機械学習によるネットワーク内部の脅威検知サービス

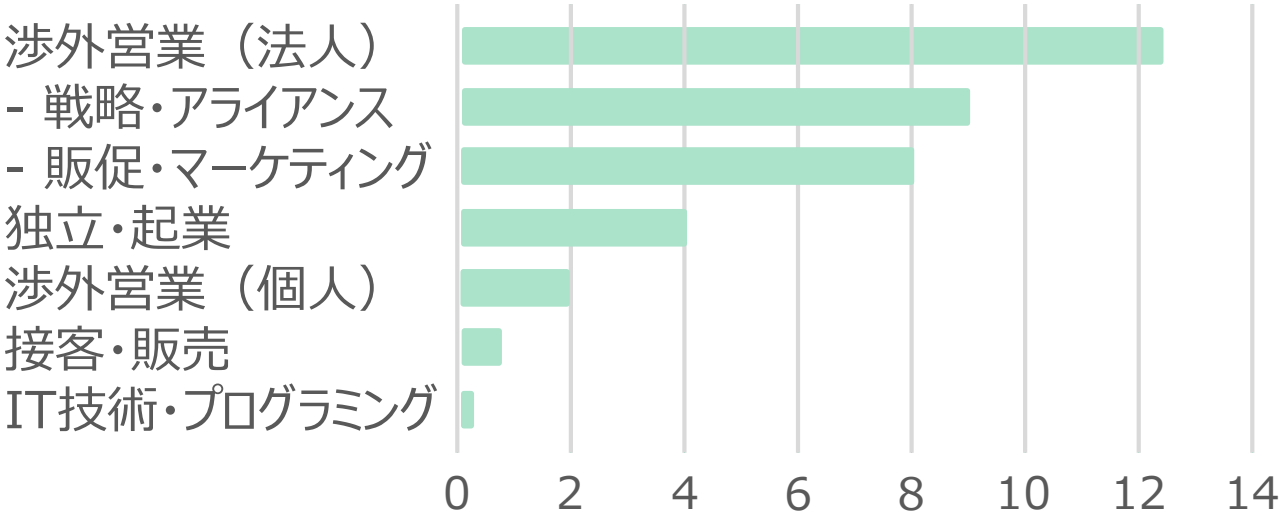
～ 企業内ネットワークの不審な挙動をリアルタイムで発見！ ～

京西テクノス株式会社
システムサービス本部　営業部
平松 健太郎

KYOSAI

自己紹介

名前：ひらまつ けんたろう
年齢：36歳（天秤座）
生息地：千葉県の緑豊かな田舎
家族：俺、嫁、長女、次女、犬（長男）の計5人
体格：今どき流行りの細マッチョ体型ではない。
特技：意図せず街中で目印にされること。



これまでの業界遍歴
・ブライダルプランナー
・店舗向け清掃業務
・コンシューマソフトウェア
・ビジネスプロデュース
・Webソリューション
・ITシステムソリューション
・家庭用英語教材

