Corda Tech Meetup 秋の陣

SBI R3 Japan

Intel® SGX

Conclave

インテルSGXのアプリケーション開発キット「Conclave」のご紹介

SBI R3 Japan株式会社

2021年11月25日

秘密計算を実現する conclave

サービスプロバイダーやクラウドベンダーからデータを保護したまま処理を実行

- ✓ Conclaveは、秘密計算を行うためのハードウェアであるIntel SGXに、アプリケーションの安全な実行環境(TEE)の実装を容易にするSDK(Software Development Kit)
- ✓ ホストアプリケーションの内部にEnclaveという隔離領域を作り、処理を実行
- ✓ 秘匿データにアクセスできるのはこの内部プログラムだけなので、サービスプロバイダーやクラウドベンダーなどからは見えない。またプログラム自体の改ざん不可

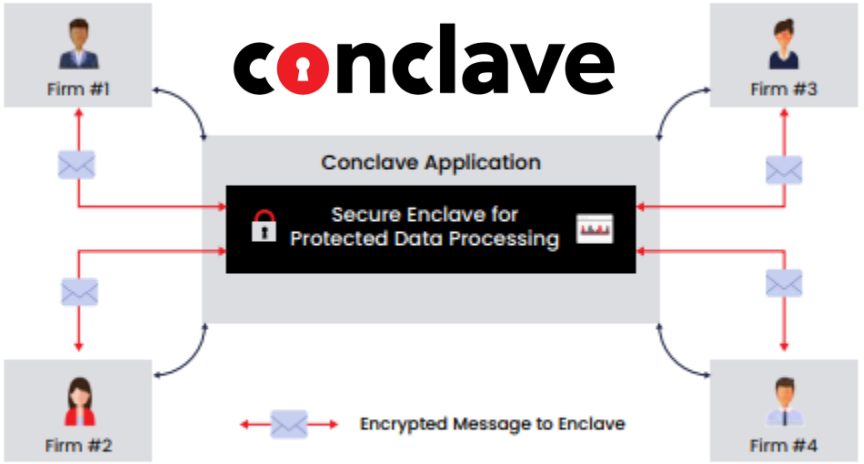


Figure 1: Multi-party data pooling

Conclave公式サイト：リンク

SBI R3 Japan

秘密計算により内容の結果だけを取得：

入力された
原材料情報

原材料
小麦粉……10g
塩……5g
そば粉……20g
ねぎ……5g
鰹節……1g

レシピ詳細を見せたくない

情報の格納は暗号化

原材料
dy374899095tsf35s56ac
sds3sjudte5h998780987
hjs63473902yshdtge633
jfh56352938654378thw
2ujd67wp9hvcdjsker667

アレルゲン情報

小麦粉は入っていますか？

小麦粉は入っています

プラットフォーム上の
アプリケーション

栄養成分表示

エネルギー	360 kcal
たんぱく質	11.2 g
脂質	3.0 g
炭水化物	75.0 g
ナトリウム	14 mg
ビタミンB1	0.45 mg
…	

（重量100g当たり）

原材料は分からないが
栄養成分表示に変換

あらかじめ合意した質問に対して
（計算して）回答だけを表示
中身のデータを見ることができない

SBI R3 Japan

Conclaveのコンポーネント

Conclaveアーキテクチャーを構成する３つのコンポーネント

Enclave

Enclave(エンクレーブ：飛び地）とはインテル® SGXマシンの保護されたメモリ空間で動作し、外部から隔離されたプログラムのことです。プライベートなデータを秘密裏に処理し、処理結果を返します。ホストと同じJVMを共有しない専用のサブJVM（GraalVM）にロードされます。

Host

エンクレーブは隔離されており、クライアントはエンクレイブに直接アクセスすることはできず、メッセージをエンクレイブに届けるのはホストになります。ホストマシンでは以下のようなホストプログラムを実行します。
- エンクレーブのプログラムを読み込む
- エンクレーブに必要なリソースの提供
- クライアントとの間の代理人としての役割

