Intersight Success Community Webinar

やっぱりSplunkでしょ。IntersightデータをSplunk連携

シスコシステムズ合同会社

Toshiyuki Jimbo
Customer Success Specialist

2025年3月6日

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。

目次

1．SplunkとIntersightの概要

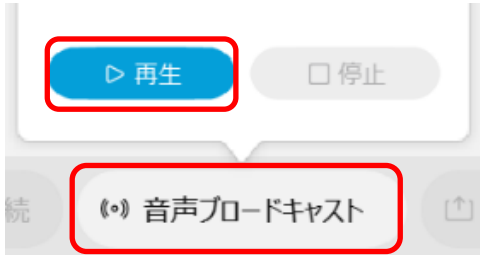
2．Intersigthtデータ連携のユースケースとメリット

3．デモ
連携方法とダッシュボードご紹介

音声について

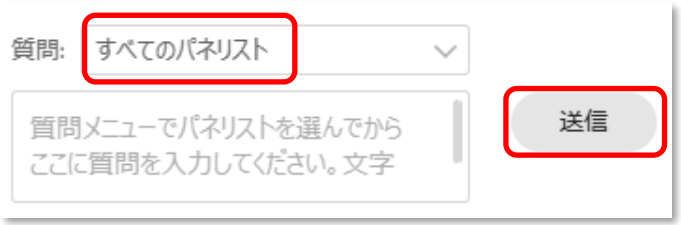
イベントが開始されると自動的に音声が流れ始めます。

音声が流れない場合は、画面下の [音声ブロードキャスト]を
クリックし、表示された画面から[再生]をクリックしてください。



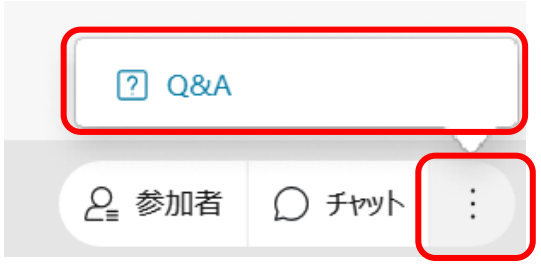
音声接続に関する詳細はこちらをご参照ください。
https://community.cisco.com/t5/-/-/ta-p/3129991

解決しない場合は、画面右側の Q&A ウィンドウより
[すべてのパネリスト (All Panelist)] 宛にお知らせください。



ご質問方法

ご質問は、画面右側の Q&A ウィンドウから
[すべてのパネリスト (All Panelist)] 宛に送信してください。



※ Q&A ウィンドウが
画面右側に見つからない
場合はここから表示

本日のプレゼンター

Tiffany Guo

カスタマーエクスペリエンス
カスタマーサクセススペシャリスト

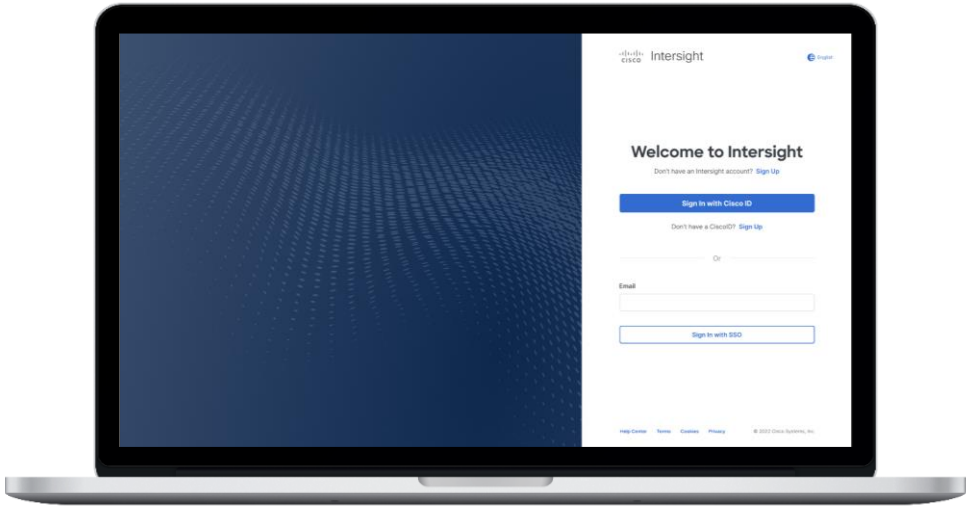
Toshiyuki Jimbo

カスタマーエクスペリエンス
カスタマーサクセススペシャリスト

Intersightとは？

クラウドから統合管理する SaaS サービス

CISCO INTERSIGHT



シスコのクラウドオペレーション
プラットフォーム...

