

最新個人情報漏えい事件・関連ニュース

DATE : 2022.11.16

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

- 11月16日：Twitterアカウント狙うフィッシング攻撃が増加 - 「Twitter Blue」に便乗
- 11月15日：請求案内に見せかけた「So-net」を装うフィッシング
- 11月15日：外部指摘で4年以上前の不正アクセスが判明 - 出版社
- 11月15日：ETC 利用照会サービスをかたるフィッシング
- 11月14日：通信事業者がサイバー攻撃被害、出演者など7,000名の情報流出か
- 11月11日：漁協直売店で「なりすましメール」 - 8月の「Emotet」感染が原因か
- 11月11日：金融保険事業者の海外グループ、サイバー攻撃で暗号化被害
- 11月11日：米子会社に不正アクセス、個人情報流出の可能性 - 化学製造会社
- 11月11日：サイトが改ざん被害、送受信メールも流出の可能性 - システム開発事業者
- 11月11日：サービス業会社、サーバーにランサムウェア攻撃、情報流出の可能性
- 11月10日：団体、不正アクセス受け全会員情報流出の可能性
- 11月10日：楽天市場および楽天カードをかたるフィッシングに注意
- 11月09日：給食提供施設、ランサムウェア攻撃、給食提供時間に遅れ発生
- 11月09日：電気機器メーカー、不正アクセス、原因や漏えい有無を調査中
- 11月08日：「ゆうちょ銀」装うフィッシングに注意 - 20種類以上の件名バリエーション
- 11月04日：酒類小売事業者へ不正アクセス、ネットショッピングでカード情報漏えい
- 11月04日：健康食品取扱事業者のネットショッピングで不正アクセス、カード情報漏えい
- 11月04日：自治体にランサムウェア攻撃、マイナンバー含む個人情報流出の可能性
- 11月04日：医療機関、ランサムウェア攻撃で電子カルテに障害、通常診療行えず
- 11月01日：医療機関、ランサムウェア攻撃で電子カルテ使えず



一定の停止期間を経て、Emotetの活動再開を観測、警戒を

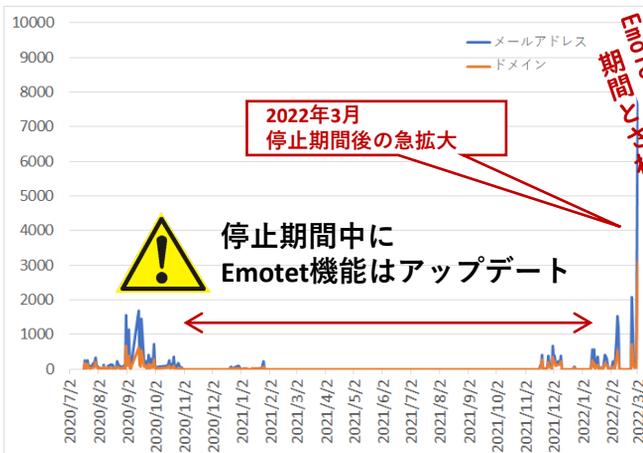
PICKUP!

出展：JPCERT/CC、NICT Blog



マルウェアEmotetの活動再開を観測！ 巧妙に「コンテンツの有効化」を促す新しい手口に注意

観測期間 2020年7月～2022年3月



出典：JPCERT/CC Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移 (外部からの提供観測情報)

Emotetメールの配信時間帯の傾向



図2. Emotetメールの配信時間帯 (JST)

2021年12月-2022年2月の急拡大の際の特徴として、Emotetの配信日も平日に集中しており、日本のワーキングタイムを狙ったような配信傾向は以前のEmotetメールでは観測されなかった傾向です。

