Linux 製品のパターンファイルファイルのリセット方法について教えてください

質問 - Linux 製品のパターンファイルファイルのリセット方法について教えてください

回答 - 各Linux 製品によってパターンファイルのリセット方法が異なります。手順は以下。

<アンチウイルス Linux ゲートウエイ v5.xx の場合>

cd /opt/f-secure/fsigk; make stop

ps -efl | grep fsupdated（更新関連のプロセス（fsupdated）の起動状態を確認します）

kill ＜残っている fsupdated プロセスの PID＞（残っている場合、強制終了を行います）

rm -rf /opt/f-secure/fsigk/fsaua/data/content/*

cd /opt/f-secure/fsigk; make start

/opt/f-secure/fsigk/dbupdate　（外部接続可能な環境）

または

/opt/f-secure/fsigk/dbupdate fsdbupdate9.run
（非インターネット環境/fsdbupdate9.run 最新版を別途入手）

<ポリシーマネージャサーバ(Ver12.40 以前)の場合>

/etc/init.d/fsaua stop

/etc/init.d/fspms stop

（プロセスの完全停止を確認すること）

rm -rf /var/opt/f-secure/fsaua/data/content/*

rm -rf /var/opt/f-secure/fsaus/data/db

rm -rf /var/opt/f-secure/fsaus/data/misc

rm -f /var/opt/f-secure/fspms/logs/fspms-fsauasc.state

rm -f /var/opt/f-secure/fsaua/data/subscriptions/*

/etc/init.d/fsaua start

/etc/init.d/fspms start

sudo -u fspms /opt/f-secure/fspms/bin/fsavupd --debug　（外部接続可能な環境）

または

./fsdbupdate9.run　（非インターネット環境/fsdbupdate9.run 最新版を別途入手）

※fspms サービスを停止させても、現在処理中の場合には stop コマンド終了後もサービスが停止していない場合があります。このため、stop コマンド完了後、プロセスの停止を ps コマンドで確認してください。

※外部接続可能な環境において最後に実行する fsavupd コマンドは、cron で定期的に実行されるジョブとして登録されています。このため、そのジョブの実行を待てば手動で実行する必要はありません。今直ぐ更新したい場合に実行してください。多重実行による不要な負荷の発生を防ぐため、ジョブの実行時刻を確認することをお勧めします。

<ポリシーマネージャサーバ(Ver13.00 以降)の場合>

/etc/init.d/fspms stop （※プロセスの完全停止を確認すること）

rm -rf /var/opt/f-secure/fspms/data/guts2/*

/etc/init.d/fspms start

※fspms サービスを停止させても、現在処理中の場合には stop コマンド終了後もサービスが停止していない場合があります。このため、stop コマンド完了後、プロセスの停止を ps コマンドで確認してください。

<Linux Security64/Linux Protection の場合>

Linux Security64/Linux Protection では機能向上されたパターンファイル更新機能により、パターンファイルリセットが必要な事態が想定されておりません。

<Linux セキュリティ 11.xx フルエディションの場合>

/etc/init.d/fsma stop

/etc/init.d/fsaua stop

ps -efl | grep fsupdated（更新関連のプロセス”fsupdated”の起動状態を確認します）

kill ＜残っている fsupdated プロセスの PID＞（残っている場合、強制終了を行います）

rm -rf /var/opt/f-secure/fsaua/data/content/*

/etc/init.d/fsaua start

/etc/init.d/fsma start

dbupdate （外部接続可能な環境）

または

dbupdate fsdbupdate9.run （非インターネット環境/fsdbupdate9.run 最新版を別途入手）

<Linux セキュリティ 11.xx コマンドラインエディションの場合>

/etc/init.d/fsaua stop

/etc/init.d/fsupdate stop

ps -efl | grep fsupdated（更新関連のプロセス（fsupdated）の起動状態を確認します）

kill ＜残っている fsupdated プロセスの PID＞（残っている場合、強制終了を行います）

rm -rf /var/opt/f-secure/fsaua/data/content/*

/etc/init.d/fsaua start

/etc/init.d/fsupdate start

dbupdate　（外部接続可能な環境）

または

dbupdate fsdbupdate9.run　（非インターネット環境/fsdbupdate9.run 最新版を別途入手）

外部接続可能な環境で fsaua を起動すると、必要な最新パターンファイルのダウンロードが自動的に開始されます。ここで行う dbupdate コマンドは更新状況確認が目的です。dbupdate コマンド自身はデフォルトで 15 分のタイムアウトを持っており、更新が 15 分以内に完了しない場合、dbupdate コマンドは終了してしまいますが、更新自身はバックグラウンドで継続して行われていますので、dbupdate コマンドの終了は影響ありません。この場合、再度 dbupdate コマンドを実行すると、引続きバックグラウンドで実行されている更新状況の確認が行えます。