AIを利用したクラウドセキュリティの自動化

クラウドセキュリティ自動化 WG

CASB WG

根塚　昭憲

自己紹介

根塚　昭憲

経歴　　：株式会社マクニカ入社２０年オーバー
過去にはネットワーク、セキュリティプロダクトのエンジニアとしてサポートから製品提案、ニューライン調査などの業務を経験
現在は、SSE系プロダクトのマネジメントをしながら、
クラウドセキュリティ、特にSaaSセキュリティの啓発活動を行う

CSAでの活動　：CASB WG / Cloud Security Automation WGに参加

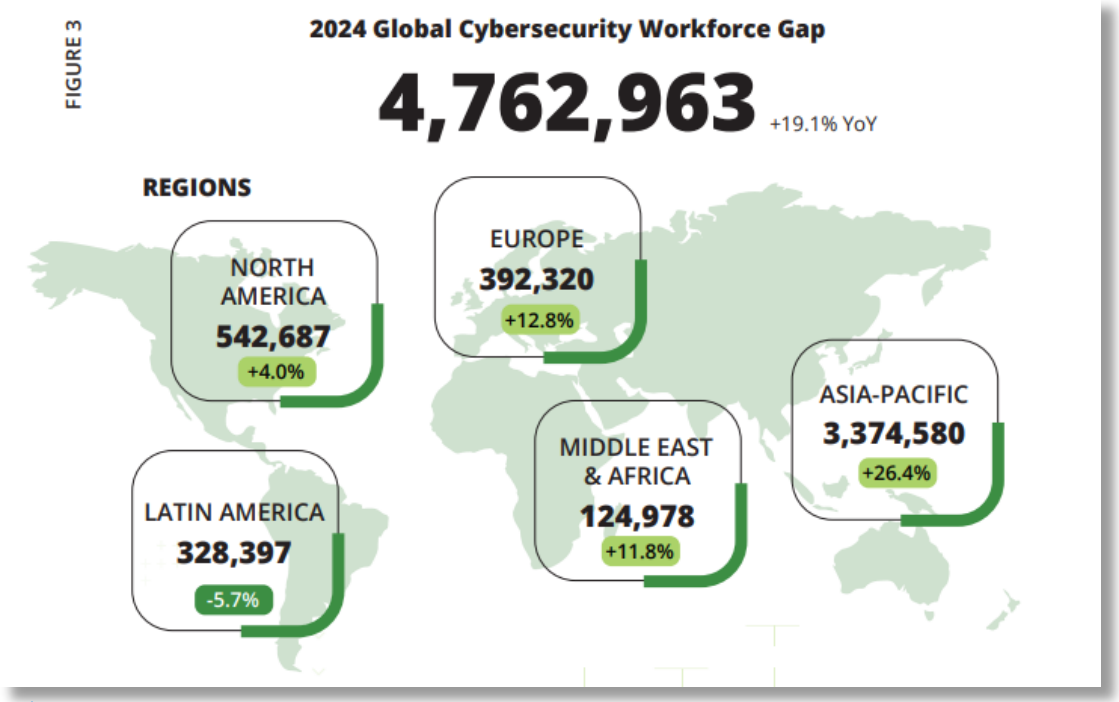
好きな仕事　　：検証環境の構築、自身で手を動かして検証すること

Agenda

1. クラウドセキュリティ自動化の必要性
2. すでに導入が進んでいるクラウドセキュリティ
3. クラウドセキュリティへのAI活用事例
4. 「セキュリティ計画」の最適化・自動化

