CONFIDENTIAL

CLOMO ユーザーミーティング 2020

CLOMO のインフラセキュリティ

株式会社アイキューブドシステムズ
製品開発運用本部
田崎 大輔

今日お話しすること

- CLOMOのインフラストラクチャ
- CLOMOのセキュリティ
- CLOMOの今後の取り組み

CLOMOのインフラストラクチャ

CLOMOはどこにある？

■Webアプリケーションはどこで動いてる？

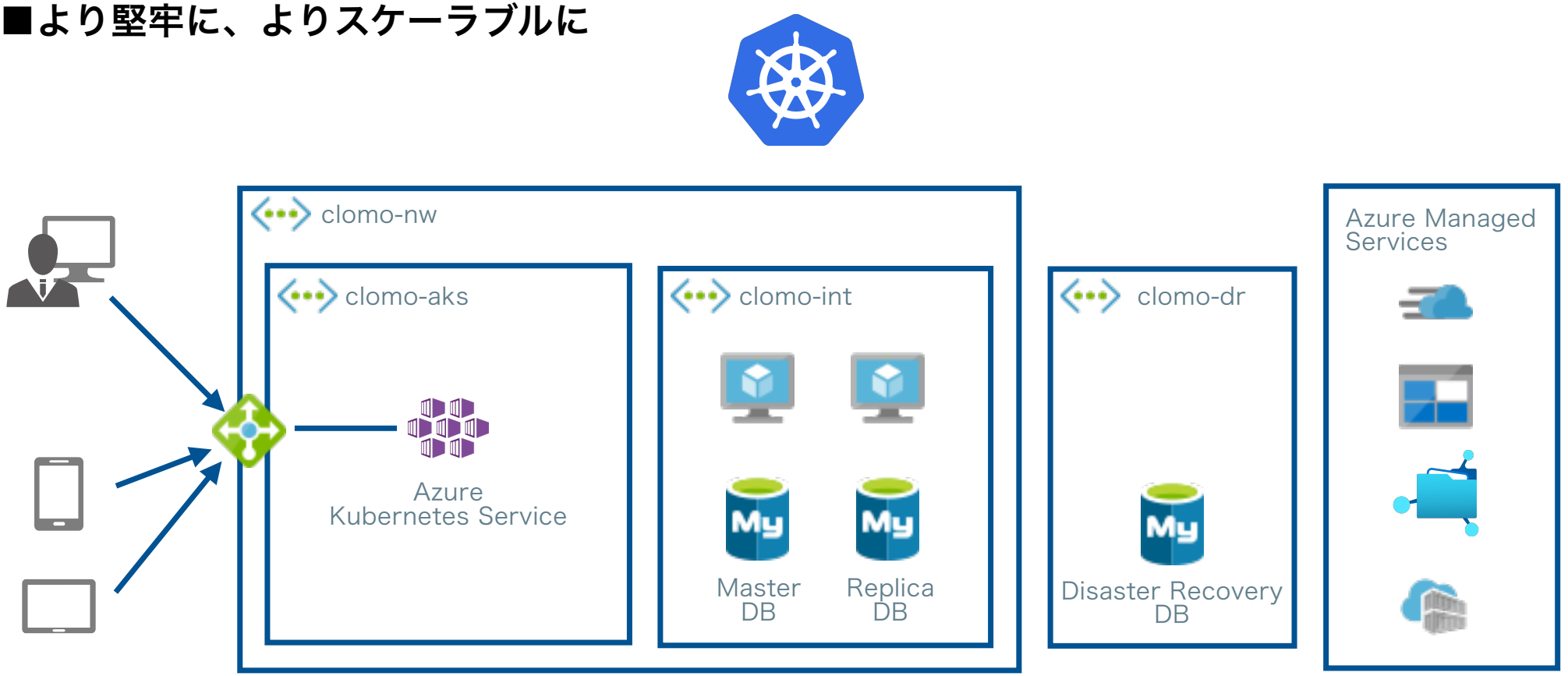
福岡？ 東京？
米国？

CLOMOはクラウドに

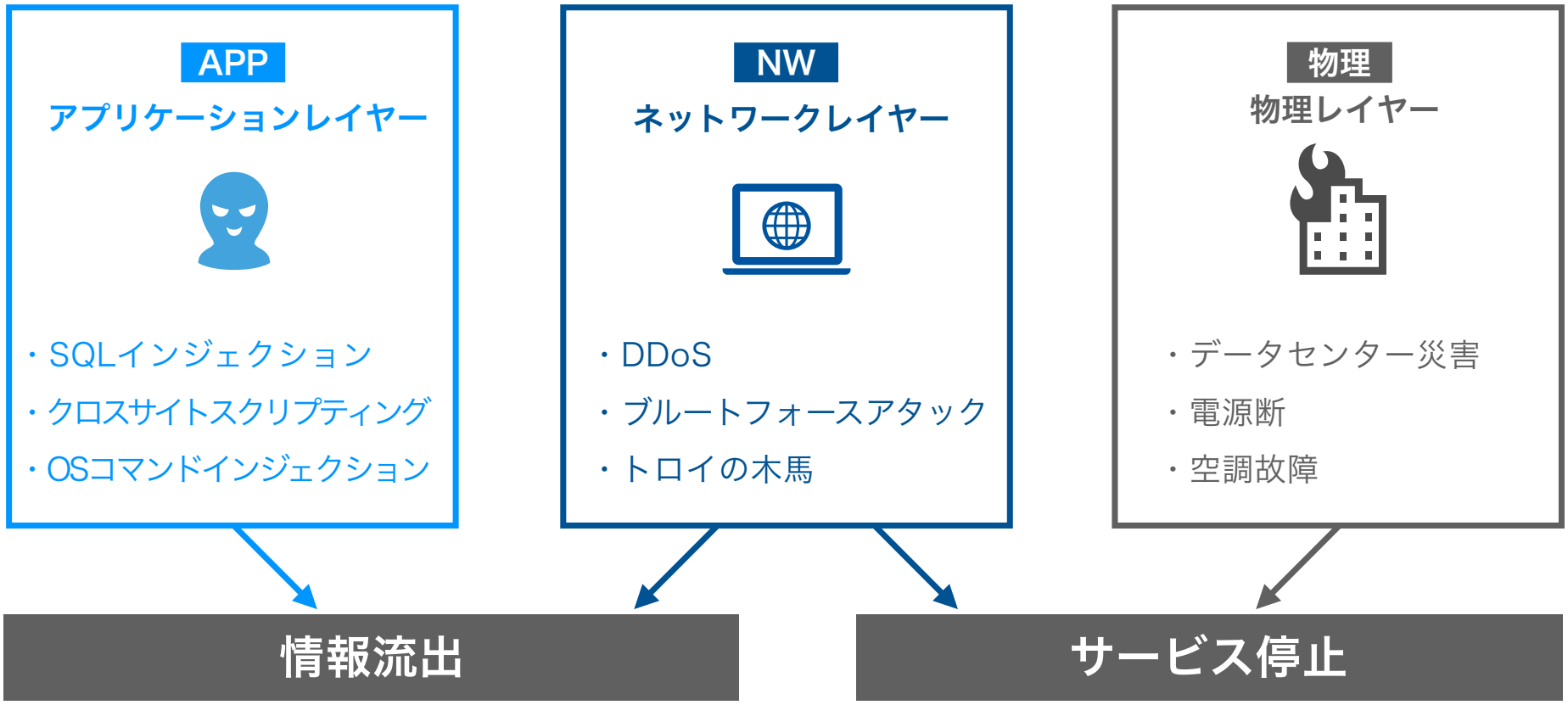
■Microsoft社のAzureを使用

CLOMOシステム構成

■より堅牢に、よりスケーラブルに



どんなリスクがあるのか？



CLOMOのセキュリティ

