LANSCOPE
Cyber Protection

マルウェアの侵入、断固お断り！

狙われやすい感染経路と今スグできる6つの対策

はじめに

近年、攻撃者は企業をマルウェアに感染させるため、さまざまな経路から侵入してきます。例えば、委託先企業のネットワーク環境を経由した侵入や取引先を装ったメールに添付されたファイルを開封させて侵入するなどのケースが確認されています。これらの感染経路は、事前に把握できていれば対策することができます。

そこで、今回はマルウェアの攻撃に狙われやすい5つの感染経路をご紹介します。それぞれの感染経路で実際に起こった事例や、その経路が狙われる原因を掲載しています。また、今すぐできる6つの対策も併せて紹介していますので、マルウェア感染対策にお役立ていただければ幸いです。

「ランサムウェアによる被害」が4年連続で1位に
サイバー攻撃被害が増加傾向にあり、セキュリティ対策の強化が必須です

順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	2位
3位	内部不正による情報漏えい	4位
4位	標的型攻撃による機密情報の窃取	3位
5位	修正前の公開前を狙う攻撃（ゼロデイ攻撃）	6位
6位	不注意による情報漏えい等の被害	9位
7位	脆弱性対策情報の公開に伴う悪用増加	8位
8位	ビジネスメール詐欺による金銭被害	7位
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位
10位	犯罪のビジネス化（アンダーグラウンドビジネス）	10位

※ 引用：IPA「情報セキュリティ10大脅威2024」

👉 今期のポイント

1位：「ランサムウェアによる被害」

2023年もランサムウェア被害は多く確認されました。ランサムウェア感染によってシステムに障害が発生し、一時的に業務が停止した企業もありました。また、ファイルを暗号化せずに窃取だけ行い、身代金を要求するといった新たな手法も確認されています。

2位：「サプライチェーンの弱点を悪用した攻撃」

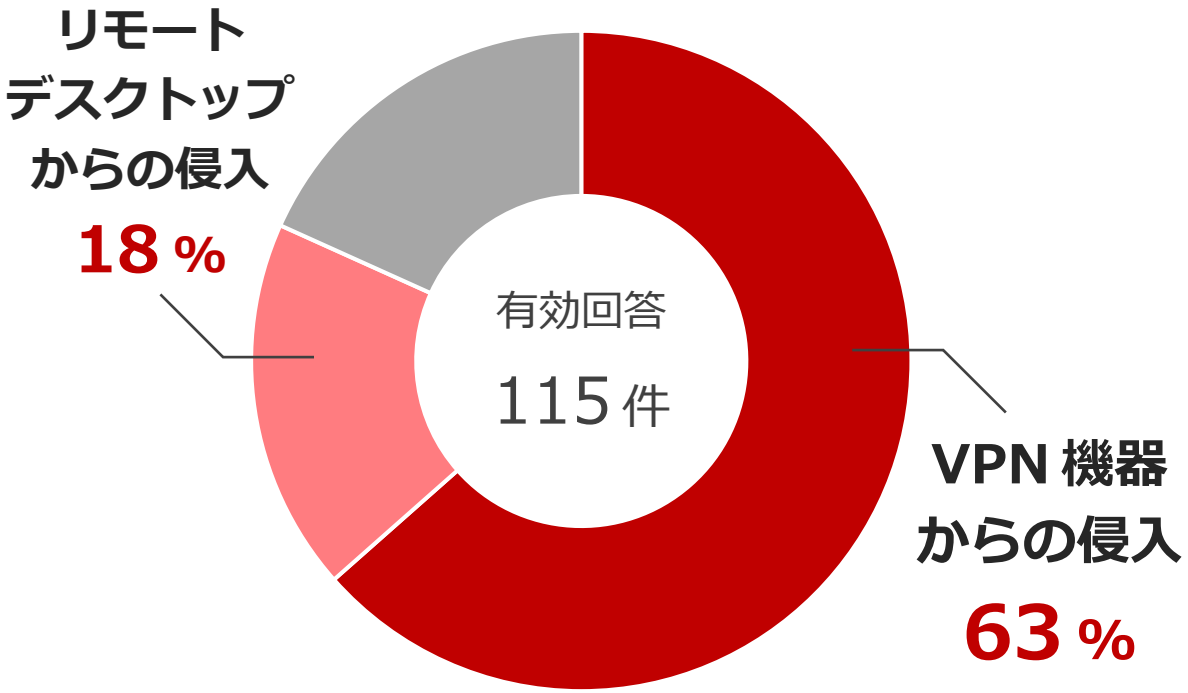
業務委託先の企業が攻撃されることで、委託元の企業に感染が広がってしまったというケースが確認されています。その結果、委託元企業の業務が一時停止するなどの被害が発生しています。

4位：「標的型攻撃による機密情報の窃取」

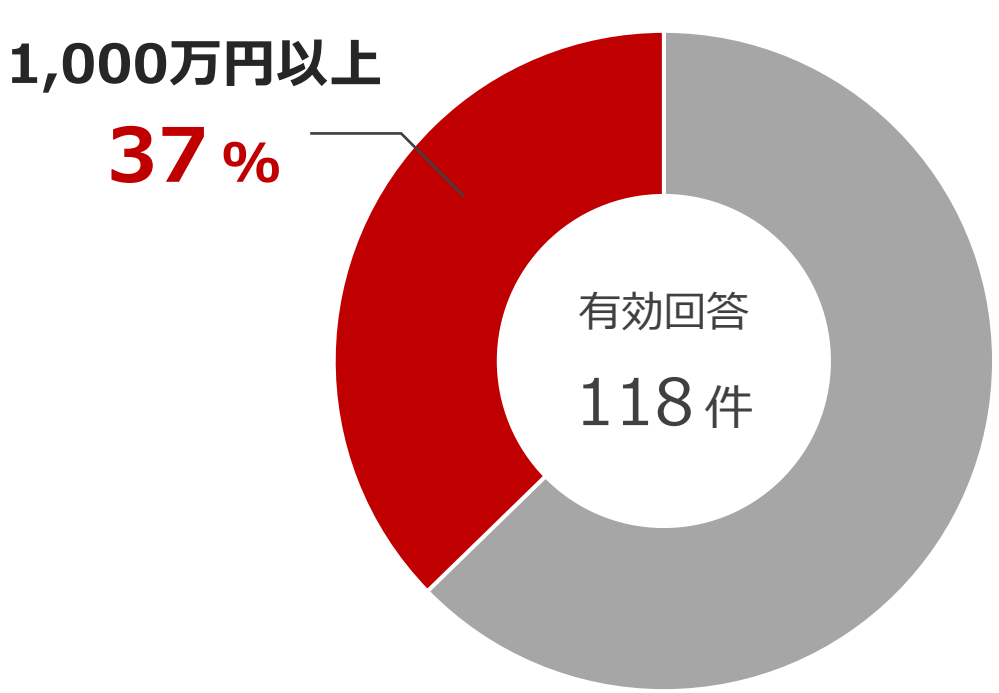
特定の企業や組織に狙いを定め、メールやウイルスなどを使い情報窃取を行います。近年では、手口が巧妙化しており、実在する組織の担当者を騙ったメールも確認されています。

