【発明の名称】有限閉包センサーシステムおよび同期鍵生成装置
【特許内容の概要】
本装置は、センサー出力の時間信号を解析し、同期状態（meaning 一致）が成立したときにだけ暗号鍵を生成する仕組みを持ちます。時系列信号に対して窓処理・差分・自己相関・モジュラ変換などの多段前処理を施し、その出力から候補スコア列を作ります。次に L1 ノルム・選択数・一意マージン Δ などの制約のもとで重要な信号成分を自律的に選択します。この構造は「GD-Attention（Ghost Drift Attention）」と呼ばれ、有限エネルギー内で最も一貫した共鳴を検出します。同期が確実に成立したときだけ、鍵導出関数（KDF）が起動します。同期判定には上包絡 E_upper・余裕 δ・連続成立長 τ を用い、指標 S が E_upper＋δ を τ 連続で上回ったときに“共鳴成立”と認定されます。この条件を満たすと、KDF が動き、PUF（物理的複製困難関数）と真性乱数（TRNG）から一度きりのセッション鍵 SK を生成します。つまり、この装置は「物理的に意味が一致した瞬間にだけ鍵が出る」仕組みです。装置はタンパ検知・副チャネル監視を備え、異常検知時には即時ゼロ化を実行。鍵や中間値を完全に消去します。また周期入力に対しては ラップ検出とアンラップ補正 を自動で行い、常に Δ の一意性を確認しながら安全に判定を継続します。複数デバイスが M-of-N 合議 で同期成立を確認する仕組みも備えています。全装置が相互に**SYNC_PROOF（同期証跡）**を交換し、合議が成立したときにのみ全体鍵を生成。一台でも異常があれば全体が止まる、という構造です。これにより、攻撃・誤作動・改ざんに対する耐性が極めて高くなります。装置は 監査ログ を自動記録し、時刻・デバイス ID・上包絡・δ・τ・ハッシュを追跡可能。固定小数点演算や飽和処理によって数値安定性を確保しています。この構造はすでに Ghost Drift 理論の「有限閉包エネルギー原理」をハードウェア上で実装した最初の例といえます。
【技術分野】
【０００１】
本発明は、信号処理および暗号技術に関し、特にセンサー出力に基づき動的に同期イベントを検出し、当該イベントに応じて鍵導出を制御する装置および方法に関する。さらに、本発明は、GD-Attention（Ghost-Drift Attention）構造を用いた有限エネルギー領域内での特徴選択および鍵導出の安全化処理に関し、暗号モジュール、ハードウェアセキュリティモジュール（HSM）、および IoT センサー等への応用に適する。
【背景技術】
【０００２】
従来、各種センサー（加速度、振動、音響、電磁、化学等）から得られる時系列信号に対し、イベント検出・同期確立・通信保護を一連で扱うために、前処理（フィルタリング、差分化、自己相関、スペクトル解析等）としきい値判定を組み合わせる技術が用いられてきた。これらは比較的軽量でリアルタイム実装に適する一方、環境ドリフトやノイズの非定常性、周期信号の位相巻き込み（wrap）などにより誤検出・見逃しが発生しやすいという課題がある。
【０００３】

鍵配布の領域では、TRNG（真性乱数生成器）やPUF（物理的複製困難関数）を情報源としてKDF（鍵導出関数）に入力し、セッション鍵を生成する方式が知られている。しかし、センサー由来の「同期成立」を正確に検出できない場合、KDFを開始すべきでないタイミングで鍵生成が走り、側信道解析の観点でも望ましくない処理が発生し得る。さらに、従来はイベント検出系と暗号鍵導出系が疎結合であり、判定の一意性や連続性が鍵導出のゲートに厳密に結び付いていない。

【０００４】

イベント検出の高精度化に向けて、テンプレートマッチング、CUSUM／SPRT型の逐次判定、機械学習を用いた分類器等も提案されているが、学習データの準備や計算資源の確保を要し、エッジ側（低消費電力デバイス）では適用が難しい場合が多い。また、複数候補からの選択において「上位候補間の差が十分離れていること（マージンの確保）」を保証できず、しきい値超過だけで誤って起動条件を満たす事例が残る。

【０００５】

セキュリティの観点では、サイドチャネル（消費電力・電磁放射・タイミング）対策やタンパ（改ざん）検知は周知であるが、検知結果を鍵導出の可否に即時かつ不可逆に反映し、同時に監査ログとして残す統一的な枠組みは十分に整備されていない。とりわけ、検知直後のゼロ化（鍵・中間値の消去）と起動ゲートの閉止を確実に連動させる設計は、実装依存のばらつきが大きい。

【０００６】

IoT／産業センサーの大規模展開においては、演算・エネルギー・レイテンシの上限が厳しく、検出処理・選択処理・暗号処理を「有限のリソース枠」に収める設計が不可欠である。従来の多段判定や学習器を組み合わせた方式は、最悪時の演算量が読みにくく、所要電力量や応答時間の確約を与えにくい。

【０００７】

また、周期性をもつ観測（回転体、AC電源、周期振動など）では、位相の巻き込みにより特徴量が同値類に写ってしまい、真の一致と偽一致の識別が難しくなる。一般的なアンラップ補正はヒューリスティックに依存し、軽量実装では安定性に欠ける場合がある。

【０００８】

通信プロトコル面では、PQ（耐量子）KEMや電子署名、リモートアテステーションの採用が進む一方、これらを「同期イベント成立」という物理世界の条件と安全に結び付け、鍵そのものを外部に出さずに合意確認を行う手順（例：ハッシュによる確認）を一貫して適用する設計は、システム横断で未だ統一されていない。

【０００９】

以上のように、（i）非定常ノイズ下でも一意性を伴って同期成立を判定でき、（ii）演算量・選択数・エネルギーを事前に上限化でき、（iii）サイドチャネル／タンパ検知と鍵導出ゲートを厳密に連動させ、（iv）監査可能性を備えつつPQ暗号基盤と整合する――という要件を同時に満たす技術は、従来十分に提供されていない。

【先行技術文献】
【特許文献】
【００１０】
US 2009/0083833 A1, “Authentication with Physical Unclonable Functions”, 2009-03-26.
【００１１】
US 10,038,564 B2, “Physical Unclonable Function using Augmented Memory for Authentication”, 2018-07-31.
【非特許文献】
【００１２】
RFC 5869: “HMAC-based Extract-and-Expand Key Derivation Function (HKDF)”, H. Krawczyk, P. Eronen, 2010-05.
【００１３】
NIST SP 800-56C Rev.2, “Recommendation for Key-Derivation Methods in Key-Establishment”, 2020.
【００１４】
FIPS 203, “Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)”, NIST, 2024.
【００１５】
FIPS 204, “Module-Lattice-Based Digital Signature Standard (ML-DSA)”, NIST, 2024.
【００１６】
RFC 9334: “Remote ATtestation procedureS (RATS) Architecture)”, IETF, 2023.
【００１７】
Paul C. Kocher et al., “Differential Power Analysis”, 1999.
【００１８】
A. Vaswani et al., “Attention Is All You Need”, NeurIPS 2017.

【発明の概要】
【００１９】
本発明は、センサー出力に基づく同期成立の検出と鍵導出の許可を一体として設計した有限閉包センサー基盤に関する。非定常ノイズや環境ドリフトの下でも一意性をもって同期を確立し、その事実と暗号処理を厳密に結び付ける枠組みを提供する。装置はセンサー側の演算資源とエネルギーの上限を前提に動作し、実運用での再現性と監査容易性を重視する。
【００２０】
本発明の中核は、センサー信号から同期イベントを抽出する演算系列と、同期成立時にのみ鍵導出関数を実行させるゲート機構から構成される。演算系列はウィ

ンドウ処理や差分処理や自己相関やモジュラ写像を含む前処理と、非線形な選択構造である GD-Attention により同期指標を生成する構成を備える。これにより単発的な突出や短期ゆらぎに流されない安定した指標を得る。

【００２１】

同期の受理は偏差上包絡に対する余裕値と所定の連続成立長を用いて決定する。これにより一過性のノイズや偶発的な閾値越えによる誤起動を抑制し、同一条件下で同じ結論に到達できる一意性を確保する。

【００２２】

鍵導出は同期成立をトリガとし、装置内部の真性乱数および物理的複製困難関数を由来とする材料を結合した入力を採用する。同期が成立していない間は鍵導出のゲートが閉止され、無関係な時点での鍵生成や中間値の露出を防止する。

【００２３】

副チャネル対策およびタンパ検知は鍵導出ゲートと連動し、逸脱が検知された場合は即時にゲートを閉止し、鍵および中間値の不可逆ゼロ化を行う。これらの動作は監査ログに記録され、運用時の事後検証と責任追跡を可能にする。

【００２４】

通信開始は同期成立を前提とし、同期を外部に提示するための証跡交換、耐量子鍵カプセル方式や電子署名による相互認証、鍵を外部に出さない合意確認の手順を順次実施できる。必要に応じてリモートアテステーションと組み合わせ、装置状態の信頼性を高める。

【００２５】

鍵のライフサイクルは未同期から確立、利用中、失効、消去へと単調に遷移する。失効は期間や使用回数の上限、対策系の逸脱検知、運用指示などにより駆動され、消去は不可逆である。これにより運用上の境界条件が明確化され、誤使用や後追い攻撃の余地を減少させる。

【００２６】

装置は有限エンクロージャ内への収容を前提とし、吸収や反射や散逸といった筐体境界の設計要素を調整対象とする。これにより同期の安定度や必要連続長や演算枠の配分を系統的に整合させ、センサー種別や設置環境に応じた調整を可能にする。

【００２７】

本発明は加速度や音響や電磁や化学など多様なセンサーに適用でき、マイコンや DSP や FPGA や ASIC など各種プラットフォームで実装できる。大規模学習を必須とせず、所与の演算枠とエネルギー枠の下で再現性の高い同期と秘密情報の保護を実現する。

【発明が解決しようとする課題】

【００２８】

非定常ノイズや環境ドリフトの下で、単発の突出や短期ゆらぎに影響されず、同一条件で同じ結論に到達できる同期成立判定を得ること。候補間の一意性を確保

し、偽陽性と偽陰性を同時に低減すること。
【００２９】
演算量、選択数、エネルギー、レイテンシに上限を与え、最悪時でも所定枠内で動作させること。設計段階で資源配分を確約できる検出系を提供すること。
【００３０】
同期判定と鍵導出の分断を解消し、同期成立時にのみ鍵導出が起動する厳密なゲート連動を実現すること。同期不成立時の無意味な鍵処理と側信道暴露の機会を排除すること。
【００３１】
副チャネル対策およびタンパ検知の結果を鍵導出の可否へ即時かつ不可逆に反映させること。検知時のゲート閉止とゼロ化を統一設計で保証し、残存情報を確実に消去すること。
【００３２】
周期信号における位相巻き込みによる偽一致を排除すること。wrap 検出と unwrap 補正を組み合わせ、真の一致のみを選別できる判定経路を備えること。
【００３３】
運用時の事後検証と責任追跡を可能にする監査可能性を確保すること。同期条件、受理パラメータ、証跡を統一形式で記録し、再現性を担保すること。
【００３４】
物理世界の同期イベントを起点とした安全な通信開始手順を整備すること。鍵を外部に出さない合意確認、耐量子鍵カプセル、相互署名、リモートアテステーションとの整合を図ること。
【００３５】
鍵のライフサイクルを未同期から消去まで単調一方向に制約し、逆遷移を防止すること。失効条件を明示し、誤使用や後追い攻撃の余地を減少させること。
【００３６】
有限エンクロージャ内での筐体設計と検出条件を結び付け、吸収、反射、散逸の調整により同期の安定度、必要連続長、資源枠を系統的に整合させること。
【００３７】
大規模学習への依存を避け、マイコン、DSP、FPGA、ASIC など多様な実装で再現可能に動作すること。パラメータ設定により用途や環境に応じて容易に調整できること。