Azureのセキュリティ

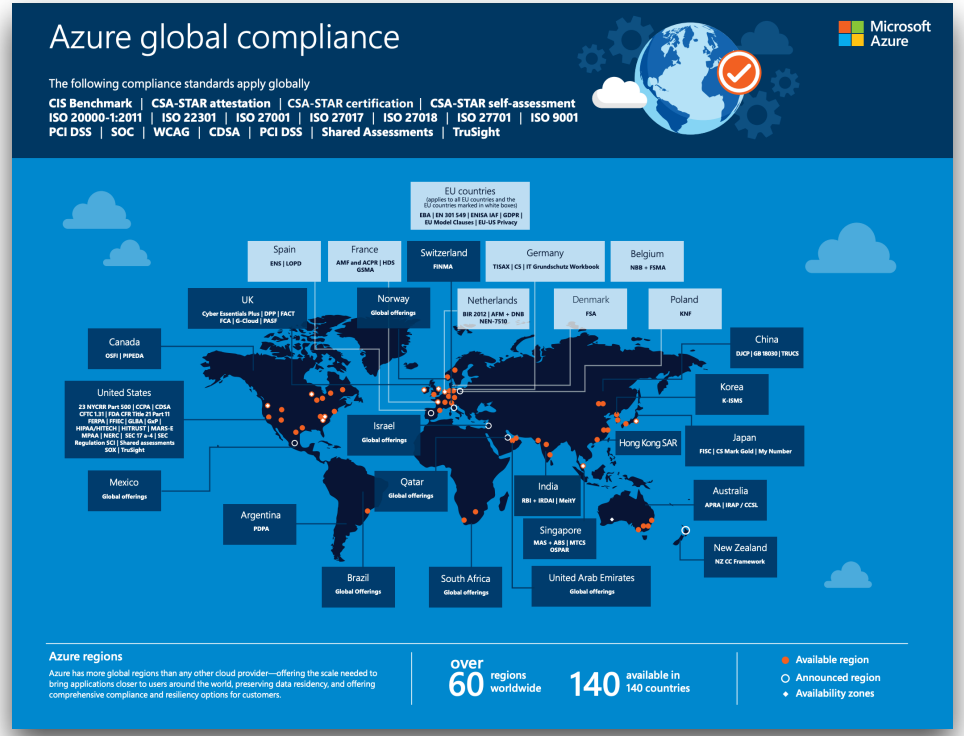
APP NW 物理

■90を超えるコンプライアンス認定資格

【 例 】

・ISO / IEC 27001:2013

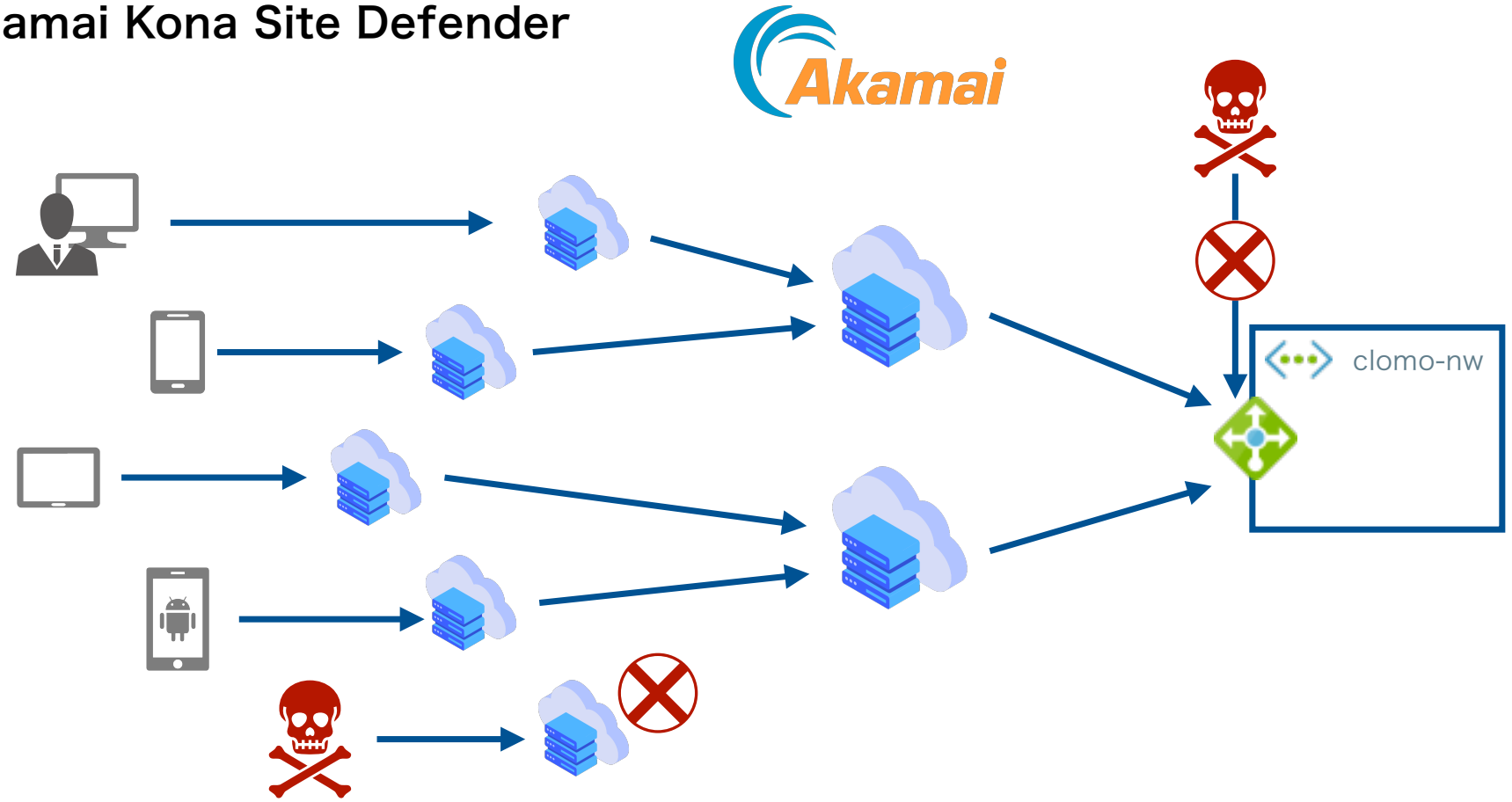
・FISC（金融機関向けコンピューターシステムに関するセキュリティガイドライン）



