Cisco
Customer Experience

# Ask the Experts

アップグレード計画とベストプラクティス：
ISE のアップグレード
（Upgrade Planning and Best Practices: Upgrading ISE）

# Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

# 免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

# 本日のトピック

01 | アップグレードする理由

02 | 計画と準備

03 | アップグレードの実行

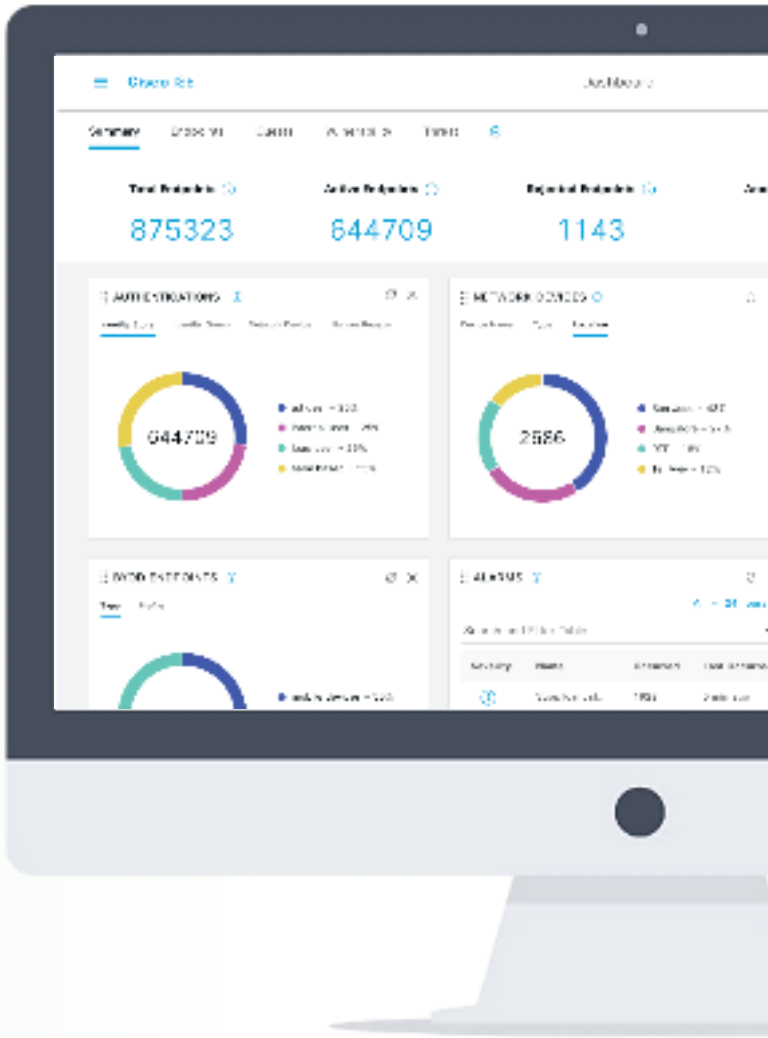
04 | アップグレード後の作業

# アップグレードする理由

# ISE 3.1 リリースのハイライト

## シスコが推奨する（ゴールドスター）リリース

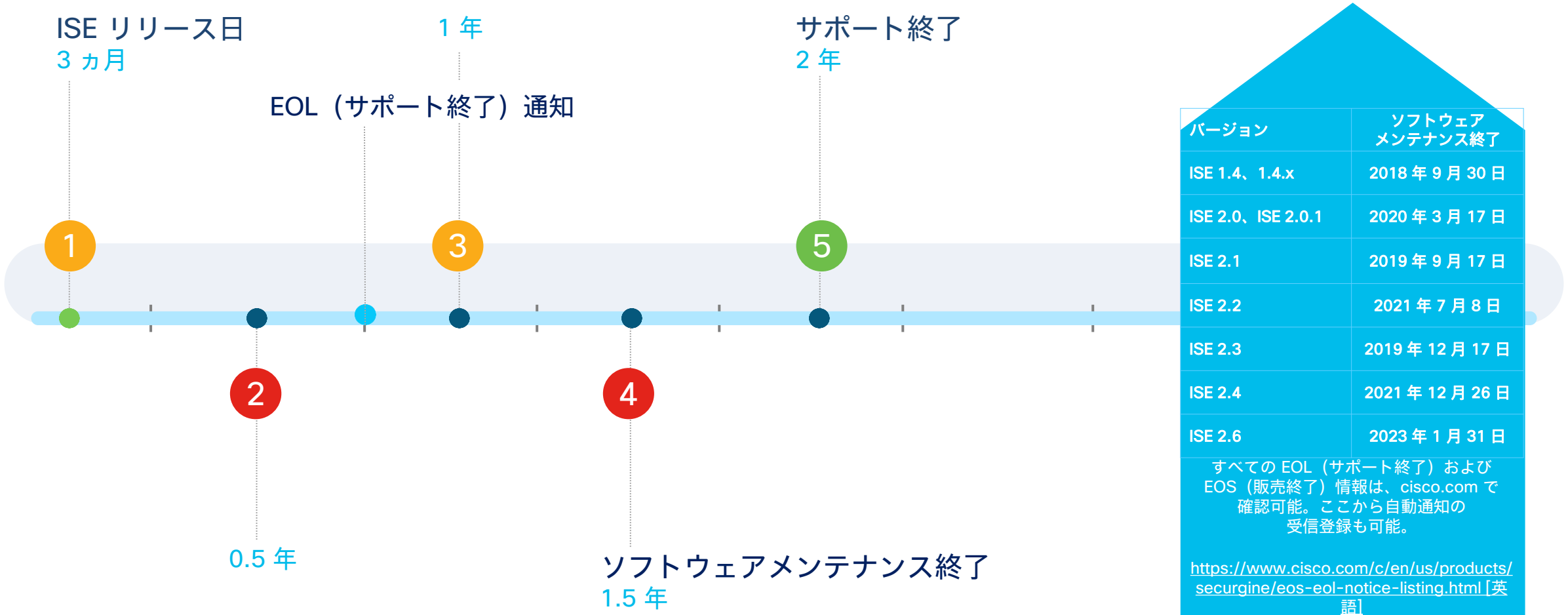
- 管理者ログイン用の SAML SSO
- AWS での ISE の導入
- システム管理とポリシー管理のための API
- MACアドレスランダム化対応
- ゼロタッチプロビジョニング
- アップグレードエクスペリエンスの効率化
- 強化された監査ログ
- エンドポイント修復スクリプト
- Linux ポスチャ
- ポスチャの双方向トリガー
- 拡張されたポスチャディスカバリ
- 認証ダッシュボードアラーム
- Active Directory DC フェールオーバー強化
- Context visibility のインポート/エクスポート
- AD アカウントのロックアウト防止
- RADIUS CoA プロキシ
- シームレスな EA 統合
- Logical profile ダッシュレット






