スマートコントラクトによる招待付きオンラインストレージのアクセス制御

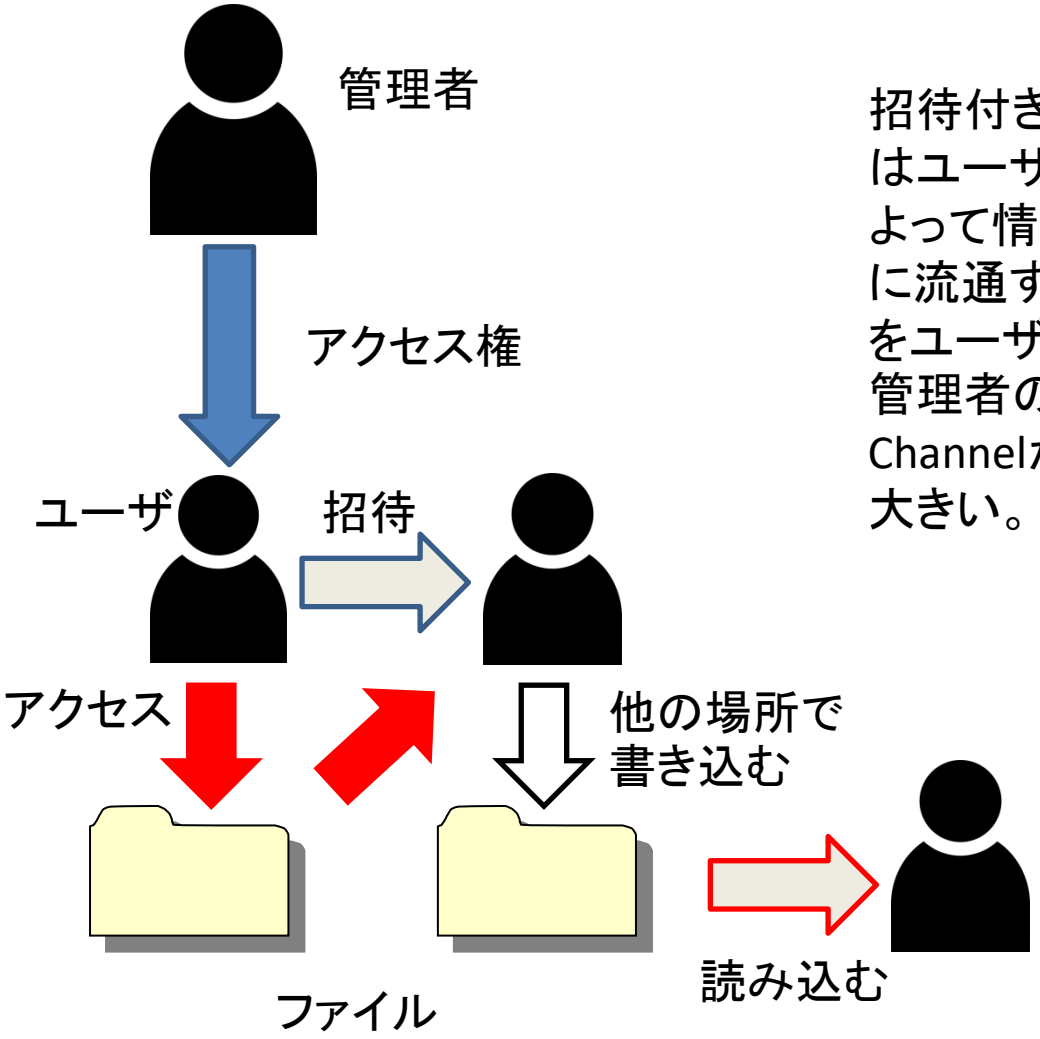
201503894
関根有紀

背景

- 近年、ownCloudやiCloudなどのオンラインストレージの利用が多くなり、扱う情報量が増加している。

- オンラインストレージの招待機能はファイルに対して複数のユーザのアクセスを許可するため意図しない情報漏洩であるCovert Channelが発生する可能性がある。

