【書類名】　　明細書
【発明の名称】通信一体型ゼロトラストセキュリティ装置、方法及びプログラム
【技術分野】
【０００１】
本発明は、情報通信ネットワークにおけるセキュリティ技術に関し、特に通信プロトコル層とセキュリティ核を一体化し、(i) 時間窓制約（RTT≦T_max、±DELTA_Ssync）によるメッセージ有効化、(ii) nonce/CTR による再生攻撃防止、(iii) PUF バインドと KDF によるセッション鍵 SK(t) の周期ローテーション（重なり epsilon を含む）、(iv) 侵害兆候時の即時ゼロ化と PUF 再加入による経路再確立、(v) 非ブロックチェーン型監査ハッシュ鎖へのイベント記録、を通信運用として統合する技術に関する。適用対象は、IP 系（TCP/UDP/QUIC）、無線（5G/4G/LPWA）、産業用フィールドバス、エッジ-クラウド構成、OS/半導体実装を含む広範な通信システムである。
【背景技術】
【０００２】従来、ネットワークのセキュリティは通信スタックとは独立した層（TLS/IPsec/VPN、ID 基盤、監査系）として運用されることが多く、運用ポリシーとプロトコル動作が分離していた。この分離は、ポリシー違反の検知や鍵運用の失敗が、実際のパケット授受や遅延特性に反映されにくいという構造的な弱点をもたらす。
【０００３】具体的には、以下の課題が知られている。
（１）層間断絶：認証・認可・鍵更新の判断がアプリ/管理プレーンに偏在し、データプレーンの実時間制約（往復遅延、ジッタ、順序性）と連動しない。
（２）時間窓・同期の未統合：実運用では RTT の上限やクロックずれの許容幅を明示しないまま、再送・再試行を重ねるため、攻撃時にタイムウィンドウが拡張され、攻撃面が広がる。
（３）再生攻撃と鍵ローテの整合：nonce あるいはカウンタの重複検知、並びに鍵ローテーションの重なり期間の扱いが製品ごとに相違し、順序逆転や再生攻撃の温床となる。
（４）信頼の起点の脆弱化：証明書中心の設計では端末実体への結び付きが弱く、複製困難性の低い秘密情報に依存しがちである。物理的複製困難関数（PUF）の組み込みが標準化されていない。
（５）侵害時の復旧遅延：侵害兆候検知後のゼロ化（鍵・一時領域の消去）と再加入（信頼の再確立）の手順が体系化されておらず、復旧の遅れや残留リスクを招く。
（６）監査の重さ・断片化：改ざん耐性の高い監査はブロックチェーン等の重厚な基盤へ寄りがちで、軽量なハッシュ鎖やイベント連鎖の最小運用が整理されていない。
（７）多者連携での強制参加性：委任・中継・フェデレーション環境において、沈黙・遅延・拒否といった振る舞いを通信レベルで一義に取り扱う基準が不足する。
（８）OT/産業系の制約：フィールドバスやエッジ-クラウド混在の現場では厳格な遅延上限・可用性が求められる一方、既存フレームワークは一般 IT 前提でチューニングされており、現場要件と齟齬をきたす。
【０００４】ゼロトラストの考え方は広く知られるが、実装段階では、（１）から（８）の各要素が通信プロトコルの一次制御量として明示化・数理化されていないため、運用と通信の乖離が残存する。特に、時間窓（RTT≦T_max、同期許容 ±DELTA_Ssync）、再生攻撃

防止（nonce/CTR の一意性と単調性）、鍵ローテの重なり期間 epsilon の厳格運用、侵害時の即時ゼロ化と再加入の規範化、軽量監査鎖への逐次コミットを、通信運用として一体的に実装・検証可能な形で提供する基盤が望まれている。

【０００５】また、端末実体と鍵素材の結合については、秘密鍵保護のみならず、PUF による端末固有性の担保と KDF によるセッション鍵 SK（t）の周期更新を、再送・順序制御・遅延境界と同一の設計座標で扱う必要がある。これにより、鍵運用の失敗が通信上の異常（RTT 超過、順序違反、再生）として即時に現れ、逆に通信異常が鍵運用の抑制・ゼロ化へ自動連鎖するような、双方向の統一制御が実現される。

【０００６】以上の通り、従来技術には、（１）から（８）に列挙した運用と通信の分断、および時間・順序・鍵運用の未統合という課題が存在する。これらを解消し、通信プロトコル層とセキュリティ核を一体化して、時間窓・再生防止・鍵ローテ・ゼロ化復旧・監査連鎖を最小限の規則集合で運用できる枠組みが求められている。

【先行技術文献】

【特許文献】

【０００７】

US 2009/0083833 A1, “Authentication with Physical Unclonable Functions”, 2009-03-26.

【０００８】

US 10,038,564 B2, “Physical Unclonable Function using Augmented Memory for Authentication”, 2018-07-31.

【非特許文献】

【０００９】

RFC 5869: “HMAC-based Extract-and-Expand Key Derivation Function (HKDF)”, H. Krawczyk, P. Eronen, 2010-05.

【００１０】

NIST SP 800-56C Rev.2, “Recommendation for Key-Derivation Methods in Key-Establishment”, 2020.

【００１１】

FIPS 203, “Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)”, NIST, 2024.

【００１２】

FIPS 204, “Module-Lattice-Based Digital Signature Standard (ML-DSA)”, NIST, 2024.

【００１３】

RFC 9334: “Remote ATtestation procedureS (RATS) Architecture”, IETF, 2023.

【００１４】

NIST SP 800-207, “Zero Trust Architecture”, 2020.

【００１５】

RFC 8446: “The Transport Layer Security (TLS) Protocol Version 1.3”, IETF, 2018-08.

【００１６】
RFC 4303: “IP Encapsulating Security Payload (ESP)”, IETF, 2005-12.（再生防止ウィンドウ）
【００１７】
RFC 9000/9001/9002: “QUIC: Transport/Using TLS/Loss Detection & Congestion Control”, IETF, 2021-05.
【００１８】
RFC 9147: “Datagram Transport Layer Security (DTLS) 1.3”, IETF, 2022-04.
【００１９】
B. Schneier, J. Kelsey, “Secure Audit Logs to Support Computer Forensics”, ACM TISSEC, 1999.
【発明の概要】
【００２０】
本発明は、通信プロトコル層とセキュリティ核を一体化し、往復遅延・同期・順序・鍵ライフサイクル・監査を同一の設計座標で制御する枠組みを提供する。運用ポリシーと通信実装の乖離をなくし、時間窓の上限化・再生防止・迅速復旧・軽量監査を小規則で実現する点に特徴がある。
【００２１】
中核として、リアルタイム版 UWP(adaptive finite closure)を導入する。可変帯域 Xi(t)・可変平滑 tau(t)・固定 lambda の下で、窓付きカーネルの正性下界 delta_hat_pos(t) を逐次算出し、これを安全余裕としてプロトコル制御に直結する。delta_hat_pos(t) が閾値を下回ると、プロトコルは fail-close（メッセージ無効化・ゼロ化・再加入）へ即時遷移する。※数式・記号は特許方針に従い ASCII で記述。
【００２２】
本枠組みにおいて、時間窓（RTT <= T_max）、同期許容（±Delta_sync）、再生防止（nonce/CTR の一意・単調）、鍵ローテ期間（T_rot）および併存窓（epsilon）は、delta_hat_pos(t) に基づきリアルタイム適応される。観測される遅延・ジッタ・損失・順序乱れが増すほど、許容窓は自動的に狭まる方向に働き、攻撃面を有限に保つ。
【００２３】
さらに、本発明は異論（＝意味的外乱）検知と再整合（SemOps）層を統合する。意味エネルギー E_sem(t) を定義し、（ａ）ポリシー矛盾（purpose/data_class/policy_id の不整合）、（ｂ）監査ログや RATS 証跡との矛盾、（ｃ）ヒューマン・フィードバック（承認/留保/却下）から得られる異論度 A_sem(t) と dE_sem/dt を監視する。A_sem(t) の上昇または dE_sem/dt > 0 が検知された場合、プロトコルは（ｉ）時間窓の即時縮小、（ｉｉ）当該フローのセーフホールド（一時停止）と人間確認の挿入、（ｉｉｉ）必要に応じたゼロ化→再加入へと安全側に自動遷移する。
【００２４】
運用上は、各メッセージに軽量メタデータ（policy_id, purpose, data_class, attestation_digest など）を付す意味タグ付け通信を採用し、SemOps 層が提案→整合→コミットの最小手続きを実行する。コミット済みイベント（加入/ローテ/ゼロ化/意味整合

結果）は非ブロックチェーン型ハッシュ鎖へ逐次記録することで、改ざん検出性と低遅延を両立する。

【００２５】

制御の単調性は、V(t) := E_mech(t) + lambdaE_sem(t) + (rho/2)||x||^2 を用いて表現される。ここで Security(t) := -dV/dt、A_mech(t) := ||grad_x E_mech||^2、A_sem(t) は意味的外乱の指標である。通信マージン M_comm(t)（T_max-RTT, Delta_sync-|clock_skew|, T_rot-key_age 等）と意味マージン M_sem(t)（整合スコアや人間承認状態）を設け、適応則により

dV/dt <= -kappa_mech*||phi||^2 - kappa_commM_comm(t) - kappa_semM_sem(t) + gamma*||w||^2

を満たすよう制御することで、**有限閉包（finite closure）**を維持する。

【００２６】

本発明は、（１）IP 系（TCP/UDP/QUIC）、（２）無線（５G/LPWA）、（３）産業用フィールドバス、（４）エッジ-クラウド連携に適用でき、PUF バインド/KDF 生成/鍵ローテ/ゼロ化-再加入/監査鎖/SemOps を単一の状態遷移機械として実装できる。

【００２７】

効果は次の通りである。（１）時間窓の厳格化で攻撃面を時間上限化し、（２）再生防止の一義化で遅延再提出・順序逆転を遮断し、（３）鍵ローテ併存窓の厳格運用で旧鍵悪用を抑止し、（４）ゼロ化-再加入の即時連鎖で復旧を高速化し、（５）軽量監査鎖で責任追跡性を確保し、（６）SemOps 層により意味的外乱（異論）を検知して再整合できるため、ソーシャルエンジニアリングや内部不正、ポリシー逸脱に対しても安全単調性を維持できる。

【００２８】

以上により、本発明は、従来の「セキュリティ運用を通信に付加する」方式と異なり、通信そのものを UWP による有限閉包と SemOps に従属させる設計原理を提供する。負荷変動時や組織的異論発生時にも、小さな規則集合で大域的な安全単調性と意味整合を両立できる。

【発明が解決しようとする課題】

【００２９】

本発明が対象とする技術分野では、セキュリティ運用と通信プロトコルが分断されている結果、実時間の遅延・順序・同期特性と、認証・鍵運用・監査・復旧の各手続が乖離し、攻撃面の拡大・復旧遅延・監査断片化を招いている。さらに、運用上の「異論（＝意味的外乱）」が通信面に反映されず、意味整合の破れが安全性に直結しないという構造的な欠陥が残存する。

【００３０】

解決すべき具体的課題は、少なくとも次のとおりである。

（１）層間断絶：通信データプレーンとセキュリティ運用（認証・認可・鍵管理・監査）の分離。

（２）時間窓・同期の未統合：RTT 上限や ±Delta_sync の明確化・強制がなく、再送・リ

トライで実効窓が弛緩する。
（３）再生攻撃/順序逆転の一義的拒否欠如：nonce/CTR の一意・単調運用が不徹底で、並列経路・遅延再提出を許容。
（４）鍵ローテの併存管理の未整備：T_rot と併存窓 epsilon の規定不足により旧鍵悪用や不整合が発生。
（５）侵害時の遅延復旧：ゼロ化と再加入の規範化不足により、復旧時間が読めず残留リスクが高い。
（６）監査の重さ・断片化：ブロックチェーン偏重またはログ分散により、低遅延・改ざん検出性・実装容易性の両立が困難。
（７）PUF/実体バインド不足：証明書依存で端末実体との結合が弱く、複製困難性に基づく識別・鍵導出が標準化されていない。
（８）多者連携における強制参加性の不在：沈黙・遅延・拒否の扱いが統一されず、委任や中継で曖昧さが残る。
（９）ＯＴ/産業系への適合困難：厳格な遅延・可用性要件を、少数パラメータで通信と一体に制御できない。
（１０）意味的外乱（異論）の未検知/未整合：policy_id・purpose・data_class、RATS/監査証跡と運用実態の不一致を通信面で即時に扱えない。
（１１）リアルタイム適応の欠如：ネットワーク状態変動に応じて許容窓を自動で狭める仕組み（adaptive finite closure：Xi(t), tau(t), lambda, delta_hat_pos(t)）が欠落。
（１２）安全単調性の証明可能設計の不在：E(t), -dE/dt, ||grad E||^2 に基づく機械的整合と意味的整合の統一的な減衰（finite closure）が示せない。
【００３１】
したがって、（１）から（１２）を同一の設計座標で同時に扱い、少数の公開パラメータ{T_max, Delta_sync, T_rot, epsilon} と適応指標 delta_hat_pos(t) を核に、通信・鍵運用・監査・復旧・意味整合（SemOps）を一体で制御できる枠組みが求められる。これにより、攻撃面の時間的上限化、再生防止の一義化、旧鍵悪用の抑止、迅速復旧、監査一貫性、意味的外乱への即応を、小さな規則集合で実現することが課題である。
【００３２】
本発明は、上記課題を解決し、通信そのものを適応型有限閉包（UWP）と SemOps に従属させる設計原理を確立することを目的とする。
【課題を解決するための手段】
【００３３】
本発明は、装置・方法・プログラムとして実装され、通信プロトコル層とセキュリティ核を一体化する複数の手段を状態遷移機械で統合する。主要構成は、（１）時間窓・同期管理手段、（２）再生防止手段、（３）ＰＵＦバインド鍵生成・ローテ手段、（４）ゼロ化・再加入手段、（５）適応型ＵＷＰ（adaptive finite closure）推定手段、（６）SemOps（異論＝意味的外乱）検知・再整合手段、（７）軽量監査ハッシュ鎖記録手段、（８）状態遷移オーケストレーション手段、（９）ポリシー交渉・伝達手段、から構成される。
【００３４】
時間窓・同期管理手段は、各メッセージについて往復遅延（ＲＴＴ）を計測し、ＲＴＴ≦Ｔ

