

「メールでトホホ」

坂口 裕靖

酷暑に関しては何も言いません。平成30年7月豪雨で被害を受けた方、熱中症で殺された方、亡くなられた方々のご冥福を祈るばかりです。平成最後の夏は長く記憶に残ることとなるでしょう。

そんな中、メールサーバの移設を行いました。基本的にメールシステムはG Suiteを使っているのですが、一部古いメーリングリストを運用する関係上、受けのメールサーバは自前のものを使っていました。なのでまあ、G Suiteの最大のウリである障害耐性を使える状態ではなく、しかも一番重要な受け側のサーバがsingle point of failerになっているという、まあちょっとアレな状況なわけです。それもこれもgmailのメーリングリストが、発信者に対してメールを配送しないので、自分が出したメールが届いていないと誤解して、何度も何度もメールを出すユーザーが山ほどいる、という仕様が原因ではあるのですが、まあgoogle様は変える気がないのでしかたないわけです。

今回は、機材の関係でメールサーバの収容ラックを変更する必要があり、その関係で接続するネットワークを変更しなければなりません。ネットワークが変わるので、当然ながらIPアドレスも変わることになります。IPアドレスは変わりますが、mxレコードを変更する必要はありません。mxレコードに対応するホスト名のAレコードは変わりますが、メール配送系はmxレコードを見てIPアドレスを探すことになるので、特に問題ないだろう、と思っていました。

さて、休日の作業当日、メールサーバの移設自体は大変すんなりと終わり、IPアドレスの付替えもあっけなく終了しました。試しに外からメールを送ってみても、問題なく受信できているようです。メールログを監視すると、「お前のIPアドレスは見かけたことがないから、レート制限かけよ」といってるメールサーバがあることに気づきました。それでも出現頻度としては低かったため、まあ中にはそういうサーバ

もあるだろうね、という程度でさほど気にせず、休日の作業は終了としました。

明けて営業日。いよいよいろんなユーザーが使い始めるため、設置時のテストでは把握できなかった状況が発生するわけです。しばらくすると、「一部のメールが大変遅延する」という声が上がってきました。とりあえずは「一部メールサーバが見慣れないIPアドレスのメールサーバに拒否反応を起こしている模様。こちらからはどうしようもない」とりあえずは伝えました。

とはいえ何が起きているのかが気になるので、メールログを丹念に見ていきます。そうすると、ほぼ同じメールサーバが「レート制限かけよ」と言っていること、レート制限をかける原因の説明が徐々に変わってきていること、そして拒否しているのがG Suiteのサーバであることがわかりました。

まずいじゃん。

というわけで他のすべての仕事を放り出して、どこで発生しているのか、原因が何

One Point BUZZ WORD

IoT

固定価格買取制度の関係で、今日本の田舎の風景が変わりつつあります。雑草が生い茂っていた空き地の下草がきれいに刈られ、二度とペンペン草が生えてこないようにシートなどが敷き詰められたあと、太陽電池パネルが設置されていきます。緯度が低い九州地方においても、この傾向は強いようです。

一方で、九州電力管内の太陽光発電設備は、出力制御をできるようになっている必要があります。このためには、制御する機材が九州電力のサーバと通信し、スケジュールデータを取得しなければなりません。太陽光発電設備は良くても街のハズレ、悪いと山の中に設置されているため、ぱっと使えるネットワークはケータイ電話系のものぐらいしかありません。具体的にはデータ通信専用SIMなどを用いてアクセスすることになります。スケジュールデータは発電事業者毎に異なるため、おそらくは発電事業者の数だけSIMが設置されていることでしょう。となると、そ

もそも人気のない場所にSIMが一気に増えたりするわけで、空き地だけでなく通信環境も大きく変わるはず。もしかしたら、なんか最近ケータイつながらないよね、といった経験をされている方がいるかもしれません。

まあ今の所太陽光発電設備ぐらいなので設置密度は大したことないでしょうが、これがIoTということで大量の機材が通信を必要とするようになってくると、結局は電波資源をどう使うかという話になるような気がします。機器それぞれは協調できるかどうかわかりませんが、単純に同じネットワークを共用できるかどうかは微妙な問題です。ちょっと本気出した攻撃用デバイスが絡んできたらひとたまりもないでしょうから、基本は個別に通信手段を持つ方向でしょう。となると、結局は利用帯域を各種機材が割り合うという描像はしばらく変わらないのではないのでしょうか。今後の動向に注目しましょう。

