AI時代に必要な
セキュリティ
マネジメントスキル

Google Cloud Next Tokyo

大田原 慶道

経営企画本部

Executive Manager

Agenda

01. セッションの目的とゴール
02. セキュリティマネジメントとは
03. AIと人間の協働モデルとは？
04. AI時代に必要な
    セキュリティマネジメントスキル
05. Google Cloudで実現するには
06. まとめ

01.セッションの目的とゴール

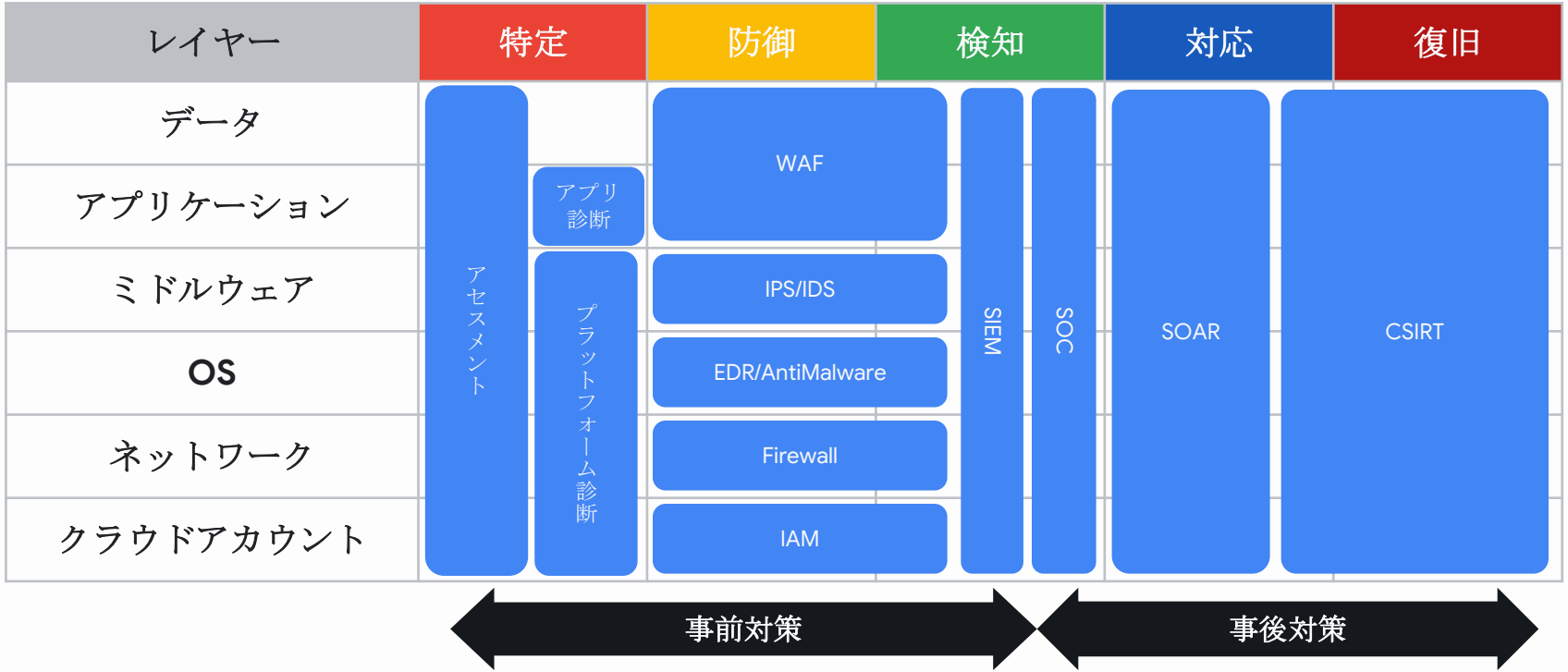
セッションの目的とゴール

クラウドセキュリティ領域での
“AIと人間の協働モデル”について解説とGoogle Cloudの最新のセキュリティプロダクトについてご紹介します。
“AIの得意とする領域”と**“人間が得意とする領域”**の両側面からアプローチし、**効率的**で**安全**な**セキュリティマネジメント**の実現方法をユースケースを交えてご案内します。

