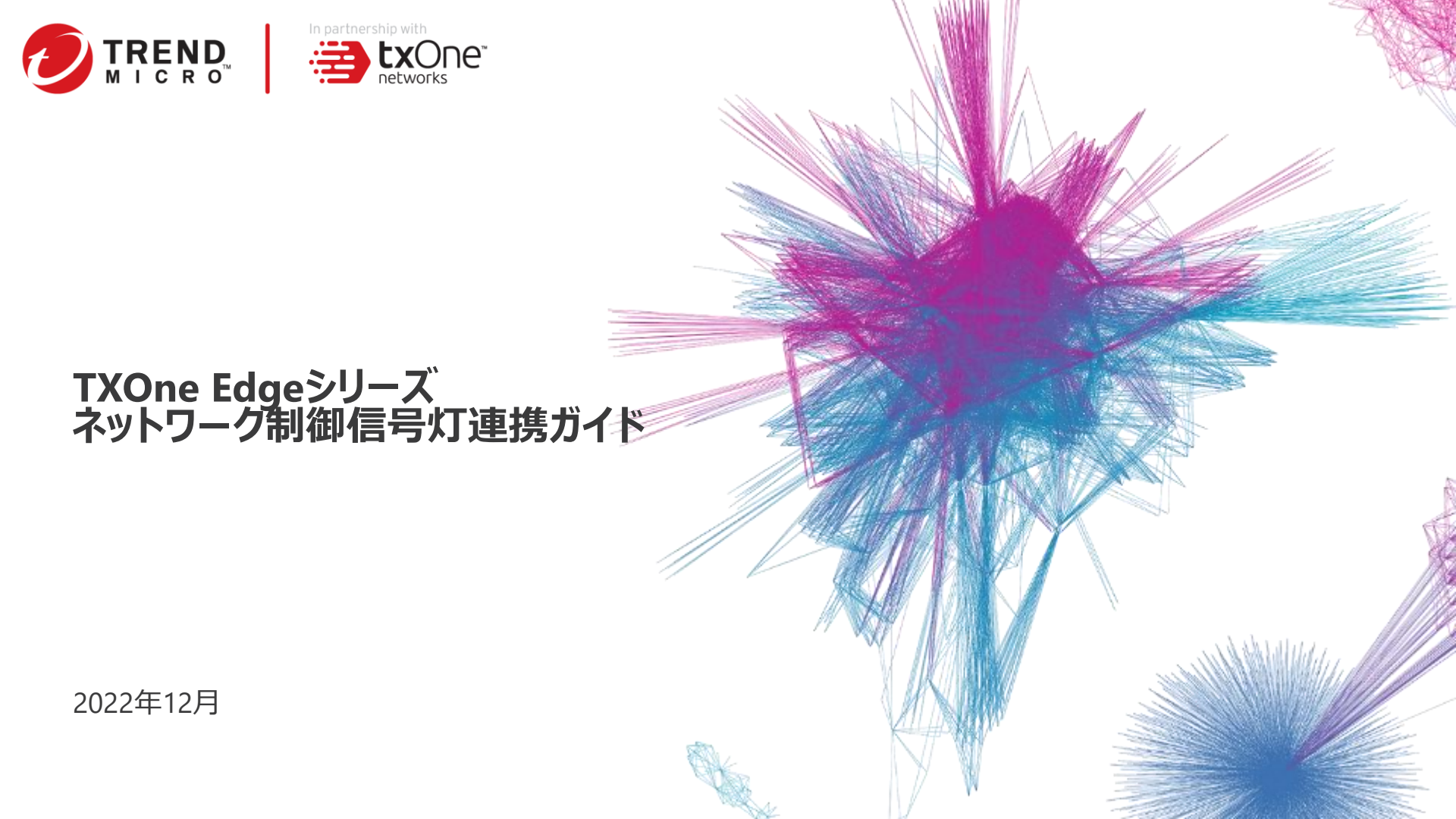


TXOne Edgeシリーズ
ネットワーク制御信号灯連携ガイド

2022年12月

本書について

- 本資料は、Trend Micro Edgeシリーズとパトライト社信号灯の連携に関する内容を記載しています。
- Trend Micro Edgeシリーズの基本機能については、トレンドマイクロ公式ホームページをご参照ください。
- 本資料は改訂日の情報を元に作成されているため、設定項目や記載されている画面イメージなどは現行のサービス内容とは異なる場合があります。あらかじめご了承ください。
- 本書は、2022年12月時点の製品仕様に基づいています。

用語と略称

用語や略称	正式名称、または用語の意味
ODC	OT Defense Console