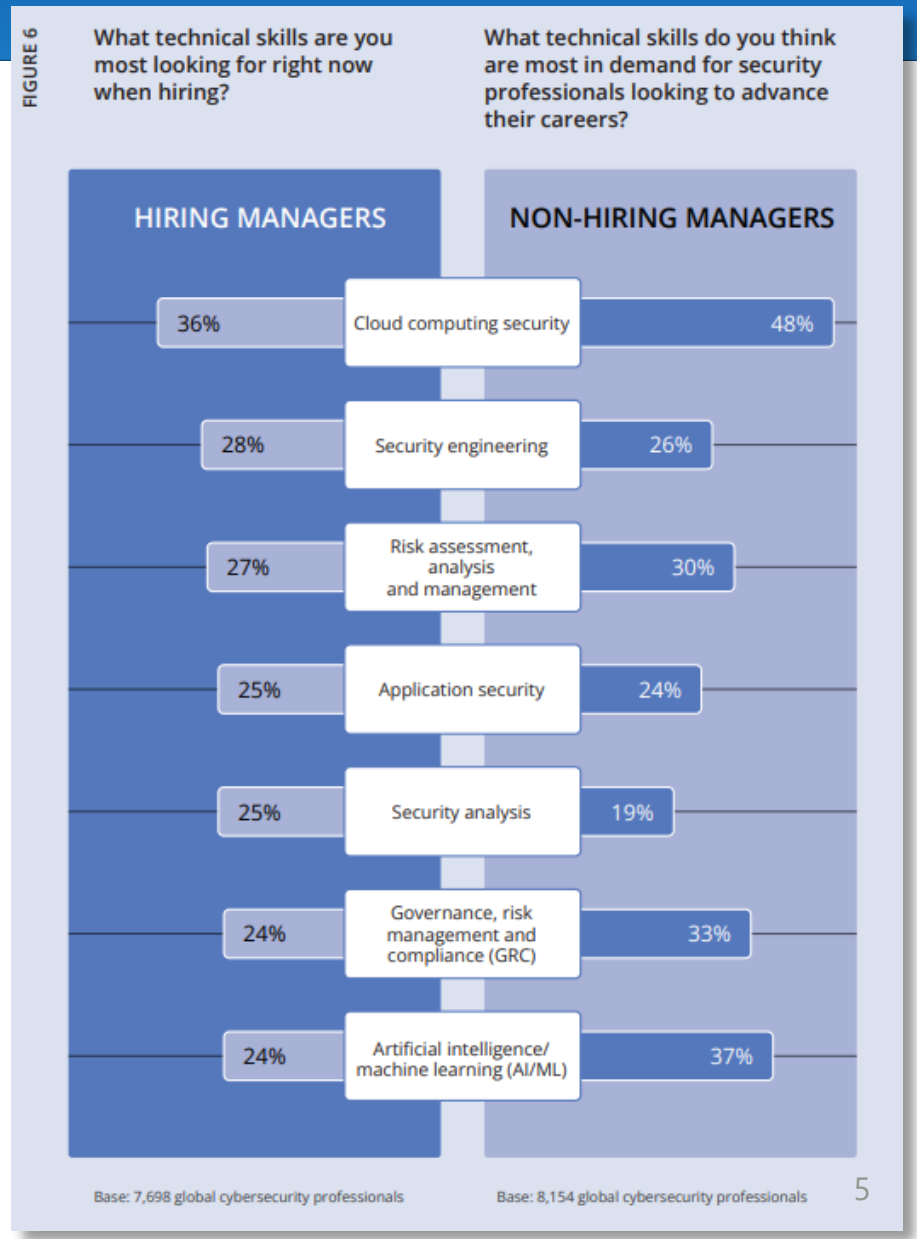
クラウドセキュリティ自動化の必要性

クラウドセキュリティ人材の不足



各地域のサイバーセキュリティ人材の不足数（理想と現実のギャップ）

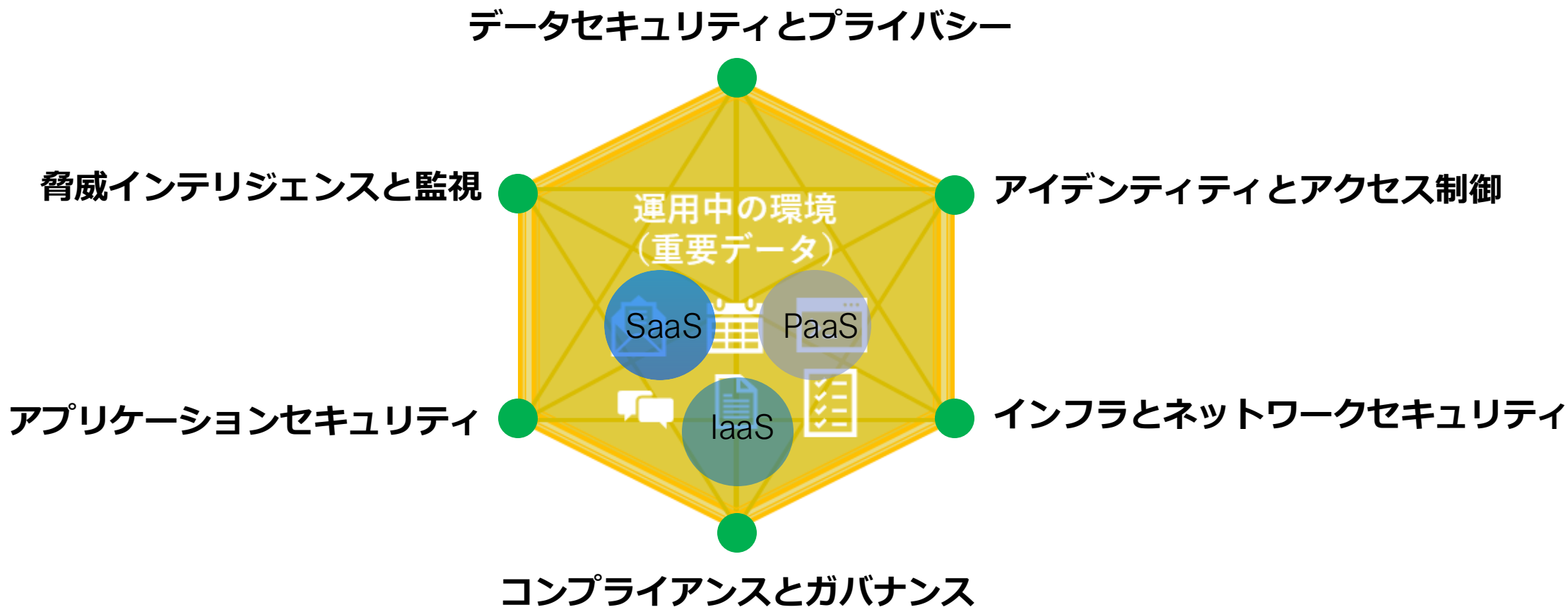
（左）雇用時に求めるスキル
（右）キャリアアップを目指すセキュリティ専門家に最も求められる技術的スキル



"2024 ISC2 Cybersecuirty Workforce Study" ISC2, 2024-10-31
https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study（2024/11/13）

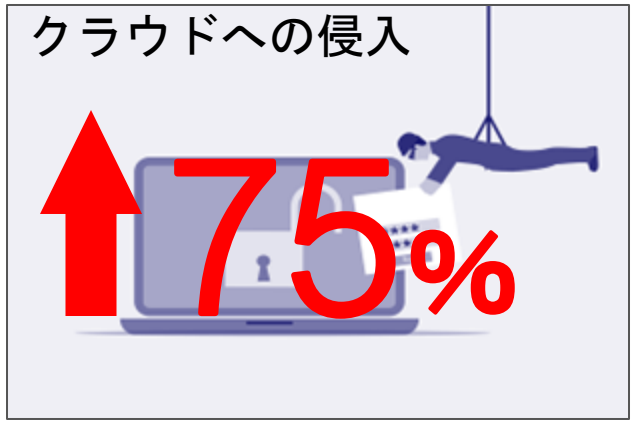
クラウドセキュリティカバー範囲は広範

クラウドセキュリティのカバー領域は広い



クラウドを意識した攻撃の増加

クラウドへの侵入は75%増加、クラウドを意識した攻撃は110%増加（前年比）（※）



- サイバー犯罪者の傾向（※）
  - サイバー犯罪攻撃者は**クラウド環境を積極的に標的**に
  - **クラウドを意識**した侵入の84%はサイバー犯罪アクターによるものと考えられる

- アイデンティティベースの手法が好まれる（※）
  - 正規の認証情報を使用して、**クラウド環境への初期アクセス**を達成
  - アイデンティティレベルで永続性を達成、その後権限を昇格させていく

“2024年版グローバル脅威レポート” クラウドストライク, 2024-03-25
https://www.crowdstrike.com/global-threat-report/（2024/11/13）

