



Cloudflare連続勉強会 #6

# Cloudflare Zero Trustの紹介 (前編)

## - 導入準備編

カスタマーサクセス 部長 八塚 俊次郎

カスタマーソリューションエンジニア 西原 誠

**Cloudflare Japan**

東京都中央区京橋 2-2-1京橋エドグラン 26階

[www.cloudflare.com/ja-jp/](https://www.cloudflare.com/ja-jp/)

# Agenda

- 1 はじめに
- 2 Cloudflare Zero Trust導入の流れ
- 3 Cloudflareダッシュボードの初期設定
- 4 WARPクライアントのインストール
- 5 Q&A

# はじめに

## 1. はじめに

2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. Q&A

## 目的

本WebinarはCloudflareのEnterpriseプランのご契約をお持ちのお客様向けにCloudflare製品の機能及び設定概要を紹介することで、製品をよりよくご活用いただくことを主目的とします。

時間配分	内容
50分	メインセッション
10分	Q&A

## 注意事項

本Webinarご参加に当たっての注意事項を以下記載いたします。

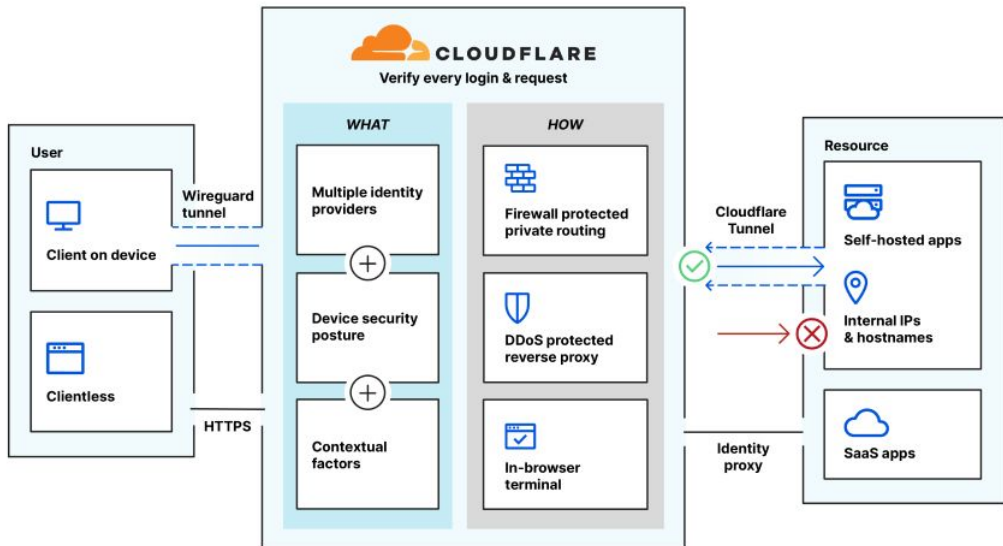
- 本Webinarはレコーディングを行い、後日、弊社Webinarサイトにご登録のお客様は再視聴できるようにいたします。各セッションの最後にはブラウザ上のテキストボックスからご質問を受付けますが、起票者のお名前は伏せてのQ&A対応となります。
- お時間の制約から、Webinar中に頂いたすべてのご質問にお答えできないかもしれません。最善は尽くさせていただければと考えておりますが、その旨、ご了承ください。
- 本セッションで用いるスライドはセッション終了後、当Webinarのご登録ページからPDF形式でダウンロード頂けます。

# Cloudflare Zero Trust導入の流れ

1. はじめに
- 2. Cloudflare Zero Trust導入の流れ**
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. Q&A

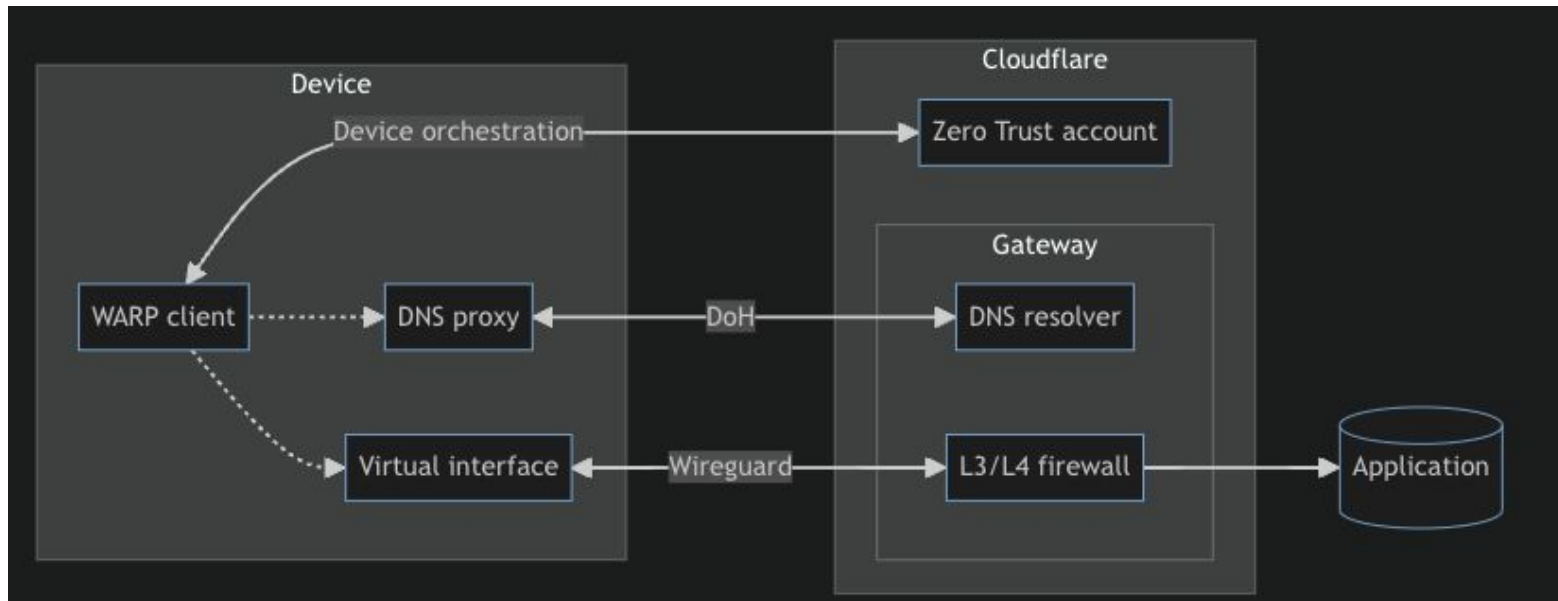
## Cloudflare Zero Trust導入の流れ

Cloudflare Zero Trust導入の流れとしては[Roadmap to Zero Trust](#)をご参照いただけます。



参照) [Cloudflare Zero Trust Network Accessの鳥瞰図](#)

## Cloudflare Zero Trust導入の流れ - WARPのアーキテクチャ



参照) [Cloudflare Docs - WARP architecture](#)  
[Cloudflare Docs - WARP with firewall](#)

## Cloudflare Zero Trust導入の流れ - 導入フェーズ定義例

### Phase.1)

- ダッシュボードの初期設定
- ZTNAの設定
- WARPの部分展開 (一部ユーザー間での試験導入)

### Phase.2)

- SWGの基本設定 (DNS / Networkポリシーの適用)
- WARPの全社展開

### Phase.3)

- SWGの追加設定 (HTTPポリシーの適用※)
- CASB / DLP / RBIの設定

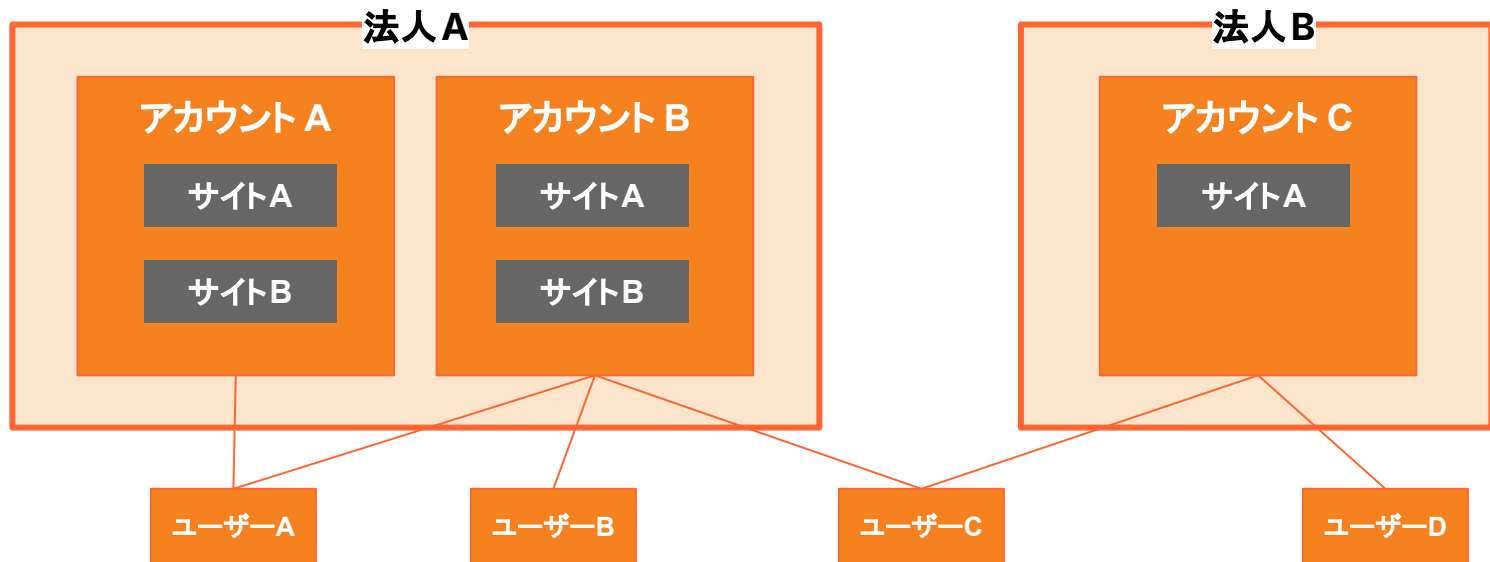
※ SWGで、HTTPSの通信にポリシーを適用させる場合には[TLS Decryption](#)を有効化いただく必要がありますが、それに伴い特定のサイトアクセスにおいて、証明書エラー (526エラー等)の発生可能性があります。  
個別に後述のDo Not InspectポリシーもしくはSplit Tunnelの設定が必要となりますため、ご注意ください。

[参照\) Cloudflare Docs - TLS Decryption](#)

## Cloudflare Zero Trust導入の流れ - 複数アカウントの管理

Enterprise Planご利用のお客様に限っては、検証等を目的として、複数のアカウントに分割した管理も可能となります。

※前提として、ご契約数量（シート数）を分けた管理が必要となります



# Cloudflareダッシュボードの初期設定

1. はじめに
2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. Q&A

## Cloudflareダッシュボードの初期設定

1. チーム名の設定
2. 認証方法の設定
3. ダッシュボードのSSO登録 (オプション)
4. Logpush設定


## チーム名の設定


1. [Cloudflareダッシュボード](#)のアカウントレベルメニューから、Zero Trustをクリック
2. Team名を指定
3. サブスクリプションプランおよびお支払い方法を設定

※Freeプランを選択の際にも、お支払い方法の設定が必要となりますが、実際の引き落としはなされませんので、ご安心ください。

参照) [Cloudflare Docs - Start from the Cloudflare Dashboard](#)

## チーム名の設定 - 初回設定画面

 Cloudflare Zero Trust Cancel and exit



Choose your team name

Your team name creates a unique domain for your Cloudflare Zero Trust account.  
Don't worry – you can change this later.

.cloudflareaccess.com

Next

## Cloudflareダッシュボードの初期設定

1. チーム名の設定
2. **認証方法の設定**
3. ダッシュボードのSSO登録 (オプション)
4. Logpush設定

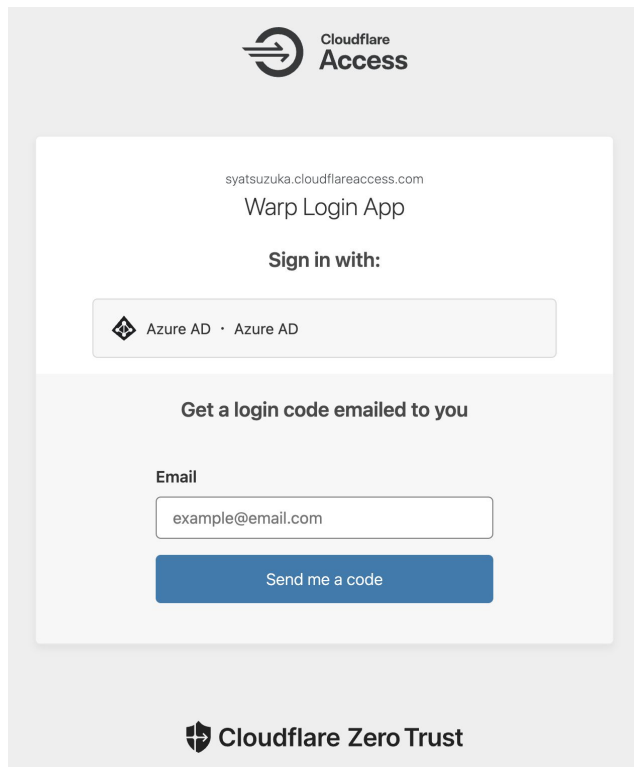
## 認証方法の設定

Cloudflare Zero Trustでは大きく、ご登録されたIdPの設定に基づき、以下の2つのレベルでユーザー認証が行われます。

- **Cloudflare Access (ZTNA)における認証イベント**  
App LauncherおよびAccessの機能として登録した"Application"へのアクセス時に行われる認証。  
詳細は後編の「ZTNAの設定」で紹介。
- **Cloudflare Secure Web Gatewayにおける認証イベント (WARPにおけるログイン認証)**  
WARPの初回ログイン時に行われる認証  
詳細は後編の「SWGの設定」で紹介。

※こちらの認証結果を元に Access, Secure Web Gateway 双方のご利用シート数が算出されます。

参照) [Cloudflare Docs - Seat Management](#)



Cloudflare Access

syatsuzuka.cloudflareaccess.com

Warp Login App

Sign in with:

Azure AD • Azure AD

Get a login code emailed to you

Email

example@email.com

Send me a code

Cloudflare Zero Trust


## 認証方法の設定

認証方法としては、デフォルトでOne-time PIN login (OTP)を選択いただけますが、ここでは一般的にMicrosoft Entra ID (旧称 Azure Active Directory)の設定の流れを例として紹介させていただきます。

1. IdPのご用意 (例: Microsoft Entra ID)
2. [Zero Trustダッシュボード](#)から、Settings > Authenticationをクリック
3. Login methodsカードから、Add Newをクリック
4. IdPを選択 (複数選択可能)
5. 各種項目を入力し、Saveボタンをクリック
6. Testボタンをクリックし、接続が成功することを確認

参照) [Cloudflare Docs - SSO Management](#)

# 認証方法の設定 - Microsoft Entra ID



Support ▼

Back to add a login method

## Add Azure AD

**Name** (Required)  
Unique name to identify this identity provider in the login page.

**Application ID** (Required)

**Application secret** (Required)

**Directory ID** (Required)

**Azure cloud**

Default ▼

**Proof Key for Code Exchange (PKCE)**

Disabled ☐

PKCE is an extension to the Authorization Code flow that prevents Cross-Site Request Forgery (CSRF) and authorization code injection attacks. Only check this if your identity provider supports PKCE for confidential clients.

**Support groups**

Disabled ☐

Allow Zero Trust to collect group information about your users. The feature requires the Read All Groups permission in your list of Azure AD application permissions.

**Enable SCIM** (Beta)

Disabled ☐

System for Cross-domain Identity Management (SCIM) allows for automatic synchronization of users and groups between your identity provider and Access.

Save

## Instructions for setup

### Microsoft Azure AD®

You can integrate Microsoft Azure AD® (Active Directory) with Cloudflare Zero Trust and build policies based on user identity and group membership. Users will authenticate to Zero Trust using their Azure AD credentials.

#### Set up Azure AD as an identity provider

##### 1. Obtain Azure AD settings

The following Azure AD values are required to set up the integration:

- Application (client) ID
- Directory (tenant) ID
- Client secret

To retrieve those values:

1. Log in to the [Azure dashboard](#).
2. Navigate to **All services** > **Azure Active Directory**.
3. In the Azure Active Directory menu, go to **Enterprise applications**.
4. Select **New application** > **Create your own application**.
5. Name your application.
6. Select **Register an application to integration with Azure AD (App you're developing)** and then select **Create**.
7. Under **Redirect URI**, select the Web platform and enter the following URL:

```
https://<your-team-name>.cloudflareaccess.com/cdn-cg/access/callback
```

You can find your [team name](#) in Zero Trust under **Settings** > **General**.

Microsoft Azure

Home > 26562 | App registrations >

### Register an application

The user-facing display name for this application (this can be changed later).

Cloudflare Access

Supported account types

Who can use this application or access this API?

