サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2020 年 7 月～9 月]

2020 年 10 月 29 日
IPA（独立行政法人情報処理推進機構）
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、2020 年 9 月末時点の運用体制、2020 年 7 月～9 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

2020 年 7 月～9 月期（以下、本四半期）は、次の通り参加組織の増加があり、全体では 2020 年 6 月末の 13 業界 259 組織＋2 情報連携体制から、13 業界 263 組織[2]＋2 情報連携体制（医療業界 4 団体およびその会員約 5,500 組織、水道関連事業者等 9 組織）の体制となった。（図 1）。

- 2020 年 8 月、電力業界 SIG に新たな参加組織があり、42 組織から 46 組織となった。

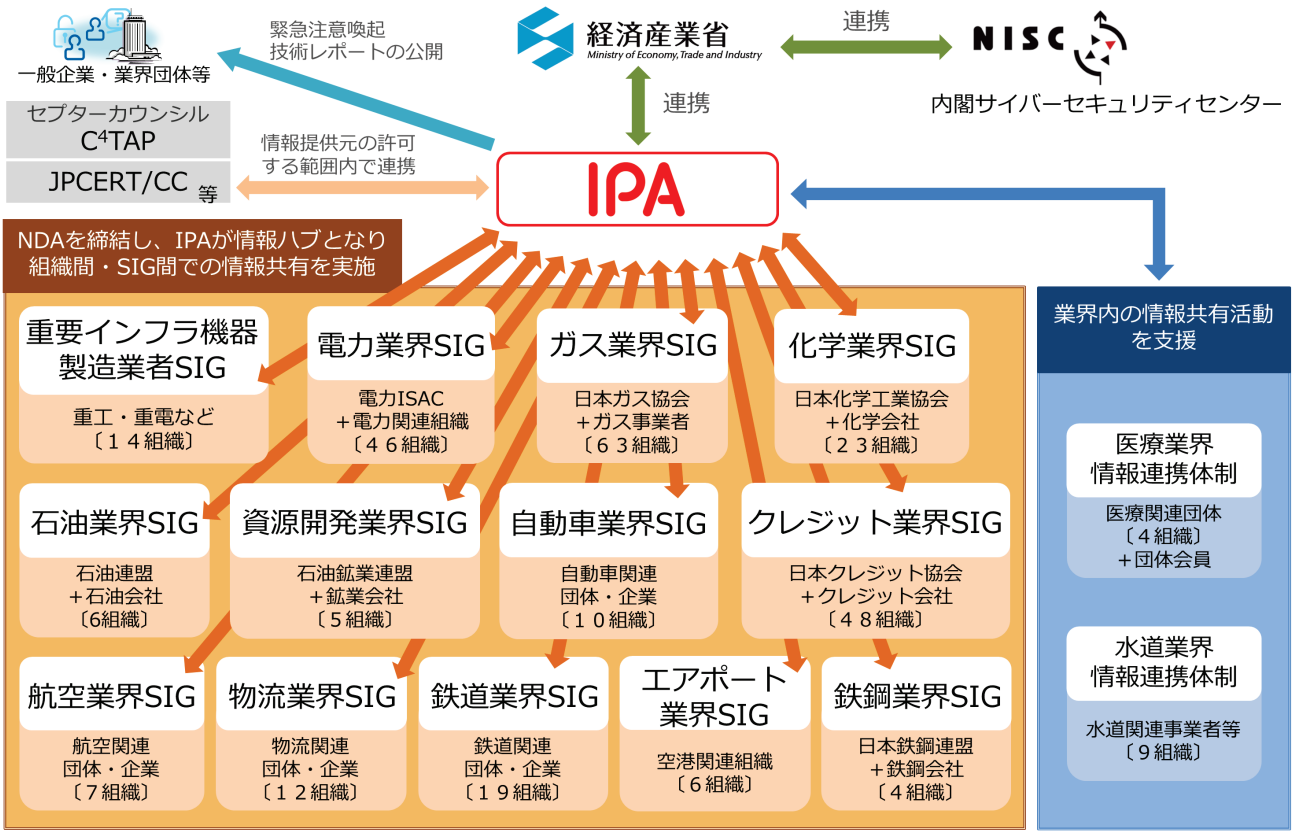

図 1 J-CSIP の体制図

[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（2020 年 7 月～9 月）

2020 年 7 月～9 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（9 月末時点、13 の SIG、全 263 参加組織と、2 つの情報連携体制での合算）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	2019 年	2020 年		
		10 月～12 月	1 月～3 月	4 月～6 月	**7 月～9 月**
1	IPA への情報提供件数	1,042 件	602 件	325 件	**4,988 件**
2	参加組織への情報共有実施件数※1	40 件	56 件	55 件	**29 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 **20 件**を含む。

本四半期は情報提供件数が **4,988 件**であり、うち標的型攻撃メールとみなした情報は **9 件**であった。提供された情報の主なものとして、Emotet への感染を狙う攻撃メールについての情報提供が 9 割以上を占めている。これについては、3 章で述べる。

また、複数組織へ継続して行われた CEO を詐称する一連の攻撃や、2020 年 4 月に公開したビジネスメール詐欺第三報 [3]にある、「日本語化」された CEO 詐欺の攻撃についての情報提供もあった。これについては、4 章で述べる。

前四半期で観測されなかったプラント関連事業者を狙う一連の攻撃について、本四半期でも観測数は少なかった。しかし、同一の攻撃者による別の業界を狙った攻撃について、本四半期で注目するものが確認された。これについては、5 章で述べる。

これまでと異なる手法で Excel のマクロの悪用が試みられた攻撃について情報提供があった。また、この手口では、悪性のコードを細切れにすることで、セキュリティソフトによる検知を避ける仕掛けも施されていた。これについて、6 章で述べる。

[3] 【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（第三報）（IPA）
https://www.ipa.go.jp/security/announce/2020-bec.html

