



# 金融庁の新ガイドラインに基づく最新セキュリティ！ CTEMとCNAPPを徹底解説

東京エレクトロン デバイス株式会社

CNBU CN営業本部 アカウント第二営業部  
久山 慶

**01**

**金融分野におけるサイバーセキュリティガイドラインについて..... P.3**

**02**

**ペネトレーションテストに関する内容とCTEMについて..... P.5**

**03**

**クラウドセキュリティに関する内容とCNAPPについて ..... P.17**

**04**

**東京エレクトロンデバイスの紹介とまとめ ..... P.33**

**01**

**金融分野におけるサイバーセキュリティガイドラインについて..... P.3**

02

ペネトレーションテストに関する内容とCTEMについて..... P.5

03

クラウドセキュリティに関する内容とCNAPPについて ..... P.17

04

東京エレクトロンデバイスの紹介とまとめ ..... P.33

# 金融分野におけるサイバーセキュリティガイドラインについて

## ● 目的

- 金融機関に対してサイバーセキュリティに関するより詳細な対応要件や対応事項を示すため

## ● ターゲット

- 銀行、生命保険、損害保険、証券、資金決済分野の事業者など、金融機関全般
- 伝統的な金融機関だけでなく、Fintech事業者等も対象

## ● 特徴

- 「基本的な対応事項」と「対応が望ましい事項」が明言されている

## ● 今回のテーマ

- ペネトレーションテスト
- クラウド（IaaS/PaaS）のセキュリティ

金融分野におけるサイバーセキュリティに関する  
ガイドライン

令和6年10月4日  
金融庁

01

金融分野におけるサイバーセキュリティガイドラインについて..... P.3

02

**ペネトレーションテストに関する内容とCTEMについて..... P.5**

03

クラウドセキュリティに関する内容とCNAPPについて ..... P.17

04

東京エレクトロンデバイスの紹介とまとめ ..... P.33

## ガイドラインの内容① : 2.2.2.4 継続的な改善活動

### 【基本的な対応事項】

- **内外の環境変化に応じて**セキュリティリスク評価のプロセスを  
**少なくとも年に1回**は実施し、**継続的な改善活動**をおこなうこと
  
- サイバーセキュリティリスク管理体制の整備状況及び運用状況の有効性を  
**少なくとも1年に1回は評価**し、改善すること
  
- 演習・訓練、脆弱性診断及びペネトレーションテスト、監査、リスク評価、及び実際のインシデントから得られた推奨事項、発見事項、教訓については、関連手続等に従って改善すること

参照 : <https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf>

## ガイドラインの内容②：2.2.4 脆弱性診断及びペネトレーションテスト

※ペネトレーションテストに関する内容のみを抜粋

### 【基本的な対応】

- リスクの大きさやシステムの重要度を考慮し、**定期的に脆弱性診断およびペネトレーションテストを実施**すること
- **特定された問題を優先順位付け**し、対応方法と対応期限を決定し、対応状況を管理すること
- 重要な結果については**迅速に経営陣に報告**すること

### 【対応が望ましい事項】

- インターネットに接続していない**VPN網や内部環境も対象に**すること
- **定期的に脅威ベースのペネトレーションテスト（TLPT）を実施**すること

参照：<https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf>

## ガイドラインの内容③ : 2.2.4 脆弱性診断及びペネトレーションテスト

※ペネトレーションテストに関する内容のみを抜粋


### 【対応が望ましい事項】

#### TLPT実施時の留意点

- 脅威インテリジェンスを踏まえ、**実際の攻撃者が行うテクニック**を用いたテストを行うこと
- 関係主体に対するサービスの提供に影響を及ぼしうる、深刻だが**現実に起こり得る脅威シナリオ**を考慮すること
- **ブルーチーム（防御側）のインシデント対応能力を評価**すること
- **本番環境を利用し、ブルーチーム（防御側）に予告なくテストを実施**すること
- **自組織の内部人材によるペネトレーションテスト**を実施すること
- 定期的にテストの方法と結果をレビューし、テストベンダーの交代要否を検討すること