Microsoft Entra ID側操作は、こちらに記載の手順をご参照いただけますが、以下 Microsoft社のページからも同様の内容をご参照いただけます。

## 認証方法の設定 - Microsoft Entra ID

入力項目	設定内容	設定例
Name	SSOのLoginページで表示する名称	“Microsoft Entra ID”
Application ID	(Microsoft Entra IDから取得)	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Application Secret	(Microsoft Entra IDから取得)	
Directory ID	(Microsoft Entra IDから取得)	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Azure Cloud	基本Defaultを選択	“Default”
Proof Key for Code Exchange	CSRF (Cross Site Request Forgery)および認証コードInjectionの回避のためのオプション	“Enabled”   “Disabled”
Support groups	Zero Trustユーザーにおけるグループリスト情報の取得	“Enabled”   “Disabled”
Enable SCIM	SCIM (System for Cross Domain Identity Management)の利用	“Enabled”   “Disabled”

## 認証方法の設定 - Microsoft Entra ID を使用した SCIM 同期

“クロスドメイン ID 管理システム (SCIM) とは、ID ドメインと IT システムの間で行うユーザー ID 情報の交換を自動化するためのオープンな標準プロトコルです。SCIM を使用すれば、人材管理 (HCM) システムに追加された従業員のアカウントを、確実に Microsoft Entra ID または Windows Server Active Directory によって自動的に作成することができます。ユーザーの属性およびプロファイルは 2 つのシステム間で同期されているので、ユーザーの状態または役割の変更に基づいてユーザーの更新および削除が行われます。”

参照) [Microsoft Entra ID を使用した SCIM 同期](#)

## 認証方法の設定 - Microsoft Entra ID



Your connection works!

Below is the user identity we will use to check against your rules.

```
{
  "name": "Yatsuzuka Shunjiro",
  "email": [REDACTED],
  "amr": [
    "pwd",
    "mfa"
  ]
}
```

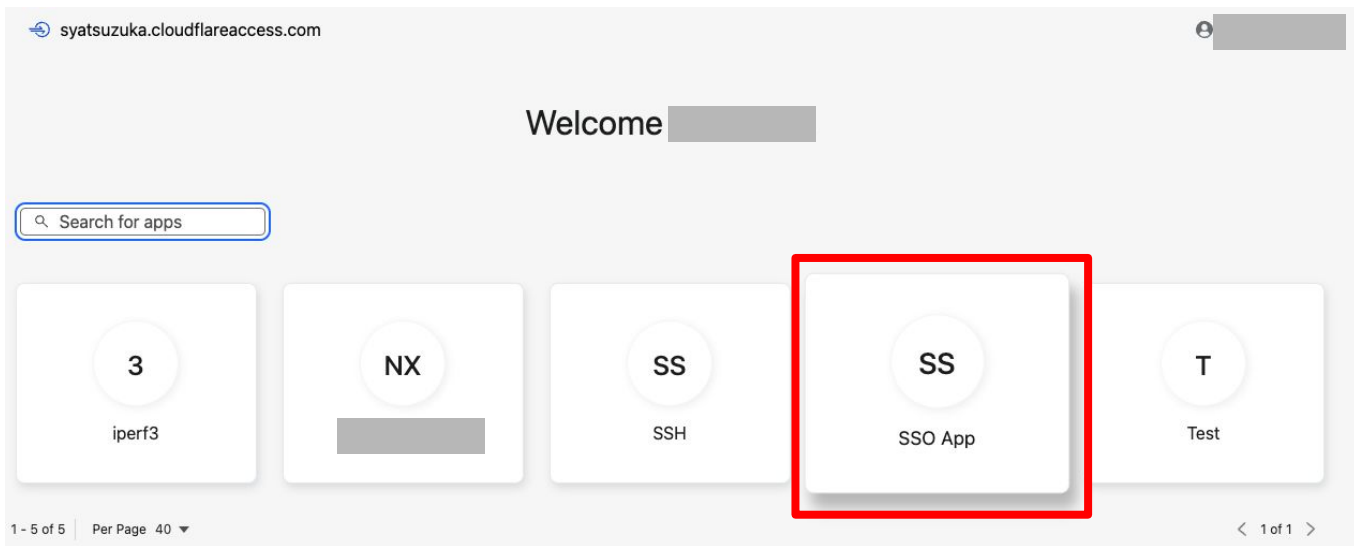
## Cloudflareダッシュボードの初期設定

1. チーム名の設定
2. 認証方法の設定
3. **ダッシュボードの SSO登録 (オプション)**
4. Logpush設定

## ダッシュボードのSSO登録

Cloudflare Dashboardへの認証に、Cloudflare Zero Trustで指定したSSOを経由させることがオプションとして可能となります。

以下はDashboardへのアクセスにZero TrustのSSOを適用の上、Zero TrustのLauncherにアプリケーション登録したイメージです。



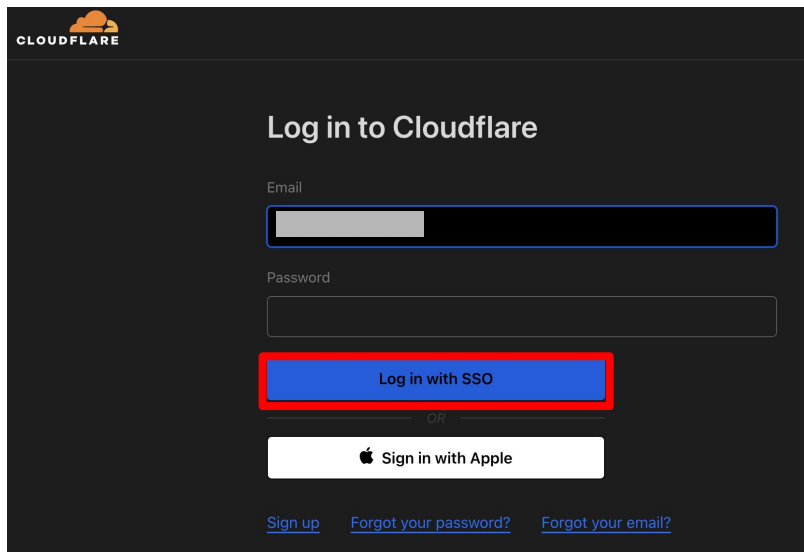
## ダッシュボードのSSO登録

以下にCloudflare DashboardにSSOを適用させる流れを記します。

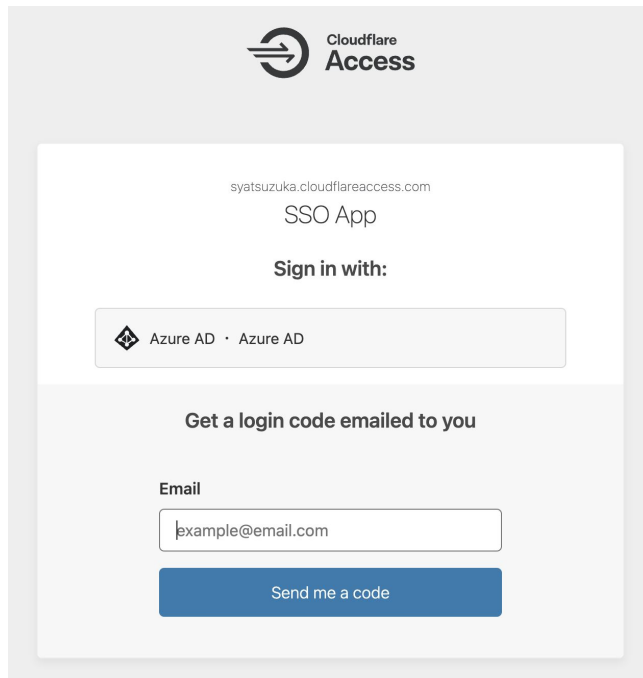
1. 担当のCSMへ、SSO Connectorの作成依頼 (SSOに用いるメールアドレスのドメインをご連絡)
2. [Zero Trustダッシュボード](#)から、Settings > Authenticationをクリック
3. Cloudflare dashboard SSOカードで該当するドメインを有効化
4. 管理画面をオープンしながら、別のブラウザウィンドウ(もしくは、Chromeをご利用の場合には、Incognitoなど)を利用の上、SSOの動作確認を実施
5. 動作確認ができれば、終了。動作不良が確認された場合には、SSOカードを無効化の上、調査。(もし管理画面をクローズし、SSOの無効化を行えない場合には、弊社サポートもしくは、担当CSMへ無効化を依頼。

参照) [Cloudflare Docs - Setup Cloudflare dashboard SSO](#)

## ダッシュボードのSSO登録



The image shows the Cloudflare dashboard login page. It has a dark background with the Cloudflare logo at the top left. The main heading is "Log in to Cloudflare". Below it are input fields for "Email" and "Password". A blue button labeled "Log in with SSO" is highlighted with a red rectangle. Below this is a white button with the Apple logo and "Sign in with Apple". At the bottom, there are links for "Sign up", "Forgot your password?", and "Forgot your email?".



The image shows the Cloudflare Access SSO app screen. It has a light gray background with the Cloudflare Access logo at the top. The URL "syatsuzuka.cloudflareaccess.com" is displayed. Below it is the text "SSO App". The heading "Sign in with:" is followed by a button labeled "Azure AD · Azure AD". Below this is a section titled "Get a login code emailed to you". It includes an "Email" input field with "example@email.com" and a blue button labeled "Send me a code".

SSOにより、都度パスワードを入力することなく、Loginへ進むことが可能となります。

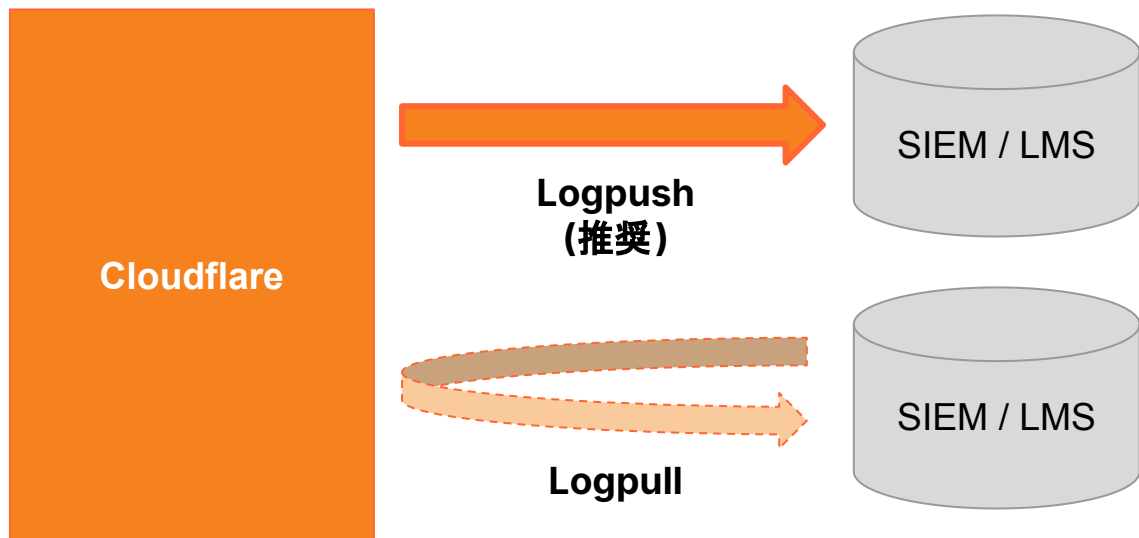
まだ、セッションが確立されていない場合には、初回認証画面へ

## Cloudflareダッシュボードの初期設定

1. チーム名の設定
2. 認証方法の設定
3. ダッシュボードのSSO登録 (オプション)
4. **Logpush設定**

## Logpush設定

Cloudflareでは各種ログ情報を「データセット」という形で外部の SIEM (Security Information and Event Management)もしくはLMS (Log Management System)へ転送することが可能です。  
転送の方法としては大きく、Logpushジョブによる転送とLogpullによる転送(取得)が挙げられます。



## Logpush設定

以下にLogpushによるログ連携の流れについて、紹介させていただきます。

1. [Zero Trustダッシュボード](#)から、Logs > Logpushをクリック
2. Connect a Serviceボタンをクリック
3. 入力項目を設定し、Nextボタンをクリック
4. ログ情報を格納するStorage Serviceを選択

※APIをご利用いただくことで、よりフレキシブルな設定が可能となります。

参照) [Cloudflare Logpush Integration](#)

## Logpush設定

データセット	概要
Gateway DNS	Cloudflare Gatewayで検出されたDNS Query情報
Gateway HTTP	Cloudflare Gatewayで検出されたHTTPリクエスト
Gateway Network	Cloudflare Gatewayで検出されたネットワークパケット情報
Audit Logs	Cloudflare Accessを通した認証イベント情報
Access Requests	Cloudflare Accessで保護されたサイトへのHTTPリクエスト
CASB findings	Cloudflare CASBで確認されたセキュリティイシュー
Devise Posture	WARPクライアントによるDevise Postureステータス情報
Session Logs	Cloudflare GatewayでProxyされたネットワークセッションログ

参照) [Cloudflare Docs - Zero Trust datasets](#)

# Logpush設定

## Logs

[Logs documentation](#)

### Logpush - Account-scoped datasets

Have logs of Cloudflare traffic uploaded to a destination of your choice. Logs are pushed to your destination in batches as soon as possible.

[Add Logpush job](#)

Service	Data set	Path	Status	
R2 Object Storage		cloudflare-zt-sessionlogs	Pushing	<input checked="" type="checkbox"/> <a href="#">Edit</a>   <a href="#">Delete</a>
R2 Object Storage	Access requests	cloudflare-zt-accessrequests	Pushing	<input checked="" type="checkbox"/> <a href="#">Edit</a>   <a href="#">Delete</a>
R2 Object Storage	Gateway network	cloudflare-zt-gatewaynetwork	Pushing	<input checked="" type="checkbox"/> <a href="#">Edit</a>   <a href="#">Delete</a>
R2 Object Storage	Gateway DNS	cloudflare-zt-gatewaydns	Pushing	<input checked="" type="checkbox"/> <a href="#">Edit</a>   <a href="#">Delete</a>
R2 Object Storage	Gateway HTTP	cloudflare-zt-gatewayhttps	Pushing	<input checked="" type="checkbox"/> <a href="#">Edit</a>   <a href="#">Delete</a>
R2 Object Storage	Audit logs	cloudflare-audit-log	Pushing	<input checked="" type="checkbox"/> <a href="#">Edit</a>   <a href="#">Delete</a>

[Help](#)

## Logpush設定 - R2にログを格納した際のクエリー実行例

```
$ curl -s -g -X GET  
"https://api.cloudflare.com/client/v4/accounts/${CF_ACCOUNT_ID}/  
logs/retrieve?start=2023-05-04T16:00:00Z&end=2023-05-06T16:0  
0:00Z&bucket=${CF_LOG}&prefix={DATE}" \  
-H "X-Auth-Email: ${CF_EMAIL}" \  
-H "X-Auth-Key: ${CF_APIKEY}" \  
-H "R2-Access-Key-Id: ${R2_ACCESS_KEY_ID}" \  
-H "R2-Secret-Access-Key: ${R2_SECRET_ACCESS_KEY}" | jq .
```

参照) [Cloudflare Docs - Logs Engine](#)

## Logpush設定 - R2にログを格納した際のクエリー実行例

Cloudflareでは各種ログはJSONフォーマットで出力されます。

右図の例は、DLPで検知され、指定されたFirewall Policyでブロックされたログの例となります。

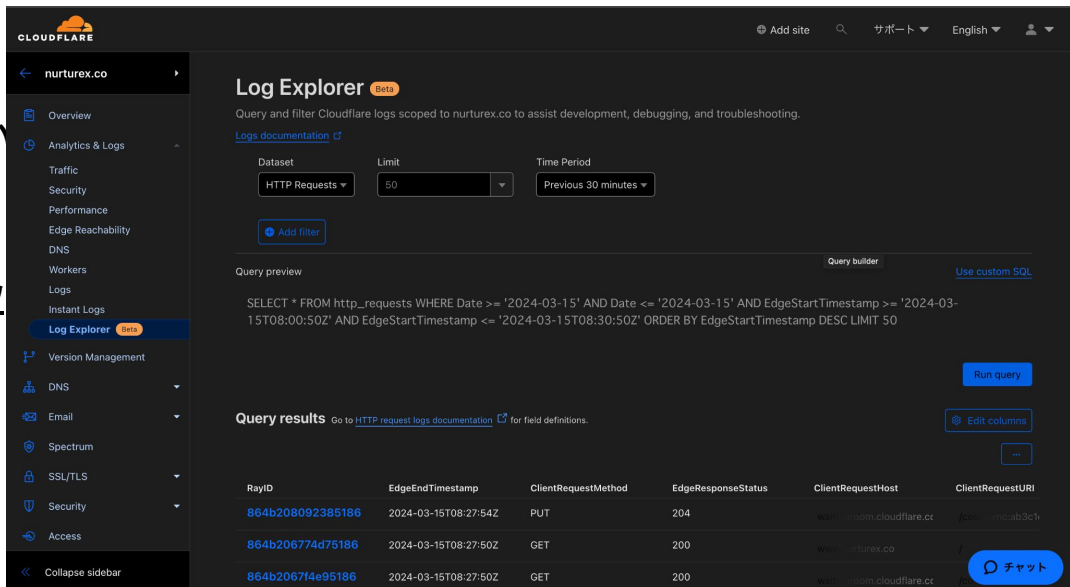
```
{
  "Datetime": "2024-04-05T00:21:44Z",
  "AccountID": "<Account ID>",
  "Action": "block",
  "BlockedFileHash": "",
  "BlockedFileName": "<unknown file name>",
  "BlockedFileReason": "unknown",
  "BlockedFileSize": 0,
  "BlockedFileType": "",
  "DestinationIP": "2404:6800:4004:828::200e",
  "DestinationPort": 443,
  "DeviceID": "<Device ID>",
  "DeviceName": "WindowsPC",
  "DownloadedFileNames": [],
  "Email": "<Email Address>",
  "FileInfo": {
    "files": [
      {
        "direction": "upload",
        "file_name": "<unknown file name>",
        "file_hash":
"02e131789ea580261172ba96490e40f5e0e78fc6d7d5fa93152f7bbaad4b16d",
        "file_size": 23367,
        "content_type": "application/vnd.chrome.ukm",
        "action": "block"
      }
    ]
  },
  "HTTPHost": "clients4.google.com",
  "HTTPMethod": "POST",
  "HTTPStatusCode": 302,
  "HTTPVersion": "HTTP/2",
  "Isolated": false,
  "PolicyID": "afd4ad33-a437-44f8-8ebc-a0cfb40f1cbe",
  "PolicyName": "Test - DLP",
  "Referer": "",
  "RequestID": "1f4d3b16ff00001f0f0824f400000001",
  "SourceIP": "60.118.112.139",
  "SourceInternalIP": "",
  "SourcePort": 51260,
  "URL": "https://clients4.google.com/ukm",
  "UntrustedCertificateAction": "none",
  "UploadedFileNames": [],
  "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36",
  "UserID": "<User ID>"
}
```

