


研究背景 | Society 5.0

第五期科学技術基本計画 [1] にて Society 5.0 が策定

- 現実空間から**センサー**と **IoT** を通じてあらゆる情報が集積 (= **ビッグデータ**)
- **AI** がビッグデータを解析し、高付加価値を**現実空間にフィードバック**



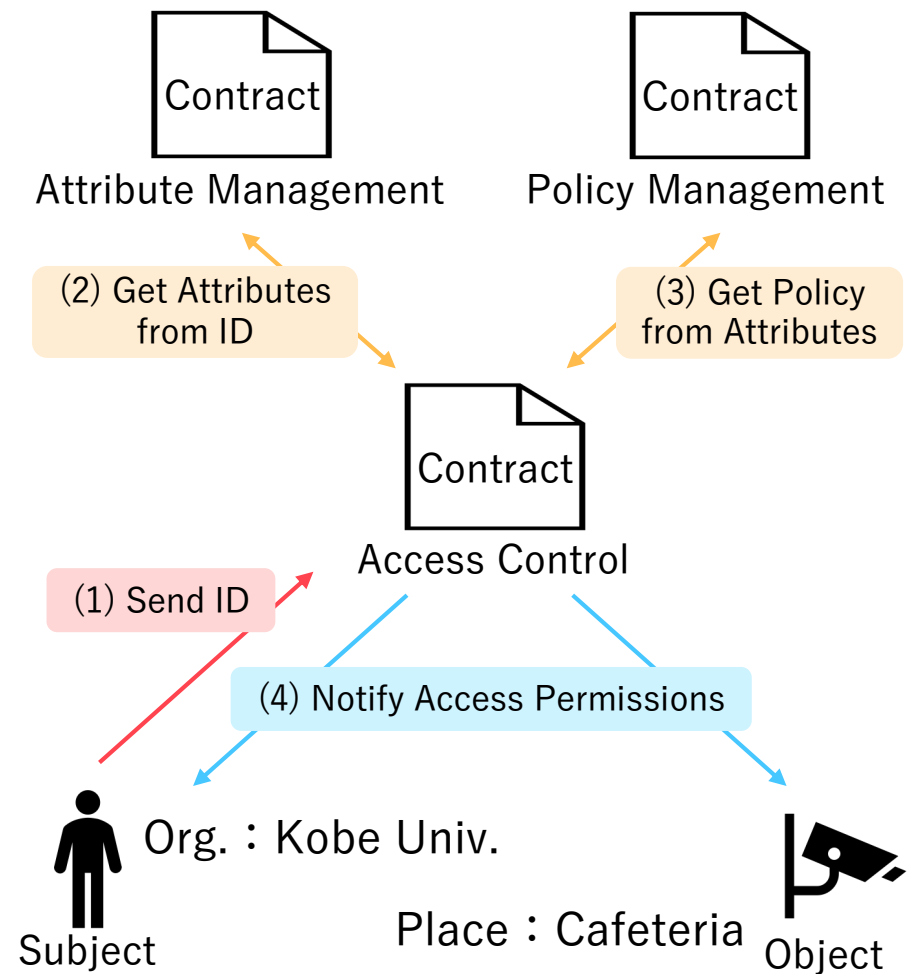
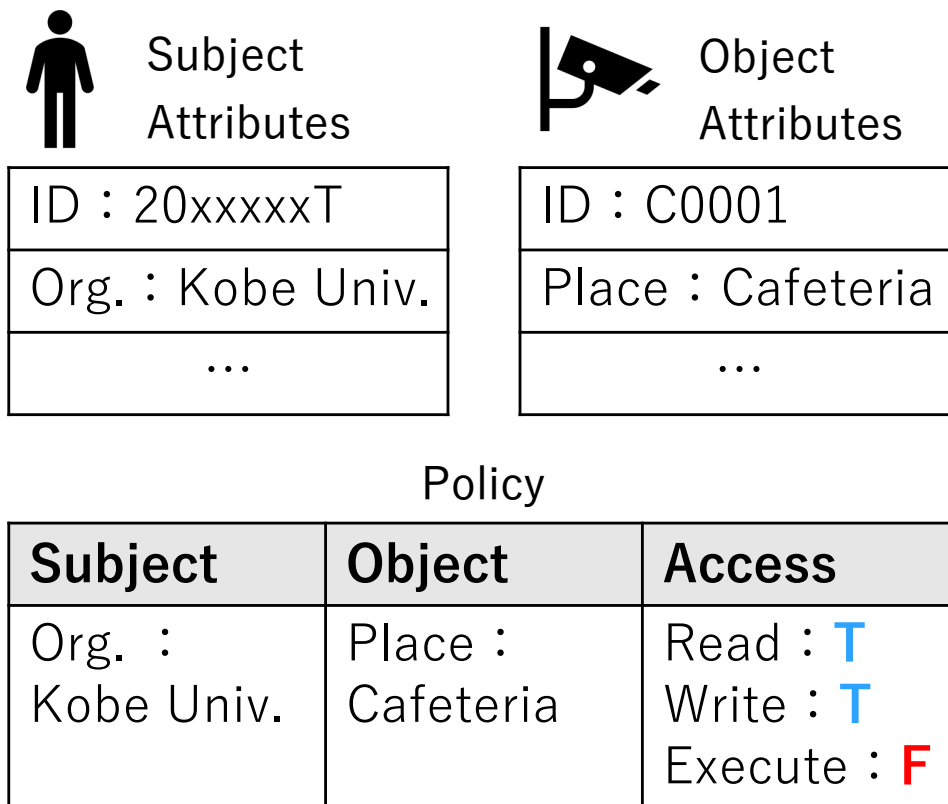
センサー, IoT への**アクセス制御**による
操作や情報閲覧の**権限管理が重要**

