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 2.10

日本事務器株式会社

改版履歴

Version	日付	変更内容
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＞

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
お客様システムへインストールする 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://success.trendmicro.com/jp/solution/1313399

(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/jp/solution/1098225

(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 バージョンアップ手順

(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、SSL 資格情報(秘密鍵)を管理サーバ(管理コンソール)にインポートする必要があります。
※復号を行うためサーバへの負荷が高くなる可能性があります。
※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。
設定手順やサポート対象の暗号化方式については以下サイトを参照ください。

SSL または TLS トラフィックの検査

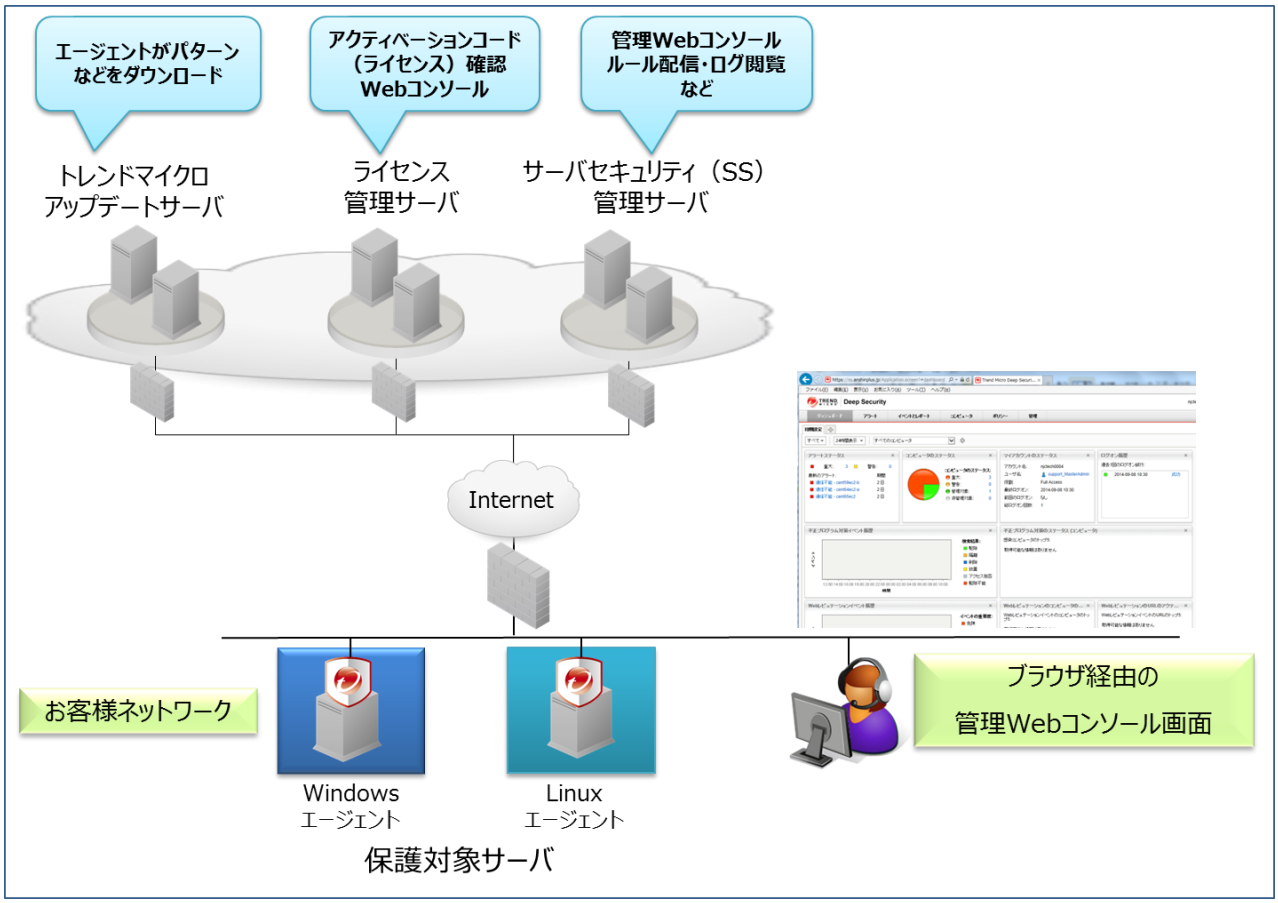
(10) Docker 環境の保護については以下サイトをご確認ください。
Docker コンテナの保護

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/jp/solution/1114910

1.2. システム構成イメージ

■イメージ図



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　　} 管理 Web コンソールアクセス用
＜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　　} ライセンス情報確認用

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-b319-6c48b987556f

※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

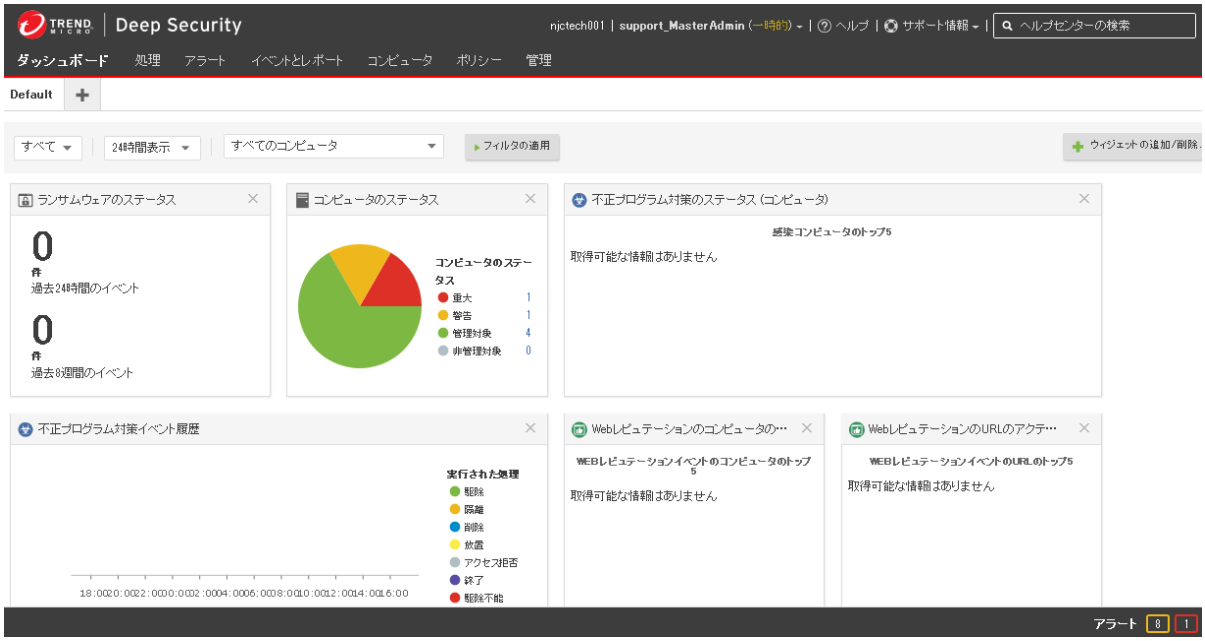
※上記ライセンス登録完了メールおよびアカウント登録完了メールはサンプルです。お客様へ送信されたライセンス登録完了のお知らせメールに記載されているアクティベーションコードを使用してください。

(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。

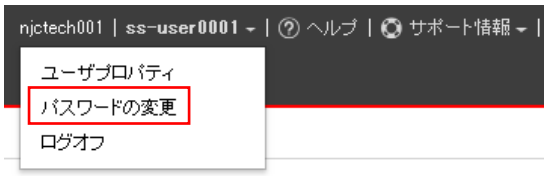
アカウント通知メールに記載されているアカウント名、ユーザ名およびパスワード通知に記載されているパスワードを入力してログオンをクリックしてください。

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。



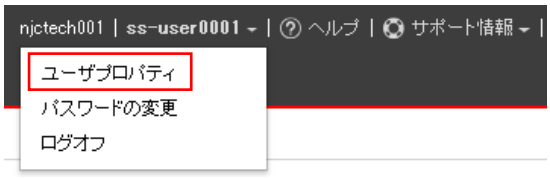
(3) ログオンパスワードの変更

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。



(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。

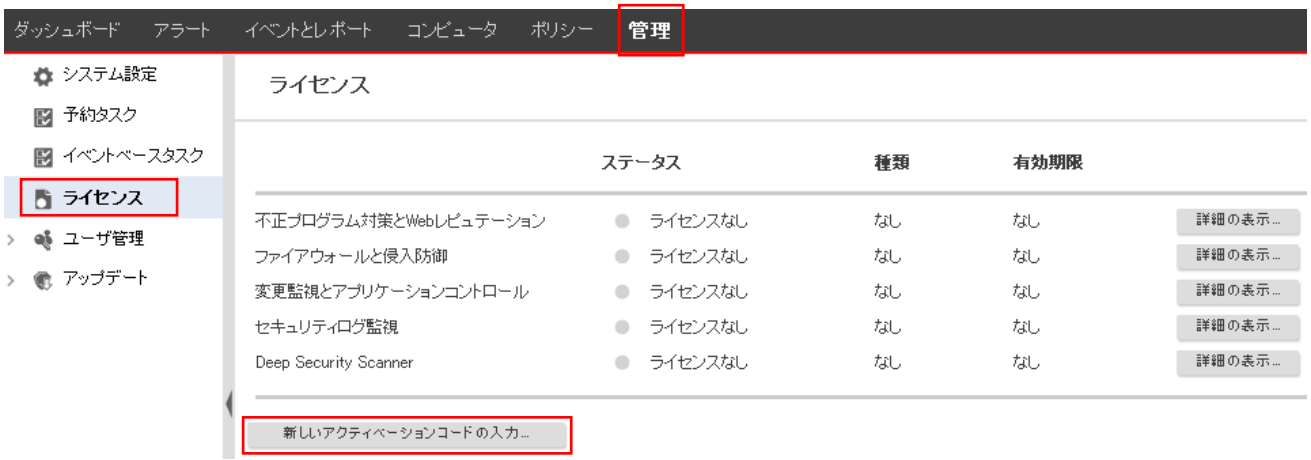


2.2. 利用ライセンスの登録 ＜アクティベーションコード登録＞

(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。

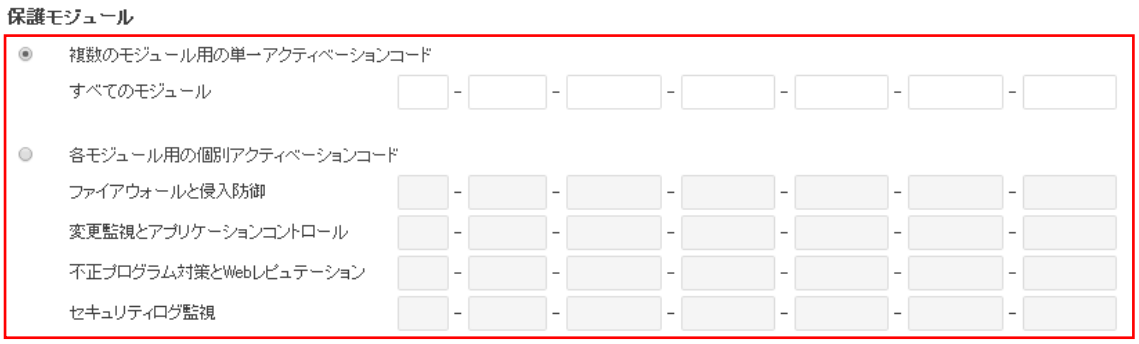


(2)アクティベーションコード登録

「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)

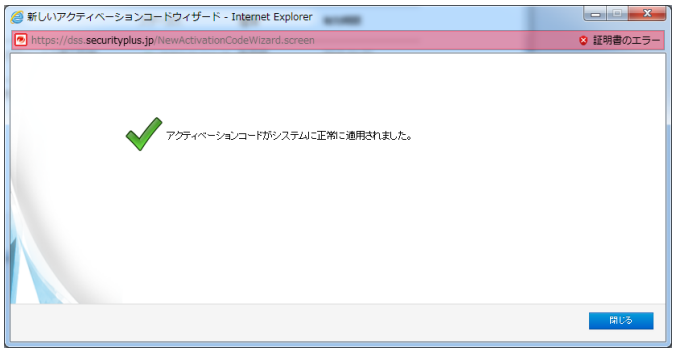


正しく入力が完了すると登録したライセンスが有効になります。

※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。

「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。

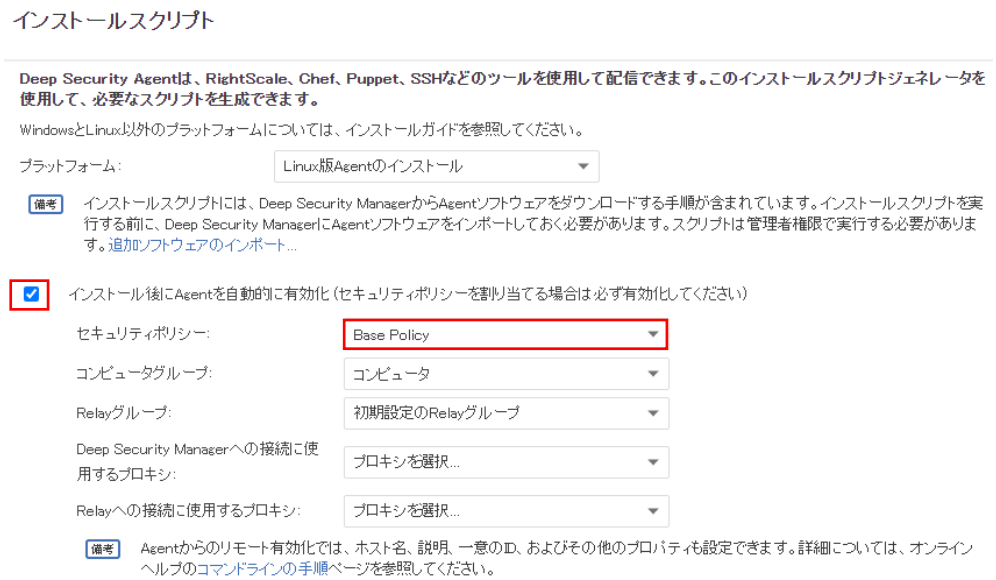
(2)パラメータの設定

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。

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。)



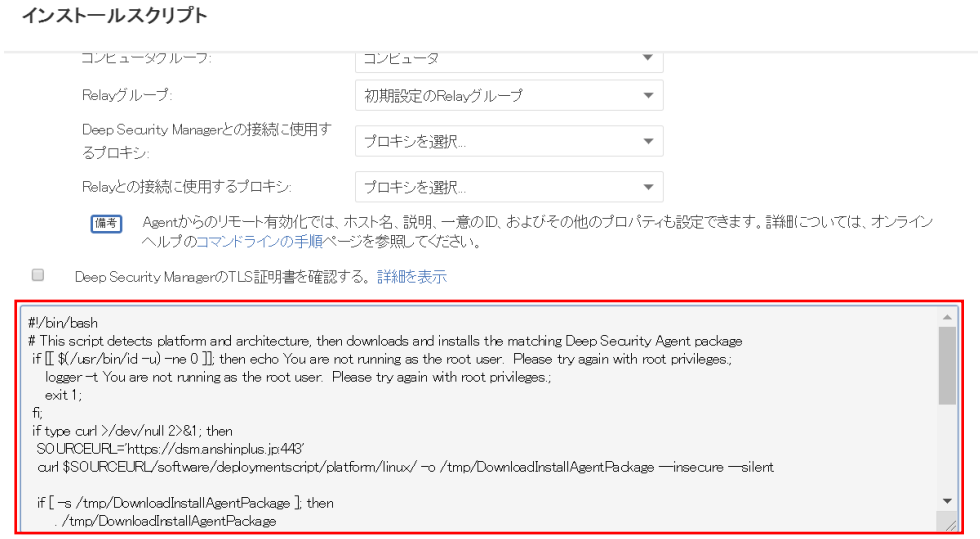
(3)インストールスクリプトの保存

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。



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 version 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

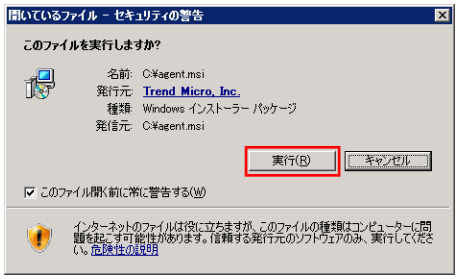
エージェントインストールプログラムをダウンロードします。ファイル名：agent.msi

【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

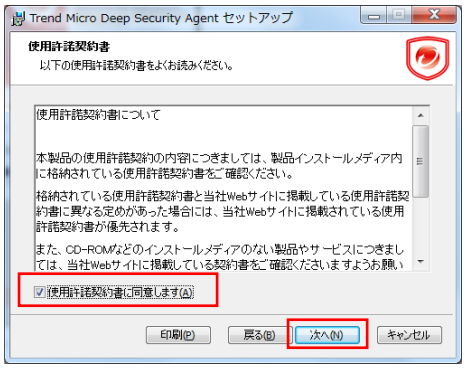
agent.msi を実行します。セキュリティの警告が表示された場合は「実行」をクリックしてください。



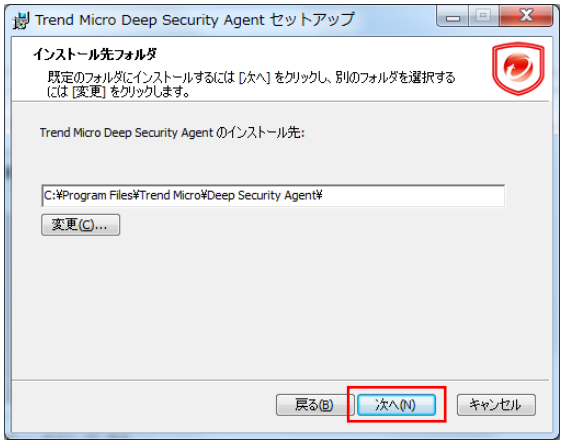
(3)インストールウイザード

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。



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。



「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。

「完了」をクリックします。

(4)エージェント有効化の準備

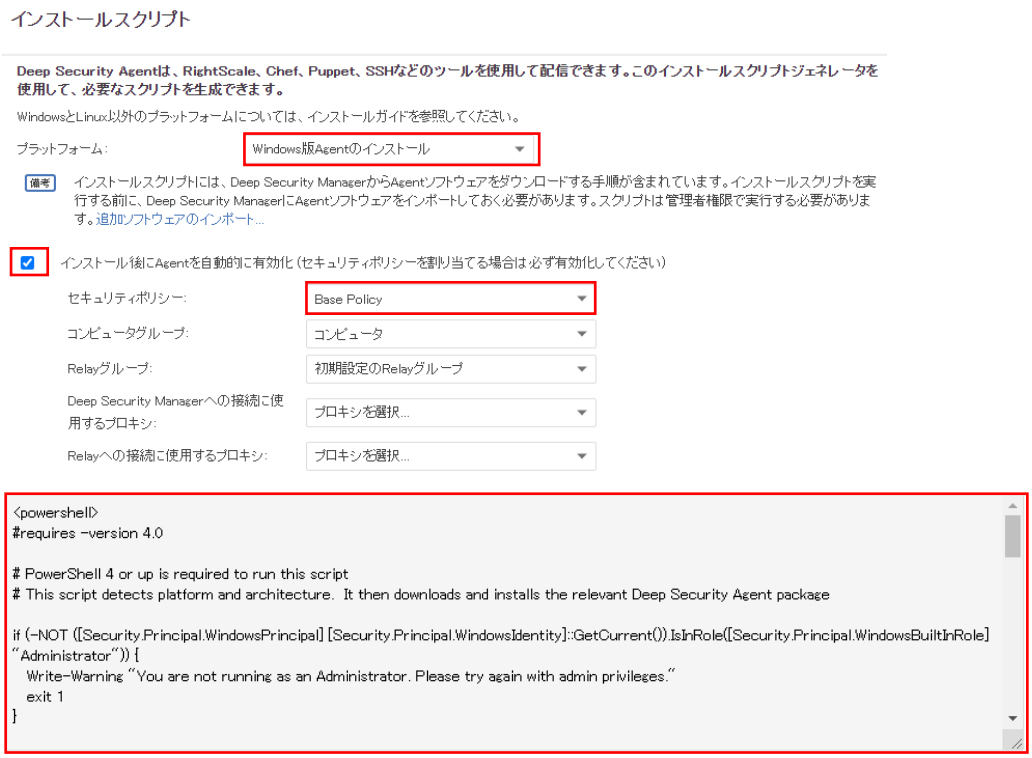
インストールスクリプトの一部コマンドを実行するため管理 Web コンソールよりインストールスクリプト作成画面を開きます。

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。



(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ダに移動します。

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...
～～　中略　～～
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　]

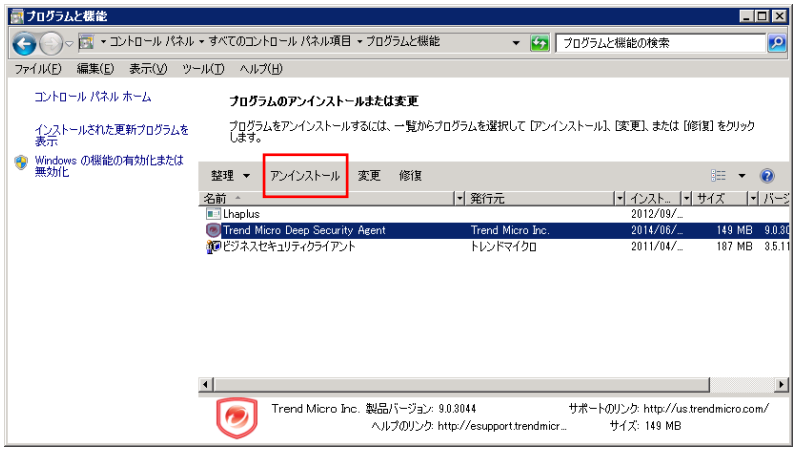
Unloading dsa_filter module... [　OK　]

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。

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

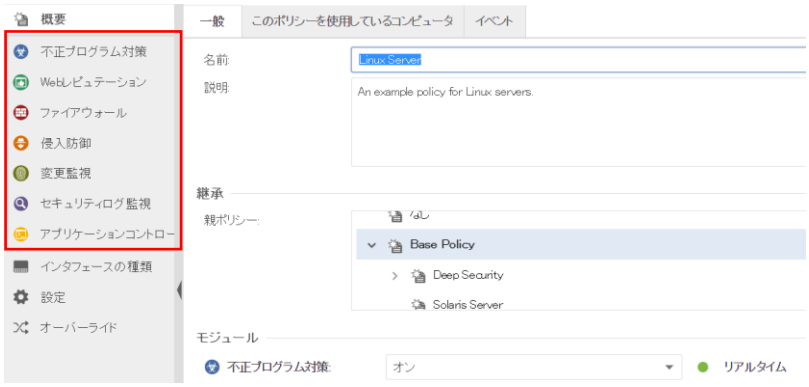
ポリシーでは、ルールや設定をまとめて保存し、複数のサーバに簡単に割り当てることができます。
例えば、侵入防御（仮想パッチ）の設定を複数サーバに割り当てる場合や、Linux サーバ用、Windows サーバ用のポリシーを作成しておき、サーバを追加した時にポリシーを選ぶだけというような運用ができます。
ポリシーをサーバに割り当てても個々に修正（オーバーライド）することができます。

