DARKTRACE

NDRソリューション評価のための

バイヤーズチェックリスト

NDRソリューションを
最も効果的に比較

はじめに

ネットワーク検知・対応（NDR）の市場は、乱立するAIの誇大広告とベンダーの訴求で飽和状態にあり、CISOやIT意思決定者が自社のニーズに最適で、本当に効果的なソリューションを見つけ出すことがますます困難になっています。

本ガイドは、体系的な評価フレームワークと実践的なチェックリストにより、NDRベンダーを具体的な基準で客観的に比較できるよう支援します。各チーム、組織ごとにユースケースは異なりますが、これらの基準は市場のベンダーを評価、比較するための第一歩としてご活用いただけます。

第1部

評価手法

この資料の使い方

このチェックリストは、最新のNDRソリューションを評価、比較するためのものです。

第2部では、評価のカテゴリーを、組織のロードマップとROI、対象範囲とデプロイ、ネットワーク挙動分析、検知、アラート、調査、脅威の検知、その他の機能などのセクションに分けて説明します。

各カテゴリーには、解説のほか、NDRのベンダーへの質問リストを記載しています。お求めの機能にハイライトを引き、記載の質問を評価基準の一部として活用されることをお勧めします。

以下の方法を実践すれば、このチェックリストを最大限に活用できます。

ベンダーとの交渉を開始する

チェックリストを使用し、ベンダー候補との**会話のきっかけ**としてご利用ください。チェックリストの基準に基づいて自由回答式の質問をすることにより、貴社の優先事項に対する各ソリューションの適合性を見極めましょう。

ソリューションを比較する

チェックリストを使って体系的に**異なるソリューションを比較**してください。各ソリューションが貴社の必要条件を満たしているか、超えているか、不足しているかを見極めることができます。

懸念点を明確にし、検証する

特定の機能について懸念や不明点がある場合、チェックリストで関連する評価基準を参照して**議論を深め**、より詳細な情報や製品デモを依頼してください。ベンダーからの情報が、正確で事実に裏づけられたものであることを確認しましょう。

機能の優先順位を決める

貴社のリスクプロファイルとセキュリティ目標に基づき、各評価項目に「高」「中」「低」の優先順位を付けてください。これにより自社に**本当に必要な機能**だけを**重点的**に評価できます。

ネットワークセキュリティソリューションを公平、客観的に評価するには、**A/B比較アプローチ**つまりベンダーを同じ基準で並べて比較するのが効果的です。**この方法でバイアスを排除し、実際の機能の違いを明確にし、公平な評価ができます。**

以下は、公平な比較を行うために検討すべき項目です。

展開環境

同一の対象範囲を設定：すべてのソリューションで、関連するサブネットおよび指定のネットワークエンティティにおいて同一の可視環境を確保してください。

具体的なタイムラインを設定： すべてのソリューションを同一環境、同一日数でテストしてください。同じタイムラインを設定することで、各ソリューションで異なる学習期間や学習の進化を比較できます。

チューニングと設定

最適性能で比較：選定したベンダーに、どのようにデプロイするのが最適か相談しましょう。特に複雑なネットワークや特化したいセキュリティ成果がある場合は、それに応じて調整してください。

長期的な運用を考慮：長期を見据えてソリューションを調整してください。短期的な修正や設定プロセスでは、将来の設定要件が明らかになりません。

データの可視性： すべてのソリューションで、評価期間中の全データを保持、検索可能な状態にしてください。

評価

評価基準を統一： すべてのベンダーを事前に定めた同一の評価基準で評価してください。

ベンダーの脅威分類法を理解： ベンダーによって脅威のスコアリング、タグ、説明、基準が異なります。正しく比較するため、これらの違いを十分に理解してください。

能動的な機能、受動的な機能の違いを考慮： 試用期間、PoCの間、非アクティブにしていた機能が、本番運用の際に大きな影響を与える場合があります。レスポンスアクションなどがその一例です。実運用でパッシブ機能がアクティブ化された際に、攻撃に対するソリューションの処理にどのような影響が出るかを考慮してください。

コミュニケーションを維持： 結果が正確でないと思われる場合は、該当するベンダーに連絡してください。これによりベンダーのサポート力と問題解決能力を見極めることができます。

まとめ

結果に基づいてソリューションを評価：自社で定めた成功基準と指標で結果を比較してください。これらは、アラートノイズの削減、重大インシデントの発生数、テスト期間中にアナリストが調査に費やす合計時間の削減などを含みます。

定性的な要素も評価：数値だけではなく、質的な要素となる総合的なユーザー体験、ベンダーチームとの協力関係、サポート体制、統合機能、ベンダーのプラットフォーム全体の能力も考慮してください。

評価基準と結果を審査：社内で結果と評価基準を確認し、選定したベンダーに必ず結果を共有してください。

第2部

評価カテゴリー

以下のチェックリストは、組織が最新のNDRソリューションを評価する際に検討すべき主要な機能をまとめています。ベンダーを体系的に比較するためのツールとして活用してください。各ソリューションがもつ機能の有無だけでなく、機能の質、効果、手法も評価していきます。一部のベンダーは特定の機能や能力を謳っていますが、その内容を深く検証すると、セキュリティー上意義のある成果には結びつかないことがあります。

