DARKTRACE

モダンセキュリティスタックの構築

なぜNDRとメールセキュリティは連携が必要なのか?

目次

要約

多くのサイバー攻撃は受信箱から始まりますが、そこが最終目的地であることは稀です。脅威アクターは、メールで始まりネットワークやクラウド環境へ急速に拡散するAI駆動型の多段階攻撃を継続的に仕掛けています。この環境下では、サイロ化されたセキュリティソリューションは攻撃の全体像を把握できず、防御の速度を低下させる重大な死角を残してしまいます。現代の脅威に対する最も効果的な防御策は、メールセキュリティとネットワークセキュリティを深く連携させる統合的なAIアプローチです。

このホワイトペーパーでは、以下を詳しく探ります：

- AIがどのように多段階・多領域攻撃を加速させているか
- サイロ化されたメールとネットワークソリューションが対応しきれていない理由
- 統合された多層のAIアプローチが脅威の検知と対応を向上させる仕組み
- 統合アプローチによるセキュリティ、運用、商業上のメリット

統合セキュリティが もはや選択肢ではない理由

AIの助けを借りて、メール攻撃がより巧妙になっています

メールは依然としてサイバー犯罪者が最も標的とする、効果的な初期侵入経路の一つとなっています。さらにAIによってこれらの脅威は急速に巧妙化・高度化し、検知が困難になっています。脅威アクターは生成AIを活用し、高度にパーソナライズされたフィッシングメールを大量に作成すると同時にQRコードフィッシングのような新たな手法も悪用しています。

ガートナー社によれば、メールは依然としてマルウェアや認証情報の窃取における主要な攻撃経路で、その目的はネットワーク侵害にあります。

- **23%のセキュリティリーダー**
  が、組織に対する最近の外部攻撃の根本原因としてソーシャルエンジニアリングを挙げ、**フィッシングが21%でそれに続きました**。

（2024年のフォレスター社によるセキュリティ調査）

ネットワークの脅威も同様です

組織内部に侵入した攻撃者は、AIを活用して攻撃ライフサイクルの全段階を加速・自動化することができます。

AIの悪用例は以下が挙げられます：

- 潜在的なインフラストラクチャおよび無料ホスティングプロバイダーの調査
- 標的組織に対する迅速な偵察
- 適応型マルウェアの挙動
- 大規模な認証情報の収集
- ペイロード開発
- 悪意あるスクリプトの作成支援およびセキュリティ回避技術の支援

AIの進化によって、攻撃者は以前より迅速に、より高い精度で、そしてはるかに大規模な攻撃を実行できるようになりました。英国の国家サイバーセキュリティセンター（NCSC）によれば、AIは2027年までに攻撃者が脆弱性を悪用する能力をほぼ確実に強化し、国家・非国家主体双方による高度な侵入攻撃の実行を容易にする、とのことです。

しかし、すでにセキュリティ専門家の74%が「AI駆動型攻撃が組織にとって重大な課題となっている」と回答しています(AIサイバーセキュリティの現状 2025)。

サイロ化されたソリューションでは不十分な理由

複雑化する脅威環境に対応するため、多くの組織ではベストオブブリードのツールを寄せ集めのように導入しています。メールセキュリティ用、ネットワーク監視用、エンドポイントやクラウド防御用などと、それぞれ別のツールが存在します。しかしこのようにサイロ化されたソリューションでは、お互いが効果的に連携し合うことは稀です。

おそらくこれらのツールはSIEMやSOARプラットフォームでデータを共有し、攻撃の全容を理解するのに必要なコンテキストを欠いたアラートを生成していると思われます。この断片的なアプローチでは攻撃チェーンの段階の間に死角を生み出し、セキュリティチームが、分断されたダッシュボードやログから起きた事象を手動でつなぎ合わせざるを得なくなるでしょう。攻撃者が環境内をより迅速で巧妙に移動するにつれ、検知と調査の遅れが壊滅的な結果をもたらす可能性があります。

EDRやXDRソリューションへの多額の投資をしてもなお、特にネットワークアクティビティで監視の隙が生じ、SOCの可視性に対する誤った自信を生み出しています。現代のネットワーク全体にエージェントを設置することはできず、従来の「既知の悪意ある」アクティビティにのみ焦点を当てるツールでは、未知の脅威、新たな脅威、内部者による脅威を検知することはできません。