情報提供に付随して、IPA へ次のような相談・報告事例があった（表 2）。

表 2 相談・報告事例

項番	相談・報告内容	件数
1	Office 365 のアカウント情報を狙うフィッシングメールが大量に着信した。	1 件
2	組織内から外部の不審サイトに不正通信を行っていることを検知した。	4 件

項番 1 は、Office 365 のアカウント情報を狙うフィッシングメールが大量に着信したというもので、本四半期では、一つの組織で約 160 通のフィッシングメールが着信したという情報提供があった。これまでも Office 365 のアカウント情報を狙うフィッシングメールは観測されており、J-CSIP の運用状況レポートで度々紹介している。Office 365 といったアカウント情報を狙う攻撃は、騙された利用者のアカウントを通じ、企業・組織内の情報等が侵害される可能性をもたらす脅威であり、注意が必要である。フィッシング詐欺への対策は、二要素認証の導入のほか、利用者一人ひとりが、騙されないよう手口を知ることが重要である。

項番 2 は、組織内の PC から不審サイトへのアクセスをセキュリティ機器で検知したというもので、URL 等はそれぞれ異なるが、同様の情報提供・相談が継続している。調査の結果、いずれも、ウェブ閲覧中に不正な広告があるページを開いたものや、何らかの理由で詐欺サイトのような悪意のあるウェブサイトへ誘導されたものであった。意図的に不審なサイトを閲覧せずとも、通常業務の中でこのようなことは発生しうるため、攻撃の被害に遭わないよう、OS やブラウザ等のソフトウェアの脆弱性を解消するとともに、不審サイト・詐欺サイト・偽警告 [4]等に騙されないようにするといった従業員への教育を継続的に実施すべきであろう。

[4] 被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20170411.html

3 Emotet への感染を狙う攻撃メールについて

本四半期、複数の J-CSIP 参加組織より、Emotet への感染を狙った攻撃メール（以降、Emotet 攻撃メール）を確認したという情報提供が、4,730 件あった。本四半期での情報提供件数のおよそ 95%が Emotet に関連したものである。

Emotet への感染を狙う攻撃については、特定の組織・企業を狙ったものではなく、公開情報でも多数観測されており、被害を受けたという事例も複数確認されている。本章では、本四半期で J-CSIP 参加組織より情報提供を受けた Emotet 攻撃メールの観測状況と、攻撃手口について説明する。

3.1 Emotet とは

Emotet とは、感染した端末の情報の窃取に加え、さらに他のウイルスへの感染のために悪用されるウイルスである。

海外では、2014 年頃から観測されていると言われており、J-CSIP では 2017 年 6 月には参加組織内で観測している。その後、2019 年 9 月中旬頃から Emotet 攻撃メールが日本国内で観測されはじめ、2020 年の 2 月上旬頃まで大規模なばらまきが観測された。その後、一時的に観測されていない時期があったが、2020 年 7 月より再び Emotet 攻撃メールのばらまきが観測されている。

メールの件名や内容は、正規のメールへの返信を装うものや、賞与通知や新型コロナウイルス感染症（COVID-19）のように時事の話題を題材としたものが観測された。

なお、IPA では Emotet 攻撃メールについて複数回の情報発信[5]をしており、本四半期でも 2 回の情報発信（2020 年 7 月 28 日、2020 年 9 月 2 日）を行っている。この情報発信では、攻撃メールの他 Word 文書ファイルの内容等についても記載している。J-CSIP の参加組織から情報提供があった Emotet 攻撃メールも当該の情報発信と同等の攻撃手口が使われていた。

3.2 本四半期での Emotet への感染を狙った攻撃メールの観測状況

2020 年 7 月から 9 月において、Emotet 攻撃メールの J-CSIP 内での観測状況（日別の件数）を図 2 に示す。

先述の通り、Emotet 攻撃メールは、2020 年 2 月上旬以前と、2020 年 7 月中旬以降に観測している。Emotet 攻撃メールには悪意のあるマクロが仕込まれた Word 文書ファイルが添付されているものや、メール本文中に URL リンクが記載されているものを確認した。メール本文中の URL リンクをクリックすると、悪意のあるマクロが仕込まれた Word 文書ファイルがダウンロードされる。受信者が、これらの Word 文書ファイルを開き、マクロ機能を有効化（コンテンツの有効化ボタンのクリック）してしまうと、Emotet がダウンロードされ、感染させられてしまうという仕組みは、過去に観測されていたものと同じであった。

さらに、2020 年 9 月以降は、メールにパスワード付きの ZIP ファイルを添付した Emotet 攻撃メールも観測された。パスワードはメール本文中に記載されており、ZIP ファイルにはこれまでと同様の悪意のあるマクロが仕込まれた Word 文書ファイルが含まれている。添付ファイルが暗号化されていることから、メール配送経路上でのセキュリティ製品の検知・検疫をすり抜け、受信者の手元に Emotet 攻撃メールが届いてしまう可能性が高く、攻撃者にはその狙いがあると思われる。

---

[5] 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて（IPA）
https://www.ipa.go.jp/security/announce/20191202.html

なお、ZIP ファイル内の悪意のある Word 文書ファイルについては、着信日時により見た目の変化がいくつか確認されたが、いずれもマクロ機能を悪用しており、利用者のマクロを有効化する操作により Emotet を感染させるという点は共通していた。

これら Emotet 攻撃メールの件名や添付ファイル名、メール本文の内容については様々な種類があり、一般的な用件（請求書等）を装うような件名や添付ファイル名の他に、トレンドマイクロ社を騙るもの[6]や、正規のメールへの返信（Re:）や転送（Fwd:）を装うものも確認されている。メール本文については、比較的日本語に不自然な点が少ないものも見られたが、簡素な文面であったり、日本語に不自然な点が見られるものもあった。また、正規のメールの返信を装う手口では、メールの本文内で正規のメールを引用（転載）しているため、攻撃者が独自に作成した本文部分が多少不自然であったとしても、利用者が添付ファイルを開いてしまう可能性が高く、危険である。

