The Border

クララオンラインの自社IT戦略とエンドポイント入れ替え実録

株式会社クララオンライン
ビジネスストラテジー部
コーポレートIT
山崎隼人

当セッションの流れ

前半：クララオンライン 山崎

- クララオンラインの自社の取り組みについて
- 次世代型エンドポイント保護(NGAV/EPP+EDR)の
  導入時の検証(PoC)や製品選定のポイント

後半：東京エレクトロンデバイス 三吉様

「SentinelOne」について

- **国内販売までの背景や製品の評価ポイント**
- **導入・運用トピックス**

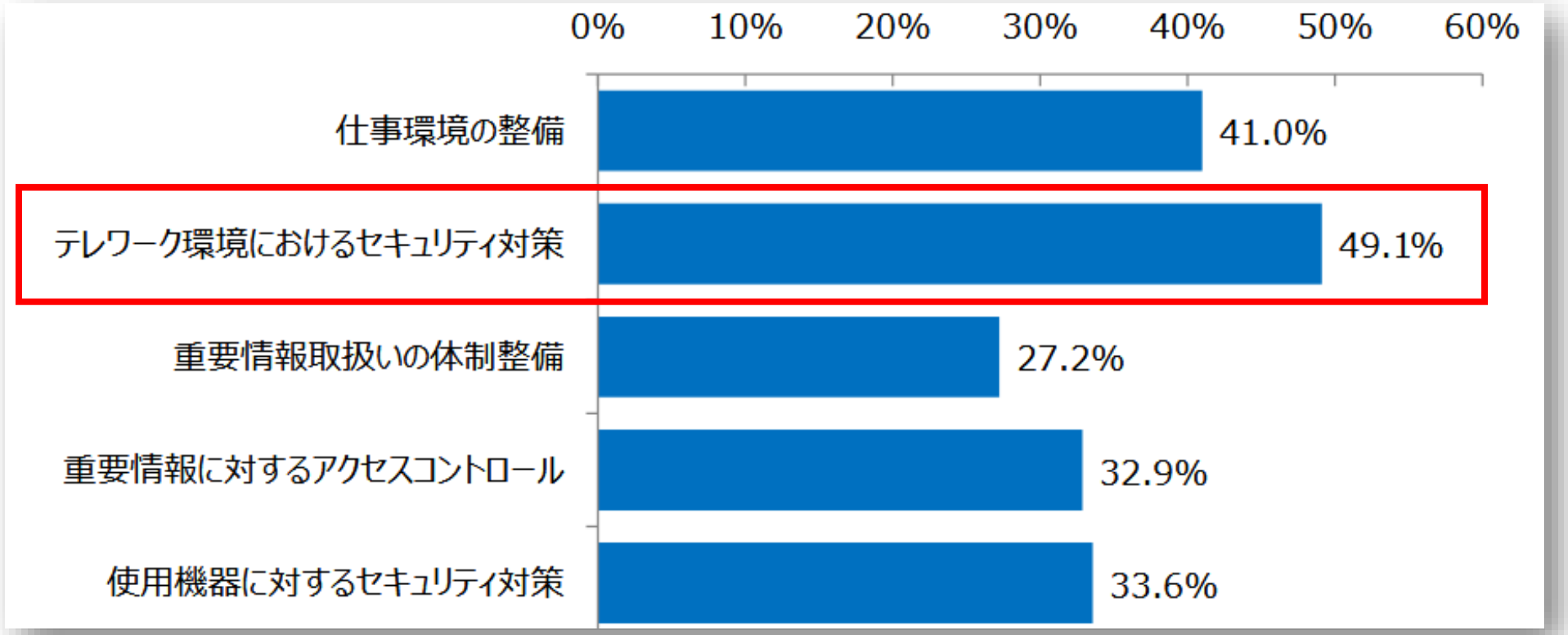
- コロナ禍による変化
- 当社の取り組み
- 次世代型エンドポイント保護の導入のポイント
  - 課題意識／比較検討
  - 導入検証のコツ
  - 製品評価・選定ポイント

