イグアス お薦めソリューション

2023年 9月号

セキュリティ・ソリューション特集！

- DeTCT Starter　外部脅威情勢管理プラットフォーム
- Jamf Pro　Appleデバイス管理のデファクトスタンダード
- GUARDIANWALL　脱PPAP情報漏えい対策の決定版
- Deep Instinct　世界初！深層学習を活用したエンドポイントセキュリティ

その他

- mitoco+GPT　Salesforceと連携する最適グループウェア
- MOTTA GREEN FORK　電動フォークリフトのバッテリーソリューション

株式会社イグアス　ソリューション営業部

IPA 「情報セキュリティ10大脅威 2023 」

組織におけるセキュリティ被害、3年連続ランサムウェアが1位を更新中！

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 不正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

圏外：昨年はランクインしなかった脅威

「情報セキュリティ10大脅威 2023」は、2022年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

出展サイト：情報セキュリティ10大脅威 2023 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

サイバーハイジーン（衛生管理）という考え方

ランサムウェア直近の被害状況

- 2023年1月、米国のパイプライン会社であるColonial Pipelineがランサムウェア攻撃を受け、同社のネットワークが一時的に停止しました。攻撃者は、DarkSideという名前のランサムウェアグループであり、同社に445万ドル相当のビットコインを支払うよう要求。同社は身代金を支払ったものの、復旧には時間がかかり米国東海岸の燃料供給に大きな影響を及ぼした。
- 2023年2月、ニュージーランドの最大の健康保険会社であるAccuro Health Insuranceがランサムウェア攻撃を受け、顧客の個人情報が流出した可能性がありました。攻撃者はREvilという名前のランサムウェアグループであり、同社に200万ドル相当のビットコインを支払うよう要求。同社は身代金を支払わないと発表し、警察やセキュリティ専門家と協力して事件を調査しました。
- 2023年3月、日本の大手ゲーム会社がランサムウェア攻撃を受け、約35万人分の個人情報や企業情報が流出したことが判明。攻撃者は、Ragnar Lockerという名前のランサムウェアグループであり、同社に1100万ドル相当のビットコインを支払うよう要求しました。同社は身代金を支払わないと発表し、法的措置やセキュリティ強化に取り組みました。

サイバーハイジーンとは

2000年に「インターネットの父」として有名なヴィントン・グレイ・サーフ氏が提唱したサイバーハイジーン（衛生管理）は、社内のIT環境や社員のPC及びインターネット接続環境等を把握・セキュアな状態を可視化し、会社全体のセキュリティ意識を醸成し「リスクの軽減、予防」を目指す取り組みのことです。

サイバーハイジーン具体的な取り組み

データのバックアップ

定期的かつ複数の場所にデータをバックアップすることが重要です、大切なデータを定期的にバックアップしデータの損失に備えます。

ソフトウェアの更新

オペレーティングシステムやアプリケーションの定期的なソフトウェア更新、パッチ、セキュリティ勧告、
脅威情報などの新たな情報を取得・評価し、この情報に基づいて措置を講じることで、脆弱性を特定して修復し、攻撃チャンスを最小限に抑える。

メールの注意（フィッシング対策・マルウェア対策）

ランサムウェアは、メールに添付されたファイルやリンクを開くことで感染することが多いです。そのため、差出人や件名が怪しいメールは開かないようにしましょう。
フィッシング対策として：不審なメールやリンクをクリックしないことや不審な送信者からのメールやリンクに注意し、個人情報を提供しない。
マルウェア対策として：アンチウイルスソフトウェアのインストール: デバイスにアンチウイルスソフトウェアをインストールし、定期的なスキャンを実施します。
不明なファイルのダウンロードを避けること、信頼性のあるソースからのみファイルをダウンロードするようにすること。

サイバーセキュリティ意識の向上：（教育・啓発）

サイバーセキュリティに関する教育とトレーニング: サイバーセキュリティの基本を教育し注意を促します。
①多要素認証 (MFA) の使用:MFAを有効にして、アカウントへの不正アクセスを防ぎます。
②不正アクセスの監視:インターネットトラフィックやシステムログの監視を行い、不正アクティビティを検出します。
これらの取り組みを実施することで、個人と組織はオンライン環境でのセキュリティを向上させ、サイバー攻撃からのリスクを最小限に抑えることができます。
サイバーハイジーンは日常的な習慣として実践し、定期的に見直すことが重要です。

