サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2018 年 10 月～12 月]

2019 年 1 月 31 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、2018 年 12 月末時点の運用体制、2018 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

2018 年 10 月～12 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 2018 年 9 月末の 11 業界 238 組織＋1 情報連携体制から、13 業界 249 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）。

- 2018 年 11 月、物流業界 SIG に新たな参加組織があり、11 組織から 12 組織となった。
- 2018 年 11 月、新たに「エアポート業界 SIG」の運用を開始した。
- 2018 年 11 月、新たに「水道業界　情報連携体制」の運用を開始した。
- 2018 年 12 月、新たに「鉄鋼業界 SIG」の運用を開始した。
- 2018 年 12 月、ガス業界 SIG に新たな参加組織があり、63 組織から 64 組織となった。

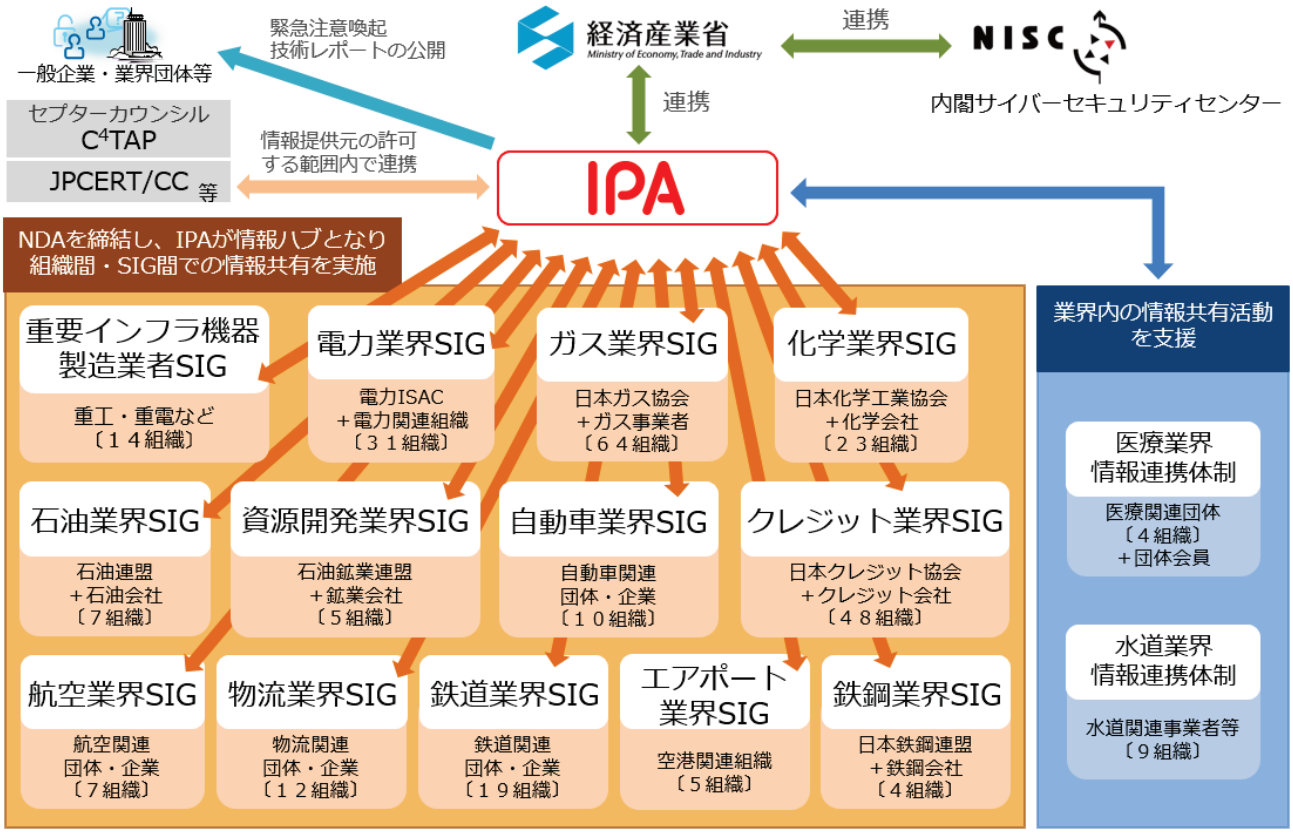

図 1 J-CSIP の体制図

[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（2018 年 10 月～12 月）

2018 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、13 の SIG、全 249 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	2018 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	256 件	191 件	519 件	**1,072 件**
2	参加組織への情報共有実施件数※1	76 件	49 件	39 件	**59 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 **12 件**を含む。

本四半期は情報提供件数が **1,072 件**であり、うち標的型攻撃メールとみなした情報は **93 件**であった。その他、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を受けた（表 2 項番 3）として、当該事案に関する合計 483 件のメール等の検体の提供があった。

標的型攻撃メールとみなした情報の主なものとして、プラント関連事業者を狙う攻撃が約 6 割（63 件）を占めている。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（産業スパイ活動）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。

さらに、本四半期でもビジネスメール詐欺が試みられたという事例を引き続き観測した。詳しくは 3 章で述べるが、本四半期では 4 件のビジネスメール詐欺について情報提供を受けている。いずれの事例でも英語のメールであるが、実際に被害を受けた事例もある。ビジネスメール詐欺は沈静化する様子がなく、注意・対策の徹底が必要である。