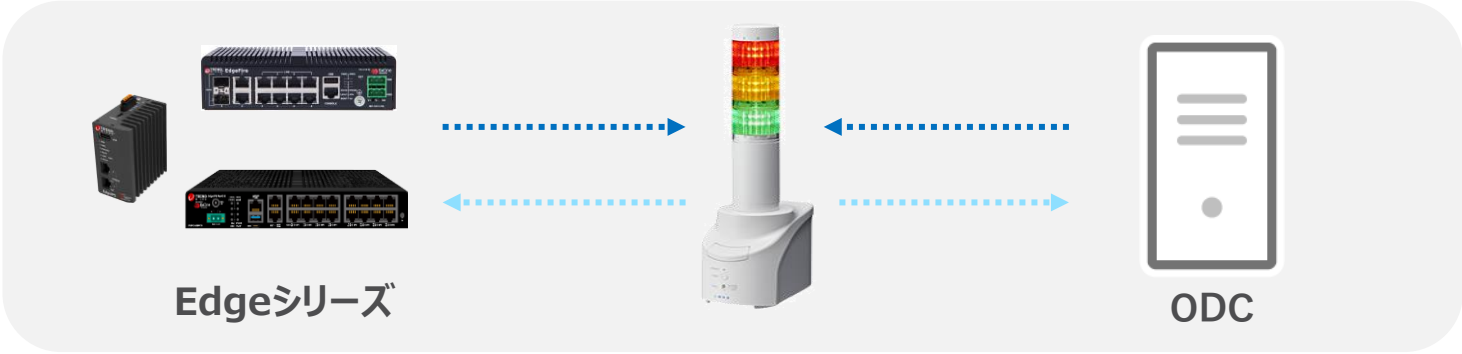
改訂履歴

版数	改訂日	備考
第1版	2022/12	第1版として公開

Edgeシリーズ連携ガイド　概要

- Trend Micro Edgeシリーズ,OT Defense Console(以下、ODC)と、ネットワーク監視表示灯 信号灯(以下 信号灯)を接続し、信号灯からのpingでの死活監視方法、Edgeシリーズまたは ODC から SNMP トラップを送信、信号灯で受信するための設定手順をご紹介します。

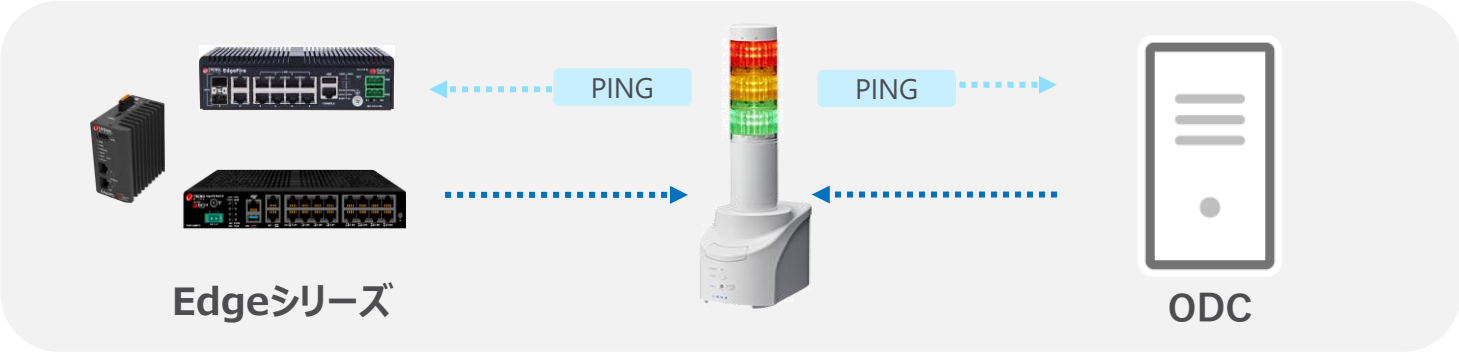
- トラップを送信することで Edgeシリーズ・ODC のハードウェア高負荷時、死活監視などが可能になります。 各機器の初期設定、IP アドレス設定や詳細な設定などは、それぞれの機器の取扱説明書や管理者ガイドをご参照ください。



