# ウィルス対策ソフト（Ｃｙｌａｎｃｅエンドポイントセキュリティ）のご提案

あなたの「いつものつなぐ」を創る。

エネコム

# 次世代マルウェア防御製品のご提案


## 特徴

1. AI技術（機械学習）により抽出された特徴点から総合的に判断して
   高い検知率を実現
2. パターンファイルの更新不要、クラウド環境による集中管理で
   運用負荷を低減

# 会社概要

BlackBerry

- 設立：1984年
- 本社：カナダ　オンタリオ州　ウォータールー
- 従業員：約4000名
- FY2020売り上げ：$1,099 million (Non-GAAP revenue)
- 取得特許数： 37,000
- 研究開発センター：7カ国、18拠点

BlackBerry 実績:

- 顧客数：12,000社以上
- ５億台のエンドポイントデバイスを保護
- JCDCの数少ない民間企業
- 2020年度 約2,000 件の特許を取得
- ２億台のQNX搭載車

CYLANCE

2019年2月
Cylance社買収

DEFCON

Defcon 29　2021年
1位と３位

Enterprise Advanced Security アワード
SE Labs アワード 受賞製品
SE Labs AAA January 2022 Enterprise Advanced Security (Protect)
BlackBerry Protect and Optics

SE-Lab Advanced Security 2022年　最高の「AAA」評価

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021

2021 Cyber Security Excellence Award Artificial Intelligence Security

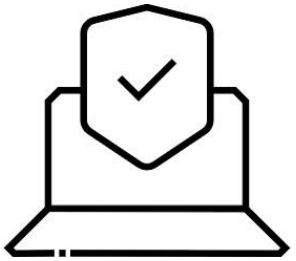
GOLD Center for Threat-Informed Defense FOUNDING AFFILIATE MITRE ENGENUITY

MITRE Engenuity Center for Threat-Informed Defense (Center) ゴールドアフィリエイト

# CylancePROTECTの4つの機能

数理モデルを活用したマルウェア防御機能含む4つの機能

## マルウェア防御

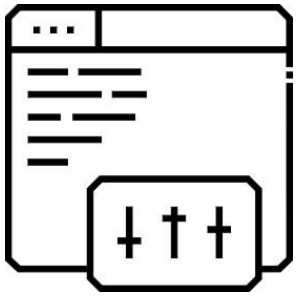


〇AI（人工知能）で脅威を予測
〇マルウェアを実行前に阻止
〇シグネチャ不要
〇毎日のスキャンが不要
〇ファイルシステム変更時にスキャン
〇潜在的に望ましくないプログラムが
　環境に入るのを拒否

## メモリ防御

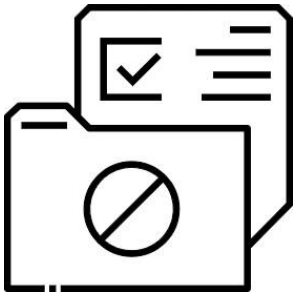
〇メモリの悪用防御
〇脆弱性攻撃の防御
〇プロセスインジェクション防御
〇特権昇格の防御
〇シェルコード/ペイロード攻撃の防御