また、組織のメールアカウントが攻撃者によって乗っ取られ、大量のフィッシングメールがばらまかれたという事案について情報提供を受けた。これについて、4 章で述べる。

[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（続報） （IPA）
https://www.ipa.go.jp/security/announce/201808-bec.html

本四半期では、国内の正規のウェブサイトが改ざんされ、当該ウェブサイトにアクセスすると、「IPA フォント [4]」のインストールが必要であるかのように見せかけ、ウイルスがダウンロードされる事案を確認している。これについては、5 章で述べる。

本四半期に限らず、不審なメールとして日本語のウイルスメールが長期間観測され続けているが、本四半期、複数のドメインから、正規のメールへの返信としてウイルスメールがばら撒かれたという事案が発生したことを確認している。これについては、6 章で述べる。

その他、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の攻撃を確認した。	9 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。	2 件
3	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を受けた。	3 件
4	実在する外部組織を騙るウイルスメールが送られてきた。	2 件

これらは、いずれも業務に少なからず影響が発生するものである。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であり、引き続き確認されている。Office 365 を導入している組織の利用者は、自身のアカウント情報の重要度を認識し、そのアカウントを狙う攻撃があるということ、悪意のある人物にその情報を騙し取られた場合、大きな被害につながる可能性があることを認識する必要がある。

項番 2 については、前四半期から引き続き相談がある事例であり、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ある。いずれもウェブ閲覧中に、改ざんされたサイトや不正な広告等により、詐欺や偽警告を行う悪意のあるウェブサイトへ誘導されたと考えられるものであった。通常業務においても発生しうるため、攻撃の被害に遭わないよう、不審サイト・詐欺サイト・偽警告 [5]等にだまされないよう従業員への教育を行うべきである。また、PC のソフトウェアの脆弱性の悪用も考えられるため、脆弱性の対策も必須である。

項番 3 は、企業の公開ウェブサイトの問い合わせフォームに大量の投稿を行うことで、業務の妨害等を行うことが目的であるとも考えられる。これについては、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が必要であろう。

そして項番 4 については、実在する組織を騙ったウイルスメールが送り付けられたというもので、着信者が、メールに添付されていた Word 文書ファイルを開いてしまったというものである。この Word 文書ファイルからは、EMOTET[6]と呼ばれるウイルスがダウンロードされることを確認している。EMOTET は世界中で拡散されているウイルスであり、これまで日本国内にもウイルスメールが着信していることを観測している。本四半期においても、EMOTET への感染を企図するウイルスメールを複数観測しており、注意が必要である。

---

[4] IPA では、システムの種類を問わず無償で利用できる高品位なフォントである「IPA フォント」や、その改良版である「IPAex フォント」を開発・公開している。（IPA）
https://www.ipa.go.jp/osc/ipafont

[5]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

[6]流行マルウェア「EMOTET」の内部構造を紐解く（MBSD）
https://www.mbsd.jp/blog/20181225_2.html

3　ビジネスメール詐欺（BEC）複数の攻撃を確認

本四半期、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 月に IPA より注意喚起を行ったが、その後も継続して攻撃を確認しており、その勢いは衰えておらず、注意が必要な状況は今後も続くものと考えられる。

本四半期では、4 件のビジネスメール詐欺が試みられたとの情報提供を受けている。4 件の事例のうち、2 件は実際に金銭被害を受けている。今回確認しているビジネスメール詐欺の事例ではすべて英文のメールであった。本章では、このうち 1 件の事例を説明する。

3.1 事例

本事例は、2018 年 11 月、参加組織の国内関連企業（A 社）と、その海外取引先企業（B 社）で取引を行っている中で、攻撃者がB 社の担当者になりすまし、偽の振り込みを要求するメールがA 社に送られたものである。IPA が 2017 年 3 月に公開した注意喚起レポート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。

この事例では、支払い側であるA 社の担当者が偽のメールであると気づくことができたため、金銭的な被害は発生していない。

本事例では、詐欺の過程において、次の手口が使われた。

- 詐称用メールアドレスの取得と悪用
- ビジネスメールの授受に割り込み、詐欺を試みる

（1） 詐称用メールアドレスの取得と悪用

攻撃者は、B 社のメールアドレスに似通った「詐称用メールアドレス」を取得していた。詐称用メールアドレスは、次の例に示すように、本物のメールアドレスのドメインの一部（b-company）を、ローカル部に使用したフリーメールサービスのメールアドレスであった。

【本物のメールアドレス】 alice @ b-company . com
【偽物のメールアドレス】 alice . b-company @ *フリーメールのドメイン*

※実際に悪用されたものとは異なる。

また、なりすましメールの差出人（From:）には、本物のドメインのメールアドレスが設定されていたが、返信先（Reply-To:）には、上記の詐称用メールアドレスが設定されていた。この状態で返信メールを作成すると、詐称用メールアドレスが返信メールの宛先となる。

これらの手口により、攻撃者はメール受信者に、返信先が偽のメールアドレスであることに気づかせにくくし、本物のメールアドレスへの返信と誤認させる狙いがあったものと考えられる。

