構成管理DBで脆弱性管理を見える化
ついでにサーバのパッチ適用も自動化してみた

2025/1/23（木） 10:15 – 11:00

日本電気株式会社
クラウド開発統括部
栗原大樹　松高直輝

構成管理DBで脆弱性管理を見える化
ついでにサーバのパッチ適用も自動化してみた

1. 自己紹介
2. はじめに
3. 事業紹介
4. 脆弱性対応の運用
5. サーバのパッチ適用自動化
6. まとめ
7. 議論したいこと

1. 自己紹介

自己紹介

- 名前
  - 栗原 大樹

- 経歴
  - 2022年　NEC入社（まだ3年目）

- 業務内容
  - NEC Cloud IaaS基盤サーバの開発保守
    - エンドユーザに係らない部分の
      基盤サーバを担当
    - （事実上のなんでも屋状態）

- 名前
  - 松高 直輝

- 経歴
  - 2018年　NEC入社（もう7年目）

- 業務内容
  - NEC Cloud IaaS ポータルサイトの開発保守
    - サービス企画・設計、脆弱性診断・ペネト
      レーションテスト等を担当

2. はじめに

はじめに

- 保守の役割はいろいろありますが、脆弱性対応はその中でも大切な1つ
  - ただし、保守する機器が多くなると負担が大きい
  - クリティカルな問題は即日対応、軽微な問題は優先度を落とす
    といったことをしないと人手が足りない。。。

→ いかに効率よく脆弱性情報を管理し、対処の運用をするかが重要!

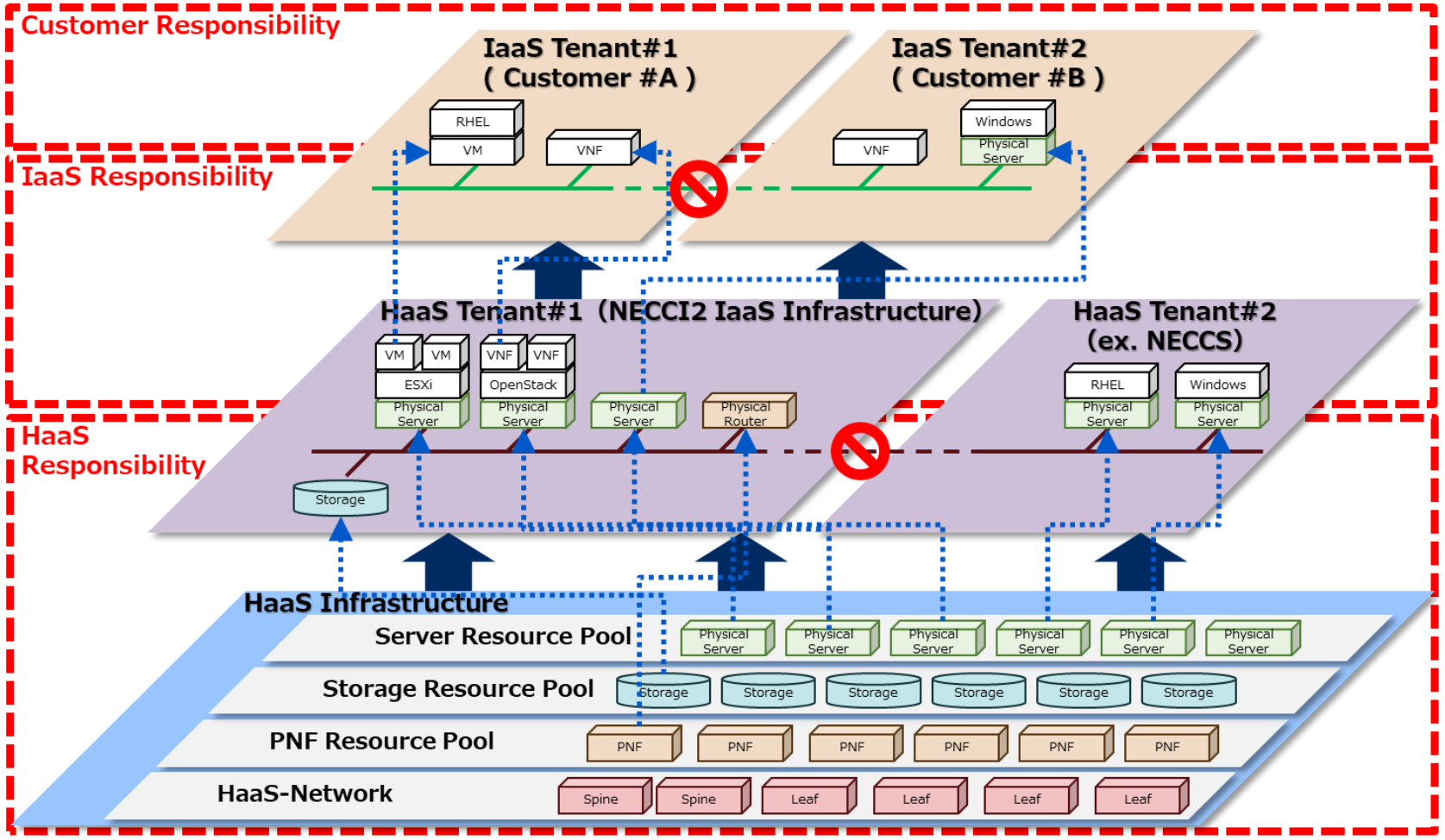
今回は、我々が脆弱性対応に対して
どのように運用を行っているのかをご紹介します。