## スクリプト制御



〇不正なパワーシェルと
　アクティブスクリプトの制御
〇危険なVBAマクロを制御
〇ファイルを残さない攻撃の阻止
〇危険なドキュメントファイルの制御

## アプリケーション制御



〇機器で利用する機能を限定して利用
　・バイナリを制御
〇不正なバイナリの実行を阻止
〇任意のバイナリ変更を防止
〇Windowsの変更は許可

# CylancePROTECT 製品の位置づけ

**静的解析**

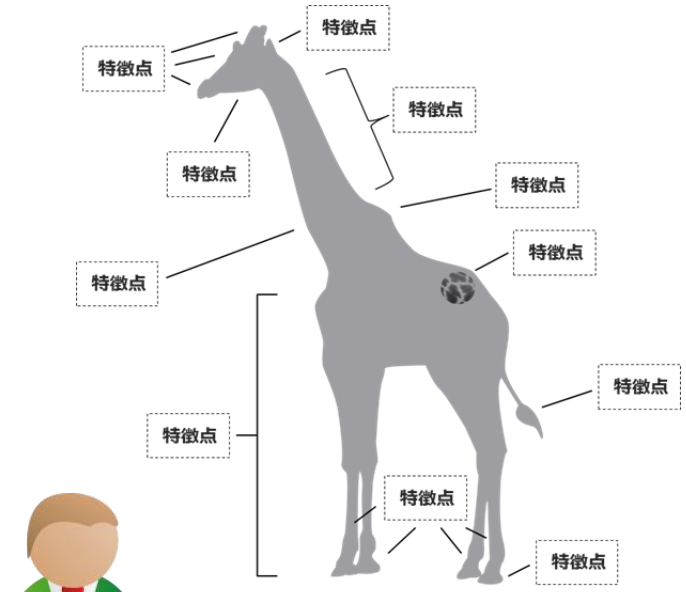
マルウェアの実行前に検知、防御
従来のパターンマッチング手法では限界

**動的解析**

マルウェア実行後の挙動等により検知、防御
静的解析と比べて安全性が劣る
動的解析環境をすり抜けるマルウェアの増加

# ファイルの特徴点（構造）を解析

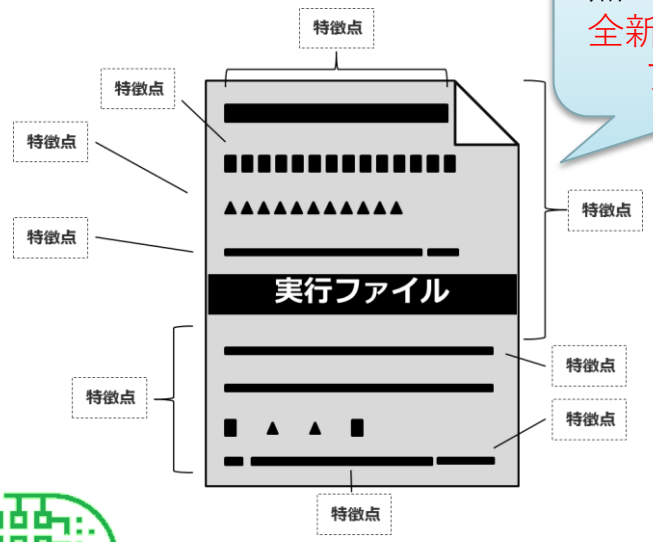
全ての特徴点が**完全一致しなくても**
**複数の特徴点**から**総合的に判断**