※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



(3)コンピューター一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。

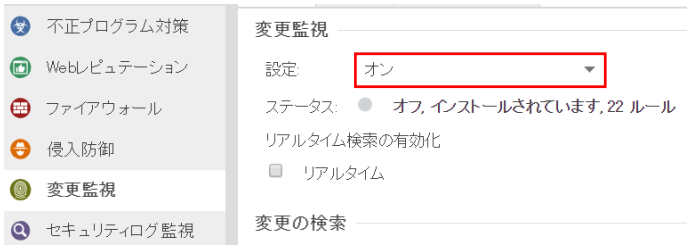
(4)サーバに適切なポリシーを割り当てます。

■サーバ設定画面

(5)個別設定例

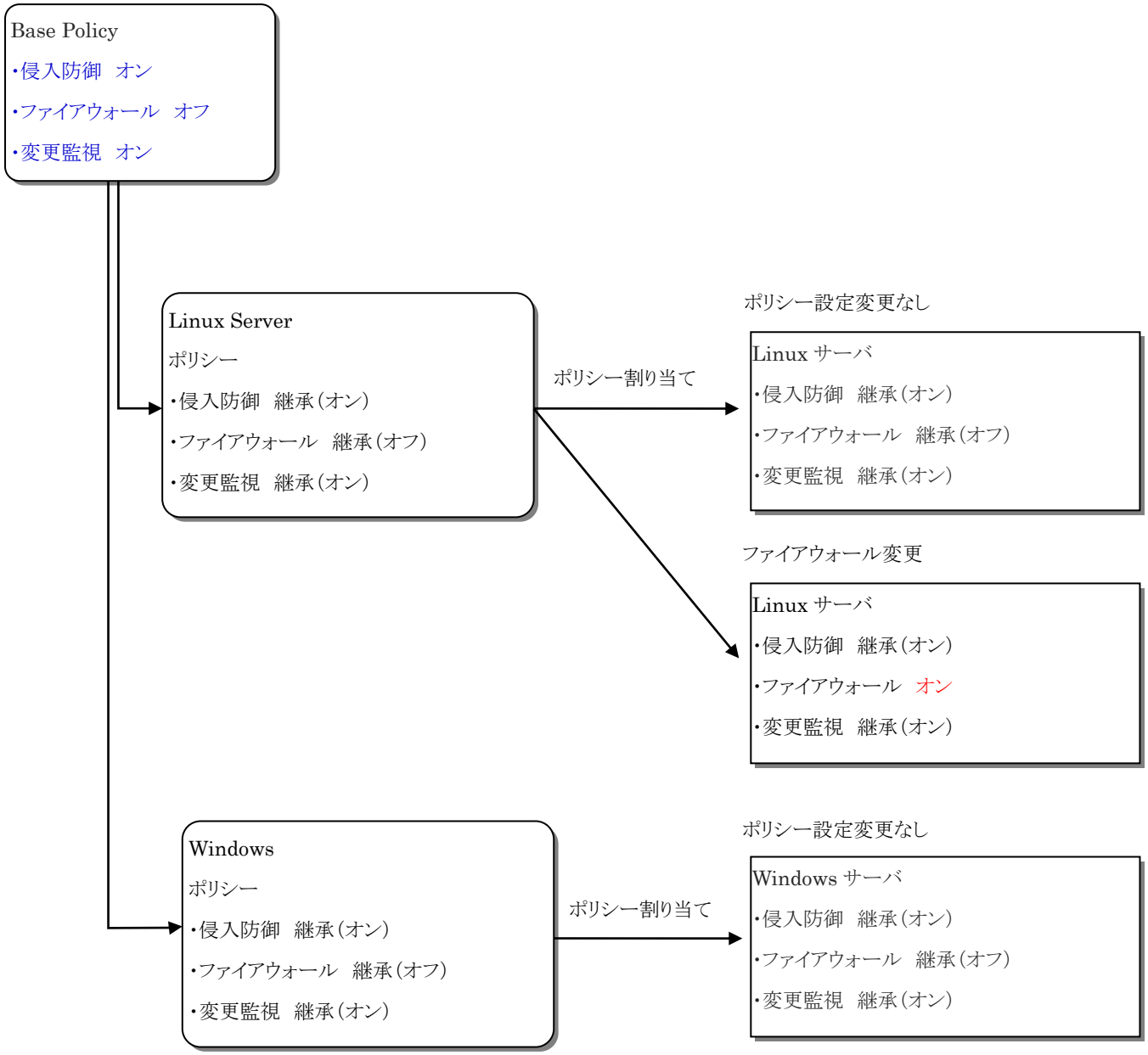
割り当てたポリシー「Linux server」では変更監視が継承(オフ)になっているとします。

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変更監視が有効になります。



※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。

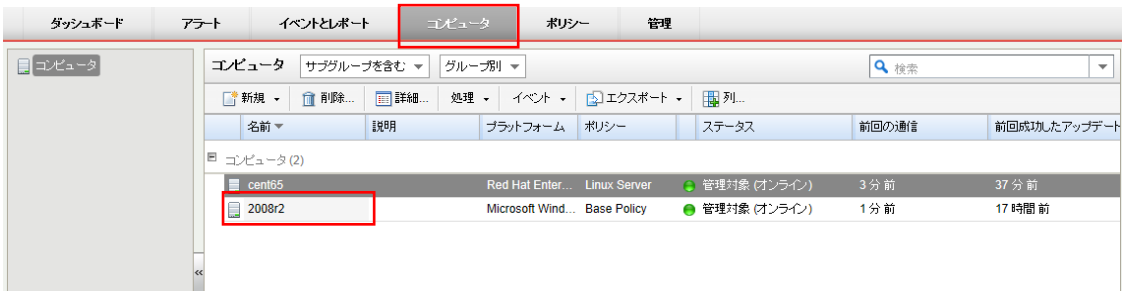
4. ウイルス対策『不正プログラム対策』

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

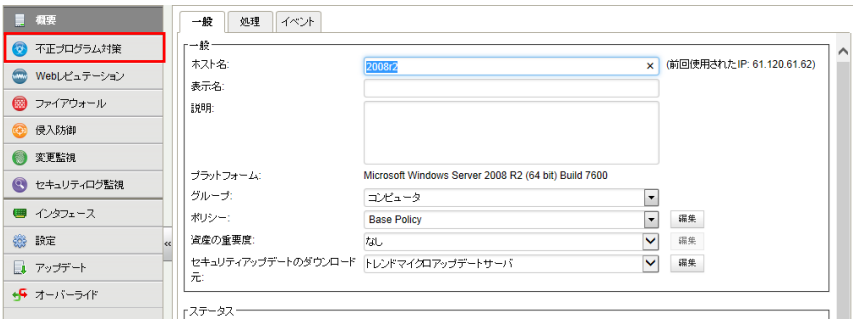
(1) 管理 Web コンソールにログオンしてください。

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。



(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。



(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。

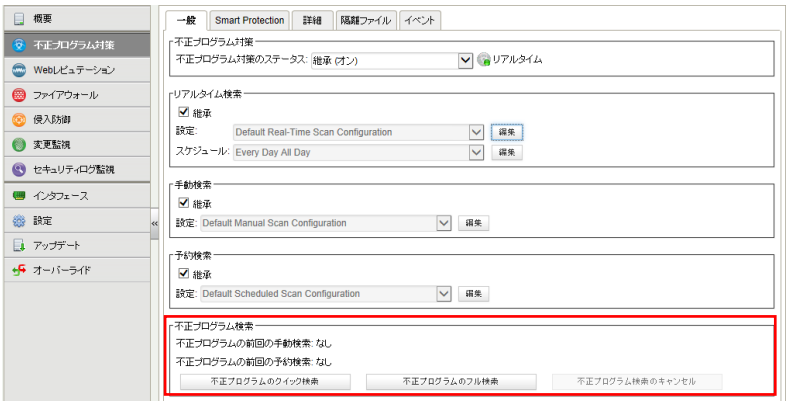
4.2. 不正プログラム対策設定

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

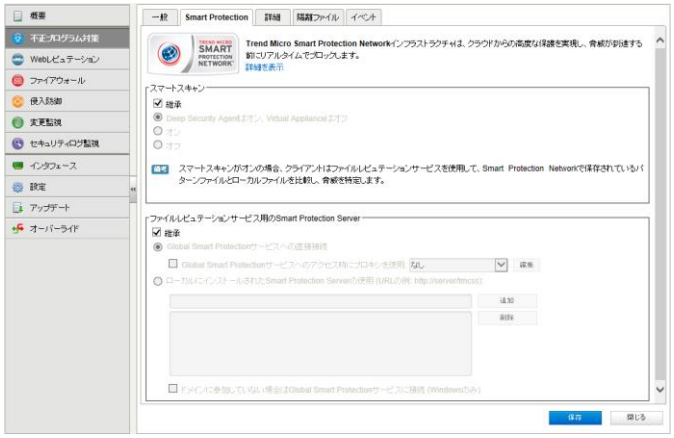
・パターンのアップデート時に使用されるネットワーク帯域幅を削減。パターン定義のアップデートの大半は、クラウドで保持され、多数のエンドポイントへの配信は不要

・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」

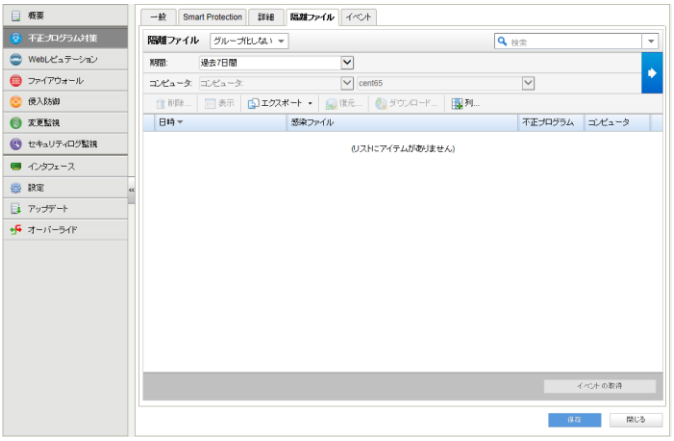
隔離ファイルの保存に使用される最大ディスク容量、検索するファイルの最大サイズなどが設定できます。

通常は初期値のままで問題ありません。

(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。

(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。

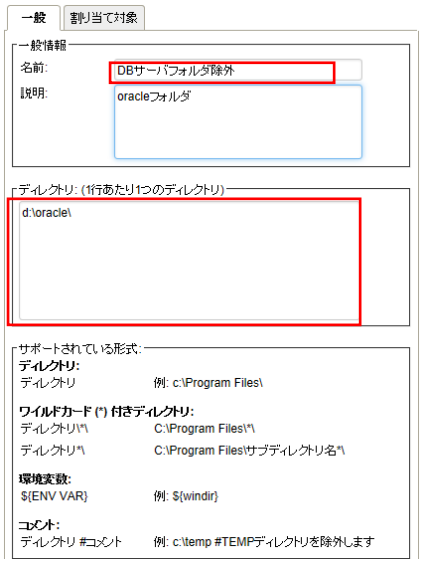
※一度作成したリストは保存され以後、選択できるようになります。

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)

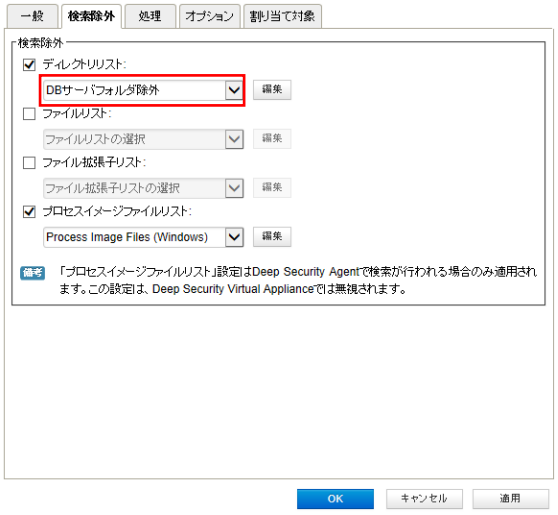
例) d:¥oracle　フォルダを除外する場合　d:¥oracle¥

決定は「OK」をクリックしてください。



ディレクトリリストに作成したリストが表示されます。

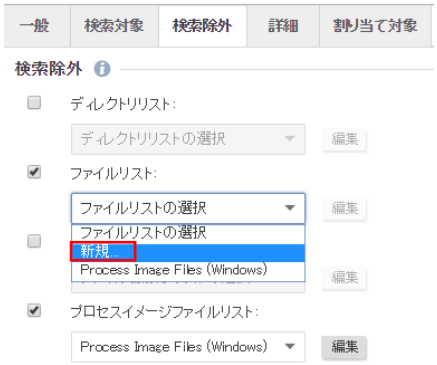
「OK」をクリックして完了します。



(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。

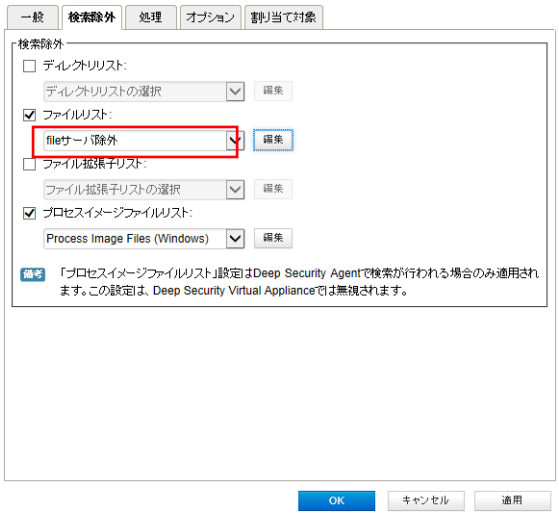
ファイル:ファイル名を入力します。(複数指定可)

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。

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。



(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。

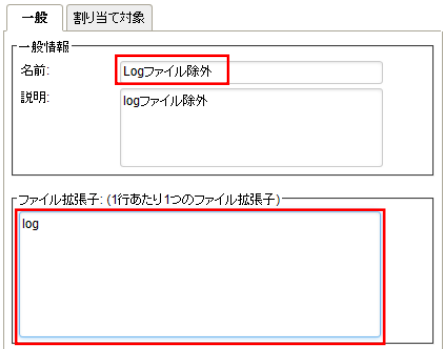
※一度作成したリストは保存され以後、選択できるようになります。

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。



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。

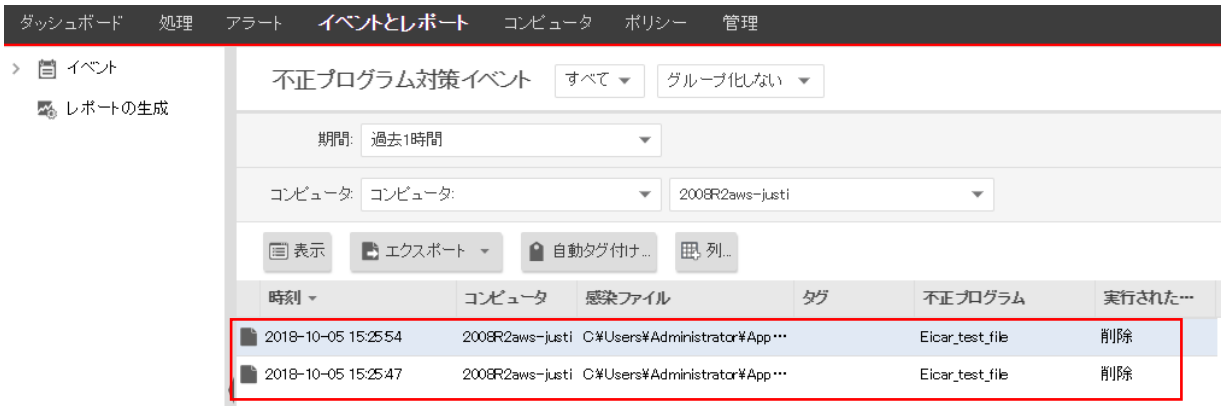
4.4. 予約検索

予約検索は予約タスクにて実行します。

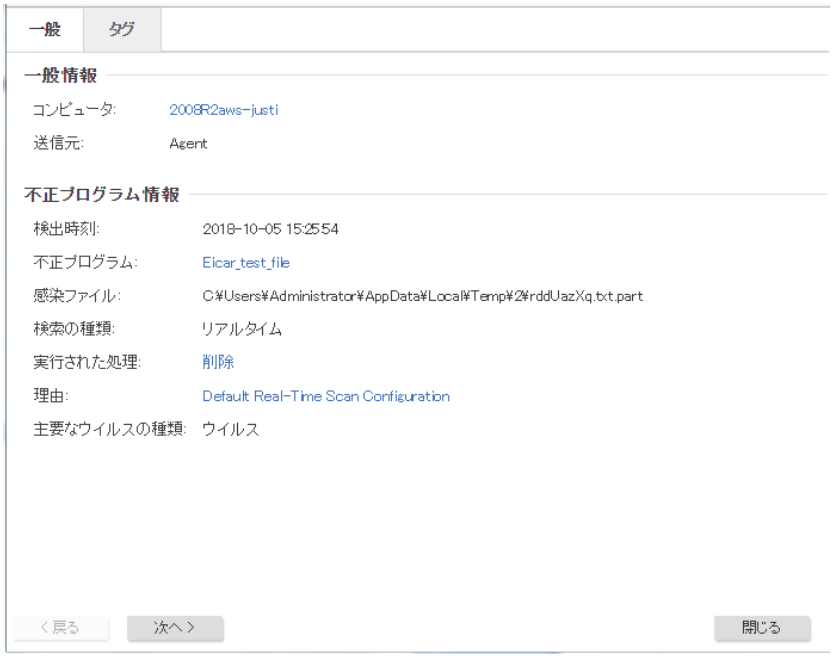
予約タスク(スケジュール設定)を参照してください。

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。



イベントをダブルクリックすると詳細が表示されます。



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」

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。

※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。

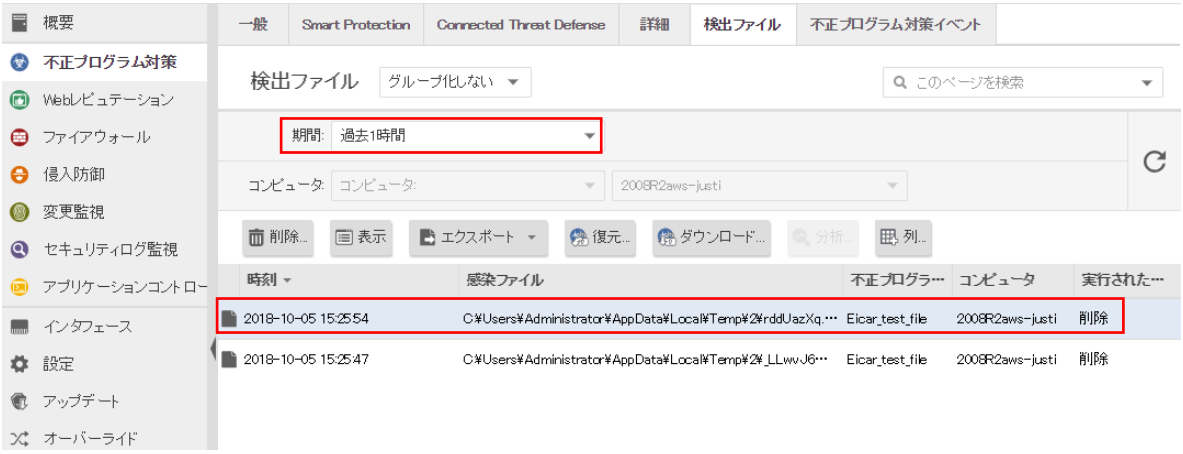
4.7. 隔離ファイルの復元方法

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。

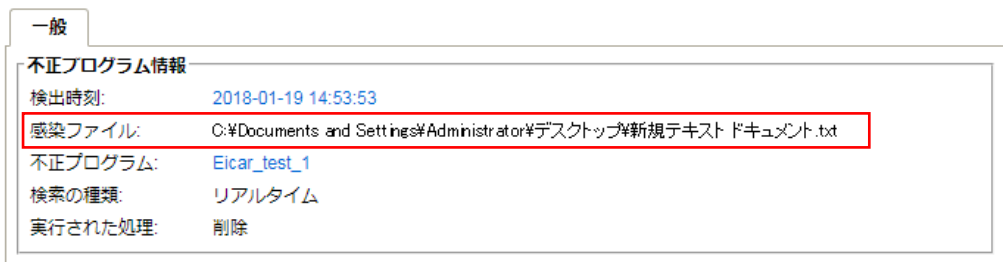
隔離ファイルを復元する前の準備

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。

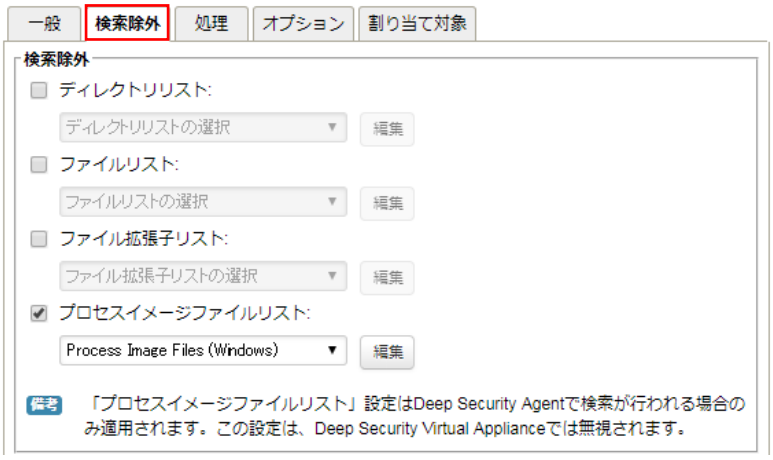


(2)「感染ファイル」でファイルが元々あった OS 上のファイル名とパスを確認しておきます。

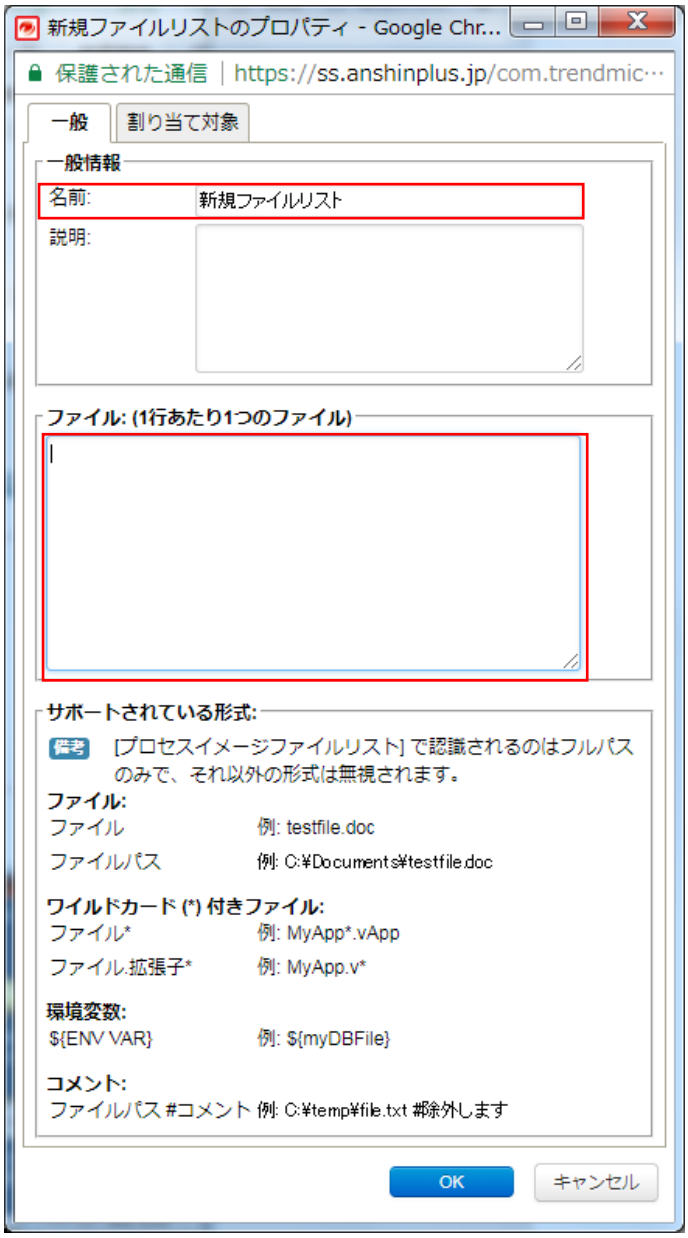


(3)引き続きコンピュータのエディタで、[不正プログラム対策]→[一般]タブに進み、それぞれの[不正プログラム検索設定]の［編集］ボタンをクリックし、不正プログラム検索設定のプロパティ画面を開きます。
※「リアルタイム検索」、「手動検索」、「予約検索」それぞれ必要に応じて検索設定を行います。

