロード
	 ・ 日単位 ・ 週単位 ・ 月単位 ・ 月単位 ・ 1回のみ 	開始日: 2014-07-03 開始時刻: 14:00 ② ● 毎日 ○ 平日 ○ 2 ▼ 日ごと
		OK キャンセル 適用

12.3. 予約タスクの設定例 ②コンピュータの推奨設定を検索

(1)管理 Web コンソールにログオンしてください。

管理より、予約タスクを選択します。

新しく予約タスクを作成する場合は、新規をクリックしてください。

ダッシュボード	7 5 -ŀ	イベントとレポート	コンピュータ	ポリシー	管理				
ジステム設定 マンテム設定	予約タ	ウ				-	🔍 検知	*	
 ゴイベントペースタスク 	2前	(視…	パティ <u>し</u> 複製	今すぐタスク スケジュー	7を実行 ・ル	前回の実行日時 次回の実行日時 詳細			
 マイセンス 国 ユーザ管理 	עב 💈	ポーネントアップデートタスク	セキュリティアップ	デー 毎日14:00)	2014-07-16 14:55	2014-07-17 14:00	選択したセキュリティアップデートの取得	
📑 アップデート									

(2)予約タスクの種類を選択します。

種類:「コンピュータの推奨設定を検索」を選択します。

自動実行される単位を選びます。

※推奨設定の検索はサーバに負荷がかかる可能性があるため、開始時間は業務時間外などに予約します。

また、OS やアプリケーション環境は頻繁に変更されることは少ないため、週単位ごとの実施を推奨します。 選択後、「次へ」をクリックしてください。



(3)開始時刻、週ごと、曜日を選択します。

選択後、「次へ」をクリックしてください。


(4) 推奨設定検索を行うコンピュータを指定します。

すべてのコンピュータ、グループ、使用ポリシー、コンピュータを選択できます。

コンピュータ毎に異なるスケジュールにする場合は、コンピュータを指定し、別々の予約タスクを作成します。

選択後、「次へ」をクリックして下さい。

推奨設定を検索するコン	ビュータを指定してください。		
⊚ すべての⊐ンピュー	9		
○ グループ:	コンピュータ	-	
	☑ サブグループも含める		
○ 使用ポリシー:	tal.	*	
	■ サブボリシーも含める		
○ コンピュータ:	2008r2	\checkmark	
		<戻る 次へ	キャンセル

(5)設定の確認が表示されます。

名前:任意で入力することもできます。

完了後にタスクをすぐに実行する場合は、「完了」でタスク実行にチェックを入れます。

設定完了は「完了」をクリックしてください。

この予約タスクの一意の	名前を入力してください。
名前: 種類: スケジュール 次回の実行: 詳細:	週単位 コンピュータの推奨× コンピュータの推奨設定を検索 毎週の月曜03:00 2014-07-21 03:00 すべてのコンピュータ
[売了] でタスクを実	7

(6) 推奨設定検索の予約タスクが作成されました。

スケジュールや前回の実行日時が確認できます。

変更する場合は、予約タスクの名前をダブルクリックしてください。

ダッシュボード	7 5 -ŀ	イベントとレポート	コンピュータ	ポリシー	管理			
🌼 システム設定	予約タ	マク					へ 検索	
▶ 予約タスク		視… 💼 削除… 🔲 ヺ	パフィー・ 📋 複製	▶ 今すぐタスク	を実行			
	名前	· •	種類	スク	アジュール	前回の実行日時	次回の実行日時	目羊糸田
■ № ユーザ管理	👔 🖘	ポーネントアップデートタスク	セキュリティ	(アップデー 毎日	14:00	2014-07-16 14:55	2014-07-17 14:00	選択したセキュリティアップデート
	🐉 週単	位コンピュータの推奨設定を	検索 コンビュータ	ぬの推奨設 毎;	週の月曜03:00	なし	2014-07-21 03:00	すべてのコンビュータ

