令和7年度　インターネット上の偽・誤情報等への対策技術の開発・実証事業

放送波を活用した災害時における偽・誤情報対策技術の開発・実証

成果報告書

2026/3/19

技09_関西テレビソフトウェア株式会社

目次

1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

目次

1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

1-1. 開発・実証のサマリ

アプローチする課題・目指す姿	• 災害時には通信環境の途絶により情報不足に陥ることが多く、わずかな情報に避難住民や災害対策支援者が過敏に反応しやすくなる。そのような状況下においては文脈から切り離された情報が流入し、真偽を確認できない不安から誤解や憶測が連鎖的に広がり、被災地全体の混乱を助長するリスクが高まる。 • 災害時などインターネットが利用できない環境下においても、放送波とブロックチェーンを活用することにより偽・誤情報の拡散を抑制し、避難者や災害対策支援者が信頼できる情報に基づいて判断できる環境の構築を目指す。		
技術区分	情報の拡散防止・無効化技術、真正性保証・信頼性判断支援技術	実施体制 （下線：技術開発主体）	関西テレビソフトウェア(株)、関西テレビ放送(株)、(株)アトラクター、(株)ベリサーブ、(株)Opening Line
対象とするモーダル種	画像、動画、文章（文章はメタデータ・位置情報として活用）		

技術開発の取組・成果

- 前年度実証に引き続き、証明書発行サブシステムと証明書検証サブシステムを開発。実運用を視野に操作性や速度パフォーマンスを大幅に改善。また、両システム上で稼働する「防災コンパス」と「ファクト注釈コード（FAコード：Fact Annotation Code）」を実装。
- 防災コンパスでは、真正性が保証された情報をコンパス上にプロットし、災害時に拡散する偽・誤情報に惑わされない判断を支援。
- ファクト注釈コードでは、拡散された画像に対するファクトチェックの存在有無が確認できる、かつ軽微な変更が画像に加えられた場合でも検知可能な視認性の高いコードを考案。

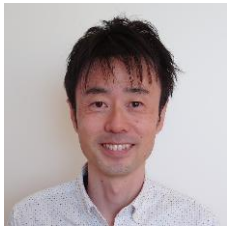
社会実装に係る取組・成果

- 放送に重畳させたデータを、放送局内設備を経由して有線で受信機に配信。放送マスタ管理システムに対して想定される影響の有無および運用上の課題を確認。
- ブロックチェーンを活用した単方向で受信したデータの信頼性確認手法を体系化し、第三者検証企業によるセキュリティ評価を実施。
- ブロックチェーン活用時に必要となる暗号資産について、代払い事業者を介在させることで、ユーザーの主体性を維持しつつ、会計面および税制面での運用負荷の低減が可能であることを確認。

技術開発及び社会実装にあたっての課題・展望

- 社会実装に向けて、実電波を用いたフィールド実証が不可欠となる。段階的な実電波技術検証の実施のために、技術的および運用的な課題の整理を進める。
- 放送データを活用するためには、受信機側におけるデータ蓄積から検証までを安定稼働させる実装設計が重要となる。普及を見据え、低コストでの量産体制に必要な最小限の機能に絞った設計を行う。
- ユーザーの導入条件や予算感に応じて、放送と通信の両方の経路から受信可能なハイブリッド構成の設計。また、災害時に限らず、平時活用を前提とした運用モデルの構築を目指す。

代表者コメント



関西テレビソフトウェア(株)
ソリューションセンター
デジタルデザイングループ
チーフエキスパート
横島 裕明

災害時の偽・誤情報拡散は、信頼できる情報配信による早急な対策が必要です。

弊社では放送波を活用し、通信困難な環境でも切れ目のない安心・安全な情報を届けるため、継続的な開発・実証を重ね、実用化を目指します。

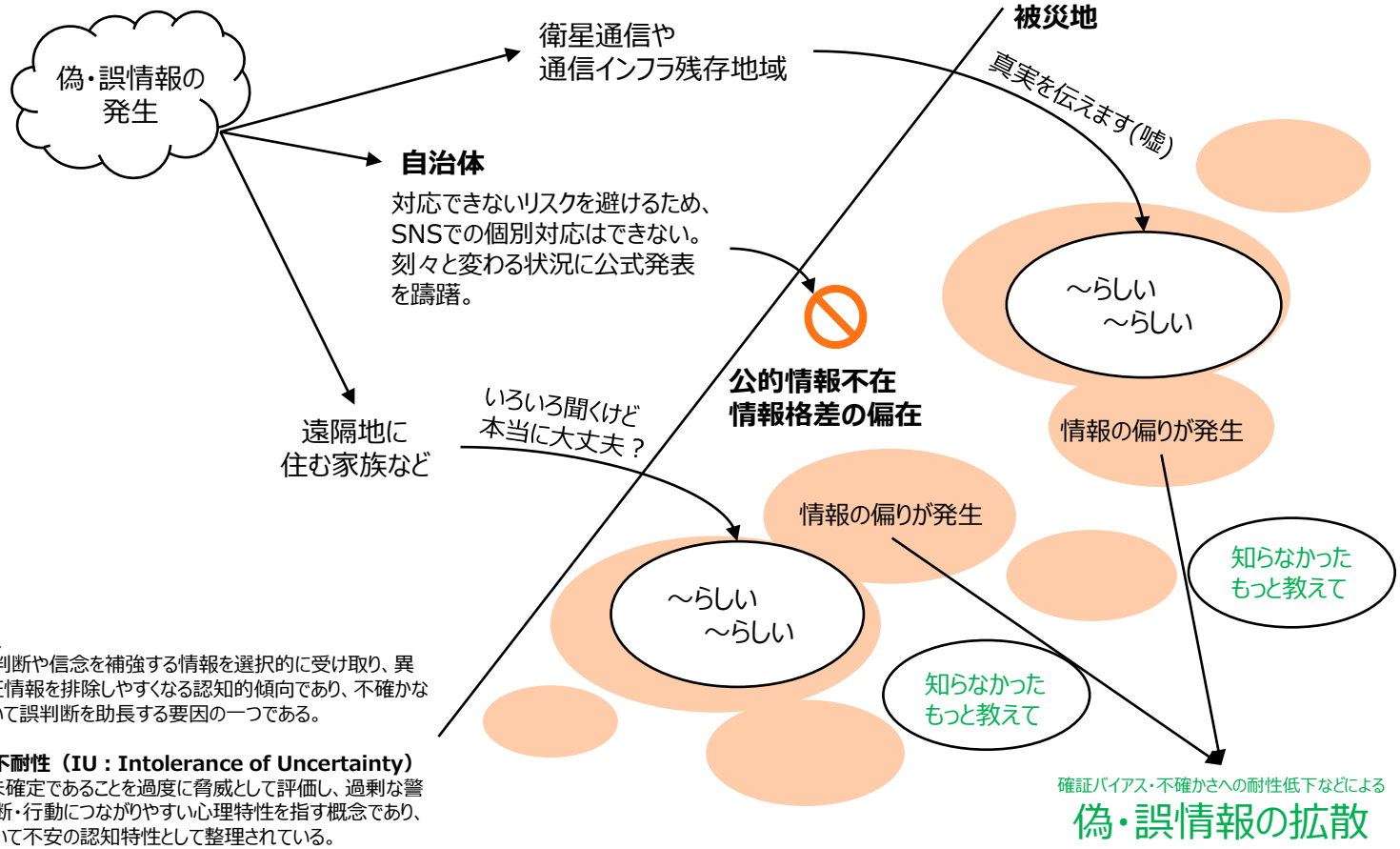
目次

1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

2-1. 開発技術によりアプローチする課題

開発技術によりアプローチする課題

災害時には情報の入手可否や内容に偏りが生じ、被災者や災害時支援者の間で**情報格差**が拡大する。一方で自治体は、対応できない場合のリスクを考慮するとSNSでの個別対応は行えず、また刻々と変わる状況に公的発表は躊躇してしまうため、**公的情報不在**の状況となる。こうした環境では、「どの情報を信頼してよいか」という判断基準が共有されにくくなり、**確証バイアス**（※1）や**不確かさへの耐性低下**（※2）を通じて、信頼構造そのものが変容する。その結果、限られた情報源や断片的な発信に依存する状況が生じやすく、情報の集中や誤解が連鎖的に増幅される。また、関係者へのヒアリングにおいても、災害時においては各組織が多くの異なる情報を元に行動しており、判断の前提となる情報を共有できていない状況が指摘されている。



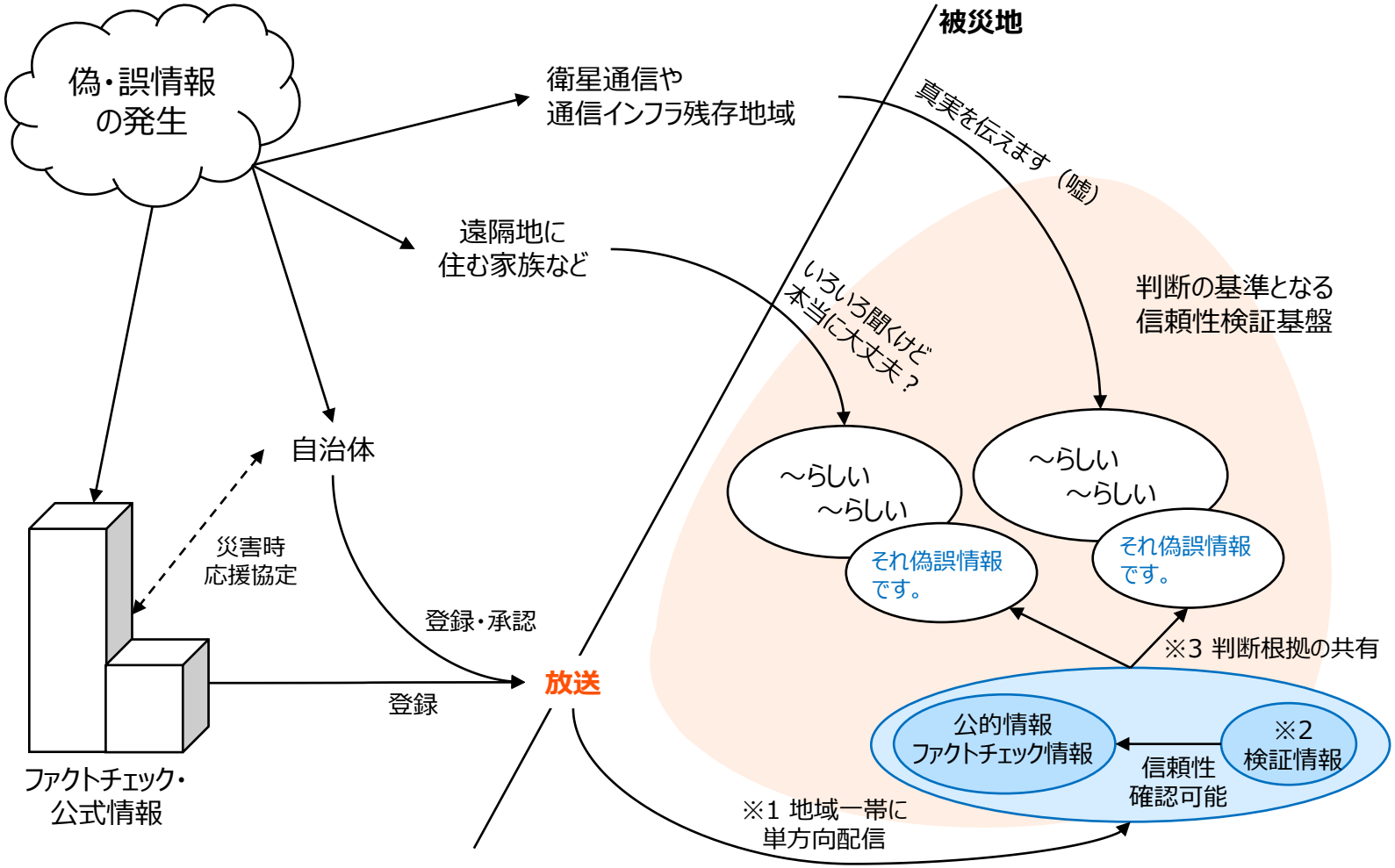
※1 確証バイアス
既に形成された判断や信念を補強する情報を選択的に受け取り、異なる可能性や反証情報を排除しやすくなる認知的傾向であり、不確かな情報環境下において誤判断を助長する要因の一つである。

※2 不確かさの不耐性（IU：Intolerance of Uncertainty）
結果や状況が未確定であることを過度に脅威として評価し、過剰な警戒や不適応な判断・行動につながりやすい心理特性を指す概念であり、臨床心理学において不安の認知特性として整理されている。

2-2. 開発技術により目指す姿・ゴール

開発技術を通して目指す姿・ゴール

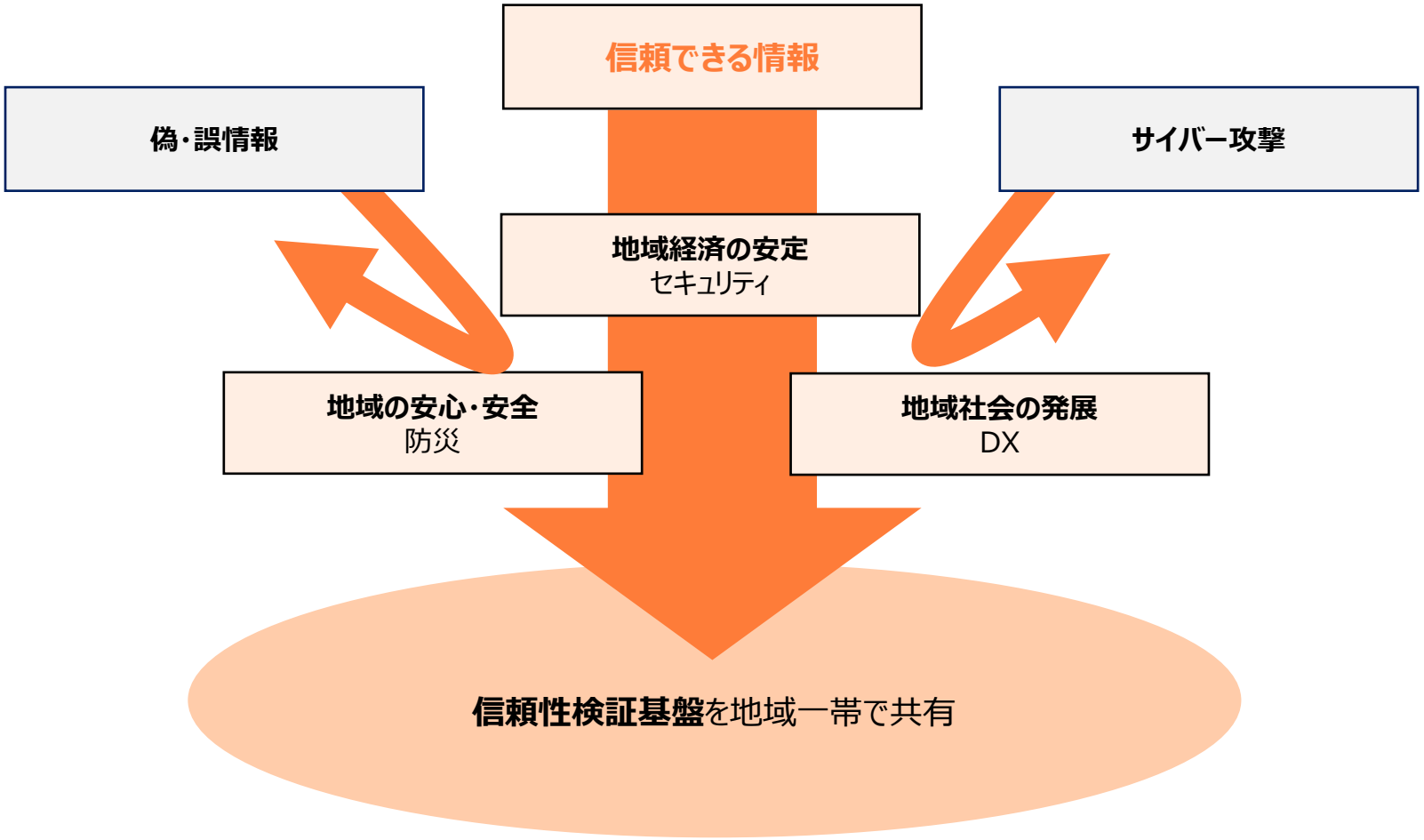
情報を個別に送受信する通信とは異なり、放送で**地域一帯に単方向配信**（※1）する。さらに、配信される情報それ自身の信頼性を確認するための**検証情報**（※2）を付与しておくことで、情報の信頼性確認を受信者側のみで実現する。災害時にSNSや避難所などを介して横断的に広まる偽・誤情報に対して、地域一帯で判断根拠を共有（※3）できる信頼性検証基盤の構築を目指す。



2-2. 開発技術により目指す姿・ゴール

開発技術を通して目指す姿・ゴール

いつでも、どこでも、地域のいたるところで検証可能な**信頼性検証基盤を**共有することにより、偽・誤情報に惑わされることのない社会の実現を目指す。また、平常時から継続的に活用することで、サイバー攻撃や情報の改ざんといった脅威にも強い社会基盤を形成し、災害時の対応にとどまらず、**地域経済の安定**、さらには持続的な**地域社会の発展**までを幅広く支えることをゴールとする。



