



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%

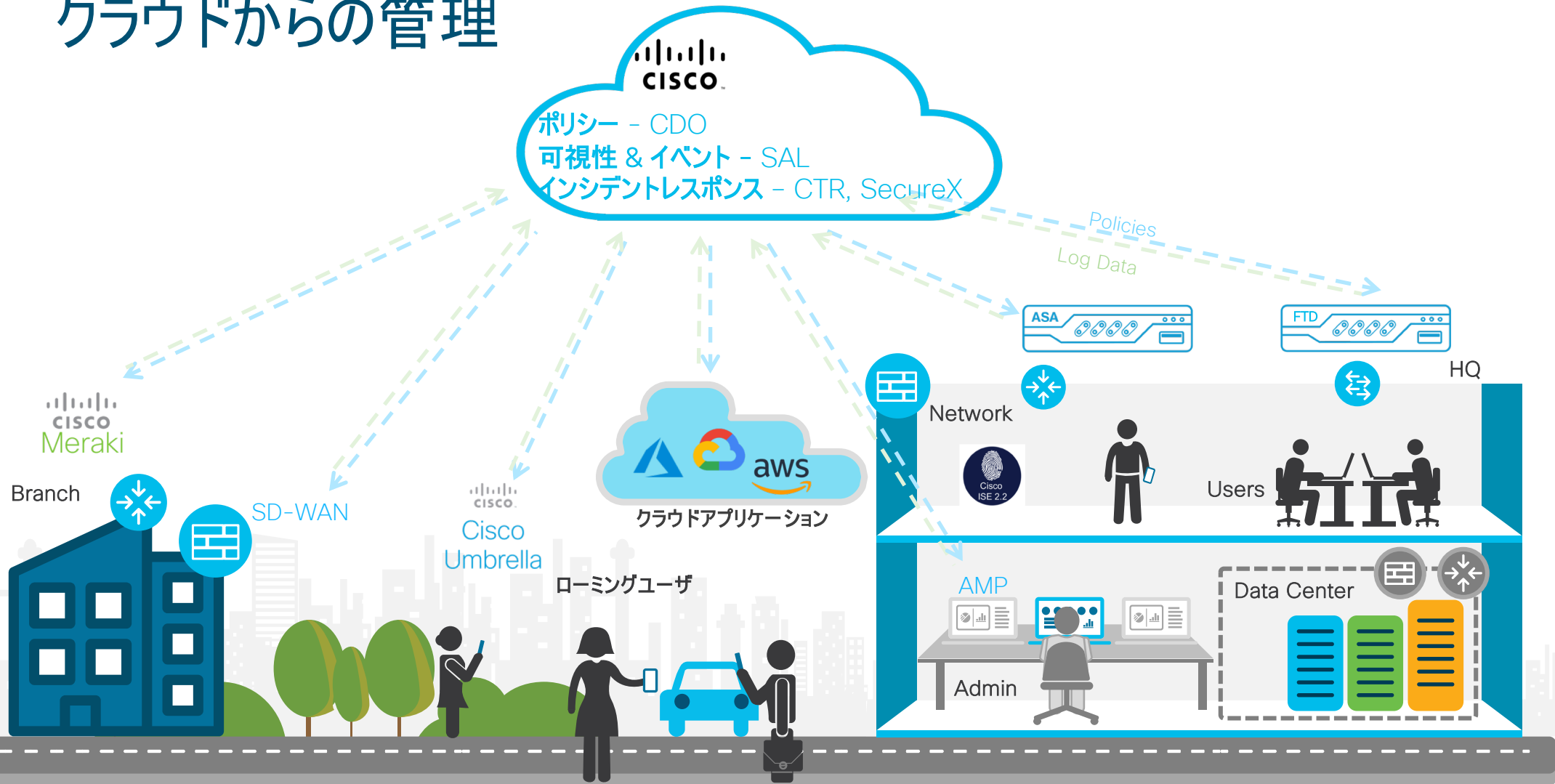
ここ12ヶ月の間に複雑さが増したことにより発生したセキュリティインシデントを経験している管理者の割合

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

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 Defense Orchestrator (CDO) の特長