現実は明らかです：

真に統合されたソリューションのみが、メールとネットワークテレメトリをシームレスに連携させ、AI強化型攻撃を検知し対応するのに必要な速度、可視性、流動性を提供できるのです。

攻撃の舞台裏：脅威が受信箱から社内侵害へと広がっていく仕組み

Darktraceが観測した最近の攻撃を見てみましょう。

当該顧客はDarktraceを検知専用モードで設定しており、対応機能が有効化されていなかったため、セキュリティチームがDarktraceの警報に対応するまで侵害行為がエスカレートし続けました。

自律応答が有効化されていれば、攻撃を封じ込める迅速な措置を講じていたはずです。そのような状況でも、Darktraceは顧客のデジタル資産の各領域を可視化して攻撃の全容を把握することができたため、顧客は迅速に修復措置を講じることができました。下図は、攻撃がこの環境下でどう進行したかを示しています。

この脅威事例は、現代の攻撃に見られる共通パターンを浮き彫りにしています：

攻撃者はメールからネットワーク、そしてその先へと、デジタル資産全体をスムーズに移動します。セキュリティがサイロ化して運用されると、防御側は断片的な情報しか得られず検知が遅れ、対応が妨げられて、最終的に攻撃者に優位に立たせてしまいます。

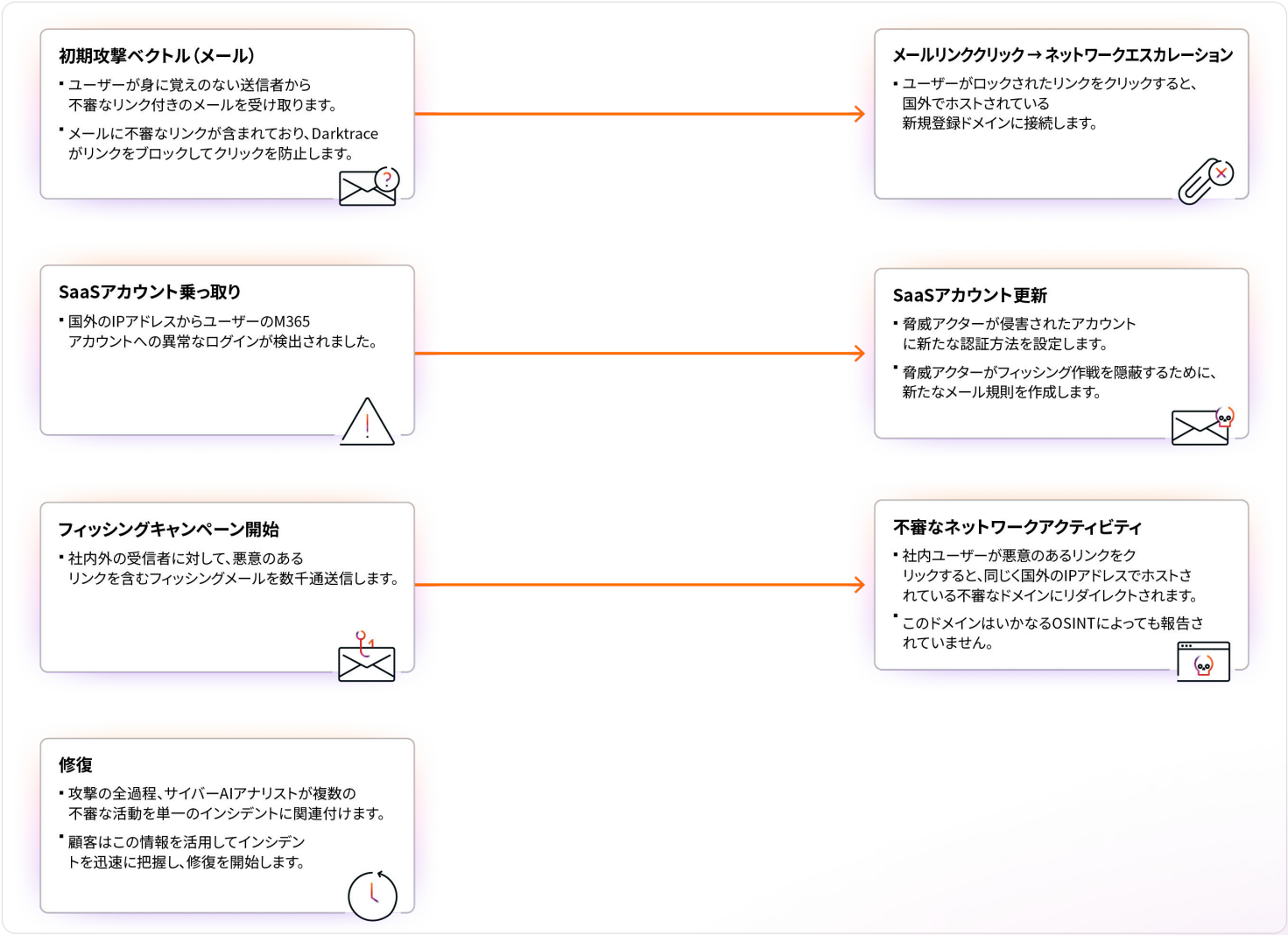


Figure 01: メールからネットワークおよびSaaSへの攻撃進行を示す図

Darktrace / NETWORK + / EMAIL

2つの最高水準のソリューションと1つのAIアプローチ

Darktrace / NETWORKおよびDarktrace / EMAILは、
それぞれが業界をリードする強力なソリューションです。

/ NETWORK

リーダーとして認定（2025年Gartner® Magic Quadrant™ for NDR）、Darktrace / NETWORKは強力な多層AIを現代のネットワークに展開。既知・未知の脅威をリアルタイムで無効化します。

ガートナー・ピア・インサイト: ★★★★★ 4.7* (2025年8月時点で465件の評価)

99%

Darktrace / NETWORKは既存の従来型NDRベンダーと比較すると、**アラートノイズをほぼ99%削減することが実証されています**

