CPMS Cyber Protection Managed Service

# 被害拡大中の中小企業を狙った サプライチェーン攻撃とは

セキュリティ対策で押さえておきたい10個のポイントもご紹介

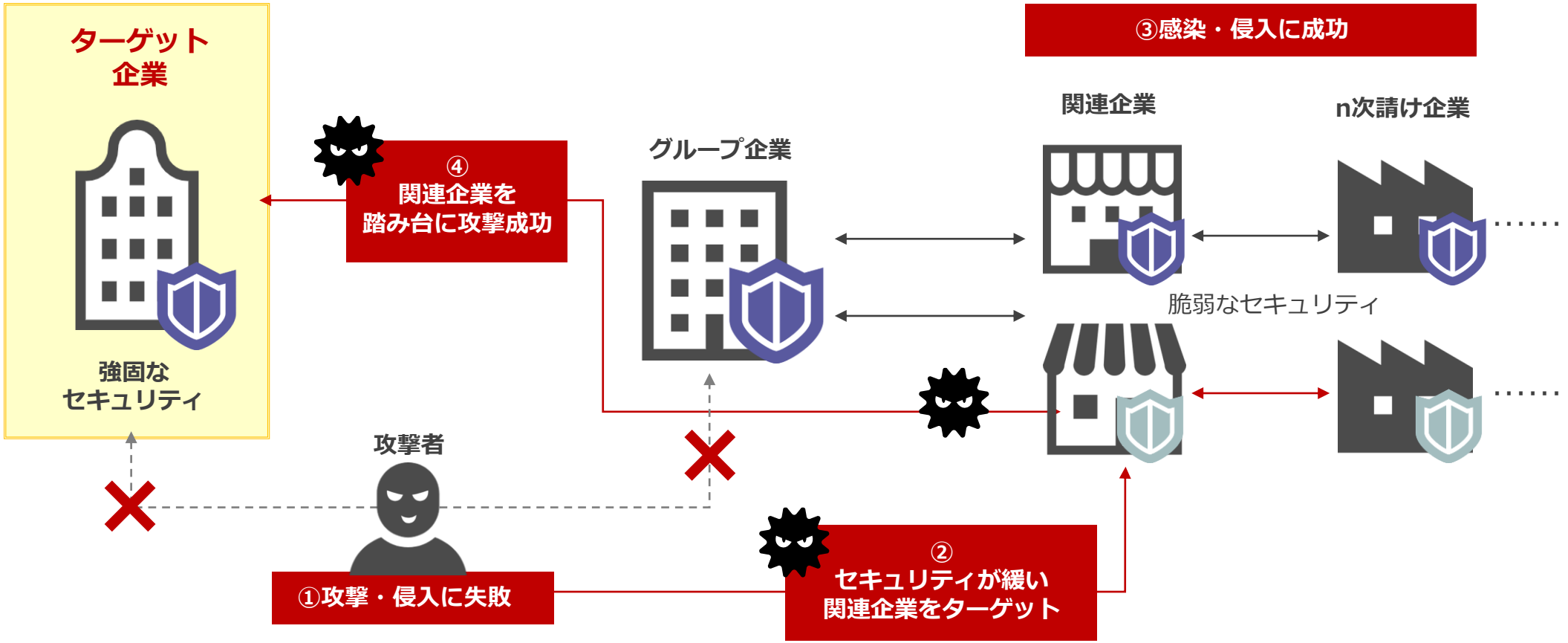
# 「サプライチェーンの弱点を悪用した攻撃」が 3位にランクイン
# 昨年順位からランクアップしているため、さらなる警戒が必要

| 昨年順位 | 個人 | 順位 | 組織 | 昨年順位 |
|---|---|---|---|---|
| 2位 | フィッシングによる個人情報等の詐取 | 1位 | ランサムウェアによる被害 | 1位 |
| 3位 | ネット上の誹謗・中傷・デマ | 2位 | 標的型攻撃による機密情報の窃取 | 2位 |
| 4位 | メールやSMS等を使った脅迫・詐欺の手口による金銭要求 | 3位 | サプライチェーンの弱点を悪用した攻撃 | 4位 |
| 5位 | クレジットカード情報の不正利用 | 4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 | 3位 |
| 1位 | スマホ決済の不正利用 | 5位 | 内部不正による情報漏えい | 6位 |
| 8位 | 偽警告によるインターネット詐欺 | 6位 | 脆弱性対策情報の公開に伴う悪用増加 | 10位 |
| 9位 | 不正アプリによるスマートフォン利用者への被害 | 7位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | NEW |
| 7位 | インターネット上のサービスからの個人情報の窃取 | 8位 | ビジネスメール詐欺による金銭被害 | 5位 |
| 6位 | インターネットバンキングの不正利用 | 9位 | 予期せぬIT基盤の障害に伴う業務停止 | 7位 |
| 10位 | インターネット上のサービスへの不正ログイン | 10位 | 不注意による情報漏えい等の被害 | 9位 |

