

AI共創を支えるデジタル環境ガードレールの取り組み ～多層防御の1ピース：Netskope～

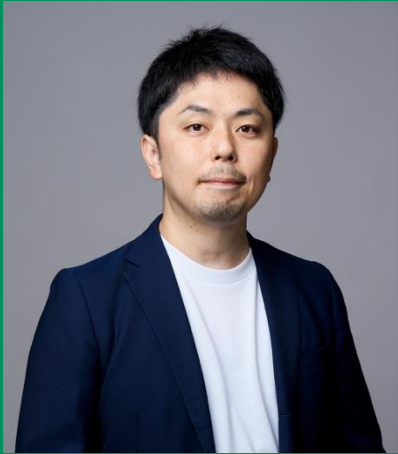
三井住友カード株式会社 デジタルイノベーションオフィス

ソフトウェアディベロップメントオフィス プラットフォームエンジニアリンググループ

グループ長 児島 恭平

2026年10月2日（金）

自己紹介



三井住友カード株式会社
デジタルイノベーションオフィス
ソフトウェアディベロップメントオフィス
プラットフォームエンジニアリンググループ
グループ長 児島 恭平

- Sler、大手監査法人、大手ネット銀行を経て、2023 年に三井住友カード株式会社へ入社
- 三井住友カードにて、システムリスク管理業務 及び M&A案件のITデューデリジェンスに従事
- その後、公共交通機関向けソリューション「stera transit」のシステム担当等を歴任後、デジタルイノベーションオフィスに着任
- ソフトウェアディベロップメントオフィス・プラットフォームエンジニアグループの立ち上げを担い、手の内化プラットフォーム「Polaris」の構築・運営に従事

三井住友カード株式会社

項目	内容
設立	1967 年 12 月 26 日
資本金	340 億 3 千円（2026年3月末時点）
代表者	代表取締役社長 佐々木 丈也
従業員数	5,200 人（2026年3月末時点）
事業内容	クレジットカード業務、デビットカード・プリペイドカード・ その他決済業務、ローン業務、保証業務、信販業務、 トランザクション業務、その他付随業務
株主	株式会社三井住友フィナンシャルグループ



世界を変えるキャッシュレスをつくる

沿革

1980	2007	2019	2020	2021	2023
日本初	日本初		日本初		
日本初のVisaカード	日本初の銀聯カード	決済プラットフォーム「stera」	公共交通機関向けソリューション「stera transit」	三井住友カード（NL）	個人向け総合金融サービス「Olive」
国内外共通で利用できる「住友VISAカード」発行	中国・銀聯カードを日本で初めて発行	事業者向けの次世代決済プラットフォーム	公共交通機関にクレジットカード等のタッチ決済を導入	券面から番号を無くした次世代カード	銀行・カード・証券等を1つに

ビジョン

VISION	MISSION	グループ中期経営計画
The most innovative cashless company. 未来の当たり前をつくる最も先進的なキャッシュレスカンパニー	世界を変える キャッシュレスをつくる	過去最大のIT投資 ITトランスフォーメーション - IT基盤の抜本的強化とAI活用のさらなる加速 -