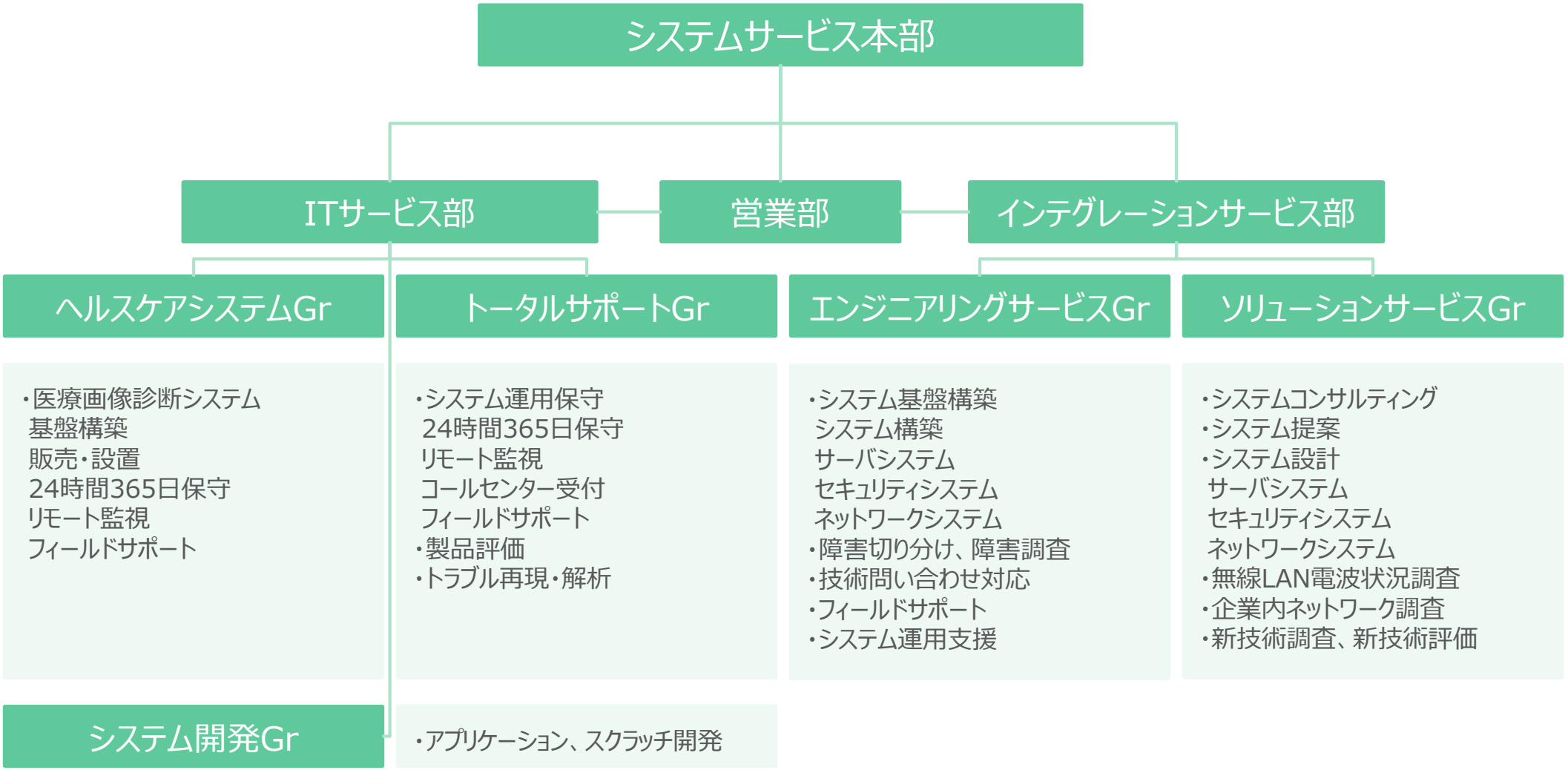
京西テクノスって何やってる会社？

KYOSAI

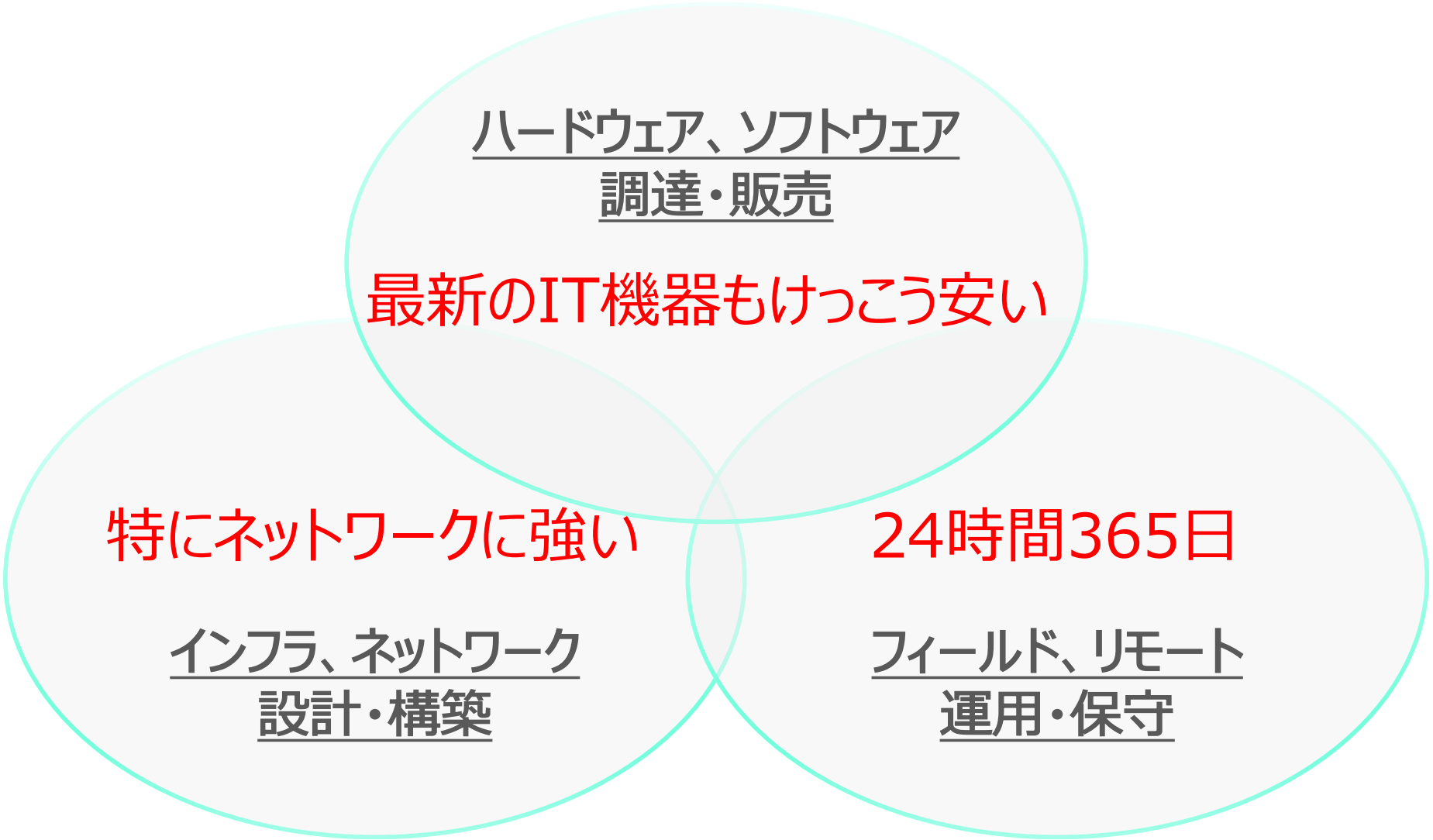
会社概要

商号	京西テクノス株式会社
所在地	東京都多摩市愛宕4-25-2
設立	2002年02月
資本金	4,000万円
代表取締役	代表取締役社長 臼井 努
従業員数	約300名
グループ会社	京西科技有限公司 / 株式会社テクノトレンド /Mテックサポート株式会社
拠点	全国 8 拠点（東京/名古屋/大阪/広島/福岡/郡山/仙台/札幌）
主な事業内容	1.計測器/医療機器/通信機器/環境エネルギー分野における 設計・製造・評価・修理・校正 2.システムサービス事業 ・ITインフラシステムの構築・運用 ・ネットワークシステムの設計・構築 ・システム運用管理、24時間365日運用サポートなどのITサービス

システムサービス本部のビジネスユニット



システムサービス本部のビジネス領域



複雑化・高度化するサイバー攻撃に対抗するためのセキュリティ対策課題

KYOSAI

サイバー攻撃による脅威が変わってきた

【予防】
- これまでの対応
- 検知して駆除する

【リアルタイム調査】
- これからの対応
- まずは可視化
- 検知したものを調査
- 調査した上で対処

予防ではなく、リアルタイムでの調査がとても重要に

昨今のサイバー攻撃では、既存の境界型セキュリティ製品を
すり抜けるか、全てテストしているので、これまでのようなパターンマッチングでは
悪意のある攻撃からの防御に間に合わなくなってきている