コロナ禍による変化

市場調査クリップ(1/2)

緊急事態宣言下で業務を円滑に遂行するために重視した点として

「セキュリティ対策」が半数を占めている



出典：「企業IT利活用動向追跡調査2020」調査結果 - JIPDEC／株式会社アイ・ティ・アール
https://www.jipdec.or.jp/topics/news/20200924.html

コロナ禍での環境の変化

The Border

	ITインフラ	セキュリティ	ビジネスとIT
～2018	独自システム オンプレミス	境界防御 旧来対策	便利な道具
2019			
2020	クラウド必須	ゼロトラスト	IT活用が企業の生き残りを左右

緩やかな変化から
コロナにより社会全体で **強制的な変化** が起き、状況は一変

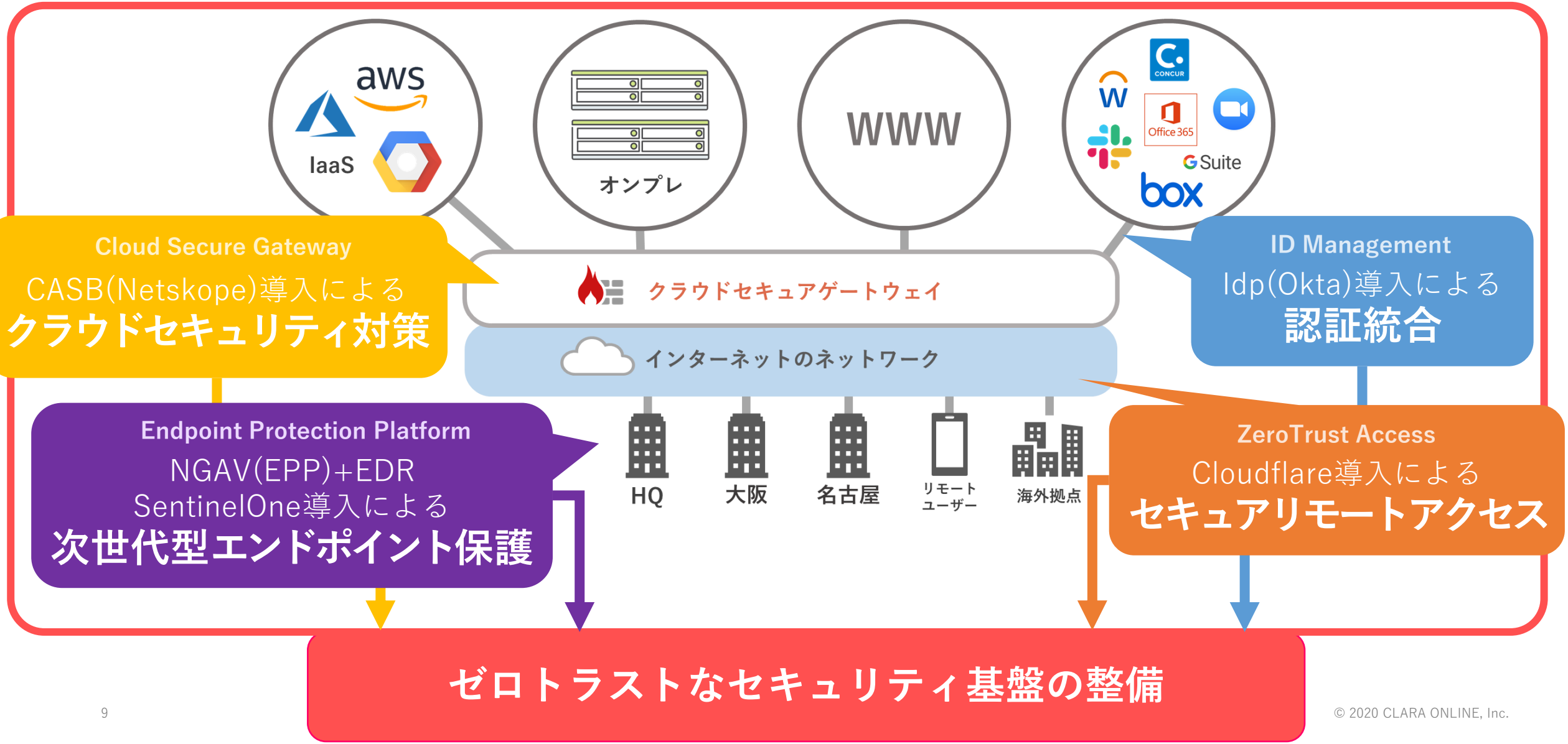
当社の取り組み

コーポレートITの活動の変化

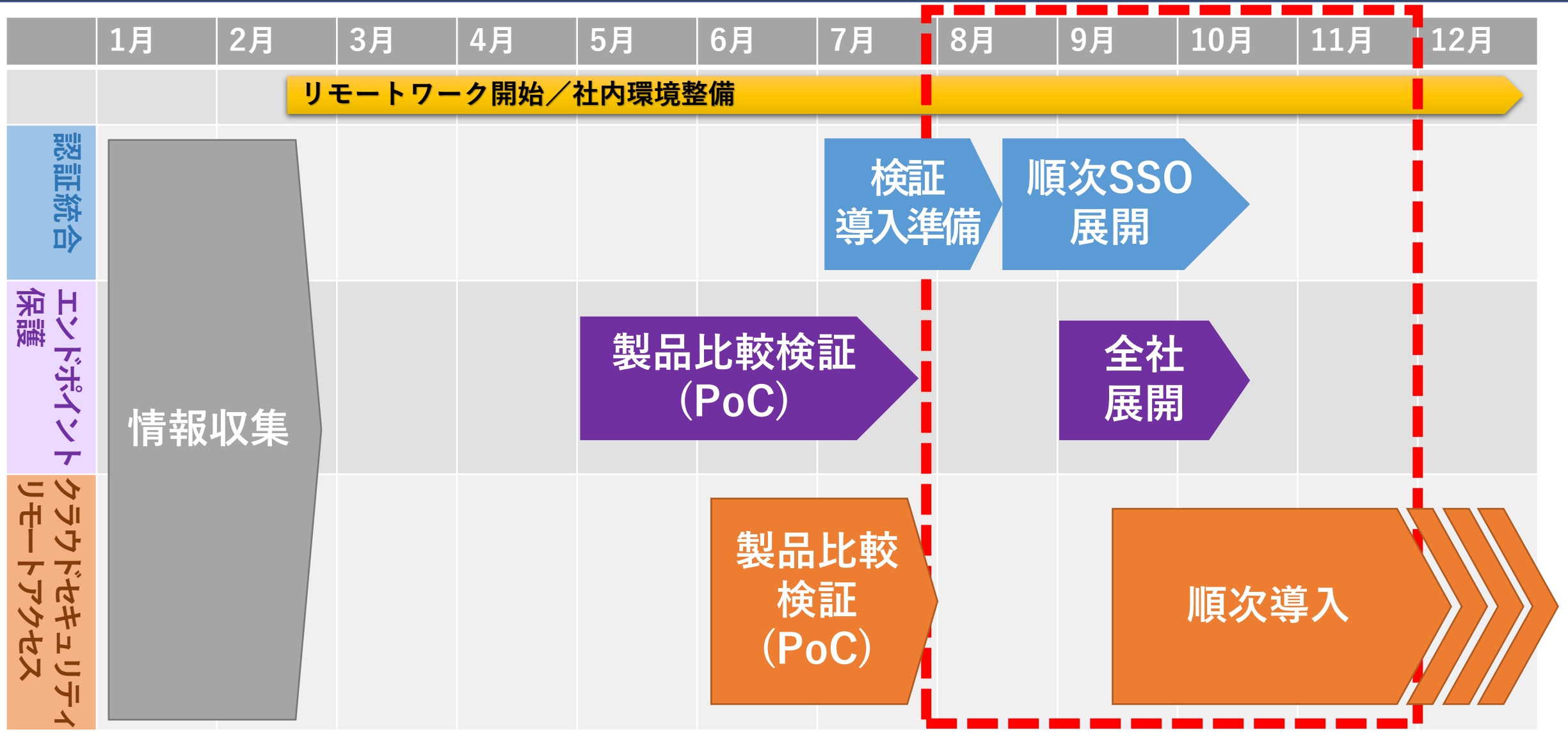
コーポレートITの活動が **事業サービスの強み、競争力** に
(自社の経験とノウハウをサービスに還元)

