

働き方改革待ったなし！ 残業せずにファイアウォールの ポリシー管理をする方法とは？

2019年11月7日

SB C&S株式会社

ICT事業本部 販売推進本部 ネットワーク&セキュリティ統括部

ネットワーク&セキュリティMD1部 セキュリティプロダクト推進課

北畠 裕史

本日のアジェンダ

1. セキュリティ管理者が抱える課題
2. FireWallの統合管理ソリューションのご紹介
3. 工数削減効果

セキュリティ管理者が抱える課題

複雑化

- ✓ アプリ/サービス増加に伴うポリシー数の増加
- ✓ マイクロセグメンテーションによる台数増加
- ✓ UTMマルチベンダー管理の必要性

設定ミスのリスク

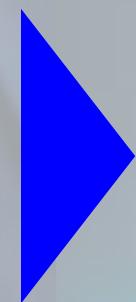
- ✓ 設定ミスによる情報漏えいリスク
- ✓ 無駄なルールによるパフォーマンス低下
- ✓ 企業コンプライアンスへの準拠

スピードアップ

- ✓ DevOpsによるアプリ開発サイクルのスピードアップ
- ✓ 脆弱性発生による、緊急ルール変更の増加
- ✓ 承認プロセスの欠落



働き方改革



生産性UP



働き方改革

課題山積・・・



FireMonで FireWallの統合管理と自動化を実現

課題山積・・



FIREMON



FireMonとは

FireMon社について

- ◆ 2001年設立（「NSPM」カテゴリにおいてシェアNo.1）
2018年に日本への展開開始
- ◆ 実績 WWで1,500社（53か国）以上の導入実績
過去5年間の年平均成長率：約45%成長
- ◆ Fortune500へ100社以上の導入

FireMon本社
Overland Park,
Kansas, USA



F | R | E | M | N

国内ご支援体制

SB C&S

パートナー支援・ディストリビューター

JSECURITY

日本語による保守・テクニカルサポート

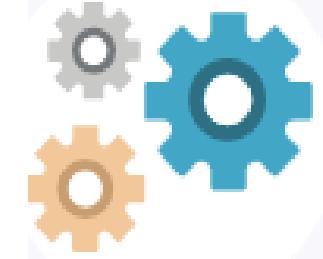
FireMonで出来る事



統合管理



コンプラ対策



自動化

FireMonで出来る事



統合管理

- ✓ マルチベンダー間の FireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の 比較分析・レポート



コンプラ対策

- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック



自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

FireMonで出来る事



統合管理

- ✓ マルチベンダー間の FireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の 比較分析・レポート



コンプラ対策

- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック

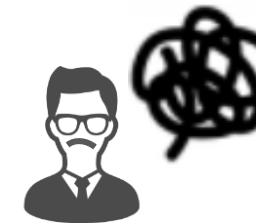


自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

マルチベンダー環境

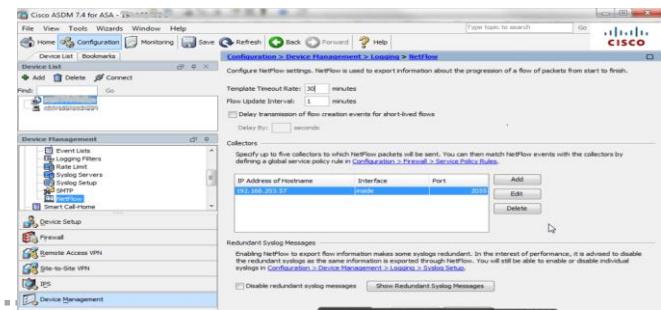
Internet



セキュリティ管理者



Cisco技術者



CISCO
Partner

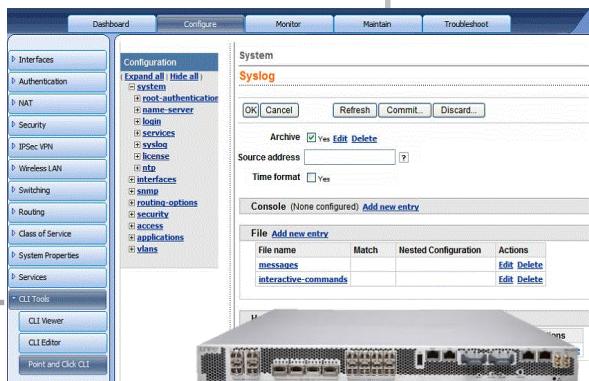
Distribution Partner



拠点A



Juniper技術者



JUNIPER
NETWORKS



拠点B



Fortinet技術者



FORTINET®



拠点C

一元管理

Enterprise | Overview Dashboard

Key Performance Indicators

44 Device Inventory	0% Devices Revised (Last 7 days) 0 Devices Revised	59.39% Unused Rules (Last 90 days) 389 Unused Rules	3.59 Average Security Concern Index ▼ <1% in 89 days
------------------------	--	---	--

