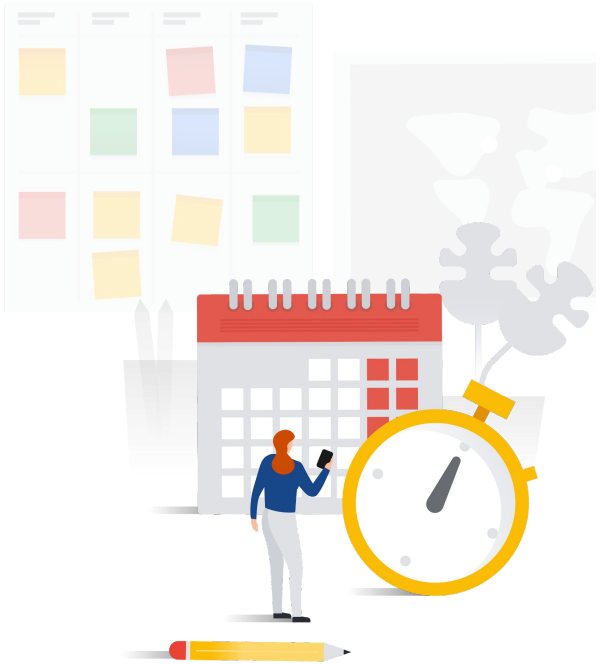
SCSK 株式会社 御中

Google Cloud のセキュリティ製品とゼロ トラスト モデルの実現

2021 年 9 月 29 日
グーグル・クラウド・ジャパン合同会社

アジェンダ



1. Google Cloud のインフラ セキュリティ
2. Google Cloud のセキュリティ ソリューション
3. BeyondCorp Enterprise のご紹介
4. Google Cloud アップデート

Self Introduction

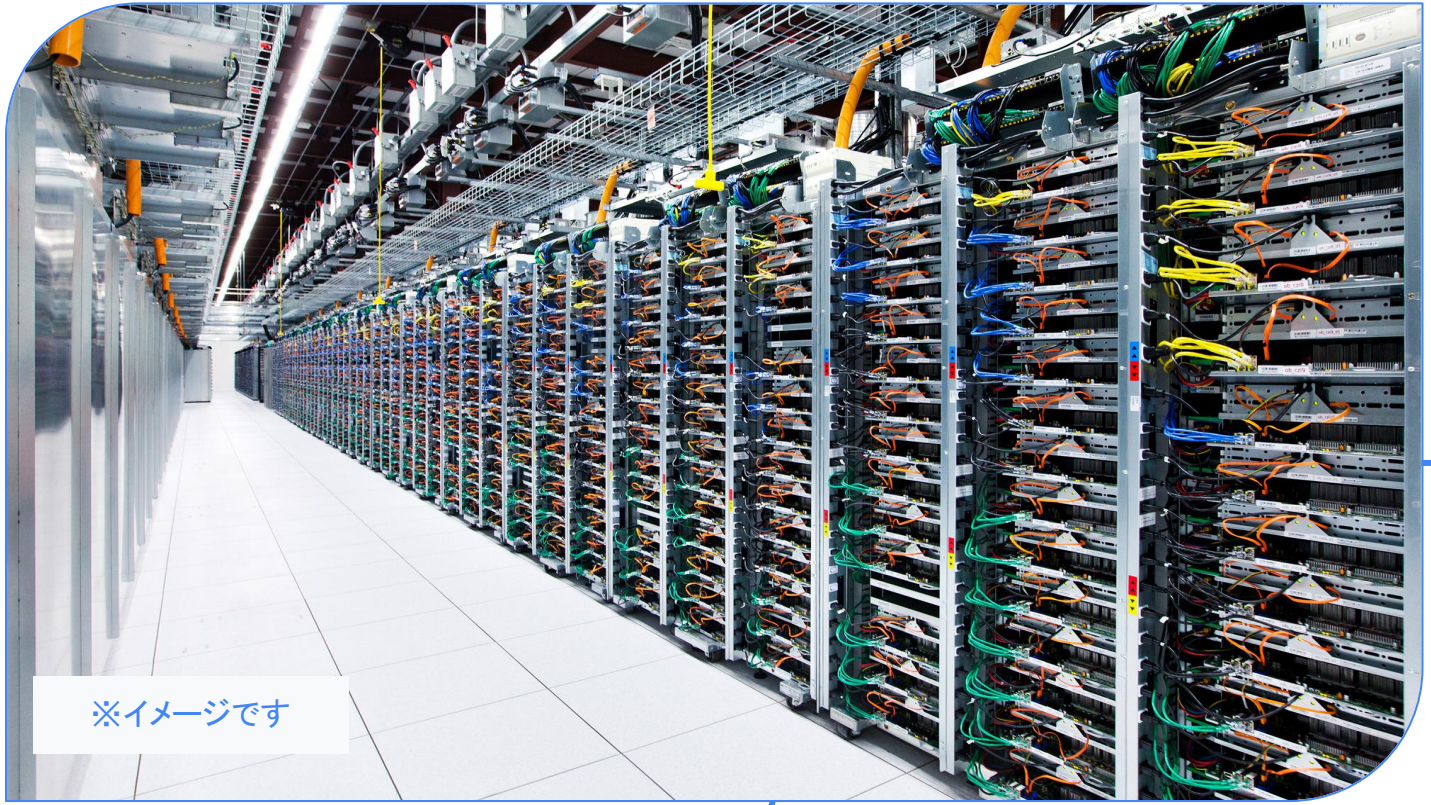
中谷　祐輔 (なかや　ゆうすけ)

グーグル・クラウド・ジャパン合同会社
パートナーエンジニア

1

Google Cloud の インフラ セキュリティ

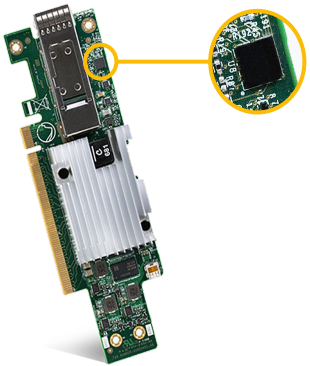
Security First, Everything Follows.



※イメージです

セキュアな基礎を用いた構成

Titan



専用の
チップ

専用の
サーバー

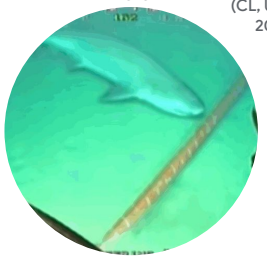
専用の
ストレージ

専用の
ネットワーク

専用の
データ センター

周辺の HW、ブートは電子証明書で確認
悪意ファームウェア（UEFI、ドライバーなど）があれば検知し、起動不可能
Google の専用 TPM チップ

「ベンダーを間にはさむ」リスクを低減



Faster (US, JP, TW) 2016
Unity (US, JP) 2010
PLCN (US, TW) 2020
Curie (CL, US) 2019
Monet (US, BR) 2017
Junior (Rio, Santos) 2018
Tannat (BR, UY, AR) 2018
Equiano (PT, NG, ZA) 2021
Dunant (US, FR) 2020
Grace Hopper (US, UK, ES) 2022
Havfrue (US, IE, DK) 2019
SJC (JP, HK, SG) 2013
JGA-S (GU, AU) 2019
Indigo (SG, ID, AU) 2019
Oregon
Salt Lake City
Las Vegas
Los Angeles
Iowa*
Toronto
Montréal
N. Virginia
S. Carolina
São Paulo
Santiago
Finland
Netherlands
Warsaw
London
Belgium
Frankfurt
Zurich
Paris
Turin
Milan
Madrid
Doha
Delhi
Mumbai
Seoul
Tokyo
Osaka
Hong Kong
Taiwan
Singapore
Jakarta
Sydney
Melbourne

