# ClientSecurity/ ServerSecurity(Protection) 14/15 のファイヤーウォール機能について

Client Security14/15、Server Protection(Server Security14以降)に搭載されているファイヤ ーウォール(FW)機能は、Windows FW 機能をコントロールする「管理機能」となります。例えば、 Windows FW を有効/無効化したりルールを追加/削除/無効化する等です。その為独自の F-SecureFW が搭載されていた Client Security(CS)13/Server Security(SS)12以前とは FW ルール メカニズムが異なり、ルールの再検討をせずにバージョンアップを実施した場合、想定通りの動 作が見込めません。また CS13 以前の既存 FW ルールは引き継がれない為、PolicyManager ヘルー ル移行を行うか、PolicyManger でのファイヤーウォール管理を停止する必要があります。

### [ファイヤーウォール適用順の違いについての解説]

CS13/SS12 以前の F-secure ファイヤーウォールは順序を考慮します。ルールは上から下へ順番に チェック/適用され、例えば下図のようにルールを設定した場合、RDP 通信(TCP:3389 使用)は、最 上段の RDP 許可ルールに一致し、その時点で通信許可されます。それ以降のルールはチェックさ れません。ルール最下部に「全ての通信を拒否」(暗黙の Deny)が存在していてもルールはチェッ クされず、リモートデスクトップ通信は成功します。

・CS13/SS12 以前(F-secure 製ファイヤーウォール)



・CS/ SS(SP) 14 以降(Windows ファイヤーウォール)

ー方、ClientSecurity/ServerSecurity(Protection) 14 以降が利用する Windows ファイヤーウ オールは、設定されたルールの順序を考慮せず全てのルールをチェックします。通信に対して複 数のルールが一致した場合、**拒否が優先**されます。その為、ルール最下部に「全ての通信を拒 否」(暗黙の deny)がある場合、RDP 通信施行は失敗します。また、Windows FW に既存の拒否ルー ルが存在している場合も RDP 通信施行は失敗します。当手順では、そういった Windows ファイヤ ーウォール既存ルールついて無効化を行います。



つまり、CS13/SS12 以前のルールをそのまま CS/SS(SP) 14/15 以降に設定しても狙った動作は見 込めません。

[対処方法]下記のどちらかを実施してください。

- PolicyManger で Windows FW 機能コントロール機能を無効にする。
   → "Windows FW 機能コントロール無効化手順 "を実施
- Window FW ルール設定を Policy Manager 経由で行うように設定し、FW ルールを全て移行 する。当シナリオでは、「暗黙の Deny」("許可条件に合致しない通信は全ブロック")を Windows ファイヤーウォールに担当させ Policy Manager に許可ルールのみ登録する手法を 採用しております。
  - → "Policy Manger での FW ルール管理手順"を実施

## [Windows FW 機能コントロール無効化手順]

CS/SS が所属するポリシードメインで下記2点を無効化(チェック解除)してポリシー配布する。 「ポリシーマネージャを使用してファイヤーウォール構成を有効にする」 「Windows firewallを有効にする」

ドメイン ツリーに含まれていないホスト 保留中 (0) 管理されていない (0)	ルート > 設定 > Windows > ファイアウオール	
ドメインッリー	- 📕 Windows	ファイアウォール
<b>Γ</b> Ω μ~Γ	リアルタイム スキヤン	14×/15×クライアント 13×クライアント
	マニュアル スキヤン	□ オリシーマネージャを使用してファイアウオール構成を有効にする 🗗 消去
	スパイウエア制御	
	隔離保存ファイルの管理	/ Mundows firewallを有効にする ┏ <sup>∩</sup> 消去
	> ファイアウオール	クステーションのホストプロフィール: Office, file and printer sharing 🔻 🗗
	ネットワークのアクセス制御	サーバホストプロフィール: Server 🗸 🗗
	アプリケーション制御	□ ワークステーション用のファイアウォール プロフィールを自動的に設定する ┏╹ 消去
	ソフトウエア アップデーター	ワークステーション用のファイアウオール プロフィールの自動選択を設定す。
	データガード	編集中のプロフイール: Office, file and printer sharing (プリセット) × クローン

