ものづくり業界必見 最新のセキュリティ対策
～IaaSの正しい運用IT/OTセキュリティ～

クラウドの利活用で重要なガードレール型セキュリティとは

～設定ミスによるインシデントを防ぐ２つの社内統制法～

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
服部奈々美

本日の内容

1. 東京エレクトロンデバイスのご紹介

2. クラウド利用の現状・課題と解決策

3. 東京エレクトロンデバイスのソリューションご紹介（Hashicorp Terraform/Vault、WIZ CNAPP）

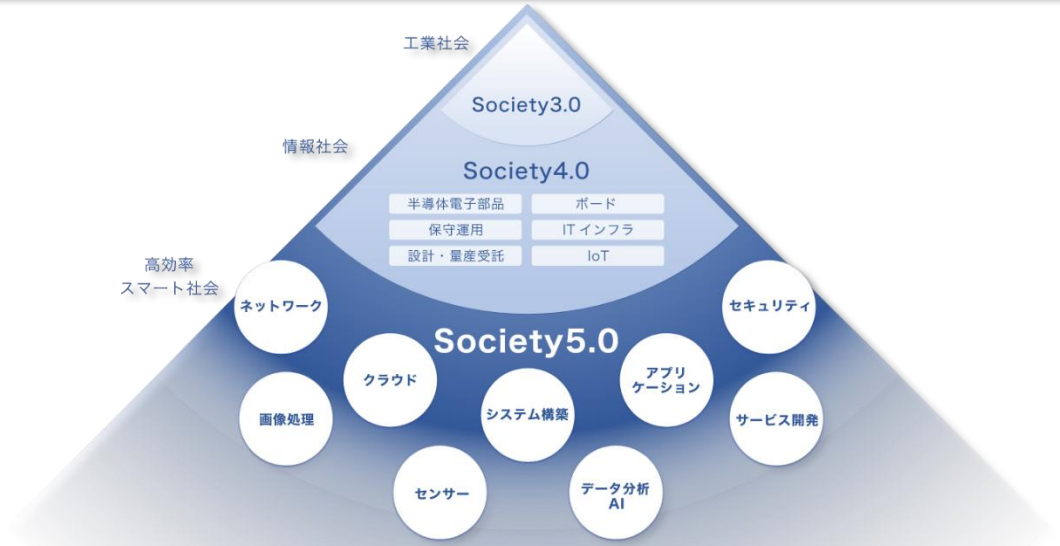
東京エレクトロンデバイスのご紹介

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	： 2,428億88百万円（2024年3月期）
従業員	： 1,357名（2024年3月31日）
子会社	： 株式会社ファースト 東京エレクトロン デバイス長崎株式会社 TOKYO ELECTRON DEVICE ASIA PASIFIC LTD.（TED APAC） TOKYO ELECTRON DEVICE (SHANGHAI). LTD TOKYO ELECTRON DEVICE SINGAPORE PTE. LTD.（TEDSG） TOKYO ELECTRON DEVICE (THAILAND) LIMITED.（TEDTH） TOKYO ELECTRON DEVICE AMERICA, INC.（TEDAI）