J-CSIP 参加組織から情報提供されたメールの件名と添付ファイル名について、表 3 に示す。これらのメールは日本国内に送られた Emotet 攻撃メールの一部であるが、同様の攻撃メールが広くばらまかれたものと考えられる。また、組織によっては、一定期間の間に数百から数千という単位で Emotet 攻撃メールを観測しているところもあれば、数通しか確認していないといった組織もあった。

また、J-CSIP 参加組織においても、パスワード付きの ZIP ファイルが検疫できずメール受信者の手元まで配送されたというケースや、受信者が Word 文書ファイルを開いてしまった（ウイルス感染は免れている）という情報提供もあり、攻撃者による手口の巧妙化が現実的な脅威となっている。

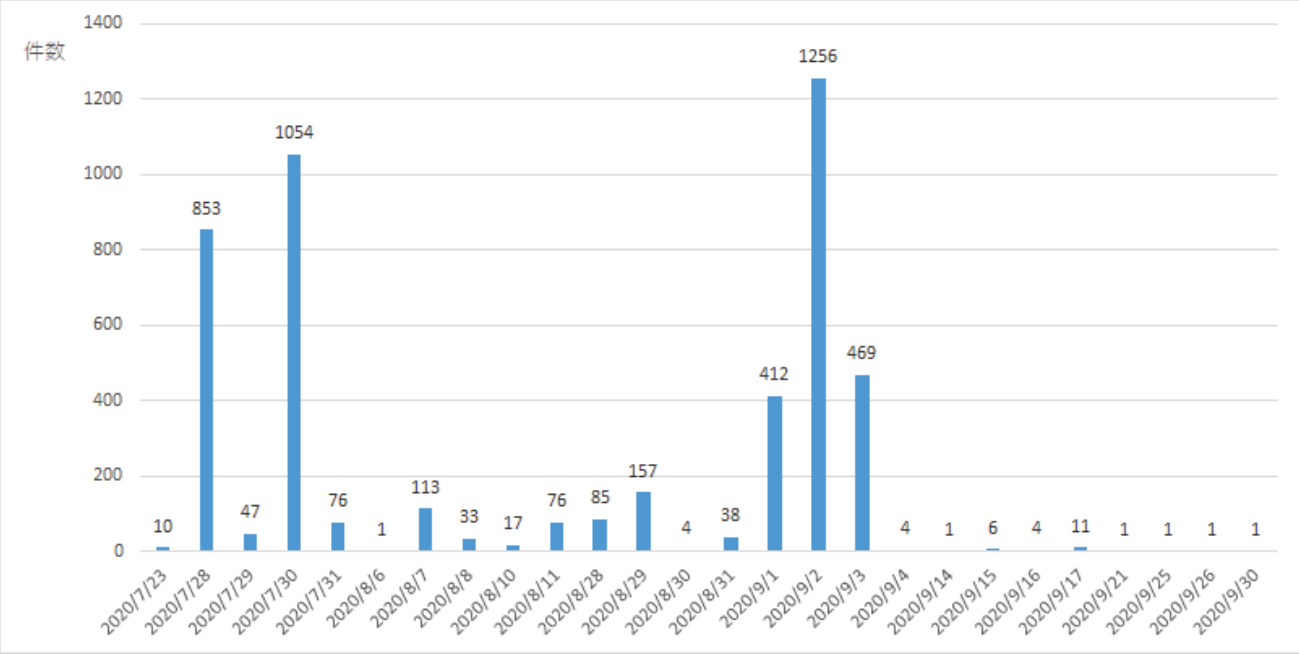

図 2 J-CSIP 内で観測された日別の Emotet 攻撃メールの件数（7 月～9 月期）

[6] 「EMOTET」がトレンドマイクロのアンケートメールを偽装（トレンドマイクロ）
https://blog.trendmicro.co.jp/archives/26049

表 3 J-CSIP 内の Emotet 攻撃メールの件名と添付ファイル名（タイプ別整理）

	請求書関連	会議関連	英語（主に請求書等を装う）	その他（時事話題、返信・転送を装う等）
メールの件名	・ 請求書の送信 ・ 確認して承認してください ・ 請求書ステータスの更新 ・ 請求書の件です。[ランダム数字と日付] ・ 請求書送付のお願い[ランダム数字と日付] ・ サービス請求書 ・ 未請求書 ・ ご入金額の通知・ご請求書発行のお願い[ランダム数字と日付] ・ の請求書（メーラの表示名が先頭につくケースもある） ・ [メーラの表示名] からの延滞請求書 ・ 3 月の請求書 ・ 請求書の請求 ・ 表示用の［メーラの表示名］アカウントの請求書 ・ 特別請求書 ・ 毎月の請求書 ・ 注意事項：請求書 ・ 未請求書 ・ 期限切れ請求書 ・ あなたの請求書 ・ 見積もり依頼の件	・ ビジネス会議への招待（メーラの表示名が後ろにつくケースもある） ・ ミーティング ・ 会議への招待（メーラの表示名が後ろにつくケースもある） ・ 仕事への招待	・ Comments ・ ACH Payment[日付] ・ Past Due invoice ・ Payment status ・ payment ・ Invoice#[ランダム英数字]	・ 異動のご挨拶 ・ コロナ対策のお願い ・ Re:[メーラの宛先表示名] ・ Fwd:[メーラの宛先表示名] ・ 消防検査 ・ トレンドマイクロ・サポートセンター満足度アンケート調査　ご協力のお願い ・ トレンドマイクロ・カスタマー満足度アンケー ・ トレンドマイクロ・ ・ 問題 ・ 助けてください ・ 助けが必要 ・ 各位 ・ Re:[実際に過去送受信した件名] ・ Fwd:[実際に過去送受信した件名] ・ Re: ・ Fwd:

	請求書関連	会議関連	英語（主に請求書等を装う）	その他（時事話題、返信・転送を装う等）
添付ファイル名	・ 請求書送付のお願い[ランダム数字と日付].doc ・ ご入金額の通知・ご請求書発行のお願い[ランダム数字と日付].doc ・ 請求書の件です。[ランダム数字と日付].doc ・ [ランダム英数字と日付]請求書の件です.doc ・ [ランダム英数字と日付]請求書送付のお願い.doc ・ [ランダム英数字と日付]ご入金額の通知・ご請求書発行のお願い.doc	・ 会議への招待.doc ・ ミーティング.doc ・ 仕事への招待.doc ・ ビジネス会議への招待.doc	・ Scan-[ランダム数字と日付].doc ・ form.doc ・ Invoice#[ランダム数字].doc ・ Copy Invoice#[ランダム数字].doc ・ report.doc ・ October documentation.doc ・ info.doc ・ Information.doc ・ confidential docs.doc ・ comment_[ランダム英数字].doc ・ August Invoice.doc ・ Inv.[ランダム数字].doc ・ Payment[ランダム数字].doc ・ Payment Status.doc ・ Electronic report.doc ・ Electronic form.doc ・ PO#[ランダム数字].doc ・ check copy.doc ・ copy.doc	・ [ランダム英数字][日付].doc ・ [ランダム英数字].doc ・ に修 [日付].doc ・ 変化 [日付].doc ・ からの変更 [日付].doc ・ 消防検査.doc ・ トレンドマイクロ・カスタマー満足度アンケー.doc ・ ト調査 ご協力のお願い.doc ・ トレンドマイクロ・.doc ・ トレンドマイクロ・カスタマー満足度アンケート調査 ご協力のお願い.doc ・ カスタマー満足度アンケー.doc ・ 最新の構造図.doc ・ 構造図.doc ・ 総会 [日付].doc ・ 各位.doc ■ZIP ファイル名パターン ・ [ランダム英数字].zip ・ [ランダム英数字] [日付].zip ・ [ランダム英数字].doc.zip ・ からの変更 [日付].zip ・ 変化 [日付].zip

※ここで示すメールの件名や添付ファイル名は、Emotet 攻撃メールの一部である。すべてのパターンを網羅していない。

※一部トレンドマイクロ社名が見られるが、攻撃者によって詐称・悪用されているだけであり、当該企業に原因や問題があるわけではない。

3.3 対策

Emotet をはじめとした、ばらまき型メールの攻撃者は、メールフィルタリング等のセキュリティ対策をかいくぐり、受信者が添付ファイルを開いてしまう、メール内の URL リンクをクリックしてしまうよう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）を行っていくことが重要である。

Emotet への感染を防ぐということにとどまらず、次のような基本的なウイルス対策を徹底していただきたい。

- 身に覚えのないメールの添付ファイルは開かない。メール本文中の URL リンクはクリックしない。
- 自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。
- OS やアプリケーション、セキュリティソフトは常に最新の状態にする。
- 信頼できないメールに添付された Word 文書ファイルや Excel ファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。
- メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する。
- 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する。

また、Emotet 攻撃メールへの対策・対応として、Word のマクロ機能に関する設定の変更、Emotet に感染した場合の影響等について、下記 JPCERT/CC から公開されている注意喚起を併せて参照していただきたい。

「マルウエア Emotet の感染に関する注意喚起」（JPCERT/CC）
https://www.jpcert.or.jp/at/2019/at190044.html

「マルウエア Emotet への対応 FAQ」（JPCERT/CC）
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

4　ビジネスメール詐欺（BEC）の事例

本四半期においても、引き続き J-CSIP の参加組織に対してビジネスメール詐欺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、2017 年 4 月と 2018 年 8 月、そして 2020 年 4 月の 3 回にわたり IPA より注意喚起を行ったが、その後も継続して事例を確認しており、今後も注意が必要な状況である。

ビジネスメール詐欺の被害に遭わないようにするため、ビジネス関係者全体で、この脅威を認識し、手口を理解するとともに、不審なメールやなりすましメールへ警戒する必要がある。社内ルールを整備し、組織全体で被害を防止するという体制も必要であろう。また、社内だけではなく、取引先や銀行等、ステークホルダ全体でビジネスメール詐欺の被害防止に向けた対策が進むことが望ましい。

本四半期は、J-CSIP の参加組織から 7 件のビジネスメール詐欺について情報提供を受けた。いずれも、タイプ 2（経営者等へのなりすまし）であった。さらに、J-CSIP 外の一般企業・組織からも 11 件のビジネスメール詐欺の情報提供があった。

本章では、2019 年 10 月～12 月期から継続して観測していた「複数組織へ行われた CEO を詐称する一連の攻撃」や、2020 年 4 月の注意喚起レポートに掲載した、「日本語化」された CEO 詐欺の攻撃について、本四半期でも継続して確認されたため、あわせて説明する。

4.1 事例 1 複数組織へ行われた CEO を詐称する一連の攻撃（続報）

2019 年 10 月以降、J-CSIP の参加組織から、国内グループ会社の経営層を詐称したなりすましメールについて、前四半期までと同様、継続して情報提供があった。また、IPA で J-CSIP 外の情報等を含め独自に調査を行ったところ、情報提供されたものと合わせて新たに **7 件**（2019 年 10 月～12 月期では 62 件、2020 年 1 月～3 月期では 46 件、2020 年 4 月～6 月期では 50 件確認）の類似するメール検体を入手するに至った [7]。

これらのメールは次に示す点が共通しており、同一の攻撃者による攻撃が、国内外の多数の組織へ行われたものと推測される状況である [8]。この一連の攻撃については、攻撃手口等からビジネスメール詐欺の一種であると考えており、「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」の 2.3 章 事例 3 も、この一連の攻撃の一部である。

