

人、デバイス、AI Agent が共存する ゼロトラスト環境を実現する SASE の今後



シスコシステムズ合同会社
セキュリティ事業

Identity Security 担当セールス 福留 康修
Identity Security 担当SE 坂川 健太

2026年10月9日

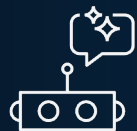
アジェンダ

- 1 人、デバイス、AI Agent の違い
および AI によってもたらされる
リスク
- 2 SASE に必要な変化
- 3 関連ソリューション

アジェンダ

- 1 人、デバイス、AI Agent の違い
および AI によってもたらされる
リスク
- 2 SASE に必要な変化
- 3 関連ソリューション

AI エージェント: 回答からアクションへ



AI チャットボット



データ拡張型 AI(RAG)



エージェント型 AI

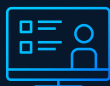
AI の自律性向上に伴い、入出力だけでなくアクションの管理もセキュリティの重要課題に

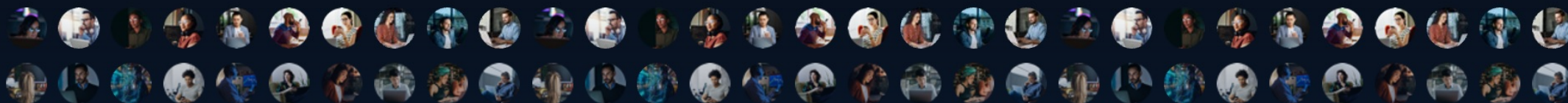
デバイス ID と AI エージェントの ID における急増



比較 - 人 (Human ID) とデバイス (Non-Human ID)

サービスアカウント、シークレット、エージェント、トークン、API キー、SSH キー、ボット、その他...

	人 Human ID	デバイス Non-Human ID	
	攻撃ベクトル	クレデンシャルスタッフィング、ソーシャルエンジニアリング、MFA 疲労、パスワード再利用、内部脅威	権限超過のサービスアカウント、シークレット漏洩 (コードリポジトリ内)、トークン盗難
	脆弱性	脆弱または再利用されたパスワード、不適切に構成された MFA、孤立したアカウント (不適切なオフボーディング慣行)	認証情報のローテーションの欠如、(過剰な) デフォルト権限、所有権の欠如
	ガバナンス フレームワーク	一元化、IT 部門と人事部門による管理、明確なオンボーディング/オフボーディングワークフロー、RBAC	多くの場合、ライフサイクル管理はバラバラ、かつ自動化されていない
	ライフサイクル管理	HRIS との統合	孤立したアカウントの自動検出とプロビジョニング解除が必要



AI エージェントは「両方の悪い面を併せ持つ存在」

	 人	 AI エージェント	 デバイス
対象範囲	広範	広範	限定的
速度	限定的	高速	高速
拡張性	限定的	急拡大	中程度
感性	常識/判断力あり	常識/判断力なし	厳密な実行とルール 遵守

企業の AI アプリケーション開発に潜むリスク



意思決定 1:

AI のユースケース

使用例として、コード生成、エンタープライズ検索、カスタマーサポート、エージェントアシスタント、自動化など

リスクはユースケースによって異なり、AI アプリケーションが外部の攻撃者と企業内部の内部脅威の両方にさらされる可能性



意思決定 2:

使用するモデル

社内でモデルを開発することは、コストが高く、労力を要する。

基盤モデルを利用することは、より単純で一般的。

AI サプライチェーンのオープンソースモデル、サードパーティのデータセット、その他のコンポーネントが最初から侵害される可能性



意思決定 3:

モデルのカスタマイズ

検索拡張生成(RAG)、プロンプトエンジニアリング、ファインチューニングにより、特定のコンテキストに合わせてモデルをカスタマイズ

AI アプリケーションのカスタマイズに使用されるデータが汚染される可能性があり、機密性の高いビジネスデータが抽出されたり漏洩したりする可能性



意思決定 4:

サードパーティ製 AI 活用

承認する AI アプリケーション、セキュリティレビュー方法についての決定

従業員がサードパーティの AI アプリケーションを不適切に使用し、機密性の高い内部データを共有すると、そのセキュリティとプライバシーの危険性



意思決定 5:

連携対象アプリケーション

サードパーティ製ツールを活用して複雑なワークフローを実行し、さまざまなエンタープライズアプリケーションにおいて自律的な処理を実施

AI エージェントが自律的なワークフローを実行し、サードパーティ製ツールと連携することで、機密データが露出したり、悪意のあるコードが実行されたりする可能性

自立型 AI Agent がもたらす既存インフラへの影響

サイバー脅威、ダウンタイム、そして質の低いユーザー体験から身を守るために、
可視性と実用的なインサイト: 洞察力 = 本質を見抜く力の必要性はかつてないほど高まっています。

数兆個の
エージェント

エージェントは、人間より、
450%も多くのトラフィック
を生成します

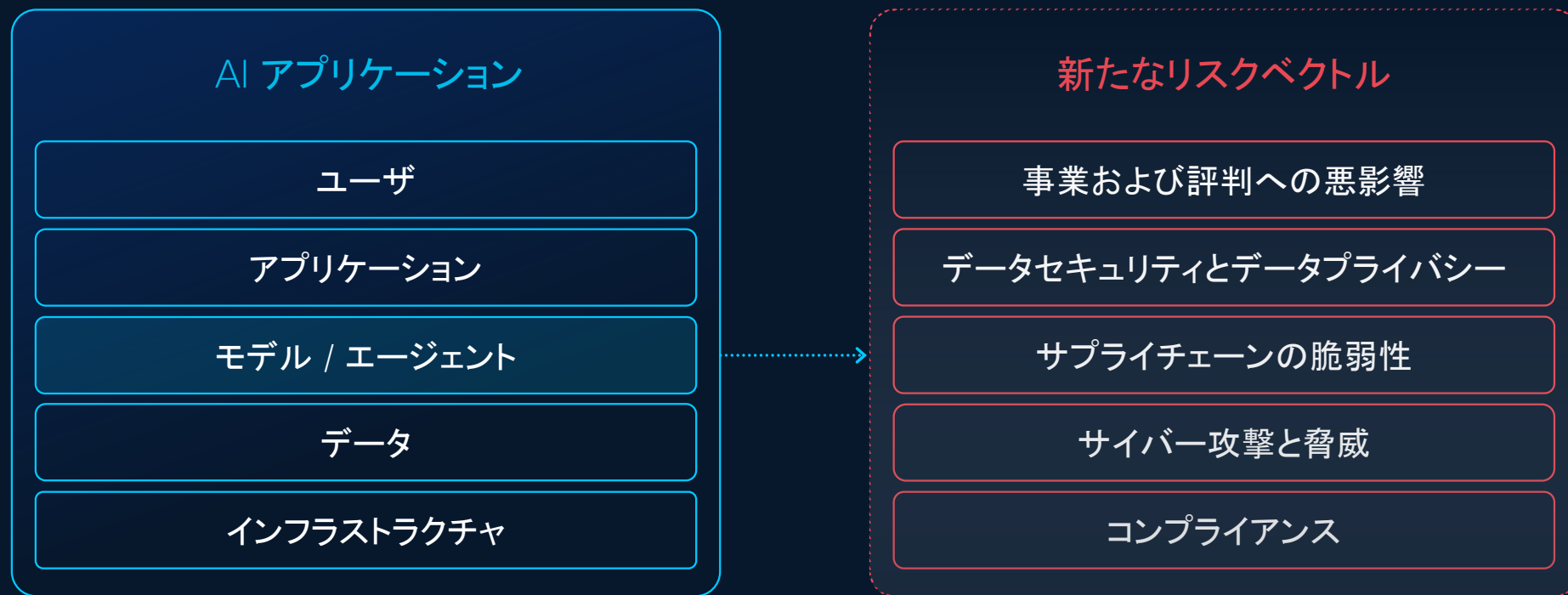
生成されるデータ

3つの主要な課題: 複雑さ、制御、可視性

Global 2000企業では、セキュリティとITの問題によるダウンタイムは、
直接的な費用と収益損失だけで年間4,000億ドル(およそ60兆円)の損失をもたらしています。

