2023年
4月
APRIL

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

キヤノンマーケティングジャパン株式会社

はじめに

「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

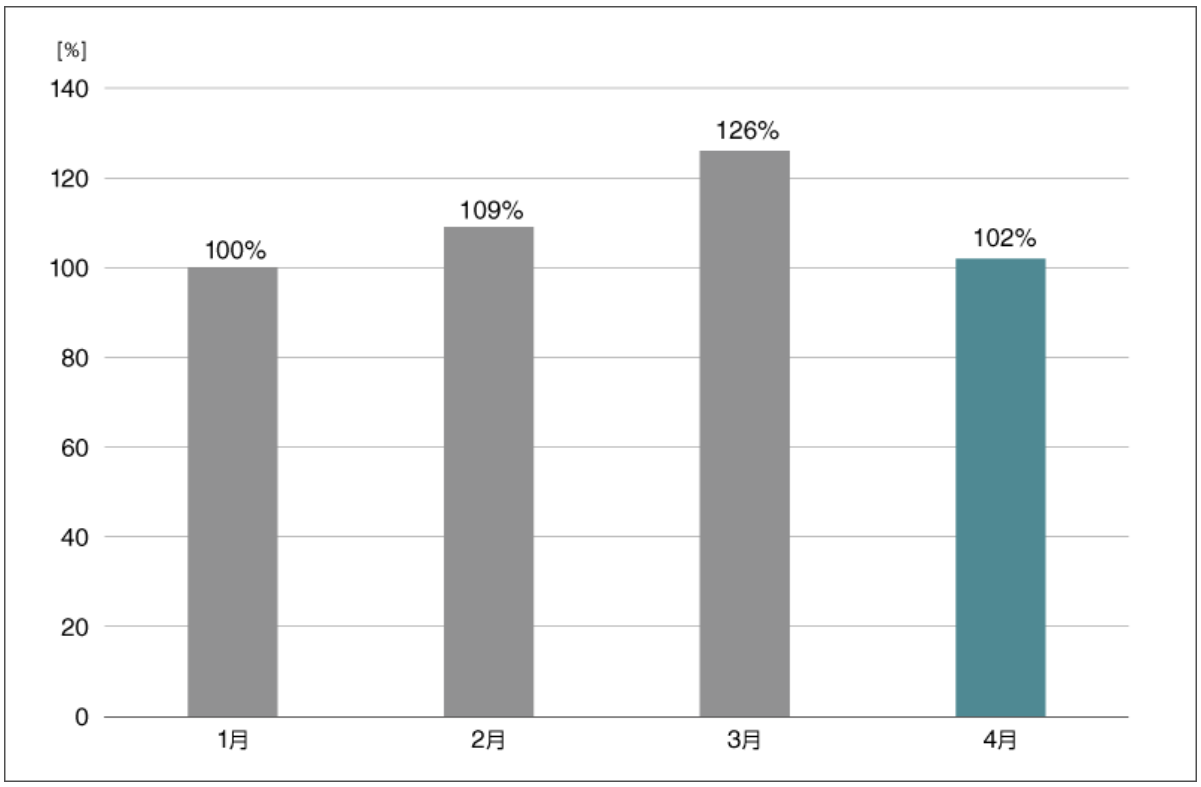
「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

2023 年 4 月マルウェア検出状況

今回のマルウェアレポートより、集計データを刷新し 2023 年の統計を再集計しました。それに伴い、国内マルウェア検出数の推移では 2023 年 1 月以降のデータを掲載しています。

2023 年 4 月（4 月 1 日～4 月 30 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。



国内マルウェア検出数*1の推移

（2023 年 1 月の全検出数を 100%として比較）

*1 検出数には PUA（Potentially Unwanted/Unsafe Application；必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2023 年 4 月の国内マルウェア検出数は、2023 年 3 月と比較して減少しました。検出されたマルウェアの内訳は以下のとおりです。

国内マルウェア検出数[*2]上位（2023 年 4 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	39.1%	アドウェア
2	HTML/Phishing.Agent	12.9%	メールに添付された不正な HTML ファイル
3	JS/Adware.TerraClicks	7.7%	アドウェア
4	HTML/Phishing	2.4%	悪意のある HTML コードの汎用検出名
5	JS/Adware.Sculinst	2.2%	アドウェア
6	DOC/Fraud	2.2%	詐欺サイトのリンクが埋め込まれた DOC ファイル
7	JS/Agent	2.1%	不正な JavaScript の汎用検出名
8	JS/Adware.Popcash	2.1%	アドウェア
9	HTML/Fraud	1.2%	詐欺に用いられる不正な HTML ファイル