- メールの宛先は、国内外の複数の企業（経営者、役員、職員等と思われるメールアドレス）である。
- 実在する CEO や弁護士等を詐称している。
  - CEO を詐称する際、ほぼ、攻撃先の各企業の実際の CEO を名乗っている。（少数だが、取引先の CEO を名乗る事例も確認している）
- 攻撃者が使用したメールアドレスは様々に異なるが、命名に規則性がある。具体的には、差出人（From）や返信先（Reply-To）に、「secure」等という単語と、天体（惑星・衛星・星座等）に関する単語を組み合わせたメールアドレスが多く観測されている（天体以外のケースも観測している）。
- これまで確認した一連の攻撃メールの件名や本文はほぼ英文であり、日本語 [9]、スペイン語、フランス語のメールを確認している。メールの件名・本文の内容は多数のバリエーションがある。メールへ返信すると、金銭の振り込みの要求等の詐欺が試みられるものと思われる。
  - 2019 年 7 月 23 日から 2020 年 9 月 16 日までのメールの特徴としては、メール本文は 5～10 行程度の簡素なもので、具体的な用件は書かれていないが、「重要な用件がある」、「計画について話がしたい」として、メールへ返信することを求める内容である点が共通している。
  - 2020 年 3 月 24 日以降、新型コロナウイルス感染症（COVID-19）の話題を文章の書き出しとして使用する攻撃メールを複数確認している。
    - 2020 年 3 月 24 日から 2020 年 5 月 12 日までのメールでは、「COVID-19 による世界的な危機の中、皆様の安全や健康を願っている」という書き出しのもの [10]が多かったが、2020 年 5 月 20 日以降のメールでは、「世界中の国々が徐々に規制を緩和していく中で、経済活動を再開していかなければならない」といったように、文章に変化が見られた。
    - 2020 年 5 月以降に観測されたメールでは、件名に「Project」が入るものも観測されるようになった。
- メールの着信時期は、確認できている限り、2019 年 7 月 23 日から 2020 年 9 月 16 日である。

---

[7] 本事例については、本レポート執筆時点である 2020 年 10 月 2 日までの情報で記載している。

[8] これらメールの特徴については、米国 Agari Data 社が次の URL で公開しているレポートと同様であり、同一の攻撃者による攻撃であると推測している。
https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/

[9] 日本語のメールについては、サイバー情報共有イニシアティブ（J-CSIP）運用状況[2019 年 10 月～12 月]にメールの例を記載している。

[10] 本件のメールについては「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」で紹介している。
http://www.ipa.go.jp/security/announce/2020-bec.html

本四半期に IPA で確認したメールの情報の一覧を、表 4 に示す。

この一連のビジネスメール詐欺は、特定の組織や業種のみを狙うものではなく、多数の業種に対して試みられたことを確認している。このため、業種に関わらず、継続して国内外の組織に対して攻撃が試みられる可能性があり、注意が必要である。

なお、本四半期では本件と同等のビジネスメール詐欺の観測数は大きく減少している。本件の攻撃について、攻撃が一時的に停止しているのか、または本件の攻撃そのものが停止したのかは不明である。

表 4 事例 1 IPA で確認している本件の攻撃メール情報の一覧

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
1.	製造業	2020/1/17	Corporate matter follow up	secure-neptune@secure-mx-gateway.cc
2.	学術研究，専門・技術サービス業	2020/4/20	Liaise with external legal counsel	【匿】.comserver@relay-secure-smtp.com
3.	製造業	2020/4/24	Corporate matter Action needed	legal@privileged-secured.com
4.	製造業	2020/7/8	Project Cheetah	node-saturn@mx-gateway-host.cc
5.	-	2020/7/16	External legal counsel	secure@ssl-encrypted.live
6.	製造業	2020/8/4	Project Hubble	secscan-saturn@intranet-host.cc
7.	製造業	2020/8/4	Project Hubble	secscan-saturn@intranet-host.cc

4.2 事例 2「日本語化」された CEO 詐欺の攻撃（続報）

2020 年 4 月、「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」の 2.1 章 事例 1 にて、英語で行われていた攻撃が「日本語化」され、日本の企業へ着信したビジネスメール詐欺の事例を公開した[11]。その後、J-CSIP の参加組織から、国内企業の経営層を詐称したなりすましメールについて、継続して情報提供があった。また、IPA で J-CSIP 外の情報等を含め独自に調査を行ったところ、情報提供されたものと合わせて新たに **8 件**（2020 年 3 月末時点では 7 件、2020 年 4 月～6 月期では 25 件確認）の類似するメール検体を入手するに至った[12]。

これらのメールは次に示す点が共通しており、同一の攻撃者による攻撃が、国内外の多数の組織へ行われたものと推測される状況である。

- メールの宛先は、国内外の複数の企業（CEO 等と思われるメールアドレス）である。
- 実在する CEO を詐称している。
- 攻撃者が使用したメールアドレスは様々に異なるが、命名に規則性がある。具体的には、送信元や、返信先メールアドレス（From ヘッダや Reply-To ヘッダ）で、「board」や「board-1」、「relay」、「smtp」という単語がローカル名に使われており、ドメイン部分には「intern」や「mobile」、「server」といった単語を組み合わせたメールアドレスが使用されている。
- 英語と日本語の差はあるが、件名や本文はほぼ同じ内容である。最初に着信するメール（1 通目）の本文は 5 行～10 行程度の簡素なもので、「出張中であるが、企業買収について協力してほしいことがある」といった内容が書かれている。
  - メールに返信をすると、外国企業買収のため、外部の弁護士と協力して支払いを実施してほしいという旨のメールが攻撃者から送られてくる。
  - 本四半期に情報提供された事例では、1 通目のメールに返信をしたところ、攻撃者は実在する弁護士を騙り、連絡手段を教えてほしいといった旨のメールを送ってくることを確認した（図 3）。
- メールの着信時期は、確認できている限り、2019 年 11 月 20 日から 2020 年 8 月 17 日である。
- メールの送信に「SendGrid」というメールサービスを使用している[13]。SendGrid が提供する機能として、受信者がメールを開封したことを送信者が追跡できる仕掛け（ウェブビーコン）をメールに埋め込むことが可能であり、実際に、SendGrid のビーコンと思われる HTML タグが一部のメール検体で確認できている。
  - 攻撃者が意図的にビーコンを仕掛けているのかは不明だが、この点も、攻撃手口の巧妙化を示している可能性がある。