ゼロトラストなセキュリティ環境の実現に向けて

The Border



導入スケジュール



次世代型エンドポイント保護の導入のポイント

課題意識

- **従来型の仕組みでは防ぎきれない現状**
  - 攻撃の約8割が、未知のマルウェアやファイルレス攻撃
  - 攻撃を受け、感染する前提での環境整備の必要性
- **次世代環境(EDR)の運用コスト**
  - 高度なセキュリティスキル、人的リソース

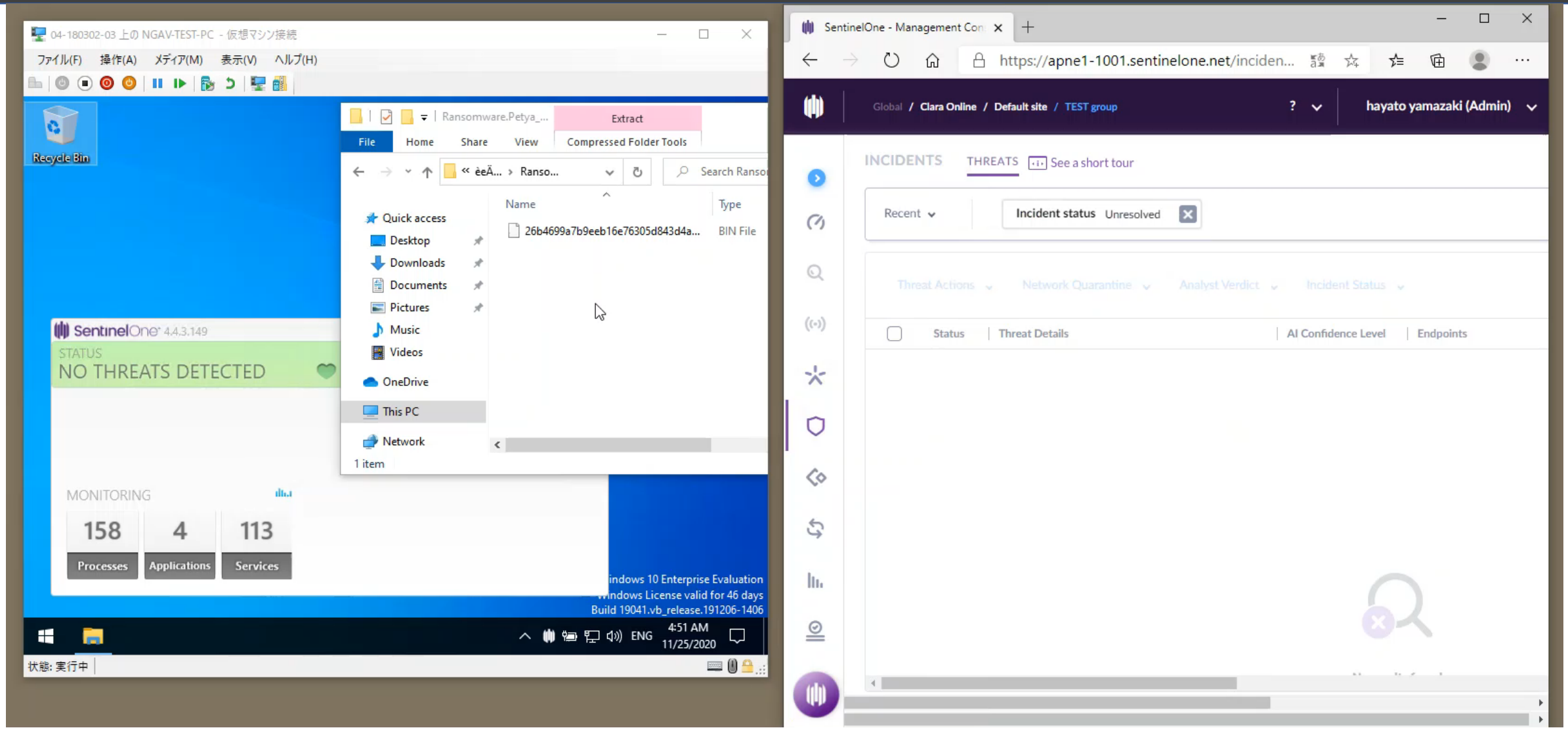
比較検討

- 従来型、次世代型より約10製品を比較
- **価格、機能、運用、サポート品質、カルチャー、など**

1）本物のウィルスを使い感染と対処

- スマホのテザリング接続したPCに仮想マシンを構築して検証
- ふるまい検知や、その時の自動防御の理解
- **実際に感染した際の対処方法の把握**

導入検証のコツ - 本物のウィルスを動作させる(自動防御)