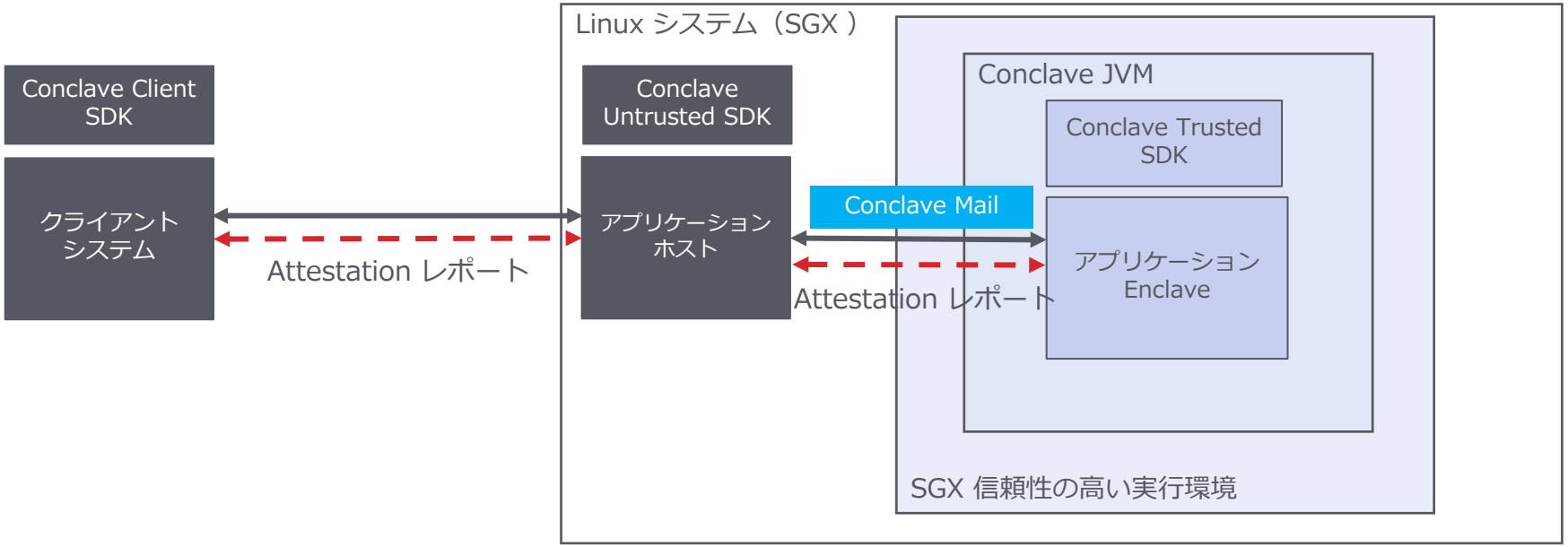
Client

クライアントは、機密データをエンクレイブに送信し、ホスト経由で処理するプログラムです。Conclaveには、エンクレイブとクライアント間のコミュニケーションを容易にするためのMail APIが付属しています。

SBI R3 Japan

アーキテクチャ　イメージ図

Conclaveにより信頼性の高い実行環境を容易に構築可能



- Conclaveは専門家でなくても使用可能
  - ✓ Intel SGXの専門知識不要
  - ✓ SDKクラスでTEE技術をシンプルに
  - ✓ 明確なドキュメントやチュートリアル が用意されている

