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

目次

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

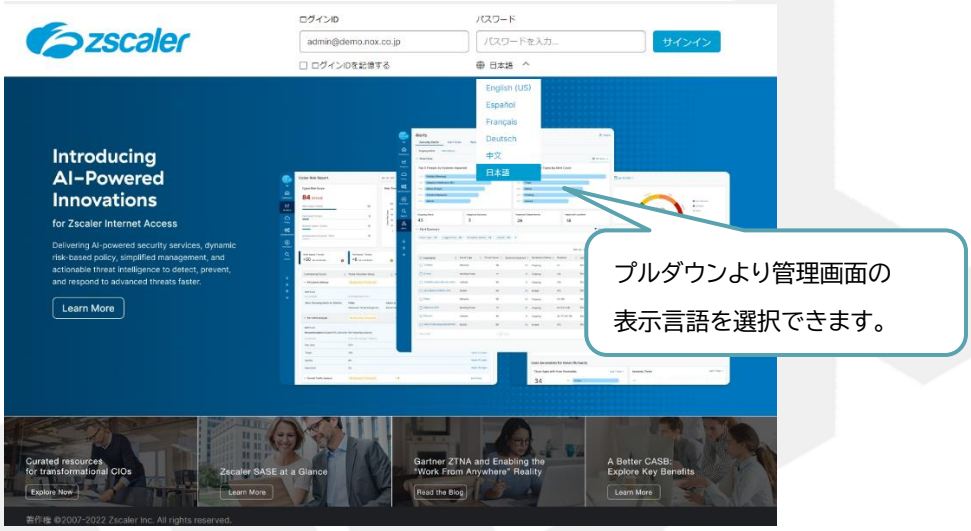
2. ZIA 管理ポータルへのログイン

2-1. 概要

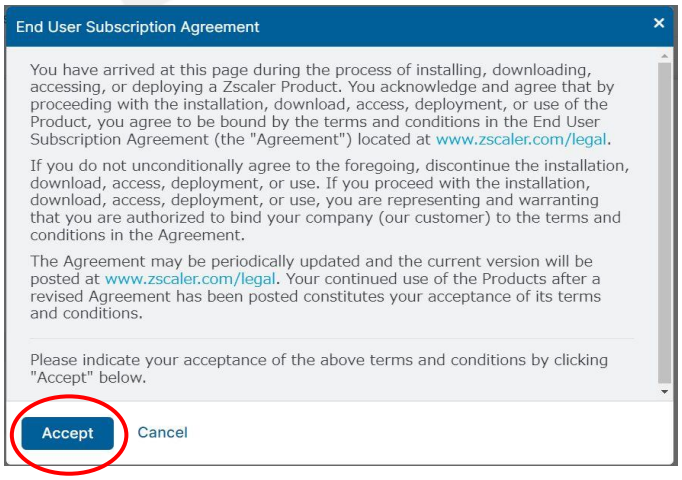
ZIA サービスポータルへのログイン方法、利用情報の入力方法を説明します。

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。

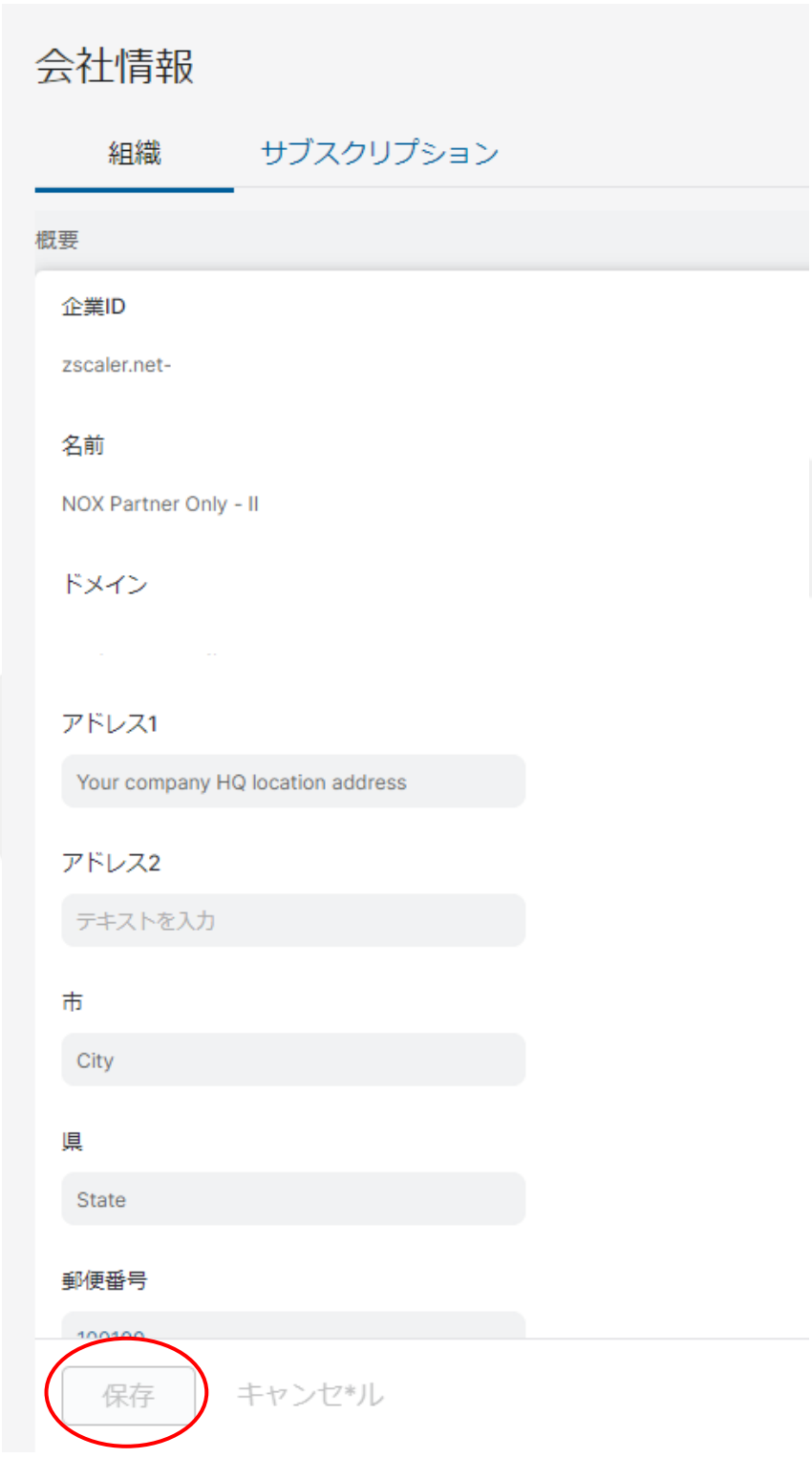


2-3. Company Profile の記入方法

