LANSCOPE
Endpoint Manager

LANSCOPE
Cyber Protection

最恐のマルウェア “EMOTET”に どう対抗するか

はじめに

「Emotet（エモテット）」というマルウェアは、日本では2020年に大流行しました。翌2021年1月27日、欧州各国によるOperation Ladybird が Emotet サーバーをテイクダウンしました。そのため、現時点では Emotet は無害化しています。しかしながら、日本国内では引き続き Emotet の感染端末が存在しており、認証情報の窃取や、他マルウェアへの二次感染の可能性もあります。

テイクダウンの結果、現在は感染被害のある組織に対して通知を行うことができるようになっています。2019年は4月と9月に大規模なEmotet のばらまき型攻撃が観測された際、JPCERT コーディネーションセンター（JPCERT/CC）は、マルウェア「Emotet（エモテット）」に感染した国内の組織が少なくとも約3,200組織に上ることを明らかにしました。これは同日時点でJPCERT/CC に寄せられた情報をもとに感染が確認されたものであるため、報告されていないケースを考えるとさらに多くの企業が Emotet の感染被害にあっていると想定されます。

特に2020年9月は急激な被害増加がみられ、エムオーテックスに対しても、「Emotet に感染してしまった」「Emotet の被害を防ぎたい」というご相談が相次ぎました。このホワイトペーパーでは、Emotet の特徴と、有効な対応策について解説します。本資料が、皆様の組織のセキュリティ対策強化の一助になりましたら幸いです。

【2022年4月21日追記】
2022年3月9日 IPA の報告では、Emotetの被害件数が急増しているようです。
3月1日～8日に、323件もの相談が寄せられたそうで、先月同時期（2月1日～8日）の、約7倍になります。
また、JPCERT/CCからも「Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年のピーク時の約5倍以上に急増」しているとの注意喚起が
ありました。メール経由で入手したOffice 文書ファイルは、信用できないものはクリックしないように注意してください。

【参考】感染再拡大に関する注意喚起

出典：JPCERT/CC
マルウェアEmotetの感染再拡大に関する注意喚起（2022年4月26日）
https://www.jpcert.or.jp/at/2022/at220006.html

Emotet の侵入経路

Emotet は、メールに添付したMicrosoft Word 文書ファイルのマクロを利用して端末へ侵入・感染するという手法での攻撃が確認されています。

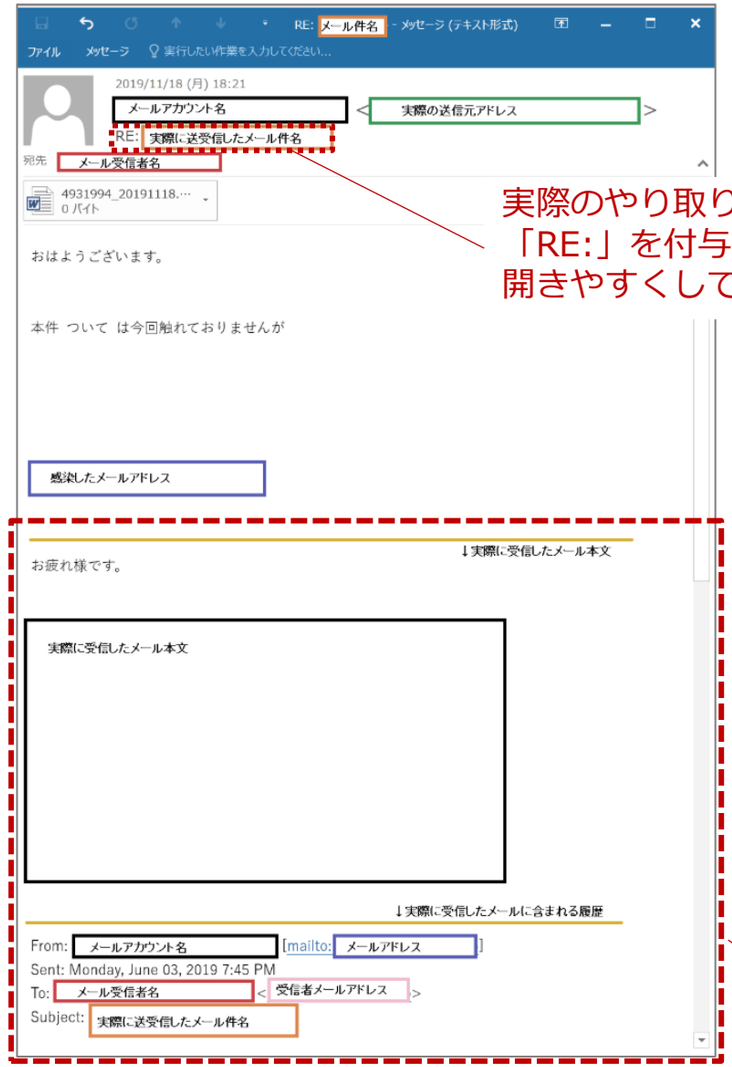
Emotet 拡散の目的でばらまかれたメールには、Microsoft Word 文書ファイルが添付されており、添付ファイルを開くと、マクロコンテンツを有効化するように求められます。

ここでコンテンツの有効化をしてしまうと、複数のコマンドや Powershell が実行され、最終的には不正サーバーへ接続され Emotet の本体ファイルがダウンロード・実行され、感染します。