[1] 内閣府. “第五期科学技術基本計画.” (2016), [Online]. Available: <https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf>

研究背景 | Attribute-Based Access Control (ABAC) への Blockchain の応用

■ ABAC :

- 大規模 IoT ネットワークなどに採用
- 属性情報で構成される
規則（**ポリシー**）によりアクセス制御



研究背景 | Attribute-Based Access Control (ABAC) への Blockchain の応用

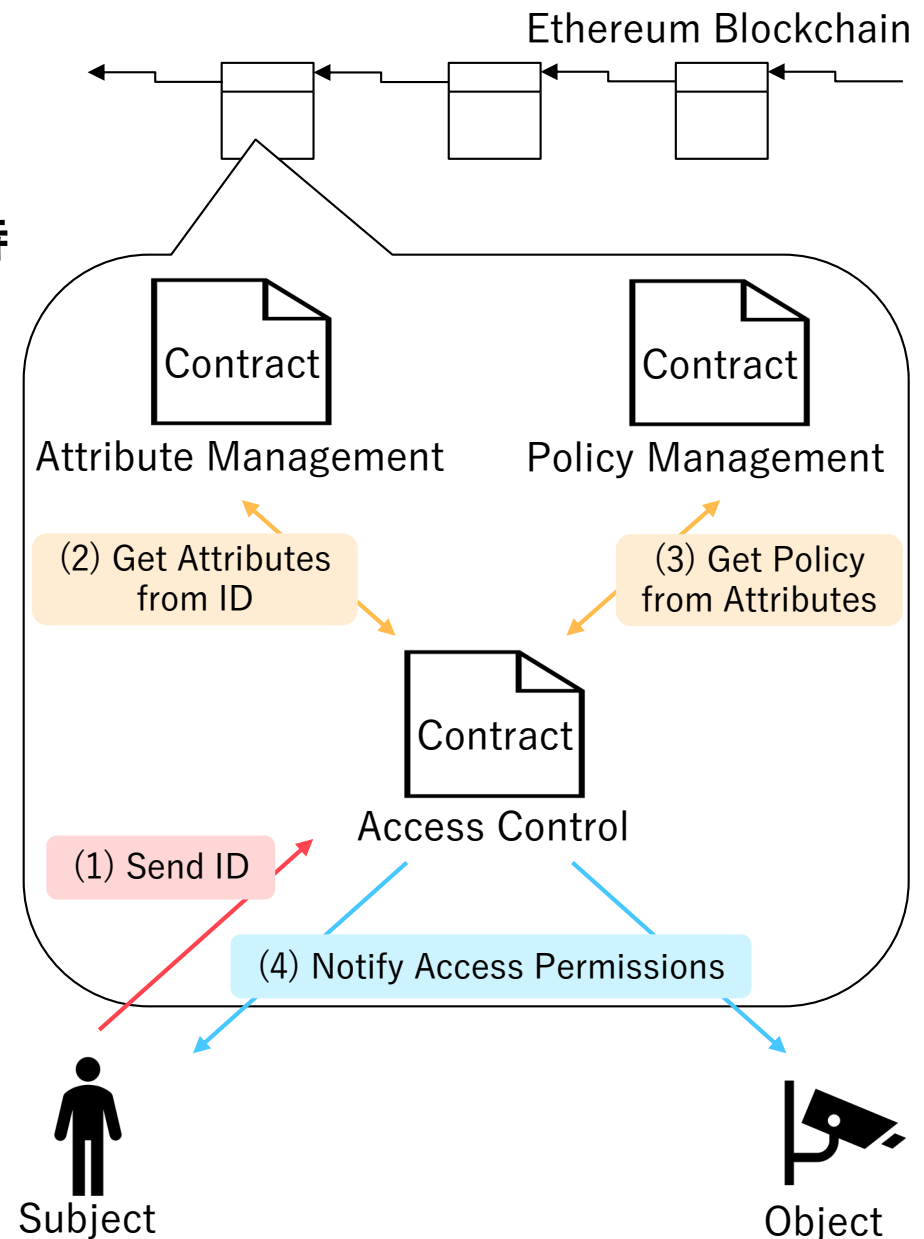
■ Blockchain 応用 [2] の利点

- ・ 参加ノードがシステムデータを保持
- ・ 互いにデータの整合性を維持
 - └ 単一故障の回避
 - └ 改ざんへの堅牢性の高さ

■ Blockchain 応用の問題点

- ・ OPCODE に **GAS (手数料)**

→ 保持するポリシーの量と
ポリシー検索コストとの関係は？



[2] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2018.

課題 | ABAC への Blockchain 応用に際した ポリシー検索の改善

Policy	Subject	Object	Access
	Org. : Kobe Univ.	Place : LR	Read : T Write : T Execute : F

