クラウド型総合ゲートウェイセキュリティアプライアンス

Cloud Edge初期設定ガイド

■トレンドマイクロへのお客さま情報の送信について
(1)「Webレピュテーションサービス」、「フィッシング詐欺対策」、「ペアレンタルコントロール/URLフィルタリング」および「Trend ツールバー」等について
①トレンドマイクロでは、お客さまがアクセスしたWebページの安全性の確認のため、お客さまより受領した情報にもとづき、お客さまがアクセスするWebページのセキュリティチェックを実施します。なお、お客さまがアクセスしたURLの情報等（ドメイン、IPアドレス等を含む）は、暗号化してトレンドマイクロのサーバに送信されます。サーバに送信されたURL情報は、Webサイトの安全性の確認、および当該機能の改良の目的にのみ利用されます。
②当該機能を有効にしたうえで、Webページにアクセスした場合、以下の事象がおこることがありますのでご注意ください。
(a) お客さまがアクセスしたWebページのWebサーバ側の仕様が、お客さまが入力した情報等をURLのオプション情報として付加しWebサーバへ送信する仕様の場合、URLのオプション情報にお客さまの入力した情報（ID、パスワード等）などを含んだURLがトレンドマイクロのサーバに送信され、当該Webページのセキュリティチェックが実施されます。
(b) お客さまがアクセスするWebページのセキュリティチェックを実施する仕様になっていることから、お客さまがアクセスするWebサーバ側の仕様によっては、URLのオプション情報に含まれる内容により、お客さまの最初のリクエストと同様の処理が行われます。
③Webサイトのセキュリティ上の判定はトレンドマイクロの独自の基準により行われております。当該機能において判定されたWebサイトのアクセス可否の最終判断につきましては、お客さまにてお願いします。
(2) Trend Micro Smart Protection Network（「スマートフィードバック」、「ファイルレピュテーションサービス」、「脅威情報の送信」および「ウイルストラッキング」等を含みます）について脅威に関する情報を収集、分析し保護を強化するために、お客さまのコンピュータに攻撃を試みる脅威に関連すると思われる情報を収集して、トレンドマイクロに送信することがあります。送信された情報はプログラムの安全性の判定や統計のために利用されます。また情報にお客さまの個人情報や機密情報等が意図せず含まれる可能性がありますが、トレンドマイクロがファイルに含まれる個人情報や機密情報自体を収集または利用することはありません。お客さまから収集された情報の取り扱いについての詳細は、<http://jp.trendmicro.com/jp/about/privacy/spn/index.html>をご覧ください。
(3)「迷惑メール対策ツール」についてトレンドマイクロ製品の改良目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
(4)「E-mailレピュテーションサービス」についてスパムメールの判定のために、送信元のメールサーバの情報等をトレンドマイクロのサーバに送信します。
(5)「ユーザービヘイビアモニタリング」についてトレンドマイクロ製品の改良目的のために、お客さまがトレンドマイクロ製品をどのような設定にして利用しているのかがわかる設定の情報およびお客さまがトレンドマイクロ製品をどのように操作したのかがわかる操作履歴の情報を、匿名でトレンドマイクロのサーバに送信します。

■輸出規制について
お客さまは、本製品およびそれらにおいて使用されている技術（以下「本ソフトウェア等」といいます）が、外国為替および外国貿易法、輸出貿易管理令、外国為替令および省令、ならびに、米国輸出管理規則に基づく輸出規制の対象となる可能性があること、ならびにその他の国における輸出規制対象品目に該当している可能性があることを認識の上、本ソフトウェア等を適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出しないものとします。
お客さまは、2021年3月現在、米国により定められる禁輸国が、キューバ、イラン、北朝鮮、スーダン、シリアであること、禁輸国に関する情報が、以下のウェブサイトにおいて検索可能であること、ならびに本ソフトウェア等に関連した米国輸出管理法令の違法行為に対して責任があることを認識の上、違法行為が行われないよう、適切な手段を講じるものとします。

また、お客さまが本ソフトウェア等を使用する場合、米国により現時点で輸出を禁止されている国の居住者もしくは国民ではないこと、および本ソフトウェア等を受け取ることが禁止されていないことを認識し、お客さまは、本ソフトウェア等を、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意するものとします。

■著作権について
本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

■商標について
TRENDMICRO、TREND MICRO、ウイルスバスター、ウイルスバスター On-LineScan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro ControlManager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、Trend Park、Trend Labs、Trend Micro NetworkVirusWall、Network VirusWall Enforcer、LEAKPROOF、Trend Micro ThreatManagement Solution、Trend Micro Threat Management Services、Trend MicroThreat Mitigator、Trend Micro Threat Discovery Appliance、Trend MicroUSB Security、InterScan Web Security Virtual Appliance、InterScanMessaging Security Virtual Appliance、Trend Micro Reliable SecurityLicense、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend MicroCollaboration Security、Trend Micro Portable Security、Trend MicroStandard Web Security、Trend Micro Hosted Email Security、Trend MicroDeep Security、ウイルスバスタークラウド、Smart Surfing、スマートスキャン、Trend Micro Instant Security、Trend Micro Enterprise Security forGateways、Enterprise Security for Gateways、Trend Micro Email SecurityPlatform、Trend Micro Vulnerability Management Services、Trend Micro PCIScanning Service、Trend Micro Titanium AntiVirus Plus、Smart ProtectionServer、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、トレンドマイクロ オンラインストレージ SafeSync、Trend MicroInterScan WebManager SCC、Trend Micro NAS Security、Trend Micro DataLoss Prevention、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend MicroDeep Security Virtual Patch、Trend Micro Threat Discovery SoftwareAppliance、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Trend Micro Deep Security あんしんパック、こどもーど、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、トレンドマイクロ バッテリーエイド、Trend Micro Safe Lock、トレンドマイクロセーフバックアップ、Deep Discovery Advisor、Deep Discovery Inspector、Trend Micro Mobile App Reputation、あんしんブラウザ、Jewelry Box、カスタム ディフェンス、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、プライバシースキャナー、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、Smart Protection Integration Framework、InterScan Web Security as aService、Client/Server Suite Premium、Cloud Edge、Trend Micro RemoteManager、Threat Defense Expert、スマートプロテクションプラットフォーム、Next Generation Threat Defense、セキュリティアットホーム、セキュリティエブリウェア、セキュリティコンシェルジュ、およびTrend Micro Smart HomeNetworkは、トレンドマイクロ株式会社の登録商標です。
本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。
記載内容は2021年3月現在のものです。内容は予告なく変更になる場合がございます。
Copyright © 2022 Trend Micro Incorporated. All rights reserved.