なのかを追求します。レート制限のメッセージを受けている状況を総合すると、どうやら一度に複数のメールアドレスに対して配送するような場合に、G Suiteが中継を遅延させているらしいことに気づきます。ついで、宛先となっているメールアドレスをたどっていったところ、結局は aliases に登録されたアドレスあてに出したメールが遅延させられていることがわかりました。逆にメーリングリストだったり、宛先の数が少ないメールだったりについては、レート制限がかかっていないようでした。

ここまでわかれば、とりあえず回避策を組み立てることができます。aliases に登録されているようなアドレスについて、現在のところ遅延が発生しているので、hangout など別手段を使ってほしい旨アナウンスし、時間を稼ぎます。

問題の本質はG Suiteのメールサーバが、IP アドレスの変ったメールサーバを異物として排除しようとしている、つまりは免疫疾患ということになります。であるならば、このメールサーバが異物ではないというメッセージを送ることができれば、症状が緩和される可能性があるでしょう。各方面に相談した結果、とりあえず SPF レコードを登録してみることにしました。SPF は Sender Policy Framework の略で、「うちのメールはこのメールサーバからしか出さないよ、他はニセモノだよ」と告知できるメカニズムです。具体的には DNS の TXT レコードとして登録します。アドバイスに従って SPF レコードを登録し、メールログを見ていると、レート制限のメッセージが徐々に減っていき、ついになくなりました。つまり、メールサーバの IP アドレスを変えようと思ったら、基本的には SPF レコードも修正しなければならない、ということだったようです。

SPF レコードは、メールの出し元を制限することになります。逆に言うと、SPF レ

コードを運用できるようにするためには、すべてのメール発信点を把握しておかなければならない、ということです。古い常識で言えば、「受け」、すなわちメールの配信先となるメールサーバは mx レコードにより拘束されていましたが、「出し」、すなわちメールの発信元となるメールサーバは、何にも拘束されていませんでした。逆に言えば、だからこそスパムメール配信が容易でしたし、メール差出人の詐称が簡単だったわけです。

一方、SPF を運用するとすると、「出し」のサーバを管理する必要が出てきます。これはすなわち、「非公式」な発信元の存在を許すことができないのですから、きちんと管理しなければいけなくなるわけです。古い常識ではそのコストを見積もっていません。メールを出そうと思ったら、中央の発信局経由でしか出さないように修正するか、そのウェブサーバを発信点として登録しておく必要があります。ところが SPF レコードの長さには現実的に上限があるため、ほいほい登録していくと、上限を超えてしまうかもしれませんし、そもそも送信元の IP アドレスを簡単には変えられなくなってきます。つまり、そもそも中央の送信用メールサーバ以外からメールが出せる、という考え方自体を改めて、すべてのメールは送信用メールサーバから出すのだ、という運用ポリシーの変更が

必須となるのです。歴史のオリが溜まったような環境で、これを解きほぐすのがどれくらい面倒なのか、経験があればおわかりでしょうが、つまり、まあ、とても、大変、至極、面倒です。

ここいら辺の問題は、そもそもメールシステムがオープンであり、水平分散的なデザインであることが原因でしょう。そして、その性善説的立ち位置を悪用するようなユーザーが出てきたときに、対抗手段がとれないのであれば、制限を強くするしか方法がないのかもしれない。自由であったために低コストでできると思っていたことが、実は実在する管理コストの存在から目を背けていただけであり、見えないところでちゃりん、ちゃりんとは負債が積み上がっていたのかもしれない。ハードウェア要件の変更はハードウェアが売れて経済的な価値を生むかもしれませんが、ソフトウェアの設定変更は出銭が増える一方でメリットありません。まあだから、年号変わるのが悪夢になるわけですが。

Hiroyasu Sakaguchi
(株) IMAGICA イメージワークス

映像スタジオ施工

多様化するデジタル映像環境に対応、映像スタジオ施工なら豊富な実績、直営システムに依る徹底したコストダウンを実現する



匠の技をスタジオに

MA室 プース 各種 編集室

新設、リニューアルに関わらず何でもご相談ください。

～映像・音響専門で
40年～

(映像・音響・防音・建築・設計・施工)

一級建築士事務所

高橋建設株式会社

本社 〒216-0032 神奈川県川崎市宮前区神木1-7-8

TEL044-853-0547 FAX044-852-1588

(社)日本プロダクション協会会員 / (社)日本音楽スタジオ協会会員
(社)日本音響学会会員

http://www.takahashi-kensetsu.co.jp
info@takahashi-kensetsu.co.jp