

秘密計算を実現する conclave/conclave Cloud

c·rdaDay

～ブロックチェーンで変わる新たな世界～

2022年11月10日 | 東京開催

アジェンダ

- Conclaveとは？
- Conclaveのしくみ
- Conclave適用分野/事例紹介
- Conclave Cloud Demo解説
- デモ実演

Conclaveとは？

- TEE (Intel® SGX) を使うアプリケーション用構築SDK/基盤
- **簡単**にアプリケーションを開発できる
- **柔軟**にアプリケーションを開発できる
- **高速**に実行できる

全く新しいセキュリティモデルの活用！

Introducing **conclave**

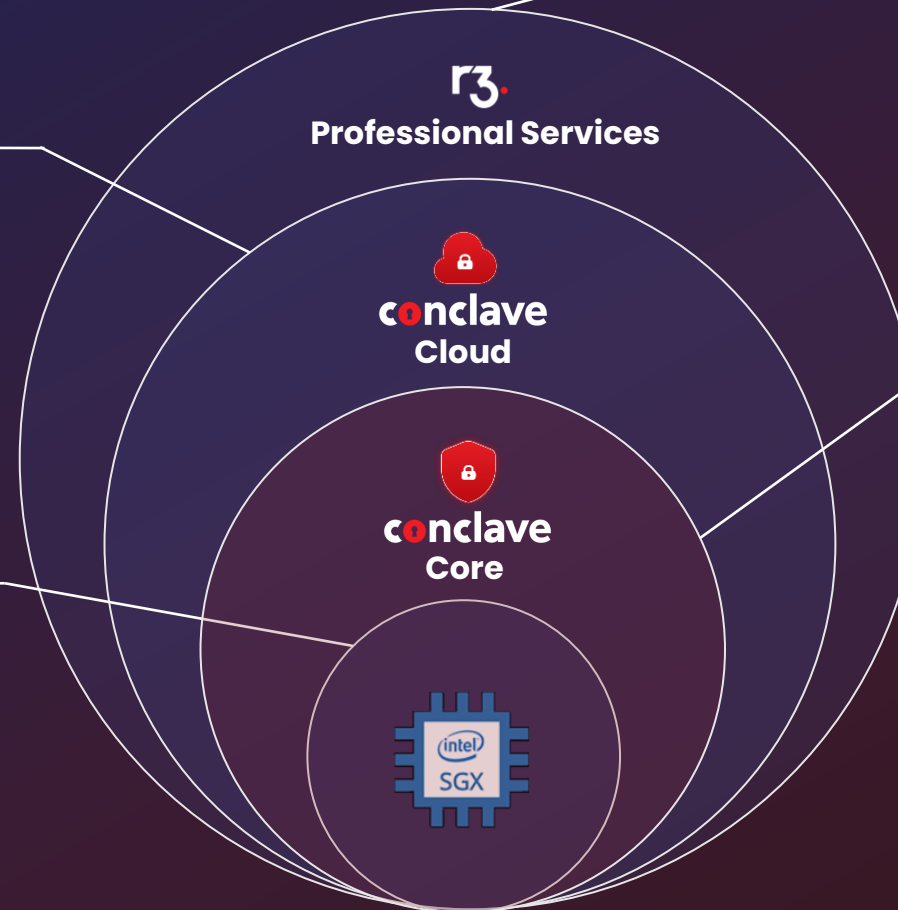
The easiest platform to build and deploy privacy preserving applications, in the cloud or on-premise

CONCLAVE CLOUD (On Microsoft Azure)

- Managed, serverless confidential computing platform
- Confidential Functions as a Service (FaaS)

INTEL SGX

- Hardware-based encryption
- Protects select code and data in use
- Provides integrity and confidentiality guarantees