従来手法 [3] : ポリシー検索に**線形探索**を採用

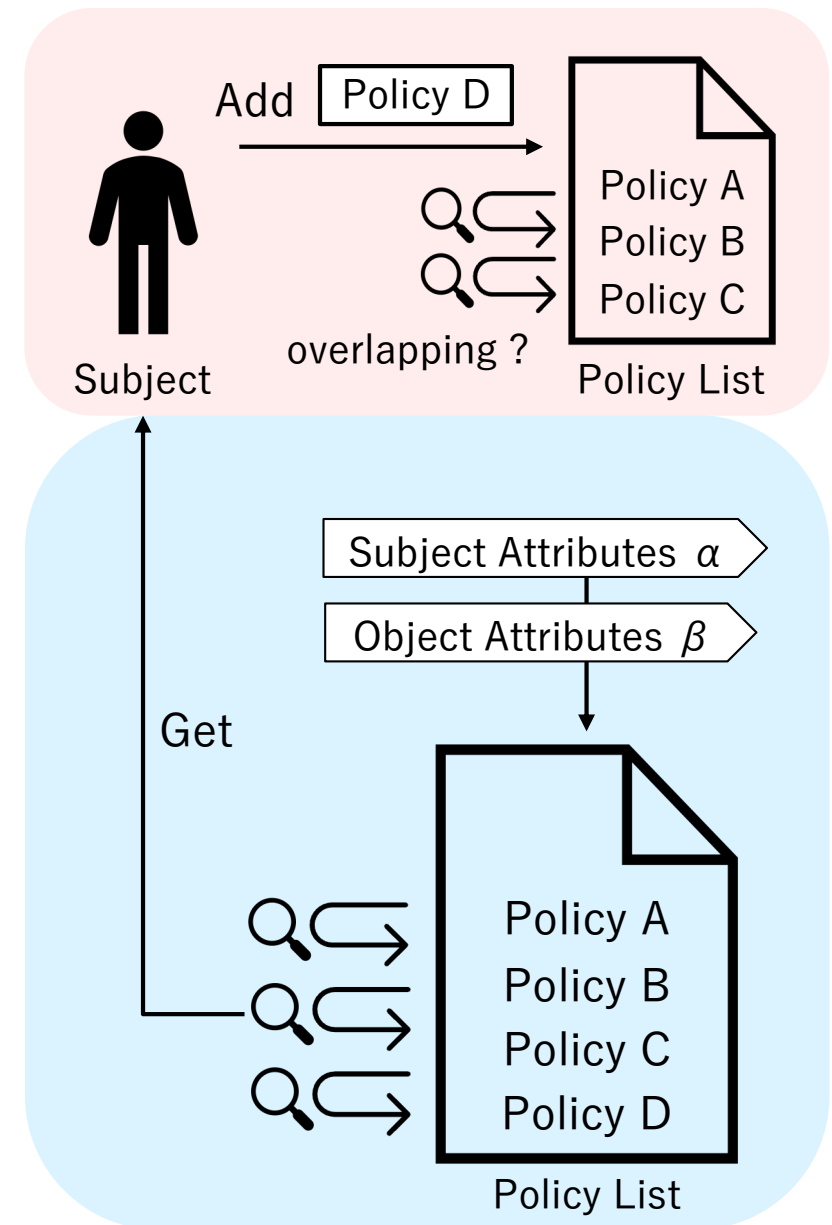
→ ポリシー数増加に伴って

GAS (手数料) ・ 実行時間は増加

課題 : GAS, 実行時間の**削減**

1. 新規ポリシー追加時の包含判定

2. 属性情報をキーとしたポリシー探索



[3] Y. Zhang, M. Yutaka, M. Sasabe, and S. Kasahara, "Attribute-based access control for smart cities: A smart-contract-driven framework," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6372–6384, 2020.

GAS・実行時間削減のポイント

