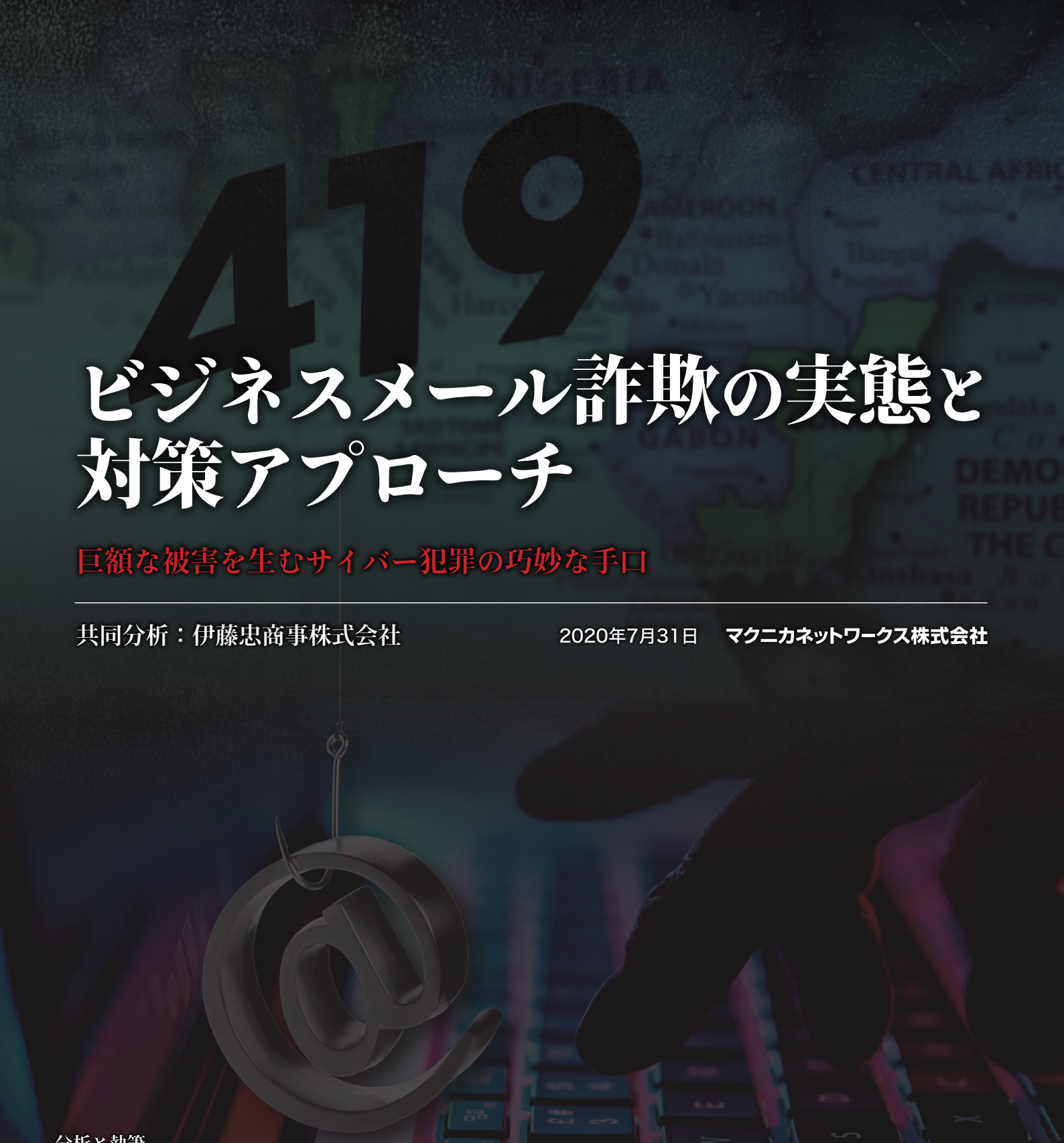
ビジネスメール詐欺の実態と対策アプローチ

巨額な被害を生むサイバー犯罪の巧妙な手口

共同分析：伊藤忠商事株式会社

2020年7月31日　マクニカネットワークス株式会社



分析と執筆

佐藤 元彦
伊藤忠商事株式会社 ITCCERT 上級サイバーセキュリティ分析官
国立大学法人 千葉大学 運営基盤機構情報環境部門 准教授

政本 憲蔵
マクニカネットワークス株式会社 セキュリティ研究センター センター長

勅使河原 猛
マクニカネットワークス株式会社 第1技術統括部セキュリティサービス室 主席

目　次

1. エグゼクティブサマリー

米国連邦捜査局（FBI）傘下の米インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）によると、2013 年 10 月から 2018 年 5 月までの 5 年弱の間に発生したビジネスメール詐欺（Business Email Compromise：BEC）の報告件数は 8 万件弱、被害総額は約 125 億ドル（約 1 兆 4000 億円）に達しました。日本国内においても、2017 年末に大手航空会社が約 3.8 億円の被害に遭ったとの報道 [1] があり、2019 年に入っても、大手報道機関の米子会社が約 32 億円 [2]、大手製造企業の欧州子会社が約 40 億円 [3] の被害に遭ったとの報道がされました。日本国内で報道される BEC の被害事案は氷山の一角に過ぎず、被害額が比較的小さいものを含めると被害件数はかなり多数に上るとみています。

マクニカネットワークスでは、2015 年から 2019 年までに親会社（マクニカ・富士エレホールディングス）のグループ傘下に届いた BEC だけでなく、マクニカ・富士エレグループを装って取引先へ届いた BEC、さらにはマクニカネットワークスが提供するインシデント対応サービスにて対処した BEC 事案を分析し、攻撃者が使う手口を明らかにしてきました。そして、今回、伊藤忠商事の ITCCERT 様 [4]（以下敬称略）のご協力を得て、世界中に展開する伊藤忠グループに日々届いた BEC の分析結果を共有頂いたことで、攻撃者の手口や素性がより明らかになってきました。ITCCERT では 2014 年から BEC の監視を開始し、2017 年には日本語で書かれた BEC も観測しており、日本国内では BEC に関する最も深い知見を有している組織と言えます。伊藤忠グループおよびマクニカ・富士エレグループにて観測された BEC の実態については、2 章で実例を交えて解説しています。

BEC メールが届く前段階から、攻撃者による用意周到な準備段階があります。多くの場合、攻撃者が取引に割り込んで詐欺をはたらくには、取引状況の詳細を把握する必要があるため、様々な方法で電子メールアカウントに不正ログインを試みます。不正ログインした電子メールアカウントでやり取りされるメールを盗聴することで、効果的なタイミングでメールのやり取りに割り込み、詐欺をはたらくことができるのです。このように、用意周到な準備を経て、BEC メールを届け、詐欺をはたらき、攻撃者が用意した口座へ振り込ませるまでの一連の流れを BEC Kill Chain として 3 章にまとめました。

BEC の対策に、特効薬はありません。IT システム面での対策だけでなく、会計部門の気づきによる水際対策が非常に重要となります。現時点で一定の効果があると考えている対策を、IT システム面および会計部門の観点から 4 章にまとめました。さらに、ビジネスメール詐欺に直面したときに必要なインシデント対応を 5 章にまとめました。

本レポートが、日本国内の組織が BEC 対策を考える上で有益な情報となり、少しでも被害軽減につながることを願うばかりです。

1 https://piyolog.hatenadiary.jp/entry/20171220/1513795615
2 https://www.nikkei.com/article/DGXMZO51583520Q9A031C1SHA000/
3 https://www.asahi.com/articles/ASM965H5HM96OIPE02Q.html
4 https://tech.nikkeibp.co.jp/it/atcl/column/16/080500167/081100004/

2. ビジネスメール詐欺の実態

マクニカネットワークスでは、2015 年に初めて BEC メールを観測し、その後、今日に至るまで継続的に BEC メールを観測しています。その中から複数の実例を取り上げて特徴や手口を解説します。

2.1 取引先の CEO を装う

図 1 のメールは、2019 年に、マクニカ富士エレグループ傘下の企業へ届いた BEC メールで、差出人は米国取引先の CEO を装っています。しかし、差出人のメールアドレスは、取引先とは無関係のドメインになっており、比較的容易に気が付くことができます。しかし、メール内容は取引先 CEO からの至急の依頼を装っているので、「疑うことで失礼だと思われたくない」という心理がはたらき、依頼を断りにくい状況にあります。

図 1：米国取引先を装って届いた BEC メール

調査目的でこのメールに返信したところ、図 2 のような返信が攻撃者から返ってきました。「ドバイから機械を購入する予定だが、米国へ直接輸入すると関税が高いので、日本（マクニカ）へいったん輸入してから、米国へ送ってほしい。」という内容でした。

図 2：米国取引先を装った攻撃者からの依頼内容

その後、騙されたふりをして攻撃者とやり取りを続けると、ドバイにある販売元を騙る攻撃者から振込先の口座情報が送られてきました。口座情報はしかるべきコミュニティを通して銀行に共有し、さらなる犯罪の予防を図っています。

2.2 自組織の CEO からの社内メールを装う

図 3 のメールは、2019 年にマクニカ富士エレグループの代表取締役社長からの社内メールを装った BEC メールです。CEO を装う詐欺は、BEC の中でも特に CEO 詐欺とも呼ばれます。ブラジルの海外現法宛てに届いていますが、差出人のドメインが正規ドメイン macnica.com の類似ドメイン **rn**acnica.com（m を r と n で表現）になっています。（図 4）

