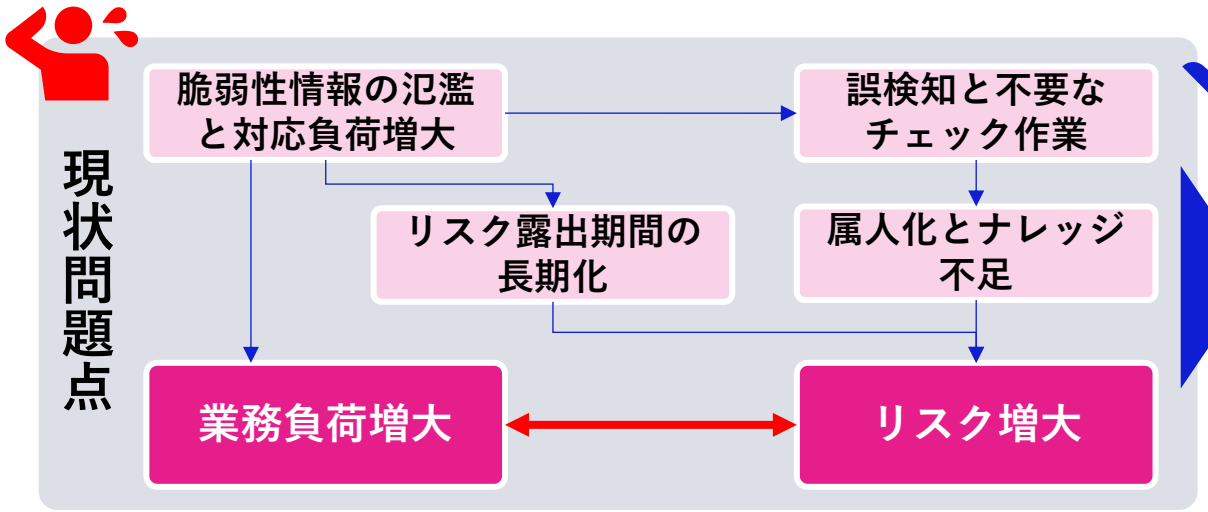
SymBPO関係者外秘

脆弱性対応要否判定（AI判定）

Index

脆弱性管理DX

現状のネットワーク機器脆弱性対応における「誤検知」「判断遅延」「属人化」「高コスト」といった課題を解決し、運用工数50%以上削減とサイバーリスク低減



解決策

カテゴリ	主要要件（優位点）
判定精度	Config前提の**実環境リスク評価**
説明性	**説明可能なAI**（初動として暫定回避策実行）、日本語対応 **判定根拠のナレッジ化**
網羅的情報収集	マルチベンダ対応、エージェントレスの情報収集
品質保証	平均判定時間/誤判定率のSLO公開による信頼性確保

処理フロー

構成情報/CVE自動突合 → Config分析 → 実環境リスク評価（AI判定） → ITSMへ自動通知/記録

期待効果

年間工数削減
1M
・朝チェック自動化
・受入教育効率化

対応LT短縮
50～80％短縮

重大インシデントによる損失機会低減
1,000～3,000万円規模

参考）脆弱性管理DX化

ネットワーク機器脆弱性対応における「誤検知」「判断遅延」「属人化」「高コスト」という課題が顕在化
網羅的情報収集、判定精度、説明性で解決策を検討

脆弱性管理の課題（市場調査、アカウント部ヒアリング）

	表層事象	原因
1	脆弱性情報収集が半自動～手動	NVD、JVN、各ベンダサイトに情報が分散、個別フォーマット
2	脆弱性検知～スキャンは対象へのAgentインストールが必要	各ベンダーでCLI構文・SNMP MIB・APIが非互換
3	ベンダ製品毎に管理手法が異なる	製品名・ファーム呼称の差によるマッピング不安定
4	脆弱性情報-構成情報の関連付けが手動依存	スキャナ/ITSM製品がAgent中心の設計前提で高価
5	判断・優先順位付けが属人化	Agentレスで情報収集・スキャンする仕組みはSIが必要
6	コスト面でのハードルにより、脆弱性の網羅的管理が困難	機能有効/モジュール存在/特定設定依存などベンダ固有で共通化が困難
7	構成情報の最新化が手動	CVSS単独評価で、ビジネス重要度・適用条件がルール化されていない
8	構成情報スキャンは対象へのAgentインストールが必要	標準化されたプロセス・判断基準がない
9	脆弱性対応状況報告が手動	集計・グラフ化がエクセルベース

