



Zscaler Internet Access (ZIA)

基本操作ガイド

Ver.6.2 対応版

Rev.1.2

2023年 4月

ノックス株式会社



- ※ 本出版物の著作権はノックス株式会社が権利を保有しています。本出版物の配布は、Zscaler サービスのサブスクリプション購入者による使用のみを目的としています。
- ※ 本出版物中に用いられている商標については、全て該当する会社が権利を保有しています。
- ※ 当社の許可なく、本出版物の複製・転載・配布を禁じます。
- ※ 本出版物は無保証で提供されるものであり、当社は本製品についてその商品性、特定の目的に対する適合性、使用による権利侵害の不発生を保証するものではなく、かつこれに限定されずいかなる事項についても明示的または暗示的に保証しません。
- ※ 本出版物には技術的内容に関して不適切な部分および誤植部分が含まれている恐れがあります。当社は事前の通知なく本出版物の内容を改訂する場合があります。
- ※ クラウド側のバージョンアップにより設定項目が追加/変更される可能性がございます。予めご了承の程お願いいたします。

Copyright(C)2023ノックス株式会社

目次

1. ZSCALER サービス設定の流れ.....	6
1-1. 概要.....	6
1-2. ZIA サービス設定フロー.....	6
2. ZIA 管理ポータルへのログイン.....	7
2-1. 概要.....	7
2-2. ZIA サービスポータルへのログイン方法.....	7
2-3. COMPANY PROFILE の記入方法.....	8
2-4. ZIA 管理ポータルの管理者設定方法.....	9
2-4-1. 管理者ロールの設定方法.....	9
2-4-2. 管理者の追加方法.....	10
3. WEBトラフィックの転送設定.....	12
3-1. 概要.....	12
3-2. GRE でのトラフィックの転送設定方法.....	12
3-2-1. GRE 接続についての概要.....	12
3-2-2. GRE 設定方法.....	12
3-3. IPSEC でのトラフィックの転送方法.....	14
3-3-1. IPSec 接続についての概要.....	14
3-3-2. IPSec 接続先情報の確認方法.....	14
3-3-3. IPSec 設定方法.....	15
4. ユーザーのプロビジョニングと認証.....	18
4-1. 概要.....	18
4-2. プロビジョニング.....	18
4-3. ユーザー認証.....	18
5. ユーザー、グループ、部署の設定.....	19
5-1. 概要.....	19
5-1-1. ポリシーのルックアップ条件.....	19
5-2. グループの設定方法.....	19
5-3. 部署の設定方法.....	20
5-4. ユーザーの設定方法.....	21

5-4-1.	認証設定	21
5-4-2.	ユーザーの設定方法.....	23
6.	ロケーション設定	24
6-1.	概要.....	24
6-2.	ロケーションの設定方法	24
6-2-1.	静的 IP アドレスの設定方法	24
6-2-2.	ロケーションの設定方法.....	26
7.	ZSCALER サービスへのログイン	27
7-1.	概要.....	27
7-2.	ZSCALER サービスへのログイン方法	27
8.	URL フィルタリングポリシーの設定と動作確認	28
8-1.	概要.....	28
8-1-1.	ポリシーの適用フロー.....	28
8-2.	URL フィルタリングポリシーの設定方法.....	29
8-3.	URL フィルタリングポリシーの設定確認方法.....	30
8-4.	URL フィルタリングポリシーの確認方法.....	30
8-5.	対象サイトの URL カテゴリの確認方法.....	31
8-6.	カスタムカテゴリの設定方法	32
9.	クラウドアプリケーションコントロールポリシーの設定と動作確認	33
9-1.	概要.....	33
9-2.	クラウドアプリケーションコントロールポリシーの設定方法	34
9-3.	クラウドアプリケーションコントロールポリシーの動作確認方法.....	36
10.	SSL インспекションの設定.....	37
10-1.	概要	37
10-1-1.	SSL インспекションの利用条件	37
10-2.	ZSCALER の SSL 証明書の入手方法.....	37
10-2-1.	手動での入手方法.....	37
10-3.	SSL インспекションポリシーの設定方法	38
10-3-1.	SSL インспекションポリシーの設定方法	38
11.	マルウェアプロテクションの設定.....	40
11-1.	概要	40
11-2.	マルウェアプロテクションの設定方法.....	40
11-3.	アンチウイルス保護の確認方法	41

本書について

本書は Zscaler の導入時にスムーズに設定が行えることを目指した導入マニュアルです。

本書は基本的な設定・流れの把握を目的としています。また、難解さを極力避けるようにしていますので、一部内容に関して不足や補足が必要な個所がある場合がありますが、本書の趣旨をご理解の上、ご利用いただきますようお願い申し上げます。

なお、詳細な内容解説については、恐れ入りますが英語版の各種ドキュメントおよびヘルプをご参照くださいますようお願い申し上げます。

ヘルプページ：<https://help.zscaler.com/>

Zscaler Config：<https://config.zscaler.com/zscaler.net/cenr>

サポートバージョン：<https://help.zscaler.com/eos-eol/supported-versions>

障害/メンテナンス情報など：<https://trust.zscaler.com/zscaler.net>

Zscaler への接続状況の確認：<https://ip.zscaler.com/>

1. Zscaler サービス設定の流れ

1-1. 概要

Zscaler Internet Access(ZIA)サービスの利用手順を説明します。

1-2. ZIA サービス設定フロー



2. ZIA 管理ポータルへのログイン

2-1. 概要

ZIA サービスポータルへのログイン方法、利用情報の入力方法を説明します。

2-2. ZIA サービスポータルへのログイン方法

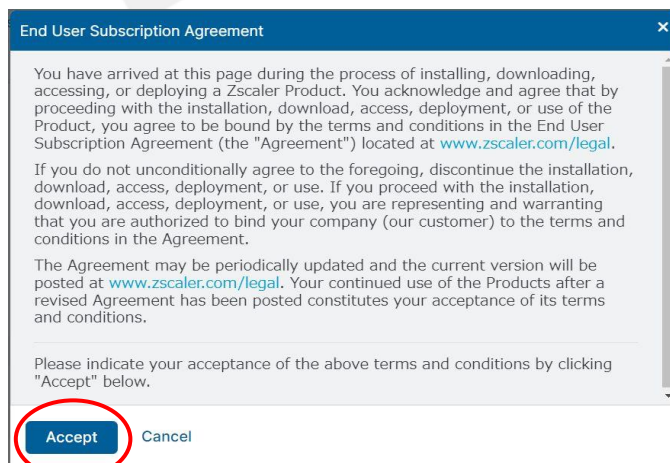
(1) 弊社からご連絡した URL ログイン ID、パスワードを使用して Zscaler サービスポータルへログインします。ポータルサイトの URL は「admin.zscalerthree.net」(※)です。

(※)admin.zscalerthree.net の赤字部分は、ご契約のクラウド名を入力してください。



(2) 初回ログイン時は以下の The End User Subscription Agreement (EUSA) が表示されるので、「Accept」をクリックします。

「Cancel」を選択した場合もサービスを継続し、ポリシー設定やユーザー追加は可能ですが、EUSA の承認を行うまでは設定が有効化されず Zscaler サービスを経由したインターネットの接続はできません。



2-3. Company Profile の記入方法

- (1) ZIA 管理ポータルを開きます。
- (2) 左側メニューより「管理」→「設定」→「会社情報」を選択します。
- (3) 使用者の情報を入力し、保存をクリックします。