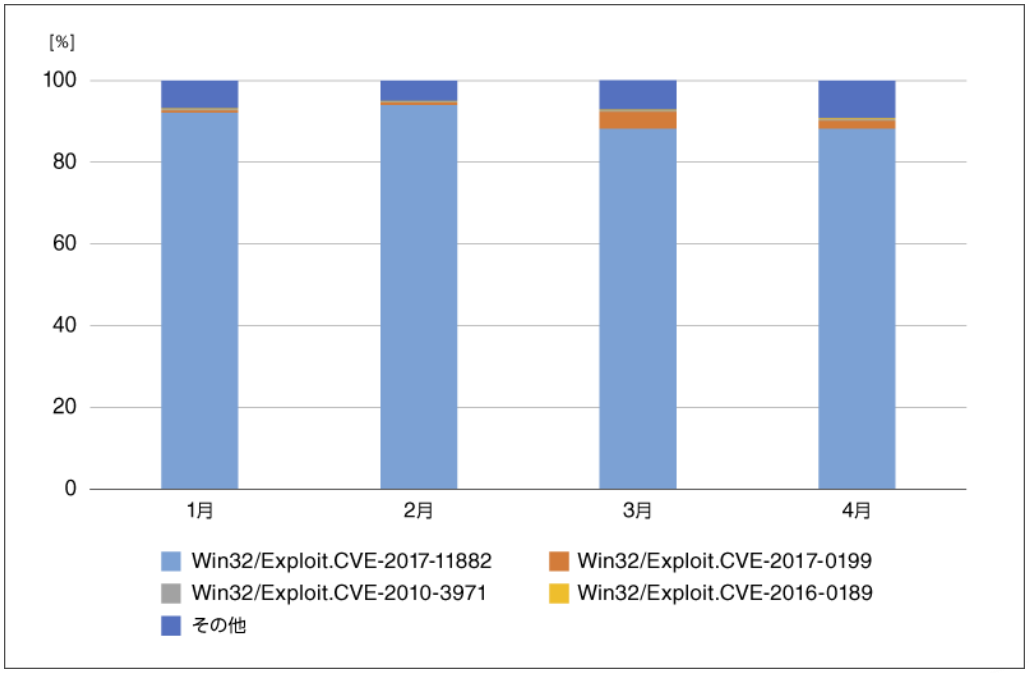
10	Win32/Exploit.CVE-2017-11882	1.1%	エクスプロイト

*2 本表には PUA を含めていません。

4 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

CVE-2017-11882 の国内の検出状況について

今月のマルウェア検出数第 10 位に Win32/Exploit.CVE-2017-11882 がランクインしています。Win32/Exploit.CVE-2017-11882 とは、CVE-2017-11882 の脆弱性を悪用するコードを含むファイルを検出した際に用いられる検出名です。
検出名に特定の CVE 番号を含むマルウェアの検出割合と推移を以下のグラフに示しました。検出数上位 4 種をピックアップして表示しています。



検出名に特定の CVE 番号を含むマルウェアの検出割合と推移

Win32/Exploit.CVE-2017-11882 が全体の 8 割以上を占めており、ほかの検出名と比べて突出しています。このことから、CVE-2017-11882 への対策が疎かになっていると攻撃者に認識されていることが伺えます。今回のマルウェアレポートでは、CVE-2017-11882 がどのように悪用されるのかを説明し、その対策について紹介します。

CVE-2017-11882 の概要

CVE-2017-11882 は Microsoft Office のコンポーネントである数式エディター 3.0（以下、数式エディター）におけるスタックバッファオーバーフローの脆弱性です。古いバージョンの Microsoft Office を使用している場合、攻撃者が作成した悪意ある Word や Excel ファイルの実行時に、ファイル内に仕込まれたコードが実行されます。多くの場合はダウンローダーとして使用され、C&C サーバーと通信した後に Agent Tesla や FormBook などのマルウェアをダウンロードし実行します。[*3]

CVE-2017-11882 の影響を受ける Microsoft Office は以下のとおりです。[*4]

- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 Service Pack 2 （32-bit editions）
- Microsoft Office 2010 Service Pack 2 （64-bit editions）
- Microsoft Office 2013 Service Pack 1 （32-bit editions）
- Microsoft Office 2013 Service Pack 1 （64-bit editions）
- Microsoft Office 2016 （32-bit edition）
- Microsoft Office 2016 （64-bit edition）