## Logpush設定 - Log Explorer (beta)

Log Explorer (beta)を有効化することで、一部ログをR2で管理の上、Cloudflareのダッシュボード上でご確認いただく事が可能となりました。

※今日においてはZero Trustのデータセットは対応されておりませんが、今後対応データセットも増えていくことが期待されます。

参照) [Cloudflare Docs - Log Explorer \(beta\)](#)



RayID	EdgeEndTimestamp	ClientRequestMethod	EdgeResponseStatus	ClientRequestHost	ClientRequestURI
864b208092385186	2024-03-15T08:27:54Z	PUT	204	192.168.1.1.cloudflare.cf	/api/v1/accounts/3c1k
864b206774d75186	2024-03-15T08:27:50Z	GET	200	192.168.1.1.cloudflare.cf	/api/v1/accounts/3c1k
864b206774e95186	2024-03-15T08:27:50Z	GET	200	192.168.1.1.cloudflare.cf	/api/v1/accounts/3c1k

# WARPクライアントのインストール

1. はじめに
2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. Q&A

## WARPクライアントのインストール

1. **Device Enrollment Permissionの定義**
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. ログの確認
6. その他確認画面

## Device Enrollment Permissionの定義

Device Enrollment Permissionは、WARPのTeamへのアクセスを許可する対象ユーザーを指定する設定です。  
以下に設定の流れを記載いたします。

1. Zero Trustダッシュボードから、Settings > WARP Clientへアクセス
2. Device enrollmentカードから、Manageボタンを選択
3. RulesタブでAccess policies (どのユーザーが彼らのデバイスからZero Trust環境への接続を許すか)を定義
4. Authenticationタブで、ユーザーが利用可能なidentity providersを選択
5. Saveボタンをクリック

参照) [Cloudflare Docs - Device enrollment permissions](#)

# Device Enrollment Permissionの定義

## Device enrollment rules

These rules do not impact permissions for any of the applications behind Access.

Rule name (Required)

Rule action (Required)

Allow

### Include

Selector

Emails ending in

Value

@domain.com

x

[+ Add include](#)

[+ Add require](#)

[+ Add exclude](#)

## Assign a group Showing 1 - 1

Assign a group to your application to enforce a set of predefined rules.

Search

Name

☐

test

Include

# Device Enrollment Permissionの定義

Rules

Authentication

## Identity providers

[Learn more](#)

Accept all available identity providers



Manually select identity providers users can use to connect

[Deselect all](#) [Select all](#)

Azure AD



One-time PIN

## Instant Auth

Skip identity provider selection if only one is configured



## WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. **WARPクライアントのインストール**
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. ログの確認
6. その他確認画面

## WARPクライアントのインストール

WARPクライアントのインストールの流れを以下に記します。

1. カスタムルート証明書をCloudflareへ[アップロード](#) (オプション)
2. Zero Trustダッシュボードから、Settings > WARP Clientへアクセス
3. Install CA to system certificate storeを有効化
4. WARPクライアントを[ダウンロード](#)の上、インストール
5. Zero TrustのTeamへデバイスを[登録](#)  
カスタム証明書がアップロードされていない場合には、デフォルトのCloudflare証明書がインストールされます。
6. インストールされた証明書の[確認](#)

参照) [Cloudflare Docs - Install a certificate using the WARP client](#)

## WARPクライアントのインストール - WARPによる証明書のインストール

HTTPSトラフィックのチェック (TLS Decryption)、Data Loss Prevention、アンチウィルススキャン、Browser Isolationといったセキュリティ機能を利用するには、Cloudflareの証明書設定が必要となります。

デスクトップデバイスにWARPクライアントをインストールする際には、証明書も自動インストールされますが、モバイル端末にWARPクライアントをインストールする際には、手動による証明書のインストールが必要となります。

参照) [Cloudflare Docs - User-side certificates](#)

# WARPクライアントのインストール - サイレントインストールコマンド

以下コマンドでサイレントインストールが可能です(詳細についてはマイクロソフト社 Apple社にお問い合わせください)

## (Windows)

```
PS> msixexec /i "Cloudflare_WARP_Release-x64.msi" /qn ORGANIZATION="your-team-name"  
SUPPORT_URL="http://support.example.com"
```

※ご利用のPC環境によっては、コマンドとしてmsiexecではなく、WARPのMSIファイルを直接呼び出すことでもインストールされるケースも確認されております。なお、ORGANIZATIONおよびSUPPORT\_URLはオプションであり、インストール後に追加設定可能です。

## (Mac)

```
$ sudo installer -pkg <WARP/パッケージファイル> -target /
```

## 参照)

[Cloudflare Docs - Install WARP](#)

[Cloudflare Docs - Manual deployment](#)

## WARPクライアントのインストール - WARPのバージョン管理

2023年11月時点においては、WARPは以下の様なバージョン管理がなされ、一つのブランチで継続メンテナンスされる形が取られ、Long Term Supportに相当するバージョンの管理はございません。

**YYYY.MM.<パッチバージョン>.<リリースタイプ>**

<リリースタイプ>

0: GA

1: αもしくはβバージョン

※ 安定稼働が期待される場合には、MDM等を用いて組織内で所定のバージョンをご利用いただき、その後は動作検証の上で、アップデートを行っていただくことが推奨されます。

参照)

[Cloudflare Docs - Download WARP](#)

[Cloudflare Docs - Managed deployment](#)

## WARPクライアントのインストール - 必要なFirewall設定

WARPをご利用される際には、以下ドキュメントで指定されたポートに対するFirewall設定(穴あけ)が必要となります。

参照) [Cloudflare Docs - WARP with firewall](#)

## WARPクライアントのインストール - レガシーVPNとの併用

レガシーVPNとの併用をご検討の場合には以下設定の元での動作をご確認いただければと思います。

### <VPN側設定>

- サードパーティーVPNにおけるスプリットトンネルの有効化
- サードパーティーVPNにおけるDNS設定の無効化

### <WARP側設定>

- VPNで利用されるプライベートIPをスプリットトンネルで除外
- VPNの接続先ホストをスプリットトンネルで除外
- (オプション) VPNのプライベートDNSで名前解決させたいドメインをLocal Domain Fallbackで指定

参照) [Cloudflare Docs - WARP with legacy VPN](#)

## WARPクライアントのインストール - レガシーVPNとの併用

**Other parameters - optional**

☒ Enable DNS servers

**DNS server 1 IP address**  
The IP address of the DNS server to use. There are no default DNS servers.

**DNS server 2 IP address**  
The IP address of the DNS server to use. There are no default DNS servers.

☒ Enable split-tunnel [Info](#)

サードパーティーVPNのスプリットトンネルの設定イメージ

## WARPクライアントのインストール - WARP to WARP

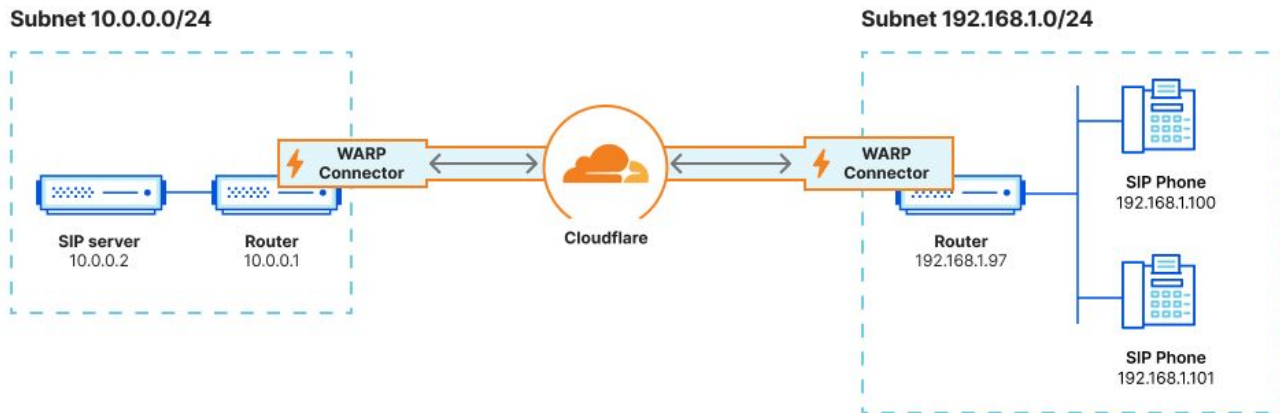
WARP to WARPを用いることで、PC間のPeer-to-Peer接続を確立することが可能となります。



参照) [Cloudflare Docs - Create private networks with WARP-to-WARP](#)

## WARPクライアントのインストール - WARP Connector (Beta)

WARP Connectorを用いることで、cloudflaredなしに、また、個別のPCにWARPをインストールすることなく、複数拠点間の通信が可能となります。  
(ただし、認証にはService Tokenが利用されるため、ユーザーの特定ができません)



参照) [Cloudflare Docs - Set up WARP Connector](#)

## WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. **Zero Trust**インスタンスへのログイン
4. WARPクライアントの詳細設定
5. ログの確認
6. その他確認画面

## Zero Trustインスタンスへのログイン

1. メニューバーから、Cloudflareのロゴマークのアイコンをクリック
  2. 設定アイコンをクリック
  3. Preferences > Accountをクリック
  4. Login with Cloudflare Zero Trustを選択
  5. 登録したTeam名を入力
  6. Teamで登録されている認証ステップを実施
- ご利用のデバイスがチームに登録され、Zero Trustのポリシーが適用されます。

参照) [Cloudflare Docs - Manual deployment](#)

## WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. **WARPクライアントの詳細設定**
5. ログの確認
6. その他確認画面

## WARPクライアントの詳細設定

Settings > WARP ClientのDevice Settingsから、各クライアントに対する詳細設定を行う事が可能です

### Configure settings

#### Captive portal detection

Allow the WARP client to turn off for a set amount of time when a captive portal is detected. This enables users to connect to hotel, airplane, or other WiFi networks.

#### Mode switch

Allow users to manually switch between Gateway with WARP and Gateway with DNS. This enables users to turn off the WARP client when still being

#### Lock WARP switch

Prevent users from turning off the WARP switch and disconnecting the client.

#### Allow device to leave organization

If enabled, users who manually join their device to the organization are allowed to leave the organization.

#### Allow updates

Allow local administrators to receive notifications on available updates for the client, and to initiate the updates.

#### Auto connect

Allow the WARP client to turn on automatically after a specified amount of time.

各端末におけるWARPの解除を禁止する設定  
(試験導入フェーズにおいてはLockを外すことが推奨)

安定稼働のためには自動アップデートをオフにすることを推奨

WARPを解除後、一定時間後に自動で有効化させる設定

Disabled ☐

# WARPクライアントの詳細設定

## Service mode

Choose how you want the WARP Client to be configured.

- ☒ **Gateway with WARP**  
All traffic is encrypted by Gateway. This mode is required if you want to enable HTTP rules, Browser Isolation, Anti-Virus scanning and DLP.
- ☐ **Gateway with DoH**  
Only DNS traffic is encrypted by Gateway. This mode only allows for DNS policies to be enforced.
- ☐ **Proxy mode**  
Gateway only encrypts traffic sent to the localhost proxy. Does not process DNS traffic.

プライベートネットワークにおける名前解決の設定  
(後述のResolver Policyでも類似の設定が可能となります)

## Local Domain Fallback

Configure Cloudflare Zero Trust to ignore DNS requests to a given list of domains. These DNS requests will be passed back to other DNS servers configured on existing network interfaces on the device.

[Manage](#)

## Split Tunnels

Configure Cloudflare Zero Trust to exclude or include traffic to a given set of IP addresses or domains. Any traffic directed to an excluded destination will be handled by the local machine. Use wildcards to match against multiple subdomains at the same time.

- ☐ Include IPs and domains
- ☒ Exclude IPs and domains

[Manage](#)

## Directly route Office 365 traffic

Exclude Office 365 traffic from going through Cloudflare Zero Trust. To enable, Split Tunnels must be set to exclude IPs and domains. Office 365 entries are automatically appended every hour but will not be visible in the UI. [View IPs from Microsoft's official list.](#)

WARPのバイパス設定

# WARPクライアントの詳細設定 - Split Tunnel

Support ▾ [← Back to Profile](#)

## Manage Split Tunnels (exclude)

Configure Cloudflare Zero Trust to exclude or include traffic to a given set of IP addresses or domains. Any traffic directed to an excluded destination will be handled by the local machine. Use wildcards to match against multiple subdomains at the same time.

[Learn more](#)**Selector** (Required)

IP Address ▾

**Value**

192.0.2.0/24

**Description (optional)**

Example: additional info

Save destination

### Your Split Tunnel entries (exclude) Showing 1-16 of 16

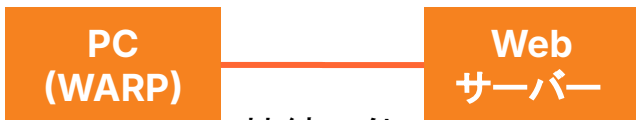
View and manage the IPs and domains Cloudflare Zero Trust excludes.

[Restore default entries](#)

<input type="checkbox"/>	Type ↑	Value	Description	
<input type="checkbox"/>	address	10.0.0.0/8	-	⋮
<input type="checkbox"/>	address	100.64.0.0/10	-	⋮
<input type="checkbox"/>	address	169.254.0.0/16	DHCP Unspecified	⋮
<input type="checkbox"/>	address	172.16.0.0/12	-	⋮
<input type="checkbox"/>	address	192.0.0.0/24	-	⋮
<input type="checkbox"/>	address	192.168.0.0/16	-	⋮
<input type="checkbox"/>	address	224.0.0.0/24	-	⋮
<input type="checkbox"/>	address	240.0.0.0/4	-	⋮
<input type="checkbox"/>	address	255.255.255.255/32	DHCP Broadcast	⋮
<input type="checkbox"/>	address	fe80::/10	IPv6 Link Local	⋮
<input type="checkbox"/>	address	fd00::/8	-	⋮
<input type="checkbox"/>	address	ff01::/16	-	⋮
<input type="checkbox"/>	address	ff02::/16	-	⋮
<input type="checkbox"/>	address	ff03::/16	-	⋮
<input type="checkbox"/>	address	ff04::/16	-	⋮
<input type="checkbox"/>	address	ff05::/16	-	⋮

## WARPクライアントの詳細設定 - Managed Network

Settings > WARP ClientのManaged networksで、特定のネットワーク環境でのみアクセス可能なサーバーの証明書情報を設定いただくことで、接続先ネットワークに応じてProfile Settingを切り替える事で、接続先ネットワークに応じたSplit Tunnelを設定することが可能となります。



接続可能

→ Profile Setting (Office)を適用

オフィスネットワークのサーバーに Split Tunnelを適用 (直接アクセス)



接続不可

→ Profile Setting (Remote)を適用

オフィスネットワークのサーバーに Split Tunnelを非適用 (Cloudflare Tunnel経由)

# WARPクライアントの詳細設定 - Managed Network

## Network locations

### Managed networks

Beta

Selectively apply device settings policies based around the office location of a WARP client.

[Add new](#)

Example

[Edit](#)

### Virtual networks

Manage how traffic routes to different private networks with overlapping IP ranges. Your users can select which network to connect to from the WARP client settings on their device.

No virtual networks are currently configured.

