

## 猛威を振るうマルウェア「Emotet」の解析情報を公開 ～ 「i-FILTER®」・「m-FILTER®」最新の機能で脅威を検知 ～

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、12月3日頃より発生していたマルウェア「Emotet(エモテット)」に感染させると考えられるメール・URLの解析情報を公開したことを発表いたします。

2014年に初めてその活動が報告されたのち、何度も進化を繰り返してきたマルウェア「Emotet」は、2019年9月に再度活性化し、改ざんされたWebサイトからダウンロードされ感染するケースを弊社で確認いたしました。(※1)そして、また12月3日頃より再度攻撃の手口を変え、国内での感染事例が増加しており、IPA・JPCERTからも注意喚起が先日発表されました。(※2)

被害を増加させている要因の一つとして、攻撃メールの受信者が過去にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容等の一部が攻撃メールに流用されるなど、手口が巧妙になっている点が挙げられます。正規のメールへの返信を装う内容となっており、業務上開封してしまいそうになるため、人間の目では判断が難しいものです。

Webセキュリティ製品「i-FILTER」Ver.10と、メールセキュリティ製品「m-FILTER」Ver.5は、マルウェア「Emotet」の攻撃を検知し、メールの受信・URLアクセスを未然にブロックすることで、同製品のユーザー様を守ることが出来ました。

また、アクセスログからマルウェア解析し、メールの件名や添付ファイル、URLの特徴等を弊社コーポレートサイト上で公開しております。クリスマスや年末年始商戦を意識した攻撃キャンペーンが、例年12月初旬から中旬にかけて活性化しますので、これらの情報を活用いただき、今後の継続的な注意喚起に繋げていきます。

### マルウェア「Emotet」の解析情報

以下、弊社コーポレートサイト上にて公開しております。

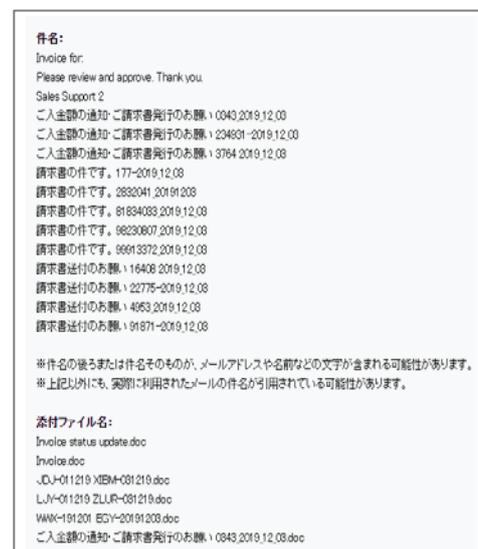
#### ◆公開ページ

サイバーリスク情報提供サービス「Dアラート」

<https://www.daj.jp/bs/d-alert/bref/?bid=48>

#### ◆公開している情報

- ・メールの件名
- ・添付ファイル名
- ・添付ファイルのHASH値
- ・対処手順
- ・感染プロセス
- ・マクロ実行時に通信するURL
- ・弊社製品の対応状況



<公開した情報のイメージ図>

### 弊社製品によるマルウェア「Emotet」への対処

今回の攻撃メールの脅威に対して、弊社のお客様が利用されている「i-FILTER」と「m-FILTER」の機能によって、未然にブロックが可能であることが実証できました。

#### 【Webセキュリティ製品「i-FILTER Ver.10」の機能と特徴】

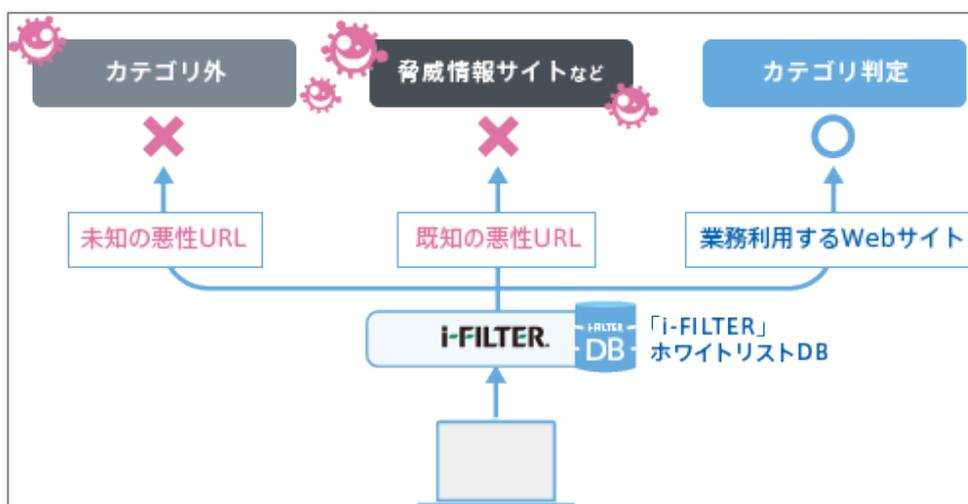
安全と判断したWebのみアクセス可能とする、ホワイトリストDBにより、安全なWeb環境を創出