AI アプリケーションによってもたらされるリスク

AI アプリケーションは複雑で、非決定論的



管理されていない AI リスクの影響



金銭的損害



訴訟リスク



評判の低下



ポリシー違反



セキュリティリスク



知的財産漏えい

人、デバイス、AI Agent 対応ゼロトラスト環境にむけて SASE に必要な変化

1. エージェント検出

自組織の環境内(クラウド(IaaS、SaaS)、オンプレミス)にどの AI エージェントが存在するかを把握

2. 「非人間」アイデンティティ(NHI)への対応

AIエージェントがAPIやアプリケーションにアクセスするためのアイデンティティと認証への対応

3. 接続性の爆発と隠れた依存関係

MCP等の普及によるアプリケーション間通信の複雑な連鎖に起因する、AI エージェントむけの動的な通信制御

4. サードパーティリスク

悪意のあるコードの取り込み、外部サービスへの機密データ流出、コンプライアンス違反、ライセンスリスク等のリスク除去

5. 通信内容の「ブラックボックス化」による従来型境界防御の無効化と情報の流動化

人間(LLM)およびAIエージェントの通信に潜む機微なデータ授受、悪意ある利用の可視化と制御

6. より細かな権限／認可設定

AI 操作(コマンド)レベルの細かな権限設定と動的な制御



通信の主体は「人間」から「エージェント」(NHI) へ。SASEは 接続の制御から
「振る舞いの制御」へ進化しなければならない (LLM, RAG, AI Agent に対応)

アジェンダ

- 1 人、デバイス、AI Agent の違い
および AI によってもたらされる
リスク
- 2 SASE に必要な変化
- 3 関連ソリューション

SASE に必要な進化 – アイデンティティ セキュリティ

保護すべき対象は「人」だけではありません。人(Human)・デバイス(Device)・AI Agent(AI Identity) を統合管理し、継続的に信頼を検証することが、これからのゼロトラストの基盤となります。

⚠ 変化するIdentityリスク

⚡ 攻撃の加速

AIによる侵入スピードの急速な高速化

🔴 自動化脅威

ランサムウェア攻撃の自動化・高速化

🔴 セッション攻撃

Cookie窃取によるセッションハイジャック

🔴 ソーシャル攻撃

AIを悪用したVishing・ソーシャルエンジニアリング

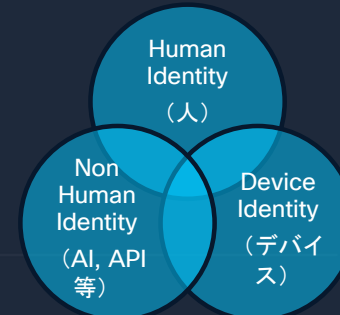
新たな標的

AI Agent・Machine Identity・AI Identityへの攻撃

🛡 求められる4つのIdentity Security対策

① 統合管理(IAM)

AI AgentのIdentityも
ユーザ・デバイスと
共に統合管理



② フィッシング耐性を持つ認証

- 近接認証
- Passkey/FIDO2
- Device Trust
- リスクベース認証

侵入を防ぐ

③ 継続的なIdentity監視 (ISPM & ITDR)

