

# 次世代FW/PAN-OSにおける Youtubeのコンテンツ単位の視聴制限 設定方法

2024年7月

パロアルトネットワークス株式会社

# はじめに

- 本資料では、教育委員会などでニーズの高いYoutube動画のアクセス制御を行う設定方法を説明します。尚、本資料ではPAN-OSの基本的な操作ができる方を想定して作成されておりますので、基本的なPAN-OSの操作方法までの説明は含まれませんが、ご了承ください。
- Youtubeトラフィックの概略の解説と、効率よく動画のアクセス制御を行うためのSSL復号の設定方法も説明します。
- quicプロトコルに対応してるWebブラウザでYoutubeにアクセスした場合、優先的にquicプロトコルが利用されるため制御が不可能です。従いまして、quicプロトコルを禁止するポリシーが必須となります。
- また、iPhoneやAndroidなどのYoutubeのネイティブアプリケーションについてはYoutube動画のアクセス方法が異なるため、本資料の設定では制御できません。スマートデバイスでもWebブラウザベースでの動画視聴に関しては制御可能です。
- 尚、Youtubeのアクセスに関しての仕様が変更された場合、本資料で紹介している設定方法では制御できなくなる可能性があります。ご容赦ください。
- Prisma Accessの場合、本資料の設定内容と同等のポリシーを設定していただくことで制御可能です。

## 想定シーン

- 本資料で紹介する設定では、Youtube動画のコンテンツID単位での視聴を許可する方法です。許可した動画コンテンツ以外は視聴できません。
- Youtubeのホームページの参照もできませんので、Google検索などでYoutube動画を検索し、動画を視聴する操作を想定しています。利用者のホームページなどで動画コンテンツへのリンクからの視聴も可能です。
- Youtubeの動画視聴時に画面右側に推奨動画のサムネイルが表示されますが、クリックしても動画の視聴はできません。また、Youtubeのページでの検索もできません。

# Youtube動画のアクセス制御に必要なトラフィックのみSSL復号

Youtube動画の視聴をWebブラウザで行う場合、複数のDNSドメインへアクセスしている。アクセス制御に必要なSSL通信のみをSSL復号対象とし、実際の動画コンテンツのSSL通信はSSL復号処理から除外することで、SSL復号対象の通信を減らす。

## すべての通信はSSL

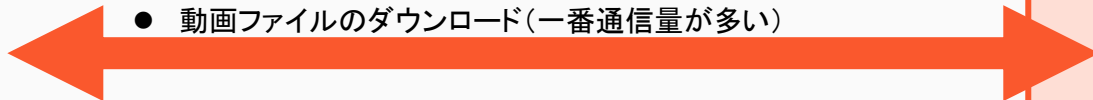


- Youtubeホームページ、動画アクセスに関する通信全般 (※SSL復号対象)



www.youtube.com

- 動画ファイルのダウンロード(一番通信量が多い)



\*.googlevideo.com

- サムネイルやリンク情報など (※SSL復号対象)



\*.ytimg.com

## Youtube動画 主な利用ドメイン

# PAシリーズでのYoutube動画の コンテンツ単位でのアクセス制限 設定方法

※Prisma AccessのStrata Cloud Manager(SCM)はGUIが異なりますが、同等の設定を行うことでYoutubeの動画アクセスの制御可能です。

# Youtube動画アクセス制御のためのSSL復号設定

## 1. SSL復号に利用するルート証明書の設定

SSL復号で利用する証明局。アルゴリズムがRSAとECDSAの2つを作成。これらの証明書をエクスポートし、クライアントに信頼できる証明機関としてインポートしてください。

名前	サブジェクト	発行者	CA	キー	有効期限	状態	アルゴリズム	用途
RootCA_PA-VM	CN = RootCA_PA-VM	CN = RootCA_PA-VM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 9 07:54:08 2023 GMT	有効	RSA	フォワードプロキシ用の信頼された証明書
RootCA_PA-VM_ECDSA	CN = RootCA_PA-VM_ECDSA	CN = RootCA_PA-VM_ECDSA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Dec 9 01:19:00 2023 GMT	有効	Elliptic Curve DSA	フォワードプロキシ用の信頼された証明書
untrustCA	CN = untrustCA	CN = untrustCA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Dec 9 01:19:16 2023 GMT	有効	RSA	フォワードプロキシ用の信頼されない証明書