ランサムウェアの感染経路は VPN 機器が最多で、一度感染してしまうと多額の費用を要します

感染経路※



調査・復旧費用の総額※



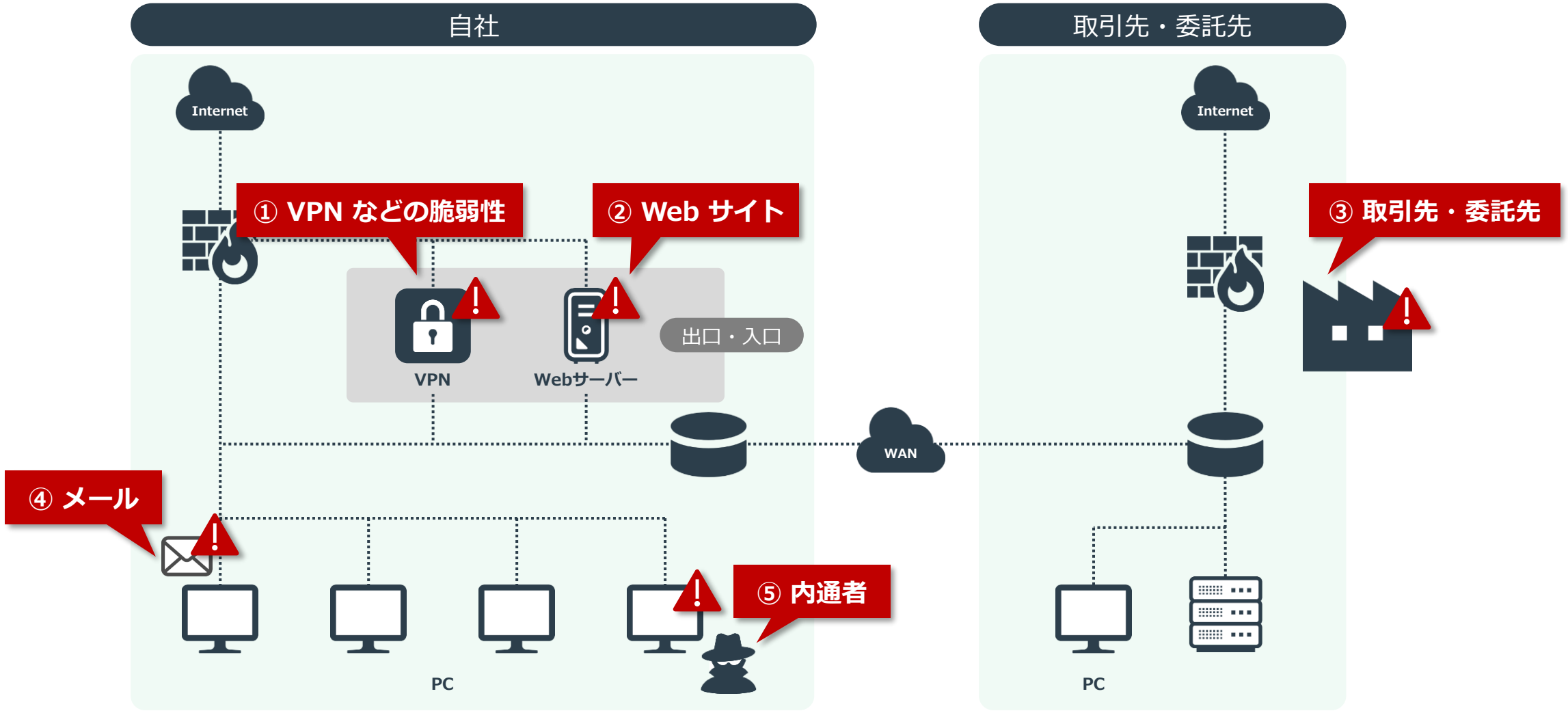
ポイント

VPN 機器からの侵入が73件で63%、リモートデスクトップからの侵入が21件で18%となっており、テレワークなどで利用される機器などを利用して侵入されているものが8割以上を占めています。また、万が一ランサムウェアに感染した場合、調査・復旧費用が莫大なものとなってしまう可能性があり、1,000万円以上要した企業が約4割を占めています。

※ 引用：警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢等について」

マルウェアの感染経路は多様化しています

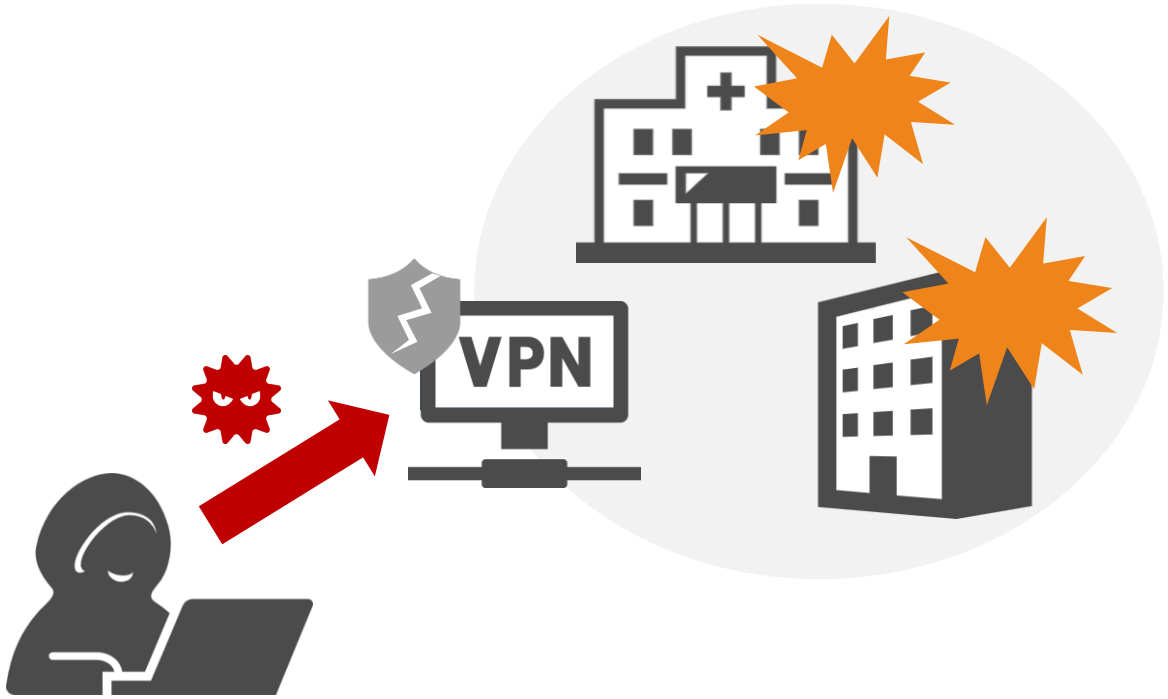
マルウェアの感染を予防するためには、侵入経路や犯行手口を把握しておくことが重要です



VPN などの機器の脆弱性を狙った感染

セキュリティ対策が不十分な VPN やリモートデスクトップなどの脆弱性を狙い、攻撃者はマルウェア攻撃を仕掛けます。VPN 機器やリモートデスクトップの管理が行き届かず、最新のセキュリティパッチが適用されていなかったため、被害が発生しました。

VPN の脆弱性を狙った攻撃



事例

① 医療機関では VPN の脆弱性を悪用されランサムウェアに感染し、暗号化によってカルテが利用できず長期間診療などの業務が停止となりました。

② リモート接続機器の脆弱性を悪用されてコンテナターミナルシステムがランサムウェアに感染し、操業停止を余儀なくされ重要インフラに影響を及ぼしました。

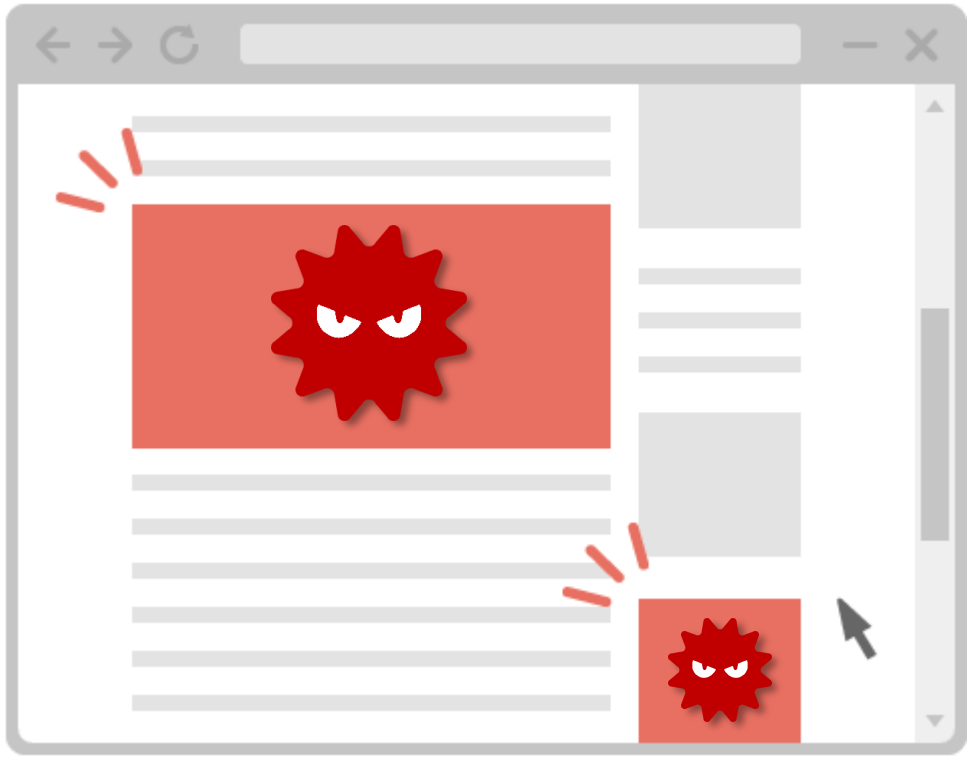
原因

- VPN や RDP（リモートデスクトッププロトコル）には管理者の認証ファイル閲覧、遠隔操作が可能となるなどのあらゆる脆弱性がある。
- VPN 機器やリモートデスクトップ装置はネットワークの入り口であり、認証さえ突破すれば内部ネットワークに侵入できる。