Emotet の危険な点として、このばらまきメールが非常に巧妙であるという点が挙げられます。

実は Emotet 自体に感染させた端末のOutlook のメール情報を窃取する機能が備えられています。正規にやり取りされているメールに「re：」をつけて実際のメールの返信を装い、元のメールのスレッドに割り込む形で Emotet のダウンロードを誘導するメールを配信するため、Emotet のばらまきメールであることを見破るのが非常に難しいといえます。

▼ **Emotetの感染メールのイメージ**



実際のやり取りのメール件名に「RE:」を付与することでメールを開きやすくしている

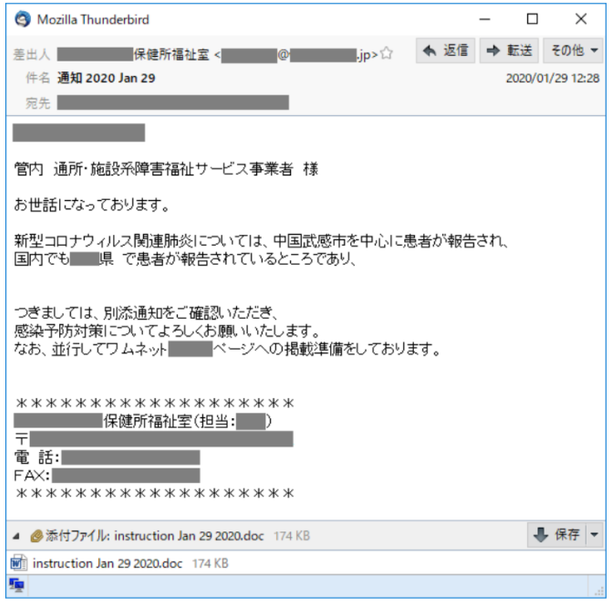
実際のやり取りのメール本文を引用

出典：JPCERT/CC

より巧妙さを増す Emotet ばらまきメールの例

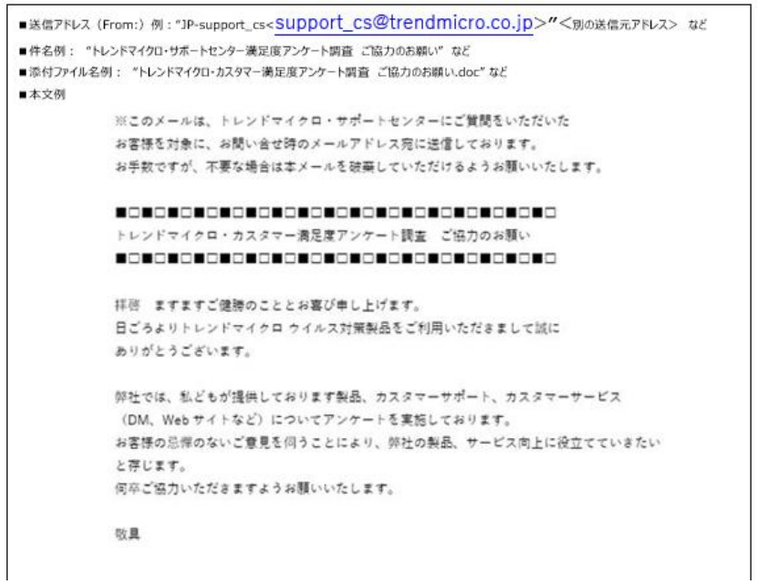
2019年11月頃には、正規にやり取りされているメールに「RE：」をつけて実際のメールの返信を装う手法が多く確認されていましたが、2020年に入って以降、新型コロナウイルスの注意喚起を装ったものや、企業のアンケートを装ったものなど、新たなバリエーションが確認されています。その巧妙さはさらに進化しており、Emotet のばらまきメールであると見破ることは、ますます難しくなっています。

地域の保健所から、新型コロナに関する注意喚起の書面が添付されたと装ったメール



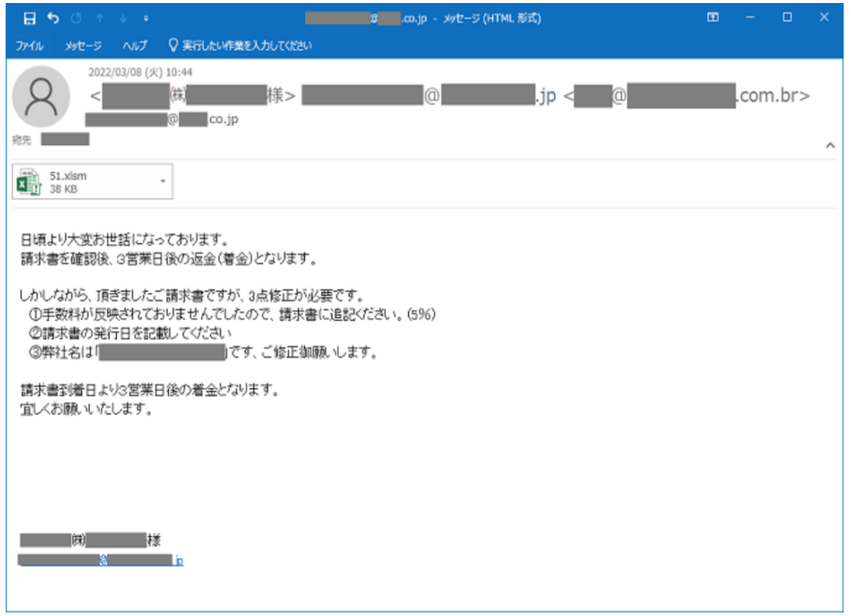
出展：IPA
『「Emotet」と呼ばれるウイルスへの感染を狙うメールについて』
https://www.ipa.go.jp/security/announce/20191202.html

