

**PRESS RELEASE**

# 見慣れない XLL ファイル (Excel アドイン) を使う攻撃に要注意！ ～サンドボックスやアンチウイルスをすり抜ける Excel アドインとは？～

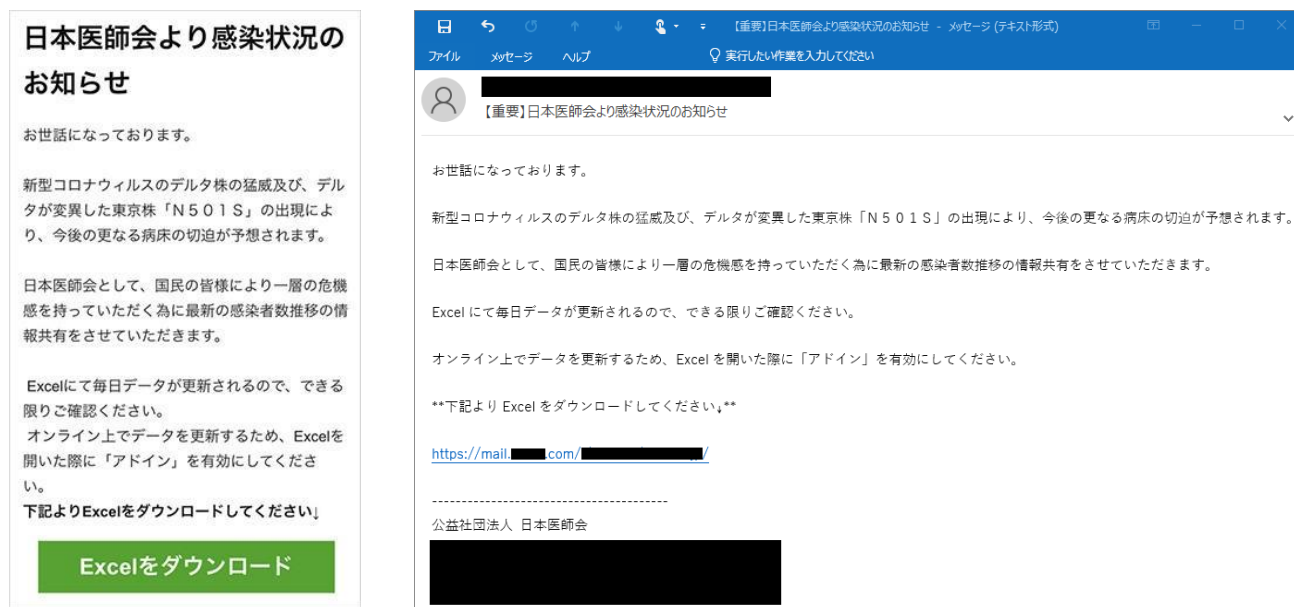
情報セキュリティメーカーのデジタルアーツ株式会社(本社:東京都千代田区、代表取締役社長:道具 登志夫、以下 デジタルアーツ、証券コード 2326)は、まだ注意喚起がほとんど行われていない XLL ファイル(Excel アドイン)を使う攻撃についてのセキュリティレポートを公開したことを発表いたします。

昨今、見慣れない XLL ファイル(Excel アドイン)を使う攻撃が増えています。弊社が入手した不審な XLL ファイルをもとに、どのようにマルウェアに感染するのか検証しました。また、XLL ファイルの懸念点として、サンドボックスで挙動を再現できず、アンチウイルス製品での検知率が低いことが判明しました。

## 見慣れない XLL ファイル (Excel アドイン) を使う攻撃が増加中

2021年9月2日、日本医師会を騙る不審なメールがばらまかれているとして、日本医師会の公式サイトにて注意喚起が発出されました。

### 【注意喚起】日本医師会を騙る不審メールの流通について



左: 日本医師会を騙る不審メールの例(公式サイトより)

右: 日本医師会を騙る不審メールの例(注: 報告情報をもとに弊社で再現)

メールに記載のリンクをクリックすると、インターネット上から Excel ファイルのダウンロードがされたとのことです。デジタルアーツでは、この不審な Excel ファイルを入手しました。XLL ファイルを使用した攻撃は海外では観測されているものの、国内ではあまり観測されておらず、また注意喚起もほとんど行われていません。

