YNU Initiative for Global Arts & Sciences 横浜国立大学

エンドポイントセキュリティ製品の公開情報に基づく定性評価

2022年12月28日

Sponsored by HP

目次

著者：

森井 裕大, 渡辺 露文, 佐々木 貴之, 田辺 瑠偉, 徐　浩源, 吉岡 克成

横浜国立大学

第1章 はじめに

近年、組織の情報ネットワークに侵入し、重要情報の盗取や身代金要求を行うランサムウェアや標的システムに重大な障害をもたらす破壊的マルウェア等によるサイバー攻撃が急増し、大きな脅威となっている。DX が進展し、働き方が多様化する現在、サイバー攻撃はどこでも起こり得るというゼロトラストセキュリティの考え方が注目されており、その中核としてエンドポイントでのセキュ リティ対策の重要性が高まっている。一方、FORRESTER による調査によると47%の回答者は現在のエンドポイントセキュリティ製品が最新の脅威に対して十分でないと考えている[44]。本報告では、これらの脅威への対策技術として特にエンドポイントセキュリティ対策技術に着目し、攻撃の手順を外部からの侵入、横展開を含む内部での活動、外部への情報の持ち出しに分けた上で、それぞれにおいてエンドポイントセキュリティ対策技術の効果について公開情報に基づき考察し、定性的な評価を行う。なお、各エンドポイントセキュリティ対策技術はそれぞれに異なる特徴を持っており、本評価はこれらの対策技術の代替可能性を議論するものでもない。
本報告では、特に攻撃活動の「検知」と「防止」という観点に着目する。本報告では、攻撃活動が行われていることを防御側が認識することを「検知」と定義する。例えば、なりすましメールを発見することでエンドポイントへの侵入を試みる活動を認識することが「検知」にあたる。一方、「防止」は、攻撃活動が行われないように予防したり、攻撃活動を阻害することと定義する。一般に「検知」は保護対象の組織へのサイバー攻撃の脅威を認識する上で重要である一方、検知をするだけではセキュリティ対策としては不十分であり、検知した攻撃活動を「防止」する機能が必要となる。
一方、「防止」は必ずしも「検知」を必要とせず、ゾーニングにより横展開を防止したり、アプリケーション隔離によって他の構成要素への侵入を防ぐ方法が存在する。以降では、これらの差異に着目しつつ、各エンドポイントセキュリティ対策技術がどのように組織の防御を支援し得るのかを定性的に評価する。

第2章 用語の定義

本報告において使用する用語の定義を行う。

エンドポイント	組織内部の情報ネットワークに接続されており、組織のメンバが業務を行うためのコンピュータであり、本報告では Windows クライアント PC を想定する。
ホスト	組織内部の情報ネットワークに接続されている機器全体を指す。エンドポイントや各種サーバなどが該当する。
(エンドポイントへの)侵入	マルウェア感染などにより、攻撃者がシステムに侵入した直後の初期状態を指す。この時点では、エンドポイントは完全には侵害されておらず、攻撃者に完全に制御される状態ではない。
(エンドポイントの)侵害	侵入後に攻撃者がエンドポイントの制御できる状態に至ることを指す。よって、エンドポイントの侵害はエンドポイントへの侵入後に発生する。
(攻撃活動の)検知	攻撃活動が行われていることを防御側が認識することを指す。
(攻撃活動の)防止	攻撃活動が行われないように予防したり、攻撃活動を阻害することを指す。
(攻撃活動の)対処	攻撃活動が行われた後に、この影響や被害を軽減したり、回復することを指す。

第3章 評価対象となるエンドポイントセキュリティ対策技術

前章の通り、本報告では組織内部の情報ネットワークに接続され、組織のメンバが業務を行うための Windows クライアント PC をエンドポイントと定義し、これに導入するセキュリティ対策技術をエンドポイントセキュリティ対策技術と呼ぶ。本報告では、エンドポイントセキュリティ対策技術のカテゴリとしてNGAV (Next Generation AntiVirus)、アプリケーション隔離、EDR(Endpoint Detection and Response)の 3 種類を取り上げる。なお、これらのカテゴリの評価は、特定製品ではなく、同一カテゴリに属する複数の製品群に共通する機能を主な対象として行う。なお、一部の製品しか有さない機能が評価に影響する場合はその旨を記述する。

3-1 NGAV (Next-Generation Antivirus)

NGAV は、エンドポイントに導入するセキュリティ対策技術であり、エンドポイント内のファイルを実行前に検査し、パターンマッチング[5,8]、AI/機械学習[1,2,5,7,8,9,14]、サンドボックス[5,8,9,14]等により悪性ファイルを検知、実行防止、隔離することを主な目的にしている。上記の検知機能に加えて、事前に悪性ファイルを検知できず悪性ファイルが実行された場合やファイルレスマルウェアが動作している場合に、システムの挙動に基づきこれを検知する振る舞い検知機能 [1,3,5,7,8,9,10,11]を有する。NGAV に分類される製品は上記以外にも様々な保護機能を含むパッケージ製品として提供される場合が多く、例えば、ネットワークからのリモート侵入に対するエクスプロイト防御機能やデータ暗号化によるデータ流出防止機能を有する NGAV も存在する[12, 13]。