本製品は日本国内での使用を前提に製作されておりますので、日本国外でのご使用は出来ません。また、ACアダプタと電源ケーブルは分離して使用することはできません。

はじめに

Cloud Edgeは、次世代のオンプレミスのファイアウォールの利点とManaged Service Provider向けの「Security as a Service」の便利さを同時に提供します。Cloud Edgeは、オンプレミスまたはクラウド経由でネットワークパケットを徹底的に検索およびフィルタし、脅威をゲートウェイで食い止めます。Cloud Edgeは、アプリケーションコントロールとユーザ識別およびポート識別、ゼロデイ脆弱性検出、不正プログラム検出、Webレピュテーションセキュリティ、URLフィルタを統合し、ユーザをネットワーク違反とビジネスの中断から守ります。またVPNでは、モバイルデバイス、コーポレートサイト、遠隔地の従業員からの安全な接続をサポートします。

Cloud Edgeアプライアンスをユーザの世界中のオフィスに配信し、直観的なコンソール画面からユーザアクセスとセキュリティポリシーを中央管理することができます。

本書は、Cloud Edgeを設置、初期設定をおこなうエンジニアや、管理者向けに作成されています。新規インストールの手順、運用に関する内容や注意点などについて解説しています。

また、本書は2021年3月時点で公開されているバージョンを基に作成しております。バージョンやService Packの違い、旧バージョンからバージョンアップした場合は、機能の有無や既定値が異なる場合があることを、あらかじめご了承ください。

目次

はじめに.....3

第1章 Cloud Edgeの概要を知る.....5
1.1 Cloud Edgeの概要.....6

第2章 Cloud Edgeを設置する.....7
2.1 ネットワークの設定.....8
2.2 アプライアンス本体の設定.....10
2.3 クイックセットアップの初期設定.....11
2.4 On-Premises Consoleの初期設定.....23
2.5 Cloud Edge Cloud Console (CECC)へのログイン.....27
2.6 ゲートウェイの登録.....30

トラブルシューティング Cloud Edge　サポートページについて.....32

第1章
Cloud Edgeの概要を知る

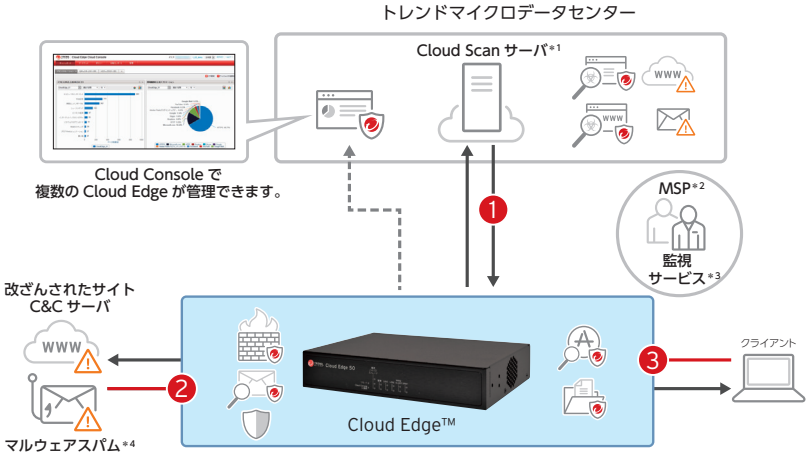
Cloud Edge の概要について解説します。

■ Cloud Edgeの概要

Cloud Edgeは、お客さまのネットワーク上に設置していただくハードウェア（Cloud Edge本体）と、トレンドマイクロのクラウドサービス（Cloud Scanサーバ／Cloud Edge Cloud Console (CECC)）を組み合わせた中小企業向けクラウド型総合ゲートウェイ セキュリティアプライアンスです。

ランサムウェアや標的型サイバー攻撃など、さまざまな脅威からネットワークを保護するために、セキュリティ機能を統合したUTM（Unified Threat Management＝統合脅威管理）アプライアンスが注目されています。しかし、一般的なUTMでセキュリティ機能を有効にすると、ネットワークのパフォーマンスが低下して、業務に悪影響を及ぼすおそれも考えられます。

Cloud Edgeは、そうしたUTMの課題を解決するためにトレンドマイクロが開発したセキュリティ対策専用アプライアンスです。ハードウェアによる検索に加え、クラウド経由でネットワークパケットを徹底的に検索およびフィルタすることで、ハードウェアに依存しない高いスループット、および脅威からの保護を両立します。



＊1 Cloud Scanサーバは、トレンドマイクロがWebアクセスセキュリティをクラウド上で提供する、
クラウド型セキュリティサービスです。Cloud Edgeの機能として利用します。
＊2 MSPは、マネージドサービスプロバイダーの略です。
＊3 監視サービスは、販売店からの提供となります。販売店にご確認お願いします。
＊4 マルウェアスパムとは、不正プログラムの拡散を目的としたスパムメールのことです。

①クラウド利用によりハードウェアに依存しない高いパフォーマンスを実現
②ファイアウォール、IPS、メールセキュリティ対策で社外からの攻撃をブロック
③マイナンバーなどの重要情報の流出をブロック

第2章
Cloud Edgeを設置する

Cloud Edgeを社内ネットワークに設置する際の初期設定を紹介します。

2.1 ネットワークの設定

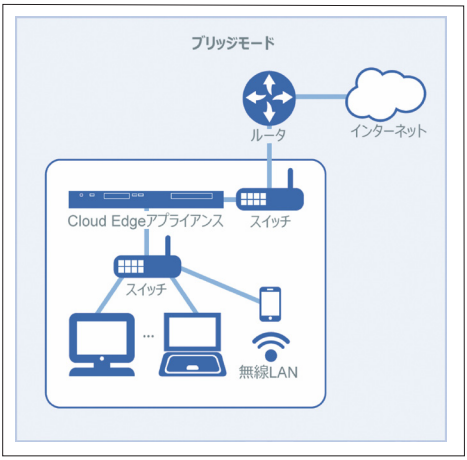
対応可能なネットワークモード一覧

	CE 50	CE 100	CE SB	CE 100G2
ブリッジモード	○	○	○	
ルーティングモード	○	○		○
スイッチモード				○

2.1.1 ブリッジモード

設定可能なモデル：CESB, CE50, CE100

ブリッジモードは、Cloud Edgeをネットワークブリッジとして利用するモードです。このモードでは、Cloud Edgeはネットワーク上で認識されません。既存のファイアウォール、またはルータとネットワークスイッチの間に設置することで、Cloud Edgeはデータリンク層（レイヤ2）ブリッジとして機能し、双方向のトラフィックを透過的に検索します。



