金融業界必見！今考えるべきセキュリティとは
～2024年のペネトレーションテストとIaaSセキュリティ最新トレンド～

東京エレクトロン デバイス株式会社
CN営業本部　アカウント第二営業部
寺田 涼太

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

本日の内容

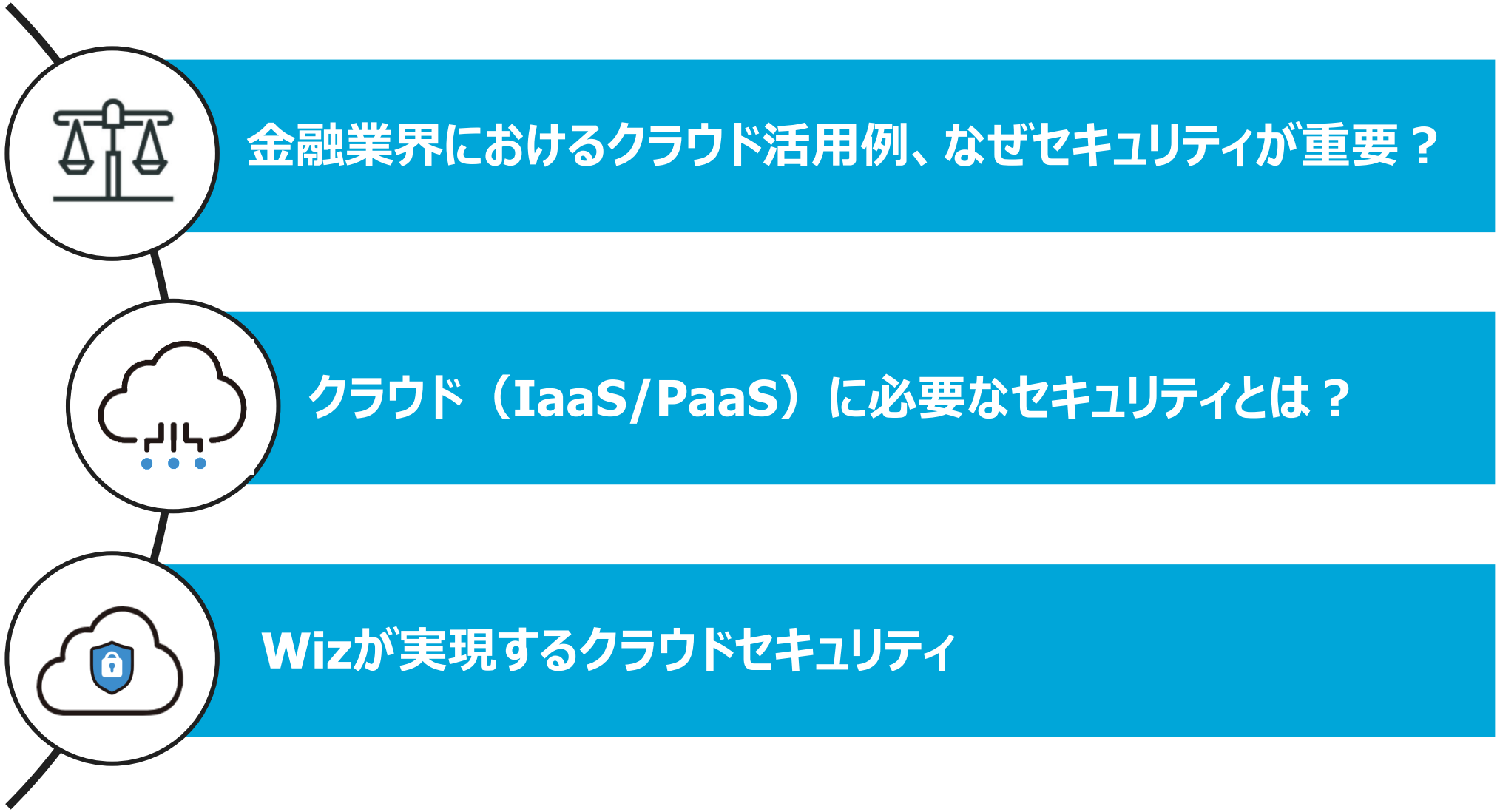
- 金融業界でも活用が加速するクラウド環境に対するセキュリティ
- 金融業界におけるセキュリティ運用の理想像
- 東京エレクトロンデバイスについて

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融業界でも活用が加速する
クラウド環境に対するセキュリティ

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融業界でも活用が加速するクラウド環境に対するセキュリティ



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融業界におけるクラウド活用例

インターネットバンキングのデータベースをAWSに移行

ビジネスの俊敏性、柔軟性の確保を目的としてインターネットバンキングのデータベースをAWSに移行

コンタクトセンターをAWSに移行

レイアウト変更や増員へのスピーディーな対応、顧客サービスの拡充を目的としてコンタクトセンターをAWSに移行

情報系、勘定系などのバンキングシステムをAuzreに移行

社内業務システム、情報系システムのみならず勘定系システムをAzure等のクラウド移行する企業も登場

CXの観点からIaaS/PaaSを活用したスピーディーなサービス拡充が求められている

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウド（IaaS/PaaS）活用においてセキュリティが重要な理由

クラウド環境を狙った サイバー攻撃の増加

情報資産はクラウド側に集約されつつあり、この領域を狙ったサイバー攻撃が増加

クラウド環境で広く利用されているAPIを悪用した**不正アクセス**やクラウド上のシステムを狙った**ランサムウェア**によるサイバー攻撃など手口も巧妙化

クラウド環境特有の セキュリティリスク

物理インフラに対するセキュリティはプロバイダー側が担保するが、クラウド上のアプリケーションやデータのセキュリティ設定、アクセス管理等は**利用者である企業側が責任を持つ**