(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。



2-4. ZIA 管理ポータルの管理者設定方法

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。

（4）左側メニューより「有効化」を実施します。

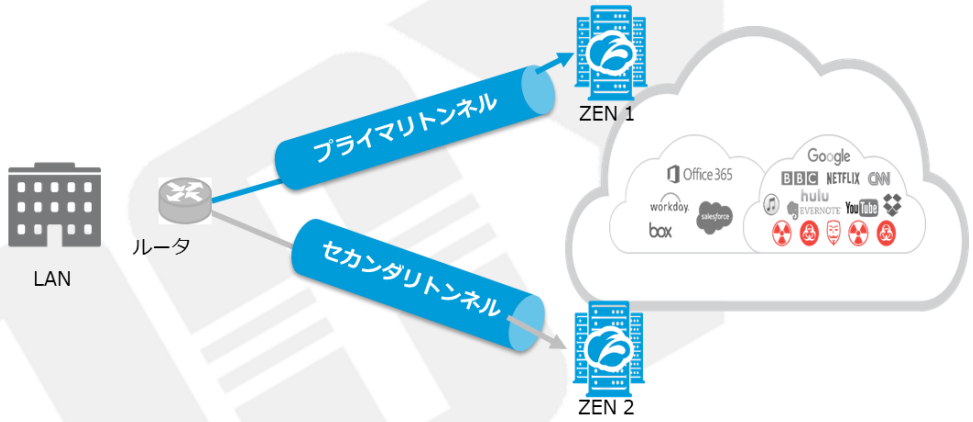
3. Webトラフィックの転送設定

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

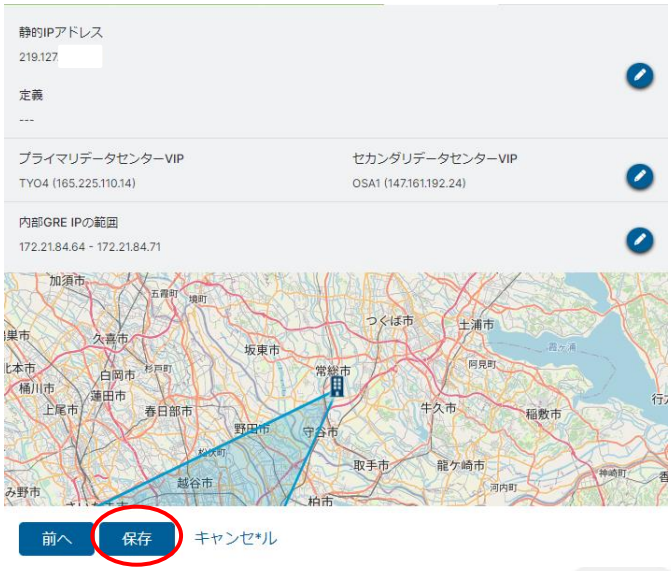
(1) ZIA 管理ポータルの「管理」→「静的 IP と GRE トンネル」→「GRE トンネル」のタブを開きます。
(2)「追加 GRE トンネル」をクリックします。