Cloud Edgeを接続するネットワークは、すべて同じサブネット上に存在しなければなりません。ブリッジに固定IPアドレスを設定してCloud Edgeを管理したり、Trend Micro Smart Protection Networkから提供されるリアルタイムのセキュリティ情報を活用したりすることも可能です。

ワンポイントアドバイス

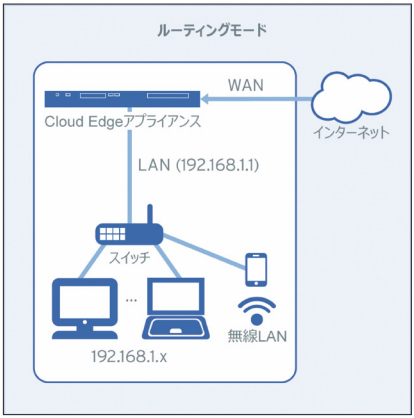
Cloud Edge 5.3からブリッジモードにソフトウェアスイッチ機能が追加され、LAN2、LAN3の配下に各種デバイスを接続することが可能です。

設定方法については、2.3.2.1 ソフトウェアスイッチの接続設定を参照してください。

2.1.2 ルーティングモード

設定可能なモデル：CE50, CE100, CE100G2

ルーティングモードは、Cloud Edgeを内部ネットワークと外部ネットワーク（通常はインターネット）の間のゲートウェイとして使用するモードです。Cloud Edgeはネットワーク上で認識され、トラフィックストリームの検索機能を持つネットワーク層（レイヤ3）ルーティングデバイスとして機能します。



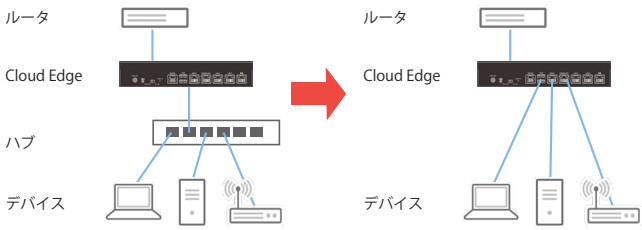
ルーティングモードでは、NATモードのファイアウォールポリシーを作成し、内部ネットワークと外部ネットワークとの間のトラフィックフローを制御します。PPPoE（Point-to-point Protocol over Ethernet）機能により、光回線およびADSL（非対称型デジタル加入者回線）経由でISPへ接続することが可能です。

2.1.3 スイッチモード

設定可能なモデル：CE100G2

CE100G2はブリッジモードを利用できません、代わりにスイッチモードを利用できます。

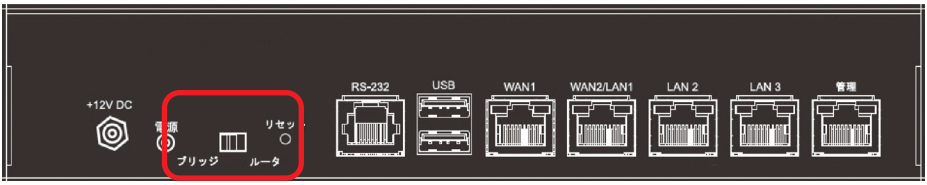
スイッチモードはブリッジモードと同じく、Cloud Edgeはネットワーク上で認識されないブリッジとして機能します。ブリッジモードはLAN1しか使えませんが、スイッチモードの場合、LAN側に複数のポートを利用可能で、スイッチやハブを利用せず直接複数のデバイスを接続することが可能です。



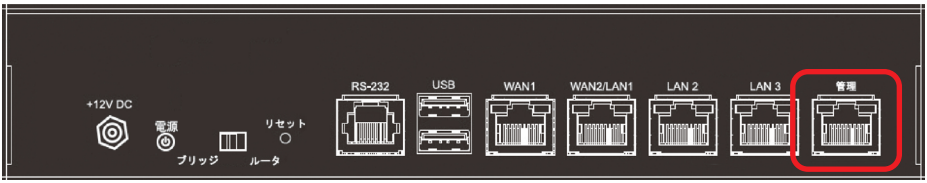
■ 2.2 アプライアンス本体の設定

Cloud Edgeでは、「ブリッジモード」「ルーティングモード」のどちらかの配信モードを選択したかによって、トラフィックの転送方法が決まります。以下の手順で操作してください。

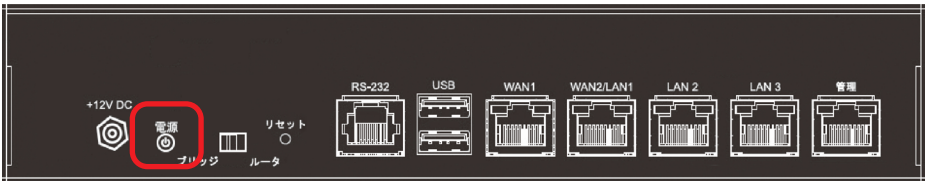
① 電源をオンにする前に、アプライアンス本体の背面パネルにある切り替えスイッチを操作して、使用するモードを選択します。工場出荷時における初期状態は、ブリッジモードになっています。ルーティングモードに切り替えるには、スイッチを「ルータ」側へ切り替えてください。なお、配信モードを切り替えてから電源をオンにすると、設定が初期化されます。



② コンピュータとCloud Edgeの「管理」ポートを、製品付属のイーサネットケーブルで接続します。



③ 製品付属の電源ケーブルをアプライアンス本体の背面パネルに接続します。通電すると、電源ボタンが赤色に点灯します。電源ボタンを押すと起動合図のビープ音が鳴ったのちに電源ボタンが緑色に点灯して、アプライアンス本体の電源がオンになります。



