VeritasChain Standards Organization (VSO)

XOR完全性不変量
技術解説資料

デジタル証拠における「削除検出」問題を解決する暗号学的アプローチ

文書名	XOR完全性不変量（XOR Completeness Invariant）技術解説資料
対象技術	Content Provenance Protocol (CPP) v1.5 - Completeness Invariant
実装製品	VeraSnap - 暗号学的証拠キャプチャアプリケーション
発行者	VeritasChain Co., Ltd.（東京都）
IETF I-D	draft-vso-cpp-core-00
学術論文	DOI: 10.5281/zenodo.18455556（Zenodo、5機関検証済）
発行日	2026年2月6日
分類	プレス配布用 / Press Use

エグゼクティブサマリー

XOR完全性不変量は、デジタル証拠の「完全性」を暗号学的に保証する技術です。従来の暗号学的手法（ハッシュチェーン、Merkle Tree、デジタル署名）が個々のデータの「改ざん検出」に優れる一方、データセットからの選択的削除（オミッション攻撃）を検出する手段は存在しませんでした。

XOR完全性不変量は、XOR演算の数学的特性を活用し、O(1)の計算量でデータセット全体の完全性を検証可能にします。ISO/IEC 27037が定める電子証拠の4要件（真正性・正確性・完全性・整合性）のうち、唯一暗号学的解決策が存在しなかった「完全性」問題に対する画期的なアプローチです。

1. デジタル証拠の「完全性」問題

1.1 既存技術の限界

デジタルフォレンジクスの分野において、ISO/IEC 27037は電子証拠が満たすべき4つの要件を定義しています。このうち「真正性」「正確性」「整合性」については、暗号学的ハッシュ関数やデジタル署名といった確立された技術により十分に対処されています。しかし、「完全性」（証拠が欠落なく揃っていること）を暗号学的に保証する手段は、これまで存在しませんでした。

1.2 既存暗号技術の比較

技術	主目的	改ざん検出	削除検出	検証計算量	プライバシー
ハッシュチェーン	順序保証	O	X	O(n)	X
Merkle Tree	包含証明	O	X	O(log n)	Triangle
デジタル署名	真正性保証	O	X	O(1)	O
XOR完全性不変量	完全性保証	0	0	0(1)	0

※ XOR完全性不変量は上記既存技術を「置き換える」ものではなく、「補完する」技術です。CPP v1.5では多層防御アーキテクチャとしてこれらを組み合わせています。

1.3 オミッション攻撃の脅威

オミッション攻撃（選択的削除攻撃）とは、不都合な証拠のみを選択的に削除し、残った証拠はすべて正当な暗号学的署名を保持したまま提出する攻撃手法です。例えば、保険金請求において100枚の現場写真のうち被害が軽微であることを示す写真を削除し、被害が深刻に見える写真のみを提出するケースが該当します。

> **オミッション攻撃の具体例**
> 攻撃前： 写真1[署名OK] + 写真2[署名OK] + 写真3[署名OK] + 写真4[署名OK]
> 攻撃後： 写真1[署名OK] + 写真3[署名OK] + 写真4[署名OK]
> 結果 ： 写真2が削除されたが、残りの署名はすべて有効 → 従来技術では検出不可能

2. XOR完全性不変量の技術的仕組み

2.1 XOR演算の数学的特性

XOR（排他的論理和）演算には、完全性検証に最適な4つの数学的特性があります。

特性	数式	完全性不変量への応用
交換法則	A XOR B = B XOR A	検証順序が結果に影響しない
結合法則	(A XOR B) XOR C = A XOR (B XOR C)	増分計算が可能（中間結果不要）
単位元	A XOR 0 = A	初期値からの構築が容易
自己反転性	A XOR A = 0	削除検出の数学的基盤

2.2 不変量の生成メカニズム

完全性不変量の計算式

$$Hash\_Sum = H(E1) \text{ XOR } H(E2) \text{ XOR } H(E3) \text{ XOR } \ldots \text{ XOR } H(En)$$

※ H() = SHA-256 暗号学的ハッシュ関数、XOR = 排他的論理和演算
※ E1 ~ En = 各キャプチャイベント（写真・動画等の証拠データ）

各証拠アイテムのSHA-256ハッシュ値をXOR演算で累積集約し、256ビットの完全性不変量を生成します。この不変量はRFC 3161準拠の外部タイムスタンプ局（TSA）によりタイムスタンプされ、改ざん不可能な状態で保存されます。

2.3 削除検出の原理

削除検出の仕組み

正常状態：
期待値 I = H(E1) XOR H(E2) XOR H(E3) XOR H(E4)
検証値 I = H(E1) XOR H(E2) XOR H(E3) XOR H(E4)
結果：I = I → 完全性 OK

E2が削除された場合：
期待値 I = H(E1) XOR H(E2) XOR H(E3) XOR H(E4)
検証値 I' = H(E1) XOR H(E3) XOR H(E4)
結果：I != I' → オミッション攻撃を検出