(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。）

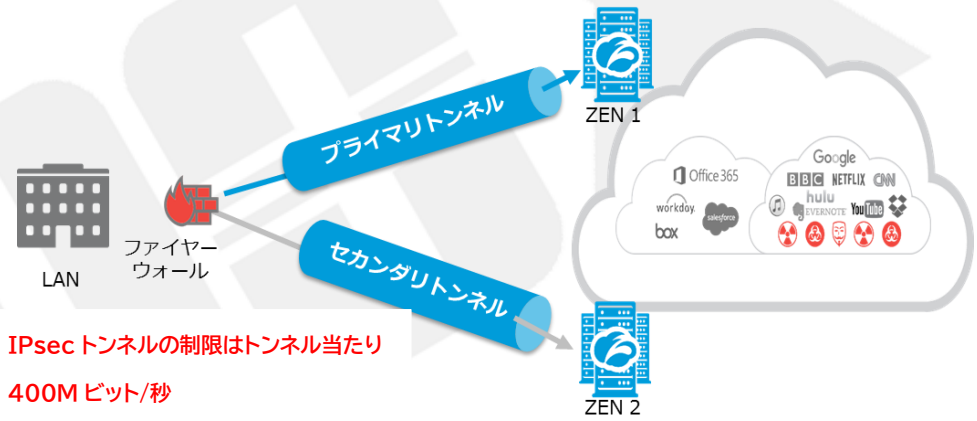
（5）「内部 GRE IP 範囲」を選択し、「次へ」をクリックします。

（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

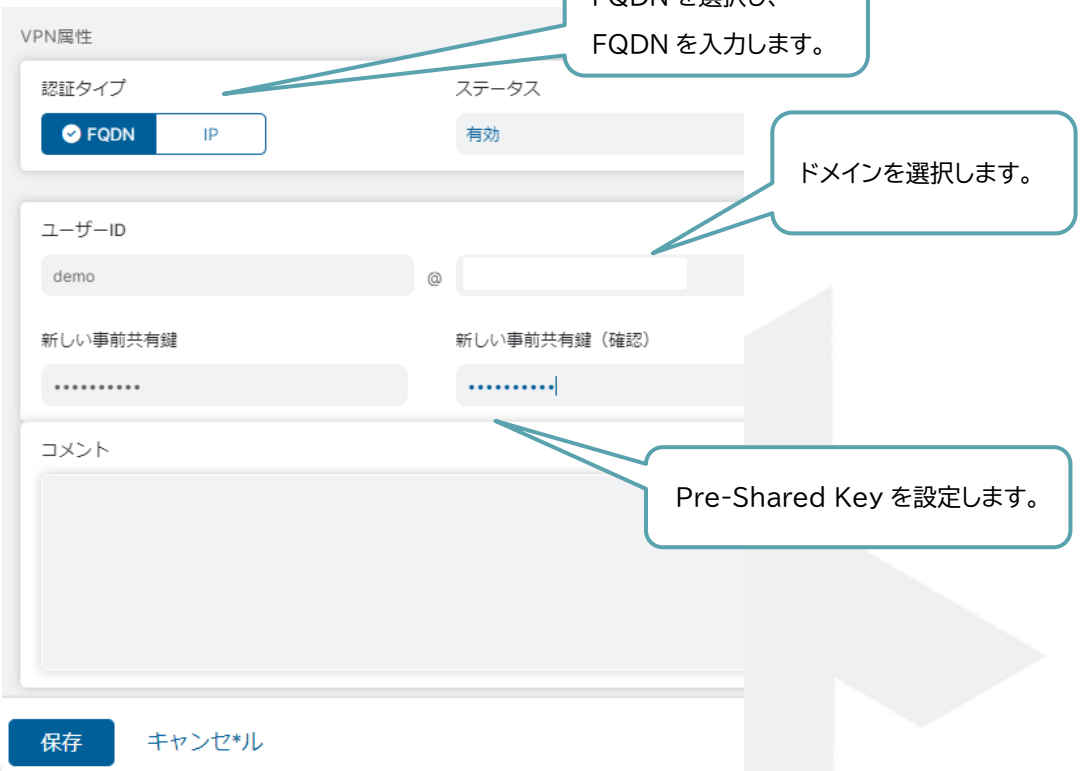
※https://config.zscaler.com/zscalerthree.net/cenr の赤字部分は管理ポータルURLのクラウド名を入力してください。