事業内容

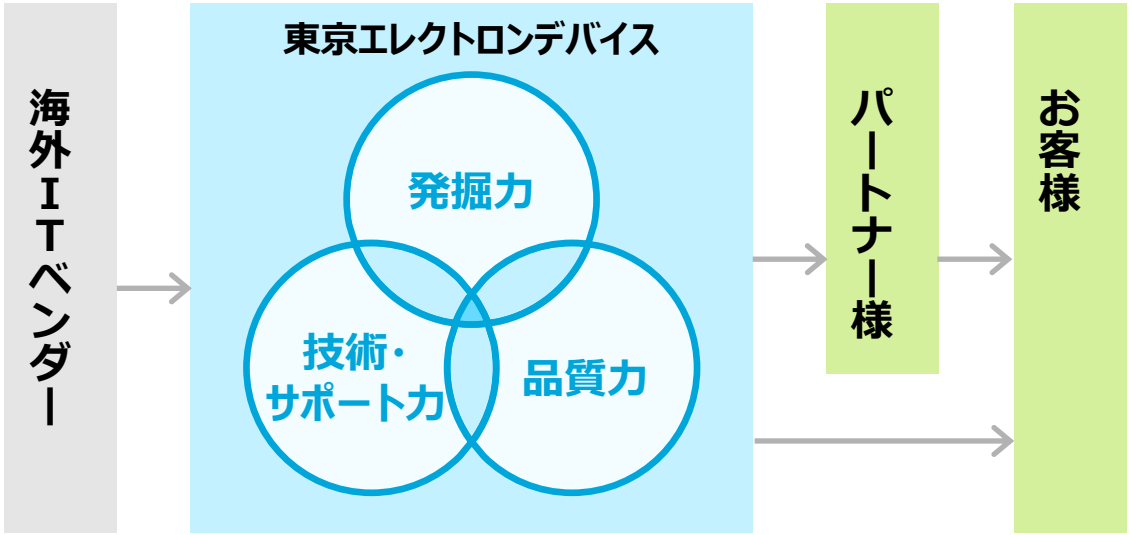


CN BU（Computer Network Business Unit）について

CN事業（Computer Network事業）

■ 3つの力

- **発掘力**
  最先端テクノロジー・ビジネスの発掘と開拓
- **技術・サポート力**
  導入支援・アフターサービス
- **品質力**
  受入検査・出荷検査



■ フォーカスエリア

セキュリティ

高度化するサイバー攻撃対策
やセキュリティ対策

ネットワーク

高速・高可用性ネットワーク環境を構築、
効率的な運用管理の支援

ストレージ

オンプレとクラウドをシームレスにつなぐ
データ保護・管理

AI

ビジネスを加速する
AIプラットフォーム／サービスを提案

クラウド

管理性・運用性・可用性が高く、
スケーラブルなクラウド環境の構築

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			SSO/多要素認証
netskope			okta

エンドポイント	HSM	シークレット管理
Active EDR/XDR	ENTRUST	Hashicorp
SentinelOne	THALES	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	f5	f5 Distributed Cloud Services
FORTINET		

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

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 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		Unity XT
DELL Technologies	PURESTORAGE	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	キャンパス	f5
	ARISTA	Extreme networks	
	NVIDIA		

