\Orchestrating a brighter world NEC

Hardening Designers Conference 2023
「濃厚なサイバーセキュリティ最前線:攻撃手法の解析とAnsibleによる堅牢化の自動化」

Ansible Playbookによるログ設定の自動化

2023年5月20日

NEC　サイバーセキュリティ戦略統括部　セキュリティ技術センター
実装技術アーキテクチャグループ

© NEC Corporation 2023

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

目次

1. CIS Benchmarksの紹介
2. CIS Benchmarksに基づいた堅牢化
3. Ansible Playbookを利用した自動化

CIS Benchmarksの紹介

堅牢化が大切といわれても

色々な**課題**がある

どうやって**設定**すればよいか**分からない**

組織内の詳しい人に**属人化**している

そこで！

具体的に、どう堅牢化をすればよいのか
NECで実践している一手段をご紹介します

© NEC Corporation 2023

要塞化ツール

NEC社内で使用している自動堅牢化ツール
サーバやクライアントのセキュアな設定を自動適用

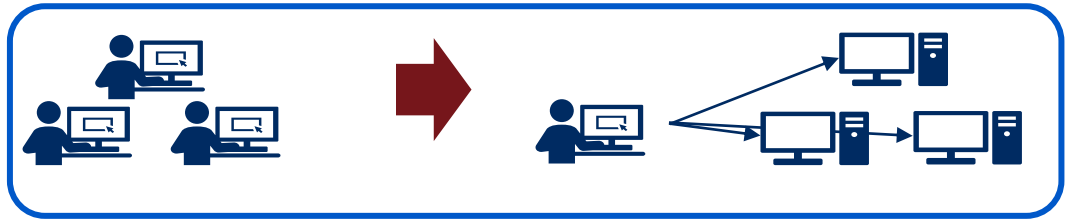
概要

- 堅牢化を自動化
- 業界のベストプラクティスである CIS Benchmarksに基づいた設定
- Ansibleを活用することでエージェントレスで設定可能

メリット

- 個人スキルに依存せず、誰でも高度なセキュアな設定が可能
- 自動化による工数削減と人的なミス防止
- 台数が増えても一律の管理が可能
- 要件に合わせたカスタマイズ性

ガイドを見ながら
手動で設定していたのが…



1コマンドで全てのサーバに
自動設定が可能に！

© NEC Corporation 2023

そもそも堅牢化(要塞化)とは？

サーバやPCのセキュリティを高めること

不要なサービスの停止
不要なファイルやプログラムの削除

適切なパスワードポリシー

最新のセキュリティパッチ適用

etc..

具体的には

・パスワード: 4文字以上
・ログイン試行回数: 制限なし

- パスワード: 記号、大文字、小文字、数字を各一つ以上含む14文字以上
- ログイン試行回数: 5回連続でログインに失敗した場合、900秒間アカウントをロック

© NEC Corporation 2023

オフライン環境では堅牢化はいらない？

オフラインのシステムであっても様々な脅威にさらされている

脅威が侵入する経路は数多くある

- USBメモリなどを介して侵入
- 従業員の機器の持ち込み
- 実は一部の機器がWi-Fiと接続
- 専用回線で保守業者が接続
- オンラインのシステムと接続可能

横展開による組織内外への被害拡大も考えられるので堅牢化は必須

© NEC Corporation 2023

堅牢化のベストプラクティス集

セキュリティを考慮した詳細な設定が記載してあり、対象OS、ミドルウェアが豊富なCIS Benchmarks

CIS(Center of Internet Security)
※複数の米国政府機関が、企業や学術機関などと連携してセキュリティ標準化に取り組む非営利団体

↓ 発行

CIS Benchmarks

OS/MW等の設定ベストプラクティス

メリット

- 設定が具体的
- 世界的に認められている

CIS Benchmarksとは

Center for Internet Security(CIS)という機関が発行するOS/MW等の設定ベストプラクティス

- 主要なOS,ミドルウェア, ネットワーク製品, クラウド環境について、各バージョンごとのセキュリティ設定(対策内容、対象、詳細、実施方法)が詳細に記載されている
- 対象分野の専門家、テクノロジーベンダー、公的および民間のコミュニティメンバー、およびCISベンチマーク開発チームの寛大なボランティア活動を通じて開発されている
- IPAの「セキュリティ仕様策定プロセス」において、「ユーザ・ベンダー間のリスクコミュニケーションにおいて参照することが望ましい資料」として挙げられている。また、Microsoft、AWSなどではセキュリティのレギュレーションとして紹介されている

© NEC Corporation 2023

CIS Benchmarksの入手方法

CIS WorkBench（CISのコミュニティサイト）で入手可能

https://workbench.cisecurity.org/

© NEC Corporation 2023

CIS Benchmarks章構成の例

Windows Server2019 RTM

1.アカウントポリシー
- 1.1 パスワードポリシー
- 1.2 アカウントロックアウトポリシー

2.ローカルポリシー
- 2.2 ユーザ権限の割り当て
- 2.3 セキュリティオプション

9.セキュリティが強化されたWindowsファイアウォール
- 9.1 ドメインプロファイル
- 9.2 プライベートプロファイル
- 9.3 パブリックプロファイル

17. 高度な監査ポリシーの設定
- 17.1 アカウントログオン
- 17.2 アカウントマネジメント
- 17.3 詳細な追跡
- 17.4 DSアクセス
- 17.5 ログオン/ログオフ
- 17.6 オブジェクトアクセス
- 17.7 ポリシーの変更
- 17.8 特権の使用
- 17.9 システム

18.管理用テンプレート(コンピュータ)
- 18.1 コントロールパネル
- 18.2 LAPS
- 18.3 MSセキュリティガイド
- 18.4 MSS(Legacy)
- 18.5 ネットワーク
- 18.7 スタートメニューとタスクバー
- 18.8 システム
- 18.9 Windowsコンポーネント

19.管理用テンプレート(ユーザ)
- 19.1 コントロールパネル
- 19.5 スタートメニューとタスクバー
- 19.6 システム
- 19.7 Windowsコンポーネント

※ 一部番号が飛んでいるのは過去版と構成の一貫性を保つため

© NEC Corporation 2023

CIS Benchmarksの項目例

1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)

項目名

Profile Applicability:

項目の適用対象

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

詳細

This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does thi
of minutes a locked out account will remain unavailable. If the v
is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them.

Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer.

The recommended state for this setting is: `15 or more minute(s)`.

Rationale:

根拠

A denial of service (DoS) condition can be created if an attacker abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once you configure the Account lockout threshold setting, the account will be locked out after the specified number of failed attempts. If you configure the Account lockout duration setting to 0, then the account will remain locked out until an administrator unlocks it manually.

Audit:

設定の確認方法

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

設定方法

To establish the recommended configuration via GP, set the following UI path to `15 or more minute(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration
```

Impact:

影響

Although it may seem like a good idea to configure this policy setting to never automatically unlock an account, such a configuration can increase the number of requests that your organization's help desk receives to unlock accounts that were locked by mistake.

Default Value:

デフォルト値

None, because this policy setting only has meaning when an Account lockout threshold is specified. When an Account lockout threshold is configured, Windows automatically suggests a value of 30 minutes.

References:

参照

1. CCE-37034-6

CIS Controls:

CIS Controlsとのマッピング

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

16.7 Configure Account Lockouts
Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

CIS Benchmarksに基づいた堅牢化

CIS Benchmarksによるログ設定

ログ設定が25項目以上存在

ログ設定例

ログインイベントの監査 **成功時（デフォルト値） →成功時と失敗時**	共有フォルダへのアクセス施行 **監査なし →成功時と失敗時**	共有フォルダ上ファイルへのアクセス施行 **監査なし →失敗時を含める**
ユーザアカウントの管理 **成功時 →成功時と失敗時**	リムーバブル記憶域の監査 **監査なし →成功時と失敗時**	重要な特権の使用 **監査なし →成功時と失敗時**

© NEC Corporation 2023

ログ解析テクニックセッションで登場したIR対応の設定

ローテーションや時刻に関する項目も存在

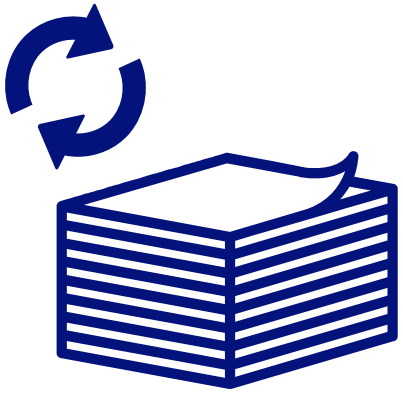
ログローテーションに関する項目

ログファイルの最大サイズ指定

なし(20,489KB)
→32,768KB以上

最大サイズ到達時にログを停止

無効
→無効(デフォルト値通り)



時刻に関する項目

システム時刻の変更権限(DC)

Administrators, Server Operators, LOCAL SERVICE
→Administrators, LOCAL SERVICE

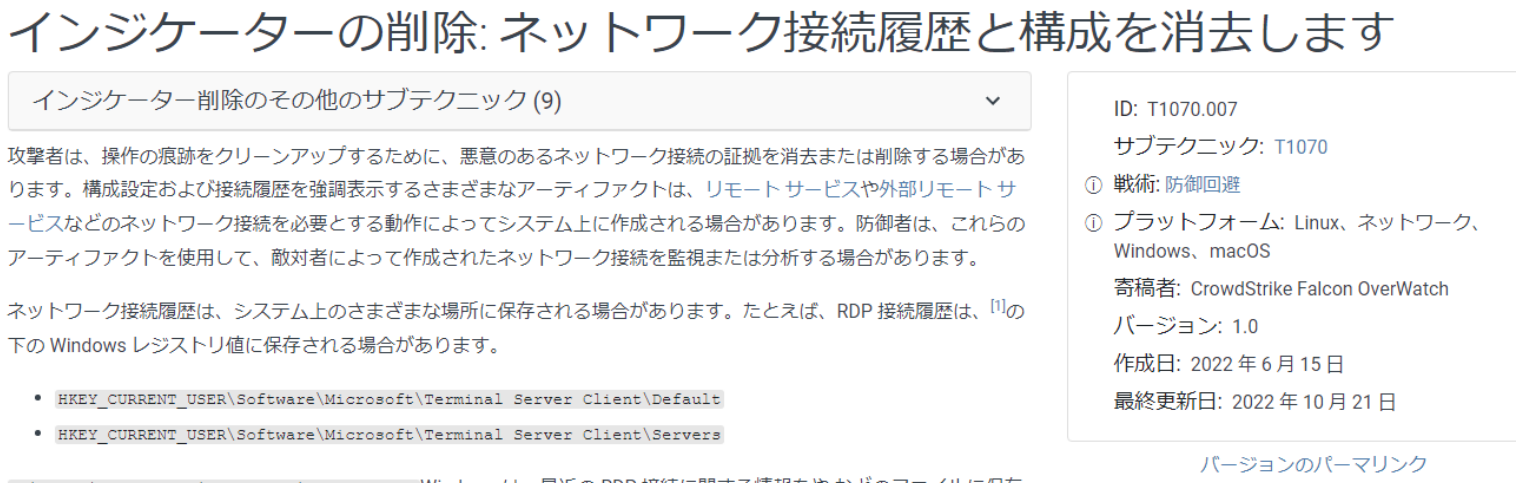
タイムゾーンの変更権限

→Administrators, LOCAL SERVICE
(デフォルト値通り)

© NEC Corporation 2023

MITREセッションで登場したテクニックの緩和策(一例)

レジストリ値に保存されているネットワーク接続履歴等を消去するテクニックは CIS Benchmarksに沿った設定が緩和策に



インジケーターの削除: ネットワーク接続履歴と構成を消去します

インジケーター削除のその他のサブテクニック (9)

攻撃者は、操作の痕跡をクリーンアップするために、悪意のあるネットワーク接続の証拠を消去または削除する場合があります。構成設定および接続履歴を強調表示するさまざまなアーティファクトは、リモート サービスや外部リモート サービスなどのネットワーク接続を必要とする動作によってシステム上に作成される場合があります。防御者は、これらのアーティファクトを使用して、敵対者によって作成されたネットワーク接続を監視または分析する場合があります。

