サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2021 年 7 月～9 月] 《 付録 》
～Excel-DNA を悪用した Excel アドインファイルのウイルス～

2021 年 10 月 27 日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

目次

1 はじめに

サイバー攻撃は、あらゆる企業・組織に対して試みられている。このような状況において、自組織（あるいはISAC[1]等の会員組織）に試みられた攻撃を分析し、その情報を蓄積し、他の組織と情報共有するといった活用を行っていくことは一定の意義があるものと考える。特に、攻撃者によって意図的に狙われて攻撃された場合（標的型攻撃）、分析・蓄積・共有を重ねた結果、自組織や関連業界が過去に受けた攻撃との関係性（連続性）の有無や攻撃手口の類似性等の点について、把握できる場合がある。あるいは、新たな技術的な攻撃手口が確認された場合も、今後の対策検討のための分析が重要である。こういった分析には様々な観点や方法があり、その一つとして、攻撃に用いられたウイルス等の不正ファイルの解析がある。

IPA セキュリティセンターでは、J-CSIP の運用をはじめとして、サイバー攻撃の情報を分析するため、必要に応じてウイルス等の解析を行っている。その中には、広く無差別にばらまかれたと思われるウイルスだけでなく、特定の業種・業界を狙った攻撃に使用されたと思われるウイルスもある。そして、これらの情報について、必要な範囲で情報共有を進めている。

この活動の中で、本四半期、J-CSIP 参加組織から、Excel アドイン(拡張子 .xll)形式のファイル（以下、Excel アドインファイルとする）が添付された、不審なメールの情報提供があった [2]。また、公開情報においても、Excel アドインファイルを悪用した、日本語で記載された攻撃メールの情報も確認された。これらの Excel アドインファイルを解析したところ、Excel-DNA と呼ばれるツールを使用している共通点があった。そこで、これらの事例以外にも攻撃事例がないか、IPA で調査したところ、公開情報から 59 個の Excel-DNA を悪用した Excel アドインファイルを入手できた。これらの検体を解析、比較したところ、攻撃者の環境や攻撃手法について、いくつかの知見を得ることができたため本書にて紹介する。なお、同等の攻撃については、詳細な調査結果を公開しているセキュリティベンダがある [3]。

本書では、Excel アドインファイルを使用した多数のウイルス検体について解析、比較した結果を一つの事例として説明する。ファイルを開いてしまった際の対策や、システム的な対策についてはレポート本紙を参照していただきたい。また、本書はあくまで特定のウイルスの解析結果から推定した内容を参考情報として示すものであり、今後のサイバー攻撃への直接的な対策となるものではない。一方、このようなウイルスの特徴や動作の仕組みを把握することは、ウイルス解析者のみならず、企業・組織のセキュリティ担当者においても、サイバー攻撃への対応・対策を検討する上で、役立つ可能性があるであろうと考え、報告するものである。

本書の対象読者

本書では、次の方々を主な対象読者と想定している。

- 企業の CSIRT[4]や ISAC 等、組織のセキュリティを扱う部門の方
- ウイルスの解析等を行う方、ウイルスの解析を外部専門組織へ依頼して業務を遂行する方

---

[1] Information Sharing and Analysis Center（ISAC、アイザック）。同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織。

[2] J-CSIP の参加組織から提供された不審メールや Excel アドインファイルについては、レポート本紙を参照ください。

[3] Digital Arts Security Reports －見慣れない XLL ファイル（Excel アドイン）を使う攻撃が増加中 https://www.daj.jp/security_reports/211005_1/

[4] Computer Security Incident Response Team（CSIRT、シーサート）。組織内の情報セキュリティ問題を専門に扱う、インシデント対応チーム。

2 Excel アドインファイルを悪用したウイルス

本四半期、IPA では Excel アドインファイルを悪用した攻撃を観測した。この攻撃手口について独自に調査したところ、公開情報より複数の類似の検体を入手した。これらの検体を調査したところ、Excel-DNA と呼ばれるツールを使用して作成されたものであることや、このウイルスを使用した攻撃について共通する動作を持つことが判明した。

本章では、まずウイルス作成に悪用されたツール Excel-DNA について説明する。その後、Excel アドインファイルを悪用したウイルスを使用した攻撃の流れ、Excel-DNA を悪用し作成された Excel アドインファイルのウイルス（以下、Excel-DNA を悪用したウイルスとする）の共通する動作について説明する。

2.1 Excel-DNA

Excel-DNA とは、通常 C 言語や C++言語で開発する Excel アドインファイルを、C#（.NET）等で開発可能とするツールである。このツールはインターネット上に公開されており [5]、自由に利用できる。Excel-DNA を使用するには、ユーザが C#でプログラムを作成し、そこからライブラリファイル(拡張子 .dll)を作成する。そのライブラリファイルを読み込むように「<任意の名称>.dna」ファイルを作成する。そして、それらのファイルを Excel-DNA ツールを使うことによって、Excel アドインファイルが作成できる。作成した Excel アドインファイルを Excel で実行することによって、C#で作成したプログラムが使用可能となる。Excel-DNA を使用した Excel アドインファイルを作成した例を図 1 に示す。