- 異常な認証
- 権限昇格(オンプレAD含む)
- AI Agentの異常利用
- Machine Identityの悪用
- ラテラルムーブメント検知

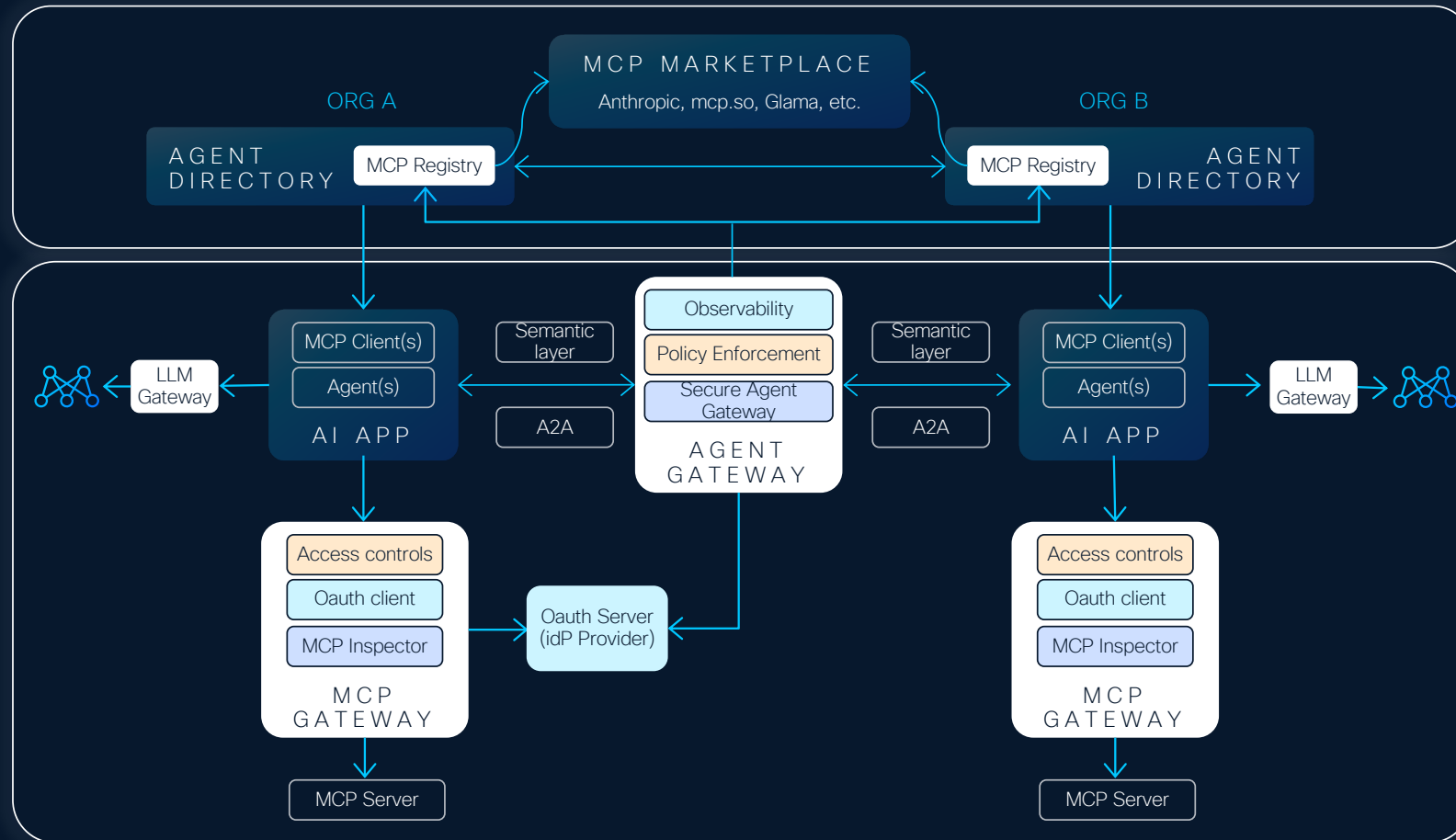
侵入後の
被害拡大
を防ぐ

④ セキュリティと利便性の両立

- Passwordless
- SSO
- シームレスな認証

セキュリティを
強化しながら
業務を止めない

SASE に必要な進化 – 安全な AI 利用のためのセキュリティ機能



サプライチェーン保護

侵害されたモデル、エージェント、
インフラストラクチャのリスクを軽減

Agent レジストリ

MCP レジストリ

モデル ファイル スキャン

アルゴリズム的レッドチームング

ランタイム保護

継続的なセキュリティと運用の完全性

Agent から LLM への通信

MCP クライアント／サーバ通信

Agent から Agent Gateway (A2A)