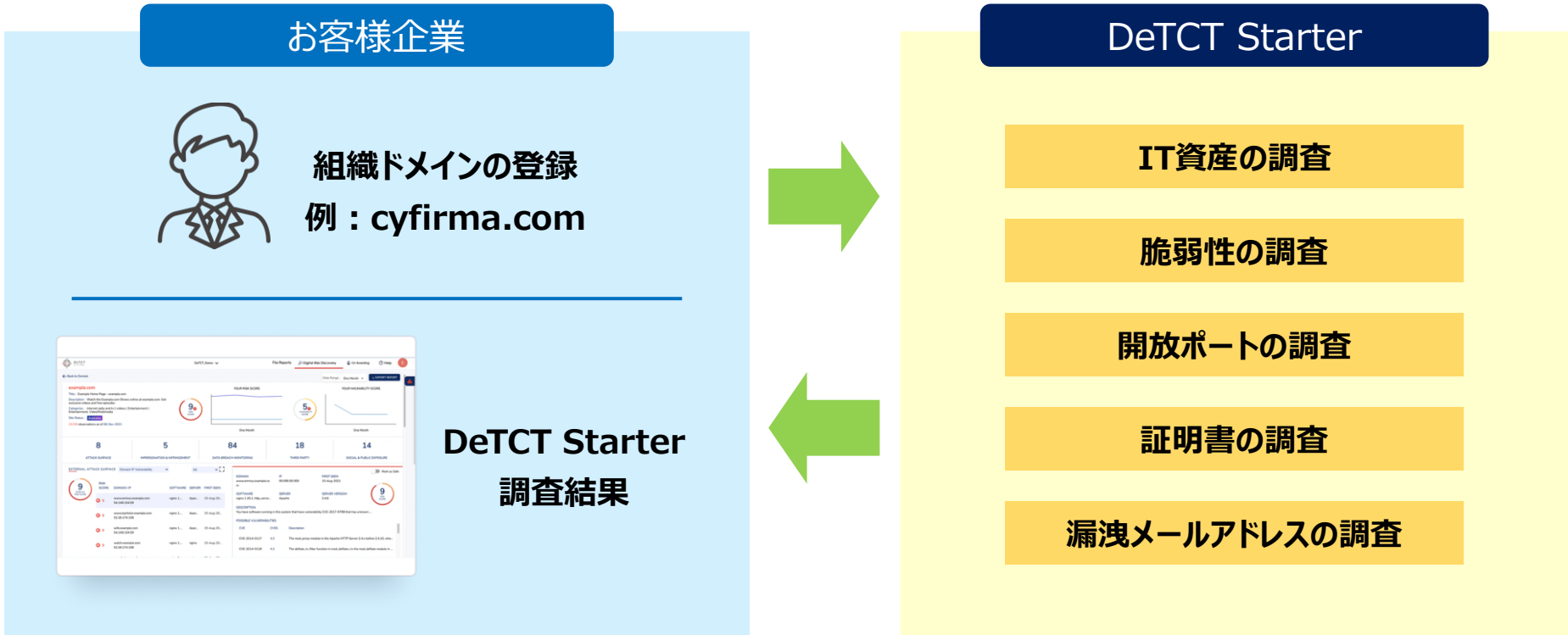
CYFIRMA DeTCT Starter

– 外部脅威情勢管理プラットフォーム –

Cyfirma K.K.

CYFIRMA DeTCT Starter とは

- **DeTCT Starter はお客様企業の組織ドメインをご登録いただくだけで、お客様の外部公開資産とその潜在的な問題、更に攻撃に悪用される可能性のある漏洩メールアドレスの有無を調査し、その調査結果を提供するSaaSサービス**
- **お客様企業はこの調査結果を用いて、セキュリティの改善に活用することが可能**



DeTCT Starterを用いた運用例

	① 公開 IT資産の把握	② 公開資産の問題・脆弱性の把握	③ 個人情報の漏洩の把握
お客様の課題(例)	守るべき資産対象の一覧に抜け漏れがあり、資産（野良資産）が認識できていない	公開資産に問題（不要なポートの開放や脆弱性）があり、サイバー攻撃に悪用される可能性がある	社員が利用する外部サービス（例:SNS、イベントサイト、ECサイトなど）からメールアドレスなどが漏洩し、不正アクセスやフィッシングに利用される可能性がある
DeTCT Starterでできること	お客様の公開資産を自動的に特定	資産の設定不備や潜在的な脆弱性を自動で特定	漏洩してしまった認証情報を自動的に調査

組織ドメイン / サブドメイン / IPアドレス

組織ドメイン	サブドメイン	IPアドレス
cyfirma.com	www.cyfirma.com	123.123.123.1
cyfirma.com	mail.cyfirma.com	123.123.123.2
cyfirma.com	test.cyfirma.com	123.123.123.3
cyfirma.com	ftp.cyfirma.com	133.123.123.4
cyfirma.com	vpn.cyfirma.com	133.123.123.5

