お客様の事例

# MicroSoftのメールサーバにメールが送信できなくなる

【目次】



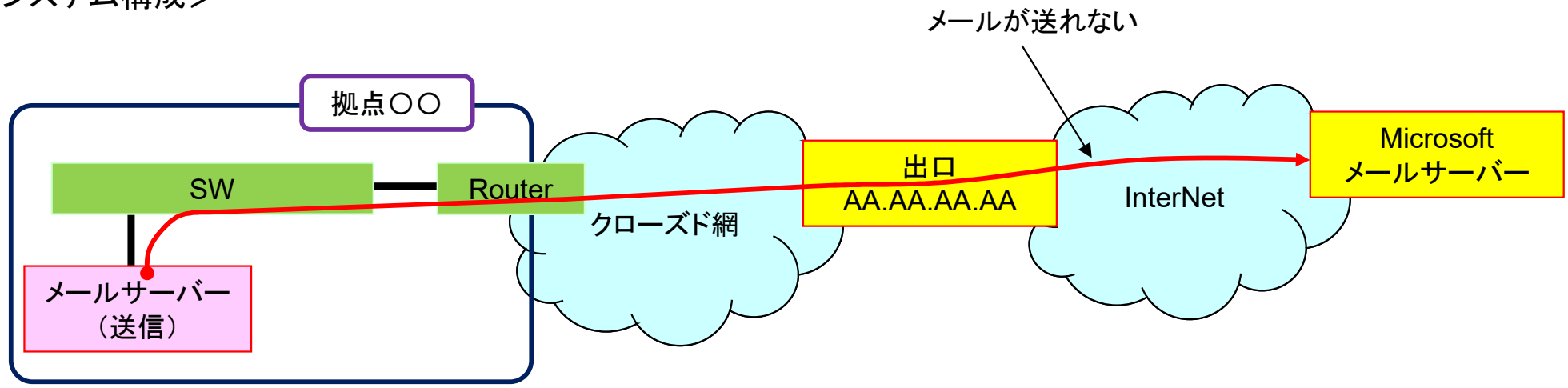

アイティエスコンサルティング株式会社


2022/ 05/ 16

# 1．概要（システム構成）

ある日突然、お客様のロケーションに設置されたメールサーバーから、Micro Softのメールサーバーにメールが送信できなくなりました。

＜システム構成＞



メールサーバのlogより
https://www.spamhaus.org/ のサイトを参照のこと

https://check.spamhaus.org/ のサイトで、spam mail の Block List に該当のIPが載っているかどうかを検索できる。
このサイトで検索すると InterNetの出口 AA.AA.AA.AA が リストに載っていることが判明


**Why was this IP listed?**

This IP is making SMTP connections with HELO values that indicate a problem.

The HELOs that it is connecting with are as follows:

**Technical information**

(IP, UTC timestamp, HELO value)

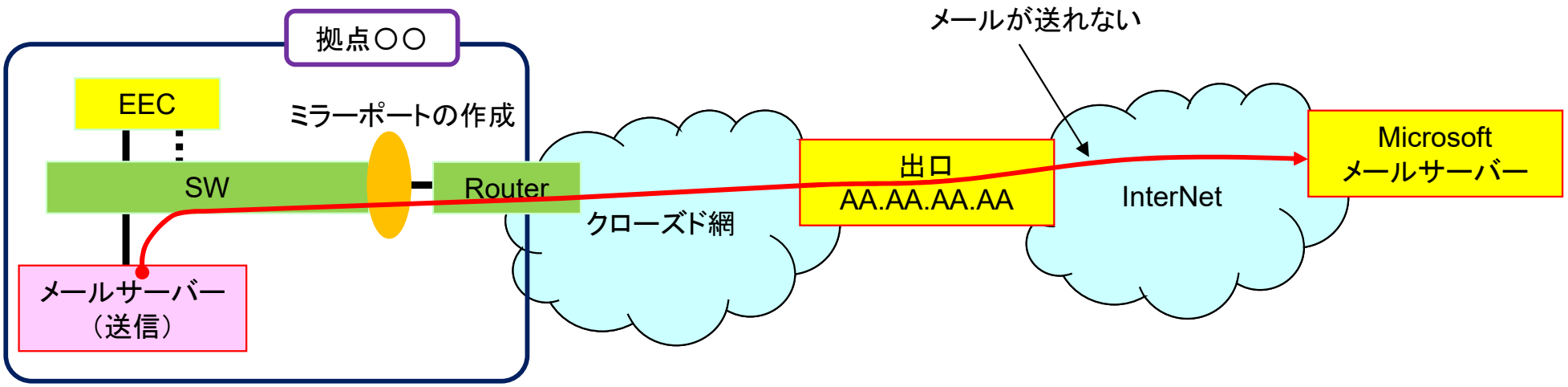
AA.AA.AA.AA 2022-03-19 00:10:00 111[redacted]net