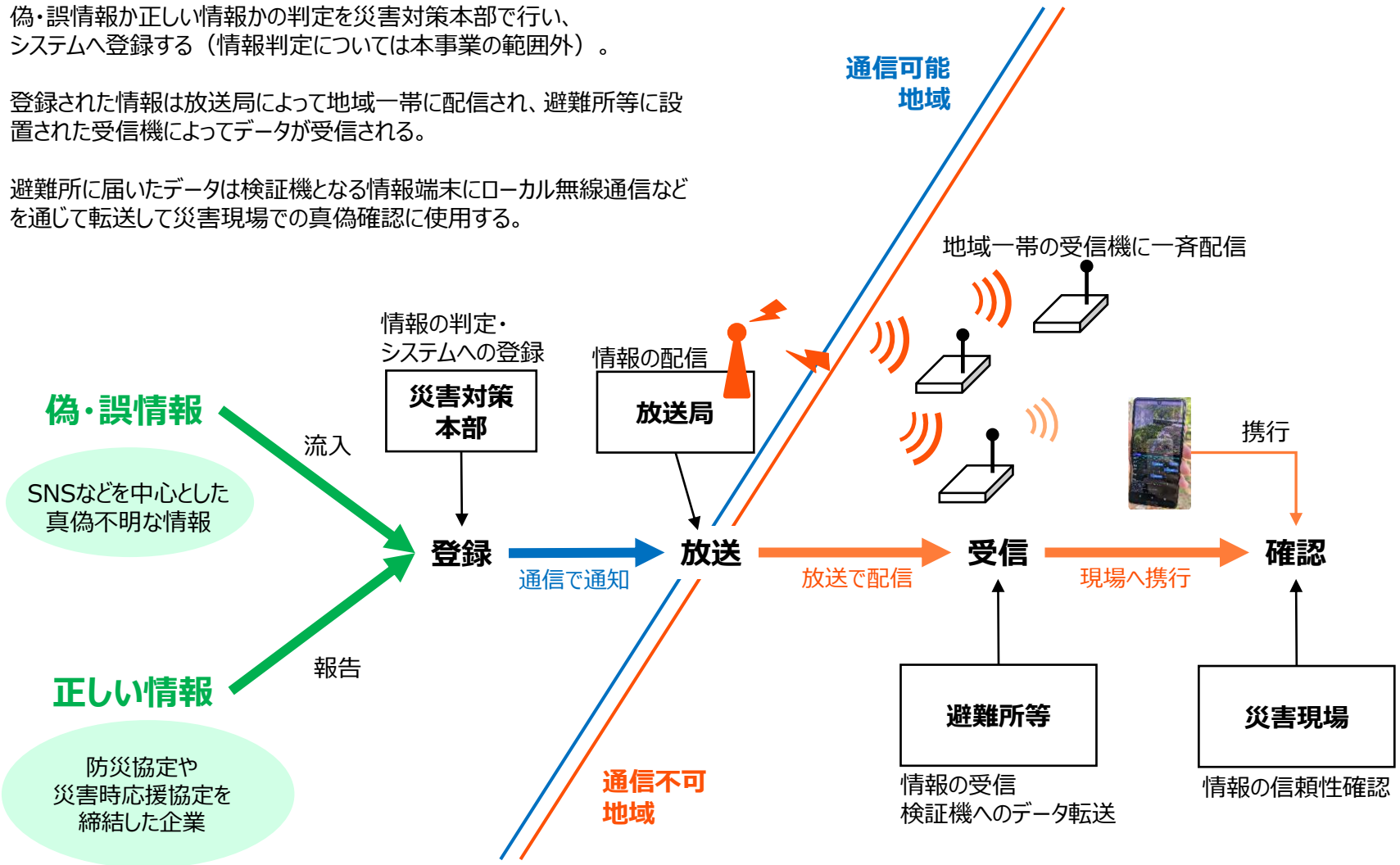
2-3. 開発技術により対処可能なユースケース

開発技術により対処可能なユースケース

偽・誤情報か正しい情報かの判定を災害対策本部で行い、
システムへ登録する（情報判定については本事業の範囲外）。

登録された情報は放送局によって地域一帯に配信され、避難所等に設置された受信機によってデータが受信される。

避難所に届いたデータは検証機となる情報端末にローカル無線通信などを通じて転送して災害現場での真偽確認に使用する。



情報の受信者は災害時や警察や消防、災害時応援企業、避難住民などを想定。

2-3. 開発技術により対処可能なユースケース

災害時に被害が甚大化するリスクに対する偽・誤情報の影響整理

災害時において、偽・誤情報が被害を拡大させる要因として4つの類型（**初動の遅れ、危険側への偏り、未覚知の放置、更新の遅延**）を定義し、本実証で開発したアプリケーションがどのような効果を期待できるかを、避難誘導、物流、医療へのユースケースへ展開するために整理した。

避難誘導の場合

災害時に被害を甚大化させてしまう要因

初動の遅れ	自分は大丈夫と思い込んでしまう正常性バイアスから抜け出せずに逃げ遅れる。
危険側への偏り	先入観で安全・確実と思い込まれていた情報に人や資源が集中してしまう。
未覚知の放置	共有されていない危険を認識できず、想定外のケースとして無視してしまう。
更新の遅延	状況が変化しているにもかかわらず、古い情報が判断基準として残り続ける。

偽・誤情報が与える影響

初動の遅れ	緊急速報をオオカミ少年のように扱う雰囲気の醸成。 強引な避難誘導により、熱中症や転倒などの事故を引き起こす。
危険側への偏り	安全であるはずの避難経路が、過去の動画拡散でふさがっているように感じさせる。 キャパシティを超えた避難所や路地に避難住民が殺到する。
未覚知の放置	連絡が取れない孤立集落が無事であるかのように感じさせる。 延焼寸前、倒壊寸前の建物のそばを安全な避難経路として選んでしまう。
更新の遅延	古い情報に画像や動画が付与されて最新情報として拡散される。

他分野への影響

物流

初動の遅れ	食料品の劣化、燃料の枯渇
危険側への偏り	キャパシティを超えた物資集中
未覚知の放置	孤立集落の把握漏れ
更新の遅延	在庫情報の更新遅れ

医療

初動の遅れ	重症患者の処置遅れ
危険側への偏り	間違った応急処置の拡散
未覚知の放置	自宅待機患者の把握遅れ
更新の遅延	満床情報の更新遅れ

本実証で開発したアプリケーションのユースケースとして整理

防災コンパス

真正性が保証された情報をコンパス上にプロットし、災害時に拡散する偽・誤情報に惑わされない判断を支援。

現在位置を参考に、適切な初動を促す情報をプッシュ型で配信。通信に依存しないことで情報の更新遅延を緩和し、情報に有効期限を設定することで頻繁な情報更新を促し、危険側への偏りを是正すると共に情報の空白地域(未覚知状態)を可視化。

FAコード

拡散された画像に対するファクトチェックの存在有無が確認できる、かつ軽微な変更が画像に加えられた場合でも検知可能な視認性の高いコード。

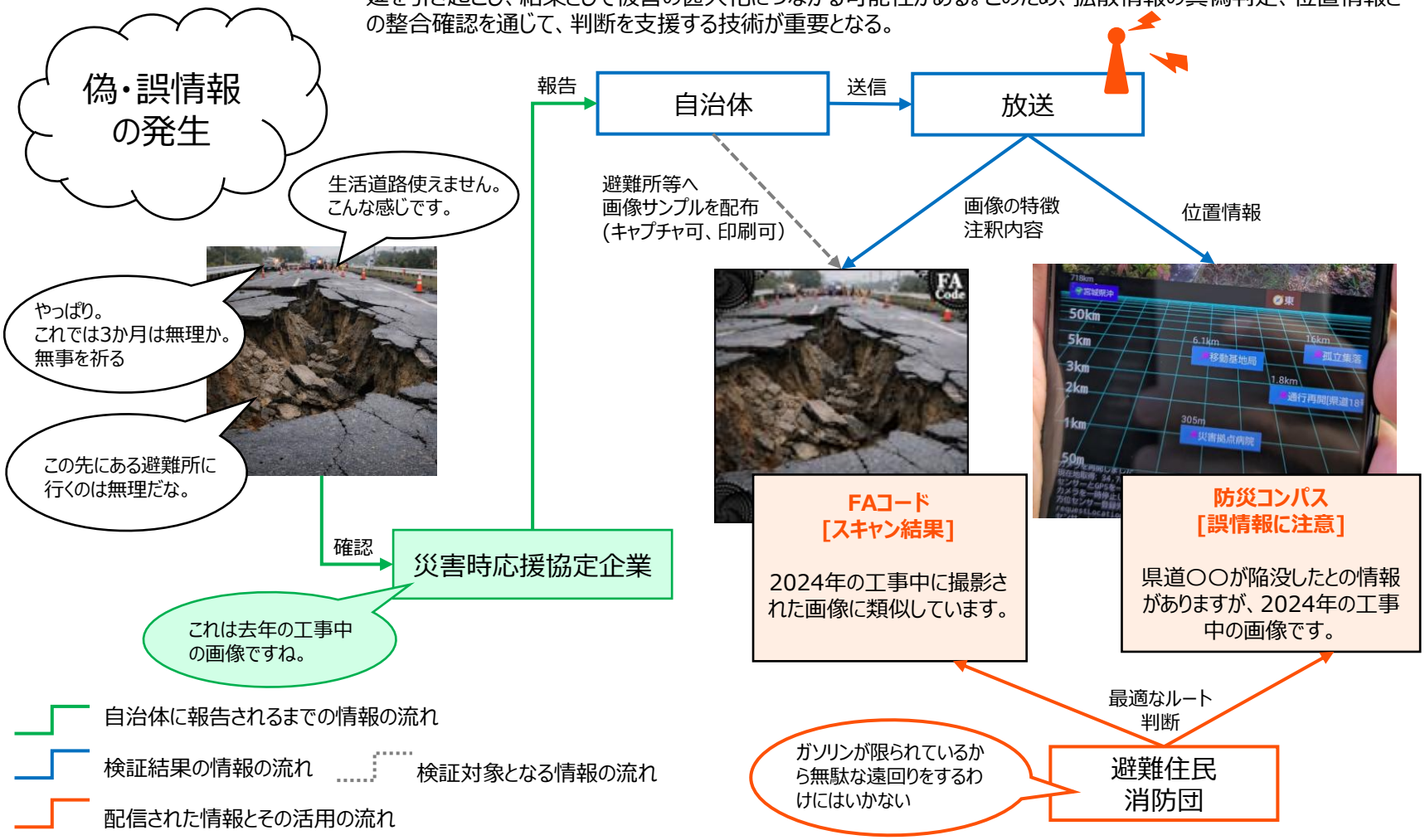
公式画像だけではなくて、拡散された誤画像に対しても情報のタグ付け（注釈）を行うことが可能。また、状況が刻々と変化する地図情報のバージョン管理など柔軟な用途に使用可能。

2-3. 開発技術により対処可能なユースケース

開発技術により対処可能なユースケース

避難所でのユースケース

災害発生直後の避難誘導から避難所での生活に至るまで、避難住民は、断片的かつ不確かな情報に基づいて判断を迫られる。例えば道路状況、受入可否、物資供給状況等に関する誤認が密集、資源の偏在、支援の遅延を引き起こし、結果として被害の甚大化につながる可能性がある。このため、拡散情報の真偽判定、位置情報との整合確認を通じて、判断を支援する技術が重要となる。

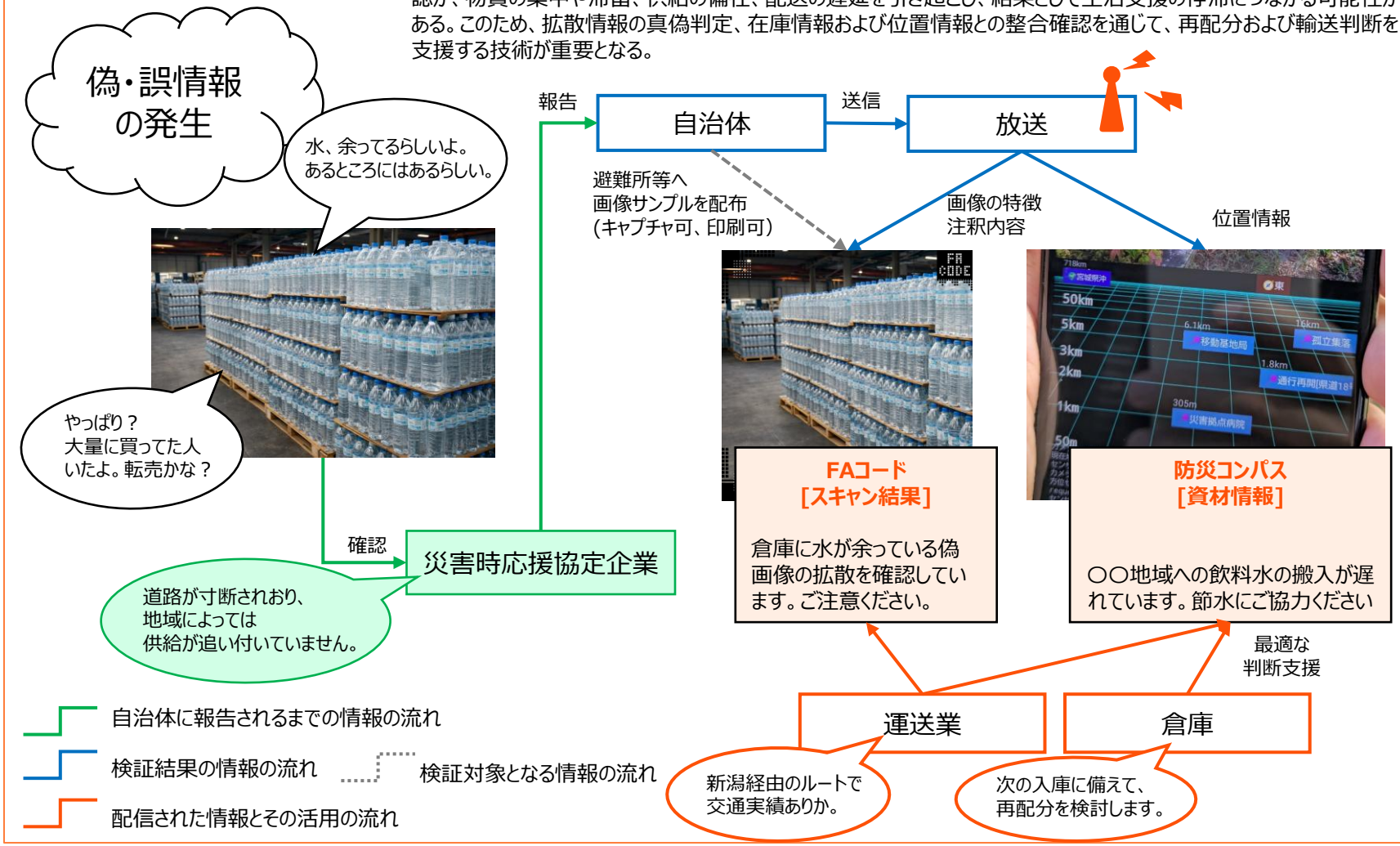


2-3. 開発技術により対処可能なユースケース

開発技術により対処可能なユースケース

物流でのユースケース

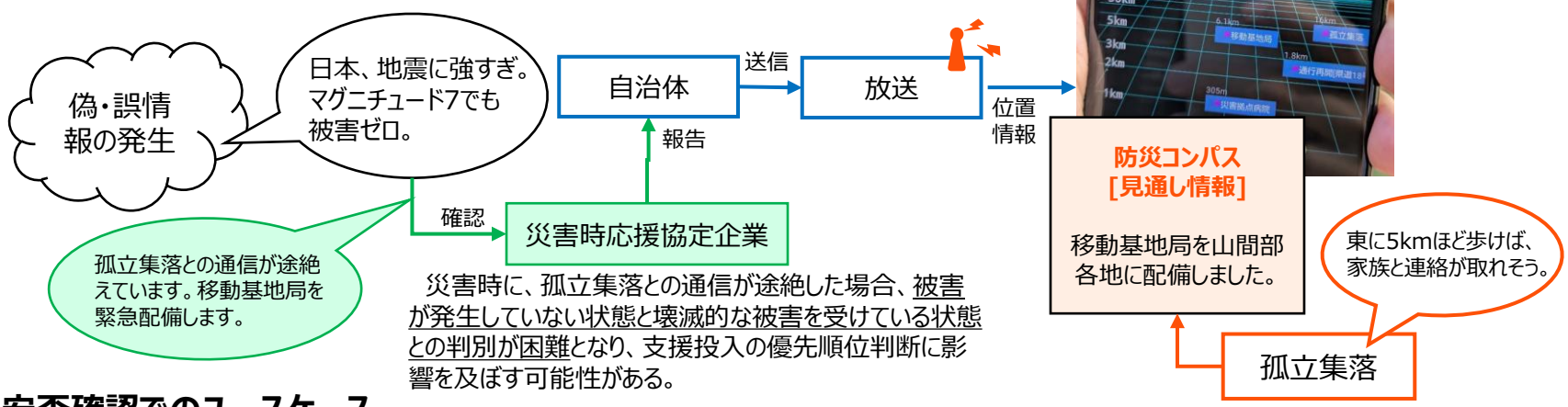
災害発生直後から復旧期に至るまで、物流事業者および物資集積拠点は、断片的かつ不確かな情報に基づいて再配分や輸送判断を迫られる。例えば在庫状況、輸送経路の通行可否、地域ごとの需給逼迫状況等に関する誤認が、物資の集中や滞留、供給の偏在、配送の遅延を引き起こし、結果として生活支援の停滞につながる可能性がある。このため、拡散情報の真偽判定、在庫情報および位置情報との整合確認を通じて、再配分および輸送判断を支援する技術が重要となる。