多数の特徴点から総合的に判断

⇒ **キリン** と断定

既存のものと特徴点が全く異なる完全新種のマルウェアは少ない




マルウェアに見られる特徴点を
（数値データ化して）総合的に判断

⇒ **マルウェア** と断定

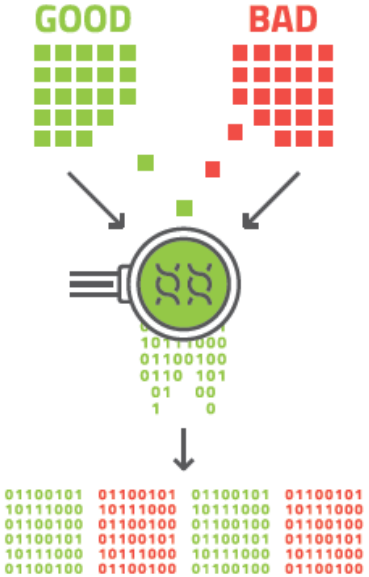
# Cylance AIによる学習の仕組み

## 収集と学習

良いファイル、悪いファイルから機械学習を行う
※**累計4兆のファイルを学習済み**


## 特徴抽出・数値化

教師データの特徴点を抽出（１ファイルあたり**最大６００万点の特徴点**）、各ファイルのマルウェアらしさを数値化




## 数理モデル作成

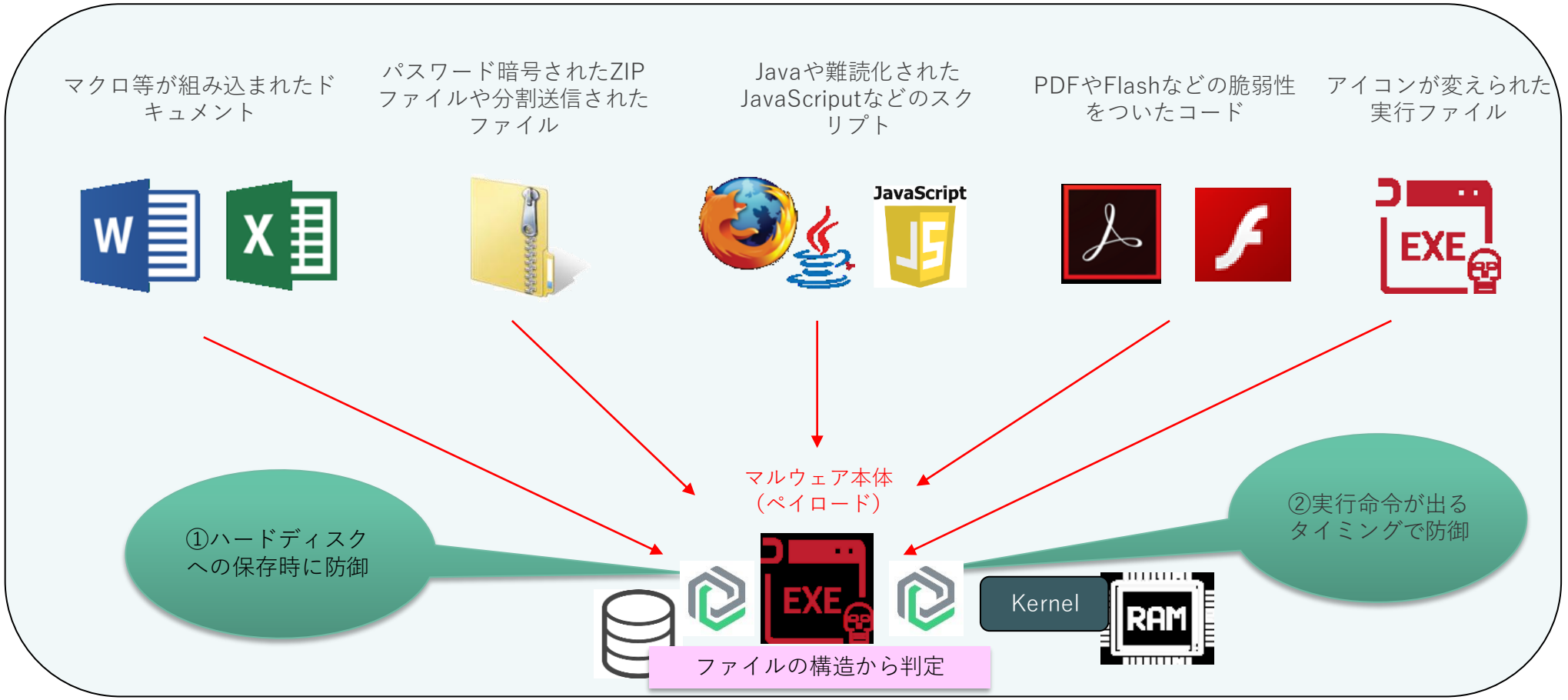
数学者やアナリストのチューニング後、膨大なノウハウを反映した数理モデルを作成。**端末上は数理モデルのみ稼動**
数理モデルは８ヶ月程度で更新

