Press Release

2021 年 5 月 14 日
株式会社インテリジェント ウェイブ

PPAP 回避や、テレワークによるセキュリティリスク回避にも
多層エンジンのコンテンツ無害化ソリューション「ReSec（リセック）」国内販売開始

ファイルの脅威を無害化し、
マクロウイルスを含む既知および未知のマルウェアを除去

株式会社インテリジェント ウェイブ（本社：東京都中央区、代表取締役社長：佐藤邦光、以下：IWI）は、サイバー攻撃による既知および未知（ゼロデイ）のファイルベースのマルウェアを“無害化”し防御するソフトウェアソリューション「ReSec」（リセック）の開発元イスラエル・ReSec 社と国内販売契約を締結し、ディストリビューターとして 5 月 14 日より販売を開始します。

ReSec は、ゼロトラストのコンセプトに則り、組織の外部から持ち込まれるファイルをそのまま組織の内部に取り込まず、代わりに、CDR 技術（Content Disarm and Reconstruction）＝ファイル無害化技術や、アンチウイルスエンジン、ReSec 社開発の Intelligent File Firewall（IFF）エンジンによるファイル処理など、多層的な防御機能を用いて危険な/不許可のファイルをブロックし、外部から持ち込まれるファイルに含まれる危険な部分を除去した安全なレプリカファイルを生成し、組織内のユーザーに提供します。

ReSec の特長
・既知/未知(ゼロデイ)マルウェアの駆除
・業務効率を損なわないリアルタイム処理
・暗号化ファイル対応（多重パスワード）
・ハイパーリンクを用いたフィッシングの対策
・危険なマクロウイルスの検知・駆除
・メール、外部ストレージ、エンドポイント、ウェブダウンロードなど、多様なシステムに対応

昨年 11 月 24 日、平井卓也デジタル改革担当大臣が会見で PPAP（パスワード付き zip ファイルの添付とそのパスワードを別送する、ファイルのメール送付方式）を内閣府、内閣官房で廃止すると発表したことから、PPAP の廃止は大きなうねりとなり、注目されています。PPAP 回避策としてはクラウドストレージサービスの活用などが挙げられますが、クラウドストレージサービスでは、パスワード付暗号化ファイルを含めファイルの無害化は行われません。例えば、申込書などのファイルを社内システムに取り込むには、多重パスワードを解凍し、ファイルの無害化を行う事がセキュリティとして必須になりますが、ReSec ではクラウドストレージにあるファイルを無害化することが可能となります。

テレワークが新常態となりつつある現在、テレワーク環境下にある社員が境界防御外からお客様のクラウドメールやストレージにアクセスしたり、勝手に Web アクセスしてファイルをダウンロードしたりした場合、ファイルと一緒にマルウェアが持ち込まれるなどのリスクが存在します。この場合も、ReSec により多重パスワードの解凍、マクロウイルスを含めたファイル無害化を行い、社内に安全にファイルを取り込む事が可能となります。

■ReSec による組織防護

ReSec は複数の防御層を用いて組織を既知/未知の脅威から守る 3 層の防御機構で構成されています。ReSec 社が特許を取得している CDR 技術をはじめとし、厳選されたアンチウイルスや同社が開発したハイパーリンク/マクロスキャン機能が、ファイルベースマルウェアを組織に侵入する前に駆除します。

本製品は、メールなどの限られた侵入経路ではなく、オンプレミス/クラウドメール、エンドポイント、外部記憶媒体、ウェブダウンロード、ファイルサーバー、クラウドストレージや API などを対象とし、どのようなシステムにおいても危険なファイルを侵入させません。

■ファイルを無害化する 3 層エンジン　・・・安全なファイルを提供する仕組み

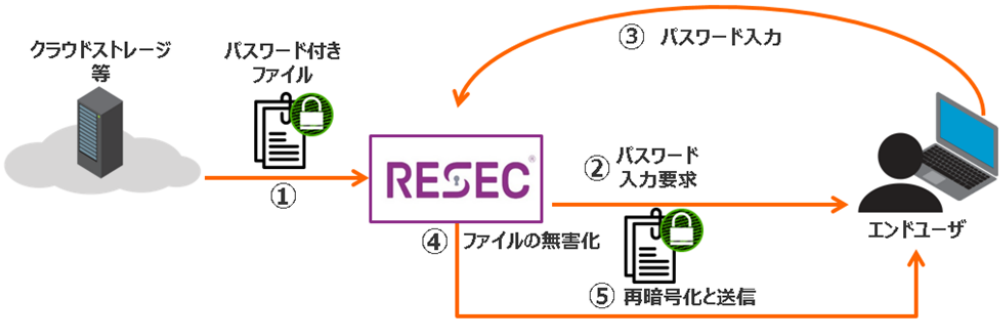
●1.　IFF（Intelligent File Firewall）– ReSec 社開発のセキュリティエンジン

IFF はマクロの検査やハイパーリンクの改竄検知/レピュテーションチェックに加え、暗号化ファイルの復号化や圧縮ファイルの解凍を行い、すべてのファイルが処理可能な状態にします。