*3 2021 年サイバーセキュリティレポートを公開 | サイバーセキュリティ情報局

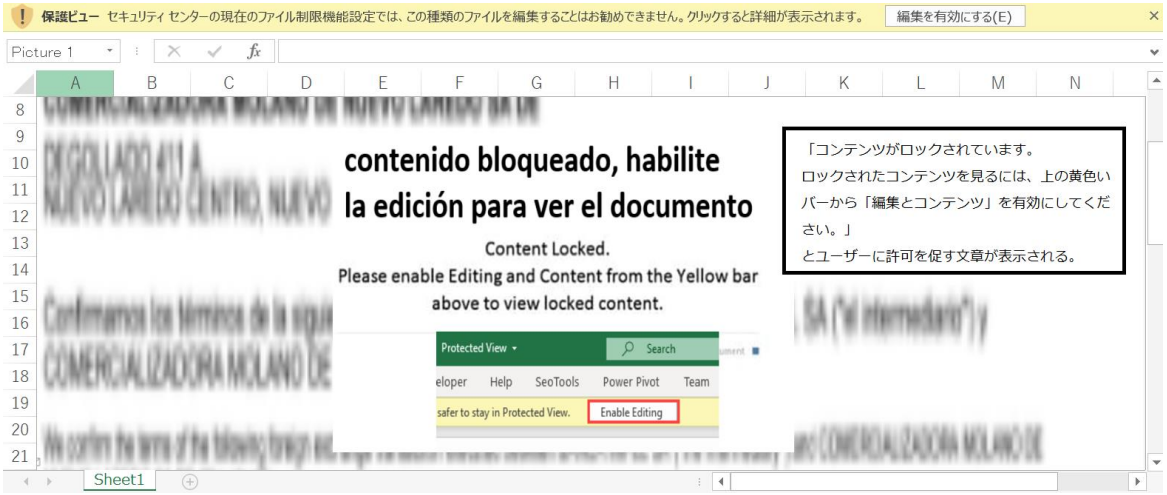
*4 CVE-2017-11882 | Microsoft Security Response Center

CVE-2017-11882 が悪用される流れ

CVE-2017-11882 の脆弱性が悪用される流れを次の Excel ファイルを例に紹介します。この検体は 2023 年 4 月に確認されたフィッシングサイトで配布されていたものと思われます。

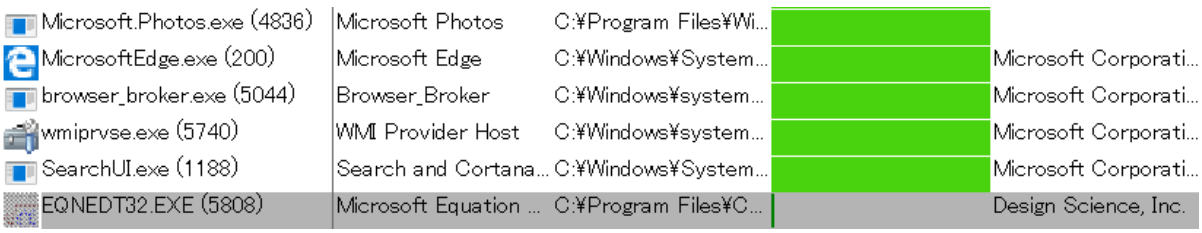
CVE-2017-11882 の脆弱性を悪用する Excel ファイル

この Excel ファイルを実行すると、以下のようにファイル内のコンテンツをすべて表示させることを名目に、ユーザーに編集の有効化を促す画像が表示されます。



Excel ファイルを実行した際に表示される画像

右上に表示されている「編集を有効にする」をクリックした場合、自動的に数式エディターが立ち上がり、スタックバッファオーバーフローが発生した後に攻撃者が用意したコードが実行されます。
実際に編集を許可してみると、以下のように Process Monitor[*5] のプロセス一覧に EQNEDT32.EXE が現れます。この EQNEDT32.EXE が Microsoft Office の数式エディターです。数式エディター起動時に特定のウィンドウが立ち上がるなどの動作はなく、ユーザーに気付かれにくい形でコードが実行されます。