- 国内で検索可能なWebサイトを網羅し、弊社で安全と確認されたURLのみアクセス可能とし、安全が確認できないURLまたは未知の危険なURLは全てブロックするホワイトリストDBを採用
- 業務上必要なURL等を事前に登録したり、組織の運用ルールに従ってフィルタリングによるアクセス許可／不許可等を設定することも可能
- URLのメンテナンス等管理者の負担となる業務は不要で、お客様にセキュリティによる不安や手間を感じさせません

#### <「Emotet」をブロックした機能>

##### ■ ホワイトリストDBとダウンロードフィルター機能

ホワイトリストDBによる未知の脅威URLへのアクセスと、ダウンロードフィルター機能による、改ざんされたWebサイトからのマルウェアダウンロードのブロック機能を組み合わせてマルウェア感染をブロックしました。



<「i-FILTER Ver.10」のホワイトリストDBの説明図>

#### 【メールセキュリティ製品「m-FILTER Ver.5」の機能と特徴】

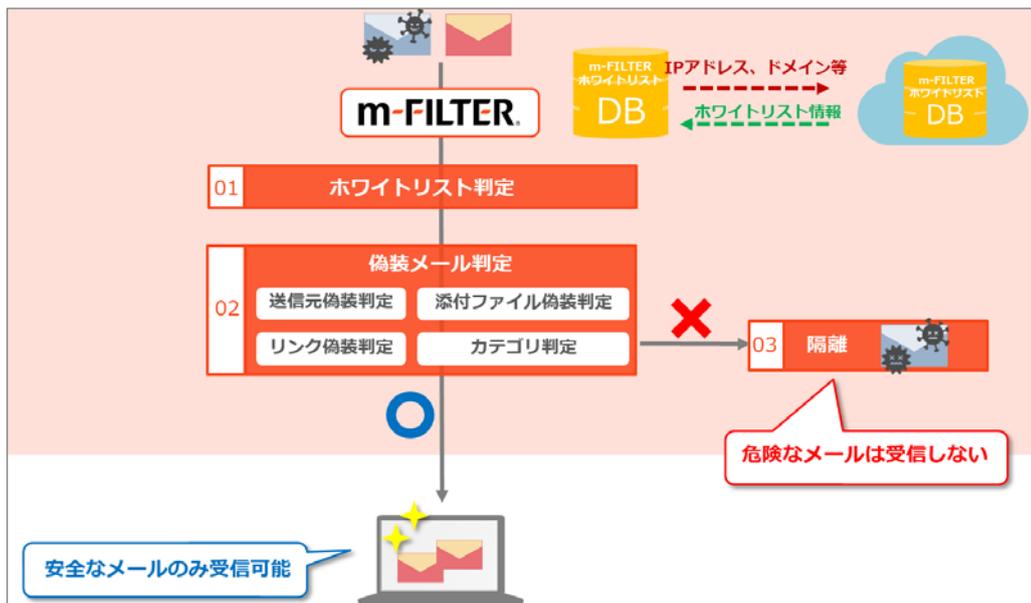
安全と判定したメールのみ受信可能とする、ホワイトリストDBにより、安全なメール環境を創出

- 安全な「IPアドレス」と「メールアドレス」の組み合わせを収集し、安全と判定された送信元のメールのみを受信可能とする、メールセキュリティ製品
- 送信元偽装メールや偽装した添付ファイル、本文を偽装したメール等を判定し、隔離
- 添付ファイル削除、リンク無効化等、メール無害化が可能で、ネットワーク分離環境にも適用

