i-FILTER × m-FILTER × FINALCODE

安心・安全な国産のWeb・メール・ファイルセキュリティをご提供

2020年1月の話題のインシデントにも対応！

[インシデント内容]
2020年1月20日、三菱電機がサイバー攻撃の被害を受け、最大で8,000人以上の個人情報及び企業機密情報が漏洩した可能性があるとの報道がありました。

大手企業がサイバー攻撃によって、社会インフラに関する機微な情報等が流出した可能性が考えられ、国家規模でセキュリティの課題が指摘されています。

[サイバー攻撃のイメージ]

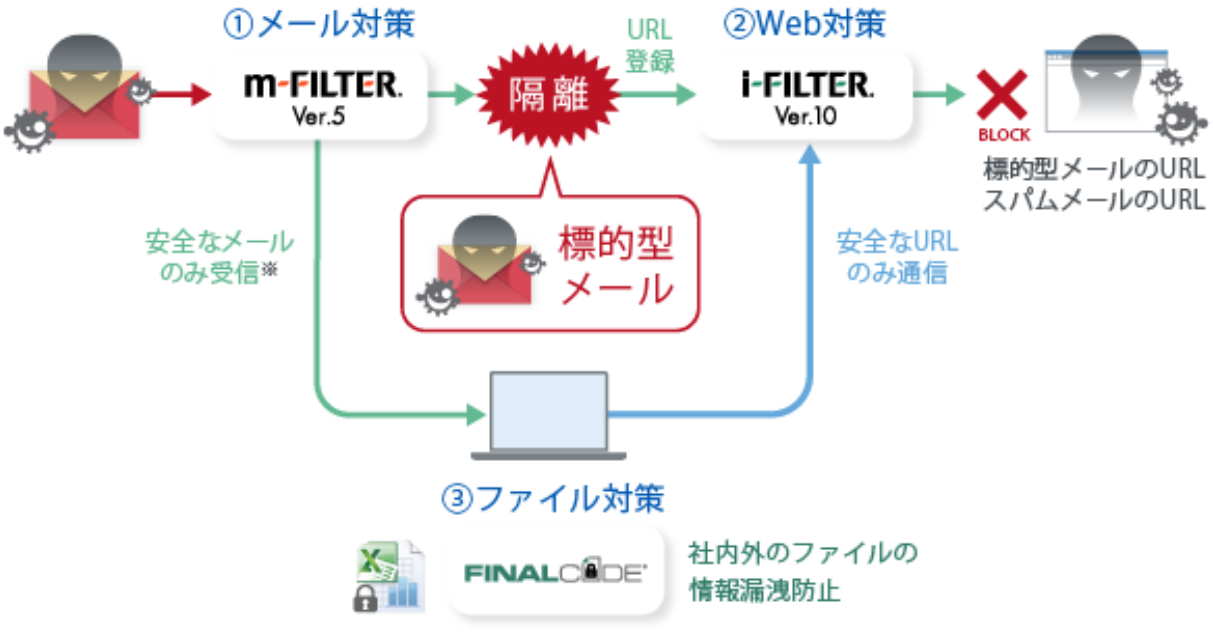
[インシデントの原因]
今回のインシデントについて、原因やハッキングを行った団体については明らかにされてはいませんが、攻撃の手法としては以下が考えられます 。

①メールによる標的型攻撃
②メールからのURL誘導でマルウェアに感染
③マルウェアによるファイル流出

これらについては、メール・Web・ファイルのセキュリティ対策を十分に行うことで、最新の脅威を防ぐことが可能です 。


[弊社製品のイメージ]

