サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2017 年 10 月～12 月]

2018 年 1 月 26 日
IPA（独立行政法人情報処理推進機構）
技術本部セキュリティセンター

サイバー情報共有イニシアティブ（J-CSIP）[1]について、2017 年 12 月末時点の運用体制、2017 年 10 月～12 月の運用状況を報告する。1 章、2 章は全体状況を、3 章以降は本四半期で把握、分析した特徴的な攻撃事例や、通年での動向等を併せて解説する。

目次

[1] IPA が情報ハブ（集約点）となり、サイバー攻撃等に関する情報を参加組織間で共有する取り組み。
https://www.ipa.go.jp/security/J-CSIP/

1　運用体制

2017 年 10 月～12 月期（以下、本四半期）は、各 SIG での参加組織拡大があり、全体では 2017 年 9 月末の 11 業界 190 組織の体制から、11 業界 227 組織[2]の体制となった（図 1）。

- 2017 年 10 月、ガス業界 SIG に新たな参加組織があり、26 組織から 54 組織となった。
- 2017 年 10 月と 11 月に、重要インフラ機器製造業者 SIG に新たな参加組織があり、11 組織から 14 組織となった。
- 2017 年 11 月、化学業界 SIG に新たな参加組織があり、22 組織から 23 組織となった。
- 2017 年 12 月、クレジット業界 SIG に新たな参加組織があり、47 組織から 48 組織となった。
- 2017 年 12 月、航空業界 SIG に新たな参加組織があり、5 組織から 6 組織となった。
- 2017 年 12 月、物流業界 SIG に新たな参加組織があり、10 組織から 11 組織となった。
- 2017 年 12 月、鉄道業界 SIG に新たな参加組織があり、17 組織から 19 組織となった。

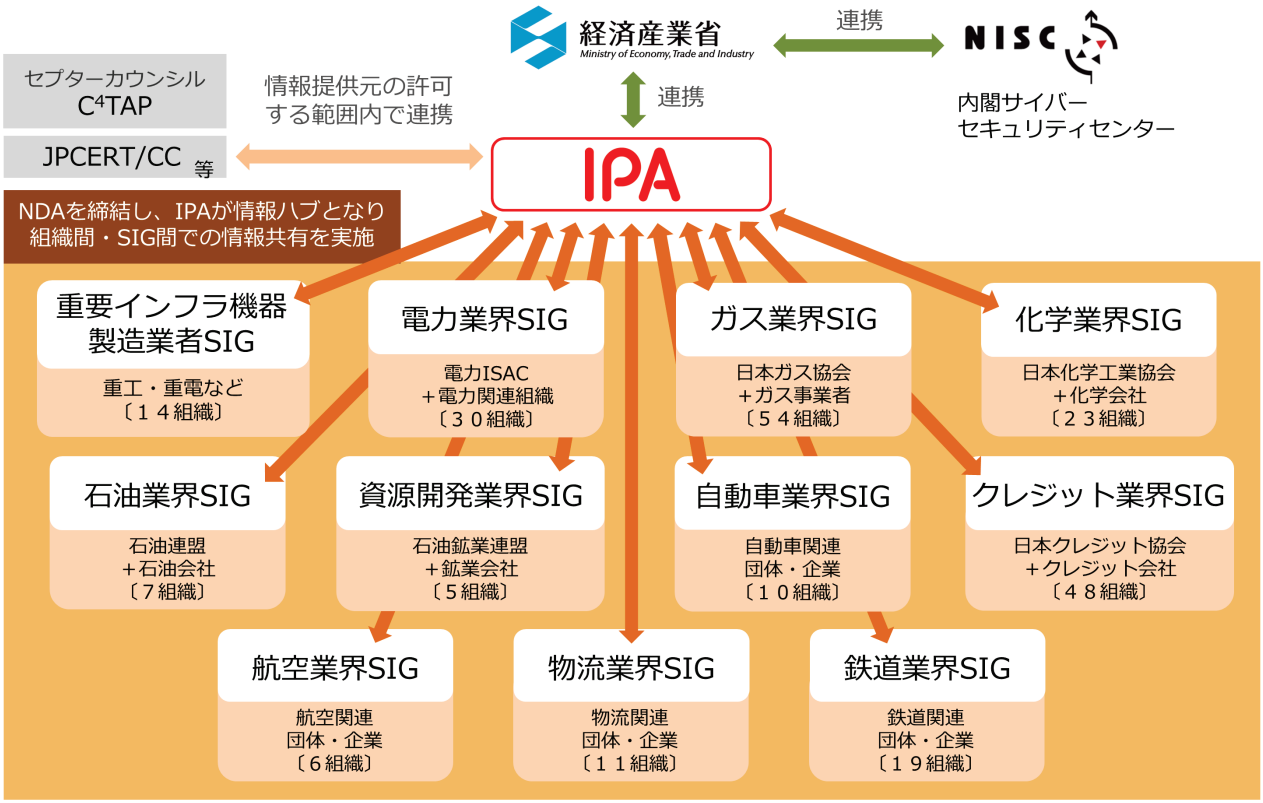


図 1 J-CSIP の体制図

[2] 複数業界に関係する組織が、複数の SIG に所属するケースも現れている。ここでは延べ数としている。

2　実施件数（2017 年 10 月～12 月）

2017 年 10 月～12 月に、J-CSIP 参加組織から IPA に対し、サイバー攻撃に関する情報（不審メール、不正通信、インシデント等）の情報提供が行われた件数と、それらの情報をもとに IPA から J-CSIP 参加組織へ情報共有を実施した件数（12 月末時点、11 の SIG、全 227 参加組織での合算）を、表 1 に示す。

表 1 情報提供および情報共有の状況

項番	項目	2017 年			
		1 月～3 月	4 月～6 月	7 月～9 月	**10 月～12 月**
1	IPA への情報提供件数	73 件	1,213 件	57 件	**1,930 件**
2	参加組織への情報共有実施件数※1	9 件	26 件	17 件	**123 件※2**

※1 同等の攻撃情報（不審メール等）が複数情報提供された際に情報共有を 1 件に集約して配付することや、広く無差別にばらまかれたウイルスメール等、情報共有対象としない場合があるため、情報提供件数と情報共有実施件数には差が生じる。

※2 IPA が独自に入手した情報で、J-CSIP 参加組織へ情報共有を行ったもの **14 件**を含む。

本四半期は情報提供件数が **1,930 件**であり、うち標的型攻撃メールとみなした情報は **164 件**であった。

提供された情報の主なものとして、日本語のばらまき型メールが大部分を占めている。ばらまき型メールとは、国内の一般利用者を攻撃対象に、広く大量に送信されているウイルスメールであり、添付ファイルやメール本文中の URL リンクを開いた場合、インターネットバンキングの情報を窃取するウイルス等に感染させられることを確認している。これについて、3 章で改めて述べる。

本四半期、プラント関連事業者を狙う攻撃メールを多数観測した。これは、プラント等の設備や部品のサプライヤーに対し、実在すると思われる開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽のメールであり、短期間で多岐にわたる文面のバリエーションを確認している。現時点では、攻撃者の目的が知財の窃取にある（産業スパイ）のか、あるいはビジネスメール詐欺（BEC[3]）のような詐欺行為の準備段階のものかは不明だが、ある程度特定の標的へ執拗に攻撃が繰り返されていることから、標的型攻撃の一種とみなして取り扱っている。これについては、4 章で改めて述べる。なお、本四半期に標的型攻撃メールとみなした 164 件のうち、156 件が本件に該当する。

この他、本四半期では、「企業の公開ウェブサイトにある問い合わせフォームに対して大量の投稿を行う」攻撃や、「組織内の実在する人物のメールアドレスを詐称して大量にウイルスメールがばらまかれた」事例について情報提供を受けた。これらの事例は、標的型攻撃とはみなしていないが、企業の業務に少なからず影響が発生する。前者については、同一 IP アドレスからの投稿回数に制限を設けるといった対策、後者については、自組織が詐称されてウイルスメールがばらまかれた際の対応方針を定めておくといった対策が必要である。

さらに、ビジネスメール詐欺（BEC）が試みられたという事例や、Office 365 等のアカウント情報を狙ったフィッシングメールも引き続き観測された。ビジネスメール詐欺（BEC）については 5 章で改めて述べるが、国内での大規模な被害事例が報道されており、今後も注意が必要な状況にある。

---

[3] Business E-mail Compromise （ビーイーシー）
【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口 （IPA）
https://www.ipa.go.jp/security/announce/20170403-bec.html

3　2017 年の日本語のばらまき型メールの動向

2015 年 10 月頃から国内で多く観測されるようになった日本語のばらまき型メールは、着信した業界等に偏りは見られず、個人・法人によらず広く無差別に、かつ継続的・大量に送信されている。日本サイバー犯罪対策センター[4]等からもばらまき型メールの注意喚起情報が定期的に発信されており、本章で説明するものも、これらと同等の攻撃である。