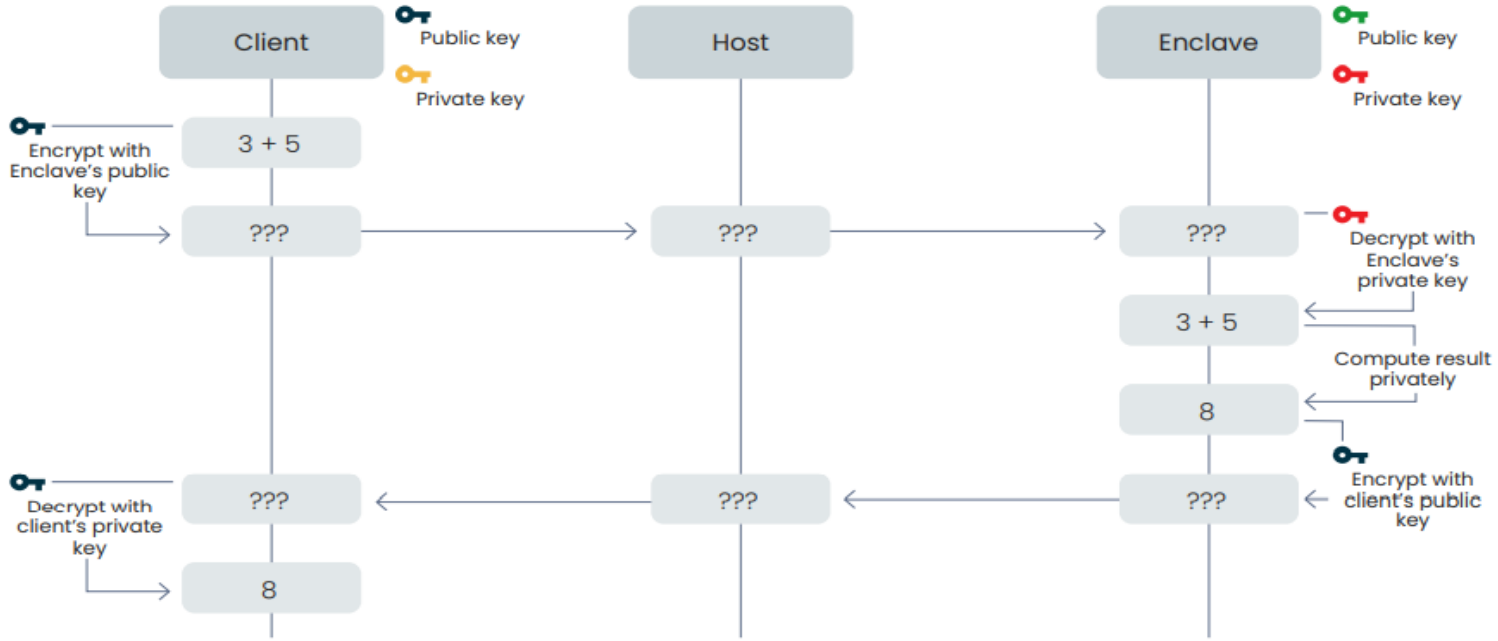
信頼されていない
信頼できる
暗号化

SBI R3 Japan

暗号化メッセージング

Conclaveの各コンポネントは信頼性の高い暗号で通信します

- エンクレイブとクライアントは、キーペアを使用して、両者の間で交換される情報を暗号化および復号化します。
- クライアントは、エンクレイブに送信された情報をエンクレイブの公開鍵を使って暗号化し、エンクレイブの秘密鍵を使ってのみ復号できるようにします。
- このため、情報を中継する役割を担うホストは、その情報を読み取ったり改ざんしたりすることができません。
- 同様に、エンクレイブはクライアントの公開鍵を使用して処理結果を暗号化するため、クライアントのみが復号化して読み取ることができます。



Conclaveの強み

Conclaveは開発者フレンドリーな秘密計算SDKです

秘密計算のハードルの高さ

- Intel SGXにTEEを実装するためには、低レベル言語や暗号技術に対する専門知識が必要
- 専門人材の確保が必要、または開発者への学習コスト高

Conclaveにより秘密計算を使ったサービス構築が容易に

1. Conclaveは専門家でなくても使用可能
   - Intel SGXの専門知識不要
   - SDKクラスでTEE技術をシンプルに
   - 明確なドキュメントやチュートリアルが用意されている
2. GraalVMとの統合
   - Java、Kotlin、Scalaなどの標準的なJVM言語や、Javascriptなどのスクリプト言語でアプリを開発可能
3. Windows、Linux、MacOS対応

SBI R3 Japan

リモート認証(Remote Attestation)

エンクレイブの信憑性を検証するために、「リモート認証」が使用されます

どんなプログラムもランダムなキーペアを使用して正当なエンクレイブを騙ることができます。クライアントにとって重要なことは、エンクレイブであると宣伝しているソフトウェアが実際に正当なエンクレイブであることを確認することが必要です

リモート認証とはエンクレイブを確認するための重要な情報を含んだデータのことです。測定値(measurement)が含まれています。
測定値は、特別なツールを使用して生成された一意のハッシュで、ハッシュはenclaveにロードされたfat-jarから生成されます。測定値はenclaveのソースコードをコンパイルすることで検証できます。(同じソースコードの複数のビルドが同じ測定値を生成する)

