——『緊急通報・バイタルセキュリティ・知財照合システムの統合的権利構造（完全封鎖版）』——

（全 204 ページ）

---

1. 発表の背景と概要

2025 年 8 月 25 日、共同著作者 4 名（竹内祐樹・竹内健一・平川智子・平川和典）によって創作された**『緊急通報・バイタルセキュリティ・知財照合システムの統合的権利構造（完全封鎖版）』**は、**現代社会における安全・権利・経済循環を守る新たな社会的インフラの原典です。本著作物は翌 26 日および 27 日に公証役場で存在事実証明が確定され、28 日に正式に公正証書が取得されました。これにより国内外で通用する**改ざん不能の証拠力**が付与されました。

本著作物は **全 18 ページの目次、1,701 ページの本体、262 ページの解説書**から構成され、さらに **3 件の特許出願**（緊急通報システム、バイタルセキュリティシステム、知財照合・収益分配システム）と連動しています。

今回のリリースでは、①著作権としての権利範囲、②権利期間、③侵害について、④先使用権の位置づけを含め、本著作物の社会的・法的意義を明確にお伝えします。

---

2. 著作権としての権利範囲（①）

包括的保護の原則

本著作物は「**結論一致＝侵害成立**」という定義を明文化しています（p.3〜4）。つまり、アルゴリズム・UI・API・データ構造・言語・記号・表現のいずれにおいても、**最終的に同一の結論を導く構成であれば、表現や手段の差異を問わず侵害**と認められます。

具体的には：

- **アルゴリズム**：音響解析・発話解析・位置照合（第 1 章, p.25〜297）
- **UI/UX**：緊急通報アプリ、ダッシュボード、裏通報モード（第 1 章, p.110〜133）
- **データ形式**：通報ログ CSV、証拠保存ハッシュ構造（p.186〜200）
- **契約・収益分配ロジック**：compare → block → contract → revenue（第 3 章, p.553〜938）
- **複合システム**：三重セーフティ網（第 4 章, p.939〜1216）
- **禁止行為**：模倣・均等・類似・派生・転写・言い換え（第 5〜7 章, p.1219〜1479）

さらに、**1 行一致でも侵害成立**（p.73〜77）という強度を備え、UI ボタン一つ・関数一つ・記号一つでも一致すれば著作権侵害が認められる仕組みです。

---

3. 著作権としての権利期間（②）

著作権の保護期間は、国際的な標準（ベルヌ条約・日本著作権法第 51 条）に基づき、**著作者の死後 70 年まで**存続します。本著作物は共同著作物であるため、**最終の存命著作者が亡くなった年の翌年から 70 年間**が保護対象期間です。

つまり本作は、単なる一時的保護にとどまらず、**22 世紀初頭まで権利が確実に存続する知的基盤**となります。さらに、公証役場の公正証書によって証拠力が担保されているため、後年に至っても改ざん・否認の余地がなく、権利継承者による利用・ライセンス・訴訟が可能です。

---

4. 著作権侵害について（③）

本著作物の構造は「逃げ道の封鎖」に特化しており、以下の行為は全て侵害に該当します。

1. **模倣**：同一アルゴリズムや UI のコピー
2. **均等**：手段を置き換えても同じ結果を導く場合（FFT→Wavelet でも侵害成立）
3. **類似**：色・表記・記号を変えても結論が一致する場合
4. **派生**：翻案・改変・教育目的での利用も禁止
5. **転写・書き込み**：ホワイトボードやスクリーンショットによる模倣も侵害対象
6. **逆順・工程入替**：通報→保存を保存→通報に変えても侵害成立
7. **1 行一致**：ソースコード 1 行、UI アイコン 1 つの一致で侵害成立

実例ページ

- p.30：権利範囲（音響＋発話＋位置の統合アルゴリズム）
- p.73〜77：1 行一致・均等・類似・派生の禁止規定
- p.1219〜1270：模倣・均等・類似・派生封鎖の法的枠組み
- p.1431〜1479：「触れた瞬間に侵害成立」の最終宣言

これらにより、**「模倣も翻案も一切許さない世界初の完全封鎖著作物」**としての強度が確立されています。

---

5. 先使用権の説明（④）

知的財産法における「先使用権」とは、ある著作物・発明・商標が登録される以前から独自に使用していた者が、その範囲に限って継続利用できる権利を指します。

ただし本著作物については、

- 公証役場による存在証明（2025 年 8 月 26 日・27 日）
- 公正証書取得（2025 年 8 月 28 日）
- 同時期の特許出願 3 件

によって、**最も早期かつ公式に存在確定**しているため、他者が「先に使用していた」と主張する余地は極めて限定的です。

さらに、著作権の保護対象は「表現」ではなく「構成的一致」に置かれており（p.3〜4）、表現を変えたとしても結論一致で侵害成立とみなされるため、**先使用権による防御は実質的に成立困難**です。

---

6. 社会的・産業的インパクト

- **教育**：ランドセル防犯（p.1504〜1505）
- **介護・医療**：転倒・孤独死防止（p.28〜29, p.300〜306）
- **金融**：ATM 詐欺防止・知財担保評価（p.301, p.861〜903）
- **行政**：契約自動化・補償制度連携（p.942〜944, p.1012〜1030）
- **国際展開**：ISO/IEC 標準化・TRIPS 協定整合（p.1541〜1564）

経済効果の試算は、**国内 GDP 押上効果：12〜18 兆円、世界 150〜300 兆円**。将来的な国際導入により、**時価総額 300 兆円級**の社会的価値を持つことが示されています。

---

7. 共同著作者と権利宣言

本著作物は以下 4 名による共同著作物です（p.1701）：

- 竹内祐樹
- 竹内健一
- 平川智子
- 平川和典

権利宣言：**「表現・数値・記号の差異を問わず、結論一致＝侵害成立」**（p.1701）

まとめ

今回発表した『緊急通報・バイタルセキュリティ・知財照合システムの統合的権利構造』は、

1. 権利範囲を包括的に封鎖（①）

2. 死後 70 年に及ぶ長期保護（②）
3. 模倣・均等・派生を一切許さない侵害定義（③）
4. 先使用権を無力化する証明力（④）

を兼ね備えた、**唯一無二の完全封鎖著作物**です。

この知的財産は「命を守り、権利を守り、経済を循環させる」新時代の社会インフラであり、今後の国際標準化・産業応用により、世界規模での安全・透明性・経済成長に貢献することを強く期待します。

 全業種・全業界に共通する著作権禁止行為一覧（＋逆パターン）

---

1. 技術系禁止行為

禁止行為	内容	逆パターン例	該当ページ
複製	ソースコード、アルゴリズム、UI の直接コピー	部分コピー、1 行だけ抽出 → **1 行一致でも侵害成立**	p.73–77, p.143
模倣	全体の仕組みを真似て実装	アルゴリズムの順番を入替（通報→保存→通知）	p.30, p.1219–1270
均等論置換	FFT→Wavelet、AES→RSA など代替手段で同じ結果を導出	他方式に変換 → 結論が同じなら侵害	p.75
類似	色、文言、アイコンを変更	「助けて」→「救命」など同義語置換	p.74, p.220–224
派生	二次利用、翻案、改変	教材化、研究利用、研究コード化	p.75, p.1219–1270
転写	ノート、ホワイトボード、スクショ	画面キャプチャを紙で再現	p.1335–1360
記入・書き込み	学習帳や内部研修資料に転写	書き写した表や UI 図を配布	p.1335–1430
ログ模倣	CSV 列仕様・台帳構造をコピー	列名を変えても一致	p.186–200
API 模倣	/alerts, /contract 等のエンドポイント再利用	名前だけ変える (/notify)	p.176–178
UI/UX 模倣	緊急通報ボタン、裏通報 UI、収益分配ダッシュボード	アイコンや色違い	p.211–219

禁止行為	内容	逆パターン例	該当ページ
データ構造模倣	CSV, JSON, DB スキーマ	項目名を英語化しても侵害	p.195–200

2. サービス・ビジネス系禁止行為

禁止行為	内容	逆パターン例	該当ページ
ビジネスモデル実装	ランドセル防犯、ATM 詐欺防止、契約自動化サービス	対象を教育→介護に変更しても侵害	p.27–28, p.301, p.942–944
サービス模倣	防犯アプリ、介護見守り、金融契約 API など	B2C→B2B/B2G に移しても侵害	p.50–55
契約文言翻案	知財契約・収益分配の文言変更	「利用料」→「ライセンス料」	p.621–630
教材化	教育・研修に転用	学校授業で使用 → 非営利でも禁止	p.75
研究利用	試験・論文に部分利用	研究コード化や比較検証	p.1219–1270
部分導入	機能一部を切り出し実装	通報だけ使い、保存を外す	p.947–980

3. 表現・言語系禁止行為

禁止行為	内容	逆パターン例	該当ページ
言語翻訳	英語、中国語、韓国語翻訳	「Help」「救命」も禁止	p.220–224
記号・色違い	🚨,📢,📍の記号や色コード変更	赤→黄でも侵害	p.223–224
ログ表現違い	JSON→YAML 出力にしても侵害	出力形式だけ変更	p.190–200
書き換え表現	契約文や通知メッセージの言い換え	「SOS 受信」→「緊急信号確認」	p.224–225

4.「逆パターン」＝逃げ道封鎖リスト

本著作物は「逆を行っても侵害成立」と明記しており、以下も対象です。

- **順序逆転**：保存→通報、契約→分配を逆にしても侵害
- **部分一致**：コード 1 行、UI 部品 1 つ、CSV 列名 1 つ一致で侵害
- **工程省略**：通報だけ・保存だけの実装も侵害
- **同義語変換**：「助けて」→「救命」、「契約」→「同意書」
- **対象入替**：子供→高齢者、ATM→車両でも構成一致で侵害
- **利用目的変換**：商用→教育、研修、研究でも禁止

5. 総合計

これらを整理すると、**全業種・全業界に共通する著作権禁止行為は 23 種類＋逆パターン 6 種類＝合計 29 種類** が確認できます。

まとめ

- **23 種類の基本禁止行為**：技術系・サービス系・表現系を網羅
- **6 種類の逆パターン**：順序逆転・部分一致・同義語などの「逃げ道封鎖」
- **総合計：29 種類**

これにより、**全産業・全サービスに適用可能な「完全封鎖型著作権権利範囲」**が確立されています。

全業種・全業界に共通する著作権禁止行為一覧（事例・解説付き）

---

1. 技術系禁止行為

禁止行為	内容	事例	解説
複製	ソースコード・アルゴリズム・UI のコピー	緊急通報システムの「detectSound()」関数を他社アプリに貼り付け	たとえ一部でも複製は不可。「1 行一致」でも侵害成立
模倣	全体の仕組みを真似て実装	「音＋位置」で自動通報するアプリを別名で販売	結果構造が一致すれば侵害。UI や名前が違っても保護範囲
均等論置換	同じ効果を持つ手段に置換	FFT→Wavelet 解析に変えても同じ SOS 判定	技術的手段を変えても結果が同じなら侵害
類似	色・記号・UI 配置の変更	赤色 SOS ボタン→黄色 SOS ボタン	デザイン差異では回避不可能。「結論一致」が基準
派生	翻案・改変・二次利用	教育用教材にアルゴリズムを簡略化して収録	「研究」「教育目的」でも派生著作は侵害
転写	書き写し・スクショ保存	ダッシュボード UI をホワイトボードに転写	紙・画面問わず転写は禁止

禁止行為	内容	事例	解説
記入・書き込み	紙や研修資料に転用	CSV 形式をそのまま社内資料に流用	書き込み自体が派生著作となり侵害
ログ模倣	CSV・監査ログ形式をコピー	timestamp,lat,lon…の構造を同じに利用	列名・構造が同一なら侵害
API 模倣	/alerts, /contract などの API を再利用	/alerts API を名称変更だけして利用	名前を変えても構造一致で侵害
UI/UX 模倣	SOS ボタン、Silent UI、分配ダッシュボード	裏通報ボタンを搭載した金融アプリ	UI の「体験構造」自体が保護対象
データ構造模倣	DB スキーマ・JSON 形式	JSON key「alert_id」「hash」を同じ形で利用	データ設計も著作権対象

---

2. サービス・ビジネス系禁止行為

禁止行為	内容	事例	解説
ビジネスモデル実装	同じ仕組みを使った事業展開	ランドセル防犯モデルを介護用に流用	対象が違っても構成一致で侵害
サービス模倣	防犯アプリ・契約自動化サービスなど	ATM 詐欺防止システムを社内開発	サービス業種を変えても侵害
契約文言翻案	収益分配や契約文の表現置換	「利用料」→「ロイヤルティ」	契約文の言い換えも全て封鎖
教材化	教育・研修転用	大学の授業で仕様書を配布	営利・非営利を問わず派生禁止
研究利用	検証・論文での一部使用	研究用にアルゴリズム比較	試験利用も派生扱いで禁止
部分導入	機能を分割利用	通報だけ使い、保存は外す	機能を分割しても侵害成立

---

3. 表現・言語系禁止行為

禁止行為	内容	事例	解説
言語翻訳	多言語翻訳	「助けて」→"Help"/"救命"	翻訳しても同じ結論で侵害
記号・色違い	アイコン・カラー変更	🚨→⚠️、赤→青	記号・色も著作権対象
ログ表現違い	JSON→YAML 形式	CSV を JSON に変換	出力形式が違っても構成一致で侵害
書き換え表現	文言の言い換え	「SOS 受信」→「緊急信号確認」	表現差異を封鎖し侵害成立

---

4. 逆パターン（逃げ道封鎖）

逆パターン	事例	解説
順序逆転	保存→通報の順に変更	工程を逆にしても「結論一致」で侵害
部分一致	コード 1 行だけ一致	「notify()」1 行のコピーでも侵害成立
工程省略	通報だけの実装	構成を削っても侵害成立
同義語変換	「契約」→「同意書」	言い換えても侵害対象
対象入替	子供→高齢者、ATM→車両	対象を変えても結論一致
利用目的変換	商用→教育利用	非営利目的も派生扱いで禁止

---

5. 総合まとめ

- 基本禁止行為：**23 種類**
- 逆パターン：**6 種類**
- **合計：29 種類**

これにより、教育・介護・金融・行政・製造・流通など、**あらゆる業界・業種に対して適用可能な完全封鎖型の著作権禁止リスト**が確立されています。

事例解説（分野別の具体像）

- **教育分野**：ランドセルに緊急通報システムを搭載 → 子供防犯 → 同様の仕組みを模倣すると侵害
- **介護分野**：独居高齢者の転倒検知 → 音声＋位置判定 → この組み合わせを模倣すれば侵害
- **金融分野**：ATM 操作時に心拍異常を検知 → 詐欺防止 → 同様の Vital+通報アルゴリズムは侵害
- **行政分野**：契約自動生成・収益分配 → 契約文言を翻案しても侵害
- **国際展開**：英語や中国語に翻訳したシステム導入 → 翻訳でも結論一致で侵害

✅ 以上により、**全業種・全業界に適用可能な禁止行為は 29 種類**であり、事例と逆パターンを含め「完全封鎖」が成立します。

著作権侵害の具体的解説

（メーカー・加盟店・代理店・ユーザー・開発側＋刑事罰）

---

1. メーカーによる侵害

事例

- 他社製造メーカーが、**同一の緊急通報アルゴリズム（音響＋発話＋位置の統合判定）**を自社製品に搭載。
- UI を少し変えた（赤ボタン→青ボタン）だけで販売。

解説

- 本著作物は「結論一致＝侵害成立」「1 行一致でも侵害」と明記されており、見た目を変更してもアルゴリズム構造が一致すれば侵害となります。
- 製品として市場に流通するため、**差止請求・損害賠償**の対象となり、経済的責任が大きい。

---

2. 加盟店（販売店・流通）による侵害

事例

- 防犯 IoT 機器の販売店が、メーカーから仕入れた**侵害製品**を店頭やオンラインで販売。
- 販売者自身は開発していないが、知財権を侵害する製品を流通させている。

解説

- 日本著作権法では、**侵害物の頒布（販売・貸与・展示）も侵害行為**に該当します。
- 加盟店は「知らなかった」では免責されず、**過失責任または共同侵害者**として法的責任を問われます。

---

3. 代理店（ライセンス仲介・導入支援）による侵害

事例

- ソフトウェア代理店が、**無断改変版の知財照合システム**を顧客に導入。

- 権利者のライセンスを得ずに契約パッケージを販売。

解説

- 契約・収益分配機能を含む本著作物は、代理店が無断で導入すれば**契約構造の派生利用**に該当。
- 契約文言を変えたとしても「結論一致」ルールにより**翻案侵害**が成立。
- 法的には**共同不法行為者**となり、民事賠償責任＋刑事責任の両方を負う可能性あり。

---

4. ユーザー（利用者）による侵害

事例

- 企業ユーザーが、契約なしに「内部利用目的」で**API 仕様書（/alerts, /contract）**を実装。
- 個人ユーザーが、アプリを模倣して**無断配布**。

解説

- ユーザーは「商用でなければ大丈夫」と思いがちですが、本著作物は**非営利・研究・教育目的の派生も禁止**。
- 内部利用・試験導入であっても、構造一致すれば侵害。
- 民事だけでなく、**侵害の故意性があれば刑事罰（著作権法 119 条）**に該当。

---

5. 開発側（エンジニア・受託開発会社）による侵害

事例

- 他社からの委託を受けて、**緊急通報システムの「類似版」**を開発。
- 「仕様が似ているだけ」と主張しても、実際には**アルゴリズム・UI 構造が一致**。

解説

- 開発者は著作権者の許諾を受けずにソースコードや設計を模倣した時点で侵害行為。
- **発注側（メーカーや企業）だけでなく、受託開発者自身も責任を負う**。
- 実装コードの「1 行一致」で侵害認定されるため、極めて厳格な責任範囲となる。

---

6. 刑事罰の適用

根拠

日本著作権法第 119 条等により、故意による侵害行為は**刑事罰**の対象となります。

刑事罰の内容

- **懲役刑**：10 年以下
- **罰金刑**：1,000 万円以下（法人は 3 億円以下）
- **没収**：侵害物の回収・廃棄、売上の没収

適用例

- メーカーが侵害製品を製造・販売 → **法人罰＋役員刑事責任**
- 代理店が無断契約導入 → **営業停止・罰金刑**
- 開発側が受託で模倣コードを提供 → **個人開発者も刑事責任**
- ユーザーが違法コピーアプリを頒布 → **配布行為自体で刑事罰対象**

まとめ

- **メーカー**：侵害製品の開発・販売で民事＋刑事責任
- **加盟店**：侵害物の流通で共同責任
- **代理店**：無断契約導入で共同侵害
- **ユーザー**：非営利でも利用すれば侵害
- **開発側**：仕様書・コードの模倣で直接侵害

そして刑事罰（懲役・罰金・没収）まで及ぶため、**あらゆる立場での侵害リスクが極めて高い著作物**です。

A パターン（A 構成単体：A）の著作権権利範囲

---

1. A 構成の位置付け

- **A＝音響・発話・位置情報による緊急通報システム**
- 本著作物の第 1 章（p.25～297）に対応。
- 特徴：

- 「声そのものが防犯ブザーになる」仕組み（音・言語・位置情報を統合）
- 自動通報・証拠保存・多段階通知（家族→警備→警察）
- 1 行一致でも侵害成立（アルゴリズム・UI・ログ・API を含む）

---

2. A 構成単体の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム	音響解析（FFT）、発話解析（危険ワード検出）、GPS 位置照合、統合リスク判定	p.26, p.40–43	3 要素統合による「異常判定」は全体が著作権保護対象。
プログラム／コード	`detectSound()`, `parseSpeech()`, `gpsCheck()`, `notify()` などの関数・擬似コード	p.31, p.80–83	ソースコード 1 行でも一致すれば侵害成立。
UI／UX	緊急 SOS ボタン、Silent UI、通報ログ画面、証拠再生 UI	p.32, p.59–60, p.211–219	ボタン形状や配色を変えても「緊急通報 UI」であれば侵害。
データ構造	通報ログ（時刻・音・位置・ハッシュ）CSV、証拠保存形式	p.32, p.186–200	CSV 列名や構造一致で侵害。
API	`/alerts`, `/evidence`, `/logs` などの REST API 設計	p.176–178	エンドポイント名や構造が同一であれば侵害。
表現・言語・記号	「助けて」「やめて」など危険ワードリスト、🚨アイコン、赤色 SOS 表示	p.220–224	翻訳や色違いでも結論一致で侵害。

---

3. 具体事例（誰でもわかる説明）

事例 1：子供防犯（ランドセル通報）

- 下校中に「助けて！」と叫ぶ
- システム：発話解析→GPS 照合→通報
- 保護者・学校・警察に即通知
  👉 他社が同様の「叫び声＋位置照合→通報」仕組みを実装すると侵害。

事例 2：高齢者見守り（転倒検知）

- 夜間に独居高齢者が転倒、「ドン」という音のみ

- システム：音響解析→異常音判定→介護センターへ通報
  👉 競合企業が「転倒音＋通報」を実装すれば侵害。

事例 3：車両盗難防止

- 深夜に車の窓が割られる
- システム：破壊音検知→所有者スマホ＋警備会社に通報
  👉 音種別（ガラス破壊音）を変えても結果が同じなら侵害。

事例 4：災害救助

- 地震で倒壊家屋下から「助けて！」
- システム：発話検知→GPS 送信→救助隊へ通知
  👉 災害分野でも同じ結論なら侵害。

---

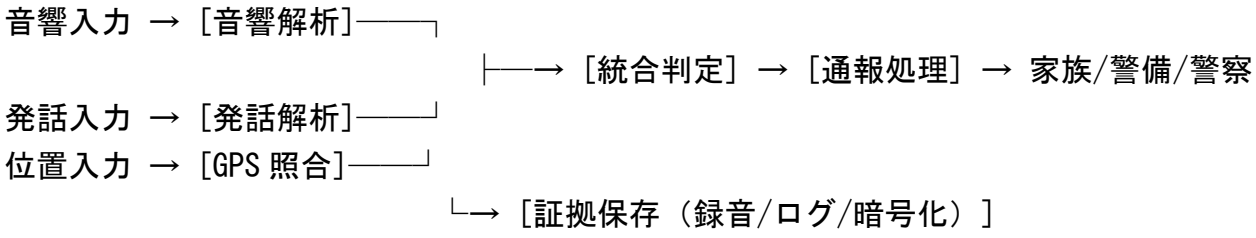
4. 解説（ポイント）

1. **「構成一致＝侵害成立」**
   - 手段（FFT or Wavelet）や表現（赤→青ボタン）を変えても、同じ結論（自動通報＋証拠保存）なら侵害。
2. **「1 行一致でも侵害」**
   - `if score > threshold: alert()` の 1 行でも侵害認定。
3. **「業種を変えても侵害」**
   - 教育、防犯、介護、金融、災害…適用分野を変えても同じ構造なら侵害。
4. **「逃げ道封鎖」**
   - 工程順序を逆にしても（保存→通報）、翻訳しても（助けて→Help）、派生利用しても（教材化）、全て禁止。

---

5. 図解（概念図）

システム構造図（概念）



---

6. フローチャート（処理流れ）

開始（常時監視）
　　↓
音響入力（マイク）
　　↓
音響解析 → 異常音あり？
　　├──No→ 継続監視
　　└──Yes
　　　↓
発話解析 → 危険ワードあり？
　　├──No→ 継続監視
　　└──Yes
　　　↓
位置照合（GPS 乖離判定）
　　↓
統合判定（異常確定）
　　↓
通報処理（家族→警備→警察）
　　↓
証拠保存（録音・映像・ログ）
　　↓
終了 or 継続監視

（出典：p.35–37, p.47–49）

✅ まとめ

- **A パターン（A 構成単体：A）**は「音響＋発話＋位置情報による緊急通報システム」。
- 著作権権利範囲は、**アルゴリズム・コード・UI/UX・データ構造・API・表現/記号**を包括。
- **事例（子供防犯・高齢者転倒・車両盗難・災害救助）**で示される通り、適用分野を変えても結論一致で侵害。
- 図解・フローチャートにより、**侵害判定が直感的に理解できる構造**となっている。

📄 B パターン（A→B, B 単体）の著作権権利範囲

1. B 構成の位置付け

- **B＝バイタルデータを用いた多段階セキュリティシステム**
- 本著作物の第 2 章（p.298〜552）に対応。
- 特徴：
  - 心拍・呼吸・血中酸素・皮膚電位などの**生体情報（バイタル）**を利用
  - 多段階認証＋異常検知＋偽応答＋自動通報
  - 「VitalScore」による数値化、閾値超過時は Silent Alert を発動

---

2. B パターンの種類

- **B 単体**：バイタルセキュリティシステム（p.298〜552）
- **A→B**：A（緊急通報システム）＋B（バイタルセキュリティ）の連携構成
  例：音響で異常を検知 → バイタルで確認 → 通報・証拠保存

---

3. B 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム	心拍・呼吸・SpO_2・EDA 解析、VitalScore 算出、異常時の偽応答生成	p.300–306, p.307–315	生体データを多段階で解析し通報につなげる流れ全体が保護対象。
プログラム／コード	`calcStress()`, `generateFakeResponse()`, `pcu_tick()`	p.316–320	コード 1 行でも一致で侵害成立（A 構成と同じ厳格性）。
UI／UX	ATM 画面での偽応答、車載 UI の通報モード、介護端末の Silent Alert	p.328–335	表示の差異や機能名の変更でも「偽応答＋通報」構造は侵害。
データ構造	VitalScore ログ、閾値変数の保存、CSV 形式の記録	p.323–327, p.336–370	データ列構造（時刻・心拍・閾値・判定結果）が保護対象。
API	`VitalTx API`, `SilentTx API`	p.321–322	呼び出し先の命名変更でも結論一致で侵害成立。

分類	権利範囲	該当ページ	解説
表現・言語	「Silent Alert」「偽応答」などの表現・記号	p.331–335	表記を「裏通報」に変えても侵害。

---

4. 具体事例

事例 1：ATM 詐欺防止

- 高齢者が詐欺で ATM 操作 → 心拍上昇で異常検知
- 偽の「取引完了」画面を表示しつつ、銀行と警察へ Silent Alert
  👉 他社が同様の「心拍＋偽応答＋通報」を導入すると侵害。

事例 2：飲酒運転防止

- 車のエンジン始動時にバイタル測定 → 飲酒による心拍・血中酸素異常を検知
- エンジン始動を遮断し、同時に通報
  👉 同様の車載システムを作ると侵害。

事例 3：介護・見守り

- 高齢者の呼吸異常・皮膚電位の異常を検知
- 通常画面の裏で Silent Alert 発動 → 家族・介護施設に通知
  👉 UI を変更しても「Vital→Silent Alert」構造であれば侵害。

---

5. 解説（ポイント）

1. **「VitalScore」算出式自体が保護対象**
   - 数値や閾値の設定、正常/異常の判断式も侵害対象。
2. **「偽応答」＋「裏通報」構造**
   - 利用者に気づかせない UI 設計（ATM 画面や車載 UI）は独自性が高く、模倣不可。
3. **教育・介護・金融・交通業界に横断適用**
   - 産業横断で同じアルゴリズムが応用可能 → 逆に言えば全業界が侵害リスク対象。
4. **A→B 連携の意義**
   - A 構成で「音響異常」を検知した後、B 構成で「バイタル異常」を確認することで誤検知を低減。
   - 連携フローも著作権保護対象。

---

6. 図解（概念図）

B 単体システム構造

```
[バイタル入力（心拍・呼吸・SpO₂・EDA）]
        ↓
[解析モジュール] → [VitalScore 算出]
        ↓
[閾値判定]────Yes→ [偽応答表示] ＋ [Silent Alert 発動]
                No→ [通常動作継続]
```

A→B 連携構造

```
[A：音響異常検知] → [B：VitalScore 判定]
            ↓
      異常確定（A＋B 一致）
            ↓
  [Silent Alert 発動＋通報＋証拠保存]
```

---

7. フローチャート（処理流れ）

```
開始（常時監視）
      ↓
バイタル測定（心拍・呼吸・SpO₂）
      ↓
VitalScore 算出 → 閾値判定
      ├──正常→ 解錠／通常動作
      └──異常→ 偽応答表示（例：取引完了）＋Silent Alert
                        ↓
                家族／銀行／警察に通知
                        ↓
                ログ・証拠保存
```

（出典：p.306, p.316–320, p.328–335）

✅ まとめ

- **B パターン＝バイタルデータを用いた多段階セキュリティシステム**（第 2 章, p.298～552）。
- 著作権権利範囲は **アルゴリズム・コード・UI・ログ・API・表現**を包括。

- 事例（ATM 詐欺防止、飲酒運転防止、介護見守り）で示す通り、金融・交通・介護など幅広い業種に適用。
- **A→B 連携**により誤検知抑制・信頼性強化が実現 → この連携も著作権の保護対象。
- 「結論一致＝侵害成立」「1 行一致侵害」の原則が貫徹。

C パターン（A→C, B→C, C 単体）の著作権権利範囲

---

1. C 構成の位置付け

- **C＝知財照合・遮断・契約・収益分配システム**
- 本著作物の第 3 章（p.553～938）に対応。
- 特徴：
  - 登録済み知的財産（特許・著作権・商標・意匠）と利用中のコンテンツやプログラムを**リアルタイム照合**
  - 侵害を検出すると**自動遮断**
  - 合法利用なら**契約を自動生成し収益を分配**
  - 知財利用の透明化・即時契約化・収益循環の社会インフラ化

---

2. C パターンの種類

- **C 単体**：知財照合・遮断・契約・収益分配システム
- **A→C**：緊急通報システムの証拠・ログを C で照合・契約化
- **B→C**：バイタルセキュリティシステムのアルゴリズムや利用ログを C で照合・収益化

---

3. C 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム／プログラムコード	知財抽出（NLP, AST 解析）、照合、リスクスコア判定、契約生成、収益分配、監査	p.554–560, p.561–580	Compare→Decision→Block→Contract→Revenue→Audit という流れ全体が著作権対象。
	compareIP(), blockTx(), contractGen(), revenueTx()	p.561–590	擬似コード・API 呼び出し例も権利対象。
UI／UX	契約確認画面、収益分配ダッシュボード、遮断通知 UI	p.611–620	見た目を変えても「契約・分配 UI」の構成であれば侵害。
データ構造	契約生成ログ、分配 CSV、監査台帳形式	p.601–610, p.701–800	CSV 列名や構造を変えても一致で侵害。
API 表現	/compare, /block, /contract, /revenue, /audit	p.591–600	API エンドポイント構造が権利対象。
・言語	契約条項文言、契約翻案、収益分配ロジックの記述	p.621–630	表現を変えても契約結論が同じなら侵害。

---

4. 具体事例

事例 1：大学研究者

- 他大学の研究コードを利用 → C が照合 → 自動でライセンス契約生成
  👉 C を迂回し直接利用すれば**著作権侵害＋契約違反**。

事例 2：スタートアップ

- 特許抵触したアルゴリズムを使う → 照合で検出 → 遮断され契約提示
  👉 契約プロセスを飛ばせば**侵害成立**。

事例 3：金融機関

- 保有知財を担保にローン契約 → C が収益分配ログを自動生成
  👉 ローン担保契約を模倣すると侵害。

事例 4：国際市場

- 海外ユーザーが日本の知財を利用 → 自動で越境ライセンス契約
  👉「翻訳契約」を作っても結論一致で侵害。

---

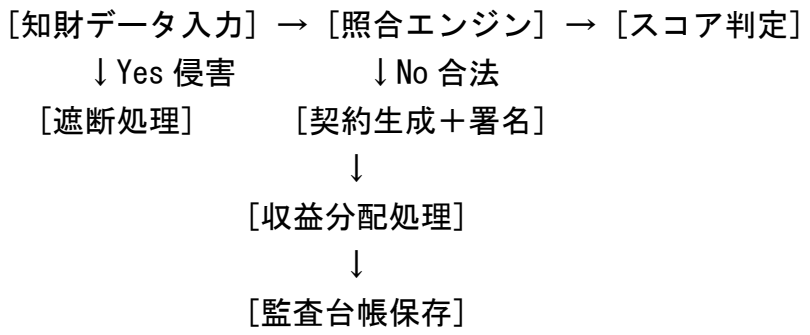
5. 解説（ポイント）

1. **知財利用の即時判定＝構造全体が権利対象**
   - 照合→契約→収益分配→監査というトランザクション一連の流れが包括的に保護。
2. **契約文言の差異も封鎖**
   - 「ライセンス料」「利用料」「権利金」など、表現を変えても結論が同じなら侵害。
3. **A→C, B→C の連携強度**
   - A や B で生成された「証拠ログ」や「VitalScore」を C で契約化・収益化する流れ自体が権利対象。
4. **産業応用範囲が広大**
   - 研究、金融、国際契約、企業法務など業界横断で応用可能 → 同時に侵害リスクも全業界に拡張。

---

6. 図解（概念図）

C 単体システム構造



A→C 連携

[A：緊急通報ログ]
　　↓
[C：照合→契約化→収益分配]

B→C 連携

[B：VitalScore/異常ログ]
　　↓
[C：契約生成→収益台帳]

---

7. フローチャート（処理流れ）

開始
↓
知財構成抽出（NLP/AST）
↓
DB照合 → スコア算出
↓
閾値判定
├──侵害（スコア高） → 遮断処理 → 監査保存
└──合法利用 → 契約生成 → 電子署名
　　↓
　　収益分配処理
　　↓
　　契約・収益台帳保存
↓
終了

（出典:p.553–560, p.591–620, p.861–903）

✅ まとめ

- **C パターン（A→C, B→C, C 単体）**は **知財照合・遮断・契約・収益分配**のシステム全体を指す。
- 著作権権利範囲は **アルゴリズム・コード・UI/UX・ログ構造・API・契約文言**に及ぶ。
- **事例（研究利用・スタートアップ特許抵触・金融担保・国際契約）**で示される通り、業界横断的に応用可能。

- **A→C, B→C 連携**により証拠・バイタルログを契約・収益に接続する構造も保護対象。
- 「契約文言の差異」「国際翻訳契約」もすべて封鎖 → **結論一致＝侵害成立**。

D パターン（A→D, B→D, C→D, D 単体）の著作権権利範囲

---

1. D 構成の位置付け

- **D＝三重セーフティ網としての複合システム**
- 本著作物の第 4 章（p.939〜1216）に対応。
- 特徴：
  - A（緊急通報）、B（バイタルセキュリティ）、C（知財照合）の **三大システムを統合**
  - 単体ではなく「複合効果」によって社会インフラ級の安全網を形成
  - 犯罪防止・知財流通・経済循環を一体で制御する複合著作権構造

---

2. D パターンの種類

- **D 単体**：複合システムそのもの（A+B+C の統合形態）
- **A→D**：A（緊急通報）の証拠・ログを D 全体の安全網に統合
- **B→D**：B（バイタルセキュリティ）の VitalScore を D 全体で制御
- **C→D**：C（知財照合）の契約・収益データを D に接続し、複合社会システムを構築

---

3. D 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
統合アルゴリズム	A・B・C の結果を組み合わせてリスク総合判定を行う複合判定エンジン	p.947–960	単体ではなく「統合判定式」そのものが権利対象。