本四半期を含め、2017 年の 1 年間における日本語のばらまき型メールでは、インターネットバンキングの情報を窃取する「DreamBot（ドリームボット）」と呼ばれるウイルスに感染させる目的のものが非常に多いことを確認している。この、DreamBot への感染を狙うばらまき型メールは、J-CSIP 参加組織でも多数観測されている状況であり、一部公開情報を含め、**観測状況と攻撃手口の変化**について、本章で説明する。

なお、ばらまき型メールの一連の攻撃のうち、2017 年 11 月 15 日に修正プログラムが公開された Microsoft Office の脆弱性（CVE-2017-11882[5]）を悪用する攻撃を、約 1 週間後の 11 月 23 日から 24 日にかけて観測した事例もあった。手口の変化・巧妙化が絶え間なく進んでいることから、個人・法人にとって今後も大きな脅威となるものと考えられ、公表された脆弱性への迅速な対応も重要となっている。

3.1 DreamBot とは

DreamBot とは、一般に Ursnif（アースニフ、別名は Gozi／Snifula／Papras 等）と呼称されるウイルスの機能強化版である（Ursnif が Tor[6]通信に対応したものを DreamBot と呼んでいる）[7]。

このウイルスは 2016 年 12 月頃から日本国内で観測されており、2017 年 2 月以降、DreamBot への感染を目的としたウイルスメールの大規模なばらまきが断続的に観測されている。DreamBot は銀行や信用金庫のインターネットバンキングの情報、クレジットカードを扱う信販会社の情報に加え、ビットコイン等の仮想通貨の情報も窃取対象にしていると思われる[8]。

3.2 ばらまき型メールの観測状況

2017 年 1 月から 12 月の期間において、DreamBot 感染を目的としたばらまき型メールの観測状況（メールの件名と攻撃手口）を表 2 に示す。

9 月頃までは、メールに悪意のあるファイル（ウイルス）が添付されており、それらは実行形式のファイル（exe ファイル、スクリプトファイル、ショートカット（LNK）ファイル等）や、細工された Word・Excel 等の文書ファイルであった。また、それらのファイルが zip や rar 形式で圧縮されていることもあった。これらの悪意のあるファイルはダウンローダ[9]の機能を持つものであり、外部サーバから DreamBot 本体をダウンロードし、PC に感染させる動作を行う点が共通している。

---

[4] 一般財団法人日本サイバー犯罪対策センター（JC3）
https://www.jc3.or.jp/topics/virusmail.html

[5] Microsoft Office 数式エディタにスタックベースのバッファオーバーフローの脆弱性（JVN）
https://jvn.jp/vu/JVNVU90967793/

[6] The Onion Router（トーア）

[7] 国内ネットバンキングを狙う新たな脅威「DreamBot」を解析（トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/14588

[8] 新たに「ビットコイン」を狙う「URSNIF」を国内で確認（トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/15633

[9] 別のウイルスをダウンロードし感染させることを目的としたウイルス。

実行形式のファイルの場合、ファイルの種類をよく確認せずにダブルクリックして開いてしまうと（実行してしまうと）DreamBot に感染させられてしまう。悪意のある文書ファイルの場合、マクロの悪用、OLE の機能を使った実行形式ファイルの埋め込み、脆弱性の悪用といった細工が施されており、受信者が不適切な操作をしたり、OS 等を最新の状態にしていないと、DreamBot に感染させられてしまう。

さらに、9 月以降は、ファイルが添付されておらず、メール本文中に URL リンクが記載されており、受信者が URL リンクをクリックすることで、「DreamBot をダウンロードして感染させるためのスクリプトファイル（ダウンローダ）が入った圧縮ファイル」をダウンロードさせる、という手口も新たに見られるようになった。

ばらまかれたメールの件名は様々な種類があり、一般的な用件を装うような件名の他に、何らかの業界の専門用語が用いられたものもあった。また、IPA が観測できた範囲で、同時期にばらまかれたメールの量をメールの件名別に一部比較したところ、大量に送信されたメールと、ごく少数しか送信されなかったメールがあり、大きな偏りが見られることがあった。攻撃者の意図は不明だが、メールがばらまかれた量に多寡があることによって、メールフィルタリングでの検知率や組織での対応等に差異が生じる可能性がある。例えば、何百通と着信する攻撃メールを検知・対処できる一方で、数通しか着信しない攻撃メールが見逃されてしまうという可能性が考えられる。

攻撃者は、ウイルスメールの内容や、ウイルスに感染させる手口を様々に変化させ、巧妙化を重ねてきたものと思われる。2015 年末～2016 年と比べ、2017 年の 1 年間は攻撃手口の変化が目立った年であった。今後も攻撃手口の変化・巧妙化が続くものと思われ、注意が必要である。

表 2 ばらまき型メールの観測状況

	1 月～3 月	4 月～6 月	7 月～9 月	10 月～12 月
メールの件名	・ 勘定書き ・ アカウント ・ 付出し ・ 付け出し ・ 会計 ・ 口座 ・ 支払請求書 ・ 支払いの請求書 ・ アカウント ・ 直話	・ キャンセル完了のお知らせ ・ 休炉について ・ 助燃剤購入及び使用量 ・ 固定床炉前処理日報 ・ 保安検査 ・ 節税効果 ・ 凛とした現場写真 2 ・ のご注文ありがとうございます ・ 駐禁報告書 ・ 資格取得の届	・ Express Mail Service (EMS) ・ 日本郵便追跡サービス ・ Re:【お振込口座変更のご連絡】 ・ 【NTT-X Store】商品発送のお知らせ	・ お支払いが確認できませんでした ・ 【取組同意完了のご確認】オリックス・クレジット ・ ご注文ありがとうございました ・ 口座振替日のご案内【楽天カード株式会社】(楽天カード) ・ 【重要】カスタマセンターからのご案内【楽天カード株式会社】 ・ 【楽天カード】ご請求予定金額のご案内 ・ カード利用のお知らせ ・ ディズニーランドの入場券をご獲得になりました！
攻撃手口	・ 実行形式のファイルを添付 ・ 悪意のあるマクロ付きの文書ファイルを添付	・ 実行形式のファイルを添付 ・ 悪意のある OLE オブジェクトが埋め込まれた文書ファイルを添付 ・ 文書ソフトの脆弱性（CVE-2017-0199[10]）を悪用する文書ファイルを添付	・ 悪意のある OLE オブジェクトが埋め込まれた文書ファイルを添付 ・ メール本文中に URL リンクを記載しウイルスをダウンロードさせる	・ 悪意のある OLE オブジェクトが埋め込まれた文書ファイルを添付 ・ 文書ソフトの脆弱性（CVE-2017-11882）を悪用する文書ファイルを添付 ・ メール本文中に URL リンクを記載しウイルスをダウンロードさせる

※ ここで示すメールの件名や攻撃手口は、ばらまき型メールの攻撃で使われた一部である。すべてのパターンは網羅していない。

※ 一部実在する企業名等がメール内に表れているが、これは攻撃者によって詐称・悪用されているだけであり、これら企業に原因や問題があるわけではない。

[10] Microsoft OLE URL Moniker における遠隔の HTA データに対する不適切な処理 （JVN）
https://jvn.jp/vu/JVNVU98665451/

3.3 攻撃手口の巧妙化

組織や企業のウイルスメール対策をかいくぐるため、ばらまき型メールの攻撃者は手口の巧妙化を続けている。ここでは、攻撃手口の巧妙化の一部について説明する。

（1） メールフィルタリングによる対策の回避

「ばらまき型メールの観測状況」で述べたとおり、2017 年 9 月頃から、ウイルスを添付ファイルとして送りつけてくるだけでなく、メール本文中に悪意のあるファイルをダウンロードさせるための URL リンクを記載するという手口も用いられるようになった。これにより、これまで有効であったメールフィルタリング（ウイルスメール対策やスパムメール対策等）をすり抜けて、組織内へ一部メールが流入してしまっている（利用者のメールボックスまでメールが到達している）という報告があった。

例えば、2017 年 10 月には、J-CSIP 内の複数の組織から、メール本文中に URL リンクがあるばらまき型メールが、数十通～数百通単位で組織内に流入しているとの情報提供があった。

さらに、この攻撃者は存在しないメールアドレスを含めて大量にウイルスメールをばらまいているという傾向が長期間みられたが、2017 年 12 月、ある組織で確認したところ、特定のウイルスメールについて、すべて存在するメールアドレスのみに送信が試みられたことが分かった。これは、攻撃者が、メールの送信エラーの結果の反映等により、メールをばらまく先のリストを実在するメールアドレスのみに「クリーニング [11]」した可能性を示唆している。

[J-CSIP 内の事例（1）]

2017 年 10 月 12 日から 19 日にかけて、メール本文中に URL リンクが記載された、楽天を詐称するばらまき型メールが、メールゲートウェイに 200 通以上着信。その内の 46%（約 100 通）が、メールフィルタリングでブロックできず組織内に流入した。

[J-CSIP 内の事例（2）]

2017 年 10 月 11 日頃、メール本文中に URL リンクが記載された、オリックス・クレジットを詐称するばらまき型メール約 300 通が、メールフィルタリングでブロックできず組織内に流入した。