特徴点の一例

- *ファイルサイズ*
- *アイコン*
- *ファイルヘッダ*
- *セクションヘッダ*
- *セクションデータ*
- *文字列　,etc.*

# マルウェア検知のタイミング

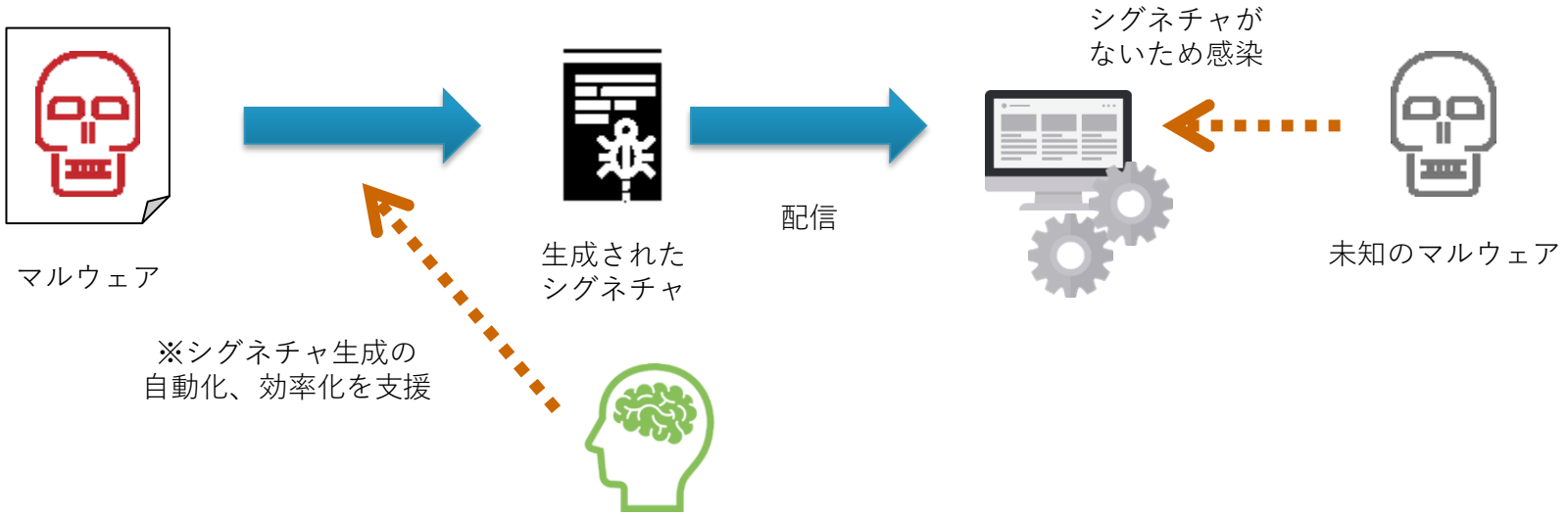
以下のタイミングでCylancePROTECTによる検知、防御が行われる
①マルウェアがハードディスクに保存されるタイミング
②マルウェアが実行される直前（カーネルから実行命令が出るタイミングでフック）




※検知対象は実行形式のファイル

# 他社AI対応製品との違い

■他社AI対応製品（人間の作業を補助する一機能）




※機械学習を一部の作業の自動化、効率化に使用しており、検知技術はあくまでシグネチャがベース

**未知のマルウェア認知後、対策までの時間を短縮**
**シグネチャが初めから存在しているわけではないためマルウェア感染のリスクは残存**

# Cylance AI データモデルにおけるアドバンテージ

一部のメーカーでは人工知能が作成したデータモデルによる
静的解析という Cylance と同じアプローチを導入してきている
しかし、以下のように内容に大きな違いあり

## Cylance AIによるデータモデル

・ディープラーニングを含む高度なアルゴリズム
・10億を超える大量のデータセット（教師データ）
・優れたデータサイエンティスト（数学者）
・データモデル生成に使われる特徴点：最大600万