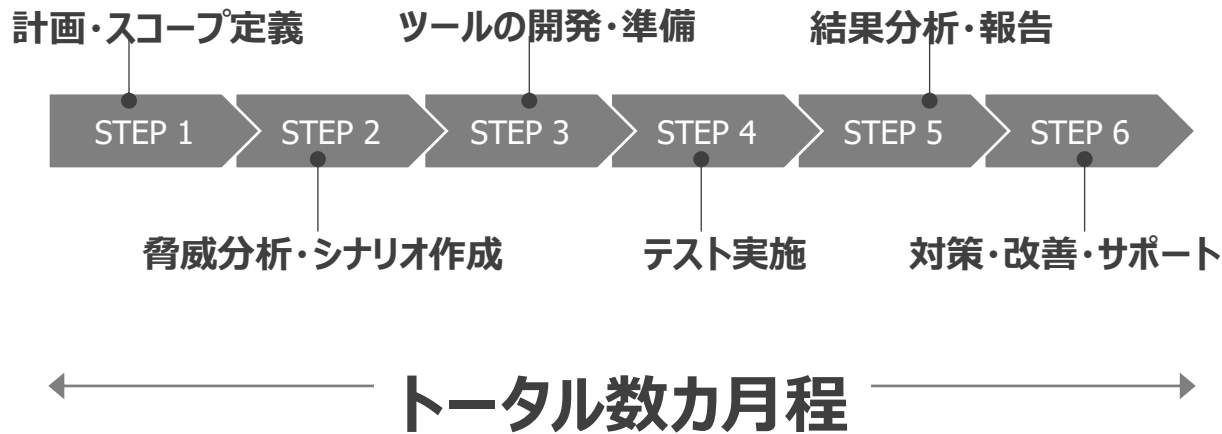
参照 : <https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf>