Web サイトからの感染

改ざんされた Web サイトを閲覧したり、不正なファイルをダウンロードしたりすることでマルウェアに感染します。広告が細工されている場合などもあるほか、ユーザーが特定の操作をせずともサイトに訪れるだけで感染してしまうような攻撃手法もあります。

改ざんされた Web サイト



事例

① 新聞社では Web システムの脆弱性を悪用されて求人情報サイトが改ざんされ、氏名やパスワードなどの顧客情報250名分が流出した可能性があります。

② 業務用食品メーカーでは、通信販売サイトが改ざんされる被害がありました。不適切な コンテンツが表示され、注文情報が流出しました。

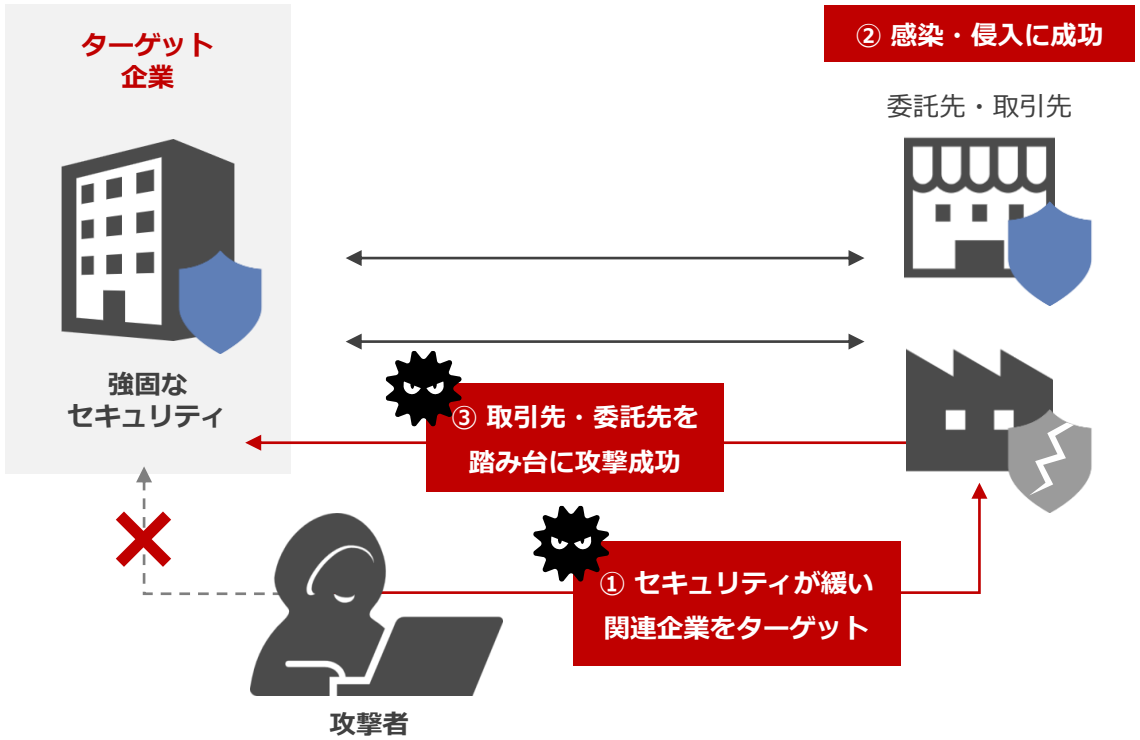
原因

- Web アプリケーションの脆弱性や Web サイトに使用しているソフトウェアの脆弱性を悪用される。
- Web サーバーの管理アカウントに不正にログインされ、Webサイトにマルウェアを仕組まれてしまう。

取引先や委託先を経由して感染

攻撃者は取引先や委託先など、サプライチェーンに関与する企業を攻撃してそれを足掛かりにして侵入し、マルウェアに感染させます。「サプライチェーン攻撃」とも呼ばれます。ソフトウェア開発元や MSP（マネージドサービスプロバイダー）に対し、脆弱性などを悪用されて侵入されるケースもあります。

取引先・委託先を足掛かりにした感染



事例

① 関西の医療センターでは、委託先である給食事業者のネットワーク環境からランサムウェアに侵入され感染。診療系システムに障害が起き、診療停止に陥りました。

② 大手インターネット企業は、再委託先企業で従業員の PC がウイルス感染したことを発端とし、同社の保有する顧客情報が漏えいしました。

原因

- 攻撃者が標的にする企業や組織よりも、サプライチェーンに関与する企業のセキュリティが脆弱なことがある。
- サプライチェーンが複雑で多層化していた場合に、セキュリティ管理が難しくなり、攻撃者が侵入できる機会が増える。

メールからの感染

マルウェアが仕込まれたメールの添付ファイルや、メール本文に記載されたリンク先を開くことで感染します。攻撃者は企業や公的機関になりすましたメールを送り、確実に添付ファイルや URL を開かせようと仕向けてきます。近年は取引先を装ってこれまでやり取りしていた内容を悪用し、ユーザーに不信感を持たせないメールでの攻撃も増えています。

取引先を装った巧妙なメール

事例

① 大手通信企業では、メールの添付ファイルを開いてマルウェアに感染し、ヘルプデスクのメール情報が流出。さらに返信を装ったなりすましメールも送信されました。

② 関東の大学では、標的型攻撃メールによって教員の PC がマルウェアに感染し、教員や学生の個人情報が漏えいした形跡が発見されました。

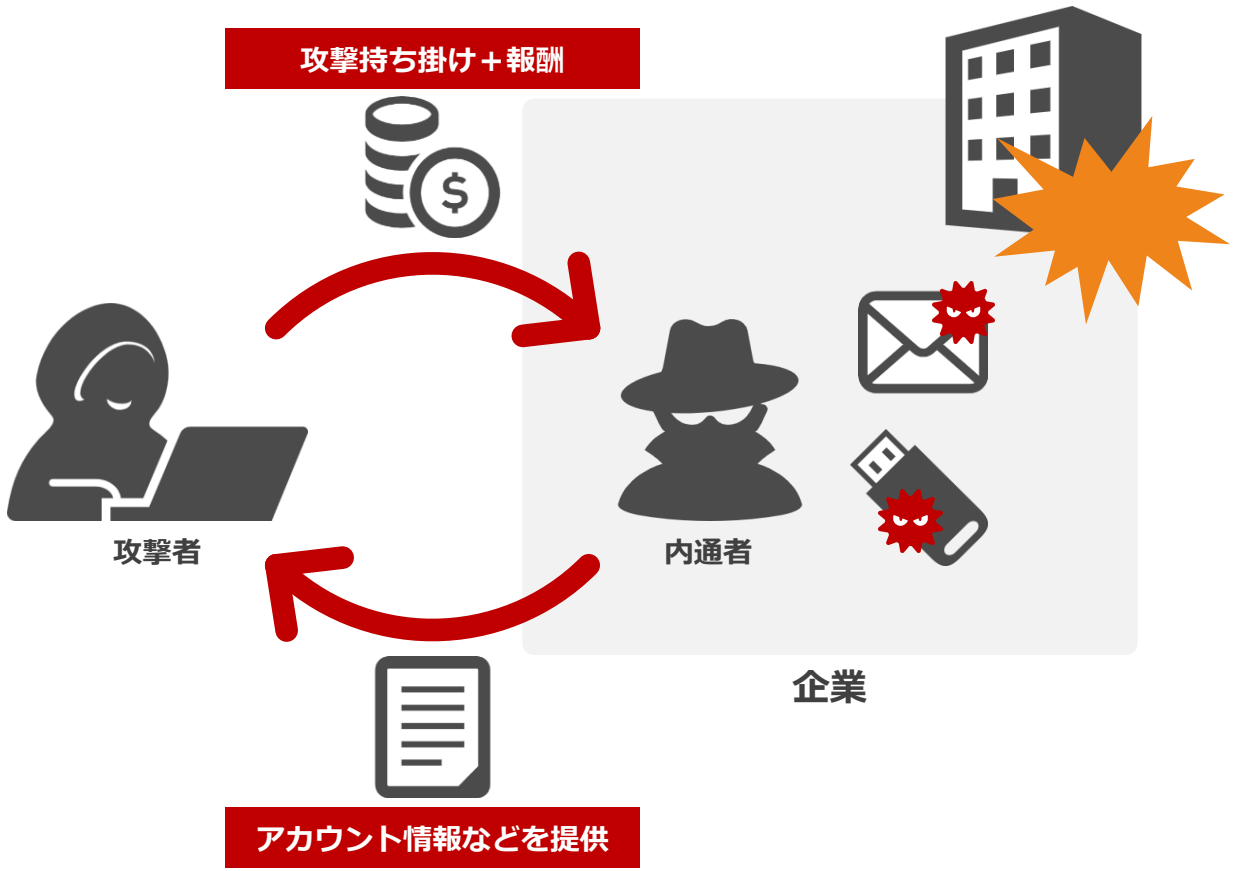
原因

- メールの内容が巧妙になっているため、攻撃者が取引先などになりすましたメールであることに気づきにくい。
- 近年は生成AIツールを使い、日本語を知らなかったとしても流暢な日本語の文章を誰でも作成可能。