**マルウェア検知率99.7% / 誤検知率0.002%**

Cylance AIのアドバンテージ
・5年間の開発先行期間
・優秀なデータサイエンティスト
・特許出願中の技術

## 他社AI製品によるデータモデル

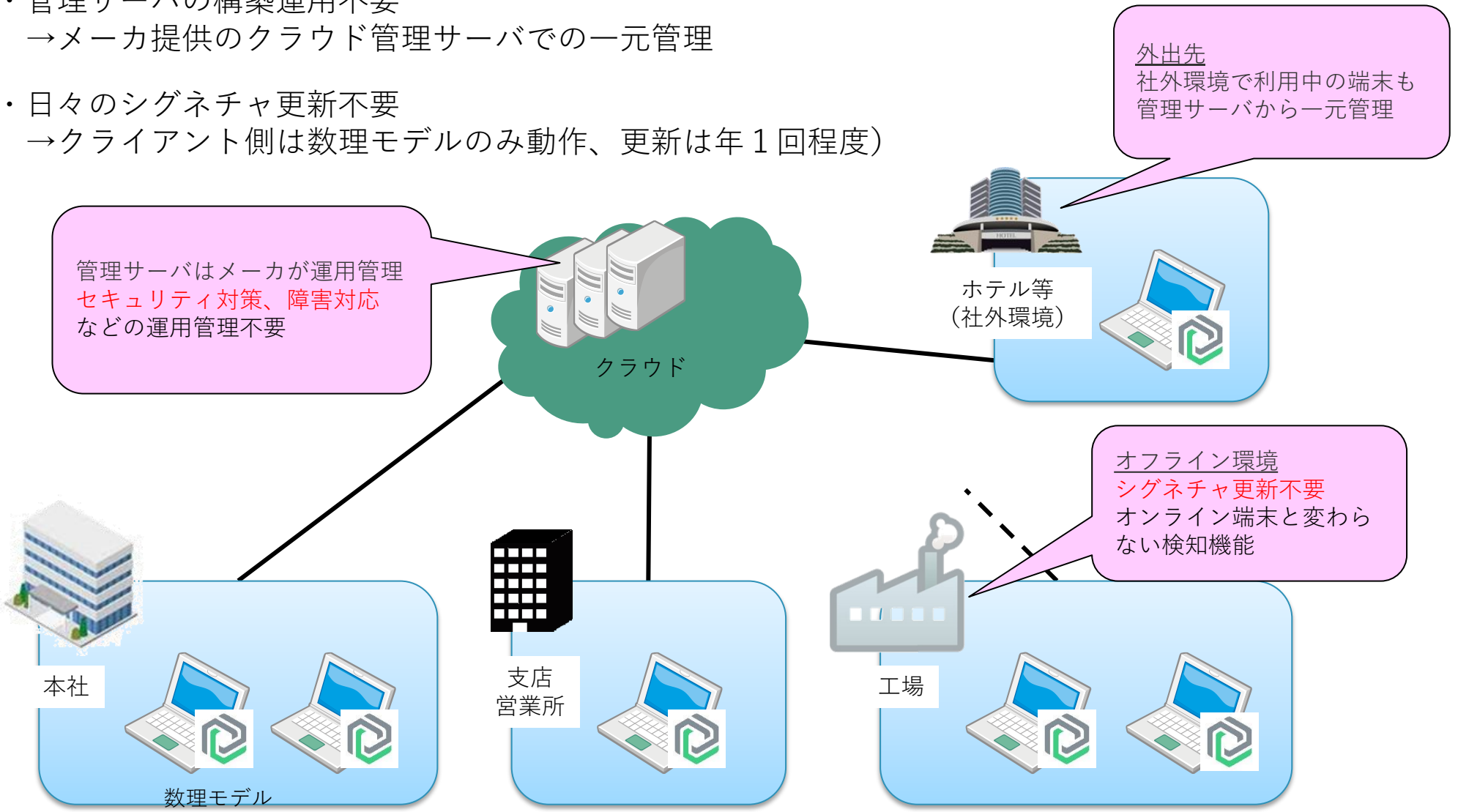
・オープンソースを流用した簡易なアルゴリズム
・偏りがある少量のデータセット（マルウェア中心）
・データサイエンティストがいない
・データモデル生成に使われる特徴点：70-150