現状が引き起こすセキュリティリスク

クラウドセキュリティには効率化（自動化）のためセキュリティツールが必須

これらを、すぐに変えることは不可能

- クラウドセキュリティ人材不足
- カバー範囲が広範
- クラウドを意識した攻撃の増加

①脅威検知/調査/対応の遅れ
- 膨大な数のアラート、トリアージの対応に遅れ
- クラウド特有の調査が出来ず、初期段階での対応が困難

②セキュリティギャップの発生
- 全ての領域で均等に保護することが困難
- 連携不足/設定ミスなどが発生する

③コンプライアンス違反のリスク増加
- 新しい規制などを満たすための準備が不足

④コスト増加

組織全体の
(クラウド)セキュリティリスク増

対策
（自動化）

セキュリティ
プロダクト

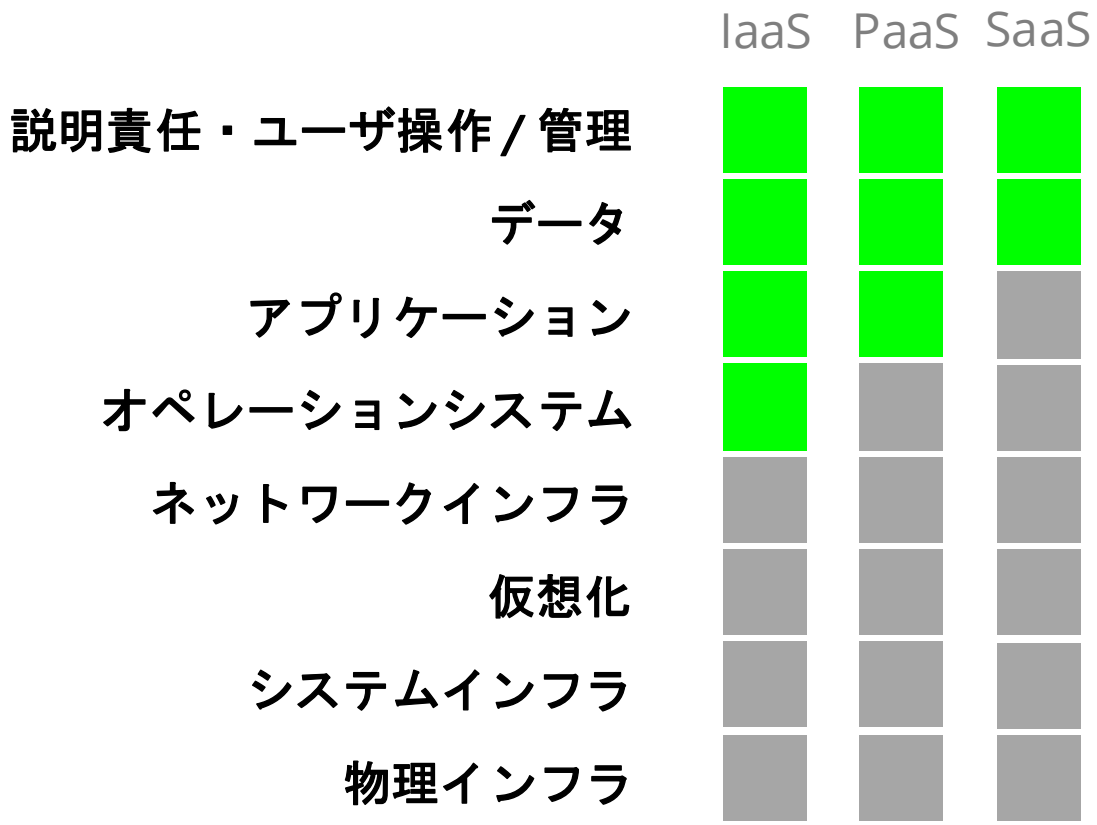
セキュリティ
ツール

導入がマスト

すでに導入が進んでいるクラウドセキュリティ

どこを守れば良いのか？ 責任共有モデル

クラウドの種類による異なる責任共有モデル



一般的な責任共有モデル

ユーザやデータの管理はいずれのクラウドでもユーザ側の責任範囲

クラウドユーザ側の責任範囲

チェックシートなどで確認

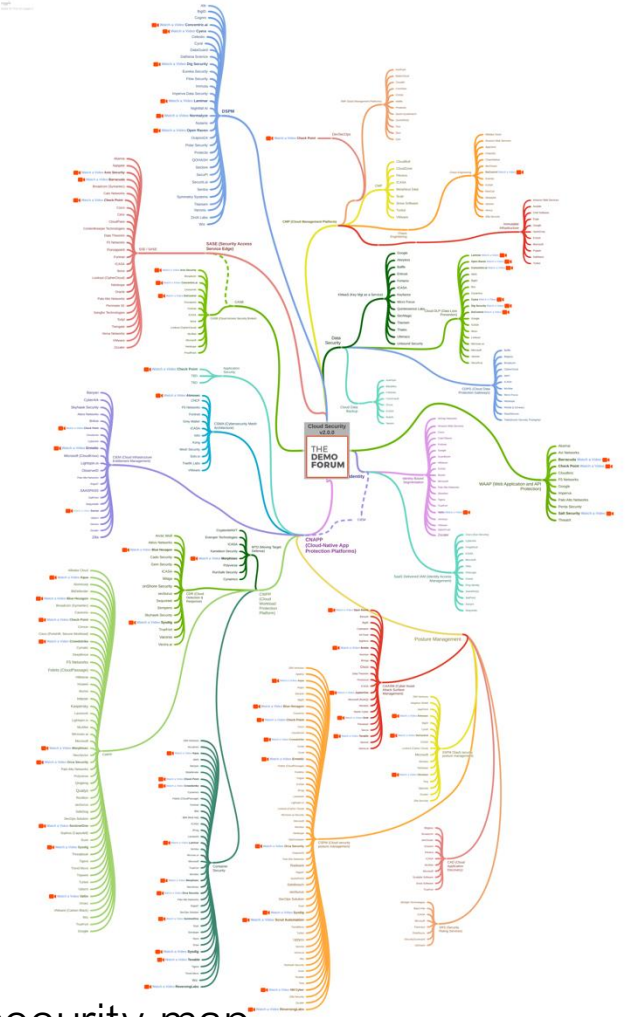
クラウドベンダ側の責任範囲

※事業者やサービスにより異なる可能性がありますので、各クラウドのご利用前に必ずご確認ください。

クラウドセキュリティ カテゴリー一覧

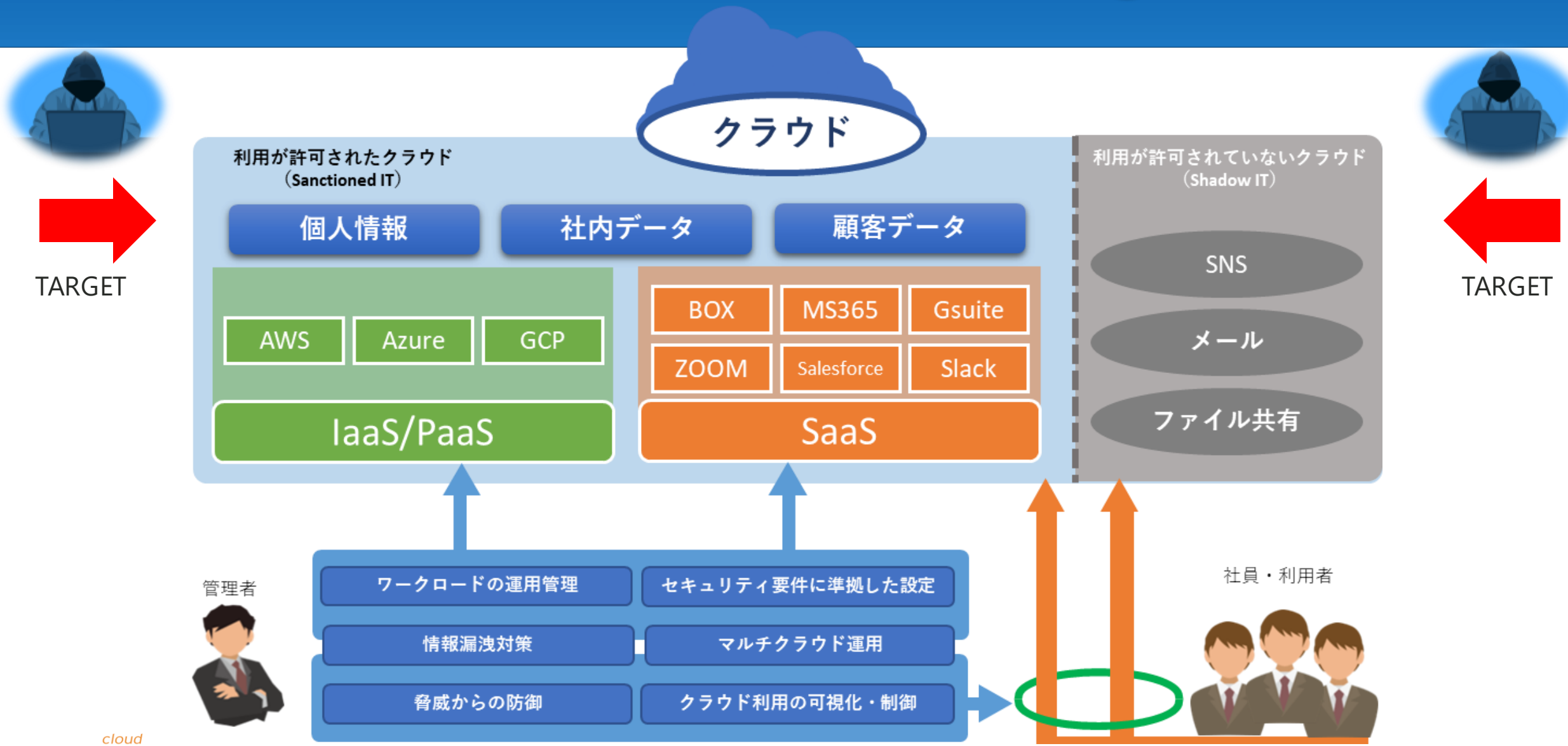
※太字は多くの企業で導入が進んでいるカテゴリ

CAASM Cyber Asset Attack Surface Management	CAD Cloud Application Discovery	**CASB** **Cloud Access Security Broker**
SSE/SASE **Secure Access Service Edge**	CDPG Cloud Data Protection Gateway	CDR Cloud Detection & Response
Chaos Eng Chaos Engineering	CIEM Cloud Infrastructure Entitlement Management	Cloud Data Backup
Cloud DLP Cloud Data Loss/Leak Prevention	CMP Cloud Management Platform	Container Security
CSMA Cyber Security Mesh Architecture	**CSPM** **Cloud Security Posture Management**	**CWPP** **Cloud Workload Protection Platform**
DSPM Data Security Posture Management	WAAP Web Application & API Protection	Identity-based Segmentation
Immutable Infrastructure	KMaaS Key Management as a Service/HSM	MTD Moving Target Defense
SaaS Delivered IAM	SMP SaaS Management Platform	SRS Security Rating Service
SSPM **SaaS Security Posture Management**		