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



Main Mode の場合

(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。

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

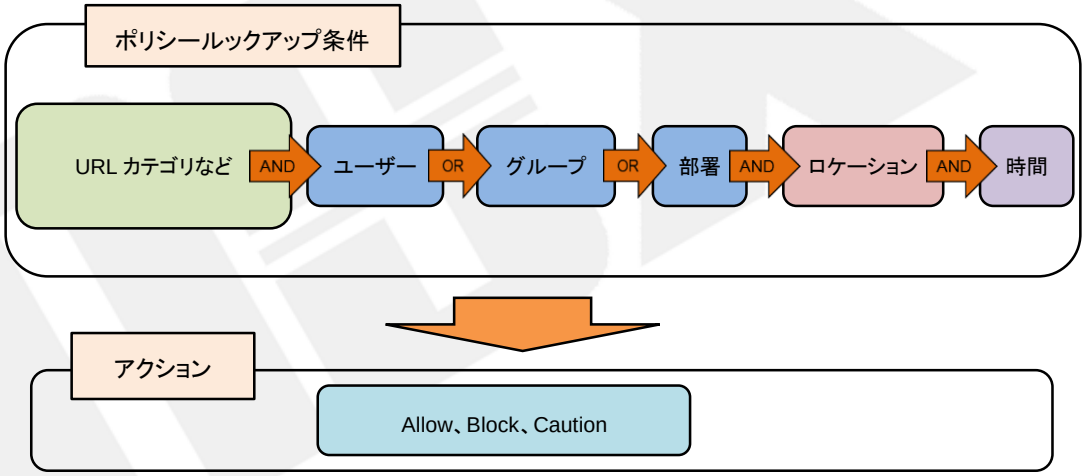
5. ユーザー、グループ、部署の設定

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。

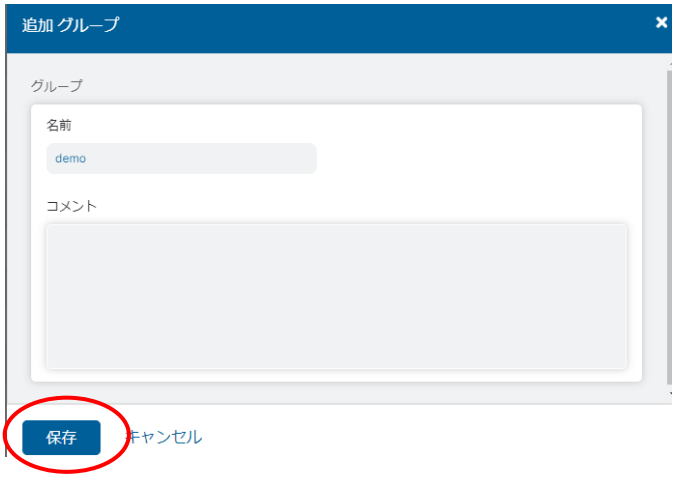


5-2. グループの設定方法

(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。



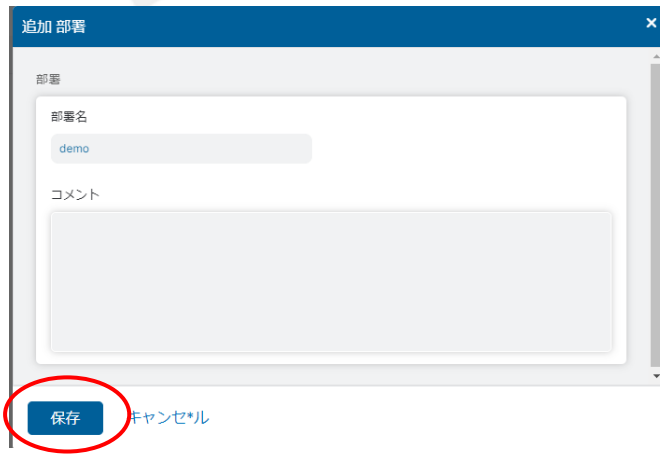
(※)CSV 形式でグループ情報をインポートおよびエクスポートすることができます。

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。



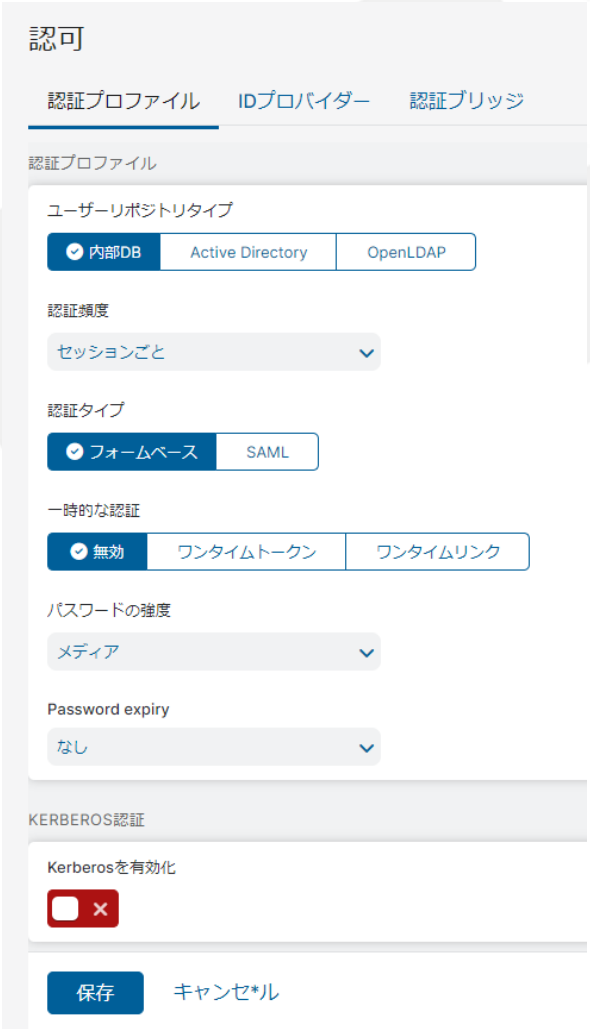
(※)CSV 形式で部署情報をインポートおよびエクスポートすることができます。

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 管理ポータルの「管理」→「認可」から認証プロファイルを設定します。



・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
※ASCⅡ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。