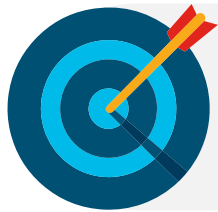
シンプル

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

簡単なファイアウォールソフトウェアアップグレード

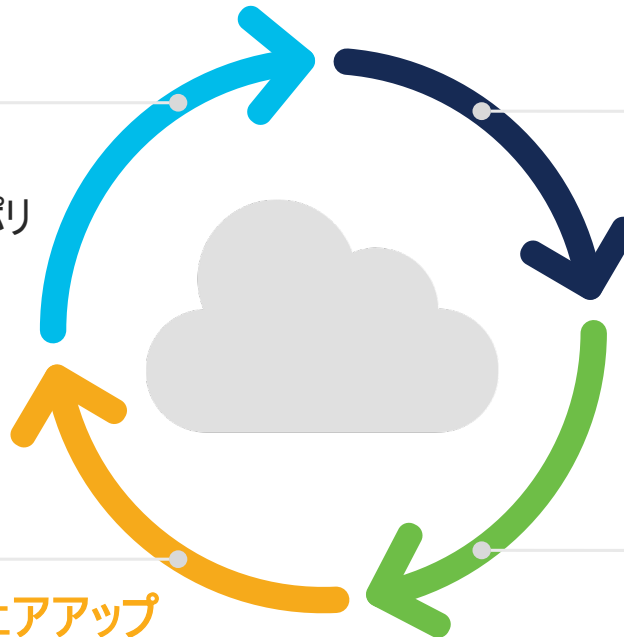
ソフトウェアのアップグレードは少ないクリックで完了可能なため、新機能やパッチの適用はより迅速に対応

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

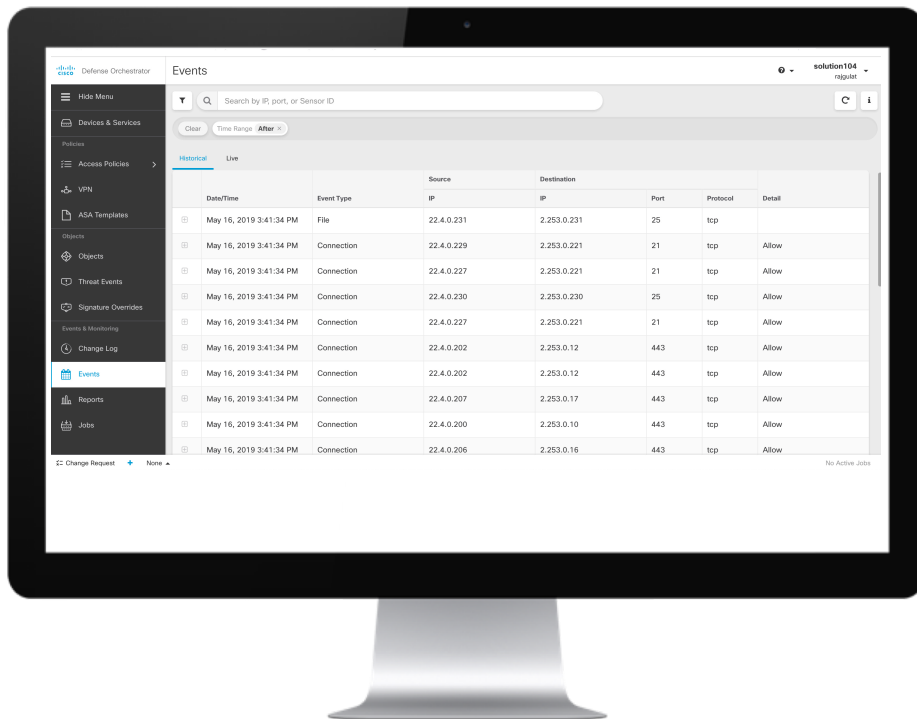
よりスマートな構成管理

全ての変更履歴をログに残せる
いつでもコンフィギュ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+)
ASA 5500-X (ASA 8.4+, FTD 6.4+)
Firepower 2100 (ASA 9.8+, FTD 6.4+)
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>