施策

対応方針	具体的な解決策
網羅的情報収集	**脆弱性** • NEC脆弱性情報提供サービスを利用（NVD、JVN、ベンダ提供情報を網羅的にカバー） **構成情報** • 監視システム（Zabbix）のディスカバリ機能を活用したエージェントレスによるインベントリ情報収集 • Zabbixテンプレートのカスタマイズによるマルチベンダ対応 **脆弱性-資産構成の関連付け** • 製品マスタを作成し、脆弱性-構成情報の自動マッピング
判定精度	• Config参照に実環境リスク判定 • 暫定回避策の対応要否（バージョンアップ以外の回避策の有無） • 脆弱性対応フェーズ判定（暫定/恒久） • AI判定精度の信頼性担保
説明性	• 脆弱性対応プロセスの自動化、ITSMによる管理 （脆弱性検知⇒対象製品特定⇒対応要否判定⇒起票） • 判定根拠の機会学習・ナレッジ化
UX向上	• 統合ダッシュボードで一元管理 • 自動レポーティング

参考）Config参照した脆弱性リスク判定機能

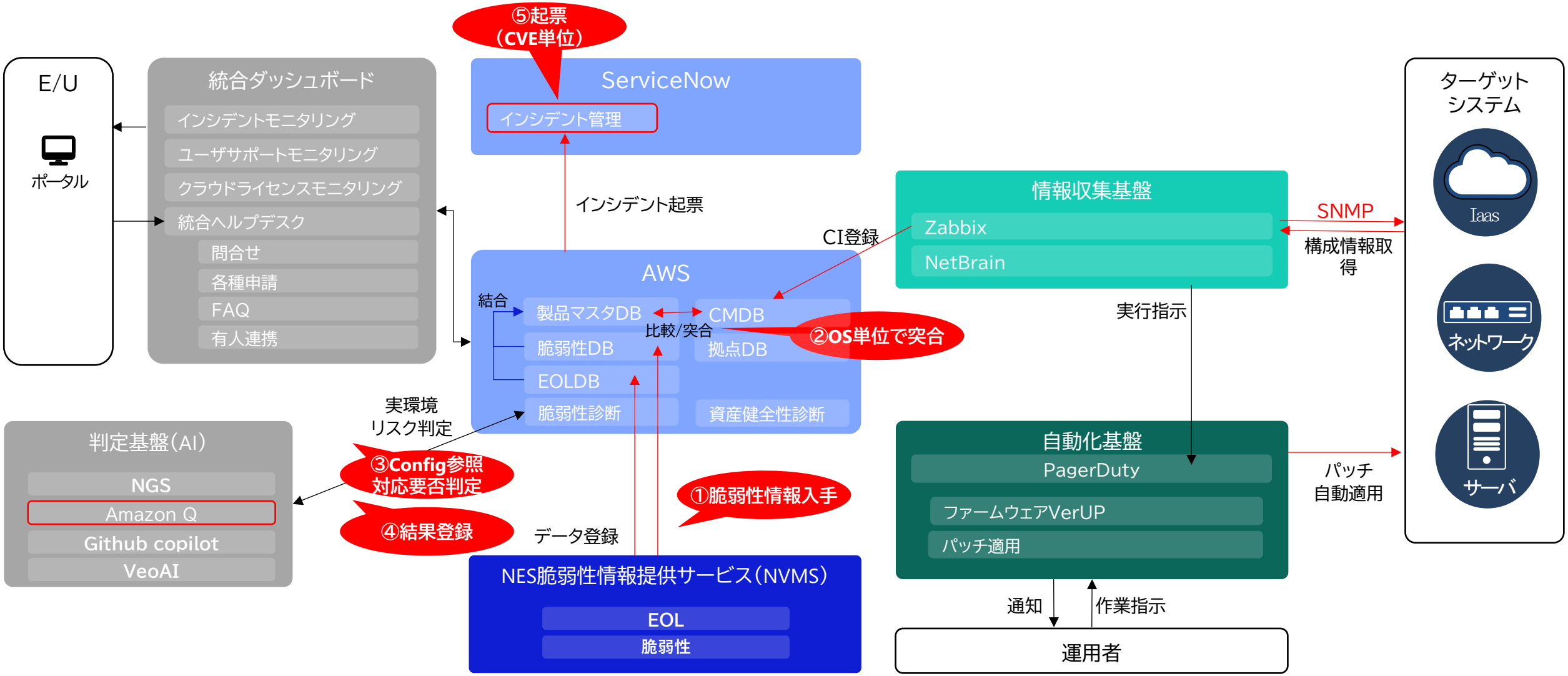
■ 目的

1. **対応要否判定**
   - 脆弱性脅威に晒されているConfig状態なのか判定する
     →さらされていなければ、緊急度を下げる
2. **暫定回避策の対応可否判定**
   - バージョンアップ対応以外の回避策があるか判定（脆弱性機能のOFFなど）
     →バージョンアップ評価は時間を要するため、緊急度が高い脆弱性の場合は暫定回避策の適用を初動で実施する
     ※一般的に、緊急度・リスクレベルが高いものほど、暫定回避策もセットで発表されるケースが多い
3. **暫定回避策適用のためのConfig出力**
   - NVISデータベース内にある情報で、変更用のConfigを出力する
4. **脆弱性対応フェーズ判定**
   - 現行のConfigが、暫定対策済み/恒久対策済み、どちらのフェーズか判定する

■ 前提条件

- 1ホストが、複数脆弱性に該当するケースがある（1：他の管理をする必要あり）
- ホスト・Config・脆弱性の関係は、1：1：他
  ※Configは、常に最新版のConfigをみて判定をするべき（Configが変更されたら、脆弱性判定が実行されてほしい）