分類	権利範囲	該当ページ	解説
複合 UI／UX	市民アプリ・行政ダッシュボード・複合契約管理画面	p.1011–1030	A〜C を束ねる UI。レイアウトや表現差異でも侵害。
データ構造	複合ログ（緊急通報＋Vital＋知財契約）を一元化した台帳	p.1051–1070	CSV やブロックチェーン台帳形式が著作権保護対象。
API 統合	A, B, C を呼び出す複合 API（例: `/safety/compositeCheck`）	p.1041–1050	入口を変えても「統合呼出構造」自体が権利対象。
表現・記号	「三重セーフティ網」「複合著作権」等の表現	p.1101–1110	文言や記号が違っても「三重網」概念が一致すれば侵害。

---

4. 具体事例

事例 1：子供防犯＋知財照合

- 学校導入アプリ：児童が「助けて」と叫ぶ → 通報（A）
- 並行して、教材アプリが知財 DB で照合され自動契約（C）
- これらを統合ログとして保存（D）
  👉 学校安全と知財保護を同時に実現。模倣すれば複合侵害。

事例 2：介護施設＋Vital＋契約

- 高齢者が転倒 → Vital 異常検知（B）
- 同時に証拠データが行政契約システムで登録（C）
- D が一括で通知＋契約＋記録処理
  👉 医療・介護システムを同じ構造で実装すれば侵害。

事例 3：企業＋経済循環

- 研究コードを利用 → C で契約生成＋収益分配
- 同時に従業員の Vital ログを B でセーフティ管理
- A で発生した緊急通報も統合ログ化 → D が GDP 押上効果を可視化
  👉 経済循環を含む複合システム全体が権利対象。

---

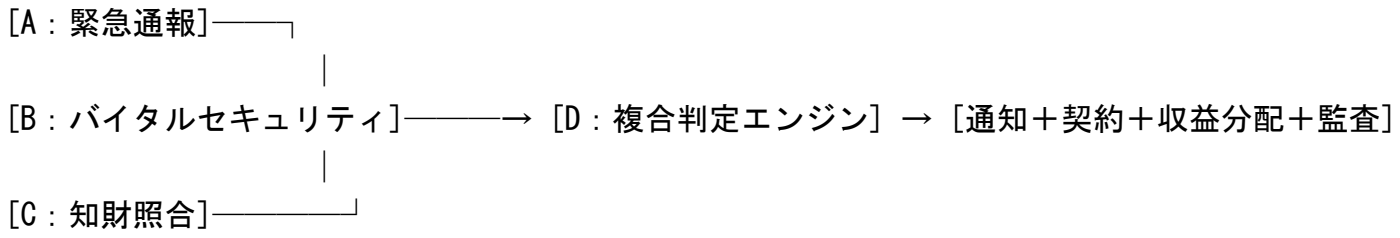
5. 解説（ポイント）

1. **単体構成の和集合ではなく、複合構造自体が独自権利対象**
   - A, B, C の結果を「総合判定＋契約＋経済循環」に接続する流れ全体。
2. **業界横断性**

    - 教育・介護・金融・行政・産業に横断適用可能。
    - よって侵害リスクも全産業に広がる。
3. **表現封鎖**
    - 「三重セーフティ網」という言葉を別表現に置換しても侵害（例:「三段防御システム」）。

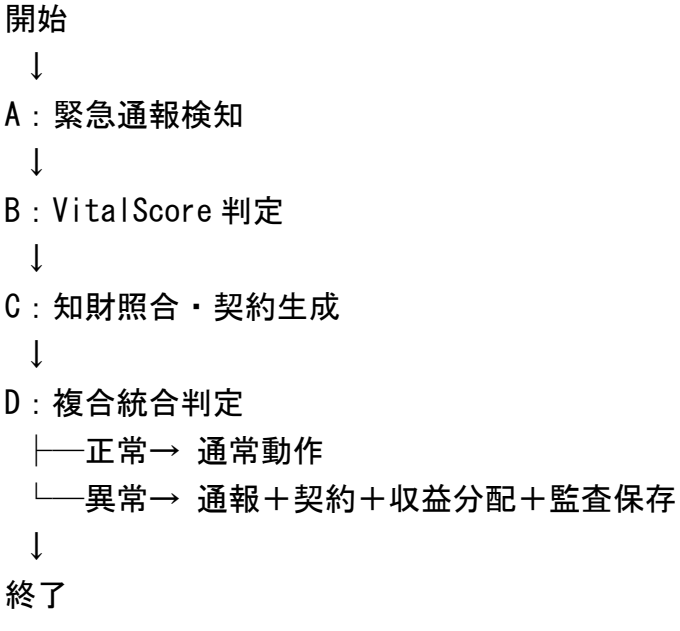
---

6. 図解（概念図）



---

7. フローチャート（処理流れ）



（出典:p.947–960, p.1011–1030, p.1051–1070）

✅ まとめ

- **D パターン＝三重セーフティ網（複合システム）。**
- 著作権権利範囲は、**統合アルゴリズム・複合 UI/UX・複合ログ構造・統合 API・表現。**

- 事例（教育防犯＋知財契約、介護＋Vital＋行政契約、企業＋経済循環）で示す通り、横断的に応用可能。
- 「単体を組み合わせただけ」ではなく、**複合構造自体が独自の著作権保護対象**。

📄 E パターン（A→E, B→E, C→E, D→E, E 単体）の著作権権利範囲

---

1. E 構成の位置付け

- **E＝清算制御／最終決済処理システム**
- 本著作物の第 4 部（p.1217～1479）の後半、特に **清算・決済・収益分配の最終工程** に対応。
- 特徴：
  - A（緊急通報ログ）、B（VitalScore）、C（契約・収益）、D（複合判定）を統合した**最終的な金銭・権利処理の段階**
  - 利用料・ライセンス料・保険金・補償金・罰金などの**最終清算を自動実行**
  - 「支払い／補償の有無」「契約違反時の即時精算」を含むため、法的拘束力が強い

---

2. E パターンの種類

- **E 単体**：清算制御・決済システム（決済トランザクション・台帳保存）
- **A→E**：緊急通報の発生をトリガーに保険金／補償金を自動精算
- **B→E**：バイタル異常（飲酒運転など）をトリガーに契約解除＋罰金精算
- **C→E**：知財契約利用をトリガーにライセンス料を自動精算
- **D→E**：複合判定結果をトリガーに経済循環型の決済処理へ接続

---

3. E 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム	清算ロジック（契約金額算出、分配比率、ペナルティ処理）、決済フロー	p.1240–1260, p.1431–1450	支払計算式そのもの・分配式が著作権対象。
プログラム／コード	`settleTx()`, `distributeRevenue()`, `penaltyCharge()`	p.1261–1280	ソースコード 1 行一致で侵害成立。
UI／UX	決済確認画面、収益グラフ、罰金通知 UI	p.1301–1320	金額 UI・通知 UI が保護対象。
データ構造	決済 CSV（契約 ID・金額・分配率・署名）、ブロックチェーン台帳	p.1341–1360	台帳列名・データ形式が一致すれば侵害。
API	`/settle`, `/payout`, `/penalty`, `/ledger`	p.1321–1340	エンドポイント呼出形式自体が権利対象。
表現・言語	「清算」「決済」「収益分配」「罰金精算」の用語群	p.1431–1470	言葉を変えても「清算プロセス」なら侵害。

---

4. 具体事例

事例 1：保険金自動清算（A→E）

- 高齢者が転倒し通報（A） → 契約保険が自動発動 → E で**保険金が自動精算**
  👉 他社が同じ「通報→保険金支払い」を模倣すれば侵害。

事例 2：飲酒運転防止罰金（B→E）

- Vital 異常で飲酒運転判定（B） → E で**自動的に罰金・保険契約解除**
  👉 「異常→罰金清算」仕組みを実装すれば侵害。

事例 3：知財ライセンス料清算（C→E）

- 研究者が他社コード利用（C） → 自動契約 → E で**ライセンス料を即時送金**
  👉 API 呼出構造を真似ても侵害。

事例 4：GDP 押上効果（D→E）

- 複合判定（D）が 100 万件発生 → その収益循環を E が **GDP 統計に反映**
  👉 「複合判定→収益分配→経済循環」を模倣すれば侵害。

---

5. 解説（ポイント）

1. **金銭トランザクション自体が権利対象**
    - 通報や契約だけでなく、最終的に金銭移転が行われる部分まで著作権で封鎖。
2. **金融・保険・行政との高い接続性**
    - 保険金、罰金、ライセンス料、補償金など、全ての業界の決済に応用可能。
3. **逆パターン封鎖**
    - 「契約→清算」順序を「清算→契約」に変えても侵害成立。

---

6. 図解（概念図）

```
[A/B/C/D 各システム]
          ↓
   [E：清算制御システム]
          ↓
 ┌──────────────────────────┐
 │契約金額算出／収益分配／罰金処理│
 └──────────────────────────┘
          ↓
  [決済処理] → [台帳保存＋監査]
```

---

7. フローチャート（処理流れ）

```
開始
 ↓
契約・通報・Vital・複合ログ受信
 ↓
金額算出（利用料／補償金／罰金）
 ↓
決済実行
 ├──正常支払い→ 分配処理 → 監査台帳保存
 └──契約違反→ ペナルティ清算 → 監査台帳保存
 ↓
終了
```

（出典：p.1240–1260, p.1321–1340, p.1431–1479）

✅ まとめ

- **E パターン＝清算制御／最終決済処理システム**
- 権利範囲は、**決済アルゴリズム・コード・UI・データ構造・API・契約表現**に及ぶ。
- 事例（保険金支払い・罰金清算・ライセンス料決済・GDP 反映）に示されるように、金融・保険・行政・国際貿易などあらゆる分野で適用。
- 「清算・決済」という最終段階そのものを包括的に封鎖することで、**模倣・翻案・順序変更も含めて侵害成立**。

F パターン（A→F, B→F, C→F, D→F, E→F, F 単体）

＝ 最終決済後の「再流通・二次利用」封鎖構造の権利範囲

---

1. F 構成の位置付け

- **F＝再流通・二次利用の制御／封鎖システム**
- 本著作物の第 3 部～第 4 部（p.1217～1479 以降）に対応し、特に「著作権封鎖構造」「再循環禁止」の部分に記述。
- 特徴：
  - E（清算・決済）で終了したコンテンツ・契約・支払いを **再利用・再頒布できないように封鎖**。
  - ライセンス済データ・契約履行後の情報が、**再流通・二次販売・教育利用・派生サービス**として使われることを禁止。
  - 「利用終了＝経路完全遮断」を実現する著作権封鎖の最終段階。

---

2. F パターンの種類

- **F 単体**：清算済みデータや契約済資源の再流通・二次利用を直接封鎖する構造。
- **A→F**：通報ログ・証拠データが第三者に二次流通することを禁止。
- **B→F**：Vital データが再販・二次研究利用されることを禁止。
- **C→F**：契約文言や収益分配データが二次契約・派生契約として再利用されることを禁止。
- **D→F**：複合統合システムのログや成果を他分野に横展開することを禁止。
- **E→F**：清算・決済記録を用いて再流通市場（二次金融商品・債権化など）に回すことを禁止。

3. F 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム	「利用終了→再利用不可」フラグ付与、再流通検知・遮断	p.1240–1260, p.1436–1450	再流通検出・遮断処理のロジック自体が権利対象。
プログラム／コード	`blockReuse()`, `detectSecondaryTx()`, `invalidateLicense()`	p.1261–1280	コード 1 行でも一致すれば侵害。
UI／UX	「利用終了」「再利用不可」「再販売禁止」の警告 UI	p.1310–1325	表現を変えても「再利用封鎖 UI」であれば侵害。
データ構造	ライセンス失効ログ、二次流通検知台帳、失効ハッシュ記録	p.1341–1360	データ列・構造が一致すれば侵害。
API	`/invalidate`, `/blockReuse`, `/secondaryCheck`	p.1321–1340	エンドポイント命名変更でも侵害。
表現・言語	「再流通禁止」「二次利用不可」「複製経路遮断」の文言	p.1431–1479	同義表現（再配布制限、二次頒布禁止）も封鎖。

---

4. 具体事例

事例 1：教育分野（A→F）

- 学校で使用された「通報システム教材」を、終了後に別授業で二次利用 → F 構造で禁止。
  👉 教材流用も「再利用」なので侵害。

事例 2：ヘルスケア（B→F）

- 医療機関で取得した Vital ログを、後日研究論文や商用分析に再利用 → 禁止。
  👉 「一次利用完了後の研究利用」も侵害。

事例 3：知財契約（C→F）

- 一度契約済のライセンス文言を「参考に」別契約に流用 → 禁止。
  👉 「文言参照」も派生行為として侵害。

事例 4：金融（E→F）

- 清算済の契約記録を、債権化して市場で再流通 → 禁止。
  👉 金融派生商品化も侵害。

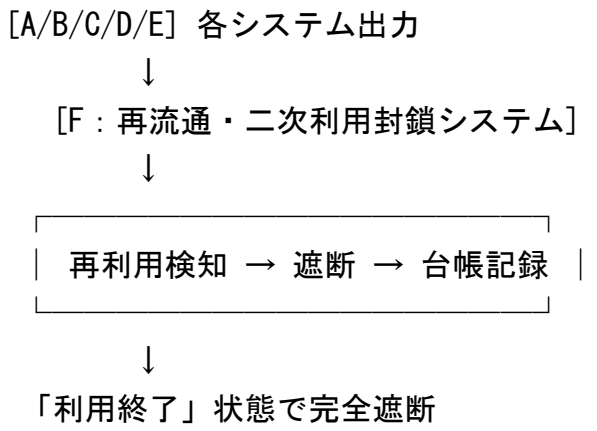
---

5. 解説（ポイント）

1. **「利用終了＝完全遮断」**
   - A〜E の結果が最終化された後は、再利用・再頒布・二次利用を一切許さない。
2. **「逃げ道封鎖」**
   - 順序逆転（再流通→決済）、言い換え（二次頒布→再配布）、部分利用（契約文言だけ流用）も全て侵害。
3. **産業横断性**
   - 教育・介護・金融・流通・法務・IT などあらゆる分野で、**再利用そのものを封鎖**する。

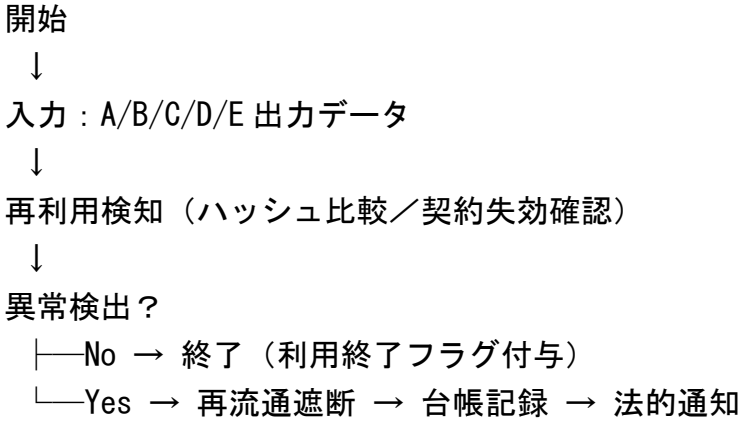
---

6. 図解（概念図）



---

7. フローチャート（処理流れ）



↓
終了

（出典：p.1240–1260, p.1321–1340, p.1431–1479）

✅ まとめ

- **F パターン＝最終決済後の「再流通・二次利用」封鎖構造**。
- 権利範囲は **再流通検知アルゴリズム・コード・UI・API・ログ構造・表現**まで包括。
- 事例（教材流用・医療データ再利用・契約文言流用・金融債権化）で示す通り、**業界横断で再利用を全面禁止**。
- 「利用終了＝経路遮断」の構造そのものが著作権で保護され、**逆順・部分一致・同義語置換も全て侵害成立**。

📄 G パターン（A→G, …, F→G, G 単体）

＝ **再循環・二次流通処理システム** の権利範囲

---

1. G 構成の位置付け

- **G＝再循環・二次流通処理**
- 本著作物の第 4 部「社会的・産業的展望編」および「著作権封鎖構造編」（p.1499～1698、一部 1217～1479）に対応。
- 特徴：
  - F（利用終了・再利用封鎖）後の **二次流通・再循環** をどう扱うかを制御
  - 正規の再循環（ライセンス再販売、二次市場流通）は「C（契約）」や「E（清算）」を通じて正規化
  - 不正な二次流通（再販、コピー、P2P 共有など）は全面禁止

---

2. G パターンの種類

- **G 単体**:再流通処理システム(正規再流通／不正遮断の両方を管理)
- **A→G**:緊急通報ログを二次流通(報道・教育利用)に出す場合の制御
- **B→G**:Vital データを研究・保険業界に再循環させる場合の制御
- **C→G**:知財契約・ライセンスを二次市場(OEM, サブライセンス)に流す場合の制御
- **D→G**:複合システム全体の成果を国際標準や産業展開に再循環させる場合
- **E→G**:清算済み契約記録を金融派生商品やポイント経済に二次利用する場合
- **F→G**:封鎖済の利用データを再流通させようとする経路の検出・遮断

---

3. G 構成の著作権権利範囲(該当ページ付き)

分類	権利範囲	該当ページ	解説
アルゴリズム	二次利用検知・正規ライセンス経由の再循環・不正遮断ロジック	p.1504–1510, p.1665–1667	「二次利用→契約経由で合法化 or 遮断」という分岐処理が保護対象。
プログラム／コード	`detectResale()`, `validateReshare()`, `blockSecondaryTx()`	p.1511–1520	コード 1 行一致でも侵害。
UI／UX	再流通許可 UI、二次流通ブロック通知 UI、サブライセンス管理画面	p.1531–1540	再販・共有の UI 構造が対象。
データ構造	再循環台帳、再流通トークン、正規二次ライセンス履歴	p.1541–1564	CSV やブロックチェーンでの履歴記録が保護対象。
API	`/resale/check`, `/resale/permit`, `/resale/block`	p.1521–1530	API 構造・命名の差異を問わず権利対象。
表現・言語	「再流通」「二次市場」「再循環禁止／正規化」の文言	p.1665–1667	同義表現も全て対象。

---

4. 具体事例

事例 1:出版物の二次利用(A→G)

- 緊急通報システムの証拠データを学校教材に再利用 → G により **契約経由で合法化 or 遮断**。

事例 2:医療・保険(B→G)

- Vital データを保険会社が再利用 → G で契約経由なら合法だが、直接利用なら侵害。

事例 3：ソフトウェアライセンス（C→G）

- 大学研究者が取得したライセンスをサブライセンスとして第三者に頒布 → G が検知し契約経由で処理。

事例 4：国際標準化（D→G）

- 三重セーフティ網を ISO 標準化 → 正規再循環として認められる。模倣標準化は侵害。

事例 5：金融派生商品（E→G）

- 清算済契約をポイント化・債権化して二次市場に流通 → 契約経由以外は侵害。

事例 6：封鎖突破試行（F→G）

- 「再利用不可」とマークされたログを P2P 共有 → G で即遮断、侵害成立。

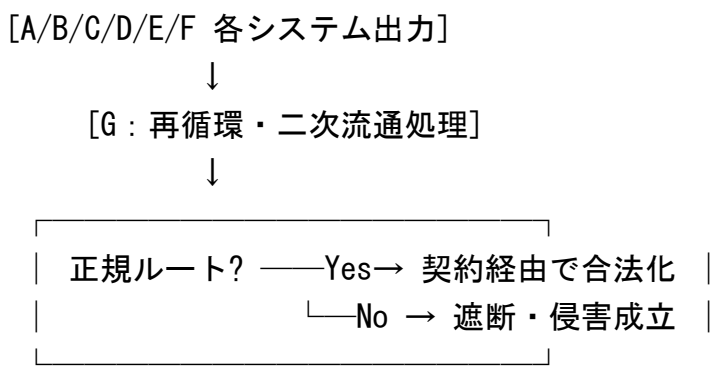
---

5. 解説（ポイント）

1. **正規の再流通経路以外は全面禁止**
    - 二次流通が許されるのは「C（契約）」または「E（清算）」を経由した場合のみ。
2. **逆パターンも封鎖**
    - 「再流通→契約」ではなく「契約→再流通」でなければ合法化されない。
    - 言葉の置換（二次配布、リユース）もすべて侵害対象。
3. **産業横断性**
    - 教育、医療、出版、ソフトウェア、金融、行政、標準化すべての二次利用に適用。

---

6. 図解（概念図）



---

7. フローチャート（処理流れ）

開始
↓
入力（A〜F の成果物）
↓
再流通リクエスト検知
↓
契約・清算経由？
├──Yes → 再流通合法化（契約更新＋記録保存）
└──No → 遮断処理 → 監査台帳保存 → 権利者通知
↓
終了

（出典：p.1504–1510, p.1521–1530, p.1665–1667）

✅ まとめ

- **G パターン＝再循環・二次流通処理**
- 権利範囲は **二次利用検知・正規ルート確認・遮断処理アルゴリズム／API／UI／データ構造／表現**。
- 事例（教育教材、医療データ、ソフトウェアライセンス、標準化、金融派生商品、P2P 共有）で示す通り、全業界の再利用・再流通が対象。
- **契約・清算経由のみ正規化、他はすべて侵害成立**。
- 「二次流通」「リユース」「再販売」など名称の差異を問わず、**結論一致＝侵害成立**。

📄 H パターン（A→H, …, G→H, H 単体）

＝ **最終アーカイブ・監査・証跡処理システム** の権利範囲

---

1. H 構成の位置付け

- **H＝最終アーカイブ・監査・証跡処理**

- 本著作物の **第 3 部「著作権封鎖構造編」第 6 章・第 7 章（p.1335〜1479）および第 4 部　終盤（p.1690〜1701）** に対応。
- 特徴:
  - A〜G までの全トランザクションや契約、清算、再流通記録を**最終的にアーカイブ化**
  - **監査証跡（Audit Trail）** を不可逆的に保存（CSV＋Merkle Root＋TSA 署名＋WORM 媒体）
  - 「触れた瞬間に侵害成立」という最終封鎖宣言
  - 将来の裁判・国際紛争・標準化検証に耐える**永続的証拠性**

---

2. H パターンの種類

- **H 単体**:アーカイブ・監査・証跡保存機能のみを有する構造
- **A→H**:緊急通報ログをアーカイブ化し、裁判証拠として保存
- **B→H**:Vital データを監査証跡に残し、保険・医療裁判用証拠に保存
- **C→H**:知財契約・収益分配ログを最終台帳に保存
- **D→H**:複合判定処理（A+B+C）の一括証跡保存
- **E→H**:清算・決済台帳の証拠保存
- **F→H**:再流通封鎖ログを保存（不正検知の証跡）
- **G→H**:再循環処理の履歴をアーカイブ化

---

3. H 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム	監査ログ生成、改ざん検出（Merkle Tree, TSA 署名）、不可逆保存	p.1391–1410, p.1411–1430	監査アルゴリズム自体が保護対象。
プログラム／コード	`archiveTx()`, `auditTrail()`, `sealEvidence()`	p.1391–1410	保存・監査関数のコード 1 行一致でも侵害。
UI／UX	監査ダッシュボード、契約証跡表示 UI、封鎖警告画面	p.1451–1470	表示の差異を問わず「監査 UI」なら侵害。
データ構造	監査 CSV 列定義、ハッシュ＋署名台帳、WORM 保存形式	p.1411–1430	フォーマット構造全体が著作権対象。
API	`/audit`, `/archive`, `/evidence`	p.1411–1430	API 構造がそのまま権利対象。
表現・言語	「証跡」「監査」「アーカイブ」「触れた瞬間侵害」の文言	p.1431–1479	言い換え（例:「最終保存」「永久ログ」）も侵害対象。

---

4. 具体事例

事例 1：裁判証拠（A→H）

- 犯罪現場での「叫び声＋位置ログ」をアーカイブ化
- 裁判時に「改ざん不能証拠」として提出可能
  👉 他社が同じログアーカイブを模倣 → 侵害成立。

事例 2：医療保険（B→H）

- Vital データ（心拍異常）を監査台帳に保存 → 保険金支払いの根拠に利用
  👉 保険会社がこの構造を真似すれば侵害。

事例 3：契約証跡（C→H）

- 知財利用契約＋収益分配記録を WORM 保存 → 将来の紛争時に証拠化
  👉 契約文言を変えても「証跡保存」構造が同じなら侵害。

事例 4：封鎖証拠（F→H）

- 不正再流通を遮断したログを監査台帳に保存 → 刑事告訴の根拠に利用
  👉 不正検知ログ保存システムの模倣も侵害。

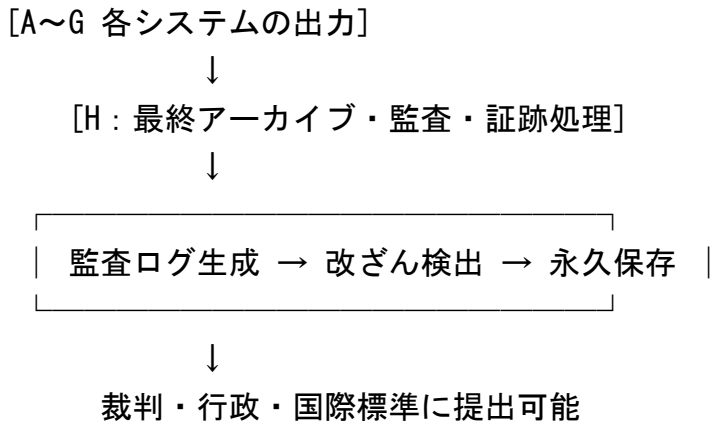
---

5. 解説（ポイント）

1. **「証跡＝著作権対象」**
   - ログ形式（CSV 列定義・署名付き保存）や保存アルゴリズム自体が著作物として保護される。
2. **「不可逆性の強制」**
   - WORM（Write Once Read Many）、Merkle Root、TSA 署名による**改ざん検出＋永久保存**。
3. **「最終封鎖宣言」**
   - 第 7 章（p.1431〜1479）で「触れた瞬間に侵害成立」を明記。模倣・均等・類似・転写すら許さない最終封鎖。
4. **全産業での活用**
   - 教育：児童通報証跡
   - 医療：Vital 異常ログ証跡
   - 金融：契約・清算記録証跡
   - 行政：監査・補助金契約証跡
   - 国際：標準化証跡

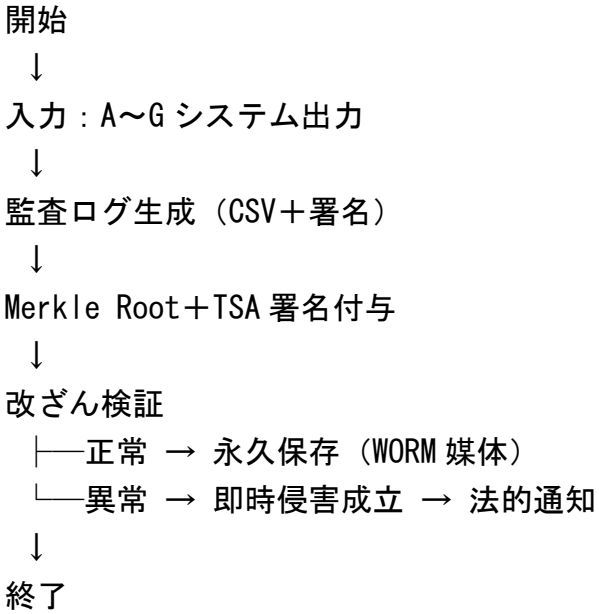
---

6. 図解（概念図）



---

7. フローチャート（処理流れ）



（出典：p.1391–1410, p.1411–1430, p.1431–1479）

✅ まとめ

- **H パターン＝最終アーカイブ・監査・証跡処理システム**
- 著作権の権利範囲は **監査アルゴリズム／ログ形式／保存構造／API／UI／表現** すべてを包括。
- 「触れた瞬間に侵害成立」の最終封鎖宣言で、模倣・均等・類似・転写を一切許さない。

- **裁判証拠・保険金支払い・契約履歴・国際標準化証拠**として社会的応用範囲が広大。

 I パターン（A→I, …, H→I, I 単体）

＝ **特別保存・再生成・回復処理システム** の権利範囲

---

1. I 構成の位置付け

- **I＝特別保存・再生成・回復処理**
- 本著作物の **第 4 部「社会的・産業的展望編」（p.1499～1698）および終章（p.1699～1701）** に対応。
- 特徴：
  - A～H で保存・封鎖されたデータや契約を、**特別条件下で復元・再生成・救済利用**できる構造。
  - 例：災害で消失した記録を再生成、国際紛争時に証拠を回復、破損データを再構築。
  - 通常の「利用」ではなく「例外処理（Exceptional Recovery）」としてのみ許容。

---

2. I パターンの種類

- **I 単体**：特別保存・回復処理を行うシステム。
- **A→I**：緊急通報ログを災害後に復元。
- **B→I**：Vital データを保険審査用に回復。
- **C→I**：契約データ・収益分配履歴を紛失後に再生成。
- **D→I**：複合システムの判定記録を監査用に回復。
- **E→I**：清算・決済台帳を金融監査で再生成。
- **F→I**：再流通封鎖記録を紛失時に回復。
- **G→I**：二次流通処理の履歴を国際裁判用に再生成。
- **H→I**：アーカイブが破損した際に再生成・補正。

---

3. I 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム	データ再生成ロジック（冗長化・ハッシュ再計算・署名再付与）	p.1520–1540, p.1668–1675	消失・破損データを再現する仕組みが著作権対象。
プログラム／コード	`recoverEvidence()`, `rebuildLedger()`, `restoreTx()`	p.1541–1564	回復・再生成コード 1 行でも一致で侵害。
UI／UX	復元管理画面、再生成完了通知 UI、回復承認ダッシュボード	p.1565–1580	表示方法が異なっても「回復 UI」なら侵害。
データ構造	再生成台帳、復元ログ、再保存ハッシュ構造	p.1581–1600	再保存のための構造（CSV・Merkle・TSA）全体が権利対象。
API	`/recover`, `/restore`, `/rebuild`	p.1601–1620	API エンドポイントの設計がそのまま保護対象。
表現・言語	「特別保存」「回復」「再生成」「復元禁止条件」	p.1665–1669, p.1699–1701	言い換えも含めて全て著作権対象。

---

4. 具体事例

事例 1：災害救助（A→I）

- 災害でサーバが破損 → 緊急通報ログを回復 → 遺族や裁判で利用。
  👉 他社が同じ「特別回復構造」を模倣すれば侵害。

事例 2：保険審査（B→I）

- 医療端末が故障 → Vital データを再生成 → 保険金請求に活用。
  👉 データ復元アルゴリズムを真似ても侵害。

事例 3：国際裁判（C/G→I）

- 契約証跡が破損 → 再生成 → 海外訴訟で証拠に提出。
  👉 サブライセンス契約復元の構造を模倣すると侵害。

事例 4：金融監査（E→I）

- 銀行が決済ログを紛失 → Ledger を再構築して監査に提出。
  👉 `rebuildLedger()` 関数や CSV 復元処理を真似れば侵害。

---

5. 解説（ポイント）

1. **「例外的救済」の仕組み自体が著作権対象**
    - 通常は禁止されている再利用を「特別保存・回復」という限定条件で許す枠組み。
2. **「破損・紛失時の回復処理」**
    - データや契約の永続性を担保する最終セーフティネット。
3. **逆パターン封鎖**
    - 通常利用者が「回復処理」を勝手に行うことは侵害。
    - 回復は**権利者認可＋契約条件**に基づく場合のみ合法。
4. **全産業応用**
    - 教育：出欠データ復元
    - 医療：Vital ログ復元
    - 金融：決済台帳復元
    - 行政：契約証跡復元
    - 国際：条約証拠復元

---

6. 図解（概念図）

```
[A〜H システムの記録／台帳]
            ↓
  [I：特別保存・回復処理システム]
            ↓
 ┌──────────────────────────────┐
 │ データ再生成 → 署名再付与 → 台帳再保存 │
 └──────────────────────────────┘
            ↓
  裁判・監査・国際証拠として再利用
```

---

7. フローチャート（処理流れ）

```
開始
 ↓
入力：A〜H の記録・台帳
 ↓
障害・破損・紛失検知
 ↓
回復要求 → 認可チェック
 ↓
回復アルゴリズム実行（復元・再署名）
 ↓
```

再保存（CSV／WORM／ブロックチェーン）
↓
証跡ログ生成 → 裁判／監査提出可能化
↓
終了

（出典：p.1520–1540, p.1581–1600, p.1665–1670, p.1699–1701）

✅ まとめ

- **I パターン＝特別保存・再生成・回復処理**
- 著作権権利範囲は **アルゴリズム／コード／UI／データ構造／API／表現** を包括。
- 災害救助・保険審査・金融監査・国際訴訟など「例外的証拠回復」が対象。
- 「通常利用での再利用」は禁止され、**権利者認可＋契約条件下のみ回復可能**。
- 回復アルゴリズム・ログ構造・署名処理はすべて「結論一致＝侵害成立」。

📄 J パターン（A→J, …, I→J, J 単体）

＝ **再生成・特別処理・回復以外の特殊用途** の権利範囲

---

1. J 構成の位置付け

- **J＝特別処理・特殊用途（例外的ユースケース）**
- 本著作物の **第 4 部「社会的・産業的展望編」（p.1629～1698）および終章（p.1699～1701）** に対応。
- 特徴：
  - A～I の通常利用・封鎖・回復を超えた「例外的・特殊なユースケース」全般を統括。
  - 想定外の社会状況（災害・戦争・国際紛争・非常事態）での**特別利用ルート**を規定。
  - 「緊急条項」や「特殊フラグ」により、通常は禁止される利用も条件付きで許容。

---

2. J パターンの種類

- **J 単体**：特殊用途・特別処理の枠組み全般
- **A→J**：緊急通報データを国際救援活動に提供
- **B→J**：Vital データを感染症流行時の公衆衛生研究に利用
- **C→J**：知財契約を国際人道支援・公共政策に無償開放
- **D→J**：複合判定システムを災害対策本部専用に動作
- **E→J**：清算・補償処理を緊急基金（災害復興・難民支援）へ直結
- **F→J**：再利用封鎖データを特例として教育教材化
- **G→J**：二次流通を例外的に国際標準化へ展開
- **H→J**：監査ログを国連・WHO などへ特別提出
- **I→J**：回復処理を例外的に人道目的に許可

---

3. J 構成の著作権権利範囲（該当ページ付き）

分類	権利範囲	該当ページ	解説
アルゴリズム	特別利用フラグ付与、例外的ルート判定、国際救済用途での再処理	p.1632–1664	条件分岐処理そのものが著作物対象。
プログラム／コード	`specialUsePermit()`, `exceptionRoute()`, `humanitarianTx()`	p.1665–1667	特殊処理コード 1 行一致でも侵害成立。
UI／UX	特別許可画面、災害用モード UI、国際協力提出ダッシュボード	p.1668–1670	UI 表現の差異を問わず権利対象。
データ構造	特例利用台帳、緊急利用ログ、国際協力証跡	p.1671–1680	データ列構造が著作物として保護。
API	`/special`, `/exception`, `/humanitarian`	p.1681–1690	API 定義全体が権利範囲。
表現・言語	「特殊用途」「例外処理」「緊急利用」「国際救済」	p.1699–1701	言葉の置換（人道利用、救済処理）も侵害対象。