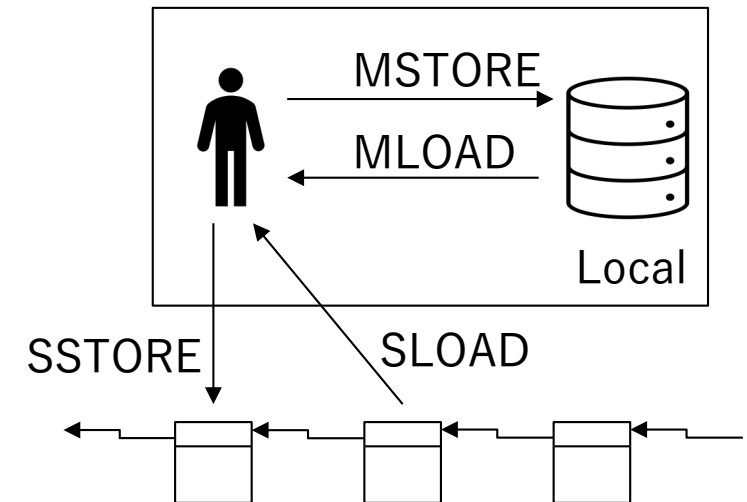
Blockchain 上のデータを操作するOPCODE

◆ Blockchain からの読み込み **SLOAD**

◆ Blockchain への書き込み **SSTORE**

はローカルのメモリ領域上で動作する

OPCODE より **GAS** (手数料) が大きい



OPCODE	GAS
<u>MLOAD</u>	3
<u>MSTORE</u>	3
SLOAD	2,100
SSTORE	5,000~20,000

挿入，検索について

計算量と Blockchain 操作を減らすことが重要

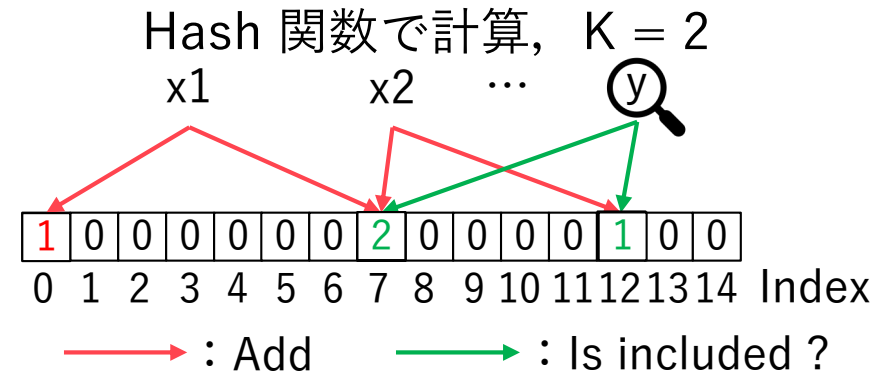
Add using Counting Bloom Filter (ACBF) 方式

課題 1：新規ポリシー追加時の包含判定の改善

Counting Bloom Filter (CBF)