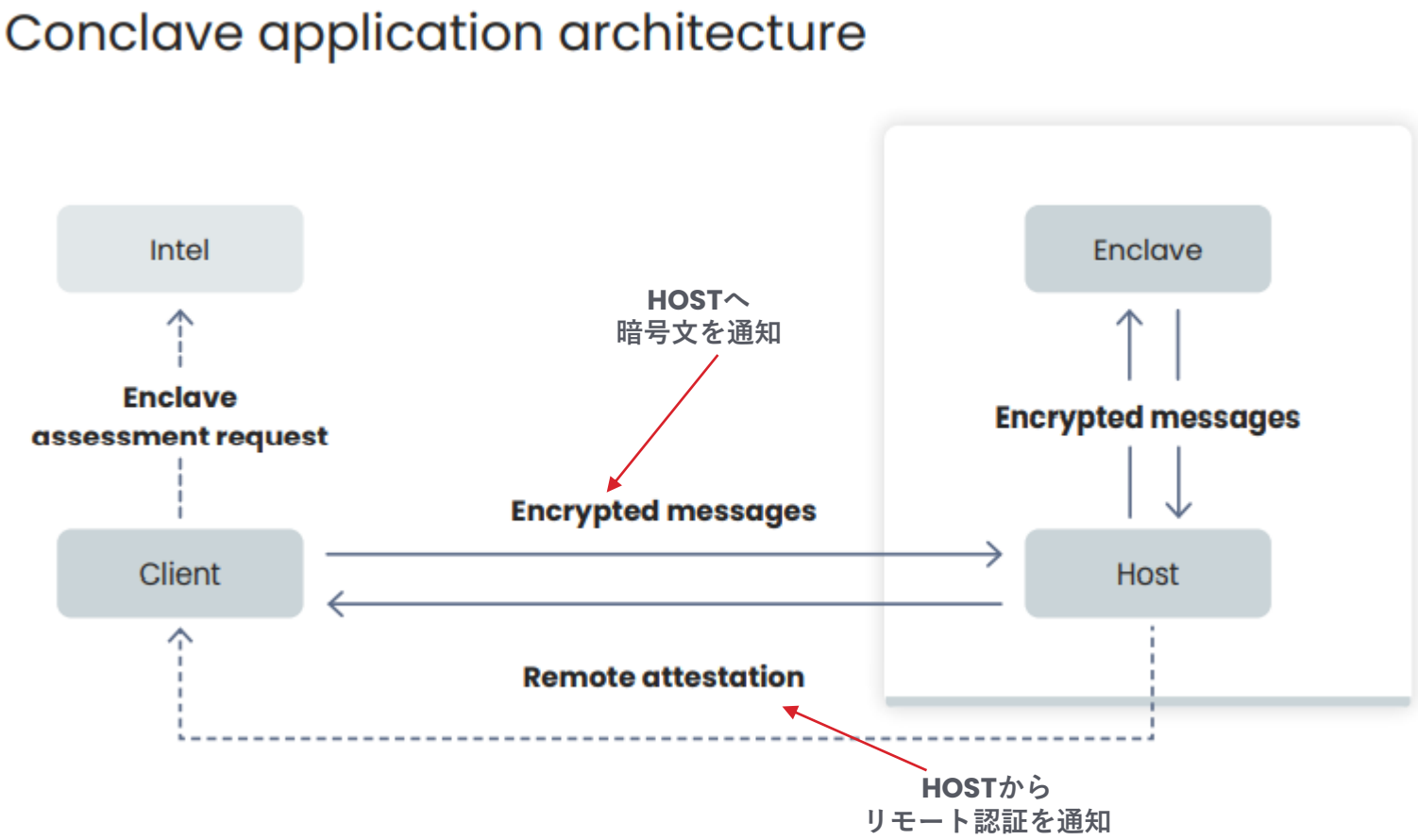
リモート認証に加えて、クライアントはインテル® SGX にエンクレイブの評価を依頼し、エンクレイブが安全であるかどうかを確認することができます。インテル® SGX は、エンクレイブのハードウェアが最新のバージョンを使用しているか、セキュリティ上の脆弱性があるかなど、重要な情報を提供します。

SBI R3 Japan

Conclaveのアーキテクチャー図

conclave

Conclaveの３つのコンポーネントの関係は下記の概念図になります。



SBI R3 Japan

Conclaveメール

開発者がクライアントとエンクレイブ間の通信を容易にするMail API

Encryption	クライアントとエンクレイブ間のメッセージをAES暗号を用いてエンドツーエンドで暗号化。
Headers	メールには、暗号化されていない改ざん防止されたヘッダーがあり、これを使ってメッセージを結びつけることができます。また、トピックとシーケンス番号を使用することで、メッセージの順番を変えたり、メッセージを取りこぼしを防ぎます。
Authentication	メールは、メッセージが特定の鍵の所有者から送られてきたことを証明するとともに、送信先の公開鍵に暗号化することができます。
Framing	メールは、メッセージの始まりと終わりが簡単に識別できるように区切りますが、その上にフレーミングを実装する必要はありません。

