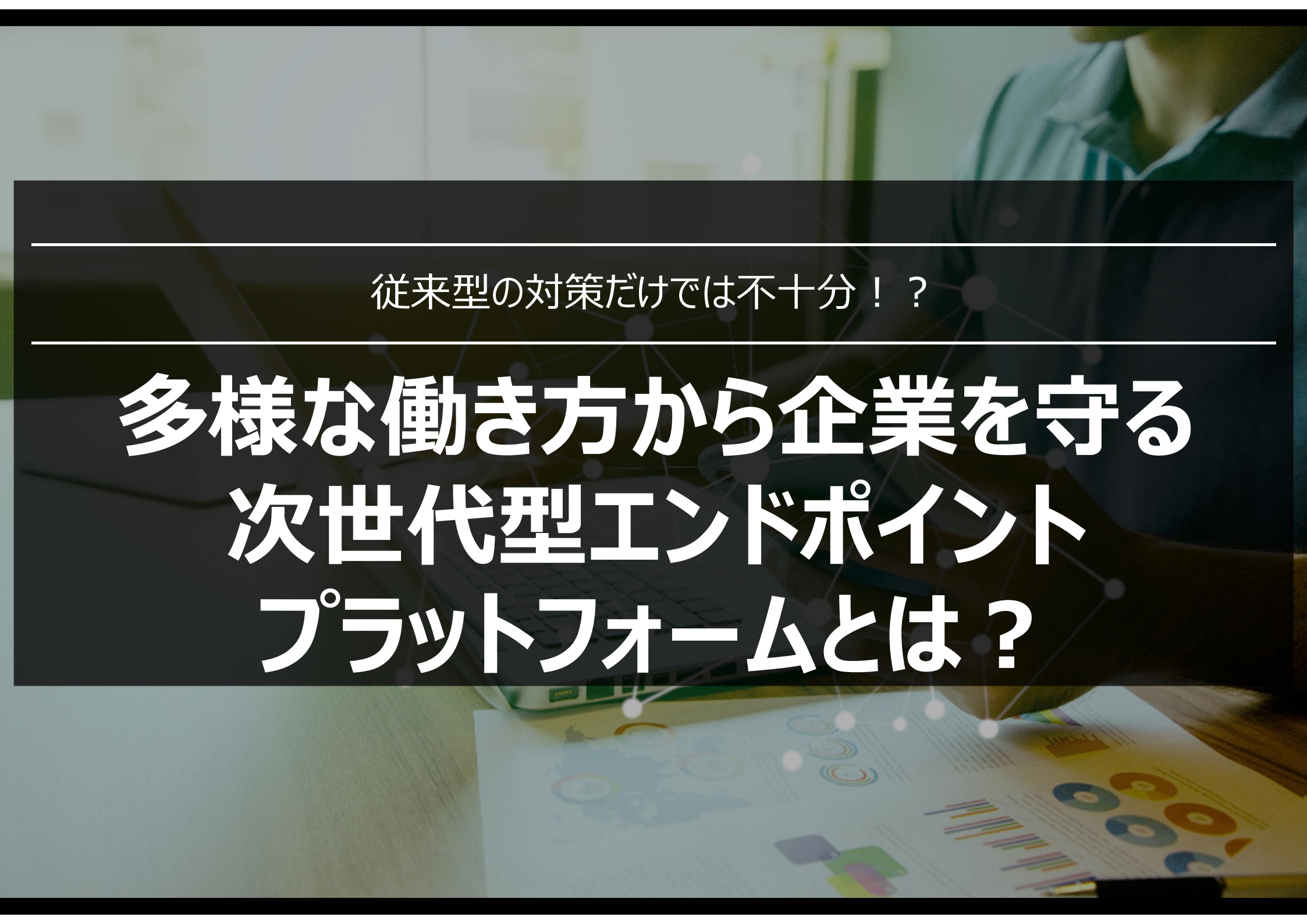


従来型の対策だけでは不十分！？

多様な働き方から企業を守る次世代型エンドポイントプラットフォームとは？

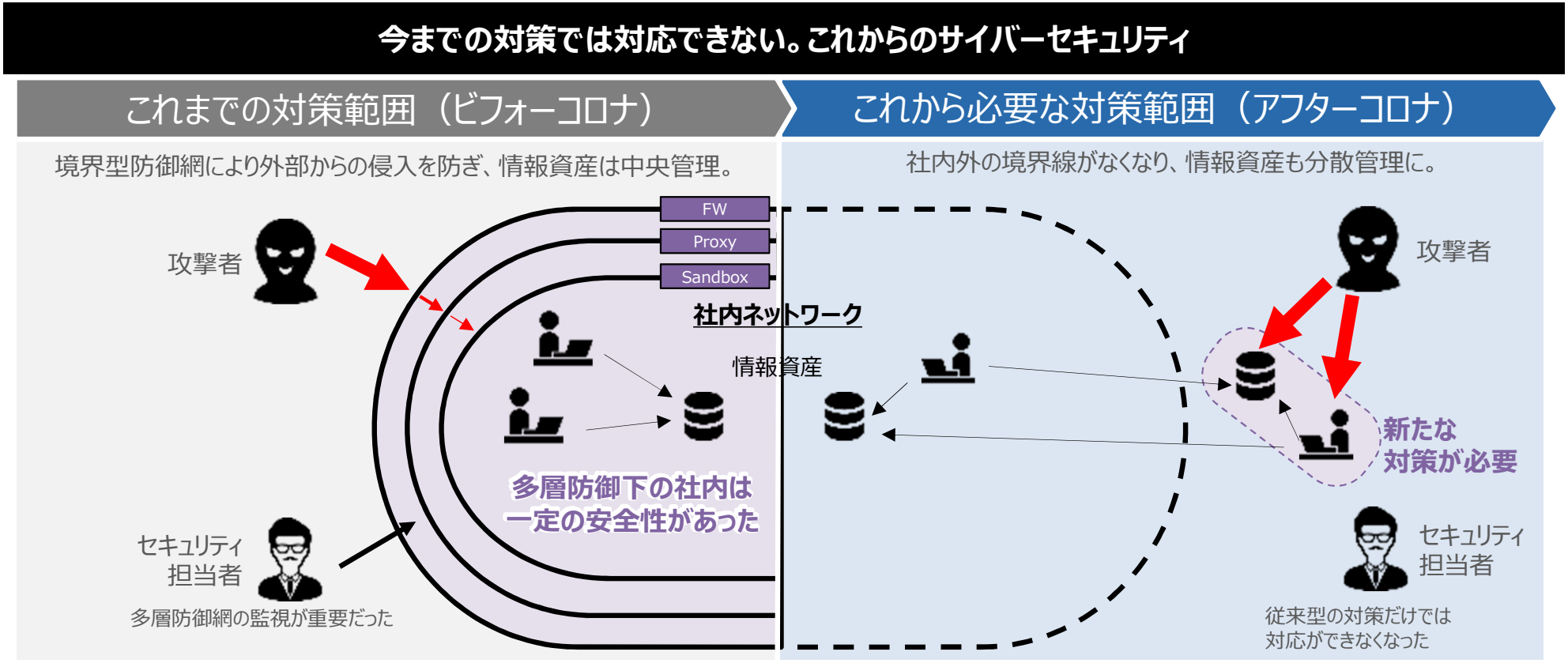
目次

1章
働き方の変化とサイバーセキュリティの対応

働き方の多様化により、セキュリティ対策にも変化が必要

感染症対策の一環として在宅勤務を取り入れる企業や、働き方改革推進の影響から、時短勤務やサテライトオフィス勤務を導入する企業は増加しています。**このような変化に伴い、環境変化に合わせてセキュリティ対策を最適化するために見直しをする必要性が強まっています。**

今までは社内からアクセスすることが前提だったため、境界型防御網を構築することでセキュリティを高めていました。しかし、多様な働き方が認められるようになったため、様々な場所・端末からのアクセスに対応した**新たなセキュリティ対策が必要となってきています。**



働き方の変化に伴い増える主なセキュリティリスクのポイント

前述のとおり、働き方の変化に伴い、セキュリティ対策においても変化が求められるようになりました。
留意すべき主なセキュリティリスクのポイントとして、以下のような点が挙げられます。

従来のセキュリティ対策が通用しなくなり、これまでとは異なったポイントに留意してセキュリティ対策を行う必要があります。

これからの変化に伴う主なセキュリティポイント

監視時間の増加に伴う負担の増加など

柔軟な勤務時間を採用したことで、従来よりも、**監視すべき時間が長くなる**。