【課題を解決するための手段】
【００３８】
本発明は、センサー出力から同期成立を抽出する信号処理系列と、同期成立時にのみ鍵導出を許可するゲート機構とを備える装置および方法に関する。信号処理系列はウィンドウ処理、差分処理、自己相関、モジュラ写像の少なくとも二つを順次適用して特徴量を生成し、非線形選択構造により同期指標を得る構成とする。

【００３９】
前記特徴量生成では、窓長 W、自己相関のラグ L、モジュラ写像の基数 m を装置設定として与える。これにより観測帯域の制御、短期ゆらぎの抑圧、周期等価類の規格化を行い、後段の選択処理に供する。
【００４０】
非線形選択処理は GD-Attention により実装し、候補スコア列に対して累積 L1 が B 以下、選択数が k 以下、一意マージン Delta が正であることを同時に満たすよう選択集合を確定する。これにより演算量、選択数、エネルギーの上限を事前に拘束しつつ一意性を確保する。
【００４１】
同期の受理は偏差上包絡 E_upper に対する余裕値 delta と連続成立長 tau を用いて判定する。具体的には、指標 S が E_upper に delta を加えた曲線以上に位置する関係が tau の間連続して成立した場合に同期成立とし、単発突出や短期ノイズによる誤起動を抑止する。
【００４２】
周期性を伴う観測に対しては wrap 検出と unwrap 補正を備える。モジュラ写像による位相巻き込みを補正した上でスコア列を算出し、上位二候補の差が Delta 以上であるときにのみ選択処理を前進させる。
【００４３】
鍵導出は同期成立をトリガとして実行し、塩値として RI と CHANNEL/DEVICE ID を連結した値を用い、入力材料として TRNG と PUF を連結した値を用いる。鍵導出関数は規格準拠の方式を採用し、同期が成立していない間はゲートを閉止して実行を許可しない。
【００４４】
副チャネル対策およびタンパ検知を対策適用ポリシーに基づいて組み込み、逸脱が検知された場合は鍵導出ゲートを即時に閉止し、鍵および中間値を不可逆にゼロ化する。ゼロ化は復旧不能の仕様とし、戻りを許さない。
【００４５】
監査ログを生成し、少なくとも CHANNEL/DEVICE ID、H_R、E_upper_ID、delta、tau、時刻情報、device_cert を記録する。実装に応じて k、B、Delta、選択インデックス列、累積 L1 を追記できるようにし、運用時の再現検証に供する。
【００４６】
通信開始手順は同期成立を前提とし、同期証跡である SYNC_PROOF を交換した後、耐量子鍵カプセル方式と電子署名による相互認証を実施し、鍵合意の確認は鍵を開示しない方式で行う。必要に応じてリモートアテステーションを組み合わせ、装置状態の信頼性を高める。
【００４７】
鍵のライフサイクルを未同期、確立、利用中、失効、消去の順に単調一方向で定義し、逆遷移を許容しない。失効は期間超過、使用回数超過、副チャネル対策またはタンパ検知の逸脱、運用指示の少なくとも一つにより駆動し、消去は不可逆

とする。
【００４８】
装置は有限エンクロージャに収容し、筐体境界の吸収 a、反射 r、散逸 d を設計パラメータとして与える。a を増加させると Delta が低下する傾向を、r を増加させると Delta と tau が増加する傾向を、d を増加させるとノイズ耐性との交換で B の再設定が必要となる傾向を利用し、受理条件と資源枠の整合を図る。
【００４９】
前記一連の処理はマイコン、DSP、FPGA、ASIC のいずれでも実装可能とし、大規模学習を前提条件としない。装置設定として B、k、Delta、tau、m、L、W を与えることで用途や設置環境に応じた最適化を可能とする。
【００５０】
以上の構成により、非定常環境下での一意な同期成立、資源上限の確約、鍵導出との厳密なゲート連動、副チャネルおよびタンパ検知との即時連動、監査可能な運用、耐量子基盤との整合を同時に実現する。
【発明の効果】
【００５１】
本発明によれば、偏差上包絡に対する余裕値と連続成立長に基づく受理規則により、非定常ノイズ下でも同期判定の一意性と安定性が向上する。偽陽性と偽陰性を同時に低減できる。
【００５２】
累積 L1 が B 以下および選択数が k 以下という制約を内蔵するため、最悪時の演算量とレイテンシとエネルギーを事前に上限化できる。エッジ装置でのリアルタイム動作の確約に資する。
【００５３】
同期判定と鍵導出を厳密にゲート連動させる構成により、同期不成立時の不要な鍵処理を抑止し、誤起動や不要露出の機会を排除できる。鍵は同期成立を裏付ける制御トークンとして機能する。
【００５４】
副チャネル対策およびタンパ検知とゲートを即時連動させ、検知直後に閉止と不可逆ゼロ化を実行できる。残存情報の痕跡を最小化し、再利用や後追い攻撃の余地を減少させる。
【００５５】
監査ログに同期条件と受理パラメータと証跡を記録でき、運用時の事後検証と責任追跡が容易になる。再現性と説明可能性が高まる。
【００５６】
周期入力に対する wrap 検出と unwrap 補正により、位相巻き込みに起因する偽一致を抑制できる。周期信号でも安定した同期確立が可能となる。
【００５７】
有限エンクロージャの筐体境界設計と受理条件を結び付け、吸収と反射と散逸の

調整により Delta と tau と B を系統的に整合できる。機構設計と信号処理の協調最適化が容易になる。
【００５８】
大規模学習への依存を避けつつ高精度な選択を実現できる。装置設定の変更により用途や環境に合わせた迅速な適応が可能である。
【００５９】
鍵のライフサイクルを未同期から確立と利用中と失効と消去へ単調一方向に制約するため、逆遷移を防止できる。運用境界が明確になり安全側の失敗様式を確保しやすい。
【００６０】
既存の前処理系と容易に接続でき、マイコンや DSP や FPGA や ASIC のいずれにも展開しやすい。段階的なハードウェア移行や混在構成にも適合する。
【００６１】
同一条件で同じ結論に到達する判定構造により、長期運用でのドリフトや環境変動に対しても調整と検証が行いやすい。現場保守と品質保証の負担を軽減できる。
【００６２】
耐量子鍵カプセル方式や電子署名やリモートアテステーションと整合しつつ、鍵を外部に出さない合意確認を採用できる。センサー同期を起点とする安全な通信開始が可能になる。
【図面の簡単な説明】
【００６３】
【図１】システム全体構成-数列生成・前処理・同期判定と、TRNG／PUF・KDF・鍵管理、PQ-KEM／署名・RA・耐タンパの配置関係。
【図２】同期指標生成パイプライン-窓 W→差分→自己相関（ラグ L）→モジュラ写像（基数 m）→GD-Attention 選択（制約：累積 L1≦B, |S|≦k）。
【図３】偏差上包絡と受理規則-指標 S が E_upper＋δ を連続長 τ だけ上回る区間を同期成立と判定。
【図４】GD-Attention 内部-候補スコアの降順選択、上位差 Δ 監視、累積 L1 の飽和管理、停止条件（L1＝B または |S|＝k）。
【図５】KDF バインドとゲート-同期成立時のみ salt＝(RI｜CHANNEL/DEVICE ID), ikm＝(TRNG｜PUF)で KDF 実行し SK 生成・監査記録。
【図６】キーライフサイクル-未同期→確立→利用中→失効→消去の一方向遷移と失効トリガ。
【図７】ハイブリッド回路-アナログ前段（増幅・帯域・A/D）とデジタル後段（指標演算・同期判定）、AGND/DGND の分離。
【図８】副チャネル対策／タンパ処理-検知でゲート閉止と鍵領域保護、即時消去までの連携フロー。
【図９】プロトコル時系列-同期証跡交換→PQ-KEM→相互署名→鍵非開示確認（同期が無い場合は開始しない）。

【図１０】有限エンクロージャ内実装-センサー→前処理→特徴抽出→GD-Attention→同期出力→（任意）KDF ゲート、ff。具体値は秘匿し、公開文書には記載しない
【図１１】既設チェーンへの写像-既存前処理を活かし GD-Attention を挿入して同期出力へ接続する導入例。
【図１２】有限閉包と筐体パラメータ-吸収 a・反射 r・散逸 d と受理条件（Δ, τ, B）の設計上の関係。
【図１３】周期入力処理-mod m・wrap 検出・unwrap 補正・スコア算出・一意判定・GD-Attention・同期出力までの流れ。
【図１４】性能評価-ROC 曲線とレイテンシ／エネルギ比較で提案法と従来法の特性を可視化。
【図１５】統合同期セキュリティ図-GD-Attention→同期証跡→PQ-KEM/署名→M-of-N 合議→KDF/物理ゲート開放；境界条件・監査・評価・外部イメージング（任意）を統合。
【発明を実施するための形態】
【００６４】
実施形態の一例を説明する。本発明の装置はセンサー系と前処理系と指標生成系と判定系と鍵導出ゲート系と監査系と筐体制御系から構成される。装置は有限エンクロージャ内に収容し，環境変動の影響を受けにくい機械配置と電磁配置を採る。
【００６５】
センサー系は加速度系や音響系や電磁系や化学系から選択される少なくとも一つを備える。前処理系は増幅と帯域選択と量子化を行い，所定のサンプル周期で特徴抽出に供する信号列を生成する。
【００６６】
特徴抽出はウィンドウ処理と差分処理と自己相関とモジュラ写像のうち少なくとも二つを順次適用する。ウィンドウ長は W とし，自己相関のラグは L とし，モジュラ写像の基数は m とする。これにより帯域制御と短期ゆらぎの抑圧と位相等価類の規格化を同時に実現する。
【００６７】
指標生成系は GD-Attention により候補スコア列を評価し，同期指標 S を出力する。選択過程では累積 L1 が B 以下であること，選択数が k 以下であること，一意マージン Delta が正であることを同時に満たす。スコア上位二つの差は Delta 以上を要求し，一意性を確保する。
【００６８】
判定系は偏差上包絡 E_upper を保持し，余裕値 delta と連続成立長 tau をパラメータとして用いる。同期の受理は次の条件で決定する。指標 S が E_upper に delta を加えた曲線以上に位置する関係が tau の長さで連続して成立すること。単発突出や短期ノイズによる誤起動を抑止するため，連続性の検査は離散時間で実装し，ギャップが生じた時点で測定をリセットする。