ネットワーク、サーバ、ストレージ、
仮想マシンを可視化、運用の自動化

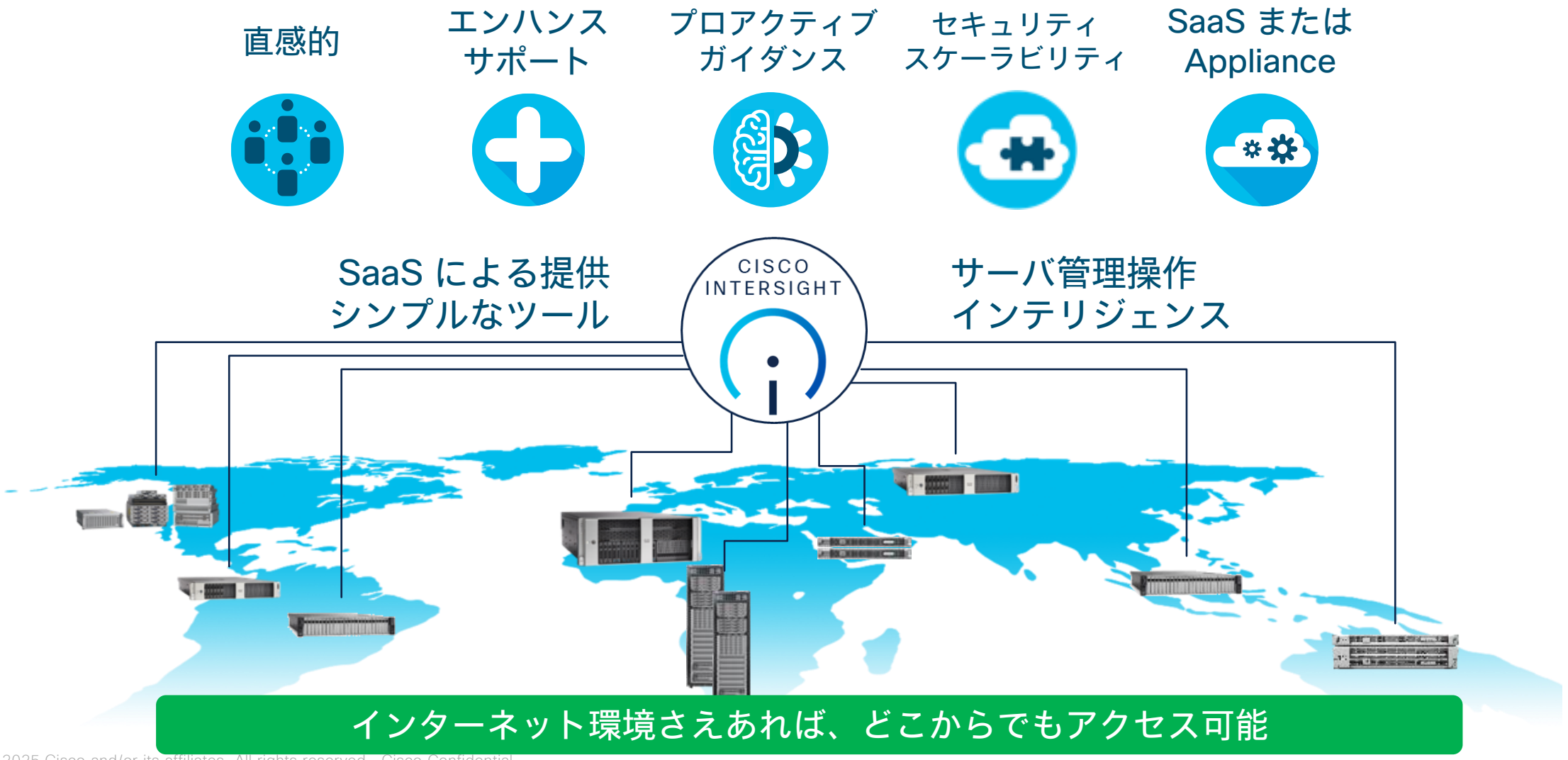
基本的には、SaaSで提供、
（仮想アプライアンス提供も可能）

どこからでも、

1つのダッシュボードから
全体の運用管理を実現

Intersightで何ができる？

クラウドから統合管理する SaaS サービス



Splunkとは？

セキュリティとオブザーバビリティ向上のための統合プラットフォーム

- セキュリティとITサービスのデータを集約し、分析・可視化する業務支援を行う
- AI技術（自動化や機械学習）で、予兆や運用効率の向上

統合プラットフォームとそれを支える**AI機能**
- Splunk Cloud
- Splunk Enterprise

パブリック
クラウド

ハイブリッド環境

オンプレミス型
データセンター

アプリケーション/
サービス

エッジ・IoT

Splunkで何ができる？

セキュリティとオブザーバビリティ向上のための統合プラットフォーム

- セキュリティとITサービスのデータを集約し、分析・可視化する業務支援を行う
- AI技術（自動化や機械学習）で、予兆や運用効率の向上

セキュリティ業務をご支援するハットトリック*を達成した
セキュリティ製品群
- Enterprise Security （ES）
- SOAR
- UEBA
- Attack Analyzer （フィッシング、マルウェア等）
- Mission Control

* Gartner, IDC, Forrester Wave3社よりリーダー認定

ITサービス運用、開発業務をご支援するオブザーバビリティ製品群 (Gartner, GigaOmにてリーダー評価)
- Observability Cloud / AppDynamics
  - IM：Infrastructure Monitoring（インフラ管理）
  - APM（性能管理）
  - RUM (Real Time User Monitoring)
  - Synthetic (外形監視)
- ITSI：SI for SAP など(機械学習でSAP運用強化)

サードパーティツール

カスタム/サードパーティのアプリケーション/サービス

統合プラットフォームとそれを支える**AI機能**
- Splunk Cloud
- Splunk Enterprise

エコシステム
- 1,800種類を超えるSplunk Baseアプリケーション
- パートナー様

パブリッククラウド

オンプレミスのデータセンター

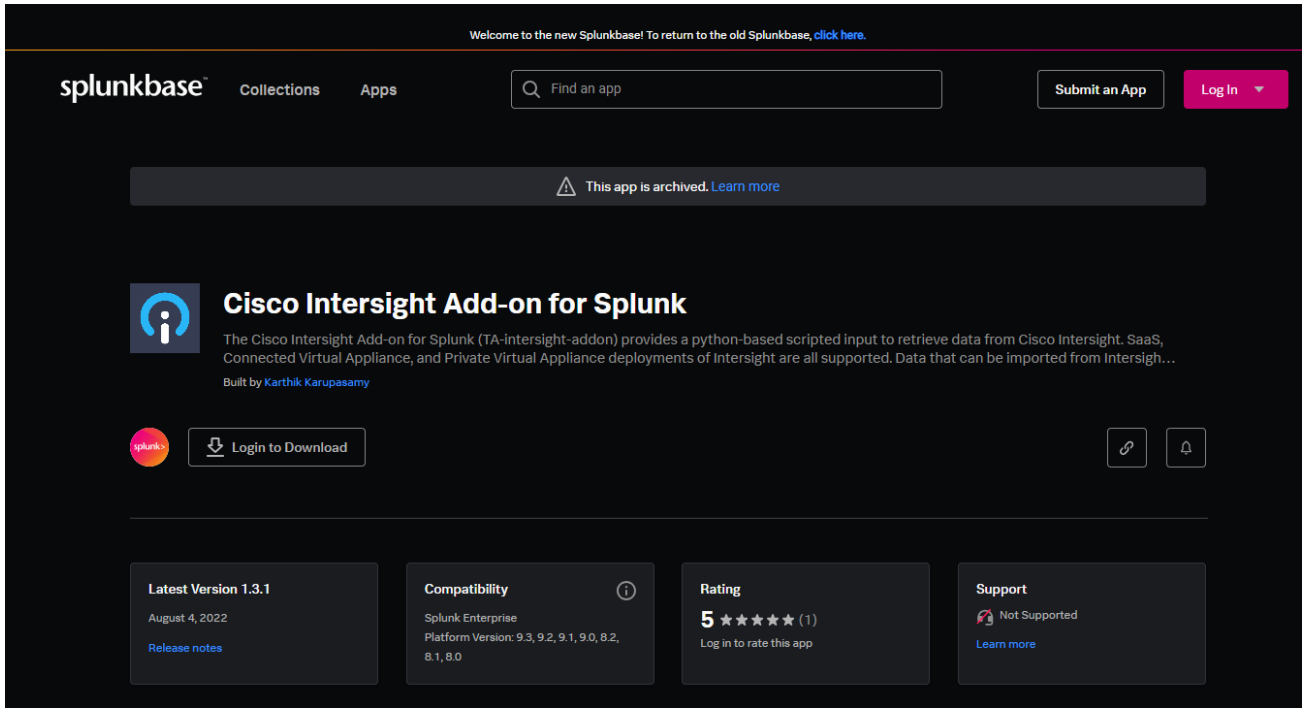
プライベートクラウド

デバイス

パブリッククラウド　ハイブリッド環境　**オンプレミス型データセンター**　アプリケーション/サービス　**エッジ・IoT**

SplunkとIntersight連携 Intersight Add-on

エコシステム
1,800種類を超えるSplunk Base
アプリケーション(Apps)
パートナー様



SplunkとIntersight 連携による可観測性の向上

- Intersight 監査ログ
- Intersight アラーム
- Intersight　インベントリ

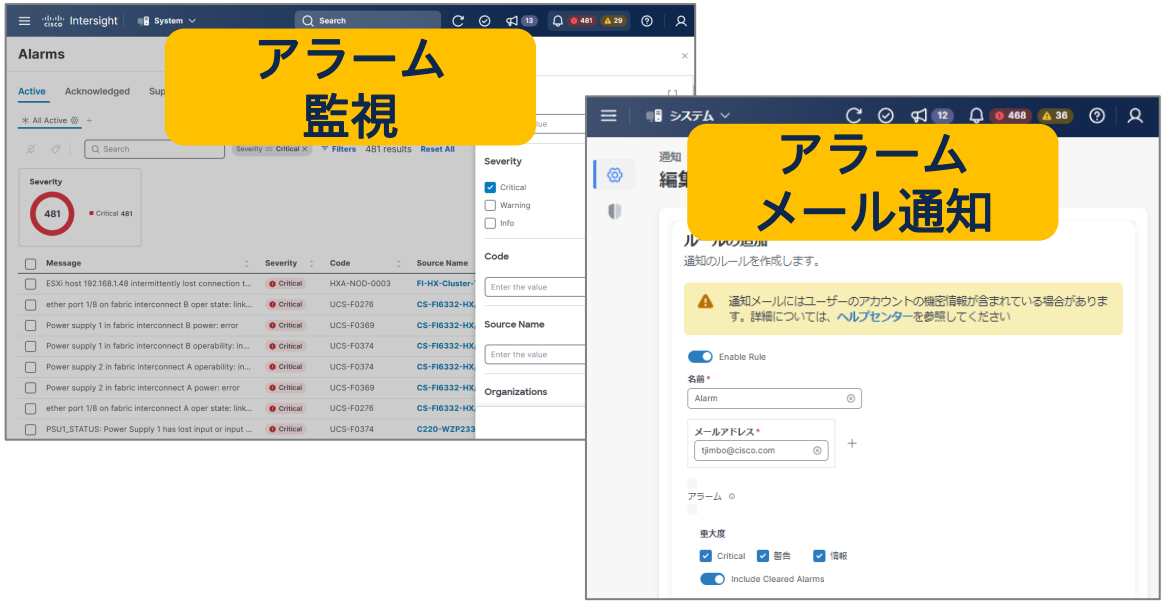
- ログ保管
- 統計 / 可視化
  （ダッシュボード）
- アラート

- Intersight でのトラブルシューティングや障害対応の高度化
- Intersight 管理機器の傾向分析とプロアクティブな問題検出
- Intersight の監査ログの可視化と活用