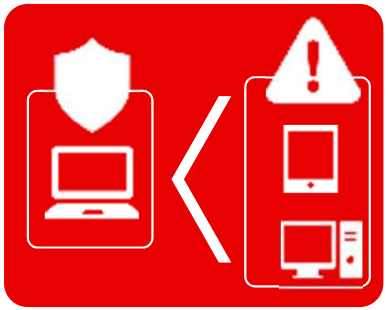
ユーザーガバナンスの低下による感染リスク

誰も見ていないという環境からのヒューマンエラーや、**巧妙化した攻撃からの感染のリスク拡大**。

NW設定不備、境界防御不足による感染リスク

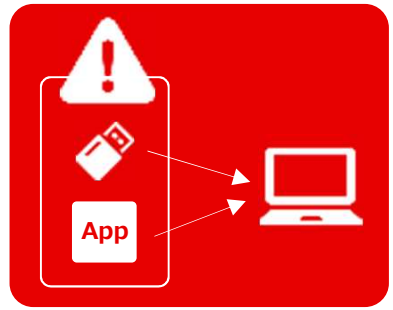
家庭や公共施設のWi-Fi利用を想定した設定、セキュリティ対策が必要となる。

端末の増加による感染状況把握不可など



端末増加に伴い、セキュリティレベルにばらつきが出る。また、**感染状況の把握も困難**になる。

勝手アプリやUSB利用による内部不正リスク



USB接続や会社指定外アプリの利用による不正・感染リスクの増加。

巧妙化するサイバー攻撃に対策を強化してきた企業

80年代、90年代は不特定多数を対象にした愉快犯によるサイバー攻撃が多かったと言われています。一方で、2000年以降から現在にかけては、特定の組織や個人を狙った金銭や機密情報の取得といったように攻撃の目的が変化しています。**その為、サイバー攻撃を受けた企業の被害規模も拡大傾向にあり、セキュリティ対策の必要性が増加していることがわかります。**
近年の攻撃者は、ターゲットとなる企業の組織や取引先を始めとした情報収集を行い、関係者しかわからない企業名、担当者名等を駆使し攻撃ツールの配送を行うなど巧妙な手口を利用してきます。また、利用される攻撃ツールの半数以上はマルウェアフリーの手法となり従来のセキュリティ対策では検疫が困難となります。その為、**企業の対策も”侵入を前提として侵攻を防ぐ対策”を取ることも重要**となります。