02.セキュリティマネジメントとは

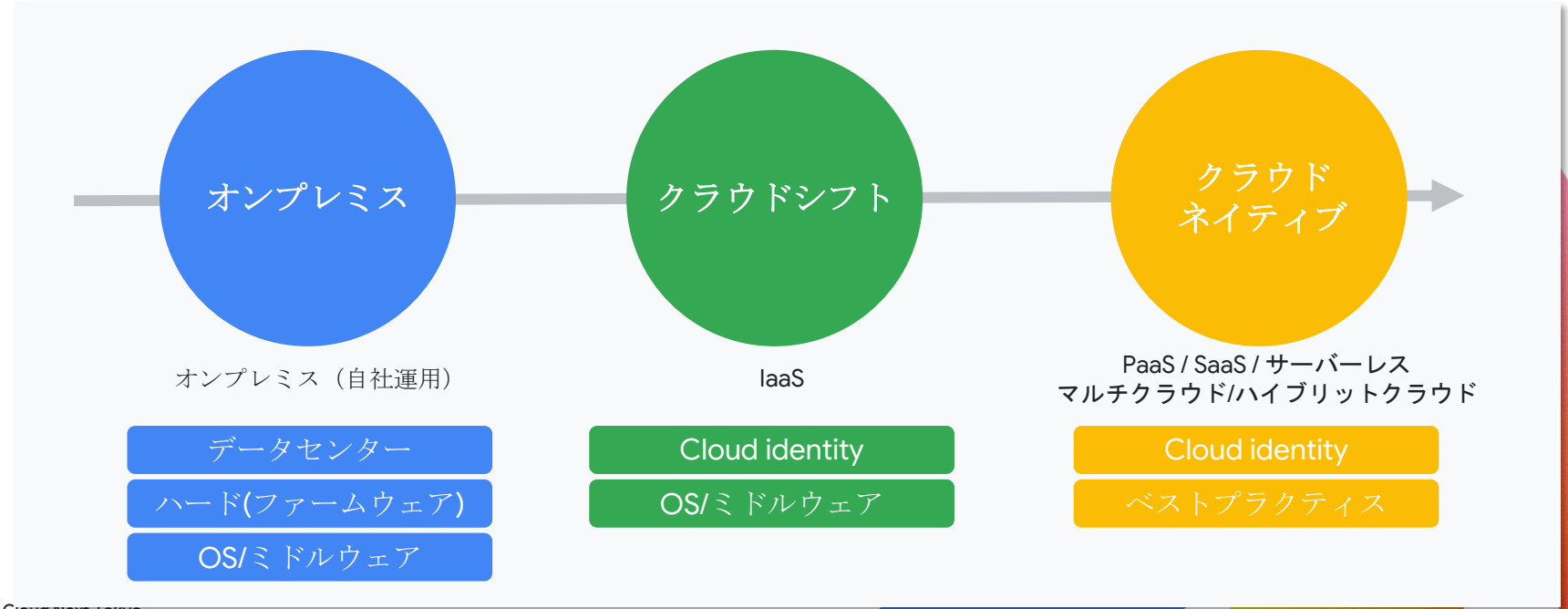
セキュリティマネジメントとは

以下のセキュリティ領域における計画、実行、管理を行うこと



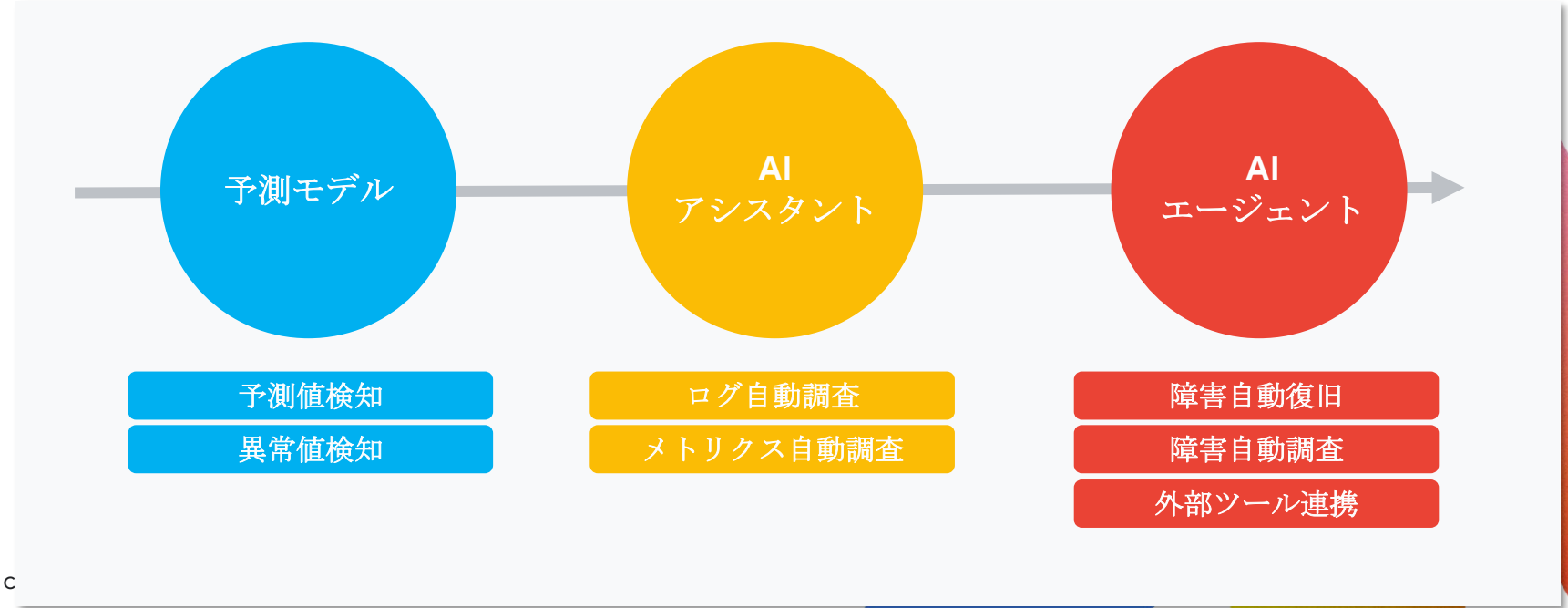
セキュリティマネジメントの変容

オンプレミス主流からクラウド主流へシフト
クラウドプラットフォームそのもののセキュリティ管理が必要となってきている



AIの登場と進化によるマネジメント業務の変革

ビッグデータ活用による予測値・異常値検知から始まり、AIアシスタントへの進化、
自律型AIエージェントの登場 によりオペレーションの一部置き換えによる変革が進む



03. AIと人間の協働モデルとは？

人間とAIの協働モデルの全体像