[J-CSIP 内の事例（3）]

2017 年 12 月 27 日頃、メール本文中に URL リンクが記載された、楽天を詐称するばらまき型メールが、実在するメールアドレス宛てに 100 通以上着信。そのうち 2 通はメールフィルタリングでブロックできず組織内に流入した。さらに、この組織には、これまでは存在しないメールアドレスへもばらまき型メールが送付されていたが、この時は、すべて実在するメールアドレスのみへ送付が試みられた。

[11] メールアドレスのリストについて、存在しない（無効な）ものを除去する処理。

（2）メール文面の巧妙化

ばらまき型メールは、当初は不自然な件名や文面が目立っていたが、時を経るにつれ、比較的流暢な日本語で実在の企業を詐称する巧妙なものになってきており、メール受信者が不審と見抜くことが困難になりつつある。

ここでは、一例として 2016 年 12 月～2017 年 12 月に観測されたメールの文面を 4 件示す。

2016 年 12 月（図 2）や 2017 年 4 月（図 3）に送信されていたメールは、不自然な点が多く見られる。しかし、2017 年 7 月（図 4）のメールでは実在する企業を詐称し、日本語としても自然な文面になっている。さらに、2017 年 12 月（図 5）のメールでは、実在する企業を詐称するだけでなく、見た目も本物のメールのような内容となった。