クラウドサービスの複雑さ

VM、コンテナ、サーバーレス環境など様々なワークロードが存在し、**セキュリティの統制**が求められる

新しいサービス、バージョンが次々とリリースされ、利用者が**最新の仕様を把握することが難しい**

高度なセキュリティ対策が求められる金融業界において
IaaS/PaaS環境に対しても十分なセキュリティ対策が求められる

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

クラウド（IaaS/PaaS）に必要なセキュリティとは？

よく挙がってくるキーワードは・・・

CSPM
Cloud Security Posture Management

IaaS/PaaSにおける管理の可視化

- リソースの可視化
- 設定ミス
- コンプライアンス診断

CWPP
Cloud Workload Protection Platform

クラウド上のワークロードの監視・保護

- マルウェアなどの脅威検知
- 脆弱性スキャン
- 攻撃の可視化/防御

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

CSPM、CWPPだけでは網羅できないセキュリティ課題

各部/利用者が自由にリソースを作るので
全体像が把握できていない

新しいサービスが次々登場しているが
利用によるリスクが把握できず躊躇

クラウド上にKubernetes環境もあるが
他環境と統合的に運用ができない

アタックサーフェスや侵入経路が把握できて
おらず、対策ができていない

日々新しいリスクが登場するが
優先対応すべき問題の整理に苦慮

マルチアカウント・クラウドを横断する
資産管理やリスク分析ができない

そもそもどこにリスクがあるか
把握しきれていない

IaaSのアカウント設定や
管理者権限の可視化や制御ができない

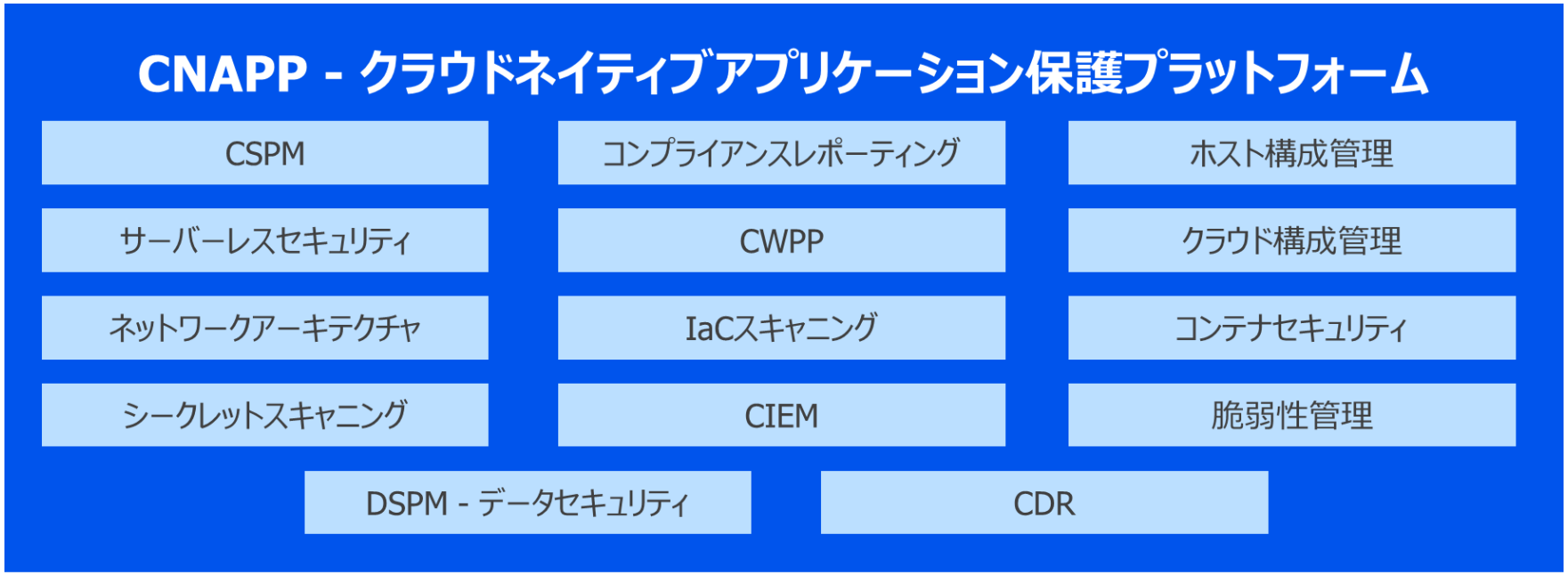
インフラ構築時のコードが安全であることの
確認に時間がかかってしまう

CSPM・CWPPだけでなく、統合されたセキュリティプラットフォームが必要

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

CNAPPとは？

CNAPP＝**C**loud **N**ative **A**pplication **P**rotection **P**latform
IaaS/PaaS環境における複数の異なるセキュリティ機能を１つのプラットフォームとして統合

