様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ２２ 日現在

機関番号：５２２０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１８０３

研究課題名（和文）クロック・フィンガープリント：ハードウェアのバイオメトリック的機器識別技術の確立

研究課題名（英文）Clock Fingerprint: Establishment of Biometric-like Identification Technique for Computer Hardware

研究代表者

干川　尚人（Hoshikawa, Naoto）

小山工業高等専門学校・電気電子創造工学科・准教授

研究者番号：１０８１９３１１

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：Society 5.0実現に不可欠なIoT機器は，素性の不明な機器の混入や詐称による情報漏洩・不正操作のリスクが高い．そのため，安全で確実な機器識別技術が必要になる．本研究はこの解決方法として，例えば人間の指紋を用いた生体情報のような，ハードウェア固有のクロック信号特徴（クロック・フィンガープリント)を活用する方法を考案した．本研究期間では，機器ごとの特徴量を推定する数理モデルと特徴データ抽出手法を考案し，これを用いた機器識別手法を開発した．

研究成果の学術的意義や社会的意義
セキュアなIoTサービスの利用には機器識別技術が重要である．攻撃に強いディジタル識別子を活用する技術として物理複製困難関数（PUF）が注目されているが，これは多くのケースで専用のハードウェア機構を要求する．クロックフィンガープリント技術はクロック発信器に由来する新たなPUFの一種で，その固有の特徴量をコンピュータが必ず利用するシステム時刻から得ることができるため，ソフトウェアのみの実装で適用できる点が特徴である．そのため，設置された既存の機器や低コスト性の求められる製品などに対しても適用可能なので，幅広いコンピュータ機器の識別基盤技術として有望である．

研究成果の概要（英文）：IoT devices, which are indispensable for the realization of Society 5.0, are at high risk of information leakage and tampering due to the inclusion of devices with unknown identities and fraudulent identification. Therefore, secure and reliable device identification technology is necessary. As a solution to this problem, this research devised a method that utilizes hardware-specific clock signal features "clock fingerprints" like biometric. In this research period, we devised a mathematical model for estimating the amount of features for each device and an efficient feature data extraction method, and developed a device identification method using this model.

研究分野：情報システム

キーワード：機器識別　セキュリティ基盤　PUF　クロック信号　IoT

１．研究開始当初の背景

物理空間に作用するセンサやロボットなどの機能をネットワークでつなぐ IoT 機器と人間に匹敵する状況判断を可能にする AI システムの融合(超スマート社会，Society 5.0 の実現）は，少子高齢化・労働力不足などの社会課題の解決技術として期待されている．その基幹インフラである IoT 機器は，さまざまな場所に膨大な数が配備されるので，厳重なデータセンターに配備されたサーバ機器などとは異なり管理性が低い．そのため，素性の明らかでない機器の混入や，正規の機器が詐称されるリスクも増大するので，IoT 機器を利用するシステムにとって，その信頼性の確認がより一層重要になり，機器を確実に識別する手段が不可欠である．

ネットワークサービスが利用する機器の識別はサービスによって付与された識別子を利用する方法が一般的であるが，近年は利用者（ヒト）の識別手段として，生体情報（指紋，虹彩など）を使って個人を識別するいわゆるバイオメトリックス認証を利用することも増えてきた．生体情報を活用する場合，データ識別子と異なって改変が困難で，識別子の発行・付与の工程も削減できる利点がある．しかし，コンピュータ機器の持つ物理的な固有性（ハードウェア特性）を特別な機器を使わずに，ネットワーク経由の情報通信で取得する手法は確立されていない．