(ついでに)基盤サーバの保守を担当している我々のチームが
脆弱性対応のパッチ適用を自動化した話も紹介

3. 事業紹介

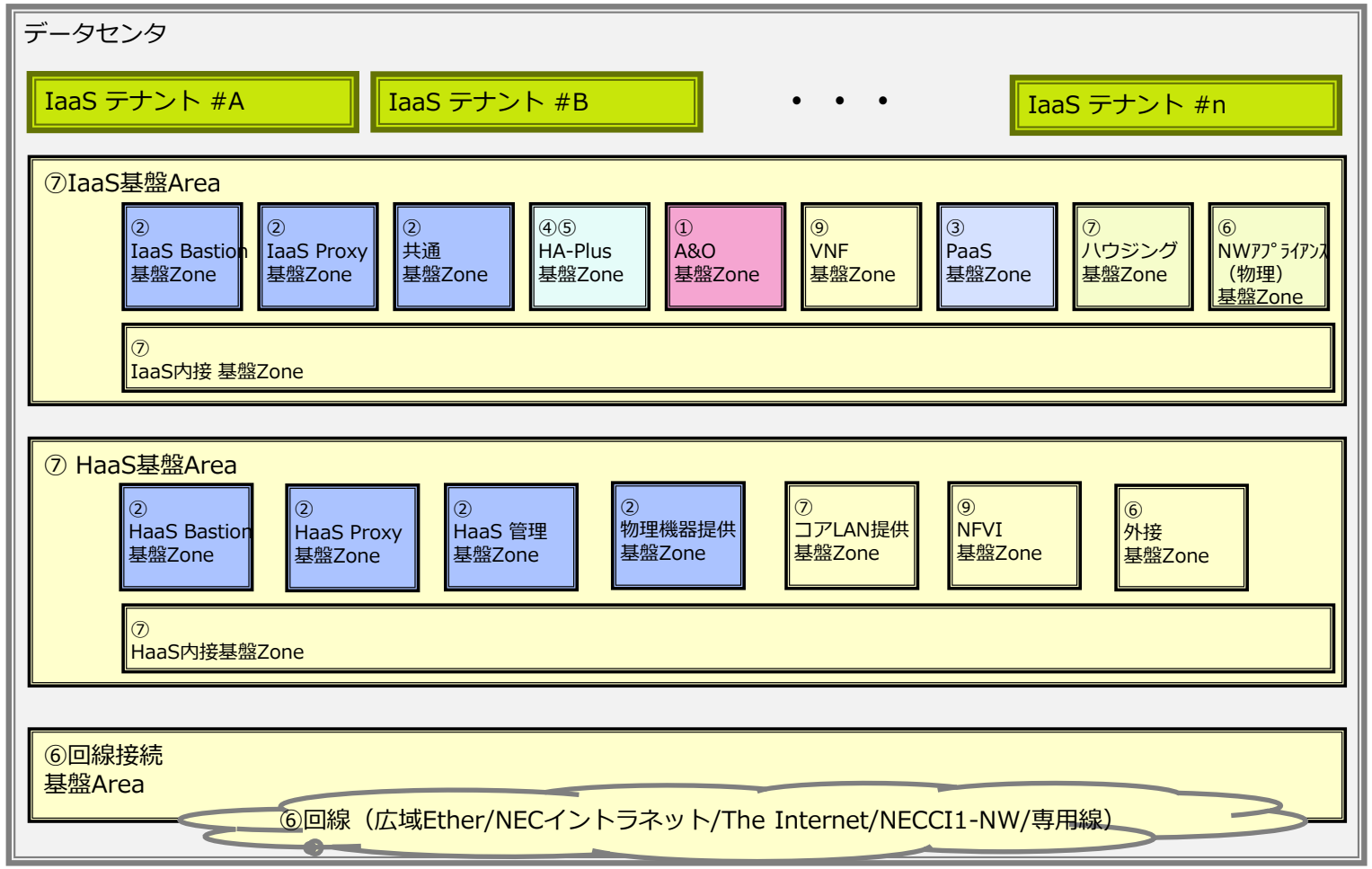
NEC Cloud IaaS

- 標準化されたHaaSの上でIaaSを提供
- サーバ/ネットワーク機器ともに約1000台で構成されているクラウド基盤



NEC Cloud IaaS

- 保守チームは機能別に10チーム以上



各チーム、脆弱性対応に毎日奮闘中。。。

①ポータル

②共通基盤 **③PaaS基盤**

④HA-plus (ストレージ) **⑤HA-plus (サーバ)**

⑥回線 (外部NW) **⑦基盤NW** **⑨NFVI**

他にも
- 監視
- 供給構築
- 物理サーバ

などの保守チームもあります

4. 脆弱性対応の運用

脆弱性対応の運用に関する背景

脆弱性診断も、パッチ適用も、ぜんぶ自動化して楽したい！

定期的に脆弱性の対処を求められるけど……。
他の業務が忙しくて、それどころじゃない！

脆弱性診断？
対象の機器が多いし、人手でやるのは無理だよ……

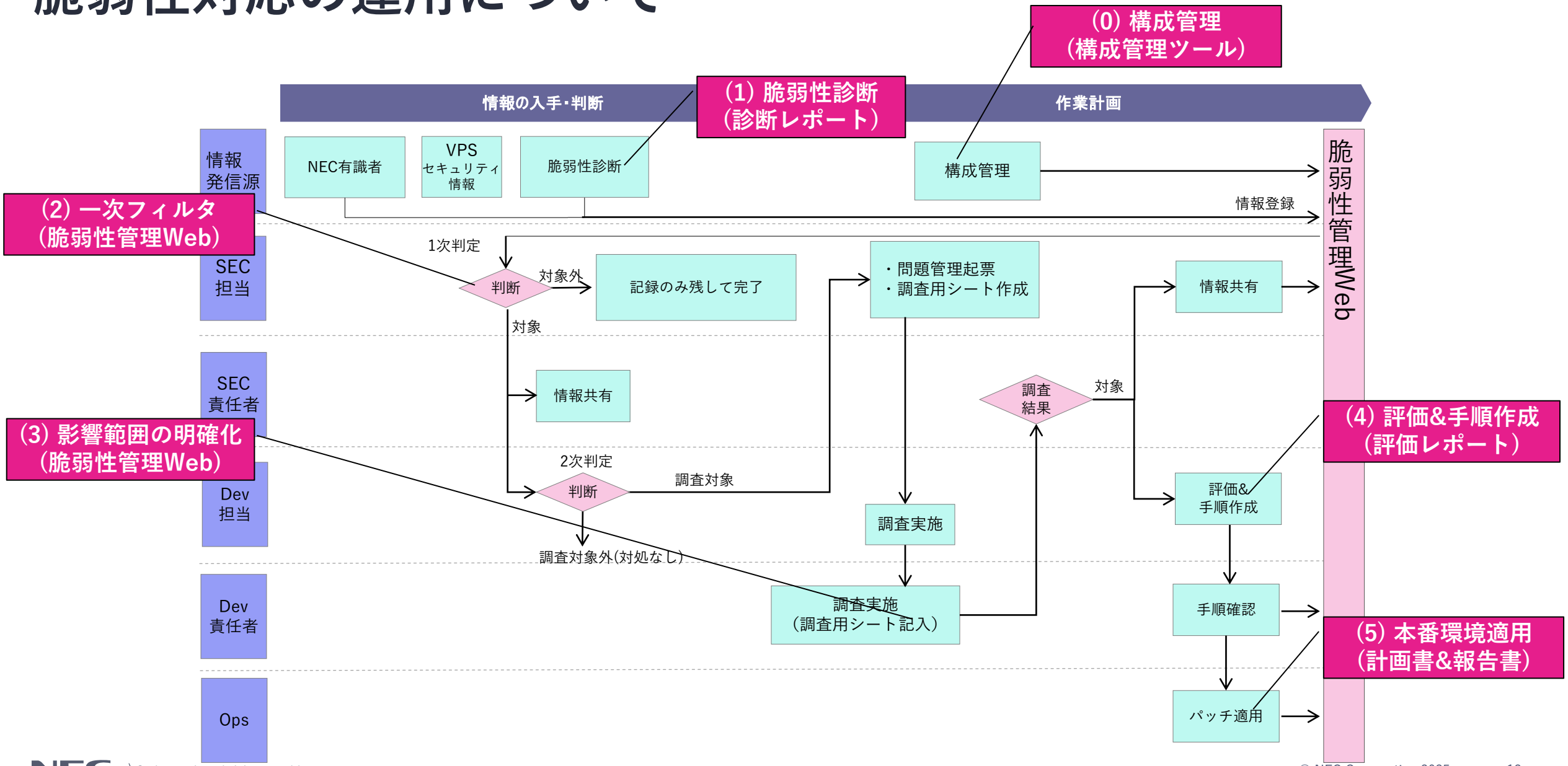
どこから脆弱性の情報を取ってくればいいの？
どうやって管理すればいいの？

脆弱性が有るのは分かったけど、どうやって対処すれば良いの？？

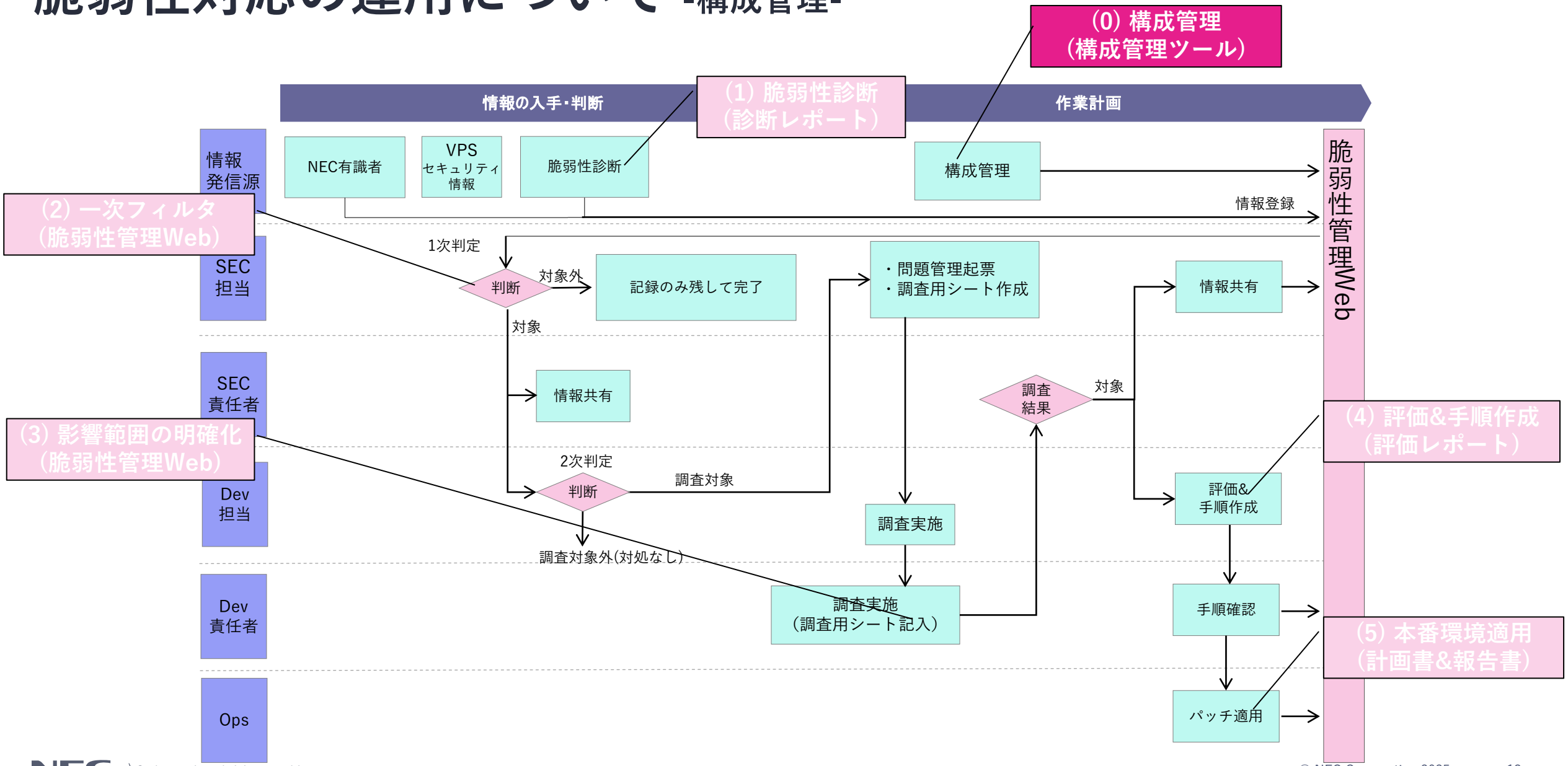
パッチ適用の手順書作って、レビューして、検証して、本番環境にリリースして……。
あぁ、めんどくさっ！

実際の現場の声

脆弱性対応の運用について