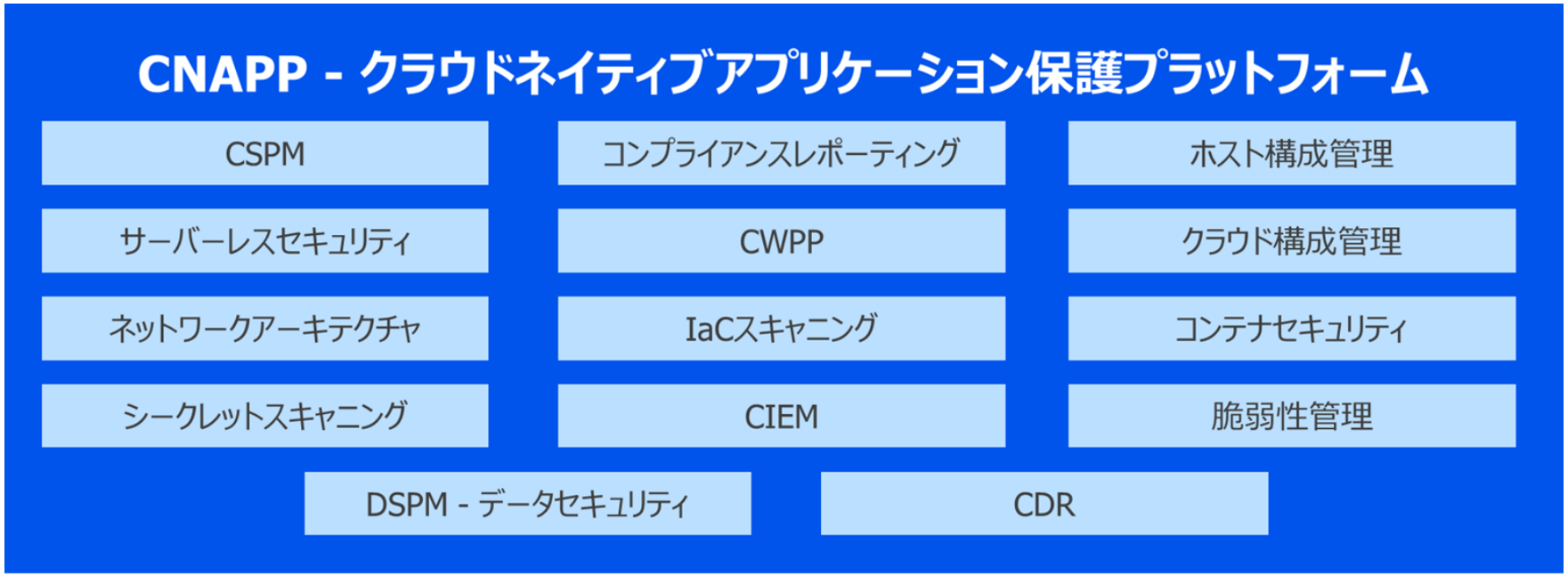


セキュリティツールの複雑さを軽減し、セキュリティの向上とコンプライアンスへの準拠、開発から運用までのガイドラインとして効果を発揮します。

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

CNAPPとは？

CNAPP＝Cloud Native Applicati n
複数の異なるセキュリティ対策と保護 フォームとして統合し、提供



クラウドで構築および実行するすべてのものを保護する

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Wiz CNAPPとは

クラウドで構築および実行する すべてのものを保護する

- 設立：2020年
- 本社：米国ニューヨーク
- 資本：＄900M
- 世界で最も急速に成長しているソフトウェア会社
- 設立18カ月で売上1億ドル、設立3年で評価額100億ドル超の“デカコーン”企業
- Fortune100のうち40%が導入
- 市場評価額：1.8兆円

Wiz CNAPPの主なセキュリティ機能	
CSPM	クラウドの構成を診断、リスクとなる設定を特定
CIEM	クラウドアイデンティティの権限と影響範囲を可視化
CWPP	仮想マシン、コンテナ、サーバーレスなどワークロードを保護
Kubernetes & コンテナセキュリティ	Kubernetesやコンテナの実行基盤やコンテナ自身の保護
脆弱性管理	ワークロードの脆弱性を特定、管理
IaCスキャニング	IaCコードをデプロイ前にスキャンしセキュリティ診断
コンプライアンス対応	様々なレギュレーションに対応したコンプライアンスレポートを提供
DSPM	機密データの保存場所を特定し、リスクとなる構成を特定
シークレットスキャン	シークレットの保存場所を特定し、リスクとなる構成を特定
CDR	クラウドの脅威検知と対応

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Wiz CNAPPの特徴

1
エージェントレス・スキャン

サーバレス
コンテナ
仮想マシン
PaaS

試しやすい

2
クラウドアセスメントの実行

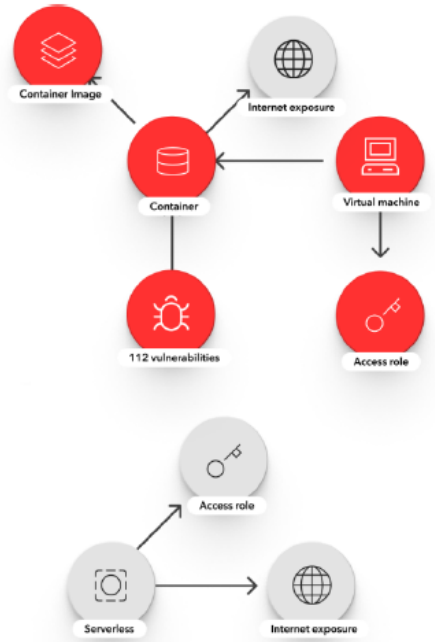
基本的なスキャン
脆弱性とパッチ不足
設定ミス
マルウェア
機密データの発見

クラウド・リスクエンジン
外部への情報漏えい
過剰な権限設定
公開シークレット
ラテラルムーブメントの移動経路

Wiz脅威リサーチ
クラウドの新しい脆弱性と攻撃

オールインワン

3
最重要リスクの優先順位付け



分かりやすい

4
必要な連携が簡単に可能

インテグレーション
20+ インテグレーション

クラウドの修復
ワンクリック修復
セキュリティ対応の自動化
修復ガイダンス

CI/CDのガイドライン
スタック全体で１つのポリシー
コンテナおよびVMイメージのスキャン
IaCテンプレートスキャン
K8アドミッションコントローラー

導入しやすい

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

まとめ

- **WizはIaaS/PaaSに必要なセキュリティ機能を全て提供**
  - ・マルチクラウドに対応
  - ・セキュリティ統制、運用負荷を大幅に削減
  - ・エージェントレスでシステム影響を気にせず利用可能
  - ・コンテキスト化により、重大なリスクを特定