従来のペネトレーションテストの手法で  
対応することはできるのでしょうか

## テストの流れ



**定期的なペネトレーションテスト  
継続的な改善活動ができない**

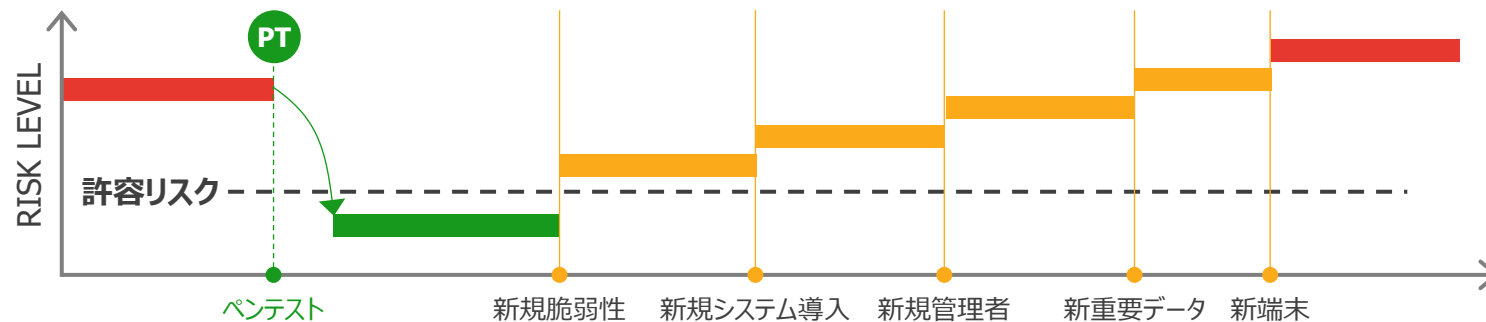
その他にも、、、

- 迅速に経営陣に報告できない
- 内部人材によるテストではない

**特に定期的なペネトレーションテスト、継続的な改善活動が難しい**

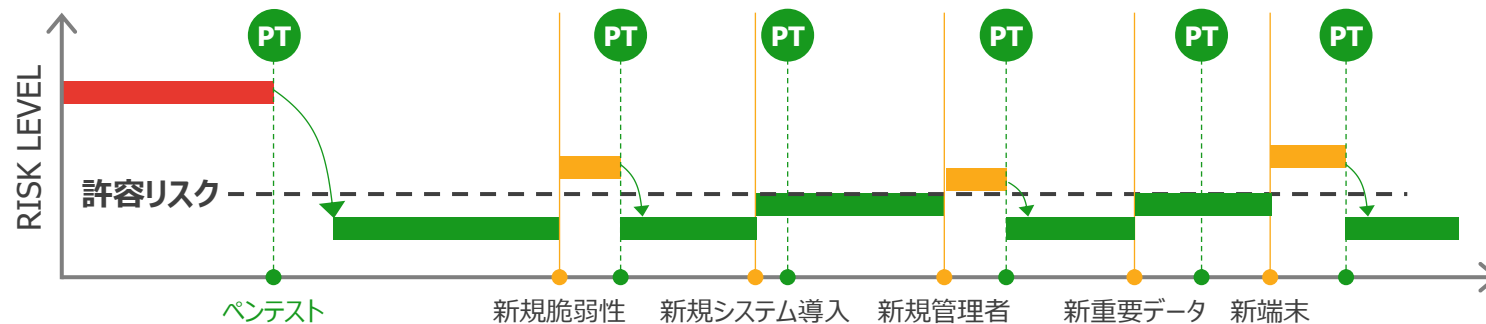
# ペネトレーションテストの頻度について

## ▶▶ 年1回のみでのペネトレーションテストの場合



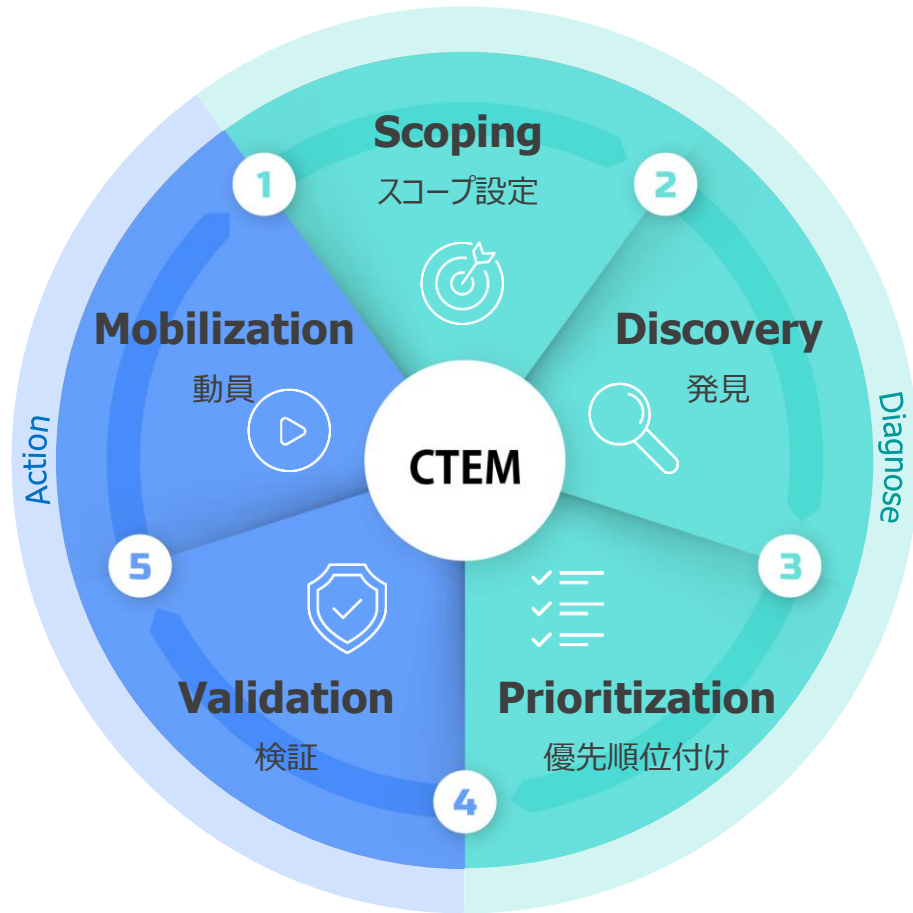
いつの間にか  
セキュリティリスクが高い状態に

## ▶▶ 継続的なペネトレーションテストの場合



組織内外の環境変化に応じて  
高まるリスクに対応

**年に複数回の継続的なセキュリティ検証が必要**



## Continuous Threat Exposure Management = 継続的な脅威エクスポージャー管理

- 某リサーチ会社が提唱する新たなセキュリティアプローチ
- 脅威にさらされている資産を、継続的に評価し、リスクを特定、対処するための戦略
- 組織の内部資産と外部公開資産の両方を対象とし、組織全体のリスクを管理

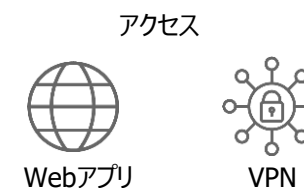
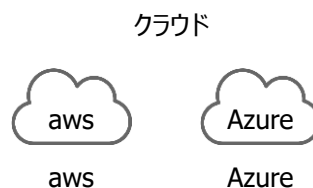
CTEMへの注目が国内でも高まっている