AIが得意とする領域

高速かつ無制限の処理能力	安定した品質
指示への順応力	エージェント間連携
大量データ解析	異常検知
無数の情報からの推論	24/365労働

人間が得意とする領域

抽象的な問題への理解	感情的文脈の把握
コミュニケーション	ルールの整備
経験に基づく判断	意思決定
柔軟な対応	深い領域知識

効率・素材提供　/　選択肢・情報提供

高い成果

方向性・最終判断　/　指示・フィードバック

AIに任せる領域

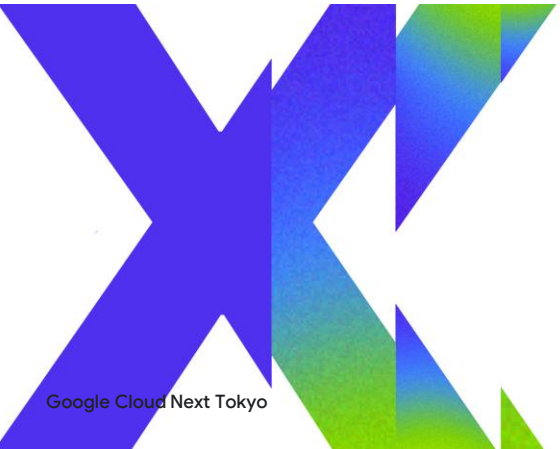
- ■定型的な業務の自動化：定型業務の自動化
- ■制限のない稼働：24時間稼働可能
- ■高い処理能力：大量のデータから分析
- ■膨大なデータの参照：人間の何百倍もの情報のインプットが可能