内通者による感染

攻撃者が組織の関係者に協力を持ち掛け、攻撃者と共謀してマルウェア攻撃を実行する手口も注目されています。組織の機密情報やアクセス権限を持っている従業員を利用することで、攻撃が容易になります。内通者がメールに添付された悪性のファイルを故意に開く、感染した USB を使って社内ネットワークにウイルスを仕込むような手口もあります。

内通者によるマルウェア攻撃



事例

① アメリカでは、製造工場で働く従業員に対し、多額の報酬と引きかけに内部ネットワークにランサムウェアを仕掛けるよう提案した事件が発生しました（未遂で終了）。

② ランサムウェア攻撃グループ「LockBit2.0」は、企業の内部の人に対し、多額の報酬と引き換えに悪用可能な内部のアカウント情報などを提供するよう募集していました。

原因

- 企業側のセキュリティ対策が不十分で、不正行為を検知・監視できる仕組みがない。
- 経済的な困窮や会社の待遇に不満を抱いているような人が利用されてしまう。

感染を予防するには、感染経路や犯行手口を理解し、適切な対策を行うことが重要です

基本的な対策

- ☐ PC の OS やソフトウェアのバージョンを常に最新にしている
- ☐ 定期的に PC などのセキュリティパッチを欠かさず適用している
- ☐ マルウェアに感染した際に検知・防御する仕組みを導入し、日々運用している

VPN などの脆弱性を悪用した攻撃対策

- ☐ VPN 機器やリモートデスクトップ機器は常に最新バージョンにしている
- ☐ 未使用のリモート接続ツールは全て無効にしている
- ☐ 不要なポートは全て閉じていることを確認している

Web サイトを経由した攻撃対策

- ☐ 安全が確認できない Web サイトを利用できないように制御している
- ☐ 定期的に Web アプリケーションの脆弱性の検査を行っている
- ☐ 信用できない Web サイトへのアクセスやファイルのダウンロードをしないように教育しており、徹底もできている

取引先・委託先への対策

- ☐ 定期的に取引先のセキュリティレベルを確認している
- ☐ 新たな取引先と契約する際に、セキュリティ対策状況も詳細に確認している
- ☐ 取引や委託契約におけるセキュリティ上の責任範囲を明確化している

メールからの感染対策

- ☐ スパムメールや不正な実行ファイルが添付されているものは検知・駆除できている
- ☐ 不審なメールの開封やリンクを踏まないように周知徹底している
- ☐ 定期的に標的型メール攻撃の訓練を行い、従業員が攻撃メールの識別力や対応力を身に着けている

内通者による攻撃対策

- ☐ 不審な USB メモリを使わないように制御している
- ☐ 従業員の操作履歴などのログを取得し、不審な操作を日々監視している
- ☐ 組織の内部不正対策に関する方針や重要情報の取り扱いなどの手順を周知徹底している

上記は一般的なセキュリティ対策の例ですが、全てを完璧に実施することは容易ではありません
そのため、必要に応じてセキュリティツールや各種サービスを利用して対策をすることも重要です

今回紹介したマルウェアの５つの感染経路は、LANSCOPE で対策できます
巧妙化するサイバー攻撃に対し、エンドポイントからネットワークまで幅広く対策が可能です

エンドポイントセキュリティ

AI アンチウイルス

未知・亜種の脅威を高精度に検知可能

Cyber Protection

- EPP
- EDR
- MDR

— Product 1 —

CylancePROTECT

CylanceOPTICS

CylanceGUARD

— Product 2 —

deep instinct

ネットワークセキュリティ

AI ネットワーク脅威検知

内部のネットワークを監視

DARKTRACE

- NDR
- ネットワーク遮断
- Email 監視

サプライチェーンリスクマネジメント

外部からのリスクを評価

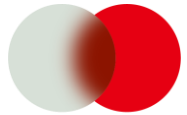
Panorays

- セキュリティスコアリング
- ASM

内部不正対策

統合エンドポイント管理

組織の IT 資産・ログを管理



Endpoint Manager

- IT 資産管理・MDM
- 内部情報漏えい対策
- 外部脅威対策

AI 型アンチウイルス × エムオーテックス支援

LANSCOPE Cyber Protection

AI が未知・既知問わず脅威を99%防御

パターンファイルを使っていないから、運用もカンタン

必要に応じて EDR・MDR も選択できる

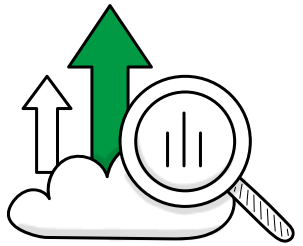
https://www.lanscope.jp/cpms/

- powered by CylancePROTECT（EPP・EDR・MDR）
  - 》 オンライン相談 》 無料体験版 》 製品セミナー
- powered by Deep Instinct（EPP）
  - 》 オンライン相談 》 無料体験版 》 製品セミナー

POINT 1

「しっかり守れて、運用はカンタン」

AI による高精度な検知により、未知・既知問わず脅威を99%※防御！
アップデート頻度も年1回ほどで、
少ない手間で運用可能です。

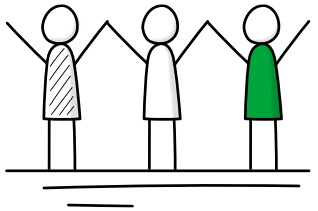


※ CylancePROTECT：2023年3月 Tolly 社のテスト結果より
※ Deep Instinct：Unit221B 社調べ

POINT 2

「防御・分析・監視を、まとめてお任せ！」

ウイルス対策ソフトだけでなく、
EDR や MDR も利用したいなど、
お客様の用途にあった製品を選択いただけます。



事前に膨大な情報を AI に与え、マルウェアの特徴を徹底学習
AI が「未知のマルウェア」を判定し、マルウェアが動く前に隔離を実施

マルウェアのモデル

過去に発見されたマルウェアなど
ありとあらゆる危険なファイルの
特徴を分析・数理モデル化

【特徴点】

ファイルサイズ

アイコン

比較

セクションヘッダー

セクションデータ

文字列

etc…

膨大な特徴点から総合的に判断

検査対象のファイル

マルウェアのモデルと比較することで
過去に発見されたマルウェアと全く同じでなくとも
その特徴からマルウェアであると特定できる

サイバープロテクションは 2 種類のマルウェア対策製品から、用途に応じて選択いただけます

多くの導入実績と EDR・MDR が利用可能

CylancePROTECT
CylanceOPTICS
CylanceGUARD

- **EDR 要件**への対応をお求めのお客様
- **EDR の運用を外部に任せたい**とお考えのお客様
- **インターネット非接続環境**※での運用をお考えのお客様

※ インターネット非接続環境での利用は CylancePROTECT のみ可能

幅広い OS やファイルタイプに対応

deep instinct™

- **コストを重視**されるお客様
- **PC とスマホに**マルウェア対策ソフトを導入したいお客様
- **EXE ファイルだけでなく Word や Excel など多くのファイルタイプ**への対応をご要望のお客様

