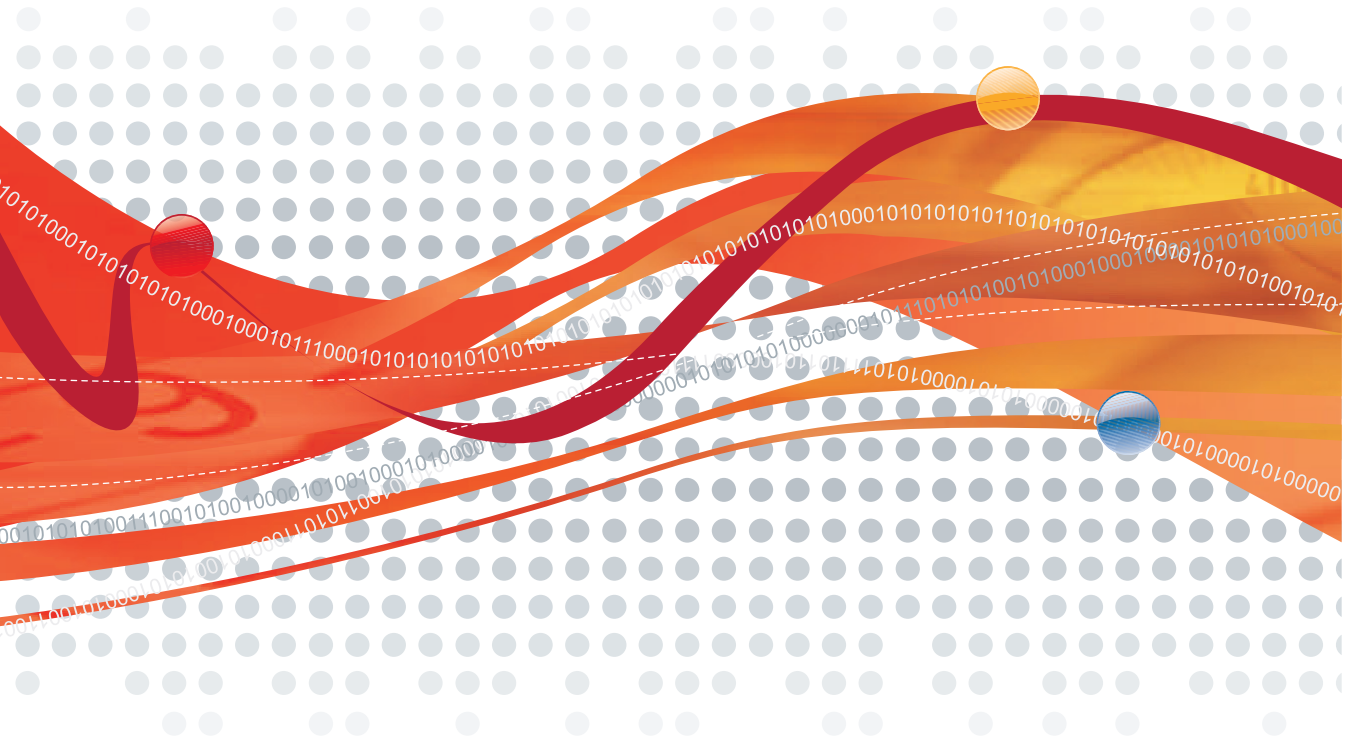




脆弱性対策オプション™ 1.5

管理者ガイド



※注意事項

トレンドマイクロへのお客さま情報の送信について

- (1) 「Webレピュテーションサービス」、「フィッシング詐欺対策」、「ベアレンタルコントロール/URLフィルタリング」および「Trend ツールバー」等について
- ①トレンドマイクロでは、お客さまがアクセスしたWebページの安全性の確認のため、お客さまより受領した情報にもとづき、お客さまがアクセスするWebページのセキュリティチェックを実施します。なお、お客さまがアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)は、暗号化してトレンドマイクロのサーバに送信されます。サーバに送信されたURL情報は、Webサイトの安全性の確認、および当該機能の改良の目的にのみ利用されます。
- ②当該機能が有効にしたり、Webページにアクセスした場合、以下の事象がおこることがありますのでご注意ください。
- (a) お客さまがアクセスしたWebページのWebサーバ側の仕様が、お客さまが入力した情報等をURLのオプション情報として付加しWebサーバへ送信する仕様の場合、URLのオプション情報にお客さまの入力した情報(ID、パスワード等)などを含んだURLがトレンドマイクロのサーバに送信され、当該Webページのセキュリティチェックが実施されます。
- (b) お客さまがアクセスするWebページのセキュリティチェックを実施する仕様になっていることから、お客さまがアクセスするWebサーバ側の仕様によっては、URLのオプション情報に含まれる内容により、お客さまの最初のリクエストと同様の処理が行われます。
- ③Webサイトのセキュリティ上の判定はトレンドマイクロの独自の基準により行われております。当該機能において判定されたWebサイトのアクセス可否の最終判断につきましては、お客さまにてお願いいたします。
- (2) Trend Micro Smart Protection Network (「スマートフィードバック」、「ファイルレピュテーションサービス」、「脅威情報の送信」および「ウイルストラッキング」等を含みます)について
- 脅威に関する情報を収集、分析し保護を強化するために、お客さまのコンピュータに攻撃を試みる脅威に関連すると思われる情報を収集して、トレンドマイクロに送信することがあります。送信された情報はプログラムの安全性の判定や統計のために利用されます。また情報にお客さまの個人情報や機密情報等が意図せず含まれる可能性があります。トレンドマイクロがファイルに含まれる個人情報や機密情報自体を収集または利用することはありません。お客さまから収集された情報の取り扱いについての詳細は、<http://jp.trendmicro.com/jp/about/privacy/spn/index.html>をご覧ください。
- (3) 「迷惑メール対策ツール」について
- トレンドマイクロ製品の改良目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
- (4) 「E-mailレピュテーションサービス」について
- スパムメールの判定のために、送信元のメールサーバの情報をトレンドマイクロのサーバに送信します。
- (5) 「ユーザービヘイビアモニタリング」について
- トレンドマイクロ製品の改良目的のために、お客さまがトレンドマイクロ製品をどのような設定にして利用しているのかわかる設定の情報およびお客さまがトレンドマイクロ製品をどのように操作したのかわかる操作履歴の情報を、匿名でトレンドマイクロのサーバに送信します。

輸出規制について

お客さまは、本製品およびそれらにおいて使用されている技術(以下「本ソフトウェア等」といいます)が、外国為替および外国貿易法、輸出貿易管理令、外国為替令および省令、ならびに、米国輸出管理規則に基づく輸出規制の対象となる可能性があること、ならびにその他の国における輸出規制対象品目に該当している可能性があることを認識の上、本ソフトウェア等を適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出しないものとします。

お客さまは、2012年5月現在、米国により定められる禁輸国が、キューバ、イラン、北朝鮮、スーダン、シリアであること、禁輸国に関する情報が、以下のウェブサイトにおいて検索可能であること、ならびに本ソフトウェア等に関連した米国輸出管理法令の違法行為に対して責任があることを認識の上、違法行為が行われないよう、適切な手段を講じるものとします。

<http://www.treas.gov/offices/enforcement/ofac/>

<http://www.bis.doc.gov/complianceand/enforcement/Lists/ToCheck.htm>

また、お客さまが本ソフトウェア等を使用する場合、米国により現時点で輸出を禁止されている国の居住者もしくは国民ではないこと、および本ソフトウェア等を受け取ることが禁止されていないことを認識し、お客さまは、本ソフトウェア等を、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用することに同意するものとします。

複数年契約について

- お客さまが複数年契約(複数年分のサポート費用前払い)された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認いただけます。
<http://jp.trendmicro.com/jp/support/lifecycle/index.html>

著作権について

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本書の記述に誤りや落格があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容が予告なしに変更される場合があります。

商標について

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScan WebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・ブレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、LEAKPROOF、Trend プロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、DataDNA、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、Trend Micro Threat Management Agent、Trend Micro Threat Mitigator、Trend Micro Threat Discovery Appliance、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro IM Security、Trend Micro Email Encryption、Trend Micro Email Encryption Clients、Trend Micro Email Encryption Gateway、Trend Micro Collaboration Security、Trend Micro Portable Security、Portable Security、Trend Micro Standard Web Security、トレンドマイクロクラウドセキュリティソリューション、Trend Micro Hosted Email Security、Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、ウイルスバスター CLOUD、Smart Surfing、スマートスキャン、Trend Micro Instant Security、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Trend Micro Email Security Platform、Trend Smart Protection、Vulnerability Management Services、Trend Micro Vulnerability Management Services、Trend Micro PCI Scanning Service、Trend Micro Titanium、Trend Micro Titanium AntiVirus Plus、Smart Protection Server、Deep Security、Worry Free Remote Manager、ウイルスバスター ビジネスセキュリティサービス、HOUSECALL、SafeSync、トレンドマイクロ オンラインストレージ SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、TREND MICRO ENDPOINT PROTECTION、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、Trend Micro Threat Discovery Software Appliance、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンアップサービス、Trend Micro Deep Security あんしんバック、こどもモード、Deep Discovery、およびTCSEは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2008-2012 Trend Micro Incorporated. All rights reserved.

P/N: OSEM15025/110817_JP_R1 (2012/10)

目次

はじめに	1
ドキュメント	2
対象読者	2
ドキュメントの表記規則	3
第 1 章 脆弱性対策オプションの導入.....	5
脆弱性対策オプションについて	6
本リリースの新機能	6
第 2 章 脆弱性対策オプションのクイックスタート	9
脆弱性対策オプションサーバプラグイン	10
脆弱性対策オプションクライアントプラグイン	10
脆弱性対策オプションサーバプラグインのインタフェースを開く	11
サーバプラグインのインタフェース	12
ナビゲーション画面	12
タスク画面	13
レイアウトコントロール	13
表示コントロール	14
ツールバー	14
検索および詳細検索	14
ステータスバー	16
コンテキストメニュー	16
プログラムの概要	16
ダッシュボード	17
アラート	18
レポート	19

コンピュータ	20
セキュリティプロファイル	21
ファイアウォール	22
Deep Packet Inspection	23
コンポーネント	24
システム	25
第 3 章 ダッシュボード	27
ダッシュボードについて	28
ウィジェットについて	28
ダッシュボードをカスタマイズする	29
ウィジェットレイアウトを設定する	29
ダッシュボードウィジェットを追加したり削除する	30
情報をタグでフィルタする	30
日時の範囲で情報をフィルタする	31
コンピュータおよびコンピュータドメインでフィルタする	31
ダッシュボードの設定を管理する	31
保存したダッシュボードの設定を開く	32
第 4 章 アラート	33
アラートについて	34
アラートを表示する	34
アラートを設定する	35
アラートメールを設定する	36
第 5 章 レポート	37
レポートについて	38
レポートの生成	38

第 6 章 コンピュータを管理する	41
コンピュータについて	42
コンピュータ情報を表示する	42
コンピュータのプレビューを表示する	43
コンピュータのステータスを確認する	43
コンピュータを検索する	44
コンピュータの一覧をウイルスバスター Corp. と同期する	44
開いているポートがあるコンピュータを検索する	45
実行中のポート検索をキャンセルする	46
推奨設定についてコンピュータを検索する	46
推奨設定の検索の結果を管理する	48
推奨ルールを設定する	49
推奨設定をクリアする	49
セキュリティプロファイルを割り当てる	50
コンピュータにセキュリティプロファイルを割り当てる	50
ドメインにセキュリティプロファイルを割り当てる	50
クライアントプラグインを管理する	51
プラグイン通信を設定する	51
クライアントプラグインを配信する	53
サーバからクライアントプラグインを配信する	53
スタンドアロンクライアントプラグインインストーラを使用する	53
クライアントプラグインを有効化/無効化する	54
クライアントプラグインを停止および起動する	55
コンピュータ上のクライアントプラグインをアップデートする	55
クライアントプラグインの手動によるアップデート	56
コンピュータ上のクライアントプラグインを無効にする	56
クライアントプラグインをアンインストールする	58
コンピュータのイベントを表示する	58
警告/エラーをクリアする	59

コンピュータをロックまたはロック解除する	60
コンピュータ資産評価を割り当てる	60
コンピュータの詳細を表示および編集する	61
コンピュータ情報	62
継承および優先	69
その他プロパティ	70
コンピュータまたはセキュリティプロファイルの優先を表示する	73
第 7 章 セキュリティプロファイル	75
セキュリティプロファイルについて	76
セキュリティプロファイルの管理	76
セキュリティプロファイルの作成	76
セキュリティプロファイルの詳細の表示および編集	77
第 8 章 脆弱性対策オプションを使用する	83
脆弱性対策オプションについて	84
ファイアウォールのオンとオフを切り替えます	84
ファイアウォールイベント	84
DPI イベントのプロパティを表示する	87
リストをフィルタし、イベントを検索する	87
イベントをエクスポートする	88
ファイアウォールイベントにタグを付ける	88
ファイアウォールルール	90
ファイアウォールルールについて	90
ルール処理	90
ルール優先度	92
ルール処理およびルール優先度を集約する	92
ステートフルフィルタ	93
放置ルール	94

ファイアウォールルールのシーケンス	95
ログに関する注意	96
ファイアウォールポリシーをまとめて設計する	97
重要事項	98
新規ファイアウォールルールを作成および適用する	99
ステートフル設定	105
ステートフル設定を管理する	105
第 9 章 Deep Packet Inspection を使用する.....	111
Deep Packet Inspection について	112
パケット処理のシーケンス	112
Deep Packet Inspection をオンまたはオフにする	113
DPI イベント	114
リストをフィルタし、イベントを検索する	115
DPI イベントのプロパティを表示する	116
イベントログをエクスポートする	117
DPI イベントにタグを付ける	117
DPI ルール	119
DPI ルールプロパティを作成する	120
カスタム DPI ルールを作成する	123
DPI ルールの考慮事項	123
Hello World	123
XML での記法	124
アプリケーションの種類とルールの方向	124
ステートを使用してルールを細かく定義する	125
コメントを追加する	125
その他のルール処理	126
接続をリセットする (drop)	126
検出モードと予防モードについて	126
接続の遅延リセット (setdrop)	126

ルール属性について	127
ステート	127
大文字小文字の区別の照合	127
範囲の制約	127
カウンタの使用	128
パターンに関するその他の事項	129
高度なルール処理	130
レジスタの割り当て	131
レジスタへアクセスする	132
レジスタを比較する	132
実行の順序	136
UDP 擬似接続	137
URI の Web ルール	137
Web リソースとクエリルール	138
Web ルールの考慮事項	138
アプリケーションの種類	138
第 10 章 コンポーネント	141
コンポーネントについて	142
IP リスト	142
IP リストのプロパティ	143
MAC リスト	143
MAC リストのプロパティ	144
ポートリスト	144
ポートリストのプロパティ	145
ポート検索を設定する	145
コンテキスト	146
コンテキストのプロパティ	147
スケジュール	148
スケジュールのプロパティ	149

第 11 章 脆弱性対策オプションサーバプラグインの管理	151
脆弱性対策オプションサーバプラグインの保護	152
サーバプラグインのアップグレード	153
より大容量のデータベースへの移行	154
管理下のコンピュータの新規脆弱性対策オプションサーバへの移行	156
管理下の単一コンピュータの新規脆弱性対策オプションサーバへの移行	157
組込みデータベースの最適化	158
Microsoft SQL Server Express の上限 : 4GB	158
ログのアーカイブ	158
データベースで使用するスペースを最小化する	158
脆弱性対策オプションデータベースの容量の縮小	159
脆弱性対策オプションデータの別のデータベースへの移行	160
脆弱性対策オプションのバックアップおよび復元	161
バックアップ	162
復元	162
バックアップおよび復元のオプションを変更する	163
バックアップ	163
IDFBackup.bat を使用してスケジュールバックアップを設定する	163
復元	164
サーバプラグインのアップグレード	164
第 12 章 システム	165
システムについて	166
システムイベントの表示	166
リストのフィルタリングおよびイベントの検索	167
イベントをエクスポートする	168
イベントのタグ付け	168
イベントにタグを付ける	169

システム設定	170
コンピュータ	171
ファイアウォールと DPI の設定	175
インタフェースの分離設定	181
コンテキスト設定	182
攻撃の予兆設定	183
検索設定	185
通知設定	185
ランク付け設定	186
アップデート	187
システム	188
タグ	189
タスク	190
ライセンス	191
アップデート	191
セキュリティアップデート	192
セキュリティアップデートの適用	192
クライアントプラグインのアップデート	193
サーバ診断	194
第 13 章 ログ	195
ログについて	196
ログの設定	196
通知の設定	196
Syslog	197
SNMP	197
スクリプト	197

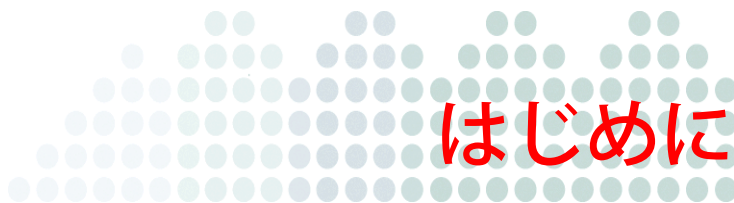
Syslog の統合の設定	197
Red Hat Enterprise で Syslog を設定する	198
脆弱性対策オプションサーバプラグインの設定	198
Syslog メッセージを解析する	199
ファイアウォールイベントログの形式	201
DPI イベントログの形式	205
システムイベントログの形式	211
詳細ログポリシーモード	213
第 14 章 サポート情報.....	217
製品サポート情報	217
サポートサービスについて	218
製品 Q&A のご案内	218
セキュリティ情報	219
トレンドマイクロ「セキュリティ情報」	219
トレンドマイクロへのウイルス解析依頼	219
ウイルス解析サポートセンター「TrendLabs」	220
付録 A 脆弱性対策オプションが使用するポート	221
ポート : 4118	221
ポート : 4119 (初期設定)	221
ポート : 4120 (初期設定)	222
ポート : 514 (初期設定)	222
ポート : 25 (初期設定)	222
ポート : 80	223
ポート : ランダムに選択	223

付録 B コンピュータとクライアントプラグインのステータス.....	225
コンピュータの状態	226
クライアントプラグインの状態	228
コンピュータエラー	229
付録 C イベント	231
ファイアウォールイベント	232
DPI イベント	234
システムイベント	238
クライアントプラグインイベント	253
索引	261

表のリスト

表 1. 本書で使用している表記規則	3
表 9-1. XML での記法	124
表 9-2. パターン	129
表 9-3. 予約語	130
表 9-4. 仮想レジスタ	131
表 9-5. 等式	134
表 9-6. 符号付き比較	134
表 9-7. 符号なし比較	134
表 9-8. Modulo32 比較	135
表 9-9. 基本演算命令	135
表 9-10. ビット単位命令	136
表 12-1. クライアントプラグインの有効化に関するコマンドラインのオプション	173
表 13-1. 署名 ID	200
表 13-2. ファイアウォールイベント拡張フィールド	201
表 13-3. DPI イベントログの形式拡張	206
表 13-4. システムイベントログの形式拡張	211
表 13-5. 無視するイベント	213
表 B-1. コンピュータの状態	226
表 B-2. クライアントプラグインの状態	228
表 B-3. コンピュータエラー	229

表 C-1. ファイアウォールイベント.....	232
表 C-2. DPI イベント	234
表 C-3. システムイベント.....	238
表 C-4. クライアントプラグインイベント	253



はじめに

脆弱性対策オプション™ 管理者ガイドへようこそ。このガイドでは、クイックスタートのための情報、クライアントのインストール手順、および脆弱性対策オプションサーバとクライアントの管理について説明します。

この章で扱うトピックは次のとおりです。

- 2 ページの「ドキュメント」
- 3 ページの「ドキュメントの表記規則」
- 2 ページの「対象読者」

ドキュメント

本製品には、次のドキュメントが付属しています。

- Readme — 基本的なインストール方法と既知の制限事項に関する説明
- オンラインヘルプ — 各種作業を実行するための詳細な手順の説明
- インストールガイド — 製品の概要、インストール計画、インストール、設定、起動方法に関する説明
- 管理者ガイド — 製品の概要、インストール計画、インストール、設定、および製品環境を管理するために必要な詳細情報の説明

注意： 最新の情報については次の Web サイトを参照してください。
(http://www.trendmicro.co.jp/requirement/IDF1_5)

対象読者

脆弱性対策オプション™ 1.5 のドキュメントは、以下を含むセキュリティシステムについて基本的な知識があることを前提としています。

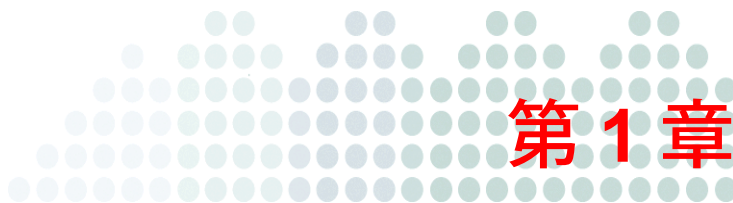
- ウイルス対策およびコンテンツセキュリティ保護
- ネットワークおよびサーバ管理
- ウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）の管理

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表記	説明
<u>注意:</u>	設定上の注意
<u>ヒント:</u>	推奨事項
<u>警告:</u>	避けるべき操作や設定についての注意

表 1. 本書で使用している表記規則



脆弱性対策オプションの導入

この章では、脆弱性対策オプション™ 1.5 を紹介し、本リリースの新機能について説明します。

この章で扱うトピックは次のとおりです。

- 6 ページの「脆弱性対策オプションについて」
- 6 ページの「本リリースの新機能」

脆弱性対策オプションについて

ウイルスバスター Corp. Web アプリケーションを含む、商用ソフトウェアおよびカスタムソフトウェアの脆弱性を悪用する攻撃に最強かつ最終的な防御を提供します。脆弱性対策オプションは、機密性の高いデータ、アプリケーション、コンピュータまたはネットワークのセグメントをプロアクティブに保護することで、包括的なセキュリティポリシーを構築および強化します。同システムは、脆弱性対策オプションサーバプラグイン™と複数の脆弱性対策オプションクライアントプラグイン™で構成されます。

本リリースの新機能

脆弱性対策オプション™ 1.5 には、次の新機能および拡張機能が含まれています。

パフォーマンスおよびスケーラビリティ

脆弱性対策オプション 1.5 では、セキュリティアップデート配信、ハートビート、推奨設定の検索、メモリの使用においてスピードと効率の大幅な向上、さらに脆弱性対策オプションサーバプラグインのユーザインタフェースの改善によって、パフォーマンスとスケーラビリティが全体的に向上しています。

新しく追加したコンピュータを自動で有効化/保護

タスクでは、条件に基づいて自動的にセキュリティプロファイルの有効化やコンピュータへの割り当てを行えるようになりました。対象となるコンピュータは次のとおりです。

- クライアントプラグインが開始した有効化で追加されたコンピュータ
- ウイルスバスター Corp. クライアントインベントリの同期時に追加されたコンピュータ

ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) の拡張サポート

脆弱性対策オプション 1.5 では、次のウイルスバスター Corp. の機能がサポートされます。

- ウイルスバスター Corp. 10.6 および PLM 2.0
- ウイルスバスター Corp. のダッシュボードウィジェット
- ウイルスバスター Corp. のマッシュアップウィジェット

イベントのタグ付け

イベントのタグ付けを使用すると、定義済みのラベルまたはカスタムラベルでイベントを手動でタグ付けできます。これにより、イベント、ダッシュボード、およびレポートを専用のビューで表示でき、単一のイベント、複数の類似イベント、または将来の類似イベントすべてに適用できます。

プラットフォームおよびファイルシステムの拡張サポート

脆弱性対策オプション 1.5 では、次のクライアントプラットフォームおよびサーバプラットフォームがサポートされます。

- 32 ビットおよび 64 ビットのクライアントとサーバ
- 32 ビットクライアントと 64 ビットクライアントの個別配信
- FAT32 ファイルシステム
- Microsoft SQL Server 2008

複数言語のサポート

脆弱性対策オプション 1.5 は複数の言語バージョンで利用可能です。利用可能な言語については、トレンドマイクロにお問い合わせください。



第2章

脆弱性対策オプションのクイックスタート

この章では、脆弱性対策オプション™ 1.5 サーバプラグインについて紹介し、サーバプラグインインタフェースの基本とサーバプラグインの画面の概要を説明します。脆弱性対策オプションのインストールと設定方法の説明については、「[脆弱性対策オプションインストールガイド](#)」を参照してください。

この章で扱うトピックは次のとおりです。

- 10 ページの「脆弱性対策オプションサーバプラグイン」
- 10 ページの「脆弱性対策オプションクライアントプラグイン」
- 11 ページの「脆弱性対策オプションサーバプラグインのインタフェースを開く」
- 12 ページの「サーバプラグインのインタフェース」
- 16 ページの「プログラムの概要」

脆弱性対策オプションサーバプラグイン

脆弱性対策オプションサーバプラグインは、すべてのクライアントコンピュータを管理するアプリケーションです。サーバでは、次の2つの重要な機能を実行します。

- クライアントをインストール、監視、管理する。
- クライアントに必要なコンポーネントをダウンロードする。サーバは、コンポーネントをトレンドマイクロのアップデートサーバからダウンロードし、クライアントに配布します。

脆弱性対策オプションサーバプラグインで、サーバとクライアント間のリアルタイムで双方向の通信を実現できます。脆弱性対策オプションサーバプラグインは、ウイルスバスター Corp. のプラグインとして動作し、クライアントを仮想的にネットワーク上からアクセスできる、ブラウザベースのウイルスバスター Corp. Web コンソールから管理できます。サーバはクライアントと（また、クライアントはサーバと）ハイパーテキスト転送プロトコル (HTTP) 経由で通信します。

脆弱性対策オプションクライアントプラグイン

各コンピュータに脆弱性対策オプションクライアントプラグインをインストールすることで、コンピュータをセキュリティリスクから保護します。クライアントはポート検索と推奨設定の検索を実行できます。

脆弱性対策オプションサーバプラグインのインタフェースを開く

脆弱性対策オプションプラグインのインタフェースは、インターネット防御ファイアウォールの中心部です。脆弱性対策オプションプラグインのインタフェースは、ウイルスバスター Corp. Web コンソールのプラグインとして起動します。ウイルスバスター Corp. Web コンソールにログインすると、脆弱性対策オプションサーバプラグインにアクセスできます。

脆弱性対策オプションサーバプラグインを起動するには

1. ウイルスバスター Corp. Web コンソールを開きます。
2. ナビゲーション画面で、「プラグインマネージャ」をクリックします。
3. 「脆弱性対策オプション」セクションで、「プログラムの管理」をクリックします。
「脆弱性対策オプション - はじめに」画面が表示されます。
4. これ以降、「はじめに」画面を表示せずに脆弱性対策オプションを起動するには、「**次回脆弱性対策オプションにアクセスする際に、このメッセージを表示しない**」を選択します。
5. 「脆弱性対策オプション - はじめに」画面で、「**続行**」をクリックします。
ダッシュボードが開いた状態の脆弱性対策オプションインタフェースが表示されます。

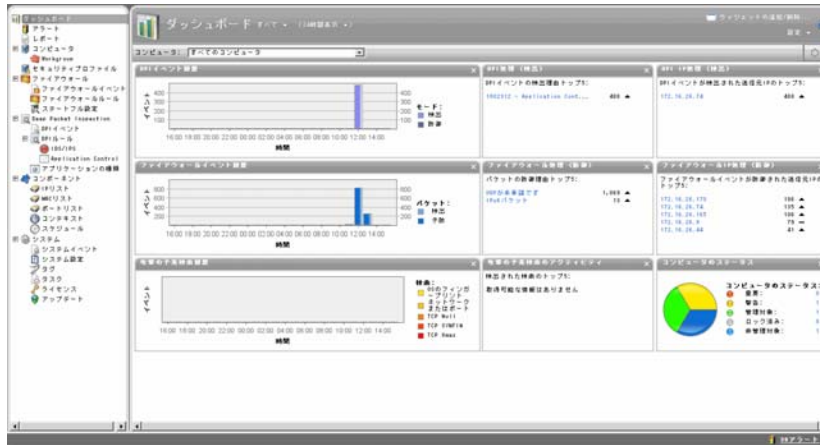


図 2-1. 脆弱性対策オプションダッシュボード

サーバプラグインのインタフェース

脆弱性対策オプションサーバプラグインの Web ベースのユーザインタフェースは、脆弱性対策オプションシステムの全エレメントへ簡単にアクセスできるように設計されています。主な機能は、次のとおりです。

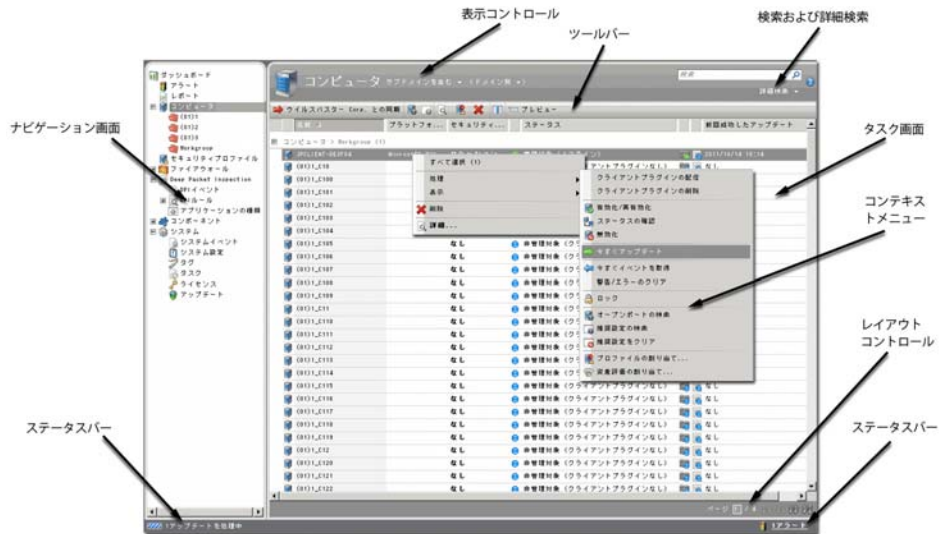


図 2-2. 脆弱性対策オプションのユーザインタフェース

ナビゲーション画面

ナビゲーション画面には、ツリーベースのナビゲーションシステムが組み込まれています。脆弱性対策オプションシステムのエレメントは、次のように構成されています。

- **ダッシュボード**: 脆弱性対策オプションシステムのステータスを一目で理解できる概要表示
- **アラート**: システムイベントまたはセキュリティイベントに関する現在の重大アラートと警告アラートの概要
- **レポート**: システムステータスの概要およびアクティビティの概要のレポート生成
- **コンピュータ**: ネットワーク上にあるコンピュータとそのステータス情報のリスト
- **セキュリティプロファイル**: 定義済みのセキュリティプロファイルのリスト

- **ファイアウォール**
 - **ファイアウォールイベント**: セキュリティ関連のファイアウォールアクティビティのログ
 - **ファイアウォールルール**: ファイアウォールルールを定義および管理する場所
 - **ステートフル設定**: ステートフル設定を定義および管理する場所
- **Deep Packet Inspection**
 - **DPI イベント**: セキュリティ関連の DPI アクティビティのログ
 - **DPI ルール**: DPI ルールを定義および管理する場所
 - **アプリケーションの種類**: アプリケーションの種類は、接続の方向、プロトコル、およびポートで定義されます。DPI ルールが動作するトラフィックを定義します。
- **コンポーネント**: 脆弱性対策オプションシステムの各種エレメントによって使用される共通コンポーネントのリスト
- **システム**: 脆弱性対策オプションシステムの処理を管理し、記録を表示してシステムイベントをレポートするための管理ツールを検索できる場所

タスク画面

ナビゲーション画面のエレメントをクリックすると、タスク画面にエレメントの画面が表示されます。ほとんどすべての作業は、タスク画面上で実行されます。アイテムのリストが表示されているタスク画面では、ツールバー (🔧) の「列の追加 / 削除」ボタンをクリックして列を追加または削除できます。列の表示順序は、列を表示する位置にドラッグして変更できます。一覧表示されたアイテムは、列の内容でソートおよび検索できます。

レイアウトコントロール

タスク画面に表示されるリストの中には、1 画面で表示可能な数より多くのエレメントを含んでいるものがあります。この場合、レイアウト情報で、表示しているアイテムのサブセットが表示されます。レイアウトツールを使用して、リストのページ間を移動するか、アイテム番号をテキストボックスに入力してリスト表示の開始点にします。ページごとに表示するアイテム数は、「システム」セクションで設定できます。

表示コントロール

該当する場合は、表示コントロールを使用して、一覧表示されたアイテムを表示するためのオプションを選択できます。たとえば、ナビゲーション画面のコンピュータドメインをクリックすると、そのドメインに所属するコンピュータがタスク画面に一覧表示されます。表示管理では、そのドメインのコンピュータのみを表示するか、そのドメインのコンピュータとサブドメインのコンピュータすべてを表示するかを選択できます。該当する場合は、表示コントロールを使用して一覧表示されたアイテムをカテゴリに整理できます。たとえば、一覧表示されたコンピュータを、割り当てられたセキュリティプロファイルごとに分けるなどです。

ツールバー

ツールバーには、作業している画面で各種処理を実行する固有のボタンがあります。通常、こうしたボタンを使用して、リストアイテムを削除、変更、および作成します。ツールバーのオプションの多くは、コンテキストメニューからも使用できます。サーバプラグインでは、検索を保存して再利用できます。これにより、再利用可能なフィルタを効率的に作成して、一覧表示されたアイテムへ適用できます。

検索および詳細検索

最も簡単な検索方法は、「簡易」検索バーを使用することです。

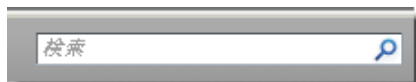


図 2-3. 簡易検索バー

この検索バーでは、「ファイアウォール」画面のファイアウォールイベントや「システムイベント」画面のシステムイベントなど、一覧表示されたアイテムの一致についてデータベースを検索します。

注意： 表示中のアイテムだけでなく、すべてのアイテムが検索されます。たとえば、全コンピュータで過去 7 日間のファイアウォールイベントを表示している場合、「ファイアウォールイベント」画面には「55,056 アイテム中、最新のアイテム 1,000 のみが含まれています。日付範囲を絞り込むか、検索条件を追加することを検討してください。」と表示されます。表示できるのが 1,000 アイテムのみであったとしても、55,056 アイテムすべてが検索されるということです。検索エンジンは、データベース内の日付以外の各フィールドを検索します。

高度な検索を行うには、「詳細検索」をクリックして「詳細検索を開く」をクリックしてください。



図 2-4. 詳細検索

「期間」 ツールバーを使用してリストをフィルタし、特定の期間内に発生したイベントだけを表示できます。

「コンピュータ」 ツールバーを使用すると、ドメイン別またはコンピュータセキュリティプロファイル別にイベントログエントリの表示を整理できます。

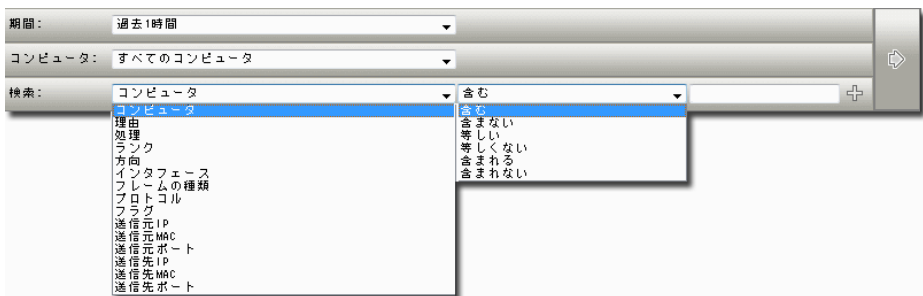


図 2-5. 「コンピュータ」 ツールバー

検索機能 (大文字 / 小文字の区別なし):

- ・ **含む**: 選択した列の入力内容に検索文字列が含まれる
- ・ **含まない**: 選択した列の入力内容に検索文字列が含まれない
- ・ **等しい**: 選択した列の入力内容と検索文字列が完全に一致する
- ・ **等しくない**: 選択した列の入力内容が検索文字列と完全には一致しない
- ・ **含まれる**: 選択した列の入力内容がカンマ区切りで入力された検索文字列 1 つと完全に一致する
- ・ **含まれない**: 選択した列の入力内容がカンマ区切りで入力されたどの検索文字列とも完全には一致しない

検索バーの右側にある「プラス」ボタン (+) をクリックすると、追加の検索バーが表示され、検索に複数のパラメータを適用できます。準備が整ったら、送信ボタンをクリックします (ツールバーの右側にある上部に右矢印の付いたボタン)。

ステータスバー

ステータスバーは、脆弱性対策オプションシステムの現在の状態に関する情報を表示します。ステータスバーの右端には、有効になっているアラートがある場合、その数が表示されます。ステータスバーの左端には、コンピュータ検出、ポート検索操作、クライアントプラグインの有効化、クライアントプラグインのアップデートまたはアップグレードなど、現在進行中の処理が表示されます。

コンテキストメニュー

脆弱性対策オプションサーバプラグインの画面の多くには、状況に応じたメニューがあります。たとえば、セキュリティプロファイルを右クリックすると、その画面のツールバーの多くのオプションにすばやくアクセスできるコンテキストメニューが表示されます。コンピュータドメインを右クリックすると、現在のドメインを管理したり新しく作成したりするためのオプションを含むコンテキストメニューが表示されます。

注意： UIの多くのエレメントでは、マウスのポインタを重ねると有用なヒントを表示します。

プログラムの概要

サーバプラグインでは、脆弱性対策オプション用に次の画面が用意されています。

- ダッシュボード
- アラート
- レポート
- コンピュータ
- セキュリティプロファイル
- ファイアウォール
- Deep Packet Inspection
- コンポーネント
- システム

アラート

アラート画面では、アラートを表示したり設定できます。処理が必要な可能性がある重要なイベントが発生したときに、アラートを通知します。次の図は「アラート」画面です。

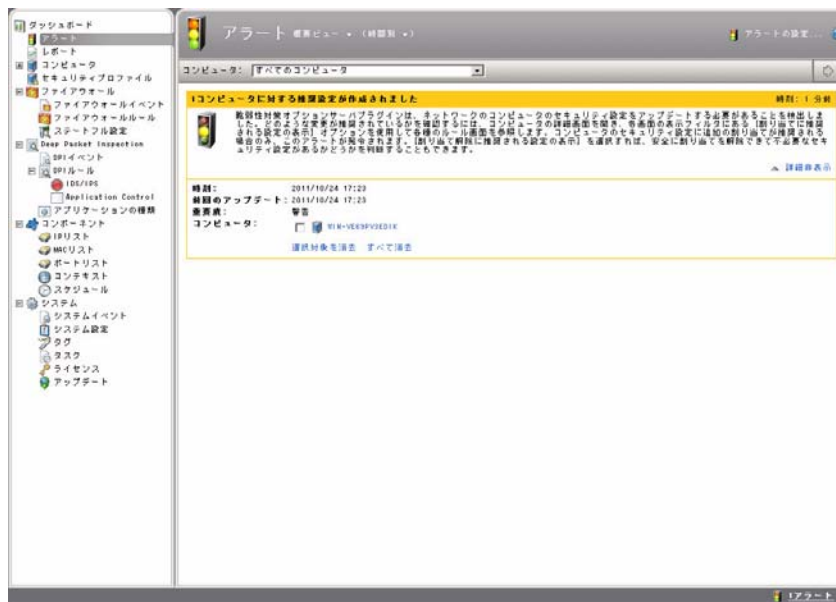


図 2-7. 「アラート」画面

「アラート」画面の詳細については、「33 ページの「アラート」」を参照してください。

レポート

「レポート」画面ではレポートを生成できます。次の図は「レポート」画面です。

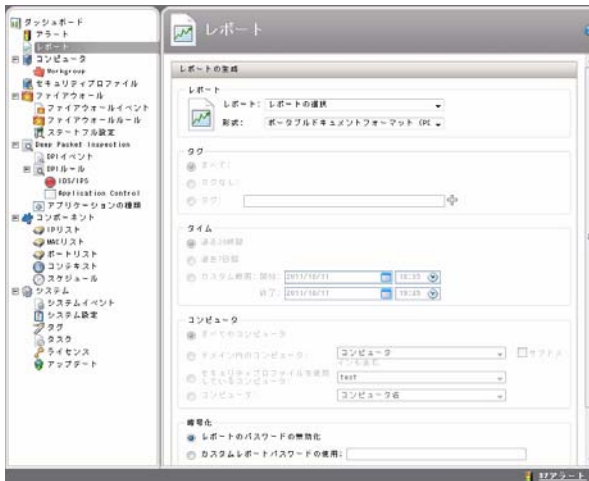


図 2-8. 「レポート」画面

レポート生成の詳細については、「37 ページの「レポート」」を参照してください。

コンピュータ

「コンピュータ」画面を使用して、ネットワーク上のコンピュータを管理および監視できます。次の図は「コンピュータ」画面です。

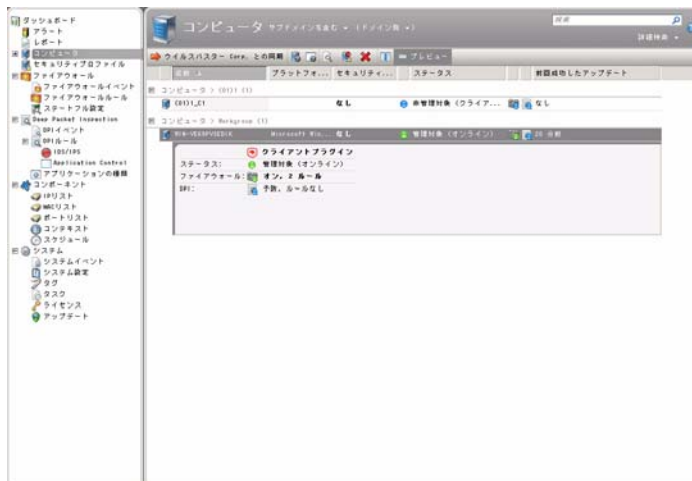


図 2-9. 「コンピュータ」画面

コンピュータの管理方法の詳細については、「41 ページの「コンピュータを管理する」を参照してください。

セキュリティプロファイル

セキュリティプロファイルを使用すると、ファイアウォールルール、ステートフル設定、および DPI ルールの共通の設定を、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。次の図は「セキュリティプロファイル」画面です。

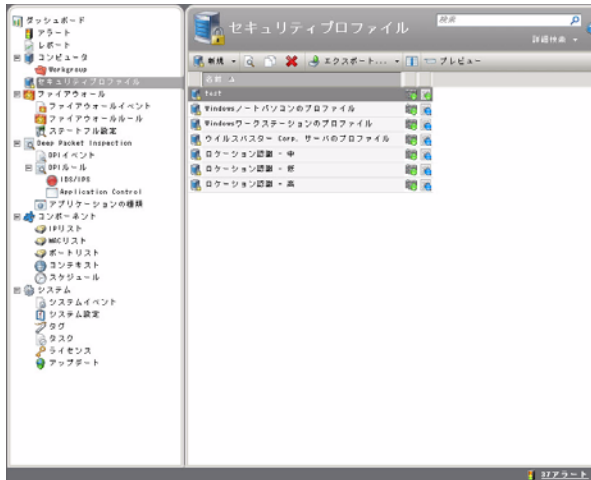


図 2-10. 「セキュリティプロファイル」画面

セキュリティプロファイルの詳細については、「75 ページの「セキュリティプロファイル」」を参照してください。

Deep Packet Inspection

「Deep Packet Inspection」画面で、DPI イベントの監視や DPI ルールの設定ができます。次の図は「DPI ルール」画面です。

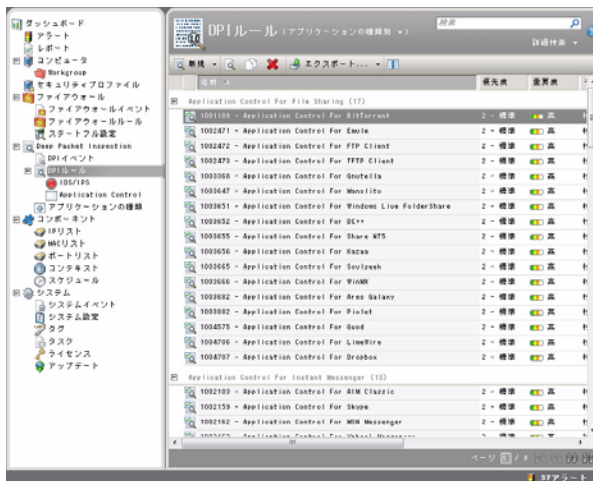


図 2-12. 「Deep Packet Inspection」の「DPI ルール」画面

Deep Packet Inspection の管理の詳細については、「111 ページの「Deep Packet Inspection を使用する」を参照してください。

コンポーネント

「コンポーネント」画面では、IP リスト、MAC リスト、ポートリスト、コンテキスト、スケジュールの管理ができます。次の図はコンポーネントの「ポートリスト」画面です。

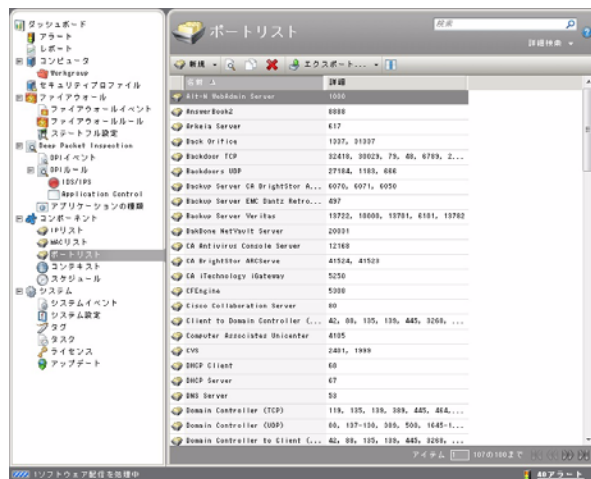


図 2-13. 「コンポーネント」の「ポートリスト」画面

コンポーネントの管理の詳細については、「141 ページの「コンポーネント」」を参照してください。

システム

「システム」画面では、システムイベントの監視、システム設定、イベントタグの定義、タスクの定義、ライセンスとアップデートの管理などのシステムタスクの管理ができます。次の図は「システムイベント」画面です。

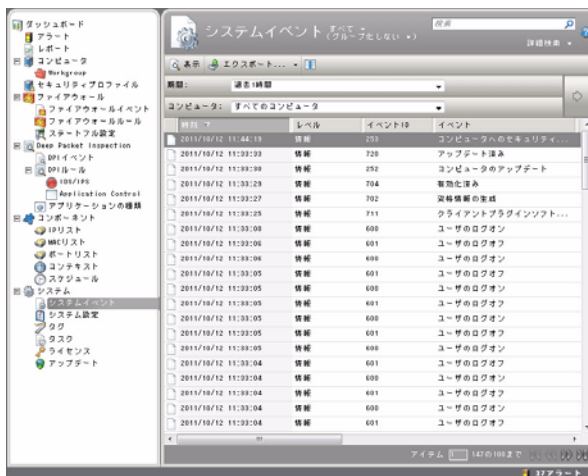


図 2-14. 「システムイベント」画面

詳細については、「165 ページの「システム」」を参照してください。



第3章

ダッシュボード

この章では、脆弱性対策オプション™ 1.5 ダッシュボードの使用方法について説明します。

この章で扱うトピックは次のとおりです。

- 28 ページの「ダッシュボードについて」
- 29 ページの「ダッシュボードをカスタマイズする」
- 31 ページの「ダッシュボードの設定を管理する」
- 32 ページの「保存したダッシュボードの設定を開く」

ダッシュボードについて

ダッシュボードは、脆弱性対策オプションサーバプラグインにログインして表示される最初の画面です。ダッシュボードには、設定可能な「ウィジェット」と呼ばれるいくつかの情報画面が表示され、脆弱性対策オプションの状態を一目で理解できるビューが備えられています。ウィジェットにはアラート履歴とステータス、コンピュータステータス、ファイアウォール処理、DPI アクティビティ、攻撃の予兆検索履歴、およびシステムイベント履歴などの情報が表示されます。脆弱性対策オプションサーバプラグインにログインすると、前回のセッションのダッシュボードのレイアウトが保持されています。

