

ハードウェアのバイオメトリック的 機器識別技術、 クロックフィンガープリンティング

国立高等専門学校機構

小山工業高等専門学校 電気電子創造工学科

准教授 干川 尚人

2021年7月6日

発表者の略歴

小山高専 電気電子創造工学科
准教授 干川 尚人

情報システム開発エンジニアを経験した
ネットワークサービス技術の研究者です

▼主な経歴

2009年 NTT東日本に入社

主に同社のシステム開発を経験

2012年 NTTネットワークサービスシステム研究所に転籍

災害時の安否伝言交換システムの研究開発, IoT/AIのサービス基盤の研究

2018年 小山高専に着任

ネットワークサービス技術, セキュリティ技術, ICT教育技術などを研究

企業では情報システムの開発や維持管理エンジニア, IoT/AIサービス基盤技術の研究などを経験。
産業界と学术界の両方に精通しております（産の立場から、産学連携の経験あり）

<企業時代の主な仕事>

- 商用サービス基盤の保守管理ソフトウェアの開発
- Web-テレコム連携基盤の研究開発
- 災害用伝言サービスシステムの開発, 維持管理, セキュリティ対応
- 安否確認向け音声-テキストメディア変換基盤の研究開発
- 将来IoT/AI向けサービス基盤の研究

▼開発に携わったNTT東日本, NTT西日本 災害用伝言板web171
<https://www.web171.jp/>

災害用伝言板 (web171)
English 한국어 中文
NTT東日本
NTT西日本

TOP画面

伝言の登録や確認ができます。

電話番号 例 03~/090~
登録
確認

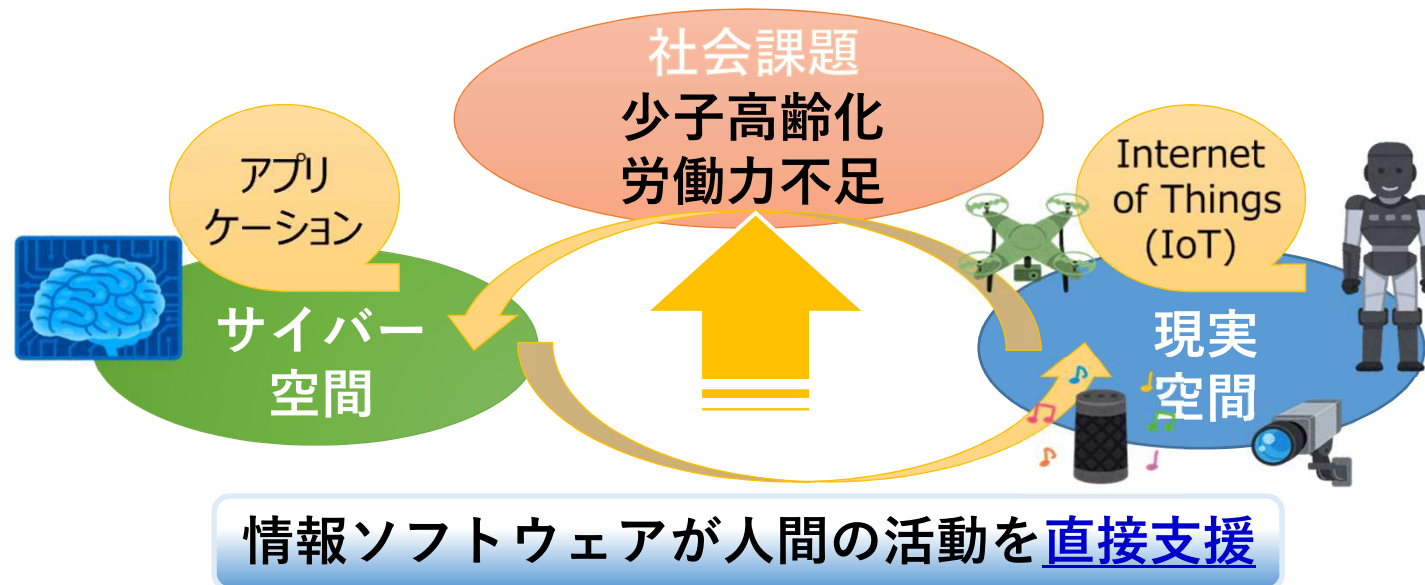
お知らせ

本日は体験利用が可能です。
この機会に、ご家族等と利用方法を確認していただき、使い方を覚えてください。

■SSLサーバ証明書移行について

技術ターゲットの背景

Society 5.0 実現によって、技術で社会課題解決の期待



Internet of Things (IoT)