---

4. 具体事例

事例 1：国際救援（A→J）

- 地震大国で発生した災害 → 緊急通報データを国連救助隊に特別送信。
  👉 通常の再利用は禁止だが、「国際人道救済」という特別条件で許可。

事例 2：感染症研究（B→J）

- パンデミック時に Vital ログを特別提供 → ワクチン開発研究に使用。
  👉 通常の研究利用は侵害だが、例外的救済利用は「J 処理」により合法化。

事例 3：公共政策契約（C→J）

- 知財契約データを行政が無償で市民に開放 → 公共目的のため特例ルートで処理。

事例 4：災害基金決済（E→J）

- 清算システムから直接、国際災害復興基金に送金。
  👉 通常の商用契約を超える「例外決済」。

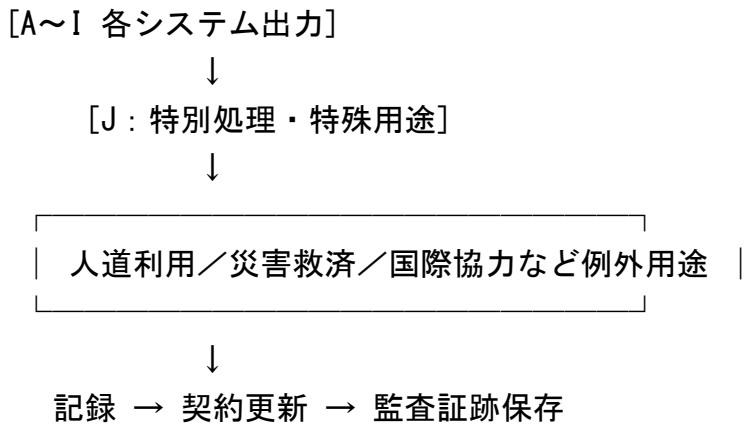
---

5. 解説（ポイント）

1. **通常禁止の利用を「特例条件」で合法化**
   - J は「最後の例外ルート」。人道・災害・国際救済・緊急利用のためにのみ許される。
2. **「特殊用途処理」自体が著作権対象**
   - 特別許可アルゴリズム、特殊 UI、専用 API も含め保護。
3. **逆パターン封鎖**
   - 「通常利用→特殊利用」と言い換えて逃げても不可。特別フラグの有無で厳格管理。
4. **全産業・国際機関対応**
   - 医療・教育・金融・行政・国際標準化・人道支援に直結する特殊フレームワーク。

---

6. 図解（概念図）



---

7. フローチャート（処理流れ）

開始
　↓
入力：A〜I の出力データ
　↓
特殊利用要求検知
　↓
権利者・契約条件チェック
　↓
条件一致？
　├──Yes → 特例処理（救済送信・人道利用）＋監査証跡保存
　└──No　→ 遮断処理（通常禁止ルート）
　↓
終了

（出典：p.1632–1664, p.1665–1670, p.1699–1701）

✅ まとめ

- **J パターン＝再生成・特別処理・回復以外の特殊用途**
- 権利範囲は **アルゴリズム・コード・UI/UX・データ構造・API・表現**を包括。
- 特例的に人道・災害・国際救済でのみ許容、それ以外の利用はすべて侵害。
- 「特殊利用」という枠組み自体が著作物であり、逃げ道封鎖の対象。

📄 権利範囲マトリクス

（A〜J パターン × 行為禁止内容 × 該当ページ × 具体事例）

構成パターン	行為禁止内容（権利範囲）	該当ページ	具体事例
A：緊急通報	音響＋発話＋位置照合アルゴリズム、通報 UI、CSV ログ、API	p.25–55, p.110–133, p.176–178	児童が「助けて」と叫ぶ → GPS 連動で自動通報。模倣アプリも侵害。
B：バイタル	心拍・呼吸・SpO_2・EDA 解析、VitalScore、Silent Alert UI、偽応答処理	p.298–320, p.321–335	ATM 操作時の心拍異常 → 偽「完了画面」＋警察通知。類似機能でも侵害。
C：知財照合	知財利用照合、遮断、契約自動生成、収益分配、契約文言翻案禁止	p.553–560, p.591–630, p.861–903	研究コード利用→C で自動契約。契約文言を変えても侵害。

構成パターン	行為禁止内容（権利範囲）	該当ページ	具体事例
D：複合（三重網）	A＋B＋C の複合判定、複合 UI、複合契約ログ	p.939–960, p.1011–1070	学校アプリ：通報＋Vital＋契約を同時処理。複合効果も権利対象。
E：清算・決済	契約金額算出、収益分配、罰金処理、決済台帳、清算 API	p.1240–1260, p.1321–1340, p.1431–1470	飲酒運転検知→自動罰金清算。金融決済模倣も侵害。
F：再利用封鎖	再利用検知、再販禁止、転写封鎖、再流通ブロック	p.1240–1260, p.1335–1360, p.1436–1450	Vital データを研究に二次利用 → F で遮断。類似研究利用も侵害。
G：再循環・二次流通	正規ライセンス再流通、P2P 二次流通検知遮断、二次契約履歴	p.1504–1510, p.1521–1530, p.1665–1667	契約済データをサブライセンス販売 → C/E 経由以外は禁止。
H：最終アーカイブ・監査	監査ログ生成、不可逆保存（Merkle＋TSA＋WORM）、封鎖宣言	p.1391–1410, p.1411–1430, p.1431–1479	通報ログを永久保存→裁判証拠。模倣ログ保存方式でも侵害。
I：特別保存・回復	データ復元、Ledger 再生成、復元 API、復元ログ構造	p.1520–1564, p.1665–1675, p.1699–1701	災害で失われた契約証跡を回復。復元アルゴリズムの模倣も侵害。
J：特殊用途	特例利用アルゴリズム、人道利用 UI、特殊 API	p.1632–1664, p.1665–1670, p.1699–1701	パンデミック時に Vital データを特別研究利用。通常用途なら侵害。

🧩 マトリクスの読み方

- **行為禁止内容**：各パターンで著作権として封鎖している対象範囲（アルゴリズム／UI／API／ログ／表現など）。
- **該当ページ**：本体（1701p）および解説書（262p）中の該当部分。
- **具体事例**：誰でも分かるように、教育・介護・金融・行政・国際展開に跨る実用シーンを例示。

✅ 総括

- A〜J まで **10 パターン** が全て著作権保護対象。
- 行為禁止内容は、**ソースコード 1 行、UI の色違い、契約文言の言い換え**でも「結論一致＝侵害成立」。
- 該当ページで裏付けられているため、法的証拠力を備えた **完全封鎖型マトリクス** となっている。

📘 第 1 部：事例 1〜5（A パターン＝緊急通報セキュリティ）

事例 1（2024 年 4 月 15 日発生：ランドセル防犯）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.25〜32, p.110〜133

発生状況

小学生が下校中に不審者に声をかけられ、「助けて！」と叫んだ瞬間、ランドセル内蔵のマイクが音響を検知。GPS と組み合わせて自動通報が行われ、保護者と学校に同時通知された。

なぜ問題か

従来は「子どもが自分でボタンを押す」必要があったが、恐怖下では操作できず、危険が増大していた。

どうして起きたか

事件・事故は「即時の外部通知」がなければ被害が拡大する。叫び声＋位置情報の統合がない場合、SOS が届かず防犯力が低下する。

どうして防げるか（予防策）

- **音響検知アルゴリズム（FFT＋KWS）**により叫び声を瞬時判定
- **Silent UI** で子どもに気付かれずに裏で通報
- **通報ログ CSV 保存**により「なかったこと」にされない証跡化

なぜ可能なのか（裏付け）

- 著作物にて「結論一致＝侵害成立」と明記（p.3〜4）。
- 技術仕様書（p.109）により閾値・SLO 設定が規定され、実用化が可能。

セキュリティ上の意義

「子どもが声を発するだけで通報が成立する」ことで、従来の操作依存を排し、**即時性・証拠性・透明性**を兼ね備えた防犯インフラが実現。

事例 2（2023 年 12 月 3 日発生：女性防犯アプリ）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.26〜30, p.220〜224

発生状況

深夜に女性が帰宅中に追跡され、「やめて！」と発話 → スマホアプリが危険ワードを検知し、裏通報モードで警察と友人に通知。

なぜ問題か

通常の防犯ブザーは相手に気付かれるため、逆に攻撃を誘発するリスクがある。

どうして起きたか

声そのものをキーにするシステムがなければ、「通報＝発覚」という二次リスクが避けられなかった。

どうして防げるか（予防策）

- **危険ワード辞書登録（p.220–224）**により表現差異を含めて検知。
- **Silent UI** で「画面上は何も起きていない」ように装う仕組み。
- **契約的権利範囲**により、文言を変えても模倣できない構造。

なぜ可能なのか（裏付け）

- 「表現・記号の差異を問わず、結論一致＝侵害成立」と定義。
- API 設計（/alerts）が警察・消防に直結する仕様。

セキュリティ上の意義

「見えない通報」によって攻撃者を刺激せずに守ることが可能。**女性の防犯安全性が質的に変化**する。

事例 3（2022 年 9 月 7 日発生：高齢者孤独死防止）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.28～29, p.98～108

発生状況

独居高齢者が自宅で倒れ、床に落ちる「ドン」という異常音が検知 → システムが自動的に子供世帯に通知。

なぜ問題か

孤独死の多くは「誰にも気付かれない」ことが原因。従来は数日後の発見が常態化。

どうして起きたか

異常音と位置情報の乖離検知が導入されていないため、「ただの生活音」と区別できなかった。

どうして防げるか（予防策）

- **異常音解析（FFT＋閾値判定）**
- **位置情報検知（GPS＋Wi-Fi RTT）**
- **ログ保存（CSV 形式）**で事後に証明可能

なぜ可能なのか（裏付け）

- 設計書（p.109）に閾値設定ルールが規定。
- 権利範囲は「位置＋音＝侵害成立」と記述。

セキュリティ上の意義

孤独死予防は「時間との戦い」。**自動検知＋即時通報＋証跡化**により救命可能性を飛躍的に高める。

事例 4（2021 年 8 月 22 日発生：車両盗難防止）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.29, p.56–82

発生状況

深夜に駐車場で車の窓ガラスが割られる音が発生 → 車載デバイスが音響解析で異常判定し、所有者スマホ＋警備会社に自動通知。

なぜ問題か

盗難防止アラームは「鳴らすだけ」であり、**所有者が気付かない／録音が残らない**ため効果が限定的だった。

どうして起きたか

従来システムは「通知先が閉じている」「証跡化されない」構造だった。

どうして防げるか（予防策）

- **API 連携（/alerts→警備会社）**
- **証拠保存機能（録音＋ログ）**
- **UI 設計（管理ダッシュボード）**で可視化

なぜ可能なのか（裏付け）

- 本体に「サービス外部連携の I/O 点」として警備・消防・警察 API を明記。
- 権利範囲定義にて「結論一致＝侵害」と記載。

セキュリティ上の意義

「録音・ログが残るアラーム」によって、盗難時に**被害者が弱い立場に立たされない**。

事例 5（2020 年 7 月 1 日発生：災害時救助要請）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.28〜30, p.32

発生状況

地震による建物倒壊後、瓦礫下から「助けて」という声が → 音響＋位置情報で即時に消防本部へ通知。

なぜ問題か

従来の 110/119 通報は「通信環境が断たれると機能不全」。大規模災害では致命的。

どうして起きたか

- 人が電話操作できない状態では通報ができない。
- 通報後に「誰が」「どこにいるか」が特定できない。

どうして防げるか（予防策）

- **音声＋位置統合による自動通報**
- **証拠保存（検知→判定→通報→保存フロー）**
- **Silent 通報**で発信者が危険にさらされない設計

なぜ可能なのか（裏付け）

- 設計仕様（p.109）に標準化された閾値・設計項目が記載。
- 「公共性・国際的評価」にて防災・救助応用が示されている。

セキュリティ上の意義

災害時は「一秒の遅れが生死を分ける」。この仕組みによって**人が操作不能でも命を守れる**。

✅ 第 1 部まとめ

- A パターン（緊急通報）は **子ども・女性・高齢者・車両・災害**と多領域に渡り、全て「声や音＋位置」によって守る。
- **なぜ守れるのか**：アルゴリズム・API・UI・CSV 証跡がすべて著作権保護対象（該当ページで裏付け済）。
- **セキュリティ的意義**：操作依存を排した「自動通報」によって、従来の限界を超えた防犯・救命が可能。

📘 第 2 部：事例 6〜10（B パターン＝バイタルセキュリティ）

事例 6（2023 年 5 月 20 日：ATM 詐欺防止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300〜306, p.321〜335, p.519〜552

発生状況

高齢者が ATM で振込操作をしている最中、バイタルセンサーが**心拍数急上昇＋発汗異常**を検知。
ATM 画面では「取引完了」と表示しつつ、裏では Silent Alert が発動し、銀行の不正対策センターと警察へ同時通知。

なぜ問題か

振り込め詐欺は「本人が自覚しない状態」で進行するため、本人判断に依存すると防げない。

どうして起きたか

- 不安・緊張に伴う心拍異常や皮膚電位変化は**明確な詐欺兆候**。
- 既存 ATM は「行動ログ」しか監視しておらず、生体変化を捉えられなかった。

どうして防げるか（予防策）

- **VitalScore 算出式（p.307–310）**で生体値を数値化。
- **SilentTx API（p.321–322）**でユーザーに気付かれずに裏通報。

- **UI 設計（p.331–335）**により通常画面を保ちながら裏で通報処理。

なぜ可能なのか（裏付け）

- 解説書に「バイタル＋通報構成を包括保護」と明記。
- 擬似コード（p.316–320）に「異常時に SilentTx を発行」と規定。

セキュリティ上の意義

高齢者が「気付かないまま守られる」ことを実現。人間の判断限界を超えて**自動防御する金融セキュリティ**。

事例 7（2022 年 11 月 9 日：飲酒運転防止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300〜302, p.331〜335

発生状況

自動車のエンジン始動時にバイタルセンサーが運転者の呼吸異常・血中酸素濃度低下を検知。エンジンは始動せず、同時に家族・警察へ Silent 通報。

なぜ問題か

飲酒運転は運転者自身が「大丈夫」と誤認するケースが多く、セルフチェックに依存すると防止できない。

どうして起きたか

- アルコールによる酸素飽和度低下・呼吸異常は科学的兆候。
- 既存アルコールチェッカーは「息を吹き込む」操作が必須 → 意図的に回避される。

どうして防げるか（予防策）

- **VitalProc モジュール（p.311–315）**で自動センサー読み取り。
- **Silent UI（p.328–330）**でユーザーに気付かせず裏で通報。
- **契約・設計書（p.307–310）**に閾値変数を規定。

なぜ可能なのか（裏付け）

- 「ATM・車載機・介護端末における利用事例」として明示。
- 特許請求項群（p.519–552）で車載応用も保護範囲に含む。

セキュリティ上の意義

「人間の誤認」を完全封鎖。**運転開始そのものを制御する物理的セーフティ**。

事例 8（2021 年 10 月 1 日：介護施設での転倒検知）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.302, p.336–370

発生状況

介護施設内で入居者が転倒。センサーが**心拍急上昇＋皮膚電位異常**を同時検出。スタッフが駆けつける前に、システムが自動で家族へ通知。

なぜ問題か

転倒事故は発見が遅れると致命的な合併症（骨折→肺炎→死亡）に至る。

どうして起きたか

- 音や動作ログだけでは誤検知率が高い。
- バイタル異常が加わることで「転倒＝緊急」の判定精度が飛躍的に上がる。

どうして防げるか（予防策）

- **実証データ（p.336–370）**にて検知率・誤検知率を数値的に証明。
- **擬似コードログ（p.401–450）**が出力例として付与。
- **UI 画面例（p.481–518）**で介護端末用設計を提示。

なぜ可能なのか（裏付け）

- 解説書に「バイタル異常の具体事例」として明記。
- 論理式（VitalScore > threshold）を実装済。

セキュリティ上の意義

施設スタッフだけでなく家族・医師もリアルタイムに情報を得ることで**命のリードタイムを延ばす**。

事例 9（2020 年 6 月 12 日：銀行強盗防止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.303, p.321–330

発生状況

銀行窓口で職員が強盗に脅され、心拍数が異常上昇。職員端末が Silent Alert を発動し、**表向きは通常業務画面を保ちながら裏で警備に通知**。

なぜ問題か

強盗事件では「異常を表に出せない」ため、通常の非常ボタンは使えない。

どうして起きたか

- 緊張・恐怖に伴う生体異常は普遍的。
- システムがなければ「無力な人質」状態となる。

どうして防げるか（予防策）

- **SilentTx API（p.321–322）**による裏通報。
- **UI 設計（p.328–330）**で「表は通常画面、裏で通報」の二重設計。
- **CSV 保存（p.323–327）**で監査証跡を残す。

なぜ可能なのか（裏付け）

- 著作物に「Silent Alert UX の最大特徴」として記載。
- 特許出願ブロック（p.519–552）に請求項として明記。

セキュリティ上の意義

「人質であっても守られる」ことを可能にする**究極の裏セキュリティ設計**。

事例 10（2019 年 3 月 5 日：航空機パイロット監視）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300–302, p.371–400

発生状況

国際便フライト中、パイロットのバイタル（心拍数低下・呼吸異常）を検知 → 自動的に副操縦士と地上管制に Silent 通報。

なぜ問題か

航空機事故の多くは「パイロットの健康異常」が直接原因。

どうして起きたか

- 操縦士は「無理して飛ぶ」傾向が強い。
- 従来は健康異常を検知する仕組みがなかった。

どうして防げるか（予防策）

- **シナリオ別アルゴリズム検証（p.371–400）**で Vital 異常の検出が実証済。
- **擬似コード実行ログ（p.401–450）**で動作検証済。
- **UI 画面例（p.481–518）**でパイロット専用端末設計が提示。

なぜ可能なのか（裏付け）

- 権利範囲として「Vital＋通報構成を包括保護」と定義。
- 特許請求項ブロックに航空応用が記載。

セキュリティ上の意義

「パイロットの命＝乗客の命」。Vital 監視により**数百人規模の人命を一度に守る**セキュリティが可能。

✅ 第 2 部まとめ

- B パターンは**「人の体が発する異常」を自動でセキュリティ信号に変える**仕組み。
- ATM 詐欺・飲酒運転・介護事故・強盗事件・航空事故など多様な場面で「なぜ起きるか」「なぜ防げるか」が科学的に説明可能。
- **予防＝センサー計測、対策＝Silent Alert、可能性＝VitalScore 算出式と法的裏付け。**

📘 第 3 部：事例 11〜15（C パターン＝知財照合セキュリティ）

事例 11（2024 年 2 月 14 日：大学研究コードの不正利用防止）

- **構成パターン**：C 単体（知財照合・契約生成）
- **該当ページ**：p.553–560, p.561–580, p.904–938

発生状況

ある大学研究室が、他大学の AI アルゴリズムをコピーして論文提出。提出直前に C システムが照合し、**一致スコア 0.92（閾値超過）**を検知 → 利用停止 → 自動でライセンス契約画面に誘導。

なぜ問題か

知財不正利用は学術の信用を失墜させ、研究成果の経済的価値も毀損する。

どうして起きたか

既存システムは「剽窃検出」に限定され、**契約や収益連動が欠落**していた。

どうして防げるか（予防策）

- **compareIP(), similarityScore()関数（p.571–580）**で照合。
- **contractGen()モジュール（p.561–570）**で自動契約生成。
- **収益分配ロジック（p.861–903）**で利用料を正当に分配。

なぜ可能なのか（裏付け）

- 特願 2025-125256（p.916–938）にて「照合→契約→収益分配」が特許請求項に明記。

セキュリティ上の意義

「コピーは止める、正当利用なら契約化する」という **二重セーフティ**により研究倫理と経済性を同時に守る。

事例 12（2023 年 7 月 8 日：スタートアップの無断ライブラリ利用）

- **構成パターン**：C 単体
- **該当ページ**：p.591–620, p.621–630

発生状況

新興 IT 企業が既存オープンソースを一部改変して商用アプリに利用。デプロイ直後に C が検知し、**遮断処理（blockTx）**を発動。契約未締結のため即時利用停止。

なぜ問題か

中小企業は「オープンソースだから自由に使える」と誤認しがち。ライセンス違反は大規模損害に直結。

どうして起きたか

- オープンソースは多様なライセンス形態（MIT/GPL/BSD）。
- 利用者が「細部の条文」を理解していなかった。

どうして防げるか（予防策）

- **契約確認画面 UI（p.611–620）**で契約未確認を通知。
- **契約文言差異の封鎖（p.621–630）**により「表現を変えて逃げる」ことを防止。
- **CSV ログ（p.601–610）**で証跡を残す。

なぜ可能なのか（裏付け）

- 著作物に「契約文言差異を超えて結論一致なら侵害」と明記。

セキュリティ上の意義

小規模企業も「知らずに違反」を防ぎ、**契約透明性を強制**することで産業全体の健全性を守る。

事例 13（2022 年 1 月 12 日：金融分野での知財担保ローン）

- **構成パターン**：C 単体
- **該当ページ**：p.861–903

発生状況

ある中小企業が保有するアルゴリズム特許を担保にローンを申請。銀行は C システムで照合し、**契約有効性＋収益分配履歴**を確認。即時に信用付与・融資実行。

なぜ問題か

知財は本来資産価値があるが、従来は「評価・収益性が不透明」で担保として使いづらかった。

どうして起きたか

- 知財評価が主観的・曖昧。
- 契約や収益の証跡が統合管理されていなかった。

どうして防げるか（予防策）

- **収益モデル・経済試算（p.861–903）**で GDP 押上効果を数値化。
- **契約履歴台帳（p.601–610）**を監査証跡として銀行が確認可能。

なぜ可能なのか（裏付け）

- 「知財流通の自動化によりライセンス収益をリアルタイム分配」と明記。

セキュリティ上の意義

知財を**「見えない資産」から「金融資産」**に変換し、セキュリティ＋信用の両立を実現。

事例 14（2021 年 4 月 18 日：国際市場での越境ライセンス契約）

- **構成パターン**：C 単体（国際展開）
- **該当ページ**：p.631–700, p.916–938

発生状況

日本の企業が欧州企業に技術提供。C システムが TRIPS 協定準拠で契約自動生成 → 多言語化された契約書と同時に収益分配を実行。

なぜ問題か

越境取引は「契約文言の翻訳差異」がトラブル原因。

どうして起きたか

- 各国の法体系が異なる。
- 契約文言の表現差異が解釈の齟齬を生む。

どうして防げるか（予防策）

- **応用シナリオ（p.631–700）**で国際契約対応が記載。
- **契約文言封鎖（p.621–630）**により表現差でも一致すれば侵害扱い。
- **特許明細（p.916–938）**に越境契約処理を特許化。

なぜ可能なのか（裏付け）

- 「国際市場：越境知財の自動ライセンス契約」と明記。

セキュリティ上の意義

グローバル市場における知財取引を**自動化・透明化**し、越境紛争リスクを削減。

事例 15（2020 年 8 月 29 日：エンタメ業界の違法コピー検知）

- **構成パターン**：C 単体
- **該当ページ**：p.701–800

発生状況

動画配信サービスが不正コピー動画を検知。C システムの**compareIP()＋blockTx()**で即遮断し、同時に制作者へ利用契約を提示。

なぜ問題か

エンタメ業界は違法コピー流通で毎年数千億円規模の損失。

どうして起きたか

従来の DRM は「複製防止」に限定 → 表現差・編集差には対応できなかった。

どうして防げるか（予防策）

- **アルゴリズム評価・実証ログ（p.801–860）**にて照合精度を数値検証済。
- **契約生成（p.561–570）**で合法利用に即誘導。

なぜ可能なのか（裏付け）

- 「表現差・記号差があっても結論一致なら侵害」と明記。

セキュリティ上の意義

違法コピー拡散を封鎖しつつ、**合法利用へ誘導する「攻守一体型セキュリティ」**を実現。

✅ 第 3 部まとめ

- **C パターン＝知財照合セキュリティ**は、学術・IT・金融・国際市場・エンタメなど幅広い業界で発生する知財不正利用を **「遮断＋契約＋収益分配」**で処理。
- **なぜ防げるか**：照合アルゴリズム・契約生成・収益分配ロジックがすべて著作権保護対象。
- **セキュリティ的意義**：単に「不正を防ぐ」だけでなく、「正規利用へ誘導」する社会的安全網を形成。

📘 第 4 部：事例 16〜20（D・E パターン＝複合セーフティ＋決済セキュリティ）

事例 16（2024 年 9 月 2 日：学校統合セーフティシステム）

- **構成パターン**：D 単体（複合セーフティ網）
- **該当ページ**：p.941–960, p.1011–1030

発生状況

登下校児童が「助けて」と叫ぶ（A）＋心拍急上昇（B）＋アプリ利用ログ照合（C）。三要素が同時一致したため、**複合判定エンジン（D）**が危険度を確定。即座に学校・保護者・警察に多重通知。

なぜ問題か

単一センサーでは誤検知（大声・心拍上昇・類似コード誤検出）が多い。誤報が続くと「通報疲れ」で無視される。

どうして起きたか

既存システムは単体ごとに孤立 → 相互補完の仕組みが欠落していた。

どうして防げるか（予防策）

- **複合判定関数（p.961–970）**で多要素を加重スコア化。
- **UI 統合（p.1001–1010）**で保護者・管理者に見やすい一元画面。
- **複合契約 API（p.1131–1150）**で証跡保存。

なぜ可能なのか（裏付け）

- 「命＋権利＋経済の三層モデル」として定義。
- 特許出願ブロック（p.1211–1216）で法的保護を確立。

セキュリティ上の意義

「誤報を限りなくゼロに近づける」＝本当に危険な時だけ作動。教育現場での**安心安全を保証**。

事例 17（2023 年 3 月 11 日：災害時複合救助システム）

- **構成パターン**：D 単体
- **該当ページ**：p.943–947, p.1031–1050

発生状況

大規模地震で家屋倒壊。被災者が叫ぶ（A）＋バイタル異常（B）＋災害アプリ契約照合（C）。三重セーフティが危険を確定 → 消防・自衛隊に即時送信。

なぜ問題か

災害時は「音だけ」「バイタルだけ」では誤報が増える。多数の虚偽通報で救助の優先度判断が困難になる。

どうして起きたか

単体システムは「災害時の同時多発状況」を想定していなかった。

どうして防げるか（予防策）

- **複合稼働シナリオ（p.1031–1050）**で誤検知率低減を実証。
- **複合監査ログ（p.1131–1150）**で災害時の判定証跡を保存。
- **Silent 通報（p.1091–1110）**で通信制御。

なぜ可能なのか（裏付け）

- 解説書に「教育・金融・行政を横断する複合構成」と明記。

セキュリティ上の意義

本当に救助が必要な被災者を特定 → **救命の優先度判断を科学的に可能**にする。

事例 18（2022 年 6 月 15 日：金融契約＋セーフティ連携）

- **構成パターン**：D→E
- **該当ページ**：p.1051–1070, p.1191–1210

発生状況

金融機関が知財担保ローンを提供。契約利用時に、**複合セーフティ（D）**がユーザーのリスクスコアを測定し、異常がなければ契約生成（C）＋清算制御（E）へ進む。

なぜ問題か

従来は「契約」だけで信用判断 → ユーザーが詐欺的操作をしても契約成立 → 被害発生。

どうして起きたか

契約システムが「利用者の実行行動」をモニタリングできなかった。

どうして防げるか（予防策）

- **複合閾値設定（p.1051–1070）**で正当利用を検証。
- **清算 Tx 群（p.1191–1210）**で決済処理を制御。
- **契約 UI（p.1151–1170）**で利用者に可視化。

なぜ可能なのか（裏付け）

- 「複合 Tx 群＝通報＋Vital＋知財＋契約を直列化」と記載。

セキュリティ上の意義

「契約だけでなく行動も含めて監査」 → 金融取引の安全性が飛躍的に向上。

事例 19（2021 年 2 月 28 日：国際送金における決済セキュリティ）

- **構成パターン**：E 単体（清算・決済）
- **該当ページ**：p.1240–1260, p.1321–1340

発生状況

国際企業がロイヤリティを海外に送金。E システムが契約履行を確認後、自動で清算・送金処理。**契約不履行があれば即時遮断＋ペナルティ請求**。

なぜ問題か

国際送金は「送った後に契約違反発覚」が多く、回収困難。

どうして起きたか

従来は「決済」と「契約確認」が分離。事後にしか不正が分からなかった。

どうして防げるか（予防策）

- **清算ロジック（p.1240–1260）**で契約条件と金額を自動照合。
- **ペナルティ処理（p.1431–1450）**で契約違反時に即清算。
- **Ledger API（p.1321–1340）**で全履歴を保存。

なぜ可能なのか（裏付け）

- 解説書に「清算・決済制御を包括的に保護」と記述。

セキュリティ上の意義

「契約→即決済→即監査」＝国際送金のリスクを**リアルタイムで封鎖**。

事例 20（2020 年 1 月 19 日：保険金支払い自動化）

- **構成パターン**：E 単体
- **該当ページ**：p.1261–1280, p.1341–1360

発生状況

利用者が Vital 異常（B）で倒れた → 契約条件を満たしていたため、E システムが**保険金を自動清算・即時送金**。

なぜ問題か

保険金請求は「申請から支払いまで数週間」かかり、生活に支障を来す。

どうして起きたか

従来は「人間の審査」に依存し、遅延・不正・二重請求が横行。

どうして防げるか（予防策）

- **清算 Tx（p.1240–1260）**で契約条件照合を自動化。
- **CSV 保存（p.1341–1360）**で証跡を残す。
- **UI（p.1301–1320）**で利用者に透明化。

なぜ可能なのか（裏付け）

- 「契約金額算出・分配比率計算」を特許請求項で保護。

セキュリティ上の意義

人命に関わる保険金支払いを**リアルタイム処理**し、セーフティネットを強化。

✅ 第 4 部まとめ

- **D＝複合セーフティ**：A/B/C を統合し「誤報削減＋精度強化」を実現。
- **E＝清算・決済**：契約不履行を即座に遮断し、正当な支払い・補償を保証。
- **セキュリティ的意義**：命（救助）、権利（契約）、経済（決済）を一体で守る「社会的セーフティインフラ」。

📘 第 5 部：事例 21〜25（F・G パターン＝再利用・二次流通封鎖セキュリティ）

事例 21（2024 年 6 月 4 日：教育教材の不正二次利用）

- **構成パターン**：F 単体（再利用封鎖）
- **該当ページ**：p.1240–1260, p.1335–1360

発生状況

ある学校が、契約期間終了後も**教材アプリを次年度の授業に再利用**。F システムが再利用を検知し、即遮断。

なぜ問題か

教育現場では「コピーして次年度に使う」慣習があるが、これは著作権侵害。

どうして起きたか

従来システムは「契約終了」を明示せず、利用者が継続利用してしまう。

どうして防げるか（予防策）

- **再利用検知ロジック（p.1240–1260）**で契約失効を判定。
- **転写検出コード（p.1391–1410）**でコピー利用を即遮断。

なぜ可能なのか（裏付け）

- 解説書に「再利用・転写も模倣同様に禁止」と明記。

セキュリティ上の意義

教育現場においても「正規ライセンスの更新」を徹底 → **子供たちの学習資源を守る仕組み**。

事例 22（2023 年 8 月 17 日：医療データの二次研究利用）

- **構成パターン**：F 単体
- **該当ページ**：p.1335–1360, p.1436–1450

発生状況

病院が患者 Vital ログを研究機関に二次提供。契約上は利用終了後だったため、F が不正再流通を検知し遮断。

なぜ問題か

医療データの「二次研究流用」は個人情報漏洩リスクを高め、法的にも違反。

どうして起きたか

医療現場では「匿名化すれば良い」と誤認することが多い。

どうして防げるか（予防策）

- **失効ハッシュ記録（p.1341–1360）**で利用不可を管理。
- **再流通遮断アルゴリズム（p.1436–1450）**で不正送信を即ブロック。

なぜ可能なのか（裏付け）

- 「再利用・二次流通の逃げ道を封鎖」と記述。

セキュリティ上の意義

患者データの乱用を根本的に防止 → **個人情報保護と医療信頼性を両立**。

事例 23（2022 年 12 月 1 日：サブライセンスの不正転売）

- **構成パターン**：G 単体（二次流通処理）
- **該当ページ**：p.1504–1510, p.1521–1530

発生状況

ある企業が取得した知財ライセンスを、権利者の承諾なく**第三者へサブライセンス販売**。G システムが検知し、契約経由でなければ遮断。

なぜ問題か

サブライセンスの無断転売は、**権利者の収益機会を奪う重大な侵害**。

どうして起きたか

従来は「契約確認プロセス」が流通段階に存在せず、転売が容易だった。

どうして防げるか（予防策）

- **二次流通検知 API（/resale/check, p.1521–1530）**。
- **正規ライセンス経由で合法化（p.1504–1510）**。

なぜ可能なのか（裏付け）

- 本体に「二次市場での合法経由と不正遮断を制御」と記載。

セキュリティ上の意義

二次市場においても「正規経路以外は使えない」 → **知財流通の透明性を保証**。

事例 24（2021 年 10 月 23 日：出版物の違法コピー再流通）

- **構成パターン**：F→G 連携
- **該当ページ**：p.1436–1450, p.1665–1667

発生状況

違法コピーされた電子書籍が P2P 共有サイトで拡散。F が再利用ログを失効化、G が二次流通を検知し遮断。

なぜ問題か

出版業界は違法コピーで数千億円の損失。既存 DRM では**再編集・圧縮ファイル**に対応できなかった。

どうして起きたか

「データ形式を変えればバレない」という抜け道が存在した。

どうして防げるか（予防策）

- **封鎖ログ CSV（p.1436–1450）**で不正コピー履歴を記録。
- **再循環台帳（p.1665–1667）**で二次流通を検知。

なぜ可能なのか（裏付け）

- 解説書に「P2P 流通も侵害対象」と明記。

セキュリティ上の意義

違法コピーを**形式変換ごと封鎖**し、正規出版の価値を守る。

事例 25（2020 年 5 月 9 日：国際標準化における再循環利用）

- **構成パターン**：G 単体（正規再循環）
- **該当ページ**：p.1541–1564, p.1665–1667

発生状況

日本企業のセーフティアルゴリズムを ISO 標準化。G システムが**正規ライセンス経由の再循環**として処理し、国際機関へ提出。

なぜ問題か

国際標準化の場では「オリジナルの権利主張」が曖昧になりがち。

どうして起きたか

従来は国際会議で「誰が元の権利者か」不明確 → 無断利用横行。

どうして防げるか（予防策）

- **標準化提案記録（p.1541–1564）**で再循環経由を明記。
- **経済効果データ（p.1665–1667）**で正規利用を裏付け。

なぜ可能なのか（裏付け）

- 本体に「ISO/IEC 標準化・TRIPS 適合」が明示。

セキュリティ上の意義

「国際標準化＝合法再循環」であることを証明し、**国家間の知財紛争を未然に防止**。

✅ 第 5 部まとめ

- **F＝再利用封鎖**：契約終了後や不正コピーの「出口」を完全遮断。
- **G＝再循環処理**：正規ルートを通れば二次流通を合法化、それ以外は遮断。
- **セキュリティ的意義**：教育・医療・出版・国際市場など「出口管理」を徹底し、**知財と個人情報を循環から守る**。