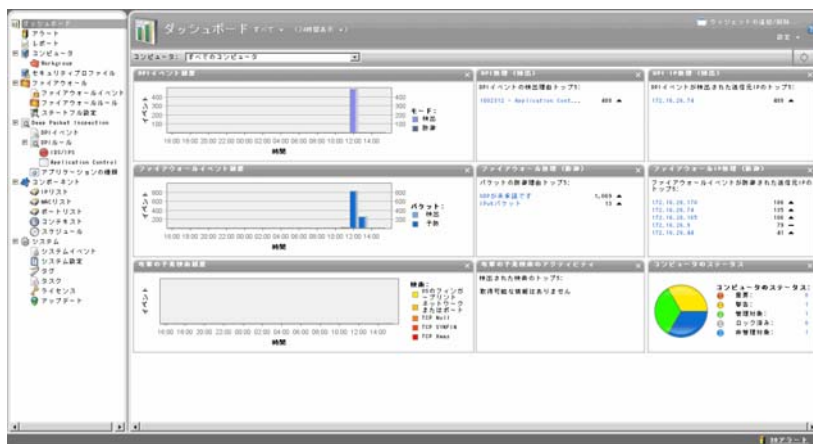


図 3-1. ダッシュボード

ダッシュボードを開くには、メインメニューから「ダッシュボード」を選択します。

ウィジェットについて

多くのウィジェットには、データを絞り込むためのリンクが含まれています。たとえば、DPI 履歴グラフの列をクリックすると「DPI イベント」画面が表示され、その日に発生した DPI イベントすべてを確認できます。

注意： ウィジェットの数値の横に推移を表すインジケータがあります。上向きまたは下向きの三角形は、直前の期間と比較した増加または減少をそれぞれ示し、横線は変化がないことを示しています。

ダッシュボードをカスタマイズする

ダッシュボードの機能を設定したりカスタマイズしたりできます。またレイアウトを保存してログイン時に表示することもできます (ダッシュボードは、前回ログアウトしたときそのまま表示されます)。

ダッシュボードの表示で設定可能な要素はタグで、取得するデータの期間、データを表示するコンピュータまたはコンピュータグループ、表示する「ウィジェット」、およびそのウィジェットの画面上的レイアウトです。

ウィジェットレイアウトを設定する

ウィジェットは、タイトルバーで選択し、新しい位置にドラッグアンドドロップすることで画面上で整理できます。既存のウィジェットの上を選択したウィジェットを移動すると、それぞれのウィジェットの場所が交換されます。(表示しようとしているウィジェットは、一時的にグレー表示になります。) 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ができます。

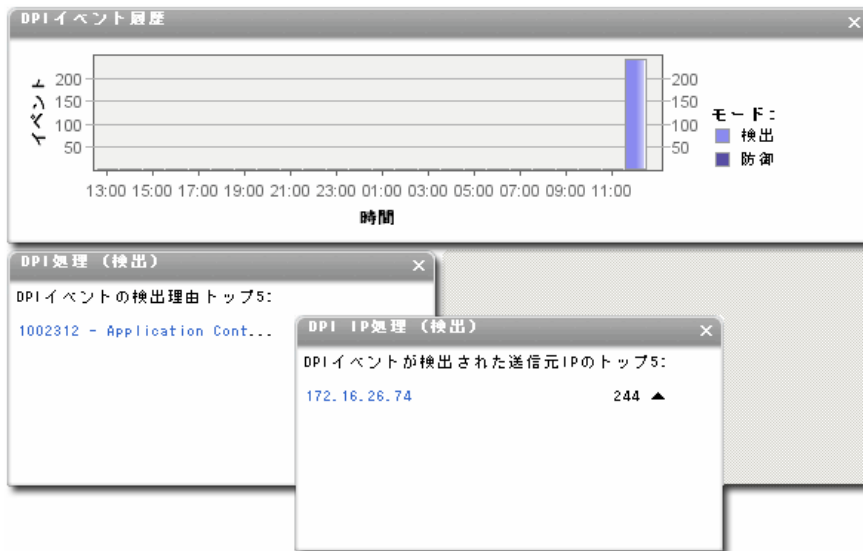


図 3-2. ウィジェットレイアウトを変更する

ダッシュボードウィジェットを追加したり削除する

ダッシュボードの右上にある「ウィジェットの追加 / 削除...」をクリックして「ウィジェットの追加 / 削除」ウィンドウを開き、使用できるウィジェットのリストを表示して、どのウィジェットを表示するかを選択します。

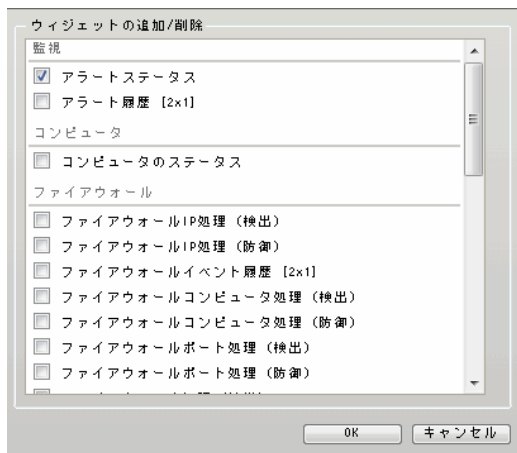


図 3-3. ダッシュボードウィジェットを追加したり削除する

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

情報をタグでフィルタする

ダッシュボードで、1つ以上のタグで情報をフィルタしたり、すべての情報やタグが付いていない情報を表示したりできます。これらのビューを切り替えるには、画面上部のドロップダウンメニューを使用します。



図 3-4. タグで表示する

タグでフィルタするには、タグ名を「タグ」ボックスに入力します。*を使用して任意の文字列を、?で任意の文字を示します。フィルタを削除するには、「すべて」または「タグなし」を選択します。

日時の範囲で情報をフィルタする

ダッシュボードは、過去 24 時間または 7 日間のデータを表示します。これらの 2 つのビューを切り替えるには、画面上部のドロップダウンメニューを使用します。



図 3-5. 日時の範囲

コンピュータおよびコンピュータドメインでフィルタする

コンピュータを使用する：ドロップダウンメニューを使用して、特定のコンピュータからのデータのみが表示されるように表示データをフィルタします。



図 3-6. コンピュータおよびコンピュータドメイン

ダッシュボードの設定を管理する

ダッシュボードの右上にある「設定」メニューを使用して、個々のダッシュボードの設定を保存、ロード、および削除できます。

ダッシュボードの設定を保存するには

パス: [メインメニュー](#) | 「[ダッシュボード](#)」

1. ウィジェットを追加、削除、位置の調整をし、必要に応じてフィルタを設定します。
2. ダッシュボードの右上にある「設定」メニューをクリックして「設定の保存 ...」を選択します。
3. 「名前」ボックスに名前を入力して「OK」をクリックします。

ダッシュボードの設定を削除するには

パス: [メインメニュー](#) | 「[ダッシュボード](#)」

- ダッシュボードの右上にある「設定」メニューをクリックして設定名の隣にある「X」をクリックします。

保存したダッシュボードの設定を開く

保存した設定を開くには、「設定」をクリックしてドロップダウンメニューから設定を選択します。

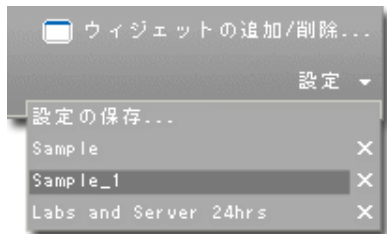


図 3-7. 保存したダッシュボードの設定を開く



第4章

アラート

この章では、脆弱性対策オプション™ 1.5 アラートを使用してイベントを監視する方法を説明します。

この章で扱うトピックは次のとおりです。

- 34 ページの「アラートについて」
- 34 ページの「アラートを表示する」
- 35 ページの「アラートを設定する」
- 36 ページの「アラートメールを設定する」

アラートについて

侵入防止ファイアウォールシステムでアラートをトリガする条件は 60 種類以上あります。通常、アラートは、コンピュータがオフラインになった、DPI ルールが期限切れになったなどのシステムステータスの異常を警告するために存在しますが、フィンガープリント検索やその他のセキュリティ関連イベントの検出を通知するアラートもあります。(個々の DPI イベントおよびファイアウォールイベントに関する通知については、Syslog サーバの設定を検討してください。)

アラートを表示する

「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、同様の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々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。



図 4-1. アラート

概要ビューで、「詳細の表示」をクリックしてアラートパネルを拡大すると、その特定のアラートを生成したコンピュータがすべて表示されます (コンピュータをクリックすると、コンピュータの「詳細」画面が表示されます)。

概要ビューでは、コンピュータのリストが 5 項目を超える場合、5 つ目のコンピュータの後ろには省略記号 (「...」) が現れます。省略記号をクリックすると、リスト全体が表示されます。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、「**消去**」リンクをクリックすることで、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。)

アラートには、システムおよびセキュリティの 2 つのタイプがあります。システムアラートは、クライアントプラグイン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でトリガされ、セキュリティアラートは、DPI ルールやファイアウォール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。

注意：「コンピュータ」フィルタバーを使用して、特定のコンピュータドメイン内のコンピュータや、特定のセキュリティプロファイルを保持するコンピュータなど、特定のコンピュータに関連するアラートだけを表示できます。

アラートを設定する

アラートのオン/オフを切り替えたり、重大度を警告または重大に設定したり、アラートが発生したときに次のいずれの処理が行われるようにするかを設定したりできます。

- このアラートが発生したら、通知メールを送信します。
- このアラートのアイテム数などの条件が変更されたら、通知メールを送信します。
- このアラートが存在しなくなったら通知メールを送信します。

アラートを設定するには

パス：侵入防止ファイアウォールのメインメニュー | 「アラート」

パス：脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」 → 「システム」

1. 「アラート」画面右上にある「アラートの設定 ...」をクリックするか、または「システム」画面で「アラート設定の表示 ...」をクリックします。

「アラート設定」ウィンドウが開き、重大度とオン/オフ情報の入ったアラートのリストが表示されます。

2. リストにフィルタをかけるには、画面の上端にあるドロップダウンリストから「重要度別」または「グループ化しない」を選択します。
3. アラート情報を表示して各アラートに関連する処理を編集するには、アラートを右クリックし、「プロパティ ...」を選択して「プロパティ」ウィンドウを開きます。

アラートはオンとオフを切り替えたり、重要度の警告と重大を切り替えられます。

注意： アラートにセキュリティプロファイルやコンピュータごとに異なる設定を行うことはできません。1つのアラートに関するプロパティに加えた設定変更は、すべて全体に適用されます。

すべてのメールアラートの送信先となる初期設定のメールアドレスを指定できます。アラートメールを設定する方法については、次のセクション「アラートメールを設定する」を参照してください。

アラートメールを設定する

選択されているアラートがトリガされたときに、脆弱性対策オプションサーバプラグインによってメールを送信することができます。このメールシステムを有効にするには、サーバプラグインにSMTP メールサーバへのアクセス権を与える必要があります。SMTP 設定を行い、メールをトリガするアラートを選択します。アラートをトリガさせる条件の数は 30 を超えますが、そのすべてでメール送信をトリガしない設定にすることもできます。

SMTP 設定を設定するには

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」 → 「システム」

1. 「SMTP」エリアで、SMTP メールアドレスを入力します (必要に応じてポートも入力します)。
2. メールの送信元とする「送信元」メールアドレスを入力します。オプションで、アラートメールを送信できなかった場合の配信不能通知の送信先とする「バウンス」メールアドレスを入力します。
3. SMTP メールサーバで送信認証が必要な場合は、ユーザ名とパスワードの資格情報を入力します。必要な情報を入力したら、「SMTP 設定のテスト」を使用して設定をテストします。

どのアラートによりメールが送信されるようにするかをトリガするには

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

4. 「システム」タブをクリックし、「アラート設定の表示 ...」をクリックして、すべてのアラートの入ったリストを表示します。
「オン」列に表示されるチェックマークは、アラートがオンになっているかどうかを示します。アラートがオンの場合、該当する状況になった場合にそのアラートがトリガされますが、メールが送信されるというわけではありません。
5. アラートをダブルクリックしてその「アラート設定」画面を表示するか、またはアラートを右クリックしてポップアップメニューから「プロパティ ...」を選択します。
6. アラートによってメールがトリガされるようにするには、「オン」を選択し、少なくとも 1 つの「メールを送信」チェックボックスをオンにします。



第5章

レポート

この章では、脆弱性対策オプション™ 1.5 レポートを設定および生成する方法について説明します。

この章で扱うトピックは次のとおりです。

- 38 ページの「レポートについて」
- 38 ページの「レポートの生成」

レポートについて

「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、コンピュータドメイン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。利用可能なレポートの種類は次のとおりです。

- アラートレポート
- 攻撃レポート
- ファイアウォールレポート
- コンピュータフォレンジックス監査レポート
- コンピュータレポート
- DPI レポート
- 推奨設定レポート
- 概要レポート
- 不審なアプリケーション活動レポート
- システムイベントレポート

レポートの生成

「レポート」では、PDF または RTF の形式でレポートを生成できます。レポートの種類を選択し、タグ別、期間別、セキュリティプロファイル別、およびコンピュータ別に、含める情報をフィルタできます。レポートを保護するパスワードを選択できます。

レポートを生成する方法は、次のとおりです。

パス : 脆弱性対策オプションメインメニュー | 「レポート」

1. 「レポート」エリアで、生成するレポートの種類と形式を選択します。レポートは、PDF または RTF の形式で出力することができます。
2. 「タグ」エリアで、レポートに対するタグを定義します。
イベントデータを含むレポートを選択する場合、イベントタグでレポートをフィルタするオプションを使用できます。「すべて」はすべてのイベント、「タグなし」はタグ付けされていないイベントのみ、また、「タグ」を選択して 1 つ以上のタグを指定すると、指定したタグを含むイベントのみをレポートに含めることができます。

-
3. 「タイム」エリアで、時間のフィルタを設定して、ログの記録期間を任意で設定できます。これは、セキュリティ監査に役立ちます。

注意： レポートには、カウンタに保存されたデータが使用されます。カウンタは、イベントから定期的集計されたデータです。カウンタのデータは、最新の3日間は時間単位で集計されます。3日より古いデータは日単位で集計されてカウンタに保存されます。そのため、レポートでカバーされる期間は、最新の3日に関しては時間単位で指定できますが、3日より前になると日単位のみ指定可能になります。

4. 「コンピュータ」エリアで、データをレポートに含めるコンピュータを設定します。
5. 「暗号化」エリアで、パスワード保護を設定します。

注意： 脆弱性対策オプションサーバプラグインに含まれている元のレポートでは要件を満たさない場合、独自に設計したカスタムレポートを作成することもできます。



第6章

コンピュータを管理する

この章では、脆弱性対策オプション™ 1.5 コンピュータと脆弱性対策オプションクライアントプラグインの管理方法について説明します。

この章で扱うトピックは次のとおりです。

- 42 ページの「コンピュータについて」
- 42 ページの「コンピュータ情報を表示する」
- 45 ページの「開いているポートがあるコンピュータを検索する」
- 46 ページの「推奨設定についてコンピュータを検索する」
- 50 ページの「コンピュータにセキュリティプロファイルを割り当てる」
- 51 ページの「クライアントプラグインを管理する」
- 58 ページの「コンピュータのイベントを表示する」
- 60 ページの「コンピュータをロックまたはロック解除する」
- 60 ページの「コンピュータ資産評価を割り当てる」
- 61 ページの「コンピュータの詳細を表示および編集する」
- 69 ページの「継承および優先」

コンピュータについて

脆弱性対策オプションでは、ネットワークのコンピュータの監視、各コンピュータのクライアントプラグインの管理、ポートスキャンと推奨設定の検索の実施、セキュリティプロファイルの割り当て、コンピュータのイベントの表示を行います。

コンピュータ情報を表示する

「コンピュータ」画面で、ネットワーク上のコンピュータの管理や監視ができ、各コンピュータのプラットフォーム、セキュリティプロファイル、ステータス、前回成功したアップデートなどの情報と共に管理しているコンピュータが表示されます。

「コンピュータ」画面を開くには、メインメニューの「コンピュータ」をクリックします。

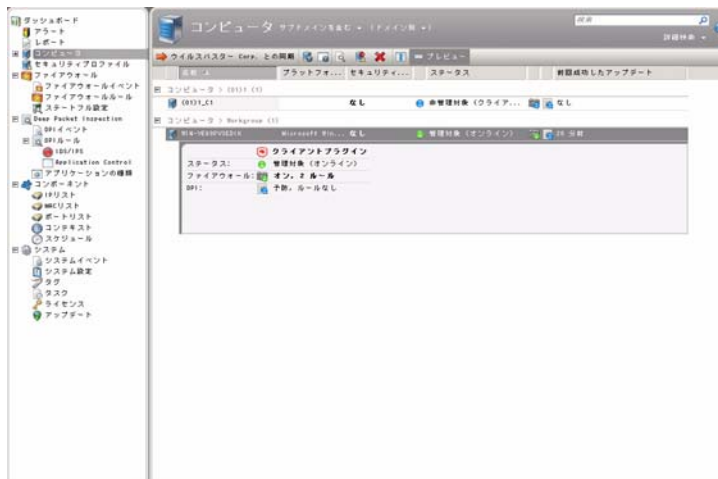


図 6-1. 「コンピュータ」画面

この画面は、定期的に自動でアップデートされます。情報列を追加または削除するには、ツールバーの「列の追加 / 削除」ボタンをクリックし、含める列を「列の追加 / 削除」ポップアップウィンドウから選択します。

コンピュータのプレビューを表示する

プレビューは、一覧表示されたコンピュータの下の表示領域に展開されます。プレビュー画面には、クライアントプラグインの有無とその状態、さらにファイアウォールモジュールと DPI モジュールに関する詳細が表示されます。

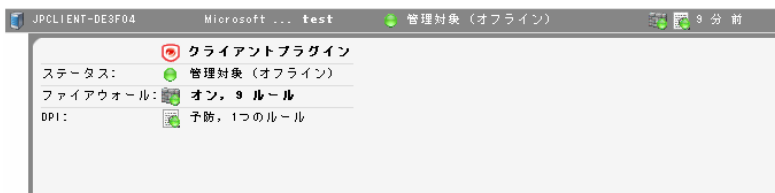


図 6-2. コンピュータのプレビュー画面

コンピュータのプレビューを表示するには：

パス: メインメニュー | 「コンピュータ」

1. ツールバーの「プレビュー」をクリックします。
2. プレビューするコンピュータを選択します。「プレビュー」オプションは、「プレビュー」ボタンを再度クリックするまで有効のままです。

コンピュータのステータスを確認する

このコマンドは、検索や有効化を実行せず、コンピュータのステータスを確認するだけです。コンピュータのステータスについての情報の詳細については、「225 ページの「コンピュータとクライアントプラグインのステータス」」を参照してください。

ステータスを確認するには

パス: メインメニュー | 「コンピュータ」

1. ステータスを確認するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」 > 「ステータスの確認」を選択します。

コンピュータを検索する

「検索」テキストボックスで、コンピューター一覧から特定のコンピュータを検索します。より高度な検索オプションについては、その下にある「詳細検索」オプションを使用してください。

詳細検索機能 (大文字 / 小文字の区別なし):

- **含む**: 選択した列の入力内容に検索文字列が含まれる
- **含まない**: 選択した列の入力内容に検索文字列が含まれない
- **等しい**: 選択した列の入力内容と検索文字列が完全に一致する
- **等しくない**: 選択した列の入力内容が検索文字列と完全には一致しない
- **含まれる**: 選択した列の入力内容がカンマ区切りで入力された検索文字列 1 つと完全に一致する
- **含まれない**: 選択した列の入力内容がカンマ区切りで入力されたどの検索文字列とも完全には一致しない

コンピュータの一覧をウイルスバスター Corp. と同期する

侵入防御のコンピューターリストは、サーバプラグインが起動されるたびにウイルスバスター Corp. と自動的に同期されますが、サーバプラグインの稼働中にコンピュータがウイルスバスター Corp. に追加された場合はアップデートされません。ツールバーの「**ウイルスバスター Corp. との同期**」ボタンを使用して、サーバプラグインの稼働中にウイルスバスター Corp. と同期させます。

注意: ウイルスバスター Corp. クライアントがコンピュータにインストールされる際、ウイルスバスター Corp. サーバによりコンピュータには一意の ID 番号が割り当てられます。この一意の ID 番号は、ウイルスバスター Corp. および脆弱性対策オプションが個々のコンピュータを追跡する際に使用します。ウイルスバスター Corp. クライアントがコンピュータからアンインストールされた後 (脆弱性対策オプションクライアントプラグインとともに) に再インストールされた場合、ウイルスバスター Corp. はコンピュータに新しい一意の ID を割り当てます。次にウイルスバスター Corp. と同期してコンピューターリストをアップデートする際、脆弱性対策オプションが新しい一意の番号を確認し、そのコンピュータを新規エントリとして扱います。コンピュータのホスト名は変更されないため、コンピュータの新しいリストには、ホスト名の末尾に「_1」(または「_2」、「_3」など) が付きます。これで同じコンピュータが「hostname」と「hostname_1」としてリストに 2 回表示されます。リストの最初の表示名「hostname」を削除し、2 番目の表示名「hostname_1」を保持します。(元の表示名「hostname」を削除した後に、表示名「hostname_1」を「hostname」に変更できます。)

開いているポートがあるコンピュータを検索する

ポートのスク্যানは、選択したすべてのコンピュータでポート検索を実行し、コンピュータにインストールされているクライアントプラグインを確認して、その状態が「クライアントプラグインの無効化が必要」、「クライアントプラグインの有効化が必要」、「クライアントプラグインの再有効化が必要」、または「オンライン」のいずれであるかを判別します（初期設定では、検索処理はポート 1～1024 を検索します。この範囲は、「検索」タブの「システム」→「システム設定」で変更できます）。

検索するポートの設定方法については、「145 ページの「ポート検索を設定する」」を参照してください。

注意： ポート範囲の設定に関係なく、ポート 4118 は常に検索されます。これは、サーバプラグインで開始された通信が送信されるコンピュータのポートです。コンピュータに対して通信方向が「クライアントプラグインによる開始」（「コンピュータの詳細」>「システム」>「システム設定」>「コンピュータ」>「通信方向」）に設定されると、ポート 4118 は閉じます。

コンピュータの一覧から開いているポートを検索するには

パス：メインメニュー | 「コンピュータ」

1. 検索するコンピュータを選択します。
2. ツールバーの「開いているポートの検索」をクリックするか、右クリックしてポップアップメニューから「処理」>「開いているポートの検索」を選択します。

コンピュータの「ファイアウォール」画面から開いているポートを検索するには

パス：メインメニュー | 「コンピュータ」

1. コンピュータを選択します。
2. 右クリックして、ポップアップメニューから「詳細...」を選択します。
3. ナビゲーション画面で、「ファイアウォール」をクリックします。
4. 「オープンポートの検索」ボタンをクリックします。

また、「予約タスク」を作成して、コンピュータのリストに対して定期的にポート検索を実行する方法もあります。

実行中のポート検索をキャンセルする

多数のコンピュータまたは広範囲のポートに対して一連のポート検索を開始し、検索に時間がかかりすぎる場合、このオプションを使用して、検索をキャンセルできます。

検索をキャンセルするには

パス: [メインメニュー](#) | 「[コンピュータ](#)」

1. 検索をキャンセルするコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「[処理](#)」 > 「[オープンポートの検索のキャンセル](#)」または「[推奨設定の検索のキャンセル](#)」を選択します。

推奨設定についてコンピュータを検索する

「推奨設定についてコンピュータを検索」を使用すると、脆弱性対策オプションサーバプラグインによって、コンピュータ上のセキュリティルールが検索され、検出結果に基づいた推奨設定が作成されます。推奨設定の検索の結果は、コンピュータのさまざまな「ルール」画面の「詳細」画面にも表示されます。詳細については、「61 ページの「[コンピュータの詳細を表示および編集する](#)」」を参照してください。

コンピュータで推奨設定の検索を実行するよう脆弱性対策オプションを設定すると、脆弱性対策オプションクライアントプラグインはコンピュータのレジストリ、実行中のプロセス、開いているポート、ファイルシステム、およびサービスの既知の脆弱性を検索します。クライアントプラグインは、OS だけでなくインストール済みアプリケーションも検索します。検出結果に基づいて、脆弱性対策オプションは DPI ルールを推奨します。

注意: 大規模な環境の場合、トレンドマイクロでは、セキュリティプロファイルレベルで推奨設定を管理することを推奨します。つまり、検索対象のすべてのコンピュータに、セキュリティプロファイルを割り当てておく必要があります。これにより、1つのソース (セキュリティプロファイル) からすべてのルールを割り当てることができます。各コンピュータで個々のルールを管理する必要はありません。

推奨設定の検索は手動で開始できます。または、特定のコンピュータで検索を定期的に行う予約タスクを作成することもできます。

推奨設定の検索を手動で行うには

パス: メインメニュー | 「コンピュータ」

1. 検索するコンピュータを選択します。
2. ツールバーの「推奨設定の検索」をクリックするか、右クリックしてポップアップメニューから「処理」>「オープンポートの検索」を選択します。

推奨設定の検索の予約タスクを作成するには

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「タスク」

1. ツールバーの「新規」をクリックして「新規予約タスク」を選択し、「新規予約タスク」ウィザードを表示します。
2. 「種類」メニューから「推奨設定についてコンピュータを検索」を選択し、検索の頻度を選択します。「次へ」をクリックします。
3. 次に表示される画面では、選択した内容に応じて、検索の頻度をより詳細に指定できます。該当する項目を選択し、「次へ」をクリックします。
4. 検索対象のコンピュータを選択し、「次へ」をクリックします。

注意: 通常、大規模な環境の場合は、セキュリティプロファイルを通じてすべての処理を実行することを推奨します。

5. 最後に、新しい予約タスクの名前を指定して、終了時にタスクを実行するかどうか (「完了」でタスクを実行) を選択し、「完了」をクリックします。

推奨設定の検索の結果を管理する

推奨設定の検索が完了したら、検索したコンピュータに割り当てられているセキュリティプロファイルを開きます。「Deep Packet Inspection」→「DPI ルール」に進みます。ルールを「アプリケーションの種類別」でソートし、フィルタの表示メニューから「割り当てに推奨される設定の表示」を選択します。

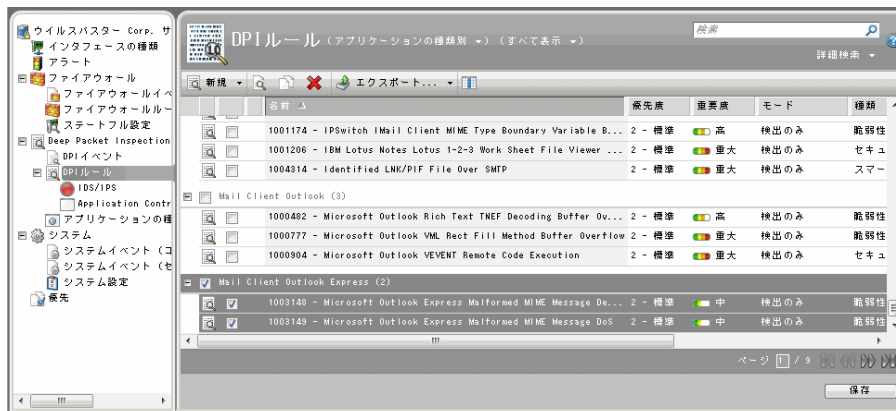


図 6-3. 推奨設定の検索の結果

セキュリティプロファイルに含まれるすべてのコンピュータに対する推奨設定がすべて一覧表示されます。

注意： 緑色のフラグには2つの種類があります。完全フラグ (■) と部分フラグ (■) です。推奨ルールには常に完全フラグが指定されます。アプリケーションの種類には、どちらかのフラグが指定されます。完全フラグの場合は、このアプリケーションの種類に属するすべてのルールの割り当てが推奨されていることを示します。部分フラグの場合は、このアプリケーションの種類に属する一部のルールのみが推奨されていることを示します。

また、上記のスクリーンショット内のヒントにも注目してください。ヒントには「このセキュリティプロファイルが割り当てられている 21 台のコンピュータの内の 3 台に対し、この DPI ルールの使用をお勧めします」といった内容が表示されています。トレンドマイクロでは、セキュリティプロファイルの対象となるすべてのコンピュータにすべての推奨ルールを割り当てることを推奨します。これにより、一部のルールが、それを必要としないコンピュータに割り当てられる可能性があります。しかし、パフォーマンスに最小限の影響が及ぶことよりも、セキュリティプロファイルを通じて行われる処理によって管理が簡単になるメリットの方が重要です。

推奨設定の検索では、DPI ルールの推奨設定が作成されます。

推奨設定の検索が実行されると、推奨設定の作成の対象となるすべてのコンピュータでアラートが生成されます。

注意： 推奨設定の検索の結果には、ルールの割り当てを解除する推奨設定を含めることもできます。この処理は、アプリケーションをアンインストールする場合、ベンダからのセキュリティパッチを適用する場合、または不要なルールが手動で適用されている場合に行うことができます。割り当ての解除が推奨されているルールを表示するには、フィルタの表示メニューから「割り当て解除に推奨される設定の表示」を選択します。

推奨ルールを設定する

適用前に設定が必要なルールもあります。たとえば、ある DPI ルールで、1 日に受信するメール数の最小しきい値と最大しきい値を設定する必要があるとします。この場合、推奨設定が作成されたコンピュータでアラートが生成されます。アラートのテキストには、ルールの設定に必要な情報が含まれます。

推奨設定をクリアする

このコンピュータの推奨設定の検索の結果として作成されたルールの推奨設定をクリアにします。また、推奨設定の検索によって生成されたアラートに一覧表示された中から該当するコンピュータを削除します。

注意： この処理では、過去の推奨設定によって割り当てられたルールの割り当ては解除されません。

推奨設定をクリアするには

パス： [メインメニュー](#) | [「コンピュータ」](#)

1. 推奨設定をクリアするコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「**処理**」 > 「**推奨設定をクリア**」を選択します。

セキュリティプロファイルを割り当てる

セキュリティプロファイルを1台または複数のコンピュータに割り当てたり、プロファイルを現在のドメインに割り当てることができます。セキュリティプロファイルの詳細については、「75 ページの「セキュリティプロファイル」」を参照してください。

コンピュータにセキュリティプロファイルを割り当てる

セキュリティプロファイルを、1台または複数のコンピュータに割り当てることができます。コンピュータに割り当てるセキュリティプロファイルの名前が、コンピュータリストの「セキュリティプロファイル」列に表示されます。

注意： ファイアウォールルールの追加やステートフル設定の変更など、他の設定をコンピュータに適用する場合は、セキュリティプロファイルの名前の横に初期設定が変更されたことがわかるよう太字で表示されます。

セキュリティプロファイルを1台または複数のコンピュータに割り当てるには

パス：[メインメニュー](#) | 「[コンピュータ](#)」

1. プロファイルを割り当てるコンピュータを選択します。
2. ツールバーの「**セキュリティプロファイルの割り当て ...**」をクリックするか、右クリックしてポップアップメニューから「**処理**」 > 「**セキュリティプロファイルの割り当て ...**」を選択します。
3. 「**セキュリティプロファイルの割り当て**」ウィンドウで、割り当てるセキュリティプロファイルを選択し、「OK」をクリックします。

ドメインにセキュリティプロファイルを割り当てる

セキュリティプロファイルをドメインに割り当てると、そのドメイン内のすべてのコンピュータにそのプロファイルを割り当てたことと同じ結果になります。セキュリティプロファイルは、ドメインレベルではなく、コンピュータレベルでコンピュータに割り当てられる点に留意してください。セキュリティプロファイルをドメインに割り当てると、そのセキュリティプロファイルはドメイン内のすべてのコンピュータに割り当てられます。ただし、それ以降にドメインに追加されたコンピュータには、そのセキュリティプロファイルが自動的に割り当てられません。

クライアントプラグインを管理する

クライアントプラグインは、ネットワーク内のすべてのクライアントコンピュータでインストールされ、サーバプラグインでクライアントコンピュータと通信し、セキュリティを管理できます。

プラグイン通信を設定する

初期設定（双方向）では、クライアントプラグインによってハートビートが開始しますが、サーバプラグインの接続をクライアントプラグインのポートで待機するため、サーバプラグインは必要に応じて処理を実行するためにクライアントプラグインに自由に接続できます。「サーバプラグインによる開始」では、サーバプラグインによってすべての通信が開始します。サーバプラグインによって予約アップデートまたはハートビート処理（下記）が実行された際、およびサーバプラグインインタフェースから「有効/無効」オプションまたは「今すぐ更新」オプションを選択した際に、通信が発生します。リモートの送信元から開始された通信に対してコンピュータを遮断する場合は、クライアントプラグイン自体で定期的にアップデートの有無を確認し、ハートビート処理を管理するように選択できます。この場合、「クライアントプラグインによる開始」を選択します。

注意： ハートビート中にサーバプラグインによって次の情報が収集されます。ドライバのステータス（オンラインまたはオフライン）、クライアントプラグインのステータス（時刻を含む）、前回のハートビート以後のクライアントプラグインのログ、カウンタをアップデートするデータ、およびクライアントプラグインのセキュリティ設定のフィンガープリント（設定が最新のものかどうか判断するために使用）。ハートビートの実行間隔（クライアントプラグインまたはサーバプラグインによる開始）およびアラートがトリガされるまでに失われるハートビートの許容数を変更できます。

この設定は（他の多くの設定と同様に）、次の3つのレベルで設定できます。システム全体の初期設定を設定することによってすべてのコンピュータに設定、特定のセキュリティプロファイルが割り当てられているコンピュータにのみ設定、あるいは個々のコンピュータに設定が可能です。

全システムに設定する：

1. サーバプラグインの「システム」>「システム設定」画面で「コンピュータ」タブをクリックします。
2. 「通信方向」パネルのドロップダウンリストから、「サーバプラグインによる開始」、「クライアントプラグインによる開始」、または「双方向」を選択します。

特定のセキュリティプロファイルが割り当てられているコンピュータにのみ設定する：

1. 該当するセキュリティプロファイルの「セキュリティプロファイルのプロパティ」画面を開き、通信を設定します。
2. 「システム」>「システム設定」へ進み、「コンピュータ」タブをクリックします。
3. 「脆弱性対策オプションサーバプラグインとクライアントプラグインの通信方向：」ドロップダウンメニューで、3つのオプション、「サーバプラグインによる開始」、「クライアントプラグインによる開始」、または「双方向」のいずれかを選択するか、「継承」を選択します。「継承」を選択した場合、セキュリティプロファイルでは、「システム」>「システム設定」画面で指定された設定が継承されます。その他のオプションのいずれかを選択すると、それはグローバルでの選択より優先されます。
4. 「保存」をクリックして変更を適用します。

特定のコンピュータのみ：

1. コンピュータの「詳細」画面を開き、通信を設定します。
2. 「システム」>「システム設定」へ進み、「コンピュータ」タブをクリックします。
3. 「脆弱性対策オプションサーバプラグインとクライアントプラグインの通信方向：」ドロップダウンメニューで、3つのオプション、「サーバプラグインによる開始」、「クライアントプラグインによる開始」、または「双方向」のいずれかを選択するか、「継承」を選択します。「継承済み」を選択した場合、コンピュータでは、セキュリティプロファイルの「詳細」画面またはサーバプラグインの「システム」>「システム設定」画面で指定された設定が継承されます。その他のオプションのいずれかを選択すると、それはセキュリティプロファイルまたはグローバルでの選択より優先されます。
4. 「保存」をクリックして変更を適用します。

注意： クライアントプラグインは、サーバプラグインのホスト名によってネットワーク上の脆弱性対策オプションサーバプラグインを検索します。このため、クライアントプラグインによる開始または双方向の通信を使用する場合は、サーバプラグインのホスト名が必ずローカル DNS 内にある必要があります。

クライアントプラグインを配信する

クライアントプラグインは、一般に、サーバプラグインインタフェースを使用してインストールおよび管理できます。ただし、場合によっては、クライアントコンピュータ上で処理を実施する必要があります。

サーバからクライアントプラグインを配信する

クライアントプラグインをウイルスバスター Corp. クライアントにインストールすると、クライアントプラグインは自動的に有効化されます。

注意： クライアントプラグインは、「<PROGRAM FILES>Trend Micro¥IDF Client」にインストールされます（これは初期設定された場所で、変更はできません）。

クライアントプラグインを配信するには

パス：メインメニュー | 「コンピュータ」

1. クライアントプラグインを配信するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」 > 「クライアントプラグインの配信」を選択します。

スタンドアロンクライアントプラグインインストーラを使用する

脆弱性対策オプションのスタンドアロンクライアントプラグインのインストーラパッケージは、クライアントコンピュータ上で実行される自動展開型の .msi ファイルです。トレンドマイクロの「最新版ダウンロード」サイトから入手できます (<http://www.trendmicro.co.jp/download/>)。クライアントコンピュータには、すでにウイルスバスター Corp. クライアントがインストールされている必要があります。クライアントプラグインはインストール後にエージェントによる自動アクティベーションを実行しますが、自動アクティベーションを動作させるには、クライアントプラグインによる開始のアクティベーションを、サーバプラグインコンソールから有効にする必要があります（「システム」 → 「システム設定」 → 「コンピュータ」）。

スタンドアロンのインストーラは、ウイルスバスター Corp. クライアントが次のデフォルトの場所にインストールされているものとして、ウイルスバスター Corp. クライアントで脆弱性対策オプションクライアントプラグインをインストールします。

C:¥Program Files¥Trend Micro¥OfficeScan Client.

スタンドアロンのクライアントプラグインインストーラを使用するには：

1. ログインする必要がない場合：32 ビットプラットフォームの場合、`IdfClient-1.5.0.xxxx-en.i386.msi` をダブルクリックします。64 ビットプラットフォームの場合 `IdfClient-1.5.0.xxxx-en.x86_64.msi` をダブルクリックします。(xxxx は内部ビルド番号です)。
2. ログインが必要な場合、上記の手順 1 の代わりに次を行ってください。
 - a. 「コマンドプロンプト」ウィンドウを開きます。
 - b. standalone msi が入っているフォルダに移動します。
 - c. 次のコマンドを実行します。

```
msiexec /i IdfClient-1.5.0.xxxx-en.i386.msi /l*v idf_standalone.log
```

ログファイルの名前は、idf_standalone.log になります。
3. クライアントが「コンピュータ」画面にあり、ステータスが「管理対象」となっていることを確認します。

注意： スタンドアロンのインストーラは一時的にクライアントのネットワーク接続を中断させるため、インストーラはホストコンピュータ上でローカルに実行する必要があります。

クライアントプラグインを有効化 / 無効化する

コンピュータが非管理対象の場合、クライアントプラグインを有効にし、コンピュータを管理対象状態に移行する必要があります。有効にする前は、クライアントプラグインは次の状態のいずれかになります。

- ・ **クライアントプラグインなし**：初期設定のポートで稼働中または待機中のクライアントプラグインが存在しないことを示しています。また、「クライアントプラグインなし」ステータスは、クライアントプラグインがインストールされ稼働中であるが、別のサーバプラグインと連携しており、通信が「クライアントプラグインによる開始」として設定されているため、クライアントプラグインがこのサーバプラグインを待機していないことも示しています（後者の状況を修正する場合は、コンピュータからクライアントプラグインを無効にする必要があります）。
- ・ **クライアントプラグインがインストール済み**：クライアントプラグインはインストールされ待機中で、いつでもサーバプラグインによって有効になります。
- ・ **クライアントプラグインの有効化が必要**：クライアントプラグインはインストールされ待機中で、サーバプラグインによる有効化を待ち受けています。

- ・ **クライアントプラグインの再有効化が必要**: クライアントプラグインはインストールされ待機中で、サーバプラグインによる有効化を待ち受けています。
- ・ **クライアントプラグインの無効化が必要**: クライアントプラグインはインストールされ待機中ですが、すでに別のサーバプラグインによって有効になっています。このサーバプラグインによって有効にするには、コンピュータ上でクライアントプラグインをローカルで無効にする必要があります。

有効化が正常に実行されると、クライアントプラグインの状態は「管理対象」に変わります。有効化に失敗すると、コンピュータのステータスに、「クライアントプラグインの有効化に失敗しました」と括弧内に失敗の理由が表示されます。このリンクをクリックすると、有効化の失敗理由の詳細を示すシステムイベントが表示されます。

クライアントプラグインを有効化するには

パス: [メインメニュー](#) | 「[コンピュータ](#)」

1. クライアントプラグインを有効化するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「[処理](#)」 > 「[有効化 / 再有効化](#)」を選択します。

クライアントプラグインを停止および起動する

クライアントプラグインの停止または起動は、そのコンピュータでのみローカルに実行できます。

クライアントプラグインを停止または起動するには

- ・ 停止: コマンドラインから、次のコマンドを実行します。 `sc stop ds_agent`
- ・ 開始: コマンドラインから、次のコマンドを実行します。 `sc start ds_agent`

コンピュータ上のクライアントプラグインをアップデートする

コンピュータ上のクライアントプラグインをアップデートすると、そのコンピュータに加えたすべての設定の変更が、サーバプラグインからクライアントプラグインに配信されます。アップデートはハートビートのたびに自動的に発生しますが、変更をただちに適用する場合に、このオプションを使用できます。「[クライアントプラグインを今すぐアップデート](#)」ボタンを使用すると、コンピュータアクセススケジュールよりも優先され、また、前回の試行に失敗した場合には、サーバプラグインによってアップデートが強制的に再試行されます。

注意: 通信が「クライアントプラグインによる開始」に設定されていない場合は、自動アップデートはただちに実行されます。「クライアントプラグインによる開始」にされている場合は、次のハートビート時に実行されます。

クライアントプラグインをアップデートするには

パス: メインメニュー | 「コンピュータ」

1. クライアントプラグインを無効化するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」>「今すぐアップデート」を選択します。

クライアントプラグインの手動によるアップデート

サーバプラグインのコンピュータとクライアントプラグインのコンピュータの間に接続の制限があるために、サーバプラグインのインタフェースからコンピュータ上のクライアントプラグインソフトウェアをアップグレードできない場合があります。そのような場合は、コンピュータ上のクライアントプラグインソフトウェアのアップグレードを手動で実行する必要があります。

新しいクライアントプラグインソフトウェアは、トレンドマイクロのダウンロードセンターから手動でダウンロードする必要があります。

クライアントプラグインを手動でアップグレードするには、クライアントプラグインのインストーラをコンピュータにコピーして実行します。以前のクライアントプラグインが検出され、アップグレードが実行されます。

コンピュータ上のクライアントプラグインを無効にする

クライアントプラグインの無効化は、クライアントプラグインのアンインストールとは異なります。無効化では、クライアントプラグインからすべてのルールやフィルタなどが削除され、サーバプラグインの排他的制御からクライアントプラグインが解放されます (サーバプラグインによりクライアントプラグインが有効化されると、インストールされた他のどの脆弱性対策オプションシステムもそのクライアントプラグインとは通信できません。無効化されたクライアントプラグインは、脆弱性対策オプションサーバで再度有効化することができ、そのサーバがクライアントプラグインを排他的に制御します)。手動による無効化は、サーバプラグインがクライアントプラグインと通信できなくなった場合に必要です。

サーバプラグインのインストール間でコンピュータ / クライアントプラグインのコントロールを転送場合があります。その場合、クライアントプラグインを無効にしてから、再度、新しいサーバプラグインによって有効にする必要があります。クライアントプラグインの無効化はクライアントプラグイン UI によりローカルのコンピュータで実行することもできれば、現在クライアントプラグインを管理しているサーバプラグインから実行することもできます (無効にするために、コンピュータへのアクセスが可能である必要はありません)。アクセス不可で無効になったコンピュータがアクセス可能になった場合、コンピュータリストに「新規 (不明)」コンピュータとして表示されるだけです。

サーバプラグインからクライアントプラグインを無効にするには

パス: メインメニュー | 「コンピュータ」

1. クライアントプラグインを無効化するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」 > 「無効化」を選択します。

クライアントプラグインを手動で無効にするには

1. クライアントコンピュータで「コマンドプロンプト」画面を開きます (「スタート」 > 「ファイル名を指定して実行」 > 「cmd.exe」)。
2. クライアントプラグインのインストールディレクトリに進みます。
`cd c:¥Program Files¥Trend Micro¥IDF Client`
3. クライアントプラグインを無効化するコマンドを入力します。

```
dsa_control /r /c ds_agent.crt
```

クライアントプラグインは、他の (または同じ) 脆弱性対策オプションサーバで有効化できるようになりました

注意: コンピュータが脆弱性対策オプションのフィルタおよびルールで保護されなくなっている
ので注意してください。

クライアントプラグインをアンインストールする

クライアントプラグインは通常、サーバプラグインインタフェースからアンインストールできますが、場合によっては、クライアントプラグインをクライアントコンピュータから手動でアンインストールしなければならない場合があります。

注意： 脆弱性対策オプションクライアントプラグインは、コントロールパネルの「プログラムの追加と削除」アプレットを使用してアンインストールすることはできません。

サーバからクライアントプラグインを削除するには

パス：[メインメニュー](#) | 「[コンピュータ](#)」

1. クライアントプラグインを削除するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」 > 「クライアントプラグインの削除」を選択します。

クライアントプラグインを手動でアンインストールするには

1. クライアントコンピュータで「コマンドプロンプト」画面を開きます（「スタート」 > 「ファイル名を指定して実行」 > 「cmd.exe」）。
2. 32 ビット Windows の場合、次を入力して Enter キーを押します。

```
rundll32 "C:¥Program Files¥Trend Micro¥IDF  
Client¥IdfClientAgent.dll",Uninstall
```

3. 64 ビット Windows の場合、次を入力して Enter キーを押します。

```
rundll32 "C:¥Program Files (x86)¥Trend Micro¥IDF  
Client¥IdfClientAgent.dll",Uninstall
```

コンピュータのイベントを表示する

特定のコンピュータに関連付けられたシステムイベントと管理イベント、つまりセキュリティ関連以外のイベントを確認したり、このコンピュータ上のクライアントプラグインからアップロードされた最新のファイアウォールイベントを確認できます。通常のイベント取得スケジュール（通常はハートビートごと）よりも優先し、コンピュータから今すぐイベントログを取得できます。コンピュータのイベントの情報の詳細については、「253 ページの「クライアントプラグインイベント」」を参照してください。

コンピュータのシステムイベントを表示するには

パス: メインメニュー | 「コンピュータ」

1. システムイベントを表示するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「表示」 > 「システムイベントの表示 ...」を選択します。
3. 新しいウィンドウが開き、選択したコンピュータのシステムイベントが表示されます。システムイベントの詳細については、「238 ページの「システムイベント」」を参照してください。

コンピュータのファイアウォールイベントを表示するには

パス: メインメニュー | 「コンピュータ」

1. ファイアウォールイベントを表示するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「表示」 > 「ファイアウォールイベントの表示 ...」を選択します。
3. 新しいウィンドウが開き、選択したコンピュータのファイアウォールイベントが表示されます。システムイベントの詳細については、「232 ページの「ファイアウォールイベント」」を参照してください。

クライアントプラグインから今すぐイベントを取得するには

パス: メインメニュー | 「コンピュータ」

1. イベントを取得するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」 > 「今すぐイベントを取得」を選択します。

警告 / エラーをクリアする

無効にする前やコンピュータをコンピュータリストから削除する前にクライアントプラグインがローカルでリセットされた場合や、または単にネットワークから削除した場合は、コンピュータで生成された警告やエラーをクリアできます。

警告およびエラーをクリアするには

パス: メインメニュー | 「コンピュータ」

1. 警告やエラーをクリアするコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」 > 「警告 / エラーのクリア」を選択します。

コンピュータをロックまたはロック解除する

コンピュータ上で保守操作を実行する際に、サーバプラグインに一連のアラートがトリガされないようにする場合は、コンピュータをロックできます。

注意： ロックされている間、コンピュータのステータスは「ロック済み」と表示されます。サーバプラグインはクライアントプラグインと通信しなくなるか、コンピュータ/クライアントプラグイン関連のアラートがトリガされます。既存のコンピュータアラートには影響しません。コンピュータアップデートが進行中の場合は、正常に完了できます。クライアントプラグインは、コンピュータがロック済み状態であることを認識していない点に注意してください。クライアントプラグインとサーバプラグインの間の通信が「クライアントプラグインによる開始」または「双方向」に設定されている場合、クライアントプラグインはイベントを生成する場合があります。このイベントは、最終的にサーバプラグインに再接続したときにレポートされます。

コンピュータをロックするには

パス: [メインメニュー](#) | 「[コンピュータ](#)」

1. ロックするコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「[処理](#)」>「[ロック](#)」を選択します。

コンピュータをロック解除するには

パス: [メインメニュー](#) | 「[コンピュータ](#)」

1. ロック解除するコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「[処理](#)」>「[ロック解除](#)」を選択します。

コンピュータ資産評価を割り当てる

コンピュータ資産評価は、コンピュータに値を割り当てるために使用されるカスタマイズ可能な評価システムです。評価システムのグレードごとに、1～100の範囲の値があります。この値とルール的重要度の値を乗算することで、ファイアウォールイベントとDPIルールイベントをランク付けできます。ランク付けを設定するには、「[システム](#)」→「[システム設定](#)」→「[ランク付け](#)」に進みます。

