セキュアなWebアプライアンスアクセスログの理解

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)アクセスログの構造について説明します。

前提条件

要 件

次の項目に関する知識が推奨されます。

- SWAのコマンドラインインターフェイス(CLI)へのアクセス。
- SWAへの管理アクセス。
- SWAワークフローの基本知識

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

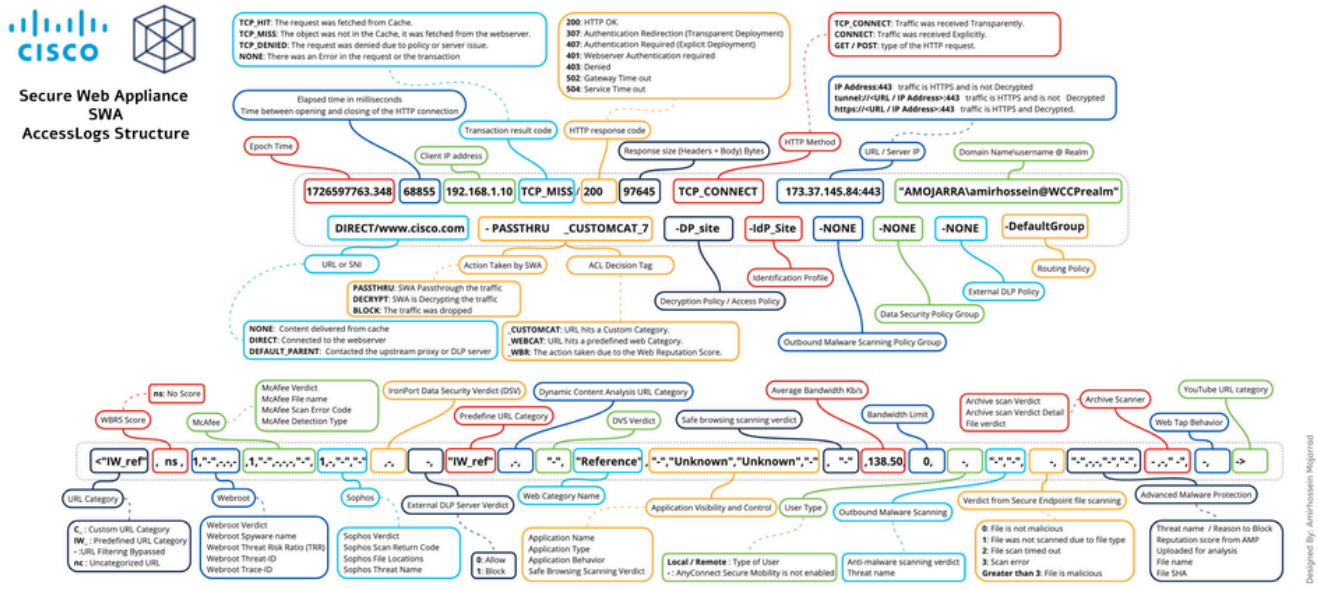
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

アクセスログ構造

この記事では、次の例でアクセスログ構造について説明します。

```
1726597763.348 68855 192.168.1.10 TCP_MISS/200 97645 TCP_CONNECT 10.37.145.84:443 "AMOJARRA\amirhossein
```



イメージ – アクセスログ構造

注：アクセスログの構造は、SWAのバージョンによって異なります。各Accesslogファイルの先頭には、構造とフォーマット指定子の順序を示す行があります。

セクション	アクセスログからのサンプル	形式指定子	詳細
エポック時間	1726597763.348	%t	エポック時間(Epoch time)（Unix時間またはPOSIX呼ばれます）は、1970年1月1日から経過した合計秒/マイクロ秒）を00:00:00 UTC(GMT)でカウント追跡するシステムです

<table>
<tr><td></td><td></td><td></td><td>トランザクションが完了したエポック時間。

この値は、オンラインのエポックタイムコンバータ
意のLinuxオペレーティングシステムで変換できます</td></tr>
<tr><td>Elapsed Time</td><td>68855</td><td>%e</td><td>要求が完了または中止され、接続が閉じられるまで
時間（ミリ秒）。</td></tr>
<tr><td>ソース IP アドレス</td><td>192.168.1.10</td><td>%a</td><td>クライアント/送信元IPアドレス。</td></tr>
<tr><td>トランザクション結果コード</td><td>TCP_MISS</td><td>%w</td><td>Transaction Result Codeは、SWAがクライアント要
する方法を示します。

トランザクション結果コードのリストを次に示しま
<table><tr><td>TCP_HIT</td><td>要求され
クトはデ
ッシュか
されまし</td></tr><tr><td>TCP_IMS_HIT</td><td>クライア
ジェクト
Modified-
を送信し
クトがキ
で見つか
プロキシ
（変更な
するか、
場合は20
れたオブ
応答しま</td></tr><tr><td>TCP_メモリ_ヒット</td><td>要求され
エクトは
ッシュか
されまし</td></tr><tr><td>TCP_MISS</td><td>オブジェ
ャッシュ</td></tr></table></td></tr>
</table>

				らなかっ のサーバ ッチされ
			TCP_REFRESH_HIT	オブジェ ッシュ内 たが、有 れました は元のサ IMS (If-M Since)要 、サーバ ェクトが いないこ ました。 、アプラ ディスク リキャッ ブジェク チしまし
			TCP_CLIENT_REFRESH_ミス	クライア Pragma: cacheへ 行して、 fetch res cache要求 ました。 アントか ーにより アンスは からオブ フェッチ
			TCP_DENIED	アクセス により、 ト要求が した。
			TCP_DENIED_SSL HTTPS（認証）	「Acces NONE」 ションで 生しまし

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>ば、DNS
トウェイ
ウトが発
などです</td></tr>
<tr><td>TCP_CLIENT_REFRESH_MISS_SSLの設定</td><td>HTTPS更</td></tr>
<tr><td>TCP_MISS_SSLのHTTPS</td><td>オブジェ
ッシュに
んでした</td></tr>
</table>
</td></tr>
<tr><td>HTTP応答コード</td><td>/200</td><td>%h</td><td>
HTTP応答コードは、クライアントのHTTP要求に応
Webサーバが返すステータスコードを表します。