(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。



(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。



(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。

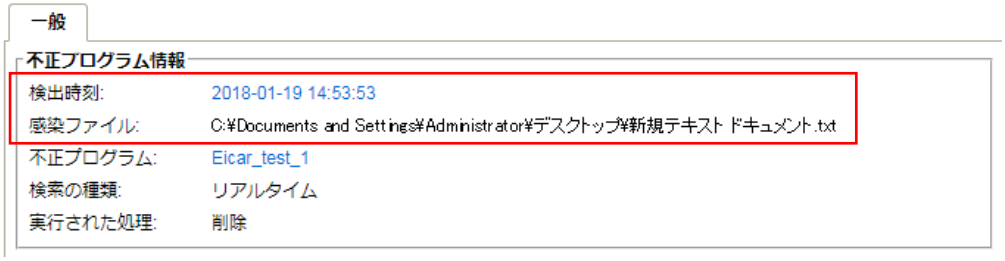
(8)コンピュータのエディタで、すべての[不正プログラム検索設定]の編集を終えたら、[保存] ボタンをクリックします。

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。

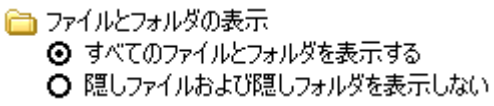


(2)復元ツールのダウンロード
ダウンロード URL
http://usersguide.anshinplus.jp/SS/QFAdminUtil.zip

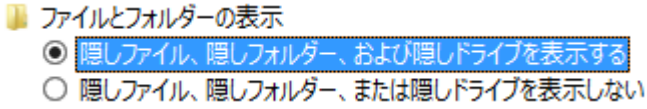
ダウンロードした QFAdminUtil.zip を解凍します。※3 つのファイルが展開されます。

★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



>WindowsXP、2003

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

または

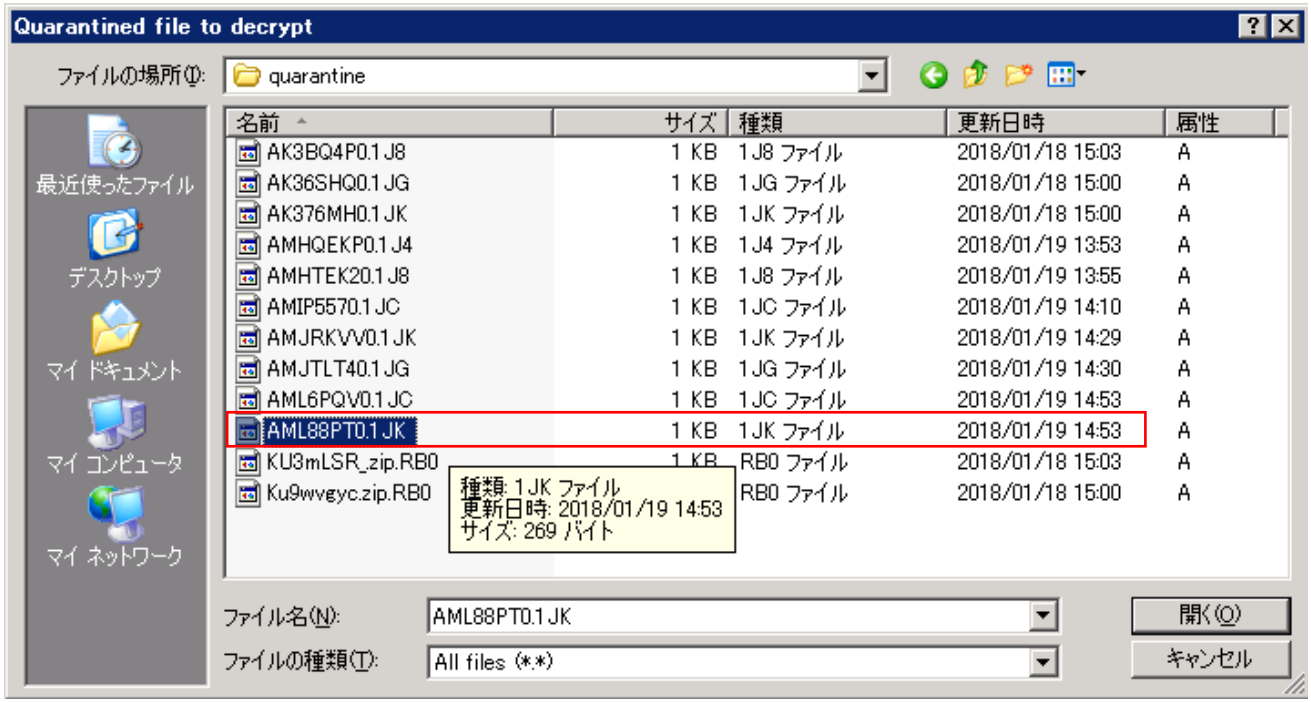
C:¥Documents and Settings¥All Users¥Application Data¥Trend Micro¥AMSP¥quarantine

>Windows Vista、2008 以降

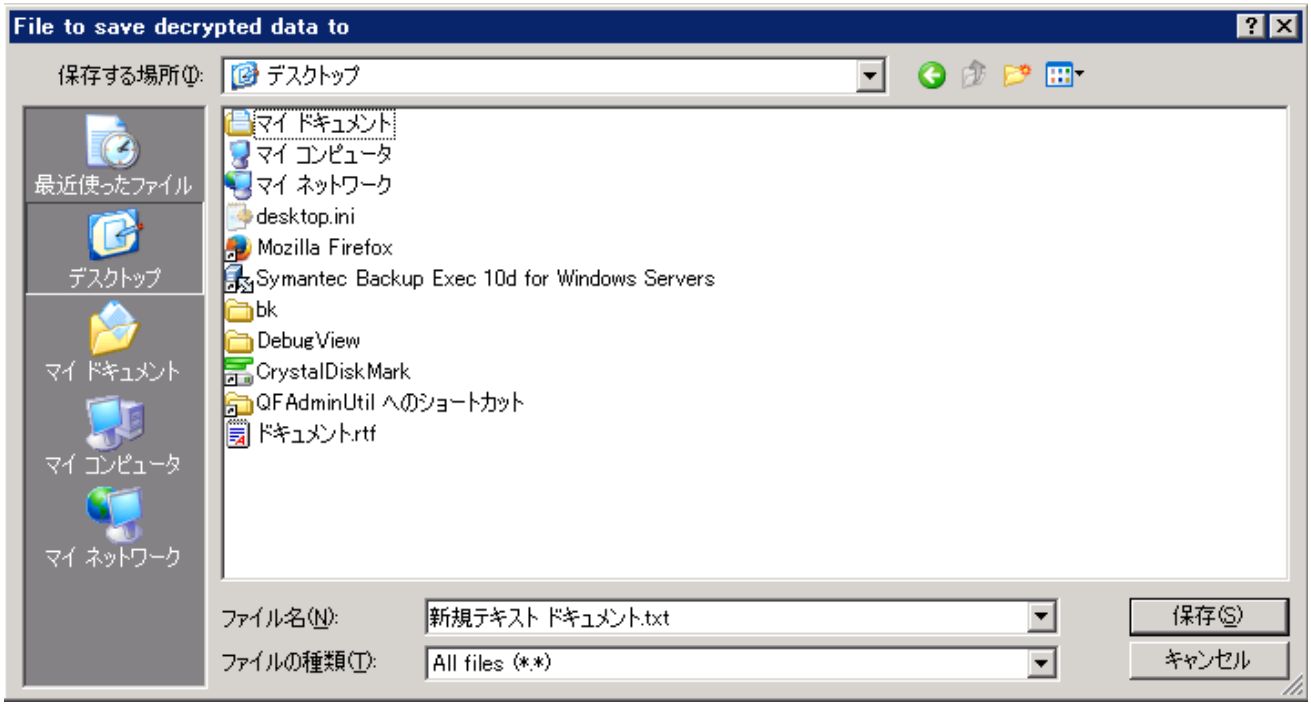
C:¥ProgramData¥Trend Micro¥AMSP¥quarantine

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。



復元するファイルの保存先を指定して[保存]を押します。



「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。

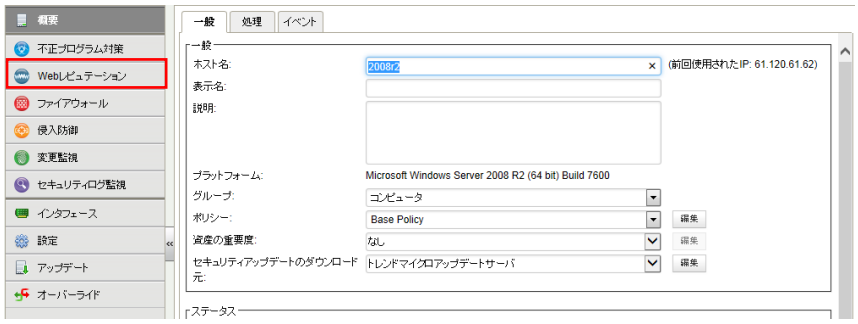
5.1. Web レピュテーションの有効化

(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。

(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。



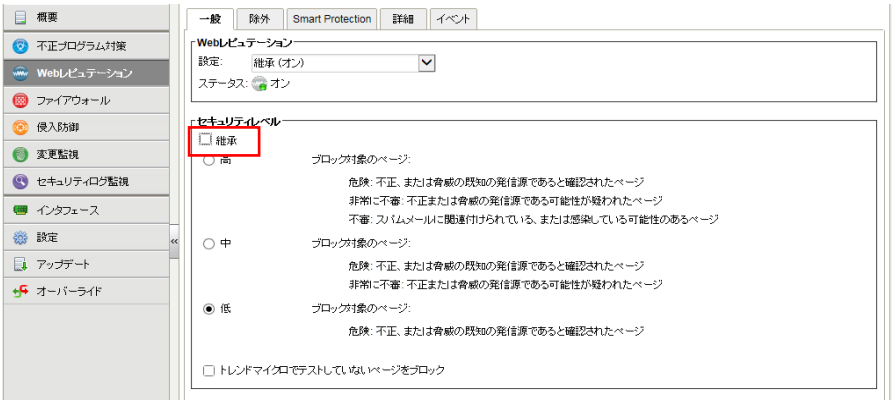
(3) Web レピュテーションのステータスを「オン」にして「保存」をクリックしてください。

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

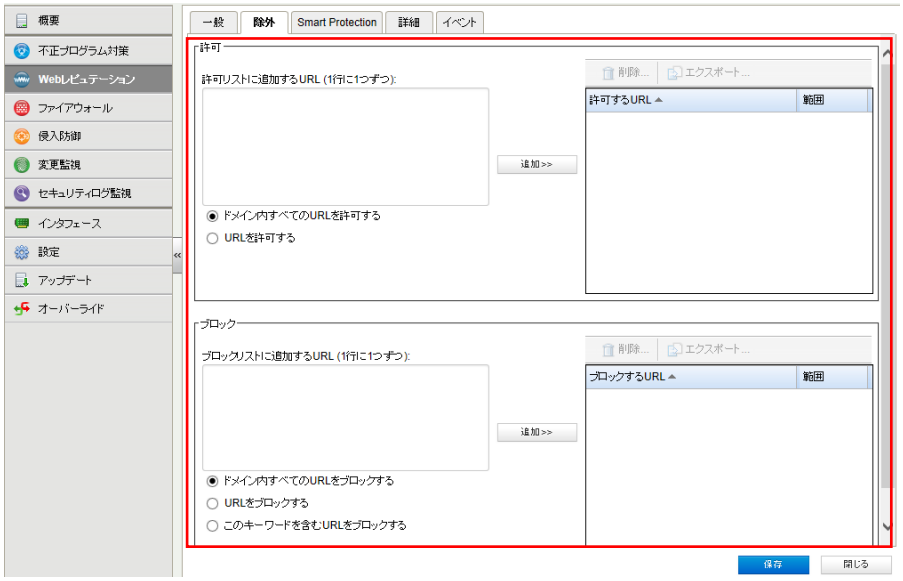
トレンドマイクロでテストしていないページをブロック ： 次のリスクレベルのページをブロックします。
・トレンドマイクロで規定していないレベル

(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。

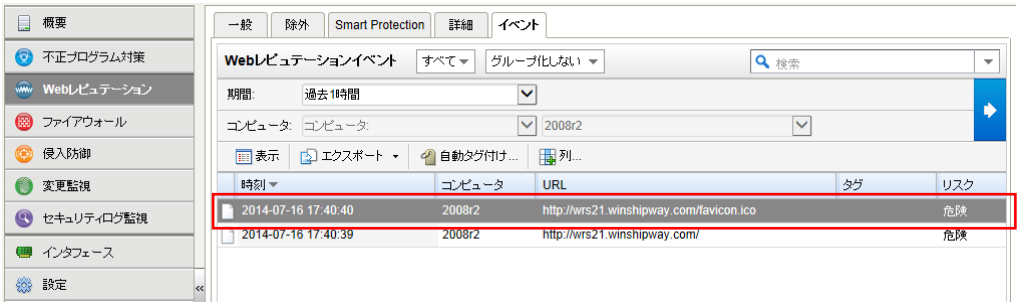
[ブロック] リストに含まれているURL、およびこのリストで指定したキーワードを含むURLは、常にブロックされます。ただし、[許可] リストに優先エントリが存在する場合は除きます。一度に複数のURLまたはキーワードを追加できますが、その場合は改行で区切る必要があります。URLをブロックする場合は、ドメイン内のすべてのURLをブロックするのか、特定のURLをブロックするのか、それとも特定のキーワードを含むURLをブロックするのかを選択します。

決定は「保存」をクリックしてください。



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。



イベントをダブルクリックすると詳細が表示されます。

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。

■「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。

※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

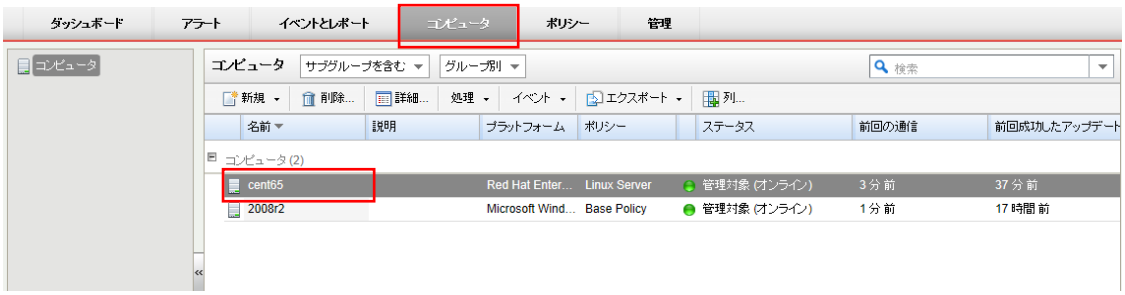
6. 不正な通信を防御『ファイアウォール』

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

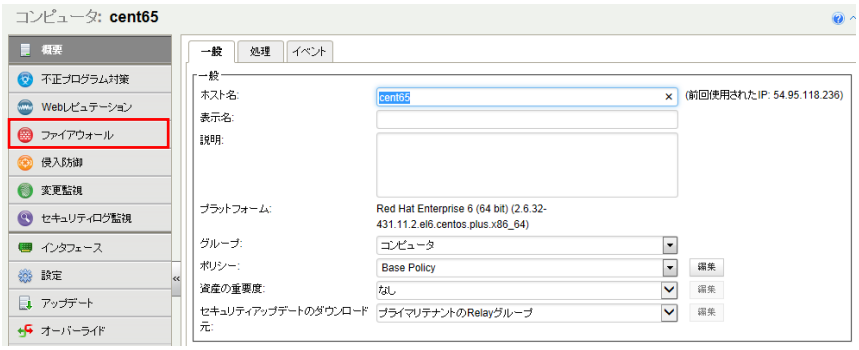
(1) 管理 Web コンソールにログオンしてください。

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。



(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。



(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。

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
・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

⑪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。

⑫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。

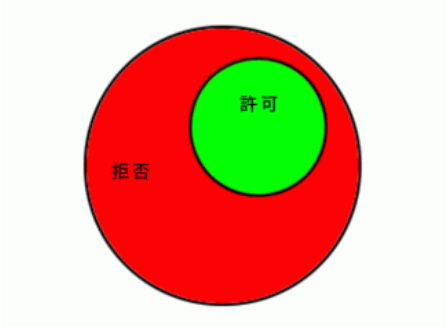
2.ログのみ: パケットがログのみルールに一致した場合は、通過してイベントがログ記録されます。

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。

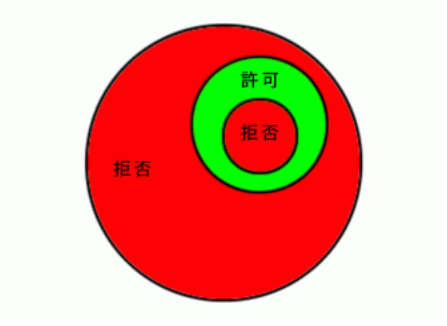
4.拒否: パケットが拒否ルールに一致した場合は、破棄されます。

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。

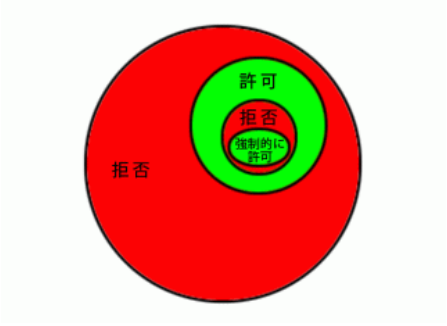
■許可ルールを実装すると、許可ルールに一致しないその他すべてのトラフィックが拒否されます。



■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。



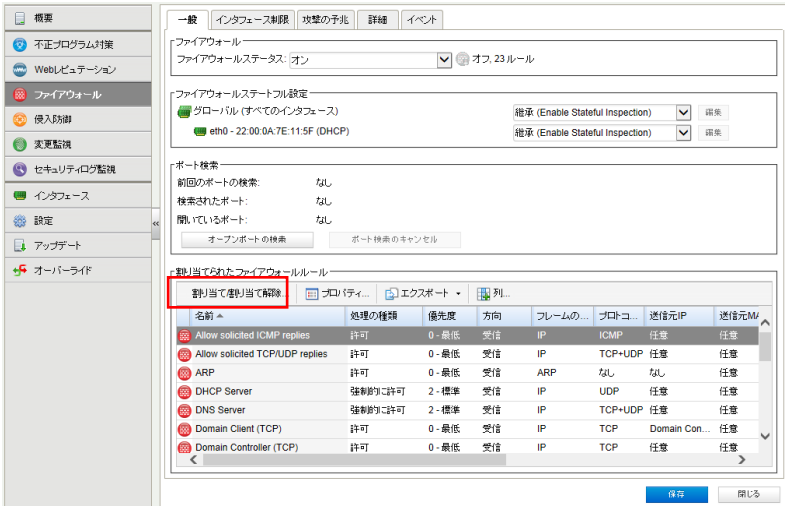
■強制的に許可ルールを拒否トラフィックに適用すると、例外のみ通過させることができます。



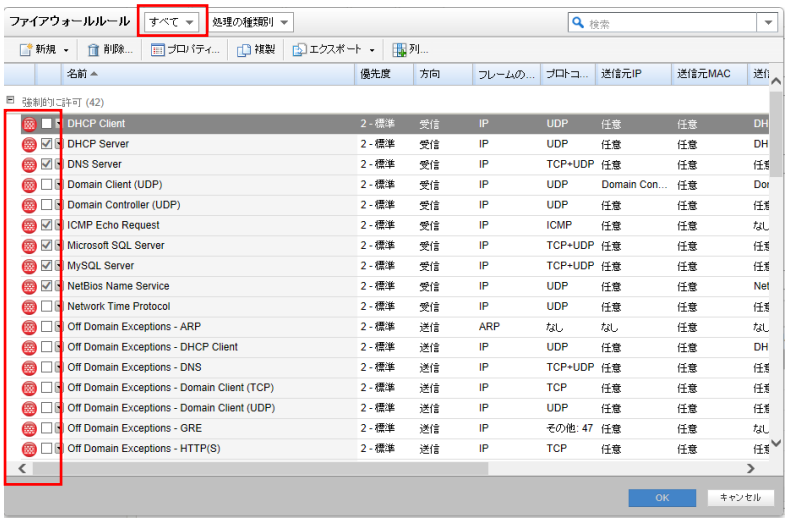
6.3. ファイアウォールルール設定

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。



(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。



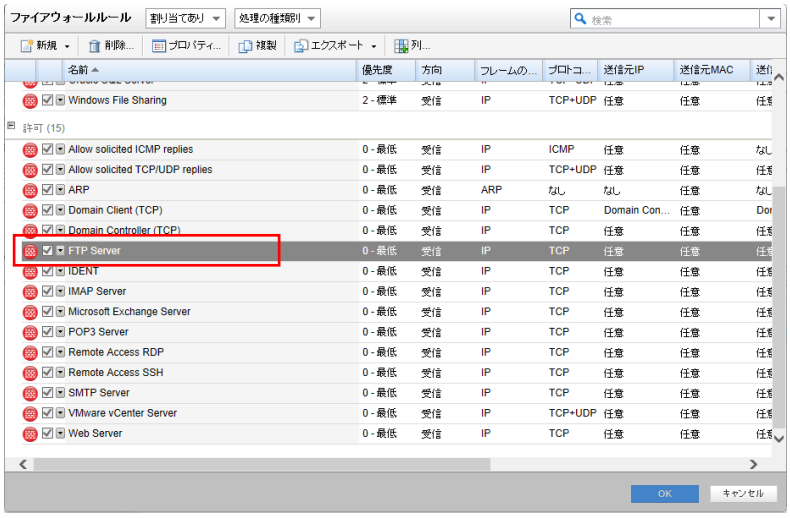
(3)ファイアウォールルールの変更

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

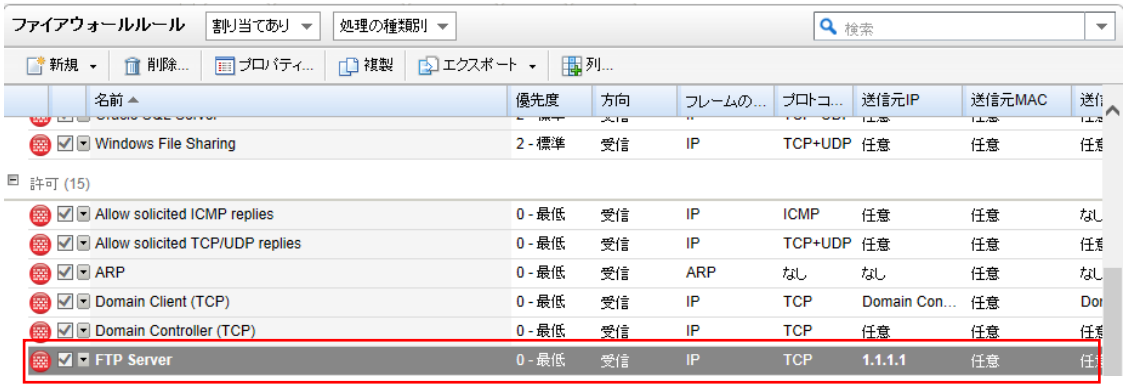


「ファイアウォールルールプロパティタブ」

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。

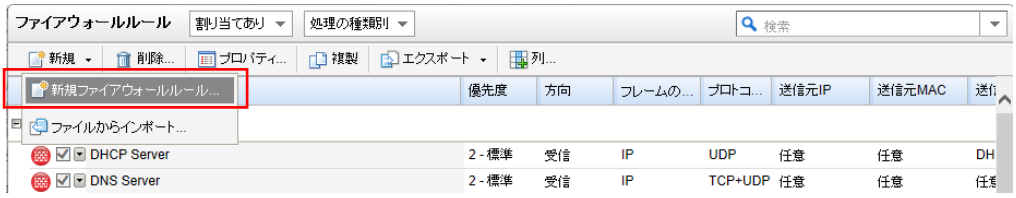
FTP Server ルールの送信元 IP アドレスが「任意」」から 1.1.1.1 へ変更されました。