1）本物のウィルスを使い感染と対処

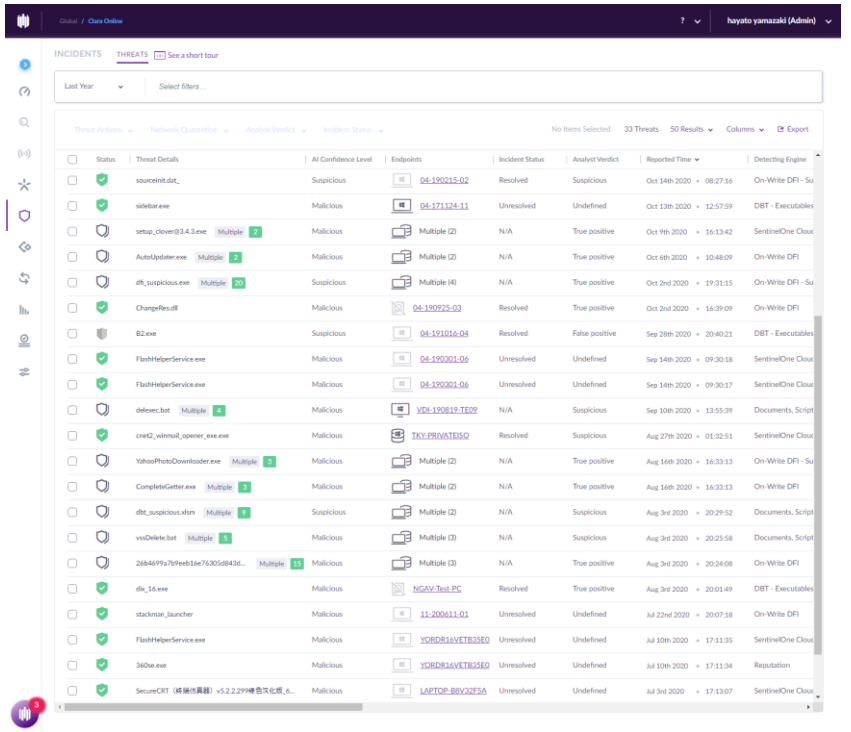
- スマホのテザリング接続したPCに仮想マシンを構築して検証
- ふるまい検知や、その時の自動防御の理解
- 実際に感染した際の対処方法の把握

2）実業務の環境で検証

- **業務環境下での干渉問題の有無**
- **誤検知(頻度)の体験と、検知内容や対処方法の把握**

導入検証のコツ – 干渉問題や検出例

- **一般**
  - Windowsデスクトップガジェット
  - PCメーカーのプリインストールアプリ
  - 広告系アプリ(e.g. JWord)
- **エンジニア関連**
  - XAMPPに含まれるランチャーモジュール
  - ハッシュファイルを変換するプログラム
- **中国関連**
  - 中華圏のセキュリティソフトウェア(e.g. 360)
  - 国境を超える特殊なネットワーク系ソフトウェア
  - 中華圏で取得されたFlashプレイヤー