WAF: Web Application Firewall

APP NW 物理

■Akamai Kona Site Defender



脆弱性診断

APP NW 物理

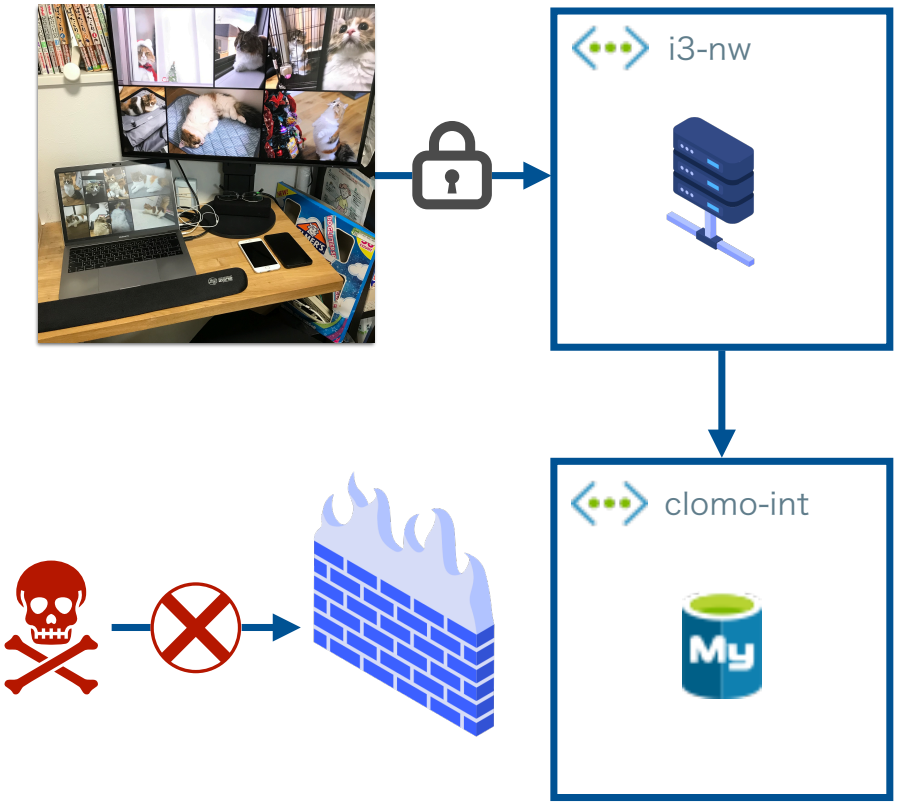
■Webアプリケーション診断

CLOMOのWebアプリケーションに脆弱性
が存在していないか、第三者機関により
定期的に診断

リモートワーク環境

■Firewall + VPN

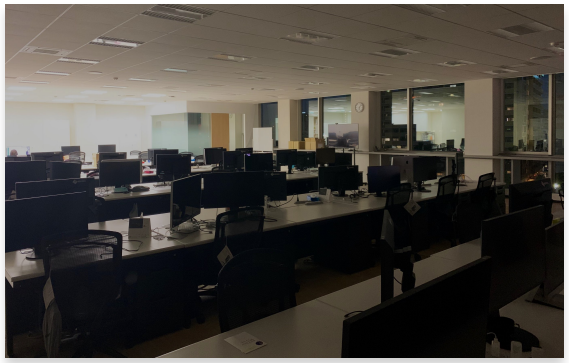
コロナ禍の中でもVPNを経由して安全に
CLOMOの運用・バージョンアップリリース

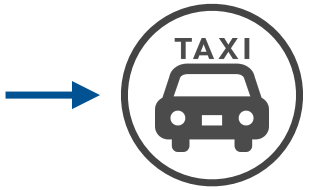


（余談）新バージョンリリース作業

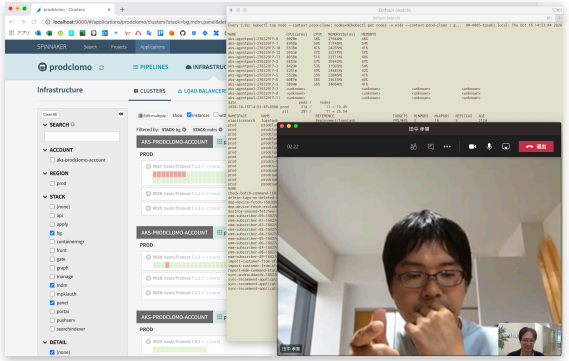