(4)ファイアウォールルールの作成

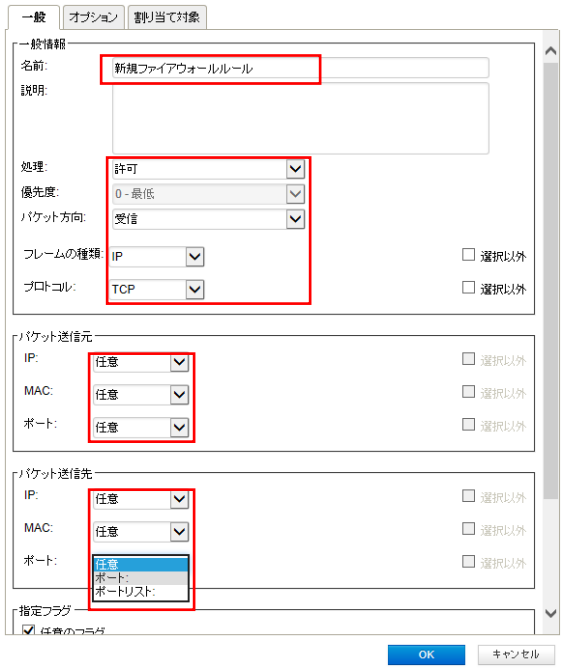
既定のルールがない場合は、独自にルールを作成できます。

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。



「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。



(5)ファイアウォールルールの確認／変更

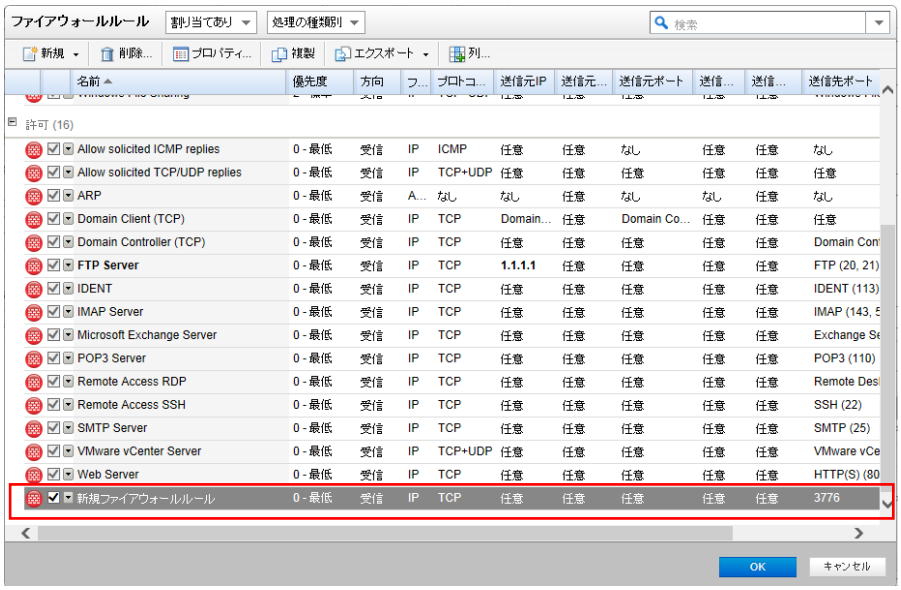
新しく作成したルールにチェックがついていれば割り当てされ有効になっています。

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。



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

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。

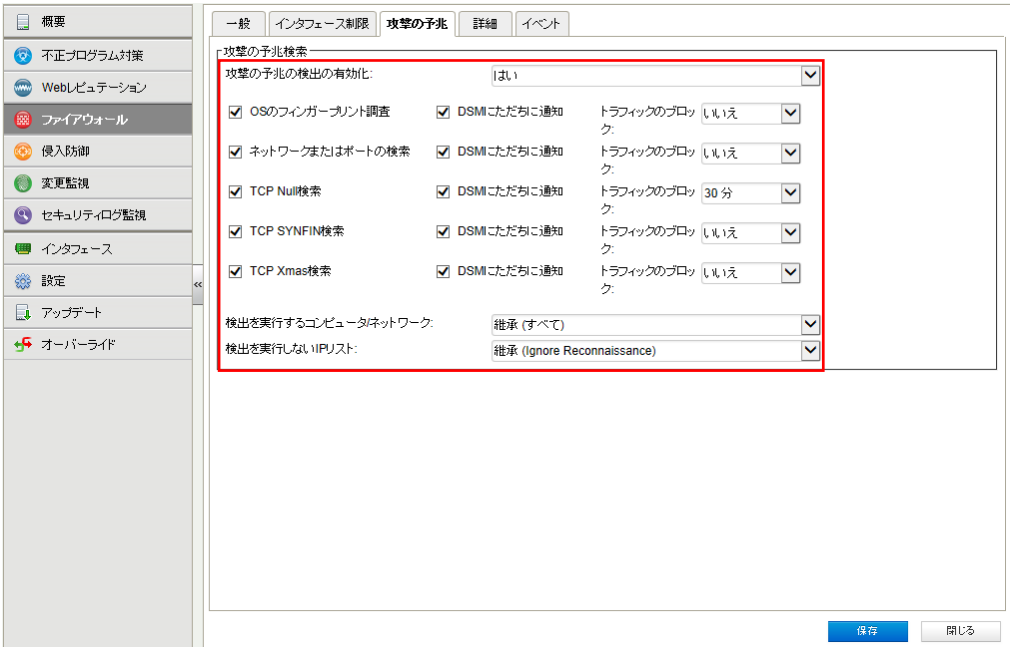
・攻撃の予兆の検出の有効化: 攻撃の予兆の検出のオン/オフを切り替えできます。

・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」



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。

イベントをダブルクリックすると詳細が表示されます。

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」

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。

※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。

(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。

(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。

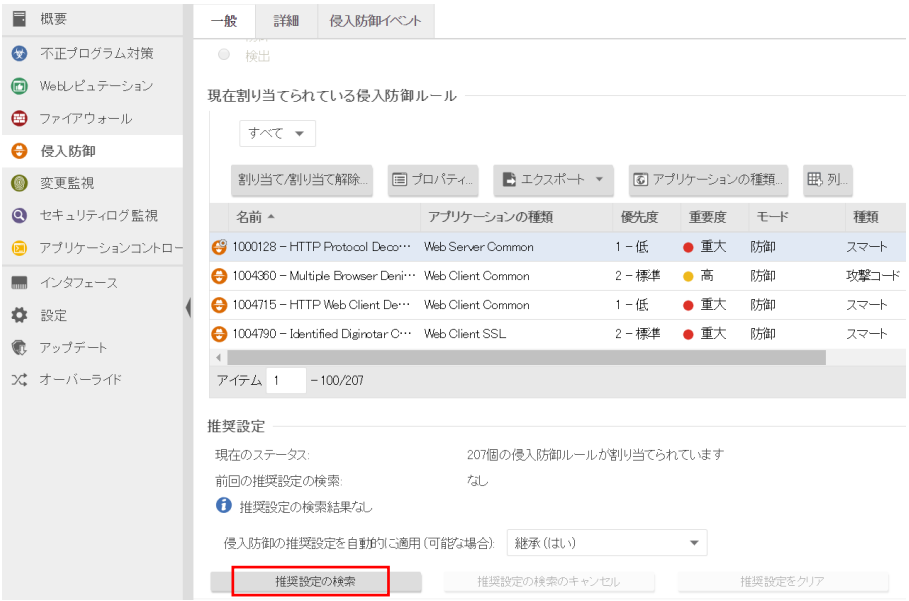
これで侵入防御が有効になります。 継承（オン）になっている場合は既に有効になっています。

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。

(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。)



(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。

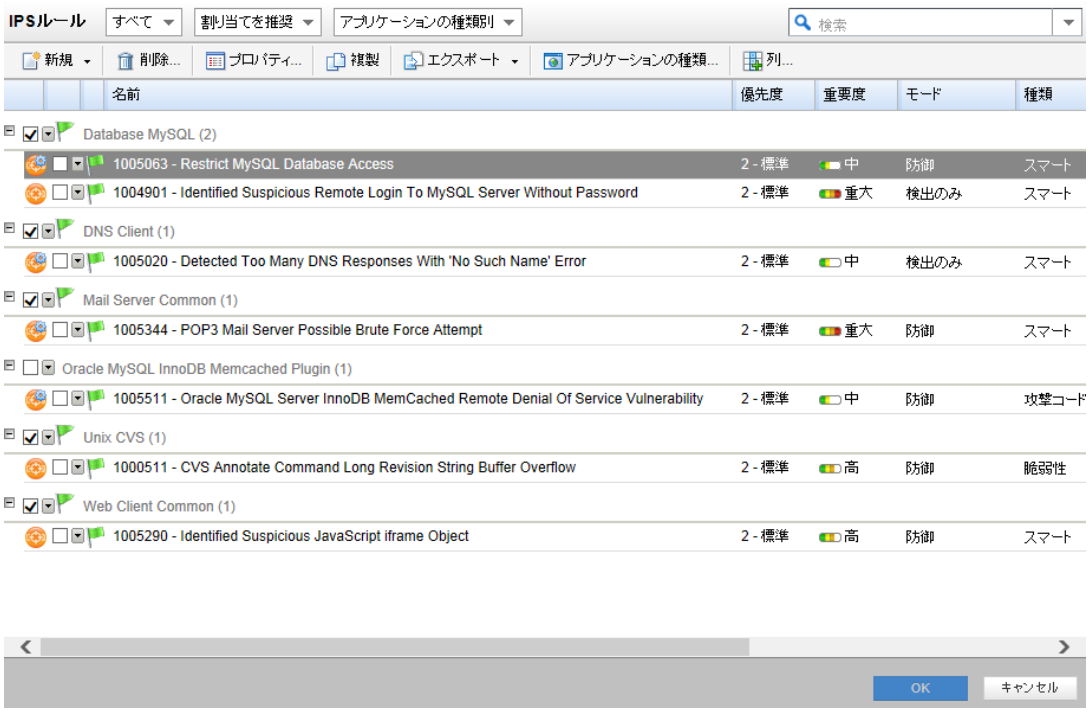
(4)未解決の推奨設定

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。

(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。

・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。



7.3. 侵入防御（カスタム設定）

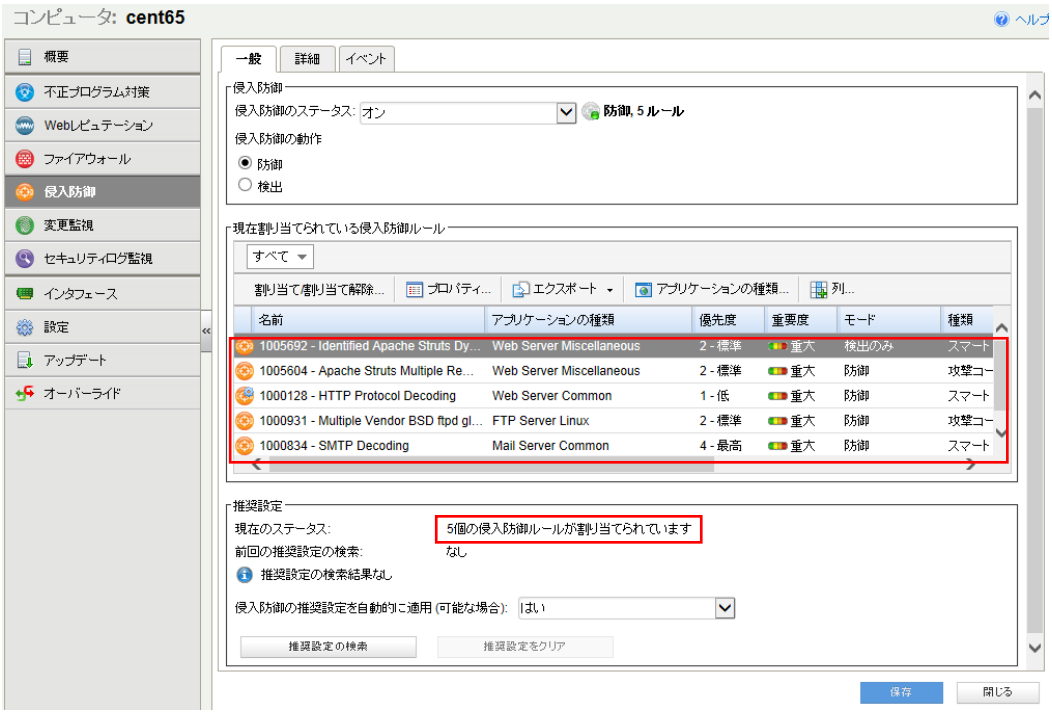
侵入防御ルールの割り当てを手動で行う方法です。推奨設定とカスタム設定を合わせて使うこともできます。
※全てのルールから必要な侵入防御ルールを設定、メンテナンスすることは非常に困難だと思われるため、推奨設定（自動）による運用をおすすめします。

(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。

(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。

例では 5 個の侵入防御ルールが割り当てられています。



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。

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。

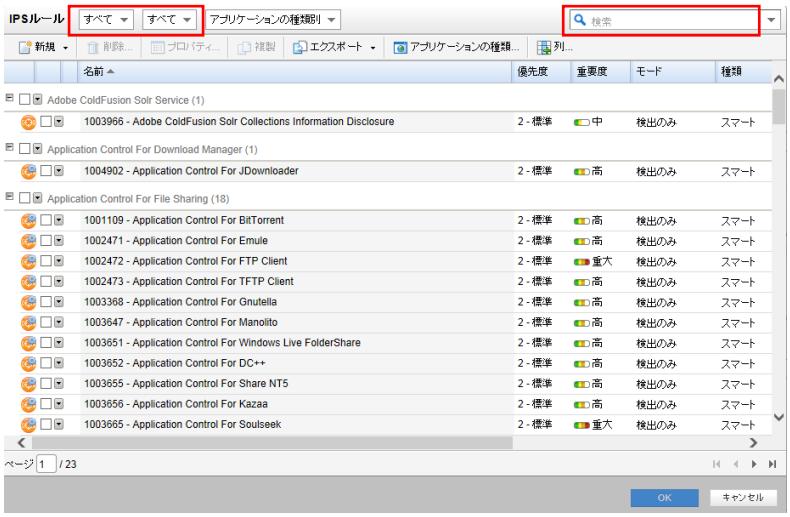
(2)キーワード検索

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)

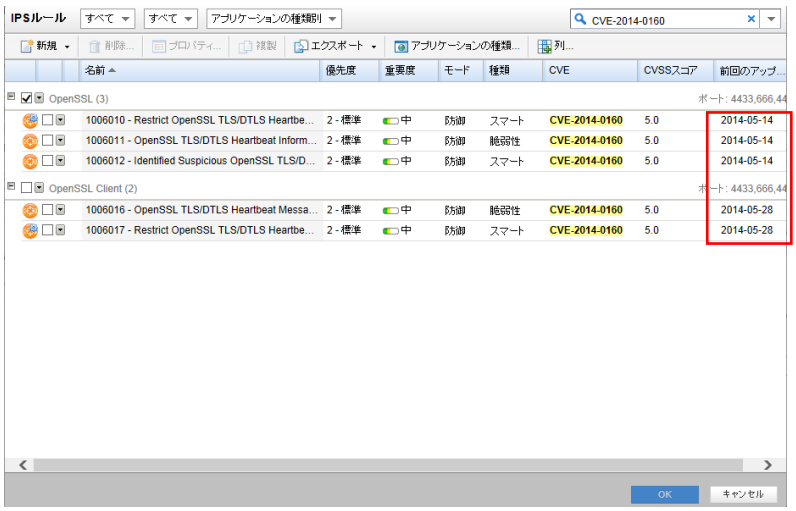
表示フィルタは「すべて」を選択し、検索キーワードを入力しエンターキーを押してください。

CVE-2014-0160 を検索してみます。



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。



(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

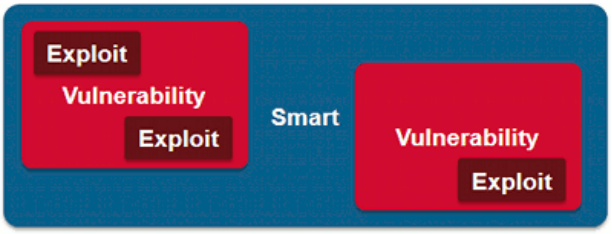
特定の脆弱性を攻撃する〝特定の攻撃〟を検知するためのルール

・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

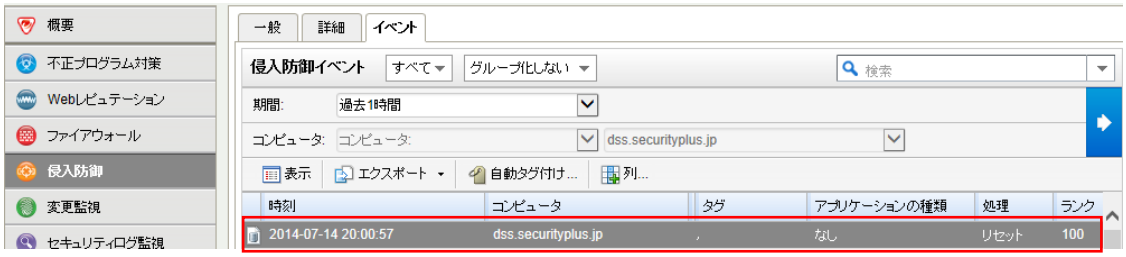
・スマート / Smart

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

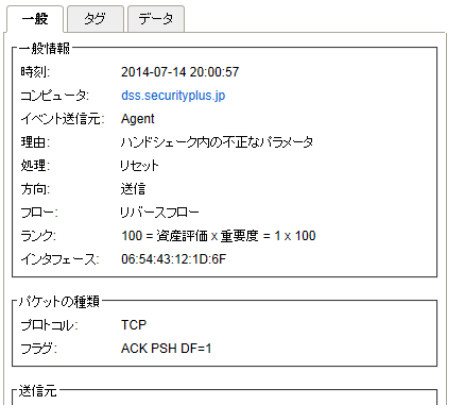


7.5. 侵入防御イベント

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。



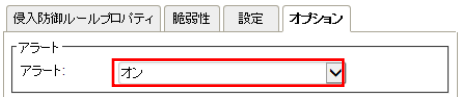
イベントをダブルクリックすると詳細が表示されます。



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」



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。

※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。

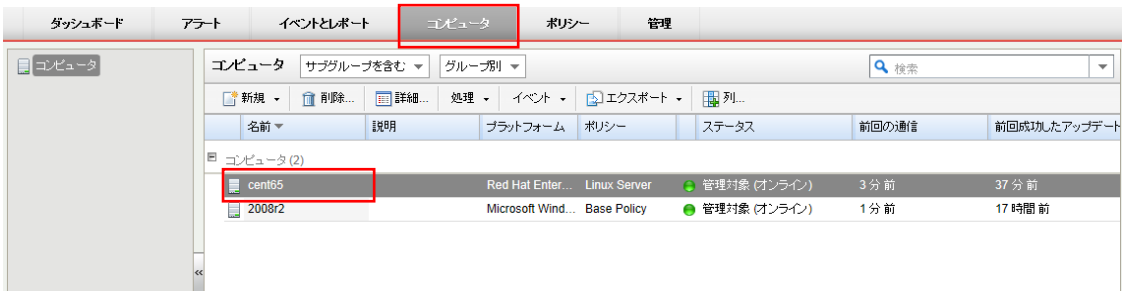
8. 改ざん検知『変更監視』

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

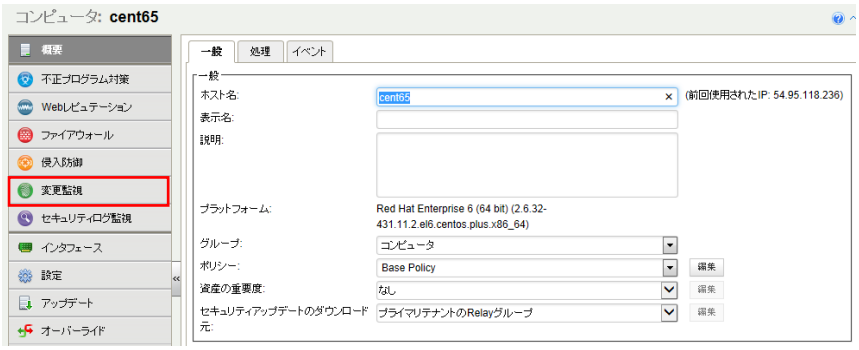
(1) 管理 Web コンソールにログオンしてください。

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。



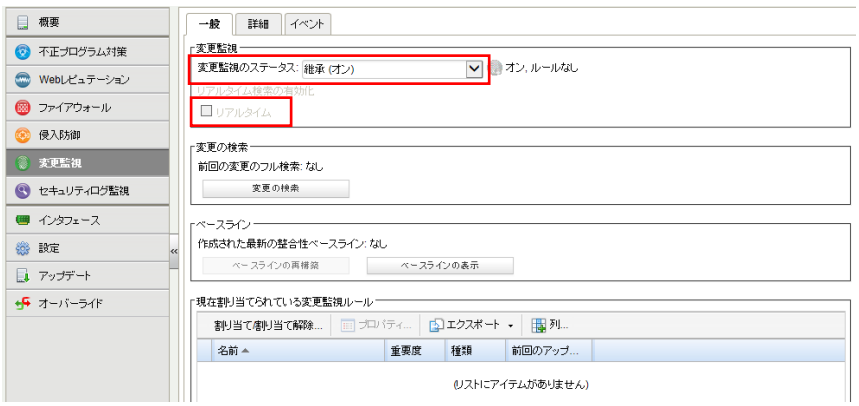
(2) サーバの設定画面が表示されます。

「変更監視」をクリックします。



(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。

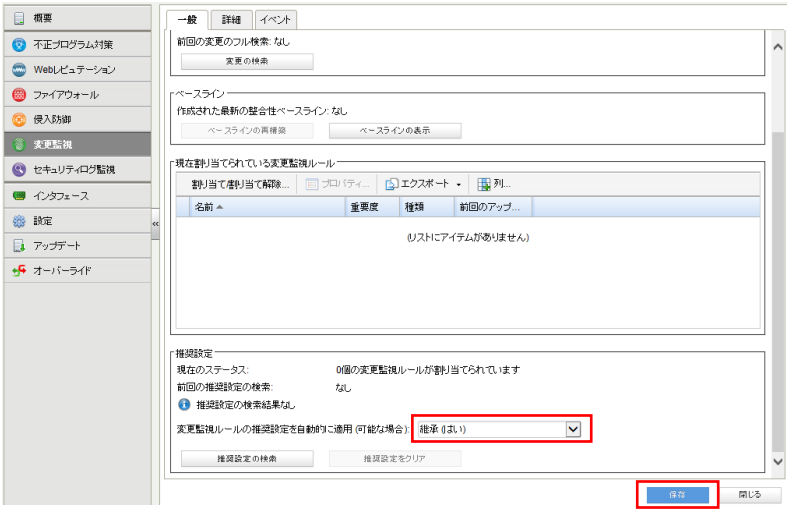
これで変更監視が有効になります。 継承（オン）になっている場合は既に有効になっています。



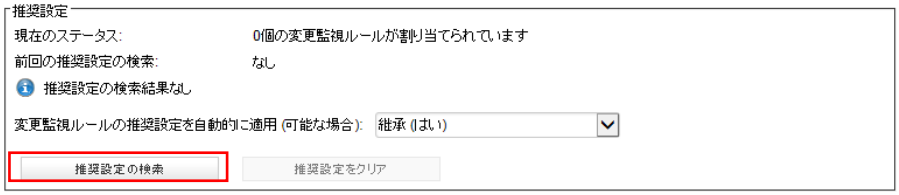
8.2. 変更監視(推奨設定)

