詐欺メールは
どこからやってくるのか？

調　査　資　料

2021年6月

詐欺メールの本文の一例

amazon

あなたのアカウントは停止されました

新しいデバイスからアカウントサービスへのサインインが検出されました。

お客様のアカウントで異常な行為が検出されたため、ご注文を一時停止いたしました。私たちの検証システムはあなたが行った支払いを検証することはできません。

Amazon保護のセキュリティと整合性の問題により、セキュリティ上の理由でアカウントが停止されます。

永久的な停止を避けるために、アカウント情報を確認してください。

確認用アカウント

アカウントの警告は、停止や無効化が避けられない状態になる前にお送りするように努めております。ただし、著しく悪質なポリシー違反の場合には、直ちにアカウントを停止または無効化することがあります。

怪しいメールにはじゅうぶん注意しましょう。

怪しいとおもったら、発信者情報(メールアドレス、メールヘッダーに記載してあるメールサーバーのアドレス、発信者のIPアドレスなど)を調べて、本物か偽物の判断をしましょう。

詐欺メールなどの分類

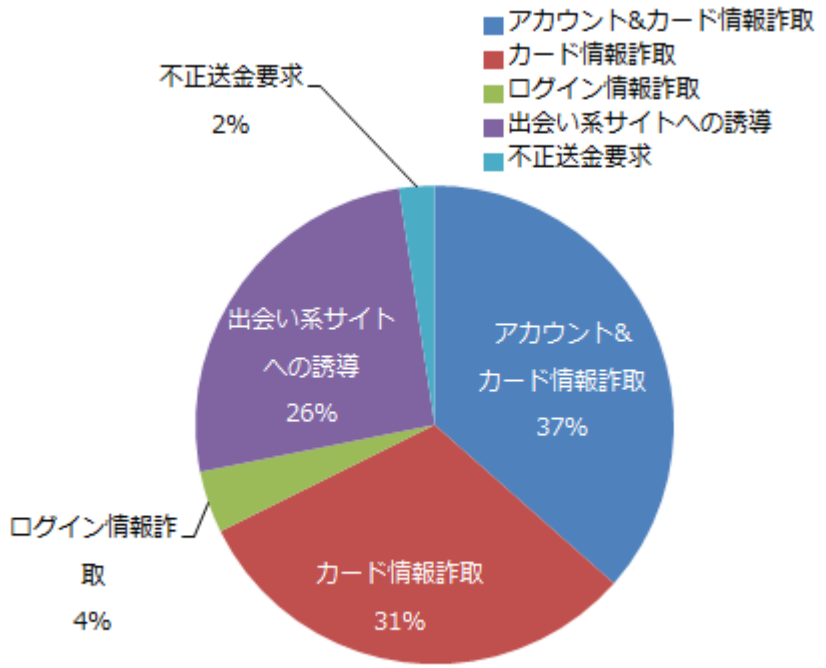
詐欺メールの内訳

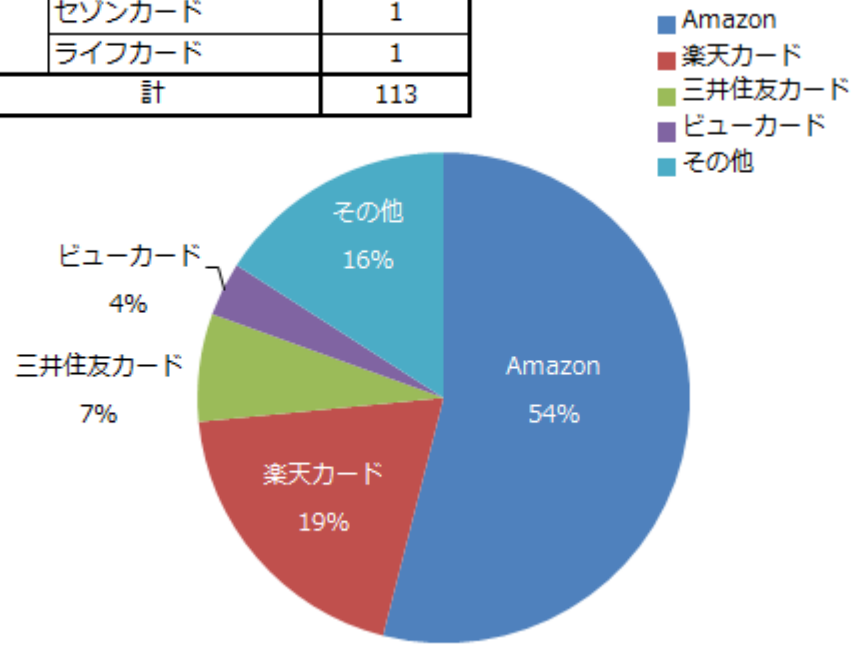
メール内訳	件数
アカウント&カード情報詐取	61
カード情報詐取	52
ログイン情報詐取	7
出会い系サイトへの誘導	43
不正送金要求	4
合 計	167