https://circle.cloudsecurityalliance.org/learn/tech-maps/cloud-security-map

導入が進むクラウドセキュリティ①



導入が進むクラウドセキュリティ②

TARGET

TARGET

クラウド

② IaaS/PaaSを活用した公開環境や開発環境向けのセキュリティ

- 設定監査
- インベントリの可視化
- ワークロードの運用管理
- 脆弱性チェック

など

①社員などが利用するクラウドサービス（メインはSaaS）に対するセキュリティ

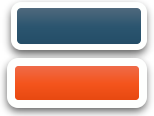
- 利用クラウドの可視化
- 利用先クラウドのセキュリティレベルの調査
- コンプライアンスの監視
- ユーザ動作の制御
- 不正動作検知、DLP（Data Loss Prevention）
- SaaSの設定監査　など

CSPM
CWPP
CNAPP

CASB
SSPM
SASE
SSE

管理者

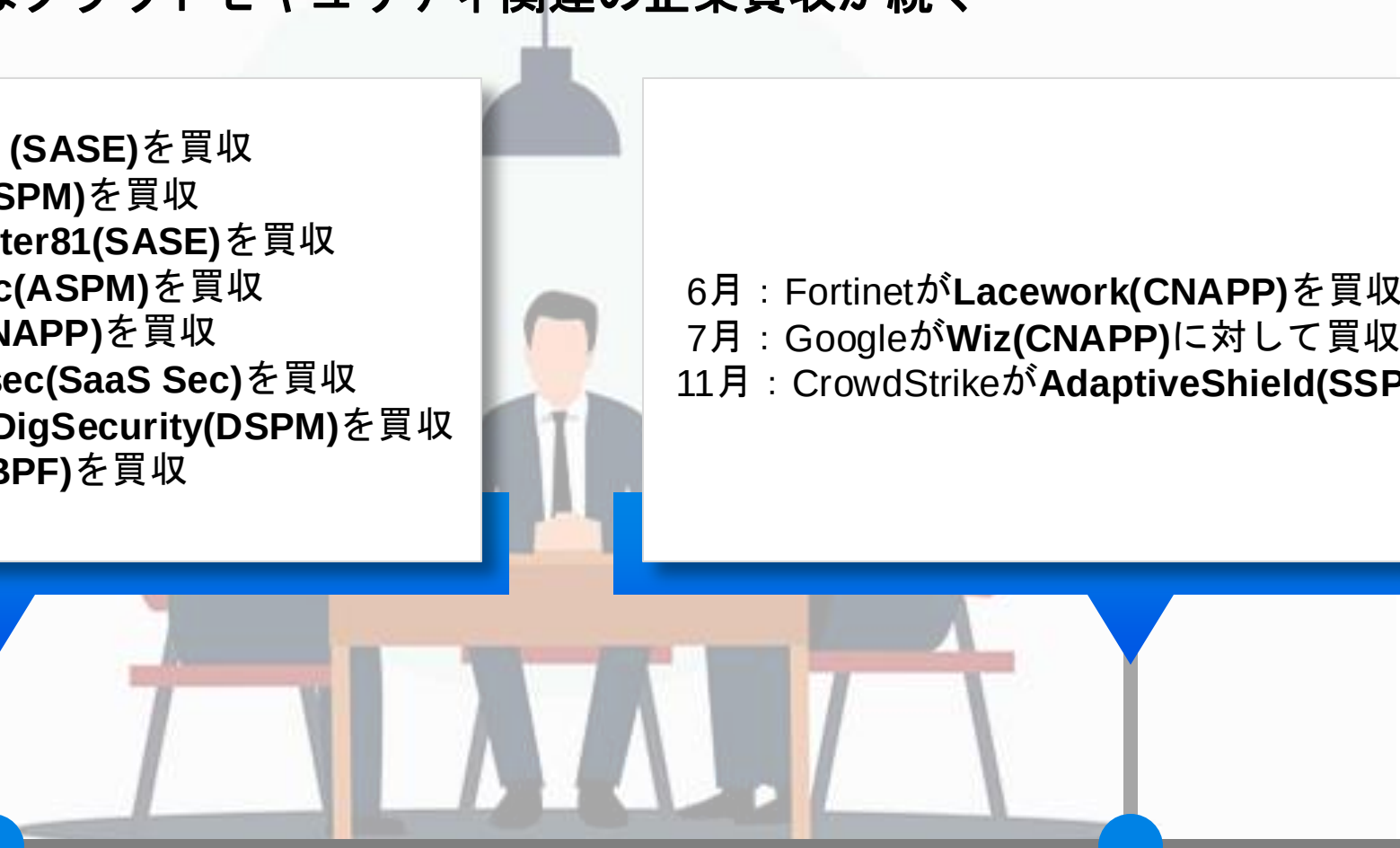
社員・利用者



ソリューション名

クラウドセキュリティ界隈のざわつき

2023年～2024年ではクラウドセキュリティ関連の企業買収が続く



3月：HPEが**Axis Security (SASE)**を買収
3月：Ciscoが**LightSpin(CSPM)**を買収
8月：CheckPointが**Peremiter81(SASE)**を買収
9月：CrowdStrikeが **Bionic(ASPM)**を買収
9月：tenableが**Ermetic(CNAPP)**を買収
9月：Check Pointが**Atmosec(SaaS Sec)**を買収
10月：PaloAltoNetworksが**DigSecurity(DSPM)**を買収
12月：Ciscoが**Isovalent(eBPF)**を買収

2023

6月：Fortinetが**Lacework(CNAPP)**を買収
7月：Googleが**Wiz(CNAPP)**に対して買収交渉も失敗
11月：CrowdStrikeが**AdaptiveShield(SSPM)**を買収

2024

CASB/SSE/SASEの関係性

CASB（Cloud Access Security Broker）

ユーザのクラウドへのアクセスを可視化、分析し非認可クラウドサービスへのアクセス状況を把握したり、各クラウドサービスのセキュリティレベルの把握が可能。APIでの各クラウドとの連携することで、データプロテクションや振る舞い検知、脅威防御などの様々な機能を提供します。