両製品とも無料体験版をご用意しています！
無償で操作方法のレクチャーや疑問点にお答えしますので、ぜひお試しください

CylancePROTECT

CylanceOPTICS

▼体験版のお申し込みはこちら

概　　要	CylancePROTECT・OPTICS がライセンス数無制限でお試しいただけます。また、検知したファイルについて希望者の方にサマリーレポートを作成させていただきます。さらに、専任スタッフによる導入時の支援付きで、負担なく使い始められます。
対　　象	CylancePROTECT・OPTICS を初めて導入するユーザー様
ご利用期間	1カ月間
申し込みURL	https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr
申込期間	常時受付

deep instinct™

▼体験版のお申し込みはこちら

概　　要	Deep Instinct が 100ライセンスまで、1カ月間無料でお試しいただけます。さらに、専任スタッフによる導入時の支援付きで、負担なく使い始められます。体験中のお問い合わせにも対応しますので、じっくりしっかり体験が可能です。
対　　象	Deep Instinct を初めて導入するユーザー様
ご利用期間	1カ月間
申し込みURL	https://go.motex.co.jp/l/320351/2021-02-25/4gnpt1
申込期間	常時受付

AI ネットワーク検知（NDR）

DARKTRACE

サイバー攻撃や内部不正をリアルタイムに検知・遮断

ネットワークの可視化と早急な解析が可能

容易に導入可能　コアスイッチにミラーポートするのみ

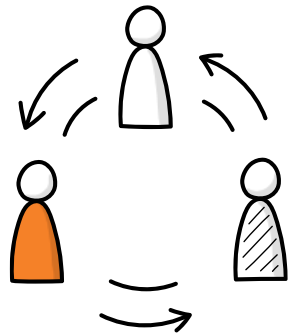
https://www.lanscope.jp/professional-service/service/product/darktrace/

» 無料体験　» 製品セミナー　» お問い合わせ

POINT 1

「自己学習型 AI を搭載」

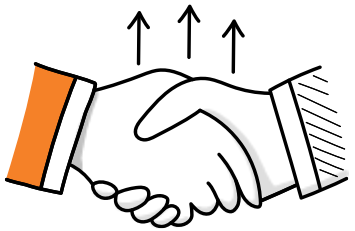
「自己の正常な状態」を常時学習し、それと異なる不自然な挙動を自動的かつリアルタイムに検知します。



POINT 2

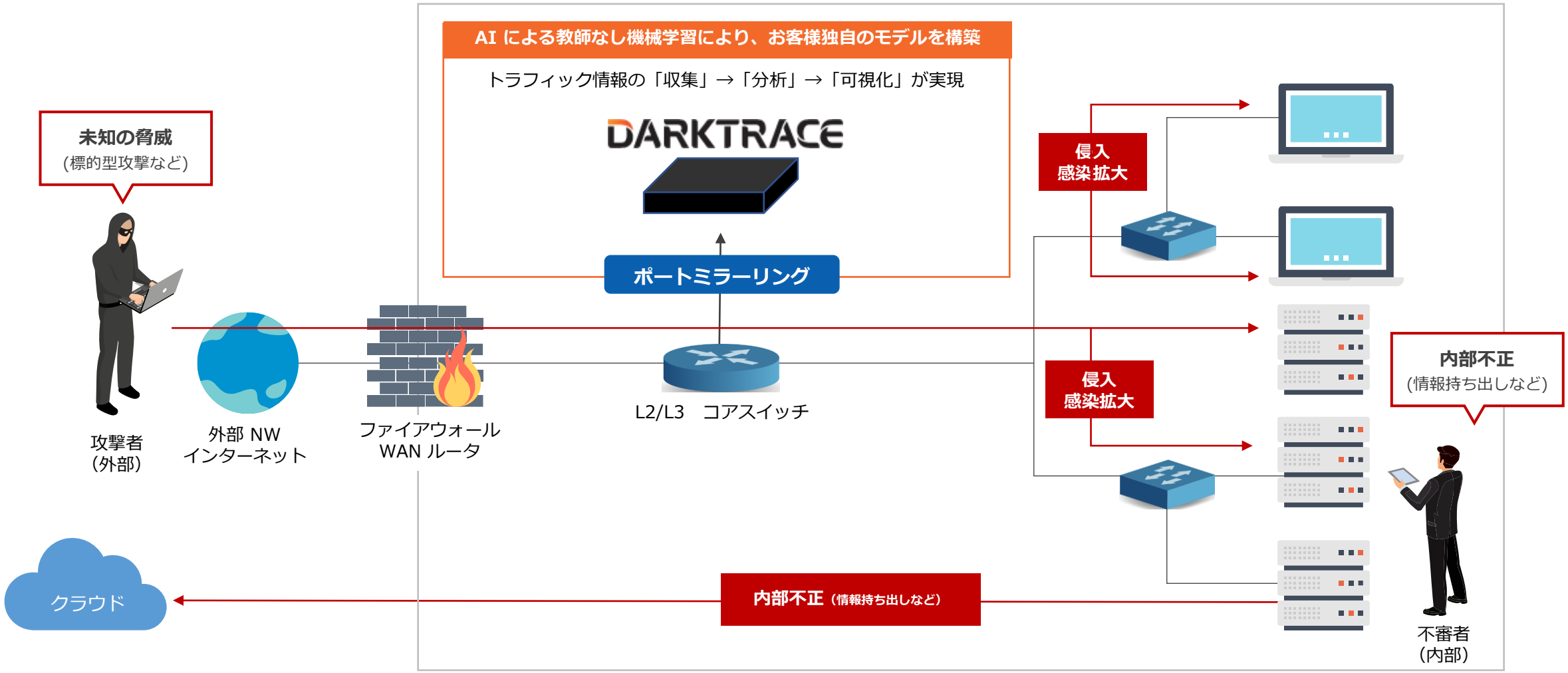
「セキュリティアナリスト雇用と同じ効果」

アラート内容を AI が自己分析し、レポートまで自動作成するため、優秀なセキュリティ人材を雇った場合と同様の効果が期待できます。



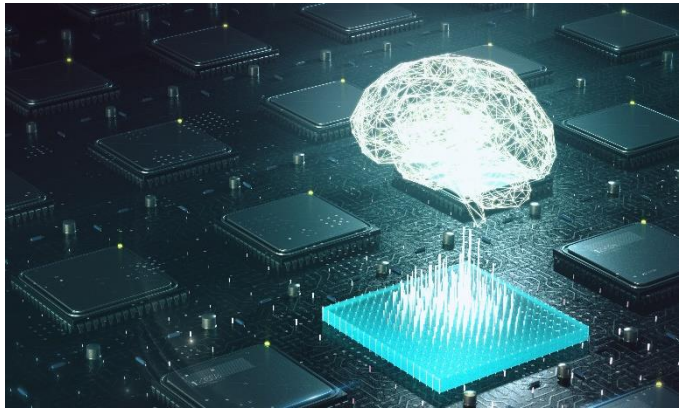
導入済みのスイッチにミラーポートを設定し、ネットワーク機器に流れるトラフィックを AI が監視

ネットワークに接続したさまざまなデバイスやユーザーの行動パターンを学習・分析することで、未知のサイバー攻撃や内部不正の兆候を検知します



ネットワークに接続するだけで簡単に導入可能！AI がネットワーク全体を可視化し未知の脅威を検知

AI による脅威検知・遮断



●AI による「教師なし機械学習」で検知

自社の業務状態を分析、**通常の業務パターンに外れた挙動をスコアリングして検出（ホワイトリスト型検知）**未知の脅威も検知

●AI が自動で問題抽出・対応提案・遮断

さまざまな起点のアラートも**AIが関連脅威単位で自動トリアージ**し対応策を提示。さらに自動遮断もでき、ワンストップで対応が可能

監視領域が広い

●監視ツールが未導入な機器も可視化

ネットワークで監視するためエンドポイント管理ツールが導入できない**IoT 機器やレガシー OS** などもエージェントレスで監視可能

●外部脅威・内部不正・怪しい挙動を検知

監視領域が広いため、**外部からの攻撃はもちろん、内部の不正も検知**。フォレンジックに必要なレベルで情報を網羅しており、影響範囲の特定に活用可能

管理者・環境負荷が少ない

●既存ネットワークに影響を与えない

アプライアンスを設置するだけなので**今の環境を変えず**、他システムに影響を与えない

●アップデートチューニングが不要

AI の自律的学習により自動でチューニングするため、**アップデートの手間がなく**、管理者負担が少ない

無料リスク評価キャンペーン

※ 本調査は、NDR 製品である「Darktrace」の評価プログラムを利用して提供いたします。
※ AI 学習上の特性により、**従業員数250名以上の企業様が対象**となります。