最も重要なHTTP応答コードのリストを次に示しま
いては、この記事の「HTTP応答コード」のセクシ
してください)。
<table>
<tr><td>Status Code</td><td>意味</td></tr>
<tr><td>000</td><td>000は、TLSフェーズ以降のデータ転送中
断された場合の非標準の応答コードです。</td></tr>
<tr><td>2xx成功</td><td></td></tr>
<tr><td>200</td><td>OK</td></tr>
<tr><td>204</td><td>コンテンツなし</td></tr>
<tr><td>206</td><td>部分的なコンテンツ（範囲要求とも呼ば</td></tr>
<tr><td></td><td></td></tr>
<tr><td>3xxリダイレクト</td><td></td></tr>
<tr><td>301</td><td>永続的なリダイレクト。</td></tr>
<tr><td>302</td><td>一時的なリダイレクト</td></tr>
<tr><td>304</td><td>変更なし</td></tr>
<tr><td>307</td><td>認証のための一時的なリダイレクト

（通常、SWAがユーザを認証している間</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>導入で見られます）</td></tr>
<tr><td></td><td></td></tr>
<tr><td>4xxクライアントエラー</td><td></td></tr>
<tr><td>400</td><td>不正な要求</td></tr>
<tr><td>401</td><td>Webサーバ認証が必要（通常は、SWAが証している間に透過的な導入で見られる</td></tr>
<tr><td>403</td><td>禁止</td></tr>
<tr><td>404</td><td>見つかりません</td></tr>
<tr><td>407</td><td>明示的なプロキシ認証が必要</td></tr>
<tr><td></td><td></td></tr>
<tr><td>5xxサーバエラー</td><td></td></tr>
<tr><td>500</td><td>内部サーバエラー</td></tr>
<tr><td>502</td><td>不正なゲートウェイ</td></tr>
<tr><td>503</td><td>利用不能なサービス</td></tr>
<tr><td>504</td><td>ゲートウェイタイムアウト</td></tr>
</table></td></tr>
<tr><td>転送された合計サイズ</td><td>97645</td><td>%s</td><td>要求に対して転送された合計バイト数です。</td></tr>
<tr><td>HTTP メソッド</td><td>TCP_接続</td><td>%1r</td><td>HTTPメソッドは、GETを使用したデータの取得や用したデータの送信など、Webサーバによってリソして実行される必要なアクションをクライアントがための標準化された方法です。<table>
<tr><td>GET</td><td>HTTP GETメソッドは、サータを要求するために使用情報の取得のみを目的としッセージ本文を含めること ん。簡単に言うと、GETはドを意味します。</td></tr>
<tr><td>POST</td><td>HTTP POSTメソッドは、サ</td></tr>
</table></td></tr>
</table>

			ータを送信するために使用 は要求の本文に含まれてい に、フォームの送信、ファ プロード、またはサーバー 更するデータの送信に使用
			コネクト HTTP CONNECT方式は、 ーバを介したトンネルを確 に使用され、クライアント バへの直接TCP接続を作成 にします。これは、プロキ 号化通信を有効にするため HTTPSトラフィックでよく ます。 トラフィックがSWAによっ に受信されたことを示しま 、クライアントはプロキシ するように設定されていま
			TCP_接続 トラフィックが、WCCPま 4リダイレクション経由など WSAによって透過的に受信 とを示します。
宛先	10.37.145.84:443	%2r	このセクションでは、宛先サーバのURLとTCPポー 示します。 トランスペアレントリダイレクションでは、トラフ 復号化される前に、SWAは宛先IPアドレスとポート します。 URLがtunnel:// で始まる場合は、SWAがまだトラフ 復号化していないことを意味します。 URLがhttps://で始まる場合、SWAでトラフィックが れることを意味します。
ユーザー名と認証レルム	「アモジャラ\amirhossein@WCCPrealm」	%A	この接続に使用される資格情報。 要求が認証されると、SWAはユーザ名と認証レルム うにログに記録します。 <ドメイン名> \ <ユーザー名> @ <認証レルム名>

<table>
<tr><td></td><td></td><td></td><td>要求がまだ認証されていないか、認証が免除されて
は、ログにハイフン「-」が表示されます</td></tr>
<tr><td>アクセス タイプ</td><td>ダイレクト/</td><td>%H</td><td>要求内容を取得するために接続されたサーバーを説
ードです。

最も一般的な値は次のとおりです。
<table><tr><td>なし</td><td>Webプロキシはコンテンツを
ので、コンテンツを取得する
サーバに接続しませんでした</td></tr><tr><td>ダイレクト</td><td>Webプロキシは、コンテンツ
で指定されたサーバにアクセ
。</td></tr><tr><td>DEFAULT_PARENT</td><td>Webプロキシは、コンテンツ
ためにプライマリ親プロキシ
DLPサーバに送信しました。</td></tr></table></td></tr>
<tr><td>Server address</td><td>www.cisco.com</td><td>%d</td><td>データソースまたはサーバのIPアドレス。</td></tr>
<tr><td>MIMEコンテンツタイプ/サブタイプ</td><td>-</td><td>%c</td><td>MIMEドキュメント、ファイル、または一連のバイ
形式を示します。MIMEタイプは、IETF RFC 6838
び標準化されています

デフォルトタイプの役割を果たすためには、次の2
MIMEタイプが重要です。

• text/plainは、テキストファイルのデフォルト
キストファイルは人間が読める形式でなけれ
バイナリデータを含んでいてはなりません。
• application/octet-streamは、その他すべての場
ォルト値です。不明なファイルタイプはこの
用する必要があります。ブラウザがこれらの
操作するときには特に注意を払い、ソフトウ
性や危険な動作からユーザを保護します。

MIMEタイプの完全なリストについては、次のサイ
てください。メディアタイプ(iana)</td></tr>
</table>

<table>
<tr>
<td>ACLデシジョンタグ</td>
<td>パススルー_CUSTOMCAT_7-</td>
<td>%D</td>
<td>ACLデシジョンタグは、Webプロキシがトランザクどのように処理したかを示す、アクセスログエントィールドです。これには、Webレピュテーションフ URLカテゴリ、およびスキャンエンジンからの情報ます。

注:ACL決定タグの末尾には、パフォーマンスるためにWebプロキシが内部で使用する、動的れた番号が含まれています。この番号は無視しませんん。

次に、最も重要なACLデシジョンタグのリストを示(詳細については、この記事の「ACLデシジョンタグションを参照してください)
<table>
<tr><th>ACLデシジョンタグ</th><th>説明</th></tr>
<tr><td>許可_CUSTOMCAT</td><td>Webプロキシは、リシーグループのURLカテゴリフィ設定に基づいてトョンを許可しまし</td></tr>
<tr><td>WBRSを許可(_W)</td><td>Webプロキシは、リシーグループのテーションフィルづいてトランザク可しました。</td></tr>
<tr><td rowspan="5">AMP_FILE_判定</td><td>ファイルに対するテーションサーバを表す値：</td></tr>
<tr><td>1 – 不明</td></tr>
<tr><td>2 – クリーン</td></tr>
<tr><td>3 – 悪意のある</td></tr>
<tr><td>4 – スキャン不能</td></tr>
<tr><td>ブロック管理</td><td>アクセスポリシーデフォルト設定にロックされたトラン。</td></tr>
<tr><td>BLOCK_ADMIN_接続</td><td>アクセスポリシーHTTP CONNECTで定義された宛先トに基づいてブロトランザクション</td></tr>
<tr><td>ブロック管理者カスタムユーザ</td><td>アクセスポリシー</td></tr>
</table>
</td>
</tr>
</table>