[Add new](#)

## WARPクライアントの詳細設定 - Managed Network

Profile Settingsの適用ルールにManaged Networkを指定した例

**Build an expression**

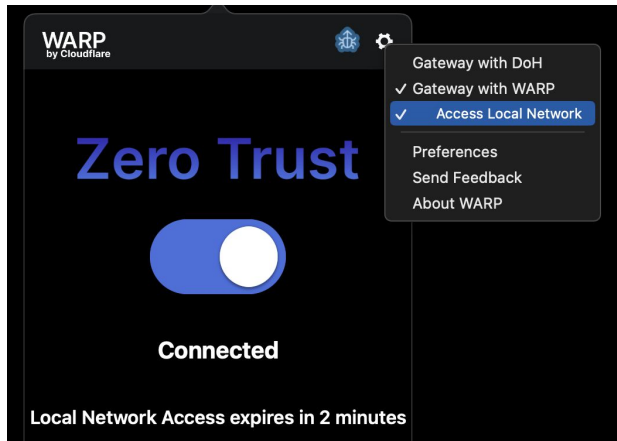
Selector <small>(Required)</small>	Operator <small>(Required)</small>	Value
<div>Managed network ▼</div>	<div>is ▼</div>	<div>Example ▼</div>
<div><a href="#">+ AND condition</a>    <a href="#">+ OR condition</a></div>		

参照) [Cloudflare Docs - Add a Managed Network](#)

## WARPクライアントの詳細設定 - Allow users to enable local network exclusionオプション

WARPの設定オプションで、一時的にプライベートネットワークへの直接通信を可能とするオプションがリリースされました。

参照) [Cloudflare Docs - WARP Settings - Allow users to enable local network exclusion](#)



## WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. **ログの確認**
6. その他確認画面

## ログの確認 - WARPログ

WARPでなにか障害が確認された際には、Cloudflareのサポートチケットを起票の上、以下操作で取得されたWARPログを添付いただければと思います。

(Mac or Linux)

```
$ warp-diag
```

(Windows)

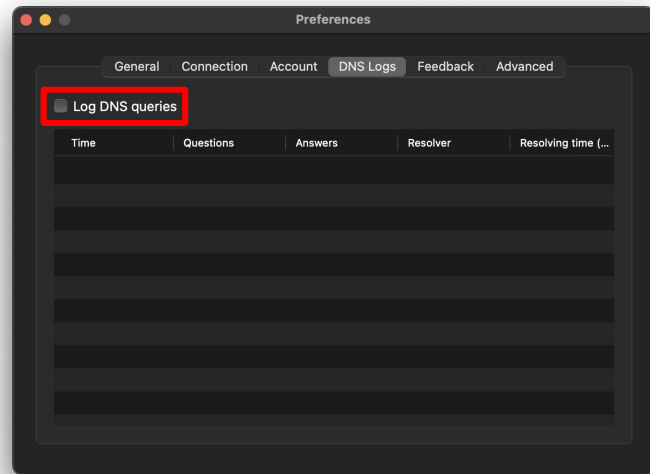
```
C:\Users\¥xxx> warp-diag
```

参照) [Cloudflare Docs - Debug logs](#)

## ログの確認 - その他のログ取得

チケットにてお問い合わせの際、お問い合わせの内容によっては、以下を追加で依頼させていただくケースもございます。

- WARPにおけるDNS Logsの有効化
- 以下ホストへのtraceroute  
([connectivity check](#))
  - [engage.cloudflareclient.com](#)
  - [connectivity.cloudflareclient.com](#)
- [Tunnel Log](#)の取得

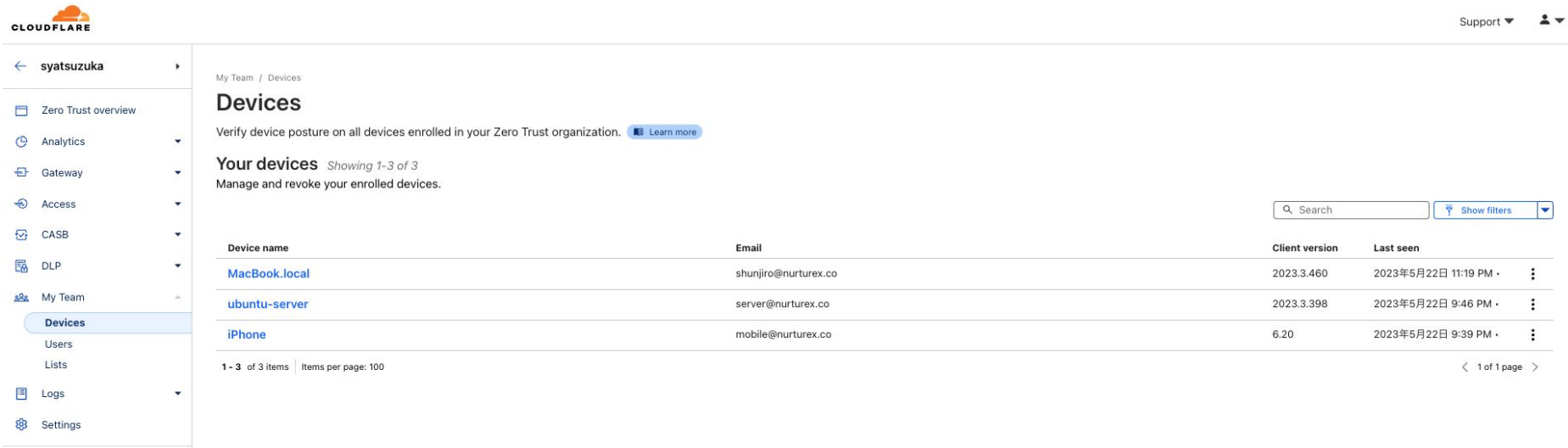


## WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. ログの確認
6. **その他確認画面**

## その他確認画面 - 登録デバイス

1. Zero Trustダッシュボードから、My Teams > Devicesをクリック  
登録デバイスの一覧から、それぞれのデバイスのWARPクライアントバージョン、  
最終ログイン日時をご確認いただけます。



My Team / Devices

### Devices

Verify device posture on all devices enrolled in your Zero Trust organization. [Learn more](#)

**Your devices** Showing 1-3 of 3  
Manage and revoke your enrolled devices.

Device name	Email	Client version	Last seen
<a href="#">MacBook.local</a>	shunjiro@nurturex.co	2023.3.460	2023年5月22日 11:19 PM • ⋮
<a href="#">ubuntu-server</a>	server@nurturex.co	2023.3.398	2023年5月22日 9:46 PM • ⋮
<a href="#">iPhone</a>	mobile@nurturex.co	6.20	2023年5月22日 9:39 PM • ⋮

1 - 3 of 3 items | Items per page: 100

< 1 of 1 page >

# その他確認画面 - 登録デバイス

## MacBook.local

Device details

ACTIVE




Device name

MacBook.local

Registration ID

OS Version	Product version extra	Manufacturer	Model	Mac address	Serial number
13.3.1	-	-	MacBookPro18,3		

Client details



Client

Cloudflare WARP

Status

Connected

Client version

2023.3.460

Last seen

May 22 2023 • 11:19:14 PM

Virtual network	DoH subdomain	Virtual IP addresses
default	-	IPv4: <div></div> IPv6: <div></div>

## その他確認画面 - 登録デバイス

各登録デバイスから、その利用ユーザーをご確認いただけます。

### User details

[View all](#)**Name**

Shunjiro Yatsuzuka

**Email address****Number of active devices**

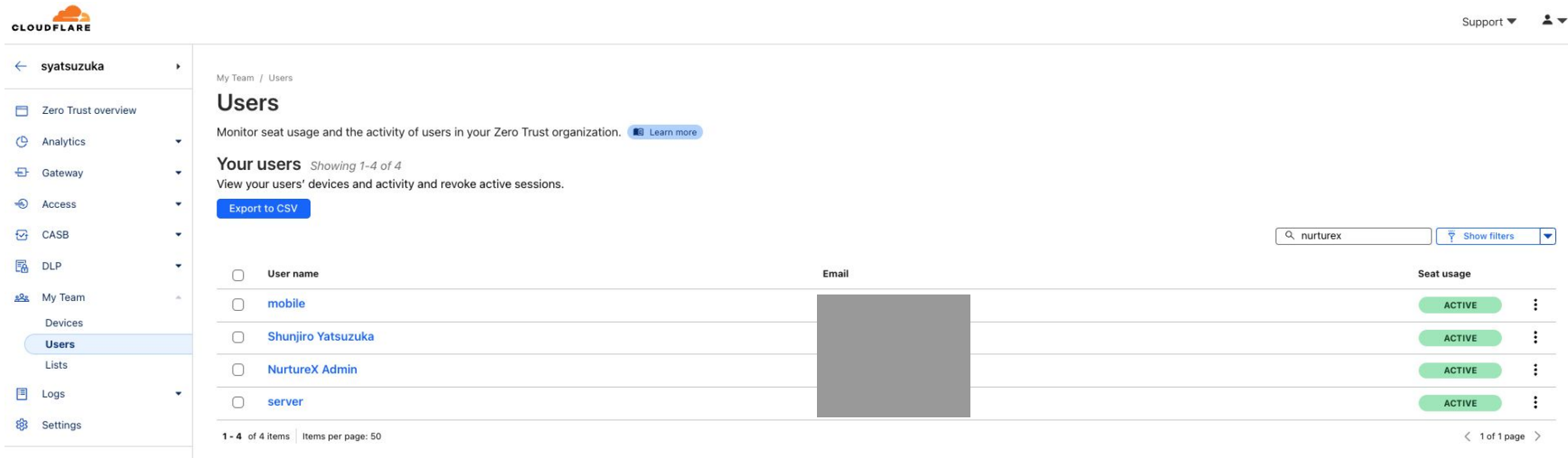
1

**Override code** ⓘ

--

## その他確認画面 - 登録ユーザー

1. Zero Trustダッシュボードから、My Teams > Usersをクリック  
登録ユーザーの一覧から、現在のアクティブユーザー、ユーザーの登録解除、最終ログイン日時、ロケーション、利用デバイスを確認可能




The screenshot shows the Cloudflare Zero Trust dashboard for a user named 'syatsuzuka'. The left sidebar contains navigation links: Zero Trust overview, Analytics, Gateway, Access, CASB, DLP, My Team, Devices, Users (selected), Lists, Logs, and Settings. The main content area is titled 'Users' and includes a description: 'Monitor seat usage and the activity of users in your Zero Trust organization.' Below this, it says 'Your users Showing 1-4 of 4' and 'View your users' devices and activity and revoke active sessions.' There is an 'Export to CSV' button. A search bar contains 'nurturex' and a 'Show filters' button. A table lists four users: 'mobile', 'Shunjiro Yatsuzuka', 'NurtureX Admin', and 'server'. Each user has a checkbox, a status 'ACTIVE' in a green pill, and a three-dot menu icon. The table has columns for 'User name', 'Email', and 'Seat usage'. At the bottom, it shows '1 - 4 of 4 items' and 'Items per page: 50'.

User name	Email	Seat usage
<input type="checkbox"/> mobile		ACTIVE
<input type="checkbox"/> Shunjiro Yatsuzuka		ACTIVE
<input type="checkbox"/> NurtureX Admin		ACTIVE
<input type="checkbox"/> server		ACTIVE

# その他確認画面 - 登録ユーザー

Shunjiro Yatsuzuka

User details



Name

Shunjiro Yatsuzuka

Email address

Access

ACTIVE

Gateway

INACTIVE


Number of active devices

1

Last login


May 22 2023 • 9:18:56 PM

Most recent location


Japan  [View all](#)

Revoke

## Devices

Name	Registration ID	Client version	Last seen	
 MacBook.local		2023.3.460	May 22 2023 • 11:19:14 PM	⋮

## Recent activity

Application	Application URL	Last login
 Syatsuzuka	syatsuzuka.cloudflareaccess.com	May 22 2023 • 9:12:10 PM

# Q&A

1. はじめに
2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール

## 5. Q&A

# Thank you

→ 1 888 99 FLARE

✉ enterprise@cloudflare.com

🌐 cloudflare.com



Cloudflare連続勉強会 #7

# Cloudflare Zero Trustの紹介 (後編)

## - 導入編

カスタマーサクセス シニアマネージャー 八塚 俊次郎  
シニアカスタマーソリューションエンジニア 西原 誠

**Cloudflare Japan**

東京都中央区京橋 2-2-1京橋エドグラン 26階

[www.cloudflare.com/ja-jp/](https://www.cloudflare.com/ja-jp/)

# Agenda

- 1 はじめに
- 2 Cloudflare ZTNAの機能および設定
- 3 Cloudflare SWGの機能および設定
- 4 Cloudflare CASBの機能および設定
- 5 Cloudflare DLPの機能および設定
- 6 Q&A

# はじめに

## 1. はじめに

2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
5. Cloudflare DLPの機能および設定
6. Q&A

## 目的

本WebinarはCloudflareのEnterpriseプランのご契約をお持ちのお客様向けにCloudflare製品の機能及び設定概要を紹介することで、製品をよりよくご活用いただくことを主目的とします。

時間配分	内容
50分	メインセッション
10分	Q&A

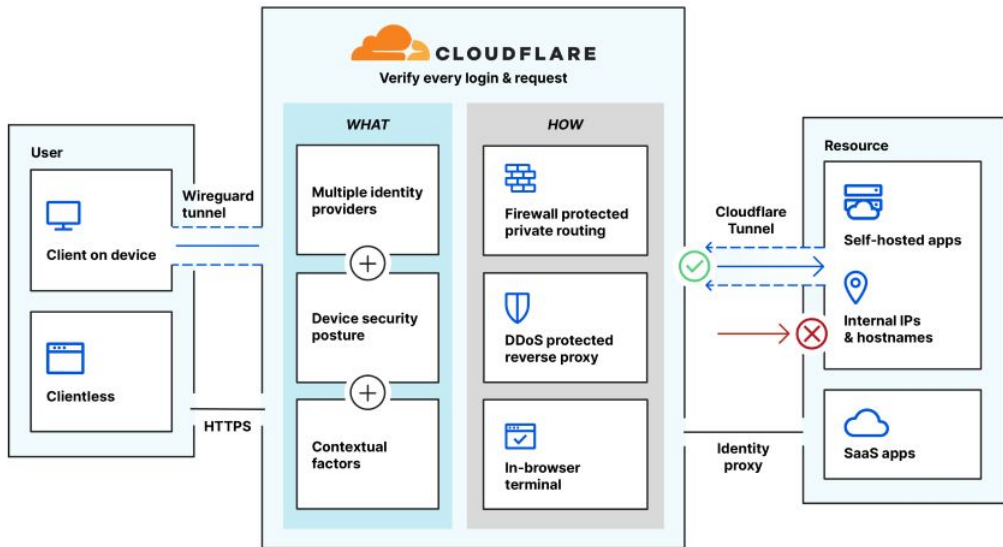
## 注意事項

本Webinarご参加に当たっての注意事項を以下記載いたします。

- 本Webinarはレコーディングを行い、後日、弊社Webinarサイトにご登録のお客様は再視聴できるようにいたします。各セッションの最後にはブラウザ上のテキストボックスからご質問を受付けますが、起票者のお名前は伏せてのQ&A対応となります。
- お時間の制約から、Webinar中に頂いたすべてのご質問にお答えできないかもしれません。最善は尽くさせていただければと考えておりますが、その旨、ご了承ください。
- 本セッションで用いるスライドはセッション終了後、当Webinarのご登録ページからPDF形式でダウンロード頂けます。

## 前回セッションの振り返り

Cloudflare Zero Trust導入の流れとしては[Roadmap to Zero Trust](#)をご参照いただけます。



参照) [Cloudflare Zero Trust Network Accessの鳥瞰図](#)

# 前回セッションの振り返り

1. Cloudflare Zero Trust導入の流れ
2. Cloudflareダッシュボードの初期設定
  - a. チーム名の設定
  - b. 認証方法の設定
  - c. ダッシュボードのSSO登録 (オプション)
  - d. Logpush設定
3. WARPクライアントのインストール
  - a. Device Enrollment Permissionの定義
  - b. WARPクライアントのインストール
  - c. Zero Trustインスタンスへのログイン
  - d. WARPクライアントの詳細設定
  - e. ログの確認
  - f. その他確認画面

※前回セッションのレコーディングは [Cloudflare Resource Hub](#)からご参照いただけます。

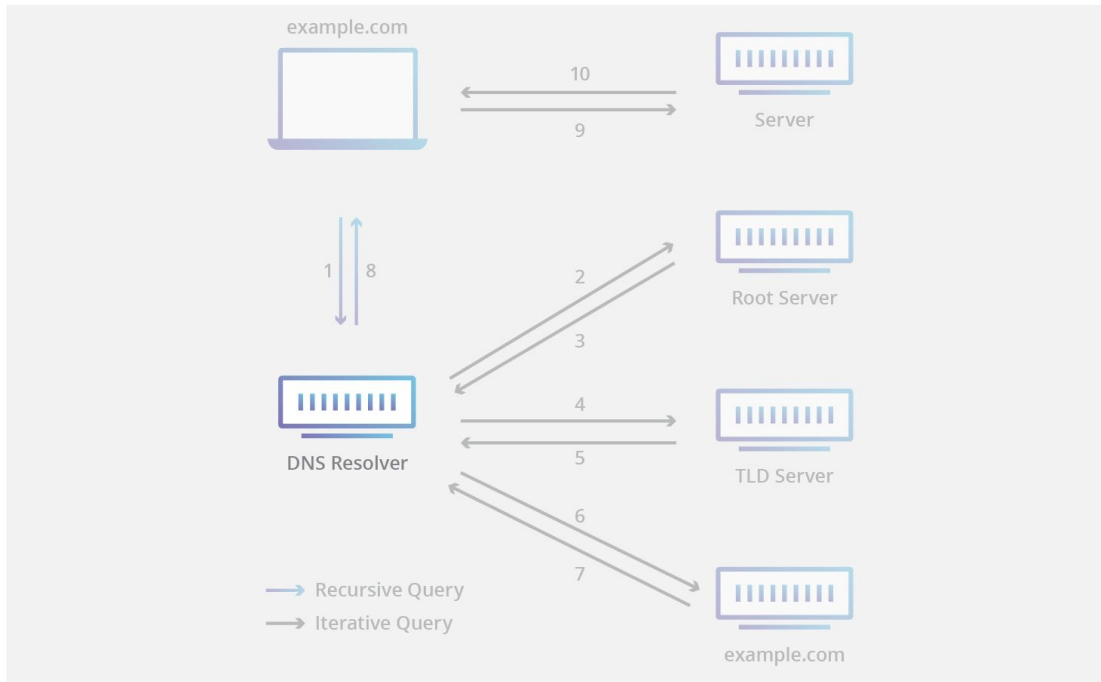
# Cloudflare ZTNAの機能および設定

1. はじめに
- 2. Cloudflare ZTNAの機能および設定**
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
5. Cloudflare DLPの機能および設定
6. Q&A

