

## Cisco ASA Firepower モジュール

# かんたんセットアップ ガイド



本ガイドの手順で ASA Firepower モジュールを かんたんにセットアップできます

事前設定
 セキュリティ ポリシーの設定
 データベースの更新
 レポーティングとモニタリング



事前設定

はじめに 1-1

本ガイドでは、Cisco ASA 搭載の「Cisco ASA Firepower モジュール」による、ネットワークトラフィックを制御するための基本的なセキュリティ(アクセス コントロール)ポリシーを設定します。別冊の『Cisco ASA with Firepower Services かんたんセットアップ ガイド』などを参考に、ライセンスのインストールまでの初期セットアップを完了してから、本ガイドの設定を開始してください。設定には、Cisco Adaptive Security Device Manager (ASDM)を使用します。

また、本ガイドの一部の設定では、オプション ライセンスがインストール済みであることを前提 としています。その場合には「MEMO」「注意」コラムなどで、必要なライセンスを明記しています。 Cisco ASA with Firepower Services には、デフォルトで Application Visibility and Control (AVC) ライセンスが付属していますが、オプションの Next-Generation IPS (NGIPS)、 Cisco Advanced Malware Protection (AMP)、および URL フィルタリング (URL) ライセ ンスを購入することで、さらに高度な機能を追加できます。

● AVC: 3,000 を超えるアプリケーションの識別および制御機能が使用できます。

- NGIPS:きわめて効果的な脅威保護と、ユーザ、インフラストラクチャ、アプリケーション、およびコンテンツに対するフル コンテキスト認識機能を備え、マルチベクトルな脅威も検出し、防御対策を自動化します。
- AMP:高度なマルウェアに対してインライン ネットワーク保護および Cisco Threat Grid サンドボックスを提供します。
- URL: 2.8 億以上のトップレベルのドメインをリスクレベルごとに 82 以上のカテゴ リにフィルタリングできます。

オプション ライセンス	SKU に 含まれる 文字列	NGIPS	AMP	URL
NGIPS ライセンス	TA		-	-
AMP ライセンス	AMP	-		-
URL ライセンス	URL	-	-	
NGIPS & AMP ライセンス	TAM			-
NGIPS & URL ライセンス	TAC		-	
NGIPS & AMP & URL ライセンス	TAMC			

### 1-2 サービス ポリシーの設定

ASA Firepower モジュールにネットワークトラフィックをリダイレクトするためのサービス ポリ シーを設定します。ASDM を起動します。

File Yee Taole March Minder He		Fight topic to search 00 11111		[Configuration] をクリック
Home S Configuration	Cater Cater Cater Cater	cisco		- 0
Device Dashboard Strevel	I Dushboard 🛛 🛃 AGA FirePOWER Dushboard 🔤 AGA FirePOWER Reporting 🛛 🔀 A	A FeePOWER Status		
Denke Information     General License     Host Name: 5508x.dkload     ASA Version: 5x6(1)3     ASOM Version: 7x6(1)     Prevail Mode:	dzierce.com Device Uptrier: 16d 19h 5m 4% Device Type: A&A 500 Crotes 10th Stock	Tote Teres Status         The Address/Mark         Line         Lth         Tops           Invide         199.13.25.25(1)         Φ         Φ         Φ         07           made         199.13.25(1)         Φ         Φ         Φ         07         07           madespreet for the top 549th         Φ         Φ         Φ         Φ         Φ         07           notation         (190.13.131.12)18         Φ         Φ         Φ         Φ         0		
Environment Status	4 0K Tutal Flash 8192 MB	Taket as steefing to see and and once the		
1171 Sessions		Seecon monace to new reportant coport tops		
IPsec: 0 Cleridess 53.	VHz 0 AnyConnect Clent: 0 Catalo	Fallow not configured. Click the link to configure it. Configure it.		
Vystevn Resources Status Total Nemory Usage   Total CPU Usage Memory Usage / 1950	( Czec Usage   Detals			
9000		UOP: 0 TOP: 0 TOP: 0 TOP: 0		
94000 3000 2000				
15 05 - 4 0 05:31	0932 0933 0934 0938	andruzer p Conductable ve		
Latest ASDM Syskog Messages	ACCP1 logging is disabled. To enable ACCP1 logging is 	h reformational level, dick the batton below. $\label{eq:constant} \log \left( \frac{1}{2} + 1$		
		adam 15 🕼 🚂 🔒 1220606 5.05-46 APTURC		
File Vew Tools Woards Window Heb	1 5	Type topic to search 92 altitutity	2	「Firewall] をクリック
Home S Configuration D Monitoring	g 🔄 Save ASA Changes 🔇 Refresh 🔇 Back 🕐 Forward 🤶 Help	CISCO		
Carter Want     Carter Want     Carter Settings	CONSTRUCTION AND CONTRACTOR			
20 +1+ Routing Device Name,Password	Click the "Launch Startup Wizard" button to start the vicard.			
a C Internet	Startup Wizard			
	Ciso Adaptive Security Agalance configured and running. Use this ward to create a basic configuration that enforces			
	The Startup Wood can be run at ony time and will be initialized			
	PROTVINIES INCLUMENTATION OF COMPANY AND A DESCRIPTION OF COMPANY			
3 containe				
3 Dever State	-2			
3. Dente Solar By Trond Solar Local (PA Solar Local (PA Solar Local (PA	-2			
Ports Solar     Trend     Ports Solar     Trend     Solar Solar     Solar     Solar Solar     Solar	-0			
Const Size     Const Size     Const Size     Const Size     Specia Size (S)     S	-2	Last fore low		





