寄稿

被害額は世界で1.4兆円 脅威高まるBECの今

メールの相手、本当は誰だ 手の内を知って対策を

企業版振り込め詐欺ともいえる「ビジネスメール詐欺（BEC）」の脅威が高まっている。人をだます行為であり、従来のセキュリティー対策製品だけでは対策しにくい。犯罪者の手の内を知ることが対策の第一歩だ。

佐藤 元彦 氏
伊藤忠商事 IT企画部 上級サイバーセキュリティ分析官 兼 千葉大学 准教授

「BEC（ビジネスメール詐欺）」という言葉に世界で注目が集まっている。攻撃者が取引先などを装ってメールで送金を促し、大金を一瞬にして奪うサイバー詐欺である。BECはBusiness E-mail Compromiseの頭字語で米国での発音は「ビーイーシー」が主流だ。

米国でBEC被害の抑制に力を入れる連邦捜査局（FBI）は2018年7月に最新状況を公表した。2013年10月から2018年5月までの5年弱の間に世界中で発生したBECによる被害件数は7万8617件で、損失額は合計125億ドル（約1兆4000億円）に達したという。

日本でも2017年末に大手航空会社が4億円弱の被害に遭い、大きく報じられた。脅威は他人事ではない。

表に出ない最新情報

筆者はサイバーセキュリティーの専門家として、伊藤忠商事でセキュリティー対策について企画立案から運用実務まで担当している。商社は世界中の企業を相手にするため、BECに限らず多様な詐欺メールが日々届く。

特にBECに関して、当社のCSIRT（コンピューター・セキュリティー・インシデント・レスポンス・チーム）である「ITCCERT」は数年前から社内の様々な部門と連携しながら、被害を防ぐ策に注力してきた。昨今、国内の専門家がBECに言及し始めているが、タイミングが遅く、その見解を的外れと感じている。例えばセキュリティー会社や情報処理推進機構（IPA）は日本語で書かれた詐欺メールを2018年になって初めて確認したと公表しているが、ITCCERTは2017年に複数観測し、関連機関に共有するとともに内外に注意喚起を発した。

この時間差が生じる理由は、BECが大規模な一斉攻撃やマルウエアを使う攻撃ではなく、企業の個別メールのやり取りに入り込む詐欺行為だからだ。セキュリティー会社や公的機関がその動きをすぐに知るのは難しい。

業務上、筆者はあらゆるサイバーセキュリティー分野をリサーチしているが、BECは現在最も注視する分野の一つである。リサーチの一環で2018年7月に米国カリフォルニア州で開かれた、BECの被害を防ぐためのクローズドなコミュニティーに日本企業から唯一参加した。米国企業における被害の

深刻さと手口の変化を肌で感じるとともに、その対策の実情やコミュニティーの取り組みについても学ぶことができた。残念ながら日本で同様の取り組みはまだ存在しない。

BECに2つの攻撃タイプ

BECについて改めて定義しておこう。FBIは次のように定義する。「恒常的に海外送金しているサプライヤーや企業とのビジネス上の仕組みを狙う洗練された詐欺である。操作端末への不正侵入やソーシャルハッキング（編集部注：人間の心理や行動の隙を悪用して重要情報を盗む手法でソーシャルエンジニアリングともいう）によって得たビジネスの電子メールアカウントに不正侵入して、不正送金させる」。

企業を狙うBECに対処するにはまずその仕組みを理解したい。攻撃タイプは主に2つで、取引に入り込むタイプと、CEO（最高経営責任者）やCFO（最高財務責任者）などの役職者を詐称するタイプがある。

前者は主に請求書を不正に入手し、口座番号を改ざんしたり口座変更を依頼してたりして不正入金を誘う。後者は役職者が担当者にM＆A（合併・買収）といった機密情報を伝えて極秘の送金を依頼してくる。

BECに対応する最も効果のある抜本的な対策は会計部門が業務を進めるなかで異常を検知して対処する取り組みである。会計部門に対して、役職者から秘密の送金を頼む詐欺や緊急の口座変更を依頼する詐欺がある事実を周知徹底する取り組みがBEC対策の根幹といえる。

情報システム部門やセキュリティー部門は自分たちが取り組むBEC対策はあくまで補助的な役割にすぎないと認識しておきたい。そのうえで何ができるかを考える必要がある。

FBIなどの啓発活動でBECの手口に関する認識が広がるなか、攻撃者は手口を新たなステージに移行させつつある。最新の攻撃手法はビジネスのやり取りの「途中」から犯人がなりすます「マン・イン・ザ・Eメール（MITE：Man in the E-mail）」である。