（2）ビジネスメールの授受に割り込み、詐欺を試みる

本事例では、A社（国内企業）とB社（海外取引先）の間でビジネスメールをやりとりしていた中に、詐称用ドメインを使って B 社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。

攻撃者から送られてきた偽のメールと同時期に、B 社の担当者から正規のメールが A 社の担当者に届き、それぞれのメールの内容に食い違いがあったことから、A 社の担当者が不審に思い、B 社担当者に電話確認を行った結果、偽のメールであると判明したため、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。

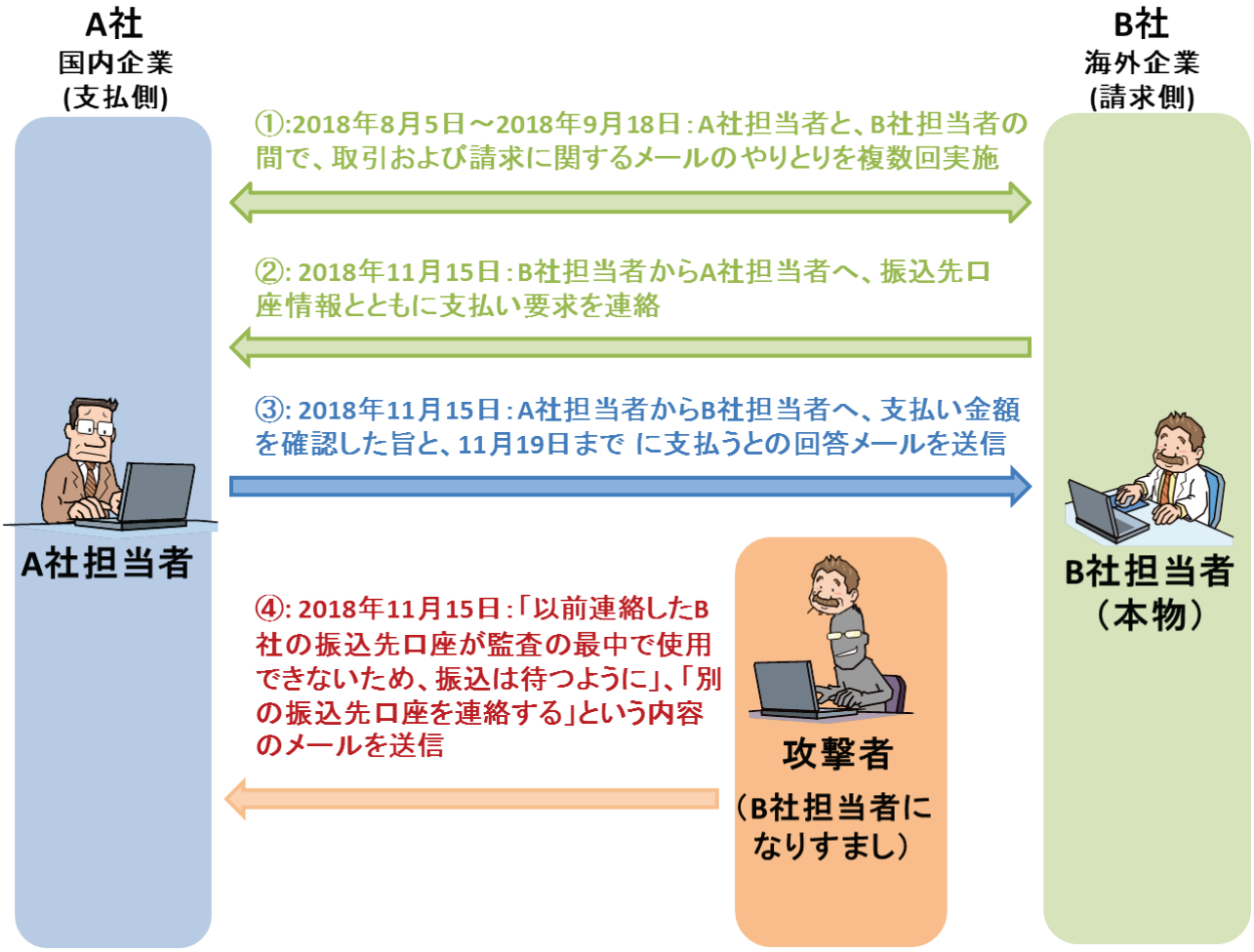

図 2 攻撃者とのやりとり

4　メールアカウントの乗っ取りによる大量スパムメール送信事例

本四半期、攻撃者によってメールアカウントが乗っ取られ、大量のフィッシングメールを送信するための踏み台にされたという情報提供があった。本事例の攻撃者の目的は、国内企業（A 社）の従業員のメールアカウントを足掛かりとして、さらに関連組織等のメールアカウントの詐取を企図したものであったと思われる。本章では、この攻撃に至る経緯を説明するとともに、実施した対策について説明する。

攻撃に至る経緯

メールアカウントの詐取：

2018 年 11 月、米国企業のメールアドレスから、A 社の従業員宛てにフィッシングメールが着信した。フィッシングの手口は、グループウェアを悪用し、アップロードされたファイルに情報を入力させるというものであった。A 社の従業員は、このフィッシングメールの内容に騙され、メールアカウントの ID とパスワードを入力し、詐取されたものと思われる。