現実空間の情報をネットワーク通信でデータとしてサイバー空間に取り込み、現実空間に直接作用する役割

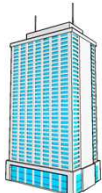
Society 5.0 実現に不可欠なキーテクノロジー

世界中でつながるIoT機器は500億台超



技術ターゲットの背景

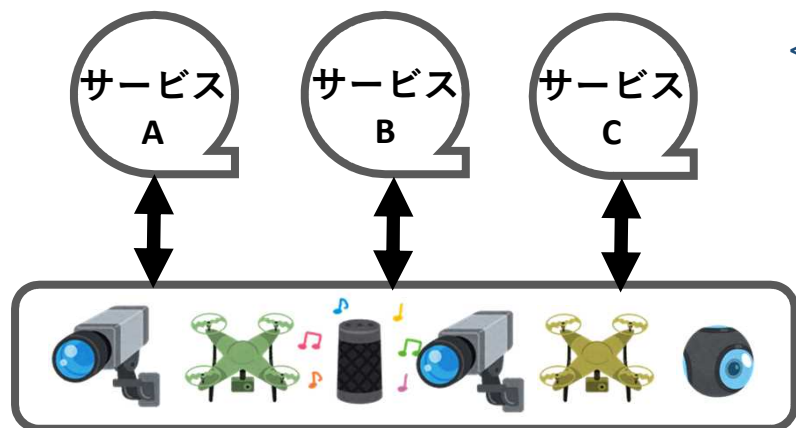
IoT向けネットワークサービスならではの特徴

	従来のネットワークサービス	IoTネットワークサービス	従来型システムと比べると...
規模・数	Webサイト  約10億	IoT機器  500億超	▼数が膨大 <u>必要なものを</u> どうやって<u>見つける</u>？
設置される場所	データセンター  管理された 建物内に設置	街中  様々な場所 に設置	▼管理品質が低い <u>攻撃から</u> どうやって<u>守る</u>？
利用するコンピュータ	サーバ ネットワーク アプライアンス  信頼性が高く均質な コンピュータ	組込制御 センサGW ウェアラブル  用途性能さまざまな コンピュータ	▼コンピュータの 性能がバラバラ <u>違いを</u> どうやって<u>補う</u>？

IoTシステムにとって最適な
機器の発見, 防御, 補完技術が不可欠

技術ターゲットの背景

IoT機器を利用するサービスアプリケーションに求められるオープン性



＜オープンなIoT＞

サービス，場所，時間，人
…問わず，相互にIoT機器を
利用できる



必要な時に空いている
誰かのカメラ機器をシェア
広域見守りサービス

▼便利で快適になるはずのIoTサービスに，危険性や不安感

サイバー空間どころか
現実空間も危険！？

機器の乗っ取り
(盗聴・詐称)

管理が
甘い



今後のIoTサービスの進展とともに
サイバー・フィジカルセキュリティ
の懸念も顕在化していく

技術ターゲットの背景

- ◆安全なネットワークサービスの利用には**認証**が必要
機器は**識別キー**を用いて**発見**し、**認証**する



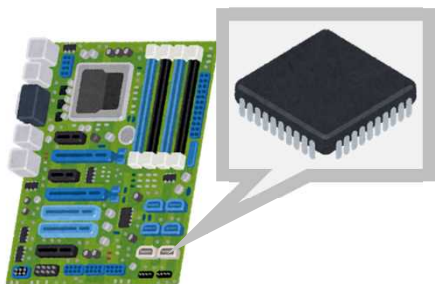
しかし、識別キーが盗まれると容易に詐欺が可能に

**耐タンパ性の高い識別キーデータ
保護技術が必要**

従来技術とその問題点

▼現在の研究開発のトレンド

1. ハードウェアベースの保護機構



防御用ハードウェア
を実装する

- ◆耐タンパ性の高い揮発メモリ上の識別キー保護機構
⇒電力制約と継続動作が不安定なIoT機器では利用が困難

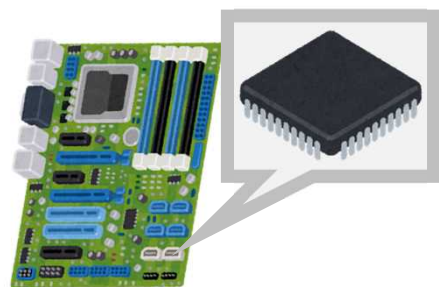
- ◆物理複製困難関数（PUF）による識別キーの生成
⇒強固だが、固有のハードウェア機構が必要

2. ソフトウェアベースの保護機構

- ◆ネットワークトラフィック分析による機器特徴の判別
ソフトウェアで解決できるため、幅広い機器に対応できる可能性あり
⇒しかし、学習コストが高い。機器の仕様変更に弱い。識別精度が悪い。