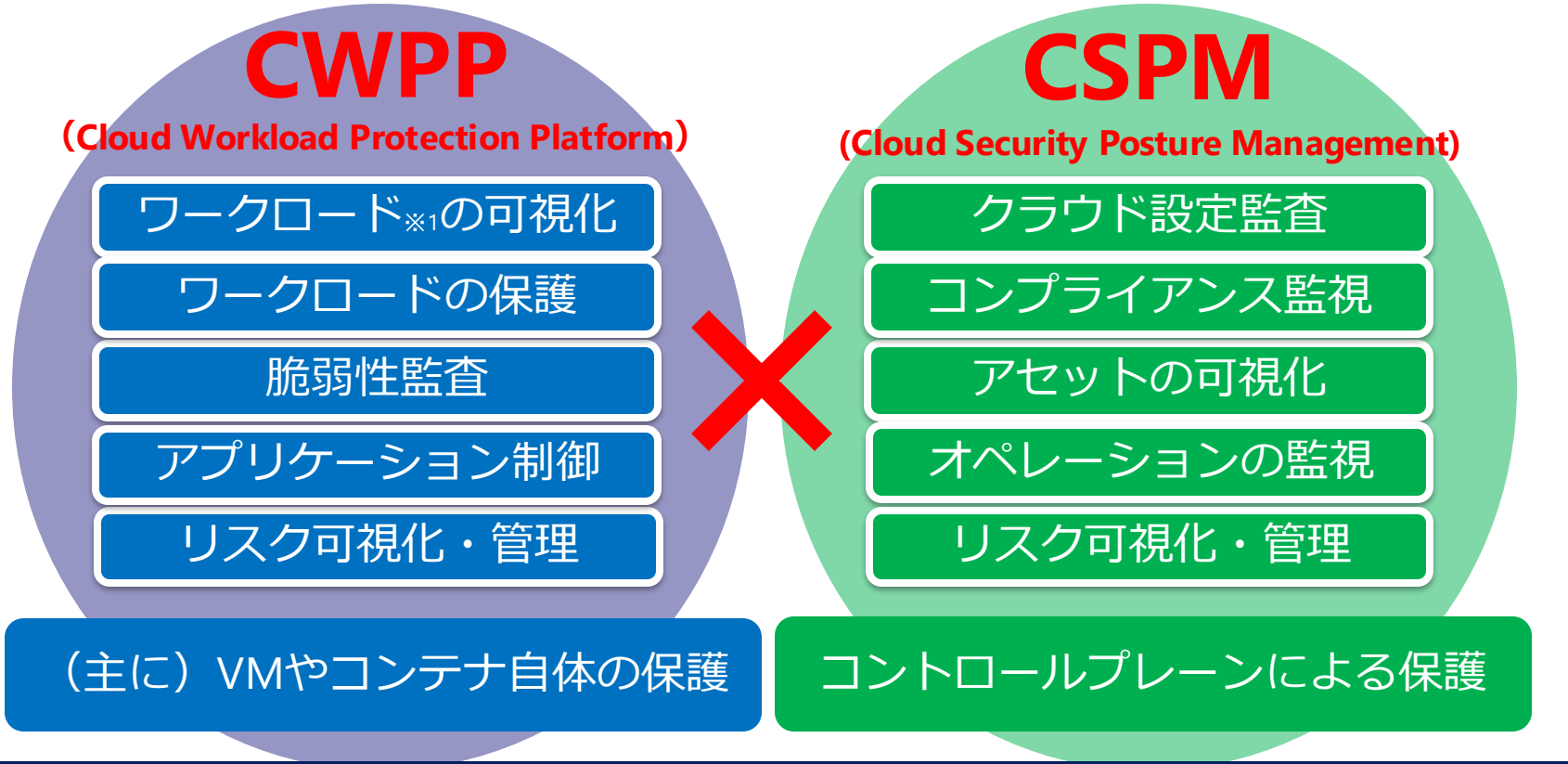
SASE（Secure Access Service Edge）

SASEはクラウド中心のソリューションで、従来の境界型セキュリティに関する課題を、クラウド中心のセキュリティ機能と、
ネットワークソリューションを組み合わせて提供することで解決します。

SSE（Secure Access Service Edge）

SASEにおけるSecurity As A Serviceの部分の機能を提供するものをSSEとして扱います。
コアの機能としては、「ZTNA」「CASB」「Secure Web Gateway（Proxy）」があげられます。

Cloud Native Application Protection Platformとは



CNAPP

追加の期待値
- DevSecOpsの手助け
- KSPM（Kubernetes管理）※2
- CIEMの統合（最小特権）

など

CNAPPの目的

開発中においてもセキュリティの問題についてスキャンし、ランタイムワークロードを保護する。
開発環境、実行環境を自動的、且つ継続的に監視することで、クラウド全体のセキュリティを強化。

※1 ワークロード＝ サーバー、VM、アプリケーション、データ、またはアプライアンス
※2 KSPM＝ Kubernetes Security Posture Managementの略でk8sのセキュリティ態勢管理

SaaS Security Posture Management

SSPM(SaaS Security Posture Management)の機能(※1)と仕組み

各セキュリティベンチマーク(※2)を
元にした設定診断項目を提供

検出した設定ミスの影響、
脅威レベル、改善方法を提示

利用SaaSの現在のセキュリティリスク、
コンプライアンス違反を可視化、スコア化

例)
Guestユーザープロファイルに割り当てられたAPIアクセス権を診断

通常情報共有ポータルやパートナーポータルとして使われており、こちらのSaaSでは、ゲストユーザは匿名でログインすることができます。

その為、アクセス権を最低限にして情報漏洩のリスクをコントロールする必要があります。特にAPI権限については**オフにすることが推奨**されています。

※1 CASBの一部の機能として同等の機能を提供するベンダもあります
※2 SOC2, CIS, ISO/IEC 27001等

クラウドセキュリティへのAI活用事例

Artificial Intelligence (AI)の得意分野

音声・画像・データの認識・解析

ディープラーニング技術の進化により、膨大なデータから特長を自動的に抽出し、高精度なパターン認識が可能となりました。
複数のモデルを使い分けることで、画像や音声データの複雑な構造を効果的に解析。
さらに、高性能なハードウェアの発展により、大規模データの処理が迅速かつ効率的に行えるようになりました。

自然言語処理

膨大なテキストデータから文法や文脈を学習し、高精度な言語理解と生成が可能になりました。
特にトランスフォーマーモデル（BERTやGPTなど）が文脈の依存関係を解析し、多様なタスクで優れた性能を発揮します。

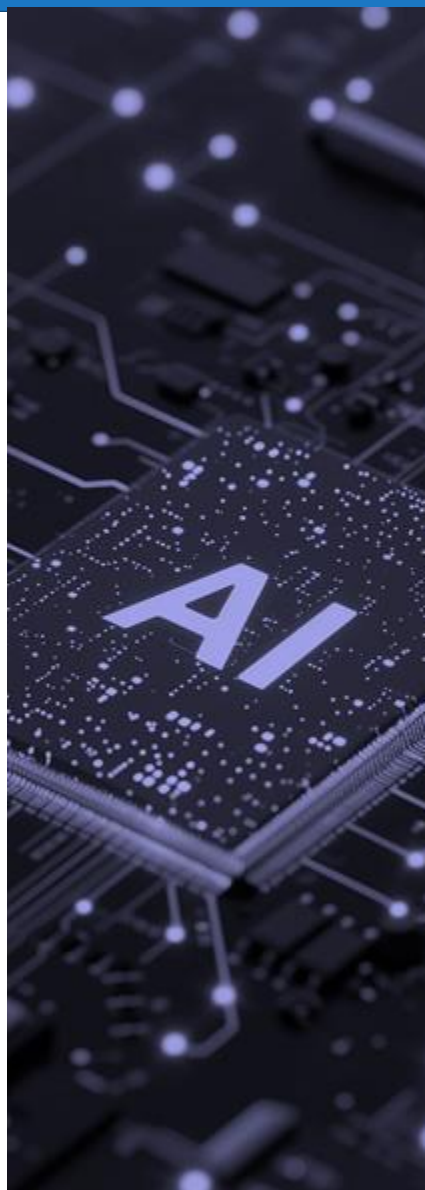
AI

データからの推論・予測

大量のデータを高速に処理し、複雑なパターンや相関を見つける能力に優れる。さらに、機械学習アルゴリズムが過去のデータをもとに将来の結果をモデル化するのに適しており、統計的手法を超えた精度の高い予測が可能となっている。