※インストーラにポリシーを含めるとバージョンアップ直後にWindowsFWが無効化できます。

インストールパッケージ作成ウィザードで「初期ポリシー」に FW 無効化ポリシーを指定。



## [Policy Manger での FW 許可ルール管理手順]

- 1. ポリシーマネージャコンソールの左ベインで設定したいドメインを選択します。
  - DU-F CORPWINCS14BETA Winde
- 右画面の「設定」→「ファイヤーウォール」に移動します。
   「Office, File and printer sharing」から「クローン」をクリックし、自由にカスタムで きる新しいプロフィールを作成します。

編集中のプロフィール:	Office, file and printer sharing (プリセット) 💙	クローン	

※新しいプロフィールとして 〒新レぃプロフィール名 ×	「AAA-Corp」	を作成
新しいプロフィール名		
名前: AAA-Corp		
OK キヤンセル		

3. 「編集中のプロフィール」を「AAA-Corp(範囲)」に切り替えます。

編集中のプロフィール:	Office, file and printer sharing (プリセット) 🛛 👻
	AAA-Corp (範囲)
编集中:   Office	<u>Mobile (プリーート)</u>
□ ファイアウオールが	Office, file and printer sharing (プリセット)
	Server (プリセット)

4. デフォルトルールが下記になっている事を確認します。

デフォルト ルール			
🗌 すべての受信接続をブロック			
不明な受信接続:	ブロック 💙		
不明な送信接続:	ブロック 👻		

5. 「プロフィールにないファイヤーウォールルールをすべて無視する」を有効(チェックを入 れる)します。この設定により Window FW の既存ルールが無効化されます。



6. 「ネットワークサービスを設定する」をクリックします。

	< 🗲	
	🖌 ユニキャスト レスポンスをマ	ルチキャストに許可
4	シトワーク サービスを設定する	
		-
ネッ	トワーク隔離	
	ALLER, AROMARIAN PARTY	0

「ネットワークサービス」が開きます。「追加」をクリックします。
 ネットワークサービス

名前 🔺	プロトコル	イニシエータ ボート	リスポンダ ポート	能用
HTTP	TCP (6)	>1023	80	プリセ
HTTPS	TCP (6)	>1023	443	プリセ
ICMP (1)	ICMP (1)			プリセ
ICMP r	ICMP (1)	3:*,4:*,11:*,12:*		プリセ
ICMPv	ICMPv6 (58)			プリセ
ICMPv	ICMPv6 (58)	128:0		プリセ
ICMPv	ICMPv6 (58)	1:0,1:1,1:2,1:3,1:4,2:*,3		プリセ
ICMPv	ICMPv6 (58)	1:0,1:1,1:2,1:3,1:4,4:0,4		プリセ
Ping	ICMP (1)	8:*		プリセ
RDP	TCP (6)	0-65535	3389	範囲
SMB (	TCP (6)	>1023	445	プリセ
SMB (	UDP (17)	445,>1023	445	プリセ
TCP (6)	TCP (6)	>0	>0	プリセ
UDP (17)	UDP (17)	0-65535	>0	プリセ
Windo	UDP (17)	137-138	137-138	プリセ
	TCP (6)	>1023	139	プリセ

8. 「サービス名」を入力します。 ※RDP と入力しています。

> サービスの名前およびコメントを入力 やすい名前を指定してください。サー い。コメントには、より詳細な内容を

名前: RDP

プロトコルを選択し、「次へ」をクリックします。
 ※一般的には TCP か UDP となり、RDP の場合 TCP です。

.P プロトコル番号 :	TCP (6)	×	

10. 「イニシエータポート」を入力し、「次へ」をクリックします。 ※イニシエータポートは送信(開始)ポートとなります。 ※指定されていない場合、0-65535 を入力してください。RDP の場合は指定は不要。 イニシエータボート: 0-65535