cs.co/ise-videos

# ISE リリースサイクル（ISE 2.7 より前）
## ショートタームリリース（2 年、奇数バージョン）

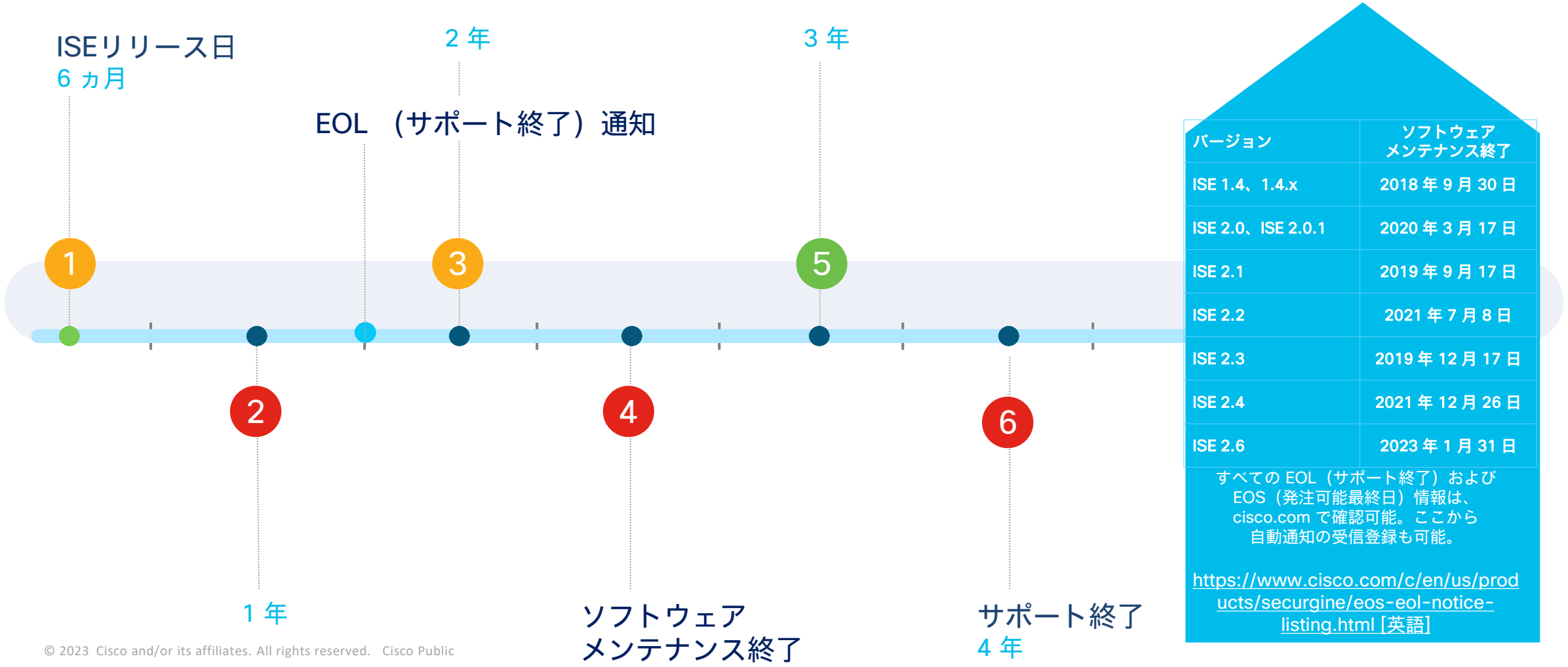



| バージョン | ソフトウェア メンテナンス終了 |
|---|---|
| ISE 1.4、1.4.x | 2018 年 9 月 30 日 |
| ISE 2.0、ISE 2.0.1 | 2020 年 3 月 17 日 |
| ISE 2.1 | 2019 年 9 月 17 日 |
| ISE 2.2 | 2021 年 7 月 8 日 |
| ISE 2.3 | 2019 年 12 月 17 日 |
| ISE 2.4 | 2021 年 12 月 26 日 |
| ISE 2.6 | 2023 年 1 月 31 日 |

