CryptoAuditor – McAfee Web Gateway 連携

SFTP を悪用したウイルス送信の防止

2014 年 6 月 25 日

重要なファイルを転送する場合、通信経路上での情報漏えいを防ぐ為、暗号化された SFTP を用いて通信内容を秘匿します。しかし、暗号化による強力な秘匿性が、皮肉にも重要なサーバーへのウイルス転送の隠ぺいに悪用され、重大なインシデントに繋がる事案が世界中で発生しています。

SSH Communications Security 社製品 CryptoAuditor は、ウイルススキャンサーバと連携し、これまで不可能とされた暗号化ファイル転送においても、通信経路上でのウイルススキャンを実現します。

本書では SSH Communications Security 社製品 CryptoAuditor(以下 CrA)と McAfee 社 McAfee Web Gateway(以下 MWG)の Data Loss Prevention(DLP)ウイルススキャン機能を連携し、SFTP により転送されるウイルスを検知する簡便な手法についてのテスト結果を紹介します。

1. MWS を介した SFTP 転送

図 1-1 の通り、サーバーに MWS を経由し SFTP でアクセス出来る環境を用意しました。

図 1-1. 基本構成

SFTP クライアントにはウイルスチェックテスト用のファイルとして図 1-2 の内容が記述された"eicar.com.txt"を保存しています。また、MWS には、"eicar.com.txt"をウイルスとして検出し、アップロードを阻止するよう、ウイルススキャン機能の設定を行いました。