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

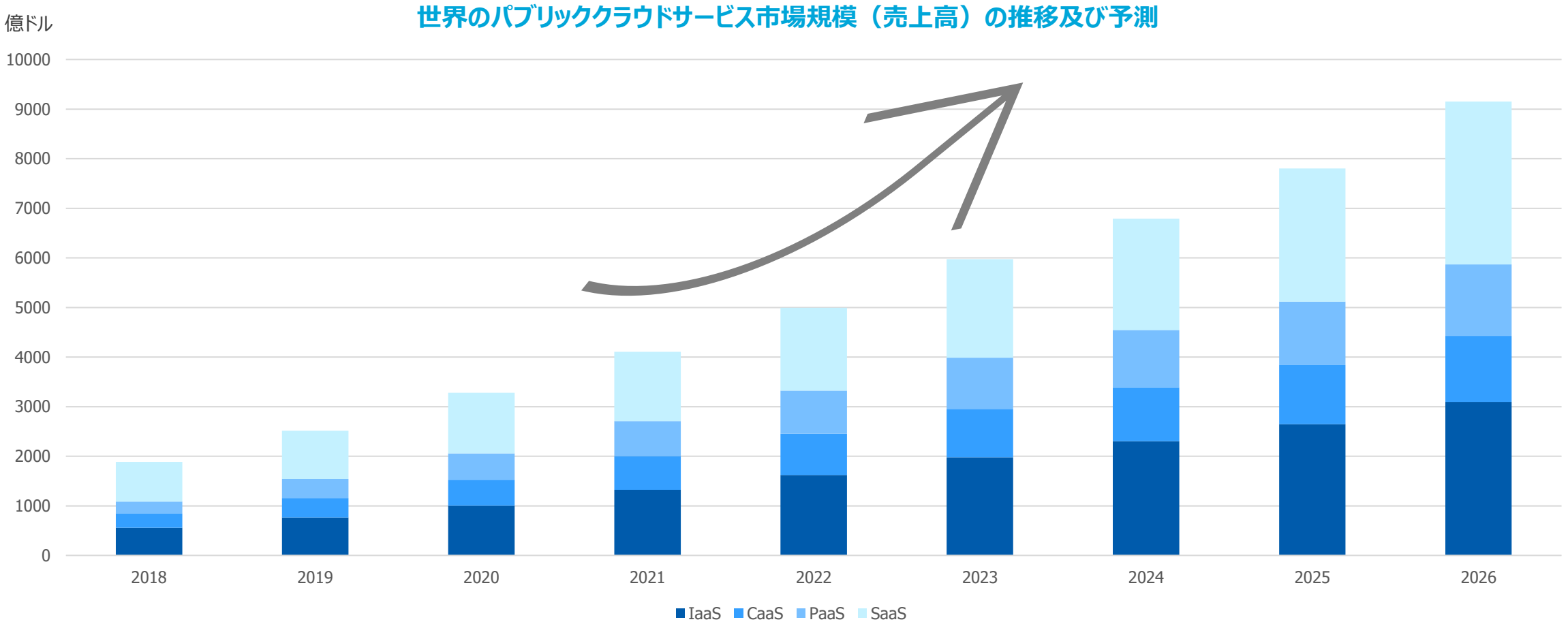
東京エレクトロン デバイス

クラウド利用の現状・課題と解決策

パブリッククラウドサービスの市場規模（2018年～2026年）

世界のパブリッククラウドサービス市場は年々増加傾向にあります。

- 日本市場においても、年々クラウドへの移行が進んでいることなどを背景に、今後も増加を見込んでいます。

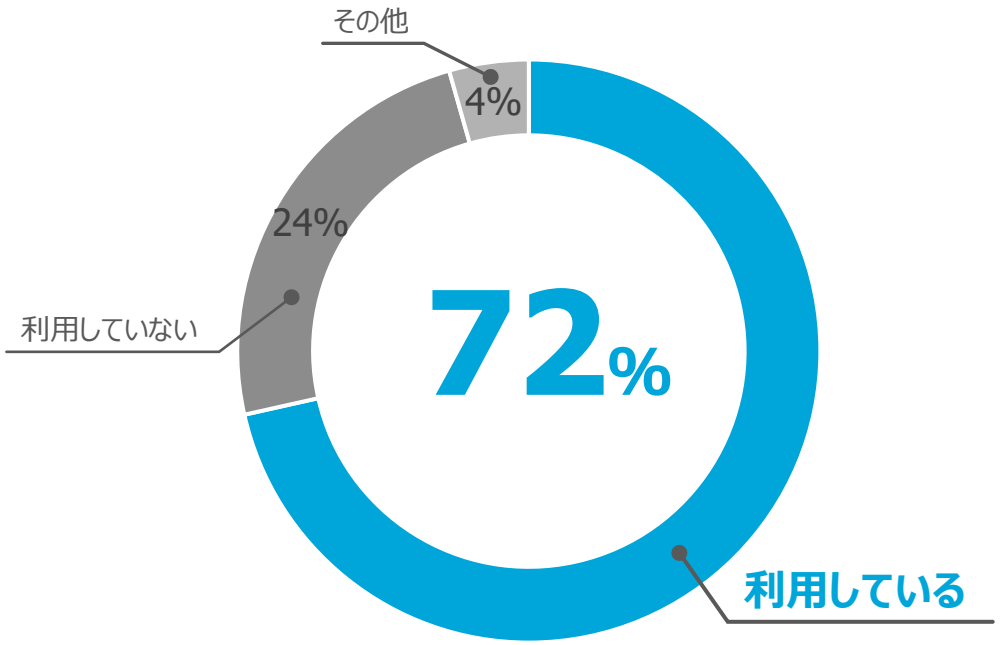


総務省｜令和5年版 情報通信白書｜クラウドサービス (soumu.go.jp)