			エージェント	[カスタムユーザーエントのブロック]設されているユーザエントに基づいてブたトランザクショ
			BLOCK_ADMIN_トンネリング	Webプロキシは、リシーグループのトでの非HTTPトのトンネリングにトランザクションしました。
			BLOCK_ADMIN_FILE_タイプ	アクセスポリシー定義されているフプに基づいてブロトランザクション
			ブロック管理プロトコル	アクセスポリシー[プロトコルのブロで定義されたプロづいてブロックさザクション。
			ブロック_アンプ_応答	アクセスポリシー高度なマルウェア(AMP)の設定に基Webプロキシが応クしました。
			ブロック_AVC	アクセスポリシー対して構成されたション設定に基づザクションがブロした。
			BLOCK_CONTENT_UNSAFE安全でない	アクセスポリシーサイトコンテンツ定に基づいてトランがブロックされライアントの要求コンテンツに対すたが、ポリシーはンテンツをブロッに設定されていま
			BLOCK_CUSTOMCAT	アクセスポリシーカスタムURLカテタリング設定に基ンザクションがブました。
			ブロックICAP	Webプロキシは、リシーグループで

				いる外部DLPシス に基づいて、要求 しました。
			ブロックWBRS(_W)	アクセスポリシー Webレピュテーシ タ設定に基づいて れたトランザクシ
			ブロック_WEBCAT	アクセスポリシー URLカテゴリフィ 設定に基づいてト ョンがブロックさ
			ブロック_YTCAT	Webプロキシは、 リシーグループの YouTubeカテゴリ ング設定に基づい クションをブロッ 。
			復号化_管理者	Webプロキシは、 シーグループのデ 定に基づいてトラ ンを復号化しまし
			復号化_EUN_CUSTOMCAT	Webプロキシは、 シーグループのカ URLカテゴリフィ 設定に基づいてト ョンを復号化しま EUNが有効な場合 ックはドロップさ
			復号化_EUN_WBRS	Webプロキシは、 シーグループのW ーションフィルタ いて、トランザク 号化しました。EU 場合、トラフィッ プされます。
			復号化_EUN_WEBCAT	Webプロキシは、 シーグループのUR フィルタリング設 てトランザクショ しました。EUNが 、トラフィックは れます。
			復号化_WEBCAT	Webプロキシは、 シーグループのUR フィルタリング設 てトランザクショ

				しました。
			WBRSの復号化	Webプロキシは、 シーグループのW ーションフィルタ いて、トランザク 号化しました。
			DROP_ADMIN（削除）	Webプロキシは、 Policyグループの 設定に基づいてト ョンをドロップし
			DROP_WEBCAT	Webプロキシは、 シーグループのUR フィルタリング設 てトランザクショ プしました。
			ドロップ_WBRS	Webプロキシは、 Policyグループの Reputationフィル づいてトランザク ロップしました。
			パススルー_管理者	Webプロキシは、 シーグループのデ 定に基づいてトラ ンを通過しました
			パススルー_WEBCAT	Webプロキシは、 シーグループのUR フィルタリング設 てトランザクショ ました。
			パススルー_WBRS	Webプロキシは、 シーグループのW ーションフィルタ いてトランザクシ しました。
			その他	認証の失敗、サー 、クライアントか どのエラーが発生 Webプロキシは要 ませんでした。
ポリシー名	DP_サイト –	N/A	トラフィックのタイプに応じて、次のように表示さ • 復号化ポリシー名：トラフィックがHTTPSで 復号化されていない場合 • アクセスポリシー名：トラフィックがHTTPで または復号されている場合。	

アイデンティティポリシー	IdP_Site-	N/A	識別プロファイル名を表示します
アウトバウンドマルウェアスキャンポリシーグループ	NONE-	N/A	アウトバウンドマルウェアスキャンポリシーのグル ポリシーグループ名に含まれるスペースはすべてア コア(_)に置き換えられます
データセキュリティポリシーグループ	NONE-	N/A	Cisco Data Security Policyグループ名。トランザク ローバルCiscoデータセキュリティポリシーに一致 この値はDefaultGroupになります。 このポリシーグ は、Ciscoデータセキュリティフィルタが有効な場 示されます。データセキュリティポリシーが適用さ い場合は、「NONE」と表示されます。 ポリシーグループ名に含まれるスペースはすべてア コア(_)に置き換えられます
外部DLPポリシーグループ	NONE-	N/A	トランザクションがグローバル外部DLPポリシーに 合、この値はDefaultGroupです。 外部DLPポリシー れていない場合は、「NONE」と表示されます。 ポリシーグループ名に含まれるスペースはすべてア コア(_)に置き換えられます。
ルーティングポリシーグループ	デフォルトグループ –	N/A	ルーティングポリシーグループ名 asProxyGroupName/ProxyServerName。 トランザクションがグローバルルーティングポリシ する場合、この値はDefaultRoutingです。 アップス ロキシサーバが使用されていない場合、この値はD ポリシーグループ名にスペースがある場合は、アン ア(_)に置き換えられます。
Webトラフィックタップ	なし	N/A	Webトラフィックタップポリシー名。
URLカテゴ	<"C_Cisc",	%XC	要求が一致するURLカテゴリ。

<table>
<tr><td>リの省略形</td><td></td><td></td><td>
<table>
<tr><td>-</td><td>バイパスされたURLフィルタリング</td></tr>
<tr><td>ニコン</td><td>分類されていないURL</td></tr>
<tr><td>err</td><td>バイパスされたURLフィルタリング</td></tr>
<tr><td>インプ</td><td>不可能</td></tr>
<tr><td>IW_</td><td>カテゴリ名がIW_で始まる場合、要求がシスコの事前定義されたURLカテゴリに一致したことを意味します</td></tr>
<tr><td>C_</td><td>カテゴリ名がIC_で始まる場合、要求がカスタムURLカテゴリにヒットしたことを意味します</td></tr>
</table>
</td></tr>
<tr><td>Webレピュテーションスコア</td><td>-,</td><td>%XW</td><td>このフィールドには、Webレピュテーション(WBR
表示されます。

nsは、URLにスコアがないことを意味します。</td></tr>
<tr><td>Webrootスキャン</td><td>-,"-",-,-,-,</td><td></td><td>これらの5つのフィールドは、Webrootスキャンに関
ます
<table>
<tr><td>Webrootによる判定</td><td>%Xv</td><td>マルウェアスキャンWebrootがDVSエンされました。Webrて検出された応答にされます。