ネットバンキングからの不正送金を誘う際によく使われる攻撃手法「マン・イン・ザ・ミドル（中間者攻撃）」をメールに拡大したものだ。最近のBEC事案を分析するとMITEを使うケースが増えていると実感している。

以下は伊藤忠商事グループで実際にあった貿易取引のやり取りだ。原文は英語だったが、ここでは日本語に訳している。攻撃者がどこで割り込んできたか、考えながら見てほしい。

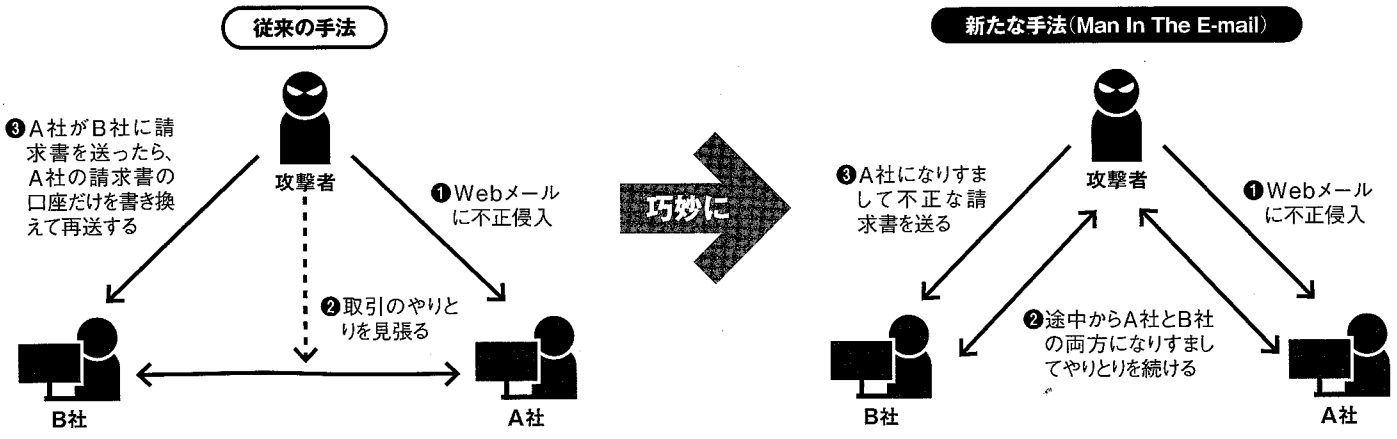
【1通目】
こんにちは。署名済みのPL（出荷商品の容積数量書）とP/I（見積書）をお送りします。ご確認ください。
※PLとP/Iのファイルが添付されている
【2通目】
発注を受け付けました。外出していますのでアシスタントが署名済みのP/Iを後ほどお送りします。また、元地（もとち）回収したB/L（船荷証券）をお送りします。ご確認ください。
※B/Lのファイルが添付されている
【3通目】
ご確認いただきありがとうございます。送金する前にお知らせいただけませんか。会社の口座に関して、ちょっと問題が発生しまして。
【4通目】
送金予定を教えていただきありがとうございます。送金していただく新しい銀行口座を書いた新しいP/I（編集部注：ここでは請求書の役割を果たす）をお送りします。ご注意ください。お手間をおかけして申し訳ないです。
※P/Iのファイルが添付されている

さて、いかがだろうか。実はこのやり取りでは「1通目」から攻撃者が送信してきている。

このケースでも攻撃者はじっと取引

攻撃者がずっとメール相手になりすます

図 BEC（ビジネスメール詐欺）の手法の変化



を監視しながらやり取りを学び、BECの準備をしている。その点は従来のBECの手口と変わらない。

だが、従来のように相手に請求書を相手に送るタイミングで割り込んでくるのはなく、契約が成立する頃から間に入って、ビジネスのやり取り自体を巧みにコントロールしてくる。2通目にある不在の言い訳や3通目の口座に問題が生じた部分などがそれである。

メールをやり取りしている途中で相手が違う人、すなわち攻撃者に入れ替わったらさすがに気付くと思うかもしれない。だがここも巧みでボロを出さない。攻撃者は基本的にお互いのメールを転送しているだけなので、当人にとっては「いつものやり取り」なのだ。