セキュリティメーカーからのアンケートを添付していると装ったメール



出展：トレンドマイクロ
『「EMOTET」がトレンドマイクロのアンケートメールを偽装』
https://blog.trendmicro.co.jp/archives/26049

ファイルを開かせるために必要な情報の入力を迫るメール

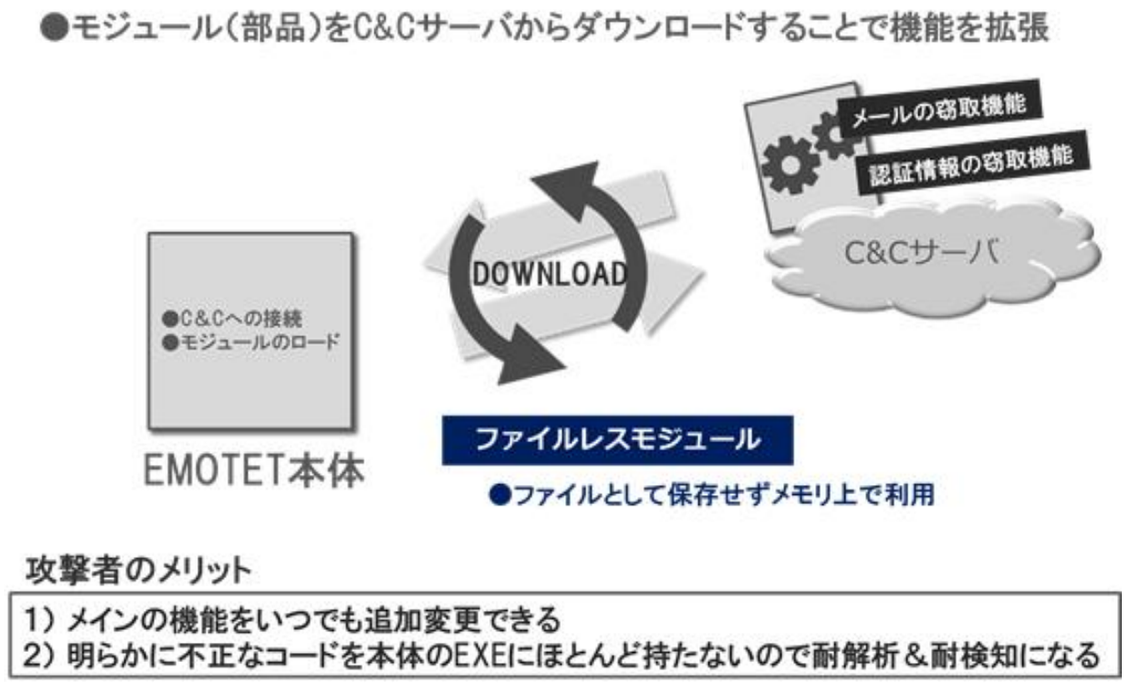


出展：IPA
『「Emotet」と呼ばれるウイルスへの感染を狙うメールについて』
https://www.ipa.go.jp/security/announce/20191202.html

Emotet の危険性＝見つかりにくいさまざまな工夫

実はEmotet 本体には不正なコードが多く含まれていません。Emotet 自体は他のマルウェアを感染させるプラットフォームとしての機能がメインであり、情報窃取などの不正な動作をするモジュールを、攻撃者が用意したサーバー（C&Cサーバー）からダウンロードし、活動します。ダウンロードしたモジュールも、端末にファイルとして保存せずに端末のメモリ上で動作させるファイルレスな仕組みも取り入れており、セキュリティ調査者から解析されにくい工夫がされているといえます。

Emotet にはこの他にもセキュリティ担当者から見つかりにくくするさまざまな工夫が施されており、気づかない間にネットワークに潜伏し、不正な活動を行っている恐れがあります。従来型のアンチウイルス製品では検知できない可能性が高いため、専門機関による診断サービス等を活用し、Emotet が組織のネットワーク内に潜伏していないかを調査することをお勧めします。



出典：三井物産セキュアディレクション　流行マルウェア「Emotet」の内部構造を紐解く(2018/12/25)
https://www.mbsd.jp/blog/20181225_2.html

感染有無確認ツール「EmoCheck」

「EmoCheck」とは、JPCERT/CCが提供する、Emotet感染有無の確認を行うツールです。ソースコード共有サービスの「GITHUB」にて無料公開されており、誰でもダウンロードし、利用できます。

検査をしたいPCで実行すると検索画面が表示され、感染の有無を知らせるというシンプルな構成になっています。感染が発覚した場合は感染先を含むフォルダのイメージパスを表示し、対処をサポートします。

▼ダウンロードはこちら
JPCERTCC/EmoCheck - GitHub
https://github.com/JPCERTCC/EmoCheck/releases