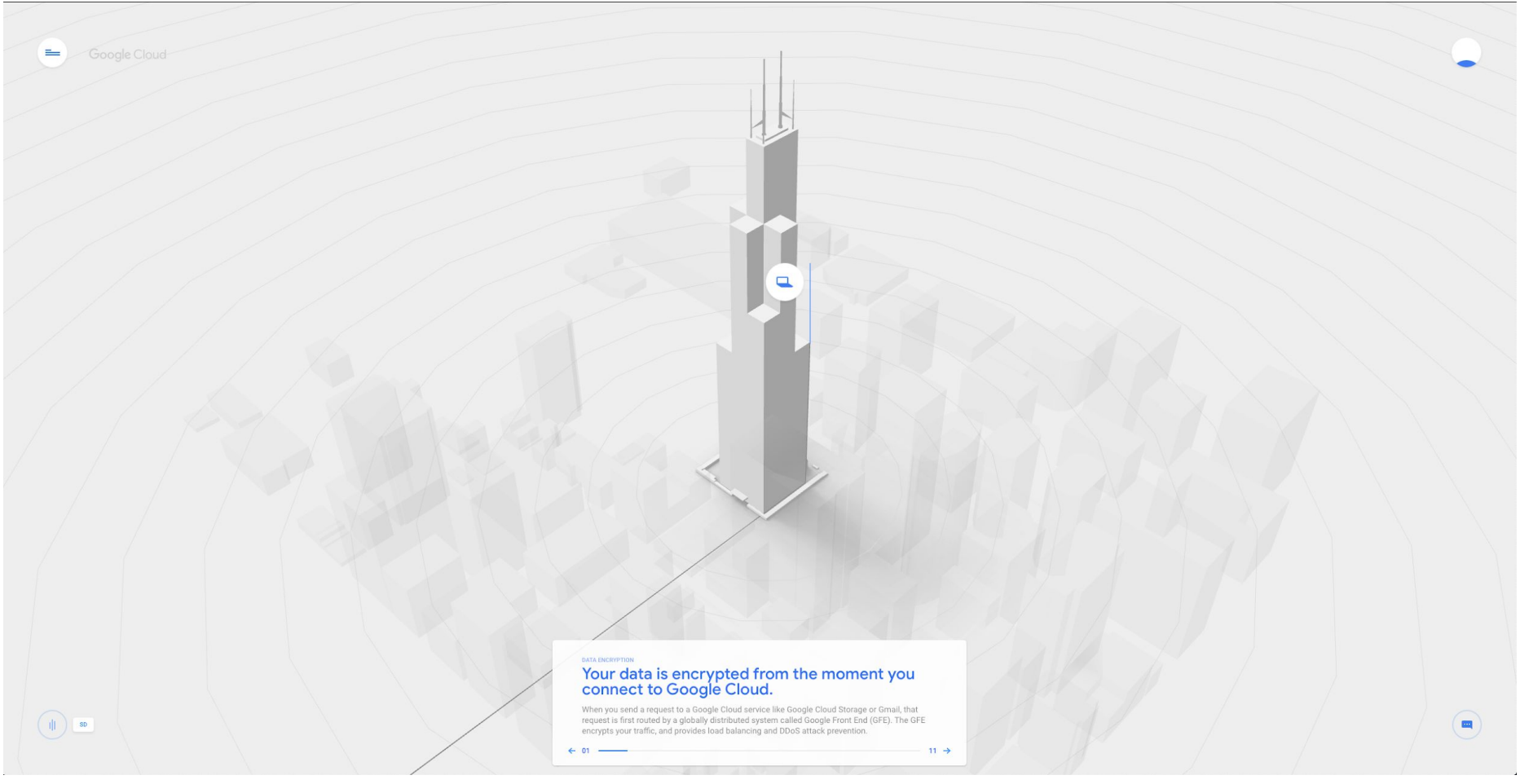
Google Cloud

エッジPOP　通信ケーブル　現行リージョン　今後のリージョン

全世界に展開するネットワークとリージョン

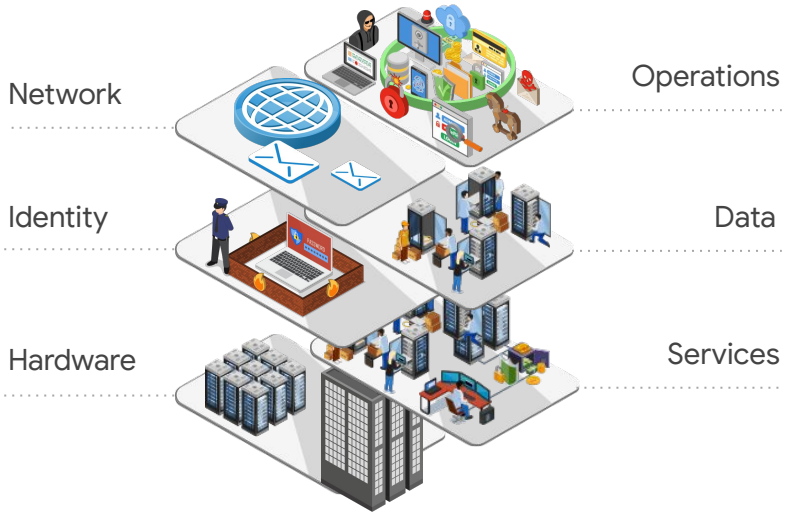
*Exception: region has 4 zones.