コンピュータ資産評価を割り当てるには

パス: メインメニュー | 「コンピュータ」

1. 資産評価を割り当てるコンピュータを選択します。
2. 右クリックしてポップアップメニューを表示し、「処理」 > 「資産評価の割り当て ...」を選択します。
3. 「資産評価の割り当て」ウィンドウで、資産評価を選択して「OK」をクリックします。

コンピュータの詳細を表示および編集する

コンピュータの「詳細」画面には、脆弱性対策オプションサーバプラグインのメインインタフェースと同じものが表示されます。上位の設定や構成がある場合でも、それを変更して優先するように設定および構成できます。

「コンピュータの詳細」ウィンドウを開くには

パス: メインメニュー | 「コンピュータ」

1. 詳細を表示または編集するコンピュータを選択し、ツールバーの「詳細」をクリックするか、右クリックしてポップアップメニューを表示し「表示」 > 「詳細 ...」を選択します。
2. 新しいウィンドウが開き、選択したコンピュータの詳細にアクセスするためのナビゲーションバーが表示されます。



図 6-4. 「コンピュータの詳細」ウィンドウ

コンピュータ情報

「コンピュータの詳細」ウィンドウの「コンピュータ情報」画面で、選択したコンピュータのホスト名やドメインなどの情報を編集したり、クライアントプラグインステータスなどの情報を表示できます。

コンピュータ情報を表示または編集するには

パス: **メインメニュー** | 「**コンピュータ**」 > 「**詳細**」

1. コンピュータを選択してツールバーの「**詳細**」をクリックするか、右クリックしてポップアップメニューを表示し、「**詳細 ...**」を選択します。
2. 「一般」領域で、次のオプションを編集します。
 - **ホスト名**: 「コンピュータ」画面の「名前」列に表示されます。名前は、コンピュータの IP アドレスまたはコンピュータのホスト名のいずれかを指定する必要があります (IP アドレスの代わりにホスト名を使用する場合は、完全修飾ホスト名または相対ホスト名のいずれも使用できます)。
 - **説明**: コンピュータの説明。
 - **プラットフォーム**: コンピュータの OS の詳細は、ここに表示されます。
 - **ドメイン**: コンピュータの所属するコンピュータドメインがドロップダウンリストに表示されます。コンピュータの割り当てを既存の別のコンピュータドメインに変更できます。
 - **セキュリティプロファイル**: このコンピュータに割り当てたセキュリティプロファイルです (存在する場合)。

注意: コンピュータのセキュリティプロファイルの割り当てを解除するとき、セキュリティプロファイルに対してルールが独立して割り当てられている場合は、コンピュータに対しルールは引き続き有効な場合があることに注意してください。

- **資産の重要度**: 脆弱性対策オプションサーバプラグインは、ランク付けシステムを使用して、セキュリティイベントの重要度を数値化できます。ルールには重要度 (高、中、低など) が割り当てられ、資産 (コンピュータ) には「資産重要度」が割り当てられます。これらのレベルは、数値で表記されます。コンピュータでルールがトリガされると、資産重要度の値と重要度の値が乗算されます。この結果がスコアとなり、イベントを重要度別にソートする際に使用できます。(イベントのランク付けは「イベント」画面で参照できます。) この「資産重要度」ドロップダウンリストを使用して、このコンピュータに資産の重要度を割り当てます。(重要度と重要度の数値は、「システム」→「システム設定」→「ランク付け」で編集できます)。

- **コンピュータのロック (すべての通信を禁止)**: このオプションを設定すると、クライアントプラグインとサーバプラグインの間のすべての通信がブロックされます。コンピュータのセキュリティプロファイルは有効のまま、すべてのルールがすべてのトラフィックに適用されます。アラートが生成されたとしても、アラートはサーバプラグインに送信されません。

注意: コンピュータ上で保守操作を実行する際に、サーバプラグインに一連のアラートが表示されないようにする場合は、コンピュータをロックできます。

3. 「ステータス」領域では、次のステータス情報とオプションを使用できます。

- **ステータス**: 現在のコンピュータのステータスを、次のように表示します。
 - コンピュータが管理されていない場合は「非管理対象」とその後にクライアントプラグイン状態 (クライアントプラグインなし)、「不明」、「再有効化が必要」、「有効化が必要」、または「無効化が必要」) が括弧付きで表示されます。
 - コンピュータが管理対象で、コンピュータのエラーがない場合、ステータスに「管理対象」と表示され、その後の括弧内にクライアントプラグインの状態 (「オンライン」と「オフライン」のどちらか) が示されます。
 - コンピュータが管理対象で、クライアントプラグインがクライアントプラグインのアップグレード (インストールプログラムの送信) などの処理を実行している場合は、そのタスクのステータスが表示されます。
 - コンピュータ上に、「オフライン」、「更新に失敗しました。」などのエラーがある場合、ステータスにはそのエラーが表示されます。複数のエラーが存在する場合、ステータスには「複数のエラー」と表示され、その下に各エラーが一覧表示されます。
- **ファイアウォール**: ファイアウォールのオン / オフの状態と有効なルールの数を示します。
- **DPI**: DPI のオン / オフの状態と有効なルールの数を示します。
- **オンライン**: サーバプラグインが現在クライアントプラグインと通信可能かどうかを示します。
- **前回の通信**: サーバプラグインがこのコンピュータのクライアントプラグインと正常に通信した前回の日時。

- **ステータスの確認**: このボタンを使用すると、サーバプラグインによってただちにハートビート操作が強制的に実行され、クライアントプラグインのステータスを確認できます。ステータスの確認では、クライアントプラグインのアップデートを実行しません (アップデートが必要な場合は、「処理」タブの「今すぐアップデート」ボタンをクリックします)。サーバ/クライアント間通信が「クライアントプラグインによる開始」に設定されている場合、「ステータスの確認」ボタンは無効になっています。(ステータスを確認しても、コンピュータのログはアップデートされません。コンピュータのログをアップデートするには、「処理」タブに進みます。)
 - **警告/エラーのクリア**: このコンピュータに対するアラートまたはエラーを消去します。
4. 「アクティベーション」領域では、次のステータス情報とオプションを使用できます。
- 新しくインストールされた脆弱性対策オプションクライアントプラグインは、セキュリティプロファイル、ルール、イベントログへのリクエストなどを受信する前に脆弱性対策オプションサーバプラグインにより「有効化」する必要があります。有効化するには、サーバプラグイン (またはサーバプラグインのノードの1つ) とクライアントプラグインが互いを一意に識別するためのSSLキーを交換します。脆弱性対策オプションサーバプラグインによって有効化されると、クライアントプラグインは有効化を実施した脆弱性対策オプションサーバプラグイン (または脆弱性対策オプションサーバプラグインのノードの1つ) からの指示または通信のみを許可するようになります。
- 有効化されていないクライアントプラグインは、サーバプラグインならどれでも有効化できません。
- クライアントプラグインの有効化は、コンピュータからローカルに実施するか、または有効化を行ったサーバプラグインで実施することしかできません。クライアントプラグインがすでに有効化されている場合は、このエリアのボタンが「有効化」ではなく「再有効化」と表示されます。再有効化は、有効化と同等の効果があります。再有効化することで、クライアントプラグインは最初にインストールされた時点へリセットされ、新しいSSLキーセットの交換が行われます。
5. 「アップデート」領域で、次の情報とオプションを使用できます。
- サーバプラグインを使用してコンピュータ上のクライアントプラグインに新規DPIルールの適用、ログ設定の変更といった設定の変更を行った場合、サーバプラグインは新しい情報をクライアントプラグインに送信しなければなりません。これがアップデートです。アップデートは通常ただちに実行されますが、「今すぐアップデート」ボタンをクリックすることで強制的にアップデートすることができます。

6. 「ソフトウェア」領域では、次のステータス情報とオプションを使用できます。

ここでは、コンピュータ上で現在実行されているクライアントプラグインのバージョンが表示されます。コンピュータのプラットフォームに対応する新しいクライアントプラグインのバージョンが利用可能になったら、「クライアントプラグインのアップグレード...」ボタンをクリックして、脆弱性対策オプションサーバプラグインからリモートでクライアントプラグインをアップグレードできます。使用するコンピュータに対応した新しいクライアントプラグインのバージョンが出た場合に脆弱性対策オプションサーバプラグインでアラートをトリガさせるには、脆弱性対策オプションサーバプラグインのメイン画面から「システム」>「アップデート」に進みます。
7. 「サポート」領域では、診断パッケージを作成できます。

「**診断パッケージの作成**」ボタンでは、コンピュータのクライアントプラグインの状態に関するスナップショットを作成できます。スナップショットは、サポート担当者がトラブルシューティングの目的で要求することがあります。

コンピュータとの通信が失われた場合は、診断パッケージをローカルに作成できます。

Windows コンピュータで診断パッケージをローカルに作成するには

 - a. コマンドラインで、次のように入力します。

```
C:\Program Files\Trend Micro\IDF Client Plug-in> dsa_control.exe /d
```

Enter キーを押します。
 - b. 同じディレクトリに、診断結果を含む番号付けされた zip ファイル (たとえば「341234567.zip」) が作成されます。
8. インタフェースを表示したり変更するには、ナビゲーション画面で「**インタフェース**」をクリックします。

「インタフェース」画面にコンピュータ上で検出したインタフェースが表示されます。複数のインタフェース割り当てがされたセキュリティプロファイルがこのコンピュータに割り当てられている場合、セキュリティプロファイルで定義されたパターンと一致するインタフェースが検出されます。
9. アラートを表示したり変更するには、ナビゲーション画面で「**アラート**」をクリックします。

アラートはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのコンピュータに関するアラートのみです。ここでアラートを消去すると、メインの「サーバプラグイン」画面からも消去されます。アラートの詳細については、「33 ページの「アラート」」を参照してください。

10. ファイアウォール設定を表示したり変更するには、ナビゲーション画面で「ファイアウォール」をクリックします。

コンピュータのファイアウォールは、優先するよう選択しないかぎり、セキュリティプロファイルまたはサーバプラグインのグローバル設定にあるステートフル設定 (オン/オフ) を継承します。

注意： ファイアウォールをオフに切り替えてセキュリティプロファイルをコンピュータに適用し、そのコンピュータがファイアウォール設定を継承するように設定されている場合、そのコンピュータでは、セキュリティプロファイルが適用される前に直接コンピュータに割り当てられたエレメントであっても、すべてのファイアウォールエレメント (ファイアウォールルールとステートフル設定) がオフになります。

- **イベント：**ファイアウォールイベントはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのコンピュータに関するイベントのみです。
- **ルール：**サーバプラグインで定義されるファイアウォールルールは、ここに表示されます。このコンピュータで有効化するルールを選択します。コンピュータに複数のインタフェースがある場合は、下向き矢印をクリックしてドロップダウンメニューを表示し、ファイアウォールルールを全インタフェースに適用するか、特定のインタフェースにのみ適用するかを選択します。

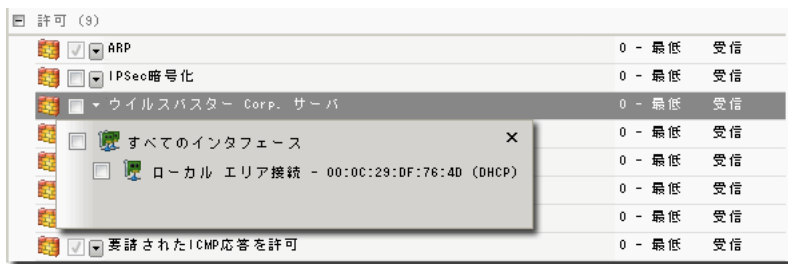


図 6-5. ルール

有効化されたファイアウォールルールの横にあるチェックマークに注目してください。グレー表示されたチェックマークは、セキュリティプロファイルがコンピュータに対してファイアウォールルールを適用し、有効であることを示しています。(その他のルールについても同様です。)

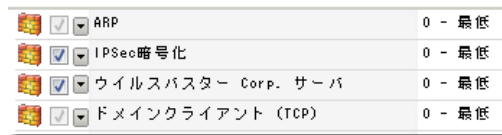


図 6-6. ルールチェックマーク

- ・ **ステートフル設定**: このコンピュータに適用するステートフル設定を選択します。コンピュータに複数のインタフェースがある場合は、各インタフェースに個別の設定を指定できます。
11. ナビゲーション画面の「Deep Packet Inspection」をクリックして表示や変更します。

コンピュータの DPI エンジンには、優先するよう選択しないかぎり、割り当てられたセキュリティプロファイルまたはサーバプラグインのグローバル設定にあるステートフル設定 (オン/オフ)、インライン動作、推奨設定の検索を継承します。

- ・ **イベント**: DPI イベントはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのコンピュータに関するイベントのみです。
- ・ **ルール**: サーバプラグインで定義される DPI ルールは、ここに表示されます。このコンピュータで有効化するルールを選択します。
- ・ **アプリケーションの種類**: サーバプラグインで定義されるアプリケーションの種類は、ここに表示されます。プロパティは、このセキュリティプロファイルに対してのみ、またはグローバルで編集できます。
- ・ **SSL 設定**: サーバプラグインでは、SSL トラフィックの DPI 分析がサポートされます。ユーザは、「SSL 設定」画面を使用して、1 つ以上のインタフェース上で指定された認証とポートが対になっている SSL 設定を作成できます。証明書は P12 または PEM 形式でインポートでき、Windows のコンピュータでは直接 Windows CryptoAPI を使用するオプションが用意されています。

新規に SSL 設定を作成するには、「新規」をクリックして **SSL 設定** ウィザードの手順に従います。

設定するコンピュータがサーバプラグインをホストするコンピュータにインストールされている場合、ウィザードはすでにサーバプラグインに格納されている資格情報を提供します。

既存の設定をダブルクリックして、「プロパティ」画面を表示します。

割り当て：

- **一般情報：**SSL 設定の名前と説明、およびコンピュータでその SSL 設定が有効かどうかを示します。
- **インターフェースの割り当て：**この設定が適用されているインターフェースです。
- **IP の割り当て：**この設定を適用する IP です。
- **ポート選択：**この設定を適用するポートです。

資格情報：

「資格情報」タブには現在の資格情報が一覧表示され、それらを変更するための「新しい資格情報の割り当て ...」ボタンがあります。

注意： 脆弱性対策オプションクライアントプラグインでサポートされるのは、SSL トラフィックのフィルタです。クライアントプラグインは、SSL 圧縮が実装されている SSL 接続のフィルタはサポートしません。

12. システム情報を表示または編集するには、「システム」、「システム設定」、または「システムイベント」をクリックして「システム」画面を開きます。
 - **システムイベント：**システムイベントはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのコンピュータに関するイベントのみです。
 - **システム設定：**特定のコンピュータで上書き可能なサーバプラグインのシステム設定が、すべてここに表示されます。
13. 「優先」をクリックして、コンピュータで上書きされた要素を表示または編集します。

継承および優先

グローバル設定よりも、セキュリティプロファイルまたはコンピュータレベルで行った設定が優先されることがあります。たとえば、脆弱性対策オプションは、脆弱性対策オプションサーバプラグインメイン画面にあるファイアウォール画面で「ファイアウォール」をオフに設定すれば、グローバルでオフにすることができます。



図 6-7. ファイアウォール設定

初期設定では、低い階層レベルは上の階層レベルの設定を継承します。よって、グローバルレベルでファイアウォールをオフにすると、すべてのセキュリティプロファイルと、「継承」に設定されたコンピュータすべてのファイアウォールがオフになります。

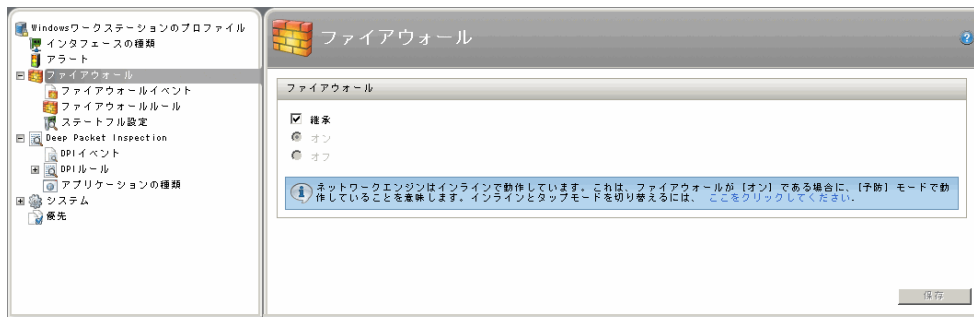


図 6-8. 継承

その他プロパティ

ファイアウォールルールや DPI ルールなどのエレメントは、特定のコンピュータに対していくつかのプロパティを変更できます。たとえば、FirewallRuleAlpha というファイアウォールルールがあるとします。そのプロパティの中では、ファイアウォールルールを設計したアプリケーションはポート 12345 で動作するため、そのルールは受信ポート 12345 で動作することになります。

ただし、たとえばあるコンピュータのポート 44444 番でアプリケーションが動作していたとします。このコンピュータに新規ファイアウォールルールを記述する代わりに、コンピュータの「詳細」画面を開いて「ファイアウォールルール」へ進み、リストからファイアウォールルールを探して右クリックし、「プロパティ (このコンピュータ用)」を選択して設定できます。

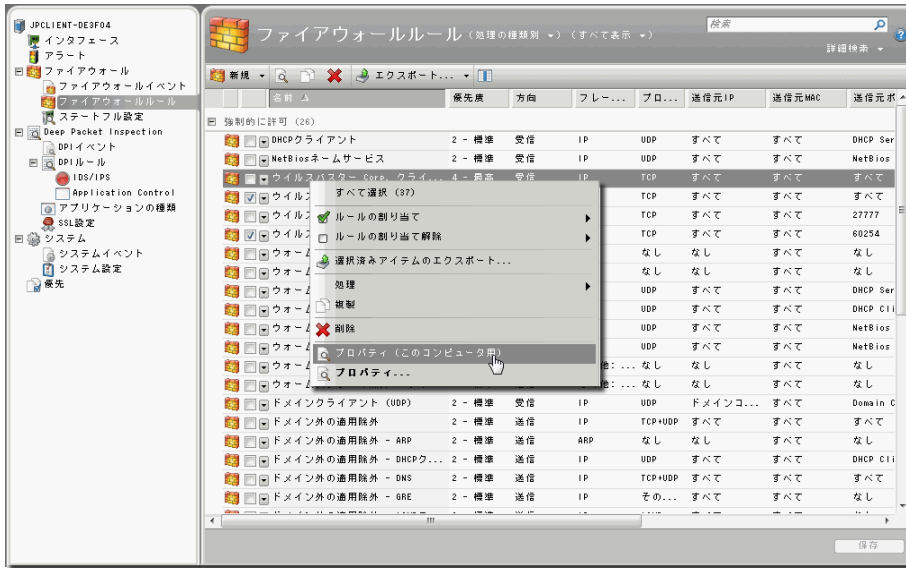


図 6-9. プロパティ (このコンピュータ用)

このファイアウォールルールの「プロパティ」画面には、多くのプロパティが表示され、その横には「継承」と呼ばれるチェックボックスがあります。つまり、設定が階層の範囲内で上位のレベルから継承されることを示します（セキュリティプロファイルまたはグローバルリストのいずれかから継承されます）。「ポート:」の横にある「継承済み」チェックボックスをオフにして、44444に変更すると、このコンピュータに限ってファイアウォールルールがポート 44444 で動作することになります。

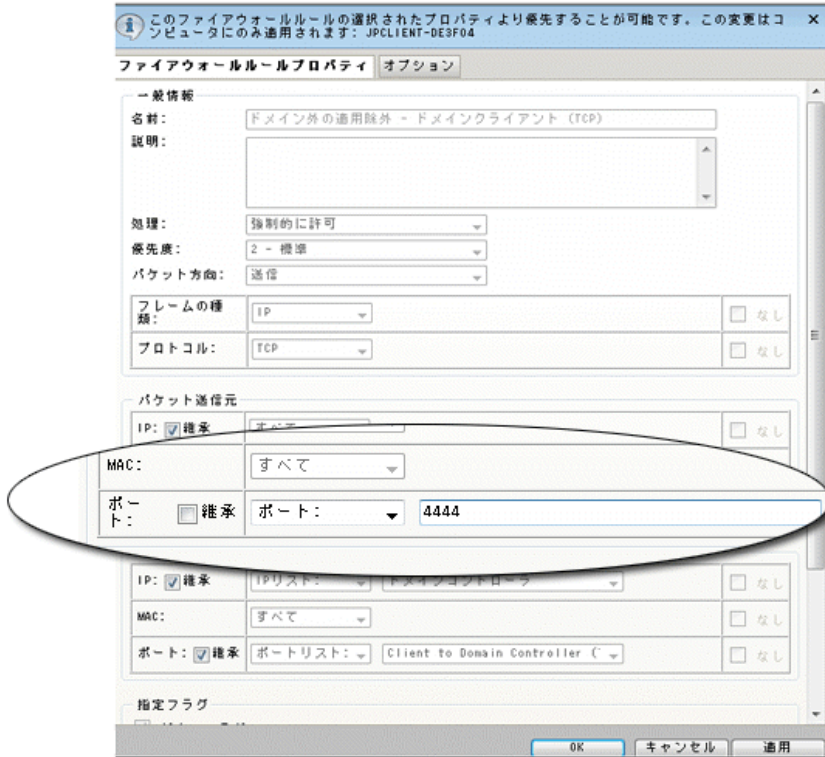


図 6-10. 継承プロパティ

ファイアウォールルールがセキュリティプロファイルの一部になっている場合は、セキュリティプロファイルレベルでこの操作を実行することもできます。セキュリティプロファイルの「詳細」画面を開いて、同様の変更を行います。（特定のコンピュータでこの変更を再度優先できます。）

コンピュータまたはセキュリティプロファイルの優先を表示する

セキュリティプロファイルまたはコンピュータにどのエレメントが優先されたかを確認するには、「詳細」画面を開いて「優先」画面へ進みます。



図 6-11. 優先を表示する



第7章

セキュリティプロファイル

この章では、脆弱性対策オプション™ 1.5 セキュリティプロファイルについて説明します。

この章で扱うトピックは次のとおりです。

- 76 ページの「セキュリティプロファイルについて」
- 76 ページの「セキュリティプロファイルの管理」
- 77 ページの「セキュリティプロファイルの詳細の表示および編集」

セキュリティプロファイルについて

セキュリティプロファイルを使用すると、ファイアウォールルール、ステートフル設定、および DPI ルールの共通の設定を、それぞれのインタフェース割り当てとともに保存し、それらを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。

セキュリティプロファイルの管理

「セキュリティプロファイル」画面を開くには、脆弱性対策オプションメインメニューの「セキュリティプロファイル」をクリックします。メインの「セキュリティプロファイル」画面には、既存のプロファイルのリストが表示されます。この画面から、次のことを実行できます。

- 新規セキュリティプロファイルを作成する (📄 新規)
- XML ファイルからセキュリティプロファイルをインポートする (📄)

注意： 新しいセキュリティアップデートから、古いセキュリティアップデートを実行中のシステムに、セキュリティプロファイルをインポートしないでください。新しいセキュリティプロファイルは、古いバージョンに存在しないルールを参照している場合があります。常に、セキュリティアップデートが最新であることを確認してください。

- 既存のセキュリティプロファイルのプロパティを確認または変更する (🔍)
- 既存のセキュリティプロファイルを複製し、変更してから名前を変更する (📄)
- セキュリティプロファイルを削除する (✖)
- セキュリティプロファイルを XML ファイルにエクスポートする (📄)

セキュリティプロファイルの作成

「新規」(📄 新規) をクリックすると、セキュリティプロファイルウィザードが開き、新規プロファイルの名前の入力が必要になります。入力後、「セキュリティプロファイル詳細」画面を開くためのオプションが表示されます。「詳細」(🔍) をクリックすると、「セキュリティプロファイル詳細」画面が表示されます。

注意： 新規セキュリティプロファイルは、コンピュータの推奨設定の検索結果に基づき作成できます。実行するには、「コンピュータ」画面でコンピュータを右クリックして、「処理」→「推奨設定の検索」を選択します。検索が終了したら、「セキュリティプロファイル」画面に戻り、「新規」をクリックして新規セキュリティプロファイルウィザードを起動します。プロンプトが表示されたら、新規セキュリティプロファイルを「既存のコンピュータの現行設定」にします。次に、コンピュータのプロパティから「推奨されるアプリケーションの種類と DPI ルール」を選択します。

注意： セキュリティプロファイルは、現在コンピュータにどのようなルールが割り当てられているとしても、そのコンピュータの推奨エレメントのみで構成されます。

セキュリティプロファイルの詳細の表示および編集

メインの「サーバプラグイン」画面は脆弱性対策オプションシステム全体のエレメントを管理および整理するのに対し、セキュリティプロファイルの「詳細」画面はサーバプラグインから利用可能なエレメントを選択して特定のセキュリティプロファイルへ適用することができます。

セキュリティプロファイルの「詳細」画面はメインの「サーバプラグイン」画面と似ていますが、「詳細」画面にある全エレメントはセキュリティプロファイルに対してのみ適用できます。初期設定では、すべての設定はメインの「サーバプラグイン」画面にあるグローバル設定を継承します。「セキュリティプロファイル」画面での変更は、そのセキュリティプロファイルにのみ適用されます。メインの「サーバプラグイン」画面において、ファイアウォールルールや DPI ルールといったエレメントのプロパティの修正は、「プロパティ」でのみ行えます。セキュリティプロファイルの「詳細」にあるエレメントのプロパティを修正する場合は、追加オプションの「プロパティ (このセキュリティプロファイル用)」を使用します。



図 7-1. セキュリティプロファイルの詳細

「プロパティ (このセキュリティプロファイル用)」を修正した場合、その変更内容は、このセキュリティプロファイルによりコンピュータに適用されるエレメントのみに反映されます。

「プロパティ」を修正した場合は、他で優先されていないかぎり、エレメントに対しグローバルに反映されます。

プロパティが修正されたエレメントでは、タスク画面に太字で「このセキュリティプロファイル用」と表示され、このセキュリティプロファイルがコンピュータに適用されたときの特別なプロパティが存在することを明示します。

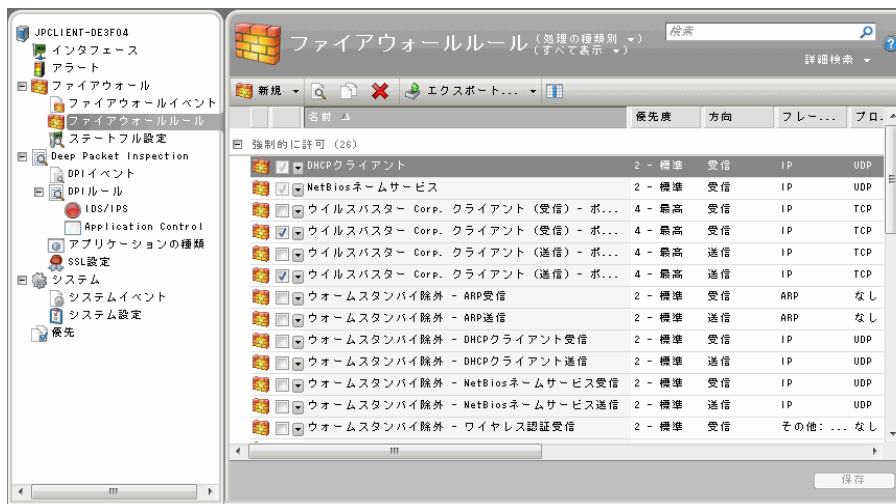


図 7-2. プロパティ (このセキュリティプロファイル用)

セキュリティプロファイルを表示または編集する方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「セキュリティプロファイル」

1. 表示または編集するプロファイルを選択して をクリックするか、そのプロファイルを右クリックして「詳細 ...」を選択します。
2. 「詳細」画面でナビゲーション画面を使用して画面を移動し、以下のように目的の変更を実行します。

- **インタフェースの種類**: コンピュータに複数のインタフェースがある場合は、ファイアウォールルールなどのセキュリティプロファイルの各種エレメントを各インタフェースに割り当てることができます。

複数のインタフェースに対してセキュリティプロファイルを設定するには、「複数のインタフェースの割り当て」を選択して、下のフィールドに名前とパターン照合文字列を入力します。

インタフェースの種類の名前は、参照用でのみ使用されます。一般的な名前としては「LAN」、「WAN」、「DMZ」、「Wi-Fi」などがありますが、任意の名前を使用してネットワークのトポロジにマッピングできます。

パターン照合ではワイルドカードによるインタフェース名の照合ができ、インタフェースを適切な種類へ自動マッピングします。たとえば、「ローカルエリア接続*」、「eth*」、および「Wireless*」などです。自動でインタフェースをマッピングできないときは、アラートがトリガされます。その際は、コンピュータの「詳細」画面にある「インタフェース」画面から手動でマッピングできます。

注意： コンピュータ上でインタフェースが検出されても、これらのエントリと一致しない場合、サーバプラグインはアラートをトリガします。

- **アラート：**アラートはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのセキュリティプロファイルを使用するコンピュータに関するアラートのみです。ここでアラートを消去すると、メインの「サーバプラグイン」画面からも消去されます。
- **ファイアウォール (イベント、ルール、ステートフル設定)：**セキュリティプロファイルのファイアウォールは、優先しないかぎり、サーバプラグインのグローバル設定にあるステートフル設定 (オン / オフ) を継承します。

注意： ファイアウォールをオフに切り替えてセキュリティプロファイルをコンピュータに適用し、そのコンピュータがファイアウォール設定を継承するように設定されている場合、そのコンピュータでは、セキュリティプロファイルが適用される前に直接コンピュータに割り当てられたエレメントであっても、すべてのファイアウォールエレメント (ファイアウォールルールとステートフル設定) がオフになります。

- **イベント：**ファイアウォールイベントはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのセキュリティプロファイルを使用するコンピュータに関するイベントのみです。

- ルール**: サーバプラグインで定義されるファイアウォールルールは、ここに表示されます。このセキュリティプロファイルで有効にするルールを選択します。上記のセキュリティプロファイルに対して複数のインタフェースを定義した場合は、灰色のドロップダウンメニューでファイアウォールルールを全インタフェースに適用するか、それとも特定のインタフェースにのみ適用するかを選択します。

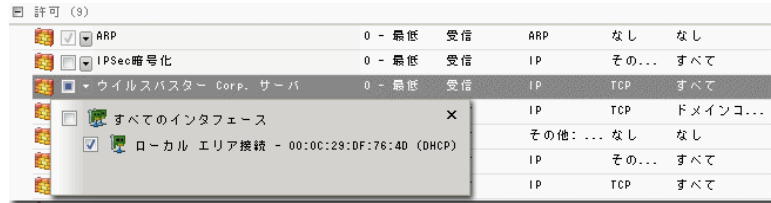


図 7-3. プロパティ (このセキュリティプロファイル用)

- ステートフル設定**: このセキュリティプロファイルに適用するステートフル設定を選択します。上記のセキュリティプロファイルに対して複数のインタフェースを定義した場合は、各インタフェースに対して個別にステートフル設定することができます。
- Deep Packet Inspection (イベント、ルールやアプリケーションの種類)**: セキュリティプロファイルの DPI エンジン、優先するよう選択しないかぎり、グローバル設定またはセキュリティプロファイル設定にあるステートフル設定 (オン/オフ)、インライン動作、推奨設定の検索を継承します。
 - イベント**: DPI イベントはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのセキュリティプロファイルを使用するコンピュータに関するイベントのみです。
 - ルール**: サーバプラグインで定義される DPI ルールは、ここに表示されます。このセキュリティプロファイルで有効にするルールを選択します。上記のセキュリティプロファイルに対して複数のインタフェースを定義した場合は、灰色のドロップダウンメニューで DPI ルールを全インタフェースに適用するか、それとも特定のインタフェースにのみ適用するかを選択します。
 - アプリケーションの種類**: サーバプラグインで定義されるアプリケーションの種類は、ここに表示されます。セキュリティプロファイルレベルのその他のエレメントと同様に、これらのプロパティはグローバルに修正したり、またはこのセキュリティプロファイルに対してのみ修正したりすることができます。

- システム：
 - イベント (コンピュータ用): システムイベントはサーバプラグインのメイン画面と同様の方法で表示されますが、表示内容はこのセキュリティプロファイルを使用するコンピュータに関するイベントのみです。
 - イベント (セキュリティプロファイル用): このセキュリティプロファイルで作成、修正されたシステムイベントは、この画面に表示されます。
 - システム設定: サーバプラグインの全システム設定は、ここに表示されている特定のセキュリティプロファイルに優先できます。
 - 優先: 「優先」には、セキュリティプロファイルに対して優先されたエレメントが表示されます。
3. 「保存」をクリックします。

脆弱性対策オプションを使用する

この章では、脆弱性対策オプション™ 1.5 ファイアウォールについて説明します。

この章で扱うトピックは次のとおりです。

- 84 ページの「脆弱性対策オプションについて」
- 84 ページの「ファイアウォールのオンとオフを切り替えます」
- 84 ページの「ファイアウォールイベント」
- 90 ページの「ファイアウォールルール」
- 105 ページの「ステートフル設定」

脆弱性対策オプションについて

脆弱性対策オプションは、ネットワーク上のクライアントとサーバを保護します。脆弱性対策オプションサーバプラグインインタフェースには、ファイアウォールイベント、ファイアウォールルール、ステートフル設定を管理する画面が用意されています。初期設定では、ハートビートごとにクライアントプラグインからファイアウォールログと DPI イベントログがサーバプラグインで収集されます。ファイアウォールルールでパケットの制御情報を検査し、ルールに基づいてこれらのパケットをブロックまたは許可できます。脆弱性対策オプションのステートフル設定メカニズムでは、トラフィック履歴との関連におけるパケット、TCP および IP ヘッダ値の正当性、および TCP 接続状態の推移が分析されます。

ファイアウォールのオンとオフを切り替えます

ファイアウォールのオンとオフを切り替えるには

パス: [脆弱性対策オプションメインメニュー](#) | 「ファイアウォール」

1. 「ファイアウォール」エリアで、「オン」または「オフ」にします。

情報エリアには、ネットワークエンジンがインラインモードとタップモードのどちらで動作しているかが表示されます。インラインモードで動作する場合、実際のパケットストリームはネットワークエンジンを通過します。ステートフルテーブルは維持され、ファイアウォールルールは適用され、侵入防御ルールがペイロードコンテンツに適用されるようトラフィックの正規化が実行されます。タップモードで動作する場合、実際のパケットストリームはクローン化され、メインストリームを迂回して流れます。タップモードでは、実際のパケットストリームは変更されません。すべての操作はクローン化されたストリーム上で行われます。





2. インラインモードとタップモードを切り替えるには、「システム」→「システム設定」→「ファイアウォールと DPI」に進んでください。

ファイアウォールイベント

初期設定では、ハートビートごとにクライアントプラグインからファイアウォールログと DPI イベントログがサーバプラグインで収集されます（これは、「システム」→「システム設定」画面の「ファイアウォールと DPI」タブでオフにできます）。ログのデータを使用して、サーバプラグインの各種レポート、グラフ、およびチャートが作成されます。

イベントログは、サーバプラグインによって収集された後、「システム」→「システム設定」画面の「システム」タブで設定された一定の期間保持されます。

「ファイアウォールイベント」画面に、現在のファイアウォールイベントが次の情報列と共に表示されます。

- **ファイアウォールイベントのアイコン**: イベントの種類を示します。イベントは次のいずれかです。
 -  単一イベント
 -  データ付き単一イベント
 -  折りたたみイベント
 -  データ付き折りたたみイベント

注意: イベントの折りたたみは、同じ種類のイベントが数回続けて発生したときに実行されます。これによりディスク容量を節約でき、ログメカニズムに負荷をかける DoS 攻撃から防御することができます。

- **時刻**: コンピュータ上でイベントが発生した時刻。
- **コンピュータ**: このイベントのログが記録されたコンピュータ。(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます。)
- **理由**: この画面のログエントリが、ファイアウォールルールによって生成されたか、またはステートフル設定によって生成されたかを示します。エントリがファイアウォールルールによって生成された場合、列エントリには、「ファイアウォールルール:」と表示され、続いてファイアウォールルールの名前が表示されます。それ以外の場合、列エントリには、ログエントリを生成したステートフル設定の内容が表示されます。
- **タグ**: イベントに関連付けられたタグ。
- **処理**: ファイアウォールルールまたはステートフル設定によって実行された処理。処理には、許可、拒否、強制的に許可、ログのみがあります。
- **ランク**: ランク付けシステムでは、DPI およびファイアウォールイベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、DPI ルールとファイアウォールルールに「重要度」を割り当て、これら 2 つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、DPI イベントまたはファイアウォールイベントを表示するときに、イベントをランクでソートできます。
- **方向**: 影響を受けるパケットの方向 (受信または送信)。
- **インタフェース**: パケットが経由するインタフェースの MAC アドレス。
- **フレームの種類**: 対象となるパケットのフレームの種類。値は、「IP」、「ARP」、「REVARP」、および「その他:XXXX」(XXXX はフレームの種類を示す 4 桁の 16 進コード) のいずれかになります。

- **プロトコル**: 値は、「ICMP」、「IGMP」、「GGP」、「TCP」、「PUP」、「UDP」、「IDP」、「ND」、「RAW」、「TCP+UDP」、「N/A」、「その他: nnn」(nnn は、3 桁の 10 進値) のいずれかになります。
- **フラグ**: パケットに設定されたフラグ。
- **送信元 IP**: パケットの送信元 IP です。
- **送信元 MAC**: パケットの送信元 MAC アドレス。
- **送信元ポート**: パケットの送信元ポート。
- **送信先 IP**: パケットの送信先 IP。
- **送信先 MAC**: パケットの送信先 MAC アドレス。
- **送信先ポート**: パケットの送信先ポート。
- **パケットサイズ**: バイト単位のパケットのサイズ。

注意: ログのみルールは、対象のパケットが、拒否ルールまたはそのパケットを除外する許可ルールによって、それ以降に停止されない場合にログエントリのみを生成します。この 2 つのルールのいずれかによってパケットが停止される場合は、ログのみルールではなく、これらのルールがログエントリを生成します。以降のルールでパケットを停止しない場合は、ログのみルールがエントリを生成します。

「ファイアウォールイベント」画面から、次のことを実行できます。

- 特定のイベントのプロパティを表示 (🔍) する
- リストをフィルタする: イベントのリストをフィルタするには、「期間」および「コンピュータ」ツールバーを使用します。
- イベントリストのデータを CSV ファイルにエクスポート (📄) する
- 特定のイベントを検索 (🔍) する

さらに、ログエントリを右クリックすると、次のオプションが表示されます。

- **タグの追加**: イベントタグをこのイベントに追加します (「168 ページの「イベントのタグ付け」を参照してください)。
- **タグの削除**: 既存のイベントタグを削除します。
- **コンピュータの詳細**: ログエントリを生成したコンピュータの「詳細」画面を表示します。
- **ファイアウォールルールプロパティ**: このイベントに関連付けられたファイアウォールルールのプロパティを表示します。
- **Whois 送信元 IP**: 送信元 IP に対して whois を実行します。
- **Whois 送信先 IP**: 送信先 IP に対して whois クエリを実行します。

DPI イベントのプロパティを表示する

イベントをダブルクリックすると、そのエントリの「プロパティ」画面が表示され、画面上のイベントに関するすべての情報が表示されます。「タグ」タブには、このイベントに関連付けられているタグが表示されます。イベントのタグ付けを設定するには、「システム」>「タグ」に移動します。イベントのタグ付けの詳細については、「168 ページの「イベントのタグ付け」」を参照してください。

リストをフィルタし、イベントを検索する

「詳細検索」ドロップダウンメニューから「詳細検索を開く」を選択すると、詳細検索オプションが表示されます。

「期間」ツールバーを使用してリストをフィルタし、特定の期間内に発生したイベントだけを表示できます。

「コンピュータ」ツールバーを使用すると、コンピュータドメイン別またはコンピュータセキュリティプロファイル別にイベントログエントリの表示を整理できます。

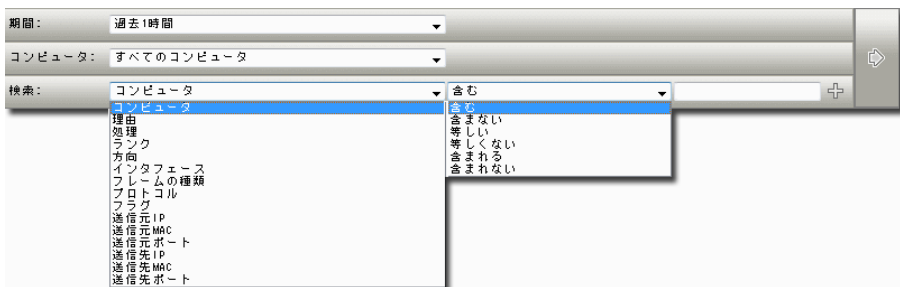


図 8-1. 「コンピュータ」ツールバー

詳細検索機能 (大文字 / 小文字の区別なし):

- **含む**: 選択した列の入力内容に検索文字列が含まれる
- **含まない**: 選択した列の入力内容に検索文字列が含まれない
- **等しい**: 選択した列の入力内容と検索文字列が完全に一致する
- **等しくない**: 選択した列の入力内容が検索文字列と完全には一致しない

- ・ **含まれる** : 選択した列の入力内容がカンマ区切りで入力された検索文字列 1 つと完全に一致する
- ・ **含まれない** : 選択した列の入力内容がカンマ区切りで入力されたどの検索文字列とも完全に一致しない

検索バーの右側にある「プラス」ボタン (+) をクリックすると、追加の検索バーが表示され、検索に複数のパラメータを適用できます。準備が整ったら、送信ボタンをクリックします (ツールバーの右側にある上部に右矢印の付いたボタン)。

イベントをエクスポートする

「エクスポート ...」 ボタンをクリックして、すべてのイベントまたは選択されたイベントを CSV ファイルへエクスポートします。

ファイアウォールイベントにタグを付ける

イベントのタグ付けでは、ファイアウォールイベントにカスタムのラベル (「これは Tom が再確認」など) を手動でタグ付けできます。イベントのタグ付けを使用すると、イベントの特殊なビュー、ダッシュボード、およびレポートが有効になります。また、イベントのタグ付けは単一イベント、類似する複数のイベント、または将来的に発生する同様のすべてのイベントに適用できます。

タグを 1 つまたは複数の選択したイベントに適用するには :

パス : [脆弱性対策オプションメインメニュー](#) | [「ファイアウォール」](#) > [「ファイアウォールイベント」](#)

1. 「イベント」リストでイベントを選択してから右クリックして「**タグを追加 ...**」を選択します。
2. タグの名前を入力します (文字を入力していくと、一致する既存のタグが候補として表示されます)。
3. 「**選択された 1 個のシステムイベント**」を選択します。(「イベント」リストから複数のイベントを選択した場合、選択したイベントの数が表示されます。)「**次へ**」をクリックします。
4. 必要に応じてコメントを記入し、「**完了**」をクリックします。

「イベント」リストで、イベントにタグが付けられたことを確認できます。

複数の同様のイベントにタグを付けるには

1. 「イベント」リストの中からベースにするイベントを右クリックし、「**タグを追加 ...**」をクリックします。
2. タグの名前を入力します (文字を入力していくと、一致する既存のタグが候補として表示されます)。

3. 「類似のファイアウォールイベントにも適用」を選択します。
4. イベントの選択を絞る場合は、「詳細オプションを含める」を選択します。
5. 「次へ」をクリックします。
6. 詳細オプションを選択した場合は、選択を行います。たとえば、特定のコンピュータまたはコンピュータドメインに限定して類似するイベントを表示できます。この場合は、該当するイベントを選択して、「次へ」をクリックします。
7. イベントが同様のものかどうかの判定基準となる属性を選択します。ほとんどの場合、属性オプションは「イベント」リスト画面の列に表示される情報と同じです。イベントの選択処理に含めるための属性を選択したら、「次へ」をクリックします。
8. このルールを適用する類似ファイアウォールイベントの種類を選択してください。

注意：「自動タグルールの保存」オプションについて。指定した選択条件を保存すると、将来、新しいイベントが増えたときに、その条件を適用することができます。保存した自動タグ付けルールは、「システム」>「タグ」画面で確認できます。

9. 「次へ」をクリックします。
10. 必要に応じてコメントを記入し、「次へ」をクリックします。
11. イベントの選択条件を概要で確認し、「完了」をクリックします。

「イベント」リストで、ベースにしたイベントおよび同様のすべてのイベントにタグが付けられていることを確認できます。

複数の同様のイベントおよび将来の同様のイベントにタグを付けるには

複数の同様のイベントや将来の同様のイベントにタグ付けする手順は、上記の手順と、手順8を除いて同じです。手順8では「新規ファイアウォールイベント」も選択します。「新規ファイアウォールイベント」を選択すると、脆弱性対策オプションサーバプラグインは5秒（またはそれ以上）ごとにデータベースを検索して新しいイベントを探し、該当するイベントにタグを付けます。

注意： タグ付けが実行されるのは、クライアントプラグインから取得されたイベントが脆弱性対策オプションサーバプラグインのデータベースに登録された後です。

ファイアウォールルール

ファイアウォールルールは、個々のパケットの管理情報を確認します。これらの画面に定義されたルールに基づいて、パケットをブロックまたは許可します。ファイアウォールルールは、直接、コンピュータまたはセキュリティプロファイルに割り当てられ、さらに、コンピュータまたはコンピュータ全体に割り当てられます。

ファイアウォールルールについて

脆弱性対策オプションルールには、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、脆弱性対策オプションルールは、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、定義された順序や割り当てられた順序とは無関係です。

ルール処理

各ルールには、以下の処理のいずれかを設定できます。

- **放置**: パケットが放置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 DPI エンジンを通過します。
- **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。
- **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。
- **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。
- **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か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。

許可ルールを追加すると、他のすべてのルールが拒否されます。

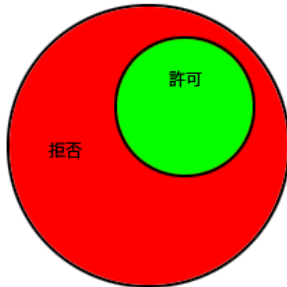


図 8-2. 許可ルール

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。

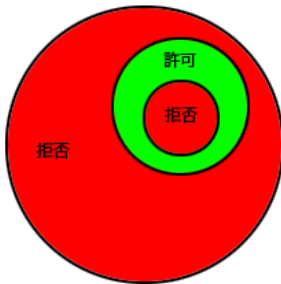


図 8-3. 拒否ルール

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。

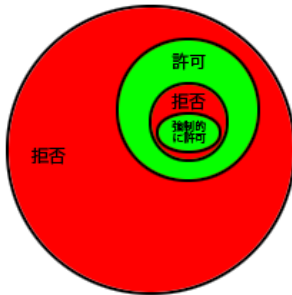


図 8-4. 強制的に許可ルール

ルール優先度

拒否および強制的に許可のルール処理を 5 つの優先度のいずれかで定義できます。これにより、許可されるトラフィックを許可ルールのセットでさらに細かく定義できます。ルールは、最高 (優先度 4) から最低 (優先度 0) の順に実行されます。特定の優先度内では、ルール処理 (強制的に許可、拒否、許可、ログのみ) に基づいた順序で処理されます。

優先度のコンテキストによって、拒否 / 強制的に許可の組み合わせを使用してトラフィック管理をさらに詳細に定義することが可能になるため、柔軟性に優れた処理を実現できます。同じ優先度のコンテキスト内では、拒否ルールによって許可ルールを無効にし、また、強制的に許可ルールによって拒否ルールを無効にすることもできます。

注意： 許可のルール処理は優先度 0 でのみ動作し、ログのみのルール処理は優先度 4 でのみ動作します。

ルール処理およびルール優先度を集約する

ルールは、最高 (優先度 4) から最低 (優先度 0) の順に実行されます。特定の優先度内では、ルール処理に基づいた順序で処理されます。同じ優先度のルールが処理される順序は次のとおりです。

- 放置
- ログのみ
- 強制的に許可

- 拒否
- 許可

注意： 許可のルール処理は優先度 0 でのみ動作し、ログのみのルール処理は優先度 4 でのみ動作します。

注意： 強制的に許可ルールと拒否ルールが同等の優先度の場合、強制的に許可ルールが拒否ルールよりも優先されるので、強制的に許可ルールと一致するトラフィックが許可されます。

ステートフルフィルタ

ステートフル分析が有効になっている場合は、トラフィック履歴のコンテキスト、TCP および IP ヘッダ値の正当性、および TCP 接続状態の変化の範囲内でパケットが分析されます。UDP や ICMP などのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフル機能が実装されます。