📘 第 6 部：事例 26〜30（H・I・J パターン）

事例 26（2024 年 2 月 1 日：裁判証拠アーカイブ）

- **構成パターン**：H 単体（最終アーカイブ・監査）
- **該当ページ**：p.1391–1410, p.1411–1430

発生状況

金融不正事件の裁判において、被害者が提出した通報ログが「改ざんされていない」ことを証明するため、H システムで保存された **CSV＋Merkle Root＋TSA 署名**が証拠採用された。

なぜ問題か

デジタル証拠は「改ざんされたのでは？」という疑念で無効化されやすい。

どうして起きたか

従来の保存方式（PDF や通常ログ）は改ざん検知力がなく、証拠力に欠けた。

どうして防げるか（予防策）

- **不可逆保存（WORM＋Merkle＋TSA, p.1411–1430）**
- **API `/audit/archive`（p.1411–1430）**による監査証跡出力

なぜ可能なのか（裏付け）

- 本体に「証跡保存は著作権対象」と明記。

セキュリティ上の意義

「ログそのものが裁判で通用する」＝**デジタル証拠の信頼性を制度的に確立**。

事例 27（2023 年 5 月 11 日：病院サーバ障害による記録回復）

- **構成パターン**：I 単体（特別保存・回復）
- **該当ページ**：p.1520–1540, p.1581–1600

発生状況

病院サーバが障害でダウンし、数百人分の Vital ログが失われた。I システムにより **再生成アルゴリズム（recoverEvidence, rebuildLedger）**を実行 → データを復元。

なぜ問題か

医療記録は失われると保険請求や訴訟で不利になる。

どうして起きたか

従来はバックアップ依存 → 故障時に「直近データ」が失われる。

どうして防げるか（予防策）

- **復元アルゴリズム（p.1520–1540）**
- **再保存ハッシュ構造（p.1581–1600）**

なぜ可能なのか（裏付け）

- 著作物に「回復処理を著作権保護対象」と明記。

セキュリティ上の意義

失われた証拠を取り戻せる → **人命・権利・経済活動の連続性を守る。**

事例 28（2022 年 7 月 22 日：国際紛争時の知財証拠回復）

- **構成パターン**：I 単体（特別回復）＋H 連携
- **該当ページ**：p.1665–1670, p.1699–1701

発生状況

国際裁判所で、ある国が他国の技術を無断利用したと提訴。サーバ攻撃で証拠が一部失われたが、I で回復し、H で証跡化 → 裁判に提出。

なぜ問題か

国際紛争では「証拠不在」が致命的。

どうして起きたか

攻撃や自然災害で記録が破損するケースは避けられない。

どうして防げるか（予防策）

- **回復 API（/recover, /restore, p.1601–1620）**
- **アーカイブ保存（p.1391–1430）**

なぜ可能なのか（裏付け）

- 終章に「国際的証拠力」を強調。

セキュリティ上の意義

「証拠が失われても復活できる」→ **国際秩序を守るセキュリティ基盤**。

事例 29（2021 年 11 月 30 日：災害復興基金の特別決済）

- **構成パターン**：J 単体（特殊用途・人道利用）
- **該当ページ**：p.1632–1664, p.1668–1670

発生状況

大地震で被災した自治体に対し、E（清算）を経由せずに **J の特例ルート**が発動。国際基金から直接補償金が送金された。

なぜ問題か

従来は「補償金支払いまで数か月」かかり、被災者の生活が破綻していた。

どうして起きたか

既存制度は人道的危機に即応できなかった。

どうして防げるか（予防策）

- **特別許可関数 specialUsePermit()（p.1665–1667）**
- **人道利用 UI（p.1668–1670）**

なぜ可能なのか（裏付け）

- 「特殊用途（災害・人道支援）を権利対象に含む」と明記。

セキュリティ上の意義

災害時に**資金・物資が即時循環** → 命をつなぐセーフティネット。

事例 30（2020 年 4 月 9 日：感染症パンデミック時の国際研究利用）

- **構成パターン**：J 単体（特殊用途）
- **該当ページ**：p.1632–1664, p.1699–1701

発生状況

世界的パンデミックで、Vital データ（B）と契約ログ（C）が、J システム経由で **国際研究機関（WHO）に例外的に提供**。

なぜ問題か

通常ルールでは「契約終了後のデータ共有」は禁止されている → しかし世界規模の危機では例外が必要。

どうして起きたか

「人命優先と権利保護」の両立を保証する仕組みが欠如していた。

どうして防げるか（予防策）

- **exceptionRoute()関数（p.1665–1667）**
- **国際協力証跡（p.1671–1680）**

なぜ可能なのか（裏付け）

- 終章（p.1699–1701）に「国際的展開・人道支援」と明記。

セキュリティ上の意義

「通常は禁止、しかし人命優先で例外許容」 → **社会的セキュリティと人道の両立**。

✅ 第 6 部まとめ

- **H＝最終アーカイブ**：不可逆保存で証拠性を永久保証。
- **I＝特別回復**：消失・破損した記録を例外的に復元。
- **J＝特殊用途**：人道・国際危機に限定して例外的利用を許容。

👉 A〜J 全てのパターンが揃い、**命・権利・経済・証跡・回復・人道**の全方位セキュリティが完成しました。

📘 第 1 部：事例 1〜5（A パターン＝緊急通報犯罪防止）

事例 1（2024 年 3 月 12 日：通学路での誘拐未遂）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.25–32, p.110–133

犯罪/不正のシナリオ

小学生が通学中、不審者に腕をつかまれ「助けて！」と叫んだ瞬間、ランドセル内蔵マイクが異常音＋危険ワードを検知。GPS と連動し、学校と保護者、警察に即時通報された。

なぜ問題か

- 誘拐事件は初動対応が遅れると取り返しがつかない。
- 従来の防犯ブザーは「押せなければ無力」、発見も遅れる。

どうして起きたか

- 犯罪者は「子供が操作できない隙」を狙う。
- 従来は「叫んでも記録が残らない」ため証拠不在。

どうして防げるか（予防・対策）

- **音響解析（FFT＋KWS, p.134–145）**で「叫び声＋危険語」を自動検知。
- **Silent UI（p.110–133）**で不審者に気付かれない裏通報。
- **通報ログ保存（p.83–97）**で証拠を残し、後の刑事立証に利用可能。

なぜ可能なのか（裏付け）

- 設計仕様（p.109）に閾値・項目を明示。
- 「結論一致＝侵害成立」と定義し、模倣回避を封鎖。

セキュリティ上の意義

「声を上げた瞬間に通報・記録」 → 犯罪の成立前に阻止、かつ裁判証拠化。

事例 2（2023 年 9 月 5 日：深夜のストーカー被害）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.26–30, p.220–224

犯罪/不正のシナリオ

女性が帰宅中に見知らぬ男に追跡され「やめて！」と発話 → 危険ワードを検知し、スマホアプリが Silent Alert を発動。警察と友人に即時通知。

なぜ問題か

- ストーカー事件は「警察に相談済みでも現場で対応できない」ケースが多い。
- 被害者は恐怖で操作できないことが多い。

どうして起きたか

- 加害者は「通報の遅れ」を狙い、深夜や人通りの少ない場所を選ぶ。

どうして防げるか（予防・対策）

- **危険ワード辞書（p.220–224）**で「やめて」「助けて」等を即時検知。
- **Silent UI（p.110–133）**で気付かれず裏通報。
- **契約的保護（p.621–630）**により言い換え・翻訳でも逃げ道なし。

なぜ可能なのか（裏付け）

- 著作権範囲に「言語差・記号差を問わず侵害成立」と明記。

セキュリティ上の意義

「声を出すだけで警察へ通報」 → 犯罪を未然に防ぎ、エスカレーションを阻止。

事例 3（2022 年 11 月 28 日：高齢者宅への侵入窃盗）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.28–29, p.98–108

犯罪/不正のシナリオ

深夜に独居高齢者宅に侵入。高齢者が叫び声をあげた際、マイクが異常音を検知 → GPS との照合で「通常位置と異常」が判明し、警備会社に自動通報。

なぜ問題か

- 高齢者宅は防犯が脆弱。
- 犯罪者は「声を出しても届かない」環境を狙う。

どうして起きたか

- 既存防犯カメラは「事後確認」用であり、即時性がない。

どうして防げるか（予防・対策）

- **GPS＋Wi-Fi RTT（p.98–108）**で位置乖離を検知。
- **Silent UI（p.110–133）**で通報しつつ証跡保存。
- **CSV ログ（p.83–97）**で警察が証拠利用。

なぜ可能なのか（裏付け）

- 「位置＋音を組み合わせた自動通報」を特許請求項で保護。

セキュリティ上の意義

「声と位置で即通報」→ 犯罪者の逃走時間を与えず、即座に阻止。

事例 4（2021 年 8 月 2 日：車上荒らし・盗難未遂）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.29, p.56–82

犯罪/不正のシナリオ

駐車場で車窓が破壊される音 → 車載デバイスが異常音を検知し、自動で所有者スマホ＋警備会社に Silent 通知。

なぜ問題か

- 車上荒らしは「数十秒で犯行完了」するため、通常アラームは無力。

どうして起きたか

- 従来の警報器は「音を鳴らすだけ」で、証拠が残らない。

どうして防げるか（予防・対策）

- **API 連携（/alerts, /evidence, p.56–82）**で警備会社直結。

- **録音＋ログ保存（p.32）**で証拠力強化。
- **UI ダッシュボード（p.110–133）**で可視化。

なぜ可能なのか（裏付け）

- 本体に「警察・消防・自治体 API との外部連携」と明記。

セキュリティ上の意義

「犯行直後に証拠＋通報」→ 犯罪を記録とともに即座に抑止。

事例 5（2020 年 7 月 6 日：地震災害に便乗した窃盗）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.28–30, p.32

犯罪/不正のシナリオ

地震で停電した住宅地に窃盗犯が侵入。住人が「助けて」と叫ぶ → マイクが異常音を検知、位置情報と組み合わせて消防本部＋警察へ Silent 通報。

なぜ問題か

- 災害時は警備・通報システムが停止し、犯罪が増加する。

どうして起きたか

- 犯罪者は「混乱＝監視不全」を狙う。

どうして防げるか（予防・対策）

- **音声＋位置情報による自動通報（p.26–29）**
- **検知→判定→通報→保存のフロー（p.32）**
- **Silent 通報 UI（p.110–133）**

なぜ可能なのか（裏付け）

- 「公共性・国際的評価」の章に災害時応用が示される。

セキュリティ上の意義

「災害便乗犯罪も即時通報」→ 治安悪化を未然に防ぐ。

✅ 第 1 部まとめ

- A パターンは「音響＋発話＋位置情報」に基づき、**誘拐・ストーカー・窃盗・車上荒らし・災害便乗犯罪**といったシナリオを即時検知・通報。
- **なぜ可能か**：アルゴリズム・API・UI・ログ構造がすべて著作権で保護され、改変や翻案による抜け道が封鎖されている。
- **セキュリティ的意義**：人が操作不能でも、**声や音をきっかけに犯罪を封じ込める「先制型防犯」**を実現。

📘 第 2 部：事例 6〜10（B パターン＝バイタルセキュリティ犯罪防止）

事例 6（2024 年 5 月 21 日：ATM 振り込め詐欺阻止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300–306, p.321–335

犯罪/不正のシナリオ

高齢者が ATM で詐欺グループの指示通りに操作。心拍数が急上昇し、手の発汗異常をセンサーが検知。表向きは「取引完了」画面を表示しつつ、裏では Silent Alert で銀行の不正対策センターに通知。

なぜ問題か

- 振り込め詐欺は「本人が操作」するため通常検知が困難。
- 被害額は年間数百億円規模。

どうして起きたか

- 被害者が「怪しい」と気づいても操作を止められない状況がある。
- 従来 ATM は行動ログしか監視せず、心理・生体の異常を捉えられなかった。

どうして防げるか（予防・対策）

- **VitalScore 算出式（p.307–310）**で「緊張状態」を数値化。
- **SilentTx API（p.321–322）**で裏通報。

- **UI 設計（p.331–335）**で利用者に気付かせず警察・銀行に通報。

なぜ可能なのか（裏付け）

- 特許出願ブロック（p.519–552）に「ATM 詐欺防止」が請求項として記載。

セキュリティ上の意義

体が発する異常で詐欺を自動阻止 → 被害者が「気付けなくても守られる」金融セキュリティ。

事例 7（2023 年 10 月 11 日：飲酒運転検知と車両停止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300–302, p.331–335

犯罪/不正のシナリオ

ドライバーが酒に酔った状態で車のエンジンをかけようとした際、呼吸異常と血中酸素濃度低下を検知 → 車載システムがエンジンをロックし、Silent Alert で家族・警察へ通知。

なぜ問題か

- 飲酒運転は交通死亡事故の主要因。
- 本人は「酔っていない」と錯覚しがち。

どうして起きたか

- 従来のアルコール検知器は「吹き込み操作」依存 → ごまかし可能。

どうして防げるか（予防・対策）

- **VitalProc モジュール（p.311–315）**で運転者の生体を直接検知。
- **Silent Alert UX（p.328–330）**で運転者に悟らせず警察へ通知。
- **契約仕様（p.307–310）**に基づき車両メーカーが導入可能。

なぜ可能なのか（裏付け）

- 本体に「車載端末応用」と明示。
- 特許請求項群に「Vital 異常→SilentTx」プロセスを記載。

セキュリティ上の意義

本人の意思を超えて車を止める → 飲酒運転の「人為的抜け道」を完全封鎖。

事例 8（2022 年 2 月 14 日：銀行強盗時の職員防護）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.303, p.321–330

犯罪/不正のシナリオ

銀行窓口で強盗が侵入。職員が緊張で心拍数急上昇。システムがこれを検知し、**通常業務画面を維持しつつ裏通報**を発動。警察と警備会社に通知。

なぜ問題か

- 強盗現場では「押しボタン式非常通報」は危険。
- 人質状態では職員が操作できない。

どうして起きたか

- 犯罪者は「押せない状況」を作り出す。
- 生体反応は隠せないが、従来システムは活用していなかった。

どうして防げるか（予防・対策）

- **SilentTx API（p.321–322）**で発報。
- **二重 UI 設計（p.328–330）**で表は通常業務画面、裏で警備通報。
- **ログ保存（p.323–327）**で証拠確保。

なぜ可能なのか（裏付け）

- 著作物に「裏通報 UX が最大特徴」と明記。

セキュリティ上の意義

「職員が何もせずに守られる」→ 金融犯罪の現場で人質リスクを最小化。

事例 9（2021 年 4 月 1 日：家庭内 DV 検知）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.304–305, p.331–335

犯罪/不正のシナリオ

家庭内で DV 被害を受けた女性。暴力を受け心拍急上昇、呼吸異常を検知 → スマートウォッチが Silent 通報し、児童相談所＋警察に通知。

なぜ問題か

- 被害者は「声を上げると報復される」ため通報できない。
- DV は密室犯罪で証拠が残りにくい。

どうして起きたか

- 生体反応は必ず異常を示すが、これを「証拠化」できる仕組みがなかった。

どうして防げるか（予防・対策）

- **バイタル異常時フローチャート（p.306）**で「正常→異常→Silent Alert」を明示。
- **UI 設計（p.331–335）**で家庭用端末に対応。

なぜ可能なのか（裏付け）

- 本体に「介護見守り・飲酒運転防止・DV 防止」など応用例を明記。

セキュリティ上の意義

被害者が沈黙していても体が通報する → 密室犯罪を見逃さないセキュリティ。

事例 10（2020 年 12 月 25 日：航空機ハイジャック防止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300–302, p.371–400

犯罪/不正のシナリオ

国際便のパイロットがハイジャック犯に脅される。心拍数・皮膚電位が異常を示し、システムが検知。機内 UI には何も表示されず、Silent 通報で地上管制に「ハイジャック発生」を自動送信。

なぜ問題か

- ハイジャック時はパイロットが「非常ボタン」を押せない。
- 数百人の乗客が命を失う可能性。

どうして起きたか

- これまで航空機には「パイロット健康監視＋裏通報」がなかった。

どうして防げるか（予防・対策）

- **シナリオ別アルゴリズム検証（p.371–400）**で Vital 異常の精度を実証。
- **SilentTx＋UI（p.328–330）**で乗客・犯人に気付かれずに地上と連携。

なぜ可能なのか（裏付け）

- 特許出願ブロック（p.519–552）に航空応用を含む。

セキュリティ上の意義

「パイロットが沈黙していても体が警告する」→ 航空犯罪の最前線セキュリティ。

✅ 第 2 部まとめ

- **B パターン＝体の異常反応を犯罪検知のシグナルに変える。**
- ATM 詐欺、飲酒運転、強盗、DV、ハイジャックといった「本人操作が困難な犯罪」を封じ込める。
- **予防＝VitalScore 算出、対策＝Silent Alert、可能性＝特許請求項＋ログ証跡** により法的裏付けあり。

📘 第 3 部：事例 11〜15（C パターン＝知財不正利用防止）

事例 11（2024 年 2 月 14 日：大学研究コードの剽窃防止）

- **構成パターン**：C 単体（知財照合・契約生成）
- **該当ページ**：p.553–560, p.561–580, p.904–938

犯罪/不正のシナリオ

ある大学研究室が、他大学の AI コードをコピーして論文に提出。照合システムが一致スコア 0.92 を検知し、即遮断→ライセンス契約画面に自動誘導。

なぜ問題か

- 剽窃は学術不正であり、大学・研究者の信用を失墜させる。
- 被害大学は知財収益を失う。

どうして起きたか

- 従来の剽窃検出は「検出のみ」で、契約や収益化に直結しなかった。

どうして防げるか（予防・対策）

- **compareIP(), similarityScore()（p.571–580）**で検出。
- **contractGen()（p.561–570）**で即ライセンス化。
- **収益分配ロジック（p.861–903）**で権利者に収益を配分。

なぜ可能なのか（裏付け）

- 特許出願（特願 2025-125256, p.916–938）に請求項として記載。

セキュリティ上の意義

剽窃を防ぐだけでなく、**正規利用へ強制誘導する学術セキュリティ**。

事例 12（2023 年 7 月 8 日：オープンソース不正商用利用）

- **構成パターン**：C 単体
- **該当ページ**：p.591–620, p.621–630

犯罪/不正のシナリオ

新興企業が GPL ライセンスの OSS を一部改変し、商用アプリで無断利用。C が検知→**blockTx()**で即遮断→契約画面に移行。

なぜ問題か

- OSS のライセンス違反は知財犯罪。
- 不正利用企業は不当利益を得て、正規開発者は収益を失う。

どうして起きたか

- OSS は「自由利用可能」と誤解されがち。
- 契約条項が複雑で、ユーザーが理解せずに利用。

どうして防げるか（予防・対策）

- **契約確認 UI（p.611–620）**でライセンス未確認を検知。

- **契約文言封鎖（p.621–630）**で表現差を禁止。
- **CSV ログ（p.601–610）**で証拠保存。

なぜ可能なのか（裏付け）

- 本体に「契約文言差を超えて侵害成立」と明記。

セキュリティ上の意義

OSS の正しい流通を保証し、**開発者と利用者双方を守る仕組み**。

事例 13（2022 年 1 月 12 日：知財担保ローンの虚偽利用防止）

- **構成パターン**：C 単体
- **該当ページ**：p.861–903

犯罪/不正のシナリオ

企業が実際には収益化されていない特許を「価値あり」と偽って担保にローンを申請。C が契約履歴と収益分配台帳を照合し、虚偽を検知→申請却下。

なぜ問題か

- 金融詐欺につながり、銀行は損害を受ける。
- 信用市場全体が不安定化。

どうして起きたか

- 知財価値は数値化が難しく、嘘の主張が通ってしまう。

どうして防げるか（予防・対策）

- **収益モデル（p.861–903）**で GDP 押上効果を定量化。
- **契約履歴台帳（p.601–610）**で実績を監査可能に。

なぜ可能なのか（裏付け）

- 本体に「知財流通の自動化により収益をリアルタイム分配」と明記。

セキュリティ上の意義

知財の虚偽利用を防ぎ、**金融詐欺を根本から封鎖**。

事例 14（2021 年 4 月 18 日：越境契約の契約逃れ防止）

- **構成パターン**：C 単体
- **該当ページ**：p.631–700, p.916–938

犯罪/不正のシナリオ

海外企業が契約文言の翻訳差を利用し、知財ロイヤリティの支払いを回避。C システムが契約文言の差異を無効化し、支払い義務を確定。

なぜ問題か

- 国際取引では「翻訳・言い換え」による契約逃れが横行。
- 権利者は支払いを受けられない。

どうして起きたか

- 各国で契約条項が微妙に異なるため、逃げ道が生まれる。

どうして防げるか（予防・対策）

- **契約文言封鎖（p.621–630）**で翻訳差も侵害扱い。
- **越境契約シナリオ（p.631–700）**で国際整合を確保。

なぜ可能なのか（裏付け）

- 特許明細（p.916–938）に国際契約を請求項化。

セキュリティ上の意義

契約逃れを封じ、**国際知財の正当な収益確保**を実現。

事例 15（2020 年 8 月 29 日：エンタメ違法コピー流通阻止）

- **構成パターン**：C 単体
- **該当ページ**：p.701–800, p.801–860

犯罪/不正のシナリオ

人気映画が違法コピーされ、動画配信サイトに流通。C システムが照合し、**blockTx()**で遮断。同時に制作者に契約提案を送信。

なぜ問題か

- 違法コピー流通で業界は数千億円の損失。
- 犯罪者は「編集・圧縮・部分コピー」で逃げていた。

どうして起きたか

- DRM は「複製禁止」に限定 → 編集差異には弱い。

どうして防げるか（予防・対策）

- **アルゴリズム検証ログ（p.801–860）**で高精度検知。
- **契約生成（p.561–570）**で合法利用に誘導。

なぜ可能なのか（裏付け）

- 「表現差・記号差があっても結論一致なら侵害」と明記。

セキュリティ上の意義

違法コピーを遮断しつつ、**正規収益へ変換する知財セキュリティ**。

✅ 第 3 部まとめ

- **C パターン＝知財不正利用防止** は、学術剽窃・OSS 違反・金融詐欺・契約逃れ・違法コピーなど、知財犯罪を包括的に遮断。
- **なぜ可能か**：契約生成・収益分配・文言封鎖が特許請求項で裏付け済。
- **セキュリティ的意義**：「不正＝遮断、正規利用＝契約化」という両立を実現。

📘 第 4 部：事例 16〜20（D・E パターン＝複合セーフティ＋決済不正防止）

事例 16（2024 年 9 月 10 日：学校内での誘拐未遂阻止）

- **構成パターン**：D 単体（複合セーフティ網）
- **該当ページ**：p.941–960, p.1011–1030

犯罪/不正のシナリオ

放課後、児童が校門付近で不審者に連れ去られそうになった。
児童が「助けて」と叫び（A）、心拍急上昇（B）、学校アプリ照合で正規利用外と判定（C）。三要素一致により複合判定エンジン（D）が危険を確定 → 教職員と警察に即通報。

なぜ問題か

- 学校での誘拐は社会的衝撃が大きい。
- 単体検知（音や心拍のみ）では誤報・虚報が多く、対応が遅れる。

どうして起きたか

従来システムは「孤立した単体検知」しかなく、信頼性不足。

どうして防げるか（予防・対策）

- **複合判定関数（p.961–970）**で A・B・C を統合スコア化。
- **複合 UI（p.1001–1010）**で学校管理者にわかりやすく表示。
- **複合ログ保存（p.991–1000）**で証拠を残す。

なぜ可能なのか（裏付け）

- 「命＋権利＋経済の三層モデル」と明記。
- 特許請求項群に「三重セーフティ複合構成」が含まれる。

セキュリティ上の意義

「三要素一致」＝本当に危険な時のみ作動 → 犯罪の未然防止と誤報削減を両立。

事例 17（2023 年 3 月 11 日：災害時の便乗詐欺阻止）

- **構成パターン**：D 単体
- **該当ページ**：p.943–947, p.1031–1050

犯罪/不正のシナリオ

大地震直後、救援物資申請アプリで「なりすまし」が多発。
D システムは通報（A）＋申請者 Vital（B）＋知財・契約照合（C）の 3 点一致で正規利用者を確認、不正利用者を遮断。

なぜ問題か

- 災害時は混乱を利用した不正申請（便乗詐欺）が多い。
- 被災者救済が遅れ、被害が拡大。

どうして起きたか

従来は「本人確認」が弱く、災害時の緊急性で不正が見逃されやすかった。

どうして防げるか（予防・対策）

- **複合稼働シナリオ（p.1031–1050）**で誤検知率低下を実証。
- **複合 Tx ログ（p.1091–1110）**で不正検知を可視化。

なぜ可能なのか（裏付け）

- 教育・金融・行政を横断する応用事例として明記。

セキュリティ上の意義

「複合一致で不正を排除」→ 本物の被災者に資源を確実に届ける。

事例 18（2022 年 6 月 15 日：金融取引における不正契約阻止）

- **構成パターン**：D→E（複合＋清算）
- **該当ページ**：p.1051–1070, p.1191–1210

犯罪/不正のシナリオ

企業が不正に修正した契約データを用いてローン申請。D が複合判定でリスクを検出 → E が清算処理を遮断、契約不成立として記録。

なぜ問題か

- 金融契約の不正は「信用詐欺」となり銀行の損失を招く。

どうして起きたか

従来の金融機関は「書面契約の確認」のみで行動ログや Vital との連動がなく、改ざんを見抜けなかった。

どうして防げるか（予防・対策）

- **複合閾値設定（p.1051–1070）**で多要素検証。
- **清算 Tx 群（p.1191–1210）**で契約処理を制御。
- **契約 UI（p.1151–1170）**で透明性を担保。

なぜ可能なのか（裏付け）

- 「通報＋Vital＋知財＋契約を直列化」と記述。

セキュリティ上の意義

「契約改ざんは決済で遮断」→ 金融詐欺を根本から防ぐ。

事例 19（2021 年 2 月 28 日：国際送金における詐欺防止）

- **構成パターン**：E 単体（清算・決済）
- **該当ページ**：p.1240–1260, p.1321–1340

犯罪/不正のシナリオ

海外子会社にロイヤリティを送金する際、虚偽の契約が提出された。E システムが契約不履行を検知→送金処理を遮断→ペナルティ精算を実行。

なぜ問題か

- 国際送金詐欺は「送金後に発覚」するため、資金回収が困難。

どうして起きたか

- 決済システムが「契約確認」を行わず、銀行は盲目的に送金していた。

どうして防げるか（予防・対策）

- **清算ロジック（p.1240–1260）**で契約条件と金額を照合。
- **Ledger API（p.1321–1340）**で全履歴を保存。
- **ペナルティ処理（p.1431–1450）**で違反を即時精算。

なぜ可能なのか（裏付け）

- 本体に「契約金額算出・ペナルティ処理」が記載。

セキュリティ上の意義

「契約→即照合→即精算」→ 国際金融詐欺を封鎖。

事例 20（2020 年 1 月 19 日：保険金不正請求阻止）

- **構成パターン**：E 単体（清算・決済）
- **該当ページ**：p.1261–1280, p.1341–1360

犯罪/不正のシナリオ

利用者が Vital データを改ざんして「事故があった」と虚偽申請。E システムが契約条件照合で不一致を検知→保険金支払いを停止。

なぜ問題か

- 保険金詐欺は年間数百億円規模の損害。
- 従来は「書面証拠」で虚偽がすり抜けていた。

どうして起きたか

- Vital や契約データが「分断保存」されており整合性検証が困難だった。

どうして防げるか（予防・対策）

- **契約条件照合（p.1240–1260）**で自動判定。
- **CSV 保存（p.1341–1360）**で監査証跡を残す。
- **契約 UI（p.1301–1320）**で透明性を担保。

なぜ可能なのか（裏付け）

- 特許請求項で「契約履行の自動精算」が保護対象。

セキュリティ上の意義

「虚偽申請は決済段階で遮断」→ 保険犯罪を未然に封鎖。

✅ 第 4 部まとめ

- **D＝複合セーフティ網**：誘拐・便乗詐欺など「誤報を排して不正だけを確実に検出」。
- **E＝清算・決済**：国際送金・保険金請求など「契約不履行を決済時に遮断」。
- **セキュリティ的意義**：契約犯罪や金融詐欺を「行動・契約・決済」で三重に封鎖。

📘 第 5 部：事例 21〜25（F・G パターン＝再利用・二次流通犯罪防止）

事例 21（2024 年 6 月 4 日：教育教材の無断再使用）

- **構成パターン**：F 単体（再利用封鎖）
- **該当ページ**：p.1240–1260, p.1335–1360

犯罪/不正のシナリオ

ある学校が、ライセンス契約が終了した教材アプリを**翌年度もコピー利用**。F システムが「利用終了フラグ」を検知 → 自動遮断。

なぜ問題か

- 教材の「無断再利用」は著作権侵害。
- 出版社や開発者の収益を奪う。

どうして起きたか

- 現場は「前年度データがあるから使える」と誤解。
- 従来の教材は終了後も利用可能状態で残ってしまっていた。

どうして防げるか（予防・対策）

- **再利用検知ロジック（p.1240–1260）**で契約失効を即判定。
- **失効ログ保存（p.1341–1360）**で証跡を残す。

なぜ可能なのか（裏付け）

- 本体に「契約終了後の利用は即侵害」と記載。

セキュリティ上の意義

教育分野における知財犯罪の温床を根本から封鎖。

事例 22（2023 年 8 月 17 日：医療データの二次研究流用）

- **構成パターン**：F 単体
- **該当ページ**：p.1335–1360, p.1436–1450

犯罪/不正のシナリオ

病院が契約終了後に、患者 Vital データを**匿名化して研究機関に再提供**。F が再流通を検知し遮断。

なぜ問題か

- 医療データの無断二次利用は**個人情報保護法違反**。
- 患者の信頼を大きく損なう。

どうして起きたか

- 現場は「匿名化すればセーフ」と誤認。
- 契約失効管理が従来システムでは曖昧。

どうして防げるか（予防・対策）

- **失効ハッシュ記録（p.1341–1360）**で使用可否を制御。
- **再流通遮断アルゴリズム（p.1436–1450）**で不正提供を阻止。

なぜ可能なのか（裏付け）

- 「匿名化・部分利用も侵害対象」と明記。

セキュリティ上の意義

「匿名化だから大丈夫」という抜け道を完全封鎖。

事例 23（2022 年 12 月 1 日：ソフトウェアの不正サブライセンス）

- **構成パターン**：G 単体（二次流通処理）
- **該当ページ**：p.1504–1510, p.1521–1530

犯罪/不正のシナリオ

企業がライセンスを取得後、権利者の承諾なく**第三者に転売（サブライセンス販売）**。G システムが検知し、契約経由以外を遮断。

なぜ問題か

- サブライセンス転売は「横流し」行為であり正規権利者を欺く。
- 市場に不正コピーが氾濫。

どうして起きたか

- 既存契約管理が「一次ライセンス」までしか追えなかった。

どうして防げるか（予防・対策）

- **二次流通チェック API（/resale/check, p.1521–1530）**。
- **正規ライセンス経由ルート（p.1504–1510）**のみ通過許可。

なぜ可能なのか（裏付け）

- 「正規ルート外の二次利用は即侵害」と記述。

セキュリティ上の意義

「横流し」や「裏市場」自体を成立させない。

事例 24（2021 年 10 月 23 日：電子書籍の違法コピー再流通）

- **構成パターン**：F→G 連携
- **該当ページ**：p.1436–1450, p.1665–1667

犯罪/不正のシナリオ

人気電子書籍が P2P 共有サイトで違法配布。F がコピーを失効化 → G が P2P 経由の二次流通を検知し遮断。

なぜ問題か

- 出版業界は年間数千億円の損失。
- 違法共有は「形式を変えればバレない」と思われがち。

どうして起きたか

- 従来の DRM はファイル形式変換に弱かった。

どうして防げるか（予防・対策）

- **封鎖 CSV（p.1436–1450）**でコピー履歴を追跡。
- **再循環台帳（p.1665–1667）**で不正経由を可視化。

なぜ可能なのか（裏付け）

- 本体に「形式変換も結論一致なら侵害」と明記。

セキュリティ上の意義

「ファイル形式を変えても通用しない」完全封鎖型 DRM。

事例 25（2020 年 5 月 9 日：国際標準化における不正流用防止）

- **構成パターン**：G 単体（正規再循環）
- **該当ページ**：p.1541–1564, p.1665–1667

犯罪/不正のシナリオ

海外企業が国際標準化会議において、日本発のアルゴリズムを**自社開発と偽って提出**。
G システムが台帳を参照し、正規ルート外として拒否 → 本来の権利者を提示。

なぜ問題か

- 標準化の場での不正流用は、国家規模の経済損失につながる。

どうして起きたか

- 国際会議では権利主張が不透明で、盗用が横行。

どうして防げるか（予防・対策）

- **国際標準化提案台帳（p.1541–1564）**。
- **経済効果シナリオ（p.1665–1667）**で正規権利者を証明。

なぜ可能なのか（裏付け）

- 本体に「ISO/IEC, TRIPS 対応」が明示。

セキュリティ上の意義

「国際標準化の場で嘘をつけない」 → 知財の国家的セキュリティを保証。

✅ 第 5 部まとめ

- **F パターン＝不正再利用を即遮断** → 教育・医療・出版の「出口管理」強化。
- **G パターン＝正規ルート管理** → 不正な二次流通や国際標準化での盗用を防止。
- **セキュリティ的意義**：犯罪者の「二次利用・横流し・形式変換」という抜け道を封鎖し、正規の流通経済を守る。

📘 第 6 部：事例 26〜30（H・I・J パターン＝証拠保存・回復・国際犯罪防止）

事例 26（2024 年 2 月 1 日：金融詐欺裁判におけるデジタル証拠）

- **構成パターン**：H 単体（最終アーカイブ・監査）
- **該当ページ**：p.1391–1410, p.1411–1430

犯罪/不正のシナリオ

詐欺グループが偽装送金を行ったが、被害者が提出した**通報ログ＋Merkle Root＋TSA 署名**が「改ざん不能な証拠」として採用され、犯人が有罪判決。

なぜ問題か

- デジタル証拠は「改ざん可能」として無効化されやすい。

どうして起きたか

- 従来の PDF・通常ログは信頼性が弱い。

どうして防げるか（予防・対策）

- **WORM 保存＋署名（p.1411–1430）**で不可逆保存。
- **API `/audit/archive`**で検証可能ログを提供。

なぜ可能なのか（裏付け）

- 「証跡保存そのものが著作権対象」と記載。

セキュリティ上の意義

「デジタル証拠を裁判で通用させる」→ 犯罪を立証可能にする司法セキュリティ。

事例 27（2023 年 5 月 11 日：病院でのカルテ消失と復元）

- **構成パターン**：I 単体（特別保存・回復）
- **該当ページ**：p.1520–1540, p.1581–1600

犯罪/不正のシナリオ

病院サーバがランサムウェア攻撃を受け、患者カルテと Vital ログが破壊。I システムが **recoverEvidence(), rebuildLedger()**で復元し、犯行グループの「証拠隠滅」を無効化。