本四半期に IPA で確認したメールの情報の一覧を、表 5 に示す。

この一連のビジネスメール詐欺は、これまでに複数の業種に対して試みられたことを確認しており、特定の組織や業種のみを狙うものではない。このため、業種に関わらず、継続して国内外の組織に対して攻撃が試みられる可能性があり、今後も注意が必要である。

---

[11] 【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（第三報）（IPA）
https://www.ipa.go.jp/security/announce/2020-bec.html

[12] 本事例については、本レポート執筆時点である 2020 年 10 月 2 日までの情報で記載している。

[13] SendGrid を使用していない事例も確認しており、必ずしも本サービスを使用するというわけではない。

事例 1 と共通して言える点として、これらは冷静に考えれば不審と判断できそうなメールに見える一方で、企業・組織が相対している敵は「偽メール」ではなく、そのメールを送り付けている攻撃者（人間）であり、その攻撃者は複数の組織に対して執拗に攻撃を繰り返していることが明白である。偽物だと見破ることが容易に見えるようなメールであったとしても、侮るべきではないだろう。

表 5 事例 2 IPA で確認している本件の攻撃メール情報の一覧

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
1.	卸売業	2020/1/16	金融合併と買収につきまして	board@mobile-intern81.com
2.	卸売業	2020/6/17	金融合併と買収につきまして	relay@secure-sec-gov.com
3.	化学工業	2020/7/1	金融合併と買収につきまして	relay@secure-sec-gov.com
4.	石油・石炭製品製造業	2020/7/1	金融合併と買収につきまして	relay@secure-sec-gov.com
5.	製造業	2020/7/14	headquarter project	smtp3@secure-sec-gov.com
6.	卸売業	2020/7/16	金融合併と買収につきまして	relay@secure-sec-gov.com
7.	卸売業	2020/7/20	金融合併と買収につきまして	secure@board-jp.co
8.	製造業	2020/8/17	Finance M&A	-

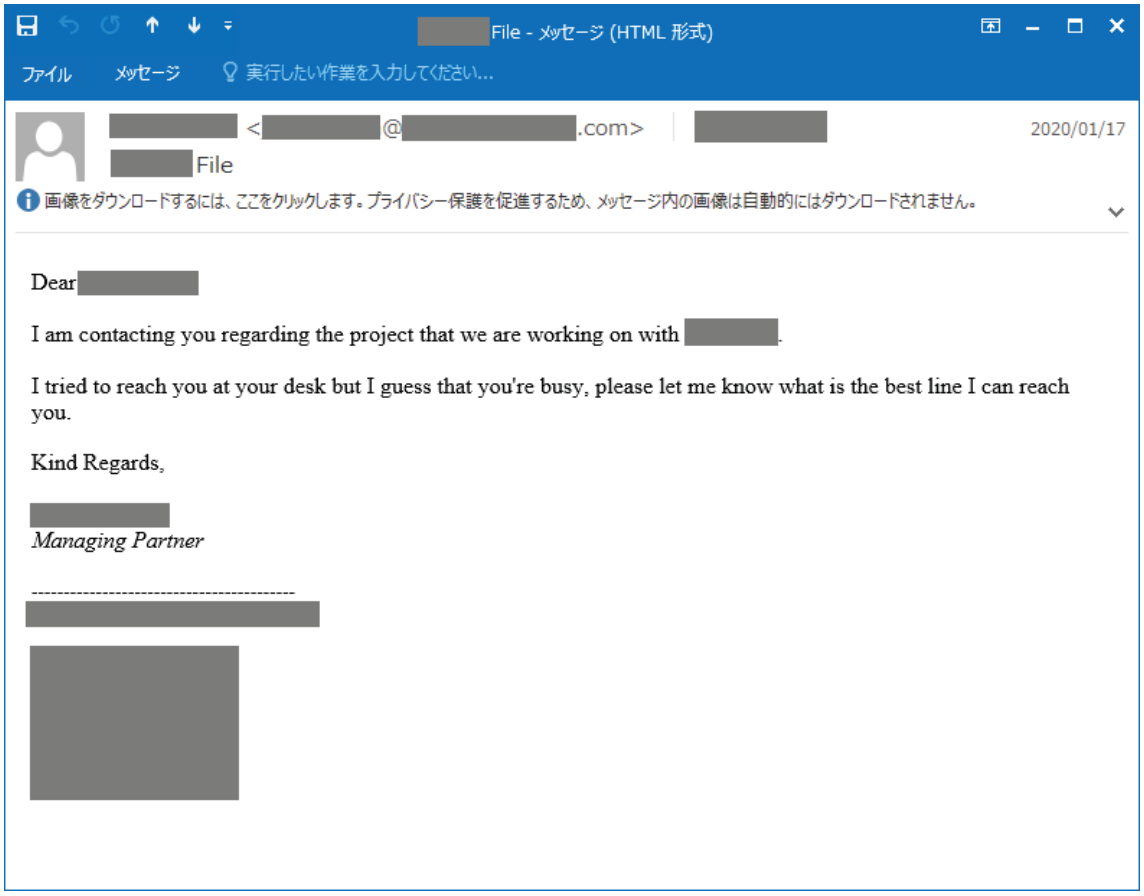

図 3 偽の弁護士になりすました攻撃者からのメール

5 プラント関連事業者を狙う一連の攻撃（続報）

2017 年 10 月以降、継続して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てきた。

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い。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ものが作成したと思われ、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作られる一方で、J-CSIP 内の数組織で確認している限り、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る。観測数が多くないという点でも、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。

5.1 攻撃の観測状況

これまで継続して確認してきた攻撃メールであるが、日本語のメールは、2019 年 11 月 26 日以降観測されていない。また、英語のメールについては 2020 年 3 月 6 日に観測して以降、本四半期で 1 通の観測のみであった。本件の攻撃について、攻撃が一時的に停止しているのか、または攻撃そのものが停止したのかは不明である。