- 静的ルールで明確に許可されている場合、パケットはステートフルルーチンを通過します。
- パケットが既存の接続に属しているかどうかは、接続テーブルでエンドポイントと一致するかどうかを確認することによって調査されます。
- TCP ヘッダの正当性 (シーケンス番号、フラグの組み合わせなど) が調査されます。

ステートフルエンジンが有効になると、インタフェースを横断するすべてのトラフィックに適用されます。

UDP の擬似ステートフルインスペクションは、初期設定で「未承諾」の UDP パケットの受信を拒否します。コンピュータで UDP サーバを実行している場合は、強制的に許可ルールをポリシーに設定してサーバへのアクセスを許可する必要があります。たとえば、UDP のステートフルインスペクションが DNS サーバで有効になっている場合は、53 番ポートに対する UDP トラフィックを許可する強制的に許可ルールが必要です。

ICMP の擬似ステートフルインスペクションは、初期設定で、未承諾の ICMP 要求 / 応答およびエラーパケットの受信を拒否します。未承諾の ICMP パケットを許可するには、強制的に許可ルールを明確に定義する必要があります。静的ルールで明確に許可されていなければ、要求 / 応答やエラータイプではないその他すべての ICMP パケットは破棄されます。

放置ルール

放置ルールという特別な種類のファイアウォールルールがあります。フィルタリングを望まないメディア集約プロトコルのために設計されています。放置ルールを作成するには、新しいファイアウォールルールを作成するときルールの「処理」として「放置」を選択します。

ファイアウォールルールの「放置」処理は、次の点で強制的に許可ルールとは異なります。

- 放置ルールと一致するパケットは、DPI ルールで処理されません。
- 強制的に許可ルールとは異なり、ステートフル設定がオンになっている場合、放置ルールは TCP 接続での応答を自動的に許可しません (詳細については、下記を参照してください)。
- 放置ルールの中には最適化されているものもあり、クライアントプラグインが存在しないかのように効率的にトラフィックが流れます (詳細については、下記を参照してください)。

注意： ファイアウォールルールの放置がバージョン 5.0 以前のクライアントプラグインに送信されると、強制的に許可ルールと同等に扱われ、DPI ルールの処理をスキップしません。

ステートフル設定の有効時に放置を使用する

放置ルールを使用して TCP 送信先ポートに対する受信トラフィックで DPI ルールをスキップし、ステートフル設定を設定して TCP でステートフルインスペクションを実行する場合は、送信元ポートの照合送信フィルタを必ず作成して TCP 応答を許可する必要があります。(これは強制的に許可ルールには必要はありません。強制的に許可されたトラフィックはステートフルエンジンによって処理されるためです。)

すべての放置ルールは単一方向です。トラフィックの各方向に対して明確なルールが必要です。

最適化

一致するトラフィックを可能なかぎり早く通過させるには、放置ルールを作成します。次の設定により、最大スループットを実現できます。

- **優先度:** 最高。
- **フレームの種類:** IP。
- **プロトコル:** TCP、UDP、またはその他の IP プロトコル (「任意」オプションは使用しないでください)。
- **送信元および送信先の IP および MAC:** すべて「任意」。

- プロトコルが TCP または UDP でトラフィックの方向が「受信」の場合は、送信先ポートを「任意」ではなく 1 つ以上指定する必要がある、送信元ポートを「任意」にする必要があります。
- プロトコルが TCP または UDP でトラフィックの方向が「送信」の場合は、送信元ポートを「任意」ではなく 1 つ以上指定する必要がある、送信先ポートを「任意」にする必要があります。
- **予約**: なし。

ログ

放置ルールに一致するパケットはログに記録されません。このオプションは設定できません。

ファイアウォールルールのシーケンス

クライアントプラグインを実行している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、ステートフル設定条件、および DPI 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
 - a. 放置
 - b. 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)
 - c. 強制的に許可
 - d. 拒否
2. 優先度 3 (高) のファイアウォールルール
 - a. 放置
 - b. 強制的に許可
 - c. 拒否
3. 優先度 2 (中) のファイアウォールルール
 - a. 放置
 - b. 強制的に許可
 - c. 拒否
4. 優先度 1 (低) のファイアウォールルール
 - a. 放置
 - b. 強制的に許可
 - c. 拒否

5. 優先度 0 (最低) のファイアウォールルール

- a. 放置
- b. 強制的に許可
- c. 拒否
- d. 許可 (許可ルールは優先度 0 (最低) にのみ割り当て可能なことに注意してください)

同じ優先度のコンテキスト内では、拒否ルールが許可ルールに優先し、強制的に許可ルールが拒否ルールに優先します。ルールの優先度システムを使用すると、優先度の低い強制的に許可ルールよりも優先度の高い拒否ルールを優先することができます。

強制的に許可ルールを使用して TCP/UDP ポート 53 の受信 DNS クエリをすべて許可する DNS サーバのポリシーの例について考えてみます。この場合、強制的に許可ルールよりも優先度の高い拒否ルールを作成することによって、特定範囲の IP アドレスを指定して、同一の公開サーバへのアクセスを禁止する必要があります。

優先度に基づいたルール設定によって、ルールを適用する順序を設定できます。拒否ルールに最も高い優先度を設定し、同じ優先度の強制的に許可ルールがない場合、拒否ルールに一致するパケットはすべて自動的に破棄されて残りのルールは無視されます。反対に、強制的に許可ルールに最も高い優先度が設定されている場合、強制的に許可ルールに一致する受信パケットは他のルールに対して確認されることなくすべて自動的に許可されます。

ログに関する注意

放置ルールはログエントリを生成しません。これは設定できません。

ログのみルールは、対象のパケットが、次のいずれかのルールによって、それ以降に停止されない場合にログエントリのみを生成します。

- 拒否ルール
- そのパケットを除外する許可ルール

この 2 つのルールのいずれかがパケットを停止する場合は、ログのみルールではなくこれらのルールによって、ログエントリが生成されます。以降のルールでパケットを停止しない場合は、ログのみルールがエントリを生成します。

ファイアウォールポリシーをまとめて設計する

一般的に、コンピュータのファイアウォールポリシーを定義するには次の2つの方法があります。

- **禁止**: 明確に許可されていないトラフィックを禁止します。許可するトラフィックを記述した許可ルールと許可するトラフィックをさらに制限した拒否ルールの組み合わせを使用することによって、禁止ポリシーを作成できます。
- **許可**: 明確に禁止されていないトラフィックを許可します。破棄する必要のあるトラフィックを記述した拒否ルールを例外的に使用することによって許可ポリシーを作成できます。

通常、禁止ポリシーを優先して許可ポリシーを使用しないようにします。

許可および拒否ルールで禁止されているトラフィックのサブセットを許可するには、許可および拒否ルールと連動して強制的に許可ルールを使用する必要があります。また、ICMP および UDP ステートフルが有効になっている際に、未承諾の ICMP および UDP トラフィックを許可するように強制的に許可ルールを設定する必要があります。

Web サーバ用の単純なファイアウォールポリシーを作成する方法の例を示します。

1. まず、オプションが有効になっているグローバルなステートフル設定を使用して、TCP、UDP、および ICMP のステートフルインスペクションを有効にします。
2. ワークステーションからの要求に対する TCP および UDP の応答を許可するファイアウォールルールを追加します。そのためには、受信許可ルールを作成してプロトコルセットを「TCP+UDP」に設定し、「指定フラグ」の下にある「なし」チェックボックスと「Syn」チェックボックスをオンにします。この時点で、ワークステーションのユーザからの要求に応答する TCP と UDP のパケットだけがポリシーによって許可されます。たとえば、手順 1 で有効にしたステートフル分析オプションと連動してこのルールを使用すると、コンピュータのユーザは DNS 検索 (UDP 経由) や HTTP (TCP 経由) の Web 閲覧ができるようになります。
3. ワークステーションからの要求に ICMP 応答を許可するファイアウォールルールを追加します。そのためには、プロトコルを「ICMP」に設定した受信許可ルールを作成し、「任意のフラグ」チェックボックスをオンにします。このコンピュータのユーザは別のワークステーションに ping を送信して応答を受信できますが、他のユーザはこのコンピュータに ping を送信できなくなります。
4. 「指定フラグ」セクションの「Syn」チェックボックスをオンにして、受信 TCP トラフィックをポート 80 およびポート 443 に対して許可するファイアウォールルールを追加します。外部ユーザがこのコンピュータの Web サーバにアクセスできるようになります。

この時点で、他の受信トラフィックをすべて拒否するコンピュータで、承諾された TCP、UDP、および ICMP 応答と Web サーバへの外部アクセスを許可する基本的なファイアウォールポリシーが設定されます。

拒否および強制的に許可ルール of 処理を使用してこのプロファイルをさらに詳細に定義する方法の例について、ネットワーク内の他のコンピュータからのトラフィックを制限する方法を考察します。たとえば、内部ユーザに対してはこのコンピュータの Web サーバへのアクセスを許可し、DMZ にあるコンピュータからのアクセスは拒否するものとします。この場合、DMZ の IP 範囲にあるサーバからのアクセスを禁止する拒否ルールを追加することによって設定が可能になります。

- 次に、送信元 IP 10.0.0.0/24 (DMZ 内のコンピュータに割り当てられた IP 範囲) を使用して、受信 TCP トラフィック用に拒否ルールを追加します。このルールでは、DMZ 内にあるコンピュータからこのコンピュータへのトラフィックをすべて拒否します。

ただし、このポリシーをさらに詳細に定義すると DMZ 内にあるメールサーバからの受信トラフィックを許可できます。

- そのためには、送信元 IP アドレス 10.0.0.100 からの受信 TCP トラフィックに強制的に許可ルールを使用します。この強制的に許可ルールは、前の手順で作成した拒否ルールよりも優先して DMZ 内にあるコンピュータからのトラフィックを許可します。

重要事項



- すべてのトラフィックは、まずファイアウォールルールと照合されてからステートフルインスペクションエンジンで分析されます。トラフィックがファイアウォールルールを通過した場合は、ステートフルインスペクションエンジンによって分析されます (ステートフルインスペクションがステートフル設定で有効になっているものとします)。
- 許可ルールは暗黙の拒否ルールを含んでいます。許可ルールで指定されていないトラフィックは自動的に破棄されます。このルールには他の種類のフレームのトラフィックが含まれるため、他のフレームの種類の必要なトラフィックを許可するルールを含める必要があります。たとえば、静的 ARP テーブルを使用していない場合には ARP トラフィックを許可するルールを忘れずに含める必要があります。
- UDP のステートフルインスペクションが有効になっている場合は、強制的に許可ルールを使用して未承諾の UDP トラフィックを許可する必要があります。たとえば、UDP ステートフルが DNS サーバで有効になっている場合に、サーバが受信 DNS 要求を受け入れるように、強制的に許可ルールをポート 53 に設定する必要があります。
- ICMP のステートフルインスペクションが有効になっている場合は、強制的に許可を使用して未承諾の ICMP トラフィックを許可する必要があります。たとえば、外部の ping 要求を許可する場合は、ICMP タイプ 3 (エコー要求) を強制的に許可するルールが必要です。

- ・ 強制的に許可の処理は、同じ優先度のコンテキスト内でのみ切り札として機能します。
- ・ テスト環境でよく見られるように DNS または WINS サーバが設定されていない場合は、受信の UDP ポート 137 を強制的に許可するルールが NetBios に必要となることがあります。

注意： 新しいファイアウォールポリシーのトラブルシューティング時は、まずクライアントプラグインにあるファイアウォールルールのログを確認してください。ファイアウォールルールのログには、ファイアウォールのエレメントによって拒否しているトラフィックを判断するために必要な情報がすべて含まれています。ファイアウォールのエレメントは、必要に応じてポリシーを詳細に設定できるように定義されています。

新規ファイアウォールルールを作成および適用する

「ファイアウォールルール」画面で、ファイアウォールルールを表示、作成、編集できます。画面には、現在のファイアウォールルールが、以下を含む情報列と共に一覧表示されます。

- ・ **ファイアウォールアイコン：**ルールごとに以下を示します。
 -  通常のファイアウォールルール
 -  スケジュールに従って動作するファイアウォールルール
- ・ **処理：**クライアントプラグインが実行する処理は次のとおりです。ルール条件に一致すれば、他のルールがブロックしていても、パケットを許可する（「強制的に許可」）、ルール条件に一致するパケットをブロックする（「拒否」）、ルール条件に一致するパケットのみを排他的に許可してその他すべてをブロックする（「許可」）、またはルール条件に一致するパケットをログに記録して通過させる（「ログのみ」）。優先度レベル内でルールは次の順序で適用されます。（優先レベルについては後の項目を参照してください。）
 - a. 「放置」
 - b. 「強制的に許可」
 - c. 「拒否」
 - d. 「許可」
 - e. 「ログのみ」
- ・ **優先度：**ファイアウォールルールには 0（最低）から 4（最高）の優先度があります。優先度の高いルールが最初に適用されます。
- ・ **パケットの方向：**パケットの受信または送信です。
- ・ **パケット送信元：**フレームの種類、プロトコル、IP、ポート、フラグなど、パケットの送信元を表すすべての情報です。

- **パケット送信先**: フレームの種類、プロトコル、IP、ポート、フラグなど、パケットの送信先を表すすべての情報です。
- **指定フラグ**: トリガするルールについて、いずれのフラグを設定するかを指定します。(フラグはプロトコルによって異なります。)

「ファイアウォールルール」画面から、次のことを実行できます。

- 新規ファイアウォールルールを作成する (📄 新規)
- XML ファイルからファイアウォールルールをインポートする (📄)
- 既存のファイアウォールルールのプロパティを確認または変更する (🔍)
- 既存のファイアウォールルールを複製 (および変更) する (📄)
- ファイアウォールルールを削除する (✖)
- 1つ以上のファイアウォールルールをXMLファイルにエクスポート (📄) する (「エクスポート...」ボタンをクリックしてすべてのIPリストをエクスポートするか、ドロップダウンリストで選択して、選択または表示されたIPリストのみをエクスポートする)

注意: 1台以上のコンピュータに割り当てられたファイアウォールルール、またはセキュリティプロファイルの一部であるファイアウォールルールは削除できません。

「新規」(📄 新規) または「プロパティ」(🔍) をクリックして、「ファイアウォールルールのプロパティ」画面を表示します。

ファイアウォールルールを作成または編集するには

パス: 脆弱性対策オプションメインメニュー | 「ファイアウォール」 > 「ファイアウォールルール」

1. 「📄 新規」をクリックして新規ファイアウォールルールを作成するか、既存のファイアウォールルールを選択して「プロパティ」(🔍) を選択し、ファイアウォールルールを変更します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - **名前**: ファイアウォールルールの名前。
 - **説明**: ファイアウォールルールの詳細な説明。

- **処理**: ファイアウォールルールによって、4つの異なる処理が可能です。これらについて、次に順を追って説明します。
 - ファイアウォールでは、トラフィックの放置 (バイパス) が可能です。これは、パケットがファイアウォールと DPI エンジンですべて迂回できるようにするための特別なルールです。この設定は、フィルタリングを望まないメディア集約プロトコルのために設計されています。放置ルールの詳細については、「94 ページの「放置ルール」」を参照してください。
 - ログのみが可能です。つまり、ログにエントリを作成するだけで、トラフィックに干渉しません。
 - 定義済みのトラフィックを強制的に許可できます (他のトラフィックを除外することなく、このルールによって定義されたトラフィックを許可できます)。
 - トラフィックの拒否が可能です (このルールによって定義されたトラフィックを拒否します)。
 - トラフィックの許可が可能です (このフィルタによって定義されたトラフィックを例外的に許可します)。

注意: 特定の packets に適用されるのは、1つのルール処理だけです。同じ優先度のルールが複数ある場合は、上記の順序で適用されます。

- **優先度**: 「強制的に許可」、「拒否」、または「ログのみ」をルール処理として選択した場合、ここで優先度を 0 (低) から 4 (最高) まで設定できます。優先度を設定すると、ルール処理を組み合わせ、階層型のルール効果を実現できます。ログのみルールでの優先度は 4 のみ設定でき、許可ルールでは 0 のみが設定できます。

注意: 優先度により、ルールが適用される順序を決定します。優先度の低いルールよりも先に優先度の高いルールが適用されます。たとえば、ポート 80 の受信を強制的に許可する優先度 2 のルールが適用されるより前に、ポート 80 の受信を拒否する優先度 3 のルールが適用され、パケットを破棄します。

- **パケットの方向**: このルールが受信または送信のどちらのトラフィックに適用されるかを選択します。

- ・ **フレームの種類**: 使用しているルールが検索するフレームの種類を選択または指定します。このチェックボックスを使用して、このフレームの種類をフィルタリングするのか、このフレーム以外の種類をフィルタリングするのかを指定します。

注意: フレームの種類のリストについては、Internet Assigned Numbers Authority (IANA) の Web サイトを参照してください。

- ・ **プロトコル**: ルールで検索するプロトコルを選択または指定します。このチェックボックスを使用して、このプロトコルをフィルタするのか、またはこのプロトコル以外をフィルタするのかを指定します。

注意: 事前定義された共通プロトコルのドロップダウンリストから選択するか、「その他」を選択してプロトコル番号 (0 ~ 255 の 3 桁の 10 進値) を入力できます。

3. 「パケット送信元」エリアで、パケットのヘッダの送信元情報に適用するオプションを指定します。
 - ・ **IP**: IP アドレス、マスクされている IP アドレス、IP 範囲を指定するか、または「IP リスト」画面で定義した IP リストから選択します。
 - ・ **MAC**: MAC アドレスを指定するか、または「MAC リスト」画面で定義した MAC リストから選択します。
 - ・ **ポート**: ポートオプションで、カンマ区切りのポートリスト、ダッシュ区切りのポート範囲、または単一のポート (80、443、1-100 など) を指定するか、または「ポートリスト」画面で定義したポートリストから選択できます。
4. 「パケット送信先」エリアで、パケットのヘッダの送信先情報に適用するオプションを指定します。
 - ・ **IP**: IP アドレス、マスクされている IP アドレス、IP 範囲を指定するか、または「IP リスト」画面で定義した IP リストから選択します。
 - ・ **MAC**: MAC アドレスを指定するか、または「MAC リスト」画面で定義した MAC リストから選択します。
 - ・ **ポート**: ポートオプションで、カンマ区切りのポートリスト、ダッシュ区切りのポート範囲、または単一のポート (80、443、1-100 など) を指定するか、または「ポートリスト」画面で定義したポートリストから選択できます。
5. 前述の「一般情報」セクションでプロトコルに TCP、ICMP、または TCP+UDP を選択した場合、「指定フラグ」エリアで、特定のフラグを監視するようにファイアウォールルールに指示できます。

6. ポップアップウィンドウの「一般」タブの「一般情報」エリアに必要な情報を指定します。
7. 「オプション」タブをクリックして必要な情報を指定します。
 - ・ **アラート**: このファイアウォールルールがトリガされたときに、アラートを発令する必要があるかどうかを選択します。このルールを特定の期間だけ有効にする場合は、ドロップダウンリストのスケジュールを割り当てます。

注意: アラートをトリガするように設定できるのは、「処理」が「拒否」または「ログのみ」に設定されているファイアウォールルールのみです。(これは、アラートがカウンタによってトリガされるためです。カウンタはログファイルのデータを使用して増加します。)

- ・ **予約**: 予約された時間のみファイアウォールルールを有効化するかどうかを選択します。

注意: 予約された時間のみ有効になるファイアウォールルールは、「ファイアウォールルール」画面に、小さな時計が付いたアイコン () で表示されます。

- ・ **コンテキスト**: ルールコンテキストは、コンピュータのネットワーク環境に応じて異なるセキュリティポリシーを実装する強力な方法です。コンテキストは一般的に、コンピュータ (通常はモバイルノートパソコン) が社内または社外にあるかどうかで異なるファイアウォールや DPI ルールを適用するセキュリティプロファイルを作成するために使用します。コンテキストは、ファイアウォールルールと DPI ルールと関連付けられるよう設計されています。ルールに関連付けられたコンテキストの定義条件に一致した場合、ルールは適用されます。コンピュータの場所を決定するには、コンピュータがどのようにドメインコントローラと接続されているかコンテキストで検証します。コンテキストの詳細については、「146 ページの「コンテキスト」」を参照してください。

注意: コンテキストを使用したファイアウォールルールを実装するセキュリティプロファイルの例は、「Windows モバイルノートパソコン」セキュリティプロファイルのプロパティを参照してください。

8. 「割り当て対象」タブをクリックして、このファイアウォールルールおよびこのルールが直接適用されるすべてのコンピュータを含む、セキュリティプロファイルのリストを表示します。ファイアウォールルールは、「セキュリティプロファイル」画面のセキュリティプロファイルと、「コンピュータ」画面のコンピュータに割り当てることができます。
9. 「OK」をクリックします。

新しいファイアウォールルールをコンピュータに割り当てる必要があります。コンピュータに対するファイアウォールルールのアプリケーションを管理する最善の方法は、セキュリティプロファイルを使用することです。たとえば、「開発者のノートパソコン」というセキュリティプロファイルを設定することによって、「開発者のノートパソコン」というプロファイルが機能する特定の環境向けに設計されたファイアウォールルールを作成できます。その後、すべてを「開発者のノートパソコン」セキュリティプロファイルに割り当てて、そのセキュリティプロファイルを一連のコンピュータに割り当てます。「開発者のノートパソコン」プロファイルに新しいファイアウォールルールを作成および割り当てる必要がある場合は、セキュリティプロファイルに新しいルールを割り当てるとすべての「開発者のノートパソコン」コンピュータが新しいファイアウォールルールにアップデートされます。

セキュリティプロファイルに新しいファイアウォールルールを設定するには

パス: 脆弱性対策オプションメインメニュー | 「セキュリティプロファイル」

1. 新しいルールを割り当てるセキュリティプロファイルをダブルクリックします。プロファイルの「詳細」画面が開きます。
2. 左側のナビゲーション画面の「ファイアウォールルール」をクリックします。
3. リストから新しいファイアウォールルールを探して、チェックボックスをオンにします。
4. 「保存」をクリックします。

「システム」>「システム設定」画面の「コンピュータ」タブで「脆弱性対策オプションシステムの要素のいずれかを変更した後、該当するすべてのコンピュータは自動的にアップデートされます。」オプションを有効にした場合、そのセキュリティプロファイルが割り当てられたコンピュータすべてに新規ルールが適用されます。

新しいファイアウォールルールを直接コンピュータに割り当てるには

パス: メインメニュー | 「コンピュータ」

1. 新しいルールを割り当てるコンピュータをダブルクリックします。
2. 左側のナビゲーション画面の「ファイアウォールルール」をクリックします。
3. リストから新しいファイアウォールルールを探して、チェックボックスをオンにします。
4. 「保存」をクリックします。

前述したとおり、「システム」>「システム設定」画面の「コンピュータ」タブで「脆弱性対策オプションシステムの要素のいずれかを変更した後、該当するすべてのコンピュータは自動的にアップデートされます。」オプションを有効にした場合、そのセキュリティプロファイルが割り当てられたコンピュータすべてに新規ルールが適用されます。

注意： ファイアウォールの追加やステートフル設定の変更など、他の設定をコンピュータに適用する場合は、「コンピュータ」画面の「セキュリティプロファイル」列のセキュリティプロファイル名の横にアスタリスクが表示されます。このアスタリスクは、初期設定が変更されていることを示しています。

ステートフル設定

脆弱性対策オプションのステートフル設定メカニズムでは、トラフィック履歴との関連における各パケット、TCP および IP ヘッダ値の正当性、および TCP 接続状態の推移が分析されます。UDP や ICMP などのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実装されます。パケットは、ステートフルメカニズムによって次のように処理されます。

1. 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
2. パケットが既存の接続に属しているかどうかを判断するには、パケットの調査が実行されます。調査では、ステートフル機能によって作成された接続テーブルで、エンドポイントと一致するかどうかをチェックします。
3. TCP ヘッダの正当性 (シーケンス番号、フラグの組み合わせなど) が調査されます。

ステートフル設定を管理する

「ステートフル設定」画面では、複数のステートフルインスペクション設定を定義して、セキュリティプロファイルに含めることができます。画面に、現在のステートフル設定が、名前、説明、通常のステートフル設定アイコン (🔒) と共に一覧表示されます。

ツールバーまたはコンテキストメニューで、次のことを実行できます。

- 新規 (🔒 新規) ステートフル設定を作成する
- XML ファイルからステートフル設定をインポートする (📄)
- 既存のステートフル設定のプロパティ (🔗) を確認または変更する
- 既存のステートフル設定を複製 (📄) (および変更) する

- ステートフル設定を削除 (✖) する
- 1つ以上のステートフル設定をXMLファイルにエクスポート (📁) する (「エクスポート ...」ボタンをクリックして対象をすべてエクスポートするか、ドロップダウンリストで選択して、選択または表示された対象のみをエクスポートする)

「新規」(🆕 新規) または「プロパティ」(🔗) をクリックして、「ステートフル設定のプロパティ」画面を表示します。

新しいステートフル設定を作成または編集するには

パス: 脆弱性対策オプションメインメニュー | 「ファイアウォール」 > 「ステートフル設定」

1. 🆕 「新規」をクリックして新しいステートフル設定を作成するか、既存の設定を選択して「プロパティ」(🔗) をクリックし、変更します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - **名前**: ステートフル設定の名前。
 - **説明**: ステートフル設定の説明を入力します。この説明は、ここでのみ表示されます。
3. 「IP パケットインスペクション」エリアで、受信したフラグメント化されたすべてのパケットを拒否するかどうかを選択します。このオプションを有効にすると、「フラグメント化された IP パケット」というログが記録され、フラグメント化されたすべてのパケットが破棄されます。このルールの特徴の例外は、合計の長さが IP ヘッダより短いパケットがある場合です。そのようなパケットは、ログに記録されずに破棄されます。

警告: 攻撃者は、ファイアウォールルールを迂回するために、フラグメント化されたパケットを作成して送信する場合があります。

初期設定では、ファイアウォールルールエンジンは、フラグメント化されたパケットに対して一連のチェックを実行します。これは初期設定の動作で、設定し直すことはできません。次のような特徴を持つパケットは、破棄されます。

- **無効なフラグメントのフラグ/オフセット**: IP ヘッダの DF フラグおよび MF フラグに 1 が設定されている場合、またはヘッダに 1 が設定された DF フラグおよび 0 以外のオフセット値がある場合、パケットは破棄されます。
- **小さすぎる最初のフラグメント**: MF フラグに 1 が設定されていて、オフセット値が 0、合計の長さが (最大組み合わせヘッダ長である) 120 バイトよりも短い場合、パケットは破棄されます。

- **範囲を超えた IP フラグメント**: 合計パケット長と組み合わせられたオフセットフラグの値が最大データグラム長である 65,535 バイトを超えた場合、パケットは破棄されます。
 - **小さすぎる IP フラグメントのオフセット**: 60 バイトよりも小さい値を持つ 0 以外のオフセットフラグがある場合、パケットは破棄されます。
4. 「TCP」タブをクリックして、「TCP パケットインスペクション」エリアで必要な情報を指定します。

- **CWR、ECE フラグを含む TCP パケットを拒否する**: これらのフラグは、ネットワーク輻輳時に設定されます。

RFC 3168 では、ECN (Explicit Congestion Notification) に使用する予約済みフィールドの 6 ビットのうち 2 ビットを、次のように定義しています。

- ビット 8 から 15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
- TCP ヘッダフラグのビット名参照
- ビット 8: CWR (Congestion Window Reduced) 「RFC3168」
- ビット 9: ECE (ECN-Echo) 「RFC3168」

警告: パケットの自動転送 (特に DoS 攻撃によって生成されたものなど) によって、これらのフラグが設定されたパケットが作成されることがよくあります。

- **TCP ステートフルインスペクションを有効にする**: TCP レベルでのステートフルインスペクションを有効にします。ステートフル TCP インスペクションを有効にすると、次のオプションが利用可能です。
 - **TCP ステートフルログを有効にする**: TCP ステートフルインスペクションイベントがログに記録されます。
 - **単一コンピュータからの着信接続数の上限**: 単一コンピュータからの接続数を制限すると、DoS 攻撃の影響を低減できます。
 - **単一コンピュータへの送信接続数の上限**: 単一コンピュータへの送信接続数を制限すると、Nimda などのワームの影響を大幅に低減できます。
 - **単一コンピュータからのハーフオープン接続数の上限**: この制限を設定すると、SYN フラッドなどの DoS 攻撃から保護できます。ほとんどのサーバでは、ハーフオープン接続を終了するためにタイムアウトが設定されています。この値を設定することにより、ハーフオープン接続が重大な問題にならないようにします。SYN-SENT (リモート) エントリが指定された制限に達した場合、その特定のコンピュータからの後続の TCP パケットは破棄されます。

注意： 単一コンピュータからのオープン接続を許可する数を決定する際に、使用している種類のプロトコルで妥当と考えられる単一コンピュータからのハーフオープン接続数と、輻輳を引き起こすことなくシステムが維持できる単一コンピュータからのハーフオープン接続数との間の数を選択します。

- ・ **ハーフオープン接続数が次を超過したときに SYN フラッド防御を有効にする：** 単一コンピュータからのハーフオープン接続数のハードリミットの設定とは異なり、SYN フラッド保護メカニズムは、オープン接続の設定数に達すると、単一コンピュータからの接続であるかどうかにかかわらず、SYN-Cookie の使用を開始します。SYN-Cookie を使用することは、接続が拒否されていないことを意味します。ただし、ステートテーブルに SYN-Cookie 用のエントリは作成されず、送信先のコンピュータから適切な SYN-ACK が受信されるまで、SYN-Cookie はアプリケーションに渡されません。
-

注意： SYN フラッド保護は、バージョン 7.5 以前の Windows クライアントプラグインでのみサポートされます。バージョン 7.5 SP1 以降の Windows クライアントプラグインではサポートされません。

- ・ **すでに確認されたパケット数が次を超過したときに ACK ストーム防御を有効にする：** このオプションを設定すると、ACK ストーム攻撃が発生したというイベントが記録されます。
 - ・ **ACK ストームが検出されたときに接続を中断する：** このオプションを設定すると、ACK ストーム攻撃が検出された場合に接続が切断されます。
5. 「FTP オプション」エリアで、目的の情報を指定します。
- ・ **アクティブ FTP**
 - ・ **着信を許可する：** このコンピュータがサーバとして動作しているときにアクティブ FTP を許可します。
 - ・ **送信を許可する：** このコンピュータがクライアントとして動作しているときにアクティブ FTP を許可します。

- **パッシブ FTP**
 - **着信を許可する** : このコンピュータがサーバとして動作しているときにパッシブ FTP を許可します。
 - **送信を許可する** : このコンピュータがクライアントとして動作しているときにパッシブ FTP を許可します。

ヒント: 一般的に、サーバの観点から見るとアクティブ FTP の方が安全であり、クライアントの観点から見るとパッシブ FTP の方が安全です。

6. 「UDP」タブをクリックして、「UDP パケットインスペクション」エリアで必要な情報を指定します。
- **ステートフル UDP インスペクションを有効にする** : UDP トラフィックのステートフルインスペクションを有効にする場合はオンにします。

注意: UDP ステートフル機能は、未承諾の受信 UDP パケットを破棄します。送信 UDP パケットごとに、ルールがその UDP 「ステートフル」テーブルをアップデートし、要求に対して 60 秒以内に UDP 応答が発生した場合のみ、UDP 応答を許可します。特定の受信 UDP トラフィックを許可する場合は、強制的に許可ルールを作成する必要があります。たとえば、DNS サーバを実行している場合、送信先のポート 53 に受信 UDP パケットを許可するには、強制的に許可ルールを作成する必要があります。

警告: UDP トラフィックのステートフルインスペクションがない場合、攻撃者は DNS サーバになりすまして、未承諾の UDP 「応答」を送信元のポート 53 からファイアウォールの内側にあるコンピュータに送信する可能性があります。

- **ステートフル UDP ログを有効にする** : このオプションをチェックすると、ステートフル UDP インスペクションイベントのログを記録できるようになります。

7. 「ICMP」タブをクリックして、「ICMP パケットインスペクション」エリアで必要な情報を指定します。

- **ステートフル ICMP インスペクションを有効にする** : ICMP トラフィックのステートフルインスペクションを有効にする場合はオンにします。

注意： ICMP (擬似) ステートフル機能は、未承諾の受信 ICMP パケットを破棄します。送信 ICMP パケットごとに、ルールがその ICMP 「ステートフル」テーブルを作成またはアップデートし、要求に対して 60 秒以内に ICMP 応答が発生した場合のみ、ICMP 応答を許可します。(サポートする ICMP ペアの種類は、タイプ 0 と 8、13 と 14、15 と 16、17 と 18 です)。

警告： たとえば、ステートフル ICMP インスペクションを有効にすると、エコー要求が送信された場合に ICMP エコー応答を許可できます。要求されていないエコー応答は、Smurf 増幅攻撃、マスターとデーモン間のライブフラッドネットワーク通信、Loki2 バックドアなど、さまざまな種類の攻撃の予兆である可能性があります。

- **ステートフル ICMP ログを有効にする** : このオプションをチェックすると、ステートフル ICMP インスペクションイベントのログを記録できるようになります。

8. 「割り当て対象」タブをクリックして必要な情報を指定します。

「割り当て対象」タブには、このステートフルインスペクション設定を使用するセキュリティプロファイルとコンピュータが一覧表示されています。



第9章

Deep Packet Inspection を使用する

この章では、脆弱性対策オプション™ 1.5 Deep Packet Inspection を使用してネットワークとコンピュータをセキュリティリスクから保護する方法について説明します。

この章で扱うトピックは次のとおりです。

- 112 ページの「Deep Packet Inspection について」
- 113 ページの「Deep Packet Inspection をオンまたはオフにする」
- 114 ページの「DPI イベント」
- 119 ページの「DPI ルール」
- 123 ページの「カスタム DPI ルールを作成する」
- 138 ページの「アプリケーションの種類」

Deep Packet Inspection について

新規に DPI ルールのセットを適用する場合、DPI 動作を「検出」に設定できます。検出モードでは、DPI エンジンはずべてのトラフィックに同一の DPI ルールを適用しますが、パケットを破棄する代わりに、イベントのみをログに記録してトラフィックを通過させます。この動作により、新規 DPI ルールは正規のトラフィックを妨げることはありません。

この設定は、ネットワークエンジンがインラインで動作しているときのみ、つまり実際のトラフィックが脆弱性対策オプションネットワークエンジン内を流れているときのみ適用できます。インラインモード以外ではタップモードがあります。これは、実際のトラフィックをクローン化し、ネットワークエンジンではクローン化されたトラフィックのみを分析するモードです。タップモードではネットワークエンジンが実際のトラフィックストリームを制御しないので、防御モードは設定できません。

パケット処理のシーケンス

受信ネットワークトラフィックも送信ネットワークトラフィックも、次のモジュールのルートを通して供給されます。

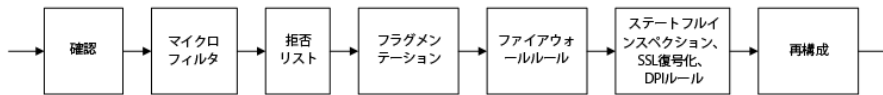


図 9-1. モジュールパイプライン

- ・ **確認**: パケットの正当性についての基本的な確認を行います。
- ・ **マイクロフィルタ**: 基本的なファイアウォールの放置ルールは、この階層で実施されます。
- ・ **拒否リスト**: トラフィック分析機能で使用される既知の不正 IP のリストを保持します。
- ・ **フラグメンテーション**: MTU より大きいパケットをフラグメント化します。
- ・ **ファイアウォールルール**: マイクロフィルタで処理されないパケットすべては、ファイアウォールで処理します。
- ・ **ステートフルインスペクション、SSL 復号化、および DPI ルール**: 1 つのモジュールとして次の機能を実行します。
 - ・ **ステートフルインスペクション**: 応答の際に有効な既知の接続を維持します。接続制限の管理および SYN フラッドと ACK ストームの保護も行います。

- **SSL 複合化**: この機能が必要な場合や設定されている場合は、SSL で保護されたトラフィックを解読して DPI エンジンで分析します。
- **DPI**: パターン照合やカスタムコード操作を実行する Deep Packet Inspection エンジンです。
- **再構成**: DPI エンジンで後に使用するフラグメント化されたパケットを再構築します。

受信および送信トラフィックは同じ順序でパイプラインを通りますが、ステートフルインスペクション、SSL、および DPI モジュール内部での順序はトラフィック方向によって異なります。

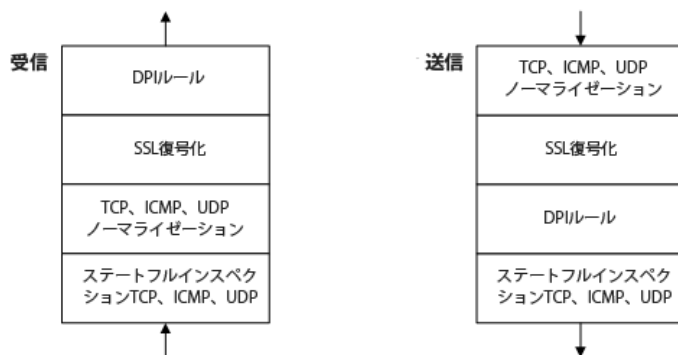


図 9-2. モジュールパイプライン

Deep Packet Inspection をオンまたはオフにする

Deep Packet Inspection をオンまたはオフにするには：

パス：メインメニュー | 「**Deep Packet Inspection**」

1. 「Deep Packet Inspection」エリアで、「オン」または「オフ」にします。
2. インライン DPI 動作を「予防」または「検出」に設定します。

インラインモードとタップモードを切り替えるには、「システム」→「システム設定」→「ファイアウォールと DPI」に進んでください。

3. 推奨設定の検索を有効にするかどうかを選択します。

クライアントプラグインでは、通常推奨設定の検索を実行するよう設定できます。これは、コンピュータを検索してさまざまなセキュリティルールのアプリケーションを推奨するものです。チェックボックスをオンにすると、コンピュータに推奨ルールが自動で割り当てられ、不要なルールは自動的に外されます。

注意： このオプションを選択する場合は、脆弱性対策オプションルールアップデートによる新しい DPI ルールの自動割り当ても許可する必要があります。「システム」>「システム設定」>「アップデート」に進み、「脆弱性対策オプションルールアップデート」エリアで「新しい DPI ルールの自動割り当てを脆弱性対策オプションルールアップデートに許可する」を選択してください。

推奨設定の検索を定期的に行うには、「システム」→「システム設定」→「検索」に進みます。

DPI イベント

初期設定では、ハートビートごとにクライアントプラグインからファイアウォールログと DPI イベントログがサーバプラグインで収集されます。(これは、「システム」>「システム設定」画面の「ファイアウォールと DPI」タブでオフにできます。) ログのデータを使用して、サーバプラグインの各種レポート、グラフ、およびチャートが作成されます。

イベントログは、脆弱性対策オプションサーバプラグインによって収集された後、「システム」>「設定」画面の「システム」タブで設定された一定の期間保持されます。初期設定値は 1 週間です。メイン画面から、次のことを実行できます。

- 特定のイベントのプロパティを表示 (🔍) する
- リストをフィルタする: イベントのリストをフィルタするには、「期間」および「コンピュータ」ツールバーを使用します
- イベントログのデータを CSV ファイルにエクスポート (📄) する
- 特定のイベントを検索 (🔍) する

さらに、ログエントリを右クリックすると、次のオプションが表示されます。

- **タグの追加:** イベントタグをこのイベントに追加します (「168 ページの「イベントのタグ付け」を参照してください)。
- **タグの削除:** 既存のイベントタグを削除します。
- **コンピュータの詳細:** ログエントリを生成したコンピュータの「詳細」画面を表示します。
- **DPI ルールのプロパティ:** 開いている「プロパティ」画面で特定のログエントリのプロパティをすべて表示します。
- **Whois 送信元 IP:** 送信元 IP に対して whois を実行します。
- **Whois 送信先 IP:** 送信先 IP に対して whois を実行します。

リストをフィルタし、イベントを検索する

「詳細検索」ドロップダウンメニューから「詳細検索を開く」を選択すると、詳細検索オプションが表示されます。

「期間」ツールバーを使用してリストをフィルタし、特定の期間内に発生したイベントだけを表示できます。

「コンピュータ」ツールバーを使用すると、コンピュータドメイン別またはコンピュータセキュリティプロファイル別にイベントログエントリの表示を整理できます。

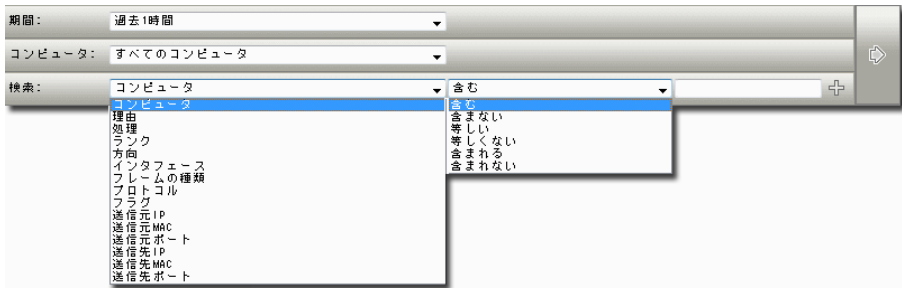


図 9-3. 「コンピュータ」ツールバー

詳細検索機能 (大文字 / 小文字の区別なし):

- **含む**: 選択した列の入力内容に検索文字列が含まれる
- **含まない**: 選択した列の入力内容に検索文字列が含まれない
- **等しい**: 選択した列の入力内容と検索文字列が完全に一致する
- **等しくない**: 選択した列の入力内容が検索文字列と完全には一致しない
- **含まれる**: 選択した列の入力内容がカンマ区切りで入力された検索文字列 1 つと完全に一致する
- **含まれない**: 選択した列の入力内容がカンマ区切りで入力されたどの検索文字列とも完全には一致しない

検索バーの右側にある「プラス」ボタン (+) をクリックすると、追加の検索バーが表示され、検索に複数のパラメータを適用できます。準備が整ったら、送信ボタンをクリックします (ツールバーの右側にある上部に右矢印の付いたボタン)。

DPI イベントのプロパティを表示する

イベントをダブルクリックすると、そのエントリの「プロパティ」画面が表示されます。「タグ」タブには、このイベントに関連付けられているタグが表示されます。イベントのタグ付けの詳細については、「システム」>「タグ」と「168 ページの「イベントのタグ付け」を参照してください。

DPI イベント情報を表示するには：

パス： [メインメニュー](#) | **「Deep Packet Inspection」**

「DPI イベント」画面の列：

- ・ **時刻：** コンピュータ上でイベントが発生した時刻。
- ・ **コンピュータ：** このイベントのログが記録されたコンピュータ。(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます。)
- ・ **理由：** このイベントに関連付けられた DPI ルール。
- ・ **タグ：** イベントに関連付けられたタグ。
- ・ **アプリケーションの種類：** このイベントの原因となった DPI ルールに関連付けられたアプリケーションの種類。
- ・ **処理：** DPI ルールが実行する処理 (許可、拒否、強制的に許可、ログのみ、または検出のみ (フィルタが検出のみモードの場合))。
- ・ **ランク：** ランク付けシステムでは、DPI およびファイアウォールイベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、DPI ルールとファイアウォールルールに「重要度」を割り当て、これら 2 つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、DPI イベントまたはファイアウォールイベントを表示するときに、イベントをランクでソートできます。
- ・ **重要度：** ルールの重要度。重大、高、中、低、またはエラーの重要度評価に関連付けられています。
- ・ **方向：** パケットの方向 (受信または送信)。
- ・ **フロー：** パケットの送信元。「接続フロー」はパケットが TCP 接続のイニシエーターから来ていることを示します。「リバースフロー」はパケットが TCP 接続のレシーバーから来ていることを示します。
- ・ **インタフェース：** パケットが通過したインタフェースの MAC アドレス。
- ・ **プロトコル：** 値は、「ICMP」、「IGMP」、「GGP」、「TCP」、「PUP」、「UDP」、「IDP」、「ND」、「RAW」、「TCP+UDP」、「N/A」、「その他: nnn」(nnn は、3 桁の 10 進値) のいずれかになります。
- ・ **フラグ：** パケットに設定されたフラグ。

- **送信元 IP:** パケットの送信元 IP です。
- **送信元 MAC:** パケットの送信元 MAC アドレス。
- **送信元ポート:** パケットの送信元ポート。
- **送信先 IP:** パケットの送信先 IP。
- **送信先 MAC:** パケットの送信先 MAC アドレス。
- **送信先ポート:** パケットの送信先ポート。
- **パケットサイズ:** バイト単位のパケットのサイズ。

イベントログをエクスポートする

「エクスポート ...」 ボタンをクリックして、すべてのイベントログエントリを CSV ファイルへエクスポートします。

DPI イベントにタグを付ける

イベントのタグ付けでは、DPI イベントにカスタムのラベル（「これは Tom が再確認」など）を手動でタグ付けできます。イベントのタグ付けを使用すると、イベントの特殊なビュー、ダッシュボード、およびレポートが有効になります。また、イベントのタグ付けは単一イベント、類似する複数のイベント、または将来的に発生する同様のすべてのイベントに適用できます。

タグを 1 つまたは複数の選択したイベントに適用するには：

パス： [メインメニュー](#) | [「Deep Packet Inspection」](#) > [「DPI イベント」](#)

1. 「イベント」リストでイベントを選択してから右クリックして「**タグを追加 ...**」を選択します。
2. タグの名前を入力します（文字を入力していくと、一致する既存のタグが候補として表示されます）。
3. 「**選択された 1 個のシステムイベント**」を選択します。（「イベント」リストから複数のイベントを選択した場合、選択したイベントの数が表示されます。）「**次へ**」をクリックします。
4. 必要に応じてコメントを記入し、「**完了**」をクリックします。

「イベント」リストで、イベントにタグが付けられたことを確認できます。

複数の同様のイベントにタグを付けるには

1. 「イベント」リストの中からベースにするイベントを右クリックし、「タグを追加 ...」をクリックします。
2. タグの名前を入力します (文字を入力していくと、一致する既存のタグが候補として表示されます)。
3. 「類似のイベントにも適用」を選択します。
4. イベントの選択を絞る場合は、「詳細オプションを含める」を選択します。
5. 「次へ」をクリックします。
6. 詳細オプションを選択した場合は、選択を行います。たとえば、特定のコンピュータまたはコンピュータドメインに限定して類似するイベントを表示できます。この場合は、該当するイベントを選択して、「次へ」をクリックします。
7. イベントが同様のものかどうかの判定基準となる属性を選択します。ほとんどの場合、属性オプションは「イベント」リスト画面の列に表示される情報と同じです。イベントの選択処理に含めるための属性を選択したら、「次へ」をクリックします。
8. このルールを適用する類似 DPI イベントの種類を選択してください。

注意： 「自動タグルールの保存」オプションについて。指定した選択条件を保存すると、将来、新しいイベントが増えたときに、その条件を適用することができます。保存した自動タグ付けルールは、「システム」>「タグ」画面で確認できます。

9. 「次へ」をクリックします。
10. 必要に応じてコメントを記入し、「次へ」をクリックします。
11. イベントの選択条件を概要で確認し、「完了」をクリックします。

「イベント」リストで、ベースにしたイベントおよび同様のすべてのイベントにタグが付けられていることを確認できます。

複数の同様のイベントおよび将来の同様のイベントにタグを付けるには

複数の同様のイベントや将来の同様のイベントにタグ付けする手順は、上記の手順と、手順 8 を除いて同じです。手順 8 では「新規 DPI イベント」も選択します。「新規 DPI イベント」を選択すると、脆弱性対策オプションサーバプラグインは 5 秒 (またはそれ以上) ごとにデータベースを検索して新しいイベントを探し、該当するイベントにタグを付けます。





注意： タグ付けが実行されるのは、クライアントプラグインから取得されたイベントが脆弱性対策オプションサーバプラグインのデータベースに登録された後です。

DPI ルール







ファイアウォールルールとステートフル設定がパケットの制御情報 (パケットを説明するデータ) を確認するのに対して、DPI ルールはパケット (および一連のパケット) の実際のコンテンツを確認します。DPI ルールに定義された条件に基づいて、さまざまな処理がこれらのパケットに対して実行されます。処理には、明確に定義されたバイトシーケンスや疑わしいバイトシーケンスの置換から、パケットの完全な破棄や接続のリセットまで含まれます。



「DPI ルール」画面に、現在の DPI ルールと次の項目を含む情報が一覧表示されます。

DPI ルールのアイコン：

-  通常の DPI ルール
-  スケジュールに従って動作する DPI ルール
-  設定オプションがある DPI ルール
-  設定オプションが必要な DPI ルール