8 [ASA FirePOWER Inspection] をクリック

CTIQBE		1
Cloud Web Security	Configure	
DCERPC	Configure	
DNS	Configure	
ESMTP	Gerfigure	
FTP	Configure	
H.323 H.225	Configure	
H.323 RAS	Configure	
HTTP	Configure	
ICMP		
ICMP Error		
ILS		
IM	Configure	
IP-Options	Gerfigure	
IPSec-Pass-Thru	Configure	
IPv6	Configure	
MMP	Configure	
MGCP	Configure	
AISTOTOC	Carlinson	



- 9 [Enable ASA FirePOWER for this traffic flow] をクリッ ク
- 10 [Permit traffic]または[Close] traffic] をクリック

障害が発生した場合など、ASA Firepower モジュールが利用不 可能な場合の動作を選択します。 [Permit traffic] を選択した場合、 すべてのネットワーク トラフィックを 検知なしで通過させます。[Close traffic]を選択した場合、すべてのネッ トワークトラフィックを遮断します。



11 [Finish] をクリック



### 2-1 ファイル ポリシーの設定:マルウェア対策

マルウェア対策として、ユーザがアップロード(送信)またはダウンロード(受信)するファイル の検知やブロックなど、特定の種類のファイルをコントロールするためのファイル ポリシーを設 定します。ここで設定するファイル ポリシーは「2-2 アクセス コントロール ポリシーの設定: 可視化」で使用します。









#### 🛕 注意

③で選択できる [Malware Cloud Lookup] または [Block Malware] 設定が実際に機能するためには NGIPS ライセンスまたは AMP ライセンスが必要です。これらのライセンスをインストールしていない場合は [Detect Files] または [Block Files] を選択してください。

- Detect Files: ⑨で選択した種類のファイルを検知します。
- Block Files: ⑨で選択した種類のファイルをブロックします。
- Malware Cloud Lookup: ⑨で選択した種類のファイルに対してマルウェア検査を実行します。
- Block Malware: <sup>●</sup>で選択した種類のファイルに対してマルウェア検査を実行し、脅威の疑いが ある場合にはブロックします。





12 [Store ASA FirePOWER Changes] をクリック

[Apply Access Control Policy]ポッ プアップ ウインドウが表示されます。

### 🗾 МЕМО

ファイル ポリシーには、複数のルールを設定できます。ファイルの種類のカテゴリ別や種類別にルールを設定する場合は、2から10の手順をくり返してルールを追加します。

### 2-2 アクセス コントロール ポリシーの設定:可視化

デフォルトの [Default Allow All Traffic] ポリシーを編集して、ネットワーク トラフィックを可視 化(ロギングおよびモニタリング)するためのルールを設定します。

1	Cisco ASDM 7.4 for ASA - 198119110254 In View Took Waards Window Heb				Free topic to search		1		Control Pa	licy] を
4	home of Configuration 🖂 Monitoring	p 🔚 Sava ASA Changes 🔇 Rafred	h 🞧 teck 💭 Forward 🛛 🤊 Help		Type to	picto sauch CISCO		[ACCC33	001110110	JIICy
	ASA FirePOWER Coefigur Ø 9	Configuration > ASA FirePOWIR Co	ediquation > Policies > Eiles							
<ul> <li>Bootmark</li> </ul>	Access Control Policy      Access Control Policy      Users      Gram      Gram	Block Malware			You 1	have unsaved changes		クリック		
L	Device Plans ensert     Object Plans ensert	Rules Advanced			the second se	O HILLON				
L	Local     Sostern Information	His Tapas	Analysis Restored	Direction	Autors	ETT O HOU HIE HURE				
	a Brance	D Cargoni Staten Res D Cargoni Staten Res D Cargoni Staten Res D Cargoni Profiles C Cargoni Profiles (4 mm.)	Αρμικατία πουστο	ker	noom	/ 8				
	Covers Solution     Covers Solution     Covers Solution     Covers Solution     Covers Solution     Covers Management			Rore ASA FreePowEll Changes 🛛 🧲	I Cancel					
	:									



#### 🛕 注意

●で選択できる侵入防御ポリシー設定が実際に機能するためには NGIPS ライセンスが必要です。ライセンスをインストールしていない場合は [None] を選択してください。

