

初版：2020年9月28日

改訂：2020年9月30日

改訂：2020年10月2日

お客様、取引先 各位

株式会社ひらまつ

法務総務部長 清松 久典

コンピューターウイルス感染発生によるお詫びとお知らせ

(続報 3)

令和2年9月23日にお知らせした表題事項について、新たに判明いたしました情報を掲載いたします。今後も新たな情報が判明いたしましたら、適時お知らせいたします。本日アップデートした部分は、青字のとおりです。

この度はお客様、お取引先各位に大変なご迷惑をおかけして誠に申し訳ございません。

【1】 ウィルスメールの特徴は次のとおりです。

(ア) 当社が送受信したメールの返信を装っています

(イ) 発信先は当社が表示されていますが、メールアドレスは当社(・・・@hiramatsu.co.jp)と異なる表示となっています。

(ウ) 添付ファイルとして、ワードファイルや他の形式のファイルが添付されています。

(エ) ウィルスメールの特徴については、情報処理推進機構 (IPA) の情報もご参照ください。

(オ) ひらまつオンラインおよびひらまつ共通食事券から送信されるメールには、添付ファイルはお付けいたしません。添付ファイルが必要な場合、別途ご確認のメールを個別に送付させていただきます。事前の確認メール無しでひらまつオンラインおよびひらまつ共通食事券から送信される添付ファイル付きのメールは、当社からのご案内ではありませんので、そのメールを削除し、ごみ箱も空にしてください。

(2020年10月2日追記)

【2】 確認できている事実

下記は現在確認できている限りの情報であり、継続して調査を進めており、新たな情報が分かり次第、ホームページ上でお知らせします。

(ア)9月21日、営業部門の従業員の会社貸与のパソコンが Emotet というウイルス

に感染して、当該従業員のパソコン内に格納されているメール情報から、ウィルスメールが社内関係者を中心に配信されています。

- (イ)9月25日、営業部門の従業員の会社貸与のパソコンが **Emotet** というウィルスに感染して、当該従業員のパソコン内に格納されているメール情報を盗取された可能性があります。また当該パソコンでは、当社オンライン販売におけるワインの受注情報を受領していたため、このメール本文内に記載された受注情報（住所、電話番号、氏名、メールアドレス）の情報も漏洩した可能性があると考えています。このウィルスの性質上、メール情報から不正メールを自動生成していますので、メール本文中の個人情報悪用することは想定しづらいところではありますが、確定的なことは申し上げられない状況となっており、大変申し訳ございません。被害の範囲や対処方法については引き続き調査を行っています。（2020年9月30日追記）
- (ウ)当該メール情報から、お客様を含む社内外関係者にウィルスメールが広範に配信されています。なお、2020年9月29日にさらに多数の不正メールが配信されていることが確認されています。不正メール対策については、「対処方法」に追記いたしました。（2020年9月30日追記）
- (エ)当該ウィルスは **Windows** パソコンには感染いたしますが、**Mac** パソコン、スマートフォンへの感染は確認できていません。
- (オ)サーバへのアクセス情報は確認できておりません。個人のパソコンの中に入っていたメール情報が流出したと考えています。
- (カ)お客様のクレジット情報等の決済情報は、当社該当パソコン内にも当社サーバ内にも記録されていないので、当社からの流出の可能性は低いと考えています。

【3】 対処方法

- (ア)添付ファイルやリンクが貼られているものが多いので、過去のメールのやりとりの内容を転用した、非常に紛らわしい内容のメールとなっています。上記のウィルスメールの特徴があるもの等、不審なメールが送信された場合、添付ファイルを実行せずそのまま削除して、ごみ箱も空にしてください。
- (イ)仮に添付ファイルを実行してしまったら、ウィルス対策ソフトでウィルス検査を実行してください。

また、一般社団法人 **JPCERT** コーディネーションセンターより、**Emotet** 感染有無の確認を行うツール「**EmoCheck**」が配布されていますので、ご案内させていただきます。**Emotet** は一般のウィルス対策ソフトでは検知されないケースがございますので、「**EmoCheck**」のご利用もご検討ください。

「**EmoCheck**」の詳細に関しては下記リンクの項番2「**2. Emotet** の感染有無を確認するためにはどうすればよいですか？」をご確認ください。

マルウェア Emotet への対応 FAQ(JPCERT)

<https://blogs.jpCERT.or.jp/ja/2019/12/emotetfaq.html>

※Emotet の亜種が最新の定義ファイルに対応していない場合もある為、翌日もしくは数日後に定義ファイルが更新された状態で、再度ウイルスチェックを行う事をおすすめします。

(ウ) ウィルス感染が確認された場合、下記お問い合わせ窓口までご連絡ください。

(エ) 「Emotet」と呼ばれるウィルス感染を狙うメールについてはこちらをご参照ください。

情報処理推進機構<IPA>

<https://www.ipa.go.jp/security/announce/20191202.html>

(オ) 不正メールがお客様、取引先各位にも多数送信される事実が確認されています。

メールプロバイダの迷惑メールフィルタリングサービスの活用もご検討いただけましたら幸いです。当社で確認したところ、不正メールはフィルタリングサービスで大部分がブロックされています。