- **2016 年 12 月に送信されたばらまき型メール**

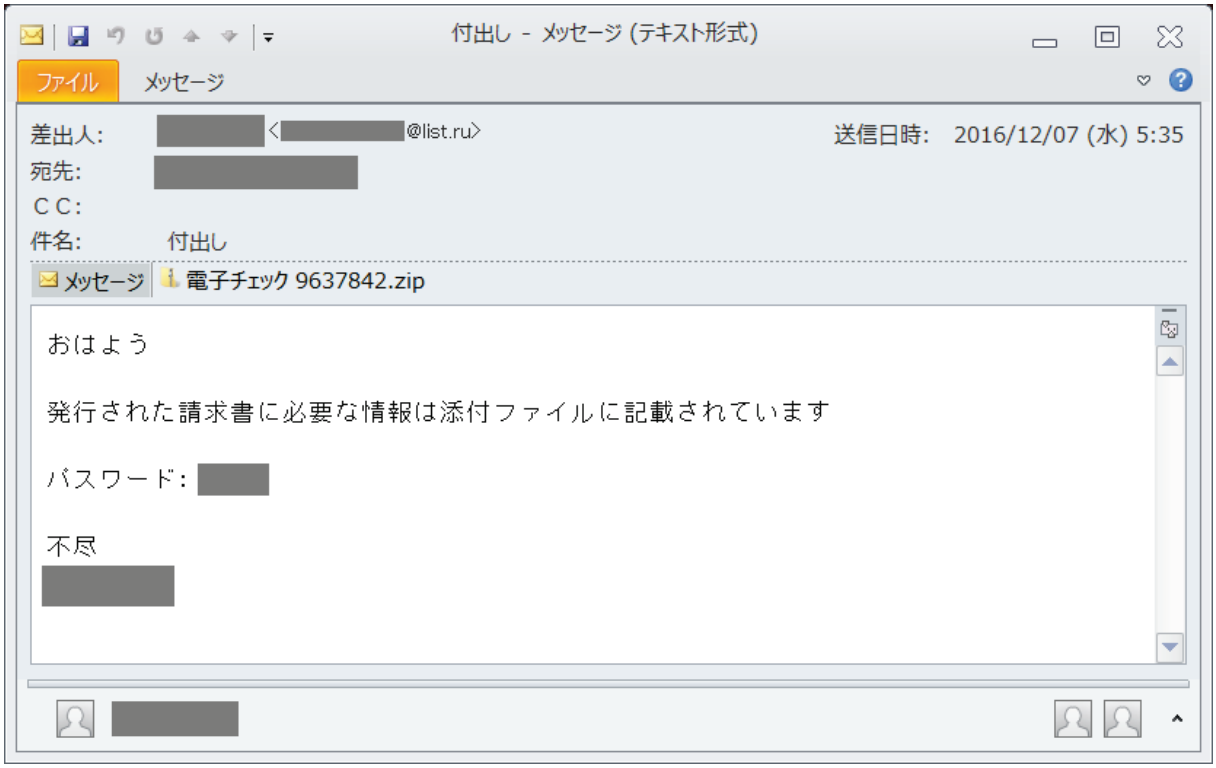


図 2 2016 年 12 月のメール

- **2017 年 4 月に送信されたばらまき型メール**

図 3 2017 年 4 月のメール

- **2017 年 7 月に送信されたばらまき型メール**

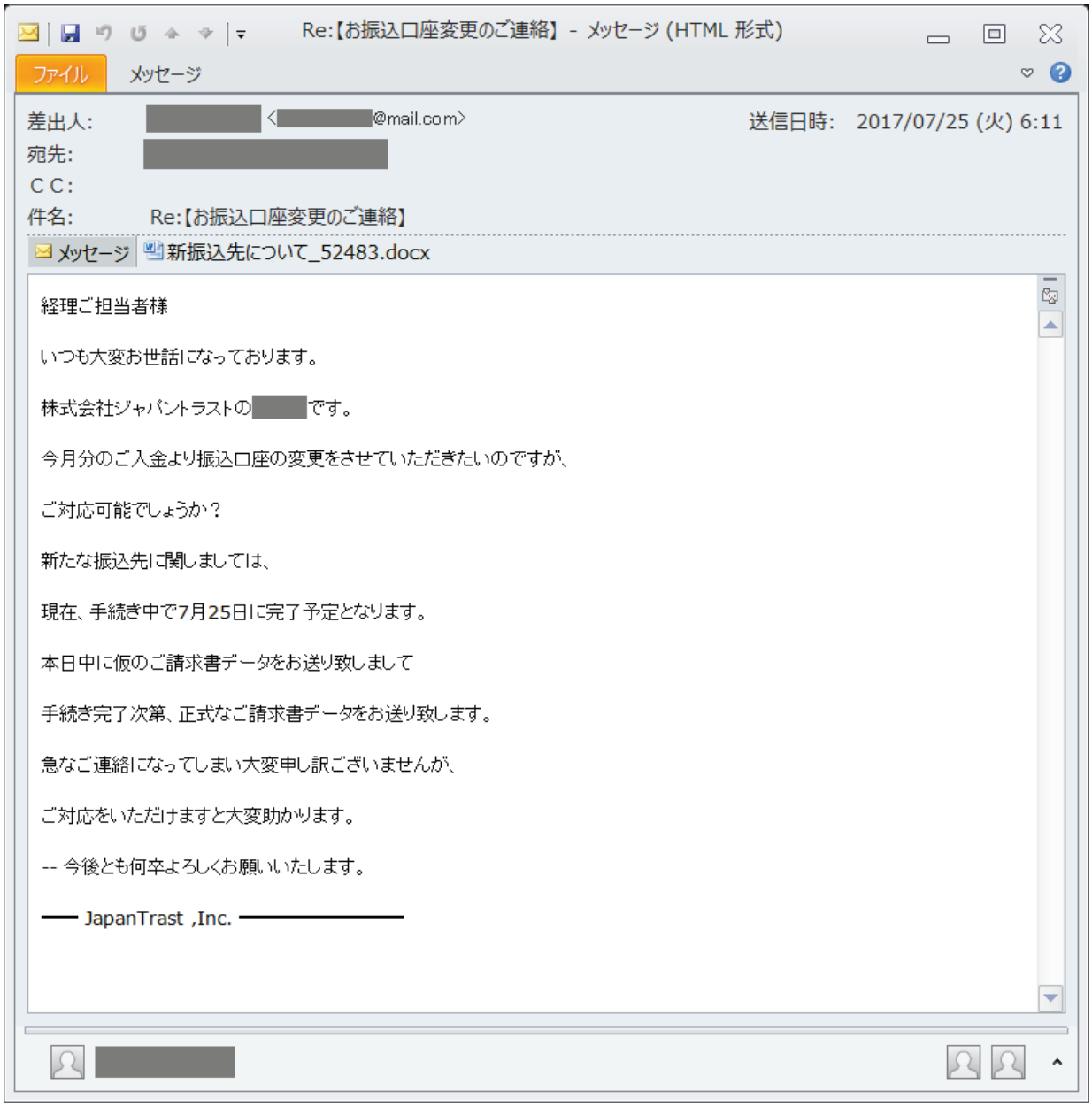


図 4 2017 年 7 月のメール

- **2017 年 12 月に送信されたばらまき型メール**

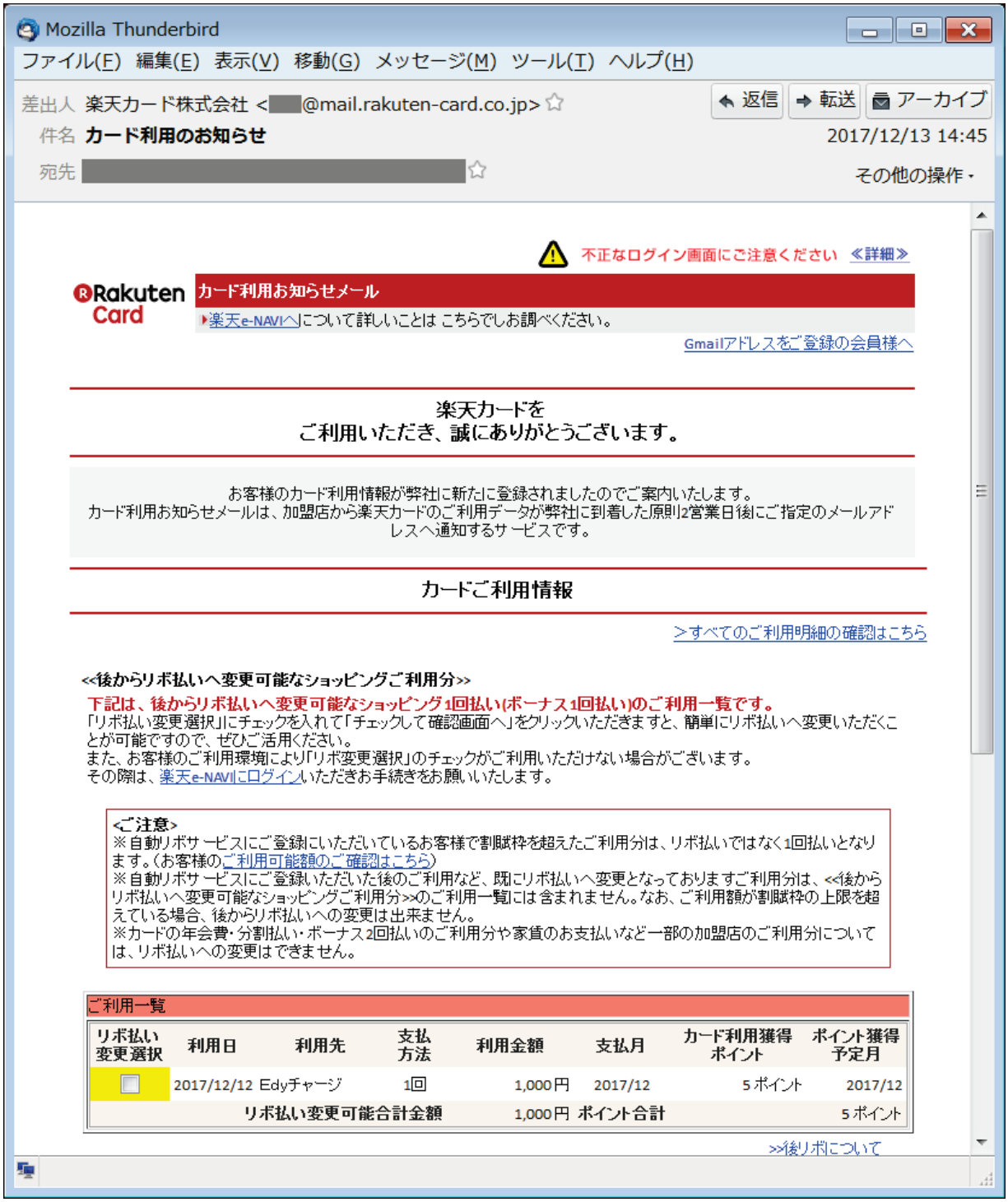


図 5 2017 年 12 月のメール

（3） ウイルスの内部構造の変化

攻撃者が感染させようとしているウイルス、DreamBot 本体の内部構造も、短期間で徐々に変化している。これにより、セキュリティソフトのパターンマッチング等による検知をすり抜ける例がある。実際に、ウイルスメールがばらまかれてからの数日間、感染させられる DreamBot のファイルをセキュリティソフトがウイルスとして検知できていないケースを確認している。

3.4 対策

ばらまき型メールの攻撃者は、メールフィルタリングによる対策をかいくぐるために、様々な手口の工夫を凝らしており、今後も今までに観測していない新たな手口で攻撃してくる可能性がある。このような攻撃をひとつの対策で防ぐことは難しく、メールフィルタリング、セキュリティソフト、メール受信者の自己防衛まで含めた総合的な対策（多層防御）を行うことが重要である。

この攻撃に限らず一般的なウイルス対策（ウイルスメール対策）ではあるが、次のような対策を徹底していただきたい。

- **脆弱性の対策**
  - OS やブラウザ、Office 製品等の修正プログラムを適用し、常に最新の状態にする。

- **セキュリティソフトの最新化**
  - セキュリティソフトの定義ファイル等を常に最新の状態にする。

- **メール利用者への注意点の徹底**
  - メールに添付されているファイルや、外部からダウンロードしたファイルは、安全と判断できるもの以外は不用意に開かない。
  - ファイルを開く前に、ファイルのプロパティ等によって「ファイルの種類」を確認する。「アプリケーション」や「Script」等、文書ではない形式の場合は、危険を及ぼす可能性がある。
  - 文書ファイルを開いた際、マクロの有効化が求められたり、警告ウインドウが表示された場合、「はい」や「OK」を不用意にクリックしない（表示された警告等の意味が分からない場合は操作を中断する）。
  - メールに記載されている URL リンクには、安全と判断できるもの以外は不用意にアクセスしない。
  - 少しでも不審に感じたら、組織内のシステム管理部門／セキュリティ部門／CSIRT 等へ連絡する。

「メールの文面の巧妙化」で示したとおり、詐称する組織、件名・文面・添付ファイル名等は、一見して不審と見抜きにくくなりつつある。しかし、利用者ひとりひとりが注意することは依然として重要であり、不審なメールが着信していることを組織内で共有できれば、組織全体として被害を低減できる可能性がある。組織全体として、利用者からの報告を受け、同種の不審メールの組織への着信状況を確認・対処できる体制とすることが望ましい。

4 プラント関連事業者を狙う一連の攻撃

本四半期、プラント等の設備や部品のサプライヤーに対し、実在すると思われる開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽のメールを送り付け、添付ファイル（ウイルス）を開かせようとする攻撃を多数観測した。

偽のメールの内容は巧妙で、使われている英文には不審な点は少なく、プラントの設計・調達・建設に関わる企業や資機材等について一定の知識を持つ者が作成したものと思われ、無作為に個人を狙うような攻撃ではなく、プラント関連事業者を標的とした攻撃だと推測している。また、短期間で多岐にわたる文面のバリエーションがあることを確認しているが、J-CSIP 内の数組織で確認している同等のメールの着信数はそれぞれ数通から数十通程度であり、その点でも、広く無差別にばらまかれているウイルスメールとは様相が異なっている。

現時点では、攻撃者の目的が知財の窃取にある（産業スパイ）ものか、あるいはビジネスメール詐欺（BEC）のような詐欺行為の準備段階のものかは不明である。もしくは、プラントの設計・調達・建設に関わるサプライチェーン全体を攻撃の対象としている可能性（セキュリティが比較的弱い可能性のある、下流の資機材メーカーを侵入の入口として狙っている可能性）もありうる。いずれにせよ、ある程度特定の組織へ執拗に攻撃が繰り返されていることから、標的型攻撃の一種とみなして取り扱っている。

4.1 攻撃の観測状況

2017 年 10 月、プラント資機材の販売や輸出業を行っている国内の企業や、プラント設計等を行っている韓国の企業を詐称し、プラント関連事業者向けに送られたと思われる攻撃メールを IPA で入手した（図 6）。

この攻撃メールについて J-CSIP 参加組織へ情報共有を行ったところ、複数の組織で類似する攻撃メールが着信していたことが判明し、IPA が入手していない攻撃メールが数十種類あることが情報提供により把握できた（これら情報についても情報共有を実施している）。これらは、メールの文面、メールの送信元 IP アドレス、添付されていたウイルスの種類やその不正接続先といった要素で共通点がみられ、同一の攻撃者（または攻撃グループ）による一連の攻撃であると推定している。

また、J-CSIP 参加組織の協力により得られた過去の類似のメールの着信状況から、この攻撃者は少なくとも 2016 年 12 月頃から攻撃活動を行っており、2017 年 5 月頃には使用するウイルスを変更、2017 年 12 月にはフィッシング攻撃を併用するようになったことが推測できた。

攻撃は現時点でも継続している。

4.2 攻撃メールの例と特徴

攻撃者は標的とする企業に対し、メールの文面等を変化させながら、執拗に攻撃メールを送り付けている。添付ファイルは主に rar 形式の圧縮ファイルが使われていたが、一部、ace 形式の圧縮ファイルや、xlam ファイル [12]が添付されていたケースもある。これらは全て、PC 内の情報の窃取を目的とするウイルスへの感染を狙うものであった。また、12 月には、PDF ファイルが添付されたメールも確認した。これは、フィッシングによるメールアカウント情報の詐取を狙うものであった。なお、この攻撃者による、提案や見積もり等を依頼する偽のメールでは、その締め切り日として、メールの送信日から 1 週間から 10 日後程度を提示してくることが多く、添付ファイルを急いで確認させようとする意図があると思われる。