サイバー攻撃、情報漏洩は他人事ではない

	漏洩原因	漏洩規模
某大手教育事業社	個人スマートフォンへのデータ移行による個人情報売買	2,895万件もの個人情報が流出、売買される
某なんちゃら機構	標的型攻撃メールからの不正アクセスによる感染	125万件の情報が外部に流出
某大手旅行事業社	標的型攻撃メール、なりすましによるウィルス感染	793万件の個人情報が外部に流出
【海外事例】 某医療保険事業社	サーバに国外からのハッカーが侵入、PW盗難	8,000万件もの個人情報が流出、海外でも最大級の規模
【国内小規模事例】 某美容関連販売事業社	自社サイトへの不正アクセス、外部サーバに不正プログラムの仕掛け	1,955件の個人情報流出、サイトは長期間閉鎖に。

KYOSAI

小規模企業はサイバー攻撃の標的にされやすい

情報セキュリティ対策担当者がいる

19.6%

（全体平均：44.6%）

社員のBYODを認めている

50.3%

（全体平均：38.9%）

出典：IPA「2015年度 中小企業における情報セキュリティ対策に関する実態調査」https://www.ipa.go.jp/security/fy27/reports/sme/

被害は大企業だけではなく、中小以下の企業においても
重要、かつ深刻な問題となっており、早急な対策が必要

セキュリティ対策の現実① 現状把握が困難

入口対策	出口対策	内部対策
・エンドポイントセキュリティ ・ファイアウォール ・IPS/IDS（不正侵入防止） ・サンドボックス ・スパムゲートウェイ	・ウェブフィルタリング ・アプリケーションファイアウォール	・ネットワークIDS ・ファイル暗号化 ・ID管理 ・SIEM（ログ相関分析） ・統合ログ管理

セキュリティの重要性は理解しているが、具体的に
何をどうすれば良いのかわからない。

セキュリティ対策の現実② 全ての脅威に対する対抗策が困難

入口対策	出口対策	内部対策
・エンドポイントセキュリティ ・ファイアウォール ・IPS/IDS（不正侵入防止） ・サンドボックス ・スパムゲートウェイ	・ウェブフィルタリング ・アプリケーションファイアウォール	・ネットワークIDS ・ファイル暗号化 ・ID管理 ・SIEM（ログ相関分析） ・統合ログ管理

セキュリティ製品の多くは高価なものも多く、
十分な予算確保ができない、また運用できる人もいない。

セキュリティ対策の現実③ それでも完璧な防御は不可能

入口対策	出口対策	内部対策
・エンドポイントセキュリティ ・ファイアウォール ・IPS/IDS（不正侵入防止） ・サンドボックス ・スパムゲートウェイ	・ウェブフィルタリング ・アプリケーションファイアウォール	・ネットワークIDS ・ファイル暗号化 ・ID管理 ・SIEM（ログ相関分析） ・統合ログ管理

重要な対策要素ではあるが不十分。

完璧なセキュア化は極めて困難	侵入者や攻撃者は巧妙な抜け道を見つけ出し攻撃する	既に内部に侵入した攻撃や内部から起こる不正は見えない	ルールやシグネチャを常に最新、完全の状態に保つのは無理

じゃあどうするの？

具体的に何をすれば 良いのかわからない	十分な予算確保ができない、 運用管理ができる人がいない	完璧な防御が不可能なら どうしようもないじゃん！
何が起こっていて、何を優先的におこなうべきか把握をしましょう！	適正予算で無理なく、かつ当社専門技術者が運用をお手伝いします！	侵入や内部不正を前提とした体制の構築が必要なんです！