他製品との組合せで更なる効率化・セキュリティ強化も可能

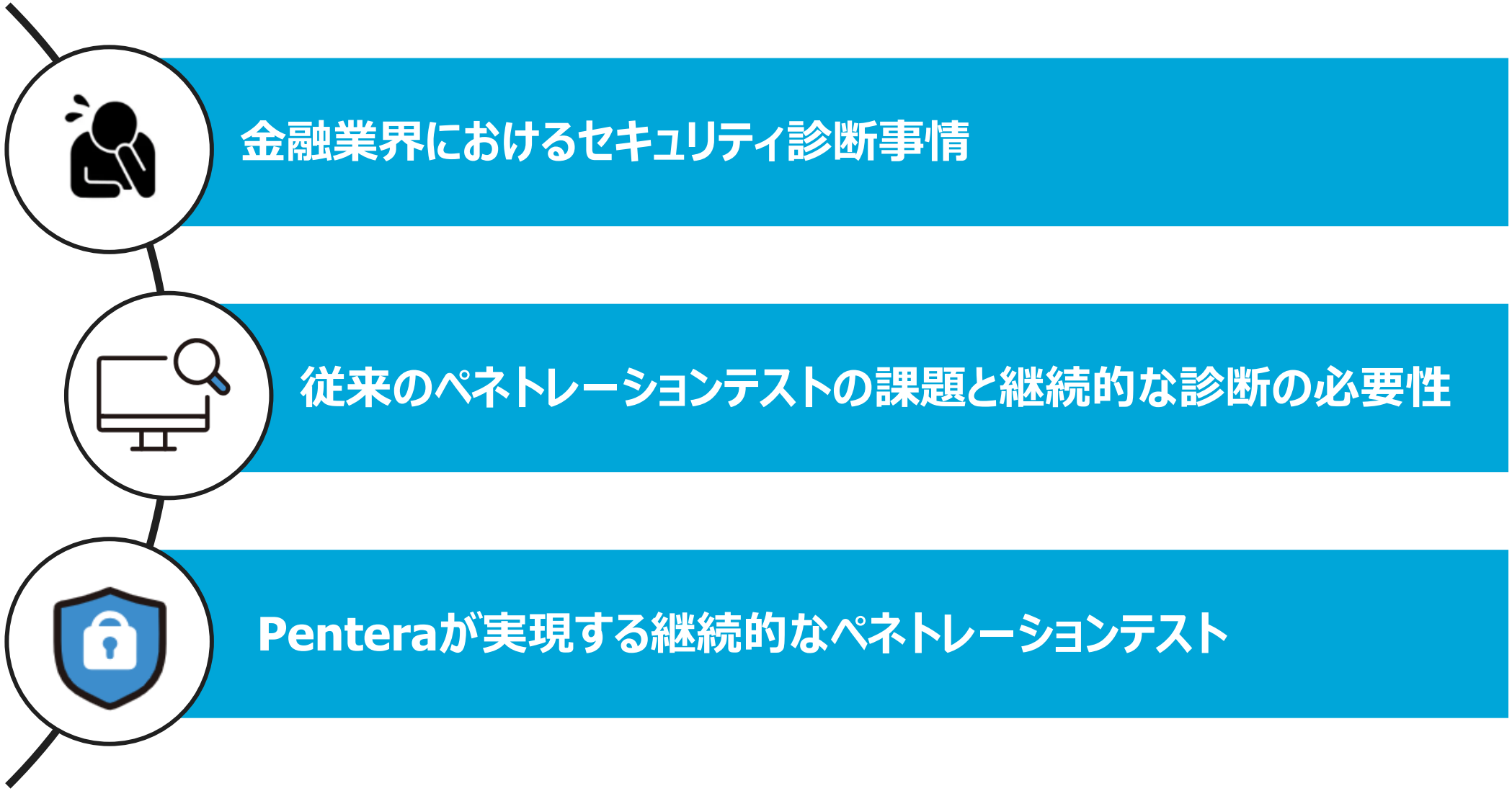
HashiCorp Vault	クラウド上にあるシークレット情報（アクセスキー等）の動的管理
HashiCorp Terraform	クラウド上におけるインフラ設定のコード化（IaC）とガバナンス統制
netskope	野良クラウドをそもそも作らせない(URLフィルタ等) SaaS側の制御も行いたい

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融業界におけるセキュリティ運用の理想像

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融業界におけるセキュリティ運用の理想像とは



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

金融業界のセキュリティ診断事情

金融分野におけるサイバーセキュリティ強化に向けた取組方針(Ver.3.0)

（1）モニタリング・演習の高度化 - ①サイバーセキュリティ管理体制の検証

（a）大手行等
グローバルに業務を展開している3メガバンクについては、サイバー攻撃の脅威動向の変化や海外大手金融機関における先進事例を参考にしたサイバーセキュリティの高度化に着目しつつ、**通年検査においてサイバーセキュリティ管理態勢を検証**する。

（b）地域金融機関
金融機関がリスク管理を高度化すべき範囲が拡大している中で、**サイバーセキュリティに関する基礎的な管理態勢の実効性を向上させるために、継続的な取組みが必要である。**こうした状況を踏まえ、リスクが高いと考えられる金融機関に対する検査の実施を含め、サイバーセキュリティ管理態勢の実効性を検証する。