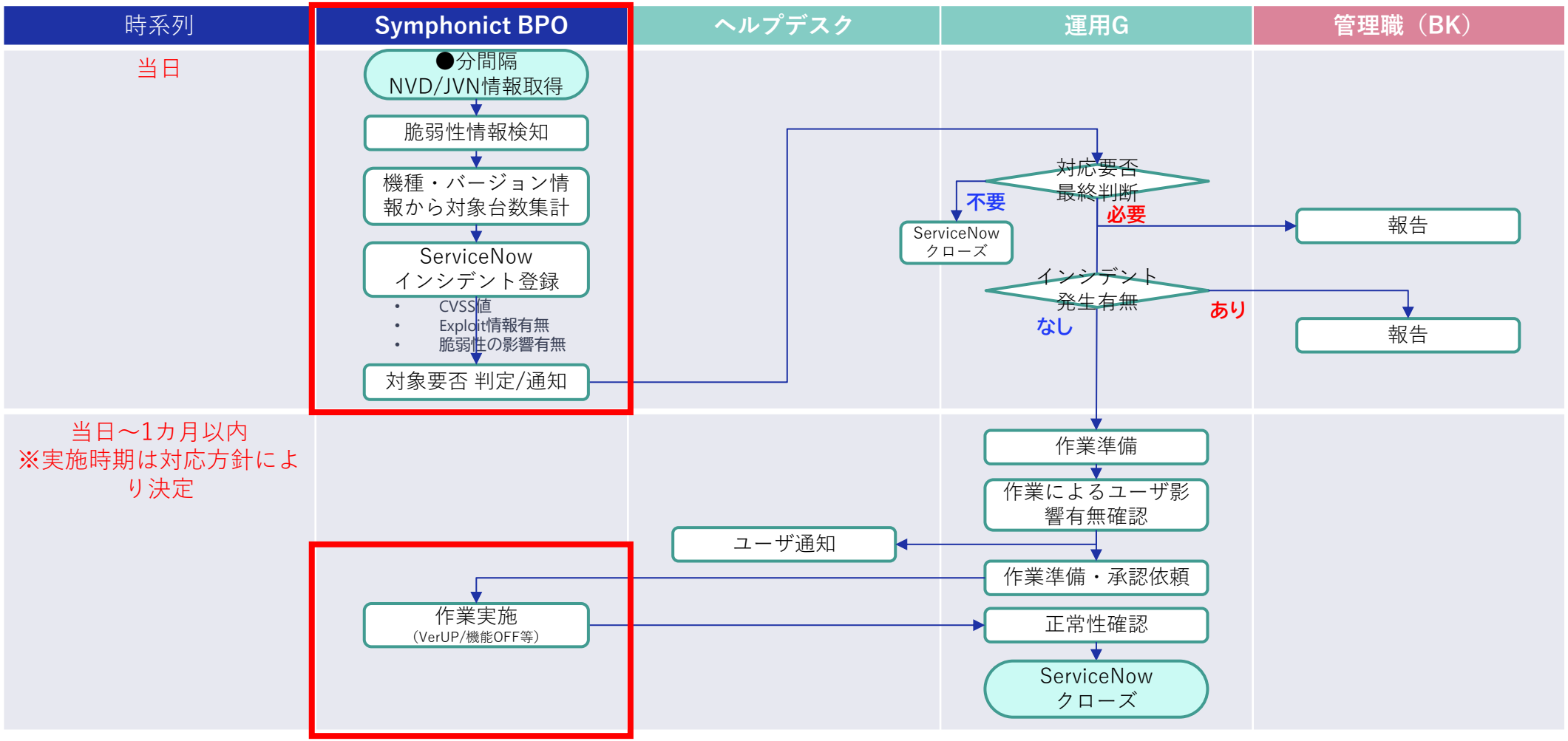
2.システムイメージ



詳細はSymphonictBPO(ライフサイクル管理)_業務フロー_v0.3.xlsx
「5_脆弱性情報自動取得・検知・通知・登録フロー」参照

3.業務フロー

脆弱性検知、対象機種/台数の集計、インシデント登録、脆弱性対象要否判定/通知までを自動化
対応要否の最終判断移行は運用者にて実施



4.AIによる対応要否の自動判定の出力イメージ

■ 運用者への脆弱性通報

- 通報対象は設定可能（重要度、機器区分など通報対象をユーザ側でカスタムできる機能を導入）
- 集計された結果を速報（視認性向上のため）

お客様名	製品名(ソフトウェア)	バージョン	CvssSortKey	脆弱性識別子	要否	理由	台数
A社	Cisco IOS XE Software	17.6.5	10	cisco-sa-iosxe-webui-privesc-j22SaA4z	必要	・・・であるため	30