6 [Intrusion Policy] メニュー Add Rule 8 Name Logging and Monitoring Enabled Insert into Ca V IPS: Conne から [Connectivity Over Action of Aller ones Networks Users Applications Ports URLs on Logging 6 Security] を選択 7 [File Policy]メニューから「2-1 ファイル ポリシーの設定:マル 7 ウェア対策」
らで入力したポリ Add Cencel シー名を選択 8 [Logging] タブをクリック ログの設定画面が表示されます。 Add Rule 9 [Log at End of Connection] Enable me Logging and Monitoring Y Standard Ru V IPS: no policies Variables をクリック Action 🖌 Allow Zones Networks Users Appl ns Ports URLs Inspection Logging Con 9 10 [Add] をクリック File Events 10 Send Connection Events to ☑ Event Viewer Syslog (Connection Event only) SNNP Trap 11 [Apply ASA FirePOWER ards <u>Window</u> Help Type topic to search CISCO Sever ASA Changes 💽 Extract 💽 Eack 🕥 Proverd 🏆 Help Changes] をクリック Default Allow All Traffic [Apply Access Control Policy]ポッ Rules Security Intelligence HTTP Resp es Advanced Saurce Dest Source Dest US... Appli... Src P... Dest... UR.s a Name プアップ ウインドウが表示されます。 Action Standard Rules 1 Logging and Monitoring Aller 0 2 0 / 6 Default Action . 11 Device Setup Emote Access 101 att s si e 12 [Apply All] をクリック Apply Access Control Policy ? X Access Control Policy: Default Allow All Traffic Apply this Access Control policy and all associated rule configurations, objects, and policy changes to affected devices. 12

Apply All

Details...

Cancel

2 セキュリティ ポリシーの設定



デフォルトの [Default Allow All Traffic] ポリシーではすべてのネットワーク トラフィックが通 過するため、業務に関係がないアプリケーションの利用や危険な URL へのアクセスを禁止し たい場合など、特定のネットワーク トラフィックをブロックするためのルールを設定します。

الكاني الماني الماني المانية الم	1 [Add Rule] をクリック
	[Add Rule] ポップアップ ウインドウ が表示されます。
Add Rule ? X Teame Blockers 2 Doubler Variables (* Toshed Loging rok bype)  Advent X Block * Proceeding of Particles in expendition Loging in the bype)  Advent X Block * Proceeding of the set of the	<ol> <li>[Name] 欄に任意のルール名</li> <li>を入力</li> </ol>
Ave alls zones c sorth by name visible antitice antite antitice antite antitice antitice antitice antitice	<ul><li>3 [Action] メニューから [Block]</li><li>を選択</li></ul>
	<ul> <li>[Insert] メニューから [above rule] を選択</li> </ul>
	5 [Applications] タブをクリック
	アプリケーションの選択画面が表示 されます。







- 6 利用を禁止したいアプリケーションを選択
- 7 [Add to Rule] をクリック

アプリケーションはグループ別およ び個別に検索と選択が可能です。

8 [URL] タブをクリック

URL の選択画面が表示されます。

- 9 アクセスを禁止したい URL カテ ゴリを選択
- 10 アクセスを禁止したい URL レ ピュテーションを選択
- 11 [Add to Rule] をクリック

URL はカテゴリ別に検索と選択、およびレピュテーション別に選択が可能です。



12 [Logging] タブをクリック

ログの設定画面が表示されます。

[13] [Log at Beginning and End of Connection] をクリック

14 [Add] をクリック



#### 🛕 注意

◎で選択できる URL レピュテーションが実際に機能するためには URL ライセンスが必要です。





15 [Apply ASA FirePOWER Changes] をクリック

[Apply Access Control Policy]ポッ プアップ ウインドウが表示されます。

16 [Apply All] をクリック



新たな脅威が発見されるたびに、シスコはセキュリティ データベースを更新しています。定期 的なデータベース更新を設定して、常に最新のデータベースに基づいてネットワークを保護で きるようにします。