「DPI ルール」画面では、DPI ルールを作成および管理できます。ツールバーまたは右クリックのコンテキストメニューで、次のことを実行できます。

- ・ 新規 DPI ルールを作成する ( 新規)
- ・ XML ファイルから DPI ルールをインポートする (
- ・ 既存の DPI ルールのプロパティを確認または変更する (
- ・ 既存の DPI ルールを複製 (および変更) する (
- ・ DPI ルールを削除する (
- ・ 1 つ以上の DPI ルールを XML ファイルにエクスポートする ()(「エクスポート ...」ボタンをクリックして対象をすべてエクスポートするか、ドロップダウンリストで選択して、選択または表示された対象のみをエクスポートする)



「新規」( 新規) または「プロパティ」() をクリックしてスケジュールの「プロパティ」画面を表示します。

注意： 「設定」タブを確認します。トレンドマイクロが提供する DPI ルールは、脆弱性対策オプションサーバプラグインを使用して直接編集することはできません。その代わりに、DPI ルールの設定が必要な場合や設定が可能な場合は、「設定」タブの設定オプションを使用します。ユーザ自身で作成したカスタム DPI ルールは、「ルール」タブが表示され、直接編集可能です。

DPI ルールプロパティを作成する

DPI ルールプロパティを作成したり編集するには

パス: [メインメニュー](#) | [「Deep Packet Inspection」](#) > [「DPI ルール」](#)

1. 「 **新規**」をクリックして新規 DPI ルールを作成するか、既存の DPI ルールを選択して「**プロパティ**」() を選択して DPI ルールを変更します。
2. ポップアップウィンドウの「**一般**」タブの「**一般情報**」エリアで必要な情報を指定します。
 - **名前**: DPI ルールの名前。
 - 「**説明**」: DPI ルールの概要。
 - **クライアントプラグインの最小バージョン**: DPI ルールを実装するのに最小限必要な脆弱性対策オプションクライアントプラグインのバージョン。
3. 「**詳細**」エリアで、目的の情報を指定します。
 - **アプリケーションの種類**: この DPI ルールがグループ化されるアプリケーションの種類。既存のタイプを選択することも、新しいタイプを作成することもできます。

注意: このパネルで既存のタイプを編集することもできます。ここで既存のアプリケーションの種類を編集すると、そのアプリケーションの種類を使用するすべてのセキュリティコンポーネントに対して変更内容が適用されることを忘れないください。

- **優先度**: DPI ルールの優先度レベル。優先度の低いルールよりも先に優先度の高いルールが適用されます。
- **重要度**: ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、DPI ルールのリストを表示するときに条件をソートする際に役立ちます。何より、それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産値を掛けたものが、イベントのランキングを決定します。(「[システム](#)」 > 「[システム設定](#)」 > 「[ランク付け](#)」を参照してください)。
- **CVSS スコア**: 脆弱性情報データベースに基づいた、脆弱性の重要度の基準。
- **検出のみ**: 新しいルールをテストするときはこのチェックボックスを使用します。このチェックボックスをオンにすると、ルールは「**検出のみ**」という言葉で始まるログエントリを作成しますが、トラフィックに干渉しません。後述する次のパネルの「**ログの無効化**」チェックボックスをオンにすると、「**検出のみ**」がオンかオフにかかわらず、ルールの処理がログに記録されなくなります。

注意： DPI ルールの中には、「検出のみ」モードでのみ動作するように設計されていて、トラフィックをブロックするように設定できないものもあります。それらのルールについては、「検出のみ」オプションが設定され、変更できないようにロックされます。

4. 「イベント」エリアで、目的の情報を指定します。
 - **ログの無効化：** イベントログを無効にする場合はオンにします。
 - **パケット破棄時にイベントを生成：** パケットの破棄/ブロックをログ記録します。
 - **常にパケットデータを含める：** ログエントリにパケットデータを含めます。
 - **デバッグモードを有効にする：** ルールをトリガしたパケットの前後にある複数パケットをログに記録します。トレンドマイクロでは、サポート担当者が指示した場合のみ、このオプションを使用することを推奨します。
5. 「ID」エリア (ダウンロードされたルールのみが表示されます) で、目的の情報を指定します。
 - **種類：** 「スマート」(1 つ以上の既知または不明なゼロデイの脆弱性)、「セキュリティホール」(通常、署名ベースのセキュリティホール) または「脆弱性」(1 つ以上のセキュリティホールが存在する可能性のある特定の脆弱性) のいずれかになります。
 - **発行済：** ルールがリリースされた日付 (ダウンロードされた日付ではありません)。
 - **識別子：** ルールに一意的識別子タグ。
 - **前回のアップデート：** ルールがアップデートされた最後の日付です。
6. 「脆弱性」タブ (トレンドマイクロのルールにのみ表示) をクリックして、この特に脆弱性が高い箇所についての情報を表示します。

適用可能な場合は、共通脆弱性評価システム (CVSS) が表示されます。(この評価システムの詳細は、脆弱性情報データベースの CVSS ページを参照してください。)
7. 「設定」タブ (トレンドマイクロのルールにのみ表示) をクリックして、ダウンロードルールの設定オプションを設定します。
 - **設定オプション：** ダウンロード済みルールに設定可能なオプションがある場合は、ここに表示されます。オプションの例としては、ヘッダ長、HTTP で許可された拡張子、Cookie 長などがあります。必要なオプションを設定しないでルールを適用した場合、アラートが発令され、設定が必要なコンピュータのルールが示されます。(これは、セキュリティアップデートによってダウンロードされ自動的に適用されたルールにも適用されます。)

注意： 設定オプションのある DPI ルールは「DPI ルール」画面に表示され、アイコンには小さなチェックマークが付きます (🔍)。

- ・ 「**ルールの表示**」 (カスタム DPI ルールのみ利用可能): トレンドマイクロによって機密とマークされていない DPI ルールでは、「**ルールの表示 ...**」 ボタンが利用できるようになります。
8. 「**オプション**」 タブをクリックしてオプションを表示します。
 9. 「**アラート**」 エリアで、トリガされたときにこの DPI ルールがアラートを発令する必要があるかどうかを選択します。このルールを特定の期間だけ有効にする場合は、ドロップダウンリストのスケジュールを割り当てます。
 10. 「**スケジュール**」 エリアで、予約された時間のみ DPI ルールを有効化するかどうかを選択します。

注意： 予約された時間のみ有効になる DPI ルールは、「DPI ルール」画面に、小さな時計が付いたアイコン (🕒) で表示されます。

11. 「**コンテキスト**」 エリアで、目的の設定をします。

コンテキストは、コンピュータのネットワーク環境に応じてさまざまなセキュリティポリシーを実装する強力な方法です。コンテキストは一般的に、コンピュータ (通常はモバイルノートパソコン) が社内または社外にあるかどうかで異なるファイアウォールや DPI ルールを適用するセキュリティプロファイルを作成するために使用します。

コンテキストは、ファイアウォールルールと DPI ルールと関連付けられるよう設計されています。ルールに関連付けられたコンテキストの定義条件に一致した場合、ルールは適用されます。

コンピュータの場所を決定するには、コンピュータがどのようにドメインコントローラと接続されているかコンテキストで検証します。コンテキストの詳細については、「146 ページの「コンテキスト」」を参照してください。
12. 「**推奨オプション**」 エリアで、推奨設定の検索後にルールの推奨設定からこの DPI ルールを除外します。
13. 「**割り当て対象**」 タブで、この DPI ルールが割り当てられるコンピュータとセキュリティプロファイルの一覧を確認できます。

カスタム DPI ルールを作成する

脆弱性対策オプションでは、パケットの内容を検査し、イベントをログに記録するかまたは接続をリセットするかを決定するように設計された XML ベースの言語が提供されています。

DPI ルールの考慮事項

DPI ルールは、パケットがアプリケーションに配信される前 (受信パケットの場合) またはネットワークに転送される前 (送信パケットの場合) に、パケットがカーネルで処理されるときにネットワークデータに適用されます。このため、ルールの効率性が非常に重要であり、DPI ルールは処理などの単純な命令に制限されます。

Hello World

パターンの出現を検出するための単純なルールの例を以下に示します。

```
<rule pat="hello">
    log "hello found"
</rule>
```

この pattern-rule は、パケット内で文字列「hello」が検出されるとトリガされます。ルールがトリガされると、コードの action ブロックが実行されて、脆弱性対策オプションサーバプラグインにイベントを記録します。DPI イベントの注記として文字列「hello found」が脆弱性対策オプションサーバプラグインに渡されます。

注意: 大文字と小文字を区別しないようにパターンルールが初期設定されているため、文字列が「hello」、「HELLO」、「hElLo」のいずれの場合でも、このルールはトリガされます。

注意: DPI エンジンには、raw パケットデータにはパターンルールを直接適用しません。不正なペイロードは、複数のセグメントまたはパケットフラグメントに分割され、ランダムにまたは 1 バイト単位のセグメントで転送されることがあります。DPI エンジンには、パターンルール分析を行う前にデータストリームを分析して、このような攻撃から保護します。

XML での記法

XML で特別な意味を持つ一部の文字列については、パターンまたは注記文字列として使用する際に、特別な形式で記述する必要があります。特別な形式で記述する必要があるのは、次の文字です。

< > & " ' "

表 9-1. XML での記法

文字	XML での記法
<	<
>	>
&	&
"	"
'	'

たとえば、文字列 one&"2" は次のように記述します。

```
<rule pat="one&amp;&quot;2&quot;">
    log "onetwo"
</rule>
```

場合によっては、16 進エンコードの方が簡単なパターンもあります。(「129 ページの「パターンに関するその他の事項」参照。)

これらの文字を特別な形式で記述しないと、ルールを割り当てたときに「コンピュータのアップデート」システムエラーが発生します。

アプリケーションの種類とルールの方向

初期設定では、フォワード接続方向でパターンが検出されたときに、ルールがトリガされます。方向の意味は、ルールが配信される場所によって異なります。

トラフィックを待機している Web サーバの場合、ポート 80 に着信する受信 http 要求はフォワード方向として扱われ、Web サーバからの送信 http 応答はバックワード方向として扱われます。

Web クライアントの場合は、ポート 80 に送られた送信 http 要求はフォワード方向として扱われ、受信 http 応答はバックワード方向として扱われます。

DPI ルールには、フォワード方向またはバックワード方向に文字列を検索するパターンルールを複数含めることができます。

```
<fwd pat="hello">log "hello found"</fwd>
```

```
<bwd pat="goodbye"> log "goodbye"</bwd>
```

ステートを使用してルールを細かく定義する

上述の例では、「hello」が検出されるかどうかにかかわらず「goodbye」イベントがトリガします。このルールを修正して、次のように「hello」が検出された後の「goodbye」が意味を持つようにすることができます。

```
<fwd pat="hello">
    stateset 1
</fwd>
<!-- this rule resets the connection when goodbye is seen after hello -->
<bwd pat="goodbye" state="1">
    log "goodbye"
    stateset 0
</bwd>
```

上記のルールが示しているのは、同じ接続の逆方向で、「goodbye」の前に出現する「hello」を常時識別する単純なステートコンピュータを実装するために、「stateset」処理命令と「state」ルール制約属性を組み合わせる方法です。

このように、ステートを追跡するために、パターンルールをいくつでもまとめて定義することができます。

コメントを追加する

ルールの記述は複雑になりやすいため、上記のようにコメントを追加すると役に立ちます。またコメントを使用して、テスト時に、コードの一部を一時的に処理されないようにすることもできます。XMLの標準のコメントは「<!-- ... -->」の形式です。

その他のルール処理

接続をリセットする (drop)

接続をリセットするには、次のように「drop」命令を使用します。

```
<rule pat="bad">  
    drop "bad"  
</rule>
```

「drop」命令で接続をリセットすると、その接続に対してルールの適用が停止されるか、同じパケットが継続している場合はそれ以降のパケット内容に対してルールが適用されなくなります (接続が両方のエンドポイントにリセットされ、以降のパケットは受け付けなくなります)。

検出モードと予防モードについて

1 つの DPI ルールを検出モードで実行できます。検出モードの DPI ルールで実行された「drop」命令は、ログには記録されますが、接続はリセットされません。接続がリセットされないため、他の DPI ルールが予防モードで実行されていると、ルール処理はそれ以降も継続します。

また、DPI エンジンも「検出モード」で実行できます。このモードで接続はリセットされませんが、それ以降のルール処理は行われません。

接続の遅延リセット (setdrop)

接続をリセットするタイミングを遅らせ、別のルールを実行しておくことが適切な場合があります。

```
<fwd pat="bad">  
    setdrop "bad"  
</fwd>  
<fwd pat="worse">  
    drop "worse"  
</fwd>
```

この場合、データに「bad」と「worse」のどちらかが含まれていれば接続がリセットされますが、両方が含まれている場合は、リセットの理由となるのは常に「worse」です。

遅延リセットは取り消すこともできます。その場合は、次のように記述します。

```
<fwd pat="good">
    clrdrop
</fwd>
```

setdrop により、drop 処理はパケットの終わりまで実行されません。「worse」が出現してもリセットの理由とならないのは、そのパターンが他のパケットにあると考えられます。これは、「worse」が後のパケットにあることを DPI エンジンが認識せず、最初のパケットで不正と判断されるとドロップされるからです。

ルール属性について

以下の制約属性を使用して、事前に決めた条件が満たされないかぎり、ルールがトリガされないようにすることができます。

ステート

「state」属性は、前の処理の結果、現在の状態が指定された値になったときのみルールの処理が実行されることを指定します。指定できる値の範囲は 0 ~ 255 です。

「state」属性を指定しない場合、現在の状態にかかわらずルール処理がトリガされます。

大文字小文字の区別の照合

「case」属性を使用して、大文字小文字の区別を照合できます。

```
<fwd pat="hello" case="1"> ... </fwd>
```

範囲の制約

「dist」属性を使用して、2つのパターンがパターン間の指定範囲内に出現することを制約条件にすることができます。

```
<fwd pat="hello"> ... </fwd>
```

```
<fwd pat="goodbye" dist="10,20">
```

```
    log "goodbye"
```

```
</fwd>
```

```
<fwd pat="salut" distmax="10">
    log "salut"
</fwd>
```

```
<fwd pat="ciao" distmin="10">
    log "ciao"
</fwd>
```

最初の形式の属性は、相手のパターンの出現から 10 バイト～ 20 バイトの範囲で「goodbye」を検出することを指定します。

2つ目の形式の「distmax」属性は、その範囲の上方の限界のみを指定し、下方は制限しないことを指定します。

最後の形式の「distmin」属性は、上方は制限せず、下方の限界のみを制限することを指定します。

注意： 範囲の制約は接続方向のパターンに適用されます。フォワード方向の出現パターンとバックワード方向の出現パターンとの間の範囲を制約することには使用できません。

カウンタの使用

たとえばヘッダフィールドの最大サイズを制限するなど、ある範囲内にパターンが出現しない場合に、ルールをトリガすることが適切なことがあります。1つのパターンルールを使用してカウンタを開始し、必要に応じて、他のルールを使用してカウンタをクリアすることができます。カウンタを使用すると、特定のパターンを決めずにルールをトリガすることができます。

```
<fwd pat="HELLO">
    startcount 1024
</fwd>

<!-- reset if the line is longer than 256 bytes -->
<counter>
    stateset 0
</counter>
```

```

<!-- clear the counter when newline is found -->

<fwd pat="¥n">
    clrcount
</fwd>

```

同じルールドメイン内では、カウンタは一度に1つしかアクティブにできません。1つのカウンタがペンディング状態のときに別のカウンタを開始すると、ペンディングされているカウンタが自動的にクリアされます。

注意： ルールでカウンタを開始する場合は、その後に `<counter> ...</counter>` を指定する必要があります。これはルールコンパイラによって実施されます。

パターンに関するその他の事項

パターンは、固定長の文字列に制限されます。次のようなワイルドカード文字も同様です。

表 9-2. パターン

¥a (¥A)	アルファベット、a～z、A～Z (アルファベット以外)
¥w (¥W)	英数字 a～z、A～Z、0～9 (英数字以外)
¥d (¥D)	数字 0～9 (数字以外)
¥s (¥S)	スペース (スペース以外) 「¥r、¥n、¥t、0x32」
¥p (¥P)	区切り文字、上記以外の出力可能な ASCII 文字
¥c (¥C)	制御文字、< 32, >= 127 (スペースを含まず)
¥.	すべての文字

特殊な予約語またはバイナリ文字は引用符で囲むか、次のようにエスケープする必要があります。

表 9-3. 予約語

¥xDD	16進バイト 0xDD
¥¥	「¥」 エスケープ
¥	パイプ「 」 エスケープ
xx xx xx...	16進パイプ (バイトシーケンス)

その他のルール：

- ・ ワイルドカードだけでパターンを作成することはできません。
- ・ 16進エンコードシーケンスは、初期設定で大文字小文字が区別されません。
- ・ +,*などの正規表現形式の可変長シーケンスは許可されません。

例：

```
<rule pat="|90 E8 C0 FF FF FF|/bin/sh" case="1">
    drop "IMAP overflow"
</rule>

<rule pat="port¥s¥d¥d"> ...</rule>
```

高度なルール処理

パターンルールがトリガし、制約条件が満たされると、ルールの処理が実行されます。これまでは、「log」、「drop」、および「stateset」などの簡単な処理を説明してきました。ルールの処理を使用して、「distance」や「case」などの簡単な属性を使用して記述した制約よりもさらに複雑な制約を定義することができます。

ルール処理は、通常、下位レベルの命令シーケンスとして定義されます。命令は一連の仮想レジスタへアクセスして、単純な計算処理と比較処理を行うことができます。ルール処理には、if、then、elseなどの条件ブロックを含めることができます。各命令は次のいずれかの形式をとります。

```
instruction STRING
instruction REG OPAND
```

たとえば、次のとおりです。

```
<fwd pat="login">
    add r5 0x100 <!-- r5 <- hex 100 (=256) -->
</fwd>

<fwd pat="two">
    add r4 256 <!-- r4 <- decimal 256 -->
    load r6 r4 <!-- r6 <- -->
    <if>eq r4 r5<then/>
        log "ok"
    </if>
</fwd>
```

レジスタの割り当て

命令で使用するために、次の仮想レジスタ r0 ~ r7 および c0 ~ c7 が定義されています。

表 9-4. 仮想レジスタ

レジスタ番号	フィルタレジスタ (r0 ~ r7)	接続レジスタ (c0 ~ c7)
0	状態	接続状態
1	カーソル	UTC 時刻 / 秒
2	予約済み	パケットカウント
3	予約済み	予約済み
4 - 7	ユーザ定義	ユーザ定義

状態レジスタは、「state」属性で使用される状態を参照するもう 1 つの方法です。

パケットカウンタレジスタの c2 レジスタには、各接続方向で処理されたパケットの数が保持されます。c1 レジスタには、現在の時刻 (1970 年以降の秒数) が保持されます。これらのレジスタを使用して、時刻またはパケットベースの制約を記述することができます。

その他のレジスタの説明：

- レジスタ c0 ~ c3 および r0 ~ r3 にはあらかじめ定義された意味があります。
- レジスタ r4 ~ r7 は汎用の用途です。
- 接続レジスタ c0 ~ c7 は、同じ接続内のすべてのルールで共有されます (各接続に固有のセットを持つ)。
- レジスタ r0 ~ r7 は、DPI ルールの各ルールドメインの専用レジスタです。
- どのレジスタにも、32 ビット値を含めることができます。

レジスタへアクセスする

「load」命令を使用して、値をレジスタに登録したり、レジスタ間で値を移動したりできます。

```
<rule pat="test">
    load r4 100 <!-- load value 100 decimal into r4 -->
    load r5 r4 <!-- copy contents of register r4 into r5 -->
</rule>
```

r0 が状態レジスタであるため、stateset 命令は単に「load」命令を別の形で表したものです。つまり、以下のコードと同じです。

```
<rule pat="test">
    load r0 1
    load stateset 1 <!-- same as above -->
</rule>
```

レジスタを比較する

if ブロックと比較命令を使用して、レジスタどうしを比較できます。たとえば、次のルールは、パターン「login」が 3 回以上出現したときに接続をリセットします。

```
<rule pat="login">
    add r4 1
    <if>
        gt r4 3<then/>
```

```
        drop "repeated3"  
    </if>  
</rule>
```

if-Statement

if文は一般的に次のような形式になります。

```
<if> (condition) <then/>  
    <!-- if blocks can be nested -->  
    <if> (condition) <then/>  
        (statements)  
</if>
```

```
<elseif/> (else condition) <then/>  
    (elseif statements)  
<else/>  
    (else statements) </if>
```

break

「break」命令で、処理命令の処理を中止します。ネストされたifブロックを簡素化するのに役立つことがあります。

```
<if>lt r4 0<then/>  
    break  
</if>
```

```
<if>gt r4 10<then/>  
    drop "range"  
</if>
```

レジスタの比較には、次の命令を使用することができます。

等式

表 9-5. 等式

命令	True になる場合
eq	REG == OPERAND
leq	REG != OPERAND

符号付き比較

次の命令を使用した比較では、レジスタとオペランドは 32 ビットの符号付きで扱われます。

表 9-6. 符号付き比較

命令	説明
gt	REG > OPERAND で True
lgt	REG < OPERAND で True
lt	REG < OPERAND で True
llt	REG > OPERAND で True

符号なし比較

次の命令を使用した比較では、レジスタとオペランドは 32 ビットの符号なしで扱われます。

表 9-7. 符号なし比較

命令	説明
ugt	符号なし: REG > OPERAND
lugt	符号なし: REG <= OPERAND
ult	符号なし: REG < OPERAND
lult	符号なし: REG >= OPERAND

Modulo32 比較

以下の命令では、レジスタとオペランドは modulo32 で扱われます。TCP などのプロトコルでは、32 ビットの全範囲を包括するシーケンス番号が使用されます。

表 9-8. Modulo32 比較

命令	説明
mlt	Mod32: REG < OPERAND
!mlt	Mod32: REG >= OPERAND
mgt	Mod32: REG > OPERAND
!mgt	Mod32: REG <= OPERAND

基本演算命令

演算命令により、加算、乗算、除算、およびモジュロ（剰余）などの演算を実行できます。

表 9-9. 基本演算命令

命令	説明
add	REG += OPERAND
sub	REG -= OPERAND
mul	REG *= OPERAND
div	REG /= OPERAND
mod	REG %= OPERAND

ビット単位命令

ビット単位の論理命令では、オペランドとレジスタは 32 ビット単位で扱われます。

表 9-10. ビット単位命令

命令	説明	
および	REG &= OPERAND	ビット単位 AND
または	REG = OPERAND	ビット単位 OR
xor	REG ^= OPERAND	ビット単位排他 OR
shiffl	REG <<= OPERAND	左ビットシフト (ゼロで埋める)
shiftr	REG >>= OPERAND	右ビットシフト (ゼロで埋める)

実行の順序

DPI エンジンは、すべてのパターンを同時に分析し、トラフィックストリーム内のパターンの出現順序に基づいてルールを実行します。エンジンは、接続をリセットしてからすべてのルール処理を停止します。このため、接続をドロップするルールが 2 つある場合は、それらのうち最初に出現したルールが実行され、2 つ目のルールによる影響はありません。

2 つのパターンが同じ位置に出現する場合、エンジンは定義された順序でルールを実行します。

```
<rule pat="goodbye">drop "goodbye"</rule>
```

```
<rule pat="bye">drop "bye"</rule>
```

この例では、最初に定義されたルールが実行されてから、2 番目のルールが実行されます。

パターンルールが異なる DPI ルールで定義されている場合、脆弱性対策オプションサーバの優先度で定義の順序を制御できます。この場合、優先度の高いパターンが実行されてから、同じ位置にある優先度の低いパターンが実行されます。

UDP 擬似接続

ルールは TCP トラフィックだけでなく、UDP トラフィックにも割り当てることができます。UDP トラフィックはコネクション指向ではありませんが、同一の送信元と送信先の IP および同一のポート間の要求 / 応答シーケンスは TCP データの場合と同じ方法で調査することができます。次のような違いがあります。

- DPI エンジンによって UDP メッセージの順序が変えられることはない
- UDP 擬似接続は、TCP のように明示的にリセットすることができない

UDP 擬似接続に「drop」命令を使用するルールの場合、UDP のタイムアウト期間 (初期設定 10 秒) は、これらのエンドポイント間でトラフィックがブロックされます。

URI の Web ルール

特定の Web サーバリソースへのアクセスをチェックするように標準ルールを記述できます。ただし、URI のエンコードにはさまざまな方法があります。たとえば、次の例はすべて同じ URI を示しています。

```
http://server/index.html
```

```
http://server././index.html
```

```
http://server/index%2ehtml
```

```
http://server/i%6edex.html
```

DPI エンジンには、URI の正規化をサポートしています。この機能は、Web Protocol Decoding ルールが適用されている場合のみ有効です。

次のパターンルールは、正規化されている URI にも適用されます。このルールは、上記のどちらのエンコーディングにも一致します。

```
<uri pat="index">  
    log "index"  
</uri>
```

新しいルールを使用して、HTTP の本文またはヘッダでこれらのルールが実行されないように制約する必要はありません。Web のデコーディングルールによって、HTTP プロトコルの状態は追跡されます。

Web リソースとクエリルール

?の前の URI の前半部分とクエリの後に続くパラメータ部分を区別できると役に立つ場合があります。uri ルールは、?の前の URI の前半部分のみに実行されます。パラメータどうしを照合するには、uriquery ルールを使用します。

```
<uriquery pat="client=firefox">  
  log "firefox"  
</uriquery>
```

URI パラメータは、HTTP POST 要求の本文でエンコードできます。uriquery ルールは、POST 本文のパラメータだけでなく、?の後の URI の後半部分も照合を行います。

Web ルールの考慮事項


uri ルールと通常のルールを混在させる場合や状態を使用する場合は注意が必要です。URI ルールが実行されるのは、URI のデコードと正規化の後です。通常、要求行の URI は完全な要求行になるまでデコードされませんが、raw トラフィックの他のルールは実行されます。raw 要求行に一致するパターンがある場合、通常、これらのパターンがトリガされてから uri ルールがトリガされます。


アプリケーションの種類

「アプリケーションの種類」で定義されたアプリケーションは、トラフィックの方向、使用しているプロトコル、およびトラフィックが通過するポートによって識別されます。アプリケーションの種類は、DPI ルールをグループ化するのに役立ちます。これらは DPI ルールを共通の目的でグループに分類するために使用されます。これにより、DPI ルールセットを選択してコンピュータに割り当てる処理が簡略化されます。たとえば、Oracle Report Server への HTTP トラフィックの保護に必要な DPI ルールセットを検討してみます。DPI ルールをアプリケーションの種類にグループ化することで、たとえば IIS サーバに固有のルールセットなどを除外しながら「Web Server Common」および「Web Server Oracle Report Server」セットでルールを簡単に選択できます。

「アプリケーションの種類」画面に、定義したアプリケーションの種類が、次の情報列と共に一覧表示されます。

アプリケーションの種類アイコン:

 通常の種類

 設定オプションがある種類

メイン画面から、次のことを実行できます。

- 新規 (📄) にアプリケーションの種類の新規定義を作成する
- 既存のアプリケーションの種類のプロパティ (🔗) を表示または変更する
- 既存のアプリケーションの種類を複製 (および変更) する (📄)
- アプリケーションの種類を削除する (✖)

「新規」(📄 新規) または「プロパティ」(🔗) をクリックして、「アプリケーションの種類プロパティ」画面を表示します。

アプリケーションの種類を作成または編集するには

パス: メインメニュー | 「Deep Packet Inspection」 > 「アプリケーションの種類」

1. 「📄 新規」をクリックして新しいアプリケーションの種類を作成するか、既存のアプリケーションの種類を選択して「プロパティ」(🔗) を選択し、アプリケーションの種類を変更します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - **名前**: アプリケーションの種類の名前。
 - **説明**: アプリケーションの種類の説明。
 - **クライアントプラグインの最小バージョン**: アプリケーションの種類を実装するのに最小限必要な脆弱性対策オプションクライアントプラグインのバージョン。
3. 「接続」エリアで、目的の情報を指定します。
 - **方向**: 通信を開始する方向。つまり、2つのコンピュータ間で接続を確立する最初のパケットの方向です。たとえば、Web ブラウザのアプリケーションの種類を定義する場合、これは通信を確立するための最初のパケットをサーバに送信する Web ブラウザであるため、「送信」を選択します (サーバからブラウザに流れるトラフィックを調査する場合も同じです)。特定のアプリケーションの種類に関連付けられた DPI ルールは、いずれかの方向に流れる個々のパケットを調査するために作成できます。
 - **プロトコル**: このアプリケーションの種類に適用されるプロトコル。
 - **ポート**: このアプリケーションの種類が監視するポート (トラフィックが例外的に許可されているポートは含まれません)。
4. 「設定」タブで、アプリケーションの種類に関連付けられた DPI ルールの処理を制御できます。たとえば、「Web Server Common」のアプリケーションの種類には「Web サーバからの応答を監視する」オプションがあります。このオプションの選択を解除すると、アプリケーションの種類に関連付けられた DPI ルールでは、送信元のポート 80 を経由する応答トラフィックが検査されません。

5. 「オプション」タブで、脆弱性対策オプションサーバプラグインがアプリケーションの種類を使用および適用する方法を設定できます。

たとえば、ほとんどのアプリケーションの種類には、そのアプリケーションを推奨設定の検索から除外するためのオプションがあります。つまり、「推奨設定から除外」オプションを選択すると、推奨設定の検索では、対象のアプリケーションが検出された場合でも、このアプリケーションの種類およびアプリケーションの種類に関連付けられた DPI ルールがコンピュータに推奨されません。

6. 「割り当て対象」タブで、アプリケーションの種類に関連付けられた DPI ルールを表示できます。



第10章

コンポーネント

この章では、脆弱性対策オプション™ 1.5 コンポーネントについて説明します。

この章で扱うトピックは次のとおりです。

- 142 ページの「コンポーネントについて」
- 142 ページの「IP リスト」
- 143 ページの「MAC リスト」
- 144 ページの「ポートリスト」
- 146 ページの「コンテキスト」
- 148 ページの「スケジュール」

コンポーネントについて

コンポーネントは、以下の再利用可能な項目のリストを作成します。

- **IP リスト**: 再利用可能な IP のリスト。
- **MAC リスト**: 再利用可能な MAC アドレスのリスト。
- **ポートリスト**: 再利用可能なポートのリスト。
- **コンテキスト**: ファイアウォールルールまたは DPI ルールが有効な状況を指定するコンテキスト。
- **スケジュール**: 再利用可能なスケジュール。

IP リスト

「IP リスト」画面を使用して、再利用可能な IP アドレスのリストを作成し、複数のファイアウォールルールで使用します。

メイン画面から、次のことを実行できます。



- 一から新しい IP リストを作成する (👤) (「新規」)
- XML ファイルから IP リストをインポートする (📄)
- 既存の IP リストのプロパティを確認または変更する (🔍)
- 既存の IP リストを複製 (および変更) する (📄)
- IP リストを削除する (✖)
- 1 つ以上の IP リストを XML ファイルにエクスポートする (📄) (「エクスポート ...」 ボタンをクリックして対象をすべてエクスポートするか、ドロップダウンリストで選択して、選択または表示された対象のみをエクスポートする)

「新規」 (👤「新規」) または「プロパティ」 (🔍) をクリックして、「IP リストプロパティ」ウィンドウを表示します。

IP リストのプロパティ

IP リストプロパティを作成または編集するには







パス: 脆弱性対策オプションのメインメニュー | 「コンポーネント」 → 「IP リスト」



1.  「新規」をクリックして、新しい IP リストプロパティを一から作成するか、または既存の IP リストを選択してから「プロパティ」() をクリックして、IP リストを修正します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - ・ **名前**: IP リストの名前。
 - ・ **「説明」**: IP リストの説明。
3. 「一般」タブの「IP」エリアで、リストに入れる IP アドレス、マスクされた IP アドレス、および IP アドレスの範囲を入力します。1 行ごとに 1 つのみ入力してください。
個々のアドレスだけでなく、IP 範囲とマスクされている IP も入力できます。「サポートされている形式」エリアの例を使用して、入力内容の形式を正しくします (テキストの先頭にナンバー記号 (#) を付けたコメントを IP リストに挿入できます)。
4. 「割り当て対象」タブで、この IP リストを使用するルールを表示できます。ルール名をクリックして「プロパティ」画面を表示します。

MAC リスト

「MAC リスト」を使用して、再利用可能な MAC アドレスのリストを作成します。

メイン画面から、次のことを実行できます。



- ・ 新規 () MAC リストを一から作成する
- ・ XML ファイルから MAC リストをインポートする ()
- ・ 既存の MAC リストのプロパティを確認または変更する ()
- ・ 既存の MAC リストを複製 (および変更) する ()
- ・ MAC リストを削除する ()
- ・ 1 つ以上の MAC リストを XML ファイルにエクスポートする () (「エクスポート ...」ボタンをクリックして対象をすべてエクスポートするか、ドロップダウンリストで選択して、選択または表示された対象のみをエクスポートする)

「新規」() 「新規」) またはプロパティ () をクリックして MAC リストの「プロパティ」ウィンドウを表示します。

MAC リストのプロパティ

MAC リストのプロパティを作成または編集するには

パス : 脆弱性対策オプションのメインメニュー | 「コンポーネント」 → 「MAC リスト」







1.  「新規」をクリックして、新しい MAC リストのプロパティを一から作成するか、または既存の MAC リストを選択してから「プロパティ」() をクリックして、MAC リストを修正します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - ・ **名前** : MAC リストの名前。
 - ・ **説明** : MAC リストの説明。
3. 「MAC」エリアで、リストに追加する MAC アドレスを入力します。1 行ごとに 1 つのみ入力してください。



MAC リストは、ハイフン区切りおよびカンマ区切りの両方の形式の MAC アドレスをサポートしています。「サポートされている形式」エリアの例を使用して、入力内容の形式を正しくします (テキストの先頭にナンバー記号 (＃) を付けたコメントを MAC リストに挿入できます)。
4. 「割り当て対象」タブで、この MAC リストを使用するルールを表示できます。ルール名をクリックして「プロパティ」画面を表示します。

ポートリスト

「ポートリスト」画面を使用して、再利用可能なポートのリストを作成します。

メイン画面から、次のことを実行できます。

- ・ 新規ポートリストを一から作成する ( 「新規」)
- ・ XML ファイルからポートリストをインポートする ()
- ・ 既存のポートリストのプロパティを確認または変更する ()
- ・ 既存のポートリストを複製 (および変更) する ()
- ・ ポートリストを削除する ()
- ・ 1 つ以上のポートリストを XML ファイルにエクスポートする () (「エクスポート ...」ボタンをクリックして対象をすべてエクスポートするか、ドロップダウンリストで選択して、選択または表示された対象のみをエクスポートする)

「新規」() または「プロパティ」() をクリックして、「ポートリストのプロパティ」ウィンドウを表示します。

ポートリストのプロパティ

ポートリストのプロパティを作成または編集するには

パス : 脆弱性対策オプションのメインメニュー | 「コンポーネント」 → 「ポートリスト」

1. 📁「新規」をクリックして、新しいポートリストのプロパティを一から作成するか、または既存のポートリストを選択してから「プロパティ」(🔗)をクリックして、ポートリストを修正します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - **名前** : ポートリストの名前。
 - **説明** : ポートリストの説明。
3. 「ポート」エリアで、リストに追加するポートを入力します。1 行ごとに 1 つのみ入力してください。

ポートの用途のリストについては、Internet Assigned Numbers Authority (IANA) を参照してください。

個々のポートおよびポート範囲をリストに含めることができます。「サポートされている形式」エリアの例を使用して、入力内容の形式を正しくします (テキストの先頭にナンバー記号 (#) を付けたコメントをポートリストに挿入できます)。
4. 「割り当て対象」タブで、このポートリストを使用するルールを表示できます。ルール名をクリックして「プロパティ」画面を表示します。

ポート検索を設定する

初期設定では、検索対象のポート範囲は「一般ポート」と言われる 1 ~ 1024 の範囲ですが、別のポートセットを検索するよう定義できます。

注意 : ポート範囲の設定に関係なく、ポート 4118 は常に検索されます。これは、サーバプラグインで開始された通信が送信されるコンピュータのポートです。コンピュータに対して通信方向が「クライアントプラグインによる開始」(「システム」→「システム設定」→「コンピュータ」) に設定されると、ポート 4118 は閉じます。

検索する新しいポート範囲を定義するには

1. 「コンポーネント」→「ポートリスト」に進み、メニューバーの「新規」をクリックします。「新規ポートリスト」画面が表示されます。
2. 「ポート」ボックスで、許容される形式を使用して新しいポートリストの名前と説明を入力してから、ポートを定義します (たとえば、ポート 100、105、および 110 ~ 120 を検索するには、1 行目に「100」、2 行目に「105」、および 3 行目に「110-120」と入力します)。「OK」をクリックします。
3. 「システム」→「システム設定」→「検索」に進み、「検索するポート」ドロップダウンメニューをクリックします。新しく定義したポートリストが 1 つの選択肢として表示されます。

コンテキスト

コンテキストは、コンピュータのネットワーク環境に応じてさまざまなセキュリティポリシーを実装する強力な方法です。

コンテキストは、ファイアウォールルールと DPI ルールと関連付けられるよう設計されています。ルールに関連付けられたコンテキストの定義条件に一致した場合、ルールは適用されます。(コンテキストにセキュリティルールを関連付けるには、セキュリティルールの「プロパティ」ウィンドウの「オプション」タブへ進み、「コンテキスト」ドロップダウンメニューからコンテキストを選択します。)







コンテキストは、クライアントプラグインに「場所を認識」させることができます。コンピュータの場所を判別するために、コンテキストでは、コンピュータとドメインコントローラとの接続方法、およびインターネットとの接続状況を確認します。「ドメインコントローラの接続が次の場合にコンテキストを適用」オプションを選択し、次のいずれかを選択します。



- **ドメインへのローカル接続**: コンピュータが直接ドメインコントローラへ接続できる場合にのみ設定する
- **ドメインとのリモート接続**: コンピュータが VPN 経由でドメインコントローラへ接続できる場合にのみ設定する
- **ドメインに接続されていない**: いかなる方法でもコンピュータがドメインコントローラへ接続できない場合に設定する
- **ドメインへの接続なし、インターネット接続なし**: いかなる方法でもコンピュータがドメインコントローラへ接続できず、インターネットにも接続されていない場合に設定する (インターネット接続のテストは、「システム」>「システム設定」>「コンテキスト」で設定可能)

コンピュータがドメインコントローラやインターネットへ接続可能かどうかを評価することで、クライアントプラグインは、ルート不可の(「プライベート」) IP アドレスにのみ HTTP トラフィックを限定するといったルールを実装できるようになります。

コンテキストを使用してファイアウォールルールを実装するセキュリティプロファイルの例については、「ロケーション識別 - 高」セキュリティプロファイルのプロパティを参照してください。

「コンテキスト」画面のツールバーまたは右クリックのショートカットメニューで、次の操作を実行できます。



- ・ 「新規」(「新規」) コンテキストを作成する
- ・ XML ファイルからコンテキストをインポートする()
- ・ 既存のコンテキストのプロパティを確認または変更する()
- ・ 既存のコンテキストを複製および変更する()
- ・ コンテキストを削除する()
- ・ 1つ以上のコンテキストを XML ファイルにエクスポートする() (「エクスポート ...」 ボタンをクリックして対象をすべてエクスポートするか、ドロップダウンリストで選択して、選択または表示された対象のみをエクスポートする)

「新規」() または 「プロパティ」() をクリックして、コンテキストの「プロパティ」ウィンドウを表示します。

コンテキストのプロパティ

コンテキストのプロパティを作成または編集するには

パス : 脆弱性対策オプションのメインメニュー | 「コンポーネント」 → 「コンテキスト」

1.  「新規」 をクリックして、新しいコンテキストルールのプロパティを一から作成するか、または既存のコンテキストルールを選択してから 「プロパティ」() をクリックして、コンテキストルールを修正します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - ・ **名前** : コンテキストルールの名前。
 - ・ 「説明」 : コンテキストルールの説明。
 - ・ **クライアントプラグインの最小バージョン** : ルールが互換性を持つ最も古いバージョンの脆弱性対策オプションクライアントプラグイン。

3. 「オプション」エリアで、以下の設定を行います。
 - **ドメインコントローラの接続が次の場合にコンテキストを適用**：このオプションは、コンピュータがドメインコントローラに接続する場合、またはインターネット接続に接続する場合、ファイアウォールルールを有効化するかどうかを決定します。(インターネット接続テストの条件は、「システム」>「システム設定」>「コンテキスト」で設定可能)。

ドメインコントローラへ ICMP 経由で直接接続できる場合は、「ローカル」接続になります。VPN 経由でのみ接続できる場合は、「リモート (VPN)」接続になります。

ドメインコントローラの接続テストの間隔は、インターネット接続テスト間隔と同じです。この間隔も、「システム」→「システム設定」→「コンテキスト」で設定できます。

注意： インターネット接続テストは、コンピュータがドメインコントローラに接続できない場合にのみ実行されます。

 - **インタフェース制限により制限されたインタフェースにコンテキストを適用**：このコンテキストは、インタフェース制限のためにトラフィックが制限されているネットワークインタフェースに適用されます。(主に許可または強制的に許可のファイアウォールルールで使用。)
4. 「割り当て対象」タブで、このコンテキストを使用するルールのリストを表示できます。

スケジュール

スケジュールは、特定のファイアウォールルールまたは DPI ルールを有効にする時間の定義に使用されるルールのコンポーネントです。スケジュールは、セキュリティプロファイルをアップデートするために、いつサーバプラグインがクライアントプラグインと通信するかを指定するのにも使用できます。

新しいセキュリティアップデートのダウンロードや適用など、ルール以外をベースとするその他の予約タスクは、「システム」→「タスク」から定義できます。

ツールバーまたは右クリックのコンテキストメニューで、次のことを実行できます。

- 新規スケジュールを作成する (🕒「新規」)
- XML ファイルからスケジュールをインポートする (📄)
- 既存のスケジュールのプロパティを確認または変更する (🔍)
- 既存のスケジュールを複製および変更する (📄)

- スケジュールを削除する (✖)
 - 1つ以上のスケジュールをXMLファイルにエクスポートする (🌐)(「エクスポート ...」ボタンをクリックして対象をすべてエクスポートするか、ドロップダウンリストで選択して、選択または表示された対象のみをエクスポートする)
- 「新規」(🕒「新規」)または「プロパティ」(🔗)をクリックして、スケジュールの「プロパティ」ウィンドウを表示します。

スケジュールのプロパティ

スケジュールのプロパティを作成または編集するには

パス: [脆弱性対策オプションのメインメニュー](#) | 「コンポーネント」 → 「スケジュール」

1. 🕒「新規」をクリックして、新しいスケジュールのプロパティを一から作成するか、または既存のスケジュールを選択してから「プロパティ」(🔗)をクリックして、スケジュールを修正します。
2. ポップアップウィンドウの「一般」タブの「一般情報」エリアで必要な情報を指定します。
 - **名前**: スケジュールの名前。
 - **説明**: スケジュールの説明。
3. スケジュールを定義します。スケジュール期間は、1時間の時間枠で定義します。時間枠をクリックするとその時間枠が選択され、<Shift> キーを押しながらクリックすると選択解除されます。
4. 「割り当て対象」タブで、このスケジュールを使用するルールを表示できます。



第11章

脆弱性対策オプションサーバプラグインの管理

この章では、脆弱性対策オプション™ 1.5 サーバの管理および設定について説明します。

この章で扱うトピックは次のとおりです。

- 152 ページの「脆弱性対策オプションサーバプラグインの保護」
- 153 ページの「サーバプラグインのアップグレード」
- 154 ページの「より大容量のデータベースへの移行」
- 157 ページの「管理下の単一コンピュータの新規脆弱性対策オプションサーバへの移行」
- 158 ページの「組込みデータベースの最適化」
- 160 ページの「脆弱性対策オプションデータの別のデータベースへの移行」
- 164 ページの「サーバプラグインのアップグレード」

脆弱性対策オプションサーバプラグインの保護

クライアントプラグインでサーバプラグインを保護する

脆弱性対策オプションサーバプラグインを保護するには、ホストコンピュータにクライアントプラグインをインストールして「**サーバプラグイン**」セキュリティプロファイルを適用します。

サーバプラグインのコンピュータ上でクライアントプラグインを設定する

1. 同じコンピュータにサーバプラグインとしてウイルスバスター Corp. クライアントをインストールします。
2. このコンピュータが、ウイルスバスター Corp. Web コンソールに「ネットワークで結ばれたコンピュータ」として表示されていることを確認してください。
3. 「コンピュータ」画面に進み、「**ウイルスバスター Corp. との同期**」ボタンをクリックします。
4. 「コンピュータ」画面で、新しいコンピュータをダブルクリックして「**詳細**」画面を表示し、「**Deep Packet Inspection**」→「**SSL 設定**」へ進みます。
5. 選択したコンピュータの SSL 設定リストが表示されます。「**新規**」をクリックしてウィザードを開始し、新規 SSL 設定を作成します。
6. サーバプラグインで使用するインタフェースを指定したら、「**次へ**」をクリックします。
7. 「**ポート選択**」画面で、HTTPS 上のサーバプラグインの Web アプリケーション GUI で使用しているポートを保護するよう選択します。インストール時に別のポートを選択しないかぎり、初期設定では 4119 です。サーバプラグインで使用しているポートを確認するには、アクセスに使用する URL を確認してください。「**次へ**」をクリックします。
8. SSL DPI 分析をこのコンピュータのすべての IP アドレスで実行するのか、それとも 1 つの IP アドレスでのみ実行するのかを指定します。(この機能は、1 つのコンピュータに複数の仮想マシンを設定する場合に使用できます。)
9. 次に、「脆弱性対策オプションサーバプラグインに組み込まれている SSL 資格情報を使用します」を選択します(このオプションは、サーバプラグインのコンピュータの SSL 設定を作成する場合にのみ表示されます)。「**次へ**」をクリックします。
10. ウィザードを終了して、「**SSL 設定**」画面を閉じます。
11. コンピュータの「**詳細**」画面に戻り、「**サーバプラグイン**」セキュリティプロファイルを適用します。これには、脆弱性対策オプションサーバプラグインがポート 4119 で動作するのに必要なファイアウォールルールおよび DPI ルールが含まれます。

これでサーバプラグインのコンピュータは保護され、サーバプラグインへの SSL を含むトラフィックはフィルタされます。

注意： SSL トラフィックをフィルタするようにクライアントプラグインを設定すると、脆弱性対策オプションクライアントプラグインからいくつかの更新エラーイベントが返されることがあります。これらは、サーバプラグインコンピュータで発行された新しい SSL 証明書が原因の証明書の更新エラーです。サーバプラグインのブラウザセッションを再起動して、サーバプラグインコンピュータから新しい証明書を取得する必要があります。

「サーバプラグイン」セキュリティプロファイルには、サーバプラグインをリモートで利用できるように基本のファイアウォールルールが割り当てられています。サーバプラグインのコンピュータを別の目的で使用する場合は、追加でファイアウォールルールを割り当てる必要があります。また、このセキュリティプロファイルには、アプリケーションの種類「Web Server Common」の DPI ルールが含まれます。必要に応じて、DPI ルールを追加で割り当てることもできます。

アプリケーションの種類「Web Server Common」は、「HTTP」ポートリストのポート (4119 を含まない) をフィルタすることが一般的であるため、セキュリティプロファイルの「詳細」画面の「DPI ルール」画面にあるポート設定に対して、ポート 4119 を優先として追加します。

サーバプラグインのアップグレード

脆弱性対策オプションサーバプラグインの新規バージョンが使用可能かどうかは、「ウイルスバスター Corp. プラグインマネージャ」画面に表示されます。新規バージョンは現行バージョンの上に表示されます。新規バージョンにアップグレードするには、「ダウンロード」ボタンをクリックします。新規バージョンのダウンロードが終了したら、「**今すぐアップグレード**」をクリックしてサーバプラグインをアップグレードします。

注意： 脆弱性対策オプションサーバプラグインをアップグレードする前に、ウイルスバスターコーポレートエディションおよびプラグインマネージャの必要最低限のバージョンがインストールされていることを確認してください (「[脆弱性対策オプションインストールガイド](#)」を参照)。

より大容量のデータベースへの移行

脆弱性対策オプションでは、Microsoft SQL Server 2005 をインストールして、それをデータベースとして使用します。しかし、4GB の上限がある Microsoft SQL Server 2005 では、容量が足りない場合もあります。容量がより大きい SQL Server Enterprise データベースへ移行するには、次の手順に従ってください。別の対応するデータベースへ移行する場合は以下の製品 Q&A をご参照下さい。

<http://esupport.trendmicro.co.jp/Pages/JP-2080172.aspx>

注意： 一般的には SQL Browser サービスを起動しませんが、特に「初期設定」インスタンスを使用する場合など、インスタンスによっては起動させる必要があります。詳細は、Microsoft の SQL Server Browser サービスのページを参照してください。