「リスポンダポート」を入力し、「完了」をクリックします。
 ※リスポンダポートは受信ポートとなります。RDPの場合は 3389 となります。

リスポンダ ボート: 3389

12.「ネットワークサービス」にサービスが追加された事を確認し、この画面を閉じます。 ネットワークサービス

$\circ$	名前 🗕	プロトコル	イニシエータ ポート	リスポンダ ポート	範囲
-	POP3	TCP (6)	>1023	110	プリセ
	POP3 (SSL)	TCP (6)	>1023	995	プリセ
	Radius	UDP (17)	>1023	1812	プリセ
$\boldsymbol{<}$	RDP	TCP (6)	0-65535	3389	範囲
_	Remote Desktop	TCP (6)	>1023	3389	プリセ

13. 「ファイヤーウォールルール」の画面で、「ルールを追加」をクリックします。

=> TCP (6) 3	5
⇒ UDP (17)	
⇒ Ping 3	5
CMP restricted	
	COP (17)     Ping     COP restricted     COP restricted

14.「名前」(RDP)「タイプ」(許可)を入力し、「次へ」をクリックします。 ルールのタイプ

ルール名とタイプを指定します。

名前:	RDP			
タイプ:	許可	V		

15.「追加」をクリックします。



16. 空白のサービスが追加されます。



17.「サービス」フィールドをダブルクリックし、追加したいサービスを選択します。
 ※ 先程追加したサービス「RDP」を選びます。

ルールが適用されるネットワーク サービスを指定します。



18.「方向」フィールドで[着信/発信/両方]のどれかを選択し、「次へ」をクリックします。

サービス	方向
Remote Desktop	着信 🛛 🖌 🖌
	着信
	発信
	両方

※RDP 接続を受ける側は「着信」を選びます。

19.「全てのリモートアドレス」を選択し「次へ」をクリックします。 リモート アドレス

トラフィックを許可またはブロックするホストまたはネットワークを指定し ます。デフォルトでは、ルールはすべてのリモート アドレスに適用されます
<u> <u> </u> <u> </u></u>
○ プリセットのコンピュータ:
デフォルトのゲートウェイ \vee
○ 塩定したリモート ホスト:

20. デフォルト設定のまま、「完了」をクリックします。 範囲



21.「ファイヤーウォールルール」にルールが追加された事を確認します。

2	RDP	許可	[適用] : RDP	すべてのリモート ホスト	すべてのネットワーク
			[週用]:Windows Networking (2) [適用]:SMB (TCP) [谪用1:SMB (UDP)		
$\checkmark$	Allow inbound computer browsing and file sharing from local subnet	許可	[適用]: Windows Networking (1)	ローカル サブネット	すべてのネットワーク
			[適用]:ICMPv6 restricted in [除外]:ICMPv6 restricted out		
	Allow commonly needed ICMP messages	許可	[除外]:Ping [適用]:ICMP restricted	すべてのリモート ホスト	すべてのネットワーク
	Allow all outbound traffic	許可	[除外] : TCP (6) [除外] : UDP (17)	すべてのリモート ホスト	すべてのネットワーク
有効	名前	タイプ	サービス	リモート ホスト	ネットワークタイプ

22. デバイスに適用するファイヤーウォールプロフィールを指定します。
 ※ 今回作成した「AAA-Corp」を選びますが既に切り替わっている場合は不要です。

一般				
😽 Windows firewa	訓を有効にする ⊡			
ワークステーション	∕のホストプロフィ <del>〜</del>	AAA-Corp		⊡ 消去
サ <del>ー</del> バ ホスト プロ	フィール:	Server	×	ď