※例の筐体はCE50です。
CESBの場合「ブリッジモード」のみ選択可能です。
CE100G2の場合「ブリッジ」を選択しますとスイッチモードになります。

2.3 クイックセットアップの初期設定

運用を開始する前に、Cloud Edgeのアプライアンス本体に内蔵されているWebコンソール「Cloud Edge On-Premises Console（オンプレミス・コンソール）」にアクセスし、「クイックセットアップ」を使ってネットワークの初期設定を行います。

【初期設定の流れ】

2.3.1 On-Premises Consoleへのログイン

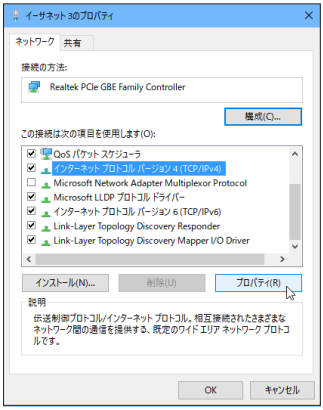
① 設定に利用するコンピュータのイーサネットポートとCloud Edgeの管理ポートをLANケーブルでつなぎます。

②コンピュータのIPアドレスを設定します。以下の手順に従って、ネットワークの設定を変更してください（ここではWindows 10での設定方法を紹介します）。

(1) スタートメニューの「設定」をクリックし、「Windowsの設定」を開きます。
(2)「ネットワークとインターネット」をクリックします。
(3) 左ペインの「イーサネット」をクリックし、「アダプターのオプションを変更する」をクリックします。

(4)「ネットワーク接続」ウィンドウが開くので、Cloud Edgeを接続するイーサネットポートをクリックし、「この接続の設定を変更する」をクリックします。

(5)「イーサネットのプロパティ」ダイアログボックスが開きます。中央の一覧から「インターネット プロトコル バージョン4（TCP/IPv4）」をクリックして選択し、「プロパティ」をクリックします（チェックマークを外さないように注意してください）。



(6)「インターネット プロトコル バージョン4（TCP/IPv4）」ダイアログボックスが開きます。「次のIPアドレスを使う」をクリックし、以下を入力して「OK」をクリックします。

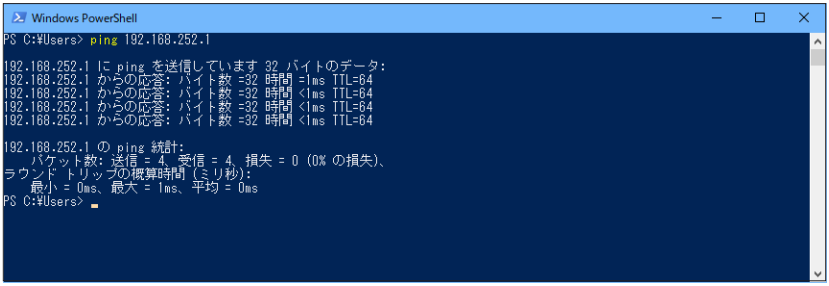
IPアドレス：192.168.252.2
サブネットマスク：255.255.255.0
（デフォルトゲートウェイとDNSサーバーは入力不要です）

(7)「イーサネットのプロパティ」ダイアログボックスを閉じます。

③コンピュータとCloud Edgeが接続できているかどうかを確認します。

(1) Windowsのスタートボタンを右クリックしてメニューを開き、「Windows PowerShell」をクリックします。
(2) Windows PowerShellが開いたら、コマンドラインに以下を入力します。
> ping 192.168.252.1

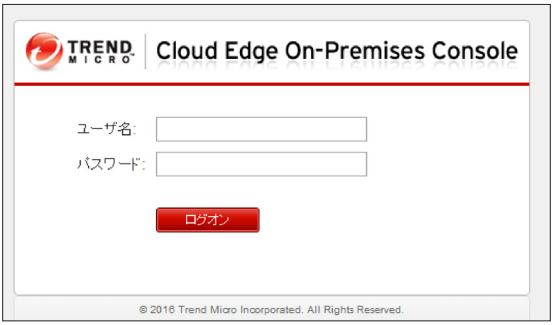
(3) 以下の画面のように応答があれば、コンピュータとCloud Edgeは接続できています。



タイムアウトが表示された場合は、LANケーブルが正しく接続されているか、②の設定に問題がないかをもう一度確認してください。

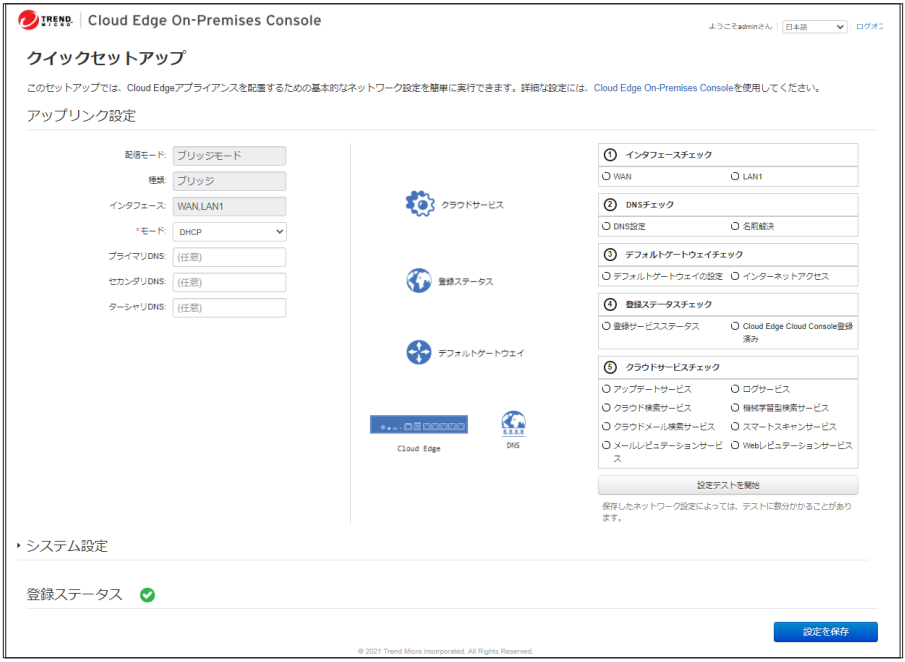
④設定に利用するコンピュータでWebブラウザを開き、アドレスバーに以下のURLを入力します。
https://192.168.252.1:8443