（エネルギー分野のDarktrace顧客）

08

Darktrace / NETWORKは、ゼロデイ脆弱性を公式発表の平均**8日前に検出し封じ込めます**

(Darktraceによるリサーチ)

/ EMAIL

カスタマーズチョイスに選出（2025年Gartner® Peer Insights™ Voice of the Customer for Email Security）、Darktrace / EMAILは業界初のAIイノベーションをメッセージングエコシステム全体に展開。新規・標的型攻撃を阻止します。

ガートナー・ピア・インサイト: ★★★★★ 4.8* (2025年8月時点で323件の評価)

55%

Darktrace / EMAILによって検出された**脅威の55%**が、既存の全セキュリティ層を突破

(2024年 年間脅威レポート)

13

Darktrace / EMAILは**他のソリューションよりも13日早く脅威を検知**

(Darktraceによるリサーチ)

独自のAIアプローチを製品の要に

Darktraceのネットワークとメール製品が**これほど強力な理由とは？**

これらを支えているのがAIであるためです。

ほとんどのサイバーセキュリティベンダーは、依然としてルールとシグネチャベースの旧来の検知手法に依存しています。AIを使っていても、通常は既知攻撃データと脅威インテリジェンスで訓練した教師ありモデルに限定されます。既知の脅威を特定する効果はあるものの、このようなモデルは継続的な再学習を必要とし、過去のパターンに一致しない新規またはAI駆動型の攻撃には依然として対応が困難な状況です。結果、検証不可能な異常と信頼性の低いアラートが氾濫し、セキュリティチームを疲弊させ、アラート疲労を引き起こし、過剰または精度の低い対応を招きます。

Darktraceの自己学習型AIは、サイバーセキュリティに対して根本的に異なるアプローチを採用し、各組織の固有のデジタル環境を**継続的に学習**します。多層的なAIアプローチにより、教師なしの機械学習、大規模言語モデル（LLM）、グラフニューラルネットワーク（GNN）、自然言語処理（NLP）など、様々なAI技術を戦略的に統合します。AIアプローチとAI技術は両者とも、順次的かつ階層的に実施されます。