製造業界のクラウドサービスの利用状況と管理の実態

クラウドの利活用が進む一方で管理は複雑に

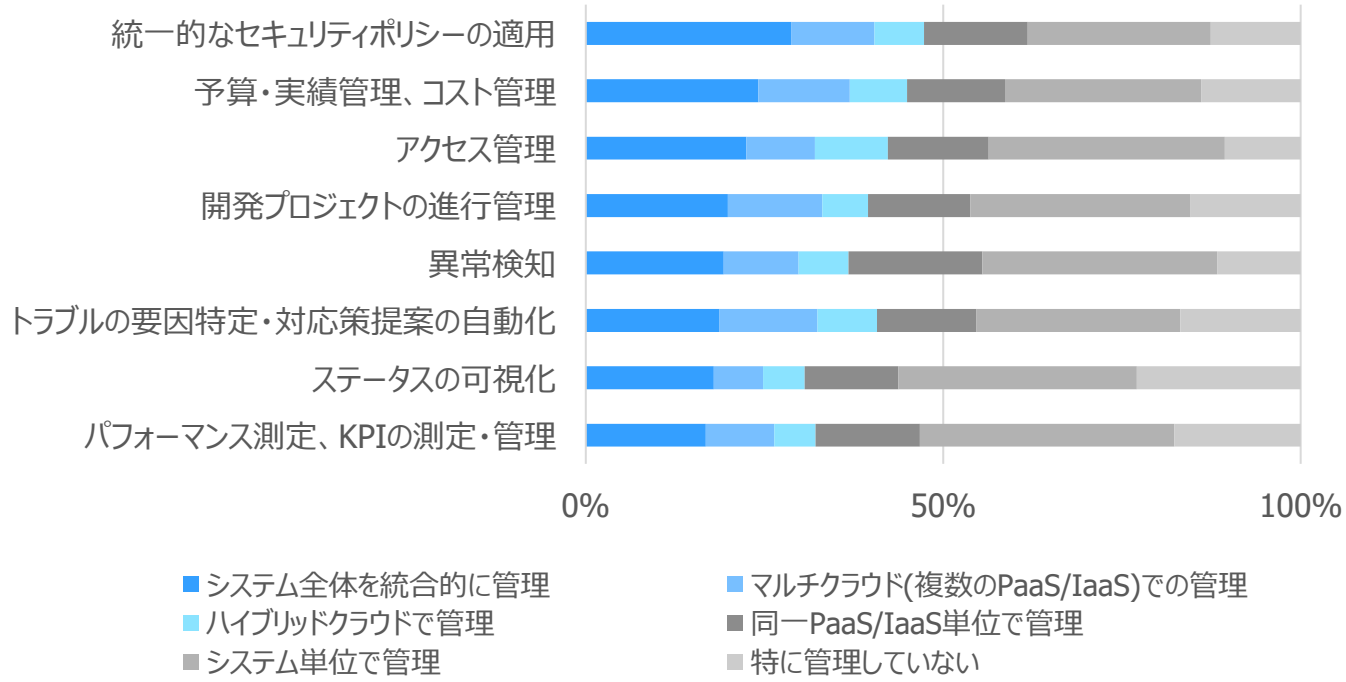
製造業界のクラウドサービスの利用状況



※2022年5月29日時点

（出典）総務省「通信利用動向調査」
https://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

マルチクラウド・ハイブリッドクラウド利用時の管理項目別・統合管理の対象範囲



（出典）MM総研「国内クラウドサービス需要動向調査」（2022年6月時点）
https://www.m2ri.jp/release/detail.html?id=549

クラウドサービスの設定ミスという重大リスク

2025年までには、クラウドセキュリティの障害の 約99% は利用者の責任になると言われています。※1

クラウドサービスは便利な一方で設計や運用が難しく、使い方を誤れば重大なインシデントに繋がるリスクを孕んでいます。

クラウドサービスには**「責任共有モデル」**というものがあり、SaaS、PaaS、IaaSそれぞれで**定められた範囲の責任を利用者側が背負う**必要があります。

また、米CSAの「クラウドコンピューティングの重大脅威 パンデミックイレブン」で公開されているように**クラウド事業者要因のセキュリティ障害は年々減少しており**、より一層利用者側で十分な設定・管理の対応を実施することが重要となっています。

順位	脅威名
1位	不十分なアイデンティティ、クレデンシャル、アクセス、鍵の管理
2位	安全でないインターフェースとAPI
3位	設定ミスと不適切な変更管理
4位	クラウドセキュリティのアーキテクチャと戦略の欠如
5位	安全でないソフトウェア開発
6位	安全でないサードパーティリソース
7位	システムの脆弱性
8位	偶発的なクラウドデータの漏えい
9位	サーバーレスおよびコンテナのワークロードの構成ミスと悪用
10位	組織的な犯罪、ハッカーと APT
11位	クラウドストレージデータ流出