ひとつのベンダーがすべての機能を満たす必要はありませんが、このチェックリストを使うことで、自社のネットワークセキュリティに対する期待要件が確立できます。

組織のロードマップとROI評価

評価基準	ベンダーへの質問項目
ビジネスケースのパラメータ	▪ ベンダーはROI（投資収益率）モデル、TCO（総所有コスト）、ライセンスモデルの明確さ、運用に必要なリソースの負担について提示していますか？
セキュリティ運用におけるAIの使用方法に関する透明性	▪ ベンダーは、検知、アラート、対応におけるAIの使用方法を明確に説明していますか？AIモデルの種類（教師あり学習、教師なし学習、ルールベース等）、学習データの出所、偽陽性への対処法、アナリストの管理メカニズムに関する詳細は含まれていますか？ ▪ ベンダーはAIに関する以下の規制のいずれか、もしくは双方に準拠していますか？： ▪ ISO/IEC 42001:2023 - AIマネジメントシステム規格 ▪ ISO/IEC 23894:2023 - AIリスク管理規格 ▪ ベンダーはAIの限界、判断根拠の説明機能、アップデートの通知と管理方法を文書化していますか？
ベンダーの透明性とロードマップの調整	▪ ベンダーは、製品の文書一式、定期的なリリースのサイクル、長期的なサポートモデル、および顧客の要望をロードマップに反映する体制を有していますか？
製品のスケーラビリティと性能指標	▪ ベンダーは、スループット、センサー密度、レイテンシ、取り込み容量などの指標で、規模や利用負荷が増大した場合に対応できますか？
価格のスケーラビリティ	▪ ベンダーは、ボリューム・複数年割引をなど、スケーラブルなライセンスモデルをサポートしていますか？
デプロイの柔軟性	▪ ベンダーは、マルチ環境でのデプロイをサポートしていますか？（オンプレミス、仮想ネットワーク、コンテナ環境、ハイブリッドクラウド、リモートデバイス、メール、OTデバイス、エアギャップ環境など）
ライセンスの柔軟性	▪ ベンダーは、オンプレミスのIPをクラウドワークロードへ移行するなど、インフラの変更に応じた柔軟なライセンスオプションを提供していますか？
コア機能	▪ ベンダーのコア製品にはどの機能が含まれていますか？どの機能が別料金または追加ライセンスが必要ですか？

対象範囲とデプロイ

項目	説明	主要検討ポイント
アウトオブバンド監視	本番環境への影響を回避するよう、ネットワークトラフィックをパッシブに監視	▪ SPANセッションやTAPを通じたポートミラーリングを通常はコアスイッチ内に実装 ▪ 生のネットワークトラフィック（パケット）の解析 ▪ インライン展開ではなくパッシブネットワーク監視 ▪ ユーザーやアクティブスキャンに依存せず、すべてのネットワーク資産を自動的に識別 ▪ ソリューションはデフォルトでエージェントレス ▪ 取り込まれるデータの品質（例えば、単に送信元と宛先のIPのみか）通常、データが豊富であるほど解析の精度は向上
連携機能	サードパーティーのテクノロジーを接続し、検知、対応、調査のワークフローを強化	▪ 以下のツールに依存することなく、連携、統合が可能： ▪ ファイアウォール、VPN、SASEおよびZTNAソリューション ▪ EDRおよびXDRソリューション ▪ SIEMおよびSOARプラットフォーム ▪ Microsoft 365 ▪ Microsoft AzureやAWSなどのクラウドサービス ▪ Microsoft Entra ID、Okta、DuoなどのIAMプラットフォーム ▪ Dropbox、Salesforce、Slack、ZoomなどのSaaSアプリケーション ▪ Rapid7やTenableなどの脆弱性管理ツール ▪ ServiceNowやJiraなどのワークフロー・チケット管理ツール ▪ 脅威インテリジェンスフィードおよび既知のCVEによる強化
データ保持	分析と調査のための生のネットワークパケットとメタデータの保持	▪ 以下を保持する能力： ▪ PCAPファイル ▪ フローおよび主要メタデータ ▪ より深い調査のためのログデータ
エアギャップ方式の高セキュアな分離ネットワーク	エアギャップ環境において中核的な機能を失わない	▪ アウトバウンド接続なしでの完全な独立運用オプション ▪ 全てのデータを提供される機器内で現場において保持できる ▪ 外部接続に依存せず以下が可能： ▪ 検知と対応 ▪ インシデント調査 ▪ 継続的なAIモデルの更新 ▪ サードパーティ脅威インテリジェンス ▪ PCAPの保存と検索 ▪ カスタム検知・対応モデルの作成 ▪ システムおよび検知・対応モデルのカスタム設定と編集

