# 公開された画像およびサプライチェーンにおける権利保護と活用促進を両立する革新的セキュア分散台帳技術の開発

自然科学研究科

野上保之

小寺雄太（画像に対する権利保護）

博士後期課程２年・那須弘明（サプライチェーン企業間連携システム）

# キーワードを幾つか焦点を絞っても

1. ターゲット分野

   交通/医療・介護/観光/農業/食品/防災・減災/インフラ維持管理/

   製造業/エネルギー/働き方改革/金融（FinTech）/教育（EdTech）/その他

2. Society5.0を支える**ツール**
   - IoT（Internet of Things）デバイス：（FPGA，RaspberryPi，GPGPU，WEBカメラ）
   - AI（Artificial Intelligence），Tensorflow，YoLo
   - 各種センサ（GPS，LiDAR，人体，工場・ロボット，トラフィック）
   - 無線通信（Wifi，Bluetooth，LPWA（Sigfox，LoRa，WiSUN），5G）
   - クラウド（Connected to Connected）・エッジ（クレンジング）
   - ロボット（サーボモーター，マイコン制御）
   - OS（UNIX）・プログラミング（Python）・NoCode/LowCode
   - 信号処理・画像処理（OpenCV），ブロックチェーン（Block Chain）
   - 3Dプリンタ，ドローン，タブレット，スマホ，WEB，etc

# 時代の象徴：仮想通貨

警視庁はこのほど、仮想通貨関連事業者のコインチェック社から流出した仮想通貨NEM（ネム）を盗品と知りつつ不正交換した人物らについて、2021年1月までに合計31名を立件したと明らかにしました。

問題の事件は2018年1月に起きたもので、コインチェック社の従業員の端末がマルウェアに感染したことにより、ネムを管理する秘密鍵を悪用され、当時の時価で約580億円相当のネムが、不審な通信先に転送されたという事件です。


**580億円相当の仮想通貨流出、被害者は約26万人 - コインチェック**

画像：Coincheck HPより 2018年1月26日、大手仮想通貨取引所の「Coinch

2018.1.29

警視庁は事件発生後も犯人や流出した通貨の行方を追い続け、これまで盗品と知りつつ別の仮想通貨と交換したと見られる北海道在住の男性医師ら合計31名を、組織犯罪処罰法違反容疑で逮捕および送検。合計約188億円の交換貨幣を挙げたとのことです。