エンドポイントマネージャー オンプレミス版を活用して、複数の端末に対してEmoCheckツールを配布し、ツールの実行結果を指定した共有サーバーにアップロードする手順をご紹介しています。
定期的なEmoCheckの活用にぜひご活用ください。

詳細はこちら▶https://www.lanscope.jp/trend/17714/

Emotet に感染するとどうなるの？

社内にEmotet に感染した端末が存在した場合、主に次の4つの被害が発生します。

①重要な情報を盗み取られる
②ランサムウェアに感染する
③社内の他の端末にEmotet が伝染する
④社外へのEmotet ばらまきの踏み台にされる

①重要な情報を盗み取られる

Emotet が媒介して情報を窃取するモジュールがダウンロードされ、認証情報などのさまざまな情報がC&Cサーバーへ送信されて悪用されます。

②ランサムウェアに感染する

ランサムウェアやワイパーがダウンロードされ、端末内のデータを暗号化、もしくは破壊して活動の痕跡を消し去ってしまいます。
こうなると、Emotet によってどのような情報が漏洩したのかの調査すらできなくなってしまいます。
また、ランサムウェア(※1)やワイパー(※２)の被害により端末自体が利用できなくなり、復旧作業を行う間業務がストップしてしまいます。

③社内の他の端末にEmotet が伝染する

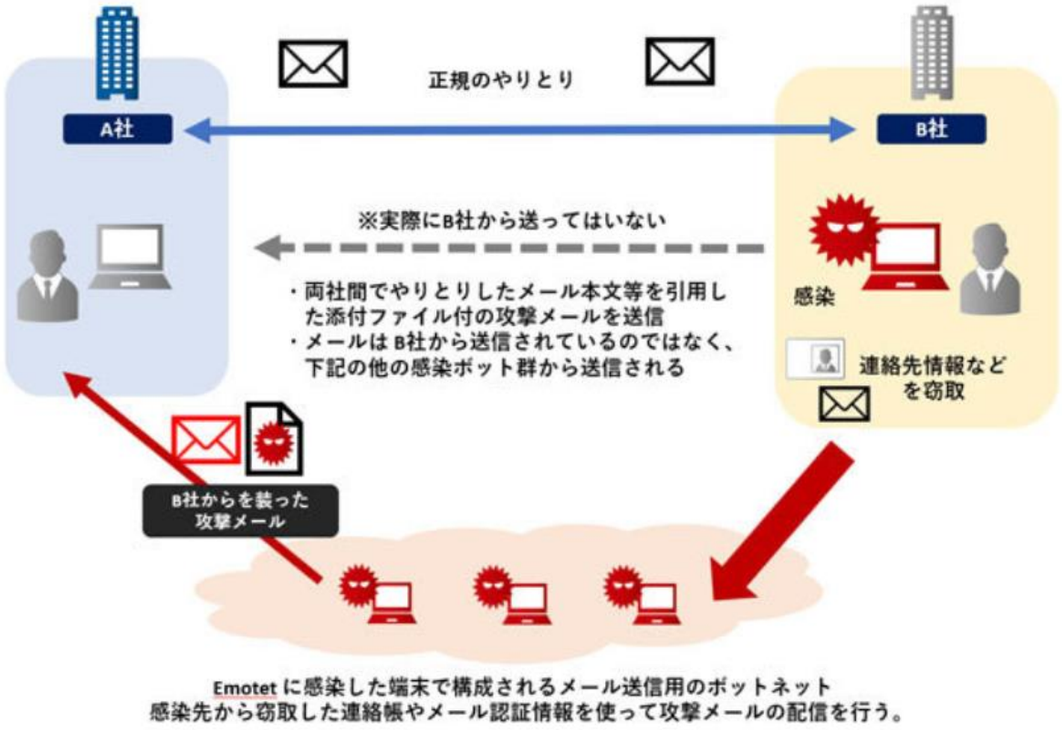
Emotet は自己増殖するワーム機能を有しており、ひとたびネットワーク内に侵入すると、保護機能の隙間を探し、ネットワーク内の他の端末への侵入を試みます。
Emotet はネットワークに侵入し、端末に潜伏して活動を行いながらも頻繁にアップデートが行われていることも確認されています。もしOS に新たな脆弱性が発見されたら、組織内で爆発的に感染が拡大する恐れもあります。

※１：ハードディスクドライブを暗号化するなどしてシステムへのアクセスを制限し、制限を解除するため、被害者がマルウェアの作者に身代金を支払うよう要求するマルウェア
※２：コンピュータの中にあるファイルやデータの破壊、あるいはコンピュータのシステム自体の破壊のみを目的としたマルウェア

