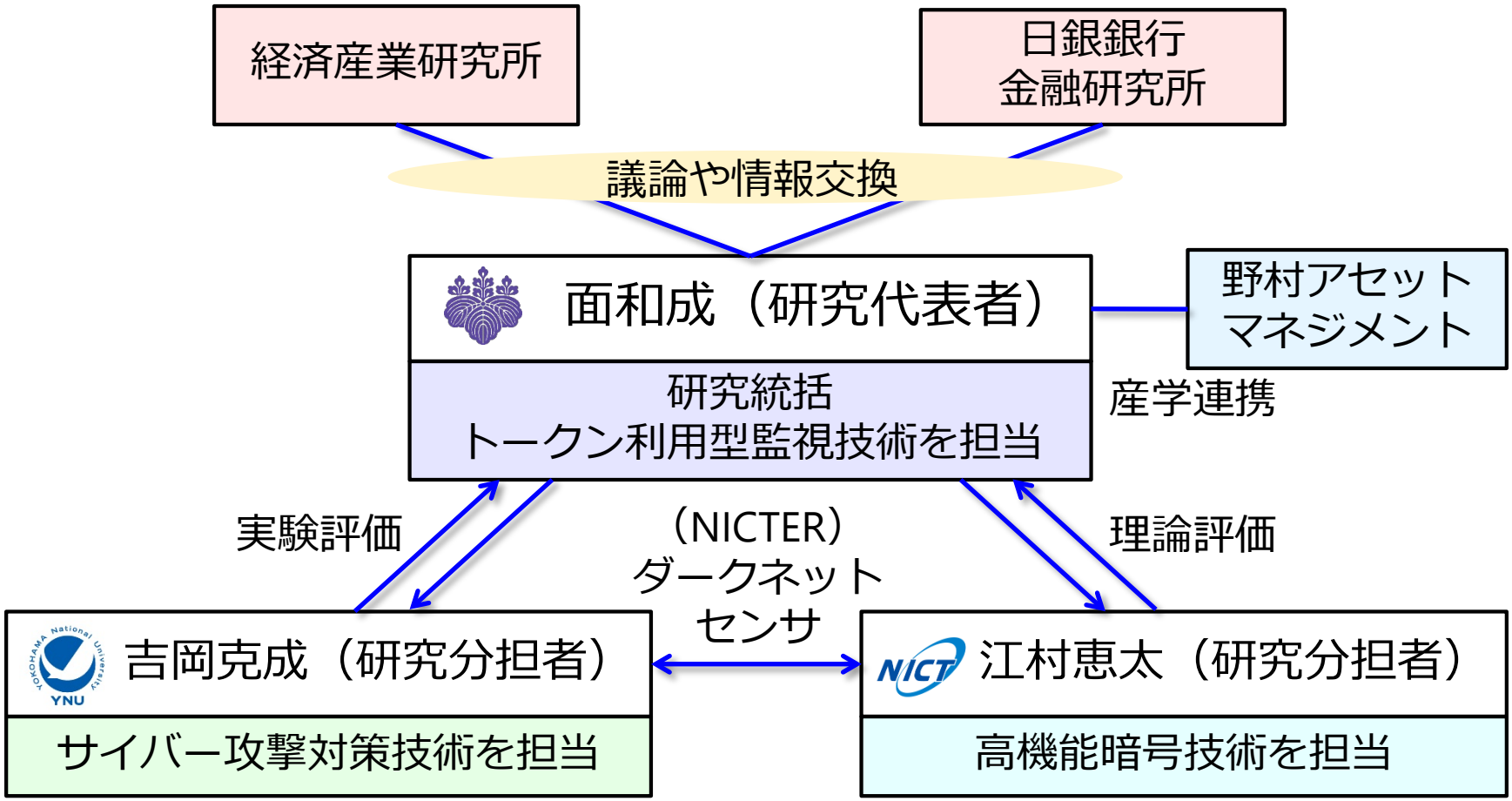
ブロックチェーンに関するセキュリティ研究活動2020

筑波大学システム情報系
面 和成
omote@risk.tsukuba.ac.jp

オンライン会場（Microsoft Teams）
2020年9月25日

BSEC研究会の背後にある研究体制



科学研究費補助金 基盤研究(B)，「ブロックチェーンを基盤とする高信頼性を持った自律分散型監視技術」(19H04107)