_max の制約を適用する。端点間の時刻差を監視し、±Delta_sync を超えた場合は再同期手続に遷移する。これにより、再送・リトライに起因する実効タイムウィンドウの弛緩を防ぎ、攻撃面を時間的に上限化する（図１３参照）。

【００３５】

再生防止手段は、各方向のメッセージへ nonce/ＣＴＲ を付与し、一意・単調性を検証する。同一 nonce、逆順ＣＴＲ、ウィンドウ外の番号は即時拒否する。並列経路・遅延再提出・順序逆転に対して通信レイヤでの一義的拒否を実現する（図１３参照）。

【００３６】

ＰＵＦバインド鍵生成・ローテ手段は、端末のＰＵＦ応答を用いて SK(t) を ＫＤＦ（例：ＨＫＤＦ） で導出し、Ｔ_rot 毎に更新する。旧鍵との併存時間 epsilon を規定し、併存窓外での旧鍵利用を禁止する。鍵年齢・ローテ状態は通信制御に露出し、運用とプロトコルが同一座標で制御される（図１４参照）。

【００３７】ゼロ化・再加入手段は、侵害兆候、時間窓違反、再生検知、又は後述の適応指標低下に応じて、鍵素材・一時領域・カウンタを即時ゼロ化し、ＰＵＦチャレンジに基づく再加入手続を実行する。ゼロ化→再加入はプロトコル規則として
自動連鎖する（図１４参照）。

【００３８】

適応型ＵＷＰ推定手段は、可変帯域 Xi(t)・可変平滑 tau(t)・固定 lambda の下で、窓付きカーネルの正性下界 delta_hat_pos(t) を逐次算出する。delta_hat_pos(t) を安全余裕として用い、ネットワーク状態（遅延・ジッタ・損失・順序乱れ）が悪化するほど、Ｔ_max/Delta_sync/Ｔ_rot/epsilon を自動的に厳格化する。delta_hat_pos(t) が閾値未満の場合、当該フローは fail-close（無効化・ゼロ化・再加入）へ即時遷移する。

【００３９】

SemOps（異論＝意味的外乱）検知・再整合手段は、メッセージへ policy_id/purpose/data_class/attestation_digest 等の意味タグを付与させ、（ａ）ポリシー矛盾、（ｂ）ＲＡＴＳや監査証跡との齟齬、（ｃ）人間承認イベントの留保・却下、を異論度として計測する。異論度上昇時は、（ｉ）時間窓の即時縮小、（ｉｉ）当該フローのセーフホールド（一時停止）と人間確認挿入、（ｉｉｉ）必要に応じたゼロ化→再加入に自動遷移して再整合を完了する。

【００４０】

軽量監査ハッシュ鎖記録手段は、加入/離脱/鍵更新/ゼロ化/意味整合結果を非ブロックチェーン型ハッシュ鎖に逐次コミットする。検証は０（１）で可能であり、改ざん検出性と低遅延を両立する。外部アンカー（時刻署名等）への定期ピン留めも選択的に行える。

【００４１】

状態遷移オーケストレーション手段は、少なくとも（１）初期化、（２）認証中、（３）稼働、(４)ローテ中、(５)ゼロ化、(６)再加入、の状態を持ち、各遷移に Ｔ_max/Delta_sync/Ｔ_rot/epsilon/nonce の整合条件と delta_hat_pos(t) の閾値を付与する。通信マージン M_comm（Ｔ_max−ＲＴＴ、Delta_sync−|clock_skew|、Ｔ_rot−key_age 等）と意味マージン M_sem を監視し、d/dt V<=−kappa_mech||phi||^2−kappa_commM_comm−kappa_semM_sem+gamma||w||^2** の形で有

限閉包を維持する。
【００４２】
ポリシー交渉・伝達手段は、ハンドシェイク時に｛T_max, Delta_sync, T_rot, epsilon, Xi_profile, tau_range｝を相互通告・合意し、不一致時は安全側デフォルトへフォールバックする。交渉結果は意味タグと共に監査鎖へコミットされる。
【００４３】
本構成は、ＩＰ系（ＴＣＰ/ＵＤＰ/ＱＵＩＣ）、無線（５Ｇ/ＬＰＷＡ）、産業用フィールドバス、エッジ-クラウド混在へ横断的に適用可能である。ハードウェア（ＰＵＦ内蔵セキュア素子）、ＯＳドライバ、ユーザ空間ライブラリのいずれの層にも配置できる。図１から図１０の基礎図に加え、**図１３（Attack/Delay Map）および図１４（Zero-Trust Deployment）**が本手段の実装要点を示す。
【００４４】
本発明は、プログラムとして提供され、プロセッサが前記手段を実行することで同等の効果を奏する。設定パラメータは運用ポリシーに応じて外部から更新可能であり、更新イベントは監査鎖に記録される。
【００４５】
非限定例として、運用初期値は Ｔ_max＝○○○、Delta_sync＝○○○、Ｔ_rot＝○○○、epsilon＝○○○ とし、Xi(t)・tau(t) は回線品質に応じて自動調整される。delta_hat_pos(t) の閾値はサービス重要度に応じて設定し、境界付近では図１３の時間窓を縮小、図１４のゼロ化→再加入の連鎖を優先させる。
【００４６】
以上の構成により、通信・鍵運用・復旧・監査・意味整合が同一の一次制御量で結び付けられ、ネットワーク状態変動や運用上の異論発生時にも、小さな規則集合で大域的な安全単調性（適応型有限閉包）を維持できる。

【発明の効果】
【００４７】
本発明は通信プレーンとセキュリティ核を一体化し、往復遅延がＴ_max を超えない時間窓と時刻同期の許容幅±DELTA_Ssync を通信規則として強制し、各方向メッセージにｎｏｎｃｅ/ＣＴＲの一意・単調運用を課すことで、再生攻撃と順序逆転を一義に拒否し攻撃面を有限に保つ。さらに鍵ローテ周期Ｔ_rot と旧鍵併存時間 epsilon を厳格管理して旧鍵悪用を抑止し、侵害兆候や時間窓違反等の検知時には即時ゼロ化からＰＵＦ再加入へ自動連鎖させて復旧時間を短縮し残留リスクを低減する。
【００４８】
本発明はリアルタイム版ＵＷＰ（ａｄａｐｔｉｖｅ ｆｉｎｉｔｅ ｃｌｏｓｕｒｅ）によりネットワーク状態に応じてＴ_max・DELTA_Ssync・Ｔ_rot・epsilon を自動適応し安全単調性を維持する。意味的外乱を扱うＳｅｍＯｐｓ層がｐｏｌｉｃｙ＿ｉｄ・ｐｕｒｐｏｓｅ・ｄａｔａ＿ｃｌａｓｓやＲＡＴＳ証跡と運用実態の不整合を検知し、対象フローをセーフホールドや時間窓の即時縮小、必要に応じたゼロ化→再加入へ強制遷移させて再整合を完了する。加入・鍵更新・ゼロ化・意味整合結果は非ブロックチェーン型ハッシュ鎖へ

逐次コミットし、改ざん検出性と低遅延を両立する。

【００４９】

本発明は委任・中継・フェデレーションを含む多者連携で沈黙・遅延・拒否を一義に取り扱う強制参加性を確立し、ＴＣＰ/ＵＤＰ/ＱＵＩＣやＤＴＬＳ、ＩＰｓｅｃ、産業用フィールドバス等へ段階的に適用できる。ＰＵＦバインドとＫＤＦにより装置固有性と方式非依存の鍵導出を実現し、ポスト量子暗号への移行にも耐性を持つ。公開パラメータを少数集合｛Ｔ_max, DELTA_Ssync, Ｔ_rot, epsilon｝に集約することで監査容易性と運用自動化を促進し、ＯＳ/ドライバ/半導体層での実装容易性と低コスト展開、規制適合性とＳＬＡ遵守の向上を同時に達成する。

【図面の簡単な説明】

【００５０】

【図１】端末・ゲートウェイ・コア鍵管理・時刻同期・監査鎖を一体化し、通信プレーンとセキュリティ核を同一構成で示す全体ブロック図

【図２】入出力から時刻同期・RTT 測定・PUF 応答取得・KDF 導出・セッション鍵確立・意味タグ付与・監査コミットまでの連続パイプライン図

【図３】沈黙・遅延・拒否を強制参加規則で一義に扱い、タイムアウト到達時にゼロ化へ遷移し再加入で復帰する分岐運用図

【図４】初期化・認証中・稼働・ローテ中・ゼロ化・再加入の状態と、T_max・Delta_sync・鍵年齢・nonce/CTR 整合に基づく遷移を示す状態機械図

【図５】侵害兆候・時間窓違反・再生検知をトリガとして鍵素材・一時領域・カウンタを即時消去し PUF 再加入に自動連鎖させるゼロ化手順図

【図６】加入・鍵更新・ゼロ化・意味再整合の各イベントを prev_hash で連結し、RATS 測定と署名、必要に応じ外部時刻署名へアンカーする監査およびアテステーション手順図

【図７】ハンドシェイクからデータ送受信までの時系列上で RTT 測定・nonce/CTR 検査・再送条件・鍵ローテ挿入点・再同期条件を示すシーケンス図

【図８】委任主体・中継主体・受益主体を分離し最小権限で鍵配布し、沈黙・遅延・拒否を共通規則で扱うマルチパーティ通信経路図

【図９】PUF 内蔵セキュア素子・デバイスドライバ・カーネルモジュール・ユーザ空間ライブラリの対応と、RTT 計測フック・再生検査・MMIO ゼロ化経路の低レイヤ実装を示す層構成図

【図１０】有限エネルギー制約 B と一致性マージン Delta による受理域を示し、E_upper を基準に S(x) ¥geqE_upper+Delta を連続維持して安全単調性を確保する位置付け図

【図１１】接続時のポリシー交渉をハンドシェイクに組み込み、T_max・Delta_sync・T_rot・Epsilon・XI_profile・TAU_range を相互通告し合意または安全側フォールバックし、その結果を監査鎖にコミットする手順図

【図１２】加入・鍵更新・ゼロ化・意味再整合の各イベントを prev_hash で鎖状に記録し、必要に応じ第三者時刻署名へアンカーする軽量監査ハッシュ鎖の構造と検証方法を示す図

【図１３】RTT 境界と再生拒否と再同期条件の関係を時間窓上に可視化し、窓外イベントおよび重複 nonce・逆順 CTR を即時拒否し、境界接近時は許容窓を自動縮小する適応挙動図