サブドメイン / ウェブサーバ／ソフトウェア / 開放ポート / 可能性のある脆弱性

サブドメイン	ウェブサーバ／ソフトウェア	開放ポート	可能性のある脆弱性
www.cyfirma.com	Microsoft IIS 8.0	80, 443	CVE-2022-11111
mail.cyfirma.com	Microsoft IIS 10.0	25, 80, 443	
test.cyfirma.com	Apache 2.4	80, 8104	CVE-2022-22222
ftp.cyfirma.com	Nginx 1.8	22	
vpn.cyfirma.com	FortiOS	443	

メールアドレス / パスワード / 漏洩元

メールアドレス	パスワード	漏洩元
aaa@cyfirma.com	**********	Facebook
bbb@cyfirma.com	*******	Adobe
ccc@cyfirma.com		Twitter
ddd@cyfirma.com	**********	LinkedIn
eee@cyfirma.com		

お客様の運用（例）

- ① 認識していない資産を把握する
- ① 全ての公開資産を管理台帳で管理する
- ① 不要なDNSレコードを削除する
- ② OSやソフトウェアのバージョンアップを行う
- ② OSやソフトウェアに最新のセキュリティパッチを適用する
- ② 不要な開放ポートを閉じる
- ③ 社員が在籍しているか確認
- ③ 退職している場合 ➡メールアドレスを削除
- ③ 在籍している場合 ➡パスワードの変更を推奨・実施

導入ポイント

- **ドメイン名を元に自社の公開資産の一覧や潜在的な問題を簡単に把握することが可能**
- **サイバー攻撃に悪用される可能性のある従業員のメールアドレス、パスワードの情報を提供し、適切な対策を支援**

Jamf Pro

– Appleデバイス管理のデファクトスタンダード –

Jamf Japan合同会社

Jamf Proとは

Appleデバイス管理のデファクトスタンダード

- **Jamf Proは、Mac、iPhone、iPad、Apple TVをシームレスに管理できる業界唯一のApple専用MDMソリューション。**
- **職場や教室でAppleデバイスを利用するエンドユーザの生産性と創造性を保ちながら、IT管理者はデバイス管理業務を大きく自動化を実現。**
- **現在、世界中の71,000以上の組織が導入し、3,000万台以上のApple製品の管理でJamfの製品を使用。**

① Jamf Proの特徴

デバイス管理に必要な機能が１つのパッケージに!

デバイス管理

**Wi-FiやVPN、パスコード、OSの各種機能などの設定を反映した構成プロファイルを使ってデバイスを管理できます。
独自スクリプトによるMacの高度な管理も可能です。**

アプリ配信

**Apple の「VPP」（アプリー括購入）と連携することでアプリを一括購入し、エンドユーザはApple ID不要でアプリをデバイスやグループへ自動でインストールすることができます。
組織固有のニーズに合わせて、カスタムアプリの配付も可能です。**

リモートコマンド

デバイスの盗難、紛失時のデータ消去やロックのほか、リモートコマンドによるアプリ配付、OSのアップデートを行えます。

インベントリ管理

**ハードウェアやソフトウェア情報、セキュリティ設定等のあらゆるインベントリ情報を自動的に収集します。
カスタムレポート機能やアラート機能も搭載します。**

セルフサービス

**企業や学校専用のアプリストアを作成できます。
エンドユーザ自らインストールやアップデート作業を行ってもらうことで、IT管理者の工数を削減できます。**

② Jamf Proの特徴

最新のOSのアップデートに即日対応【OS同日サポート】

セキュリティの観点からも、利用者にはApple社がリリースした最新のソフトウエアを 使ってもらいたいものです。
企業にとって非常に重要な役割を担うMDM/デバイス管理システムにも関わらず、最新のOS への対応に数ヶ月要してしまっては危険です。Jamfなら速やかに最新の、より安全な環境に移行することが可能です。

「ゼロタッチ導入」新規端末導入時のキッティングを自動化

Appleの自動デバイス登録をJamf Proで完全にサポート。
1台1台設定を行う必要はありません。事前に設定を仕込んでおけば、デバイスが届き、Wifiに接続したら、すぐに使用できる状態になります。
IT管理者の工数・コスト削減に大きく貢献します

設定内容の即時反映と配信エラー履歴確認

新しい構成プロファイルアプリを配信したのにデバイスに反映されず、トラブルになったことはありませんか？
Jamf Proでは確実な配信と、エラー履歴の確認ができるため、設定適用できなかったデバイスも容易に抽出、確認可能です。

安心の構築導入支援

導入時の構築の支援を行う有償の「Premium Onboarding」を用意しており、Jamfの技術認定を受けた専門家がお客様のMDM設定・構築のお手伝いをいたします。
対象デバイスに合わせて複数のメニューをご用意しております。

