CryptoAuditor – McAfee Web Gateway 連携

暗号化(SSH)通信を悪用した情報漏えいの検知

2014 年 6 月 25 日

一般的に重要なデータ通信は、通信経路上での情報漏えいを防ぐ為、SSH や SFTP などの暗号化プロトコルを用いて、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不正操作（攻撃）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、コンテンツ検知システムと連携し、これまで不可能とされた暗号化通信においても、通信経路上での不正操作の検知を実現します。

本書では SSH Communications Security 社製品 CryptoAuditor(以下 CrA)のインスペクション機能と McAfee 社 McAfee Web Gateway(以下 MWG)の Data Loss Prevention(DLP)アラート機能を連携し、SSH 及び SFTP のトラフィック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. root 権限による SSH アクセス

図 1-1 の通り、SSH によりアクセスが可能なサーバーと管理者 PC による基本的な SSH 環境を用意しました。サーバーにはクレジットカード番号を想定した”XXXX-XXXX-XXXX-XXXX”形式のランダムな数字を複数行記述したファイルが保存されています。

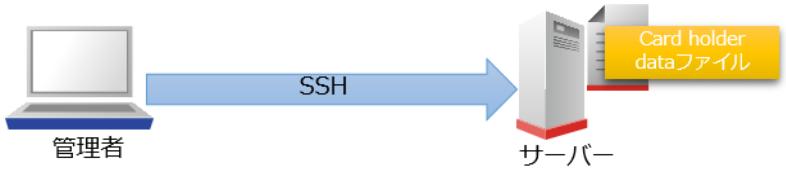

図 1-1. 基本構成

この環境下で管理者 PC の CLI よりサーバーに対して root 権限での SSH アクセスを行い、”cat”コマンドにより、Card holder data ファイルの内容の閲覧を試みます。

```
[root@demo data]# ls
card_data
[root@demo data]# cat card_data
card_holder_data

1_1234-5678-9012-3456 XXXX
2_2345-6789-0123-4567 XXXX
3_3456-7890-1234-5678 XXXX
4_4567-8901-2345-6789 XXXX
5_5678-9012-3456-7890 XXXX
6_6789-0123-4567-8901 XXXX
7_7890-1234-5678-9012 XXXX
8_8901-2345-6789-0123 XXXX
9_9012-3456-7890-1234 XXXX
0_0123-4567-8901-2345 XXXX
11_1111-1111-1111-1111 XXXX
12_2222-2222-2222-2222 XXXX
13_3333-3333-3333-3333 XXXX
14_4444-4444-4444-4444 XXXX
15_5555-5555-5555-5555 XXXX
16_6666-6666-6666-6666 XXXX
17_7777-7777-7777-7777 XXXX
18_8888-8888-8888-8888 XXXX
19_9999-9999-9999-9999 XXXX
20_0000-0000-0000-0000 XXXX
[root@demo data]#
```

図 1-2. CLI による実行結果画面

図 1-2 の通り、問題なく、ファイルの内容であるクレジットカード番号を CLI 上で閲覧出来ました。

SSH は暗号化されておりますので、通信経路上での情報漏えいを防止しますが、その通信内容が正常な操作で無いことを経路上で検知、及び制限出来ません。もし、SSH による操作を制限する場合、端末上に監視や制限を行うソリューション(エージェント型)を導入する必要がありますが、管理者が root 権限を持つ限り、その効果に疑問が残ります。

2. CrA を介した root 権限による SSH アクセス

次に、図 2-1 の通り、管理者 PC やサーバーの設定は前項より変えず、CrA 及び MWS を追加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設定し、取得したトラフィックを ICAP により MWS へ転送します。