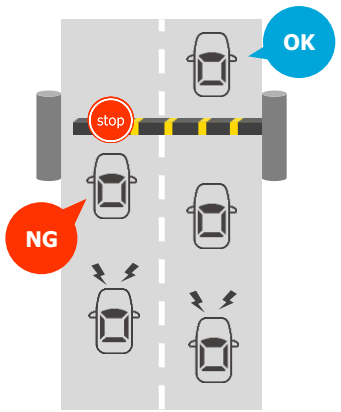
（出典：CSA、Top Threats to Cloud Computing – Pandemic Eleven
（訳：CSA ジャパ ン、クラウドコンピューティングの重大脅威 パンデミックイレブン）

※1 出展: ガートナージャパン株式会社,"Is the Cloud Secure?",2019-10-10
https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

クラウドサービスの利用に重要な考え方 ～ガードレール型セキュリティ～

従来の “ゲートキーパー型” 運用から “ガードレール型” 運用へ

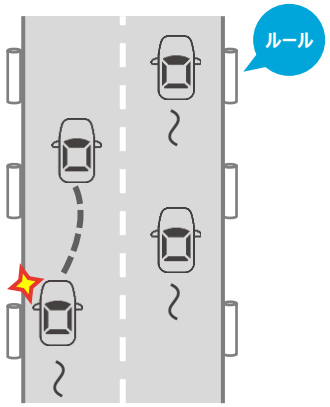
ゲートキーパー型



設定の追加や変更を
逐一チェックし問題の有無を判断

× チェックする工数が発生
× 人為的ミスが起こりやすい

ガードレール型



事前に決めたルールの中で自由に利用

✓ 確認の工数が不要
✓ 人為的ミスの抑制

ガードレール型にすることでクラウド利用のメリットである **スピード感を維持** しつつ **セキュリティを担保** することが可能になります。
人為的ミスへの対策としてガードレール(ルール)を設け、そこから逸脱するようなミスが発生した場合、迅速に是正することが重要です。

※ 出展：クラウドセキュリティ ～設定ミスとの付き合い方～（2023年7月時点）
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2023/t6hhco000000vx75-att/t6hhco000000vxj1.pdf

東京エレクトロン デバイス

ガードレール型セキュリティに必要な2つの統制

ガードレール型セキュリティには「予防的統制」と「発見的統制」があり、クラウド利活用において、
この2つの統制を組織内でうまく機能させることが重要。

01 予防的統制

不正な操作・設定を事前に防止し、
インシデント発生を未然に防ぐこと

例）

- セキュリティポリシーの策定
- 最小権限の原則
- セキュリティチェック
- 設定ミスに対する教育

02 発見的統制

リソースが不正な状況になっていないか
継続的に監視し修正すること

例）

- 外部及び内部脅威の監視・分析
- セキュリティ設定の監視・監査

発見的統制は、完璧に実施することが難しい予防的統制を補完する役割

出展：クラウドセキュリティ ～設定ミスとの付き合い方～（2023年7月時点）
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2023/t6hhco000000vx75-att/t6hhco000000vxj1.pdf

予防的統制の具体策 ～ IaC の導入～ (1/2)

01 **予防的統制**

不正な操作・設定を事前に防止し、インシデント発生を未然に防ぐこと

IaC (Infrastructure as Code)の導入によって 主に以下の５つの課題を解決し、インシデント発生を未然に防止

手作業によるエラー

手動でインフラを設定する場合、人的ミスが発生しやすくなります。特に複雑な設定や大規模な環境では、ミスが致命的な問題を引き起こすことがあります。

一貫性の欠如

手動での設定は環境ごとに異なるため、開発、テスト、本番環境間での一貫性を保つことが難しくなります。これにより、環境間での動作不具合が発生しやすくなります。

時間とコストの増加

手動でのインフラ構築は時間がかかり、その分コストも増加します。また、特定の知識を持つ人に依存するため、リソースの確保が難しくなることもあります。

スケーラビリティの問題

手動での設定変更やスケーリングは時間がかかり、迅速な対応が難しくなります。これにより、ビジネスの成長や変化に柔軟に対応することが難しくなります。

バージョン管理とドキュメンテーションの不足

手動での設定はバージョン管理が難しく、変更履歴を追跡することが困難です。また、ドキュメンテーションが不足しがちで、引き継ぎがスムーズに行えないことがあります

IaCを導入することで、インフラの設定や管理が自動化され、一貫性が保たれ、エラーが減少し、コストも削減できます。

予防的統制の具体策 ～シークレット管理ツール の導入～ (2/2)