ここでは、本件の攻撃者による攻撃メールの事例を 5 件、ピックアップして紹介する。

---

[12] Microsoft Excel 2007 以降で作成された Excel のアドインファイル形式。ファイルを開き、表示される警告画面で「マクロを有効にする」ボタンをクリックすると、プログラムが実行される。

- **事例 1 プラント資機材の販売や輸出を行っている国内企業を騙る攻撃メール**

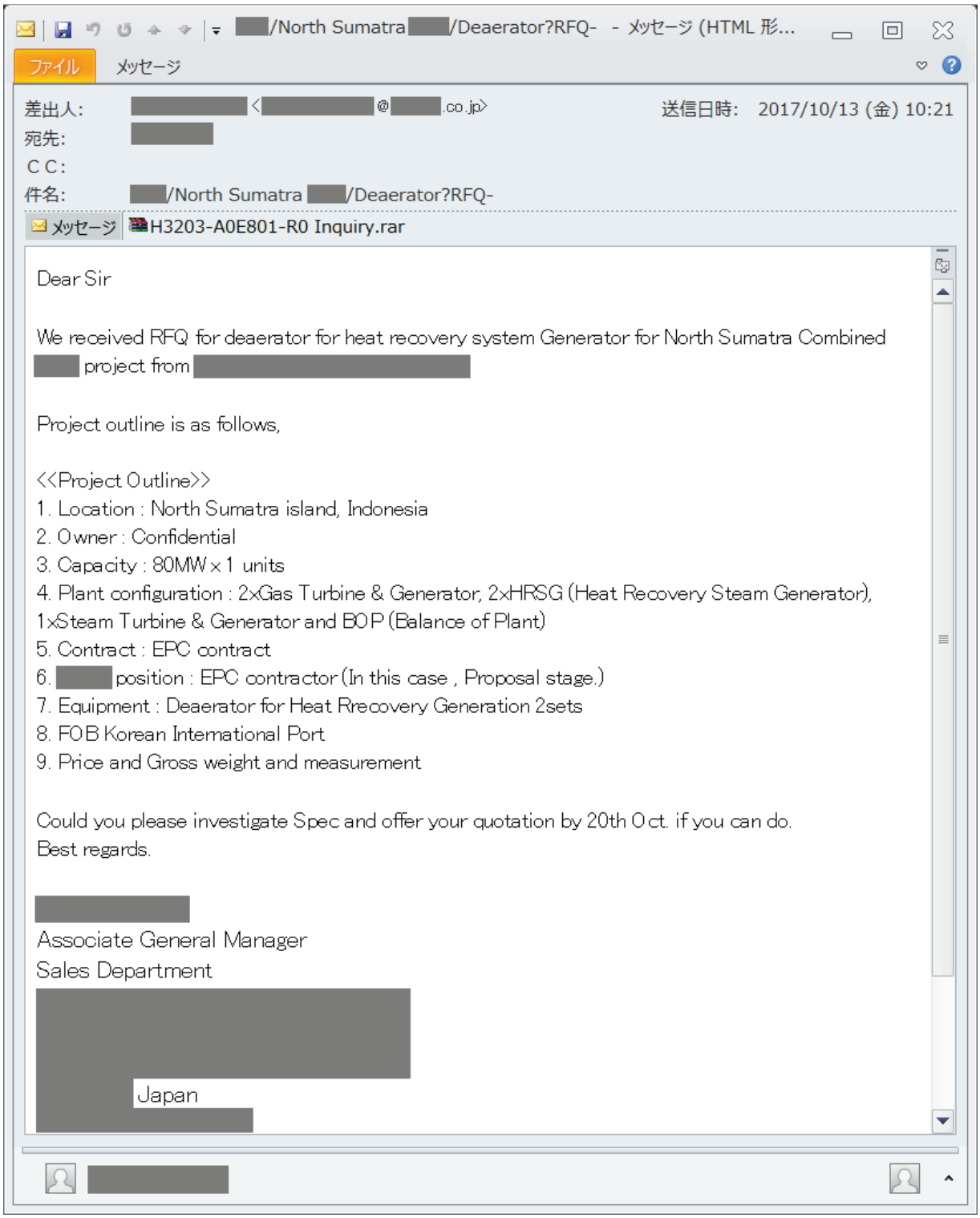


図 6 プラント資機材の販売や輸出を行っている国内企業を騙る攻撃メール

このメールでは、プラント資機材の販売や輸出を行っている国内企業を騙り、北スマトラの、とあるプロジェクトの熱回収システム用脱気装置の見積もり依頼を装っている。

- **事例 2 韓国のプラントエンジニアリングを提供する企業を騙る攻撃メール**

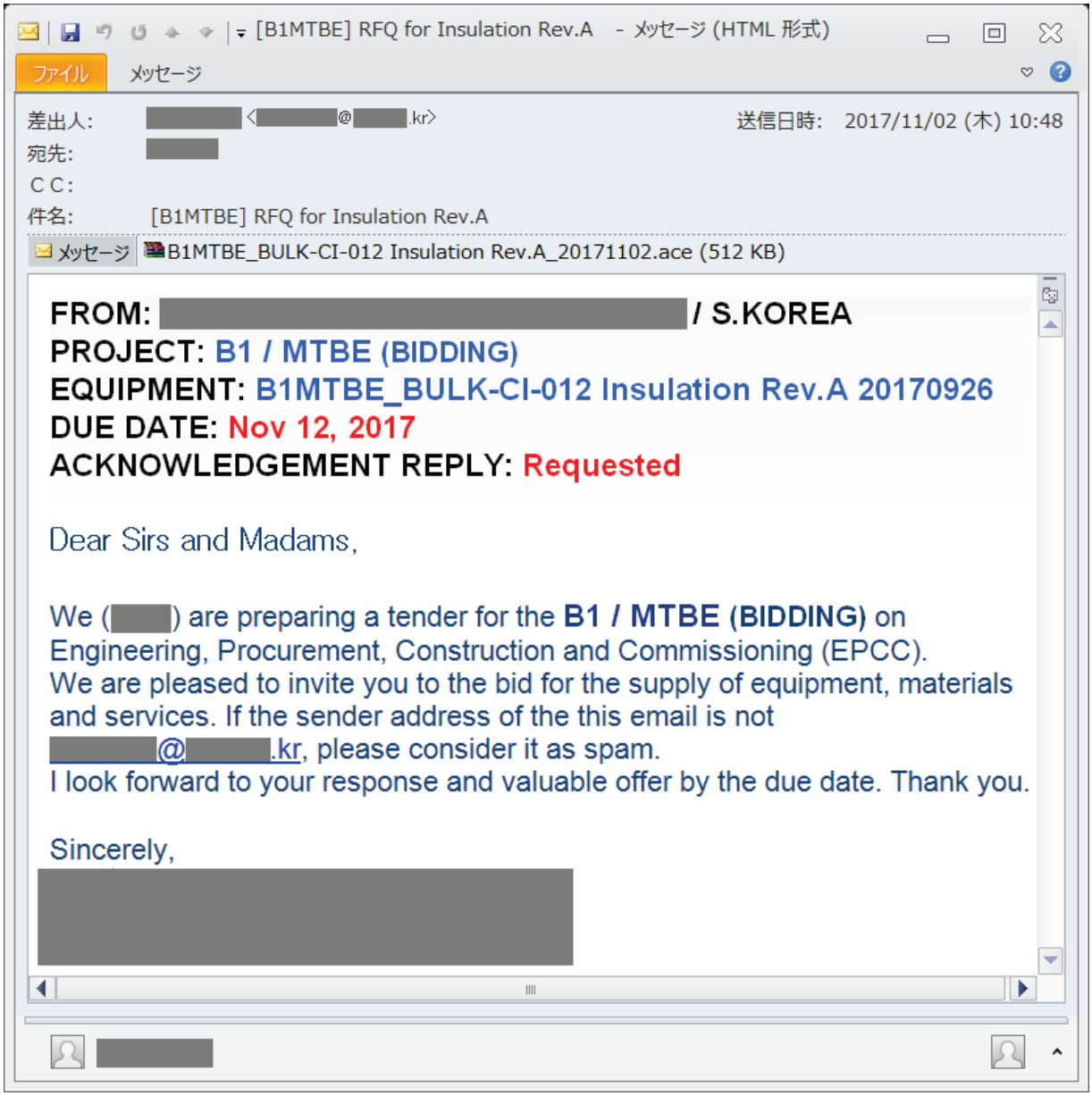
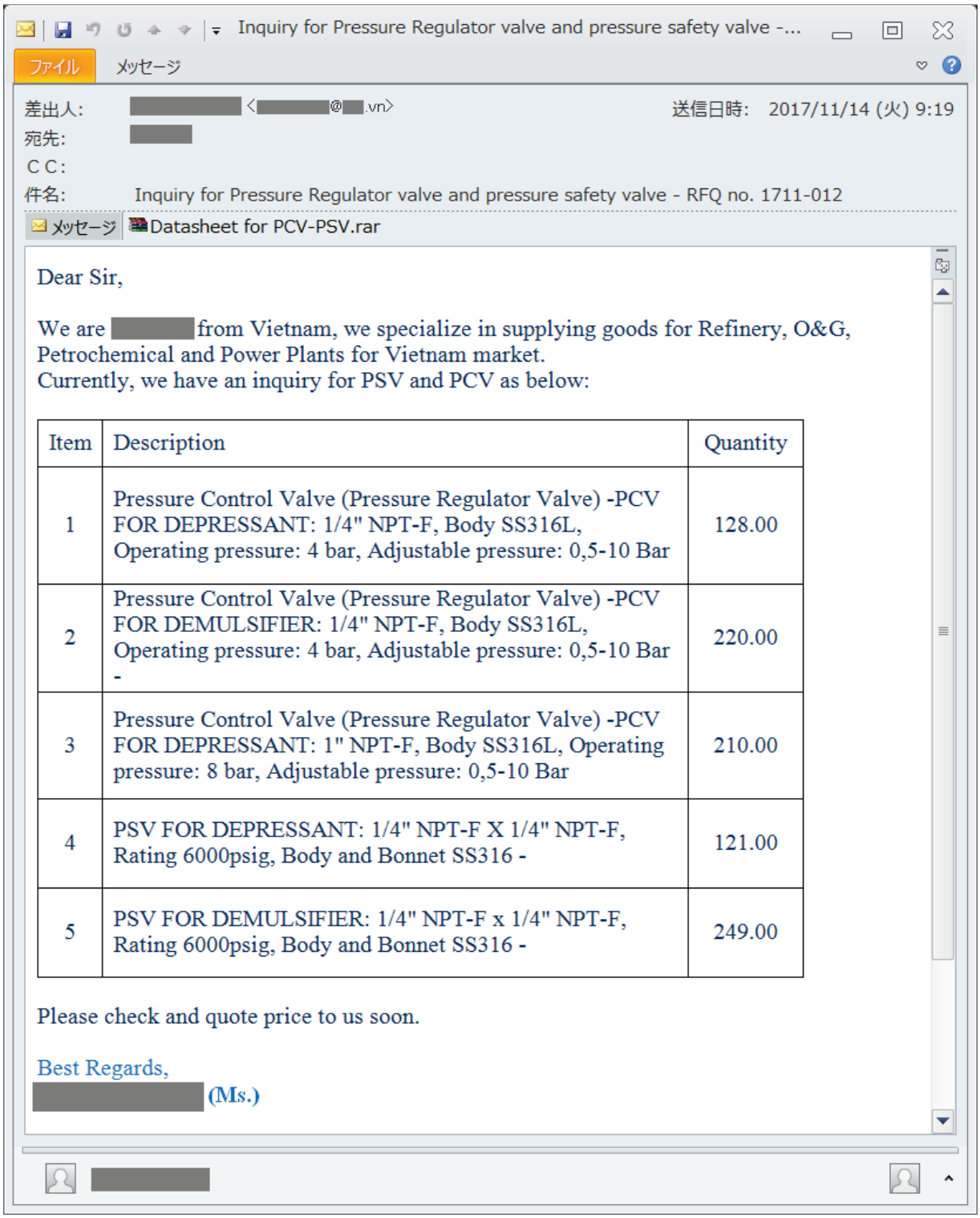