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

- 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

02 メンテナンス不要

03 新機能の早期利用

1日以内での
プロビジョニング



04 コスト削減

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



99.99999%

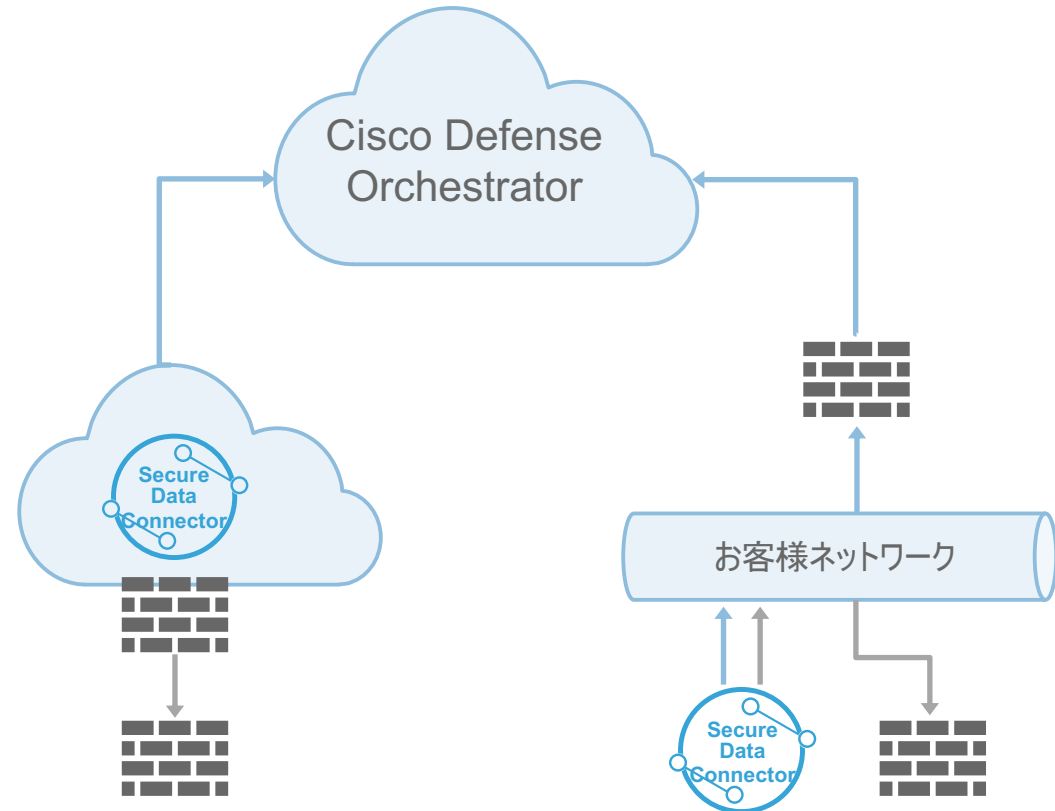
Uptime

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

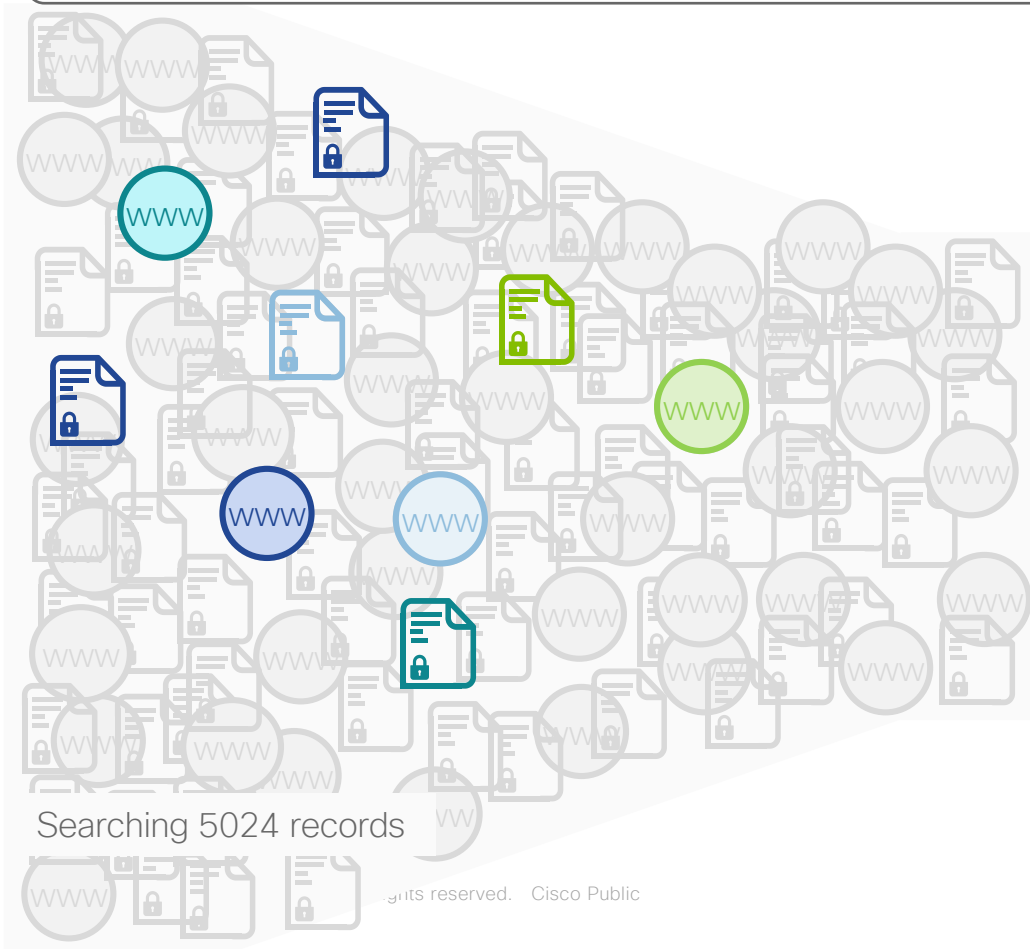
コネクタをクラウドに設置

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 13 Allow
Facebook Chat	Application	FTD	15 Block 13 Allow
Facebook Games	Application	FTD	20 Block 15 Allow
Social Networking	URL Category	FTD	10 Block 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

重複を検知し修正してファイアウォールを最適化



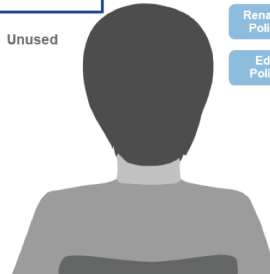
Policies Quickly see Duplicate Objects

Duplicate	Object 1
Inconsistent	Object 1
Unused	

Rename Policy
Edit Policy



不整合の修正



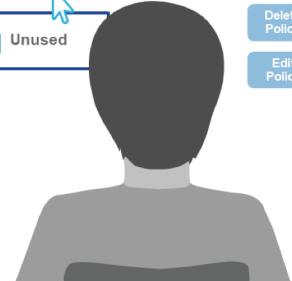
Policies Quickly see Inconsistent Policies

Duplicate	Policy 1 Objects	Policy 2 Objects
Inconsistent	• 1	• 1
	• 2	• 2
	• 3	• 3b
Unused		

Rename Policy
Edit Policy



未使用のポリシーを自動検出、削除



Policies Quickly see Unused Policies

Duplicate	Policy 5
Inconsistent	Policy 6
Unused	Policy 7

Delete Policy
Edit Policy



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



Security Policy



CDO ユースケース: ASA から FTD へのマイグレーション

The screenshot shows the Cisco CDO 'Devices & Services' interface. At the top, there is a search bar and a status indicator 'Displaying 5 of 5 devices'. Below this is a table with columns for Name, Configuration Status, and Connectivity. The table lists five branches: Boston Branch (ASA), Chicago Branch (ASA), Dallas Branch (ASA), San Jose Branch (ASA), and Vancouver Branch (ASA). The San Jose Branch is selected, and its configuration status is 'Synced' and connectivity is 'Online'. To the right of the table, there is a 'San Jose Branch' details panel showing the IP address 'ASA 10.82.109.176' and a 'Synced' status with the message 'Your device's configuration is up-to-date.'.