## Automated Security Validation (自動セキュリティ検証プラットフォーム)

対象のPC、サーバー等のシステムに対して安全に攻撃を仕掛け、  
攻撃の結果を基に、改善すべき箇所を確認できる製品





# Penteraが提供するメリット①

## 金融庁のガイドラインの内容

定期的にペネトレーションテストを実施すること

特定された問題を優先順位付けし、対応方法と対応期限を決定し、対応状況を管理すること

重要な結果は迅速に経営陣に報告すること

インターネットに接続していないVPN網や内部環境も対象にすること

脅威インテリジェンスを踏まえ、実際の攻撃者が行うテクニックを用いたテストを行うこと

## Penteraなら対応できます！

**内外の環境変化に応じて**任意のタイミングもしくはスケジューリングして定期的にテストを実施

汎用的な脆弱性のスコアではなく、**実際の攻撃結果を基に重要度に応じて優先順位付け**

テスト結果のレポートを即時自動発行

スタンドアロンで稼働し、**インターネットに接続していない環境も対象にできる**

Penteraのリサーチチームが収集した情報をもとに**実際の攻撃者が行う水準のテクニック**を用いたテストが可能

## Penteraが提供するメリット②

### 金融庁のガイドラインの内容

深刻だが現実には起こりうる脅威シナリオを  
テスト計画において考慮すること

ブルーチーム(防御側)の  
インシデント対応能力を評価すること

本番環境を利用し、ブルーチーム（防御側）に  
予告なくテストを実施すること

自組織の内部人材による  
ペネトレーションテストを実施すること

継続的な改善活動を実施すること

### Penteraなら対応できます！

検査対象に対して**可能な攻撃手法をすべて**実行し、  
「現実には起こりうる脅威シナリオ」を網羅的にテスト

実際の攻撃を行うため、**セキュリティ製品やブルーチームのインシデント対応能力も評価可能**

レッドチーム（攻撃側）でPenteraを利用することで、  
**ブルーチームに予告することなくテスト可能**

**シンプルなGUI**で内部人材でも運用可能

任意のタイミングで**何度でも**テストを実施し、  
継続的な改善活動を実現



01

金融分野におけるサイバーセキュリティガイドラインについて..... P.3

02

ペネトレーションテストに関する内容とCTEMについて..... P.5

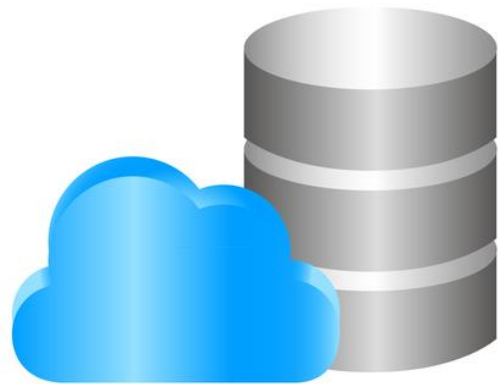
03

クラウドセキュリティに関する内容とCNAPPについて ..... **P.17**

04

東京エレクトロンデバイスの紹介とまとめ ..... P.33

## 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



## 情報系、勘定系などのバンキングシステムをAzureに移行



金融業界において様々なシステムがIaaS/PaaSに移行している

## 【基本的な対応事項】

- 利用するクラウドサービスの仕様を確認し、理解を深めること
- 責任共有モデルを理解し、**クラウド事業者との責任範囲等を明確にすること**
- 情報公開等の**設定にミスがないか確認**すること  
必要に応じて、専門家によるシステム監査や**誤設定の自動検知等の診断サービス等を利用**すること
- 責任分界に応じて、サービス仕様が変わる際には影響を確認すること
- 多岐にわたる関係主体等を把握し、情報共有体制・インシデント対応体制を構築すること
- クラウドサービスの利用終了時における、クラウドサービス上のデータの取扱い（論理的な廃棄）について確認すること

**(参考) 「クラウドサービス利用・提供における適切な設定のためのガイドライン」(総務省) も参照**すること

## ● 目的：

令和6年4月公表の「クラウドサービス利用・提供における適切な設定のためのガイドライン」をわかりやすく解説するために作成され、クラウドの活用状況と、予防策まで提示されている