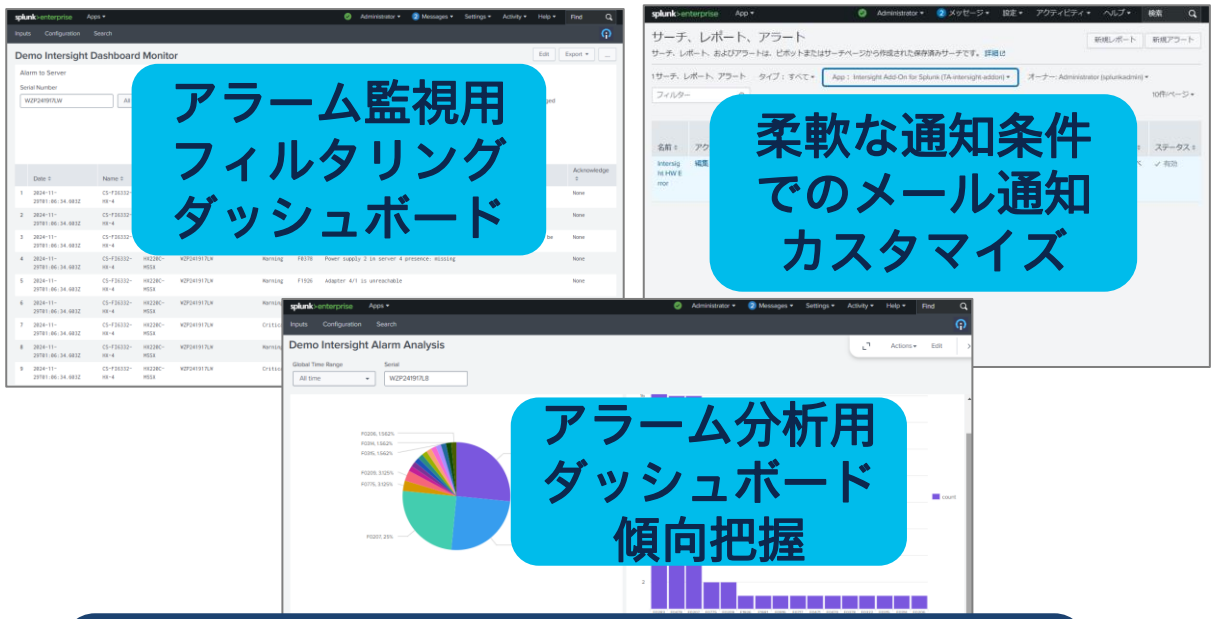
ユースケース 1
Intersight でのトラブルシューティング / 障害対応高度化