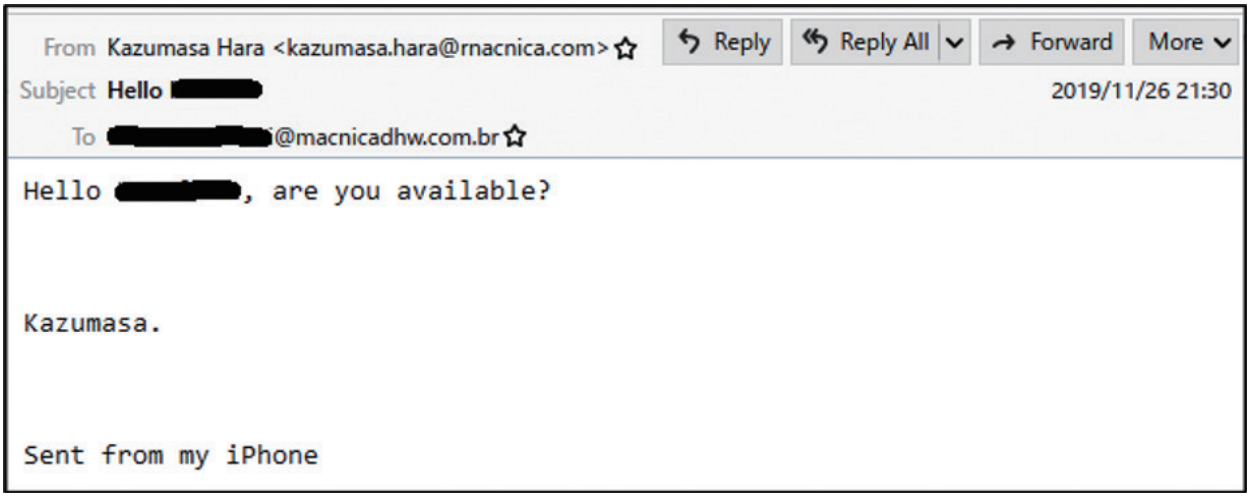


図 3：代表取締役社長からの社内メールを装った CEO 詐欺メール

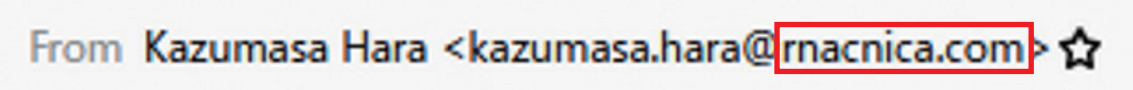


図 4：差出人のメールアドレスとして使われた類似ドメイン

図 5 のメールは、代表取締役会長からの社内メールを装った CEO 詐欺メールです。

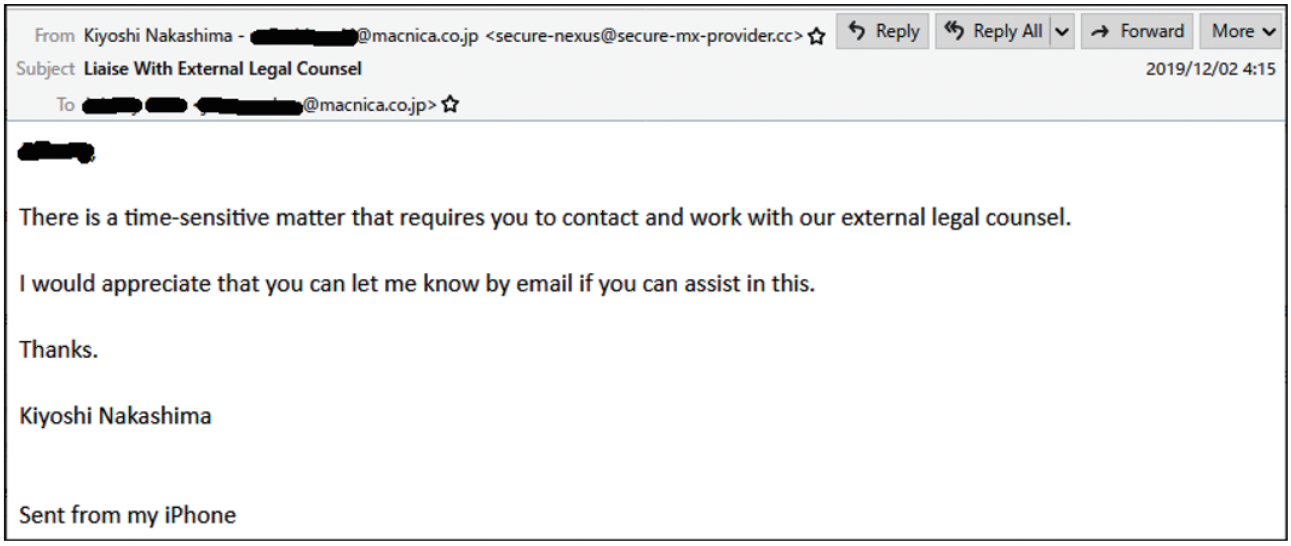


図 5：代表取締役会長からの社内メールを装った CEO 詐欺メール

このメールに返信しないでいると、1 週間後に図 6（次頁）のような催促が届きました。

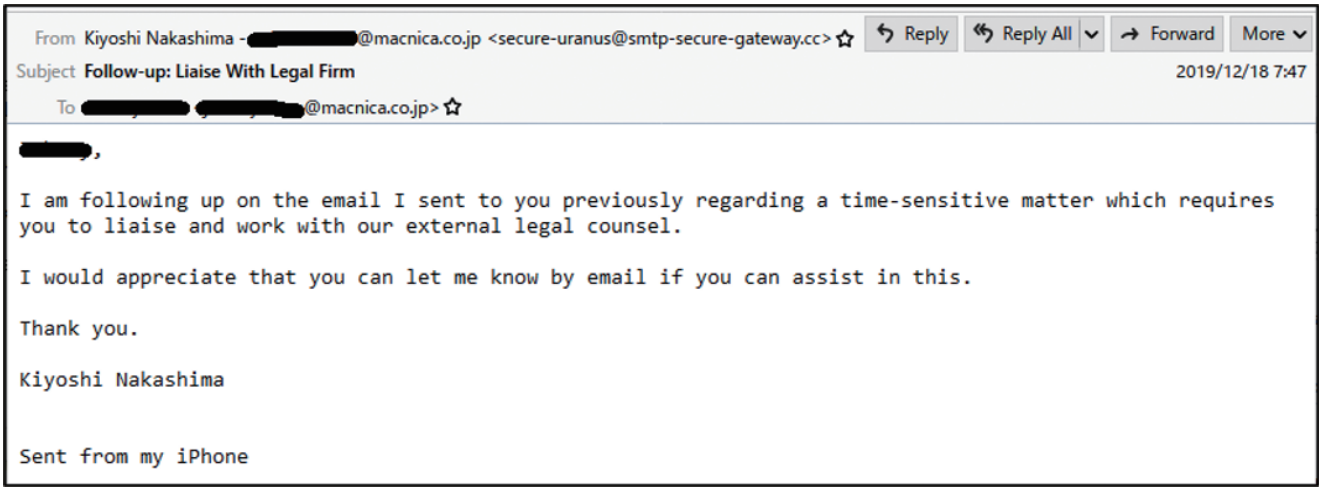


図 6：代表取締役会長を装った攻撃者からの催促

ちなみに、この手の CEO 詐欺メールに返信をした場合、「極秘の M&A 案件が成立したので至急支払いが必要になった」などと支払いを急かす依頼をしてきます。

2.3 類似ドメインの登録

図 7 のメールは、2019 年に、マクニカ富士エレグループ傘下の Netpoleon 社を装って顧客に届いた BEC メールです。このメールの直後に銀行口座情報が送られています。攻撃者は、Netpoleon 社の正規ドメインに類似したドメインを取得し、そこから顧客へ BEC を仕掛けました。幸い、顧客側が不審なドメインに気づき、未遂に終わっています。

図 7：Netpoleon 社を装って顧客へ送られた BEC メール

2018 年 5 月に、マクニカ富士エレグループが持つ正規ドメイン macnica.com に類似した macniica.com（i が 2 つ）というドメインが何者かによって取得されました。このドメインが実際に使われた BEC メールは確認できませんでしたが、図 8 の通り、このドメインの Whois 情報から、攻撃者のものと思われるメールアドレスが分かり、そのメールアドレスに紐づく他のドメインを確認（Reverse Whois）することができました。

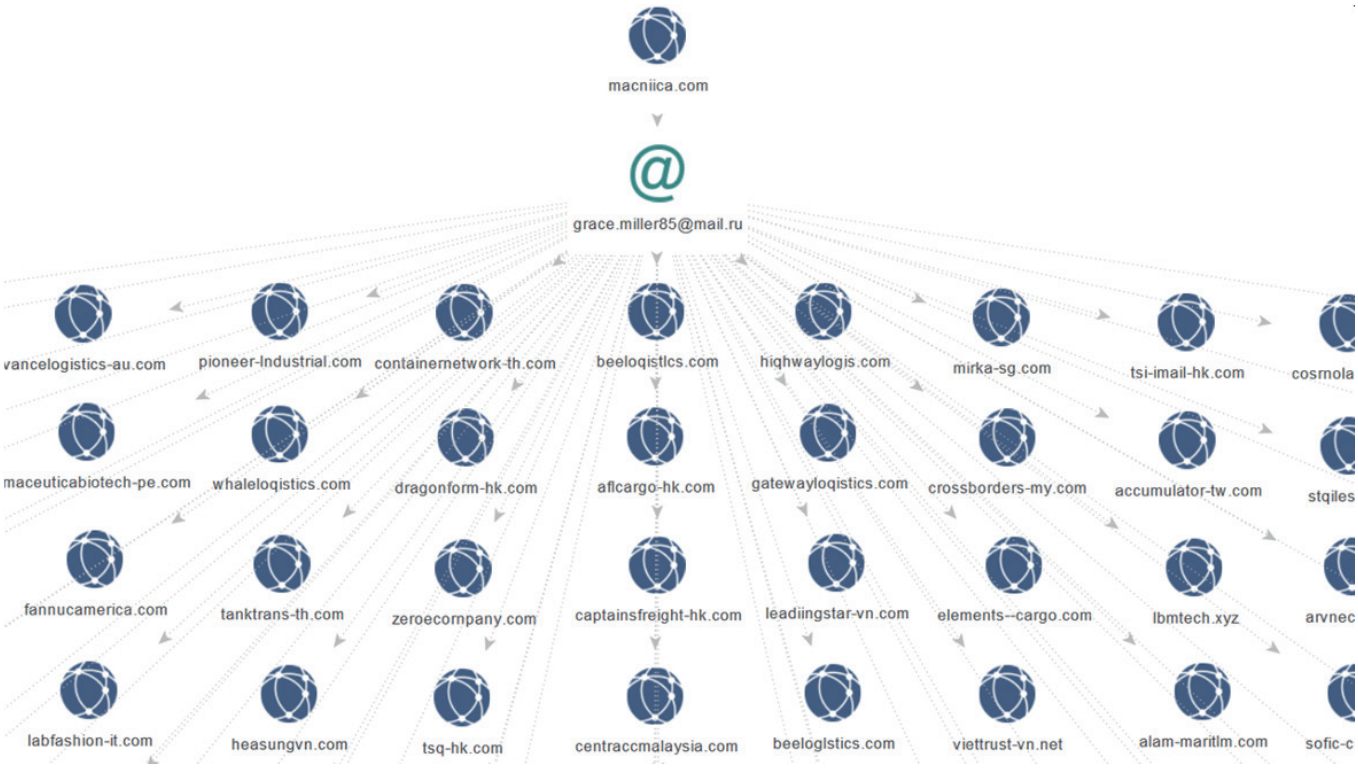


図 8：macniica.com を取得した攻撃者が取得した他のドメイン

これらのドメインをよく見ると、正規に存在するドメインに類似したものであることが分かりました。g が q になっていたり、i が l になっていたり、m が rn（r + n）となっていたりします。BEC を仕掛けるために取得したドメインである可能性が高いと考えています。