Devices Recently Revised (Last 10) [View All](#)

Device Name	Last Revision	SCI ⓘ	% Change (Trend)
Azure Test/Vr...	5/16/2018 3:00 AM	4.95	No change in 8...
Azure Test/Vr...	5/16/2018 3:00 AM	9.89	No change in 8...
vB Azure Test	5/16/2018 3:00 AM	7.42	No enough hi...
Juniper SRX	5/15/2018 12:16 AM	8.79	No change in 8...
KeithTest	5/12/2018 4:58 AM	2.92	No change in 8...
R7730-SMS-fw	5/12/2018 4:32 AM	2.7	No change in 8...
vB RSA2017-CP-M...	5/12/2018 4:29 AM	2.7	No enough hi...
Panorama Lab	5/12/2018 3:23 AM	3.51	No enough hi...
SE-pan300	5/12/2018 3:23 AM	4.46	No change in 8...
PA-VM-70	5/12/2018 3:06 AM	2.56	No change in 8...

Rule Search

SOURCE	Search for IPv4/IPv6 address OR Network/Net	Include: *Any ⓘ
DESTINATION	Search for IPv4/IPv6 address OR Network/Net	Include: *Any ⓘ
SERVICE	Search for protocol/port	Include: *Any ⓘ
APPLICATION	Search for application name (exact match)	Include: *Any ⓘ
USER	Search for user name (exact match)	Include: *Any ⓘ

[Search](#)



セキュリティ管理者

FIREMON



CISCO
Partner

Distribution Partner



拠点A

JUNIPER
NETWORKS



拠点B



FORTINET



拠点C

マルチベンダーFWを一元管理



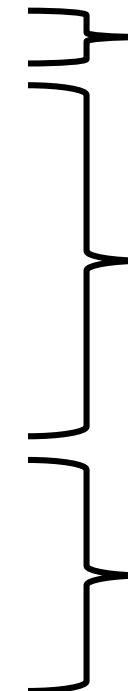
統合管理

ADMINISTRATION

System Device Access FireMon Objects Compliance Workflow Settings

Devices Management Stations Device Groups Device Packs Clusters Normalization Status Collection Configurations

	Name ▲	Description	Management IP Address	Vendor
1	192.168.22.69	Discovered by Cisco FMC - 192.168.22.68	192.168.22.69	Cisco
2	60C/FM_VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
3	60C/PC-DP-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
4	60C/PC-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
5	60C/QA-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
6	60C/root	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
7	60C/TIMS-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
8	60C/VDOM-VIP	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
9	CheckPoint - cp-fw1	Test	10.0.4.1	Check Point
10	CheckPoint - cp-mgr-logserver		10.0.4.2	Check Point
11	CheckPoint - R7730-SMS-fw	Discovered by Check Point SCS or CMA - 192.168.20.88	192.168.20.88	Check Point
12	CheckPoint - R7730-SMS-logserver...	Discovered by Check Point SCS or CMA - 192.168.20.88	192.168.20.88	Check Point
13	CheckPoint - RSA2017-CP-Manager...	Discovered by Check Point SCS or CMA - 192.168.20.88	192.168.20.88	Check Point



Distribution Partner



異なるベンダーのFWの設定内容を自動で反映・一元的に可視化

リアルタイム変更履歴の管理



統合管理

The screenshot shows the FireMon Security Manager interface with the following details:

- Header:** SECURITY MANAGER, Search bar: Search by Name or IP Address, User: FireMon firemon, Settings.
- Navigation:** Enterprise (selected), Dashboard, Policy, Security & Compliance, Change (highlighted in blue), Map, Risk Analyzer, Reports, Tools, Help.
- Sub-navigation:** Overview, Revisions, Changes (selected).
- Title:** Enterprise | Change | Changes
- Buttons:** All Changes, Export CSV.
- Table Headers:** どの機器に, 誰が, いつ, 何を行ったか
- Table Data:** The table displays 11 rows of change history for various devices and users. The columns include:
 - Device:** Palo Alto, CheckPoint - cp-mgr.
 - Revision:** 10135, 10103.
 - Action:** Added, Modified.
 - User:** admin, admin@JWENDEL-P51.
 - Date/Time:** 3/29/2019 6:01 AM.
 - Object Type:** Route, Virtual Router, Network Object.
 - Object:** 10.0.12.0/24 -> ethern..., default, testing-825, .inmotionhosting.com, 1.1.1.0/24 -> eth1_tem..., 1.1.1.0/24 -> Cluster1_..., 10.0.0.0/24 -> eth1_cp..., 10.0.4.0/24 -> eth0_te..., 10.0.4.0/24 -> eth0_te..., 10.0.4.0/24 -> Cluster_...
 - Summary:** Added route, Route(s) modified, Added network object, FQDN changed from ..., Added route, Added route, Added route, Added route, Added route, Added route.