ネットワーク接続履歴は、システム上のさまざまな場所に保存される場合があります。たとえば、RDP 接続履歴は、[1]の下の Windows レジストリ値に保存される場合があります。

- `HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default`
- `HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers`

`C:\Users\%username%\Documents\Default.rdp` Windows は、最近の RDP 接続に関する情報をや などのファイルに保存する場合があります。`C:\Users\...\AppData\Local\Microsoft\TerminalServer Client\Cache\`。[2]同様に、...する情報をシステム ログ (`/Library/Logs`や に保存されます など `/var/log/`) に保存する場合があります。[3] [4] [5]

...ファイアウォールの無効化または変更、またはプロキシを有効にする改ざんなど、ネットワーク構成設定の変更が必要になる場合もあります。敵対者は、指標を隠蔽したり防御分析を妨害したりするために、このデータを削除または変更する可能性があります。

ID: T1070.007
サブテクニック: T1070
戦術: 防御回避
プラットフォーム: Linux、ネットワーク、Windows、macOS
寄稿者: CrowdStrike Falcon OverWatch
バージョン: 1.0
作成日: 2022 年 6 月 15 日
最終更新日: 2022 年 10 月 21 日

バージョンのパーマリンク

リモートからアクセス可能な レジストリパスを制限

- ネットワーク接続履歴情報が格納されている レジストリへのアクセスを制限

「ファイルとその他のオブジェクトの所有権」の取得を制限

- この所有権は、アクセス権に関係なくレジストリキー等の所有権を得られる権利
- 管理者のみに付与させることで悪用を制限

© NEC Corporation 2023

その他堅牢化項目の例

様々な角度から網羅的に堅牢化が可能

設定可能な パスワードの長さ **7文字（デフォルト値）** **→14文字**	ロックアウトされるまでの ログイン試行回数 **0回（ロックアウトなし）** **→10回以下**	Administratorの アカウント名を変更 **Administrator** **→ リネーム**
添付やDLファイルを開く際、 アンチウイルスプログラムに通知 **無効** **→有効**	サービスとしてログイン不可な アカウントにGuestsを追加 **No one** **→Guests**	RDP接続時、 毎回パスワードを要求 **Disabled** **→Enabled**

© NEC Corporation 2023