## ● 設定ミスの4つの対策

### 組織・ルール

- ・体制整備
- ・方針・規則

### 人

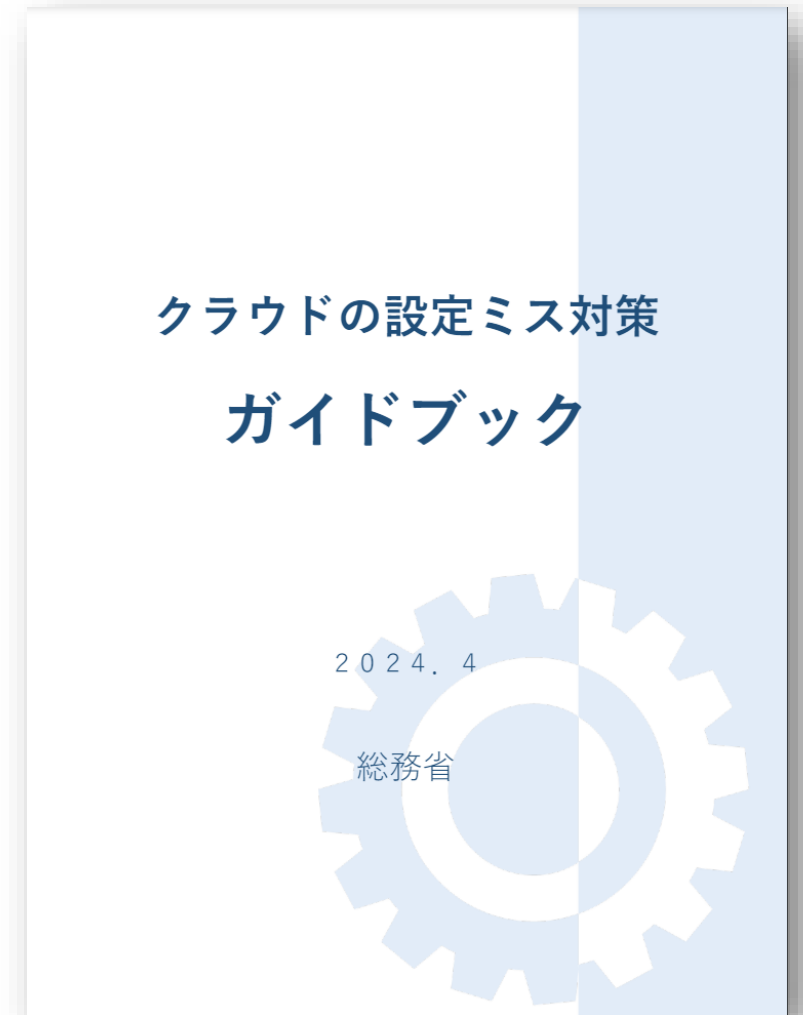
- ・人材育成
- ・コミュニケーション

### 作業手順

- ・設定、チェック、修正
- ・マニュアル

### 道具

- ・チェックリスト
- ・支援ツール



[soumu.go.jp/main\\_content/000944467.pdf](https://soumu.go.jp/main_content/000944467.pdf)

# 設定ミスの4つの対策（ツールによる対策）

## 3種類の支援ツール

**道具**

- ・チェックリスト
- ・支援ツール

**CASB**  
(Cloud Access Security Broker)

- ・ クラウドサービス利用状況の可視化
- ・ アプリケーションやデータへのアクセス監視
- ・ セキュリティポリシーに照らしたリスク検出  
etc....

**CSPM**  
(Cloud Security Posture Management)

- ・ IaaS/PaaSの監査ツール
- ・ クラウドの設定を自動的にチェック
- ・ コンプライアンス違反等のリスクを特定  
etc....

**SSPM**  
(SaaS Security Posture Management)

- ・ SaaSの監視ツール
- ・ 各アプリケーションの設定や状況管理
- ・ コンプライアンス違反や脅威検出  
etc....

すでに導入済み企業多数



現在注目度アップ

- ※ガイドラインでの規定
- ※設定ミスによるインシデントニュース
- ※マルチクラウド環境管理の複雑さ

今後需要拡大見込み



# 設定ミスの4つの対策（ツールによる対策）

## 3種類の支援ツール

### 道具

- ・チェックリスト
- ・支援ツール

#### CASB

(Cloud Access Security Broker)

- ・ クラウドサービス利用状況の可視化
- ・ アプリケーションやデータへのアクセス監視
- ・ セキュリティポリシーに照らしたリスク検出  
etc....

#### CSPM

(Cloud Security Posture Management)

- ・ IaaS/PaaSの監査ツール
- ・ クラウドの設定を自動的にチェック
- ・ コンプライアンス違反等のリスクを特定  
etc....

#### SSPM

(SaaS Security Posture Management)

- ・ SaaSの監視ツール
- ・ 各アプリケーションの設定や状況管理
- ・ コンプライアンス違反や脅威検出  
etc....

すでに導入済み企業多数



現在注目度アップ

- ※ガイドラインでの規定
- ※設定ミスによるインシデントニュース
- ※マルチクラウド環境管理の複雑さ

今後需要拡大見込み



- **Cloud Security Posture Management (クラウドセキュリティ態勢管理)**
- **クラウド環境 (IaaS/PaaS) におけるセキュリティ状態を管理・監視するためのツール**

セキュリティ状態が管理・監視できていないと・・・



外部に公開されるべきでないデータが誤って公開されてしまう



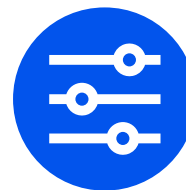
コンプライアンス違反による法的な問題や罰金



クラウド環境全体が可視化できず、異常や不正アクセスを検知できない



CSPMがあれば・・・



**設定ミスの検出**



**コンプライアンスの維持**



**可視化と一元管理**



**CSPMを導入すればクラウド環境のセキュリティは完ペキ**

というわけではありません



クラウドアクセストークンの不適切管理により、  
内部機密データを誤ってインターネットに公開

- ✓ ストレージへアクセススコープの過剰付与
- ✓ アクセストークンへの過剰な権限付与
- ✓ ストレージをインターネットに意図せず公開

出典: 38TB of data accidentally exposed by Microsoft AI researchers (2023/9/18)  
<https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers>