誰が・いつ・どの機器に・何を行ったか、履歴を管理

リアルタイム変更履歴の比較



統合管理

SECURITY MANAGER | Search by Name or IP Address | FireMon firemon | Reports | Tools | ?

CheckPoint - cp-fw1 | Dashboard | Policy & Security & Compliance | Change | Map | Reports | Tools | ?

Overview Policy View Security Rules Network Objects Service Objects User Objects Application Objects Security Profiles NAT Rules Interfaces Routes Zones

CheckPoint - cp-fw1 | Policy | Policy View

View Changes: Revision Compare To:

On Off [6008 | 10/19/2018 3:39 AM] [2804 | 10/3/2017 6:22 AM]

Modified Added Removed No Changes

Security Rules ▲ Network Objects ▲ Service Objects User Objects Application Objects ▲ Security Profiles NAT Rules Interfaces Zones Routes Raw Files

Policy: ▲ Standard ▾

Enter text to filter table data by Rule No., Rule Name, Source, Destination, User, Application, Service, or Comments.

	Rule No.	Rule Name	Status	Source Zone / Interface	Source	Destination Zone / Interface	Destination	User	Application	Service	Action / Security Profile	Logging	Comments
●	6	Test Nat 1	Enabled		nat-10.0.4.11		test-1.1.1.6			TCP http	Action ACCEPT	Enabled	
●	7	Test Nat 2	Enabled		test-10.0.0.100		test-10.0.4.12			TCP http	Action ACCEPT	Enabled	
▲	13		Disabled Enabled		* Any		ubuntu-10.0.4.5	* All Users		TCP smtp	Action ACCEPT	Enabled	

設定変更の前と後の内容を、並べて比較確認

FireMonで出来る事



統合管理

- ✓ マルチベンダー間の FireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の 比較分析・レポート



コンプラ対策

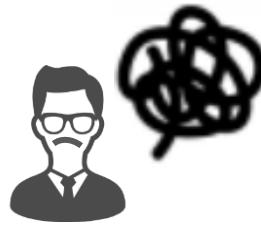
- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック



自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

重複ルール

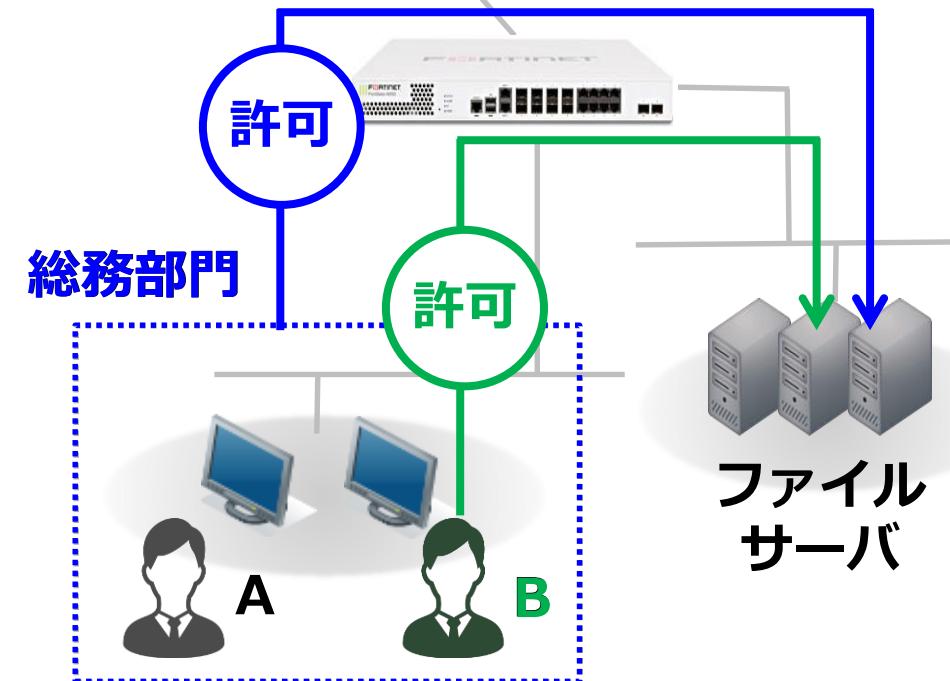


セキュリティ管理者



- ①総務部門からのアクセスを許可
- ②総務部門の担当Bからのアクセスを許可

無駄な重複ルール



重複ルールのチェック



コンプラ対策



セキュリティ管理者



FIREMON

Removable Rules Report
January 30, 2019 6:33:10 PM UTC
Displays the security rules that may be safely removed because they are shadowed or redundant. Security profiles defined are not considered when computing results.
Include Rules Causing Shadowing or Redundancy: Yes | Include Object Details: Yes

Device	Management IP Address	Product	Last Revision
Palo Alto (ID: 5)	10.0.1.1	Palo Alto Networks PA Firewall	January 14, 2019 9:41:50 PM

This device has 5 rules which have been identified as removable.

