# LATEST & PICKUP! SECURITY NEWS

Fuva Brain
Vol.45

## 最新個人情報漏洩事件・関連ニュース

LATEST

DATE：2022.04.19

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

- 04月18日：大和証券の**英国子会社が不正アクセス**被害
- 04月18日：**日本年金機構をかたるフィッシング　住所やクレカ情報など盗まれる恐れ**
- 04月18日：**So-netを偽るフィッシングを確認、注意を**
- 04月18日：**「ZOZOTOWN」装いクレカ情報だまし取るフィッシング**
- 04月18日：スマホゲーム「イケメン戦国」、不正アクセスでアクセス障害
- 04月15日：月桂冠株式会社、不正アクセスで社内システムが一時停止状態に
- 04月15日：**「mixi」をかたるフィッシング －「アカウントの使用を制限」とだます**
- 04月15日：キッチン用品販売の下村企販でも**Emotet感染**、不審メールに注意を呼びかけ
- 04月15日：ネット印刷のプリントオンも**Emotet感染**、顧客から不審メールについて連絡があり発覚
- 04月14日：産業サイバーセキュリティ研究会開催、中小企業への支援など提言
- 04月14日：サガン鳥栖、クラブスタッフは**Emotet感染**で不審メール
- 04月13日：**au装うフィッシング － 誘導に「Google翻訳」を悪用するケースも**
- 04月13日：厚労省事業の受託企業がマルウェア感染、個人情報流出の可能性
- 04月13日：大和証券グループ本社の**英国子会社に不正アクセス**、情報流出状況は調査中
- 04月13日：相模原市の業務委託先で**Emotet感染**、消去していなかった過去のメール情報が流出
- 04月13日：園芸情報サイト「Gadenet」に不正アクセス、悪意あるサイトへ誘導する改ざん
- 04月12日：エディオングループ会社がサイバー攻撃被害、配送情報など約7万件不正削除
- 04月12日：日本野鳥の会も**Emotet感染**、なりすましメールに注意呼びかけ
- 04月11日：ソフトウェア販売業者、4段階防御をすり抜け**Emotet感染**、再発防止策としてPPAP廃止も
- 04月11日：日邦産業グループ会社の**マレーシア工場に不正アクセス**、連結業績への影響は軽微
- 04月11日：国家戦略特区に設置した「雇用労働相談センター」で**「Emotet」感染**


## Emotet、引き続き

PICKUP!

出典：2022年4月15日 マイナビニュース/ Check Point Software Technologiesは4月12日発表
https://news.mynavi.jp/techplus/article/20220415-2320819

### Emotet、前月比2倍、国内組織の12.52%に影響
### 猛威続く、引き続きご注意ください。

*Emotetが先月から引き続いて世界中で最も影響を与えたマルウェアと位置づけられた。3月は、2月と比較して2倍となる10%の組織が影響を受けたとされており、最も流行しているマルウェアとしての地位を確かなものにしつつある。*
*2022年3月はAgent Teslaが2位にランクインした点も注目される。Agent Teslaは遠隔操作型トロイの木馬(RAT: Remote Administration Trojan)であり、キーロガーや情報窃取の機能を備えている。2022年2月は4位だったことから増加傾向にある。実際、Agent Teslaは世界中で新たなスパムキャンペーンを展開しており、中にはロシアのウクライナ侵攻を利用して被害者を誘い出すものもあるとされている。*