Google Cloud data encryption journey



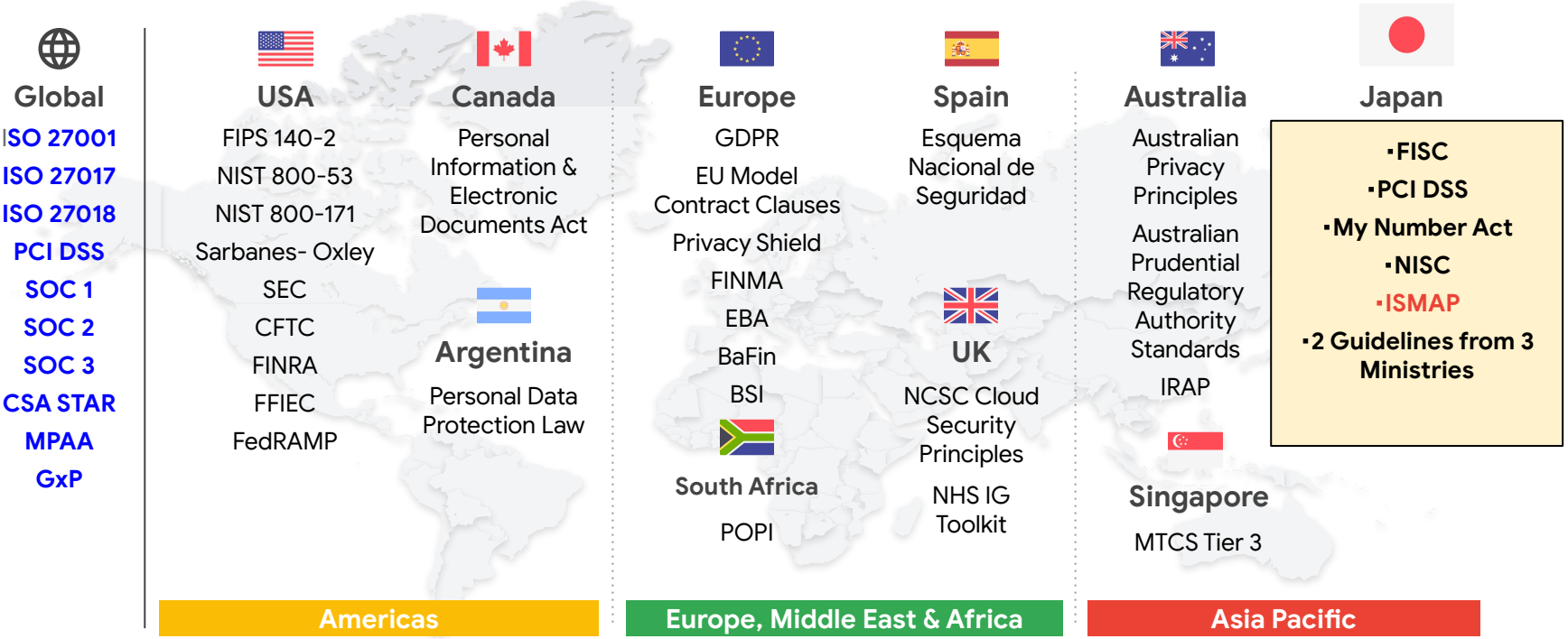
多層防御によるセキュアなシステム

Layered Defense in Depth（多層防御）



レイヤ	主なセキュリティ対策の例
オペレーション	侵入検知システム、インサイダーリスク低減技術、 従業員によるU2F 使用、ソフトウェア開発プラクティス
ネットワーク	Google Front End 、DoS 攻撃防御の組み込み
データ	保存データの暗号化
アイデンティティ	U2F サポートを含む一元的な識別サービス
サービス	サービス間通信の暗号化
ハードウェア	ハードウェアの設計と供給、ブートスタックの セキュリティ、構内セキュリティ

各種コンプライアンスへの対応



コンプライアンス リソース センター https://cloud.google.com/security/compliance?hl=ja

政府情報システムのためのセキュリティ評価制度（ISMAP）対応

- 政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウド サービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度

- 2021 年 3 月 12 日に公表された ISMAP クラウドサービスリストに、Apigee、Google Cloud Platform、Google Workspace が登録されました

登録番号	登録日 / 更新期限	サービス名	事業者名	詳細情報 ※補足
C21-0001-2	2021/03/12 / 2022/01/31	OpenCanvas(IaaS)	株式会社エヌ・ティ・ティ・データ（法人番号9010601021385）	詳細
C21-0002-2	2021/03/12 / 2022/02/28	FUJITSU Hybrid IT Service FJcloud	富士通株式会社（法人番号1020001071491）	詳細
C21-0003-2	2021/03/12 / 2022/04/09	Apigee Edge	Google LLC（法人番号3700150072195）	詳細
C21-0004-2	2021/03/12 / 2022/04/09	Google Cloud Platform	Google LLC（法人番号3700150072195）	詳細
C21-0005-2	2021/03/12 / 2022/04/09	Google Workspace	Google LLC（法人番号3700150072195）	詳細

https://www.ipa.go.jp/security/ismap/cslist.html

2

Google Cloud の セキュリティ ソリューション

Google Cloud のセキュリティ関連サービス

ガバナンス、リスク管理 コンプライアンス

- Third-party audits
- International Certifications
- Access Transparency
- Access Approvals
- Key Access Justifications
- Google Vault for G Suite
- Cloud Storage Retention Policy
- Cloud Audit Logging

IDとアクセス管理

Cloud Identity　IAM　IAP　Conditions　Recommender　Troubleshooter　Validator

アプリケーションセキュリティ

ReCaptcha　Web Risk　BeyondCorp　Web Security Scanner　Binary Authorization

データセキュリティ

Encryption by Default　CMK　CSK　HSM　External Key Manager　DLP API　GWS ACLs

インフラセキュリティ

Titan　Shielded VM・GKE　Binary Auth　Confidential Computing　Container Threat Detection

ネットワークセキュリティ

Shared VPC　VPC Firewalls　ALTS　Cloud Armor　VPC Service Controls　Packet Capture

端末セキュリティ

Chrome OS　Chrome Browser　SafeBrowsing　Device Management　ChromeBook　Pixel

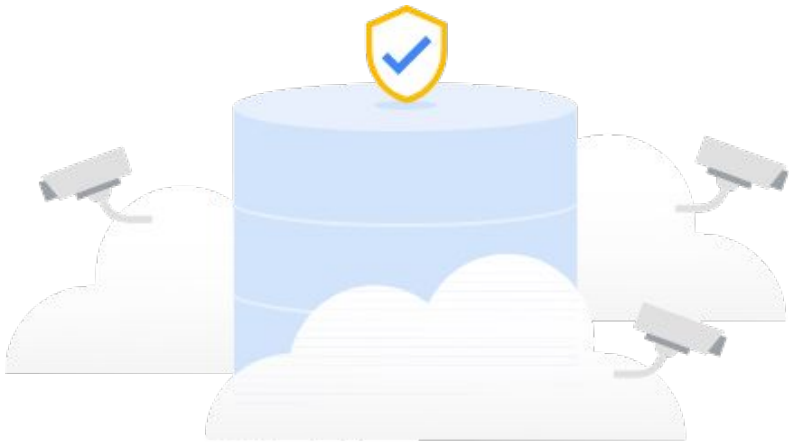
セキュリティの監視と業務

- Cloud Operations
- Security Command Center
- Incident Response Management
- Security Health Analytics
- Event Threat Detection
- Cloud Anomaly Detection
- VirusTotal
- Chronicle

内部からのデータ流出を防止

VPC Service Controls

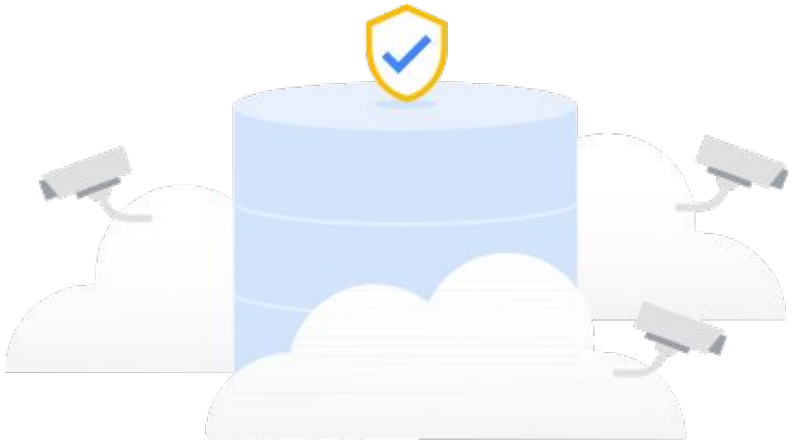
- **VPC Service Controls** を使うと、仮想的な「**セキュリティ境界**」を構築できる
- 内部から外部へのデータ流出を遮断できる
- オンプレからクラウドへの、安全なハイブリッド接続が可能となる



内部からのデータ流出を防止

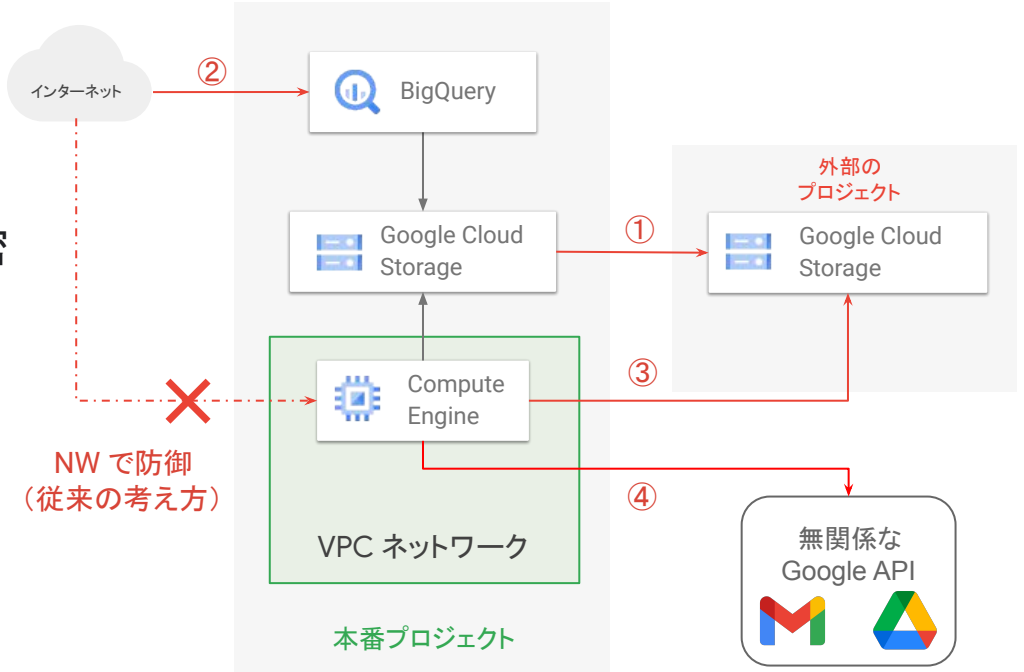
VPC Service Controls

- **VPC Service Controls** を使うと、仮想的な「**セキュリティ境界**」を構築できる
- 内部から外部へのデータ流出を遮断できる
- オンプレからクラウドへの、安全なハイブリッド接続が可能となる



