LATEST & PICKUP!
SECURITY NEWS

Fuva Brain
Vol.48

最新個人情報漏洩事件・関連ニュース

LATEST

DATE：2022.07.19
サイバーセキュリティ.com　SecurityNEXT、jiji.com、Yahoo!NEWS

- 07月13日：カタログギフト販売サイトに不正アクセス　**最大2万8700件のクレカ情報、最大15万236件の個人情報が漏えいか**
- 07月13日：不動産取り扱いショウインホームで**Emotet感染**、不審メールの送信を確認
- 07月13日：販促物問合せフォームの**メール本文を流用した迷惑メール**の送信を確認　濵田酒造株式会社
- 07月13日：サンドラッグ2サイトにリスト型攻撃、19,057件の不正ログインか
- 07月13日：名古屋商工会議所で**システムサーバー暗号化**、情報流出は確認されず
- 07月12日：新潟県立高校2校で**「高野連」を名乗ったなりすましメール、添付ファイル開封しEmotet感染**
- 07月12日：不動産取り扱いショウインホームで**Emotet感染**、不審メールの送信を確認
- 07月12日：インフィニット社ECがサイバー攻撃被害、**カードや会員情報流出懸念**
- 07月11日：杏林大学医学部付属病院、患者27名のUSBメモリ紛失
- 07月11日：室蘭工業大学で**Emotetと推測されるウイルスに感染**、メールサーバから不審メールを送信
- 07月11日：京都で不動産業を行う長栄のサーバに不正アクセス、情報流出の痕跡は確認されず
- 07月08日：過去のやり取りを模倣し**Emotet感染狙う不審メール送信**放電精密加工研究所
- 07月08日：旧PATRICKオンラインショップがサイバー被害、**5,172名のカード情報流出**か
- 07月08日：キンコーズのサーバに不正アクセス、**名刺や年賀状等の印 字内容が流出**した可能性
- 07月07日：人形の松永、サイバー攻撃被害で**カード情報や会員情報流出懸念**
- 07月07日：読売新聞オンラインがサイバー被害、期間中3万件のアクセス確認
- 07月06日：安江病院、不正アクセスにより**最大11万件以上の個人情報流出**の可能性
- 07月06日：NTTデータ関西が**Emotet感染**、自治体等向けの電子申請サービス問い合わせメールが流出

PICKUP!

Emotet、海外と比べて日本の検知率高い、引き続き警戒を

- 出典：2022年7月12日 JPCERT/CC　2022年4月から6月を振り返って　https://www.jpcert.or.jp/newsflash/2022071201.html

JPCERT/CC　2022年4月から6月を振り返って（2022年7月12日 注意喚起）

マルウェアEmotetの感染再拡大に関する注意喚起

- 直近3カ月においてもマルウェア「Emotet」の感染再拡大が特に注目すべきトピックに挙げられる。
- ブラウザ認証情報窃取機能が追加され、Chromeのクレカ情報が標的になっている。
- ショートカットファイル（LNKファイル）を含んだパスワード付きZipファイルを添付するなど、WordやExcelを使用せずに感染に至らせる新たな手口が広がる。

引き続き、不審なメールの添付ファイルやリンクは開かぬようご注意ください。

https://www.jpcert.or.jp/newsflash/2022071201.html

その他、2022年4月から6月にかけて確認された影響範囲の広い脆弱性情報や脅威情報などがまとめられております。

Emotet引き続き警戒、JPCERT/CC　EmoCheck2.3.2で感染チェックを

PICKUP!

- 出典：2022年5月27日 JPCERT/CC　https://www.jpcert.or.jp/at/2022/at220006.html

マルウェア「Emotet」に新機能
JPCERT/CCが注意喚起
感染チェックツールをアップデート

動作確認環境

- Windows 11 21H2 64bit 日本語版
- Windows 10 21H2 64bit 日本語版
- Windows 8.1 64bit 日本語版
- ~~Windows 7 SP1 32bit 日本語版~~
- ~~Windows 7 SP1 64bit 日本語版~~