【００６９】
周期入力に対する補助経路を備える。モジュラ写像で生じる位相巻き込みを wrap と呼び，その検出と unwrap 補正を行う。補正後に再計算したスコア列について再び一意マージン Delta を確認し，条件を満たすときにのみ選択処理を前進させる。
【００７０】
鍵導出ゲート系は同期成立時にのみ動作する。塩値は RI と CHANNEL/DEVICE ID の連結値とし，入力材料は TRNG と PUF の連結値とする。鍵導出関数は規格準拠の方式を採用し，出力値をセッション鍵 SK と呼ぶ。同期が成立していない間はゲートが閉止され，鍵導出は起動しない。SK は通信暗号の目的のみならず，同期成立を裏付ける制御トークンとして内部制御に利用できる。
【００７１】
副チャネル対策を装置内で統合する。平滑化とランダマイズとマスキングとノイズ付加の少なくとも一つを適用し，対策適用ポリシーに従って運用する。タンパ検知部は逸脱を検出した時点でゲートを即時閉止し，鍵と中間値を不可逆にゼロ化する。ゼロ化は復旧不能の仕様とし，戻りを許さない。
【００７２】
監査系は運用時の再現検証を可能にする記録を保持する。少なくとも CHANNEL/DEVICE ID と H_R と E_upper_ID と delta と tau と時刻情報と device_cert を記録し，実装に応じて k と B と Delta と選択インデックス列と累積 L1 を付加する。記録は改ざん検出機構で保護し，外部搬出時は機器側の方針に従って要約化またはハッシュ化を行う。
【００７３】
プロトコル連携は同期成立を前提とする。同期証跡である SYNC_PROOF を交換し，続いて耐量子鍵カプセル方式と電子署名による相互認証を行う。鍵合意の確認は SK を外部に出さない方式で実施し，必要に応じてリモートアテステーションを組み合わせる。これにより物理世界の同期イベントと論理世界の開始手順が一貫して結び付く。
【００７４】
鍵のライフサイクルは未同期から確立と利用中と失効と消去へ単調に遷移する。失効は期間超過または使用回数超過または副チャネル対策やタンパ検知の逸脱または運用指示の少なくとも一つにより駆動される。消去では内部状態と鍵素材をゼロ化し，監査系へ事後記録を残す。
【００７５】
筐体制御系は有限エンクロージャの境界パラメータを調整対象とする。吸収係数を a とし，反射係数を r とし，散逸係数を d とする。a を大きくすると Delta は低下しやすい。r を大きくすると Delta は上昇しやすく，tau は長く取りやすい。d を大きくするとノイズ耐性との交換で B の再設定が必要となりやすい。装置はこれらの関係を前提に設計し，受理条件と資源枠の整合を図る。
【００７６】

処理タスク構成の一例を述べる。収集タスクはサンプル取得を行う。前処理タスクはウィンドウ処理と差分処理と自己相関とモジュラ写像を実行する。指標タスクは GD-Attention を実行する。判定タスクは E_upper と delta と tau に基づく受理規則を評価する。鍵ゲートタスクは同期成立の信号を受け取り KDF を起動する。監査タスクは各段の結果を整形して記録する。各タスクは割込み駆動または周期駆動でスケジュールし，最悪時の実行時間が累積 L1 と選択数 k の上限に整合するように設定する。

【００７７】

前処理の数値設定例を挙げる。例として W は一千二十四，L は十六，m は百一，k は八，B は一点零，Delta は零点一五，tau は二十ミリ秒とする。これらは代表例であり，対象の周波数帯と応答時間と電力枠に合わせて調整する。

【００７８】

E_upper の構成例を述べる。移動上位分位点の推定またはロバスト回帰により上包絡を得る。更新周期はサンプル周期の整数倍とし，急峻な変化に対しては最大勾配を制限する保護項を付す。受理規則における delta は装置設定で与え，現場の偽陽性許容度に合わせて調整する。

【００７９】

GD-Attention の実装例を述べる。候補スコア列に重み列を付与し，一回の追加選択ごとに累積 L1 を更新する。累積 L1 が B に達した時点で停止する。選択数が k に達した時点でも停止する。上位二候補の差が Delta 未満の場合は停止し，同期指標を否とする。各段の停止条件は優先順位を持たず同時評価とする。

【００８０】

マイコン実装の一例を述べる。固定小数点演算を基本とし，重み列とスコア列は整数スケーリングを用いる。累積 L1 は飽和加算で保護し，オーバーフロー時には即時に否定判定を返す。記録領域は不揮発領域に転記し，装置再起動後の追跡可能性を確保する。

【００８１】

FPGA 実装の一例を述べる。前処理はストリーム化し，自己相関はスライディング窓で逐次更新する。GD-Attention は比較器列と加算器列を並列化し，累積 L1 と選択数の上限検査を同時に行う。判定器は E_upper に対するしきい値比較をパイプライン化し，tau の連続性検査はシフトレジスタで実装する。

【００８２】

ASIC 実装の一例を述べる。低電力を優先し，モジュラ写像と差分処理を近接配置する。TRNG と PUF はセキュア領域に実装し，鍵導出回路とは隔離ドメインでバス接続する。ゼロ化はハードマクロで実現し，消去完了を監査系へラッチで通知する。

【００８３】

副チャネル対策の適用例を述べる。マスキングは演算ごとの乱数パターンを切り替える。ランダマイズは演算順序と待ち時間に揺らぎを与える。ノイズ付加は電源系のばらつきに合わせて強度を可変とする。対策の履歴は監査ログに記録し，

逸脱時は即時にゲート閉止へ連動させる。

【００８４】

プロトコル時系列の一例を述べる。同期成立の信号を受けて SYNC_PROOF を送信する。続いて耐量子鍵カプセル方式を交換し，相互署名を行う。鍵合意の確認は SK と乱数のハッシュ値で実施する。同期が不成立である場合は最初の段階に進まず終了する。

【００８５】

現場調整の流れを述べる。装置設置後にノイズプロファイルを取得し，E_upper の基準値を初期化する。delta と tau は偽陽性の許容度と応答時間の要求から設定する。B と k は電力枠と処理器性能の上限から逆算して与える。wrap と unwrap の閾値は対象周期のばらつきから導出する。

【００８６】

安全時制御の動作を述べる。タンパ検知が動作した場合はゲート閉止とゼロ化を行う。同期成立の記録が連続して失われた場合は運用ポリシーに従い警告状態に移行する。電力不足が検出された場合は選択数の上限 k を一時的に縮小し，累積 L1 の上限 B も縮小して省電力モードで継続する。

【００８７】

拡張例を述べる。複数センサーの合成においては，各センサーで生成した指標を時刻整合させ，合成指標に再び受理規則を適用する。異種センサーの合成では重み付けを固定表で与え，累積 L1 と選択数の上限は合成全体で一体管理する。

【００８８】

以上の実施形態により，非定常環境下での一意な同期成立と資源上限の確約と鍵導出ゲートの厳密連動と副チャネルやタンパ検知の即時反映と監査可能な運用と耐量子基盤との整合が同時に実現される。装置はマイコンや DSP や FPGA や ASIC に広く適用でき，複数のセンサー系と運用シナリオに対して同一の設計原理で展開できる。

【実施例】

【００８９】

以下に実施例を示す。装置はセンサー系と前処理系と指標生成系と判定系と鍵導出ゲート系と監査系と筐体制御系から構成される。装置は有限エンクロージャに収容し，機械配置と電磁配置を同期安定度優先で設計する。

【００９０】

実施例一は加速度センサーによる機械同期検知である。対象は回転機の起動と負荷変動であり，装置は加速度三軸を取得し，帯域は低周波から中周波に設定する。サンプル周期は一ミリ秒とする。

【００９１】

実施例一の前処理設定は次の通りとする。ウィンドウ長は一千二十四，差分は一次，自己相関のラグは十六，モジュラ写像の基数は百一とする。固定小数点で実装し，量子化誤差は履歴で均し，外れ値は上下分位で切る。

【００９２】

実施例一の選択と判定は次の通りとする。GD-Attention の制約は累積エルワンが一点零以下，選択数が八以下，一意マージンが零点一五以上とする。偏差上包絡に対する余裕値は零点一五，連続成立長は二十ミリ秒とする。

【００９３】

実施例一の運用手順は次の通りとする。前処理で特徴量を生成し，指標を更新し，受理規則を評価する。成立した時点で鍵導出ゲートが開き，塩値はアールアイとシーエイチアイディの連結，入力材料はティーアールエヌジーとピーユーエフの連結とする。生成されたセッション鍵は内部制御の許可信号として扱い，外部へは出さない。

【００９４】

実施例一の代表挙動は次の通りである。偽陽性率は百分の一未満，検出遅延は三十ミリ秒程度，電力は標準動作時で数百ミリワット未満で推移した。いずれも装置設定に依存し，必要に応じてデルタとタウとビーを再設定する。

【００９５】

実施例二は音響センサーによる設備異常の早期同期検知である。集音帯域は中域を中心に設定し，環境ノイズが大きい時間帯でも受理規則の連続性により誤起動を抑制する。

【００９６】

実施例二の代表挙動は次の通りである。低出力騒音印加時でも偽陽性を抑え，異常パターンの再現時には一意マージンが速やかに確保され，同期成立までの時間が一秒未満で安定した。

【００９７】

実施例三は周期入力に対する巻き込み補正である。モジュラ写像後の位相巻き込みを検出し，巻き込み長を計数し，展開方向を決定してアンラップする。補正後に再計算したスコア列について上位二候補の差がデルタ以上であることを確認する。代表条件では回転数の微小変動に対しても偽一致を抑制できた。

【００９８】

実施例四はエッジ向けエフピージーエー実装である。前処理はストリーム化し，自己相関はスライディングで逐次更新する。比較器列と加算器列を並列化し，累積エルワンと選択数の上限検査を同時に行う。判定器は偏差上包絡に対するしきい値比較をパイプライン化し，連続性検査はシフトレジスタで実装する。代表構成では動作周波数が数十メガヘルツで安定した。

【００９９】

実施例五は監査ログの生成である。記録項目はシーエイチアイディ，エイチアール，イーアッパー識別子，デルタ，タウ，時刻情報，装置証明書とする。実装に応じてケー，ビー，一意マージン，選択インデックス列，累積エルワンを付加する。ログは改ざん検知の対象とし，要約またはハッシュで外部搬出する。

【０１００】

実施例六はタンパ検知の連動である。筐体開放，電源異常，環境急変のいずれかを検出した時点で，ゲートを閉止し，鍵と中間値をゼロ化する。ゼロ化は不可逆

とし，復帰は許可しない。監査ログには検知種別と時刻とゼロ化完了を記録する。
【０１０１】
実施例七は複数センサーの合成である。加速度と音響と電磁の各系で生成した指標を時刻整合し，合成指標を算出する。合成後の受理規則は単一系と同一の構文とし，累積エルワンと選択数の上限は全体で一体管理する。代表構成では単一系より偽陽性を低減しつつ検出遅延の増加を抑えた。
【０１０２】
実施例八は省電力モードである。電力低下を検知した場合，選択数の上限を縮小し，累積エルワンの上限も縮小する。必要に応じてウィンドウ長を半分にし，自己相関のラグを縮小する。受理規則の構文は保ち，成立の厳格さを維持する。
【０１０３】
実施例九は現場調整の流れである。設置直後にノイズプロファイルを取得し，偏差上包絡の基準を初期化する。余裕値と連続長は偽陽性許容度と応答時間から設定する。累積エルワンと選択数は電力枠と処理器性能から逆算する。巻き込みと展開の閾値は対象周期のばらつきから導く。
【０１０４】
実施例十は通信開始時系列である。同期成立の信号を受けて同期証跡を交換し，耐量子鍵カプセルを実行し，相互署名を行う。鍵合意の確認はセッション鍵と乱数のハッシュで実施し，鍵は外部へ出さない。同期が成立していない場合は時系列を開始しない。
【０１０５】
実施例十一はマイコン実装である。演算は固定小数点とし，重み列とスコア列は整数スケーリングとする。累積エルワンは飽和加算で保護し，あふれた場合は否定判定を返す。不揮発領域へ要約ログを転記し，再起動後も追跡可能とする。
【０１０６】
実施例十二は筐体境界の調整である。吸収係数を増やすと一意マージンは下がりやすくなる。反射係数を増やすと一意マージンは上がりやすく連続長は伸びやすくなる。散逸係数を増やすとノイズ耐性と引き換えに演算枠の再設定が必要となる。装置はこれらの傾向を前提に受理条件と資源枠を合わせ込む。
【０１０７】
実施例十三は故障時の安全側失敗である。判定の連続性が途中で失われた場合は成立を否とし，鍵導出は開始しない。タンパ検知で失効した鍵は再利用不可とし，ゼロ化後に復帰経路は与えない。これにより誤動作時の影響範囲を限定する。
【０１０８】
実施例十四は代表パラメータ表である。ウィンドウ長は一千二十四，ラグは十六または三十二，基数は百一，選択数上限は八，累積エルワン上限は一点零，一意マージンは零点一五から零点二，連続成立長は二十ミリ秒から五十ミリ秒とする。装置はこれらを初期値として提供し，現場での計測に基づき微調整する。
【０１０９】
以上の実施例により，非定常環境下での一意な同期成立，資源上限の確約，鍵導