社内ネットワークに潜むリスクを無料調査します

1. PC へのインストール不要！ネットワークに接続するだけで導入完了！
2. 自社のセキュリティの現状と課題点を可視化したレポート＆解説付!
3. セキュリティ専門家が結果を分かりやすく解説・報告会を開催！

セキュリティは**経営課題**です
経営層の皆様もぜひ**報告会**にご参加ください！

リスク評価を申し込む

構成などヒアリング&打合せ
弊社 お客様

→ **機器 設定/出荷**
弊社 お客様

→ **機器 現地設置**
お客様

→ **評価期間（1カ月）**
学習期間 → レポート① 報告会 → レポート② 報告会 → レポート③ 報告会

サプライチェーンリスクマネジメント

Panorays

SaaS 型のセキュリティリスク評価システム

自社だけでなくグループ会社や取引先にも対応

外部脅威と内部脅威に対するセキュリティリスクを評価

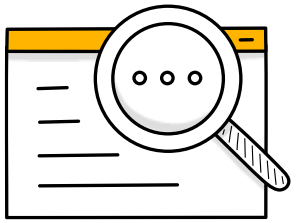
https://www.lanscope.jp/professional-service/service/product/panorays/

» 無料体験　» お見積り　» お問い合わせ

POINT 1

「サプライヤーの負担は一切なし」

ドメインを入力するだけで、関連する外部に公開されたIT資産の洗い出しと、サイバーリスクを可視化できます。



POINT 2

「手間取るリスクアセスメントを効率化」

オンラインのセキュリティ調査表を使って、グループ会社や取引先などのセキュリティ対策レベルを可視化できます。

外部公開された IT 資産の「外部評価」とオンライン調査表による「内部評価」でサイバーリスクを総合評価

総合評価
Cyber Risk Rating

- ✓ 外部評価と内部評価を組み合わせた総合評価を提供
- ✓ ビジネスへの影響に応じた対処の優先順位付けが可能に

外部評価
Cyber Posture Rating

- ✓ ドメイン情報などをもとにアタックサーフェス（外部に公開された IT 資産のサイバーリスク）を可視化
- ✓ 対象に影響を与えずにサイバーリスクを可視化
- ✓ 登録後、72時間（3日間）以内にサイバーリスクを可視化

Panorays

内部評価
Smart Questionnaires

- ✓ オンライン調査票を用いて内在するリスク（セキュリティ対策状況）の把握から集計までクラウド上で容易に可能
- ✓ 対象との関係性を踏まえた内容にカスタマイズ可能

公開 ※ ドメイン/グローバル IP アドレスを保有

非公開

👉 サプライチェーンとは、自社に関連するグループ会社、委託先、販売会社やクラウド事業者などを指します。

シンプルな構成で専門知識がなくとも運用可能な製品を提供

すぐに使い始められる

SaaS 型プラットフォーム（システム導入は不要）
3クリック（ドメイン登録）でモニタリング開始

サプライチェーンのドメイン登録だけで
モニタリングを開始可能

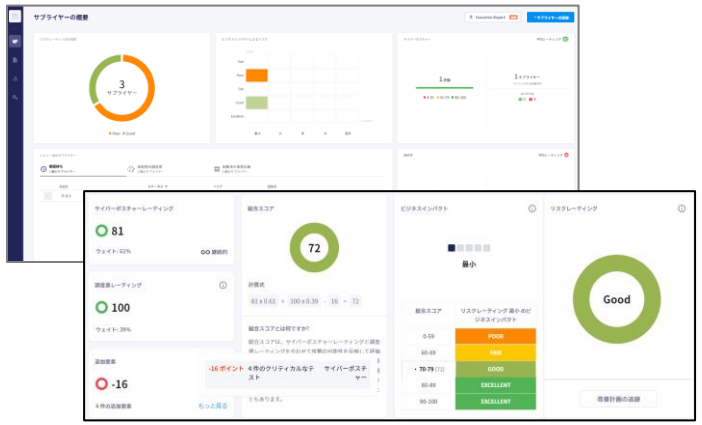
サイバーリスクを360度評価

サプライチェーンのサイバーリスク全体の可視化
（アタックサーフェス＋内在するリスクの可視化）

日々、変化を続けるリスクに対して
継続的な監視が可能

分かりやすい画面構成

GUI の日本語対応
直感的・シンプルな画面構成



GUI が日本語対応しており、直感的に操作が
できる画面構成のため、容易に運用可能

Panorays

サプライチェーンリスク無料レポート

リスクを可視化

自社とサプライヤー企業を対象に、サプライチェーンリスクレポートを無料でプレゼントします。
特別な設定は一切不要で、**対象企業のドメインを提供するだけ**で**2週間以内**にレポートが届きます。
国家資格を保有するセキュリティプロフェッショナルによる解説・相談付で
疑問・不安もその場で解決できます。
※ 対象：自社とサプライヤー企業2社の最大3社まで

レポートをご希望の場合は以下 URL もしくは QR コードよりお申し込みください。
https://www.lanscope.jp/professional-service/service/product/panorays/

無償レポートで分かること

- 各サプライヤーのリスクレベル
- 自社のリスクレベル
- どのサプライヤーにどんなリスクがあるのか
- ダークウェブに情報が流れていないか
- サプライヤーが行うべき対策

PC・スマホを一元管理

LANSCOPE
Endpoint Manager

PC・スマホをクラウドで一元管理

操作ログなど PC 管理に必要な機能を網羅

Apple・Google のプログラムに対応した MDM 機能

https://www.lanscope.jp/endpoint-manager/

» オンライン相談 » 無料体験版 » 製品セミナー

※ iOS・Android はエンドポイントマネージャー クラウド版のみ対応しています。

POINT 1

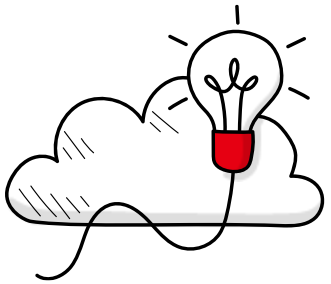
「多くの支持を集める使いやすさ」

充実の機能を使いやすい管理コンソールで提供。レビュープラットフォーム「ITreview」では多くの評価を得ています。

POINT 2

「クラウドでいつでも・どこでも管理」

クラウドサービスならではの特長を活かしたデバイス管理。社内・社外など所在を問わないデバイス管理を支援します。



PC・スマホ・タブレットの一元管理をクラウドで実現
「使いやすい」管理コンソールで、充実の「IT 資産管理機能」と「MDM 機能」を実装

01 | IT 資産管理ツールをクラウド化したい

エンドポイントマネージャー クラウド版は一般的な IT 資産管理ツールと同等の PC 管理に必要な機能を網羅。社内のシステムのクラウドシフトを推進するお客様において、IT 資産管理ツールのクラウド移行を支援します。