3-2 アプリケーション隔離

アプリケーション隔離とは、エンドポイントへの侵入を試みる攻撃に対して、ホスト OS から隔離された仮想環境を提供し、この環境においてリスクの高い業務を行うことで侵入を防止する対策技術である。特にサイバー攻撃の経路となることが多い E メールやチャットアプリ、USB メモリ、ネットワーク共有等により受け取ったファイルを使用する際に、Web ブラウザや Office アプリケーション等を隔離環境内で動作させることで、攻撃を受けた場合にもその影響が他の構成要素に影響しないようにする[15]。また、重要データを特定の隔離環境内でのみ利用可能とすることで、ホスト OS への侵入時のデータ流出を防ぐ機能[16]や、攻撃を受けた際にこれを検知するモニタリング機能を有するものがある[15]。さらに、プロセッサの仮想化支援技術等を利用したハードウェアベースの対策により、アプリケーション隔離を強化するソリューションが提供されている[15]。この評価では、導入されたアプリケーション隔離が、仮想化環境下で任意のファイル形式を開くことができることを前提とする。

3-3 EDR (Endpoint Detection and Response)

EDR とは、複数のエンドポイントにおけるシステムレベルの動作を監視し、これらのログをクラウドやオンプレミスのサーバに記録・保存・集約し、その分析により、組織内の疑わしいシステムの動作を検知し、悪意のある動作をブロックし、影響を受けたシステムの修正案を提供するソリューションである。エンドポイントへの侵入に成功した攻撃の検出と対処を主な目的としており、侵入の検出や侵入を受けたエンドポイントの封じ込め、悪性なプロセスの中断などの迅速な対応を行うことを目的とする [17,18,19,20,21]。対処作業は、自動または脅威分析者による手動で実行される。なお、実際の EDR 製品は上記の機能に加えて攻撃の検知等のために、NGAV の機能を含むものが存在するが、本評価では、EDR の主要な機能である侵入後の振る舞い検知機能を評価対象とする。

第 4 章 評価方法

本報告の評価対象である 3 つのエンドポイントセキュリティ対策技術を定性的に評価するための方法を示す。まず、組織への侵入や内部での活動、外部への情報持ち出しといった一連の攻撃活動のうち、特にエンドポイントに関わる攻撃活動を整理し、次に、それぞれの活動において、各対策技術を評価する項目を定める。

4-1 攻撃活動の整理

本報告では、MITRE ATT&CK [23]において定義されているサイバー攻撃のうち、特にエンドポイントに関わるものを抽出し、整理を試みる。MITRE ATT&CK は、攻撃者の戦術と攻撃手法を蓄積したナレッジベースであり[23]、本報告ではその中でもエンタープライズ向けに作成されたフレームワークである Enterprise Matrix[24]を活用する。Enterprise Matrix は、攻撃活動の目的や意図を表す戦術(Tactic)と各戦術を実現するための活動を表す手法(Technique)で構成されている。 ATT&CK の戦術のうち、エンドポイントに直接的に影響をもたらす 12 の戦術に着目し、A(1)エンドポイントへの侵入、A(2)組織内部への展開、A(3)目的実行という 3 つのフェーズに区分する。A(1)エンドポイントへの侵入は、A(1.1) 外部からの侵入と A(1.2)横展開による侵入に細分化される。また A(2)組織内部への展開は、A(2.1) エンドポイント内部での活動と A(2.2)横展開を行う、に細分化される。図 1 にエンドポイント視点でのサイバー攻撃活動と対応する MITRE ATT&CK の戦術を示す。図 1 において青色の文字の記載は ATT&CK における戦術を指している。以降では各フェーズについて説明する。