項目	説明	主要検討ポイント
クラウド環境、ハイブリッドクラウド、IaaS、PaaS、SaaS	完全クラウドベースおよびハイブリッド環境のカバレッジと可視性	▪ クラウド環境にネイティブでネットワークカバレッジを拡張し、単一プラットフォームで両環境を可視化 ▪ 完全クラウドネイティブおよびハイブリッド環境への展開、オンプレミスからクラウドへの移行時も可能 ▪ AWS VPC Flow Logs、Azure NSG Flow Logsなど、フローログの取り込み ▪ デフォルトでエージェントレス、またはVPCトラフィックミラーリングや仮想TAPを活用 ▪ コンテナやサーバーレスアプリケーションなどの一時的なリソースを含むAzureのアーキテクチャを動的にマッピング ▪ 仮想マシンおよびコンテナオーケストレーション環境での展開オプション ▪ アイデンティティ、コントロールプレーン、ネットワークコンテキスト把握のため、AWS Security Hub、IAM、CloudTrailならびにAzure相当サービスと統合
OT/CPSおよびIoTデバイス	運用技術（OT）/サイバーフィジカルシステム（CPS）およびIoTデバイス（IoT、IIoT、mIoT、BMS、SCADA、HMI、PLC）のカバレッジと可視性	▪ 統合および分離されたIT/OTシステム、IoT、IIoT、リモートエッジデバイスを単一プラットフォームでネイティブ対応 ▪ 完全なエアギャップ環境で展開が可能 ▪ OT固有のプロトコルを横断したディープパケットインスペクションを実行可能 ▪ OT資産インベントリーと脆弱性インサイトのためのアクティブディスカバリー ▪ Level 0の物理プロセスからLevel 5のエンタープライズネットワークまで、Purdueモデルの全階層対応 ▪ ソリューションはベンダー非依存 ▪ リアルタイムでの資産の挙動、ネットワーク露出、悪用可能性の分析による継続的なリスク評価および脆弱性相関分析の実施
リモートワーカーエンドポイント	リモートワーカーデバイスの完全なネットワーク可視性	▪ リモートワーカーのエンドポイントおよび移動デバイスに対する完全なネットワーク可視性、EDRアラート対応 ▪ ネットワークインフラが不十分な小規模サテライトオフィスや共有ワークスペースのカバレッジ

ネットワーク挙動分析

項目	説明	主要検討ポイント

人工知能および機械学習	脅威検知、調査、対応に複数のAI技術を活用	▪ 以下の、逐次・階層的に構成されたAIの多層アプローチ：
		  ▪ 教師なし機械学習
		  ▪ 教師あり機械学習
		  ▪ ベイズ学習
		  ▪ クラスタリングアルゴリズム
		  ▪ アンサンブル手法 グラフニューラルネットワーク（GNN）
		  ▪ 自然言語処理（NLP）
		  ▪ ドメイン特化言語モデル（DSLM）
		  ▪ セキュリティ特化型カスタム大規模言語モデル（LLM）

自己学習型AI	導入した環境の特徴を自律的に学習し、自動適応を行うAI	▪ 事前定義されたルールやシグネチャに依存せず、各固有環境における「正常」の状態を学習 ▪ 過去の攻撃データではなく、正常な挙動として見なされているものに基づき、異常なアクティビティを検知 ▪ 従来のツールと比較し、継続的な手動での検知エンジニアリングを大幅に削減 ▪ 環境の変化に自動的に適応でき、手動の更新や設定は不要 ▪ 挙動の類似性により、機器をグループとクラスターに自動的に分類 ▪ ソリューションが完全に任意設定可能であり、希望に応じて微調整が可能
AIの展開	継続的な学習とデータ処理のためのAIの配置場所	▪ AIがローカルに展開され、展開された各固有環境に基づき学習する
コンプライアンス	コンプライアンス関連のアクティビティの検知	▪ 生成AIツールの不正利用などのコンプライアンス方針違反を検知する機能 ▪ カスタムのコンプライアンスモデルを作成、編集できる機能

項目	説明	主要検討ポイント
暗号化トラフィック分析	暗号化されたネットワークトラフィックにおける異常および不審なアクティビティを特定可能	▪ 暗号化されたトラフィックにおける既知および新規の脅威を復号せずに検知する機能が実証済み
復号化	暗号化ネットワークトラフィックの復号化	▪ コンプライアンス目的などで必要に応じてネットワークトラフィックの復号化が可能 ▪ ネイティブおよびサードパーティの復号化オプション ▪ 復号化に依存せず、異常や悪意ある挙動を検知
インバウンドおよびラテラルのネットワークトラフィック分析	南北・東西方向のネットワークトラフィックの双方を分析	▪ ベンダーはセキュリティ侵害防止のため、受信ネットワークトラフィックを脅威検知の目的で分析していますか？ ▪ ベンダーはラテラルムーブメント（水平展開）やインサイダー脅威など、組織内の脅威の検知と対応のため、内部ネットワークトラフィックを分析していますか？
保持	ネットワークトラフィック、イベント、その他の関連するメタデータの保存 遡及分析および法令遵守のために、生のネットワークトラフィックとメタデータを保持	▪ 遡及分析および法令遵守を遂行するために、生のネットワークトラフィックとメタデータを保持
資産の可視性	ネットワークエンティティの識別と管理	▪ ネットワーク資産を自動的に発見し、単一の場所にマッピング ▪ 各デバイスごとの資産情報の詳細およびネットワークアクティビティログの閲覧が可能 ▪ デバイスに対する自動および手動のタグ付けにより、容易に識別、検索および管理