これにより**進化する脅威に適応し**、ユーザー、デバイス、システム全体にわたる正常動作を動的に理解することが可能になります。このようなAIモデルを組み合わせることにより、当社の自己学習型AIはシグネチャ、ルール、手動調整に依存せずに、真に悪意のあるアクティビティと、未知であっても無害な事象を区別できます。

当社の自己学習型AIはDarktraceのActiveAIセキュリティプラットフォームの基盤であり、メールやネットワークを含む完全なエンドツーエンドのカバレッジを実現するため、ドメイン横断的なテレメトリを相関分析します。**これによりDarktraceは環境を横断したインサイトをつなぎ合わせ、リスクの統一的な可視化を実現します。**

ネットワーク上で検知された不審なログインなど、ある領域からの行動シグナルがメールでの意思決定に即座に反映され、その逆もまた同様です。この緊密な統合により脅威検出を高速化し、文脈に応じた高度なアラートが生成され、人間の介入や複雑なルールベースの統合を必要とせずに、より賢い自律的対応が可能になります。

ネットワークとメールを横断する包括的なAI搭載防御により、個々の機能の総和を超える統合的な保護の恩恵が得られるのです。現実世界の攻撃の展開を忠実に再現したシームレスで適応性の高い保護を提供し、防御側に一貫した統合的な優位性をもたらします。

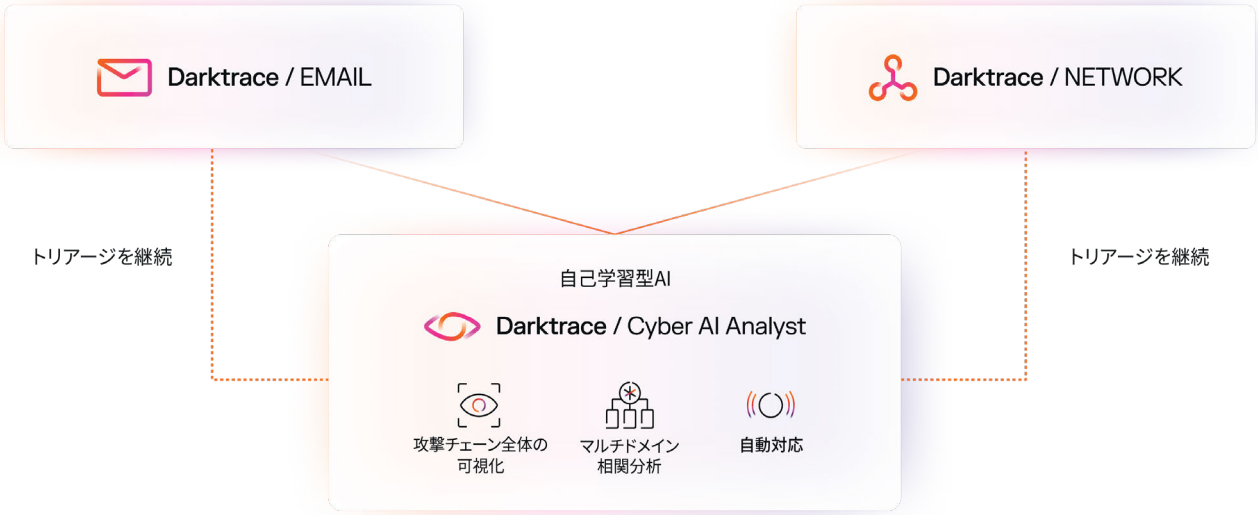


Figure 02: Darktrace/NETWORKと/EMAILを組み合わせることで、プロアクティブなレジリエンスと統一された脅威の可視化・検知を実現し、AI主導のSOCへの移行を実現

調査の参謀役：サイバーAIアナリスト

自己学習型AIがクロスドメイン脅威検知と対応を担うなら、サイバーAIアナリストはSOCの**不眠不休のデジタル探偵です。**

このサイバーAIアナリストは自律的なAIシステムで、Darktraceおよびサードパーティ製セキュリティツール(ファイアウォール、EDR、SIEM）からの関連するすべてのセキュリティアラートを自律的に調査します。ただの生成AIチャットボットではありません。サイバーAIアナリストは、機械学習、専門アナリストの行動を学習したモデル、セキュリティ特化型カスタムLLM、自然言語処理(NLP）など多様なAI技術を活用し、人間の調査プロセスを再現します。