京西テクノスの脅威検知サービスがお役に立ちます！

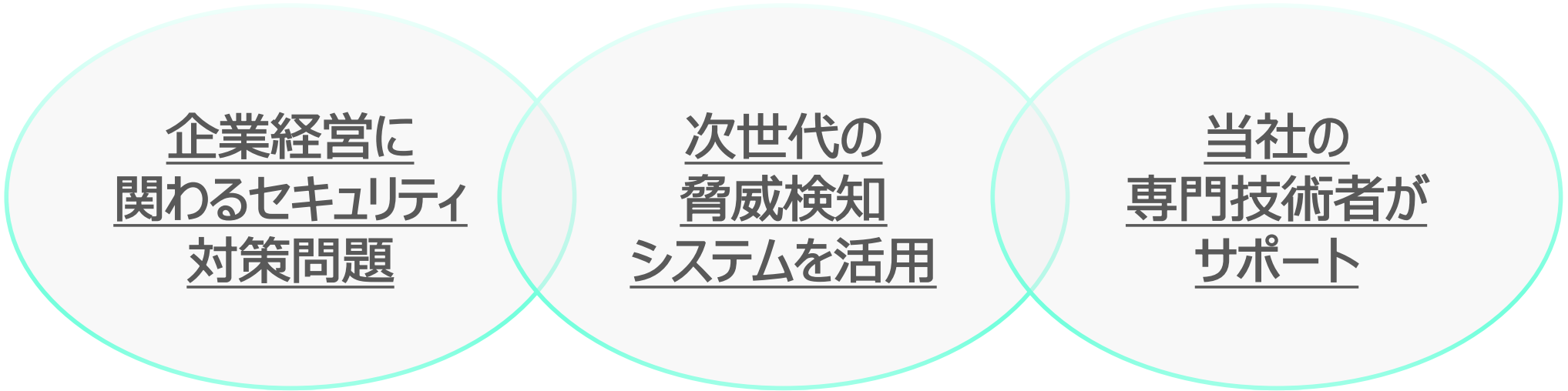
KYOSAI

京西テクノスが提供する脅威検知サービス

KYOSAI

脅威検知サービスってなに？

企業内ネットワーク環境の「定常動作」を機械学習により
可視化し、ネットワークの異常な挙動を検知、従来の
セキュリティ対策では防御や発見が困難な脅威を未然に
把握するためのシステム、ネットワーク運用を支援するサービス