# ブロックチェーン

**ブロックチェーン**とは、分散型ネットワークを構成する複数のコンピューターに、暗号技術を組み合わせ、取引情報などのデータを同期して記録する手法。*透明性・合意性・分散管理*

- 情報銀行
- 自動運転、自動車履歴
- トレード履歴
- 医療保険
- 配送システム
- 仮想通貨（暗号通貨）← BATなどその目的は

# 目的

研究目的及び内容

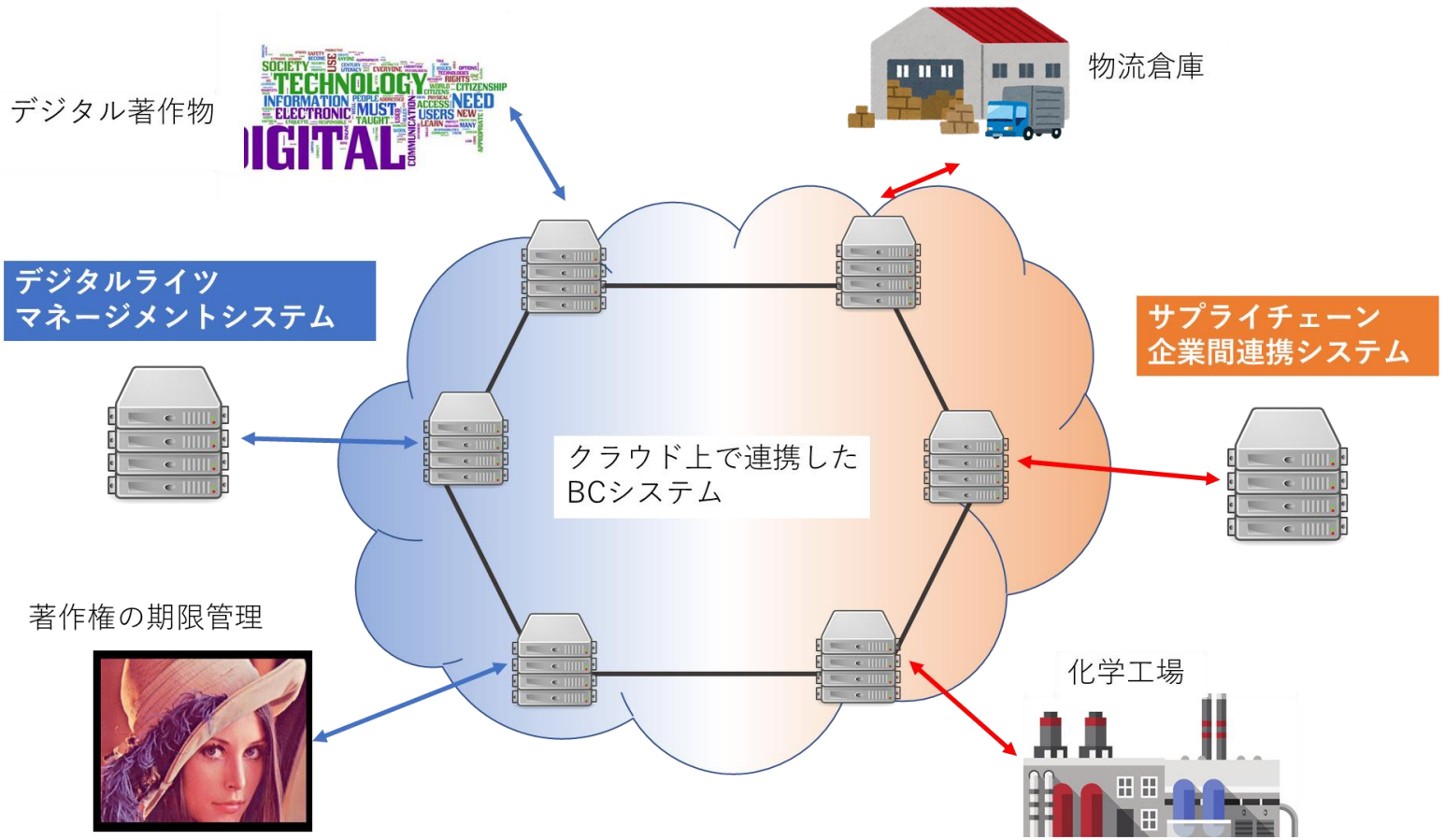
　Society5.0の促進には、膨大なデータを誰もが信頼できる形で共有・連携させることが重要となる。その最先端のツールとして、いま注目を浴びているのがブロックチェーン技術（分散台帳技術のこと、以下BC技術と省略する）である。これまで、BitCoinなど仮想通貨（暗号通貨）に活用され、そのシステムの安定性と信頼性が認知されてきた。そして昨今、その信頼足りえる分散台帳技術としての高度かつ斬新な使い道が模索されている。

# 個別テーマ

1. **デジタルライツマネージメントシステム**：流出などにより漏洩した画像に対して、後発的に権利情報を付与し、その公開の妥当性を検証できるようなフレームワークの構築を目指す。情報を漏洩させない技術ではなく、既に漏洩（公開）している情報に対する権利保護を考えるという点で他の研究と大きく視点が異なっており、公開の流れを止めるのではなく、加速させつつ巧妙に紐づけさせて悪用を防ぐことができる点において他に類を見ない研究である。

2. **サプライチェーン企業間連携システム**：サプライチェーン上の企業間では、自由にデータ連携し、サプライチェーン全体で高効率生産などが行えるエコシステムの構築が望まれている。しかし機密情報保持の観点からその構築は進んでいない。本プロジェクトでは、BC技術と暗号化したまま演算可能な準同型暗号を組み合わせ、オープンなデータ連携・業務協調を可能にするセキュアサプライチェーン企業間連携システムの構築をめざす。