	Cisco IOS XE Software	17.6.5	10	cisco-sa-iosxe-webui-privesc-j22SaA4z	不要		15

■ 脆弱性判定サンプル

【インプット情報（CMDB/脆弱性情報DB/ConfigDBから取得）】

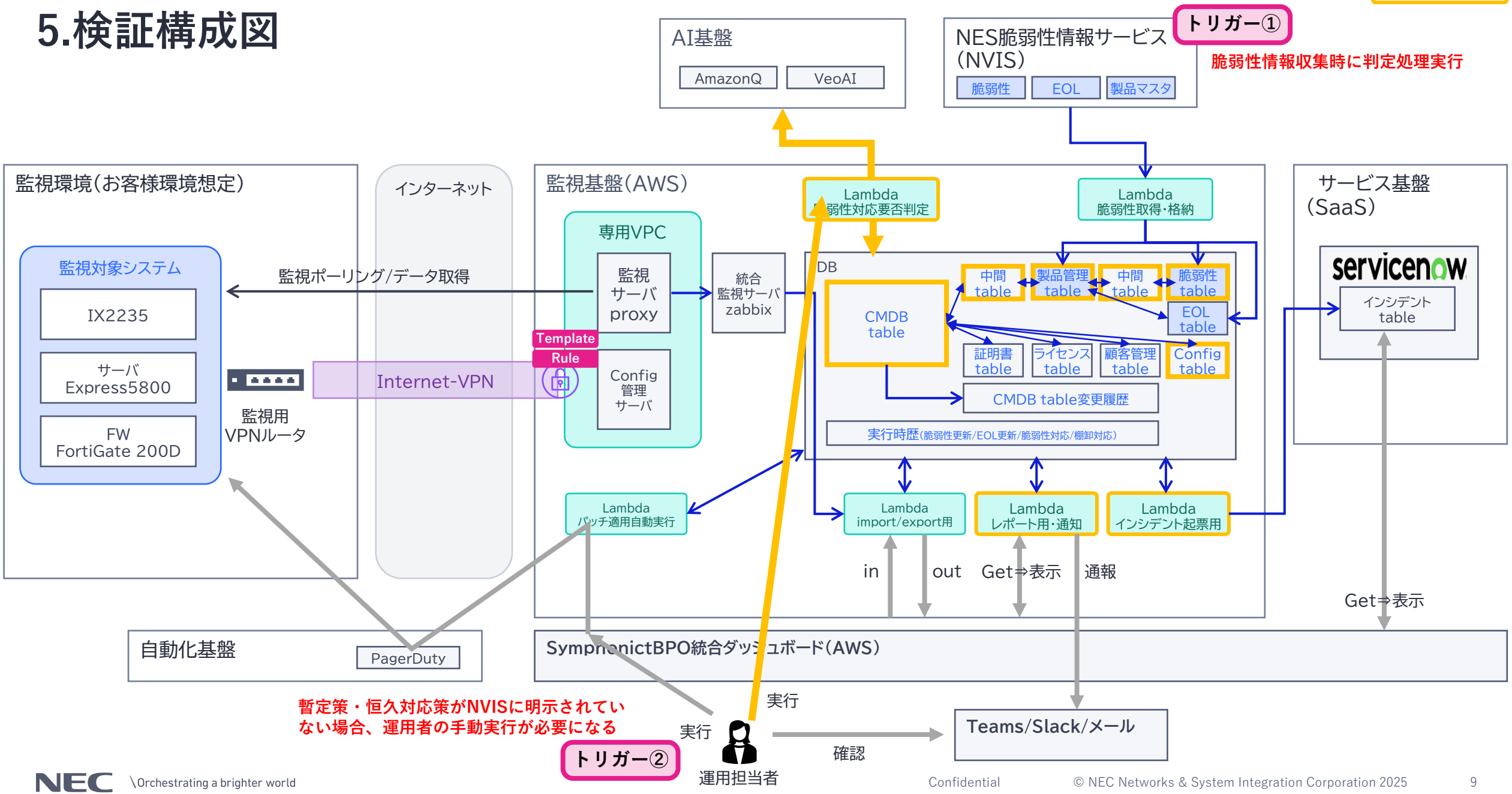
- **脆弱性（CWE-787）**
  - FortiOS および FortiProxy の範囲外書き込みの脆弱性 [CWE-787] により、認証されていないリモートの攻撃者が特別に細工した HTTP リクエストを介して任意のコードまたはコマンドを実行できる可能性があります。
- **回避策**
  - SSL VPN を無効にする
    (Web モードを無効にすることは有効な回避策ではありません)

```
edit "ssl.root"
    set vdom "root"
    set type tunnel
    set alias "SSL VPN interface"
    set snmp-index 10
next
```