すべての EOL（サポート終了）および EOS（販売終了）情報は、cisco.com で確認可能。ここから自動通知の受信登録も可能。

https://www.cisco.com/c/en/us/products/securgine/eos-eol-notice-listing.html [英語]

# ISE リリースサイクル（ISE 2.7 以前）
## ロングタームリリース（4 年、偶数バージョン）




| バージョン | ソフトウェア メンテナンス終了 |
|---|---|
| ISE 1.4、1.4.x | 2018 年 9 月 30 日 |
| ISE 2.0、ISE 2.0.1 | 2020 年 3 月 17 日 |
| ISE 2.1 | 2019 年 9 月 17 日 |
| ISE 2.2 | 2021 年 7 月 8 日 |
| ISE 2.3 | 2019 年 12 月 17 日 |
| ISE 2.4 | 2021 年 12 月 26 日 |
| ISE 2.6 | 2023 年 1 月 31 日 |

すべての EOL（サポート終了）および EOS（発注可能最終日）情報は、cisco.com で確認可能。ここから自動通知の受信登録も可能。

https://www.cisco.com/c/en/us/products/securgine/eos-eol-notice-listing.html [英語]

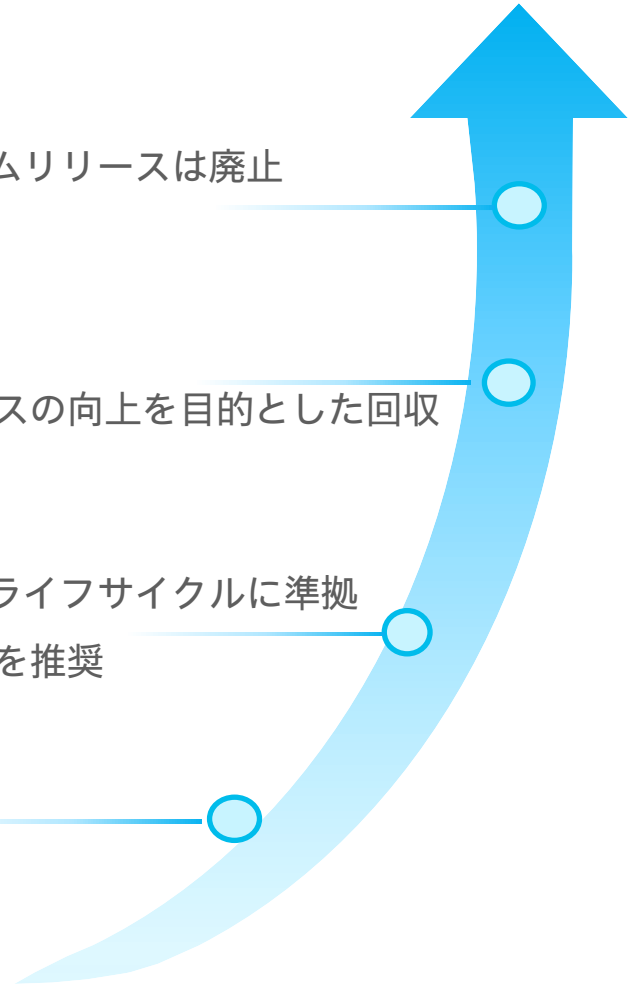
# ISE リリースサイクル ー 新しいモデル

2.7 以降、ショートタームリリースとロングタームリリースは廃止
新しいリリースサイクルを適用

ISE 2.7 はさらに 6 ヵ月間の改修を実施
お客様の導入実例に基づき安定性とパフォーマンスの向上を目的とした回収
2.7 以降のすべてのバージョンに適用

2.7 以降のすべてのバージョンは、標準化されたライフサイクルに準拠
推奨ソフトウェアバージョンを常時確認することを推奨

ISE ライフサイクルの詳細については
このリンク [英語] をクリック



# アップグレードの準備

# 計画と準備

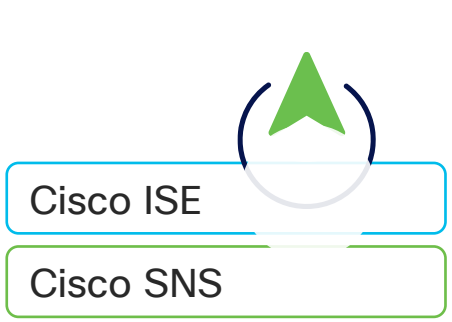
01 | 互換性チェックとアップグレードパス

02 | アップグレード前のアクティビティ

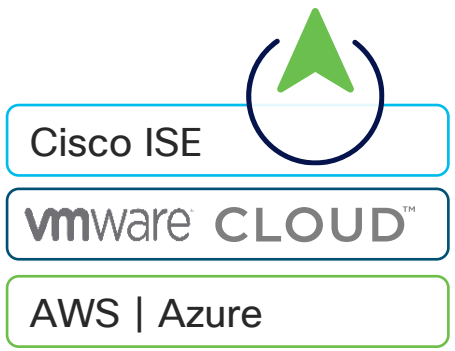
03 | アップグレード準備ツール

04 | メンテナンス ウィンドウ

# ISE をサポートしているプラットフォーム









| アプライアンス | スタンドアロン セッション数 | PSN セッション数 | プロセッサ | コア | メモリ | ディスク | RAID | ネットワーク インターフェイス |
|---|---|---|---|---|---|---|---|---|
| SNS-3615 | 10,000 | 10,000 | Intel Xeon 2.10 GHz 4110 X 1 | 8 | 32 GB （16 GB X 2） | 1（600GB） | なし | 10Gbase-T X 2<br>1GBase-T X 4 |
| SNS-3655 | 25,000 | 50,000 | Intel Xeon 2.10 GHz 4116 X 1 | 12 | 96 GB （16 GB X 6） | 4（600GB） | 10 | 10Gbase-T X 2<br>1GBase-T X 4 |
| SNS-3695 | 50,000 | 100,000 | Intel Xeon 2.10 GHz 4116 X 1 | 12 | 256 GB （32 GB X 8） | 8（600GB） | 10 | 10Gbase-T X 2<br>1GBase-T X 4 |
| ~~SNS-3515~~ | ~~7500~~ | ~~7500~~ | ~~Intel Xeon 2.40GHz E5-2620 X 1~~ | ~~6~~ | ~~16 GB （8 GB X 2）~~ | ~~1（600GB）~~ | ~~なし~~ | ~~1GBase-T X 6~~ |