脅威の検出ツールにDarktraceを採用

Darktraceの特徴

人間の免疫システムが多様な外的や環境変化に対抗することと同じ仕組みを
ITセキュリティシステムに適用、お客様ごとに異なる正常状態を定義する。

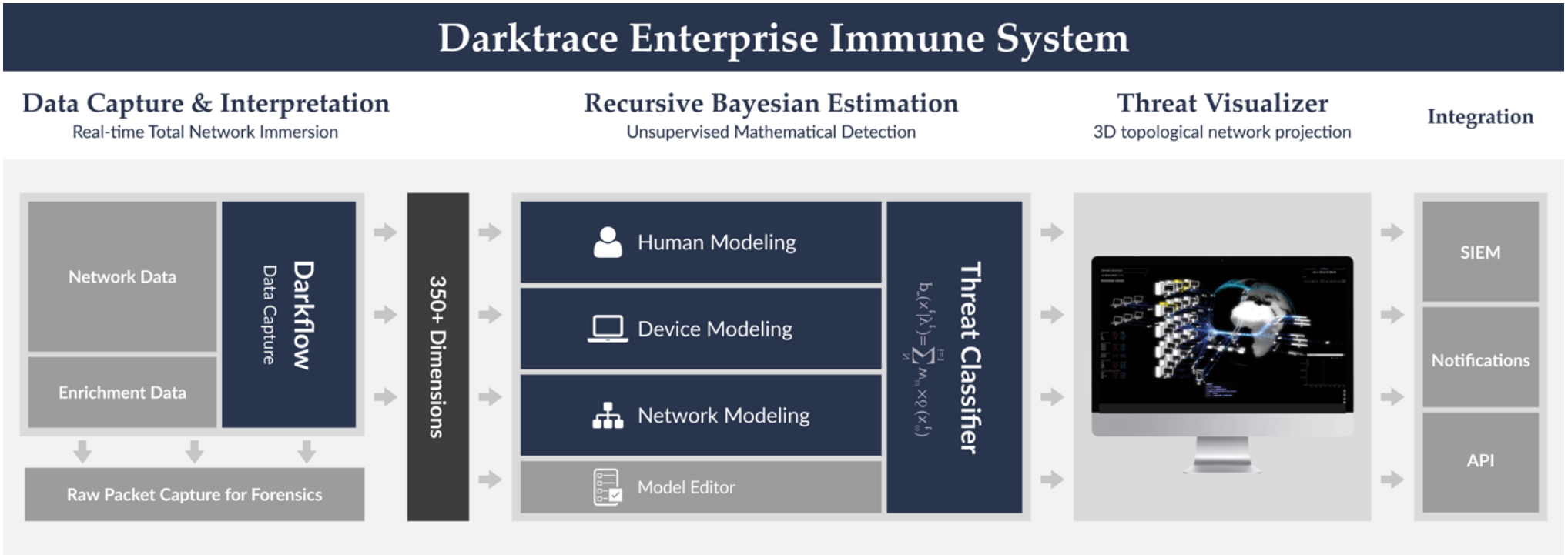
ルールやシグネチャに
依存しないシステム

優れた機械学習による
未知の脅威への対応

発見された脅威の
リアルタイム通知

Darktraceのアーキテクチャ

ケンブリッジ大学のバックグラウンドによる非常に優れた機械学習数学アルゴリズムを採用



ホストやネットワーク機器からネットワークパケットをキャプチャ（情報収集）

膨大なネットワーク情報を分析・学習し正常状態をモデリング（ベースライン定義）

正常状態との比較により発見された不審な挙動を可視化し検出する

KYOSAI

定常外挙動の一例

- ビデオ会議デバイスへの不正侵入
- 稀な外部宛先への異常なデータアップロード
- 外国からの制御システムへの不正アクセス
- 稀な外部デバイスとのビーコン通信
- 標的型メール攻撃を経たランサムウェアのダウンロード
- 特定ファイルサーバへの異常なアクセス
- 機密情報を自宅の機器に向けて送信
- 遠隔操作プログラムを埋め込まれたのち、DDoS攻撃の踏み台
- 指紋スキャナシステムからの指紋データ盗難、物理的セキュリティが無効化
- ウェブサーバ乗っ取り、違法薬品売買のウェブページ運営に不正利用

昨今のサイバー攻撃は、気付きが遅れるケースや検出に時間が掛かるケースも多く、如何に早く不審な挙動に気付けるかがポイントとなる

Darktraceの導入実績と確かな信頼性

エネルギー・公益業界

“Darktraceのテクノロジーにより当社のシステムを崩壊させる危険性をもった脅威を発見できました”

交通・輸送業界

“Darktraceのサイバーインテリジェンスプラットフォームによりリアルタイムに何が起こっているかを完全に把握できるようになりました”

保険業界

“Darktraceは事前に何を見つけだすかを定義・仮定することなく、起こり得る脅威を検出できます”

ゲーム業界

“Darktraceによってセキュリティの信頼度が向上し、社員や顧客、保有データに対する環境の安定化につながりました”