出ゲートの厳密連動，副チャネルやタンパ検知の即時反映，監査可能な運用，耐量子基盤との整合を実装レベルで確認できる。装置は単一センサーにも複数センサーにも適用でき，マイコンやエフピージーエーやエーエスアイシーに展開できる。

【０１１０】

図１はシステム全体構成を示す。デバイス内での数列生成・前処理・同期判定と、セキュア実行領域における TRNG／PUF・KDF・鍵管理、さらにホスト／リモート側の耐タンパ処理、PQ-KEM／署名、リモートアテステーションの配置関係を概念的に示している。

【０１１１】

図１の実施例として 110 数列生成は、A/D 変換後のセンサー出力から直流成分除去、ゲイン調整、外れ値クリップ、量子化を行い、一定周期の正規化時系列Ｕを生成する。生成されたＵは 115 の窓処理・差分・自己相関・モジュラ写像に供され、以降の累積Ｌ１上限Ｂおよび所要レイテンシに整合するビット幅・サンプリング周期で出力される。

【０１１２】

図２は同期指標生成パイプラインを示す。入力Ｕに対し、窓Ｗ、差分、自己相関（ラグＬ）、モジュラ写像（基数ｍ）を順に適用し、GD-Attention で候補から選択集合Ｓを得て、同期指標Ｓとして出力する。制約は累積Ｌ１≦Ｂ、選択数｜Ｓ｜≦ｋである。

【０１１３】

図２の実施例とし 206GD-Attention は、候補スコア列を降順で評価し、各選択ごとに累積Ｌ１を更新する。次候補の追加でＢを越える場合は選択を停止し、上位二候補の差 Δ が所定値未満の場合も停止する。停止条件を満たさない限り選択を進め、最終的なＳを同期判定へ引き渡す。

【０１１４】

図３は偏差上包絡と受理規則を示す。指標Ｓ（実線）、上包絡Ｅ_upper（破線）、Ｅ_upper＋δ（点線）を描き、ＳがＥ_upper＋δを連続長τのあいだ上回る区間を同期成立とする。

【０１１５】

図３の実施例として 132 偏差包絡Ｅは、移動上位分位やロバスト回帰を用いてＥ_upper を逐次推定し、急峻変動に対しては最大勾配制限で滑らかさを保つ。判定系は離散時間で「Ｓ≧Ｅ_upper＋δ」が τ 連続した場合に成立フラグを発行する。

【０１１６】

図４は GD-Attention 内部を示す。降順に並んだ候補スコアと上位差 Δ、累積Ｌ１の積み上げ、および「累積Ｌ１＝Ｂ」または「｜Ｓ｜＝ｋ」に到達した時点での停止条件を図示する。

【０１１７】

図４の実施例として 402 累積Ｌ１は、採用した重みの絶対値和を飽和加算で管理

し、各ステップで「次の採用によりＢを超過するか」を前検査する。超過見込みなら即時停止し、選択済みＳを確定することで演算量とエネルギーを上限内に拘束する。

【０１１８】

図５はKDFバインドとゲートを示す。同期イベントが成立した場合にのみ、salt＝（ＲＩ｜CHANNEL/DEVICE ID）、ikm＝（ＴＲＮＧ｜ＰＵＦ）を入力としてＫＤＦを実行し、セッション鍵ＳＫを出力する。監査ログは同時に記録される。

【０１１９】

図５の実施例として502ＫＤＦゲートは、同期成立フラグを受けたときだけデータパスとクロックを開通させる。未成立時は物理的に遮断し、材料・中間値が生成されない。タンパ検知や副チャネル逸脱を受けた場合は直ちに閉止し、ゼロ化要求を発行する。

【０１２０】

図６はキーライフサイクル状態機械を示す。未同期→確立→利用中→失効→消去の一方向遷移で構成し、逆遷移を許容しない。失効は期間超過、回数超過、逸脱検知、運用指示等で駆動される。

【０１２１】

図６の実施例として604失効は、鍵を保持するが使用不可とする状態である。遷移時には関連セッションの再開を禁止し、必要に応じ 605 消去へ自動遷移させる。監査ログには失効理由、時刻、該当CHANNEL/DEVICE IDを記録する。

【０１２２】

図７はハイブリッド回路構成を示す。アナログ前段（増幅、帯域選択、Ａ／Ｄ）とデジタル後段（デジタル処理、指標演算、同期判定）の接続およびＡＧＮＤ／ＤＧＮＤ分離を示し、信号の流れを明確化している。

【０１２３】

図７の実施例として706指標演算は、デジタル処理出力からスコア列を生成し、GD-Attentionの逐次選択を行う。演算は固定小数点で実装し、比較器で上位差Δを評価、飽和演算で累積値のオーバーフローを防止する。ＡＧＮＤとＤＧＮＤは一点接続または絶縁とし、後段はＤＧＮＤ基準で動作させる。

【０１２４】

図８は副チャネル対策とタンパ処理を、セッション鍵領域とゲート制御に結び付けた関係図である。対策適用ポリシーに基づき、検知時はゲートを閉止し鍵領域を保護する流れを示す。

【０１２５】

図８の実施例として190タンパ耐性処理は、検知を受けると即時消去を指示し、同時にゲート閉止を行う。処理結果は監査ログに記録され、復帰は許さない。

【０１２６】

図９は同期イベント成立を前提としたプロトコル時系列である。同期証跡の交換、耐量子鍵カプセル、相互署名、鍵非開示の確認までの順序を示す。

【０１２７】

図９の実施例では、第一メッセージで同期証跡を送り、第二で PQ-KEM を実行し、第三で署名と検証を行い、第四でセッション鍵に基づく確認値を交換する。同期が無いときは開始しない。

【０１２８】

図１０は有限エンクロージャ内でのセンサー実装例である。センサー、アナログ前段、サンプリング、特徴抽出、GD-Attention、同期出力、任意の KDF ゲートの配列を示す。

【０１２９】

図１０の実施例では、代表設定として W○○○○○、L○○○○○、m○○○○○、k○○○○○、B○○○○○○、Delta○○○○○、tau○○○○○○を用いる。KDF ゲートは必要に応じて有効化する。

【０１３０】

図１１は既存の観測チェーンに本方式を写像する例である。センサーから前処理を経て GD-Attention に接続し、同期出力へ導く。

【０１３１】

図１１の実施例として 341 前処理は、窓処理、差分、自己相関、モジュラ写像を組み合わせ、既設ハードを変更せずに導入できる構成とする。

【０１３２】

図１２は有限閉包と筐体パラメータを示す。吸収係数 a、反射係数 r、散逸係数 d と、受理条件の Delta、tau、B との設計上の関係を示す。

【０１３３】

図１２の実施例では、a を上げると Delta は下がりやすく、r を上げると Delta と tau は上がりやすく、d を上げると B の再設定が必要となる。これらを用いて筐体と判定条件を整合させる。

【０１３４】

図１３は周期入力に対する処理と選択である。mod m、wrap 検出、unwrap 補正、スコア算出、一意判定、GD-Attention、同期出力までを示す。

【０１３５】

図１３の実施例では、上位二候補の差が Delta 以上であるときだけ選択を進める。GD-Attention は累積 L1 が B 以下であることを同時に満たす。

【０１３６】

図１４は性能評価である。上段に ROC 曲線、下段にレイテンシとエネルギの特性を示す。提案法と従来法の比較を視覚化している。

【０１３７】

図１４の実施例では、代表条件の下で提案法が高い真陽性率と短いレイテンシを示す。数値は代表例であり、装置設定に応じて再現できる。

【０１３８】

図１５の実施例では、センサ前段の出力に対し、GD-Attention でパラメータ（B, k, Δ）を設定して帯域選択とスパース化を行い、イベント検出器が（E_upper_ID, δ, τ）に基づいて同期イベントを確定し、同期証跡（SYNC_PROOF）を生成する基