主な詐欺の対象物 (113件)

内訳		件数
Amazon		61
楽天カード		22
三井住友カード		8
ビューカード		4
その他	JCBカード	3
	アプラスカード	3
	JACCSカード	2
	Oricoカード	2
	TS CUBIC CARD	2
	エムアイカード	2
	三菱UFJニコスカード	2
	セゾンカード	1
	ライフカード	1
計		113

圧倒的に、Amazonに関するものが過半数、次いで、楽天に関するものとなっています。





メールヘッダーの例 （ Amazon を詐称 ）

```
(省略)
Return-Path: <dsajzjqrho@nbym.com>
(省略)
Received: from (省略)
        by (省略)
        for (省略)
Received: from (省略)
        by (省略)
        for (省略)
Received: from nbym.com (unknown [14.128.38.79])
        by (省略)
        for (省略)
Date: Sat, 22 May 2021 21:09:52 +0800
(省略)
From: Amazon.co.jp <dsajzjqrho@nbym.com>
To: (省略)
Subject: =?UTF-8?B?44GK5p(省略)
(省略)
X-Mailer: Foxmail 7, 0, 1, 91[cn]
(省略)
X-IP: 14.128.38.79
(省略)
X-FROM-DOMAIN: nbym.com
X-FROM-EMAIL: dsajzjqrho@nbym.com
(省略)
```

Amazonではない

中国製のメールソフト

Amazonではない

```
(省略)
Return-Path: <no-reply@amanuom-mail.net>
(省略)
Received: from (省略)
        by (省略)
        for (省略)
Received: from (省略)
        by (省略)
        for (省略)
Received: from mail0.amanuom-mail.net
   (v118-27-8-25.8m7b.static.cnode.io [118.27.8.25])
        by (省略)
        for (省略)
Sender: no-reply@amanuom-mail.net
From: "Amazon-card.co.jp" <account@amazon.co.jp>
To: (省略)
Subject: =?gb2312?B?pKKkyqS/pM52 (省略) eWl6g==?=
        =?gb2312?B?pcalo8n (省略) KTepLekvw==?=
(省略)
X-IP: 118.27.8.25
(省略)
X-FROM-DOMAIN: amanuom-mail.net
X-FROM-EMAIL: no-reply@amanuom-mail.net
(省略)
```

メールヘッダーと呼ばれる部分に、発信者の情報、発信元メールサーバーの情報、メールソフトの情報、日本語文字コードの情報などが記述されています。

詐欺メールのメールソフトと日本語文字コード

詐欺メールに使用されたメールソフト

メールソフト	件数
Acoyx 3	1
Foxmail 6, 13, 102, 15 [cn]	6
Foxmail 7, 0, 1, 91[cn]	10
Microsoft MimeOLE V6.00.2900.2869	4
Microsoft MimeOLE V6.00.2900.5512	3
Microsoft Outlook 16.0	27
Microsoft Outlook Express 6.00.2900.5512	19
sFOiGDyTZ	1
不明	42
計	113