2-3. 開発技術により対処可能なユースケース

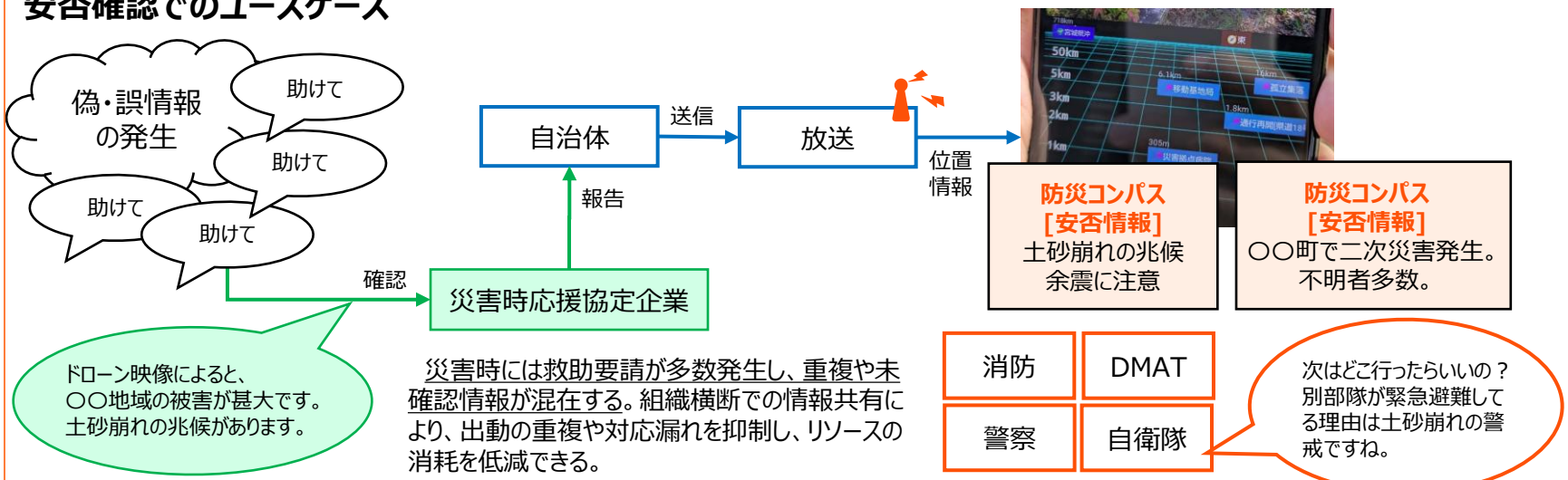
開発技術により対処可能なユースケース

孤立集落でのユースケース



災害時に、孤立集落との通信が途絶した場合、被害が発生していない状態と壊滅的な被害を受けている状態との判別が困難となり、支援投入の優先順位判断に影響を及ぼす可能性がある。

安否確認でのユースケース



災害時には救助要請が多数発生し、重複や未確認情報が混在する。組織横断での情報共有により、出動の重複や対応漏れを抑制し、リソースの消耗を低減できる。

自治体に報告されるまでの情報の流れ　検証結果の情報の流れ　配信された情報とその活用の流れ

目次

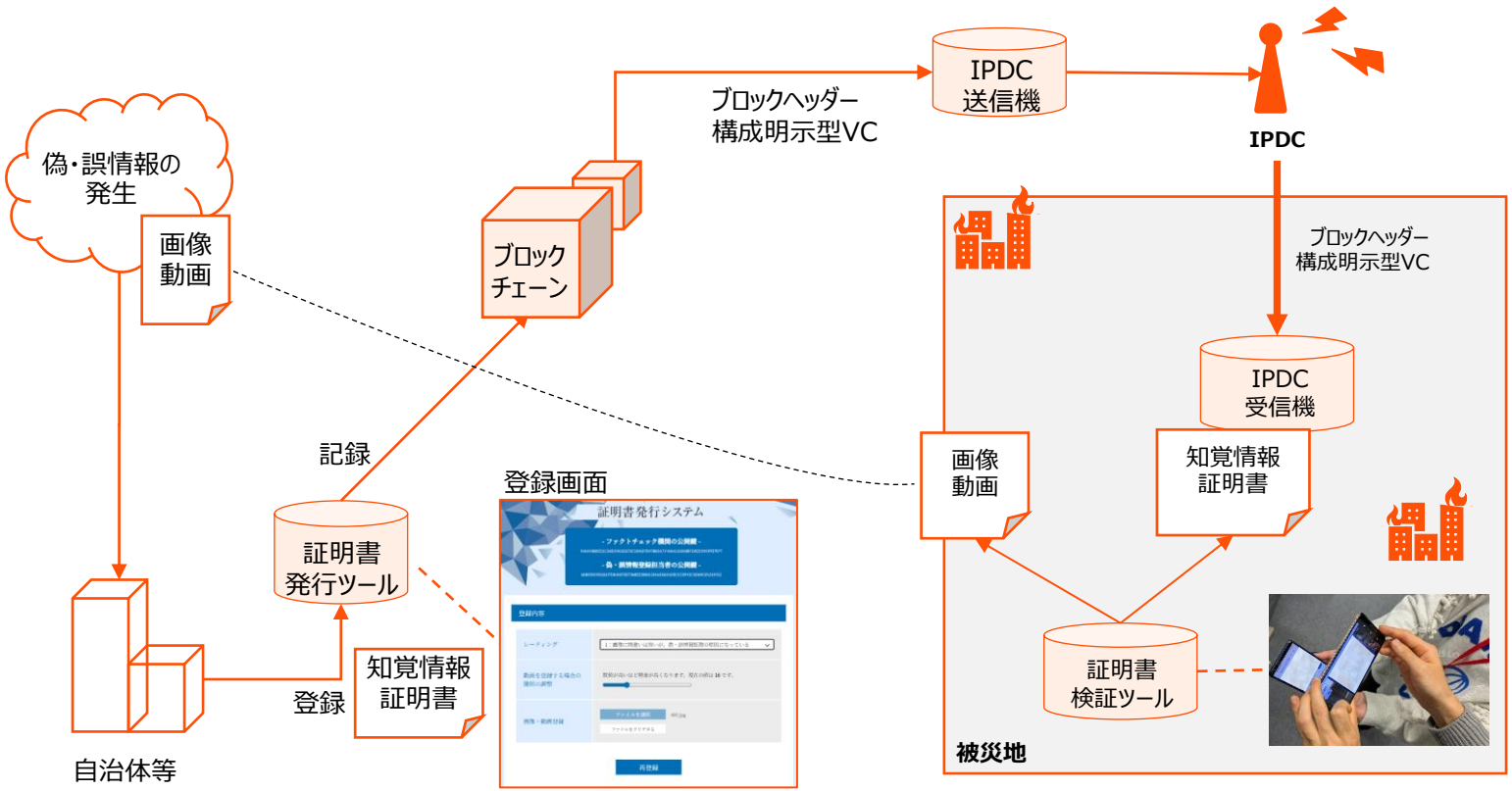
1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

3-1. 技術開発の全体像

技術開発に係る取組・成果の全体像（前年度実証の概要）

前年度実証において、放送波とブロックチェーンを活用し、地域一帯に対して信頼できる情報を配信できる基盤を構築し、その基盤上で開発されたアプリケーションが機能することを実証。送出機から有線で受信機に直接接続することで、電波を用いず検証を実施。また受信機から証明書検証ツールへのデータ転送はUSBメモリを使用した手作業での作業で実施。

放送波を活用した**IPDC**（IP Datacast）技術により、**通信環境に依存せず**に地域一帯へのデータ配信が可能となる。また、改ざん耐性の高い**ブロックチェーン**を活用することで、**通信による信頼性検証を必要とせずに**受信したデータの保存性と信頼性を確保することが可能となっている。

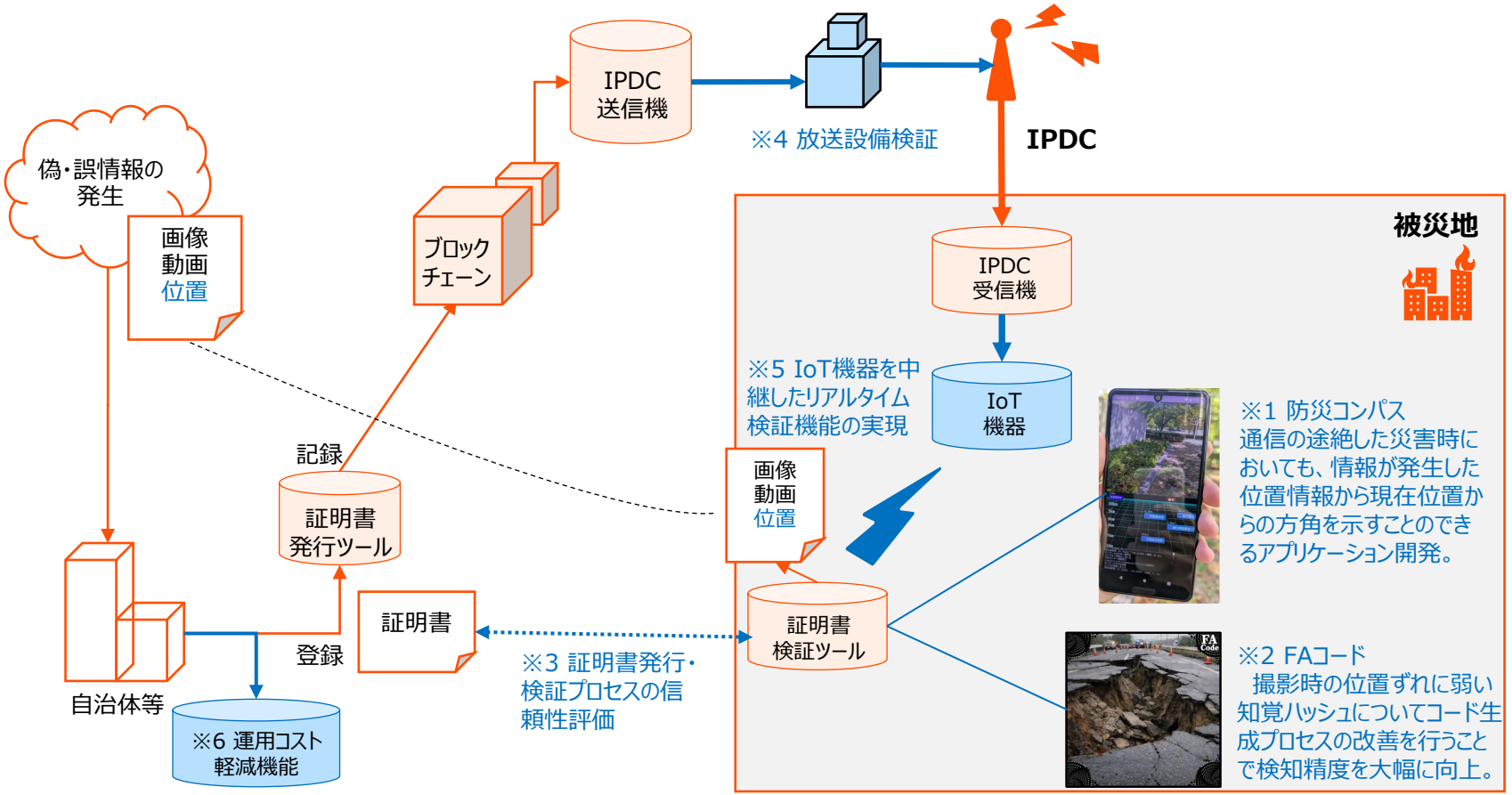


3-1. 技術開発の全体像

技術開発に係る取組・成果の全体像（今年度開発・実証の特徴）

本年度実証において、被災地で発生する偽・誤情報の特徴として、位置情報についても検証可能な情報とし防災コンパスを開発（※1）。また、前年度開発した知覚ハッシュ生成プロセスや検知アルゴリズムを改善して大幅な精度向上を実現した（※2）。

また、本対策技術の有効性等に関する検証として、証明書発行・検証プロセスについて第三者検証企業による信頼性評価を実施（※3）。さらに対策技術の社会実装に向けた取組として、放送局内設備を経由した検証（※4）、IoT機器を中継したリアルタイム検証機能の実現による今後のIPDC受信機普及に向けた環境整備（※5）、運用コスト軽減に向けた環境整備（※6）を実施した。



3-1. 技術開発の全体像

技術開発に係る取組・成果の全体像

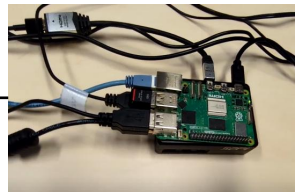
災害時には、通信の途絶などにより、未確認の情報が流通しやすく、結果として判断のばらつきや混乱が生じやすい。このような課題には、放送などのブロードキャストによる情報拡散を防止し無効化する技術、またブロックチェーンを活用した、被災地においても検証可能な真正性保証・信頼性判断を支援する技術が有効である。本年度は、前年度に開発した証明書発行サブシステムと証明書検証サブシステムに大幅な改善を加え、また、本放送に影響を出さないデータサイズの配信でも効率よく機能する、二つの偽・誤情報対策技術を実装した。

証明書発行サブシステム

災害時でも発信者確認が可能な証明書を発行するシステムを開発。本年度開発した下記アプリケーションに対応するためのカスタマイズと送信にかかる様々なコストを大幅に改善。

証明書検証サブシステム

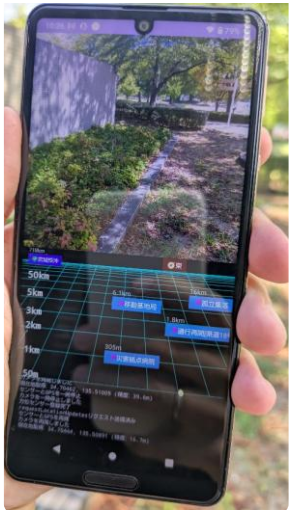
LAN線
(FTP)



ローカルWiFi
(WebSocket)

リアルタイム
検証システム

オフライン環境でも証明書の検証が可能なシステムを開発。検証に係る様々なコストを大幅に改善。



防災コンパス

災害時などの通信が使えない環境においても、利用者が周囲の状況を直感的に把握できる手段として、位置情報と連動したコンパス型アプリケーションを開発。

本アプリケーションは、端末が取得可能な位置情報および方位情報を用いて、信頼性が担保された情報を空間的な方向として可視化する構成とした。

災害時には、地名や文字情報のみでは状況把握が難しい場面が多いことから、利用者自身の現在地を起点として、どの方向にどの情報が存在するかを示すことで、直感的な理解を支援する設計とした。

ファクト注釈コード：FAコード（Fact Annotation Code）

災害時に流通する画像情報について、その真偽や根拠を受信者側で確認できる手掛かりを提供するため、FAコード（ファクト注釈コード）を開発。

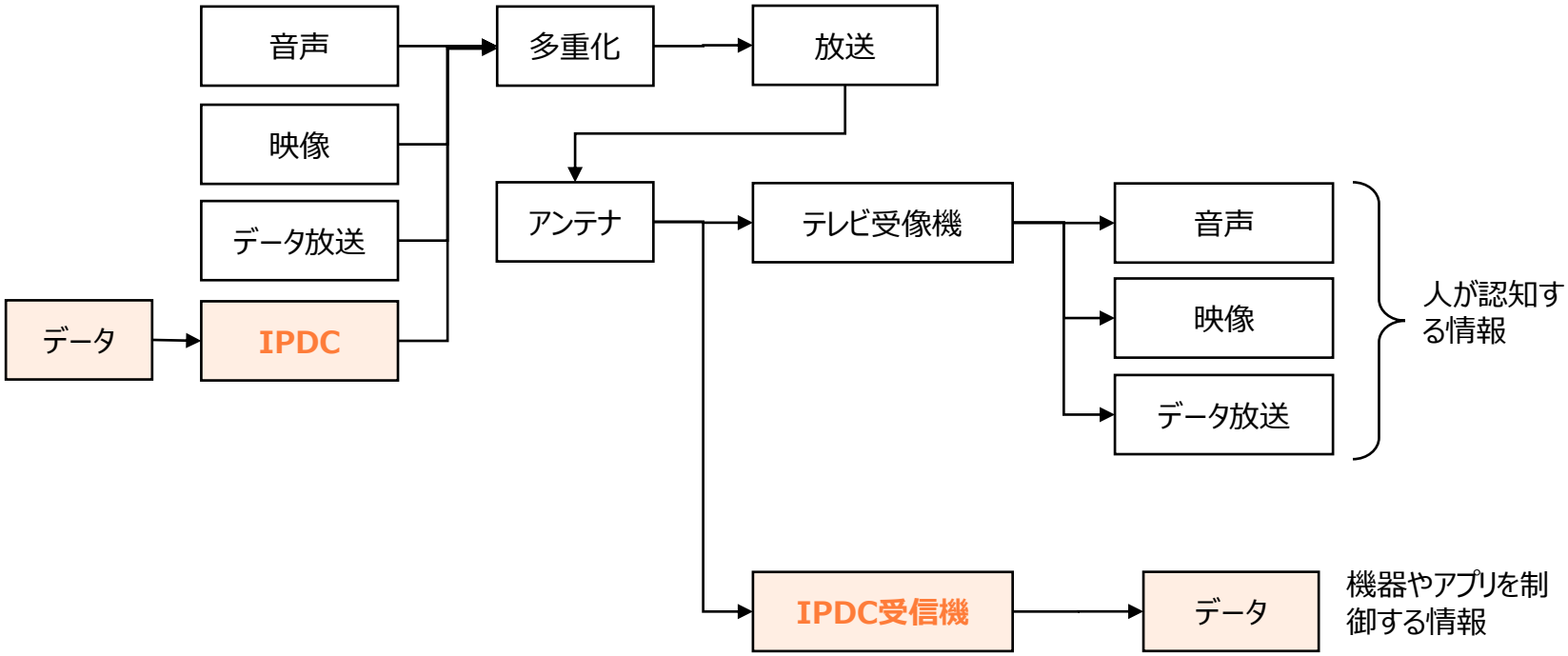
FAコードは、知覚ハッシュ技術を活用する。画像の特徴をコード化して、ブロックチェーン上でそのコードと注釈情報を紐づけることで、災害時などにおいても、流入した写真や画像について、その信頼性を検証することが可能。また、FAコードでは、画像に視認性の高いデザインを付与することで、利用者が直感的にファクトチェック済みであることを認識できる構成とした。