| SNS-3595 | 20,000 | 40,000 | Intel Xeon 2.60 GHz E5-2640 X 1 | 8 | 64 GB （16 GB X 4） | 4（600GB） | 10 | 1GBase-T X 6 |

EOL



* SNS-3515 は ISE 3.1 のサポート対象外になる
* VMware バージョン 6.5 以降が必要

# 互換性チェック

## サポート対象のハードウェア

Cisco SNS-3595-K9（大規模）
EOL
Cisco SNS-3615-K9（小規模）
Cisco SNS-3655-K9（中規模）
Cisco SNS-3695-K9（大規模）
Cisco ISE-VM-K9**

## サポート対象の仮想環境

- VMware Cloud または AWS Marketplace Web サービスおよび Azure VMware における ISE
- ESXi 6.5+ (RHEL 8.2 における KVM)
- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V

## Microsoft Active Directory のサポート

Microsoft Active Directory Server:

- 2012、2012 R2
- 2016
- 2019

## Cisco DNA との互換性

Cisco DNA Center：

- Cisco DNA Center 2.1.1.0 から ISE 3.0 + を対応
- Cisco DNA Center 2.2.2.6 から ISE 3.1 + を対応

**仮想マシンが ISE のインストール要件を満たしていることを確認する

cisco.com の ISE リリースノートで
最新の互換性ガイダンスを定期的に確認

# ISE ライセンスモデル

## 2.x モデル

**Plus**

コンテキスト

**Apex**

コンプライアンス

**Base**

ユーザーの可視性と適用

- ハイブリッド：PAK またはスマートライセンスのいずれかをサポート
- 階層モデル：ライセンスが重複しない
- Base は 常時、Plus と Apex は 期間ベース
- デバイスアドミンには Baseライセンスが 100 必要

## 3.x モデル

**Premier**

コンプライアンスとクラウド ー フルスタック

**Advantage**

コンテキスト

**Essentials**

ユーザーの可視性と適用

- スマートライセンスのみをサポート
- ネステッドモデル：上位階層ライセンスは　下位階層ライセンスをカバー
- エンドポイント ライセンスはすべて期間ベース
- デバイスアドミンに階層ライセンスは不要

# アップグレードパス

## 直接アップグレード

次の ISE バージョンを使用している場合は、3.1 への直接アップグレードが可能

- Cisco ISE リリース 2.6
- Cisco ISE リリース 2.7
- Cisco ISE リリース 3.0

## 2 段階のアップグレード

Cisco ISE リリース 2.6 より前のバージョンを使用している場合は、
まず上記のいずれかのリリースにアップグレードしてから、
リリース 3.1 へのアップグレードが必要

# アップグレード

## アップグレード前の確認（to-do リスト）

このリストの前に、ネットワークデバイスのソフトウェア互換性チェックを ISE 互換性マトリックスを使用してすべて実行する。

### ベストプラクティス

#### バックアップ

- Configuration、Operational、Endpoints.csv
- ロード バランサ
- 証明書および秘密キーのエクスポート
- CLI から内部 CA 証明書をエクスポート