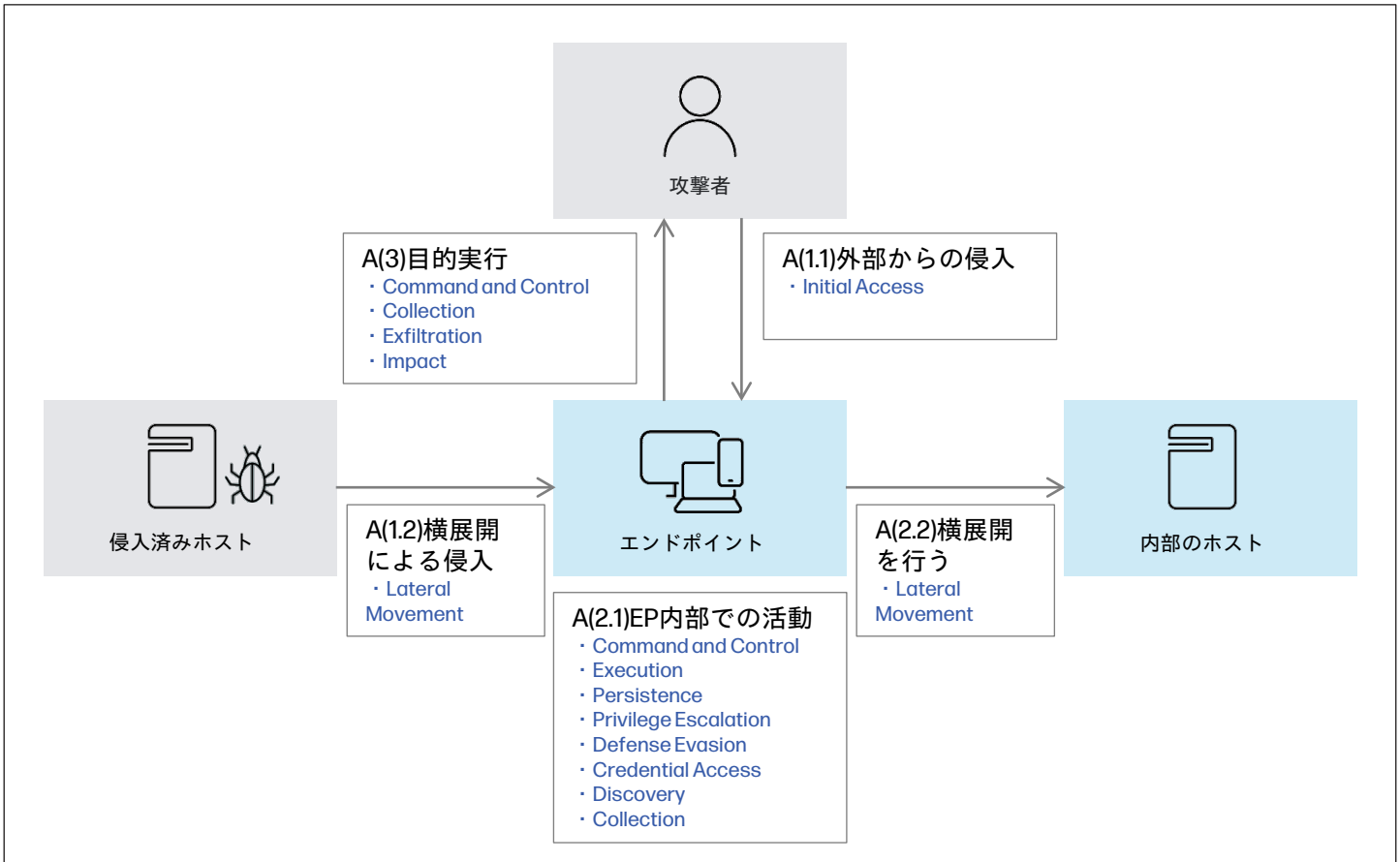

図 1 . エンドポイント視点でのサイバー攻撃活動と対応する MITRE ATT&CK の戦術

A(1) エンドポイントへの侵入

エンドポイントへの侵入は、A(1.1)外部からの侵入と A(1.2)横展開による侵入に細分化される。 A(1.1)外部からの侵入は、組織外部ネットワークからエンドポイントへの侵入を試みる攻撃活動である。ATT&CK の戦術“Initial Access”[25]を実現する手法の中で、E メールやチャットアプリ等を経由して悪性なファイルやリンクを配布する“T1566: Phishing”[26]、ドライブバイダウンロード攻撃などの悪性なWeb サイトを用意する“T1189: Drive-by Compromise”[27]、USB 等のリムーバブルメディアを経由して悪性なファイルを配布する“T1091: Replication Through Removable Media”[28]、VPNやVNCなどのリモートサービス経由で侵入を行う “T1133: External Remote Services”[29]が含まれる。一方、A(1.2)横展開による侵入は、組織内部ネットワークの他ホストに侵入後、当該ホストを経由してエンドポイントに侵入を試みる攻撃活動であり、ATT&CK の戦術“Lateral Movement”[30]に対応する。戦術“Lateral Movement”を実現する手法のうち、A(1.2)横展開による侵入の経路としては、組織内部の侵入済みエンドポイント上のメールアカウントを悪用し、組織内の他のユーザに悪性なファイルやリンクを添付した E メールを送信する“T1534: Internal Spearphishing”[31]、USB 等のリムーバブルメディアを経由して悪性なファイルを配布する“T1091: Replication Through Removable Media”、ネットワークドライブ等共有サービスを利用し、悪性なファイルを配布する“T1080: Taint Shared Content”[32]、SMB やRDP などのリモートサービスの脆弱性を悪用する “T1210: Exploitation of Remote Services”[33]の4 つが該当する。

また、エンドポイントへの侵入は、“T1566: Phishing”、“T1189: Drive-by Compromise”、“T1091: Replication Through Removable Media”、“T1534: Internal Spearphishing”、“T1080: Taint Shared Content”のようにエンドポイントユーザが何らかの操作を行うことを契機として発生するものと、SMB やRDP などのリモートサービスの脆弱性を悪用する“T1210: Exploitation of Remote Services”のように攻撃者が能動的に実施可能なものに区別することが出来る。以降、前者を「ユーザ実行型の侵入」、後者を「ユーザ非実行型の侵入」と呼ぶこととし、評価項目においては前者を U (User-triggered)、後者を N (Non-user-triggered)と記載する。