判定の詳細について記事の「マルウェアによる判定の値」をください。</td></tr>
<tr><td>Webroot Spyname氏</td><td>「%Xn」</td><td>オブジェクトに関連ているスパイウェア</td></tr>
</table>
</td></tr>
</table>

					Webrootによって検 応答にのみ適用され
			Webroot TRR、	%Xt	マルウェアが存在す を決定する、脅威リ (TRR)値に関連付け Webroot固有の値。 よって検出された応 適用されます。
			Webroot ThreatID、	%X	Webrootが脅威IDと する値。シスコカス ポートは、問題のト ューティングを行う 値を使用できます。 Webrootによって検 応答にのみ適用され
			Webrootトレース ID、	%Xi	Webrootがトレース して使用する値。シ タマーサポートは、 ラブルシューティン 際にこの値を使用で Webrootによって検 応答にのみ適用され
McAfeeスキャン	-,"-",-,-,"-",		これらの6つのフィールドは、McAfeeスキャンに関す。		
			マカフィー評決、	%Xd	マルウェアスキャン McAfeeがDVSエン れました。McAfee 出された応答にのみ ます。 判定の詳細について 記事の「マルウェア による判定の値」を ください。
			McAfeeファイル名、	"%Xe"	McAfeeがスキャン ルの名前。McAfee

					出された応答にのみ ます。
			McAfee Scanエラーコード、	%Xf	McAfeeがスキャン て使用する値。シス マーサポートは、問 ブルシューティング にこの値を使用でき McAfeeによって検 答にのみ適用されま
			McAfee検出タイプ	%Xg	McAfeeが検出タイ 用する値。シスコカ サポートは、問題の シューティングを行 の値を使用できます McAfeeによって検 答にのみ適用されま
			McAfeeウィルスのタイプ	%Xh	McAfeeがウイルス て使用する値。シス マーサポートは、問 ブルシューティング にこの値を使用でき McAfeeによって検 答にのみ適用されま
			マカフィーウイルス名、	「%Xj」	McAfeeがスキャン スの名前。McAfee 出された応答にのみ ます。
Sophosスキャン	-,-,"-","-",		これらの4つのフィールドは、Sophosスキャンに関 ます		
			Sophos判定	%XY	マルウェアスキャン SophosがDVSエン れました。Sophos 出された応答にのみ ます。 判定の詳細について

					記事の「マルウェア による判定の値」を ください。
			Sophosスキャン リターンコード、	%Xx	Sophosがスキャン ードとして使用する コカスタマーサポー 題のトラブルシュー を行う際にこの値を ます。Sophosによ れた応答にのみ適用 。
			Sophosファイル の場所	"%Xy"	Sophosが不適切な を検出したファイル Sophosによって検 答にのみ適用されま
			Sophos脅威名、	「%Xz」	Sophosが脅威名と る値。シスコカスタ ートは、問題のトラ ーティングを行う際 を使用できます。S って検出された応答 用されます。
Cisco Data Security Scanの判定	-,	%Xl	Cisco Data Securityスキャンの判定は、Cisco Data PolicyのContent列のアクションに基づいて行われま 次のリストは、このフィールドに指定可能な値を示 す。 0.許可 1.ブロック -（ハイフン）。Cisco Data Security Filtersによっ が開始されませんでした。この値は、Cisco Data S Filtersが無効の場合、またはURLカテゴリアクショ Allowに設定されている場合に表示されます。		
外部DLPスキャン判定	-,	%Xp	外部DLPスキャンの判定は、ICAP応答で指定され づいて行われます。		

			次のリストは、このフィールドに指定可能な値を示す。 0.許可 1.ブロック -（ハイフン）。外部DLPサーバーによってスキャれませんでした。この値は、外部DLPスキャンが無いる場合、またはExternal DLP Policies > Destinati で除外URLカテゴリが原因でコンテンツがスキャンった場合に表示されます。
定義済みのURLカテゴリ判定	"-",	%XQ	事前定義されたURLカテゴリ判定は、要求側のスキ決定され、短縮されます。 URLフィルタリングが無効な場合、このフィールトフン(-)が表示されます。 リクエストがカスタムURLカテゴリにヒットした場アクセスログに定義済みのURLカテゴリ名が表示さ、決定はカスタムURLカテゴリによって行われます URLカテゴリの省略形のリストについては、「URの説明」を参照してください。
URLカテゴリ判定	-,	%XA	応答側のスキャン中に動的コンテンツ分析(DCA)エって決定されるURLカテゴリ判定の省略形。 Cisco Web Usage Controls URLフィルタリングエンみ適用されます。 nc：この値は、動的コンテンツ分析エンジンが有効時にURLカテゴリが割り当てられていない場合に、スキャン判定に表示されます。これは、応答側のスURLがカテゴリ化される前の初期要求フェーズで、テゴリ化されていないことを示します
統合インバウンドDVS判定	"-",	%XZ	統合された応答側のアンチマルウェアスキャン判定有効になっているスキャンエンジンに関係なくマルテゴリが提供されます。サーバー応答スキャンによクまたは監視されたトランザクションに適用されま
Webレピュテーション	"-",	%Xk	カテゴリ名または脅威タイプは、Webレピュテーションルタによって返されます。カテゴリ名はWebレピ

<table>
<tr><td>フィルタ脅威タイプ</td><td></td><td></td><td>ンが高いときに返され、脅威タイプはレピュテーシ
いときに返されます。

通常、このフィールドは、レピュテーションが–4以
トに対して入力されます。</td></tr>
<tr><td>Googleがカプセル化されたURLを翻訳</td><td>"-",</td><td>%X#10#</td><td>Google翻訳エンジン内にカプセル化されたURL。
されたURLがない場合、フィールド値は「-」にな</td></tr>
<tr><td>アプリケーション制御(AVC/ADC)</td><td>"-","-","-",</td><td></td><td>この3つのフィールドには、Application Visibility an
Control(AVC)とApplication Discovery and Control(A
情報が記録されます。
<table><tr><td>AVC/ADCアプリケーション名</td><td>「%XO」</td><td>AVCまたはADCエンジン
されるアプリケーション
る場合）。AVCまたはAD
が有効な場合にのみ適用</td></tr><tr><td>AVC/ADCアプリケーションタイプ</td><td>「%Xu」</td><td>AVCまたはADCエンジン
されるアプリケーション
（該当する場合）。AVC
ADCエンジンが有効な場
用されます。</td></tr><tr><td>AVC/ADCアプリケーションの動作</td><td>「%Xb」</td><td>AVCまたはADCエンジン
されるアプリケーション
当する場合）。AVCまた
ジンが有効な場合にのみ
す。