02 | 所在を問わないデバイス管理を実現したい

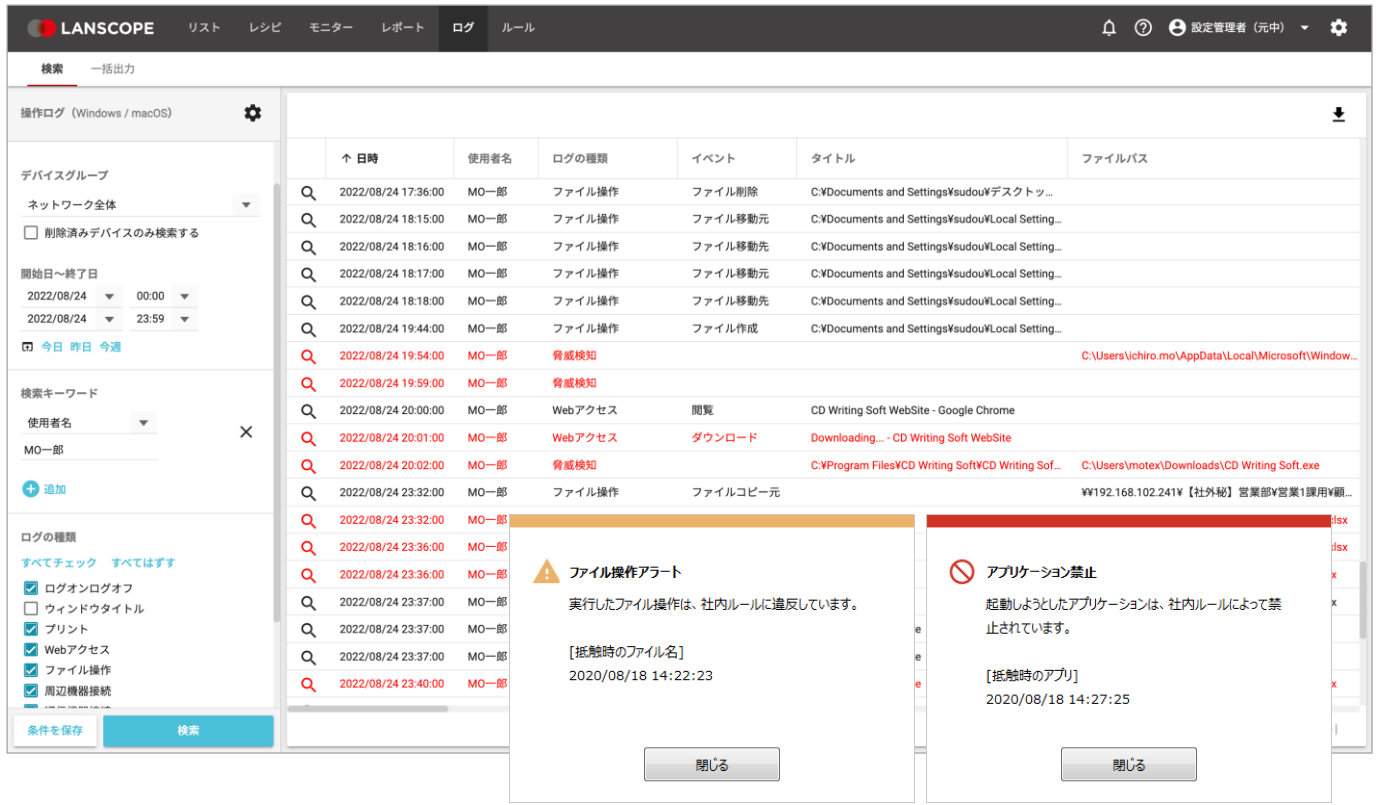
エンドポイントマネージャー クラウド版はデバイスがインターネットに接続されていれば、オフィスワークやテレワーク、これらを組み合わせたハイブリッドワークにおいても、デバイスの所在を問わず管理できます。

03 | PC・スマホを一元管理したい

iOS・Android 管理に欠かせない Apple Business Manager・Android Enterprise に対応。PC だけでなく、現在多くの組織で利用されるスマホ・タブレットの管理をエンドポイントマネージャー クラウド版で実現します。

「どの部署の」「誰が」「いつ」「何をしたのか」をリアルタイムに取得

取得した操作ログは2年間保存され、検索によるログの抽出と CSV ファイルによる出力が可能。ログ運用オプションの導入で最大5年保存されます。



違反操作があった場合は、リアルタイムに警告通知が可能

取得できる操作ログ

ログオン・ログオフログ
電源ON・OFF・ログオン・ログオフのログを取得できます。

ウィンドウタイトルログ
デバイス上での閲覧画面（ウィンドウタイトル・アプリ名）のログを取得できます。

ファイル操作ログ
デバイス上でのファイル操作（ファイル・フォルダのコピー／移動／作成／上書き／削除／名前の変更）でのログを取得できます。

Web アクセスログ※1
Webサイトの閲覧、Webメールやクラウドストレージのアップロード／ダウンロードログを取得できます。

プリントログ
印刷状況を記録し、ドキュメントやプリンター、PCごとに印刷枚数を集計できます。

周辺機器・通信機器接続ログ※2
USB メモリなどの周辺機器、Wi-Fi・Bluetooth などへの接続／切断などのログを取得できます。

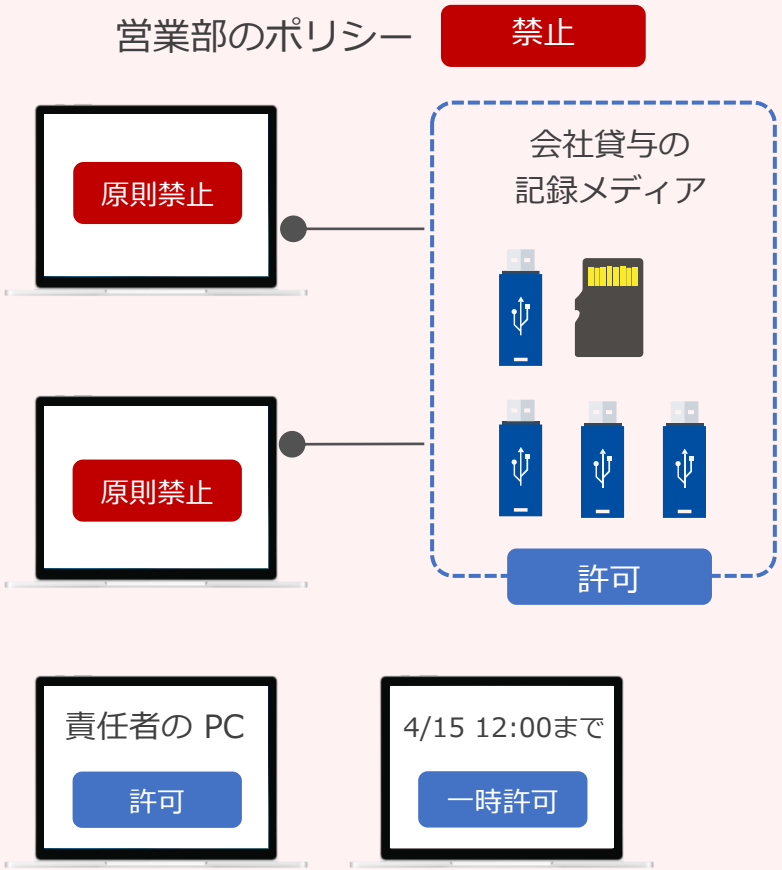
アプリ稼働・アプリ通信ログ※3
バックグラウンドで稼働しているアプリ情報、通信元／先のIPアドレスやポート番号、アプリのハッシュ値を取得できます。

※1 macOS は Web サイトの閲覧ログのみ対応しています。また対応ブラウザは Microsoft Edge・Google Chrome・FireFox・Safari です。
※2 macOS は周辺機器接続ログのみ対応しています。
※3 外部脅威調査オプションの導入が必要です。尚、macOS は非対応です。

