メールがいきなり届かなくなった咄

2021/11/20(土)
姫路IT系勉強会 2021.11(オンライン)
さとう at なんだか

※発表後に若干加筆しています

たぶん、皆さんの興味は薄いかと

- ちょっと巻き込まれた咄です。
- (略)

こんなとき、普通どうしてるのですか

From: MAILER-DAEMON@XXXXXXXXXXX
[mailto:MAILER-DAEMON@XXXXXXXXXXX]
Sent: A_Day_of_Week, November DD, 2021 HH:MM AM
To: XXXXXXX@YYYYYYYY
Subject: failure notice

Hi. This is the qmail-send program at XXXXXXXXXXX.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

<ZZZZZZZ@QQQQQQQ>:
Connected to SOME_IPv4_ADDR but connection died. (#4.4.2)
I'm not going to try again; this message has been in the queue too long.

--- Below this line is a copy of the message.

確認したこと(1)

- 送信元ユーザ: これまで届いていましたが、エラーメールが返るようになりました
- 送信元の管理者: こちらのメールサーバには異常ありません
- 送信先の管理者: そんなメール来てません。どこからですか
- 送信先ユーザ: 何も変えてないのに、いきなり届かなくなりました

確認したこと(2)

- 送信元、送信先とも、他のドメインとは送受信できています
- そもそも、送信先にメールが来ていません
- 送信先のWebメールにも何もなし
- 送信先メールサーバのスパムフィルタにも何も引っかかってない
- 送信先メールボックスの空きは十分なはず

- 少し考えればわかりそうなものですが、ここで疑うべきものが何なのか、その時点ではわかりませんでした...

ここで黙っていても

- メールサーバの管理人たちは何もやってくれないです
- このままではどうも解決しそうにない...

で、仕方ないので

- 送信先の管理者に、転送されたエラーメールを送りました
- どこからのメールかわからないというので、送信元を自分で確認するため、メールを一通、こちらのメールサーバに送ってもらい、SMTPのログの一部を送付しました。
- メールヘッダを見れば良かったのですが。

```
connect from $HOSTNAME[$IPv4_ADDR]
client=$HOSTNAME[$IPv4_ADDR]
from=<XXXXXXX@YYYYYYYY>, size=4092, nrcpt=1 (queue active)
disconnect from $HOSTNAME[$IPv4_ADDR] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
```

おわかりと思いますが

- 送信先(の関連会社?)がファイアウォールを締めたのが敗因でした
- いきなり一方的に締めるのは何なのかという気もしますが、とりあえずは解決しましたです
- じつは送信元にも、ちょっと疑問がなくもなくて

んで、それから?

- 転送されたエラーメールを見ても、送信元がどこかはわかりません(肝心のメールヘッダが無かった)
- でも、メール送信ができなかったら、そっちの管理者に連絡できそうな気がしますが...?

  (送信先のDNSを確認すると、SOAレコードにあったメールアドレスは、送信先のサポート窓口と同じでした)

意見いろいろ

- 送信元メールサーバのログを見れれば、届かない理由も、もう少しわかりやすかったかも
- 送信元のオペレータに、ちゃんと伝わっていたかどうか(伝言ゲームの可能性)
- qmailは流石に新規では無いだろう
- エラーメールの持ち主から、eml形式で貰えればよかった(肝心のメールヘッダがなければどうにもならない)

  と、送信先の担当者は言いたかったはずです
- サービス業者によってはspam判定が厳しく、相手先ごとに細かく分けているそうです

  ブラックリスト入りしたら、エラーメールさえ返さないことも
- Microsoft Exchange OnlineとGoogle Workspaceは基本認証を廃止してAOuth2.0 only になります
- そもそも、メールなんてパスワード再設定など以外では使うべきではない

それくらいです。

- ご静聴、ご意見ありがとうございました。

終