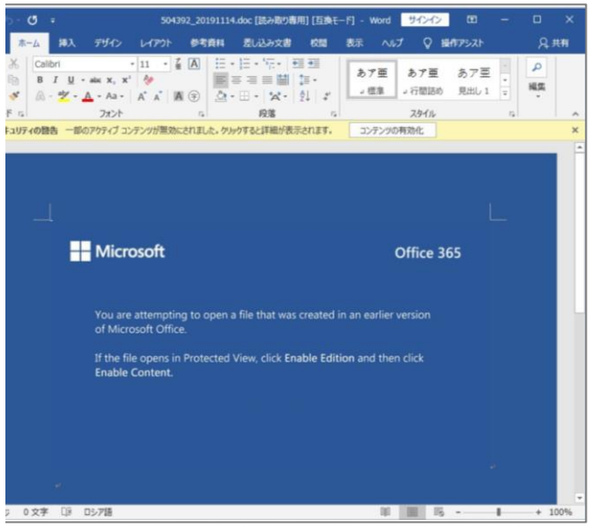
Emotet に感染するとどうなるの？

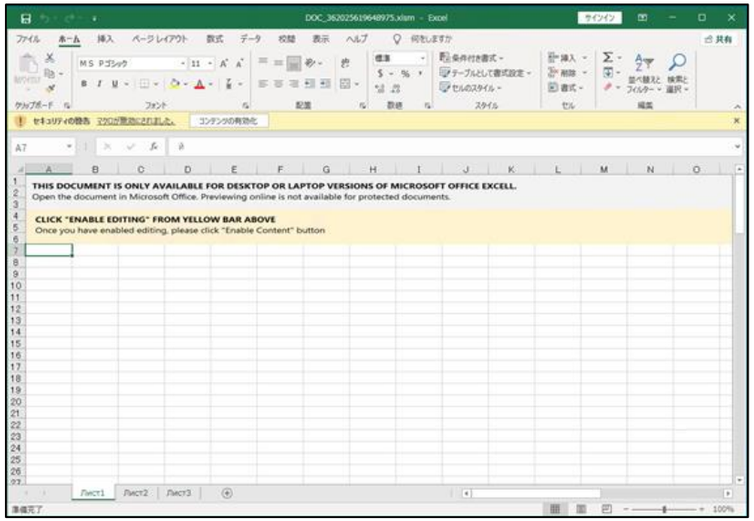
④社外への Emotet ばらまきの踏み台にされる

Emotet で窃取したOutlook のメール情報を利用し、取り引き先や顧客へEmotet のばらまきメールを配信します。さらにEmotet 感染端末が増加するだけでなく、顧客へのばらまきメールが発生した場合には顧客への注意喚起や補償の対応が必要となり、企業のブランドイメージの低下につながります。



▼ Emotetの感染メールに添付されるファイルのイメージ





出典：JPCERT/CC

Emotet の感染予防策

ここまで、国内で猛威を振るう Emotet について、その特徴と感染した場合の影響について解説してきました。
Emotet の特徴を踏まえると、対策のポイントとしては次の3点があげられます。

Emotet の特徴	対応策
メール添付したMicrosoft Word やExcel ※のマクロを利用してEmotet の本体ファイルをダウンロードし、感染する。	マクロの利用に対してセキュリティ製品で制御を行う。
情報窃取などの活動を行う際には、専用のモジュールをダウンロードし、メモリ上で動作させる。	メモリ上の不審な動作に対して対策ができるセキュリティ製品を活用する。
ワーム機能を有しており、ネットワーク内で自己増殖し、感染端末を増加させる。	境界型ではなくエンドポイントでのマルウェア対策（アンチウイルス）を強化する。

※2021年11月16日に確認された Emotet は攻撃に Excel も利用していることが報告されています。

また前提として基本的な対策が行われていることも非常に重要となります。
Emotet への対策の基本として、JPCERTコーディネーションセンターでも以下の対策を推奨しています。

●組織内への注意喚起の実施

マクロの自動実行の無効化（事前にセキュリティセンターのマクロの設定で「警告を表示してすべてのマクロを無効にする」を選択しておく）
メールセキュリティ製品の導入によるマルウェア付きメールの検知
メールの監査ログの有効化
OS に定期的にパッチを適用（SMB の脆弱性を突く感染拡大に対する対策）
定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）

出典：JPCERT/CC　マルウェア Emotet の感染拡大および新たな攻撃手法について（2020-09-04）　https://www.jpcert.or.jp/newsflash/2020090401.html

Emotet に感染してしまったら…実施すべきアクション

万が一、Emotet に感染してしまった場合、どのようなアクションを行ったらよいかを解説させていただきます。
Emotet の感染後の動きとして、JPCERTコーディネーションセンターで以下をご案内されています。

■感染端末の隔離、証拠保全、および被害範囲の調査
・感染した端末を証拠保全する
・端末に保存されていた対象メール、およびアドレス帳に含まれていたメールアドレスの確認(端末に保存されていたこれらの情報が漏洩した可能性がある)

■感染した端末が利用していたメールアカウントなどのパスワード変更
・Outlook や Thunderbird などのメールアカウント
・Webブラウザに保存されていた認証情報　など

■感染端末が接続していた組織内ネットワーク内の全端末の調査
・横断的侵害で組織内に感染を広げる能力を持っているため、添付ファイルを開いた端末だけでなく、他の端末も併せて調査を実施する

■ネットワークトラフィックログの監視
・感染端末を隔離できているか、他の感染端末がないかの確認

■他のマルウエアの感染有無の確認
・Emotet は別のマルウエアに感染させる機能を持っているため、Emotet 以外にも感染していたか調査する。
　もし、別のマルウエアに感染していた場合には、更なる調査・対応が必要となる。

■被害を受ける (攻撃者に窃取されたメールアドレス) 可能性のある関係者への注意喚起
・調査で確認した対象メール、およびアドレス帳に含まれていたメールアドレスを対象
・不特定多数の場合は、プレスリリースなどでの掲載

