

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】

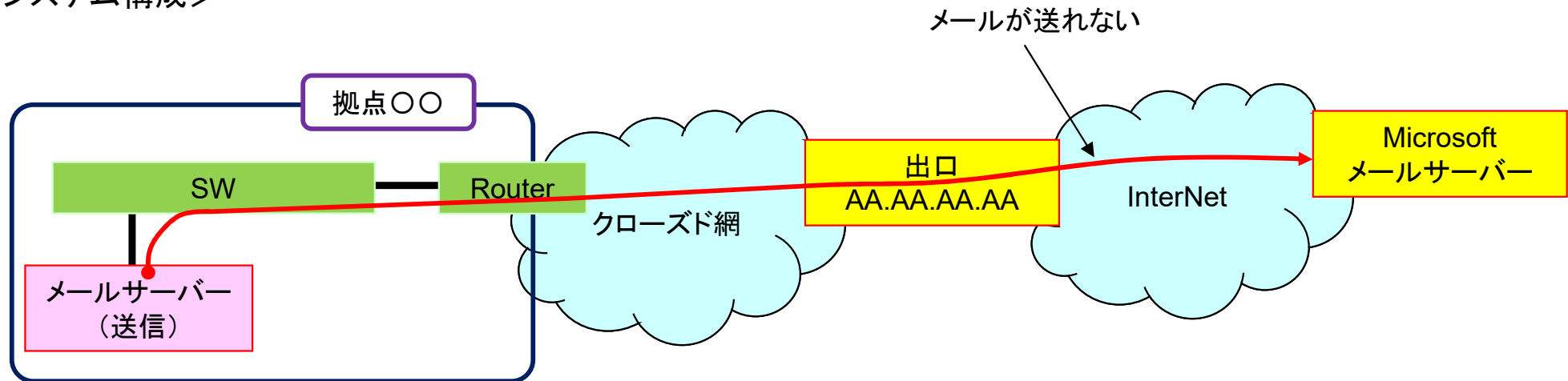
1. 概要(システム構成)
2. 事象
3. 対応
4. 分析
 - (1) Block List の揭示確認
 - (2) パケットキャプチャーのlog解析
 - (3) WireSharkを利用した分析
5. まとめ

アイティエスコンサルティング株式会社

2022/ 05/ 16

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

AA.AA.AA.AA has **1** listing



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]et

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

Notable things about the HELOs:

UTC時間

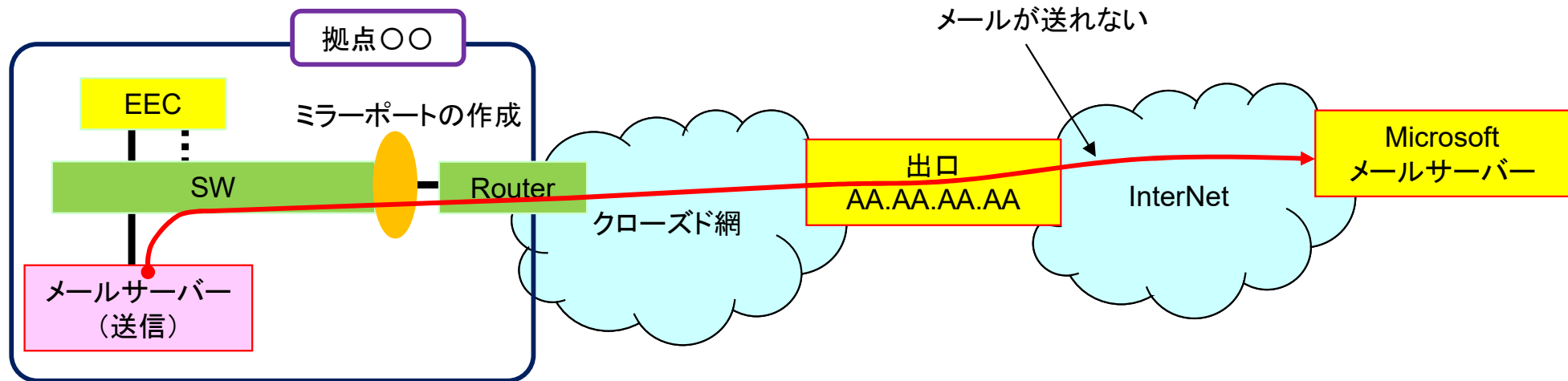
2022-03-19 00:10:00

2022-03-15 11:00:00 に

AA.AA.AA.AA のIPから、不適切な 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ーを実施

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。

⇒ 暫く様子を見ましたが、再度メールが送信できない事象が発生しました。

(1) Block List の揭示確認

<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

Technical information

(IP, UTC timestamp, HELO value)

```
AA.AA.AA.AA 2022-04-26 06:25:00 fi: [REDACTED] et
AA.AA.AA.AA 2022-03-19 00:10:00 T [REDACTED] et
AA.AA.AA.AA 2022-03-15 11:00:00 18E [REDACTED] rs
```

← 追加される

Notable things about the HELOs:

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 | 通信先 |
|-------|-----------------------|------------------------------------|
| • 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