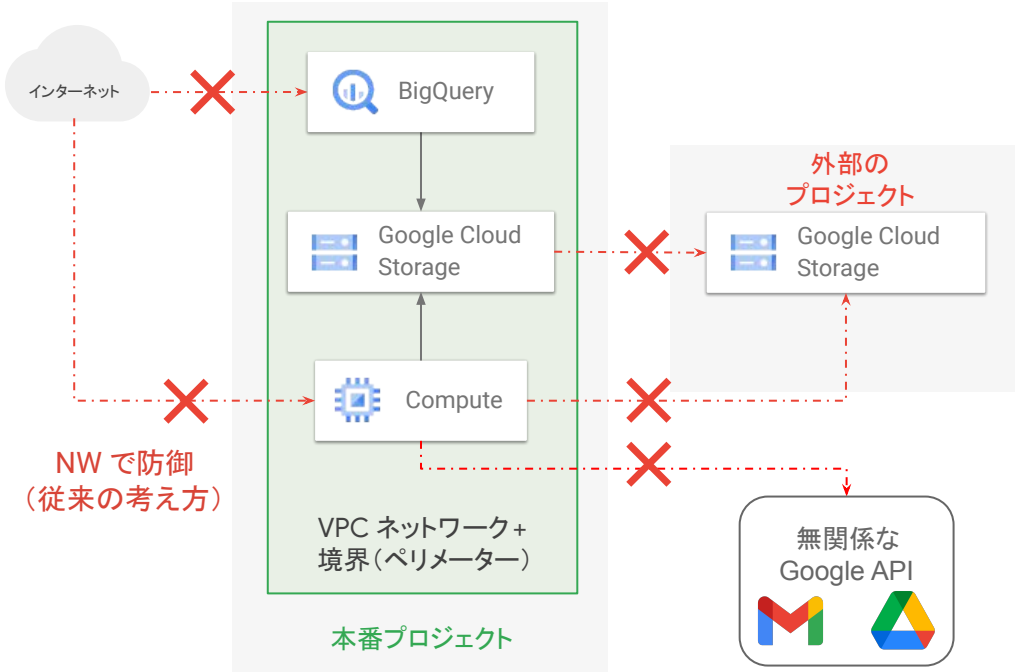
従来の考え方では守り切れないケースの例

1. IAM ポリシーの設定誤りによる想定外の共有
2. 盗まれた ID / サービス アカウントとキー を使用してインターネットから機密データへアクセス
3. 内部犯や、危険なコードで不正なクラウド リソースへのデータコピー
4. 他の Google API 群へデータ転送



VPC Service Controls による防御

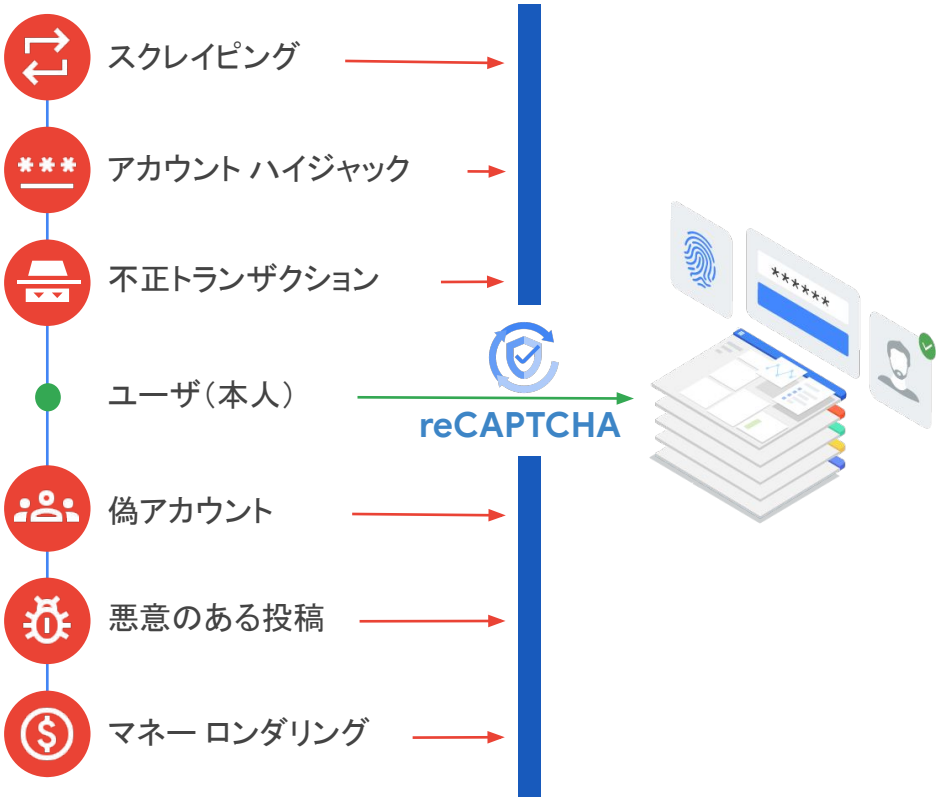
- 境界 / ペリメーターという
  セキュリティの境界を
  プロジェクトの外側に新たに持つ
- 境界をまたぐデータの移動をIAM
  とは別にチェック
- 境界をまたげる条件をアクセス
  レベル で定義
- プロジェクト オーナーにも変更不可



reCAPTCHA Enterprise

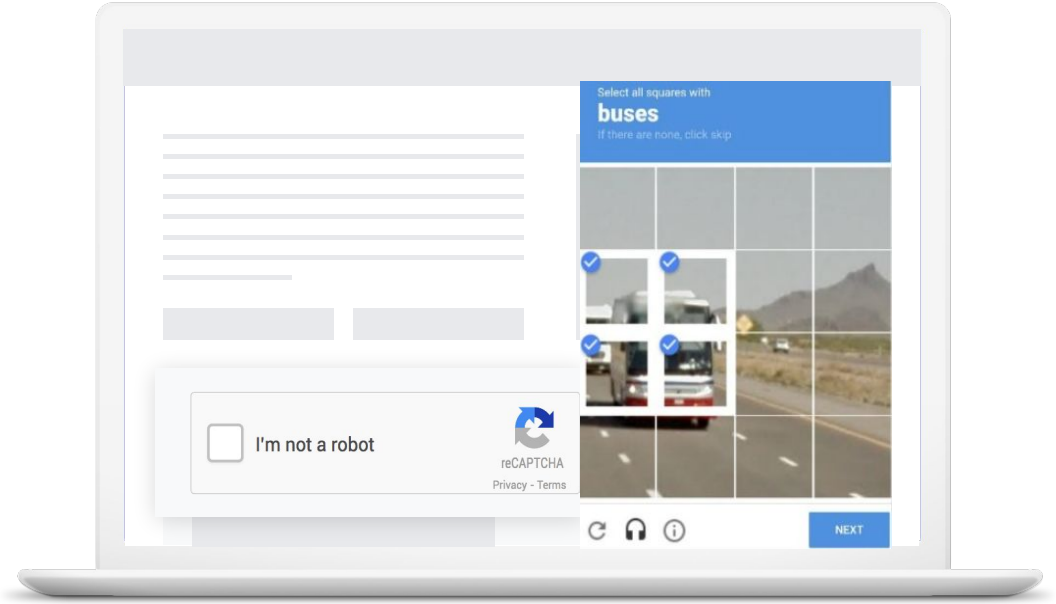
ボット検出と防止システム

ボット、詐欺、自動攻撃からビジネスを守ります



reCAPTCHA の進化(1)