脆弱性対応の運用について -構成管理-



構成管理 -IPアドレス管理DB-

Id	address	prefix	base_id	pod	vlan_id	user	state	comment	init_date
1	10.40.62.0	24	34	WTE1	2024	IAAS	use	DMZ基盤Zone_SVmng	2024-01-01 12:00:00
2	10.40.66.0	24	34	WTE1	2025	IAAS	use	管理基盤Zone_SVmng	2024-01-01 12:00:00

セグメントテーブル
- セグメント
- プレフィックス
- vlan_id
- ステータス
- 用途

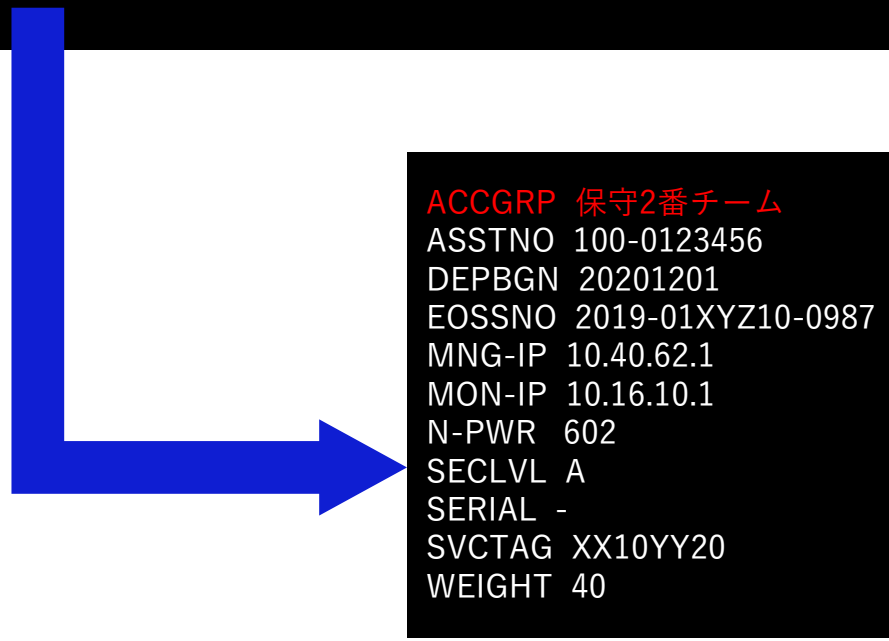
address	base_id	role	auto	user	state	hostname	comment	init_date
10.40.62.0	2024	network	0	EE	use			2024-01-01 12:00:00
10.40.62.1	2024	server	0	EE	use	sshgw001	sshgw1号機	2024-01-01 12:00:00
10.40.62.2	2024	server	0	EE	use	sshgw002	sshgw2号機	2024-01-01 12:00:00
10.40.62.3	2024	server	0	EE	use	VIP	sshgw_VIP	2024-01-01 12:00:00
10.40.62.4	2024	server	0	EE	no_use			2024-01-01 12:00:00