Ansible Playbookを利用した自動化

CIS Benchmarksによる堅牢化の課題

設定項目が膨大

Windows Server 2019
の場合300項目以上

設定ミスの発生

サーバ1台につき300項目
サーバが5台10台となると…

文章が全て英語

Windows Server 2019
の場合900ページ以上

© NEC Corporation 2023

要塞化ツール(再掲)

NEC社内ではCIS Benchmarkに基づいた堅牢化を自動化するツールを開発
システム開発時に活用

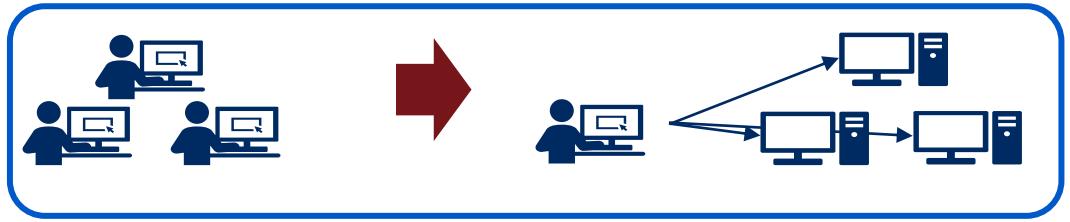
概要

- 堅牢化を自動化
- 業界のベストプラクティスである CIS Benchmarksに基づいた設定
- Ansibleを活用することでエージェントレスで設定可能

自動化のメリット

- 個人スキルに依存せず、誰でも高度なセキュアな設定が可能
- 自動化による工数削減と人的なミス防止
- 台数が増えても一律の管理が可能
- 要件に合わせたカスタマイズ性

ガイドを見ながら
手動で設定していたのが…



1コマンドで全てのサーバに
自動設定が可能に！

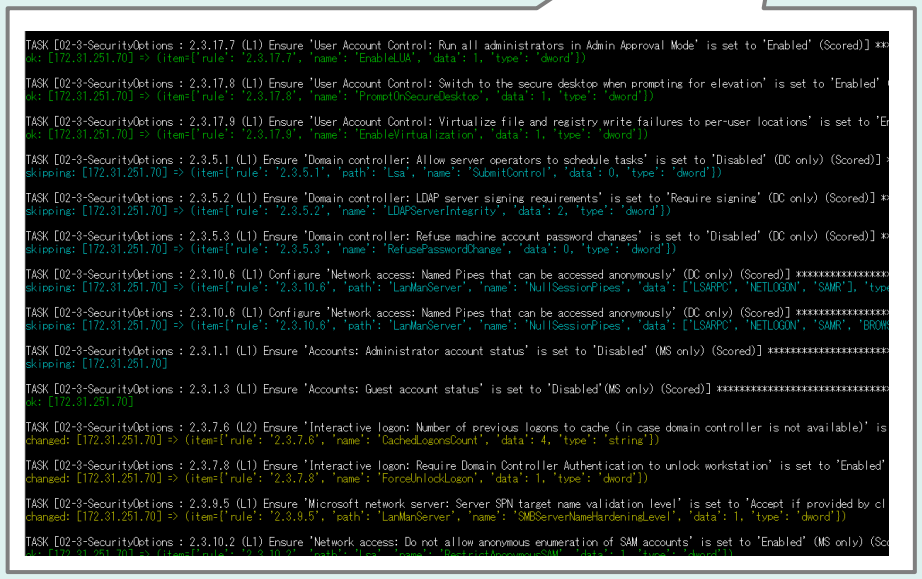
© NEC Corporation 2023

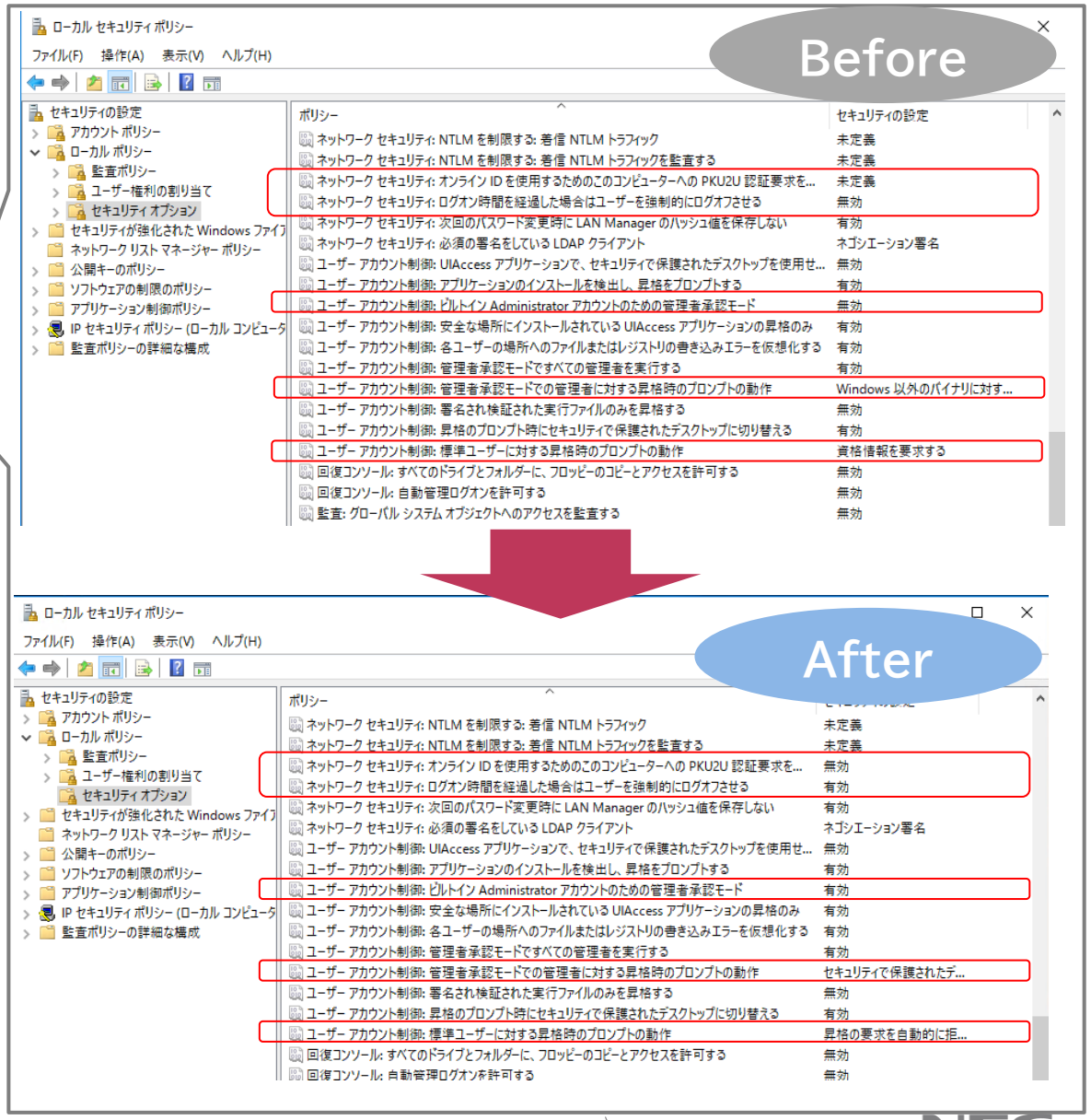
自動化のイメージ

自動化ツール

設定対象
マシン

SSH or
WinRM

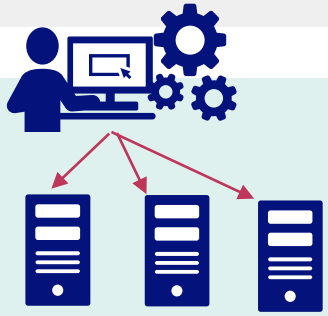




© NEC Corporation 2023

自動化のための構成管理ツール

サーバ構成管理ツールAnsibleを活用



構成管理ツール

- サーバの構築、設定などを
  コードで定義して管理するツール
  （Infrastructure as Code）

- サーバのセットアップを自動化
- 複数台のサーバの構築や設定を一度に
  実行可能

構成管理ツールの選定

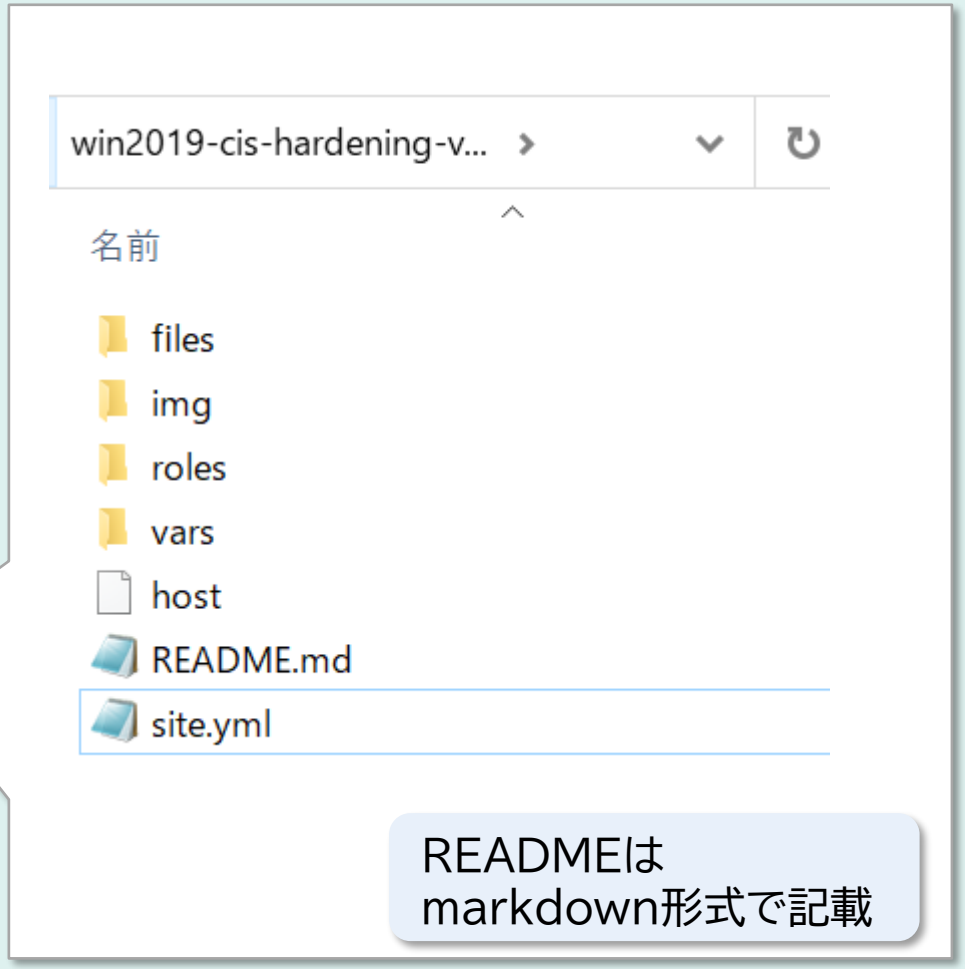
- Chef
  - マスターとエージェントによって構成
  - 設定をRuby DSLで記載
- Puppet
  - マスターとエージェントによって構成
  - Puppet DSLという独自DSLで記載
- Ansible
  - エージェントレス、SSH(もしくは
    WinRM)で接続して設定反映
  - 設定をYAMLで記載

採用

© NEC Corporation 2023

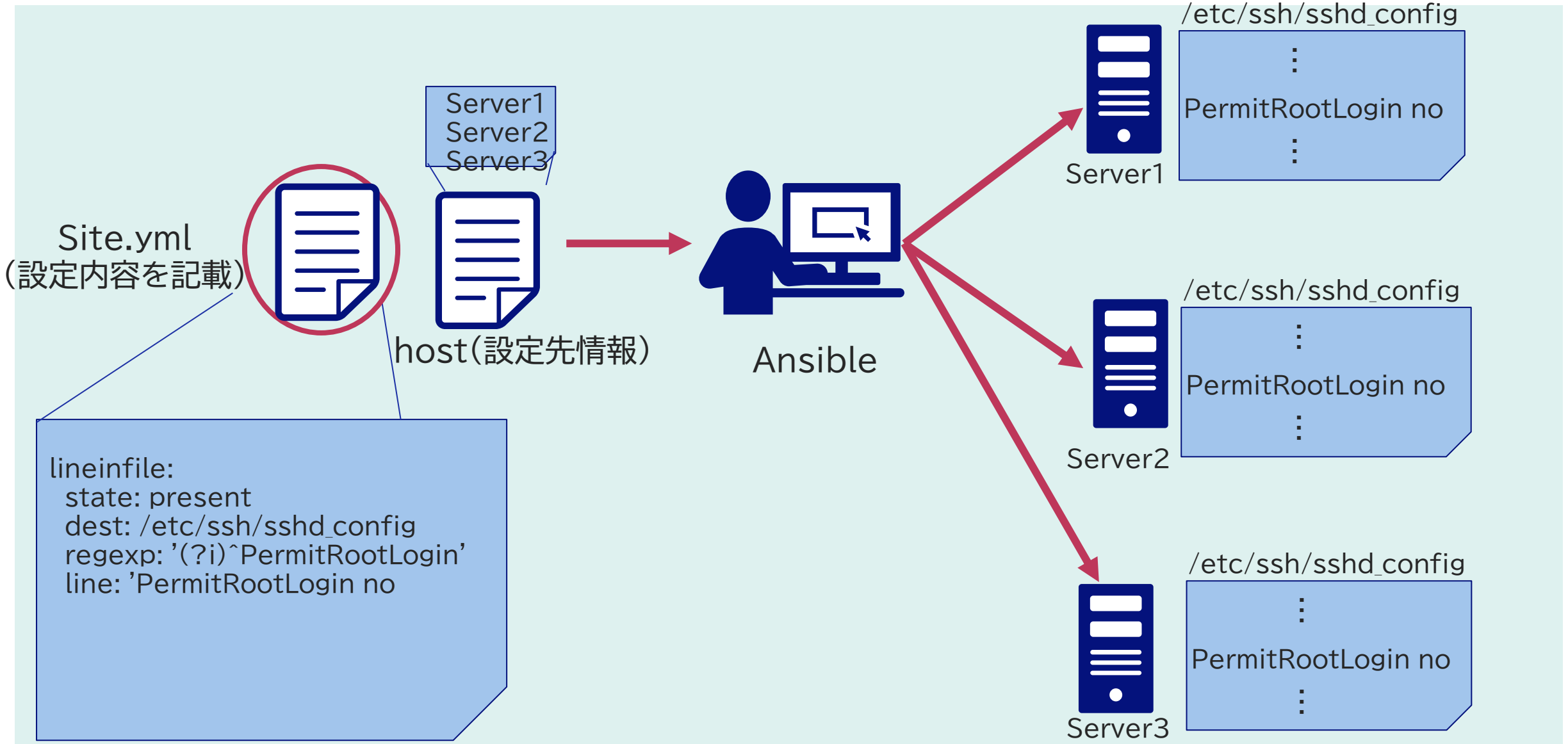
自動化ツールの構成例

- 各ディレクトリの内容
  - **filesディレクトリ**
    playbook実行時に利用されるファイルを格納
