LATEST & PICKUP!
SECURITY NEWS
Fuva Brain
Vol.50

## 最新個人情報漏えい事件・関連ニュース

LATEST

DATE：2022.10.13
サイバーセキュリティ.com　SecurityNEXT、jiji.com、Yahoo!NEWS

- 10月13日：自治体、メールサーバーの情報流出でスパム踏み台に、8万1084件の迷惑メール
- 10月13日：私立大学、学生62名の延納申請情報を誤送信
- 10月13日：運輸・倉庫業、サーバー2台に不正アクセス、一部ファイルが暗号化被害
- 10月13日：自治体、市民549名の保険情報や口座情報記録のUSBメモリ紛失
- 10月12日：自治体、庁舎内移動中に48名の個人情報記録のUSBメモリ紛失
- 10月12日：アパレルメーカーへの不正アクセスで個人情報流出、犯人からの恐喝メールも確認
- 10月12日：電子製造業で個人情報3,000件記録のパソコン紛失、リモート追跡も未発見
- 10月11日：自動車メーカー、コネクティッドサービスの登録情報29万件超が漏えいの可能性を発表
- 10月11日：団体、委託先誤送信で大会参加者2,388名のアドレス流出
- 10月11日：金属加工業、システム脆弱性原因でカード情報317件が流出可能性
- 10月07日：建築業、不正アクセスで個人情報流出の可能性
- 10月07日：元従業員不正アクセスで社内ファイル数万点を削除か
- 10月06日：自治体委託先、ダブルチェックするも新型コロナ診断結果メールを誤送信
- 10月06日：ITソフトウェアサービス業、管理者向け機能不具合で団体会員約11万件を誤表示
- 10月03日：電力小売事業、ファイルサーバーがランサムウェア感染、情報流出の可能性
- 09月28日：画材・文房具取り扱いオンラインショップに不正アクセス、最大186,704件のメールアドレスが漏えい
- 09月26日：デジタル庁「Gビズ ID」のメール中継サーバーに不正アクセス、約13,000件の迷惑メールを送信


## IPA　ビジネスメール詐欺（BEC）対策特設ページを開設

PICKUP!

出展：IPA ビジネスメール詐欺（BEC）対策特設ページ
https://www.ipa.go.jp/security/bec/index.html

### 各種認証情報やメールアドレスの情報窃取などの被害へ 巧妙なビジネスメール詐欺にご注意ください。

ビジネスメール詐欺（Business E-mail Compromise：BEC）とは、メールアカウントを乗っ取ったり、メールの持ち主になりすまして情報やお金を盗み取る詐欺行為です。

#### 基本的な対策

- ウイルス対策ソフトやOSを最新の状態に保つ。
- 添付ファイルやリンク先を不用意に開かない。
- 脅威や手口を組織内で情報共有する。
- IDやパスワードの使いまわしをしない、推測されにくいパスワードを使う。
- 受け取ったメールが正しいものかを注意深く確認する。