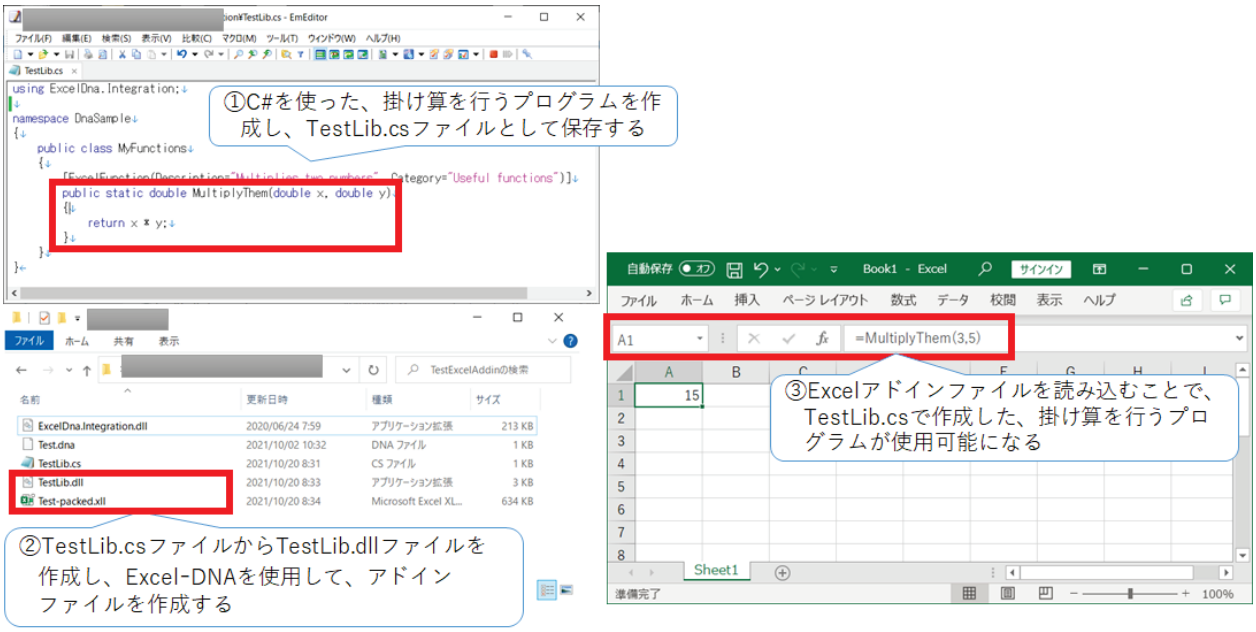

図 1：Excel-DNA を使用した Excel アドインファイルの作成

2.2 Excel アドインファイルを悪用した攻撃の流れ

IPA で確認している Excel アドインファイルを悪用した攻撃の流れの例を図 2 に示す。まず、悪意のあるメールに添付された Excel アドインファイルが実行される(利用者によってファイルが開かれ、Excel の警告ウインドウで「アドインを有効にする」旨のボタンが選択される)ことでウイルスが動作する [6]。Excel アドインファイルは、動作すると DLL ファイルがメモリ上に展開され実行される。この DLL ファイルが表示用のダミー文書ファイルを作

[5] Excel-DNA https://excel-dna.net/

[6] 添付されているファイルは rar 形式のファイルで、そのファイルを解凍したら Excel アドインファイルが得られるという事例や URL リンクで Excel アドインファイルをダウンロードされる事例を確認している

成し、画面に表示する。その後、DLL ファイル内に含まれているデータもしくはインターネット上からデータを取得し、別のウイルス（以下、二次ウイルスとする）に感染させる。その後の動作は二次ウイルスの種類によって異なるが、例えば不正通信等が発生する。

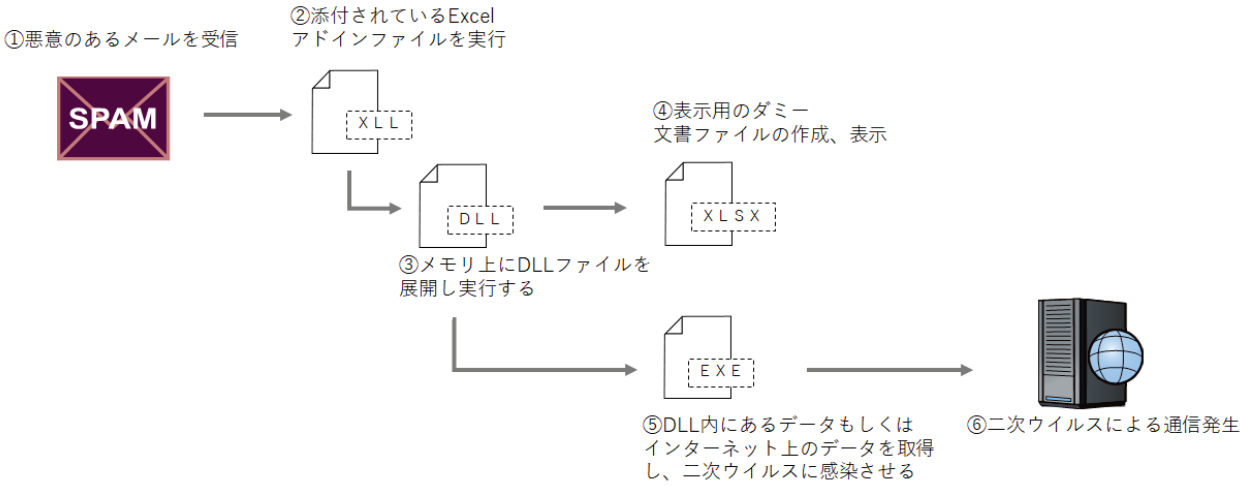

図 2：Excel アドインファイルを悪用したウイルスが動作するまでの流れ

IPA で入手した検体では、2.1 節にて説明した Excel-DNA を用いて作成されたものを複数確認した。

2.3 Excel-DNA を悪用したウイルスの動作

IPA で入手した 59 検体の Excel-DNA を悪用したウイルスには、図 3 に示すように、「JACK」いう名前のファイル及び「JACK」ファイルを使用する内容の Excel-DNA で使用する「_MAIN_.dna」ファイルが共通して存在した。また、「JACK」ファイルは圧縮されており、解凍することで「JACK.dll」という名前のライブラリファイルを得ることができる。Excel-DNA を悪用したウイルスが実際に動作する際は、この JACK.dll はメモリ上に展開される。