Intersight でのトラブルシューティング / 障害対応高度化

Intersightのアラーム状況を自由なレイアウト＆切り口で可視化・分析・通知



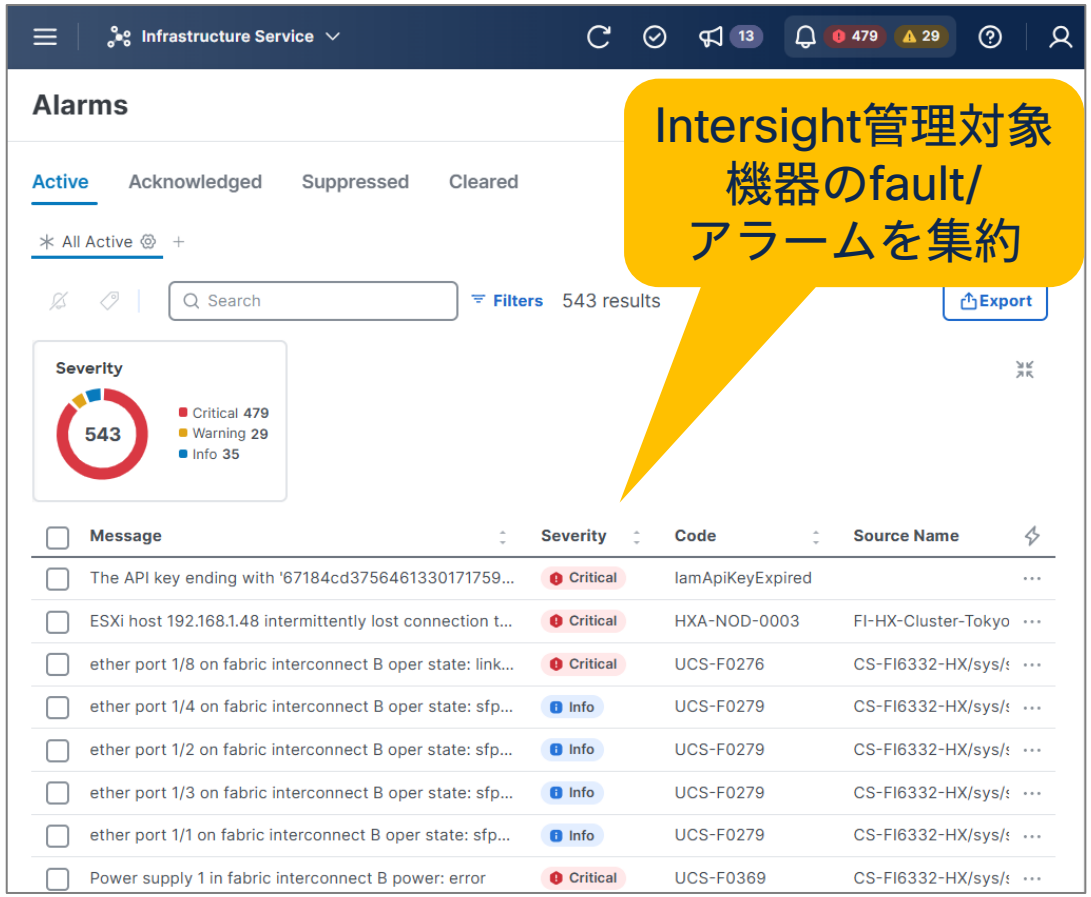
管理ポータルで提供される
基本的なモニタリングとメール通知

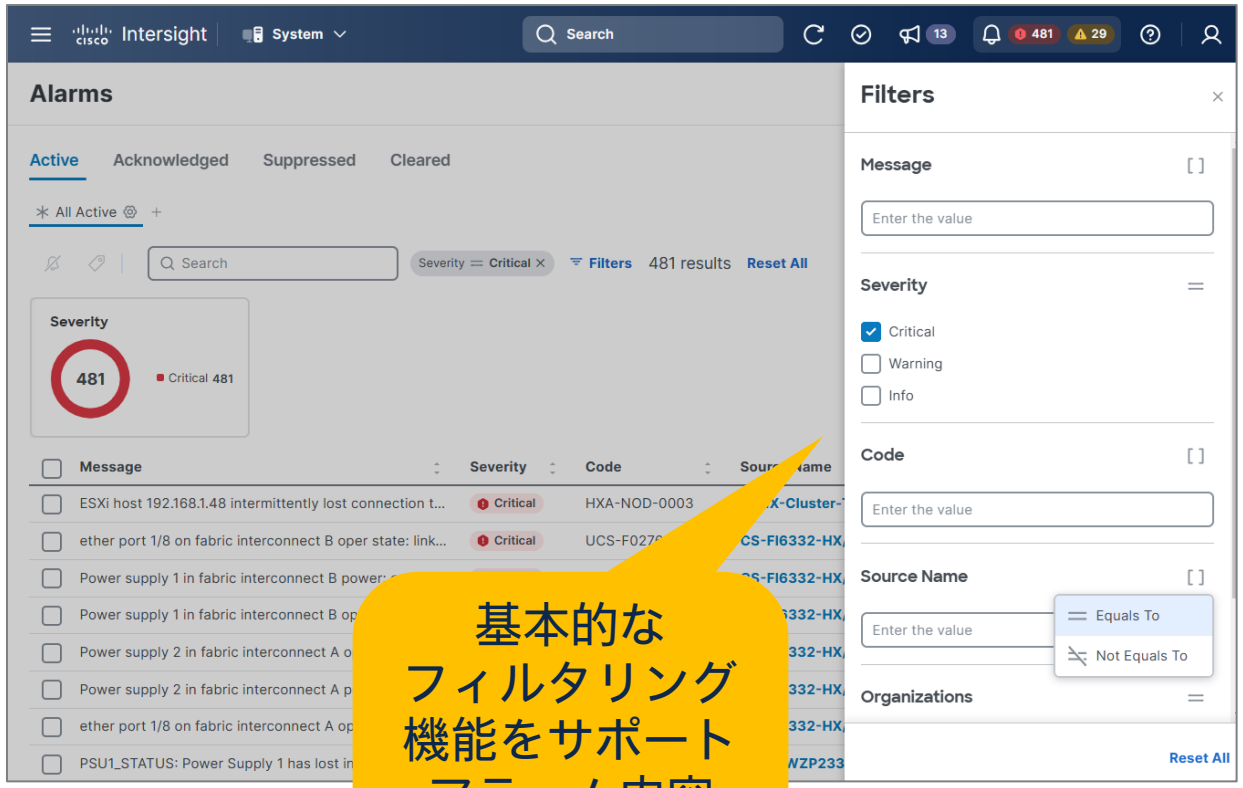


Intersight管理データを活用した
高度な可視化・分析・監視のカスタマイズ

Intersight でのトラブルシューティング / 障害対応高度化

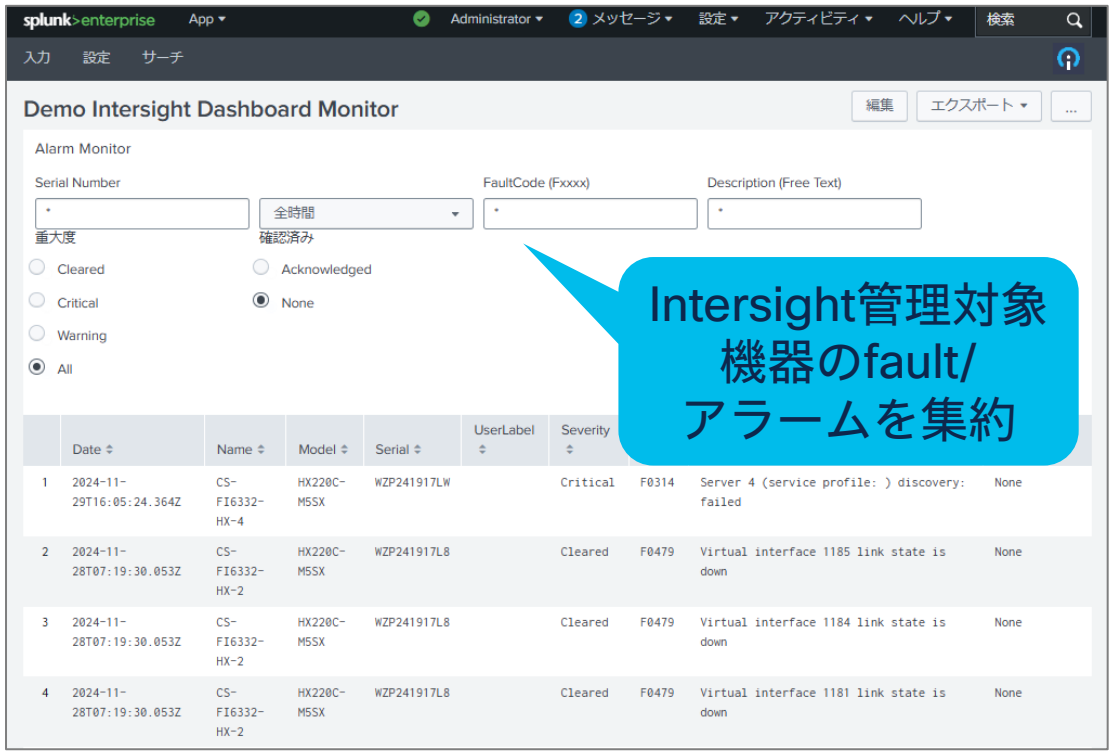
アラーム監視



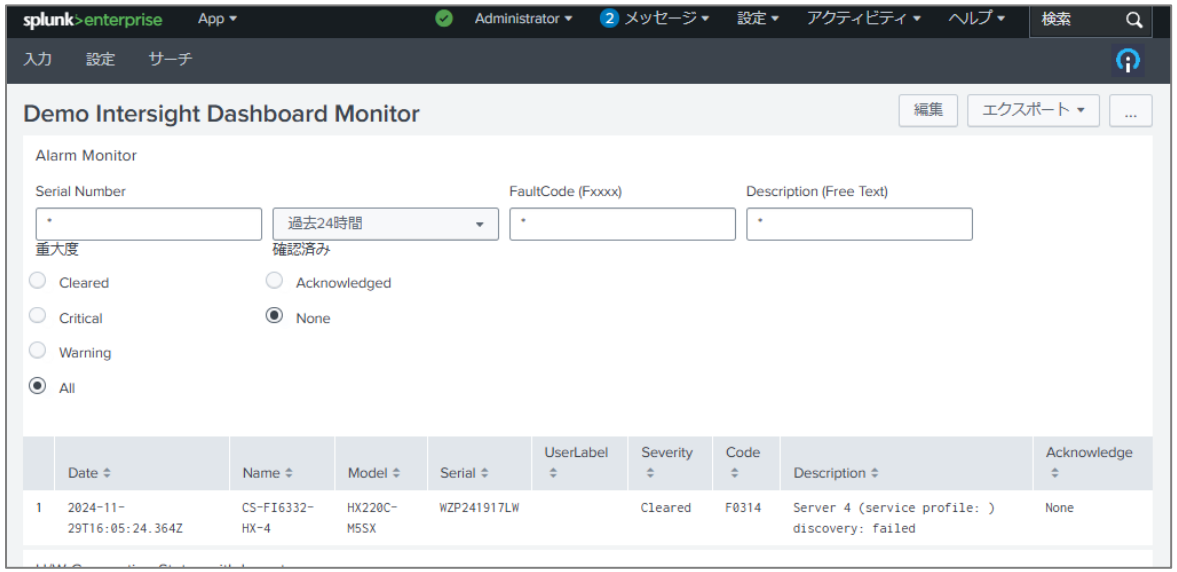


Intersight でのトラブルシューティング / 障害対応高度化

アラーム監視



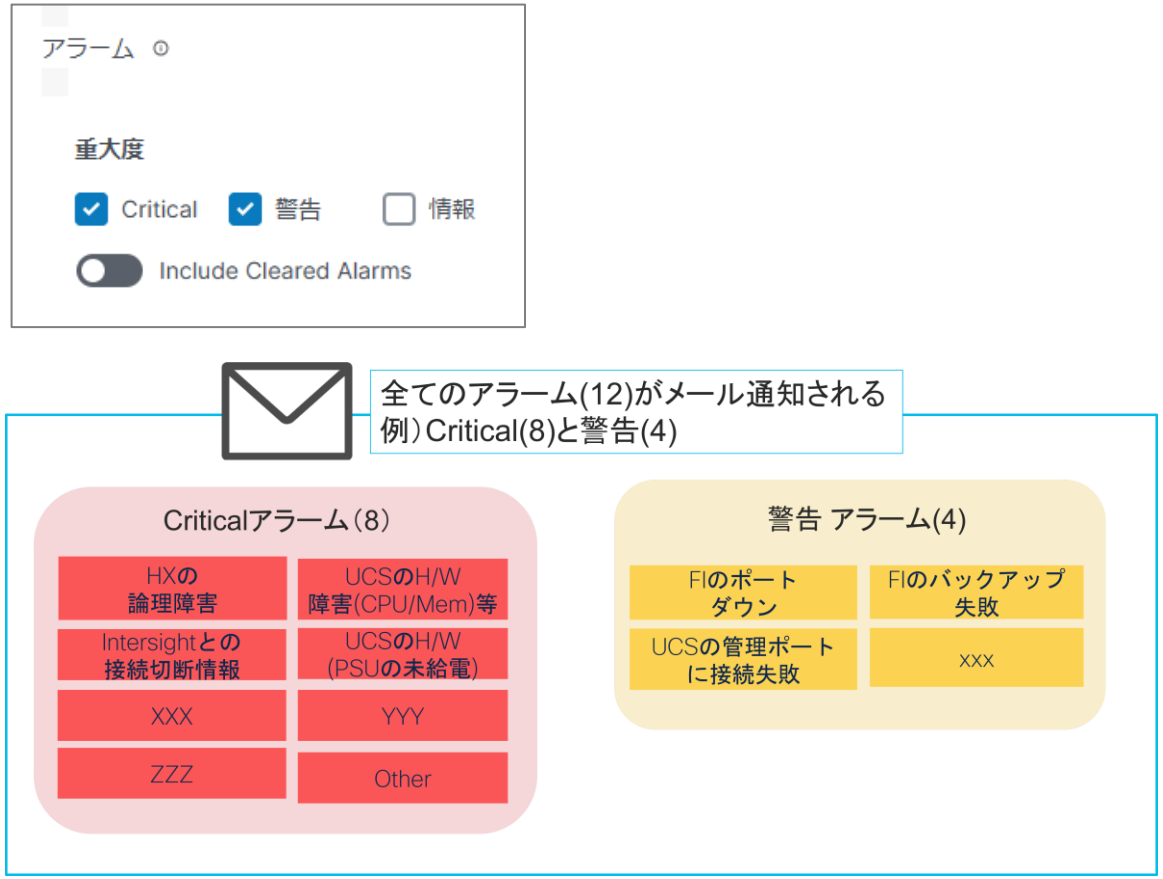