もし相手が口座変更を申し入れてきて「おかしい」と感じてメールの差出人を確認しても、取引が成立した頃から使っているメールアドレスのままだ。「おかしいところはない」と、担当者は口座変更を了承してしまうのだ。

署名の電話番号を信じるな

前述したようにBEC対応の本丸は会計部門である。ではどんな「異常」に気付けば被害を未然に防げるのか。例えば「突然の口座変更を依頼された」や「個人口座あるいは取引先と社名の異なる口座に入金するよう依頼された」「追加の手数料や税金を別口座に入金するよう依頼された」といったケースは要注意だ。

こうした場合、「お金を振り込む前に相手先に電話で確認する必要がある」とされている。だが既に攻撃者はそうした注意喚起を逆手に取って、攻撃者につながる電話番号をメールの署名に記載するようになっている。

電話先は秘書代行サービスのような会社だ。もちろん電話をかけてきた人にはそんなことは言わず、「担当者が不在なので折り返す」とだけ回答して電話を切った後、サービス利用者、つまり攻撃者にいつ誰から電話があったかを伝える。攻撃者は標的にコールバックして「その口座は正しい」と伝えて信頼させ、振り込ませるのだ。

BECの被害を防ぐにはメールの署名に記載された電話番号は無視しよう。必ず相手先の名刺にある電話番号や取引先のWebサイトに記載された電話番号に電話をする必要がある。

実際に未遂に終わったBEC被害事例を調べると、電話番号を再確認する過程で相違に気付き、詐欺を免れた

やりとりを巧みに操る「MITE」

図 伊藤忠商事のグループ会社の貿易取引で届いた実際のBECメール

（取引先と取引が成立後、攻撃者が割り込む）

↓

【1通目】
Good day
We would like to send the signed PL and P/I, please see attachment.
Thank you for your understand.
Best Regards.

こんにちは。署名済みのPL（出荷商品の容積数量書）とP/I（見積書）をお送りします。ご確認ください。

※PLとP/Iのファイルが添付されている

↓

【2通目】
Have good day for you
1. Refer to the new order, It'ok.I am out of office, So assistant will send you the signed PI
2. We would like to send you the Surrendered B/L. Please see attachment.
Best Regards

発注を受け付けました。外出していますのでアシスタントが署名済みのP/Iを後ほどお送りします。元地（もとち）回収したB/L（船荷証券）をお送りします。ご確認ください。

※B/Lのファイルが添付されている

↗

【3通目】
Thank you for your confirm.
kindly inform us before any remmittance is made to us, as we have abit of issues with our company account at the moment.

ご確認いただきありがとうございます。送金する前にお知らせいただけませんか。会社の口座に関して、ちょっと問題が発生しまして。

↓

【4通目】
Thanks for the update on payment schedule.
Please see attachment with the PI containing new bank information for the remmittance.
Please take note.
Apologies for the inconveniences.

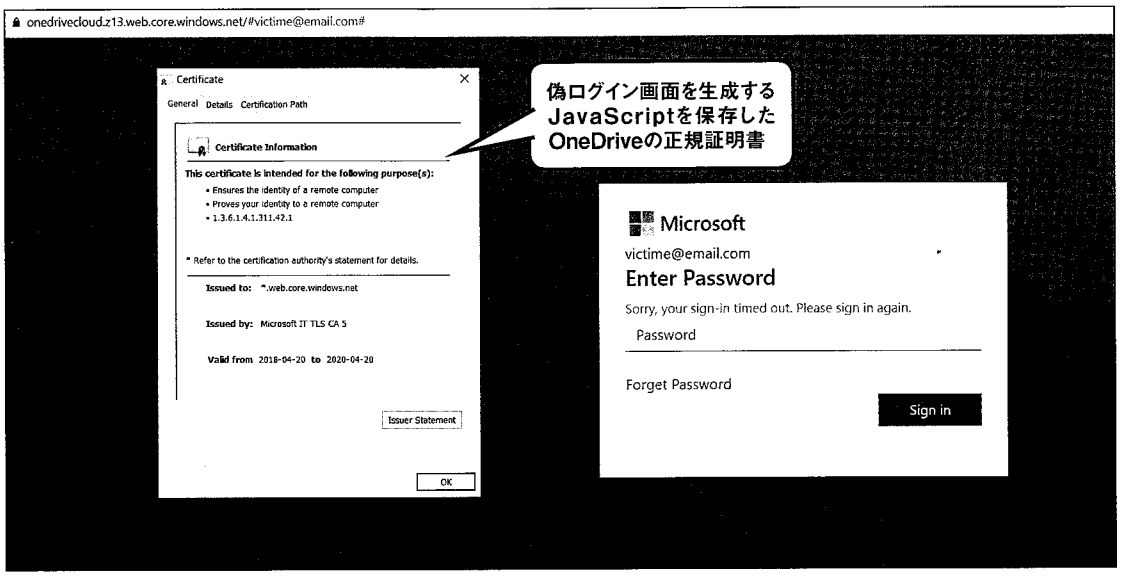
送金予定を教えていただきありがとうございます。送金していただく新しい銀行口座を書いた新しいP/I（編集部注：ここでは請求書の役割を果たす）をお送りします。ご注意ください。
お手間をおかけして申し訳ないです。