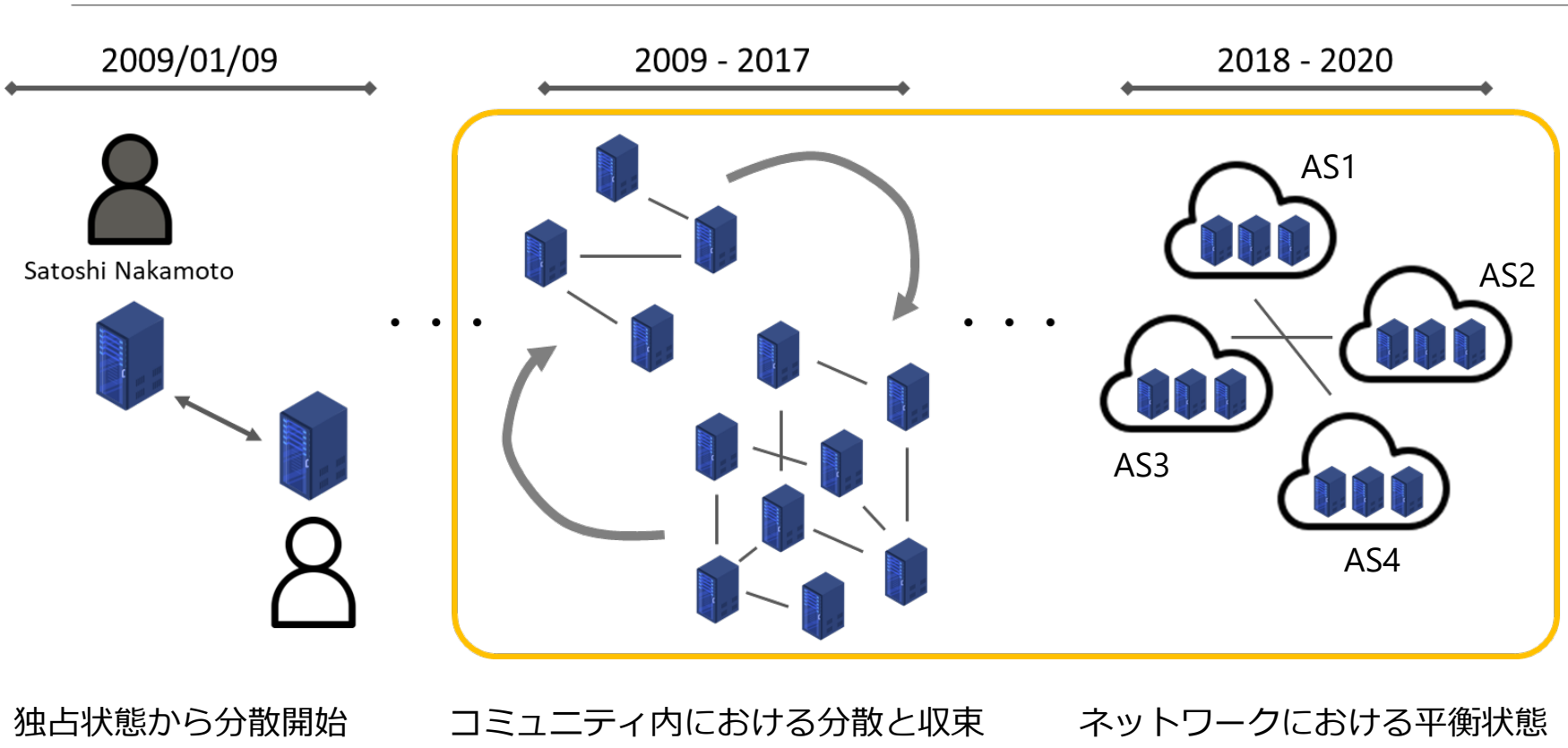
本発表の内容

- ブロックチェーンに関する最近のセキュリティ研究
  - ブロックチェーンの安全性評価
    - Topic 1. ブロックチェーンネットワークの再中央集権化
  - ブロックチェーンを適用した安全なシステム構築
    - Topic 2. ブロックチェーンを用いたIoT機器ファームウェア配布手法
- まとめ