13. 管理者へのメール通知設定

管理者への通知メール設定について説明します。

13.1.アラート通知メールの受信設定

(1)管理 Web コンソールにログオンしてください。

管理より、ユーザを選択してください。

管理 Web コンソールにログオンしている管理者のユーザ名が登録されています。

ユーザ名をダブルクリックします。

※support_MasterAdmin は変更、削除できません。

ダッシュボード	7 7 -ト	イベントとレポート	コンピュータ	ポリシー	管理	
 ジステム設定 予約タスク 	ユーザ	7 役割別 ▼	ار		na autor	
ー		17月	前 ロック	·アウト ログオン	メディレンドリとの.	10月月 1日 10月 1日 ジオン
E 🌮 ユーザ管理	E Full.	Access (2) ss_user005		V	2014-	07-16 18:12
▲ 役割 ■ 連絡先 ■ アップデート	<u>&</u> (support_MasterAdmin			2014-	07-16 18:52
	~~					

(2) ユーザ名のプロパティが表示されます。

「連絡先情報タブ」を選択します。

メールアドレス:管理者のメールアドレス

アラートメールを受信にチェックを入れて「OK」をクリックしてください。

一般 連絡先情報	設定		
「連絡先情報			
電話番号:			
携帯電話番号:			
ポケットベル番号:			
メールアドレス:	security@security.co.jp	×)
┃ ✔ 主担当者の連絡先			
┃ ☑ アラートメールを受	ſĒ		

アラートメール受信者(メールアドレス)を複数登録する場合はユーザを作成してください。

(3) アラートメールサンプル

詳細は管理 Web コンソールのイベントやアラートより確認します。

ご使用の Deep Security アカウントについて次のアラートが発生しました:

アラート:1台のコンピュータで、不正プログラム検索設定(Default Real-Time Scan Configuration)アラートが発生しました 重要度:警告 アラートのインスタンス ID: 7471 時刻:2018-10-02 10:59 前回のアップデート:2018-10-02 10:59

説明:1台以上のコンピュータで、アラートを発するように設定された不正プログラム検索設定によってイベントが発生しました。 コンピュータ:

2012R2—SV

14. 管理 WEB コンソール

管理 Web コンソールの基本的な使用方法について説明いたします。

14.1.ダッシュボード

ダッシュボードには、Deep Security システムの状態を一目で理解できるビューがあります。ログオンすると、前回のセッション時のダッシュボードのレイアウトが保持されています。

情報パネル(「ウィジェット」)は、ドラッグすることで、画面上の表示位置を調整できます。また、ウィジェットをダッシュボードの表示に追加したり、削除したりすることもできます。

ダッシュボードからウィジェットを削除するには、右上隅の [X] をクリックします



ウィジェットの追加/削除



14.2.アラート

[アラート] 画面には、有効なアラートがすべて表示されます。アラートは、同じようなアラートをグループ化した概要ビュー、またはすべてのアラートを個別に一覧表示したリストビューで表示できます。これらの2つのビューを切り替えるには、 画面のタイトルの [アラート] の横にあるドロップダウンメニューを使用します。

アラートに対して適切な処理を実行したら、対象のアラートの横にあるチェックボックスをオンにし、[選択対象を消去] リ ンクをクリックして、アラートを消去できます。(リストビューでは、アラートを右クリックすると、ショートカットメニューにオプ ションのリストが表示されます。)

※「アップデート失敗」などの消去できないアラートは、アラートの状態が存在しなくなったときに自動的に消去されま す。



アラートには、システムアラートとセキュリティアラートの2種類があります。システムアラートは、Agentのオフライン化やコ ンピュータの時計の変更などのシステムイベントによってトリガされます。セキュリティアラートは、侵入防御、ファイアウォ ール、変更監視、およびセキュリティログ監視の各ルールによってトリガされます。アラートは、[アラートの設定...]をクリ ックして設定できます

各アラートをダブルクリックするとアラートのオン/オフを設定できます。



14.3.イベントとレポート

ダッシュボード 処理	アラート イベントとレポー	- 	ータ ポリシ	— 管理		
> 首 イベント	システムイベント	すべて 🗸	グループ化しない	● ● このページを検索		
	期間: 過去24時間	1	•			a
	コンピュータ: すべてのコ	ンピュータ	•			
	■ 表示 🗈 エクスポ		動タグ付け	田, 列		
	時刻 ▼	レベル	イベントID	1~~~~~	タグ	*
	(■ 2018-10-11 04:00:26	情報	273	セキュリティアップデート: セキュリティアップデートの確認とダウンロード要求		
	2018-10-11 04:00:26	情報	273	セキュリティアップデート: セキュリティアップデートの確認とダウンロード要求		
	2018-10-11 04:00:26	情報	273	セキュリティアップデート: セキュリティアップデートの確認とダウンロード要求		
	2018-10-11 04:00:26	情報	1600	Relayグループのアップデートの要求		
	2018-10-11 04:00:26	情報	564	予約タスクの開始		