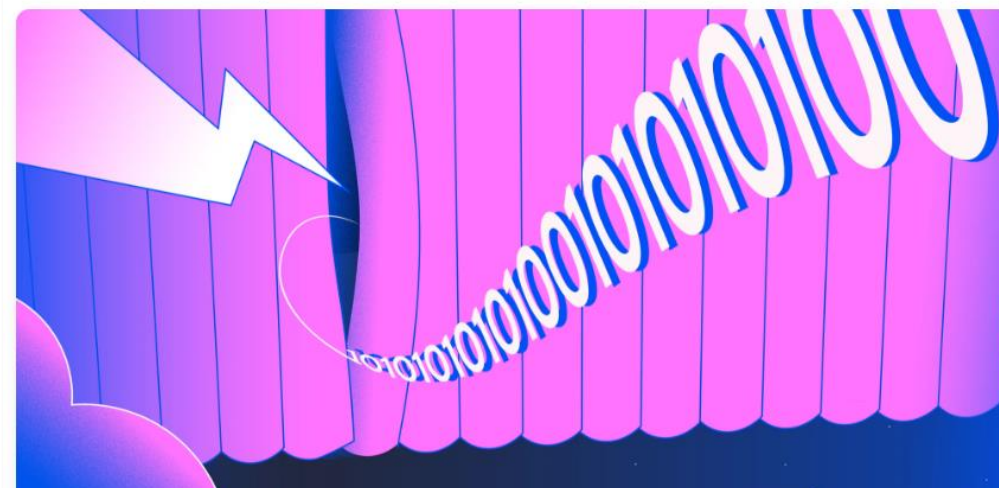
## 38TB of data accidentally exposed by Microsoft AI researchers

Wiz Research found a data exposure incident on Microsoft's AI GitHub repository, including over 30,000 internal Microsoft Teams messages – all caused by one misconfigured SAS token



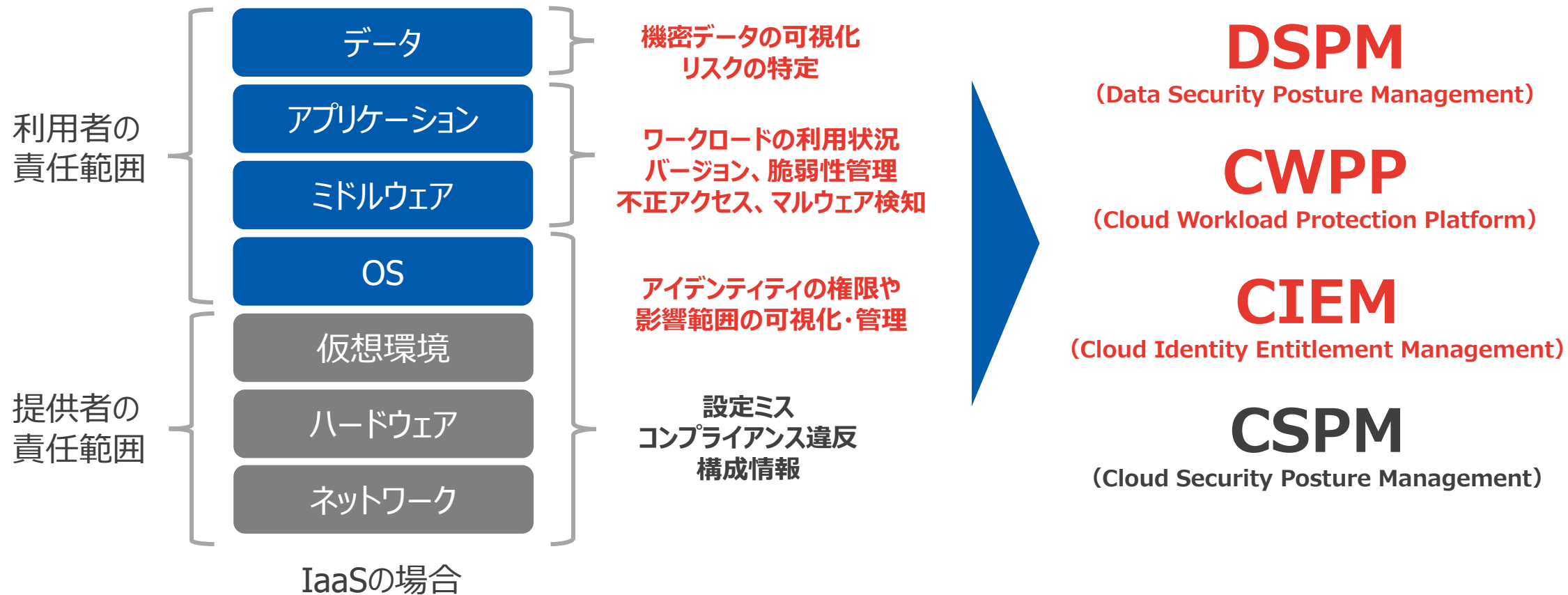
Hilla Ben-Sasson, Ronny Greenberg  
September 18, 2023