3-2. 技術開発の個別詳細

参考：活用した技術

IPDC (IP Datacast)

IPDC（IP Datacast）は、放送波を用いてIPパケット形式のデータを一方向に配信する技術である。地上デジタル放送や衛星放送の伝送路を利用し、映像・音声とは独立したデータストリームとして情報を広域かつ同報的に届けることができる点に特徴がある。通信回線を前提とせず、受信のみで成立するため、回線輻輳やネットワーク断といった影響を受けにくい。



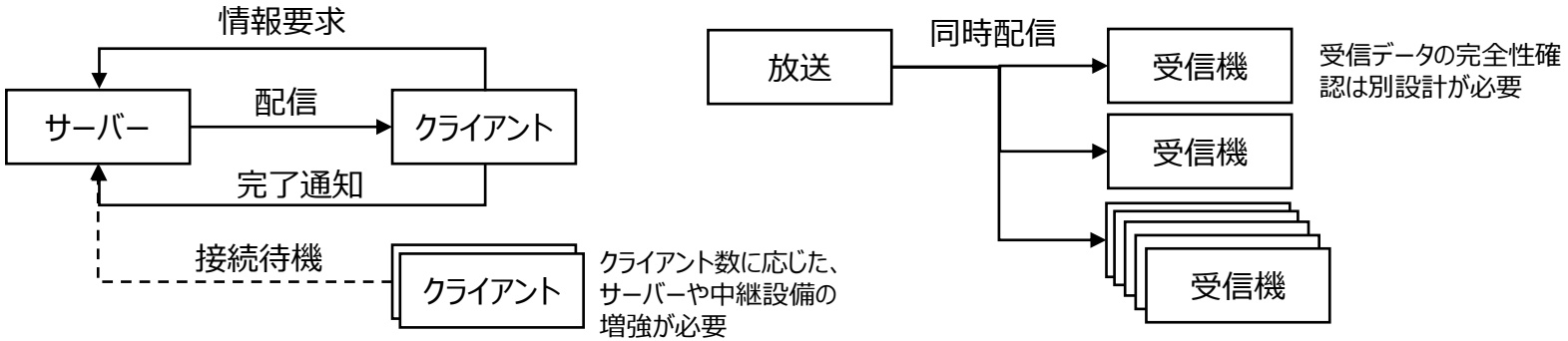
3-2. 技術開発の個別詳細

参考：活用した技術

IPDC (IP Datacast)

IPDCでは、送信側が一度データを放送すれば、受信可能な範囲にある多数の端末が同一内容を同時に受信できる。これは個別通信を前提とするインターネット配信とは異なり、受信者数の増加によって送信側の負荷が増大しないという放送特有の性質を持つ。そのため、広域に対して一斉に情報を届ける用途に適している。

一方で、IPDCは双方向通信を行わないため、受信確認や再送要求といった制御は行えない。このため、放送としての信頼性は「安定した伝送性能」によって担保される一方、受信したデータの正当性や完全性をどのように確認するかは、アプリケーション側の設計に委ねられる。本実証においては、IPDCを「一方向に確実に情報を届けるための伝送基盤」と位置づけ、その上で受信データの正当性や完全性確認を別の技術要素と組み合わせて補完する構成を採用している。



FLUTE(File Delivery over Unidirectional Transport)

本実証では、IPDC伝送におけるデータ配信方式として、FLUTEによる単方向ファイル転送プロトコルを使用する。インターネットの配信方法と比較して、再送制御や誤り訂正を前提とした設計であり、伝送路品質が不安定な環境においても、ファイル単位での完全性を確保した配信が可能であるという特徴を持つ。

また、本実証では単方向配信環境における信頼性確保の手段として、後述するブロックチェーンを使用する。ブロックチェーンは、単位時間あたりに生成されるブロックを順次確定させていくため、FLUTEによるファイル指向の配信方式との親和性が高い。

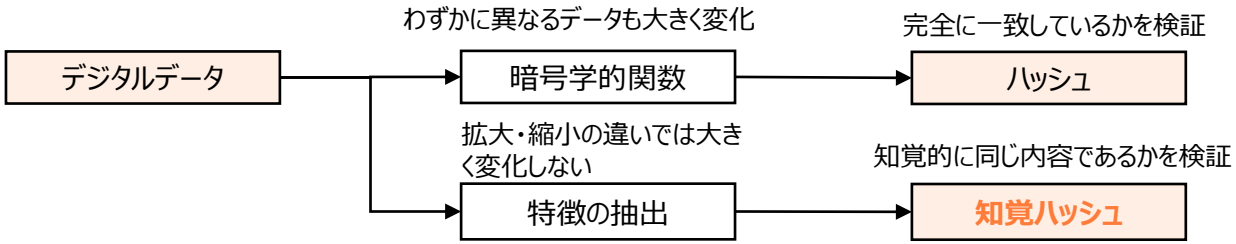
3-2. 技術開発の個別詳細

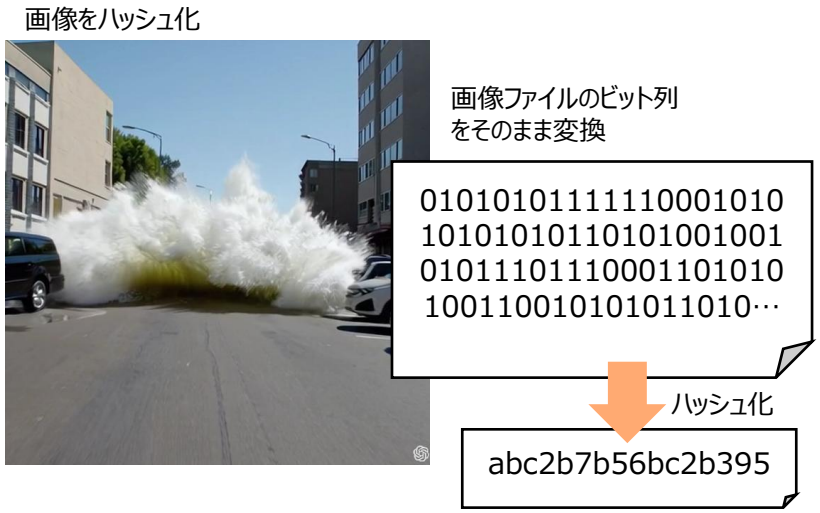
参考：活用した技術

知覚ハッシュ

ハッシュはデジタルデータの内容を一定の長さの値に変換するための仕組みであり、主にデータの同一性確認を目的として用いられる。一般的な**ハッシュ**では、画像のサイズ変更といった軽微な変化であっても出力が大きく変化するという性質を持つ。このため、同一のハッシュ値が得られることは、元のデータが完全に一致していることの強い根拠となる。

知覚ハッシュは、画像などのデータから、人間の知覚に基づく特徴を抽出し、それを固定長の値として表現する。拡大縮小など、人間が内容を同一と認識する範囲の変化については、ハッシュ値が大きく変化しない設計となっている。





3-2. 技術開発の個別詳細

参考：活用した技術

知覚ハッシュ

電子透かしやQRコードとの違い

電子透かしは、画像や音声の内部に識別情報を埋め込む技術。埋め込み処理が行われていないデータに対しては適用できず、また、加工によって透かし自体が失われる可能性がある。これに対し、知覚ハッシュは事前の埋め込み処理を必要とせず、既に拡散している画像にも適用が可能。

QRコードは、外部情報への正確な参照を可能にするが、QRコードが切り取られたりすり替えられた場合はデジタルデータの参照情報として機能しない。一方、知覚ハッシュは対象データの内容そのものからコードを生成するため切り離すことはできない。

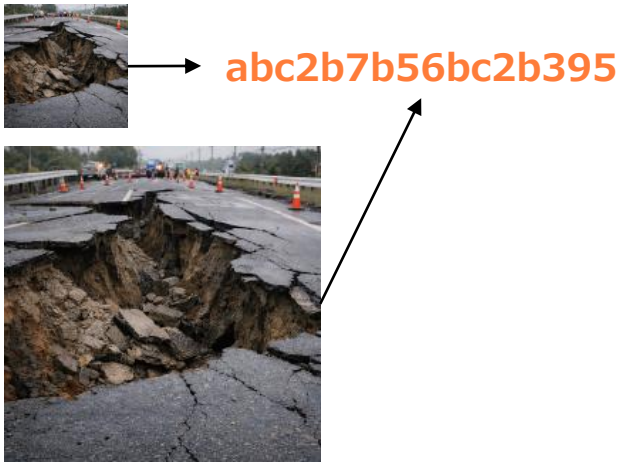
電子透かし

コピー、加工によって情報を失う

QRコード

すり替えによって参照機能を失う

知覚ハッシュ



画像の特徴自体が持つコード

人工知能の視点

人工知能との違い

人工知能は、類似度に基づいて画像を評価する技術であり、同一性を判定する用途には適さない。また、一般にインターネットでのアクセスや相応の計算を必要とするため、通信環境や端末性能に依存する側面がある。

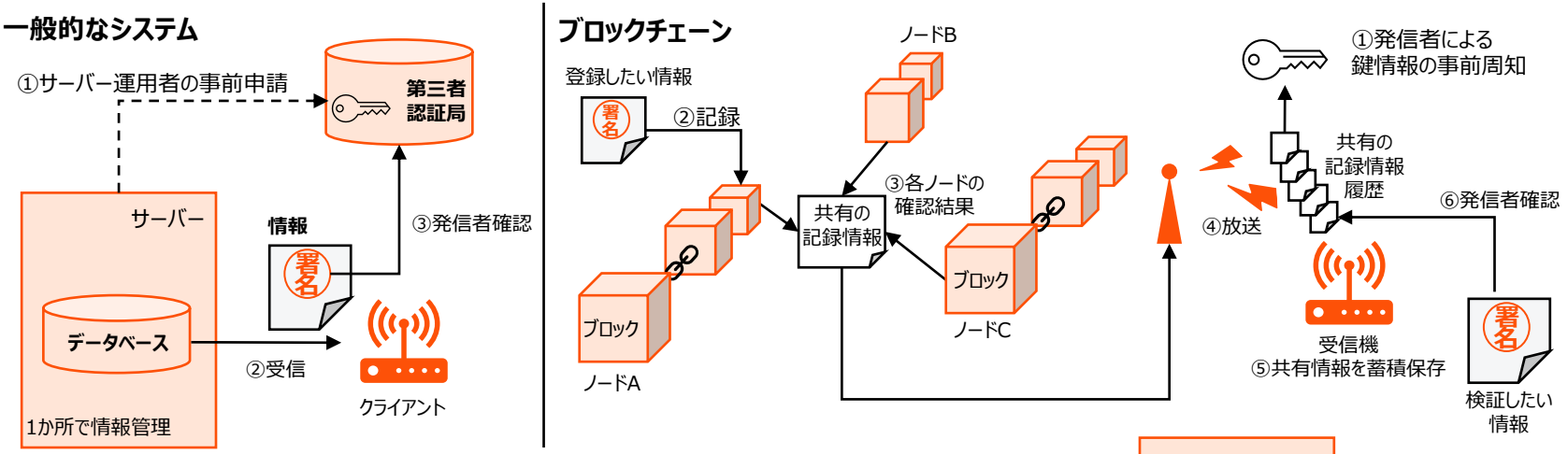
3-2. 技術開発の個別詳細

参考：活用した技術

ブロックチェーン

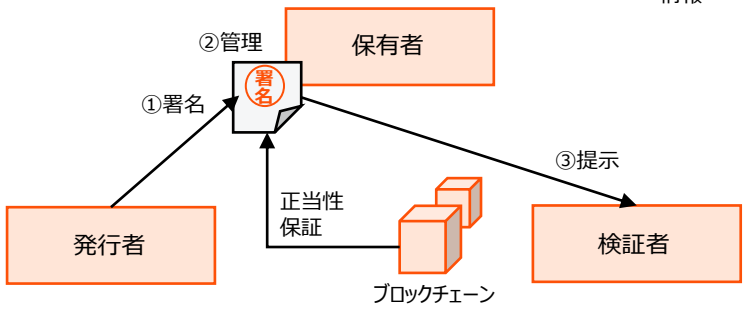
一般的なシステムでは、**情報の信頼性を確認**するために、**第三者認証局**へのインターネットアクセスを前提とすることが多い。そのため、放送のように単方向で情報配信する環境では、同じ方法をそのまま使うことが難しい。一方、ブロックチェーンを活用することで、単方向配信された情報であっても、受信側のみで信頼性検証を行うことが可能となる（詳細は4-2. 検証及び調査の個別詳細：構成明示型VC参照）。

ブロックチェーンは、特定の管理者が1か所で情報を管理するのではなく、同じルールで動作する多数のコンピュータ（ノード）が、それぞれ記録を確認しながら保存・検証する仕組みである。**各ノードの確認結果**は一定の時間ごとに完全に一致するよう保たれており、この**共通の記録情報**を参照することで、特定のサーバーに頼らなくても、記録内容が途中で改ざんされていないかを確認することができる。また、特定の事業者のシステムに依存しないため、災害時のサービス障害や、いざ使おうとした際に利用期限が終了しているといったリスクを低く抑えられる。



VC（Verifiable Credential：検証可能な証明書）

発行者が署名したデジタル証明書を、保有者が第三者である検証者に提示する。検証の際には特定のサービスが管理するサーバーへのアクセスを必要とせず、ブロックチェーン上に記録された情報を参照することで証明書の正当性を確認できる。このように、発行・保持・検証の各主体が特定サービスへの接続を前提としない構成であるため、VCは放送などの単方向配信による情報伝達とも整合しやすい。



3-2. 技術開発の個別詳細

参考：活用した技術

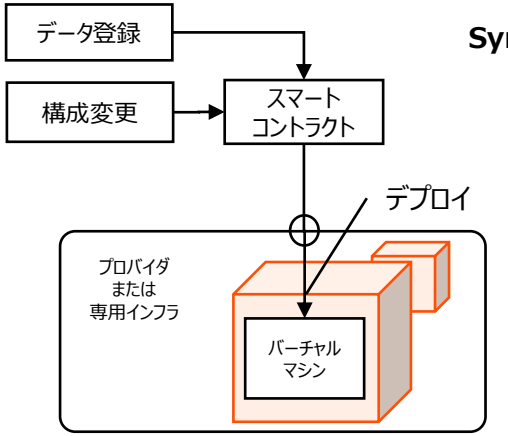
Symbolブロックチェーン

ブロックチェーンにはSymbolを採用する。まずSymbolは、**CRYPTREC**（※1）において評価対象とされている電子署名方式 **ed25519**（※2）を採用しており、公的な用途での技術選定において採用根拠の説明が容易となっている。

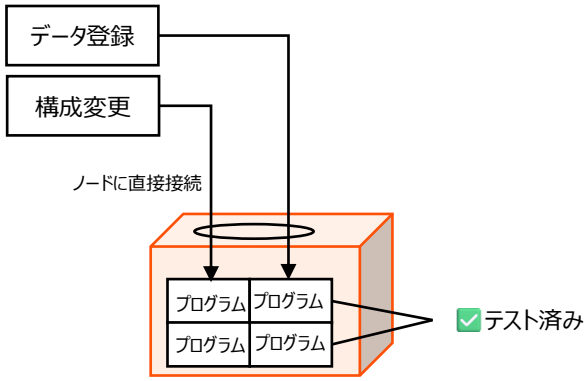
また、Symbolは電子署名の条件や手順などをプログラムする**スマートコントラクト**を自由に公開する方式ではなく、あらかじめ定義されたテスト済みプログラム機能の組み合わせによってブロックチェーン操作を実行する。これにより、安全性の確認されていないプログラムがネットワーク上に公開されてしまうなどのセキュリティリスクを構造的に排除している。スマートコントラクト専用言語を前提としない構成であるため、複雑なプログラム言語の習得や高度な監査体制の準備をする必要がなく、組織内の既存リソースを有効活用してコストを抑えた段階的展開が可能となる。