なお、プラント関連事業者を狙う一連の攻撃と同一と考えている攻撃者による、別の業界を狙った攻撃について、本四半期で注視に値する攻撃を観測した。この攻撃については、J-CSIP 内で情報共有をしつつ、調査を行っているところである。

5.2 まとめ

プラント関連事業者を狙う一連の攻撃について、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、対象を絞って長期に渡り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。

本四半期では類似の攻撃メールは 1 通しか観測されなかったが、今後も引き続き、本攻撃者の動向を注視していく。合わせて、同一の攻撃者による別の業界への攻撃についても、引き続き調査を進めていく。

6　Excel のマクロを悪用した攻撃の手口

本四半期、Microsoft Excel のマクロ機能について、これまでと異なる手法で悪用が試みられた攻撃について情報提供があった。本件の Excel ファイルは、攻撃者によってセキュリティ製品でウイルス検知がしにくくなる手口が使われていた。本章では、この攻撃に使われた Excel ブックファイル（拡張子が .xls や .xlsx のファイル。以下、Excel ファイル）の手口について説明する。

マクロ有効化操作の誘導

攻撃メールの添付ファイルとして送られてきた Excel ファイルを開くと、マクロ機能を有効にさせる操作を行わせるよう誘導する指示が書かれている。「DocuSign（実在する海外企業）のサービスにより暗号化されているファイルであるため操作が必要」という騙し方であり、同様の手口は多く見られる。

ここで、書かれている指示に従い、Microsoft Excel のウインドウ上段部分にある黄色いセキュリティ警告バーにある「編集を有効にする」あるいは「コンテンツの有効化」といったボタンをクリックすると、Excel ファイル内に仕掛けられている悪意のあるコードの実行を許すことになり、ウイルスに感染させられてしまう。

なお、Excel ファイルを開いただけでは、ウイルスに感染しないため、利用者はこのようなファイルを開いた際に、安易にセキュリティ警告バーにあるボタンをクリックしないように徹底することが必要である。

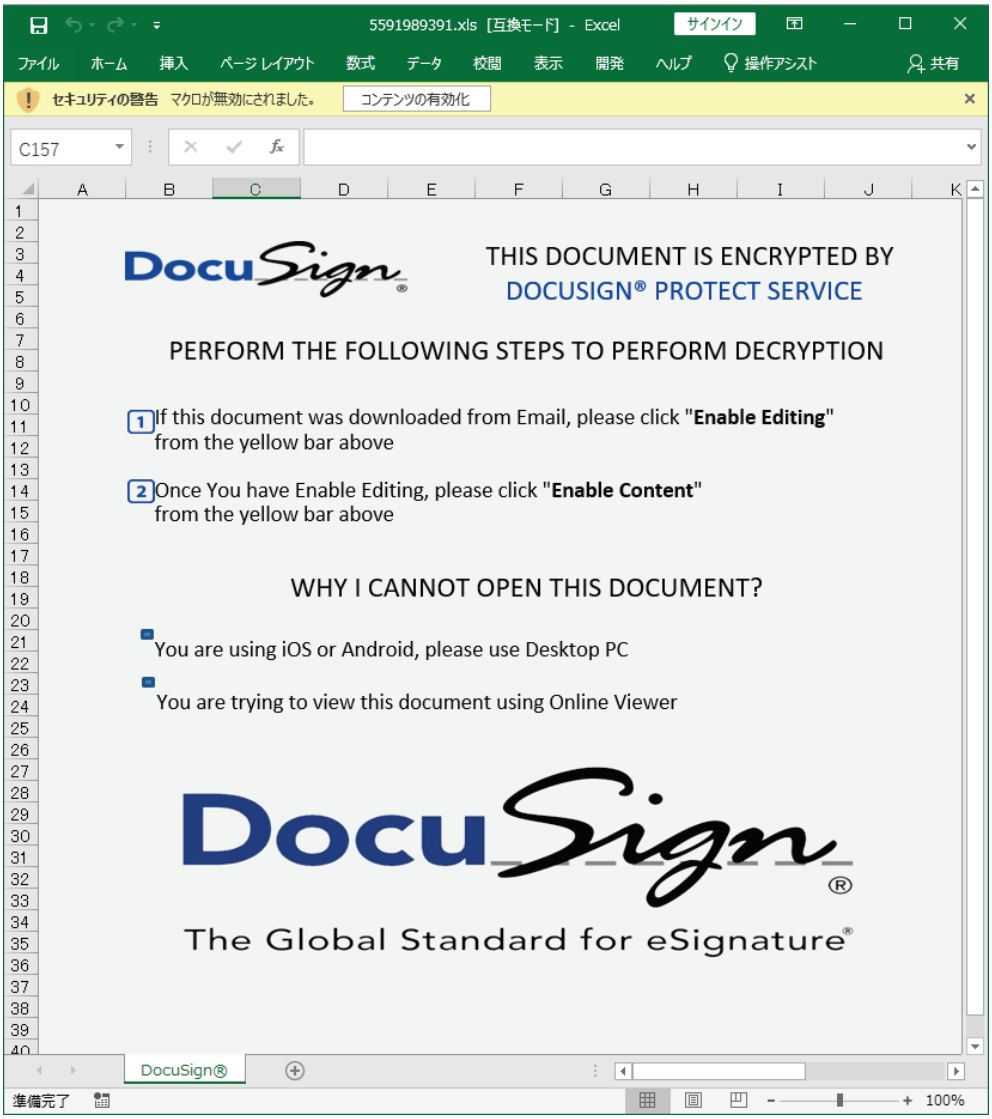

図 4 攻撃に使われた Excel ファイルの見た目

コードの秘匿の手口

本件の Excel ファイルでは、一般的によく使われるマクロ機能（Microsoft Visual Basic for Application：VBA）とは異なる手口でコードが仕掛けられ、秘匿されている。これらの仕掛けは Microsoft Excel の次の機能を悪用したものである。