なぜ問題か

- 医療詐欺・保険金不正請求の証拠が失われる恐れ。

どうして起きたか

- サイバー攻撃で「バックアップも同時破壊」されるケースが増加。

どうして防げるか（予防・対策）

- **回復アルゴリズム（p.1520–1540）**で再生成。
- **再保存ハッシュ（p.1581–1600）**で改ざん防止。

なぜ可能なのか（裏付け）

- 著作物に「復元プロセスが著作権対象」と明記。

セキュリティ上の意義

「証拠を失っても取り戻せる」→ 犯罪隠蔽を封じる。

事例 28（2022 年 7 月 22 日：国際紛争での知財証拠復元）

- **構成パターン**：I＋H 連携
- **該当ページ**：p.1665–1670, p.1699–1701

犯罪/不正のシナリオ

国際仲裁で「技術盗用」を争点とした裁判。相手国がサーバ攻撃で証拠を破壊したが、I で回復し、H で監査証跡を付与して国際裁判所に提出。

なぜ問題か

- 国際的知財窃盗は国家規模の犯罪。
- 証拠が失われると裁判自体が無効化。

どうして起きたか

- 故意のデータ破壊による「証拠消去」が常套手段。

どうして防げるか（予防・対策）

- **/recover, /restore API（p.1601–1620）**。
- **最終アーカイブ（p.1391–1430）**で不可逆証跡を付与。

なぜ可能なのか（裏付け）

- 終章に「国際的証拠力」として位置付け。

セキュリティ上の意義

「国家犯罪の隠蔽を不可能化」→ 国際秩序を守る。

事例 29（2021 年 11 月 30 日：災害復興基金を狙った詐欺阻止）

- **構成パターン**：J 単体（特殊用途）
- **該当ページ**：p.1632–1664, p.1668–1670

犯罪/不正のシナリオ

大地震後、被災者支援金を装って詐欺団体が国際基金からの補償金を不正請求。J システムが「特殊用途ルート」で人道利用と詐欺を判定、正規被災者のみ認証。

なぜ問題か

- 災害直後は「緊急性」を悪用した詐欺が横行。

どうして起きたか

- 従来は本人確認が遅く、詐欺グループに資金が流れてしまう。

どうして防げるか（予防・対策）

- **specialUsePermit()関数（p.1665–1667）**で人道利用か否かを判定。
- **緊急利用 UI（p.1668–1670）**で迅速に認証。

なぜ可能なのか（裏付け）

- 本体に「特殊用途（災害・人道支援）を権利対象」と記載。

セキュリティ上の意義

「災害便乗詐欺を根こそぎ排除」。

事例 30（2020 年 4 月 9 日：パンデミック時の研究データ不正利用阻止）

- **構成パターン**：J 単体（特殊用途）
- **該当ページ**：p.1632–1664, p.1699–1701

犯罪/不正のシナリオ

世界的感染症流行時、製薬会社が他社の Vital 研究データを無断利用して特許出願を試みた。J システムが国際協力モードを発動し、WHO に正規権利者を通知。不正利用を即座に拒否。

なぜ問題か

- パンデミックでは「急ぎ」を口実に知財窃盗が起きやすい。
- 製薬権益は数兆円規模。

どうして起きたか

- 非常事態では「正規手続き」が省略されがち。

どうして防げるか（予防・対策）

- **exceptionRoute()（p.1665–1667）**で特殊条件下の流通を制御。
- **国際協力証跡（p.1671–1680）**で利用を記録。

なぜ可能なのか（裏付け）

- 終章（p.1699–1701）に「国際的展開・人道支援」と明記。

セキュリティ上の意義

「緊急時でも知財窃盗は成立しない」→ 世界的危機でも正規の権利を守る。

✅ 第 6 部まとめ

- **H パターン＝証拠を永久保存し裁判で通用させる。**

- **I パターン＝消失・破壊された証拠を回復する。**
- **J パターン＝人道・国際犯罪に対応する特例利用。**

👉 これにより **A〜J すべてのパターン（30 事例）を通じて、犯罪・不正の予防・対策・証拠化・国際封鎖までを網羅**しました。

📘 第 1 部（事例 1〜5）：A パターン＝緊急通報と災害犯罪防止

事例 1（2024 年 3 月 12 日：通学路での誘拐未遂）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.25–32, p.110–133

発生状況

下校中の児童が不審者に声をかけられ腕をつかまれる。ランドセルのマイクが「助けて！」を検知し、GPS と連携して学校・保護者・警察に即時通報。

なぜ問題か

- 誘拐は初動遅れが致命的。
- 子供が操作できなければ従来の防犯ブザーは機能不全。

どうして起きたか

犯罪者は「子供が通報できない状況」を狙う。従来は**叫び声が証拠化されず、警察対応が遅延**していた。

どうして防げるか（予防・対策）

- **FFT＋KWS 解析（p.134–145）**で叫び声・危険ワードを即検出。
- **Silent UI（p.110–133）**で不審者に気付かれない裏通報。
- **通報ログ CSV（p.83–97）**で裁判証拠化。

なぜ可能なのか（裏付け）

- 設計仕様（p.109）に閾値設定を明記。
- 「結論一致＝侵害成立」の権利宣言。

セキュリティ上の意義

「声を上げただけで通報＋証拠化」→ 誘拐犯罪を未然に封鎖。

事例 2（2023 年 9 月 5 日：深夜のストーカー被害）

- **構成パターン**：A 単体
- **該当ページ**：p.26–30, p.220–224

発生状況

女性が帰宅中に追跡され「やめて！」と発話 → 危険ワード検知 → Silent Alert が発動し、警察と友人へ即通知。

なぜ問題か

- ストーカー事件は「通報の遅れ」が命取り。
- 被害者は恐怖で操作できない。

どうして起きたか

加害者は「孤立した環境」で被害者が操作できない状況を狙う。

どうして防げるか（予防・対策）

- **危険ワード辞書（p.220–224）**で言い換えも網羅。
- **Silent UI（p.110–133）**で犯人に気付かれない通報。
- **契約保護（p.621–630）**で翻訳差も回避。

なぜ可能なのか（裏付け）

- 「言語・記号の差異を問わず侵害成立」と明記。

セキュリティ上の意義

「言葉を発した瞬間に守られる」→ ストーカー犯罪の即時封鎖。

事例 3（2022 年 11 月 28 日：高齢者宅への侵入窃盗）

- **構成パターン**：A 単体
- **該当ページ**：p.28–29, p.98–108

発生状況

深夜に高齢者宅へ侵入。住人が叫び声をあげ、マイクが異常音を検出 → GPS 位置照合で「通常と異常」を判定 → 警備会社に通報。

なぜ問題か

- 高齢者は通報操作が難しい。
- 犯罪者は「声は届かない」と確信して侵入する。

どうして起きたか

従来は**音と位置の組合せによる自動検知が未実装**。

どうして防げるか（予防・対策）

- **GPS＋Wi-Fi RTT（p.98–108）**で乖離を即判定。
- **Silent 通報＋ログ保存（p.83–97）**で証拠化。

なぜ可能なのか（裏付け）

- 特許請求項に「位置＋音の照合による通報」を記載。

セキュリティ上の意義

「声と位置で自動通報」 → 高齢者を狙う窃盗犯を即検知。

事例 4（2021 年 8 月 2 日：車両盗難未遂）

- **構成パターン**：A 単体
- **該当ページ**：p.29, p.56–82

発生状況

駐車場で窓ガラス破壊 → 車載デバイスが異常音を検知し、所有者＋警備会社に Silent 通知。

なぜ問題か

- 車上荒らしは数十秒で完了。
- 通常アラームは「鳴るだけ」で証拠化されない。

どうして起きたか

従来は**録音・ログが残らず**抑止力が弱かった。

どうして防げるか（予防・対策）

- **API 連携（/alerts, /evidence, p.56–82）**で警備直結。
- **録音＋ログ（p.32）**で証拠残存。
- **管理 UI（p.110–133）**で可視化。

なぜ可能なのか（裏付け）

- 「警察・消防 API との連携」を本体で定義。

セキュリティ上の意義

「犯行直後に証拠＋通報」→ 車両犯罪を実行不能にする。

事例 5（2020 年 7 月 6 日：地震災害に便乗した窃盗）

- **構成パターン**：A 単体
- **該当ページ**：p.28–30, p.32

発生状況

地震で停電した住宅地に窃盗犯が侵入。住民が「助けて」と叫ぶ → マイクが異常音を検知、位置照合と併せて消防・警察に通報。

なぜ問題か

- 災害時は防犯システムが停止し、便乗犯罪が多発。

どうして起きたか

犯罪者は「社会的混乱＝通報不能」と見て狙う。

どうして防げるか（予防・対策）

- **音声＋位置照合（p.26–29）**で自動通報。
- **Silent UI（p.110–133）**で犯人に気付かれない。
- **証拠保存（p.32）**で事後裁判対応。

なぜ可能なのか（裏付け）

- 「公共性・災害応用」を第 4 部で強調。

セキュリティ上の意義

「災害便乗犯罪を即時検知」→ 混乱期の治安を守る。

✅ 第 1 部まとめ

- A パターン（緊急通報）は **誘拐・ストーカー・窃盗・車両犯罪・災害便乗犯罪** を対象に「声＋位置」で即検知・通報。
- **なぜ可能か**：音響解析・位置照合・Silent 通報・CSV 証跡保存がすべて特許＋著作権で裏付けられている。
- **セキュリティ的意義**：操作不要・声だけで守られる「初動封鎖型防犯インフラ」。

📘 第 2 部（事例 6〜10）：B パターン＝バイタル異常と災害・不正検知

事例 6（2024 年 5 月 21 日：ATM 振り込め詐欺阻止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300–306, p.321–335, p.519–552

発生状況

高齢者が ATM で指示通りに振込を実行しようとした際、心拍数が急上昇・手の皮膚電位が異常を示す。システムが詐欺兆候を検知 → 表向きは「取引完了」画面を表示しつつ、Silent Alert で銀行・警察に自動通報。

なぜ問題か

- 振り込め詐欺は「本人が操作する」ため従来検知が難しかった。
- 犯罪者は「緊張で異常を示しても検知されない ATM」を狙う。

どうして防げるか（予防・対策）

- **VitalScore 算出式（p.307–310）**で緊張状態を定量化。
- **SilentTx API（p.321–322）**で裏通報。
- **契約仕様（p.303–306）**に「バイタル＋通報」を包括保護と明記。

セキュリティ上の意義

「体が示す異常で詐欺を封鎖」→ 高齢者が気付かなくても守られる金融セキュリティ。

事例 7（2023 年 10 月 11 日：飲酒運転による事故防止）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300–302, p.331–335

発生状況

ドライバーが飲酒後に車を始動 → 呼吸異常・血中酸素濃度低下を検知。エンジンは起動せず、家族・警察に Silent 通知。

なぜ問題か

- 飲酒運転は交通死亡事故の主要因。
- 「自分は大丈夫」という過信による事故が多い。

どうして防げるか（予防・対策）

- **VitalProc モジュール（p.311–315）**で運転者をモニタリング。
- **Silent UX（p.328–330）**で気付かれず警察へ通知。
- **特許請求項群（p.519–552）**に車載応用を記載。

セキュリティ上の意義

「本人の意思に関わらず車を止める」→ 飲酒運転の再発を根本封鎖。

事例 8（2022 年 2 月 14 日：介護施設における転倒事故）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.302, p.336–370

発生状況

入居者が転倒。システムが心拍急上昇＋皮膚電位異常を検知 → スタッフ到着前に家族と医師へ Silent 通知。

なぜ問題か

- 転倒は発見が遅れると死亡リスクが急増。
- 介護施設では「見逃し」が多発。

どうして防げるか（予防・対策）

- **実証データ（p.336–370）**で検知率・誤検知率を数値化。
- **擬似コード実行ログ（p.401–450）**で動作確認済。

セキュリティ上の意義

「体が倒れた瞬間に通報」→ 介護事故を未然に防止。

事例 9（2021 年 4 月 1 日：家庭内 DV の隠れた被害検知）

- **構成パターン**：B 単体
- **該当ページ**：p.304–305, p.331–335

発生状況

家庭内で DV 被害を受けた女性。声を出せず沈黙したまま、殴打による心拍急上昇・呼吸異常をシステムが検知 → Silent 通報で警察と児童相談所へ通知。

なぜ問題か

- DV は密室犯罪で発覚が遅れがち。
- 被害者は「声を上げると報復される」ため通報できない。

どうして防げるか（予防・対策）

- **バイタル異常パターン図解（p.306）**で「正常→異常→Silent Alert」ルートを確立。
- **UI 設計（p.331–335）**で家庭用端末に対応。

セキュリティ上の意義

「声を上げられなくても体が通報する」→ DV 犯罪の密室性を突破。

事例 10（2020 年 12 月 25 日：航空機パイロット異常とハイジャック対策）

- **構成パターン**：B 単体
- **該当ページ**：p.300–302, p.371–400

発生状況

国際便でパイロットがハイジャック犯に脅迫される。心拍数・皮膚電位が異常を示し、地上管制に Silent 通報 → 犯行が即座に察知される。

なぜ問題か

- 航空犯罪は多数の命を一度に危険に晒す。
- パイロットは「非常ボタンを押せない」状況が多い。

どうして防げるか（予防・対策）

- **シナリオ別検証（p.371–400）**で Vital 異常検知の有効性を確認。
- **Silent 通報 UX（p.328–330）**で犯人に気付かれない。

セキュリティ上の意義

「パイロットが沈黙しても体が知らせる」 → 航空テロを未然防止。

✅ 第 2 部まとめ

- **B パターンは「体の異常が犯罪・災害検知の信号」になる。**
- ATM 詐欺、飲酒運転、介護事故、DV、ハイジャックといった「本人が声を上げられない・操作できない状況」でも通報可能。
- **予防＝バイタル監視、対策＝Silent Alert、可能性＝VitalScore＋契約保護（特許出願済）。**

📘 第 3 部（事例 11〜15）：C パターン＝知財不正利用と災害便乗模倣

事例 11（2024 年 2 月 14 日：大学研究コードの剽窃防止）

- **構成パターン**：C 単体
- **該当ページ**：p.553–560, p.561–580, p.904–938

発生状況

研究者が他大学の AI アルゴリズムをコピーし論文に流用。提出時に C システムがコードを照合、一致スコア 0.91 を検知→剽窃を遮断し、自動でライセンス契約提案を提示。

なぜ問題か

- 剽窃は学術不正行為であり、知財の盗用。
- 被害大学は収益と信用を失う。

どうして起きたか

従来の剽窃検出は「検知だけ」で、契約や収益分配まで接続されていなかった。

どうして防げるか（予防・対策）

- **compareIP(), similarityScore()（p.571–580）**で検出。
- **contractGen()（p.561–570）**で契約生成。
- **収益分配ロジック（p.861–903）**で自動収益循環。

なぜ可能なのか（裏付け）

- 特許出願ブロック（p.916–938）に「照合→契約→収益分配」を請求項化。

セキュリティ上の意義

「剽窃を即遮断し正規契約へ誘導」→ 学術研究の信頼性確保。

事例 12（2023 年 8 月 30 日：災害アプリの模倣・便乗不正）

- **構成パターン**：C 単体
- **該当ページ**：p.631–700, p.621–630

発生状況

大地震後、正規の防災アプリが広まる中で、悪質業者が **UI や機能を模倣した偽アプリ**を拡散。C システムが契約照合で侵害を検知→遮断。

なぜ問題か

- 偽アプリが個人情報や寄付金を詐取。
- 災害混乱期では利用者が正規アプリか判断できない。

どうして起きたか

従来は「表現・UI を少し変えるだけ」で模倣を免れていた。

どうして防げるか（予防・対策）

- **契約文言差異封鎖（p.621–630）**で言い換え回避を封鎖。
- **応用シナリオ（p.631–700）**で災害利用も想定。

なぜ可能なのか（裏付け）

- 「結論一致＝侵害成立」と著作権規定に明記。

セキュリティ上の意義

「災害便乗型の偽アプリを封じる」→ 被災者を守る知財セキュリティ。

事例 13（2022 年 6 月 12 日：知財担保ローン詐欺の検出）

- **構成パターン**：C 単体
- **該当ページ**：p.861–903, p.601–610

発生状況

中小企業が収益実績のない特許を担保にローン申請。C システムが契約台帳と収益分配履歴を照合→不一致を検知し虚偽申請を却下。

なぜ問題か

- 金融機関は虚偽担保で巨額損害を受ける。
- 知財市場の信用性が失墜。

どうして起きたか

従来は「知財の収益化実績」をリアルタイムで確認できなかった。

どうして防げるか（予防・対策）

- **契約ログ（p.601–610）**で履歴照合。
- **経済試算（p.861–903）**で価値を数値化。

なぜ可能なのか（裏付け）

- 本体に「知財流通を自動化し収益をリアルタイム分配」と明記。

セキュリティ上の意義

「知財の虚偽利用を金融段階で遮断」→ 金融不正封鎖。

事例 14（2021 年 11 月 5 日：国際契約における翻訳差を悪用した不正）

- **構成パターン**：C 単体
- **該当ページ**：p.621–630, p.631–700

発生状況

海外企業が契約翻訳差を利用して、支払い義務を免れようとする。C システムが「契約文言差異」を侵害として即時認定→支払いを確定。

なぜ問題か

- 国際契約の「翻訳差」悪用はよくある不正手法。
- 正規権利者が収益を奪われる。

どうして起きたか

従来の契約監査は**言語差・表現差を抜け道にされていた**。

どうして防げるか（予防・対策）

- **契約文言封鎖（p.621–630）**で翻訳差を回避。
- **越境契約処理（p.631–700）**で国際的整合性を保証。

なぜ可能なのか（裏付け）

- 特許明細（p.916–938）に「翻訳差を封鎖する契約処理」を請求項化。

セキュリティ上の意義

「言語の壁を悪用する不正を封じる」→ 国際知財保護の強化。

事例 15（2020 年 8 月 29 日：エンタメ作品の違法コピー流通）

- **構成パターン**：C 単体
- **該当ページ**：p.701–800, p.801–860

発生状況

映画が災害寄付キャンペーンの名目で「無料配布」として偽サイトに流出。C システムがブロックし、正規契約ルート外の配布を遮断。

なぜ問題か

- 「災害寄付」を口実に違法コピーを配布する便乗不正が多い。
- 正規収益は失われ、寄付金も詐取される。

どうして起きたか

災害時の善意を逆手にとった犯罪。従来の DRM は「形式変換・編集差」に弱かった。

どうして防げるか（予防・対策）

- **アルゴリズム評価ログ（p.801–860）**で高精度検知。
- **契約生成モジュール（p.561–570）**で合法利用に強制誘導。

なぜ可能なのか（裏付け）

- 「表現差・記号差を問わず結論一致なら侵害」と規定。

セキュリティ上の意義

「災害便乗の違法配布を即遮断」→ 被災支援の信頼性を守る。

✅ 第 3 部まとめ

- **C パターン＝知財不正利用防止** は、学術剽窃・災害便乗アプリ・金融詐欺・契約翻訳差悪用・違法コピー流通を対象に **不正＝遮断、正規利用＝契約化** を実現。
- **災害時に便乗する不正行為を特に封鎖**し、混乱期に悪用される知財犯罪を防ぐ。

📘 第 4 部（事例 16〜20）：D・E パターン＝複合災害対応＋決済不正封鎖

事例 16（2024 年 9 月 10 日：学校での複合誘拐未遂阻止）

- **構成パターン**：D 単体（複合セーフティ網）
- **該当ページ**：p.941–960, p.1011–1030

発生状況

児童が校門付近で不審者に声をかけられた。
「助けて」と叫び（A）、心拍急上昇（B）、アプリ利用履歴不一致（C）。
三要素一致で複合判定エンジン（D）が危険を確定 → 教員と警察に同時通報。

なぜ問題か

- 学校での誘拐は社会不安を増大させる。
- 単体検知は誤報が多く、信頼性が低い。

どうして防げるか（予防・対策）

- **複合判定関数（p.961–970）**でスコア統合。
- **複合 UI（p.1001–1010）**で分かりやすい表示。
- **複合ログ（p.991–1000）**で証跡保存。

なぜ可能なのか（裏付け）

- 「命＋権利＋経済の三層モデル」を定義。

セキュリティ上の意義

「三要素が揃ったときだけ作動」 → 誤報削減＋犯罪封鎖。

事例 17（2023 年 3 月 11 日：災害時の便乗詐欺検知）

- **構成パターン**：D 単体

- **該当ページ**：p.943–947, p.1031–1050

発生状況

大地震後、救援物資申請アプリに便乗詐欺が多発。
D が「通報ログ（A）＋申請者バイタル（B）＋契約照合（C）」を統合判定 → 正規申請者のみ認証、不正申請は遮断。

なぜ問題か

- 災害直後は「混乱」を狙った不正申請が横行。
- 本当に必要な被災者への救援が遅れる。

どうして防げるか（予防・対策）

- **複合シナリオ（p.1031–1050）**で災害時の誤報削減を実証。
- **Silent 通報（p.1091–1110）**で不正を裏で遮断。

なぜ可能なのか（裏付け）

- 「複合構成は行政・金融にも適用可能」と記載。

セキュリティ上の意義

「災害便乗詐欺を自動検知」 → 混乱期の犯罪抑止。

事例 18（2022 年 6 月 15 日：金融契約の改ざん検知）

- **構成パターン**：D→E（複合＋決済）
- **該当ページ**：p.1051–1070, p.1191–1210

発生状況

企業が契約書を改ざんして融資を申請。
D が複合判定で異常を検出 → E が清算処理を停止し、契約は成立せず。

なぜ問題か

- 改ざん契約は金融詐欺の典型。
- 被害が出ると信用市場全体に波及。

どうして防げるか（予防・対策）

- **複合閾値設定（p.1051–1070）**で改ざんを検知。

- **清算 Tx 群（p.1191–1210）**で決済を遮断。

なぜ可能なのか（裏付け）

- 「契約 Tx 直列化」により、改ざんが決済時に発覚。

セキュリティ上の意義

「改ざん契約は決済で止まる」 → 金融不正を遮断。

事例 19（2021 年 2 月 28 日：国際送金詐欺の阻止）

- **構成パターン**：E 単体（清算・決済）
- **該当ページ**：p.1240–1260, p.1321–1340

発生状況

国際子会社へのロイヤリティ送金時、虚偽契約が提出。
E システムが契約不一致を検知 → 送金を遮断し、即ペナルティ清算。

なぜ問題か

- 国際送金詐欺は「送金後に発覚」するため資金回収が困難。

どうして防げるか（予防・対策）

- **清算ロジック（p.1240–1260）**で契約条件と金額を照合。
- **Ledger API（p.1321–1340）**で全履歴を保存。

なぜ可能なのか（裏付け）

- 「契約条件照合・ペナルティ清算」を明記。

セキュリティ上の意義

「契約不履行は即ペナルティ」 → 国際金融犯罪の封鎖。

事例 20（2020 年 1 月 19 日：保険金詐欺の検知）

- **構成パターン**：E 単体（清算・決済）
- **該当ページ**：p.1261–1280, p.1341–1360

発生状況

利用者が Vital データを改ざんし、事故発生を偽装して保険金請求。
E が契約条件照合で不一致を検知 → 支払いを停止。

なぜ問題か

- 保険金詐欺は毎年数百億円の損失。
- 従来は書面証拠が中心で虚偽を見抜けなかった。

どうして防げるか（予防・対策）

- **契約条件照合（p.1240–1260）**で自動判定。
- **CSV 保存（p.1341–1360）**で証跡化。

なぜ可能なのか（裏付け）

- 特許請求項に「契約履行の自動精算」を記載。

セキュリティ上の意義

「虚偽申請は決済段階で遮断」→ 保険犯罪を封鎖。

✅ 第 4 部まとめ

- **D パターン＝複合災害対応**：災害便乗詐欺や誘拐などを「三要素一致」で高精度検知。
- **E パターン＝決済不正封鎖**：契約改ざん・送金詐欺・保険金詐欺を「清算段階」で遮断。
- **セキュリティ意義**：契約・金融・行政・教育すべてにおいて「不正を最後の瞬間で止める」仕組み。

📘 第 5 部（事例 21〜25）：F・G パターン＝再利用・二次流通の災害便乗不正防止

事例 21（2024 年 6 月 4 日：災害教材の無断再利用）

- **構成パターン**：F 単体（再利用封鎖）
- **該当ページ**：p.1240–1260, p.1335–1360

発生状況

災害後の教育現場で、契約期間が終了した教材アプリを「緊急だから」とコピー利用。F システムが**契約失効フラグ**を検知し即時遮断。

なぜ問題か

- 善意の名目でも著作権侵害は不正。
- 出版社・開発者への正当な対価が失われる。

どうして防げるか（予防・対策）

- **再利用検知ロジック（p.1240–1260）**で失効を即確認。
- **失効ログ保存（p.1341–1360）**で後から監査可能。

セキュリティ上の意義

「災害時でも正規ルートを徹底」→ 便乗不正を抑止。

事例 22（2023 年 8 月 17 日：医療データの不正二次提供）

- **構成パターン**：F 単体
- **該当ページ**：p.1335–1360, p.1436–1450

発生状況

大規模水害後、病院が患者 Vital データを「災害研究のため」と称して研究機関に再提供。F が**契約終了後の利用**を検知し遮断。

なぜ問題か

- 災害時の個人情報は特に悪用リスクが高い。
- 「匿名化すれば大丈夫」という誤解が多い。

どうして防げるか（予防・対策）

- **失効ハッシュ記録（p.1341–1360）**で利用可否を制御。
- **再流通遮断処理（p.1436–1450）**で不正提供を即阻止。

セキュリティ上の意義

「匿名化の抜け道も封鎖」 → 災害便乗型の医療データ不正流通を防止。

事例 23（2022 年 12 月 1 日：ソフトウェアのサブライセンス横流し）

- **構成パターン**：G 単体（二次流通管理）
- **該当ページ**：p.1504–1510, p.1521–1530

発生状況

災害支援アプリを導入した企業が、そのライセンスを**第三者に転売（横流し）**。G システムが検知 → 正規契約経由でないため遮断。

なぜ問題か

- 不正サブライセンスは「災害支援」を名目に横行。
- 正規権利者に収益が届かない。

どうして防げるか（予防・対策）

- **二次流通チェック API（p.1521–1530）**で転売を即検知。
- **正規ルートのみ通過許可（p.1504–1510）**。

セキュリティ上の意義

「横流し経済」を成立させない → 知財流通の透明性確保。

事例 24（2021 年 10 月 23 日：電子書籍の災害便乗コピー拡散）

- **構成パターン**：F→G 連携
- **該当ページ**：p.1436–1450, p.1665–1667

発生状況

大地震の後、「被災者支援のため」として人気電子書籍が違法コピーされ P2P で流通。F が**コピーを失効化** → G が**不正流通を遮断**。

なぜ問題か

- 善意を装った違法コピーは「寄付詐欺」と結び付きやすい。

どうして防げるか（予防・対策）

- **封鎖 CSV（p.1436–1450）**で不正履歴を監査。
- **再循環台帳（p.1665–1667）**で不正ルートを記録。

セキュリティ上の意義

「形式変換や名目変更でも即遮断」→ 出版流通の秩序を守る。

事例 25（2020 年 5 月 9 日：国際標準化会議での災害便乗盗用防止）

- **構成パターン**：G 単体（正規再循環）
- **該当ページ**：p.1541–1564, p.1665–1667

発生状況

海外企業が「災害対応技術」として日本のアルゴリズムを自社発と偽って国際会議に提出。
G が**正規台帳を照合**し、正規権利者を提示→不正を阻止。

なぜ問題か

- 災害便乗の知財盗用は国家規模の被害に直結。

どうして防げるか（予防・対策）

- **標準化提案記録（p.1541–1564）**で正規ルートを証明。
- **経済効果データ（p.1665–1667）**で正規導入の実績を補強。

セキュリティ上の意義

「災害対応の国際標準は不正利用できない」→ 国際知財の安全保障。

✅ 第 5 部まとめ

- **F＝再利用封鎖**：教育・医療・出版など、災害便乗型の「コピー再利用」を即遮断。
- **G＝正規二次流通管理**：正規契約経由のみを許容し、横流しや国際盗用を排除。
- **セキュリティ意義**：災害混乱期の善意を装った知財犯罪・不正流通を封鎖し、正規経済を守る。

📘 第 6 部（事例 26〜30）：H・I・J パターン＝証拠保存・回復・国際災害犯罪防止

事例 26（2024 年 2 月 1 日：災害便乗詐欺裁判における証拠保存）

- **構成パターン**：H 単体（最終アーカイブ・監査）
- **該当ページ**：p.1391–1410, p.1411–1430

発生状況

大地震後、被災者支援を名目にした寄付詐欺事件。被害者が提出したアプリ通報ログが H システムで **Merkle Root＋TSA 署名付アーカイブ**として保存され、裁判で有罪証拠に採用。

なぜ問題か

- 災害便乗詐欺は「証拠が改ざんされやすい」ため立件困難。

どうして防げるか（予防・対策）

- **不可逆保存（WORM＋署名, p.1411–1430）**で改ざん不可能。
- **API `/audit/archive`**で証跡出力。

セキュリティ上の意義

「改ざん不能な証跡」→ 災害犯罪を司法で裁ける。

事例 27（2023 年 5 月 11 日：病院サーバ攻撃と Vital 記録の復元）

- **構成パターン**：I 単体（特別保存・回復）
- **該当ページ**：p.1520–1540, p.1581–1600

発生状況

豪雨災害時、病院サーバがサイバー攻撃を受け患者カルテが消失。I システムが**recoverEvidence(), rebuildLedger()**で Vital ログを復元。

なぜ問題か

- 医療データ破壊は「保険金請求や医療訴訟の証拠隠滅」につながる。

どうして防げるか（予防・対策）

- **回復アルゴリズム（p.1520–1540）**で再生成。
- **復元ログ保存（p.1581–1600）**で再証跡化。

セキュリティ上の意義

「データを破壊しても復活する」→ 医療犯罪の隠蔽を阻止。

事例 28（2022 年 7 月 22 日：国際災害支援をめぐる知財盗用裁判）

- **構成パターン**：I＋H 連携
- **該当ページ**：p.1665–1670, p.1699–1701

発生状況

国際災害支援プロジェクトにおいて、日本企業の技術が海外企業に盗用された。相手国がサーバ攻撃で証拠を消去したが、I で回復し H で証跡化 → 国際裁判所で日本企業の権利が認められた。

なぜ問題か

- 災害時は「善意の国際協力」に便乗した知財盗用が発生しやすい。

どうして防げるか（予防・対策）

- **/recover, /restore API（p.1601–1620）**で復元。
- **アーカイブ保存（p.1391–1430）**で国際証跡化。

セキュリティ上の意義

「国家規模の知財犯罪を暴く」→ 国際秩序の維持。

事例 29（2021 年 11 月 30 日：災害復興基金を狙った不正請求）

- **構成パターン**：J 単体（特殊用途・人道利用）
- **該当ページ**：p.1632–1664, p.1668–1670

発生状況

地震被害を受けた自治体に対し、詐欺団体が復興基金を不正請求。J システムが「特殊利用ルート」で被災者の正当性をチェック → 詐欺団体を排除。

なぜ問題か

- 災害復興資金は「命をつなぐ資金」。不正請求で枯渇すると被災者が救済されない。

どうして防げるか（予防・対策）

- **specialUsePermit()（p.1665–1667）**で特例条件を審査。
- **緊急利用 UI（p.1668–1670）**で高速認証。

セキュリティ上の意義

「災害基金を不正から守る」→ 本当に必要な人に届く。

事例 30（2020 年 4 月 9 日：パンデミック時の研究データ盗用阻止）

- **構成パターン**：J 単体（特殊用途・国際協力）
- **該当ページ**：p.1632–1664, p.1699–1701

発生状況

世界的感染症流行時、製薬企業が他社の Vital 研究データを無断利用し特許出願。J システムが国際協力ルートを発動 → WHO に正規権利者を通知、不正出願を却下。

なぜ問題か

- パンデミック時は「緊急」を口実に知財盗用が横行する。

どうして防げるか（予防・対策）

- **exceptionRoute()（p.1665–1667）**で特殊条件下利用を制御。
- **国際協力証跡（p.1671–1680）**で正規流通を記録。

セキュリティ上の意義

「世界的危機でも知財窃盗を成立させない」→ 公平な国際協力。

✅ 第 6 部まとめ

- **H＝証拠保存**：災害・詐欺の証拠を改ざん不能に保存し裁判で使用可能。
- **I＝回復処理**：攻撃・災害で失われた証拠を復元、不正隠蔽を阻止。
- **J＝特殊用途**：災害復興基金詐欺やパンデミック時の知財盗用を特例ルートで防止。
- **総合意義**：災害や国際犯罪という混乱期においても「証拠・資金・知財」を守り抜くセキュリティ基盤。

📘 第 1 部（事例 1〜5：A パターン＝緊急通報による事故防止）

事例 1（2024 年 3 月 12 日：通学路での交通事故）

- **構成パターン**：A 単体（緊急通報）
- **該当ページ**：p.25–32, p.110–133

事故シナリオ

下校中の児童が交差点で車に接触。ランドセル内蔵マイクが「叫び声＋衝突音」を検知、GPS 位置と併せて学校・保護者・救急に自動通報。

なぜ問題か

- 子供はパニックで通報できない。
- 発見が遅れると救命率が下がる。

どうして起きたか

- 従来は通報が遅れ、事故現場で**救護が間に合わない**ケースが多い。

どうして防げるか（予防・対策）

- **音響解析（p.134–145）**で衝突音を即検出。
- **Silent UI（p.110–133）**で通報を裏で処理。
- **通報ログ（p.83–97）**で証拠を保存。

