

安全と先進のバランスを両
立させる

Chrome Enterprise
Premium

による シャドー AI 運用



Tokyo

Proprietary



廣山 豊

アイレット株式会社

内部統制推進室 室長

CI事業部 副事業部長

AI 管理責任者

情報セキュリティ管理責任者

Google Developer Expert - Cloud

Partner Top Engineer Fellow



企業が直面する AI 利用の課題



生成 AI の急速な普及

Gemini、ChatGPT、Claude などの生成 AI ツールが急速に普及し、従業員が業務効率化のために個人的に利用するケースが激増しています。企業の公式な導入プロセスを待たずに、個人判断での利用が拡大しています。



セキュリティ統制

従来のセキュリティ対策では、多様な AI ツールの利用を包括的に管理することが困難。どの AI サービスが使用されているか、どのようなデータが共有されているかの可視化と制御が重要な課題となっています。



コンプライアンス対応

GDPR、個人情報保護法、業界固有の規制要件への対応が複雑化。AI 利用における法的責任の所在、データ処理の透明性、監査証跡の確保など、コンプライアンス要件の充足が急務となっています。

企業が直面する AI 利用の課題



生成 AI の急速な普及

さまざまな生成 AI ツールが急速に普及している。従業員が業務効率化のために個人的に利用するケースが激増。



セキュリティ統制

従来のセキュリティ対策では、多様な AI ツールの利用を管理することが困難な場合がある。



コンプライアンス対応

各要件への対応が複雑化。法的責任の所在、データ処理の透明性、監査証跡の確保など、コンプライアンス要件の充足が急務。

企業が直面する AI 利用の課題



生成 AI の急速な普及

さまざまな生成 AI ツールが急速に普及している。従業員が業務効率化のために個人的に利用するケースが激増。



セキュリティ統制

従来のセキュリティ対策では、多様な AI ツールの利用を管理することが困難な場合がある。



コンプライアンス対応

各要件への対応が複雑化。法的責任の所在、データ処理の透明性、監査証跡の確保など、コンプライアンス要件の充足が急務。

どの AI サービスが使用されているか、
どのようなデータが共有されているかの可視化と制御
= シェドウ AI 管理が求められる状況



シャドウ AI とは？

企業の承認を得ずに従業員が独自に AI ツールを使用する現象。

⚠ 具体的な利用例



機密文書の要約や翻訳を
ChatGPT に依頼



社内システムのコードレビューを
GitHub Copilot で実施



顧客データの分析を
Claude に依頼

🔍 発生要因



業務効率化への欲求



承認プロセスの遅さ



AI の多様性

シャドウ AI のリスク



セキュリティリスク

外部サービスのセキュリティ基準が不明で、データの保存場所や処理方法が企業のセキュリティポリシーに適合しない可能性がある。



コンプライアンス違反

GDPR、個人情報保護法、業界固有の規制要件に違反し、法的責任や罰金のリスクが発生する可能性がある。



ガバナンス低下

IT 統制が効かない状況が発生し、組織全体のデジタルガバナンスが低下、リスク管理が困難になる。

Chrome Enterprise Premium 概要

Chrome Enterprise Premium は、Chrome Enterprise Core の効率化された管理機能に加えて、高度なセキュリティ保護をご利用いただけるサービスです。エンドポイントセキュリティをシンプルに強化し、企業のブラウザ利用を包括的に保護します。

機能(一部抜粋)	Core	Premium
セーフブラウジング	スタンダード	リアルタイム
セキュリティインサイト	レポートのみ	対策措置実施
データ損失防止 (DLP)	-	✓
コンテキストアウェアアクセス	-	✓
URL フィルタリング	-	✓



月額 \$6

ユーザーあたり

シャドウ AI 対策の実例 ①

～ 会社標準以外のものを利用時にアラート

【準備】

URL カテゴリで Generative AI に分類されるものにアクセス時に警告を出す設定にする。検証済みのものは除外しておく。

【利用時】

警告して注意を促す。

(禁止設定をすることも可能)



