

Press Release

2020年12月9日
株式会社インテリジェント ウェイブ

【導入事例】

ネットワーク未接続のクローズド環境でも攻撃を防御するセキュリティソリューション 大日本印刷株式会社が蕨工場のセキュリティ対策に モルフィセック Morphisecを導入

Microsoft Defender と統合され、管理機能を提供する “攻撃を成立させない” エンドポイントセキュリティ対策

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、大日本印刷株式会社が、同社・蕨工場（埼玉県蕨市）のクローズドネットワークに、最新の技術で攻撃の実行を不可能にし、いかなる未知の攻撃でも防御することができるエンドポイントセキュリティソリューション「Morphisec」（モルフィセック）を導入したことを発表します。IWI は「Morphisec」の国内唯一の戦略パートナーであり、イスラエルの Morphisec 社が開発しグローバルに展開する製品を国内で唯一販売、サポートしています。

Morphisec は、シグネチャー方式ではないため、パターンファイルの更新は不要です。このため、常時外部接続を必要とせず、オフラインのクローズド環境で利用される工場の制御系 PC の運用にも全く支障がありません。Morphisec は Moving Target Defense テクノロジーにより、既知の攻撃はもとより、ファイルレス攻撃、脆弱性悪用、ゼロデイ攻撃を含む未知の攻撃に対する保護・防御を提供します。本テクノロジーは、Windows PC などエンドポイントでアプリケーションが起動する際、実行モジュールをローディングするメモリーアドレスを、毎回ランダムイズして動的に変化させます。攻撃者は新しいメモリー構造を知る術はなく、攻撃に必要ないかなる機能にもアクセスできないため、攻撃の実行が不可能となります。

■大日本印刷株式会社 蕨工場の Morphisec 導入

<従来の運用状況と課題>

厳重なセキュリティ体制を敷く大日本印刷株式会社の蕨工場では、次の課題がありました。

- ・常時外部接続が不可のクローズドネットワーク環境での内部システムの運用
- ・一般のアンチウイルスソフトウェア（以下：AV）の単体利用による未知の脅威

セキュリティ対策として広く導入されている製品は常時外部接続での運用が前提となっているため蕨工場内への導入が難しく、これまでは一般の AV を単体で使用する状況でした。

AV を使った従来の方式では、既知の脅威に対応できますが、刻々と出現する新たな脅威からの防御が困難です。また外部接続用サーバーで更新データを受信する際に侵入されるリスクが内在し、USB メモリーなどネットワーク以外からの侵入リスクも考慮する必要があります。蕨工場では、こうした課題に対応し、セキュリティレベルを向上するために、新たなセキュリティ対策製品の導入を検討しました。

<選定ポイント>

蕨工場の厳格なクローズド環境で運用可能なソリューションとして、大日本印刷株式会社のグループ会社である IWI が販売元となっている Morphisec が候補に挙げられ、<新ソリューションの要件>を

満たすか検討されました。その結果、本製品が要件に合致し、蕨工場のエンドポイント防御に最適との判断に至り、導入が決定されました。

<新ソリューションの要件>

- ① 常時外部接続が不可のクローズドのネットワーク環境で運用が可能であること。
- ② シグネチャー更新が不要で、未知の攻撃から防御可能であること。
- ③ 端末には制御系 PC も多く含まれ、蕨工場にて独自開発したソフトウェアが複数存在するため、導入する製品がこれらと競合せず、PC に負荷をかけずに正常稼働すること。工場生産に支障をもたらす誤検知、過検知が少ないこと。
- ④ 外部接続用サーバーを使用する現行の運用方式を踏襲して導入すること。新たな管理サーバーは追加しないこと。

<導入効果>

	環境と要件		従来運用状況と課題		Morphisec の導入効果
リスク	クローズドネットワーク	×	常時外部へ接続が必要なセキュリティ製品の利用ができない	○	シグネチャー更新不要で、クローズドネットワークで稼働可能
リスク	一般のアンチウイルスソフトを利用	×	既知の攻撃には対応できるが、未知の攻撃は防御できない	○	ファイルレス攻撃など、未知の攻撃を含めあらゆる「攻撃を成立させない」環境の実現
運用	独自開発ソフトウェアが複数存在	×	独自ソフトウェアとの競合、CPU への負荷が懸念される	○	独自ソフトウェアと競合せず、CPU やネットワークに負荷をかけず正常稼働を維持
運用	外部接続専用サーバーの設置、サーバーの追加	×	定期的なポート開閉のみが認められ、常時外部接続は不可、かつ新たなサーバーの追加も不可	○	Morphisec は常時外部接続が不要であり、追加のサーバーも不要