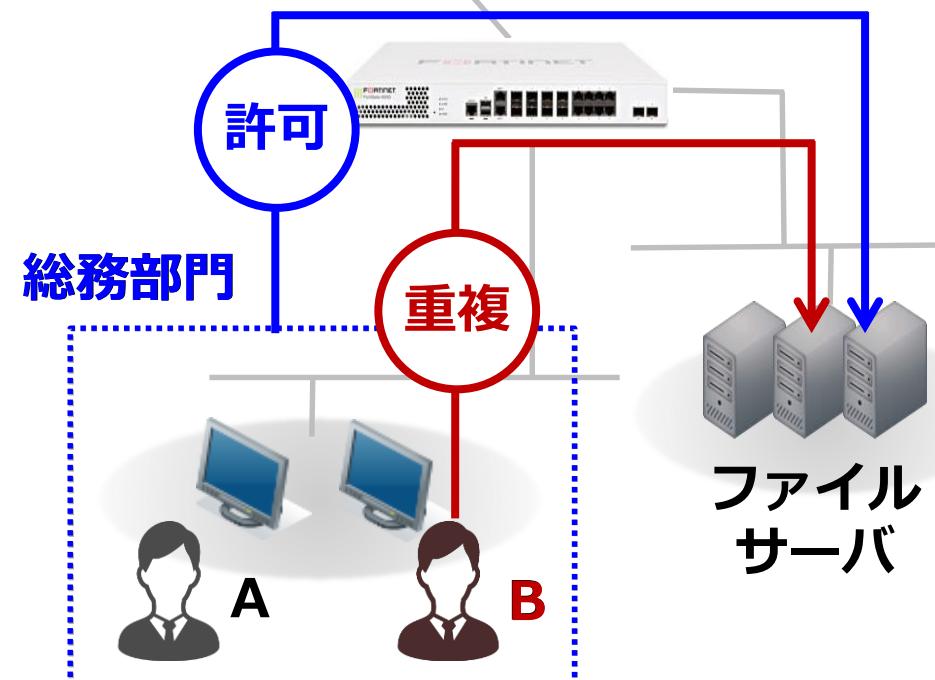
Policy | Policy (IPV4)
This policy has 5 rules which have been identified as removable.
Recommendation: Remove Rule 16

Rule Summary	Source / User	Destination	Application / Service	Action / Security Profile	Logging	Tags	Comments
Policy: Policy Number: 16 Name: rule3	Source Zone └ WAN Source └ fe6-trust [19.0.6.0/24] └ fe2-trust [19.0.2.0/24] └ fe4-trust [19.0.4.0/24] └ fe3-trust [19.0.3.0/24] User	Destination Zone └ Trust Destination └ FireMon-DC-10.0.1.5 [19.0.1.5/32]	Application └ ICMP Service └ Any	Action └ Accept	Enabled		

Rule 16 is made redundant by rule 15.

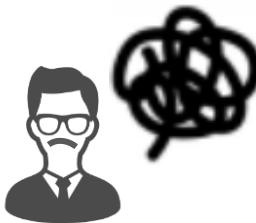
Rule Summary	Source / User	Destination	Application / Service	Action / Security Profile	Logging	Tags	Comments
Policy: Policy Number: 15 Name: rule15	Source Zone └ WAN Source └ fe6-trust [19.0.6.0/24] └ fe2-trust [19.0.2.0/24] └ fe4-trust [19.0.4.0/24] └ fe3-trust [19.0.3.0/24] User	Destination Zone └ Trust Destination └ FireMon-DC-10.0.1.5 [19.0.1.5/32]	Application └ ICMP Service └ Any	Action └ Accept	Enabled		