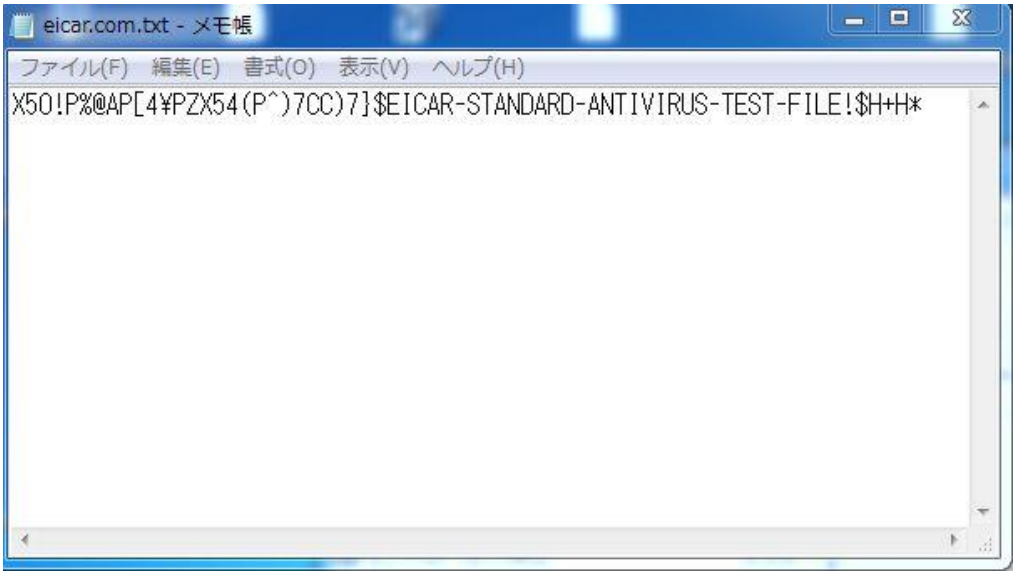

図 1-2. テスト用ウイルスファイル

この環境下で SFTP クライアントから SFTP サーバーに対し、SFTP でアクセスを行い、"eicar.com.txt"のアップロードを試みます。

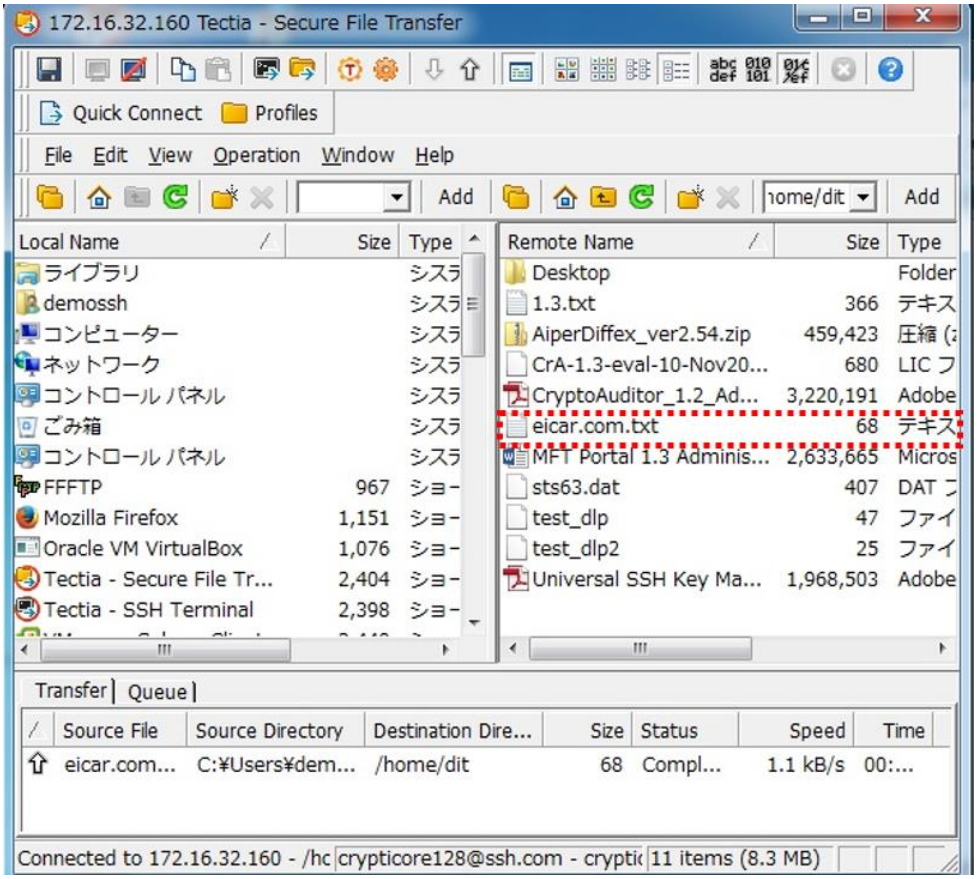

図 1-3. SFTP でのアップロード実行結果

図 1-3 の通り、本来ウイルスとして検出されるべき”eicar.com.txt”のアップロードが成功しました。

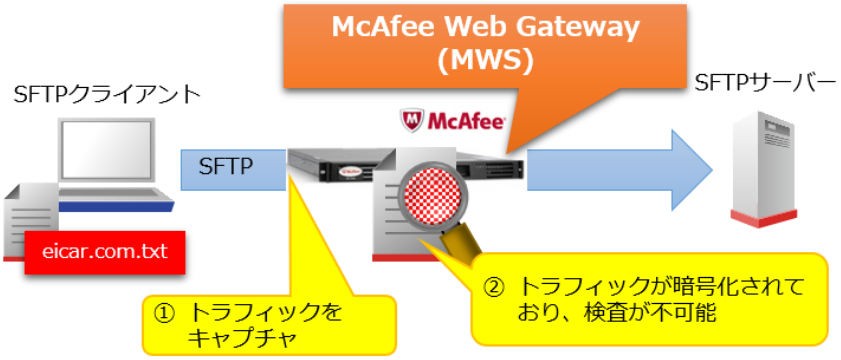

図 1-4. 実際の動作

SFTP で暗号化されたファイル転送は、通信経路上での情報漏えいを防止しますが、その内容を経路上で検知、及び制限出来ません。本項の検証においても、図 1-4 の通り、MWS はトラフィック内のウイルスを検出出来ず、正常にファイル転送が完了されてしまうことが確認できました。その為、ウイルスの検出及び排除を行う為には、アップロード後にサーバーにインストールされたウイルススキャンプログラムのみで行う必要があります。

2. CrA を介した SFTP 転送

次に、図 2-1 の通り、SFTP クライアント、SFTP サーバー、及び MWS のウイルススキャン機能の設定は前項より変えず、CrA を経由した環境を用意しました。CrA にはインスペクション機能を用いて MWS へ ICAP でトラフィックを転送する設定を行いました。

