

コンピュータの情報を悪用・窃取する**恐怖**のマルウェア

# Emotet

## 感染注意

### 主な感染経路は メールの添付ファイルとURLリンク



#### メール添付のパスワード付きZIPファイル

セキュリティで検知しにくいパスワード付きZIPファイルを利用しWordやExcelへマクロを仕込むことで、感染させます。



#### メール添付の「マクロ」付きファイル

「.docm」や「.xlsm」などのマクロ付添付ファイルを利用し、返信メールや業務に関連しそうな件名を使いファイルを開かせることで感染させます。



#### メール本文内のURLリンク

メール本文内のURLリンクから、クッションページや改ざんサイトへアクセスさせ、マルウェアをダウンロードさせることで感染させます。

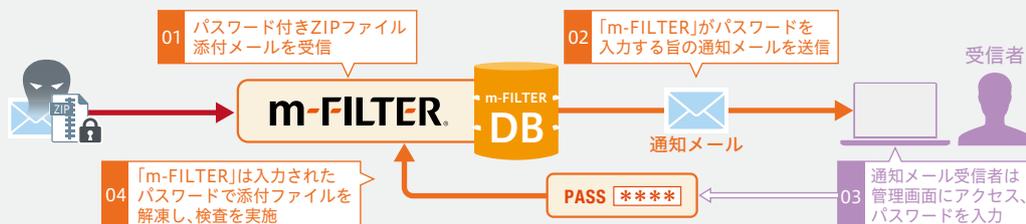
# i-FILTER® m-FILTER®

POINT  
1

メールに添付されたパスワード付きZIPファイルの安全性を  
m-FILTERが判定してから配信します

特許取得済み 第6882217号

m-FILTER



POINT  
2

メールの添付ファイルのマクロを検知し、  
ブロックまたはマクロを除去してから配信します

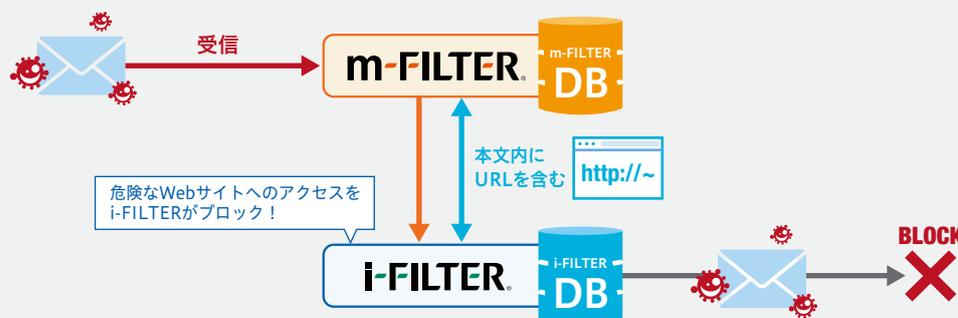
m-FILTER



POINT  
3

メール本文内のURLリンクから誘導される  
改ざんサイトやクッションページのアクセスをブロック

i-FILTER



Emotetなどのマルウェア感染はランサムウェア侵入の原因となることも…

機密情報や個人情報ファイルは暗号化しておくことで情報漏洩を対策

ファイル暗号化・追跡ソリューション  
「FinalCode(ファイナルコード)」

FINALCODE @Cloud™

DigitalArts®

デジタルアーツ株式会社

〒100-0004 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 ウェストタワー14F

■本書は、2022年3月現在の情報を基に作成されています。最新の情報は弊社Webサイトをご参照ください。■ActiveDirectory、Internet Explorer、Microsoft Edge、Microsoft 365およびWindowsは、Microsoft Corporationの登録商標または商標です。Android、GmailおよびGoogle Chromeは、Google LLCの登録商標または商標です。iOSは、Apple Inc.のオペレーティング・システムの名称です。IOSは、Cisco System, sIn.cの登録商標または商標です。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、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER File Scan、Mail Detox、m-FILTER EdgeMTA、EdgeMTA、FinalCode、DigitalArts@Cloud、Desk@Cloud、Desk、DアラートおよびDコンテンツの他の弊社・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。■本書に記載されている製品の各種ライセンスの定義およびライセンス別の価格については、各製品の価格表をご参照ください。■本書に掲載されている画面および画面設定例は、解説のためのイメージ図であり、実際の画面とは異なる場合がございます。■本書に記載の内容は変更される場合があります。予めご了承ください。

2022/3 DD-11317-001