# 本申請の提案


デジタル著作物
物流倉庫
デジタルライツ
マネージメントシステム
サプライチェーン
企業間連携システム
クラウド上で連携した
BCシステム
著作権の期限管理
化学工場

# サプライチェーン企業間連携システム

◆2020年度の研究目標

BC基盤上で企業間連携を促進する仕組みを提案

◆研究背景

➢金融などの分野でブロックチェーン（BC）などの技術が台頭

➢製造業でも、BCを活用しサプライチェーン（SC）上の企業間で

製品の品質情報や設備情報、受発注情報などを共有し、

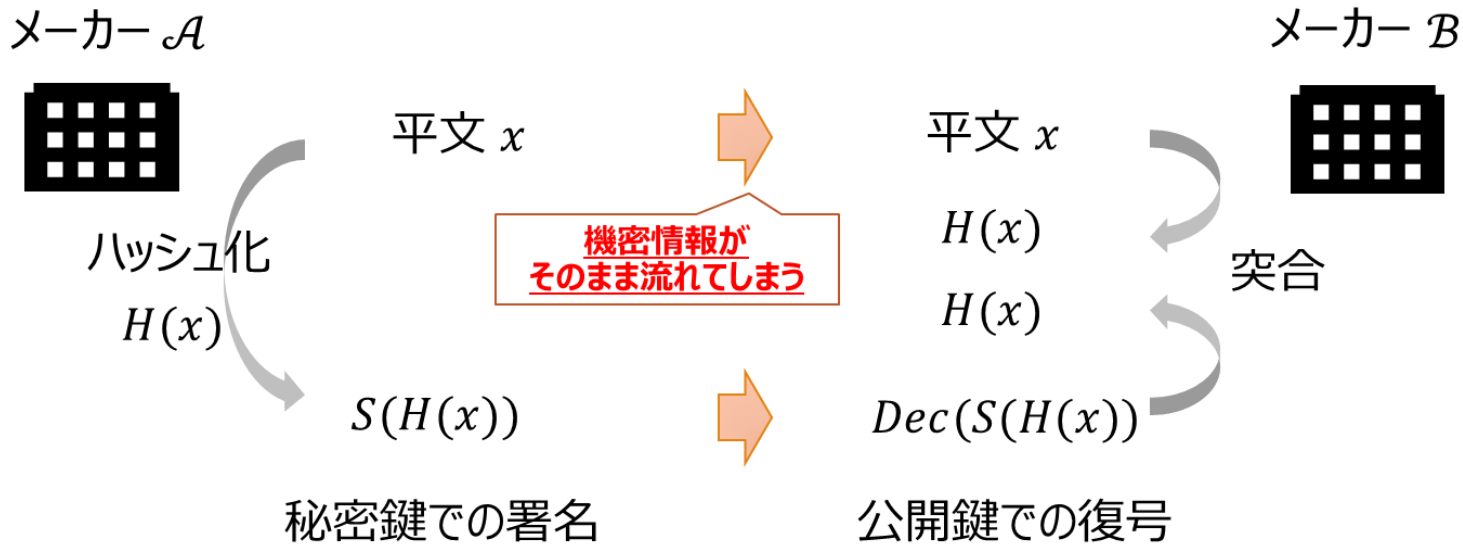