A(2) 組織内部への展開

組織内部への展開は、エンドポイントへの侵入後、エンドポイントの状態を把握し、不正活動の拠点を確保すると共に、組織内部の他ホストへの更なる侵入を行う攻撃活動であり、A(2.1)エンドポイント内部での活動と A(2.2)横展開を行うに細分化できる。A(2.1)エンドポイント内部での活動は、エンドポイント内のセキュリティ対策製品の無効化、権限昇格、永続化など、侵入に成功したエンドポイントに対して直接的に行う攻撃活動であり、 ATT&CK の戦術における ”Execution”[34] 、 ”Persistence”[35] 、 ”Command and Control”[36] 、 “Privilege Escalation”[37]、”Defense Evasion”[38]、”Credential Access”[39]、”Discovery”[40]、”Collection”[41]に該当する。一方、A(2.2)横展開を行うは、エンドポイントへの侵入に成功した後、組織内部ネットワークの他ホストへの侵入を試みることで攻撃範囲を拡大する攻撃活動であり ATT&CK の戦術における”Lateral Movement”に該当する。

A(3) 目的実行

目的実行は侵入によって得た機密情報を外部に持ち出したり、暗号化して復号のために対価を要求するなど、攻撃の最終目的に関わる活動である。ATT&CK の戦術においては、”Command and Control”、”Collection”、”Exfiltration”[42]、”Impact”[43] が該当する。

4-2 評価項目

4-1節の攻撃活動の整理に基づき、エンドポイントセキュリティ対策技術の評価項目を定める。攻撃活動への対策は、活動を認識する「検知」、活動を予防する「防止」、活動の拡大の封じ込めや被害の回復等を行う「対処」などが考えられる。以降では、攻撃の各フェーズにおける対策とその評価方法を示す。なお、以降の評価項目においては、検知を D (Detection) 、防止を P(Prevention)、対処を R (Response)という記号で表す。

A(1) エンドポイントへの侵入に関する評価項目

エンドポイントへの侵入は一連の攻撃活動の初期フェーズにあたることから、その対策としては主に「検知」と「防止」が考えられる。特に、本報告書で評価対象とする NGAV は侵入の試みを未然に検知することで内部への侵入を防ぐことに主眼が置かれた技術である。一方、アプリケーション隔離は、環境の隔離により重要情報や内部ネットワークへの侵害を防ぐことに主眼が置かれており、検知できるか否かに関わらず、侵入を防止できるという特徴がある。それらの性質の違いを明確に表現するため、「検知」と「防止」それぞれの評価項目を設定する。

加えて、前述の通り、エンドポイントへの侵入は、ユーザ実行型の侵入とユーザ非実行型の侵入が考えられる。ユーザ非実行型の侵入は、 VPN や RDP 等のネットワークサービスのセキュリティ不備を突く攻撃であり、A(1.1)外部からの攻撃において発生し得る。また、A(1.2) 横展開による侵入においても、RDP やSMB 等のネットワークサービスを介した侵入が想定される。

また、エンドポイントへの侵入を検知する際、侵入が発生する前に悪性ファイルなどを検知する未然検知と、侵入後の不正な振る舞いを検知する方法が考えられる。具体的にはマルウェアがシステム内にファイルとして保存される際、NGAV により検知される場合は前者に該当し、当該ファイルが未然検知をすり抜け、実行された際に、その振る舞いを EDR により検知する場合は後者に該当する。本評価項目では前者の未然検知の能力を対象とし、後者については、後述する評価項目「エンドポイント内部での活動の検知・防止・対処」として評価する。

上記をまとめると、エンドポイントへの侵入に関するセキュリティ対策技術の評価項目は以下となる。

- A(1.1)-D-U 外部からの侵入の未然検知(ユーザ実行型)
- A(1.1)-P-U 外部からの侵入と侵害の防止(ユーザ実行型)
- A(1.1)-D-N 外部からの侵入の未然検知(ユーザ非実行型)
- A(1.1)-P-N 外部からの侵入と侵害の防止(ユーザ非実行型)
- A(1.2)-D-U 横展開による侵入の未然検知(ユーザ実行型)
- A(1.2)-P-U 横展開による侵入と侵害の防止(ユーザ実行型)
- A(1.2)-D-N 横展開による侵入の未然検知(ユーザ非実行型)
- A(1.2)-P-N 横展開による侵入と侵害の防止(ユーザ非実行型)

A(2) 組織内部への展開に関する評価項目

組織内部への展開は、エンドポイントへの侵入後、エンドポイントの内部状態を把握し、不正活動の拠点を確保すると共に、組織内部への更なる侵入を行う攻撃活動であり、A(2.1) エンドポイント内部での活動とA(2.2)横展開を行うに細分化できる。また、この活動においては、すでに侵入が発生していることから、検知、防止に加えて、対処が対策として重要となる。そのため、組織内部での活動に関するセキュリティ対策技術の評価項目として以下を設定する。

- A(2.1)-DPR エンドポイント内部での活動の検知・防止・対処
- A(2.2)-DPR 他ホストへの横展開の検知・防止・対処

なお、前述の評価項目 A(1.2)-D-U, A(1.2)-P-U, A(1.2)-D-N, A(1.2)-P-N は既に侵入された組織内の他のホストからのエンドポイントへの侵入を防ぐ観点での評価項目であるのに対して、評価項目 A(2.2)-DPR はエンドポイントが侵入を受けた後、他のホストへの更なる侵入(横展開)を防ぐ観点での項目である。

A(3) 目的実行に関する評価項目

攻撃の目的実行の段階は、侵入と内部展開によって得た機密情報を外部に持ち出したり、暗号化して復号のために対価を要求するなど、攻撃の最終目的に関わる活動であり、セキュリティ対策としては、「検知」「防止」「対処」のすべてが重要となる。そのため、攻撃の目的実行に関するセキュリティ対策技術の評価項目として以下を設定する。