さらに、Symbolはブロックチェーンへの接続先について、特定のサービスや専用インフラに依存せず、公開ノードへ直接接続することができる。結果として、災害発生時に運用を継続するための冗長構成を必ずしも自前で準備する必要がなく、初期導入時および運用コストを抑制することができる。

一般的なスマートコントラクト対応ブロックチェーン



Symbolブロックチェーン



※1 CRYPTREC（Cryptography Research and Evaluation Committees）
日本政府の関連省庁が連携して運営する暗号技術評価プロジェクト。電子政府で利用する暗号技術の安全性や妥当性について評価・整理を行い、推奨リスト等を公表している枠組み。特定の製品を認証する機関ではなく、暗号アルゴリズムの評価基準を整理する役割を担う。

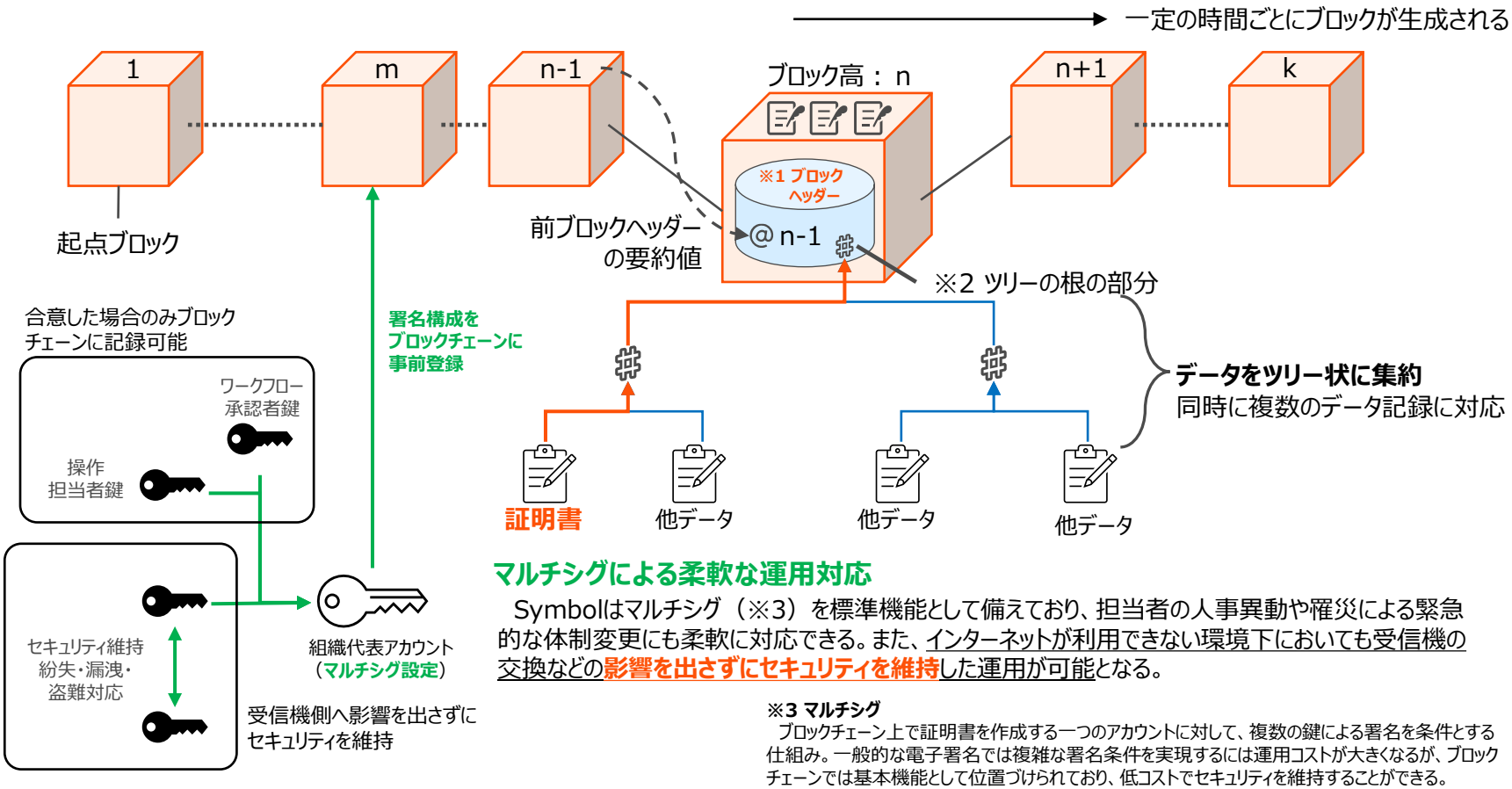
※2 ed25519
楕円曲線暗号の一種であるEdDSA（Edwards-curve Digital Signature Algorithm）に基づくデジタル署名方式。高速で実装しやすく、乱数生成の不備による致命的な事故が起きにくい設計特性を持つ。公開鍵暗号による署名方式の一つとして広く利用されている。

3-2. 技術開発の個別詳細

参考：活用した技術

ブロックチェーンへデータ（証明書）への記録と検証の仕組み

一定の時間ごとに各ノード間で一致させる小さいデータサイズの「共通の記録情報」を**ブロックヘッダー**（※1）と呼び、ブロックチェーンに記録したデータはブロックヘッダーにその「痕跡」が残されている。ブロックヘッダーは同時に複数のデータ記録に対応するため、それぞれのデータのハッシュ値をツリー状にしてまとめ上げ、その根となる部分（※2）のみがブロックヘッダーに保存される。ブロックヘッダー上に証明書データの「痕跡」を確認することができれば、そのデータはブロックチェーンの特性により、改ざんされずに保存されていることが保証される。



マルチシグによる柔軟な運用対応

Symbolはマルチシグ（※3）を標準機能として備えており、担当者の人事異動や罹災による緊急的な体制変更にも柔軟に対応できる。また、インターネットが利用できない環境下においても受信機の交換などの**影響を出さずにセキュリティを維持**した運用が可能となる。

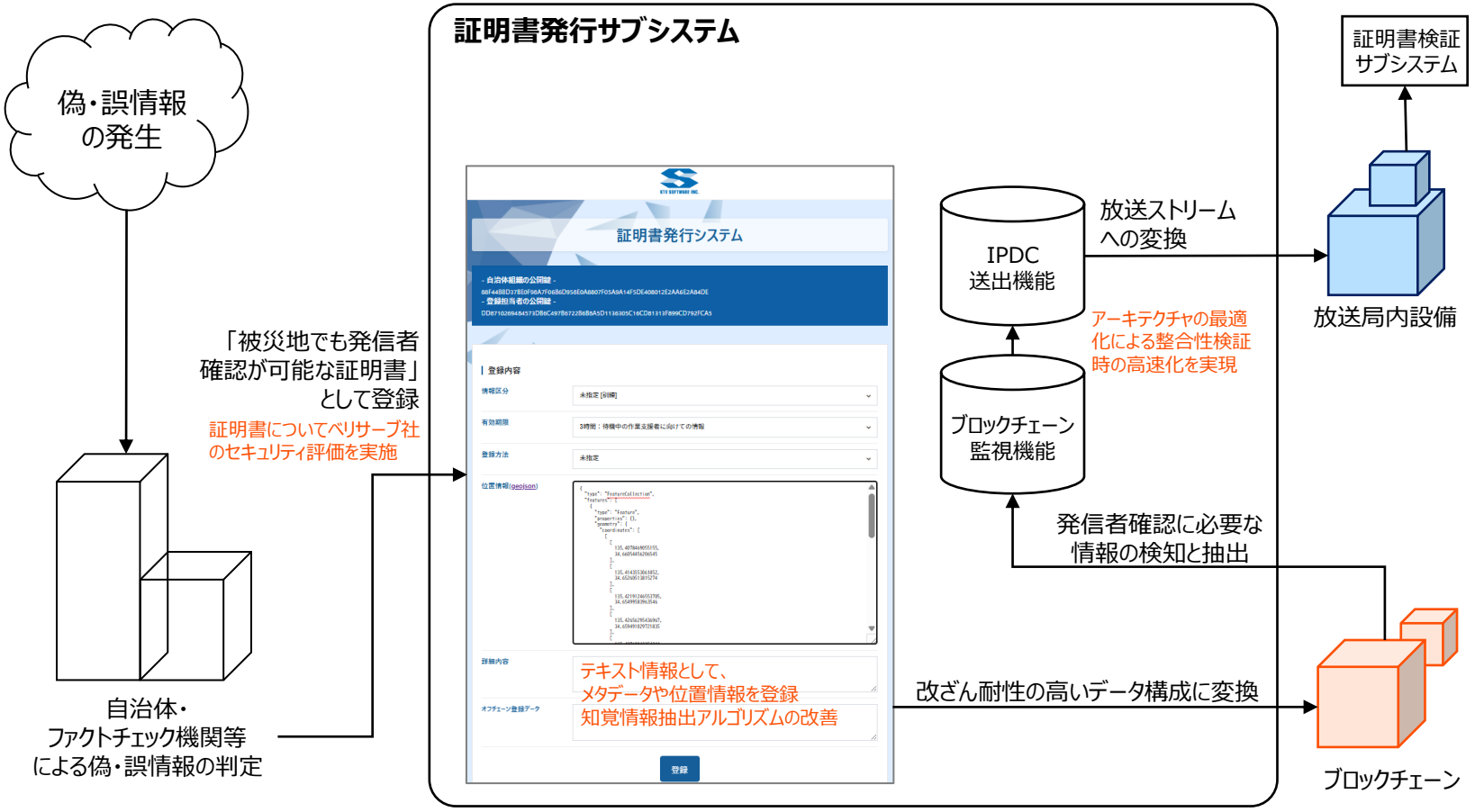
※3 マルチシグ
ブロックチェーン上で証明書を作成する一つのアカウントに対して、複数の鍵による署名を条件とする仕組み。一般的な電子署名では複雑な署名条件を実現するには運用コストが大きくなるが、ブロックチェーンでは基本機能として位置づけられており、低コストでセキュリティを維持することができる。

3-2. 技術開発の個別詳細

システム構成　ー証明書発行サブシステムー

本実証で開発する偽・誤情報対策技術は「**証明書発行サブシステム**」と「証明書検証サブシステム」で構成される。

本サブシステムは前年からの継続開発であり、本年度は特に、テキスト情報への範囲拡大（メタデータとしての活用や位置情報としての活用）、整合性検証の高速化に向けたアーキテクチャの最適化、知覚情報抽出アルゴリズムの改善を行うことで、ユーザー体験を向上させることができた。
また、対策技術の有効性等に関する検証及び調査として、被災地でも発信者確認が可能な証明書発行についてベリサーブ社によるセキュリティ評価を実施した。

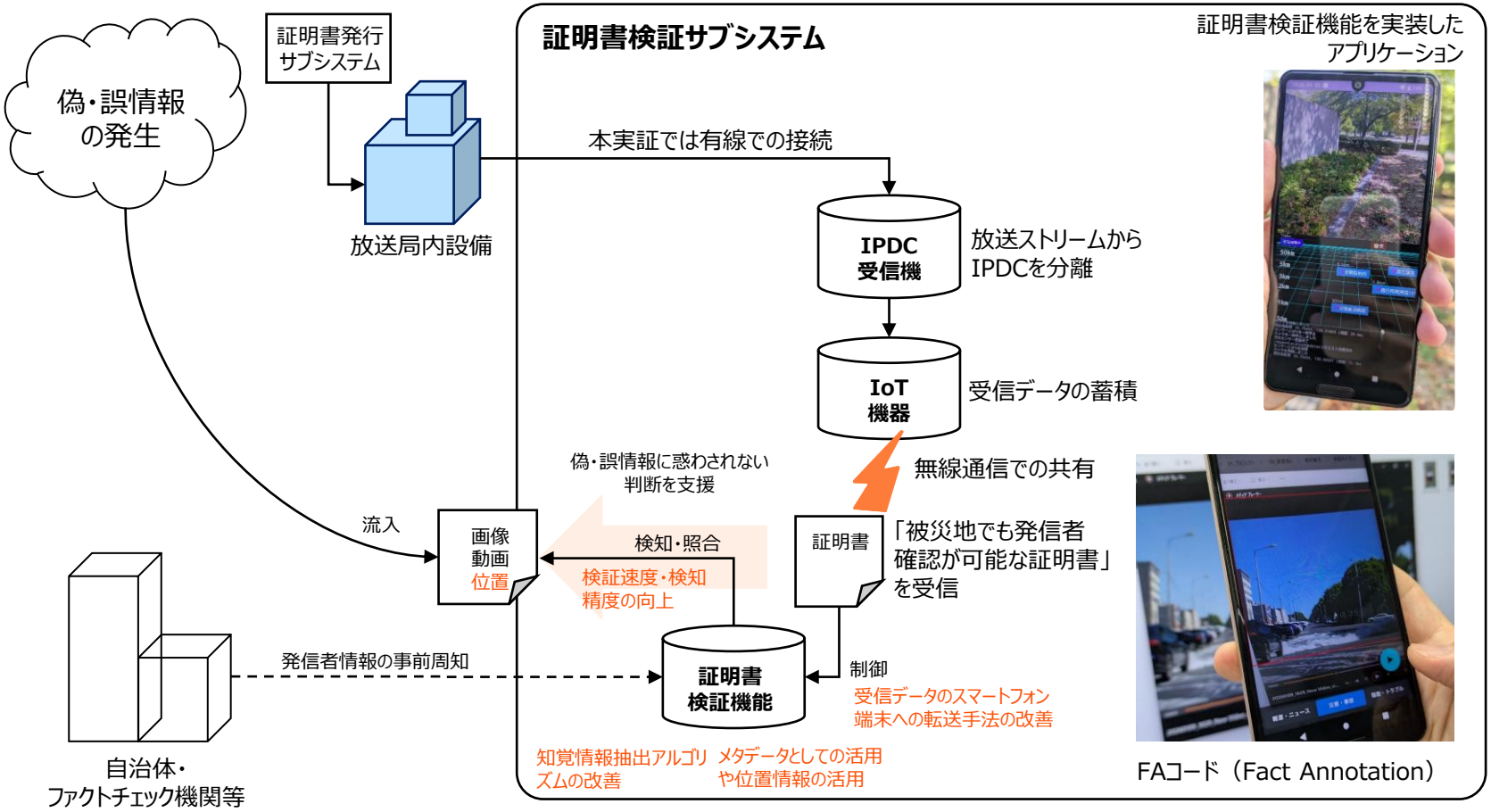


3-2. 技術開発の個別詳細

システム構成　ー証明書検証サブシステムー

本実証で開発する偽・誤情報対策技術は「証明書発行サブシステム」と「**証明書検証サブシステム**」で構成される。

本サブシステムは前年からの継続開発であり、本年度は特にテキスト情報への範囲拡大（メタデータとしての活用や位置情報としての活用）、検証速度・検知精度の向上、受信データのスマートフォン端末への転送手法の改善、知覚情報照合アルゴリズムの改善を行うことでユーザー体験を向上させることができた。
また、対策技術の有効性等に関する検証及び調査として、被災地でも発信者確認が可能な証明書検証についてベリサーブ社によるセキュリティ評価を実施した。



