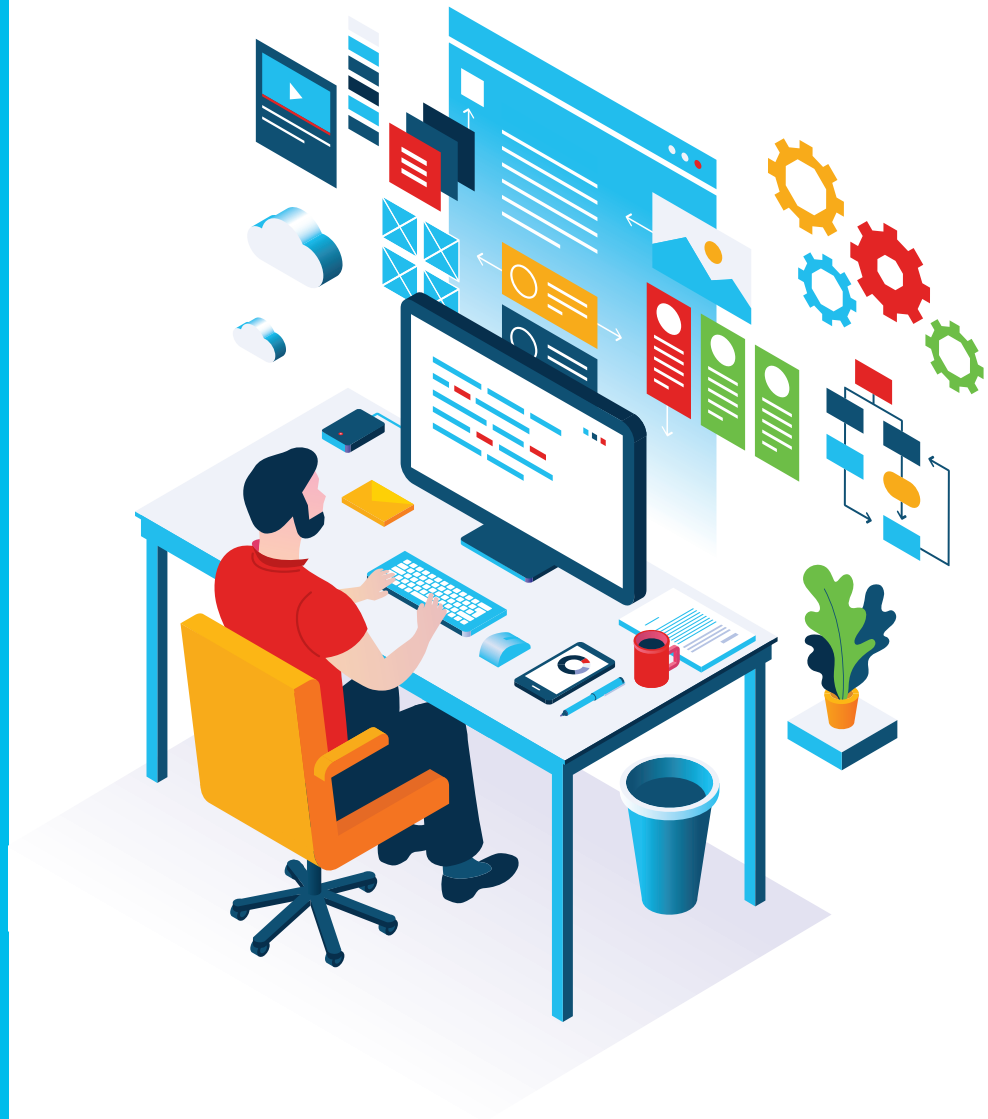
# 30分でわかる Cisco Defense Orchestrator ~ クラウドから Firewall を統合管理 ~

2020年11月12日

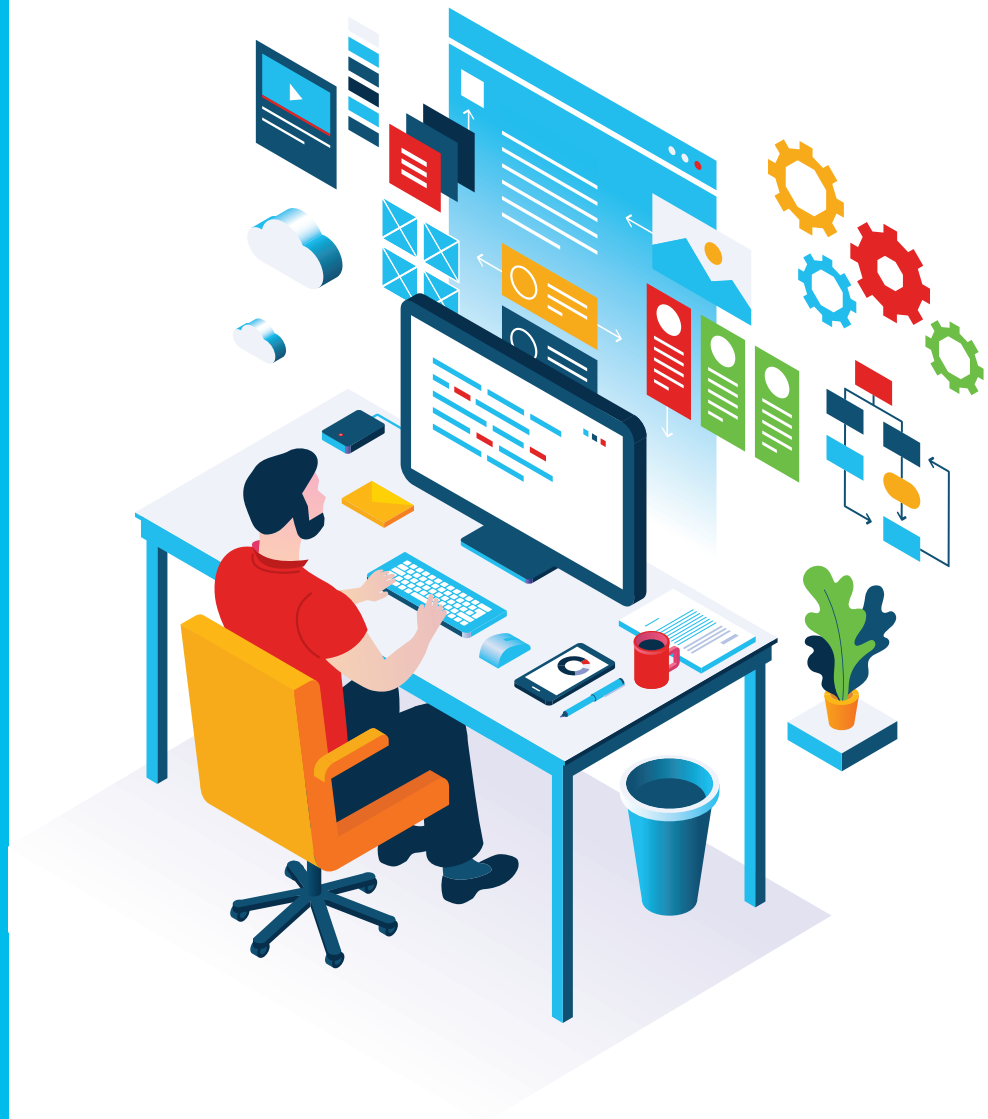
シスコシステムズ合同会社
セキュリティ事業 テクニカルソリューションズアーキテクト
小林 達哉 (tatskoba@cisco.com)