AVCの場合は「_」、ADC
「Unknown」です。</td></tr></table></td></tr>
<tr><td>セーフブラウジング判定</td><td>"-",</td><td>%X</td><td>この値は、安全な検索またはサイトコンテンツの評
トランザクションに適用されたかどうかを示します
<table><tr><td>インストール</td><td>元のクライアント要求は安全ではなく
索機能が適用されました。</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td>エンクロージャ</td><td>元のクライアント要求は安全ではなくンテンツの評価機能が適用されました</td></tr>
<tr><td>unsupp（非対応）</td><td>元のクライアント要求は、サポートさ検索エンジンに対するものでした。</td></tr>
<tr><td>err</td><td>元のクライアント要求は安全ではあり安全な検索もサイトコンテンツの評価ーのために適用できませんでした。</td></tr>
<tr><td>-</td><td>クライアントの要求がバイパスされた、カスタムURLカテゴリでトランザク可された）か、サポートされていないションから要求が行われたため、安全イトコンテンツの評価機能も適用された。</td></tr>
</table></td></tr>
<tr><td>平均帯域幅</td><td>11.35,</td><td>%XB</td><td>要求の処理で消費された平均帯域幅（Kb/秒）。</td></tr>
<tr><td>帯域幅制限制御</td><td>0,</td><td>%XT</td><td>帯域幅制限制御設定によって要求が調整されたかと
す値。
「1」は要求が調整されたことを示します。
「0」は、要求が調整されなかったことを示します</td></tr>
<tr><td>User Type</td><td>-,</td><td>%l</td><td>要求を行うユーザのタイプ(「[Local]」または「[Re
AnyConnectセキュアモビリティが有効になってい
み適用されます。
有効になっていない場合、値はハイフン(-)です</td></tr>
<tr><td>アウトバウンドマルウェアスキャン</td><td>"-","-",</td><td></td><td>これらの2つのフィールドは、アウトバウンドマルャンポリシーが適用される際に、クライアント要求が原因でブロックまたはモニタされるトランザクシ用されます。<table>
<tr><td>ユニファイドアウトバウンドDVS判定</td><td>"%X3"</td><td>リクエスト側のマルスキャンの統合によ効化されているスキ</td></tr>
</table></td></tr>
</table>

					ンに依存しない）アン ドマルウェアスキャン が適用される際に、イ ト要求スキャンのため クまたはモニタされる クションに適用されま
			アウトバウンド脅威の名前	"%X4"	適用可能なアウトバウ ウェアスキャンポリシ ブロックまたはモニタ クライアント要求に割 れた脅威名。 この脅威名は、有効に るマルウェア対策スキ ジンとは無関係です。
高度なマルウェア防御	-,"-",-,"-","-","-",		次の6つのフィールドは、セキュアエンドポイント（ ルウェア防御とも呼ばれる）に関連しています。		
			ファイル判定	%X#1#	Secure Endpo ャンからの判 0：ファイルは りません 1：ファイルが め、ファイル ンされません 2：ファイルス タイムアウト 3：スキャンス [4 ~ 15]（3よ ）：ファイル あります
			脅威の名前	%X#2#	Secure Endpo ャンによって る脅威名。 「-」は脅威な ます。

			レピュテーションスコア	%X#3#	Secure エンファイルスキのレピュテーコア。このスクラウドレピョンサービスルの明確な判ことができなのみ使用され
			分析のアップロードアクション	%X#4#	アップロード析要求のイン： 「0」は、セドポイントがファイルのアドを要求しなとを示します 「1」は、セドポイントDにファイルのードを要求し示します。
			ファイル名	%X#5#	ダウンロード析されるファ前。
			ファイルSHA	%X#6#	このファイル256識別子。
アーカイブスキャン	-,-,"-",		次の3つのフィールドは、アーカイブファイルのステータスを示します。		
			アーカイブスキャン判定	%X#7#アーカイブスキャン判定。	
				ARCHIVESCAN_ALLCLEAR	検ファイルはす

					ARCHIVESCAN_BLOCKEDFILETYPE	
					ARCHIVESCAN_NESTEDTOODEEP	

					ARCHIVESCAN_UNKNOWNFMT	
					ARCHIVESCAN_UNSCANABLE	
					ARCHIVESCAN_FILETOOBIG	

					A B -
			アーカイブスキャン判定の詳細	%Xo	アーカイブスキャン判定の詳細。アクセ ：カスタムオブジェクトブロックの設定 検査可能アーカイブファイル (ARCHIVESCAN_BLOCKEDFILETYPE) された場合、この[判定の詳細]エントリ ックされたファイルの種類とブロックさ ルの名前が表示されます。 「UnScanable Archive-Blocked」または ブロックされたファイルタイプがアーカ れていないことを示します。
			ファイル判定	%Xm	Archive Scannerによるファイル判定
Webタップ	-,	%XU	Webタップの動作		
YouTube URLカテゴリ	->	%X#29#	トランザクションに割り当てられたYouTube URL （省略形）。カテゴリが割り当てられていない場合 ィールドには「nc」と表示されます。		

HTTP応答コード

HTTP応答コードの完全なリストは次のとおりです

Status Code	意味
1xx情報	
100	[Continue]
101	スイッチングプロトコル
102	処理中
103	初期ヒント

2xx成功	
200	OK
201	Created
202	承諾
203	権限のない情報
204	コンテンツなし
205	コンテンツのリセット
206	部分的なコンテンツ
207	マルチステータス
208	報告済み
226	使用するIM
3xxリダイレクト	
300	複数選択
301	完全に移動
302	見つかりました（以前は「一時的に移動」）
303	その他を参照
304	変更なし
305	プロキシを使用
306	スイッチプロキシ
307	認証のための一時的なリダイレクト （通常、SWAがユーザを認証している間の透過的な導入で見られます）
308	永続的なリダイレクト
4xxクライアントエラー	
400	不正な要求
401	Webサーバ認証が必要（通常は、SWAがユーザを認証している間に透過的な導入で見られる）
402	支払いが必要
403	禁止