アクセスしようとしたサイトは組織でフラグが付けられています

管理者からのメッセージ: 「この生成AIは未評価なんだ」

サイトへ移動

戻る

シャドウ AI 対策の実例 ②

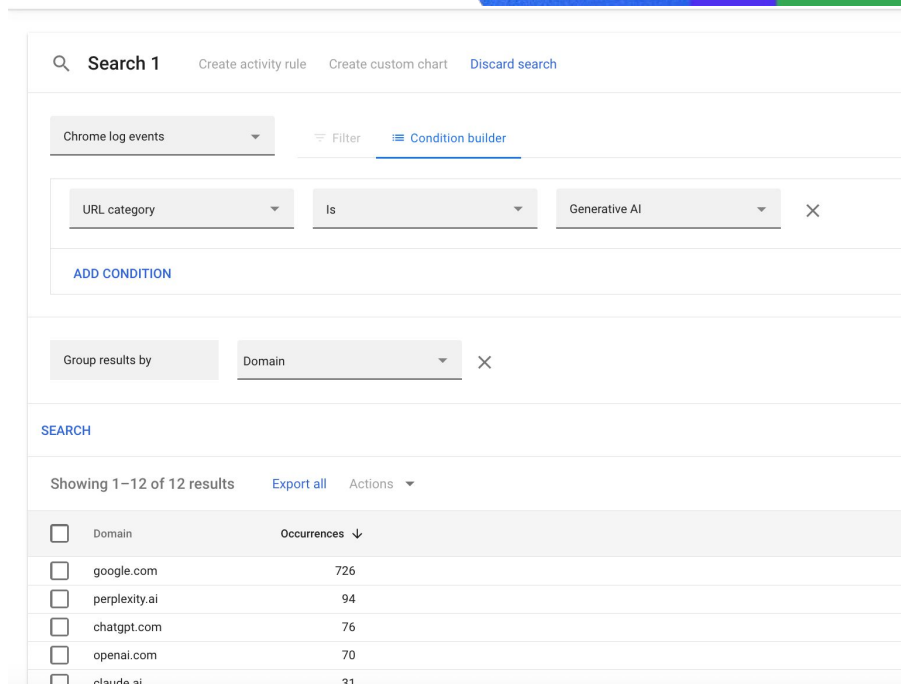
～ 使われている生成 AI サービスをリストアップ

【準備】

URL カテゴリで Generative AI に分類されるものをログ出力するようにしておく。

【検索】

コンソールのレポートから、Domain でグルーピング表示する。



The screenshot shows the Google Cloud console search interface. At the top, there's a search bar with 'Search 1' and links for 'Create activity rule', 'Create custom chart', and 'Discard search'. Below the search bar, the 'Chrome log events' dropdown is selected. The 'Filter' tab is active, and a condition is set: 'URL category' is 'Is' 'Generative AI'. An 'ADD CONDITION' link is visible. Below the filter, the 'Group results by' dropdown is set to 'Domain'. The search results are displayed in a table with columns for 'Domain' and 'Occurrences'. The results show 12 total results, with the first 12 displayed.

Domain	Occurrences
google.com	726
perplexity.ai	94
chatgpt.com	76
openai.com	70
claudia.ai	31

シャドウ AI 対策の実例 ③

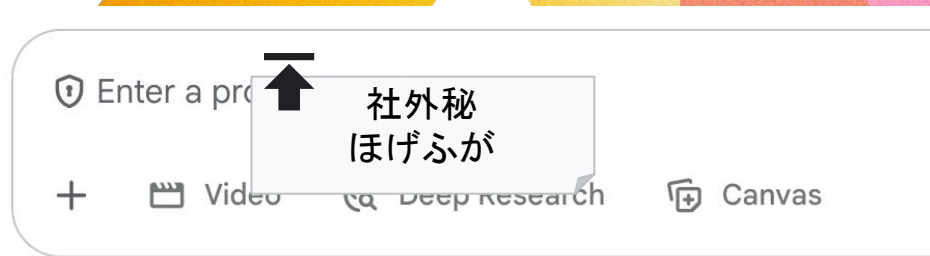
～ 社外秘文書の AI サービスアップロードを抑止

【準備】

「社外秘」文字列を含む、ファイルアップロードおよびコピペを検出および抑止。

【利用時】

ユーザー操作を遮断する。



導入アプローチ

現状評価

現在の AI 利用状況
を把握

設計

許可するもの・
禁止するものを分類

試験導入

小規模グループで
パイロット運用

本運用

全社へ導入し、継続的な
評価と改善を繰り返す

まとめ

**AI の進化は爆速で、従来の統制は追いつけないことも多い
無秩序は既存の統制レベルも落としかねない**

Chrome Enterprise Premium はその解決手段になりうる