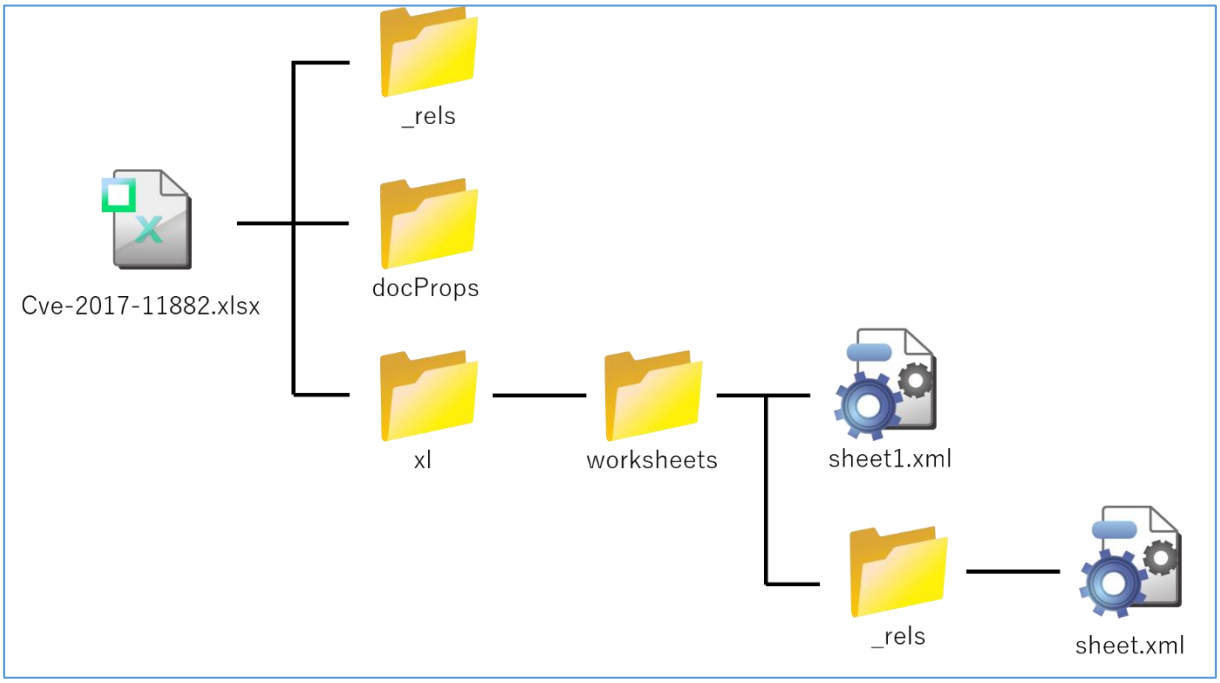
Process Monitor のプロセス一覧（一部）

*5 Process Monitor | サイバーセキュリティ情報局

どのようなコードが実行されるのかを確認するために、以下の手順で Excel ファイルを調査しました。なお、以下に示すファイル名や値は、検体によって異なります。

① 該当の Excel ファイルを解凍する

Excel ファイルは XML ファイルなどの構成要素を 1 つのファイルに圧縮したものです。そのため、Excel ファイルを解凍することで、依存関係を記した XML ファイルやマクロなどの内容物を個別に確認することが可能です。



Excel ファイルのファイル構造

② sheet1.xml を確認する

worksheets フォルダーにある sheet1.xml を確認します。

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<worksheet xmlns:x14ac="http://schemas.microsoft.com/office/spreadsheetml/2009/9/ac" mc:Ignorable="x14ac"
xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships"
xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main">
    <dimension ref="A1"/>
  + <sheetViews>
    <sheetFormatPr x14ac:dyDescent="0.45" defaultRowHeight="14.25"/>
    <sheetData/>
    <pageMargins footer="0.3" header="0.3" bottom="0.75" top="0.75" right="0.7" left="0.7"/>
    <drawing r:id="rId1"/>
    <legacyDrawing r:id="rId3"/>
  - <oleObjects>
        <oleObject r:id="rId2" autoLoad="true" shapeId="1752" progId="iSlPE9FffTbpln6ARrnasmh9fD8tUpQzh"/>
    </oleObjects>
</worksheet>
```

sheet1.xml の内容

oleObjects として指定されているものが実行されるコードです。id が rId2 であることを覚えておきます。

③ _rels フォルダー内の sheet.xml を確認する

worksheets/_rels フォルダーにある sheet.xml を確認します。

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Target="../drawings/drawing1.xml"
        Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/drawing" Id="rId1"/>
    <Relationship Target="../drawings/vmlDrawing1.vml"
        Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/vmlDrawing" Id="rId3"/>
    <Relationship Target="../embeddings/i1H.1Xjab"
        Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Id="rId2"/>
</Relationships>
```

sheet.xml の内容

Id が rId2 である要素のターゲットは embeddings フォルダーの i1H.1Xjab です。このファイル内に記された数式が実行されます。

④ Relationship target として指定されているファイルを確認する

スタックバッファオーバーフローを引き起こすコードを含むファイル

i1H.1Xjab はファイルサイズがかなり大きく、Excel ファイルの大部分を占めています。このコードがスタックバッファオーバーフローを引き起こし、結果として攻撃者の用意したコードが実行される仕組みとなっています。