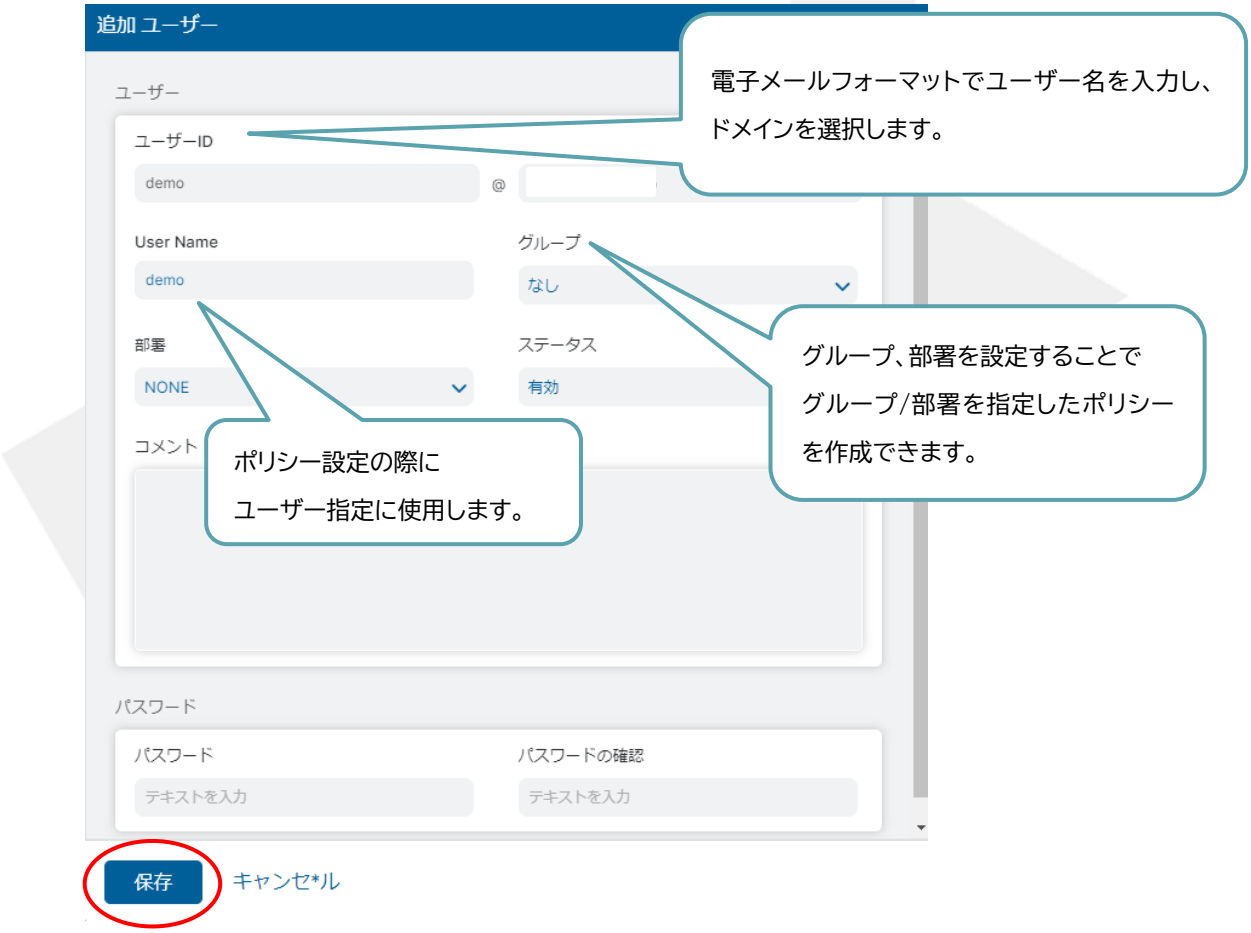
ワンタイムトークン：一時パスワード
ワンタイムリンク：一時リンク
※リンク、パスワード共に 24 時間有効となります。