**マルウェア検知率60-70% / 誤検知率5-10%**

# 管理サーバ、シグネチャアップデート不要

・管理サーバの構築運用不要
　→メーカ提供のクラウド管理サーバでの一元管理

・日々のシグネチャ更新不要
　→クライアント側は数理モデルのみ動作、更新は年１回程度）



# オンプレミス管理サーバ機能（CylanceHYBRID）

端末が直接インターネットに接続することが許可されていない環境
クラウド管理サーバに代理でアクセスする機能を提供
端末が直接接続する場合と同等の機能を提供

特徴

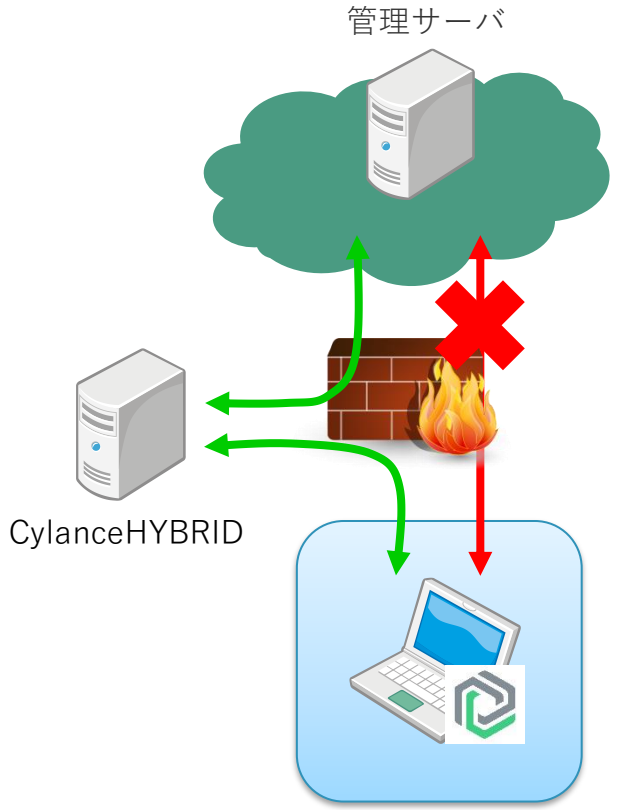
・端末のプロキシとして動作

・デバイス、ポリシ等の管理はクラウド管理サーバ
※管理者用にクラウド管理サーバへ接続可能な端末
（最低1台）の準備が必要

〇さまざまなHypervisor上で稼働可能

〇接続可能な端末数は1台あたり最大10,000台まで

〇無償オプション（ライセンス費用に含む）

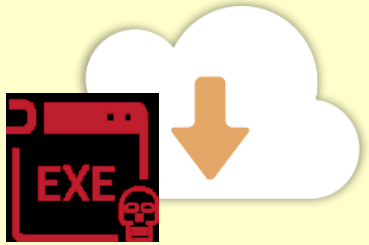


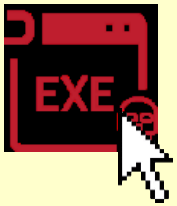
# エンドポイント端末環境

常駐時の負荷が低く、必要最小限の場面での検知
シグネチャ更新等の日々の運用管理不要

- **インストール直後**のみフルスキャン実行
  定期的なフルスキャン不要
- ファイルの**ダウンロード時と実行時**のみ検知
- CPU使用率　１～２％
- メモリ消費　４０～６０MB
- 毎日の**シグネチャ更新不要**
- サーバ環境、仮想環境に対応

**ダウンロード時**　　**実行直前**



# システム要件

最新情報はメーカサイト（https://docs.blackberry.com/en/unified-endpoint-security/blackberry-ues/setup/setup/UES-requirements/Software-requirements-Protect-Desktop ）をご参照ください。

## オペレーティングシステム:

Windows 7
Windows 8.1
Windows 10
Windows 11
Windows Server 2012, R2 (Standard, Data Center, Essentials, Server Core, Embedded & Foundation)
Windows Server 2016 (Standard, Data Center, Essentials, Server Core)
Windows Server 2019 (Standard, Data Center & Server Core)
Windows Server 2022 (Standard, Data Center & Server Core)

Legacy OS
Windows XP SP3
Windows Vista
Windows 8
Windows Sever 2003, SP2, R2
Windows Sever 2008, R2

macOS 12 (Monterey)
macOS 11 (Big Sur)
macOS 10.15 (Catalina)
macOS 10.14 (Mojave)
*MAC版エージェントは一部機能に対応しておりません

Ubuntu 18.04, 20.04, 20.04LTS
SUSE Linux Enterprise Server 12 SP5, 15
Red Hat/CentOS 7.8, 7.9, 8.3, 8.4, 8.5
Red Hat Enterprise Linux 8.6
Oracle Linux Server UEK 6, 6, UEK 7, UEK 8, 8
Debian 10, 11
Amazon Linux 2

## システム要件：

| | |
|---|---|
| クライアント端末搭載メモリ | 2GB以上<br>※常駐時の使用メモリーは約50MB程度 |
| 空きディスク容量 | 600MB以上<br>※Quarantine（隔離）に必要な容量は含みません |
| インターネットブラウザ | ・Microsoft Edge　最新バージョン<br>・Internet Explorer　10 / 11<br>・Firefox　最新バージョン<br>・Google Chrome　最新バージョン<br>※製品登録時インターネット接続が必要です。 |
| その他要件 | ・クライアントのAdmin権限(インストール時)<br>・.NET Framework4.6.2 以降<br>※Windows版のみ必要 “.NET Frame Work4.0”以降を推奨 |

## 制限・留意事項：

- マイクロソフト社サポート終了製品に関して不具合発生時の調査に責任を負えません。
- 他社製アンチウィルス製品と併用する場合特定フォルダを除外頂くなどの対処が必要となります。
- 他社製メモリ監視製品とメモリ防御機能との併用はできません。
- 導入前に事前の動作検証を推奨致します。