Topic 1：
ブロックチェーンネットワークの再中央集権化
（ブロックチェーンの安全性評価）

ブロックチェーン (Bitcoin) の構造の変化

※AS (Autonomous System) とは，ある一つの管理主体によって保有・運用されている独立したネットワーク



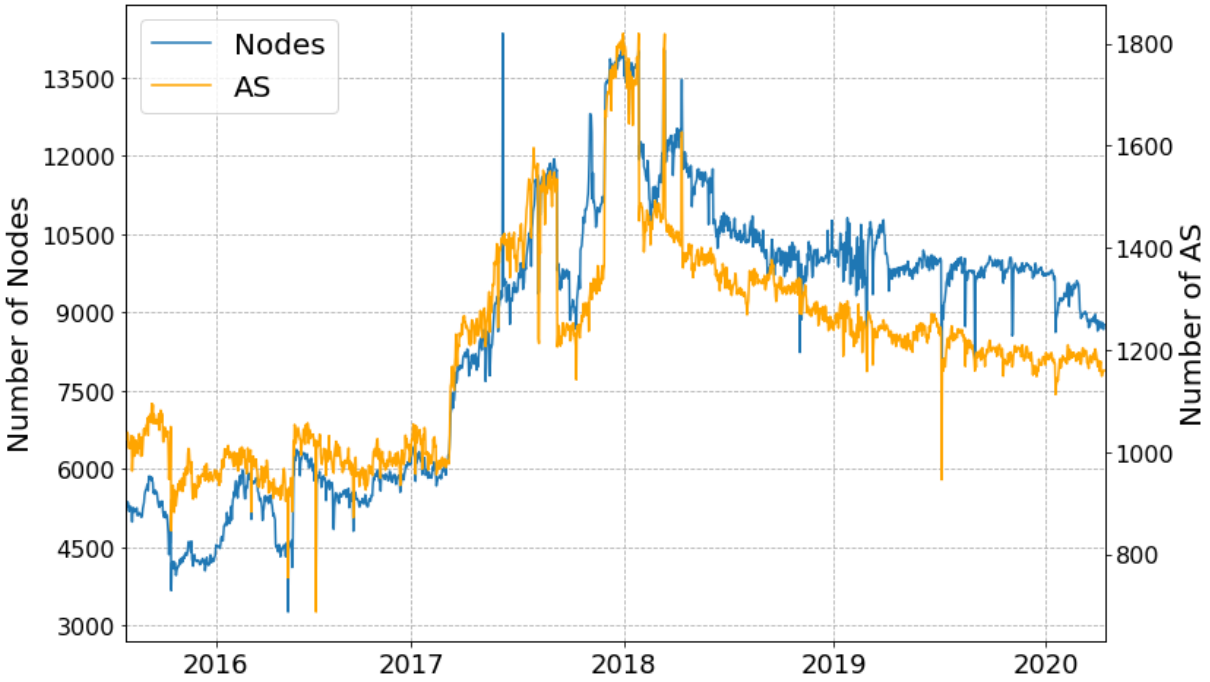
[IO20] 今村, 面,「ブロックチェーンネットワークの不均衡と収束による再中央集権化の評価」, ISEC, 2020年5月.
[IO19] M. Imamura and K. Omote, “Difficulty of decentralized structure due to rational user behavior on blockchain”, NSS 2019, pp.504-519, 2019.

観測と分析

- 構造として非中央集権化が保たれているのか
  - ノードだけでなくASの観点も入れて評価
  - 不均衡性と収束性を定量的に評価して構造を推定
- ネットワークに展開されるBitcoinノードの動態を観測
  - データセット：DSN Bitcoin Monitoring (https://dsn.tm.kit.edu/bitcoin/index.html)
  - 期間：2015/07/15～2020/04/09
- 不均衡性
  - AS間のジニ係数で評価
    - 特定のASが中央集権的（独占的）なら1に近づき，均等分布なら0に近づく
- 収束性
  - 各ASが占めるノード数の割合で評価

分析：ノード数とAS数の推移

- ノード数は，観測開始時点で約4,000台，2018年のピーク時は13,500台に到達
- 直近までは9,000～10,000台の間を推移
- IPv4アドレスの割合は約90%，IPv6の利用はわずか

