Chrome Enterprise Premium で実現するゼロトラストモデル事例

～運用セキュリティと開発アジリティの両立～

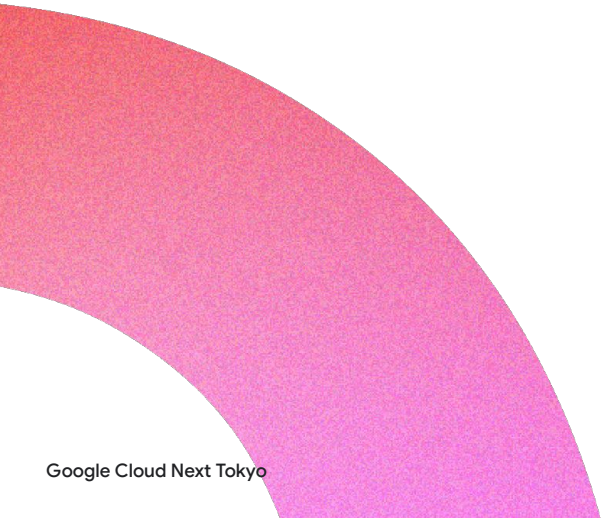
Google Cloud Next Tokyo

砂川 鉄雄

パーソルキャリア株式会社
テクノロジー本部
ITマネジメント&インフラ・
セキュリティ統括部
インフラ部
クラウド基盤グループ
マネジャー

アジェンダ

01 我々が直面した 2 つの課題
02 CEP 導入で解決するスコープ
03 導入技術
04 導入結果
05 まとめ



01. 我々が直面した 2 つの課題

従来環境の課題

『生産性』と『セキュリティ』のジレンマ

1. 境界型防御の限界
2. 機密データ取り扱い
3. デバイスのソフトウェアの制限

新環境 のコンセプト

ゼロトラスト・セキュリティの採用

クラウド中心のデータ管理

開発者の生産性向上

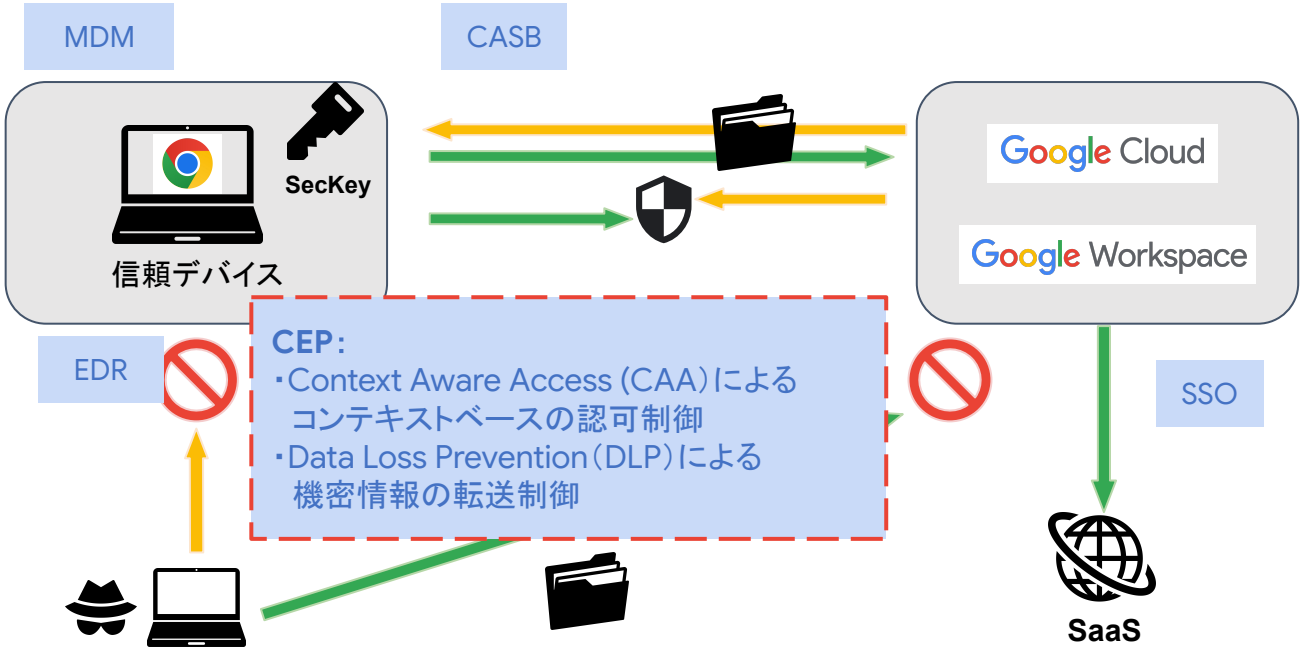
新環境の課題

『自由』と『統制』のジレンマ

開発者に与えた「自由」（管理者権限、自由なソフト導入）と背中合わせになる、新たなセキュリティリスクへの対応