IPアドレステーブル
- IPアドレス
- 使用機器
- ステータス
- ホスト名
- 説明

構成管理 -構成情報管理DB-

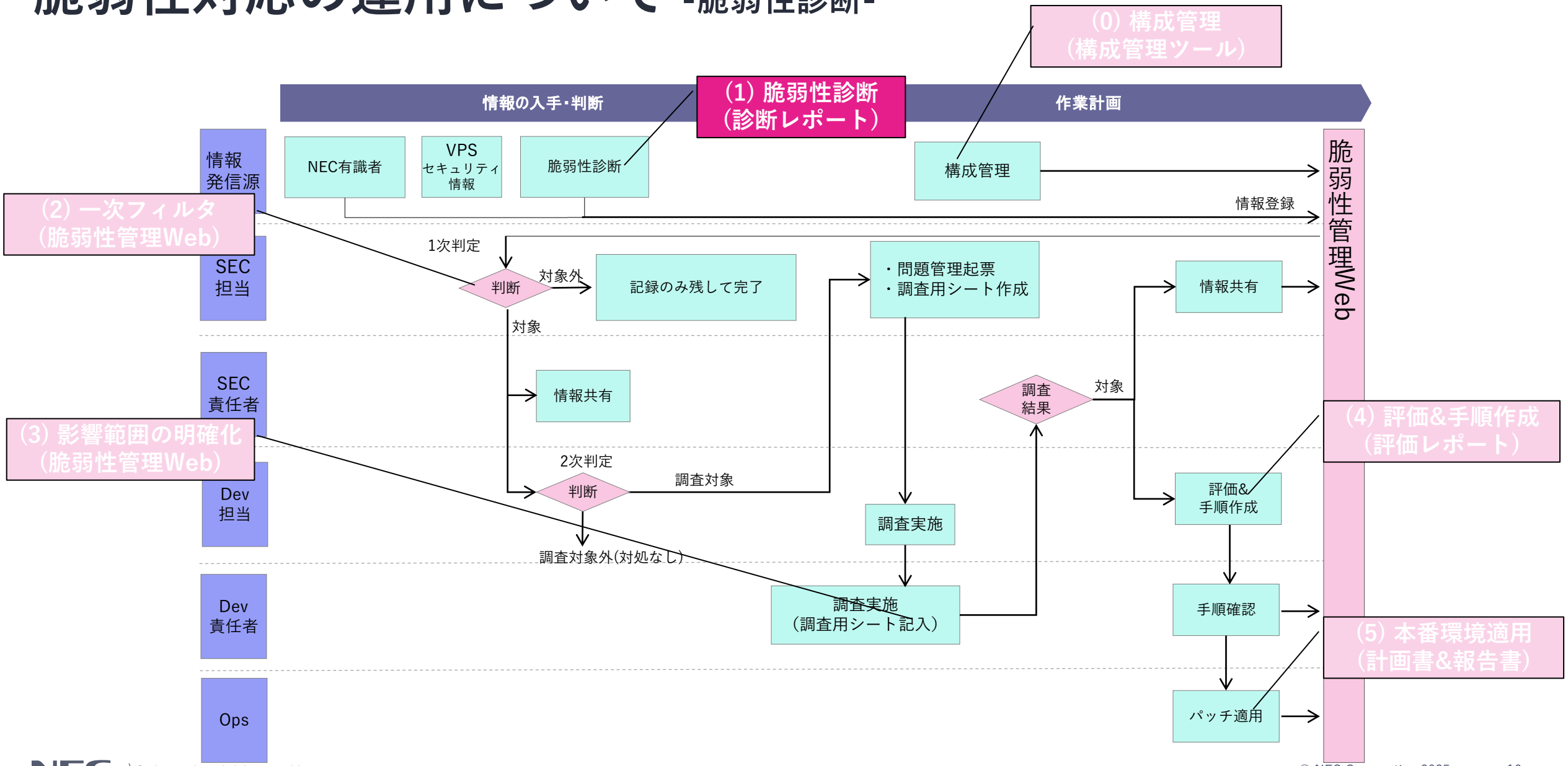
rscId	rscType	rscCode	ref	status	locationCode	rackId	fromUnitNo	toUnitNo	regDate
00010	SERVER	sshgw001	SSH-GWサーバ#01	30	100	00018	21	22	20240101
00011	SERVER	sshgw002	SSH-GWサーバ#02	30	100	00018	23	24	20240101
00012	SERVER	admsv001	管理サーバ#01	30	100	00019	15	16	20240101

リソーステーブル
- リソースID
- リソースタイプ
- サーバ名
- 説明文
- 現在の稼働ステータス
- 所在DC
- ラック番号
- ラック内位置
- 最終変更日



属性テーブル
- 管理チーム
- 資産管理番号
- 構築完了日
- 手配番号
- マネジメントIPアドレス
- モニタリングIPアドレス
- 定格電力量(VA)
- シリアルナンバー
- セキュリティレベル
- 重量(KG)