PINGによる死活監視

PINGによる死活監視　概要

- 信号灯からPINGを送信することで Edgeシリーズ・ODC の死活監視などが可能になります。各機器の初期設定、IP アドレス設定や詳細な設定などは、それぞれの機器の取扱説明書や管理者ガイドをご参照ください。



PINGによる死活監視　設定手順

1. 信号灯の設定画面にログインし、Ping監視設定の項目を確認します。
2. 監視対象機器に対象となるEdgeデバイス・ODCのIPアドレス、Pingの送信回数・監視周期・送信個数を設定します。

Ping監視設定

設定番号	1

監視対象機器 1

監視対象アドレス	172.18.1.201
装置名	EdgeIPS
監視グループ設定	未登録
送信回数(0-30)	1
Ping監視周期(1-600)秒	10
送信個数(1-3)	1

監視対象機器 1 - 異常発生時の動作設定

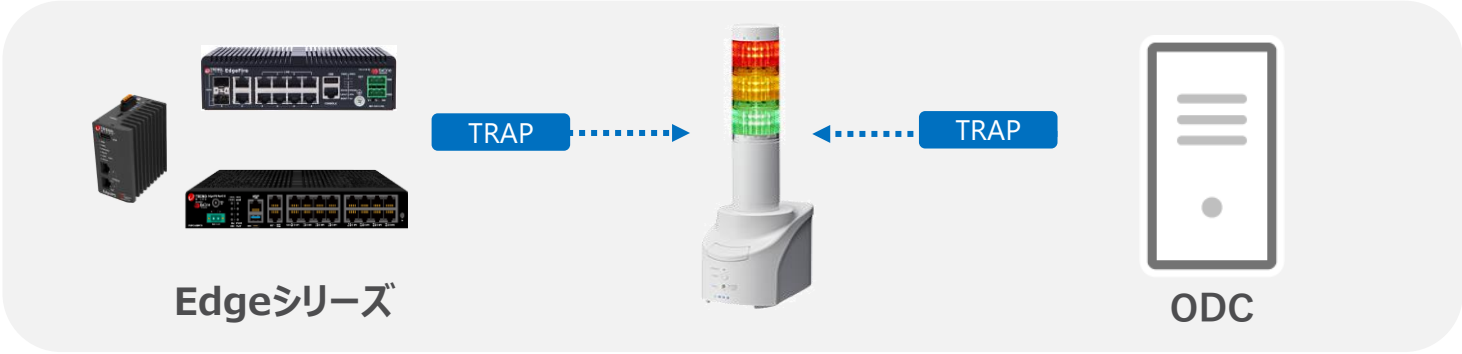
赤	点灯

SNMP TRAPによる監視

SNMP TRAPによる監視　概要

- Trend Micro Edgeシリーズ,OT Defense Console(以下、ODC)と、ネットワーク監視表示灯 信号灯(以下 信号灯)を接続し、Edgeシリーズまたは ODC から SNMP トラップを送信、信号灯で受信するための設定手順をご紹介します。