- A(3)-DPR 攻撃の目的実行の検知・防止・対処

以上で検討した評価項目を表 1 にまとめる。

表 1. 評価項目

評価項目	説明
A(1.1)-D-U 外部からの侵入の未然検知(ユーザ実行型)	フィッシングや標的型メールなどユーザの操作を契機とする外部からの侵入を未然検知する能力
A(1.1)-P-U 外部からの侵入と侵害の防止(ユーザ実行型)	フィッシングや標的型メールなどユーザの操作を契機とする外部からの侵入とエンドポイントの侵害を防止する能力
A(1.1)-D-N 外部からの侵入の未然検知(ユーザ非実行型)	VPN やRDP 等のネットワークサービスのセキュリティ不備を突く外部からの侵入を未然検知する能力
A(1.1)-P-N 外部からの侵入と侵害の防止(ユーザ非実行型)	RDP やSMB 等のネットワークサービスのセキュリティ不備を突く外部からの侵入とエンドポイントの侵害を防止する能力
A(1.2)-D-U 横展開による侵入の未然検知(ユーザ実行型)	組織内の他ホストからファイル共有や悪性ファイルのメール送付などによりエンドポイントへの侵入を未然検知する能力
A(1.2)-P-U 横展開による侵入と侵害の防止(ユーザ実行型)	組織内の他ホストからファイル共有や悪性ファイルのメール送付などによるエンドポイントへの侵入と侵害を防止する能力
A(1.2)-D-N 横展開による侵入の未然検知(ユーザ非実行型)	組織内の他ホストからRDP 等のネットワークサービスを経由したエンドポイントへの侵入を検知する能力
A(1.2)-P-N 横展開による侵入と侵害の防止(ユーザ非実行型)	組織内の他ホストからRDP 等のネットワークサービスを経由したエンドポイントへの侵入と侵害を防止する能力
A(2.1)-DPR エンドポイント内部での活動の検知・防止・対処	エンドポイントへの侵入後の活動(セキュリティ対策製品の無効化、権限昇格、永続化など)を検知、防止する能力
A(2.2)-DPR 他ホストへの横展開の検知・防止・対処	エンドポイントへの侵入後の他ホストへの侵入を検知、防止する能力
A(3)-DPR 攻撃の目的実行の検知・防止・対処	組織内での攻撃活動後、機密情報を外部に持ち出したり、暗号化して復号のために対価を要求する攻撃を防止・対処する能力

第 5 章 評価結果

第 4 章で設定した評価項目に基づき、第 3 章で説明したセキュリティ対策技術の 3 つのカテゴリについて 4 段階の定性評価を行った結果を表2 に示す。なお、評価が完全に合致した複数の項目については、結果を簡潔に示すために評価項目を統合している。それぞれの記号が持つ意味は以下の通りである。また、※印は条件付きの評価結果であることを示す。

◎：想定されるほとんどの攻撃に対応し、組織を防御できる。
〇：多くの攻撃に対応するものの、最善の防御とは隔たりがある。求められるセキュリティレベルに応じて組織は必要な対策を講じる必要がある。
△：一部の攻撃に対応しているものの、現在の脅威には十分に対応できない。
×：効果を期待できない。

表 2. 評価結果

評価項目	NGAV	アプリケーション隔離	EDR
A(1.1)-D-U 外部からの侵入の未然検知(ユーザ実行型) A(1.2)-D-U 横展開による侵入の未然検知(ユーザ実行型)	〇	×～◎	×
A(1.1)-P-U 外部からの侵入と侵害の防止(ユーザ実行型) A(1.2)-P-U 横展開による侵入と侵害の防止(ユーザ実行型)	△	◎	△
A(1.1)-D-N 外部からの侵入の未然検知(ユーザ非実行型) A(1.2)-D-N 横展開による侵入の未然検知(ユーザ非実行型)	×～△	×	×
A(1.1)-P-N 外部からの侵入と侵害の防止(ユーザ非実行型) A(1.2)-P-N 横展開による侵入と侵害の防止(ユーザ非実行型)	×～△	×	〇
A(2.1)-DPR エンドポイント内部での活動の検知・防止・対処 A(2.2)-DPR 他ホストへの横展開の検知・防止・対処	△	×	◎
A(3)-DPR 攻撃の目的実行の検知・防止・対処	×～△	△～◎	△

以下、各評価項目の評価結果を説明する。

5-1 ユーザ実行型の侵入の検知

	NGAV	アプリケーション隔離	EDR
A(1.1)-D-U 外部からの侵入の未然検知(ユーザ実行型) A(1.2)-D-U 横展開による侵入の未然検知(ユーザ実行型)	○	×～◎	×

NGAV は、ウイルス定義ファイルとのパターンマッチ、ヒューリスティック検知、サンドボックスによる挙動解析、AI等による検知など悪性ファイルを検知する様々な方策を有しており、一定の検知能力を有していることが期待される。一方で、攻撃者は事前に NGAV に検知されないことを確認した上で攻撃に利用するなど[Counter AV service Reference]、検知を回避する高度な攻撃の見逃しの可能性は排除できないことから、「○」と判断する。