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。

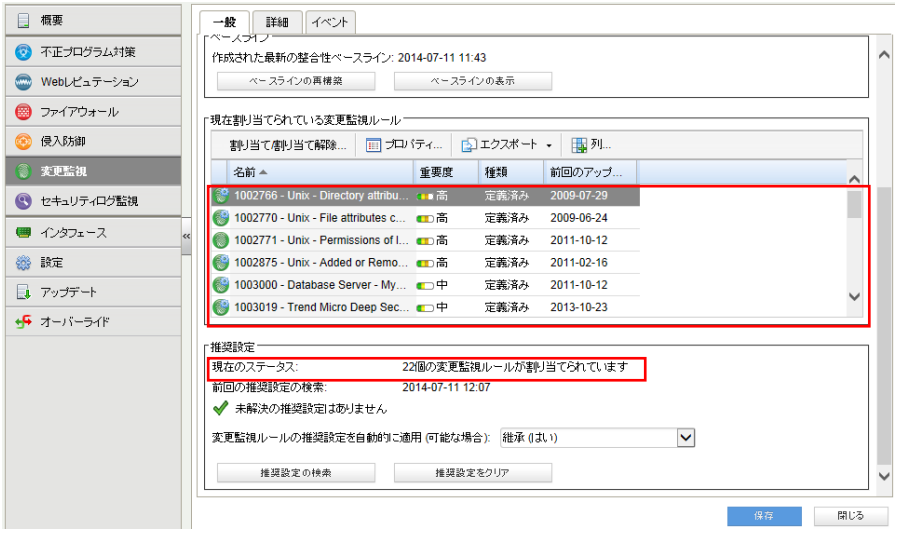
(1)変更監視ルールの推奨設定を自動的に適用(可能な場合):を「はい」にします。
「保存」をクリックして設定を保存します。継承(はい)になっている場合は既に有効になっています。



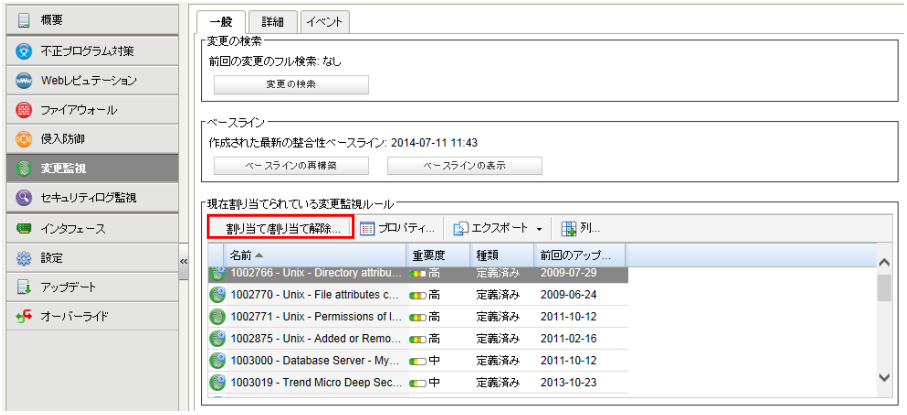
(2)推奨設定の検索
「推奨設定の検索」をクリックするとサーバに指示が出され検索を実行します。
検索が終了するまで数分から数十分かかります。
※推奨設定の検索は「予約タスク」機能によって定期的に自動で行うことができます。新しいアプリケーションが追加された場合など、自動的にルールを追加するように日単位、週単位などのスケジュールを予約タスクで設定することもできます。



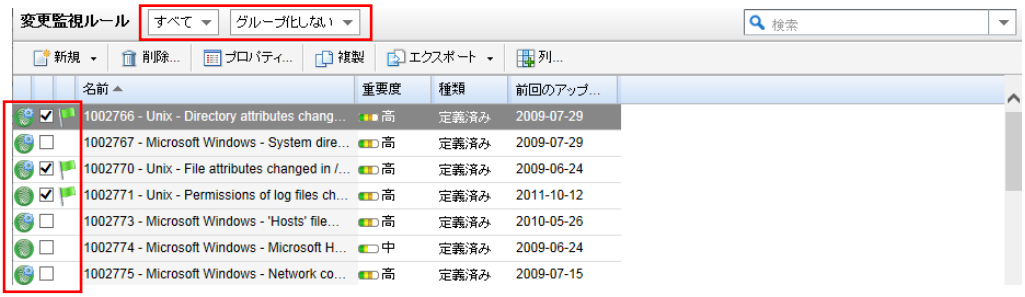
(3)推奨設定の検索が完了すると変更監視ルールがサーバに割り当てされます。
例では 22 個のルールが割り当てられています。



(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。



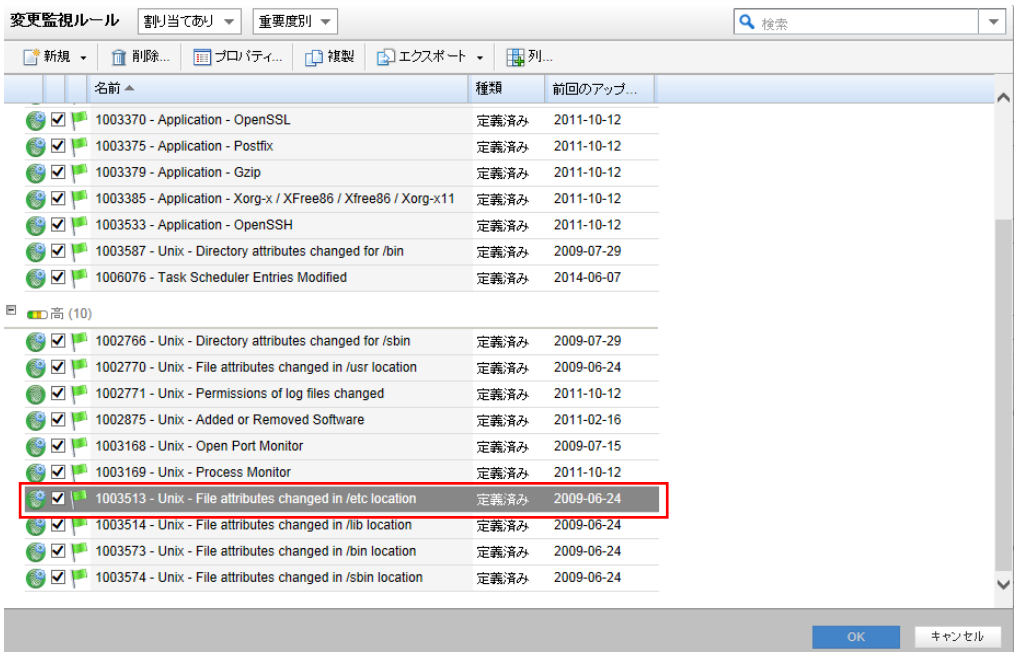
変更監視ルール一覧が表示されます。
表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。旗マークが推奨設定により検索されたルールで、アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックスのオン／オフでルールの割り当て／割り当て解除を行えます。決定は「OK」をクリックしてください。



(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。



(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。

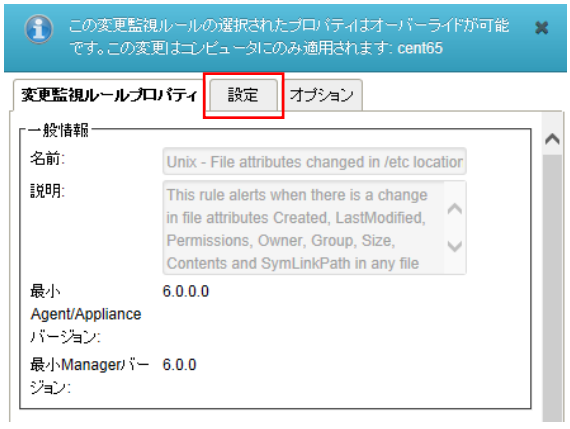
ルールをコンピュータに対して編集するには、ルールを右クリックして［プロパティ...］をクリックします。

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。

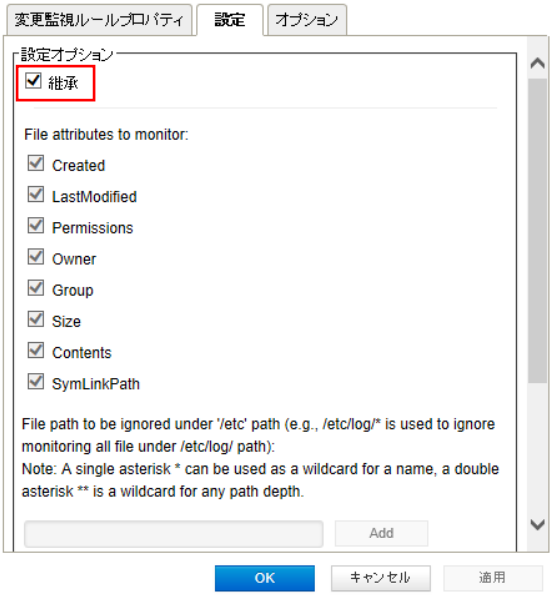
※グローバルに編集した場合は、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容が適用されます。

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。

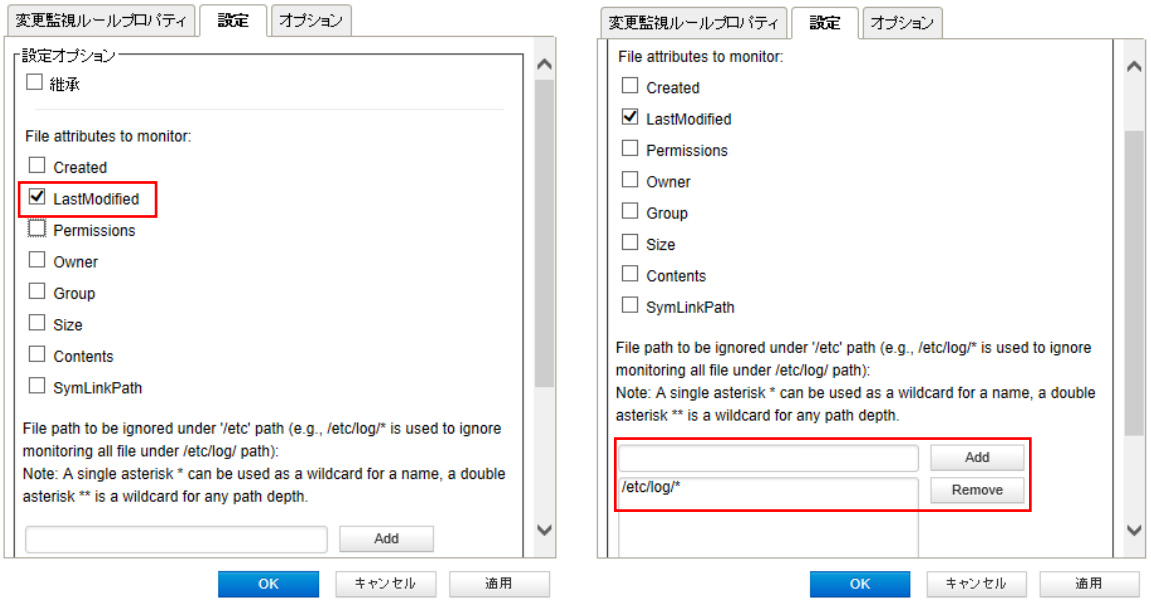


コンピュータに対して割り当てる場合は「継承」のチェックを外します。



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。



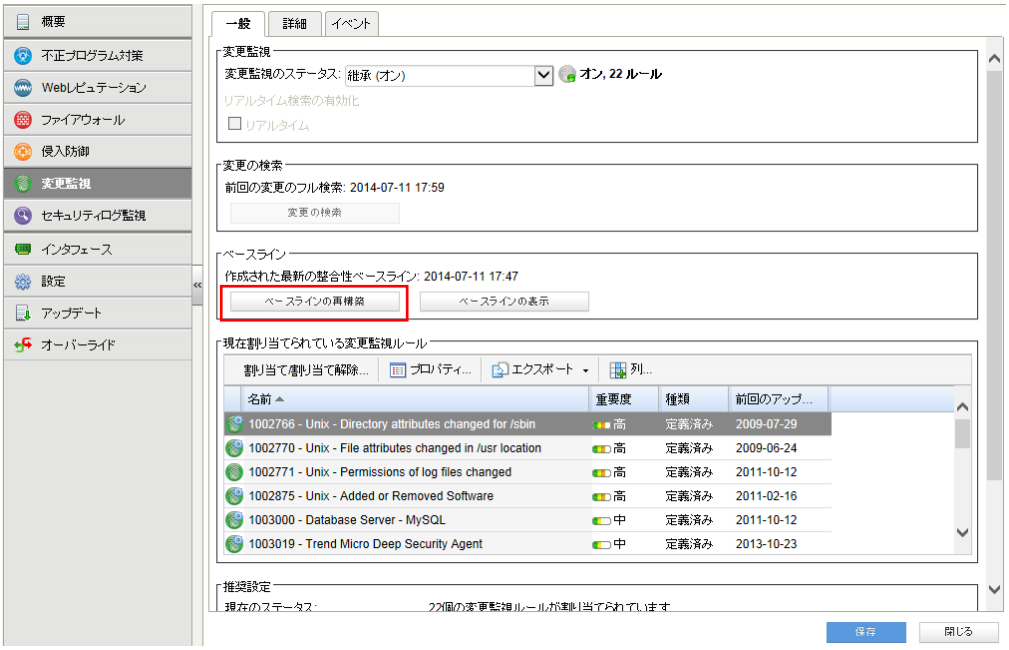
（7）ベースラインの再構築【重要】

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。

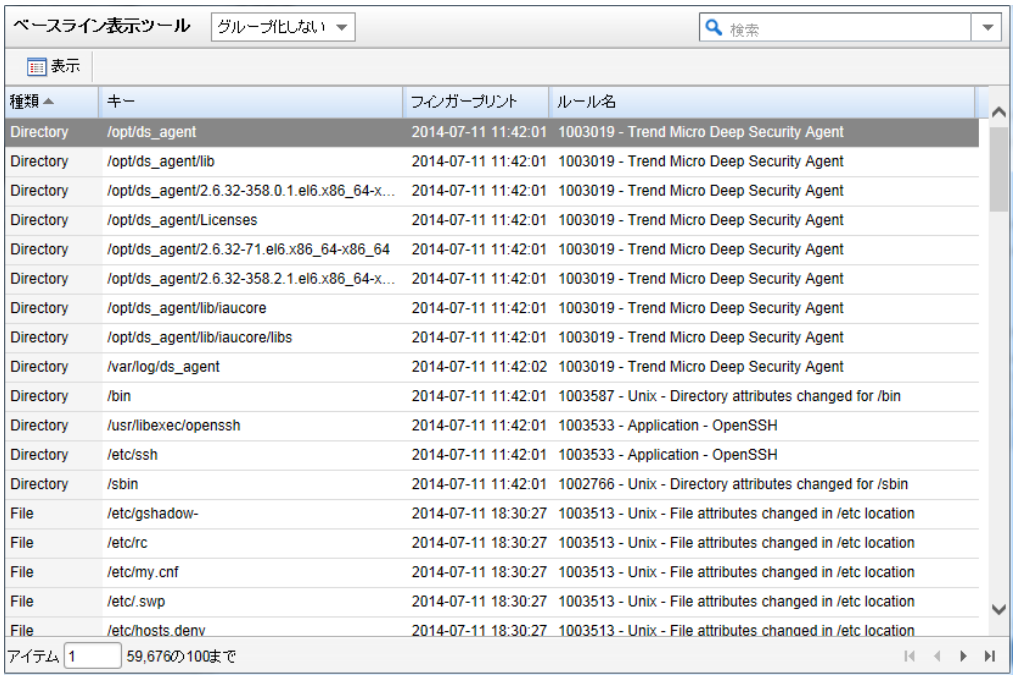
※変更監視をリアルタイムで行っている場合、コンテンツ変更などでイベント記録及びアラート通知が発生します。

「ベースラインの再構築」をクリックします。



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。

ベースライン表示

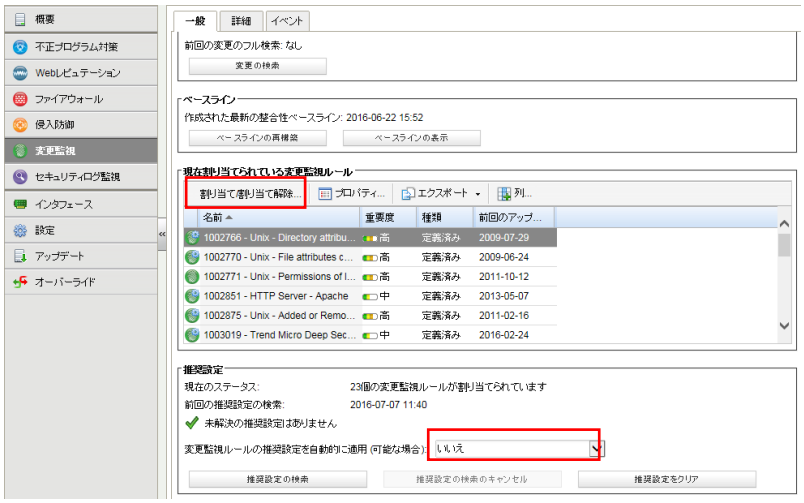


8.3. 変更監視(カスタム設定)テンプレートによる設定

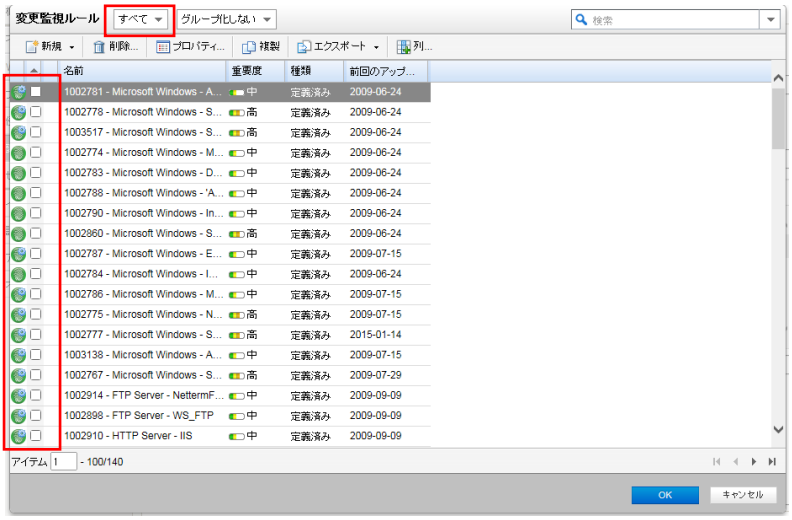
変更監視ルールの割り当てを手動で行う方法です。推奨設定とカスタム設定を合わせて使うこともできます。
多数の一般的なOSおよびアプリケーション用の変更監視ルールが用意されていますが、独自のカスタムルールを作成することもできます。カスタムルールを作成する場合は、「基本ルール」テンプレートを使用するか、新しいルールをXMLで記述できます。ルールをポリシーで作成することによりポリシーを割り当てているコンピュータ全てにルールを割り当てることもできます。
※定義済みルールに加えて、Web サーバとして変更監視を適用しておくべきルールをカスタムルールとして作成することを推奨します。

■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。

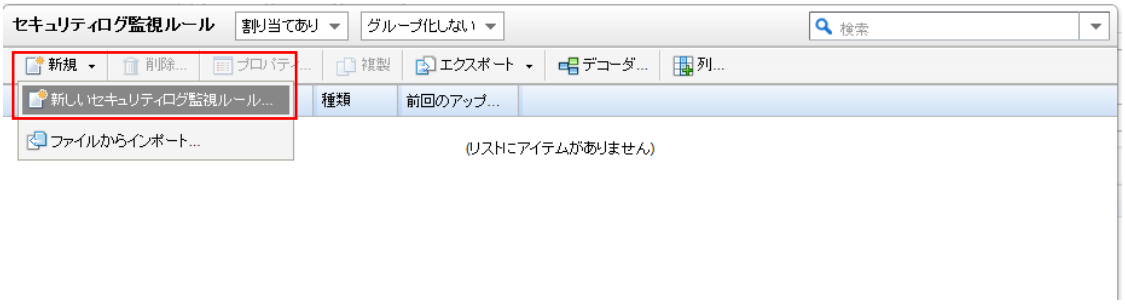


(2)表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックスにチェックを入れ「OK」をクリックすることで、選択したルールが割り当てされます。



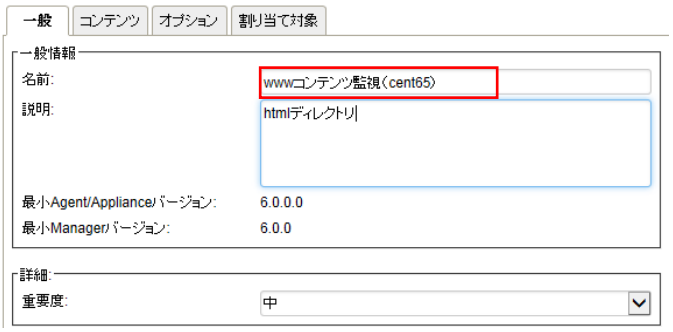
(3)変更監視ルールの作成

新規から「新しい変更監視ルール」を選択します。



(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。

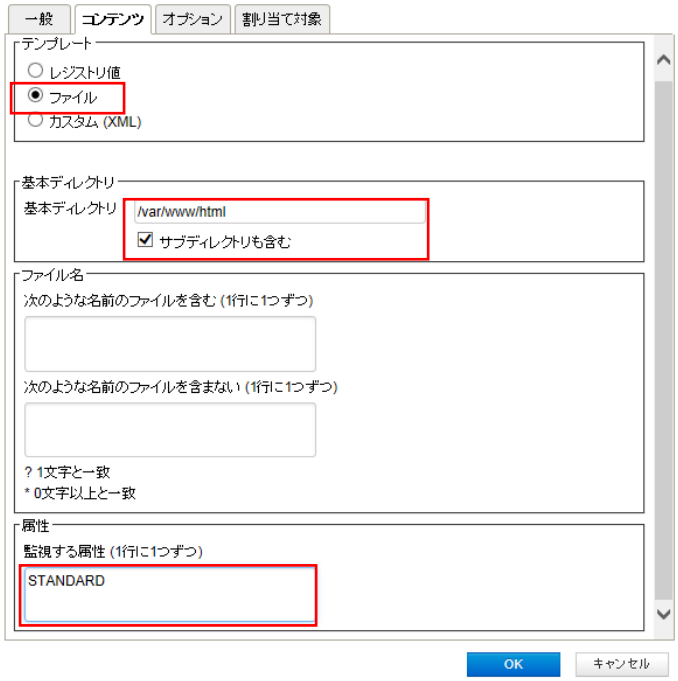


「コンテンツタブ」

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



※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

■変更監視で監視できるファイル属性

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 ハッシュ
Md5	MD5 ハッシュ

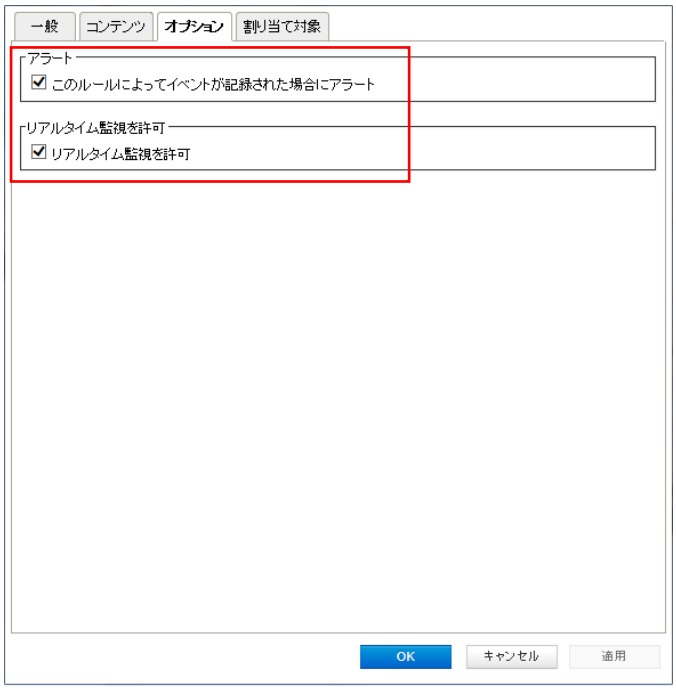
Flags	Windows のみ。GetFileAttributes() Win32 API から返されるフラグ。Windows エクスプローラでは、これらをファイルの「属性」(読み取り専用、アーカイブ、圧縮など) とみなします
SymLink Path (UNIX のみ)	ファイルがシンボリックリンクである場合は、そのリンクのパスがここに格納されます。Windows NTFS では、UNIX ライクなシンボリックリンクをサポートしますが、ファイルではなくディレクトリ専用です。Windows のショートカットオブジェクトは OS では処理されないため、本当の意味でのシンボリックリンクではありま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