- 要素の包含判定が $O(K)$
- 偽陽性のみ存在する

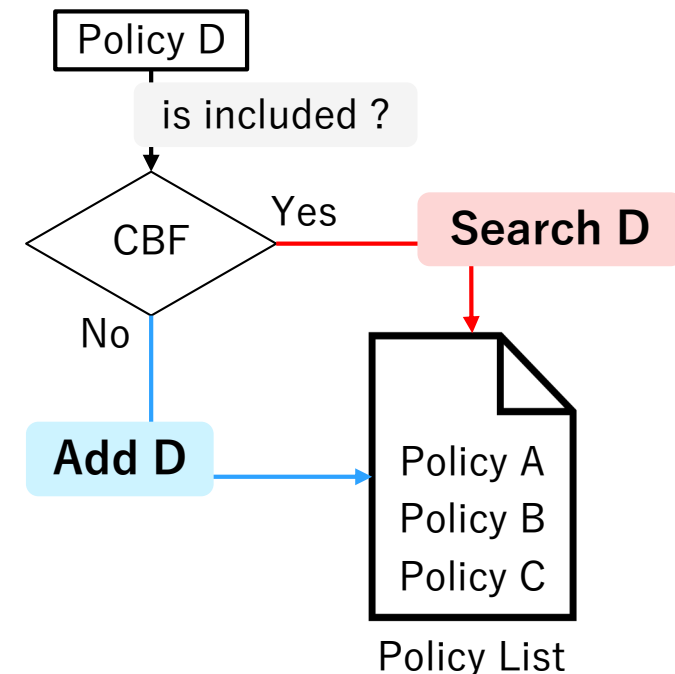
K : Hash関数の数



ACBF 方式

- 追加ポリシーを CBF で包含判定
- $O(K)$ でポリシーを追加
- SLOAD は K 回
- SSTORE は $K + 1$ 回

定数 K に従ってポリシーの追加が可能

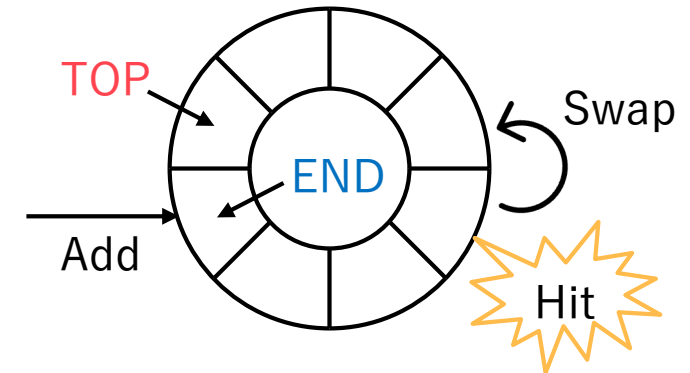


Get using Ring Buffer (GRB) 方式

課題 2：属性情報をキーとしたポリシー探索

Ring Buffer (RB)

- キャッシュとしての役割を果たす
- 要素 Hit 時は，先端側へ要素を一つ移動
… 消費 GAS が大きい~~ため~~，LRU ではない
→ 参照頻度が高いポリシーを再参照できる



GRB 方式

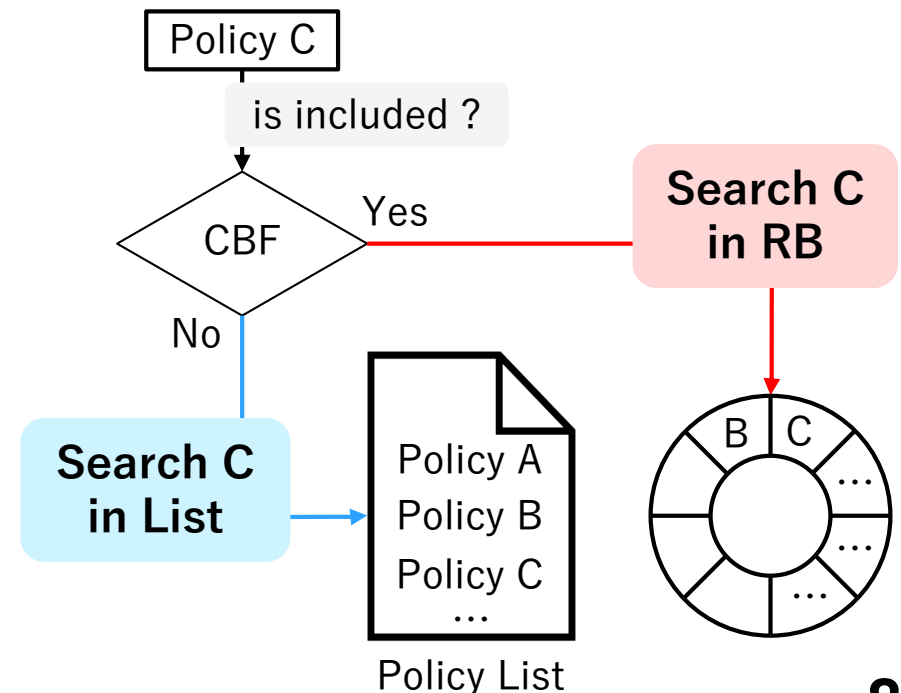
- キャッシュにより，再参照を容易に
- $O(B)$ でポリシーを検索
- SLOAD は $B + K$ 回
- SSTORE は $K + 1$ 回