（c）その他業態
証券会社や外国為替証拠金取引業者については、サイバーセキュリティに関する基礎的な取組みにおいて進捗が認められる一方、不正アクセス等による被害も複数発生していることを踏まえ、**引き続き、検査・モニタリングを通じて、サイバーセキュリティ管理態勢を検証する。**保険会社についても同様に、インシデントの発生状況等を踏まえ、**引き続き、検査・モニタリングを通じ、リスクベースでサイバーセキュリティ管理態勢を検証する。**

出典：金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）

金融業界では規模・業態問わずセキュリティ診断体制の見直しと高度化が求められる

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

セキュリティ診断の見直し・高度化の方法

自社のセキュリティ環境をより堅牢にするために必要なポイント

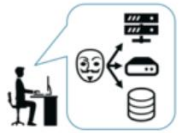
- **攻撃者視点での疑似攻撃**によって被害範囲を把握する
- 実際に**攻撃者が利用する脆弱性を可視化**し優先的に対応する
- 導入している**セキュリティ製品の有効性を確認**する

攻撃者視点でのセキュリティ診断(ペネトレーションテスト）が必要になる

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

従来（マニュアル）のペネトレーションの課題

1回の実施に時間がかかり過ぎてしまう



その他にも・・・
限られた視点
ペンテスターの能力依存
高額なコスト
第三者による実施
最新脅威に対する調査の確約無し

年１回の実施で有効性はあるのか

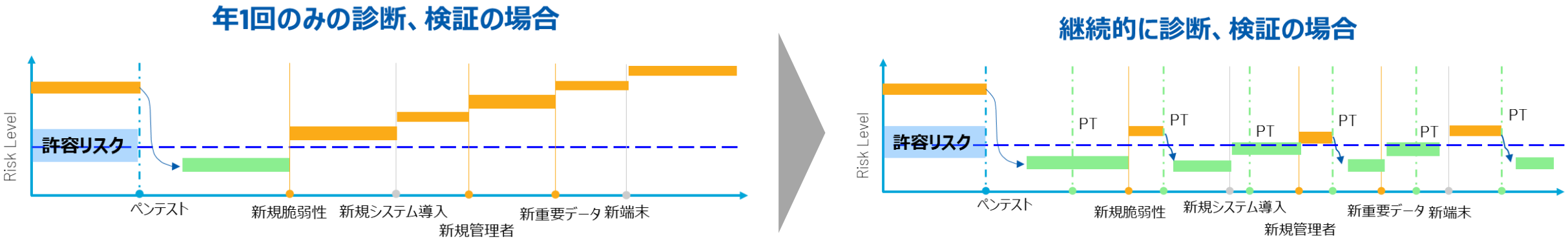
システムは24/365で脅威にさらされています
ワンショットの検査はハッカー視点を持ったテストと言えますか？

マニュアル作業の限界、ペネトレーションテストに変革が必要

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

セキュリティ運用の理想像

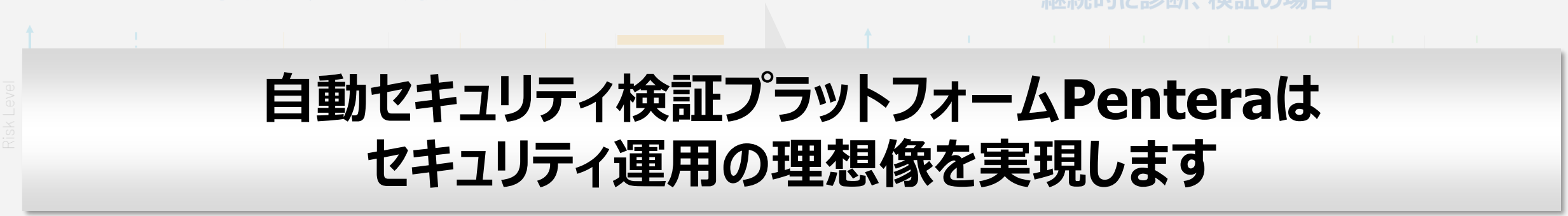
- **セキュリティ検証を自動化**することで運用負荷をかけずに対応できる
- **継続的な診断**によって自社のセキュリティを常に安全な状態にできる
- 特定のシステムのみではなく、社内システム全体に対する**網羅的な診断**ができる



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

セキュリティ運用の理想像

- **セキュリティ検証を自動化**することで運用負荷をかけずに対応できる
- **継続的な診断**によって自社のセキュリティを常に安全な状態にできる
- 特定のシステムのみではなく、社内システム全体に対する**継続的な診断**ができる



自動セキュリティ検証プラットフォームPenteraは
セキュリティ運用の理想像を実現します

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

会社紹介

PENTERA

Autmated Security Validation

自動化されたセキュリティ検証

ミッション

Forging your Cyber Resilience
with Continuous Penetration Testing

継続的なペネトレーションテストによる
サイバーレジリエンスの構築

- 本社：イスラエル
- 販売およびサポート拠点：ボストン、トロント、ロンドン
  - APAC（シンガポール、日本、オーストラリア）
- 従業員数：350人以上
- 顧客：銀行、保険、リテール、法律事務所、ヘルスケア、政府系など
  60か国 1000社以上
- イスラエル国防軍エリートサイバー部隊出身者による強力なリサーチチーム
- Gartner社によるカテゴリー　”Network Penetration Testing”
- 各種受賞
- 準拠