No.	Time	Source	Destination	Protocol	Length	Info
40587	2022-04-26 15:26:25.670822	10.75.10.214	104.47.17.97	TCP	66	52383 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1340 WS=256 SACK_PERM=1
40588	2022-04-26 15:26:25.906329	104.47.17.97	10.75.10.214	TCP	66	25 → 52383 [SYN, ACK] Seq=0 Ack=1 Win=13400 Len=0 MSS=1366 WS=1 SACK_PERM=1
40589	2022-04-26 15:26:25.908317	10.75.10.214	104.47.17.97	TCP	60	52383 → 25 [ACK] Seq=1 Ack=1 Win=65536 Len=0
40590	2022-04-26 15:26:26.144583	10.75.10.214	104.47.17.97	SMTP	171	S: 220 DB8EUR05FT040.mail.protection.outlook.
40591	2022-04-26 15:26:26.202502	10.75.10.214	104.47.17.97	TCP	60	52383 → 25 [ACK] Seq=1 Ack=118 Win=65536 Len=0
40592	2022-04-26 15:26:26.713112	10.75.10.214	104.47.17.97	SMTP	94	C: EHLO fixed-1[redacted]ay.net
40593	2022-04-26 15:26:26.945819	104.47.17.97	10.75.10.214	TCP	60	25 → 52383 [ACK] Seq=118 Ack=41 Win=13440 Len=0
40594	2022-04-26 15:26:26.946423	10.75.10.214	104.47.17.97	SMTP	266	S: 250-DB8EUR05FT040.mail.protection.outlook.
40595	2022-04-26 15:26:26.995258	10.75.10.214	104.47.17.97	TCP	60	52383 → 25 [ACK] Seq=41 Ack=330 Win=131072 Len=0
40596	2022-04-26 15:26:27.265521	10.75.10.214	104.47.17.97	SMTP	141	C: MAIL FROM:<office@circleraintree.com> BODY
40597	2022-04-26 15:26:27.498369	10.75.10.214	104.47.17.97	TCP	60	25 → 52383 [ACK] Seq=330 Ack=128 Win=13527 Len=0
40598	2022-04-26 15:26:27.516586	10.75.10.214	104.47.17.97	SMTP	99	S: 250 2.1.0 Sender OK 250 2.1.5 Recipient OK

```

> Frame 40592: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Ethernet II, Src: Cisco_93:bf:90 (e4:d3:f1:93:bf:90), Dst: NECPlatf_7c:27:ec (6c:e4:da:7c:27:ec)
> Internet Protocol Version 4, Src: 10.75.10.214, Dst: 104.47.17.97
> Transmission Control Protocol, Src Port: 52383, Dst Port: 25, Seq: 1, Ack: 118, Len: 40
▼ Simple Mail Transfer Protocol
  ▼ Command Line: EHLO fixed-1[redacted]et\r\n
    Command: EHLO
    Request parameter: fixed-1[redacted]et

```

```

0000 6c e4 da 7c 27 ec e4 d3 f1 93 bf 90 08 00 45 00  1..|'... ..E.
0010 00 50 e4 87 40 00 7f 06 88 6f 0a 4b 0a d6 68 2f  .P..@... .o.K..h/
0020 11 61 cc 9f 00 19 d5 15 92 48 62 40 f3 1d 50 18  .a.... ..Hb@..P.
0030 02 00 4d 0e 00 00 45 48 4c 4f 20 66 69 78 65 64  ..M...EH LO fixed
0040 2d 31 38 39 2d 32 30 33 2d 39 31 2d 34 38 2e 74  -1[redacted]t
0050 6f 74 61 6c 70 6c 61 79 2e 6e 65 74 0d 0a      o[redacted]t..

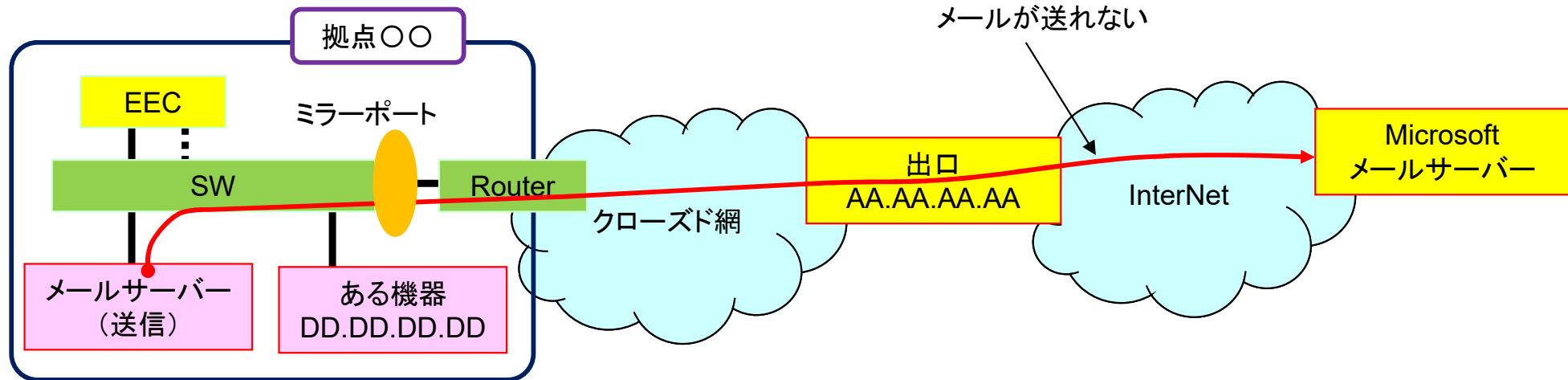
```

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.xxet ← 今回

UTC 時間 4/26 06:25:00 HELO値が 適切でないがあります。



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、メールサーバとして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。他のメールサーバーには送信できる状況でした。