# ネットワークセキュリティ管理の作業負荷はとても大きい



# 今日のセキュリティ管理

- 多様なセキュリティデバイスやサービスへの対応が必要
- それぞれ異なり統一されない管理コンソールやポリシーフォーマット
- マニュアル、サイロになった変更管理プロセス



# 複雑性に起因する高コスト

- 非効率な作業プロセスが時間を無駄にしている
- それぞれのデバイスに対して製品を熟知したスタッフが必要になる
- ポリシーの一貫性が保てずエラーに繋がり、それが情報漏洩の潜在リスクを高めてしまう



無駄な時間

コストの上昇

情報漏洩のリスク

# 複雑性とセキュリティリスク

83%

ここ2年でネットワークセキュリティが複雑になったと考えている管理者の割合

94%

複雑性によりネットワークが脆弱になることを懸念している管理者


29%

ここ12ヶ月の間に複雑さが増したことにより発生したセキュリティインシデントを経験している管理者の割合

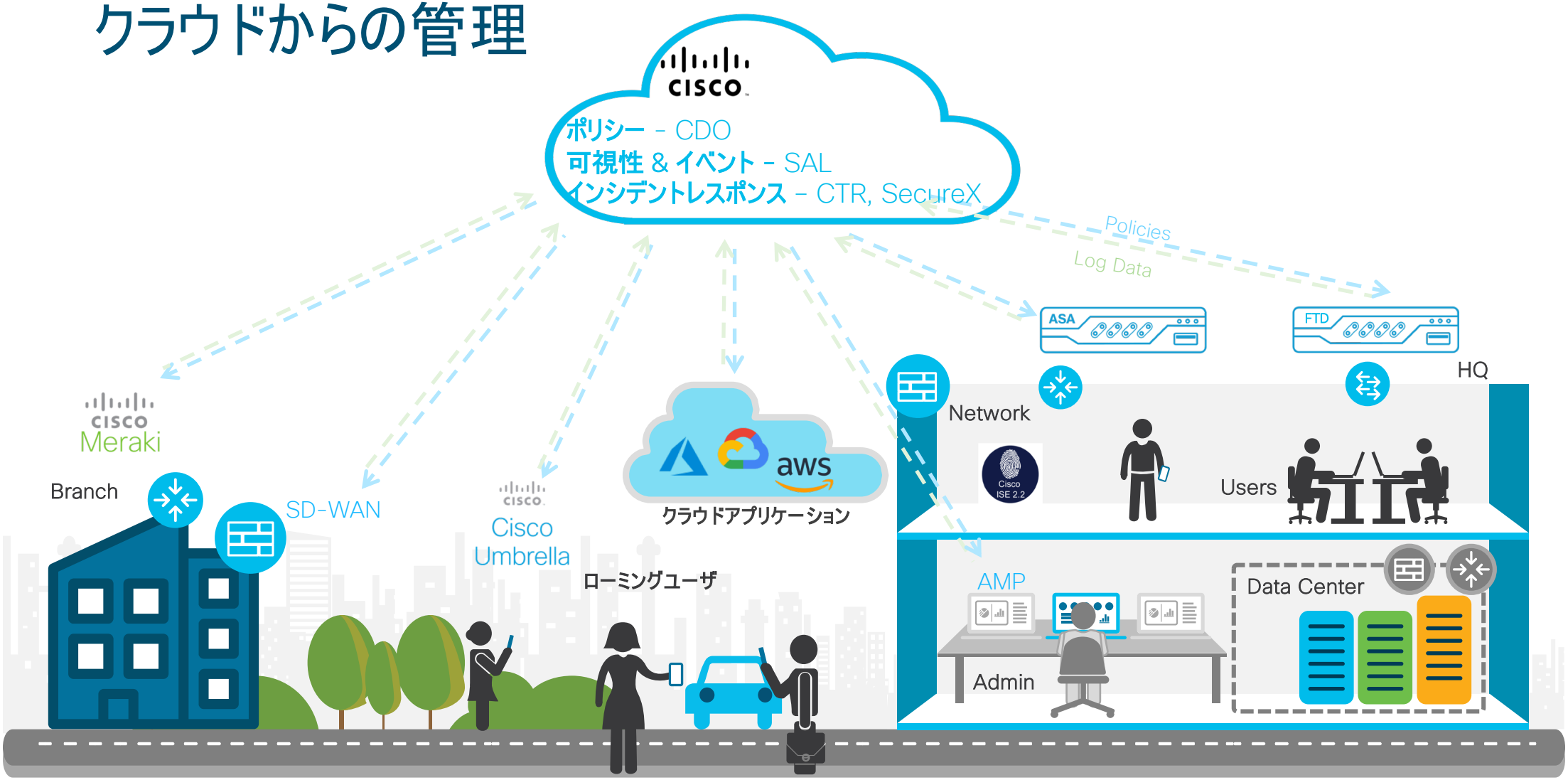
**88% の組織がネットワークポリシーの変更をもっと機敏に行いたいと考えている**



*Source: ESG Research, 2019*

# セキュリティポリシーとイベント管理の問題をクラウドで解決できないか？

# クラウドからの管理


cisco
ポリシー – CDO
可視性 & イベント – SAL
インシデントレスポンス – CTR, SecureX
Policies
Log Data
ASA
FTD
HQ
Network
Cisco ISE 2.2
Users
cisco Meraki
Branch
SD-WAN
cisco Cisco Umbrella
aws
クラウドアプリケーション
ローミングユーザ
AMP
Admin
Data Center

