IEA ／ Solution Brief
Immutable Evidence Architecture

TriStruct

特許第 7892230 号　特願 2026-8383・175106

EDR・SIEM の検知範囲を「行・列・値」単位へ拡充する。
データの変化を証明し、汚染イベントを除去した安全な状態へ戻す。
SOC のための「データ証明・侵害除去レイヤー」

導入効果

IEA は特許第 7892230 号に記載の不可分な確定処理によるデータ真正性証明方式です。
全てのイベントによる変更を原本として固定することで、以下のような効果を生みます。

侵害範囲検出 ／ 解析範囲限定

IEA は固定時刻順にイベントを記録するため、異常が検知された時間帯のデータ変化を行単位で提示可能です。

汚染イベント除外復旧

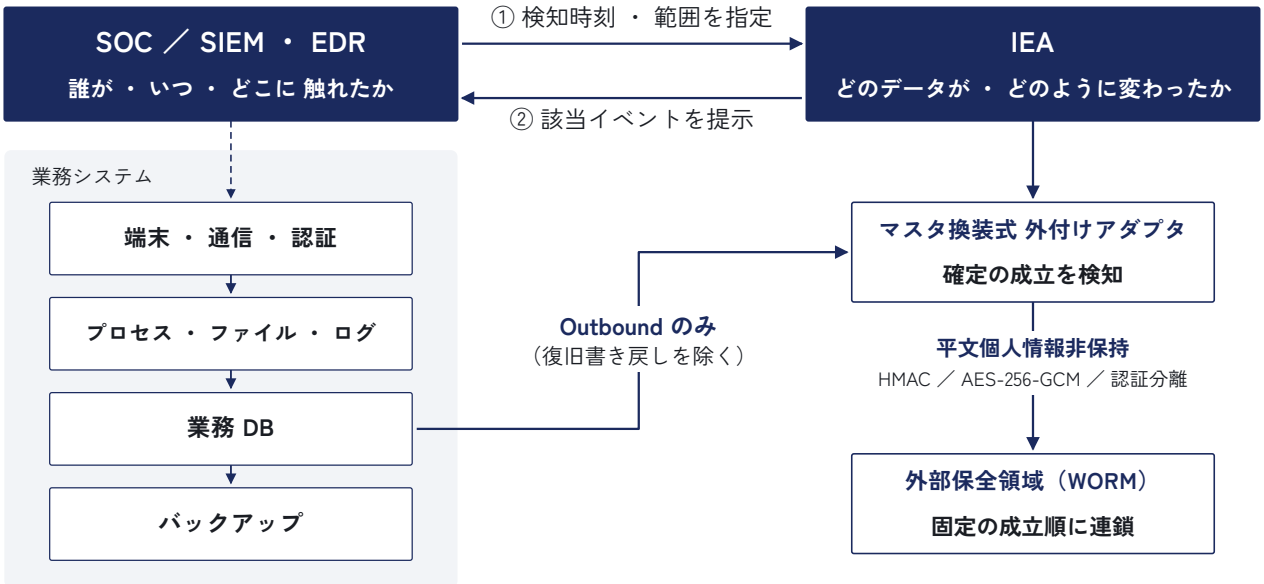
行単位の証明データを個別に除外する形式での復旧（再構築）が可能です。汚染によりバックアップ適用が困難な区間を IEA が補います。

マスタ換装アダプタ方式

IEA の導入はシステム改修を必要としません。復旧時の書き戻しを目的に、導入先システムのデータマスタを換装するだけで殆どの調整が完了します。

接続と構成

データ原本と固定時の監査証跡を、ランサムウェアの影響を受けない範囲へ転送します。
システム改修不要のアダプタ形式・Outbound のみ・PostgreSQL／MySQL 対応確認済



特許第 7892230 号　図1 の構成に対応
WebORCA ・ 大手グループウェア 2 社の稼働環境で動作確認済み

IEA は、値の正・不正を問わず各検知時点の原本を固定・保持します。

実機でのデモを承ります。　partner@tristruct.co.jp ／ 技術詳細の開示は NDA 締結後となります

TriStruct

特許第 7892230 号　特願 2026-8383 ・ 175106

実機実証

自社の受入試験（破壊／改ざん検知／復旧／耐障害／同一性・約 50 本）を、継続的に検証しています。
以下は約 1,498 原本のグループウェア環境における実測値です。負荷試験は 1 万件、添付 500 件で実施しています。

環境ごと失われた後の再構築	**55.3 秒**　空の新規 DB に原本だけを流し込み、元の全表・全行・全列と一致する状態まで戻します。
削除された記録の復旧	**99.8 秒**　実際に消去した状態から、原本だけで元どおりに復元します。
改ざん・削除の検知	**62.8 秒**　書き換えられた値も、消された行も、原本との照合で洗い出します。
真正性の検算	**0.16 秒**　596 記録・1,498 件を検算し、内容の改ざんと並びの破壊を検出します。第三者が同じ式で再計算できます。
汚染を除外した復旧	侵害と判断されたイベントだけを外し、親子関係と外部キーの整合を保ったまま最新まで組み直します。

権限設計

平常時	読み取り専用の権限だけで動作します。**IEA は業務データへ書き込む権限を持ちません。**
復旧時	書き込みは復旧時に限り、別の資格で行います。自動で書き戻すことはなく、明示的な操作を経て実行されます。
外部保全領域	対象 DB から物理的または論理的に分離し、追記だけを許して上書きと削除を受け付けない領域に保存します。暗号化したうえで、鍵は分離して管理します。

可用性と非干渉

IEA 停止の可視化	更新の有無に関わらず、ハートビートを一定間隔で記録します。**停止区間と無更新区間を区別できます。**
取得の自動再開	監視プロセスが停止した取得を再開します。ストリーミングが張れない場合はポーリングへ退避します。
未取得区間の明示	取得できなかった区間は、裏付けを欠く区間として記録します。推測で補うことはしません。
業務 DB への影響回避	取得失敗が続いても WAL を滞留させません。しきい値超過時は外部へ発報します。復旧は取得を停止してから行い、ロックが取得できない場合は待たずに中止します。

記載の数値は上記の規模における実測であり、大規模環境では改めて計測を要します。外部保全領域の隔離の強さは配置構成によって決まります。強い隔離を要する場合は、別ホストと外部の不変ストレージを用いる構成とします。滞留を検知した際の退避操作は、運用側の判断によります。集計値のように他の値から導かれる列は復旧の対象から除外でき、復旧後に業務システム側で再集計します。

実機でのデモを承ります。　partner@tristruct.co.jp　／　技術詳細の開示は NDA 締結後となります