脅威の検知

項目	説明	主要検討ポイント
検知モデル	不審、悪意あるアクティビティを検知するAIモデル	▪ セキュリティおよびコンプライアンス・ユースケースをカバーする多様な検知モデル ▪ 追加開発、ベンダーサポート、外部接続が不要、直接UI上で全モデルを閲覧、編集、カスタマイズ可能 ▪ 標準のモデル群ではカバーしきれないコンプライアンス要件や特殊なエッジケースに対応するための、完全なカスタム検知モデルを構築可能
新規脅威検知	AIを活用した異常検知で、過去に基づく指標がない新型攻撃やゼロデイ攻撃を発見	▪ 以下のような脅威に対する保護効果を実証： ▪ 新種ランサムウェアおよびその亜種 ▪ ゼロデイ脆弱性 ▪ 内部脅威 ▪ 正規ツールの悪用 ▪ 以下に非依存： ▪ 脅威インテリジェンスフィード ▪ 他の顧客環境とのデータ比較 ▪ ルールやシグネチャ ▪ CVEの取り込み ▪ ベンダーがルール・シグネチャ・学習データ・事前想定に頼らず、公表前にゼロデイ脅威を検知した実績の詳細事例を、少なくとも3件以上、文書化して提示できること
既知の脅威の検知	既知の脅威を示す異常なアクティビティを照合	▪ ランサムウェアやマルウェアなどの既知の脅威の検知 ▪ 必要に応じて脅威インテリジェンスフィードを取り込み、活用することが可能
既知の侵害	環境内に既に存在する脅威や侵害状況を検知	▪ 類似デバイスやピアグループとの比較によって、異常行動を特定 ▪ 過去の侵害の痕跡を示す不審なアクティビティを特定
アカウント乗っ取りとラテラルムーブメント（水平展開）	乗っ取られたアカウントがシステム間を横断し、アクセス権限を広げて制御を奪う行動を検知	▪ 内部ネットワークトラフィックの異常を分析する機能はありますか？ ▪ 侵害された認証情報やセッションハイジャックを、ネットワークアクティビティと関連付けすることが可能ですか？ ▪ インバウンド、アウトバウンド、ラテラルネットワークフローの分析 ▪ 異常な通信パターンを特定するための行動モデリング機能 ▪ 高精度イベントのシミュレーション ▪ ネットワーク、エンドポイント、アイデンティティ、SaaS等を跨いだクロスドメインの相関分析機能
C2通信	DNSやHTTPSなど、一般的なプロトコル内に潜む悪意あるコマンド＆コントロール（C2）トラフィックを識別	ベンダーは以下を検知できますか： ▪ ビーコニングパターン（定期的な間隔でのコールバック） ▪ DNSトンネリングやICMPベースのC2など、一般的でないプロトコルの利用 ▪ 既知の悪意あるIPやドメインへの接続 ▪ 非標準ポートや想定外サービスを使った暗号化C2通信

項目	説明	主要検討ポイント
マルウェアとペイロードの配信	実行前に、ネットワーク上での悪意あるファイルやコードの転送を検知	▪ ベンダーは以下の兆候を検知できますか： ▪ SMB、FTP、HTTP を経由した悪意あるファイルの転送 ▪ 不審な実行ファイルの転送やペイロードの投下 ▪ TFTPやTelnet など、一般的ではない、または廃止されたプロトコル経由の配信
内部脅威の行動および正規認証情報の悪用	正規ユーザーによる異常なアクティビティにフラグを立て、悪意や過失の可能性を検知 盗用または意図的に共有された有効認証情報の不正利用も特定	ベンダーは以下の兆候を検知できますか： ▪ 権限の乱用 ▪ 異常なデータアクセスまたはデータ転送 ▪ 認証やセッション動作の異常 ▪ 不明または信頼されていない外部ホストへの データ転送や持ち出し ▪ 通常とは異なる、または新規の外部宛先への 大容量送信 ▪ 不明ドメインへのDNSやHTTPSなどの隠れチャネル経由で送信されるデータ ▪ 通常FTPやSFTPを使用しないエンドポイントからの異常プロトコルの利用 ▪ トリクル送信など、DLP回避を狙った異常なタイミング
CVEの悪用	システム、サービス、アプリケーションにおける既知の脆弱性を悪用	▪ ネットワーク全体で以下のような異常なアクティビティを検知： ▪ 異常なログインアクティビティ ▪ 異常なデータ転送 ▪ 異常なエンドポイントへの接続 ▪ 異常な内部ネットワークスキャン ▪ SMBによる偵察活動 ▪ ラテラルムーブメント ▪ 権限昇格
不審なスキャンおよび偵察活動	攻撃に先立つネットワーク資産の探査やマッピング活動を特定	内部ネットワークに対するスキャンおよび偵察手法の検知
データ漏洩の検知	暗号化されていても外部やクラウド宛先への機密データの不正な移動にアラートを通知	異常なエンドポイントへの接続の検知 WeTransferやDropboxなどのファイル共有サイトへの接続とアップロードの検知 大容量の内部ダウンロードや内部ロケーションへの異常接続の検知