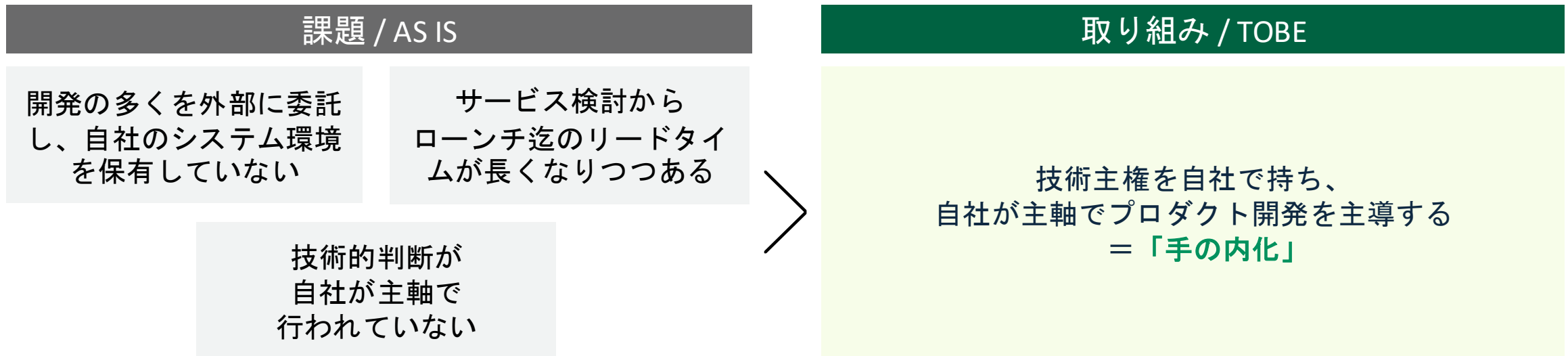
Agenda

- 1 デジタルイノベーションオフィスと「手の内化」推進
 - 2 デジタル環境の構築
 - 3 開発スピードとセキュリティを両立させるガードレール
 - 4 AI共創に向けて
-

01 デジタルイノベーションオフィスと 「手の内化」推進

エンジニアリング専門組織の立ち上げ

デジタルイノベーションオフィス（DIO）は2025年9月に設立
IT・デジタルプロダクト開発を専門的に行うエンジニアリング組織



ビジネスにテクノロジーで貢献する：テクノロジーによる顧客価値の最大化

「手の内化」とは

技術主権を自分たちで持ち、自社が主軸でプロダクト開発を主導すること

「顧客への価値提供の最大化」のためには アジャイル / プロダクトドリブン がセット



「手の内化」とは、顧客に速く・最大の価値を届けるための方法

プラットフォームで実現しようとしていること

目指す先はプラットフォームエンジニアリングによる認知負荷の削減
開発チームがプロダクト開発に集中できる環境を創出する

ソフトウェアエンジニアの「認知負荷」とは

内在的認知負荷 Intrinsic	業務ロジック等（開発チームの領域）
外在的認知負荷 Extraneous	インフラ基盤・CI/CD・セキュリティ等
学習関連認知負荷 Germane	Golden Path テンプレート・ 開発者ドキュメント・Runbook

排除

支援

プロダクト開発の「生産性を向上」するために

プラットフォームエンジニアリングとは、ソフトウェア開発者を支援するツールとプロセスを構築する技術
開発者がソフトウェアを作る過程全体で必要とするものを満たすように設計されたセルフサービスを作るようなもの。これらのツールとワークフローを提供することで、**開発者がより速く、より効率的に作業できるようにする**

Platform engineering is the art of building tools and processes that empower software developers. It's like creating a self-service station specifically designed to meet developers' needs throughout the software creation journey. By providing these tools and workflows, platform engineering helps developers to work faster and more efficiently.