3-2. 技術開発の個別詳細

防災コンパス（位置情報と連動させたコンパス型アプリケーション）ー位置としての情報活用ー

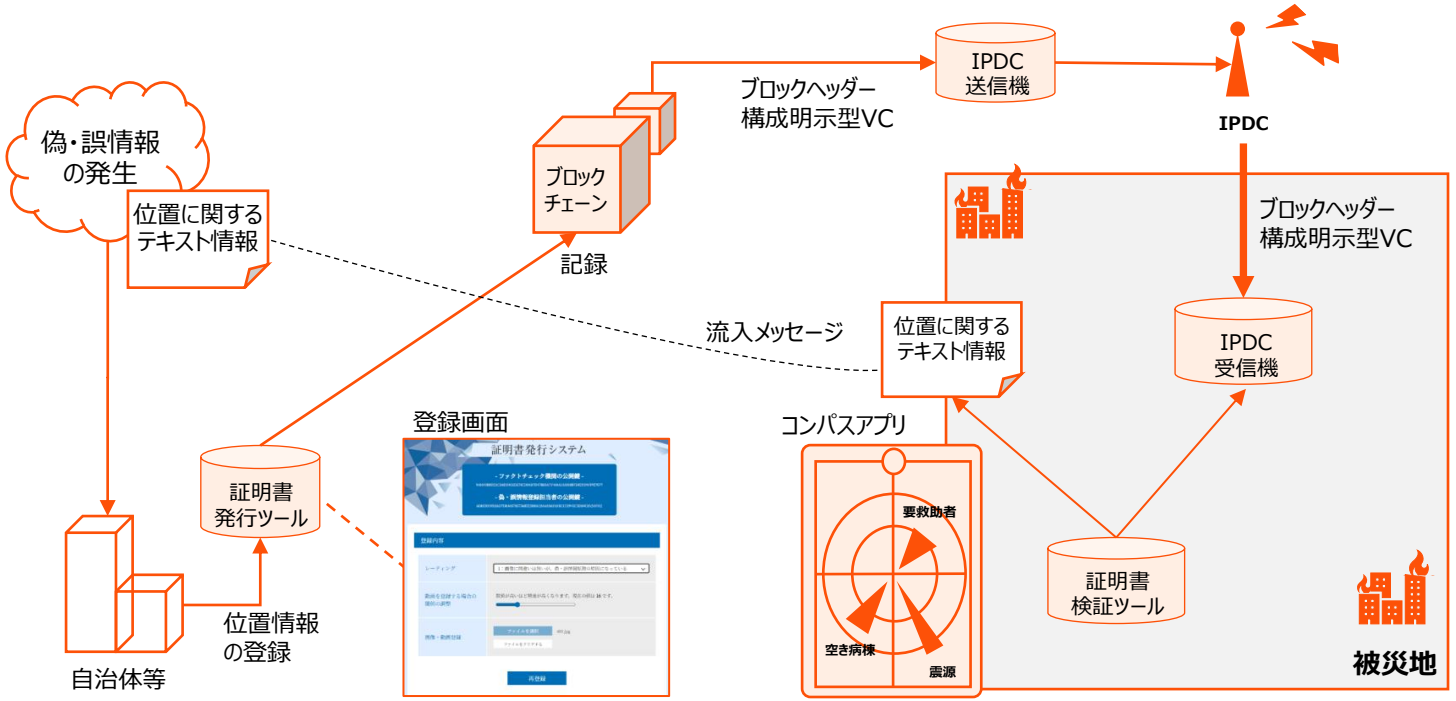
アプリケーション概要

災害時には、SNS等で拡散される偽・誤情報に惑わされず、現場で本当に必要な情報を識別できることが重要である。こうした現場支援を支える手段として、真偽が確定した災害関連の投稿に含まれる地名や施設名から位置情報（緯度・経度等）を登録することで、それを受信端末にGPSで測位した現在位置からの「方角情報」として提示できるアプリケーションを開発した。

このアプリケーションにより、災害対策支援者は場所に関する通報や相談を受けた際にアプリケーション上に提示される方角と照合し、情報の信頼性を正確に評価できる。

新規性と独自性

既存の災害情報アプリケーションが「情報の提供」を目的としているのに対し、本アプリケーションは「何を根拠に判断するか」という前提を利用者間で揃えることを目的としている。通信が不安定な状況でも同一の情報を参照できる仕組みにより、偽・誤情報が混在する状況においても共通の根拠に基づいた判断を可能とする点が特徴である。



3-2. 技術開発の個別詳細

防災コンパス（コンパス機能）

アプリケーション利用イメージ

方位磁石表示

チップ表示
左上に距離詳細

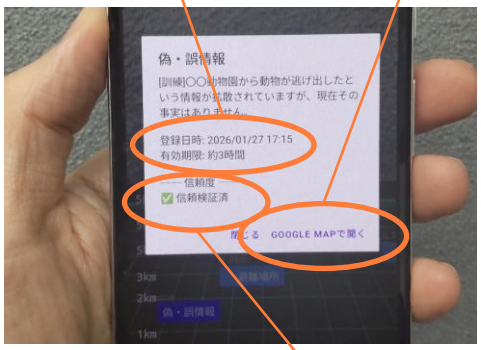
直近で発生した地震

現在地からの距離を
対数スケールで表示
近距離の情報を多く
表示可能

ログ表示エリア

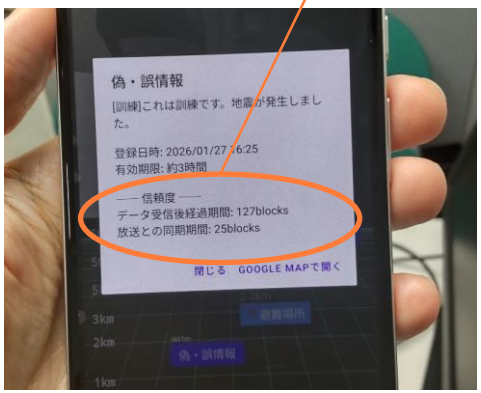
事前ダウンロード（オフライン）に
対応している地図アプリとの連携

情報の登録日と有効期限を明示



事前に周知されたトラストアンカー（信頼基点）
に到達できれば信頼性検証済みマークを表示。

トラストアンカーに到達できなかった場合は、
放送と同期した期間を信頼度として表示



3-2. 技術開発の個別詳細

防災コンパス（登録機能）

位置情報登録サブシステム画面

登録内容

情報区分

訓練、偽・誤情報、復旧情報、規制情報、見通し情報
安否情報、資材情報、制御情報　より選択

有効期限

3時間、12時間、3日間、2週間　より選択

公式情報は常時閲覧可能が一般的であるが、災害時においてはそのアクセス容易性が発信を躊躇させ、また古い公式情報が誤情報として扱われてしまう。

登録方法

情報提供、公式情報、緊急速報　より選択
（ブロックチェーンに記録する方法が異なる）

「情報提供」はマルチシグにより自治体担当者の承認を必要とする登録を想定。「公式情報」は自治体が暗号資産を所有せずにWeb3企業による暗号資産代払いによる登録を想定。緊急速報はブロックチェーンの承認プロセスを待たずに、未承認状態でIPDC配信する運用を想定。

位置情報

インターネット標準仕様で定められた、GeoJSON形式（RFC7946）で指定。

詳細内容

コメントの登録
（登録内容は暗号化して記録）

3-2. 技術開発の個別詳細

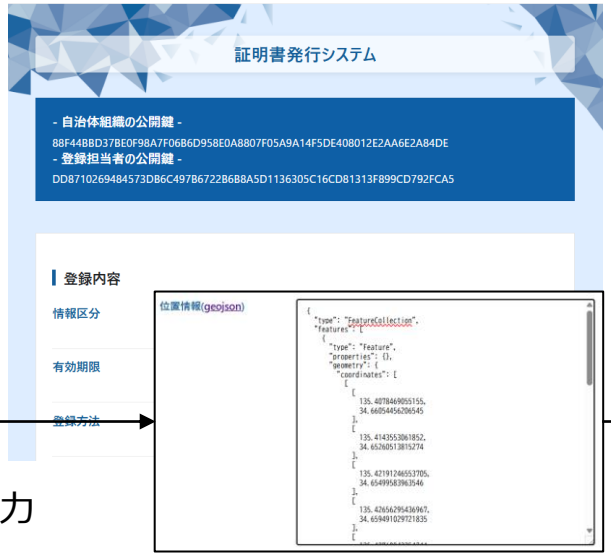
防災コンパス（その他の機能）

通知機能

防災コンパスには、今後の拡張性を見据えてプッシュ通知機能を実装。地図アプリなどでエリア指定して登録すると、受信機側の位置情報と照合してエリア内であればプッシュ通知を送ることができる機能。これにより、災害時に対象地域のIoT機器のみを信頼できるデータで遠隔制御することができる。

GeoJSONエディタで
津波の到達予想
地域を枠で囲む

リスト形式の
GeoJSON出力



登録システムに登録

IPDC放送

判断の根拠となる情報
を対象地域内のIPDC
機器を遠隔制御

津波到達エリア内のスマートフォンにプッシュ通知

3-2. 技術開発の個別詳細

防災コンパス(評価)

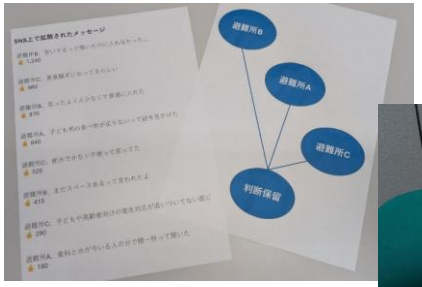
防災コンパスを使用して、災害時における避難所選択の判断支援に関する実験を実施。

初めに、避難所に関するSNS投稿を「いいね数順」で提示。

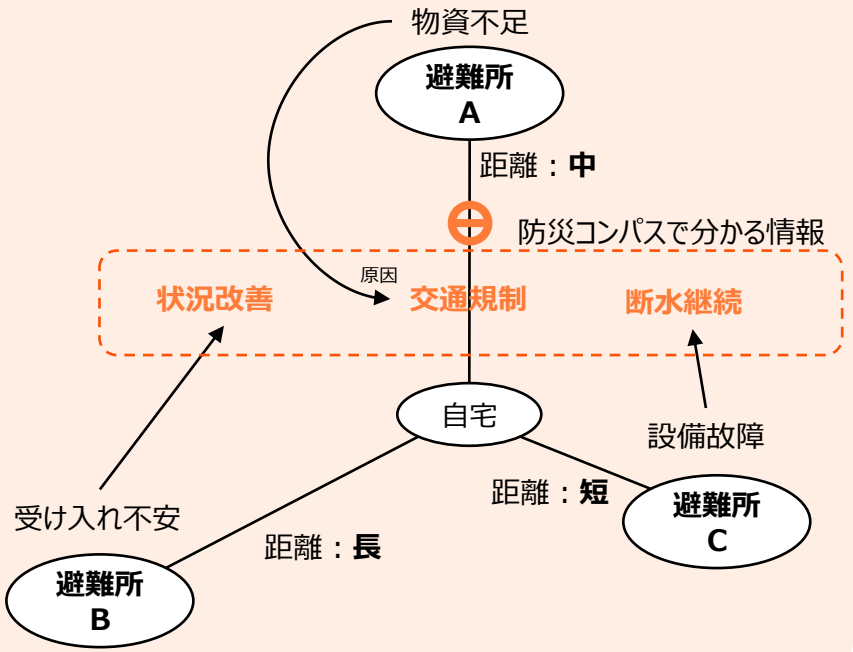
避難所Aに関する物資不足を示唆する投稿
避難所Bに関する「入れた」「入れなかった」という相反する投稿
避難所Cに関する断水・衛生面の不安を示す投稿

次に、防災コンパス上で整理された以下の情報を提示。

避難所A：交通規制のため、物資・避難者ともに到達できず。
避難所B：スタッフ追加による受入状況の改善報告
避難所C：断水継続中、衛生対応に一部制約



SNSの情報を参考にどの避難所に避難しますか？



最初に受け入れたデメリット

受け入れ拒否	57.1%
設備故障	14.3%
食糧不足	28.6%

避難先変更・変更なしの根拠

受け入れ改善	50.0%
交通規制(断念)	35.7%
距離が近い(遠い)	14.3%

(全員が判断の変更・維持を即答)

結果

すべての被験者において、相反する内容が混在する不確かな情報を頼りとして最初に選択した避難所から、防災コンパスによって整理された情報を得ることで、避難先の変更や現状維持を選択した根拠を、より短時間で明確に回答できた。

3-2. 技術開発の個別詳細

ファクト注釈コード（Fact Annotation Code：FAコード）ー知覚情報抽出アルゴリズムの改善ー

ファクト注釈コード（Fact Annotation Code：FAコード）

偽・誤情報と判定された画像に対し、視認性の高い装飾を付与して「注釈（アノテーション）が世に存在している」ことを周知できるコードを開発。

画像の知覚的特徴をコード化するため、画像が知覚的意味を持つ限り、**切り離すことができない**という特性があり、QRコードのようにすり替えや切り離しが不可能であり、また電子透かしのように劣化コピーによって埋め込まれた情報の欠落が起こりえないのが強みとなる。

また前年から引き続き、この技術の元となる知覚ハッシュ技術に改良を加えることで、真陽性率を維持したまま、偽検知率を大幅に低減することができた。

画像の知覚的特徴をそのままコード化

abc2b7b5-6bc2b395-153b
20文字(80bit)

ブロックチェーン上に登録されたデータとリンク

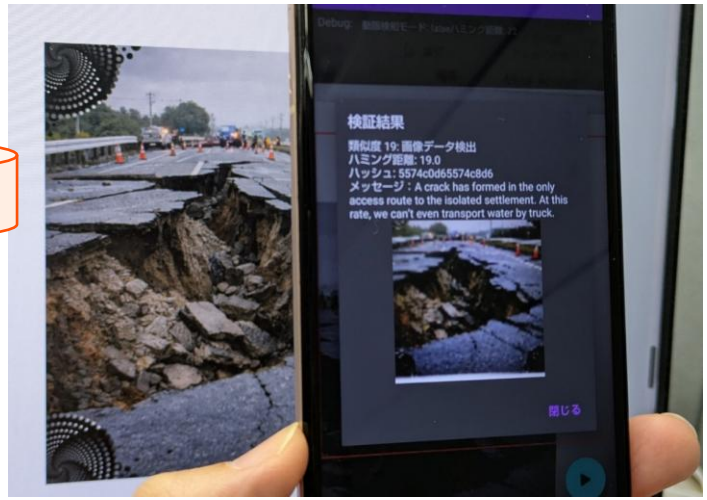
{著作情報}
{来歴情報}

さまざまなデータとコンテンツとの橋渡しに。

検証機

物から意味を切り離すことのできない、**コンテンツ起点**の来歴証明を実現（偽・誤情報起点の注釈管理として本筋で活用可能）

検証機（スマートフォン）で画像をスキャンすることで、注釈情報への参照が可能。



3-2. 技術開発の個別詳細

ファクト注釈コードの開発

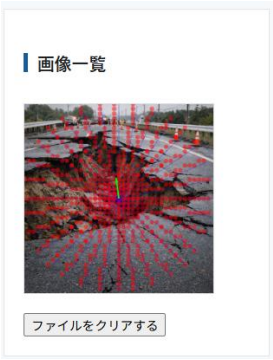
登録内容

情報区分　訓練、偽・誤情報、12時間有効
3日間有効、2週間有効　より選択
（災害時は状況が刻々と変わるため有効期間を設定）

登録方法　情報提供、公式情報、緊急速報、より選択
（ブロックチェーンに記録する方法が異なる）

詳細内容　言説内容の登録
（登録内容は暗号化して記録）

画像の登録



　指定画像を放射状にサンプリングした輝度情報からハッシュ値を作成することで、拡大や縮小しても似た値を出力するハッシュ値を得ることができる。

　また、位置ずれや偶然一致してしまうハッシュパターンに対して異なる対策を取る。

動画の登録　シーンの切り替わりでサムネイルを切り出し画像リストを作成

3-2. 技術開発の個別詳細

ファクト注釈コードの開発

ファクト注釈コード（FAコード）は、80bitで構成される。同コードは、ベースとなる32bitの知覚ハッシュに加え、撮影条件や取得環境の差異によって生じる揺らぎを吸収する位置ずれ補正項（32bit）、および誤検知を抑制するための補助識別ベクトル（16bit）から構成されている。災害時などインターネットを通じて画像を共有・転送できないような環境においても、カメラスキャンを通じて同一性を判定できることを目的としている。

FAコード　abc2b7b5 - 6bc2b395 - 153b
知覚ハッシュ　位置ずれ補正項　補助識別ベクトル

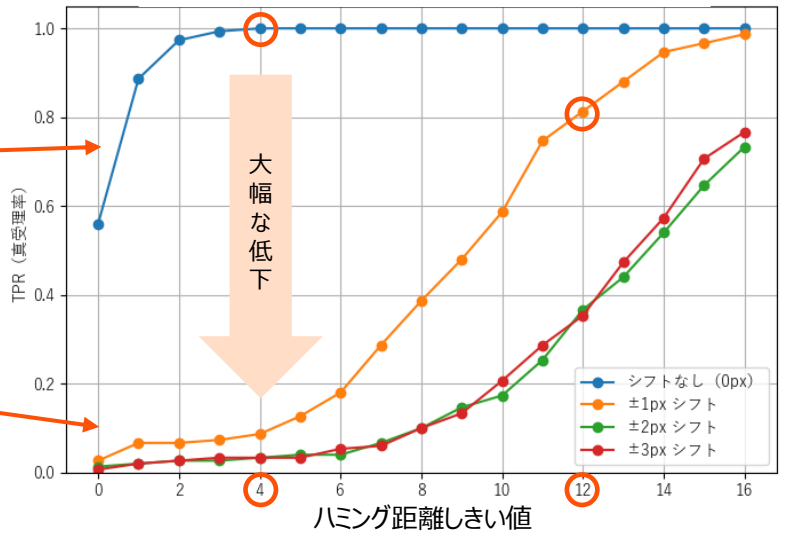
従来の画像認識手法では、数KBから場合によっては1MB程度のデータを用いることが一般的であるが、IPDCにおいては本放送に影響を与えないデータサイズでの利用が重要となるため、小サイズでの同一性判定を可能とするFAコードを開発した。知覚ハッシュは人間が内容を同一と認識する範囲の変化については、ハッシュ値が大きく変化しない設計となっているため、その差を取る（**ハミング距離**）ことで画像の類似度を測ることができる。

従来の知覚ハッシュは、データを転送してファイル単位で比較すれば、ほぼ確実に同一性の検知が可能である。一方で災害時などでは紙資料あるいはトリミングで切りぬかれた画像と比較するケースが想定され、1pxでも位置ずれが発生すると正解検知率（TPR：True Positive Rate）が大幅に低下する（下図グラフ参照）。そのため、次頁以降で解説する位置ずれ補正項と補助識別ベクトルを導入することで検知精度の向上を図る。