トリアージと調査

項目	説明	主要検討ポイント
自動トリアージ	アラート疲労を引き起こす手動トリアージと調査作業を排除	▪ ネットワークイベントの自動トリアージと調査により、最も異常で注目すべきアクティビティのみを表面化 ▪ 自己学習により通常の挙動を理解し、継続的に更新する機能 ▪ 人的介入やプロンプト、スクリプトが不要
アラートの優先順位付けおよび管理	重要度に基づきアラートの優先度を決定	▪ 最も重大なアクティビティを自動的に優先順位付けし、アナリストに通知 ▪ 重大、情報、コンプライアンスといったカテゴリーでアラートを分類 ▪ 特定ユーザーへのアラートの割り付けが可能 ▪ モバイルアプリおよびブラウザーを介したアラートの表示と管理が可能 ▪ ServiceNowやJiraなどのサードパーティソリューションと接続が可能

アラートの相関	複数の関連アラートを、単一のインシデントとして相関付け	▪ NDR、OT、メールなど、ベンダー独自プラットフォーム内のアラートを相関付け
		▪ 以下を含むサードパーティーテクノロジーからのアラートを相関：
		  ▪ EDR/XDR
		  ▪ SASEおよびZTNA
		  ▪ SaaSアプリケーション
		▪ 人的介入なしで複数の関連アラートをグループ化し、真のインシデントを特定

AI主導の調査	生成AIベースではないエージェント型AIシステムが自律的にエンドツーエンドの調査を実行	▪ 関連アラートを既存または新規インシデントに自動統合し、重大ケースを人的レビューへエスカレーションする機能 ▪ エージェント型AIによるレベル2 SOCアナリストと同等の調査品質 ▪ プロンプトベースのチャットボット、生成AI、人的介入には非依存 ▪ 外部ソースによって、手動または自動での調査開始が可能 ▪ AIが、各インシデントごとに完全レポートを自動生成し、完了した調査プロセスのタイムラインと明確な説明を表示 ▪ 上位ライセンスやマネージドサービス限定ではなく全顧客が利用可能
脅威ハンティングおよび高度分析	脅威ハンティング、より詳細な調査、法医学分析、インシデント対応のための追加機能	▪ 必要に応じて手動でPCAPをダウンロードし、分析が可能 ▪ シンプルなクエリによるネットワークトラフィックの高度な検索と分析が可能で、カスタムクエリの作成と保存が可能 ▪ 上級ユーザー向けの、複雑なクエリ構文を使用した構造化検索の構築が可能 ▪ 高度な検索機能がコア製品の機能に含まれており、追加ライセンス、追加費用、外部接続が不要

封じ込めと対応

項目	説明	主要検討ポイント
自律対応	脅威に対する最適な対応策を自律的に実行	▪ 24時間365日、自律的かつ機械速度で稼働 ▪ 人的介入なしで、最も効果的な応答アクションを選択し、適用が可能。 ▪ 脅威の進化に応じて、応答アクションの深刻度を自律的にエスカレーションすることが可能 ▪ 必要に応じて、応答アクションを実行する前に、人的確認を要求するよう設定することが可能 ▪ サブネット、時間帯、曜日などでの設定が可能 ▪ 対応モデルとパラメータの詳細を完全にカスタマイズ可能 ▪ 静的ルールやシグネチャが不要 ▪ 新規脅威、既知脅威、内部脅威の最も初期段階での封じ込め実績
ネイティブ対応	サードパーティ技術に依存せず、ベンダーがネイティブに応答アクションを実行できる能力	▪ EDRやファイアウォール統合なしでネットワーク脅威にネイティブ対応が可能 ▪ 業務を中断せず、特定トラフィックをブロックする対象絞り込みアクションの実行が可能 ▪ ネットワークエンティティにおいて正常と見なされるアクティビティのみを許可し、それ以外のすべての遮断が可能 ▪ デバイス群のピアグループで正常と見なされるアクティビティに基づいても適用が可能 ▪ セグメンテーションがほとんどないフラットネットワークでも動作が可能
サードパーティーの対応	ネイティブでの対応能力を強化するために、サードパーティ技術と連携する能力	▪ 応答アクション能力を拡張するため、以下のサードパーティソリューションと統合が可能： ▪ EDR/XDRソリューション ▪ ファイアウォール ▪ Microsoft 365とEntra ID ▪ SIEMとSOAR
脅威の封じ込め	最も初期の段階で脅威の進行を阻止	▪ EDRアラートや手動の調査開始を待たずに、脅威アクティビティの最も初期の兆候で対応が可能 ▪ 通常の業務活動を中断することなく、脅威または不審な挙動を封じ込めが可能 ▪ アナリストが対応する時間を確保するため、必要に応じて封じ込め期間の延長が可能 ▪ 認識されていない新規ネットワークエンティティを自律的に隔離するのに使用が可能