乗っ取られたメールアカウントの悪用：

それから約 3 週間後、A 社従業員の Office 365 のメールアカウントが乗っ取られ、アドレス帳に登録されていた社内外を含むメールアドレスに対して、約 1 万通のフィッシングメールが 7 分間のうちに送信された。当該アカウントの不正アクセス元はナイジェリアであった。

送信されたフィッシングメールには Word 文書ファイル（図 3）が添付されており、「クラウドサービス上に受信者宛のメッセージがある」という内容で、メッセージを読むための URL リンクが書かれていた。リンクを開くとフィッシングサイトへ誘導される。フィッシングサイトには、文書を読むためにログインが必要であるかのように誤認させ、メールアカウントの ID とパスワードを入力させる偽の画面が設置されていた（図 4）。

また、A 社従業員のメールボックスには、自動返信を行う設定が攻撃者によって仕掛けられており[7]、当該フィッシングメールの受信者からメールが返信されてくると、自動的に「確かに送付したものなので、内容を確認してほしい」という旨のメールが返信されるようになっていたことも分かった。

A 社が実施した本件の対策

A 社では、本事案をうけ次の対策を実施した。

- Office 365 利用者全員にパスワードの変更を指示
- Office 365 の Advanced Threat Protection（ATP）[8]を適用
- Office 365 へグローバル IP アドレスでログインする場合、2 要素認証を必須とするよう設定

[7] Outlook の「仕分けルール」の機能を悪用したものと思われる。

[8] Office 365 Advanced Threat Protection サービスの説明（Microsoft）
https://technet.microsoft.com/ja-jp/library/exchange-online-advanced-threat-protection-service-description.aspx