AI リスクを概説する業界標準

シスコ統合 AI セキュリティおよび安全フレームワーク



OWASP Top 10 for LLMs

OWASP Top 10 for Agentic
Applications



MITRE ATLAS



NIST Adversarial ML Taxonomy

現在利用可能な最も包括的で将来を見据えたアプローチの一つ

アジェンダ

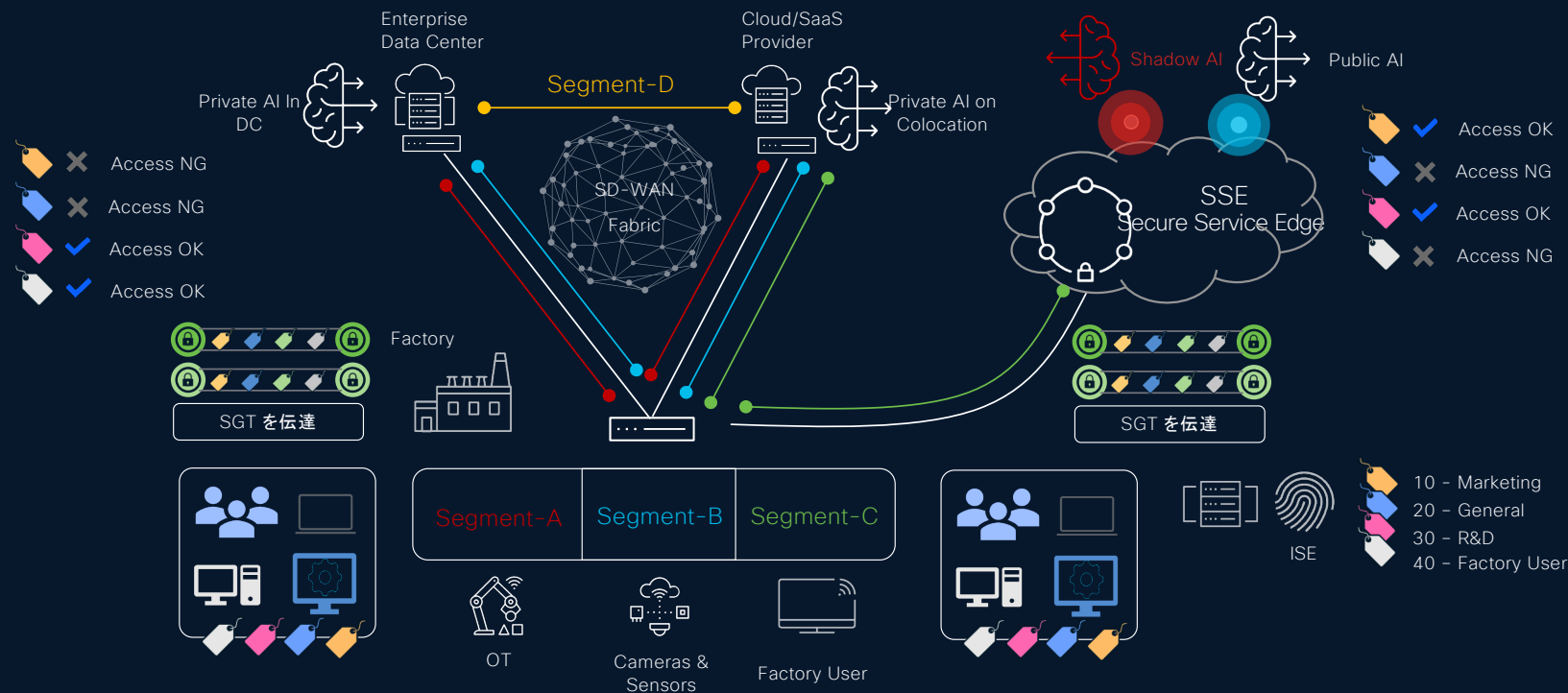
- 1 人、デバイス、AI Agent の違い
および AI によってもたらされる
リスク
- 2 SASE に必要な変化
- 3 関連ソリューション