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Penteraの特徴

PENTERA

エージェントレス

他のツールと異なりインストールは不要なため、
稼働しているシステムへの変更は不要です。

実際の攻撃

脆弱性を洗い出すだけでは無く、疑似攻撃を実施し、
脆弱性が悪用された場合の被害想定が可能です。
導入されているセキュリティ製品の対処能力も評価可能です。

継続的な診断

日々変化する環境、脆弱性に対して、定期的な検査を実施し、
セキュリティ状況の変化に素早く対処が可能です。

網羅的な診断

主要なサーバーだけでは無く、IT資産全体の診断が可能で、
いわゆるシャドウITなども発見可能です。

優先修復

攻撃の結果を基に環境に沿った対処すべき問題点の
優先度付けを行い、問題点の修復手順を提示します。

クローズドな診断

インターネットに接続していない環境でも診断ができます。

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

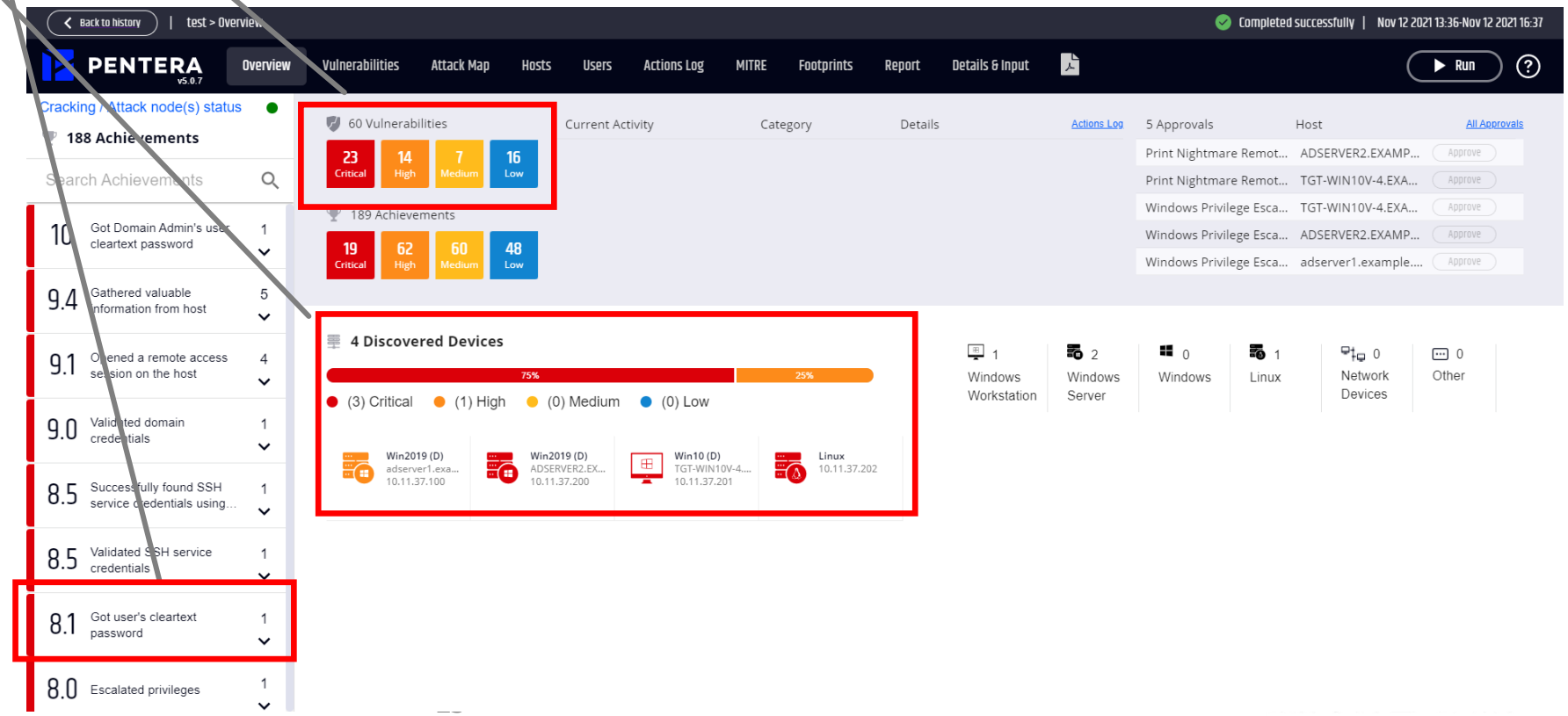
Penteraがもたらす効果

- **時間をかけず能動的な確認が可能に**

1. 未対応の脆弱性のチェック
2. パスワードの強度のチェック
3. 野良端末情報のチェック

- **発見したセキュリティホールへの改善の簡易化**

1. 対応すべき箇所の優先度の把握
2. GUIに記載の改善方法で対応方法の把握

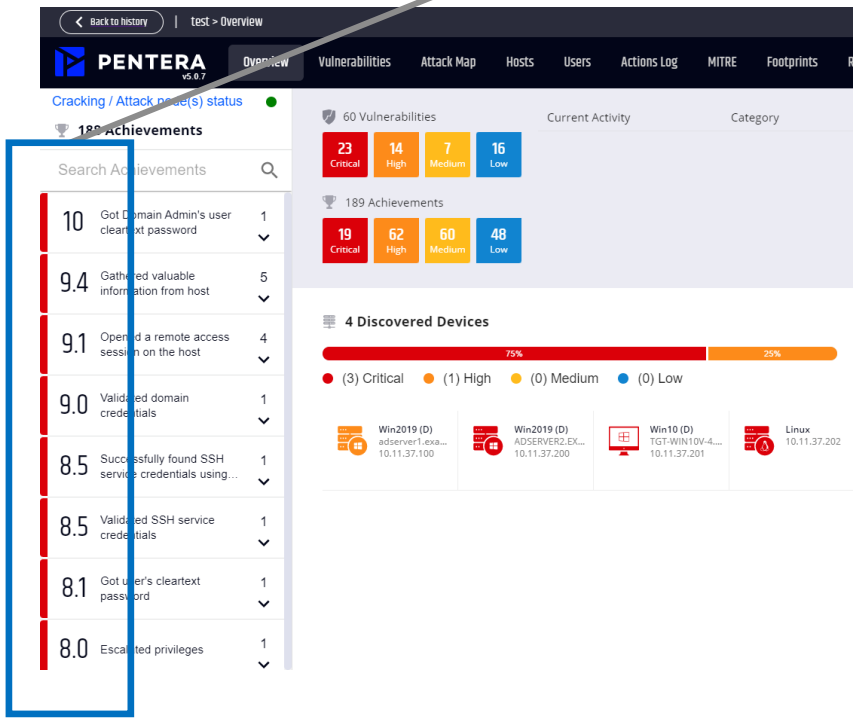


Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Penteraがもたらす効果

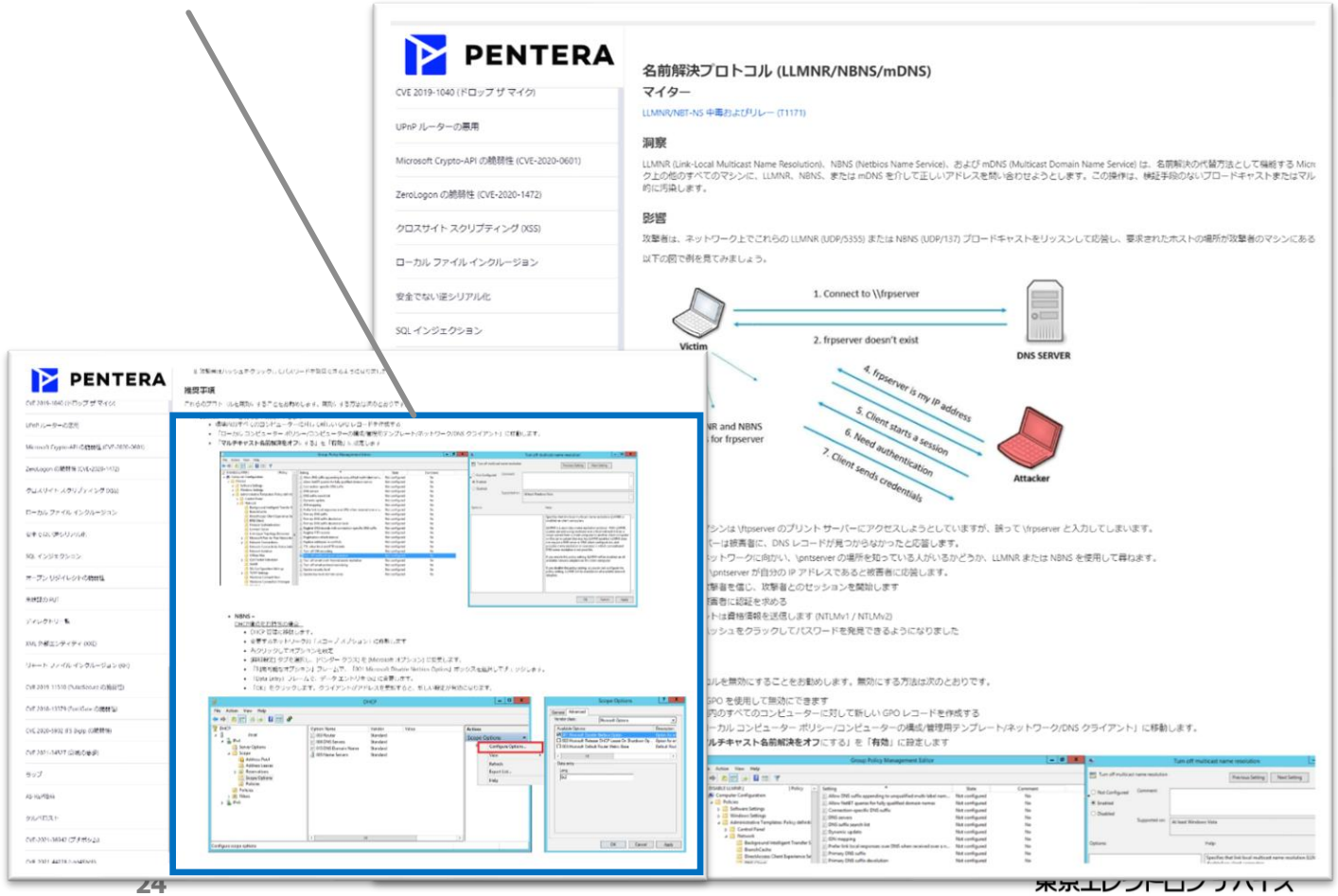
- **時間をかけず能動的な確認が可能に**

1. 未対応の脆弱性のチェック
2. パスワードの強度のチェック
3. 野良端末情報のチェック



- **発見したセキュリティホールへの改善の簡易化**

1. 対応すべき箇所の優先度の把握
2. GUIに記載の改善方法で対応方法の把握