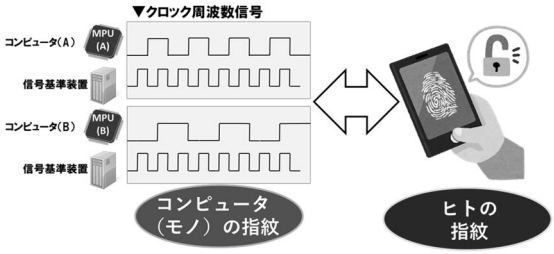

図 1 CFP（モノの指紋）のイメージ

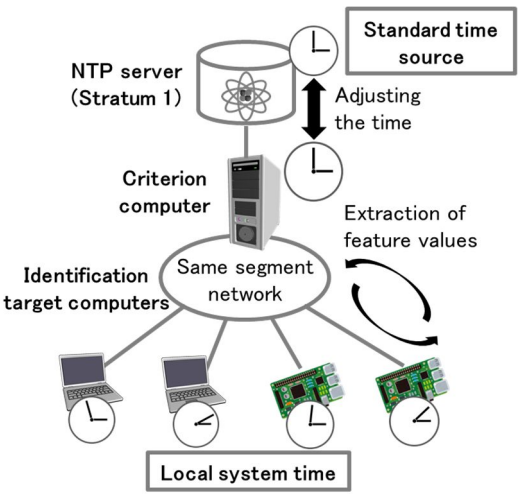

図 2 時刻ずれ値を抽出する仕組み

２．研究の目的

コア技術は，コンピュータ機器のハードウェア特徴として，機器が必ず持つクロック周波数信号に着目し，この周波数の機器ごとのわずかな違いをネットワーク経由で抽出する技術である．代表研究者はここで得られる特徴量を人間の生態認証で使う指紋になぞらえ，「クロックフィンガープリント（以下 CFP）」と名付けた．2019 年度までの研究では CFP のソースとなるクロック信号のずれ値をネットワーク経由でコンピュータのシステム時刻から抽出する仕組みを確立し（図 2），環境温度とクロックのずれ値に相関性が見えることを確認している（図 3）[1].

本研究の目的は，この CFP によるコンピュータ機器固有の識別子を取得するための原理の確立と，識別に必要な要素技術を完成させることである．この目標に到達することにより，技術の

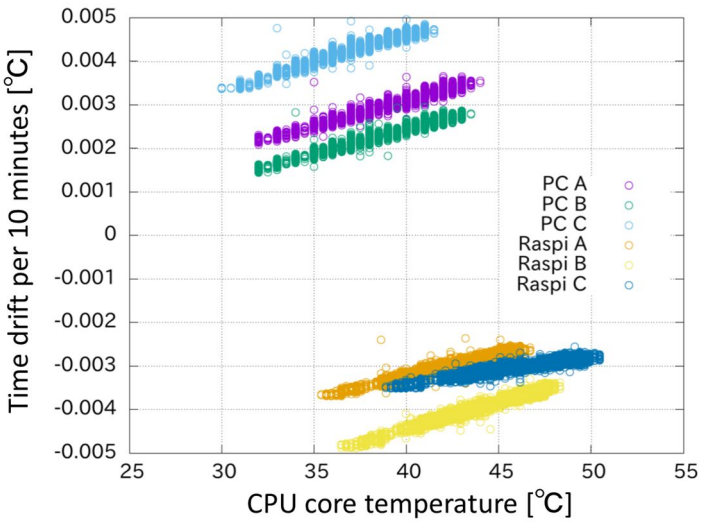

図 3 時刻ドリフト値の温度相関 [参考 1]

実用化の土台が完成する見込みである．本研究が目指している将来のビジョンは Society 5.0 実現に寄与する安価で確実な IoT サービス向けの認証基盤技術の創出である．そして，認証技術に不可欠な IoT 機器個体の識別を CFP によって実現する．このイノベーションが達成した際は，セキュリティ認証の要素技術として新しい研究領域が開拓され，そして IoT・AI によるスマートサービスでの産業応用へ繋がり，社会に幅広い波状効果が期待できる．

図 4 恒温槽による時刻ドリフト値抽出システム

[参考 1] Naoto Hoshikawa, Ryo Namiki, Katsumi Hirata, Atsushi Shiraki, Tomoyoshi Ito, “Extraction of Computer-Inherent Characteristics Based on Time Drift and CPU Core Temperature”, IEEE Access, No.8, pp.207134-207140, Nov 2020.

３．研究の方法

CFP 特徴はコンピュータ機器の持つクロック発信機の物理的な発信特性に由来する．本研究の土台となるコア技術はコンピュータのシステム時刻情報をネットワーク越しに取得し，基準時刻情報と比較することで，機器固有の特徴データを抽出するものである．しかし，発信機の周波数特性は一般に温度に応じて変化するため，固有の特徴データを得るための十分な温度範囲で時刻のずれ（時刻ドリフト）情報を収集する必要がある．なお，本研究では機器の温度情報を中央演算装置（CPU）のコア温度より取得する．CPU コア温度は一般的なコンピュータ機器ならば取得可能な情報であるため，非常に汎用性が高い．

この研究テーマでは，全体の取り組みを大きく二つのフェーズに分けて進める．まず，フェーズ 1 として，特徴量を表現する数理モデルを確立すること，そしてフェーズ 2 にて機器を識別するための具体的な手法を確立する．