現状ではIoT機器向けの保護機構はハードウェアベースが有望だが、実用化には課題あり

従来技術とその問題点



防御用ハードウェア
を実装する



安価で低能力な機器も
混ざっているIoT機器に
組み込みにくい
すでに使われているIoT機器
では使えない

問題

既存の技術方式を規格化，標準化して，
製品化そして，必要な数のIoT機器に普及させるまで，
どれだけ時間がかかるか？

IoT機器識別技術の課題

- (1) 迅速な実装可能性
- (2) 攻撃に対する防御性

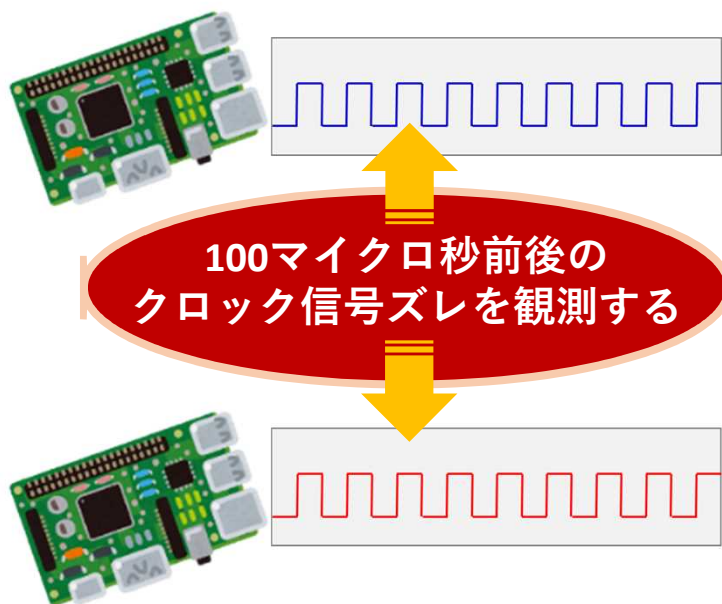


早期のSociety 5.0を実現する
イノベーションに不可欠な要素

クロックフィンガープリンティング

コンピュータの処理能力を持つ機器であれば幅広く実装可能
コピーの困難な識別キーを生成し，識別に利用する
新たなネットワークソフトウェア技術

コンピュータ機器が必ず持っているクロック周波数信号
ネットワーク通信を介して，そのわずかな信号特性の差である
「クロックフィンガープリント」を特徴データとして識別子に使う技術



似たイメージ：音紋
同じ発声でも人によって声音が違う

ゆたかな

ゆたかな

振幅

時間

(a) 女声1

振幅

時間

(b) 女声2

引用 Tech Village 音声信号処理の基礎理論（前編）
<http://www.kumikomi.net/archives/2010/09/ep27riro.php>