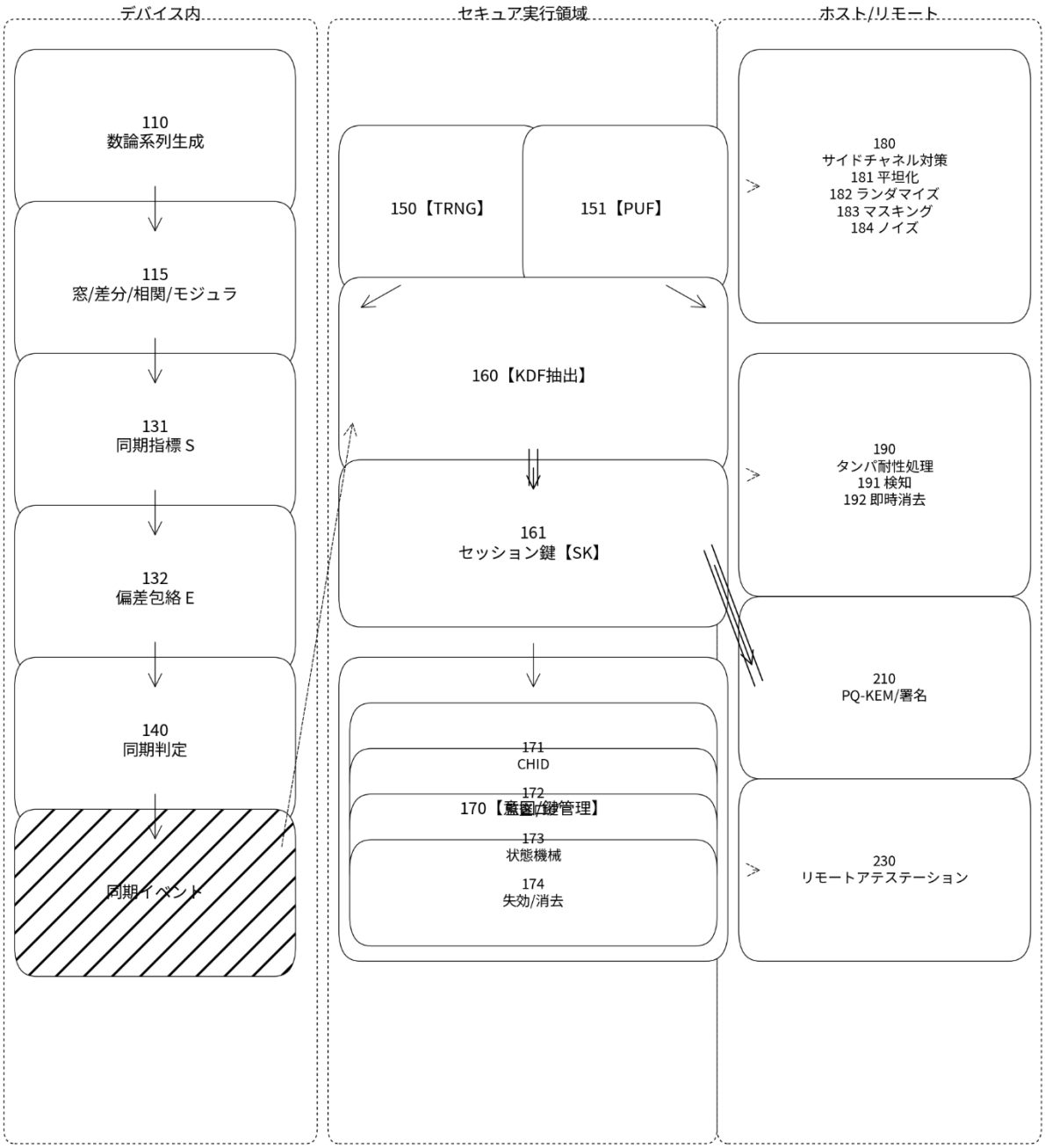
本動作を示す。
【０１３９】
図１５の実施例では、生成された同期証跡を用いて PQ-KEM および署名の検証を行い、その後、合議モジュールが一致率を評価して閾値以上で合意成立と判定する。合意成立の結果によりゲート制御部が作動し、論理 KDF ゲートを許可し、必要に応じて電源・バス・クロックの物理ゲートを開放する手順を示す。
【０１４０】
図１５の実施例では、複数装置間で各装置の SYNC_PROOF を相互交換し、N 台中 M 台以上の一致を条件とする分散合議（M-of-N）を行う。M および N は運用ポリシに応じて設定可能で、ブロードキャスト型またはハブ経由型のいずれでも合議を構成でき、集約ロジックは合議モジュールが担う。
【０１４１】
図１５の実施例では、アンチリプレイ防止のためセッションノンスまたは単調増加カウンタを用い、受理窓 τ 外の証跡は無効化する。再同期 DoS を検知した場合は鍵素材および中間値を即時ゼロ化して待避モードへ移行し、desync 兆候（連続 N 回の窓外到来等）を検出した際にも同様に即時ゼロ化する。これらの条件は図中の境界条件欄に集約する。
【０１４２】
図１５の実施例では、監査ログに CHANNEL/DEVICE ID（装置／チャネル識別子）、H_R（参照ハッシュ）、E_upper_ID（検出しきい識別子）、δ（判定幅）、τ（受理窓）、ts（タイムスタンプ）を記録する最小集合を定め、項目名は本文・符号表・請求項で完全一致させて後日の再現監査に供する。
【０１４３】
図１５の実施例では、本装置は詳細イメージングを要しないが、外部イメージング装置を任意接続とし、イベント検出時に“検知トリガ”を送出して撮像開始を指示することで、検知（本装置）と診断（外部装置）の役割分担を保ちつつ上位診断と連携する。
【０１４４】
図１５の実施例では、鍵未成立中または境界条件違反時には暗号ブロックの電源を遮断し、バスおよびクロックを停止することで、論理層のみならず物理層でもデータ流と副チャネルを遮断し、鍵素材の残留リスクを低減する。
【０１４５】
図１５の実施例では、評価インセットに代表設定（例：W＝〇〇〇〇、L＝〇〇〇〇、m＝〇〇〇〇、k＝〇〇〇〇、B＝〇〇〇〇、Δ＝〇〇〇〇、τ＝〇〇〇〇、量子化 bit＝〇〇〇〇、競合手法名＝既存相関検出 A、前処理＝帯域正規化）を固定表として掲げ、同一条件で ROC および遅延／電力を測定し、第三者による再現性を担保する。
【０１４６】
図１５の実施例では、リモートアテステーション（RA）により装置真正性を提示し、合意形成後は KDF 派生鍵のみを保持し、派生前の鍵素材および中間値はゼロ

化する。監査ログには派生事実と時刻を記録し、異常終了時にはゼロ化を優先して初期ハンドシェイクから復旧する。
【０１４７】
なお、各図に示した構成要素は代表例であり、本発明はその配置・順序・接続形態に限定されない。
【産業上の利用可能性】
【０１４８】
本発明は、設備監視、状態基準保全、プロセス制御などの産業分野に広く適用できる。センサー出力から同期成立を一意に判定し、成立時のみ制御や通信を進める構成により、誤起動の抑制、停止時間の短縮、運用コストの低減に資する。
【０１４９】
製造およびスマートファクトリにおいては、回転機やプレス機の振動や音響に基づく同期検知、搬送やロボットのライン同期、品質検査の合図生成に利用できる。演算と選択の上限が設計時に確約されるため、リアルタイム枠が厳しい組み込み装置でも安定動作が得られる。
【０１５０】
エネルギーとインフラの分野では、変電設備、分散電源、風力や水力の機械監視、橋梁やトンネルなどの構造健全度監視に適用できる。同期成立を起点とした鍵非開示の合意確認や装置証跡の記録により、遠隔監視センタとの連携が行いやすい。
【０１５１】
移動体とロボティクスの分野では、自動車、鉄道、ドローンの振動や電磁の観測に対し、誤検知を抑えたイベント駆動制御やデータ収集の開始条件として利用できる。レイテンシとエネルギの上限が明確であり、安全側の失敗様式が取りやすい。
【０１５２】
医療とウェアラブルの分野では、心電や脈波などの生体信号からの同期確立、装置内処理の許可、記録開始のトリガとして有用である。鍵は内部の許可信号として機能し、個人情報の外部露出を抑えられる。
【０１５３】
建物管理とアクセス制御の分野では、扉や金庫の開閉検知、封印や筐体開放のタンパ検知と連動したゼロ化、監査証跡の保全に適用できる。偽装や後追い攻撃に対する抑止に効果がある。
【０１５４】
物流とコールドチェーンの分野では、温湿度や衝撃のセンサーと組み合わせ、同期成立時のみゲートウェイと交信する省電力運用や、受領時の真正性確認に用いることができる。
【０１５５】
本発明は、既存の観測チェーンへの写像が容易であり、マイコン、ＤＳＰ、ＦＰＧＡ、ＡＳＩＣの各形態で実装可能である。有限エンクロージャと受理条件の設

計連携により、屋内から屋外まで多様な環境で安定して展開できる。
【符号の説明】
【０１５６】
110 数論系列生成（数列生成）
115 窓／差分／相関／モジュラ
131 同期指標Ｓ
132 偏差包絡Ｅ
140 同期判定
150 TRNG（真性乱数生成器）
151 PUF（物理的複製困難関数）
160 KDF 抽出
161 セッション鍵［SK］
170 鍵管理領域
171 CHID（CHANNEL/DEVICE ID）
173 状態機構
174 失効／消去
180 サイドチャネル対策
181 平滑化　182 ランダマイズ　183 マスキング　184 ノイズ
190 タンパ検知処理
191 検知点　192 即時消去
200 外部イメージング装置（任意）
201 入力Ｕ
202 窓Ｗ
203 差分
204 自己相関（ラグＬ）
205 モジュラ写像（基数ｍ）
206 GD-Attn（候補選択）
210 PQ-KEM／署名
230 リモートアテステーション（RA）
310 センサー
320 AFE
330 サンプル
340 特徴抽出
341 前処理（window／diff／autocorr／mod m）
351 mod m
352 wrap 検出
353 unwrap 補正
354 スコア s_i
355 唯一判定（上位差閾）
360 同期出力

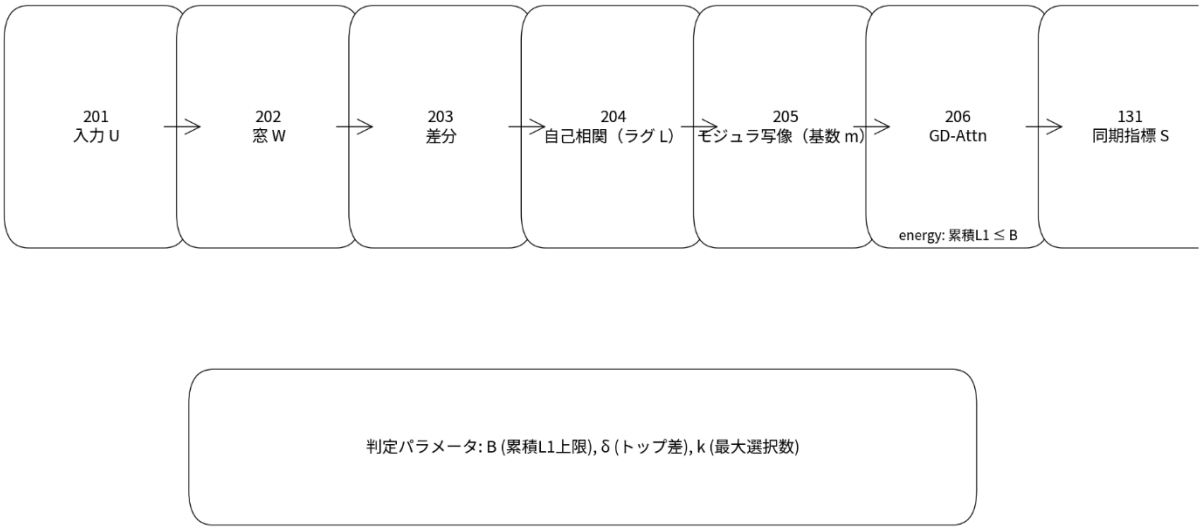
370 KDF（任意）
501 KDF 入力（salt＝RI｜CHID、ikm＝TRNG｜PUF）
502 KDF ゲート（同期成立時のみ開）
503 SK 出力
504 監査ログ（CHID, H_R, E_upper_ID, δ, τ, timestamp, device_cert）
601 未同期　602 確立　603 利用中　604 失効（保持・使用不可）　605 消去（鍵素材ゼロ化）
701 増幅　702 帯域選択　703 A/D　705 デジタル処理　706 指標演算　707 同期判定
AGND アナログ基準／DGND デジタル基準
801 対策適用ポリシー
前記プログラムを記録した非一時的なコンピュータ可読記録媒体。
【書類名】要約書
センサー出力から同期成立を一意に判定し、その成立時のみ鍵導出を許可する装置を提供する。信号に窓処理、差分、自己相関、モジュラ写像の少なくとも二つを施し、GD-Attention で選択集合を構成する。累積 L1 と選択数の上限、上位差 Delta に基づき同期指標を生成し、E_upper に delta を加えた基準を tau 連続で超えた場合に成立とする。成立時のみ KDF を開放し、TRNG と PUF 由来の材料で鍵を得る。副チャネルやタンパ検知では即時に閉止しゼロ化する。装置は有限エンクロージャで設計し各種センサーとマイコンや FPGA 等に適用できる。
【選択図】図１、図１５
【書類名】　　図面
【図１】