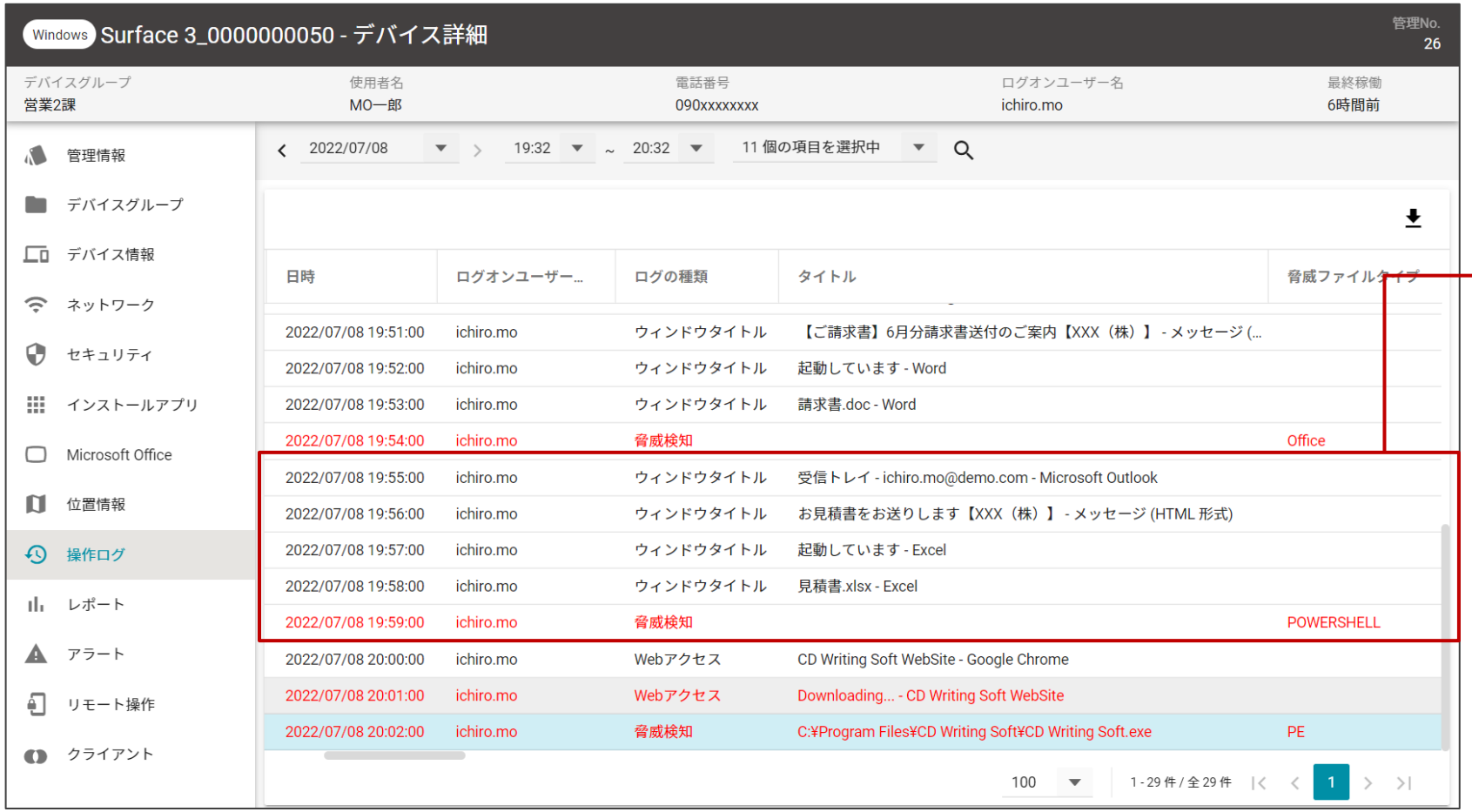
USB メモリなどの記録メディアの利用を制御し、情報漏えいを防止

グループ単位で禁止・読取専用・許可のいずれかから基本ポリシーを設定。特定記録メディアのみ許可 / 特定 PC のみ許可 / 特定時間のみ許可など柔軟な設定が可能。

記録メディア制御のイメージ



LANSCOPE エンドポイントマネージャー クラウド版の管理画面から ログを検索すると「添付ファイルの開封」が流入原因だと判明



流入原因の操作ログ

1. Outlook を起動
2. メールを開封
3. 添付ファイルの Excel を起動
4. 「見積書.xlsx」が画面表示
5. Deep Instinct で検知

※ 上図はエンドポイントマネージャー クラウド版と Deep Instinct を連携した画面です。
※ 連携機能は Windows の操作ログのみ対応です。

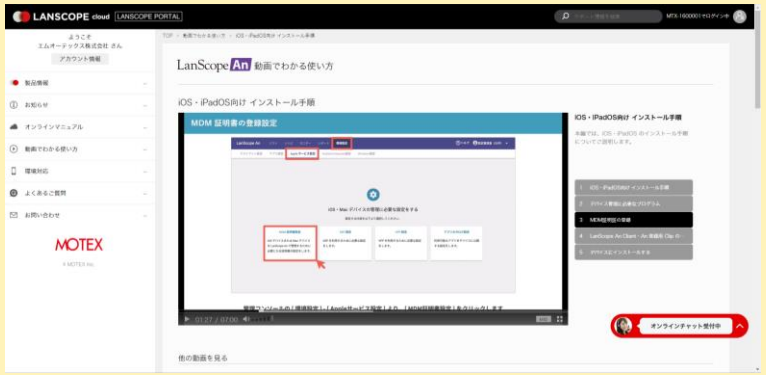
Endpoint Manager Cloud

60日間無料体験キャンペーン中

エンドポイントマネージャー クラウド版の体験版は、設定したポリシーや取得した情報を含め、そのまま製品版へのデータ引き継ぎが可能です。また体験版利用中も、弊社サポートセンターにお電話やメールで問い合わせが可能。体験期間中は、マニュアルやオンラインで学べるトレーニング動画も公開しています。

●各種マニュアル・問い合わせが可能

●動画で設定方法を説明



https://go.motex.co.jp/l/320351/2017-06-21/c55z

インシデント対応パッケージで、マルウェア感染後の対処をご支援します！

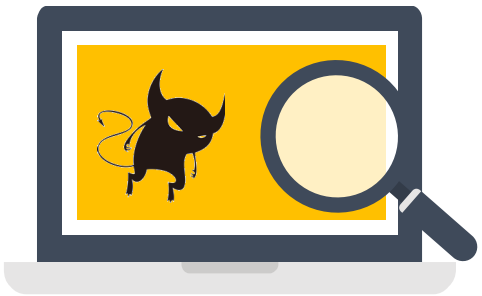
インシデント対応パッケージは、CylancePROTECT、Deep Instinct、Darktrace、Panorays、
エンドポイントマネージャー クラウド版などが未導入のお客様でも購入いただけます。

サイバー攻撃による『感染端末』や『感染のおそれがある端末』に対してフォレンジック調査が可能
また、被害の調査方針や対策方法などのアドバイスを実施します

フォレンジック調査

端末調査

対象端末の深堀調査



■サービス提供対象：日本国内※

■OS：主要対応（Windows/Linux）その他の通信ログ調査も可

■納期：最短 3 週間/台

対応支援

インシデント対応アドバイザリ

インシデント対応に不安な場合など調査方針や対策方法のアドバイス

■サービス提供対象：日本国内※

■セキュリティ専門家によるサポートを提供

- 感染時の初動対処や、インシデント対応方法などをアドバイス

※ 海外対応や macOS での端末調査などが必要な場合は、委託先（BlackBerry 社）提供のフォレンジックサービスをご提供可能です。
詳細は、別紙をご確認ください。

収集データから攻撃の痕跡を調査し、インシデントの原因究明をご支援
特定した痕跡情報から対策などを含めた報告書も作成します

項目	内容
対象端末	Windows / Linux 端末
調査対象	ヒアリング結果に応じて、以下などのデータを調査対象とします。また、状況に合わせて、別の調査手法をご提示します。 **■端末調査（標準）** （1）端末：ディスク、メモリ、ツール実行結果 （2）各種機器：資産管理ツールの操作ログ、セキュリティ機器のアラート（EPP / EDR / IDS / IPS） **■通信ログ調査（オプション）** （3）通信機器（FW / Proxy / VPN 機器など）：通信ログ、アクセスログ、認証ログ
調査内容	保全作業後、収集データに対し【侵害の痕跡 / 侵入原因 / 感染拡大 / 情報漏えいを示唆する痕跡】を調査・分析します。 調査対象 (1) (2) が全て揃わない場合や情報欠落している場合など、情報漏えいや感染拡大などの影響特定に至らない場合があります。
調査手法	ファイルシステム調査、タイムライン調査、カービング調査、メモリ解析、各種ログ調査、マルウェア簡易調査（IoC 調査）
調査期間	保全作業後、最短 15 営業日～/台 で報告書提出 ※ 弊社にて調査対象データ受領後に必要な期間です。調査量などに応じて変更する場合があります。
報告・提供物	調査中に情報漏えいなどの重大な事実の痕跡が確認された場合、暫定対策に活用できる痕跡が確認された場合（不審な通信先、ハッシュ値など）は随時ご報告差し上げます。また、最終報告として調査結果報告書の提出および報告会を実施いたします。

国家資格を保有する経験豊富なセキュリティエンジニアが
インシデントの調査方針や対策方法などをアドバイスいたします

項目	内容
概要	定期的なインシデント調査のお打ち合わせに参加し、対応方針などをアドバイスさせていただきます。
期間	別途お見積り ※ 弊社営業日の日中の対応となります。
要員	情報処理安全確保支援士（国家資格）保有メンバー
内容	・ 原因究明に向けた技術アドバイス ・ インシデント終結に向けたロードマップ提案および推進のアドバイス ・ 暫定対策、対処へのアドバイス ・ インシデント対応後の恒久対策のアドバイス
備考	・初動/封じ込めなどの対応は、適宜リモート会議を開催 ・状況確認などの定期的な会議体は、1時間程度/回のリモート会議を想定

※ 本サービスには、フォレンジック調査は含みません。

製品について詳細な説明を聞きたい場合は、オンライン相談へお申し込みください
実際の管理画面や各種資料を利用しながら、ご相談に応じます

こんな方におすすめ！

- **詳細な製品説明**をしてほしい
- 製品の**管理画面**を見たい
- **他社の運用事例**を聞いて利用イメージを持ちたい

「オンライン相談」のお申し込みはコチラ

https://www.lanscope.jp/cyber-protection/cylance/businesstalk/

製品に関するお問い合わせ

■ 営業本部

大阪本社	06-6308-8980
東京本部	03-3455-1811
名古屋支店	052-253-7346
九州営業所	092-419-2390
E-mail	sales@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター	0120-968995 （携帯・PHSからは06-6308-8981）
お電話受付時間	9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ	support@motex.co.jp