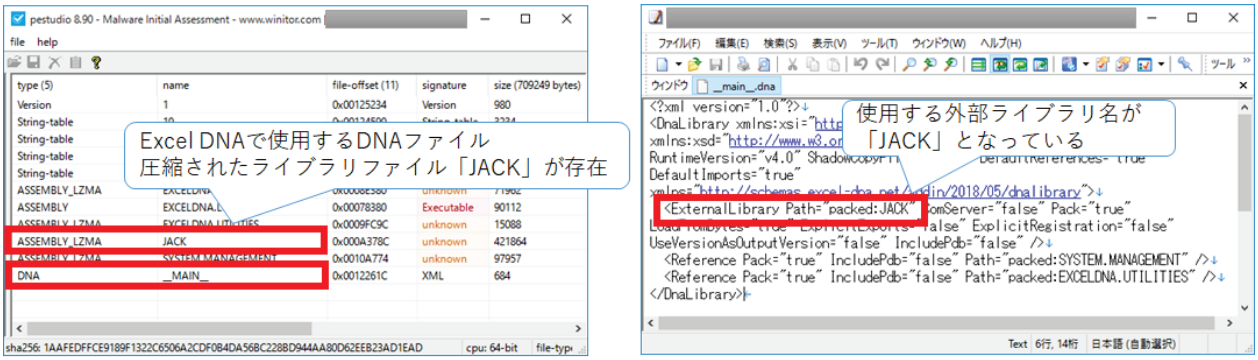

図 3：Excel-DNA を悪用したウイルスに含まれているファイル

ウイルスに含まれていた「JACK.dll」ファイルをデコンパイルした結果、このウイルスは図 4 に示す動作を行った。まず、表示用のダミー文書ファイルの作成有無を判定し、作成する場合はプログラム内で決められたフォルダに表示用のダミー文書ファイルを作成し、Excel アプリケーションから作成した表示用のダミー文書ファイルを表示する。表示用のダミー文書ファイルの例を図 5 に示す。その後、二次ウイルスをインターネット上からダウンロードするかを判定する変数を確認し、ダウンロードする場合は、Jack.dll ファイル内に記述してある URL から二次ウイルスをダウンロードし、実行する。ダウンロードしない場合は Jack.dll ファイル内に保持しているデー

タを実行ファイルとして保存し、それを二次ウイルスとして実行するという動作になっている。
　以上の動作から、Excel-DNA を悪用したウイルスは二次ウイルスへの感染を目的としたドロッパーもしくはダウンローダーの機能を持つウイルスである。また、最終的に感染する二次ウイルスは、検体によって異なる。