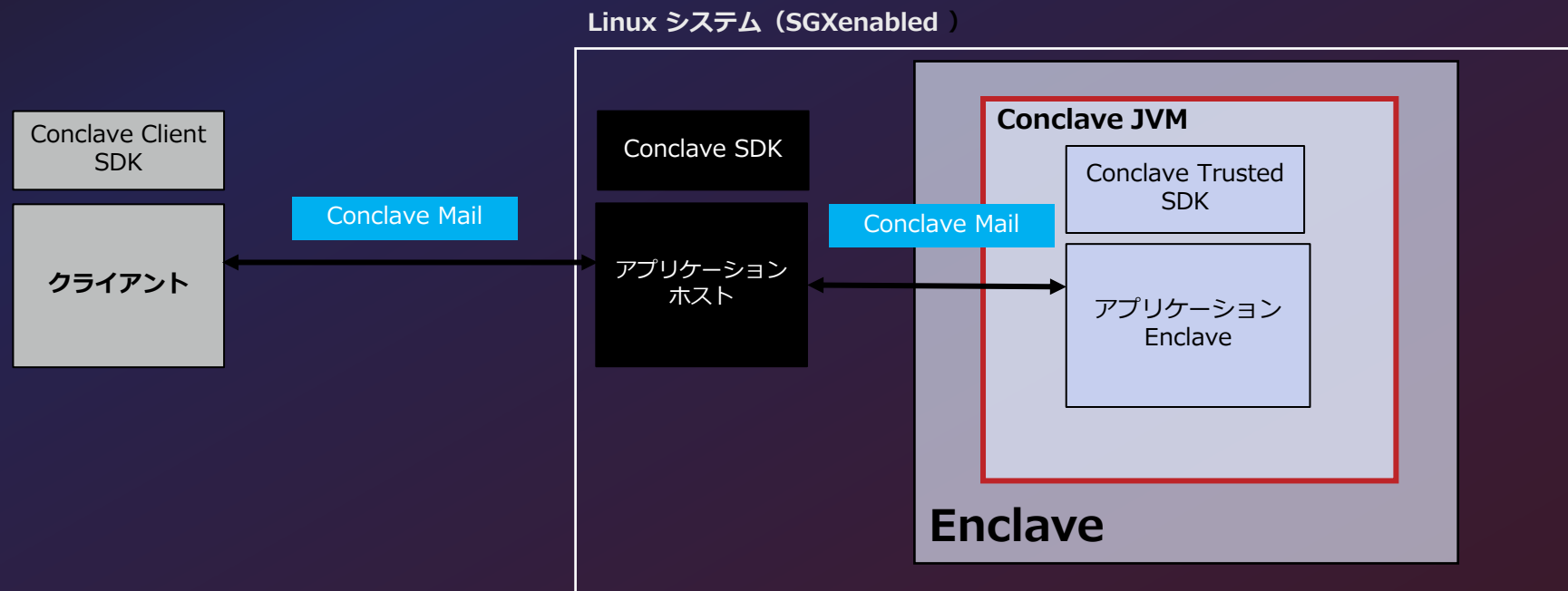
R3 PROFESSIONAL SERVICES

- Access to world 's leading firms
- Accelerated design, development, and deployment
- Extensive Financial Services expertise
- Enterprise-grade confidential computing solutions

CONCLAVE CORE

- Full Software Development Kit (SDK)
- Simplifies the development of confidential computing applications