01 **予防的統制**

不正な操作・設定を事前に防止し、インシデント発生を未然に防ぐこと

シークレット管理ツールの主に以下の４つの機能によってインシデント発生を未然に防止

シークレット情報の安全な管理

複数のシステムで使用される認証情報や機密データを一元管理し、漏えいリスクを低減します。
シークレット情報の動的管理により、必要な時にのみシークレットを生成し、利用後は自動で破棄することでセキュリティを強化します。

アクセス制御の強化

手動での設定は環境ごとに異なるため、開発、テスト、本番環境間での一貫性を保つことが難しくなります。これにより、環境間での動作不具合が発生しやすくなります。

機密データの暗号化

クレジットカード情報や個人情報などの機密データを堅牢に暗号化し、法令遵守をサポートします。
暗号化キーのライフサイクル管理を自動化し、運用負荷を軽減します。

監査とコンプライアンス対応

認証や操作履歴を記録し、監査要件に対応します2。
PCI DSSなどのセキュリティ基準に準拠した暗号化とキー管理を実現します1。

これらの機能により企業のセキュリティ強化と運用効率化に大きく貢献します。

発見的統制の具体策 ～CNAPPの導入～

02 **発見的統制**

リソースが不正な状況になっていないか継続的に監視し修正すること

CNAPP(Cloud Native Application Protection Platform)の予防的統制で敷いたガードレールに問題がないか定期的に監視し修正

セキュリティの一元管理

複数のセキュリティツールを統合し、クラウド環境全体のセキュリティを一元管理できます。これにより、セキュリティの複雑さが軽減されます。

設定ミスの防止

CSPM（Cloud Security Posture Management）機能により、クラウド環境の設定ミスを検出し、修正することで、セキュリティリスクを低減します。

権限管理の強化

CIEM（Cloud Infrastructure Entitlement Management）機能を使用して、過剰な権限が付与されたアカウントを監視し、適切な権限管理を実現します。

データ保護

DSPM（Data Security Posture Management）機能により、重要なデータの保護を強化し、データ漏えいのリスクを低減します。

ワークロード保護

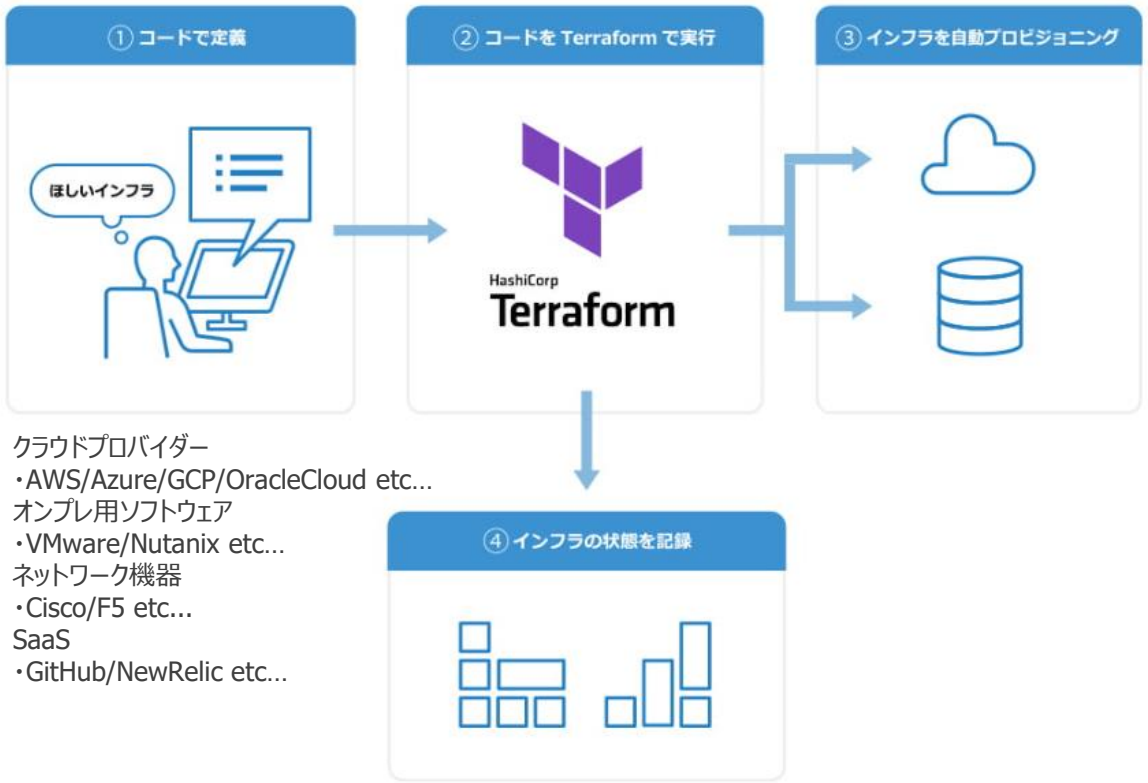
CWPP（Cloud Workload Protection Platform）機能により、クラウド上のサーバーやアプリケーションのセキュリティを確保します。