一貫したセルフサービス体験でケイパビリティを取得・利用し、
開発に集中できるエコシステム「Polaris」を構築

手の内化プラットフォーム「Polaris」

技術主権を担う「Polaris」を構築

2026年6月より本格稼働（8月顧客向けプロダクトリリース）



「Polaris」は技術主権を担う手の内化プラットフォーム
その構築・運用およびプロダクト開発のために「デジタル環境」が必要だった

02 デジタル環境の構築

コンセプト

プロダクト開発に必要な環境をアジリティを持って揃えていく

クラウドネイティブ

AIネイティブ

開発体験・生産性を向上するスムーズなコラボレーション

ツールは必要なものを早く使い始める
整備されたツールを選び、早く調達し、自分たちで育てる

場所を選ばず、リアルタイムでコラボレーション
円滑かつ迅速にコミュニケーション/意思決定を行う

エコシステムによるプロダクトドリブンの支援
コラボツール・開発ツールの連携によるスムーズな運営

AI共創によるスピード向上と品質向上

設計・実装・テストをAIと分担する
AIエージェントによる一人当たりの開発スピード向上

レビューと検査を自動化する
パイプライン組込・コンテキスト読解等にて品質向上

定例・定型作業の自動化による業務生産性向上
属人化排除やシフトアップによる高度業務への集中

クラウドおよびAIのアジリティを最大限に活用することを選択

デジタル環境 = 出島環境

技術主権を自分たちで持つため、既存環境の延長ではない選択

既存環境 | SMBCグループ共通の堅牢な基盤

グループ共通の運用

SMBCグループとして整備された標準の仕組み

金融機関の堅牢性

統制・監査・セキュリティを共通で担保する

安定して動かせる

堅牢な基盤の上で既存業務を安全に支える

制約 技術選定は共通ルールに従い、柔軟性が低い



デジタル環境 | やりたいこと

技術主権を自社に持つ

環境・技術を自分たちの手の内に置く

使いたいものを自分たちで選択する

クラウド・AIの進化にその都度追従する

素早く作って素早く変える

クラウド/AIネイティブのアジリティを活かす

だから 出島環境として切り出し、選択の自由を

技術主権を自分たちの手の内に置くために 出島環境 を選択

優先事項はエンジニアがプロダクト開発に集中できること

外在的認知負荷を排除するためルールベースではなく、
細かく制御ができる仕組み・ガードレールが必要だった



開発チームはガードレールの中で プロダクト開発 に集中する

03 開発スピードとセキュリティを両立させるガードレール

デジタル環境の現在地

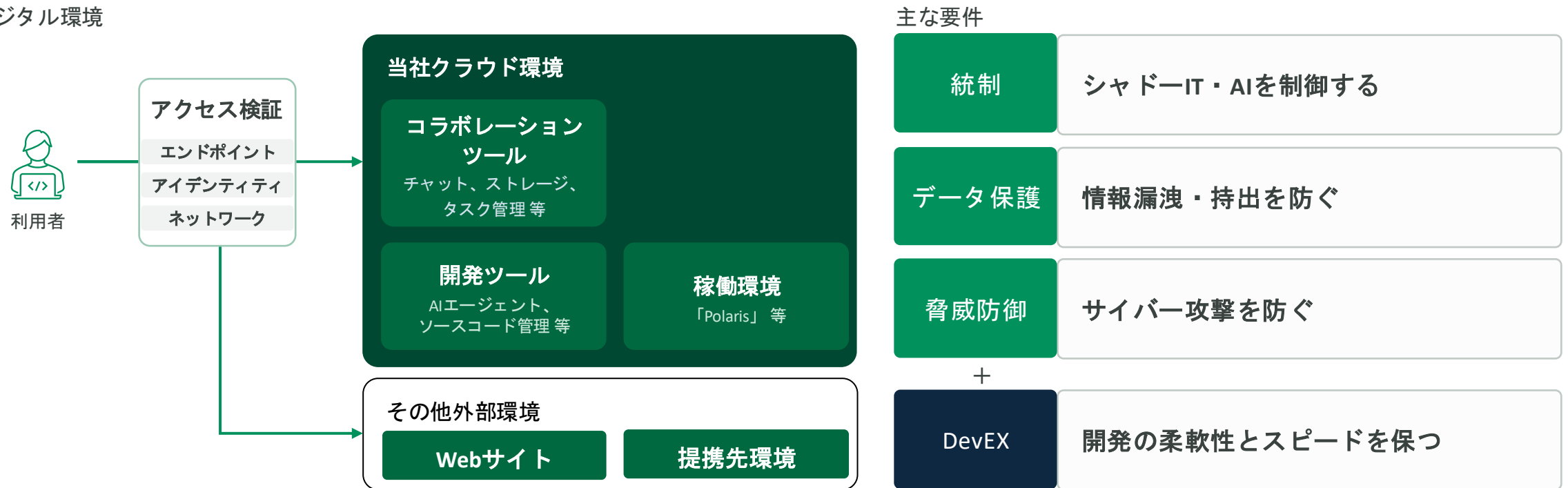
AIエージェントを最大限に活用するための環境を整備・運用開始済
クラウドネイティブかつAIネイティブな機能に沿ったセキュリティ対策が必要



