

DNCT: 人工知能時代における資産の自然法則的証明のためのフレームワーク

人工的に生成される情報の時代に向けた、資産の検証可能な自然法則的証拠の提案

DNCT (Research Initiative) — <https://dnct.org>

Hirosato Matsuura【松浦弘智】hiro@dnct.org (mtzhiro@gmail.com)

文書の位置づけ: 概念的研究提案。実験によって検証済みの認証標準ではない。

要旨

人工知能(AI)の進歩に伴い、物体、文書、本人確認情報などのデジタル表現を生成・変更・配布する能力が高まっている。暗号技術やデジタル認証は情報セキュリティにおいて不可欠であるが、デジタル上の証拠だけで、対応する物理的物体の存在、組成、真正性が必ず証明されるわけではない。また、計算機による暗号技術の長期的な安全性は、数学的な前提、実装品質、鍵管理、攻撃者が利用できる能力に依存する。近年、AIによる暗号解読リスクも取りざたされている。

本稿では、測定可能な物理的特性と再現可能な検証手順によって、自然法則に関する特定の主張を補強する概念的フレームワークとして“DNCT”を提案する。この構想では、規格化された物理的・化学的基準物体、専用ケース、校正された測定、必要に応じたデジタル認証記録を組み合わせた手法を具体的に提案する。

DNCTは暗号認証を置き換えるものではなく、それを補完することを意図している。製造時の物理的ばらつきを利用して機器固有の指紋を生成する物理的複製困難関数(PUF)とは異なる方式である[2, 11]。DNCTは、明示的に定めた物理的・化学的仕様と、独立した検証者が調査・再現できる手順を出発点とする。本構想は、物理的物体が偽造不可能であるとも、質量と体積だけで材質を証明できるとも仮定しない。構想の評価に必要な測定、脅威モデル、公差、独立した試験を明確にすることを目的とする。

本稿の目的は、フレームワークを定義し、その前提と限界を明らかにし、実験的検証に向けた研究計画を提示することである。

キーワード: DNCT、自然法則的証明、人工知能、物理的検証、デジタル認証、偽造、偽札、暗号、セキュリティ、銀行、お金、紙幣、硬貨、密度、体積、重量、白金、金、ケース、化学組成。

1. はじめに

デジタルシステムは、金融取引、本人確認、所有権記録、通信、情報交換など、現代社会の多くの場面を支えている。暗号署名や安全な通信プロトコルは、これらのシステムに不可欠な要素である。しかし、物理的な物体を表すデジタル情報は、必ずしもその物体そのものと同一ではない。コインの写真は、そのコインが実際に存在することを立証せず、デジタル記録だけでは資産が物理的に存在することを独立して証明できない。

AIによって、説得力のあるデータ、記録、暗号化された情報、合成画像、文書、その他を生成・解読しやすくなったことから、この区別はさらに重要になっている。こうした進歩は、デジタル情報が本質的に信頼できないことを意味しない。むしろ、デジタル表現の見た目や出所とは独立して主張を検証できる手段の価値を示している。

Bitcoinの設計論文は、技術的提案において、bitcoin.org にて問題を定義し、前提を示し、仕組みを説明し、限界を論じる構成した[1]。これに習い、我々の提案 DNCT【/'dɛ·n·sɪ·ti /】(英単語: density {密度} から派生)もサイト dnct.org で提案・定義・試験等をする。

DNCTの基本原則は次のとおりである。

可能な限り、物理世界に関する主張は、物理世界において自然法則の下に独立に調査・測定できる証拠によって裏づけられるべきである。

2. 計算機暗号と長期的な安全性の不確実性

現代の暗号システムは、特定の数学的問題を計算によって解くことの困難さに依存している場合が多い。RSAは十分に大きな整数の素因数分解の困難さに依存し、楕円曲線暗号(ECC)は楕円曲線群に関する数学的問題に依存する。SSL/TLSなどの安全な通信システムや、PGPなどの暗号ツールは、複数のアルゴリズムを組み合わせ、機密性、認証、データの完全性を実現する。