アプリケーション隔離は、マルウェアを検知することなく感染を防御することができるが、ホストOSから隔離された仮想環境内のファイルやアプリケーションを検査することで攻撃を検知する能力を有する。この検知能力は、前述の仮想環境にどのような検知技術を導入するかに依存する。例えば、当該仮想環境内にNGAVのような悪性ファイル検知機能やEDRのような振る舞い検知機能を導入することで、これらと同等の検知能力を実現可能である。さらに、悪性活動の検知と停止を迅速に行わないと効果がないEDRとは異なり、アプリケーション隔離は安全な環境下でマルウェアの実行や挙動情報の計測を行うことが可能である。これは検知機能により詳細なデータを供給し、検知能力の強化に役立てることを可能にする。要約すると、アプリケーション隔離における検知機能の有効性は、統合する検知技術の選択、アプリケーション隔離環境の計測機能、さらにはマルウェアが隔離された環境にいることの検知を妨げる機能(例えば、保護されているホストをうまく模倣した隔離環境の生成) などの多くの要因に依存することになる。そのため、これらの選択に依存し、未然検知の能力を「×～◎」と幅広く判断する。

EDR は、エンドポイントへの侵入を試みる攻撃を未然に検知する対策技術ではなく、主に侵入後の活動の検知や対処を目的としているため「×」と評価する。

上記のセキュリティ機能は、エンドポイントユーザが行う主な操作に対応しており、外部からの攻撃、内部での横展開のいずれに対しても効果を発揮すると考えられる。

5-2 ユーザ実行型の侵入の防止

	NGAV	アプリケーション隔離	EDR
A(1.1)-P-U 外部からの侵入と侵害の防止(ユーザ実行型) A(1.2)-P-U 横展開による侵入と侵害の防止(ユーザ実行型)	△	◎	△

NGAV は、エンドポイントへの侵入を未然に検知することに主眼が置かれており、前述の通り、多様な検知技術を有する。また、実行前に未然検知した悪性ファイルについては実行を防止することができる。さらに、未然に攻撃を検知できなかった場合にも侵入後の振る舞いからこれを検知する能力を有する。一方、これらの検知を回避する高度な攻撃に対して見逃しの可能性は排除できず、振る舞い検知したマルウェアに対しては実行を停止することが困難な場合もあることから、「△」と判断する。

アプリケーション隔離は、エンドポイントへの侵入を試みる攻撃に対して、ホスト OS から隔離された仮想環境を提供する。そのため、検知の可否に関わらず、ユーザの操作を契機とした侵入に対して高い侵入防止効果が期待される。そのため、「◎」と評価する。

EDR は、エンドポイントへの侵入を未然に防止するための対策技術ではないが、初期侵入後にシステムの振る舞いの異常により、エンドポイントの侵害を防止する機能を有するため「△」と評価する。

5-3 ユーザ非実行型の侵入の検知・防止

	NGAV	アプリケーション隔離	EDR
A(1.1)-D-N 外部からの侵入の未然検知(ユーザ非実行型) A(1.2)-D-N 横展開による侵入の未然検知(ユーザ非実行型)	×～△	×	×

ユーザ非実行型の侵入は、RDP や SMB などのネットワークサービスを介してユーザの操作を伴わずにエンドポイントに侵入する攻撃である。NGAV のうち、このようなエクスプロイトに対する防御機能を有している場合には、一定の効果が期待されるため、「×～△」と評価する(エクスプロイト防御機能を有していない場合は×)。アプリケーション隔離は、ユーザ非実行型の侵入の未然検知を目標としていないため、「×」と評価する。EDR はユーザ非実行型の侵入を未然に検知する機能を有さないため「×」と評価する。

	NGAV	アプリケーション隔離	EDR
A(1.1)-P-N 外部からの侵入と侵害の防止(ユーザ非実行型) A(1.2)-P-N 横展開による侵入と侵害の防止(ユーザ非実行型)	×～△	×	○

上記と同様にNGAV のうち、エクスプロイト防御機能を有している場合に限り、一定の効果が期待できるため、「×～△」と評価する(エクスプロイト防御機能を有していない場合は×)。EDR はユーザ非実行型の侵入を受けた後の不正な振る舞いを検知し、この活動を防止できるため、「○」と評価する。

5-4 組織内部への展開の検知・防止・対処

	NGAV	アプリケーション隔離	EDR
A(2.1)-DPR エンドポイント内部での活動の検知・防止・対処 A(2.2)-DPR 他ホストへの横展開の検知・防止・対処	△	×	◎

エンドポイントへの侵入後の攻撃活動は一般に多様であり、特定の悪性挙動だけでなく、内部での攻撃活動がもたらす様々なシステム状態の変化を継続的に監視し、異常を捉える必要がある。 NGAV は、エンドポイントの挙動を監視する機能により、侵入後の活動に伴う悪性な挙動を検出し、これを防止することが期待される。しかし、NGAV の主眼は侵入の未然検知であり、侵入後の攻撃者の振る舞いの検知機能は、後述する EDR に比べて、十分であるとは言い難い。よって、「△」と評価する。

アプリケーション隔離は、エンドポイントへの侵入を防ぐことを主眼とし、侵入に成功した攻撃に対処することを目的としていないため、「×」と評価する。

EDR は、組織全体のホストの挙動を継続的に監視することで情報を収集・分析する。そのため、エンドポイントへの侵入に成功した攻撃を検出し、対処する能力が期待される。このことから「◎」と評価する。