23. ポリシーを配布します。



24. 管理クライアント(CS/SS)側の Window ファイヤーウォール管理画面-詳細設定-受信の規則 に、RDP(Remote Desktop in)が存在している事を確認してください。

■ セキュリティが強化された Windows	Defender ファイアウォール								
ファイル(F) 操作(A) 表示(V)	ヘルプ(H)								
💠 🏟 🖄 📷 🗟 🛙 🛅									
🔗 ローカル コンピューター のセキュリティ	: 受信の規則								
受信の規則	名前	グループ	プロファイル	有効	操作	優先	プログラム	ローカル アドレス	Uf- ^
接続セキュリティの規則	Allow inbound computer browsing and file sharing from local subnet (Windo	F-Secure Firewall	すべて	はい	許可	いいえ	任意	任意	0-;
> 見. 監視	SF-Secure: Allow DHCP (In)	F-Secure Firewall	すべて	はい	許可	いいえ	%System	任意	任意
	SF-Secure: Allow DHCP IPv6 (In)	F-Secure Firewall	すべて	はい	許可	いいえ	%System	任意	任意
	Secure: Allow DNS (In)	F-Secure Firewall	すべて	はい	許可	いいえ	%System	任意	任意
(	RemoteDeskTop (Remote Desktop:in) (F-Secure)	F-Secure Firewall	すべて	はい	許可	いいえ	任意	任意	任意
			+				2	1	1

25. 「F-Secure Firewall」グループ以外が無効(緑色のチェックが無い)である事を確認する。

ター のセキュリテ	右 受信の規則								
	名前	グループ	70771%	有効	操作	便先	プログラム	ローカル アドレス	ルモー
LORE	Allow inbound computer browsing and file sharing from local subnet (Windo	F-Secure Firewall	3778	121.1	許可	いいえ	任意	任意	0-:
THERE	G F-Secure: Allow DHCP (In)	F-Secure Firewall	すべて	1211	許可	wit	%System_	任意	任意
	G F-Secure: Allow DHCP IPv6 (In)	F-Secure Firewall	すべて	1211	許可	unt	%System_	任意	任業
	G F-Secure: Allow DNS (In)	F-Secure Firewall	すべて	(21)	許可	いいえ	%System_	任意	任業
	RemoteDeskTop (Remote Desktopsin) (F-Secure)	F-Secure Firewall	すべて	1211	許可	UNI	任業	任實	任業
	Gene ba	Came bar	すべて	UNT	許可	UNT	任意	任意	任意
1	Google Chrome (mDNS-In)	Google Chrome	TAT	いいえ	許可	unt	C-YProgr.	任意	任意
	Google Chrome (mDNSインパウンド)	Google Chrome	\$1C	いいた	許可	いいえ	CHProgr	任意	任日
	Groove Music	Groove Music	FX-7.7.	いいえ	許可	いいえ	任意	任意	任意
	iSCSI サービス (TCP 受信)	iSCSI サービス	FX42	いいえ	許可	いいえ	%System	任章	任意
	iSCSi サービス (TCP 受信)	iscsi サービス	ブライバートー	11112	許可	UNI	%System_	任意	0-;
	Mail and Calendar	Mail and Calendar	すべて	いいえ	許可	unt	任意	任意	任意
	mDNS (UDP 受信)	mDNS	FX4V	いいえ	許可	いいえ	C-WIND	任意	任意
	mDNS (UDP 受信)	mDNS	プライベート	いいえ	許可	UUX	CWWND.	任意	0-
	mDNS (UDP 受信)	mONS	パブリック	unt	許可	いいえ	CWWIND	任意	0-
	Media Center Extender - HTTP ストリーミング (TCP-In)	Media Center Extender	すべて	UNT	許可	unt	System	任意	0-1
	Media Center Extender - gWave (TCP 受信)	Media Center Extender	すべて	いいえ	許可	いいえ	%System_	任意	0-3
	Media Center Extender - gWave (UDP 受信)	Media Center Extender	すべて	いれた	許可	いいえ	%System_	任意	0-3
	Media Center Extender - RTSP (TCP 受信)	Media Center Extender	3/17	いれえ	許可	いいえ	%System_	任意	0-
	Media Center Extender - SSDP (UDP 受信)	Media Center Extender	3/1	いいえ	(中市)	ULIZ	%System_	任意	0-
	Media Center Extender - WMDRM-ND/RTP/RTCP (UDP 受信)	Media Center Extender	\$1.2	unt	許可	unt	%System_	任意	0-
	Media Center Extender - XSP (TCP 受信)	Media Center Extender	TAT	UUR	(19月)	unt	%System_	任意	0-
	Media Center Extenders - Media ストリーミング (TCP-In)	Media Center Extender	すべて	UNE	許可	いいえ	System	任意	0-3
	Microsoft Edge	Microsoft Edge	FX12.7.	いいえ	許可	いいえ	任意	任實	任言
	Microsoft Edge	Microsoft Edge	FX17, 7	UNT.	許可	いいえ	任意	任意	任書
	Microsoft Edge	Microsoft Edge	FX17, J	LULT	許可	いいえ	任意	任意	任常
	Microsoft Messaging	Microsoft Messaging	すべて	いいえ	許可	UUX	任意	任意	(±1
	Microsoft Photos	Microsoft Photos	すべて	1112	許可	いいえ	任意	任意	任意
	Microsoft Solitaire Collection	Microsoft Solitaire Collection	FX17, 7	UN	許可	unt	任意	任意	任何
	Microsoft Solitaire Collection	Microsoft Solitaire Collection	FX17, 7	いいえ	許可	いいえ	任意	任意	任日
	Microsoft Solitaire Collection	Microsoft Solitaire Collection	FX17, 7	1112	許可	white	任意	任意	任日
	Microsoft Sticky Notes	Microsoft Sticky Notes	FX47, 7	unt	許可	LULIZ	任意	任意	任日
	Microsoft Sticky Notes	Microsoft Sticky Notes	FX17.7	kuu.	許可	UNT	任意	任意	任
	Microsoft Store	Microsoft Store	すべて	UNT	許可	いいえ	任意	任章	<b>E</b>
	Mahila Wane	Mahila Blanc	ENTYT	11114	-	Aste B	14.00	11.00	15.4