※P/Iのファイルが添付されている

（内容は一部筆者が改変。スペルミスは原文のまま）

ログイン情報を盗むフィッシングはより巧妙に

図 米マイクロソフトのクラウドストレージサービス「OneDrive」を悪用して同社の証明書を表示させるフィッシング手法



ケースが圧倒的に多い。海外取引がある企業の会計部門では上記の取り組みの周知徹底が最も効果的であると考える。情報システム部門やセキュリティー部門からも再度確認してほしい。

とはいえ自社の守りを高めてもBECの被害を防げるとは限らない。取引先がBECの被害に遭って、自社に入金されるはずの金銭が詐取されるケースがあるからだ。自社への入金が滞ったり、最悪の場合、回収できなくなったりする可能性がある。

現段階ではサイバー攻撃による損害を補償する「サイバー保険」や貿易上の損害を補償する「貿易保険」はBEC被害を適用外とするケースがある。BECの被害額がそのまま損失につながる可能性が高いため、自社や取引先を守るためにも全社で取り組みたい。

例えばBEC攻撃者の行為と誤解されないためにも「メールによる突然の口座変更を決してしない」と会社として宣言し、社員にもそう教育して徹底させる。そのうえで宣言を取引先にも伝えるような取り組みが欠かせない。

ある会社の海外取引の多い部署は全部員のメールのフッターに「当社はメールで振込口座の変更を依頼しません」と英語で記述しているという。組織全体にBECの存在を周知し、組織全体で対策する。当たり前だがそれが効果的な策の一つである。

多要素認証の導入で全て解決？

全社を挙げたBEC対策を進めるに当たり、情報システム部門やセキュリティー部門が取り組む内容は3つある。「被害を防ぐ間接的なセキュリティー対策」「不審なメールの真偽判断」「事案発生時の原因追及と侵害対応」である。順に説明しよう。

攻撃者はBECを仕掛けようとする場合、まず標的のメールアカウントに侵入するのが常とう手段だ。そもそも攻撃者はどのようにアカウント情報を入手するのだろうか。

伊藤忠商事グループで観測したBECの未遂事案を取引先とともに分析すると、BECで使われたアカウント情報の多くはフィッシングで盗まれていた。次に多かったのはパスワード推測攻撃による窃盗である。マルウエア感染が原因で盗まれたと疑われるケースもあったが、割合は非常に少ない。

これらの攻撃を防ぐのが「被害を防ぐ間接的なセキュリティー対策」だ。ただ従来のセキュリティー対策の枠内であり、ここでは詳しく言及しない。

とはいえ、攻撃手法は日々巧妙になっている。筆者が最近舌を巻いたのは米マイクロソフトのクラウドストレージサービス「OneDrive」を悪用したケースだ。偽のログイン画面を生成するための暗号化されたJavaScriptがOneDrive上にあるため、証明書は正規なものになるのだ。さらに、偽ログイン画面はhttps通信を使っており、URLやコンテンツからフィッシングサイトだと見破ったりアクセスを制限したりするのは相当に難しい。

攻撃手法が進化するなか、既存の対策はどれも完全ではなく、ログイン情報はいつ盗まれてもおかしくない。こう考え、多くの組織が安全性を高める目的で「多要素認証」を導入しつつある。画面にログイン情報を入力するだけでなく、スマートフォンなどでも証明書を認証に使ったり、SMS（ショー

ト・メッセージング・サービス）で通信したPINを追加入力させたりするなど、複数の認証機能を設ける仕組みだ。

多要素認証は不正ログインに対して非常に効果的だ。伊藤忠商事でもグループ会社に導入を勧めている。ただ残念ながら多要素認証を併用しても完全な対策にはならないケースがある。それどころか、システム管理者の認識不足によって、攻撃対応が手遅れになってしまう事態が生じかねない。