これらの技術は今後も不可欠である。しかし、その安全性は、選択されたアルゴリズムとパラメーター、実装品質、秘密鍵の保護、プロトコル設計、攻撃者が利用できる能力などの条件に依存する。NISTのデジタル署名および鍵管理に関する文書は、これらの分野における正式な指針を提供している[4, 5]。

AIは、数学的推論、コード解析、アルゴリズム発見、実装上の脆弱性の特定を支援する可能性がある。しかし、こうした進歩が自動的に現代の暗号を破れることを意味するわけではない。科学的に慎重な主張は、将来の進歩によって攻撃の実質的な困難さが変わり得るため、技術の変化に応じて安全性の前提を再評価する必要がある、というものである。

量子コンピューティングは、これとは区別すべき問題である。Shorは、十分な能力を持つ量子コンピューター上で整数の素因数分解と離散対数計算を行うアルゴリズムを示した[3]。この結果は、大規模で耐故障性を持つ量子コンピューターが実用化された場合、従来型のRSAやECCが脅かされる可能性を意味する。しかし、現在、あらゆる既存システムを解読できる量子コンピューターが利用可能であることを示すものではない。NISTによる耐量子暗号標準の策定は、将来的な脅威に対する重要な対応である[6]。

一方で、暗号通貨開発企業 Ethereum で働く研究者Justin Drake は2026年10月07日に次のように述べている「AIの進化や長年の数学的仮説の崩壊を背景に、ECDSA(楕円曲線暗号)が従来の予想をはるかに超えるスピードで破られる可能性が浮上している。(原文: Recent breakthroughs—catalyzed by AI advancements and the collapse of long-standing mathematical hypotheses—raise the alarming possibility that ECDSA (elliptic curves) could be broken much faster than previously expected.)」[7]。OpenAIのHuggingFace攻撃事件だけ取り上げても[8]、人間がすでにAIがコントロール不能に陥るリスクに直面していることは明らかで、こうしたことへの安全性の工夫・技術が必要である。

DNCTは、暗号技術を放棄すべきだとも、AIが必然的に暗号を破るとも主張しない。むしろ、物理的な主張の一部について、デジタル暗号方式の安全性が将来も維持されるという前提だけに依存しない、追加的な証拠の源を利用できないかを検討する。また、最悪AIの暴走等により、電氣的・電磁的検証能力が失われたとしても、アナログ的な手法で確認がとれる手段を維持することも提案する。

長期的な検証フレームワークは、その前提を明示し、可能な場合には、単一の信頼の仕組みだけに全面的に依存しない設計を目指すべきである。

3. DNCTの基本原則

DNCTは、次の3要素を結びつける自然法則に基づいたフレームワークを提案する。

1. 物理的な基準物体：公開された仕様を持つ物体。
2. 再現可能な検証手順：独立した検証者が実行できる手順。
3. 任意のデジタル記録：仕様、識別番号、来歴情報、検査履歴などを記録する仕組み。

物理的物体は、特定の主張を検証するための実体ある基準を提供する。デジタル記録は文書化と情報伝達を支えるが、物体が記述どおりであることを単独で立証するものではない。

この提案は、物理的認証に関するより広い研究分野と関連している。例えばPUFの研究は、製造時のばらつきを機器固有の物理的指紋として利用する方法と、それらの方式に対する攻撃やモデル化の可能性を扱っている[2, 11]。DNCTは、予測困難な製造上の指紋を主な根拠とするのではなく、明示的に定めた測定可能な仕様と、反復可能な検査手順を出発点とする。

この違いは設計上の仮説であり、実証済みの安全性上の優位性ではない。どの方式が特定の用途に適しているかを判断するには、比較評価が必要である。

4. 基準物体:CT100の構想

説明用の試作案として、DNCTは**CT100**または**D100**と仮称する規格化されたコイン状の金属物体を提案する。

想定する基準仕様は次のとおりである。

- 公称質量:100グラム
- 基準材料:白金。純度要件は別途定義する。
- 基準密度:室温付近の白金について約21.45 g/cm³
- 公称直径:5.0cm
- 推定体積:約4.66 cm³
- 理想的な円柱形状における推定厚さ:約0.237cm