1）本物のウィルスを使い感染と対処

2）実業務の環境で検証

- 製品ごとの違いが明確になり、比較は容易
- 運用の負荷についても予めの想定が可能
  (運用イメージを具体化)

自社の運用環境に適した製品を選定

1. 既存EDRの課題をクリア → 効率的な運用、負荷の軽減

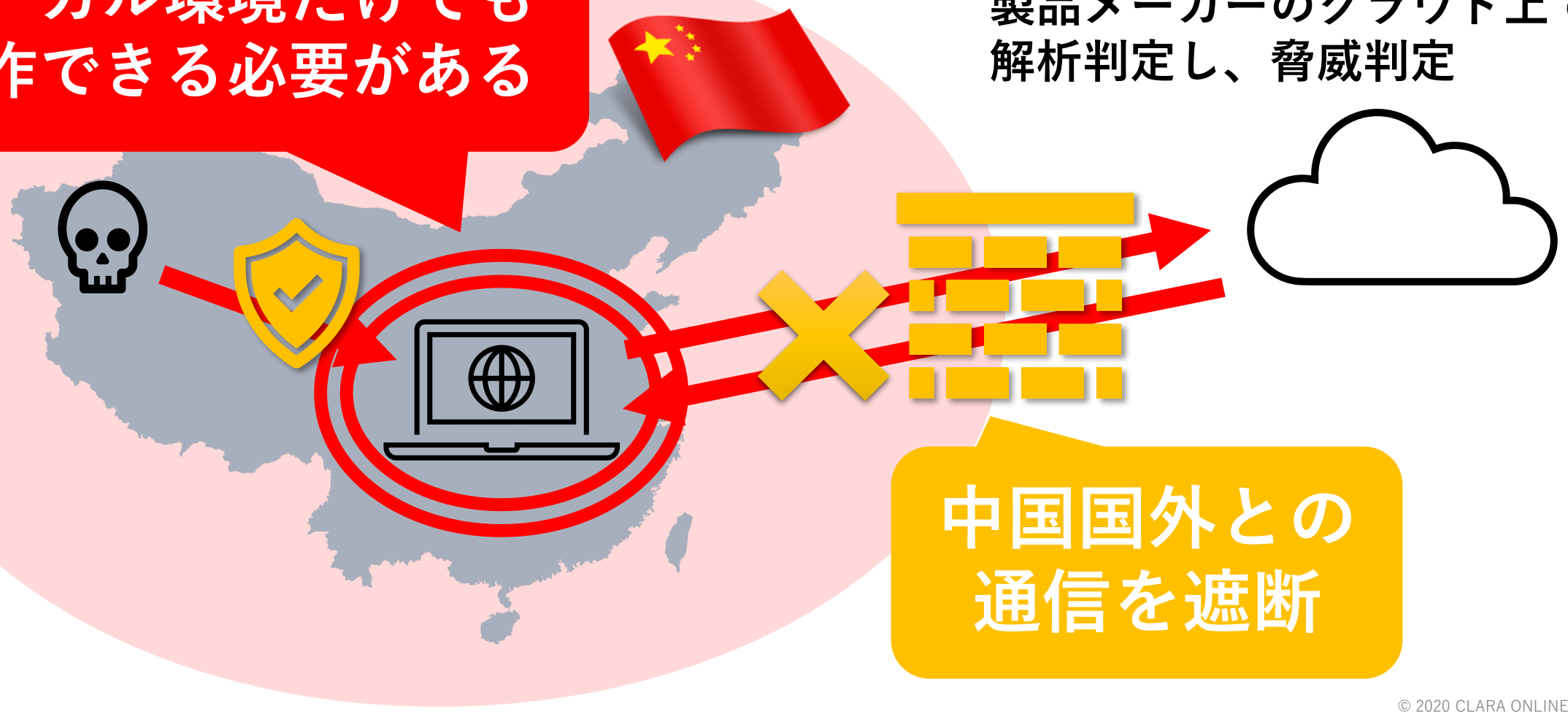
- 自律的(Autonomous)、能動的(Active)EDRとして**できる限りの自動化**
- 専門性の高い操作を減らし、脅威発生から対応までの**工数削減**