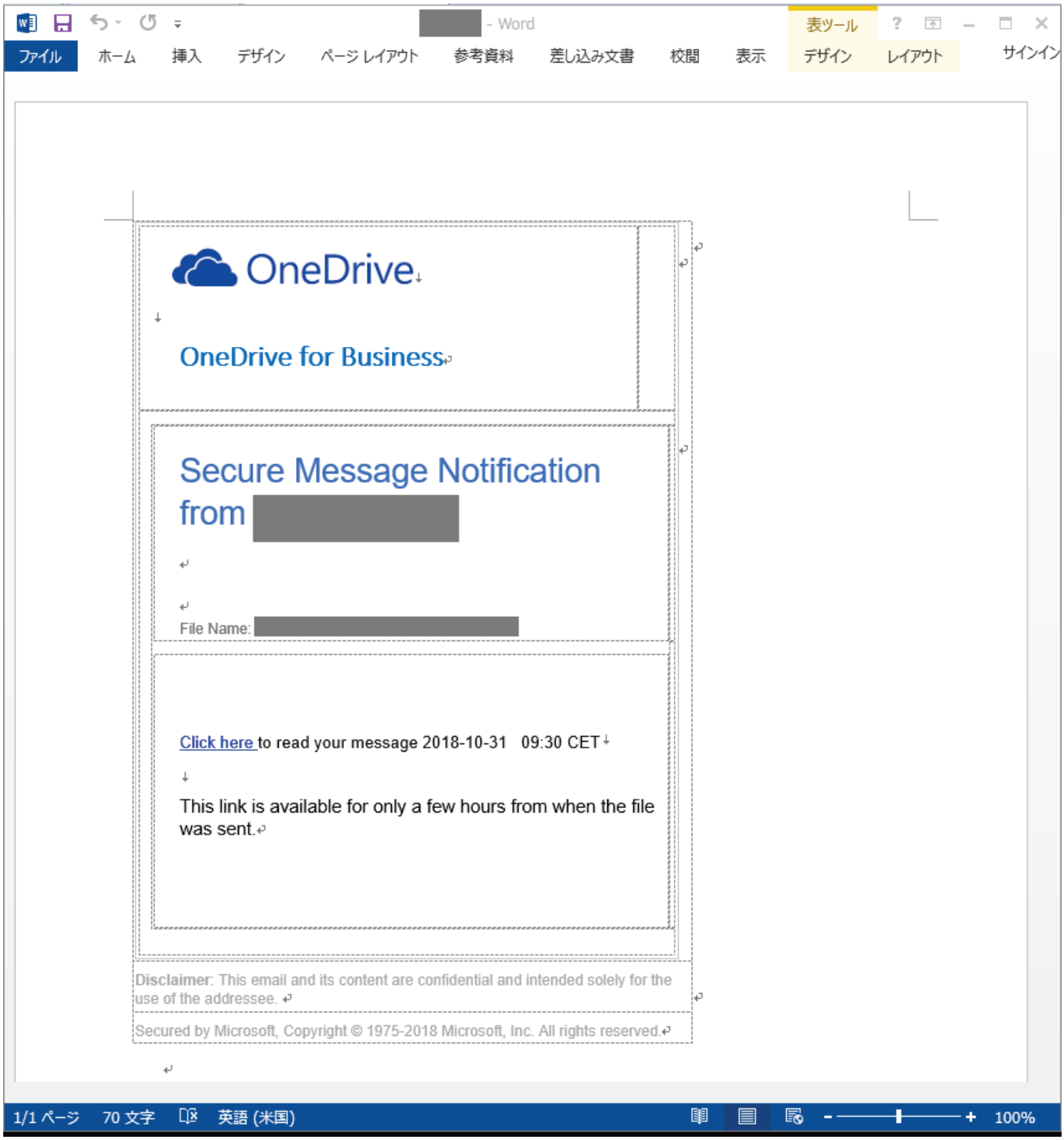

図 3 ばらまかれたフィッシングメールに添付されていた Word 文書ファイル

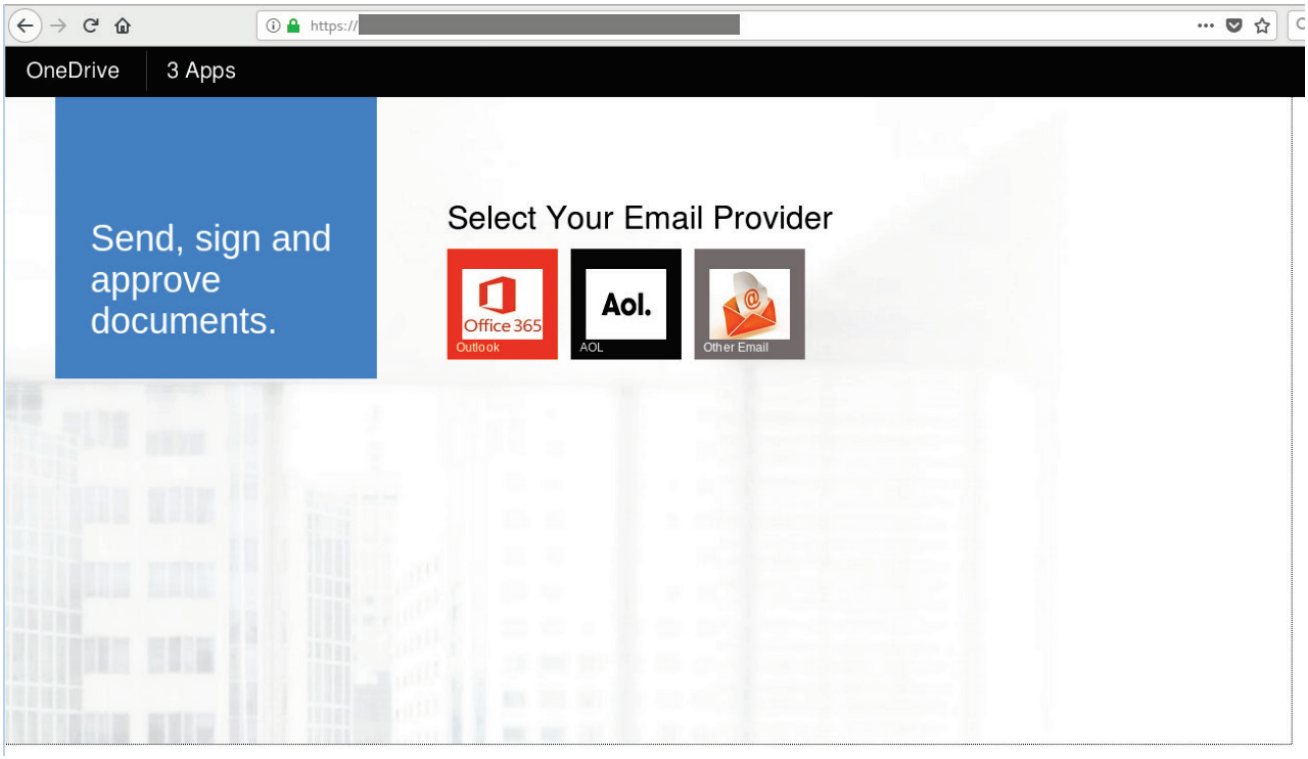

図 4 フィッシングサイトの画面

5　IPA フォントのダウンロードに見せかけた攻撃

本四半期、IPA は、国内のとある正規サイトが改ざんされ、「IPA フォントが見つからない」という偽の警告を出して、ウイルスをダウンロードさせる状態となっていた事案を確認した。改ざんされたウェブサイトにアクセスすると、「不足しているフォント」と書かれ、「IPA フォント」のインストールが必要であるかのように見せかける偽のウインドウが表示（図 5）される。このメッセージに従って「IPA フォントのダウンロード」というボタンをクリックすると、ウイルスがダウンロードされる状態であった。

ダウンロードされたファイルを開くと（ウイルスを実行すると）、PC が遠隔操作ウイルス（RAT）に感染させられてしまうことを確認した。本件が、無作為な対象へ広くウイルス感染を企図したものであるのか、攻撃対象をある程度絞ったもの（標的型とみなすべき攻撃）であったのかは不明である。