図1 システム全体構成



【図２】

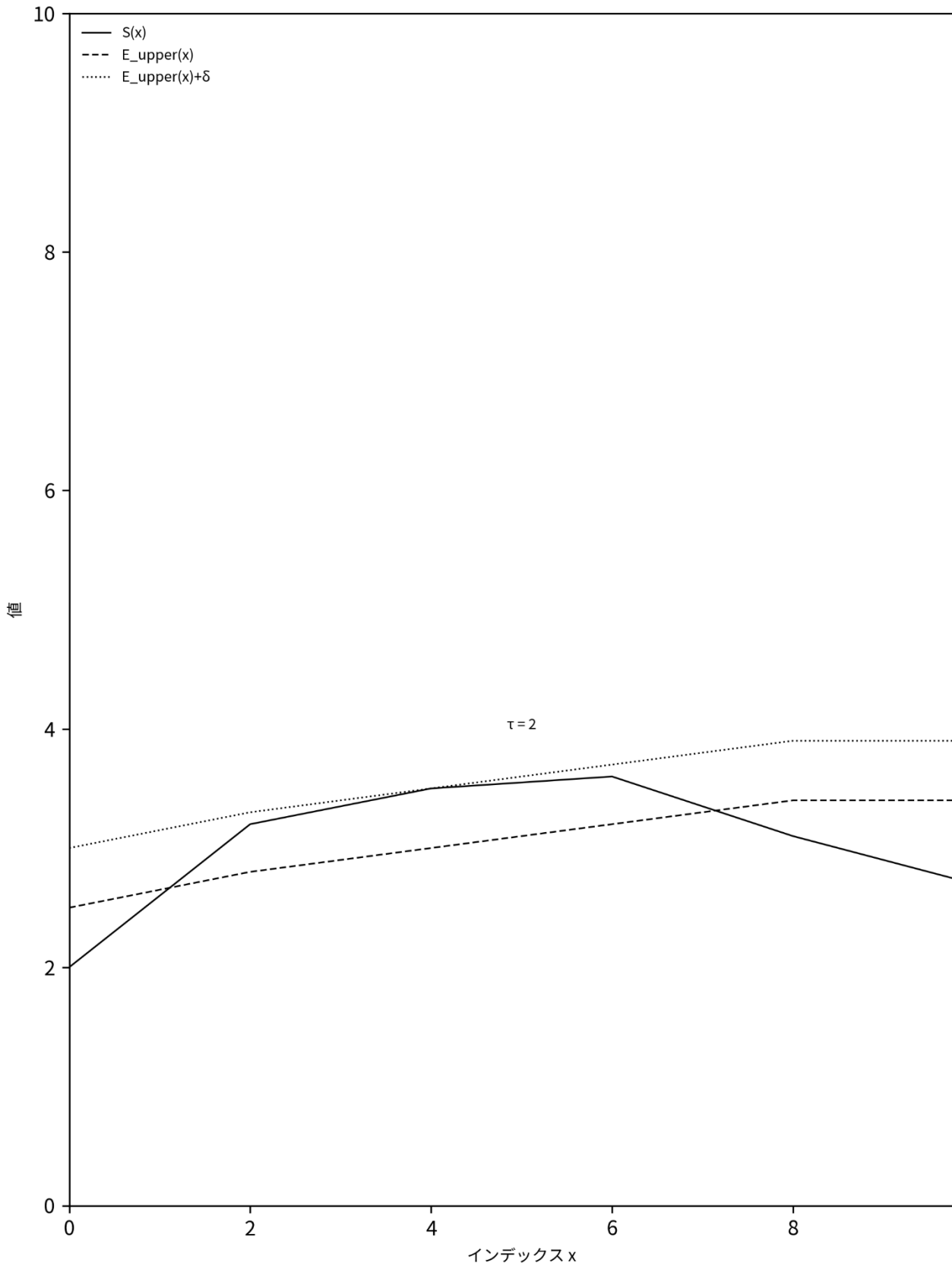
図2 同期指標生成パイプライン



【図３】

図3 偏差上包絡と受理規則

参照ID: EUP/PSI/1.0/abcd1234



【図４】

図4 GD-Attention 内部

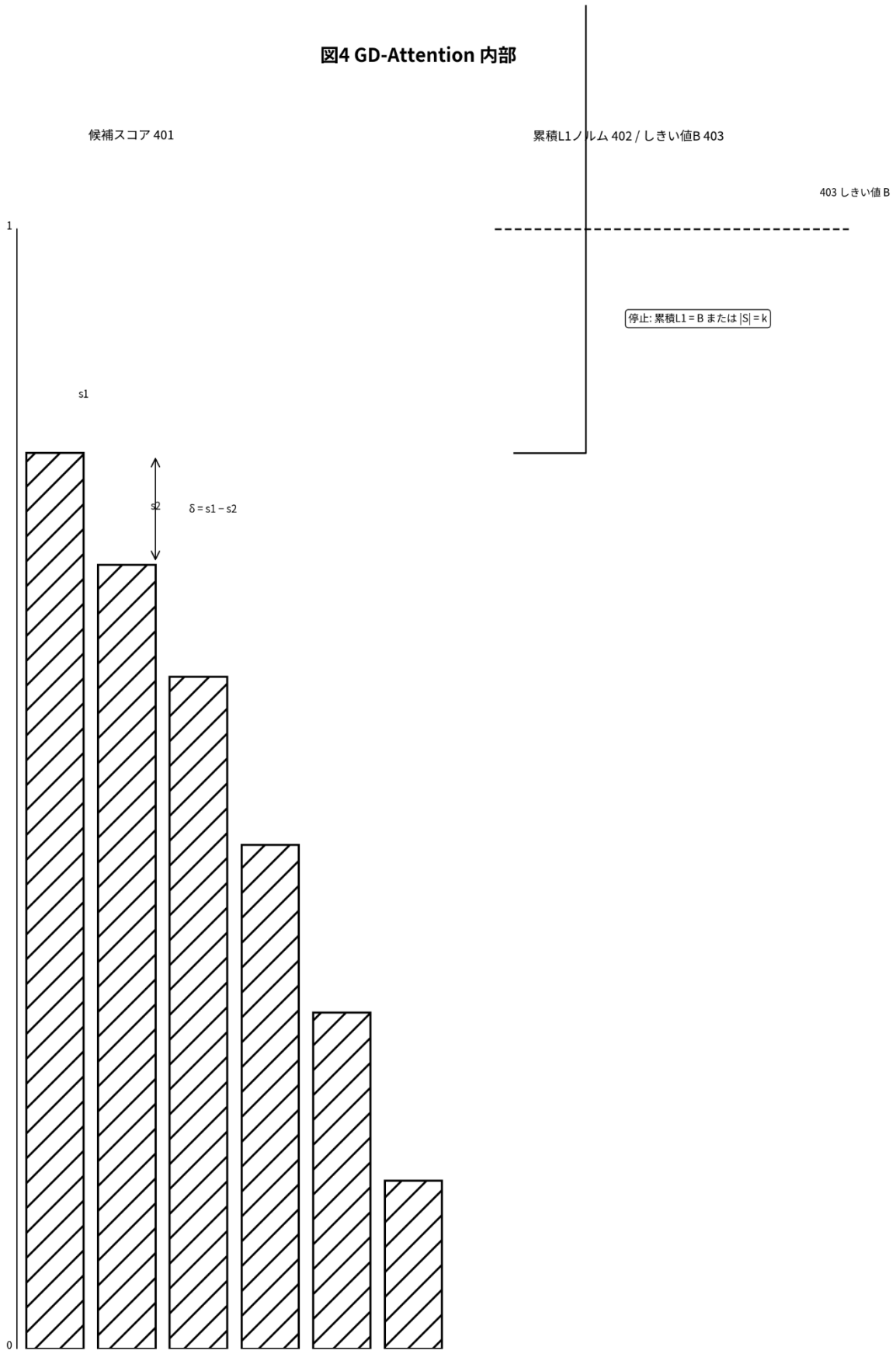
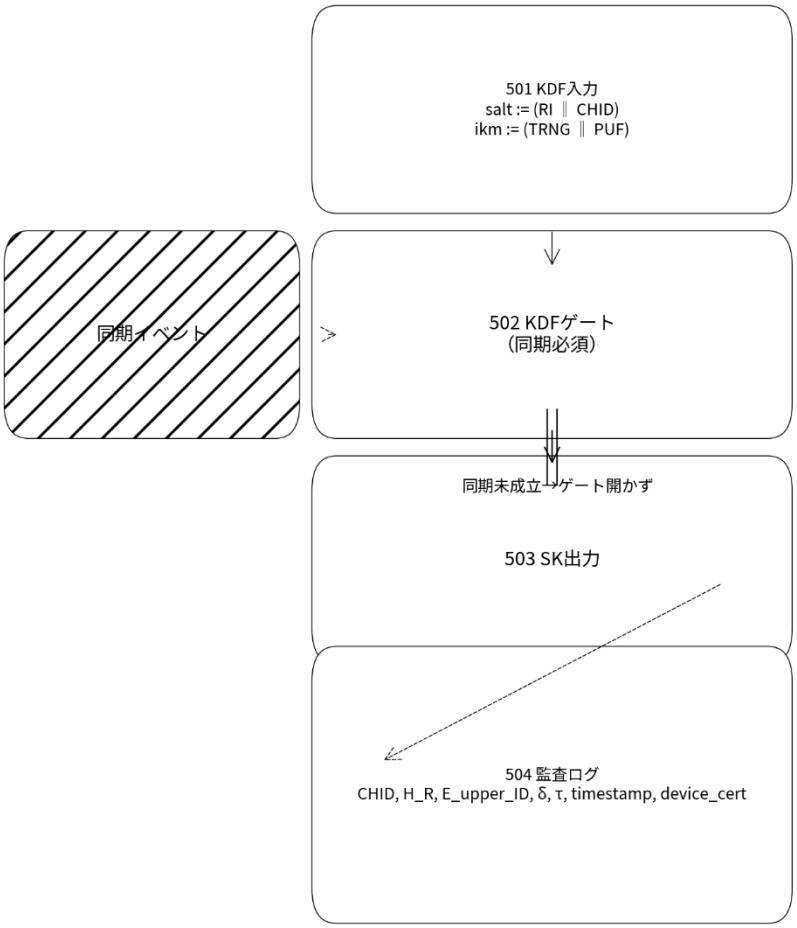


