2021 年 9 月 3 日
デジタルアーツ株式会社

**PRESS RELEASE**

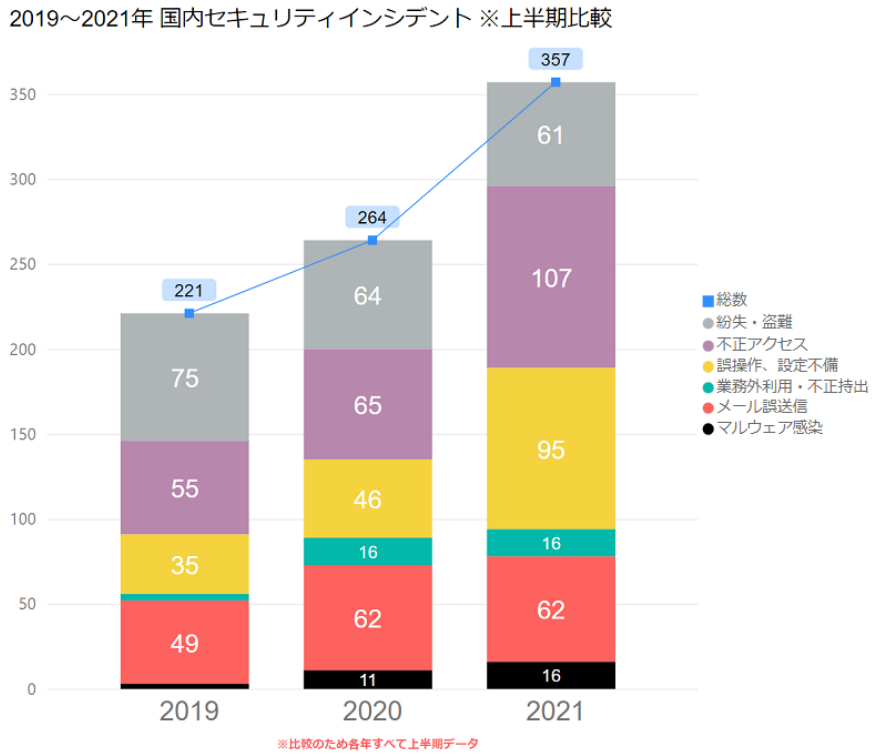
# マルウェア感染のインシデントは、Emotet からランサムウェアへ
# ～二重脅迫を行うランサムウェアに注意～

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、2021 年上半期のインシデント集計とランサムウェアの手口の考察に関するレポートを公開したことを発表いたします。

昨年までは、マルウェア「Emotet」※1 が猛威を振るっていましたが、現在は、ランサムウェアの被害報告が増えています。ランサムウェアは、感染すると大切なデータが暗号化され、元に戻すことと引き換えに「身代金」を要求する悪質なマルウェアです。最近では、データを暗号化するだけでなく、身代金を支払わなければデータを公開すると二重で脅す「二重脅迫」の手口が流行しています。こうした「マルウェア感染」の最新の状況とランサムウェアの新たな手口について考察しました。

## 「マルウェア感染」インシデントは Emotet からランサムウェアへ

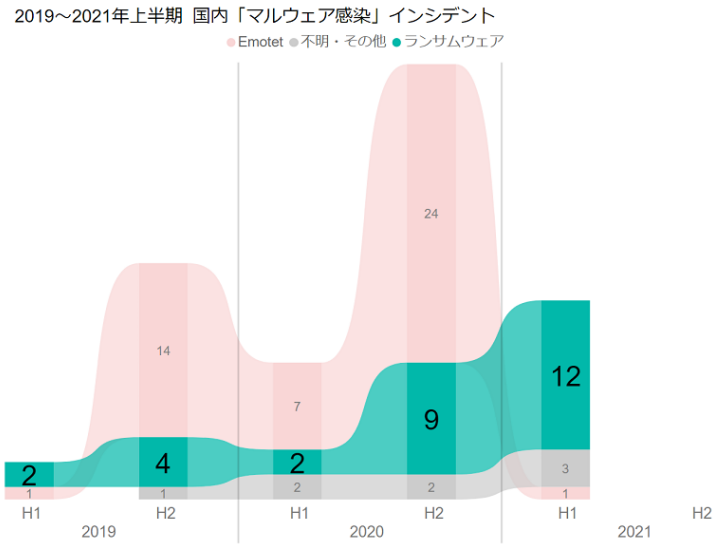
2021 年上半期（1～6 月）国内組織における情報漏洩等のセキュリティインシデントを、対象組織による公開報告書およびマスメディアによる報道資料をもとに独自集計しました。




【図 1】2019～2021 年　国内セキュリティインシデントの上半期比較

2021 年上半期で多く報告されたものは、最多が「不正アクセス」、次いで「誤操作、設定不備」によるインシデントでした。過去の上半期と比較してもかなり増加しています。「不正アクセス」の例としては、あるプロジェクト情報共有ツールへの不正アクセスにより、内閣サイバーセキュリティセンター（NISC）や外務省、経済産業省、国土交通省など多くの組織に影響を与えたものがあります。

