



AI駆動型マルチエージェントクラウド監査システム

第2回 AI Agent Hackathon with Google Cloud

富田 晋

2025-06-21



アジェンダ

1. 問題提起 - クラウドセキュリティの課題
2. ソリューション概要 - Paddiの提案
3. アーキテクチャ - マルチエージェントシステム
4. デモ - 実際の動作
5. 技術詳細 - 実装の詳細
6. 将来ビジョン - 今後の展望



問題提起

クラウドセキュリティ監査の現状



手動プロセスの課題

- ・ 時間がかかる: 数百のIAMポリシーを手動でレビュー
- ・ エラーが発生しやすい: 人的ミスによる見落とし
- ・ 専門知識が必要: セキュリティベストプラクティスの深い理解
- ・ スケールしない: マルチクラウド環境での複雑性



ビジネスインパクト

- ・ セキュリティインシデントのリスク増大



ソリューション: Paddi

Paddiとは？

🤖 AIエージェントによる自動化

3つの専門エージェントが協調して動作：

1. Collector Agent

- GCP設定を自動収集

2. Explainer Agent

- Gemini AIでリスクを分析

3. Reporter Agent

- 人間が読みやすいレポートを生成

なぜマルチエージェント？

🎯 単一責任の原則

各エージェントが専門的なタスクに集中

🔄 モジュール性とスケーラビリティ

- エージェントの独立した開発・テストが可能
- 新しいクラウドプロバイダーの追加が容易

🚀 パフォーマンス



アーキテクチャ

システムアーキテクチャ



技術スタック

🐍 Python実装

- CLIフレームワーク: Fire
- GCP SDK: `google-cloud-iam`, `google-cloud-securitycenter`
- AI統合: `google-cloud-aiplatform` (Vertex AI)
- テンプレート: Jinja2

📊 出力形式

- Markdown (Obsidian対応)

Google Cloud サービスの活用



コンピューティングサービス

- **Cloud Run:** エージェントのデプロイとスケーリング（予定）
- **Cloud Build:** CI/CDパイプライン



AIサービス

- **Vertex AI (Gemini Pro):** セキュリティリスクの分析
- **IAM API:** ポリシー情報の収集
- **Security Command Center API:** セキュリティ findings の取得



デモ

デモシナリオ

1 設定の収集

```
$ python main.py collect --project-id my-gcp-project
✓ IAMポリシーを収集: 47件
✓ SCC findingsを取得: 12件
```

2 AI分析

```
$ python main.py analyze
✓ Gemini Proで分析中...
✓ リスクスコア計算: 7.3/10
```

3 レポート生成

生成されるレポート例

エグゼクティブサマリー

- 総合リスクスコア: **7.3/10**
- 重大な発見事項: **3件**
- 推奨事項: **15件**

主な発見事項

1. 過剰な権限: 5つのサービスアカウントにOwner権限
2. 未使用的IAMメンバー: 90日以上アクセスなし
3. 暗号化の欠如: 3つのデータベース



🔧 技術詳細

Geminiプロンプトエンジニアリング



構造化プロンプト

```
prompt = f"""
クラウドセキュリティ専門家として、以下の
GCP IAM設定を分析してください：

{iam_config}
```

以下を特定してください：

1. セキュリティリスクと重要度
2. ベストプラクティス違反
3. 具体的な修正手順

形式： リスクスコア、発見事項、推奨事項を含むJSON

"""

エージェント間通信

✉ データフロー

```
# Agent A 出力
collector_output:
  timestamp: "2025-06-21T10:00:00Z"
  project_id: "my-project"
  iam_policies:
    - member: "user:admin@example.com"
      role: "roles/owner"
  scc_findings:
    - severity: "HIGH"
      category: "PUBLIC_BUCKET"
```



将来ビジョン

ロードマップ

🌐 マルチクラウド対応

- AWS (IAM, Security Hub)
- Azure (AD, Security Center)
- クロスクラウド比較レポート

🤖 高度なAI機能

- 予測的リスク分析
- 自動修復提案

ビジネスインパクト

コスト削減

- 監査時間を**80%**削減
- 手動エラーをゼロに

セキュリティ向上

- 24/7継続的監査
- プロアクティブなリスク検出

スケーラビリティ

🙏 ありがとうございました！

ご質問はありますか？

🔗 リンク

- GitHub: github.com/susumutomita/Paddi
- Website: susumutomita.netlify.app

✉️ 連絡先

- Email: (メールアドレス)

付録: 実装の詳細

セキュリティ考慮事項

- Application Default Credentialsの使用
- 最小権限の原則
- 監査ログの暗号化

テスト戦略

- 単体テスト: 各エージェント
- 統合テスト: エンドツーエンド