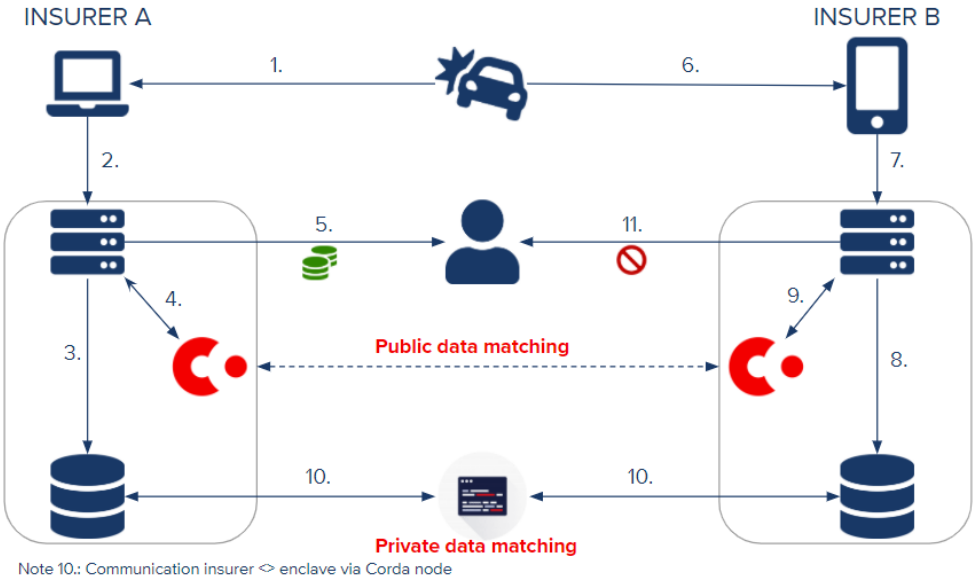
SBI R3 Japan

Conclave事例①ClaimShare（保険金の二重支払防止）

概要

Insurance EuropeとKPMGの調査によると、2017年だけでもヨーロッパでの不正請求の推定総額は130億ユーロでした。各保険会社はデータ分析によって防止に努めているものの、個人情報の共有に関する規制が理由で、自社データの分析に限られていました。

しかし、Cordaのプライバシー設計により、企業横断的な新しい不正検知のモデルが実現しました。



サービス名	**ClaimShare**
開発パートナー	intellect EU
ユースケース	損害保険／生命保険
サービス特徴	• 保険会社は保険金の支払い履歴をCordaに記録します。それにより、新たに保険金請求を受けた保険会社は、別の保険会社で既に支払いが行われているか検証できます。疑わしい請求が検知された場合は、より詳細な比較検証を行います。詳細情報も一致する場合は不正請求と見なして保険金は支払われません。 • R3社のConclave(Intel SGXを利用してConfidential Computingの機能を実装したもの)を使用することにより、データを他の保険会社に公開することなく検証できます。
紹介動画	Link
Next Step	• R3社とB3i社がスポンサーを務めるCorda Challenge 2020 保険部門で優勝 • 自動車以外の保険にも適用予定

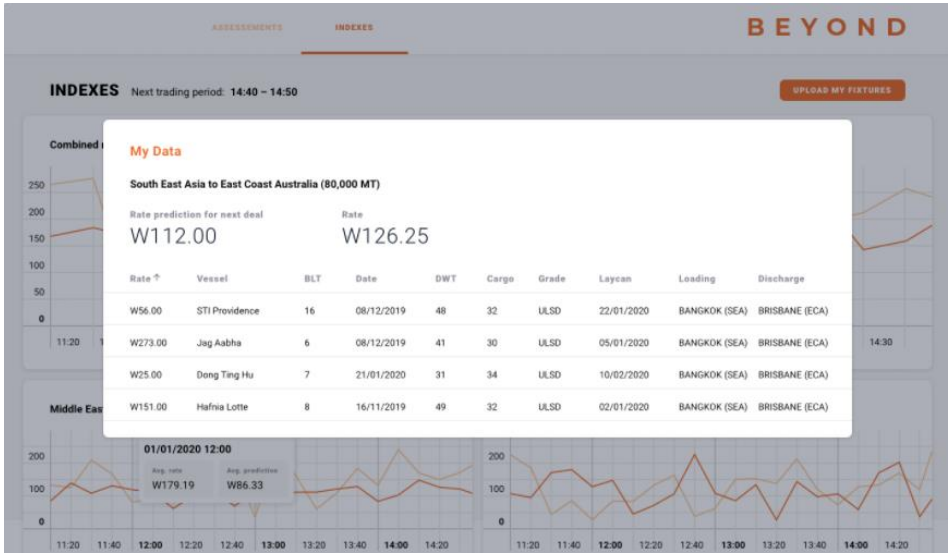
SBI R3 Japan

Conclave事例②Beyond（機密取引プラットフォーム）

課題

トレーダーはマーケットで流動性を求めるが、自分の取引条件や価格条件がマーケットに悪影響を及ぼす可能性があるため、それらを公開したくない場合がある。

また、取引所の運営者とその従業員は、取引相手の身元や取引条件など、悪用される可能性のある重要な商業情報にアクセスすることができる。



サービス名	**Beyond**
開発パートナー	appliedblockchain
ユースケース	キャピタルマーケット
サービス特徴	• Conclaveにより機密取引プラットフォームを実現 • 取引履歴、取引量、価格データは、取引所運営者から秘匿された状態で取引が処理される • マッチングやプライシングのアルゴリズムの透明性の担保 • 取引所運営者に個別の取引データを開示することなく、コンプライアンス管理を実行 • トレーダーは取引ユーザインタフェースやAPIを介して取引可能
Webサイト	Link
Next Step	• コモディティ市場でテスト中