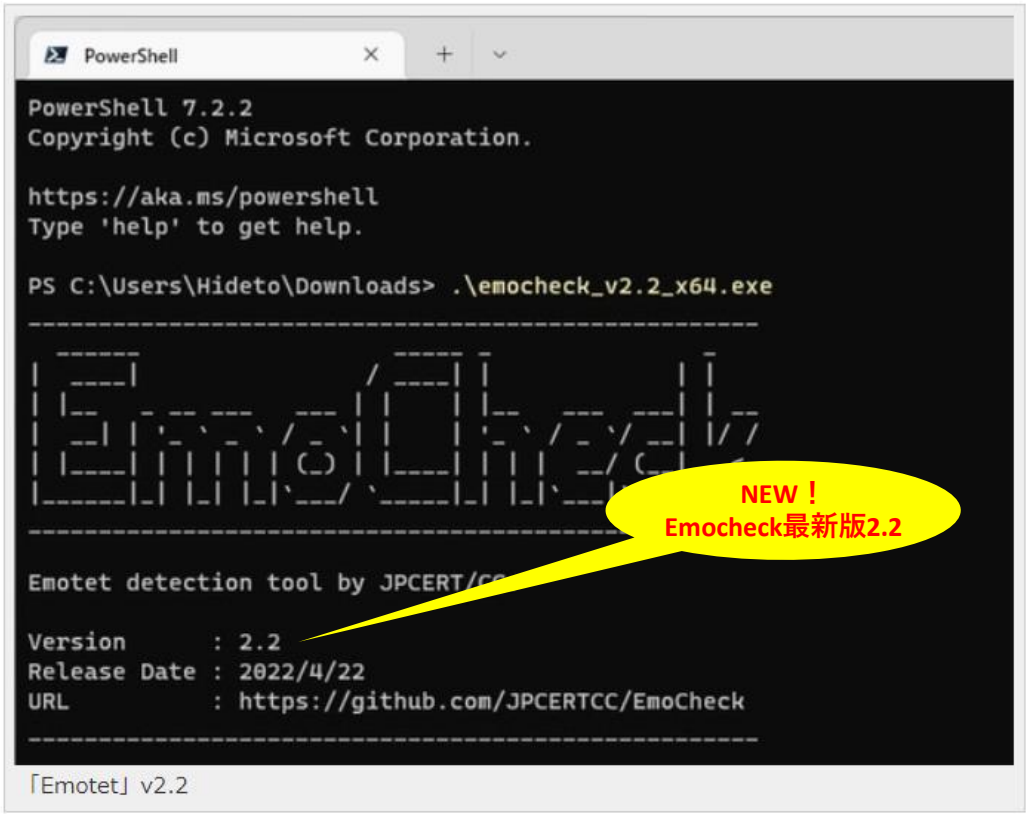

***Check Point Software Technologiesは、サイバー犯罪者は企業ネットワークに侵入するために人間の信頼に頼るようになってきており、今後さらにフィッシング詐欺メールを使ったサイバー犯罪が増加することに注意を呼びかけている。***

PICKUP!

出典：2022年４月２６日 JPCERT/CC
https://www.jpcert.or.jp/at/2022/at220006.html

# マルウェア「Emotet」の拡散に新手法 JPCERT/CCが注意喚起

JPCERT コーディネーションセンター（JPCERT/CC）は4月26日、マルウェア「Emotet」の拡散に**ショートカットファイル（LNKファイル）を使う新手法**を25日に確認したと発表した。新手法を含めた感染攻撃への注意を呼び掛けている。