以下のようなSOCレベル1およびレベル2に相当する調査と分析を実施：

- 仮説の形成と洗練
- 情報の照会と相関付け
- 複数ドメインにわたる複雑な攻撃の追跡
- 人間のレビュー用に重大なインシデントを表面化
- 生活様態分析に基づく対応措置の提案

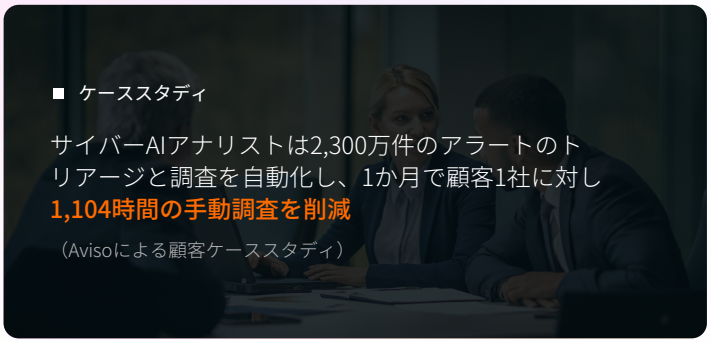
通常数分で結論を出し、明確でインタラクティブなインシデント概要を提示します。これには関連アラート、コンテキスト分析、グラフベースのインタラクティブな可視化が組み込まれており、最も複雑な攻撃であっても容易に調査・理解が可能です。

サイバーAI アナリストはレベル2 SOC基準での調査とトリアージを自動処理し、人間のアナリストが脅威ハンティングとより高度調査に集中できるようにします。

サイバーAIアナリストにより調査を10倍に加速

年間最大5万時間の人間アナリストの時間を獲得

フルタイムのSOCアナリスト最大30名の人員追加に相当



■ ケーススタディ

サイバーAIアナリストは2,300万件のアラートのトリアージと調査を自動化し、1か月で顧客1社に対し**1,104時間の手動調査を削減**

（Avisoによる顧客ケーススタディ）

共通アプローチによるメリット

ネットワークセキュリティとメールセキュリティを統合することで、あらゆる組織に定量的・定性的な多様なメリットがもたらされます。これらは技術的、運用、商業的なメリットに分類されます。**これより詳しく見ていきましょう。**

技術的優位性

技術的な観点では、そのメリットは事前アラート情報とアラート関連情報の2つに分類できます。

事前アラートインテリジェンス：脅威発生前のデータ収集

多くのセキュリティツールは、明確な侵害兆候が現れて初めて分析を開始します。他のツールとは異なり、当社のAIはアラートが発生していない場合でも、メールとネットワークの両方から継続的にデータを収集・分析します。この継続的な分析によって、組織内で相互作用するすべてのユーザー、デバイス、ドメインに関する豊富な行動理解が構築されます。

このことが意味するのは、メールがユーザーの受信箱に届く時点で、Darktraceは既にネットワーク可視性に基づいて送信者のドメインに関するコンテキストを把握している、ということです。同様にメール内で不審なドメインが検出された場合、この情報は直ちに今後のネットワークアクティビティの解釈に反映されます。この共通認識はDarktraceエコシステム全体に及び、インテリジェンスがメール、ネットワーク、エンドポイント、脅威インテリジェンスフィードなどの外部ソースから発生した場合でも、一度取り込むだけで共有されます。そこから、すべての製品における検知と対応を強化し、一貫性のある状況に応じた判断を保証します。

その結果、動的な情報収集・共有プロセスが実現し、ツール内に脅威ではなくリアルタイムの行動ベースラインに関する知識が蓄積されます。Darktraceはこれにより侵害発生前に脅威を検知できます。

アラート関連インテリジェンス：リアルタイムで点と点を結び合わせる

セキュリティアラートが発生すると、サイバーAIアナリストが直ちに調査を開始し、仮説を立て、ドメイン横断的なリアルタイムデータと履歴データを分析します。そして、関連する行動を自律的に結びつけます。例えば、不審なメールを受信者のデバイス上の異常なネットワークアクティビティと関連付け、SOCが確認するための単一包括インシデントを作成します。