ilet:				7 <sub>/pe</sub> topic to search	00	ababe		Loba	ales	をソリン	11
ntaring 📊 Sava AS	A Changes 🚱 Rafresh 🕓 Back 🕑 Forme	ard ? Help				cisco		•			
454	L'AL FRANCINER										
ter a des	cription										
Rules	Security Intelligence   HTTP Respons	es ádvanced									
			C Add Category	Add Rule Search Rules		×					
Nam	e Source Dest Sour Zones Zones Netv	nce Dest n Netw U	sers Appli Sec Po Dest P	URLs Action	🦁 🔈 🗿 🤤	9					
ninist	rator Rules										
Standard	ory is empty Rules										
1 Blocks	ng any any any	819 B	ny 📑 Risksi Leny eny	Adult and Kelock	U 🗅 🖉 I	0 🥒 🛙					
0 10	gging and 8 min min min min	aty a	ny any any any	acy 🗳 Alaw	000	• / 5					
Root Rule This cate;	pory is empty										
Default i	Action		Access Control: T	rust All Treffic		× 1					
			Display	ing 1 - 2 of 2 rules  < <	Page 1 of 1	> > C					
	20	tore ASA FenPOWER Ch	anges Cancel Apply AGA TimPOWER C	hanges							
<u> </u>			ednin 16	19 👙 🖬	🔒 របទា	17-6:45:33 AM UTC					
1254			adwin (15	De la B	B 1150	1764633AHUIC	0	[Pulo	IInda	tos] /	コブをクロ
4 \$ 9 🔄 Sone AS	Schargen 🚱 Kafrach   🚱 Keck 🛞 Proce	ard   🦻 Help	adhin (15	Type topic to enarch	60 (00		2	[Rule	Upda	tes] 🖇	マブをクリ
Som AS Conferention Produc	Kolungan (Q. Safenda) (Q. Safe (Q. Terrer 2. MAR Part Office Conference in Conference Updates Rule Updates Geolo	ard 2 Help	adwn (19	Type topic to search	@ 1/181	LIGIX LIGIX LIGIX CISCO	2	[Rule ク	Upda	tes] 🤌	マブをクリ
Sove AS Conferention Produc	Courges (Stafenh) Stade (Promo SAAC Part PUPER Conference (Stafe Stafe Versidees ) (Stafe Stafe	urd   🥐 Help   8. Scattion Updates: - ]	iathan 115	Type topic to search	0 UIST		2	[Rule ク	Upda	tes] 绪	マブをクリ
See AS Confese alian Praduc 30 Device Updates	Concer (2 Jackob) (2 Sak) (2 Torre > Saki Perf Oldra Cardonardian - U Ladates U Ladates (2 Rake Epistens) (3 Geolo Torring safkares ven en 5.4.1.4	ard   🥐 Help   K Scation Updates	jatun its	Type topic to search	2000	CISCO cod Update	2	[Rule ク	Upda	tes] 4	マブをクリ
Save AS analise Produc Device dates	Songer (2 Joins) (2 tot. (2) Trans 2 AAI Art STREE Conference on a binder Unputder Conference on a binder contrig software version 2 A.1.4	urd   🥐 Heb   Scation Updates	John 15	Fightings to march	0 USO	CISCO cod Update	2 JV-	<b>[Rule</b> ク ール デー	・ <b>Upda</b> ータベー	tes] <b>∕</b>	<b>ヌブをクリ</b> 新の設定
3 Seve AS Generation Produc 30 Device Jpdates Trace	Couge (2 tétes) (2 tét (2 tét) 2 A Charles (2 tétes) (2 tét) 1 (sidate (2 tét) (2 tét) (2 tét) 2 tét) 2 tét) (2 tét) (2 tét) (2 tét) 2 tét) (2 tét) (2 tét) (2 tét) (2 tét) 2 tét) (2 tét) (2 tét) (2 tét) (2 tét) (2 tét) 2 tét) (2 t	sard   🥐 Hebo   Securition Updates   Xecutes	John 15	Professor Sources	Contraction of the second seco	176-Histomute - Id IX - Id I	2 JV-	<b>[Rule</b> ク ール デー	• <b>Upda</b> ータベー	tes] <b>?</b> ス更新	<b>&gt;ブをクリ</b> 新の設定
Sam AS solaur diso Produc 30 Device Updates <u>Tree</u> Cisco Net Cisco Net	Sarger (2 total) (2 tot. (2) res. 2 Addref Will Calastation Mader Under Under State States Derrig States virtue 5.4.1.4 und States Factoreade	station Updates       Yersitea       54.1.4-7       54.1.4-7	4000 15	Pron Track To ensemble	UISY	els -	<b>2</b> ル-	[Rule ク ール デー が表示さ	• Upda ータベー わます	tes] <b>?</b> ス更新	<b>&gt;ブをクリ</b> 新の設定
Som AS College al los Praduce Updates Tree Cisco Met Cisco Met	Songer & Johns Onto, Ornor Ald Ald Statistics Conferences - Makine Ald Ald Statistics Conferences Annong sthears van et B.4.1.4 wat Statist Public Nordalf- wat Statist Public Nordalf- wat Statist Public Nordalf-	scalion Updates ) <b>Xerrien</b> 5.4.1.4-7 5.4.1.3-26	John         15           Bate	Provinger to smarth	C una C una		<b>2</b> ル- 面が	<b>[Rule</b> ク ール デー	・ <b>Upda</b> ータベー れます。	tes] <b>?</b> ース更新	<b>&gt;ブをクリ</b> 新の設定
Some AS contract about Produce Upclates Types Cisco Met Cisco Met Cisco Met	Souge Statute Cale Cale Cale Cale Cale Cale Cale Cal	Image: The second sec	John         15           Data	Provinger to exactly	C union C union Redecas Yes Yes Yes Yes	CISCO COLUMBRE COLUMBRE	2 ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>?</b> ス更新	<b>&gt;ブをクリ</b> 新の設定
Save AS Saration Produc Device Scilates SEE Sco Net Sco Net Sco Net Sco Net	Company & Felenki & Tesh. () Provide MARANGENI Collectuation : Market Testing and any response in a Lat. () word: Starser Felenki Unstatler word: Starser Felenki Unstatler word: Starser Felenki Unstatler word: Starser Felenki Unstatler	Yes         Yes           Scalion ()udates         )           \$ 4.14-7         \$ 4.14-7           \$ 4.12-25         \$ 4.13-25           \$ 4.12-32         \$ 4.12-32	Johns         16           Pate         The ship 55 21:04-32 UTC 3033           The ship 55 21:04-32 UTC 3033         The ship 55 21:04 UTC 3033           The ship 55 21:04-32 UTC 3033         The ship 55 21:05 UTC 3033           The ship 55 21:05 UTC 3033         The ship 52 21:05 UTC 3033	Fign logi to menth	1000     1000	274-14-03 AMULE CISCO COLUMBRE CO	<b>2</b> ル- 面が	[Rule ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	<b>tes] </b> ス更新	<b>&gt;ブをクリ</b> 新の設定
3 Device Updates Updates Cisce Mel Cisce Mel	Course to the first term of the course of th	ver 2 nob k Secation Updates 5.4.1.4-7 5.4.1.3-25 5.4.1.3-25 5.4.1.3-25	John         15           Bate	Pyre type to exact.	Control Contro		<b>2</b> ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	<b>tes] </b> ス更う	<b>&gt;ブをクリ</b> 新の設定
Produc Device Device Updates Izec Cisco Met Cisco Met Cisco Met	Source Statest Concernation	xral 2 not xraina 5 41.6-7 5 41.3-25 5 41.3-25 5 41.3-25	John         15           Bate	The Table is mark	susce     or     susce     or     susce     or     susce     or     susce     or     susce     ves     ves     ves     ves     touris	(1)     (	<b>2</b> ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	<b>tes] ?</b> ス更新	<b>&gt;ブをクリ</b> 新の設定
St To To Produce SD Device Updates <u>Trac</u> Crises Met Crises Met	Course to the other to the othe	ver 2 mb x x x x x x x x x x x x x	John         15           Parter         10           Parter <td>E D D</td> <td>Autor     Autor     A</td> <td>274433347UKG</td> <td>2 ル- 面が</td> <td>[Rule ク ール デー が表示さ</td> <td>・<b>Upda</b> ータベー れます。</td> <td>tes] <b>?</b> ス更き</td> <td><b>タブをクリ</b> 新の設定</td>	E D D	Autor     A	274433347UKG	2 ル- 面が	[Rule ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>?</b> ス更き	<b>タブをクリ</b> 新の設定
SS4 Inte Troy in Serie & D Content with a Updates Inter Cises Met Cises Met Cises Met	Allergen and the second	xrel <b>? http:</b> xreation (Updates 5.4.1.4-7 6.4.3.2-5 5.4.1.23 5.4.1.23	John         15           Bate	E B B	Develop	IT A 41 50 APULTO	<b>2</b> ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	<b>tes] </b> ス更新	<b>タブをクリ</b> 新の設定
ASSS Be Contact live as a series Contact live as a series Contact live as a series Contact live as the Contact live as the Conta	Source Detected To the Control of th	xr380 5.414-7 5.414-7 5.414-7 5.413-25 5.413-25 5.413-23	Juster         15           Parter         1           The Key S 20 (34:52 UVC 2015)         1	gradient auch	b) URC:     Corrison     Corrison     Corrison     Corrison     Corrison	IT A 41 30 APU UT C IT IT IT IT IT CISCO OOI UV492 UV49 UV49 UV492 UV49 UV49 UV49 UV49 UV	<b>2</b> ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>?</b> ス更う	<b>タブをク!.</b> 新の設定
Alza     Inh	AGunga Statisti Carlo Carlo Markar Statisti Carlo Carlo Markar Statisti Carlo Carlo Markar Statisti Carlo Mark	ver 2 nob catalon Updates 54.14-7 54.12-23 54.13-23	John         15           Bate	Brites trace	All Super-	T2-44-33 APULC	<b>2</b> ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	<b>tes] </b> ス更語	<b>ヌブをクリ</b> 新の設定
ASSA Lek Terrer and an and an and President Store for Cases Mer Cases Mer Cases Mer Cases Mer	A Grager & Selfert & Tests () First Market Carlorations - Market Typedate Carlorations - Market Typedate Carlorations - Self-4 - Annotation - Self-4 - Self-4	cardin Updates Cardina Updates 9.4.1.6.7 5.4.1.9.25 5.4.1.9.25 5.4.1.1.23	John         15           Date	E g g g	O take     Rebeat     Yvs     Vvs     Vvs     Vvs     Vvs     Vvs     Vvs     Double	174.44.33 APULC	<b>2</b> ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>分</b> 一ス更新	<b>&gt;ブをク!</b> 新の設定
nD24 Tel: Perioduce Perioduce Perioduce Deditections	A Gueger & Matter & Set & A A Darper (1997 Conference on the Set of the A Darper (1997 Conference on the Set of Conference on the Conference on the Set of Set of of Set of Set of the Set of Set of Se	ref 2 tob cratics (Values ) 54.14-7 54.13-25 54.13-25 54.13-25	John         15           Pate	(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	C Galo Referent Yes Yes Yes Downlot		2 ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>?</b> ス更新	<b>ヌブをクリ</b> 新の設定
54 be Transformer Produce at like Produce at like Device at like Device at like Device at like Device at like Cisce at like Cisce at like Cisce at like Cisce at like Cisce at like	A Garger & statistic & etc. () or esc. a data before Carlos and the statistical and t	ard 2 map accators Updates 5.4.1.4.7 5.4.3.2.6 5.4.3.2.2 5.4.3.2.2 5.4.3.2.2	John         15           Bats	E g S	O     Unio	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	2 ル- 面か	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>\$</b> ス更왕	<b>&gt;ブをク!.</b> 新の設定
a See 85 Contraction Preduct 20 Device Updates Creas Mit Creas Mit Creas Mit	Adduger (* Helsen (* 1efe (* ) a Adduger (* Helsen (* ) a Adduger (* Helsen (* ) ) Under and (* ) Under and (* ) Under and (* ) Sector (* ) S	xrz] 2 hdp x xzzine 5.4.1.6-7 5.4.1.6-7 5.4.1.2-2 5.4.1.2-23 5.4.1.2-23	John         15           Parter	(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	O     UNC     O	1754-1334016 1754-1334016 1764-134 1764-134 1764-134 1774-134	2 ル- 面が	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>?</b> ス更う	<b>ヌブをクリ</b> 新の設定
4 Contractions of the second	A Gueger () terrini () esc. () () esc. () () esc. () () () esc. () () () esc. () () () esc. () () () () esc. () () () () () esc. () () () () esc. () () () () () () () () () () () () ()	ver	John         15           Bate	Contract to each	Control of the second s	() () () () () () () () () () () () () (	2 ル- 面か	<b>[Rule</b> ク ール デー が表示さ	・ <b>Upda</b> ータベー れます。	tes] <b>?</b> ス更き	<b>ヌブをク!.</b> 新の設定



