イグアスお薦めソリューション
2023年2月号

■お薦めソリューション2月号ラインアップ■

サイバーセキュリティー・監視ソリューション特集！

- サイバーセキュリティートレンド
  ゼロトラストとは
  サイバーセキュリティー対策マップ
- Deep Instinct (情報技術開発株式会社)
- GMOトラストログイン (GMOグローバルサイン株式会社)
- DataClasys (株式会社DataClasys)
- DDHBOX (デジタルデータソリューション株式会社)
- Pathfinder Apollo (三和コムテック株式会社)
- コンプライアンスチェックサービス (三和コムテック株式会社)

【お知らせ】

- イグアスRPG研修【2月】
- ウェビナー開催「未知への脅威の対策とデータ復旧のための最後の砦」

株式会社イグアス　ソリューション営業部

サイバーセキュリティートレンド

ゼロトラストとは

- IPAの調査によると近年企業へのサイバー攻撃はランサムウェア、標的型攻撃、サプライチェーン、テレワーク等ニューノーマルな働き方をターゲットにした攻撃が増加。これまでの境界型セキュリティー対策では対応が不十分となってきている。こうしたことから、**すべての通信を信頼しないことを前提とした「ゼロトラスト」の考え方が重要となっている**

- 一方で外部からの攻撃だけでなく、企業組織内部からの不正な、または不注意による情報漏洩も大きな課題となっている。セキュリティ対策としてはこれらも十分な対応が迫られる

前年順位	個人	順位	組織	前年順位
1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
2位	ネット上の誹謗・中傷・デマ	**2位**	サプライチェーンの弱点を悪用した攻撃	3位
3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**	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	**4位**	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	**5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	4位
7位	不正アプリによる スマートフォン利用者への被害	**6位**	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	**7位**	ビジネスメール詐欺による金銭被害	8位
8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**	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの 不正ログイン	**9位**	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の 不当請求による金銭被害	**10位**	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

サイバーセキュリティー対策マップ

サイバーセキュリティー対策には、

問題発生そのものを抑制・防止する
「予防対策」、
いち早く問題を検知するための
「発見対策」、
万一事故が発生した場合の
被害拡大を抑えるための
「事後対策」がある

つまり・・・

外部脅威と内部脅威へのセキュリティー対策ツールをバランスよく導入することで会社の情報資産と信用を守る

サイバーセキュリティー対策マップ

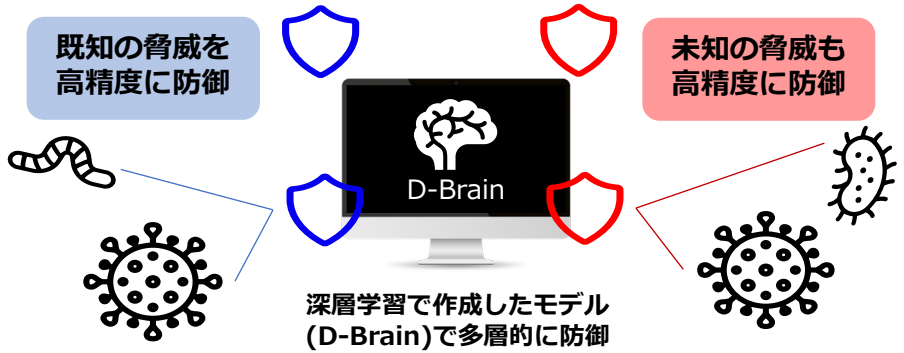
Deep Instinct

世界初！ディープラーニング（深層学習）を活用したエンドポイントセキュリティ製品

Deep Instinctは、世界で初めてディープラーニング（深層学習）を活用した
エンドポイントセキュリティ製品として、既知の脅威だけではなく、
未知の脅威も99%以上の高い検知率で予防することができます。