人間が担うべき領域

- ■重要な意思決定：ビジネス影響を踏まえた意思決定
- ■抽象的な問題の対処：定義の曖昧な問題への対応力
- ■柔軟な対応：想定外の事象への対応力
- ■高度なコミュニケーション：状況や背景に合わせた、柔軟な対人コミュニケーション

AIに任せるべきセキュリティ業務例

ベストプラクティスを参照し、大量なリソースの脆弱性やポリシー違反を診断を行ったり、セキュリティインシデントの迅速な発見に力を発揮します。



脆弱性スキャンの自動化

システムやネットワークの脆弱性を定期的にスキャンし、リスクのある箇所を自動で特定します

インシデント対応の初動支援

インシデント発生時にAIが初期対応の手順を提示し、迅速な対応をサポート

セキュリティポリシーの自動適用と監査

ポリシー違反を検知し、自動で修正提案や適用を行い、コンプライアンスを維持します

人間が担うべきセキュリティ業務例

セキュリティインシデントの影響度から自社のビジネス影響への判断や顧客資産の保護などの重要な判断が求められます。

重要な意思決定

業種やシステムにおいては顧客の資産や個人情報などに影響がある場合があります。発生したセキュリティインシデントから影響度を判断し、その後の対処、対応の判断を行います。

関係者とのコミュニケーション

インシデント対応チームやIT部門、経営層など、関係者への正確かつ迅速な情報共有の他、インシデントが顧客情報や取引先に影響を与えた場合は、適切なタイミングで連絡し、信頼回復に努める必要があります。

複雑な原因分析や調査・再発防止策の検討

AIでは判断が難しい複雑な原因分析やセキュリティポリシーの見直しや教育といった自社に合った再発防止策の検討

協働モデルのメリット

24時間の稼働

- ひとりの人間が24時間365日稼働するのは難しい
- AIは稼働時間の上限がなく、24時間連続稼働が可能
- システム監視やセキュリティ監視など、24時間稼働が求められる業務に最適
- 一次対応はAIが担当し、二次対応以降は人間が対応することで役割分担ができる

分析・解析スピード

- 大量のログやメトリクスデータ、イベントを扱える
- 人が分析・解析するよりも圧倒的に高速で処理
- 事象や問題の特定が迅速に実現可能

単純作業の自動化

- ルールや定義が明確に整備されていること
- ランブックや対応プロセスが整っていること
- AIが自動対応することで対応スピードが向上
- 品質向上と業務効率化が実現可能

協働モデルの課題

情報の不正確性

- AI利用で避けられない課題はハルシネーション問題
- 生成情報が必ずしも正確とは限らない
- 情報の正確性を前提にせず、注意して活用する必要がある

AIが持ち合わせてない暗黙知や独自ノウハウ

- 人間の暗黙知やシステム固有のノウハウが存在する
- AIはこれらの情報を持っていない場合がある
- 不足している情報はAIに学習させる必要がある

重大な報告相談の減少

- AIとのやり取りだけで完結し、対人コミュニケーションが減少
- 重要な情報共有が不足しがちになる
- 自己完結が増え、重大な二次災害のリスクが高まる

04. AI時代に必要な
セキュリティマネジメントスキル

AIリテラシーの必要性

AIの限界と誤検知過検知への理解

- AIセキュリティシステムには誤検知（False Positive）や見逃し（False Negative）の可能性がある
- AIの判断を過信しないことが重要
- 検証を行い、必要に応じて人間が最終判断を下すリテラシーが必要

