

## 統一的・厳密なライセンス

License as Code (LaC)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software ...

```
{
  "BY": true,
  "NC": false,
  "SA": true,
  "ND": false,
}
```

機械的な検証が可能に！

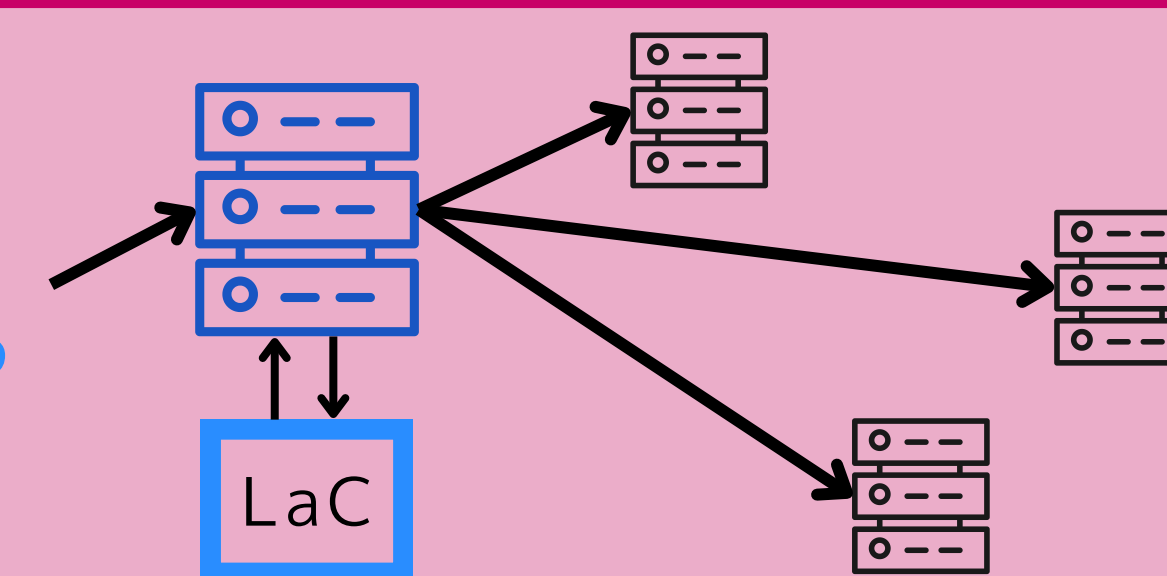
※もう少し自由度がほしい

## 「伝播・保存」で参加する裁判

Gossipsub・SPoRA・自己検閲

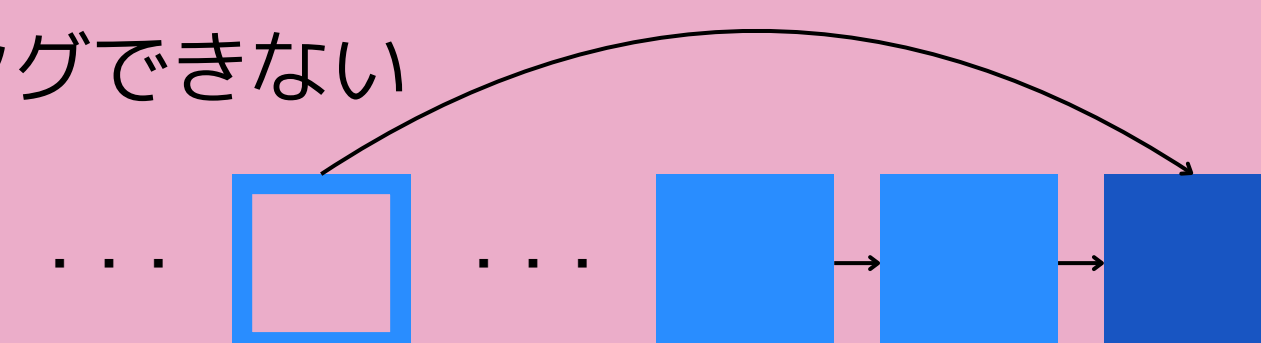
### Gossipsub

- 役割: P2P通信
- 伝播ロジックにLaC検証が含まれる
  - LaC検証が通れば伝播



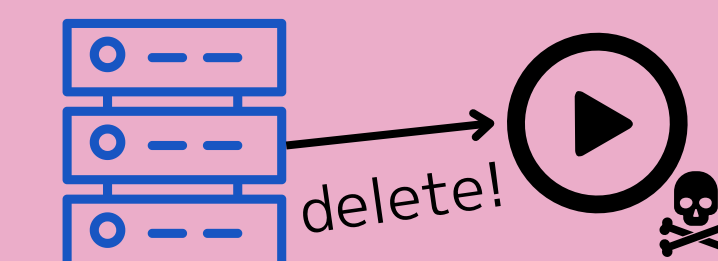
### SPoRA

- 役割: マイニング
- 過去データがないとマイニングできない (長期保存奨励)