重要な特性として、この検証はプライバシー保護型です。検証者は完全性不変量の値のみを比較するため、個々の証拠アイテムの内容を確認する必要がありません。これはGDPR等のプライバシー規制に対応した設計です。

2.4 CPP v1.5における実装

Content Provenance

Protocol（CPP）v1.5では、XOR完全性不変量は4層セキュリティアーキテクチャの一部として実装されています。

層	機能	技術	検出対象

Layer 1	イベント整合性	SHA-256 + ECDSA P-256	個別データの改ざん
Layer 2	完全性保証	XOR完全性不変量	選択的削除（オミッション）
Layer 3	時間アンカー	RFC 3161 TSA	タイムスタンプ偽造
Layer 4	発行者認証	Secure Enclave署名	なりすまし・偽造

3. 学術的背景と独立検証

3.1 学術的基盤

XOR完全性不変量の理論的基盤は、MIT（マサチューセッツ工科大学）のClarke, Devadas, van Dijk, Gassend, Suhによる「Incremental Multiset Hash Functions and Their Application to Memory Integrity Checking」（ASIACRYPT 2003）に遡ります。この研究は、XORベースのアキュムレータが暗号学的ハッシュ出力上で構築された場合にセット衝突耐性を提供することを証明しました。

XOR完全性不変量は、この基礎理論を「デジタル証拠の完全性検証」という新しい応用ドメインに適用したものです。従来のメモリ整合性チェックとは異なり、オミッション攻撃の検出とプライバシー保護型検証を主目的とする点が技術的な差別化要因です。

3.2 Zenodo学術論文と独立検証

> 学術論文情報
> DOI: 10.5281/zenodo.18455556
> タイトル: XOR-Based Completeness Invariants in Digital Forensics
> プラットフォーム: Zenodo（CERN運営）
> 検証状況: 5つの独立機関による検証済み

3.3 IETF標準化

Content Provenance Protocol（CPP）は、IETF Internet-Draft（draft-vso-cpp-core-00）として公開されています。これは、XOR完全性不変量を含むプロトコル全体が国際標準化のプロセスに入っていることを意味します。IETFへの提出は、プロトコルの技術的妥当性に関する独立した評価プロセスを提供するものであり、技術の信頼性を裏付ける重要なマイルストーンです。

3.4 C2PA標準との関係

C2PA（Coalition for Content Provenance and Authenticity）は、Adobe, Microsoft, Google等が推進するコンテンツ来歴標準です。C2PAは個々のメディアファイルの来歴追跡に優れますが、データセット全体の完全性保証（オミッション攻撃検出）は仕様範囲外です。

CPPおよびXOR完全性不変量は、C2PAを「補完」する技術として位置づけられています。VeraSnapは、CPPで生成した証拠をC2PA形式にエクスポートする機能を備えており、両エコシステムの相互運用性を実現しています。

比較項目	C2PA	CPP / XOR完全性不変量
主な目的	メディアファイルの来歴追跡	証拠セットの完全性保証
推進組織	Adobe, Microsoft, Google等	VeritasChain (VSO)
オミッション攻撃検出	非対応	対応
外部タイムスタンプ	オプション	必須（RFC 3161）
生体認証バインド	非対応	対応（ACEパターン）
関係性	コンテンツ来歴の事実上の標準	C2PAを補完するフォレンジック層

4. VeraSnapにおける実装

4.1 製品概要

VeraSnap（VeritasChain Co., Ltd.開発）は、CPPの世界初の商用実装として2026年1月16日にリリースされました。App Storeにおいて175カ国で配信中であり、10言語に対応しています。

項目	詳細
製品名	VeraSnap - Cryptographic Evidence Capture
開発元	VeritasChain Co., Ltd.（東京都）
プラットフォーム	iOS（配信中） / Android（開発中、Kotlin）
配信地域	175カ国、10言語対応
準拠プロトコル	Content Provenance Protocol (CPP) v1.5
署名アルゴリズム	ECDSA P-256 (ES256) / Apple Secure Enclave
ハッシュアルゴリズム	SHA-256
タイムスタンプ	RFC 3161準拠（複数TSAフォールバック対応）
反スプーフィング	LiDARベーススクリーン検出
生体認証	Face ID / Touch ID（ACEパターン）

4.2 XOR完全性不変量の実装フロー

VeraSnapでは、以下のフローでXOR完全性不変量を生成・検証します。

ステップ	処理内容	技術的詳細
1	証拠キャプチャ	カメラで写真/動画を撮影。生体認証で人間の存在を確認
2	正規化	RFC 8785 (JCS) に準拠しメタデータをJSON正規化
3	ハッシュ計算	正規化されたイベントデータのSHA-256ハッシュを計算
4	XOR累積	runningHashSum = XOR(runningHashSum, eventHash)
5	不変量確定	チェーン完了時に不変量をシール。カウント・タイムスタンプを記録
6	外部タイムスタンプ	RFC 3161 TSAにより不変量に第三者タイムスタンプを付与
7	検証	再計算した不変量と保存値を比較。不一致で削除を検出