## ZTNAの設定

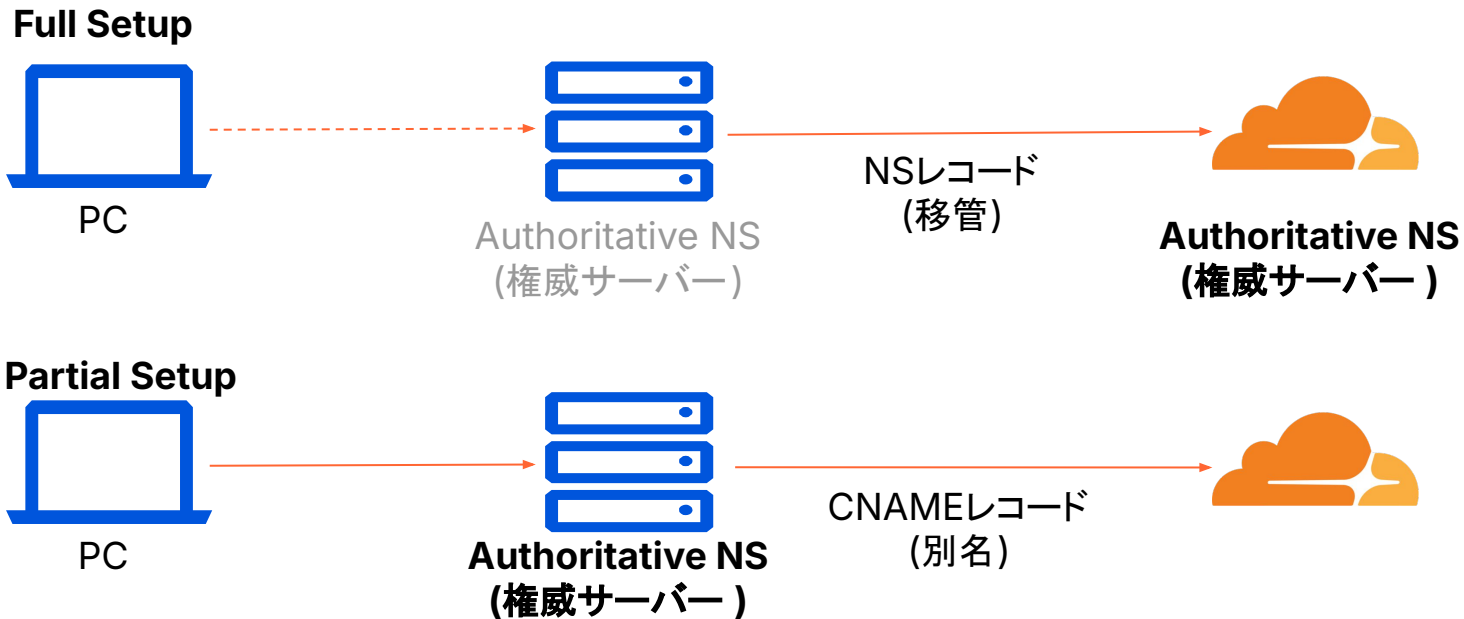
1. サイトの登録 (オプション)
2. Tunnel設定
3. アプリケーションの登録

## サイトの登録 - 名前解決の仕組み



参照) [What are the different types of DNS server?](#)

## サイトの登録 - Full SetupとPartial Setup



## サイトの登録

1. Cloudflareへのサイトの登録
2. DNSの[Full Setup](#)
3. DNSの[Partial Setup](#)
4. SSL/TLSセットアップ

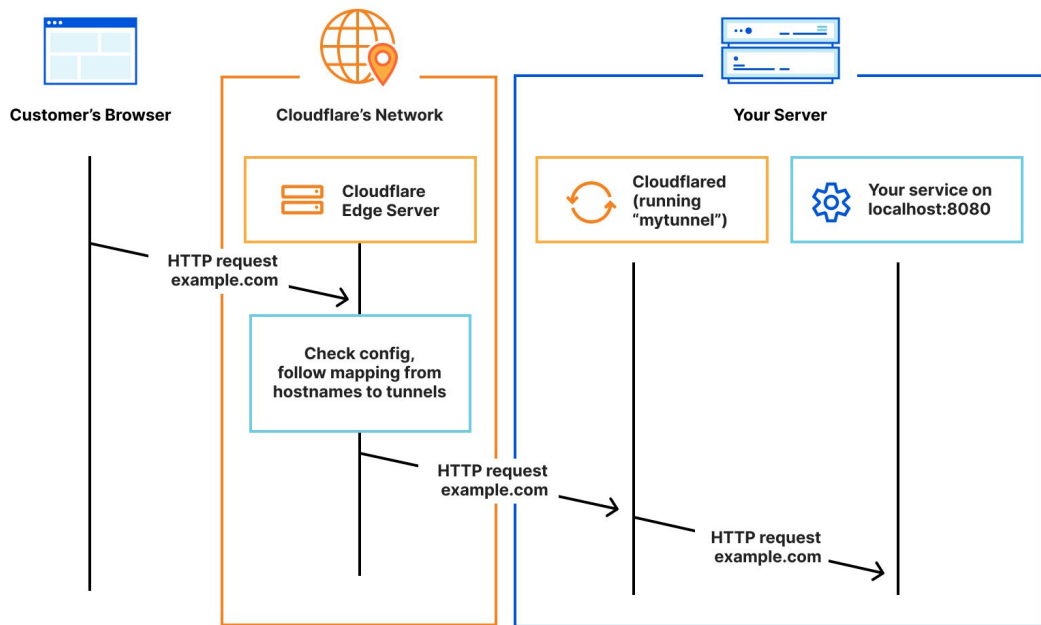
参照) [Cloudflare Docs - Add site to Cloudflare](#)

※詳細は[Cloudflare連続勉強会 #3 - Cloudflare DNSおよびSSL/TLSのご紹介](#)をあわせてご参照くださいませ。

## ZTNAの設定

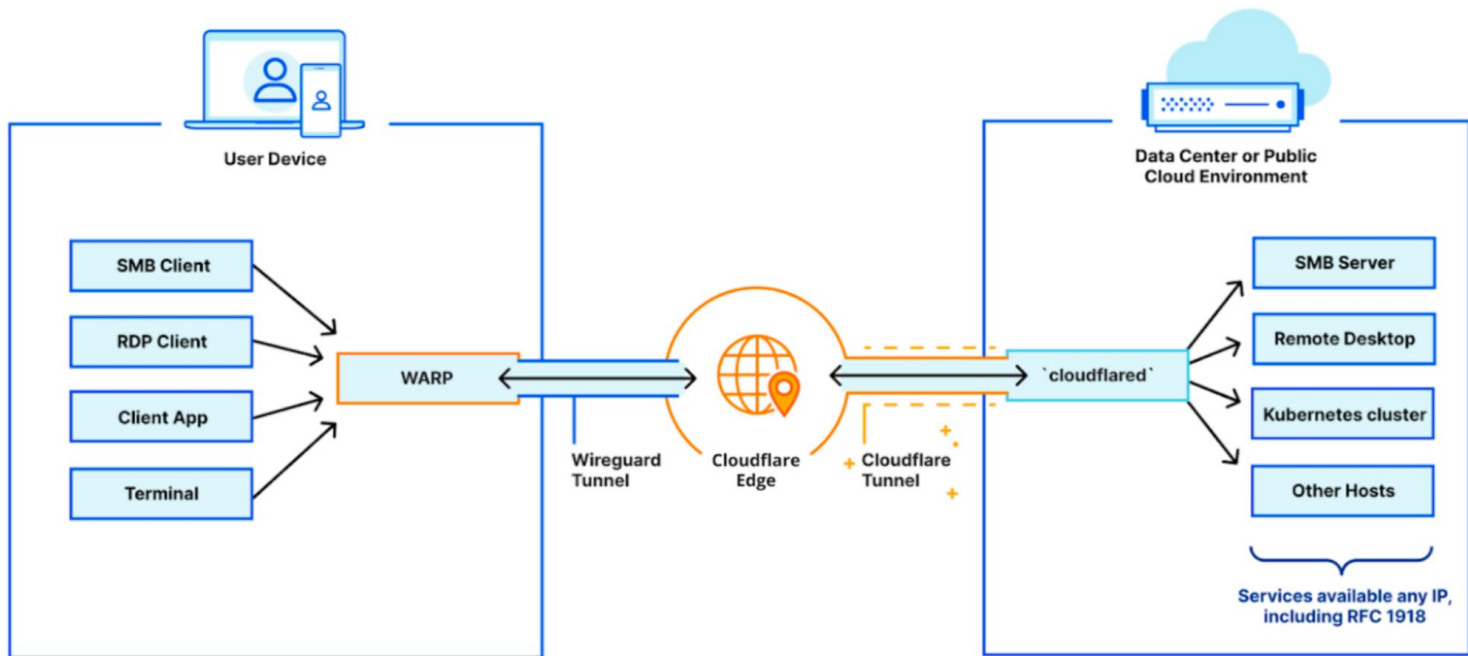
1. サイトの登録 (オプション)
2. **Tunnel**設定
3. アプリケーションの登録

# Tunnel設定



参照) [Cloudflare Docs - Cloudflare Tunnel](#)

## Tunnel設定



参照) [Cloudflare Docs - Private hostnames and IPs](#)

## Tunnel設定

cloudflaredによるTunnel設定は大きく2つのアプローチがあります。

- Public Hostnameの設定: ホスト名を指定した接続を実現したい場合 (HTTP以外のプロトコルでアクセスさせたい場合には、クライアント端末にcloudflaredの追加インストールが必要になる場合あり)
- Private Networkの設定: プライベートIPアドレスを指定した接続を実現したい場合 (WARP経由でのアクセス)

※SSHサーバーへの接続においては、新たにAccessの認証情報を元にshort-lived certificateを作成し、SSHサーバーへの接続を実現するAccess for Infrastructureをご利用いただけます。

## Tunnel設定

1. Zero Trustダッシュボードから、Access > Tunnelsへアクセス
2. Create a tunnelボタンをクリック
3. Tunnel名を設定
4. Connectorの作成
5. ルーティング設定
6. Save tunnelボタンをクリック
7. 追加設定

参照) [Cloudflare Docs - Setup a tunnel through the dashboard](#)

# Tunnel設定 - Tunnel名を設定

## Create a tunnel

Create a tunnel to connect HTTP web servers, SSH servers, remote desktops, and other protocols safely to Cloudflare.

[📖 Learn more](#)

**Name your tunnel** > Install connector > Route tunnel

### Name your tunnel

Use a descriptive name based on the network you want to connect. We recommend creating only one tunnel for each network.

Tunnel name (Required)

For example, enterprise-VPC-01

[Back](#)[Save tunnel](#)

# Tunnel設定 - Connectorの作成

## Configure ubuntu-server

Name your tunnel > **Install connector** > Route tunnel

### Choose your environment

Choose an operating system:



### Install and run a connector

To connect your tunnel to Cloudflare, copy-paste one of the following commands into a terminal window. Remotely managed tunnels require that you install cloudflared 2022.03.04 or later.

① **Store your token carefully.** This command includes a sensitive token that allows the connector to run. Anyone with access to this token will be able to run the tunnel.

If you don't have cloudflared installed on your machine:

```
brew install cloudflare/cloudflare/cloudflared &&
sudo cloudflared service install
```

If you already have cloudflared installed on your machine:

```
sudo cloudflared service install
```

[View Frequently Asked Questions](#)

こちらで表示されるコマンドをcloudflaredをインストールしたいホスト上で実行することで、Connectorが作成されます。

※すでに同じサーバー上にConnectorが存在する場合、削除しないと新規Connectorが正しく作成・認識されない場合がありますのでご注意ください。

<既存Connector削除コマンド>  
`$ sudo cloudflared service uninstall`

### Connectors

Connector ID	Status	Data centers	Origin IP	Version
	Connected	NRT, KIX		2023.5.0 

# Tunnel設定 - ルーティング設定 (Public Hostnames)

## Route Traffic for ubuntu-server

Name your tunnel > Install connector > **Route tunnel**

Route traffic by adding a public hostname or a private network to your tunnel. You can always add more hostnames or networks at a later time.

Protect your resource by adding an Access policy under [Access > Applications > Self-hosted](#).

[Public Hostnames](#) Private Networks

### Edit public hostname for ubuntu-server

Public hostname

Subdomain

test

Domain (Required)

Path

(optional) path

Service

Type (Required)

HTTP

URL (Required)

localhost

For example, <https://localhost:8001>

[Additional application settings](#)

サーバー接続を実現したいホスト名を設定

Save tunnel

## Route Traffic for ubuntu-server-ssh

Name your tunnel > Install connector > **Route tunnel**

Route traffic by adding a public hostname or a private network to your tunnel. You can always add more hostnames or networks at a later time.

Protect your resource by adding an Access policy under [Access > Applications > Self-hosted](#).

[Public Hostnames](#) Private Networks

### Edit public hostname for ubuntu-server-ssh

Public hostname

Subdomain

ssh

Domain (Required)

Path

(optional) path

Service

Type (Required)

SSH

URL (Required)

localhost:22

For example, <https://localhost:8001>

[Additional application settings](#)

Back

Save tunnel

# Tunnel設定 - ルーティング設定 (Private Networks)

## Route Traffic for ubuntu-server

Name your tunnel > Install connector > **Route tunnel**

💡 Route traffic by adding a public hostname or a private network to your tunnel. You can always add more hostnames or networks at a later time.

🔒 Protect your resource by adding a Gateway policy under [Gateway > Policies > Network](#).

Public Hostnames Private Networks

### Create private network for ubuntu-server

CIDR (Required)

Back

Save tunnel

サーバー接続を実現したい対象のPrivate IPレンジを設定

# Tunnel設定 - Save tunnelボタンをクリック

## Tunnels

Tunnels establish a secure connection between Cloudflare's edge and your infrastructure.

[Learn more](#)

A new version of cloudflared is available. Visit our [downloads](#) page to upgrade.

### Your tunnels Showing 1 - 1

Manage the configurations of your existing tunnels.

[+ Create a tunnel](#)

Tunnel name	Tunnel ID	Status	Routes	Uptime	Created
ubuntu-server		HEALTHY		--	2023年5月29日

1 - 1 | Items per page: 10

< 1 of 1 page >

正しく設定できた場合には、Statusとして”Healthy”、Routesに前段で設定した内容が表示されます。






## Tunnel設定 - Save tunnelボタンをクリック

DNS management for **nurturex.co** Import and Export ▼ ⚙️ Dashboard Display Settings

All changes made in the edit drawer are implemented once saved.

Search DNS Records

▼ Add filter  Search + Add record

Type ▲	Name	Content	Proxy status	TTL	Actions
A			 Proxied	Auto	<a href="#">Edit ▶</a>
CNAME	_domainconnect		 Proxied	Auto	<a href="#">Edit ▶</a>
CNAME	ssh		 Proxied	Auto	<a href="#">Edit ▶</a>
CNAME	test		 Proxied	Auto	<a href="#">Edit ▶</a>
CNAME	www		 Proxied	Auto	<a href="#">Edit ▶</a>
				Auto	<a href="#">Edit ▶</a>
				Auto	<a href="#">Edit ▶</a>

Tunnelの作成で"Public Hostname"を指定された場合には、Cloudflare DNSに対象サーバーへアクセスするためのCNAMEレコードが自動で追加作成されます

## Tunnel設定 - 必要なFirewall設定およびcloudflaredの前提条件

cloudflaredをご利用される際には、以下ドキュメントで指定されたポートに対するFirewall設定(穴あけ)が必要となります。

また、cloudflaredご利用にあたっての前提を含め、以下ご参照ください。

### Cloudflare Docs - Tunnel with firewall

<https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/deploy-tunnels/tunnel-with-firewall/>

### Cloudflare Docs - System Requirement

<https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/deploy-tunnels/system-requirements/>

## Tunnel設定 - 追加設定 (Public Hostnames経由での接続: SSH, RDP, SMB)

SSH, RDP, SMBといったプロトコル経由でのサーバーアクセスを利用したい場合には以下追加設定が必要となります。

1. [Cloudflared](#)のインストール
2. 接続対象サーバーごとの追加設定 ([SSH](#), [RDP](#), [SMB](#))
3. Self-hostedアプリケーションの登録 (推奨)\*次セクション参照

## Tunnel設定 - 追加設定 (Private Network経由での接続: Split Tunnelsからの除外)

### WARP Client

#### Device enrollment

##### Device enrollment permissions

Define who can connect devices to your organization.