脆弱性対応の運用について -脆弱性診断-

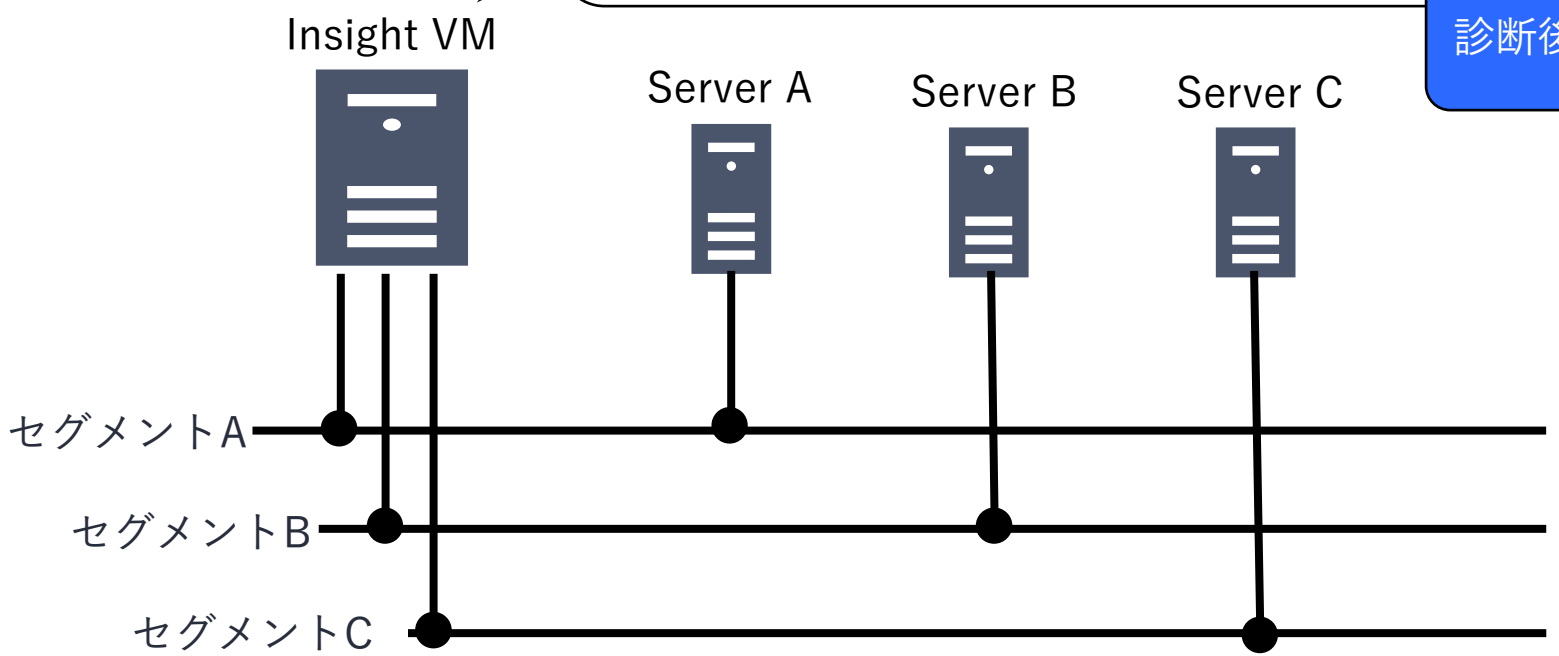


脆弱性診断 -脆弱性診断ツール-

- Insight VM（Rapid7社が提供する脆弱性情報の収集・管理ツール）を用いて月1で診断

診断内容
- ポートスキャンを実施し、開いているポートに対して詳細な診断を行う
- SSH接続し、利用しているパッケージ情報を取得することで詳細な診断を行う

診断後は、診断レポート（CSV、PDF）を出力



脆弱性診断 -診断レポート-

- Insight VMから出力される診断レポート(CSVファイル)は主に3つの情報が記載

1行ごとに1つの脆弱性が記載

①		②		③						
Site Name	Asset IP Address	Asset OS Name	Asset OS Versi	Service Name	Service Port	Service Protocol	Vulnerability CVE IDs	Vulnerability (	Vulnerability Title	Vulnerability CVE URLs
IaaS-Proxy	100.115.160.15	Red Hat Enterprise Linux	8.1	System	0	ip	CVE-2018-12699	7.5	Red Hat: CVE-2018-12699: binutils: heap-based buffer overflow in finish_st[illegible]stabs.c (Multiple Advisories)	http://nvd.nist.gov/vuln/detail/CVE-2018-12699
IaaS-Proxy	100.115.160.15	Red Hat Enterprise Linux	8.1	HTTP	80	tcp	CVE-2004-2320	5.8	HTTP TRACE Method Enabled	http://nvd.nist.gov/vuln/detail/CVE-2004-2320
IaaS-Bastion	100.120.80.245	F5 BIG-IP	16.1.3.4.0.0.2	System	0	ip	CVE-2024-45844	4.4	F5 Networks: CVE-2024-45844: K000140061: BIG-IP monitors vulnerability CVE-2024-45844	http://nvd.nist.gov/vuln/detail/CVE-2024-45844
IaaS-Bastion	100.120.80.245	F5 BIG-IP	16.1.3.4.0.0.2	System	0	ip	CVE-2024-41996	4.4	F5 Networks: CVE-2024-41996: K000148343: Diffie-Hellman key exchange protocol vulnerability CVE-2024-41996	http://nvd.nist.gov/vuln/detail/CVE-2024-41996

① 機器情報
- サイト名
- IPアドレス

② OS情報
- OS名
- OSバージョン

③ 脆弱性情報
- ポート・プロトコル
- CVE番号
- CVEスコア
- 脆弱性タイトル
- NIST URL

脆弱性診断 -診断レポート-

3.1.107. Red Hat: CVE-2024-52530: libsoup: HTTP request smuggling via stripping null bytes from the ends of header names (Multiple Advisories) (redhat_linux-cve-2024-52530)

説明：

GNOME libsoup before 3.6.0 allows HTTP request smuggling in some configurations because '\0' characters at the end of header names are ignored, i.e., a "Transfer-Encoding\0: chunked" header is treated the same as a "Transfer-Encoding: chunked" header.

影響を受けたノード：

影響を受けたノード：	追加情報：
100.112.160.5	Vulnerable OS: Red Hat Enterprise Linux 8.10 libsoup - version 2.62.3-5.el8 is installed

参照：

ソース	参照
NVD	CVE-2024-52530
REDHAT	RHSA-2024:9524
REDHAT	RHSA-2024:9559
REDHAT	RHSA-2024:9570
REDHAT	RHSA-2024:9572
REDHAT	RHSA-2024:9573

脆弱性の解決法：

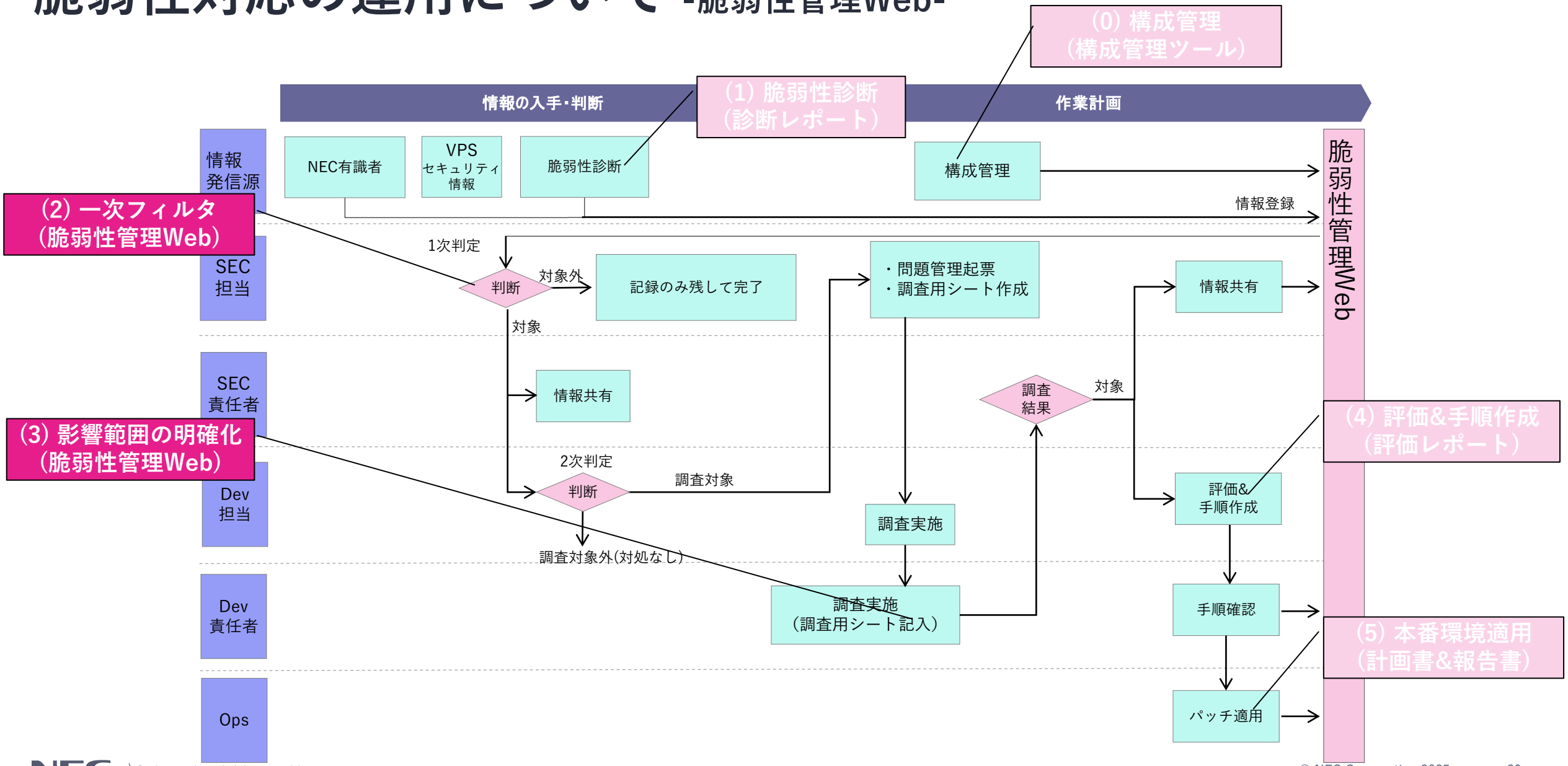
•libsoup on Red Hat Enterprise Linux

Upgrade libsoup

Update libsoup to the latest version available from Red Hat, using tools like yum or up2date.