【図１４】端末・ゲートウェイ・コア鍵管理・時刻同期監視・監査ログ・ゼロ化再加入の配備構成を示し、鍵ローテと侵害検知時のゼロ化から再加入への連鎖を運用フローとして示す図
【図１５】暗号・時間窓・再生検知・ゼロ化再加入を統合したエンドツーエンド fail-close テストベンチの構成および計測項目を示す図
【図１６】SemOps 層による異論（意味的外乱）検知から再整合・承認・監査コミットまでの介入フローを示し、policy_id・purpose・data_class・attestation_digest の処理を含む図
【発明を実施するための形態】
【００５１】
本実施形態は、図１に示す通信プレーンとセキュリティ核を一体化した構成を採用する。装置は端末装置、ゲートウェイ、コア鍵管理の３ブロックを基本単位とし、各ブロックに時間窓管理、再生防止、ＰＵＦバインド鍵生成、ゼロ化と再加入、監査ハッシュ鎖、適応型ＵＷＰ推定、SemOps の各モジュールを配置する。
【００５２】
端末装置はセキュア素子又は同等機能（ＰＵＦ、耐タンパメモリ、真性乱数源）を備え、ＯＳドライバ層でカウンタ（nonce/CTR）、鍵年齢、時刻同期情報をエクスポートする。ゲートウェイは遅延測定と順序検査を実時間で行い、コアはＫＤＦによる鍵合意、監査記録、ポリシー配信を担う。図９に各層の配置を示す。
【００５３】
通信スタックはＩＰ（ＴＣＰ/ＵＤＰ/ＱＵＩＣ）及び無線（５Ｇ/ＬＰＷＡ）、産業用フィールドバスの少なくとも一つに適合する。ハンドシェイクは図７の時系列に従い、トランスポート種別に依らず共通の意味タグとポリシー交渉を先頭に行う。
【００５４】
時間窓管理は、各メッセージごとにＲＴＴを測定し、ＲＴＴ<=T_max を満たさないメッセージを無効とする。端点間時刻差は clock_skew として推定し、|clock_skew|<=Delta_sync の範囲でのみデータ適用を許可する。超過時は再同期フローへ遷移し、適用保留とする。
【００５５】
再生防止は、送受信方向ごとに単調増加する CTR 又は一意な nonce を付与し、ウィンドウ外の番号、重複 nonce、逆順到着を即時に拒否する。並列経路を含む構成では、パス識別子と組み合わせて一意性を維持する。図６にウィンドウの概念を示す。
【００５６】
鍵生成は、端末のＰＵＦ応答とセッション固有情報を入力としてＫＤＦ（例 HKDF）を用いて SK(t) を導出する。鍵ローテーションは周期 T_rot で実行し、旧鍵と新鍵の併存時間 epsilon を設定して移行を滑らかにする。併存窓外での旧鍵適用は拒否する。
【００５７】
ゼロ化は、侵害兆候、時間窓違反、再生検知、意味的外乱による保留が所定条件を満たした場合に発火し、鍵素材、派生鍵、揮発キャッシュ、カウンタ、セッション状態を即時消去する。ゼロ化後はＰＵＦチャレンジを用いた再加入手続きを自動実行する。図５と図１４に動作を示す。

【００５８】
再加入は、端末の実体性をＰＵＦで再確認し、ポリシー交渉、意味タグの再設定、鍵合意の順に行う。中断時間が長い場合は監査鎖への復帰コミットを伴い、セッション識別子を更新する。
【００５９】
監査ハッシュ鎖は、加入、離脱、鍵更新、ゼロ化、意味整合結果、パラメータ更新をイベントとして逐次コミットする。各イベントは header||payload||prev_hash のハッシュでチェーン化し、定期的に外部時刻署名へアンカーする。検証は先頭又は任意点からの再計算で可能とする。図１２に構造を示す。
【００６０】
適応型ＵＷＰ推定は、可変帯域 Xi(t)、可変平滑 tau(t)、固定 lambda に基づく窓付きカーネルから正性下界 delta_hat_pos(t) を逐次算出する。通信品質が低下するにつれ delta_hat_pos(t) は低下し、所定閾値未満で fail-close を指示する。閾値以上では T_max、Delta_sync、T_rot、epsilon を安全側へ段階的に調整する。
【００６１】
制御ロジックは、通信マージン M_comm=(T_max-RTT, Delta_sync-|clock_skew|, T_rot-key_age 等）と意味マージン M_sem（SemOps が算出する整合スコア）を監視し、dV/dt<=-kappa_mech*||phi||^2 -kappa_comm*M_comm* -*kappa_sem*M_sem + gamma*||w||^2 を満たすよう遷移とパラメータを更新する。V は機械的整合と意味的整合を合成したエネルギー関数である。
【００６２】
SemOps は、各メッセージに policy_id、purpose、data_class、attestation_digest 等の意味タグを付与させ、ポリシー矛盾、RATS 結果の不一致、人間承認の留保・却下を異論度として計測する。異論度が閾値を超えた場合、当該フローをセーフホールドし、時間窓を縮小し、必要に応じゼロ化→再加入へ遷移させる。
【００６３】
状態遷移機械は、初期化、認証中、稼働、ローテ中、ゼロ化、再加入を含み、各遷移に T_max、Delta_sync、T_rot、epsilon、nonce の整合条件、delta_hat_pos(t) の閾値、SemOps の整合条件を紐付ける。図４に遷移条件を示す。
【００６４】
典型的な動作は次の通りである。初回接続でポリシー交渉と意味タグ交換を行い、ＰＵＦ認証とＫＤＦにより SK(t) を確立する。稼働中は図７の時系列に従い、ＲＴＴ測定と再生検査を継続する。鍵年齢が T_rot に達するとローテを開始し、epsilon 内で旧鍵を無効化する。異常検知時はゼロ化し、再加入へ遷移する。
【００６５】
マルチパーティ構成では、図８に示すように委任と中継を考慮し、参加主体ごとにポリシーと意味タグを分離管理する。鍵配布は最小権限で行い、沈黙、遅延、拒否は強制参加の規則に従って一義的に扱う。
【００６６】
ＯＳと半導体層の実装は、図９に示すように、ＰＵＦデバイスをドライバ経由でユーザ空

間へ安全に露出し、MMIO 又はメッセージバスでゼロ化命令を即時伝搬する。カーネルモジュールはＲＴＴ測定フックと再生検査を提供する。

【００６７】

代表パラメータは初期設定として T_max=〇〇〇、Delta_sync=±〇〇〇、T_rot=〇〇〇、epsilon=〇〇〇 を用いる。Xi(t) と tau(t) は回線品質に応じプロファイルから選択し、delta_hat_pos(t) の閾値はサービス重要度に応じて設定する。

【００６８】

フォールト耐性として、ネットワーク分断時はローカル監査鎖を保持し、再接続時にマージする。時刻源の異常が疑われる場合、Delta_sync を厳格化し適用を停止する。島化動作では最小限のフローのみ許可する。

【００６９】

産業用フィールドバスでは、制御周期と T_max を一致させ、図１３の時間窓を周期境界に合わせて設計する。ゲートウェイはフィールド側とＩＰ側の時刻同期を橋渡しし、意味タグのマッピングを提供する。

【００７０】

セキュリティ上の留意点として、CTR は電源断後も単調性を維持するよう安全カウンタを用いる。時刻改ざん対策として安全時刻源又は複数時刻源の合意を用意する。ＰＵＦ応答はマスク化し、派生鍵のみを上位に露出する。

【００７１】

性能面では、時間窓検査、ＲＴＴ測定、再生検査は線形時間で処理可能であり、監査鎖のコミットは定数時間で完了する。ローテ処理は epsilon 内に収束し、追加遅延は T_max の範囲内で管理される。

【００７２】

変形例として、トランスポートにＤＴＬＳ又はＱＵＩＣを用いる構成、監査鎖の外部アンカーを公的時刻署名に限定する構成、超小電力デバイスでローテ周期を延長し SemOps の介入頻度を制御する構成がある。

【００７３】

ソフトウェア提供形態として、ライブラリ、カーネルモジュール、ゲートウェイアプライアンス、クラウドサービスを用意し、設定値とポリシーは署名付きプロファイルとして配布する。更新イベントは監査鎖へ記録する。

【００７４】

検証は、準拠試験（時間窓、再生、防御遷移）、ストレス試験（遅延と損失の注入）、意味整合試験（意図的なポリシー矛盾の挿入）、復旧試験（ゼロ化→再加入の時間測定）を含む。

【００７５】

以上のように、本実施形態は、通信、鍵運用、復旧、監査、意味整合を単一の状態遷移機械で統合し、適応型ＵＷＰと SemOps を核として有限閉包を維持する。図１から図１４までの各図は、実装の理解を補助する一例であり、各構成要素は当業者の知見により適宜置換可能である。

【実施例】

【００７６】
実施例（１）は、企業ＷＡＮにおけるＱＵＩＣトランスポートを用いた構成である。初回接続で policy_id と purpose と data_class と attestation_digest を交換し、ＰＵＦ応答とエフェメラル情報を入力としてＨＫＤＦで SK(t) を導出する。初期値は T_max＝〇〇〇ｍｓ、Delta_sync＝±〇〇〇ｍｓ、T_rot＝〇〇〇、epsilon＝〇〇〇とする。
【００７７】
本実施例では、各データパケットに単調ＣＴＲとパス識別子を付与し、ウィンドウ外番号と重複ＣＴＲを即時拒否する。往復遅延が T_max を超えたメッセージは適用保留とし、再同期フローに遷移させる。図１３の時間窓に従い、許容域外のイベントはゼロ化条件に加算される。
【００７８】
適応型ＵＷＰは、Xi(t) と tau(t) をネットワーク品質からプロファイル選択し、delta_hat_pos(t) を逐次推定する。delta_hat_pos(t) が閾値近傍に低下したとき、T_max と Delta_sync を段階的に縮小し、閾値未満で fail-close を発火する。
【００７９】
実装は、図１４の配備図に従い、端末にセキュア素子、ゲートウェイにＲＴＴ測定と順序検査、コアにＫＤＦ・監査・ポリシー配信を配置する。ゼロ化→再加入の連鎖はプロトコル規則として自動化される。
【００８０】
実施例（２）は、産業用フィールドバスにブリッジするエッジ-クラウド構成である。制御周期を８ｍｓとし、T_max を８ｍｓ、Delta_sync を±２ｍｓに設定する。ゲートウェイはフィールド側クロックとＩＰ側クロックの橋渡しを行い、時刻源の異常時は Delta_sync を厳格化して適用停止とする。
【００８１】
本実施例では、ゼロ化命令をＭＭＩＯ又はメッセージバスでデバイスへ即時伝搬する。ＣＴＲは安全カウンタで保持し、電源断後も単調性を維持する。セッション復旧はＰＵＦ再加入の後、意味タグとポリシーを再コミットして再開する。
【００８２】
実施例（３）は、委任と中継を含むマルチパーティ連携である。委任主体ごとに policy_id と data_class を分離管理し、沈黙・遅延・拒否は強制参加の規則で一義的に扱う。並列経路ではパス識別子とＣＴＲの組を一意性検査に用いる。
【００８３】
SemOps は、承認・留保・却下の人間イベントを異論度として取り込み、留保又は却下の発生時は対象フローをセーフホールドし、時間窓を縮小し、必要に応じゼロ化→再加入へ遷移させる。意味整合結果は監査鎖にコミットされる。
【００８４】
実施例（４）は、ＲＡＴＳ（リモート証明）を組み込んだ高保証構成である。attestation_digest をハンドシェイクに含め、失敗時は当該主体の鍵領域と一時状態を即時ゼロ化する。再加入は新たな測定値に基づく再証明とＰＵＦ検証を前提とする。
【００８５】

本実施例では、証跡と実運用の乖離が検知された場合、SemOps が意味的外乱として評価し、M_sem を減少させる。適応型ＵＷＰの閾値制御と合成し、dV/dt の負性を確保するようパラメータを安全側に更新する。

【００８６】

実施例（５）は、エネルギー系のマイクログリッドである。需要変動や島化制御のイベントを意味タグに含め、優先負荷の供給維持を E_sem に反映する。通信側は T_max をフェイルオーバー時に一時緩和し、復旧後に段階的に原状復帰する。

【００８７】

本実施例では、負荷変動で遅延とジッタが上昇した際、Xi(t) と tau(t) を調整して delta_hat_pos(t) を監視し、閾値近傍では鍵ローテを前倒し実行する。閾値未満では該当フローを fail-close とし、ゼロ化→再加入で再確立する。

【００８８】

実施例（６）は、遠隔保守の一時的特権を扱う。特権フローは purpose に「maintenance」を付し、時間限定トークンと短周期 T_rot を設定する。トークン期限切れ又は意味的外乱検知時は、特権フローのみセーフホールドし、他フローは継続させる。

【００８９】

本実施例では、旧鍵の併存時間 epsilon を１０ｓに短縮し、特権終了の確実性を高める。監査鎖は開始と終了のイベントを隣接コミットし、検証容易性を確保する。

【００９０】

実施例（７）は、低電力デバイス群である。ローテ周期 T_rot を長く設定しつつ、SemOps の介入頻度を抑制するプロファイルを用いる。電源断後のＣＴＲ単調性は安全カウンタの省電力モードで維持し、再加入時に一貫性を検査する。