Conclaveのしくみ



- 信頼されていない
- 信頼できる
- 暗号化

Conclave適用分野・事例紹介

Conclaveの適用分野

法規制への対応
コンプライアンスへの対応

企業内データ連携による
データ活用の深耕

信頼モデルから
第三者を削除

マルチパーティデータセッ
トによるサービス向上

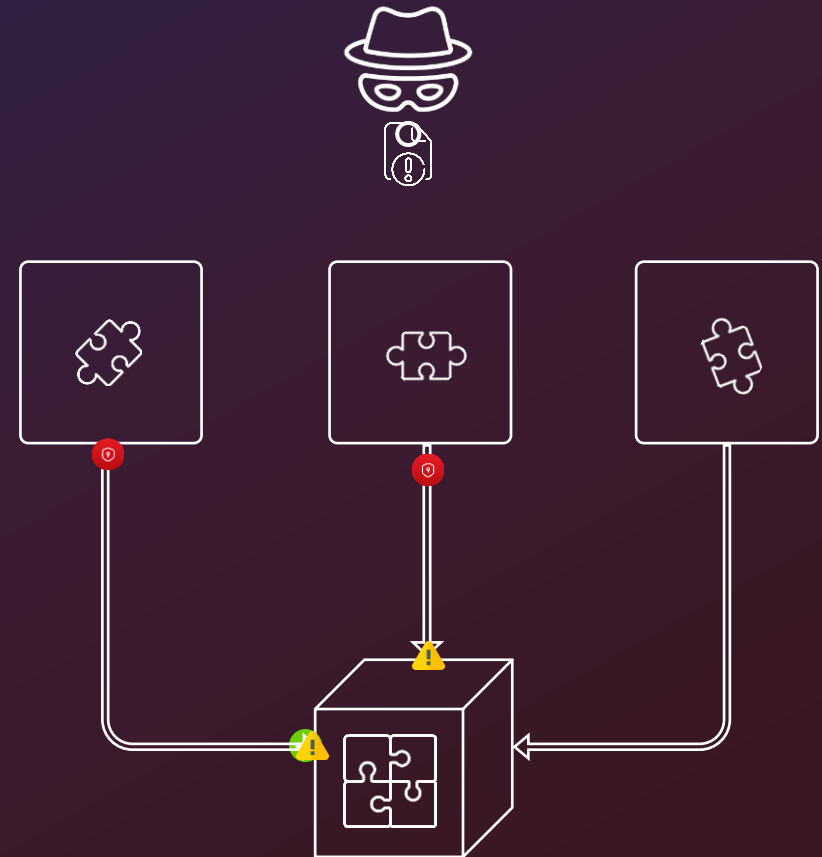
サービス向上のための
アウトソーシング機能

Conclave事例：CLAIMSHARETM

保険の二重請求不正を見抜く

IntellectEUは、個人情報照合しながら、顧客データ保護を技術的に保証し、GDPRに完全に準拠したソリューションを求めています

- ✓ Conclaveにより、ClaimShareチームは限られた秘密計算の知識のみで、アプリケーションを迅速に開発することができました
- ✓ Claimshareのソリューションにより、不正行為のコストを最大10%削減できると試算しています。
- ✓ KPMGとグローバルアライアンスパートナーシップを締結
- ✓ 世界20カ国以上の保険会社や規制当局との連携