Intersight管理対象機器のfault/アラームを集約



faultコード、アラーム内容、
重大度に加えて、
アラームの発生日時、シリアル番号
でも絞り込み可能に！

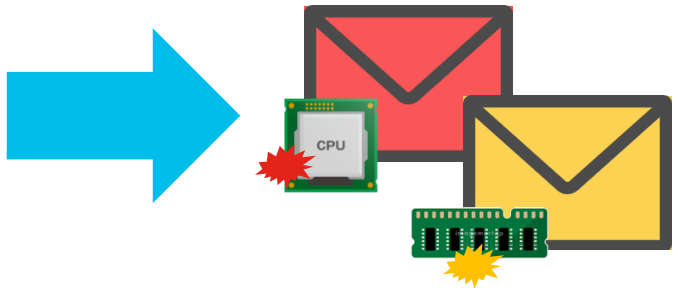
Intersight でのトラブルシューティング / 障害対応高度化

アラーム
メール通知



Intersight でのトラブルシューティング / 障害対応高度化

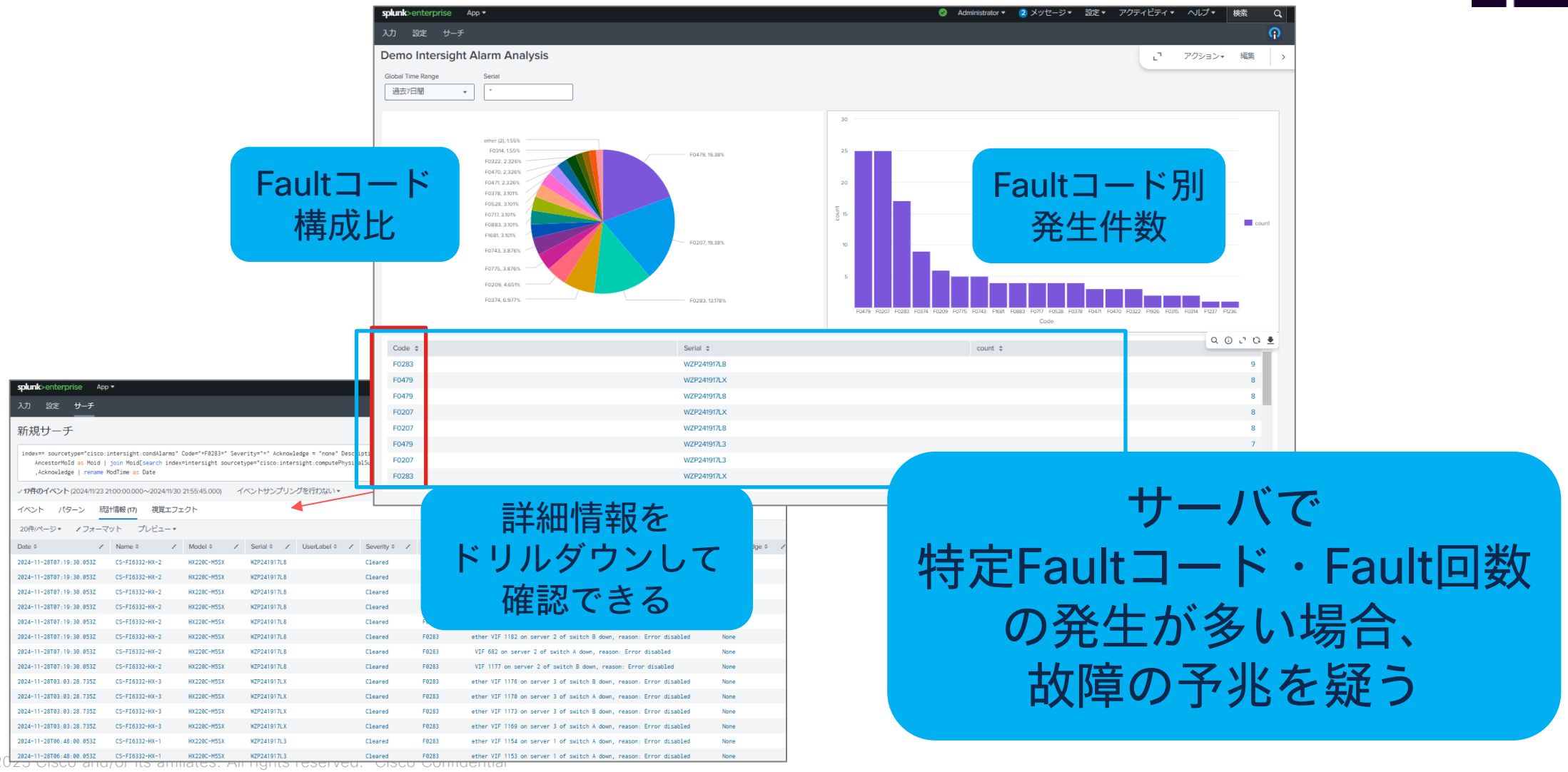
柔軟な通知条件でメール通知カスタマイズ



ユースケース 2
Intersight 管理機器の傾向分析とプロアクティブな問題検出

Intersight 管理機器の傾向分析とプロアクティブな問題検出

統計情報を整理し、グラフも組み合わせ、より分かりやすくカスタマイズ



ユースケース 3