クラウドネイティブ / AIネイティブにおけるセキュリティ要件

境界型セキュリティ：外部へアクセスさせないではなく、
インターネット接続が当たり前の状態でのセキュリティ要件：ゼロ・トラスト・セキュリティを検討

デジタル環境

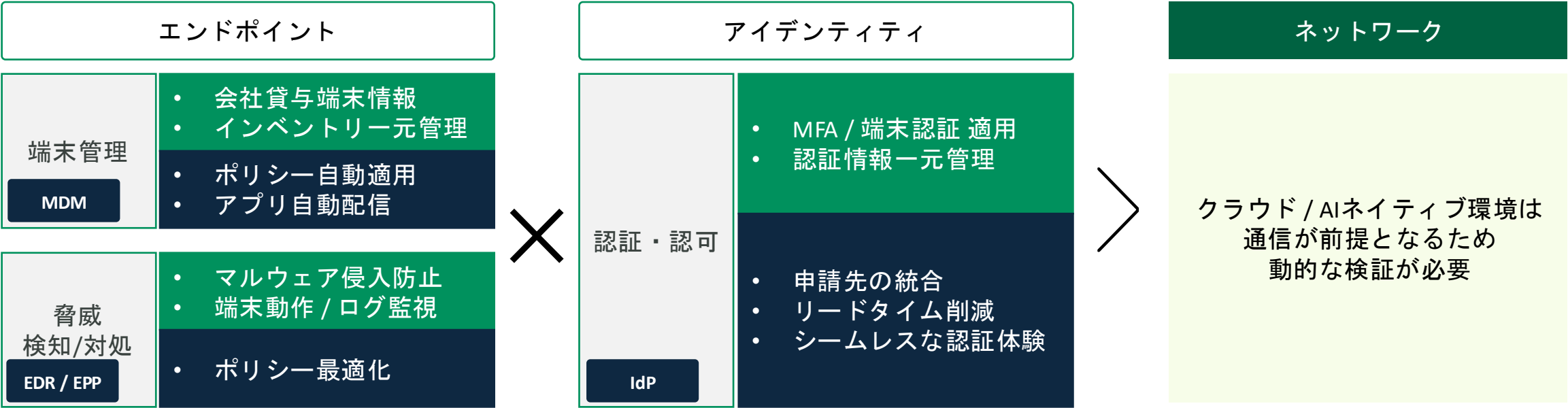


開発者体験（DevEX）とセキュリティを両立させることが重要だった

エンドポイント/アイデンティティセキュリティ

安全なモノ と 正しいヒト を識別することから始めた

アクセス検証



端末 / 認証・認可により正当な権限のアクセスを担保
アクセス先が正当かの検証は通信レイヤーで

ネットワークセキュリティ

つまりは・・・

アクセス検証

ネットワークセキュリティ要件



通信レイヤーで漏らさず制御することが必要であり、その検証を行った

Netskopeの決め手

当社環境に対してノックアウト要件なし および CASB由来の独自機能で細かい制御が可能

SaaS(当社テナント)アクセス制御

当社が利用する
コラボレーションおよび開発ツール
に対しての制御の細やかさ

- ドメイン制御、テナント識別
- インスタンス制御

サービス毎の細かな制御により、
開発生産性に影響を与えない制御が可能

DLPによる情報漏洩対策

単一製品でendpoint / Network / Mail
のDLPを実装、またUEBAと連携によ
るスコアリング

- データ検知、インライン制御
- 行動分析による制御

誤って持出をしてしまうような事象も
各レイヤーで制御され、利用者の認知負
荷を軽減可能

脅威防御

マルウェア対策（Threat Protection、
SandBox）、DNSセキュリティ等を実
装可能

利用者は意識せずに
ネットワークレイヤーでの
セキュリティが実装されている

開発生産性との両立を実現するため、細かな制御をガードレールとして設定

アジリティと統制を両立する

デジタル環境として細やかなポリシーを設定し続け、上質な開発者体験を捨てない選択をする