AA.AA.AA.AA 2022-03-15 11:00:00 188-[redacted]rs

Notable things about the HELOs:

UTC時間
2022-03-19 00:10:00
2022-03-15 11:00:00 に
AA.AA.AA.AA のIPから、不適切は HELO値が発出されたことが判明

【補足】
不適切なHELO値が送られて3日程すると、このBlock Listからリストが除外され、
（3日後には）メールの送信が可能となりました。




（1） メールサーバーにて、不適切なHELO値を出していないか確認 ⇒ 出していないことを確認

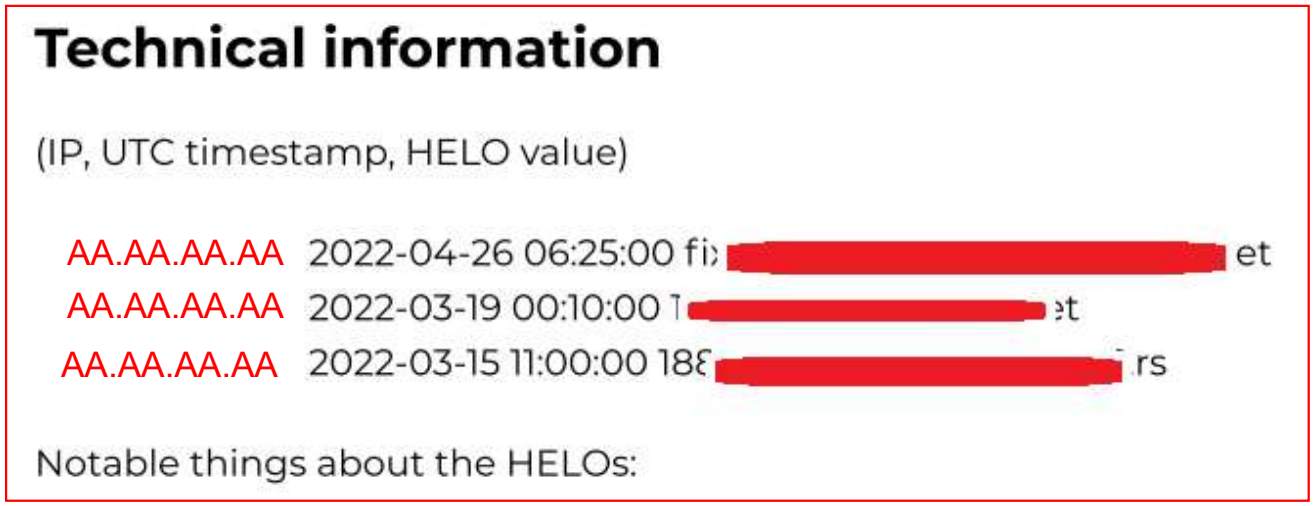
（2） パケットキャプチャーの実施
EECを設置し、
拠点〇〇にて、 ミラーポートを作成し、パケットキャプチャーを実施
全パケットでは、膨大な容量となるため
メールのプロトコルの 25port にフィルターをかけて、パケットキャプチャを実施
ポイント ： 連続取得が必須

【補足】
実際は、拠点〇〇 以外にも、もう1拠点 同様のパケットキャプチャーを行いました。

⇒ 暫く様子をみましたが、再度メールが送信できない事象が発生しました。

（1） Block List の掲示確認

https://check.spamhaus.org/ のサイトで、spam mail の Block List に該当のIPが載っているかどうかを検索
このサイトで検索すると InterNetの出口 AA.AA.AA.AA が 再度、リストに載っていることが判明