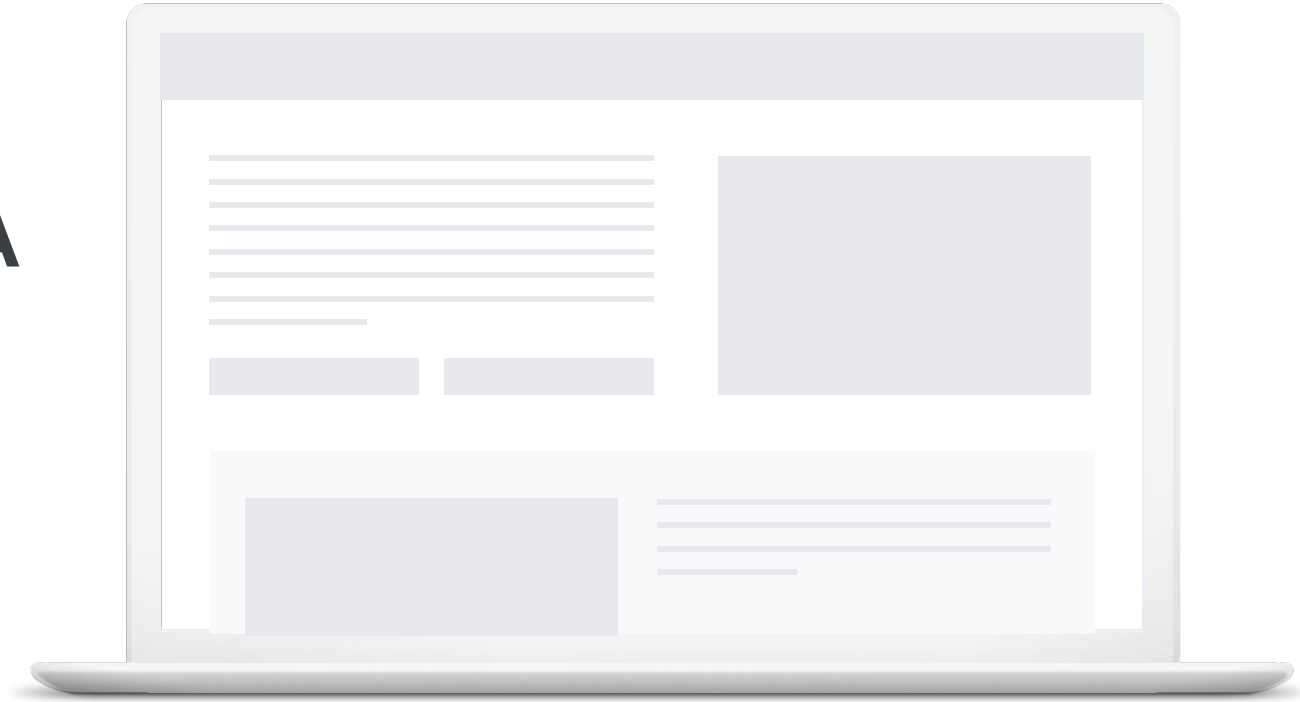
バージョン 1



バージョン 2

reCAPTCHA の進化

バージョン 3



reCAPTCHA Enterprise

- サービスレベル契約
- Google Cloud 利用規約とサポート
- 粒度の細かいリスクスコア
- Reason コード
- 機械学習済モデルとカスタマイズ
- モバイル SDKs
- 多要素認証(Account Verification - Preview)
- パスワード漏洩確認(Password Checker Preview)

3

BeyondCorp Enterprise のご紹介

一般的なネットワーク
セキュリティ環境

しかしこのアプローチには問題が・・・

境界の中は安全？

ゼロトラスト

境界の中も危険であることを前提に

150 万

SingHealth (2018 年 7 月 20 日)
シンガポール最大の医療グループは、同国首相を含む **150 万人の患者の個人情報**が不正にアクセスされコピーされたと発表

5000 万

Facebook (2018 年 9 月 28 日)
約 5000 万件のアカウント情報が流出したと公表
（後に 3000 万件の Facebookアカウントの情報に下方修正）

5 億

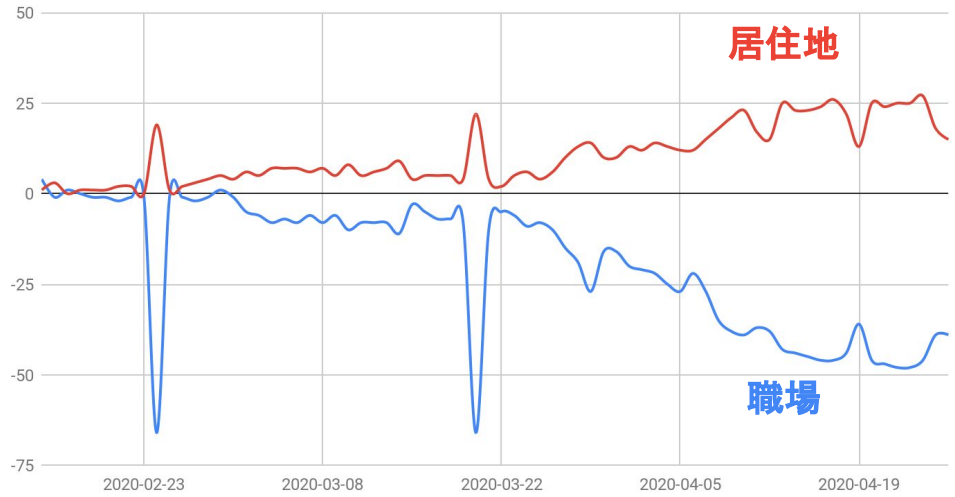
Marriott (2018 年 11 月30 日)
大手ホテルチェーンは、**5 億人のゲストに関する個人情報が漏えい**したと公表
（後に約 3 億 8,300 万件に修正）

出典：IPA「情報セキュリティ白書2019」, https://www.ipa.go.jp/files/000079041.pdf
サイバーセキュリティー.com（日本での被害事例集）, https://cybersecurity-jp.com/leakage-of-personal-information

COVID-19: 在宅勤務が当たり前に

リモートワークが
必要に迫られて
広く受け入れられるようになっ
てきている

東京での人の動きの変化



Source: COVID-19 Community Mobility Report, https://www.google.com/covid19/mobility/