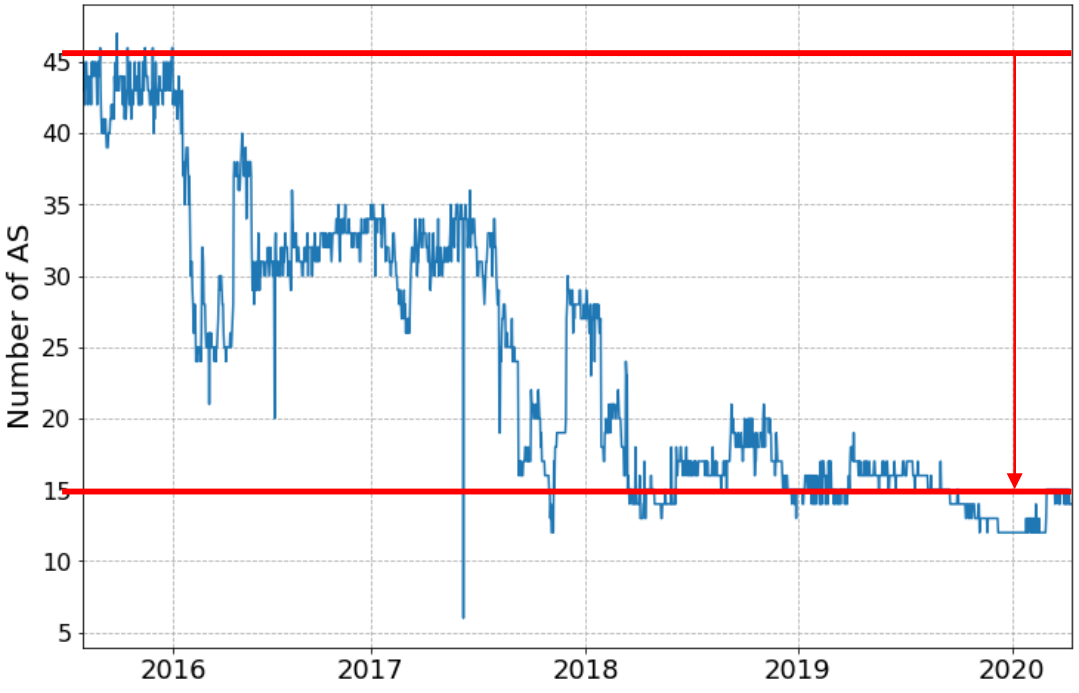


分析：AS間のジニ係数の推移（不均衡性）

- 不均衡性は0.68から0.8以上まで増加
- 2018年以降，ノード数は減少するがジニ係数は横ばい

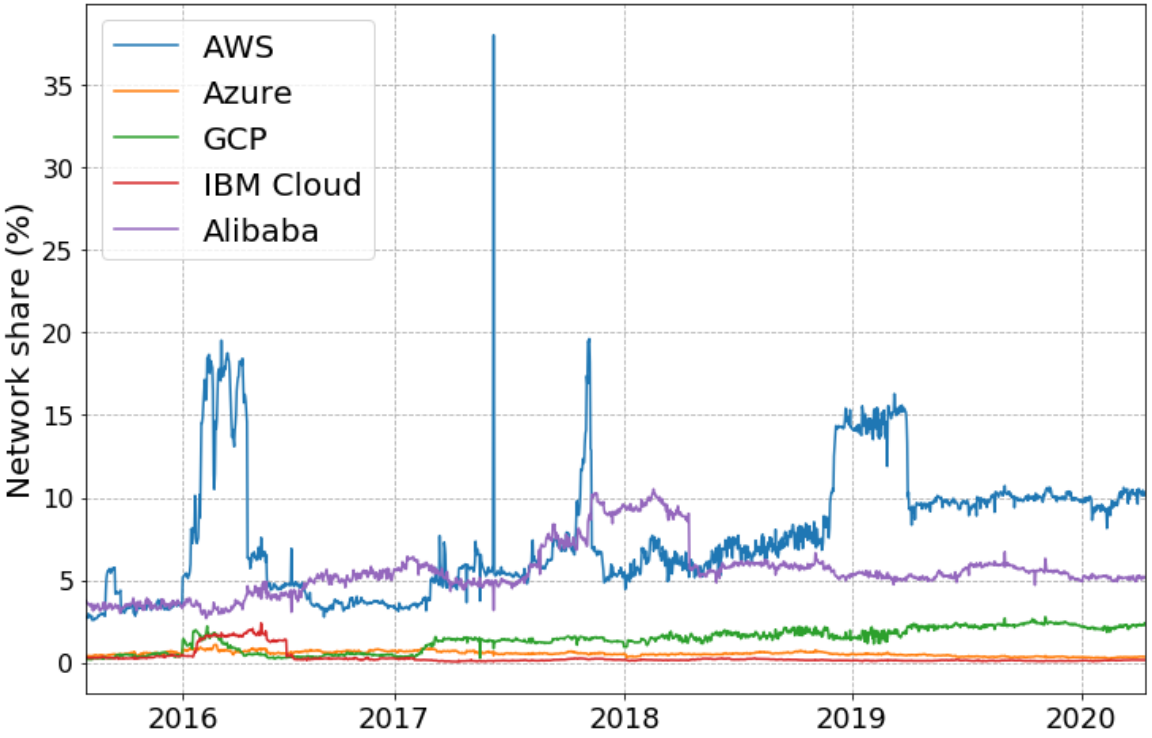
分析：上位AS数の推移（収束性）

- 観測開始時点：
  - 2,000ノードが45ASに分散，ASあたり約44ノード
- 直近：
  - 4,500ノードが15ASに分散，AS あたり約300ノード
  - 特定のASにノードが集中



分析：Bitcoinにおける利用プロバイダの傾向

- よく利用されているのはAWSとAlibabaで合わせて15%程度