2.4 フリーメールの悪用

図 9 のメールは、2015 年に、マクニカネットワークスが提供するインシデント対応サービスにて対処した事案の一つです。日本国内の企業へ届いた BEC メールですが、差出人は海外の取引先を装っています。メールの内容は、振込先の変更を依頼する典型的なビジネスメール詐欺です。

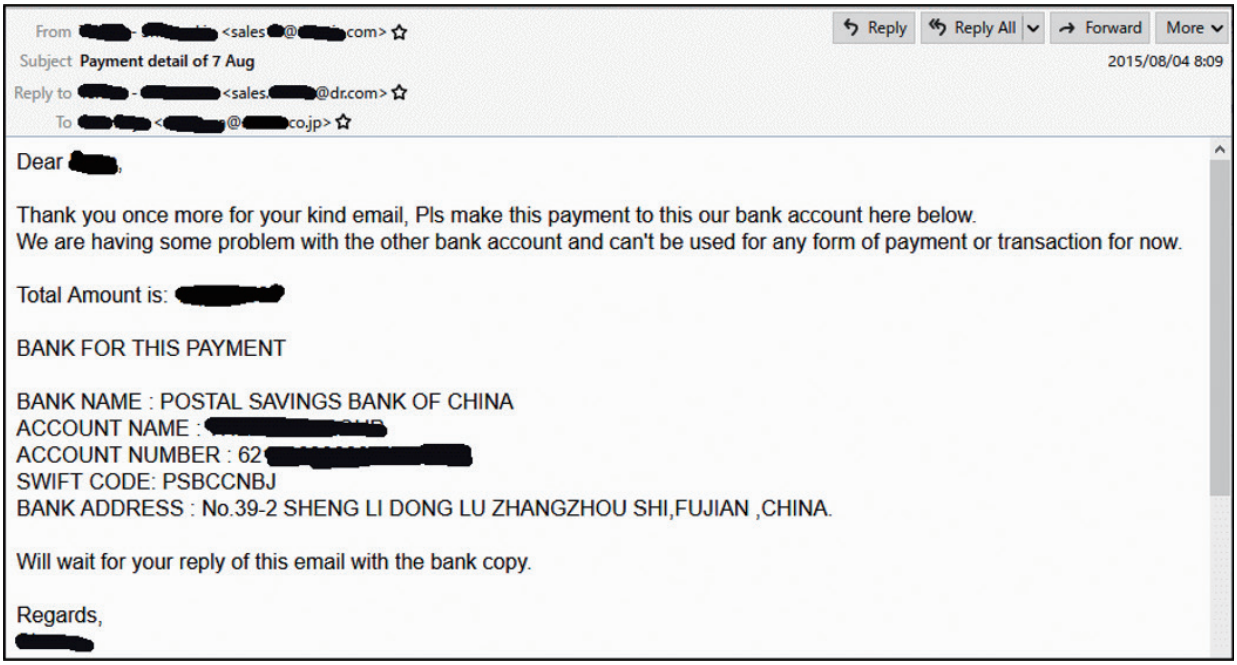
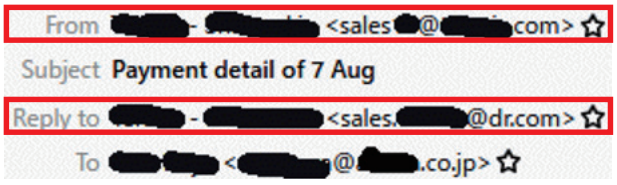


図 9：海外の取引先を装って届いた BEC メール

図 10 は偽装された送信元アドレス（From ヘッダ）と返信先アドレス（Reply-To ヘッダ）を拡大したものですが、送信元アドレスは、取引先が持つ正しいドメインに偽装されていました。また返信メールが攻撃者へ届くように、返信先アドレスは攻撃者が事前に用意したフリーメールアドレス（dr.com）です。



取引先の正しいドメインを偽装

返信先はフリーメールアドレス (dr.com)

図 10：偽装された送信元（From）と返信先アドレス（Reply-To）

dr.com というドメインは、mail.com というフリーメールサービスで選択できる約 200 個のドメインの中の 1 つです。この mail.com で選択できるドメインは、この実例のように BEC メールでよく使われます。そして、メールヘッダを確認すると、このメールの本当の送信元が分かりました。図 11 にある通り、ヘッダ内には yahoo の文字列が多数確認でき、Yahoo.com のフリーメール特有のヘッダもあることから Yahoo.com のフリーメールから送信されたことが分かります。

図 11：BEC メールのヘッダ

Return-Path ヘッダには、攻撃者が取得したと思われるメールアドレスも確認できます。そして実は Yahoo や Gmail などのフリーメールサービスでは、差出人を別のメールアドレスに変更することができます [5]。Yahoo.com の場合、差出人として別のメールアドレスを追加するには、追加したメールアドレス宛に送信される確認メールのリンク先へアクセスする必要があります [6]。つまり、この実例の場合、取引先側のメールアカウントは既に攻撃者によって乗っ取られており、Yahoo.com から送られる確認メールを攻撃者が閲覧できる状態であったことが分かります。このように、BEC においては、いずれかのメールアカウントが乗っ取られているケースが多いです。メールアカウントを乗っ取ることで、この実例のように差出人を偽装できるだけでなく、メールの盗聴によって取引内容を詳細に把握できるので、詐欺を仕掛けやすくなります。この実例が示すように、BEC の攻撃者はフリーメールをよく活用します。返信先アドレスにフリーメールアドレスを指定するだけでなく、BEC メールの送信用インフラとしてフリーメールサービスを利用するのです。

この事案では、BEC メールを受信した日本企業側が攻撃者の口座へ振り込んでしまいました。しかし、メールアカウントを侵害されていたのは振り込んだ日本企業側ではなく、海外の取引先側でした。そのため、示談交渉を行い、被害額を按分することになりました。

5 https://support.google.com/mail/answer/22370
https://www.yahoo-help.jp/app/answers/detail/p/622/a_id/47956/
6 https://help.smallbusiness.yahoo.net/s/article/SLN29479

図 12 は、2018 年にマクニカ富士エレグループ傘下の企業（macnica.com）を装って、顧客に届いた BEC メールです。こちらも同様に、返信先が mail.com のフリーメールサービスで使われるドメイン（dr.com）になっています。（図 13）

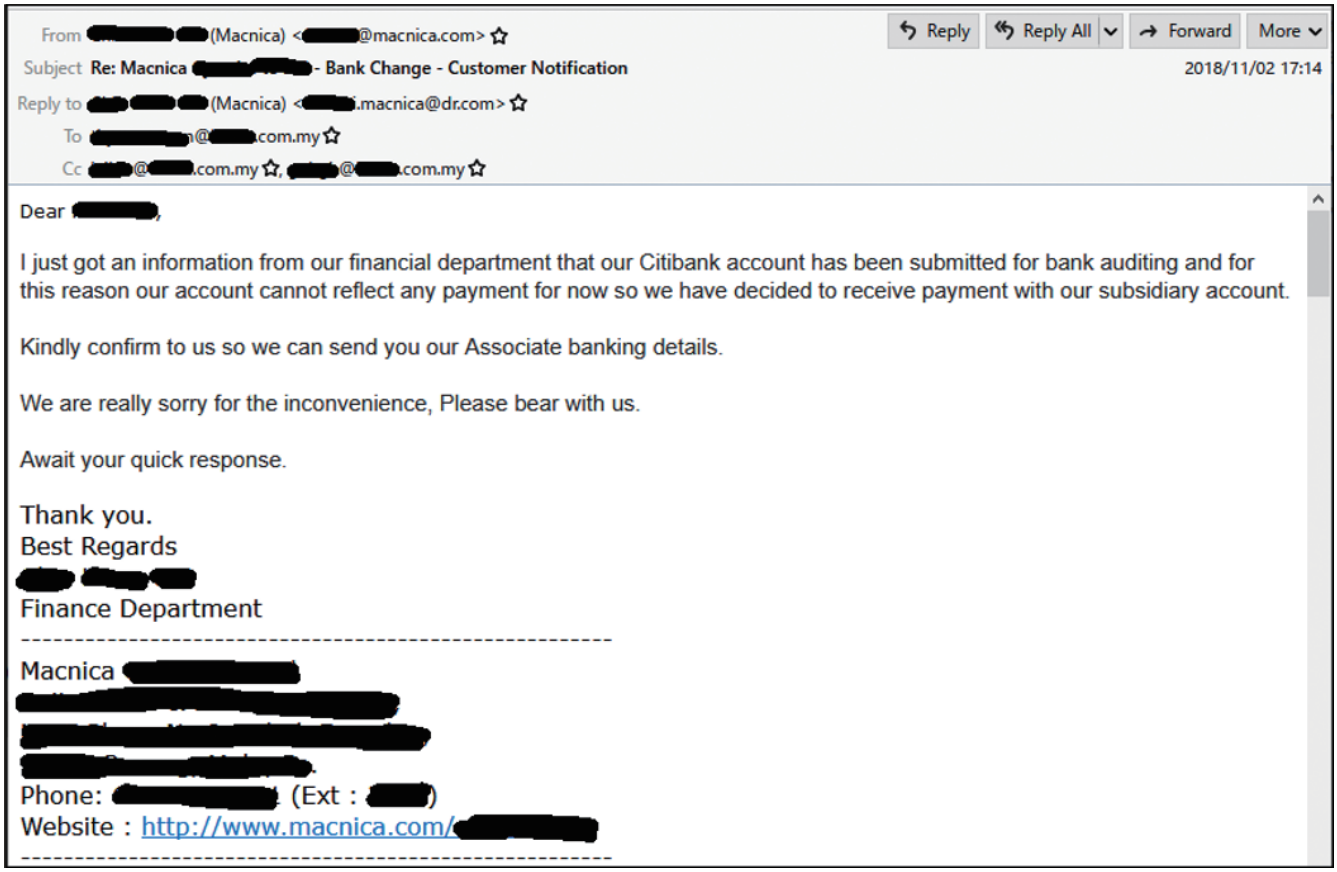


図 12：macnica.com を装って届いた BEC メール

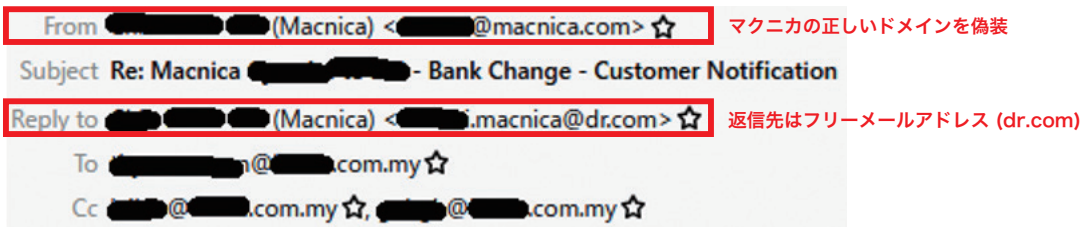


図 13：偽装された送信元（From）と返信先アドレス（Reply-To）

2.5 日本語で書かれた BEC メール

図 14 のメールは、2019 年に代表取締役社長からの社内メールを装って筆者（政本）宛てに届いた CEO 詐欺メールです。差出人のメールアドレスが見慣れないドメイン（secure-server-smtp.cc）ですが、手前の表示名に macnica.co.jp のメールアドレスを含めることで受信者の目を欺こうとしています。また、宛先のメールアドレスは、筆者（政本）の名前から攻撃者が推測したものであり、筆者所有のものと違っているため（図 15）、実際にはメールボックスに配送されず、メールゲートウェイに痕跡として残っていました。