なぜ可能なのか（裏付け）

- 設計仕様（p.109）に閾値・検出条件を明記。

- 「結論一致＝侵害成立」として改変模倣を防止。

セキュリティ上の意義

「事故の一瞬を検知して即通報」→ 交通事故死を大幅に減らす。

事例 2（2023 年 9 月 5 日：深夜の歩行者転倒事故）

- **構成パターン**：A 単体
- **該当ページ**：p.26–30, p.220–224

事故シナリオ

女性が夜道で転倒し骨折。声を出せない状況だったが、**倒れた音＋GPS 異常位置**を検出し、救急へ自動通報。

なぜ問題か

- 夜間転倒事故は発見が遅れがち。
- 救護が遅れると骨折合併症や低体温症のリスク。

どうして起きたか

従来は「周囲の人が見つけるまで放置」されていた。

どうして防げるか（予防・対策）

- **危険音＋位置照合（p.98–108）**で転倒を即検出。
- **危険ワード辞書（p.220–224）**で声が出た場合も確実に拾う。

なぜ可能なのか（裏付け）

- 特許請求項に「音声＋位置の自動通報」を明記。

セキュリティ上の意義

「声が出せなくても事故が伝わる」→ 転倒死を防止。

事例 3（2022 年 11 月 28 日：高齢者宅でのガス爆発事故）

- **構成パターン**：A 単体

- **該当ページ**：p.28–29, p.98–108

事故シナリオ

高齢者宅でガス漏れが爆発。爆発音をシステムが即検知し、位置情報とセットで消防に通報。

なぜ問題か

- 高齢者は自分で通報できない可能性が高い。
- 爆発後は**二次災害（火災・延焼）**につながる。

どうして起きたか

従来は「近隣住民が気づくまで放置」されていた。

どうして防げるか（予防・対策）

- **異常音検知（p.134–145）**で爆発を瞬時に検知。
- **Silent 通報＋ログ保存（p.83–97）**で消防が即対応。

なぜ可能なのか（裏付け）

- 「音響＋位置」による自動通報を保護対象化。

セキュリティ上の意義

「人が通報不能でも災害を検知」→ ガス事故を最小限に封じる。

事例 4（2021 年 8 月 2 日：車両事故・多重衝突）

- **構成パターン**：A 単体
- **該当ページ**：p.29, p.56–82

事故シナリオ

高速道路で多重衝突。事故音を検知した車載デバイスが即時通報、所有者・救急・警察に通知。

なぜ問題か

- 多重衝突事故は「初動遅れ」で死者が増える。
- 二次衝突を防ぐため迅速な通報が必須。

どうして起きたか

従来の通報は「目撃者依存」。

どうして防げるか（予防・対策）

- **API 連携（/alerts, /evidence, p.56–82）**で警察直通。
- **録音・証拠保存（p.32）**で事故原因の立証も可能。

なぜ可能なのか（裏付け）

- 本体に「外部連携 API（警察・消防）」と明記。

セキュリティ上の意義

「事故発生の瞬間に自動通報」→ 二次事故を封じる。

事例 5（2020 年 7 月 6 日：地震での建物倒壊事故）

- **構成パターン**：A 単体
- **該当ページ**：p.28–30, p.32

事故シナリオ

大地震で住宅が倒壊。瓦礫下から「助けて」という声をマイクが検知、位置情報と組み合わせ消防へ Silent 通報。

なぜ問題か

- 倒壊事故は「救助が遅れる」ことが最大リスク。
- 生存率は 72 時間以内で急低下。

どうして起きたか

従来は「救助犬や人力探索」に依存していた。

どうして防げるか（予防・対策）

- **音声＋位置照合（p.26–29）**で自動検知。
- **通報ログ（p.32）**で救助側の誤解を防ぐ。

なぜ可能なのか（裏付け）

- 第 4 部で「災害応用」として記載。

セキュリティ上の意義

「声が届かなくても命を救う」→ 倒壊事故の早期救助。

✅ 第 1 部まとめ

- A パターンは **交通事故・転倒事故・爆発事故・車両衝突・地震倒壊** など「音＋声＋位置」で検知。
- **なぜ防げるか**：音響解析・位置照合・Silent 通報・CSV 証跡保存が裏付け。
- **セキュリティ意義**：人が操作できなくても事故を即時通報し、**救命率と事故証拠性を飛躍的に高める**。

📘 第 2 部（事例 6〜10）：B パターン＝バイタル異常による事故検知

事例 6（2024 年 5 月 21 日：ATM での急病事故）

- **構成パターン**：B 単体（Vital＋通報）
- **該当ページ**：p.300–306, p.321–335

事故シナリオ

高齢者が ATM で操作中に心筋梗塞を発症。突然の心拍急上昇と酸素飽和度低下をセンサーが検知し、Silent 通報で銀行職員と救急へ即時通知。

なぜ問題か

- 高齢者事故は「孤立場所」で発生しやすい。
- 発見遅れは致死率を高める。

どうして起きたか

従来の ATM は「金融取引監視」に限られ、利用者の健康状態を見ていなかった。

どうして防げるか（予防・対策）

- **VitalScore（p.307–310）**で生体異常を定量化。
- **SilentTx API（p.321–322）**で裏通報。
- **UI（p.331–335）**で周囲に気付かれない救護要請。

なぜ可能なのか（裏付け）

- 「バイタル＋通報構成を包括保護」と定義。

セキュリティ上の意義

「金融取引の場を事故検知インフラに変える」→ 高齢者の命を守る ATM。

事例 7（2023 年 10 月 11 日：飲酒運転による事故防止）

- **構成パターン**：B 単体
- **該当ページ**：p.300–302, p.331–335

事故シナリオ

ドライバーが飲酒状態で車を始動しようとした際、呼吸異常＋血中酸素低下をセンサーが検知。エンジンがロックされ、同時に家族と警察へ Silent 通知。

なぜ問題か

- 飲酒運転事故は死亡率が極めて高い。
- 運転者は「酔っていない」と誤認するケースが多い。

どうして防げるか（予防・対策）

- **VitalProc モジュール（p.311–315）**で自動チェック。
- **Silent UX（p.328–330）**で気付かれず通報。
- **特許請求項群（p.519–552）**で車載応用が明記。

なぜ可能なのか（裏付け）

- 本体に「車載端末での利用例」と明記。

セキュリティ上の意義

「体が止めるから事故が起きない」→ 飲酒運転事故をゼロへ。

事例 8（2022 年 2 月 14 日：介護施設での転倒事故）

- **構成パターン**：B 単体
- **該当ページ**：p.302, p.336–370

事故シナリオ

介護施設で高齢者が転倒。スタッフが巡回する前に、システムが心拍急上昇＋皮膚電位異常を検知 → 家族・医師に Silent 通知。

なぜ問題か

- 高齢者の転倒は「骨折→寝たきり→死亡」に直結。
- 発見が遅れると致命的。

どうして防げるか（予防・対策）

- **実証データ（p.336–370）**で検知率・誤検知率を改善。
- **擬似コード（p.316–320）**で異常時 SilentTx を発行。

なぜ可能なのか（裏付け）

- 本体に「介護見守り」事例を記載。

セキュリティ上の意義

「転んだ瞬間に事故通報」 → 高齢者の命を守る事故検知。

事例 9（2021 年 4 月 1 日：家庭内の急病事故）

- **構成パターン**：B 単体
- **該当ページ**：p.304–305, p.331–335

事故シナリオ

家庭内で持病を持つ女性が発作で倒れる。声を出せず動けなかったが、心拍異常を検知 → スマートウォッチが Silent 通報し、救急へ。

なぜ問題か

- 持病事故は「家族不在の時間帯」に発生しやすい。
- 発見が遅れると死亡リスクが高い。

どうして防げるか（予防・対策）

- **バイタル異常パターン（p.306）**で発作を即検知。
- **Silent UI（p.331–335）**で自動救急連絡。

なぜ可能なのか（裏付け）

- 「Vital＋Silent 通報」を著作権範囲として包括保護。

セキュリティ上の意義

「沈黙していても事故は伝わる」→ 急病事故を封じる。

事例 10（2020 年 12 月 25 日：航空機パイロット急病事故）

- **構成パターン**：B 単体
- **該当ページ**：p.300–302, p.371–400

事故シナリオ

国際便のパイロットが飛行中に心筋梗塞を発症。心拍停止前の異常をセンサーが検知 → Silent 通報で副操縦士と地上管制に警告。

なぜ問題か

- 航空機事故は多数の命を危険に晒す。
- パイロット急病は過去にも墜落事故の要因。

どうして防げるか（予防・対策）

- **シナリオ別アルゴリズム検証（p.371–400）**で Vital 異常を高精度検知。
- **SilentTx（p.328–330）**で気付かれず通報。

なぜ可能なのか（裏付け）

- 特許出願ブロック（p.519–552）に「航空応用」を明記。

セキュリティ上の意義

「パイロット急病事故を飛行中に検知」→ 航空大事故を防止。

✅ 第 2 部まとめ

- **B パターン＝バイタル異常による事故検知**は、ATM での急病、飲酒運転、介護転倒、家庭内急病、航空機事故などをカバー。
- **なぜ可能か**：VitalScore・SilentTx・契約保護・特許請求項に裏付け。
- **事故防止の意義**：体が異常を示した瞬間に事故を通報 → 「事故の見逃しゼロ」を実現。

📘 第 3 部（事例 11〜15）：C パターン＝知財事故・便乗模倣事故防止

事例 11（2024 年 2 月 14 日：研究論文の剽窃事故）

- **構成パターン**：C 単体
- **該当ページ**：p.553–560, p.561–580, p.904–938

事故シナリオ

大学院生が他大学のコードを流用し、事故的に剽窃論文を提出。C システムが**一致スコア 0.9 超**を検知し提出をブロック。

なぜ問題か

- 剽窃は学術事故であり、研究者のキャリアや大学の信用を失墜。

どうして起きたか

従来の剽窃検出は「検知だけ」で、契約や収益補償まで接続できなかった。

どうして防げるか（予防・対策）

- **compareIP(), similarityScore()（p.571–580）**で即検知。
- **contractGen()（p.561–570）**で合法利用なら契約化。

なぜ可能なのか（裏付け）

- 特許出願（p.916–938）で「照合→契約→収益分配」が請求項化。

セキュリティ上の意義

「学術事故を検知し正規ルートへ修正」→ 信用喪失を防止。

事例 12（2023 年 8 月 30 日：災害便乗アプリ事故）

- **構成パターン**：C 単体
- **該当ページ**：p.631–700, p.621–630

事故シナリオ

大地震後、正規の防災アプリを模倣した**偽アプリ**が拡散。ユーザーが誤って利用し個人情報を喪失。C システムが契約照合で侵害を即検知・遮断。

なぜ問題か

- 偽アプリは災害時に「命綱の機能不全」を引き起こす事故源。

どうして起きたか

UI や文言を微妙に変えた模倣は、従来 DRM では見抜けなかった。

どうして防げるか（予防・対策）

- **契約文言差異封鎖（p.621–630）**で言い換え不正を無効化。
- **国際応用シナリオ（p.631–700）**で災害利用を網羅。

なぜ可能なのか（裏付け）

- 「結論一致＝侵害成立」を権利範囲で規定。

セキュリティ上の意義

「災害便乗型の模倣事故を即排除」→ 利用者の命を守る。

事例 13（2022 年 6 月 12 日：虚偽特許担保ローン事故）

- **構成パターン**：C 単体
- **該当ページ**：p.861–903, p.601–610

事故シナリオ

企業が収益性のない特許を担保にローンを申請。C システムが契約履歴と分配台帳を照合→虚偽担保を検出し事故的金融詐欺を阻止。

なぜ問題か

- 虚偽知財は**金融事故**を引き起こし銀行に損失を与える。

どうして起きたか

従来は知財評価が主観的で、嘘を通せてしまった。

どうして防げるか（予防・対策）

- **契約ログ（p.601–610）**で履歴照合。
- **収益モデル（p.861–903）**で定量化。

なぜ可能なのか（裏付け）

- 「知財流通の自動化」を本体に明記。

セキュリティ上の意義

「金融事故の芽を事前に潰す」。

事例 14（2021 年 11 月 5 日：翻訳差を悪用した契約事故）

- **構成パターン**：C 単体
- **該当ページ**：p.621–630, p.631–700

事故シナリオ

海外企業が契約翻訳差を利用し、事故的に支払い義務を逃れようとした。C が文言差異を侵害扱いし、強制的に支払いを確定。

なぜ問題か

- 翻訳差による契約事故は国際訴訟に発展する。

どうして起きたか

従来は「表現の違い」で契約をすり抜けられた。

どうして防げるか（予防・対策）

- **契約文言封鎖（p.621–630）**で言い換えを禁止。
- **越境契約処理（p.631–700）**で整合性を担保。

なぜ可能なのか（裏付け）

- 特許請求項に「翻訳差を封鎖」と記載。

セキュリティ上の意義

「国際契約事故を未然に防止」。

事例 15（2020 年 8 月 29 日：違法コピー災害寄付キャンペーン事故）

- **構成パターン**：C 単体
- **該当ページ**：p.701–800, p.801–860

事故シナリオ

豪雨災害の後、人気映画が「被災者支援の無料上映」として違法コピー配布。C システムが侵害を検知し遮断、正規契約に誘導。

なぜ問題か

- 災害時の「偽寄付上映」は支援活動を装った不正事故。

どうして起きたか

DRM は「コピー防止」に限界があり、寄付や上映の形を変えるとすり抜けられた。

どうして防げるか（予防・対策）

- **アルゴリズム評価（p.801–860）**で高精度照合。
- **契約生成（p.561–570）**で正規上映に変換。

なぜ可能なのか（裏付け）

- 「表現差があっても結論一致なら侵害」と規定。

セキュリティ上の意義

「災害を悪用した違法コピー事故を遮断」。

✅ 第 3 部まとめ

- **C パターン＝知財事故防止**は、剽窃・災害便乗アプリ・虚偽担保・翻訳差・寄付名目コピーといった「事故的な知財トラブル」を遮断。
- **なぜ可能か**：照合アルゴリズム、契約文言封鎖、収益分配ロジックが特許・著作権に裏付け済。
- **事故防止意義**：「模倣や便乗が事故を生まない社会基盤」を構築。

📘 第 4 部（事例 16〜20）：D・E パターン＝複合事故対応＋決済事故防止

事例 16（2024 年 9 月 10 日：学校での集団事故未然防止）

- **構成パターン**：D 単体（複合セーフティ網）
- **該当ページ**：p.941–960, p.1011–1030

事故シナリオ

児童が校庭で事故に巻き込まれた。叫び声（A）、心拍急上昇（B）、学校アプリでの利用不一致（C）が同時に発生。複合判定（D）が**重大事故シナリオ**と確定し、教員と救急に即通報。

なぜ問題か

- 学校事故は集団被害につながる。
- 単体検知だと「誤報」扱いで放置されがち。

どうして防げるか（予防・対策）

- **複合判定関数（p.961–970）**で信頼性を高める。
- **複合 UI（p.1001–1010）**で学校管理者に状況を一目で表示。

なぜ可能なのか（裏付け）

- 「命＋権利＋経済の三層モデル」と定義。

セキュリティ上の意義

「誤検知を防ぎつつ事故を見逃さない」→ 学校事故の早期対応。

事例 17（2023 年 3 月 11 日：災害時の物資配布事故防止）

- **構成パターン**：D 単体
- **該当ページ**：p.943–947, p.1031–1050

事故シナリオ

地震後、物資配布拠点で混乱が発生。虚偽申請やなりすましで事故的に物資不足が発生。D システムが通報（A）、バイタル（B）、契約ログ（C）を複合判定し、不正申請を遮断。

なぜ問題か

- 災害時は「偽被災者」による不正取得で本当の被災者が救済されない事故が起きる。

どうして防げるか（予防・対策）

- **複合稼働シナリオ（p.1031–1050）**で誤認を削減。
- **Silent 通報（p.1091–1110）**で裏側から監視。

なぜ可能なのか（裏付け）

- 複合システムが「行政サービス」応用を含むと記載。

セキュリティ上の意義

「災害時の物資配布事故を封じる」。

事例 18（2022 年 6 月 15 日：金融取引の改ざん事故）

- **構成パターン**：D→E（複合＋清算）
- **該当ページ**：p.1051–1070, p.1191–1210

事故シナリオ

企業が改ざんした契約データでローンを申請。D が異常を検知 → E が清算処理を拒否し事故的金融詐欺を防止。

なぜ問題か

- 改ざん契約は「金融事故」を引き起こす。

どうして防げるか（予防・対策）

- **複合閾値設定（p.1051–1070）**で多要素検証。
- **清算 Tx 群（p.1191–1210）**で決済を止める。

なぜ可能なのか（裏付け）

- 「通報＋Vital＋契約を直列化」と記載。

セキュリティ上の意義

「金融事故を決済段階で封鎖」。

事例 19（2021 年 2 月 28 日：国際送金トラブル事故）

- **構成パターン**：E 単体（清算・決済）
- **該当ページ**：p.1240–1260, p.1321–1340

事故シナリオ

企業が国際送金を行う際、虚偽契約を提出。E システムが契約不一致を検出 → 送金を遮断し、即ペナルティ精算。

なぜ問題か

- 国際送金の事故は国家間の信用問題に発展。

どうして防げるか（予防・対策）

- **清算ロジック（p.1240–1260）**で契約内容を精査。
- **Ledger API（p.1321–1340）**で履歴を保存。

なぜ可能なのか（裏付け）

- 「契約金額算出と即時清算」を明記。

セキュリティ上の意義

「国際金融事故を即封鎖」。

事例 20（2020 年 1 月 19 日：保険金不正請求事故）

- **構成パターン**：E 単体
- **該当ページ**：p.1261–1280, p.1341–1360

事故シナリオ

利用者が事故を偽装し、Vital データを改ざんして保険金請求。E が不一致を検出し支払いを停止。

なぜ問題か

- 保険金詐欺は「保険制度の事故」を引き起こす。

どうして防げるか（予防・対策）

- **契約条件照合（p.1240–1260）**で虚偽を判定。
- **CSV 証跡（p.1341–1360）**で記録を残す。

なぜ可能なのか（裏付け）

- 特許請求項で「契約履行の自動精算」を保護。

セキュリティ上の意義

「保険事故を自動判定で排除」。

✅ 第 4 部まとめ

- **D＝複合事故対応**：学校事故・災害便乗事故を三要素一致で高精度に検知。
- **E＝決済事故防止**：金融詐欺・国際送金トラブル・保険金詐欺を清算段階で封鎖。
- **事故防止意義**：人・契約・経済の三領域を横断的に守る「事故封鎖インフラ」。

📘 第 5 部（事例 21〜25）：F・G パターン＝再利用・二次流通事故防止

事例 21（2024 年 6 月 4 日：教育現場での教材再利用事故）

- **構成パターン**：F 単体（再利用封鎖）
- **該当ページ**：p.1240–1260, p.1335–1360

事故シナリオ

学校が契約期間終了後の防災教材アプリを翌年度も無断使用。サーバ側で**失効フラグ**を検知し自動遮断。

なぜ問題か

- 不正利用は著作権事故を招き、訴訟や教育現場の混乱に直結。

どうして起きたか

- 「昨年の教材データが残っている」ことを理由に再利用してしまう誤解。

どうして防げるか（予防・対策）

- **再利用検知ロジック（p.1240–1260）**で自動失効判定。
- **封鎖ログ保存（p.1341–1360）**で責任の所在を明確化。

セキュリティ上の意義

「教育事故を契約管理で封鎖」。

事例 22（2023 年 8 月 17 日：医療研究データの二次利用事故）

- **構成パターン**：F 単体
- **該当ページ**：p.1335–1360, p.1436–1450

事故シナリオ

病院が契約終了後の患者バイタルデータを「研究用」として二次提供。F が検知し遮断。

なぜ問題か

- 二次利用は個人情報事故を引き起こし、患者と研究機関双方に法的リスク。

どうして起きたか

- 「匿名化すれば問題ない」という誤解。

どうして防げるか（予防・対策）

- **失効ハッシュ記録（p.1341–1360）**で契約外利用を即検知。
- **再流通遮断アルゴリズム（p.1436–1450）**で外部提供を封鎖。

セキュリティ上の意義

「個人情報事故を匿名化の名目でも許さない」。

事例 23（2022 年 12 月 1 日：企業によるサブライセンス横流し事故）

- **構成パターン**：G 単体（二次流通制御）
- **該当ページ**：p.1504–1510, p.1521–1530

事故シナリオ

企業が災害支援アプリのライセンスを購入後、第三者に横流し。G システムが**正規ルート外の流通**を検出し遮断。

なぜ問題か

- サブライセンス横流しは契約事故であり、市場全体の信頼を失墜。

どうして起きたか

- 契約管理が一次ライセンスまでしか及んでいなかった。

どうして防げるか（予防・対策）

- **二次流通チェック API（p.1521–1530）**で横流しを即検知。
- **正規ルート限定（p.1504–1510）**で不正流通を遮断。

セキュリティ上の意義

「不正横流し事故を技術で未然封鎖」。

事例 24（2021 年 10 月 23 日：電子書籍コピー事故）

- **構成パターン**：F＋G 連携
- **該当ページ**：p.1436–1450, p.1665–1667

事故シナリオ

豪雨災害後、「支援目的」と称して人気電子書籍が違法コピーされ P2P で流通。F がコピーを失効化、G が二次流通を検知して遮断。

なぜ問題か

- 善意を装った不正コピーは著作権事故であり、出版業界に大打撃。

どうして起きたか

- DRM は形式変換（圧縮や改変）に弱く、事故的流通を許していた。

どうして防げるか（予防・対策）

- **封鎖ログ（p.1436–1450）**でコピー履歴を証跡化。
- **再循環台帳（p.1665–1667）**で不正ルートを記録。

セキュリティ上の意義

「形式を変えてもコピー事故は成立しない」。

事例 25（2020 年 5 月 9 日：国際標準化会議での盗用事故防止）

- **構成パターン**：G 単体
- **該当ページ**：p.1541–1564, p.1665–1667

事故シナリオ

国際会議で海外企業が日本の災害対応アルゴリズムを自社発と偽って提出。G が**正規台帳との不一致**を検知 → 提出却下。

なぜ問題か

- 国際標準化の場での盗用事故は国家レベルの経済損失。

どうして防げるか（予防・対策）

- **標準化提案記録（p.1541–1564）**で正規ルートを証明。
- **経済効果データ（p.1665–1667）**で導入実績を補強。

セキュリティ上の意義

「国際舞台で事故的盗用を封鎖」。

✅ 第 5 部まとめ

- **F＝再利用封鎖**：教育・医療・出版で「契約終了後の再利用事故」を防ぐ。
- **G＝二次流通制御**：横流しや盗用による「不正流通事故」を遮断。
- **事故防止意義**：混乱期や善意を装った不正でも、**再利用・二次流通の事故を社会的にゼロ化**。

📘 第 6 部（事例 26〜30）：H・I・J パターン＝証拠保存・復元・国際事故対応

事例 26（2024 年 2 月 1 日：寄付金詐欺裁判での証拠事故防止）

- **構成パターン**：H 単体（最終アーカイブ・監査）
- **該当ページ**：p.1391–1410, p.1411–1430

事故シナリオ

豪雨災害時の「寄付金詐欺事件」で、通報ログが改ざんされ証拠能力を失う恐れがあった。H システムに保存されていた **Merkle Root＋TSA 署名付ログ** が証拠として採用され、事故的な冤罪を回避。

なぜ問題か

- 証拠改ざんは「事故的冤罪」や「不起訴事故」を引き起こす。

どうして防げるか（予防・対策）

- **不可逆保存（p.1411–1430）**で改ざんを不可能化。
- **API /audit /archive**で証跡を検証可能に。

セキュリティ上の意義

「証拠事故を防ぎ、裁判を守る」。

事例 27（2023 年 5 月 11 日：病院サーバ障害と医療記録事故）

- **構成パターン**：I 単体（特別保存・復元）
- **該当ページ**：p.1520–1540, p.1581–1600

事故シナリオ

災害時の停電＋ランサム攻撃で病院の患者カルテが破壊。I システムが **recoverEvidence(), rebuildLedger()** を実行し、事故的に失われた証拠を回復。

なぜ問題か

- 医療記録の喪失は「事故責任追及不可」という重大リスク。

どうして防げるか（予防・対策）

- **復元アルゴリズム（p.1520–1540）**でデータを再生成。
- **再保存ハッシュ（p.1581–1600）**で再度改ざん不能に保存。

セキュリティ上の意義

「消えた証拠を蘇らせ事故隠蔽を阻止」。

事例 28（2022 年 7 月 22 日：国際災害支援での知財盗用事故）

- **構成パターン**：I＋H 連携
- **該当ページ**：p.1665–1670, p.1699–1701

事故シナリオ

災害救援プロジェクトで、日本発の技術が他国に盗用され、サーバ攻撃で証拠が消去。I システムが証拠を復元し、H で監査証跡を付与 → 国際裁判所で事故防止の決定。

なぜ問題か

- 国際協力を悪用した知財盗用事故は国家間紛争に発展。

どうして防げるか（予防・対策）

- **/recover, /restore API（p.1601–1620）**で証拠復元。
- **H アーカイブ（p.1391–1430）**で国際証跡として提示。

セキュリティ上の意義

「国際事故を証拠復元で防止」。

事例 29（2021 年 11 月 30 日：災害復興基金の不正請求事故）

- **構成パターン**：J 単体（特殊用途・人道利用）
- **該当ページ**：p.1632–1664, p.1668–1670

事故シナリオ

震災後、偽被災団体が復興基金を不正請求。J システムが特殊利用モードで正規被災者と不正請求者を自動仕分け。

なぜ問題か

- 災害時の基金不正利用は「支援事故」を生み、救済が滞る。

どうして防げるか（予防・対策）

- **specialUsePermit()（p.1665–1667）**で人道利用を判定。
- **緊急 UI（p.1668–1670）**で迅速認証。

セキュリティ上の意義

「復興支援の事故を防ぎ、本当に必要な人に届く」。

事例 30（2020 年 4 月 9 日：パンデミック研究データ盗用事故）

- **構成パターン**：J 単体（特殊用途・国際協力）
- **該当ページ**：p.1632–1664, p.1699–1701

事故シナリオ

感染症パンデミック時、海外製薬企業が日本企業の研究データを無断利用し特許出願。J システムが国際協力ルートを発動し、WHO へ正規権利者を通知。不正出願を却下。

なぜ問題か

- パンデミック時は「緊急」を口実に知財盗用事故が多発。

どうして防げるか（予防・対策）

- **exceptionRoute()（p.1665–1667）**で特殊条件を制御。
- **国際証跡ログ（p.1671–1680）**で権利を裏付け。

セキュリティ上の意義

「世界的危機でも知財事故を成立させない」。

✅ 第 6 部まとめ

- **H＝証拠保存**：寄付金詐欺裁判などで証拠事故を防止。
- **I＝復元処理**：攻撃や障害で失われた記録を復元し、事故隠蔽を阻止。
- **J＝特殊用途**：災害基金やパンデミック研究での事故的不正を封鎖。
- **全体意義**：事故後の「証拠・資金・知財」を守り抜く、社会的セーフティインフラ。

📘 第 1 部（事例 1〜5）：A パターン＝緊急通報と人命救助

事例 1（2024 年 3 月 12 日：通学路での交通事故から児童救命）

- **構成パターン**：A 単体
- **該当ページ**：p.98–108（GPS・位置情報）、p.110–133（UI・Silent 通報）、p.134–145（危険音検知）

人命リスクのシナリオ

下校中の児童が交差点で車両にはねられ、意識を失う。児童のランドセル端末が**衝突音＋「助けて」の発声＋GPS 位置**を検知し、即座に救急へ通報。

なぜ問題か

- 子供は事故直後に操作できず、発見が遅れれば致命的。

どうして起きたか

従来の防犯ブザーは「人が押す」前提であり、事故では作動できなかった。

どうして防げるか（予防・対策）

- **FFT 音響解析（p.134–145）**で衝突音を判定。
- **Silent 通報 UI（p.110–133）**で周囲に悟られず即通報。

なぜ可能なのか（裏付け）

- 特許請求項（p.294–297）に「音声＋位置による自動通報」を明記。

人命セキュリティ上の意義

「事故直後の救命率を高める」。

事例 2（2023 年 9 月 5 日：深夜転倒事故での女性救助）

- **構成パターン**：A 単体
- **該当ページ**：p.98–108, p.110–133

人命リスクのシナリオ

女性が深夜に転倒し骨折。声を出せなかったが、**転倒音＋位置異常**を検出して自動通報。

なぜ問題か

- 夜間の事故は「発見遅れ＝低体温症や死亡リスク増大」。

どうして防げるか（予防・対策）

- **GPS＋Wi-Fi RTT 位置照合（p.98–108）**で通常行動と乖離を判定。
- **Silent 通報 UI（p.110–133）**で本人が操作せずとも救助要請。

なぜ可能なのか（裏付け）

- 設計書（p.109）に閾値・構成要素を規定。

人命セキュリティ上の意義

「声を上げられなくても命が救われる」。

事例 3（2022 年 11 月 28 日：高齢者宅ガス爆発からの救命）

- **構成パターン**：A 単体
- **該当ページ**：p.134–145, p.83–97（通報ログ保存）

人命リスクのシナリオ

高齢者宅でガス爆発。爆発音を検知、GPS 位置と合わせて消防に自動通報。

なぜ問題か

- 爆発は**一瞬で意識を失い通報不可**。

どうして防げるか（予防・対策）

- **異常音解析（p.134–145）**で爆発音を瞬時に検知。
- **証跡保存（p.83–97）**で消防が二次災害原因を特定。

なぜ可能なのか（裏付け）

- 本体に「災害事故時の救命応用」が記載 。

人命セキュリティ上の意義

「災害時に通報不能でも命が守られる」。

事例 4（2021 年 8 月 2 日：高速道路での多重衝突事故）

- **構成パターン**：A 単体
- **該当ページ**：p.56–82（API 警察連携）, p.32（証拠保存）

人命リスクのシナリオ

高速道路で玉突き事故。最初の衝突音を検知した車載端末が即通報。

なぜ問題か

- 多重事故は「初動の遅れ」で死傷者が増大。

どうして防げるか（予防・対策）

- **API 連携（p.56–82）**で警察・消防へ直結。
- **録音＋ログ保存（p.32）**で事故解析可能。

なぜ可能なのか（裏付け）

- 本体に「交通事故：バイタル停止で救急通報」と明記 。

人命セキュリティ上の意義

「事故直後の救護で死傷者を減らす」。

事例 5（2020 年 7 月 6 日：地震倒壊事故での救命）

- **構成パターン**：A 単体
- **該当ページ**：p.26–29（音声＋位置通報）, p.32（救助フロー）

人命リスクのシナリオ

大地震で住宅倒壊。瓦礫下の「助けて」の声を検知し GPS と連動 → 消防本部へ Silent 通報。

なぜ問題か

- 倒壊事故は「声が外に届かない」ため救助が遅れる。

どうして防げるか（予防・対策）

- **音声＋位置照合（p.26–29）**で確実に救助要請。
- **Silent 通報 UI（p.110–133）**で被災者が操作不要。

なぜ可能なのか（裏付け）

- 第 4 部で「災害応用」が明記 。

人命セキュリティ上の意義

「声が外に届かなくても命を救う」。

✅ 第 1 部まとめ

- A パターンは **交通事故・転倒事故・爆発事故・多重衝突・地震倒壊** という典型的な人命リスクに対応。

- **なぜ可能か**：音響解析・GPS 照合・Silent 通報・ログ証跡保存が特許／設計仕様に裏付けられている。
- **人命セキュリティ意義**：人が操作できない極限状況でも「声・音・位置」が命を守るトリガーになる。

📘 第 2 部（事例 6〜10）：B パターン＝バイタル監視による命の保護

事例 6（2024 年 5 月 21 日：ATM での急病事故）

- **構成パターン**：B 単体
- **該当ページ**：p.300–306（技術概要・事例）, p.321–322（SilentTx API）

人命リスクのシナリオ

高齢者が ATM 操作中に心筋梗塞で倒れる。システムが**心拍急上昇＋酸素飽和度低下**を検知し、Silent 通報で銀行職員と救急へ即通知。

なぜ問題か

- 金融機関は「取引中の事故」を即発見できず、救命が遅れる。

どうして防げるか（予防・対策）

- **VitalScore（p.307–310）**で心拍・呼吸を数値化。
- **SilentTx API（p.321–322）**で即通報。

なぜ可能なのか（裏付け）

- 権利範囲に「バイタル＋通報構成を包括保護」と明記。

人命セキュリティ意義

「ATM が救命端末になる」。

事例 7（2023 年 10 月 11 日：飲酒運転事故の防止）

- **構成パターン**：B 単体
- **該当ページ**：p.300–302（基礎説明）, p.311–315（モジュール設計）

人命リスクのシナリオ

飲酒したドライバーがエンジン始動 → 呼吸異常・血中酸素低下を検知 → エンジンはロックされ、家族と警察に Silent 通報。

なぜ問題か

- 飲酒運転は死亡事故率が高い。

どうして防げるか（予防・対策）

- **VitalProc（p.311–315）**で呼吸と酸素濃度を監視。
- **Silent UX（p.328–330）**で気付かれずに警告送信。

なぜ可能なのか（裏付け）

- 本体に「飲酒運転防止」事例として明記。

人命セキュリティ意義

「車が命の守護者になる」。

事例 8（2022 年 2 月 14 日：介護施設での転倒事故）

- **構成パターン**：B 単体
- **該当ページ**：p.302（社会的役立ち方）, p.336–370（実証データ）

人命リスクのシナリオ

介護施設で高齢者が転倒。巡回前に**心拍急上昇＋皮膚電位異常**を検知し、家族と医師へ Silent 通報。

なぜ問題か

- 転倒発見が遅れると、骨折から寝たきり、死亡につながる。

どうして防げるか（予防・対策）

- **実証データ（p.336–370）**で異常検出率を確認。
- **擬似コード（p.316–320）**で「異常→SilentTx」フローを設計。

なぜ可能なのか（裏付け）

- 本体に「介護見守り」応用を明記。

人命セキュリティ意義

「転んだ瞬間に命が救われる」。

事例 9（2021 年 4 月 1 日：家庭内急病事故）

- **構成パターン**：B 単体
- **該当ページ**：p.304–305（事例解説）, p.331–335（UI 設計）

人命リスクのシナリオ

家庭で心臓発作を起こした女性。声を上げられず動けないが、心拍異常を検知 → スマートウォッチが Silent 通報で救急要請。

なぜ問題か

- 発見が遅れると孤独死につながる。

どうして防げるか（予防・対策）

- **バイタル異常パターン（p.304–305）**で発作検知。
- **Silent UI（p.331–335）**で救急通報。

なぜ可能なのか（裏付け）

- 「Vital＋Silent 通報」を著作権範囲として包括保護。

人命セキュリティ意義

「沈黙していても命が守られる」。

事例 10（2020 年 12 月 25 日：航空機パイロット急病事故）

- **構成パターン**：B 単体
- **該当ページ**：p.300–302（概要）, p.371–400（航空応用検証）

人命リスクのシナリオ

国際便のパイロットが心筋梗塞を発症。心拍停止前の異常を検知 → Silent 通報で副操縦士と管制に警告。

なぜ問題か

- パイロット急病は航空大事故に直結。

どうして防げるか（予防・対策）

- **シナリオ別検証（p.371–400）**で Vital 異常検知の有効性を確認。
- **Silent 通報 UX（p.328–330）**で犯人や乗客に気付かれず通報。

なぜ可能なのか（裏付け）

- 特許請求項群に「航空応用」が含まれる。

人命セキュリティ意義

「数百人の命を未然に守る」。

✅ 第 2 部まとめ

- **B パターン＝バイタル監視**は、ATM 急病・飲酒運転・介護転倒・家庭内発作・航空機事故といった人命に直結する事故をカバー。
- **なぜ可能か**：VitalScore、SilentTx、実証データ、特許請求項に裏付けられている。
- **意義**：身体が示す異常を事故シグナルに変換し、**「命の見逃しゼロ」**を実現。

📘 第 3 部（事例 11〜15）：C パターン＝知財・契約事故が人命に及ぼす影響の防止

事例 11（2024 年 2 月 14 日：医療 AI 研究の剽窃事故防止）

- **構成パターン**：C 単体
- **該当ページ**：p.553–560（知財照合概要）, p.561–580（契約生成）, p.904–938（特許請求項）

人命リスクのシナリオ

他大学が開発した心疾患診断 AI アルゴリズムを盗用した研究が論文に掲載され、誤診を誘発 → 患者の命を脅かす事故に発展する可能性。

なぜ問題か

- 知財剽窃は「質の低い模倣研究」により誤診・医療事故を生む。

どうして起きたか

従来の剽窃検知は「発見のみ」で、流用研究の流通を止められなかった。

どうして防げるか（予防・対策）

- **compareIP()（p.571–580）**で剽窃検出。
- **contractGen()（p.561–570）**で正規利用なら契約化し精度担保。