■22:00～26:00ごろ 深夜作業

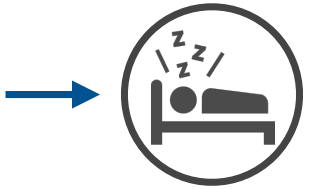
・before コロナ
オフィスにて作業 → タクシーで帰宅
→（風呂など）→ やっと就寝





・with コロナ
自宅からリモート作業 → 就寝
（プラットフォーム運用部のニューノーマルに）





お客様からお預かりした認証情報の扱い

APP NW 物理

■用途に合わせて適切な暗号化

・ログインパスワードなど
ソルト ＋ ストレッチング ＋ ハッシュ化 で不可逆に変換
(CLOMOがリリースされてからの約10年の間に一般的になった手法)

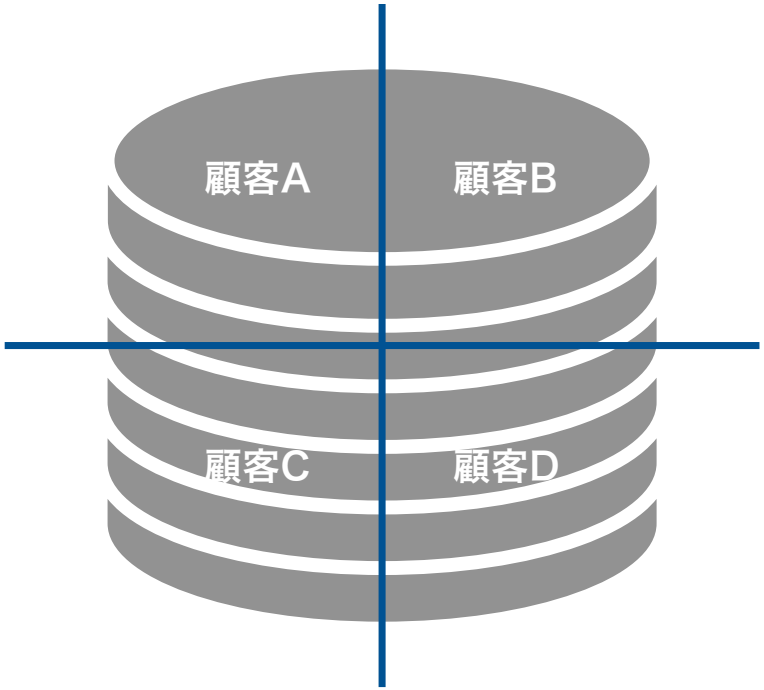
・プロキシサーバーパスワードなど
暗号化してDBレコードに保存。デバイスインストール時に復号
複合キーは別管理されており社内でも限られた担当者しか知り得ない