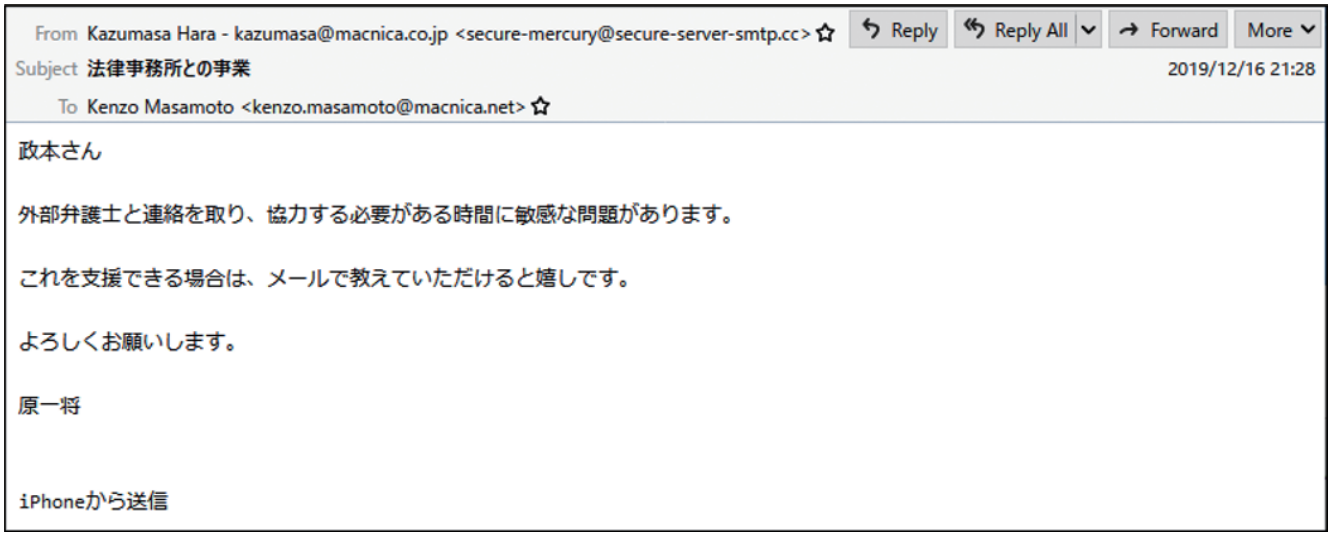


図 14：マクニカ富士エレグループの CEO を装って筆者（政本）に届いた CEO 詐欺メール

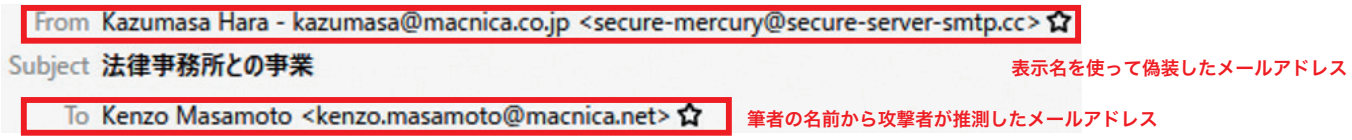


図 15：間違った宛先メールアドレス

図 16 と図 17 は、取引途中で介入する形で伊藤忠商事に届いた BEC メールです。攻撃者は日本語に堪能でないことから、明らかに普通ではない文章になり、日本語を母語とする者には違和感があります。このように、攻撃者が無理して日本語を使ってくるケースでは、攻撃者が日本語に慣れていないことから機械翻訳を使い、結果として不自然な日本語になって受信者が異常を感じて、気付くケースがあります。

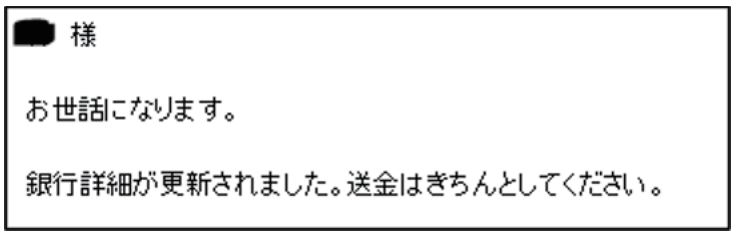


図 16：伊藤忠商事に届いた不自然な日本語のメール（1）

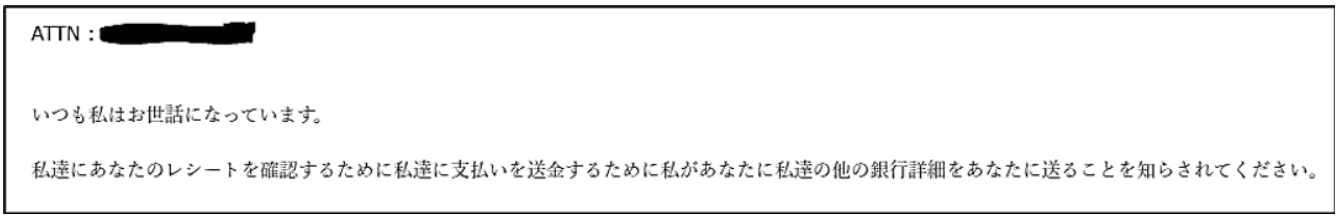


図 17：伊藤忠商事に届いた不自然な日本語のメール（2）

とはいえ、海外の取引先が日本語を使える場合においては、母語として使っていない話者の場合、やや不自然な日本語になることもあり、判断に困るケースがあるかもしれません。そのような場合には、文章だけでなくその他要素から BEC かどうかを判別する必要が出てきます。

2.6 乗っ取ったメールアカウントをそのまま使う BEC メール

BEC かどうかの分析において、非常に分析が困難なケースとして、取引先のメールアカウントが乗っ取られ、そのメールアカウントから BEC メールが送られてくることがあります。BEC メールかどうかの分析ではメールヘッダから異常を確認することが多く、メールアカウントが乗っ取られている場合は当然ですがヘッダに不審点が見つかりません。当たり前ですが、偽メール自体も正しい経路でメールが配信されているからです。ただし、そのような場合でも、丹念にメールヘッダを見ると攻撃者が痕跡を残していることがあります。図 18 は、伊藤忠商事に届いたメールで、乗っ取られたメールアカウントから口座変更依頼がされたケースのメールヘッダです。

```
Date: Wed, 26 Jul 2017 23:51:01 +0200
From: <[redacted]@9business.fr>
Sender: <[redacted]@9business.fr>
Reply-To: <[redacted]@9business.fr>
To: [redacted] <[redacted]>
Message-ID: <1076504800.277914.1501105861750.JavaMail.www@wsfrf1418>
Subject: RE: Account Update Letter.
MIME-Version: 1.0
X-SAVECOPY: true
X-ORIGINATING-IP: 41.190.30.48
X-Wum-Nature: EMAIL-NATURE
X-WUM-FROM: |~|
X-WUM-TO: |~|
X-WUM-CC: |~||~||~||~|
X-WUM-CCI: |~|
X-WUM-REPLYTO: |~|
X-sfr-mailing: LEGIT
Content-Type: multipart/mixed;
              boundary="----=_Part_277911_1790251283.1501105861741"
X-Spam-Details: rule=quarantinepolicy_notspam policy=quarantinepolicy score=0 spamscore=0
suspectscore=5 malwarescore=0 phishscore=0 adultscore=0 bulkscore=0
classifier=spam adjust=0 reason=mlx scancount=1 engine=8.0.1-1706020000
definitions=main-1707260321
Return-Path: [redacted]@9business.fr
```

図 18：伊藤忠商事に届いた乗っ取られたメールアカウントからの BEC メールのメールヘッダの例

一見すると送信元も返信先もメッセージ ID が正しく、異常があるように見えません。差出人の会社はフランスで、過去の同社からのメールのメールヘッダと比較しても異常がなく見えます。ヘッダに記載されている Date も UTC+2 の時間帯が設定されており、フランスの時間帯です。しかし、丹念にメールッダを確認すると、一点だけ異常があります。それは、X-Originated-IP というヘッダが追加されている点です。この IP アドレスに関する情報を調べると、図 19 のように、ナイジェリアの IP アドレスであることがわかります。ナイジェリアの IP アドレスがフランスの会社のオリジナルの IP アドレスとして記録されることはまずありえません。このことから、取引先のメールアカウントが乗っ取られ、ナイジェリアから接続されて不審メールが送信されたのではないか、という推定が成り立ちました。

```
inetnum:        41.190.16.0 - 41.190.31.255
netname:        EMTS-Corporate
descr:          This resource is assigned for EMTS Nigeria's corporate use
country:        NG
admin-c:        ISR1-AFRINIC
admin-c:        BM74-AFRINIC
tech-c:         ISR1-AFRINIC
tech-c:         BM74-AFRINIC
status:         ASSIGNED PA
mnt-by:         EMTS-MNT
source:         AFRINIC # Filtered
parent:         41.190.0.0 - 41.190.31.255
```

図 19：メールヘッダに残された IP アドレスの詳細

2.7 偽装されたメール署名

「お金を振り込む前に取引先に電話で確認する」といった対策を行っている組織があるかと思いますが、攻撃者はこの対策を逆手にとって、メール署名に攻撃者につながる電話番号を記載している場合があります。電話をかけると秘書代行サービスになっていて、「担当者不在のため折り返します」と言ってきます。その後、攻撃者から電話があり、メールに記載した口座番号が正しいことを伝えてくるのです。メール署名に記載された電話番号を信用してはいけません。