会社情報

組織 サブスクリプション

概要

企業ID
zscaler.net-

名前
NOX Partner Only - II

ドメイン

アドレス1
Your company HQ location address

アドレス2
テキストを入力

市
City

県
State

郵便番号
100100

保存 キャンセル

2-4. ZIA 管理ポータルでの管理者設定方法

2-4-1. 管理者ロールの設定方法

- (1) ZIA 管理ポータルを開きます。
- (2) 左側メニューより「管理」→「認証」→「ロール管理」より、管理者に与えられる権限を設定します。
- (3) 「追加管理者のロール」をクリックします。



- (4) 管理者に与える権限を選択し、「保存」をクリックします。



以下では、それぞれのメニューを表示するか、非表示にするかを選択します。



(5) 左側メニューより「有効化」を実施します。

2-4-2. 管理者の追加方法

(1) ZIA 管理ポータルを開きます。

(2) 左側メニューより「管理」→「認証」→「管理者のマネジメント」を選択し、「追加管理者」をクリックします。



(3) 必要項目を設定します。

追加 管理者

管理者

ログインID
demc| @

Email
テキストを入力

名前
テキスト

ロール
NONE

ステータス
有効

範囲
組織

エグゼクティブ解析アプリアクセス

コメント

アップデート受信を選択する

セキュリティアップデート

サービスアップデート

プロダクトアップデート

保存 キャンセル

2-4-1 で設定したロールから選択します。「Super Admin」は全権限が与えられているロールです。

管理者が管理できる範囲をロケーション、部署単位で選択します。すべてのユーザー範囲で適用する場合は「組織」を選択します。

(4) 左側メニューより「有効化」を実施します。

3. Web トラフィックの転送設定

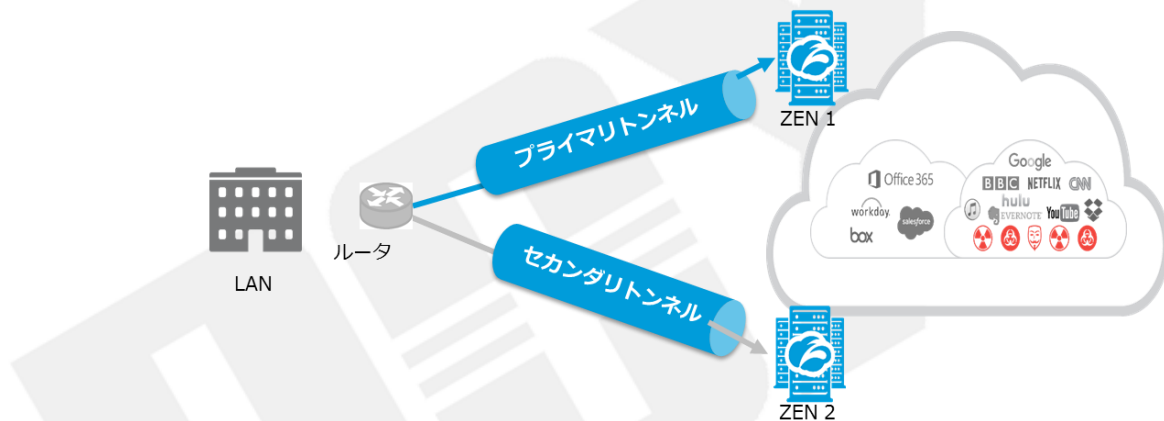
3-1. 概要

Zscaler サービスを使用するために、管理対象の Web トラフィックを Zscaler クラウドに転送します。以下は Zscaler への Proxy 方法です。

- PAC ファイル
- GRE/VPN Tunnel でのフォワーディング
- Zscaler Client Connector【ZCC】(Zscaler が提供するエージェントソフト)

3-2. GRE でのトラフィックの転送設定方法

3-2-1. GRE 接続についての概要



社内ゲートウェイの機器(ルーター)にて、ZEN へ GRE トンネルを接続します。上図のように、ZEN 障害に対応するためにプライマリとセカンダリの冗長構成にて接続してください。

3-2-2. GRE 設定方法

- (1) ZIA 管理ポータル「管理」→「静的 IP と GRE トンネル」→「GRE トンネル」のタブを開きます。
- (2) 「追加 GRE トンネル」をクリックします。



- (3) 送信元 IP を「静的 IP アドレス」プルダウンを開き選択し、「次へ」をクリックします。
(ZIA 管理ポータル→「管理」→「静的 IP アドレスと GRE トンネル」→「静的 IP」より登録したものが表示される形となっております。)

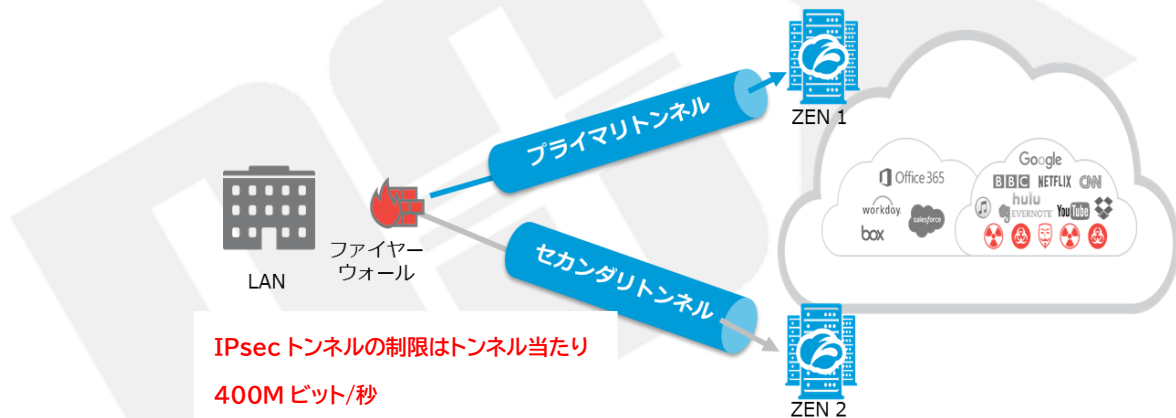
(4)「プライマリデータセンターVIP」と「セカンダリデータセンターVIP」をプルダウンより選択します。
 (「推奨」と記載があるものを選択することが一般的です。)

(5)「内部 GRE IP 範囲」を選択し、「次へ」をクリックします。

(6) 設定内容を確認し、「保存」をクリックします。

3-3. IPSec でのトラフィックの転送方法

3-3-1. IPSec 接続についての概要



社内ゲートウェイの機器(ファイアーウォール)にて、ZENへIPsecVPNトンネルを接続します。上図のように、ZEN 障害に対応するためプライマリとセカンダリの冗長構成にて接続してください。IPsec 接続は、Aggressive モード(動的 IP)および Main モード(固定 IP)での接続が可能です。

IPsecトンネルの制限は、トンネルあたり400Mbps です。

3-3-2. IPSec 接続先情報の確認方法

以下 URL より、設置拠点に近い接続先の VPN Host Name を確認し、VPN装置から接続してください。

<https://config.zscaler.com/zscalerthree.net/cenr>

※<https://config.zscaler.com/zscalerthree.net/cenr> の赤字部分は管理ポータル URLのクラウド名を入力してください。

3-3-3. IPSec 設定方法

- (1) ZIA 管理ポータルを開き、「管理」→「VPN 属性」を開きます。
- (2) 「追加 VPN 属性」をクリックします。

Aggressive Mode の場合

VPN属性

認証タイプ: FQDN IP ステータス: 有効

ユーザーID: demo @ ドメインを選択します。

新しい事前共有鍵: 新しい事前共有鍵 (確認):

コメント: Pre-Shared Key を設定します。

保存 キャンセル

Main Mode の場合

認証タイプ: FQDN IP ステータス: 有効

IPアドレス: 219.127. IP を選択します。 IP アドレスを選択しま

新しい事前共有鍵: 新しい事前共有鍵 (確認):

コメント: Pre-Shared Key を設定します。

保存 キャンセル

- (3) ZIA 管理ポータルの「管理」→「ロケーショングループ」を選択し、「追加ロケーション」をクリックします。
- (4) 設定内容を入力し、「保存」をクリックします。

国とタイムゾーンを入力

名前
demo

市町村/県/州
テキストを入力

マニュアルロケーショングループ
なし

マニュアルロケーショングループから除外

ロケーションタイプ
Corporate user traffic

Static IP Addresses and GRE Tunnels
219.127.