10 minutes read



IaaS/PaaS環境では複雑な要素が絡み合っており、  
ITリテラシーの高いメンバーがいるような組織でもこのような事件が発生してしまう

# CSPMだけでは万全な対策とは言い切れません



個別最適でツールを利用し、各機能を統合管理していくのは大変です

## Cloud Native Application Protection Platform

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



1つのプラットフォームでセキュリティを網羅的に実現できることが理想的

それが..... **WIZ**  **です**



Fortune 100のうち**40%**が採用  
国内大手企業様で**実績**あり

# Wizとは



クラウド活用に必要なセキュリティー機能を網羅的に提供するCNAPPソリューション

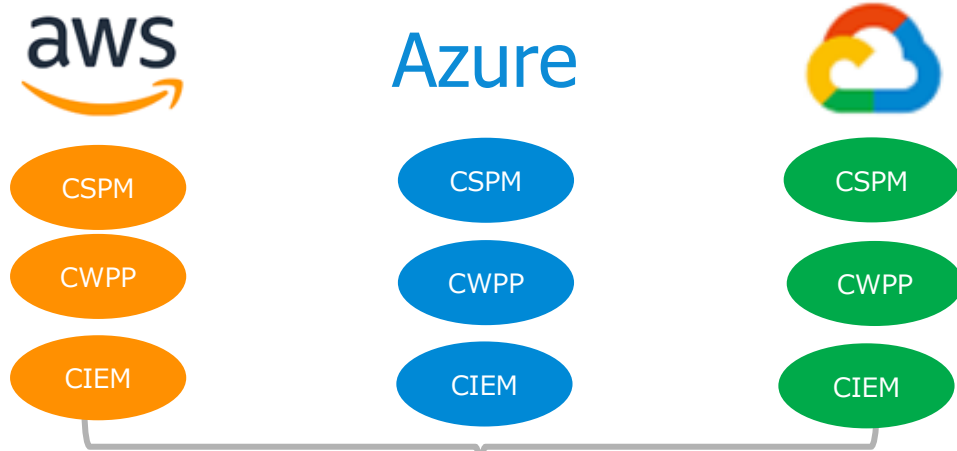
## ● 会社概要

- 設立 2020年、米国NY
- 代表 Assaf Rappaport (Co-Founder & CEO)
- 設立18ヶ月で評価額\$100M達成
- 設立3年で評価額\$10B超のデカコーン企業
- 米Google親会社のアルファベット社が過去最高額のM&Aをオファー

<h3>1 エージェントレス・スキャン</h3> <p>サーバレス コンテナ 仮想マシン PaaS</p>	<h3>2 クラウドアセスメントの実行</h3> <p><b>基本的なスキャン</b> 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</p> <p><b>クラウド・リスクエンジン</b> 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</p> <p><b>Wiz脅威リサーチ</b> クラウドの新しい脆弱性と攻撃</p>	<h3>3 最重要リスクの優先順位付け</h3> <p>Container Image Container Virtual machine 112 vulnerabilities Access role Serverless Internet exposure</p>	<h3>4 必要な連携が簡単に可能</h3> <p><b>インテグレーション</b> 20+ インテグレーション</p> <p><b>クラウドの修復</b> ワンクリック修復 セキュリティ対応の自動化 修復ガイド</p> <p><b>CI/CDのガイドライン</b> 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</p>
試しやすい	オールインワン	分かりやすい	導入しやすい