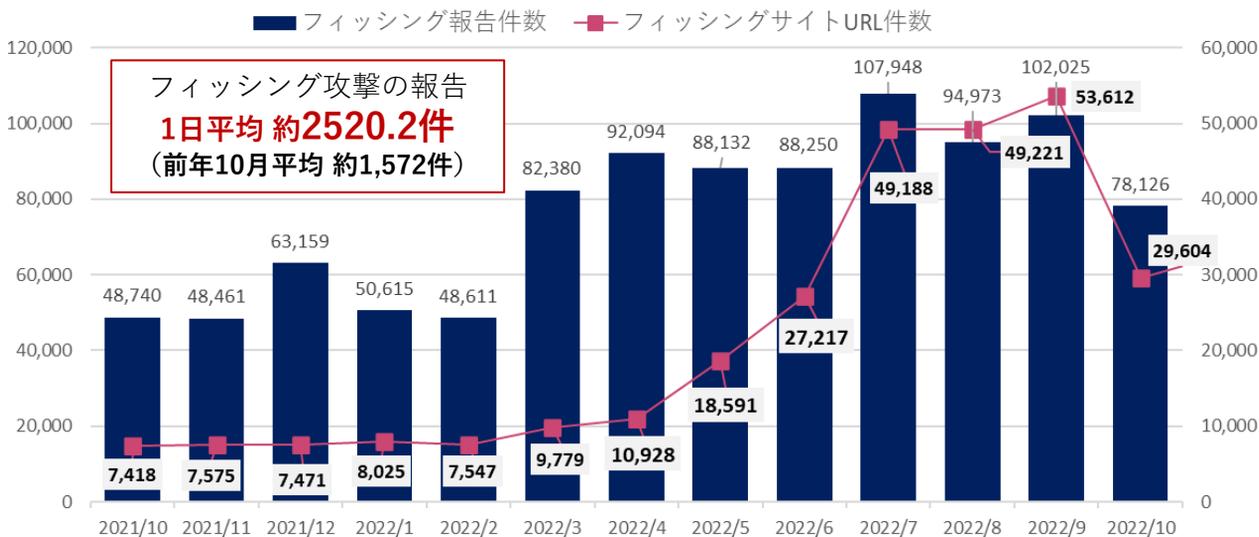
出典：NICTに届いたEmotetへの感染を狙ったメール (2021年12月～2022年2月)



フィッシング報告件数、URL件数ともに大幅に減少も 11月に入り報告、注意喚起が続く、引き続き警戒

10月にフィッシング対策協議会へ報告されたフィッシングサイトのURL件数が大幅に減少し、4か月ぶりに3万件を下回る。報告件数も8か月ぶりに8万件を下回った。

出典：フィッシング対策協議会 フィッシング報告件数 アーカイブ
当該ページを参考にフーバープレインが作成
<https://www.antiphishing.jp/news/info/>



フィッシング攻撃の報告
1日平均約2520.2件
(前年10月平均約1,572件)

フィッシングサイトにご注意ください。



フィッシング対策協議会 緊急情報 掲載一覧

- 2022年11月15日 ETC 利用照会サービスをかたるフィッシング
- 2022年11月15日 So-net をかたるフィッシング
- 2022年11月10日 楽天市場および楽天カードをかたるフィッシング
- 2022年11月08日 ゆうちょ銀行をかたるフィッシング
- 2022年11月04日 ソニー銀行をかたるフィッシング

フィッシング対策協議会は11月4日、「フィッシング対策セミナー2022」を開催

講演 警察庁が解説する フィッシング詐欺の事例と対策

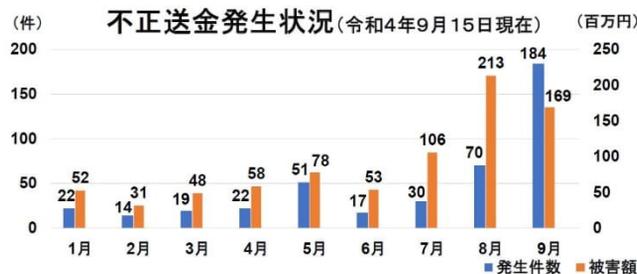
講師 警察庁の中嶋昌幸氏

インターネットバンキングを通じ、口座のお金を勝手に引き出される被害が、9月1日からの15日間で今年上半期(1~6月)を上回る184件に上ったことが警察庁の調べでわかった。大半は金融機関を装うメールでIDやパスワードを抜き取る「フィッシング」の手口とみられ、警察庁が注意を呼びかけている。