このプロセスは数分で大規模に実行され、アラート量と手動によるトリアージを劇的に削減します。

さらに、この自動相関機能により攻撃チェーンが維持され、初期侵害から横方向移動やデータ窃取に至るまでの継続的な可視性を確保します。この共有された可視性が、攻撃の規模と範囲に応じた最も的確な対応策を導きます。

ポイントソリューションやSIEMワークフローとは異なり、アナリストが断片的なアラートを
完全な文脈なしに手作業でつなぎ合わせる必要がなく、Darktraceは脅威が最初に発生した場所を問わず、統合されたアラート後のインテリジェンスを提供します。

当社のアプローチは、調査の迅速化と対応決定の確信度向上を実現するだけでなく、Darktraceのセキュリティ哲学の中核をなす理念を支えています。つまり、防御側は攻撃者が最初の侵入ポイントに到達した後も決してその動向を見失ってはならない、という理念です。

メールが侵入口かもしれませんが、

攻撃者の次の標的は通常ネットワークインフラやクラウドアカウントであるため、メールとネットワーク間の継続的かつクロス環境の相関分析が不可欠です。

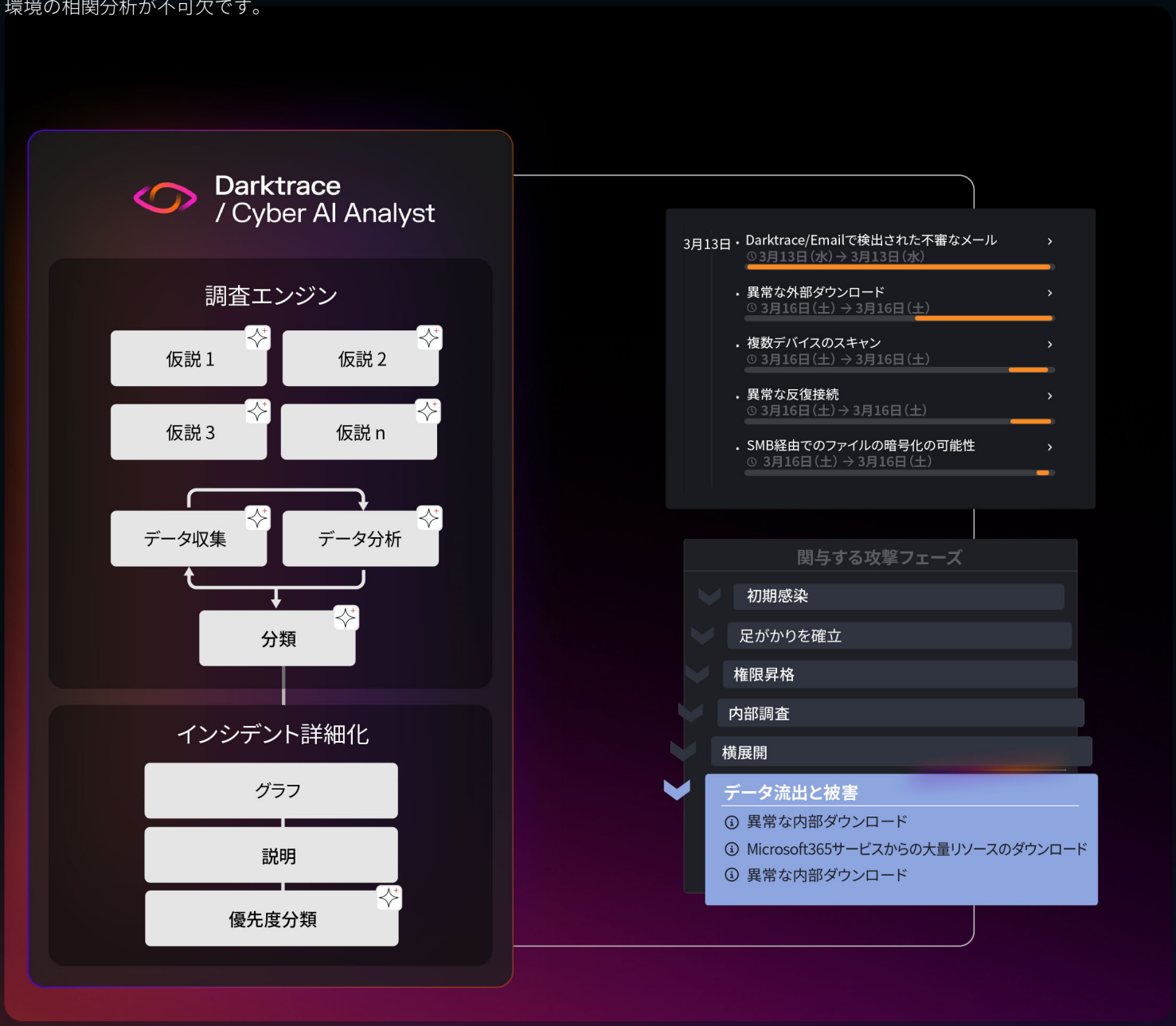


Figure 03: メールを起点としてネットワークへ拡散する攻撃の各段階。攻撃チェーンの異なるフェーズがサイバーAIアナリストで相関付けられます。

「Darktraceには膨大なデータを効果的に分析し、ノイズを除去する能力があります。これによりチームが不要な情報に圧倒されずに、本当のリスクに集中することが可能になります。」

■ CISO、地方自治体

運用上の優位性

チーム横断的なセキュリティ運用（SecOps）の効率化

多くの組織では、メールのセキュリティ対策とインシデント対応は依然として別々のチームで管理されています。メールは通常IT運用部門の管轄ですが、ネットワーク防御とインシデント対応はSOCの管轄となっています。特にメールは依然としてサイバー攻撃の最も一般的な侵入経路であるため、この分離は運用上の摩擦を生み出しています。

ネットワークセキュリティとメールセキュリティを単一プラットフォームと脅威可視化ツール内で統合すれば、重要なメール分析情報は別のコンソールやチームに限定されず、SOCの中核ワークフロー内で直接アクセス可能となります。