図 7 韓国のプラントエンジニアリングを提供する企業を騙る攻撃メール

このメールでは、韓国のプラントエンジニアリングを提供する企業を騙り、MTBE（メチル-tert-ブチルエーテルと思われる）に関するプロジェクトに必要な資機材の見積もり依頼を装っている。

- **事例 3 ベトナムのプラント資機材の販売を行っている企業を騙る攻撃メール**



Inquiry for Pressure Regulator valve and pressure safety valve -...

ファイル　メッセージ

差出人: [redacted] <[redacted]@[redacted].vn>　送信日時: 2017/11/14 (火) 9:19

宛先: [redacted]

ＣＣ:

件名: Inquiry for Pressure Regulator valve and pressure safety valve - RFQ no. 1711-012

メッセージ　Datasheet for PCV-PSV.rar

Dear Sir,

We are [redacted] from Vietnam, we specialize in supplying goods for Refinery, O&G, Petrochemical and Power Plants for Vietnam market.
Currently, we have an inquiry for PSV and PCV as below:

Item	Description	Quantity
1	Pressure Control Valve (Pressure Regulator Valve) -PCV FOR DEPRESSANT: 1/4" NPT-F, Body SS316L, Operating pressure: 4 bar, Adjustable pressure: 0,5-10 Bar	128.00
2	Pressure Control Valve (Pressure Regulator Valve) -PCV FOR DEMULSIFIER: 1/4" NPT-F, Body SS316L, Operating pressure: 4 bar, Adjustable pressure: 0,5-10 Bar -	220.00
3	Pressure Control Valve (Pressure Regulator Valve) -PCV FOR DEPRESSANT: 1" NPT-F, Body SS316L, Operating pressure: 8 bar, Adjustable pressure: 0,5-10 Bar	210.00
4	PSV FOR DEPRESSANT: 1/4" NPT-F X 1/4" NPT-F, Rating 6000psig, Body and Bonnet SS316 -	121.00
5	PSV FOR DEMULSIFIER: 1/4" NPT-F x 1/4" NPT-F, Rating 6000psig, Body and Bonnet SS316 -	249.00

Please check and quote price to us soon.

Best Regards,
[redacted] (Ms.)