４．研究成果

(1) 特徴データを表現する数理モデルの確立

過去の研究では，CFP 特徴データの抽出（学習）と識別実験を同じ温度環境下で実施していた．しかし，部屋の温度変化は季節に依存するため，特徴データを得るための十分な温度範囲変化を確認するためには四季の変化（数か月から 1 年単位）を待たなければならず，現実的ではない．そこで，恒温槽を任意の温度環境を設定するための実験システムを構築した（図 4）．この結果，学習用の特徴データの抽出に必要な時間が数日単位に短縮化を達成できた．更に，恒温槽によって通常の環境下では得られない温度範囲（-20℃から 80℃）の設定が可能になり，機器のクロック発信特性のより詳細な分析が可能になった．この取り組みの結果，多くのコンピュータのシステムクロックに起因する時刻ドリフトと温度相関について，図 5 のような三次関数で表現することが可能になった．この三次関数のパラメータは機器固有の特徴量であるため，以上の成果より，一般的なコンピュータ機器における CFP 特徴量の数理モデルは，温度を変数とした

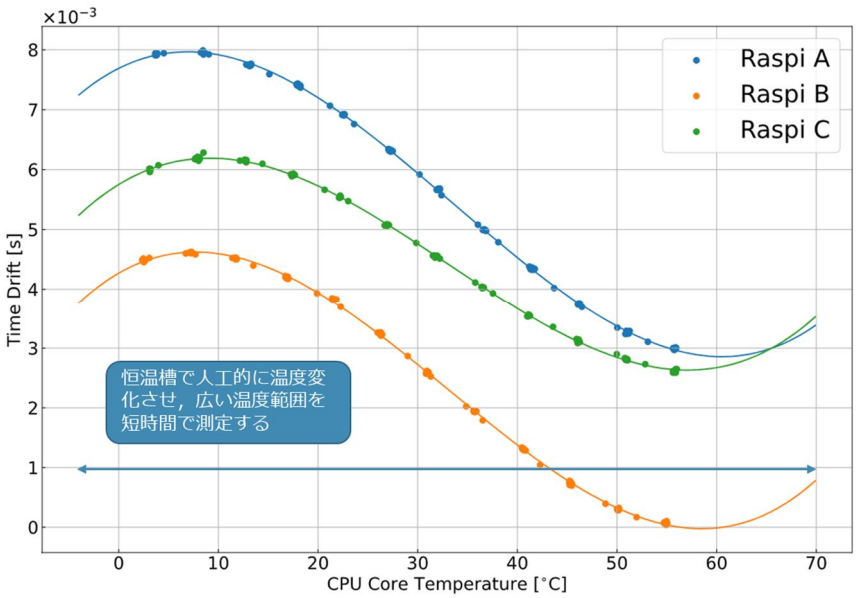

図 5 シングルボードコンピュータ 3 台の CFP 特徴データ

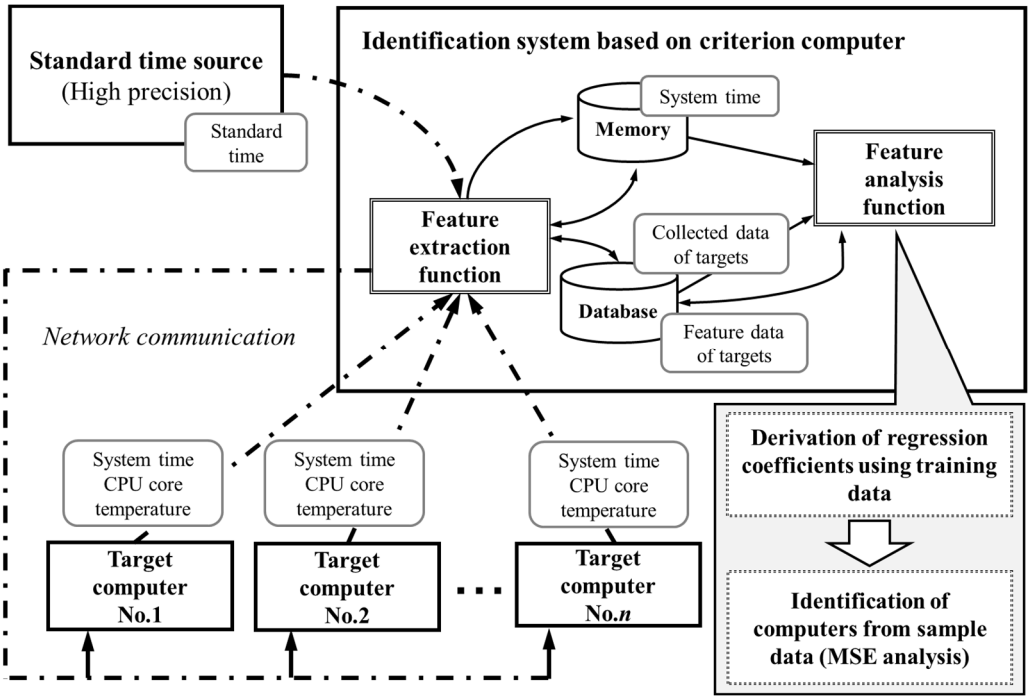

図 6 平均二乗誤差による**識別システムの機能ブロック**

時刻ドリフト値を導出する次の数式で表現できることを明らかにした.

$$\delta_t(T_C) = a_3 T_C^3 + a_2 T_C^2 + a_1 T_C + a_0 \qquad (式\ 1)$$

ここで, $a_3\ a_2\ a_1\ a_0$ **は機器固有のパラメータを意味する.なお,時刻ドリフトと温度相関が三次関数で表現できる理由は,クロック発信に利用されている水晶振動子に起因すると考えられる.一般にコンピュータのシステムクロックのソース源には** AT **カット型水晶振動子が利用されており,このタイプの水晶振動子の周波数温度特性が三次関数で表現されることが知られている.本研究で確立した特徴データ抽出システムによって,特別な装置を使わずにソフトウェア的な手法のみで水晶振動子の周波数温度特性に相当する写像データを獲得できたと言える.**

(2) **識別技術の研究**

本研究期間では,抽出した特徴データ(時刻ドリフトと温度相関性)を用いて,具体的な機器の識別手法を考案すると共に,その検証実験を進めた.

(2)-1 **平均二乗誤差,誤差(残差)分散の区間推定に基づく機器識別**