AI エージェント時代のシスコ ネットワーク セキュリティ

AIを意識したネットワーク構成例

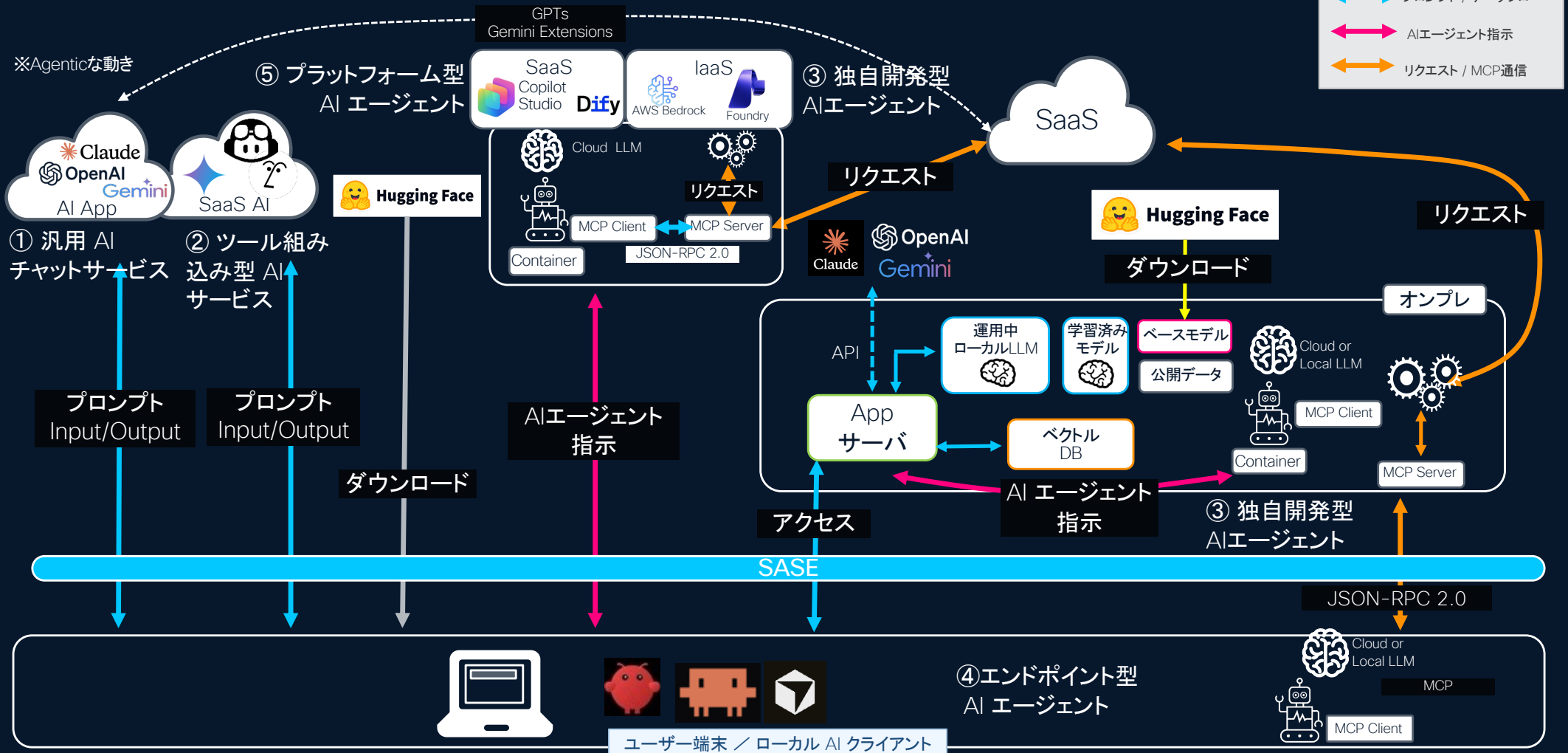
マクロセグメンテーションの中で、タグ付けを行いさらに小さなセクションに分割。個々に対して独自のセキュリティポリシーを設定してアクセス制御を適用する手法。