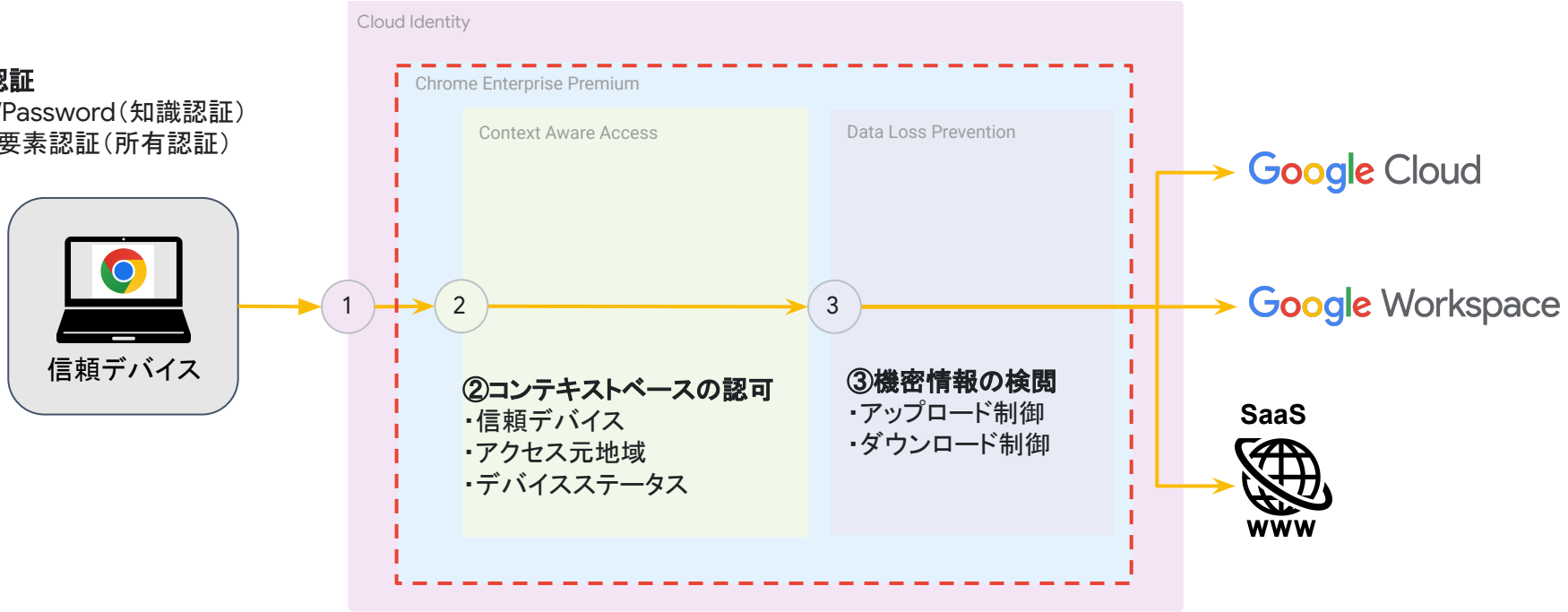
02. CEP 導入で解決するスコープ

課題解決のアーキテクチャ全体像



CEP を用いたセキュリティ強化のステップ

①認証
・ID/Password（知識認証）
・二要素認証（所有認証）



03. 導入技術

戸田 尚希

パーソルキャリア株式会社
テクノロジー本部
ITマネジメント&インフラ・
セキュリティ統括部
インフラ部
クラウド基盤グループ
リードエンジニア

CAA によるコンテキストベースのアクセス制御

Context Aware Access（CAA）とは？

アクセス時の状況を評価し、
接続の可否を動的に判断する
セキュリティの仕組み

コンテキストとは？

認可判断の際に参照する
セキュリティに関する情報

CAA によるアクセス制御のあるべき姿

CAA 適用前

ID / パスワード認証のみに依存したアクセス

認証されていれば、**アクセス元の状態**を問わず機密データにアクセス可能。
このため、**悪意ある内部関係者**による情報持ち出しや、**ID 漏洩**時の不正アクセスを技術的に防ぐことが困難。