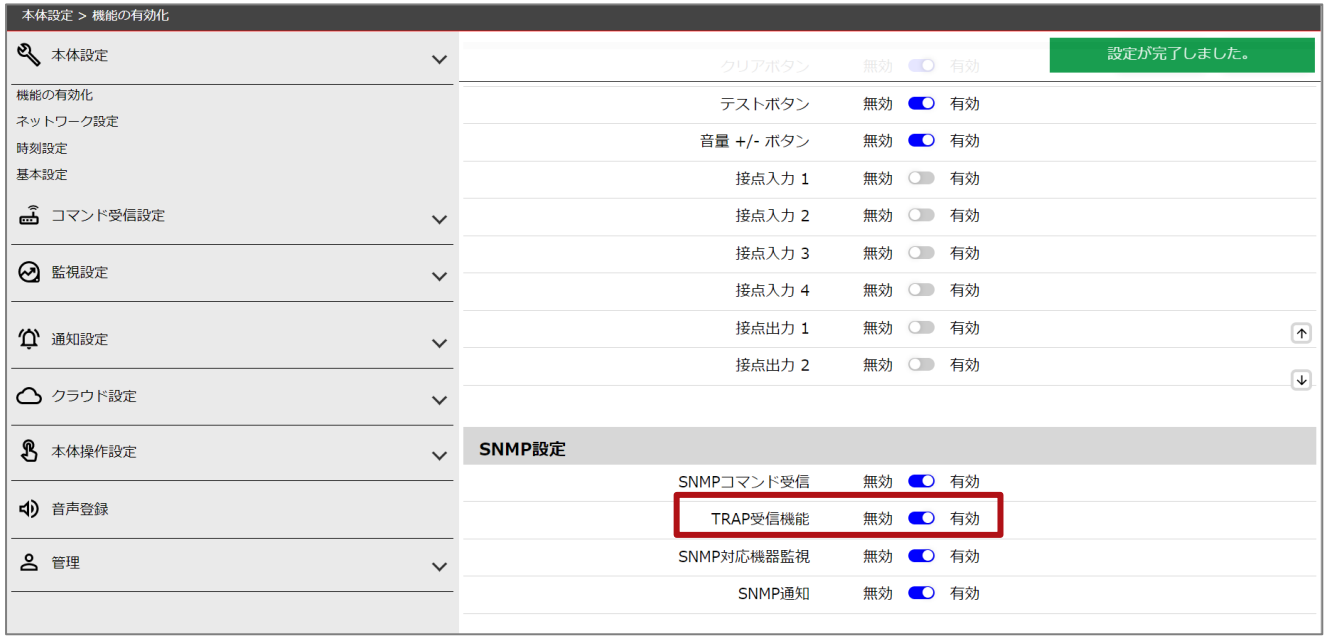
- トラップを送信することで Edgeシリーズ・ODC のハードウェア高負荷時、死活監視などが可能になります。 各機器の初期設定、IP アドレス設定や詳細な設定などは、それぞれの機器の取扱説明書や管理者ガイドをご参照ください。



SNMPによる監視　設定手順

信号灯

1. 信号灯の設定画面にログインし、TRAP受信機能が有効になっているか確認します。



SNMPによる監視　設定手順

2. TRAP受信基本設定より、使用するSNMPバージョンの指定と受信TRAPコミュニティを入力し、保存します。

SNMPによる監視　設定手順

信号灯

3. TRAP受信設定より、監視対象であるEdgeデバイスの情報を入力します。

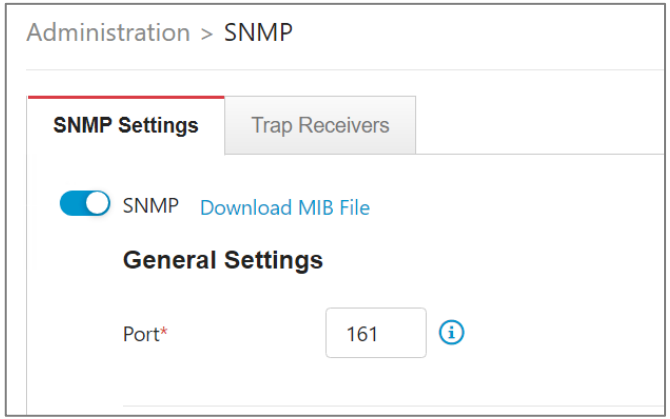
POINT :