システムイベントや不正プログラムイベントなどを閲覧、検索、エクスポートできます。

単独レポート

PDFまたはRTFの形式でレポートを生成します。[レポート] 画面で生成されたほとんどのレポートには、日付範囲、コン ピュータグループ別のレポートなどの設定可能なパラメータがあります。パラメータのオプションは、それらが適用されな いレポートの場合は無効になります。

定期レポートは予約タスクで設定します。

ジェホード 処理 アラー	urity ト イベント	侵入防御レポート 変更監視の詳細な変更レポート 変更監視ベーフライル・ポート	⑦ ヘルプ 〇 サ	ポート情報 ✔ 🗨 ヘルプセンターの検索	
 首 イベント システムイベント 	レポートの生	変更監視レポート			
> 😵 不正プログラム対接 単独	虹ポート 定 ポート	推奨設定レポート 攻撃レポート			A
● 一 ファイアウォールイ ● 侵入防御イベント		概要レポート 攻撃レポート ▼	▲	(/3L)	•
	▶ ·: 形	ポータブルドキュメントフォーマット (PDF) 🔹 🔻			
 ・ マキュリティロク監 ・ ・ ・	ゴ				
🗠 レポートの生成 🏾	● すべて:				

14.4.コンピュータ

[コンピュータ] セクションでは、コンピュータを管理および監視できます。この画面は定期的に自動更新され、最新情報 が表示されます (更新頻度はユーザごとに変更できます。[管理]→[ユーザ管理]→[ユーザ] の順に選択し、ユーザを ダブルクリックしてユーザの [プロパティ] 画面を開きます。コンピュータリストの更新頻度は、[設定] タブの [更新頻 度] エリアで設定できます)。

ダッシュボード 処理	アラート	・ イベントと	レポート	コンピュータ	ポリシ	/—	管理					
🔁 スマートフォルダ		コンピュータ	サブグル	ープを含む 🔻	グルー	プ別 ▼	-			Q 201-3	じを検索	•
📑 コンピュータ						_			_			
E 2012 ····		▶ 追加 ▼	前 削除	■ 詳純田	∮ 処理	*	I イベント ▼	🖹 エクスポート	*	睥,列		
> 🖿 ハウジング		名前 ▲		説明	プラ	ットフォ・	-4	ポリシー		ステータス	メンテナ…	ポリシーの送信の
	× :	コンピュータ(4)										
		2012R2AWS	;		Micro	osoft Wir	ndows Server 201…	Base Policy	• î	管理対象 (オンライン)	なし	0分前
		ip-10-0-0-1	23		Amaz	on Linu:	ı×2 (64 bit)	Base Policy	• î	管理対象(オンライン)	なし	0分前

コンピュータを右クリックすると「処理」から「推奨設定の検索」や「不正プログラム対策のフル検索」などをショートカットで 実効できます。

ダッシュボード 処理	アラート イベントとレポート コンピュータ ポリシー 管理	
 スマートフォルダ コンピュータ 	コンピュータ サブグルーブを含む ▼ グルーブ別 ▼ ● 有効化/再有効化 ● 無効化	Q このページを検索
2012	+ 追加 ▼ 商 削除 目 詳細	
> 🖿 ハウジング	名前・ 説明 ブラットフォーム ポリシー ・ コンピュータ(4) ・ セキュリティアップデ	ートのダウンロード ートのロールバック
	■ 2012R2AWS ■ ip=10-0-0-123 すべて選択(4)	9分前
	↓ ■ ip-10-0-0-79 ■ 選択したアイテムをCSV形式でエクスポート	アップグレード 18 分前
	■ ip-10-0-2-30 ■ 選択したアイテムをXML形式でエクスポート(インポート用)	18 分前
	 ▶ / 加理 ▶ 推奨設定をクリア 	
	首 イベント ● 不正プログラムのク	イック検索
	「前削除 「「削除	レ検索
	■ オープンボートの検:	秦
	□ 詳細… () 変更の検索	
	② 整合性ベースライン	の再構築

設定変更や推奨設定検索の実行を行った場合、ステータスに~の保留中と表示されます。 これは、コンピュータが管理サーバへの接続を5分間隔で行っているため、指示待ちの状態を表します。 指示が実行されると~の実行中と表示され、完了するとオンラインに戻ります。