Intersight 監査ログの可視化と活用

Intersightの監査ログの可視化と活用

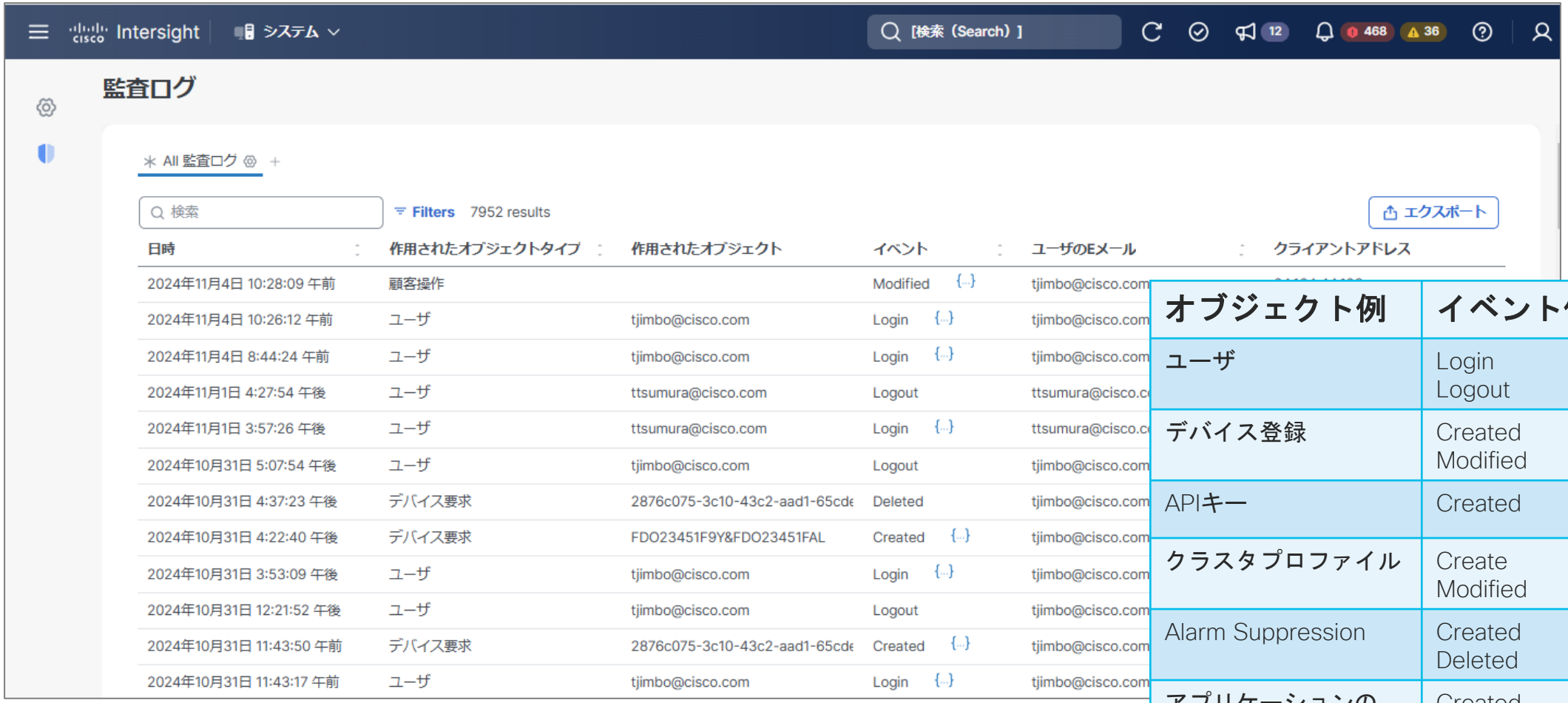
1.　退職者の利用状況チェック
退職者が出た場合は不正なアクセスや操作をしていないかチェック

２．不正操作など内部不正への備え
情報漏洩や不正操作などの内部不正をチェック

監査していることを従業員に通知すれば、内部不正の抑止力としても有効

Intersightの監査ログの可視化と活用

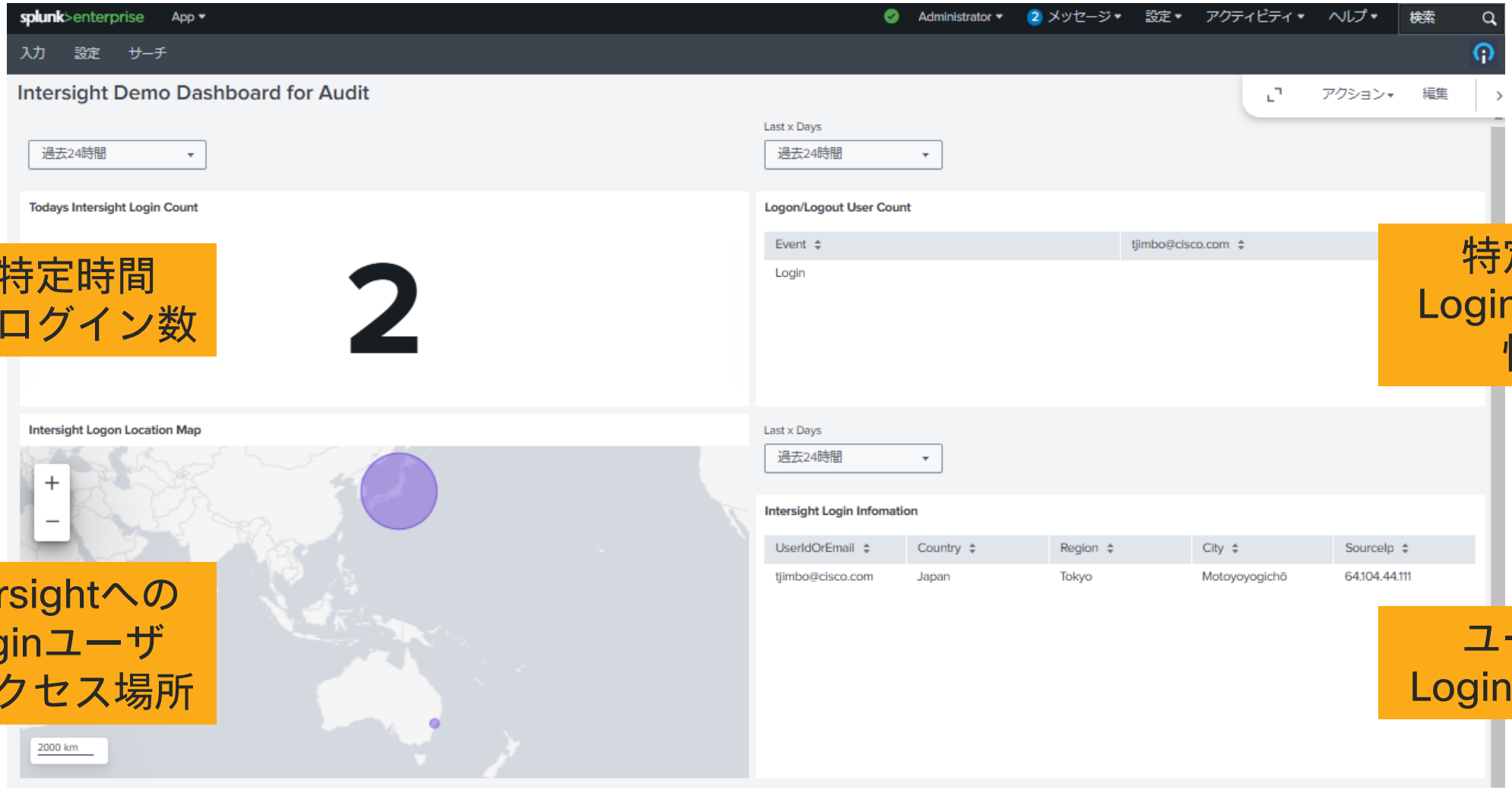
Intersightの監査ログ



オブジェクト例	イベント例
ユーザ	Login Logout
デバイス登録	Created Modified
APIキー	Created
クラスタプロファイル	Create Modified
Alarm Suppression	Created Deleted
アプリケーションの登録	Created

