

PRESS RELEASE

【セキュリティレポート】

2022年上半期国内セキュリティインシデントを集計

最多は「マルウェア感染」で前年同期比の約15倍、再び「Emotet」が台頭

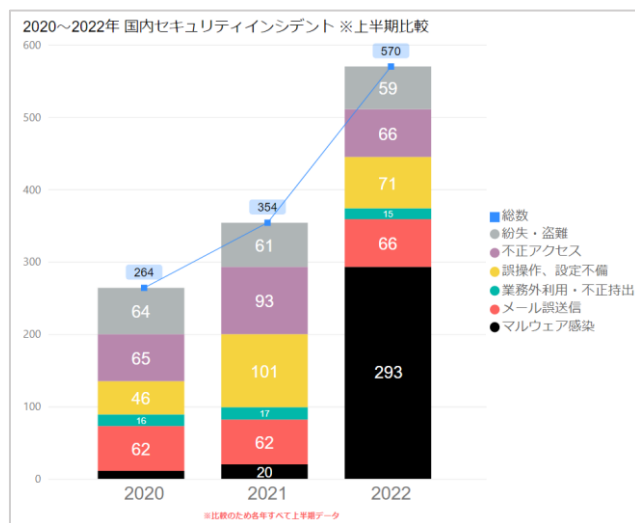
情報セキュリティメーカーのデジタルアーツ株式会社(本社:東京都千代田区、代表取締役社長:道具 登志夫、以下 デジタルアーツ、証券コード 2326)は、上半期の国内セキュリティインシデントを集計したセキュリティレポートを公開したことを発表します。

2022年上半期の国内組織における情報漏洩等のセキュリティインシデントを独自に集計

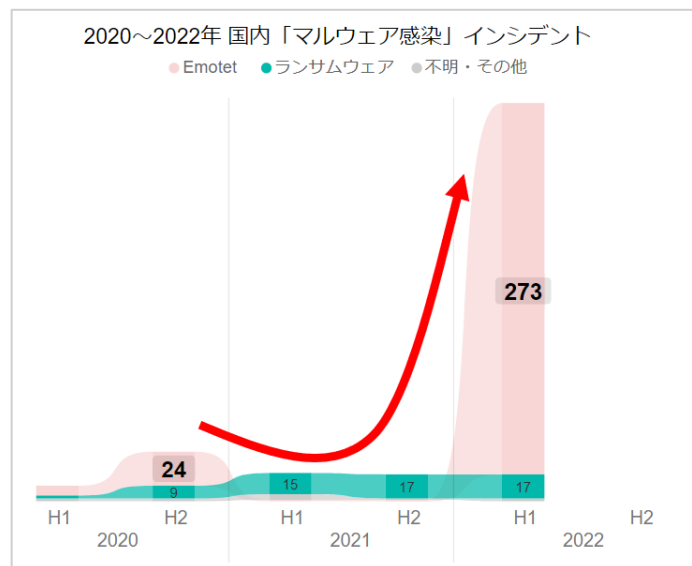
2022年上半期(1~6月)国内組織における情報漏えいなどにかかるセキュリティインシデントを、対象組織による公開報告書およびマスメディアによる報道資料をもとに独自に集計しました。

2022年上半期の国内セキュリティインシデントは、前年同期比約1.6倍の570件となることがわかりました。最多の「マルウェア感染(Emotetのようなマルウェア感染やその他ランサムウェアへの感染など)」は前年同期比約15倍の293件となりました。

次いで「誤操作、設定不備」は前年同期よりは減少し、71件となりました。



最多のセキュリティインシデントは「マルウェア感染」、特に「Emotet」への感染が多い



最多のセキュリティインシデント「マルウェア感染」293件のうち、「Emotet」への感染が273件と最も多く、被害の深刻さがわかります。Emotetは、2014年頃から活動が確認されているマルウェアで、2021年初頭にテイクダウン(停止措置)されましたが、2021年11月頃から活動が再開し、今日に至るまで断続的に活発な活動が見られています。