# Cisco Defense Orchestrator（CDO）の特長

## シンプル

セキュリティポリシーとデバイス管理の合理化

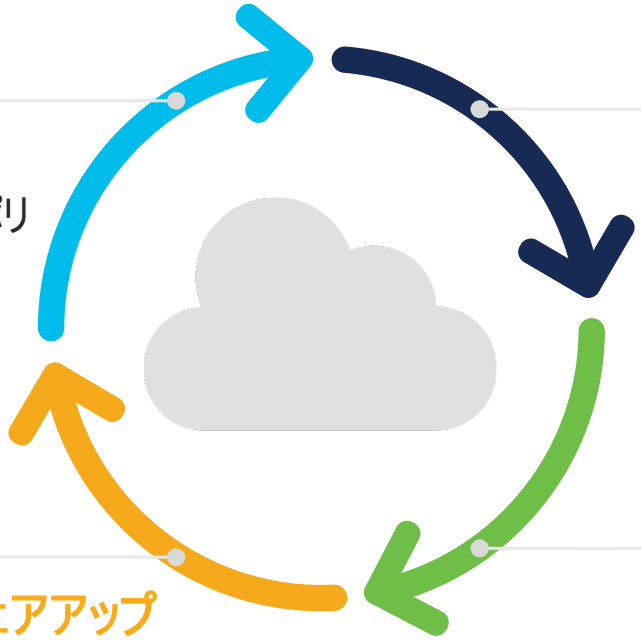
## 効率的

セキュリティ管理に費やす時間を最大90%削減

## 効果的

複雑性を排除しながら、セキュリティの向上を実現

# Cisco Defense Orchestrator でできること



## ポリシーの課題を解決

環境を横断的に、既存のセキュリティポリシーを分析し、迅速に最適化

## 一貫したセキュリティポリシー

一度セキュリティポリシーを作成すれば、ネットワーク全体で一貫したセキュリティ制御を数十・数百・数千という規模に拡大可能

## 簡単なファイアウォールソフトウェアアップグレード

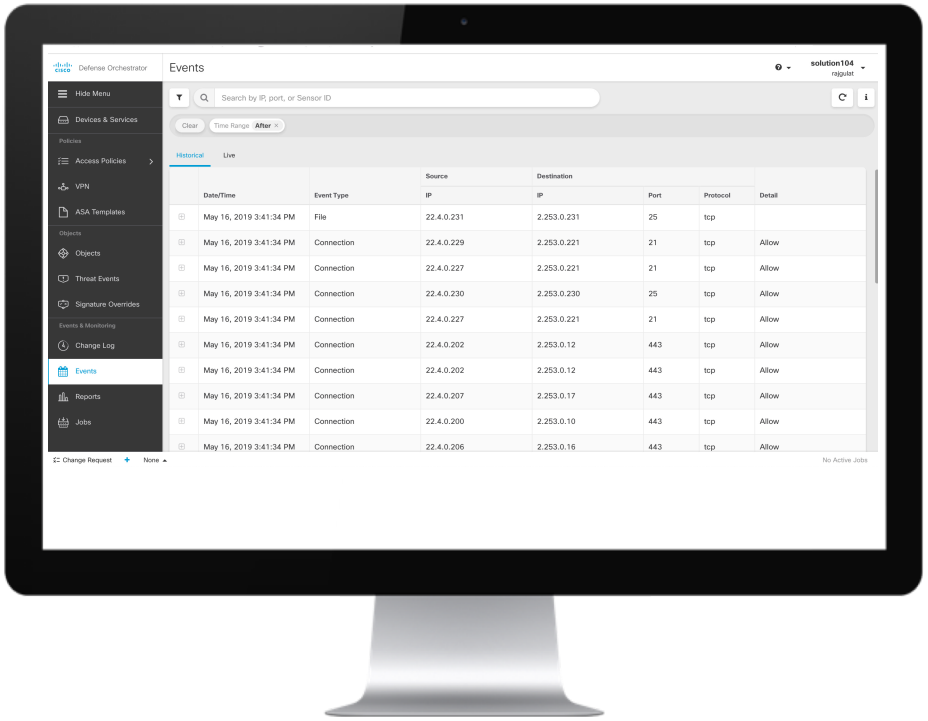
ソフトウェアのアップグレードは少ないクリックで完了可能なため、新機能やパッチの適用はより迅速に対応

## よりスマートな構成管理

全ての変更履歴をログに残せる
いつでもコンフィグレーションのロールバック可能

# [参考] Cisco Security Analytics and Logging

## 高度な分析機能を備えたクラウドベースのロギングによる効果的なポリシー管理




- ファイアウォールおよびネットワークログをクラウドに安全に保存し、CDOからアクセスおよび検索可能
- ログを分析し、高忠実度（High-Fidelity）のアラートに識別、強化する
- インシデントへの対応がよりスマートになり、調査にかかる時間を削減
- 業界最高のセキュリティ分析を使用して侵害検知能力を強化

# サポートプラットフォーム

| | |
|---|---|
| Cloud FW | AWS & Azure (ASAv 8.4+, FTDv 6.5+) |
| Virtual FW | KVM & VMware (ASAv 8.4+, FTD 6.4+) |
| Meraki MX | Meraki MX |
| Hardware Firewall Platforms | Firepower 1000 (ASA 9.13+, FTD 6.4+)<br>ASA 5500-X (ASA 8.4+, FTD 6.4+)<br>Firepower 2100 (ASA 9.8+, FTD 6.4+)<br>Firepower 4100 & 9300 (ASA8.4+, FTD 6.5+) |