データの品質とバイアスへの配慮

- AIの精度は学習データの質と量に大きく依存する
- 偏ったデータや古いデータで学習したAIは新しい攻撃や特定環境に弱い
- データの偏りやバイアスを理解することが重要
- 定期的なデータ更新と多様なデータ収集のリテラシーが求められる

AI活用におけるプライバシー・倫理法令遵守の意識

- AIでログや通信データを分析する際は個人情報や機密情報扱うことが多くなる
- プライバシー保護と法令遵守が必須
- AIの自動判断の透明性や説明責任といった論理的な観点を理解することが重要
- 上記を踏まえた適切な運用リテラシーが不可欠

リスク管理スキル(ガバナンス)

AIモデルの定期的な評価・監査体制の構築

- AIモデルのパフォーマンスや判断根拠を定期的に評価・監査する仕組みを設置
- 誤検知やバイアス、精度低下を防止
- 現状の脅威環境や業務要件に合っているか継続的にチェック
- 必要に応じてモデルの再学習や改善を実施しリスク最小化

データガバナンスとアクセス管理の徹底

- AIが扱うデータの収集・保存・利用・廃棄のルールを明確化
- アクセス権限を厳格に管理
- 個人情報や機密情報の漏洩・不正利用を防止
- 法令や社内ポリシーに準拠したAI運用を実現

AI活用に関する倫理・法令遵守のガイドライン策定と教育

- AI利用の倫理的・法的ガイドラインを策定
- 関係者への教育・啓発を定期的に実施
- 差別や不透明な判断、法令違反のリスクを未然に防止
- 説明責任と透明性を確保

スキル習得のためのステップ

4 継続的な改善

最新のモデルや新しい概念の登場など目まぐるしく進化するAIプロダクトのなかで1~3を継続的に行いガイドラインや運用プロセス、人材の教育を継続していく必要がある

3 定期的なモデルの監査、性能アップデートの体制

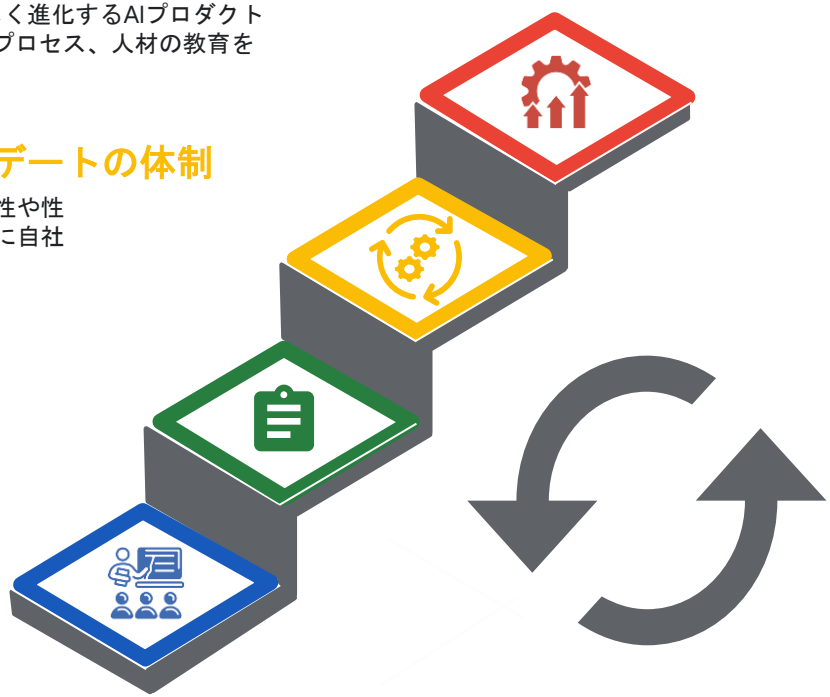
LLMのモデルは日進月歩で進化しており、モデルの正確性や性能は日々アップデートされている、それらを監査し適切に自社に取り込むことができる体制を構築する