ネットワークの境界の消滅

社内システムへのアクセス元は、もはやオフィス内／従業員の自宅といった環境に限定されない

働く環境が変わりつつある

モバイル デバイスに対するユーザーの期待が変化している

生産性を支える主要なアプリケーションやデータはクラウド上に存在する

BeyondCorp Enterprise

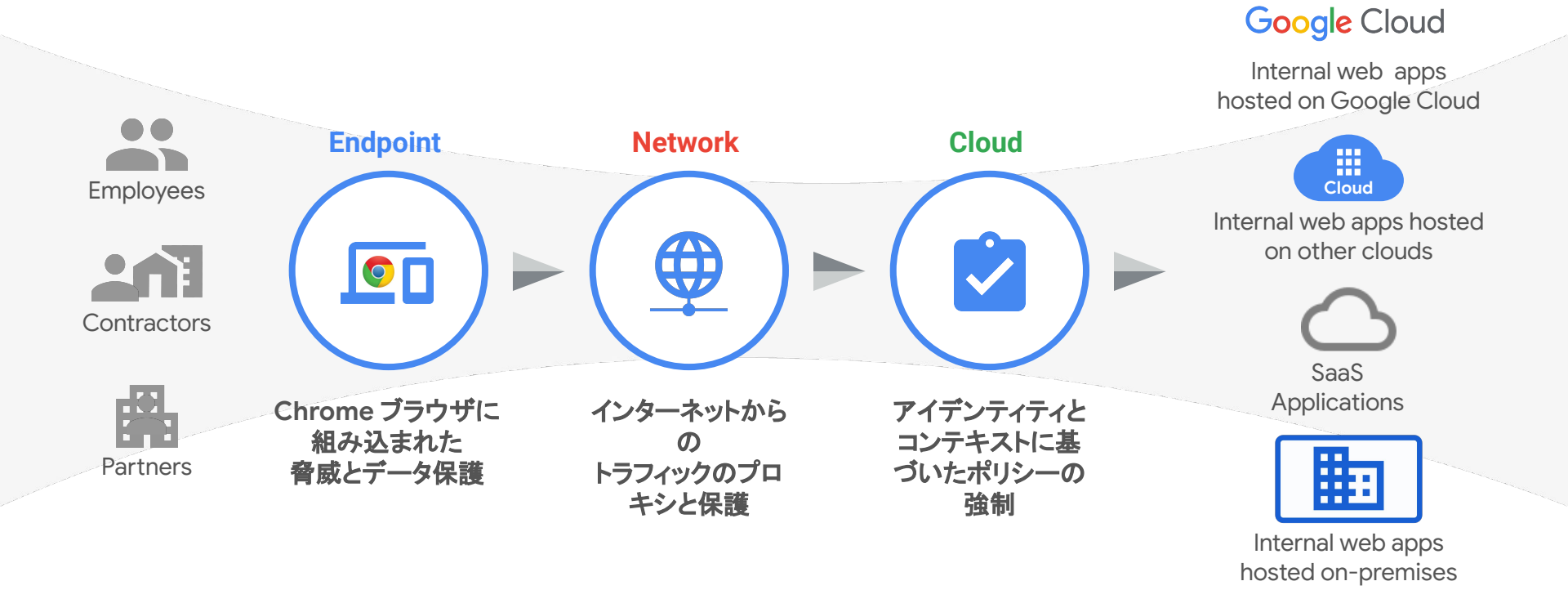
企業向け ゼロトラスト
セキュリティ サービス

BeyondCorp Enterprise

Google の 2011 年から始まった BeyondCorp のミッション

すべての Google 従業員が
VPN を使わずに信頼できないネットワークから
問題なく業務できるようにする

BeyondCorp Enterprise



BeyondCorp:アーキテクチャ

EndPoint Verification: 端末状況の確認
Google MDM：スマホ端末の管理と状況確認

EndPoint Verification

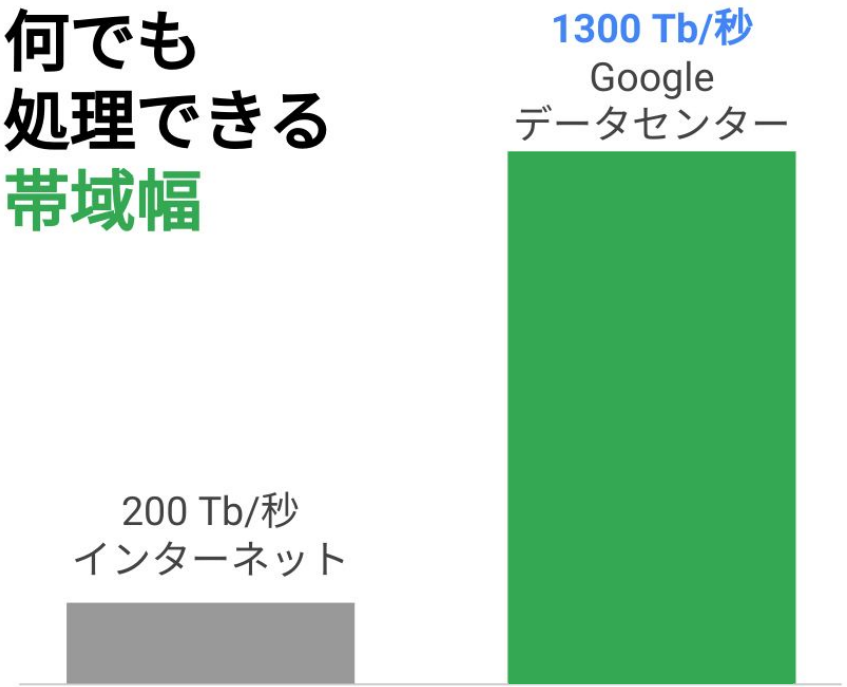
- 社給・私用 PC
- OS ポリシ (バーション最低限)
- HDD 暗号化
- スクリーン ロック
- 連携セキュリティ ソフト条件
- OSX, Win, Chrome, Linux サポート
- Chrome ブラウザ

Google MDM

- 社給・私用スマホ
- MDM ポリシ
- Google Workspace アクセス
- 電子証明書
- 連携 MDM 条件
- Chrome と Android サポート
- Admin コンソールで管理

BeyondCorp:ビジネスの可用性

自社のフロントエンドが Google Cloud であればセキュリティはどう変わる



“最大の攻撃を吸収するには、50万のYouTubeビデオを同時に視聴するために必要な帯域幅が必要です...”

Dr. Damian Menscher
DDOS防衛チーム, Google

BeyondCorp:アーキテクチャ

Cloud Identity: Google 機械学習でアカウント保護

Google は、毎日、正しいパスワードを使った 100 万アカウントの不正アクセスを検出し、止めている。

- 多要素認証
- プッシュ通知
- ワンタイム パスワード（OTP）
- パスワード アラート
- FIDO 基準セキュリティキー

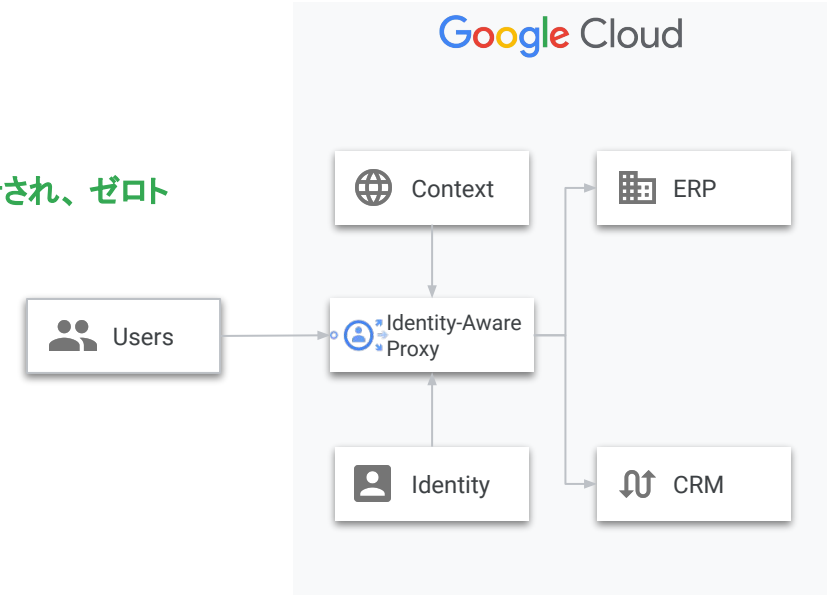
Cloud Identity Aware Proxy (Cloud IAP)