注意： Windows 認証によるリモート接続には、対応していません。データベースへの脆弱性対策オプション接続は、混合モードまたは SQL Server 認証で行います。

1. 対象となるデータをバックアップします。この処理は、予約タスクで実行できます。「システム」→「タスク」→「新規」に進みます。
2. 頻度を「一回のみ」に設定します。
3. 保存先を「C:¥dbbackup」などとして、「バックアップ」タスクタイプを選択します。
4. タスクを実行します。
5. 「バックアップの完了」イベントのシステムイベントを監視します。
6. イベントが表示されたら、すぐに Windows サービスの「コントロールパネル」から「脆弱性対策オプション」サービスをシャットダウンします。これにより、バックアップ後に新規のログ/データが作成されなくなります。
7. データベースのバックアップファイル (C:¥dbbackup¥IDFBackup.bak など) を探し、新規データベースが保存されるコンピュータへファイルをコピーします (または、そのファイルを利用可能にします)。
8. バックアップを復元します。たとえば、「idf-restore1」というデータベースを新しく作成します。ファイルを右クリックして「タスク」→「復元...」を選択し、「デバイス」内のファイルをリンクしてから「オプション」タブの「既存データベースの上書き」を選択します。

注意： 実際の設定は、利用環境によって異なる場合もあります。

9. データベースを移行したら、新規データベースを参照するように脆弱性対策オプションで設定します。脆弱性対策オプションサーバホストで、次のファイルを編集します。

```
C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense
Firewall\webclient\webapps\ROOT\WEB-INF\dsm.properties
```

10. ファイルをアップデートします。

簡単な dsm.properties ファイルは、次のように記述されています。

```
#Wed Jun 11 16:19:19 EDT 2008
database.SqlServer.user=sa
database.name=IDF
database.directory=null¥¥
database.SqlServer.password=$1$87251922972564e6bb3e2da9e688cd4ceb42b9b
fb17a942c3c8ad99ff05938c81
database.SqlServer.instance=IDF
mode.demo=false
database.SqlServer.namedPipe=true
database.type=SqlServer
database.SqlServer.server=.
manager.node=1
```

これを、次のように変更します。

```
#Wed Jun 11 16:19:19 EDT 2008
database.SqlServer.user=sa
database.name=idf-restore1
database.directory=null¥¥
database.SqlServer.password=<cleartext password>
database.SqlServer.instance=
mode.demo=false
database.SqlServer.namedPipe=false
database.type=SqlServer
database.SqlServer.server=bdurie-desktop
manager.node=1
```

注意： オプションは利用環境によって異なる場合もありますが、名前付きパイプを選択する場合は、脆弱性対策オプションサーバホストとデータベースホストの間に正しい Windows 認証 / 信頼が存在することを確認してください。TCP を選択する場合は、データベースで利用できることを確認してください。

11. 脆弱性対策オプションサーバの「脆弱性対策オプションサーバ」サービスを再起動します。

注意： アップグレード後も正常に稼働し、新しいデータベースインスタンスを参照しますが、古いデータベースは削除されません。古いデータベースを削除する必要はありませんが、必要に応じて削除できます。

管理下のコンピュータの新規脆弱性対策オプションサーバへの移行

既存のクライアントプラグインがインストールされているコンピュータは、そのクライアントプラグインがインストールされたままで無効化もされていない場合に限り、設定を失うことなく別の脆弱性対策オプションサーバに移行できます。

注意： 無効化処理（「コンピュータ」画面で、コンピュータを右クリックして、「処理」→「無効化」の順に選択して実行）によって、クライアントプラグインが現在のサーバプラグインの排他的制御から解放され、有効になっていたすべてのフィルタとルールが削除されます。

移行処理は、基本的にバックアップおよび復元処理（「161 ページの「脆弱性対策オプションのバックアップおよび復元」を参照）と同じですが、サーバプラグインに新しいホスト名を通知する手順が加わります。

コンピュータを新しい脆弱性対策オプションに移行するには

1. 「161 ページの「脆弱性対策オプションのバックアップおよび復元」で説明されているとおりに、移行元にインストールされた脆弱性対策オプションでバックアップ処理を実行します。
2. 脆弱性対策オプションのインストール手順と同じ手順で、脆弱性対策オプションサーバプラグインを新しいウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）サーバにインストールします。
3. Microsoft SQL Server のバックアップディレクトリ（通常は C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\IDFBackup.bak）にある IDFBackup.bak という名前のファイルを、移行元から新しい脆弱性対策オプションの SQL サーバのバックアップディレクトリにコピーします。
4. 「161 ページの「脆弱性対策オプションのバックアップおよび復元」で説明されているとおりに、復元処理を実行します。

- 脆弱性対策オプションのルートディレクトリから、次の `idf_c.exe` コマンドを、「NewComputerName」をアップデートしたホスト名に置き換えて実行することにより、復元した新しい脆弱性対策オプションサーバプラグインに新しいホスト名を通知します。(ホスト名は静的 IP アドレスか完全修飾名です)。

```
idf_c -action changesetting -name "configuration.dsmUrl" -value  
"NewComputerName"
```

たとえば、ホスト名を OfficeScan_Win2K に変更するには、次のコマンドを実行します。

```
idf_c -action changesetting -name "configuration.dsmUrl" -value  
"OfficeScan_Win2K"
```

新しくインストールされた脆弱性対策オプションで、移行前のクライアントプラグインが検出および認識され、処理が前と同じように続行されます。

管理下の単一コンピュータの新規脆弱性対策オプションサーバへの移行

単一コンピュータを新しい脆弱性対策オプションに移行できます。ただし、バックアップファイルを使用して元の脆弱性対策オプションから新しい脆弱性対策オプションサーバプラグインを「復元」しなければ、設定情報は保持されません(「161 ページの「脆弱性対策オプションのバックアップおよび復元」」を参照)。

単一コンピュータを別の脆弱性対策オプションに移行するには

- 現在のサーバプラグインの「コンピュータ」画面にあるコンピュータを右クリックして「処理」→「無効化」の順に選択し、クライアントプラグインを無効にします。
- ウイルスバスター Corp. 管理コンソールの「クライアントの移動」機能を使用して、コンピュータをサーバに移動します(ウイルスバスター Corp. サーバのコンピュータリストは、サーバプラグインの「コンピュータ」画面に自動的に表示されます)。
- 新しい脆弱性対策オプションサーバプラグインの「コンピュータ」画面にあるコンピュータを右クリックして「処理」→「有効化/再有効化」の順に選択し、クライアントプラグインを有効にします。

新しいサーバプラグインによってクライアントプラグインが有効になります。古いサーバプラグインはクライアントプラグインと通信できなくなります。

組み込みデータベースの最適化

サーバプラグインは、データストレージとして Microsoft SQL Server Express をインストールして使用します。特長は、次のとおりです。

Microsoft SQL Server Express の上限 : 4GB

Microsoft SQL Server Express のデータベース容量を増やすことはできませんが、SQL Server データベースのように容量制限のないデータベースへ移行することはできます。移行手順が用意されています (手順については、「154 ページの「より大容量のデータベースへの移行」」を参照)。詳細については、サポート担当者へ問い合わせてください。

ログのアーカイブ

SQL Server Express のデータ容量は、アーカイブに適していません。監査およびコンプライアンス要件に対応するには、データベースを定期的にバックアップする必要があります。スケジュールバックアップの作成の詳細については、「161 ページの「脆弱性対策オプションのバックアップおよび復元」」を参照してください。

データベースで使用するスペースを最小化する

脆弱性対策オプションサーバはデータベース内にイベントを格納し、ある期間が過ぎたイベントは自動で消去します。イベントの最大保存期間は、脆弱性対策オプションサーバで設定できます。これにより、管理者が特定の種類のイベントを脆弱性対策オプションサーバで保存する期間について調整でき、そのためデータベースの使用量を効果的に調整できます。

脆弱性対策オプションサーバで削除設定を行うには、「システム」→「システム設定」から「システム」タブを選択し、「削除」内の設定を編集します。これらの設定変更はすぐに有効になりますが、削除は 1 時間に 1 回だけ実行されるため、脆弱性対策オプションサーバから実際に削除されるのは最も遅くて一時間後になる場合があります。

どの削除設定が短縮の恩恵を被るのかを判断するには、SQL Server のデータベースツールでデータベース内を調査し、どのテーブルが最も多くの容量を使用しているかを探ります。

<http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en>

上記のツールを使用する場合は、ツールを脆弱性対策オプションサーバのホストにインストールします。ツールを起動して脆弱性対策オプションインスタンスへログインしたら、「脆弱性対策オプション」データベースを開いてテーブルを表示し、下にリストされたテーブルのプロパティを取得して容量を確認します。Microsoft SQL Server Express は最大でも 4GB であることから、下記のテーブルで 1GB を超えているものは「大きすぎる」ので、可能であれば削除する設定値を下げます。以下のテーブルは、「ファイアウォール /DPI イベント」の削除設定に含まれています。

packetlogs

payloadlogs

payloadlogdatas

以下のテーブルは、「システム / クライアントプラグインのイベント」の削除設定に含まれています。

systemevents

agentevents

以下のテーブルは、「カウンタ」の削除設定に含まれています。

counter3s

counter3ports

counter3ips

脆弱性対策オプションデータベースの容量の縮小

初期設定の Microsoft SQL Server Express データベースの最大データ容量は 4GB ですが、データベース自体のログファイル (IDF_Log.mdf) は必要に応じて拡張できます。極端な例では、本体のデータベースファイルと同じ 4GB まで増やすことができます。

状況によっては、実際のディスクスペースの消費を抑えるために、データベースを圧縮することができます。

脆弱性対策オプションデータベースでは、SQL Server ツールからのみこの操作を実行できます。操作は Microsoft SQL Server Express 管理ツール、または同様のコマンドラインツールで実行します。いずれも Microsoft より無償で提供されています。

<http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en>

<http://www.microsoft.com/Downloads/details.aspx?familyid=FA87E828-173F-472E-A85C-27ED01CF6B02&displaylang=en>

脆弱性対策オプションサーバにコマンドラインツールをインストールしたら、次のコマンドでデータベースを圧縮します。

```
sseutil -shrink name=IDF -server .¥IDF -m
```

一般的に縮小は論理ログで実行します。論理ログはデータベースよりも急速に増大し、消去されないこともあります。

論理ログのスペースを解放するには

1. フルバックアップを実行します。
2. 論理ログをバックアップします。
3. 次の2つのSQLクエリを実行して、スペースを解放します。

```
USE idf
GO
Checkpoint
USE idf
DBCC SHRINKFILE(idf_log, 1)
BACKUP LOG WITH TRUNCATE_ONLY
DBCC SHRINKFILE(idf_log, 1)
```

注意：他にも、Microsoftでは推奨していませんが、技術的にはファイルを圧縮するオプションがあります。脆弱性対策オプションデータベースを「自動縮小」モードに切り替える方法です。これは上記で述べた後者のGUIツールを使用し、「データベース」→「脆弱性対策オプション」モードを選択したら、右クリックして「プロパティ」→「オプション」を選択し、「自動縮小」モードを「True」に設定します。

脆弱性対策オプションデータの別のデータベースへの移行

移行手順が用意されています（「154ページの「より大容量のデータベースへの移行」を参照）。詳細については、サポート担当者へ問い合わせてください。

脆弱性対策オプションのバックアップおよび復元

脆弱性対策オプションでは、データベースとして Microsoft SQL Server Express が使用されます。このデータベースには、以下のような脆弱性対策オプションのすべてのデータが格納されます。

- すべてのログおよびイベント
- セキュリティプロファイル
- IPS フィルタ
- ファイアウォールルール
- ステートフル設定
- すべてのコンポーネント (IP リスト、MAC リスト、ポートリストなど)
- アラート設定
- システム設定
- すべてのコンピュータのクライアントプラグインの設定

注意： 脆弱性対策オプションでは常に、これらの項目の最初の 8 つをウイルスバスター Corp. サーバに復元できますが、9 番目の「すべてのコンピュータのクライアントプラグインの設定」を復元するには、ウイルスバスター Corp. サーバに、脆弱性対策オプションのバックアップが実行されたときと同じウイルスバスター Corp. 生成の一意の ID を持つネットワークで結ばれたコンピュータの同じリストが必要です。このリストがあると、次のアップデート処理のときに、バックアップされているセキュリティプロファイル (その他の要素すべて) がサーバプラグインからクライアントプラグインに配信され、クライアントプラグインはバックアップ実行時と同じ設定の同じ状態に戻ります。

ウイルスバスター Corp. サーバで、ネットワークで結ばれたコンピュータのリストを最初から再度作成する必要がある場合、新しい一意の ID が各コンピュータに割り当てられますが、その場合サーバプラグインではコンピュータを認識できなくなるため、前の設定を復元することはできません。

バックアップ

定期的なデータベースバックアップをスケジュールするには、「システム」→「タスク」に進み、ツールバーの「新規」ボタンをクリックして予約タスクウィザードを開始します。ドロップダウンリストから「バックアップ」を選択し、次に表示される2つの画面で、バックアップ実行の頻度を指定します。出力場所の指定を求められたら、SQL サーバのバックアップディレクトリを指定します。通常、以下の場所にあります。

```
C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\
```

ウィザードの次の手順で、新しいスケジュールタスクの名前を入力するように求められ、スケジュールタスクウィザードの終了後にタスクを実行するオプションが提供されます。

バックアップは、IDFBackup.bak という名前の1つのSQL Server バックアップファイルに格納されます。バックアップが実行されるたびに、データがバックアップファイルに追加されます。バックアップファイルに追加される各バックアップ「インスタンス」は、バックアップファイルに15日間保持された後、バックアップが次に実行されるときに上書きされます。

復元

最後のバックアップから復元するには

1. Microsoft 管理コンソールスナップインの「サービス」から「脆弱性対策オプション」サービスを停止します。
2. 脆弱性対策オプションのルートディレクトリ (通常は C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall) から IDFRestore.bat を実行します。
3. 「脆弱性対策オプション」サービスを開始します。

復元時には、IDFRestore.bat によって、SQL SERVER バックアップディレクトリにある IDFBackup.bak からの復元が試行されます。

バックアップおよび復元のオプションを変更する

バックアップ

脆弱性対策オプションには、バックアップを手動で実行する際に使用する IDFBBackup.bat というファイルが含まれています。このファイルは、脆弱性対策オプションのルートディレクトリ (通常は C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall) にあります。

バックアップを格納するディレクトリ、バックアップファイル名、またはバックアップ保持日数 (初期設定では 15 日間) を変更する場合は、IDFBBackup.bat を使用します。

バックアップファイルが格納されるディレクトリを変更したり、バックアップ「インスタンス」が保持される日数を変更するには、IDFBBackup.bat をテキストエディタで編集する必要があります。

backUpFile パラメータによって、バックアップファイルのファイル名と格納場所が指定されません。retainDays パラメータによって、バックアップ「インスタンス」が保持される日数が指定されます。

たとえば、バックアップファイルを C:\IDF Backups\MyIDFBBackup.bak に変更して、保持日数を 7 日間に変更するには、IDFBBackup.bat に次のような変更を加えます。

```
CALL sqlcmd -S localhost\IDF -E -v backUpFile="C:\IDF
Backups\MyIDFBBackup.bak" retainDays=7 -i "IDFBBackup.sql"
```

注意： バックアップを格納するディレクトリは、バックアップを実行する前にすでに存在している必要があります。上の例では、ディレクトリは C:\IDFBackups\ です。

IDFBBackup.bat を使用してスケジュールバックアップを設定する

IDFBBackup.bat を使用して定期的なバックアップをスケジュールするには、Windows のスケジュールタスクを作成する必要があります。Windows のスケジュールタスクには、Windows の「コントロール パネル」からアクセスできます。

スケジュールバックアップタスクの作成時には、Windows で実行するプログラムとして IDFBBackup.bat を選択します。これには、脆弱性対策オプションのルートディレクトリ (通常は、C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall) を参照する必要があります。Windows のスケジュールタスクウィザード内で、バックアップを実行する時間と周期を選択できます。

復元

バックアップの復元元のディレクトリおよびファイルを変更するには、IDFRestore.bat をテキストエディタで編集する必要があります。backUpFile パラメータを変更します。

たとえば、バックアップファイルを C:¥IDF Backups¥MyIDFBackup.bak に変更するには、IDFRestore.bat に次のような変更を加えます。

```
CALL sqlcmd -S localhost¥IDF -E -v backUpFile="C:¥IDF
Backups¥MyIDFBackup.bak" -i "IDFRestore.sql"
```

サーバプラグインのアップグレード

ウイルスバスター Corp. プラグインマネージャから、「脆弱性対策オプション」画面の「アンインストール」をクリックします。



図 11-1. サーバプラグインのアンインストール

注意： 脆弱性対策オプションサーバプラグインは、コントロールパネルの「プログラムの追加と削除」アプレットを使用してアンインストールすることはできません。



第12章

システム

この章では、脆弱性対策オプション™ 1.5 システムを監視および管理する方法について説明します。

この章で扱うトピックは次のとおりです。

- 166 ページの「システムについて」
- 166 ページの「システムイベントの表示」
- 170 ページの「システム設定」
- 189 ページの「タグ」
- 190 ページの「タスク」
- 191 ページの「ライセンス」
- 191 ページの「アップデート」

システムについて

「システム」画面では、以下のすべてを管理できます。

- ・ **システムイベント**：「システムイベント」画面を使用して、セキュリティ関連のイベントではない、システム関連のイベントを確認します。
- ・ **システム設定**：「設定」セクションでは、脆弱性対策オプションシステムの管理を制御できます。
- ・ **タグ**：現在定義されているすべてのタグは、「タグ」画面に表示されます。
- ・ **タスク**：「タスク」セクションでは、定期的なイベントベースの自動タスクを設定することができます。
- ・ **ライセンス**：「ライセンス」ページには、利用可能な脆弱性対策オプションモジュールや、クライアントプラグインソフトウェアをインストールできるコンピュータ数など、トレンドマイクロ製品のライセンスの詳細が表示されます。
- ・ **アップデート**：「アップデート」セクションでは、セキュリティやソフトウェアのアップデートを管理できます。

システムイベントの表示

「システムイベント」画面には、システムイベントログが一覧表示されます。このログは、セキュリティ関連のイベントとは対照的な、システム関連のイベントの記録です。可能性のあるシステムイベントのリストについては、「238 ページの「システムイベント」」を参照してください。「システムイベント」画面には、イベントごとに次の情報が表示されます。

- ・ **時刻**：脆弱性対策オプションサーバプラグインをホストするコンピュータ上のシステムクロックに準じた時刻。
- ・ **レベル**：発生したイベントの重要度。イベントレベルには、情報、警告、エラーが含まれます。
- ・ **イベント ID**：イベントの種類に一意の識別子。
- ・ **イベント**：イベント ID に関連付けられたイベントの名前。
- ・ **対象**：イベントに関連付けられたシステムオブジェクトは、ここで識別されます。オブジェクトの ID をクリックすると、オブジェクトのプロパティシートが表示されます。
- ・ **イベント送信元**：イベントの送信元。
- ・ **処理実行者**：イベントがユーザによって開始された場合は、イベントを開始したユーザ。
- ・ **サーバプラグイン**：脆弱性対策オプションサーバプラグインコンピュータのホスト名。

メイン画面から、次のことを実行できます。

- ・ システムイベントの詳細（プロパティ）を**表示** (🔍) する
- ・ 特定のシステムイベントを**検索** (🔍) する
- ・ 現在表示されているシステムイベントを CSV ファイルに**エクスポート** (📄) する

さらに、ログエントリを右クリックすると、次のオプションが表示されます。

- ・ **タグの追加**: イベントタグをこのイベントに追加します（「168 ページの「イベントのタグ付け」を参照してください）。
- ・ **タグの削除**: 既存のイベントタグを削除します。

システムイベントの詳細の表示方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システムイベント」

1. イベントを選択し、「**表示**」 (🔍) をクリックすると、「システムイベント表示ツール」画面が表示されます。
2. 「一般情報」エリアには、選択したイベントの情報を表示できます。
3. 「説明」エリアには、必要に応じて、どのような処理が実行されてシステムイベントログにこのエントリがトリガされたのか、処理の詳細が表示されます。
4. 「**タグ**」タブをクリックすると、このイベントに関連付けられているタグが表示されます。
詳細なタグ情報を表示するには、「システム」 → 「システム設定」 → 「タグ」を参照してください。イベントのタグ付けの詳細については、「168 ページの「イベントのタグ付け」を参照してください。

リストのフィルタリングおよびイベントの検索

「期間」 ツールバーを使用してリストをフィルタし、特定の期間内に発生したイベントだけを表示できます。

「コンピュータ」 ツールバーを使用すると、コンピュータドメイン別またはコンピュータセキュリティプロファイル別にイベントログエントリの表示を整理できます。

「詳細検索」をクリックすると、検索バーの表示を切り替えることができます。



図 12-1. 「コンピュータ」ツールバー

検索バーの右側にある「検索バーの追加」ボタン (+) をクリックすると、追加の検索バーが表示され、検索に複数のパラメータを適用できます。準備が整ったら、「送信」ボタンをクリックします（ツールバーの右側にある上部に右矢印の付いたボタン）。

イベントをエクスポートする

表示されたイベントは CSV ファイルにエクスポートできます。（ページングは無視され、すべてのページがエクスポートされます。）表示されたリストを表示するか、または選択したアイテムを表示するかを選択できます。

イベントのタグ付け

イベントのタグ付けでは、管理者が手動でイベントにカスタムのラベル（たとえば「これは Tom が再確認」など）を付けることができます。

イベントに手動でタグを付けるだけでなく、「参照コンピュータ」を使用してタグ付けを自動化することもできます。たとえば、あるパッチの計画済みのロールアウトを参照コンピュータに適用し、パッチの適用に関連付けられたイベントに「Patch X」というタグを付けて、その他のシステムで発生する同様のイベントを自動的に「許容可能な変更」と見なすことで、管理者が検討対象にするイベント数を減らせます。

イベントのタグ付けを使用すると、イベントの特殊なビュー、ダッシュボード、およびレポートが有効になります。また、イベントのタグ付けは単一イベント、類似する複数のイベント、または将来的に発生する同様のすべてのイベントに適用できます。

イベントにタグを付ける

イベントのタグ付けでは、手動でシステムイベントにカスタムのラベル (たとえば「これは Tom が再確認」など) を付けることができます。イベントのタグ付けを使用すると、イベントの特殊なビュー、ダッシュボード、およびレポートが有効になります。また、イベントのタグ付けは単一イベント、類似する複数のイベント、または将来的に発生する同様のすべてのイベントに適用できます。

タグを 1 つまたは複数の選択したイベントに適用するには：

パス：脆弱性対策オプションメインメニュー | 「システム」 → 「システムイベント」

1. 「イベント」リストでイベントを選択してから右クリックして「タグを追加 ...」を選択します。
2. タグの名前を入力します (文字を入力していくと、一致する既存のタグが候補として表示されます)。
3. 「選択された 1 個のシステムイベント」を選択します。(「イベント」リストから複数のイベントを選択した場合、選択したイベントの数が表示されます。)「次へ」をクリックします。
4. 必要に応じてコメントを記入し、「完了」をクリックします。

「イベント」リストで、イベントにタグが付けられたことを確認できます。

複数の同様のイベントにタグを付けるには

1. 「イベント」リストの中からベースにするイベントを右クリックし、「タグを追加 ...」をクリックします。
2. タグの名前を入力します (文字を入力していくと、一致する既存のタグが候補として表示されます)。
3. 「類似のシステムイベントにも適用」を選択します。「次へ」をクリックします。
4. イベントが同様のものかどうかの判定基準となる属性を選択します。ほとんどの場合、属性オプションは「イベント」リスト画面の列に表示される情報と同じです。イベントの選択処理に含めるための属性を選択したら、「次へ」をクリックします。
5. このルールを適用する類似システムイベントの種類を選択します。

注意：「自動タグルール」の保存」オプションについて。指定した選択条件を保存すると、将来、新しいイベントが増えたときに、その条件を適用することができます。保存した自動タグ付けルールは、「システム」 > 「タグ」画面で確認できます。

6. 「次へ」をクリックします。

7. 必要に応じてコメントを記入し、「次へ」をクリックします。
8. イベントの選択条件を概要で確認し、「完了」をクリックします。

「イベント」リストで、ベースにしたイベントおよび同様のすべてのイベントにタグが付けられていることを確認できます。

複数の同様のイベントおよび将来の同様のイベントにタグを付けるには

複数の類似イベントおよび将来のイベントにタグを付ける手順は、上述の手順と手順 5 以外は同じです。ここでは、「新規システムイベント」も選択できます。「新規システムイベント」を選択すると、脆弱性対策オプションサーバプラグインは 5 秒 (またはそれ以上) ごとにデータベースを検索して新しいイベントを探し、該当するイベントにタグを付けます。

注意: タグ付けが実行されるのは、クライアントプラグインから取得されたイベントが脆弱性対策オプションサーバプラグインのデータベースに登録された後です。

システム設定

「システム」→「システム設定」画面では、脆弱性対策オプションシステムの管理を制御できます。このセクションは、セッションタイムアウト、システムアラート、クライアントプラグインとサーバプラグイン間の通信、ハートビート設定などのシステム設定などを管理するために使用します。

注意: 「設定」画面の右下に「保存」ボタンがあります。これらの設定 (すべてのタブ) に加えられた変更は保存しないと、有効になりません。

- コンピュータ
- ファイアウォールと DPI
- インタフェースの分離
- コンテキスト
- 攻撃の予兆検索
- 通知
- ランク付け
- アップデート
- システム

コンピュータ

コンピュータ設定の設定方法は、次のとおりです。

パス：脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. まだ開いていない場合は、「コンピュータ」タブをクリックします。
2. 「通信方向」エリアで、次のいずれかを選択します。
 - **双方向**：初期設定では、通信は双方向です。クライアントプラグインはハートビートを正常に開始しますが、サーバプラグインの接続をクライアントプラグインのポートでまだ待機しています。サーバプラグインは、必要に応じて処理を実行するためにクライアントプラグインに自由に接続できます。これによって、サーバプラグインは、セキュリティ設定に変更が発生すると、その変更内容をクライアントプラグインに適用できます。
 - **サーバプラグインによる開始**：このオプションを選択すると、すべてのサーバプラグインとクライアントプラグイン間の通信はサーバプラグインから起動されます。これには、セキュリティ設定のアップデート、ハートビートの処理、およびイベントログの要求が含まれます。
 - **クライアントプラグインによる開始**：このオプションを選択すると、クライアントプラグインはポート 4118 で待機しません。代わりに、ハートビート設定によって決められているハートビートのポート（初期設定では 4120）のサーバプラグインに接続します。クライアントプラグインがサーバプラグインと TCP 接続を確立したら、すべての通常の通信タスクが実行されます。サーバプラグインはクライアントプラグインにステータスとイベントを問い合わせます。（これはハートビートの処理です。）コンピュータで実行する必要がある未解決処理がある場合（セキュリティプロファイルのアップデートが必要など）、これらの処理は接続が終了する前に実行されます。このモードでは、サーバプラグインとクライアントプラグイン間の通信のみがハートビートごとに発生します。クライアントプラグインのセキュリティ設定が変更された場合、次のハートビートまでアップデートされません。

注意： クライアントプラグインは、サーバプラグインのホスト名によってネットワーク上の脆弱性対策オプションサーバプラグインを検索します。このため、クライアントプラグインによる開始または双方向の通信を使用する場合は、サーバプラグインのホスト名が必ずローカル DNS 内にある必要があります。

サーバプラグインとクライアントプラグイン間の通信を有効にするために、サーバプラグインは、クライアントプラグインのポート 4118 を開く (非表示の) ファイアウォールルール (優先度 4、放置) を受信 TCP/IP トラフィックに自動的に実行します。初期設定では、すべての IP アドレスおよびすべての MAC アドレスを開くようになっています。特定の IP または MAC アドレスから受信 TCP/IP トラフィックのみを許可する新しい優先度 4 (強制的に許可またはファイアウォールルールを放置) を作成することで、このポートの受信トラフィックを制限できます。設定が次の内容と一致する場合、この新しいファイアウォールルールは、非表示のファイアウォールルールと置き換わります。

- **処理**: 強制的に許可または放置
- **優先度**: 4 – 最高
- **パケットの方向**: 受信
- **フレームの種類**: IP
- **プロトコル**: TCP
- **パケットの送信先ポート**: 4118 (または 4118 を含むリストまたは範囲)

これらの設定が有効な限り、新しいルールが非表示のルールと置き換わります。その後、IP または MAC アドレスのパケットソース情報を入力して、コンピュータへのトラフィックを制限できます。

3. IP がホスト名として使用されており、クライアントプラグインによって通信または検出が開始された後にコンピュータの IP の変更が検出された場合は、「ホスト名」エリアで、「ホスト名」エントリをアップデートするかどうかを選択します。たとえば、ネットワークに DNS がなく、動的 IP を使用している場合に、このオプションをオンにします (サーバプラグインは、通常、IP アドレスではなく一意のフィンガープリントによって、コンピュータ / クライアントプラグインを特定します)。
4. 「リモート有効化」エリアで、リモート有効化を有効にするかどうかを選択します。

クライアントプラグインをコンピュータへインストールおよび有効化するための初期設定プロセスは、次のとおりです。クライアントプラグインがコンピュータにインストールされてから、ユーザは脆弱性対策オプションサーバプラグインで「クライアントプラグインを有効化」します。有効化されると、サーバプラグインは独自の暗号化フィンガープリントをクライアントプラグインへ送信します。これにより、クライアントプラグインはフィンガープリントに基づき、サーバプラグインからの指示以外は許可しくなくなります。ただし、大規模な分散インストール環境など、サーバプラグインではなくクライアントプラグインで有効化することが望ましい状況もあります。その場合は、クライアントプラグインがコンピュータと通信して有効化できるよう、サーバプラグイン側で設定する必要があります。「リモート有効化」パネルを使用して、どのコンピュータがクライアントプラグインを独自に有効化できるかに制限を設けます。

クライアントプラグインによる有効化は、コマンドラインから実行します。クライアントプラグインの有効化に関するコマンドラインのオプションは、次のとおりです。

表 12-1. クライアントプラグインの有効化に関するコマンドラインのオプション

使用方法 : dsa_control 「/a <str>」 「/g <str>」 「/c <str>」 「/r」	
/a <str>	指定された URL の脆弱性対策オプションサーバからクライアントプラグインを有効化します。URL の形式は必ず「dsm://hostOrIp:port/」にしてください。「ポート」は、サーバプラグインのハートビートのポート (初期設定は 4120 です)。
/g <str>	クライアントプラグインの URL。初期設定は「https://127.0.0.1:4118/」。
/c <str>	証明書ファイル
/r	クライアントプラグインの設定をリセットします。

注意： 脆弱性対策オプションサーバプラグインに対して、初期設定のセキュリティプロファイルをセキュリティプロファイルが割り当てられていない、自身で有効化するクライアントプラグインへ送信するよう指示することができます。「割り当てるセキュリティプロファイル (セキュリティプロファイルが割り当てられていない場合)」を使用して、セキュリティプロファイルを選択します。

5. 「ハートビート」エリアで、次のオプションを設定します。

- ・ **ハートビート間隔 (分):** ハートビート間の経過時間。
- ・ **次の数を超えるハートビート数が失われた場合にアラートを発令:** 連続して複数のハートビートが失われる場合、クライアントプラグインまたはコンピュータに問題があることを示している可能性があります。この設定は、サーバプラグインがアラートを発令する前に許容される失われたハートビートの数を決定します (たとえば 3 を設定すると、サーバプラグインは 4 つ目の失われたハートビートのときにアラートを発令します)。

- ・ ハートビート間でコンピュータのローカルシステム時間が次の時間を超えて変更された場合にアラートを発令: クライアントプラグインがシステム時計への変更を検出できる場合 (Windows クライアントプラグイン)、これらのイベントはクライアントプラグインイベント 5004 としてサーバプラグインにレポートされます。ここに一覧表示された時間への変更を超えた場合、アラートがトリガされます。この機能をサポートしないクライアントプラグイン (Windows のクライアントプラグイン以外) については、サーバプラグインはハートビートの処理ごとにクライアントプラグインが報告するシステム時間を監視し、設定で指定された最大変更値よりも大きい場合にアラートを発令します。

注意: 時計の変更の検出 (Computer-Clock-Changed) アラートが発令されたら、アラートを手動で消去する必要があります。

6. 「コンピュータの自動アップデート」エリアで、コンピュータを自動的にアップデートするかどうかを指定します。

初期設定では、脆弱性対策オプションシステムのエLEMENTに変更を加えるたびに、該当するすべてのコンピュータはただちにアップデートされます。たとえば、ポートリストを編集する場合、すでにそのポートリストを使用しているすべてのコンピュータはただちにアップデートされます。(このような変更を加えた場合、「コンピュータ」画面を表示すると、アップデートされていることが確認できます。)「脆弱性対策オプションシステムの要素のいずれかを変更した後、該当するすべてのコンピュータは自動的にアップデートされます」オプションを設定しない場合は、変更が行われた後に、影響を受けるコンピュータを「コンピュータ」画面で探して右クリックし、コンテキストメニューの「クライアントプラグインを今すぐアップデート」を選択する必要があります。

注意: これはセキュリティアップデートにも適用されます。たとえば Oracle サーバ用の最新のポートリストがセキュリティアップデートに含まれている場合、手動オプションを選択しないかぎり、そのポートリストを現在使用しているすべてのコンピュータに対し、最新のポートリストが配信されます。

ファイアウォールと DPI の設定

ファイアウォールと DPI の設定の設定方法は、次のとおりです。

パス : 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「ファイアウォールと DPI」 タブをクリックします。
2. 「ネットワークエンジンモード」 エリアで、クライアントプラグインのネットワークエンジンが、インラインモードとタップモードのどちらで動作するかを選択します。

インラインモードで動作する場合、実際のパケットストリームはネットワークエンジンを通過します。ステートフルテーブルは維持され、ファイアウォールルールは適用され、侵入防御ルールがペイロードコンテンツに適用されるようトラフィックの正規化が実行されます。タップモードで動作する場合、実際のパケットストリームはクローン化され、メインストリームを迂回して流れます。タップモードでは、実際のパケットストリームは変更されません。すべての操作はクローン化されたストリーム上で行われます。

3. 「イベント」 エリアで、イベントを次のように設定します。

個々のログファイルの最大サイズ、および保持される最新ファイルの数を指定できます。イベントログファイルは、最大許容サイズに達するまで書き込まれ、最大サイズに達すると新しいファイルが作成され、そのファイルが最大サイズに達するまで書き込まれます。最大ファイル数に達すると、最も古いファイルが削除され、その後、新しいファイルが作成されます。通常、イベントログエントリのサイズは平均約 200 バイトであるため、4MB のログファイルには約 20,000 ログエントリが保持されます。ログファイルがどのぐらいの期間でいっぱいになるかは、実行されるルールの数によって異なります。

- **イベントログファイルの最大サイズ (クライアントプラグイン)**: 1 台以上のコンピュータで「ディスク容量の不足」アラートが表示されるようになったら、これらの設定を調整します。
- **保管するイベントログファイル数 (クライアントプラグイン)**: 1 台以上のコンピュータで「ディスク容量の不足」アラートが表示されるようになったら、これらの設定を調整します。
- **クライアントプラグインからのファイアウォールイベントの収集**: クライアントプラグインから最新のファイアウォールイベントをハートビートごとに取得します。
- **クライアントプラグインから DPI イベントを収集する**: クライアントプラグインから最新の DPI イベントをハートビートごとに取得します。

注意： イベントは、個々のイベントのレコードです。カウンタは、個々のイベントが発生した回数のレコードです。イベントは、「イベント」画面の表示に使用されます。カウンタは、ダッシュボードのウィジェット（過去7日間のファイアウォールイベントの数など）およびレポートの作成に使用されます。たとえば、イベント収集に Syslog を使用している場合に、カウンタのデータのみを収集する場合があります。イベントには大量のディスク容量が必要となる可能性があるため、データを重複して格納することは避けることがあります。

- **次の送信元 IP のイベントは記録しない：** このオプションは、脆弱性対策オプションで特定の信頼されたコンピュータからのトラフィックのイベントを記録しないようにする場合に役立ちます。
-

注意： 集約されたイベントは、次の3つの設定で調整します。ディスク容量を節約するため、脆弱性対策オプションクライアントプラグインは複数発生する同一イベントを1つのエントリに集約し、「繰り返し回数」、「初出現」、「最終出現」のタイムスタンプに追加します。イベントエントリを集約するには、クライアントプラグインはディスクへ書き込む前、イベントが集約されている間にメモリ内へエントリをキャッシュする必要があります。

- **キャッシュサイズ：** 指定された時間にいくつのイベントの種類を追跡するか決定します。値を10に設定すると、繰り返し回数、初出現、最終出現のタイムスタンプを付けた、10種類のイベントを追跡することになります。新規のイベントの種類が発生すると、最も古い10のイベントは集約され、キャッシュから消去されてディスクに書き込まれます。
 - **キャッシュの寿命：** ディスクへ書き込まれる前に、どれだけの期間キャッシュに保存するかを決定します。値が10分に設定され、記録をフラッシュする状況が発生しなければ、10分を経過した記録はディスクへフラッシュされます。
 - **キャッシュの有効期限：** 繰り返し回数が最近更新されていないレコードをどのくらいの期間保持しておくかを決定します。キャッシュの寿命が10分で有効期限が2分の場合、更新されずに2分経過したイベントのレコードはディスクへ書き込まれ、キャッシュから消去されます。
-

注意： 上記の設定にかかわらず、イベントが脆弱性対策オプションサーバプラグインへ送信されるたびに、キャッシュは消去されます。

- ・ 「ポリシーの許可外」のパケットのファイアウォールイベントを生成: 許可ルールまたはファイアウォールルールによって特に許可されていなかったために破棄されたパケットをログに記録するかどうかを選択します。(このオプションをオンにすると、ログファイルのサイズが大幅に増える点に注意してください。)
 - ・ 各ルールの最初の検出に関するデータの取り込みを DPI ルールに許可する (期間内): ログエントリをトリガしたパケットのデータを保持します。(ログエントリとともにパケットのデータを表示できます。各ルールは、ログファイルのサイズが過度に大きくなるのを避けるため、ルールごとに 5 秒間に 1 回だけデータを取り込みます。)
4. 「詳細」エリアで、「カスタムドライバ設定を使用する」を設定します。
- ・ **CLOSED タイムアウト**: ゲートウェイで使用します。ゲートウェイが「ハードクローズ」(RST) を伝え、RST を受信したゲートウェイ側は、接続を終了するまで、設定された時間の間、接続をアライブにします。
 - ・ **SYN_SENT タイムアウト**: 接続を終了するまで SYN-SENT 状態になっている時間。
 - ・ **SYN_RCVD タイムアウト**: 接続を終了するまで SYN_RCVD 状態になっている時間。
 - ・ **FIN_WAIT1 タイムアウト**: 接続を終了するまで FIN-WAIT1 状態になっている時間。
 - ・ **ESTABLISHED タイムアウト**: 接続を終了するまで ESTABLISHED 状態になっている時間。
 - ・ **ERROR タイムアウト**: エラー状態で接続を保持する時間。(UDP 接続の場合、エラーはさまざまな UDP の問題が原因で発生する可能性があります。TCP 接続の場合、エラーはファイアウォールによって破棄されているパケットが原因で発生する可能性があります。)
 - ・ **DISCONNECT タイムアウト**: 切断するまで接続がアイドル状態になっている時間。
 - ・ **CLOSE_WAIT タイムアウト**: 接続を終了するまで CLOSE-WAIT 状態になっている時間。
 - ・ **CLOSING タイムアウト**: 接続を終了するまで CLOSING 状態になっている時間。
 - ・ **LAST_ACK タイムアウト**: 接続を終了するまで LAST-ACK 状態になっている時間。
 - ・ **ACK ストームタイムアウト**: ACK ストーム内で再送される ACK 間の最長期間。つまり、ACK が再送される頻度が低く、このタイムアウトが発生した場合、ACK は ACK ストームの一部とはみなされません。
 - ・ **再起動のタイムアウト**: ゲートウェイで使用します。ゲートウェイが再起動される時、ゲートウェイを通過している既存の接続が確立している場合があります。このタイムアウトでは、ゲートウェイが再起動される前に、確立された接続の一部である非 SYN パケットを許可する時間が定義されます。
 - ・ **起動のタイムアウト**: ステートフルメカニズムが開始される前に、確立された接続に属している非 SYN パケットを許可する時間。
 - ・ **UDP タイムアウト**: UDP 接続の最大時間。

- **ICMP タイムアウト** : ICMP 接続の最大時間。
- **Null IP を許可** : 送信元または送信先 IP アドレスがないパケットを許可またはブロックします。
- **IPv6 のブロック** : IPv6 パケットをブロックまたは許可します。(IPv6 トラフィックの DPI フィルタはサポートされていません。ブロックまたは許可のみ実行可能です。)
- **接続クリーンアップタイムアウト** : 切断された接続のクリーンアップ時間 (次を参照)。
- **最大接続数 (クリーンアップ単位)** : 定期的な接続クリーンアップごとに実施するクリーンアップで切断された接続の最大数 (前を参照)。
- **送信元と送信先が同じ IP アドレスをブロック** : 送信元および送信先 IP アドレスがないパケットをブロックまたは許可します。(ループバックインタフェースには適用されません。)
- **最大 TCP 接続数** : 最大 TCP 同時接続数。
- **最大 UDP 接続数** : 最大 UDP 同時接続数。
- **最大 ICMP 接続数** : 最大 ICMP 同時接続数。
- **毎秒最大イベント数** : 毎秒書込み可能なイベントの最大数。
- **TCP MSS の上限** : MSS は最大セグメントサイズ (またはデータの最大量) のことで、フラグメント化せずに TCP パケットへ送信できるサイズを指します。通常、2 台のコンピュータ間で通信が確立されたときに指定されます。ただし、状況によっては、トラフィックが小さい MSS の設定されたルータまたはスイッチを通過することがあります。この場合、MSS を変更できます。その際はパケットが再送され、クライアントプラグインはパケットを「再送の破棄」として記録します。再送の破棄イベントエントリが多数ある場合、上限を低くして容量が削減されるか確認してください。
- **イベントノードの数** : いつでもログ / イベントを折りたたむよう、ドライバがそれらを格納するのに使用するカーネルメモリの最大容量。

注意: イベントの折りたたみは、同じ種類のイベントが連続して多く発生したときに実行されます。このとき、クライアントプラグインはすべてのイベントを 1 つに「折りたたみ」ます。

- **ステータスコードの無視** : このオプションは、特定の種類のイベントを無視します。たとえば、たくさんの「無効なフラグ」が表示される場合は、そのイベントの全インスタンスを無視してかまいません。
- **ステータスコードの無視** : 上記と同様です。
- **ステータスコードの無視** : 上記と同様です。

- **詳細なログ記録ポリシー:**
 - **放置:** イベントをフィルタせずに。上記の「ステータスコードの無視」設定およびその他の詳細設定より優先されます。ただし、脆弱性対策オプションサーバプラグインで定義されたログ設定よりは優先されません。たとえば、脆弱性対策オプションサーバプラグインの「ステートフル設定のプロパティ」画面で設定されたステートフル設定ログオプションよりは優先されません。
 - **初期設定:** エンジンがタップモードの場合は下の「タップモード」に切り替わり、インラインモードの場合は上の「通常モード」に切り替わります。通常モード: 再送の破棄イベント以外はすべてログに記録されます。
 - **下位互換性モード:** サポートでのみ使用します。
 - **詳細モード:** 「通常モード」と同じですが、再送の破棄イベントも記録します。
 - **ステートフルと正規化の抑制:** 再送の破棄、切断、無効なフラグ、無効なシーケンス、無効な ACK、未承認 UDP、未承認 ICMP、ポリシーの許可以外を無視します。
 - **ステートフル、正規化、およびフラグメントの抑制:** 「ステートフルと正規化の抑制」が無視するものすべてに加えて、分断化に関するイベントも無視します。
 - **ステートフル、フラグメント、および検証機能の抑制:** 「ステートフル、正規化、およびフラグメントの抑制」が無視するものすべてに加えて、確認に関するイベントも無視します。
 - **タップモード:** 再送の破棄、切断、無効なフラグ、無効なシーケンス、無効な ACK、ACK 再送の上限、切断された接続上のパケットを無視します。

注意: 「ステートフルと正規化の抑制」、「ステートフル、正規化、およびフラグメントの抑制」、「ステートフル、フラグメント、および検証機能の抑制」、「タップモード」の各モードで無視されるイベントの包括的なリストについては、「213 ページの「詳細ログポリシーモード」」を参照してください。

- **TCP 途絶による接続中断:** TCP 途絶による接続中断がオンの場合、RST パケットはローカルスタックへのみ送信されます。ワイヤに RST パケットは送信されません。これにより、潜在的な攻撃者に返す情報量は削減されます。

注意： 「TCP 途絶による接続中断」を有効化する場合、DISCONNECT タイムアウトも調整する必要があります。DISCONNECT タイムアウトの値の範囲は、0 秒から 10 分までの間で設定します。この値は、クライアントプラグインが接続を切断する前にアプリケーション側で切断できるよう、十分に高く設定する必要があります。DISCONNECT タイムアウト値に影響を与える要因としては、オペレーティングシステム、接続を確立するアプリケーション、およびネットワークポロジータが挙げられます。

- **デバッグモードを有効にする：** デバッグモードの場合、クライアントプラグインは特定のパケット数を取り込みます (下記の「デバッグモードで保持するパケットの数」内の設定を参照)。ルールがトリガされてデバッグモードがオンになると、クライアントプラグインはルールがトリガされる前に通過した最後のパケット数 X を記録として保持します。パケットは、デバッグイベントとしてサーバプラグインに返されます。
-

注意： デバッグモードは簡単にログの過剰生成を引き起こすので、クライアントサービスの管理下でのみ使用してください。

- **デバッグモードで保持するパケットの数：** デバッグモードがオンのとき、維持してログするパケット数。
- **すべてのパケットデータをログに記録する：** 内部で定義されている未集計のすべてのログ (FW/DPI/ 確認のログ以外) が、すべてのパケットデータをログに追加します。この設定と次に示す 2 つの設定は、対応する DPI ログと FW ログの設定に相当します。
- **期間内で 1 つのパケットデータのみをログに記録する：** 上記のオプションが設定されていない場合に、このオプションが設定されていると、大部分のログにはヘッダデータのみが含まれます。すべてのパケットは定期的には追加されません。
- **1 つのパケットデータのみをログに記録する期間：** 上記のオプションが設定されている場合の、すべてのパケットデータがログに記録されるまでの間隔。
- **パケットデータがキャプチャされたときに格納する最大データサイズ：** ログに追加されるヘッダデータまたはパケットデータの最大サイズ。
- **TCP の接続イベントを生成する：** TCP 接続が確立されるたびにファイアウォールイベントが生成されます。
- **ICMP の接続イベントを生成する：** ICMP 接続が確立されるたびにファイアウォールイベントが生成されます。
- **UDP の接続イベントを生成する：** UDP 接続が確立されるたびにファイアウォールイベントが生成されます。

- **CISCO WAAS 接続のバイパス**: このモードでは、専用の CISCO WAAS TCP オプションを選択して開始された接続に対して、TCP シーケンス番号のステートフル分析を省略します。このプロトコルには無効な TCP シーケンスおよび ACK 番号に関する詳細情報が含まれていて、ステートフルなファイアウォールによるチェックと干渉します。CISCO WAAS を使用してファイアウォールログに無効な SEQ や無効な ACK を持つ通信が表示されている場合にのみ、このオプションを有効にします。このオプションを選択すると、WAAS が有効化されていない接続に対しても TCP ステートフルシーケンス番号の確認が実行されます。
- **回避再送の破棄**: すでに処理されたデータを含む受信パケットを破棄することで、想定される回避的再送型の攻撃を避けます。
- **TCP チェックサムの確認**: セグメントのチェックサムフィールドのデータを使用して、セグメントの整合性が確認されます。
- **最小フラグメントオフセット**: 許容可能な最小の IP フラグメントオフセットを定義します。オフセットがこの値未満のパケットは、「IP フラグメントオフセットが小さすぎます」という理由で破棄されます。0 に設定した場合は制限が適用されません (初期設定は 60)。
- **最小フラグメントサイズ**: 許容可能な最小の IP フラグメントサイズを定義します。この値より小さいフラグメント化されたパケットは、「最初のフラグメントが小さすぎます」という理由で、不正な可能性があるパケットとして破棄されます (初期設定は 120)。
- **フラグメントタイムアウト**: フラグメント化されたパケットを保持する時間。
- **保持するフラグメント化された IP パケットの最大数**: これを実行するように設定すると、パケットまたはパケットフラグメントのコンテンツが疑わしいとみなされる場合に、DPI ルールはそのコンテンツを編集します。この設定では、編集後、パケットを破棄するまで残りのパケットフラグメントを待機する時間が定義されます。
- **フラグメント化されたパケットのタイムアウトを超過したことを示すために ICMP を送信する**: 接続タイムアウトを超過したことを、ICMP パケットでリモートコンピュータに示すかどうかを設定します。