厳格な規則に則った判断

プログラムされたアルゴリズムや学習済みのモデルに従ってデータが処理されるため、厳格な規則に則った判断を行う特性があります。
この特性により、予測可能で一貫性のある結果の提供が可能です。



AIの特性を利用したセキュリティ機能例

脅威検知・振る舞い検知

・トラフィックやログデータなどの大量データをリアルタイム分析し、異常なパターンを検出する。
・機械学習（ML）を活用して、通常時と異常時の振る舞いを区別し、未知なる脅威に対応する。

対話機能（言語処理）

・高度な検索文を作成しなくても、対話形式で必要な情報を整理し表示してくれる。
・攻撃パスの説明、次のアクションへの分かりやすい言葉での指示を出してくれる。
・大量の非構造化データの中から機密情報や個人情報などを識別する

脆弱性管理とリスク評価

・システムやネットワークの脆弱性を自動的にスキャンし、リスクを優先順位付け。
・新たな脅威インテリジェンスを分析し、攻撃の可能性を予測

自動インシデント対応

・低リスクのセキュリティアラートに対するフィルタリングや初期対応を自動化
・SOARなどの自動化の部分で、プログラムの特別な知識が無くても自然言語のやり取りでプロセス作成が可能になる。

具体例①

脅威検知・振る舞い検知

SSE/CASBなどでユーザのトラフィックやダウンロードするファイルの分析、振る舞い解析、DLP（Data Loss Prevention）などにも応用されている

脅威検知・振る舞い検知でのAI活用具体例

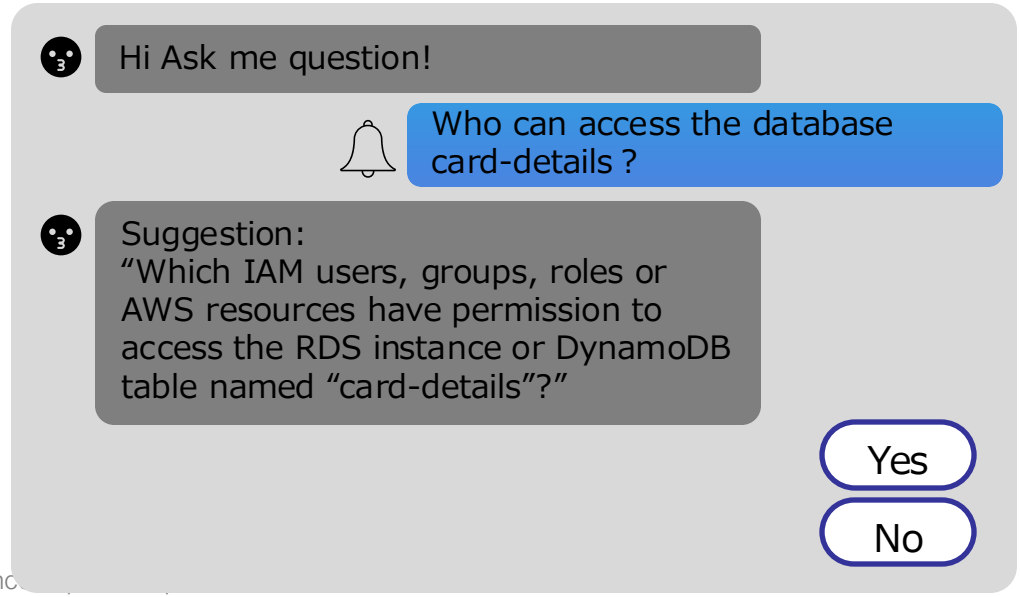
・AI/ML ドキュメント分類
・フィッシングサイト検知
・MLベースのインラインリアルタイムマルウェア検出
・自然言語処理による動的URLカテゴリ分類
・AI/MLアルゴリズムを活用した異常動作の識別

対話機能（自然言語処理）

セキュリティ管理者に特定の専門知識が無くても、ポリシーで利用する正規表現の設定、難しい検索クエリの作成、プログラマブルなワークフローの作成などを、自然言語のやり取りのみで実現できる。

対話機能の具体例

・自然言語による対応の調査・指示



具体例②

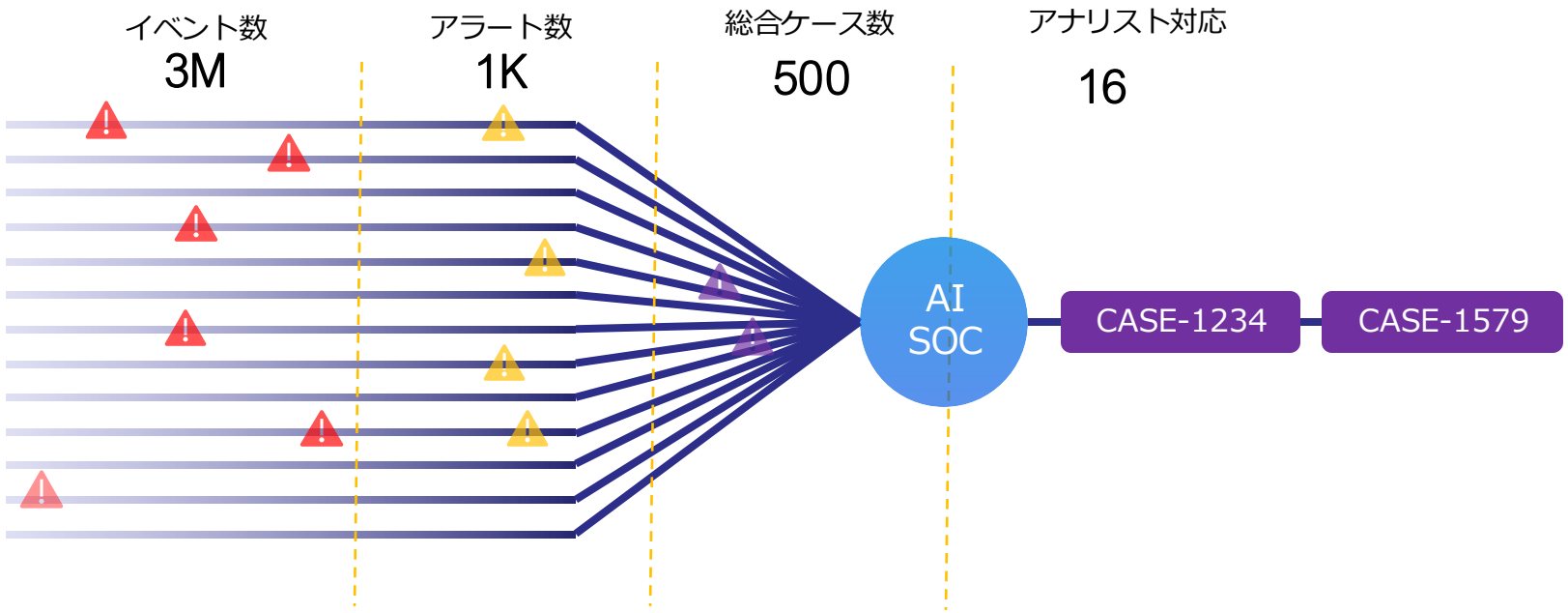
AI-SOC：高度化、複雑化、高速化する攻撃に対するAIを利用したセキュリティ運用支援