### 自己検閲

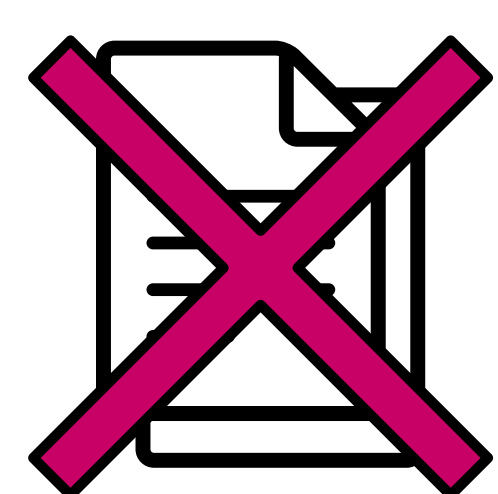
- 違法コンテンツ
- ライセンス未履行
- ノードが個々に判断して削除可能



## ライセンスをあらゆるジャンルへ

KE<Y/I>の世界観

「どこまで大丈夫...？」  
→ 毎回聞く必要がある  
→ 不安・手間



否認

許可

「ここまでなら大丈夫」がはっきり

→ 安心感

→ OO文化の  
改変の促進へ...

License as Codeがもたらす  
創作の系譜と安心感



# KE<Y/I>

# aL1sCTF

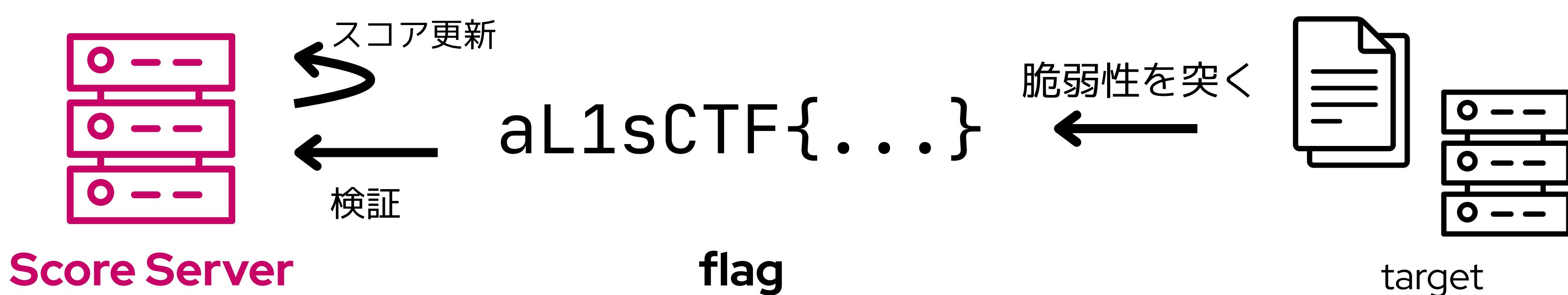


開発駆動コース仲山ゼミ 34Dn 松浦睦空

CTF Score Server,

## but "Unstoppable"

### What's CTF?



Score Server

aL1sCTF

安定稼働の難しさ

インフラ班から  
悲鳴が...

クラウドは高い...

ブロックチェーン  
→ 単一障害点が0

保守作業いらず！

圧倒的な可用性

理論上止まらないCTFが開催可能!!

### What's Blockchain?

ブロックチェーン  
= 分散データベース

透明性

改ざん困難

全体がダウンしない



ゼロ知識証明でも  
「爆速」なフラグ提出

### Poseidon

- ゼロ知識証明特化のハッシュ関数
- SHA-3から切り替え
- 制約数15分の1

### Arkworks

- Rustのゼロ知識証明ライブラリ
- Wasm・並列化でブラウザでも爆速

Suiチェーンの高速性を  
活かした運用

Sui → 高速・安価な運用へ

	Sui	Solana
処理速度 (理論値)	297,000 Tx/s	65,000 Tx/s
手数料 (ガス代)	¥0.2398	¥0.6059

※2026-01-26の平均ガス代

※Solana...  
Suiと同じく、  
Ethereumと比べて  
高速・安価で  
知られるチェーン

ゼロ知識証明を用いた  
「セキュア」なフラグ提出

オンチェーンでFlagそのものを検証  
→ 透明性が仇となってFlag大公開

ゼロ知識証明なら...?

「aL1sCTF{...}」  
...を知っている ことだけ  
暗号的に証明

※制約数...  
ゼロ知識証明でいう  
プログラムの大きさ  
小さいほど証明が速くなる

### 証明速度

ゲーミングPC	105ms
iPhone 16	130ms
Rakuten Hand	500ms

数年前のハードでも難なく動作！