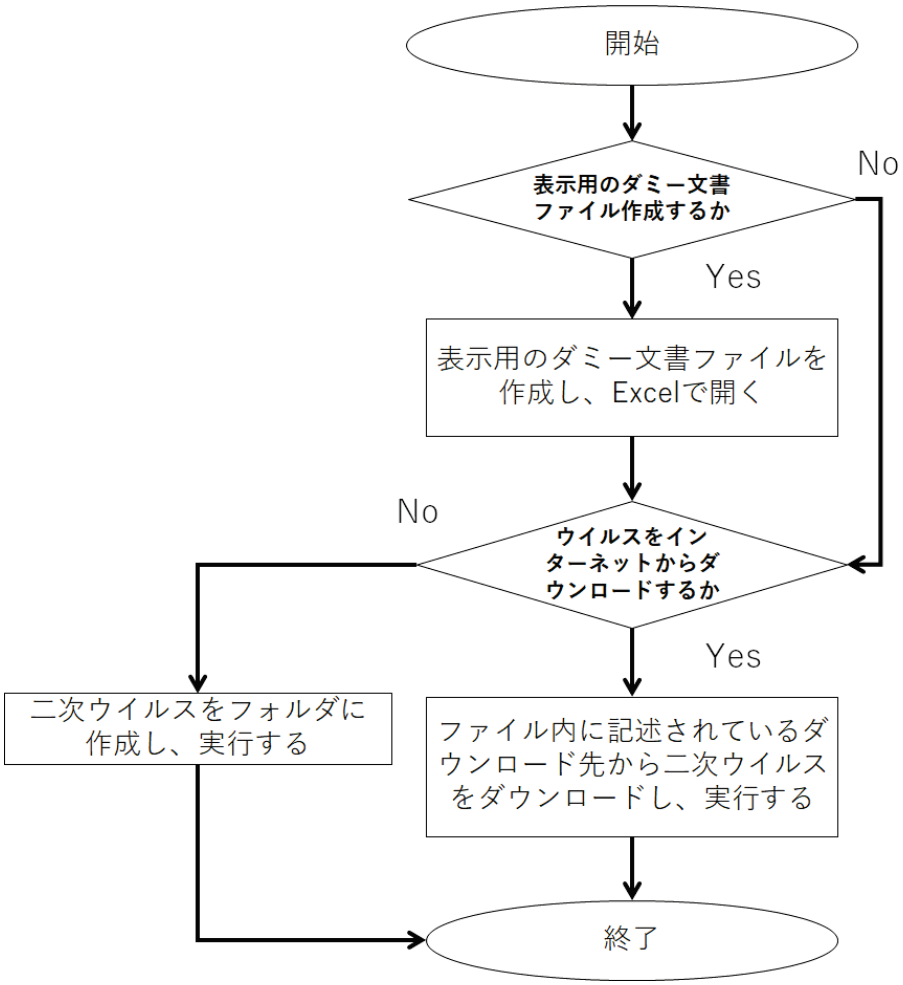

図 4：Excel-DNA を悪用したウイルスの動作

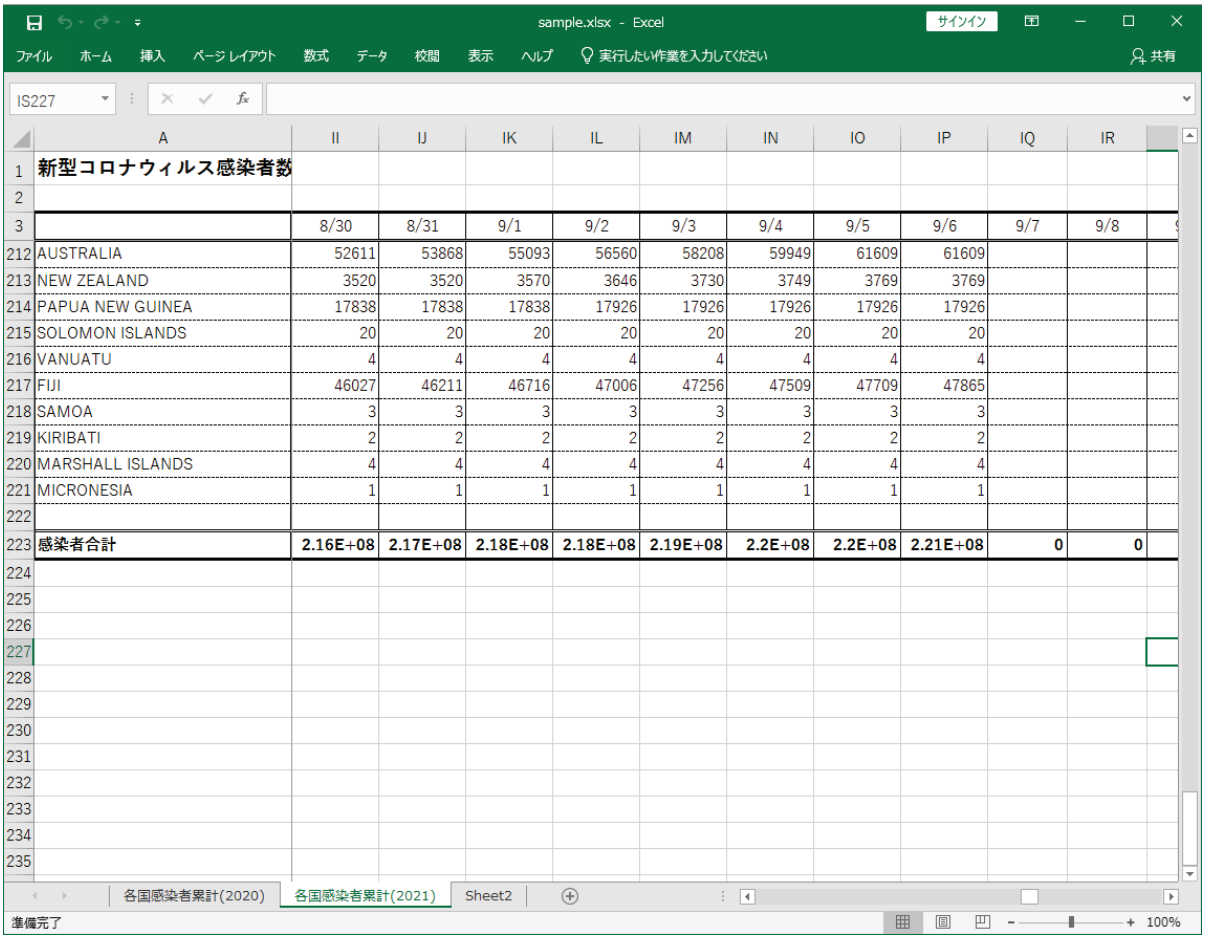

図 5:表示用のダミー文書ファイルの例

3 Excel-DNA を悪用したウイルスの比較結果

IPA で入手した Excel-DNA を悪用したウイルスの多くは図 4 に示す動作を行う。しかし、入手した 59 検体を比較したところ、最終的に感染させるウイルスが存在しない検体、表示用のダミー文書ファイルを作成しない検体、出力するウイルスの形式が異なる検体といった、少数ではあるが、他の同種のウイルスとは異なる動作を行うものを確認した。本章では、それらの異なる動作を行う検体について説明し、攻撃者の環境についての推察を行うとともに、表示用のダミー文書ファイルで使われていた言語から攻撃手法についての推察も行う。最後に、Excel-DNA を悪用したウイルスが出力するファイルの保存先について述べる。

3.1 二次ウイルスの感染有無

59 検体の中に、最終的に感染させる二次ウイルスが存在しない検体を 2 種類確認した。この検体のハッシュ値を表 1 に示す。

表 1:最終的に感染させるウイルスが存在しない検体のハッシュ値

MD5 ハッシュ値	公開情報となった日時(UTC)
31e69207c7690f14bd0de8fb4f523e25	2021-07-26 05:24:52
7ebdfe2eb644a867b1021a32f6b22278	2021-07-26 06:33:13

最終的に感染させる二次ウイルスが存在しない検体をデコンパイルした結果を図 6 に示す。 この検体では、他の検体にてウイルスの取得先 URL が記載されている箇所が「{URL}」となっていた。また、この検体の中にウイルスを作成するデータは含まれていなかった。

この検体は二次ウイルスが存在しないため、情報窃取等の被害は発生しない。そのため、この 2 つの検体は、攻撃者が設定をミスしたか、実験用のものであったものと思われる。なお、デコンパイルしたプログラムに存在する「{URL}」という文字列は、本来攻撃者が二次ウイルスのダウンロード先に設定する箇所であること、またこの中括弧「{}」の表記はテンプレートエンジン等にて置き換え先の文字列として指定されるものであろうことから、Excel-DNA を悪用するウイルスを作成するツールが存在し、それが攻撃者の間で共有されているものと推測される。