図 8 ベトナムのプラント資機材の販売を行っている企業を騙る攻撃メール

このメールでは、ベトナムのプラント資機材の販売を行っている企業を騙り、圧力制御弁や安全弁等に関する問い合わせを装っている。

- **事例 4 クウェートのプラント資機材の販売を行っている企業を騙る攻撃メール**

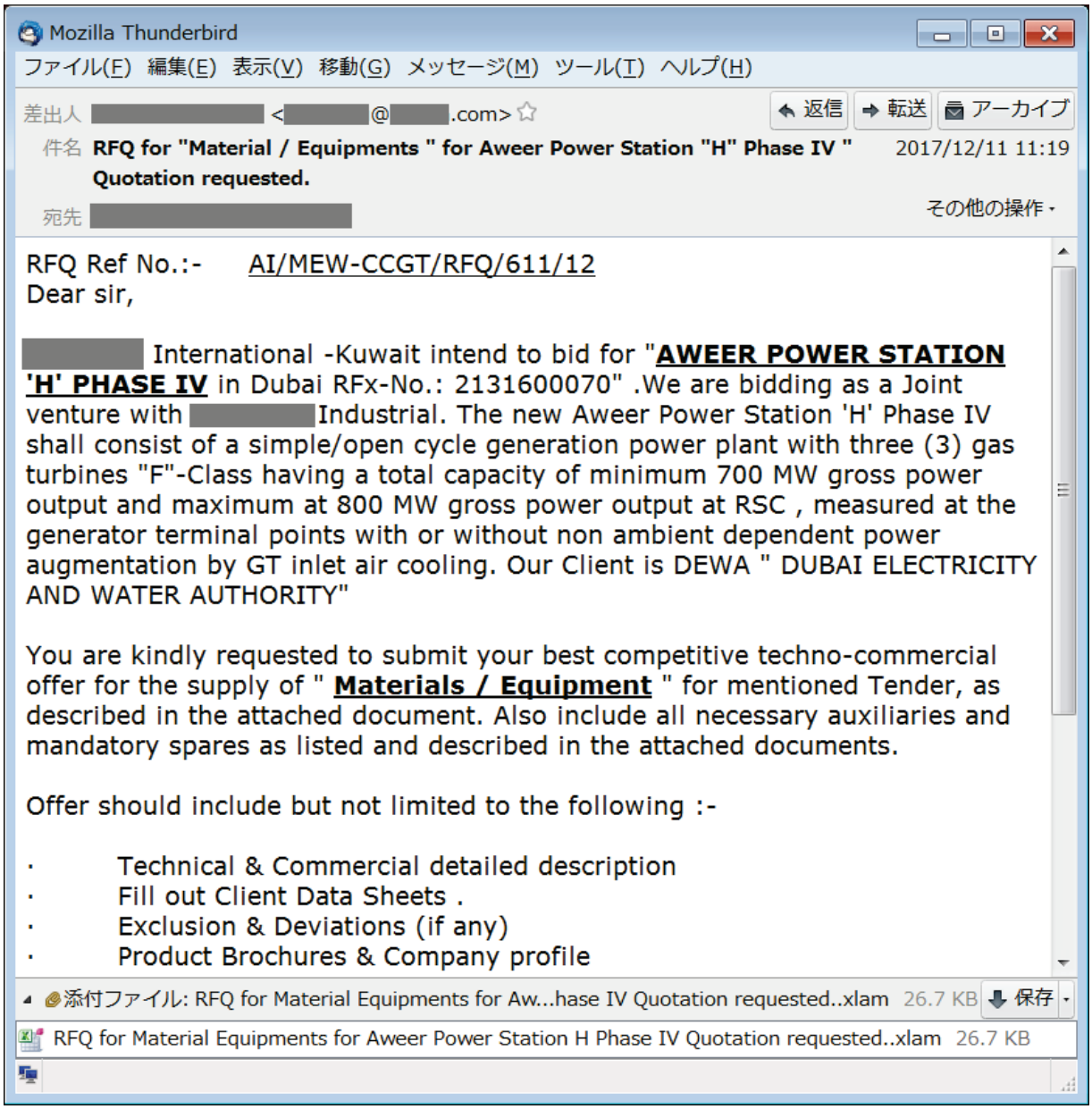
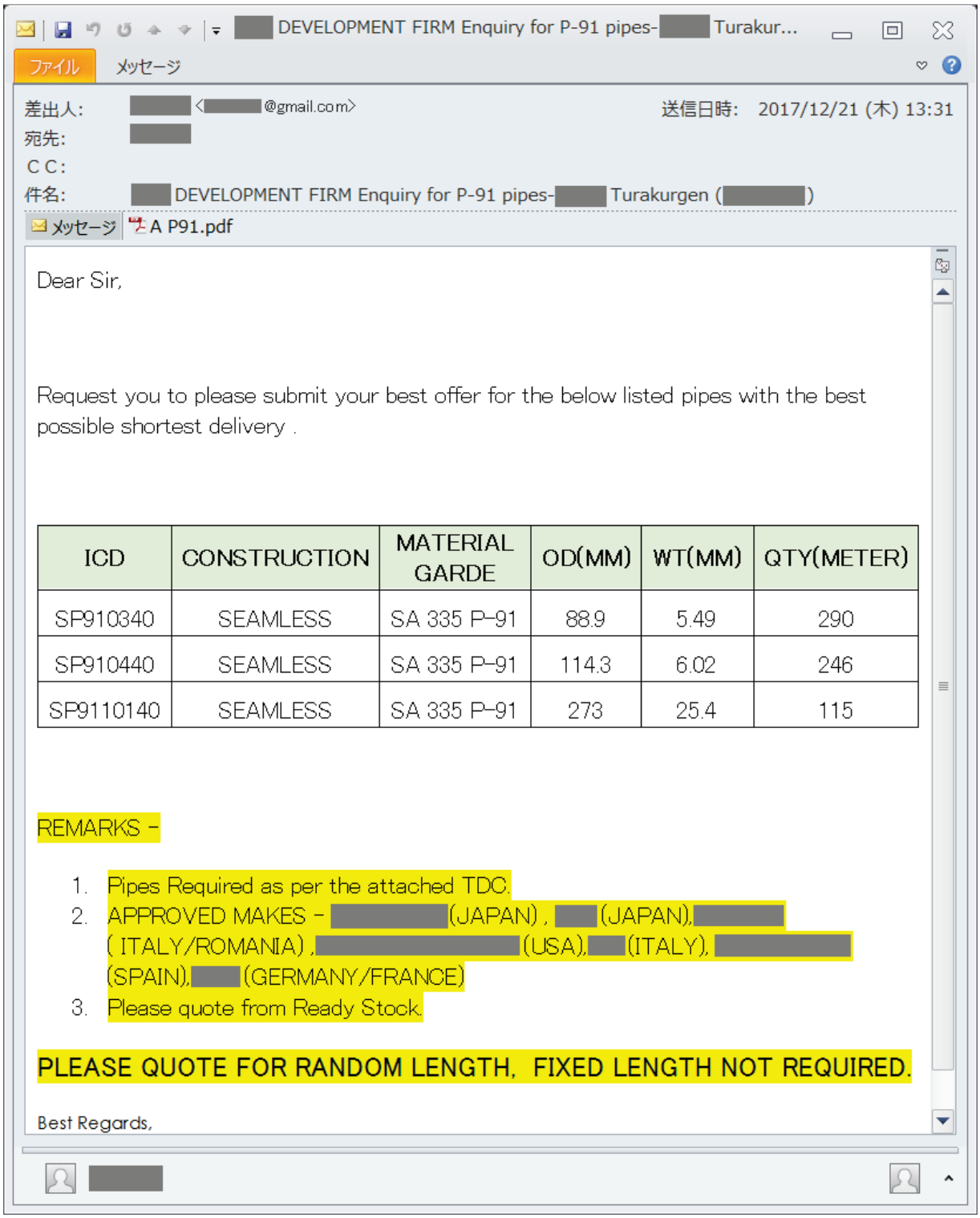


図 9 クウェートのプラント資機材の販売を行っている企業を騙る攻撃メール

このメールでは、クウェートのプラント資機材の販売を行っている企業を騙り、ドバイの発電所のための資機材の見積もり依頼を装っている。

- **事例 5 インドのプラント資機材の販売を行っている企業を騙る攻撃メール**



DEVELOPMENT FIRM Enquiry for P-91 pipes- Turakur...

ファイル　メッセージ

差出人: @gmail.com>　送信日時: 2017/12/21 (木) 13:31

宛先:

CC:

件名: DEVELOPMENT FIRM Enquiry for P-91 pipes- Turakurgen ( )

メッセージ　A P91.pdf

Dear Sir,

Request you to please submit your best offer for the below listed pipes with the best possible shortest delivery .

ICD	CONSTRUCTION	MATERIAL GARDE	OD(MM)	WT(MM)	QTY(METER)
SP910340	SEAMLESS	SA 335 P-91	88.9	5.49	290
SP910440	SEAMLESS	SA 335 P-91	114.3	6.02	246
SP9110140	SEAMLESS	SA 335 P-91	273	25.4	115

REMARKS -

1. Pipes Required as per the attached TDC.
2. APPROVED MAKES - (JAPAN) , (JAPAN), (ITALY/ROMANIA) , (USA), (ITALY), (SPAIN), (GERMANY/FRANCE)
3. Please quote from Ready Stock.

PLEASE QUOTE FOR RANDOM LENGTH, FIXED LENGTH NOT REQUIRED.

Best Regards,

図 10 インドのプラント資機材の販売を行っている企業を騙る攻撃メール

このメールでは、インドのプラント資機材の販売を行っている企業を騙り、資機材（シームレスパイプ（継ぎ目のない鋼管））の調達に関する問い合わせを装っている。

4.3 まとめ

プラント関連事業者を狙う一連の攻撃について、実際の攻撃メールの事例とともに、現時点で確認できている状況を紹介した。単純な文面の提案依頼（RFP）、見積もり依頼（RFQ）、請求書等を装うウイルスメールは多種多様な事例があるが、この攻撃者は、プラントの資機材について詳細な内容の偽のメールを作成し、また、長期に渡り対象を絞って攻撃メールを送り付けてきている。攻撃対象は、無差別ではないものの、広くプラント関連事業者全般となっている可能性がある。

J-CSIP には、プラントに関わる事業者が多く参加している関係上、注意を要する攻撃者であると考えており、今後も本攻撃者の動向に注視していく予定である。

5　ビジネスメール詐欺（BEC） 国内組織への攻撃を引き続き確認

2017 年 12 月、J-CSIP の参加組織に対してビジネスメール詐欺（BEC）が試みられた事実を把握した。ビジネスメール詐欺については、同じく 2017 年 12 月に国内での大規模な被害事例が報道されたところであり、今後もますます注意が必要な状況となっている。

今回確認されたビジネスメール詐欺の手口は、国内組織とその取引先企業（海外の企業）間で取引を行っている中で、攻撃者が取引先になりすまし、偽の口座情報を連絡して送金をさせようとするものであった。これは、IPA が 2017 年 4 月に公開した注意喚起のレポート [13]で紹介しているビジネスメール詐欺の 5 つのタイプのうち、「タイプ 1:取引先との請求書の偽装」に該当する。

5.1 攻撃手口の詳細

今回の事例では、詐欺の過程において、次の手口が使われた。

- TLD[14]違いの詐称用ドメインの取得と悪用
- ビジネスメールの授受に割り込み、詐欺を試みる

（1） TLD 違いの詐称用ドメインの取得と悪用

攻撃者は、海外の取引先企業のドメインに似通った「詐称用ドメイン」を、**なりすましメールを送信する“前日”に取得**し、DNS やメールサーバの設定を実施していた。不正な目的で自組織の類似ドメインが新たに取得されていないかを定期的にチェックしている企業があるが、そのような対策を回避しようとしているものと考えられる。あるいは、詐欺がうまく進みそうな場合に、状況に応じてドメインを適宜取得するという、柔軟かつ素早い行動をとっている可能性もある。

今回取得された詐称用ドメインの DNS 情報には、SPF[15]レコードと DKIM[16]も設定されており、「SPF 検証」および「DKIM 検証」に成功（Pass）する状態となっていた。この状態でメールを送られた場合、なりすましメール対策のための SPF 検証や、メールの改ざん対策のための DKIM 検証といったシステム対策は効果がないことになる。

なお、詐称用ドメインは、次の例に示すように、正規ドメインの 1 文字違いの TLD を使用（悪用）したものであった。

【本物のメールアドレスのドメイン名】 alice @ company-a . l**v**
【偽物のメールアドレスのドメイン名】 alice @ company-a . l**u**　⇒ 「v」と「u」が異なる