# ランサムウェア感染事例

**day1**
- 社内サーバがランサムウェアに感染した疑いがあり クラウド上のサーバの確認依頼
- クラウド上のサーバにおいて感染を確認し、お客様の依頼に基づき、バックアップからリストア

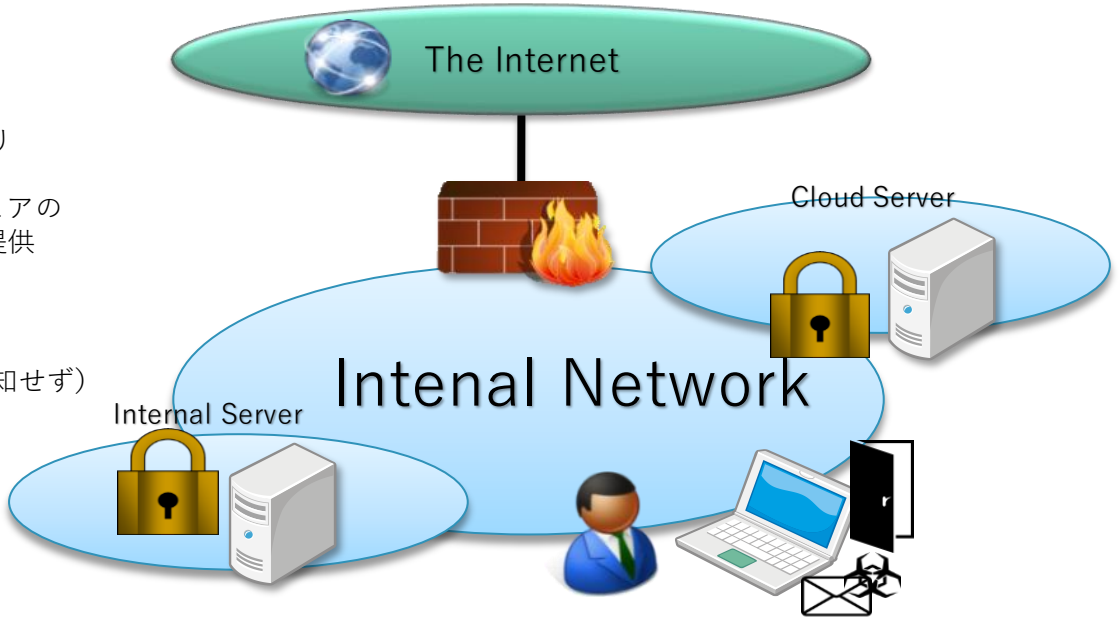
**day4**
- 全てのWindowsサーバがランサムウェアに感染しており 対応の支援依頼を受け打ち合わせに参加
- 既存のウィルス対策ソフトでは、検知できないマルウェアの疑いがあり、NGAV製品を紹介し、緊急で評価環境を提供
- 復旧用のクラウドサーバを提供

**day5**
- 該当のサーバで、マルウェアを検知（既存のAVでは検知せず）
- 全台約500台に導入を決定

**day7**
- 全台に展開を開始

**day14**
- 安全確認後メールサーバ稼動

**day21**
- 全サーバ中約半数のサーバ復旧
  ※残りのサーバについては復旧の目処たたず




ウィルス対策ソフト：某社ウィルス対策ソフト導入済み
メールセキュリティ：メールセキュリティサービス利用
UTM　　：導入済み
パッチマネジメント：WSUSあり（サーバは自動更新なし）

# ランサムウェア感染事例

**どんなランサムウェア**

- Clop Ransomeware
  2019/2/10 に検出されたランサムウェア、暗号化ファイルの拡張子として「.clop」を追加
- 正規な署名がされており、検出が困難
- NGAVが検出した時点で、VirusTotal では、ファイル情報なし

**対策状況はどうだったの**

- Virus対策ソフトは導入している。（毎日フルスキャンも）　・・・・　でも感染しました
- WSUSサーバ導入　・・・・　でもサーバについては自動更新してません。。。
- UTMを導入　・・・・　UTMによっては署名つきのファイルは検査しないので、検知は難しい。。。

**進入経路は**

- 1 台のPCで怪しい添付ファイルをクリックしたとの報告が情報システムに
- Virus対策ソフトで最新のパターンファイルにアップデートし、フルスキャンをかけたが、何も検知しなかったため、異常なしと判断しネットワークにそのまま接続。
  UTMでは許可ポリシーのログをとってなかったため、経路の特定は困難。。。。