Conclave事例： 人身売買の撲滅



Hope For Justiceは、政府間の機密データ連携を活用した安全なマッチングアルゴリズムを開発し、データ分析を強化する必要がありました。

従来の課題

- ✕ 機密性の高いデータのサイロ化
- ✕ パターンディスカバリーの限界
- ✕ 重要な組織間の信頼性の欠如

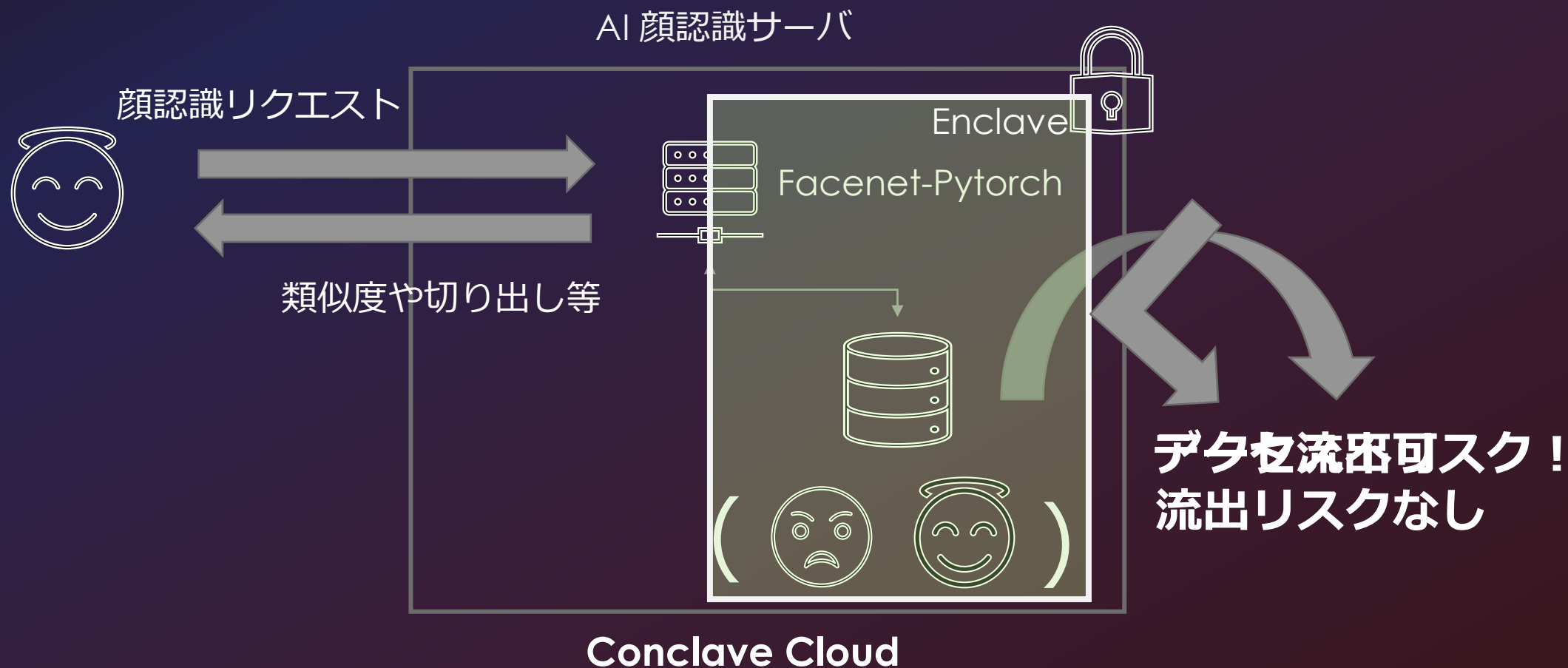
Conclaveによる解決

- ✓ 人身売買検知の強化モデルを開発
- ✓ より高度なアナリティクスの導入
- ✓ 法執行機関間の関与と信頼の向上



Conclave Cloud Demo 解説

データ保護を可能とした顔認識デモ





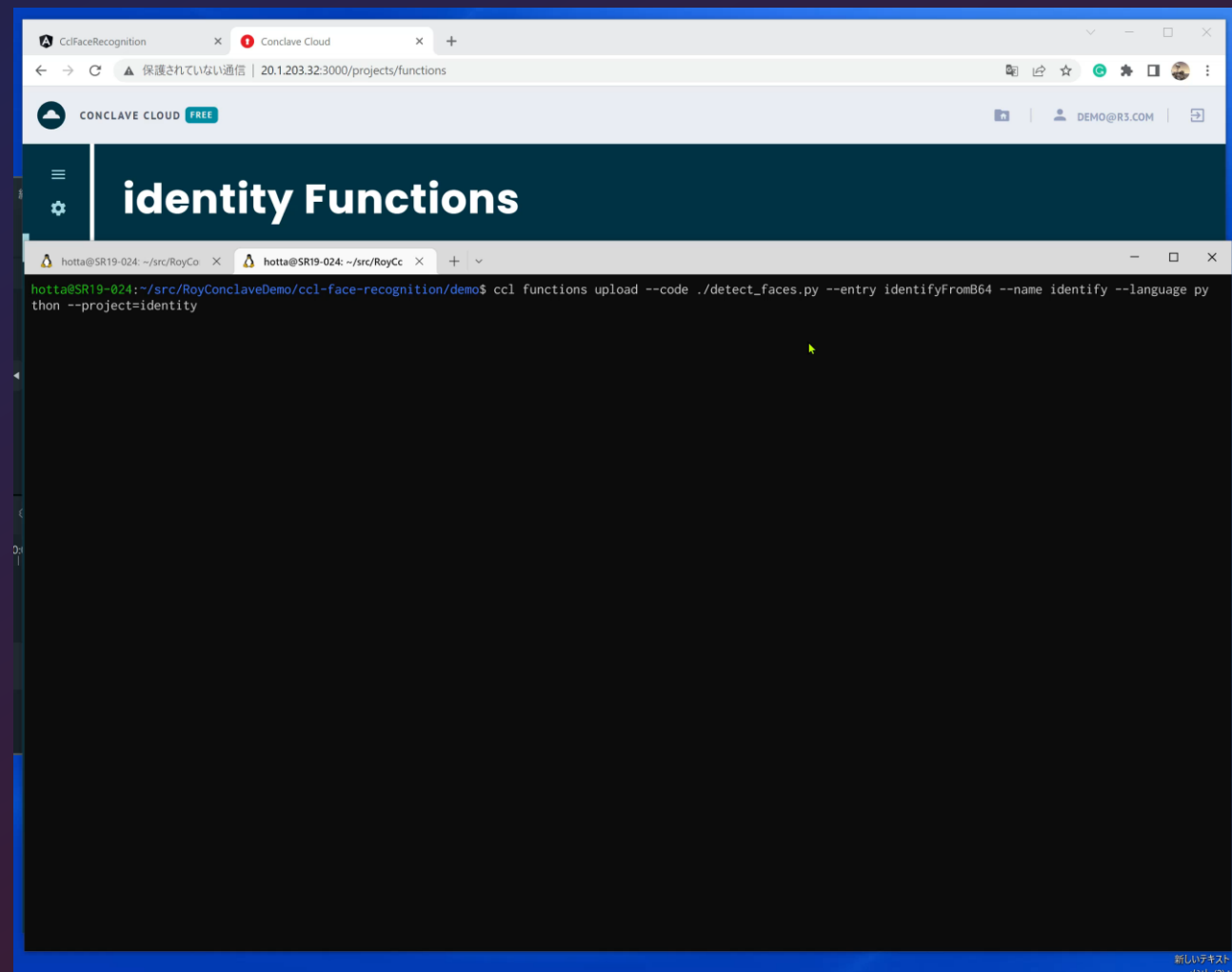
デモ実演

デモ動画 設定

The screenshot shows the Conclave Cloud website with the following content:

- Header:** "CONCLAVE CLOUD" logo on the left, "CONCLAVE.NET" and "LOGIN" on the right.
- Main Title:** "Join Conclave Cloud"
- Plans:**
 - Free:** \$0 /month. Includes: Unlimited Projects, 100 Invocations, 5,000 seconds of execution time*, Community Support. Button: "CHOOSE FREE". Note: "No credit card required".
 - Pro:** \$30 /month (from). Includes everything in Free, plus: 5,000 seconds of execution time*, \$0.00031 / second thereafter, Pay as you go pricing, No usage caps. Button: "CHOOSE PRO". Note: "Credit card details required Minimum subscription \$30/month".
 - Enterprise:** For larger organizations with enterprise requirements. Includes everything in Pro, plus optional: Priority Ticketed Support* & Enterprise, Professional Services, Custom enclave hosting, Hosted Key Derivation Service, and more... Button: "CHOOSE ENTERPRISE". Note: "*Service levels determined by spend".
- Footer:** "Start for Free Today!" and "CREATE ACCOUNT →" button.

デモ動画 設定



デモ動画 設定