アカウントとカード情報を抜き取る113件の詐欺メールのメーラーソフトは、大半がMicrosoftのものですが、一部、中国製のFoxmailが使われていました。

詐欺メールの文字コード

文字コード	件数
gb2312 (cn)	1
shift_jis	1
utf-8	111
計	113

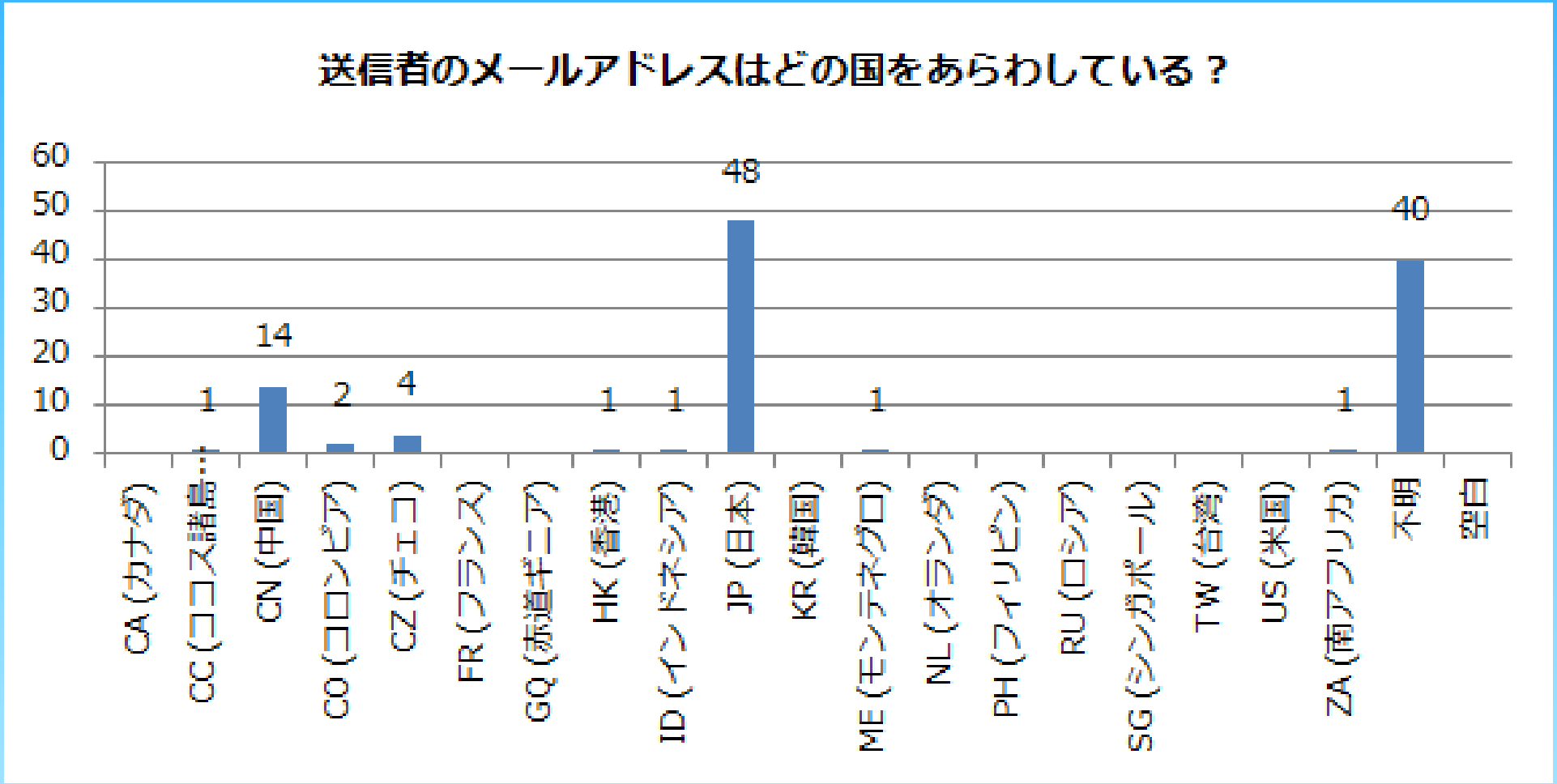
メール本文の日本語文字コードは、大半がUTF-8でしたが、中国のGB2312も一部にありました。