→ 万が一、DB情報が流出してもパスワード複合は困難

論理的なカスタマー情報の分離

■マルチテナント・アーキテクチャ

お客様ごとに論理的にデータを分離



管理者アカウントの権限分離

APP NW 物理

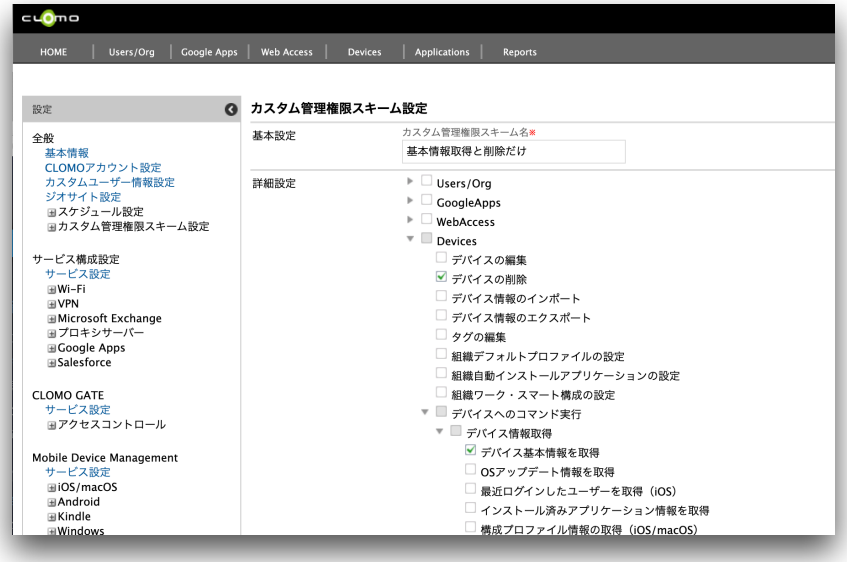
■カスタム管理権限スキーム：ロールベースアクセス権

【 例 】

・オペレーター：
デバイス情報取得とリモートワイプのみ
操作可能

・部門管理者：
特定の組織下のデバイスのみ操作可能

・カスタム管理者：
指定の操作のみ可能



24/365有人監視

APP NW 物理

■システム負荷アラートチェック

平日・定時：プラットフォーム運用部
休日・夜間： 外部パートナー
→ プラットフォーム運用部

■CLOMO機能チェック

お客様の利用を想定した動作正常性確認
・アプリケーションインストール・削除
・VPPライセンス付与・剥奪
・プロファイル自動適用・解除　　など

CLOMOの今後の取り組み

より安全に、より迅速に、より柔軟に

■お客様へ価値を提供できるように

・製品開発サイクルの改善 → リリースを短期間に高頻度に
　平日日中の無停止リリース
　一部ユーザーから部分的にリリース (カナリアリリース)

・システム監視の高度化
　不審なアクセスの検知
　負荷状況に応じた柔軟なスケーリング

→ Kubernetes および その周辺技術を使い倒す

最後に

プラットフォーム運用部の使命は、
CLOMOシステムを絶対に止めないことです。
24/365でお客様が安心してCLOMOを利用して
いただけるよう日々、運用・監視をしていきます。

CLOMOの内側を改善するだけでなく、
CLOMOの外側も外部ベンダーと協力して
より強固にしていきます。
これからもCLOMOをよろしくお願いします。

CONFIDENTIAL

i3systems