FireMonが重複ルールを指摘



設定ミスによる内部規定違反

Internet



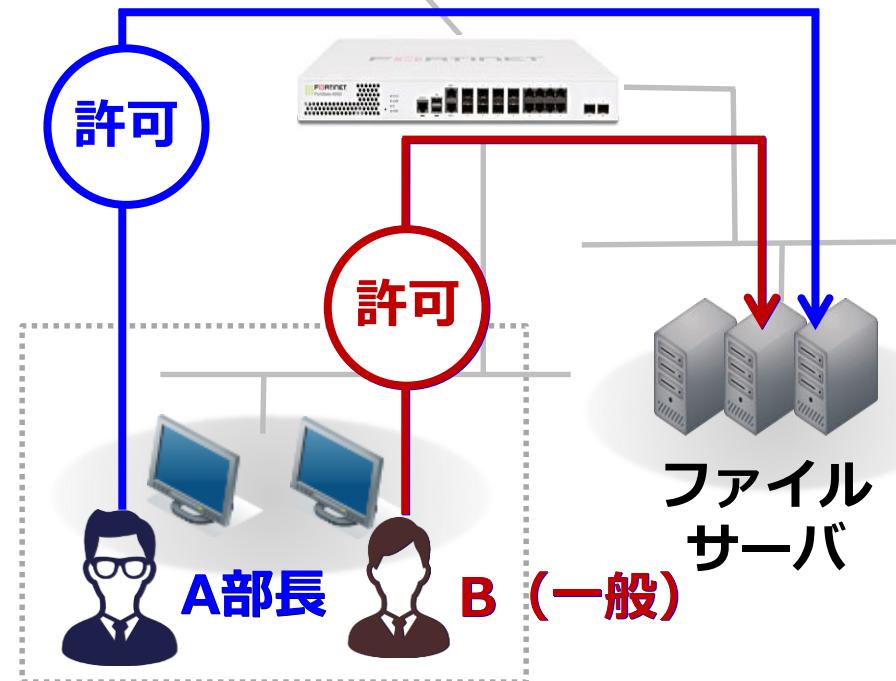
セキュリティ管理者

内部規定にそった正しい設定内容

- 総務部門のA部長からのアクセスを許可
- 総務部門のB（一般社員）はアクセスNG

設定ミスにより
Bからのアクセス許可

総務部門



内部規定への遵守状況をチェック



コンプラ対策

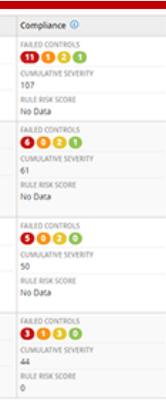
Internet



セキュリティ管理者

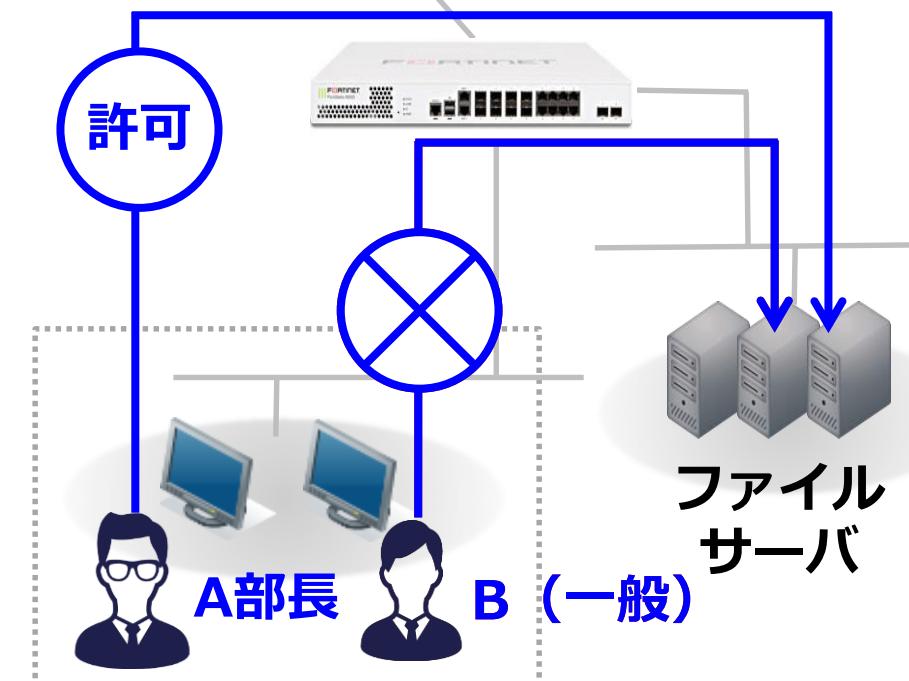
FIREMON

Rules with Control Failures						
Rule Summary		Source / User Object	Destination	Application Object / Service	Action / Security Profile	Policy
1	RULE 1 Test5	SOURCE ZONE * Any	DESTINATION ZONE * Any	APPLICATION OBJECT * Any	ACTION Accept	Hit Count: 0 LAST USED: Never PROPERTIES: Unused, No Comment
2	POLICY 2 Test3	SOURCE ZONE * Any	DESTINATION ZONE * Any	APPLICATION OBJECT * Any	ACTION Accept	Hit Count: 0 LAST USED: Never PROPERTIES: Redundant, Unused, No Comment
3	POLICY 3 fm_policy_Allow_Test_4	SOURCE ZONE * Trust * Untrust	DESTINATION ZONE * Any	APPLICATION OBJECT ping	ACTION Accept	Hit Count: 0 LAST USED: Never PROPERTIES: Redundant
4	POLICY 7 Gregs Test	SOURCE 2.2.2.2 Address	DESTINATION HOST	APPLICATION OBJECT * Any	ACTION Accept	Hit Count: 0 LAST USED: Never PROPERTIES: Redundant, No Comment