■感染した端末の初期化

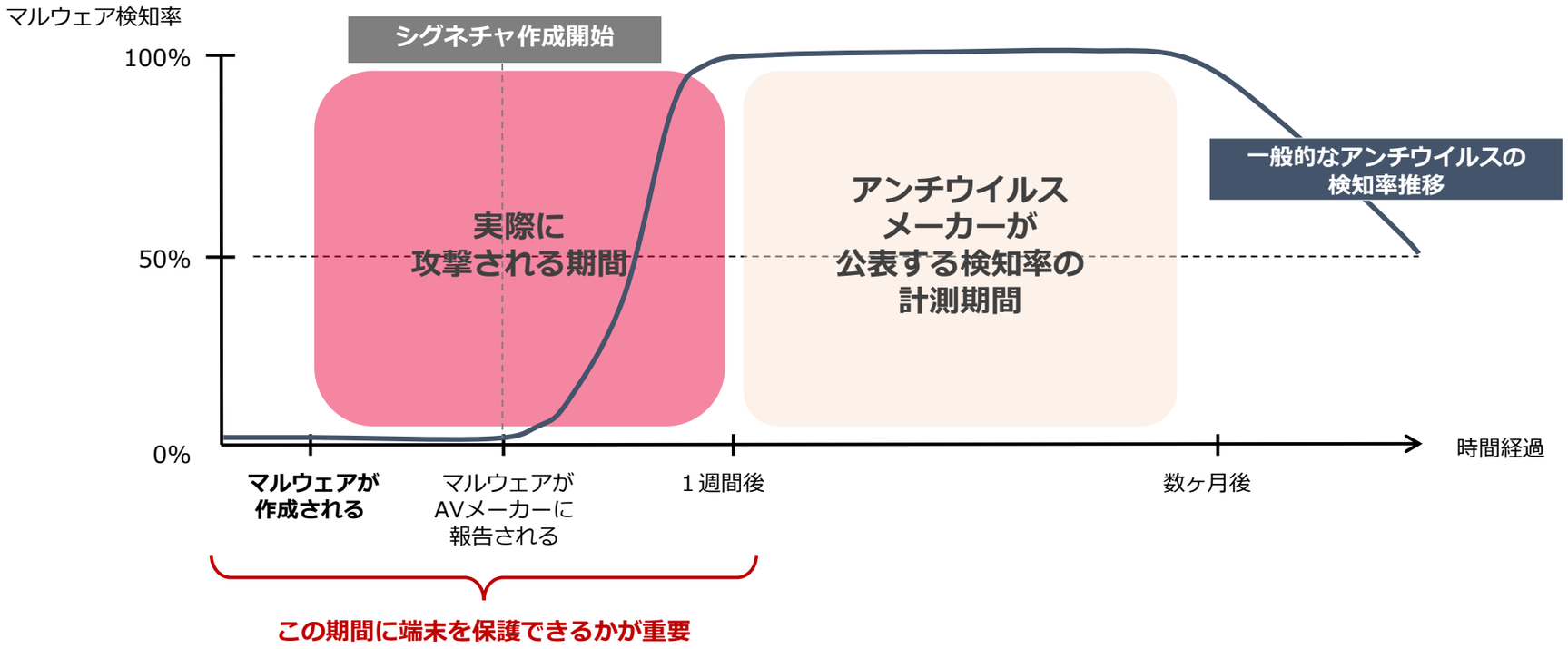
出典：JPCERT/CC：マルウエアEmotetへの対応FAQ https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html#4

再度 Emotet に感染しないために…アンチウイルス選びのポイント

セキュリティ対策として最も広く使われている従来型のアンチウイルスは、日々発見されるマルウェアをブラックリスト化してパターンファイルを更新しています。このアプローチの構造的な問題はゼロディと呼ばれる未知のマルウェアを止めることができないという点です。また仮にマルウェアが発見されたとしても、メーカーがそのファイルを入手し、パターンファイルを作成してエンドポイントに配信されるまでにはタイムラグがあります。攻撃者はこの構造的な欠陥を突くために頻繁にマルウェアコードを変更するようになり、結果的に最近のマルウェアのほとんどが従来のアンチウイルスをすり抜けるようになってしまいました。

シグネチャベースで未知のマルウェアを止めることが出来ないのは構造的な問題です。

実際に攻撃に使われてる期間にマルウェアから防御できるかどうかが、アンチウイルス選びの一番のポイントです。



Emotet の被害もエンドポイントで守る！

LANSCOPE サイバープロテクション

AI が未知・既知問わずマルウェアを隔離します
定義ファイルを使わないため、シグネチャ更新管理からも解放されます

LANSCOPE
Cyber Protection

マルウェア検知率 99%

高性能な AI により
未知・既知問わず検知可能

毎日のアップデート不要

定義ファイルを使用しないため
毎日のアップデート不要

PC 負荷が少ない

CPU 使用率1～2%
メモリ使用量40～60 MB

誤検知が少ない

従来製品と比較しても
誤検知は数十～数百分の１

LANSCOPE サイバープロテクションは2種類のマルウェア対策製品から、用途に応じて選択いただけます

多くの導入実績と EDR・MDR が利用可能

CylancePROTECT® CylanceOPTICS®

CylanceGUARD®

- **EDR 要件**への対応をお求めのお客様
- **EDR の運用を外部に任せたい**とお考えのお客様
- **インターネット非接続環境**※での運用をお考えのお客様