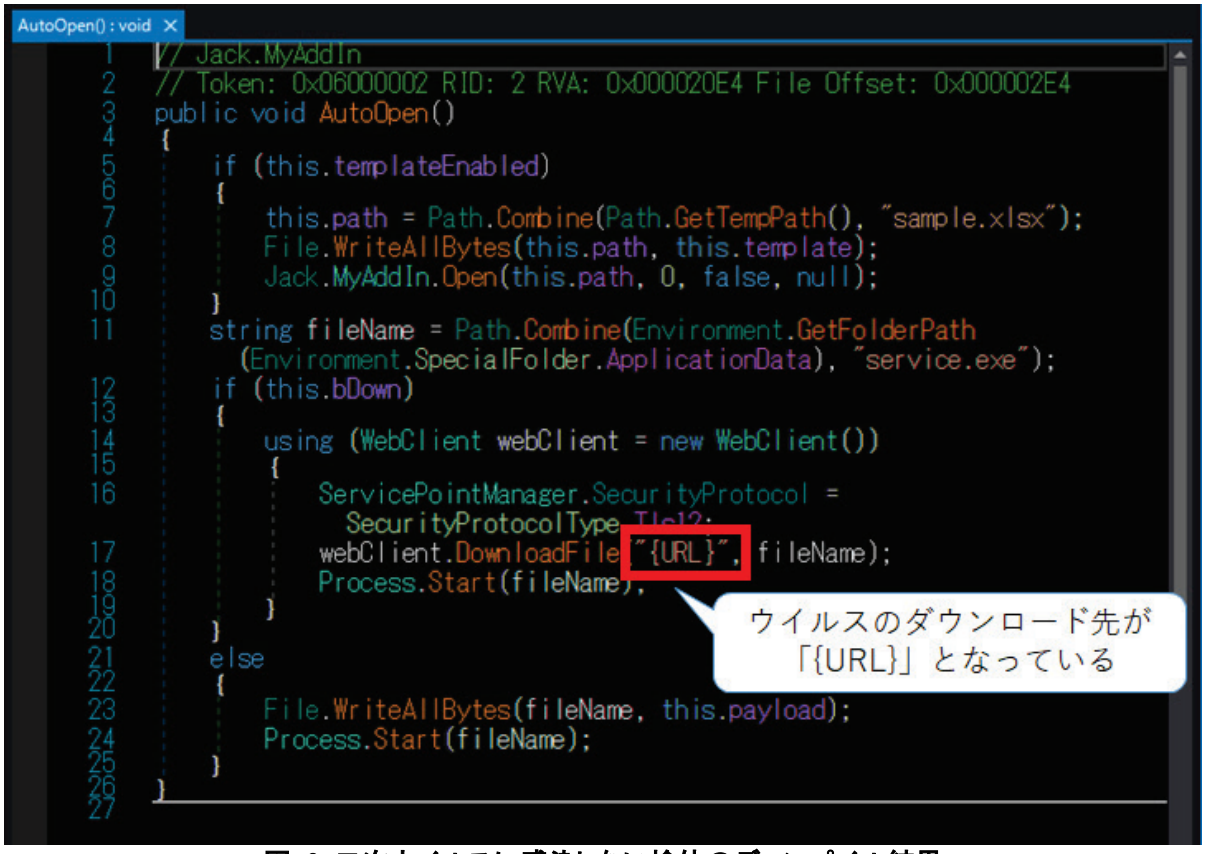

図 6:二次ウイルスに感染しない検体のデコンパイル結果

3.2 表示用のダミー文書ファイル作成の有無

59 検体のうち、47 の検体で表示用のダミー文書ファイルを作成し表示する動作となっていた。これは Excel アドインファイルを実行した利用者に、不審に思わせないための細工と考えられる。一方で、12 の検体では、表示用のダミー文書ファイルを作成しなかった。これらの検体のハッシュ値を表 2 に、またこれらの検体のうち 1 つの検体をデコンパイルした結果を図 7 に示す。表示用のダミー文書ファイルの作成有無について、攻撃者がどのように考えて設定しているのかは不明である

表 2:表示用のダミー文書ファイルを作成しない検体

MD5 ハッシュ値	公開情報となった日時(UTC)
c33eb0934e08e14ea1571b45e377bf4d	2021-07-26 08:09:38
93d9e318b33e2e2d9dfba0d43d2c91ed	2021-07-26 10:09:50
d5e7c01f9e841b6ea9dc9618b3ec8a81	2021-07-26 20:07:01
0ed458621a0e75e9dac09b9cf00b909d	2021-07-27 10:20:46
4c1eae3257dcd4303c4920077c459ebe	2021-08-02 20:50:26
8fa502b4a09f8f304b267f9c70e18de5	2021-08-03 07:38:10
d18cbb60e102844c236b7743813170f8	2021-08-19 11:45:17
fa9791a43abf9f623a66b24df3020c3e	2021-08-19 11:45:26
ba2520c951b5d25ab9df79835cafd1e6	2021-08-24 06:09:21
25167df07568495089acf8ae05573e7a	2021-09-13 16:22:49
c38250c448e02d1bd98d7a315a4d38b8	2021-09-14 22:32:20
19d334f3b4bf738a2347b1a86e87732b	2021-09-18 07:22:26