SBI R3 Japan

秘密計算の活用が見込まれる分野

- AML (Anti Money Laundering)
- ダークプール
- プライベートオークション
- AIや機械学習を使ったプライベートデータ分析
- 会社間でプライベートデータを収集して分析　など

SBI R3 Japan

秘密計算技術比較

種類		概要	課題
ソフトウェアによる秘密計算	ゼロ知識証明 (ZKP)	✓ データを公開することなく、データへのアクセス権を持つ事を証明する	• 計算能力への高い要求 • スケーラビリティ • 実装が難しい（任意のアルゴリズムを実装できるわけではない）
	準同型暗号化 (HE/FHE)	✓ 部分準同型暗号(HE) ✓ 完全準同型暗号(FHE)	• 計算コストが高い（クラウド移行すら厳しい） • 完全準同型暗号は、平文操作の除外が難しく、ユースケースに制限
	ｾｷｭｱ･ﾏﾙﾁ･ﾊﾟｰﾃｨ･ｺﾝﾋﾟｭｰﾃｰｼｮﾝ (sMPC)	✓ 各当事者がデータの断片だけを保持する「秘密の共有」に依存 ✓ バラバラのデータの一部が知られても元のデータは秘匿可	• ユースケースごとのカスタムアルゴリズム構築 • 高い通信コスト／高い計算コスト
ハードウェアによる秘密計算		✓ ハードウェア依拠 ✓ **様々なアルゴリズムに対応** ✓ コード実行とメモリを他から分離する ✓ TEE(Trusted Execution Environment)を構築	• 低レベル言語や暗号技術に対する専門知識が必要 **conclave** で実装を容易に

ハードウェア（TEE)による秘匿計算比較

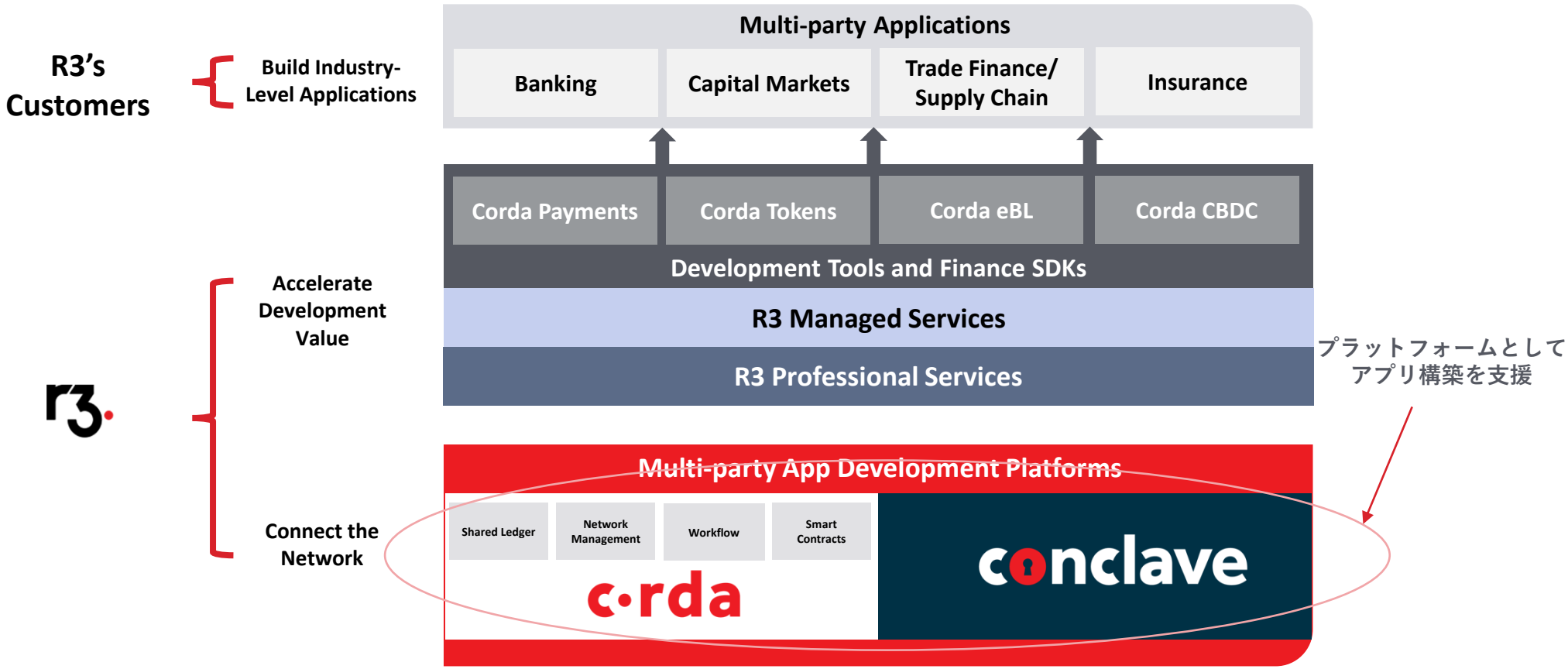
① Intel SGX
(ア) Intel SGXはビジネスロジックのセンシティブな部分だけ、つまり最小限の信頼を置くことに重点を置いています。
(イ) マルチ・パーティのコンピューティング機能に対する強力な監査プロセス
(ウ) SGX TCBリカバリー・プロセスが、ソフトウェア・バグや、サイド・チャネル・アタックの対処に成功