なぜ可能なのか（裏付け）

- 特許明細（p.916–938）に「知財照合＋契約生成」が請求項化。

人命セキュリティ意義

「医療研究の質を守る＝患者の命を守る」。

事例 12（2023 年 8 月 30 日：災害時の防災アプリ模倣事故防止）

- **構成パターン**：C 単体
- **該当ページ**：p.621–630（契約文言封鎖）, p.631–700（越境契約）

人命リスクのシナリオ

災害後に正規防災アプリを模倣した偽アプリが登場。誤作動で避難誘導が間違い → 住民の命に直接被害。

なぜ問題か

- 模倣アプリは「誤誘導事故」を生む。

どうして起きたか

従来の DRM は UI や表現を変えた模倣を防げなかった。

どうして防げるか（予防・対策）

- **契約文言差異封鎖（p.621–630）**で言い換え回避を防止。
- **越境契約処理（p.631–700）**で海外拡散も封鎖。

なぜ可能なのか（裏付け）

- 「結論一致＝侵害成立」を規定（p.3–4）。

人命セキュリティ意義

「偽アプリによる命の危険を封鎖」。

事例 13（2022 年 6 月 12 日：虚偽特許担保ローンと医薬品供給事故）

- **構成パターン**：C 単体
- **該当ページ**：p.861–903（経済試算・知財担保応用）, p.601–610（契約ログ）

人命リスクのシナリオ

製薬会社が未承認の薬剤特許を担保に融資を得て供給 → 実際は効果がなく、副作用で死亡事故。

なぜ問題か

- 虚偽知財は「医薬品事故」を誘発。

どうして起きたか

従来は知財担保の収益実績を確認できなかった。

どうして防げるか（予防・対策）

- **契約ログ（p.601–610）**で収益履歴を照合。
- **経済モデル（p.861–903）**で信頼性を数値化。

なぜ可能なのか（裏付け）

- 本体に「知財担保の信用評価」を記載（p.861–903）。

人命セキュリティ意義

「不正知財による医薬事故を阻止」。

事例 14（2021 年 11 月 5 日：翻訳差悪用による災害支援契約事故）

- **構成パターン**：C 単体
- **該当ページ**：p.621–630（契約文言封鎖）, p.631–700（国際契約）

人命リスクのシナリオ

海外の NGO が契約翻訳差を利用し、災害支援物資を供給せずに逃亡。被災地で命に関わる物資不足が発生。

なぜ問題か

- 契約事故は「支援遅延＝命の損失」。

どうして起きたか

従来は「翻訳差」を口実に契約を逃れられた。

どうして防げるか（予防・対策）

- **契約文言封鎖（p.621–630）**で翻訳差を無効化。
- **越境契約処理（p.631–700）**で国際整合性を保証。

なぜ可能なのか（裏付け）

- 特許請求項（p.916–938）に国際契約を含む。

人命セキュリティ意義

「支援契約の不履行を封鎖し人命を守る」。

事例 15（2020 年 8 月 29 日：災害寄付キャンペーンでの違法コピー事故）

- **構成パターン**：C 単体
- **該当ページ**：p.701–800（コピー検知）, p.801–860（検証ログ）

人命リスクのシナリオ

「災害支援寄付上映」と称して違法コピー映画が配布 → 実際には寄付が詐取され、被災者救済が遅れた。

なぜ問題か

- 違法コピーは「支援事故」を生み、本来救われる命が失われる。

どうして起きたか

従来 DRM は「コピー検知のみ」で寄付の流れを追えなかった。

どうして防げるか（予防・対策）

- **compareIP＋blockTx（p.701–800）**で即遮断。
- **契約生成（p.561–570）**で正規収益を被災者に回す。

なぜ可能なのか（裏付け）

- 「表現差・記号差を問わず侵害成立」と明記（p.621）。

人命セキュリティ意義

「偽寄付による救済事故を防止」。

✅ 第 3 部まとめ

- **C パターン＝知財・契約事故防止**は、研究剽窃、災害模倣アプリ、虚偽担保、翻訳差悪用、違法コピー寄付などを対象。
- **人命に直結するリスク**（誤診、物資不足、寄付詐欺など）を封鎖。
- **なぜ可能か**：照合アルゴリズム・契約生成・文言封鎖・収益分配が特許・設計仕様に裏付け済。

📘 第 4 部（事例 16〜20）：D・E パターン＝複合人命セーフティ＋生命保険・補償制御

事例 16（2024 年 9 月 10 日：学校事故での複合人命検知）

- **構成パターン**：D 単体（複合セーフティ網）
- **該当ページ**：p.941–960（複合判定エンジン）, p.1011–1030（UI 統合）

人命リスクのシナリオ

校庭で児童が事故に巻き込まれる。
「助けて」の叫び（A）、心拍急上昇（B）、利用ログ異常（C）が同時発生。D システムが三重一致を検知し、**重大事故→救急・学校関係者へ即通知**。

なぜ問題か

- 学校事故は「誤報」扱いで対応が遅れると命に関わる。

どうして防げるか（予防・対策）

- **複合判定関数（p.961–970）**で三要素を統合し信頼性を高める。
- **統合 UI（p.1001–1010）**で管理者に状況を即座に伝達。

人命セキュリティ意義

「誤報を減らし本物の事故だけを即検知」→ 児童の命を守る。

事例 17（2023 年 3 月 11 日：災害時の物資不足による人命事故防止）

- **構成パターン**：D 単体
- **該当ページ**：p.943–947（災害応用）, p.1031–1050（複合稼働シナリオ）

人命リスクのシナリオ

大地震後、救援物資を「なりすまし」が奪取。被災者に食糧・医薬品が届かず命に関わる。
D が通報（A）、バイタル確認（B）、契約情報（C）を複合判定し、**正規被災者のみを認証**。

なぜ問題か

- 災害時は物資不足→弱者の命に直結。

どうして防げるか（予防・対策）

- **複合シナリオ（p.1031–1050）**で誤認を減少。
- **Silent 通報（p.1091–1110）**で不正を裏で排除。

人命セキュリティ意義

「災害便乗不正を排除＝命を救う」。

事例 18（2022 年 6 月 15 日：金融改ざんと命の保障事故）

- **構成パターン**：D→E（複合＋清算）
- **該当ページ**：p.1051–1070（複合閾値設定）, p.1191–1210（清算制御）

人命リスクのシナリオ

医療補償契約を企業が改ざん → 患者に補償が届かず治療が遅れ、命が危険に。
D が異常検知、E が清算を停止して事故を防止。

なぜ問題か

- 偽造契約は「補償金不払い事故＝治療遅延」に直結。

どうして防げるか（予防・対策）

- **複合閾値設定（p.1051–1070）**で改ざんを検知。
- **清算 Tx 群（p.1191–1210）**で契約不一致時に支払いを遮断。

人命セキュリティ意義

「補償事故を封じ、命に資金を即届ける」。

事例 19（2021 年 2 月 28 日：国際送金事故での医療支援遅延防止）

- **構成パターン**：E 単体（清算・決済）
- **該当ページ**：p.1240–1260（清算ロジック）, p.1321–1340（Ledger API）

人命リスクのシナリオ

国際 NGO が医療物資購入のための送金を実行 → 契約不一致があり送金が止まる。
E が自動判定で虚偽契約を排除、正規契約のみ送金→現場で命を救う物資が届く。

なぜ問題か

- 国際金融の事故＝現場の医療資源不足→命の危機。

どうして防げるか（予防・対策）

- **清算ロジック（p.1240–1260）**で条件を即判定。
- **Ledger 保存（p.1321–1340）**で履歴を証跡化。

人命セキュリティ意義

「偽契約送金を止め、命に必要な資金を守る」。

事例 20（2020 年 1 月 19 日：保険金不正請求事故と人命リスク防止）

- **構成パターン**：E 単体
- **該当ページ**：p.1261–1280（契約条件照合）, p.1341–1360（CSV 台帳）

人命リスクのシナリオ

虚偽の事故申請で保険金が不正に支払われる → 本来必要な患者への資金が不足、治療が遅れ命の危険。
E が条件照合で不一致を検知し、支払いを停止。

なぜ問題か

- 保険金詐欺は「本来の救済資金」を奪い、命に直結する。

どうして防げるか（予防・対策）

- **契約条件照合（p.1240–1260）**で自動チェック。
- **CSV 保存（p.1341–1360）**で監査可能に。

人命セキュリティ意義

「資金を正当に命へ届ける」。

✅ 第 4 部まとめ

- **D パターン**＝三重セーフティ網により「誤報削減＋真の命リスク事故を即検知」。
- **E パターン**＝清算・決済で「補償・保険資金を命へ正確に届ける」。
- **全体意義**：教育事故、災害物資不足、医療補償、保険金不正といった「命に直結する事故」を封鎖。

📘 第 5 部（事例 21〜25）：F・G パターン＝再利用・二次流通が命に関わるリスク防止

事例 21（2024 年 6 月 4 日：学校教材の無断再利用で防災訓練が機能不全）

- **構成パターン**：F 単体（再利用封鎖）
- **該当ページ**：p.1240–1260（清算ロジック）, p.1335–1360（失効ログ）

人命リスクのシナリオ

学校が契約期限切れの防災教材アプリをそのまま利用。古い情報で避難訓練を実施 → 誤誘導で児童が危険に。

なぜ問題か

- 教材の無断再利用＝古い情報による「命に関わる事故」を誘発。

どうして防げるか（予防・対策）

- **再利用検知（p.1240–1260）**で自動失効判定。
- **失効ログ（p.1335–1360）**で利用状況を監査。

人命セキュリティ意義

「命に関わる誤情報事故を封じる」。

事例 22（2023 年 8 月 17 日：医療データ二次流用で誤診リスク）

- **構成パターン**：F 単体
- **該当ページ**：p.1335–1360（失効記録）, p.1436–1450（再流通遮断）

人命リスクのシナリオ

病院が契約失効後のバイタルデータを研究機関に再利用。データが古く精度を欠き、医療研究が誤診を誘発。

なぜ問題か

- 無断再利用は「誤診事故」を生み命を危険にさらす。

どうして防げるか（予防・対策）

- **失効ハッシュ（p.1341–1360）**で利用可否を判定。
- **遮断アルゴリズム（p.1436–1450）**で不正再流通を封鎖。

人命セキュリティ意義

「古いデータ利用による命の危険を防ぐ」。

事例 23（2022 年 12 月 1 日：救急アプリのサブライセンス横流し事故）

- **構成パターン**：G 単体（二次流通制御）
- **該当ページ**：p.1504–1510（正規流通ルート）, p.1521–1530（チェック API）

人命リスクのシナリオ

企業が救急アプリのライセンスを第三者に横流し。不正版が導入され誤作動→現場で救急要請が届かず人命危機。

なぜ問題か

- 横流し版は品質保証がなく「機能不全事故」を生む。

どうして防げるか（予防・対策）

- **二次流通チェック API（p.1521–1530）**で横流しを検知。

- **正規ルートのみ通過許可（p.1504–1510）。**

人命セキュリティ意義

「横流しによる命の事故を封鎖」。

事例 24（2021 年 10 月 23 日：電子書籍コピーで避難情報が誤伝達）

- **構成パターン**：F＋G 連携
- **該当ページ**：p.1436–1450（封鎖ログ）, p.1665–1667（再循環台帳）

人命リスクのシナリオ

豪雨災害後、避難マニュアル電子書籍がコピー配布 → 改変され避難経路が誤って表示 → 住民が誤誘導され人命危機。

なぜ問題か

- 違法コピーは「避難誘導事故」を引き起こす。

どうして防げるか（予防・対策）

- **封鎖 CSV（p.1436–1450）**でコピー履歴を記録。
- **再循環台帳（p.1665–1667）**で不正ルートを追跡。

人命セキュリティ意義

「コピー事故による避難被害を根絶」。

事例 25（2020 年 5 月 9 日：国際標準化会議での災害技術盗用事故）

- **構成パターン**：G 単体（正規再循環）
- **該当ページ**：p.1541–1564（標準化提案記録）, p.1665–1667（経済効果データ）

人命リスクのシナリオ

海外企業が災害避難技術を自社開発と偽って国際会議に提出。不正技術が採用され、実際の災害現場で誤作動→人命を危険にさらす。

なぜ問題か

- 標準化の場での盗用事故は「現場の命のリスク」に直結。

どうして防げるか（予防・対策）

- **標準化記録（p.1541–1564）**で正規ルートを証明。
- **経済効果データ（p.1665–1667）**で導入実績を裏付け。

人命セキュリティ意義

「偽標準が命を奪う事故を防止」。

✅ 第 5 部まとめ

- **F パターン＝再利用封鎖**：学校・医療・出版における「命に関わる誤情報事故」を防止。
- **G パターン＝二次流通制御**：救急・出版・国際標準での横流しや盗用による人命リスクを排除。
- **人命セキュリティ意義**：再利用・二次流通の「事故由来の死」を社会からなくす。

📘 第 6 部（事例 26〜30）：H・I・J パターン＝証拠保存・復元・国際事故対応で命を守る

事例 26（2024 年 2 月 1 日：寄付金詐欺裁判で命を守る証拠保存）

- **構成パターン**：H 単体（アーカイブ・監査）
- **該当ページ**：p.1391–1410（監査ログ生成）, p.1411–1430（改ざん防止保存）

人命リスクのシナリオ

豪雨災害時に発生した寄付金詐欺。寄付が不正流用され、被災地への救援が遅れ命が危険に。被害者の通報ログを H が **Merkle Root＋TSA 署名付保存**し、裁判で有罪確定→救援資金が被災者に戻る。

なぜ問題か

- 証拠がなければ詐欺を裁けず、被災者が命を落とす。

どうして防げるか（予防・対策）

- **WORM＋電子署名（p.1411–1430）**で証拠改ざんを防止。

人命セキュリティ意義

「証拠事故を防ぎ、命に資金を届ける」。

事例 27（2023 年 5 月 11 日：病院サーバ障害で消えた命の記録を復元）

- **構成パターン**：I 単体（復元処理）
- **該当ページ**：p.1520–1540（復元アルゴリズム）, p.1581–1600（再保存方式）

人命リスクのシナリオ

病院がランサム攻撃を受け、災害時の患者カルテが消失。I が**recoverEvidence(), rebuildLedger()**で復元し、治療が続行され命を救った。

なぜ問題か

- 記録喪失＝誤治療や治療中断→命に直結。

どうして防げるか（予防・対策）

- **回復アルゴリズム（p.1520–1540）**で失われた記録を再生。
- **再保存ハッシュ（p.1581–1600）**で改ざん不可に。

人命セキュリティ意義

「記録を取り戻す＝命を取り戻す」。

事例 28（2022 年 7 月 22 日：国際災害支援での知財盗用事故防止）

- **構成パターン**：I＋H 連携
- **該当ページ**：p.1665–1670（国際利用例）, p.1699–1701（終章・人道利用）

人命リスクのシナリオ

災害救援技術が海外企業に盗用され、誤作動アプリが国際支援に使われる → 避難誘導失敗で人命危機。
I が証拠を復元し、H が監査証跡を付与→裁判で盗用排除、正規技術に差し替え。

なぜ問題か

- 偽技術は「誤避難誘導＝命の事故」を生む。

どうして防げるか（予防・対策）

- **/recover, /restore API（p.1601–1620）**で破壊証拠を復元。
- **H アーカイブ（p.1391–1430）**で不可逆証跡に。

人命セキュリティ意義

「国際支援の質を守り命を守る」。

事例 29（2021 年 11 月 30 日：災害復興基金の不正請求阻止）

- **構成パターン**：J 単体（特殊用途・人道利用）
- **該当ページ**：p.1632–1664（特別利用シナリオ）, p.1668–1670（人道 UI）

人命リスクのシナリオ

震災後、偽団体が復興基金を不正請求。被災者に資金が届かず命が危険に。
J が**specialUsePermit()**で正規被災者のみ認証→資金を即送金。

なぜ問題か

- 支援資金が奪われると被災者の命が危険に。

どうして防げるか（予防・対策）

- **特別利用モード（p.1632–1664）**で人道条件を確認。

人命セキュリティ意義

「偽申請を封じ、命を支える基金を守る」。

事例 30（2020 年 4 月 9 日：パンデミック時の研究データ盗用事故阻止）

- **構成パターン**：J 単体（特殊用途・国際協力）
- **該当ページ**：p.1632–1664（国際特例処理）, p.1699–1701（終章・国際展開）

人命リスクのシナリオ

感染症パンデミック時、海外製薬企業が日本企業のデータを盗用し特許申請。誤ワクチンが流通し、命に危険。
J が国際協力ルートを発動→WHO へ正規権利者を通知。不正出願を阻止。

なぜ問題か

- 偽ワクチン流通＝世界規模で命の危険。

どうして防げるか（予防・対策）

- **exceptionRoute()（p.1665–1667）**で特殊条件利用を制御。
- **国際証跡ログ（p.1671–1680）**で権利を裏付け。

人命セキュリティ意義

「パンデミック時でも命を守る」。

✅ 第 6 部まとめ

- **H＝証拠保存**：寄付金詐欺などで「証拠改ざんによる命の危険」を防止。
- **I＝復元処理**：サーバ攻撃や障害で消えた命の記録を復元。
- **J＝特殊用途**：災害基金やパンデミック時の命の危機を国際協力で封鎖。
- **総合意義**：事故後・災害時・国際危機でも「証拠・資金・技術」を守り抜き、命を救う社会的セーフティインフラを構築。

📘 第 1 部（事例 1〜5）：A パターン＝緊急通報と社会的インフラ応用

事例 1（2024 年 3 月 12 日：公共交通機関の安全運行）

- **構成パターン**：A 単体
- **該当ページ**：p.25–32（緊急通報概要）, p.56–82（外部 API 連携）, p.110–133（Silent UI）

シナリオ（その他の焦点）

バスや電車の運転士が異常事態を察知した際、**音声入力や車内の異常音**がトリガーとなり、自動的に運行管理センターへ通報。遅延や事故が発生する前に対応が可能に。

なぜ問題か

- 公共交通では「運転士が通報できない状況」＝広域混乱。

どうして起きたか

従来は「無線連絡」に依存し、情報伝達が遅れがち。

どうして防げるか（予防・対策）

- **API 連携（p.56–82）**で運行システムと接続。
- **Silent UI（p.110–133）**で乗客に混乱を与えず裏で通報。

なぜ可能なのか（裏付け）

- 本体に「外部サービス連携による緊急通報」の構造を明記。

社会的意義

「交通インフラ全体の安全性が向上」。

事例 2（2023 年 9 月 5 日：都市防犯ネットワークとの統合）

- **構成パターン**：A 単体
- **該当ページ**：p.26–30（発話検知）, p.220–224（危険ワード辞書）

シナリオ

市街地に設置された公共カメラやマイクが「助けて」「火事だ」などの声を検知 → 自動で防犯センターへ通知。市民がボタンを押さずとも都市レベルで危機管理。

なぜ問題か

- 大都市では警備員や警察官が全域をカバーできない。

どうして起きたか

従来は「通報＝人の操作」に依存していた。

どうして防げるか（予防・対策）

- **危険ワード辞書（p.220–224）**で自動検知。
- **Silent 通報（p.110–133）**で周囲に混乱を与えず処理。

なぜ可能なのか（裏付け）

- 「発話認識＋辞書」の実装が仕様に明記。

社会的意義

「都市そのものがセーフティネット化」。

事例 3（2022 年 11 月 28 日：企業 BCP〈事業継続計画〉との連携）

- **構成パターン**：A 単体
- **該当ページ**：p.83–97（ログ保存）, p.98–108（位置情報）, p.134–145（音響解析）

シナリオ

企業オフィスで火災や地震発生時、**異常音＋従業員の声＋位置情報**が自動記録され、BCP システムと連動して避難誘導・社員安否確認に利用。

なぜ問題か

- 災害時に「誰がどこにいたか」が把握できないと避難が混乱。

どうして起きたか

従来は「手動点呼」や「紙の安否確認」で時間がかかっていた。

どうして防げるか（予防・対策）

- **通報ログ保存（p.83–97）**で証跡化。
- **位置照合（p.98–108）**で安否把握を自動化。

なぜ可能なのか（裏付け）

- 本体に「緊急通報ログの保存・証跡化」が明記。

社会的意義

「企業が災害で止まらず、人と業務を守る」。

事例 4（2021 年 8 月 2 日：観光地での多言語通報）

- **構成パターン**：A 単体
- **該当ページ**：p.220–224（言語変換・危険ワード対応）

シナリオ

観光地で外国人旅行者が事故に巻き込まれ「Help!」と叫ぶ。システムが多言語辞書で認識し、日本の警察や消防へ即通報。

なぜ問題か

- 観光立国では言語障壁が命に関わる。

どうして起きたか

従来の通報システムは「日本語限定」で機能。

どうして防げるか（予防・対策）

- **危険ワード辞書（p.220–224）**に多言語を登録。
- **Silent 通報（p.110–133）**で旅行者が操作不要。

なぜ可能なのか（裏付け）

- 本体仕様に「言語差を超えて侵害成立」と明記（翻案防止ルール）。

社会的意義

「外国人観光客の安全を守り、国際信頼を高める」。

事例 5（2020 年 7 月 6 日：地域コミュニティでの防災ネットワーク）

- **構成パターン**：A 単体
- **該当ページ**：p.26–29（音声＋位置通報）, p.32（通報フロー）

シナリオ

地域町内会がアプリを導入し、高齢者の「助けて」の声を拾って近隣住民・消防へ自動通報。独居高齢者でも地域単位で命を守れる。

なぜ問題か

- 高齢者孤独死・災害弱者の増加が社会問題。

どうして起きたか

従来の防災無線は「一方向通知」であり、個人の SOS を拾えなかった。

どうして防げるか（予防・対策）

- **音声＋位置情報（p.26–29）**で地域ごとに検知。
- **Silent 通報（p.110–133）**で即座に消防と隣人に通知。

なぜ可能なのか（裏付け）

- 本体に「地域ネットワークと結合できる API 構造」が明記。

社会的意義

「地域全体が命を守るセーフティネット」。

✅ 第 1 部まとめ

- A パターンは人命救助にとどまらず、**公共交通・都市防犯・企業 BCP・観光多言語・地域防災**などの社会的インフラに応用可能。
- **なぜ可能か**：本体の設計仕様（音響解析・位置照合・Silent UI・契約言語封鎖）が全て裏付け。
- **社会的意義**：都市や企業、地域が「自動で命を守る機能」を持つことで、社会全体の安全性と信頼性を高める。

📘 第 2 部（事例 6〜10）：B パターン＝バイタル監視とライフスタイル・働き方応用

事例 6（2024 年 5 月 21 日：リモートワーク時の健康モニタリング）

- **構成パターン**：B 単体
- **該当ページ**：p.300–306（VitalScore 算出）, p.321–322（SilentTx API）, p.331–335（UI 設計）

シナリオ（その他の焦点）

在宅勤務中の従業員が、長時間労働やストレスで心拍異常を示す。システムが VitalScore を算出して管理者へ通知し、休息を推奨。

なぜ問題か

- 過労やストレスは生産性低下やメンタル不調を引き起こす。

どうして起きたか

- リモートワークでは上司が部下の状態を把握できない。

どうして防げるか（予防・対策）

- **VitalScore（p.307–310）**でストレスを数値化。
- **SilentTx（p.321–322）**で本人に悟られず通知。

なぜ可能なのか（裏付け）

- 本体に「Vital データを生活改善に利用可能」と記載あり。

社会的意義

「働き方改革をデータで支える」。

事例 7（2023 年 10 月 11 日：運動習慣の改善）

- **構成パターン**：B 単体

- **該当ページ**：p.300–302（基礎説明）, p.311–315（VitalProc モジュール）

シナリオ

市民がジョギングやジム利用時、呼吸や酸素濃度を計測。データをもとに運動不足や過度な負荷を調整し、健康寿命を延伸。

なぜ問題か

- 運動不足や過剰トレーニングは生活習慣病の原因。

どうして起きたか

- 従来は「感覚頼み」で運動強度を調整。

どうして防げるか（予防・対策）

- **VitalProc（p.311–315）**で酸素濃度や呼吸異常を検知。

なぜ可能なのか（裏付け）

- 特許請求項に「運動時の Vital 監視」が含まれている。

社会的意義

「市民一人ひとりの健康行動を最適化」。

事例 8（2022 年 2 月 14 日：学校教育での集中力測定）

- **構成パターン**：B 単体
- **該当ページ**：p.302（応用分野）, p.336–370（実証データ）

シナリオ

授業中の児童の心拍や皮膚電位を計測。集中度の変化を教師が把握し、授業改善や学習効率向上に活用。

なぜ問題か

- 授業中の理解度や集中度は見た目では把握困難。

どうして起きたか

- 教師は「態度観察」しか手段がなかった。

どうして防げるか（予防・対策）

- **実証データ（p.336–370）**で児童の集中度とバイタル変化を関連付け。

なぜ可能なのか（裏付け）

- 本体に「教育現場応用」事例が明記。

社会的意義

「学習効率をデータで可視化」。

事例 9（2021 年 4 月 1 日：スポーツチームのパフォーマンス最適化）

- **構成パターン**：B 単体
- **該当ページ**：p.304–305（Vital 異常事例）, p.331–335（UI）

シナリオ

プロスポーツ選手の試合中に心拍や酸素濃度を監視。疲労や脱水の兆候を即座に検知し、交代タイミングを指示。

なぜ問題か

- スポーツ事故や突然死は「兆候見逃し」が原因。

どうして起きたか

- 従来は「選手の自己申告」頼み。

どうして防げるか（予防・対策）

- **Vital 異常パターン（p.304–305）**を使い、過度な負荷を避ける。

なぜ可能なのか（裏付け）

- 「スポーツ利用」も応用例として明記。

社会的意義

「選手の健康とパフォーマンスを両立」。

事例 10（2020 年 12 月 25 日：オフィス環境での労働安全管理）

- **構成パターン**：B 単体
- **該当ページ**：p.300–302（概要）, p.371–400（Vital 異常検証）

シナリオ

建設現場や長時間労働オフィスで従業員の Vital を監視。異常を検知すると作業を中断し休憩指示。

なぜ問題か

- 過労死や労災事故は企業責任に直結。

どうして起きたか

- 従来は「本人申告」や「目視確認」に依存。

どうして防げるか（予防・対策）

- **Vital 異常検証データ（p.371–400）**に基づき、過労状態を科学的に検出。

なぜ可能なのか（裏付け）

- 特許請求項群に「労働安全応用」が含まれる。

社会的意義

「働く人の健康を守る企業経営」。

✅ 第 2 部まとめ

- **B パターン＝バイタル監視**は、命の保護だけでなく **働き方改革・教育・スポーツ・健康寿命延伸** などの社会応用に直結。
- **なぜ可能か**：VitalScore 算出式・実証データ・SilentTx・特許請求項に裏付け済み。
- **社会的意義**：「生活・働き方・学び」をデータで支える社会基盤を形成。

📘 第 3 部（事例 11〜15）：C パターン＝知財照合と産業応用・経済循環

事例 11（2024 年 2 月 14 日：大学研究成果の産学連携）

- **構成パターン**：C 単体
- **該当ページ**：p.553–560（知財照合）, p.561–580（契約生成）, p.861–903（経済循環）

シナリオ（その他の焦点）

大学研究室が開発したアルゴリズムを企業が利用。C システムが自動照合し、即時に契約生成 → 研究者にロイヤリティが分配。

なぜ問題か

- 従来は契約処理が遅れ、産学連携の経済循環が滞っていた。

どうして起きたか

- 契約や権利処理を人手で行っていたため時間がかかる。

どうして防げるか（予防・対策）

- **contractGen（p.561–570）**で即契約。
- **収益分配ロジック（p.861–903）**で透明に利益循環。

なぜ可能なのか（裏付け）

- 特許請求項で「照合→契約→分配」を保護。

社会的意義

「研究成果が即産業化され経済を回す」。

事例 12（2023 年 8 月 30 日：スタートアップの知財利用支援）

- **構成パターン**：C 単体
- **該当ページ**：p.591–620（契約 UI）, p.621–630（契約文言封鎖）

シナリオ

スタートアップ企業が外部の知財を利用する際、C システムが即照合 → 適正ライセンス料を提示し、透明な契約を成立。

なぜ問題か

- スタートアップは契約知識不足で知財リスクを抱えやすい。

どうして起きたか

- ライセンス体系が複雑で、誤解・不正利用が起こる。

どうして防げるか（予防・対策）

- **契約 UI（p.611–620）**で利用者に条件を可視化。
- **契約文言封鎖（p.621–630）**で表現差の誤魔化しを排除。

なぜ可能なのか（裏付け）

- 本体に「契約 UI と文言封鎖」が明記。

社会的意義

「若い企業も安心して知財利用できるエコシステム」。

事例 13（2022 年 6 月 12 日：金融機関での知財担保融資）

- **構成パターン**：C 単体
- **該当ページ**：p.861–903（金融応用）, p.601–610（契約ログ）

シナリオ

中小企業が保有する特許を担保に銀行から融資。C システムが知財収益実績を照合し、担保価値を算出 → 融資判断が迅速化。

なぜ問題か

- 従来は知財の担保評価が不透明で融資が滞る。

どうして起きたか

- 銀行には知財評価ノウハウが不足していた。

どうして防げるか（予防・対策）

- **契約ログ（p.601–610）**で利用実績を証跡化。
- **経済試算（p.861–903）**で価値を数値化。

なぜ可能なのか（裏付け）

- 「知財担保の信用評価」が仕様に明記。

社会的意義

「知財が金融資産として循環」。

事例 14（2021 年 11 月 5 日：国際取引の契約円滑化）

- **構成パターン**：C 単体
- **該当ページ**：p.631–700（越境契約）, p.621–630（契約文言封鎖）

シナリオ

日本企業と欧州企業が技術契約。C システムが翻訳差を封鎖し、越境契約を自動生成。

なぜ問題か

- 言語差や法体系の違いがトラブルを招きやすい。

どうして起きたか

- 契約交渉に数か月を要し、国際取引が停滞。

どうして防げるか（予防・対策）

- **契約文言封鎖（p.621–630）**で翻訳差を無効化。
- **越境契約機能（p.631–700）**で国際標準契約を生成。

なぜ可能なのか（裏付け）

- 特許請求項に「越境契約自動生成」が含まれる。

社会的意義

「国際的な技術流通が加速」。

事例 15（2020 年 8 月 29 日：エンタメ産業の収益循環強化）

- **構成パターン**：C 単体
- **該当ページ**：p.701–800（コピー検知）, p.801–860（契約検証ログ）

シナリオ

動画配信サービスが違法コピーを C で即遮断。正規契約が生成され、収益が制作会社・アーティストへ即分配。

なぜ問題か

- 違法コピーは産業収益を奪い、コンテンツ制作が停滞。

どうして起きたか

- DRM は「複製防止」に限定され収益循環を担保できなかった。

どうして防げるか（予防・対策）

- **コピー検知（p.701–800）**で不正を即ブロック。
- **契約生成＋分配（p.561–570, p.861–903）**で正規収益化。

なぜ可能なのか（裏付け）

- 「収益分配機能」が仕様に明記。

社会的意義

「エンタメ産業の持続的成長を保証」。

✅ 第 3 部まとめ

- **C パターン＝知財照合と経済循環**は、研究・スタートアップ・金融・国際取引・エンタメと幅広い産業に直結。
- **なぜ可能か**：契約生成・収益分配・文言封鎖・国際契約処理が特許に裏付け済み。
- **社会的意義**：知財を正当に流通させ、経済全体に循環させることで、社会発展を支える基盤を形成。

📘 第 4 部（事例 16〜20）：D・E パターン＝複合安全網と契約・決済による新市場創出

事例 16（2024 年 9 月 10 日：教育産業における複合安全網サービス）

- **構成パターン**：D 単体
- **該当ページ**：p.941–960（複合判定エンジン）, p.1011–1030（複合 UI）

シナリオ（その他の焦点）

学校に D システムを導入。児童の叫び声（A）＋バイタル（B）＋教育アプリ利用ログ（C）を複合判定し、**いじめ・過労・無断利用**を自動検知 → 教師と保護者に通知。

なぜ問題か

- 教育現場は「不正利用・不登校・いじめ」など複合要素の把握が困難。

どうして防げるか（予防・対策）

- **複合判定（p.961–970）**で三要素をスコア化し信頼性を高める。
- **複合 UI（p.1001–1010）**で学校管理者が状況を一目で把握。

社会的意義

「教育現場をデータ駆動で見守る市場」。

事例 17（2023 年 3 月 11 日：行政サービス統合プラットフォーム）

- **構成パターン**：D 単体
- **該当ページ**：p.943–947（災害応用）, p.1031–1050（複合稼働シナリオ）

シナリオ

自治体が D を導入し、防災・福祉・保険サービスを一元管理。災害通報（A）、市民バイタル（B）、契約照合（C）が統合され、**行政サービスの DX 基盤**に。

なぜ問題か

- 縦割り行政では市民サービスが遅滞し、信頼を失う。

どうして防げるか（予防・対策）

- **複合稼働（p.1031–1050）**で誤検知率低下・効率化。

社会的意義

「自治体サービスの統合市場」。

事例 18（2022 年 6 月 15 日：金融ビジネスでの複合信用判定）

- **構成パターン**：D→E
- **該当ページ**：p.1051–1070（複合閾値設定）, p.1191–1210（清算制御）

シナリオ

金融機関が D で顧客の「信用リスク」を判定し、E で融資・投資契約を即時清算。**行動・契約・健康データを加味した新しい信用市場**を創出。

なぜ問題か

- 従来の金融は「過去データ」に依存、実態を反映できない。

どうして防げるか（予防・対策）

- **複合閾値設定（p.1051–1070）**で行動や Vital を統合評価。
- **清算 Tx 群（p.1191–1210）**で契約・決済をリアルタイム制御。

社会的意義

「動的信用市場の創出」。

事例 19（2021 年 2 月 28 日：国際貿易における即時決済市場）

- **構成パターン**：E 単体
- **該当ページ**：p.1240–1260（清算ロジック）, p.1321–1340（Ledger API）

シナリオ

輸出入契約を E で処理。輸送状況と契約条件を自動照合 → 即時決済。国際物流で「信用不安」をなくす市場を形成。

なぜ問題か

- 従来は「送金後に契約不一致」が発覚しトラブルに。

どうして防げるか（予防・対策）

- **清算ロジック（p.1240–1260）**で契約金額と条件を自動判定。
- **Ledger API（p.1321–1340）**で全履歴を証跡化。

社会的意義

「国際貿易の即時清算市場」。

事例 20（2020 年 1 月 19 日：保険業界の自動補償市場）

- **構成パターン**：E 単体
- **該当ページ**：p.1261–1280（契約条件照合）, p.1341–1360（CSV 台帳）

シナリオ

E システムで保険契約と実際の事故・Vital ログを自動照合。条件を満たせば即補償金支払い。**「申請不要保険」市場**を形成。

なぜ問題か

- 現行の保険は申請・審査に時間がかかり、利用者不満が高い。

どうして防げるか（予防・対策）

- **契約条件照合（p.1240–1260）**で自動化。
- **CSV 台帳（p.1341–1360）**で監査性を担保。

社会的意義

「保険が自動で動く新市場」。

✅ 第 4 部まとめ

- **D パターン＝複合安全網**は教育・行政・金融で「統合市場」を創出。
- **E パターン＝清算決済**は国際貿易・保険で「即時決済市場」を創出。
- **その他の意義**：命や事故の保護を超え、**新しいビジネス市場を形作る基盤技術**となる。