機器識別は候補となる識別対象機器から CPU **コア温度,時刻ドリフトを測定し,この値で得られるもっとも近い回帰係数(特徴データ)を持つ機器を選択することで判別する手法を考案し,これは平均二乗誤差に基づく機器識別手法(雑誌論文「時刻ドリフトの平均** 2 **乗誤差分析によるオンライン機器の識別技術」)として論文掲載されている(図** 6**).しかし,本手法は未知の機器であっても識別候補のいずれかに分類してしまうため,平均二乗誤差に閾値を設定する改良を行った.これを誤差分散の区間推定に基づく機器識別とした.**

(2)-2 **適合度検定を用いた機器識別**

前述の誤差分散の区間推定に基づく手法は,適切な区間の計測値を一度でも第三者に知られた場合,これを繰り返し用いることで識別条件を満たすことができる.そこで,得られたデータが想定した確率分布に従っているか検定することで,なりすましを排除する手法として,適合度検定を用いた機器識別手法を考案した.

上述の 2 **手法(**(2)-1**,** (2)-2**)について,「①識別に必要な測定回数」「②機器のすり替え」「③機器のなりすまし」の** 3 **ケースについて検証を行った.結果,①,②は前者,③は後者の手法が優れている結果を得た.今後,本提案技術の実用化を目指すためには更なる精度向上が必要であるため,両手法の短所を克服した新たな手法の創出が必要である.**

(3) **その他,実用化を見据えた技術検証**

本研究の取り組みで行った実用化を見据えた技術検証の取組結果を示す.

(3)-1 **無線通信環境下における特徴データ抽出の影響**

ここまでの研究は安定した通信環境を期待できる有線ネットワーク環境下で実験を行ってきたが,一般的な利用では無線ネットワーク環境下での運用も多いと考えられる.そこで,無線ネットワーク環境下でどのような影響があるかを検証した.結論としては有線と比べると誤差は大きいが,有線同様に三次関数の回帰曲線を得ることが可能であり,無線ネットワ

ーク環境下でも本提案技術は有効であることを確認できた.

(3)-2 CFP 手法の応用：時刻ずれ値の推測による時刻補正技術の開発

CFP の「機器固有のクロック信号のずれ値を予測する技術」を用いて，クロック信号を基準として記録されるコンピュータシステムの時刻情報のずれ値を補正する応用技術の開発を推進した．この技術はネットワークなどの外部信号に依存せずに時刻を正確に維持することができるため，補正通信用の電波が弱い，または通信のエネルギーを消費したくないなどの事情があるバッテリ駆動型のセンサデバイスなどへの適用が期待できる.