※引用：IPA「情報セキュリティ10大脅威2022」

# 無くならないサプライチェーン攻撃！自社の対策だけでは防げない被害が急増する要因

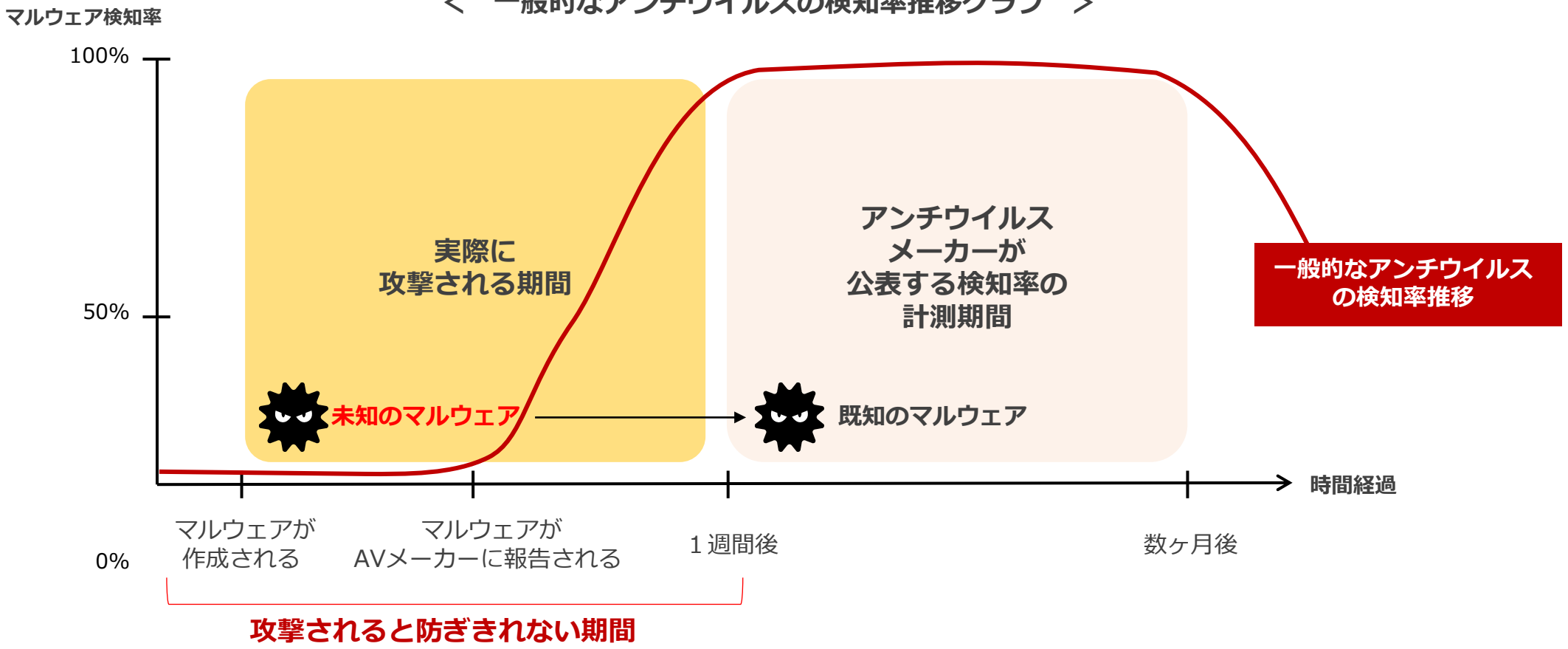
セキュリティ強度が弱い取引先（サプライチェーン）を次々と踏み台にし、最終的なターゲット企業を攻撃する手法です