tdi 情報技術開発株式会社

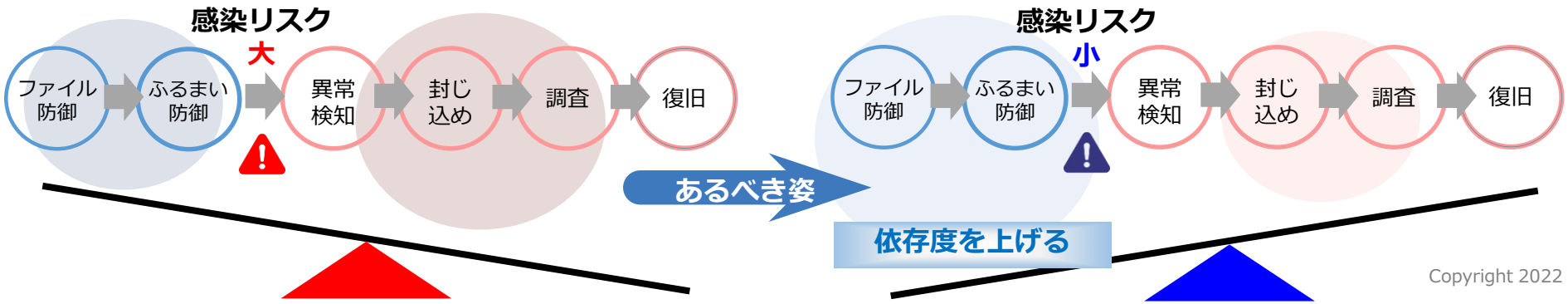
新種や亜種など、
未知の脅威も
99%以上の検知率で
実行前に防御



Deep Instinctは、日々新しくなる
マルウェアをはるか前から予測し、
初見でブロックして感染を予防しています

理想のエンドポイントセキュリティ対策

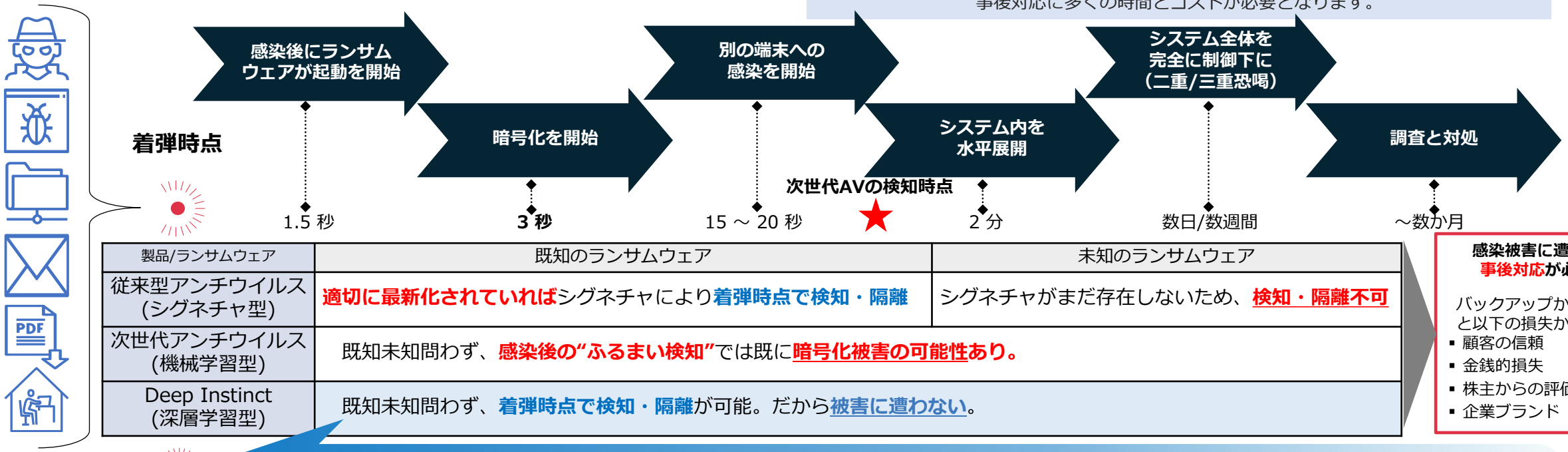
感染予防対策の依存度を上げ感染リスクを極小化し、感染事後対策の依存度を下げて
セキュリティ投資コストを最適化をするのが、本来あるべき姿です。
Deep Instinctなら深層学習による高精度な予防により、これを実現できます。



Deep Instinct

ランサムウェアの被害スピードと予防対策

昨今のランサムウェアは着弾してからわずかな時間で暗号化が開始されるため、
感染に気付いた時にはすでに被害が拡大していることも多々あり、
事後対応に多くの時間とコストが必要となります。