#### メモを取る

- AD クレデンシャル：トークンクレデンシャル（RSA）
- MDM クレデンシャル
- 各 PSN のプロファイラ設定

#### クリーン

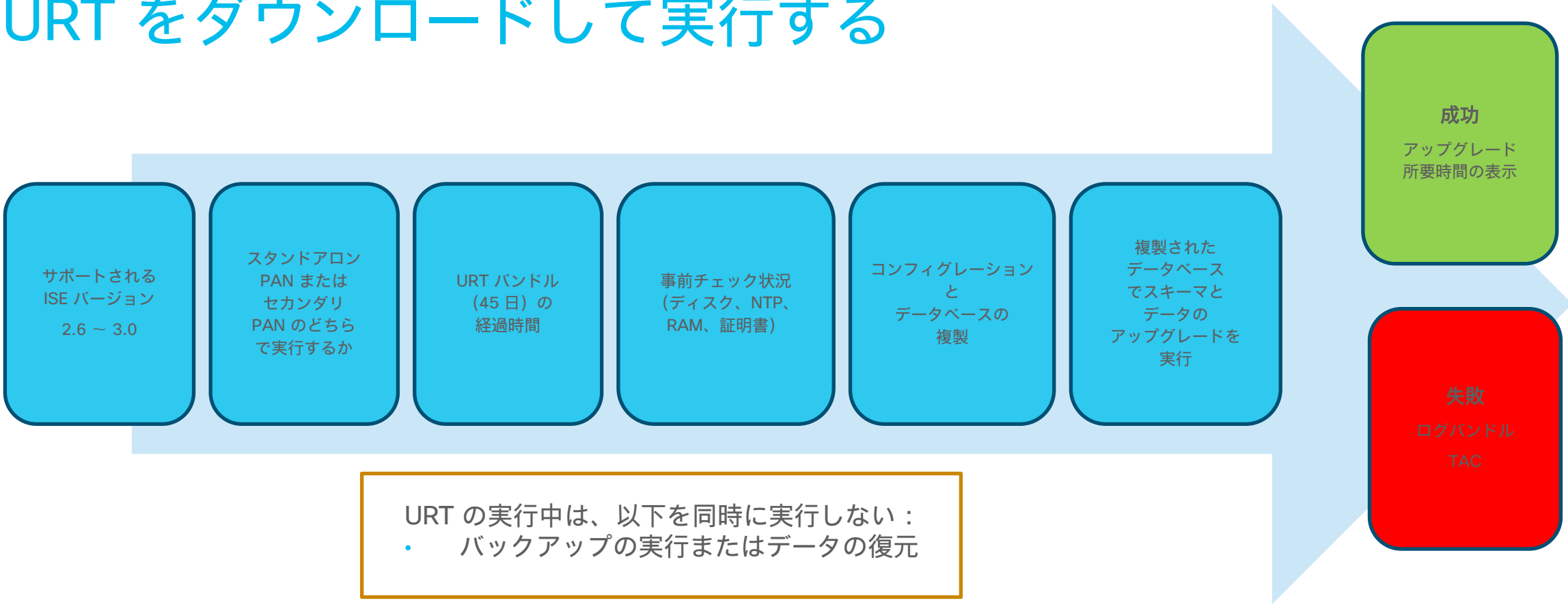
- 期限切れ証明書の削除
- 過剰な運用データ、非アクティブなエンドポイント、ゲストアカウントを消去

### 重要なポイント

- 自動 PAN フェールオーバーを無効にする
- スケジュールされているバックアップを無効にする
- リポジトリを設定し、最新の URT とアップグレードバンドルをダウンロードする

# アップグレードレディネスツール（Upgrade Readiness Tool（URT））

## URT をダウンロードして実行する




URT の実行中は、以下を同時に実行しない：

- バックアップの実行またはデータの復元

# デモアップグレードにおける URT の推定所要時間

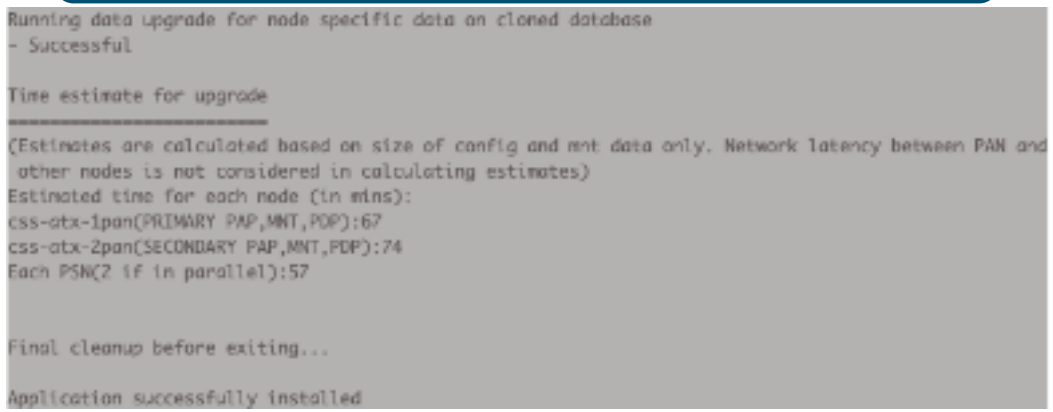
セカンダリ PAN、1 MNT、PSN – 74 分

PSN（個々またはタンデム）— 57 分

プライマリ PAN、2 MNT、PSN — 67 分

URT 推定所要時間：198 分

GUI 推定所要時間：660 分



# オンデマンドの ISE ヘルスチェック*

## 重大なエラーに対して展開を検証

検証対象：

- プラットフォームのサポート（Platform support）
- 展開の検証（Deployment validation）
- DNS の名前解決が可能か（DNS resolvability）
- 信頼ストア証明書の検証（Trust store cert validation）
- システム証明書の検証（System cert validation）
- ディスク容量（Disk space）
- NTP の到達可能性（NTP reachability）
- システム負荷の平均値（Load average）
- MDM の検証（MDM validation）
- ライセンスの検証（License validation）