Google POP に存在するグローバル リソース

Google の BeyondCorp セキュリティ モデルを元に設計され、ゼロトラストネットワークを実現

リバース プロキシをアプリケーションの前段に配置

- コンテキストベースのアクセスポリシーを適用
- ユーザー・アプリ間の暗号化を強制
- DDoS からの保護と TLS の終端
- SSH や RDP 等のプロトコルにも対応

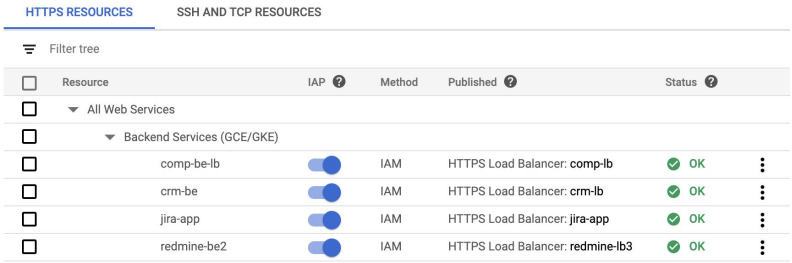


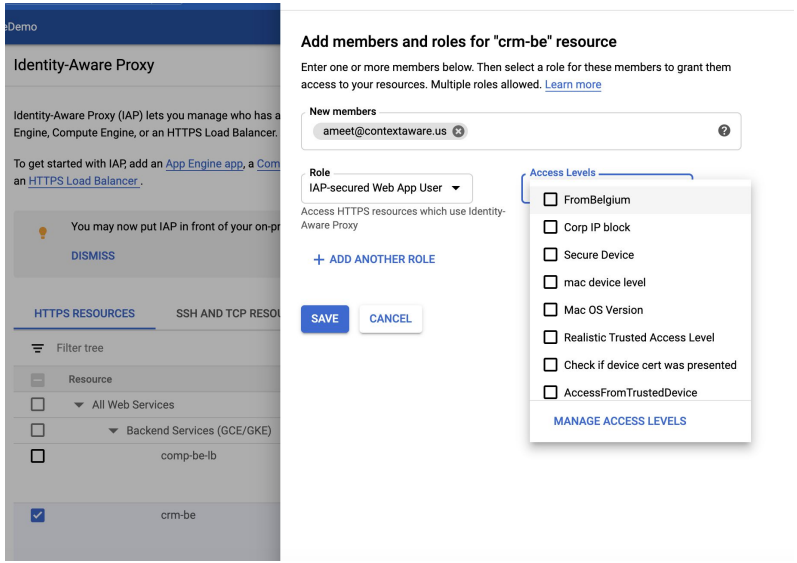
cloud.google.com/iap
cloud.google.com/beyondcorp