※実際に悪用されたものとは異なる。

---

[13] 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口 （IPA）
https://www.ipa.go.jp/security/announce/20170403-bec.html

[14] Top Level Domain （トップレベルドメイン）。ドメイン名のもっとも右側に記載されている文字列。「.jp」のような各国/地域に割り当てられた TLD には、1 文字違いのものも多く存在する。

[15] なりすましメール撲滅に向けた SPF（Sender Policy Framework）導入の手引き （IPA）
https://www.ipa.go.jp/security/topics/20120523_spf.html

[16] DKIM （Domainkeys Identified Mail） （一般財団法人インターネット協会）
http://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/dkim/

（2）ビジネスメールの授受に割り込み、詐欺を試みる

今回の事例では、A 社（国内企業）と海外取引先との間でビジネスメールをやり取りしていた中に、詐称用ドメインを使って取引先の担当者になりすました攻撃者が割り込み、詐欺を試みてきた。攻撃者は、何らかの方法でメールを盗聴していたものと考えられる。

A 社と攻撃者の間で数回のメールのやりとりが行われた（図 11）が、幸い、A 社側で**メールの受信者とは別の「外貨支払い担当部門の担当者」が途中で不審であると気づくことができた**ため、被害には至らなかった。なお、今回の事例でやりとりされたメールはすべて英文である。

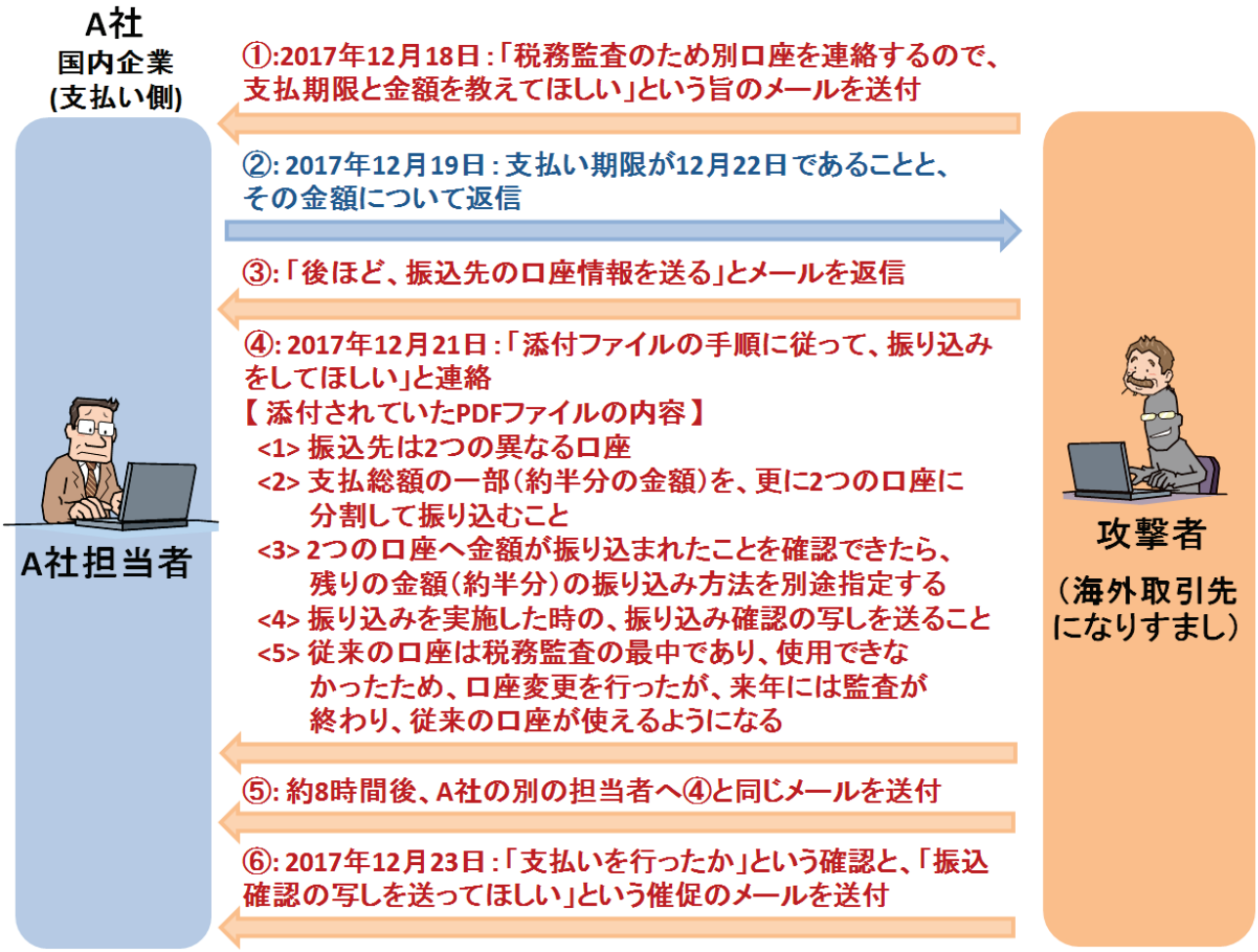


図 11 攻撃者とのやりとり

ビジネスメール詐欺のこの他の事例と対策については、2017 年 4 月の注意喚起のレポートで詳細に述べている。ビジネスメール詐欺は、特に海外と取引のある国内企業にとって、重大な脅威である。

被害に遭わないようにするため、ビジネス関係者全体で、その脅威を認識し、手口を理解するとともに、不審なメール等への注意力を高めておくことが重要である。社内だけでなく、取引先等に対しても、ビジネスメール詐欺への注意を促すことも検討していただきたい。

6　DDE を悪用した攻撃の手口

2017 年 10 月、脆弱性の悪用やマクロ機能の悪用とは異なる、Microsoft Office の DDE（Dynamic Data Exchange）という機能を用いた攻撃手口の情報を入手し、J-CSIP 内に情報共有を行った。

DDE を悪用した攻撃は別名 DDEAUTO 攻撃とも呼ばれており、この攻撃手口については、2017 年 11 月 9 日時点で、Microsoft 社から注意と緩和策を提示するセキュリティアドバイザリが公開されている [17]。また、2017 年 12 月と 2018 年 1 月に、Microsoft 社が Office 製品の Word と Excel 上でこの攻撃が動作しないよう、更新プログラムを公開している [18]。このため、現時点において、Windows Update を適用している利用者は、この攻撃手口による被害を受ける可能性は低いものと思われる。

この攻撃にはいくつかのパターンが存在し、メールに添付された Office 文書ファイルだけではなく、Outlook でメール形式のファイルを開封すると攻撃を受けてしまう手口も存在する。また、実際に攻撃が成功する（被害に遭ってしまう）ためには、画面に表示される警告ウインドウで、利用者が警告を無視するような操作を行う必要があるが、ここでは DDE 機能に特有の警告メッセージが表示されるため、何が危険な操作であるかを利用者が判断するのは難しい可能性がある。

この手口について、今後、国内での攻撃に使われるようになる可能性があるため、攻撃手口と注意点（表示される警告メッセージと、その場合に選択すべきボタン等）をまとめた一般利用者向けの参考資料を、本紙と併せて公開した [19]。

IPA で確認できている範囲では、海外で無差別にばらまかれたウイルスメールの添付ファイルで悪用された [20]手口ではあるが、一部は国内で標的型攻撃に用いられた可能性を示す情報もある [21]。このため、攻撃の特徴、表示される警告画面、ウイルス感染を防ぐため利用者が選択するべき操作について広く周知することが重要だと考える。必要に応じ、参考資料を活用していただきたい。

「標的型サイバー攻撃特別相談窓口」への情報提供のお願い

IPA では、一般利用者や企業・組織向けの「標的型サイバー攻撃特別相談窓口」にて、標的型攻撃メールを含む標的型サイバー攻撃全般の相談や情報提供を受け付けている。限られた対象にのみ行われる標的型サイバー攻撃に対し、その手口や実態を把握するためには、攻撃を検知した方々からの情報提供が不可欠である。ぜひ、相談や情報提供をお寄せいただきたい。

「標的型サイバー攻撃特別相談窓口」（IPA）
https://www.ipa.go.jp/security/tokubetsu/

以上

---

[17] マイクロソフトセキュリティアドバイザリ 4053440（マイクロソフト）
https://technet.microsoft.com/ja-jp/library/security/4053440.aspx

[18] ADV170021 | Microsoft Office の多層防御機能の更新プログラム（マイクロソフト）
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/ADV170021

[19] 【参考資料】DDE を悪用した攻撃手口に関する注意点

[20] Necurs Botnet malspam pushes Locky using DDE attack（SANS ISC）
https://isc.sans.edu/forums/diary/Necurs+Botnet+malspam+pushes+Locky+using+DDE+attack/22946/

[21] 外務省職員を発信元と詐称する巧妙な(?)不審メール調査メモ（(n)inja csirt）
https://csirt.ninja/?p=1327