情報詐取に関する国名

アカウント&カード情報詐取 (61件) / カード情報詐取 (52件)に関係する国名

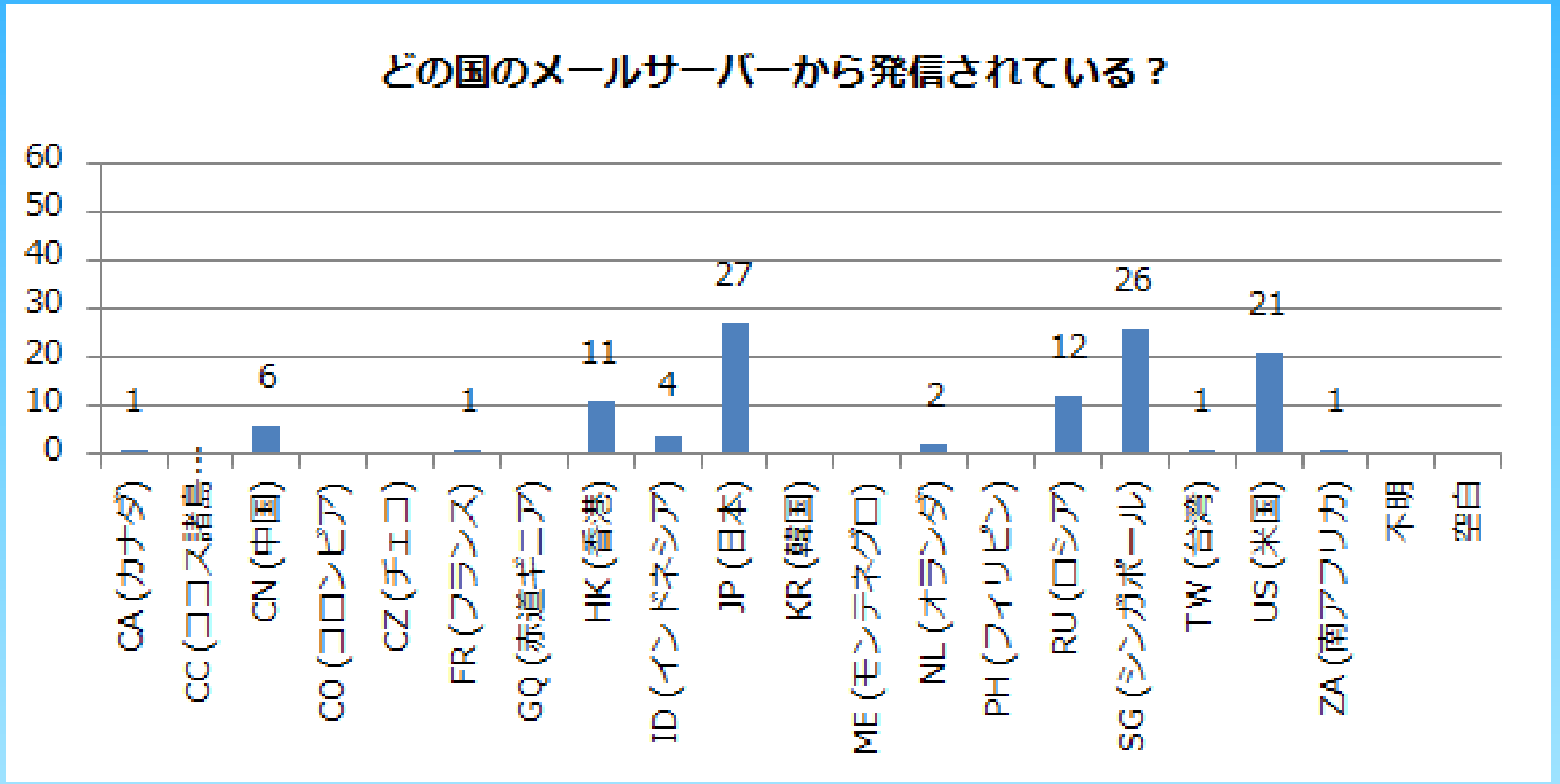
国名コード (国名)	送信者のメールアドレスはどの国をあらわしている？	どの国のメールサーバーから発信されている？	本文中にある情報入力先URLはどの国のもの？
CA (カナダ)		1	6
CC (ココス諸島(オーストラリア領))	1		3
CN (中国)	14	6	39
CO (コロンビア)	2		
CZ (チェコ)	4		
FR (フランス)		1	
GQ (赤道ギニア)			1
HK (香港)	1	11	1
ID (インドネシア)	1	4	
JP (日本)	48	27	1
KR (韓国)			3
ME (モンテネグロ)	1		
NL (オランダ)		2	
PH (フィリピン)			1
RU (ロシア)		12	
SG (シンガポール)		26	1
TW (台湾)		1	
US (米国)		21	2
ZA (南アフリカ)	1	1	
不明	40		55
合 計	113	113	113