※インターネット非接続環境での利用は CylancePROTECT のみ可能

幅広い OS やファイルタイプに対応

deep instinct™

- **コストを重視**されるお客様
- **PC とスマホに**ウイルス対策ソフトを導入したいお客様
- **EXE ファイルだけでなく Word や Excel など多くのファイルタイプ**への対応をご要望のお客様

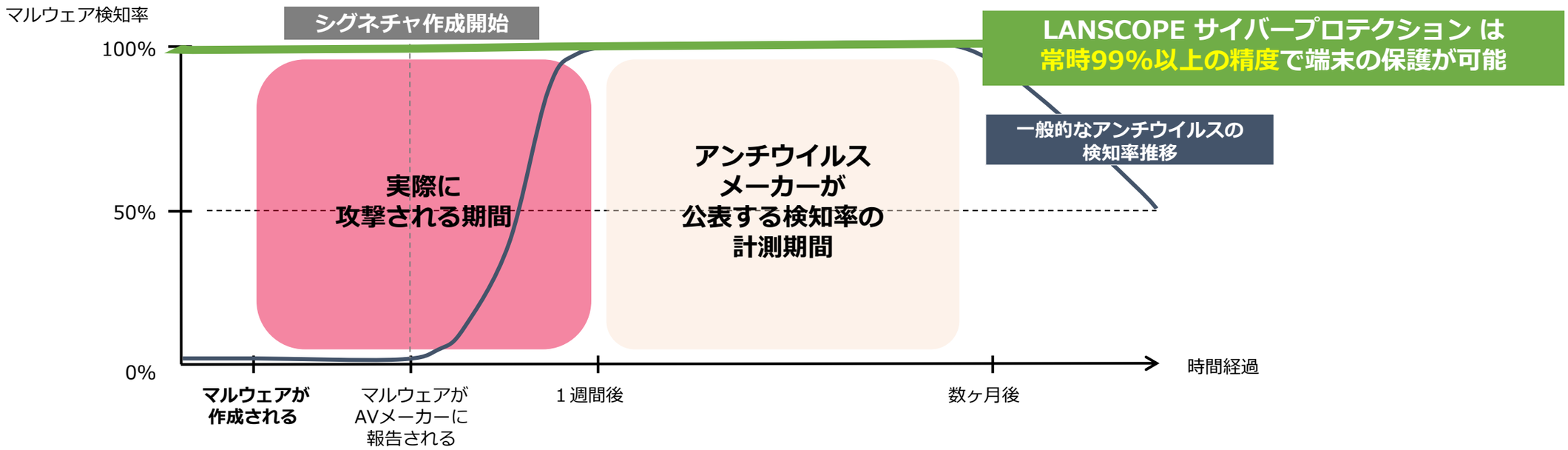
CylancePROTECT は導入社数が多くオプションも豊富
Deep Instinct は検知対象のファイルタイプが多く、マルチ OS に対応しているのが特長です

	CylancePROTECT	Deep Instinct
対応OS	Windows、macOS、Linux	Windows、macOS、Android、Linux
対応するファイルタイプ	PE（exeやdll）	PE,PDF,Office,Macro,RTF SWF,JAR,TIFF,Fonts,JTD…
EDR	CylanceOPTICS をオプション提供	無し
MDR	CylanceGUARD へのアップグレード可（有償）	無し
MOTEXの販売実績	約1,900社	約1,500社
コンソール	日本語対応済み	日本語対応済み
LANSCOPE エンドポイントポイントマネージャー オンプレミス版・クラウド版連携	連携可能	LANSCOPE エンドポイントマネージャー クラウド版と連携
価格（年額）	**5,400円**	**3,600円**
追加機能	・運用／代行（￥170／月額　￥2,040／年額） ・レポートサービス（￥80／月額　￥960／年額） ・OPTICS（￥150／月額　￥1,800／年額）	ー

LANSCOPE サイバープロテクション の実力

LANSCOPE サイバープロテクション は、従来のアンチウイルス製品のようにパターンファイルを利用しません。
AI 自身が膨大な情報からマルウェアの特徴を学び続けることで、既知はもちろんのこと未知や亜種のマルウェアを99%以上※の超高精度で検知・隔離が可能です。

LANSCOPE サイバープロテクション の最も特徴的なポイントは、まだ世の中に存在しない、全く未知のマルウェアに対しても、予測をして防御できるという点です。
実際に「WannaCry（ワナクライ）」や「Emotet（エモテット）」のような、全世界で大きな被害をもたらした危険なマルウェアに対して、世界で最初に発見されるよりも平均で20か月前のエンジンで検知できている実績があります。LANSCOPE サイバープロテクション であれば、実際に攻撃が行われている期間にも99%の精度でマルウェア検知が可能です。



Emotet 検知実績

Emotet は2014年に発生して以降、何度もバージョンアップを繰り返し、初期とは異なる機能を備えた新タイプに進化しています。従来型のアンチウイルスの場合、タイプが変わるたびにシグニチャの作成が必要となり、感染を防ぐことは不可能です。