「Emotet」v2.2

図　「Emotet」v2.2

NEW！
Emocheck最新版でチェック
してください！

**JPCERT/CC 提供**

感染チェックツール「EmoCheck2.2」

**JPCERTCC/EmoCheck - GitHub**
https://github.com/JPCERTCC/EmoCheck/releases


**参考情報**

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

４月２６日更新
マルウェアEmotetの感染再拡大に
関する注意喚起

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

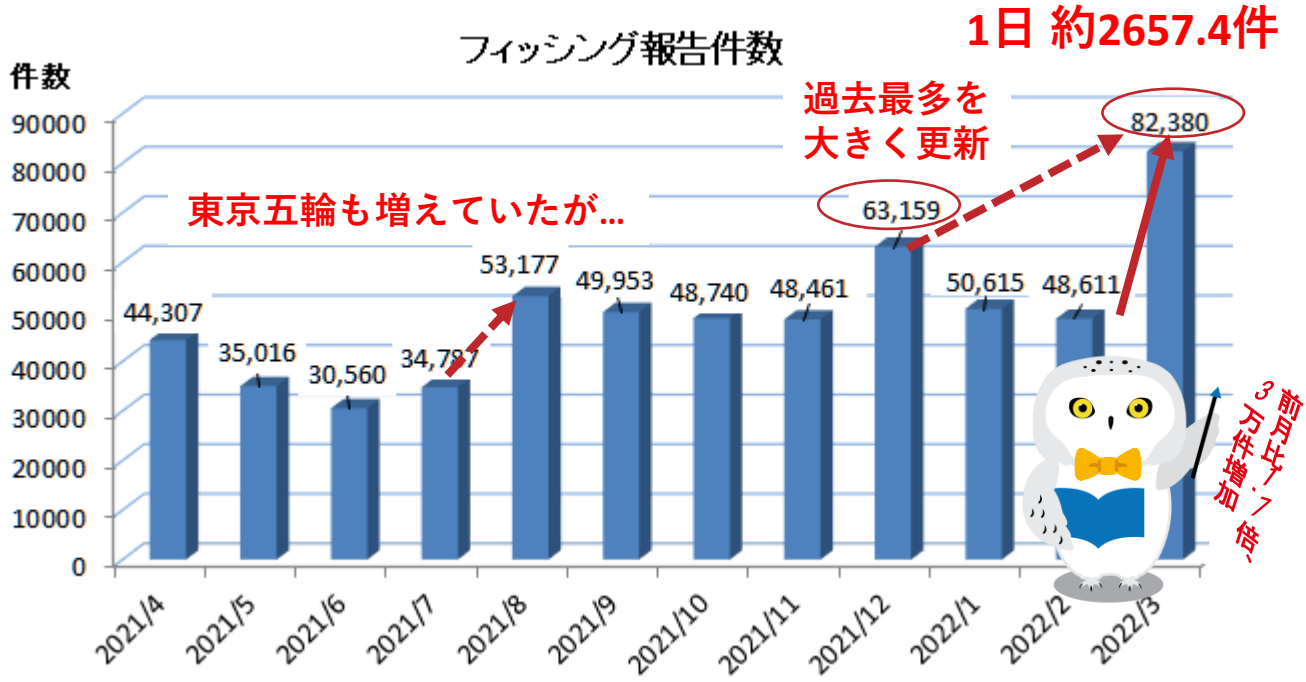
# 1日あたり約2657.4件、1カ月で過去最多8万件超

PICKUP!

出典：2022年4月5日 フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202203.html

## フィッシング報告、URL件数も過去最多

3月にフィッシング対策協議会へ寄せられたフィッシングの報告は、前月比1.7倍となる8万2380件。これまで最多だった2021年12月の6万3159件を大きく上回る。




## 感染増加に便乗！偽コロナワクチンナビが再来！

**他、日本年金機構、Mixi、ZOZOTOWN、au、FamiPay、出前館、JR東日本を騙るフィッシングも確認**

### 厚生労働省 偽コロナワクチンナビ

自衛隊大規模接種センターの予約については、下記注意事項をご覧頂き、
ページ下部に記載のWeb予約サイト、ＬＩＮＥまたは、専用お問い合わせ・予約窓口（電話）
により、予約を行ってください。

■予約サイトへ

■お問い合わせ・予約窓口

□の部分のリンク
<https://●●●●.cn/> など

予約に関するお願い
自衛隊大規模接種センターでは、原則として、接種券（原本）をお持ちいただいていない場合、ワクチンの接種はできません。接種券がお手元に届いてからご予約いただき、当日、接種券（原本）を必ずお持ち下さい。