ファイル単位で比較が可能な場合の正解検知率（青線）。
ハミング距離のしきい値を4と設定すると100%に近い精度を示す。

1pxずらして比較した場合の正解検知率（オレンジ線）。
ハミング距離のしきい値を12と設定しても正解検知率は80%。
さらにハミング距離のしきい値を大きくすると、関係の無い画像も正解として誤検知してしまう。

撮影時の位置ずれと検知精度の低下の関係



3-2. 技術開発の個別詳細

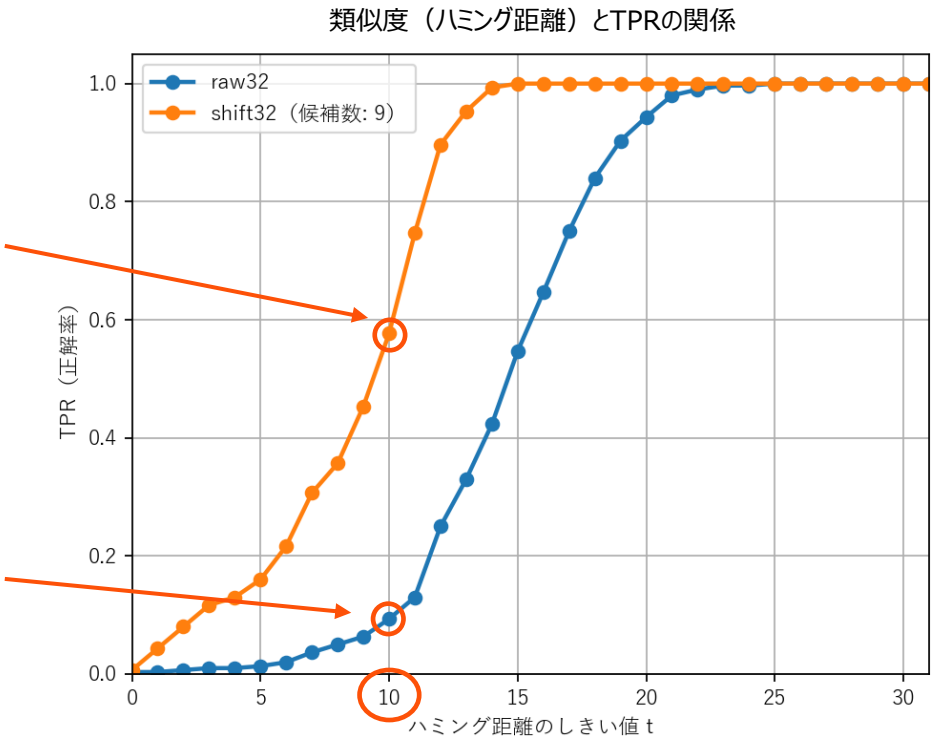
ファクト注釈コードの開発　ー位置ずれ補正項の役割ー

位置ずれ補正項　：　abc2b7b5 - **6bc2b395** - 153b

本実証では位置ずれ補正項の開発を行った。あらかじめ、位置ずれに対して変化量の少ない特徴を補正項として先に計算しておくことで、知覚ハッシュの特性であった撮影時のわずかな位置ずれによって、類似度が大きく低下してしまう問題を緩和する。下図は正解画像と、4ピクセルずらした画像について、類似度（ハミング距離）と正解検知率（TPR）の関係を示すグラフである。例えば、ハミング距離を10以下で正解と検知した場合、正解検知率が約10%から約60%に向上していることが確認できる。

位置ずれ補正項を含めて正解検知率を測定した場合

従来の知覚ハッシュで正解検知率を測定した場合



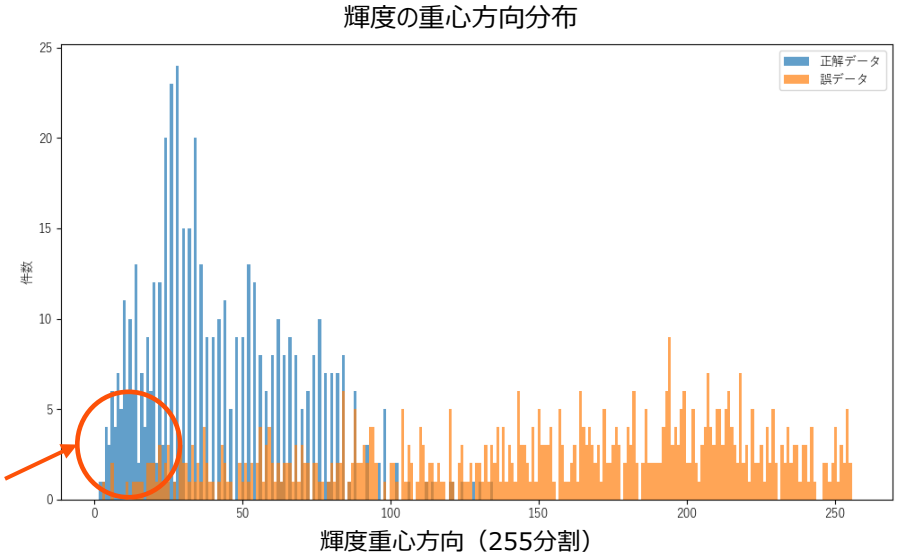
3-2. 技術開発の個別詳細

ファクト注釈コードの開発　ー補助識別ベクトルの役割と実機での効果実証ー

補助識別ベクトル　：　abc2b7b5 - 6bc2b395 - **153b**

補助識別ベクトルは、輝度の重心情報を付与することで識別精度の向上を図る（下図可視化イメージ参照）。右図グラフは輝度重心方向別に検知件数を示したグラフで、正解データを検知した時の分布と誤データを検知した分布が明確に異なっており、特定の方向に正解データが集中する傾向が確認できる。このことから、本手法は、明らかに輝度の重心方向が異なる候補を事前に除外するためのスクリーニング用途として有効であると考えられる。本実証での評価では、しきい値を42（輝度重心方向のずれ30度まで許容）とした場合に、誤データの83%を除去することができた。

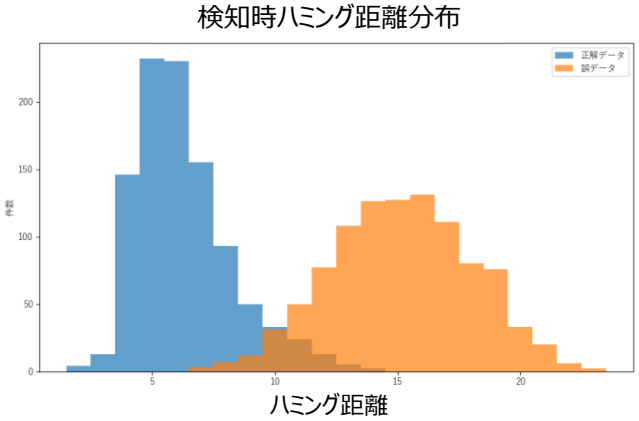
正解データは特定のベクトルに強く偏る



実機での効果実証

1000件の正解データを連続スキャンした結果、判定用データとのハミング距離は平均6.3。一方、1000件の誤データを連続スキャンした場合は、ハミング距離は平均15.2であった。両者の平均差は8.9であり、分布上は8～10付近に明確な谷が形成されるため、分類可能であることが分かる（下図左参照）。

また、KPIとして設定していた登録データ数50件の状態で検知評価を行った。800セッションを通して誤検知は観測されなかったことから、誤検知率は0.38%以下であると評価できる（KPI達成を確認）。



3-2. 技術開発の個別詳細

テキスト情報を活用した検知精度の向上 ーメタデータとして活用ー

本開発では、さらに検知精度を向上させるための方策として、画像・動画に関する**言説**を偽・誤情報の構成要素として解析対象に含める検証を行った。具体的には、言説を画像・動画のメタデータとして暗号化したものをIPDCで放送することで、補助要素として活用可能となる。たとえば豪雨災害時に拡散される画像では単一色調の水面が広く映り込み、視覚的特徴が乏しいために知覚ハッシュ技術だけでは誤検知のリスクが高まるが、テキスト文脈を加味することで、無関係の画像を効果的にスクリーニングすることによって効率的な偽・誤情報の検出が可能となる。

登録内容
偽・誤情報と判定された画像

偽・誤判定情報として配信

FAコード
暗号化したテキスト情報

検証側
アプリでスキャンした画像

機械学習
ラベリング

Asphalt,Soil,
Rock,Road
…

This image refers to **Asphalt** and **Soil**…
（これはアスファルトや土…に関しての画像です）

画像に対する言説例

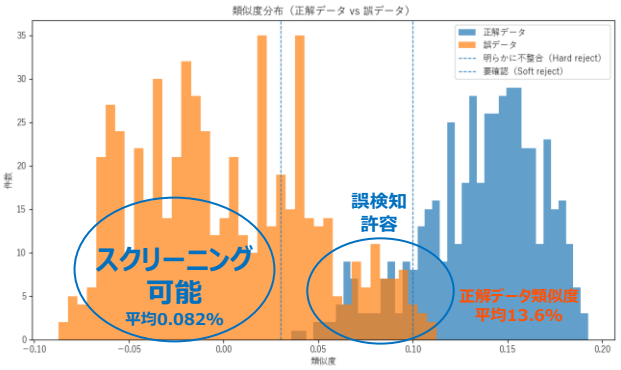
“孤立集落へ向かう唯一の道路に亀裂。これじゃトラックで水も運べない。”

A crack has formed in the only access route to the isolated settlement. At this rate, we can’t even transport water by truck.
（ラベリングに登録されていない単語で文章を作成）

インターネット環境を使わずに
被災地で直接類似検証

類似度判定
辞書サイズ17MB

偽・誤情報の検知精度向上



本実証段階ではオフラインで日本語辞書を使用する場合のデータサイズが大きくなってしまうため、登録時に英語に翻訳しての実施。実証はラベル登録されていない単語で言説データを作成

精度の高い分類には課題があるが、誤検知除去などのスクリーニング効果があることを確認

3-2. 技術開発の個別詳細

前年度からの改善（その他）ー知覚情報抽出アルゴリズムの改善ー

複数組織、複数アプリの登録対応

防災コンパスやFAコードなど、異なる機能に使用されるデータを単一の送信機器で処理可能なロジックへの修正。
これにより、地域によって限られた放送設備のリソースを複数のシステム稼働に有効活用できることを確認した。

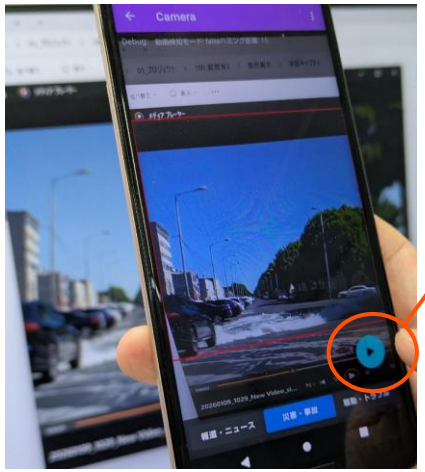
検証データの圧縮

検証に必要なデータであるブロックヘッダーをテキストデータからバイナリデータに変換することで、データサイズを70%圧縮。

動画の効率的な登録と検知

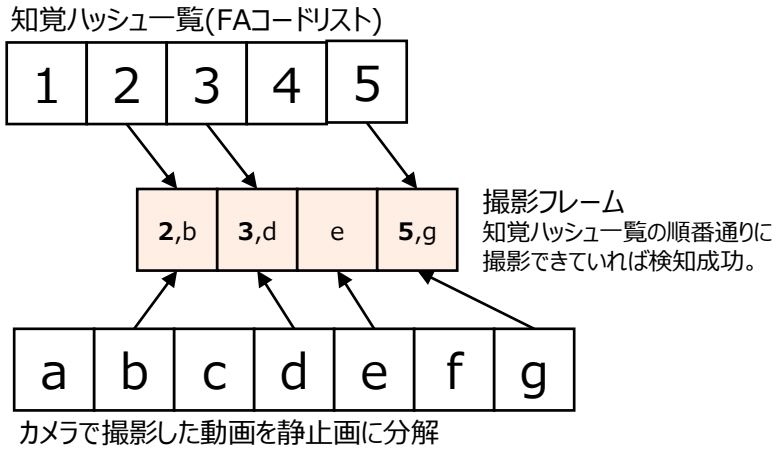
偽・誤情報の拡散に大きな影響を与える冒頭8秒間の部分のみ対象とすることで、データ登録と検出効率を改善するために、「動画検知モード」ボタンを準備し、ユーザーが意図したタイミングで動画検知を開始する方式に修正。動画の検知方式は動画を静止画に分解し、一定時間の間に複数回知覚ハッシュが一致することを条件とする方式を採用。

動画フォーカスボタン



ロングタップ中
動画検知モードとして動作

一定時間の間に複数回の知覚ハッシュ一致による動画検知



目次

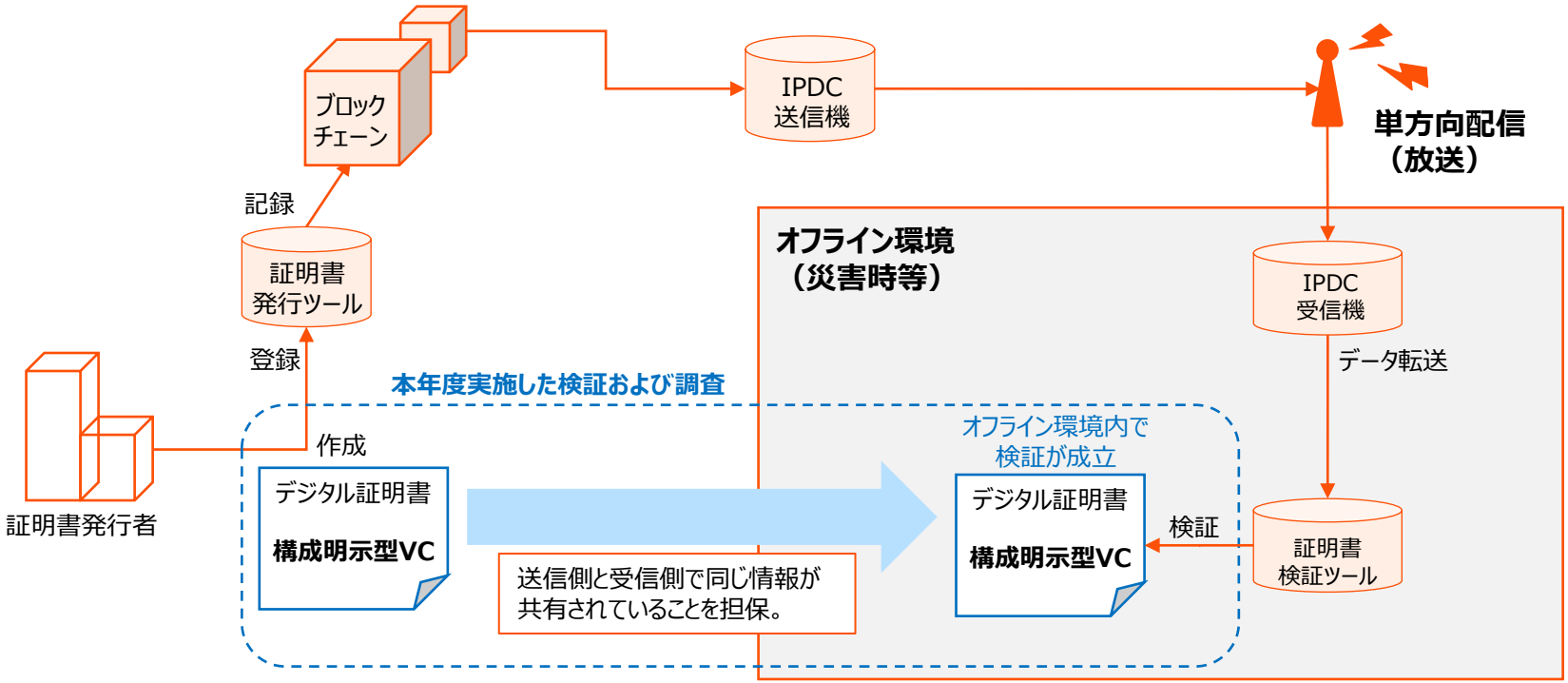
1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

4-1. 検証及び調査の全体像

検証及び調査に係る取組・成果の全体像

前章では、本実証で開発した各サブシステムの具体的な実装例となるアプリケーションの内容を整理するとともに、個別の評価・検証を行った。これらのアプリケーションは、災害時などの通信が利用できない環境（以下、オフライン環境）においても、受信した情報が信頼できることを前提として設計されており、その信頼性検証手段が十分でない場合はアプリケーションの有効性が担保されなくなる。そのため、従来のような通信を前提としたセキュリティでは、オフライン環境における信頼性を担保することができず、通信に依存しない信頼性検証手段の確立が重要となる。