「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。



(5)変更監視ルールの確認／変更

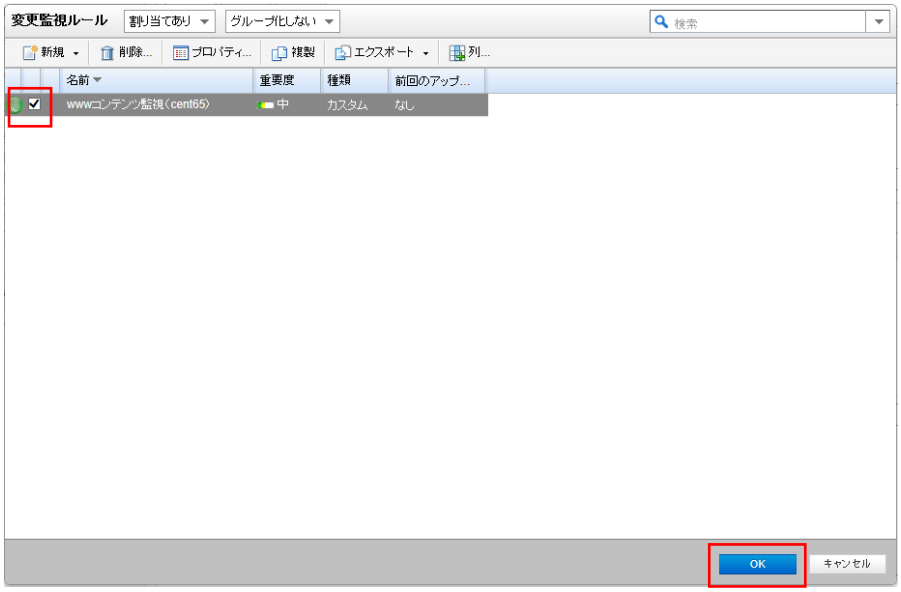
新しく作成したルールにチェックがついていれば割り当てされ有効になっています。

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。



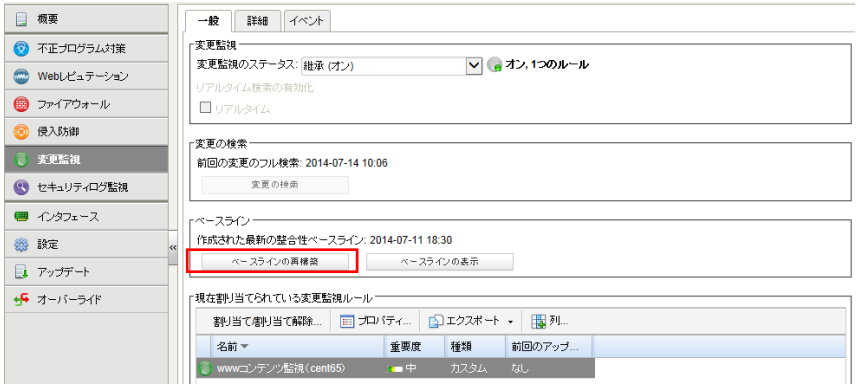
(6)ベースラインの再構築【重要】

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。



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。

ベースライン表示

8.4. 変更の検索

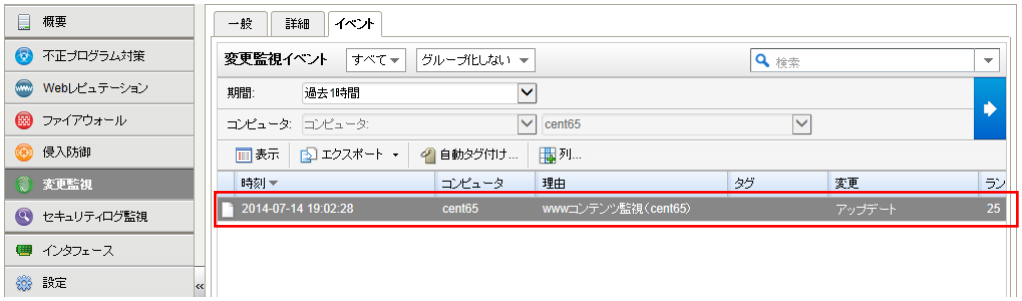
変更の検索は、「リアルタイム検索」、「予約検索」、「手動検索」に対応しています。
ファイル監視について、Linux ではリアルタイム監視には対応していません。(Windows はリアルタイム監視可)
手動検索または予約検索でのみ検知します。定期的な監視を実行するためには、予約タスクを設定する必要があります。

■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）	◎	×
ディレクトリ（DirectorySet）	◎	×
インストール済みソフトウェア（InstalledSoftwareSet）	○	○
プロセス（ProcessSet）	○	○
ポート（PortSet）	○	○
ユーザ（UserSet）	○	○
グループ（GroupSet）	○	○
サービス（ServiceSet）	○	—
レジストリキー（RegistryKeySet）	×	—
レジストリ値（RegistryValueSet）	×	—
Windows Management Instrumentation（WQLSet）	○	—

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。

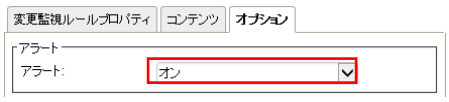


イベントをダブルクリックすると詳細が表示されます。

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」



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。

※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。

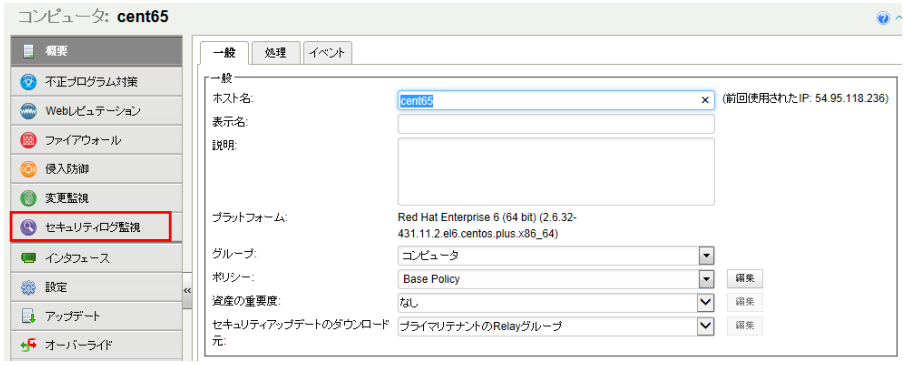
9.1. セキュリティログ監視の有効化

(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。

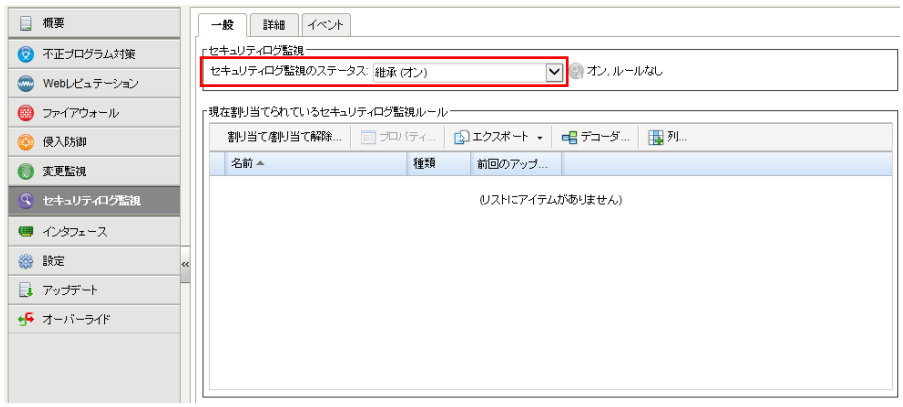
(2) サーバの設定画面が表示されます。

「セキュリティログ監視」をクリックします。



(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。

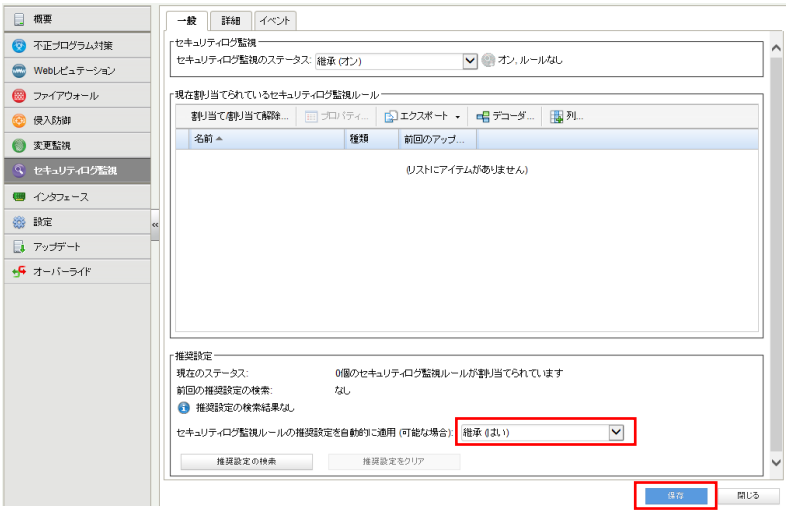
これでセキュリティログ監視が有効になります。 継承（オン）になっている場合は既に有効になっています。



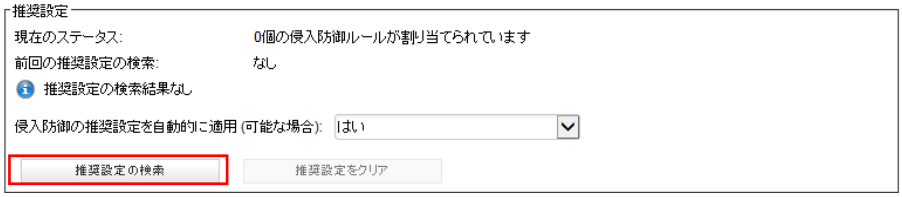
9.2. セキュリティログ監視（推奨設定）

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。

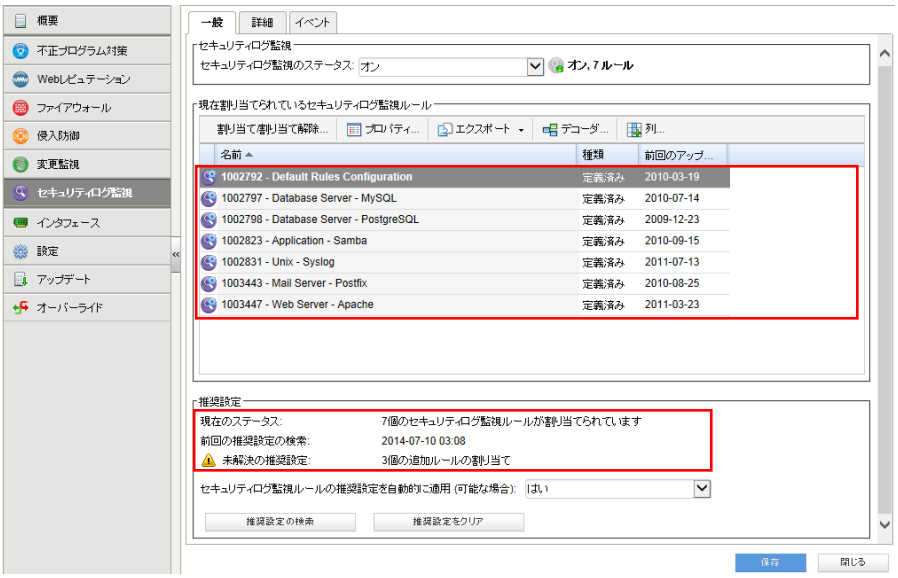
(1)セキュリティログ監視ルールの推奨設定を自動的に適用（可能な場合）:を「はい」にします。
「保存」をクリックして設定を保存します。継承（はい）になっている場合は既に有効になっています。



(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。

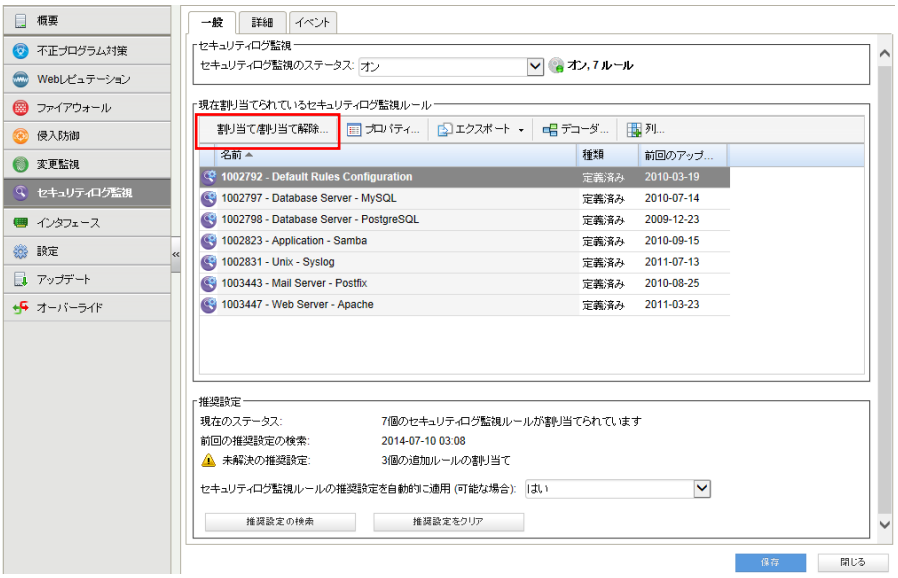


(3) 推奨設定の検索が完了するとセキュリティログ監視ルールがサーバに割り当てされます。
例では 7 個のルールが割り当てられています。
しかし、未解決の推奨設定警告(3 個)が出ています。一部ルールによっては自動設定ができず、ログファイルの指定が必要となります。

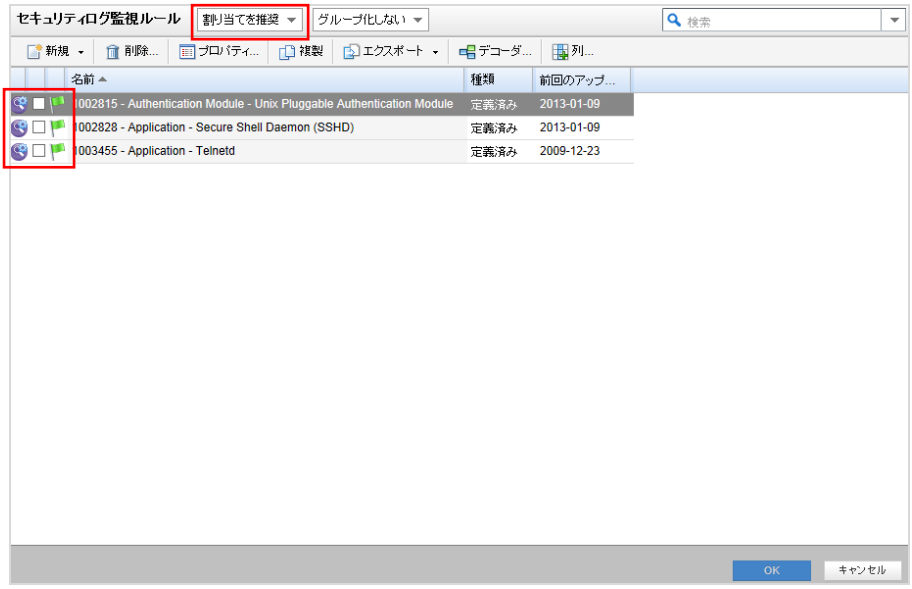


(4) 未解決の推奨設定

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。

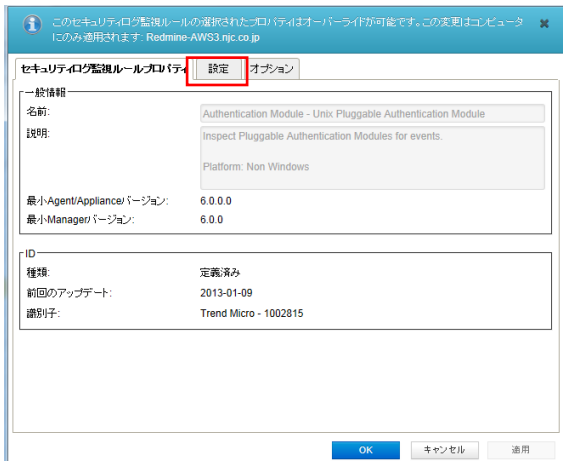


(5)セキュリティログ監視ルールの「割り当てを推奨」を選択します。
推奨設定検索によって割り当てを推奨するルール一覧が表示されます。
旗マークが推奨設定により検索されたルールで、アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。自動割り当てされない理由は、システム環境によってログファイルの指定場所が異なる場合があるためです。チェックボックスのオン／オフでルールの割り当て／割り当て解除を行えます。決定は「OK」をクリックしてください。



(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。

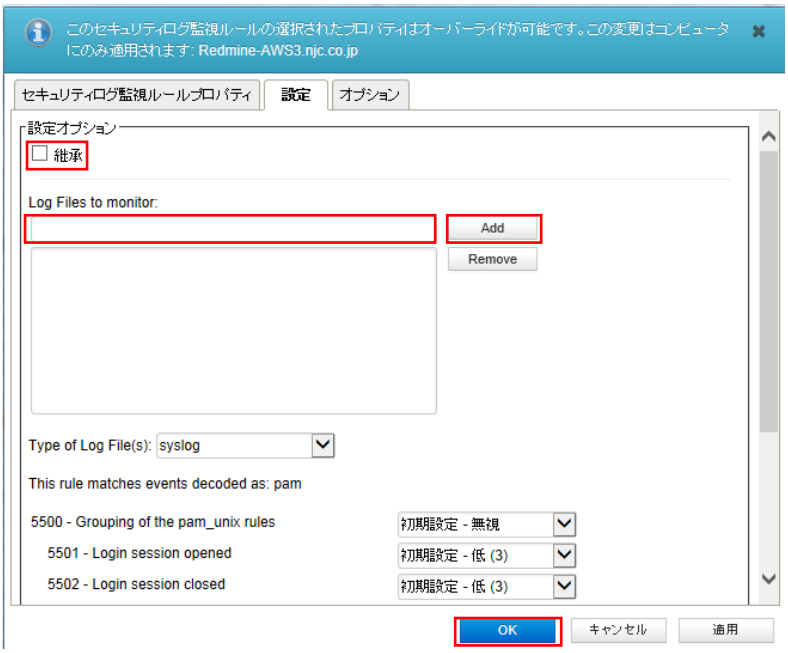
セキュリティログ監視ルールのプロパティが開きます。
設定タブを選択します。



(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。

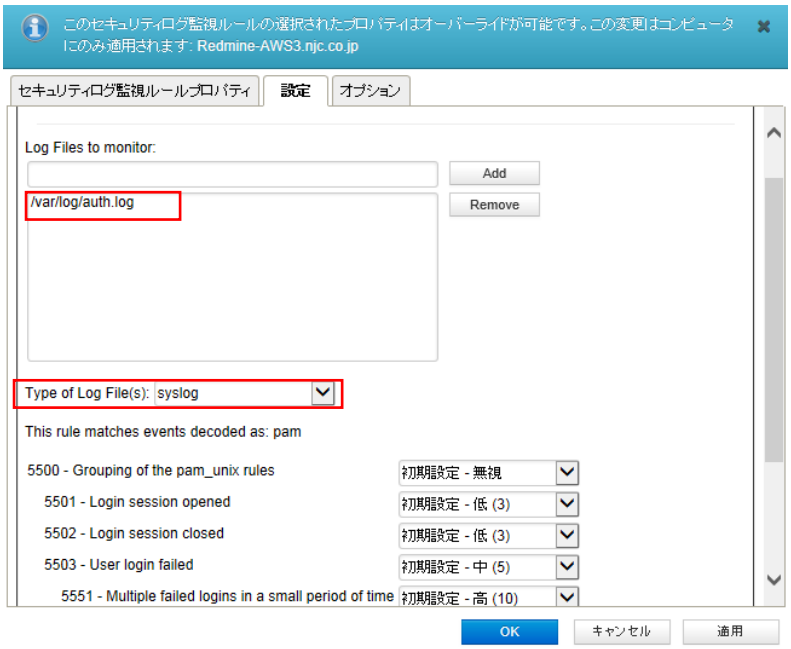
例) /var/log/auth.log

ログファイルを指定したら add をクリックしてください。



(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。



(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	ユ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

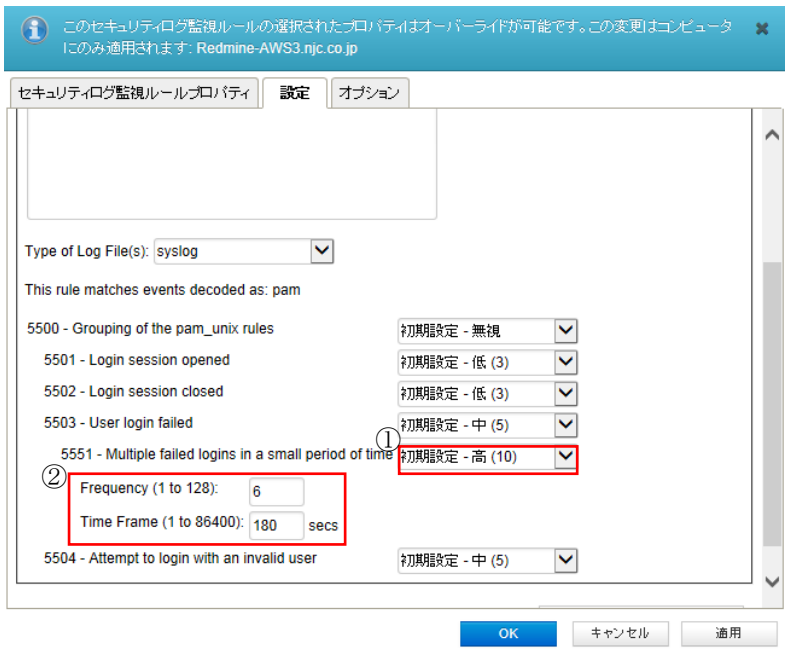
②セキュリティログ監視イベントの発生頻度設定

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。

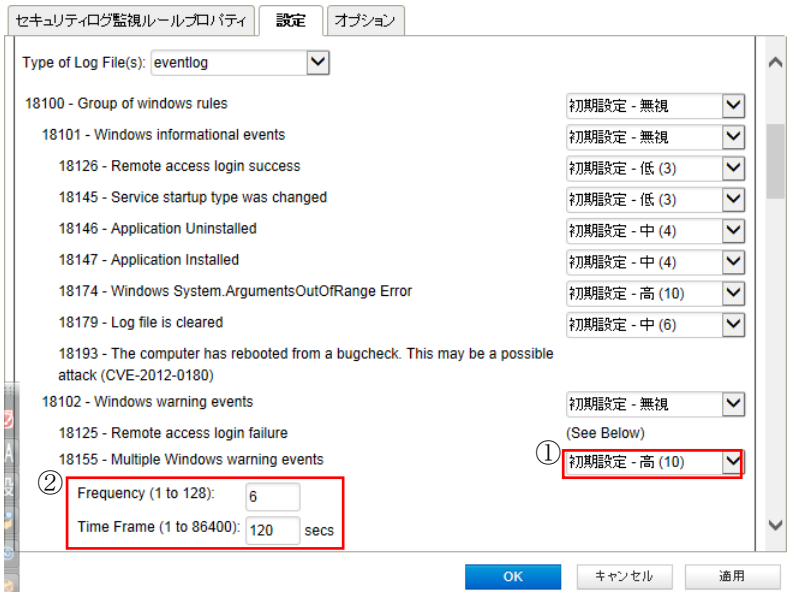
例ではログイン失敗やログインセッションオープンなどが 180 秒以内に 6 回発生した場合に重要度高(10)としてイベントに記録されます。