実際の通信先のサーバー証明書が信用できない場合に利用する証明局。クライアントには絶対にインポートしないでください。

証明書の生成

証明書タイプ  ローカル  SCEP

証明書名 RootCA\_PA-VM\_ECDSA

共通名 RootCA\_PA-VM\_ECDSA

署名者

認証局

秘密鍵のエクスポートをブロック

OCSP レスポンド

暗号設定

アルゴリズム Elliptic Curve DSA

ビット数 256

ダイジェスト sha256

有効期限 (日) 365

証明書生成時に、RSAもしくはECDSAのアルゴリズムを選択

証明書情報

名前 RootCA\_PA-VM

サブジェクト /CN=RootCA\_PA-VM

発行者 /CN=RootCA\_PA-VM

発効日時 Aug 9 07:54:08 2022 GMT

有効期限 Aug 9 07:54:08 2023 GMT

アルゴリズム RSA

認証局

フォワードプロキシ用の信頼された証明書

フォワードプロキシ用の信頼されない証明書

信頼されたルート CA

ここをチェックされた証明書がSSL復号時に利用されます。RSAとECDSAの両方にチェックしてください。

# Youtube動画アクセス制御のためのSSL復号設定

## 2. Youtube動画制御のためのSSL復号設定イメージ

The screenshot shows the Palo Alto VM console interface. The 'POLICIES' tab is active, displaying a table with one policy: 'Decrypt Youtube traffic'. The policy is configured with 'L3-Trust' as the source zone and 'L3-Untrust' as the destination zone. The 'URL カテゴリ' (URL Category) is set to 'SSL-Decrypt-Domain', and the '復号プロファイル' (Decryption Profile) is set to 'TLS1.3'. The 'サービス' (Service) is 'service-https', and the 'アクション' (Action) is 'decrypt'.

名前	送信元				宛先			URL カテゴリ	サービス	アクション	タイプ	復号プロファイル
	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス	デバイス					
1 Decrypt Youtube traffic	L3-Trust	any	any	any	L3-Untrust	any	any	SSL-Decrypt-Domain	service-https	decrypt	ssl-forward-proxy	TLS1.3

The 'カスタム URL カテゴリ' (Custom URL Category) dialog is shown. The name is 'SSL-Decrypt-Domain' and the type is 'URL List'. Below, a search bar shows '2 個の項目' (2 items) with a list of domains: 'www.youtube.com' and '\*.yimg.com'. A red box highlights the domains with the text: 'Youtube動画の視聴制御するための最小限の設定' (Minimum settings for controlling YouTube video viewing).

カスタム URL カテゴリ

名前: SSL-Decrypt-Domain

内容:

タイプ: URL List

以下の URL、ドメイン、またはホスト名のいずれかに一致

2 個の項目

- サイト
- www.youtube.com
- \*.yimg.com

YouTube動画の視聴制御するための最小限の設定

1 行あたり 1 つのエントリを入力します。各エントリはフォームである可能性があります。www.example.com または次のようなワイルドカードが含まれている可能性があります。www.\*.com。

To ensure an exact entry match, use a forward slash (/) at the end of your entry. Example: xyz.com/ matches only xyz.com. For more info, see URL Category Exceptions

OK キャンセル

The '復号プロファイル' (Decryption Profile) dialog is shown. The name is 'TLS1.3'. Under 'SSL 復号化' (SSL Decryption), '復号化なし' (No Decryption) and 'SSH プロキシ' (SSH Proxy) are selected. Under 'SSL フォワードプロキシ' (SSL Forward Proxy), 'SSL インバウンドインスペクション' (SSL Inbound Inspection) and 'SSL プロトコル設定' (SSL Protocol Settings) are selected. Under 'プロトコルバージョン' (Protocol Version), '最小バージョン' (Minimum Version) is 'TLSv1.0' and '最大バージョン' (Maximum Version) is 'TLSv1.3'. A red box highlights the '最大バージョン' (Maximum Version) field with the text: 'TLSv1.3を選択した復号プロファイルを作成し、SSL復号ポリシーに適用してください。' (Create a decryption profile with TLSv1.3 selected and apply it to the SSL decryption policy).