常に更新されているため、最新情報はデータシートを参照

https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html

# クラウド管理によるメリット

01 柔軟なスケーラビリティ

02 メンテナンス不要

03 新機能の早期利用

04 コスト削減

- 毎週の大型機能拡張
- 小さな機能拡張は日常的に実施
- フィードバックから実現までのスピード
- 段階的な機能の拡張

99.99999%

Uptime

1日以内での
プロビジョニング

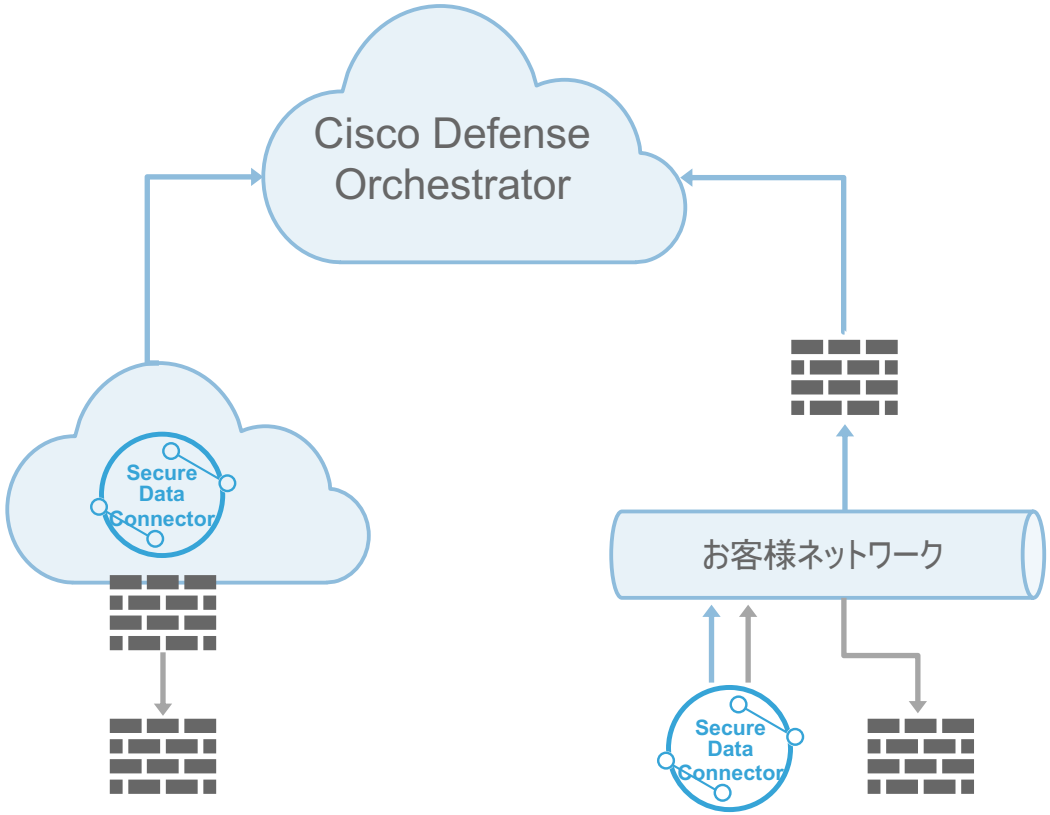
導入したモデルに合わせた
サブスクリプション

サポートコストの減少

# CDO 接続形態

## シンプルなユーザーインターフェイス


## 二種類の接続形態

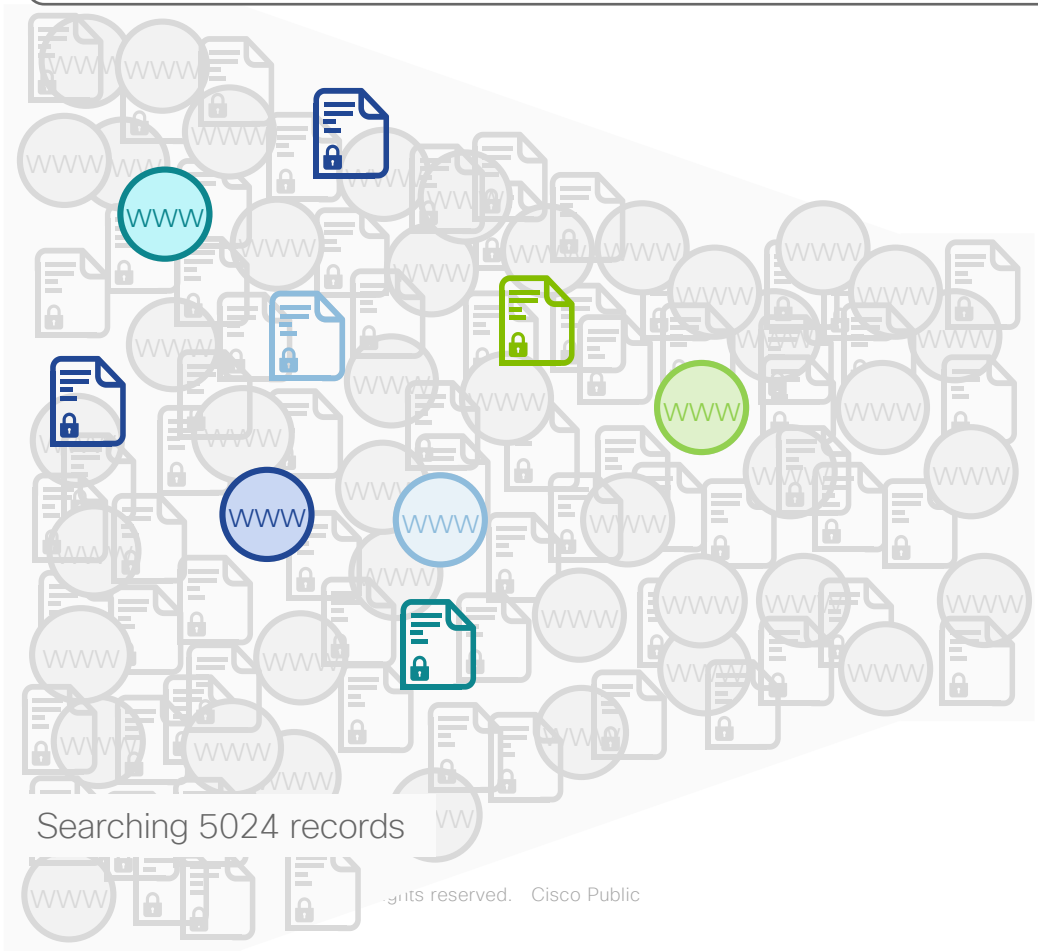



1 コネクタをクラウドに設置