同じ製品，同じソフトウェア，同じ設定
であっても，その違いを見破ることができる

新技術の特徴

クロックフィンガープリンティング技術

- ・ 高い汎用性

特別な部品は不要，古い機器でも利用OK

- ・ 強固なセキュリティ性

電子部品の特性はコピーできない（攻撃に強い）

▼ハードウェアの実装が不要（ソフトウェアのみ）

▼計算機としての高性能性も不要（低負荷）

▼ネットワーク経由で実行する

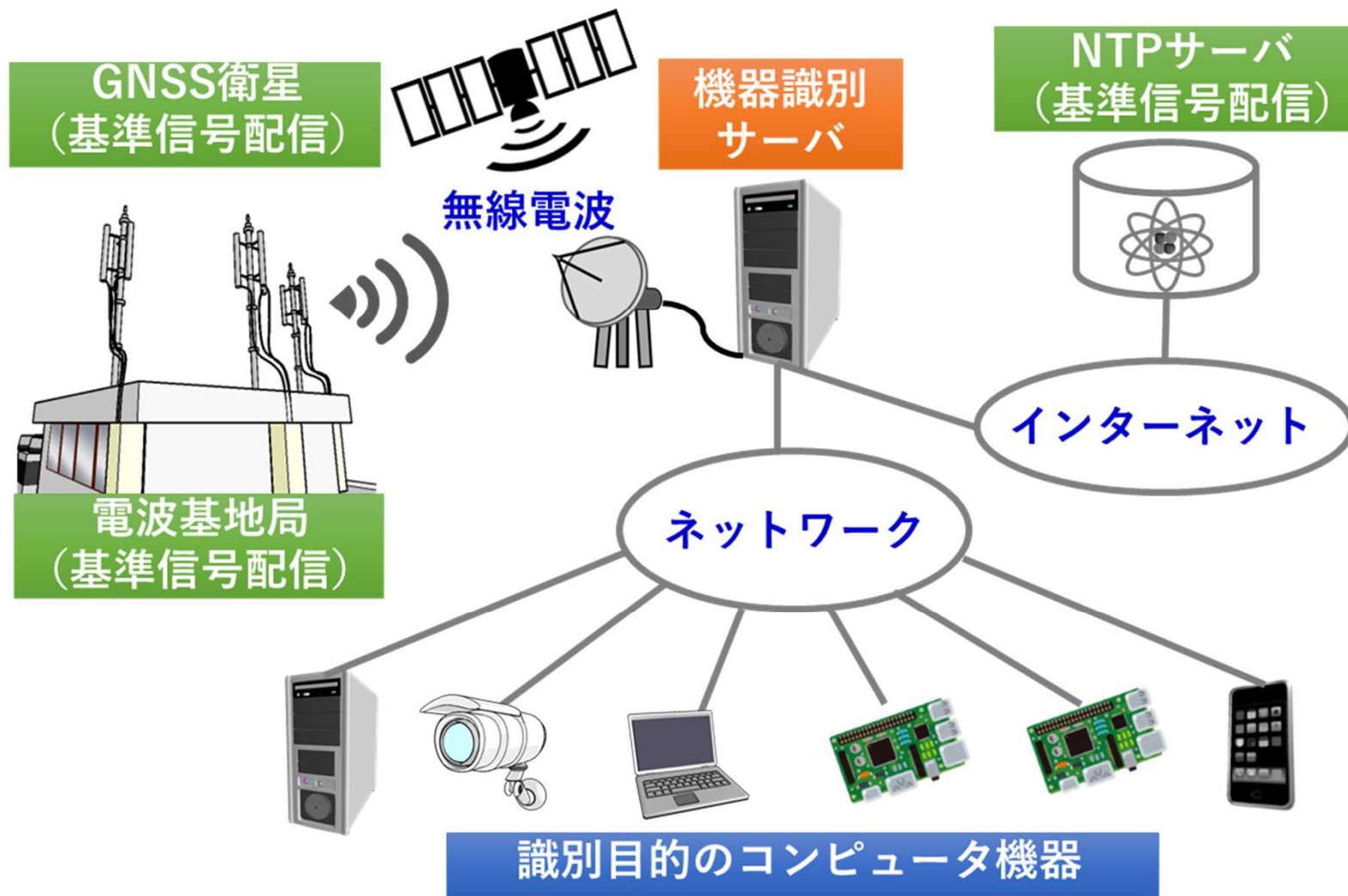
⇒ セキュリティ性と低コスト性の両立を求められる

IoT機器に最適な識別技術である

クロックフィンガープリントの抽出技術とその活用技術が