【００９１】

本実施例では、監査鎖の外部アンカーを間欠的に行い、ネットワーク分断時はローカル鎖を保持する。再接続時にマージし、prev_hash の再計算で整合を確認する。

【００９２】

実施例（８）は、学内ネットワークのラボ環境での段階移行である。初期段階では T_max＝２００ｍｓ、Delta_sync＝±３０ｍｓとし、運用観測に応じて段階的に厳格化する。意味タグは最小スキーマから開始し、policy_id の整備と共に拡張する。

【００９３】

本実施例では、教育目的のため、図１３の時間窓と図１４の復旧連鎖を可視化ダッシュボードに投影する。delta_hat_pos(t) の推移、ゼロ化発生、再加入完了がリアルタイムに表示され、手順検証を容易にする。

【００９４】

実施例（９）は、クラウド間フェデレーションである。相互に {T_max, Delta_sync, T_rot, epsilon, Xi_profile, tau_range} を通告し、合意に失敗した場合は安全側デフォルトへフォールバックする。監査鎖は相互検証用にハッシュ要約を交換する。

【００９５】

本実施例では、並列経路に対する重複適用を回避するため、フロー識別子とＣＴＲをハッシュ化した一意キーを検査に用いる。意味的外乱が一方で発生した場合でも、当該フロー

のみセーフホールドし、全体停止を避ける。
【００９６】
実施例（１０）は、インシデント対応訓練である。攻撃シナリオとして、遅延注入、再生パケット、時刻改ざん、証跡不一致、内部異論を準備し、各イベントでの自動遷移を検証する。評価指標はゼロ化から再加入までの時間、誤拒否率、監査検証時間である。
【００９７】
本実施例では、dV/dt の推定ログを取得し、M_comm と M_sem の寄与を分離評価する。適応型ＵＷＰの閾値設定を変更し、誤検知と未検知のトレードオフを運用要件に合わせて最適化する。
【００９８】
以上の各実施例は相互に独立ではなく、当業者は用途と要件に応じてパラメータおよび構成要素を組み合わせることができる。図１から図１４は理解を補助する一例であり、同等機能を有する置換構成を排除しない。
【００９９】
図１の実施例では、端末とゲートウェイとコア鍵管理と時刻同期と監査鎖を一体化し、通信プレーンとセキュリティ核を同一構成で示す全体ブロックを実装する。
【０１００】
図２の実施例では、入出力から時刻同期と遅延測定と PUF 応答取得と KDF 導出とセッション鍵確立と意味タグ付与と監査コミットまでの処理パイプラインを連続動作させる。
【０１０１】
図３の実施例では、沈黙と遅延と拒否を強制参加の規則で一義に取り扱い、タイムアウト到達時にゼロ化へ遷移し再加入で復帰する分岐を運用する。
【０１０２】
図４の実施例では、初期化と認証中と稼働とローテ中とゼロ化と再加入の各状態を定め、T_max と Delta_sync と鍵年齢と nonce/CTR 整合で遷移させる状態機械を構成する。
【０１０３】
図５の実施例では、侵害兆候や時間窓違反や再生検知をトリガとして、鍵素材と一時領域とカウンタを即時消去し、PUF 再加入に自動連鎖させるゼロ化手順を具体化する。
【０１０４】
図６の実施例では、加入と鍵更新とゼロ化と意味整合結果の各イベントおよび RATS 測定値を前件ハッシュ（prev_hash）と併せて鎖状にコミットし、必要に応じ外部時刻署名へアンカーする監査およびアテステーション手順を実装する。
【０１０５】
図７の実施例では、ハンドシェイクからデータ送受信までの時系列上で RTT 測定と nonce/CTR 検査と再送条件と鍵ローテ挿入点と再同期条件を可視化し、運用に反映する。
【０１０６】
図８の実施例では、委任主体と中継主体と受益主体を分離し、最小権限で鍵配布を行い、沈黙と遅延と拒否を共通規則で扱うマルチパーティ通信経路を構成する。
【０１０７】
図９の実施例では、PUF 内蔵セキュア素子とデバイスドライバとカーネルモジュールとユ

ーザ空間ライブラリを対応付け、RTT 計測フックと再生検査と MMIO ゼロ化経路を低レイヤに実装する。

【０１０８】

図１０の実施例では、E_mech と E_sem を合成したエネルギー関数 V と、適応型有限閉包の指標 delta_hat_pos(t)を配置し、T_max と Delta_sync と T_rot と epsilon を安全側へ自動調整して安全単調性を保証する位置付けを示す。

【０１０９】

図１１の実施例では、接続時のポリシー交渉と伝達をハンドシェイクに組み込み、T_max・Delta_sync・T_rot・epsilon・Xi_profile・tau_range を相互通告して合意し、不一致時は安全側フォールバックを適用し、その結果を監査鎖にコミットする手順を示す。

【０１１０】

図１２の実施例では、加入と鍵更新とゼロ化と意味整合結果の各イベントに前件ハッシュを連結して鎖状に記録し、必要に応じ外部時刻署名へアンカーする軽量監査の構造と検証方法を示す。

【０１１１】

図１３の実施例では、RTT 境界と再生拒否と再同期条件の関係を時間窓上に可視化し、窓外イベントおよび重複 nonce を即時拒否し、境界接近時は許容窓を自動縮小する適応挙動を示す。

【０１１２】

図１４の実施例では、端末とゲートウェイとコア鍵管理と時刻同期監視と監査ログとゼロ化再加入の配置を定め、鍵ローテと侵害検知時のゼロ化から再加入への連鎖を運用フローとして配備する構成を示す。

【０１１３】

図１５の実施例では、遅延 RTT の実測曲線とジッタ包絡を時系列で可視化し、許容窓（RTT≦T_max、+/-Delta_sync 内）を基準に、閾値接近時は T_max と Delta_sync を自動縮小し、閾値を下回れない場合は fail-close へ遷移する適応挙動を示すとともに、下段で正性下界 delta_hat_pos(t)の推移を監視して窓縮小または遮断への分岐条件を明示する。

【０１１４】

図１６の実施例では、PUF 応答から HKDF（抽出/拡張）により SK(t)を導出し、鍵ローテ時に旧鍵と新鍵を併存時間 epsilon のみ重ね、epsilon 経過後は旧鍵を拒否する運用を時系列バーで示すとともに、加入/鍵更新/ゼロ化/意味整合の各イベントを監査鎖へ逐次コミットし、侵害兆候時にはゼロ化から再加入へ遷移する手順を示す。

【産業上の利用可能性】

【０１１５】

本発明は、通信プロトコル層とセキュリティ核を一体化し、適応型有限閉包（ＵＷＰ）と意味的外乱の検知再整合（ＳｅｍＯｐｓ）を組み合わせる構成により、ＩＴ系とＯＴ系の双方で適用可能である。既存のＴＣＰ/ＵＤＰ/ＱＵＩＣ、ＤＴＬＳ、ＩＰｓｅｃ等の標準スタックに重ねて導入でき、装置・方法・プログラムの形態で段階的に展開できる。

【０１１６】

エンタープライズネットワークにおいては、ゼロトラスト運用を通信一次制御量と統合す

ることで、再生攻撃の一義拒否、時間窓の厳格化、鍵ローテ連鎖の自動化が実現される。ＳＬＡ遵守と監査容易性が向上し、インシデント時の復旧時間が短縮される。

【０１１７】

産業用制御システム（ＦＡ、プロセス制御、スマートファクトリ）では、制御周期に合わせたＴ_max 設定と時刻同期管理により、安全側へ自動遷移する運用が可能となる。ネットワーク分断や電源断を伴う環境でも、ＣＴＲ単調性保持とローカル監査鎖のマージ機構により、再起動後の一貫性が担保される。

【０１１８】

電力・エネルギー分野（マイクログリッド、配電自動化、分散電源協調）では、負荷変動時の遅延・ジッタ増大に対し、ＵＷＰの適応で許容窓を自動調整し、必要時はフェイルクローズとゼロ化→再加入へ遷移することで系統安定度とサイバー復元性を両立できる。

【０１１９】

自動車・ロボティクス・医療機器等のサイバーフィジカル分野では、端末実体に対するＰＵＦバインドが有効に機能し、ソフト更新や遠隔保守の一時特権も短周期ローテと併存窓管理により安全に運用できる。意味タグとＳｅｍＯｐｓにより、用途限定や規制準拠の確認を通信面で強制できる。

【０１２０】

通信事業者・クラウド・ＣＤＮにおいては、フェデレーションや委任・中継を含む多者連携で、強制参加性と監査鎖の相互検証により、相互接続の責任分界を明確化できる。相互通告する｛Ｔ_max, DELTA_Ssync, Ｔ_rot, epsilon｝のプロファイル管理は運用自動化と親和性が高い。

【０１２１】

ポスト量子暗号への移行期においても、鍵ローテ連鎖と監査鎖が基盤となり、ＫＥＭ/署名方式の置換に対して上位の運用規則を維持できる。ＰＵＦ＋ＫＤＦの鍵導出は方式非依存であり、将来の暗号モジュール更新に追随しやすい。

【０１２２】

規制・監査要求（金融、医療、公共）に対しては、軽量ハッシュ鎖の逐次コミットと外部時刻署名アンカーにより、改ざん検出性と低遅延を両立した証跡を提供できる。ＳｅｍＯｐｓの異論検知は内部統制やデータガバナンスの実装に資する。

【０１２３】

導入コストは既存スタックとの親和性と段階移行性により抑制できる。主要な追加処理（遅延測定、再生検査、監査コミット、適応推定）は線形または定数時間であり、追加遅延は設計パラメータ範囲内で管理可能である。

【０１２４】

以上より、本発明は、企業ＩＴ、産業ＯＴ、エネルギー、輸送、医療、公共・防災、クラウドサービス等の広範な分野で有用であり、ゼロトラスト運用の実効性と復元性を高めつつ、標準プロトコルとの互換性を保持したまま社会実装できる。