Emotet感染報告は、2021年の上半期と比べると約273倍となりますが、2021年1月下旬から11月中旬までは活動していない期間があったため単純な比較はできません。しかし、猛威をふるっていた2020年と比べても急増していることは明らかです。

一般的に被害者側からは被害について表に出されにくいのがセキュリティインシデントです。ですが、被害者側からの被害報告が増えていることに関しては、①なりすましメールを受信した外部からの指摘②「EmoCheck」によりコストや時間が大幅に軽減③隠さない、セキュリティ意識の変化などが理由として考えられます。

Emotet 感染に引き続き警戒を

Emotetはランサムウェアのように事業継続を脅かすような「感染後の大きな被害」が報告されることはあまり耳にしません。しかし、Emotetに感染するとメール情報が窃取されたり攻撃メールの送信が行われるだけでなく、過去にはTrickbotやQakbotといった別のマルウェアへも感染したり、Cobalt Strikeという様々な攻撃を展開しやすくするツールを入れるなどの動きがみられています。最近では感染端末のWebブラウザーに保存されているクレジットカード情報を窃取する機能が追加されたという報告もされています。

感染しないよう、感染してしまって自組織が重症化しないよう、および取引先等へ感染を拡げないよう、日頃からの備えが必要です。

## デジタルアーツの Emotet 対策

Emotet による攻撃は、主にメールを介して行われます。その手法はセキュリティツールで検知されにくいパスワード付き ZIP ファイルにマクロ付き Office ファイルを添付する方法、マクロ付きの Office ファイルを添付する方法、メール本文内に記載された URL を介して行う方法です。デジタルアーツの Emotet への感染対策をご紹介します。

<https://www.daj.jp/bs/lp/emotet/>

## Emotet の対策方法について解説するセミナーを開催

7月13日(水)15:00~15:40

Emotet の新たな攻撃手法「ショートカットファイル」に注意！～メールセキュリティ対策のポイントを解説～

本セミナーでは、活動再開後の Emotet の脅威をご紹介しますとともに、最新の手口の「ショートカットファイル」を添付することによる感染について解説いたします。また、デジタルアーツのメールセキュリティソリューションによる効果的な対策をご紹介します。

▶[お申し込みはこちら](#)

※お申し込み方法: デジタルアーツ Web サイトのお申し込みフォームに必要事項をご入力ください。[参加費: 無料]

## ▶ 上半期の国内セキュリティインシデントを集計したレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。

セキュリティレポート [https://www.daj.jp/security\\_reports/220705\\_1/](https://www.daj.jp/security_reports/220705_1/)

## デジタルアーツ株式会社 概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。

1995年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウェストタワー14F ▶URL: <https://www.daj.jp/>

<本リリースに関するお問い合わせ>

デジタルアーツ株式会社 広報担当 松岡 TEL : 080-8163-0311 / E-mail : [press@daj.co.jp](mailto:press@daj.co.jp)

※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせは上記とさせていただきます

※デジタルアーツ、DIGITAL ARTS、i-FILTER、i-FILTER Anti-Virus & Sandbox、i-FILTER@Cloud Anti-Virus & Sandbox、info board、Active Rating System、D-SPA、Anti-Virus & Sandbox for D-SPA、NET FILTER、SP-Cache、White Web、ZBRAIN、クレデンシャルプロテクション、ホワイト運用、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER Anti-Virus & Sandbox、m-FILTER@Cloud Anti-Virus & Sandbox、m-FILTER File Scan、Mail Detox、m-FILTER EdgeMTA、EdgeMTA、FinalCode、i-フィルター、DigitalArts@Cloud、Desk@Cloud、Desk、D アラートおよび D コンテンツその他の弊社・弊社製品関連の各種名称・ロゴ・アイコン・デザイン等はデジタルアーツ株式会社の登録商標または商標です。

※ その他、上に記載された会社名および製品名は、各社の商標または登録商標です。