※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)



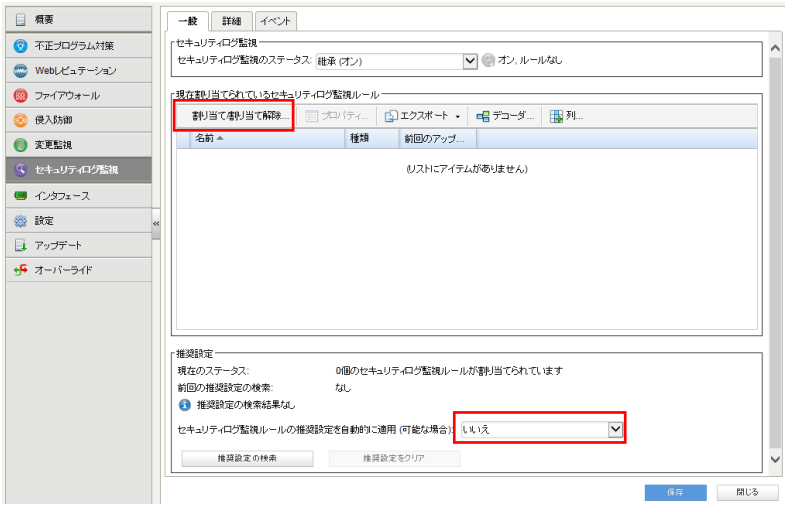
参考ルール名:1002795-Maicrosoft Windows Events(Windows)



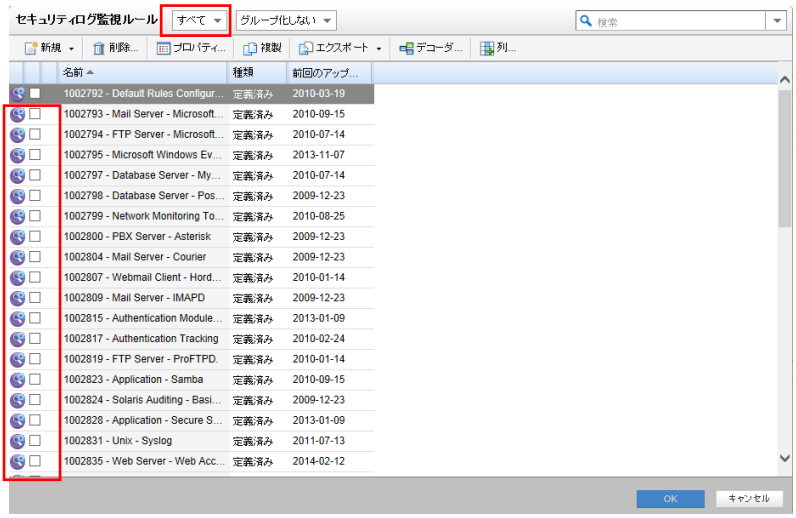
9.3. セキュリティログ監視（カスタム設定）テンプレートによる設定（Linux 例）

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。

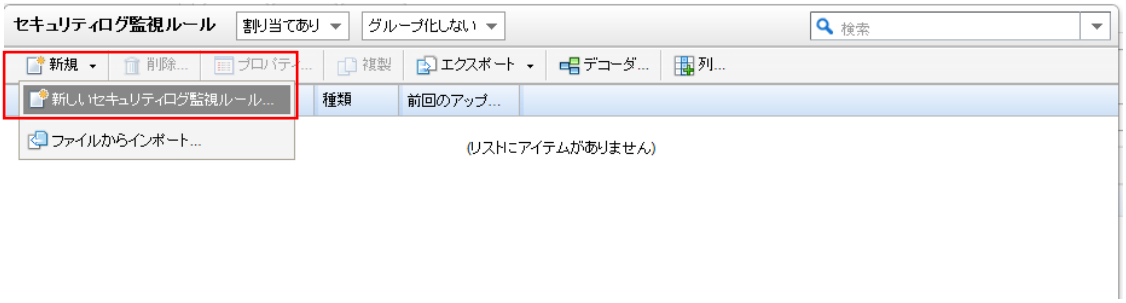


(2) 表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックスにチェックを入れ「OK」をクリックすることで、選択したルールが割り当てされます。



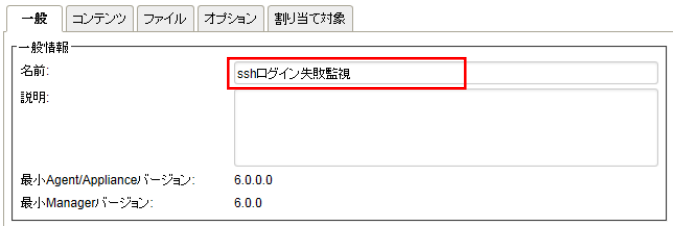
(3)セキュリティログ監視ルールの作成

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。



(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。



「コンテンツタブ」

テンプレート:基本ルール

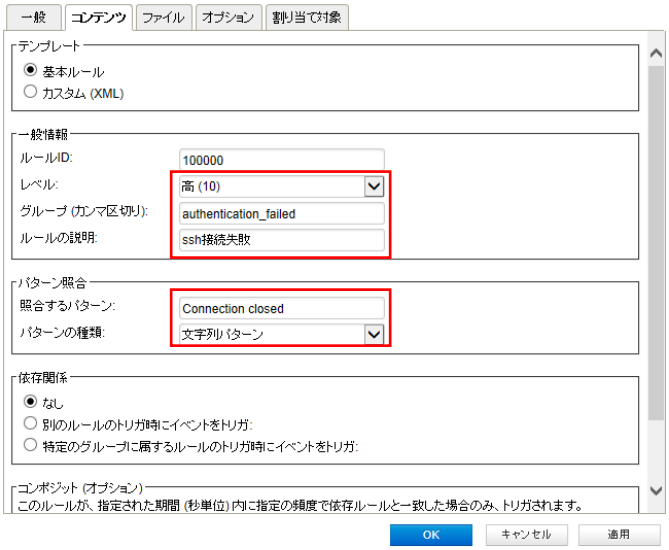
ルール ID:自動的に採番されます。

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

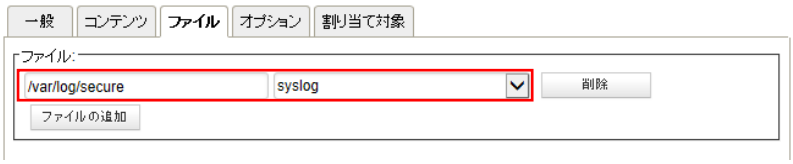


「ファイルタブ」

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。

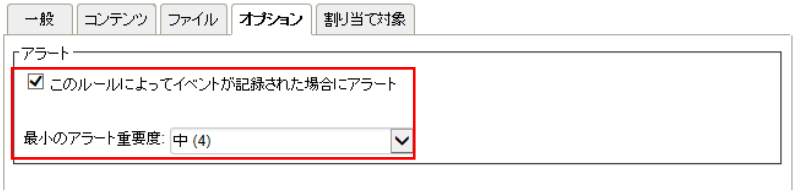


「オプションタブ」

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。



(5) セキュリティログ監視ルールの確認／変更

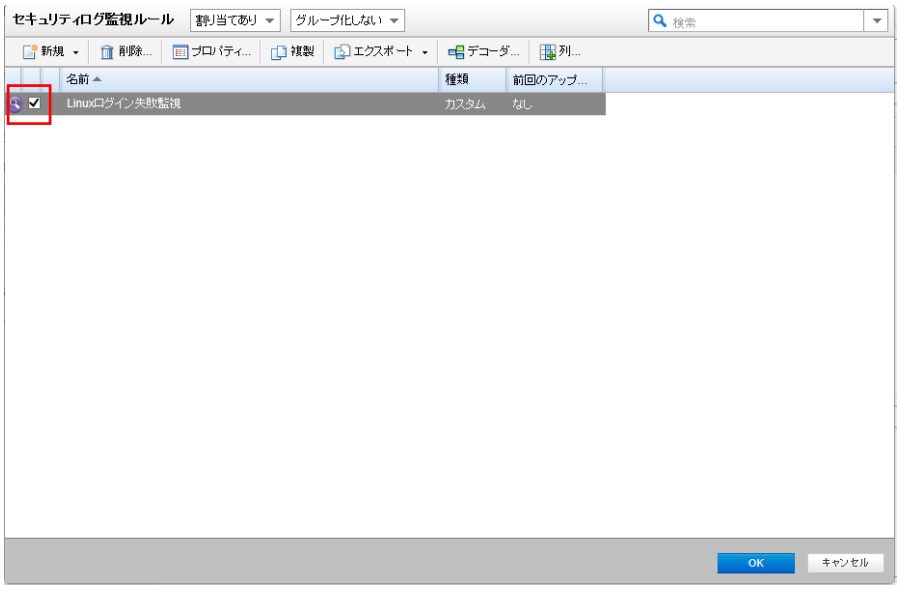
新しく作成したルールにチェックがついていれば割り当てされ有効になっています。

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。

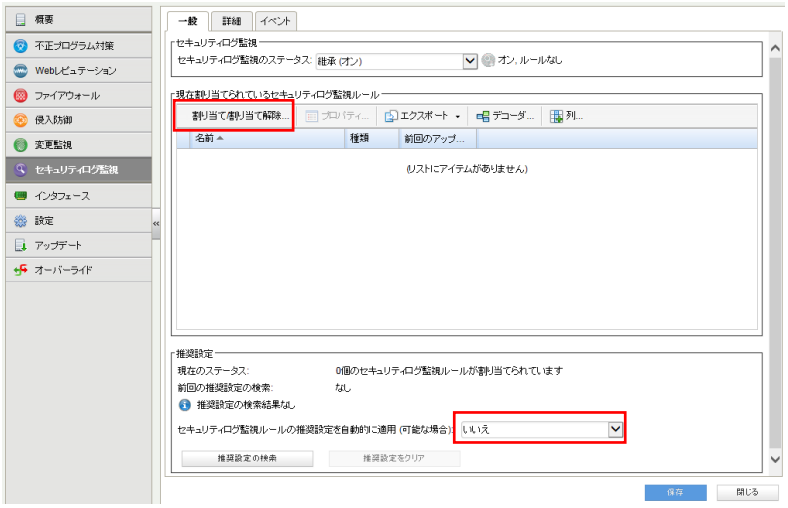
設定を終了するには、「OK」をクリックしてください。



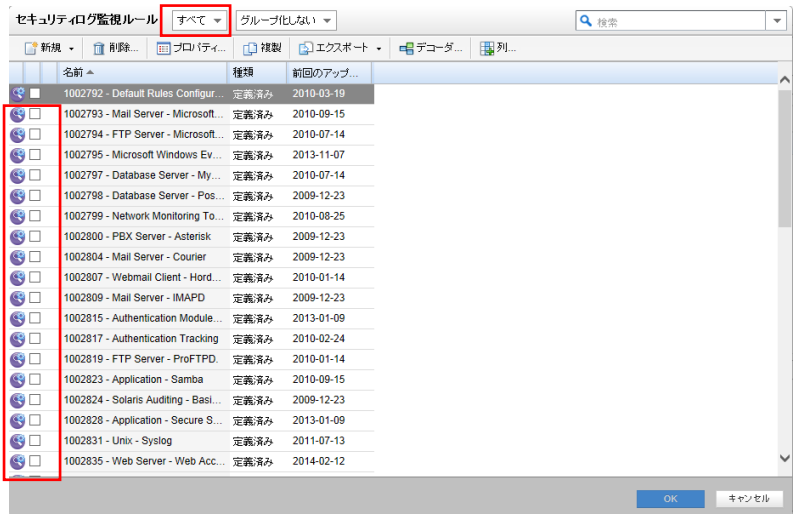
9.4. セキュリティログ監視（カスタム設定）XML よる設定（Windows 例）

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。

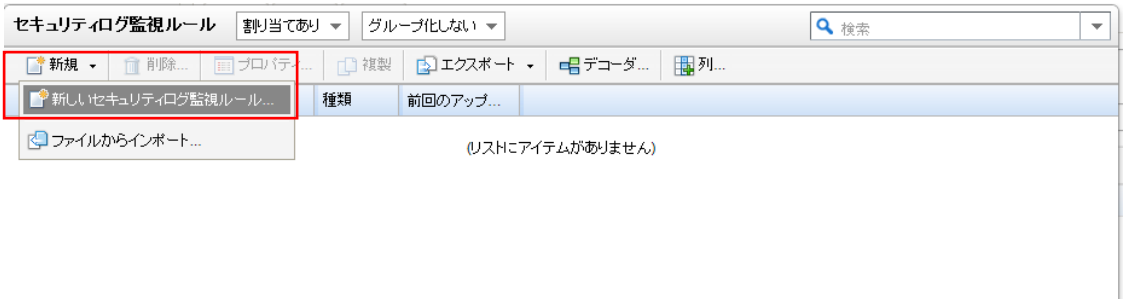


(2) 表示フィルタにより「割り当てあり」や「割り当てなし」、「種類別」や「前回のアップデート別」などで表示させることができます。「すべて」を選ぶと定義済みのすべてのルールが表示されます。アイコンに歯車がついているルールは、オプション設定ができるものや設定が必要となるルールです。チェックボックスにチェックを入れ「OK」をクリックすることで、選択したルールが割り当てされます。



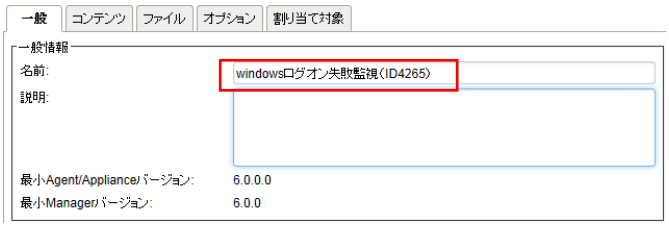
(3)セキュリティログ監視ルールの作成

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。



(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。



「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。

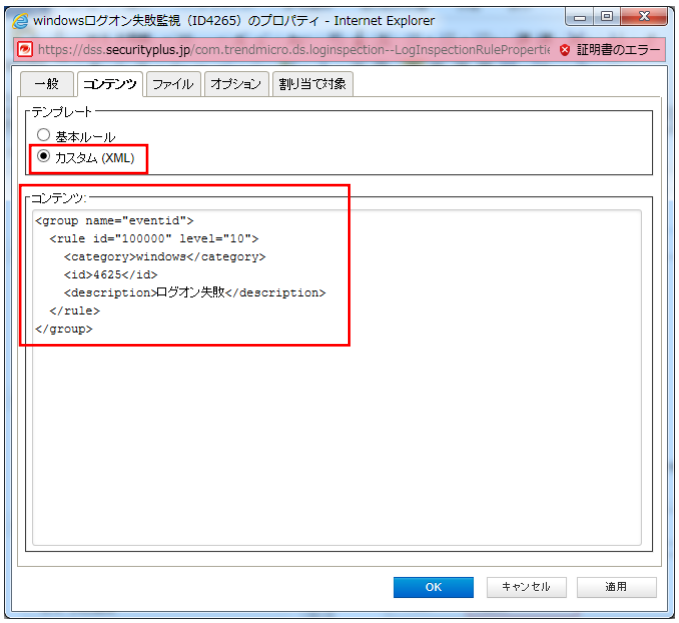
テンプレート:カスタム(XML)