新商品開発の効率化や生産計画最適化などに役立てたい

というニーズ増加

# 研究課題

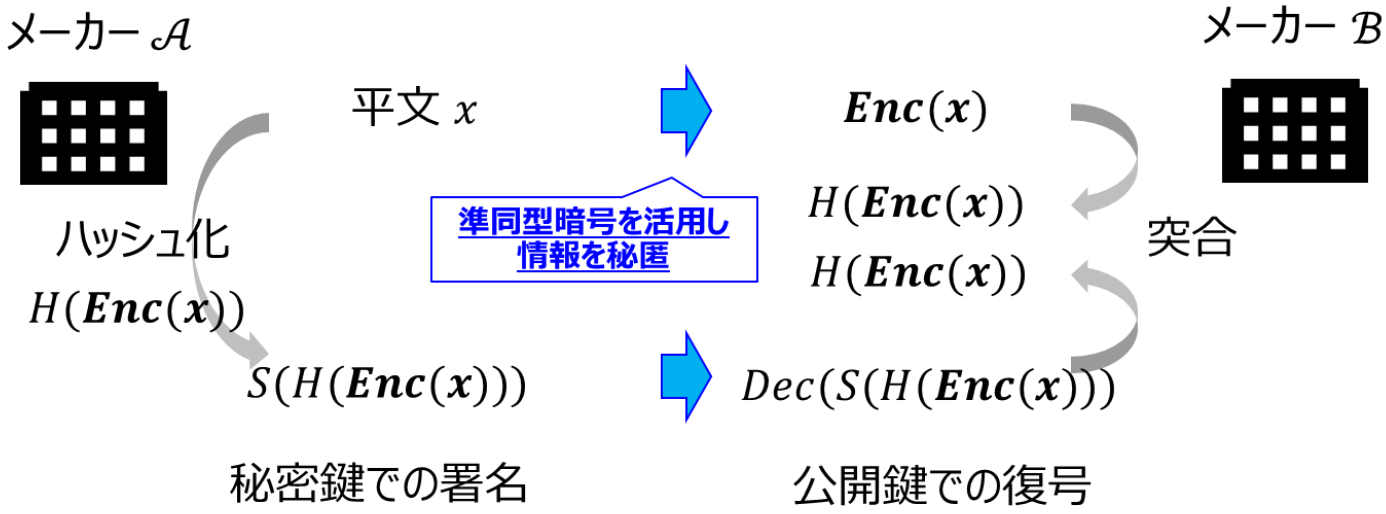
- 一般のBCの仕組みでは、平文が企業間で流れてしまう

  → 企業にとっては機密情報の開示となり、SC上での、特に製造データを対象にしたBC活用は進んでいない



# 提案する企業間連携システム

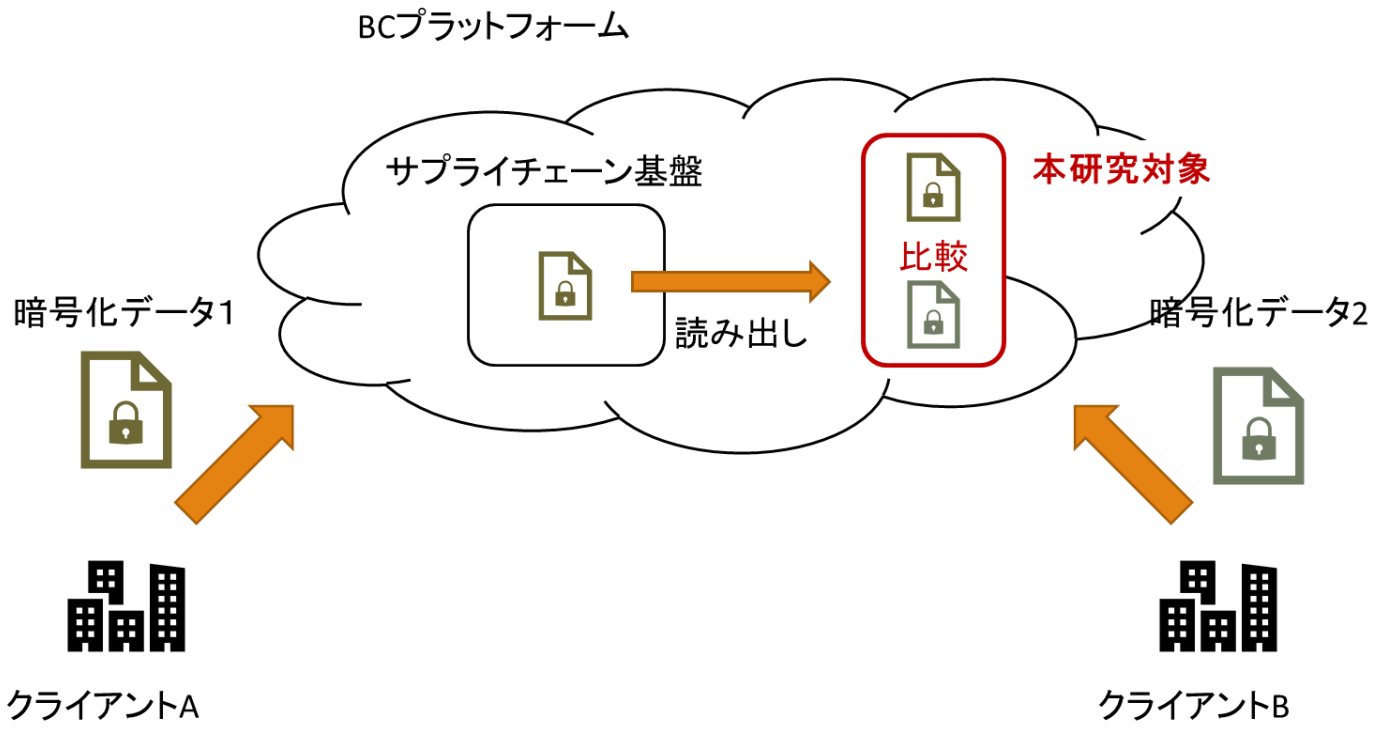
◆BCと準同型暗号を組み合わせ、
機密情報を秘匿したままでの企業間データ連携実現