[Manage](#)

#### Device settings

##### Profile settings

Beta

Set default and customized configurations for groups of devices in your organization.

[+ Create profile](#)

#	Profile name	Enabled	
1	Admin	<input checked="" type="checkbox"/>	⋮
2	Default	<input checked="" type="checkbox"/>	⋮

[Configure](#)[Duplicate](#)[Make default](#)[Delete](#)[Move up](#)[Move to...](#)

#### Global settings

##### Admin override

Only allow users to disable the WARP client with a one-time use password.

[Install CA to system certificate store](#)

Private Network経由で接続させる場合には、WARPクライアントに対して、対象のプライベートIPをSplit Tunnelsの設定に含める必要があります

IP指定でのアクセスを許諾したいユーザーに割り当てられているProfileのConfigureメニューをクリック

## Tunnel設定 - 追加設定 (Private Network経由での接続: Split Tunnelsからの除外)

Your Split Tunnel entries (exclude) Showing 1-14 of 14  
View and manage the IPs and domains Cloudflare Zero Trust excludes.

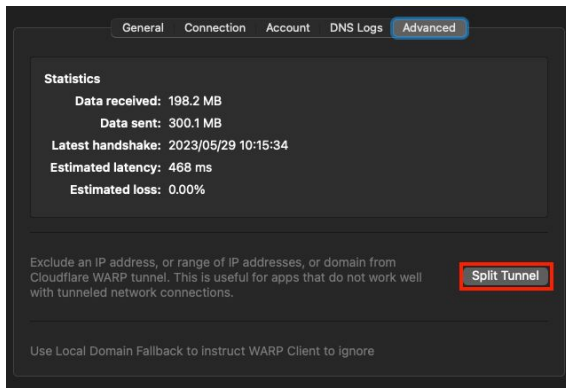
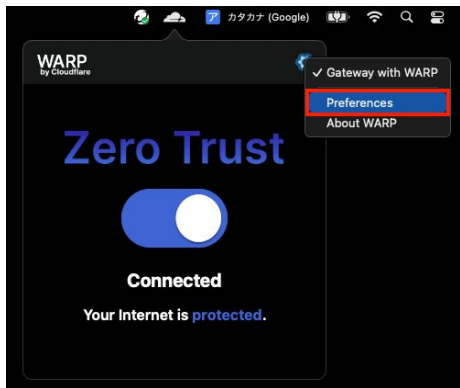
以下は192.168.0.0/16を削除した例

[Restore default entries](#)

<input type="checkbox"/>	Type ↑	Value	Description	
<input type="checkbox"/>	address	10.0.0.0/8	-	⋮
<input type="checkbox"/>	address	100.64.0.0/10	-	⋮
<input type="checkbox"/>	address	169.254.0.0/16	DHCP Unspecified	⋮
<input type="checkbox"/>	address	172.16.0.0/12	-	⋮
<input type="checkbox"/>	address	224.0.0.0/24	-	⋮
<input type="checkbox"/>	address	240.0.0.0/4	-	⋮
<input type="checkbox"/>	address	255.255.255.255/32	DHCP Broadcast	⋮
<input type="checkbox"/>	address	fe80::/10	IPv6 Link Local	⋮
<input type="checkbox"/>	address	fd00::/8	-	⋮
<input type="checkbox"/>	address	ff01::/16	-	⋮
<input type="checkbox"/>	address	ff02::/16	-	⋮
<input type="checkbox"/>	address	ff03::/16	-	⋮
<input type="checkbox"/>	address	ff04::/16	-	⋮
<input type="checkbox"/>	address	ff05::/16	-	⋮

## Tunnel設定 - 追加設定 (Private Network経由での接続: Split Tunnelsからの除外)

各WARPクライアントに適用されているSplit Tunnelsは、WARPクライアントで以下操作からご確認いただけます。



Excluded IPs/Domains	Description
10.0.0.0/8	
100.64.0.0/10	
169.254.0.0/16	DHCP Unspecified
172.16.0.0/12	
224.0.0.0/24	
240.0.0.0/4	
255.255.255.255/32	DHCP Broadcast
fe80::/10	IPv6 Link Local
fd00::/8	
ff01::/16	
ff02::/16	

## Tunnel設定 - Tunnelログの取得

Cloudflare Tunnelに関する調査には、Tunnel Logの取得・共有が期待されます。  
cloudflaredのインストール先OSによって詳細手順は変わってきますが大きくは以下の流れで取得いただくことになります。

- 1) cloudflaredの起動オプションを変更の上、再起動 (--loglevel debugを追加)
- 2) Cloudflareのダッシュボードもしくは、cloudflaredがインストールされている端末からログを参照

参考: [Cloudflare Docs - Tunnel Log](#)

## Tunnel設定 - Tunnelログの取得

### <cloudflaredのインストール先が Linux (Ubuntu Server)の場合の Tunnel再起動>

1) cloudflaredの起動スクリプトパスを確認

```
$ systemctl status cloudflared.service
```

2) cloudflared起動スクリプトの編集 (--loglevel debugを追記)

```
$ vi /etc/systemd/system/cloudflared.service
```

3) スクリプトファイルのリスタート

```
$ systemctl restart cloudflared.service
```

参考: [Cloudflare Docs - Tunnel Log](#)

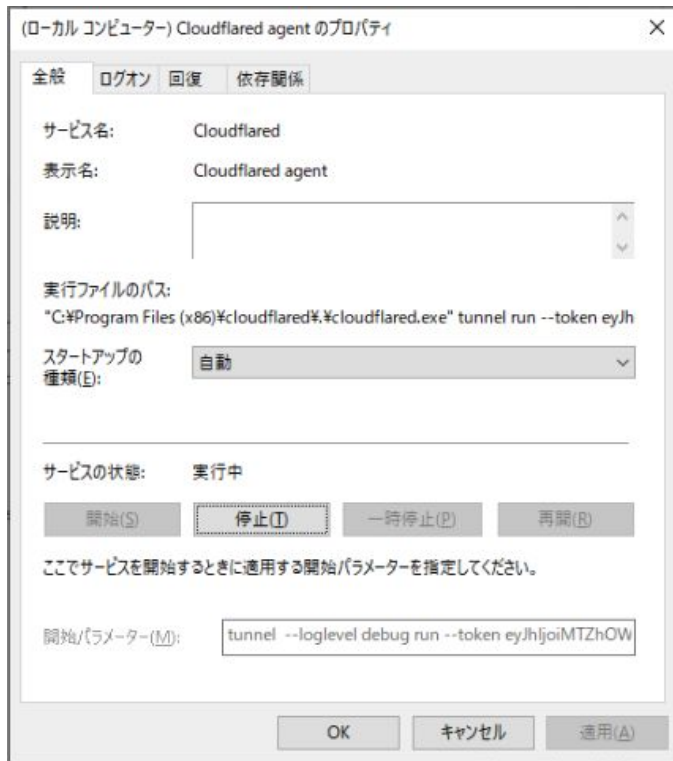
## Tunnel設定 - Tunnelログの取得

### <cloudflaredのインストール先がWindowsの場合のTunnel再起動>

- 1) サービス管理画面を起動
- 2) Cloudflaredのサービスをダブルクリック
- 3) 「実行ファイルのパス」で実行コマンドを除外した、オプション部分をコピーの上、「開始パラメータ」にペーストし、「開始パラメータ」に--loglevel debugを追記
- 4) 現在動作しているCloudflaredを停止の上、「開始」ボタンをクリック

※今回設定した「開始パラメータ」は永続保存されないため、次回PCを再起動した際には元々の設定に戻る。

参考: [Cloudflare Docs - Tunnel Log](#)



## Tunnel設定 - Tunnelログの取得

### <ダッシュボードからのログ参照>

ご利用のCloudflaredが2023.5.1以上の場合には、以下手順によりダッシュボードからTunnelログをご参照いただけます。

1. Tunnels一覧 (Access > Tunnels)へアクセスし、ログを参照したいTunnel名をクリック
2. ログを参照したいConnectorをクリック ([Replica設定](#)をしていない場合には一つのコネクタのみが表示)
3. "Begin Logstream"ボタンをクリックの後、トンネル経由での通信を試行することで、ログが出力
4. 操作終了後、"Pause Logstream"ボタンをクリックし、ログを確認

## Tunnel設定 - Tunnelログの取得

### Live logs Showing 1-2 of 2

See a live stream of your tunnel's output and exceptions.

[⏸ Pause log stream](#)[Download logs](#)[Clear logs](#)[⌵ Show filters](#)

Level	Event	Message	Time
<a href="#">Info</a>	http	304 Not Modified	Nov 21 2023 • 10:14:50
<a href="#">Info</a>	http	GET https://test.nurturex.co/ HTTP/1.1	Nov 21 2023 • 10:14:50

## Tunnel設定 - Tunnelログの取得

### <cloudflaredがインストールされた端末からの Tunnelログ取得>

1) cloudflaredでログイン認証  
以下コマンドを実行いただくと、ブラウザが自動的に起動し、登録されているIdPを用いた認証が行われます。

```
$ cloudflared tunnel login
```

認証が正常に終了すると、ブラウザ上にSuccessの表示が行われコンソールにプロンプトが帰ってきます。

参考: [Cloudflare Docs - Tunnel Log](#)

## Tunnel設定 - Tunnelログの取得

### 2) ログ取得

以下コマンドで、ログが標準出力(コンソール出力)されます。ファイルへのリダイレクトをご希望の場合には以下の2つ目のコマンドを実行いただくと、"tunnel\_log.txt"にログ情報が出力されます。

```
$ cloudflared tail <UUID>
```

(ログをファイル出力したい場合)

```
$ cloudflared tail <UUID> > tunnel_log.txt
```

※tunnel\_log.txtは任意のファイル名に変更いただくことも可能です

## ZTNAの設定

1. サイトの登録 (オプション)
2. Tunnel設定
3. **アプリケーションの登録**

# アプリケーションの登録

## Add an application

Configure the policies, authentication, and settings of your applications.

Select type > Configure application > Add policies > Setup

### What type of application do you want to add?

If you're not sure, choose self-hosted.



#### Self-hosted

Applications you host in your infrastructure that use Cloudflare's authoritative DNS.

Select



#### SaaS

Applications you do not host. Additional setup is required outside of Cloudflare Zero Trust.

Select



#### Private network

Non-HTTP applications you host that do not have public DNS records.

Select



#### Infrastructure NEW

Servers and resources in your infrastructure managed by a cloud provider or you.

① At least one target is required to create an infrastructure app.

[Get started](#)

Select



#### Bookmark

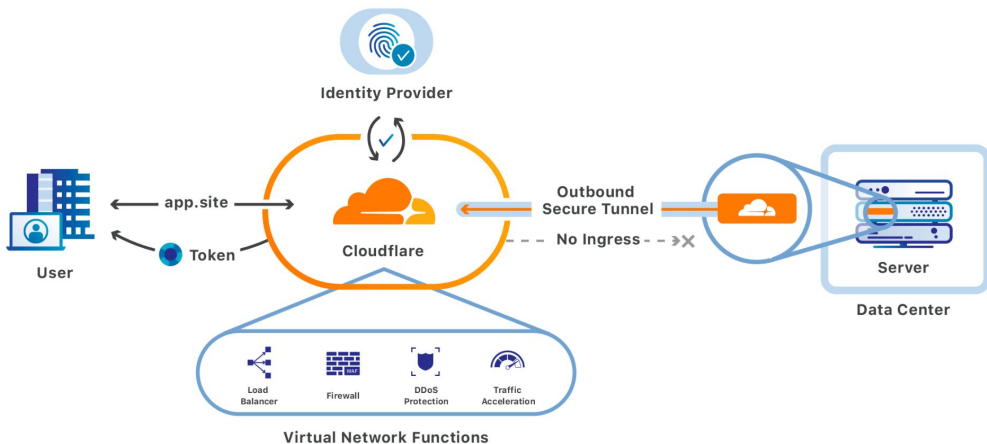
If you have apps that cannot be put behind Access, we provide a shortcut on our App Launcher.

Select

## アプリケーションの登録

タイプ	対象	条件
Self-hosted	オンプレ環境で稼働する社内アプリケーション (Cloudflare DNSを利用)	<ul style="list-style-type: none"><li>Cloudflare DNS</li><li>(Cloudflare Tunnel)</li></ul>
SaaS	インターネットで公開されているアプリケーション (SAML連携アプリ)	<ul style="list-style-type: none"><li>Cloudflare AccessとのSSO連携</li></ul>
Private network	インターネットからアクセスできないプライベートネットワークで稼働するアプリケーション (パブリックなDNSレコードの登録なし)	<ul style="list-style-type: none"><li>Cloudflare Tunnel</li></ul>
Bookmark	Cloudflare Accessと連携されていないものの、App Launcherの登録対象としたいアプリケーション	-

## アプリケーションの登録 - Self-hosted



参照) [Cloudflare Docs - Add a self-hosted application](#)

Add an application Cancel Next

Select type > **Configure app** > Add policies > Setup

---

**Application Configuration**

**Application name** (Required)  
Enter an application name

**Session Duration** (Required)  
24 hours

**Application domain**

**Subdomain** (optional) subdomain

**Domain** (Required)

**Path** (optional) path

---

**Application Appearance**

**App Launcher visibility**  
Show this app in App Launcher ☒

**Application logo**  
This will appear in the App Launcher and the main Applications page.

☒ Default ☐ Custom

---

**Identity providers** [Learn more](#)

Accept all available identity providers ☒

Manually select identity providers users can use to connect to this application De-select all Select all

☐ Okta ☐ One-time PIN - rick-sandbox-com - Cloudflare...

☐ LinkedIn

Instant Auth  
Skip identity provider selection if only one is configured ☐

## アプリケーションの登録 - Self-hosted

1. Accessへのアプリケーション登録
  - a. Zero Trustダッシュボードから、Access > Applicationsへアクセス
  - b. "Add an application"を選択
  - c. "Self-hosted"を選択
  - d. "Application Name"を設定
  - e. "Application Domain"を設定
2. Access Policyの設定
3. Authenticationの設定

参照) [Cloudflare Docs - Add a SaaS application to Access](#)

# アプリケーションの登録 - Self-hosted

## Test

[Overview](#) [Policies](#) [Authentication](#) [Settings](#)

### Application Configuration

Application name (Required)

Test

4/350

Session Duration (Required)

24 hours

Application domain

Subdomain

test

Domain (Required)

nurturex.co

Path

(optional) path

Application Audience (AUD) Tag [①](#)

Copy

Revoke existing tokens

# アプリケーションの登録 - Self-hosted

## Add an application

Configure the policies, authentication, and settings of your applications.

Select type > **Configure app** > Add policies > Setup

**Application Configuration**

Application name (Required) Session Duration (Required)

Test App 24 hours

Application domain

Subdomain Domain (Required) Path

test nurtutex.co (optional) path

+ Add domain

**Application Configuration**

Application name (Required) Session Duration (Required)

SSH 24 hours

Application domain

Subdomain Domain (Required) Path

ssh nurtutex.co (optional) path

+ Add domain

前段のTunnel作成で登録したPublic Hostnames  
で設定したホスト名を指定

# アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)

## Add an application

Configure the policies, authentication, and settings of your applications.

Select type > Configure app > **Add policies** > Setup

<b>Policy name</b> (Required)	<b>Action</b> (Required)	<b>Session duration</b>
<input type="text" value="SSH"/>	<input data-bbox="459 518 738 554" type="text" value="Allow"/>	<input type="text" value="Same as application session timeout"/>

### Create additional rules

If you're assigning one or more groups to this application, any rules you create now will be applied in addition to group rules.

**Include**

<b>Selector</b>	<b>Value</b>
<input type="text" value="Emails ending in"/>	<input type="text" value="main.com"/>

[+ Add include](#) [+ Add require](#) [+ Add exclude](#)

対象アプリへのアクセスコントロールを設定

## アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)

### Additional settings

Enable automatic cloudflared authentication



Browser rendering

BETA

SSH

Cloudflare will render an SSH terminal or VNC session for this application in a web browser.

こちらを設定することでブラウザ経由でSSH接続が可能となります

## アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)

前段の設定から、ブラウザ経由でSSHサーバーへのアクセスが可能となります

※コンソールからもアクセス可能  
\$ ssh <ユーザー名> @ <ホスト名>

SS

SSH

SS

SSO App

T

Test

ssh.nurturex.co

User

User cannot be empty.

Submit

shunjiro@ssh.nurturex.co

Password

Private Key

Password

Submit

## アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)

```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-43-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

31のアップデートはすぐに適用されます。
これらの追加アップデートを確認するには次を実行してください: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

14 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Last login: Mon Jun  5 09:55:25 2023 from 127.0.0.1
shunjiro@ubuntu-server:~$
```

## アプリケーションの登録 - SaaS

1. Accessへのアプリケーション登録
  - a. Zero Trustダッシュボードから、Access > Applicationsへアクセス
  - b. "Add an application"を選択
  - c. "SaaS"を選択
  - d. "Entity ID"および"Assertion Consumer Service URL"を設定
  - e. "Name ID Format"を選択 ("Unique ID"もしくは"Email")
  - f. "SAML attribute statements (optional)"を設定
2. Access Policyの設定
3. Authenticationの設定

参照) [Cloudflare Docs - Add a SaaS application to Access](#)

# アプリケーションの登録 - SaaS

## Add a policy to SSO App

<b>Policy name</b> <small>(Required)</small>	<b>Action</b> <small>(Required)</small>	<b>Session duration</b>
<input type="text" value="Enter a policy name"/>	<input type="text" value="Allow"/>	<input type="text" value="Same as application session timeout"/>

### Configure rules

The rules you create here define who can or cannot reach your application.