- 発見された脆弱性については
  なぜ検知されたのかも追加情報欄に記載
  - 例えば
    - 検知されたパッケージのバージョン
    - インストールパス
    - Configの記載内容 等々

脆弱性対応の運用について -脆弱性管理Web-



脆弱性管理web

IPアドレスに対する脆弱性情報を記載

診断レポート

脆弱性情報がホスト名/管理チーム
と紐づけが出来る！

脆弱性管理webへ反映

構成管理DB

IPアドレス管理DB：IPアドレスとホスト名
構成情報管理DB　：ホスト名と管理チーム

NEC Cloud IaaS 2 ：脆弱性管理情報：2024年11月集計分

チーム番号	サービス種別	脆弱性件数	IP件数
1	[redacted]		
	rapid7_IaaS	6	6
	[redacted]		
	[redacted]		
	[redacted]		
2	[redacted]		
	[redacted]		
	[redacted]		
	rapid7_HaaS	179	242
	rapid7_IaaS	471	531
	[redacted]		
	[redacted]		
	[redacted]		

脆弱性管理web -トップページ-

NEC Cloud IaaS 2 ：脆弱性管理情報：2024年11月集計分

チーム番号	サービス種別	脆弱性件数	IP件数
1	[redacted]		
	rapid7_IaaS	6	6
	[redacted]		
	[redacted]		
	[redacted]		
2	[redacted]		
	[redacted]		
	[redacted]		
	rapid7_HaaS	179	242
	rapid7_IaaS	471	531
	[redacted]		
	[redacted]		
	[redacted]		

サービス種別の脆弱性一覧へ遷移
→次ページで説明

見える化！

保守チーム ＆ サービス種別単位で、
脆弱性の件数 と IPアドレス数を表示
→各保守チームがどのくらい脆弱性件数を
抱えているかを一目で分かるように！

脆弱性管理web –サービス種別での脆弱性一覧-

NEC Cloud IaaS 2 ：脆弱性管理情報：2024年11月集計分

チーム番号：2：rapid7_IaaS

項番	grp	サーバ用途	脆弱性件数	のべIP数	承認結果	承認者	承認日	コメント	指摘数
5	A	SSH-GW	12	36	承認				0
6	A	IaaS基盤Proxy/NTP/DNS/MTA	23	69	承認				0

サーバ用途の脆弱性一覧へ遷移
→次ページで説明

見える化！

サーバ用途単位で、脆弱性を表示

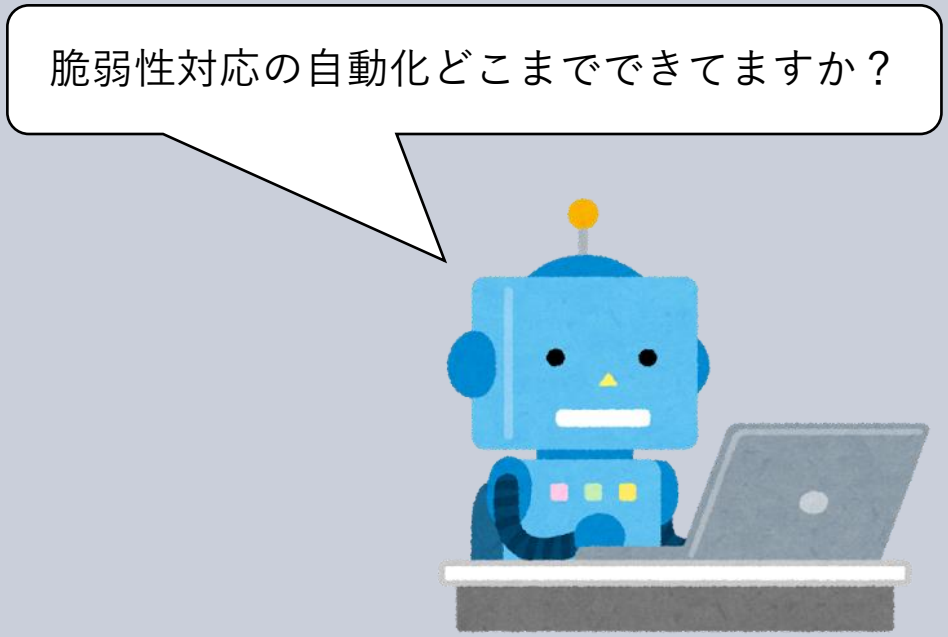
→サーバ用途ごとにどのくらい脆弱性件数を抱えているかを一目で分かるように！

ここで問題発生。。。

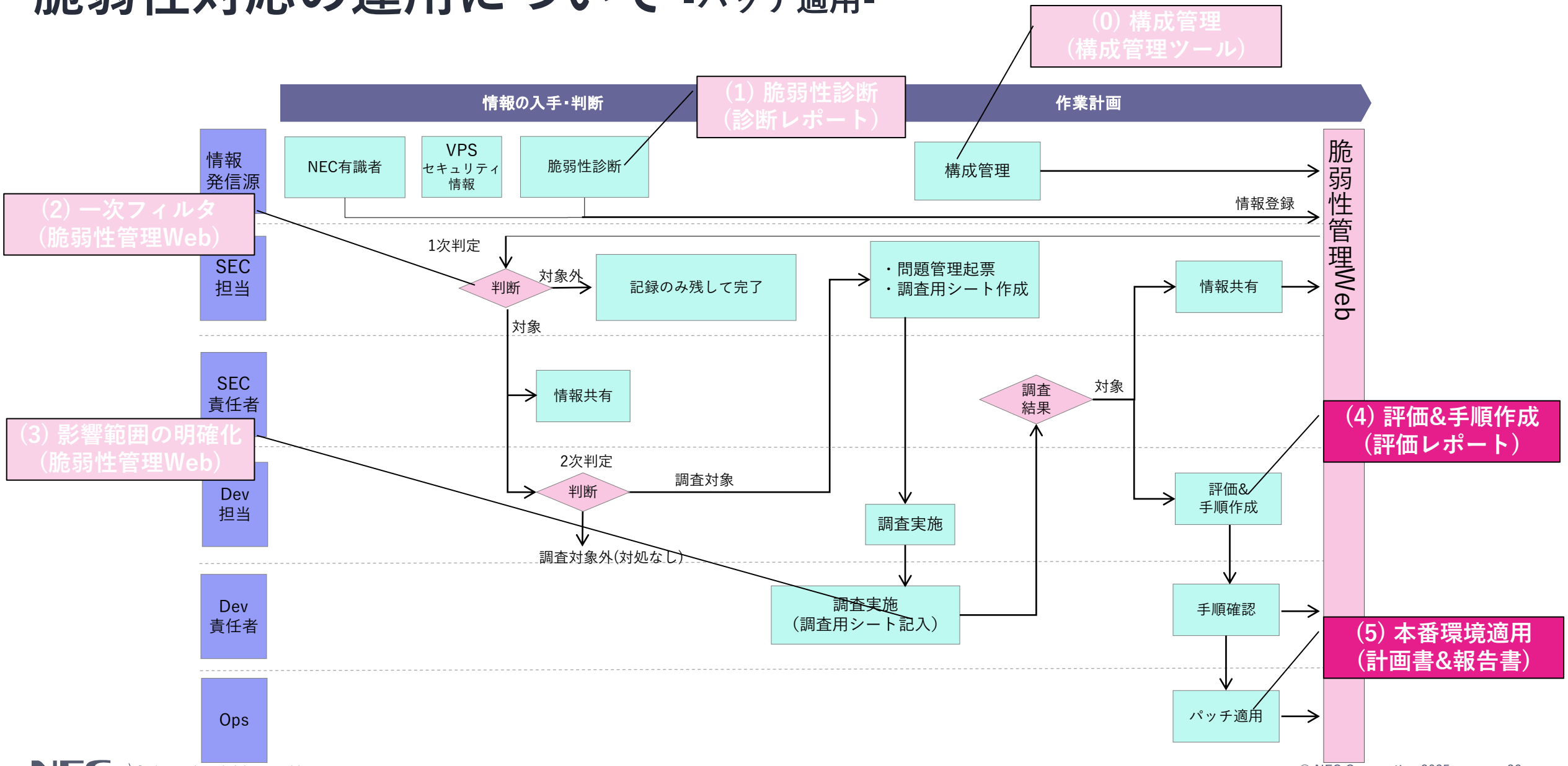
自動的に脆弱性診断・管理できるようになった！
だけど、脆弱性が多すぎて対処しきれない／(^o^)＼！！