5-5 攻撃の目的実行の検知・防止・対処

	NGAV	アプリケーション隔離	EDR
A(3)-DPR 攻撃の目的実行の検知・防止・対処	×～△	△～◎	△

攻撃の最終的な目的は、エンドポイントへの侵入後、機密情報を外部に持ち出したり、暗号化してその対価を要求するといったことであり、既に侵入を受けた状態でこれを防ぐためには、機密情報に対して事前に何らかの保護を適用するといった対応が必要となる。NGAV のうち、データ流出防止機能を有する製品については、一定の防止効果が期待されるため「×～△」と評価する(データ流出防止機能を有さない場合は×)。

アプリケーション隔離は、リスクの高い業務を隔離環境で行う技術であるが、機密情報を保持したホスト OS へ侵入を受けた場合にはこれを保護しない。一方、機密情報を扱うアプリケーションをホスト OS から隔離された仮想環境で実行することで、エンドポイントへの侵入によりホスト OSが侵害された場合であっても、機密情報を保護できることが期待される。このようにアプリケーション隔離のデータ保護効果は、その利用法や機密情報の取り扱いに依存して大きく変化し得るが、機密情報を必ず独立した隔離環境で行う運用が徹底されていれば、その効果は高いと言える。そのため、「△～◎」と評価する。

EDR は、機密情報の持ち出しに特化した機能を通常有していないものの、エンドポイント侵入後の攻撃を対処する機能を有しているため、「△」と評価する。

第6章 おわりに

本報告では、エンドポイントセキュリティ対策技術を対象に、組織への侵入と組織内部への展開、目的実行の各フェーズにおける対策の効果を定性的に評価した。その結果、NGAVはエンドポイントへの侵入を迅速に認識するための「未然検知」に優れており、アプリケーション隔離は、検知に依存せずに侵入を「防止」する性質を有し、EDR は侵入を受けた後に攻撃活動が組織内部で行われる際に、これを「対処」する機能に優れると確認できた。「検知」はサイバー攻撃の存在や 実態を防御側が認識する上で重要な評価項目であるが、攻撃の増大、多様化、高度化が進む現在、そのすべてを未然に検知することは現実的ではなく、「検知」に依存せずに確実に防御が可能な、アプリケーション隔離による「防止」の重要性はさらに高まると思われる。NGAVやEDRの限界は、侵入を阻止するために「検知」に依存することである。そのため、これらの対策の有効性は、新たな脅威に対してどれだけ早く「検知」（平均検知時間）し、「対処」（平均処時間）できるかで測られる。一般に、「検知」と「対処」が迅速であればあるほど、侵入の影響は小さくなる。攻撃の急速な進化を考えると、NGAVとEDRについては、いくつかの攻撃シナリオでこれらの指標がゼロより大きくなることが予想される。アプリケーション隔離は検知に依存しないため、平均検知時間や平均対処時間とは無関係に効果的な保護を提供できる利点がある。加えて、万が一、侵入を受けた際にこれを「対処」する仕組みと組み合わせることでその効果をさらに高められることが期待される。言い換えると、これらの性質は互いを補完するものであり、併用することで攻撃活動の各フェーズに対応した、さらに強固なセキュリティ対策が実現できるといえる。

本評価では、NGAV, アプリケーション隔離, EDR という 3 つのエンドポイントセキュリティ対策技術について、各製品群に一般的に具備されていることが期待される機能を評価したが、この評価方法にはいくつかの注意事項と課題がある。まず、実際の製品は、単一のエンドポイントセキュリティ対策技術だけでなく、複数の対策技術要素を有している場合があるため、その機能群を正確に把握した上で有用性を判断する必要がある。次に、セキュリティ対策機能自体も攻撃の対象となり、機能を停止・無効化されたり、迂回される恐れがあるため、これらの機能自体の正常性を担保する仕組みが必要である。セキュリティ対策を停止、無効化するような高度な攻撃に対しては、ハードウェアベースの検証を行うことでエンドポイントの動作の正常性を確認する機能等が求められる。さらに、今回の分析では、メンテナンスや管理者が必要とするやりとりなどの管理可能性とコストの要素を考慮していないが、適用する対策技術によっては、これらの要素は対策の実効性に直接的に影響しうる点に注意が必要である。最後に、これらのセキュリティ対策技術を導入する上では、ユーザビリティの確保も重要である。組織の生産性を低下させず、セキュリティ向上を実現するために、これらのセキュリティ対策の導入による業務への影響の度合いを検証する必要があるが、これらを含めた評価は今後の課題としたい。