  - **imgディレクトリ**
    README内で参照している画像を配置
  - **rolesディレクトリ**
    CIS Benchmarksの各章の設定を記載
  - **vars/vars.yml**
    ユーザごとに異なる値を設定する必要のある章について、その設定値を記載するファイル
    例：パスワードの長さ・有効期限、等
  - **host**
    実行先のIPやクレデンシャル等を記載
  - **README.md**
    各要塞化ツールの説明書
  - **site.yml(Playbook)**
    ツールの本体。このファイルに従って設定が実行される



© NEC Corporation 2023

自動化ツールの動作イメージ



© NEC Corporation 2023

site.yml(流し込む設定内容を記載するファイル)

保守性や可視性を考慮し、
設定や変数が格納されているディレクトリを指定するのみ

site.yml - メモ帳

ファイル(F)　編集(E)　書式(O)　表示(V)　ヘルプ(H)

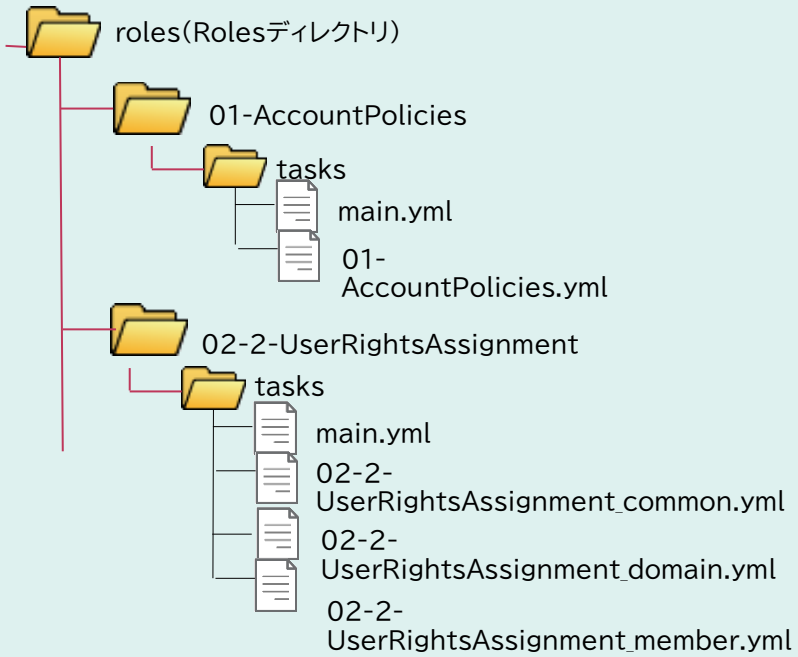
```
---
- name: CIS Microsoft Windows Server 2019 RTM (Release 1809) Benchmark
  hosts: windows
  vars_files:
    - ./vars/vars.yml
  roles:
    - 01-AccountPolicies
    - 02-LocalPolicies
    - 09-WindowsFirewallwithAdvancedSecurity
    - 17-AdvancedAuditPolicyConfiguration
    - 18-AdministrativeTemplates
    - 19-AdministrativeTemplates
```


© NEC Corporation 2023

rolesディレクトリ(設定ファイルが配置)

CIS Benchmarksの章やセクションに準じたディレクトリ構成

ファイル名
CISベンチマークの各セクションの名称



各章のファイルの構成
name:CIS Benchmarksの項目名
win_security_policy:
設定するセキュリティポリシーの場所、設定値を記載
tags: 任意に設定可能なタグ。
タグを指定して実行する項目を絞りこめる

NECでは下記のタグを作成
・該当のセクション番号
・Score
・レベル(CISベンチマークのレベル付け)
・役割等の分類
例:ドメインコントローラ or メンバサーバ
level[1 or 2]-domain_controller
level[1 or 2]-member_server

01-AccountPolicies.yml 3.13 KB