これらの値は、指定した質量と基準密度を持つ理想的な円柱形状として幾何学的に整合している。ただし、設計計算であり、実験結果ではない。実際に製造する場合は、公差、純度、表面仕様、校正された測定手順、測定不確かさの推定値を明確に定義する必要がある。

CT100の形状は、認められた計量学の原則に基づいて評価する必要がある。『測定における不確かさの表現のガイド』は、測定不確かさを評価し報告するための枠組みを提供する[9]。

CT100はDNCTの検討に用いる例であり、完成した製品や認証済み標準ではない。別の基準材料や形状も検討対象となり得る。

5. 検証用ケース(箱)

提案する物体は、専用設計の透明なホルダーまたは円筒形のケース(箱)に収め、隙間なくきっちり蓋をすることができる。その目的は、検査時の位置を一定にし、寸法検査を容易にし、反復可能な測定のためのインターフェースを提供することである。

公称体積約4.66 cm³の内部空間は、提案する基準体積に対応する。ただし、実用的な設計では、製造公差、出し入れ、熱膨張、表面の不規則性、材料の変形を考慮しなければならない。文字どおり隙間のない構造が実用的であるとは、試験なしに仮定できない。

ケースと物体と一緒に計量する場合、ケースの質量を既知かつ管理されたものにするか、妥当性が確認された手順によって考慮する必要がある。ケース自体を物体の組成の証明とみなしてはならない。透明であることだけで、高度なすり替えや改ざんを防止できるわけではない。

将来の設計では、改ざん検知用の封印、固有識別番号、文書化された検査手順を組み込むことが考えられる。ただし、それらが想定した脅威に対して有効な保護を提供するかどうかは、試験によって評価する必要がある。

6. 物理測定と材質検証

質量と寸法の測定は、初期的な整合性確認に利用できる。測定した質量と推定体積が基準仕様と一致しない場合、製造不良、異なる材料、損傷、または測定誤差などが考えられる。

一方、質量と体積が一致していても、材質の組成を一意に証明することはできない。異なる材料や複合構造でも、全体として類似した物理的特性を持つ場合がある。偽造物が内部構造や複数の材料を組み合わせ、期待される測定値に近づける可能性もある。

より強い検証手順では、次の方法を組み合わせることが考えられる。

- 校正された機器による質量測定。
- 寸法測定と体積の推定。
- 蛍光X線分析など、目的に適した材質組成の検査。
- 脅威モデルに応じた内部構造の検査。
- 表面、識別番号、封印の検査。
- 来歴と保管・受け渡し記録の確認。
- 純度について高い確度が必要な場合の独立した試験所による分析。

どの方法も、あらゆる状況で決定的なものではない。例えば表面分析だけでは、物体全体の組成を立証できない場合がある。そのため、試験所の能力と測定手順の信頼性も重要である。ISO/IEC 17025は、試験所および校正機関に対する国際的に認められた要求事項を定めている[10]。既述したように質量検査だけでは不明な時は、蛍光X線分析などの手法を用いる。

DNCTは、基本的な密度検査に合格したことを決定的な認証として扱うのではなく、実際に実施した試験と各試験の限界に応じて、検証の確度を定義すべきである。

7. デジタル検証と物理的検証の組み合わせ

DNCTは、既存のデジタルセキュリティを補完することを意図している。デジタルシステムは識別番号の記録、仕様の公開、検査履歴の管理、署名付き記録の認証などを担う。物理的な手順は、提示された物体が指定された測定可能な特性に適合しているかを検査する。

例えば、デジタル署名付き記録にコインの基準仕様と申告された来歴を記載することができる。検査者は実物を測定し、結果をその仕様と比較する。デジタル署名は記録の完全性を保護する助けとなり、物理検査は物体そのものに関する特定の主張を評価する。デジタル署名と鍵管理については、NISTの指針が関連する背景を提供する[4, 5]。

この2つの層を混同してはならない。有効な署名は、物理的物体が本物であることを証明しない。特定の検査に合格した物体も、それだけで法的所有権、市場価値、資金の償還請求権、保管を主張する機関の支払能力を証明するわけではない。