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

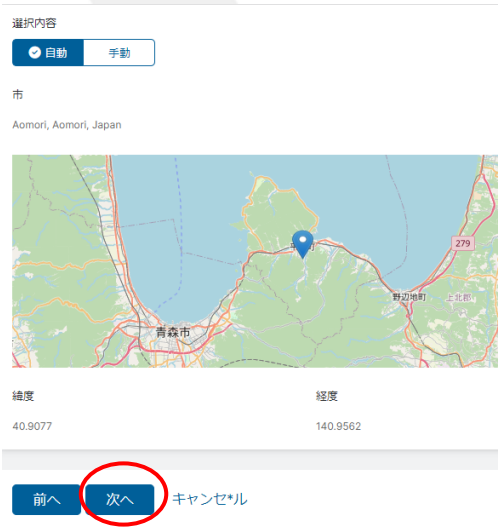
6-2-1. 静的 IP アドレスの設定方法

(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。

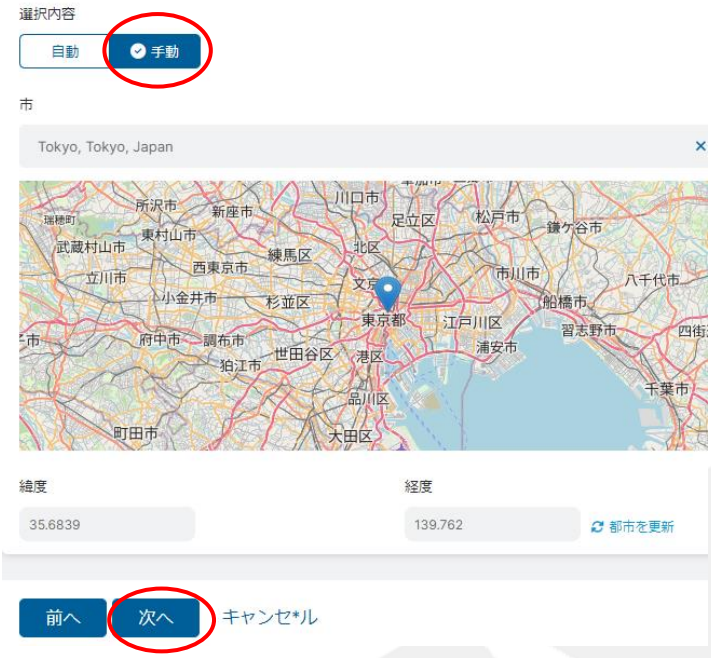
(2)「静的 IP」のタブを開き、「追加 静的 IP」をクリックします。

(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。



（5）入力内容を確認し、「保存」をクリックします。

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。

(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。

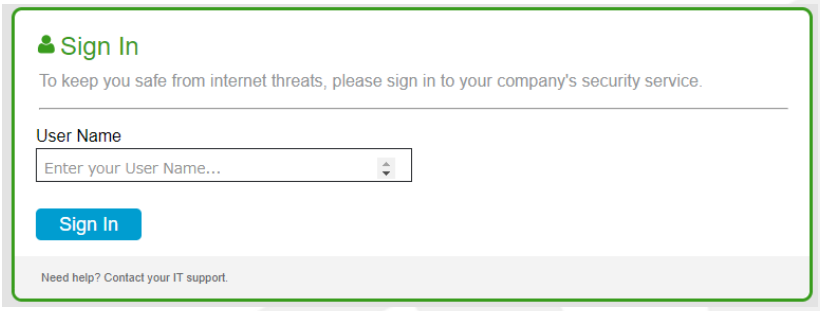
7. Zscaler サービスへのログイン

7-1. 概要

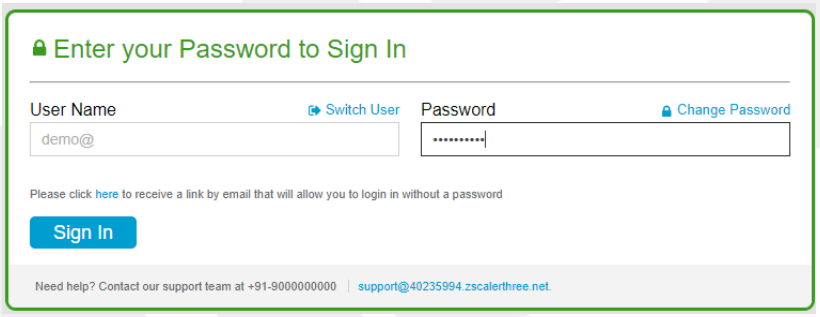
Zscaler サービスへのログイン方法を説明します。

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



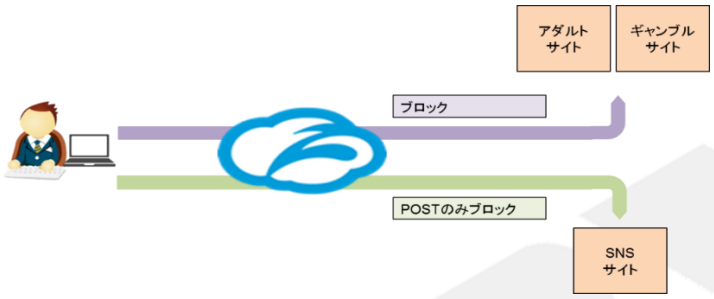
パスワード入力

(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。

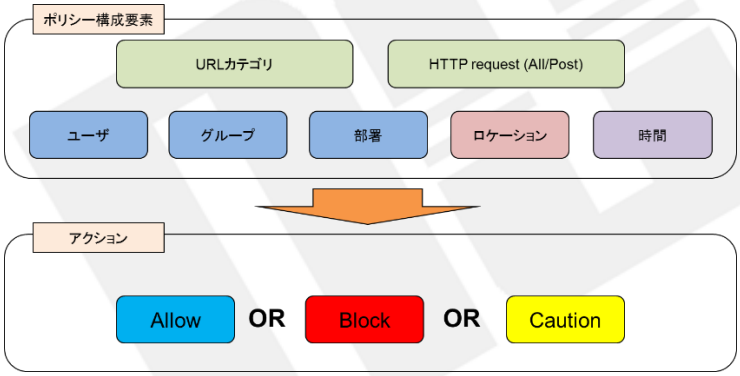
8. URL フィルタリングポリシーの設定と動作確認

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。

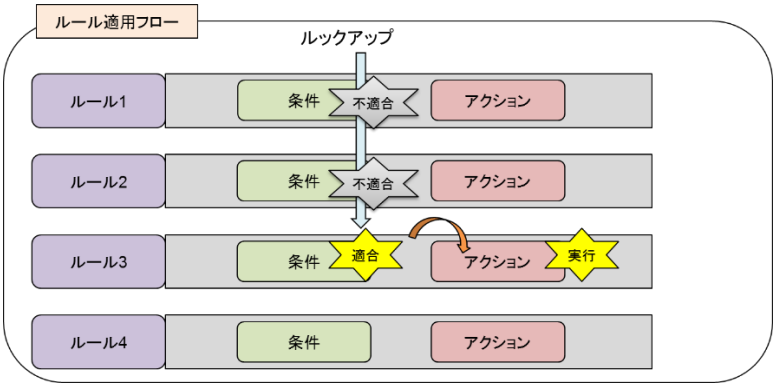


URL カテゴリに対してアクセス許可/ブロック/警告のアクションを適用できます。
ポリシーの構成要素およびアクションのイメージは以下の通りです。



8-1-1. ポリシーの適用フロー

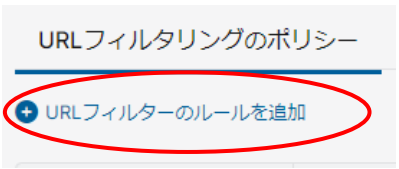
上位(数字の昇順)のポリシーから順番に条件のマッチングが行われ、最初に適合したポリシーのアクションが実行されます。