この共有可視性により、インシデント対応チームは要求をエスカレーションしたり外部委託したりすることなく、メール攻撃ベクトルに関するより深い洞察を得ることができ、セキュリティチームの異なる領域間の連携強化への道筋を築けるようになります。

状況把握までの時間を短縮し、より迅速な対応を可能に

ネットワークとメールのデータを単一プラットフォームに統合することで、セキュリティチームが異なるアラートの相関分析をするために複数のツールを行き来する必要がなくなります。手動での作業がシームレスになるだけでなく、ネットワークとメールにわたる共通のアプローチにより、ユーザーが状況を把握するまでの時間を短縮します。

同様に、サイバーAIアナリストに備わるメールとネットワーク間の脅威相関分析機能により、環境を横断した迅速なトリアージと、より確実な連携対応が可能となります。従来のワークフローがSIEM相関分析やSOARプレイブックに依存するのとは違い、Darktraceはリアルタイムで点と点を結びつけ、インテリジェントな対応アクションを自動化します。

商業的価値

ネットワークセキュリティとメールセキュリティを同時に導入することは、技術的・運用上のメリットだけでなく商業的な利益ももたらします。

単一ベンダーとの取引で、組織は調達や交渉から継続的なサポートに至るまでのあらゆるプロセスを1か所にまとめて簡素化できるメリットがあります。お客様は複数の契約を管理するのではなく、1つの統合されたアカウントチームと効率的な商業プロセスが利用できます。両製品に対するマネージドサービスやプロフェッショナルサービスを追加で組み合わせるプロセスも簡素化され、セキュリティ環境全体で一貫した専門知識を活用できるようになります。

重要な点は、単一のAI搭載プラットフォームへの投資が将来の拡張に向けた強固な基盤を築くことです。

メールとネットワークを同一プラットフォームに統合すれば、将来的にアイデンティティ管理やクラウド対応などの新機能を追加する際にも、アーキテクチャの再設計が不要になります。これは、プラットフォームがビジネスの成長に合わせて拡張できるよう設計されているためです。