【符号の説明】

【０１２５】

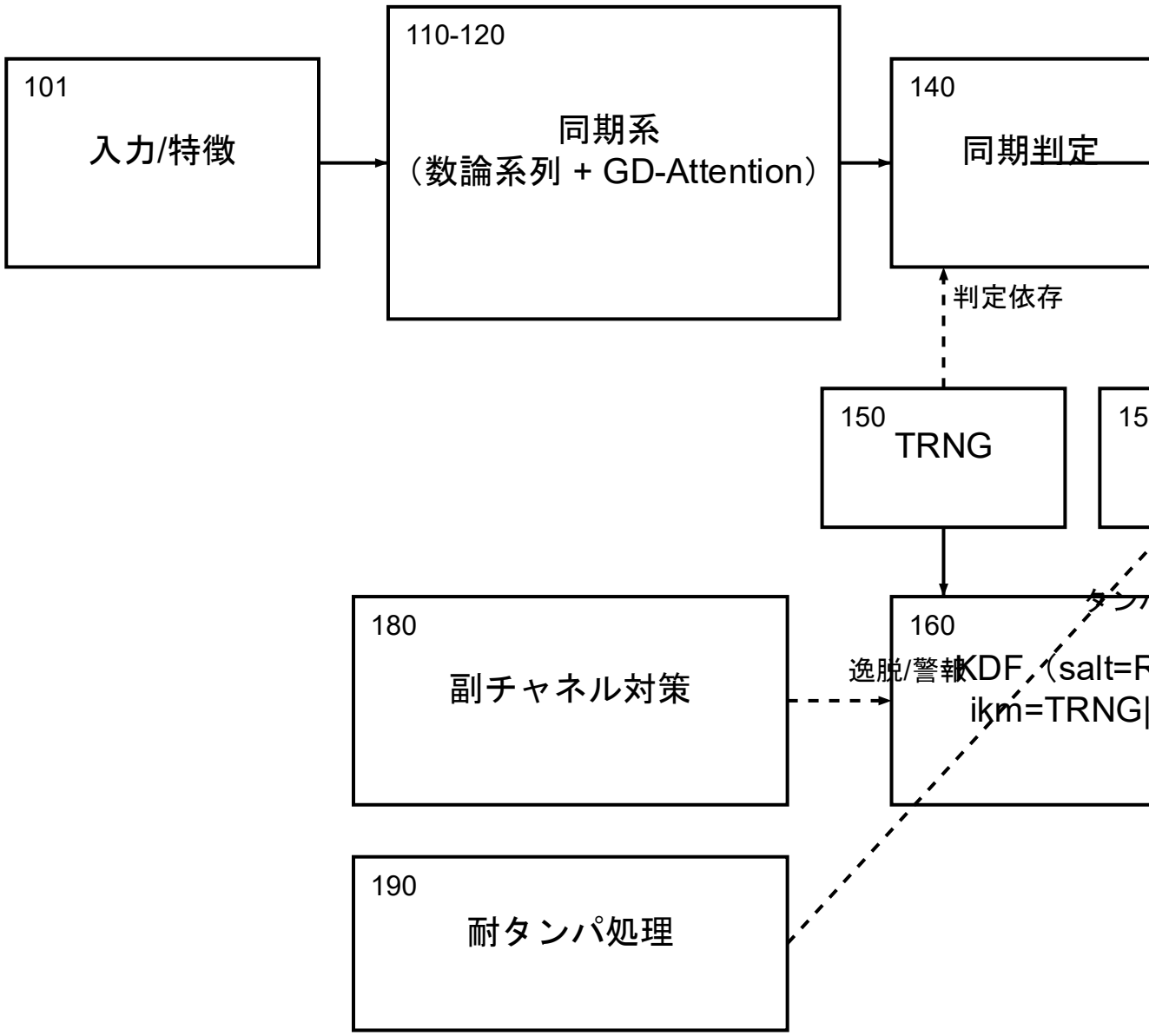
１００　端末装置

１０１　端末アプリケーション
１０２　セキュア素子（ＰＵＦ）
１０３　安全カウンタ（ＣＴＲ）
１０４　真性乱数源（ＲＮＧ）
１０５　時刻源（安全クロック）
２００　ゲートウェイ
２１０　認証中継部/ＱｏＳ制御部
２２０　ＲＴＴ測定部
２３０　順序検査部（ｎｏｎｃｅ/ＣＴＲ）
２４０　ＳｅｍＯｐｓエージェント（意味整合監視）
３００　コア鍵管理装置
３１０　ＫＤＦエンジン
３１１　ＨＫＤＦ抽出部（Ｅｘｔｒａｃｔ）
３１２　ＨＫＤＦ拡張部（Ｅｘｐａｎｄ）
３２０　鍵ローテ管理部
３２１　セッション鍵管理部（ＳＫ運用）
３３０　監査ハッシュ鎖記録部
３４０　ポリシー交渉/伝達部
３４１　プロファイル管理部（Ｔ_max/DELTA_Ssync/Ｔ_rot/epsilon）
３５０　ＲＡＴＳ検証部
４００　時刻同期/監視部
４１０　DELTA_Ssync 管理部
４２０　Ｔ_max 管理部
４２１　ジッタ監視部
４２２　ＲＴＴ包絡推定部
４３０　再生検知部（重複ｎｏｎｃｅ/逆順ＣＴＲ）
４４０　意味整合度算出部
４５０　意味タグ格納部（policy_id/purpose/data_class）
４６１　許容窓バンド表示（ＲＴＴ≦Ｔ_max, ±DELTA_Ssync）
４６２　閾値線表示
４６３　ｆａｉｌ−ｃｌｏｓｅ遷移トリガ
４６４　適応制御指令（Ｔ_max/DELTA_Ssync 縮小）
５００　ゼロ化/再加入部
５１０　ゼロ化トリガ
５２０　ＰＵＦ再加入手続
５３０　再同期手続
６００　プロトコル時系列表示部
６１０　ハンドシェイク処理
６２０　データ送受信処理
６３０　鍵ローテ処理

６４０　再送制御
６５０　再同期制御
６６１　ローテ併存区間表示（epsilon）
６６２　旧鍵禁止区間表示
６７１　監査コミットイベント列
７００　多者連携構成
７１０　委任主体
７２０　中継主体
７３０　受益主体
７４０　鍵配布サービス
８００　ＯＳ/半導体層
８１０　デバイスドライバ
８２０　カーネルモジュール
８３０　ＢＵＳ/インタコネクト
８４０　ＭＭＩＯゼロ化経路
９００　安全エネルギー指標群
９１０　Ｅ_mech（機械的整合エネルギー）
９２０　Ｅ_sem（意味的整合エネルギー）
９３０　Ｖ（合成エネルギー関数）
９４０　正性下界モニタ（delta_hat_pos 監視）
９５１　正性下界閾値表示
Ａ１　通信プレーン
Ａ２　セキュリティ核
Ａ３　監査ログストレージ
Ａ４　時刻署名アンカー
Ｔ_max　往復遅延上限
DELTA_Ssync　時刻同期許容幅
Ｔ_rot　鍵ローテ周期
epsilon　旧鍵併存時間
Ｘｉ（t）　帯域パラメータ（ＵＷＰ適応）
tau(t)　平滑パラメータ（ＵＷＰ適応）
lambda　重み係数（Ｅ_mech/Ｅ_sem 結合）
delta_hat_pos（t）　正性下界推定値
ＳＫ（t）　セッション鍵
ｎｏｎｃｅ　一意乱数
ＣＴＲ　カウンタ
ＰＲＫ　ＨＫＤＦ抽出鍵
ＯＫＭ　ＨＫＤＦ出力鍵素材
ｃｌｏｃｋ＿ｓｋｅｗ　端点間時刻差
ａｔｔｅｓｔａｔｉｏｎ＿ｄｉｇｅｓｔ　測定要約（ＲＡＴＳ）

ｐｏｌｉｃｙ＿ｉｄ　ポリシー識別子
ｐｕｒｐｏｓｅ　目的分類
ｄａｔａ＿ｃｌａｓｓ　データ区分
【書類名】要約書
通信プレーンとセキュリティ核を一体制御し、RTT<=T_max および|clock_skew|<=Delta_sync の時間窓と nonce/CTR の一意・単調性により再生・逆順を拒否する装置等を提供する。同期成立時のみ KDF を開放し、TRNG と PUF 材料から SK を導出。侵害兆候・窓違反・再生検知時は即時ゼロ化し PUF 再加入へ遷移する。UWP(adaptive finite closure)で delta_hat_pos(t)を監視し{T_max,Delta_sync,T_rot,epsilon}を自動更新、閾値未満は fail-close。SemOps で policy/実態の不整合を検知してフローを再整合。監査ハッシュ鎖に加入・更新・ゼロ化・承認を記録する。
【選択図】図１
【書類名】　　図面
【図１】