■自衛隊 東京大規模接種センター専用
お問い合わせ・予約窓口
開設時間:07時00分～21時00分（毎日）
お電話のおかけ間違いにご注意ください。
一般:0570-056-730
English:0570-056-750
副反応:0570-056-760
※問い合わせのみ

Copyright © Ministry of Health, Labour and Welfare, All Rights reserved.
転載および[illegible]を禁じます。

[illegible]をかたるフィッシング（2022/04/13）


### au 通信量制限

auサポート
@au_support

【ご注意ください！】「重要なお知らせ【月間のデータ通信量の通信速度制限】」というタイトルやロゴでauを装い、個人情報を盗みとる不正サイトに誘導する詐欺メールが確認されています。auをご利用でない方にも届いているようですが、アクセスしないようお気を付けください。

【重要なお知らせ】auサポートのauからの重要なお知らせ【月間のデータ通信量の通信速度制限】（このメールは、配信専用のアドレスで配信されています）メール番号:M708[illegible]

au

（このメールは、配信専用のアドレスで配信されています）

午前11:32 · 2022年4月8日

408 返信 共有

30件の返信を読む



**もう一歩踏み込んだ対策も必要**

- サンドボックス環境で「悪意のある内容」かどうか検査
- 添付ファイルは、必ずマルウェアかどうか検査
- Webサイトは、URLフィルタリングの機能による検査

# 最新フィッシングメール動向、最も反応が高かった件名とは？

PICKUP!

出典：2022年4月18日 PRTIMES最新フィッシングメール動向：
最も反応が高かった件名は、祝祭日／ホリデー関連のお知らせと通達
https://prtimes.jp/main/html/rd/p/000000090.000053624.html

セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームのプロバイダーであるKnowBe4社（本社：米国フロリダ州タンパベイ、創立者兼CEO：Stu Sjouwerman （ストゥ・シャワーマン））は、模擬フィッシング攻撃を通してどれくらい攻撃被害を受けやすいかをPPP（Phishing Prone Percentage:フィッシング詐欺ヒット率）として継続的にアセスメントしている。同社が2022年度第1四半期の「要注意件名」統計レポートを公開した。


**最も反応が高かった件名：**

## 祝祭日スケジュール変更などの人事関連の通達

祝祭日・年始関連のメールが、従業員にとって最もクリックしたくなるものであることがわかりました。

**＜祝祭日／ホリデー関連のメール件名の例＞**

- 人事通達：祝祭日／休日変更に関するお知らせ
- 特別な人からバレンタインデー・カードを受信しました！
- 聖パトリックの祝日： 関連の行動規範／社内規定
- あなたへのバレンタインデー・ギフト
- スターバックス： ハッピーホリデー！スターバックスでお茶しませんか。

**＜一般的に使われるフィッシングメール件名トップ5＞**

**＜米国外＞**

- あなたのウォレットに未承認のアイテムが残っています
- 人事通達： 新型コロナウイルス調査の登録のお願い
- IT通達：年末パスワードポリシー
- 人事通達：行動規範について
- あなたの年金口座が更新されました

**＜米国内＞**

- 人事通達: 新型コロナウイルスワクチン接種要件の変更
- 即時パスワード変更依頼
- 人事通達： 有給休暇取得規定の改定
- 人事通達： 重要：服装規定変更
- 人事査定確認

KnowBe4のCEOであるStu Sjouwerman氏のコメントより、

*「最新のフィッシングレポート「2022年第1四半期フィッシングレポート」では、祝祭日・年始関連のメールが、従業員にとって最もクリックしたくなるものであることがわかりました。祝祭日スケジュール変更などの人事関連の通達は、休日が増えるのか、それとも勤務時間が短縮されるのか、従業員の興味をそそるものだったのでしょう。ここで忘れてはならないことは、サイバー犯罪者は人の感情を巧みに利用することです。心理的な隙間に入り込んで、様々手口で悪質な詐欺を仕掛けてくることです。感情的な反応を引き起こすメールは、多くの従業員がふとクリックしてしまいます。このような有害なメールに対して、警戒を怠らず、疑いの気持ちを強く持つことが、サイバーセキュリティ攻撃防止の基本です。」*

**従業員がふとクリックしてしまう、興味をそそる件名には要注意！**

# ブレア元米国家情報長官、日本「英並みサイバー能力を」

PICKUP!