サイバー攻撃と企業対応の主な変化

	攻撃例	攻撃目的	攻撃対象	企業の対応
1980年代	ウイルス	愉快犯	不特定多数	侵入防止
	ワーム			
1990年代	スパイウェア			
	スパムメール			
2000年代	フィッシング	金銭・気密情報の搾取	特定の組織・個人	多層防御＋侵入後の実害を防ぐ対策
	標的型メール			
2010年代	ネットバンキング不正送金			
	ランサムウェア			
近年のトレンドやポイント		攻撃の半数以上はマルウェアフリーで侵入し、重要な情報資産に横展開され、情報が盗られてしまう。		巧妙な攻撃を想定し、横展開を可視化した上で、24時間365日の監視が重要となる。

2章
改めて意識したいセキュリティポイントとその対応

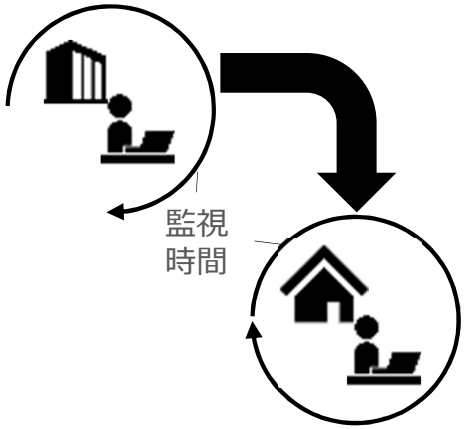
監視時間の増加｜

ブレイクアウトタイムに対応するためには、24/365のリアルタイム監視が重要に

働き方の多様化により定時で固定された時間以外にも端末を操作する社員が増えることが予想されます。昨今のブレイクアウトタイム（最初に感染した端末から、他の端末へ横展開されるまでの平均時間）は2時間を切っており、たとえ夜中であっても、攻撃を検知した場合には、対処・復旧(停止・端末隔離、遠隔修復作業等)を行う必要があります。

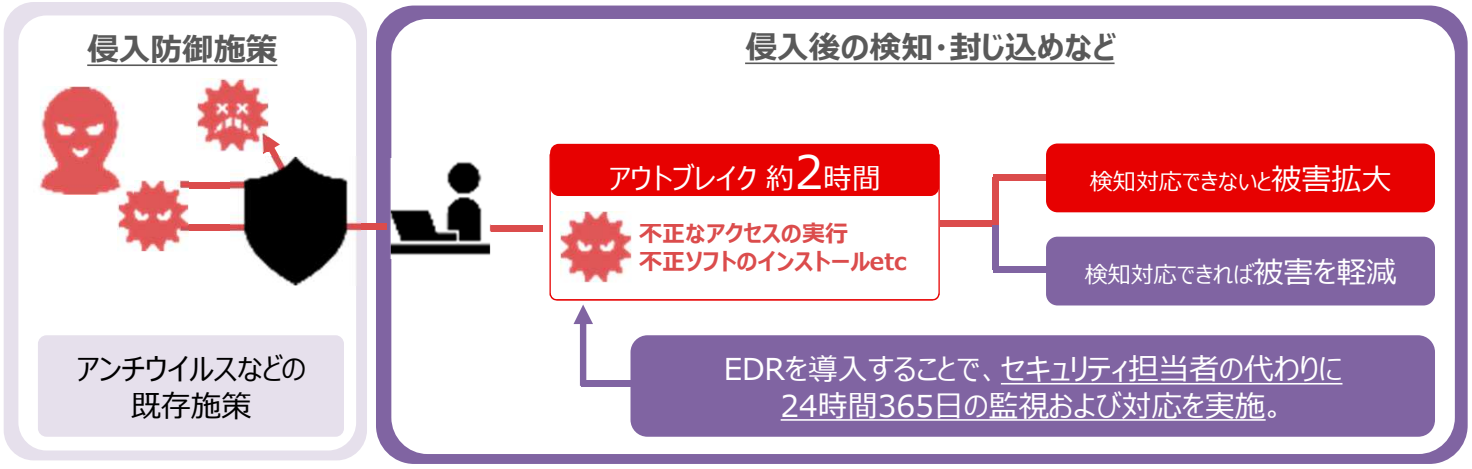
感染リスクを低減する取り組みは前提として、万が一侵入を許してしまった際にも、**リアルタイムに検知・対応できるようなEDR （Endpoint Detection and Response）の用意が重要**です。

24/365の監視が重要



多様な働き方に伴い、**稼働している端末の時間がバラバラになったことで、24時間365日の監視体制が重要**となった。

リアルタイムな状況把握・対応が可能な仕組みが重要



ブレイクアウトタイムは2時間を切っているため、早急な検知・対応が求められる。
しかし、24時間365日の監視体制を人手で行うことは難しいため、たとえ侵入を許しても、検知・対応できるような仕組み（EDR）の導入が重要。