情報詐取に関する国名



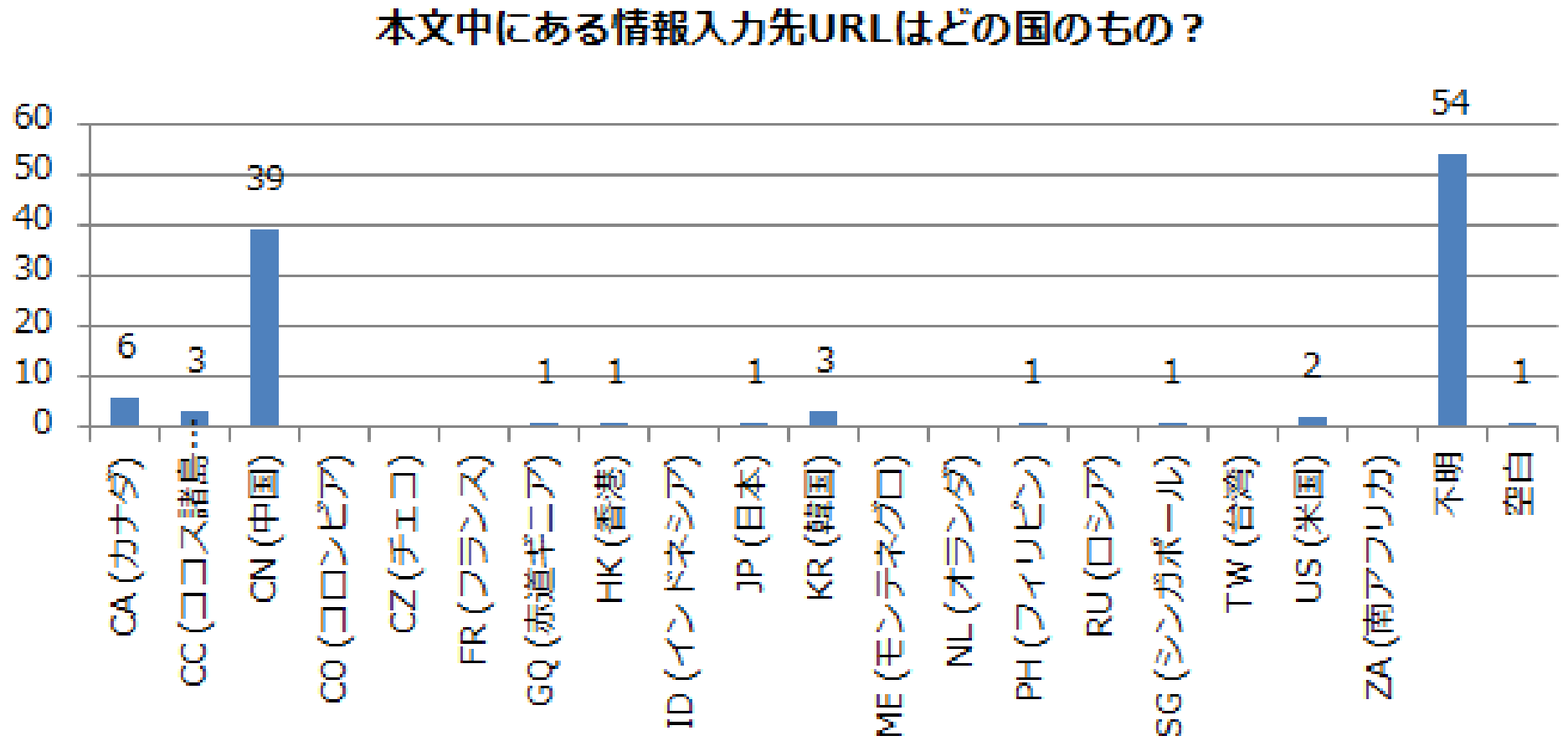
詐欺メールの送信者は、不明を除くと、日本、次いで中国の順です。

情報詐取に関する国名



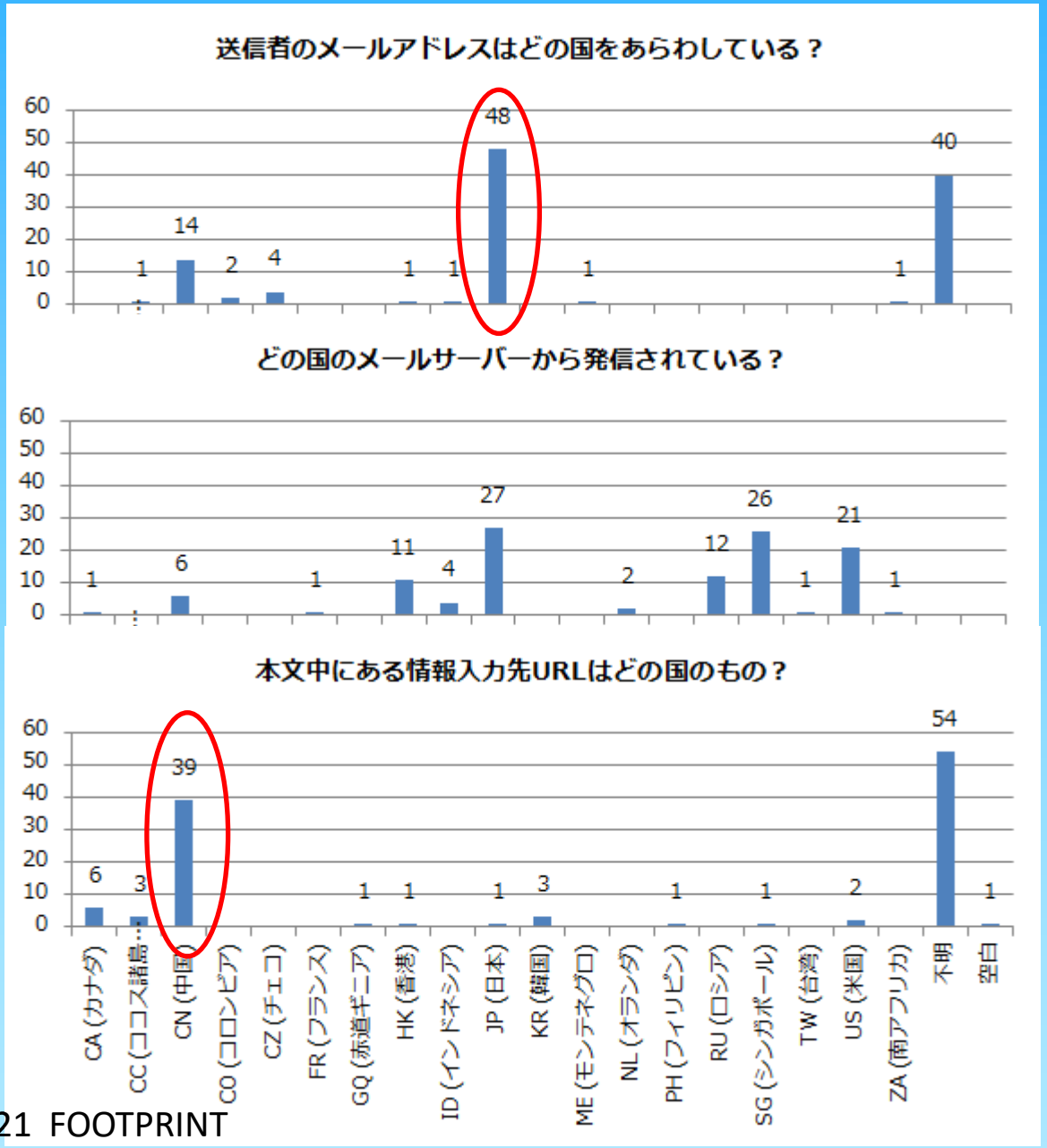
どの国のメールサーバーから発信されているかを見ると、日本、シンガポール、米国、ロシア、香港などばらばらです。

情報詐取に関する国名



本文中の情報を入力させるためのURLは、不明を除くと、中国が圧倒的に一番となっています。

情報詐取に関する国名



これらのアカウント・カード情報を詐取するのは主に中国のサイトですが、メール自体は日本から正規に発信されたように見せかけて、シンガポール、米国、ロシア、香港などの第三国のサーバーを経由して追跡しにくくしている、というように見えます。