プロキシポート
なし

仮想ZEN
なし

CC
日本

タイムゾーン
アジア/東京

動的ロケーショングループ

動的ロケーショングループから除外

VPN属性
219.127.

仮想ZENクラスター
なし

IP アドレスを選択します。
(Aggressive Mode の場合は設定不要です。)

(2)にて作成した VPN 属性を選択します。

IPSec 機器にて IPSec の設定を行ってください。

設定例

Cisco ASA

[IPSec VPN Configuration Guide for Cisco ASA 55xx | Zscaler](#)

Cisco ISR

[IPSec VPN Configuration Guide for Cisco 881 ISR | Zscaler](#)

Juniper SRX

[IPSec VPN Configuration Guide for Juniper SRX | Zscaler](#)

Juniper SSG20

[IPSec VPN Configuration Guide for Juniper SSG 20 | Zscaler](#)

Fortigate

[IPSec VPN Configuration Guide for FortiGate Firewall | Zscaler](#)

Paloalto

[IPSec VPN Configuration Guide for Palo Alto Networks Firewall | Zscaler](#)

SonicWall TZ100

[IPSec VPN Configuration Guide for SonicWall TZ 100 | Zscaler](#)

SonicWall TZ350

[IPSec VPN Configuration Guide for SonicWall TZ 350 | Zscaler](#)

サポートパラメータ等 参考情報

[Understanding IPSec VPNs | Zscaler](#)



4. ユーザーのプロビジョニングと認証

4-1. 概要

Zscaler ではユーザー/グループ/部署単位のルールを適用できるので、ユーザーごとのアクセスログを記録するために Zscaler クラウド上に利用ユーザー用のアカウント情報の展開が必要になります。利用時にユーザーID・パスワードを基本とする認証が必要で、プロビジョニングと認証それぞれどのように実現するか検討が必要です。

4-2. プロビジョニング

以下のいずれかの方法で Zscaler 上にユーザー情報を展開します。

- ・手動管理
- ・CSV アップロード
- ・SCIM
- ・SAML(要ユーザーID、部署、グループ)

4-3. ユーザー認証

以下のいずれかの方法でクライアント端末を認証します。

- ・ローカル DB(Zscaler 上)
- ・One-Time Password/Link
- ・SAML

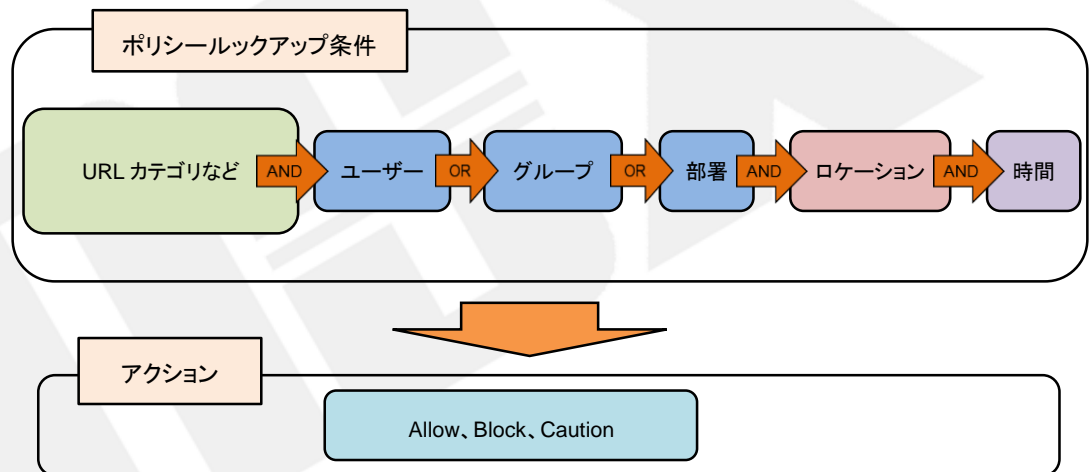
5. ユーザー、グループ、部署の設定

5-1. 概要

ユーザーベースでのポリシーを実装し、サービスの詳細なレポート機能を活用するには、Zscaler データベースでユーザーを設定し、Zscaler サービスでそれらを認証に使用できるようにする必要があります。ロケーション登録(グローバル IP の登録)をした拠点ではユーザーの設定と認証は必須ではありませんが、有効にすることを強く推奨します。ユーザー設定では、ユーザー名、グループおよび部署の設定が必要です。認証を有効にすることで、部署、グループおよびユーザーに対してポリシーを適用したり、ユーザーおよび部署のログとレポートを提供したりすることができます。本項では、グループ、部署、ユーザーの設定方法を説明します。

5-1-1. ポリシーのルックアップ条件

ポリシーのルックアップは以下の条件で実施されます。



5-2. グループの設定方法

- (1) ZIA 管理ポータルを開き、「管理」→「ユーザー管理」をクリックします。
- (2) 「Groups」のタブを開き、「追加グループ」をクリックします。



(3)「追加グループ」ウィンドウに必要情報を入力し、「保存」をクリックします。

(※)CSV形式でグループ情報をインポートおよびエクスポートすることができます。

5-3. 部署の設定方法

(1) ZIA 管理ポータルを開き、「管理」→「ユーザー管理」をクリックします。

(2)「部署」のタブを開き、「追加部署」をクリックします。

(3)「追加部署」ウィンドウに必要情報を入力し、保存をクリックします。

(※)CSV形式で部署情報をインポートおよびエクスポートすることができます。



5-4. ユーザーの設定方法

ユーザー情報は、内部データベースでの運用以外にも「Active Directory」や「Open LDAP」との連携が可能です。本書では内部データベースでの運用方法について説明します。

5-4-1. 認証設定

ZIA 管理ポータル「管理」→「認可」から認証プロファイルを設定します。

A screenshot of the ZIA '認可' (Authorization) settings page. The page title is '認可'. There are three tabs: '認証プロファイル' (Authentication Profile), 'IDプロバイダー' (ID Provider), and '認証ブリッジ' (Authentication Bridge). The '認証プロファイル' tab is selected. Below the tabs, there are several settings sections: 'ユーザーリポジトリタイプ' (User Repository Type) with buttons for '内部DB' (Internal DB), 'Active Directory', and 'OpenLDAP'; '認証頻度' (Authentication Frequency) with a dropdown menu set to 'セッションごと' (Per Session); '認証タイプ' (Authentication Type) with buttons for 'フォームベース' (Form-based) and 'SAML'; '一時的な認証' (Temporary Authentication) with buttons for '無効' (Disabled), 'ワンタイムトークン' (One-time Token), and 'ワンタイムリンク' (One-time Link); 'パスワードの強度' (Password Strength) with a dropdown menu set to 'メディア' (Medium); 'Password expiry' with a dropdown menu set to 'なし' (None); and 'KERBEROS認証' (Kerberos Authentication) with a checkbox for 'Kerberosを有効化' (Enable Kerberos) which is currently unchecked. At the bottom, there are two buttons: '保存' (Save) and 'キャンセル' (Cancel).