- AWS, Azure, GCPにおいて，Bitcoinノードを維持するために必要な最低スペックの金額や設置可能な地域に大きな違いはないが，ノード設置ユーザは特にAWSの利用を支持



Topic 2：
ブロックチェーンを用いたIoT機器ファームウェア配布手法
（ブロックチェーンを適用した安全なシステム構築）

ファームウェアダウンロード時の問題

- IoT機器の数が膨大
  - ファームウェアのダウンロード時に膨大な量のトラフィック発生
  - ベンダーの負荷が集中

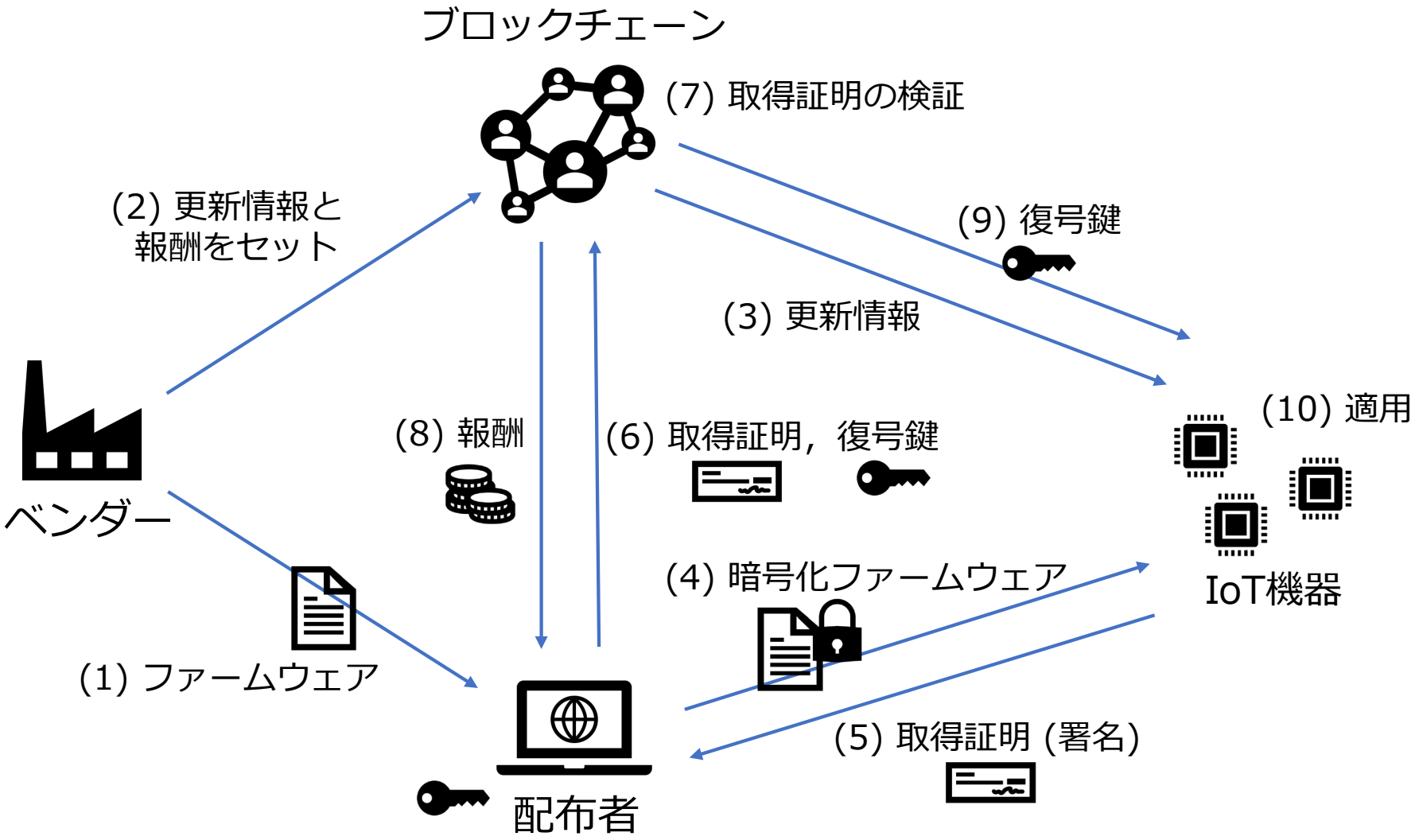
- ブロックチェーンとP2Pファイル共有システムを利用した研究がいくつか提案されている
  - ブロックチェーン
    - 整合性を保ったまま分散管理
  - P2Pファイル共有システム
    - 負荷分散のために，不特定多数の第三者に配布を手伝ってもらう