・シートの非表示機能
・Excel 4.0（XLM）マクロ機能

シート非表示機能の悪用

Excel は複数のシートを作成することができ、更に、各シートを非表示とする設定が可能である。この手口では、悪意のあるマクロが書かれているシートが攻撃者によって非表示シートとして設定されていた。この非表示のシートを表示させるには、シート見出しを右クリックし、「再表示」を選択することで表示させることができる（図 5）。

図 5 シートの非表示の解除（再表示）方法

Excel 4.0 マクロの悪用

再表示したシートには、一見すると何も書かれていないように見えるが、スクロールした先（この例の場合、1,122 行目以降）に、文字色を白色にしたマクロプログラムが記載されている（図 6）。このシートは、「Excel 4.0 マクロ」シートと呼ばれるもので、シート内に書かれた命令が実行される仕組みとなっている。マクロを VBA で記述できるようになる前の、1990 年代から存在する方式である。

さらに、このマクロは、コードを断片化してシート内の複数の行に格納し、それらを結合して実行する仕組みとなっていた。これは、セキュリティソフトによる検知がされにくくなるための細工だと考えられる。

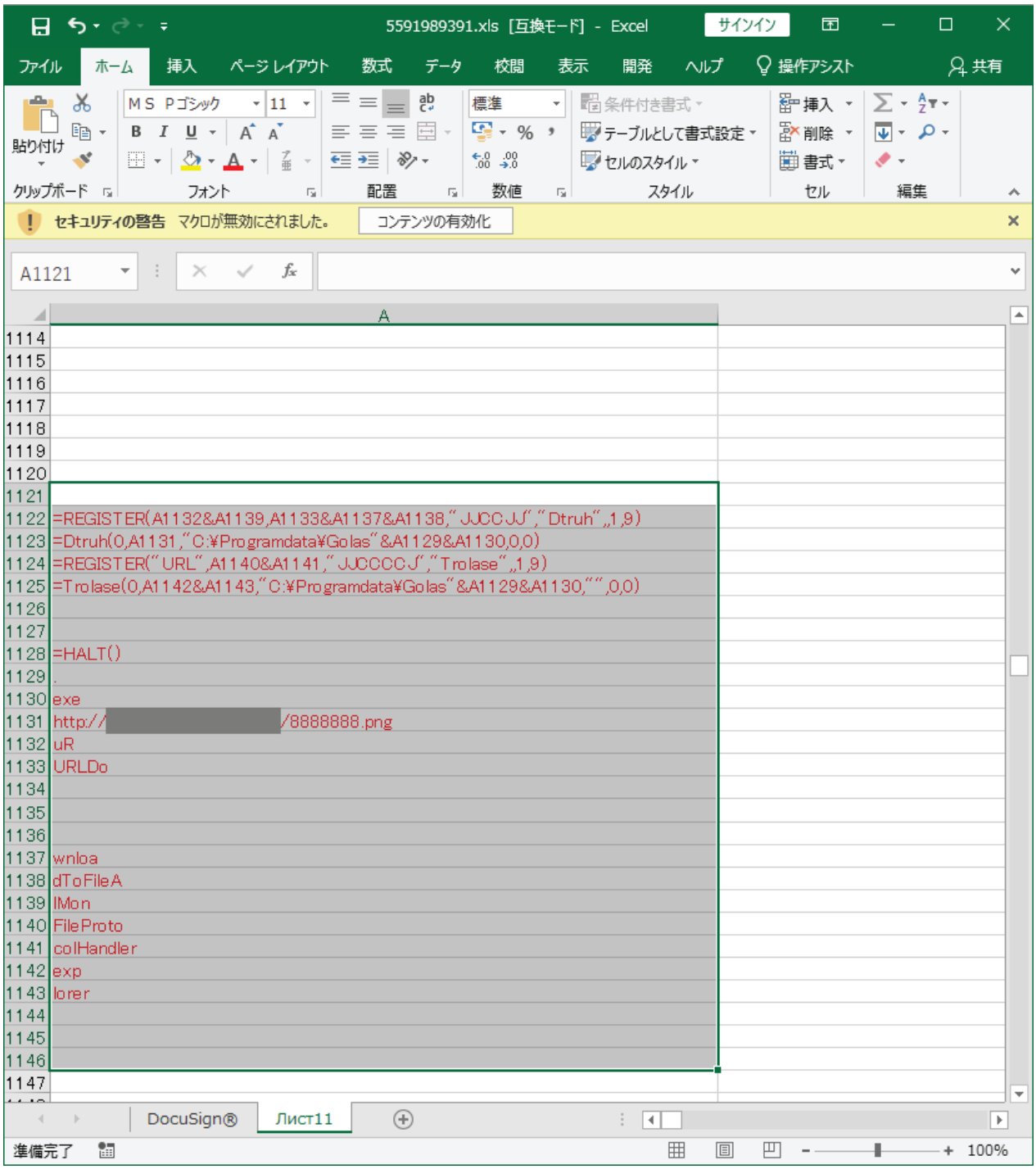

図 6 Excel 4.0 マクロシートの内容（文字色を赤に変更した状態）

検知逃れが施された本手口について、全てがメールの配送経路やセキュリティソフト等で検知・検疫できるとは限らない。Emotet の攻撃メールへの対策と同様、信頼できるファイルと判断できない場合は「編集を有効にする」や「コンテンツの有効化」のボタンはクリックしないよう、日々メールを送受信する利用者において、注意する必要がある。

また、業務上マクロを使わない利用者には、マクロ機能そのものを無効にする設定を行うことも検討してもよい。

関連情報のご提供のお願い

本書で紹介した事例について、J-CSIP では関連情報を求めています。
同様の事例を確認した場合など、下記窓口へ情報提供をいただけますと幸いです。

J-CSIP 事務局 ご連絡窓口（IPA）
jcsip-info@ipa.go.jp

標的型サイバー攻撃特別相談窓口

IPA の「標的型サイバー攻撃特別相談窓口」では、標的型サイバー攻撃を受けた際の相談を受け付けています。お気づきの点があれば、ご相談ください。

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