⑤ WebブラウザにCloud Edge On-Premises Consoleのログイン画面が表示されます。ログイン画面が表示されない場合は、コンピュータのネットワーク設定を確認し、DHCPを有効にしてください。DHCPを使用しない場合は、管理インタフェースと同じセグメントのIPアドレス（例：192.168.252.100）を設定します。



⑥「ユーザ名」「パスワード」にそれぞれ以下の文字列を半角英字で入力します。
ユーザ名：admin
パスワード：adminCloudEdge

⑦「クイックセットアップ」の画面が開きます。英語で表示されている場合はページ右上の「English」をクリックし、プルダウンメニューから「日本語」を選択してください。



ワンポイントアドバイス

管理ポートに接続するコンピュータは、有線LANポートを備えていれば、デスクトップPCでもノートPCでもかまいません。Windows PCの場合、電源を切らずにそのまま有線LANポートに接続されているケーブルを外し、付属のケーブルを使ってCloud Edgeの管理ポートと接続します。

ケーブルを接続して1～2分ほど待つと、Cloud EdgeのDHCPサーバからIPアドレスが割り当てられ、On-Premises Consoleに接続できるようになります。なお、On-Premises Consoleに接続するPCのLANポートが1つだけの場合、ネットワークセグメント（192.168.252.x）が異なる内部ネットワークやインターネットにアクセスすることはできません。

2.3.2 ブリッジモードの接続設定

①「クイックセットアップ」の「アップリンク設定」を確認します。

1.「配信モード」は、アプライアンス本体にある背面パネルのモード設定に従って「ブリッジモード」に設定されています。
2.「インタフェース」は「WAN」「LAN1」の固定になります。ブリッジモードでは、デフォルトの設定で「LAN2」「LAN3」が無効になります。
3.「モード」は初期設定で「DHCP」になっています。

固定IPアドレスを割り当てる場合は「モード」を「静的」に変更して、以下の項目をすべて入力してください。

IPv4アドレス・・・Cloud Edgeに割り当てる固定IPアドレスを入力します（例：192.168.1.50）

IPv4ネットマスク・・・ネットワークのサブネットマスクを入力します（例：255.255.255.0）※クラスCの場合

IPv4デフォルトゲートウェイ・・・ネットワークのゲートウェイ（ルータなど）のIPアドレスを入力します（例：192.168.1.1）

プライマリDNS・・・ネットワークのプライマリDNSサーバのIPアドレスを入力します（例：192.168.1.1）※一般的にはゲートウェイと同じIPアドレス

② 次に「システム設定」で「ホスト名」と「NTPサーバ」を確認します。初期設定は以下のとおりです。特に設定を変更する必要がなければ、初期設定のままでかまいません。

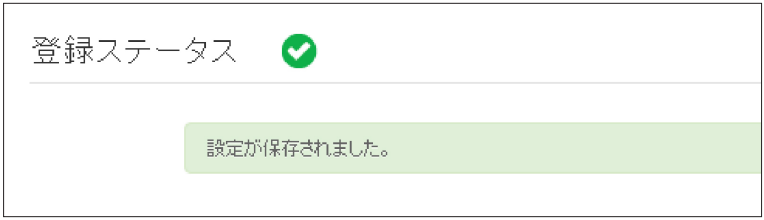
・ホスト名：localhost.localdomain
・サーバ：0.pool.ntp.org

ワンポイントアドバイス

On-Premises ConsoleからLAN2、LAN3ポートのステータスを変更できます。なお、LAN2、LAN3ポートのステータスは、Cloud Edge Cloud Consoleから確認することはできます。

③確認を終えたら「設定テストを開始」をクリックします。「WAN」接続、「DNSチェック」「デフォルトゲートウェイチェック」「登録ステータスチェック」のそれぞれに緑色のチェックマークが付くことを確認し、「設定を保存」をクリックします。

「登録ステータス」に緑色のチェックマークが付き、「設定が保存されました」と表示されたら完了です。



2.3.2.1 ソフトウェアスイッチの接続設定

① On-Premises Consoleのメニューにある「ネットワーク」をクリックし、左ペインの「ブリッジ」をクリックして、「名前」の下の「br0」をクリックします。

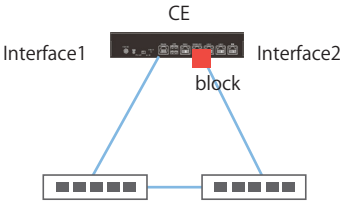
②「ブリッジの追加／編集」が開いたら、以下の設定を変更します。

1.「種類」をクリックして「ソフトウェアスイッチ」を選択します。

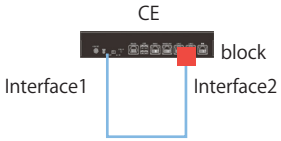
2.「スイッチインターフェイス」で利用するLANポートにチェックを入れます。「WAN」「LAN1」は必須（チェック済み）、「LAN2」「LAN3」は選択可能です。LAN2／LAN3を有効にすると、自動的にL2ポートとして有効になり、MTU/帯域以外の設定はできなくなります。

3.「モード」「MTU」の設定は、ブリッジモードと同じです。

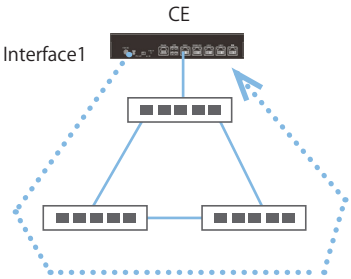
4.「詳細設定」をクリックし、「スパニングツリープロトコルを有効にする」場合は、チェックを入れます。この機能を有効にすると、Loopを防止することができます。



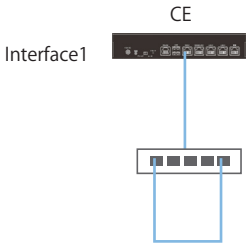
対応可能



対応可能



対応不可



対応不可

ワンポイントアドバイス

ソフトウェアスイッチ機能には、以下の制限事項があります。

- 電源オフ／障害発生時のバイパス機能はWAN-LAN1間のみの対応です。電源オフ／障害発生時は、LAN2、LAN3で通信できません。
- LANポート間のトラフィックにつきまして、メール検査は実行しません。メール以外のセキュリティ機能はポリシー設定に基づいて有効です。