その他の機能

項目	説明	主要検討ポイント
レポーティング	検知データを優先度付きの明確なレポートに変換し、セキュリティ運用やサイバーコンプライアンス対応を支援することで、NDRの価値を向上	▪ PCI-DSS、GDPR、HIPAA、ISO 27001、NIST、SOC2、MITRE ATT&CK、IEC 62443などの基準に沿ったコンプライアンスレポートを継続的に生成が可能
継続的脅威エクスポージャー管理(CTEM)	NDRを補完し、脆弱性を先回りして特定し、低減するとともに、攻撃者がネットワークで悪用可能な攻撃経路を表示することが可能	▪ パッチ遅延やCVEリスクの一般論を伝えるのではなく、自環境向けの独自の具体的なリスクスコアリングを生成 ▪ 侵害リスクが最も深刻なユーザー、デバイス、脆弱性に対するサイバーリスクディスカバリーを優先順位付けして表示が可能 ▪ インシデント発生時に影響を受ける資産への潜在的な影響を評価し、最も重大な攻撃経路に沿った効果的な対応が可能
インシデント対応準備および復旧	インシデント対応能力のテスト、改善、検証を支援	▪ ベンダーは貴社に特化したアーキテクチャ、構成、技術スタックを反映したシミュレーションを提供していますか？ ▪ そのソリューションは机上演習ではなくクラウド、SaaS、OTインフラを含む実際の環境でリアルなインシデントをシミュレーションできるものですか？ ▪ そのシステムは、クラウド移行後やM&Aなどの環境変化に合わせて進化する適応型・動的プレイブックをサポートしていますか？ ▪ セットアップと継続運用に必要なライセンス、リソース、スキルは何ですか？
攻撃対象領域管理(ASM)	外部公開資産とエクスポージャーをマッピングし、高価値または高リスクシステムに関連する検知を優先順位付けすることでNDRに情報を提供	▪ そのソリューションはIP範囲やシードデータ不要で、AI技術により未知の資産やシャドーIT資産を自動的に発見できますか？ ▪ そのソリューションはサードパーティドメイン、クラウドインスタンス、IoTインフラで、貴社のブランドに関連する資産を検知できますか？ ▪ そのソリューションはデジタルフットプリントを継続的にクローリング・監視し、新規または変化するエクスポージャーを特定できますか？ ▪ そのソリューションは定期スキャンに依存せず、ゼロデイや影響が大きい脆弱性を検知可能ですか？ ▪ 中央ITガバナンスの統制外で作成された、無許可または監視対象外のドメイン、サービス、資産を検知できますか？ ▪ そのソリューションはフィッシングドメインやなりすましインフラを含む、サプライチェーンおよびブランド濫用リスクに対応していますか？ ▪ そのASMソリューションは、なりすましドメイン防御、エンドポイントコンテキスト、AIアナリスト相関などの他のNDR機能を強化できますか？ ▪ 内部テレメトリや他のリスク管理ツールと組み合わせた統一ビューを提供可能ですか？
Eメールのセキュリティ	Eメールセキュリティと NDRの統合	▪ 受信箱のクロスドメイン脅威を受信後のネットワークアクティビティと自動相関させる能力 ▪ ツール同士が連携して脅威検知の精度向上と調査の高速化を実現できますか？ ▪ 受信箱からネットワークまでの多重防御のアプローチを提供

ボーナスセクション

AIの評価方法

AIはサイバーセキュリティの特効薬として位置づけられていますが、多くのセキュリティチームにとって疑問が残るのは、実際の技術の中身です。多くのツールはAIを採用していると主張しますが、実際は単に教師あり機械学習や生成AIモデルに依存している場合が多く、それらは限定的かつ明確に定義されたシナリオでのみ有効であり、新規の脅威を検知する能力に欠けています。

NDRソリューションのAI評価では、単一モデルや生成AIベースのLLMのような一つのAIタイプの結果だけに頼らないことが重要です。これでは限定的な結果しか得られず、不完全で偏った結果を生成する可能性があるからです。

この課題は、AIを悪用した脅威の増加によりさらに深刻化しており、より適応的で知的な防御が求められます。このようなAI能力を評価する明確な方法がないと、組織は遅れを取るか、最悪の場合不意を突かれるリスクがあります。

実際、すべてのAIが同じではありません。AIがサイバーセキュリティで効果を発揮するためには、うわべだけの宣伝文句を超えて、多様な先進技術を統合し、現代の脅威の複雑性に対処する必要があります。セキュリティ担当者は、組織ニーズに対するAI有効性を評価し、より強固なセキュリティ態勢を構築するため、どのAIがどのユースケースに使われているかを理解する必要があります。