# 未知のマルウェアは既存アンチウイルスの検知方式では攻撃を受けてしまう期間が発生

現在主流となっているやシグネチャ型は、攻撃を受けてからパッチを作成します。その間は攻撃を防ぐ手出てはありません

＜　一般的なアンチウイルスの検知率推移グラフ　＞



# ウイルス対策ソフトで検知されないように、大量の未知・亜種のマルウェアを作成

1度使ったマルウェアを再度攻撃に使用することは、ほとんど無い


## 1日に作られるマルウェアの数

最近では誰でもマルウェアを作成出来ます。
企業のシステム環境は常に悪意のあるユーザーによって、**膨大なセキュリティリスク**にさらされていると言えます。


## マルウェアの平均寿命

マルウェアは生まれてから、**58秒で消滅します。**
常に未知の新しいセキュリティリスクが
生まれては消えています。

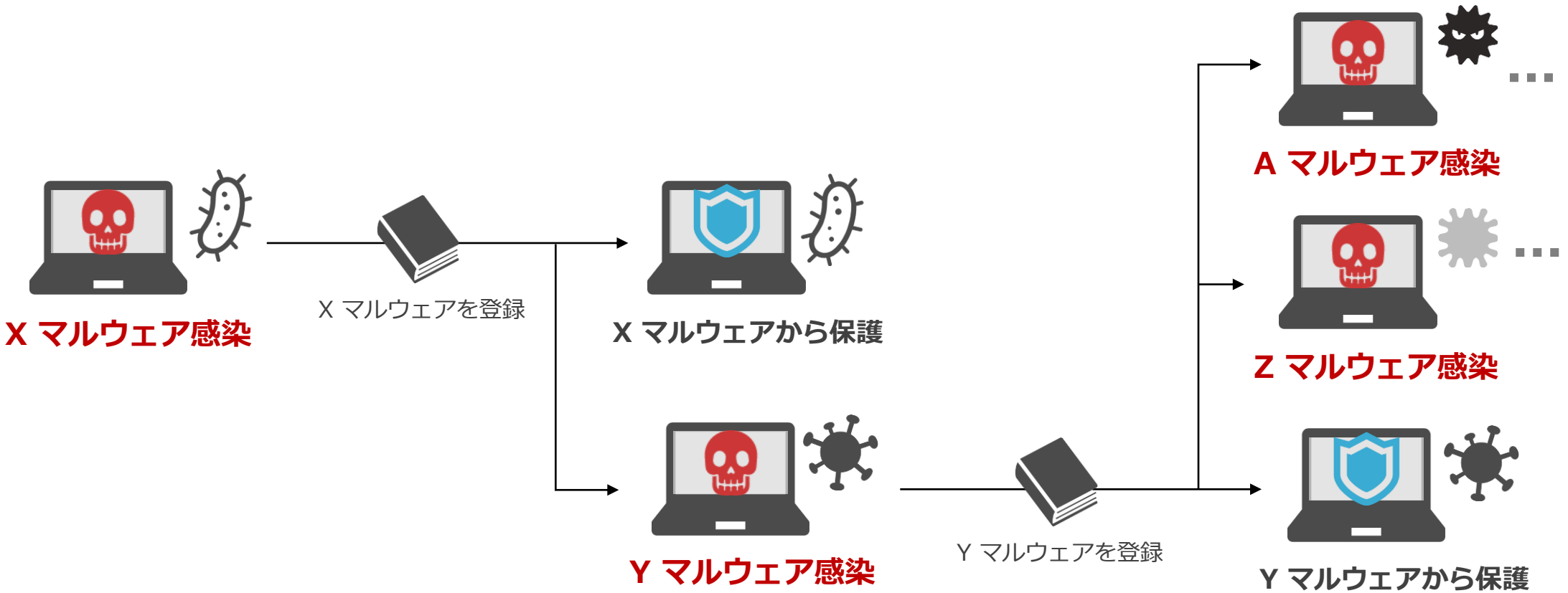

## 同じマルウェアが使われる割合

別の組織で再発見されるマルウェアは
**たったの0.5%。**つまり、同じマルウェアが
2度以上使われることはほとんどありません。
攻撃に使われる**マルウェアは、ほぼ”未知“であるといえます。**