実際の現場の声

5. サーバのパッチ適用自動化



脆弱性対応の運用について -パッチ適用-



パッケージ検索ツール

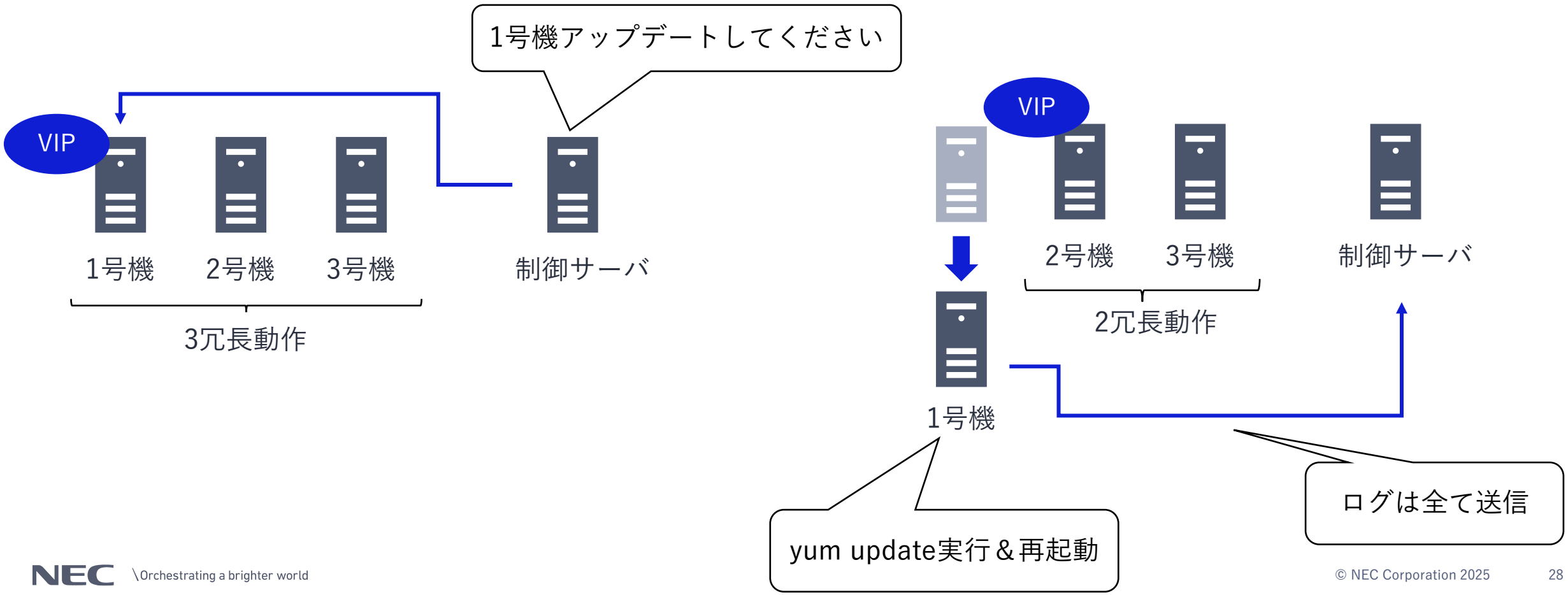
CVE ID	CVE-2024-52532 CVE-2024-525[illegible] CVE-2024-52530 CVE-2024-52530
脆弱性管理番号	vps0002005
脆弱性タイトル	【VDI-V2411-003562】Red Hat Enterprise Linux の libsoup における HTTP リクエストの隠蔽 などに関する脆弱性
Score	7.5

```
[neccirep@repoinfo]$ ./cve-repo-search.sh CVE-2024-52532

CVE URL : https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2024-52532.json

----------------------------------------
CVE no :
CVE-2024-52532

OS :
Red Hat Enterprise Linux 8

Package :
libsoup-2.62.3-6.el8_10

SnapshotDate,PackageName :
20241207,libsoup-2.62.3-6.el8_10.i686.rpm
20241207,libsoup-2.62.3-6.el8_10.x86_64.rpm
----------------------------------------
```