Intersightの監査ログの可視化と活用

Intersightの監査ログをより分かりやすく



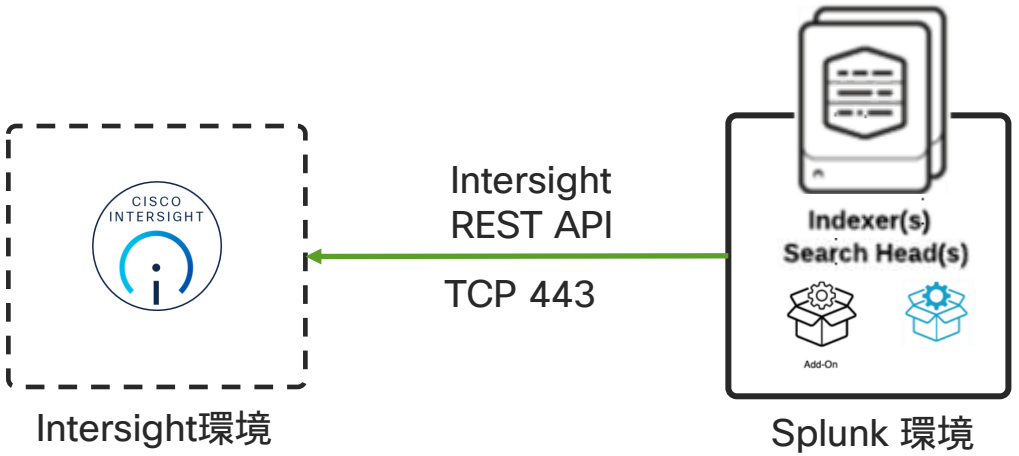
特定時間
のログイン数

特定時間
Login/Logout
情報

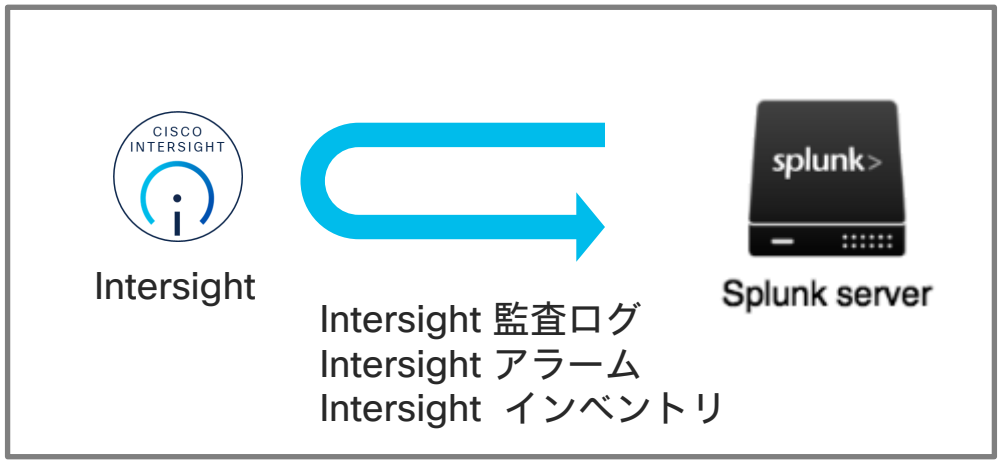
IntersightへのLoginユーザのアクセス場所

ユーザ別
Login詳細情報

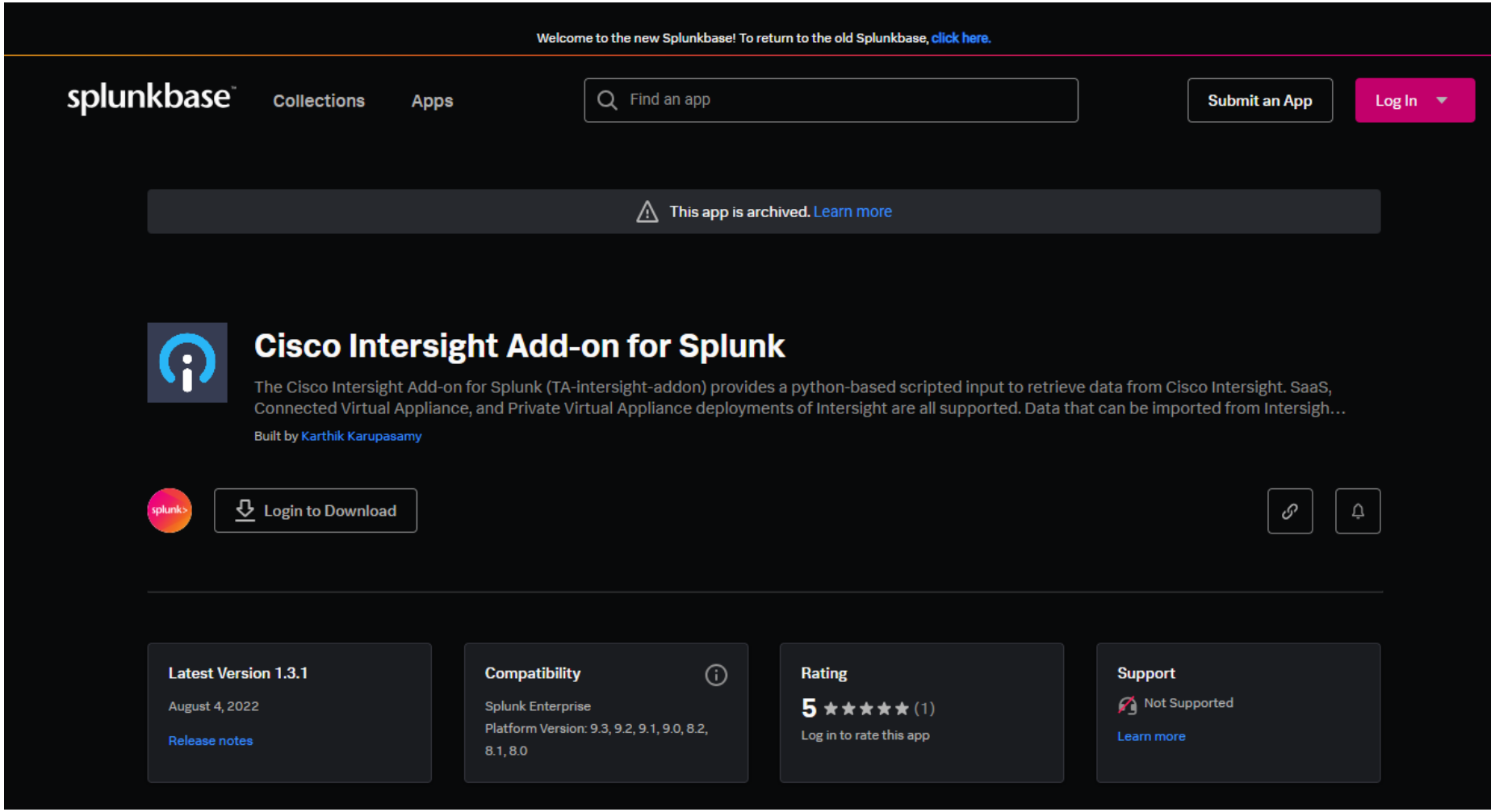
Intersight環境から情報収集する仕組み



使用例

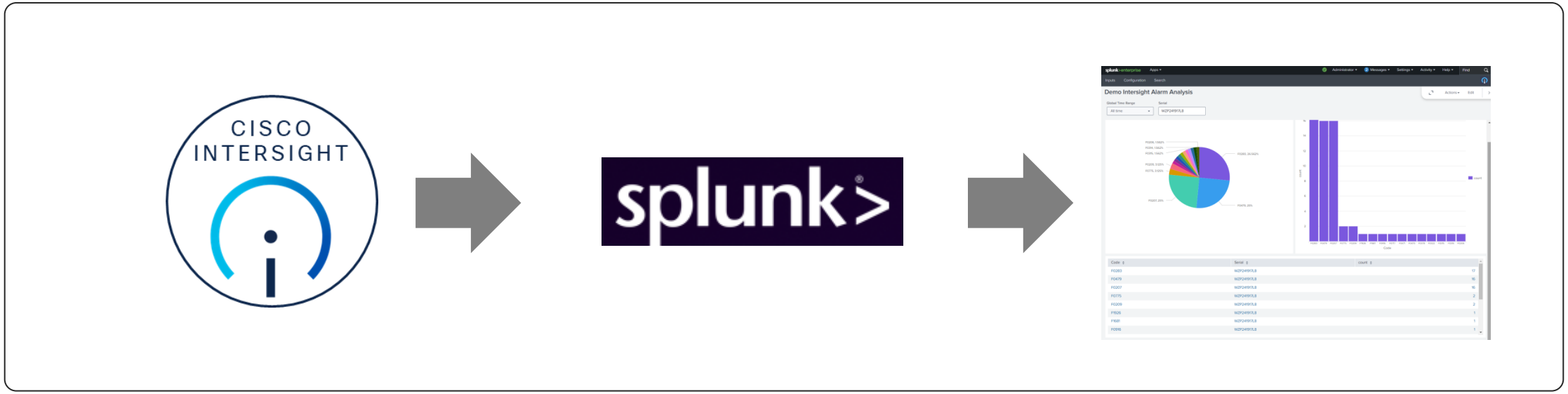


Intersight環境から情報収集する仕組み



本日のデモ

Splunk連携の方法



Step 1
Splunk Enterprise
を構築

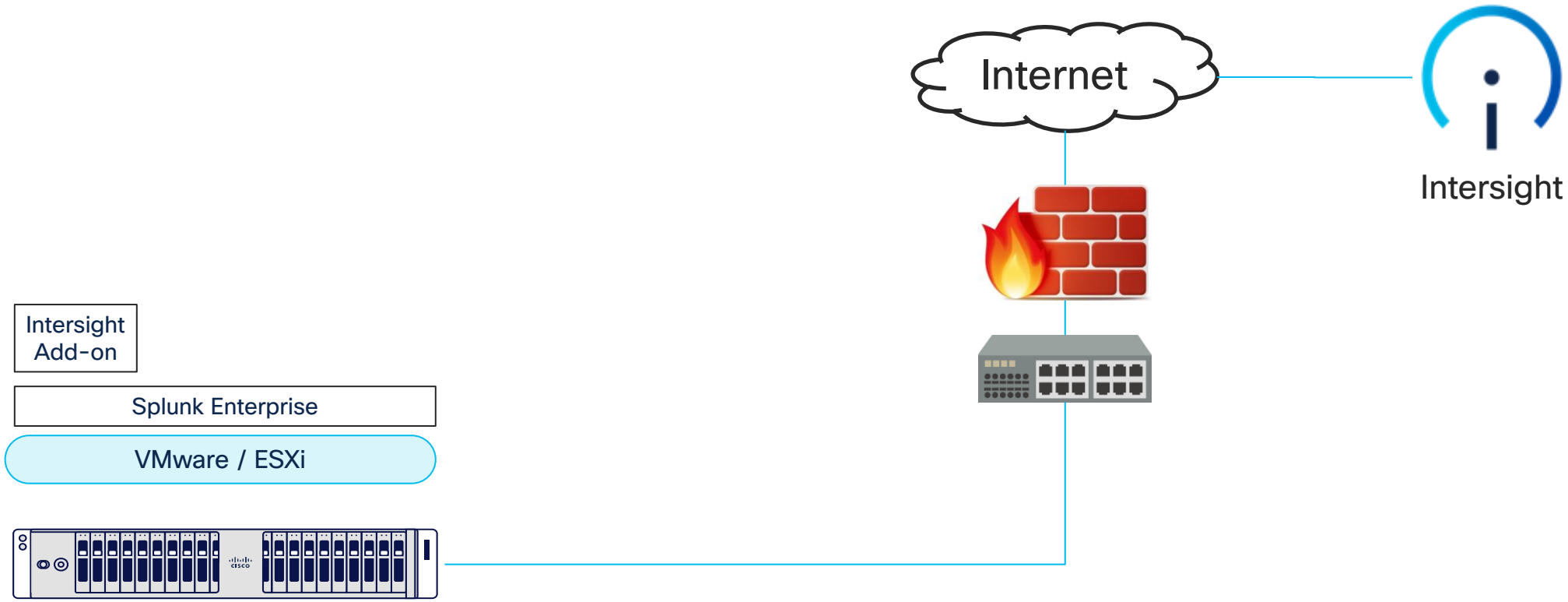
Step 2
Intersight
API Key/Id発行

Step 3
Intersight
Add-on 導入

Step 4
Splunk Add-on
Input設定

Step 5
Splunk Dashboard
作成/インポート

本日のデモ内容 (環境)



App 管理

Appを名前でサーチ...

- Intersight Add-On for Splunk
- Search & Reporting
- Splunk Dashboard Examples
- Splunk Secure Gateway
- Upgrade Readiness App

他のAppのサーチ

こんにちは, Administrator

クイックリンク ダッシュボード 最近表示したデータ 自分で作成 あなたと共有

共通のタスク

データの追加
さまざまな共通のソースからデータを追加します。

データのサーチ
Splunkサーチでデータを行動に変えます。

データの視覚化
データに適したダッシュボードを作成します。

チームメンバーの追加