準同型暗号：暗号化したまま加算や乗算が可能な暗号

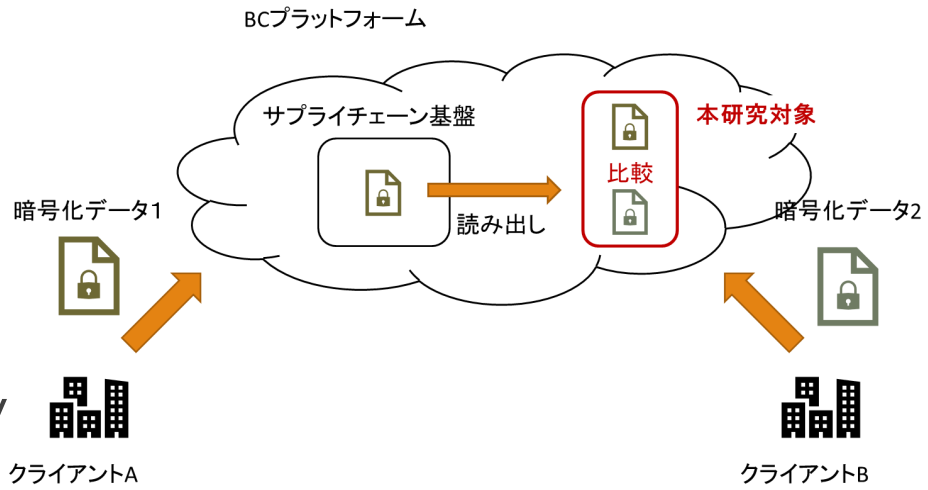
# 今回の実装にあたって – 構成 -

- AWS(Amazon Web Service)



# 今回の実装にあたって - Tools -

- AWS(Amazon Web Service)
  - Amazon Block Chain Management System ← 高い
  - Hyperledger Fabric
  - Go Language
  - **Paillier Cryptography**
    - **Homomorphic Encryption**
  - Gnu Multi-precision Library



# 本研究がめざす企業間連携システム

◆今後の課題

✓企業間連携システムを実現するプロトコル実装【一部着手済】

→ **令和３年度Cypherで申請**

**製造時の品質データに着目し、数値を秘匿したままで**

**大小比較を行い、品質変化を企業間で共有・業務連携**

✓社会実装に向けたシステムアーキテクチャの検討

✓BC基盤上にシステム実装、価値検証

→ **CRESTへ申請中（代表：小塚先生）**

**「DFFT を実現する基盤ソフトウェアの研究開発」**

DFFT：Data Free Flow with Trust（信頼ある自由なデータ流通）