問題



招待付きオンラインストレージはユーザを招待することによって情報が他のユーザ間に流通するようなアクセス権をユーザ設定で可能なため管理者の意図しないCovert Channelが発生する可能性が大きい。

スマートコントラクト

- 契約内容をブロックチェーンに記録することで契約内容と履行を保証
- 契約内容
  - 契約を履行させる条件(日時など)
  - どのように履行するかを記述したコントラクトコード(仮想通貨で借金返済など)

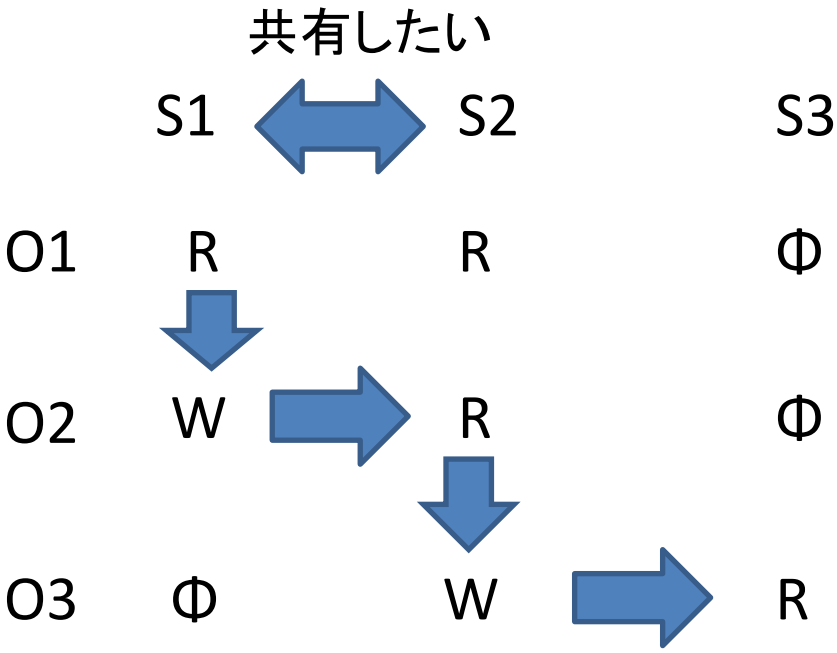
目的

- 招待によって起こる第三者への情報漏えいを防ぎ、アクセス権の変更をスマート コントラクトを用いて自動化することを目的とするシステムを提案する。
- Covert Channel分析を行い、招待された人のアクセス権をどのように変更するのかコントラクトコードにプログラミングし、自動的に変更できるようにする。
- そしてブロックチェーンにコントラクトコードを埋め込む。

オリジナリティ

- Covert Channelが発生する可能性がある条件を満たしたら、スマートコントラクトによって相手のACLを自動的に変更する。
- スマートコントラクトによってアクセス権を変更するシステムには、ブロックチェーンのシステムが使われている。
- したがって管理者が不要にもかかわらずユーザ間 で自由に情報共有の招待をし、かつ安全に情報共有することが可能である。