製品/ランサムウェア	既知のランサムウェア	未知のランサムウェア
従来型アンチウイルス(シグネチャ型)	**適切に最新化されていれば**シグネチャにより**着弾時点で検知・隔離**	シグネチャがまだ存在しないため、**検知・隔離不可**
次世代アンチウイルス(機械学習型)	既知未知問わず、**感染後の"ふるまい検知"**では既に**暗号化被害の可能性あり。**	
Deep Instinct(深層学習型)	既知未知問わず、**着弾時点で検知・隔離**が可能。だから**被害に遭わない**。	

感染被害に遭うと事後対応が必須

バックアップから復元と以下の損失から回復
- 顧客の信頼
- 金銭的損失
- 株主からの評価
- 企業ブランド

deepinstinct シフトレフト

Deep Instinctの特徴

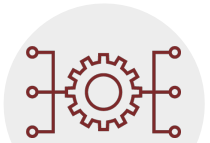
① **高精度な予測**　未知の脅威に対する検知率が非常に高く、誤検知率は低い
② **どんなファイルも検出可能**　PE以外にもPDFやOffice、RTF、SWFなど数多くのファイルに対応
③ **幅広いOSに対応**　Windows、MacOS、Android、Chrome OS、iOS、Linuxに対応
④ **毎日のシグネチャ更新不要**　モデル更新は1年に2回程度のため運用管理工数を大幅削減
⑤ **エージェントが軽い**　メモリー消費が小さく(150MB以下)、CPUの使用量も1%未満
⑥ **インターネット接続に依存しない**　デバイス上を完全自立型で動作するため、オフライン時でもセキュアな状態を維持