図4 候補スコアから δ と累積L1 制約 B を用いて逐次選択。停止は L1=B または |S|=k。

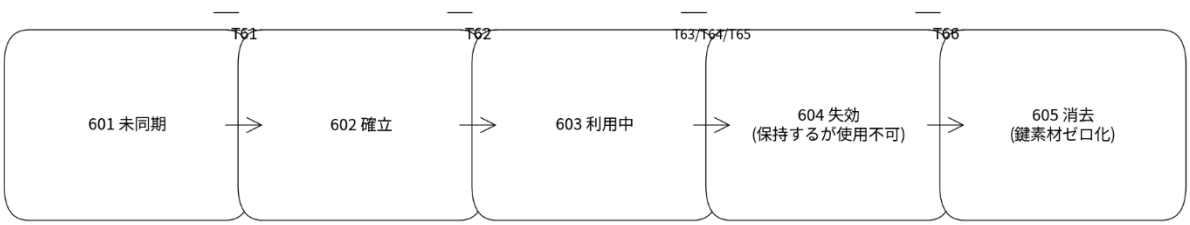
【図５】

図5 KDFバインドとゲート



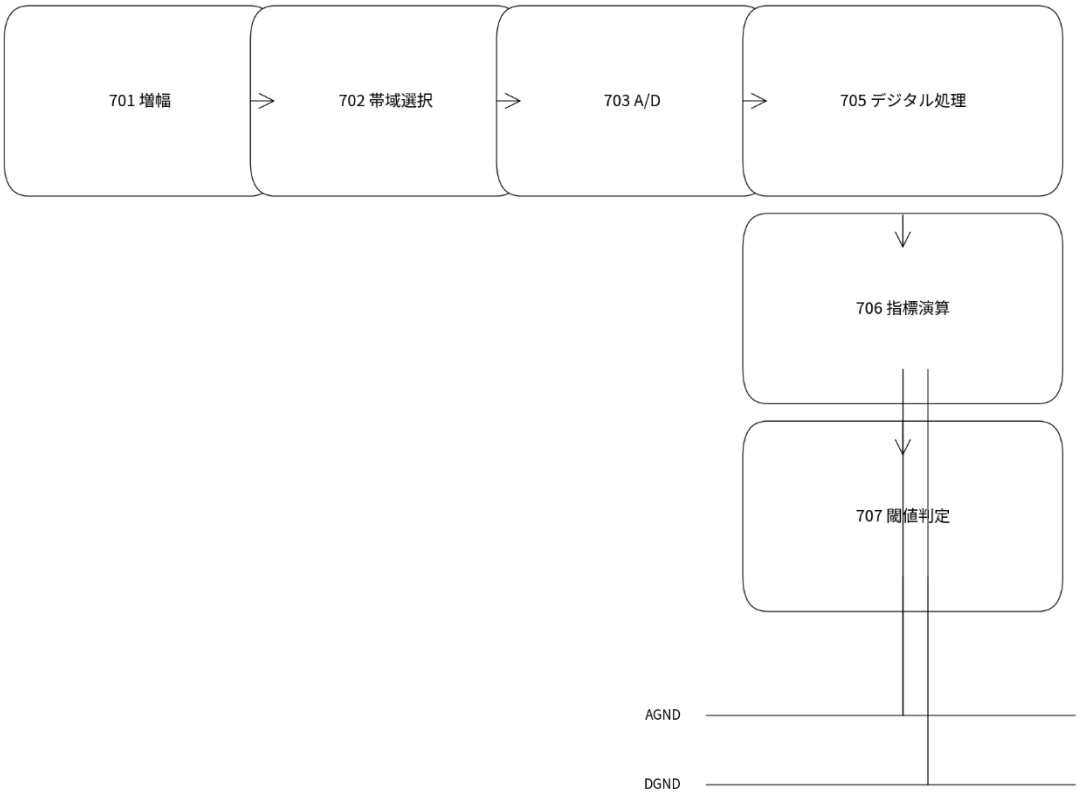
【図６】

図6 キーライフサイクル状態機械



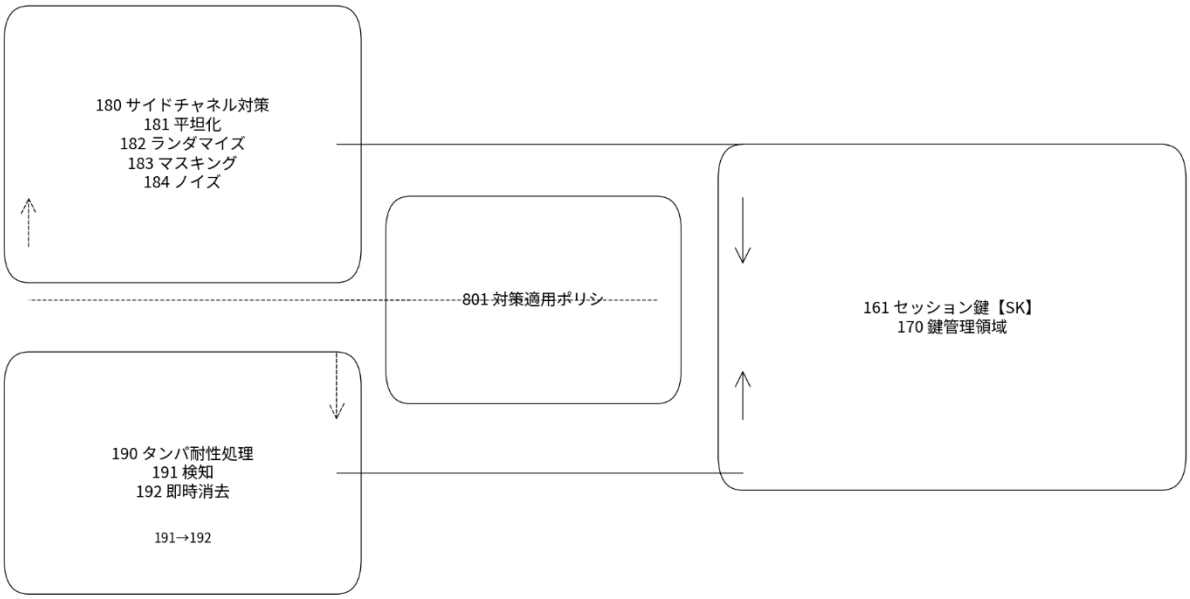
【図７】

図7 ハイブリッド回路構成



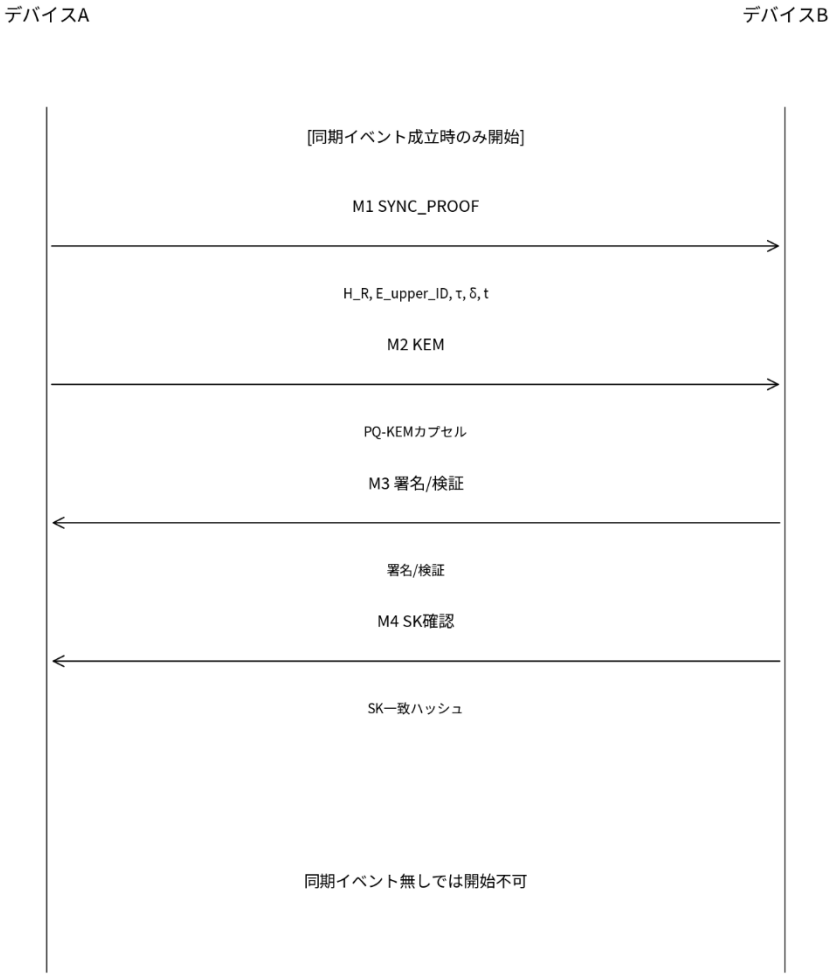
【図８】

図8 副チャネルおよびタンパ対策



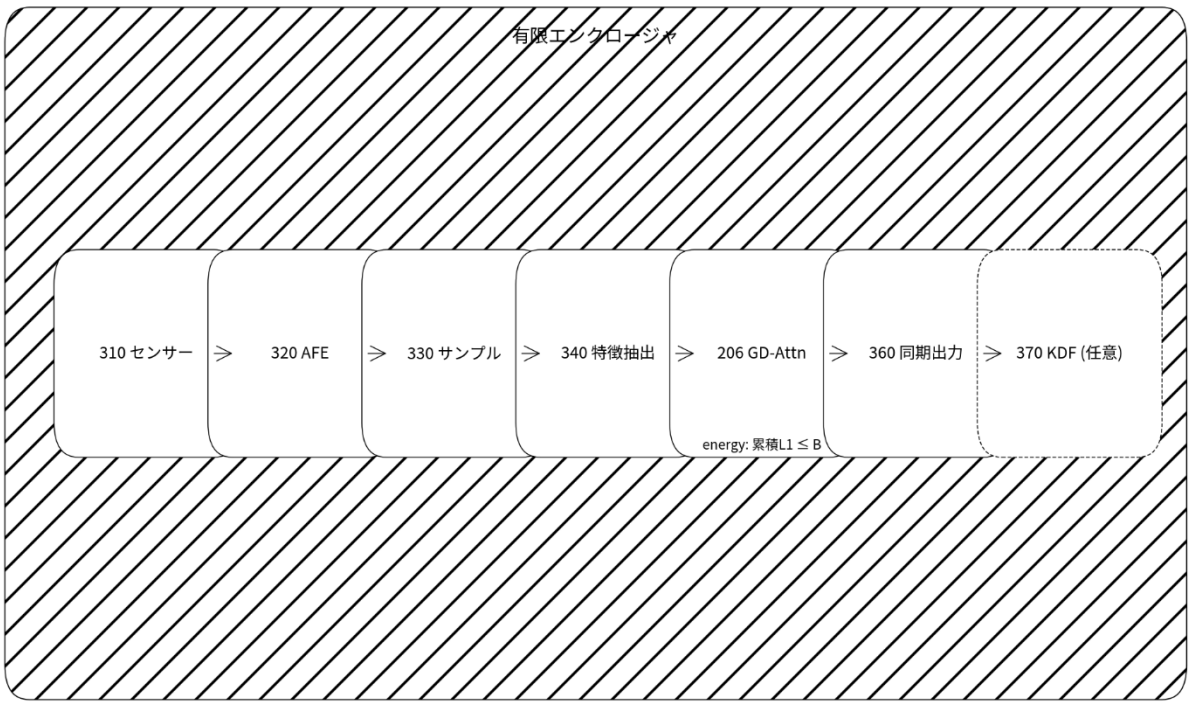
【図９】

図9 プロトコル時系列（同期トリガ）



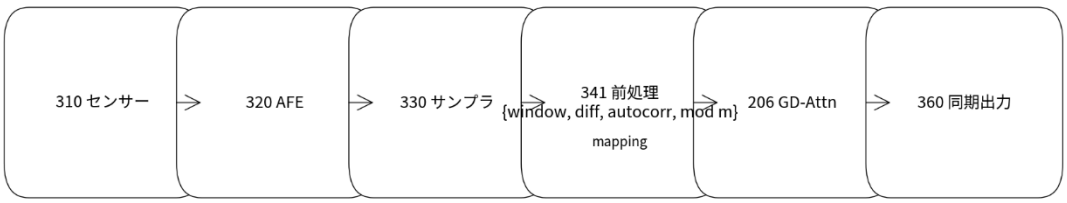
【図１０】

図10 センサー実装 (有限閉包)