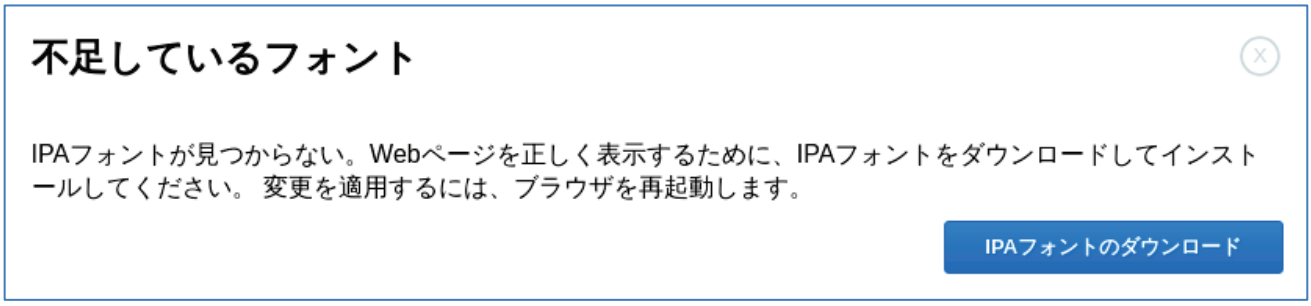

図 5 ブラウザ内に表示される偽の警告ウインドウ

本件の事例のように、利用者がウェブサイトにアクセスした際、コンテンツを表示するためにフォントデータ等のインストールが必要だと偽の警告表示を行い、ウイルスをダウンロードさせる手口は過去にも確認されている。正規サイトであっても、不用意に不審なファイルのダウンロードを行わないように注意することが必要であろう。

6　正規メールへの返信を装うウイルスメールについて

2018 年 11 月 27 日、日本国内において、複数のドメインから、正規メールへの返信としてウイルスメールがばら撒かれたという事案が発生したことを確認した。以降、同様の攻撃は観測されておらず、厳重な警戒が必要という状況ではないと考えられるが、今後も同様の攻撃が行われる可能性があることから、本章では現時点で IPA が把握できている状況、当該ウイルスメールの事例と特徴の説明、対応・対策や注意点等について説明する。

6.1 IPA が把握している状況

IPA へ情報提供等があった限りでは、少なくとも国内の計 16 のドメインから、日本時間 2018 年 11 月 27 日 5:30 頃～9:30 頃（約 4 時間）に計 25 通のウイルスメールが送信されたことを確認している。IPA へ情報提供があったのは攻撃全体のほんの一部であると考えられ、この時間帯、国内に広く同様の攻撃（アカウントの乗っ取りとウイルスメール送信）が行われた可能性がある。

ウイルスメールの受信者から、メールの送信元へ確認を行ったところ、「何者かによって、当該メールアカウントのメールの送受信履歴をもとに、複数の宛先へウイルスメールが送られた模様」との回答が複数得られた。一部のメールの配送経路を確認したところ、正規のメールサーバからの送信となっている例も確認しており、メールアカウントへ何らかの原因で不正アクセスされ、それらのアカウントが攻撃者に悪用されて[9]、短時間のうちに複数のウイルスメールが多方面に送られたと推定できる状況である（図 6）。

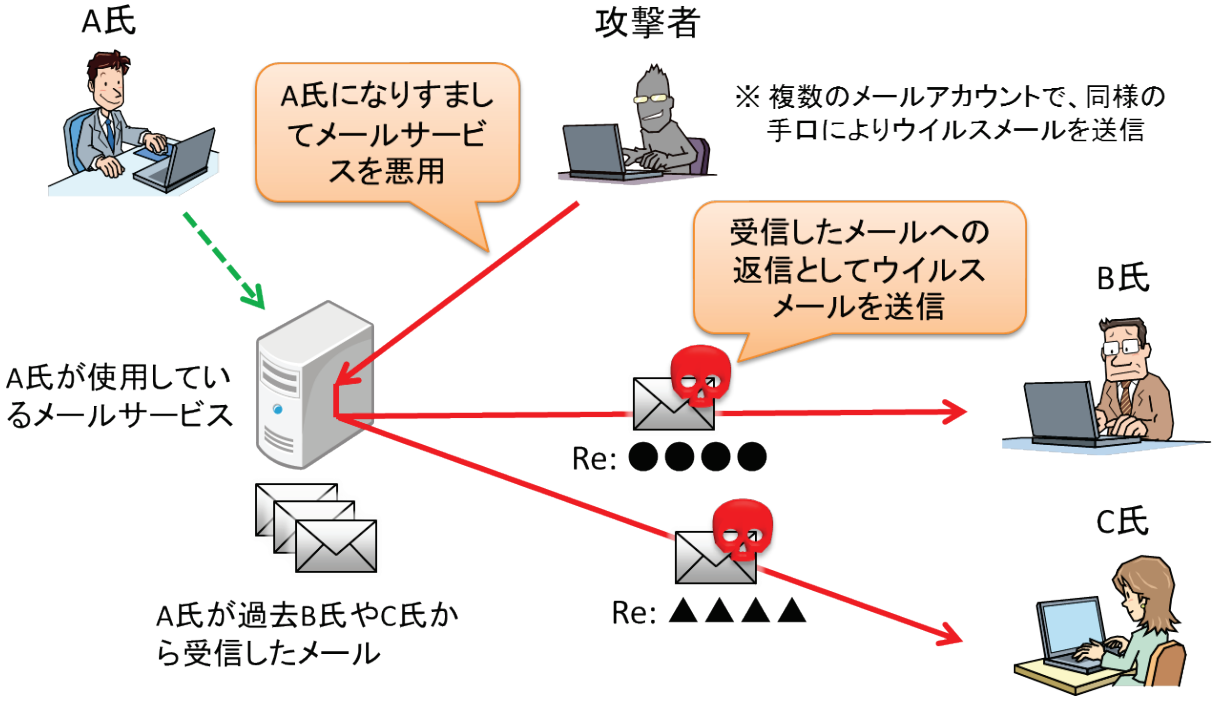

図 6 ウイルスメールが送信された状況（推定）

[9] 一方、ウイルスメールの送信元としてメールアドレスが詐称されていたにもかかわらず、不正アクセスについては身に覚えがないという事例もあるため、送信元となった全てのメールアドレスのアカウントが乗っ取りを受けたとは限らない。