```yaml
# Copyright 2021 Cyber Security Strategy Division
#
# Author:
---
- name: "1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)"
  win_security_policy:
    section: System Access
    key: PasswordHistorySize
    value: "{{PasswordHistory}}"
  tags:
    - level1-domain_controller
    - level1-member_server
    - scored
    - section1
    - section1.1
    - section1.1.1
```


© NEC Corporation 2023

vars.yml(変数を記載するファイル)

変数を定義することにより
各PJのシステム要件・セキュリティポリシーに応じてカスタマイズが可能

```
# 1.1.1 (L1) パスワード履歴の記録回数に関する設定
# 推奨設定は24回分以上です。
# 本playbookでは、推奨設定の最小値である24をデフォルトで設定しています。
# 必要に応じて、24以上の値になるように変更してください。
PasswordHistory : 24

# 1.1.2 (L1) パスワードの最大有効期間に関する設定
# 推奨設定は60日以下です。
# 本playbookでは、推奨設定の最大値である60をデフォルトで設定しています。
# 必要に応じて、60以下の値になるように変更してください。
MaxPasswordAge : 60

# 1.1.3 (L1) パスワードの変更禁止期間に関する設定
# 推奨設定は1日以上です。
# 本playbookでは、推奨設定の最小値である1をデフォルトで設定しています。
# 必要に応じて、1以上の値になるように変更してください。
MinPasswordAge : 1

# 1.1.4 (L1) 最小パスワード長に関する設定
# 推奨設定は14文字以上です。
# 本playbookでは、推奨設定の最小値である14をデフォルトで設定しています。
# 必要に応じて、14以上の値になるように変更してください。
MinPasswordLength : 14

# 1.2.1 (L1) アカウントのロックアウト期間に関する設定
# 推奨設定は15分以上です。
# この項目は、閾値を超えたログイン試行の失敗があった場合、一定期間アカウントをロックする設定する項目です。
# 本playbookでは、推奨設定の最小値である15をデフォルトで設定しています。
# 必要に応じて、15以上の値になるように変更してください。
AccountLockDuration : 15
```

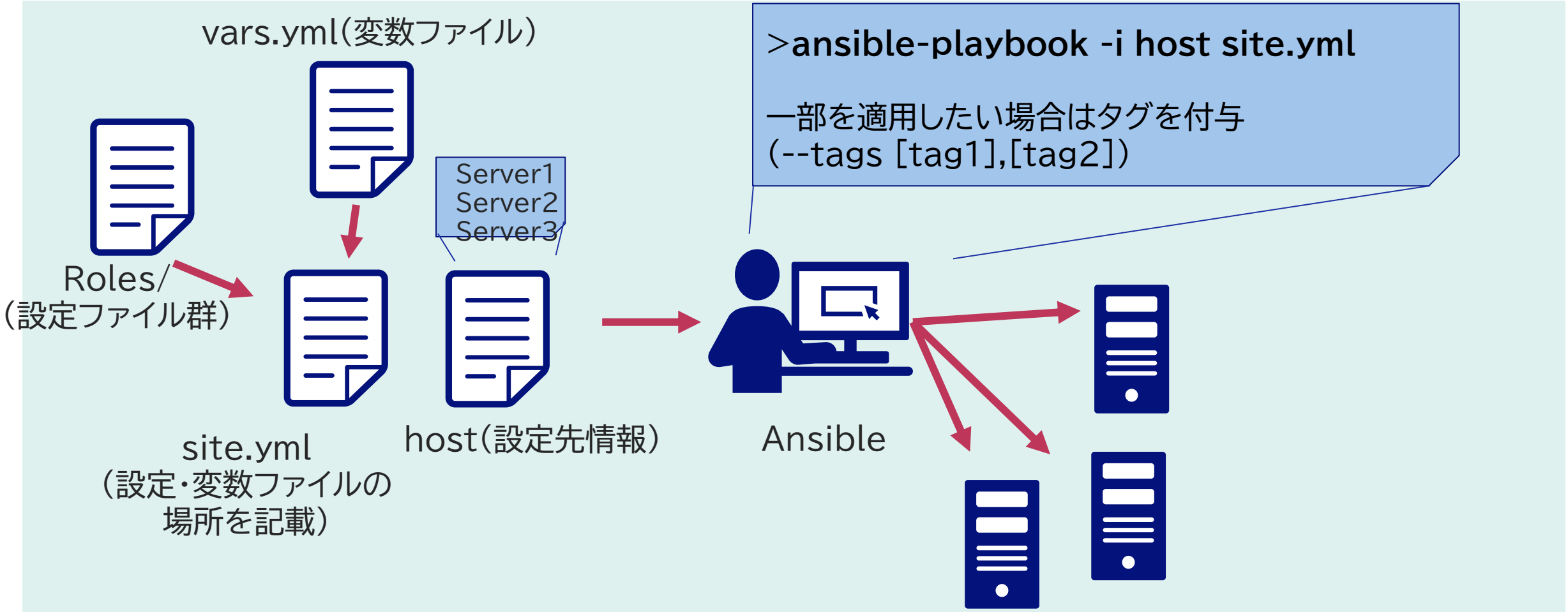
設定ファイルでの記述