## メールから誘導される不審なファイルは Excel のアドインファイル



20210901193139\_7a77664b.xll

ダウンロードされた不審な Excel ファイル

ファイル名の末尾にはあまり見慣れない「.xll」という拡張子がありますが、これは Microsoft Excel のアドインファイルです。

	1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10	1/11	1/12
中国												
CHINA	87071	87089	87117	87150	87183	87215	87278	87331	87364	87433	87536	87591
HONG KONG	8846	8888	8923	8964	9017	9049	9074	9107	9152	9211	9242	9283
MACAU	46	46	46	46	46	46	46	46	46	46	46	46
日本												
JAPAN	235811	239068	242097	245293	248625	253571	259521	267084	274947	282737	288818	293746
(CRUISE SHIP)	721	721	721	721	721	721	721	721	721	721	721	721
東アジア												
KOREA	61769	62593	63244	64264	64979	65818	66686	67358	67999	68664	69114	69651
MONGOLIA	1220	1242	1263	1286	1308	1308	1308	1395	1408	1429	1442	1456
TAIWAN	799	802	808	812	815	817	819	822	825	828	828	834
東南アジア												
PHILIPPINES	474064	475820	476916	477807	478761	479693	480737	482083	483852	485797	487690	489736
VIETNAM	1465	1474	1482	1494	1497	1504	1505	1509	1512	1513	1514	1515
LAOS	378	379	381	382	382	383	385	386	387	391	391	392
CAMBODIA												

## 新型コロナウイルス関連の資料を装うおとりファイル

XLL ファイルは「Warzone RAT」というマルウェアに感染するものでした。RAT (Remote Administration Tool または Remote Access Trojan) とは、遠隔操作型マルウェアです。「乗っ取り」の手法で、端末内の情報を盗む、もしくは端末に対して不正な操作を指示することにより、さらに攻撃の範囲を広げることが想定されます。今回の日本医師会を騙ったメールは、文章が日本語で記述され、おとりのファイルも日本語で作成されていました。明らかに日本をターゲットにしたものと想定されます。XLL ファイルを用いた攻撃について、サイバーリスク情報を無償で提供する弊社「D アラート」でも何度か発出しております。

[08/27 から発生していたマルウェア \(Warzone RAT\) に感染させると考えられるメールの受信・URL アクセスを検知](#)

[08/12 から発生していたマルウェア \(Vidar\) に感染させると考えられるメールの受信・URL アクセスを検知](#)

## サンドボックスやアンチウイルスをすり抜ける Excel アドイン

### ・サンドボックスで挙動を再現できない場合がある

サンドボックス製品でインストールされている Excel が古いバージョンの場合、アドインを動かすことができず悪性の挙動を検知できません。また、一部のサンドボックス製品においては新しいバージョンの Excel を使っても、XLL ファイルを Excel で開くように処理ができておらず、アドインの悪性の挙動を検知できていないものがありました。

### ・アンチウイルス製品での検知率が低い

オンラインマルチスキャンサービスを使って確認したところ、アンチウイルス 65 製品中 2 製品しか検知していなかったものもありました。もちろん確認する時間によって異なりますし、時間が経てば各アンチウイルス製品にシグネチャ (マルウェアや不正アクセスといった攻撃の特徴的なパターン) が登録されるため検知できる製品数は増えていきます。しかし、アンチウイルス製品に登録される前の、メールがばらまかれた当時にはアンチウイルスの検知をすり抜けているということが考えられます。

### ▶セキュリティ対策の新定番！「ホワイト運用」を実現

情報システム部門の運用負荷を削減でき、安全にアクセスできる情報のみ触れることができる「ホワイト運用」で、受信したすべてのメールを開け、アクセスしたい Web をクリックできるセキュアな世界を実現しませんか。「m-FILTER」Ver.5 では、メールに XLL ファイルが添付されている場合には偽装メール対策「添付ファイル偽装判定」により、添付ファイルを「実行形式ファイル」および「禁止拡張子」として危険性のあるファイルと判定するため、メールの受信を防ぐことが可能です。「i-FILTER」Ver.10 では、「ダウンロードフィルター」機能により Web からの XLL ファイルやその他の危険なファイルのダウンロードを防ぐことが可能です。

▶デジタルアーツの「ホワイト運用」<https://www.daj.jp/bs/ifmf/>

### ▶見慣れない XLL ファイル (Excel アドイン) を使う攻撃について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/211005\\_1/](https://www.daj.jp/security_reports/211005_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](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、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、ホワイト運用、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。