認識不足の例を2つ挙げる。一つはクラウド型メールサービスを使う際、様々なプロトコルでメールが使える事実を管理者が認識していない場合だ。

例えばマイクロソフトのグループウエアのクラウドサービス「Office 365」はWebブラウザーでメールを読み書きできるだけでなく、標準でPOPやIMAPでもメールサービスにアクセスできる。しかもその場合、多要素認証は要求されない。この事実を知らず、必要がないのにPOPやIMAPでのアクセスを放置していると危険だ。攻撃者が侵入口に使ったりパスワード推測攻撃で使ったりできてしまう。

もう一つはAPI（アプリケーション・プログラミング・インターフェース）だ。APIを公開しているWebメールサービスは少なくないが、APIでのアクセスに多要素認証を要求しないサービスもある。APIに適切なアクセス制御をかけておかないと、やはり攻撃者に悪用されかねない。

情報システム部門やセキュリティー部門はセキュリティーをクラウドサービスに任せ切りにしてはいけない。不要なプロトコルやAPIを使えなくしたり、それらによるアクセスに対しセキュリティー設定を追加したりして自らセキュリティーを高める必要がある。

「mail.com」に要警戒

加えてBECの間接対策に欠かせないのがWebメールのログの定期監査だ。特にログインの失敗やログイン操作のアクセス元の国に関するログの監査は効果が高いので勧めたい。

多要素認証を使っている場合、ログイン失敗のログ監査において、通常の認証に追加した認証で失敗しているかどうかに特に注目すべきだ。追加の認証まで進んでいると、既に通常の認証で使うログイン情報が第三者に盗まれ悪用されている可能性が高いからだ。

該当したユーザーにはパスワードを使い回していないかをすぐに確かめ、もし使い回しているようであれば変更させる。同時に攻撃者が他のサービスに侵入していないかを調べたい。

ログイン操作をされた国の監査に関しては、BECの攻撃者グループはアクセス元を秘匿する作業にそれほど注意を払っていないようで、ナイジェリアとその周辺国からのログインに注目すると異常が見つかるケースが多い。踏み台にされている端末が多いロシアやインド、ベトナム、南米諸国からのログインにも気を付けたい。ログを適正に監視していると、パスワードの定期変更のタイミングで攻撃者がログインに失敗し、侵害が判明する場合もある。

筆者がBECメールの分析を続けた結果、フリーメールが一定数悪用されていると分かった。hoge.nikkeibp.co.jp@example.comのように、標的のメールアドレスを（@より前の）ユーザー名に埋め込んだ形だ。

これを逆手に取ると受信者が異常に気付きやすくなる仕組みを構築できる。SMTPの「envelope from」がフリーメールのアドレスだったら、「フリー

詐欺メールの見破り方を学ぶ

図 伊藤忠商事のCSIRT「ITCCERT」がグループ会社のシステム管理者向けに開いている、メールヘッダーの読み方を学ぶワークショップの出題例

【演習 1】
以下は、A社担当者（以下ユーザ）が受信した不審と思われるメールです。

【前提条件】
・商流
B社⇔A社⇔C社（中国）
※A社は、B社とC社の取引を仲介

・正規担当者
B社担当者：CHEN <chenzheng@example.com>
A社担当者：Taro<taro@example.co.jp>

問1 以下メールが不正メールと判断できる根拠を、メールヘッダより可能な限り提示してください。
（例： X行目の情報から、正しくないメールサーバから送信されている、など）
さらに使われている情報から、不正行為の背景を調べてください。

問2 本メールには正規のinvoiceを改ざんしたファイルが添付されており、情報流出が疑われます。
A社情報システム部門として、今後どのような対応を行うべきか考察してください。

□メール本文

Good day!

Pls find attached 95% frt invoice of cape [redacted] and waiting chrtrs kindly remittance with many thanks.