```
- name: "1.1.1 (L1) Ensure 'Enforce password history' is
  win_security_policy:
    section: System Access
    key: PasswordHistorySize
    value: "{{PasswordHistory}}"
  tags:
    - level1-domain_controller
    - level1-member_server
    - scored
    - section1
    - section1.1
    - section1.1.1
```


© NEC Corporation 2023

自動化ツールの実行

コマンド1つで実行可能



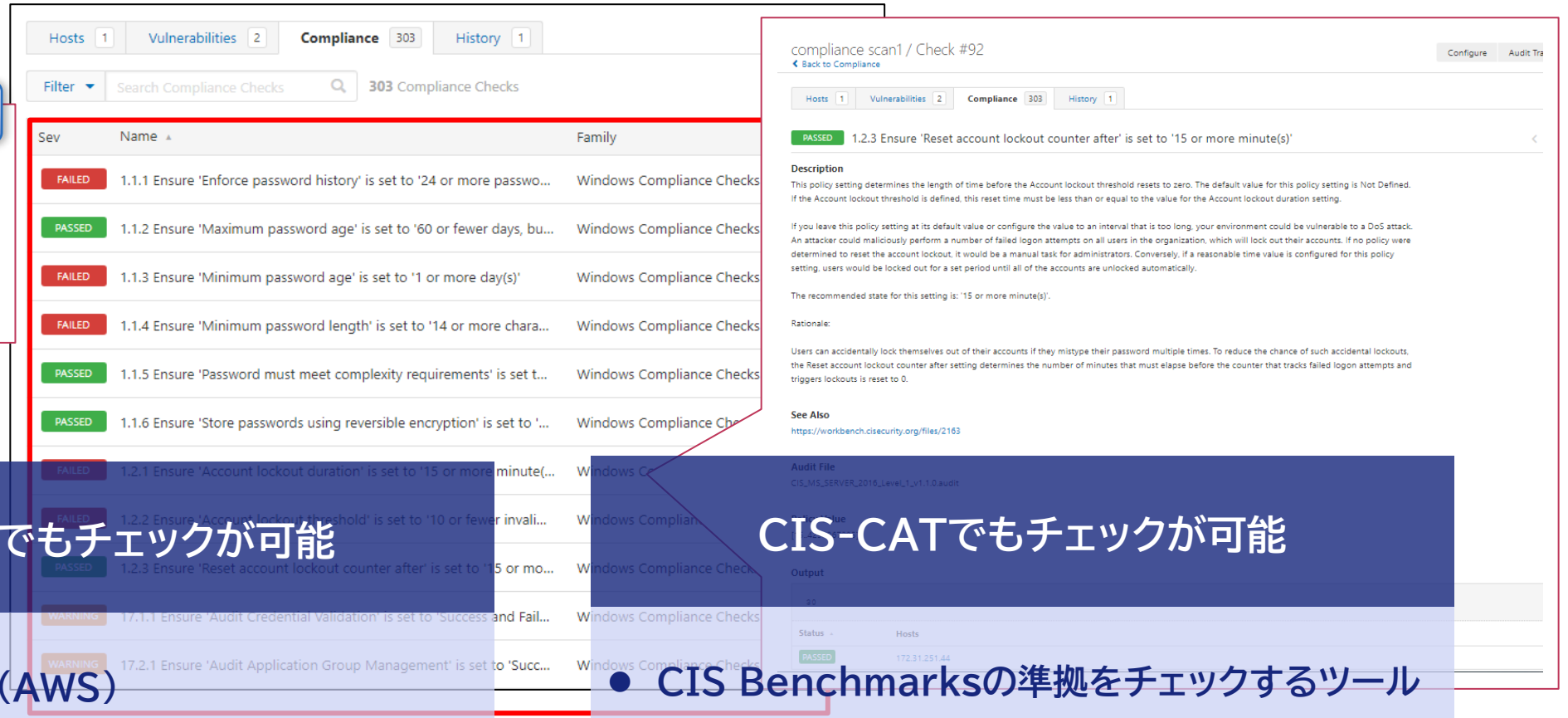
© NEC Corporation 2023

脆弱性診断ツールによる堅牢化の確認

NECではプラットフォーム脆弱性診断ツールで堅牢化の最終チェックを実施

監査結果は3種類で表示される

- FAILED 不合格
- WARNING 要手動監査
- PASSED 合格



AWSやAzureでもチェックが可能

- Amazon Inspector(AWS)
- Security Center(Azure)

CIS-CATでもチェックが可能

- CIS Benchmarksの準拠をチェックするツール
- CISが提供している

© NEC Corporation 2023

まとめ

堅牢化の課題

・どう設定すればよいか分からない
・設定が属人化しやすい
・工数がかかる

CIS Benchmarks

OSやミドルウェアのセキュア設定が記載されているドキュメント

CIS:
米国政府機関が
企業、学術機関などと連携して
インターネット・セキュリティ
標準化に取り組む非営利団体

堅牢化の自動化

Ansible Playbookを利用すれば、
堅牢化の自動化が可能

© NEC Corporation 2023

Orchestrating a brighter world
NEC