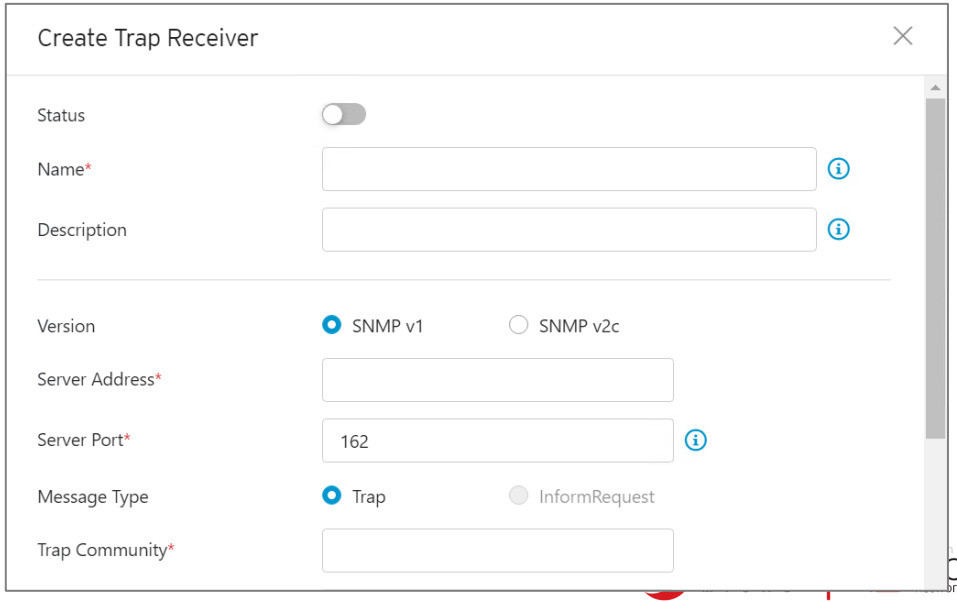
特定のTRAPのみ信号灯で通知したい場合には、TRAP番号を入力します。また特定のOIDと値で通知を行う場合にはvariable-bindingsを入力します。

SNMPによる監視　設定手順

ODC

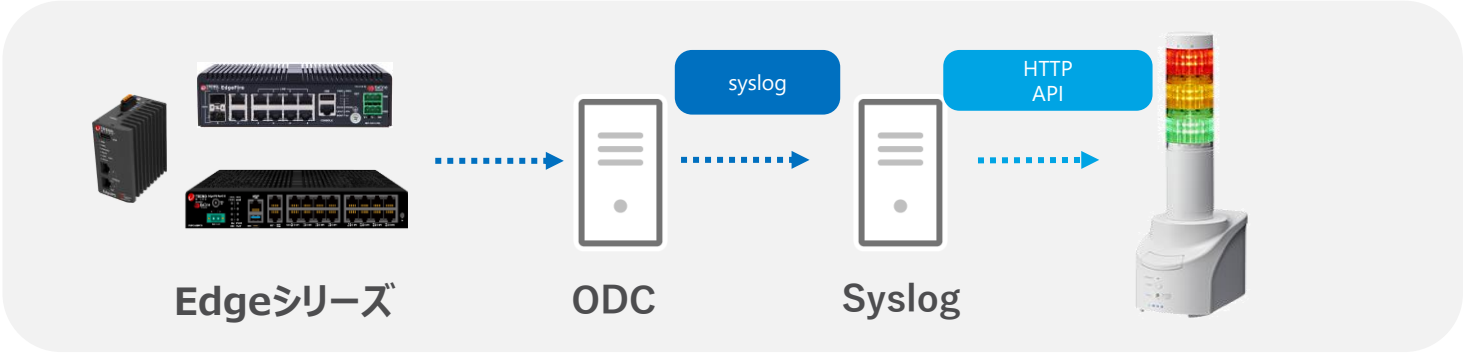
4. ODCにログインし、Administration > SNMPをクリックします。
5. SNMP Settingsより、SNMPを有効にします。
6. Trap Receiversの＋Addボタンより信号灯の情報を入力し、最後にSaveボタンをクリックします。