図　「Emotet」v2.3.2

参考情報

JPCERT/CC 提供

感染チェックツール「EmoCheck2.3.2」

JPCERTCC/EmoCheck - GitHub

https://github.com/JPCERTCC/EmoCheck/releases

EmoCheckの使用方法や更新履歴など

https://github.com/JPCERTCC/EmoCheck/blob/master/README_ja.md

マルウェアEmotetの感染再拡大に関する注意喚起

Emotetに関する最新動向

https://www.jpcert.or.jp/at/2022/at220006.html

マルウエアEmotetへの対応FAQ

Emotetに関する情報、対応を確認

https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

解説動画
社内周知
注意喚起に

JPCERT/CC 提供

日本中で感染が広がるマルウェアEMOTET

JPCERTCC/Emotetの解説動画

https://youtu.be/wvu9sWiB2_U

EMOTET感染の確認方法と対策

JPCERTCC/Emotetの感染確認方法と対策解説動画

https://youtu.be/nqxikr1x2ag

フィッシングURL件数が過去最多の前月を大幅更新

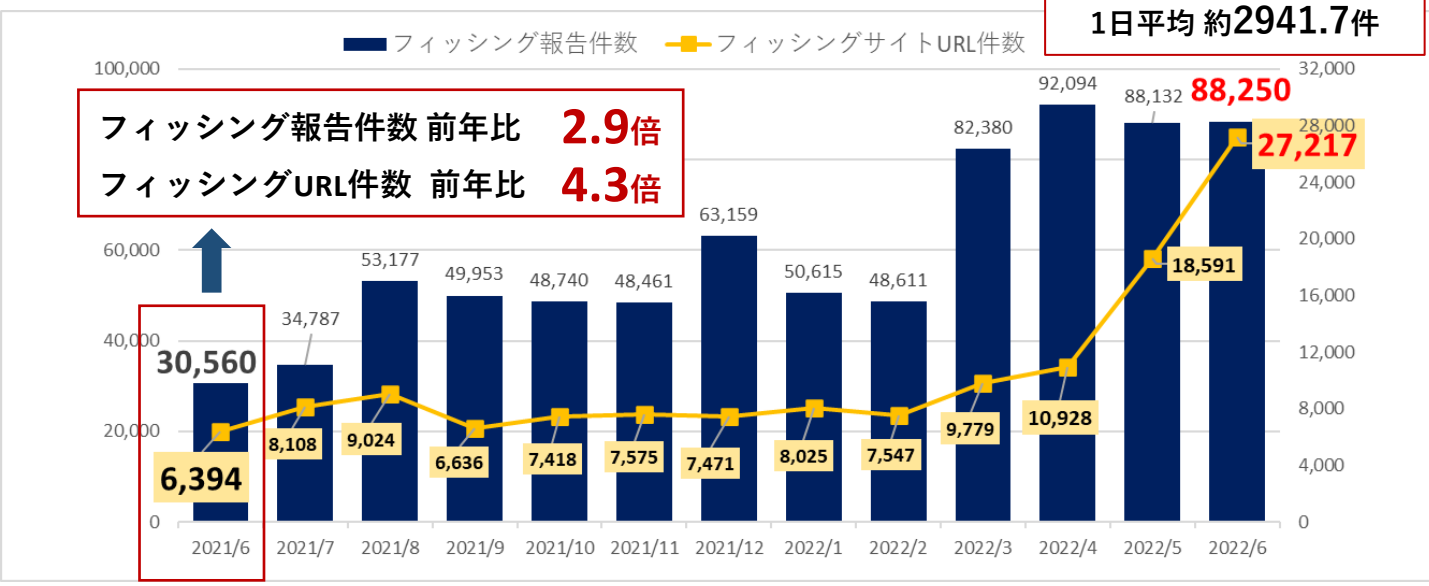
PICKUP!