(4) 今後の課題

本技術を実用化には識別精度の向上が不可欠で，そのために測定誤差と通信誤差の抑制が必要である．まず，前者の測定誤差について，現在確立した恒温槽による CFP 特徴量抽出システムは，恒温槽と実空間で特徴データにギャップが発生する事象を確認しており，これが大きな測定誤差になっている．この誤差要因となっている差は何なのか原因の解明し，特徴量抽出システムの改良を進めていく必要がある．また，後者の通信誤差については，基準信号の通信精度を向上させることは有効だと考えられる．ここまでの研究では基準時刻情報を調整するために NTP（Network Time Protocol）を利用していたが，今後は移動体通信の 5G でも採用されている，より低遅延な PTP(Precision Time Protocol)の採用も検討していく.

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 干川 尚人、古井 海里、白木 厚司、伊藤 智義	４．巻 J104-B
２．論文標題 時刻ドリフトの平均2乗誤差分析によるオンライン機器の識別技術	５．発行年 2021年
３．雑誌名 電子情報通信学会論文誌B 通信	６．最初と最後の頁 761～771
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transcomj.2020NSP0001	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計10件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 竹澤小径 ，干川尚人，白木厚司 ，伊藤智義,下馬場朋禄
２．発表標題 クロック周波数の温度特性に基づく室温環境での時刻補正方式
３．学会等名 電子情報通信学会 通信ソサイエティ ネットワークシステム研究会（2022年10月）
４．発表年 2022年～2023年

１．発表者名 小林明珠，干川尚人，白木厚司，伊藤智義
２．発表標題 適合度検定を用いたクロックフィンガープリント識別手法
３．学会等名 電子情報通信学会 通信ソサイエティ ネットワークシステム研究会（2023年1月）
４．発表年 2022年～2023年

１．発表者名 竹澤小径 ，干川尚人，白木厚司 ,下馬場朋禄，伊藤智義
２．発表標題 クロック周波数の温度特性に基づく時刻補正方式の補正精度改善
３．学会等名 電子情報通信学会 通信ソサイエティ ネットワークシステム研究会（2023年3月）
４．発表年 2022年～2023年

１．発表者名
安田光希，千川尚人，白木厚司，伊藤智義

２．発表標題
オンライン機器の識別を目的とした時刻ドリフト特徴抽出技術における無線通信の影響

３．学会等名
電子情報通信学会 通信ソサイエティ ネットワークシステム研究会

４．発表年
2021年～2022年

１．発表者名
桂潔成，千川尚人，白木厚司，伊藤智義

２．発表標題
クロック信号源の広範囲な温度ずれ特性に基づくコンピュータの時刻補正手法

３．学会等名
電子情報通信学会 通信ソサイエティ ネットワークシステム研究会

４．発表年
2021年～2022年

１．発表者名
小林明珠，千川尚人，白木厚司，伊藤智義

２．発表標題
恒温槽内で計測する時刻ドリフト特徴量の精度評価

３．学会等名
電子情報通信学会 通信ソサイエティ ネットワークシステム研究会

４．発表年
2021年～2022年

１．発表者名
安田光希，千川尚人，白木厚司，伊藤智義

２．発表標題
オンライン機器の識別を目的とした無線環境下における時刻ドリフト特徴の分析

３．学会等名
情報処理学会 第84回全国大会

４．発表年
2021年～2022年

１．発表者名
水戸部 真澄，干川 尚人，小林 明珠，白木 厚司，伊藤 智義

２．発表標題
ディジタル機器におけるReal Time Clockの時刻ドリフト特性の研究

３．学会等名
電子情報通信学会 通信ソサイエティ 第24回ネットワークソフトウェア研究会（2021年1月）

４．発表年
2020年～2021年

１．発表者名
小林 明珠，水戸部 真澄，桂 潔成，干川 尚人，白木 厚司，伊藤 智義

２．発表標題
恒温槽を用いたディジタル機器の時刻ドリフト特性の抽出手法

３．学会等名
電子情報通信学会 通信ソサイエティ ネットワークシステム研究会（2021年1月）

４．発表年
2020年～2021年

１．発表者名
桂 潔成，干川 尚人，平田 克己，白木 厚司，伊藤 智義

２．発表標題
恒温槽を用いた温度安定化による時刻ドリフト特性推定の高精度化

３．学会等名
電子情報通信学会 通信ソサイエティ ネットワークシステム研究会（2021年3月）

４．発表年
2020年～2021年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
情報処理システム、計算機、情報処理方法、及びプログラム	干川　尚人	独立行政法人国立高等専門学校機構
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願 2020-186550	2020年	国内

〔取得〕　計0件

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関