a Yawa Taola Waarda <u>Window H</u> alp		Type topic to search (5)	hab
Home 🍓 Configuration 📴 Monitoring	Sava ASA Changes 🔇 Rafresh 🔇 Back 🕥 r	roward 2 Help	isco
ASA FirePOWER Coefigur (7 4 0	iouration > ASA FirePOWIR Configuration > Upda	des and a second s	
Policies     Device Management	and an entry fraction for		
(i) 👩 Object Management	Product opdates Kule opdates G	Constant of the second se	ate Lon
System Information			
Licenses	One-Time Rule Update	/Rules Import	
🕀 🏫 Tools	Note: Importing will discard a	all unsaved intrusion policy and network analysis policy edits.	
	Saurce	Fulle update or text-rule file to uplead and install     Choose File     No file choosen	
		B Download new rule update from the Support Site	
	Policy Reapply	Reapply intrusion policies after the rule update import completes	
		in integral access control pances aren de nue option completes	
	Recurring Rule Update	Imports	
	The scheduled rule update fe Nate: Importing will discard a	where is not enabled. all unawed intrusion policy and network analysis policy edits.	
	Enable Recurring Rule Update	e Imparta 🛛 😠	
	Import Prequency	Daily 1 at 4 1 . All A America/New York	
	Policy Reapply	Reapply intrusion policies after the rule update import completes	
A Design Dates		<ul> <li>Keappy access control posces arear the rule update import completes</li> </ul>	
and a second		Sove Corcel	
07			
Con Contraction of the			
Sto-to-Site V9V			
AGA RegPOWER Configuration			
Device Management			
:			
			PV 21 10