当研究グループの持つコアコンピタンスです

新技術の特徴

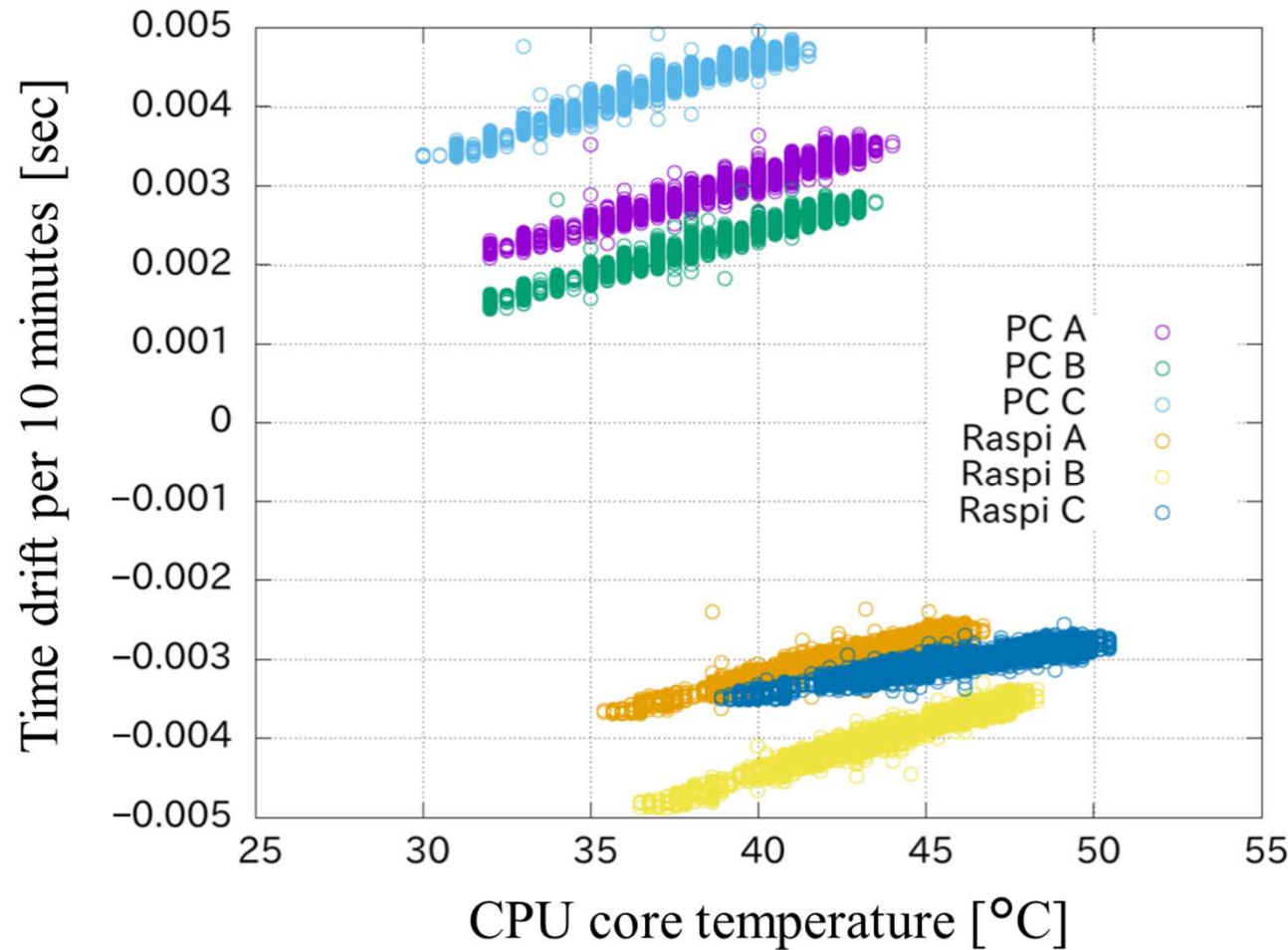
クロックフィンガープリンティング技術



■ 識別基盤を利用したシステムの構成例

新技術の特徴

クロックフィンガープリンティング技術



同機種、同設定の
ノートパソコン 3台

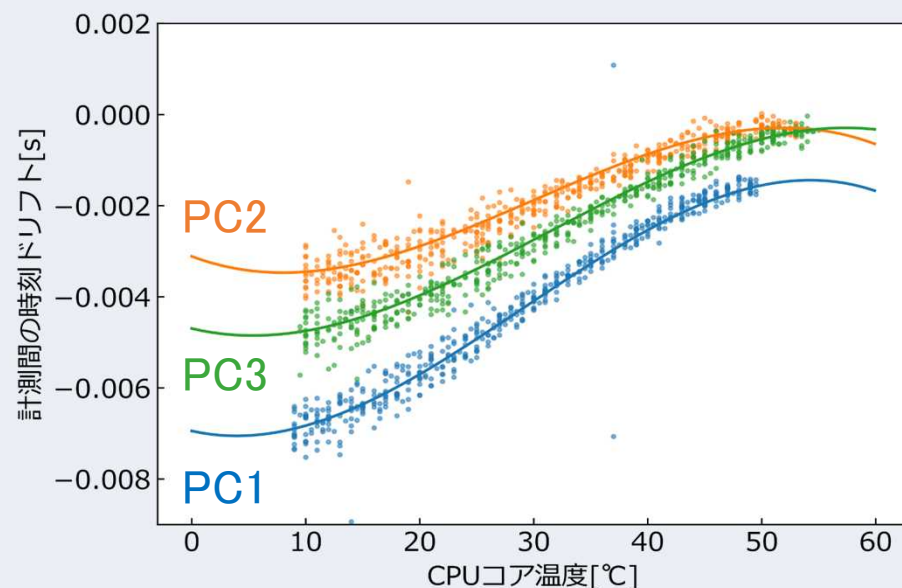


同機種、同設定の
シングルボードコン
ピュータ 3台

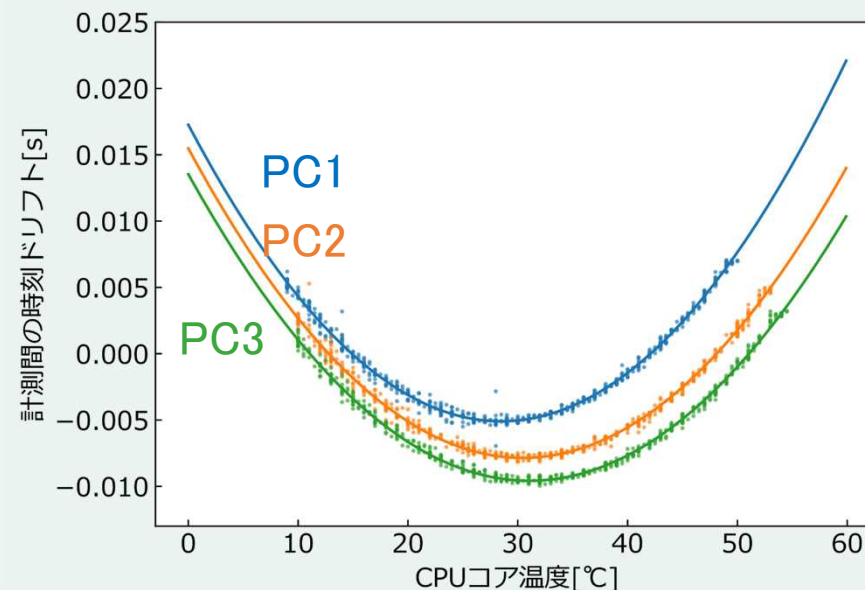
■ クロックフィンガープリントの抽出例
(2種の機種に対して、同じ信号源から抽出)