アップグレードの前に検証結果をダウンロードし、重大なエラーがある場合は、修正が可能。
これは任意の手順であり、URT の代替ではない。むしろ追加のチェックとしての機能を持つ。



* 2.x バージョンでは 2.6 および 2.7 の最新パッチでのみ利用可能

# メンテナンスウィンドウのスケジュール

## メンテナンスウィンドウの採用
アップデートとアップグレード用

## 通知
予定されるダウンタイムの共有

## ダウンタイムの最小化
すべての PSN を一度にアップグレードしない

## 万が一のために予備の時間をスケジュール

### アップグレードにかかる時間に影響する要因

エンドポイントの数
ユーザー数とゲストユーザー数
モニターリングノードまたはスタンドアロンノードのログ量
プロファイリングサービス（イネーブルの場合）

### 推定方法

| 展開のタイプ | ノードペルソナ | 推定所要時間 |
|---|---|---|
| スタンドアロン | 管理、ポリシーサービス、モニタリング | 15 GB のデータごとに 240 分 + 60 分 |
| 分散型 | セカンダリ管理ノード | 240 分 |
| | ポリシーサービスノード | 180 分 |
| | モニタリング | 15 GB のデータごとに 240 分 + 60 分 |

# アップグレードの実行

# ISE のアップグレード

01 | 展開タイプ

02 | アップグレードの種類とプロセス

03 | アップグレードオプション

# ISE の展開タイプ

ポリシー管理ノード（PAN）

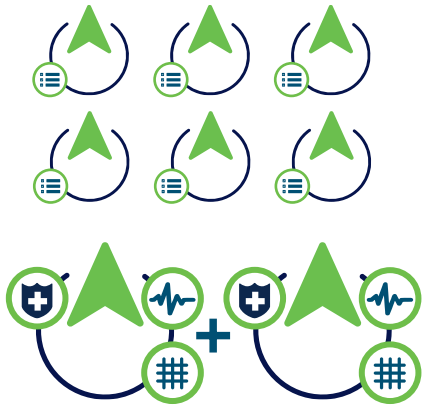
モニターリングおよびトラブルシューティング ノード（MnT）