② AMD SEV
(ア) AMD SEVはクラウド上のVM保護を強く意識している
(イ) マルチ・パーティのコンピューティング用途には不向き
(ウ) ソフトウェアに致命的なバグや、セキュリティ上の欠陥が発見された場合に、ソフトウェアのリカバリーができない

③ ARM Trustzone
(ア) ARM Trustzoneはリモート認証をサポートしていません。
(イ) 主に携帯電話メーカーにおいて、ユーザーから携帯電話をロックするために使われます。
(ウ) モバイルOSに重点を置いています

SBI R3 Japan

Cordaとならぶアプリケーション基盤の位置づけ

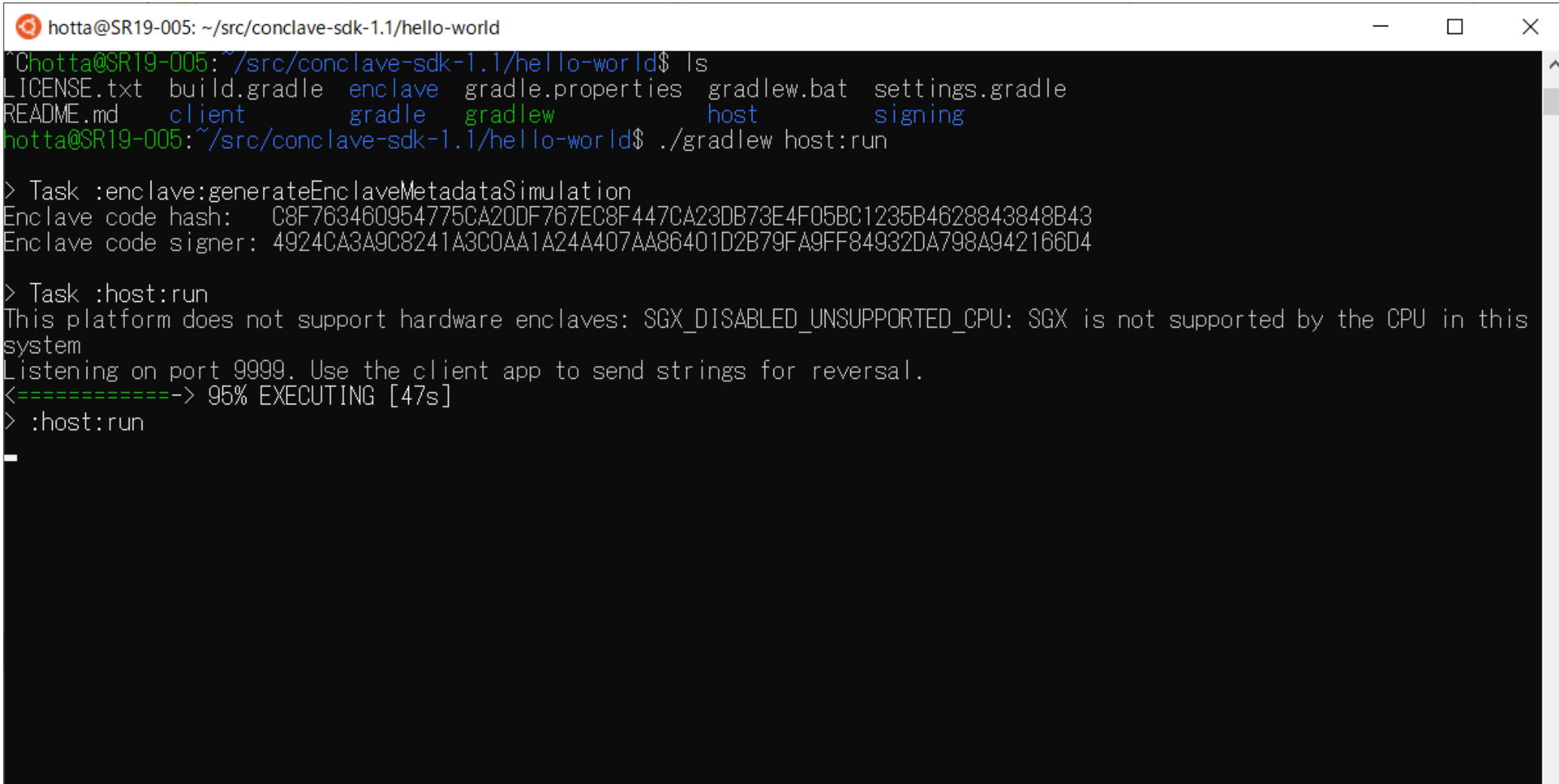


参考 Windows wsl2での
サンプル実行例

Sampleの実行例(Windows WSL2 ubuntu)