Splunkプラットフォームにチームメンバーを追加します。

権限の管理
ロールを使用して、アクセスできるユーザーを制御します。

モバイルデバイスの設定
Splunk Secure Gatewayを使用してモバイルデバイスにログインまたはモバイルデバイスを管理します。

学習およびリソース

プロダクトツアー
Splunkは初めてですか？ツアーに参加して使用方法を確認しましょう。

Splunk Docsで詳しく学ぶ
総合的なガイダンスに従ってSplunkソフトウェアをデプロイ、管理、使用します。

Splunkエキスパートの支援を受ける
Splunk Lantern カスタマーサクセスセンターの利用可能なガイダンス。

権限の拡張
Splunkbaseにある何千ものAppを参照します。

Splunkコミュニティに参加する
学び、刺激を受け、知識を共有します。

他のユーザーのSplunkの使用方法を確認する
実際のカスタマーストーリーを参照します。

トレーニングおよび認定
認定Splunk Ninjaになる。

本日のセッションのまとめ

1. IntersightとSplunkの連携により
   可観測性を向上可能

2. トラブルシューティングや障害対応の
   迅速化・プロアクティブな問題検出
   監査ログの可視化と活用

3. 無償トライアル利用可能
   Splunk Enterprise (60日)
   Splunk Cloud (15日)

Cisco Intersight/UCS サクセスコミュニティ Webinar

Cisco Intersight/UCSユーザ様、運用パートナ様向けに、Webセミナーを実施させて頂きます。

開催日時	テーマ
2025年4月10日 (木) 15:30 ～ 16:30	Intersight success community - webinar#4 <非公式> UCS C220 M5+RAID構成にNutanix CE 2.1を入れてみる

※ 途中参加、途中退席も可能です。ご自由に参加ください。
※ 開催中はQAを受け付けておりますので、お気軽にご質問ください。


Cisco
Customer Experience