3 [Download new Rule Update from the Support Site]を選択して、その下の2 つのオプションをクリック

4 [Import] をクリック

最新のルール データベースに更新 されます。

[Enable Recurring Rule Update Imports] をクリック

設定オプションが表示されます。

6 自動更新間隔を設定して、その 下の2つのオプションをクリック

デフォルトの [Daily] が推奨です。

- 7 [Save] をクリック
- 8 [Geolocation Updates] タ ブをクリック

地理位置情報データベース更新の 設定画面が表示されます。

9 [Download and install geolocation update from the Support Site] をクリック



10 [Import] をクリック

最新の地理位置情報データベース に更新されます。



[11] [Enable Recurring Weekly] Updates] をクリック

設定オプションが表示されます。



File Vew Tools Wands Window Help Type topic to exarch		
	- 00	ababa
🚳 hore 🖏 Configuration 📴 Montaining 🛄 Save ASA Changes 🔕 Refresh 🕓 Sade 🕥 Torvard 🦻 Help		CISCO
ASA TeefOWER Configur (7: 4     Configuration > ASA TeefOWER Configuration > Identities		۵
Image: Section of the image of the image.		
Recurring Geolocation Updates Exakle favoring weeks gates Update Start Time		
By Service 133 122 By Tread 133 122 By Service 134 By Servi		
t and the second	<b>a</b> 100	1/17 8.51.55 AM UTC

12	自動更新曜日を設定
----	-----------



13 [Save] をクリック



Cisco ASDM はネットワークの管理に役立つ、数々の強力なレポーティングおよびモニタリン グ機能を備えています。ASA Firepower モジュールに関するレポーティングおよびモニタリン グページにアクセスして、「2 セキュリティ ポリシーの設定」で設定した内容が機能している様 子をグラフィカルに確認してみましょう。