◆暗号化ファイル対応

従来の製品ではできなかった暗号化されたファイルをスキャンしマルウェアを検知することが可能です。ファイルサーバー/クラウドストレージのファイルはもとより、外部からパスワード付添付ファイルを受信した際にも無害化します。複数のパスワードがかかっているファイルもスキャンできる「多重パスワード解除機能」が実装され、どのようなファイルでも安全に受信できます。

図：パスワード付ファイルの処理



◆マクロ対応

安全性が保証できるマクロ(ファイル内で完結する処理のみを行うマクロ等)のみをエンドユーザーに配信し、安全と判断できないマクロ(ファイルシステムアクセス、ネットワークアクセス、プロセス生成等をするマクロ)を削除するスキャン機能を実装しています。

◆ハイパーリンクの改竄検知/レピュテーションチェック

メールやファイルに記載された文字列とその文字列に紐づいている実際のリンク先 URL が異なる場合、リンク先 URL を本文記載の文字列に修正します。多くのソリューションで検知が難しい手法を検知し防御します。また「Google Safe Browsing」を用いたレピュテーションチェックにより、安全なもののみがエンドユーザーに配信される仕組みを実装しています。

●2.　Anti Virus Multi-Scan – 既知マルウェアに対する防御

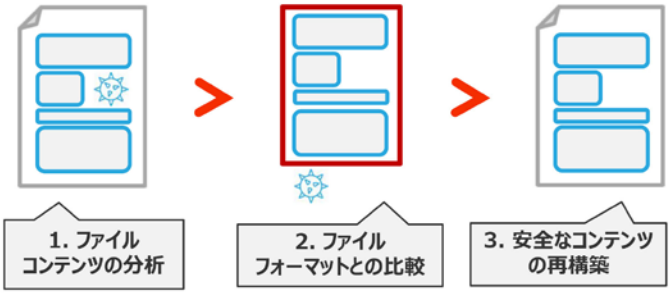
全てのファイルはグローバルで厳選された複数のアンチウイルスエンジン（AV）がスキャン。複数エンジンの利用によりマルウェアを高確率で検知します。AV は標準で 5 つ：Microsoft Security Essentials ／ Avira／ ClamAV／ F-Prot／ IncaAv が無償で提供されます。

●3.　CDR（Content Disarm and Reconstruction）技術　-ゼロディマルウェアも駆除

業界で最先端の CDR（コンテンツ無害化）技術はファイル構造を解析し、各ファイルのフォーマットに則ったコンテンツのみを利用し、全ての正常な機能を再現した安全なレプリカファイルをリアルタイムに提供します。

CDR 技術について：

1. ReSec がオリジナルファイルを分解し、ファイルの構成要素を取り出し。
   要素：画像、HTML、ハイパーリンク等
2. 取り出した構成要素をファイルの種類に応じたファイルフォーマットと比較し、
   フォーマットに定義されている要素のみを特定。
3. 2 で特定した、フォーマットに定義されていた構成要素を用いて新しいファイルを構築。
   ファイルフォーマットに則ったコンテンツは全て含まれるため、
   オリジナルファイルの全機能やコンテンツが忠実に再現されます。



★定義されていない部分（マルウェア等）はすべて無視されるため、マルウェアの場合は既知/未知を問わず、次の再構築ステップに採用されません。こうして安全なレプリカファイルが提供されます。

■販売・展開戦略

本ソリューションは年間サブスクリプションライセンスで、使用方法、契約台数あるいはメールアカウントの規模や多年度契約により価格は異なりますが、メール利用の場合、最小規模で 1 アカウントあたり年間約 3,600 円（税別）です。初年度は売上目標 2 億円を計画しています。サービス提供も可能です。

現在複数のプリセールス先に実証導入がなされており、まもなく本稼働を開始する予定です。クラウドストレージ、Menlo 等の仮想ブラウザーと連携するシステムを提案するなども含め、製造業、金融などを中心に業種や規模の大小を問わず、幅広い企業全般、および官公庁、自治体などに向け、普及を推進していきます。

以上

【株式会社インテリジェント ウェイブ（IWI）について】

IWI は、ペイメント決済システムにおけるオンラインネットワーク基盤のシステム構築を中心に、証券市場向け超高速株価情報システムなど、金融業界向けの大量データをリアルタイムかつ正確に処理するシステムの開発・構築・保守を手がけており、圧倒的な国内シェアを獲得しています。また自社開発の内部情報漏洩対策製品「CWAT」をはじめ、海外の先進的なソリューションを国内に紹介普及させていく情報セキュリティ対策事業も、その領域を大幅に拡大させています。

IWI は「次代の情報化社会の安全性と利便性を創出する」を経営理念に、高速、安全、高品質で利便性の高い IT 基盤を提供して、企業のデジタルトランスフォーメーションを支援しています。IWI は大日本印刷グループの一員であり、東京証券取引所市場第一部に上場しています。https://www.iwi.co.jp

読者からのお問い合わせ先：
株式会社インテリジェント ウェイブ
営業本部　営業第三部
TEL：03-6222-7100　FAX：03-6222-7301
iwi_security@iwi.co.jp

報道関係からのお問い合わせ先：
IWI セキュリティソリューション広報事務局
(株)アルサープ内　河端・川口
TEL：03-4405-8773
iwi-security@alsarpp.co.jp