お客様の生産性と創造性を保ち、IT管理者の業務にゆとりをもたらします

GUARDIANWALL Mailセキュリティ

– 脱PPAP情報漏えい対策の決定版 –

キャノンマーケティングジャパン株式会社

GUARDIANWALL Mail　セキュリティ・クラウドとは？

キャノンマーケティングジャパン様自社開発
脱PPAP情報漏えい対策ソリューション

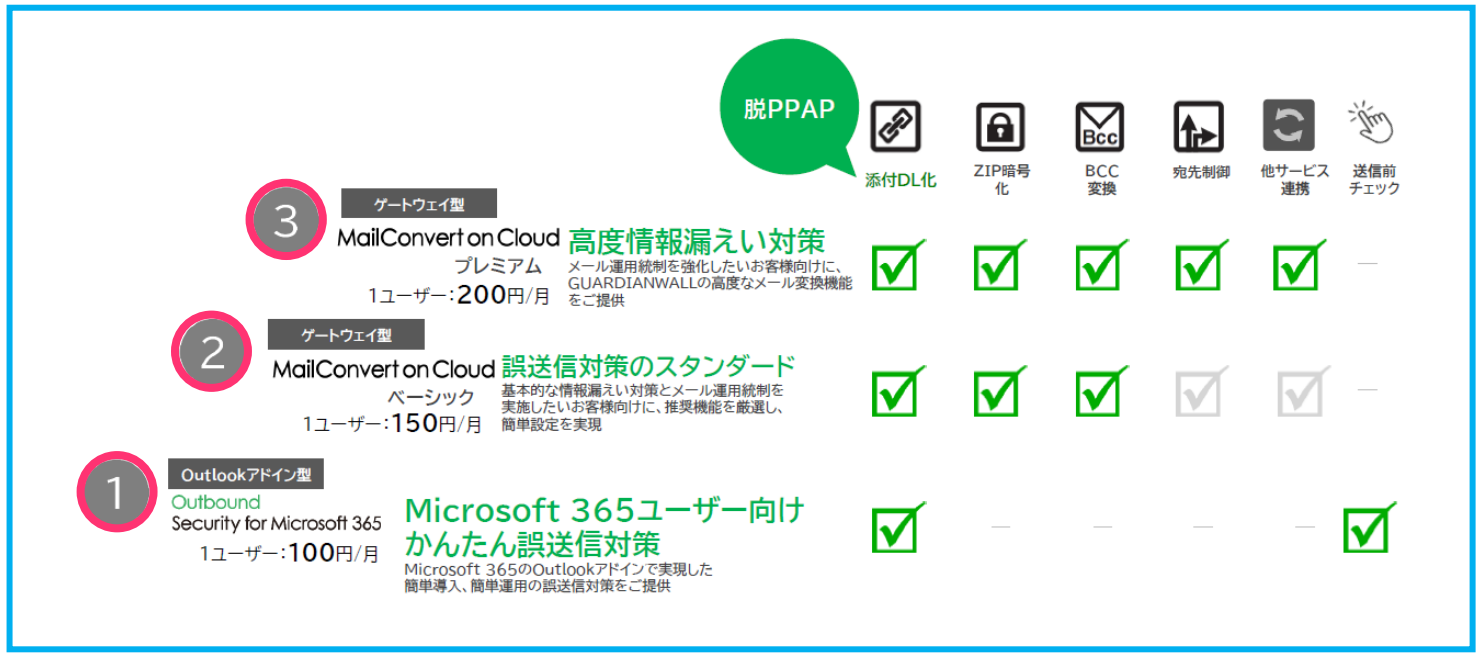
▶ 多くの採用実績

- 3,500社 を超える大手銀行様・
省庁様・グローバル企業様などへの導入実績

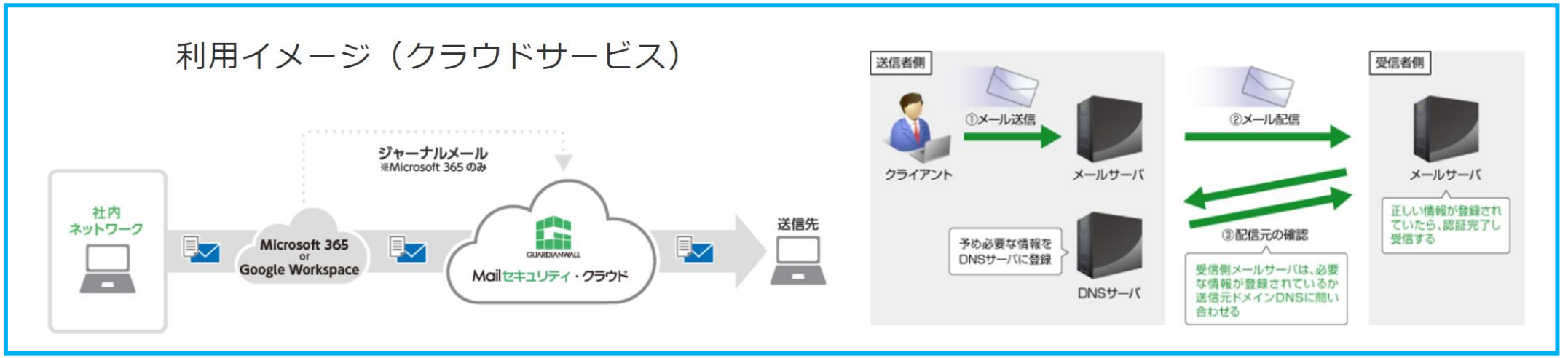
- 利用ユーザー数 500万ユーザー 以上

- サービス事業者様のサービスにも採用
（IIJさま/ソフトバンクさまなど）

▶ お客様のセキュリティ要件・運用に合わせて「３つのサービス」をご用意



GUARDIANWALL Mail　利用イメージ



利用イメージ（クラウドサービス）｜GUARDIANWALL Mailセキュリティ｜キヤノン (canon.jp)

▶ Microsoft 365もしくはGoogle Workspaceのメール送信先をMailセキュリティ・クラウドに指定いただくことでご利用可能です。
利用されるサービスによっては受信メールの経路も変更していただく必要があります。

※ 設定にあたり、SPFレコード※1の追加登録が必要となる場合がございます。

▶ 各種操作（保留メール閲覧など）は、Webブラウザーよりご対応いただけます。

※ SPFレコードとは、メールの送信元ドメインが詐称されていないかを証明するための、インターネット技術標準（RFC）で定められる仕組みです。
メール受信者側において、このIPアドレス（サーバー）から来たメールは、そのドメインから来た正常なメールであるかを確認するために用いられます。
SPFは、標的型攻撃メールや迷惑メールなどの「なりすましメール」の流通を抑止するための有効な手段の一つとされ、近年導入が強く推奨されています。