細かいリスクが積み重なった結果に起こる影響を重要度とともに可視化し、対処方法を提示

# ネイティブツールとWizの違い



個別のサービスとしてそれぞれ存在

- マルチクラウド対応 ✗ 一応可
- 統一されたセキュリティレベルの維持 △
- UI画面の提供 △
- アラートのコンテキスト化 ✗

安く活用はできるが、  
マルチクラウド対応・使いやすさに疑問



オールインワンなので、使い分けの必要なし、  
初期導入も簡易/運用・コスト観点でも低負荷に

課題

1

クラウド(IaaS/PaaS)の  
設定ミス等のセキュリティに  
懸念がある

クラウド(IaaS/PaaS)の  
リスクと潜在的な問題を  
明確化し、対処が可能に

課題

2

クラウドリソースの数や  
全体像を把握・管理・監視  
しきれない

クラウドリソースのバージョン  
まで含めた全体像の把握や  
資産管理が容易に

課題

3

マルチクラウド・マルチアカウ  
ント環境が個別に管理され、  
セキュリティレベルに差がある

複数環境を横断した資産管理  
と単一のセキュリティポリシーの  
適用を実現

**CSPM他、CIEM、CWPP等のIDおよびワークロードの保護を含む  
IaaS上のセキュリティ/コンプライアンス管理まで多岐にわたり保護が可能**



01

金融分野におけるサイバーセキュリティガイドラインについて..... P.3

02

ペネトレーションテストに関する内容とCTEMについて..... P.5

03

クラウドセキュリティに関する内容とCNAPPについて ..... P.17

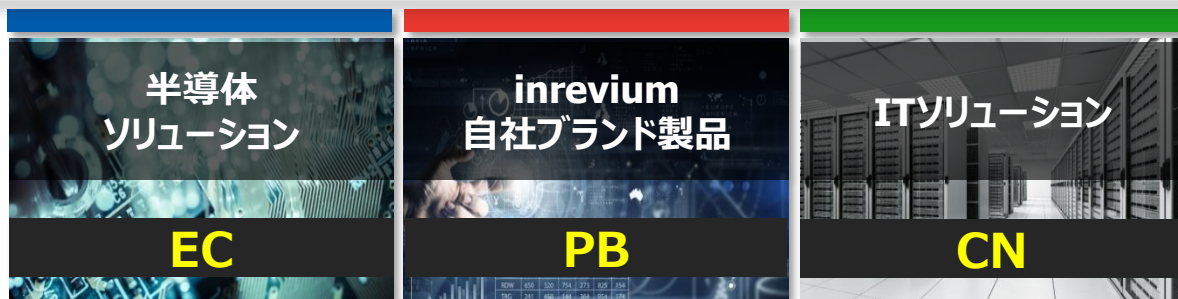
04

東京エレクトロンデバイスの紹介とまとめ ..... P.33

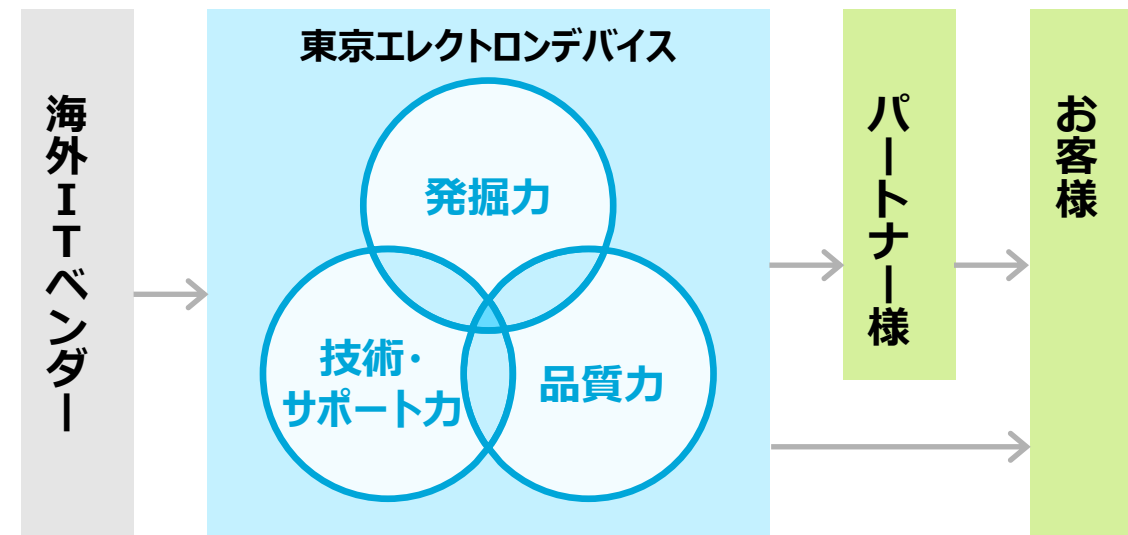
## 会社概要

- 会社名** : 東京エレクトロ 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** : 2,428億88百万円 (2024年3月期)
- 従業員** : 連結: 1,357名 (2024年3月31日現在)

## 事業内容



## CN BU



「発掘力」「技術・サポート力」「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

## CNフォーカスエリア



## 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			SSO/多要素認証
エンドポイント	HSM	シークレット管理	
Active EDR/XDR		Hashicorp	

### 社内/トラストネットワーク関連ソリューション

Firewall	VPN	WAF
 		 Distributed Cloud Services
Wi-Fi	DNS/DHCP	NDR
Cognitive Wi-Fi	DNSセキュリティ	

### セキュリティ診断

ASV

PenTest, ASM

### データ分析

SIEM/SOAR/UEBA

### 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/CNAPP	SSPM	IaC
		HashiCorp 

### クラウド

パブリッククラウド

### AI/DLソリューション

GPU	Accelerator

### 仮想化基盤ソリューション

HCI	3Tier

### ファイルストレージソリューション

Scale Out	Scale Up
Power Scale	Unity XT

### ネットワークソリューション

IP Clos	L2/L3スイッチ	ADC
	DCNW  	キャンパス 

### 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

# CTEM

(Continuous Threat Exposure Management)

脅威にさらされている資産を、継続的に評価し、  
リスクを特定、対処するセキュリティアプローチ



ペネトレーションテストを自動化し、  
継続的なセキュリティ検証を実現

# CNAPP

(Cloud Native Application Protection Platform)

IaaS/PaaS環境における複数の異なる  
セキュリティ機能を1つに統合するプラットフォーム



マルチクラウド環境にも対応し、  
IaaS/PaaSにおけるセキュリティを  
オールインワンで提供



共に創る 新たな価値を



東京エレクトロン デバイス