Hit 時に

定数 B ， K に従ってポリシーを取得

B ：バッファサイズ

K ：Hash関数の数

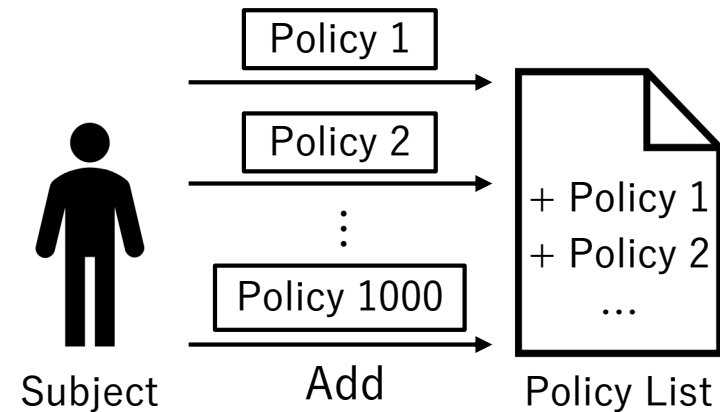


ACBF 方式

□ 評価シナリオ

➤ 1000 回ポリシーを逐次追加する

→ 保持ポリシー数が**増加していく**

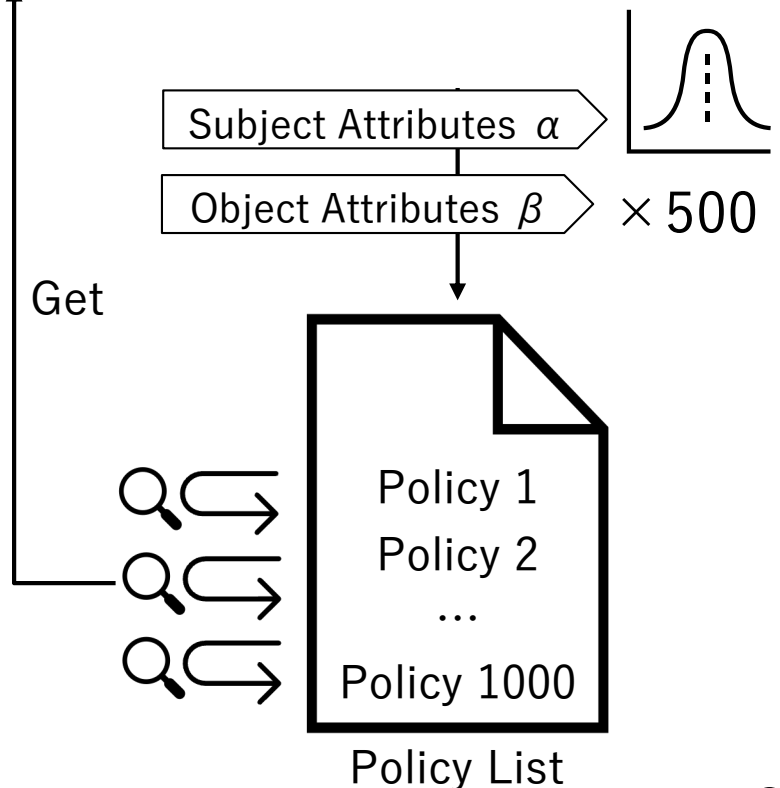


GRB 方式

□ 評価シナリオ

➤ 1000 個のポリシーから正規分布に従ってポリシーを 500 個取得する

→ 参照頻度が高いポリシーが存在



□ 実験環境

◆ MacBook Air Mac OS 14.3

結果 | Add using Counting Bloom Filter

□ 評価シナリオ

- 1000 回ポリシーを逐次システムへ追加する
- $K = 7$ (偽陽性率の最小化より)