← 追加される

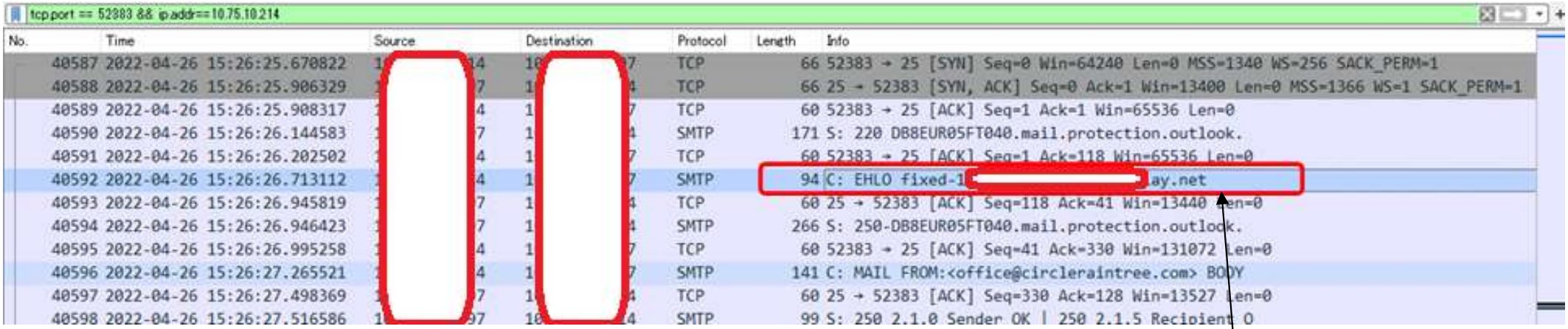
UTC時間 2022-04-26 06:25:00 に 不適切なHELO値の送信があったとの表示

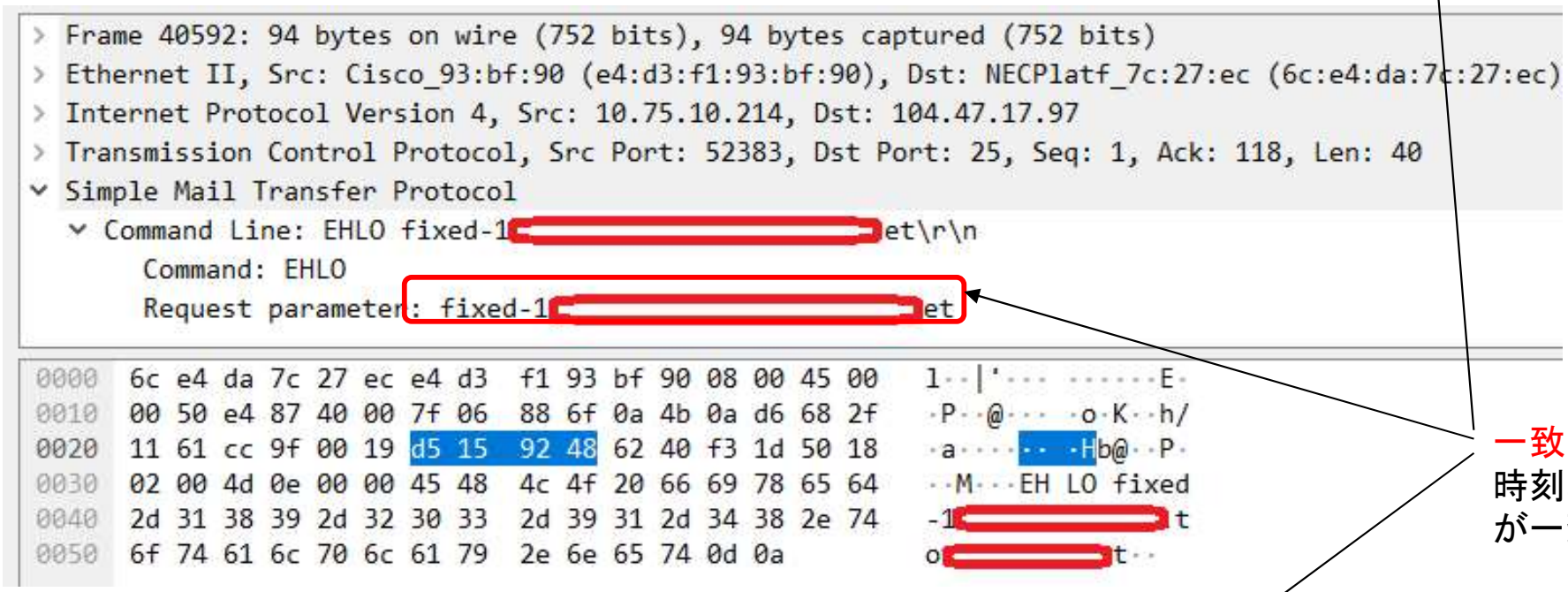
（2） パケットキャプチャーのlog解析
UTC時間 2022-04-26 06:25:00 すなわち、JST時間 4/26（火）15:25 ごろに、
余裕をみて、 4/26 15:20～ 15:39 までのパケットを抽出