### 4-2 モニタリング ページにアクセスする

A FirePOWER Monitori	Hankaring 2.654.0 Anitoring 2.System	•	-
Teck Status Statustics Real Time Eventing	Case-sensitive Exclusion	Nessapes	2 [ASA FirePOWER
	60	Jan 17 2017 04:34:27 Sourcefire3D sudo: parr_unix(sudo:session): session closed for user root	
		Jan 17 2017 04:34:27 Sourcefine3D audo: pern_unit(audo:exession): session opened for user root by (uid=0)	Monitoring] たクリッ
		Jan 17.2017 (H:34:27 SouronfineD) sudo: www: TTY=unknown; #WD=/var/sf/SRU; USDR=rost; COMMAND=/usobin/follog -u admin	wontoning 2799
		Jan 17 2017 04:34:27 Sourcefire2D cudo: part_unix(cudo:cecsion): section closed for user root	
		Jan 17 2017 04:34:27 Sourcefire3D sudo: parr_unio(sudo: session): session opened for user root by (uid=0)	
		Jan 17.2017 D4:34:27 Sourcefre3D sudo: www.: TTY=unknows ; PWD=/var/s6/SRU ; USER=rost ; COMMAND=//softstal/s0/bin/ol_shadow -u admin	
		Jan 17 2017 04:34:27 Sourcefire3D sudo: parr_unix(sudo: session): session closed for user root	
		Jan 17 2017 D4:34:27 Sourcefire3D sudo: part_unix(sudo:session): session opened for user root by (uid+0)	
		Jan 17.2017 D4:34:27 Sourcefre3D sudo: www.: TTY=unknown; PMD=/van/s6/SRU; USER=rost; COMMAND=//sorbin/Tailog -u admin	
		Jan 17 2017 D4:34:27 Sourcefire3D eudo: part_unix(sudo:eession): session closed for user root	
		Jan 17 2017 04:34:27 Sourcefire3D sudo: pars_unio(sudo:session): session opened for user root by (uid=0)	
		Jan 17.2017 D4:34:27 Sourcefre3D sudo: www.: TTY=unknown; FMD=/var/s6/SRU; USER=rost; COMMAND=/var/soul/cf/bin/ol_shadow -u admin	
[iterfaces		Jan 17.2017 D4:34:26 Sourcefine3D SF-IHS[4950]: [4450] IDSEventProcessor: IDSEventProcessor [3WF0] Rushing baskmarks	
VPU		Jan 17 2017 04:33:26 Sourcefire3D last message repeated 2 times	
gebret Traffic Pilter		Jan 17 2017 (H:31:26 SourcefineD) SF-IHS[4950]: [4450] IDSEventProcessor: IDSEventProcessor [INFO] Rushing baskmarks	
Bouting		Jan 17. 2017 (H-101:26 Sourcefire&D SF-IHS[4950]: [4460] IDSEventProcessor (DSEventProcessor [INFO] History baskmarks	
AGA PinePOWER Monitoring		Jan 17 2017 04:30:22 Sourcefire3D sudo: parn_univ(sudo:session): session closed for user root	
g Properties		Jan 17 2017 04:30:22 Sourcefire3D sudo: pam_unix(sudo:session): session opened for user root by (uid=0)	
Logging		Jan 17 2017 04:38:22 Sourcefire3D sudo: www : TTY=utknown ; PWD=/vac/st/SRU ; USER=rost ;	

ASA Tre-FOUND Manhaton _ () + Panhaton _ ASA Tre-FOUND Manhaton _ Series Panhaton _ Series	
Tak State	
Real Time Eventing	Messages
	Jan 17 2017 04:34:27 Sourcefire3D sudo: pers_unix(sudo:session): session closed for user root
	Jan 17 2017 04:34:27 Sourcefire3D sudo: parn_unix(suda:session): session opened for user root by (uid=0)
	Jan 17 2017 D4:34:27 SourcefireSD sude: www.: TTYwasknown.; PWD=/vac/s6/SRU; USBR=rost; COMMAND=/uschin/fallog -u.admin
	Jan 17 2017 04:34:27 Sourcefire3D sudo: parn_unix(sudo:session): session closed for user root
	Jan 17 2017 04:34:27 Sourcefire3D sudo: part_unix(sudo:session): session opened for user root by (uid=0)
	Jan 17 2017 D4:34:27 SourcefireSD sudo: www.iTTY=unknown.jPWD=/var/SDSRU.jUSBR=rost.j COMMAND=/uar/Scal/sbbir/cl_shadow -u admin
	Jan 17 2017 04:34:27 Sourcefire3D sudo: parr_unix(sudo:session): session closed for user root
	Jan 17 2017 04:34:27 Sourcefire3D sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
	Jan 17 2017 D4:34:27 SourcefireSD sudo: www.: TTY=unknown; PWD=/var/st/SRU; USER=root; COMMAND=/usr/bin/fellog =u admin
	Jan 17 2017 04:04:27 Sourcefire3D sudo: parr_unix(sudo:session): session closed for user root
	Jan 17 2017 04:34:27 Sourcefire3D sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
	Jan 17 2017 D4:34:27 SouroefineOD sudo: www.: TTY=unknows ; PWD=/var/st/SRU ; USDR=rost ; COMMAND=/usr0stab350bit/di_shadow =u atmin
Treafaces	Jan 17 2017 B4:84:26 Sourcefire3D SF-IHS[4950]: [4960] IDSEventProcessor: IDSEventProcessor: [INF0] Plushing bookmarks
C vry	Jan 17 2017 04:33:26 Sourcefire3D last message repeated 2 times
Generat Traffic Filter	Jan 17 2017 (M-31:26 Sourcefire3D SF-IHS[4950] [4960] IDSEventProcessor (IDSEventProcessor [INFO] Plushing baskmarks
1 Binting	Jan 17 2017 D4:30:26 Sourcefire3D SF-096[4950]: [4950] IDSE-entProcessor: IDSE-entProcessor: [DSE-entProcessor: [DSE-entProcesso: [DSE-entProcessor: [DSE-entProcesso
AGA FinePOWDR Monitoring	Jan 17 2017 04:30:22 Sourcefire3D sudo: parn_unix(suda:session): session clased for user root
Regneties	Jan 17 2017 04:30:22 Sourcefire3D sudo: part_unix(suda:session): session opened for user root by (uid=0)
1 toseo	Jan 17 2017 D4:30:22 SourcefireSD sudo: www.: TTYwasknown.; PWD=/var/St/SRU; USBR=rost; COMMAND=/usr/bin/fallog -u.admin
:	Last Updated: 1/17/17 9:34:27 49