404	見つかりません
405	メソッドは許可されていません
406	許容されない
407	明示的なプロキシ認証が必要
408	要求のタイムアウト
409	競合
410	なくなっている
411	必要な期間
412	前提条件が失敗しました
413	ペイロードが大きすぎます
414	URIが長すぎます
415	サポートされていないメディアタイプ
416	満足できない範囲
417	期待値の失敗
418	私はティーポット
421	誤った要求
422	処理不可能なエンティティ
423	ロック
424	失敗した依存関係
425	早すぎる
426	アップグレードが必要
428	前提条件が必要
429	要求が多すぎます
431	要求ヘッダーフィールドが大きすぎます
451	法的理由により利用不可
5xxサーバエラー	
500	内部サーバエラー
501	未実装
502	不正なゲートウェイ

503	利用不能なサービス
504	ゲートウェイタイムアウト
505	サポートされていないHTTPバージョン
506	バリエーションもネゴシエート
507	不十分な記憶域
508	ループの検出
510	拡張なし
511	ネットワーク認証が必要

ACLデシジョンタグ

ACLデシジョンタグの完全なリストを次に示します。

ACLデシジョンタグ	説明
ALLOW_ADMIN_ERROR_ページ	Webプロキシは、通知ページおよびその ージで使用される口ゴに対してトランザ ションを許可しました。
許可_CUSTOMCAT	Webプロキシは、アクセスポリシーグル プのカスタムURLカテゴリフィルタリン 設定に基づいてトランザクションを許可 ました。
ALLOW_REFERER（参照許可）	Webプロキシは、埋め込み/参照されたコ ンテンツ除外に基づいてトランザクショ を許可しました。
WBRSを許可(_W)	Webプロキシは、アクセスポリシーグル プのWebレピュテーションフィルタ設定 基づいてトランザクションを許可しまし 。
AMP_FILE_判定	ファイルに対するAMPレピュテーション ーバからの判定を表す値：
	1 – 不明
	2 – クリーン
	3 – 悪意のある
	4 – スキャン不能
ARCHIVESCAN_ALLCLEAR	アーカイブスキャン判定
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR：検査され アーカイブにブロックされたファイルタ プがありません。

ARCHIVESCAN_NESTEDTOODEEP	ARCHIVESCAN_BLOCKEDFILETYPE：査されたアーカイブに、ブロックされたァイルタイプがある。ログエントリの次フィールド（判定の詳細）には、詳細、体的にはブロックされたファイルのタイ、ブロックされたファイルの名前が表示れます。
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP：ーカイブは、設定された最大値よりも「プセル化」されたアーカイブまたはネスされたアーカイブが多いため、ブロックれます。判定の詳細フィールドには、「キャン不能なアーカイブブロック」と表されます。
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT：不明形式のファイルタイプが含まれているた、アーカイブはブロックされます。判定詳細は「スキャン不能なアーカイブのブック」です。
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE：スキンできないファイルが含まれているためアーカイブはブロックされています。判の詳細は「スキャン不能なアーカイブのロック」です。
	ARCHIVESCAN_FILETOOBIG：アーカブのサイズが設定された最大値を超えてるため、アーカイブはブロックされます判定の詳細は「スキャン不能なアーカイのブロック」です。
	アーカイブスキャン判定の詳細
	ログエントリのフィールドと判定フィードは、ブロックされたファイルのタイプブロックされたファイルの名前、「スキン不能なアーカイブ – ブロック」、また「 – 」など、ブロックされたファイルタプがアーカイブに含まれていないことをす、判定に関する追加情報を提供します
	たとえば、Inspectable Archiveファイル(ARCHIVESCAN_BLOCKEDFILETYPE)「アクセスポリシー：カスタムオブジェトブロック」設定に基づいてブロックさた場合は、「判定の詳細」エントリに、ロックされたファイルのタイプとブロッされたファイルの名前が表示されます。
	アーカイブインスペクションについての細は、『アクセスポリシー：オブジェク

	のブロックおよびアーカイブインスペクションの設定』を参照してください。
ブロック管理	アクセスポリシーグループのデフォルト設定に基づいてブロックされたトランザクション。
BLOCK_ADMIN_接続	アクセスポリシーグループのHTTP CONNECT Ports設定で定義された宛先のTCPポートに基づいてブロックされたトランザクション。
ブロック管理者カスタムユーザエージェント	アクセスポリシーグループの[カスタムユーザーエージェントのブロック]設定で定義されているユーザーエージェントに基いてブロックされたトランザクション。
BLOCK_ADMIN_トンネリング	Webプロキシは、アクセスポリシーグループのHTTPポートでの非HTTPトラフィックのトンネリングに基づいて、トランザションをブロックしました。
BLOCK_ADMIN_HTTPS_非ローカル宛先	トランザクションがブロックされましたクライアントは明示的なプロキシとしてSSLポートを使用して認証をバイパスしようとしました。これを防ぐために、WSA自体へのSSL接続では、実際のWSAリダイレクトホスト名への要求だけが許可されます。
ブロック管理者ID	データセキュリティポリシーグループで義されている要求本文コンテンツのMIMEの種類に基づいてブロックされたランザクション。
BLOCK_ADMIN_FILE_タイプ	アクセスポリシーグループで定義されてるファイルタイプに基づいてブロックされたトランザクション。
ブロック管理プロトコル	アクセスポリシーグループの[プロトコルのブロック]設定で定義されたプロトコルに基づいてブロックされたトランザクション。
BLOCK_ADMIN_SIZEです。	アクセスポリシーグループのオブジェクトサイズ設定で定義された応答のサイズに基づいてブロックされたトランザクション
BLOCK_ADMIN_SIZE_IDS（ブロック管理サイズID）	データセキュリティポリシーグループで義されている要求本文コンテンツのサイに基づいてブロックされたトランザクション。
ブロック_アンプ_応答	アクセスポリシーグループの高度なマルェア防御(AMP)の設定に基づいて、Webロキシが応答をブロックしました。
ブロック_AMW_要求	Webプロキシは、アウトバウンドマルウ