Deep Instinct

– ディープラーニングを活用した エンドポイントセキュリティ製品 –

情報技術開発株式会社

予防ファーストを実現する Deep Instinct

tdi 情報技術開発株式会社

iguazu

“サイバー攻撃は防御できない“ 前提から、
“早期発見、調査、対処”を、事後対処にとどまっていませんか？

従来製品の課題
（前提）

- 既知の情報からウィルスを検出するため、
  未知の脅威には対応できない
- 検知できるファイルの種類が限定されており、
  感染直後に検知ができない

deep instinct™

サイバー攻撃を防御 予防

被害や感染を限りなく少なくするためには、
攻撃を初期段階から防御(予防)することが大切です

ランサムウェアの動き

*Splunk 『ランサムウェアバイナリの実験に基づく比較分析』
https://www.splunk.com/ja_jp/form/an-empirically-comparative-analysis-of-ransomware-binaries.html

深層学習を活用した Deep Instinct (第4世代)

tdi 情報技術開発株式会社

iguazu

大量のデータサンプルを深層学習のAIへ取り込ませることで
マルウェアの**DNAを学習**するフレームワークを構築

Deep Instinct 独自
深層学習ニューラルネットワーク
フレームワーク

Deep Instinct社のLABO内で深層学習を実施

高精度に脅威を検知・予防する
D-Brain(モデル)を作成し、エージェント化

PC　サーバ
モバイル　タブレット

予防ファースト

deep instinct

第４世代
AI駆動型予防型セキュリティ

深層学習

AI-based malware

第３世代
Endpoint Detection & Response (EDR)

機械学習

Fileless　Scripts　Coin miners

第２世代
Endpoint Protection Platforms (EPP)