VERIZON DBIR（データ漏洩/侵害調査報告書）2016の調査より

# 攻撃は使い捨て未知のマルウェアばかり…シグネチャベースのパターンマッチングでは限界

パターンマッチング方式は、感染報告後シグネチャに登録されれば、検知・保護が可能だが初見では検知が難しい仕組みです



## マルウェアに対抗するには高精度のアンチウイルスが必要

**未知・亜種のマルウェアを 99% 防御**

**AI を活用した高精度のウイルス対策ソフトを 2種類ご用意しています**

**CPMS** Cyber Protection Managed Service

*— Product 1 —*

BlackBerry Protect

BlackBerry Optics

*— Product 2 —*

deep instinct™

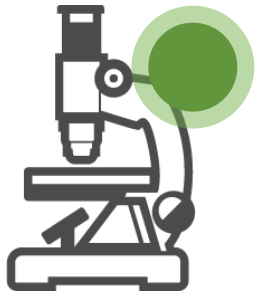
- AI による予測検知
- オフラインでも変わらない高い検知率
- 過検知が少ない

## AI 型ウイルス対策ソフト「CPMS」とは

**AI が未知・既知問わずマルウェアを隔離します**
**定義ファイルを使わないため、シグネチャ更新管理からも解放されます**

CPMS Cyber Protection Managed Service

### マルウェア検知率 99%



高性能な AI により
未知・既知問わず検知可能

### 毎日のアップデート不要

定義ファイルを使用しないため
毎日のアップデート不要

### PC 負荷が少ない

サイズは 150MB 以下、
CPU負荷 1% 以下

### オフライン環境対応

オフラインでも動作*

※インストール時にはインターネット接続が必要です

## AI 型ウイルス対策ソフトは、なぜ検知精度が高いのか？

**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 がファイルの特徴から「未知のマルウェア」を判定する**

**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
特長を分析・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

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

**ランサムウェアの可能性 99%**

# CPMS は2種類のウイルス対策ソフトのうち、用途に応じて選択頂けます

## 多くの導入実績と LANSCOPE との連携も可能

BlackBerry Protect　BlackBerry Optics

- **国内の導入実績を重視**されるお客様
- **LANSCOPE 連携**をご利用したいお客様
- **インターネット非接続環境**での運用をお考えのお客様
- **EDR 要件**への対応をお求めのお客様

## 幅広い OS やファイルタイプに対応

deep instinct™

- **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
- **スマートフォン対応**をご要望のお客様
- **複数エンジンでの防御**をお求めのお客様

# BlackBerry Protect は導入社数が多くオプションも豊富
# Deep Instinct は検知対象のファイルタイプが多く、マルチ OS に対応しているのが特長です

| | BlackBerry Protect | Deep Instinct |
|---|---|---|
| 対応OS | Windows、macOS、Linux | Windows、macOS、iOS、Android |
| 対応するファイルタイプ | PE（exeやdll） | PE,PDF,Office,Macro,RTF,SWF,JAR,TIFF,Fonts,JTD… |
| EDR | BlackBerry Optics をオプション提供 | 無し |
| MOTEXの販売実績 | 約1,400社（2016年7月から販売開始） | 約50社（2021年2月から販売開始） |
| コンソール | 日本語対応済み | 日本語対応済み |
| LANSCOPEオンプレミス版・クラウド版連携 | 連携可能 | 連携予定（LANSCOPE クラウド版） |
| 価格（年額） | **5,400円** | **3,600円** |
| 追加機能 | ・運用／代行（￥170／月額　￥2,040／年額）<br>・レポートサービス（￥80／月額　￥960／年額）<br>・Optics（￥150／月額　￥1,800／年額） | ー |

## 体験版のご案内

**両製品とも無料体験版もご用意しています！**
**無償で操作方法のレクチャーや質疑応答いたしますので、是非お試しください**

BlackBerry Protect

**▼体験版のお申込みはこちら**

| | |
|---|---|
| 概　　要 | BlackBerry Protect がキャンペーン期間中にライセンス数無制限で使えます。また、検知したファイルについてサマリーレポートを作成させて頂きます。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 | BlackBerry Protect を初めて導入するユーザー様 |
| ご利用期間 | 1ヶ月間 |
| 申 し 込 み | 上記キャンペーンサイトからエントリー |
| 申 込 期 間 | 2022年9月30日 |

deep instinct™

**▼体験版のお申込みはこちら**

| | |
|---|---|
| 概　　要 | Deep Instinct が 100L まで、1ヶ月間無料でお試し頂けます。<br>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。体験中の不明点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ヶ月間 |
| 申 し 込 み | 上記キャンペーンサイトからエントリー |
| 申 込 期 間 | 常時受付 |