In Beta

The screenshot shows the 'FTD Migration > San Jose Branch' configuration page in Cisco CDO. The page has a breadcrumb trail 'FTD Migration > San Jose Branch' and 'Cancel' and 'Save' buttons at the top right. The main content area is divided into steps:

- 1 Name:** San Jose Branch - (Edit)
- 2 Migration:** Successfully migrated the ASA model (Edit)
- 3 Apply:** This step is active. It has two radio buttons: 'Apply Migration Now' (selected) and 'Apply Migration Later'. Below 'Apply Migration Now' is a 'Device' label and a 'Select FTD Device' dropdown menu. A 'Next' button is at the bottom. A help icon and text state: 'You can apply the migration configuration either immediately or later. To apply immediately, select a device.'
- 4 Map Interfaces:**
- 5 Fill Parameters:**
- 6 Review:** (Edit)
- 7 Done:** (Edit)

CDO でのデバイス登録

The image displays four overlapping screenshots of the Cisco Onboarding web interface, illustrating the device registration process:

- Top Screenshot:** Shows the initial selection screen with the question "What would you like to onboard?". A prominent orange button labeled "ASAをクリック" (Click ASA) is highlighted.
- Second Screenshot:** Shows the "デバイスへの接続" (Connect to device) screen, which includes input fields for "デバイス名" (Device name) and "デバイスロケーション" (Device location).
- Third Screenshot:** Shows the progress of the onboarding process, with a large green checkmark indicating success.
- Bottom Screenshot:** Shows the final completion screen with the message "オンボーディングが完了しました" (Onboarding is complete) and a confirmation message: "FY20_CDO_Team_ASAv2のオンボーディングに成功しました。" (Onboarding for FY20_CDO_Team_ASAv2 was successful). Buttons for "別のオンボーディング" (Other onboarding) and "終了" (End) are visible.