□メールヘッダー

No	ヘッダー
1	Delivered-To: taro@example.co.jp
2	Received: by 127.0.0.1 with SMTP id a12csp2734512ioc;
3	Mon, 27 Nov 2018 20:04:45 -0800 (PST)
4	X-Received: by 127.0.0.1 with SMTP id b19mr27791719otb.229.15118418885344;
5	Mon, 27 Nov 2018 20:04:45 -0800 (PST)
6	Return-Path: <business+bncBAABBXOA6PIAKGQEJ3JT7HQ@example.co.jp>
7	Received: from mail-sor-f69.google.com (mail-sor-f69.google.com. [209.85.220.69])
8	by mx.google.com with SMTPS id l32sor2178294otl.22.2017.11.27.20.04.45
9	for <taro@example.co.jp>
10	(Google Transport Security);
11	Mon, 27 Nov 2018 20:04:45 -0800 (PST)

メールから受信」といった注意喚起をメールの件名に追加するようにメールサーバーを設定すればよい。

攻撃者は詐欺メールに「mail.com」のフリーメールを使うケースが多い。mail.comはdr.comなど複数ドメインを使えるので、それら全てには強い警告を発する件名を付加するとよい。

もちろん、標的の類似ドメインを取得したメールや、乗っ取ったアカウントのメールでBECを仕掛けてくるパターンもある。ただ悪用する割合が高いフリーメールに注意喚起すると標的型など他の攻撃の対策にもつながる副次的な効果も期待できる。

ヘッダーやプロパティにも注目

情報システム部門やセキュリティー部門が取り組むべき項目の2つ目が「不審なメールの真偽判断」だ。会計部門はBECの疑いを持ったとき、情報システム部門やセキュリティー部門に「メールの真偽」の判断を求めてくる。そのため、判断するためのスキルは身に付けておくべきである。

最も簡単な判断方法は疑わしいメールと明らかに正しいメールの双方のメールヘッダーを比較する方法だ。送信元サーバーやメーラーのユーザーエージェントを見比べると普段との違いがすぐに分かる。アカウントが乗っ取られている場合、メーラーのユーザーエージェントの違いや「ヘッダーが接続元IPを含んでいるか」などで比較すると真偽を判断しやすい。

見積書や請求書などがPDFファイルで添付されている場合、プロパティを開いてどんな製品でPDF化したかを調べよう。攻撃者は盗んだ請求書の口座部分だけを改ざんして、フリーのPDF変換サービスを使ってPDFを再作成するケースが多い。

もし自社や取引先で使うPDF変換ツールと異なれば疑いは濃くなる。同様にプロパティにあるタイムゾーンが自社や取引先の所在地のタイムゾーンと異なる場合も要注意だ。

筆者はグループ会社のシステム部員に対し、メールヘッダーを読んだりファイルの属性を確認したりするスキルを身に付けさせようと研修を続けている。それほど高いスキルではない割に対応の切り札として使えるからだ。

素早く的確に見分けられるようになれば、会計部門から一層頼られて疑わしいメールが集まり、さらに真偽を判断する知見がたまる。こうした好循環を作ってほしい。

組織には組織で対抗

情報システム部門やセキュリティー部門が取り組むべき最後の項目が「事案発生時の原因追及と侵害対応」である。BEC攻撃を仕掛けられたと分かったら、まず取り組むべきは情報流出を止める作業だ。

例えばメールの文章がBECに悪用され、メールシステムへの侵害が明らかになったものの、自社と取引先のどちらが情報の流出元になっているかが判然としない場合がある。このときは詐欺メールのtoとccにある全メールの所有者にパスワードを変更させる。そのうえで侵害の有無の調査に移る。

調査ではログインのログを分析して不正ログインの痕跡を調べると同時に、関係者のWebメールやメーラーの設定を調査する。調査ポイントは転送設定とメールの振り分けルールだ。

攻撃者はメールの不正ログインに成功するとメールを常に監視できるように、取引先からの受信メールを自分宛に転送してから削除するように設定する場合がある。あらかじめ確認ポイントを文書にして、有事に備えたい。

当初は手法が稚拙だったBECの攻撃者グループは今や組織化され、本稿で説明したように経験値とスキルを高めている。狙う先は世界中に広がり、しかも無差別だ。

対抗するには防御側も組織化するしかない。本稿冒頭で説明した、筆者が参加した米国のコミュニティーは捜査関係者も参加している。そこには様々な種類の情報が集まり、その結果、犯人グループの逮捕につながった例もある。日本でも企業が連携してBECの事案情報や知見を持ち寄り、組織的に対抗していく時期に来ている。 N

佐藤 元彦(さとう・もとひこ)
伊藤忠商事のサイバーセキュリティー対策について企画立案から運用実務まで担当する。グループ会社や海外拠点のセキュリティー相談や事案対応も受け持つ。趣味は標的型攻撃の分析と攻撃の痕跡を集める「シンクホール」の運用。

請求書の偽装を見破る

図 PDFファイルの「プロパティ」の確認箇所