招待付きオンラインストレージにおける Covert Channel（例）



S1がO1を読み込む

S1がO1で読み込んだ情報をO2に書き込む

S1がS2を招待してS2は招待を受け入れる

S2がO2を読み込む

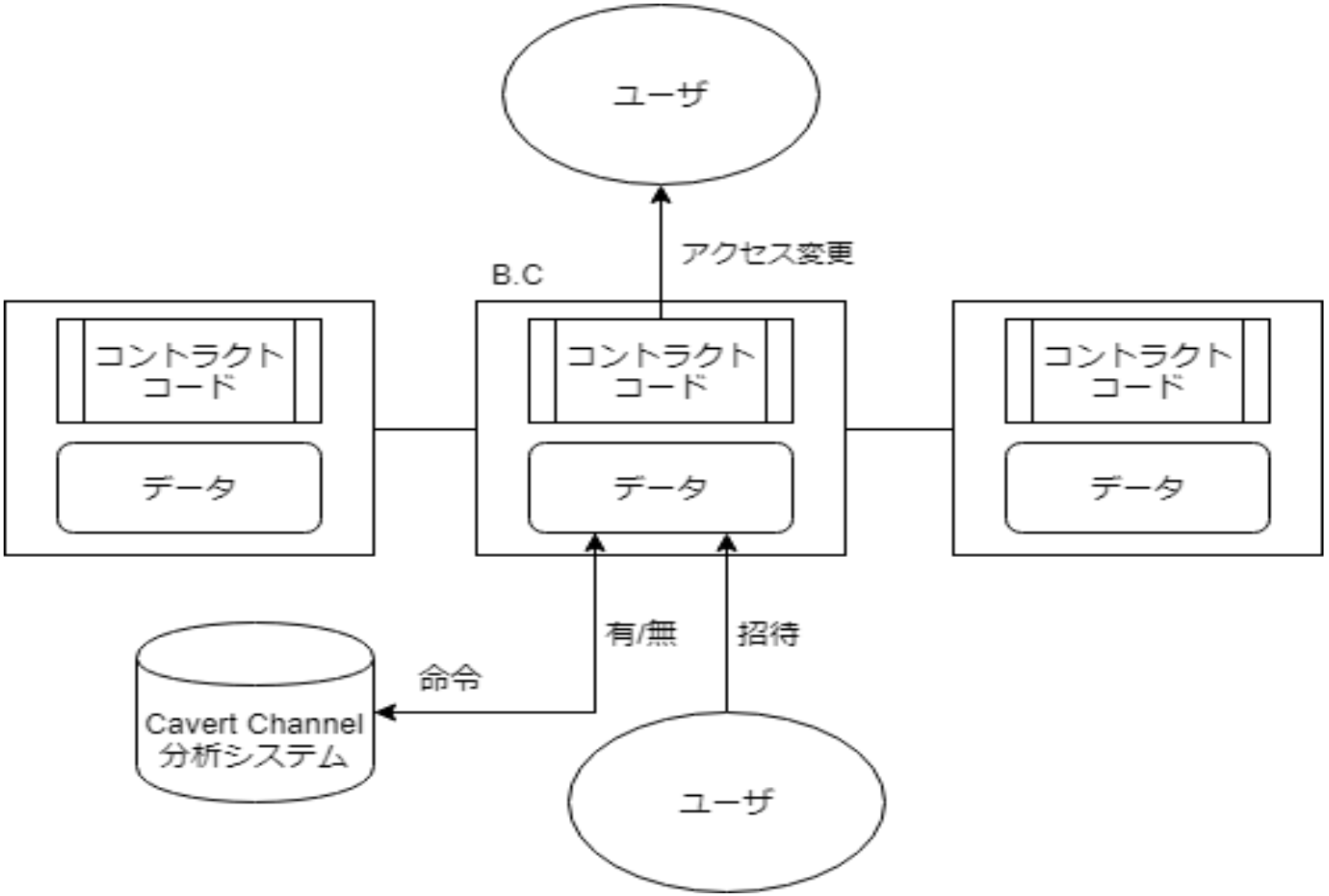
S2がO2で読み込んだ情報をO3に書き込みS3がO3を読み込む