【AI判定 期待値】

- **対応要否**
  要対応
- **理由**
  現在、SSL VPNインターフェースが設定されており、有効な状態と判断されます。
  Fortinetの公式案内にある「SSL VPNの無効化」が暫定的な唯一の有効な対策となっており、現状の設定のままでは脆弱性に晒される状況です。

5.検証構成図



Appendix

AI判定検討ログ

参考：課題放置した場合の影響

資産管理が滞っている場合、企業は様々なリスクに直面します。特にPC、サーバー、ソフトウェアライセンスといったIT資産は、ビジネスの根幹を支えるた、管理の不備が直接的かつ広範な影響を及ぼす可能性があります。

1．セキュリティリスクの増大

① 脆弱性の放置

② 不正アクセスの温床

③ 紛失・盗難時の対応遅れ

被害種別　例）	平均被害額
ランサムウェア感染	2,386万円
エモテット感染	1,030万円
ウェブサイトからの情報漏えい（カード及び個人情報）	3,843万円
ウェブサイトからの情報漏えい（個人情報のみ）	2,955万円

参照元：. https://jpn.nec.com/cybersecurity/blog/241004/

2．　業務効率の低下と生産性の損失

① 管理業務の非効率化

② 情報検索が困難

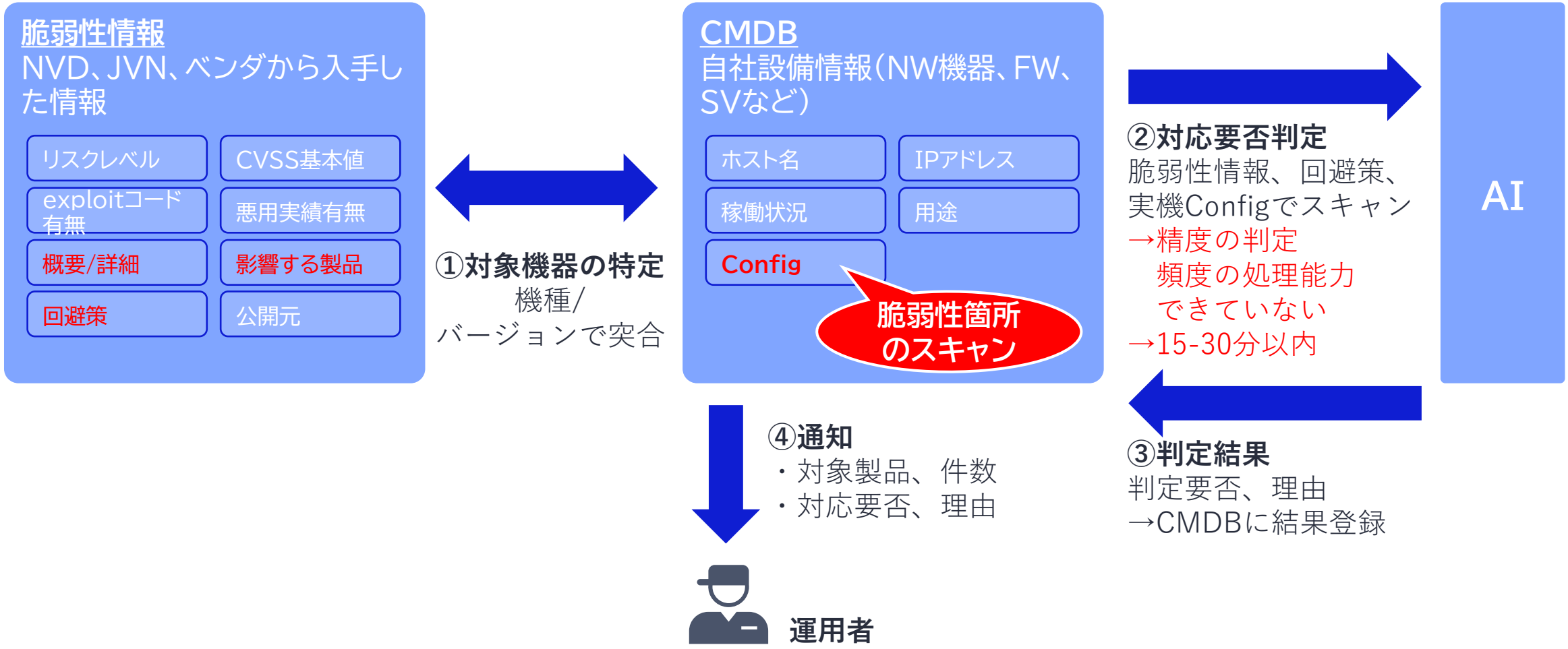
③ 計画的なIT投資の阻害

内容　例）	平均工数
構成管理（年次棚卸）　15拠点×１回	30h×時間単価
変更管理（年次棚卸）　15拠点×３回	90h×時間単価
Ver管理（年次棚卸）　100台×1回	16h×時間単価
パッチ適用（四半期）　100台×4回	400h×時間単価

参照元：エネオスマテリアル　現行：インフラ運用サービス業務一覧

全体イメージ

脆弱性検知時に、脆弱性情報、CMDB情報から、**対応要否を自動判定**させたい



対応要否 AI判定

脆弱性検知時に脆弱性情報、回避策、現行Configから、対応要否を自動判定させたい

【インプット情報（自社の脆弱性情報DB/CMDBから取得）】

■ 脆弱性

- FortiOS および FortiProxy の範囲外書き込みの脆弱性 [CWE-787] により、認証されていないリモートの攻撃者が特別に細工した HTTP リクエストを介して任意のコードまたはコマンドを実行できる可能性があります。

■ 回避策

- SSL VPN を無効にする(Web モードを無効にすることは有効な回避策ではありません)

■ 現行Config

```
edit "ssl.root"
    set vdom "root"
    set type tunnel
    set alias "SSL VPN interface"
    set snmp-index 10
```