4.3 セキュリティ上の考慮事項

XOR完全性不変量には既知のセキュリティ上の制約があり、CPP v1.5ではこれらに対する対策が実装されています。

脅威	概要	CPPでの対策
XHASH攻撃	ガウス消去法による不変量偽造	セットサイズ上限の設定
自己逆元攻撃	偶数重複の検出不能	ユニークID強制・ノンス付加
リプレイ攻撃	過去の正当な値の再利用	RFC 3161外部タイムスタンプ必須化

ソフトウェア改ざん	不変量計算の改ざん	Secure Enclave内での計算

> 重要：XOR完全性不変量は、オミッション攻撃検出のための「診断ツール」であり、それ単体で暗号学的証明を構成するものではありません。CPP v1.5の多層防御アーキテクチャの一部として、他のセキュリティ層と組み合わせて使用されることを前提としています。

5. 応用分野と社会的インパクト

5.1 ターゲット産業

産業	課題	XOR完全性不変量の適用
保険	保険金請求写真の選択的提出	現場写真セットの完全性を暗号学的に保証
法務	法的証拠の改ざん・欠落	証拠チェーンの完全性検証による裁判証拠の信頼性向上
建設	施工記録写真の不正操作	工程写真の全数撮影を暗号学的に証明
金融	監査ログの選択的削除	MiFID II RTS 25等の規制遵守監査に対応
ジャーナリズム	報道写真の信頼性確保	取材現場での証拠キャプチャの完全性を保証
不動産	物件調査記録の改ざん	地面師詐欺対策：現地調査証拠の完全性証明

5.2 規制環境との整合性

XOR完全性不変量は、以下の国際規制・標準に対応した技術基盤を提供します。

規制/標準	要件	XOR完全性不変量の貢献
EU AI Act 第50条	AI生成コンテンツの機械可読な来歴表示	AI出力の生成・拒否ログの完全性保証
ISO/IEC 27037	電子証拠の真正性・正確性・完全性・整合性	「完全性」要件に対する暗号学的解決策
GDPR第32条	処理のセキュリティ確保	プライバシー保護型検証（内容非開示）
MiFID II RTS 25	注文記録の完全保存	監査ログの選択的削除検出

5.3 基本原則：Provenance ≠ Truth

> 「来歴は真実を意味しない」
> XOR完全性不変量およびCPPは、証拠が「いつ・どこで・どのように」キャプチャされたかを暗号学的に証明します。しかし、キャプチャされた内容が「真実」であるかどうかは証明しません。これは意図的な設計上の制約であり、法的な誤用を防ぐための重要な原則です。

6. まとめ

XOR完全性不変量の意義

XOR完全性不変量は、デジタル証拠における「完全性」問題に対する初めての実用的な暗号学的解決策です。

1. 技術的革新性 - 既存の暗号学的手法では検出不可能だったオミッション攻撃を、O(1)の計算量で検出可能にした初のプロダクション実装
2. 学術的裏付け - MIT (ASIACRYPT 2003) の理論的基盤に基づき、Zenodo学術論文（5機関検証済）およびIETF Internet-Draftとして公開
3. 実用的実装 - VeraSnapとして175カ国で配信中。ハードウェアセキュリティ（Secure Enclave）と外部タイムスタンプ（RFC 3161）を組み合わせた多層防御アーキテクチャ
4. 社会的インパクト - EU AI Act、ISO/IEC 27037等の国際規制に対応し、保険・法務・建設・金融等の多様な産業でのデジタル証拠信頼性向上に貢献

7. 参考文献・リファレンス

学術論文

Clarke, Devadas, van Dijk, Gassend, Suh. "Incremental Multiset Hash Functions and Their Application to Memory Integrity Checking." ASIACRYPT 2003.

Bellare, M. & Micciancio, D. "A New Paradigm for Collision-Free Hashing: Incrementality at Reduced Cost." EUROCRYPT 1997.

VeritasChain. "XOR-Based Completeness Invariants in Digital Forensics." Zenodo. DOI: 10.5281/zenodo.18455556.

標準・仕様

Content Provenance Protocol (CPP) v1.5 - github.com/veritaschain/cpp-spec

IETF Internet-Draft: draft-vso-cpp-core-00

RFC 3161 - Internet X.509 PKI Time-Stamp Protocol (TSP)

RFC 8785 - JSON Canonicalization Scheme (JCS)

C2PA Technical Specification v2.2

規制

EU AI Act - Regulation (EU) 2024/1689 (Article 50)

ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition and preservation of digital evidence

GDPR - Regulation (EU) 2016/679 (Article 32)

お問い合わせ
VeritasChain Co., Ltd.
Web: https://veritaschain.org
VeraSnap: https://veritaschain.org/vap/cpp/verasnap
GitHub (CPP): https://github.com/veritaschain/cpp-spec
Apple ID: developers@veritaschain.org