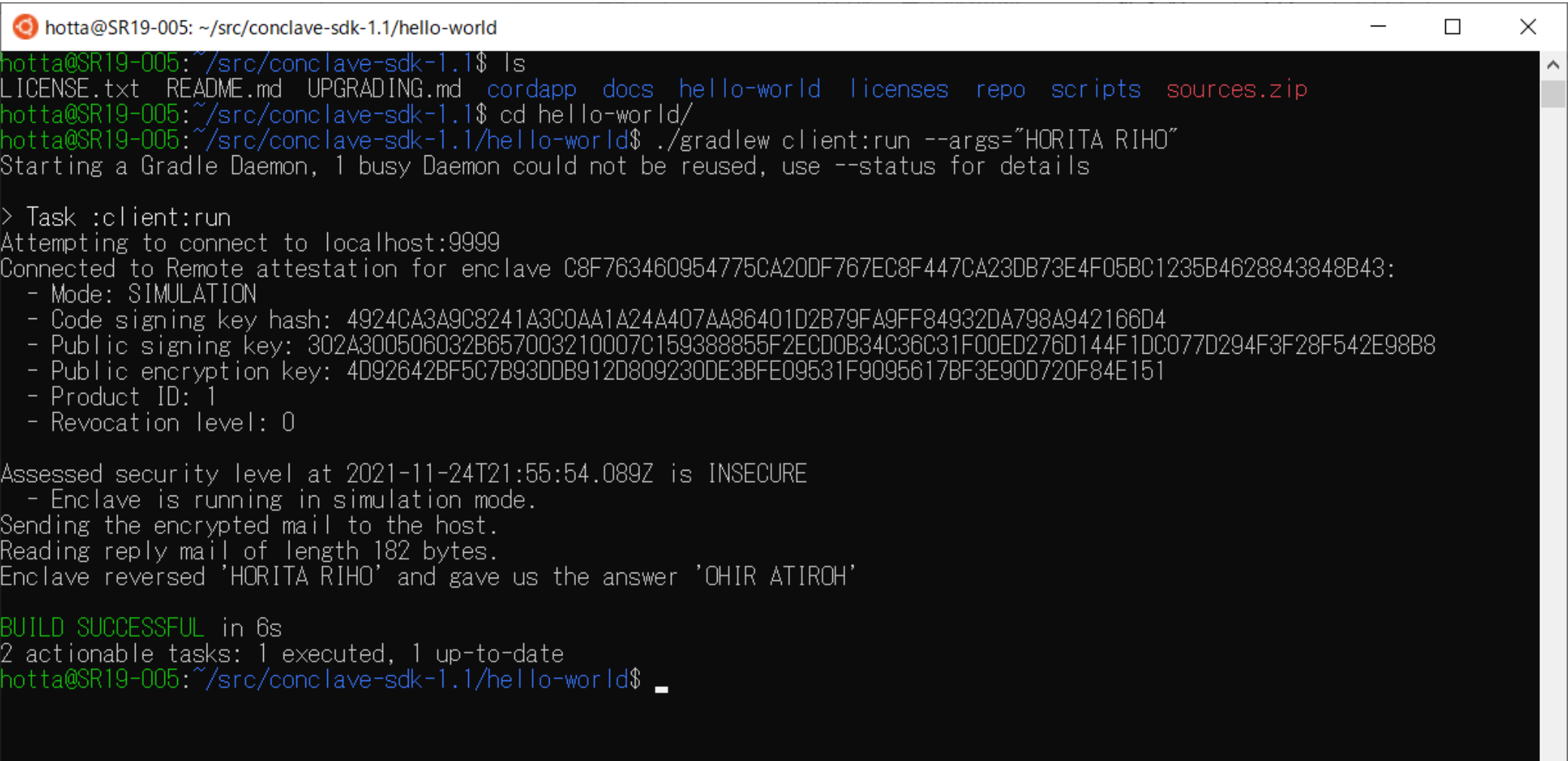
予めOpenjdkとbuild-essentialを入れておきます

Server側の立ち上げ



Sampleの実行例(Windows WSL2 ubuntu)

Client側の実行



Sampleの実行例(Windows WSL2 ubuntu)

server側(client 実行後)