今回特に注目したいのが、「マルウェア感染」に分類されるインシデントです。2021 年上半期と 2020 年上半期を比較しても「マルウェア感染」の数はあまり変わりませんが、内容が変わっています。一つは、以前のレポート※2 でも取り上げたように、2020 年には Emotet が猛威を振るっていましたが、2021 年 1 月末にテイクダウン（停止措置）および無害化されたことにより新たな被害はなくなっているということです。もう一つは、「ランサムウェア」による被害報告が増加し始めているということです。【図 2】の緑色の値のように、2020 年下半期から増え始め、特に直近 2021 年上半期では 12 件が報告されています。




【図 2】2019～2021 年上半期 国内「マルウェア感染」インシデント

## 二重脅迫を行うランサムウェアが流行中～日本の組織も狙われているため、万全の対策が必要～

ランサムウェア被害の増加は世界的にも深刻化しており、情報処理推進機構（IPA）が公開した情報セキュリティ 10 大脅威 2021 でも「ランサムウェアによる被害」が組織部門で 1 位に選出されています。最近では、二重に脅迫を行うランサムウェアが流行していることをご存知でしょうか。従来のランサムウェアといえば、侵入した端末やサーバーのデータを暗号化して使えなくさせ、戻すためには金銭を支払えと脅迫するものでした。最近では暗号化するだけでなく、暗号化前にデータを盗んでおいて支払わなければ、盗み出したデータを公開すると二重で脅す、「二重脅迫型ランサムウェア」が多くなっています。2021 年 5 月、米国の大手石油パイプライン企業が「DarkSide」と呼ばれるランサムウェア/犯罪グループに攻撃を受けました。不正アクセスにより重要データの窃取の後に暗号化が行われ 440 万ドル（約 4 億 8000 万円）もの身代金要求がされたとのことです。この影響により、同社は数日間操業停止となり、米国では大混乱に陥りました。


日本の組織も例外ではありません。2020 年 11 月、国内のゲームメーカーが「Ragnar Locker」と呼ばれるランサムウェア/犯罪グループに攻撃を受けました。海外拠点を経由に不正アクセスされ国内拠点へも被害が及び、重要データの窃取と暗号化が行われたとのことです。

※1 情報の窃取に加え、さらに他のマルウェアへの感染のために悪用されるマルウェアです。悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染が拡大していました。

※2 セキュリティレポート「過去 3 年分の国内セキュリティインシデント集計 Emotet によりマルウェア感染が激増」
https://www.daj.jp/security_reports/210126_1/

**▶デジタルアーツではセキュリティに関するオンラインセミナーを毎月実施しています**

**＜人気対談セミナー＞増え続けるランサムウェア被害に遭わないための最新情報を解説！～攻撃の「今」と「これから」の対策～**

被害が増え続けているランサムウェアの予習と復習をしませんか？セキュリティエンジニアとしてセキュリティ情勢の調査や分析、脅威情報の共有などを積極的に行っている、SB テクノロジー株式会社 辻伸弘氏をお招きして、「ランサムウェア」をテーマに、被害の事例などを交えながら対談形式で深掘りしていくオンラインセミナーを実施いたします。ランサムウェアについて長年ウォッチ、対応してきている辻伸弘氏だからこそわかる、攻撃傾向の変化や、利用される手法を含めた事例など、これからの対策に役立つ最新情報をお届けします。報道などで見聞きして言葉は知ってはいるものの、実情はどういったものかよくわからない…といった疑問を解消し、ランサムウェアについての理解が深まるセミナーです。
お申し込みはこちら▸https://mktg.daj.jp/public/seminar/view/4253 （先着順ですので、お早めに！）

**▶セキュリティ対策の新定番！「ホワイト運用」を実現**

弊社が提供する「i-FILTER」「m-FILTER」なら、デジタルアーツが安全を確認したサイトにはアクセスさせ、それ以外にはアクセスさせない、「ホワイト運用」を実現させています。出口対策は「i-FILTER」で、アクセスしたい Web サイトを安心してクリック、入口対策は「m-FILTER」で、受信したすべてのメールを安心して開くことができるので、情報システム部門の運用負荷も削減できます。Web とメール経由のマルウェア感染を防げる「i-FILTER」と「m-FILTER」を導入し、インターネットにおけるセキュアな世界を実現しませんか。
https://www.daj.jp/bs/ifmf/

**▶ランサムウェアのレポートはこちら**

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/210903_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 ウエストタワー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 山田 TEL : 090-1555-7254 / E-mail : 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、info board、Active Rating System、D-SPA、NET FILTER、SP-Cache、White Web、ZBRAIN、クレデンシャルプロテクション、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、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。