自動インシデント対応

XDR, SOAR, MDRなどの代替として、AIがアナリストに代わり、インシデント分析、トリアージなどのセキュリティ業務を自動で行います。

自動インシデント対応
AI活用具体例

- 脅威検知と対処の自動化
- トリアージ
- アラートのサマリ
- 関連情報の自動収集
- 脅威インテリジェンスの統合
- 仮想アナリストによる情報提供



「セキュリティ計画」の最適化・自動化

バックグラウンド

ロ 昨年、米国証券取委員会（SEC）がサイバーセキュリティに関する開示を義務付ける規則を制定

- 重大な（Material）サイバーインシデントが発生した際に**４日**以内に開示する義務
- **全ての企業にリスク管理、戦略、ガバナンスに関する重要な情報の年次開示する義務**
- 日本国内には同じような義務を課す法規制は無いが、米国に上場している日本企業は対象

ロ AIによる攻撃の展開スピード向上、多様化

- 防御側の準備不足を衝かれる可能性
- セキュリティ製品で検知・対処できるかの確認に多くの時間と労力が使われることに
- イリノイ大学の研究ではChatGpt4.0では**One Day脆弱性の８７%を自立的に悪用できる**との論文が出ている※。

ロ プラットフォーム化が進む大手セキュリティ商材

- １つの大手製品において、ライセンスの追加や有効化することでカバーできる対策が増加、全ての把握が困難か
- 重複するセキュリティ機能、重複するセキュリティ投資の問題

★セキュリティ計画するためのレポートがExcel等で行われる現状から脱却が必要
★ツールを使うことで迅速な攻撃の変化にも対応
★重複する製品カバレッジを見極めたROI

Cyber Defense Planning & Optimization と Automated Security Control Assessment の概要

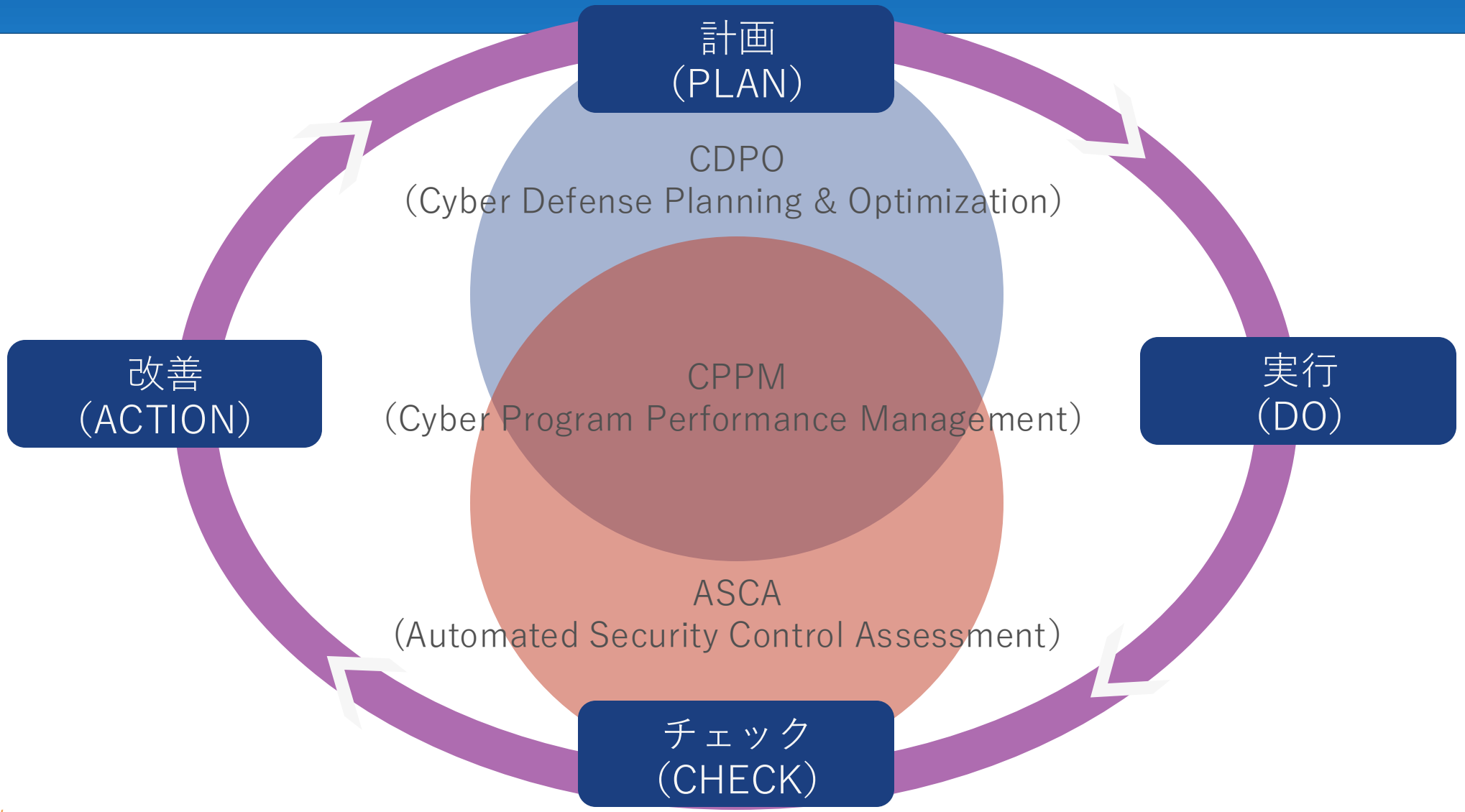
CDPO (Cyber Defense Planning Optimization)

サイバーセキュリティの計画と最適化を通じて企業の防御力を高めるソリューション。CDPOは、AIなど専門知識を活用し、サイバーリスクの評価、攻撃面の縮小、リソースの効果的な配分を支援します。これにより、攻撃の早期対応が可能となり、セキュリティ投資の最適化が実現します。
特に**CISO**の戦略的意思決定に役立つツールとして設計されています。

ASCA (Automated Security Control Assessment)

サイバーセキュリティ管理を自動化することで、セキュリティ対策の評価や不正設定の検出、リスク削減を行うプロセスです。セキュリティポリシーや防御策の継続的なチェックを提供し、リアルタイムでの脆弱性修正とコンプライアンス維持を支援します。オンプレミスやクラウドベースのセキュリティソリューションを対象にプロアクティブな設定の評価が可能となるソリューション。

CDPOとASCAの関係性



CDPO/ASCA

CDPO
(Cyber Defense Planning & Optimization)

概要	解説
リスク評価と優先順位付け	専門知識を活用して、リスクを評価し優先順位を付けます。重要なリスクや対応策に集中できるよう、リアルタイムで情報を更新して意思決定をサポート
動的な予算最適化	予算のシミュレーションやコスト効果の分析を提供。限られたリソースで最も効果的な防御策を確保し、サイバーセキュリティ投資の最大限の価値を引き出すことが可能に。
ツールの統合と重複排除	複数のセキュリティツールの統合を促進し、冗長なツールや操作を削減します。例えば、CDPOの一部ベンダでは「セキュリティスタックマップ」を通じて、現在のセキュリティ対策の可視化と最適化を実現します。
戦略的自己評価とデータ駆動型の意思決定	リアルタイムのデータとAIなどによる分析に基づき、CISOが過去のパフォーマンスを評価し、改善すべきポイントや予測。これにより、セキュリティ対策の精度を高め、透明性のある報告が可能になります。
経営陣や取締役会とのコミュニケーション支援	戦略的なレポート作成機能も備える。ビジネスリーダーに対する明確な説明や意思決定へのサポートを提供し、組織全体での理解と協力を促進する。