- ・認証頻度 ユーザーが Zscaler サービスの認証を受ける頻度を選択します。
(ZCC を利用しない場合に有効な設定です)
- ・パスワードの強度 None:パスワードの強度に制限を設けません。
Medium:8 文字以上、英字以外の文字を少なくとも 1 つ含む
Strong:8 文字以上、数字、英字大文字、特殊文字を含む
※ASC II のみ使用可能
- ・Password expiry パスワードの有効期限を選択します。
- ・一時的な認証 ユーザーが Zscaler サービスへの 1 回のログインに使用できるリンクまたは一時的なパスワードをメールで送信するように設定が可能です。
新しいユーザーを作成したり、忘れたパスワードをリセットしたりする際に使用します。

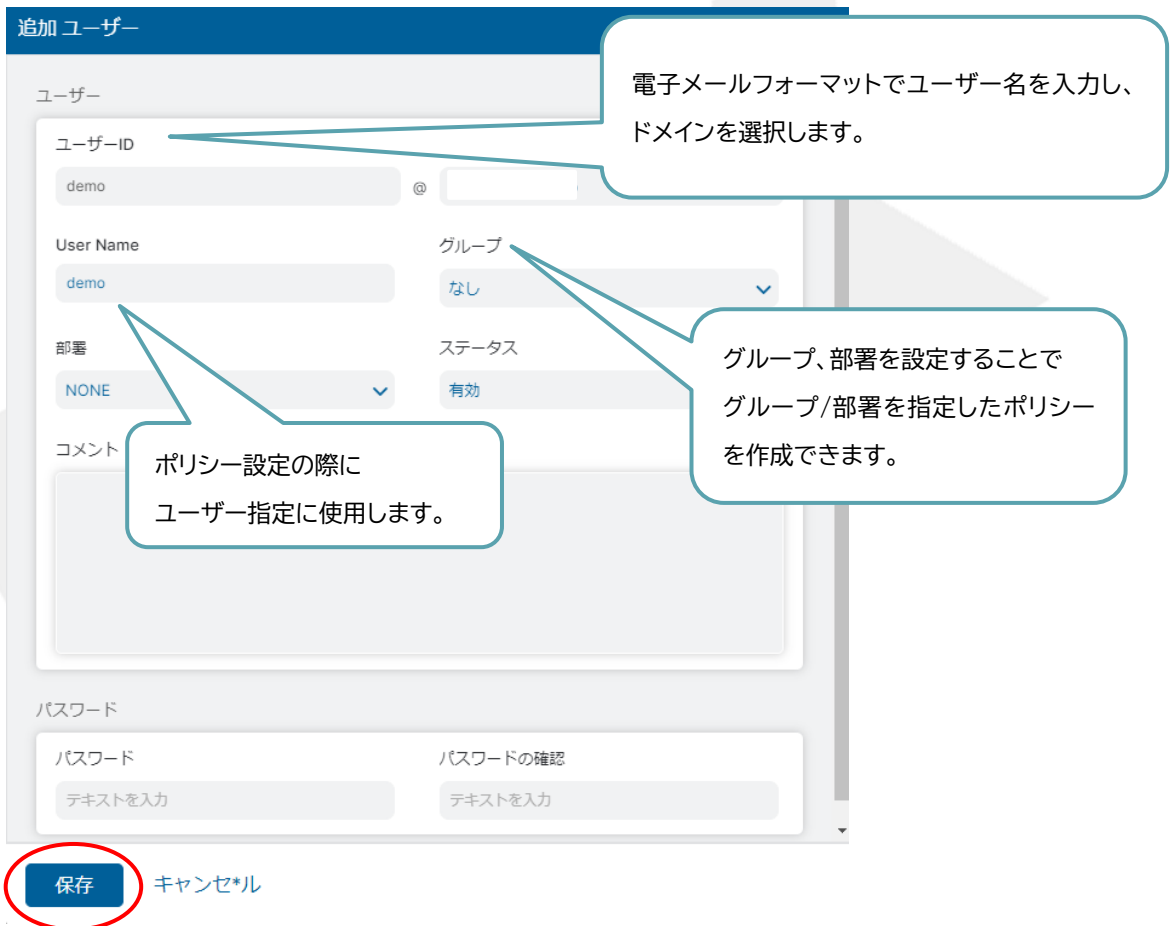
ワンタイムトークン:一時パスワード
ワンタイムリンク:一時リンク
※リンク、パスワード共に 24 時間有効となります。

5-4-2. ユーザーの設定方法

- (1) ZIA 管理ポータルを開き、「管理」→「ユーザー管理」をクリックします。
- (2) 「ユーザー」のタブを開き、「追加ユーザー」をクリックします。



- (3) 「追加ユーザー」ウィンドウに必要情報を入力し、「保存」をクリックします。



- (4) ZIA 管理ポータル左側のメニューより「有効化」を実施します。

(※)CSV 形式でユーザー情報をインポート及びエクスポートすることができます。



6. ロケーション設定

6-1. 概要

ロケーションを設定することにより、ロケーションベースのポリシー適用やレポート機能を活用することができます。拠点のグローバル IP アドレスを登録したものがロケーションとなります。

本項では、ロケーションの設定方法を説明します。

6-2. ロケーションの設定方法

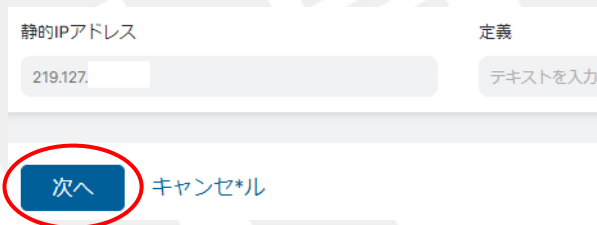
6-2-1. 静的 IP アドレスの設定方法

(1) ZIA 管理ポータルを開き、「管理」→「静的 IP と GRE トンネル」をクリックします。

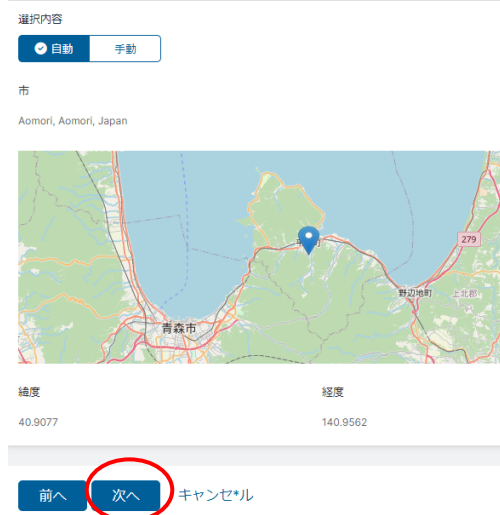
(2) 「静的 IP」のタブを開き、「追加 静的 IP」をクリックします。



(3) 「静的 IP アドレス」を入力し、「次へ」をクリックします。



(4) 地域を選択します。「自動」で正しい場合は「次へ」をクリックします。



正しくない場合は、「手動」を選択し、「市」を入力し「次へ」をクリックします。

選択内容

自動 手動

市

Tokyo, Tokyo, Japan

緯度 35.6839 経度 139.762 都市を更新

前へ 次へ キャンセル

(5) 入力内容を確認し、「保存」をクリックします。

追加 静的IPの設定

1 送信元IP 2 地域 3 レビュー

静的IPアドレス
219.127

定義

IPリージョン	緯度
Tokyo, Tokyo, Japan	35.6839
経度	
139.762	

前へ 保存 キャンセル

6-2-2. ロケーションの設定方法

- (1) ZIA 管理ポータルを開き、「管理」→「ロケーショングループ」をクリックし、「ロケーション」のタブを開き、「追加ロケーション」をクリックします。
- (2) 設定内容を入力し、「保存」をクリックします。