2.3.3 ルーティングモード

①「クイックセットアップ」の「アップリンク設定」を確認します。

1.「配信モード」は、アプライアンス本体にある背面パネルのモード設定に従って「ルーティングモード」に設定されています。

2.「WANインタフェース」は「WAN」の固定になります。

3.「モード」をクリックして「PPPoE」を選択します。

「ユーザ名」「パスワード」にISPから提供されたアカウント情報を入力します。必要に応じてDNSも設定します。

② 次に「システム設定」で「ホスト名」と「NTPサーバ」を確認します。初期設定は以下のとおりです。特に設定を変更する必要がなければ、初期設定のままでかまいません。

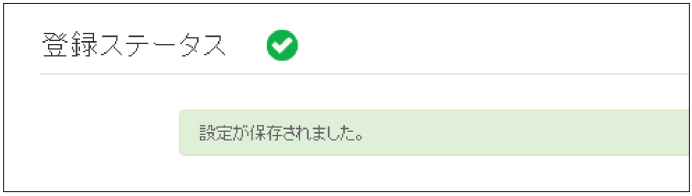
・ホスト名：localhost.localdomain
・NTPサーバ：0.pool.ntp.org

ワンポイントアドバイス

Cloud Edge 5.2以降は、On-Premises ConsoleからLAN2、LAN3ポートのステータスを変更できるようになりました。以前のバージョンでは、Cloud Edgeに割り当てられたIPアドレスが、LAN2、LAN3にデフォルトで割り当てられているIPアドレス（192.168.252.101, 192.168.252.102）と競合すると、Cloud Edge Cloud ConsoleからもOn-Premises ConsoleからもIPの変更ができず、初期出荷状態へのリセットが必要でした。なお、LAN2、LAN3ポートのステータスは、Cloud Edge Cloud Consoleから確認することはできます。

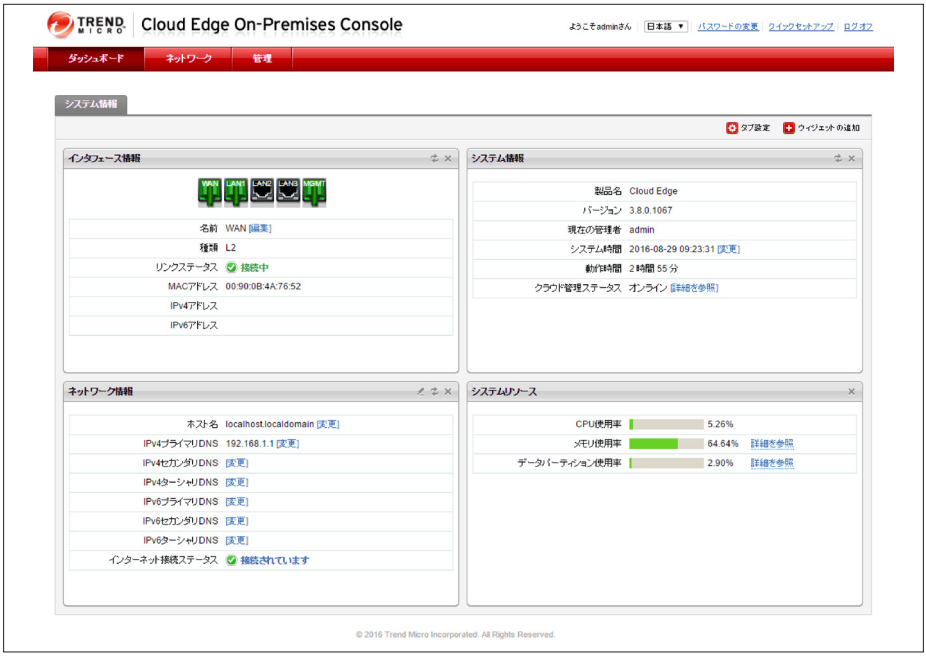
③ 確認を終えたら「設定をテスト」をクリックします。「DNS設定」「トラフィックのルーティング」「インターネット接続」のそれぞれに緑色のチェックマークが付くことを確認し、「設定を保存」をクリックします。

「登録ステータス」に緑色のチェックマークが付き、「設定が保存されました」と表示されたら完了です。



2.4 On-Premises Console の初期設定

クイックセットアップの初期設定を終えたら、「クイックセットアップ」のタイトル下にある説明文中の「Cloud Edge On-Premises Console」をクリックし、On-Premises Consoleの画面に切り替えます。



ここでは「コンポーネントのアップデート」「パスワードの変更」「設定のバックアップ」の3つを行います。

ワンポイントアドバイス

On-Premises Consoleのダッシュボードでは、Cloud Edgeアプライアンス本体のシステム情報を確認することができます。

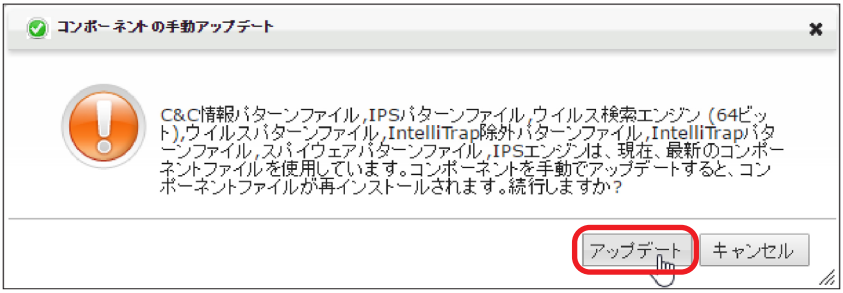
2.4.1 コンポーネントのアップデート

① On-Premises Consoleのメニューにある「管理」をクリックし、左ペインの「アップデート」をクリックします。

②「コンポーネントのアップデート」をクリックすると、Cloud Edgeにインストールされているコンポーネントの一覧が表示されます。

ここでコンポーネントに最新バージョンがあるかどうかを確認します。最新バージョンのコンポーネントが利用可能な場合は、「最新バージョン」のバージョン番号が赤色で表示されます。