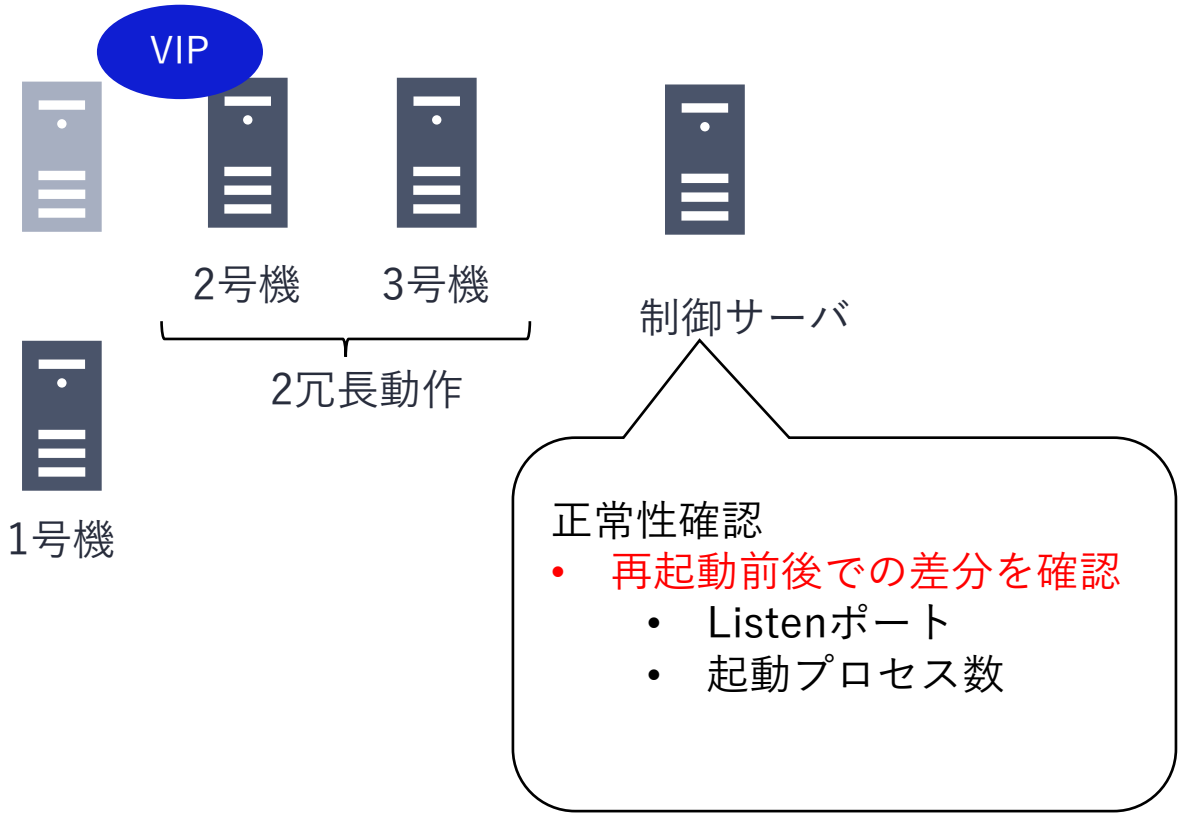
CVE番号からどのパッケージをパッチ適用する必要があるか検索可能

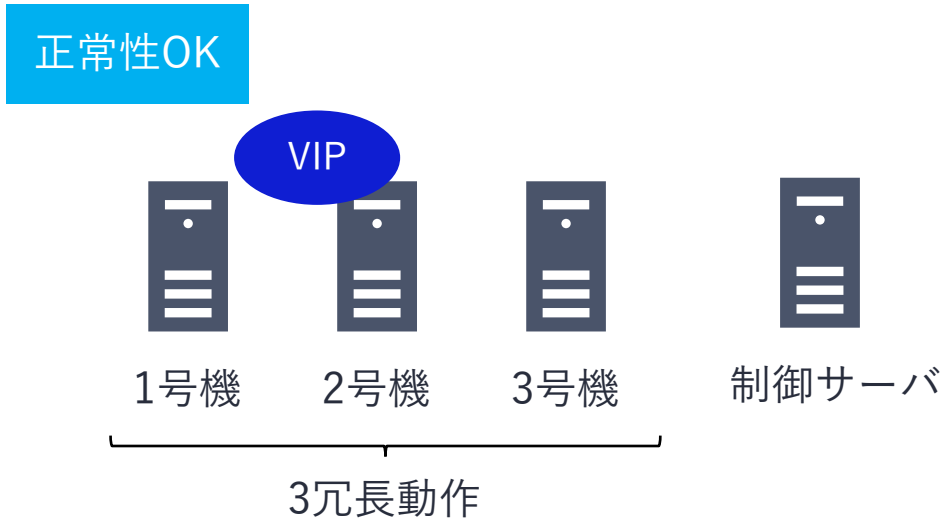
サーバのパッチ適用自動化

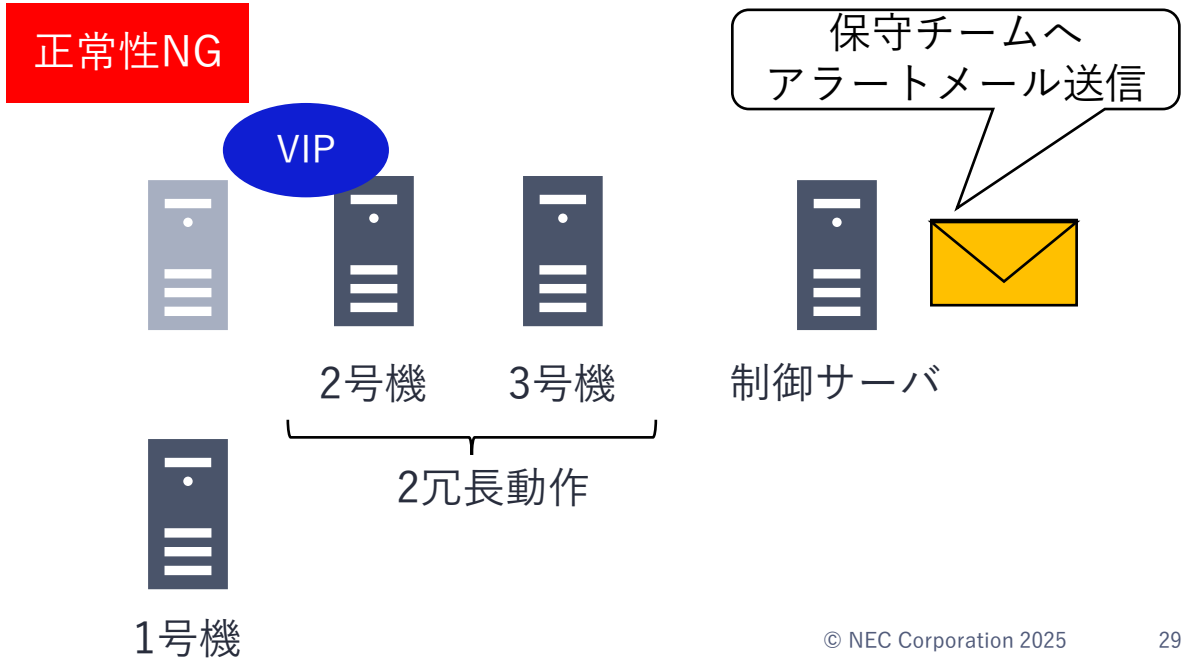
- 制御サーバからパッチ適用サーバへアップデート指令を出す
  - 夜中にスケジュールしておき自動でアップデート作業を順次実施



サーバのパッチ適用自動化







サーバのパッチ適用自動化

- 正常性NG の場合
  - 日中帯に保守チームが調査、切り戻し判断
    →事前に評価環境での適用、テスト済の状態ため
    本番環境適用時における大きな問題は今のところ起きていない

- 今までのパッチ適用作業は、
  - 自動化 → yum update 、再起動
  - 手動　 → 正常性確認(ログファイルを目視確認)
- 現在のパッチ適用作業は、
  - 自動化 → yum update 、再起動、正常性確認
  - 手動　 →正常性NGの場合の切り戻し判断

評価環境で1か月（約250台）、本番環境で1か月（約250台）掛けていた作業が
評価環境3日間、本番環境3日間、計6日間での実施は恩恵がかなり大きい。。。

6. まとめ

まとめ

- 運用が楽になるような脆弱性管理の仕組みをご紹介
  - 脆弱性管理webで月単位の脆弱性対応見える化を実現
    - 各保守チームの脆弱性対応状況が一目で分かるように！
    - （ただし、構成管理がきちんとされていることが前提）

- サーバのパッチ適用自動化の仕組みをご紹介
  - スケジュールしておけば、勝手に夜中にパッチ適用
  - yum update→再起動→正常性確認までを完全自動化
    - 朝起きたらパッチが適用されている状態に！

（裏）まとめ　というより現状の問題点

脆弱性管理webで情報を管理！パッチ当ても自動化！！とても幸せの世界！！！

のように見えるますが実態は。。。

- 構成管理DBへの登録誤りによる、この脆弱性抱えている機器は誰のモノ。。。？
  →頭を悩ます迷子の存在

- insightVMで検知される脆弱性は減る気配はない。。。
  - 保守責任者から自動化したのに減らないのなんで？って日々詰められてます★
    →担当機器が多いから数が多く見えるだけです（必死の言い訳。。。）

- そもそもinsightVMの誤検知もあるじゃん。。。
  →なぜかパッチ当てているのに消えない脆弱性情報。。。

7. 議論したいこと

議論したいこと

- 脆弱性対応の運用どうしていますか？

- 脆弱性対応管理ツール、何を使用していますか？
  - Rapid7 Insight VMはコンテナ内のパッケージはスキャン不可
  - 現在はNEC独自のベンダ情報管理DBでカバー
  - コンテナ内もスキャンできるツールがあればご紹介ください

- サーバ、ネットワーク機器のパッチ当てどうしていますか？

- 脆弱性対応の自動化どこまでできてますか？

\Orchestrating a brighter world