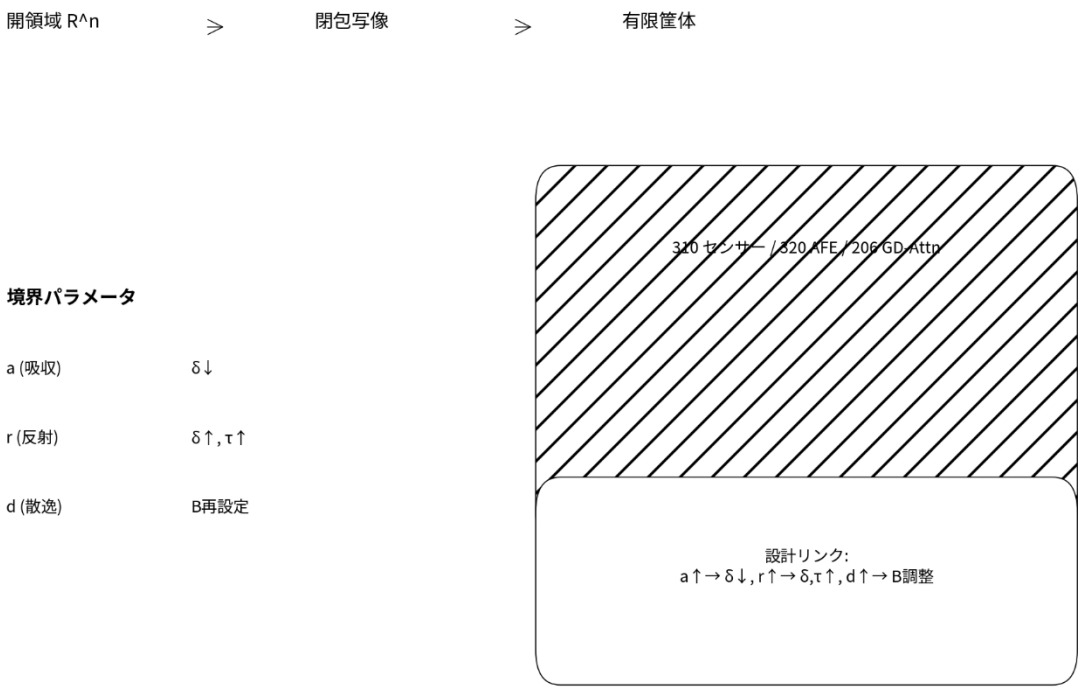
【図１１】

図11 既存観測チェーンからの写像



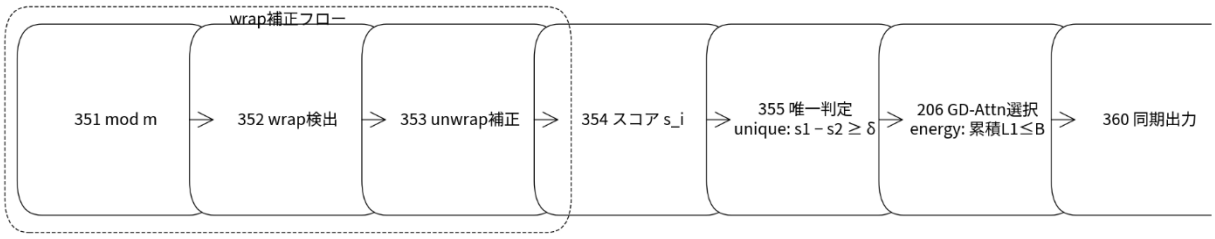
【図１２】

図12 有限閉包と筐体パラメータ



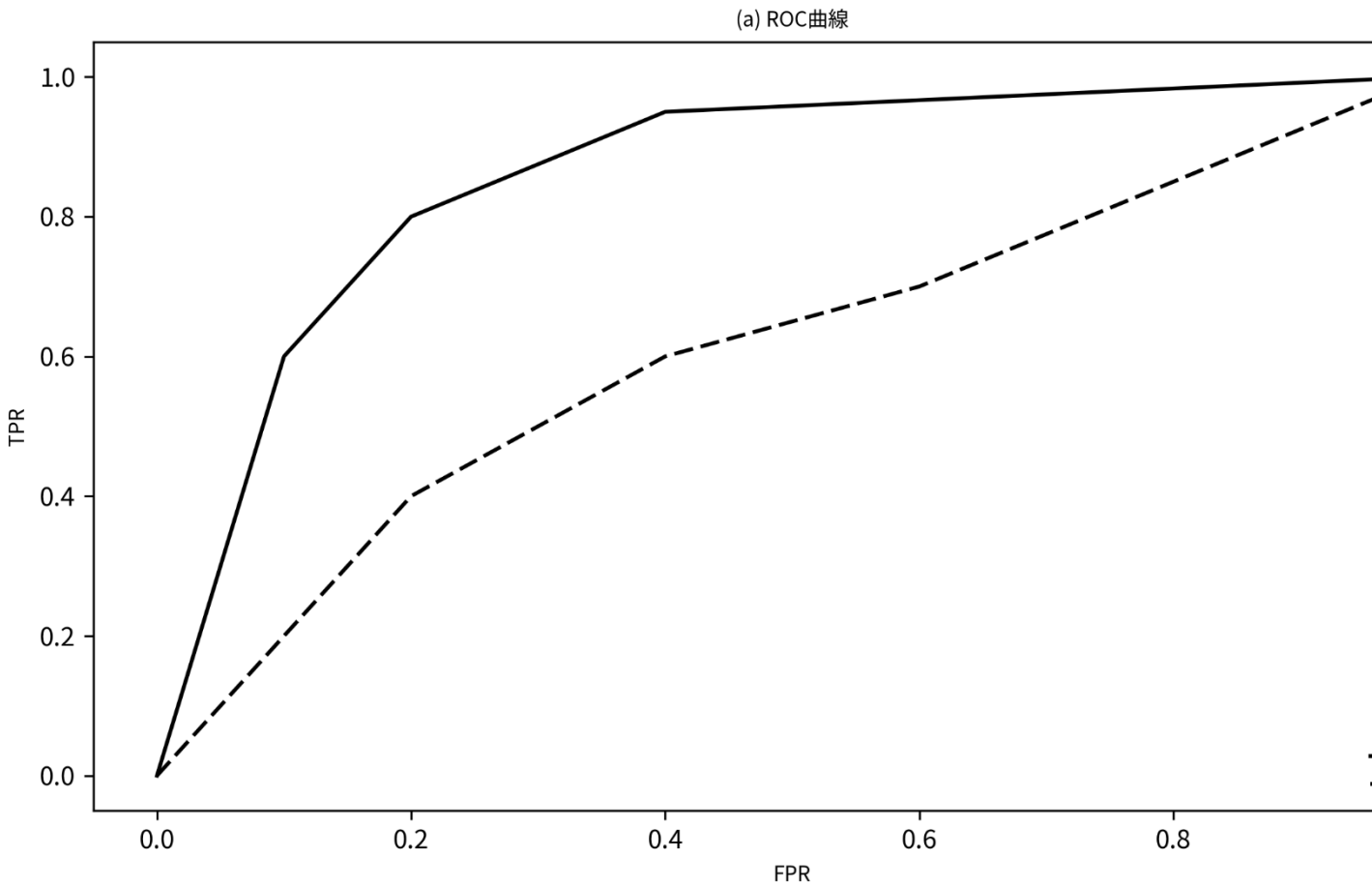
【図１３】

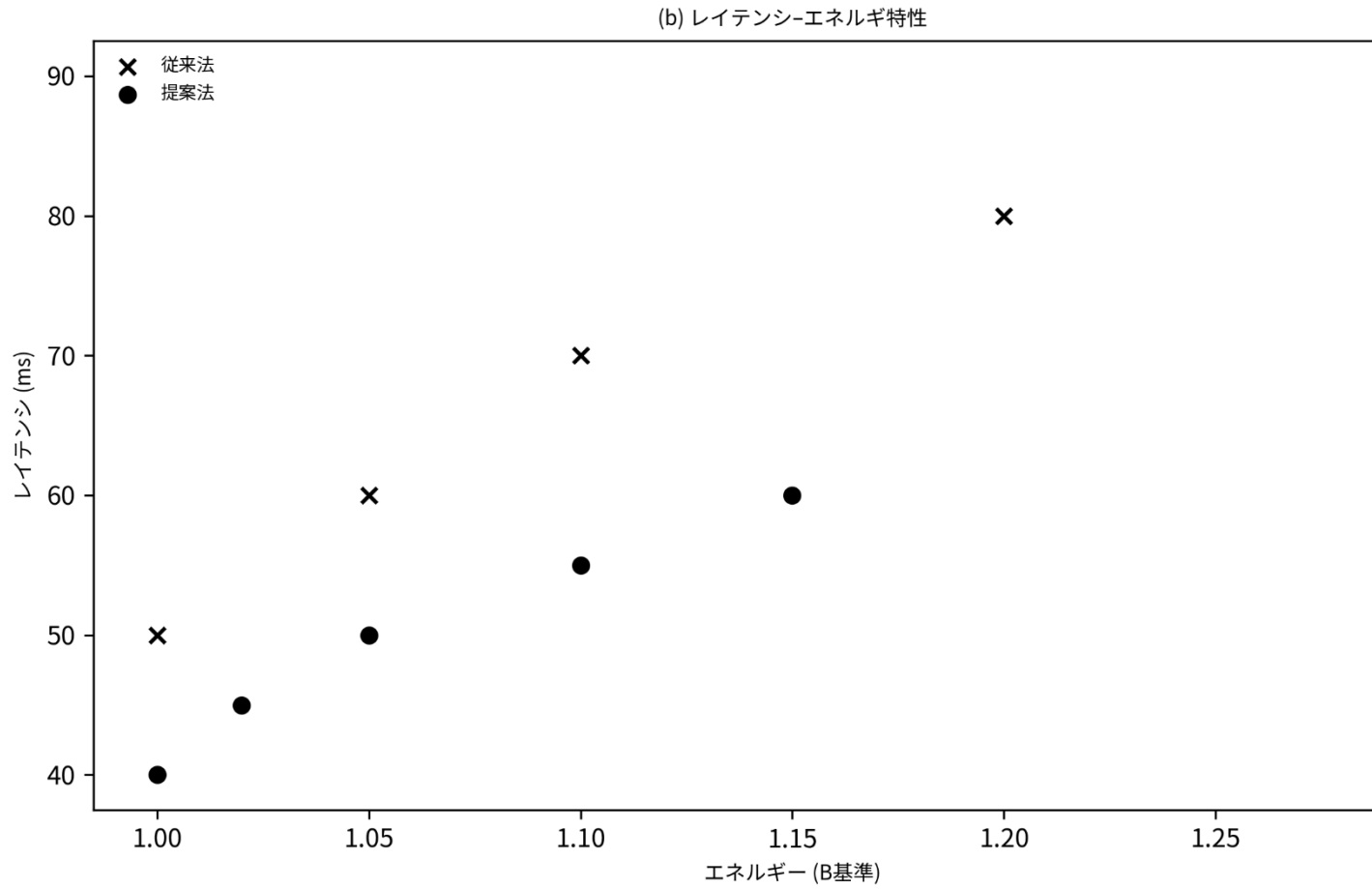
図13 周期入力処理と選択



【図１４】

図14 性能評価


(a) ROC曲線
TPR
FPR
0.0
0.2
0.4
0.6
0.8
1.0


(b) レイテンシ–エネルギ特性
従来法
提案法
レイテンシ (ms)
エネルギー (B基準)
40
50
60
70
80
90
1.00
1.05
1.10
1.15
1.20
1.25

【図１５】

図15 統合同期セキュリティ・ブロック図（番号なし／図1準拠）