したがってDNCTの目的は、あらゆる信頼を包括的に保証することではない。独立して再現可能な証拠を用い、特定の物理的な主張を補強する方法を提案することである。

8. 検証を支援するAI

AIは、測定データの分析、異常の発見、画像比較、記録の確認、独立した観測結果の不整合の検出などを通じて、DNCTの検証作業を支援できる可能性がある。

しかし、AIが生成した結論を、それ自体で決定的な証拠として扱うべきではない。信頼できる手順では、入力、方法、不確かさ、失敗条件を記録する必要がある。可能であれば、独立した測定や別の技術によって結果を再現できるようにする。

AIは証拠の解釈を支援できるが、物理的証拠や、独立した検証者が物体を検査する能力に取って代わるべきではない。ただ、究極的にはAIや機械、電気、デジタルに頼らずに人間がその目で検証ができることも必要だ。

9. 脅威モデルと限界

DNCTの実装では、対象とする脅威を明示する必要がある。例えば、次の脅威が考えられる。

- 偽造または改変されたデジタル記録。
- 実物に対応していないデジタル表現。
- 外見上の特徴が似た物体へのすり替え。
- 複合材料や積層構造を利用した偽造。
- ケース、封印、識別番号、測定機器への干渉。
- 測定、製造、文書化、校正における誤り。
- 製造者、認証者、保管者、検査者間の共謀。

物理的認証に関する研究は、物理的なセキュリティ機構にも慎重な脅威分析が必要であり、モデル化、複製、その他の攻撃に対して脆弱な場合があることを示している[2, 11]。DNCTも完全な安全性を仮定するのではなく、現実的な攻撃者を想定して評価しなければならない。

単一の測定であらゆる脅威を排除できるとは想定しない。フレームワークの安全性は、物体の仕様、実施する試験、検証の独立性、関係者や機関の誠実性に依存する。

DNCTは絶対的な偽造耐性を主張しない。特定の主張を検査しやすくし、問題を検出しやすくし、検証手順の透明性を高めることを目指す。

今後数十年(2060年代まで?)究極のセキュリティは自然法則そのものにあるはず。AIや超知能も自然法則に力を及ぼすことは当分はできないはず。

10. 研究と検証のロードマップ

DNCTを信頼できる認証標準として扱うには、実証的な試験が必要である。

研究計画には、次の項目を含める。

1. 仕様設計: 材質、寸法、質量、純度、公差、製造要件を定義する。
2. 測定手順: 認められた計量学の原則に基づき、校正された方法を確立し、不確かさを定量化する[9]。
3. 偽造試験: 想定可能な代替材料や複合構造を試験する。
4. ケースと封印の評価: 耐久性、改ざん検知、再現性、実用性を評価する。
5. 独立した再現試験: 独立した試験所や研究者に試験を再現してもらう。
6. デジタル統合: 識別番号、署名付き記録、来歴、検査履歴の管理方法を定義する。
7. 脅威モデルの公開: 前提、既知の弱点、各試験が提供する保証の範囲を文書化する。
8. 外部評価: 強い安全性の主張を行う前に結果を公開し、批判的な評価を募る。

報告には、失敗した試験、測定不確かさ、限界を含めるべきである。偽造検出率を主張する場合は、代表性のある実験と独立した評価によって裏づけなければならない。また我々は成果をできるだけオープンソース・オープンデータとして公開する。

11. 想定される応用分野

検証と適切なガバナンスを前提として、DNCTは次の分野で研究できる可能性がある。

- 規格化された物理的物体の認証。
- 申告された組成や寸法が重要な収集品・物体。
- 教育や研究における物理的検証。
- 特定の資産記録に対する補完的な確認。
- 物理的検査とデジタル認証文書を組み合わせたシステム。

金融分野への応用には、さらに慎重な検討が必要である。金属物体が本物であることは、市場価値、法的権原、所有権、償還請求権、保管機関の財務状態を証明するものではない。資産や顧客資金を保管するサービスには、別途、法務、運用、規制上の分析が必要である。