2.8 LinkedIn を使った接触

ビジネス向け SNS サービスである LinkedIn は、利用者が所属組織を登録していることから、攻撃者にとっては対象とする企業の情報を探索したり、その組織の社員にコンタクトしたりすることが容易です。米国ではビジネスで知り合った人たちが LinkedIn を介して繋がりを持つ場合もあり、ビジネスのツールとしての地位を確立していることから、攻撃者もその効果を知って悪用できないか試みているようです。

図 20 は筆者（佐藤）にコネクション申請をしてきたケースで、偽名を使い存在しない事務所のマネージャを騙っています。また、図 21 では、代表取締役会長を装ったアカウントを作り、コネクションを申請してきたケースです。もっとも、このケースでは攻撃者のスキル不足が露呈していて、会長名の綴りも間違い、写真も CFO のものを使い、さらにロケーションがナイジェリアになっている、というお粗末な偽アカウントです。とはいえ、このような形で攻撃者は情報を収集し、コンタクトをとってくることに留意しなければなりません。

なお、LinkedIn では偽アカウント対策に力をいれており、双方のケースでは、サイトから不正アカウントであるという申し立てを行ったところ、すぐにアカウント自体が削除されました。もちろん、自組織名を騙って他組織を狙うこともあり、LinkedIn で自組織名を名乗る不正なアカウントが作られていないかを定期的に検索して監視することも効果があると思われます。

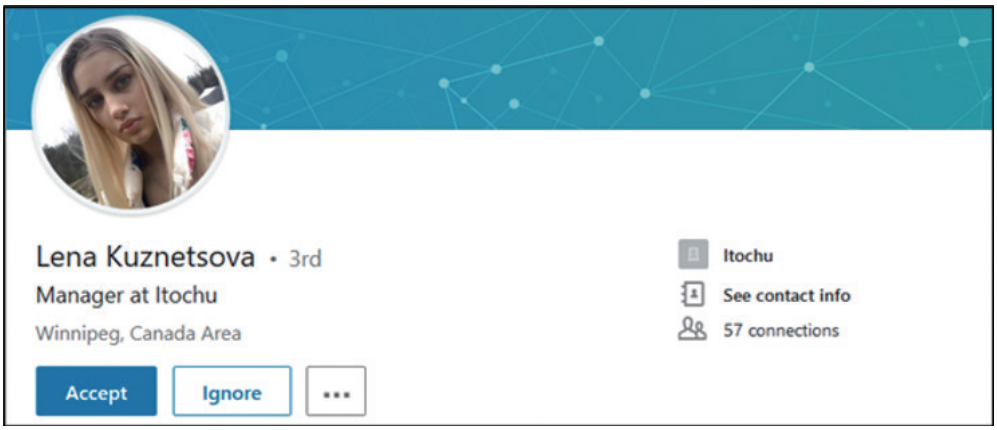


図 20：同僚を装う LinkedIn のアカウント

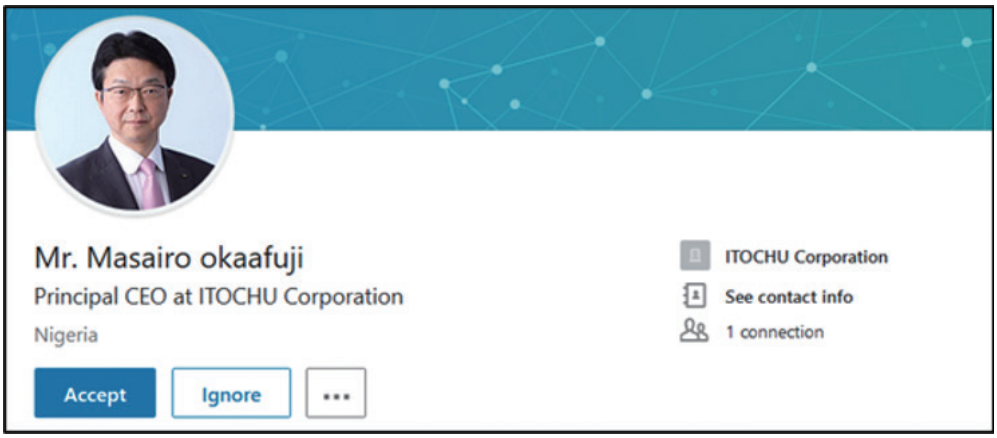


図 21：幹部を装う LinkedIn のアカウント

2.9 攻撃者の素性

2.6 で前述したように、メールヘッダなどから攻撃の発信元が推測可能な場合があります。X-Originated-IP ヘッダに加えて、Date ヘッダに発信元のタイムゾーン情報が記載されている場合があります。他にも攻撃者が偽のインボイス（PDF）を送ってきた場合、PDF ファイルのメタデータにタイムゾーン情報が残っていることがあります。以前より、ナイジェリア国籍の犯行グループが FBI などによって逮捕されるといった報道がありましたが、日本国内においては、ビジネスメール詐欺に関わった容疑で、ナイジェリア国籍の容疑者や、背後にあるナイジェリアの犯罪組織からの指示を受けた日本人の容疑者が逮捕されています [7]。手紙や FAX の時代からインターネットが普及した現在に至るまで、そしてロマンス詐欺からビジネスメール詐欺に至るまで、ナイジェリアを中心とした西アフリカが舞台となっているようです。また最近では、ロシアを拠点とする犯罪グループが BEC を仕掛けているという報告もされています [8]。

7 https://www.sankei.com/affairs/news/181003/afr1810030018-n1.html
https://www.asahi.com/articles/DA3S13954689.html
8 https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/

3. ターゲティングから送金させるまでの一連の流れ (BEC Kill Chain)

攻撃者が BEC の詐欺メールを送付する前には用意周到な準備段階があることを忘れてはいけません。ここでは、攻撃者がターゲティングから送金を促すまでの一連の行動を 5 つのフェーズに分けてモデル化し、BEC Kill Chain とします。(図 22)

図 22：BEC Kill Chain – ターゲティングから送金させるまでの一連のフェーズ

3.1 OSINT によるターゲティング

攻撃者は、ターゲットになりそうな組織の業種や使命、経営層や財務担当の名前などを調べるため、組織の Web サイト、SNS、または一般にセールスリードを獲得するために使われる下記のようなサービスを活用することが多いようです。このような公開された情報源から目的の情報を探すことを OSINT(Open Source Intelligence)と呼びます。

セールスリードを獲得するためのサービス：
Intelius - https://www.intelius.com/
leadiQ - https://leadiq.com/
lead411 - https://www.lead411.com/
Prospect.io - https://prospect.io/
SalesRipe - https://www.salesripe.com/

同時に、詐欺メールの送付先となりえるメールアドレスを収集するため、様々な OSINT ツールや入手可能な漏えいデータを活用していると考えられます。

3.2 メールアカウントへ不正ログイン

効果的に詐欺を仕掛けるには、取引の状況を事前に把握しておくことが必要です。多くの場合、狙ったメールアカウントの認証情報を窃取、そして不正にログインし、メールを盗み見することで、取引金額や振込予定時期などの詳細を監視し、絶妙なタイミングで詐欺(指定口座への振り込み依頼)を仕掛けてくるのです。認証情報を窃取する方法として、"フィッシング"、"パスワードスプレー攻撃"、そして"マルウェア"のいずれかの手口が使われます。それぞれ詳細を解説します。

まずフィッシングですが、メールシステムをクラウドサービスへ移行する昨今の流行りもあり、特に Microsoft Office 365 の認証情報を狙ったフィッシング攻撃が数多く見られます。実際にマクニカ富士エレグループにも、図 23 のようなフィッシングメールが届いており、Microsoft の Office 365 サービスの一つである OneDrive からの通知を装っています。

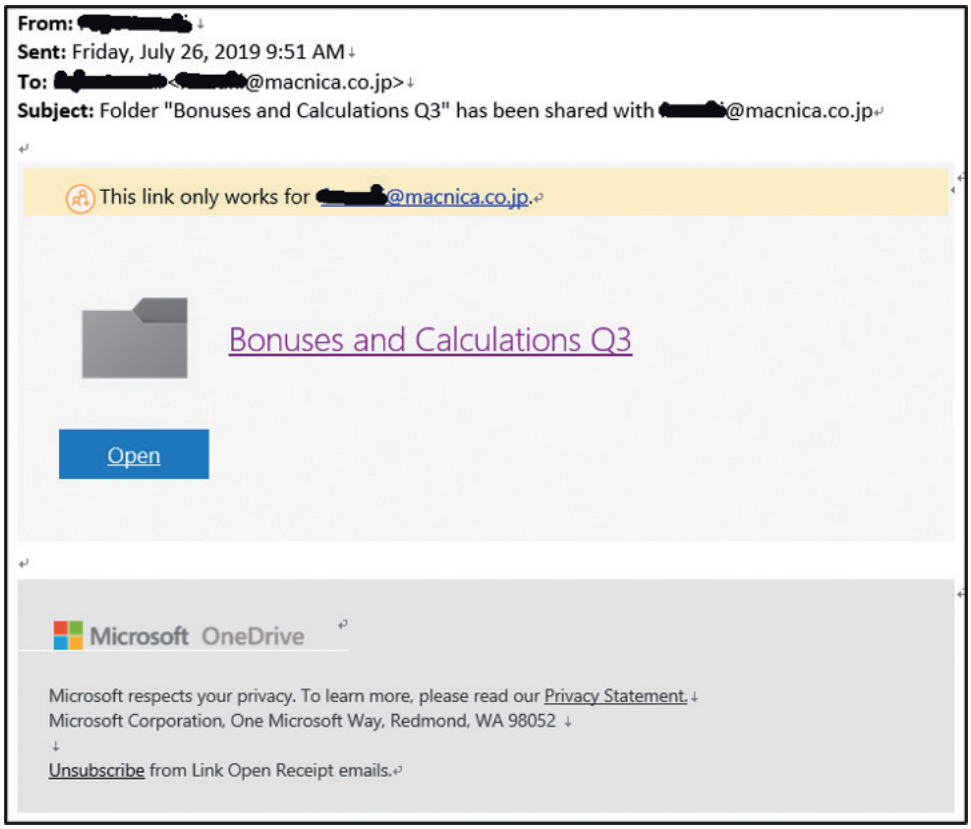


図 23：Office 365 の認証情報の窃取を狙ったフィッシングメール

メール内のリンク先へアクセスすると、図 24 のような Office 365 のログイン画面を模したフィッシングメールサイトへ誘導されます。ここでパスワードの入力を促されますが、実際に入力してしまうと、攻撃者に窃取されてしまいます。