GMOトラストログイン

**システム・働き方も
多様化し、日々
変化するITサービスを
どうやって管理する？**

**進む
クラウドへの移行**

クラウド利用による
情報漏洩リスクの増大



**利用する
システム/サービスの増加**

システム増加による
従業員の利便性低下

**働く場所や
デバイスの多様化**

企業にとっての安全性と
従業員にとって利便性の両立

GMOトラスト・ログインで
いつでも、どこからでもセキュアに利用できる業務環境へ！

**簡単最速の
シングルサインオン/
アクセス制限ソリューション**

GMOトラスト・ログイン

**情報セキュリティ
の強化**

**認証局として培った
ノウハウと技術による
情報漏洩を防ぐ堅牢性**

**システム/サービスが
増えても利便性を損なわない**

**シングルサインオンと
パスワードレスで
業務効率＆集中力UP中**

**いつでもどこでも
働ける環境の提供**

**IPアドレス制限で
どこからでも
セキュアな環境が実現**

GMOトラスト・ログインイメージ

オフィスで

自宅で

外出先で

GMOトラスト・ログイン

不正アクセス防止 IPアドレス制限 多要素認証	ID管理 シングルサインオン パスワードレスログイン

box　slack

Google Workspace　Microsoft

Dropbox　sansan

Chatwork　cybozu

... and more

いつでもどこでも、どこへでもセキュアなアクセスを実現
6,100以上のサービスとシングルサインオン連携済

社内システムの導入経験がない。不安。

任せて安心の導入アドバイスサービスもございます！
イグアスがお客様の環境への導入支援をいたします。

価格例

1ユーザー300円/1ID/月（30ユーザー様以上から）
導入アドバイスサービス 300,000円～

DataClasys

ファイル形式を問わず、3D-CADを含むあらゆるデータを暗号化保護できる、“国産”のファイル暗号化（DRM/IRM）ソリューション

＜強固なセキュリティと利便性の両立＞

①ファイルにアクセスする際はサーバ側での認証が必須

正規の権限を持つユーザのみ鍵が配信されます。
権限のない第三者には暗号化ファイルを開くことができません。