The screenshot shows the 'ロケーション' (Location) configuration page in the ZIA management portal. On the left, there is a menu with traffic types: Corporate user traffic, Guest Wi-Fi traffic, IoT traffic, and Server traffic. The main configuration area includes:

- 名前 (Name):** A text input field with a callout: "国とタイムゾーンを選択します。" (Select country and time zone).
- 市町村/県/州 (City/Town/Village/County/State):** A text input field.
- タイムゾーン (Time Zone):** A dropdown menu currently set to 'NONE'.
- マニュアルロケーショングループ (Manual Location Group):** A dropdown menu set to 'なし' (None).
- 動的ロケーショングループ (Dynamic Location Group):** A dropdown menu set to '---'.
- マニュアルロケーショングループから除外 (Exclude from Manual Location Group):** A checkbox that is unchecked.
- 動的ロケーショングループから除外 (Exclude from Dynamic Location Group):** A checkbox that is unchecked.
- ロケーションタイプ (Location Type):** A dropdown menu set to 'NONE' with a callout: "トラフィックのタイプを選択します。" (Select traffic type).

The 'アドレス' (Address) section includes:

- Static IP Addresses and GRE Tunnels:** A dropdown menu set to 'なし' (None) with a callout: "グローバル IP を選択します。" (Select global IP).
- プロキシポート (Proxy Port):** A dropdown menu set to 'なし' (None).
- VPN属性 (VPN Attribute):** A dropdown menu set to 'なし' (None).
- 仮想ZEN (Virtual ZEN):** A dropdown menu set to 'なし' (None).
- 仮想ZENクラスタ (Virtual ZEN Cluster):** A dropdown menu set to 'なし' (None).

The 'ゲートウェイオプション' (Gateway Options) section includes:

- クライアントリクエストからのXFFを使用 (Use XFF from client requests):** An unchecked checkbox.
- 認証を適用 (Apply authentication):** An unchecked checkbox with a callout: "ロケーションからの通信に対して認証の適用の有無を選択します。認証ありの場合、ユーザー識別が可能です。" (Select whether to apply authentication for communication from the location. If authentication is enabled, user identification is possible).
- 警告を有効化 (Enable warnings):** An unchecked checkbox.
- AUPを有効化 (Enable AUP):** An unchecked checkbox.
- ファイアウォールコントロールを適用 (Apply firewall control):** An unchecked checkbox.

The '帯域幅コントロール' (Bandwidth Control) section includes:

- 帯域幅コントロールを適用 (Apply bandwidth control):** A toggle switch currently set to '無効' (Disabled).

At the bottom, there are two buttons: '保存' (Save) and 'キャンセル' (Cancel). The '保存' button is circled in red.

- (3) ZIA 管理ポータル左側のメニューより「有効化」を実施します。

7. Zscaler サービスへのログイン

7-1. 概要

Zscaler サービスへのログイン方法を説明します。

7-2. Zscaler サービスへのログイン方法

(1) プロキシを設定後、任意のサイトにアクセスしようとするすると以下のログイン認証画面が表示されます。ユーザー名とパスワードを入力します。

ユーザー名入力

パスワード入力

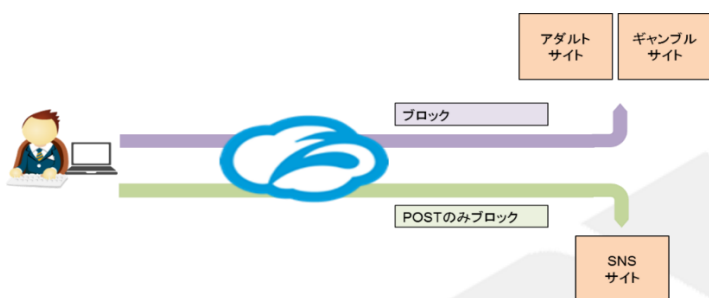
(2) パスワード入力後、アクセス先のページが表示されることを確認します。



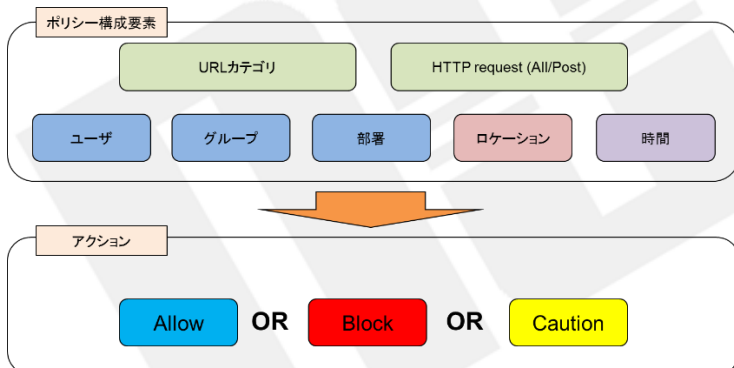
8. URL フィルタリングポリシーの設定と動作確認

8-1. 概要

URL フィルタリングポリシーは、URL カテゴリ単位にルールを作成し適用することができます。

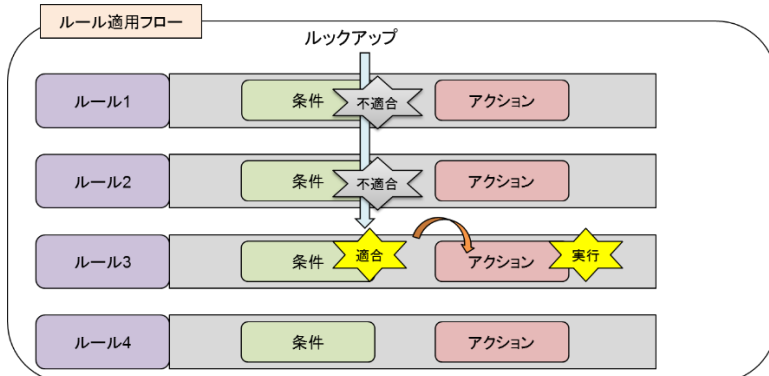


URL カテゴリに対してアクセス許可/ブロック/警告のアクションを適用できます。ポリシーの構成要素およびアクションのイメージは以下の通りです。



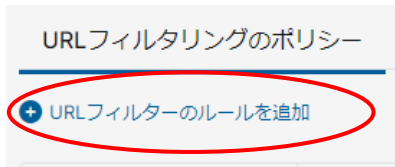
8-1-1. ポリシーの適用フロー

上位(数字の昇順)のポリシーから順番に条件のマッチングが行われ、最初に適合したポリシーのアクションが実行されます。



8-2. URL フィルタリングポリシーの設定方法

- (1) ZIA 管理ポータルを開き、「ポリシー」→「URL/クラウドアプリケーションコントロール」を選択します。
- (2) 「URL フィルターのルールを追加」をクリックします。



- (3) ポリシー内容を入力し、「保存」をクリックします。

URLフィルタリングのルール

ルールの順番: 3 (Callout: ルールの順番を選択します。上位のポリシーから順に評価されます。)

ルール名: URL_Filtering_2

ルールのステータス: 有効

CRITERIA

URLカテゴリ: --- (Callout: URL カテゴリを選択します。)

AND

ユーザー: --- (Callout: 誰にポリシーを適用するか選択します。ユーザー毎、グループ/部署ごとに設定可能です。)

部署: ---

AND

ロケーション: --- (Callout: ロケーション単位でポリシーを適用したい場合、ロケーションを選択します。)