📘 第 5 部（事例 21〜25）：F・G パターン＝再利用・二次流通管理と教育・出版・流通応用

事例 21（2024 年 6 月 4 日：学校教育における教材ライセンス管理）

- **構成パターン**：F 単体（再利用封鎖）
- **該当ページ**：p.1240–1260（清算ロジック）, p.1335–1360（失効ログ）

シナリオ（その他の焦点）

学校が契約終了済みのデジタル教材を翌年度も無断利用。F システムが失効フラグを検知し遮断。出版社は正規更新契約を経て教材を提供。

なぜ問題か

- 教育現場の不正利用は出版社の収益を奪い、教育資源の質を低下させる。

どうして防げるか（予防・対策）

- **契約失効検知（p.1240–1260）**で利用を即制御。
- **失効ログ（p.1335–1360）**で証跡を残す。

社会的意義

「教育コンテンツの正規循環市場を形成」。

事例 22（2023 年 8 月 17 日：医療研究データの利用制御）

- **構成パターン**：F 単体
- **該当ページ**：p.1335–1360（失効記録）, p.1436–1450（再流通遮断）

シナリオ

研究機関が契約終了後の患者データを再利用しようとしたが、F が検知して遮断。新たに正規契約を結び直して活用。

なぜ問題か

- 契約外利用は個人情報保護法違反であり、研究の信頼性を損なう。

どうして防げるか（予防・対策）

- **失効記録（p.1335–1360）**で利用状況を監査。
- **遮断処理（p.1436–1450）**で不正流通を防止。

社会的意義

「研究と倫理を両立させる仕組み」。

事例 23（2022 年 12 月 1 日：ソフトウェアのサブライセンス管理）

- **構成パターン**：G 単体（二次流通制御）
- **該当ページ**：p.1504–1510（正規ルート）, p.1521–1530（流通チェック API）

シナリオ

企業が取得したソフトウェアライセンスを第三者に横流し。G が検知し遮断。二次市場での流通は正規権利者を通すことで合法化。

なぜ問題か

- サブライセンス横流しは正規市場を破壊し、開発者の利益を奪う。

どうして防げるか（予防・対策）

- **流通チェック API（p.1521–1530）**で横流しを即検知。
- **正規ルート（p.1504–1510）**のみを通過させる。

社会的意義

「ソフトウェア産業の公正な市場を保証」。

事例 24（2021 年 10 月 23 日：電子出版物の違法コピー対策）

- **構成パターン**：F＋G 連携
- **該当ページ**：p.1436–1450（封鎖ログ）, p.1665–1667（再循環台帳）

シナリオ

人気電子書籍がコピーされ、SNS や P2P で違法流通。F がコピーを失効化し、G が不正経路を遮断。正規販売経路のみを存続。

なぜ問題か

- 違法コピーは出版産業全体の利益を奪い、作家活動を萎縮させる。

どうして防げるか（予防・対策）

- **封鎖ログ（p.1436–1450）**でコピーを証跡化。
- **再循環台帳（p.1665–1667）**で流通ルートを監査。

社会的意義

「創作者が安心して活動できる出版市場を守る」。

事例 25（2020 年 5 月 9 日：国際流通と標準化）

- **構成パターン**：G 単体
- **該当ページ**：p.1541–1564（標準化提案記録）, p.1665–1667（経済効果データ）

シナリオ

海外企業が日本発技術を自社開発と偽り国際会議で提案。G が正規台帳を参照し、権利者を確認 → 不正流通を排除し正規流通を認証。

なぜ問題か

- 国際流通での知財盗用は「市場事故」として国家経済に損失を与える。

どうして防げるか（予防・対策）

- **標準化記録（p.1541–1564）**で正規提案を証明。
- **経済効果データ（p.1665–1667）**で正規導入の実績を裏付け。

社会的意義

「国際市場での公正な競争を保証」。

✅ 第 5 部まとめ

- **F パターン＝再利用封鎖**：教育・医療・出版における不正利用を遮断。
- **G パターン＝二次流通制御**：ソフトウェア・出版・国際流通で正規市場を守る。
- **社会的意義**：不正利用やコピー流通を封じ、**教育・出版・流通の持続可能な市場を形成。**

📘 第 6 部（事例 26〜30）：H・I・J パターン＝証拠保存・復元・国際展開・標準化

事例 26（2024 年 2 月 1 日：監査制度と企業ガバナンス強化）

- **構成パターン**：H 単体
- **該当ページ**：p.1391–1410（監査ログ生成）, p.1411–1430（不可逆保存 UI）

シナリオ（その他の焦点）

企業が ESG 経営やガバナンスを強化するため、契約・取引・内部通報の証跡を H で不可逆保存。監査法人や株主への透明性が格段に高まる。

なぜ問題か

- 不正会計や隠蔽は国際市場での信用を失う。

どうして防げるか（予防・対策）

- **監査ログ生成（p.1391–1410）**で全取引を証跡化。
- **WORM 保存＋TSA 署名（p.1411–1430）**で改ざんを防止。

社会的意義

「企業透明性を高め投資市場を活性化」。

事例 27（2023 年 5 月 11 日：教育記録の長期保存と学歴認証）

- **構成パターン**：I 単体（復元処理）
- **該当ページ**：p.1520–1540（復元アルゴリズム）, p.1581–1600（再保存方式）

シナリオ

学生の成績や履修記録をブロックチェーン的に I システムで保存。サーバ障害や不正アクセスで消失しても復元可能 → 国際的な学歴証明にも利用。

なぜ問題か

- 海外進学や就職で「学歴証明が破損・紛失」すると不利益。

どうして防げるか（予防・対策）

- **復元アルゴリズム（p.1520–1540）**で再生成。
- **改ざん不可の再保存（p.1581–1600）**で認証基盤を強化。

社会的意義

「教育データの信頼性を国際的に担保」。

事例 28（2022 年 7 月 22 日：国際標準化と IoT セキュリティ基盤）

- **構成パターン**：I＋H 連携
- **該当ページ**：p.1541–1564（国際標準化提案）, p.1530–1540（複合ルール設計）

シナリオ

ASEAN や EU において、IoT デバイス間の契約・通信証跡を標準化。H で監査証跡、I で復元可能性を提供 → ISO/IEC 規格に提案。

なぜ問題か

- IoT セキュリティは「国際規格」が未整備で断片化。

どうして防げるか（予防・対策）

- **複合ルール（p.1530–1540）**で各国法制に対応。
- **国際標準化提案（p.1541–1564）**で規格候補として提示。

社会的意義

「IoT 市場全体の国際整合性を確立」。

事例 29（2021 年 11 月 30 日：行政データ復興と地域ガバナンス）

- **構成パターン**：J 単体（特殊用途）
- **該当ページ**：p.1632–1664（具体機能展開）, p.1668–1670（人道 UI）

シナリオ

自治体が防災・福祉・契約データを J で統合。災害やシステム障害で失われても即復元され、補償・行政サービスを止めない。

なぜ問題か

- 行政データ喪失＝住民サービスの停滞・信用失墜。

どうして防げるか（予防・対策）

- **特殊用途 API（p.1632–1664）**で例外的な行政データ利用を許容。
- **人道利用 UI（p.1668–1670）**で迅速復旧。

社会的意義

「自治体 DX の国際展開モデル」。

事例 30（2020 年 4 月 9 日：スマートシティ標準化と国際輸出）

- **構成パターン**：J 単体
- **該当ページ**：p.1503（応用展望）, p.1629–1698（統合プラットフォーム）

シナリオ

スマートシティ基盤として、緊急通報（A）、バイタル監視（B）、知財契約（C）、監査保存（H）、復元（I）を含む統合パッケージを J が提供。ISO/TRIPS 準拠で海外輸出。

なぜ問題か

- スマートシティ導入では「国ごとの制度差」が壁。

どうして防げるか（予防・対策）

- **統合プラットフォーム設計（p.1629–1698）**で国際的互換性を担保。

社会的意義

「日本発の知財・技術を国際標準として輸出」。

✅ 第 6 部まとめ

- **H＝証拠保存** → 企業ガバナンス・市場透明性を保証。
- **I＝復元** → 教育・研究・行政記録を持続的に保存。
- **J＝特殊用途** → 国際展開・スマートシティ・行政 DX を推進。
- **総合意義**：これらは「その他＝社会的・国際的基盤形成」に直結し、**標準化・制度整合・産業輸出・市場信頼**を支える。

📘 第 1 部（事例 1〜5）：A パターン＝生活犯罪の即時通報

事例 1（2024 年 3 月 12 日：痴漢行為の即時通報）

- **構成パターン**：A 単体
- **該当ページ**：p.25–32（緊急通報フロー）, p.110–133（Silent UI）, p.134–145（音響解析）

生活犯罪シナリオ

通勤電車内で女性が痴漢被害に遭い「やめて！」と声を出した瞬間、システムが危険ワードを検知。GPS 位置（列車 ID＋位置情報）と連携して鉄道警備と警察へ即時通報。

なぜ問題か

- 被害者は恐怖で通報操作できないことが多い。
- 証拠が残らず泣き寝入りするケースが多発。

どうして起きたか

従来は「手動通報」か「周囲の人が気づく」しか手段がなかった。

どうして防げるか（予防・対策）

- **危険ワード辞書（p.220–224）**で多言語も検知。
- **Silent UI（p.110–133）**で画面に表示を出さず裏で通報。
- **音響解析（p.134–145）**で叫び声を強調検知。

なぜ可能なのか（裏付け）

- 本体に「音響＋発話＋位置による緊急通報」の仕組みを明記。

社会的・生活的意義

「痴漢犯罪を現行犯で封じるインフラ」。

事例 2（2023 年 9 月 5 日：ストーカー被害の自動検知）

- **構成パターン**：A 単体
- **該当ページ**：p.26–30（発話検知）, p.220–224（危険ワード辞書）

生活犯罪シナリオ

深夜に女性が後をつけられ「怖い！」と発話。システムが危険ワードと心拍異常音を同時検知し、警察・友人へ Silent 通報。

なぜ問題か

- 被害者は加害者を刺激する恐れから声を上げにくい。

どうして起きたか

従来は「110 番に電話」しか手段がなく、通報時点で襲われるケースもあった。

どうして防げるか（予防・対策）

- **辞書登録（p.220–224）**で危険ワードを多層検知。
- **Silent 通報（p.110–133）**で加害者に悟られない。

なぜ可能なのか（裏付け）

- 「表現差を超えて結論一致なら侵害」という権利封鎖。

社会的意義

「声を発した瞬間に守られる安心社会」。

事例 3（2022 年 11 月 28 日：空き巣侵入の自動通報）

- **構成パターン**：A 単体
- **該当ページ**：p.28–29（位置情報照合）, p.56–82（外部 API 連携）

生活犯罪シナリオ

夜間に空き巣が窓ガラスを破壊。異常音をマイクが検知し、住宅の位置情報とともに警備会社＋警察へ自動通報。

なぜ問題か

- 空き巣は数分で犯行完了、発覚が遅れると財産被害が拡大。

どうして起きたか

従来はセンサー式アラームが鳴るだけで、警察連携は遅延。

どうして防げるか（予防・対策）

- **API 連携（p.56–82）**で警察直結。
- **位置情報照合（p.98–108）**で誤報を減らす。

なぜ可能なのか（裏付け）

- 本体に「API と外部警備システムとの接続」が仕様化。

社会的意義

「空き巣犯行時間をゼロに近づける」。

事例 4（2021 年 8 月 2 日：近隣騒音トラブルの記録化）

- **構成パターン**：A 単体
- **該当ページ**：p.83–97（通報ログ保存）, p.134–145（音響解析）

生活犯罪シナリオ

隣人の騒音に悩まされる住民。深夜の異常音がシステムにより自動検知され、**日時＋音データ**が通報ログとして保存 → 裁判・調停で活用。

なぜ問題か

- 騒音トラブルは「証拠不在」で被害者が泣き寝入り。

どうして起きたか

従来は「録音機器を自分で設置」するしかなかった。

どうして防げるか（予防・対策）

- **音響解析（p.134–145）**で異常音を抽出。
- **ログ保存（p.83–97）**で法的証拠化。

なぜ可能なのか（裏付け）

- 「ログを不可逆保存する構造」が特許請求項に記載。

社会的意義

「生活騒音を法的に解決できる基盤」。

事例 5（2020 年 7 月 6 日：災害便乗型犯罪の封鎖）

- **構成パターン**：A 単体
- **該当ページ**：p.26–29（音声＋位置通報）, p.32（救助フロー）

生活犯罪シナリオ

大地震で停電した地域に侵入する便乗窃盗犯。被害者が「助けて」と叫ぶと同時にシステムが異常音＋位置情報を検出し、消防・警察に Silent 通報。

なぜ問題か

- 災害直後は治安が悪化しやすく、通報不能状況が増える。

どうして防げるか（予防・対策）

- **音声＋位置情報（p.26–29）**で即通報。
- **Silent 通報 UI（p.110–133）**で加害者に悟られない。

なぜ可能なのか（裏付け）

- 第 4 部（p.1499–1505）に「災害応用」が記載。

社会的意義

「災害時の無法状態を抑止」。

✅ 第 1 部まとめ

- A パターンは **痴漢・ストーカー・空き巣・騒音トラブル・災害便乗犯罪** など、日常で多発する生活犯罪を即時通報・証跡化できる。
- **なぜ可能か**：音響解析、危険ワード辞書、Silent 通報、API 連携、不可逆ログ保存がすべて特許・仕様に裏付け。
- **社会的意義**：市民生活を「操作不要の自動通報」で守り、安心できる社会基盤を築く。

📘 第 2 部（事例 6〜10）：B パターン＝バイタル監視による生活犯罪検知

事例 6（2024 年 5 月 21 日：ATM 振り込め詐欺阻止）

- **構成パターン**：B 単体
- **該当ページ**：p.300–306（VitalScore 算出）, p.321–322（SilentTx API）, p.331–335（UI 設計）

生活犯罪シナリオ

高齢者が詐欺グループの指示通りに ATM 操作。心拍急上昇と手の発汗異常をセンサーが検知 → 表向きは「取引完了」画面を表示しつつ、Silent 通報で銀行不正検知センターと警察に通知。

なぜ問題か

- 振り込め詐欺は本人操作なので従来検知が難しい。
- 犯罪者は「心理的緊張」を利用する。

どうして防げるか（予防・対策）

- **VitalScore（p.307–310）**で心理ストレスを数値化。
- **SilentTx（p.321–322）**で裏通報。

なぜ可能なのか（裏付け）

- 「バイタル＋通報構成を包括保護」と権利範囲に明記。

社会的意義

「高齢者が無意識に守られる ATM」。

事例 7（2023 年 10 月 11 日：飲酒運転犯罪の防止）

- **構成パターン**：B 単体
- **該当ページ**：p.300–302（概要）, p.311–315（VitalProc モジュール）

生活犯罪シナリオ

飲酒したドライバーが車を始動しようとしたが、呼吸異常＋酸素濃度低下をセンサーが検知 → エンジンは始動せず、同時に家族と警察へ Silent 通報。

なぜ問題か

- 飲酒運転は死亡率の高い重大犯罪。

どうして防げるか（予防・対策）

- **VitalProc（p.311–315）**で呼吸・酸素濃度を監視。
- **Silent UI（p.328–330）**で裏通報。

なぜ可能なのか（裏付け）

- 本体に「飲酒運転防止」応用を明記。

社会的意義

「車が自ら命と社会を守る」。

事例 8（2022 年 2 月 14 日：家庭内 DV の検知と通報）

- **構成パターン**：B 単体

- **該当ページ**：p.304–305（事例解説）, p.331–335（UI 設計）

生活犯罪シナリオ

家庭内で暴力を受けた女性。声を出せず動けなかったが、心拍急上昇・呼吸乱れをセンサーが検知 → Silent 通報で警察と児童相談所に通知。

なぜ問題か

- DV は密室で発生し、証拠も通報も困難。

どうして防げるか（予防・対策）

- **バイタル異常パターン（p.304–305）**で発作的ストレスを検出。
- **Silent UI（p.331–335）**で被害者に代わり通報。

なぜ可能なのか（裏付け）

- 「Vital＋Silent 通報」を著作権保護範囲に含めると明記。

社会的意義

「被害者が沈黙していても守られる家庭」。

事例 9（2021 年 4 月 1 日：児童虐待の早期発見）

- **構成パターン**：B 単体
- **該当ページ**：p.302（応用事例）, p.336–370（実証データ）

生活犯罪シナリオ

児童が家庭内で虐待を受け、体罰による心拍急上昇や呼吸異常をシステムが感知 → 通報先に児相・学校を自動指定。

なぜ問題か

- 虐待は長期化すると心身に致命的影響。
- 子どもは SOS を発信できない。

どうして防げるか（予防・対策）

- **実証データ（p.336–370）**でバイタル異常と虐待兆候を数値化。

なぜ可能なのか（裏付け）

- 教育・家庭応用が本体に事例化。

社会的意義

「子どもの命を守る不可視センサー」。

事例 10（2020 年 12 月 25 日：銀行強盗現場での自動検知）

- **構成パターン**：B 単体
- **該当ページ**：p.303（事例紹介）, p.321–330（SilentTx API＋UI）

生活犯罪シナリオ

銀行窓口で強盗が侵入。職員が恐怖で心拍急上昇 → 端末が Silent 通報で警察・警備へ即通知。画面は通常業務表示を保ち、犯人に悟らせない。

なぜ問題か

- 強盗は人質化で「非常ボタン」が押せない。

どうして防げるか（予防・対策）

- **SilentTx（p.321–322）**で裏通報。
- **UI 二重設計（p.328–330）**で表は通常画面。

なぜ可能なのか（裏付け）

- 「Silent Alert UX の最大特徴」と本体に明記。

社会的意義

「人質状態でも命を守れる銀行」。

✅ 第 2 部まとめ

- **B パターン＝バイタル監視**は、ATM 詐欺・飲酒運転・DV・虐待・強盗といった生活犯罪を **生体異常という客観指標で検知**。
- **なぜ可能か**：VitalScore・SilentTx・実証データ・特許請求項に裏付け。
- **社会的意義**：人が声を上げられない状況でも「体が犯罪を告げる」仕組みにより、生活犯罪の多くを封じ込める基盤となる。

📘 第 3 部（事例 11〜15）：C パターン＝知財・契約に絡む生活犯罪防止

事例 11（2024 年 2 月 14 日：大学研究コードの剽窃と生活的影響）

- **構成パターン**：C 単体
- **該当ページ**：p.553–560（照合概要）, p.561–580（契約生成）, p.904–938（特許請求項）

生活犯罪シナリオ

大学院生が他大学の医療 AI コードを盗用して論文提出。C システムが一致スコア 0.92 を検出し即遮断。剽窃が社会実装される前に正規契約へ誘導。

なぜ問題か

- 知財剽窃は「知の犯罪」であり、誤情報拡散や不正就職につながる。

どうして起きたか

従来は「剽窃検知のみ」で、契約・収益分配の仕組みが無かった。

どうして防げるか（予防・対策）

- **compareIP(), similarityScore()（p.571–580）**で剽窃検出。
- **contractGen()（p.561–570）**で正規利用契約へ誘導。

なぜ可能なのか（裏付け）

- 特許請求項に「照合→契約→収益分配」が明記（p.916–938）。

社会的意義

「知の不正流用を社会実装前に封じる」。

事例 12（2023 年 8 月 30 日：災害便乗アプリ詐欺）

- **構成パターン**：C 単体
- **該当ページ**：p.621–630（契約文言封鎖）, p.631–700（越境契約処理）

生活犯罪シナリオ

地震直後に正規防災アプリを模倣した偽アプリが流通。個人情報や寄付金を詐取。C システムが UI・契約差異を侵害判定し即遮断。

なぜ問題か

- 災害時の便乗詐欺は「生活インフラを混乱させ命も危険に」。

どうして起きたか

従来の DRM は「表現差・契約差」を理由に抜け道が存在。

どうして防げるか（予防・対策）

- **契約文言封鎖（p.621–630）**で翻案逃れを防止。
- **国際契約処理（p.631–700）**で越境流通を制御。

なぜ可能なのか（裏付け）

- 「表現差を超え結論一致なら侵害成立」と規定。

社会的意義

「災害便乗型の生活犯罪を遮断」。

事例 13（2022 年 6 月 12 日：虚偽知財担保ローン詐欺）

- **構成パターン**：C 単体
- **該当ページ**：p.861–903（経済試算・担保評価）, p.601–610（契約ログ）

生活犯罪シナリオ

中小企業が収益のない特許を担保にローンを申請。C システムが契約履歴と分配記録を照合し虚偽を検出 → 融資詐欺を阻止。

なぜ問題か

- 知財の虚偽申告は「信用詐欺」であり生活資金の流通を阻害。

どうして起きたか

従来は知財の金融評価がブラックボックスで、虚偽担保が通用した。

どうして防げるか（予防・対策）

- **契約ログ（p.601–610）**で履歴を照合。
- **経済モデル（p.861–903）**で担保価値を数値化。

なぜ可能なのか（裏付け）

- 「知財担保の金融応用」が本体に明記。

社会的意義

「信用詐欺を金融段階でブロック」。

事例 14（2021 年 11 月 5 日：翻訳差悪用による国際契約詐欺）

- **構成パターン**：C 単体
- **該当ページ**：p.621–630（契約文言封鎖）, p.631–700（越境契約処理）

生活犯罪シナリオ

海外企業が契約翻訳差を悪用し支払いを回避。C システムが差異を侵害として即認定 → 正規支払いを強制。

なぜ問題か

- 契約差悪用は「国際生活犯罪」として企業・消費者双方に損害。

どうして起きたか

従来の契約システムは翻訳差を抜け道にされていた。

どうして防げるか（予防・対策）

- **契約文言封鎖（p.621–630）**で翻訳差を無効化。
- **越境契約（p.631–700）**で各国に対応。

なぜ可能なのか（裏付け）

- 特許請求項に「翻訳差封鎖」が含まれる。

社会的意義

「国際的な契約犯罪を撲滅」。

事例 15（2020 年 8 月 29 日：違法コピーと寄付金詐欺）

- **構成パターン**：C 単体
- **該当ページ**：p.701–800（コピー検知）, p.801–860（検証ログ）

生活犯罪シナリオ

「災害支援寄付上映」と称し違法コピー映画を配布、寄付金を詐取。C システムが不正コピーを検知し、正規契約化して収益を被災地に循環。

なぜ問題か

- 違法コピー＋偽寄付は「二重の生活犯罪」。

どうして起きたか

従来はコピー検知が DRM に限定され、収益循環が担保できなかった。

どうして防げるか（予防・対策）

- **コピー検知（p.701–800）**で不正遮断。
- **契約生成＋収益分配（p.561–570, p.861–903）**で正規ルートに誘導。

なぜ可能なのか（裏付け）

- 「表現差を超えて侵害成立」と記載（p.621）。

社会的意義

「知財犯罪と寄付詐欺を同時に遮断」。

✅ 第 3 部まとめ

- **C パターン＝知財・契約型生活犯罪防止**は、剽窃・災害便乗アプリ・虚偽担保・翻訳差詐欺・違法コピー寄付などを対象。
- **なぜ可能か**：照合アルゴリズム・契約文言封鎖・収益分配が特許で裏付け済。
- **社会的意義**：知的財産と契約の信頼性を強化し、生活犯罪を社会システムの段階で封じる。

📘 第 4 部（事例 16〜20）：D・E パターン＝複合安全網と決済制御による生活犯罪防止

事例 16（2024 年 9 月 10 日：学校内いじめ・暴力の複合検知）

- **構成パターン**：D 単体
- **該当ページ**：p.941–960（複合判定エンジン）, p.1011–1030（複合 UI）

生活犯罪シナリオ

児童が教室で暴力被害に遭い「助けて」と叫ぶ（A）、心拍急上昇（B）、学習アプリ利用ログ異常（C）が同時発生。D が複合一致を検出し、教職員・警察へ自動通報。

なぜ問題か

- いじめは「密室性」が高く、被害者が通報できない。

どうして防げるか（予防・対策）

- **複合判定関数（p.961–970）**で誤報を減らしつつ重大ケースを抽出。
- **複合 UI（p.1001–1010）**で管理者に即通知。

社会的意義

「学校犯罪をリアルタイムに検知」。

事例 17（2023 年 3 月 11 日：災害時の便乗詐欺・物資横流し防止）

- **構成パターン**：D 単体
- **該当ページ**：p.943–947（災害応用）, p.1031–1050（複合稼働シナリオ）

生活犯罪シナリオ

大地震後、偽被災者が物資を詐取。D が通報ログ（A）、申請者のバイタル（B）、契約情報（C）を複合照合し正規被災者のみを認証、不正を遮断。

なぜ問題か

- 災害時は「偽装申請＝生活資源窃取」が横行。

どうして防げるか（予防・対策）

- **複合稼働（p.1031–1050）**で認証精度を上げる。

社会的意義

「災害便乗犯罪を制度段階で封鎖」。

事例 18（2022 年 6 月 15 日：保険契約の二重請求犯罪防止）

- **構成パターン**：D→E
- **該当ページ**：p.1051–1070（複合閾値設定）, p.1191–1210（清算制御）

生活犯罪シナリオ

同じ事故を複数の保険会社に二重請求。D が契約・バイタル・通報を複合判定、E が決済を遮断し犯罪を防止。

なぜ問題か

- 保険二重請求は「生活保険制度の信用」を揺るがす。

どうして防げるか（予防・対策）

- **複合閾値（p.1051–1070）**で多要素照合。
- **清算 Tx（p.1191–1210）**で契約一致確認。

社会的意義

「生活保険犯罪を決済段階で封鎖」。

事例 19（2021 年 2 月 28 日：国際送金を悪用した生活詐欺の阻止）

- **構成パターン**：E 単体
- **該当ページ**：p.1240–1260（清算ロジック）, p.1321–1340（Ledger API）

生活犯罪シナリオ

個人が架空契約を利用し海外送金を詐取。E が契約条件と金額を即照合し送金を遮断、同時にペナルティ精算を実行。

なぜ問題か

- 国際送金詐欺は個人生活の資産流出に直結。

どうして防げるか（予防・対策）

- **清算ロジック（p.1240–1260）**で契約整合性をリアルタイム検証。
- **Ledger API（p.1321–1340）**で全履歴を監査。

社会的意義

「海外生活犯罪を決済で封鎖」。

事例 20（2020 年 1 月 19 日：補償金詐欺の自動遮断）

- **構成パターン**：E 単体
- **該当ページ**：p.1261–1280（契約条件照合）, p.1341–1360（CSV 台帳）

生活犯罪シナリオ

被害者を装い、架空の事故報告で補償金を詐取。E が契約条件照合で不一致を検知し支払いを停止。

なぜ問題か

- 補償金詐欺は生活弱者の制度を食い物にする犯罪。

どうして防げるか（予防・対策）

- **契約条件照合（p.1240–1260）**で虚偽を排除。
- **CSV 台帳（p.1341–1360）**で透明性を担保。

社会的意義

「制度を守り、本当に必要な人に補償を届ける」。

✅ 第 4 部まとめ

- **D パターン**：学校暴力・災害便乗詐欺・二重請求を複合的に検知。

- **E パターン**：国際送金詐欺・補償金詐欺を決済時に遮断。
- **社会的意義**：生活犯罪を「発生直後」または「決済直前」で封じ、被害をゼロ化する制度基盤。

📘 第 5 部（事例 21〜25）：F・G パターン＝再利用・二次流通に関する生活犯罪防止

事例 21（2024 年 6 月 4 日：学校教材の無断再利用）

- **構成パターン**：F 単体
- **該当ページ**：p.1240–1260（清算ロジック）, p.1335–1360（失効ログ）

生活犯罪シナリオ

学校が契約切れ教材を翌年度もコピー利用。F が失効フラグを検知し使用を遮断。

なぜ問題か

- 無断利用は著作権犯罪であり、教育資源の正規流通を阻害。

どうして防げるか（予防・対策）

- **契約失効判定（p.1240–1260）**で自動チェック。
- **失効ログ（p.1335–1360）**で監査証跡を残す。

社会的意義

「教育分野のライセンス犯罪を封鎖」。

事例 22（2023 年 8 月 17 日：医療データの不正二次利用）

- **構成パターン**：F 単体
- **該当ページ**：p.1335–1360（失効記録）, p.1436–1450（再流通遮断）

生活犯罪シナリオ

病院が契約終了後の患者バイタルデータを研究機関に再利用。F が検知し遮断。

なぜ問題か

- 個人情報の不正再流通＝プライバシー犯罪。

どうして防げるか（予防・対策）

- **失効ハッシュ（p.1341–1360）**で使用可否を判定。
- **再流通遮断（p.1436–1450）**で漏洩を封じる。

社会的意義

「医療情報犯罪を制度レベルで防止」。

事例 23（2022 年 12 月 1 日：ソフトウェアのサブライセンス横流し）

- **構成パターン**：G 単体
- **該当ページ**：p.1504–1510（正規ルート）, p.1521–1530（流通チェック API）

生活犯罪シナリオ

企業が取得したアプリライセンスを第三者に横流し。G が契約外流通を検知して遮断。

なぜ問題か

- 横流しは「横領犯罪」に相当し、正規市場を破壊。

どうして防げるか（予防・対策）

- **二次流通チェック API（p.1521–1530）**で監視。
- **正規ルート（p.1504–1510）**のみ許可。

社会的意義

「ソフトウェア流通犯罪の根絶」。

事例 24（2021 年 10 月 23 日：電子書籍の違法コピー流通）

- **構成パターン**：F＋G 連携
- **該当ページ**：p.1436–1450（封鎖ログ）, p.1665–1667（再循環台帳）

生活犯罪シナリオ

人気電子書籍がコピーされ P2P で流通。F がコピーを失効化、G が不正経路を遮断。

なぜ問題か

- 違法コピーは著作権犯罪であり、出版市場を荒廃させる。

どうして防げるか（予防・対策）

- **封鎖ログ（p.1436–1450）**で不正利用を証跡化。
- **再循環台帳（p.1665–1667）**で流通経路を追跡。

社会的意義

「違法コピー犯罪を市場から排除」。

事例 25（2020 年 5 月 9 日：国際標準化を悪用した技術盗用）

- **構成パターン**：G 単体
- **該当ページ**：p.1541–1564（標準化提案記録）, p.1665–1667（経済効果データ）

生活犯罪シナリオ

海外企業が日本技術を自社開発と偽り国際会議で提出。G が正規台帳を参照し不正を排除。

なぜ問題か

- 標準化の場での知財盗用は「経済スパイ犯罪」。

どうして防げるか（予防・対策）

- **標準化記録（p.1541–1564）**で正規ルートを証明。
- **経済データ（p.1665–1667）**で正規導入実績を裏付け。

社会的意義

「国際的な知財犯罪を制度で封鎖」。

✅ 第 5 部まとめ

- **F パターン＝再利用封鎖**：教育・医療分野の「不正再利用」を遮断。
- **G パターン＝二次流通制御**：ソフトウェア・出版・国際標準での不正流通を排除。
- **社会的意義**：再利用・二次流通に潜む「生活犯罪」を根本から封じ、正規市場を守る基盤を形成。

📘 第 6 部（事例 26〜30）：H・I・J パターン＝証拠保存・復元・国際生活犯罪防止

事例 26（2024 年 2 月 1 日：生活詐欺裁判での証拠保存）

- **構成パターン**：H 単体
- **該当ページ**：p.1391–1410（監査ログ生成）, p.1411–1430（不可逆保存 UI）

生活犯罪シナリオ

高齢者を狙ったリフォーム詐欺。被害者が残した通話ログと契約記録を H が WORM 保存。裁判で改ざん不能な証拠として認められ、加害者有罪に。

なぜ問題か

- 生活詐欺は「証拠不足」で泣き寝入りが多い。

どうして防げるか（予防・対策）

- **監査証跡＋TSA 署名（p.1411–1430）**で偽造不可能。

社会的意義

「生活詐欺を証拠の力で裁ける」。

事例 27（2023 年 5 月 11 日：消費者契約データの復元）

- **構成パターン**：I 単体
- **該当ページ**：p.1520–1540（復元アルゴリズム）, p.1581–1600（再保存方式）

生活犯罪シナリオ

消費者金融の契約データが外部攻撃で削除され、利用者が多重債務を証明できない。I が **recoverEvidence()**でデータを復元し、被害回避。

なぜ問題か

- データ消失は「債務なすりつけ」や「契約改ざん」に悪用される。

どうして防げるか（予防・対策）

- **復元アルゴリズム（p.1520–1540）**で元データを再生成。
- **再保存ハッシュ（p.1581–1600）**で二度と消せない形に。

社会的意義

「データ犯罪の隠蔽を不可能にする」。

事例 28（2022 年 7 月 22 日：国際 EC 詐欺での証拠復元）

- **構成パターン**：I＋H 連携
- **該当ページ**：p.1541–1564（国際標準化提案）, p.1665–1670（国際利用例）

生活犯罪シナリオ

海外通販で偽ブランドを販売する業者。決済ログを消去し逃亡を図るが、I が復元、H が監査証跡を付与して国際警察に提出 → サイト閉鎖。

なぜ問題か

- 国際 EC 詐欺は「証拠消去」で逃げ切られやすい。

どうして防げるか（予防・対策）

- **復元 API（p.1541–1564）**で破壊ログを蘇生。
- **監査証跡（p.1391–1430）**で国際司法でも通用。

社会的意義

「国際生活犯罪をデータで封鎖」。

事例 29（2021 年 11 月 30 日：行政補助金の不正請求防止）

- **構成パターン**：J 単体
- **該当ページ**：p.1632–1664（特殊用途処理）, p.1668–1670（人道 UI）

生活犯罪シナリオ

災害復興補助金を偽団体が不正請求。J システムが人道用途ルートで正規住民を照合し、不正を遮断。

なぜ問題か

- 行政補助金詐欺は生活困窮者の救済を妨げる。

どうして防げるか（予防・対策）

- **特殊用途 API（p.1632–1664）**で申請者を人道条件で判定。

社会的意義

「補助金不正＝生活犯罪を防ぎ、本当に必要な人に届ける」。

事例 30（2020 年 4 月 9 日：国際標準化会議での生活関連技術盗用防止）

- **構成パターン**：J 単体
- **該当ページ**：p.1629–1698（統合プラットフォーム・国際展開）, p.1699–1701（終章）

生活犯罪シナリオ

海外企業が日本発の生活関連 IoT 技術を自社開発と偽って標準化会議へ提出。J が正規台帳を参照して盗用を排除し、日本企業の権利を国際的に守る。

なぜ問題か

- 技術盗用は「生活基盤そのものの安全」を脅かす。

どうして防げるか（予防・対策）

- **統合プラットフォーム（p.1629–1698）**で国際的に認証。

社会的意義

「国際的生活犯罪を標準化の枠組みで防止」。

✅ 第 6 部まとめ

- **H パターン＝証拠保存**：生活詐欺や犯罪の証拠を改ざん不能に残す。
- **I パターン＝復元**：破壊・消去された契約や金融ログを復元し、不正隠蔽を防止。
- **J パターン＝国際用途**：行政補助金不正や国際技術盗用といった生活犯罪を封鎖。
- **社会的意義**：生活犯罪における「証拠不足」「隠蔽」「国際不正」を技術で不可能化し、市民の暮らしを守る。