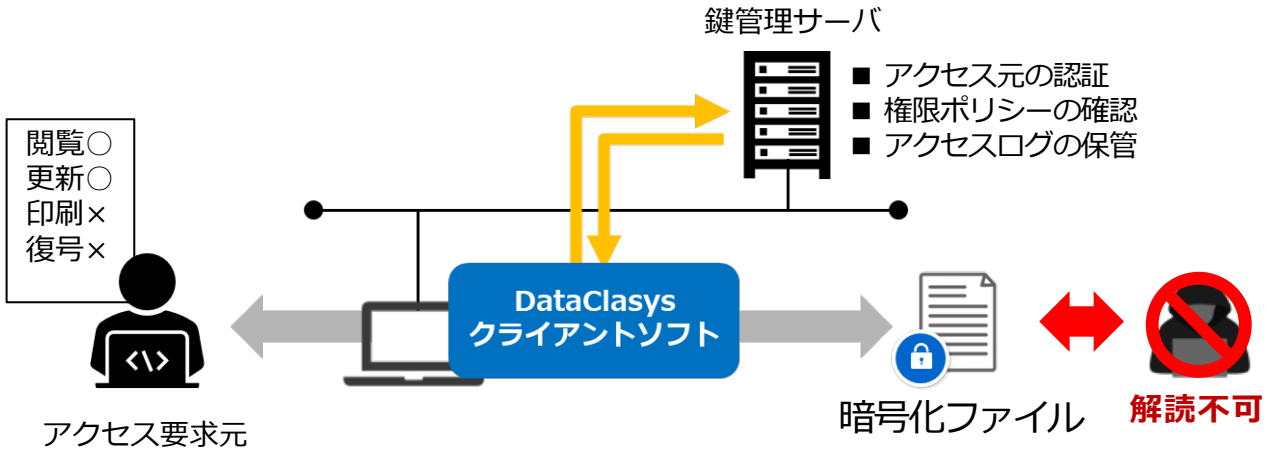
②ファイル単位での利用権限を制御することが可能

そのユーザに必要な最小限の権限でファイルを利用させることができます。
（閲覧・更新・印刷・コピペ・スクショなど...）

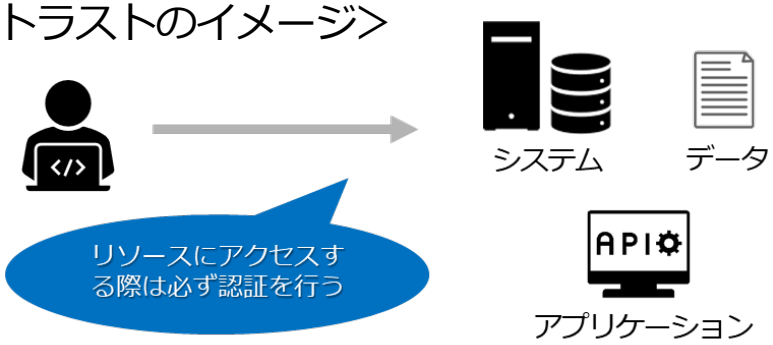
③暗号化・復号を意識せず利用できるため利便性を損なわない

パスワード暗号化とは異なり、 DataClasysが起動状態であれば、
通常のファイルを同じくダブルクリックだけでファイルを開きます。

＜認証の仕組み＞



＜ゼロトラストのイメージ＞



DataClasys

★ DataClasysで実現できること

① ファイル単位で暗号化し、暗号化したままファイルを利用

② 閲覧・更新などファイル利用権限の設定

③ ファイル利用期限の設定　　etc

★ DataClasysの特徴

① 3D CAD含め **すべてのファイルを暗号化** できる（動画やAccessなど大容量のファイルも！）

② フォルダ保存やファイル新規作成の際に **自動暗号化** されるため、利便性がよい

③ 暗号化しても **拡張子やアイコンが変わらない** ため、ファイルパスが変わってしまう心配もない

★ DataClasysで対策できるセキュリティリスク

① **ランサムウェア** を含む高度なサイバー攻撃による機密情報窃取・リークのリスク

② 転職・退職者など、関係者による機密情報持ち出し（ **内部不正** ）のリスク

③ **PCやUSBメモリーの紛失** など不注意による漏洩のリスク　　etc

標準価格：30ユーザー　200万円～　※基本導入サービス付き

DDHBOX

セキュリティー対策は感染しても外に出さない
「出口対策」が重要です

<DDHBOX 3つの特長>

①**不正通信の検知・遮断・通知が全て自動**
難しい運用の必要も無しで**ゼロ情シスでも安心**

②**低コストで出口対策**を実現
企業・官公庁などでの実績のある有人監視サービスの結果から生成される**不正サーバリストを毎日更新**

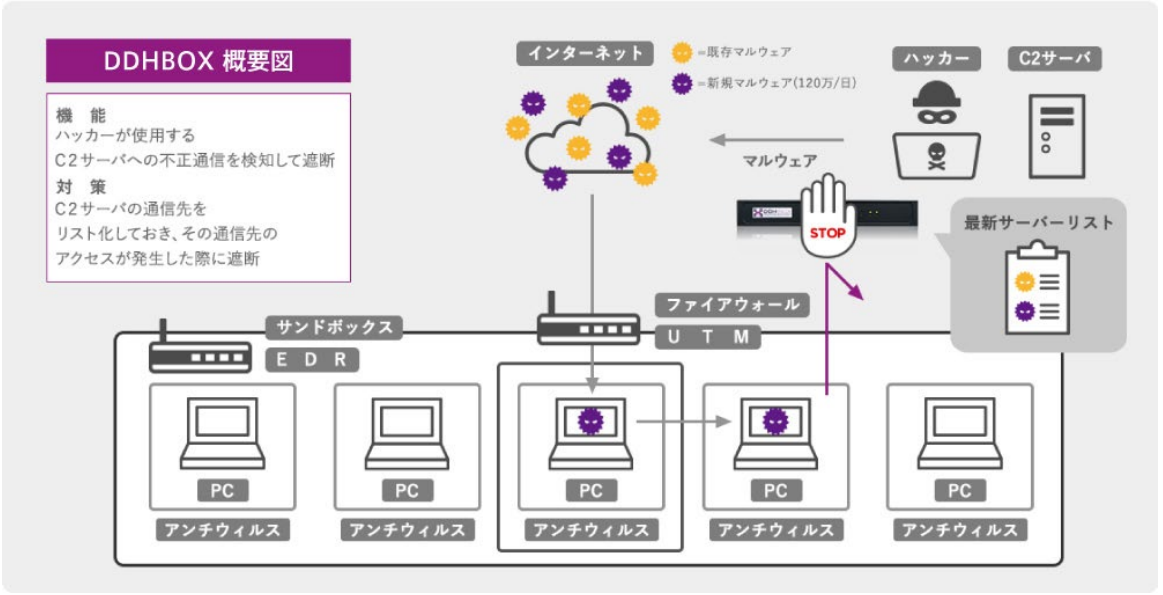
③不正通信を検知・遮断した場合は
調査・対策の費用に保険適用可能(年間300万円まで)