復号プロファイル

名前: TLS1.3

SSL 復号化 | 復号化なし | SSH プロキシ

SSL フォワードプロキシ | SSL インバウンドインスペクション | SSL プロトコル設定

プロトコルバージョン

最小バージョン: TLSv1.0

最大バージョン: TLSv1.3

TLSv1.3を選択した復号プロファイルを作成し、SSL復号ポリシーに適用してください。

鍵交換アルゴリズム

- RSA
- DHE
- ECDHE

暗号化アルゴリズム

- トリプル DES 暗号化
- RC4
- AES128-CBC
- AES256-CBC
- AES128-GCM
- AES256-GCM
- CHACHA20-POLY1305

認証アルゴリズム

- MD5
- SHA1
- SHA256
- SHA384

注: サポートされていないキーやプロトコルは、セッション確立が 12 時間キャッシュされます。このため、同じホストとサーバー間の以前のセッションは許可されません。これらのセッションをブロックするには、チェックボックスをオフにしてください。

OK キャンセル

# Youtubeのトラフィック概要/SSL復号を行い制御を行うURL

- **www.youtube.com**

- Youtube動画のアクセス制御のために制御が必要なURL

- www.youtube.com/watch?v={コンテンツID}
- www.youtube.com/user/{ユーザ名}
- www.youtube.com/channel/{チャンネル名}
- www.youtube.com/results

動画コンテンツの視聴時のURL

ユーザホームページのURL

チャンネルホームページのURL

Youtubeページでの検索時のURL

- **\*.ytimg.com**

- Youtube動画のアクセス制御のために制御が必要なURL



# 動画コンテンツIDでのアクセス制御の設定方法

- 制御方法

- Youtube動画の視聴開始時に、下記URLへアクセスを行うため、許可したい動画のコンテンツIDの許可ルールで制御

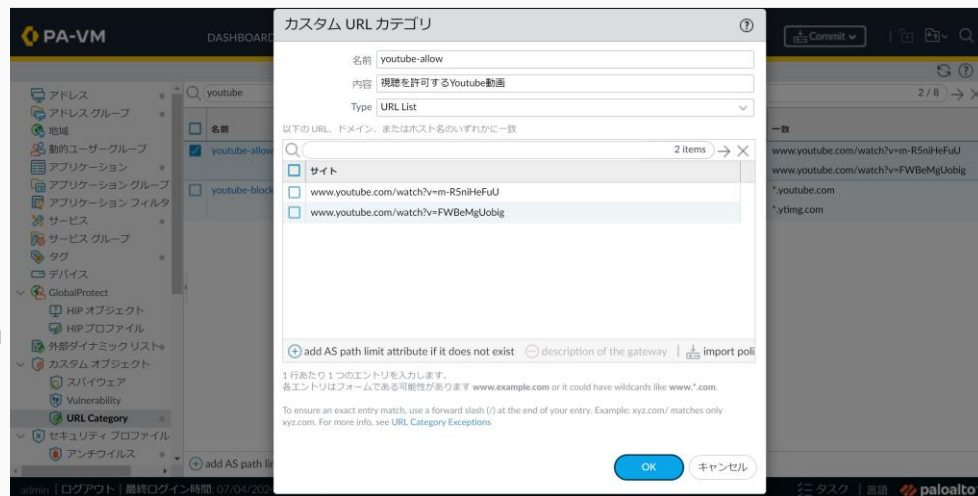
[www.youtube.com/watch?v={コンテンツID}](http://www.youtube.com/watch?v={コンテンツID})