脅威検知サービスの全体概要

お客様環境対象機器


モバイル端末


社内PC端末


NW機器


サーバ機器

対象機器のパケットを収集・蓄積

KYOSAI
【脅威検知サービス】

システム提案
ソリューション提案

パケット調査・分析

リアルタイム通知

レポート作成・提出

インシデント対応
リモートサポート

お客様運用部門

補完ソリューション導入


月次分析
結果レポート

「定常外」の挙動を把握、
脅威を未然に確認

運用定例会議

KYOSAI

サービスメリット

自社（お客様）の定常動作を可視化、把握することができる！

導入済のセキュリティソリューションの邪魔をしない！

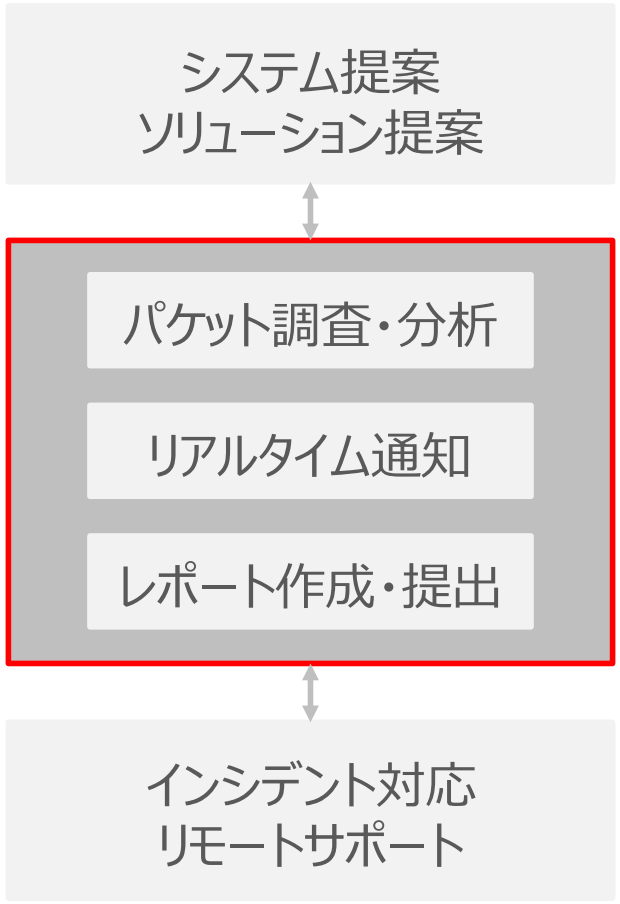
専門人員のリソース確保に多大なコストをかける必要がない！

未知のサイバー攻撃に対するセキュリティレベルを大幅に向上！

従来の検知・駆除の領域に加え、分析の領域を強力に強化！

教育、最適化された分析レポート、すぐに導入できる！

脅威検知サービス提供価格



ヒアリングにより適宜お見積もり

・脅威対策に適したソリューションやサービスを提案可能

500,000円/月～

・御社環境へDarktraceを設置
・接続端末台数目安：最大で1,000台程度
・当社にて調査・分析した結果を月次レポートとして提出

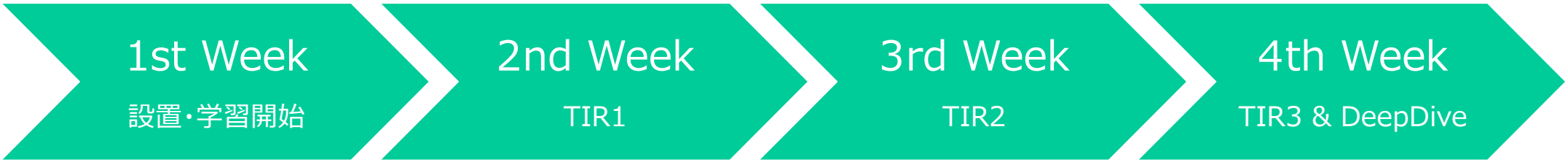
200,000円/月～

・ノード数、対応インシデント数により費用は変動
・サーバ、ネットワーク機器の監視も可能
・運用状況を定例報告会でディスカッション

お試しできます！

脅威検知サービスのご検討にあたり、まずは自社、またはお客様環境の状況を観察してみたい方に最適です。

Darktrace POV（Proof of Value）をご利用頂くことで、Darktraceを1ヶ月間御社環境へ設置可



TIR： Threat Intelligence Report（脅威レポート）御社へお伺いし実際に検出されたアラートを利用し、検出された脅威や発見されたプロセスについて説明をさせて頂きます。

DeepDive： それまでのレポートをもとに、当社サービスの利用検討に際してお打合せによるディスカッションを致します。

※ 実際の当社脅威検知サービスで提出するレポートと形式は異なります。

APPENDIX

御社お客様へ提案してみませんか？

協力頂ける
企業様を歓迎！

御社名義でサービス
提供を致します！

御社お客様へ提案してみませんか？

例えば・・
データセンター事業者様
運用サポートサービスの一環として提供してみませんか？

例えば・・
システムインテグレータ様
システム導入後のアフターサービスの一環として提供してみませんか？

例えば・・
運用アウトソース事業者様
サポートメニュー拡充の一環として提供してみませんか？

お気軽にお問い合わせ下さい！

京西テクノス株式会社
システムサービス本部　営業部

〒206-0041
東京都多摩市愛宕4-25-2
TEL：042-303-0891　FAX：042-303-0892
Mail：ss-sales@kyosaitec.co.jp
WEB：www.kyosaitec.co.jp

最後に

ご静聴ありがとうございました