2 AI利用のガイドライン策定

野良やパブリックなLLMの利用やデータ保持のルール、倫理的や問題や法務的なリスクを踏まえた利用のルールをガイドライン化し整備を行う

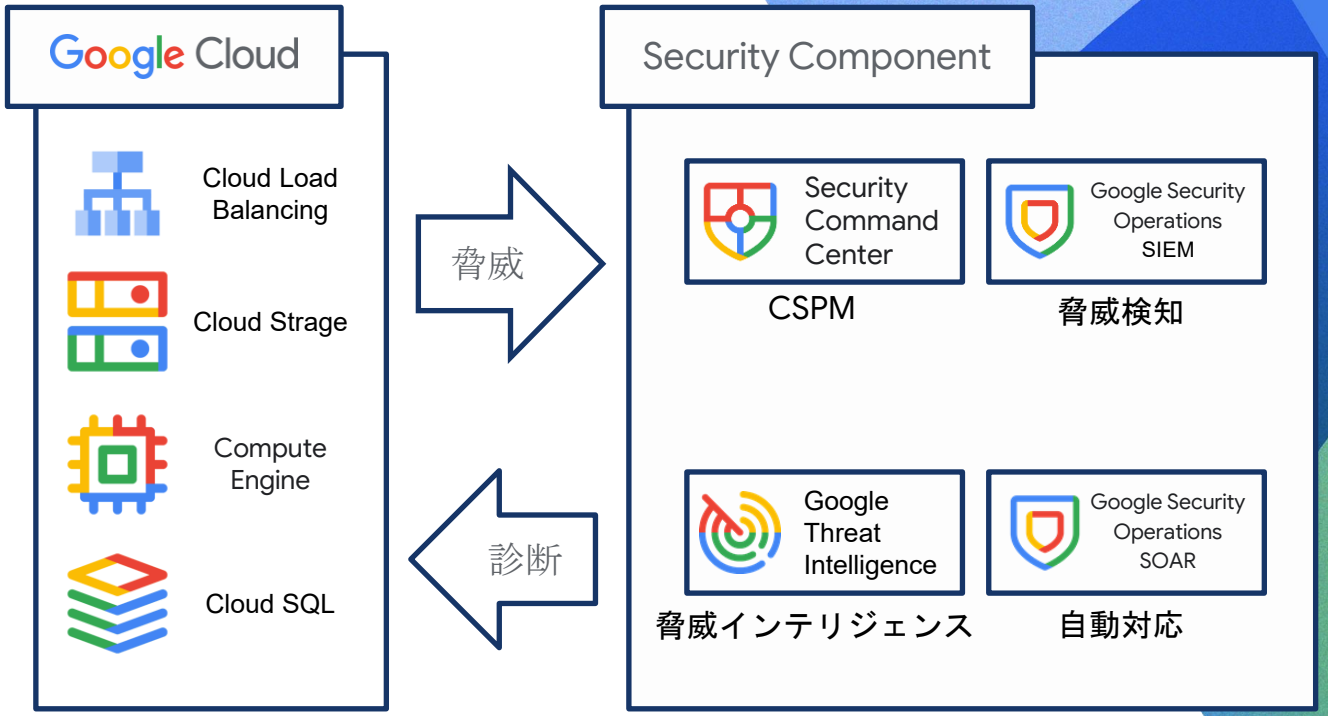
1 AI人材の育成

AIの有効な活用方法と、バッドノウハウや正しく情報を取り扱うためのリテラシー教育を行う



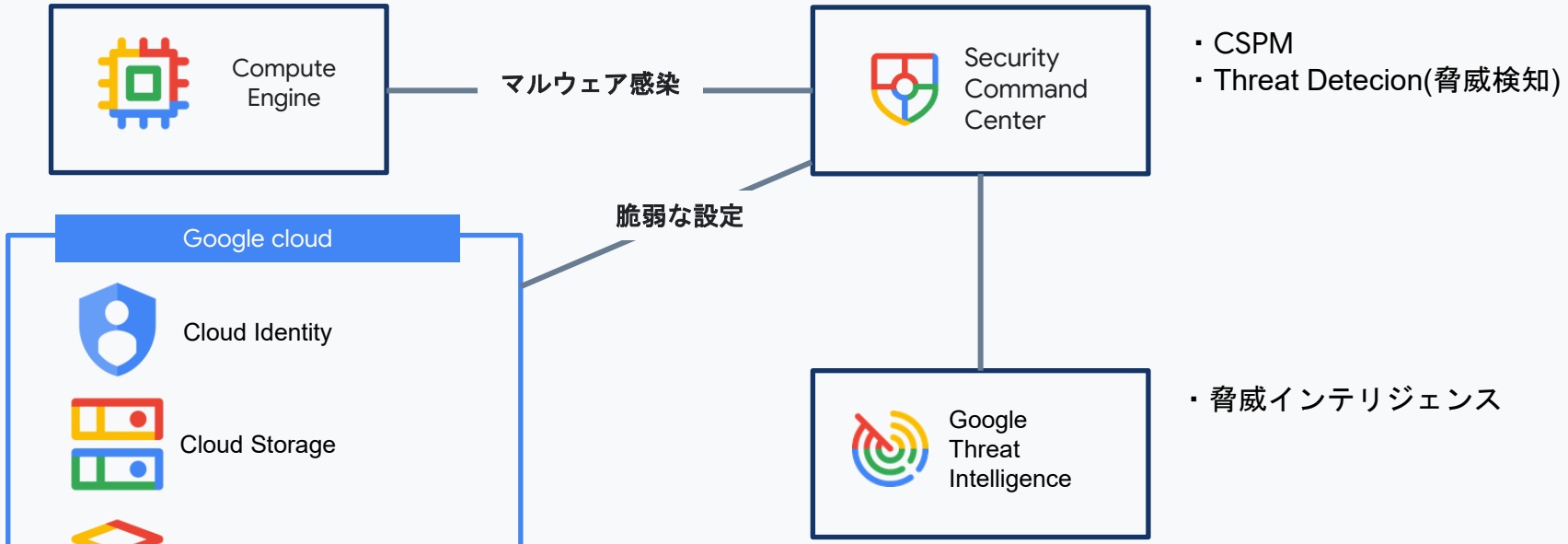