<今後の展開>

今後、工場内の PC を Windows10 に切り換えていく過程で、Windows10 付属の無料のウイルス対策ソフトである Microsoft Defender にリプレイスしていく予定です。Morphisec は Microsoft Defender と連携していることから、蕨工場はこの連携機能を活用し、エンドポイントセキュリティ対策のさらなる強化を目指します。大日本印刷株式会社では、今後各地の他の工場にも導入の拡大を予定しています。

IWI では、Morphisec の普及が進行する中、クローズドネットワーク環境、管理サーバー未接続の環境でも端末単体で保護が完結するソリューションであることを示す好例として、本件導入事例を他社の工場系への普及促進に活用していきます。

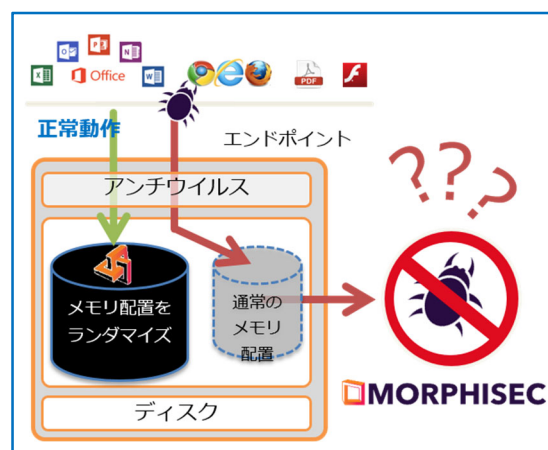
以上

【以下参考】Morphisec ソリューションについて

Moving Target Defense (MTD)

Morphisec の中核技術である Moving Target Defense (特許取得済) は、アプリケーション、Web ブラウザ、または OS が起動するたびにローディングするメモリーアドレスを毎回ランダム化します。攻撃者の悪意あるコードには新しいメモリー構造を知る術はなく、攻撃に必要ないかなる機能にもアクセスできないため、攻撃の実行ができません。正常なアプリケーションはランダム化されたメモリー空間で攻撃に遭うことなく通常通りに実行されます

Moving Target Defense



【Morphisec の特長】

- **オブジェクトを配置するメモリーをランダムイズ**
 1. 既知の攻撃だけでなく、未知の攻撃を使ったマルウェアの活動をさせない
 2. 導入時の設定が少なく、迅速・容易に導入可能
 3. マルウェア動作を阻止するためレジストリ変更などエンドポイントが汚染しない
 4. エンドポイントに導入するエージェントが 3MB と小さい（他製品は数 100MB 以上）
 5. 過検知、誤検知が発生しないため、運用負荷（工数、コスト）が軽減
- **シグネチャー方式でない（パターンファイル、IOC など不要）**
 6. シグネチャーの更新が不要のため、ネットワークと非接続でも稼働
- **プロセス監視、メモリー監視などをしていない**
 7. プロセッサ・外部記憶へのエンドポイント負荷が非常に軽い（VDI、BYOD にも最適）
 8. 他のプログラムと競合せず、ブルースクリーンの発生がない
- **Morphisec の導入実績**
 9. 全世界で（国内含む）600 万エンドポイント以上での利用実績（2020 年 10 月末現在）
- **IWI の強み**
 10. IWI はエンドポイント内部情報漏洩対策 CWAT の自社開発（約 800 社導入）により、経験豊富なセキュリティエンジニアを有しており、エンドポイントのサポート力に定評

管理サーバー未接続でも防御が可能

端末単体で保護が完結するため、独立したネットワーク環境（Morphisec 管理サーバーと未接続）での利用も可能です。Morphisec は、オフィス環境の Windows サーバーや PC はもちろんのこと、社外持ち出し端末（ノート PC）や CPU などのリソースの乏しい端末、工場の制御系 PC、ATM、PC-POS 端末、など非常に広範な用途が見込まれます。

【Morphisec（モルフィセック）について】

イスラエルの国立サイバーセキュリティセンターからスピンアウトして 2014 年 7 月に設立された Morphisec Ltd. は、本社をイスラエルと米国ボストン、インドのムンバイに設置。2016 年に最初の製品を出荷し、ガートナー Cool Vendor アワードを受賞しています。日々進化するエンドポイントへの攻撃が実行不可能な状況を作り出す卓抜の技術「Moving Target Defense」を開発し、情報セキュリティ界にインパクトを与えています。9 つの特許を取得しており、Fortune500 の米国製造会社など、グローバルで 600 社以上、600 万台のエンドポイントに導入されています。Citrix、IBM、RSA、Splunk、Ivanti、AWS など各分野のトップ企業と認定テクノロジーパートナーとして結び、2019 年からは Microsoft Defender との連携・統合が大きく進展しています。 <https://www.morphisec.com/>

【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>

※記載の商品名、会社名は各社の商標または登録商標です。

本件に関するお問い合わせ先：
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