シグネチャ＋振る舞い分析

Mobile　Wipers　Code injection　Dual use　Ransom-ware

第1世代
従来型アンチウィルス

ヒューリスティック＋
シグネチャ

Virus　Botnet　Trojans　Malware　Worm

既知未知問わず
幅広い脅威に対応

深層学習の活用で
高い検知率を実現

予測による防御のため
シグネチャ更新不要

自律的に脅威を
発見して予防

防御力

テクノロジーの進化

Deep Instinct の特徴

tdi 情報技術開発株式会社

iguazu

未知の脅威に対する圧倒的な防御力

既知や未知問わず幅広い脅威へ対応
(PE、PDF、Office、PowerShell、Image、Macro、Script等)
脅威が実行される前に予防が可能。

ひとつのモジュールで多層防御を実現

深層学習により、ドキュメントファイル、攻撃プロセスに使われる他の
ファイルやスクリプトもAIが学習し、様々なファイルのスキャンに対応。

エージェントが軽量

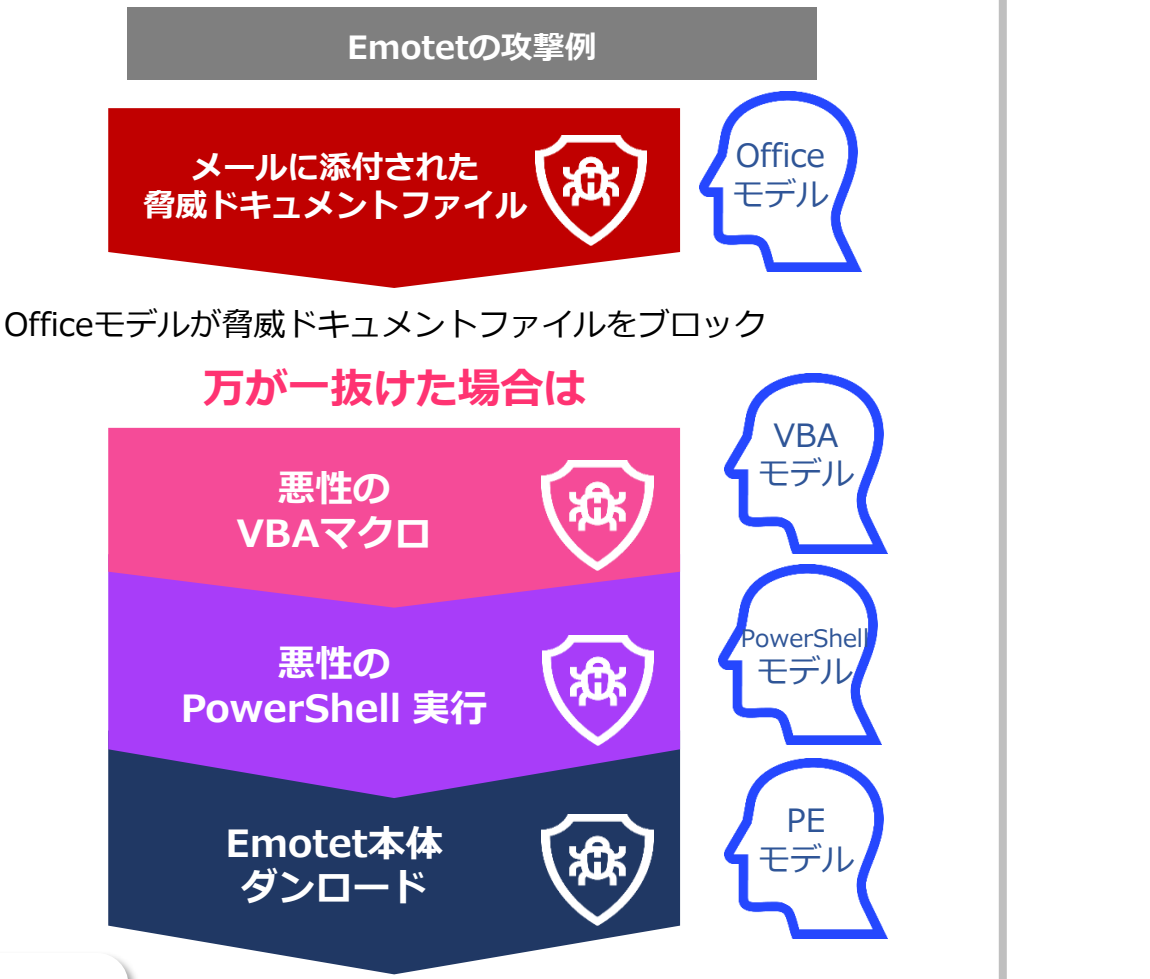
従来のAV製品に比べてリソース消費が少なく、動作が軽く、
（<150MB, <1% CPU）毎日のアップデートやアップデート毎の
フルスキャンが必要ない。