K: Hash関数の数

□ 評価方式

- Policy Management Contract (PMC)
 - └ 線形探索を採用. 先行研究での提案手法 [3]
- Add using Counting Bloom Filter
 - └ 提案手法

追加回数	GAS (手数料) (10^5)		実行時間 (s)	
	先行研究	ACBF	先行研究	ACBF
1	2.3	4.2	0.049	0.99
100	7.0 $\div 1.9$	3.6	0.63 $\div 6.3$	0.10
500	27 $\div 7.5$	3.6	2.5 $\div 23$	0.11
1000	54 $\div 15$	3.5	6.7 $\div 67$	0.10

追加回数の増加に伴い GAS・実行時間を ACBF は 先行研究 より **削減**

ACBF は追加回数に関係なく GAS・実行時間がほぼ **一定**

[3] Y. Zhang, M. Yutaka, M. Sasabe, and S. Kasahara, "Attribute-based access control for smart cities: A smart-contract-driven framework," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6372–6384, 2020.

結果 | Get using Ring Buffer

□ 評価シナリオ

- 1000 個のポリシーから
正規分布に従ってポリシーを
500 個取得する
- $B = 500$ B : バッファサイズ

□ 評価方式

- **Access Control Contract (Acc)**
 - └ 線形探索を採用. 先行研究での提案手法 [3]
- **Get using Ring Buffer**
 - └ 提案手法

標準偏差	累積 GAS (手数料) (10^9)			累積実行時間 ($s \times 10^3$)		
	先行研究		GRB	先行研究		GRB
10	2.6	$\div 6.2$	0.42	3.5	$\div 4.0$	0.87
50	2.7	$\div 2.3$	1.2	3.7	$\div 1.5$	2.4
150	2.9	$\div 1.5$	2.0	3.7	$\div 1.3$	2.7

GAS・実行時間を GRB は 先行研究 より **削減**

GRB は参照頻度が高いポリシーが多いほど GAS・実行時間を **削減**

[3] Y. Zhang, M. Yutaka, M. Sasabe, and S. Kasahara, "Attribute-based access control for smart cities: A smart-contract-driven framework," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6372–6384, 2020.

結果 | 実際のコスト (ACBF 方式)

$$\text{Cost} = \text{GAS} \times (\text{Base fee} + \text{Priority fee})$$

Ethereum では,

Base fee = 20, Priority fee = 1 (2/27 現在)

□ ACBF 方式

追加回数	先行研究 (GAS)	ACBF (GAS)	先行研究 (円)		ACBF (円)
1	2.3	4.2	2,033		3,713
100	7.0	3.6	6,021	- 2,838	3,183
500	27	3.6	23,874	- 20,691	3,183
1000	54	3.5	47,748	- 44,654	3,094

($\times 10^5$)

結果 | 実際のコスト (GRB 方式)

$$\text{Cost} = \text{GAS} \times (\text{Base fee} + \text{Priority fee})$$

Ethereum では,

Base fee = 20, Priority fee = 1 (2/27 現在)

□ GRB 方式

標準偏差	先行研究 (GAS)	GRB (GAS)	先行研究 (円/回)		GRB (円/回)
10	2.6	0.42	42,106	- 34,679 →	7,427
50	2.7	1.2	47,748	- 26,527 →	21,221
150	2.9	2.0	51,285	- 17,432 →	33,853

($\times 10^9$)

今後の課題

◆ 依然として GAS は高い

→ 手数料の低い Blockchain をレイヤー構造に導入したフレームワークの提案

Point

セキュリティ面と手数料・スケーラビリティとのトレードオフを考慮する必要がある

まとめ

■ 目的

- ◆ Blockchain ベース ABAC フレームワークに関する
ポリシー検索コスト・実行時間の削減

■ アプローチ

- ◆ CBF を用いた包含判定 による**ポリシー追加**：ACBF
- ◆ CBF, RB を用いた参照頻度を考慮した**ポリシー取得**：GRB

■ 結果

- ◆ ACBF：**定数に従った** GAS・実行時間でかつ**改善**
- ◆ GRB：参照頻度が高いほど GAS・実行時間の**改善**

■ 今後の課題

手数料の低い Blockchain を**レイヤー構造**に導入した
フレームワークの提案