S1がS2を招待したことで知らない間にS3がO1の情報を見ることが出来てしまう。

Covert Channelを防ぎたい

提案

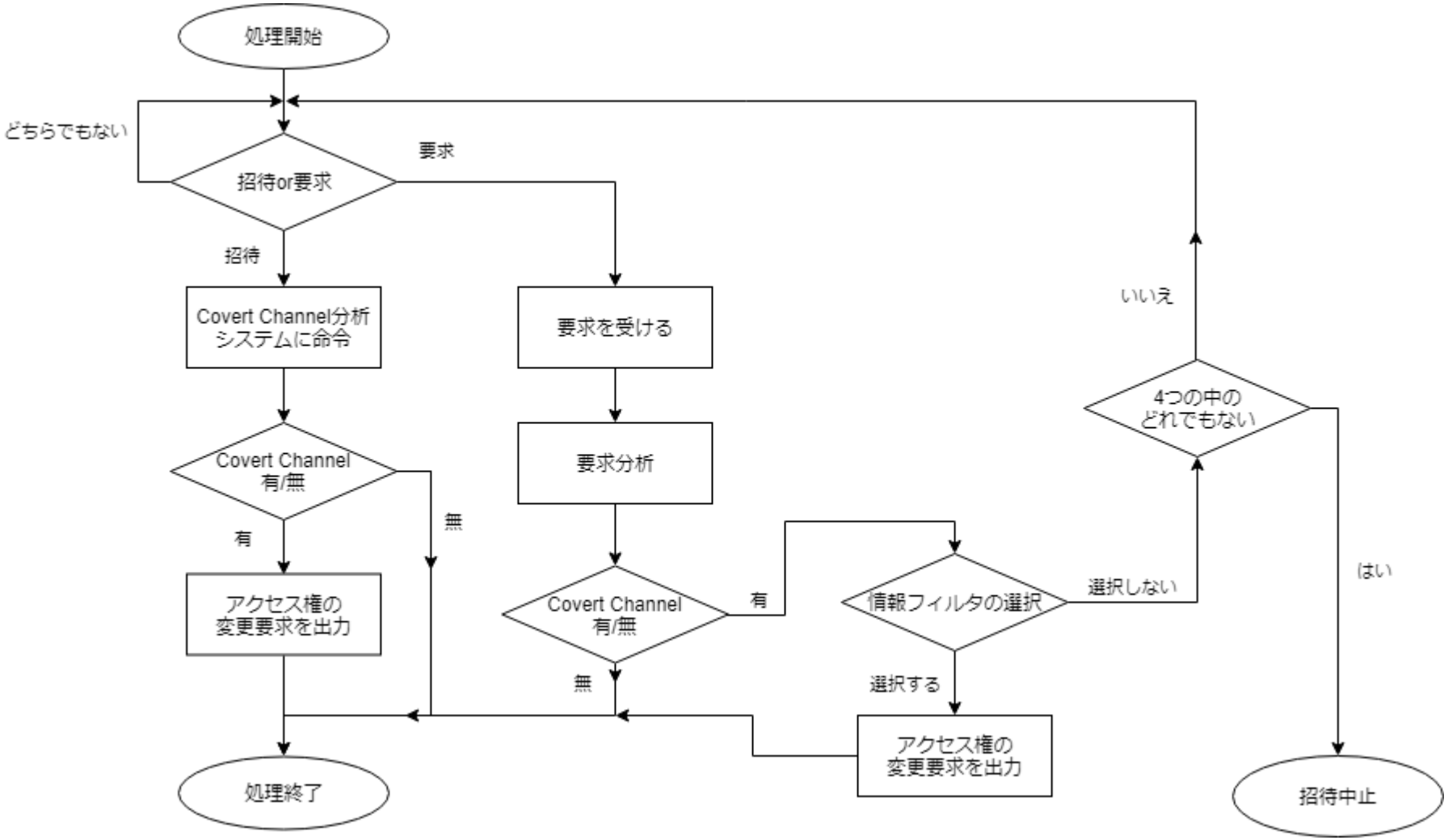
招待付きオンラインストレージにおける コントラクトコードとブロックチェーンの概要