| 行数 | IP | |
|---|---|---|
| 105 | BB.BB.BB.BB | ⇒ 105 CC.CC.CC.CC.smtp: の通信は特に問題なし |
| 440 | DD.DD.DD.DD | の機器が、以下のMicrosoftの機器とメールを送受信しています。 |
| 417 | Microsoft | DD.DD.DD.DDとの通信 ← **今回 この部分を深堀調査** |
| 12 | Microsoft | DD.DD.DD.DDとの通信 |
| 6 | Microsoft | DD.DD.DD.DDとの通信 |
| 4 | Microsoft | DD.DD.DD.DDとの通信 |

（3） WireSharkを利用した分析

tcp.port == 52383 && ip.addr==DD.DD.DD.DD　で絞込

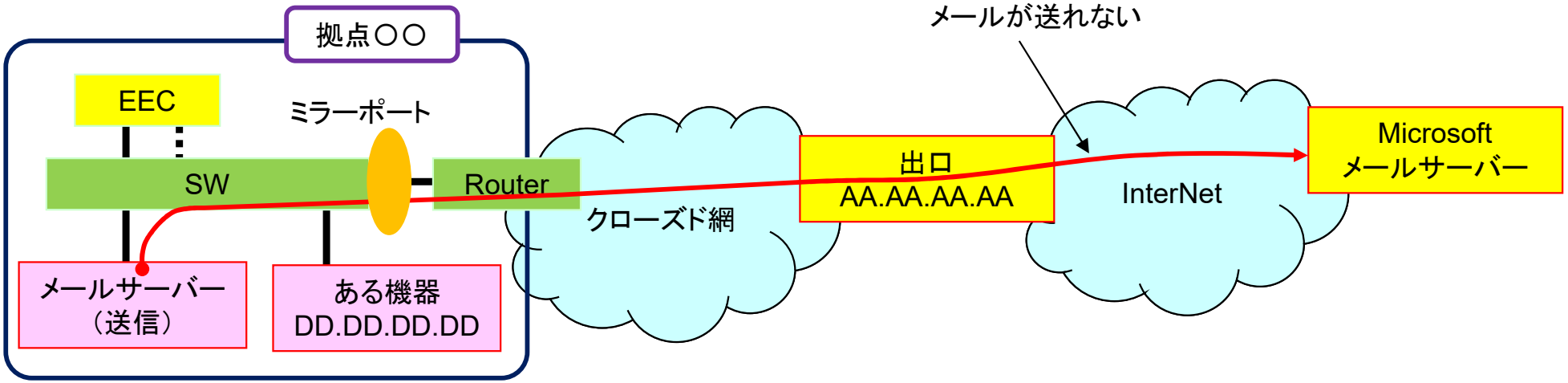



一致しています。
時刻とHELO値
が一致しています。

(IP, UTC timestamp, HELO value)
DD.DD.DD.DD　2022-04-26 06:25:00 xx.xx.xx.xx.xx.xx.xx.xxet　← 今回
UTC 時間 4/26 06:25:00　HELO値が　適切でないとあります。

# 5. まとめ




メールサーバとして使用していない　ある機器（DD.DD.DD.DD)が不適切な通信をしていることが判明しました。

この機器は、DHCPでIPが振られる業務用PCであり、メールサーバとしの利用はしていないことから、
この機器の詳細調査を実施することになりました。

今回のように、フィルターをかけたパケットキャプチャーは、原因の究明に有効です。
また、機器にlogをして情報を入手する等のカスタマイズ試験も、原因の究明には有効です。
カスタマイズ試験：https://its-consul.co.jp/itsr/customize_test.html

【補足】
　迷惑メール防止は、各Sier（メールサーバー管理者）により、迷惑メールを判断するアルゴリズムが異なります。
このアルゴリズムは公開されていたいため（公開すると、それを掻い潜る迷惑が発生するためか？）、注意が必要です。
今回、Microsoftのメールサーバーには、メールが送れませんでしたが、他のメールサーバーには送信できる状況でした。