- 出典：2022年7月5日 フィッシング対策協議会　2022/06 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/202206.html

フィッシングサイトのURL件数が前月の約1.7倍、過去最多を大幅更新。フィッシングメールに注意！

フィッシング攻撃の報告件数は、高い水準で横ばいも前月よりも118件増加し、88,250件。
フィッシングサイトのURL件数は、過去最多だった前月を大幅に更新して27,217件だった。
大量のドメインとサブドメインでURLを生成し、文面を使い回しつつ、ブランド名を変えたフィッシングメールで誘導する手口が横行しています。

フィッシング攻撃の報告
1日平均 約2941.7件

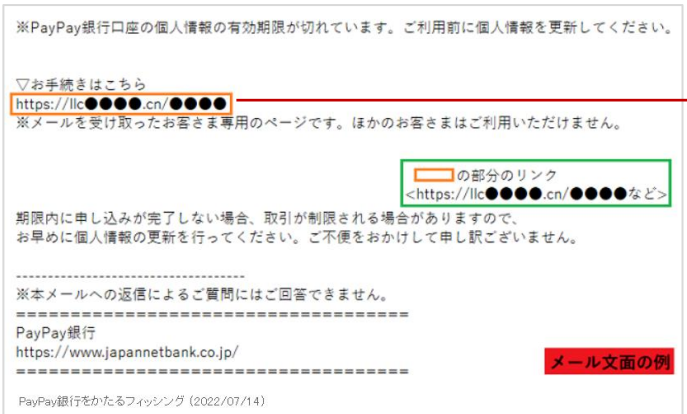


フィッシングサイトにご注意ください。

2022年07月14日 ETC 利用照会サービスかたるフィッシング
2022年07月14日 PayPay銀行をかたるフィッシング
2022年07月07日 セゾンNetアンサーをかたるフィッシング
2022年07月06日 日本郵便をかたるフィッシング
2022年07月05日 DMM をかたるフィッシング

2022.07.14 PayPay銀行をかたるフィッシング

メール件名「個人情報の更新専用URLのご案内」
※上記以外の件名も使われている可能性があります。



「個人情報の更新専用URLのご案内」といった件名のフィッシングメールが出回っています。メールの本文では「個人情報の有効期限が切れている」などと説明文が記載されており、偽サイトへ誘導。口座情報やログインパスワードなどを騙し取る手口です。

「Windows 8.1」のサポート終了まで約半年

PICKUP!

- 出典：2022年7月8日 IPA　Windows 8.1 のサポート終了に伴う注意喚起　https://www.ipa.go.jp/security/announce/win8_1_eos.html

Windows 8.1 のサポート終了に伴う注意喚起

2023 年 1 月に Microsoft 社が提供している OS である Windows 8.1 のサポートが終了します。また、同社が提供する Windows 7、Windows Server 2008、Windows Server 2008 R2 のサポート終了から 3 年が経過し、拡張セキュリティ更新プログラム（ESU）のサポートも終了します。

対象 OS を使用しているユーザは、速やかな最新版への移行等の実施が求められます。

対象OS　2023 年 1 月 10 日（米国時間）

- Windows 8.1
- Windows 7 ESU
- Windows Server 2008 ESU
- Windows Server 2008 R2 ESU

Microsoft　2023 年にサポートが終了する製品 （2022年4月1日）

https://docs.microsoft.com/ja-jp/lifecycle/end-of-support/end-of-support-2023

サポート終了が、なぜ、危険？　そのまま使っていてはダメなのか？

一般的にサポート終了後は新たな脆弱性が発見されても、製品ベンダによる修正が行われません。よって、**脆弱性を悪用した攻撃による情報漏えいや意図しないサービス停止等の被害を受ける可能性が高く**なります。

深刻度の高いレベル III の脆弱性のうち、CVE-2021-34527（PrintNightmare）、CVE-2021-34448、CVE-2021-33771、CVE-2021-31979 等については、悪用の事実が確認されており、**特に CVE-2021-34527 はランサムウェアに感染させることを目的として悪用された事例が確認されています。**

IPA　Windows 8.1 のサポート終了に伴う注意喚起 （2022年7月8日）

https://www.ipa.go.jp/security/announce/win8_1_eos.html

IPA　Microsoft Windows 製品の Windows Print Spooler の脆弱性対策について（CVE-2021-34527）

https://www.ipa.go.jp/security/ciadr/vul/20210705-ms.html

IPA　Microsoft 製品の脆弱性対策について（2021年7月）

https://www.ipa.go.jp/security/ciadr/vul/20210714-ms.html