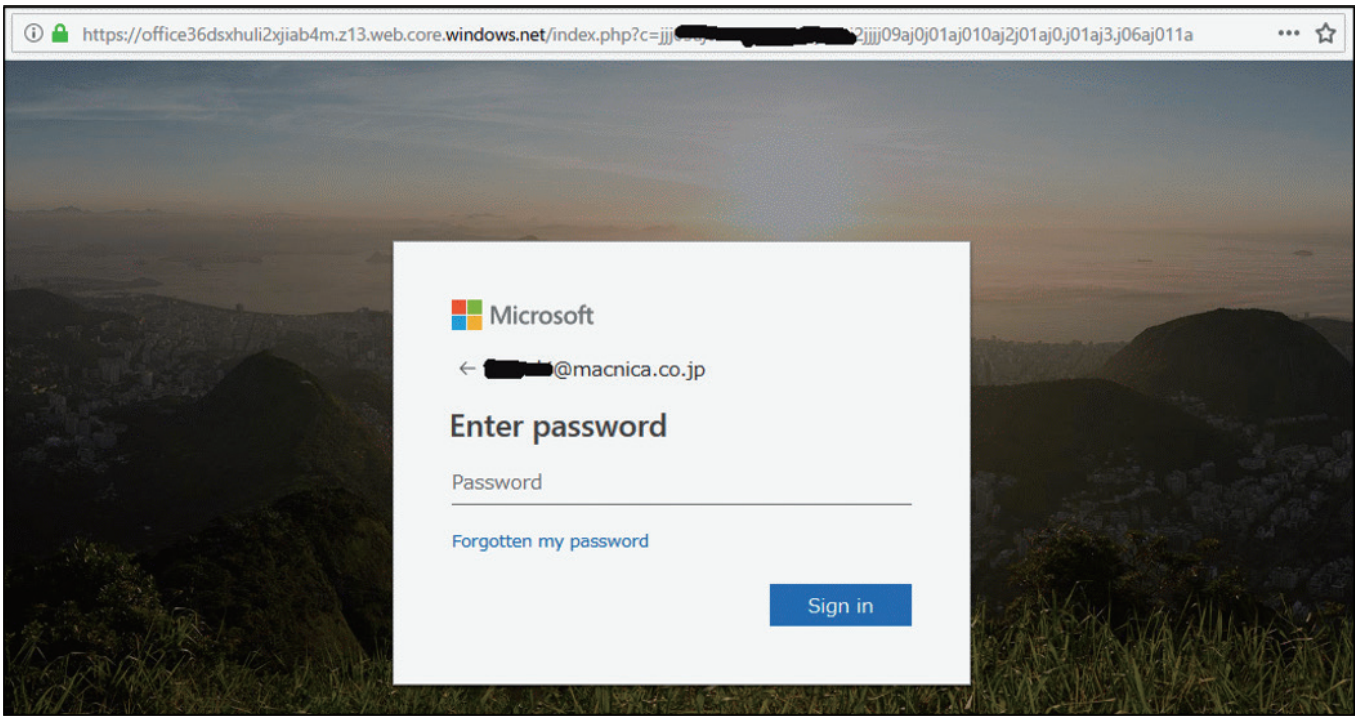


図 24：Office 365 のログイン画面を模したフィッシングサイト

図 24 で示した偽のログイン画面は Microsoft Azure のサービス上にホストされているため、図 25 のようにドメインが Microsoft 社の所有するドメイン（windows.net）である上に、SSL/TLS 接続を示す緑色の鍵マークがあるため、フィッシングサイトだと気づくことが比較的難しくなっています。

図 25：Microsoft Azure Storage の上にホストされたフィッシングサイトの URL

図 26 は、Outlook Web Access（OWA）のログイン画面を模したフィッシングサイトです。

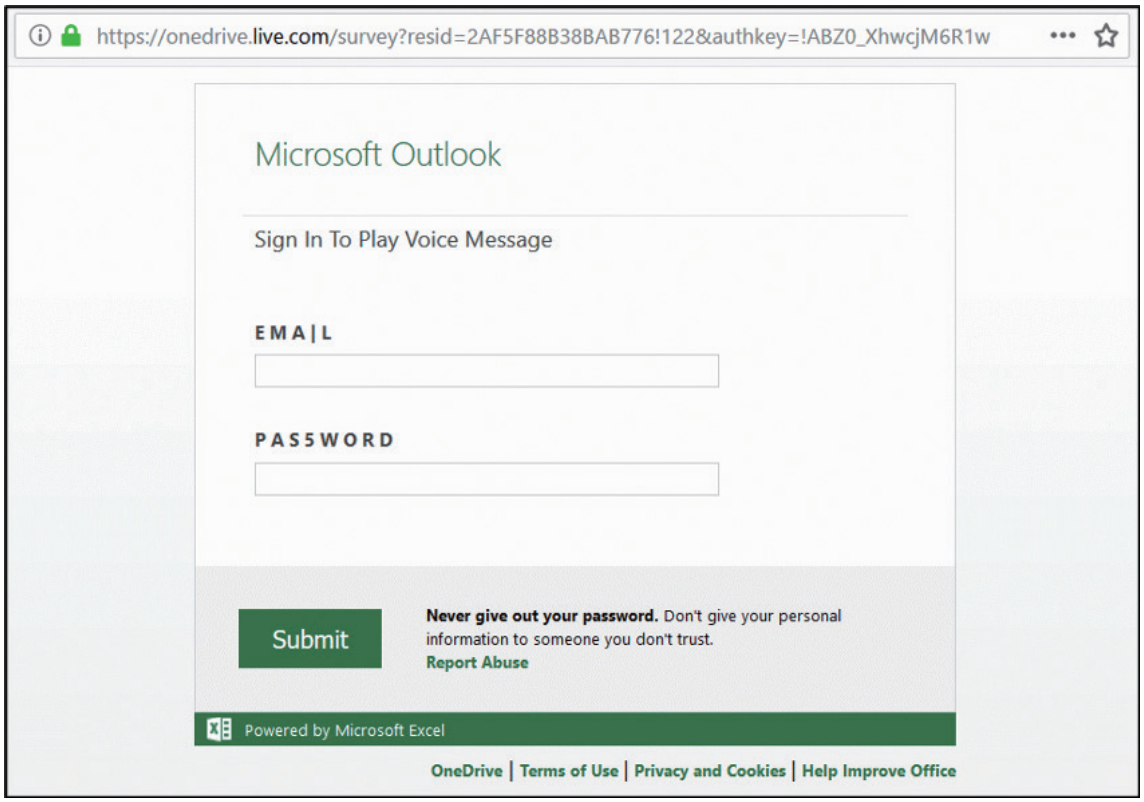


図 26：Outlook Web Access のログイン画面を模したフィッシングサイト

偽のログイン画面をよく見ると、"**EMAIL**"や"**PASSWORD**"となるべき表記が"**EMA|L**"や"**PAS5WORD**"といった検出回避を目的と思われる不審な表記になっています。また、ページ下方に"Powered by Microsoft Excel"という表記があり、Excel のアンケート機能で作られたフォームだと分かり、こちらも不審です。しかし一方で、図 27 のようにドメインは Microsoft 社が所有するドメイン（live.com）である上に、緑色の鍵マークがあるのは図 24 と同様で、一見正しいサイトに見えてしまいます。

図 27：Microsoft OneDrive の上にホストされたフィッシングサイトの URL

いずれにしても、このようなフィッシング攻撃は、メールアカウントの認証情報を窃取する手法で最もよく使われます。

次によく使われる手法は、メールシステムに対するパスワードスプレー攻撃です。IDとパスワードの組み合わせを総当たりで試すブルートフォース攻撃は、同じIDでログイン失敗が多発するとアカウントロックが発生するため有効でない場合があります。そのため、パスワードスプレー攻撃では、同じIDに対するログイン試行を連続して行わず、複数のIDに対して単一のパスワードを試行し、同じIDに対する試行間隔を広げることでアカウントロックを回避します。Office 365のIMAPやPOPに対するパスワードスプレー攻撃での被害が多いことが報告されています[9]。POP/IMAPのようなレガシー認証は二要素認証が実装できないため、パスワードスプレー攻撃の対象となります。このようなレガシー認証は無効化することを強くお勧めします。

最後に紹介する手法がマルウェアを使った認証情報の窃取です。InfoStealer系のマルウェア（LokiBot、Agent Teslaなど）、RAT（Adwind RAT、NetWire、NanoCore、DarkCometなど）、Keylogger（Ardamaxなど）がBECの準備段階として使われていることが複数のセキュリティベンダーから報告されています[10]。マクニカネットワークスが提供するインシデント対応サービスにて対処を行ったBEC事案でも、このうちのいくつかのマルウェアが実際に見つかっています。

3.3 メールボックスの偵察

メールアカウントに不正ログインできる状態になると、取引状況を把握するため、送受信されるメール内容を盗み見します。その際、メールを攻撃者のメールアドレスへ転送するための転送ルールを設定することがあります。転送ルールを設定することで、メール内容を閲覧する度に不正ログインする必要がないため、手間と発覚するリスクを軽減することができます。やり取りされるメール内容を盗み見することで、取引の内容、金額、振り込み時期などを把握します。

3.4 詐欺メールの送付

いよいよ詐欺メールを送付するフェーズです。前のフェーズで用意周到な準備と偵察を行っているため、絶妙なタイミングで詐欺を仕掛けることができます。「今まで使っていた口座が監査のために使えないから、別の口座へ振り込んでほしい」など、もっともらしい理由をつけて、攻撃者が事前に準備した口座への振り込みを促します。詐欺メールを送るために使われるインフラは３タイプに分類できます。フリーメールアドレス、類似ドメイン（rnacnica.com や ltochu など）、乗っ取ったメールアドレスの３つです。乗っ取ったメールアドレスから詐欺メールを送る場合は、発覚するリスクを軽減するために、振り分けルールを設定して、取引先から受信するメールすべてをゴミ箱などの普段閲覧しないフォルダへ自動振り分けすることがあります。また、本物と酷似した偽インボイスに振込先口座を記載することで信ぴょう性を高めようとします。

3.5 送金の説得

いつもと違う口座へ振り込むように依頼しても、口座名義（Account Name）が取引先の会社名と違っていたりすると、すんなり送金してくれない場合もあります。そういった場合には、「口座名義は関連会社の名前になっているから問題ない」など、なんとかもっともらしい理由をつけて、早く送金するように説得を試みます。

9 https://www.helpnetsecurity.com/2019/03/20/imap-based-password-spraying/
10 https://threatpost.com/nigerian-bec-scammers-growing-smarter-more-dangerous/131854/
https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf

4. 対策アプローチ

BEC 対策というと IT での対策と捉えられがちですが、それは間違った認識です。BEC 対策に特効薬はないという認識を持った上で、IT だけでなく、経営層や会計部門の観点を含めた総合力が大切です。

4.1 BEC を経営課題と捉える

経営者は次のような認識を持つ必要があります。

- 数十億円以上の被害に遭う可能性がある。
- 自組織を装って取引先に BEC が仕掛けられた場合、取引先が被害に遭う。
- 会計部門、IT 部門、法務部門など、様々なプレイヤーが総合的に対処する必要がある。

4.2 会計部門におけるチェックの強化

IT システム面での対策も重要ですが、最も重要なのは会計部門が異常に気づくことです。基本姿勢として、次のような連絡は全て怪しいと感じることが重要です。

- 「口座が変わった」という連絡
- 「監査のために今までの口座が使えないから別口座に振り込んで」という連絡
- 「経済制裁されている国とのやり取りが発生し口座が一時的に凍結されている」という連絡
- 「COVID-19 による経済封鎖により銀行口座が一時的に使えない」という連絡
- 「子会社の口座に振り込んで欲しい」という連絡
- 「追加料金（手数料や税金など）がかかることが判明したから別口座に振り込んで」という連絡
- 取引先や自組織の幹部からの振り込め連絡
- 不自然な言い回し（日本語、英語）による振り込め連絡
- 国境を跨る送金の連絡（一部例外あり）
- 振込先の口座名義が個人宛や違う会社名になっている

取引先の M&A などにより、振込先の口座が変更になることは不定期に発生することかと思います。そのような場合、事業部門から会計部門（振込担当者）へ口座変更や新規口座登録の連絡がある際に、会計部門が確認すべき項目を予めリスト化しておくことも重要です。例えば、下記のような確認項目をリスト化しておくと良いでしょう。

- 口座情報が正しいか電話で確認したか。
- 確認先の電話番号はメール署名欄に記載されたものではなく名刺などの信頼ある情報源から確認したか。
  もしくは、電話番号を公式ウェブサイトに記載された番号と照合しているか。
- 口座が変更になる理由は明確で不審な点はないか。
- 口座名義が取引先の会社名になっているか。（口座名義が正しい会社名になっている場合もあるので注意）

また、個別の取引だけでなく全ての取引口座を変更するように仕掛けてくることがあります。その際、手続きとして署名入りレターが求められることも攻撃者は想定の範囲です。手続きのプロセスとして、エビデンスのレターを求めることは有効ですが、攻撃者もそこは想定して準備をしているため、前回の申請書フォーマットとの比較や署名の比較など、オリジナルとの比較を忘れないようにしなければいけません。

4.3 取引先への周知

自組織を装った BEC が取引先に仕掛けられた場合に備え、次のようなことを取引先に周知しておく必要があります。

- 「当社から電子メールで振込先口座の変更を依頼することは絶対にない」ということを伝える。
- 不審な場合に問い合わせを受ける電話番号を予め伝えておく。

取引先側の不備による損害は取引先側で負うべきものですが、組織としての体力が低いと経営問題になったり、どちらが悪いかで関係が悪化したり、ビジネス上の問題になることがあります。そのような事態に陥らないために、取引においては BEC の可能性を排除するために双方で予め BEC に関する意識をすり合わせておく必要があります。

また、組織によっては、会計対応をアウトソーシング会社に任せている場合もあるかもしれません。そういったアウトソーシング会社に対しても、BEC の攻撃者が詐欺を仕掛けている事例を確認しています。アウトソーシング会社とも取引先と同様に BEC に関するリスク意識を共有しておく必要があります。

4.4 多要素認証

BEC Kill Chain で解説したように、攻撃者はメールを盗み見するために、メールアカウントへの不正ログインを試みます。不正ログインのリスクを少しでも減らすために、多要素認証は非常に有効な手段です。また POP や IMAP などのレガシー認証は多要素認証を強制できないため無効化することを強く推奨します。特に Office 365 や G-Suite などのクラウドを使用している場合でも、レガシー認証が有効になっていないか確認することをお勧めします。

4.5 フリーメールアドレスからの受信警告

攻撃者は、Gmail、Yahoo メールなどのフリーメールを悪用することが多く、また、受信者に馴染みがないことを狙ってか、図 28 の mail.com というフリーメールサービスに登録されたメールアドレスを悪用する傾向がみられます。

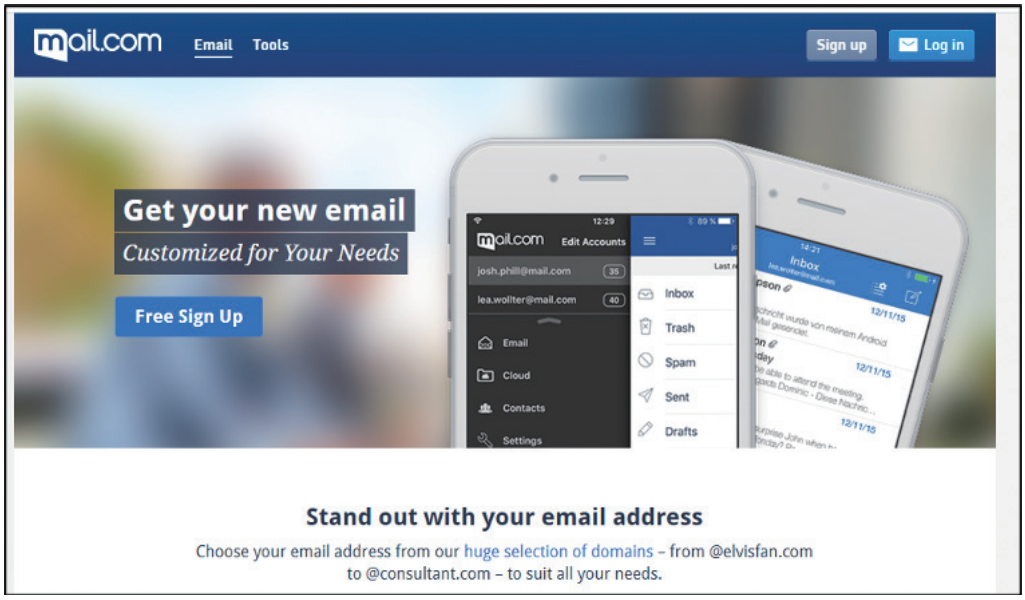


図 28：mail.com のフリーメールサービス

そのため、mail.com の保有するドメインを中心に、スパムフィルタなどで、フリーメールからのメールであることがわかる件名を付加することで、受信者に一定の注意を促す効果があります。攻撃者が盗んだメールを引き継いでメールを送信してきた際に、図 29 のようにフリーメールからの送信とわかる文字列が件名に入っていると、過去の件名と区別がつき、異常に気付く可能性が高まります。

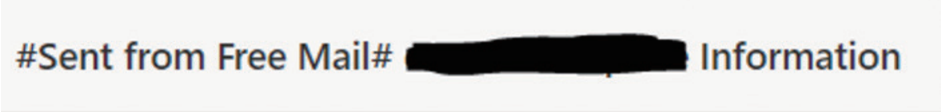


図 29：メール件名にフリーメールからの送信であることを示す標識をつけた例

東南アジアの中小企業では、フリーメールをビジネスに使っているケースも多々あるため、フリーメールの受信制限をすることは運用上困難なことがあります。そのため、フリーメールからのメールであることがわかる件名を一元的に付与することが効果的です。また、メーラーにプラグイン等を導入し、特定のメールアドレスに反応して、フリーメールからの受信であることを知らせることもできます。(図 30)

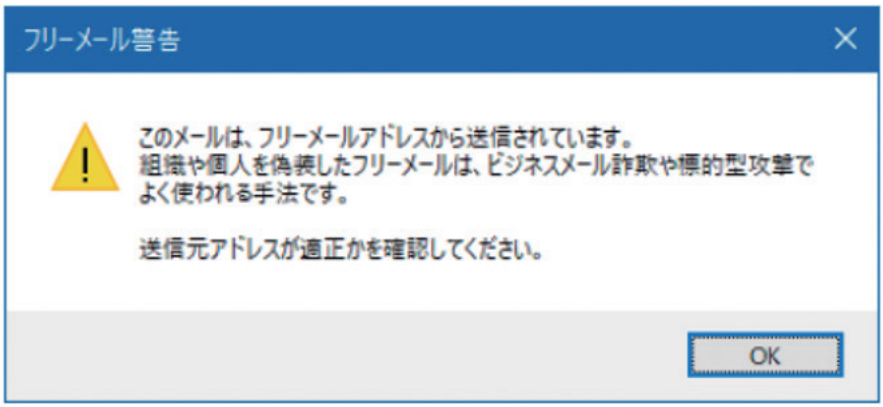


図 30：フリーメールからの送信であること警告するダイアログ(日本語)

4.6 フリーメールアドレスへの送信警告

受信と同様にフリーメール宛に返信する際に、警告をあげることも効果的です。受信と異なり、スパムフィルタ等で確認を実施することは困難ですが、メーラーにプラグインを導入することで実現が可能です。(図 31)

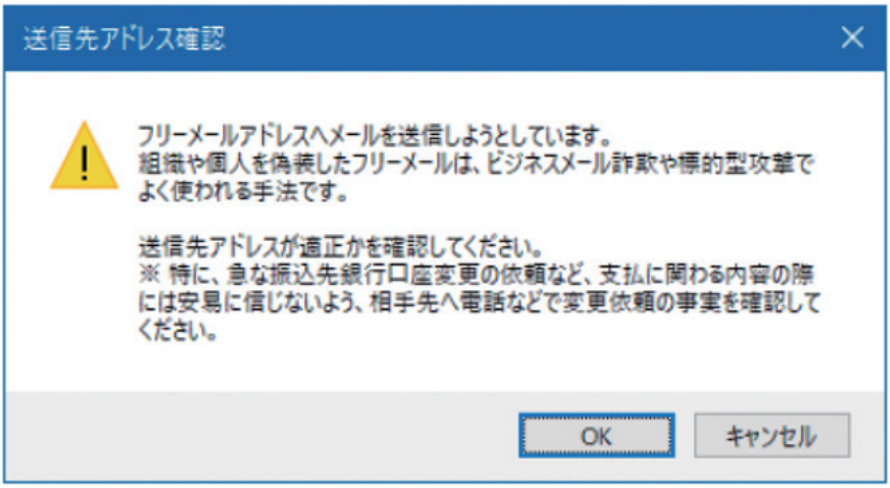


図 31：フリーメールへの送信であること警告するダイアログ(日本語)