ダッシュボード 処理 🕽	アラート イベントとレポート コンピュータ ポリシー 管理	
🔁 スマートフォルダ	コンピュータ サブグループを含む ▼ グループ別 ▼	Q
📑 コンピュータ		
2012		
> 🛅 ハウジング	名前 * 説明 プラットフォーム ポリシー ステータス	
	✓ コンピュータ(4)	
	■ 2012R2AWS Microsoft Windows Server 201… Base Policy ● 不正プログラムの手動検索の	/保留中
	■ ip-10-0-0-123 Amazon Linux 2 (64 bit) Base Policy ● 管理対象 (オンライン)	

列の追加/削除

列...をクリックすると「前回の通信」や「バージョン」など表示列のカスタマイズを行えます。

ダッシュボード 処理	アラート イベントとレポート コンピュータ ポリシー 管理	
🚺 スマートフォルダ	コンピュータ サブグループを含む ▼ グループ別 ▼	Q
🗐 コンピュータ		
2012		
> 🖿 ハウジング	名前 * 説明 プラットフォーム ポリシー ステータス	
	 コンピュータ(4) 	
	冒 2012R2AWS Microsoft Windows Server 201… Base Policy 💿 不正プログラムの手動検索の	保留中
	冒 ip-10-0-0-123 Amazon Linux 2 (64 bit) Base Policy 🛛 ● 管理対象 (オンライン)	

歹	〕の追加/削除
1	説明
1	プラットフォーム
	不正プログラム対策のステータス表示
	Webレビュテーションのステータス表示
	ファイアウォールのステータス表示
	侵入防御のステータス表示
	変更監視のステータス表示
	セキュリティログ監視のステータス表示
	アプリケーションコントロールステータスの表示
	メンテナンスモード
	資産評価
	前回の通信
	ポリシーの送信の成功
	ポリシーの送信の要求 🗸
	列名で並べ替え OK キャンセル

14.5.ポリシー

管理 魯 ポリシー ポリシー > 🗳 共通オブジェクト 🎦 新規 🔻 面削除... і झिं⊞... 💼 複製 📑 エクスポート 🔻 🗸 🍓 Base Policy 🧿 リアルタイム 不正プログラム対策 > 🐴 Deep Security Webレビュテーション: オン • オフ, 19 ルール ファイアウォール: 🏠 Linux Server ● 防御, ルールなし 侵入防御: 🍅 Solaris Server 変更監視 🕚 リアルタイム, ルールなし セキュリティログ監視 🔹 オン, ルールなし > 🍓 Windows アプリケーションコントロール: ● オフ 🐴 Base Policy (2) このポリシーを使用するコンピュータ 4 滀 Firewall

[ポリシー] 画面には、階層型のツリー構造で親子関係を示す既存のポリシーが表示されます。

ポリシーでは、ルールや設定をまとめて保存し、複数のコンピュータに簡単に割り当てることができます。

ポリシーをコンピュータに割り当てるには

1.管理 Web コンソールの[コンピュータ] に進みます。

2.コンピュータリストからコンピュータを選択し、右クリックして [処理]→[ポリシーの割り当て] を選択します。

3.階層ツリーからポリシーを選択し、[OK] をクリックします。

14.6.管理

システム設定や予約タスク、ユーザ管理などを設定します。

システム設定はお客様運用に支障が出る可能性があるため、基本的に変更しないようお願いします。

ダッシュボード 処理	アラート イベントとレポート エンピュータ ポリシー 管理
🍄 システム設定	システム設定
設 予約タスク 設 イベントベースタスク ♪ ライセンス	Agent アラート コンテキスト イベトの転送 ラング打け システムイベント セキュリティ アップデート スマートフィードバック Connected Three ホスト名
> 🔩 ユーザ管理 > 🌒 アップデート	 □ JZ2ユージをドビ虫類していてドの変更が検出された場合、JZ2ユージのレバスト名」を自動が入り更新 Agentからのリモート有効化 ② Agentからのリモート有効化と許可 ③ 任意のコンピュータ ◎ 既存のコンピュータ
	 次のPリストにあるコンピュータ: 初リ当てるポリシー(有効化スクリプトによってポリシーが割り当てられていない場合): Agentによるホスト名指定を許可 同じ名前のコンピュータがすでに存在する場合: クローンAgentの再有効化 不明なAgentの再有効化