インタフェースの分離設定

インタフェースの分離では、コンピュータで一度に使用できるインタフェースを 1 つに強制することができます。この機能は、攻撃者が 2 つのインタフェース間をブリッジすることを回避するために設計されました。

インタフェースの分離設定の設定方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「インタフェースの分離」タブをクリックします。
2. 「インタフェースの分離」エリアで、インタフェースの分離を有効にするかどうかを選択します。
3. インタフェースの分離を強制するには、「インタフェースパターン」エリアで、優先度に応じてコンピュータのインタフェース名と一致する文字列パターンを入力します。インタフェースのリストを作成するときは、標準の正規表現の構文を使用できます。

注意: コンピュータの複数のインタフェースと一致する文字列パターンを入力すると、それらのすべてのインタフェースでのトラフィックが許可されます。有効なインタフェースを1つだけにするには、「1つのアクティブインタフェースに制限」オプションを設定します。

注意: このオプションは、グローバルレベルというよりも、特定のセキュリティプロファイルまたはコンピュータにのみといったように、細かいレベルで設定します。そのためには、グローバル設定でインタフェースの分離を強制しないよう設定してから、セキュリティプロファイルまたはコンピュータの設定を優先させます。設定の優先の詳細については、「69 ページの「継承および優先」」を参照してください。

コンテキスト設定

コンテキストでは、保護対象のコンピュータにインターネット接続があるかどうかを判別されます。一部の脆弱性対策オプションルールは、コンピュータのネットワーク接続状況に応じて、条件付きで適用できます。これは「ロケーション識別」と呼ばれています。特定のルールに対するインターネット接続条件オプションは、そのルールの「プロパティ」画面の「オプション」タブで設定できます。インタフェースの分離を実装するときに、インターネット接続テストを使用することもできます。(「182 ページの「コンテキスト設定」」参照。)

コンテキスト設定の設定方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「コンテキスト」タブをクリックします。
2. 「インターネット接続テスト」エリアで、次のオプションを設定します。
 - ・ **インターネット接続ステータスのテスト用 URL:** インターネット接続をテストするための HTTP リクエストの送信先 URL (「http://」を含める必要があります)。

- ・ インターネット接続ステータスの確認に使用する返されたコンテンツの正規表現: HTTP 通信が成功したかどうかを確認するために、返されたコンテンツに適用される正規表現。
- ・ テスト間隔: 接続テストの間隔。

攻撃の予兆設定

「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。

攻撃の種類ごとに、アラートが発令されるサーバプラグインに情報を送信するようクライアントプラグインを設定できます。また、アラート発令時にメール通知を送信するようにサーバプラグインを設定できます。(「システム」→「システム設定」→「通知設定」に進みます。アラートは、「ネットワークまたはポート検索」、「コンピュータの 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「脆弱性対策オプションサーバにただちに通知」を選択してください。通知の詳細については、「185 ページの「通知設定」」を参照してください。

注意: 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と TCP および UDP のログは、「ファイアウォール」→「ステートフル設定」画面で有効にすることができます。

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クライアントプラグイン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」ドロップダウンリストを使用して分数を設定します。

「コンピュータの OS のフィンガープリント調査」および「ネットワークまたはポート検索」は、単一のパケットによって認識されないという点で、他の 3 つの攻撃の予兆とは異なります。

クライアントプラグインは、リモート IP がポートに対して異常な割合の IP でアクセスしていることを検出した場合、コンピュータまたはポート検索をレポートします。通常、クライアントプラグインのコンピュータは、コンピュータ自身宛てのトラフィックのみを監視するため、検出されるものとしてはポート検索がもっとも代表的です。ただし、コンピュータがルータまたはブリッジとして動作している場合は、多数の他のコンピュータ宛てのトラフィックを監視して、クライアントプラグインがコンピュータ検索 (サブネット全体でポート 80 が開いているコンピュータを検索するなど) を検出できます。

こうした検索を検出するには数秒かかります。これは、クライアントプラグインが接続の失敗を追跡して、比較的短い期間に単一のコンピュータからの異常な数の接続の失敗があることを確認する必要があるためです。

コンピュータ / ポート検索の検出で使用される統計的な分析方法は、「TAPS」アルゴリズムから導出されたもので、Sprint/Nextel によって発行された「Connectionless Port Scan Detection on the Backbone」で提案され、2006 年 4 月にアリゾナ州フェニックスで IPCCC と共同で開催された不正プログラムワークショップで発表されました。

注意： Windows コンピュータでブラウザアプリケーションを使用して脆弱性対策オプションクライアントプラグインを実行している場合、切断された接続からの残存トラフィックが原因で、攻撃予兆の誤検索（偽陽性）が報告されることがあります。

「脆弱性対策オプションサーバにただちに通知」オプションを動作させるには、クライアントプラグインの通信方法を「クライアントプラグインによる開始」または「双方向」に設定する必要があります（「システム」→「システム設定」→「コンピュータ」を参照してください）。設定が有効になると、クライアントプラグインは、攻撃や調査を検出後ただちに脆弱性対策オプションサーバプラグインに対してハートビートを開始します。

攻撃の予兆設定の設定方法は、次のとおりです。

パス：脆弱性対策オプションメインメニュー | 「システム」→「システム設定」

1. 「攻撃の予兆」タブをクリックします。
2. 「攻撃の予兆検索」エリアで、次のオプションを設定します。
 - **攻撃の予兆の検出の有効化：** 検出を実行します。
 - **検出を実行するコンピュータ / ネットワーク：** 保護する IP をドロップダウンリストから選択します。既存の IP リストから選択します。（このためには、「コンポーネント」→「IP リスト」画面を使用して IP リストを作成できます）。
 - **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（前述したように、このためには「コンポーネント」→「IP リスト」画面を使用して IP リストを作成できます）。
 - **コンピュータの OS のフィンガープリント調査：** クライアントプラグインは、有効な TCP スタック OS フィンガープリント試行を認識して処理します。
 - **ネットワークまたはポート検索：** クライアントプラグインは、ポートの検索を認識して処理します。
 - **TCP Null 検索：** クライアントプラグインはフラグが設定されていないパケットを拒否します。

- **TCP SYNFIN 検索**: クライアントプラグインは SYN フラグおよび FIN フラグの付いたパケットのみ拒否します。
- **TCP Xmas 検索**: クライアントプラグインは、FIN フラグ、URG フラグ、および PSH フラグの付いたパケット、または値 0xFF (ありうるすべてのフラグ) を含むパケットを拒否します。

検索設定

検索設定の設定方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「検索」タブをクリックします。
2. 「開いているポートの検索」エリアで、検出されたコンピュータ上で脆弱性対策オプションサーバプラグインによるポート検索を実行するときに使用するポートリストを選択します。(ドロップダウンリストのポートリストは、「コンピュータ」セクションの「ポートリスト」画面で定義するものと同じです。)
3. 「推奨設定の検索」エリアで、継続的な検索を実行して間隔を設定するかどうかを選択します。クライアントプラグインでは、コンピュータ上の一般的なアプリケーションを定期的に検索し、検出結果に基づいてルール of 推奨設定を作成できます。この設定によって、検索を許可するように設定されているコンピュータ上での検索の実行間隔が設定されます。

通知設定

通知の設定方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「通知設定」タブをクリックします。
2. 「アラート通知 (サーバプラグインから)」エリアに、すべてのアラートメールが送信されるメールアドレスを入力します (「システム」 → 「システム設定」 → 「システム」画面から、メール送信をトリガするアラートを設定できます)。
3. 「通知の頻度 (クライアントプラグインから)」エリアで、クライアントプラグインからアラートの受信者にイベントを送信する頻度を選択します。
4. 「ファイアウォールと DPI イベント通知 (クライアントプラグインから)」エリアで、「リモートコンピュータにイベントを転送する (Syslog 経由)」を選択します。専用の Syslog サーバにログを格納するには、これらのフィールドに必要な情報を入力します。Syslog の設定の詳細については、「197 ページの「Syslog の統合の設定」」を参照してください。

5. 「システムイベント通知 (サーバプラグインから)」エリアで、必要に応じてオプションを設定します。
 - **リモートコンピュータにシステムイベントを転送する (Syslog 経由)**: 通知は、Syslog サーバに送信できます。ここに Syslog サーバの詳細を入力します。Syslog の設定の詳細については、「197 ページの「Syslog の統合の設定」」を参照してください。
 - **リモートコンピュータにシステムイベントを転送する (SNMP 経由)**: 脆弱性対策オプションでは、SNMP もサポートされています。MIB ファイル (DeepSecurity.mib) は、以下にあります。¥Trend Micro¥OfficeScan¥Addon¥Intrusion Defense Firewall¥util。

ランク付け設定

ランク付けシステムでは、DPI およびファイアウォールイベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、DPI ルールとファイアウォールルールに「重要度」を割り当て、これら 2 つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、DPI イベントまたはファイアウォールイベントを表示するときに、イベントをランクでソートできます。

ランク付けの設定方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「ランク付け」タブをクリックします。
2. 「ファイアウォールルールの重要度」エリアで、次のいずれかを設定します。
 - **ファイアウォールルールの重要度**: ファイアウォールルールの重要度の値は、拒否、ログのみ、およびパケット拒否の処理に関連付けられています。(パケット拒否とは、ステートフル設定によってパケットを拒否することです。) このパネルで重要度の値を編集します。この値にコンピュータの資産評価を掛けたものがファイアウォールイベントのランクを決定します。(ファイアウォールルールの処理は、ルールの「プロパティ」画面から表示および編集できます。)
 - **DPI ルールの重要度**: DPI ルールの重要度の値は、重大、高、中、または低の重要度評価に関連付けられています。このパネルで重要度の値を編集します。この値にコンピュータの資産評価を掛けたものが DPI イベントのランクを決定します。DPI ルールの重要度の設定は、ルールの「プロパティ」画面で表示できます。

- **資産評価**: 資産評価は、DPI ルールやファイアウォールルールとは異なり、自身の他のプロパティには関連付けられていません。資産評価は、それ自体がプロパティです。コンピュータの資産評価は、コンピュータの「詳細」画面から表示および編集できます。資産評価の割り当て処理を簡略化するために、コンピュータの最初の「詳細」画面の「資産重要度」ドロップダウンリストに表示される値の一部を事前定義できます。既存の事前定義されたコンピュータの資産評価を表示するには、このパネルの「資産評価の表示 ...」ボタンをクリックします。「資産評価」画面に、事前定義された設定が表示されます。これらの値は変更可能で、新しい値を作成できます。(新しい設定は、すべてのコンピュータのドロップダウンリストに表示されます。)

アップデート

最大限の保護を実現するには、パターンファイルおよびソフトウェアコンポーネントを最新に保つ必要があります。「システム」→「システム設定」画面の「アップデート」タブで、脆弱性対策オプションサーバプラグインでアップデートの有無を確認する際の DPI ルールの適用方法を設定できます。現在のアップデートのステータスを確認するには、「システム」→「アップデート」画面に進みます。

アップデートの設定方法は、次のとおりです。

パス : 脆弱性対策オプションメインメニュー | 「システム」→「システム設定」

1. 「アップデート」タブをクリックします。
2. 「脆弱性対策オプションルールアップデート」エリアで、次のいずれかを設定します。
 - **新しい DPI ルールの自動割り当てを脆弱性対策オプションルールアップデートに許可する** : セキュリティアップデートの新しい DPI ルールは、アプリケーションの種類 (HTTP Server、DNS Client、MS SQL Server など) に関連付けられています。このオプションをオンにすると、新しい DPI ルールに関連付けられているアプリケーションの種類がアクティブになっているコンピュータに、新しい DPI ルールが自動的に割り当てられます。ルールをコンピュータに自動的に割り当てするには、次の 2 つの条件を満たす必要があります。
 - この画面のこのオプションがオンになっていること。
 - トレンドマイクロの作成したルールが自動割り当てを許可するように設計されていること。(一部のルールは、アプリケーションの種類に関連付けられていても、自動割り当てを目的としていません。このようなルールは脆弱性対策オプションサーバプラグインで認識され、このオプションがオンになっていても適用されません)。
 - **新しい DPI ルールでのアラートの設定を脆弱性対策オプションルールアップデートに許可する** : 新しい DPI ルールのうち、トレンドマイクロが重要であるとみなすルールについては、初期設定でアラートをトリガするように設定されています。このオプションをオフにすると、その初期設定の動作よりも優先されます。

システム

システムの設定方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「システム」タブをクリックします。
2. 「アラート設定」エリアで、発生する可能性のある脆弱性対策オプションサーバプラグインのすべてのアラートを設定します。ほとんどの場合、これはアラートのオン/オフの切り替え、重要度の設定、およびメール通知の設定を意味します。
3. 「SMTP」エリアに、SMTP メールアドレスを入力します。必要に応じてポート番号も入力します。メールの送信元とする「送信元」メールアドレスを入力します。オプションで、アラートメールを1人以上のユーザに配信できなかった場合の、配信不能通知の送信先の「バウンス」メールアドレスを入力します。SMTP メールサーバで送信の認証が必要な場合は、ユーザ名とパスワードの資格情報を入力します。必要な情報を入力したら、「SMTP 設定のテスト」を使用して設定をテストします。
4. 「削除」エリアで、イベントレコードおよびカウンタ、古いセキュリティアップデート、古いバージョンのクライアントプラグインソフトウェアをデータベースから削除するまでの保存期間を定義します。

イベント設定については、使用しているデータベースシステムの堅牢性、使用可能な記憶域の容量、およびログに記録するイベントに基づいて、決定を行う必要があります。次にログについてのヒントを示します。

- 重要でないコンピュータのログ収集を無効にします。これを実行するには、コンピュータの「詳細」画面の「詳細設定」またはセキュリティプロファイルの「詳細」画面を使用します。
- 「ステートフル設定」のログオプションの無効化によってファイアウォールルール処理のログを削減することを検討します。(たとえば、UDP ログを無効にすると、未承諾 UDP のログエントリが排除されます)
- DPI ルールの場合、破棄されたパケットのみをログに記録することをお勧めします。パケットの変更をログに記録していると、ログエントリが多くなる場合があります。
- DPI ルールの場合、攻撃元の調査が必要などときのみパケットデータを含めます (DPI ルールの「プロパティ」画面のオプション)。それ以外のときにパケットデータをオンのままにしておくと、ログサイズが非常に大きくなります。

注意: ログは、イベントページからの収集に使用します。カウンタは、ログから集計されたデータで、レポートの生成とダッシュボードのウィジェットへの入力に使用されます。

5. 「エクスポート」エリアで、脆弱性対策オプションサーバプラグインからデータファイルをエクスポートするときに利用するエンコードを選択できます。
6. 「Whois」エリアで、DPI イベントおよびファイアウォールイベントをログに記録するときに使用される Whois 検索を指定できます。

タグ

イベントのタグ付けを使用すると、「attack」、「suspicious」、「patch」、「acceptable change」、「false positive」、「high priority」などの定義済みのラベルを、管理者が手動でイベントに付けることができます。また、「確認用として Tom に割り当て」などのカスタムラベルを定義することもできます。

イベントに手動でタグを付けるだけでなく、「参照コンピュータ」を使用してタグ付けを自動化することもできます。たとえば、あるパッチの計画済みのロールアウトを参照コンピュータに適用し、パッチの適用に関連付けられたイベントに「Patch X」というタグを付けて、その他のシステムで発生する同様のイベントを自動的に「許容可能な変更」であるとみなすことで、管理者が検討対象にするイベント数を減らせます。

イベントのタグ付けを使用すると、イベントの特殊なビュー、ダッシュボード、およびレポートが有効になります。また、イベントのタグ付けは単一イベント、類似する複数のイベント、または将来的に発生する同様のすべてのイベントに適用できます。

タグの追加など、タグ付けの詳細については、「168 ページの「イベントのタグ付け」」を参照してください。

タグの表示

現在定義されているすべてのタグは、「システム」→「タグ」画面に表示されます。これには定義済みのタグとカスタムタグが含まれます。(表示されるのは、使用中のタグのみです。)

- **タグを削除**: タグを削除すると、そのタグを追加したすべてのイベントからタグが削除されます。
- **自動タグルールを表示**: 自動タグルールを作成するには、イベントを選択し、類似のアイテムにタグを付けるように選択します。

タスク

タスクを使用すると、特定の代表的なタスクを予約できます。予約タスクの処理は、定義したスケジュールに従って開始されます。

タスクを作成する方法は、次のとおりです。

パス: [脆弱性対策オプションメインメニュー](#) | 「システム」 → 「タスク」

1. 「新規」(📄) をクリックし、「新規予約タスク」を選択します。ウィザードが表示され、順を追って新しいタスクを作成できます。タスクの種類によって、入力を求められる情報が異なります。
2. ウィザードを使用すると、次のタスクを予約できます。
 - **スクリプトの実行**: Syslog オプションと SNMP オプションがイベント通知の要件に満たないとき、トレンドマイクロではカスタム記述スクリプトを使用して解決できる場合があります。
 - **コンピュータのアップデート**: 選択したコンピュータに対しては、定期的にアップデート処理を実行します。アップデート処理により、サーバプラグイン内のすべての設定変更が適用されます。
 - **コンポーネントのアップデート**: コンポーネントを定期的にアップデートします。アップデート処理により、脆弱性対策オプションルールのアップデートについて、すべてのコンポーネントのアップデートが適用されます。
 - **推奨設定についてコンピュータを検索**: 脆弱性対策オプションサーバプラグインによって、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。
 - **新規ソフトウェアの確認**: サーバプラグイン、クライアントプラグイン、または Filter Driver の新しいバージョンが入手可能かどうかを確認します。
 - **バックアップ**: 定期的にデータベースのバックアップを実行します。(このオプションは、Derby または Microsoft SQL Server のデータベースを使用している場合にのみ使用できます)。



タスクを表示または編集する方法は、次のとおりです。

パス: [脆弱性対策オプションメインメニュー](#) | 「システム」 → 「タスク」

1. タスクを選択してクリックする (👆) か、右クリックしてポップアップメニューから「プロパティ...」を選択します。
2. プロパティウィンドウで、必要に応じて「スケジュール情報」の情報を編集し、「OK」または「適用」をクリックします。


タスクを複製する方法は、次のとおりです。

パス：脆弱性対策オプションメインメニュー | 「システム」 → 「タスク」

1. タスクを選択して「複製」() をクリックするか、右クリックしてポップアップメニューから「複製 ...」を選択します。
2. タスクの名前を変更するには、クリックする () か、右クリックしてポップアップメニューから「プロパティ ...」を選択し、「プロパティ」ウィンドウで新しい名前を編集します。


タスクを削除する方法は、次のとおりです。

パス：脆弱性対策オプションメインメニュー | 「システム」 → 「タスク」

- ・ タスクを選択して「削除」() をクリックするか、右クリックしてポップアップメニューから「削除」を選択します。

予約タスクを実行する方法は、次のとおりです。

パス：脆弱性対策オプションメインメニュー | 「システム」 → 「タスク」

- ・ タスクを選択して「今すぐタスクを実行」() をクリックするか、右クリックしてポップアップメニューから「今すぐタスクを実行」を選択します。

ライセンス

「ライセンス」画面には、脆弱性対策オプションの製品ライセンスの詳細情報が表示されます。ライセンスのステータスは、「詳細情報をオンラインで確認」をクリックすると確認できます。トレンドマイクロから新しいアクティベーションコードを受け取ったら、「新しいアクティベーションコード」をクリックしてライセンスの情報を入力します。ライセンスで許可された新しい機能がすぐに使用できるようになります。詳細なアップグレード手順を確認するには、「製品購入案内の表示」をクリックします。期限切れが近い、または期限切れになったモジュールがある場合は、アラートが生成されます。

アップデート

「アップデート」画面には、現在のアップデートのステータスが表示されます。アップデートを設定するには、「システム」 → 「システム設定」 → 「アップデート」に進みます。

セキュリティアップデート

セキュリティアップデートには、新しいルールと既存の DPI ルールの変更が含まれます。

- **前回のセキュリティアップデート** : 前回セキュリティアップデートの有無を確認した日時。アップデートの有無を確認するには、「ダウンロード」をクリックします。
- **現在適用されているバージョン** : 現在適用されているセキュリティアップデートのバージョン。

「すべてのルールアップデートの表示」ボタンをクリックすると、最新の DPI ルールのリストが表示されます。必要に応じて、脆弱性対策オプションの保護対象のコンピュータに現在のルールセットを再適用することも、前のルールセットにロールバックすることもできます。「システム」→「システム設定」→「システム」タブの「削除」エリアで、脆弱性対策オプションサーバプラグインのデータベースに保持するルールのアップデートの数を設定できます。

セキュリティアップデートの適用

前のセキュリティアップデートを選択して、メニューバーの「再適用」をクリックすると、前のセキュリティアップデートに戻すことができます。(トレンドマイクロのサーバの URL は、ウイルスバスター Corp. のコンソールの「アップデート」→「サーバ」→「アップデート元」から変更できます。詳細については、ウイルスバスター Corp. のドキュメントを参照してください)。

最新のセキュリティアップデートを手動で確認、ダウンロード、および適用するには

パス : 脆弱性対策オプションメインメニュー | 「システム」 → 「アップデート」

1. 「ダウンロード」ボタンをクリックして、最新のアップデートを確認して取得します。
2. アップデートをダウンロードしたら、「セキュリティアップデートの表示 ...」ボタンをクリックすると、新しい画面が開き、ダウンロードしたすべてのアップデートが表示されます。表示されたアップデートで、クライアントプラグインに適用されているものは「適用済み」列に緑のチェックマークが付きます。
3. リストから最新のセキュリティアップデートを選択して、メニューバーの「適用 ...」(または「再適用 ...」) をクリックします。新しい画面が開き、適用されるアップデートに関する情報が表示されます。
4. 「完了」をクリックして、アップデートを配信します。

注意 : 以前のセキュリティアップデートを選択して、メニューバーの「再適用 ...」をクリックすると、以前のセキュリティアップデートに戻すことができます。

最新版アップデートの確認とダウンロードを自動的に行うには

1. 「システム」→「タスク」画面に進みます。
2. ツールバーの「新規」をクリックして「新規予約タスク」を選択し、新規予約タスクウィザードを表示します。
3. 「タイプ」ドロップダウンリストから、「コンポーネントのアップデート」を選択します。
4. ウィザードの手順に従って、このタスクの実行間隔と実行時間を選択します。アップデートが自動的にダウンロードされます。
5. 最新のセキュリティアップデートを自動的に適用するには、「脆弱性対策オプションルールアップデートの自動適用」を選択します。
6. 「完了」をクリックします。

クライアントプラグインのアップデート

クライアントプラグインのアップデートにより、最新バージョンのクライアントプラグインとドライバが適用されます。

- **前回のクライアントプラグインのアップデート**：前回クライアントプラグインのアップデートの有無を確認した日時。アップデートの有無を確認するには、「ダウンロード」をクリックします。
- **32ビットドライバの最新バージョン**：トレンドマイクロから入手可能な32ビットドライバの最新バージョン。
- **64ビットドライバの最新バージョン**：トレンドマイクロから入手可能な64ビットドライバの最新バージョン。
- **最新のクライアントプラグインの配信**：最新のバージョンのクライアントプラグインを実行しているコンピュータの数。

注意： 脆弱性対策オプションクライアントプラグインのアップデートは、すべて脆弱性対策オプションサーバプラグインを使用して配信できます。ただし、新しいバージョンの脆弱性対策オプションサーバプラグインは、ウイルスバスター Corp. Web コンソールプラグインマネージャでアップデートする必要があります。サーバプラグインのアップグレードの詳細については、「153 ページの「サーバプラグインのアップグレード」」を参照してください。

最新バージョンのクライアントプラグインとドライバを配信するには、「最新版の配信」をクリックします。

サーバ診断

サポート用の診断パッケージを作成することができます。診断パッケージウィザードの手順に従いながらパッケージに含める情報を選択することができます。このウィザードを開始するには、「**診断パッケージの生成**」をクリックします。



第13章

ログ

この章では、脆弱性対策オプション™ 1.5 ログの設定方法について説明します。

この章で扱うトピックは次のとおりです。

- 196 ページの「ログについて」
- 196 ページの「ログの設定」
- 196 ページの「通知の設定」
- 197 ページの「Syslog の統合の設定」

ログについて

脆弱性対策オプションは、Syslog サーバに情報を送信するように設定できます。クライアントプラグインからは DPI イベント情報およびファイアウォールイベント情報、サーバプラグインからはシステム情報が送信されます。脆弱性対策オプションは、通知を送信、Syslog サーバに情報を送信、およびログポリシーモードで動作するように設定できます。

ログの設定

初期設定の場合、サーバプラグインではハートビートを使用してクライアントプラグインからログが収集されます。この機能でサポートできるコンピュータの数は、ハートビート間隔 (初期設定では 60 分ごと)、コンピュータがどれくらい活動的か、およびログ設定によって異なります。

ログ収集の効率性を最大限にするためのヒントを示します。

- 重要でないコンピュータのログ収集を無効にします。これを行うには、「システム」→「システム設定」から、コンピュータの「詳細」画面またはセキュリティプロファイルの「詳細」画面で「ファイアウォールおよび DPI」タブを開きます。
- ステートフル設定の「プロパティ」画面でログオプションの一部を無効にして、ファイアウォールルール処理のログを削減することを検討します。たとえば、UDP ログを無効にすると、「未承諾 UDP」のログエントリが排除されます。
- DPI ルールの場合、破棄されたパケットのみをログに記録することをお勧めします。パケットの変更をログに記録していると、ログエントリが多くなる場合があります。
- DPI ルールの場合、攻撃元の調査が必要なときのみパケットデータを含めます (DPI ルールの「プロパティ」画面のオプション)。それ以外のときにパケットデータの追加をオンのままにしておくと、ログサイズが非常に大きくなってしまいます。

通知の設定

SMTP 経由でアラートメールを送信し、インストール時に選択したデータベース (内部 Derby、SQL Server、または Oracle など) へログを記録する以外にも、脆弱性対策オプションシステムではサーブドパーティの記録および通知メカニズムと統合するためのさまざまな方法が用意されています。

Syslog

クライアントプラグインとサーバプラグインの両方を、Syslog サーバに情報を送信するように設定できます。クライアントプラグインからは DPI イベント情報およびファイアウォールイベント情報、サーバプラグインからはシステム情報が送信されます。Syslog 設定を行うには、「システム」→「システム設定」→「通知設定」に進みます。

イベント通知を設定するためのパネルは 2 つあります。1 つはファイアウォールと DPI イベント通知用、もう 1 つはシステムイベント通知用です。

Syslog の設定の詳細については、「197 ページの「Syslog の統合の設定」」を参照してください。

SNMP

サーバプラグインには、システムイベント通知をサーバプラグインから SNMP サーバに送信するオプションもあります。同じ画面を使用して、SNMP 設定を入力します。MIB ファイル (DeepSecurity.mib) は、¥Trend Micro¥OfficeScan¥Addon¥Intrusion Defense Firewall¥util にあります。

スクリプト

Syslog オプションと SNMP オプションがイベント通知の要件に満たないとき、トレンドマイクロではカスタム記述スクリプトを使用して解決できる場合があります。

Syslog の統合の設定

脆弱性対策オプションは、Arcsight (www.arcsight.com) が提供している Common Event Format 1.0 をサポートします。他にも 2 つの Syslog 形式 (Basic Syslog および Common Event Format (legacy)) をサポートしています。ただし、これらの形式は従来のインストールで使用できますが、新しい統合プロジェクトには使用しないでください。

注意： 脆弱性対策オプションサーバプラグインで Syslog 転送を有効にしても、初期設定のログ処理には影響を与えません。つまり、Syslog を有効にしても、通常のログメカニズムが「オフ」になることはありません。

Red Hat Enterprise で Syslog を設定する

次の手順は、クライアントプラグインからログを受信できるようにする、Red Hat Enterprise 上の Syslog 設定方法を示しています。

1. root でログインします。
2. 次を実行します。vi /etc/syslog.conf
3. syslog.conf の末尾に、次の 2 行を追加します。
#Save IDF Server Plug-in logs to IDF Server.log
Local4.* /var/log/IDF Server.log
4. ファイルを保存して、終了します。
5. touch /var/log/IDF Server.log と入力した /var/log/IDF Server.log ファイルを作成します。
6. Syslog が書き込めるよう、脆弱性対策オプションサーバログに権限を設定します。
7. 次を実行します。vi /etc/sysconfig/syslog
8. 「SYSLOGD_OPTIONS」の行を編集して、オプションに「-r」を追加します。
9. ファイルを保存して、終了します。
10. Syslog を再起動します。/etc/init.d/syslog restart

Syslog が機能すると、次の場所にログが記録されます。/var/log/IDF Server.log

脆弱性対策オプションサーバプラグインの設定

すべての管理下のコンピュータから Syslog コンピュータにログが送信されるようにサーバプラグインを設定したり、あるいは個々のコンピュータを別々に設定することもできます。

すべての管理対象のコンピュータで **Syslog** を使用するようにサーバプラグインを設定する方法は、次のとおりです。

パス: 脆弱性対策オプションメインメニュー | 「システム」 → 「システム設定」

1. 「通知設定」タブをクリックします。
2. 「システムイベント通知」エリアで、「リモートコンピュータにシステムイベントを転送する (Syslog 経由)」オプションを設定します。
3. Syslog コンピュータのホスト名または IP アドレスを入力します。
4. 使用する UDP ポートを入力します (通常は 514)。

5. 使用する Syslog 機能を選択します (前述の Red Hat の例では Local4)。
6. ログ形式として「Common Event Format 1.0」を選択します。(「Basic Syslog」と「Common Event Format (legacy)」の形式は、レガシーサポートのためにのみ表示されます。新しい統合には使用しないでください。)

注意： Common Event Format 1.0 は、Arcsight (www.arcsight.com) が提供している形式です。この仕様は、Arcsight の Web サイトから入手できます。

すべての既存および新規のコンピュータが初期設定でリモート Syslog を使用するようにサーバプラグインを設定しました。

この初期設定は、特定のセキュリティプロファイルに対して、および個々のコンピュータで優先できます。コンピュータで優先するには、設定するコンピュータを「コンピュータ」画面で見つけ、それをダブルクリックして「詳細」画面を表示します。「システム」→「システム設定」へ進み、「通知設定」タブをクリックします。この設定は、コンピュータ上の他の多くの設定と同様に、初期設定を継承するように設定することも、優先することもできます。このコンピュータで継承可能な初期設定を無視するよう設定するには、「イベントの転送先」オプションを選択して別の Syslog サーバの詳細を入力するか、ログを一切転送しないようにします。同じ手順に従って、セキュリティプロファイルの設定を優先します。

Syslog メッセージを解析する

CEF の基本形式 : CEF: バージョン | デバイスベンダ | デバイス製品 | デバイスバージョン | 署名 ID | 名前 | 重要度 | 拡張

脆弱性対策オプションサーバプラグインと脆弱性対策オプションクライアントプラグインのどちらからのログエントリかを判断するには、「デバイス製品」フィールドを確認します。

ログエントリのサンプル : Jan 18 11:07:53 dsmhost CEF:0|Third Brigade|IDF Server Plug-in|5.0.1659|600|Administrator Signed In|4|suser=Master...

イベントをトリガしたルールの種類を判断するには、「署名 ID」フィールドと「名前」フィールドを確認します。

ログエントリのサンプル : Mar 19 15:19:15 chrisds7 CEF:0|Trend Micro|IDF Client Plug-in|7.0.0.2036|123|Out Of Allowed Policy|5|cn1=1...

次の「署名 ID」の値は、トリガされたイベントの種類を示します。

表 13-1. 署名 ID

署名 ID	説明
10	カスタム DPI ルール
20	ログのみのファイアウォールルール
21	拒否のファイアウォールルール
100-299	ポリシーの許可外のファイアウォールルール
300-399	SSL イベント
500-899	ステートフル設定イベント
1,000,000-1,999,999	トレンドマイクロが提供する DPI ルール

注意： 次の表に示すすべての CEF 拡張が必ずしも各ログエントリに含まれているわけではありません。同様に、これらの拡張が表示される順序も、表に示す順序とは異なる場合があります。正規表現を使用してエントリを解析する場合は、表に示す各キーと値のペアの位置や順番に依存しないようにしてください。

注意： Syslog メッセージは、Syslog プロトコル仕様によって最大 1,024 文字に制限されています。まれに、ルールおよびインタフェースに長い名前が使用されると、データが切り捨てられることがあります。

ファイアウォールイベントログの形式

CEFの基本形式: CEF: バージョン | デバイスベンダ | デバイス製品 | デバイスバージョン | 署名 ID | 名前 | 重要度 | 拡張

```

ログエントリのサンプル (1): 03-19-2010      16:19:18      Local0.Info
10.52.116.23      Mar 19 15:19:15 chrisds7 CEF:0|Trend Micro|IDF Client
Plug-in|7.0.0.2036|123|Out Of Allowed Policy|5|cnl=1 cnlLabel=Computer ID
act=Deny dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37
TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23 in=62 cs3=DF 0
cs3Label=Fragmentation Bits proto=TCP spt=24431 dpt=23 cs2=0x00 SYN
cs2Label=TCP Flags cnt=1
    
```

```

ログエントリのサンプル (2): 03-19-2010      16:18:33      Local0.Info
10.52.116.23      Mar 19 15:18:31 chrisds7 CEF:0|Trend Micro|IDF Client
Plug-in|7.0.0.2036|123|Out Of Allowed Policy|5|cnl=1 cnlLabel=Computer ID
act=Deny dmac=00:0C:29:8D:F1:C9 smac=00:1C:23:01:85:37
TrendMicroDsFrameType=IP src=10.52.116.140 dst=10.52.116.23 in=66 cs3=DF 0
cs3Label=Fragmentation Bits proto=TCP spt=24430 dpt=23 cs2=0x00 SYN
cs2Label=TCP Flags cnt=1
TrendMicroDsPacketData=AAwpjfhJABwjAYU3CABFAAA0ZjFAAIAGl4cKNHSMCjr0F19uABe
fXY81AAAAAIACIADD8gAAAgQFtaEDAwiBAQQC
    
```

表 13-2. ファイアウォールイベント拡張フィールド

拡張フィールド	名前	説明	例
act	Action	ファイアウォールルールによる処理。値は、Block、Reset、Insert、Delete、Replace、または Log のいずれかです。ルールまたはネットワークエンジンが検出のみモードで動作している場合、処理の値の前に「IDS:」が付きます。	act=Block act=Reset

表 13-2. ファイアウォールイベント拡張フィールド (続き)

拡張フィールド	名前	説明	例
cn1	Computer Identifier	特定の Syslog イベントからクライアントプラグインコンピュータを一意に識別するのに使用できる、クライアントプラグインコンピュータの内部識別子。	cn1=113
cn1Label	Computer ID	フィールド cn1 のフレンドリ名のラベル。	cn1Label=Computer ID
cnt	Repeat Count	このイベントが連続して繰り返された回数。	cnt=8
cs2	TCP Flags	(TCP プロトコルの場合のみ) raw TCP フラグバイトの後には、「URG」、「ACK」、「PSH」、「RST」、「SYN」、「FIN」の各フィールドが続きます。このフラグバイトは、TCP ヘッダが設定されている場合に存在する可能性があります。	cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	TCP Flags	フィールド cs2 のフレンドリ名のラベル。	cs2Label=TCP Flags

表 13-2. ファイアウォールイベント拡張フィールド (続き)

拡張フィールド	名前	説明	例
cs3	Packet Fragmentation Information	「DF」フィールドは、「IP Don't Fragment」ビットが設定されている場合に存在します。「MF」フィールドは、「IP More Fragments」ビットが設定されている場合に存在します。	cs3=MF cs3=DF MF
cs3Label	Fragmentation Bits	フィールド cs3 のフレンドリ名のラベル。	cs3Label=Fragmentation Bits
cs4	ICMP Type and Code	(ICMP プロトコルの場合のみ) 単一のスペースで区切って個別の順序で格納されている ICMP タイプとコード。	cs4=11 0 cs4=8 0
cs4Label	ICMP	フィールド cs4 のフレンドリ名のラベル。	cs4Label=ICMP Type and Code
dmac	Destination MAC Address	送信先コンピュータのネットワークインタフェース MAC アドレス。	dmac=00:0C:29:2F:09:B3
dpt	Destination Port	(TCP プロトコルおよび UDP プロトコルの場合のみ) 送信先コンピュータの接続ポート。	dpt=80 dpt=135
dst	Destination IP Address	送信先コンピュータの IP アドレス。	dst=192.168.1.102 dst=10.30.128.2

表 13-2. ファイアウォールイベント拡張フィールド (続き)

拡張フィールド	名前	説明	例
in	Inbound Bytes Read	(受信接続の場合のみ) 読み取られた受信バイト数。	in=137 in=21
out	Outbound Bytes Read	(送信接続の場合のみ) 読み取られた送信バイト数。	out=216 out=13
proto	Transport protocol	使用する接続転送プロトコルの名前。	proto=tcp proto=udp proto=icmp
smac	Source MAC Address	送信元コンピュータのネットワークインタフェース MAC アドレス。	smac=00:0E:04:2C:02:B3
spt	Source Port	(TCP プロトコルおよび UDP プロトコルの場合のみ) 送信元コンピュータの接続ポート。	spt=1032 spt=443
src	Source IP Address	送信元コンピュータの IP アドレス。	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	Ethernet frame type	接続のイーサネットフレームの種類。	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI

表 13-2. ファイアウォールイベント拡張フィールド (続き)

拡張フィールド	名前	説明	例
TrendMicroDsPacketData	Packet data	(パケットデータを含めるように設定されている場合)パケットデータのBase64でエンコードされたコピー。等号はエスケープされます。たとえば、「¥=」のようになります。	TrendMicroDsPacketData=AA...BA¥=

DPI イベントログの形式

CEFの基本形式: CEF: バージョン | デバイスベンダ | デバイス製品 | デバイスバージョン | 署名ID | 名前 | 重要度 | 拡張

ログエントリのサンプル: 03-19-2010 17:11:05 Local0.Info
 10.52.116.23 Mar 19 16:10:58 chrisds7 CEF:0|Trend Micro|IDF Client
 Plug-in|7.0.0.2036|1000552|Generic Cross Site Scripting(XSS)
 Prevention|10|cn1=1 cn1Label=Computer ID dmac=00:0C:29:8D:F1:C9
 smac=00:1C:23:01:85:37 TrendMicroDsFrameType=IP src=10.52.116.140
 dst=10.52.116.23 in=465 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP
 spt=26362 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=Log cn3=22
 cn3Label=DPI Packet Position cs5=22 cs5Label=DPI Stream Position
 cs1=XSS_Attack cs1Label=DPI Note cs6=8 cs6Label=DPI Flags
 TrendMicroDsPacketData=R0VUIC8lM0NTQlJJUFQlM0VhbGVydChkb2N1bWVudC5jb2...

表 13-3. DPI イベントログの形式拡張

拡張フィールド	名前	説明	例
act	Action	DPI ルールによる処理。値は、Block、Reset、Insert、Delete、Replace、または Log のいずれかです。ルールまたはネットワークエンジンが検出のみモードで動作している場合、処理の値の前に「IDS:」が付きます。	act=Block
cn1	Computer Identifier	特定の Syslog イベントからクライアントプラグインコンピュータを一意に識別するのに使用できる、クライアントプラグインコンピュータの内部識別子。	cn1=113
cn1Label	Computer ID	フィールド cn1 のフレンドリ名のラベル。	cn1Label=Computer ID
cn3	DPI Packet Position	イベントをトリガしたデータの packets 内の位置。	cn3=37
cn3Label	DPI Packet Position	フィールド cn3 のフレンドリ名のラベル。	cn3Label=DPI Packet Position
cnt	Repeat Count	このイベントが連続して繰り返された回数。	cnt=8

表 13-3. DPI イベントログの形式拡張 (続き)

拡張フィールド	名前	説明	例
cs1	DPI Filter Note	(オプション) DPI ルールに関連する短いバイナリまたはテキストによる備考を含めることのできる注記用フィールド。注記用フィールドの値がすべて印刷可能な ASCII 文字の場合、値はテキストとしてログに記録され、スペース (空白文字) はアンダースコアに変換されます。バイナリデータが含まれる場合は、Base64 エンコードを使用してログに記録されます。	cs1=Drop_data
cs1Label	DPI Note	フィールド cs1 のフレンドリ名のラベル。	cs1Label=DPI Note
cs2	TCP Flags	(TCP プロトコルの場合のみ) raw TCP フラグバイトの後には、「URG」、「ACK」、「PSH」、「RST」、「SYN」、「FIN」の各フィールドが続きます。このフラグバイトは、TCP ヘッダが設定されている場合に存在する可能性があります。	cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	TCP Flags	フィールド cs2 のフレンドリ名のラベル。	cs2Label=TCP Flags

表 13-3. DPI イベントログの形式拡張 (続き)

拡張フィールド	名前	説明	例
cs3	Packet Fragmentation Information	「DF」フィールドは、「IP Don't Fragment」ビットが設定されている場合に存在します。「MF」フィールドは、「IP More Fragments」ビットが設定されている場合に存在します。	cs3=MF cs3=DF MF
cs3Label	Fragmentation Bits	フィールド cs3 のフレンドリ名のラベル。	cs3Label=Fragmentation Bits
cs4	ICMP Type and Code	(ICMP プロトコルの場合のみ) 単一のスペースで区切って個別の順序で格納されている ICMP タイプとコード。	cs4=11 0 cs4=8 0
cs4Label	ICMP	フィールド cs4 のフレンドリ名のラベル。	cs4Label=ICMP Type and Code
cs5	DPI Stream Position	イベントをトリガしたデータのストリーム内の位置。	cs5=128 cs5=20
cs5Label	DPI Stream Position	フィールド cs5 のフレンドリ名のラベル。	cs5Label=DPI Stream Position

表 13-3. DPI イベントログの形式拡張 (続き)

拡張フィールド	名前	説明	例
cs6	DPI Filter Flags	次のフラグの値の合計を含む組み合わせの値。 1 - Data truncated - データをログに記録できませんでした。 2 - Log Overflow - このログの後、ログがオーバーフローしました。 4 - Suppressed - このログの後、ログのしきい値が抑制されました。 8 - Have Data - パケットデータが含まれます。 16 - Reference Data - 以前にログに記録されたデータを参照します。	次の例は、1 (Data truncated) と 8 (Have Data) の組み合わせです。 cs6=9
cs6Label	DPI Flags	フィールド cs6 のフレンドリ名のラベル。	cs6=DPI Filter Flags
dmac	Destination MAC Address	送信先コンピュータのネットワークインタフェース MAC アドレス。	dmac=00:0C:29:2F:09:B3
dpt	Destination Port	(TCP プロトコルおよび UDP プロトコルの場合のみ) 送信先コンピュータの接続ポート。	dpt=80 dpt=135
dst	Destination IP Address	送信先コンピュータの IP アドレス。	dst=192.168.1.102 dst=10.30.128.2
in	Inbound Bytes Read	(受信接続の場合のみ) 読み取られた受信バイト数。	in=137 in=21
out	Outbound Bytes Read	(送信接続の場合のみ) 読み取られた送信バイト数。	out=216 out=13

表 13-3. DPI イベントログの形式拡張 (続き)

拡張フィールド	名前	説明	例
proto	Transport protocol	使用する接続転送プロトコルの名前。	proto=tcp proto=udp proto=icmp
Smac	Source MAC Address	送信元コンピュータのネットワークインタフェースMACアドレス。	smac=00:0E:04:2C:02:B3
Spt	Source Port	(TCP プロトコルおよびUDP プロトコルの場合のみ) 送信元コンピュータの接続ポート。	spt=1032 spt=443
Src	Source IP Address	送信元コンピュータのIPアドレス。	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	Ethernet frame type	接続のイーサネットフレームの種類。	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	Packet data	(パケットデータを含めるように設定されている場合) パケットデータのBase64 でエンコードされたコピー。等号はエスケープされます。たとえば、「¥=」のようになります。	TrendMicroDsPacketData=AA...BA¥=

システムイベントログの形式

CEFの**基本形式**: CEF: バージョン | デバイスベンダ | デバイス製品 | デバイスバージョン | 署名 ID | 名前 | 重要度 | 拡張

ログエントリのサンプル (1): 03-19-2010 17:32:07 Local0.Info
 10.52.116.23 Mar 19 17:32:00 chrisds7 CEF:0|Trend Micro|IDF Server
 Plug-in|7.0.1591|160|Authentication Failed|4|src=10.52.116.23
 suser=MasterAdmin target=MasterAdmin msg=User password incorrect for
 username MasterAdmin on an attempt to sign in from 127.0.0.1

ログエントリのサンプル (2): 03-19-2010 17:34:38 Local0.Info
 10.52.116.23 Mar 19 17:34:30 chrisds7 CEF:0|Trend Micro|IDF Server
 Plug-in|7.0.1591|300|Scan for Recommendations|4|src=10.52.116.23
 suser=System target=localhost msg=A Scan for Recommendations on computer
 (localhost) has completed. Any changes to the computer as a result of this
 Scan for Recommendations will have been reflected in a 'Computer Updated'
 system event.

表 13-4. システムイベントログの形式拡張

拡張フィールド	名前	説明	例
src	Source IP Address	送信元の脆弱性対策オプションサーバプラグインのIPアドレスです。	src=10.52.116.23
suser	Source User	送信元の脆弱性対策オプションサーバプラグインのユーザアカウントです。	suser=MasterAdmin

表 13-4. システムイベントログの形式拡張 (続き)

拡張フィールド	名前	説明	例
target	Target entity	イベントの対象のエンティティ。イベントの対象は、脆弱性対策オプションサーバプラグインまたはコンピュータにログインした管理者アカウントである可能性があります。	target=MasterAdmin target=server01
msg	Details	システムイベントの詳細。イベントの詳細な説明が含まれる場合があります。	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...