総務部門

FireMonが規定違反を指摘



FireMonで出来る事



統合管理

- ✓ マルチベンダー間の FireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の 比較分析・レポート



コンプラ対策

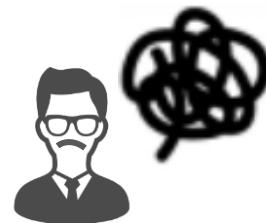
- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック



自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

頻発するポリシー変更依頼



セキュリティ管理者

Internet

このポート
空けて！

至急
対応依頼

こここのポート
閉じて下さい

緊急アラート
発生

新作アプリの
検証間環境を


CISCO
Partner

Distribution Partner



拠点A

!!



 JUNIPER
NETWORKS



!!



拠点B

 FORTINET



!!!!



拠点C

頻発するポリシー変更依頼

Internet



セキュリティ管理者

このポート
空けて！

新作アプリの
検証間環境を

このポート
閉めて下さ

緊急アラート

- 毎日何件ものポリシー変更依頼が・・・
- 設定ミスがないよう、細かく内容をチェック
- FW機器ごとにポリシーの設定変更を実施

拠点A

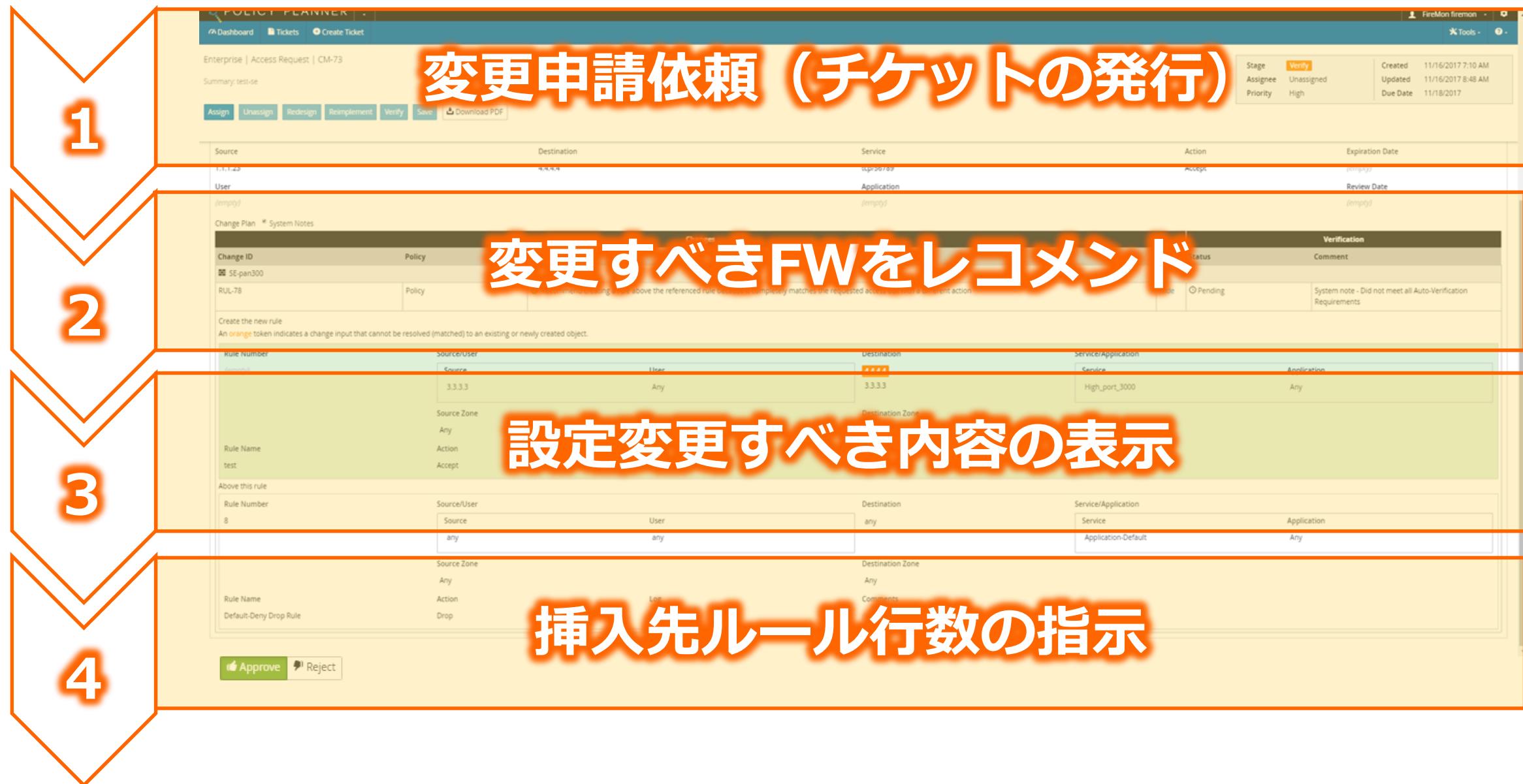
拠点B

拠点C

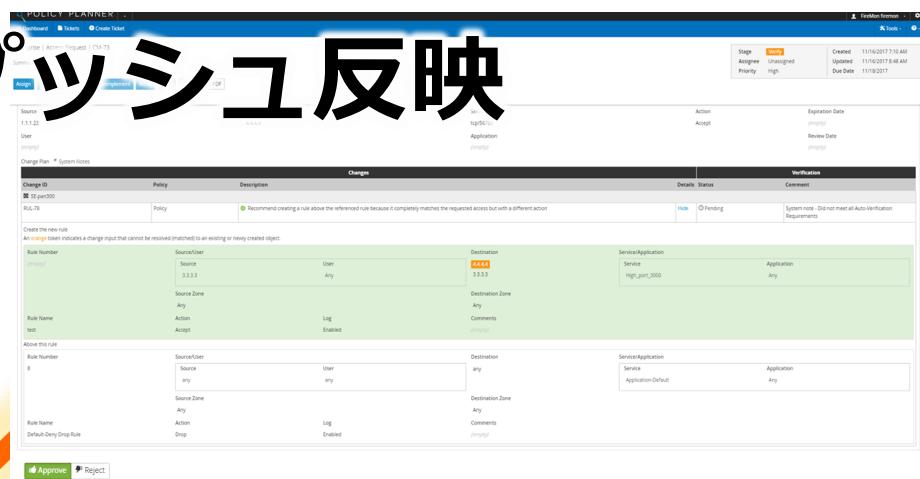


自動化

ワークフロー/レコメンド機能



ポリシーを自動プッシュ反映



FIREMON

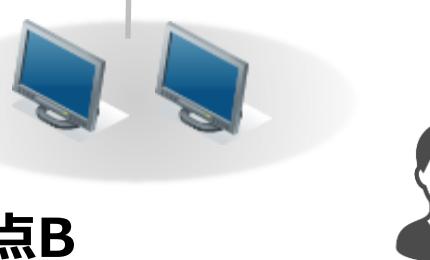


Distribution Partner



拠点A

JUNIPER
NETWORKS



拠点B



拠点C

導入例から見る 費用・工数削減効果

導入想定

FireWall導入環境

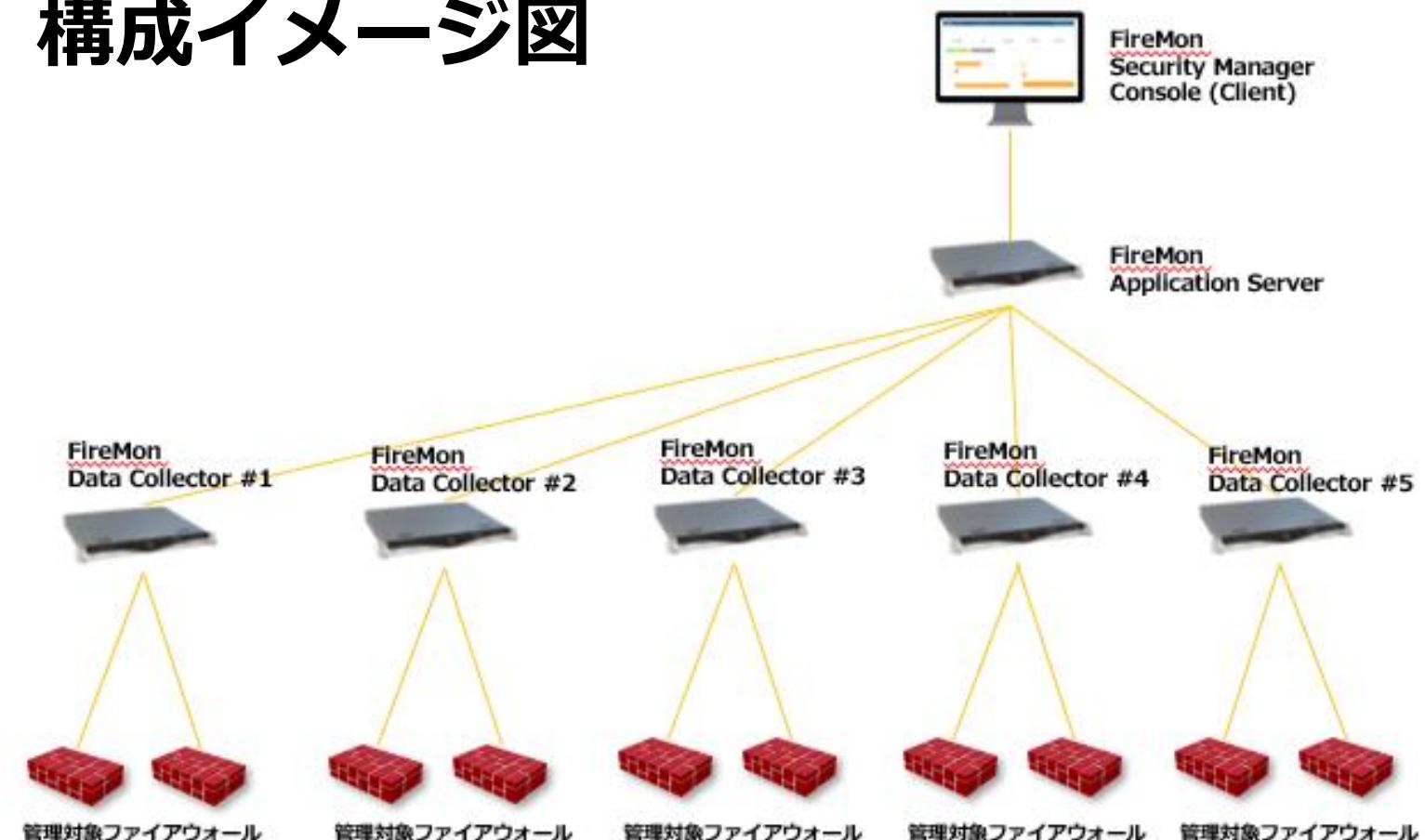
管理対象FW数：**100台**

総FWルール数：**5,000行**

FWの変更申請数：**50件/週**

FWポリシー棚卸：**1回/四半期**

構成イメージ図



導入効果 (FW1台あたり)

ポリシー設定変更作業

60分



10分

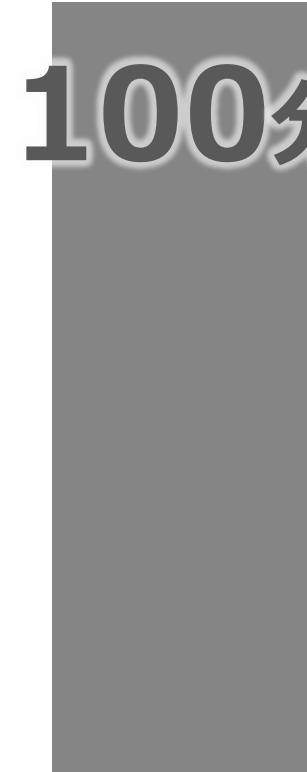


手作業

F I R E M O N

ポリシー棚卸作業

100分



10分