実装状況

ポリシー名	概要	設定数
Real-time Protection	SaaS・Web利用をインラインで許可／制限	77
Endpoint Protection	端末エージェントの動作と保護の設定	6
SSL復号	復号して検査する通信と除外対象の定義	8
DLP	機密情報の持ち出しを検知するルール	7
Threat Protection	マルウェア・不審ファイルの検知と遮断	1

ハマったポイント

カテゴリ：ストレージのブロック

Amazon S3

開発コンテナ環境の証明書相違

コンテナは独自証明書となり、
Netskopeルート証明書と相違。FQDN
単位でAllowリストに追加。今後コン
テナ内へのCA配布を検討。

Web会議の挙動遅延

会議の参加時の起動が遅いといった問合せが発生。各種Web会議側が公式に推奨するSSL復号を、対象範囲のみ除外とした。

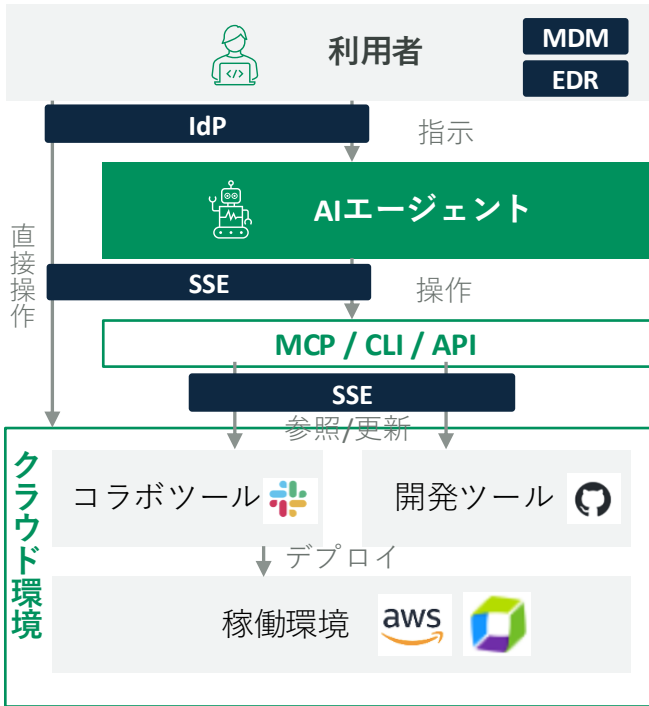
設定したら終わりではなく、DevEXおよびセキュリティを両立するための設定を継続

04 AI共創に向けて

AI共創・最大活用のためのガードレールを提供

AI駆動だからこそAI Security を備えたプラットフォームを提供する

AIネイティブのデジタル環境



AI駆動のセキュリティ対策

端末	AIエージェント
✓ シャドーAIの検知・ブロック ✓ AIエージェントが提案するライブラリや拡張機能のインストール統制	✓ エージェントのID・権限管理 ✓ 許可されたエージェントのみの利用制限 ✓ プロンプトへのDLP制御 ✓ プロンプトインジェクションへの対応
MCPサーバー	クラウド環境
✓ 接続MCPサーバーの可視化・棚卸 ✓ MCPによる権限制御 ✓ MCP接続の認証・認可	✓ エージェントの権限管理 ✓ シークレット管理 ✓ 振る舞い監視・管理

AIエージェントとMCPが新しい出入口となるため、権限・接続先・ログで押さえていく

ご清聴ありがとうございました