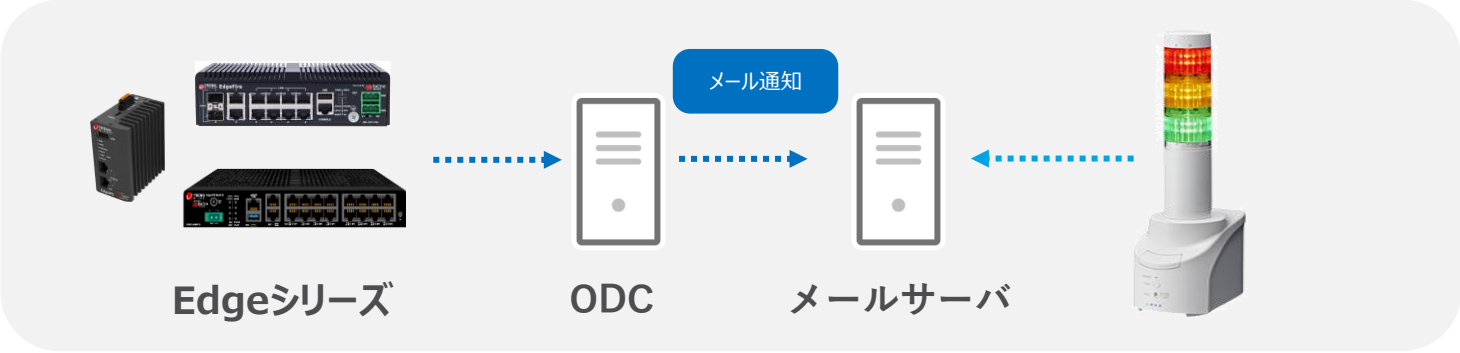
REF)Syslog-API連携による脅威検出

- ODCとSyslogを連携し、Syslog側で特定のログを検出した際に信号灯に向けてHTTP APIを投げることが可能です。
- 本連携によりEdgeシリーズ・ODC のシステム監視、IPSルール検知の通知などが可能になります。各機器の初期設定、IP アドレス設定や詳細な設定などは、それぞれの機器の取扱説明書や管理者ガイドをご参照ください。またSyslogの設定につきましては、ご利用されるSyslogの取扱説明書などをご参照ください。



REF)メールによる脅威検出

- ODCでメール設定を実施し、信号灯にてSMTPサーバを監視し、送信元メールアドレスやメール件名の文言をトリガーとして、Edgeシリーズ・ODC のシステム監視、IPSルール検知の通知などが可能になります。 各機器の初期設定、IP アドレス設定や詳細な設定などは、それぞれの機器の取扱説明書や管理者ガイドをご参照ください。



TREND MICRO

In partnership with txOne networks

THE ART OF CYBERSECURITY

An Innovative Approach to Cybersecurity

トレンドマイクロのクラウドセキュリティプラットフォームによる、日本におけるハイブリッドクラウドワークロードの自動保護。**実際のデータを使用し、トレンドマイクロの脅威リサーチャーでアーティストでもあるJindrich Karasekによって作成されました。**

サイバーセキュリティの専門家によるOTセキュリティ