- 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

The dashboard shows the overall status of the Cisco Defense Orchestrator. It includes a sidebar with navigation options like 'Hide Menu', 'デバイスとサービス', 'Configuration', 'ポリシー', 'オブジェクト', 'VPN', 'Templates', 'Migrations', 'Events & Monitoring', '監視', '変更ログ', and 'Jobs'. The main content area displays 'Cisco Defense Orchestrator' with a notification '1 devices/services are not synced'. Below this, there are several cards for 'Overview' and 'What would you like to do?'. The Overview card shows 6 Devices & Services (5 Online, 1 Offline), 31 Objects (8 Object Issues), and 2 ASA Policies (3 FTD / Meraki / AWS Policies). The 'What would you like to do?' section offers actions like 'Manage Devices & Services', 'Manage Objects', 'Manage ASA Policies', 'Migrate from ASA to FTD', 'Review Change Log', and 'View Settings'.

This screen displays a list of devices and services. The title is 'デバイスとサービス'. A search bar at the top allows filtering by name, type, IP, model, or serial number. The table below lists several devices:

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

This screen shows the configuration for an 'Internal-Access-Policy'. The left sidebar is expanded to 'ポリシー'. The main area displays a table of 'Access Control Entries' (ACEs) for the policy:

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	

Below the table, there are sections for 'ポリシーの編集', 'Troubleshoot', 'Network Policy', 'Access Control Entries', 'ロギング', 'Time Range', 'コメント', 'デバイス', and 'アクセス数'.

This screen shows the configuration for upgrading the software on the device 'FY20_CDO_Team_ASAv1'. The left sidebar is expanded to 'デバイスとサービス'. The main area displays the device details and the upgrade process:

Device: FY20_CDO_Team_ASAv1
Model: ASAv (V01)
Location: 172.16.1.31:443
Fallover Mode: Not Configured

Disk Size: 7.98 GB
Disk Usage: 20.71 MB

The upgrade process is shown in a step-by-step format:

- ASA Software Image: 9.12(2)
 - Skip Upgrade
 - Use CDO Image Repository
 - Specify Image URL
- ASDM Software Image: 7.12(2)
- Perform Upgrade

Additional instructions include: 'Select the ASA software image you want to upgrade to. Only compatible versions of ASA and ASDM are shown.' and 'DNS must be properly configured on the device before attempting the upgrade. Please reference Configure DNS on ASA for details.'

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

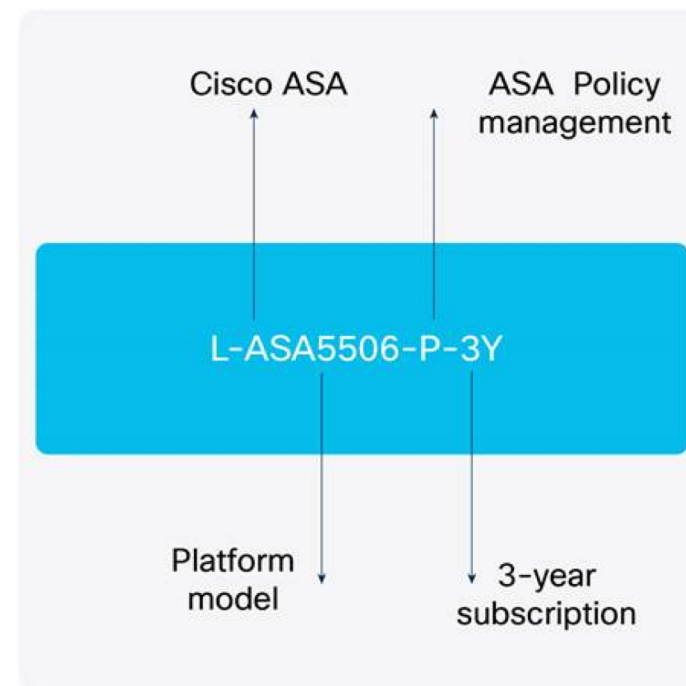


Table 1. Cisco Defense Orchestrator base licenses

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>