＜DDHBOX が採用される理由＞

①**不正サーバリストが24時間ごとに更新**されるため
日々、攻撃者の技術が上がっている攻撃者と脅威の対策
導入後も継続してセキュアな環境を構築できる

②**付帯のサイバー保険**で、侵入に利用された経路や
フォレンジック調査で安心のアフター体制

月額数万円で導入可能※



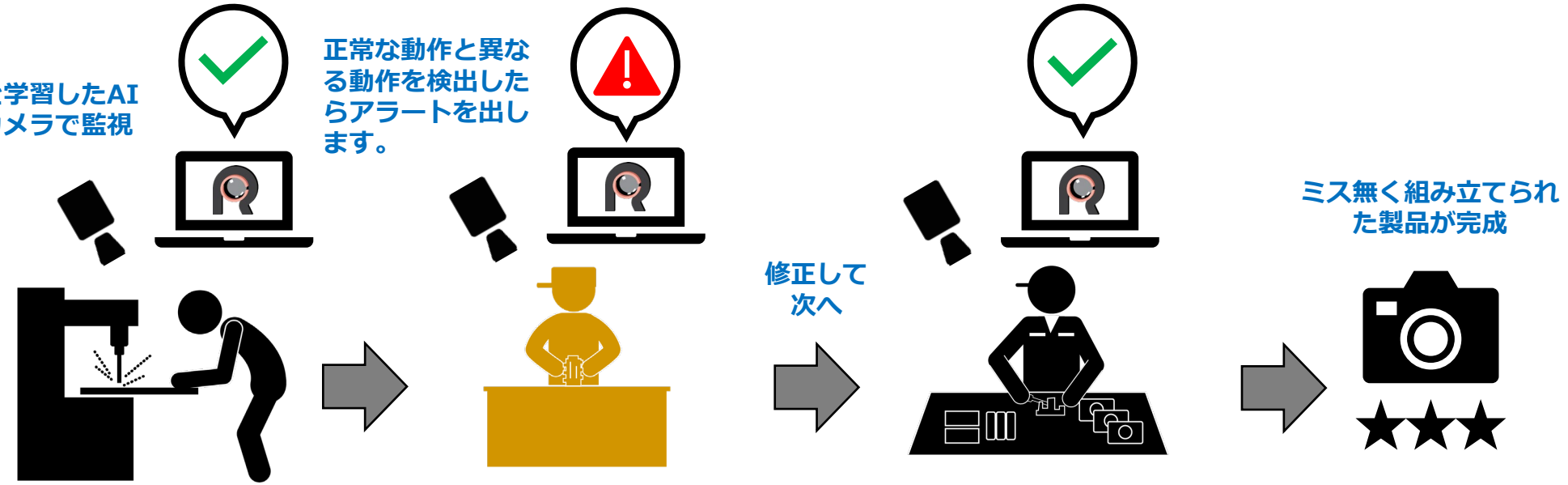
※機器本体は除く

Pathfinder Apollo (パスファインダー・アポロ)

ヒューマンエラーは”AIの目”が見逃さない！

『Retrocausal Pathfinder Apollo』は機械学習を使用して、作業の映像から現場に合わせた監視モデルを作成します。

エラー発生時にその場でアラートを出すことで、**不良品の発生と流通を製造現場から防ぎます。**



Pathfinder Apolloの導入により…

生産性10%向上！

製品不良
60%減少！44%削減！

研修期間

Pathfinder Apollo (パスファインダー・アポロ)

導入例

大型機械の組立・保守

作業領域が広く専用工具を使用したり三次元的な動作を行う場面も監視が可能
自動車のような大型機械のパーツの組み立てや最終組付け工程など幅広い現場でフレキシブルに活躍

精密電子機器の製造

小さなミスが深刻なトラブルにつながる製造現場で部品の組み忘れや工程でのミスを監視して通知
作業員の異動や習熟度に関わらず安定した品質での製造をサポート

メディカルトレーニング

ベテラン医師の施術手順を映像に記録し、確実な医療技術の継承に応用可能
映像による手順の確認やリアルタイムでの手順監視機能が医療技術者のスキルアップや施術の正確性に貢献

構成

インターネット接続

ソフトウェアのダウンロードや
ポータルを使用したタスク/マシン管理のため
インターネット環境が必要です

ゲーミングPC

リアルタイムの映像解析を行うことから、
グラフィックボード搭載の
ゲーミングPC推奨

USBカメラ(広角レンズ推奨)

映像の録画や、作業の監視に使用します

価格：
月額7万円（税別）/1ワークステーションあたりの利用料金
※PC・カメラ・導入支援・
教育費用は別途

コンプライアンスチェックサービス

反社会勢力データベースの利用環境とRPA：AutoMateによる自動チェック機能を提供

反社会勢力との取引は企業存続の危機を招きます

■直接被害
・詐欺被害
・トラブル（詐欺・不当要求）
・行政処分、指名停止
・上場廃止
・融資停止

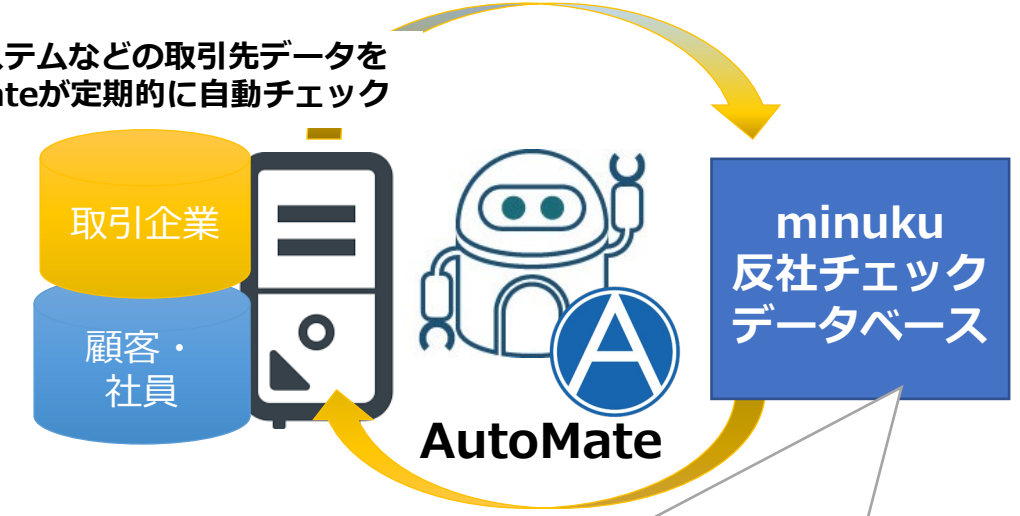
■間接被害
・信用失墜
・顧客、取引先との取引停止
・株価下落
・ネット、SNSでの炎上
・風評被害