ASCA
(Automated Security Control Assessment)

概要	解説
継続的なセキュリティ評価	セキュリティ製品の設定ミスや検出ギャップを定期的に監視・修正し、セキュリティリスクを低減します。企業のセキュリティ体制が最新の脅威にも対応できるようになります。
誤設定の自動修正と管理	セキュリティ製品の設定ミスが原因でリスクが生じがちですが、ASCAはこうしたミスを検出し、リアルタイムで修正することで、人的エラーの影響を最小化
優先順位に基づくリスク対応	脅威インテリジェンスと組み合わせてリスクの優先順位を設定し、最も影響度の高い問題から修正を実行します。これにより、重要な脆弱性への迅速な対応が可能です
監査とコンプライアンスの効率化	企業がGDPRやHIPAAなどの規制を満たすために必要な評価と報告を自動化し、コンプライアンス関連の作業を大幅に簡素化します。定期的な手動監査の負担が軽減され、コストも削減できます
脅威と攻撃パターンの連携管理	既存のセキュリティツールやフレームワーク（例：MITRE ATT&CK）と連携し、脅威パターンに基づく防御策を強化。最新の攻撃手法にも対応可能な包括的なセキュリティ体制が構築可能

CDPO/ASCA

CDPO
(Cyber Defense Planning & Optimization)

概要	解説
リスク評価と優先順位付け	専門知識を活用して、リスクを評価し優先順
動的	
ツー	
戦略 駆動	
経営 コミュニケーション支援	スリーダーに対する明確な説明や意思決定へのサポートを提供し、組織全体での理解と協力を促進する。

1．自社セキュリティスタックの可視化

・導入しているソリューションのNIST等のフレームワークのカバレッジ
・機能が重複するツール
・脆弱性対応、インシデントレスポンス等の運用状況

2．ROI

・NIST等のフレームワークを用い、現時点の投資状況分析と将来強化すべき分野の検討

3．設定監査（オンプレ、SaaS、その他セキュリティ製品）

・導入機器のライセンス、設定を分析
・設定変更による改善効果を提示

ASCA
(Automated Security Control Assessment)

概要	解説
継続的なセキュリティ	セキュリティ製品の設定ミスや検出ギャップを定
	ンに基づく防御策を強化。最新の攻撃手法にも対応可能な包括的なセキュリティ体制が構築可能

レポート機能

利用イメージ例① CDPOの一例

登録した運用中のプロダクトのアセットタイプとNIST2.0の対比表を自動出力

	Devices	Applications	Networks	Data	Users
Identify	A B C	H F	G F		O M
Protect	B C	H	D G		
Detect	B C		D G		O M
Respond					
Recover		H F		H F	
Govern	A B C	B	A B	A B	A B

セキュリティ予算の最適化

	Devices XXX$	Applications XX$	Networks XXX$	Data XXX$	Users XXX$
Identify	151,000	170,000	125,000	30,000	100,000
Protect	176,500	100,000	300,000	40,000	120,000
Detect	200,000	120,000	125,000		220,000
Respond	140,000	45,000	25,000		
Recover	50,000			50,000	
Govern	30,000				35,000

利用イメージ例② ASCAの一例

運用中の製品の設定を監査

設定監査結果に基づく分析
①各種脅威に対するリスクと推奨設定を提示
②コンプライアンス診断
・NIST/MITRE等のフレームワークとのGap分析
・改善策提示

SSPMのように特定のフレームワークへの準拠の可否ではなく、特定の脆弱性や攻撃キャンペーン毎に、EDRなどのセキュリティ製品の設定によるリスク診断と推奨設定を提示

画面例

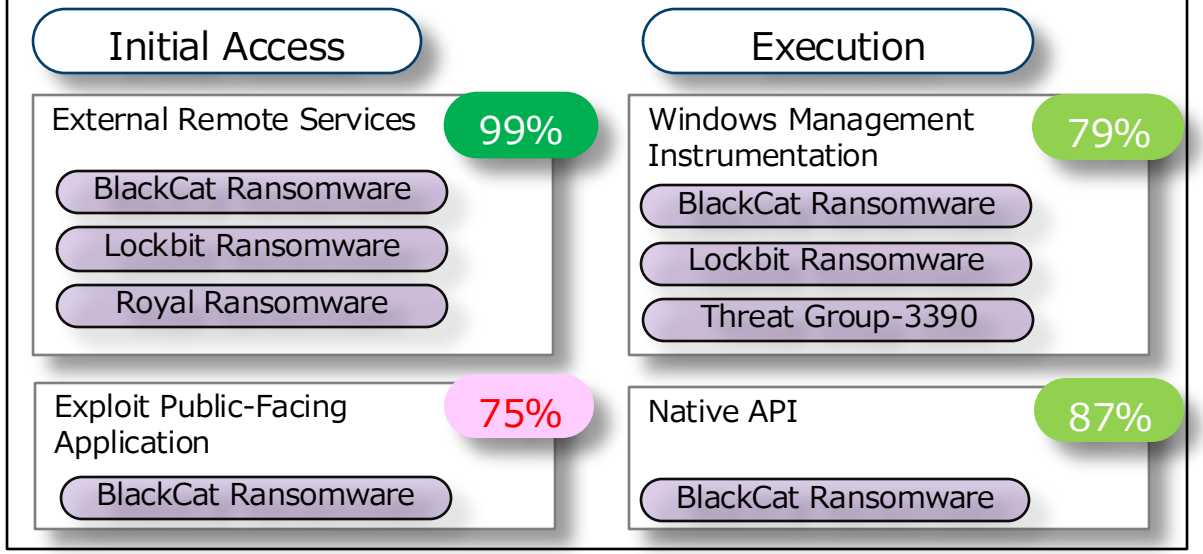
C WindowsのDriver Protectionの機能を有効にしてください

成熟度　・・・　Basic
必要条件・・・　機能Aのライセンス
OS　　・・・　Windows 10 以降
詳細情報・・・　xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

設定方法・・・　コンソール > Configure > Policies > Windows tab
において、Driver Protection機能をEnableにしてください。

ある脅威に対するMITREフレームワークを用いた分析
それぞれの脅威に対する自組織のカバー率を算出

画面例



さいごに

・クラウドセキュリティの自動化（ツール化）はAIをベースにした機能の拡張・高速化により日進月歩で進化しています。すでに導入済みのクラウドセキュリティ製品でも追加で機能が実装されていくことになります。

・今までは自動化が難しいとされたセキュリティ運用や計画についてもＡＩにより自動化の実現が可能となっている

・セキュリティベンダの学習データは基本的に英語のケースが多い、自然言語処理の部分は日本語でも同レベルの対応ができるかは確認が必要

・クラウドセキュリティのAI機能で自組織のデータを扱う場合、AIの学習データがどこに、どのように保存されるか、使われ方等について利用規約を必ず確認すること

「AI × クラウドセキュリティ」は セキュリティ人財不足を打開するだけでなく、サイバー脅威の早期検知、自動対応、リスク予測などが新たな標準に押し上げる革新的な技術アプローチです。