詳細ログポリシーモード

ログするイベント数を削減するため、脆弱性対策オプションサーバプラグインでは複数の詳細ログポリシーモード上で動作するよう設定することができます。これらモードは、「詳細」エリアの「システム」→「システム設定」→「ファイアウォールと DPI」画面で設定できます。

次の表は、より複雑な詳細ログポリシーモードのうちの 4 つの中から、どのイベントのタイプが無視されるかを一覧表示しています。

表 13-5. 無視するイベント

モード	無視するイベント
ステートフルと正規化の抑制	接続範囲外 無効なフラグ 無効なシーケンス 無効な ACK 未承諾の UDP 未承諾の ICMP ポリシーの許可外 再送の破棄

表 13-5. 無視するイベント (続き)

モード	無視するイベント
ステートフル、正規化、 およびフラグメントの 抑制	接続範囲外 無効なフラグ 無効なシーケンス 無効な ACK 未承諾の UDP 未承諾の ICMP ポリシーの許可外 CE フラグ 無効な IP 無効な IP データグラム長 フラグメント化 フラグメントオフセットが不正です 最初のフラグメントが小さすぎる フラグメントが範囲外 フラグメントオフセットが小さすぎる IPv6 パケット 受信接続の上限 送信接続の上限 SYN 送信の上限 サポート契約の期限切れ 不明な IP バージョン パケット情報が不正です ACK 再送の上限 切断された接続上のパケット 再送の破棄

表 13-5. 無視するイベント (続き)

モード	無視するイベント
ステートフル、フラグメント、および検証機能の抑制	接続範囲外 無効なフラグ 無効なシーケンス 無効な ACK 未承諾の UDP 未承諾の ICMP ポリシーの許可外 CE フラグ 無効な IP 無効な IP データグラム長 フラグメント化 フラグメントオフセットが不正です 最初のフラグメントが小さすぎる フラグメントが範囲外 フラグメントオフセットが小さすぎる IPv6 パケット 受信接続の上限 送信接続の上限 SYN 送信の上限 サポート契約の期限切れ 不明な IP バージョン パケット情報が不正です 無効なデータオフセット IP ヘッダなし 読み取り不能なイーサネットヘッダ 未定義 同一の送信元および送信先 IP TCP ヘッダ長が不正です
	読み取り不能なプロトコルヘッダ 読み取り不能な IPv4 ヘッダ 不明な IP バージョン ACK 再送の上限 切断された接続上のパケット 再送の破棄

表 13-5. 無視するイベント (続き)

モード	無視するイベント
タップモード	接続範囲外 無効なフラグ 無効なシーケンス 無効な ACK ACK 再送の上限 切断された接続上のパケット 再送の破棄



第14章

サポート情報

製品サポート情報

脆弱性対策オプション 1.5 のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポート サービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザー登録完了から1年間です（ライセンス形態によって異なる場合があります）。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意： サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

製品 Q&A

<http://esupport.trendmicro.co.jp/corporate/search.aspx>

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

トレンドマイクロ「セキュリティ情報」

トレンドマイクロでは、最新のセキュリティ情報をインターネットで公開しています。トレンドマイクロのセキュリティ情報 Web サイトでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

<http://jp.trendmicro.com/jp/threat/index.html>

管理コンソールからセキュリティ情報 Web サイトにアクセスすることもできます。セキュリティ情報 Web サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから「セキュリティ情報」リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ・ ウイルス名やキーワードから検索できるウイルスデータベース
- ・ コンピュータウイルスの最新動向に関するニュース
- ・ 現在流行中のウイルスや不正プログラムの情報
- ・ デマウイルスまたは誤警告に関する情報
- ・ ウイルスやネットワークセキュリティの予備知識

セキュリティ情報 Web サイトに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「セキュリティデータベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

<http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=jp>

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

http://inet.trendmicro.co.jp/esolution/attach_agreement.asp

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ)は、フィリピン・米国センターを本部として、日本、台湾、ドイツ、アイルランド、中国、フランス、イギリス、ブラジルの各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 1000 名以上のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

脆弱性対策オプションが使用するポート

脆弱性対策オプションサーバプラグインとクライアントプラグインを意図したとおりに機能させるには、多数のポートをアクセス可能にする必要があります。使用ポート、使用ポートの機能の説明、関連プロトコル、接続を初期化するアプリケーション、接続するためのアプリケーション、プロキシ使用の可否およびプロキシの種類、ポート設定の可否およびポートを設定できる場所のリストは次のとおりです。

ポート : 4118

- **用途** : サーバプラグインからクライアントプラグインへの通信
- **プロトコル** : TCP
- **接続元** : 脆弱性対策オプションサーバプラグイン
- **接続先** : クライアントプラグイン
- **プロキシ** : なし
- **設定** : このポートは設定不可です

ポート : 4119 (初期設定)

- **用途** : 脆弱性対策オプションサーバプラグインの Web ブラウザインタフェースへのアクセス
- **プロトコル** : TCP
- **接続元** : Web ブラウザ

- ・ **接続先**: 脆弱性対策オプションサーバプラグイン
- ・ **プロキシ**: なし
- ・ **設定**: このポートは設定不可です

ポート : 4120 (初期設定)

- ・ **用途**: クライアントプラグインからサーバプラグインへの通信
- ・ **プロトコル**: TCP
- ・ **接続元**: クライアントプラグイン
- ・ **接続先**: 脆弱性対策オプションサーバプラグイン
- ・ **プロキシ**: なし
- ・ **設定**: このポートは設定不可です

ポート : 514 (初期設定)

- ・ **用途**: Syslog
- ・ **プロトコル**: UDP
- ・ **接続元**: クライアントプラグイン
- ・ **接続先**: Syslog 機能
- ・ **プロキシ**: なし
- ・ **設定**: このポートは、「システム」→「システム設定」→「通知設定」で設定できます

ポート : 25 (初期設定)

- ・ **用途**: メールのアラート
- ・ **プロトコル**: TCP
- ・ **接続元**: 脆弱性対策オプションサーバプラグイン
- ・ **接続先**: 指定の SMTP サーバ
- ・ **プロキシ**: なし
- ・ **設定**: このポートは、「システム」→「システム設定」→「システム」で設定できます

ポート : 80

- **用途**: トレンドマイクロのアップデートサーバへ接続
- **プロトコル**: HTTP および SOCKS
- **接続元**: 脆弱性対策オプションサーバプラグイン
- **接続先**: トレンドマイクロのアップデートサーバ
- **プロキシ**: はい (オプション)
- **設定**: プロキシアドレスとポートは、「システム」→「システム設定」→「アップデート」で設定できます

ポート : ランダムに選択

- **用途**: ホスト名の DNS 検索
- **プロトコル**: TCP
- **接続元**: 脆弱性対策オプションサーバプラグイン
- **接続先**: DNS サーバ
- **プロキシ**: なし
- **設定**: 脆弱性対策オプションサーバプラグインがホスト名を検索する際に、このポートはランダムに選択されます

コンピュータとクライアントプラグインのステータス

脆弱性対策オプションサーバプラグインの「コンピュータ」画面の「ステータス」列には、コンピュータとクライアントプラグインの現在の状態が表示されます。「ステータス」列には、通常、ネットワーク上のコンピュータの状態と、それに続けて (カッコ内に) 保護を提供するクライアントプラグインの状態が表示されます (どちらかが存在する場合)。コンピュータまたはクライアントプラグインがエラー状態の場合、その状態も「ステータス」列に表示されます。操作が進行中の場合、その操作の状態が「ステータス」列に表示されます。

次の3つの表に、「コンピュータ」画面の「ステータス」列に表示されるステータスとエラーメッセージを示します。

注意：「ステータス」列には、これらの値に加えて、システムイベントまたはクライアントプラグインイベントが表示されることもあります。イベントの一覧については、「253 ページの「クライアントプラグインイベント」と「238 ページの「システムイベント」」を参照してください。

コンピュータの状態

表 B-1. コンピュータの状態

コンピュータの状態	説明
非管理対象	有効化されていません。
管理対象	クライアントプラグインが存在し、有効化されています。保留中の操作やエラーはありません。
アップデート中	クライアントプラグインは、新しい設定とセキュリティアップデートで更新中です。
アップデートの保留中 (スケジュール)	クライアントプラグインは、コンピュータのアクセススケジュールが許可した時点で、新しい設定とセキュリティアップデートの組み合わせによって更新されます。
アップデートの保留中 (ハートビート)	次のハートビートでアップデートが実行されます。
アップデートの保留中 (オフライン)	サーバプラグインは現在クライアントプラグインと通信できません。クライアントプラグインがオンラインになった時点でアップデートが適用されます。
開いているポートを検索する	サーバプラグインはコンピュータの開いているポートを検索しています。
有効化中	サーバプラグインはクライアントプラグインを有効化しています。
有効化中 (遅延)	クライアントプラグインの有効化は、関連するイベントベースタスクで指定された時間だけ遅延しています。
有効化済み	クライアントプラグインは有効化されています。
無効化の実行中	サーバプラグインがクライアントプラグインを無効化しています。このクライアントプラグインは、別のサーバプラグインによって有効化および管理することができます。
無効化の保留中 (ハートビート)	次のハートビート中にサーバプラグインから無効化の命令が送信されます。

表 B-1. コンピュータの状態 (続き)

コンピュータの状態	説明
ロック済み	コンピュータはロックされています。ロックされた状態の間、サーバプラグインはクライアントプラグインとは通信せず、コンピュータに関するアラートも生成されません。既存のコンピュータアラートには影響しません。
複数のエラー	複数のエラーがこのコンピュータで発生しています。詳細については、コンピュータのシステムイベントを参照してください。
複数の警告	複数の警告がこのコンピュータで有効になっています。詳細については、コンピュータのシステムイベントを参照してください。
クライアントプラグインのアップグレード中	このコンピュータのクライアントプラグインソフトウェアは、新しいバージョンにアップグレード中です。
推奨設定を検索する	推奨設定の検索が実行中です。
推奨設定の検索の保留中 (スケジュール)	推奨設定の検索は、コンピュータにアクセス可能となった時点で開始されます。
推奨設定の検索の保留中 (ハートビート)	サーバプラグインは、次のハートビートで推奨設定の検索を開始します。
推奨設定の検索の保留中 (オフライン)	クライアントプラグインは現在オフラインです。サーバプラグインは、通信が再確立された時点で推奨設定の検索を開始します。
ステータスの確認	クライアントプラグインの状態を確認中です。
イベントの取得	サーバプラグインはクライアントプラグインからイベントを取得しています。
アップグレード推奨	クライアントプラグインの新しいバージョンが利用可能です。ソフトウェアのアップグレードが推奨されます。

クライアントプラグインの状態

表 B-2. クライアントプラグインの状態

クライアントプラグインの状態	説明
有効化済み	クライアントプラグインは有効化されており、いつでもサーバプラグインによって管理することができます。
有効化が必要	有効化されていないクライアントプラグインが対象のコンピュータで検出されました。サーバプラグインで管理する前に有効化する必要があります。
不明	クライアントプラグインが存在するかどうか判定されていません。
無効化が必要	サーバプラグインが、すでに別の脆弱性対策オプションサーバプラグインによって有効化済みのクライアントプラグインを有効化しようとしていました。新しいサーバプラグインで有効化する前に、元の脆弱性対策オプションサーバプラグインでこのクライアントプラグインを無効化する必要があります。
再有効化が必要	クライアントプラグインはインストールされており、脆弱性対策オプションサーバプラグインによる再有効化を待機しています。
オンライン	クライアントプラグインはオンラインで、問題なく動作しています。
オフライン	クライアントプラグインとの通信は、「システム」→「設定」→「コンピュータ」画面で指定されたハートビート数の間で行われていません。

コンピュータエラー

表 B-3. コンピュータエラー

エラー状態	説明
通信エラー	一般的なネットワークエラーです。
コンピュータへのルートなし	ファイアウォールの設定または中間ルータの停止が原因でリモートコンピュータにアクセスできない場合に主に発生します。
ホスト名解決不能	ソケットのアドレスが解決されていません。
有効化が必要	まだ有効化されていないクライアントプラグインに命令が送信されました。
クライアントプラグインとの通信失敗	クライアントプラグインと通信できません。
プロトコルエラー	HTTP レイヤで通信に失敗しました。
無効化が必要	クライアントプラグインは、現在別のサーバプラグインによって有効化されています。
クライアントプラグインなし	対象のコンピュータでクライアントプラグインが検出されませんでした。
有効なソフトウェアバージョンなし	要求されたプラットフォーム / バージョンに対するインストーラが見つかりませんでした。
ソフトウェアの送信失敗	コンピュータにバイナリパッケージを送信するときにエラーが発生しました。
内部エラー	内部エラーです。サポートに問い合わせてください。
重複するコンピュータ	サーバプラグインのコンピュータリストにある 2 つのコンピュータが同じ IP アドレスを使用しています。

イベント

この章では、脆弱性対策オプションのイベントについて説明します。

この章で扱うトピックは次のとおりです。

- 232 ページの「ファイアウォールイベント」
- 234 ページの「DPI イベント」
- 238 ページの「システムイベント」
- 253 ページの「クライアントプラグインイベント」

ファイアウォールイベント

表 C-1. ファイアウォールイベント

イベント	備考
CE フラグ	CWR または ECE フラグが設定されており、ステートフル設定では、これらのパケットを拒否する必要があることが指定されています。
再送の破棄	再送が破棄されました。
最初のフラグメントが小さすぎる	フラグメント化されたパケットが発生し、フラグメントのサイズが TCP パケット (データなし) のサイズよりも小さくなっています。
フラグメントオフセットが小さすぎる	フラグメント化されたパケットシーケンスに指定されているオフセットが、有効なデータグラムのサイズよりも小さくなっています。
フラグメントが範囲外	フラグメント化されたパケットシーケンスに指定されているオフセットが、データグラムの最大サイズの範囲を超えています。
フラグメント化	フラグメント化されたパケットの拒否が許可されていないため、フラグメント化されたパケットが発生しました。
内部ドライバエラー	リソースが不足しています。
内部ステートのエラー	内部 TCP のステートフルエラーです。
無効な ACK	確認応答番号が無効なパケットが発生しました。
無効なアダプタ設定	無効なアダプタ設定を受信しています。
無効なデータオフセット	データオフセットパラメータが無効です。
無効なフラグ	パケットに設定されたフラグが無効です。現在の接続 (存在する場合) のコンテキスト内で意味をなさないフラグである可能性があります。または、フラグの組み合わせが無意味な可能性があります。(評価する接続のコンテキストに対してステートフル設定がオンになっている必要があります。)
無効な IP	パケットの送信元 IP が無効でした。

表 C-1. ファイアウォールイベント (続き)

イベント	備考
無効な IP データグラム長	IP データグラム長が IP ヘッダで指定されている長さよりも短くなっています。
無効なポートコマンド	FTP 制御チャンネルのデータストリームで無効な FTP コマンドが発生しました。
無効なシーケンス	シーケンス番号が無効なパケットまたは画面データサイズ外のパケットが発生しました。
無効な IP ヘッダ長	無効な IP ヘッダ長 ($< 5 \times 4 = 20$) が IP ヘッダに設定されています。
不明な IP バージョン	IPv4 または IPv6 以外の IP パケットが発生しました。
IPv6 パケット	IPv6 パケットが発生しました。IPv6 ブロックが有効になっています。
受信接続の上限	受信接続数が最大許容数を超過しています。
送信接続の上限	送信接続数が最大許容数を超過しています。
SYN 送信の上限	単一コンピュータからのハーフオープン接続数がステートフル設定に指定された数を超過しています。
ACK 再送の上限	再送された ACK パケットが ACK ストーム防止のしきい値を超過しています。
IP が Null	NULL (0.0.0.0) IP は現在のファイアウォール設定では許可されません。
ポリシーの許可外	パケットは、許可ルールまたは強制的に許可ルールを満たしていないため黙示的に拒否されます。
接続範囲外	既存の接続に関係のないパケットを受信しました。
重複しているフラグメント	このパケットのフラグメントは前に送信したフラグメントに重複しています。
切断された接続上のパケット	すでに切断された接続に属するパケットを受信しました。

表 C-1. ファイアウォールイベント (続き)

イベント	備考
同一の送信元および送信先 IP	送信元および送信先 IP が同じです。
SYN Cookie エラー	SYN Cookie の保護メカニズムにエラーが発生しました。
不明な IP バージョン	IP バージョンを認識できません。
読み取り不能なイーサネットヘッダ	このイーサネットフレームに含まれるデータがイーサネットヘッダよりも少なくなっています。
読み取り不能な IPv4 ヘッダ	読み取り不能な IPv4 ヘッダがパケットに含まれています。
読み取り不能なプロトコルヘッダ	読み取り不能な TCP、UDP、または ICMP ヘッダがパケットに含まれています。
未承諾の ICMP	ステートフル設定で ICMP ステートフルが有効になっています。強制的に許可ルールに一致しない未承諾のパケットを受信しました。
未承諾の UDP	コンピュータに承諾されていない受信 UDP パケットが拒否されました。

DPI イベント

表 C-2. DPI イベント

イベント	備考
Base64 のデコードエラー	Base64 形式でエンコードされるはずのパケットの内容が正しくエンコードされませんでした。
クライアントによるロールバックの試行	クライアントは ClientHello メッセージに指定されたものよりも古いバージョンの SSL プロトコルに対してロールバックを試行しました。
Deflate/GZIP コンテンツが破損しています。	Deflate/GZIP コンテンツが破損しています。

表 C-2. DPI イベント (続き)

イベント	備考
Deflate/GZIP チェックサムエラー	Deflate/GZIP チェックサムエラーです。
二重デコードのセキュリティホール	二重デコードのセキュリティホールです (%25xx、%25%xxd など)。
編集範囲が広すぎる	編集で、リージョンのサイズが最大許容サイズ (8,188 バイト) を超えようとしていました。
プレマスターキーの復号化時のエラー	ClientKeyExchange からプレマスターの秘密鍵を復号できません。
マスターキーの生成エラー	マスターの秘密鍵から、暗号化キー、MAC の秘密、およびベクタの初期設定を生成できません。
プレマスター要求の生成エラー	復号用のプレマスターの秘密鍵をキューに入れようとしたときにエラーが発生しました。
ハンドシェイクメッセージ (準備ができていません)	ハンドシェイクのネゴシエーション後に、SSL 状態のエンジンでハンドシェイクメッセージが発生しました。
URI に使用できない文字	URI に使用できない文字が使用されています。
Deflate/GZIP コンテンツが不完全	Deflate/GZIP コンテンツが破損しています。
UTF8 シーケンスが不完全	UTF8 シーケンスの途中で URI が終了しました。
Int Min/Max/Choice の制約エラー	ClientHello メッセージに指定されたものよりも古いバージョンの SSL プロトコルに対して、あるクライアントがロールバックを試行しました。
内部エラー	ループまたはネストされた型の処理中に、プロトコルデコードエンジンが内部の破損を検出しました。
無効な 16 進数のエンコード	%nn の nn が 16 進数ではありません。

表 C-2. DPI イベント (続き)

イベント	備考
無効な字句の命令	内部エラーが発生し、プロトコルデコードスタックが破損して接続処理が停止されました。
ハンドシェイク内の無効なパラメータ	ハンドシェイクプロトコルのデコードの試行中に無効または不正な値が生じました。
無効なトラバーサル	ルートの上に「.././」を使用しようとしてしました。
無効な文字の使用	無効な文字を使用しています。
無効な UTF8 のエンコード	無効または規定外のエンコードが試行されました。
鍵の交換エラー	一時的に生成した鍵を使用してサーバが SSL セッションを確立しようとしてしました。
鍵が大きすぎる	マスターの秘密鍵がプロトコル ID で指定されたものよりも大きくなっています。
パケットの最大一致数の超過	パケット内のパターン一致する箇所が 2,048 を超えています。この制限に達すると、エラーが返され、接続が破棄されます。通常これは、処理不要パケットまたは回避パケットを示しているためです。
最大編集回数の超過	パケットの 1 リージョンにおける最大編集回数 (32 回) を超えました。
メモリの割り当てエラー	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続によってバッファ (最大 2,048) や一致リソース (最大 128) が一度に要求された場合、1 つの IP パケットにおける一致数 (最大 2,048) が超過した場合、またはシステムのメモリが不足した場合に起こることがあります。
ハンドシェイクメッセージの順序が不適切	適切にフォーマットされたハンドシェイクメッセージの順序が不適切です。
パケットの読み込みエラー	パケットデータの読み込み中に低レベルの問題が発生。

表 C-2. DPI イベント (続き)

イベント	備考
レコードレイヤメッセージ	SSL 状態のエンジンがセッションの初期化前に SSL レコードを発生しました。
リージョンが大きすぎる	リージョン (編集リージョン、URI など) が閉じられずに、バッファの最大許容サイズ (7570 バイト) を超えています。これは、通常、データがプロトコルに合致しないために起こります。
更新エラー	所在のわからないキャッシュされたセッションキーによって SSL セッションが要求されました。
ランタイムエラー	ランタイムエラー。
検索上限に到達	プロトコルデコードルールには検索や PDU オブジェクトの制限が定義されていますが、オブジェクトを見つける前に制限に達しました。
スタックの深さ	ルールのプログラミングエラーが原因で、反復が行われたり、多くのネストされたプロシージャコールが使用されようとしていました。
型のネストが深すぎる	プロトコルデコードルールで、型のネストの最大の深さ (16) を超える型の定義とパケットデータが発生しました。
サポートされていない暗号化	不明またはサポートされていない暗号化スイートが要求されています。
サポートされていない Deflate/GZIP 辞書	Deflate/GZIP 辞書はサポートされていません。
サポートされていない GZIP ヘッダ形式 / 方法	GZIP ヘッダ形式 / 方法はサポートされていません。
サポートされていない SSL バージョン	クライアントが SSL V2 バージョンの処理を試行しました。
URI パスの深さの超過	分離記号「/」が多すぎます。パスの深さは最大 100 です。
URI パスが長すぎる	パス長が 512 文字を超えています。

システムイベント

次の表に、脆弱性対策オプションで記録可能なシステムイベントとその初期設定を示します（記録されていないイベントに関して通知は送信されません）。

表 C-3. システムイベント

番号	重大度	イベント	記録する	通知する
0	エラー	不明なエラー	オン	オン
100	情報	サーバプラグインの起動	オン	オン
101	情報	ライセンスの変更	オン	オン
102	情報	脆弱性対策オプションユーザアカウントの変更	オン	オン
103	警告	アップデートの確認の失敗	オン	オン
104	警告	ソフトウェアの自動ダウンロードの失敗	オン	オン
105	警告	スケジュール脆弱性対策オプションルールアップデートのダウンロードおよび適用の失敗	オン	オン
106	情報	スケジュール脆弱性対策オプションルールアップデートのダウンロードおよび適用	オン	オン
107	情報	脆弱性対策オプションルールアップデートのダウンロードおよび適用	オン	オン
108	情報	スクリプト実行済み	オン	オン
109	エラー	スクリプト実行の失敗	オン	オン
110	情報	システムイベントのエクスポート	オン	オン
111	情報	ファイアウォールイベントのエクスポート	オン	オン
112	情報	DPI イベントのエクスポート	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
113	警告	スケジュール脆弱性対策オプションルールアップデートのダウンロードの失敗	オン	オン
114	情報	スケジュール脆弱性対策オプションルールアップデートのダウンロード	オン	オン
115	情報	脆弱性対策オプションルールアップデートのダウンロード	オン	オン
116	情報	脆弱性対策オプションルールアップデートの適用	オン	オン
117	情報	サーバプラグインのシャットダウン	オン	オン
118	警告	サーバプラグインのオフライン	オン	オン
119	情報	サーバプラグインのオンライン復帰	オン	オン
120	エラー	ハートビートサーバの失敗	オン	オン
121	エラー	スケジューラの失敗	オン	オン
122	エラー	サーバプラグインメッセージスレッドの失敗	オン	オン
123	情報	サーバプラグインの強制シャットダウン	オン	オン
124	情報	脆弱性対策オプションルールアップデートの削除	オン	オン
130	情報	資格情報の生成	オン	オン
131	警告	資格情報の生成の失敗	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
150	情報	システム設定の保存	オン (オフにできません)	オン
151	情報	ソフトウェアの追加	オン	オン
152	情報	ソフトウェアの削除	オン	オン
153	情報	ソフトウェアのアップデート	オン	オン
154	情報	ソフトウェアのエクスポート	オン	オン
155	情報	ソフトウェアプラットフォームの変更	オン	オン
160	情報	認証の失敗	オン	オン
161	情報	脆弱性対策オプションルールアップデートのエクスポート	オン	オン
166	情報	新規ソフトウェアの確認の成功	オン	オン
167	エラー	新規ソフトウェアの確認の失敗	オン	オン
168	情報	コンポーネントの手動アップデート成功	オン	オン
169	エラー	コンポーネントの手動アップデート失敗	オン	オン
170	エラー	サーバプラグインの利用可能ディスク容量の不足	オン	オン
180	情報	アラートの種類のアップデート	オン	オン
190	情報	アラートの開始	オン	オン
191	情報	アラートの変更	オン	オン
192	情報	アラートの終了	オン	オン
197	情報	アラートメールの送信	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
198	警告	アラートメールの失敗	オン	オン
199	エラー	アラート処理の失敗	オン	オン
250	情報	コンピュータの作成	オン	オン
251	情報	コンピュータの削除	オン	オン
252	情報	コンピュータのアップデート	オン	オン
253	情報	コンピュータへのセキュリティプロファイルの割り当て	オン	オン
254	情報	コンピュータの移動	オン	オン
255	情報	有効化の要求	オン	オン
256	情報	アップデートの要求	オン	オン
257	情報	ロック済み	オン	オン
258	情報	ロック解除	オン	オン
259	情報	無効化の要求	オン	オン
260	情報	開いているポートの検索	オン	オン
261	警告	開いているポートの検索の失敗	オン	オン
262	情報	開いているポートの検索の要求	オン	オン
263	情報	開いているポートの検索のキャンセル	オン	オン
264	情報	クライアントプラグインソフトウェアのアップグレードの要求	オン	オン
265	情報	クライアントプラグインソフトウェアのアップグレードのキャンセル	オン	オン
266	情報	警告 / エラーのクリア	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
267	情報	ステータス確認の要求	オン	オン
268	情報	イベント取得開始の要求	オン	オン
270	エラー	コンピュータの作成の失敗	オン	オン
275	警告	重複するコンピュータ	オン	オン
276	情報	コンポーネントのアップデート	オン	オン
280	情報	コンピュータのエクスポート	オン	オン
281	情報	コンピュータのインポート	オン	オン
286	情報	コンピュータのログのエクスポート	オン	オン
290	情報	ドメインの追加	オン	オン
291	情報	ドメインの削除	オン	オン
292	情報	ドメインの更新	オン	オン
293	情報	インタフェース名の変更	オン	オン
294	情報	コンピュータブリッジ名の変更	オン	オン
295	情報	インタフェースの削除	オン	オン
296	情報	インタフェース IP の削除	オン	オン
297	情報	推奨設定の検索の要求	オン	オン
298	情報	推奨設定のクリア	オン	オン
299	情報	コンピュータへの資産評価の割り当て	オン	オン
300	情報	推奨設定の検索	オン	オン
301	情報	クライアントプラグインソフトウェアの配信の要求	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
302	情報	クライアントプラグインソフトウェアの削除の要求	オン	オン
303	情報	コンピュータ名の変更	オン	オン
306	情報	ベースラインの再構築要求	オン	オン
307	情報	アップデートのキャンセルの要求	オン	オン
330	情報	SSL 設定の作成	オン	オン
331	情報	SSL 設定の削除	オン	オン
332	情報	SSL 設定のアップデート	オン	オン
350	情報	セキュリティプロファイルの作成	オン	オン
351	情報	セキュリティプロファイルの削除	オン	オン
352	情報	セキュリティプロファイルのアップデート	オン	オン
353	情報	セキュリティプロファイルのエクスポート	オン	オン
354	情報	セキュリティプロファイルのインポート	オン	オン
368	警告	インタフェースの非同期	オン	オン
369	情報	インタフェースの同期	オン	オン
410	情報	ファイアウォールルールの作成	オン	オン
411	情報	ファイアウォールルールの削除	オン	オン
412	情報	ファイアウォールルールのアップデート	オン	オン
413	情報	ファイアウォールルールのエクスポート	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
414	情報	ファイアウォールルールのインポート	オン	オン
420	情報	ステートフル設定の作成	オン	オン
421	情報	ステートフル設定の削除	オン	オン
422	情報	ステートフル設定のアップデート	オン	オン
423	情報	ステートフル設定のエクスポート	オン	オン
424	情報	ステートフル設定のインポート	オン	オン
460	情報	アプリケーションの種類の作成	オン	オン
461	情報	アプリケーションの種類の削除	オン	オン
462	情報	アプリケーションの種類のアップデート	オン	オン
463	情報	アプリケーションの種類のエクスポート	オン	オン
464	情報	アプリケーションの種類のインポート	オン	オン
470	情報	DPI ルールの作成	オン	オン
471	情報	DPI ルールの削除	オン	オン
472	情報	DPI ルールのアップデート	オン	オン
473	情報	DPI ルールのエクスポート	オン	オン
474	情報	DPI ルールのインポート	オン	オン
505	情報	コンテキストの作成	オン	オン
506	情報	コンテキストの削除	オン	オン
507	情報	コンテキストのアップデート	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
508	情報	コンテキストのエクスポート	オン	オン
509	情報	コンテキストのインポート	オン	オン
510	情報	IP リストの作成	オン	オン
511	情報	IP リストの削除	オン	オン
512	情報	IP リストのアップデート	オン	オン
513	情報	IP リストのエクスポート	オン	オン
514	情報	IP リストのインポート	オン	オン
520	情報	ポートリストの作成	オン	オン
521	情報	ポートリストの削除	オン	オン
522	情報	ポートリストのアップデート	オン	オン
523	情報	ポートリストのエクスポート	オン	オン
524	情報	ポートリストのインポート	オン	オン
530	情報	MAC リストの作成	オン	オン
531	情報	MAC リストの削除	オン	オン
532	情報	MAC リストのアップデート	オン	オン
533	情報	MAC リストのエクスポート	オン	オン
534	情報	MAC リストのインポート	オン	オン
550	情報	スケジュールの作成	オン	オン
551	情報	スケジュールの削除	オン	オン
552	情報	スケジュールのアップデート	オン	オン
553	情報	スケジュールのエクスポート	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
554	情報	スケジュールのインポート	オン	オン
560	情報	予約タスクの作成	オン	オン
561	情報	予約タスクの削除	オン	オン
562	情報	予約タスクのアップデート	オン	オン
563	情報	予約タスクの手動実行	オン	オン
564	情報	予約タスクの開始	オン	オン
565	情報	バックアップの完了	オン	オン
566	エラー	バックアップの失敗	オン	オン
567	情報	未解決アラートの概要の送信中	オン	オン
568	警告	未解決アラートの概要の送信失敗	オン	オン
569	警告	メールの失敗	オン	オン
570	情報	レポートの送信中	オン	オン
571	警告	レポートの送信の失敗	オン	オン
572	エラー	無効な Report Jar	オン	オン
573	情報	資産評価の作成	オン	オン
574	情報	資産評価の削除	オン	オン
575	情報	資産評価のアップデート	オン	オン
576	エラー	レポートのアンインストールの失敗	オン	オン
577	エラー	レポートのアンインストール	オン	オン
580	警告	アプリケーションタイプのポート一覧の誤った設定	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
581	警告	アプリケーションタイプのポート一覧の誤った設定の解決	オン	オン
582	警告	設定が必要な DPI ルール	オン	オン
583	情報	設定が必要な DPI ルールの解決	オン	オン
590	警告	不明な予約タスクの種類	オン	オン
700	情報	クライアントプラグインソフトウェアのインストール	オン	オン
701	エラー	クライアントプラグインソフトウェアのインストールの失敗	オン	オン
702	情報	資格情報の生成	オン	オン
703	エラー	資格情報の生成の失敗	オン	オン
704	情報	有効化済み	オン	オン
705	エラー	有効化の失敗	オン	オン
706	情報	クライアントプラグインソフトウェアのアップグレード	オン	オン
707	警告	クライアントプラグインソフトウェアのアップグレードの失敗	オン	オン
708	情報	無効化済み	オン	オン
709	エラー	無効化の失敗	オン	オン
710	情報	イベントの取得	オン	オン
711	情報	クライアントプラグインソフトウェアの配信	オン	オン
712	エラー	クライアントプラグインソフトウェアの配信の失敗	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
713	情報	クライアントプラグインソフトウェアの削除	オン	オン
714	エラー	クライアントプラグインソフトウェアの削除の失敗	オン	オン
715	情報	クライアントプラグインのバージョンの変更	オン	オン
720	情報	アップデート済み	オン	オン
721	エラー	アップデートの失敗	オン	オン
722	警告	インタフェースの取得の失敗	オン	オン
723	情報	インタフェース取得の失敗の解決	オン	オン
724	警告	ディスク容量の不足	オン	オン
725	警告	イベントの抑制	オン	オン
726	警告	クライアントプラグインイベントの取得の失敗	オン	オン
727	情報	クライアントプラグインイベント取得の失敗の解決	オン	オン
728	エラー	イベントの取得失敗	オン	オン
729	情報	イベントの取得失敗の解決	オン	オン
730	エラー	オフライン	オン	オン
731	情報	オンラインに復帰	オン	オン
732	エラー	ファイアウォールルールエンジンのオフライン	オン	オン
733	情報	ファイアウォールルールエンジンのオンライン復帰	オン	オン
734	警告	コンピュータの時計の変更	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
735	警告	誤った設定の検出	オン	オン
736	情報	ステータス確認の失敗の解決	オン	オン
737	エラー	ステータス確認の失敗	オン	オン
738	エラー	オフラインの DPI ルールエンジン	オン	オン
739	情報	DPI ルールエンジンのオンライン復帰	オン	オン
740	エラー	クライアントプラグインエラー	オン	オン
741	警告	異常な再起動の検出	オン	オン
742	警告	通信の問題	オン	オン
743	情報	通信の問題の解決	オン	オン
745	警告	イベントの切り捨て	オン	オン
750	警告	前回の自動再試行	オン	オン
755	情報	脆弱性対策オプションサーバプラグインのバージョン互換性の解決	オン	オン
756	警告	脆弱性対策オプションサーバプラグインのアップグレードをお勧めします (セキュリティコンポーネントの互換性がありません)	オン	オン
760	情報	クライアントプラグインのバージョンの互換性の解決	オン	オン
761	警告	クライアントプラグインのアップグレード推奨	オン	オン
762	警告	クライアントプラグインのアップグレードが必要	オン	オン
763	警告	互換性のないクライアントプラグインのバージョン	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
764	警告	クライアントプラグインのアップグレードをお勧めします (セキュリティコンポーネントの互換性がありません)	オン	オン
765	警告	コンピュータの再起動が必要	オン	オン
766	警告	ネットワークエンジンモードの設定が非互換	オン	オン
767	警告	ネットワークエンジンモードのバージョンが非互換	オン	オン
768	警告	ネットワークエンジンモードの非互換の解決	オン	オン
770	警告	クライアントプラグインのハートビートの拒否	オン	オン
771	警告	不明なクライアントによる問い合わせ	オン	オン
780	情報	推奨設定の検索失敗の解決	オン	オン
781	警告	推奨設定の検索の失敗	オン	オン
784	情報	コンポーネントのアップデートの成功	オン	オン
785	警告	コンポーネントのアップデートの失敗	オン	オン
790	情報	クライアントプラグインが開始した有効化の要求	オン	オン
791	警告	クライアントプラグインが開始した有効化の失敗	オン	オン
800	情報	アラートの消去	オン	オン
801	情報	エラーの消去	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
850	警告	攻撃の予兆の検出: OS のフィン ガープリント調査	オン	オン
851	警告	攻撃の予兆の検出: ネットワーク またはポート検索	オン	オン
852	警告	攻撃の予兆の検出: TCP Null 検索	オン	オン
853	警告	攻撃の予兆の検出: TCP SYNFIN の検索	オン	オン
854	警告	攻撃の予兆の検出: TCP Xmas 検索	オン	オン
900	情報	サーバプラグイン監査の起動	オン	オン
901	情報	サーバプラグイン監査のシャット ダウン	オン	オン
902	情報	サーバプラグインのインストール 終了	オン	オン
903	警告	ライセンス関連設定の変更	オン	オン
910	情報	診断パッケージの生成	オン	オン
911	情報	診断パッケージのエクスポート	オン	オン
912	情報	診断パッケージのアップロード	オン	オン
913	エラー	自動診断パッケージのエラー	オン	オン
920	情報	使用状況情報の生成	オン	オン
921	情報	使用状況情報のパッケージのエク スポート	オン	オン
922	情報	使用状況情報のパッケージのアップ ロード	オン	オン
923	エラー	使用状況情報のパッケージのエ ラー	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
930	情報	証明書の受け入れ	オン	オン
931	情報	証明書の削除	オン	オン
940	情報	自動タグルールを作成	オン	オン
941	情報	自動タグルールを削除	オン	オン
942	情報	自動タグルールのアップデート	オン	オン
943	情報	タグの削除	オン	オン
970	情報	コマンドラインユーティリティの開始	オン	オン
978	情報	コマンドラインユーティリティの失敗	オン	オン
979	情報	コマンドラインユーティリティのシャットダウン	オン	オン
980	情報	システム情報のエクスポート	オン	オン
990	情報	サーバプラグインノードの追加	オン	オン
991	情報	サーバプラグインノードの削除	オン	オン
992	情報	サーバプラグインノードのアップデート	オン	オン
997	エラー	タグ付けエラー	オン	オン
998	エラー	システムイベント通知エラー	オン	オン
999	エラー	内部ソフトウェアエラー	オン	オン
1101	エラー	プラグインのインストールの失敗	オン	オン
1102	情報	プラグインのインストール	オン	オン
1103	エラー	プラグインのアップグレードの失敗	オン	オン

表 C-3. システムイベント (続き)

番号	重大度	イベント	記録する	通知する
1104	情報	プラグインのアップグレード	オン	オン
1105	エラー	プラグインの起動の失敗	オン	オン
1106	エラー	プラグインのアンインストールの失敗	オン	オン
1107	情報	プラグインのアンインストール	オン	オン

クライアントプラグインイベント

クライアントプラグインイベントは「システムイベント」画面の「システムイベント」内に表示されます。たとえば、「イベントの取得」システムイベントをダブルクリックすると、取得済みのすべてのクライアントプラグインイベントが一覧表示されたウィンドウが表示されます。

「廃止」と注記されているイベントは、最新のクライアントイベントでは生成されませんが、古いバージョンを実行している場合は表示される可能性があります。

表 C-4. クライアントプラグインイベント

番号	重大度	イベント	備考
0	エラー	不明なクライアントプラグインイベント	
ドライバ関連のイベント			
1000	エラー	エンジンが開けない	
1001	エラー	エンジンコマンドの失敗	
1002	警告	エンジンリストオブジェクトエラー	
1003	警告	オブジェクトの削除失敗	
1004	警告	エンジンが不正なルールのデータを返す	廃止

表 C-4. クライアントプラグインイベント (続き)

番号	重大度	イベント	備考
設定関連のイベント			
2000	情報	セキュリティ設定のアップデート	
2001	警告	無効なファイアウォール ルールの割り当て	廃止
2002	警告	無効なステートフル設定	廃止
2003	エラー	セキュリティ設定の保存 失敗	
2004	警告	無効なインタフェース割り 当て	
2005	警告	無効なインタフェース割り 当て	廃止
2006	警告	無効な処理	
2007	警告	無効なパケット方向	
2008	警告	無効なルール優先度	
2009	警告	認識できない IP アドレス の形式	廃止
2010	警告	無効な送信元 IP リスト	廃止
2011	警告	無効な送信元ポートリスト	廃止
2012	警告	無効な送信先 IP リスト	廃止
2013	警告	無効な送信元ポートリスト	廃止
2014	警告	無効なスケジュール	廃止
2015	警告	無効な送信元 MAC リスト	廃止
2016	警告	無効な送信先 MAC リスト	廃止

表 C-4. クライアントプラグインイベント (続き)

番号	重大度	イベント	備考
2017	警告	無効なスケジュール長	
2018	警告	無効なスケジュール文字列	
2019	警告	認識できない IP アドレスの形式	廃止
2020	警告	オブジェクトが見つからない	
2021	警告	オブジェクトが見つからない	
2022	警告	無効なルールの割り当て	
2050	警告	ファイアウォールルールが見つからない	廃止
2075	警告	トラフィックストリームが見つからない	廃止
2076	警告	DPI ルールが見つからない	廃止
2077	警告	パターンリストが見つからない	廃止
2078	警告	トラフィックストリーム変換エラー	廃止
2079	警告	無効な DPI ルールの XML ルール	廃止
2080	警告	条件指定のファイアウォールルールが見つからない	廃止
2081	警告	条件指定の DPI ルールが見つからない	廃止
2082	警告	空の DPI ルール	廃止
2083	警告	DPI ルールと XML ルールの変換エラー	廃止

表 C-4. クライアントプラグインイベント (続き)

番号	重大度	イベント	備考
2085	エラー	セキュリティ設定エラー	
2086	警告	サポートされていない IP マッチタイプ	
2087	警告	サポートされていない MAC マッチタイプ	
2088	警告	無効な SSL 資格情報	
2089	警告	SSL 資格情報が見つかりません	
ハードウェア関連のイベント			
3000	警告	無効な MAC アドレス	
3001	警告	イベントデータの取得失敗	
3002	警告	インタフェースが多すぎる	
3003	エラー	外部コマンドの実行不能	
3004	エラー	外部コマンド出力の読み取り不能	
3005	エラー	OS 呼び出しエラー	
3006	エラー	OS 呼び出しエラー	
3007	エラー	ファイルエラー	
3008	エラー	コンピュータ固有のキーエラー	
3009	エラー	クライアントプラグインの予期しないシャットダウン	
3010	エラー	クライアントプラグインのデータベースエラー	

表 C-4. クライアントプラグインイベント (続き)

番号	重大度	イベント	備考
3600	エラー	Windows システムディレクトリの取得失敗	廃止
3601	警告	ローカルデータ読み取りエラー	Windows エラー。
3602	警告	Windows サービスエラー	Windows エラー。
3603	エラー	ファイルマッピングエラー	Windows エラー。ファイルサイズエラー。
3700	警告	異常な再起動の検出	Windows エラー。
3701	情報	システムの前回起動時刻の変化	Windows エラー。
通信関連のイベント			
4000	警告	無効なプロトコルヘッダ	コンテンツ長が範囲外です。
4001	警告	無効なプロトコルヘッダ	コンテンツ長がありません。
4002	情報	コマンドセッションの開始	
4003	情報	設定セッションの開始	
4004	情報	コマンドの受信	
4011	警告	サーバプラグインへの接続に失敗しました	
4012	警告	ハートビートの失敗	
クライアントプラグイン関連イベント			
5000	情報	クライアントプラグインの起動	

表 C-4. クライアントプラグインイベント (続き)

番号	重大度	イベント	備考
5001	エラー	スレッドの除外	
5002	エラー	操作のタイムアウト	
5003	情報	クライアントプラグインの停止	
5004	警告	時計の変更	
5005	情報	クライアントプラグインの監査開始	
5006	情報	クライアントプラグインの監査停止	
5008	警告	Filter Driver 接続の失敗	
5009	情報	Filter Driver 接続の成功	
5010	警告	Filter Driver の情報イベント	
ログ関連のイベント			
6000	情報	ログデバイスのオープンエラー	
6001	情報	ログファイルのオープンエラー	
6002	情報	ログファイルの書き込みエラー	
6003	情報	ログディレクトリの作成エラー	
6004	情報	ログファイル検索エラー	
6005	情報	ログディレクトリのオープンエラー	
6006	情報	ログファイルの削除エラー	

表 C-4. クライアントプラグインイベント (続き)

番号	重大度	イベント	備考
6007	情報	ログファイルの名前変更エラー	
6008	情報	ログの読み取りエラー	
6009	警告	空き容量不足によるログファイルの削除	
6010	警告	イベントは抑制されました	
6011	警告	イベントの切り捨て	
6012	エラー	ディスク容量の不足	
攻撃 / 検索 / 調査関連のイベント			
7000	警告	OS のフィンガープリント調査	
7001	警告	ネットワークまたはポート検索	
7002	警告	TCP Null 検索	
7003	警告	TCP SYNFIN の検索	
7004	警告	TCP Xmas 検索	

索引

英数字

- break 133
- Cisco NAC
 - 概要 231
- Deep Packet Inspection 112、205
- drop 126
- setdrop 126
- UDP 擬似接続 137
- Web リソース 138
- Web ルール 137、138
- 接続をリセットする 126
- アプリケーションの種類 124、138
- イベント 114、116、234
- イベントにタグを付ける 117
- イベントログをエクスポートする 117
- イベントを検索する 115
- イベントをフィルタする 115
- オンまたはオフにする 113
- カウンタ 128
- カスタムルールを作成する 123
- クエリルール 138
- 検出モード 126
- コメント 125
- システム設定 175
- 実行の順序 136
- ステート 125、127
- 接続をリセットする 126
- 大文字小文字の区別の照合 127
- パケット処理のシーケンス 112
- パターン 129
- 範囲の制約 127
- 予防モード 126
- ルール 119
- ルール処理 130
- ルールを作成したり編集する 120
- レジスタの割り当て 131
- レジスタへアクセスする 132
- レジスタを比較する 132
- drop 126
- if 文 133
- IP リスト 142
- MAC リスト 143
- Modulo32 比較 135
- setdrop 126
- SNMP 197
- SQL Server Express
 - 上限 158
 - ログのアーカイブ 158
- Syslog 197、198
 - 統合 197
 - メッセージを解析する 199
- TrendLabs 220
- UDP 擬似接続 137
- Web コンソール 11
- Web 上の脅威 142
- Web リソース 138
- Web ルール 137、138
- XML での記法 124

あ

アップグレード

クライアントプラグイン 56

サーバプラグイン 153

アップデート 187、191

クライアントプラグイン 193

セキュリティ 192

アプリケーションの種類 124、138

アラート 34

設定する 35

メール送信する 36

アンインストール

クライアントプラグイン 58

サーバプラグイン 164

移行

コンピュータ 156、157

サーバプラグイン 154

イベント 58

DPI 114、115、116、234

エクスポートする 88、168

クライアントプラグイン 253

コンピュータ 58

システム 166、238

タグを付ける 117

ファイアウォール 84、232

イベントログの形式 205

インタフェースの分離 181

ウィジェット 28

追加や削除する 30

レイアウト 29

ウイルスバスター Corp.

Web コンソール 11

コンピュータと同期する 44

エラー

クリアする 59

コンピュータ 229

演算比較 135

か

カウンタ 128

カスタム DPI ルール 123

クエリルール 138

クライアントプラグイン 10、51

アップグレード 56

アップデート 193

アップデートする 55

アンインストール 58

イベント 253

ステータス 225、228

通信を設定する 51

停止および起動する 55

配信 53

無効にする 56

有効化 54

警告

クリアする 59

継承 69

検索設定 185

攻撃の予兆設定 183

コンテキスト 146

コンピュータ 42、58

- ウイルスバスター Corp. と同期する 44
 - エラー 229
 - 警告 / エラーをクリアする 59
 - 検索する 44
 - 資産評価 60
 - システム設定 171
 - 詳細 61
 - 情報を表示する 42
 - 推奨設定の検索 46
 - ステータス 43、225、226
 - セキュリティプロファイルを割り当てる 50
 - 開いているポートの検索 45
 - プレビュー 43
 - ロック解除する 60
 - ロックする 60
 - コンポーネント 142
 - IP リスト 142
 - MAC リスト 143
 - コンテキスト 146
 - スケジュール 148
 - ポートリスト 144
- さ
- サーバ診断 194
 - サーバプラグイン
 - Syslog の設定 198
 - アップグレード 153
 - アンインストール 164
 - 移行 154、156
 - 組込みデータベースの最適化 158
 - コンピュータの移行 157
 - データベーススペースを最小化する 158
 - データベースの容量 159
 - バックアップおよび復元 161
 - 別のデータベースへの移行 160
 - 保護 152
 - 最適化 158
 - システム 166
 - アップデート 187、191
 - イベント 166、238
 - イベントにタグを付ける 168
 - イベントをフィルタする 167
 - インタフェースの分離 181
 - クライアントプラグインのアップデート 193
 - 検索設定 185
 - 攻撃の予兆設定 183
 - コンテキスト設定
 - コンテキスト 182
 - コンピュータ設定 171
 - サーバ診断 194
 - システムの設定 188
 - セキュリティアップデートの適用 192
 - 設定 170
 - タスク 190
 - 通知設定 185
 - ファイアウォールと DPI の設定 175
 - ライセンス 191
 - ランク付け設定 186
 - 実行の順序 136
 - 新機能 6
 - 推奨設定の検索 46
 - クリアする 49

結果 48

ルールを設定する 49

スクリプト 197

スケジュール 148

ステータス

クライアントプラグイン 225、228

コンピュータ 225、226

ステート 127

ステートフル設定 94、105

ステートフルフィルタ 93

脆弱性対策オプション

概要 6

セキュリティアップデート 192

セキュリティプロファイル 76

作成する 76

表示 77

編集 77

た

大文字小文字の区別の照合 127

タグ 189

イベント 88

システムイベント 168

ダッシュボード 30

表示 189

タスク 190

ダッシュボード 27

ウィジェット 28

ウィジェットレイアウト 29

カスタマイズする 29

コンピュータおよびドメインでフィルタ
する 31

設定する 31

設定を保存する 32

タグでフィルタする 30

日時でフィルタする 31

通知設定 185

データベース

移行 160

最適化 158

スペースを最小化する 158

容量 159

テクニカルサポート 218

等式 134

は

パターン 129

バックアップ 161、162、163

スケジュール 163

範囲の制約 127

ビット単位 136

開いているポートの検索 45

キャンセルする 46

ファイアウォール 84

イベント 84、87、232

イベントにタグを付ける 88

イベントログ 201

イベントをエクスポートする 88

イベントを検索する 87

イベントをフィルタする 87

オンまたはオフにする 84

- システム設定 175
 - ポリシー 97
 - ルール 90
 - ファイアウォールルール 90
 - 作成する 99
 - シーケンス 95
 - ステートフルフィルタ 93
 - 適用する 99
 - 放置ルール 94
 - ルール優先度 92
 - ルール処理 90、92
 - ルール優先度 92
 - ログ 96
 - 復元 161、162、164
 - 符号付き比較 134
 - 符号なし比較 134
 - ポート 221
 - ポートリスト 144
 - 放置ルール 94
 - 最適化 94
 - ステートフル設定 94
 - ログ 95
- ま
- メール
 - 設定する 36
- や
- 優先 69、73

ら

- ライセンス 191
- ランク付け設定 186
- ルール優先度 92
- ルール処理 90、92
- ルール優先度 92
- レジスタ
 - アクセスする 132
 - 比較する 132
 - 割り当て 131
- レポート 38
- ログ 196
 - DPI イベントログの形式 205
 - SNMP 197
 - Syslog 197、198
 - Syslog の統合 197
 - Syslog メッセージ 199
 - サーバプラグインの設定 198
 - 詳細ログポリシーモード 213
 - スクリプト 197
 - 設定する 196
 - 通知 196
 - ファイアウォールイベントログ 201
 - 放置ルール 95
- ログのアーカイブ 158