様々なOSに対応

Windows、macOS、Android、ChromeOS、Linux、iOS
※iOSでは静的解析/動的解析の機能は実装されておりません。

オフラインでも動作

検知能力はインターネット接続有無に依存しない。



deep instinct

多彩な防御機能によりマルチステージ攻撃に対応

その他

– イグアスお薦め商材 –

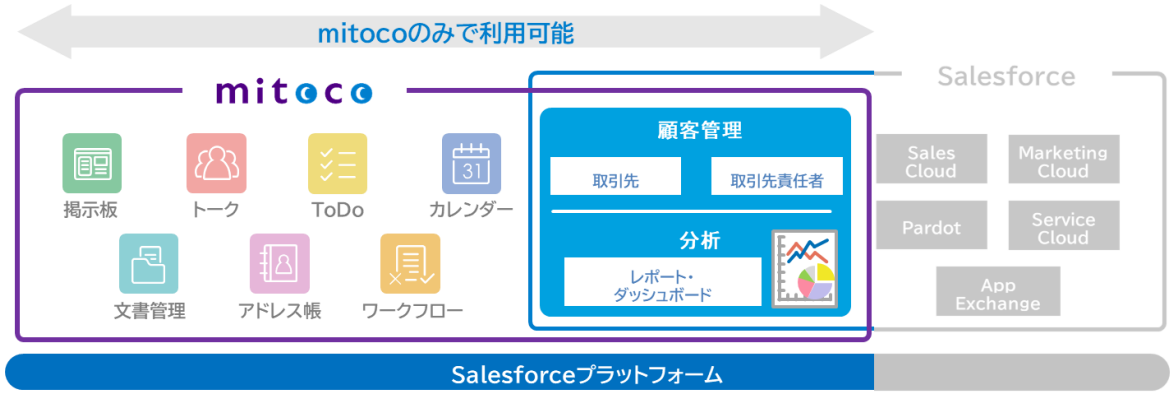
Mitoco+GPT

– Salesforceと連携する最適グループウェア –

株式会社テラスカイ

① mitoco+GPTとは

mitocoとは、Salesforce上で動作するグループウェアです



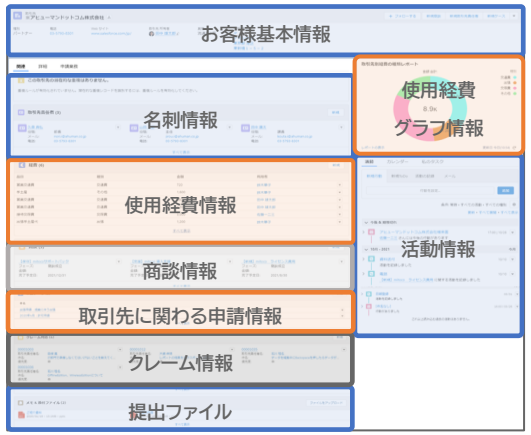
Salesforce上で稼働しているため、
Salesforceのライセンスが必要だと思われるかもしれませんが、
実際には Salesforceライセンスは不要で利用することができます。

さらに、mitocoはSalesforceの
一部機能も活用可能製品となっています。

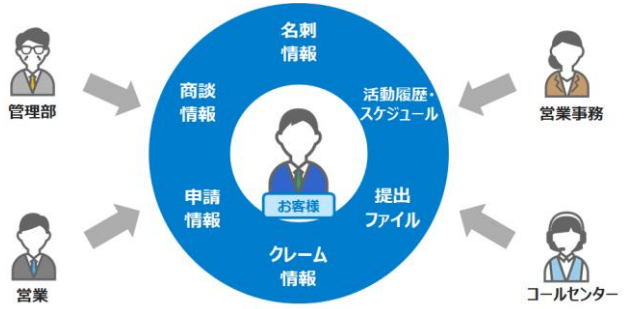
お得

[Q1] mitocoで何ができるの？

Salesforceの一部機能を使用するこにより、
お客様目線での顧客カルテを効果的に構築することができます。
顧客情報を中心にして、部署ごとに効率的な管理が行え、
情報連携や社内連携も容易に実現します。



▶ 顧客情報を
1画面で見ることが可能



▶ 部署ごとに管理されていた情報を一元管理が可能に！
▶ 顧客情報のバリアフリー化！

② mitoco+GPTとは

[Q2] モバイルでも利用可能？

新型コロナウイルス感染症も収束に向かいつつあり、
外勤営業も活発化し、訪問ニーズが増しています。
このため、モバイル利用が求められています。

機能ごとにアプリを分けているのですぐに情報にアクセス可能
パッチ通知も機能ごとに表示されるので分かりやすい

mitocoは、モバイル専用のアプリケーションを提供しており、
ブラウザ版と遜色ない利便性を実現しています。

利用開始まで最短5営業日で提供可能

mitocoライセンス	
1~300ユーザ	800円/ID
301~1,000ユーザ	700円/ID

初期導入費用 ※オプション	
管理者向けトレーニング	120,000円/4名
導入支援	個別見積

[Q3] 導入するにあたり流行りの生成AIを使用してみたい。

イグアスオリジナルの
生成AI機能追加サービス※1を提供いたします。

生成AI用いた孫の手機能

- ✓ 報告内容を要約したい
- ✓ 客観的に報告内容から次の一手のアイディアが欲しい
- ✓ 取引先の特徴を客観的に確認したい

イグアスオリジナルの
テンプレートで提供いたします!