Common Policy(Micro Segmentation)でのアクセスコントロール

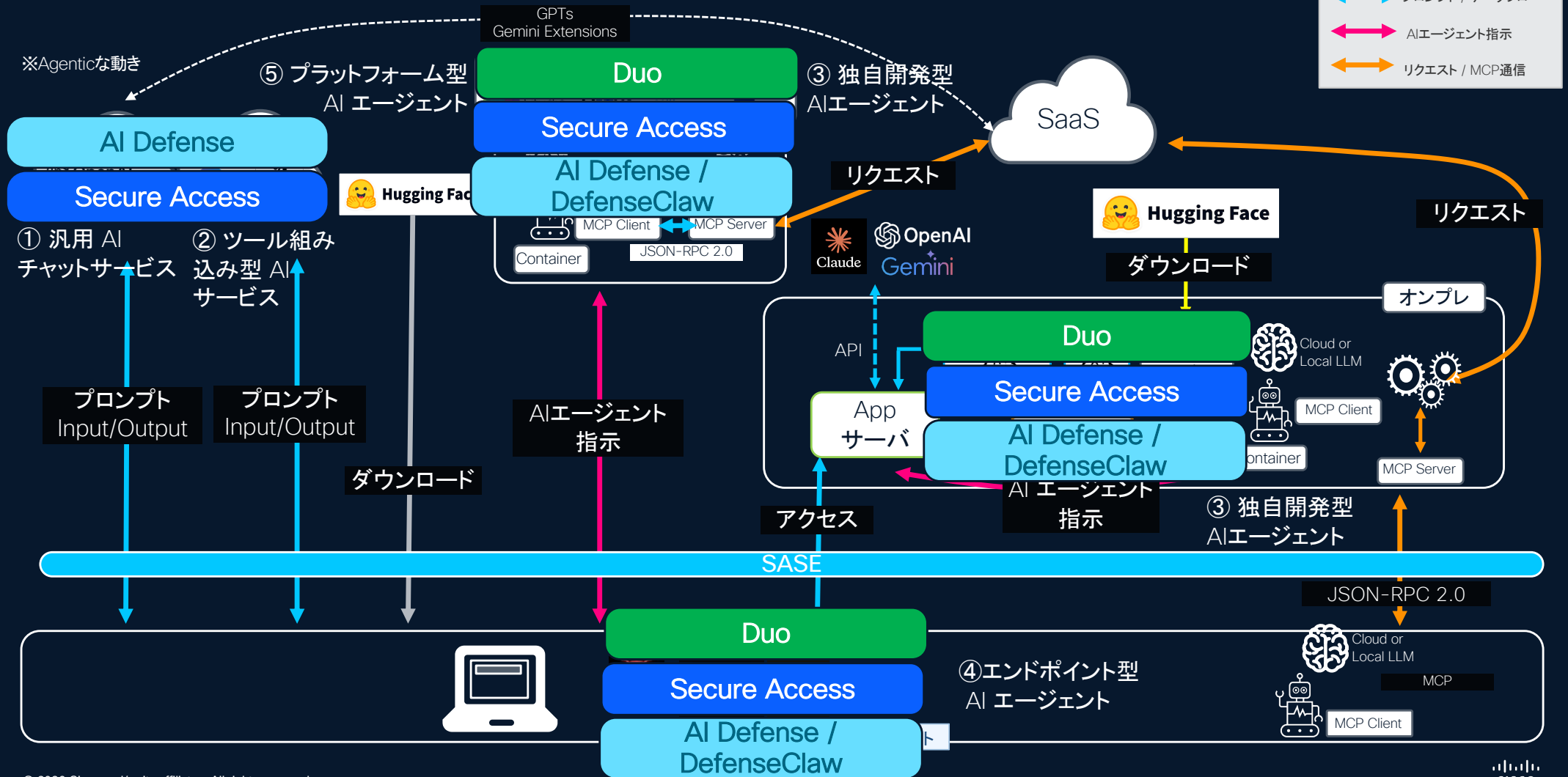


従来のACLベースでは実現できない、属性やビヘイビアに応じたダイナミックかつ詳細なセグメンテーション、有事のキル・スイッチにも対応

業務における AI のユースケースと SASE の関係



業務における AI のユースケースと SASE の関係



AI エージェント時代のシスコ セキュリティ – AI エージェントにも対応したゼロトラスト

ゼロトラストセキュリティを AI エージェントの領域まで拡大

認証・認可・振る舞いのリスク

すべてのエージェントを把握

③ ④ ⑤

AI リスクを把握する
エージェントの検出と監視

Duo

すべてのアクションを承認

③ ④ ⑤

AI エージェントを保護する
エージェントの ID と認証

Duo

③ ④ ⑤

AI へのアクセスを制御する
きめ細かな認可と適用

AI Defense

Secure Access

Duo

プロンプトのリスク

リアルタイムにリスクに対応

AI の脅威、ふるまいの
コンテキストを理解、制御する
安全性およびセキュリティ脅威
に対するランタイム保護

AI Defense

Secure Access

① ②
③ ④
⑤

レジリエント インフラストラクチャ / ライブプロテクション / Project Glasswing

「AI Agent 自体の保護」

サプライチェーンや実行環境 (ランタイム) のセキュリティ

AI Defense / DefenseClaw

③ ④ ⑤

AI Agent 自体(コンポーネント)のリスク

悪意ある攻撃から AI の実行環境そのものを保護

まとめ

1. AI 時代の新たな脅威とビジネスへの影響

- アイデンティティの爆発的増加