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Pentera提供する価値

自動化された診断による
時間、運用負荷の削減

・IP範囲を指定するだけであとは自動で診断
数か月かけて実施したテストを短時間で実行

・エージェントレスのため、システムへの影響は最小限

・脅威に対する対応の優先順位付け

・テスト実施後の分析・レポート自動発行

継続的な診断による
万全なセキュリティ体制の構築

・リソース、スキル、コストを気にせず、
網羅的に何度でも診断が可能

・実際に攻撃を受けた場合の影響範囲を診断可能

・自社にとって本当に必要なセキュリティ対策を提示

・最新の脅威に対応した診断が可能

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロンデバイスについて

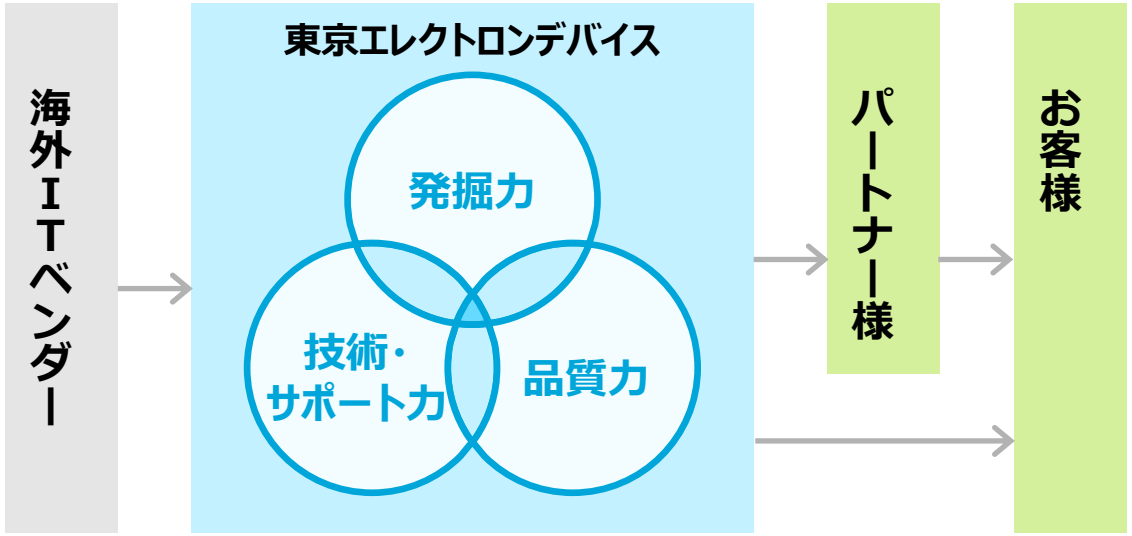
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロンデバイス 会社紹介

会社概要

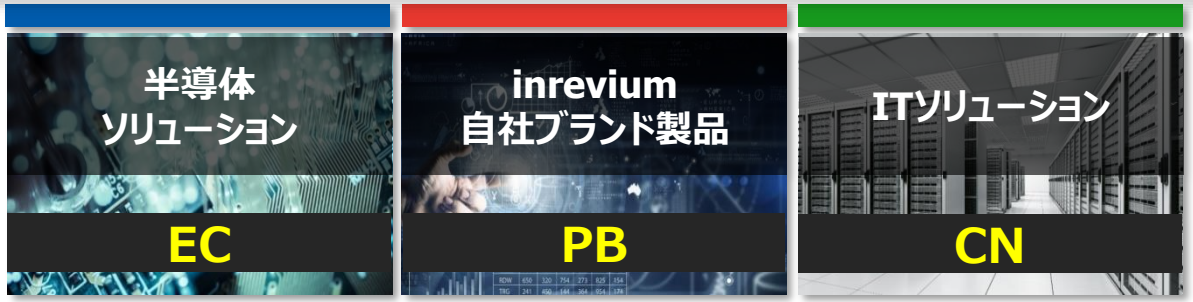
会社名	： 東京エレクトロン デバイス株式会社（TED）
設立	： 1986年3月3日
代表	： 代表取締役社長　徳重　敦之
株式	： 東京証券取引所 プライム市場（証券コード：2760）
資本金	： 24億9千5百万円
売上高	： 2,403億50百万円（2023年3月期）
従業員	： 連結: 1,318名（2023年3月31日現在）

CN BU



「**発掘力**」「**技術・サポートカ**」「**品質力**」を活かし
お客様が求める最先端技術を「**高品質**」で提供

事業内容



CNフォーカスエリア

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

CN BU ITソリューション一覧

Connect Beyond

Security

テレワーク/クラウドアクセス関連ソリューション

CASB	SWG	ZTNA	IDaas
SSE/SASE: netskope			SSO/多要素認証: okta

エンドポイント	HSM	シークレット管理