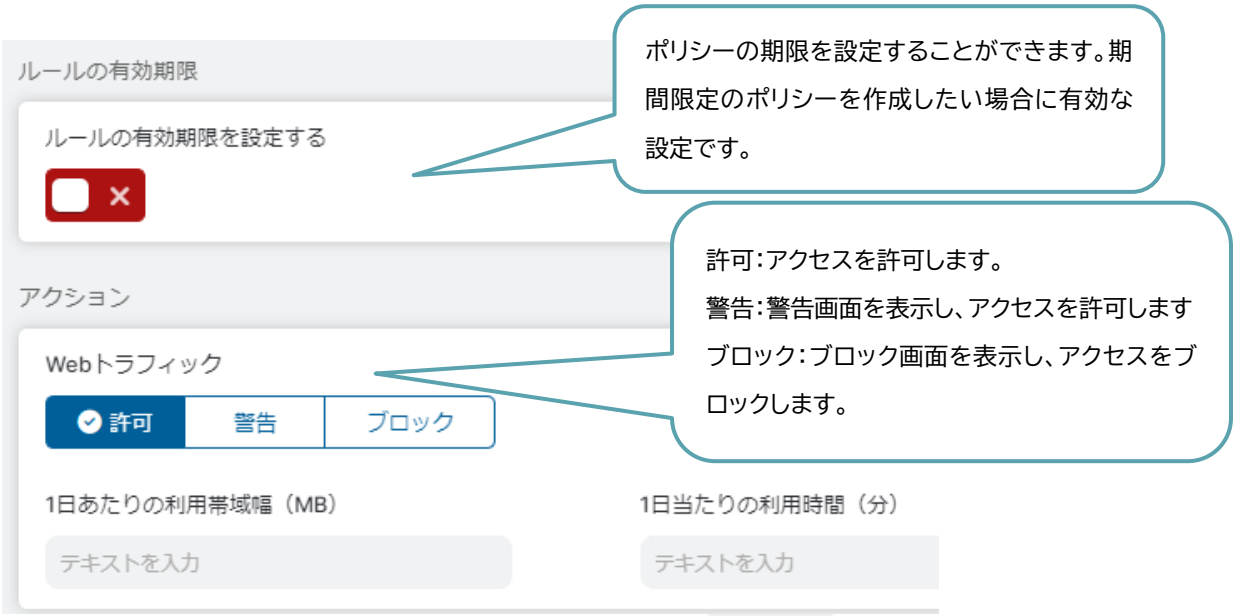
8-2. URL フィルタリングポリシーの設定方法

(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。



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

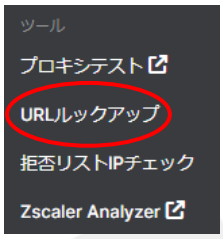
(1) Web ブラウザから、URL フィルタリングポリシーの設定項目に抵触するサイトにアクセスを行い、以下のようなメッセージが表示されることを確認します。

ブロックの場合

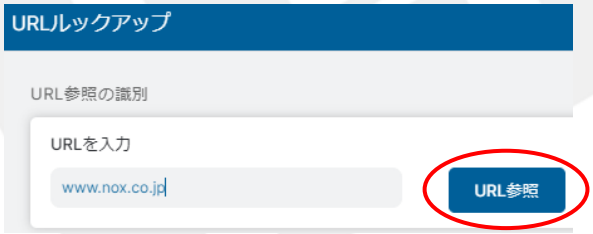
警告の場合

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。

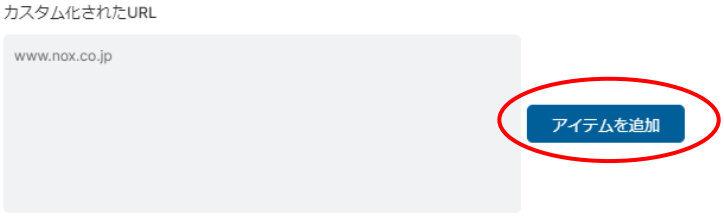
(2)「URL カテゴリを追加」をクリックします。

(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。

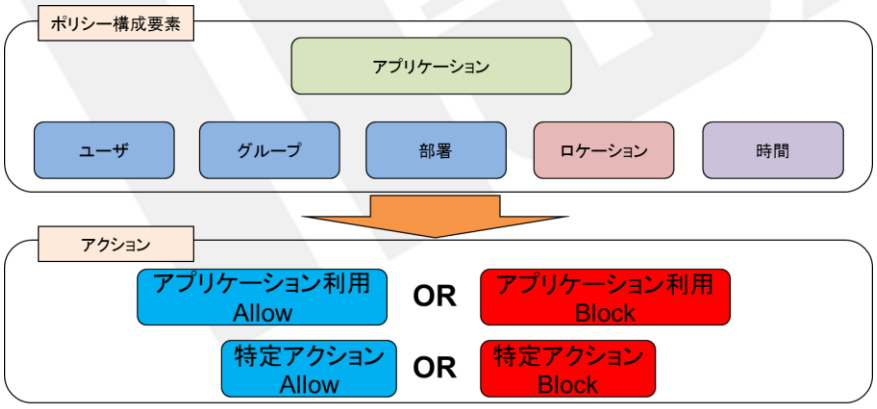


9. クラウドアプリケーションコントロールポリシーの設定と動作確認

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。

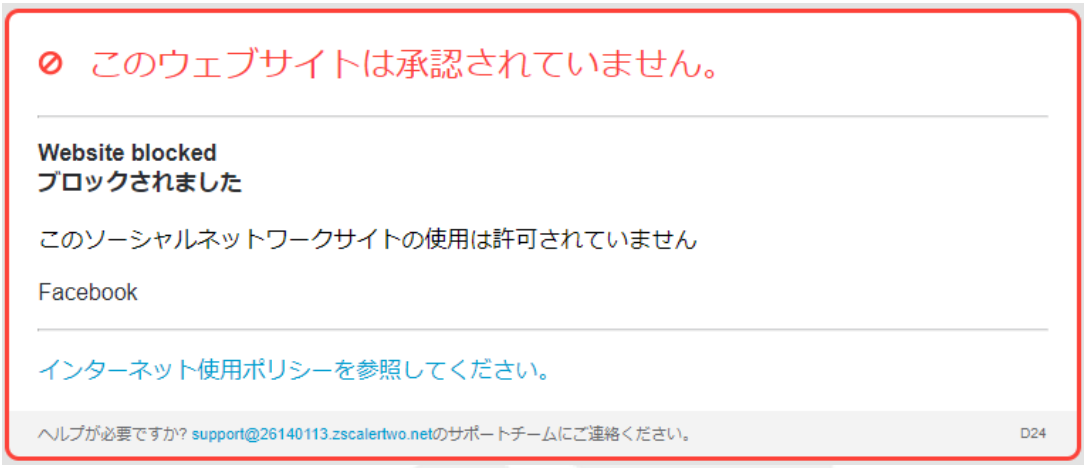
■選択可能なカテゴリ

・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)