新技術の特徴

クロックフィンガープリンティング技術



クロックフィンガープリント(信号源A)



クロックフィンガープリント(信号源B)

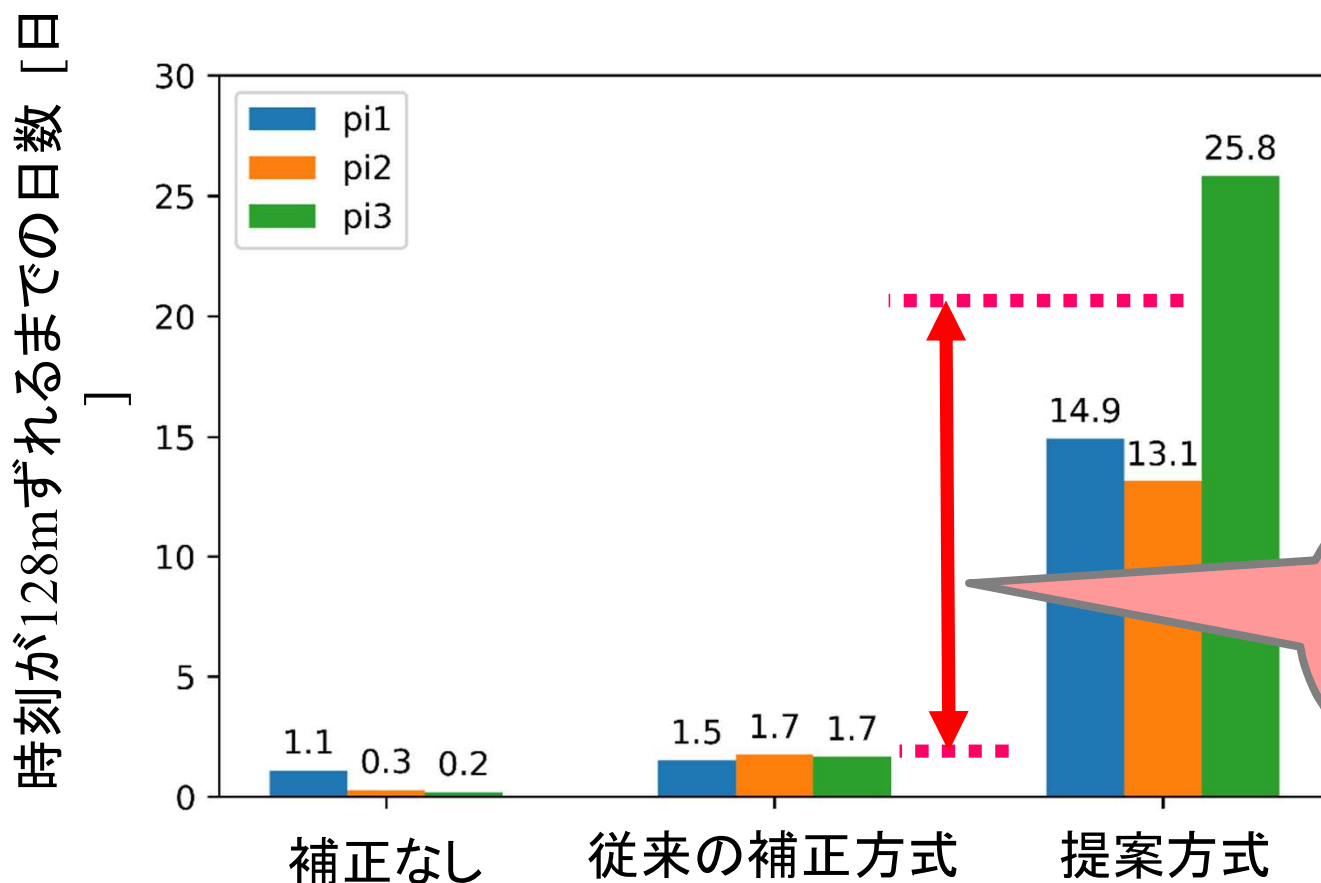
■クロックフィンガープリントの抽出例 (同一機種種の2種の信号源から抽出)