Jools Waards Mindow Help						Type topic to search	60	abab
Configuration 🕑 Monitoring	Sava ASA Changes 🔇 Refresh	Stack C Form	ord ? Help					cisco
POWER Monitori_ (7 4	Hanikaring > ASA FirePOWER Monito Real Time Exercises	wing > Real Time De	nting		-			0
A Status 1970:5 Il Time Eventing	All AGA FirePOWER Everes	Connection Dribus	on File Molware File Security	Intelligence	-4			×
	II Pause Falseds Ra	5 seconds	• 17 Jan 2017, 9:25 API (0	20151)				:0
	Receive Times	Action	Event Type	Inline Result	Reason	Hennage		
	01/17/2017 9130122 (41	HIGH	ROW PREPORED CORRECTOR					_
	01/17/2017 9:36:22 AM	Allow	ASA FirePOWER Connection					_
	01/1732017 9:35:22 AM	Allow	ASA FirePOWER Connection					
	01/1732007 9:35:15 AM	Bod: with reset	ASA FirePOWER Connection					
	01/17/2017 9:35:15 AM	Block with reset	ASA FirePOWER Connection					
	01/17/2017 9:35:05 AM	Allow	ASA ParePOWER Connection					
	01/17/2017 9:35:04 AM	Alon	ASA ParaPOWER Connection					
	01/17/2017 9:35:04 AM	Allow	AGA PhysPOWER Connection					
	01/17/2017 9:35:04 AM	Alon	ASA ProPOWER Connection					
ficPiter	01/17/2017 9:34:53 AM	Alon	ASA ProPOWER Connection					
	01/17/2007 9-54:40 AM	Block with reset	AGA PersPOWER Connection					
CR Monitoring	01/17/2007 9-34:40 AM	Block with reset	ASA PrePOWER Connection					

fin Cin



4 表示したいモニタ内容をクリック

### お問い合わせ方法

電話または E メールにてお問い合わせください。

Cisco Start テクニカル サポート総合受付窓口

### ■ 0120-092-255

「ご希望の番号を選択してください」という自動音声ガイダンスの後、 電話機のプッシュ番号 3 番 (製品/サービスご購入後の技術的なサポートについてのお問い合わせ)を押します。 続いて 7 番 (シスコ スタート)を押してください。 最後に 3 番 (ワイヤレス製品)を選択してください。

### <sup></sup> E×−ル start-jp@cisco.com

受付時間:平日午前 9 時~午後 18 時(土日祝日は休み) ※時間外のお問い合わせは翌営業日の受付となります。

製品サポート期間:購入元にご確認ください。 ご返答までの目安:受付後、翌営業日までに担当エンジニアよりご連絡いたします。 ※5 営業日を目安に復旧策/回避策をご提供いたします。

#### お問い合わせに必要な情報

お問い合わせの際には、以下の情報をご用意ください。 Eメールでお問い合わせの際には、こちらのテキストと必要事項を記入して送信してください。

#### <ご担当者情報>

- ・ご担当者のお名前(漢字/ふりがな):
- · Cisco.com ID :
- ・会社名(漢字/ふりがな):
- ・住所(漢字/ふりがな):
- 電話番号:
- ・FAX 番号:
- ・E メール アドレス:

#### <製品情報>

- ・シリアル番号:
- 問題の内容:
- ・製品設置先住所(漢字/ふりがな):
- ・サービス契約番号(お持ちの場合のみ):

お問い合わせ先

©2017 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。 本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は 2017 年 6 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。

cisco.

#### シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー http://www.cisco.com/jp