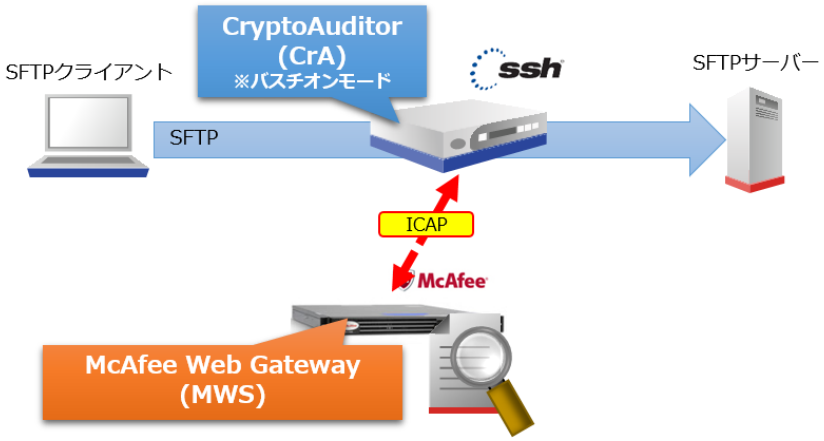

図 2-1. 検証環境

前項と同様に、SFTP クライアントから SFTP サーバーに対し、SFTP でアクセスを行い、”eicar.com.txt”のアップロードを試みます。

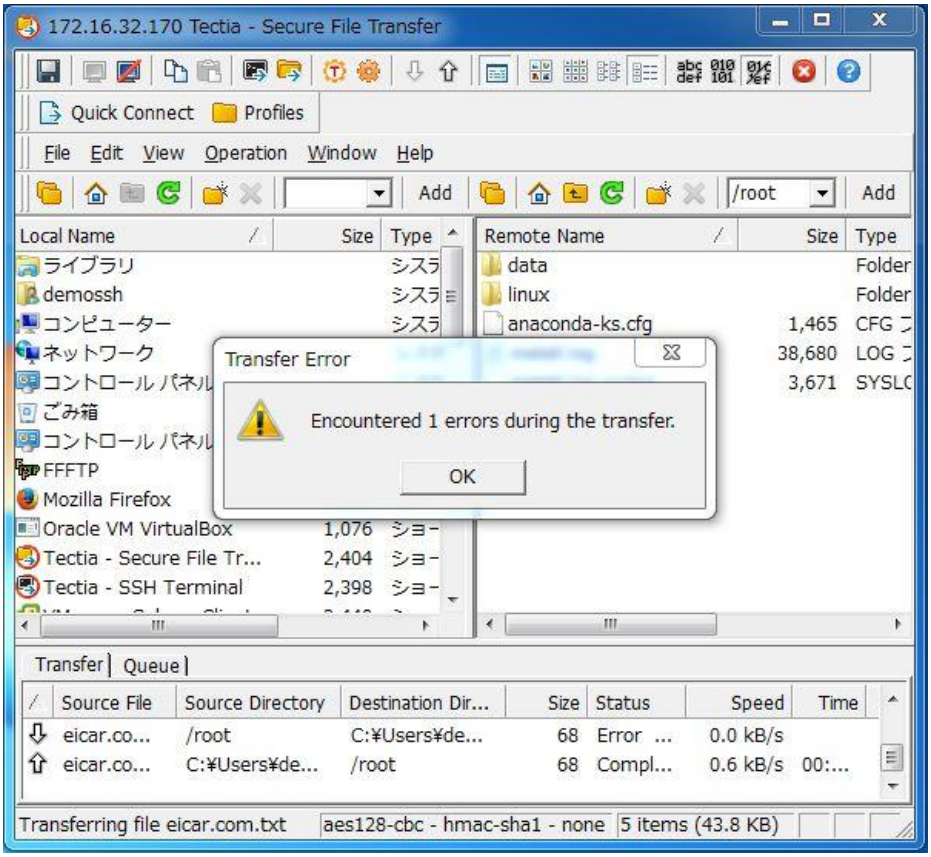

図 2-2. SFTP でのアップロード実行結果

図 2-2 の通り、エラーメッセージが表示され、”eicar.com.txt”のアップロードは出来ませんでした。

図 2-3. 実際の動作

図 2-3 の通り、SFTP によって暗号化された通信は CrA のインスペクション機能により、MWS へ ICAP で転送され、MWS のウイルススキャン機能により検査されます。アップロードされるファイルがウイルスであると判断された場合、CrA に対して遮断を要求、アップロードを阻止しています。

以上