出典：フィッシング対策協議会
警察庁が解説するフィッシング詐欺の事例と対策、民間企業には「DMARC」での対応と被害相談・報告をお願い
https://www.antiphishing.jp/news/entry/20221115_impress_watch.html

インターネットバンキング被害再増加

令和4年8月、9月に発生件数・被害額が急増



- 銀行を装ったフィッシングメールを多数確認
- 9月22日、注意喚起を実施

出典 警察庁「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について」

インターネットバンキングのフィッシング被害は一時期鎮静化したが、2022年8月から急増。8月から金融機関をかたるフィッシングメールが増えたためだという



企業・団体等のランサムウェア被害が大幅増加 医療機関へも注意喚起なされる

大阪急性期・総合医療センターへのサイバー攻撃、 復旧めど立たず 政府が専門家派遣

10月末から11月に入って医療機関におけるランサムウェア感染が連続して各メディアで取り沙汰されています。先日の大阪急性期・総合医療センターにおける記者会見では、政府が派遣した専門チームの調査結果を含めて報告されています。



”典型的なサプライチェーン攻撃、給食委託業者のサーバーを通じてシステムに侵入”

”給食委託業者のVPN機器の脆弱性を悪用した侵入”

”侵入以後は、ウイルス対策機能などが無効化された形跡を確認”

”医療センターの影響を受けた端末、サーバー約1300台、完全復旧は2023年1月の見込み”

直近であった各医療機関のサイバー攻撃の侵入もVPN機器の脆弱性を悪用した侵入で、インターネット接続された委託業者からのサプライチェーン攻撃も共通してリスクが高くなっています。これらを踏まえて、11月10日、厚生労働省によって医療機関に向けた注意喚起がなされました。

厚生労働省 医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）

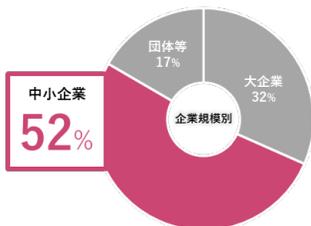
<https://www.mhlw.go.jp/content/10808000/001011666.pdf>

ランサムウェアの動向

出典：警察庁令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について
当該資料を参考にフーバーブレインが作成

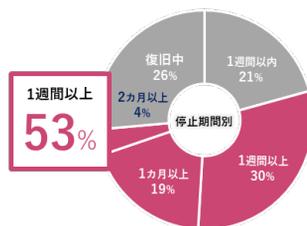
国内企業のランサムウェア被害

中小企業のリスクが高い



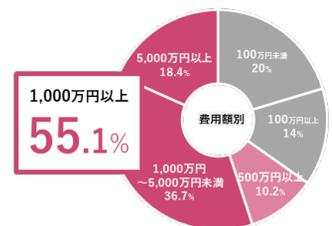
復旧にかかった時間

突然の業務停止による影響は？



調査・復旧費用の総額

金銭的な負担額も大きい



暗号化による
データ消失
顧客情報
請求情報
...

感染被害の企業
業務への影響
があったと回答 **95%**

医療機関だけでなく国内でもランサムウェアの被害が増えており、注意が必要です。

警察庁による2022年上半期のランサムウェアの被害数は前年の同じ時期と比べておよそ2倍。その侵入経路は8割がVPN機器の脆弱性を悪用した侵入です。

出典：11月4日、フィッシング対策協議会開催の「フィッシング対策セミナー 2022」
警察庁の中嶋昌幸氏（サイバー警察局サイバー企画課官民連携推進室長）による講演