	アスキャンポリシーグループのマルウェ対策設定に基づいて要求をブロックしまた。リクエスト本文は、肯定的なマルウア判定を行いました。
ブロック_AMW_応答	アクセスポリシーグループのマルウェア策設定に基づいて、Webプロキシが応答ブロックしました。
ブロックAMW_REQ_URL	Webプロキシは、HTTP要求内のURLが全でないと疑うため、アクセスポリシーループのマルウェア対策設定に基づいて要求時にトランザクションをブロックしした。
ブロック_AVC	アクセスポリシーグループに対して構成れたアプリケーション設定に基づいてトンザクションがブロックされました。
BLOCK_CONTENT_UNSAFE安全でない	アクセスポリシーグループのサイトコンンツの規制の設定に基づいてトランザクョンがブロックされました。クライアンの要求はアダルトコンテンツに対するもでしたが、ポリシーはアダルトコンテンをブロックするように設定されています
BLOCK_CONTINUE_CONTENT_安全でない	トランザクションがブロックされ、[アクセスポリシー]グループのサイトコンテンツの規制の設定に基づいて[警告と続行]ページが表示されました。クライアントの求はアダルトコンテンツに対するもので たが、ポリシーはアダルトコンテンツにクセスするユーザに警告を与えるように定されています。
BLOCK_CONTINUE_CUSTOMCAT	トランザクションがブロックされ、「Warn」に設定されたアクセスポリシーグループのカスタムURLカテゴリに基づい「Warn and Continue」ページが表示さました。
BLOCK_CONTINUE_WEBCAT（ブロック継続WEBCAT）	トランザクションがブロックされ、「Warn」に設定されたアクセスポリシーグループ内の事前定義されたURLカテゴリ基づいて「Warn and Continue」ページが表示されました。
BLOCK_CUSTOMCAT	アクセスポリシーグループのカスタムURLカテゴリフィルタリング設定に基づてトランザクションがブロックされまし。
ブロックICAP	Webプロキシは、外部DLPポリシーグループで定義されている外部DLPシステムの定に基づいて、要求をブロックしました

BLOCK_SEARCH_UNSAFE安全でない	クライアント要求に安全でない検索クエが含まれていて、安全な検索を強制するうにアクセスポリシーが構成されているめ、元のクライアント要求はブロックさました。
ブロック_疑わしい_ユーザ_エージェント	アクセスポリシーグループのSuspect UsAgent（疑わしいユーザエージェント）の設定に基づいてブロックされたトランザション。
BLOCK_UNSUPPORTED_SEARCH_アプリケーション	アクセスポリシーグループの安全な検索定に基づいてトランザクションがブロッされました。トランザクションはサポーされていない検索エンジン用でした。ポシーは、サポートされていない検索エンンをブロックするように構成されていま。
ブロックWBRS(_W)	アクセスポリシーグループのWebレピューションフィルタ設定に基づいてブロッされたトランザクション。
ブロック_WBRS_IDS	Webプロキシは、データセキュリティポシーグループのWebレピュテーションフルタ設定に基づいて、アップロード要求ブロックしました。
ブロック_WEBCAT	アクセスポリシーグループのURLカテゴフィルタリング設定に基づいてトランザションがブロックされました。
ブロック_WEBCAT_IDS	Webプロキシは、データセキュリティポシーグループのURLカテゴリフィルタリグ設定に基づいてアップロード要求をブックしました。
ブロック_YTCAT	Webプロキシは、アクセスポリシーグループの定義済みのYouTubeカテゴリフィルリング設定に基づいてトランザクションブロックしました。
BLOCK_CONTINUE_YTCAT	Webプロキシがトランザクションをブロクし、「Warn」に設定されたアクセスポリシーグループ内の事前定義されたYouTubeカテゴリに基づいて「Warn anContinue」ページを表示しました。
復号化_管理者	Webプロキシは、復号化ポリシーグルーのデフォルト設定に基づいてトランザクションを復号化しました。
DECRYPT_ADMIN_EXPIRED_証明書	サーバー証明書の有効期限が切れていまが、Webプロキシはトランザクションを号化解除しました。
DECRYPT_EUN_ADMIN_DEFAULT_アクション	EUNが有効な場合、Webプロキシは復号

	ポリシーグループのドロップ接続として フォルト設定に基づいてトランザクショ を復号化しました。
DECRYPT_EUN_ADMIN_EXPIRED_証明書	EUNが有効な期限切れの証明書が HTTPSプロキシ設定によってドロップさ れると、Webプロキシはトランザクショ を復号化しました。
DECRYPT_EUN_ADMIN_無効_リーフ証明書	EUNが有効な無効なリーフ証明書が HTTPSプロキシ設定によってドロップさ れると、Webプロキシはトランザクショ を復号化しました。
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAMEです。	EUNが有効な不一致のホスト名を HTTPSプロキシ設定がドロップしたとき に、Webプロキシがトランザクションを 号化しました。
DECRYPT_EUN_ADMIN_OCSP_その他_エラー	EUNが有効な他のエラーがあるOCSPを HTTPSプロキシ設定がドロップすると、 Webプロキシはトランザクションを復号 しました。
復号化_EUN_ADMIN_OCSP_REVOKED_CERT	EUNが有効なOCSP失効証明書を HTTPSプロキシ設定がドロップすると、 Webプロキシはトランザクションを復号 しました。
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT（復号化）	EUNが有効な認識されないルート認証局 たは発行者証明書がHTTPSプロキシ設定 によってドロップされると、Webプロキ はトランザクションを復号化しました。
復号化_EUN_CUSTOMCAT	Webプロキシは、復号化ポリシーグルー のカスタムURLカテゴリフィルタリング 定に基づいてトランザクションを復号化 ました。EUNが有効な場合、トラフィッ はドロップされます。
復号化_EUN_WBRS	Webプロキシは、復号化ポリシーグルー のWebレピュテーションフィルタ設定に づいて、トランザクションを復号化しま た。EUNが有効な場合、トラフィックは ロップされます。
DECRYPT_EUN_WBRS_スコアなし	Webプロキシは、復号化ポリシーグルー にスコアURLがないというWebレピュテ ションフィルタの設定に基づいて、トラ ザクションを復号化しました。EUNが有 な場合、トラフィックはドロップされま 。
復号化_EUN_WEBCAT	Webプロキシは、復号化ポリシーグルー のURLカテゴリフィルタリング設定に基 いてトランザクションを復号化しました

	EUNが有効な場合、トラフィックはドロップされます。
復号化_WEBCAT	Webプロキシは、復号化ポリシーグループのURLカテゴリフィルタリング設定に基づいてトランザクションを復号化しました。
WBRSの復号化	Webプロキシは、復号化ポリシーグループのWebレピュテーションフィルタ設定に基づいて、トランザクションを復号化しました。
デフォルト_ケース	Webレピュテーションやマルウェア対策スキャンなどのAsyncOSサービスがトランザクションに対して何も実行しなかったため、Webプロキシはクライアントがサーバにアクセスすることを許可しました。
拒否_管理者	Webプロキシがトランザクションを拒否しました。これは、認証が必要で、HTTPSプロキシ設定でDecrypt for Authenticationが無効になっている場合に、HTTPS要求に対して発生します。
DROP_ADMIN（削除）	Webプロキシは、Decryption Policyグループのデフォルト設定に基づいてトランザクションをドロップしました。
削除する証明書	サーバー証明書の有効期限が切れているため、Webプロキシはトランザクションを除しました。
DROP_WEBCAT	Webプロキシは、復号化ポリシーグループのURLカテゴリフィルタリング設定に基づいてトランザクションをドロップしました。
ドロップ_WBRS	Webプロキシは、Decryption Policyグループの Web Reputationフィルタ設定に基づいてトランザクションをドロップしました。
MONITOR_ADMIN_EXPIRED_証明書	サーバー証明書の有効期限が切れているため、Webプロキシはサーバーの応答を監視しました。
モニタ_アンプ_応答	Webプロキシは、アクセスポリシーグループの高度なマルウェア防御(AMP)設定に基づいてサーバの応答を監視しました。
モニタ_AMW_応答	Webプロキシは、アクセスポリシーグループのマルウェア対策設定に基づいてサーバの応答を監視しました。
MONITOR_AMW_RESP_URL（モニタAMW応答URL）	Webプロキシは、HTTP要求のURLが安全ではないと疑っていますが、アクセスポリシーグループのマルウェア対策設定に基づいてトランザクションを監視しています。