MWS には、DLP 機能を利用してクレジットカード番号を検知するよう、正規表現を用いた条件を設定しています。管理者は CrA を経由してサーバーに接続します。

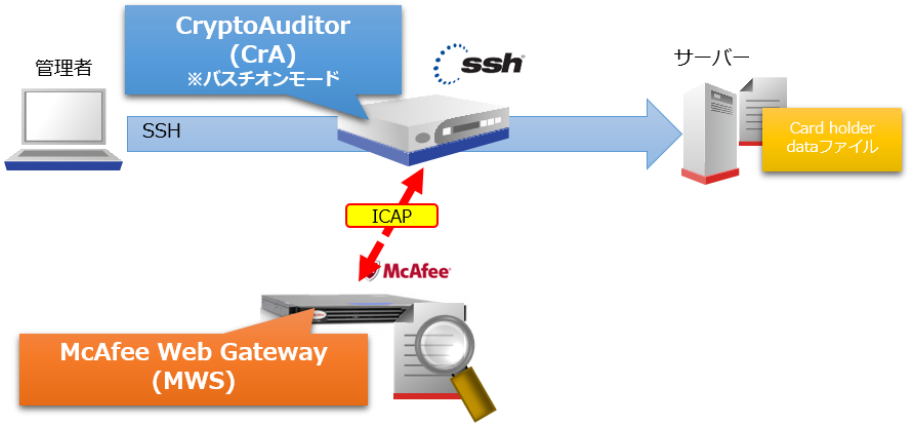

図 2-1. 検証環境

前項と同様に、管理者 PC の CLI よりサーバーに対して root 権限での SSH アクセスを行い、"cat"コマンドにより、Card holder data ファイルの内容の確認を試みます。

```
[root@demo data]#
[root@demo data]# ls
card_data
[root@demo data]# cat card_data
ICAP/1.0 200 OK
ISTag: "00002705-.132.250-00007358"
Encapsulated: res-hdr=0, res-body=172

HTTP/1.1 403 DefaultErrorTemplate
Via: 1.1 255.255.255.255 (McAfee Web Gateway 7.3.2.4.0.16508)
Content-Type: text/html
Cache-Control: no-cache
Content-Length: 2404

964
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.or
g/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<!-- FileName: index.html
     Language: [en]
-->
<!--Head-->
<head>
  <meta content="text/html; charset=UTF-8" http-equiv="Content-Type">
  <meta http-equiv="X-UA-Compatible" content="IE=7" />
```

図 2-2. CLI による実行結果画面

図 2-2 の通り、エラーメッセージが表示され、ファイルの内容は閲覧出来ませんでした。MWS の DLP 機能が正常に動作し、SSH によるアクセスからクレジットカード番号の漏えいを防止しています。

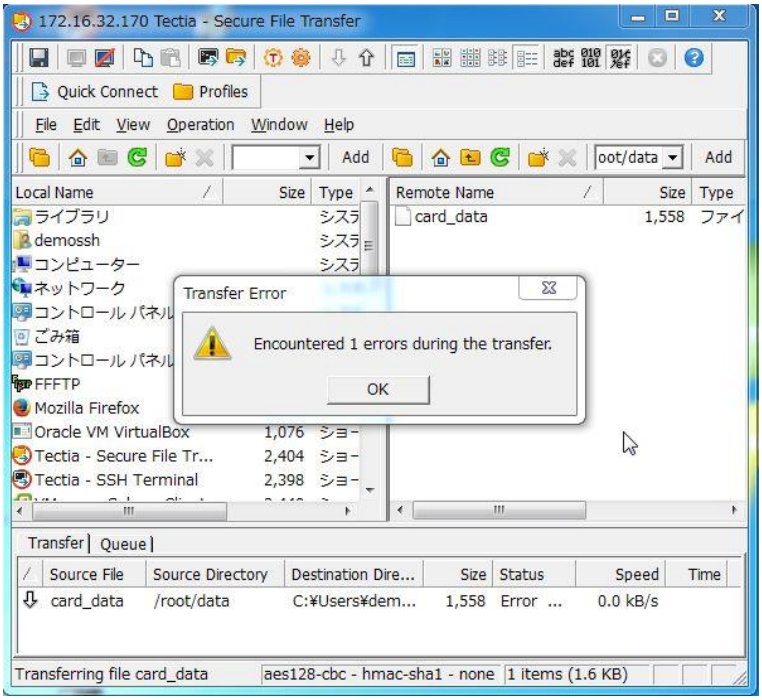

図 2-3. SFTP でのダウンロード実行結果

また、同じ環境で、SFTP を用いて Card holder data ファイルのダウンロードを試みた場合、図 2-3 の通り、MWG 側で拒否されました。

図 2-4. 実際の動作

図 2-4 の通り、SSH 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 DLP 機能により検査されます。検査でクレジットカード番号が含まれたファイルであると判断された場合、CrA に対して遮断を要求、ファイルの閲覧を阻止しています。

以上