※ ブレイクアウトタイムのデータは、2020 CrowdStrike グローバル脅威レポートより抜粋
https://www.crowdstrike.jp/resources/reports/2020-crowdstrike-global-threat-report/

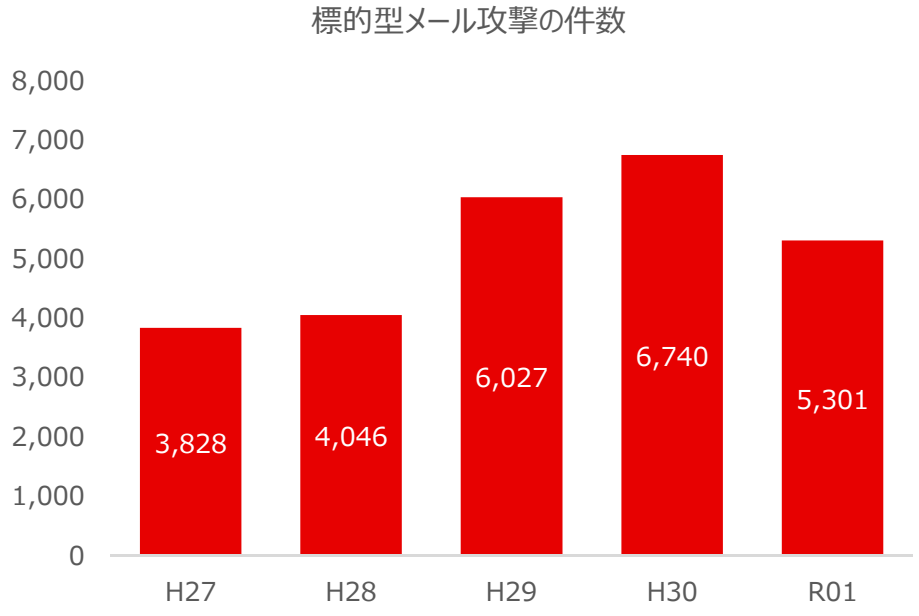
ユーザーガバナンスの低下｜

増加する標的型攻撃には水際対策だけではなく、侵入後の対応もより重要に

多様な人材が様々な場所で勤務するようになると、不用意にリスクの高いメールに添付されているファイルを開封してしまうこともあります。このような標的型攻撃は年々巧妙化しており、具体的な情報を交えて送られてくることがあり、うっかり開いてしまう人も少なくありません。

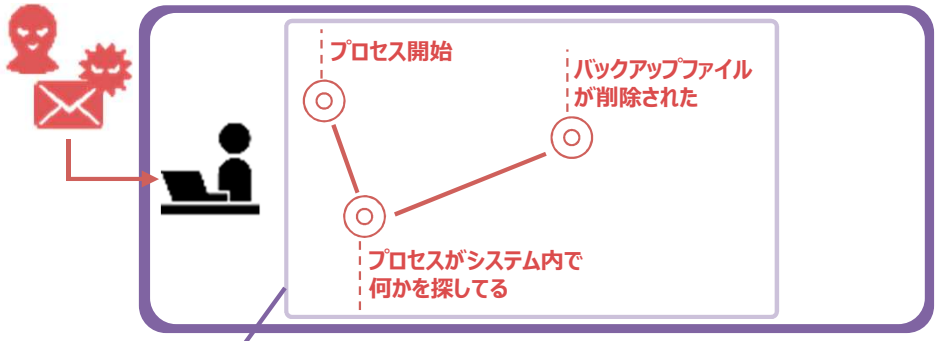
開封前の水際対策も重要ですが、侵入後に素早く検知し、対応することもより重要となってきています。

水際対策だけでは対応しきれない可能性が高い



出典:「令和元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」(警察庁)
(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei.pdf)

侵入されてしまった後に検知できる対策も重要



侵入されてしまった後にその脅威を検出する為には各端末上で発生している「振る舞い」を収集できている必要がある。

この振る舞いを収集する仕組みとしてEDR等を検討することで悪意のある攻撃者による巧妙な攻撃(OS標準コマンドを利用した攻撃手法など)を検出/ブロックすることが可能となります。