モニタ_AVC	Webプロキシは、アクセスポリシーグループのアプリケーション設定に基づいてトランザクションを監視しました。
MONITOR_CONTINUE_CONTENT_UNSAFE（安全ではない）	当初、Webプロキシはトランザクションをブロックし、[アクセスポリシー]グループのサイトコンテンツの規制の設定に基づいて[警告と続行]ページを表示していました。クライアントの要求はアダルトコンテンツに対するものでしたが、ポリシーはアダルトコンテンツにアクセスするユーザに警告を与えるように設定されています。ユーザは警告を受け入れ、最初に要求されたサイトに進み、その後に他のスキャンエンジンによって要求がブロックされることはありませんでした。
MONITOR_CONTINUE_CUSTOMCAT（続行します）	当初、Webプロキシはトランザクションをブロックし、「Warn」に設定されたアクセスポリシーグループのカスタムURLカテゴリに基づいて「Warn and Continue」ページを表示していました。 ユーザは警告を受け入れ、最初に要求されたサイトに進み、その後に他のスキャンエンジンによって要求がブロックされることはありませんでした。
MONITOR_CONTINUE_WEBCAT（続行します）	当初、Webプロキシはトランザクションをブロックし、「Warn」に設定されたアクセスポリシーグループ内の事前定義されたURLカテゴリに基づいて「Warn and Continue」ページを表示していました。ユーザは警告を受け入れ、最初に要求されたサイトに進み、その後に他のスキャンエンジンによって要求がブロックされることはありませんでした。
MONITOR_CONTINUE_YTCAT（継続モニタ）	当初、Webプロキシはトランザクションをブロックし、「Warn」に設定されたアクセスポリシーグループ内の事前定義されたYouTubeカテゴリに基づいて「Warn and Continue」ページを表示していました。ユーザは警告を受け入れ、最初に要求されたサイトに進み、その後に他のスキャンエンジンによって要求がブロックされることはありませんでした。
モニタID	Webプロキシはデータセキュリティポリシーまたは外部DLPポリシーを使用してアップロード要求をスキャンしましたが、要求をブロックしませんでした。アクセスポリシーに対して要求を評価しました。

監視_疑わしい_ユーザ_エージェント	Webプロキシは、アクセスポリシーグループのSuspect User Agent設定に基づいてランザクションを監視しました。
モニタ_WBRS	Webプロキシは、アクセスポリシーグループのWebレピュテーションフィルタ設定基づいてトランザクションを監視しました。
許可なし	Webプロキシはアプリケーションへのアセスをユーザーに許可しませんでした。ーザーは認証領域に対して既に認証されいますが、アプリケーション認証ポリシで構成されたどの認証領域に対しても認されていないためです。
パスワードなし	ユーザが認証に失敗しました。
パススルー_管理者	Webプロキシは、復号化ポリシーグルーのデフォルト設定に基づいてトランザクョンを通過しました。
PASSTHRU_ADMIN_EXPIRED_証明書	サーバー証明書の有効期限が切れていまが、Webプロキシはトランザクションを過しました。
パススルー_WEBCAT	Webプロキシは、復号化ポリシーグルーのURLカテゴリフィルタリング設定に基いてトランザクションを通過しました。
パススルー_WBRS	Webプロキシは、復号化ポリシーグルーのWebレピュテーションフィルタ設定にづいてトランザクションを通過しました
リダイレクト_CUSTOMCAT	Webプロキシは、「リダイレクト」に設されたアクセスポリシーグループ内のカタムURLカテゴリに基づいて、別のURLトランザクションをリダイレクトしました。
SAAS認証	アプリケーション認証ポリシーで設定さた認証レルムに対してユーザが透過的に証されたため、Webプロキシはユーザにプリケーションへのアクセスを許可しました。
その他	認証の失敗、サーバーの切断、クライアトからの中止などのエラーが発生したた、Webプロキシは要求を完了しませんでた。

マルウェアスキャン判定の値

マルウェアスキャン判定は、URL要求またはサーバ応答に割り当てられた値で、マルウェアが含

まれる可能性を決定します。Webroot、McAfee、およびSophosスキャンエンジンは、マルウェアスキャン判定をDVSエンジンに返します。これにより、DVSエンジンは、スキャンされたオブジェクトをモニタするか、ブロックするかを判断できます。各マルウェアスキャン判定は、特定のアクセスポリシーのマルウェア対策設定を編集した場合に、アクセスポリシー>レピュテーションおよびマルウェア対策設定ページに表示されるマルウェアのカテゴリに対応します。

次のリストは、さまざまなマルウェアスキャン判定の値と、対応する各マルウェアカテゴリを示しています。

マルウェアスキャン判定の値	マルウェアカテゴリ
-	設定しない
0	Unknown
1	スキャンされていません
2	[タイムアウト（Timeout）]
3	エラー
4	スキャン不能
10	汎用スパイウェア
12	ブラウザヘルパーオブジェクト
13	アドウェア
14	システムモニタ
18	商用システムモニタ
19	ダイヤラ
20	ハイジャッカー

マルウェアスキャン判定の値	マルウェアカテゴリ
21	フィッシングURL
22	トロイの木馬ダウンローダ
23	トロイの木馬
24	トロイの木馬フィッシャー
25	ワーム
26	暗号化されたファイル
27	ウイルス
33	その他のマルウェア
34	PUA
35	中断されました
36	アウトブレイクヒューリスティック
37	既知の悪意のあるファイルと高リスクのファイル

関連情報

- AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド
- セキュアなWebアプライアンスのベストプラクティスの使用
- Vmware 環境で適切な仮想 WSA HA グループ機能を確認する
- アクセスログのパフォーマンスパラメータの設定
- Secure Web ApplianceのHTTPSアクセスログ形式について
- セキュアなWebアプライアンスのログへのアクセス

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。