ポイントソリューションは当初は柔軟なように見えますが、しばしば対応範囲が断片的であったり、支出が重複したり、統合の困難さを招きます。AIを活用した現代的なSOCの構築を目指す組織にとって、ベスト・オブ・ブリードではなくベスト・オブ・スイートを購入することは、単純化だけでなく、より戦略的な選択と言えるでしょう。**さらにDarktraceなら、プラットフォーム型への移行で品質を犠牲にすることはありません。個々の購入商品でコアプラットフォームを強化し、共有インテリジェンスを高め、時間の経過とともにさらなる価値を提供します。**

「Darktraceは誠実さと忍耐力を示し、チームとの強固な関係構築に真のコミットメントを示してくれました。だからこそ当社は今日もここにいられるのです。」

- **CISO、グローバル技術プロバイダー**

購入シナリオ

2つの購入シナリオを見てみましょう。1つはポイントソリューション戦略を導入する組織、もう1つは統合セキュリティスタックを求める組織です。

シナリオ1：ポイントソリューション

初期導入

ある組織がスタンドアロンのメールセキュリティツール（おそらくIT部門やメッセージングチームが選定したもの）を選択し、その後セキュリティチームを通じて別のネットワーク検知・対応（NDR）製品を導入します。あるいはNDRツールを全く導入せず、代わりにEDRやXDRに依存している可能性もあります。洞察を結びつけるため、既存のSIEMやSOARプラットフォームを活用してデータを相関分析し、対応ワークフローを調整します。

運用フェーズ

このアプローチは柔軟性があり、既存のツールを活用しますが、複雑さを伴います。SOCは複数のダッシュボードとアラートシステムを管理する必要があります。調査プロセスが遅くなる可能性があります。アナリストが異なるツール間で発生事象を手動で関連付けるためです。各ツールには独自のデータモデルと検知ロジックがあります。

スケールアップ

クラウド、ID、アプリケーション層へのカバレッジ拡大には、さらなるポイント製品の調達や、それらのSIEMとの統合、またそれに応じたルールやプレイブックの調整が必要となります。

時間の経過とともにエンジニアリングと運用にかかる負担が増大します。その原因はツール間で重複する作業、断片化された可視性、一貫性のない対応調整です。

シナリオ2：プラットフォームセキュリティ

初期導入

ある組織は、同一ベンダー提供のメールとネットワーク検知ソリューションを採用しました。これらは共有のAI搭載プラットフォームと単一の操作インターフェースで提供されています。両検知機能のインターフェースは同一の行動モデルに統合され、知能と可視性が環境全体でシームレスに共有されています。

運用フェーズ

セキュリティチームは事前統合されたワークフロー、一貫したアラート通知、ネイティブなインシデント相関分析の恩恵を受けます。メールベースの添付ファイルが不審な内部活動につながる場合、両検知機能が統一ビューに表示されるため、調査時間が短縮され、ツールやチーム間のギャップを手動で埋める必要がなくなります。MDRなどのオプションサービスは、重複することなく両検知機能の統一ビューで動作できます。

スケールアップ

脅威の状況が変化するにつれ、クラウドアカウント、ユーザーID、エンドポイントなどの他の領域への拡張は、スタックの再設計なしで段階的に行うことが可能です。追加機能が同一モデルに統合され、コンテキストを維持しながらデジタル資産全体にわたる一貫した保護を実現します。

次のステップへ

攻撃者がAIを活用して調査・自動化・加速化を進める中で、防御側は統合が不十分なツールや手動プロセスに頼る余裕はありません。ネットワークとメールのセキュリティを統合することは効率化だけに留まりません。個々の要素の総和を超えるセキュリティエコシステムを構築することなのです。

Darktrace アクティブAIセキュリティプラットフォームは、攻撃者の思考を模倣する先制的な相関セキュリティを提供します。これにより、サイロ化された検知では捕捉できない標的型マルチドメイン脅威に対して、可視性と俊敏性で防御できます。

次のステップへ、ご準備はよろしいですか？

カスタマイズされたデモをリクエストし、統合セキュリティを実感してください

デモを申し込む ↗

DarktraceでMTTCを80%削減した事例をご覧ください

ケーススタディ ↗

Darktrace/EMAILで貴社のROIを試算

ROIを試算する ↗

■ **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