手作業

F I R E M O N

導入効果

ポリシー設定変更作業

約12.5人月
約2,000万円

削減

手作業

FIREMON



FireWall導入環境

管理対象FW数 : **100台**
総FWルール数 : **5,000行**
FWの変更申請数 : **50件**/週
FWポリシー棚卸 : **1回**/四半期

導入効果

FireWall導入環境

管理対象FW数：**100台**

総FWルール数：**5,000行**

FWの変更申請数：**50件/週**

FWポリシー棚卸：**1回/四半期**



ポリシー棚卸作業

約**3.8人月**

約**600万円**

削減

手作業

FIREMON

導入効果

ポリシー設定変更作業

ポリシー

Down

重大な情報漏洩事故へのリスク
約125日
約2,000万円
設定ミスによる
約30人
約60人

削減

削減

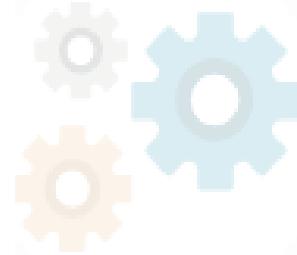
FireMonの導入効果まとめ

「人」への負担を大幅軽減し、
「自動化」により運用のスピードアップと
設定ミス防止を同時に実現！

統合管理

コンプラ対策

自動化



**製品に関するお問い合わせ
無償検証(PoC)のご依頼お待ちしております
※お問い合わせはこちら**





SBC&S