これらをどれか一つのことに対処するのではなく、広範囲にセキュリティを担保する仕組みを作ることが必要です。

onnect Beyond

東京エレクトロンデバイスがご支援いたします

IaC：Terraform ～インフラ環境の構築を自動化～



クラウドプロバイダー
・AWS/Azure/GCP/OracleCloud etc…
オンプレ用ソフトウェア
・VMware/Nutanix etc…
ネットワーク機器
・Cisco/F5 etc…
SaaS
・GitHub/NewRelic etc…

課題

・他部門で勝手にIaaSなどの利用が始まり、統制が効かない
・複数のクラウド/オンプレミス利用に伴い同じことをやりたいのに製品によって異なるGUIの操作
・マニュアルによる統制の限界

導入後の効果

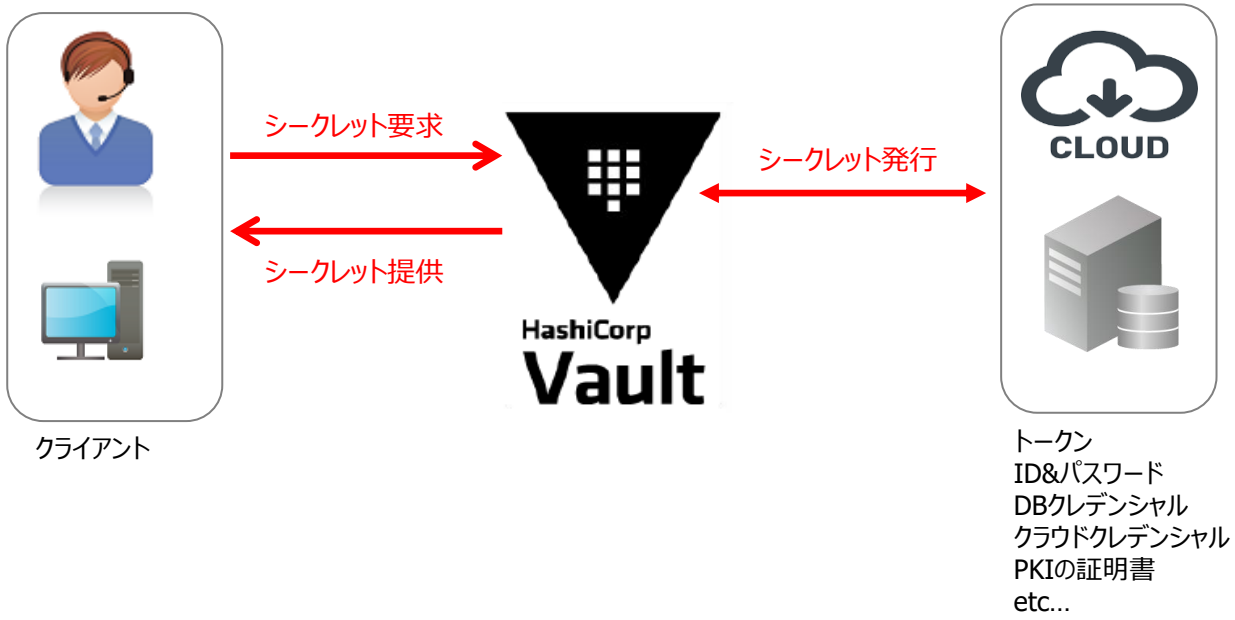
・人手からコードへの移行により、インフラ構築ミスの大幅削減
・属人化の撤廃
・学習コストの削減

