農林水産研究情報総合センターニュース

第123号
2017年 7月25日

スパム対策② Receivedヘッダの時刻、ホスト名、IPアドレスから送信元の詐称を見抜く！

電子メールのヘッダ部分には、そのメールが途中経由してきた中継サーバを表すための「Received:」というヘッダ情報が付けられています。これを調べることで、そのメールがどこからやってきたのかを知ることができます。ここでは、Receivedヘッダの読み解き方と、送信者アドレスの偽装に気づくポイントを紹介します。

※ヘッダ情報の表示方法は、センターニュース122号をご覧ください。

下の例では、4つのReceivedヘッダが記述されていますが、上の方が受信者に、下の方が送信元に近い中継サーバの情報です。

Receivedヘッダの内容をみると、"from"の後に送信したホストの情報、"by"の後に受信したホストの情報が記述されています（青字）。ここから情報を拾い上げると、右のような配送経路でメールが届いたことが分かります。

［サンプル］MAFFINに届いたスパムメールのヘッダ（抜粋）

Received: from mas2-m2.nssm2.affrc.go.jp (localhost.localdomain [127.0.0.1])
by mas2-m2.nssm2.affrc.go.jp (MAFFIN-NSS-v5.0) with ESMTP id 26AE7FFA35 for <norin@affrc.go.jp>; Mon, 12 Jun 2017 01:40:17 +0900 (JST)
Received: from mg3-i.nss.affrc.go.jp (mg3-i.nss.affrc.go.jp [150.26.186.231])
by mas2-m2.nssm2.affrc.go.jp (MAFFIN-NSS-v5.0) with ESMTP id 20390FF8A2 for <norin@affrc.go.jp>; Mon, 12 Jun 2017 01:40:17 +0900 (JST)
（中略 ※Received以外のヘッダ）
Received: from 103-14-***-249.ip.cis.***.nz (HELO WIN-2KRK00K59G1) ([103.14.***.249])
by mg3.affrc.go.jp with ESMTP; 12 Jun 2017 01:40:16 +0900
Received: from WIN-R0H480RNUEA ([103.14.***.129])
by WIN-2KRK00K59G1 with Microsoft SMTPSVC(7.5.7601.17514); Sun, 11 Jun 2017 16:40:12 +1200
From: ****銀行 <email@bk.****.jp>
To: norin@affrc.go.jp

日本国内の銀行を詐称しています。

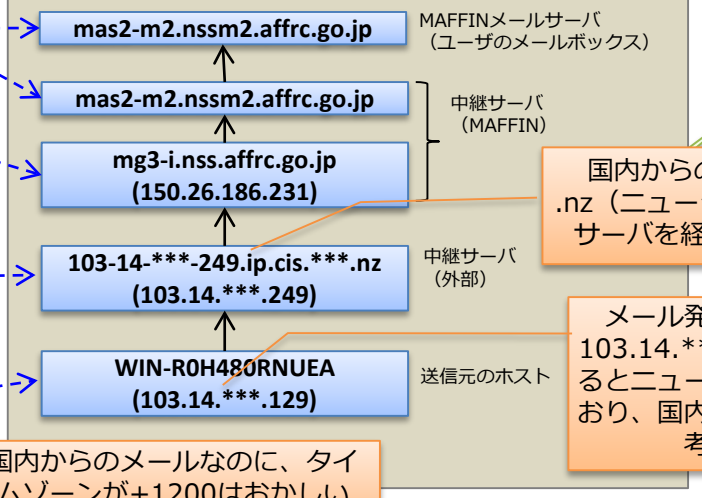
Receivedヘッダから送信元の詐称を調べるポイント

① 送信元のIPアドレスからwhoisやgeoipで組織や国名を調べましょう。送信者の属性と合っていますか？

② 送信時のタイムゾーンを調べましょう。国内からのメールは、日本のタイムゾーン +0900 で送信されるはず。

③ 中継サーバのドメインやIPアドレスを調べましょう。

Receivedヘッダから抽出したメールの配送経路



国内からのメールなのに、.nz（ニュージーランド）の中継サーバを経由するのは怪しい

メール発信元のIPアドレス103.14.***.129の国名を調べるとニュージーランドとなっており、国内の銀行のメールとは考えられない

国内からのメールなのに、タイムゾーンが+1200はおかしい

Receivedヘッダも偽造することができるので注意して下さい。
MAFFINの中継サーバが記録した外部中継サーバのIPアドレスは偽造が困難ですので、重要な手掛かりとなります。

IPアドレスから国名を調べる：GeoIP

GeoIPは、IPアドレスを国、都市、ISPにマッピングしたデータベース群です。以下のURLでデモが提供されており、手軽に調べることができます（1日最大25アドレスまで）。
https://www.maxmind.com/ja/geoip-demo

ニュースはWebで発信しています。

AFFRIT Portal » 農林水産研究情報総合センターニュース
http://itcweb.cc.affrc.go.jp/affrit/publications/start

夏季休暇中も「情報セキュリティ対策」！！

長期休暇を迎えるにあたって、先ずは、ご自身の連絡体制を確認し何かあった場合の対応を明確にしていただくとともに、普段使っているパソコンやサーバの電源管理・休暇中のログ管理等が十分に行えるよう準備をしてください。

◎ 長期休暇前のチェックポイント
http://itcweb.cc.affrc.go.jp/affrit/ric-cc-guide/security/vacation

☑休暇中必要のないパソコンや機器だけでなく、管理が手薄になる可能性がある場合は、Webサーバもあわせて電源を切りましょう。

☑パスワードは定期的に変更し、使い回しは止めましょう。

☑少しでも、不審なメールは、速やかに廃棄し、文中のリンクや添付ファイルをクリックしないようにしましょう。

☑緊急時の連絡体制を確認しましょう。

☑OS やアプリケーション（ブラウザのプラグインも！）、ウィルス対策ソフトを常に最新の状態に保ちましょう。

トピックス：

大切なデータのバックアップを取っていますか？

パソコンの故障や、ランサムウェア（データを暗号化して身代金を要求するウイルス）の被害などによるデータ喪失に備えて、日頃からデータのバックアップを定期的に行うよう、心がけましょう。

農林水産省農林水産技術会議事務局 筑波産学連携支援センター お問い合わせ先：request@affrc.go.jp