6.2 事例と特徴

今回、この手口で送信されたウイルスメールについて、IPA が入手したものはほぼ全て同一の形となっており、次のような内容となっていた（図 7）。

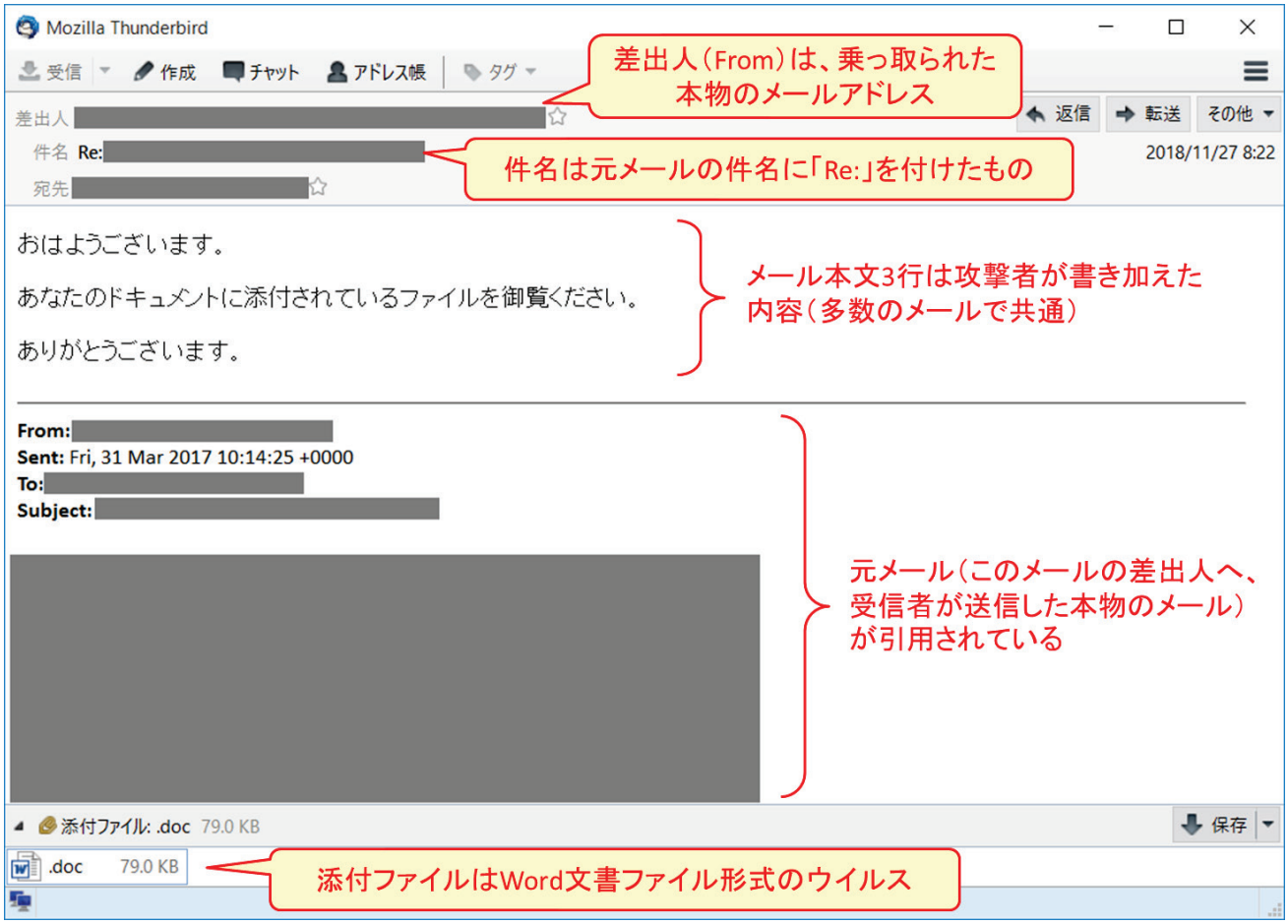

図 7 送信されたウイルスメールの例

添付ファイルは「.doc」という、拡張子のみのファイル名となっていた [10]。この状態だと、ファイルを開く際にうまく動作しない場合があり、攻撃者がミスをした可能性が考えられる。

この添付ファイルは、マクロ付き Word 文書ファイルであり、不自然な日本語で、保護ビューの解除とマクロを有効化する操作を行うよう誘導する文面が書かれている（図 8）。この誘導に従い「コンテンツの有効化」をクリックするなどしてマクロを有効にする操作をした場合、ウイルスに感染させられてしまう。