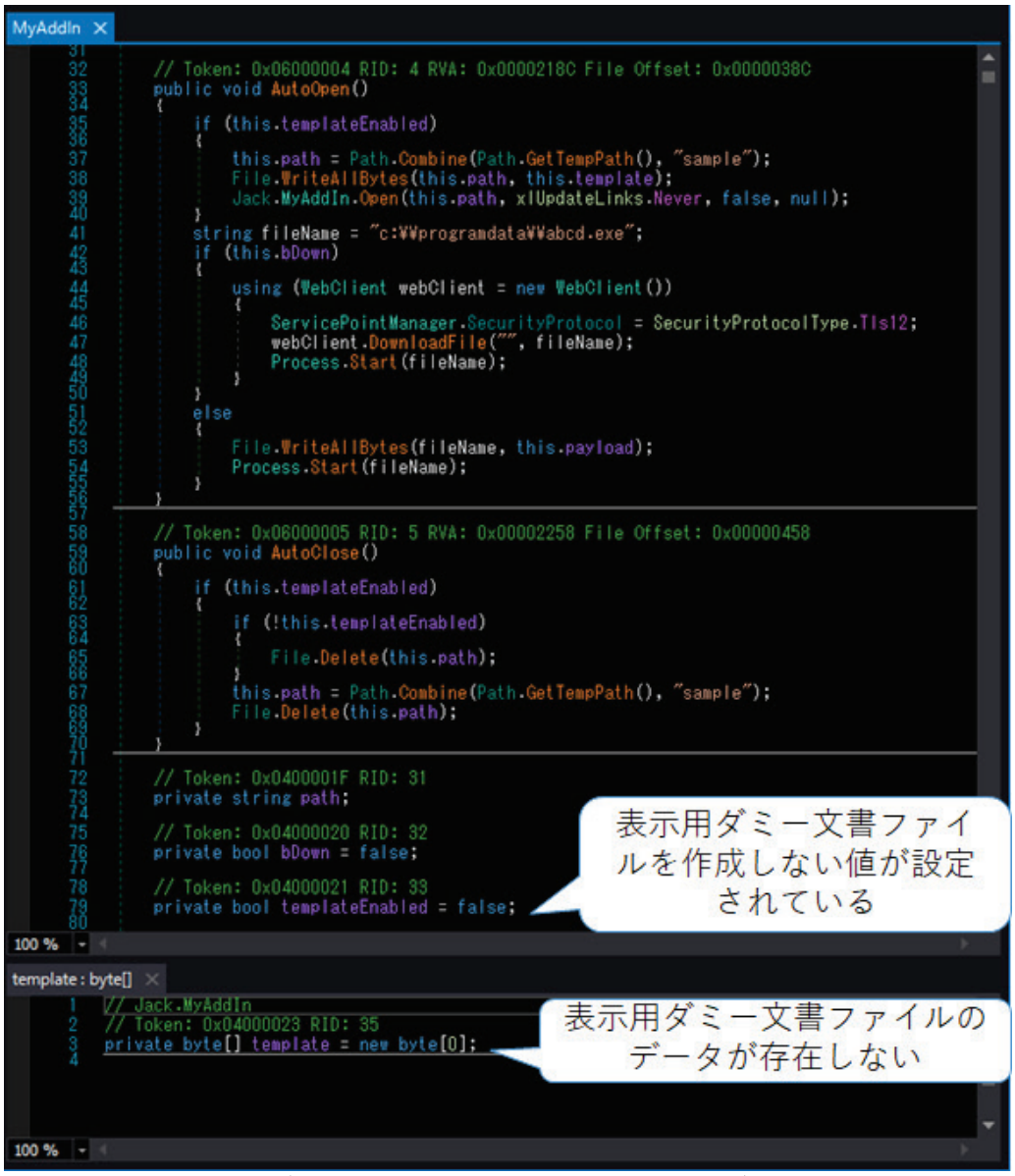

図 7:表示用のダミー文書ファイルを作成しない検体のデコンパイル結果

3.3 出力する二次ウイルスのファイル形式の差異

ここでは 59 検体のうち、二次ウイルスを内包しており、それをファイルに保存して実行する 46 の検体の比較結果について述べる。IPA で確認した検体では、最終的に感染させるウイルスのファイル形式が実行ファイル(拡張子 .exe)形式のものと、JavaScript ファイル(拡張子 .js)形式のものの 2 種類を確認した。JavaScript ファイル形式のものを出力するウイルスのハッシュ値を表 3 に示す。Excel-DNA を悪用するウイルスは 7 月以降多数確認しているが、これらは比較的最近の日時である 2021 年 9 月 27 日に初めて確認した。

表 3:JavaScript ファイル形式のウイルスを出力する検体

MD5 ハッシュ値	公開情報となった日時(UTC)
3c746829102cbd9eca1ee2df94cad3ab	2021-09-27 08:23:46
f840c60876169f5816756d4f7483b5b8	2021-09-27 08:25:10

これら 2 検体について、他の実行ファイルを作成する検体と比較した結果について説明する。実行ファイルを作成する検体のデコンパイル結果を図 8 に示し、JavaScript ファイルを作成する検体をデコンパイルした結果を図 9 に示す。なお、この 2 検体から出力される表示用のダミー文書ファイルおよび JavaScript ファイルはそれぞれ同一のハッシュ値であった。