The screenshot displays a web browser window at the top and a Visual Studio Code editor window below it. The browser shows a Conclave Cloud portal with a URL of 20.1.203.32:3000/projects/files. The VS Code editor is open to a project named 'ccl.service.ts - ccl-face-recognition [WSL: Ubuntu-20.04]'. The left sidebar shows the file explorer with a tree structure including 'README.md', 'detect_faces.ipynb', and 'ccl.service.ts'. The main editor area shows the 'ccl.service.ts' file with TypeScript code for a service that interacts with the Conclave Cloud API. The code includes imports for 'Conclave' and 'Conclave.create', and a function 'identify' that takes a data URL and returns a result. The status bar at the bottom indicates 'WSL: Ubuntu-20.04' and '0 22'.

```
1  ccl-face-recognition > src > app > TS ccl.service.ts > apiKey
2  ectable } from 'angular/core';
3  clave } from 'conclave-cloud-sdk';
4
5  = "1";
6  fyHash = "0AB1DC33B3734989D0E046ESC2C8789A726CEE96E70684D9F8F8926695BE6
7
8  {
9    : 'root'
10
11  CclService {
12
13    nclave: Conclave
14
15    n(
16
17      clave = Conclave.create({
18        : apiKey,
19        : 'http://20.75.64.114'
20
21
22
23    nc identify(dataUrl: string) {
24      64 = dataUrl.split("base64,");
25      64.length != 2) {
26        e.log("Invalid data URL");
27
28      sult = await this.conclave.functions.call('identify', identifyHash, [bas
29      esult.return;
30
31
32
33
```

まとめ

Conclaveを使用すると、

- 簡単に
- 柔軟に
- 高速に

データ/プログラムの改ざん漏洩の恐れなく
安全にデータを活用できます。

SBI r3.

Japan