このような制限は、例えば送信元アドレスを偽り、返信先(Reply-To)をフリーメールに設定している際にも有効です。

4.7 送信元アドレスと返信先アドレスが異なるときに警告

差出人の情報（From ヘッダ）を正しい送信元に偽り、返信先（Reply-To）を攻撃者のメールアドレスにしているケースが多々あります。このように、送信元と返信先が異なる際に警告をあげる機能も、気づきを与える点で有効です。（図 32）

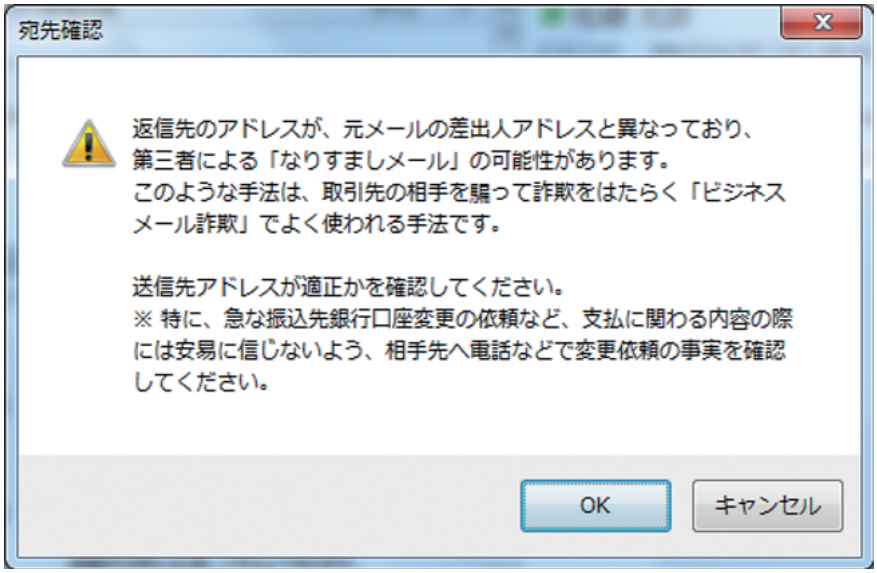


図 32：送信元アドレス（From）と返信先アドレス（Reply-To）が異なることを警告するダイアログ（日本語）

4.8 信頼性の低い TLD からの受信検知

freenom は、特定の TLD（.tk .ml .ga .cf .gq）でドメインを無料取得できるサービスですが、他の TLD と比較して、サイバー犯罪に悪用されることが多いため、基本的に検知やブロックの対象とすべきでしょう。（図 33）

図 33：freenom のドメインサービス

ただし、freenom で利用可能な TLD は、.ml がマリ共和国、.ga がガボン共和国など、それぞれ各国をあらわす TLD でもあり、実際に各国の政府が公式に利用しているケースも確認しています。このことから、freenom 自体を完全に制限することは、自組織の利用状況を把握してから行う必要があります。

4.9 @ の手前に TLD が入るアドレスからの受信検知

攻撃者は @ の手前に TLD が入っているアドレスを使い、少しでも違和感がないように装う場合があります。下記の例のようなメールアドレスは、実際のビジネスで使われることは稀で、攻撃者が使うことが多いため、危険性があるメールとしてフラグを立てたり、システム管理者がコピーを確認したりしてもよいでしょう。

不審なメールアドレス例：
*****.jp@gmail.com
*****.com@gmail.com
*****.net@gmail.com

伊藤忠商事では、この類のアドレスおよび前述したフリーメールや信頼性の低い TLD による異常メールの監査により、2019 年に 2 通の BEC メールを発見し、BEC 行為を未然に防止することができました。監視対象のメール数は一日に多くて数通で、かつ、ビジネス上の正規メールはほとんどありません（正規メールが発生した場合は、ホワイトリストで対応）。BEC による被害を考えると低コストで効果をあげられる手法の一つと言えます。

4.10 類似ドメインの検索

自組織の類似ドメインが登録されていないか確認することで、BEC に気づくことができる場合があります。TLD 違いのドメインや打ち間違えが発生しそうなドメインは下記サイトのような無料サービスである程度は検索できます（図 34）。

類似ドメインの検索に使えるサービス：
https://dnslytics.com/domain-typos
https://dnpedia.com/tlds/search.php
https://dnstwister.report/

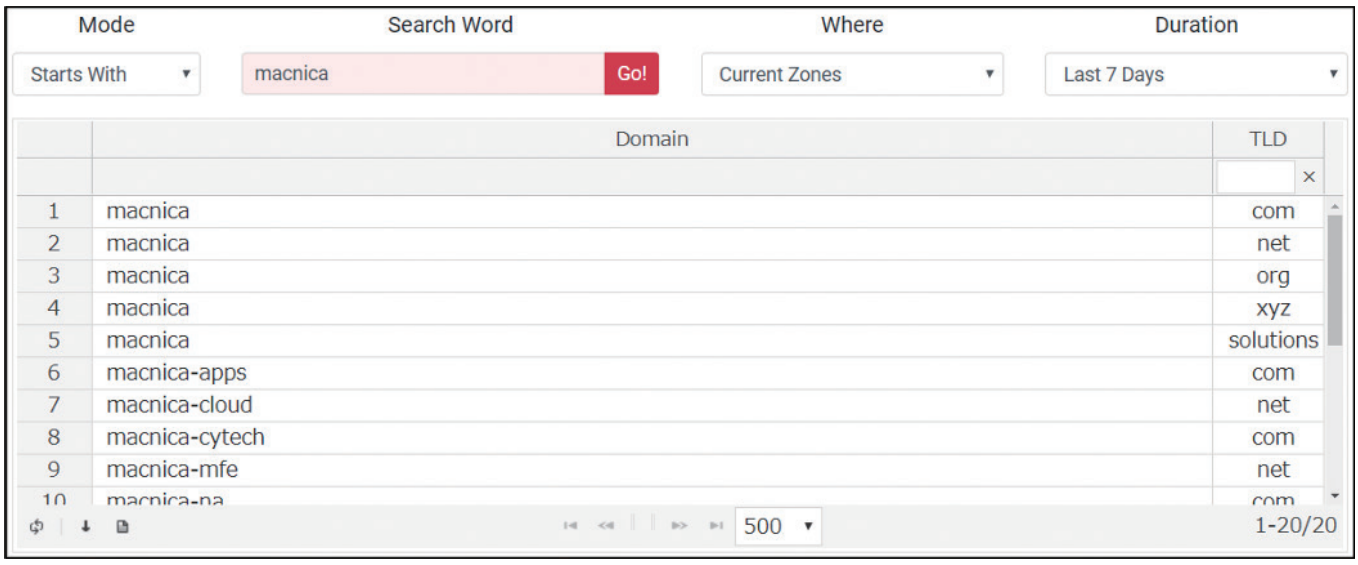


図 34：類似ドメインの検索サービス

4.11 DMARC

DMARC を実装することで、自組織のドメインを詐称したメールが、どこにどれだけ送られているのかを把握できるようになります。そのため、自組織になりすました BEC により取引先で発生する実被害を未然に防げる可能性があります。しかし、攻撃者が自組織と全く同じドメインをそのまま詐称した場合のみに効果があり、類似ドメイン（rnacnica.com や ltochu など）を使われる場合は DMARC の対象外です。また DMARC の効果を得るには、送信側と受信側の双方の組織で DMARC を実装している必要がありますが、日本国内における DMARC の普及率は現状かなり低いのが課題です。

5. インシデント対応

もし BEC に遭遇した場合、未遂、既遂問わず、様々なアクションを取る必要があります。ここでは、実際に対処として行う必要がある項目をいくつか挙げます。

5.1 銀行や法執行機関への連絡（送金の取り戻し）

攻撃者の口座に振り込んでしまった場合、何はともあれ、可能な限り早く、送金の取り戻しを行う必要があります。現地捜査機関および金融機関への連絡を、自組織の法務部門との連携しながら進めましょう。この行動は早ければ早いほどいいことは言うまでもありません。

5.2 メールアカウントが侵害されていないか確認

BEC Kill Chain のところで示したように、攻撃者が事前に取引詳細を把握するためにメールアカウントの認証情報を窃取するのは常套手段です。取引詳細を把握した上で仕掛けられた詐欺であれば、自組織もしくは取引先のメールアカウントが侵害されている可能性が高いと言えます。具体的には以下の点をチェックすることで、メールアカウントが攻撃者によって侵害されていないか確認することができます。

確認項目：
不審な転送設定がないか確認
不審なメール振り分けルールがないか確認
ログから不正ログインの形跡がないか確認

5.3 マルウェア感染がないか確認

3.2 にて前述したように、メールアカウントの認証情報を窃取するために InfoStealer、RAT、Keylogger などのマルウェアが使われることがありますが、このようなマルウェアに PC が感染していないか確認した方が良いでしょう。アンチウイルスの定義ファイルを最新にしてフルスキャンを行ったり、マルウェアの侵害痕跡を調査する専用ツールなどを使ったりします。

5.4 パスワードの変更

不正ログインされた可能性のあるメールアカウントや、マルウェア感染の疑いがある PC で使っていたアカウントに関わるパスワードは全て変更しておきましょう。

5.5 攻撃者が取得したドメインのテイクダウン

自組織の類似ドメインなどが取得されている場合、放置しておくと、攻撃者は再び自組織を装って取引先に BEC を仕掛けるでしょう。そうならないように、ドメインレジストラの Abuse 窓口へ連絡し、当該ドメインをテイクダウンしてもらいましょう。Whois 情報からドメインレジストラおよび Abuse 窓口（メールアドレス）を確認することができます。ドメインレジストラから相応のエビデンスを求められることも多いので、BEC メールのスクリーンショットなどを提出しましょう。ドメインレジストラによっては、対応が遅いなど、対応に積極性が見られない場合がありますが、粘り強く交渉し、テイクダウンまでもっていきましょう。

5.6 取引先との交渉と按分

2.4 で前述したように、取引先を騙った BEC によって、自組織で実被害（攻撃者への振り込み）が発生した場合、取引先側のセキュリティに問題（メールアカウントの侵害など）が生じている可能性があります。その事実を両社が認識することができれば、振り込んでしまった被害額を交渉によって按分することが可能な場合があります。逆に、自組織を騙った BEC によって、取引先で実被害が発生した場合は、自組織側のセキュリティに問題が生じている可能性があり、被害額の按分に応じなければならない場合もあるでしょう。

マクニカネットワークス株式会社

本社　〒222-8562 横浜市港北区新横浜1-5-5
TEL.045-476-2010 FAX.045-476-2060

西日本営業所　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916　FAX.06-6227-6917

第1版

2020年7月