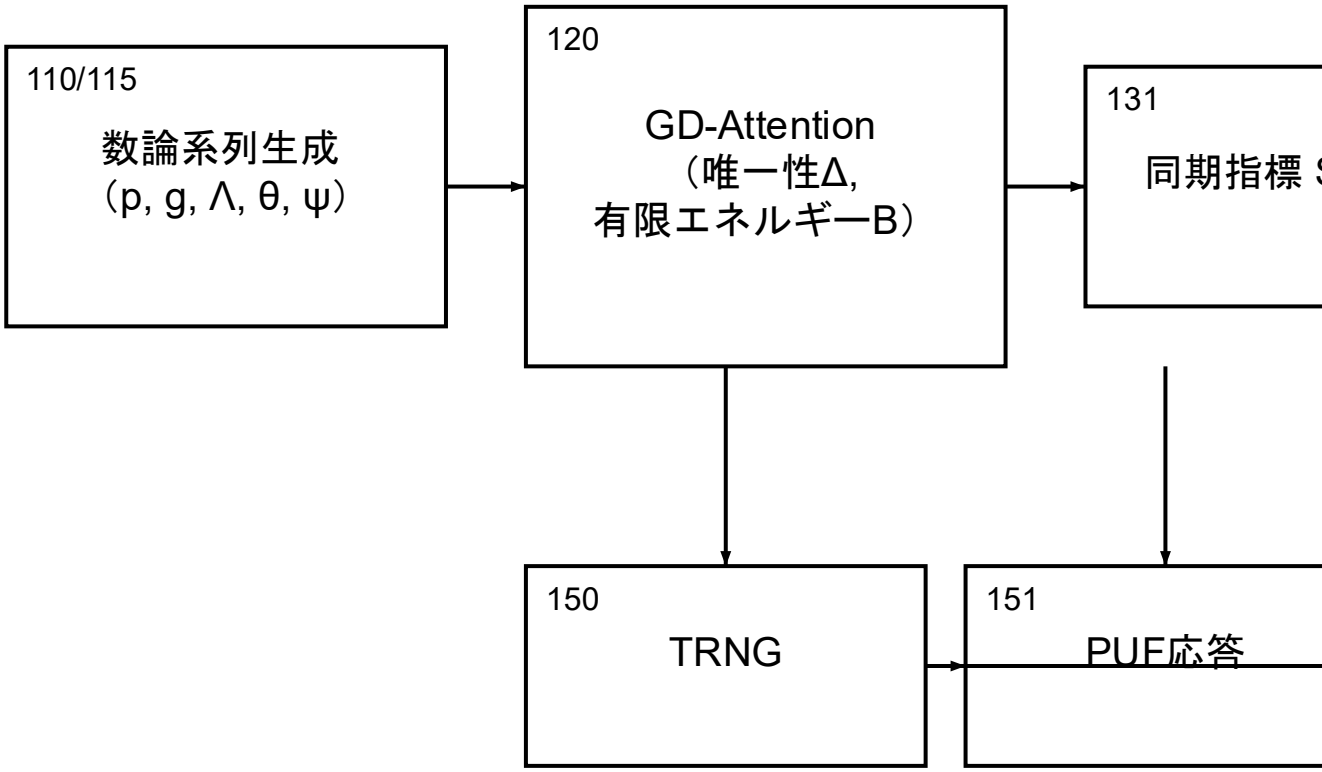
図1 システム全体構成（外部合意層なし：信頼の内在化）



注：二重線＝鍵/鍵素材の流れ、破線＝制御/監査/ポリシ

【図２】

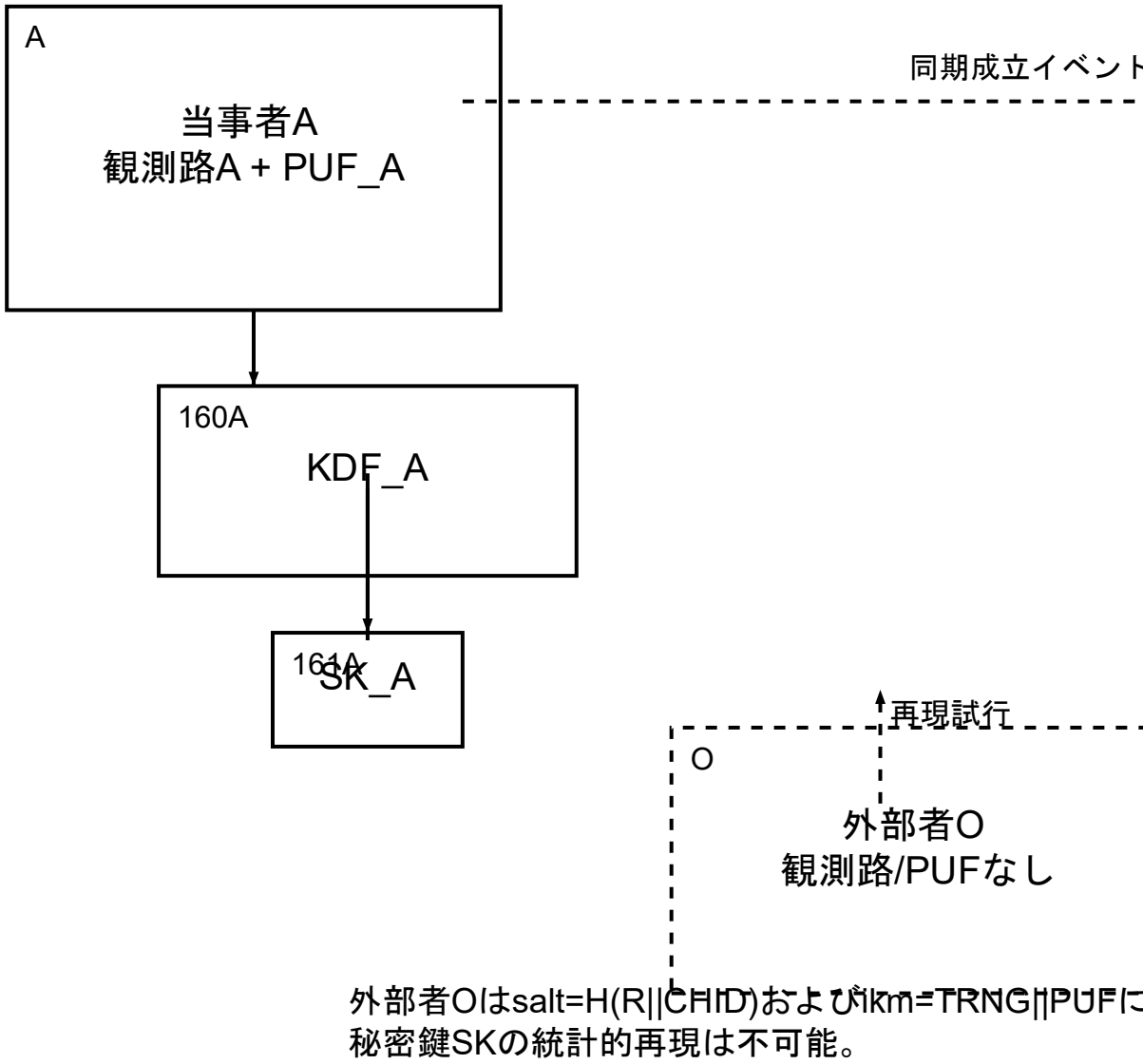
図2 意味同期→当事者バインド→鍵導出パイプライン



Δ＝一意性マージン、B＝有限エネルギー上限。
当事者バインド：salt=R||CHID、ikm=TRNG||PUF（外部合意不要）。

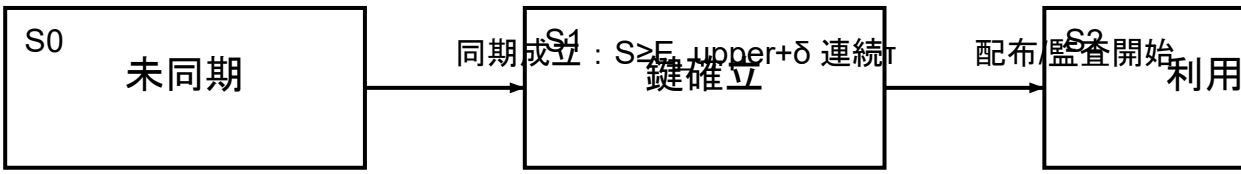
【図３】

図3 強制参加性の原理（外部者の再現不能）



【図４】

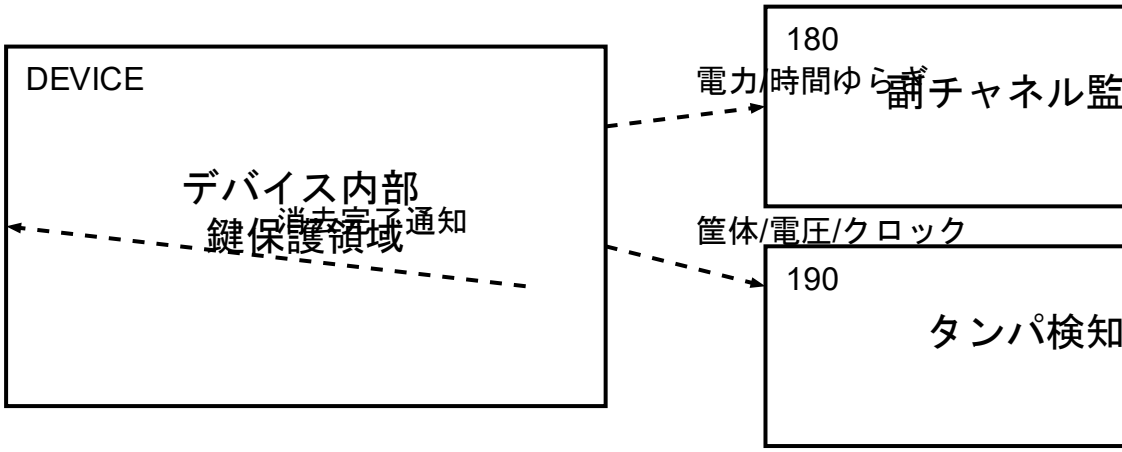
図4 セキュリティ状態機械（未同期→確立→利用→失効→即時消



逆遷移不可（時間単調）。

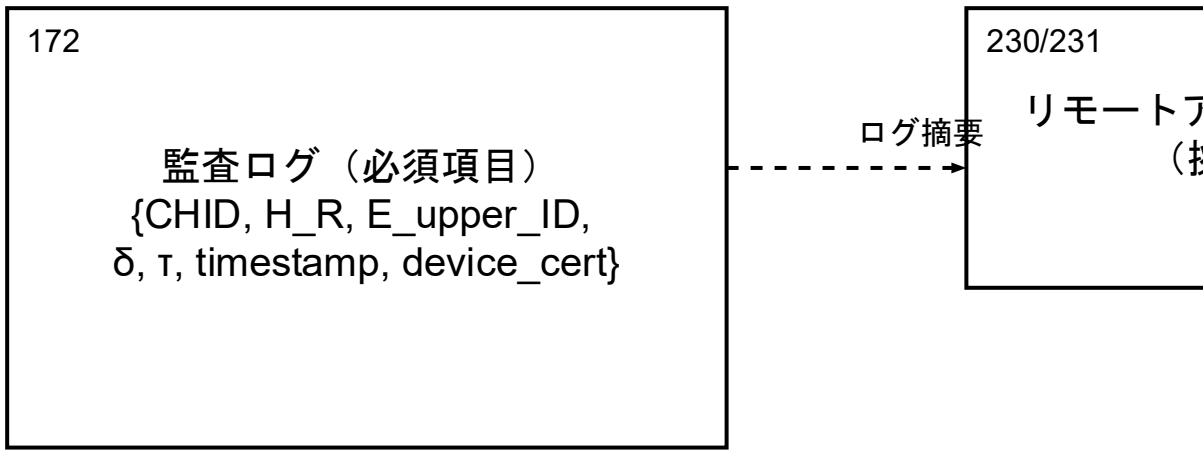
【図５】

図5 逸脱・タンパ検知とゼロ化経路



【図６】

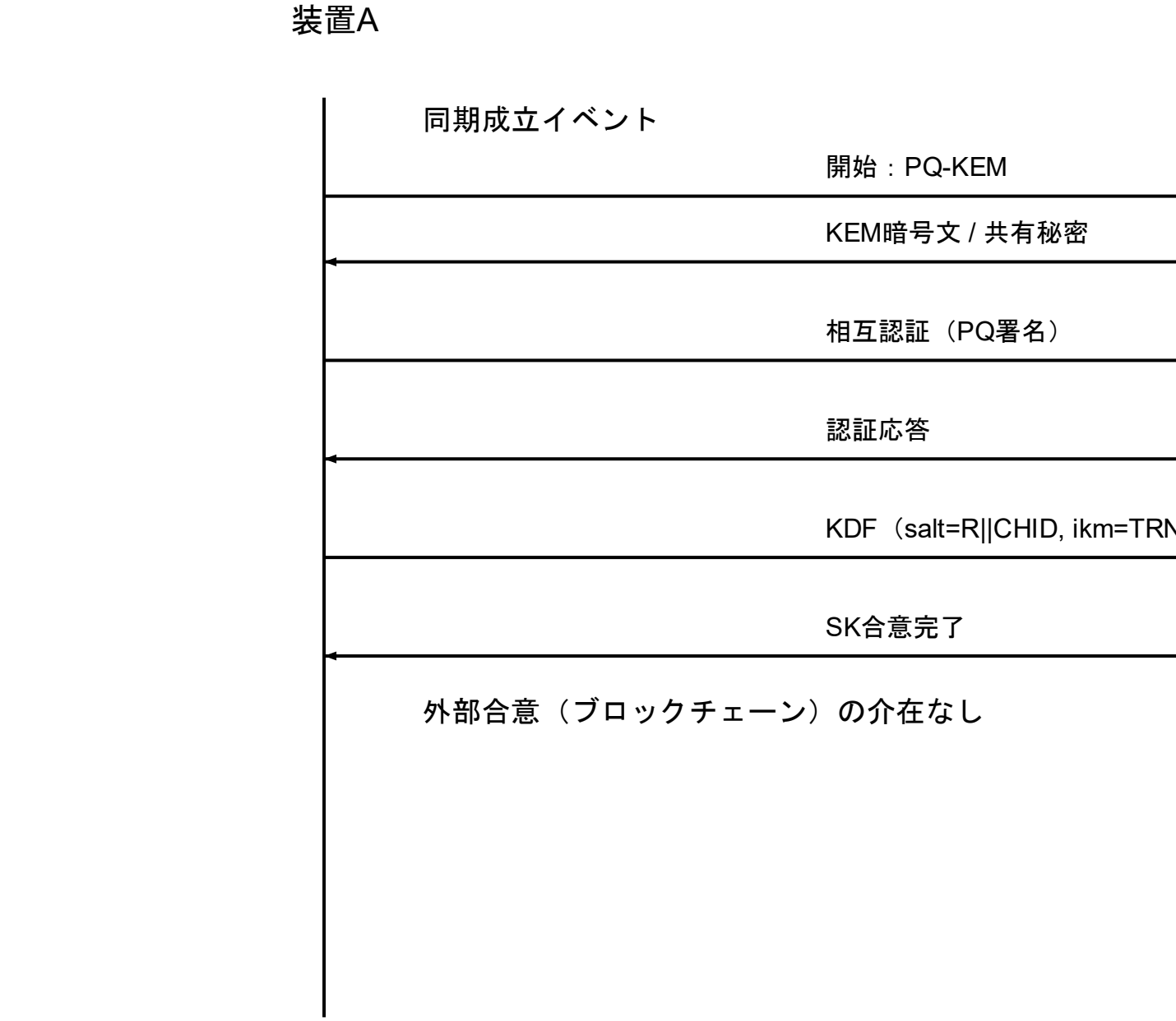
図6 監査ログと当事者性証明（リモートアテステーション）



外部合意層（ブロックチェーン）不要：
当事者性はログ＋ゼロ化一貫性で証明可能。

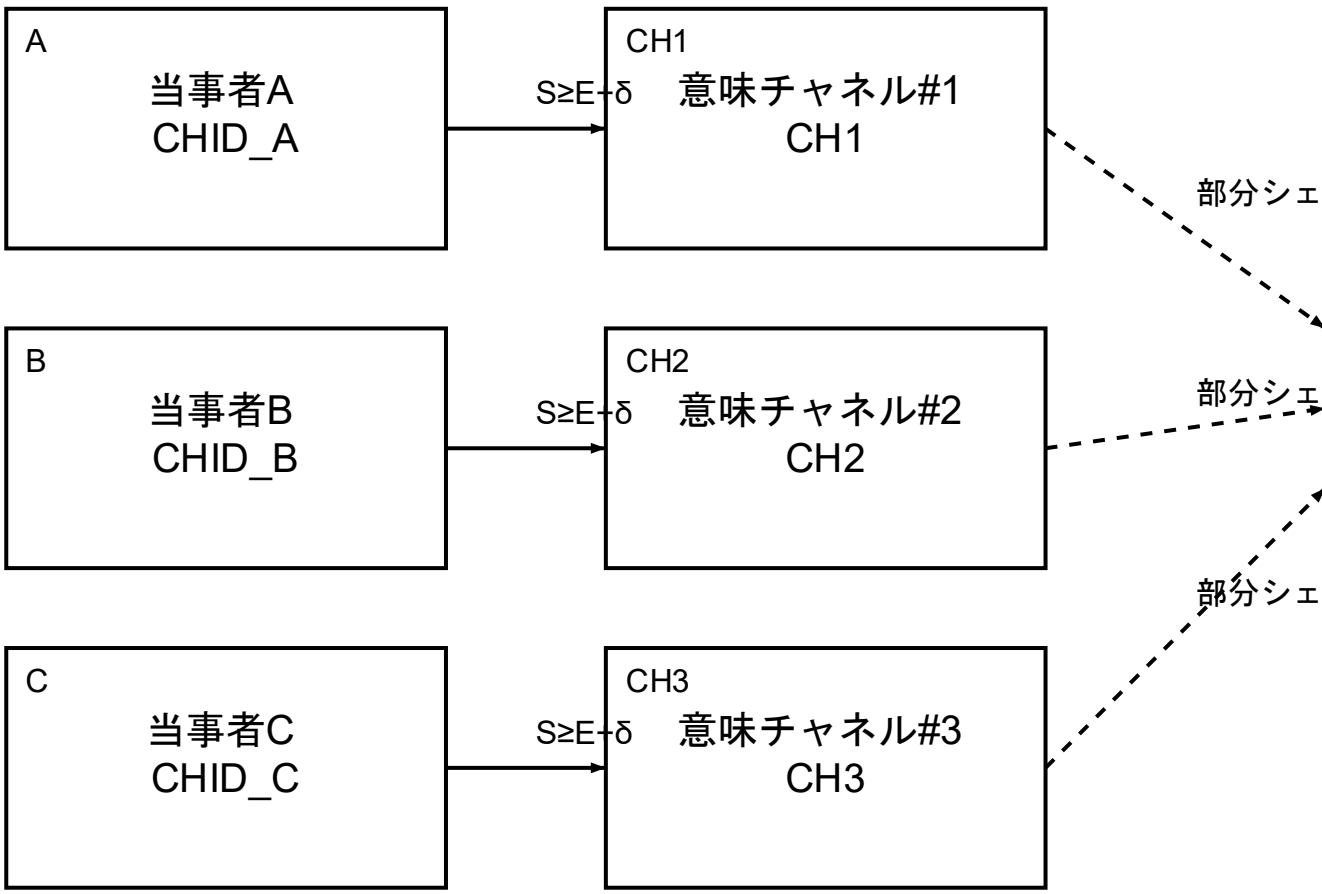