**参考情報**

IPA 提供
ビジネスメール詐欺（BEC）対策特設ページ
https://www.ipa.go.jp/security/bec/index.html

# フィッシング急増！報告件数10万件を超える

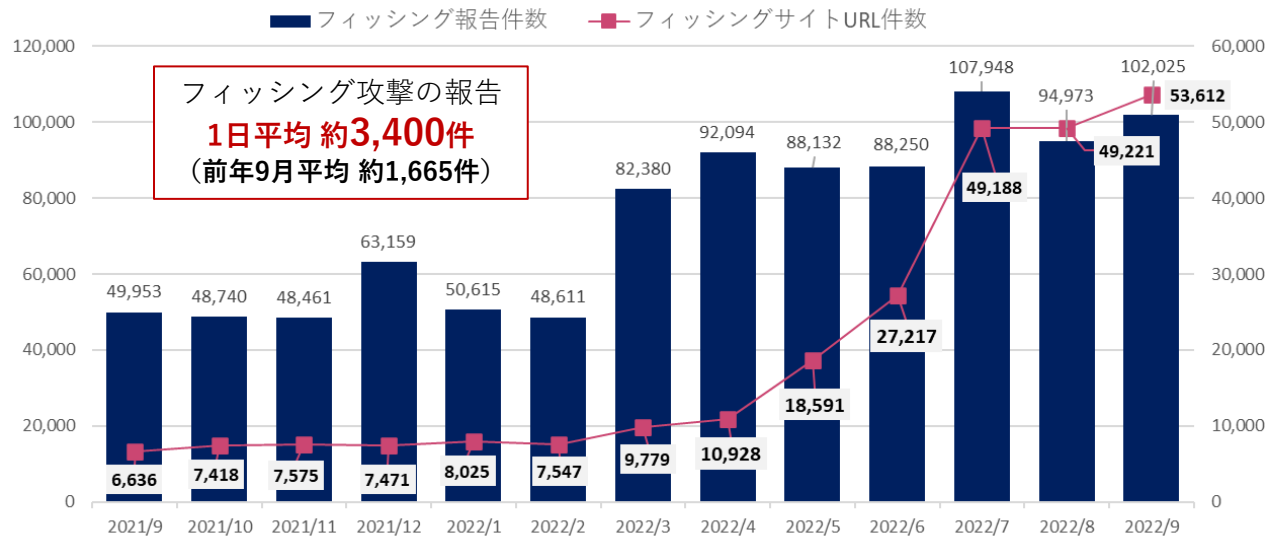
PICKUP!

- 出典：2022年10月6日 フィッシング対策協議会　2022/09フィッシング報告状況 https://www.antiphishing.jp/report/monthly/202209.html

## フィッシングサイトは高水準を維持、URL件数が最多更新。フィッシングメールに注意！

3月から高い水準を保っていたフィッシング報告件数は、
引き続き高水準を維持。URL件数は、過去最多を更新。

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ブレインが作成
https://www.antiphishing.jp/news/info/




## フィッシングサイトにご注意ください。

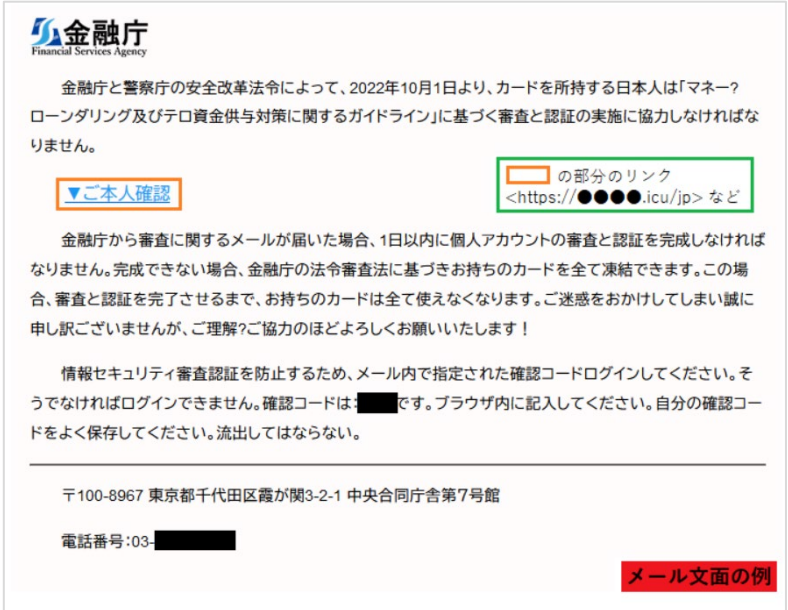

### フィッシング対策協議会　緊急情報　掲載一覧

- 2022年10月04日 金融庁をかたるフィッシング
- 2022年09月29日 ビットキャッシュをかたるフィッシング
- 2022年09月29日 スルガ銀行をかたるフィッシング
- 2022年09月20日 国税庁をかたるフィッシング
- 2022年09月20日 日本赤十字社をかたるフィッシング