今回の検体は、外部と通信を行い不審な VBS ファイルをダウンロードするものでした。
Win32/Exploit.CVE-2017-11882 を悪用する攻撃については、2021 年のサイバーセキュリティレポートでも詳しく取り上げています。[*6]

*6 2021 年サイバーセキュリティレポートを公開 | サイバーセキュリティ情報局

CVE-2017-11882 の脆弱性への対応策

CVE-2017-11882 の脆弱性への対応策は以下のとおりです。
① 最新バージョンの Microsoft Office にアップデートする
② Microsoft Office の数式エディターを無効化する[*7]

CVE-2017-11882 を引き起こす数式エディターは 2018 年 1 月のアップデートで削除されています。旧バージョンを利用する特段の理由がない場合は、対応策①を実施してください。対応策②はあくまで CVE-2017-11882 の脆弱性を回避するための一時的な対策です。

2023 年 4 月に Microsoft Office 2013 のサポートが終了しました。今後緊急性の高い脆弱性が発見されても Microsoft 社からアップデートは提供されません。可能な限り早急にアップグレードを実施することを推奨します。[*8]

*7 数式エディター 3.0 を無効にする方法 | Microsoft 365 サポート
*8 Office 2013 のサポート終了 | Microsoft 365 サポート

まとめ

前月のマルウェアレポートでは、OneNote 形式で感染を広げるマルウェアを紹介しました。しかし、今月紹介した Win32/Exploit.CVE-2017-11882 のように、Word ファイルや Excel ファイルを利用して感染を広げるマルウェアが減少しているわけではありません。メールに添付されていたファイルや Web 上からダウンロードしたファイルなど、出所の不確かなファイルを開く際は、「それが安全なものであるか」を一度立ち止まって考える必要があります。
また、十分に警戒していても、対策をすり抜けたマルウェアに感染する恐れがあります。そうした状況に備え、日頃から利用しているソフトウェアに関する情報を収集し、必要な対応策や回避策を実施しておくことが大切です。

■常日頃からリスク軽減するための対策について
各記事でご案内しているようなリスク軽減の対策をご案内いたします。下記の対策を実施してください。

１．セキュリティ製品の適切な利用

1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しています。最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新の状態にアップデートしてください。

1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

２．脆弱性への対応

2-1. セキュリティパッチを適用する

マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。「Windows Update」などの OS のアップデートを行ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

３．セキュリティ教育と体制構築

3-1. 脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

3-2. インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

４．情報収集と情報共有

4-1. 情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

4-2. 情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

引用・出典元

■2021 年サイバーセキュリティレポートを公開 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/220316.html
■CVE-2017-11882 | Microsoft Security Response Center
https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2017-11882
■Process Monitor | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/220725.html
■数式エディター 3.0 を無効にする方法 | Microsoft 365 サポート
https://support.microsoft.com/ja-jp/topic/%E6%95%B0%E5%BC%8F%E3%82%A8%E3%83%87%E3%82%A3%E3%82%BF%E3%83%BC-3-0-%E3%82%92%E7%84%A1%E5%8A%B9%E3%81%AB%E3%81%99%E3%82%8B%E6%96%B9%E6%B3%95-7e000f58-cbf4-e805-b4b1-fde0243c9a92
■Office 2013 のサポート終了 | Microsoft 365 サポート
https://support.microsoft.com/ja-jp/office/office-2013-%E3%81%AE%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88%E7%B5%82%E4%BA%86-90e4b0d1-098f-4656-b6e7-8b13b67ed62f#:~:text=2023%20%E5%B9%B4%204%20%E6%9C%88%2011%20%E6%97%A5%E4%BB%A5%E9%99%8D,%E7%B5%82%E4%BA%86%E3%81%8C%E6%84%8F%E5%91%B3%E3%81%99%E3%82%8B%E3%82%82%E3%81%AE&text=Microsoft%20Update%20%E3%81%8B%E3%82%89%20Office%202013,%E3%81%93%E3%81%A8%E3%81%8C%E3%81%A7%E3%81%8D%E3%81%AA%E3%81%8F%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82

Canon

キヤノンマーケティングジャパン株式会社