#### Include

Selector

Value

×

[+ Add include](#)

[+ Add require](#)

[+ Add exclude](#)

# アプリケーションの登録

## Applications

Protect your Self-Hosted, SaaS and Private applications with Zero Trust policies. Only users who match your policies will have access to your configured applications. [Learn more](#)

### Your applications Showing 1-4 of 4

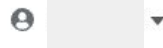
Manage the policies, authentication, and settings of your configured applications.

[+ Add an application](#)

Application name	Application URL	Total Domains	Policies assigned	Type	
 Test App	test.nurturex.co	1	1	SELF-HOSTED	⋮
 SSH	ssh.nurturex.co	1	1	BROWSER SSH	⋮
 NurtureX	https://www.nurturex.co	1	-	BOOKMARK	⋮
 SSO App	dash.cloudflare.com	1	1	DASH_SSO	⋮

# アプリケーションの登録

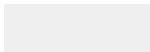
 syatsuzuka.cloudflareaccess.com



Welcome 

 Search for apps

NX



SS

SSH

SS

SSO App

TA

Test App

# Cloudflare SWGの機能および設定

1. はじめに
2. Cloudflare ZTNAの機能および設定
- 3. Cloudflare SWGの機能および設定**
4. Cloudflare CASBの機能および設定
5. Cloudflare DLPの機能および設定
6. Q&A

## SWGの設定

1. **Firewall Policy**の設定
2. Egress Policyの設定
3. Resolver Policyの設定
4. DNS Locationsの設定
5. Proxy Endpointの設定

## DNSフィルタリングの設定

1. Zero Trustダッシュボードから、Settings > Networkをクリック
2. Gateway DNS logsに対して activity loggingを有効化
3. ブラウザから任意のURLにアクセスし、DNSのログが取得されていることを確認する。

### Gateway Logging

#### Activity logging

Log DNS queries, network packets, and/or HTTP requests.

Enabled 

#### Gateway DNS logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

#### Gateway Network logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

#### Gateway HTTP logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

# DNSフィルタリングの設定

## Gateway activity logs

Monitor individual DNS queries, network packets, and HTTP requests inspected by Gateway. You can also download encrypted SSH command logs for sessions proxied by Gateway.

[Learn more](#)

[DNS](#)   [Network](#)   [HTTP](#)   [SSH](#)

### Your DNS logs Showing 1-9 of 9

View and filter your DNS queries. By default, Gateway logs all events, including DNS queries that are allowed and not a risk.

 Hide filters 

Email

Event

Select...

Policy

All Policies

Date Time Range

Jun 5th 10:31 → Jun 5th 11:31 ×

Apply filters

Clear filters

DNS	Email	Event	Date
<a href="#">test.nurturex.co</a>	shunjiro@nurturex.co	ALLOW	Jun 5 2023 • 11:29:21
<a href="#">test.nurturex.co</a>	shunjiro@nurturex.co	ALLOW	Jun 5 2023 • 11:29:21
<a href="#">test.nurturex.co</a>	shunjiro@nurturex.co	ALLOW	Jun 5 2023 • 11:29:21

# DNSフィルタリングの設定

## 4. 推奨ポリシーの設定

## 5. 個別ポリシーの設定 (オプション)

### Create a DNS policy

Create DNS policies to filter your users DNS queries. Gateway will evaluate all DNS queries against your policy criteria.

[Learn more](#)

#### STEP 1

##### Name your policy

Policy name (Required)

Block malware

Description

#### STEP 2

##### Build an expression

Set your policy's scope by adding conditions within expression groupings. Conditions can be joined with logical operators 'AND' or 'OR.' If Traffic conditions join query and response attributes, the policy will evaluate on response.

##### Traffic

Selector (Required)

Select...

Operator (Required)

Select...

Value

Choose a selector and an operator first

Application

Authoritative Nameserver IP

Content Categories

DNS CNAME Response Value

DNS MX Response Value

DNS PTR Response Value

## ネットワークフィルタリングの設定

1. Zero Trustダッシュボードから、Settings > Networkをクリック
2. TCPのProxyを有効化されていることを確認 (必要に応じてUDP, ICMPも有効化)

### Firewall

#### Proxy

Forward traffic to Gateway to filter both outbound traffic as well as traffic directed to resources connected via a Cloudflare Tunnel, GRE tunnel, and/or IPsec tunnel.

Enabled 

☒ TCP

☐ UDP

☐ ICMP Beta

#### WARP to WARP Beta

Enable a private connection between any WARP-enrolled devices within your Zero Trust organization. Traffic security can be managed through Gateway network policies.

Disabled 

## ネットワークフィルタリングの設定

3. Zero Trustダッシュボードから、Settings > Networkをクリック
4. Gateway Network logsに対して activity loggingを有効化
5. ブラウザから任意のURLにアクセスし、Networkのログが取得されていることを確認する。

### Gateway Logging

#### Activity logging

Log DNS queries, network packets, and/or HTTP requests.

Enabled 

#### Gateway DNS logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

#### Gateway Network logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

#### Gateway HTTP logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

# ネットワークフィルタリングの設定

## Gateway activity logs

Monitor individual DNS queries, network packets, and HTTP requests inspected by Gateway. You can also download encrypted SSH command logs for sessions proxied by Gateway.

[Learn more](#)

[DNS](#) [Network](#) [HTTP](#) [SSH](#)

### Your network logs Showing 1 - 50

View and filter your network traffic. By default, Gateway logs all events, including those that are allowed and not a risk.

[Hide filters](#)

Email	Action	Policy	Virtual Network	Date Time Range
<input type="text" value="shunjiro@nurturex.co"/>	<input type="text" value="All Actions"/>	<input type="text" value="All Policies"/>	<input type="text" value="All Networks"/>	<input type="text" value="Jun 5th 13:18 → Jun 5th 14:18"/>
<input type="button" value="Apply filters"/>	<input type="button" value="Clear filters"/>			

Source IP	Destination IP	Action	Session ID	Time
60.87.88.128	2600:9000:2367:5c00:b:2c2f:2e80:93a1	ALLOW	192B84C89200...	Jun 5 2023 • 14:18:05
60.87.88.128	23.46.229.98	ALLOW	192B899F7A00...	Jun 5 2023 • 14:17:57
60.87.88.128	104.119.246.150	ALLOW	192B96A43200...	Jun 5 2023 • 14:17:55

# ネットワークフィルタリングの設定

## 4. 個別ポリシーの設定 (オプション)

### Create a network policy

Create Gateway network policies to filter network traffic against your policy criteria. Note: To enable network policies, proxy must be enabled in account settings.

[Learn more](#)

#### STEP 1

##### Name your policy

Policy name (Required)

Block ports

Description

#### STEP 2

##### Build an expression

Set your policy's scope by adding conditions within expression groupings. Conditions can be joined with logical operators 'AND' or 'OR.'

##### Traffic

Selector (Required)

Select...

Operator (Required)

Select...

Value

Choose a selector and an operator first

##### Application

Destination Continent IP  
Geolocation

Destination Country IP  
Geolocation

##### IP

Destination IP

## HTTPフィルタリングの設定

1. Zero Trustダッシュボードから、Settings > Networkをクリック
2. TLS decryptionを有効化

### TLS decryption

Inspect encrypted HTTP traffic. All HTTPS traffic will be decrypted and re-signed with a new root certificate authority. You must install this CA on devices for your users to continue accessing the Internet. To install the CA [enable "Install CA to system certificate store"](#) or follow the [installation instructions](#) in our Developer Documentation.

Enabled 

☐ Enable only cipher suites and TLS versions compliant with FIPS 140-2.

## HTTPフィルタリングの設定

※以下で説明されている通り、TLS decryptionを指定された場合、いくつかのアプリケーションとの通信が阻害される可能性があります。

その際には、1) untrusted certificate actionをPass throughに設定する、もしくは、2) Do not inspectをアクション指定したGatewayポリシーの作成が対応案としてあげられます。

参照) [Cloudflare Docs - TLS description](#)

参照) [Cloudflare Docs - Do not inspect applications](#)

## HTTPフィルタリングの設定

3. Gateway HTTP logsに対して activity loggingを有効化
4. ブラウザから任意のURLにアクセスし、HTTPのログが取得されていることを確認する。

### Gateway Logging

#### Activity logging

Log DNS queries, network packets, and/or HTTP requests.

Enabled 

#### Gateway DNS logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

#### Gateway Network logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

#### Gateway HTTP logs

- ☒ Capture all
- ☐ Capture only blocked
- ☐ Don't capture

# HTTPフィルタリングの設定

## Gateway activity logs

Monitor individual DNS queries, network packets, and HTTP requests inspected by Gateway. You can also download encrypted SSH command logs for sessions proxied by Gateway.

[Learn more](#)

DNS   Network   **HTTP**   SSH

### Your HTTP logs Showing 1-3 of 3

View and filter your HTTP requests. By default, Gateway logs all events, including HTTP requests that are allowed and not a risk.

[Show filters](#)

Host	Email	Action	Request ID	Time
<a href="#">www.nurturex.co</a>	nurturex-admin@nurturex.co	ALLOW	192bbe585e0000f8afc5142400000001	Jun 5 2023 • 15:01:17
<a href="#">www.nurturex.co</a>	nurturex-admin@nurturex.co	ALLOW	192bbe54580000f8afc5114400000001	Jun 5 2023 • 15:01:16
<a href="#">www.nurturex.co</a>	nurturex-admin@nurturex.co	ALLOW	192bbe3cac0000f8afc4dcf400000001	Jun 5 2023 • 15:01:10

# HTTPフィルタリングの設定

## 5. 推奨ポリシーの設定

## 6. 個別ポリシーの設定 (オプション)

### Create an HTTP policy

Create Gateway HTTP policies to filter HTTP(S) traffic against your policy criteria. Note: To enable HTTPS inspection, decryption must be enabled in account settings.

[Learn more](#)

#### STEP 1

##### Name your policy

Policy name (Required)

Block malware

Description

#### STEP 2

##### Build an expression

Set your policy's scope by adding conditions within expression groupings. Conditions can be joined with logical operators 'AND' or 'OR.' If Traffic conditions join request and response attributes, the policy will evaluate on response

##### Traffic

Selector (Required)

Select...

Operator (Required)

Select...

Value

Choose a selector and an operator first

##### Application

Content Categories

Destination Continent IP  
Geolocation

Id

Destination Country IP  
Geolocation

## SWGの設定

1. Firewall Policyの設定
2. **Egress Policy**の設定
3. Resolver Policyの設定
4. DNS Locationsの設定
5. Proxy Endpointの設定

## Egress Policyの設定

Egress Policyを定義いただく場合には、"Dedicated Egress IP"をお買い求めいただく事が前提となります。

"Dedicated Egress IP"がお客様のご利用環境に割り当てられた後、Egress Policyを設定いただくことで、特定の通信に対して、指定のEgress IPから通信をアウトバウンドさせる事が可能となります。

参照) [Cloudflare Docs - Egress policies](#)

# Egress Policyの設定

## Create an Egress policy

Use the egress policy builder to define your preferred egress methods.

[Learn more](#)

### STEP 1

#### Name your policy

Policy name (Required)

Egress via Chicago

Description

### STEP 2

#### Build an expression

Set your policy's scope by adding conditions within expression groupings. Conditions can be joined with logical operators 'AND' or 'OR'.

##### Traffic

Add **Traffic** conditions to filter traffic based on IPs, destinations, locations, categories, and more.

[+ Add condition](#)

##### Identity

Add **Identity** conditions to filter outbound traffic at the user identity level. These conditions require deployment of the WARP client.

[+ Add condition](#)

##### Device Posture

Add **Device Posture** conditions to use signals from end-user devices to secure access to internal and external resources.

[+ Add condition](#)

### STEP 3

#### Select an egress IP

Your secondary IPs will only be used if your primary IP is rerouted.

- ☒ Use default Cloudflare egress method  
☐ Use dedicated Cloudflare egress IPs

## SWGの設定

1. Firewall Policyの設定
2. Egress Policyの設定
3. **Resolver Policyの設定**
4. DNS Locationsの設定
5. Proxy Endpointの設定

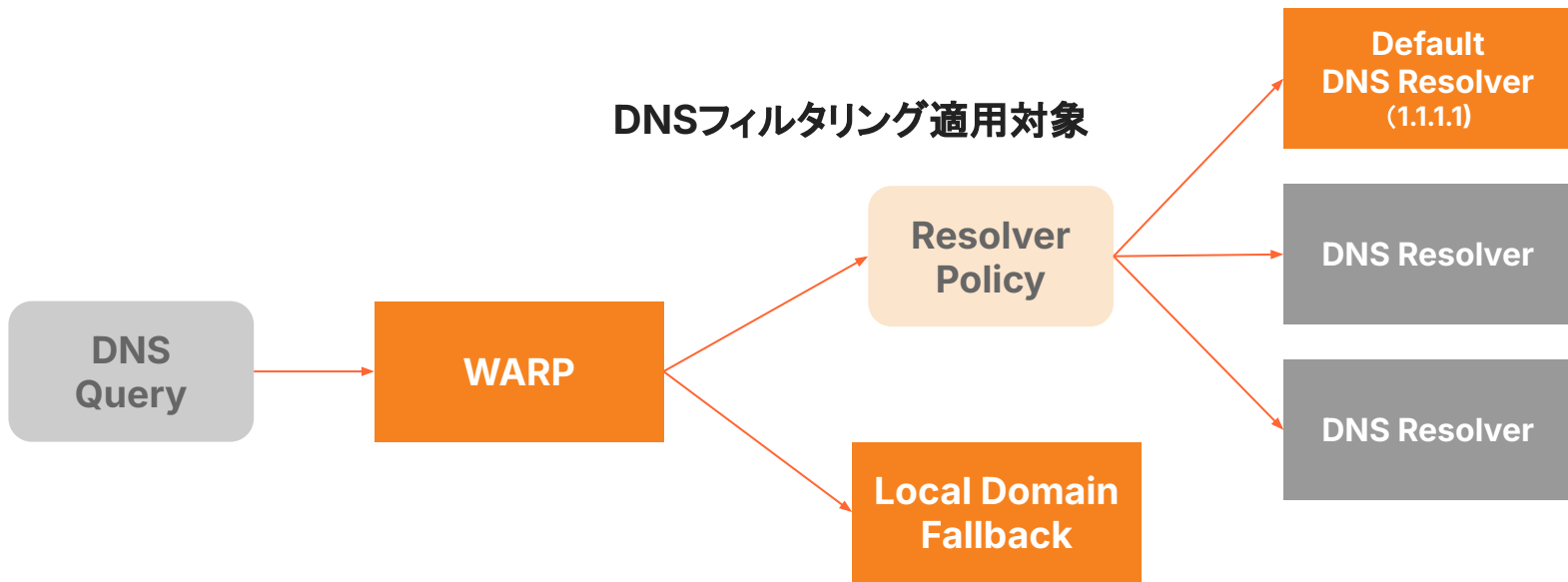
## Resolver Policyの設定

Resolver Policyを定義いただくことで、通信ごとに適用させるDNS Resolverを切り替える事が可能となります。

Resolver Policyがリリースされるまでは、Local Domain Fallbackを用いることで、所定のドメイン上のホストへのアクセスに対して、内部DNSによる名前解決を適用させる事が行われてきましたが、その場合にはCloudflare Zero Trustで設定されたDNSフィルタリングが適用されない状態にあり、Resolver Policyをご利用いただくことで、名前解決に用いるレゾルバーを切り替えながら、DNSポリシーを適用させる事が可能となります。

参照) [Cloudflare Docs - Resolver policies](#)

## Resolver Policyの設定



DNSフィルタリング適用対象外

# Resolver Policyの設定

## Create Resolver policy

STEP 1

### Name your policy

Policy name (Required)

Block malware

Description

STEP 2

### Build an expression

Set your policy's scope by adding conditions within expression groupings. Conditions can be joined with logical operators 'AND' or 'OR.'

#### Traffic

Add **Traffic** conditions to filter traffic based on IPs, destinations, locations, categories, and more.

[+ Add condition](#)

#### Identity

Add **Identity** conditions to filter outbound traffic at the user identity level. These conditions require deployment of the WARP client.

[+ Add condition](#)

STEP 3

### Select DNS resolver [Learn more](#)

Choose the default 1.1.1.1 DNS resolver or add custom resolvers for matched DNS queries.

☒ Use default 1.1.1.1 DNS resolver

☐ Configure custom DNS resolvers

Add up to 10 IPv4 and/or up to 10 IPv6 addresses. DNS queries will route to the address closest to their origin.

## SWGの設定

1. Firewall Policyの設定
2. Egress Policyの設定
3. Resolver Policyの設定
4. **DNS Locations**の設定
5. Proxy Endpointの設定

## DNS Locationsの設定

DNS Locationsを定義いただくことで、例としてWARPをインストールしない端末 (agentless) のレゾルバーに、定義されたDNS Locationsのエンドポイントを指定いただくことで、ホスト名の名前解決処理にあたり、DNSフィルタリングを適用させる事が可能となります。

参照) [Cloudflare Docs - Add locations](#)

# DNS Locations の設定

## Default Location

Configure your DNS location. Then, follow the setup instructions to change the DNS resolvers on your router, browser, or OS.