コンプライアンス・反社チェック業務の課題

- 取引先のチェックは大変・・・
- 情報源をどうするか・・・
- 手間とコストを削減したい・・・

AutoMate コンプライアンスサービスは、煩雑な反社チェック業務を自動化します

業務システムなどの取引先データを AutoMateが定期的に自動チェック



当サービスのデータベースは、
以下の情報をクローラーにより常に収集しています。
・1,000以上のメディア、Webサイト
（新聞社、TV局、他）
・全国自治体の公表情報
・中央省庁の公表情報
・警察庁の公表情報
・独自情報
※必要に応じて登記簿取得を実施

AutoMateコンプライアンスチェックサービス

価格表：

初期費用
100,000円

＋

	ミニマムプラン	ライトプラン	スタンダードプラン	プレミアムプラン
月額料金	10,000円	30,000円	50,000円	70,000円
上限件数	30件(333円/件)	100件(300円/件)	300件(166円/件)	無制限
オプション(別料金)				
超過金額	400円/件	300円/件	200円/件	-
API連携	非対応（Webブラウザによるデータ入力のみ）			20,000円/月

※全て税別

いずれのプランでもAutoMateによる自動処理が可能です。
サービス開始時に反社チェックデータベースへの接続タスクを提供します。
※ミニマムプラン、ライトプラン、スタンダードプランはWebブラウザ経由の処理タスク、
　プレミアムプランはWebブラウザ、API両方の処理タスクをご提供

【お知らせ】イグアスRPG研修サービス

IBM i エンジニア育成、DX時代の学び直しに
イグアスRPG研修サービスをご用意しました

このようなお客様にお薦め

- 若手エンジニアがRPGⅣを習得できる環境がない
- IBM iの学び直しに
- 現状RPGⅢの利用割合が高くRPGⅣを学びたい
- お客様にサーバー更新の際のご提案として

プログラム内容

プログラム１日目：IBM i 基本操作
5250エミュレータの基本操作
主要コマンドの説明
プログラム２日目：RPG基礎知識（１）
物理ファイル、論理ファイルの解説・作成
データ・ファイル・ユーティリティーの実習
QUERYユーティリティーの実習
プログラム３日目：RPG基礎知識（２）
RPGⅢ、RPGⅣ、FFRPG の違いとメリット・デメリット
RPGⅣの基本コーディング

IBM i
RPG

■研修コース
IBM i 基本操作/RPG基礎知識研修（3日間）定員10名（最低6名様～）

費用：15万円/人　※2名様目から10万円/人
研修場所：株式会社イグアス（川崎本社）
実施日：2023年2月8日、2月15日、2月22日（3日間）
※講師はソリューション・ラボ・ジャパン株式会社様より派遣

■Webセミナー「未知への脅威の対策とデータ復旧のための最後の砦」開催のお知らせ■

【開催概要】

日時　　：2023年2月21日（火）14:00～15:00（受付開始　13:45～）
対象者　：ランサムウェア等のサイバー脅威への対策をご検討中の方
主催　　：情報技術開発株式会社　共催：株式会社イグアス

【プログラム】

1．サイバー攻撃の脅威トレンドと「Deep Instinct」によるエンドポイントセキュリティ強化
2．ランサムウェア対策でのエアギャップの重要性～システム復旧の最後の砦～

【お申込み】

下記ページの内容をご確認のうえ、お申し込みください。
https://tdi.smktg.jp/public/seminar/view/4184

各ソリューションの詳細は
イグアス ソリューションポータルまで

ソリューションポータル
https://www.iguazu-sol.jp/recommend

■お問い合わせ■
株式会社イグアス
ソリューション営業部
sol_sup@i-guazu.co.jp