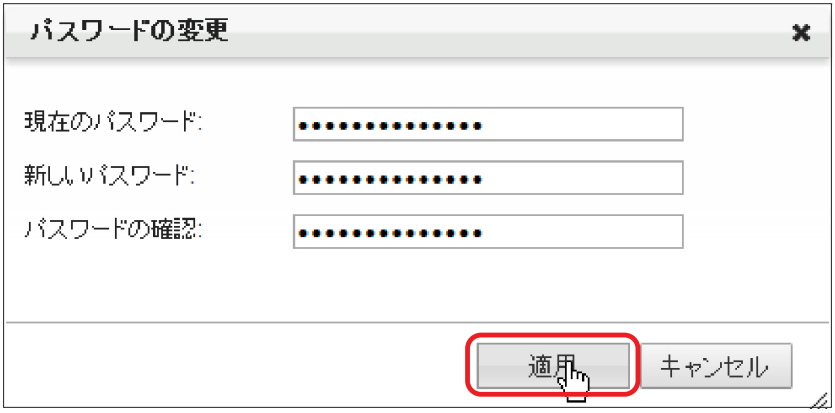
③ アップデートするコンポーネントをクリックして選択し、「アップデート」をクリックします。「続行しますか？」というダイアログボックスが表示されたら、「アップデート」をクリックします。



2.4.2 パスワードの変更

① 画面の右上にある「パスワードの変更」をクリックします。

② 「現在のパスワード」と「新しいパスワード」「パスワードの確認」を入力し、「適用」をクリックします。



ワンポイントアドバイス

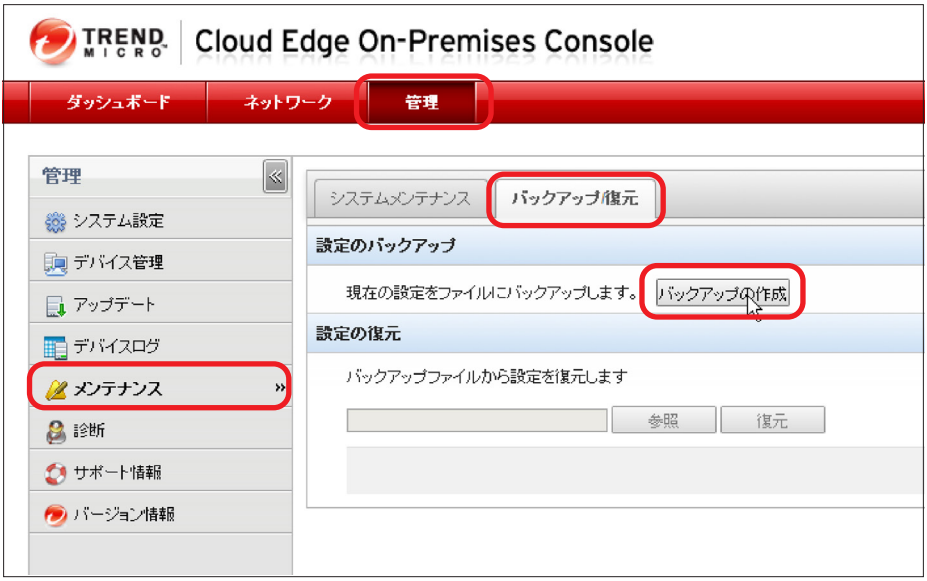
コンポーネントは、運用開始後にCloud Consoleを使ってアップデートを実施したり、アップデートのスケジュールを設定したりすることが可能です。ただし、最初に導入する際には必ずアップデートを実行し、運用開始直後のリスクを最小化してください。

また、パスワードは工場出荷時にすべて同じものが設定されています。万一の不正アクセスを防ぐためにも変更することをお勧めします。

2.4.3 設定のバックアップ

① On-Premises Consoleのメニューにある「管理」をクリックし、左ペインの「メンテナンス」をクリックします。

②「バックアップ/復元」をクリックし、「バックアップの作成」をクリックします。



③ ブラウザに従って、バックアップファイルをコンピュータの任意のフォルダに保存します。

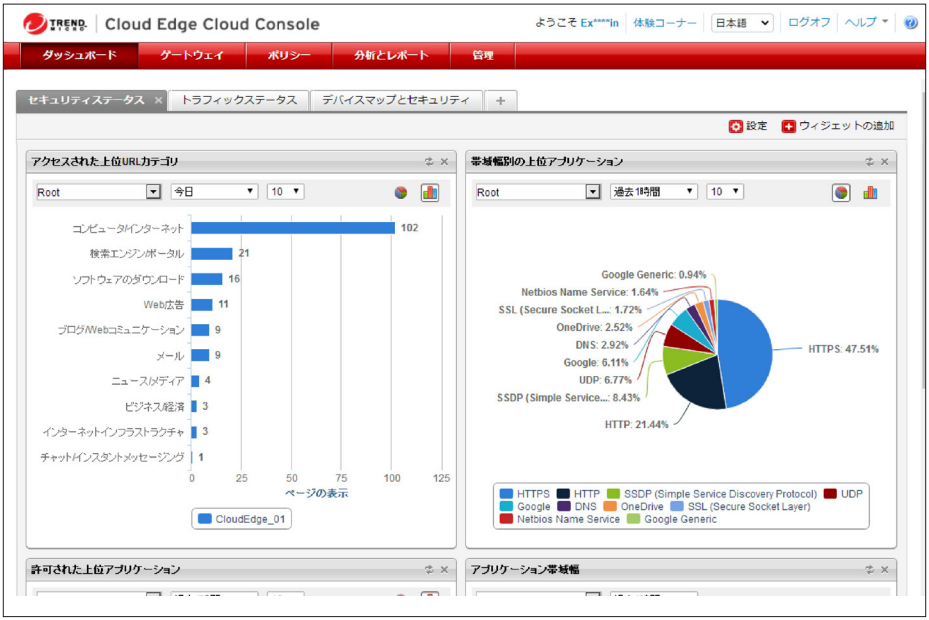
ワンポイントアドバイス

バックアップは、運用開始後にCloud Consoleを使って実施したり、スケジュールを設定したりすることも可能です。

2.5 Cloud Edge Cloud Console (CECC)へのログイン

Cloud Edge Cloud Console (CECC)は、Cloud Edge専用の管理ツールです。

クラウド上にホスティングされているため、地理的に離れた複数のネットワークに設置されたCloud Edgeアプライアンスにアクセスし、ユーザやセキュリティポリシーを一元的に管理できます。