同機種, 同設定の
小型パソコン 3台

新技術の特徴

クロックフィンガープリンティングの応用
外部の基準信号が不要な時刻補正技術



同機種、同設定の
シングルボードコン
ピュータ 3台

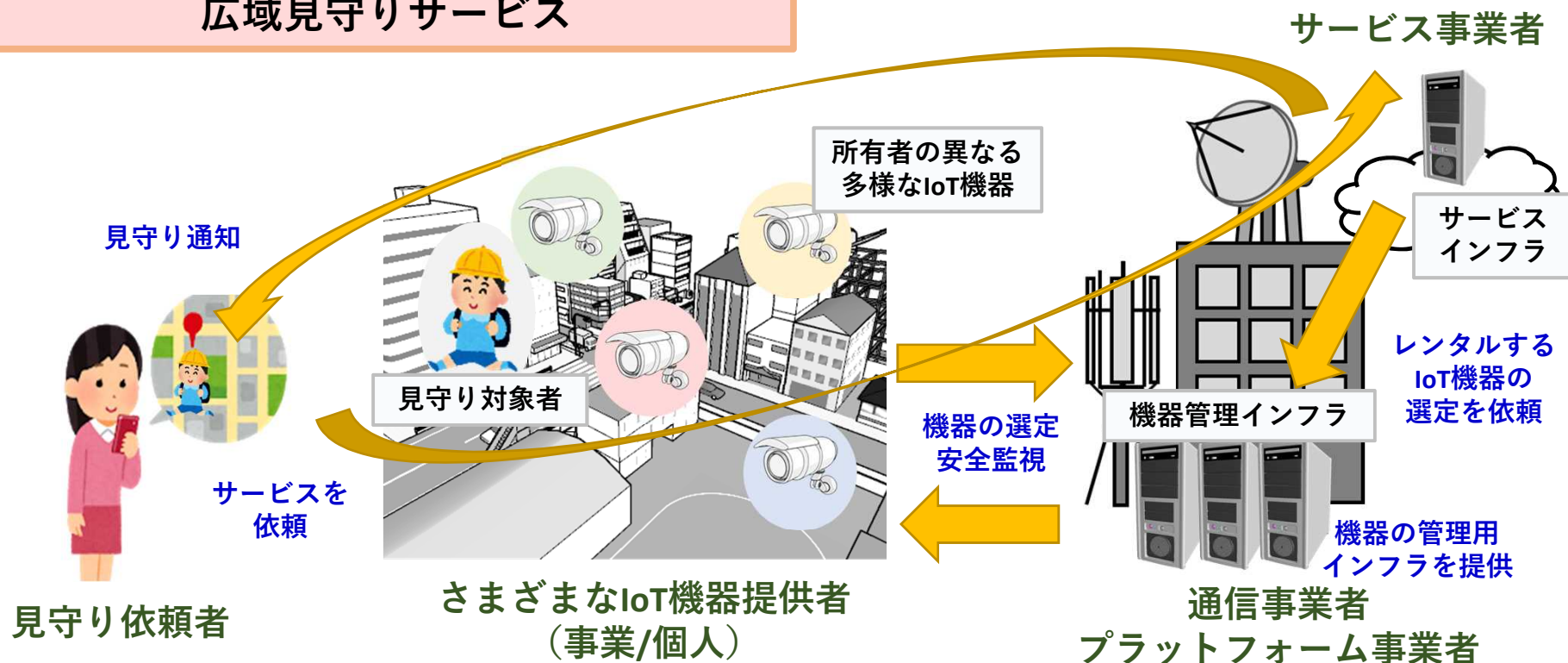
従来の補正技術と
比べて約10倍の
性能向上を達成

■コンピュータシステムの時刻情報のズレを予測し、外部からの補正無しでも
長期間正しい時刻を保つ技術

想定される用途

サイバー空間とフィジカル空間をまたぎ、人々の生活をサポートする
Society 5.0時代の社会システムを安心・安全に利用するICT基盤として

例) IoTシェアリングエコノミーベースの
広域見守りサービス



スマートアプリケーションにおける
セキュリティ基盤の要素技術 (機器の識別技術)