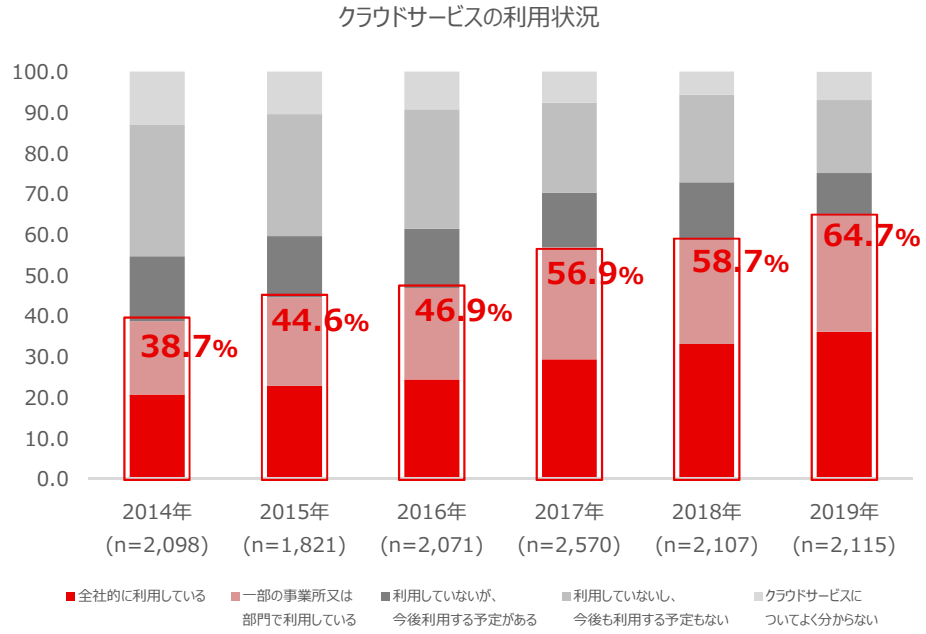
エンドポイントセキュリティ強化の必要性増加｜

クラウド利用の増加によりエンドポイントセキュリティの強化が重要に

クラウドサービスの普及や、在宅勤務のような多様な働き方が増えることにより管理外端末・ネットワークからの接続が増加します。

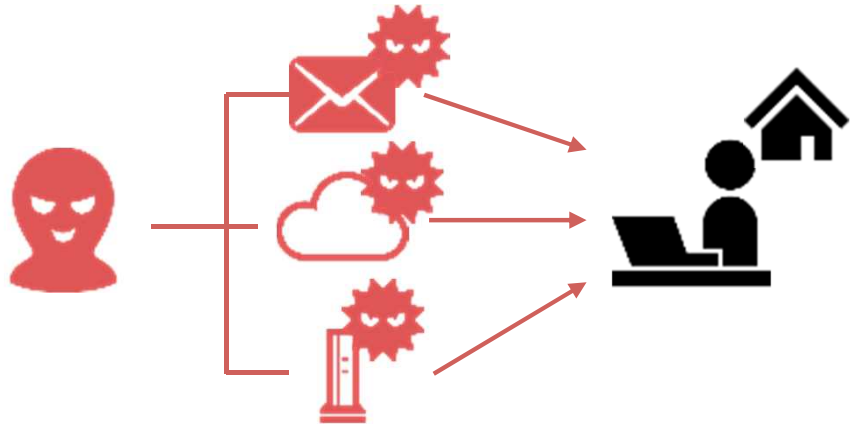
標的型メールへの注意喚起や自宅Wi-Fiルータ使用時のファームウェアの更新、偽Wi-Fiスポット接続への注意など、社員に対してセキュリティ意識を高めるような施策に加え、エンドポイントにおけるセキュリティ強化が必要となります。

6割以上の企業がクラウドサービスを導入



出典:「通信利用動向調査」(総務省) より作成
(https://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html)

エンドポイントでのセキュリティ強化が重要



従来よりも、悪意ある攻撃者からの攻撃機会が多くなると想定されるため、エンドポイントにおける侵入予防対策・侵入後の検知/対応の対策をより強化することが重要。

端末増加に伴うセキュリティ状況可視化の必要性増加｜

対策できていない脆弱性のリスクを可視化し、早期に対応可能な体制構築が重要に

従来であれば、本社内の限られた端末のみを管理していましたが、サテライトオフィスでの勤務や在宅勤務のような多様な働き方が認められるようになると、社外にある端末も管理していなければなりません。

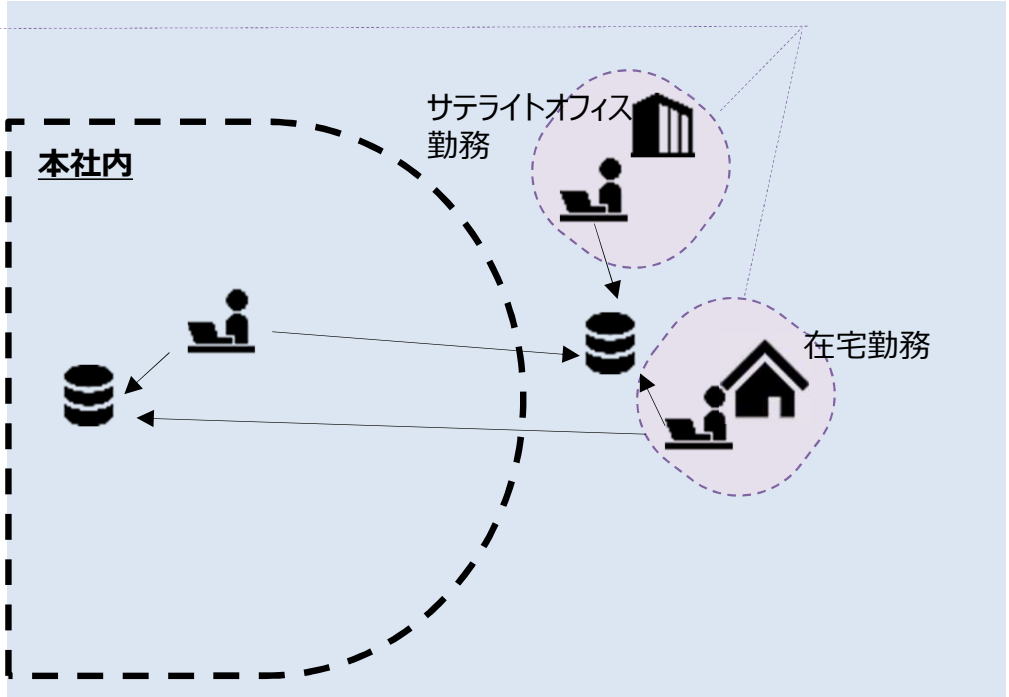
脆弱性を抱えたままの端末の数を把握できたり、パッチなどを適用できていない端末の検索できたりすることが重要です。