攻撃中心型

ビジネス中心型

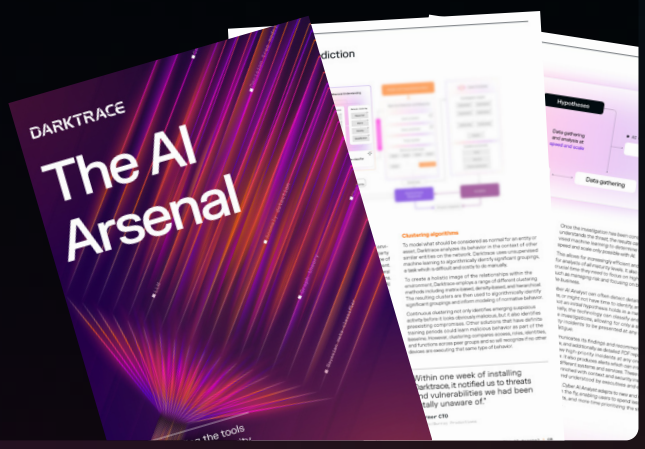
この図は、ビジネスデータを活用して挙動の異常を検知するAIベースのセキュリティツールと、過去の攻撃データで訓練されて脅威を捕捉するツールとの比較を示しています。

貴社のソリューション導入の各ステップを支援するため、サイバーセキュリティにおけるAIの3つのガイドをご用意しました。

サイバーセキュリティにおけるAIの活用を徹底検証

AI Arsenalホワイトペーパーをダウンロードして、AIモデルがサイバーセキュリティにどう活用されるか、Darktraceの自己学習AIが多層技術でプロアクティブ、レジリエントな脅威防御を実現する方法をご確認ください。

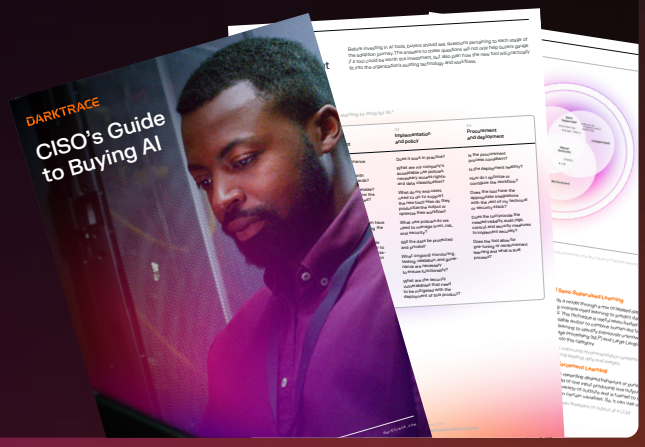
詳細はこちら ↗



AIを活用したセキュリティソリューションを評価する

CISOのためのAI購入ガイドホワイトペーパーをダウンロード。このホワイトペーパーでは、AIベースのソリューション購入時にバイヤーがどのようにアプローチすべきかを解説します。AI導入の各段階における主要な検討事項、ベンダーに尋ねるべき具体的な質問、および回答で確認すべきポイントを解説します。

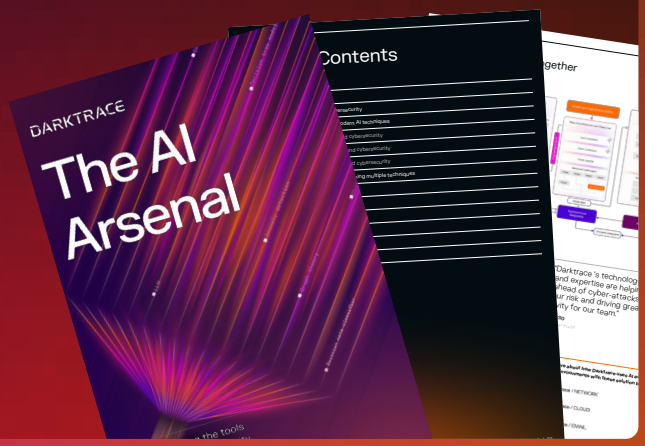
詳細はこちら ↗



組織のAI進化を評価する AI成熟度ガイド

AI成熟度モデルホワイトペーパーをダウンロード。このホワイトペーパーでは、AI成熟度モデルを徹底解説します。CISOとサイバーセキュリティ部門リーダーがAI導入を理解・評価・戦略立案・推進するための唯一のフレームワークです。

詳細はこちら ↗



第3部

評価プロセス

■ ステップ 01：

商業的評価

最初のフェーズは商業的評価、ディスカバリープロセスです。

その内容は、選定候補のソリューションが貴社のニーズに合致しているかを評価するものです。コア機能はもちろん、業務の流れへの適合性、運用モデル、さらには総合的な価値に対する期待要件も含めた多角的な評価対象となります。

このプロセスを実施する際の検討事項として、以下の点を強く推奨します。

ベンダーと積極的に交流する
評価プロセス全体を通じて、ベンダーとのオープンなコミュニケーションを維持します。ベンダーと協力して、パフォーマンスの相違点を特定・理解します。このように協力して取り組むことで、ベンダーの対応力をテストしつつ問題を迅速に解決でき、正確なデータに基づく意思決定が可能となります。

人とのつながり、パートナーシップを考慮に入れる
ソリューションの利用体験に大きな影響を与える人的要素を評価します。ベンダーの現地拠点とベンダーの顧客担当チームの体制の充実度を評価します。既存のマネージド・セキュリティ・サービス・プロバイダー（MSSP）が存在する場合はその関係性も含めて検証します。強固なパートナーシップとアクセスしやすいサポートは、長期的な成功と満足度に不可欠です。