2 コネクタをオンプレミスに設置

# CDO ユースケース: キーワードによるポリシー検索

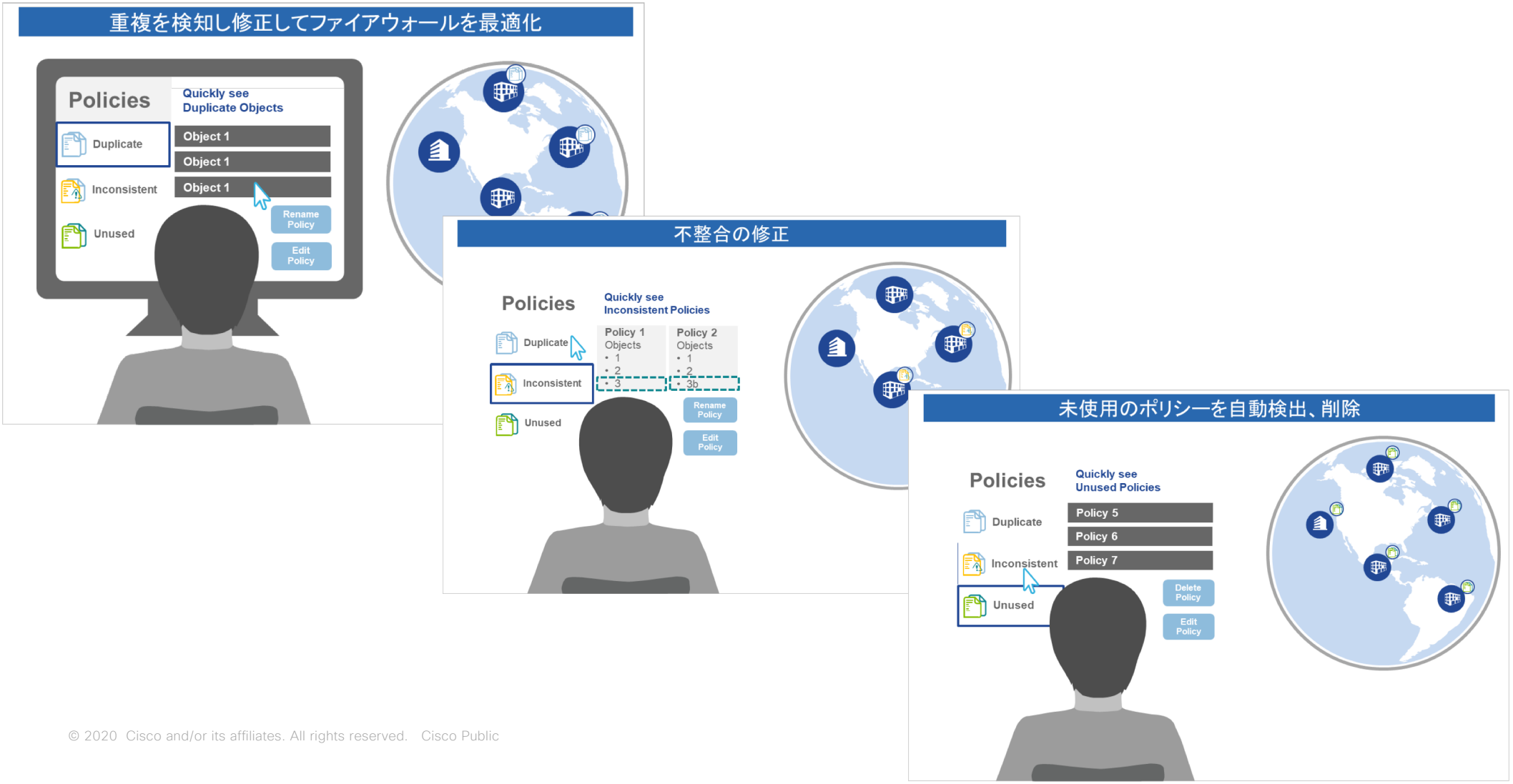
Facebook




**“Facebook” 検索結果**

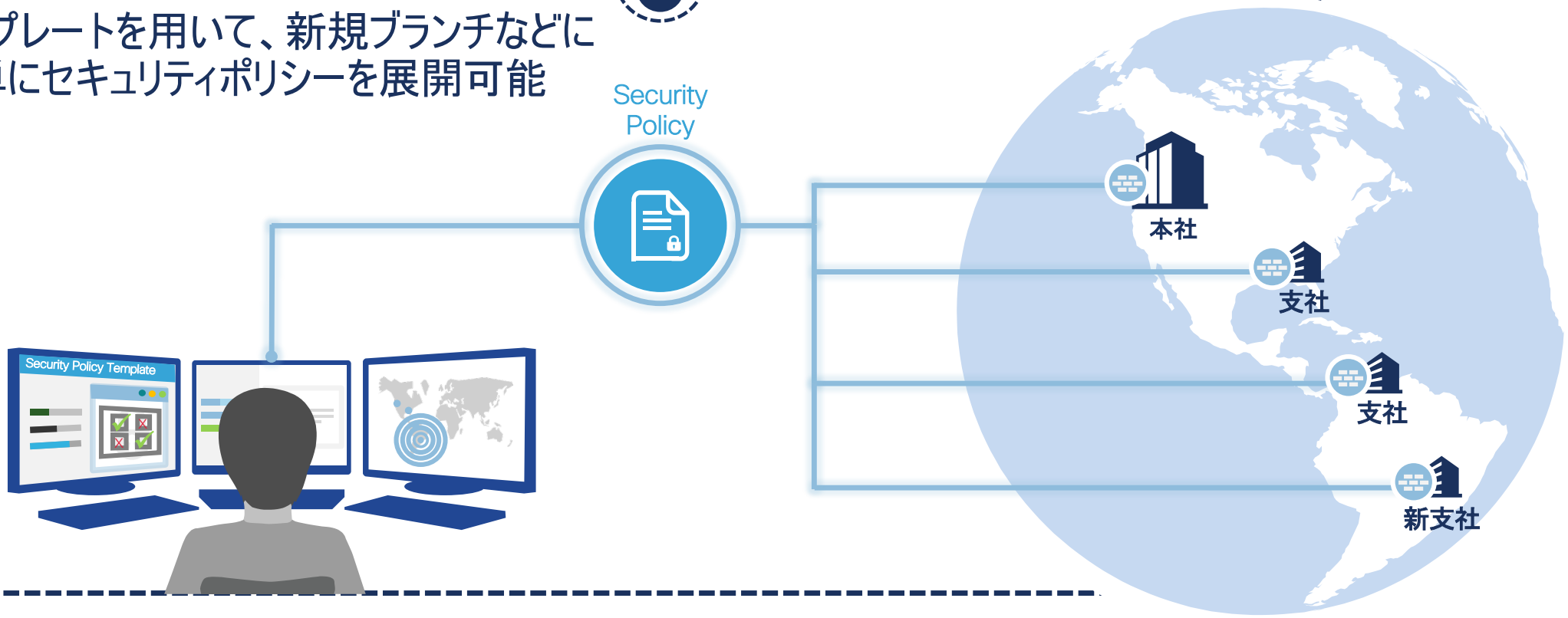
| | | | |
|---|---|---|---|
| **Facebook.com** | Domain/IP | Umbrella | 15 Block<br>13 Allow |
| **Facebook Chat** | Application | FTD | 15 Block<br>13 Allow |
| **Facebook Games** | Application | FTD | 20 Block<br>15 Allow |
| **Social Networking** | URL Category | FTD | 10 Block<br>10 Allow |