脆弱性やパッチの適用状況の迅速な可視化

以下のような情報が迅速に可視化され、適宜対応が行える体制が重要

在宅勤務やサテライトオフィスで勤務している社員の端末であっても以下のような情報を一元的に確認できるようにし、脆弱性が見られる端末（社員）には連絡が行くような仕組みづくりが重要。

- Windows OSの脆弱性を可視化しリスクのある端末の洗い出し
- 適用されていないパッチベース、CVE番号ベースで端末の検索



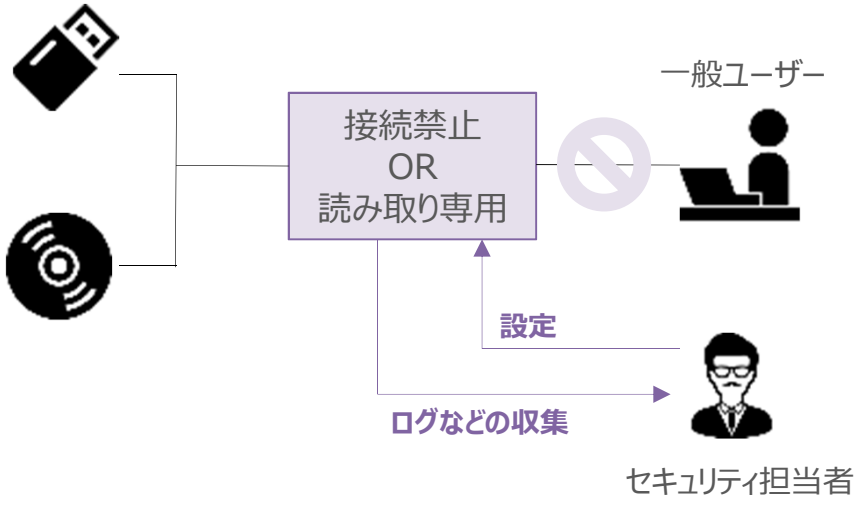
デバイス制御・IT資産管理の対応強化｜

ユーザーが勝手利用してしまうUSBやシャドーITの利用を監視・制限する対策も重要に

社内ネットワークを利用していればデータの受け渡しは社内ネットワーク上の共有フォルダを利用することで簡単に行えますが、在宅勤務やクラウドサービスの利用が増えるとそうはいきません。一般ユーザーは利便性を重視して、USBのような外部デバイスを利用したり、社内で許可されていないストレージサービスやアプリを利用したりすることも少なくありません。

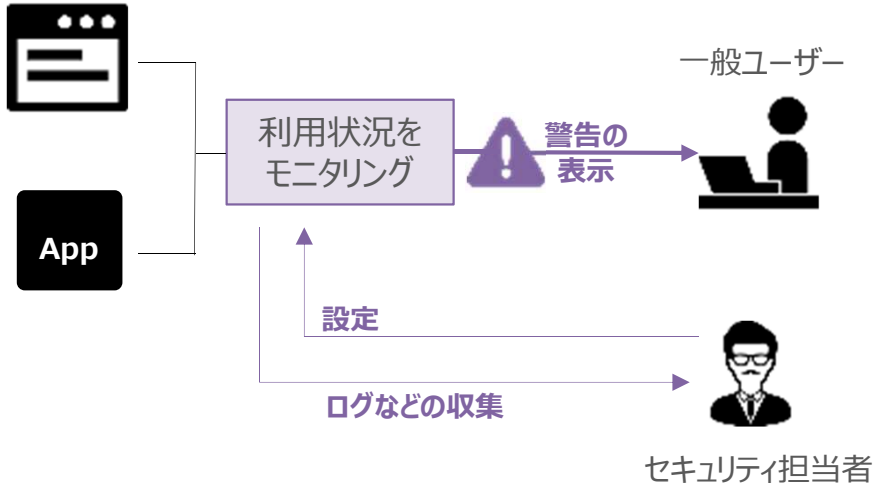
上記のようなケースからウイルスの感染や情報漏えいリスクを低減させるためには、外部デバイスの接続を制限したり、ログ情報を監視し、適宜警告を行うことが重要となります。

外部デバイスを制限することでリスク低減



外部デバイスの接続をできなくしたり、読み取り専用にすることで感染リスクや情報漏えいリスクを低減させることが重要。

勝手アプリ、シャドーITの監視、警告



業務に関係ないWebサイトの閲覧や利用が承諾されていないWebサービス、アプリの利用状況をログ情報をもとに監視。状況に応じて警告などを表示させるようにする。

各フェーズの対策を一気通貫で管理できるシステムによって業務効率も向上

資産管理ツールを利用した予防・事前対策フェーズ、侵入・感染を検知するフェーズ、不審なソフトウェアなどを検索・対処するフェーズなど多層構造での対策が必要となってきています。

各フェーズや対策において別々のシステムを導入されている企業が多いですが、管理や検知後の対応をスピーディーに行うためには、ワンストップで提供しているシステムを検討することも重要です。