05. Google Cloudで実現するには

Google Cloudのセキュリティ管理サービス

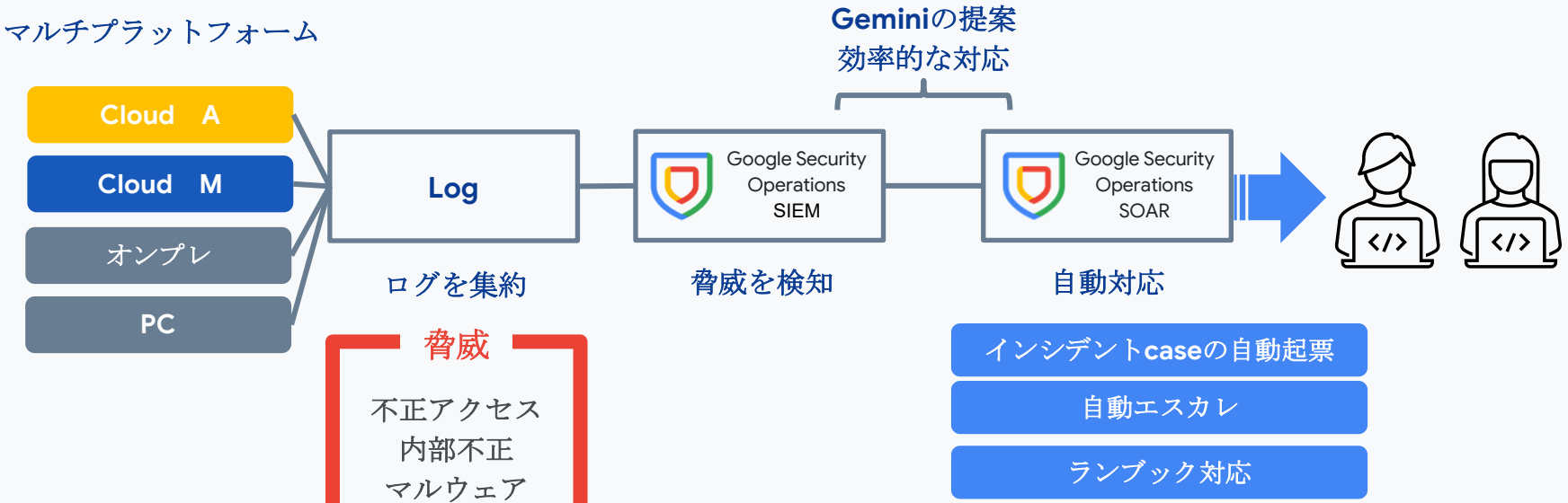


Google Cloudの脆弱性、脅威検知例

GCEがマルウェアに感染した場合



マルチプラットフォームにおける脅威検知の統合例



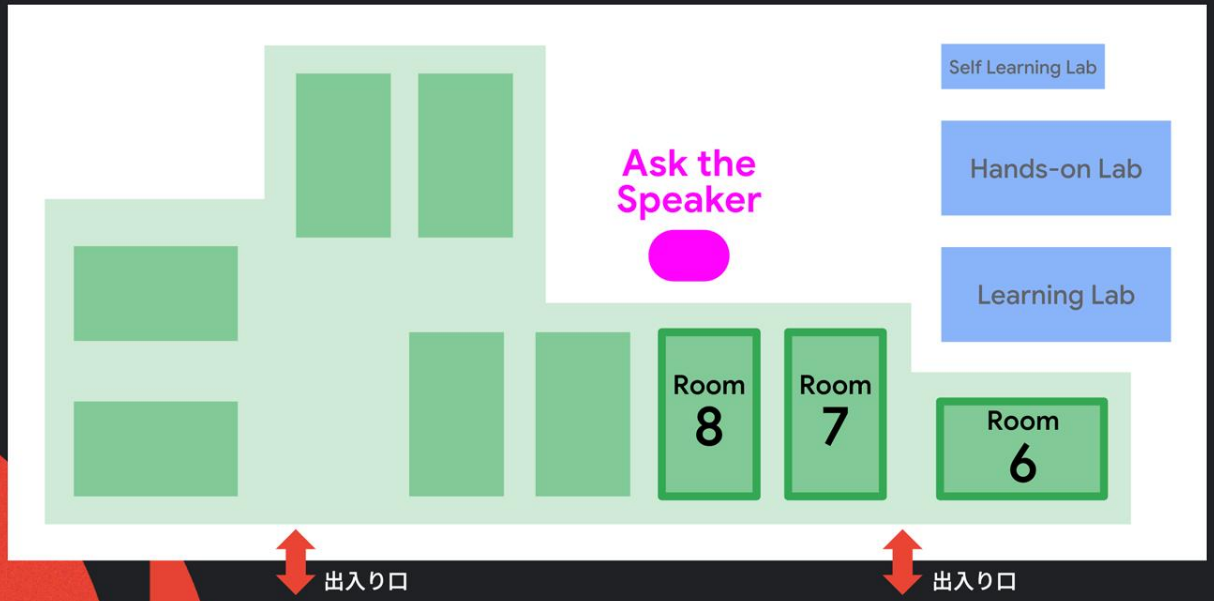
06.まとめ

AIとの協働する上で必要な
セキュリティマネジメントのポイントまとめ

- AI特有のハルシネーション/リスクの理解
- 最新のモデルや正確性の評価とアップデート
- AIを安全に使うためのガイドラインの策定
- 継続的な教育
- 重大な意思決定をAI任せにしない

Ask the Speaker にぜひお越しください（会場は 4F）

セッションに関する質問にスピーカーが直接お答えします！



Thank you

ご清聴ありがとうございました。