# CDO ユースケース: ポリシー/オブジェクトの効果的な分析

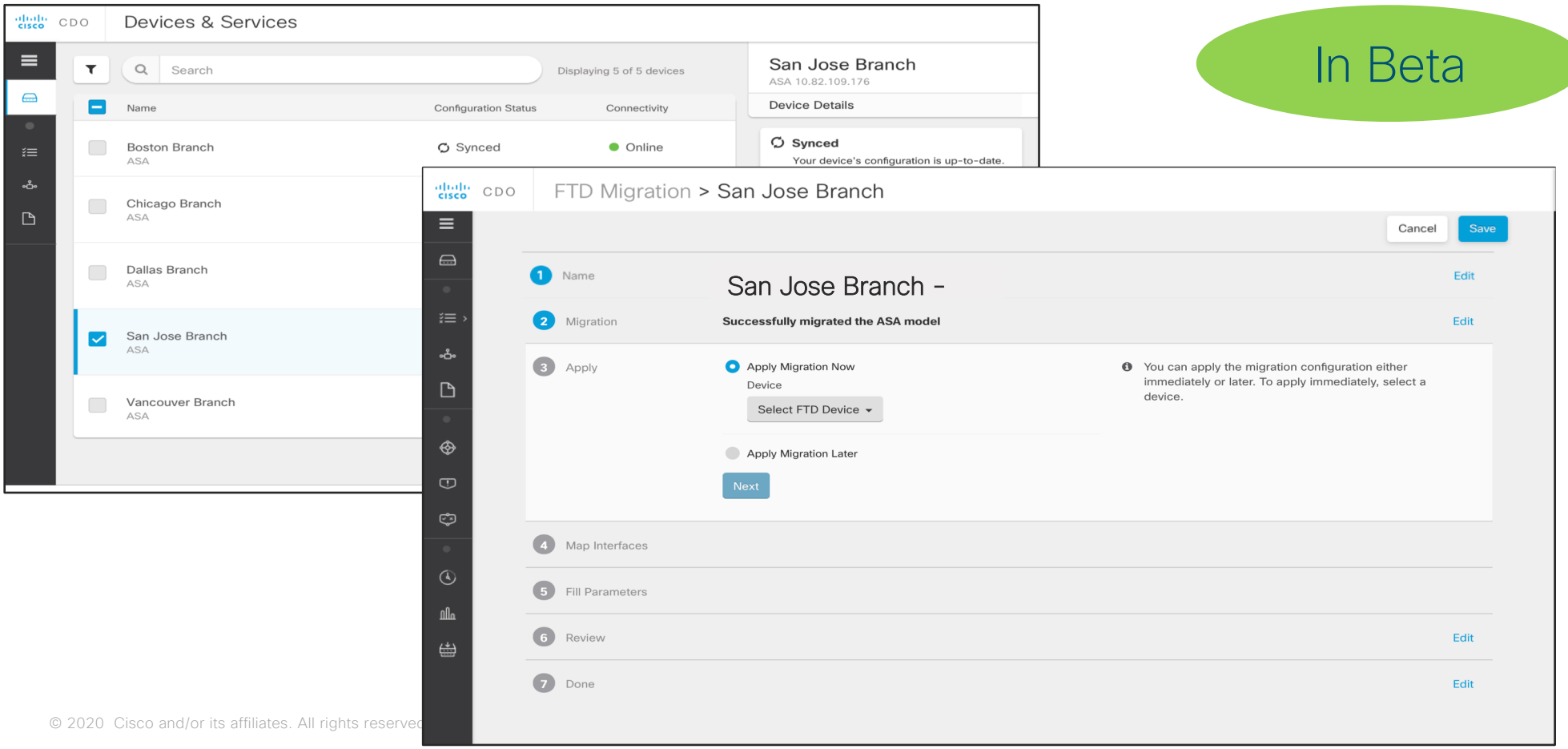


# CDO ユースケース:
# テンプレート利用によるセキュリティポリシー展開の簡素化

テンプレートを用いて、新規ブランチなどに
簡単にセキュリティポリシーを展開可能

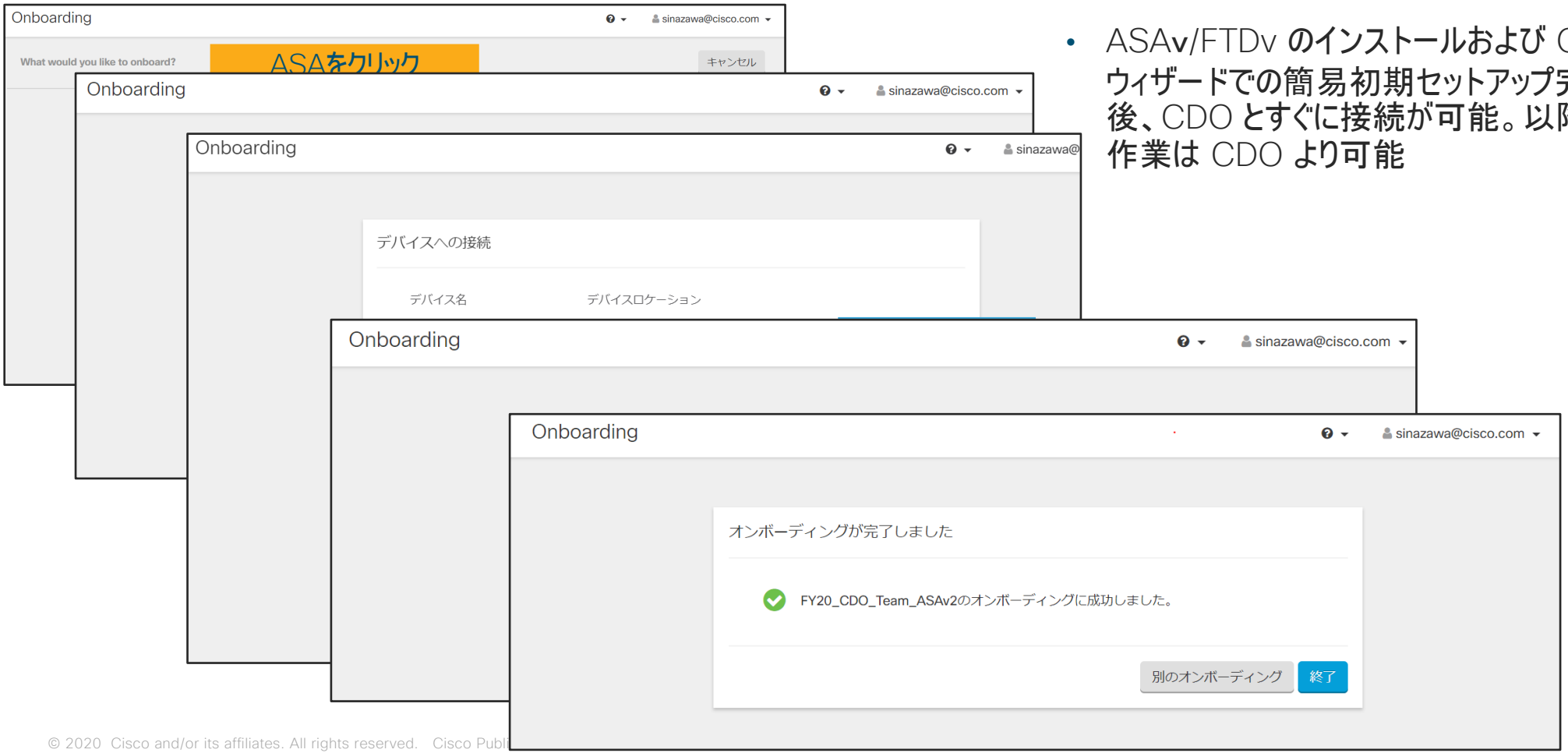


# CDO ユースケース: ASA から FTD へのマイグレーション



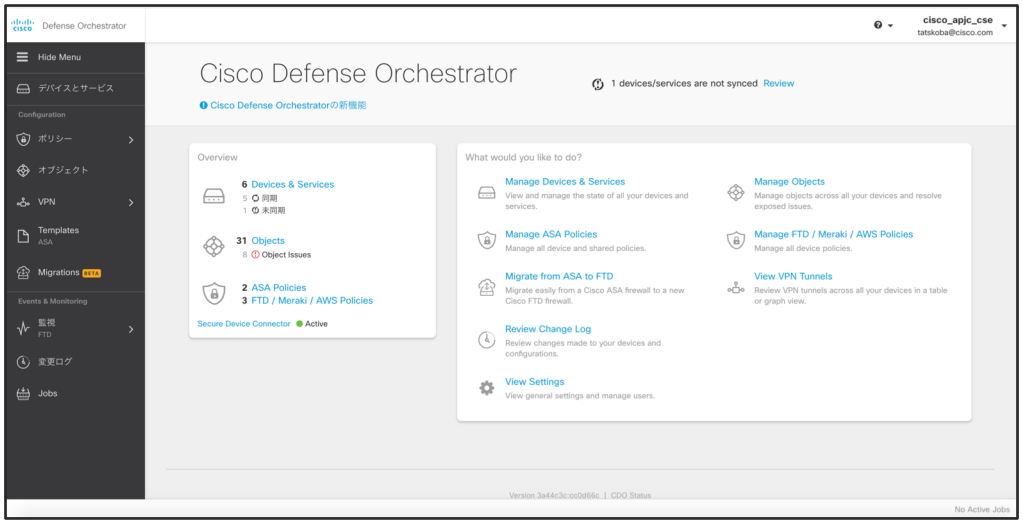

In Beta

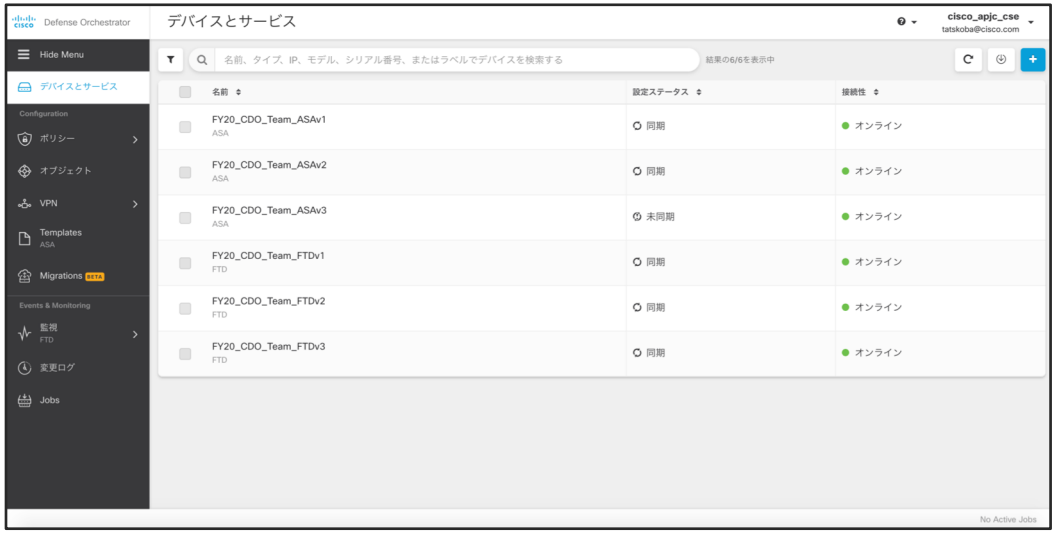
# CDO でのデバイス登録

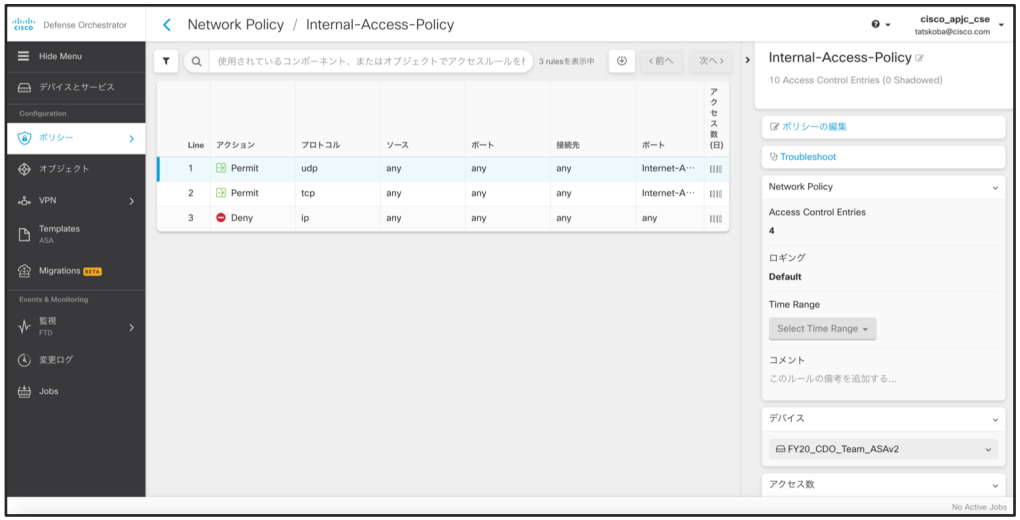


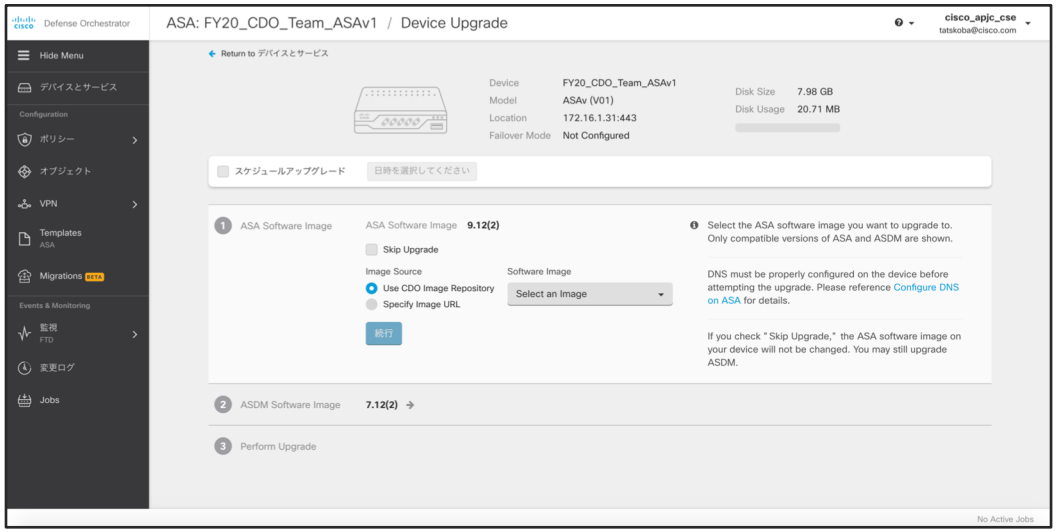

- ASAv/FTDv のインストールおよび CLI ウィザードでの簡易初期セットアップ完了後、CDO とすぐに接続が可能。以降の作業は CDO より可能

# CDO サンプル画面


Defense Orchestrator
cisco_apjc_cse
tatskoba@cisco.com
Hide Menu
デバイスとサービス
Configuration
ポリシー
オブジェクト
VPN
Templates
ASA
Migrations BETA
Events & Monitoring
監視
FTD
変更ログ
Jobs
Cisco Defense Orchestrator
1 devices/services are not synced Review
Cisco Defense Orchestratorの新機能
Overview
6 Devices & Services
5 同期
1 未同期
31 Objects
8 Object Issues
2 ASA Policies
3 FTD / Meraki / AWS Policies
Secure Device Connector Active
What would you like to do?
Manage Devices & Services
View and manage the state of all your devices and services.
Manage Objects
Manage objects across all your devices and resolve exposed issues.
Manage ASA Policies
Manage all device and shared policies.
Manage FTD / Meraki / AWS Policies
Manage all device policies.
Migrate from ASA to FTD
Migrate easily from a Cisco ASA firewall to a new Cisco FTD firewall.
View VPN Tunnels
Review VPN tunnels across all your devices in a table or graph view.
Review Change Log
Review changes made to your devices and configurations.
View Settings
View general settings and manage users.
No Active Jobs