- PAシリーズの設定方法

1. 許可する動画用のカスタムURLカテゴリを登録する
2. 制御用セキュリティポリシールールを追加
  - ① カスタムURLカテゴリへのアクセスを許可するセキュリティポリシールールを追加

# 【tips】 カスタムURLフィルタリングについての解説

- カスタムURLカテゴリとは、PAN-DBで提供されるカテゴリ以外に独自で追加できるカテゴリです
- 以下のいずれかの方法で設定可能
  - 外部ダイナミックリスト(EDL)により外部のWebサーバーから自動的に読み込み（次頁にて解説）
  - PAシリーズの管理GUIで設定
  - XML-APIを通じて設定
- URL情報の文字列にアスタリスク(\*)が利用可能
  - \*.youtube.com など
- カスタムURLカテゴリは下記などのポリシー設定で利用可能
  - URLフィルタリングのカテゴリ
  - ファイアウォールポリシールールでのURLカテゴリ
  - SSL復号対象ポリシーでのURLカテゴリ
- URL情報のインポートやエクスポートも可能



# Youtube動画アクセス制御のカスタムURLオブジェクト設定例

The screenshot shows the Palo Alto VM console interface. The top navigation bar includes 'PA-VM', 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. A 'Commit' button is visible on the right. The left sidebar shows a tree view of configuration categories, with 'URL Category' selected. The main area displays a table of custom URL objects for the search term 'youtube'.

名前	LOCATION FOR PORTAL/GATEWAY WITH MAX LENGTH 100	TYPE	URL List
<input checked="" type="checkbox"/> youtube-allow		URL List	www.youtube.com/watch?v=m-R5niHeFuU www.youtube.com/watch?v=FWBeMgUobig
<input type="checkbox"/> youtube-block		URL List	*.youtube.com *.yimg.com

視聴を許可するYoutube動画のURL

Youtube制御のためのSSL復号対象URL

add AS path limit attribute if it does not exist description of the gateway コピー PDF/CSV

# Youtube動画アクセス制御のセキュリティルール設定例

PA-VM DASHBOARD ACC MONITOR **POLICIES** OBJECTS NETWORK DEVICE Commit

セキュリティ 5 items

名前	ZONE	アドレス	USER	デバイス	ZONE	アドレス	デバイス	アプリケーション	サービス	URL CATEGORY	アクション	プロファイル
1 block quic	L3-trust	any	any	any	L3-untrust	any	any	quic	application-d...	any	拒否	none
2 permit youtube	L3-trust	any	any	any	L3-untrust	any	any	any	any	youtube-allow	許可	
3 permit All	L3-trust	any	any	any	L3-untrust	any	any	any	any	any	許可	
4 intrazone-default	any	any	any	any	(intrazone)	any	any	any	any	any	許可	none
5 interzone-default	any	any	any	any	any	any	any	any	any	any	許可	none

quicプロトコルをBlock ※SSLへ自動的にFallback

URLカテゴリに「youtube-allow」を指定し、指定した動画コンテンツのみアクセス許可するためのルール

インターネットへのアクセス許可ルールに、許可したYoutube動画以外のYoutube関連の通信をBlockするため、URLフィルタリングのプロファイルで「youtube-block」のカスタムカテゴリに対してブロックアクションを指定したルール

「permit All」のルールに適用するURLフィルタリングプロファイルの設定イメージ 「youtube-block」のカスタムカテゴリのサイトアクセスを「block」指定

URL Filtering Profile

名前 youtube-control

内容

カテゴリ URL Filtering Settings | User Credential Detection | HTTPヘッダー検査 | インライン分類

カテゴリ	サイト アクセス	USER CREDENTIAL SUBMISSION
M365-Addition *	alert	allow
Permit-Category *	alert	allow
WhiteList *	alert	allow
youtube-allow *	alert	allow
youtube-block *	block	block
zoom	alert	allow

外部動的 URL リスト

M365 URL \*

8 hex digits: 00000000 to FFFFFFFF

URL カテゴリをチェック

OK キャンセル

THANK YOU