BeyondCorp:アーキテクチャ

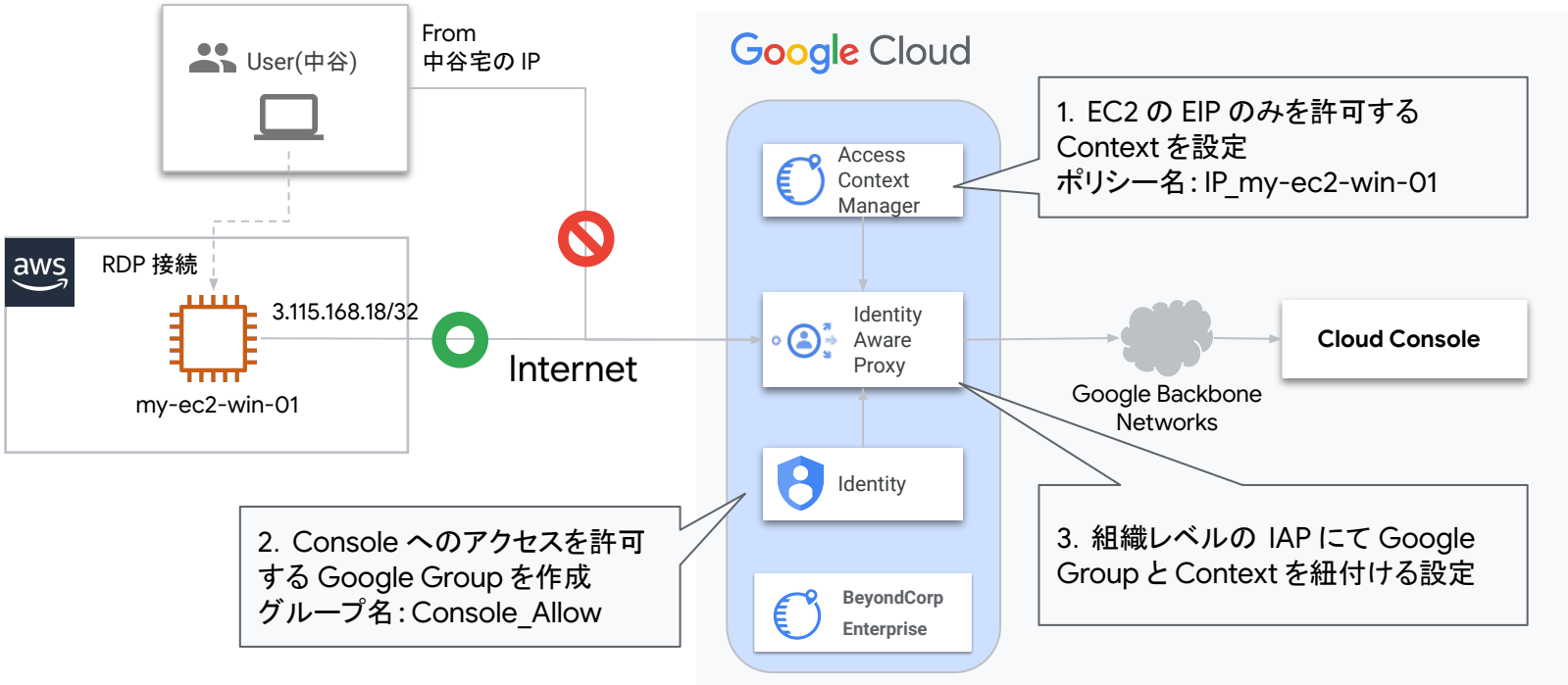
アプリのアクセス設定が簡単に

1. IAP で Backend を設定
2. Access Context Manager でアクセスレベルを設定
3. IAP でアプリを選択し、メンバーにアサインし、
   アクセスレベルをアサイン

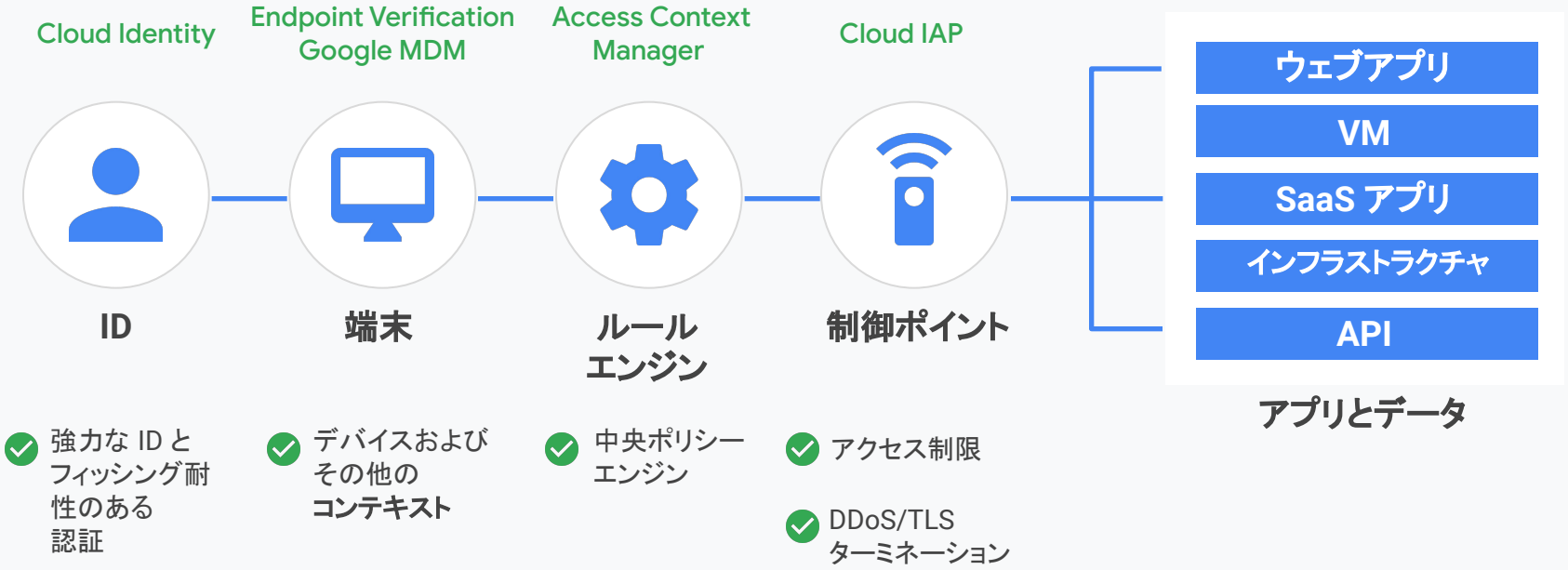




Demo
- Cloud Console を BeyondCorp で保護する -

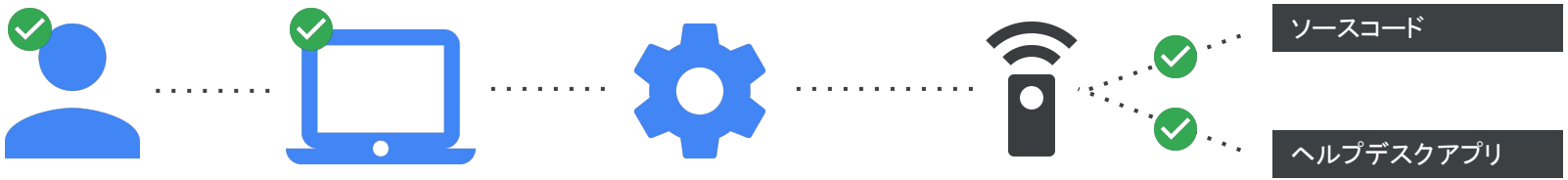


BeyondCorp のアーキテクチャー



Example scenario

国内のコーヒーショップから従業員がアクセス



alice@acme.com
開発者

Alice の PC
社給 PC
S/N: j76Ky
許可された地域からのアクセス

ルールエンジン:
開発者は**社給 PC**で、

許可された地域からのみ**ソースコード**にアクセスできる

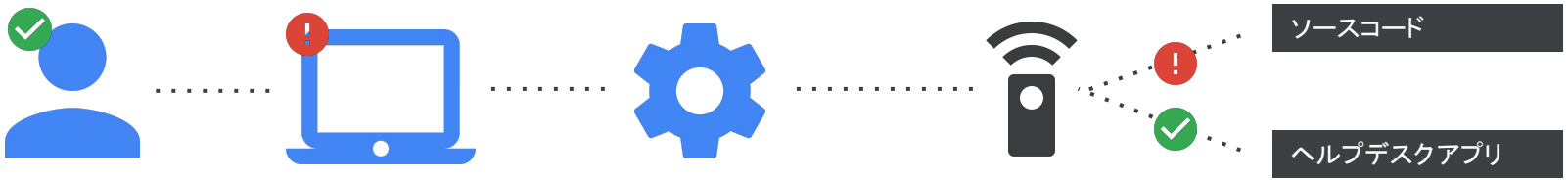
どこからでもヘルプデスク アプリにアクセスできる

制御ポイント
ID とコンテキストを検証

ソースコードと**ヘルプデスク アプリ**の両方にアクセスを許可

Example scenario

制限対象国に出張中の従業員



alice@acme.com
開発者

Alice の PC
社給 PC
S/N: j76Ky
IP: 制限対象国

ルールエンジン:
開発者は**社給 PC**で、

許可された地域からの
み**ソースコード**にアクセ
スできる

**どこからでもヘルプデス
ク アプリ**にアクセスでき
る

制御ポイント
ID とコンテキストを
検証

ヘルプデスク アプリ
のみにアクセスを許
可

NTT ドコモ様
- マイトレードにおける BeyondCorp 導入事例（1）-

https://cloudonair.withgoogle.com/events/google-cloud-day-digital-21/watch?talk=d3-sec-01

NTT ドコモ様
- マイトレードにおける BeyondCorp 導入事例(2)-

BeyondCorp 導入の経緯

- コロナ禍以降ほぼ週ゼロ出社。チーム全員が在宅ワーク🏠
  - セキュアにリモートアクセスできることが必須。ユーザ毎に細かい制御を行いたい
  - ➡ **ゼロトラストな考え方**が合っている
- 検討・PoC 検証から導入まで私ひとり🤷
  - **システム構築コストを小さく**したい
  - ➡ サービス側のシステム同様なるべくマネージドに構築したい
- 以上より、BeyondCorp の導入へ

良かったこと

- 構築コスト観点
  - **Google ですべてが完結**したのが良かった（外部セキュリティソフトが不要）
  - 組織に登録した端末は**ゼロタッチ キッティング可能**。台数が増えても管理がスケール
  - PoC 検証から自分しかメンバーがいない中、**トータル稼働 1-2 ヶ月で実践投入**いけた
- ゼロトラストの「アキレス腱」なログ集約がとってもカンタン
  - BigQuery 等に**簡単に**集約できエンプラ企業の**月次監査対応がはかどる**

Google Cloud

https://cloudonair.withgoogle.com/events/google-cloud-day-digital-21/watch?talk=d3-sec-01

4

Google Cloud アップデート

FFG / ZDF 様における Google Kubernetes Engine（GKE）+ Spanner の活用

（ふくおかフィナンシャル グループ / ゼロバンク デザイン ファクトリー）

- 2021 年 5 月に提供を開始したスマートフォン専業銀行:「みんなの銀行」
- 顧客ニーズにあわせてサービスを迅速に進化させていくために、マイクロ サービスで構築
- マイクロ サービス化に最適で、運用負担を軽減するために GKE を採用。また、急なトラフィック増にも対応し、高い可用性を提供するSpanner を 勘定系システムに採用 (東阪両現用)
- 今後は Apigee X による BaaS 展開強化や AI 活用などを予定

2021 年 9 月 10 日 Google Cloud Japan 公式ブログより引用
https://cloud.google.com/blog/ja/topics/customers/minna-no-ginko-spanner

【利用プロダクト抜粋】

GKE

BigQuery

Cloud Spanner

ビッグデータ分析基盤 IDAP における Google Cloud 導入事例

（NTT ドコモ様）

- 社内データサイエンティスト向けの統合DMP として提供している IDAP（Integrated Data Analytics Platform）に BigQuery を採用
- 採用経緯: データ量の増加に対する対策+ BigQuery の同時並列実行における高いパフォーマンスと、BigQuery GIS や BigQuery ML といった豊富な機能から採用を決定
- BigQuery（Google Cloud）と Redshift（AWS）を組み合わせた構成。現在はクエリの 6〜7 割を BigQuery で処理している。合計 5+ ペタバイト（1 日あたりの処理量 50+テラバイト）
- Google Cloud サービスへのパブリック接続の完全な遮断、および全接続をプライベートIP により完結したことでIDAP 保有の膨大なデータの情報漏洩リスクを大幅に軽減した閉域環境への導入を実現

https://k-tai.watch.impress.co.jp/docs/news/1349356.html

【利用プロダクト抜粋】

BigQuery

VPC Service Controls

Cloud Interconnect

Google Cloud

Thank you!