**影響は？**

- 2 週間経過時点において、全サーバのうち約半数が復旧、残りは復旧の目処たたず。。。
  大半のサーバは再構築。。。
- 取引先からの、原因究明および情報漏えいの有無の報告依頼あり
  詳細な侵害調査（フォレンジック）をすると、10,000千円程度かかる可能性が。。。
- 信用失墜。。。

# 運用サポート（1/2）

■運用代行

管理コンソールの利用方法等，一般的な問い合わせに対応します。

管理コンソール上より以下の作業をお客様に代わり実施します。

・検知した脅威のホワイトリストへの登録

・ポリシーの設定変更

※作業はお客様の依頼内容に基づき実施します。

・問い合わせ方法：メール，電話

・対応時間　　：（平日）９：００～１７：００

以下のようなソフトウェアは脅威として検知される可能性があります。
過検知ではなく、セキュリティ上の脅威ファイルと判定される要素を保有しているためです。
業務利用の有無等を基準にして、利用するソフトウェアはホワイトリストに登録する必要があります。
例）・端末情報を収集しサーバへ送信するソフト
・リモートコントロールソフト
・自社開発ソフト、製造元が不明なソフト、等

# 運用サポート（2/2）

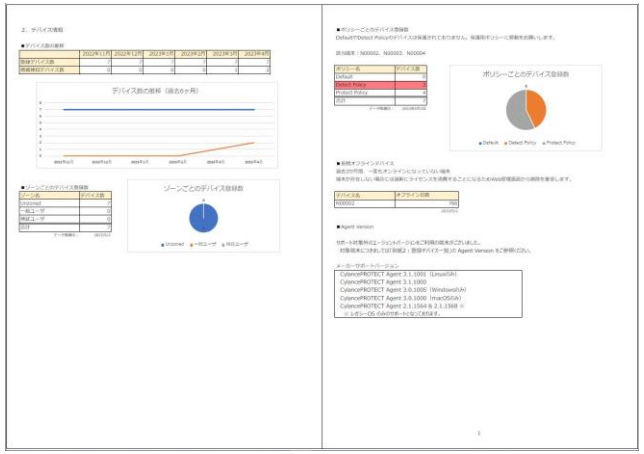
■解析サポート（オプション）

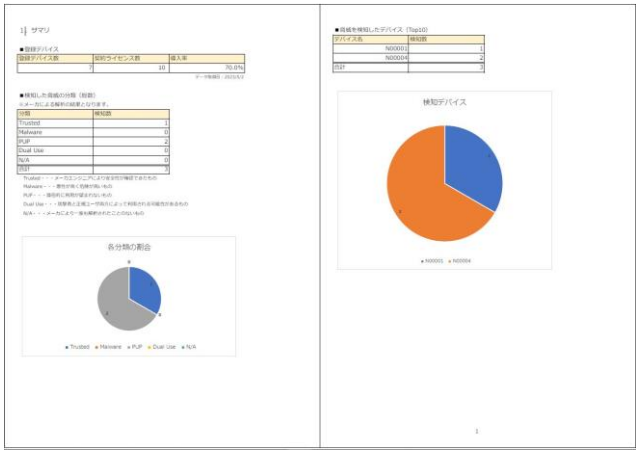
検知した脅威の解析やその対処について、お問い合わせに対応します。

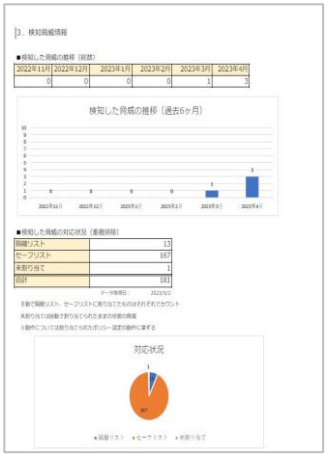
４半期に１回、以下の内容をレポートとして作成しご提出します。

・検知した脅威の総数，詳細

・ＱＡ対応，運用代行作業の履歴







# 導入までの流れ

全てのSTEPにおいて費用内での支援を実施

■STEP1

事前検証用端末を数台準備して検知モードにてエージェント導入

※業務利用する実行ファイルがカバーできる範囲の端末選定が望ましい

■STEP2

エージェント導入した端末において検知した脅威の判定業務上、

利用が必要なものはホワイトリストへの登録

■STEP3

検知モードからブロックモードへとポリシー変更した後に,

全ての端末へのエージェント展開