ポリシー サービス ノード（PSN）

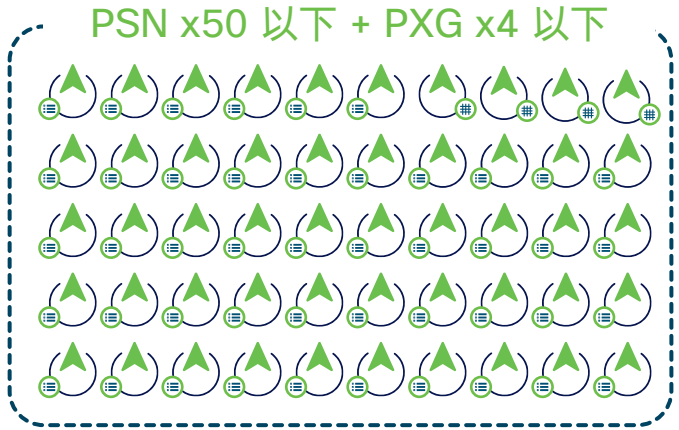
pxGrid コントローラ

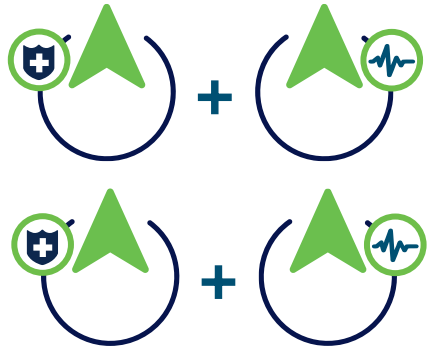
ラボと評価

小規模 HA 展開
（PAN + MNT + PSN）x2



中規模分散展開
（PAN + MNT + PSN）x2、PSN x6 以下

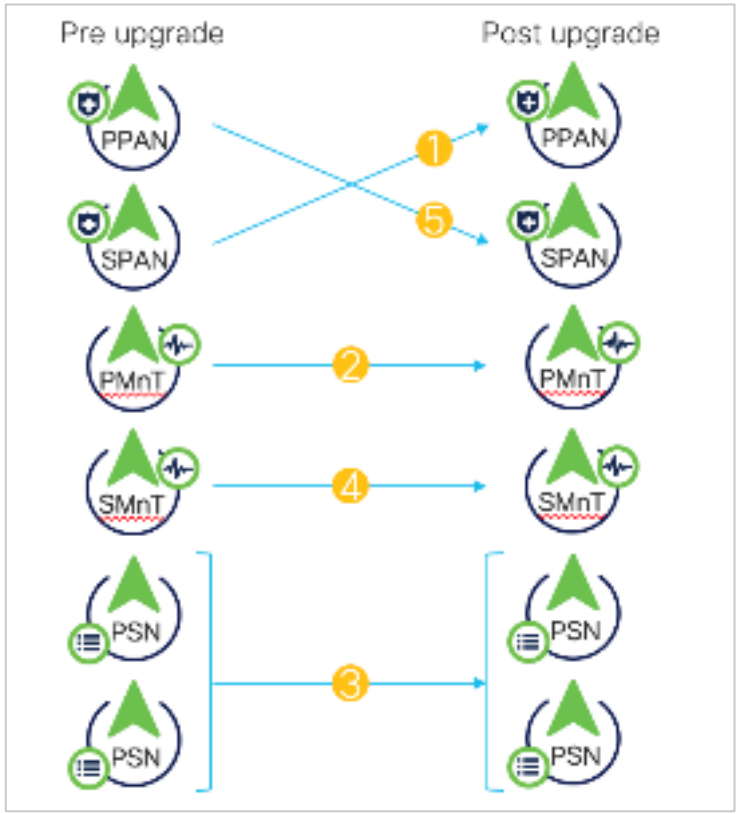


大規模分散展開
PAN x2、MNT x2、PSN x50 以下、PXG x4 以下

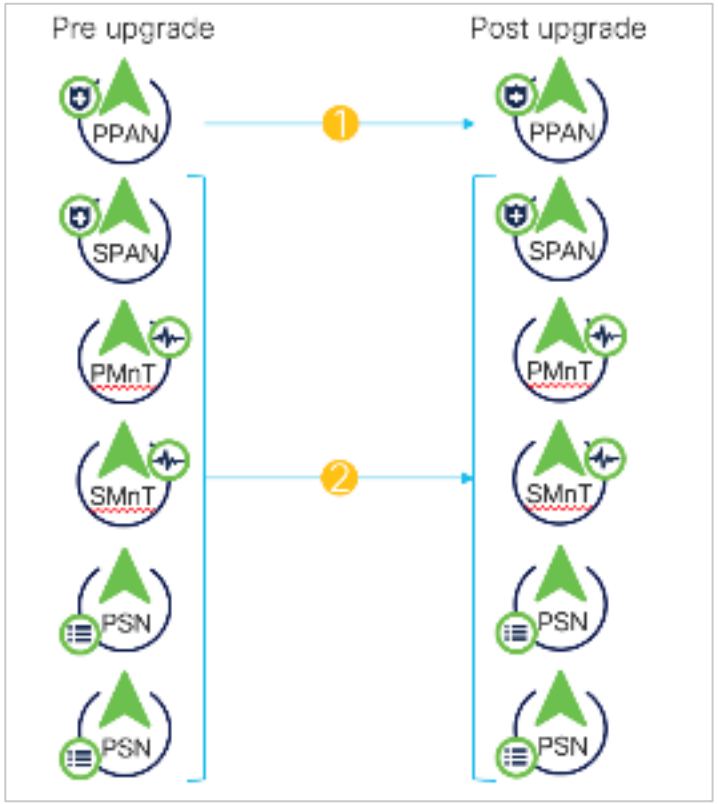
# アップグレードの種類

## スプリットアップグレードとフルアップグレード




スプリット

- サービスが利用可能な間に展開をアップグレードする、複数ステップのシーケンシャルプロセス
- フルアップグレードよりも時間がかかる




フル

- サービスの停止と並行して、すべてのノードをアップグレードする、2 ステッププロセス
- スプリットアップグレードよりも時間がかからない

# アップグレードオプション - スプリットアップグレード

## CLI、GUI、バックアップ / 復元

CLI 

- 最初にすべてのセカンダリノードをアップグレードしてから、PAN をアップグレードする*
- アップグレードバンドルをすべてのノードに手動でアップロードする必要がある

GUI 

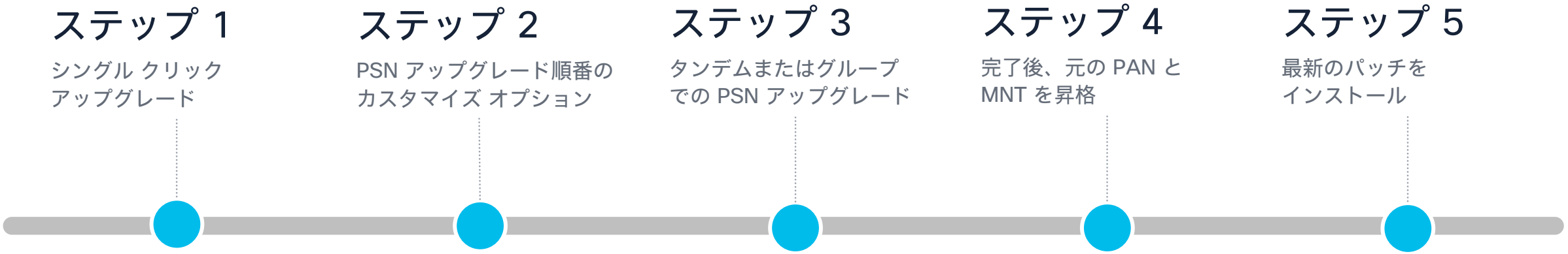
- ISE はアップグレードバンドルをすべてのノードに自動的にプッシュする
- シングル クリック アップグレード が可能