Defense Orchestrator
デバイスとサービス
cisco_apjc_cse
tatskoba@cisco.com
Hide Menu
デバイスとサービス
Configuration
ポリシー
オブジェクト
VPN
Templates
ASA
Migrations BETA
Events & Monitoring
監視
FTD
変更ログ
Jobs
名前、タイプ、IP、モデル、シリアル番号、またはラベルでデバイスを検索する
結果の6/6を表示中
名前
設定ステータス
接続性
FY20_CDO_Team_ASAv1
ASA
同期
オンライン
FY20_CDO_Team_ASAv2
ASA
同期
オンライン
FY20_CDO_Team_ASAv3
ASA
未同期
オンライン
FY20_CDO_Team_FTDv1
FTD
同期
オンライン
FY20_CDO_Team_FTDv2
FTD
同期
オンライン
FY20_CDO_Team_FTDv3
FTD
同期
オンライン
No Active Jobs


Defense Orchestrator
Network Policy / Internal-Access-Policy
cisco_apjc_cse
tatskoba@cisco.com
Hide Menu
デバイスとサービス
Configuration
ポリシー
オブジェクト
VPN
Templates
ASA
Migrations BETA
Events & Monitoring
監視
FTD
変更ログ
Jobs
使用されているコンポーネント、またはオブジェクトでアクセスルールを!
3 rulesを表示中
前へ
次へ
Line
アクション
プロトコル
ソース
ポート
接続先
ポート
アクセス数(日)
1 Permit udp any any any Internet-A…
2 Permit tcp any any any Internet-A…
3 Deny ip any any any any
Internet-Access-Policy
10 Access Control Entries (0 Shadowed)
ポリシーの編集
Troubleshoot
Network Policy
Access Control Entries
4
ロギング
Default
Time Range
Select Time Range
コメント
このルールの備考を追加する…
デバイス
FY20_CDO_Team_ASAv2
アクセス数
No Active Jobs


Defense Orchestrator
ASA: FY20_CDO_Team_ASAv1 / Device Upgrade
cisco_apjc_cse
tatskoba@cisco.com
Hide Menu
デバイスとサービス
Configuration
ポリシー
オブジェクト
VPN
Templates
ASA
Migrations BETA
Events & Monitoring
監視
FTD
変更ログ
Jobs
Return to デバイスとサービス
Device FY20_CDO_Team_ASAv1
Model ASAv (V01)
Location 172.16.1.31:443
Failover Mode Not Configured
Disk Size 7.98 GB
Disk Usage 20.71 MB
スケジュールアップグレード
日時を選択してください
1 ASA Software Image
ASA Software Image 9.12(2)
Skip Upgrade
Image Source
Use CDO Image Repository
Specify Image URL
Software Image
Select an Image
続行
Select the ASA software image you want to upgrade to. Only compatible versions of ASA and ASDM are shown.
DNS must be properly configured on the device before attempting the upgrade. Please reference Configure DNS on ASA for details.
If you check " Skip Upgrade," the ASA software image on your device will not be changed. You may still upgrade ASDM.
2 ASDM Software Image 7.12(2)
3 Perform Upgrade
No Active Jobs

# CDO 注意事項

- 管理デバイスのアドレスがプライベートな場合、オンプレミスに SDC のインストール (仮想インフラに簡単に導入可) が必須
- Proxy を介した SDC 接続不可
- Japan TAC 対応はまだ準備中
- FTD 管理について、FDM とほぼ同等機能であり、FMC の機能が必要な場合には FMC との併用が必要 (例: 自動チューニング、インパクト解析等)
- ASA 管理について、ASDM ほどの機能は無い

# CDO オーダリングガイド

- Cloud のサービスとして販売
- 管理する製品のライセンス SKU 購入
- ASA プラットホームも Firepower プラットホームも、動作させるアプリケーション (ASA or FTD) に違いなくオーダー
- 例

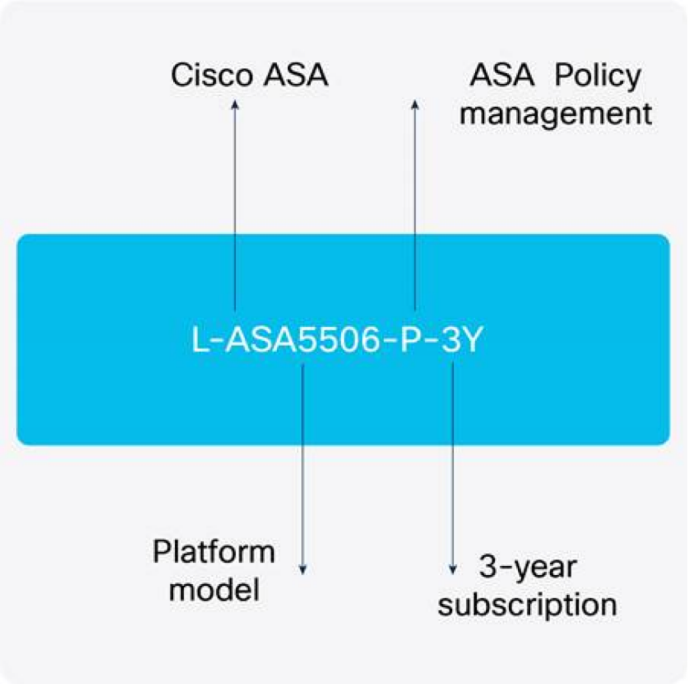



**Table 1. Cisco Defense Orchestrator base licenses**

| Part number | Description |
|---|---|
| L-FPR1010-P= | Cisco Defense Orchestrator for FPR1010 running ASA or FTD Image |
| L-FPR1120-P= | Cisco Defense Orchestrator for FPR1120 running ASA or FTD Image |
| L-FPR1140-P= | Cisco Defense Orchestrator for FPR1140 running ASA or FTD Image |

**Table 2. Cisco Defense Orchestrator 1-year subscription**

| Part number | Description |
|---|---|
| L-FPR1010-P-1Y | Cisco Defense Orchestrator for FPR1010 running ASA or FTD Image |
| L-FPR1120-P-1Y | Cisco Defense Orchestrator for FPR1120 running ASA or FTD Image |
| L-FPR1140-P-1Y | Cisco Defense Orchestrator for FPR1140 running ASA or FTD Image |

CDO オーダリングガイド
https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/guide-c07-736923.html

# Demo

# まとめ

- 複雑なセキュリティ管理の問題に対し、クラウド利用で解決するには Cisco Defense Orchestrator (CDO) を利用する
- CDO は、複数のシスコの Firewall を、シンプルに効率よく効果的に管理することが可能
- CDO は、シスコが提供するクラウドサービスであり、オンプレミスに管理製品を置く必要が無い。もしくは小さな VM 1つを置くだけで良い。

# 参考資料

- CDO への cisco.comでのショートカット (無料トライアルへのリンク有り)

  http://cisco.com/go/cdo

- CDO 技術ドキュメント

  https://docs.defenseorchestrator.com/

- パートナー向け技術資料

  https://www.cisco.com/c/m/ja_jp/partners/documents.html

- シスコサポートコミュニティ セキュリティ

  https://community.cisco.com/t5/-/ct-p/5041-security


CISCO