### 金融庁をかたるフィッシング

金融機関のマネロン等対策を騙った
フィッシングメールにご注意ください。

偽サイトのURLをクリックすると入力フォームが表示され、暗証番号等を入力・送信することで第三者に個人情報が詐取される。



金融庁
Financial Services Agency

金融庁と警察庁の安全改革法令によって、2022年10月1日より、カードを所持する日本人は「マネー?ローンダリング及びテロ資金供与対策に関するガイドライン」に基づく審査と認証の実施に協力しなければなりません。

▼ご本人確認

[redacted]の部分のリンク
<https://●●●●.icu/jp> など

金融庁から審査に関するメールが届いた場合、1日以内に個人アカウントの審査と認証を完成しなければなりません。完成できない場合、金融庁の法令審査法に基づきお持ちのカードを全て凍結できます。この場合、審査と認証を完了させるまで、お持ちのカードは全て使えなくなります。ご迷惑をおかけしてしまい誠に申し訳ございませんが、ご理解?ご協力のほどよろしくお願いいたします！

情報セキュリティ審査認証を防止するため、メール内で指定された確認コードログインしてください。そうでなければログインできません。確認コードは:[redacted]です。ブラウザ内に記入してください。自分の確認コードをよく保存してください。流出してはならない。

〒100-8967 東京都千代田区霞が関3-2-1 中央合同庁舎第7号館

電話番号:03-[redacted]

メール文面の例

- 出典：フィッシング対策協議会　金融庁を騙るフィッシング
https://www.antiphishing.jp/news/alert/fsa_20221004.html

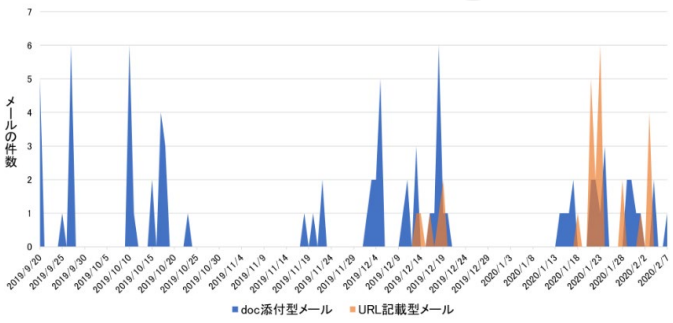
# 一定の停止期間と活動再開を繰り返す、Emotet引き続き警戒

PICKUP!

- 出典：2022年3月4日　NICTER Blog 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） https://blog.nicter.jp/2022/03/topic_emotet_2022/
  2022年5月27日 JPCERT/CC　https://www.jpcert.or.jp/at/2022/at220006.html

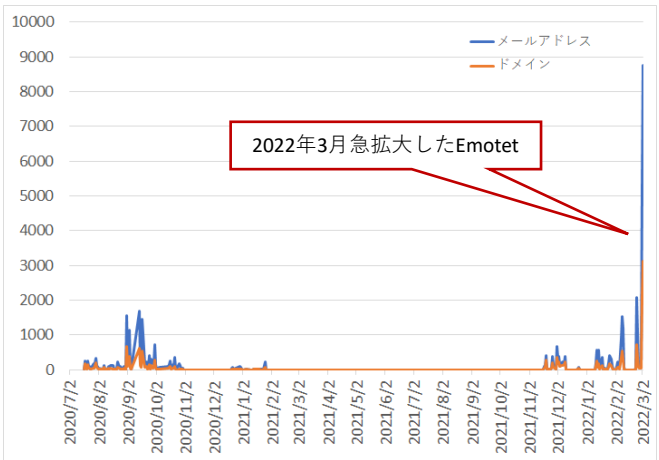
## マルウェアEmotetは、例年、一定の停止期間と検知数が活発化する期間を繰り返します。引き続きご注意を！


観測期間　2019年9月～2020年2月




出典：NICTER Blog　NICTに届いたEmotetメールの件数の推移

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)

## 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