結論

AIは、デジタル表現が物理世界を正確に反映しているかを判断するうえで、新たな課題を生み出す。暗号技術は依然として不可欠だが、その安全性は特定の数学的前提、実装、鍵管理、技術的条件に依存しており、継続的に評価する必要がある。

DNCTは、補完的なフレームワークを提案する。すなわち、物理的物体に関する特定の主張を、測定可能な特性、標準化された手順、独立して再現可能な証拠によって支えることである。CT100として提案した物体とケースは、実験を始めるための具体例であり、真正性を完全に証明するものではない。

このフレームワークの価値は、今後の研究課題である。その信頼性は、透明な仕様、現実的な脅威モデル、厳密な試験、限界の文書化、独立した再現試験によって評価されるべきである。

長期的な目標は、信頼をなくすことではなく、信頼をより検証可能なものにすることである。

この文章を書くにあたって、基本的なアイデアを書いた後は、大半はAIに作業をゆだねた。書きあがったのちにおかしなところはチェックしたが、人間から見ると人間の本当にしたいようには書いてくれない部分もあったことをここに人間の手によって記しておく。一部は人間により修正され、また、最終版はAIのチェックを通さずに最後のバージョンとしている。

DNCT (Research Initiative)

<https://dnct.org>

参考文献

[1] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."

<https://bitcoin.org/bitcoin.pdf>

[2] Gao, Y., Al-Sarawi, S. F., & Abbott, D. (2020). "Physical unclonable functions." *Nature Electronics*, 3, 81–91.

<https://doi.org/10.1038/s41928-020-0372-5>

[3] Shor, P. W. (1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 124–134.

<https://doi.org/10.1109/SFCS.1994.365700>

[4] National Institute of Standards and Technology. (2023). *Digital Signature Standard (DSS)*. FIPS PUB 186-5.

<https://doi.org/10.6028/NIST.FIPS.186-5>

[5] Barker, E. (2020). *Recommendation for Key Management: Part 1 – General*. NIST Special Publication 800-57 Part 1, Revision 5.

<https://doi.org/10.6028/NIST.SP.800-57pt1r5>

[6] National Institute of Standards and Technology. (2024). *Post-Quantum Cryptography Standards: FIPS 203, FIPS 204, and FIPS 205*.

<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>

[7] Justin Drake (2026), "(A Warning to the Blockchain Industry: Planning for "Bunker Mode" in the Age of AI)" (firefly.social)

<https://firefly.social/post/x/2107837081313505768>

[8] Maxwell Zeff and Lily Hay Newman (2026) , “ What We Still Don’t Know About OpenAI’s Hugging Face Hack ” *WIRED* .

<https://www.wired.com/story/openais-hugging-face-hack-debrief-raises-more-questions-than-it-answers>

[9] Joint Committee for Guides in Metrology. (2008). *Evaluation of Measurement Data — Guide to the Expression of Uncertainty in Measurement*. JCGM 100:2008.

<https://doi.org/10.59161/JCGM100-2008E>

[10] International Organization for Standardization & International Electrotechnical Commission. (2017). *ISO/IEC 17025:2017 — General Requirements for the Competence of Testing and Calibration Laboratories*.

<https://www.iso.org/standard/66912.html>

[11] Babaei, A., & Schiele, G. (2019). “Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges.” *Sensors*, 19(14), 3208.

<https://doi.org/10.3390/s19143208>

免責事項:本書は概念的な研究フレームワークを提示するものである。検証済みの認証標準ではなく、いかなる物理的物体の真正性を認定するものでもない。偽造耐性を保証するものではなく、金融・投資助言を構成するものでもない。

© 2026 Hirosato Matsuura. This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

AI Usage Disclosure: During the preparation of this work, the authors used ChatGPT 5.6 Luna developed by OpenAI .



https://docs.google.com/document/d/e/2PACX-1vR4yBtgEBe-aySFy5_Ymg566TwqfLd-3CqT9uwPXZVAekAMZidV7NqDwp-ERWRVw7Blf1DbDCcuP7om/pub

<https://docs.google.com/document/d/1xt5WSEaT4i3IENZnlLefJaLCU3HFXEuGHaADSDuf7xM/edit?usp=sharing>