Cloud Edge Cloud Console (CECC)の画面例

ワンポイントアドバイス

Cloud Edge Cloud Consoleの画面表記は、「日本語」のほかに「English（英語）」「繁體中文（中国語）」が選択できます。

2.5.1 Licensing Management Platform（LMP）へのアクセス

Licensing Management Platform（LMP）は、お客様がご利用中の製品/サービスのライセンスを管理し、トレンドマイクロのクラウド型セキュリティ製品（Trend Micro Security as a Service）の有効化と登録を行うためのポータルです。

① ブラウザを開いてLMPにアクセスします。LMPのURLは、販売店にご確認ください。

② 「ログインID」「パスワード」を入力し、「ログイン」をクリックします。アカウント情報は販売店にご確認ください。

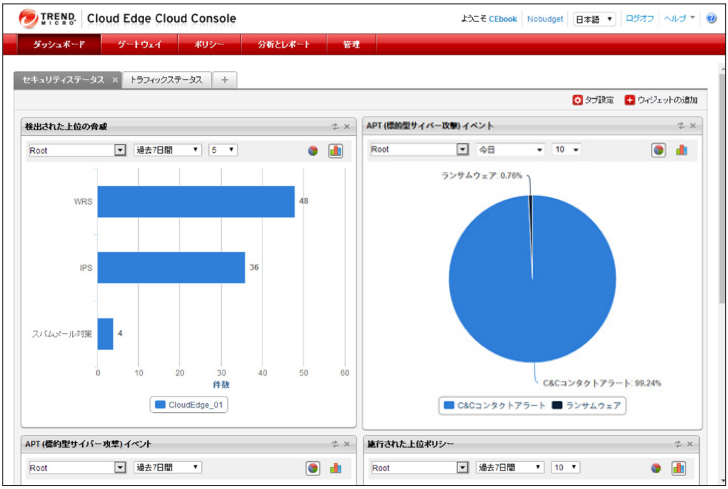
③ 「登録済みの製品/サービス」一覧が表示されます。

2.5.2 Cloud Edge Cloud Console (CECC)へのアクセス

LMPにログインすると、お客様がご購入された製品/サービス一覧が表示され、Cloud Edge Cloud Console (CECC)へのシングルサインオンが可能になります。

①「登録済みの製品/サービス」の「アクション」にある「コンソールを開く」をクリックします。

② Cloud Edge Cloud Console (CECC)が表示されます。



ワンポイントアドバイス

Cloud Edge Cloud Console (CECC)で管理者アカウントを登録すると、LMPを経由せず直接ログインできます。「管理者アカウント」につきましては第4章 4.5.2 管理者アカウントを管理するを参照してください。

2.6 ゲートウェイの登録

最初にCloud Edgeを管理するための登録を行います。複数台のCloud Edgeを管理する場合は、この作業を台数分だけ行ってください。

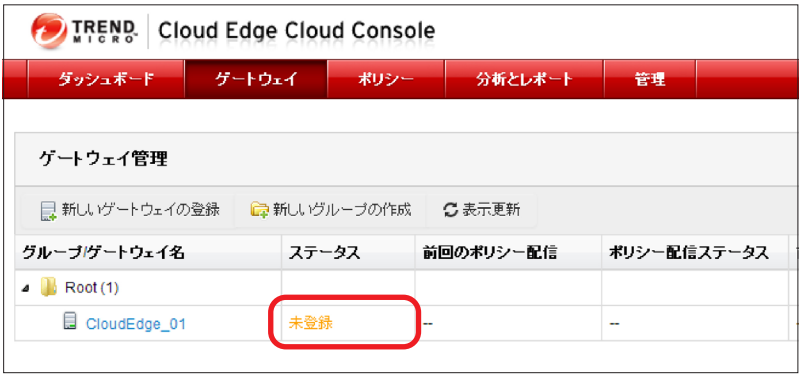
3.2.1 新しいゲートウェイの登録

① Cloud Edge Cloud Console (CECC)のメニューにある「ゲートウェイ」をクリックし、「新しいゲートウェイの登録」をクリックします。

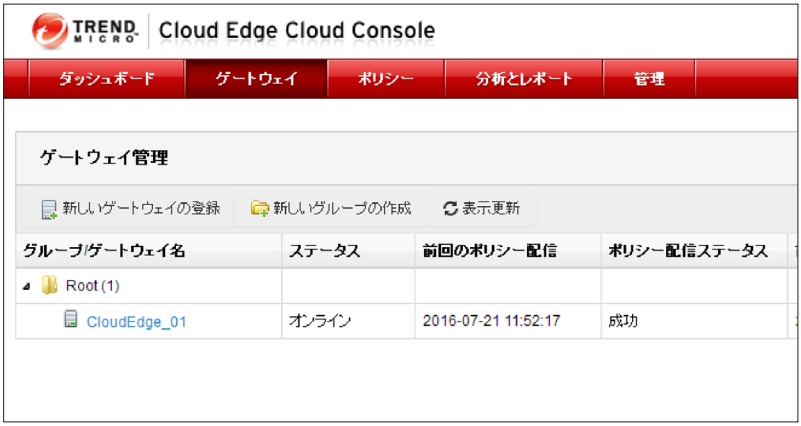
②「表示名」に任意の名前を入力し、「シリアル番号」を入力して「保存」をクリックします。

シリアル番号は、アプライアンス本体同梱のシールに記載されています。またはOn-Premises Consoleの「管理」→「デバイス管理」→「クラウド管理」で確認できます。

③新しく登録したゲートウェイが表示されます。登録した時点では「ステータス」が「未登録」と表示されます。



④しばらく経つと、「ステータス」が自動的に「オンライン」に変わります。



ワンポイントアドバイス

「ステータス」が自動的に「オンライン」に変わらない場合は、
以下のページをご参照ください
【Cloud Edgeのステータスがオフラインになっている場合の対処方法】
https://success.trendmicro.com/jp/solution/000291637

トラブルシューティング Cloud Edge　サポートページについて

Cloud Edge の設置および利用に関してサポートページをご用意しております。
設置、運用時の「困った」にご利用ください。
【ビジネスサポート Cloud Edge】
https://tmqa.jp/ce

【オンラインヘルプ】
https://tmqa.jp/aboutce

トレンドマイクロ株式会社

〒151-0053 東京都渋谷区代々木2-1-1　新宿マインズタワー

BR-CE-007