【AI判定 期待値】

- **対応要否**

  要対応

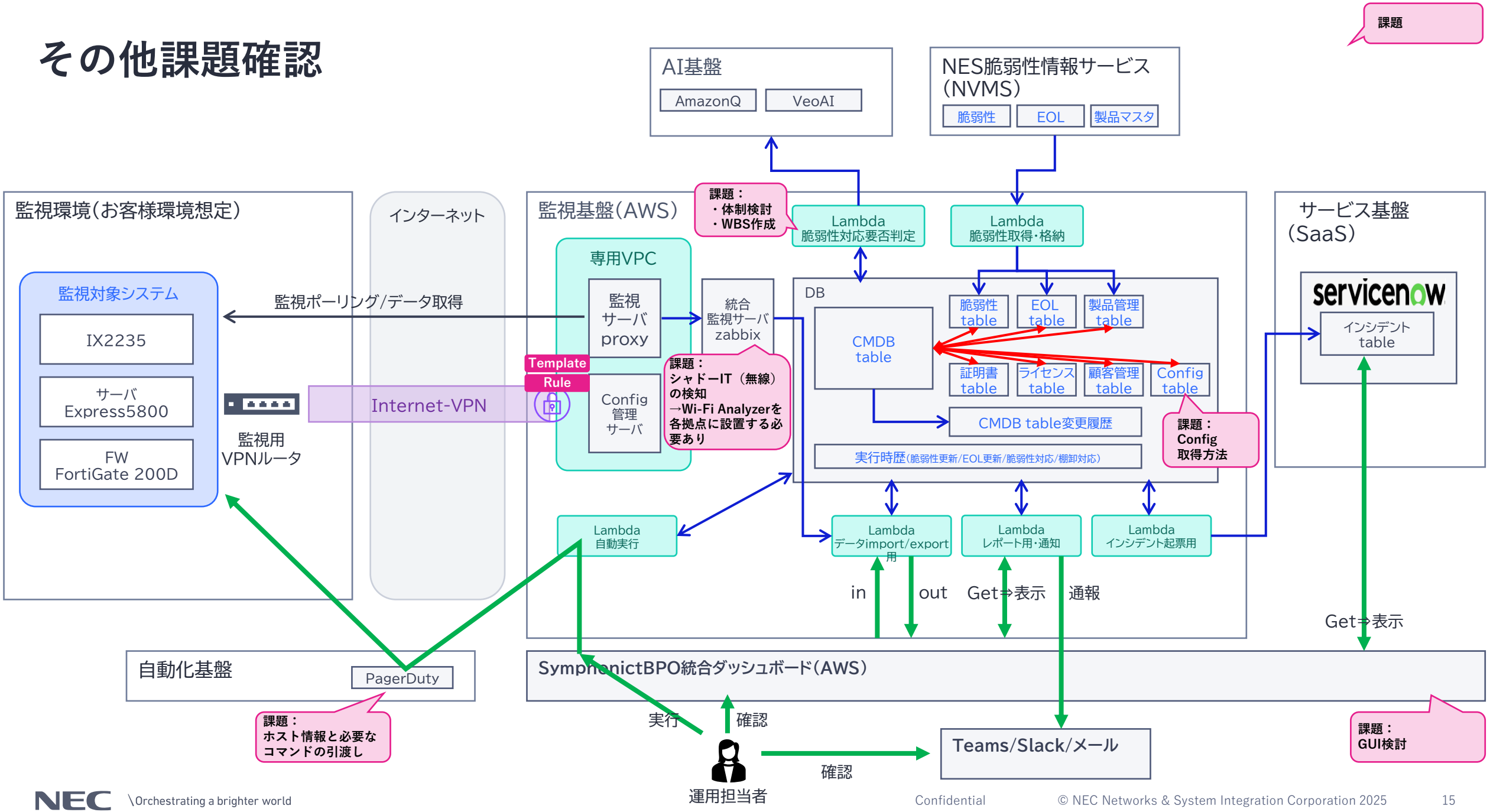
- **理由**

  現在、SSL VPNインターフェースが設定されており、有効な状態と判断されます。
  Fortinetの公式案内にある「SSL VPNの無効化」が暫定的な唯一の有効な対策となっており、現状の設定のままでは脆弱性に晒される状況です。

Appendix

その他課題

その他課題確認



明日のコミュニケーションをデザインする

　NECネッツエスアイは、お客様の目線に立った
これからのコミュニケーションをデザインする会社
としてお客様の価値向上に取り組んでまいります。

nesic　検索

\Orchestrating a brighter world

NECネッツエスアイ

※確認後、この注釈は削除してご使用ください。

このスライドはプレゼンテーションモード時に動画演出が付いたアニメーションエンドです。

- アニメーションエンドが不要な場合、当スライドは削除してください。
- アニメーション表紙（P.2）と併せて削除することでファイルの容量は軽くなります。
  ただし、これらは削除後の復元ができません。
  削除後に再度使用したい場合、改めて新規テンプレートから貼りつけてください。

NEC

\Orchestrating a brighter world