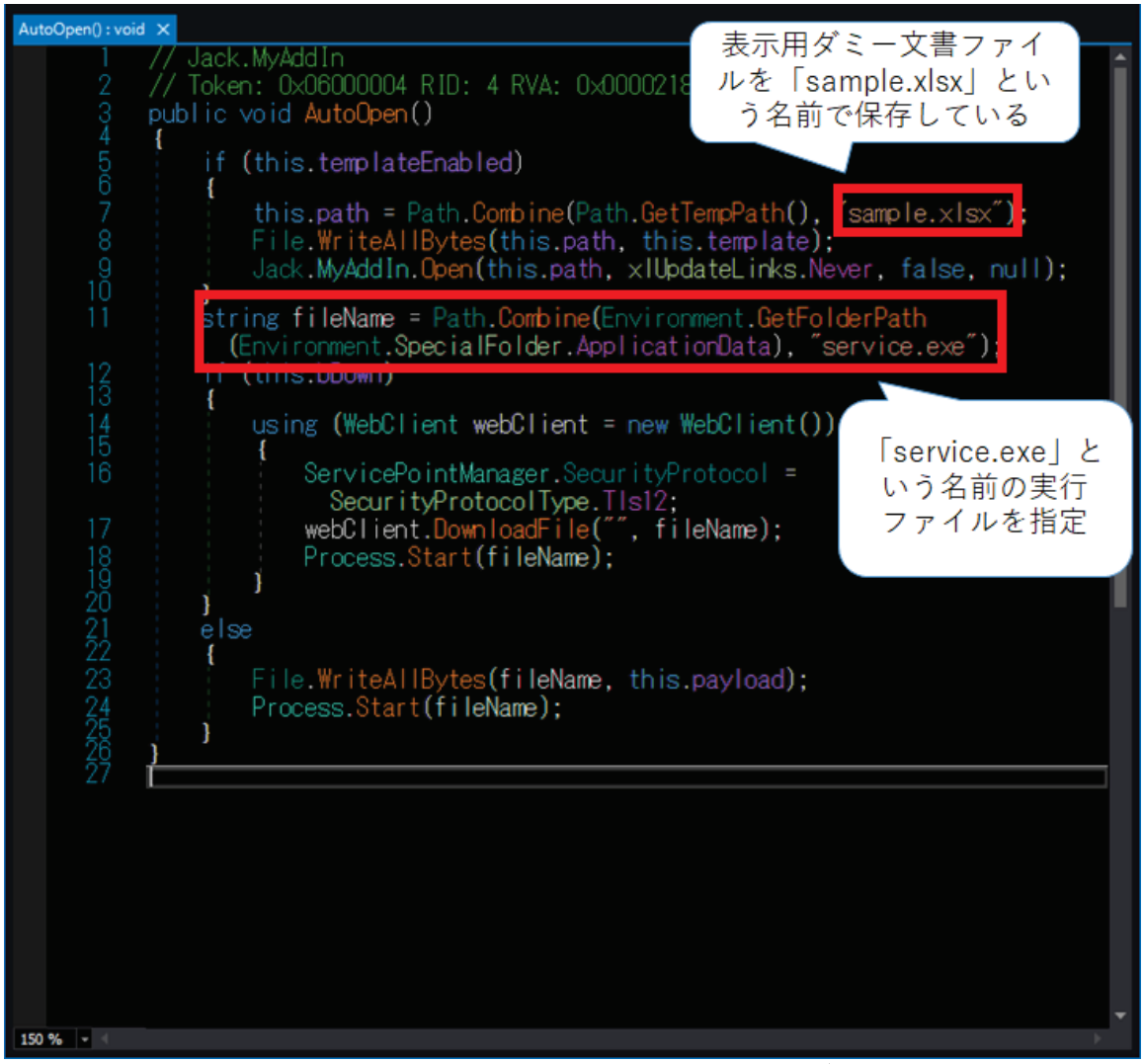

図 8:実行ファイル形式の二次ウイルスを出力する検体のデコンパイル結果

図 9：JavaScript ファイルのウイルスを出力する検体のデコンパイル結果

この 2 検体は、他の多くの検体と同様にはじめに表示用のダミー文書ファイルを作成する。しかし、この際に作成するファイル名は「sample.js」というファイル名であった。ここで、拡張子が「.js」となっているが、ファイルの実体は JavaScript ファイルではなく Excel ファイルであり、図 10 に示すファイルが表示される [7]。その後、「c:¥¥programdata¥¥abcd.js」を作成し、起動する動作を行う。なお、作成される JavaScript ファイルは図 11 に示すように難読化されていた。これは、作成したファイルがウイルスであると検知されないようにする狙いがあるためと思われる。また、JavaScript ファイルを作成する処理では拡張子が別の変数として用意されていた。これは、「.js」以外の拡張子のファイルも簡単に作成できるようにするためと推測する。

[7] 拡張子が.xlsx でないため、開く際に警告画面が表示される。

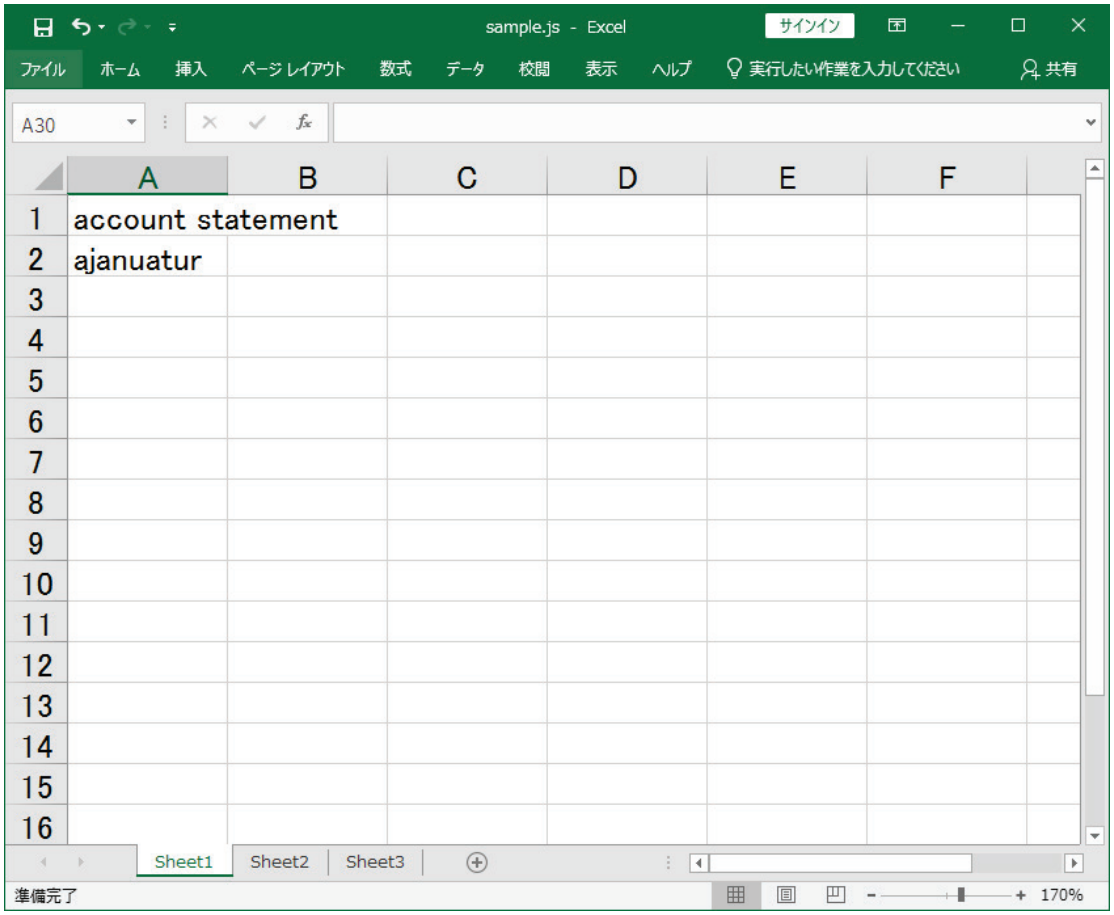

図 10:表示用のダミー文書ファイル(拡張子が「js」となっているもの)