ロケーショングループ: ---

AND

メソッドをリクエスト: GET; HEAD; POST; TRACE; OPTIONS; ... (Callout: メソッドやプロトコル単位で制御が可能です。)

時間: 常時

AND

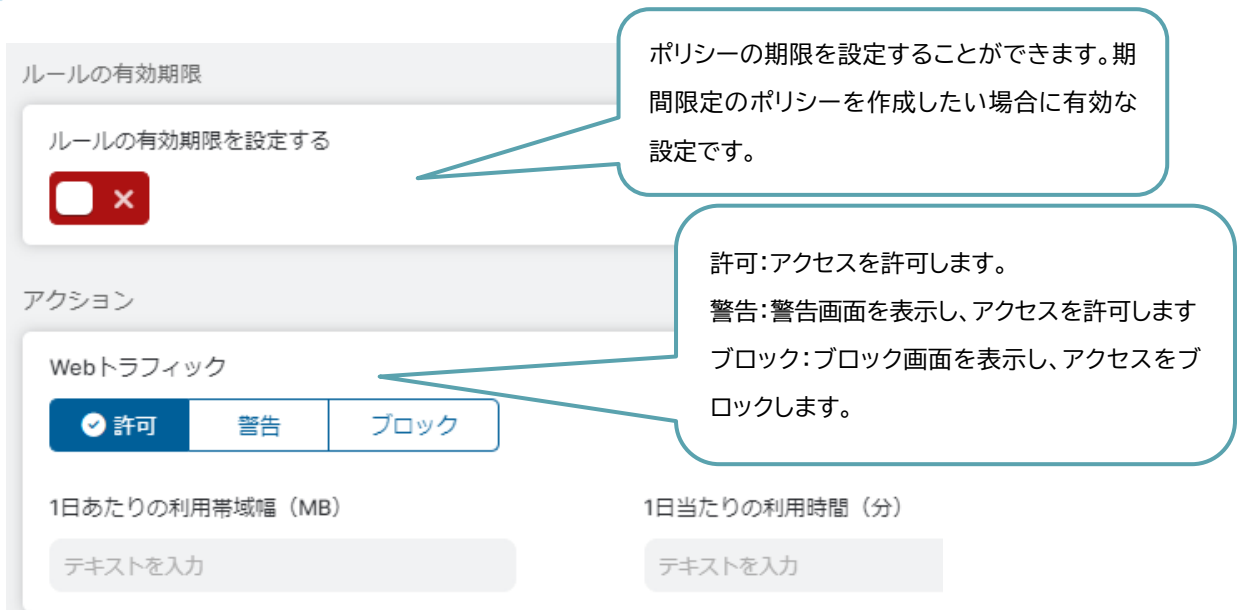
プロトコル: DNS Over HTTPS; FTP over HTTP; HT...

ユーザーエージェント: --- (Callout: ユーザーエージェントを指定することができます。)

AND

Devices: --- (Callout: ポリシーの適用時間を設定できます。業務時間中のみポリシーを適用するなどの設定が可能です。)

Groups: ---



8-3. URL フィルタリングポリシーの設定確認方法

- (1) ZIA 管理ポータルを開き、「ポリシー」→「URL/クラウドアプリケーションコントロール」を選択します。
- (2) 「URL フィルタリングのポリシー」タブを選択します。