インセンティブを考慮した手法

- Leibaらの研究[BKLNY19]
  - スマートコントラクトを用いて配布者に報酬を自動付与
    - 登録されている配布者のアドレスを用いて，トランザクションのなりすましを防止
    - 登録されているIoT機器の検証鍵を用いて取得証明を自動検証
    - 検証に成功したら報酬を自動付与
  - ファームウェアの暗号化により配布者とIoT機器の公平な取引を実現
    - IoT機器が配布者に取得証明を送信しない限り，復号鍵を入手できない
    - 配布者が正しいファイルを暗号化して渡した事を保証するためにゼロ知識証明を利用
  - ファームウェアの更新毎に配布者はgasコストを支払う必要があるが，報酬はgasコストの分も含めて得られる

[BKLNY19] R.Bitton et al., “IoTPatchPool: Incentivized delivery network of IoT software updates based on proofs-of-distribution“, Pervasive and Mobile Computing, Vol.58, 2019.

Leibaらの手法

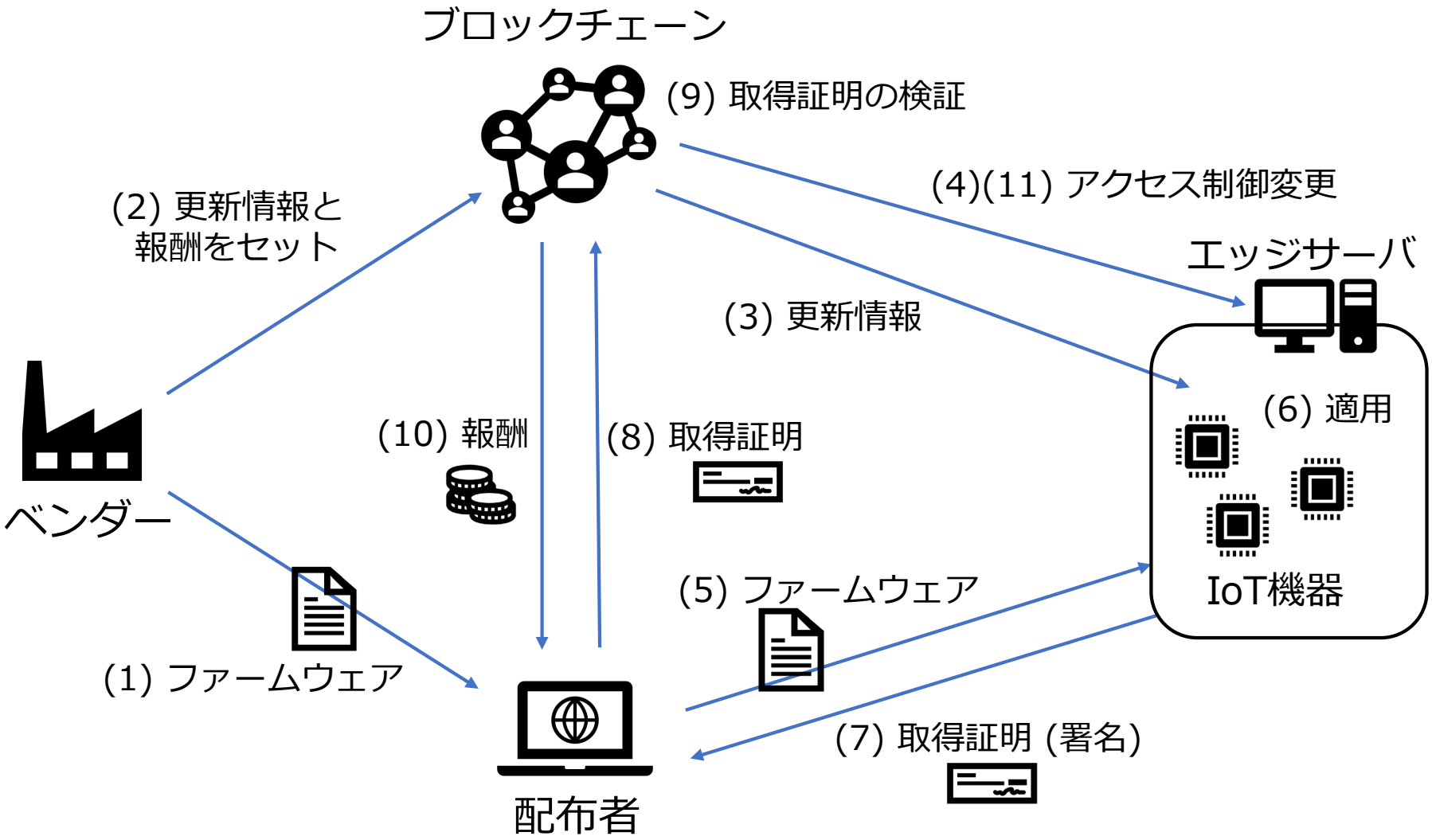

ブロックチェーン
(7) 取得証明の検証
(2) 更新情報と
報酬をセット
(9) 復号鍵
(3) 更新情報
(10) 適用
(8) 報酬
(6) 取得証明，復号鍵
ベンダー
IoT機器
(4) 暗号化ファームウェア