出典：2022年4月16日日本経済新聞
ブレア元米国家情報長官、日本「英並みサイバー能力を」より
https://www.nikkei.com/article/DGXZQODE161KY0W2A410C2000000/


日本経済新聞

ブレア元米国家情報長官、日本「英並みサイバー能力を」

政治 ＋フォローする
2022年4月16日 14:38 [有料会員限定]

デニス・ブレア元米国家情報長官

デニス・ブレア元米国家情報長官（NID）は16日、都内で記者会見した。東アジアの

## 日本は能力を高めなければ攻撃を抑止できない

*デニス・ブレア元米国家情報長官（NID）は16日、都内で記者会見した。東アジアのサイバー分野の環境について「中国、北朝鮮、ロシアのサイバー能力は非常に高い。日本は能力を高めなければ攻撃を抑止できない」と述べた。まずは英政府通信本部（GCHQ）並みの能力を目標とすべきだと訴えた。（一部抜粋）*


出典：2021/06/30　日本経済新聞
日本のサイバー能力「最下位グループ」　情報収集に弱点

## 英国IISS、世界15か国のデジタル総合力を評価
## 日本は最下位グループ　※2021年6月28日発表

| IISS報告書での日本に関する記述 |
|---|
| Japan still does not have an official military cyber strategy … |
| （日本はまだ軍事面の公式なサイバー戦略を持っていない） |
| Japan's intelligence organisations are small and underfunded … |
| （日本のインテリジェンス組織は小さく資金も不足する） |
| … offensive cyber capabilities remain underdeveloped … |
| （攻撃的なサイバー能力が未発達） |
| … many corporations unwilling to meet the costs of bolstering them |
| （企業がコストを負担しようとしない） |


*報告書は米欧やアジアの主要15カ国について、サイバー分野の戦略や体制、情報収集力、攻撃能力などを比較した。日本を巡っては「(機密情報に関する米英などの枠組みである)ファイブ・アイズの同盟国だが、サイバー空間の安全保障の能力が低い」と問題提起した。*

*サイバー空間の情報収集能力で**「日本は同規模の他国に比べてインテリジェンス組織の規模が小さく、資金も不足している」**と評した。情報収集能力を米国に依存していると記述した。*
*他には、*
***日本の民間企業にも「サイバー空間での防御は強力ではなく、多くがコストの負担をしようとしない」**と注文をつけた。*

# 4月1日「サイバー警察局」が発足、警察庁　高まる脅威に対応

PICKUP!

出典：2022年4月1日日本経済新聞
「サイバー警察局」が発足、警察庁　高まる脅威に対応より
https://www.nikkei.com/article/DGXZQOUE0182G0R00C22A4000000/


日本経済新聞

「サイバー警察局」が発足、警察庁　高まる脅威に対応

事件・司法 ＋フォローする
2022年4月1日 18:00 (2022年4月1日 18:43更新)



発足式であいさつする二之湯智国家公安委員長（1日午後、東京・霞が関）=共同

警察庁は1日、サイバー犯罪対策の強化を目的とした新組織「サイバー警察局」と重

## サイバー警察局発足
## 「深刻化するサイバー犯罪」に重点

*警察庁は1日、サイバー犯罪対策の強化を目的とした新組織「サイバー警察局」と重大事件の捜査を担う「サイバー特別捜査隊」を発足させた。日本企業や病院などでランサムウエア（身代金要求型ウイルス）などの被害が深刻化しており、捜査体制の強化で高まる脅威に対応する。（一部抜粋）*