※1：当該サービスは別料金となります

MOTTA GREEN FORK

– 電動フォークリフト 業界初のソリューション –

株式会社イグアス

① MOTTA GREEN FORK

GREEN FORK

スピーディー・高品質・安心保障

MOTTA

BATTERY SMART SOLUTION

業界初のソリューション

「GREEN FORK」は、5年間の新車リースを前提として、そのリース期間中のバッテリー稼働を保証するパッケージサービスです。
フォークリフトのバッテリーはとても高価であるにも関わらず、車体のリース期間中にバッテリーを新しく買い直さなければならないケースがあり、多くのお客様が経験されている悩みの一つなります。
「GREEN FORK」はそのコスト負担や口スを効果的に軽減し、ユーザーのリフト運用・計画をご支援いたします。

コスト課題の解決と環境対応

「GREEN FORK」のバッテリー稼働保証は、対象バッテリーの新品価格を考慮して、その30～40%のコスト削減となるように設計されています。
また、車体リースに合わせた月額支払いとなりますので、突然のバッテリー不調による想定外の費用発生を未然に防ぐことが可能となります。
さらにリース期間中に稼働が低下したバッテリーはバッテリー復元技術（特許技術）を用いて機能回復したバッテリーと交換されますので、新品と比較して、排出CO_2は約67%削減、同時にリユースによる廃棄物排出抑制からも環境に貢献。

車体準備から運用の包括サポート

お客様の業務内容やリフト稼働の状況をヒアリングさせていただき、最適な車体のご提案、その後の計画的なメンテナンス、月次検査、年次検査、定期バッテリーの状態確認、故障修繕など、お客様のリフト運用を包括的にサポートいたします。
また、お客様の繁忙期や、一時的なトランザクション増加に対応するため、スポット車両（レンタル）のご提供にも対応いたします。

② MOTTA GREEN FORK

GREEN FORKの特徴

最長7年保証　定額運用　コスト削減　CO_2削減

電動リフトの安定稼働で、高い生産性を実現します

最長７年保証

車体リース期間中、バッテリーには最長7年の稼働保証がパッケージとして組み込まれています。
バッテリー不調によるよる影響を受けず、常に安定した業務効率を実現します。

定額運用/コスト削減

バッテリーコストは毎月の定額で平準化されます。これにより、見立ての難しいバッテリー交換予算を構成する必要がなくなります。また、定額の合算は、新品バッテリーへの交換に対してコストメリットがあるように設定されています。

CO_2削減

保証期間内のバッテリー交換には、復元バッテリーが活用されます。
復元バッテリーは、新品バッテリーに対して、67%のCO2削減効果が得られます。（第三者機関による評価）

サービスラインナップ

リースプラン

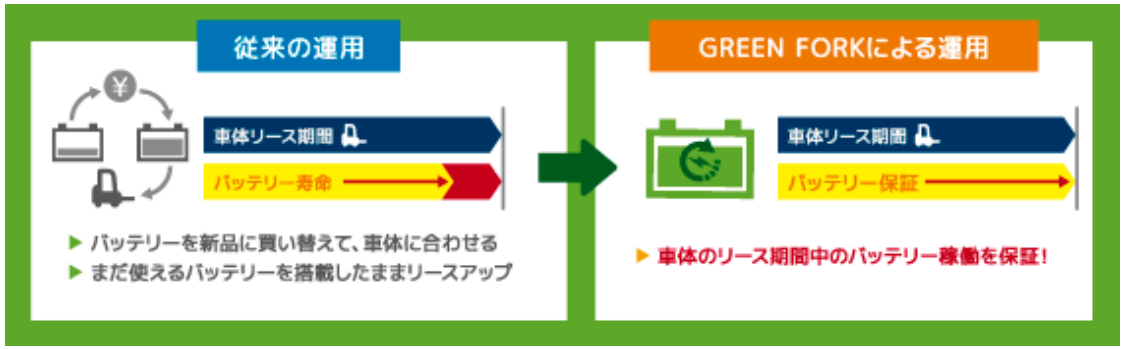
バッテリー稼働保証型
電動フォークリフト新車パッケージ
お客様の稼働状況や解決課題に合わせた最適な車体提案、
バッテリー稼働保証型のパッケージプランをご案内いたします。

車体販売プラン・バッテリー単体

車体購入のケースやバッテリー単体の場合でも、
お客様のニーズに合わせたパッケージプランをご提案いたします。

トータルメンテナンスプラン

バッテリー稼働保証型
車体メンテナンス（月次・年次検査）パッケージ
バッテリー稼働保証に加え、車体の定期メンテナンス、
月次・年次検査を含めたトータルのパッケージをご提案いたします。



200 種類を超える
IT ソリューションを掲載！！

IGUAZU
Solution Portal
イグアス　ソリューションポータル

イグアス　ソリューションポータル

サイトへの掲載を
ご希望の企業様

募集中！

イグアス ソリューションポータル
Solution Portal

https://www.iguazu-sol.jp

ソリューション検索の総合ポータルサイト

株式会社イグアスが運営する様々な IT ソリューションを紹介する総合ポータルサイトです。
業務、用途別のカテゴリーに分類された 200 種以上のソリューションが検索できます。
製品説明動画、説明資料も充実。見積依頼も簡単です。
貴社が探している最適ソリューションが必ず見つかります！

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

Webサイト: https://www.iguazu-sol.jp

お問い合わせはこちらへ

株式会社イグアス
ソリューション営業部

Mail : sol_sup@i-guazu.co.jp