CAA 適用後

コンテキストに基づいた動的なアクセス認可

認証に加え、**アクセス時の様々な状況（デバイスの状態、場所、時間、振る舞いなど）**をリアルタイムに評価し認可。
ポリシーを満たさない場合は、**たとえ本人であってもアクセスをブロックしたり、操作を一部制限**したりすることが可能に。

CEP によるアクセス制御の設定ステップ

1 **デバイス コンテキストの収集**

前提準備としてデバイスのコンテキストを
収集するため Chrome ブラウザを組織に登録。

2 **Access Levels の定義**

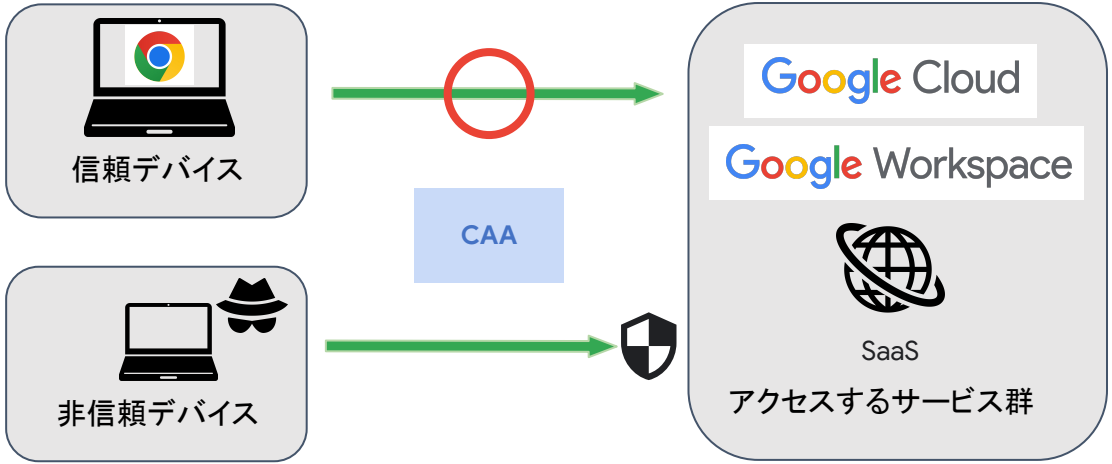
アクセス許可の条件（IP アドレス、OS バージョン、
デバイス状態など）を「アクセスレベル」としてルール化。