[DNS endpoints](#) [Endpoint protection](#) [Setup instructions](#)

Location name (Required)

Default Location

### Select DNS endpoints

DNS endpoints serve as the point of resolution for DNS queries. Toggle on at least one endpoint for Cloudflare to assign to this location. [Endpoint documentation](#).

IPv4 DNS



IPv6 DNS



DNS over TLS (DoT)



DNS over HTTPS (DoH)



 Default locations require the DoH endpoint.

## SWGの設定

1. Firewall Policyの設定
2. Egress Policyの設定
3. Resolver Policyの設定
4. DNS Locationsの設定
5. **Proxy Endpointの設定**

## Proxy Endpointの設定

Proxy Endpointを定義いただくことで、例としてWARPをインストールしない端末(agentless)のPACファイルに、定義されたProxy Endpointを指定することで、HTTPフィルタリングを適用させる事が可能となります。

参照) [Cloudflare Docs - Enable Gateway proxy with PAC files](#)

# Proxy Endpointの設定

## proxy-test

Name

proxy-test

### Source IP Address

Gateway will only proxy traffic from these IP addresses.

IPv4 or IPv6

CIDR

IPv4 or IPv6

CIDR

[Remove](#)

IPv4 or IPv6

CIDR

[Remove](#)

IPv4 or IPv6

CIDR

[Remove](#)

[+ Add IP](#)

### Proxy Endpoint

Use this proxy endpoint in a PAC file or your proxy configuration

Copy

[Developer Docs](#) [↗](#)

# Cloudflare CASBの機能および設定

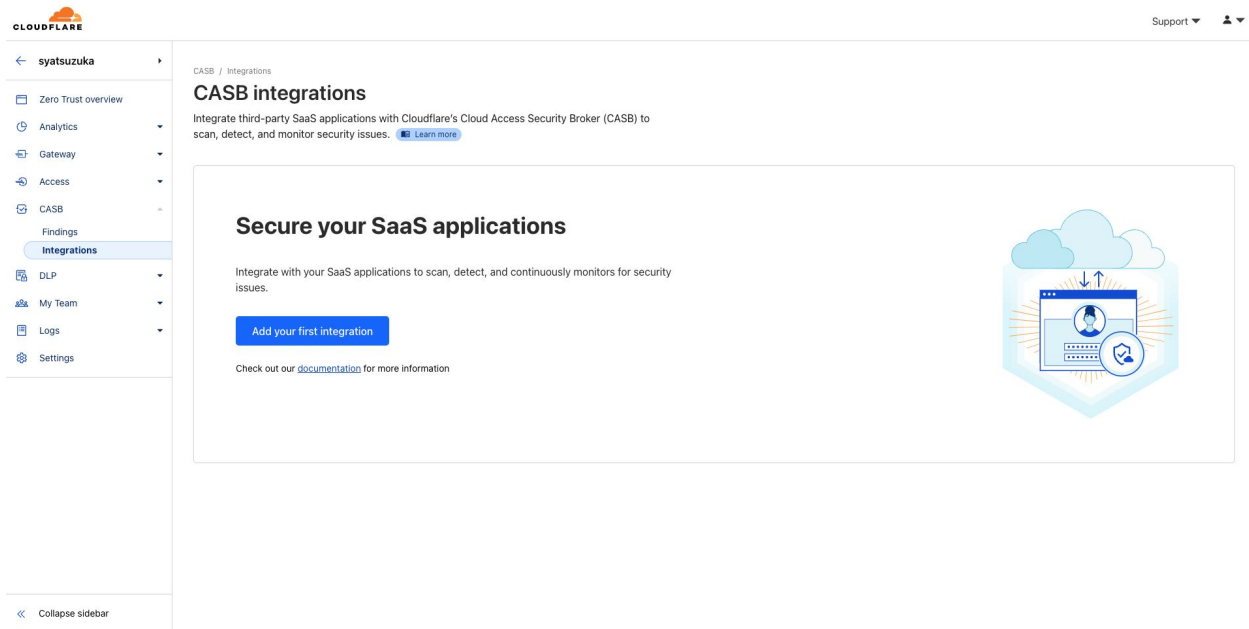
1. はじめに
2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
- 4. Cloudflare CASBの機能および設定**
5. Cloudflare DLPの機能および設定
6. Q&A

## CASBの設定

1. Integrationの追加
2. Integrationの中断・削除

## Integrationの追加

1. Zero Trustダッシュボードから、CASB > Integrationsをクリック
2. Add integrationをクリック



## Integrationの追加

3. 利用可能なSaaSとのIntegrationを選択の上、Addをクリック
4. インストラクションに従い画面操作を進め、Saveボタンをクリック

### Add a CASB Integration

Before integrating your application with CASB, confirm your SaaS account and permissions meet key requirements.

[Learn more](#)

#### Select an application

 Box Atlassian Confluence Dropbox Github Google Workspace Atlassian Jira Microsoft Salesforce Slack

### Github

Before integrating your application with CASB, confirm your SaaS account and permissions meet key requirements.

[Learn more](#)

#### About

Identify important security issues across your GitHub organization, including repository and account misconfigurations, overpermissive user access, best practices not followed, and more.

#### Security Findings

This integration looks for the following security findings. Findings highlight anything that may be off in your GitHub environment.

Public repository missing security policy Medium

Repository publicly accessible Critical

Two factor authentication disabled for Github Organization Critical

Github User does not have Two Factor Authentication enabled Medium

Default branch without branch protection rules High

Moderate Vulnerabilities Found in Repository Dependency Medium

High Vulnerabilities Found in Repository Dependency High

Low Vulnerabilities Found in Repository Dependency Low

Repository Has Deploy Key Older Than 180 Days Low

Repository has outside collaborator Medium

# Integrationの追加

## Github

Before integrating your application with CASB, confirm your SaaS account and permissions meet key requirements.

[Learn more](#)

### Create Integration

1 Name your integration

Next

2 Authorize

3 Confirmation

## Github

Before integrating your application with CASB, confirm your SaaS account and permissions meet key requirements.

[Learn more](#)

### Create Integration

✓ Name your integration

2 Authorize

Click "Authorize" to securely connect CASB to Github

Authorize

3 Confirmation

## Integrationの追加

### 5. Finding pageへリダイレクトされ、検出された 이슈を確認できる

※セキュリティ対策がとられた後、次回の自動検査で解消が確認できれば、Active Instancesの表示は自動で消えます。

#### CASB findings

CASB findings are security issues detected within your integrated SaaS applications.

[Learn more](#)

Active Ignored

#### Your active findings Showing 1-2 of 2

Manage detected security issues across your connected SaaS integrations. Click view to learn more about each finding.

[Show filters](#)

<input type="checkbox"/>	Severity	Finding type	Instances	Integration	Date detected
<input type="checkbox"/>	Medium	GitHub Repository has no Default Branch Protection	1	GitHub	Today
<input type="checkbox"/>	High	GitHub Organization 2FA Disabled	1	GitHub	Today

## Integrationの追加

### Two-factor authentication

Requiring an additional authentication method adds another level of security for your organization.

☐ **Require two-factor authentication for everyone in the nurtorex organization.**

Members, billing managers, and outside collaborators who do not have two-factor authentication enabled for their personal account will be removed from the organization and will receive an email notifying them about the change. [Learn more.](#)

Save

### Branch protection rules



#### You haven't protected any of your branches

Define a protected branch rule to disable force pushing, prevent branches from being deleted, and optionally require status checks before merging. [Learn more about protected branches](#)

Add branch protection rule

## CASBの設定

1. Integrationの追加
2. **Integrationの中断・削除**

## Integrationの中断・削除

1. Zero Trustダッシュボードから、CASB > Integrationsをクリック
2. 中断対象とするIntegrationからConfigurationを選択し、Scan for findingsを無効化。もしくは不要であれば同画面からDeleteボタンをクリック

### CASB integrations

Integrate third-party SaaS applications with Cloudflare's Cloud Access Security Broker (CASB) to scan, detect, and monitor security issues. [Learn more](#)

### Your integrations

Manage and monitor the status of your existing integrations.

[+ Add integration](#)

Integration name	Application	Created	Status
<a href="#">GitHub</a>	 GitHub	2023年6月5日 6:29 PM •	 Active 
<a href="#">Slack</a>	 Slack	2023年6月5日 6:17 PM •	 Active <a href="#">Configure</a>

### Scan for findings

When enabled, CASB will actively scan for findings. Disable to pause scanning.



# Cloudflare DLPの機能および設定

1. はじめに
2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
- 5. Cloudflare DLPの機能および設定**
6. Q&A

## DLPの設定

1. **DLP Profileの設定**
2. DLPポリシーの作成
3. DLPログの確認

参照) [Cloudflare Docs - Scan HTTP Traffic with DLP](#)

## DLP Profileの設定

1. Zero Trustダッシュボードから、DLP > DLP Profileをクリック
2. 設定対象のPredefined Profileを選択し、Configureをクリック

### Data Loss Prevention profiles

DLP profiles contain sensitive data detections used to scan uploaded or downloaded files. You can then apply [Gateway HTTP policies](#) to allow or disallow transfer of those files.

[Learn more](#)

#### Your DLP profiles

To use Microsoft Information Protection(MIP) sensitivity labels, add your MIP account through CASB integration.

[Learn more](#)[+ Create profile](#)

Profile name	Profile type	Detection entries enabled	
<a href="#">Credentials and Secrets</a>	PRE-DEFINED	0	<div><div></div><div>Configure</div><div></div></div>
<a href="#">Financial Information</a>	PRE-DEFINED	0	
<a href="#">Social Security, Insurance, Tax, and Identifier Numbers</a>	PRE-DEFINED	0	

## DLP Profileの設定

### 3. 有効化したいDetection Entryを選択の上、Save Profileボタンをクリック

#### Enabled DLP detections

Add existing predefined and integration entries or create new custom entries. Choose which detection entries you want to apply to uploaded or downloaded files through Gateway HTTP policies.

Detection entry	Type	Status
Amazon AWS Access Key ID	Pre-defined	<input checked="" type="checkbox"/>
Amazon AWS Secret Access Key	Pre-defined	<input checked="" type="checkbox"/>
Google GCP API Key	Pre-defined	<input checked="" type="checkbox"/>
Microsoft Azure Client Secret	Pre-defined	<input checked="" type="checkbox"/>
SSH Private Key	Pre-defined	<input checked="" type="checkbox"/>


## DLP Profileの設定

### 4. 必要に応じて、Custom Policyを個別追加

参照) [Cloudflare Docs - Configure a DLP profile](#)

参照) [Cloudflare Docs - Build a custom profile](#)

#### ▼ Add a custom entry

- a. Select **Add custom entry** and give it a name.
- b. In **Value**, enter a regular expression (or regex) that defines the text pattern you want to detect. For example, `test\d\d` will detect the word `test` followed by 2 digits.
  - Regexes are written in Rust. We recommend validating your regex with [Rustexp](#) .
  - Detected text patterns are limited to 1024 bytes in length.
  - Regexes with `+` are not supported as they are prone to exceeding the length limit. For example `a+` can detect an infinite number of a's. We recommend using `a{min,max}` instead, such as `a{1,1024}`.
- c. To save the detection entry, select **Done**.

## DLPの設定

1. DLP Profileの設定
2. **DLPポリシーの作成**
3. DLPログの確認

参照) [Cloudflare Docs - Scan HTTP Traffic with DLP](#)

## DLPポリシーの作成

1. [matched-data-cli](#)をダウンロード
2. ローカルPCでコマンド実行  
\$ ./matched-data-cli generate-key-pair
3. ここで得られたpublic\_keyおよびprivate\_keyは後続の操作で利用するため、メモに取っておく

参照) [Cloudflare Docs - Generate a key pair in the commandline](#)

```
→ matched-data-cli $ ./matched-data-cli generate-key-pair
{
  "private_key": "u[REDACTED]",
  "public_key": "[REDACTED]"
}
```

## DLPポリシーの作成

4. Zero Trustダッシュボードから、  
Setting > Networkをクリック
5. DLP Payload Encryption public keyに前段で確認したpublic keyを入力の上、保存

参照) [Cloudflare Docs - Upload the public key to Cloudflare](#)

### Gateway Logging

#### Activity logging

Log DNS queries, network packets, and/or HTTP requests.

Enabled 

#### Gateway DNS logs

- ☒ Capture all  
☐ Capture only blocked  
☐ Don't capture

#### Gateway Network logs

- ☒ Capture all  
☐ Capture only blocked  
☐ Don't capture

#### Gateway HTTP logs

- ☒ Capture all  
☐ Capture only blocked  
☐ Don't capture

#### Exclude PII

When the feature is enabled, Gateway will log activity without capturing any personally identifiable information. This does not apply to Logpush logs. [Read more about PII in Zero Trust](#)

Disabled 

#### Enable enhanced file detection

Allows inspection and extraction of file information from your traffic. [Learn more](#)

Disabled 

#### SSH Encryption public key

Upload your public key to download SSH logs file. This key will be used to encrypt all SSH logs recorded via SSH command logging.

[Edit](#)

#### DLP Payload Encryption public key

Input your public key to access payload log match data. Your key will be used to encrypt all payload logs recorded via DLP payload logging.

[Edit](#)

## DLPポリシーの作成

6. Zero Trustダッシュボードから、Gateway > Firewall Policies > HTTPをクリック
7. Add a policyボタンをクリック
8. TrafficのSelectorから、DLP Profileを選択
9. Actionを選択

STEP 2

### Build an expression

Set your policy's scope by adding conditions within expression groupings. Conditions can be joined and the policy will evaluate on response

**Traffic**

Selector (Required)	Operator (Required)	Value
Select...	Select...	Choose a selector and
Application		
Content Categories		
Destination Continent IP Geolocation		
Destination Country IP Geolocation		
Destination IP		
<b>DLP Profile</b>		
Domain		

Add **Identity** conditions to filter outbound traffic at the user

+ A

## DLPポリシーの作成

10. Configure policy settingsで"Log the payload of matched rule"をチェック
11. Create a policyボタンをクリック  
→ これでDLPポリシーによるスキャンが開始

STEP 4

### Configure policy settings

Log the payload of matched rule ☒

Surfaces encrypted DLP matches in Gateway activity logs.

### Display block page

Show a custom message to users who attempt to reach a blocked domain.

① To customize the block page message, enable the [custom block page](#) first.

## DLPポリシーの作成

参照) [Cloudflare Docs - Create a DLP policy](#)

参照) [Cloudflare Docs - Common DLP policies](#)

## DLPの設定

1. DLP Profileの設定
2. DLPポリシーの作成
3. **DLPログの確認**

参照) [Cloudflare Docs - Scan HTTP Traffic with DLP](#)

## DLPログの確認

1. Zero Trustダッシュボードから、Logs > Gateway > HTTPをクリック
2. policyもしくはDLP profilesに作成したDLPポリシーもしくは、DLP profileを選択の上、検索  
→ DLPポリシーでブロックされた通信を確認

Email	Action	Method	Policy	Device
<input type="text"/>	Block	All Methods	All Policies	All Devices
Payload is isolated	DLP profiles	Date Time Range		
False	All profiles	Apr 4th 23:37 → Apr 5th 00:37 ×		
<button>Apply filters</button> <a href="#">Clear filters</a>				

Host	Email	Action	Request ID	Time
		BLOCK	1f4b59d2450000734b775a3400000001	Apr 5 2024 • 0:36:03
		BLOCK	1f4b57ef930000734b77042400000001	Apr 5 2024 • 0:34:00
		BLOCK	1f4b57f1c30000734b77044400000001	Apr 5 2024 • 0:34:00

## DLPログの確認

3. 該当レコードの一つを選択し、詳細ビューを表示
4. Decrypt payload logボタンをクリックし、表示されるダイアログでPrivate Keyを入力  
→ 検知対象となった情報を特定するログ情報が表示される

参照) [Cloudflare Docs - View payload logs](#)

### Matched Policies

Policy Name

Test - DLP

Policy ID

[Redacted]

Policy Description

None

DLP profiles

[DLP-test](#)

DLP profile entries

credit number

Uploaded File Name(s)

None

Payload log match

The DLP matched portion of the request has been logged. Enter your private key to decrypt the log.

[Decrypt payload log](#)

[Report DLP false positive](#)

# DLPログの確認

## Enter the private key to decrypt

Private Key (Required)

Enter the private key

\* For security, this key will not persist if you refresh this page or navigate away from the log.

Cancel

Decrypt

## Payload log match

Profiles matched: 1

DLP-test

s="ms-3 p-2 border">xxxxxxxxxxxxxxxxx</p>

Close

## DLPログの確認 - Scan for sensitive data (CASBとの連携)

CASBとDLPをあわせてご利用いただくことで、SaaSアプリケーション上のデータに対して、DLPを適用することで、機密データの漏洩を検知することも可能です。検知された場合には、CASB Findingsおよび、DLPログからその内容をご確認いただけます。

参照) [Cloudflare Blog - Cloudflare CASB とDLPが連携してデータを保護する仕組み](#)

参照) [Cloudflare Docs - Scan for sensitive data](#)

# Q&A

1. はじめに
2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
5. Cloudflare DLPの機能および設定

## 6. Q&A

# Thank you

→ 1 888 99 FLARE

✉ [enterprise@cloudflare.com](mailto:enterprise@cloudflare.com)

🌐 [cloudflare.com](https://cloudflare.com)