#### 補足事項

(補足事項1)当手法を行うことで既存のWindows ファイヤーウォールルールの設定を変更し、既存のアプリケーション通信に影響を与える可能性がございます。あらかじめお使いのコンピュータに必要な通信(IPアドレス/ポート番号/etc)を把握した上で当手法をお試しください。また、遠隔地での操作の場合、誤ったファイヤーウォール設定を行うことで操作ができなくなる可能性があります。現地での作業をお勧め致します。

(補足事項 2) Windows ファイヤーウォールはポリシーのインポート/エクスポート、既定のポリシーの復元機能を備えております。Computer Protection での設定変更前のポリシーをエクスポートしておく事で設定ミスが発生した場合でも設定の復元が可能です。



※コントロールパネル→ファイヤーウォール→詳細設定→ポリシーのエクスポート/インポート ※「Window ファイヤーウォールのルール無効化手順」をチェックした、「プロフィールにないフ ァイヤーウォールルールをすべて無視する」のチェックを解除する事でも既存 WindowsFW を再度 有効化できます。

(補足事項 3) Windows Firewall は Microsoft 社製品のコンポーネントとなります。詳細なご案内については Microsoft 様でのサポートを受けていただくようお願いいたします。

(補足事項 4) Active Directotry のグループポリシーや Windows のローカルポリシー(GPO)で Windows ファイヤーウォールを有効/無効に設定している場合、Client Security は Windows ファ イヤーウォールをコントロールできません。ActiveDirectory やローカルポリシー(GPO)での管理 をお願いします。