Active EDR/XDR: SentinelOne	ENTRUST, THALES	Hashicorp: HashiCorp Vault

社内/トラストネットワーク関連ソリューション

Firewall	VPN	WAF
paloalto NETWORKS, FORTINET	f5	f5 Distributed Cloud Services

Wi-Fi	DNS/DHCP	NDR
Cognitive Wi-Fi: ARISTA, Extreme networks	DNSセキュリティ: infoblox.	ARISTA

セキュリティ診断

ASV
PenTest、ASM: PENTERA

データ分析

SIEM/SOAR/UEBA
DEVO

その他取扱い製品

その他の取り扱い製品については
以下のWebよりご覧ください。

https://cn.teldevice.co.jp/

Infrastructure

クラウド管理

CSPM/SSPM	IaC	CNAPP
netskope	Hashicorp: HashiCorp Terraform	WIZ

クラウド

パブリッククラウド	
aws	Azure

AI/DLソリューション

GPU	Accelerator
NVIDIA	cerebras

仮想化基盤ソリューション

HCI	3Tier
NUTANIX	PURESTORAGE

ファイルストレージソリューション

Scale Out		Scale Up
Power Scale: DELL Technologies	PURESTORAGE	Unity XT: DELL Technologies

ネットワークソリューション

IP Clos	L2/L3スイッチ		ADC
JUNIPER NETWORKS	DCNW: ARISTA, NVIDIA	キャンパス: Extreme networks	f5

バックアップソリューション

クラウドバックアップ対応	
rubrik	VEEAM

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス

共に創る　新たな価値を

東京エレクトロン デバイス

Copyright © Tokyo Electron Device LTD. All Rights Reserved.