バックアップ / 復元 

- 古いバージョンをバックアップし、新しいバージョンで復元する
- ダウンタイムを最小限に抑えることができ、仮想環境に最適

*アップグレードガイドで詳細を確認

# アップグレード オプション
## GUI – スプリットアップグレード



# アップグレードオプション
## CLI – スプリットアップグレード

### ステップ 1
手動プロセス

### ステップ 2
各ノードを
個別にアップグレード

### ステップ 3
アップグレードイメージを
各ノードにコピー（9
GB）

### ステップ 4
アップグレードを準備
および実行

### ステップ 5
各ノードを個別に監視

### ステップ 6
最新パッチをインストール

注：
トラブルシューティング
にのみ推奨

# アップグレード オプション

## バックアップ、再イメージ化（新規作成）、復元 – スプリットアップグレード

# ハイブリッドアプローチ

## ハイブリッドアプローチ – スプリットアップグレード

### ステップ 1

GUI または CLI から
セカンダリ PAN の
登録を解除

### ステップ 2

展開内の他すべての
ノードの再イメージ化

### ステップ 3

すべてのノードを手動で
PAN に追加し同期

### ステップ 4

元のプライマリ PAN を
昇格

### ステップ 5

アップグレードされた
単一ノードの再イメージ化

### ステップ 6

再イメージ化された
ノードを展開に追加

### ステップ 7

最新のパッチを
インストール

# 最適なオプション

| | バックアップ / 復元 | GUI | CLI | ハイブリッド |
|---|---|---|---|---|
| 複雑度 | 中程度 | 容易 | 複雑<br>(手動操作を多く含む) | 容易 |
| アプライアンス<br>および仮想マシン<br>へのアクセス | 必須 | 最小限<br>(主に URT 用) | 必須 | 必須 |
| 並列機能 | あり | PSN のみ | 特定の順序であり | 1 つのノードのみ<br>アップグレードが必要 |
| ロールバック | 不可能、以前のバージョンへの<br>再イメージ化が必要 | 限定的 | あり | 限定的 |
| 以前の<br>アーティファクト | なし、クリーンイメージ | 維持<br>（以前の不具合による<br>ディスクの問題) | 維持 | なし、<br>クリーンイメージ |
| 時間 | 中程度 | 長時間 | 中程度、ノードごとの<br>アクティブなモニタリ<br>ングが必要 | 長時間 |
| 関連資料 | スタッフ多数、<br>追加の仮想マシンリソース | スタッフ少数 | スタッフ少数 | スタッフ多数、<br>一時的な仮想マシン<br>リソース |
| エラー | 最小 | ベストプラクティスを<br>使用しない場合に発生 | CLI の操作スキルがな<br>い場合に発生 | 最小 |

# フルアップグレード

## 事前チェック

すべてのノードに対してリポジトリが設定されていることを確認

アップグレードバンドルをダウンロード、すべてのノードに対して DB のアップグレードを準備

PAN またはスタンドアロンで 25%、他のノードで 1GB のメモリ空き領域を確保

PAN-HA が有効になっているかことを確認

スケジュールされているバックアップが有効であるかを確認

最近（直近 1 週間）のバックアップを確認

1. リポジトリの検証
2. バンドルのダウンロード
3. メモリのチェック
4. PAN のフェールオーバーの検証
5. スケジュールされているバックアップのチェック
6. コンフィグレーションバックアップのチェック
7. コンフィグレーションデータのアップグレード
8. プラットフォームサポート状況のチェック
9. 展開の検証
10. DNS の到達可能性
11. 信頼ストア証明書の検証
12. システム証明書の検証
13. ディスク容量のチェック
14. NTP の到達可能性と時刻源の確認
15. 負荷平均のチェック
16. ライセンスの検証
17. サービスまたはプロセスの失敗

# アップグレード後の作業

# アップグレード

## アップグレード後の作業

### ベストプラクティス

- 基本的な健全性チェックを行うため、オンデマンドヘルスチェックを実施
- 前のアップグレードからのクリーンアップ：CLI から ***application upgrade cleanup*** を実行する（スプリットアップグレードのみ）
- ユースケースと認証をテストして検証
- バックアップを再構成 – 手動バックアップの実行
- 自動 PAN フェールオーバー（構成されている場合）と PAN 間のハートビートを有効化

# 本日の振り返り

アップグレードパスとアップグレードの種類（スプリットまたはフル）を選択

システムアップグレードの準備

アップグレード後に、最新パッチをインストール

アップグレード後の作業を実行

# Resources

- Cisco ISE お役立ちリンク集

https://community.cisco.com/t5/-/-/ta-p/4527229

- ※本日のATXs以外のリソースリンクも確認できます。


CISCO