- アイデンティティのタイプ(人、デバイス、AI Agent)で必要なセキュリティ施策が異なる
- プラスだけではないビジネスへの影響

2. SASE に求められる進化:「接続」から「振る舞い」の制御へ

- アイデンティティ セキュリティを拡張し、「人」、「デバイス」、「AI エージェント」対応へ
- AI セキュリティに対する多面的防御(サプライチェーン、ランタイム保護)
- ネットワークとセキュリティを統合し、振る舞いにもとづくダイナミックな制御とセグメンテーション対応

3. なぜシスコのセキュリティなのか

- AI トークンエコノミーに対応可能なハードウェアを含めた戦略と幅広いポートフォリオ
- 標準化への貢献(OWASPやMITRE等の主要フレームワーク策定等)と広範なセキュリティ カバレッジ
- AI エージェント特有のリスクに対応し既存インフラを踏襲してゼロトラストを拡張

まとめ

1. AI 時代の新たな脅威とビジネスへの影響

- アイデンティティの爆発的増加
- アイデンティティのタイプ(人、デバイス、AI Agent)で必要なセキュリティ施策が異なる
- プラスだけではないビジネスへの影響

2. SASE に求められる進化:「接続」から「振る舞い」の制御へ

- アイデンティティ セキュリティを拡張し、「人」、「デバイス」、「AI エージェント」対応へ
- AI セキュリティに対する多面的防御(サプライチェーン、ランタイム保護)
- ネットワークとセキュリティを統合し、振る舞いにもとづくダイナミックな制御とセグメンテーション対応

デモで紹介

3. なぜシスコのセキュリティなのか

- AI トークンエコノミーに対応可能なハードウェアを含めた戦略と幅広いポートフォリオ
- 標準化への貢献(OWASPやMITRE等の主要フレームワーク策定等)と広範なセキュリティ カバレッジ
- AI エージェント特有のリスクに対応し既存インフラを踏襲してゼロトラストを拡張