ワンストップでセキュリティ対策ができるシステムが重要に

予防・事前対策フェーズ			検知・対処フェーズ			自動化・効率化	
IT資産管理	脆弱性管理	デバイス管理	AV	EDR	脅威ハンティング	自動分析（脅威情報）	マルウェア検索
							
IT資産管理やデバイス制御などを通じて、端末の状況を把握・制御する。不正行為や感染などが発生するリスクを低減させる。			ウイルスの侵入予防や侵入後の振る舞い検知・対処により被害の発生を防止または、低減させる。			検知・ブロックしたマルウェアの自動解析や検索を通して、防止精度の向上や効率化を図る。	

各ツールやシステムを別々に導入するのではなく、
ワンストップで対応できるような仕組みを導入することで、管理性が高まる。

3章

次世代のセキュリティプラットフォーム「Falconプラットフォーム」

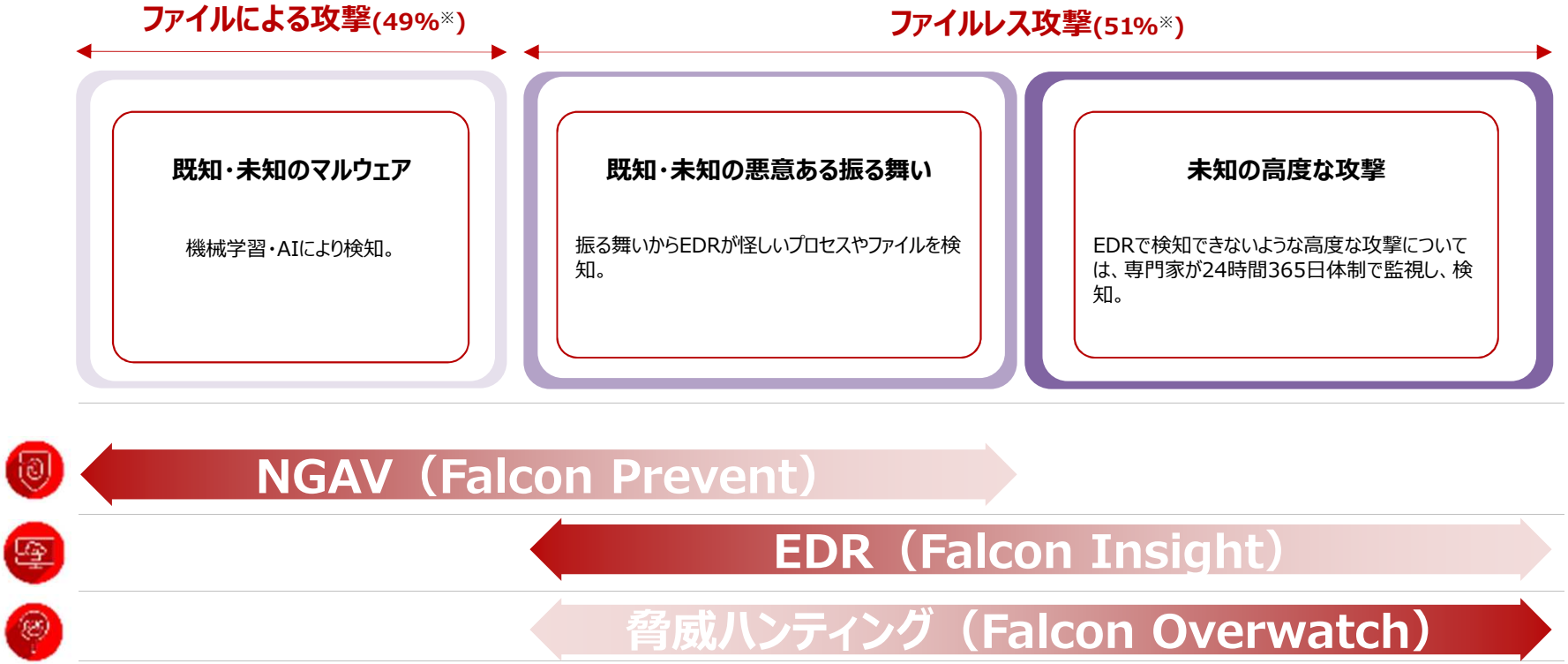
多層構造のセキュリティをワンストップで対応する
CrowdStrikeの「Falconプラットフォーム」

多様化する働き方の変化に対応するためには**エンドポイントセキュリティの強化**や**侵入予防・侵入後検知、対処**のレベルを高く保つことに加えて、情報セキュリティの担当者が、一元的に情報を閲覧・管理できる仕組みづくりも重要となります。

CrowdStrikeの「Falconプラットフォーム」を用いることで、一元管理できることに加えて、単一の軽量なエージェントを採用しており、追加機能に対して新たなソフトウェアのインストールが不要なため、ユーザー側の手間やPCへの負担は最小限に抑えることができます。
また、世界規模で収集したデータをもとに分析し、高度で新たな攻撃手法もより素早く、確実に発見できる仕組みが構築されています。

