大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

アドバンス・トップエスイー プロフェッショナルスタディ

スマートコントラクトを利用したソフトウェアライセンス認証方式の提案

キヤノン株式会社　前田 泰晴　maeda.yasuharu@mail.canon

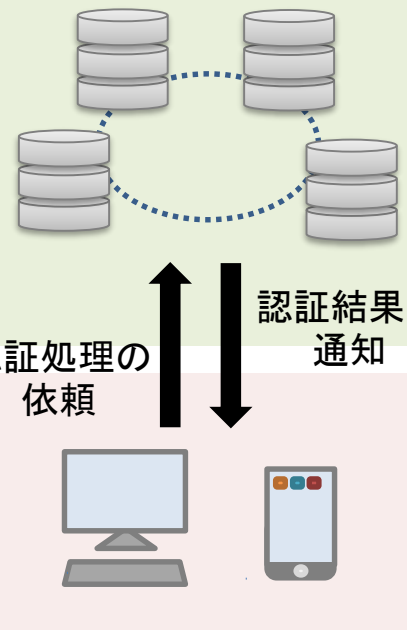
ライセンス認証における問題点

ライセンス認証は、ソフトウェアの不正利用を防止するための手段として重要視されている.
従来手法では認証サーバーを設けることが一般的だが、システムの開発費や維持費がかかる.
また、Blockchainを利用した分散管理方式が提案されているが、認証処理がクライアント側で実行されるため、セキュリティ上の課題が残る.

手法・ツールの適用による解決

スマートコントラクトは分散管理された基盤上で安全にデータベースへの処理を行う技術である. これを利用することで、複数のソフトウェアベンダーにより分散管理された基盤上で、各ベンダーが独自に定義したライセンス認証処理を安全に処理可能となる.
また、提案した手法に関して、処理性能・柔軟性・セキュリティ・コストの観点で評価を行った.

提案手法の概要



サーバー側
- ソフトベンダーにより構成される認証を行うための分散管理DB
- 各社は独自のスマートコントラクトを登録可能
- 認証はスマートコントラクトの実行により行われる.

ユーザー側
- ソフトウェア起動時などにサーバー側へライセンスの認証処理を依頼する

特徴

① ベンダー毎に独自の認証処理をスマートコントラクトに記述可能なため柔軟性の高い認証システムを実現

② 認証処理はサーバー側で処理され、更に認証の実行結果は複数のDB間で検証し合うため高セキュリティ

③ ソフトベンダーが分散管理された認証システムに参画可能な形態をとることで導入にかかるコスト削減を実現

評価

処理性能

分散管理DB構築フレームワークHyperLedger Fabricにて環境を構築して評価を行った.

DBのRead　: **約750[ms]**
DBへのWrite : **約3600[ms]**

⇒ライセンス認証のユースケースではReadがメインとなるため充分な性能と言える.

セキュリティ

ライセンス認証に関わる従来からの課題だけでなく分散管理DB特有の課題を考慮する必要がある

①多数派獲得によるDBの操作
⇒悪意のあるノードが参加しにくいコンソーシアム型にする

②脆弱なスマートコントラクトの記述
⇒記述のガイドラインや、認証クラスの継承による記述

今後の課題

技術的な課題

- ライセンス認証に関わる従来からの課題の根本的な解決方法の検討が必要（ライセンスキーの複製, コード改竄, etc）

運用上の課題

- 認証システムを運営する組織間でのシステム権限、ユーザー数、サーバーのスペックの差による不公平の解消