想定される用途

3～5年単位の実用化（技術の切り出し，応用）

機器識別技術

オフィスのデジタル機器資産の
管理アプリケーション

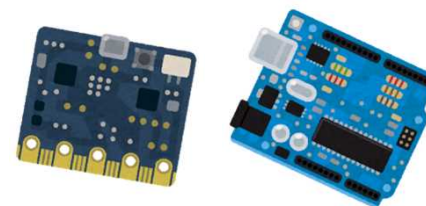
情報セキュリティ管理部門などを
持たない小規模なオフィスのDX推進



機器の管理ラベル付与の自動化
物理ラベルに依存しない資産管理

時刻補正技術

孤立したセンサ機器や頻繁な
ネットワーク通信を避けた
機器向けの時刻補正プログラム



スタンドアローンコンピュータや
バッテリーで長時間駆動するセンサ機器
を低消費電力に正確な時刻を保つ

時刻異常に伴うプログラム処理トラブル
の抑制（アプリの正常動作維持，ログ時
刻の正確性担保）

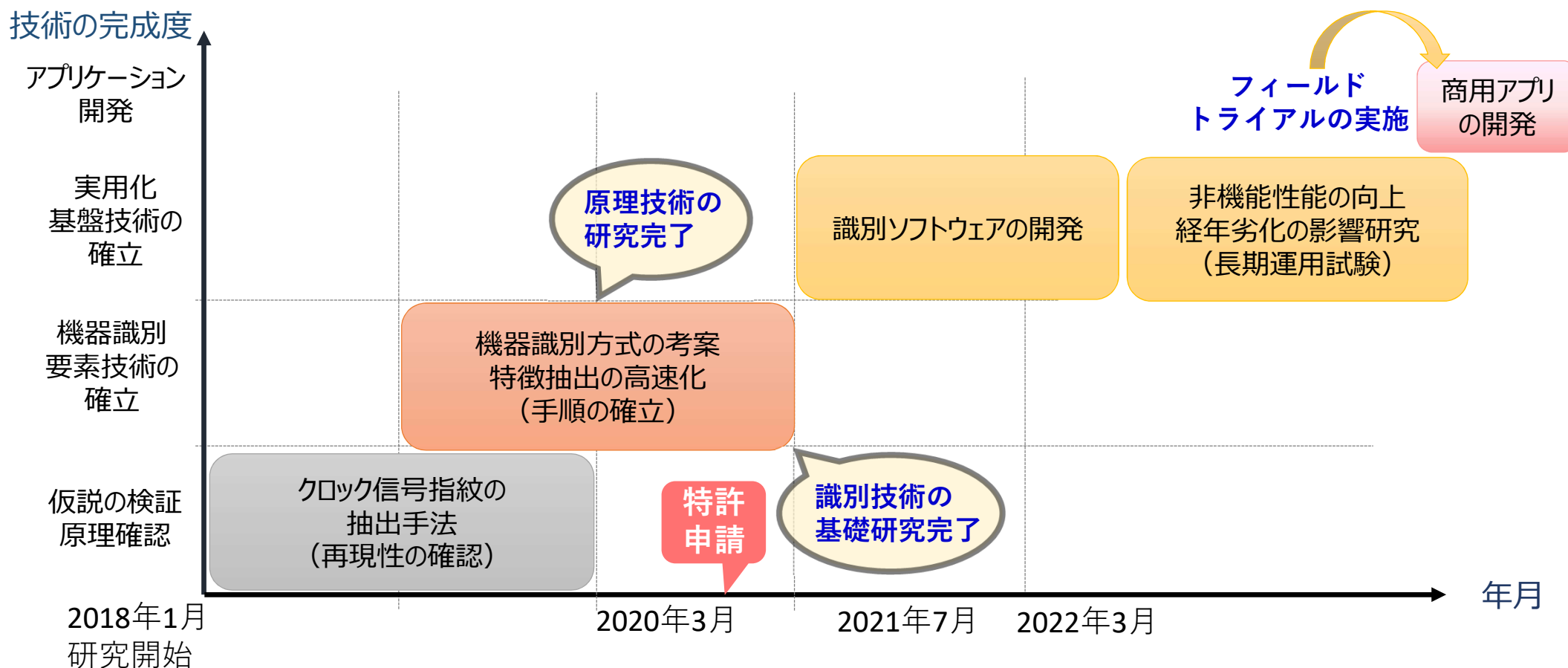
実用化に向けた課題

実用化への次のステップ：識別ソフトウェア基盤の開発と実証

課題(1) 識別ソフトウェアの実装

課題(2) 実運用上の影響除去（外乱，経年劣化などの対応）

課題(3) 非機能性能の向上（識別精度，識別速度）



企業様への期待

■ 企業の皆様にお力添えいただきたいこと

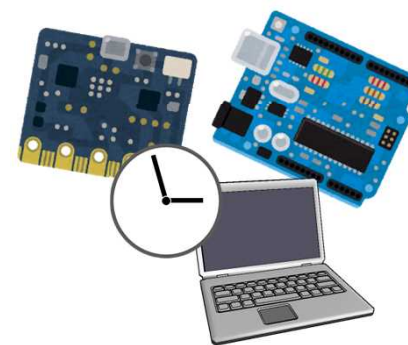
紹介技術について産業界の視点・知見から、

- ・我々のコア技術が活用できそうなユースケースのご提案
- ・実用観点の実証環境のご協力
- ・上記を踏まえた共同研究/商用化サービス開発のご提案

機器識別技術



時刻補正技術



本技術に関する知的財産権

- 発明の名称
: 情報システム、計算機、情報処理方法、及びプログラム
- 出願番号
: 特願2020-186550
- 出願人
: 独立行政法人国立高等専門学校機構
- 発明者
: 干川 尚人

お問い合わせ先

**国立高等専門学校機構
本部事務局 研究推進課**

T E L 03-4212-6832

F A X 03-4212-6810

e-mail KRA-contact@kosen-k.go.jp