特徴

・AWS/Azure/K8s以外にSaaSやオンプレまでマルチにサポート
・マルチサポート＝Hashicorpのみ覚えれば良いため学習コスト削減

マルチ・ハイブリッドのインフラ環境における構築自動化に最適なIaCツール

シークレット管理：Vault ～シークレット管理の自動化～



課題
- シークレット情報の散財、長期利用による漏えいリスク
- シークレットの乱立、管理の手間
- アプリへのシークレット直接記入による漏えいリスク

導入後の効果
- シークレットの集中管理による漏えいリスクの低減
- シークレットの自動生成から破棄まで、ライフサイクルを動的管理
- 統一化したインタフェース使用による生産性向上

特徴
- CLI、GUI、API(WEBAPI, RESTfull API)でアクセス可能
- ユーザー、マシン、アプリ事に有効期限付きシークレット自動発行

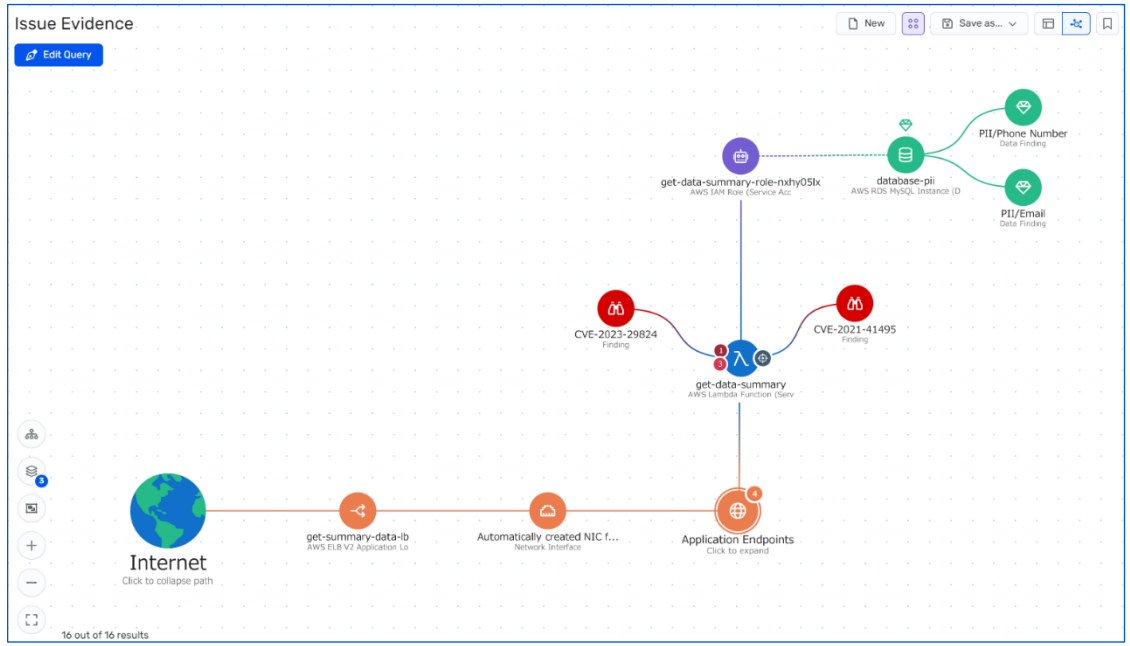
シークレットライフサイクル管理とセンシティブデータ保護ソリューション

CNAPP：WIZ CNAPP～クラウド(IaaS/PaaS)向け統合セキュリティプラットフォーム～

onnect Beyond

CNAPP – クラウドネイティブアプリケーション保護プラットフォーム

CSPM	CIEM	CWPP
Kubernetesセキュリティ	コンテナセキュリティ	脆弱性管理
IaCスキャニング	コンプライアンスレポート	DSPM - データセキュリティ
シークレットスキャニング	CDR	



課題

- クラウドリソースの数や全体像を把握・管理しきれない
- クラウド(IaaS/PaaS)のセキュリティに懸念がある、リスク管理しきれない
- マルチクラウド・マルチアカウントといった環境が個別に管理され、セキュリティレベルに差がある

導入後の効果

- 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
- 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
- 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

特徴

- エージェントレスによる容易な導入と、漏れのないリソースの検出・検査
- 包括的なクラウドセキュリティソリューション
- 個々のリスクをコンテキスト化し、本当に危険な問題をグラフィカルに表示し明確化、対処方法を提示

CNAPP – クラウドネイティブアプリケーション保護プラットフォーム ソリューション

onnect Beyond

ご清聴、ありがとうございました。