8-4. URL フィルタリングポリシーの確認方法

- (1) Web ブラウザから、URL フィルタリングポリシーの設定項目に抵触するサイトにアクセスを行い、以下のようなメッセージが表示されることを確認します。



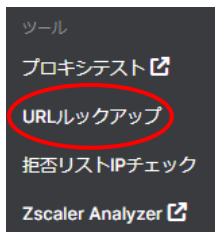
ブロックの場合



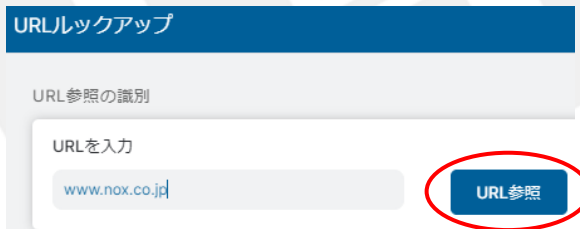
警告の場合

8-5. 対象サイトの URL カテゴリの確認方法

(1) ZIA 管理ポータルを開き、左側メニュー下部の「?マーク」→「URLルックアップ」を選択します。



(2) 対象のURLを入力し、「URLを参照」をクリックします。



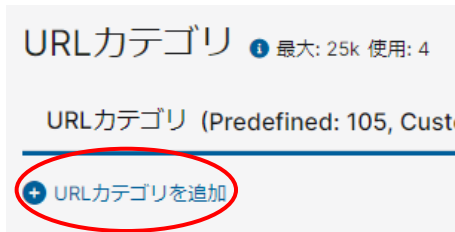
(3) カテゴリを確認します。



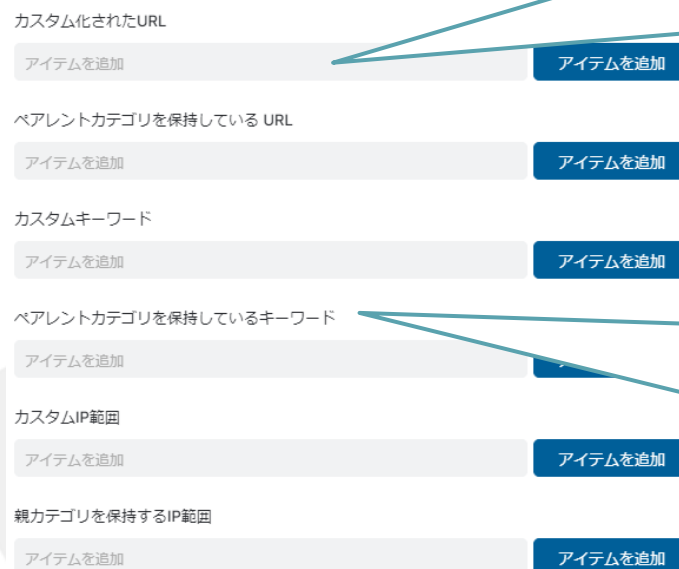
8-6. カスタムカテゴリの設定方法

ポリシーで使用するカスタムカテゴリの設定方法について説明します。ホワイトリストカテゴリ等を作成することが可能です。

- (1) ZIA 管理ポータルを開き、「管理」→「URL カテゴリ」を開きます。
- (2) 「URL カテゴリを追加」をクリックします。



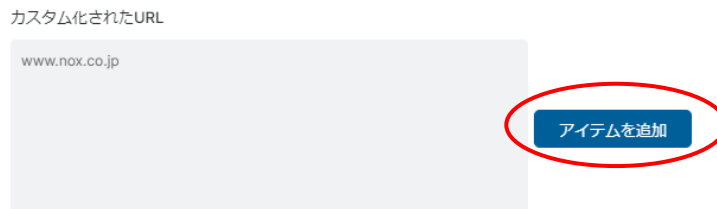
- (3) 設定内容を入力し、「保存」をクリックします。



カスタム化された(カスタム)…
Zscaler のデフォルトカテゴリを保持
しません。
カスタムカテゴリのポリシーのみに
マッチします。

ペアレントカテゴリ(親カテゴリ)…
Zscaler のデフォルトカテゴリを保持
します。
デフォルトカテゴリとカスタムカテゴリ
両方のポリシーにマッチします。

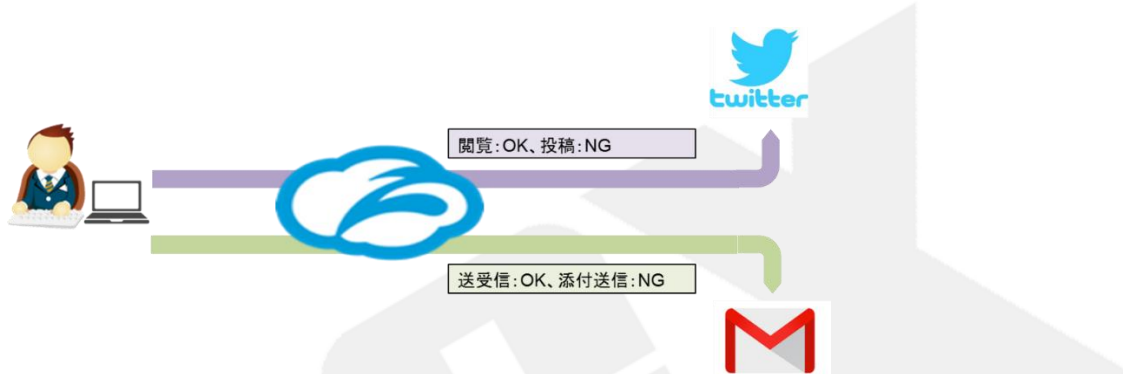
設定を入力し、「アイテムを追加」をクリックすることで、URL 等の追加ができます。



9. クラウドアプリケーションコントロールポリシーの設定と動作確認

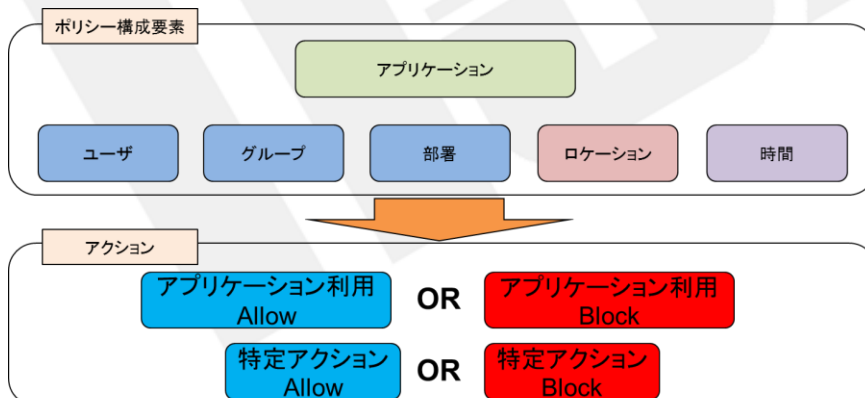
9-1. 概要

クラウドアプリケーションコントロールポリシーは、アプリケーション単位にポリシーを作成し適用することが可能です。

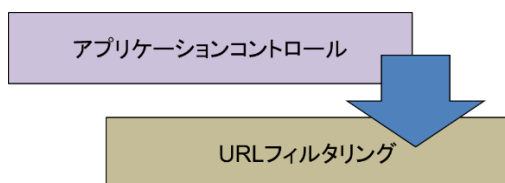


アプリケーションに対してアクセス許可/ブロックもしくは特定のアクションの許可/ブロック(アプリケーションによって異なる)を適用することが可能です。

ポリシーの構成要素およびアクションのイメージは以下の通りです。



クラウドアプリケーションコントロールポリシーは、URL フィルタリングポリシーよりも優先して評価されます。



9-2. クラウドアプリケーションコントロールポリシーの設定方法

- (1) ZIA 管理ポータルを開き、「ポリシー」→「URL/クラウドアプリケーションコントロール」を選択します。
- (2) 「クラウドアプリケーションコントロールポリシー」タブを開き、「追加」をクリックします。
- (3) 対象のクラウドアプリケーションカテゴリを選択します。



■選択可能なカテゴリ

- ・DNS Over HTTPS サービス(Google DNS, Secure DNS など)
- ・Health Care
- ・ITサービス(Google Login Services, Microsoft Login Servicesなど)
- ・SNS(Twitter, Facebookなど)
- ・Webメール(Outlook, Gmailなど)
- ・インスタントメッセージ(Chatwork, Google Chatなど)
- ・コンシューマー(Amazon, Paypalなど)
- ・システム/デベロップメント(Github, Google Developers など)
- ・ストーリーミングメディア(Youtube, Spotify など)
- ・セールス/マーケティング(Bazaarvoice, Oracle Eloqua など)
- ・ファイナンス(Mastercard, Visa Online など)
- ・ファイル共有(Gdrive, Box など)
- ・ホスティングプロバイダー(Amazon Web Services, Microsoft Azure など)
- ・人事(BizReach, Recruit など)
- ・共同作業とオンライン会議(Microsoft Teams, Zoom など)
- ・法務(Cloudsign, InTouch など)
- ・生産性と CRM ツール(Adobe Creative Cloud, Evernote など)

(4) 設定内容を入力します。

ルールの順番	1	ルール名	demo
ルールのステータス	有効	ルールラベル	---
クラウドアプリケーション	全て	クラウドアプリケーションインスタンス	なし
クラウドアプリケーションリスクプロファイル	なし	ユーザー	全て
Groups	全て	部署	全て
ロケーション	全て	ロケーショングループ	全て
時間	常時	デバイス	---
デバイスグループ	---	デバイス信頼レベル	---
ユーザーエージェント	全て		

ルールの有効期限を設定する

×

アクション

閲覧

許可 警告 ブロック Isolate

投稿

許可 ブロック

1日あたりの利用時間 (分)

テキストを入力

1日あたりの利用帯域幅 (MB)