【図７】

図7 プロトコル時系列（同期成立→PQ-KEM/署名、ブロックチェ



【図８】

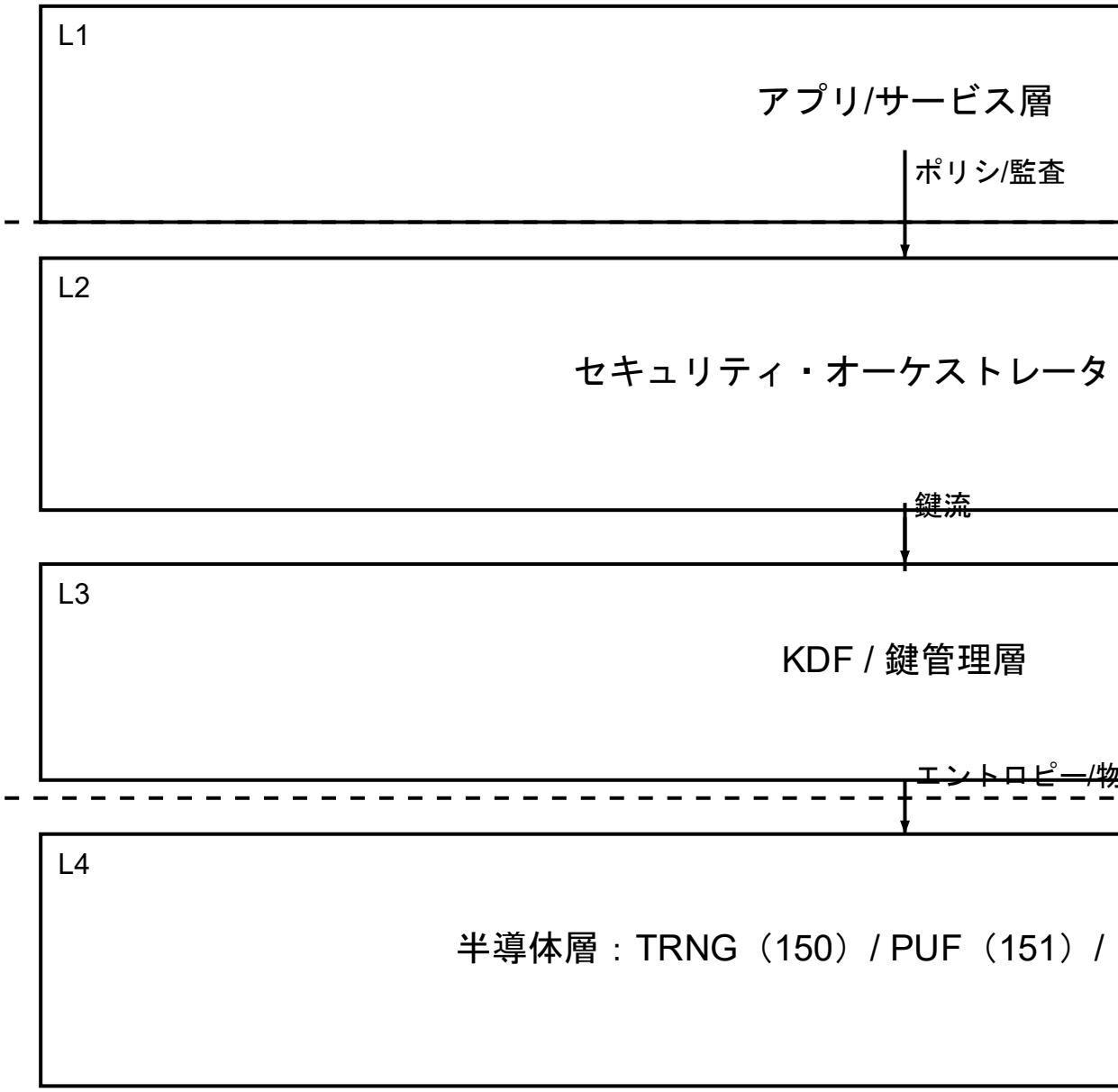
図8 多当事者チャネルの調停（意味チャネル別の鍵分離／しきい



注：（t,n）でチャネルごとに鍵を復元。各チャネルはsaltにCHIDを含み鍵が分離。

【図９】

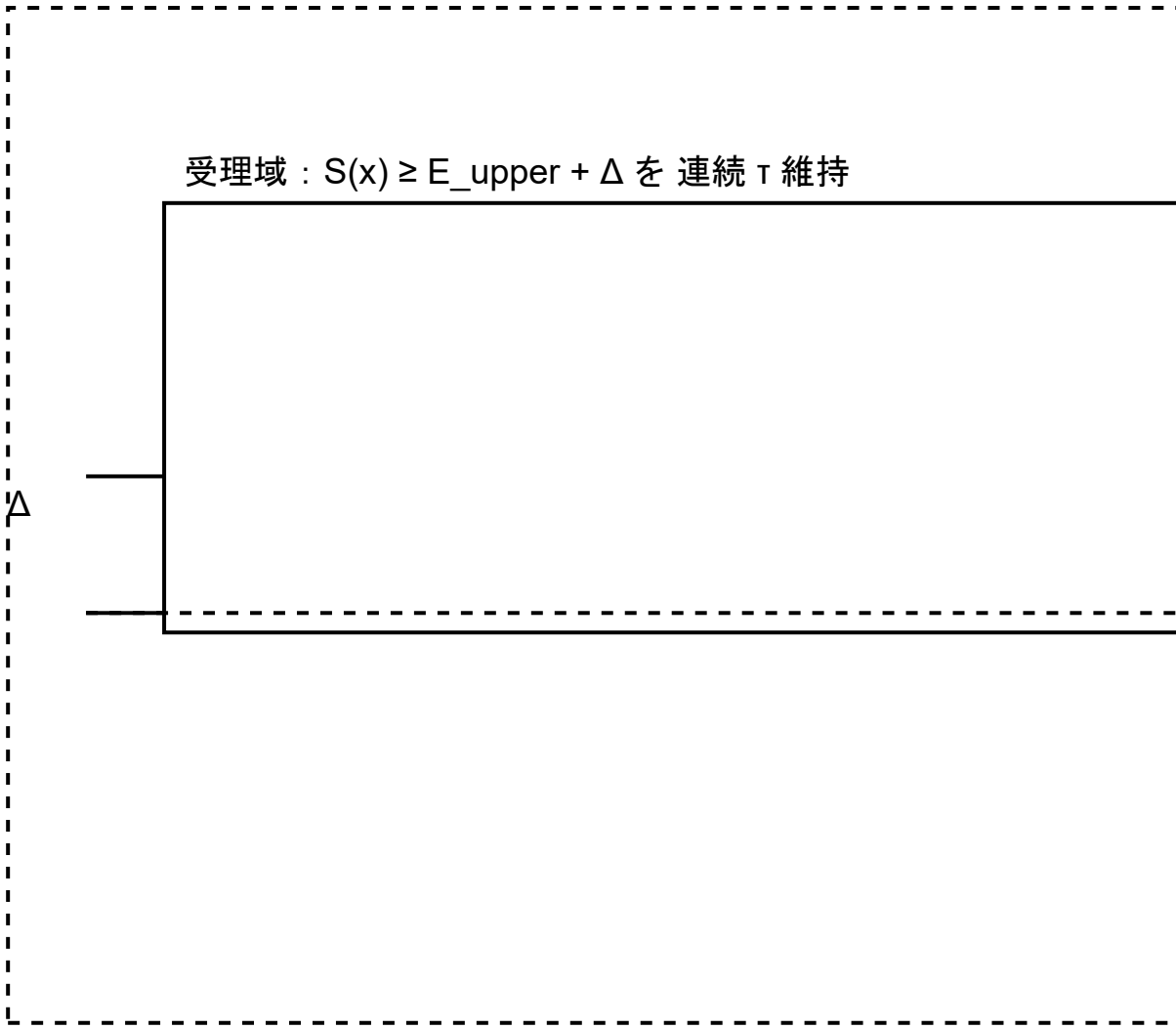
図9 OS境界と半導体境界のレイヤ統合（PUF/TRNG→KDF→SC



注：信頼はブロックチェーンに外出せず、層内で完結（内在化）。

【図１０】

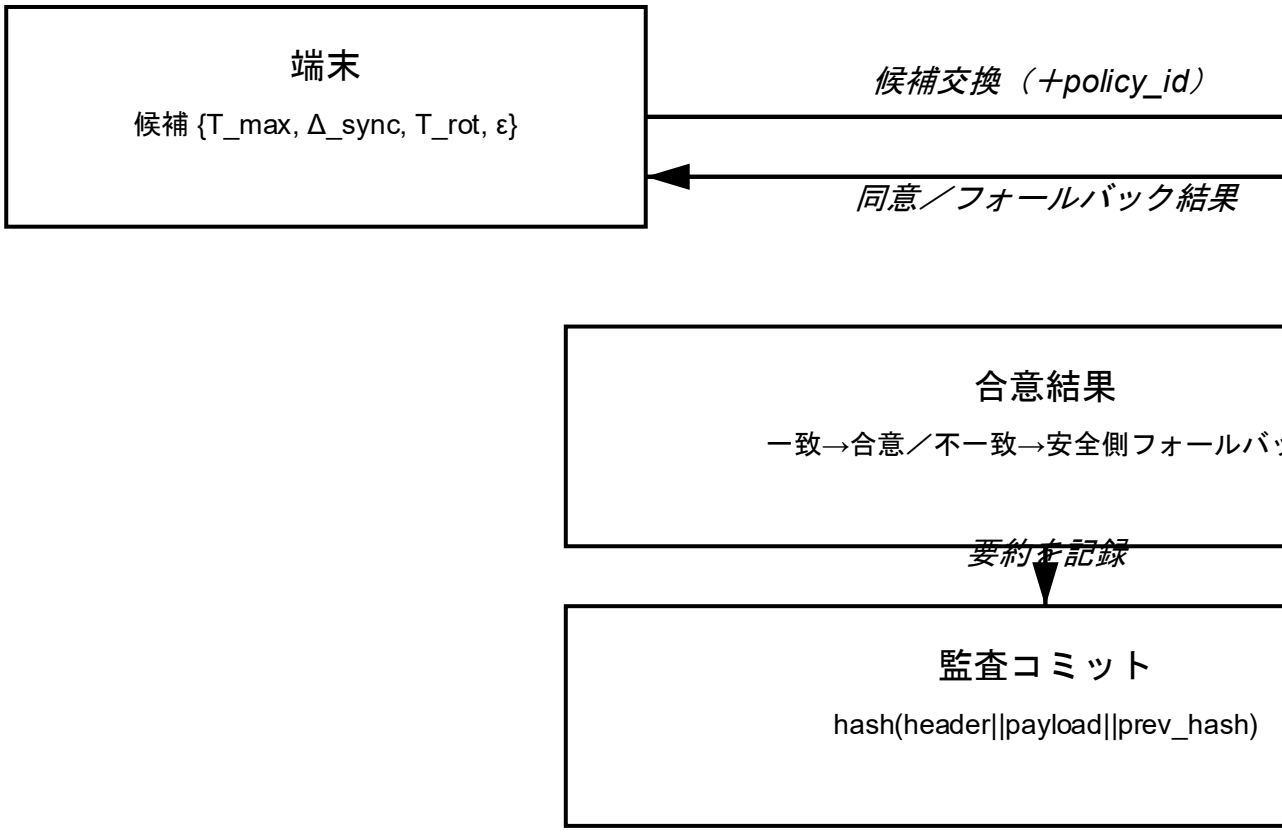
図10 有限エネルギー制約Bと一意性マージンΔ（受理域）



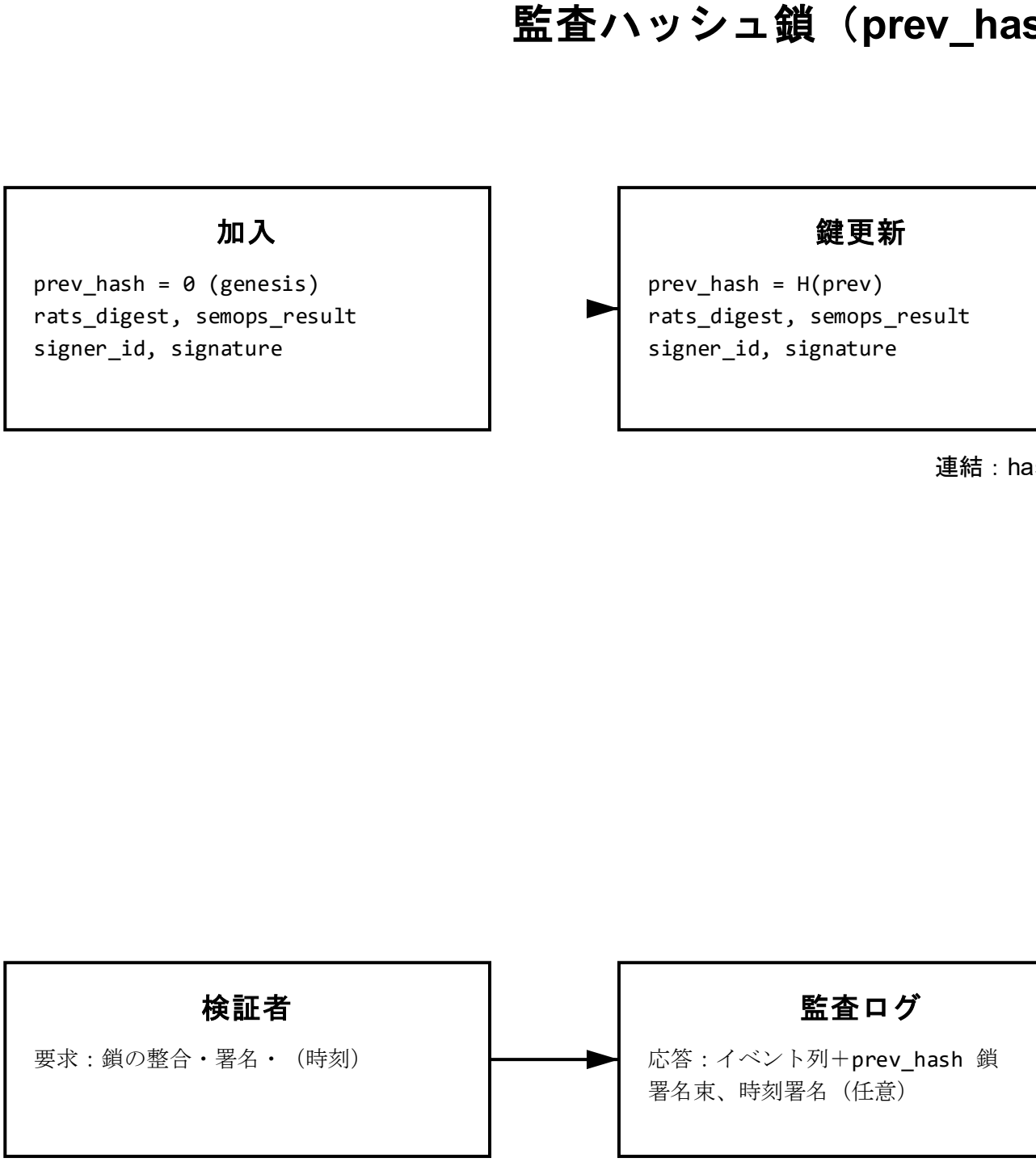
注：Bでスコアの暴走を抑制、Δで一意性を確保。ブロックチェーン的合意は不要。

【図１１】

ポリシー交渉（相互通告／フォールバ



【図１２】


監査ハッシュ鎖（prev_has
加入
prev_hash = 0 (genesis)
rats_digest, semops_result
signer_id, signature
鍵更新
prev_hash = H(prev)
rats_digest, semops_result