#### <「Emotet」をブロックした機能>

##### ■ ホワイトリストDBと添付ファイル偽装判定機能

ホワイトリストDBによる送信元メールアドレス判定と、添付ファイルに埋め込まれたマクロの偽装判定を組み合わせ、マルウェア感染をブロックしました。



＜「m-FILTER Ver.5」のホワイトリスト DB の説明図＞

デジタルアーツは、今後ますます脅威となる外部からの標的型攻撃や内部からの情報漏洩における防御・対応ソリューションについて、Web、メール、ファイルなどあらゆる情報資産の観点から、より迅速に広範囲に開発・提供し、これからもインターネット社会に対して安心と安全を実現すべく、更なる製品満足度向上を目指してまいります。

以上

※1 詳細は下記の弊社セキュリティレポートをご参照ください([https://www.daj.jp/security\\_reports/191017\\_1/](https://www.daj.jp/security_reports/191017_1/))

※2 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>)  
JPCERT マルウェア Emotet の感染に関する注意喚起(<https://www.jpcert.or.jp/at/2019/at190044.html>)

■ 「i-FILTER」について <https://www.daj.jp/bs/ifmf/i-filter/>

「i-FILTER」は、標的型攻撃をはじめとした外部からの攻撃対策と、組織内部からの情報漏洩対策の両方を 1 つの製品で実現する、プロキシ型の Web セキュリティソフトです。業界最大級の Web フィルタリングデータベースに基づいて、未登録の URL を悪性 URL と判定し、Web 経由の標的型攻撃をブロックする安全な Web の世界を実現します。また、業務中の閲覧が不適切な Web サイトのアクセスブロックや、Web メールの利用や掲示板の書き込みなどといった、Web 経由の情報漏洩を防ぐとともに、その内容を記録・確認・保存することが可能なため、内部統制対策としても有効なソリューションです。

■ 「m-FILTER」について <https://www.daj.jp/bs/ifmf/m-filter/>

「m-FILTER」は、電子メールによる情報漏洩・監査要求・年々増加するスパムメール・標的型攻撃メールといった課題を 1 つの製品で対応できる、企業・官公庁・自治体様向けのゲートウェイ型電子メールセキュリティソフトです。「m-FILTER」では、外部からの標的型メール攻撃対策機能や、内部からの情報漏洩対策機能を標準で実現する「m-FILTER MailFilter」、リアルタイムに添付ファイルを含めたメールを保存し、高速検索で運用負荷を軽減する「m-FILTER Archive」、業界最高水準の検知率である Cloudmark 社スパムエンジンによりスパムメールを徹底排除する「m-FILTER Anti-Spam」の 3 つの機能を提供します。これらの 3 つの機能から解決したい課題に合わせ機能を選択し、お客様のニーズに合わせた組み合わせで導入いただくことも、3 つの機能全てを導入いただくことも可能です。

**■ デジタルアーツについて <https://www.daj.jp>**

デジタルアーツは Web やメール、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。

インターネットの黎明期であった 1998 年に初めて国産の Web フィルタリングソフトを世に送り出した先駆者であり、これまでの知見をもとに、情報漏洩対策や標的型攻撃をはじめとするサイバー攻撃対策を実現する、最先端の情報セキュリティ製品を提供しています。

国産メーカーの強みを生かして、製品の企画・開発・販売・サポートまでを一貫して行っており、プロダクトの根幹を支える国内最大級の Web フィルタリングデータベースと、世界 27 の国と地域で特許を取得した技術力は、高い評価を得ております。契約更新率 95%以上という実績は、顧客満足度が高い証左です。

国内シェアの 50%以上を占める Web セキュリティソフト「i-FILTER」を中心に、個人・家庭向けの「i-フィルター」、メールセキュリティソフト「m-FILTER」、ファイル暗号化・追跡ソリューション「FinalCode」などの製品を揃えており、ワンストップで Web やメール、ファイルのセキュリティ対策を実現できます。

「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」という理念のもと、デジタルアーツは全てのステークホルダーの皆さまに信頼される東証一部上場企業として成長を続けています。

※ DIGITAL ARTS, i-FILTER, info board, ARS, Active Rating System, ACTIVE RATING, ZBRAIN, D-SPA, SP-Cache, NET FILTER, White Web, m-FILTER, m-FILTER MailFilter, m-FILTER Archive, m-FILTER Anti-Spam, m-FILTER File Scan, Mail Detox, FinalCode, DigitalArts@Cloud, Chat@Cloud, D Alert, D Content, and related logos and icons are trademarks or registered trademarks of Digital Arts Inc.

※ 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。

---