(1) ファームウェア
(5) 取得証明 (署名)
配布者

提案手法に向けて

- Leibaらの方式の問題
  - 暗号化を使ってIoT機器から取得証明を得るように誘導しており，アップデートを阻止するアプローチでありセンスが良くない
  - 暗号化毎に鍵を変える必要があり，鍵管理が膨大になる
- 提案方式
  - 暗号化を用いない
  - より安全サイドに倒す方向でアクセス制御を組み合わせた設計によって，IoT機器から取得証明を得るように誘導
  - 1回の更新にかかるgasコストを安く抑え，配布者のインセンティブを考慮した効率的なファームウェア配布手法を提案

[SEO19] 福田，面，「ブロックチェーンを用いたインセンティブ付与を考慮した効率的なIoT機器ファームウェア配布手法」，SCIS 2020，2020年1月.

提案手法の全体像


ブロックチェーン
(9) 取得証明の検証
(4)(11) アクセス制御変更
(2) 更新情報と
報酬をセット
エッジサーバ
(3) 更新情報
(6) 適用
(10) 報酬
(8) 取得証明
ベンダー
IoT機器
(5) ファームウェア
(1) ファームウェア
(7) 取得証明 (署名)
配布者

まとめ

- ブロックチェーン自体の安全性評価
  - Topic 1. ブロックチェーンネットワークの再中央集権化
- ブロックチェーンを適用した安全なシステムの構築
  - Topic 2. ブロックチェーンを用いたIoT機器ファームウェア配布手法


ご清聴ありがとうございました.
Mt. Tsukuba