弊社製品が実現するインシデント対策

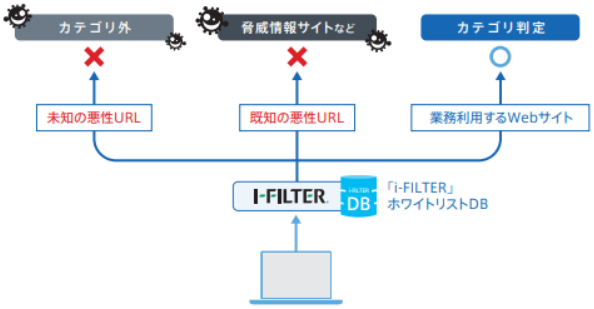


※メール偽装レベルが小さいスパムメールが一部含まれる

詳細は裏面をご確認下さい

i-FILTER

未知・安全でないURLはすべてブロックするので、ためらうことなくWebにアクセス可能



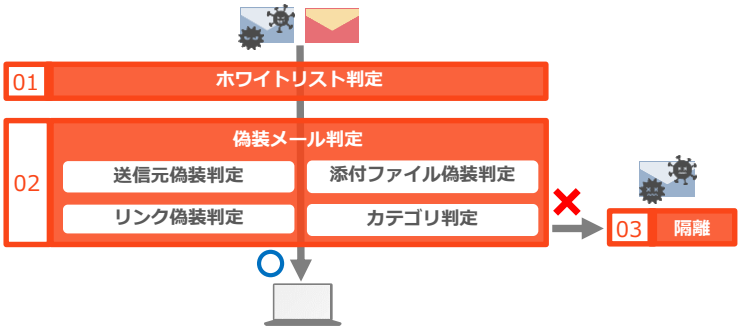
White Web 「安全なWeb」だけに通信させる仕組み

「安全なWebアクセス」だけを可能にするテクノロジー。「ホワイトリスト」運用のWebフィルタリングDBで、未知の脅威サイトへの通信をブロックします。ほぼすべての国内サイトを網羅し、業務のWeb閲覧を阻害しません。

WHITE WEB
WEB SECURITY TECHNOLOGY

m-FILTER

送信元のホワイトリスト判定と偽装判定をするので、受信したメールはすべて開封可能



Mail Detox 「安全なメール」だけを受信する仕組み 特許出願中

「安全なメール」だけを端末に受信するテクノロジー。「ホワイトリスト」DBによる正しい送信元からのみのメール受信に加え、偽装判定の実施により特定の閾値を超えたメールは隔離します。

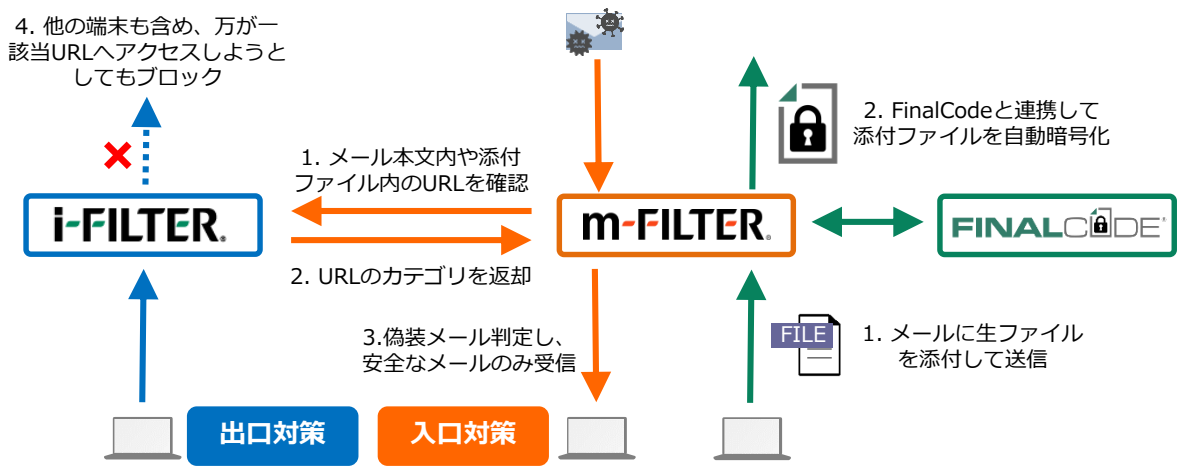
MAIL DETOX
MAIL SECURITY TECHNOLOGY

FINALCODE

ファイル作成時やダウンロードした瞬間に自動暗号化。ファイル暗号化の環境を簡単に実現

「FinalCode」の透過暗号機能で、ファイル暗号化の環境を簡単に実現。
ファイル作成時やダウンロードした瞬間に自動暗号化。
内部の不正持ち出しを防止するだけでなく、外部不正アクセスで持ち出されても社外ユーザーのファイルの閲覧を防げます。

i-FILTER × m-FILTER × FINALCODE 製品間連携



誤送信対策

送信後に削除可能

間接漏洩対策

権限がない受信者は閲覧不可

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 ウエストタワー14F
Tel 03-5220-3090　Fax 03-5220-1130
sales-info@daj.co.jp
www.daj.jp