自動ブロックと検知・対処｜CrowdStrikeのNGAV、EDR、脅威ハンティングについて

CrowdStrikeの自動ブロックと検知・対処に関するソリューション



※ 割合は、2020 CrowdStrike グローバル脅威レポートより抜粋。crowdstrike.jp/gtr　よりダウンロード可能。

自動ブロックと検知・対処のモジュール詳細｜CrowdStrikeのNGAV、EDR、脅威ハンティング機能詳細

CrowdStrikeの自動ブロックと検知・対処に関するソリューション

NGAV

Falcon Prevent

- 豊富な検知ロジックによる防御(ML・振る舞い検知・ランサムウェア・エクスプロイト)
- 検知画面によるアラートシナリオの可視化
- アラートに関するハッシュ値やドメインなどの詳細情報を把握可能
- 豊富な検知ロジックにより、多層的な防御をすることが可能であり、最新の攻撃に対して素早い検知やブロックを行うことが可能

EDR

Falcon Insight

- 豊富な検知ロジックによる検知
- 端末のイベントログをリアルタイムで収集しているため、影響範囲や原因調査が可能
- 検知画面から同一実施可能なリモートでの端末隔離可能
- Real-Time-Response機能による端末への任意コマンド実行
- Investigate(Splunk画面)による各種柔軟なイベントサーチ
- 端末間の横展開含む情報の可視化

脅威ハンティング

Falcon Overwatch

- CrowdStrike社のハンティングチームによる24365体制での脅威ハンティング
- 精度の高いNGAV, IOAをもすり抜ける新たな脅威の検出がミッション
- 新たな脅威が発見された場合は、遡りの調査と、製品側の検知ロジックへの反映

予防・事前対策｜CrowdStrikeの情報資産管理ツール

CrowdStrikeの予防・事前対策に関するソリューション

デバイス制御

Falcon Device Control

- USBデバイスの利用状況の可視化
- デバイスの種類（ストレージ、マウスなど）や固有情報を基にした利用制限が可能
- 利用制御ポリシーは、任意の端末群ごとに柔軟な適用が可能
- Insightと統合されたエージェント、コンソール

IT資産管理

Falcon Discover

- 組織内に存在するFalcon未導入端末の可視化
- 利用アプリケーションやバージョンなどの詳細の可視化（Windowsのみ）
- ログインしているユーザーアカウントとその端末情報の可視化（Windows のみ）
- AWS (Amazon Web Service) 上に展開されているサービスの可視化

脆弱性管理

Falcon Spotlight

- Windows OS含むMicrosoft製品やよく利用されるアプリケーション（Adobe製品、ブラウザ等）の脆弱性を可視化しリスクのある端末の洗い出し
- スキャンや待ち時間不要
- 適用されていないパッチベース、CVE番号ベースで端末の検索
- 脅威インテリジェンスと組み合わせ、優先度の高い脆弱性を把握可能
- Insightと統合されたエージェント、コンソール

ホストFW統合管理

Falcon FIREWALL MANAGEMENT

- ホストグループ単位にFirewallポリシーの設定/適用が可能。
- 設定もクラウドから自動的に反映されるため、容易に管理可能
- Firewallポリシーでブロック/許可した通信を、管理コンソール上に表示することが可能

自動化とプロアクティブな防御｜CrowdStrikeの脅威インテリジェンス

CrowdStrikeの自動化とプロアクティブな防御に関するソリューション

脅威インテリジェンス

Falcon X

- 帰属済み攻撃者の情報を提示
- 解析から得られたインディケータと同一サンプルと類似したサンプルのインディケータも提供
- CrowdStrike社が収集したインディケータ情報の提供
- CrowdStrike社が追跡する120を超える攻撃者のプロファイル情報 (TTPs)の閲覧
- 攻撃オペレーションに関する情報
- 新しい攻撃等に関するリアルタイムなアラート＆レポート
- Weekly/Quarterly レポート
- SIEM等に取り込むためのAPI、Feeds等
- CrowdStrike社の戦略的かつ戦術的な脅威インテリジェンスの利用可能(Premium)

マルウェア高速検索

Falcon Search Engine

- 20年以上に渡り収集された膨大な数のマルウェアの検索エンジン
- 特許取得技術により、マルウェアのバイナリなどのデータに含まれる文字列、バイト列を高速に検索
- 検索には、Yara rule も利用可能で、定期的な検索も可能
- 検索で得たマルウェアはダウンロード可能

マルウェア自動解析

Falcon Sandbox

- ブロックしたマルウェアに関する追加情報を入手する為、自動的にサンドボックスでの解析を実施
- Hybrid Analysis (動的＆静的分析)テクノロジーによる正確な分析力と高い検知力
- 動的解析環境は、常に最新のAnti-VM, Sandbox に対応
- 外部のマルウェア検査基盤との連携により、トリアージが容易
- CrowdStrike社の脅威インテリジェンス及び Falcon MalQuery との統合が可能
- Restful API による運用が可能

会 社 名	マクニカネットワークス株式会社
所 在 地	〒222-8562 神奈川県横浜市港北区新横浜1-5-5 マクニカ第2ビル
設　　立	2004年 3月 1日
代 表 者	代表取締役社長 池田 遵
資 本 金	3億円（2020年 3月31日現在） ※株式会社マクニカ100%出資子会社
事業内容	企業向けネットワーク、セキュリティ関連ハードウェア・ソフトウェアの輸出入、開発、販売コンサルティング・保守サービスにわたるITソリューションの提供

本資料についてのお問合せやご相談は下記までご連絡ください。

マクニカネットワークス株式会社

お問合せ先

Mail:cs_sales@cs.macnica.net

Tel:045-476-2010