類似するライセンシングを比較する
必ず類似したライセンスパッケージのソリューションを比較してください。一部のベンダーは同等の機能が備わらない異なるパッケージを提供している場合があります。公平に比較するため、どのような機能が含まれているか、付加価値機能があるか、明確に把握します。

購入後のサポートを考慮する
ベンダーが購入後にも強力なサポートを提供しているか、定期更新、トレーニング、認定資格、各種イベント、迅速なカスタマーサービスなども含まれtいるか確認しましょう。他の顧客およびガートナー等の業界アナリストレビューを参照し、トライアルやオンボーディング以降も長期的に価値を認識、推奨しているかを判断します。

■ ステップ 02：

技術的評価

第二の主要なステップは、技術的評価です。ここでは日々ソリューションを利用するユーザーに参加してもらうことが重要です。

このディスカバリープロセスにより、ソリューションが組織のパフォーマンス、ユーザビリティ、統合要件をどの程度満たすかを判断します。また、デプロイメントアーキテクチャ、検知効果、AI活用、ポリシー施行、既存インフラとの互換性などの重要要素を評価できます。

以下は、技術的評価を実施する際に検討すべき主要な要素です。

最適なパフォーマンスデータに基づいて評価します。

選定したソリューションは、必ず完全にデプロイした後で、評価してください。特に教師なし機械学習を使用するソリューションは、初期学習曲線が存在するため特に重要です。ベンダーと連携し、これらを確認するとともに、必要なインテグレーションの展開など、理想的な条件の下で、各ソリューションの本来のポテンシャルを理解します

学習曲線を評価する

単一時点での検知能力だけでなく、時間経過に伴う改善率と成熟度も評価してください。これにより、ソリューションの長期的な精度を正確に把握できます。

AIモデルとファインチューニング機能

ベンダーがAIモデリングと機能について透明性を完全に開示しているか確認してください。検知と対応モデルを組織のニーズに合わせて細かく微調整できるようにし、ベンダーの標準モデルライブラリではカバーされていない特定のユースケースに対応するためのカスタムモデルを自ら作成できる機能も必要です。

明確で透明性の高い説明

すべての検知・調査・対応アクションには、透明な説明が必ず伴うべきです。トリガーされた検知モデルが何であるか、自動調査の背後にあるロジック、および応答アクションの詳細リストを把握してください。この透明性は信頼と効果的な評価に不可欠です。

定量分析と定性分析を組み合わせる

AIマーケティングの訴求を超えて、特定環境でのソリューション能力を定性的、定量的分析で評価してください。可視性、検知の正確性、総合的なユーザビリティなどの要素に加え、既存ワークフローと比較可能な、トリアージと調査時間、生成インシデント総数、平均対応時間などの定量的な指標を評価します。

脅威分類を統一して比較する

ベンダーごとに脅威の分類が異なるため、評価に不整合が生じる可能性があります。必要に応じてベンダー確認を行い、同等メトリクスで比較します。これにより公平で正確な比較が可能になります。

すべての偽陽性を同等に評価しない

「偽陽性」の定義は、評価対象のソリューションにより異なることを理解する必要があります。例えば異常検知をベースにしたビジネス中心型のツールは、異常なアクティビティを検知してアラートを発します。これは正当な検知ですが、異常は必ずしも「悪意」とは限らず、従来の偽陽性の定義には該当しません。熟練アナリストと同様に、AI異常検知ソリューションは、利用可能なデータに基づいて疑わしいアクティビティを特定し、それを調査・対応のコンテキストとして活用します。より的確な評価が行えるよう、各ソリューション内における偽陽性のコンテキストと影響について十分に把握し、不明な点はベンダーに偽陽性の定義について確認してください。チームにとって懸念事項と思われないアラートを、簡単に確認、処理済みにできるかをテストしてください。

まとめ

このチェックリストが、複数のNDRソリューションを評価し、貴社ニーズに最適なものを選定するための実践的フレームワークとしてご活用いただけることを願っています。

このフレームワークを入手いただいた今、Darktrace / NETWORKを実際の環境で試す無料30日トライアルを開始しませんか。

デモを申し込む ↗

■ **Darktraceについて**

Darktraceは、日々変化する脅威環境から組織を守り続ける、AIサイバーセキュリティのグローバルリーダーです。2013年英国ケンブリッジにて設立されたDarktraceは、企業ごとにリアルタイムで学習するAIを活用し、未知の脅威から組織を守るために不可欠なサイバーセキュリティプラットフォームを提供しています。Darktraceのプラットフォームおよびサービスは当社が擁する2,700名以上のセキュリティ専門家に支えられ、世界10,000社近くの顧客を保護しています。詳細はwww.darktrace.comをご覧ください。

北米：+1 (415) 229 9100
ヨーロッパ：+44 (0) 1223 394 100
アジア太平洋：+65 6804 5010
中南米：+55 11 4949 7696

darktrace.com | info@darktrace.com