## セキュリティ対策で押さえておきたい10個のポイント

| ✓ | チェック項目 | 詳細 |
|---|---|---|
| | バックアップ | 機微な情報、リスクの高いデータについては、単にバックアップを取得するだけでなく、オフラインで保管しておく。<br>これに加えて、クラウドストレージを用いる場合でも、予めデータをもとに戻す手順の確立とテストは重要である。 |
| | ユーザー権限の厳密化 | 先に述べたように、ランサムウェア攻撃では、単にデータの暗号化による盗難だけでなく、被害者ネットワークを水平に動き回り（ラテラルムーブメント）、被害者にとって重要なデータを窃取しようとする。このため、Active Directory で管理しているユーザーアカウントを再確認し、特権ユーザーの絞り込みやルールの見直しを行い侵害を抑えることが重要 |
| | パッチ | OS などの脆弱性パッチはテストの上、更新適用しておく。最近では、Microsoft Exchange の脆弱性（ProxyShell）を悪用して水平展開を行うランサムウェアも観測されている。最新のパッチを適用することで、このような侵害の広がりを防ぐことができる。 |
| | ウイルス対策ソフト | 最新の状態で、組織に合う最良の設定で利用する。また次世代型のように未知・既知の脅威どちらでも高精度で検知・駆除できるものを検討する。 |
| | VPN機器 | VPN機器が最新バージョンになっているかを確認する |
| | ファイアウォール | ファイアウォールを用いて不正 IPアドレスへの通信を適切にブロックする。 |
| | ホワイトリスト運用 | アプリケーションのホワイトリスト運用などで、許可されたアプリケーション以外の実行を防止するような運用管理を行う。 |
| | メールスキャン | メールの送受信スキャンを実施し、スパムや不正なもの、実行ファイルが添付されているものなどを検知・駆除する。 |
| | リモート接続サービス | リモート接続サービスを棚卸し、使用していないものは無効にしたり、接続時の認証に多要素認証を取り入れたり、リスク管理方針に基づいて継続的な認証（c.f. ゼロトラストアーキテクチャー）を実装する。 |
| | 従業員教育の実施 | ユーザー認知トレーニングの実施：ユーザーは、コンピューターに一番近い存在。彼らに対して、認知を高め、トレーニングを実施する。<br>・信頼できないウェブサイト、メールの添付ファイルやリンククリックなどをしない。メールゲートウェイなどでフィルタ設定も検討する。<br>・信頼できない Webサイトからファイルをダウンロードしない。<br>・不明な USBメモリを使わない |

## セキュリティ教育のコンテンツを無償でご提供してます



**セキュリティブック**

書籍をデータで閲覧したり、
印刷してお使いいただけます。


**テスト**

復習や理解度の確認に
お使いいただけます。


**講師用資料**

セキュリティブックの内容をもとにした資料です。
投影やeラーニングでお使いいただけます。

**詳細について**

詳細やダウンロード方法などは
QRコードから Webサイトに
アクセス頂きご確認ください

# お問い合わせ先

## ■製品に関するお問い合わせ

**エムオーテックス株式会社 営業部**

大　阪本社： 06-6308-8989

東　京本部： 03-5460-0775

名古屋支店： 052-253-7346

E-Mail：sales@motex.co.jp

## ■ご導入後の運用に関するお問い合わせ

**エムオーテックスサポートセンター**

**0120-968-995**

※携帯からは06-6308-8981

※受付 9:30～12:00/13:00～17:30（月～金、MOTEXの営業日）

**メールでのお問い合わせ**

support@motex.co.jp（※24時間受付）

**関連サイト**

| | |
|---|---|
| エムオーテックス株式会社 コーポレートサイト | http://www.motex.co.jp/ |
| CPMS（Cyber Protection Managed Service） 製品サイト | https://www.lanscope.jp/cpms/ |
| BlackBerry Protect 製品紹介 | https://www.lanscope.jp/cpms/blackberryprotect/ |
| Deep Instinct 製品紹介 | https://www.lanscope.jp/cpms/deepinstinct/ |