3 **CAA ポリシーの設定**

定義したアクセスレベルを各サービス（Google Cloud、Google
Workspace）に適用し、条件を満たさないアクセスをブロック。

導入効果

主要サービス群へのコンテキストに
応じたアクセス コントロールの実装に成功



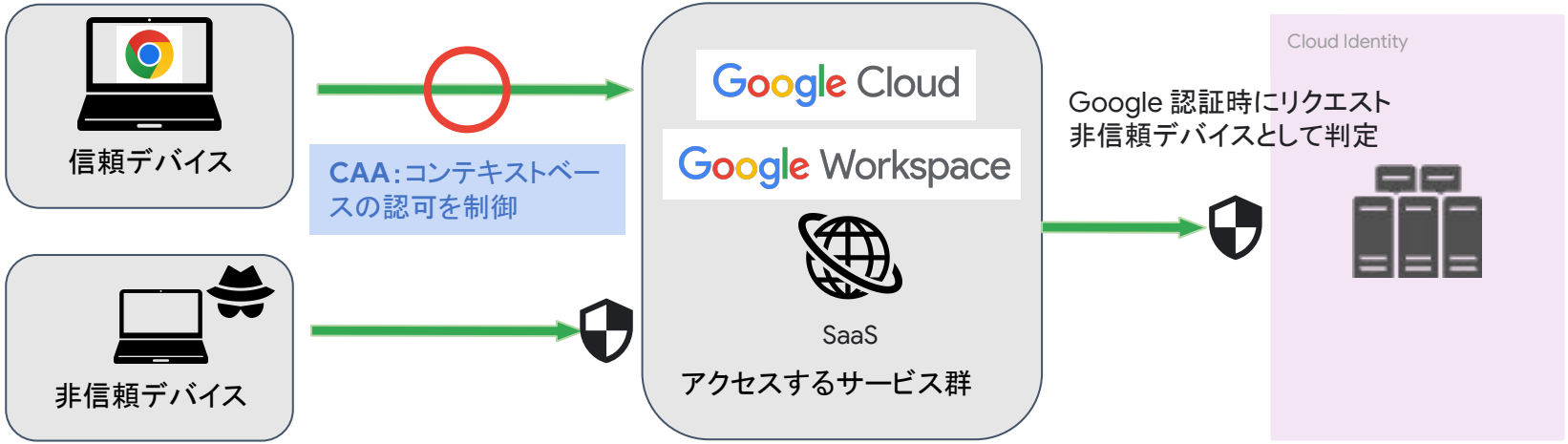
CAA 設定のハマりどころ

一部 Google サービスで機能制限発生

- Cloud Shell
- Google Apps Script

原因

- Google 認証も CAA の制御対象
- 認証リクエストが
  「信頼できないアクセス」と判定された



対策

CAA の適用を除外するアプリケーションを
restrictedClientApplication で指定する

```
# CAA の設定ファイルを作成
$ cat > settings.yaml << EOF
scopedAccessSettings:
- scope:
   clientScope:
     restrictedClientApplication:
       name: Cloud Console
  activeSettings:
    accessLevels:
    - accessPolicies/999999999999/accessLevels/xxx_xxx
EOF
```

DLP による機密情報の保護

Data Loss Prevention（DLP）とは？

ユーザーが機密情報を
許可した範囲の外と共有しようとした際に
その操作を検知し、ブロックや警告を
行うことで情報漏洩を未然に防ぐ仕組み

DLP によるデータ保護のあるべき姿

DLP 適用前

認可ベースのデータアクセス

ファイルへの**アクセス権**があれば、
その中に機密情報が含まれていても
転送が可能。
このため、従業員の**誤操作**による
意図しない情報漏洩を、
システム的に防ぐことが困難

DLP 適用後

機密情報の属性に応じた動的なアクション制御

ファイルの 転送時に内容を
リアルタイムでスキャン。
検知した機密情報の**重要度に応じてアクションを動的に変更**。

高リスク情報: 強制的にブロック
中リスク情報: 利用者に警告
低リスク情報: 監査ログに記録のみ

DLP による機密データ保護の設定ステップ

1. **ルールの作成**
   保護対象の情報と、ルールを適用する範囲、スキャンのきっかけとなる操作を定義

2. **アクションの設定**
   ルール違反を検知した際に実行するアクションを設定

3. **アラートとレポートの設定**
   ルール違反時のアラート設定とインシデント レポートの集約

導入効果

機密情報の転送検知・制御

機密情報を動的に検知し
ポリシーに該当したリクエストを
制御できるようになった。

機密情報のやり取り可視化

検知したリクエストを
アラート センターに集約。
機密情報のやり取りを
把握できるようになった。

運用課題

- 特定の業務において
  ポリシーの例外としたい
  機密情報のやり取りがあるが、
  自動的な判別が困難
- DLP 適用の例外設定を運用する
  ためのコストが高い

DLP 運用の課題：想定外アクションの対応

04. 導入結果

CEP 導入前後の比較

課題	Before	After
デバイスの信頼性証明	利用者の**自己管理やルール**に依存	**客観的な信頼性評価**が可能に
機密情報へのアクセス	**デバイスの状態に関わらず** アクセスできるリスク	CAA によりデバイス状態に合わせた **動的なブロック**の実現 **柔軟な制御**はできていない
機密情報の持ち出し	ファイル転送の**制御が不十分**	**機密情報の転送を検閲**することが可能に 一部の**ブロックが未設定**なことや、**詳細な条件に応じた動的なアクションの変更**は今後の課題。
セキュリティの考え方	**技術的な統制**に穴あり	ゼロトラストの一部実現 評価に利用するコンテキストの拡充や、より動的な制御は今後の課題

05. まとめ

まとめ

1	**背景と課題**	**『自由と統制』**という新たなジレンマの発生
2	**導入したソリューション**	CEP により**コンテキスト ベースのアクセス制御（ CAA ）と情報漏洩対策（ DLP ）**を実装
3	**導入による効果**	『自由と統制』のジレンマを解消する第一歩に
4	**今後の展望**	**「あるべき姿」に向けた運用改善**

techtekt

techtekt（テックテクト）

「techtekt（テックテクト）」は、
パーソルキャリアのエンジニアブログです。
“みんなの「はたらく」をテックでつくる”をコンセプトに、
技術、組織、学びなど、さまざまな情報を発信しています。

さまざまなテーマで事例や知見を学ぶ
IT・テクノロジー人材のための勉強会コミュニティ
「TECH Street」当社の事例を公開しています。