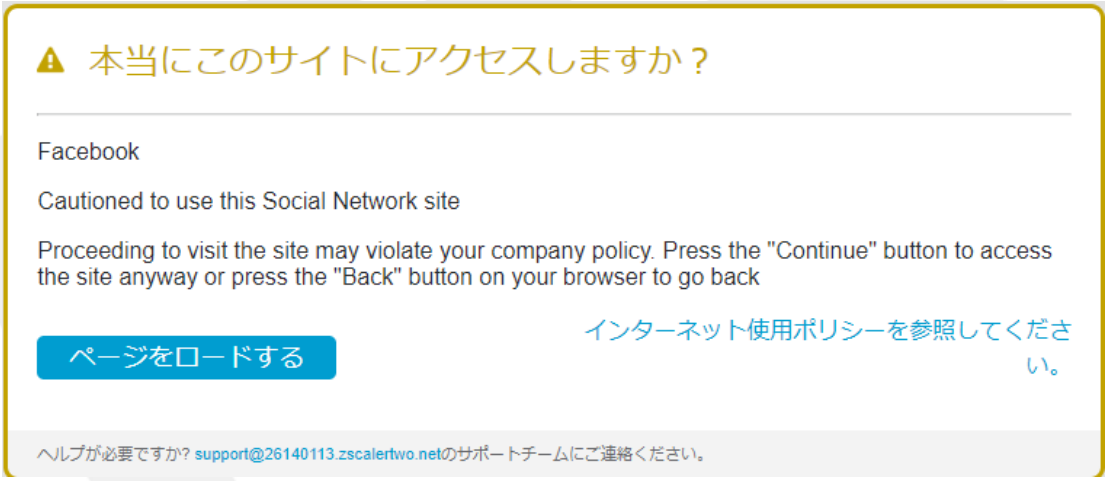
（4）設定内容を入力します。

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

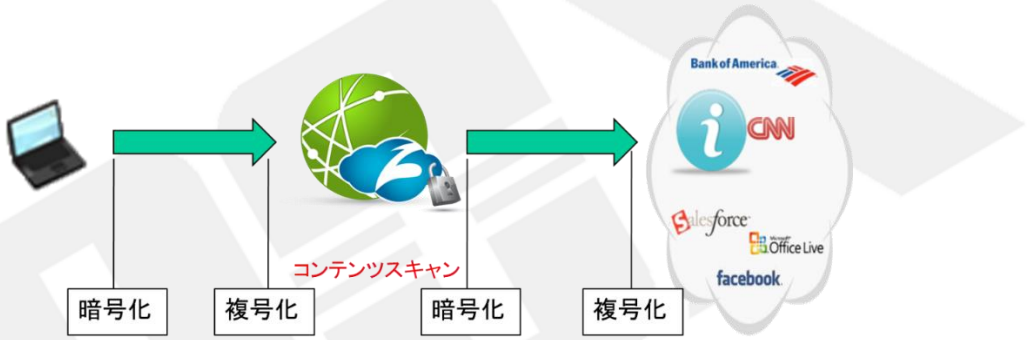
10. SSL インスペクションの設定

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 インスペク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 インスペクションの設定方法について説明します。

10-1-1. SSL インスペクションの利用条件

証明書のインストール
SSL インスペクションは 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。



Zscaler による SSL インスペクションの仕組み

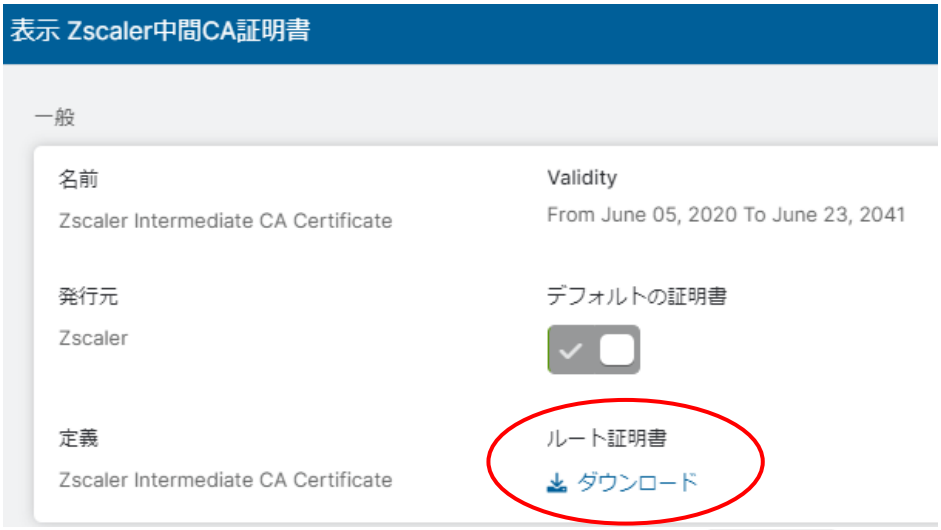
10-2. Zscaler の SSL 証明書の入手方法

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 インスペクション」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。

（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。

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 インスペクションを有効にしておく必要があります。