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">
    <category>windows</category>
    <id>4625</id>
    <description>ログオン失敗</description>
  </rule>
</group>
```

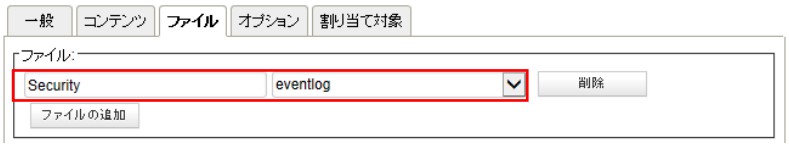


「ファイルタブ」

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。

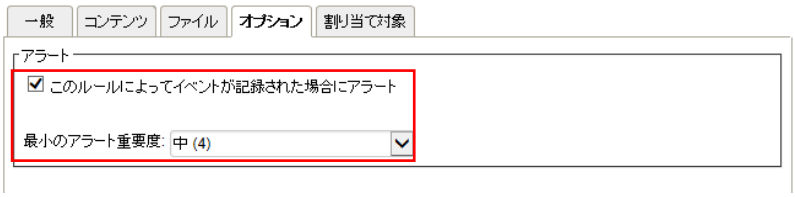


「オプションタブ」

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。



(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。

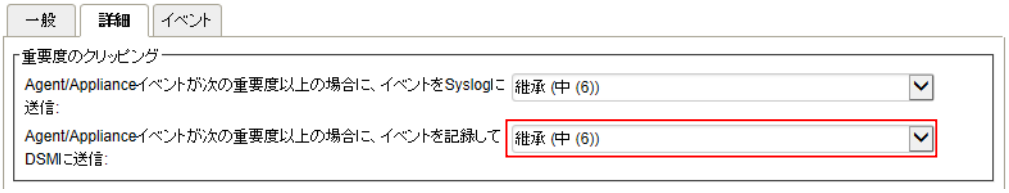
設定を終了するには、「OK」をクリックしてください。

9.5. セキュリティログ監視イベント

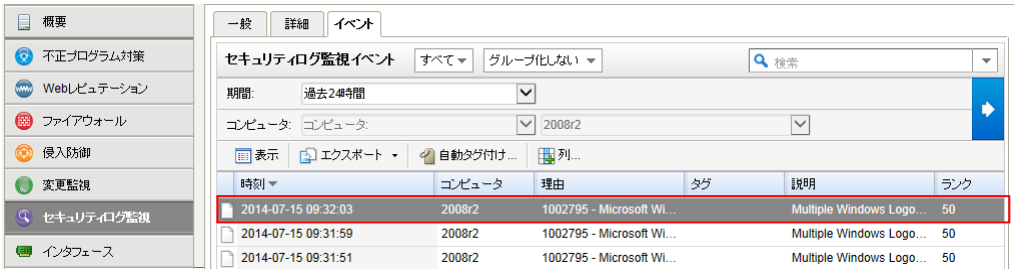
セキュリティログ監視ルール及び、重要度レベルに合致した場合、セキュリティログ監視イベントとして記録します。

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。



変更監視イベント



イベントをダブルクリックすると詳細が表示されます。

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。

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。

※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

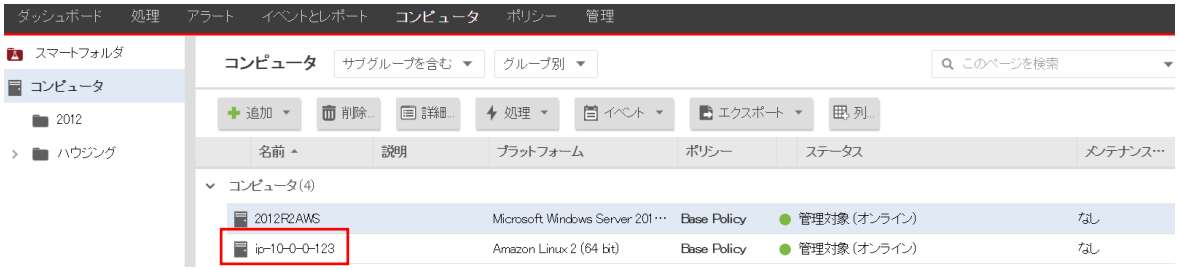
・PHP ページ、Python スクリプト、または Java アプリケーションの追加

・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

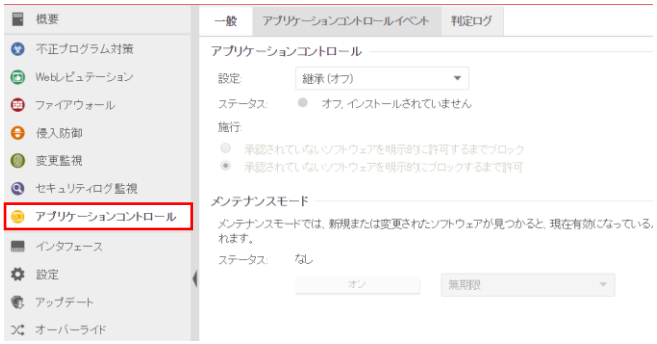
(1) 管理 Web コンソールにログオンしてください。

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。

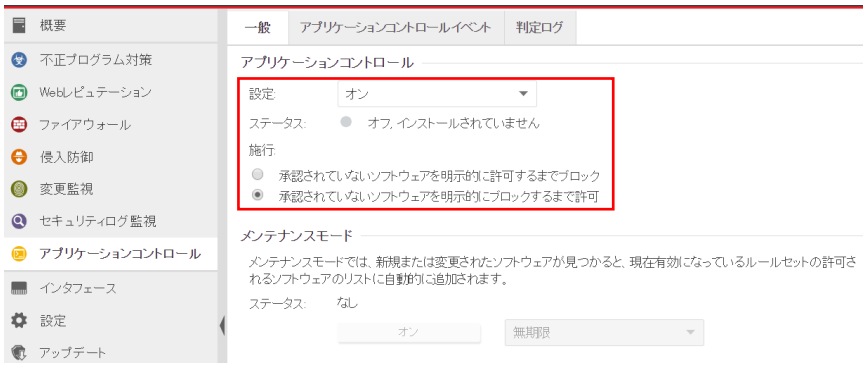


(2) サーバの設定画面が表示されます。

「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。



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。

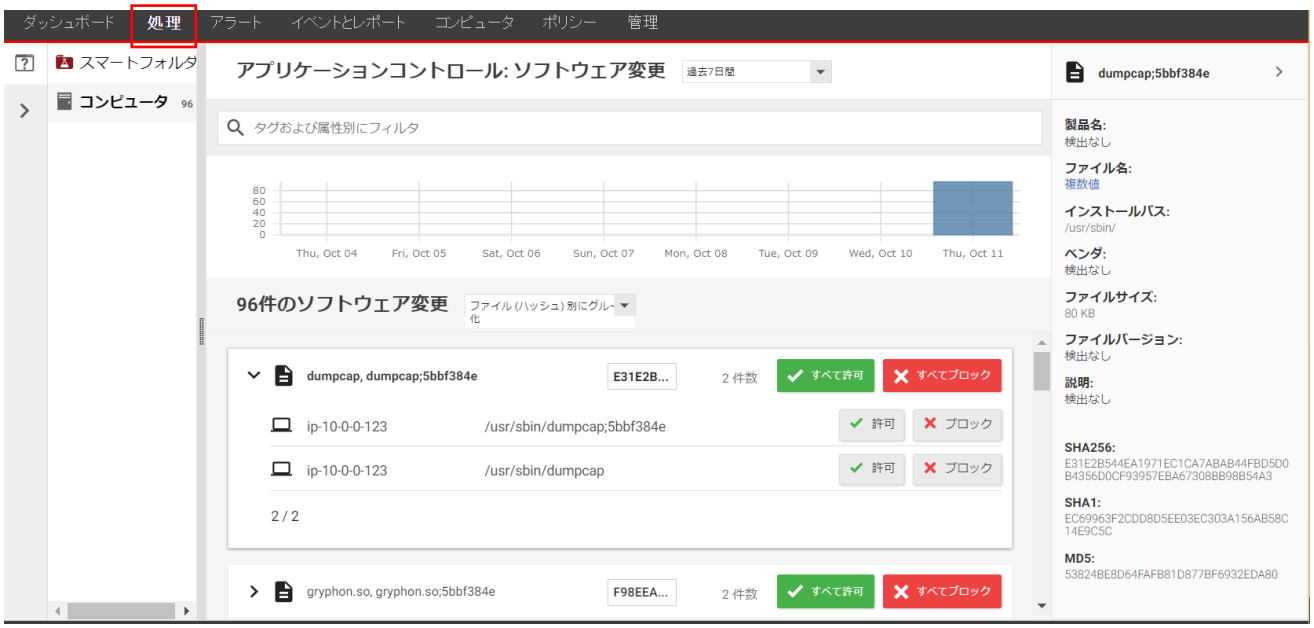
アプリケーションコントロールが有効化され、最初のソフトウェアインベントリ検索が完了すると、次の状態になります。
[コンピュータ] の [ステータス] が「アプリケーションコントロールルールセットの構築中」から「管理対象（オンライン）」に変わります。
[イベントとレポート]→[イベント]→[システムイベント] に、「アプリケーションコントロールルールセットの作成開始」および「アプリケーションコントロールルールセットの作成完了」が記録されます。

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。

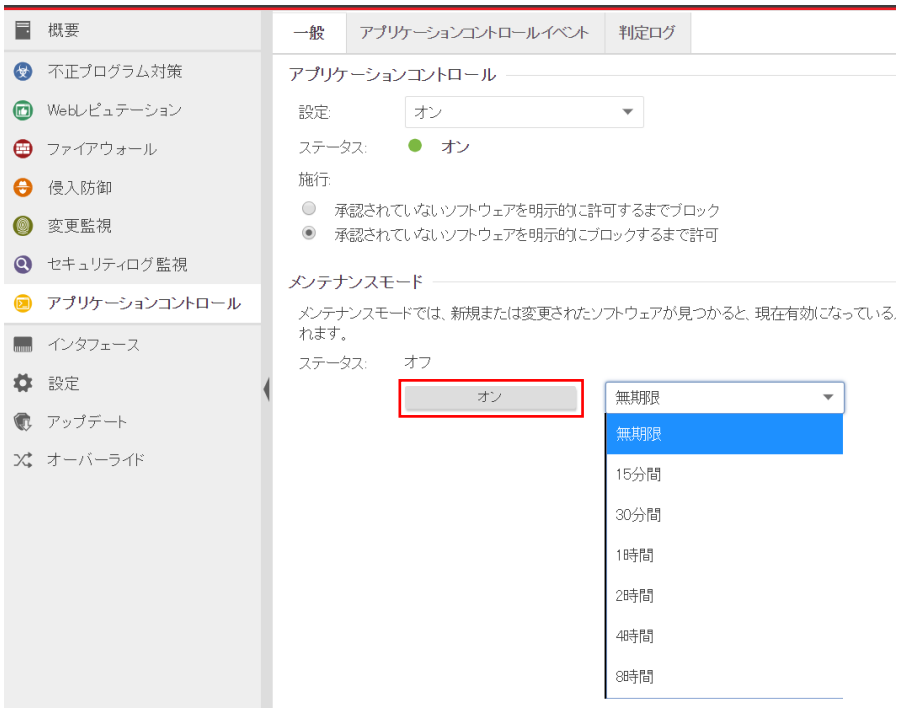


10.3. メンテナンスモード

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、

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。

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。

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一覧が表示され、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

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。

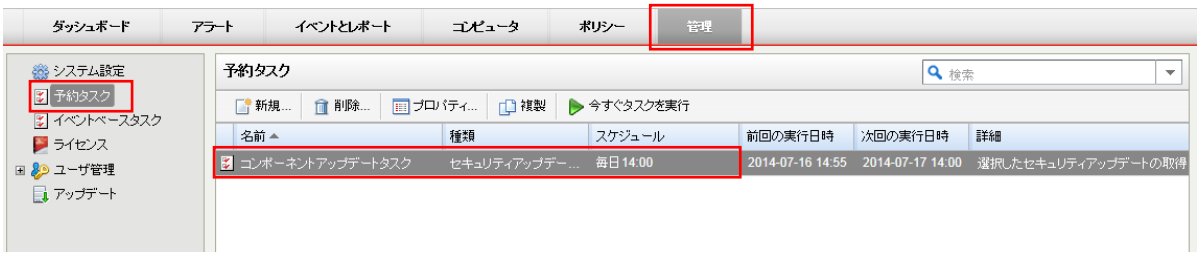
⑧コンピュータの検出: 使用しません。
⑨ポリシーの送信:使用しません。

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。

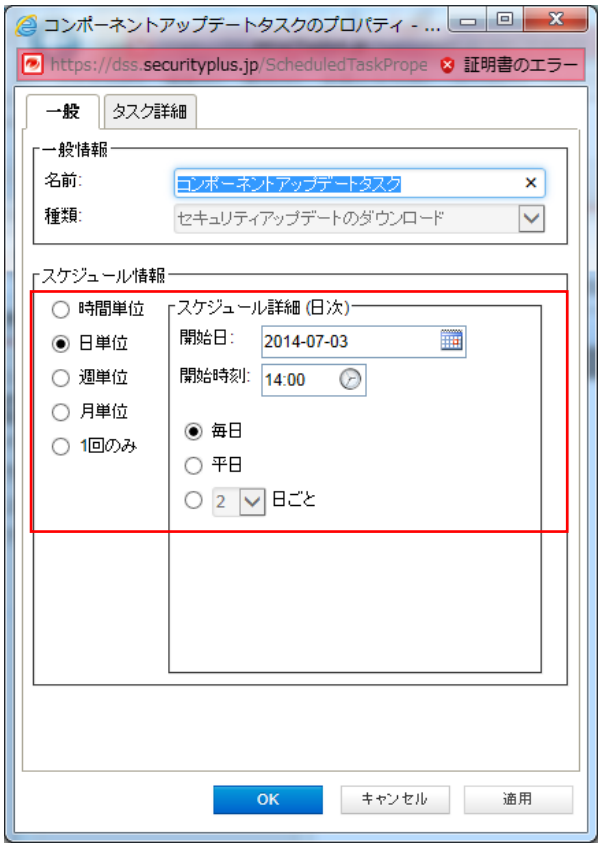
コンポーネントアップデートタスクをクリックします。



(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。



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。

(2)予約タスクの種類を選択します。

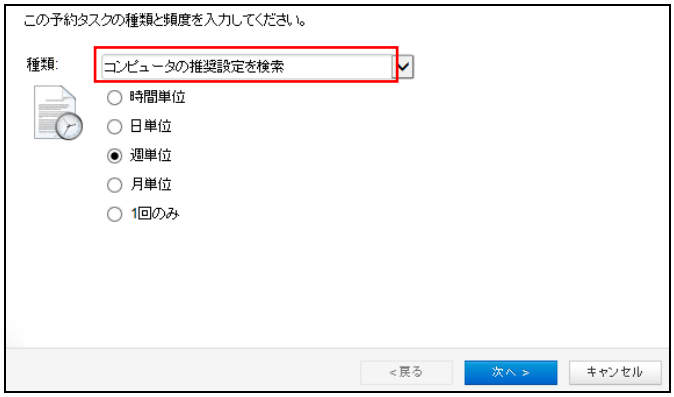
種類:「コンピュータの推奨設定を検索」を選択します。

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。

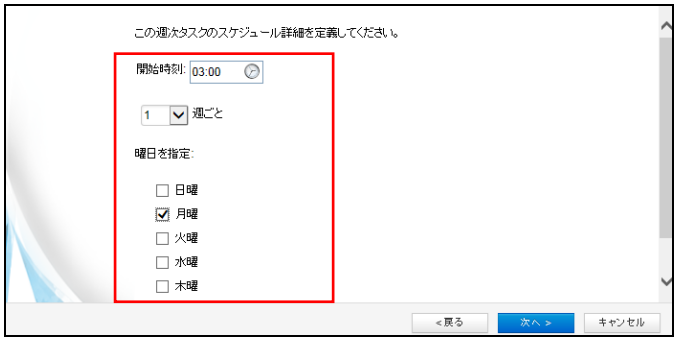
　また、OS やアプリケーション環境は頻繁に変更されることは少ないため、週単位ごとの実施を推奨します。

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。

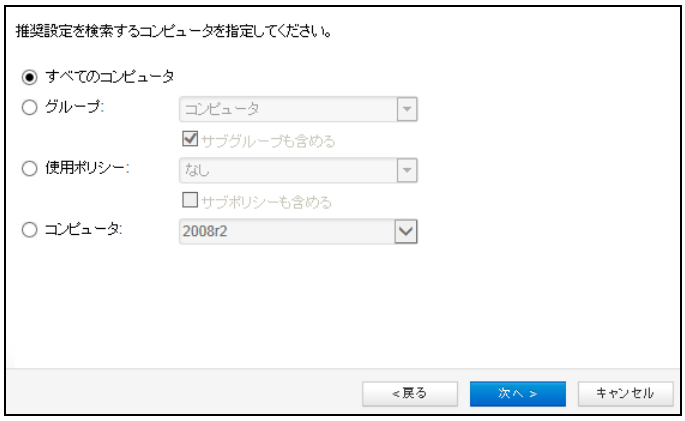


(4)推奨設定検索を行うコンピュータを指定します。

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。

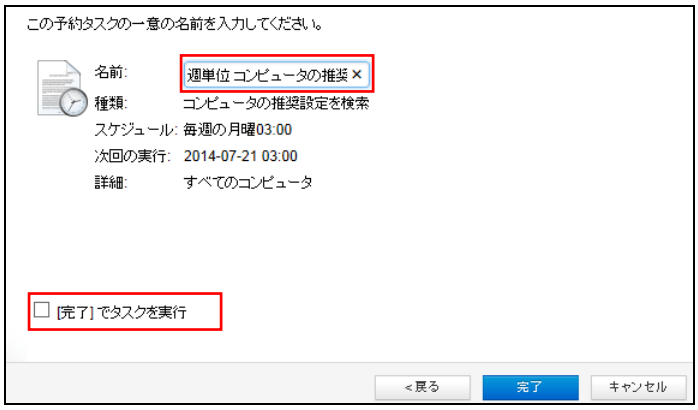


(5)設定の確認が表示されます。

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。



(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。

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

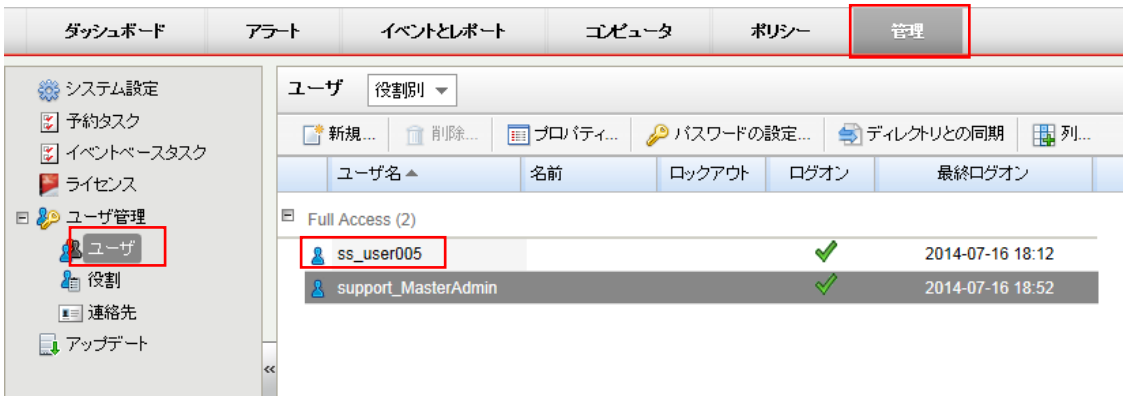
(1) 管理 Web コンソールにログオンしてください。

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。

※suppport_MasterAdmin は変更、削除できません。

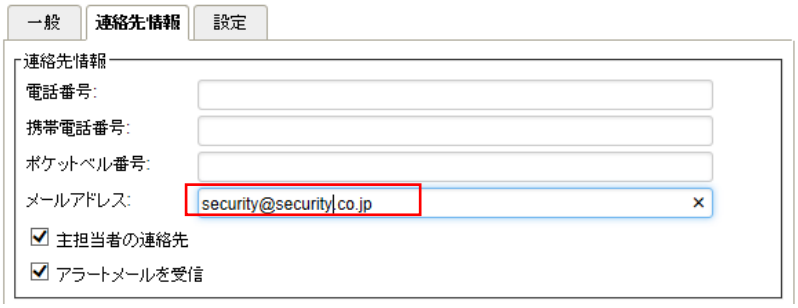


(2) ユーザ名のプロパティが表示されます。

「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。



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:

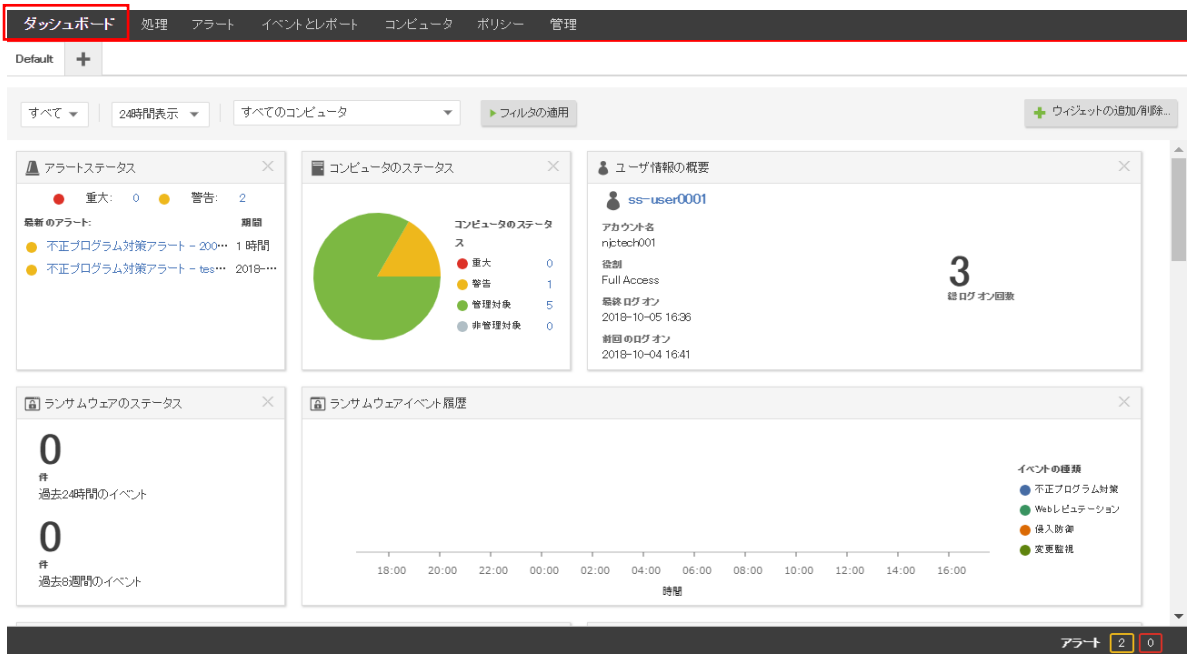
2012R2―SV

14.　管理 WEB コンソール

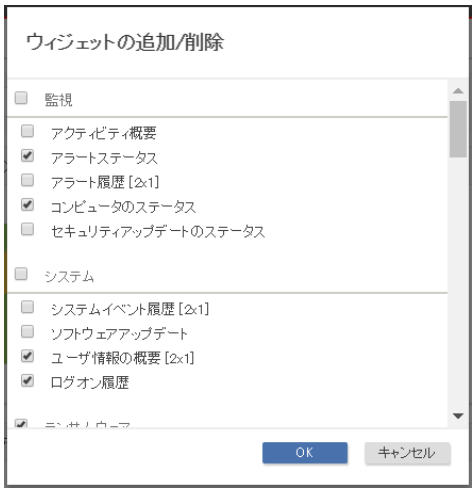
管理 Web コンソールの基本的な使用方法について説明いたします。

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



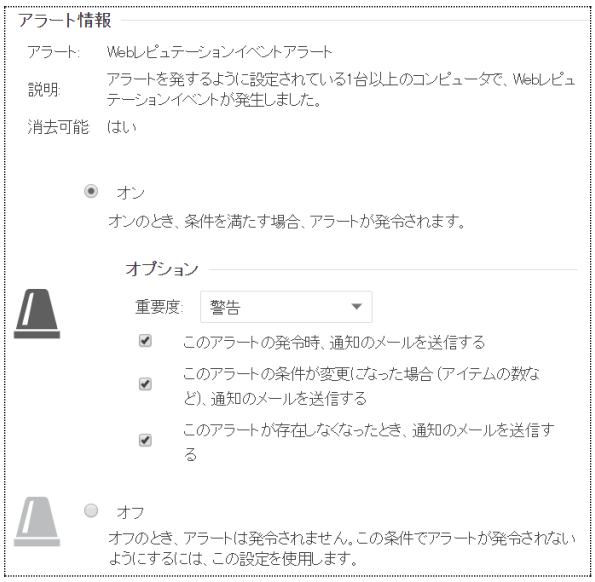
14.2. アラート

［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。



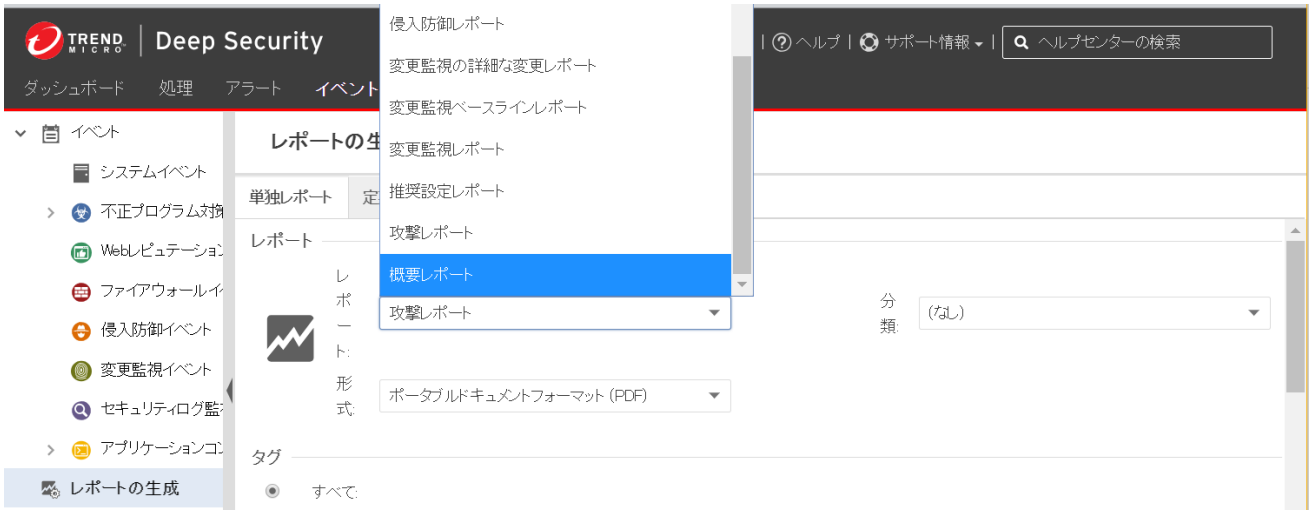
14.3. イベントとレポート

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

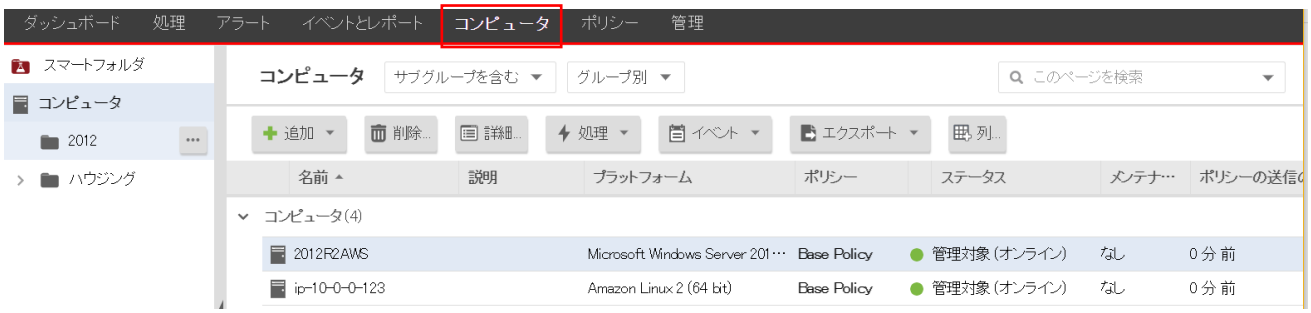
PDF または RTF の形式でレポートを生成します。[レポート] 画面で生成されたほとんどのレポートには、日付範囲、コンピュータグループ別のレポートなどの設定可能なパラメータがあります。パラメータのオプションは、それらが適用されないレポートの場合は無効になります。

定期レポートは予約タスクで設定します。



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)。

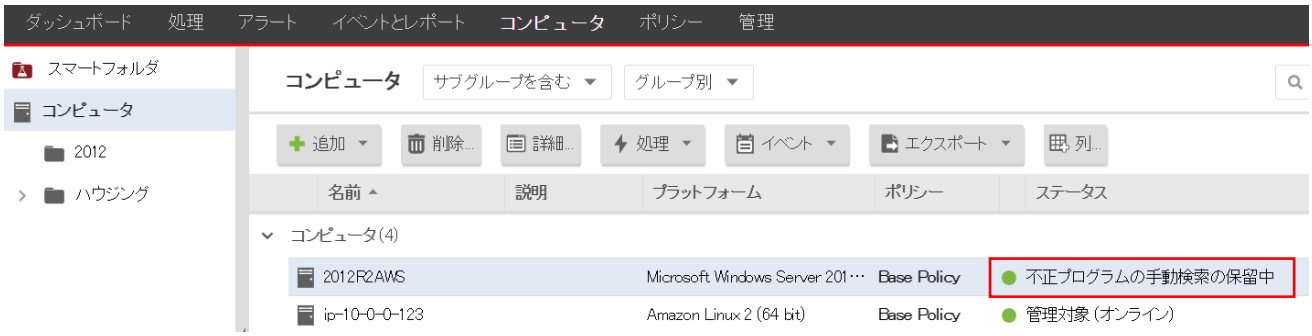


コンピュータを右クリックすると「処理」から「推奨設定の検索」や「不正プログラム対策のフル検索」などをショートカットで実効できます。

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。

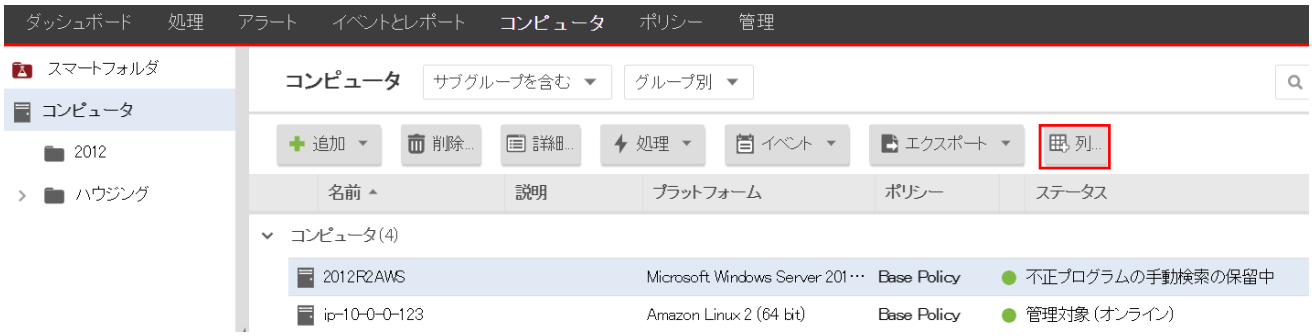
これは、コンピュータが管理サーバへの接続を 5 分間隔で行っているため、指示待ちの状態を表します。

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。



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。



14.5. ポリシー

[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。

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　第 2.10 版

発行日　：　2021 年 7 月 3 日
発行元　：　日本事務器株式会社