signer_id, signature
連結：ha
検証者
要求：鎖の整合・署名・（時刻）
監査ログ
応答：イベント列＋prev_hash 鎖
署名束、時刻署名（任意）

【図１３】

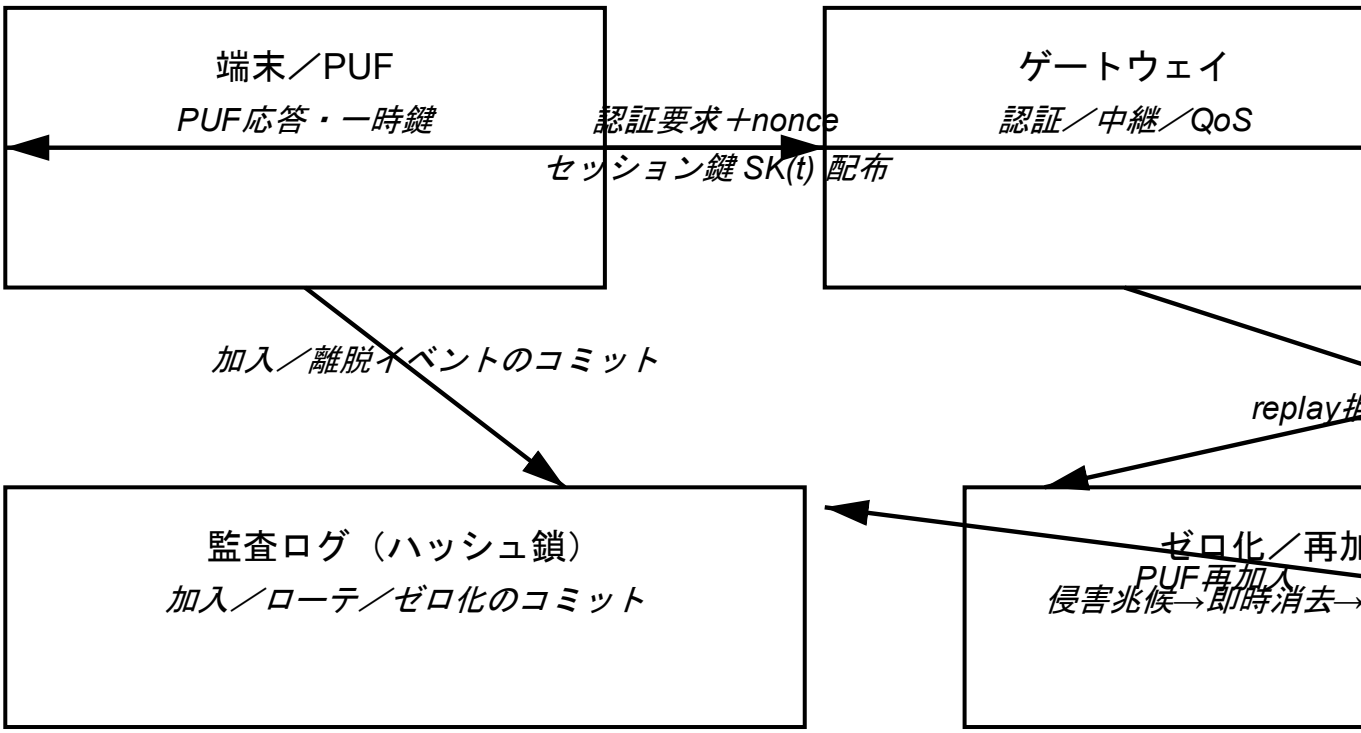
攻撃面 × 防御層 マップ

	リプレイ	副チャネル	合意型
PUFバインド(151)	◎	◎	◎
TRNG(150)	◎	◎	◎
状態機械/ポリシ(173)	◎	◎	◎
即時消去(192)	◎	◎	◎

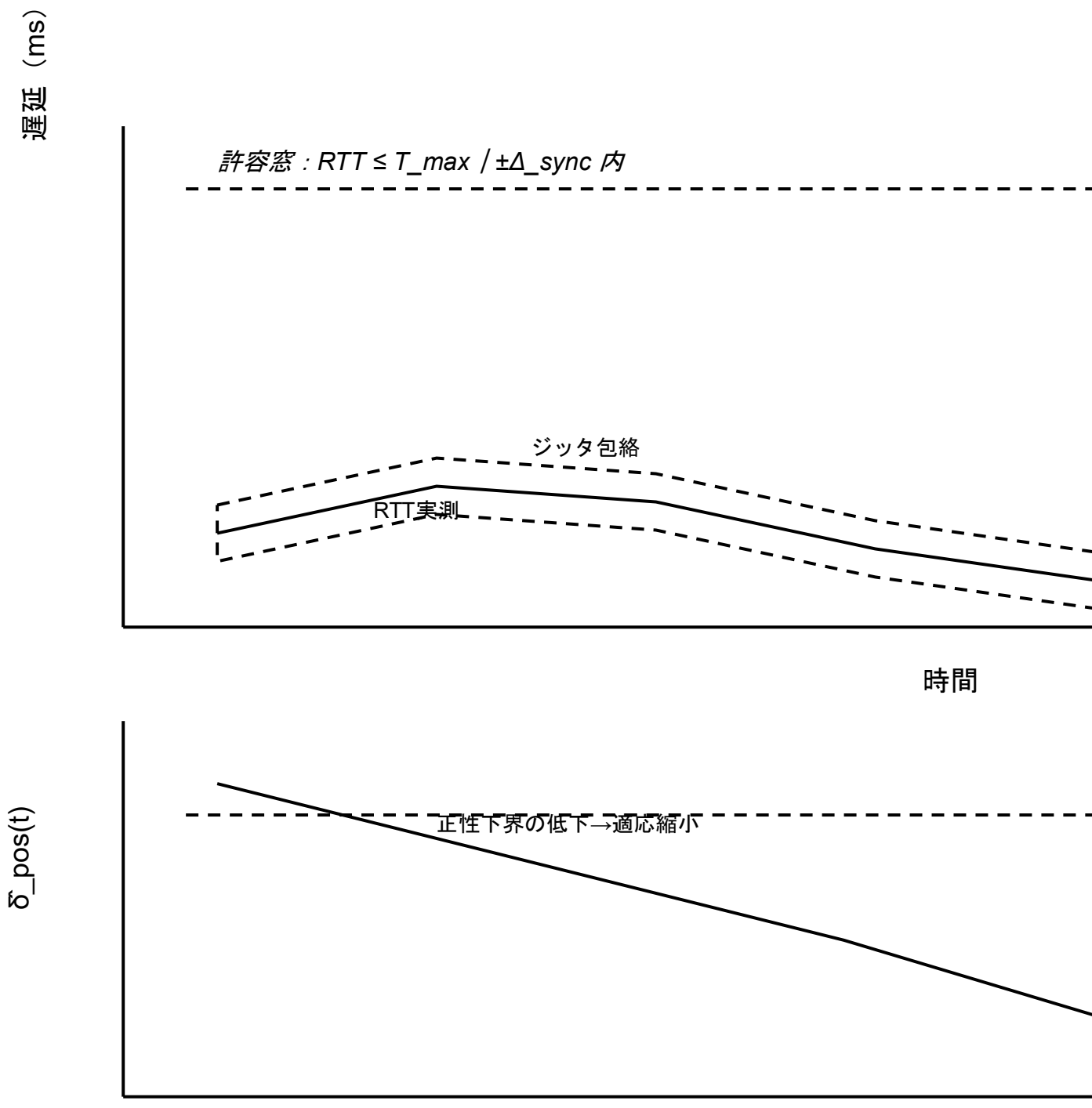
凡例：◎=設計により無効化/強力緩和。具体例→ PUF:当事者再現不能、TRNG:一度限り、状態機械

【図１４】

ゼロトラスト配備（鍵ローテ／ゼロ化

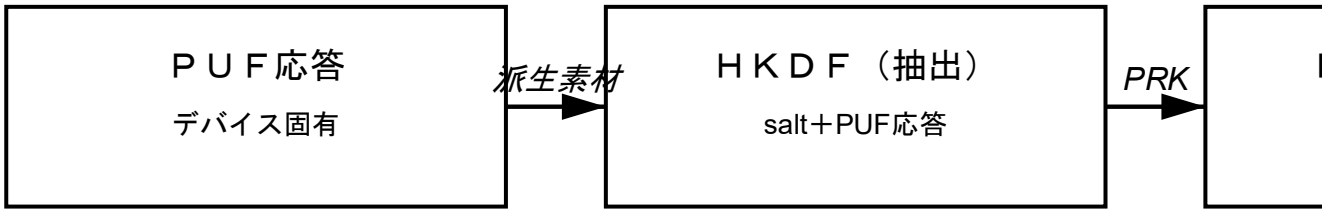


【図１５】


遅延・ジッタ包絡と適応縮小（U
遅延（ms）
許容窓：RTT ≤ T_max ／±Δ_sync 内
ジッタ包絡
RTT実測
時間
δ_pos(t)
正性下界の低下→適応縮小

【図１６】

鍵導出とローテ重なり ε の時



ε 経過後：旧鍵使用禁止

時系列

ＳＫ（t）有効期間

併存 ε

注意：旧鍵は ε 内のみ受容、窓外は拒否
置換容易性：暗号方式変更時も HKDF 入替で運用維持

監査コミット

加入 ／ 鍵更新 ／ ゼロ化 ／ 意味整合 を順次