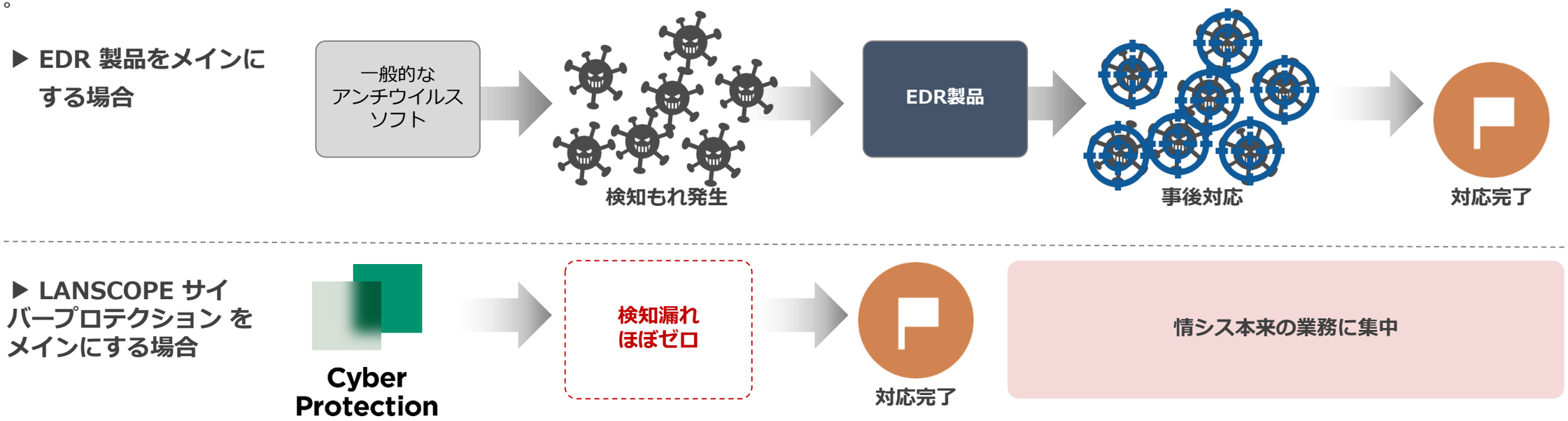
LANSCOPE サイバープロテクション は、最新の Emotet に対して、約2年前の検知エンジンで検知できたことを確認しています。
つまり、LANSCOPE サイバープロテクション の AI は約2年前もの間、更新されなくても Emotet の最新タイプに対応できていることになります。

LANSCOPE サイバープロテクション の特徴＝運用の手軽さ ～“アンチウイルスを入れておけば安心“を取り戻す～

LANSCOPE サイバープロテクション 導入の際に、よく比較検討されるのが、EDR（Endpoint Detection and Response）と呼ばれる製品です。EDR は、「アンチウイルスはマルウェア検知率が低い（マルウェア感染が避けられない）」ことを前提としたセキュリティソリューションです。エンドポイントを監視し、マルウェア感染の発生をいち早く発見して、封じ込めからフォレンジック分析まで行える専門的なツールで、効果的な運用には、収集したさまざまな情報を分析できるアナリストが必要となります。

EDR は、もちろんマルウェア対策に有効です。しかしその一方で、EDR で対処しなければならない頻度が高いと、対応する担当者の工数が大きく割かれ、運用がマンパワーに依存するという課題があります。仮に100個のマルウェアが社内ネットワークに侵入したとして、そのうち10%しかアンチウイルスで感染を防ぐことができない場合、残り90個分のマルウェアに対してはEDR を活用し、感染後の対策を行わなければなりません。

これに対して LANSCOPE サイバープロテクション の場合には、AI 技術によりマルウェア感染をほぼ100%防ぐことができ、マルウェア感染後の対応をしなければならないケース自体がほぼゼロとなります。マルウェア対策は LANSCOPE サイバープロテクション に任せて、情報システム部門本来の業務に集中することができます。



体験版もご用意しております！

両製品とも無料体験版をご用意しています！
無償で操作方法のレクチャーや疑問点にお答えしますので、ぜひお試しください

CylancePROTECT

CylanceOPTICS

▼体験版のお申し込みはこちら

概　　要	CylancePROTECT・OPTICS がライセンス数無制限でお試しいただけます。また、検知したファイルについて希望者の方にサマリーレポートを作成させていただきます。さらに、専任スタッフによる導入時の支援付きで、負担なく使い始められます。
対　　象	CylancePROTECT・OPTICS を初めて導入するユーザー様
ご利用期間	1ヶ月間
申し込みURL	https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr
申込期間	常時受付

deep instinct™

▼体験版のお申し込みはこちら

概　　要	Deep Instinct が 100ライセンスまで、1ヶ月間無料でお試しいただけます。さらに、専任スタッフによる導入時の支援付きで、負担なく使い始められます。体験中のお問い合わせにも対応しますので、じっくりしっかり体験が可能です。
対　　象	Deep Instinct を初めて導入するユーザー様
ご利用期間	1ヶ月間
申し込みURL	https://go.motex.co.jp/l/320351/2021-02-25/4gnpt1
申込期間	常時受付

製品に関するお問い合わせ

■ 営業本部

大阪本社	06-6308-8980
東京本部	03-3455-1811
名古屋支店	052-253-7346
九州営業所	092-419-2390
E-mail	sales@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター	0120-968995 （携帯・PHSからは06-6308-8981）
お電話受付時間	9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ	support@motex.co.jp