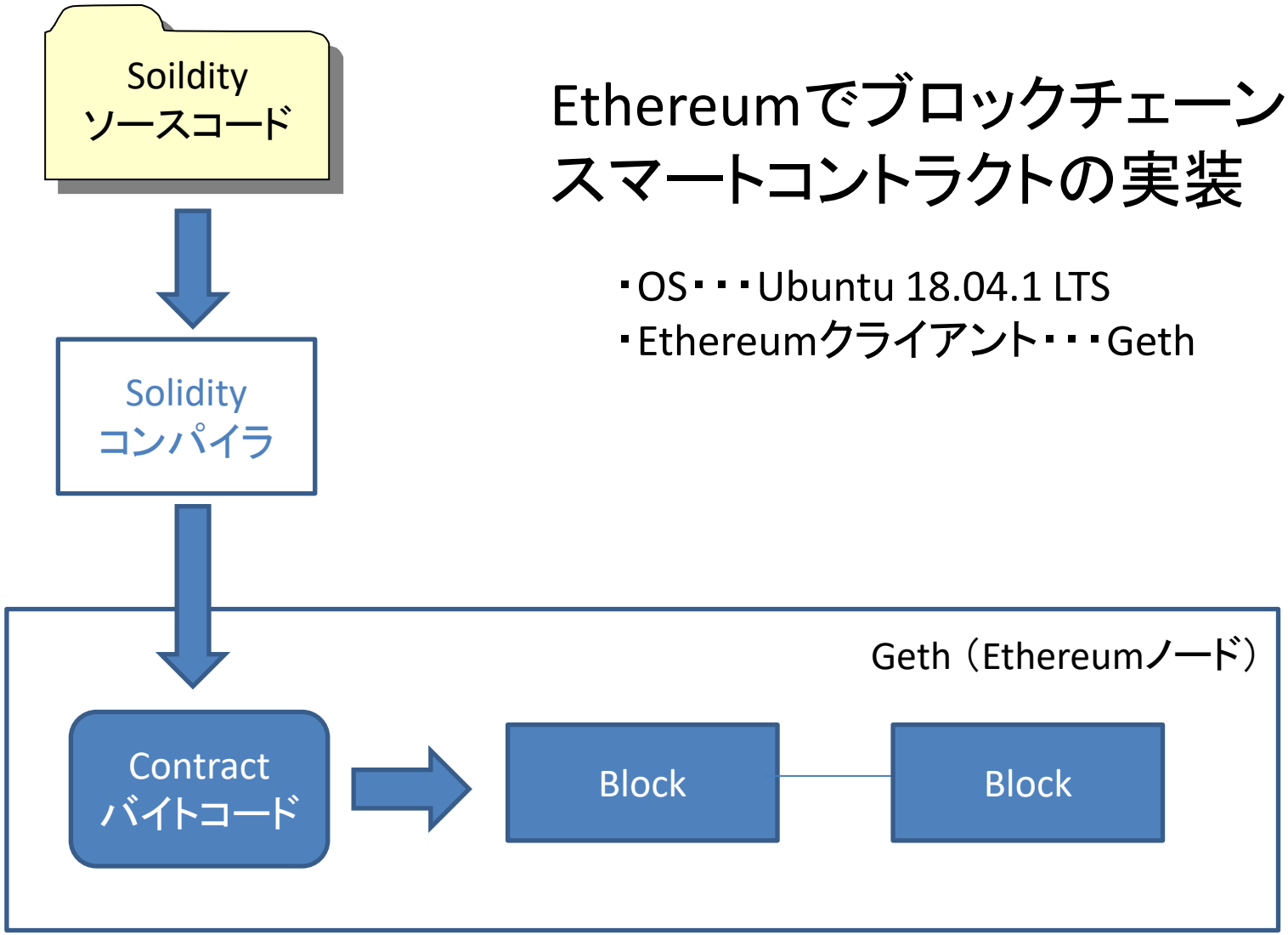
使用するコントラクトコード

- コントラクトコード1
  - 条件：招待した時
  - 実行する内容： Covert Channelを分析してその可能性があるならアクセス権を変更する
- コントラクトコード2
  - 条件： Covert Channelが発生した時
  - 実行する内容： Covert Channelを分析してその可能性があるならアクセス権を変更する

コントラクトコードのフローチャート



実装環境と
スマートコントラクト実行までの流れ



Ethereumでブロックチェーンと
スマートコントラクトの実装

・OS・・・Ubuntu 18.04.1 LTS
・Ethereumクライアント・・・Geth

まとめ

- 本研究では、招待によりCovert Channelが発生する可能性がある場合、それを 防ぐために招待されたユーザのアクセス権を変更し、スマートコントラクトで自動化するシステムを提案した。
- ブロックチェーンを利用することでユーザが互いに共有して利用者の不正、改ざん、によって発生する情報漏えいを防ぐことができ、健全性も証明することができる。

課題

- コントラクトコードのフローチャートを基にプログラムの作成
- スマートコントラクトを実行するのに時間がかかってしまう。