参考文献

[1] ソフォス、エンドポイント保護、https://www.sophos.com/ja-jp/products/endpoint-antivirus/tech-specs
[2] ソフォス、Intercept X、https://www.sophos.com/ja-jp/medialibrary/PDFs/factsheets/sophos-intercept-x-dsna.pdf
[3] ソフォス、Sophos Anti-Virus: ホスト侵入防止システム (HIPS)、https://support.sophos.com/support/s/article/KB-000033428?language=ja
[4] ソフォス、データ流出防止ポリシー、https://docs.sophos.com/central/Customer/help/ja-jp/central/Customer/concepts/datalossprevention.html
[5] トレンドマイクロ、Apex One Endpoint Security、https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/endpoint.html
[6] トレンドマイクロ、Apex One™ DLP Option、https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/endpoint/integrated-data-loss-prevention.html
[7] サイバーリーズン・ジャパン株式会社、Cybereason NGAV、https://www.cybereason.co.jp/products/ngav/
[8] イーセットジャパン株式会社、NGAV(次世代型アンチウイルス)とは？、https://www.eset.com/jp/topics-business/next-gen-antivirus/
[9] イーセットジャパン株式会社、ESET TECHNOLOGY 多層型アプローチの概要とその有効性、https://www.eset.com/fileadmin/ESET/JP/Blog/download/eset_wp_technology_20191217.pdf
[10] カスペルスキー、Kaspersky Endpoint Security for Business SELECT、https://www.kaspersky.co.jp/small-to-medium-business-security/endpoint-select

[11] カスペルスキー、Kaspersky Endpoint Security for Business SELECT、https://media.kaspersky.com/jp/business-security/endpoint-security-select-datasheet.pdf
[12] カスペルスキー、Kaspersky Endpoint Security for Business ADVANCED、https://www.kaspersky.co.jp/small-to-medium-business-security/endpoint-advanced
[13] カスペルスキー、Kaspersky Endpoint Security for Business Advanced、https://media.kaspersky.com/jp/business-security/endpoint-security-advanced-datasheet-ja.pdf
[14] 卯月義文, and 岡田遥. "次世代エンドポイントセキュリティの基盤構築と運用 (特集サイバーセキュリティ)." Unisys 技報: Unisys technology review 39.2 (2019): 95-109.
[15] HP Inc.、HP SURE CLICK ENTERPRISE、https://jp.ext.hp.com/business-solution/enterprise_security/
[16] HP Inc.、次世代AVとBromiumアプリケーション隔離によるサイバーレジリエンスの実現、https://jp.ext.hp.com/blog/security/product/cybersecurity-ngav-bromium-application-isolation/
[17] ＪＢサービス株式会社、エンドポイント対策で注目されるEDRとは何か？EPPとの違いとは？、https://www.jbsvc.co.jp/useful/security/what-is-edr.html
[18] CROWDSTRIKE、EDR(エンドポイントでの検知と対応)とは、https://www.crowdstrike.jp/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/
[19] マンディアント株式会社、エンドポイントにおける検知と対応(EDR)、https://www.fireeye.jp/products/endpoint-security/endpoint-detection-response.html
[20] サイバーリーズン・ジャパン株式会社、Cybereason EDR、https://www.cybereason.co.jp/products/edr/#tabs2
[21] VMware、Endpoint Detection and Response (EDR)、https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-datasheet-edr.pdf
[22] Fortinet,Inc.、Endpoint Detection and Response (EDR) Defined、https://www.fortinet.com/resources/cyberglossary/what-is-edr
[23] MITRE Corporation、MITRE ATT&CK®、https://attack.mitre.org/
[24] MITRE Corporation、Enterprise Matrix、https://attack.mitre.org/matrices/enterprise/
[25] MITRE Corporation、Initial Access、https://attack.mitre.org/tactics/TA0001/
[26] MITRE Corporation、Phishing、https://attack.mitre.org/techniques/T1566/
[27] MITRE Corporation、Drive-by Compromise、https://attack.mitre.org/techniques/T1189/
[28] MITRE Corporation、Replication Through Removable Media、https://attack.mitre.org/techniques/T1091/
[29] MITRE Corporation、External Remote Services、https://attack.mitre.org/techniques/T1133/
[30] MITRE Corporation、Lateral Movement、https://attack.mitre.org/tactics/TA0008/
[31] MITRE Corporation、Internal Spearphishing、https://attack.mitre.org/techniques/T1534/
[32] MITRE Corporation、Taint Shared Content、https://attack.mitre.org/techniques/T1080/
[33] MITRE Corporation、Exploitation of Remote Services、https://attack.mitre.org/techniques/T1210/
[34] MITRE Corporation、Execution、https://attack.mitre.org/tactics/TA0002/
[35] MITRE Corporation、Persistence、https://attack.mitre.org/tactics/TA0003/
[36] MITRE Corporation、Command and Control、https://attack.mitre.org/tactics/TA0011/
[37] MITRE Corporation、Privilege Escalation、https://attack.mitre.org/tactics/TA0004/
[38] MITRE Corporation、Defense Evasion、https://attack.mitre.org/tactics/TA0005/
[39] MITRE Corporation、Credential Access、https://attack.mitre.org/tactics/TA0006/
[40] MITRE Corporation、Discovery、https://attack.mitre.org/tactics/TA0007/
[41] MITRE Corporation、Collection、https://attack.mitre.org/tactics/TA0009/
[42] MITRE Corporation、Exfiltration、https://attack.mitre.org/tactics/TA0010/
[43] MITRE Corporation、Impact、https://attack.mitre.org/tactics/TA0040/
[44] FORRESTER, A Forrester Consulting Thought Leadership Paper, 2021. https://docs.google.com/viewerng/viewer?url=https://threatresearch.ext.hp.com/wp-content/uploads/2021/08/Forrester_Balance_Endpoint_Protection_And_Productivity_Through_Zero_Trust.pdf&hl=en_US