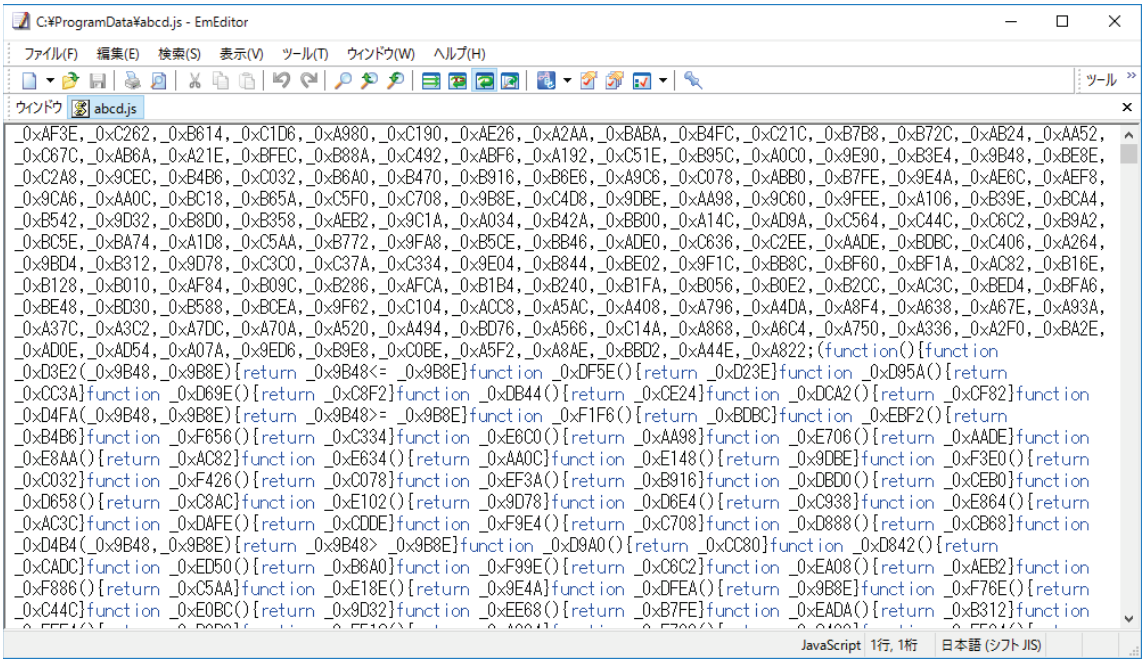

図 11:難読化された JavaScript ファイル

二次ウイルスを内包している検体のうち、多くの検体で二次ウイルスは実行ファイル形式であった。しかし、本節で説明した JavaScript ファイル形式のウイルスを使用する検体が比較的最近発見されていることや、保存するファイルの拡張子を変更可能としている(変数として用意している)ことから、攻撃者はスクリプトファイル等を二次ウイルスとできるようにウイルス作成ツールをアップデートしていると考えられる。今後、実行ファイル形式や JavaScript 形式以外の、別のファイル形式が二次ウイルスとして使われる可能性がある。

3.4 表示用のダミー文書ファイルの種類

今回解析した検体において、使用されていた表示用のダミー文書ファイルは計 13 種類あった。なお、表示用のダミー文書ファイルに使用されていた言語は表 4 の通りである。複数の言語を確認しており、様々な国を標的としていることがわかる。また、日本語のものも 2 種類確認しており、日本も攻撃対象となっていることが明らかである。日本語の表示用ダミー文書ファイルはいずれも新型コロナウイルス感染症(COVID-19)の各国の感染者数をデータとしたものであった [8]。

日本語以外の言語が使用されていた文書ファイルでは、請求書と思われる内容のもの、何らかのデータリストと思われる内容のもの、製品と思わしき画像ファイルのもの等を確認している。これらの表示用のダミー文書ファイルを使用するウイルスのうち一部はメールの添付ファイルであったが、すべてのファイルがメールの添付ファイルであったかは不明である。しかし、「請求書を確認してほしい」、「興味深いデータを入手したので確認してほしい」、「製品の画像を添付したので確認してほしい」といった内容のメールの添付ファイルとして使用し、受信者に開かせるといった、多くのばらまき型の攻撃メールで使われている攻撃方法がこの Excel-DNA を悪用するウイルスを使用した攻撃でも使われていると考えられる。

表 4:表示用のダミー文書ファイルで使用されていた言語

使用されていた言語	数
日本語	2 種類
英語	6 種類
ロシア語	1 種類
アラビア語	1 種類
その他(画像ファイルのみ等、使用されている言語が特定できないもの)	3 種類

3.5 表示用のダミー文書ファイル及び二次ウイルスの出力先

今回解析した検体の、表示用のダミー文書ファイル及び二次ウイルスの保存先のフォルダとファイル名について表 5、表 6 に示す。表示用のダミー文書ファイルの保存先は、確認できたすべての検体で「%TEMP%」フォルダに保存する動作となっていることを確認している。ファイル名については「sample.xlsx」と「sample.js」の 2 つのみであった。

表 5:表示用のダミー文書ファイルの保存先フォルダとファイル名

保存先フォルダ	ファイル名	数
%TEMP%	sample.xlsx	45 種類
%TEMP%	sample.js	2 種類

[8] この表示用ダミー文書ファイルの内容の真偽については検証していない。また、図 5 は 2 種類のうちの 1 つのものである。

表 6:二次ウイルスの保存先フォルダとファイル名

保存先フォルダ	ファイル名	数
%AppData%	service.exe	48 種類
c:¥programdata¥	abcd.exe	7 種類
c:¥programdata¥	abcd.js	2 種類

二次ウイルスの保存先のフォルダは「%AppData%」と「c:¥programdata¥」の箇所を確認しており、ファイル名については「service.exe」、「abcd.exe」、「abcd.js」の 3 つを確認している。

二次ウイルスは、検体によっては起動後自身を削除するものもあるため、必ずしも上記フォルダに検体があるとは限らない。しかし、表示用のダミー文書ファイルについては、通常は削除されないため、不審な Excel アドインファイルを発見した場合、これらのフォルダに拡張子が「.xlsx」、「.exe」、「.js」のファイルがないか確認することでファイルを開いたか否かの判断や、ウイルス感染の早期発見につながると思われる。

4 おわりに

Excel-DNA を悪用したウイルスは 7 月以降英語のばらまき型のメールの添付ファイルとして攻撃に使用されていることを確認しており、9 月からは日本語のばらまき型のメールでも悪用されていることを観測している。今回、IPA で入手した 59 検体の Excel-DNA を悪用したウイルスについて解析を行い、比較を行った結果を通して攻撃者の環境や目的についての推察を行った。

攻撃者は Excel-DNA を悪用したウイルスを作成する共通のツールを使用していることや、このウイルスを作成するツールがアップデートされている可能性が窺えた。攻撃者は攻撃対象に不審と思わせないための表示用のダミー文書ファイル及び最終的に感染させる二次ウイルスを用意することで容易に作成できると思われ、今後この攻撃方法が増加することも考えられる。また、表示用のダミー文書ファイルに使用されている言語を調査した結果、明確に日本語話者を対象としたウイルスが少数ではあるが確認されているため、今後もこのウイルスを使用した攻撃が国内で確認されることが予想される。本攻撃で使用された Excel アドインファイルが出力する表示用のダミー文書ファイルや二次ウイルスの出力先はある程度固定化されているため、不審な Excel アドインファイルを発見した際は、%TEMP%フォルダ、%AppData%フォルダ、c:¥programdata¥フォルダに不審なファイルがないか確認することでウイルスの早期発見につながると思われる。

このようにウイルスの特徴や動作の仕組みを把握することで、企業・組織のセキュリティ担当者においても、サイバー攻撃への対応・対策を検討する上で、役立つものと考えられる。

本書の内容が、企業や組織のセキュリティ対策の一助になれば幸いである。

本書執筆：竹内 俊輝

以上