テキストを入力

テナントプロファイル

なし

▲ SSLSSLインスペクションが必要

ルールの順番、ルール名を入力します。

対象のクラウドアプリケーションを選択します。

誰に対してポリシーを適用するかを選択します。ユーザー、グループ/部署ごとに選択が可能です。

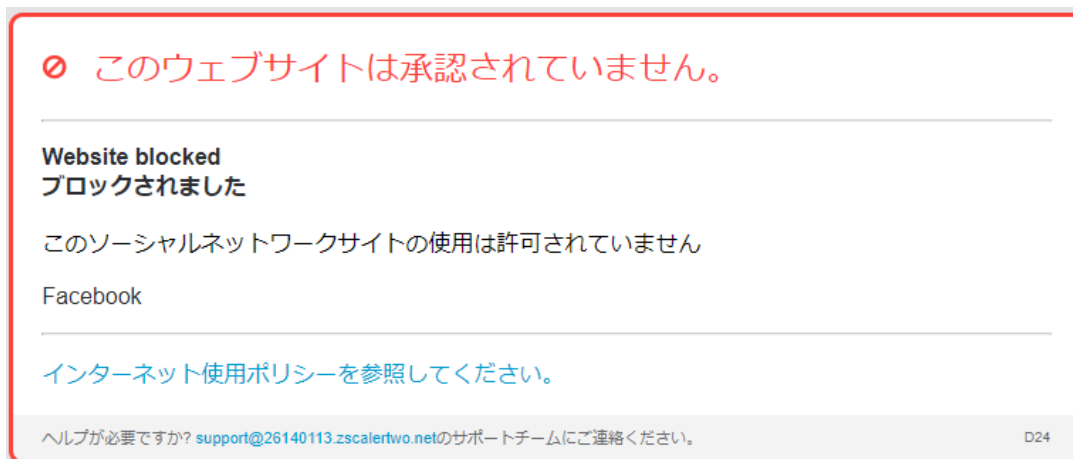
ロケーション単位でポリシーを適用する場合は選択します。

許可: アクセスを許可します。
警告: 警告画面を表示し、アクセスを許可します。
ブロック: アクセスをブロックします。

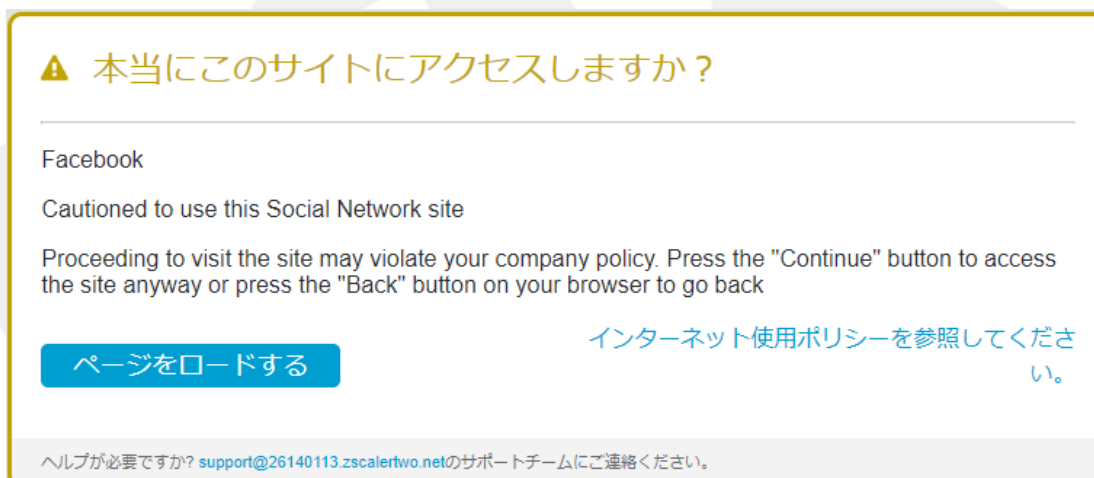
閲覧は許可
投稿はブロック
といった細かい制御ができます。

9-3. クラウドアプリケーションコントロールポリシーの動作確認方法

- (1) ブラウザから、クラウドアプリケーションコントロールポリシーの設定内容に抵触するサイトにアクセスを行い、以下のようなメッセージが表示されることを確認します。



ブロックの場合



警告の場合

10. SSL インспекションの設定

10-1. 概要

Zscalerは独自技術により、リアルタイムでSSLの複合化、スキャン、再暗号化を実現します。

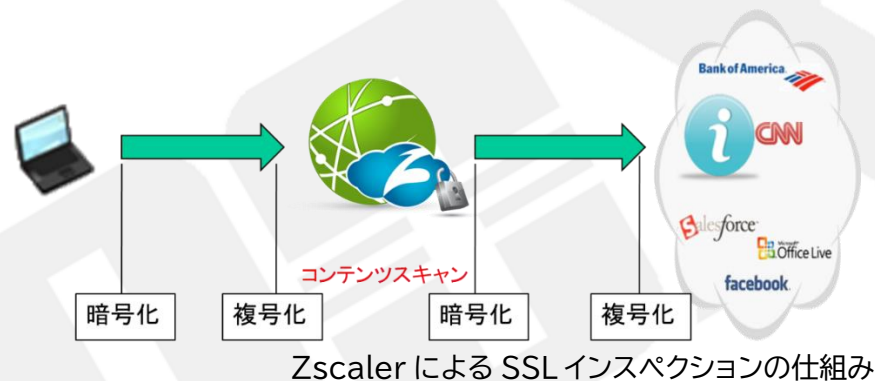
SSL インспекションを実施することで暗号化された通信の中身を確認できるため、セキュリティ性の向上や、通信の可視化を実現することが可能です。

本項では、SSL インспекションの設定方法について説明します。

10-1-1. SSL インспекションの利用条件

証明書のインストール

SSL インспекションは Man-In-The-Middle の方式で動作し、クライアントからの SSL 通信を一度 Zscaler で終端したうえで、Zscaler とサーバー間で新たに SSL を張る動作となるため、クライアント側で Zscaler の証明書をインストールしておく必要があります。



10-2. Zscaler の SSL 証明書の入手方法

ZCC(Zscaler Client Connector)をご利用の場合は、ZCC インストール時に、基本的に証明書も自動的にダウンロードされます。

10-2-1. 手動での入手方法

- (1) ZIA 管理ポータルを開き、「ポリシー」→「SSL インспекション」をクリックします。
- (2) 「中間 CA 証明書」のタブを開き、「Zscaler Intermediate CA Certificate」の右側「編集 (鉛筆アイコン)」をクリックします。

(3)「ダウンロード」をクリックします。



10-3. SSL インスペクションポリシーの設定方法

10-3-1. SSL インスペクションポリシーの設定方法

- (1) ZIA ポータル→「ポリシー」→「SSL インスペクション」を選択します。
- (2)「SSL インスペクションポリシーを追加」をクリックします。
- (3) 設定内容を入力し、「保存」をクリックします。



アクション

検査 検査しない ブロック

既定の中間CA証明書の上書き 中間CA証明書
 はい いいえ Zscaler Intermediate CA Certificate

信頼されていないサーバ証明書 復号化できないトラフィックをブロック
 許可 パススルー ブロック

OCSP失効チェック 最小クライアントTLSバージョン 最小サーバTLSバージョン
 TLS 1.0 TLS 1.0

アクション: 検査
→SSL インスペクションを実施します。

アクション

検査 検査しない ブロック

他のポリシーを評価 他のポリシーをバイパス

信頼されていないサーバ証明書 ブロックされたトラフィックの通知を表示
 許可 ブロック

OCSP失効チェック 最小のTLSバージョン
 TLS 1.0

アクション: 検査しない
→SSL インスペクションを実施しません。

他のポリシーを評価
→他のポリシー(URL フィルタリングポリシーなど)を評価します。

他のポリシーをバイパス
→他のポリシー(URL フィルタリングポリシーなど)を評価しません。

(4)管理ポータル左側のメニューより「有効化」を実施します。

11. マルウェアプロテクションの設定

11-1. 概要

Zscaler はシグネチャーベースでのマルウェアプロテクションが可能です。

本項では、マルウェアプロテクションの設定およびアンチウイルス保護の動作を確認する方法について説明します。

11-2. マルウェアプロテクションの設定方法

- (1) ZIA 管理ポータルを開き、「ポリシー」→「マルウェアプロテクション」をクリックします。
- (2) 設定内容を入力し、「保存」をクリックします。

マルウェアプロテクション

モバイルマルウェア制御ポリシーの設定
マルウェア対策ポリシーは、マルウェアやアドウェア/スパイウェアからトラフィックを保護します。

マルウェアのポリシー セキュリティの例外

マルウェアプロテクション

ウイルス

許可 ブロック

不要なアプリケーション

許可 ブロック

トロイの木馬

許可 ブロック

ワーム

許可 ブロック

Sandbox Ransomware

許可 ブロック

保存 キャンセル

11-3. アンチウイルス保護の確認方法

- (1) ブラウザを開き、<http://www.eicar.org/download/eicar.com> にアクセスします。
- (2) テストウイルスファイルをダウンロードすると、ZIA はそれをブロックし次のようなメッセージを表示します。ブラウザにキャッシュされたファイルはブロックされないため、保護の有効化と無効化の両方をテストする場合は、ブラウザのキャッシュをクリアする必要があります。



※ZIA 管理ポータル→「管理」→「リソース」→「エンドユーザー通知」にて、ユーザーに表示する通知画面をカスタマイズすることができます。

※HTTPS のテストウイルスファイルをブロックするには SSL インспекションを有効にしておく必要があります。