2. 次世代型の弱点をクリア

- **ディスクスキャン**によるウィルス隔離
- **オフラインでの動作**

ローカル環境だけでも
動作できる必要がある

製品メーカーのクラウド上で
解析判定し、脅威判定



中国国外との
通信を遮断

- **既存EDRの課題をクリア** → **効率的な運用、負荷の軽減**
  - 自律的(Autonomous)、能動的(Active)EDRとして**できる限りの自動化**
  - 専門性の高い操作を減らし、脅威発生から対応までの**工数削減**

- **次世代型の弱点をクリア** → **既存環境からの移行にスムーズ**
  - ディスクスキャンによるウィルス隔離
  - オフラインでの動作

SentinelOne™

The Border

https://www.clara.jp/wsi/

CLARA ONLINE

WSI Work Style Innovation

WSIとは？

ソリューション

プラン

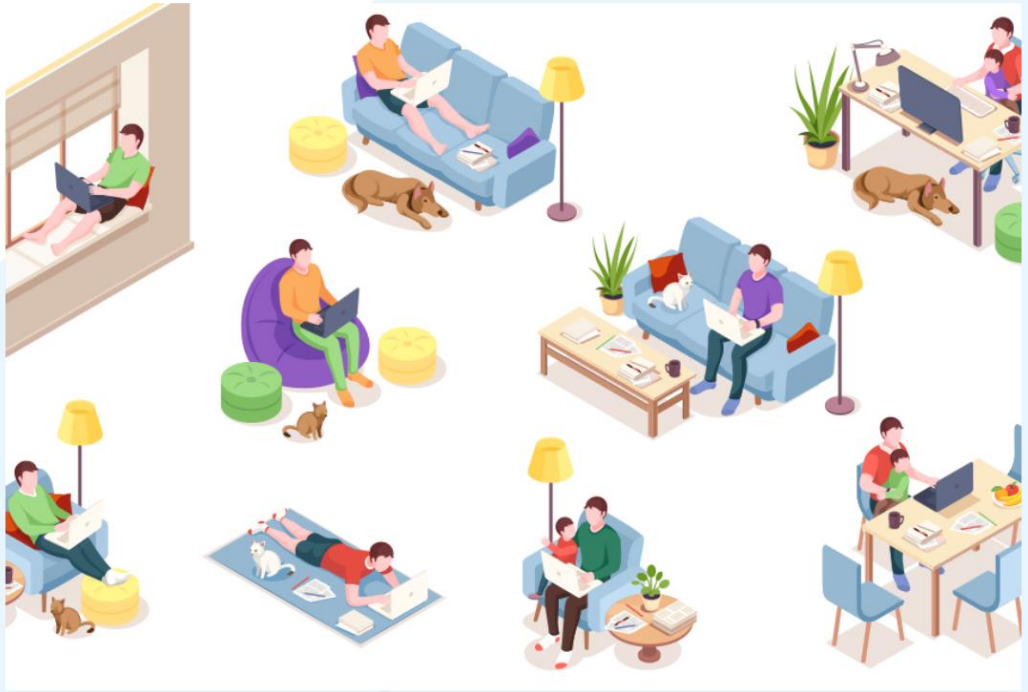
ゼロトラストとは

提供機能一覧 →

30日間無料トライアル
お申し込み

Work Style Innovation

ゼロトラストベースのセキュアなテレワーク環境を実現するクラウド活用ソリューションをワンパッケージで提供します。



SCROLL

CLARA ONLINE

The Border

ご視聴ありがとうございました