具体的には、マクロを有効にすると、不正な通信が発生し、外部からウイルスがダウンロードされ、PC へ感染させられてしまう。ダウンロードされるウイルスは、従来から国内に広く無差別に送信されている、日本語のばらまき型のウイルスメールと同等のもの（インターネットバンキング等の情報を窃取するウイルス）であった。

[10] Outlook 等、自動的に「ATTxxxx.doc」のようなファイル名を付与するメールソフトもある。

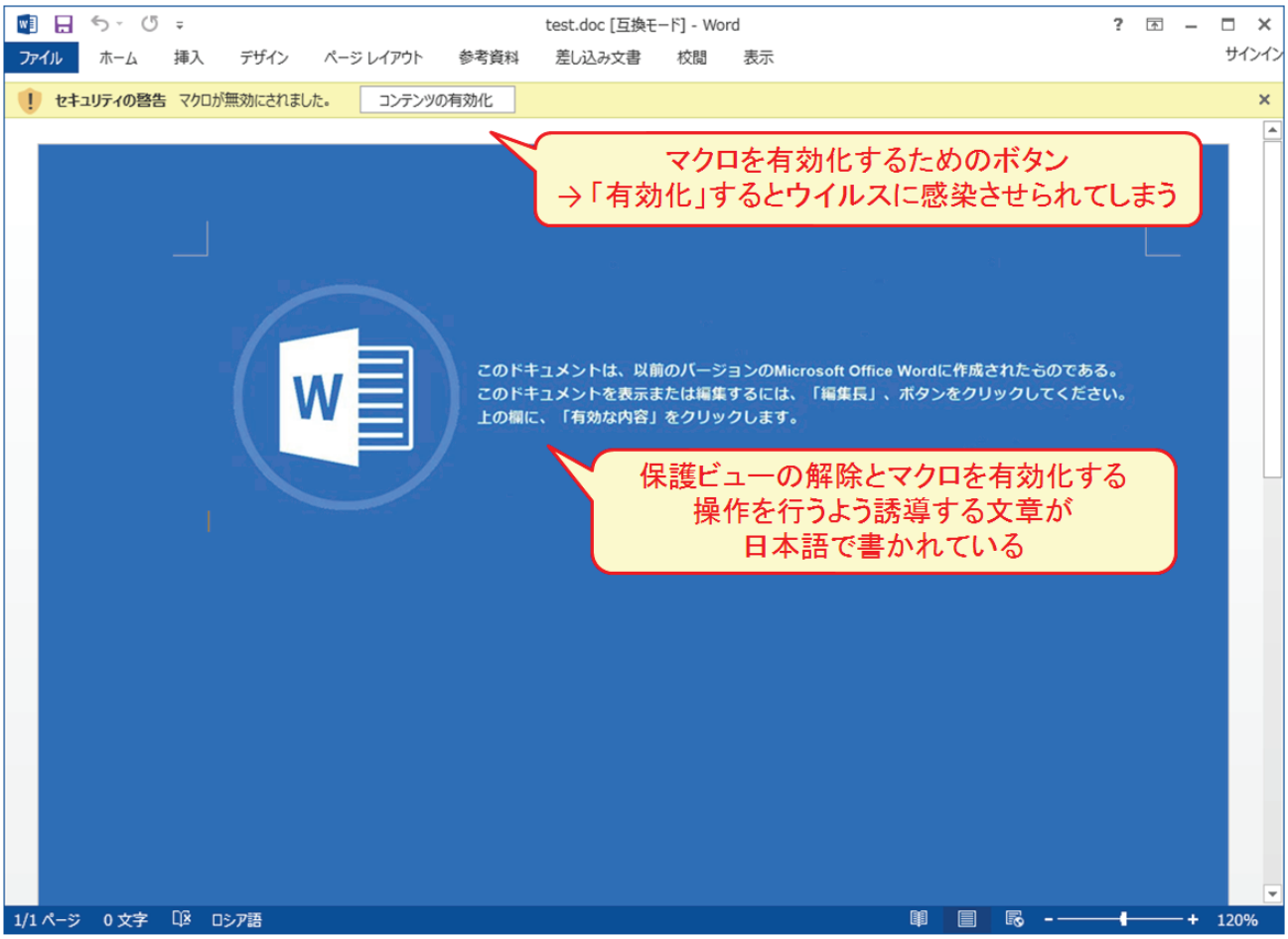

図 8 添付ファイルを開いた時の画面

6.3 まとめ

今回確認した攻撃は、過去にメールのやり取りを行ったメールアドレスから、本物のメールへの返信としてウイルスメールが送られてくる手口であった。海外では従来から同等の事例が確認されており、日本語にはまだ不自然な点があるものの、不審なメールであると見破りにくいと考えられ、注意を要する手口である。

ウイルス感染の被害に遭わないよう、基本的なウイルス対策を徹底するとともに、マクロの有効化は危険を伴うことを改めて認識する必要がある。

また、アカウントを乗っ取られ、攻撃に加担してしまうことのないよう、メールアカウントのパスワードには複雑なものを設定する、フィッシング攻撃に注意するなど、不正アクセス対策も怠らないようにすることが重要である。

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