一方で、本来は正当なメールが迷惑メールと判断されて、受信できないこともございます。

主なメールプロバイダのフィルタリングサービスは次のサイトをご覧ください。

(1) Yahoo!メール

<https://mail.yahoo.co.jp/antispam/tools.html>

(2) Gmail

<https://support.google.com/mail/answer/8151?co=GENIE.Platform%3DDesktop&hl=ja>

(3) OCN

<https://support.ntt.com/ocn/support/pid2900000s5y>

(4) Biglobe

<https://email.biglobe.ne.jp/spam/>

(5) So-net

<https://www.so-net.ne.jp/option/security/meiwaku/>

(6) Yahoo!BB

<https://mail.yahoo.co.jp/antispam/tools.html>

(7) Plala

<https://www.plala.or.jp/option/antispam/>

(8) eo 光

- <https://eonet.jp/option/mail/reject/>
- (9) au one net
<https://www.au.com/internet/service/auonenet/mail-homepage/mail-filter/>
- (10) @nifty
<https://mail.nifty.com/info/antispam/index.htm>
- (11) TNC
<https://www.tnc.ne.jp/mail/spam/>
- (12) AsahiNet
<https://asahi-net.jp/service/option/security/spamblock/>
- (13) hi-ho
<https://hi-ho.jp/service/mail/kmmf/>
- (14) IC-net
<https://www.ic-net.or.jp/member/option>
- (15) Rakuten ブロードバンド
https://broadband.rakuten.co.jp/option/advanced_spam_filter.html
- (16) DTI
<https://www-wp.dream.jp/search.php/?p=4306>
- (17) イッツコム
<https://www.itscom.co.jp/support/security/antispam/>
- (18) JCOM
<https://cs.myjcom.jp/knowledgeDetail?an=000477677>
- (19) NTT ドコモ
https://www.nttdocomo.co.jp/info/spam_mail/
- (20) au
<https://www.au.com/support/service/mobile/trouble/mail/email/filter/>
- (21) ソフトバンクモバイル
<https://www.softbank.jp/mobile/support/mail/antispam/spammailfilter/>

(2020年9月30日追記)

(カ) 不正メールはウイルスを自動的に配信するものですから、メールプロバイダ様のウイルススキャンの設定をしていただくとブロックされることがあります。

(各社仕様が異なります)

当社の調査でも、ほとんどの不正メールが迷惑フォルダに格納されています。ウイルススキャンサービスは一部有料の場合があります。

しかしながら、ウイルスには亜種が多数ありますので、一部ウイルススキャンをかいくぐって配信されるものもございます。

主なメールプロバイダのフィルタリングサービスは次のサイトをご覧ください。

- (1) Yahoo!メール
<https://support.yahoo-net.jp/PccMail/s/article/H000007384>
- (2) Gmail
<https://support.google.com/mail/answer/25760?hl=ja>
- (3) OCN
<https://www.ntt.com/personal/services/option/mail/vcheck-mail.html>
- (4) Biglobe
<https://email.biglobe.ne.jp/vcheck/service.html>
- (5) So-net
<https://www.so-net.ne.jp/option/mail/vchk/>
- (6) Yahoo!BB
<https://support.yahoo-net.jp/PccMail/s/article/H000007384>
- (7) Plala
<https://www.plala.or.jp/option/vcheck/>
- (8) eo 光
<https://eonet.jp/option/mail/spamcheck/>
- (9) au one net
<https://www.au.com/internet/service/auonenet/mail-homepage/anti-virus-receive/>
- (10) @nifty
<https://mail.nifty.com/info/virusbuster/>
- (11) TNC
<https://www.tnc.ne.jp/tos/>
- (12) AsahiNet
<https://asahi-net.jp/service/option/security/viruscheck/>
- (13) hi-ho
<https://hi-ho.jp/service/mail/vcheck/>
- (14) IC-net
<https://www.ic-net.or.jp/member/option>
- (15) Rakuten ブロードバンド
https://broadband.rakuten.co.jp/option/virus_filter.html
- (16) DTI
<https://dream.jp/mail/option/vcheck.html>
- (17) イッツコム

<https://www.itscom.co.jp/support/security/viruscheck/>

(18) JCOM

<https://www.jcom.co.jp/service/net/security.html>

(19) NTT ドコモ

https://www.nttdocomo.co.jp/service/anshin_security/

(20) au

<https://www.au.com/internet/service/auonenet/mail-homepage/anti-virus-receive/>

㊴ ソフトバンクモバイル

<https://www.softbank.jp/mobile/service/smartsecurity/>

(2020年10月2日追記)

(キ) ひらまつオンラインにつきましては、セキュリティ対策が構築できるまで休止とさせていただきますが、対策の目途が立ちましたので、ソフトウェアの改修を行い、今月中旬には再開の見込みです。詳細はホームページ等で公開させていただきます。

(2020年10月2日追記)

【4】 本件については、お問い合わせ窓口を設定いたしました。不明点がございましたら、下記お問い合わせ窓口までご連絡賜りたく、よろしくお願いいたします。

以上

<本件に関するお問い合わせ窓口>

株式会社ひらまつ 総務部

TEL03-5793-8811 (平日 9:00 ~ 18:00)

電子メール privacy@hiramatsu.co.jp