本章では、本実証で採用したオフライン環境での信頼性検証手段に対して実施したセキュリティ評価について整理する。情報の信頼性を確保するため、オフライン環境へ配信する情報はすべて電子署名が付与された**デジタル証明書**として扱う。一方、一般的なデジタル証明書は検証過程において通信を前提とする場合があり、オフライン環境での利用には制約がある。これに対して、本実証では関西テレビソフトウェアが設計した**構成明示型VC**（Verifiable Credentials：検証可能な証明書）を採用することで、オフライン環境における証明書検証を実現している。



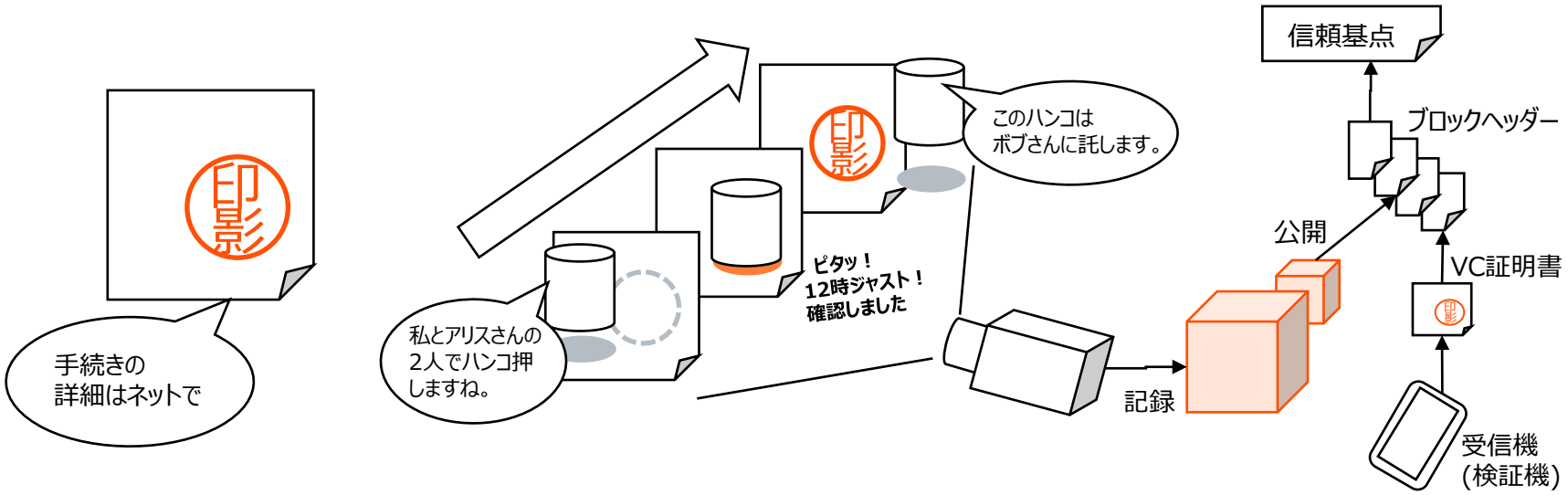
4-2. 検証及び調査の個別詳細

単方向配信データ検証 ー構成明示型VCー

まず、構成明示型VCによりオフライン環境での検証が成立する構造を整理する。続いて、本実証において実施した比較評価および脅威分析について示す。

従来のデジタル証明書（図A）では、データに付与された電子署名が正しいかどうかを確認するために、インターネットを通じて認証局（第三者機関）に問い合わせる仕組みが一般的である。そのため、放送のように一方向で配信される環境では、同じ方法をそのまま使うことが難しい。これに対して、**構成明示型VCを用いた検証方式**では、署名がどのような形で記録され、どの情報と結び付いているかを、あらかじめ検証可能な構造として示す。具体的には、署名付きデータをブロックチェーン上に記録し、そのデータがブロックチェーン上に含まれていることを確認することで、信頼性を判断する。

この方式には主に二つの特徴がある。一つ目は、ブロックチェーンが公開しているブロックヘッダー等の情報を使うことで、インターネットに接続しなくても、**受信側の端末だけで検証ができる**点である（図C）。二つ目は、ブロックチェーン上に記録されたデータの構成を読み取ることで「**どのような条件で署名されたか**」まで確認できる点である(図B)。例えば、組織を代表する署名の構成を定義しておけば（次ページ図D）、その構成に基づいてブロックチェーン上に明示的に残る。これにより、組織内部の担当者が入れ替わった場合でも、受信側は「誰が署名したか」を逐一把握する必要がなく、「同じ組織から発信された情報であるか」を変わらず確認できる。



図A：従来のデジタル証明書

図B：どのような条件で署名したかをブロックチェーンに記録

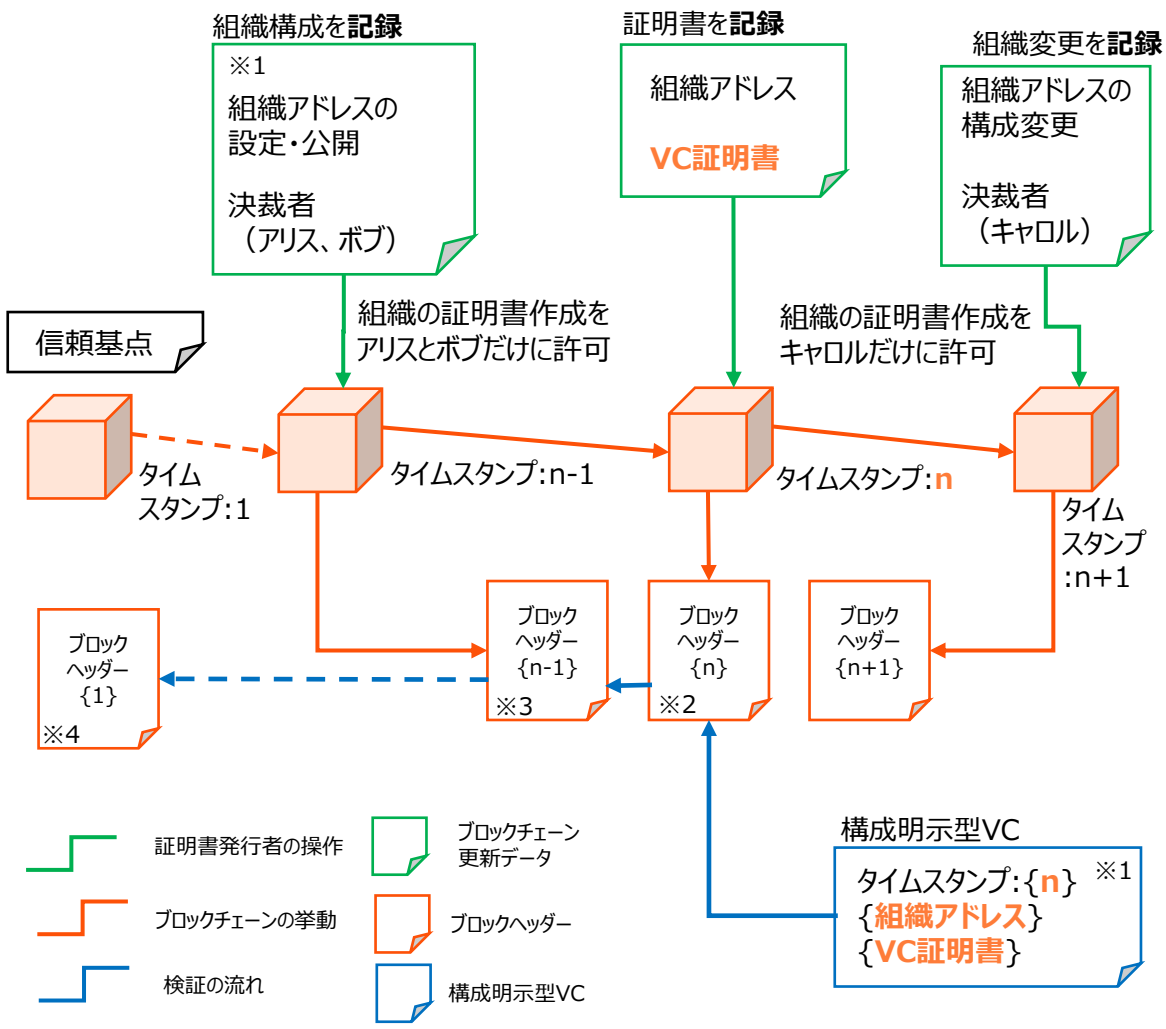
図C：受信機側だけで検証が可能

構成明示型VC

4-2. 検証及び調査の個別詳細

単方向配信データ検証 ー構成明示型VC（手続きの正当性）ー

構成明示型VCによる手続きの正当性検証(図D)



ブロックチェーン上の証明書の考え方

組織はあらかじめ自らのアドレスを公開する。そのアドレスに対応する秘密鍵を用いて、証明書をブロックチェーン上に記録する。

ブロックチェーンは、一度記録されたデータの改ざんが困難であるという性質を持つため、当該アドレスと組織との対応関係を示す鍵が適切に管理されている限り、ブロックチェーン上に記録された文書やハッシュ値は「その組織が発行した証明書」とみなすことができる。

VC証明書の検証

VC証明書（※1）が存在しなければ、ブロックヘッダー{n}（※2）が作れないことを確認。次にブロック{n-1}（※3）が存在しなければブロック{n}を作れないことを確認。以後、{n-1}→{1}まで繰り返す。{1}（※4）にたどり着ければ、検証者自らが存在を認知しているので、ブロックチェーン上にVC証明書の存在が保証されていることを確認できる。

構成明示型VCにより保証されること

通常のVCでは、ブロックチェーンは証明書の存在を保証する役割のみを担い、保証されるのはデータの存在と改ざん困難性である。

これに対し、構成明示型VCでは、証明書本体や署名構成をあらかじめ定義されたフォーマットに従って記述することにより、ブロックチェーンへのデータ登録時の条件をそのまま検証できる。つまり、単なるデータ格納ではなく「署名構成が定義どおりであるか」までを検証できる。

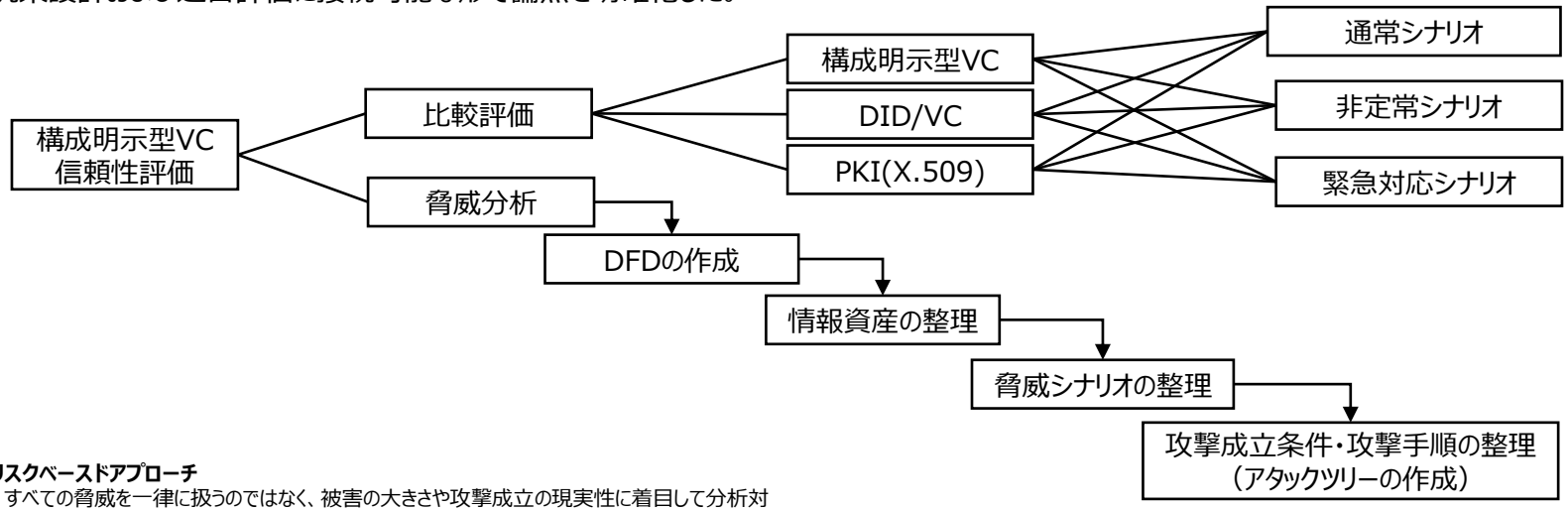
4-2. 検証及び調査の個別詳細

単方向配信データ検証手法の信頼性評価

比較評価と脅威分析

本実証では構成明示型VCを活用した検証手法を第三者検証企業であるベリサーブ社に評価を実施いただいた。
評価においては、実運用を想定した運用シナリオの下で、構成明示型VC方式、DID/VC方式、PKI（X.509）方式の**比較評価**を行い、各方式の技術的特性ならびに運用上の利点・制約を整理した。

さらに、リスクベースドアプローチに基づく**脅威分析**として、情報資産の特定、脅威シナリオの整理、攻撃成立条件の洗い出しを実施し、今後の対抗策設計および適合評価に接続可能な形で論点を明確化した。



リスクベースドアプローチ
すべての脅威を一律に扱うのではなく、被害の大きさや攻撃成立の現実性に着目して分析対象を整理する考え方。初期段階で情報資産の特定や脅威シナリオの切り分けといった分析工数は増えるが、重要度の高い論点を事前に明確化できるため、後続の対抗策設計や適合評価を過不足なく行うことが可能となる。

DFD（Data Flow Diagram）
データの流れ、処理、外部主体、保存先を整理して可視化する図であり、情報の通過点や境界を明確にすることで、脅威が発生し得る箇所の洗い出しに用いられる。

アタックツリー
攻撃者の目的を起点として、成立し得る攻撃経路や前提条件を木構造で分解・整理する手法。脅威シナリオの抜け漏れを防ぎ、現実的に成立する攻撃とそうでないものを切り分けるために用いられる。

DID/VC
W3Cで標準化された分散型識別子（DID）と検証可能な証明書（VC）に基づき、発信者や主体に関する主張を暗号的に検証可能な形で表現する仕組み。なりすましや情報改ざんに対する検証手段として、主に信頼性確保が求められる情報を対象に適用される。

PKI(X.509)
認証局が発行する証明書を用いて主体の公開鍵と身元を結び付け、通信相手や発信者の正当性を検証するための従来型の信頼基盤

4-2. 検証及び調査の個別詳細

単方向配信データ検証手法の信頼性評価

比較分析

通常シナリオ
証明書（VC）の発行から、保有者による提示、検証者による検証までの一連の流れを想定したシナリオ

No.	観点	構成明示型 VC	DID/VC	PKI(X.509)
1	検証の根拠	ブロックチェーンの記録	発行者 DID と DID ドキュメント（公開鍵）	CA 証明書
2	事前の情報連携	不要	発行者 DID と DID ドキュメント（公開鍵）	CA 証明書
3	証明書取り消し	取り消し記録を検証環境に蓄積	取り消し記録を検証環境に蓄積	証明書単位の取り消しを行うと仕様複雑化
4	オフライン検証	永続的に可能	永続的に可能だが、発行者の追加・変更に制限	永続的に可能だが、発行者の追加・変更に制限

非定常シナリオ
鍵更新や承認者の交代など、あらかじめ想定される運用上の変更が発生した場合を想定したシナリオ

No.	観点	構成明示型 VC	DID/VC	PKI(X.509)
1	鍵更新の波及範囲	発行環境	発行環境	発行環境および検証環境
2	鍵変更に影響されない制度接続用情報の設定	可能(チェーン ID+ 証明書承認 TX アカウント)	可能(発行者 DID)	不可
3	ブロックチェーンハードフォークの影響	ハードフォークの内容に応じて確認要	ハードフォークの内容に応じて確認要	影響対象外

緊急対応シナリオ
秘密鍵の漏えいや紛失、承認者の不在、証明書（VC）の紛失など、突発的な事象が発生した場合を想定したシナリオ

No.	観点	構成明示型 VC	DID/VC	PKI(X.509)
1	鍵漏えい（悪用）	単一の漏えい鍵による証明書偽造は不可	単一の漏えい鍵による証明書偽造は不可	無効化前に偽造された証明書を見破れない
2	鍵漏えい（無効化）	漏えい鍵の無効化のみで対応完了	漏えい鍵無効化のために署名者全員の鍵を更新要	漏えい鍵の速やかな無効化、検証者への注意喚起が必要
3	証明書紛失	紛失分を無効化し、再発行可能	紛失分を無効化し、再発行可能	再発行可能だが、故意に複数証明書を得ることを防げない

ブロックチェーンを活用した場合に新たに考慮しないといけない検討事項

通常シナリオ時において、証明書の取り消しを行う場合は、新たに取り消し記録を配信し、検証環境に最新情報として蓄積保存する必要がある。

また、**非定常シナリオ**においては、ブロックチェーン自体の挙動に変更が入る場合（ハードフォーク）、その内容に応じて影響がないかを確認する必要がある。

ブロックチェーンを活用した場合にその特徴が生かされるオフラインでの検証や緊急対応に強み

通常シナリオ時において、発行者の追加や変更に制限を受けずに永続的にオフライン検証が可能である。

また、**緊急対応シナリオ**において、鍵が漏洩した場合は対象となる鍵のみを無効化するだけで対応が完了となる。

4-2. 検証及び調査の個別詳細

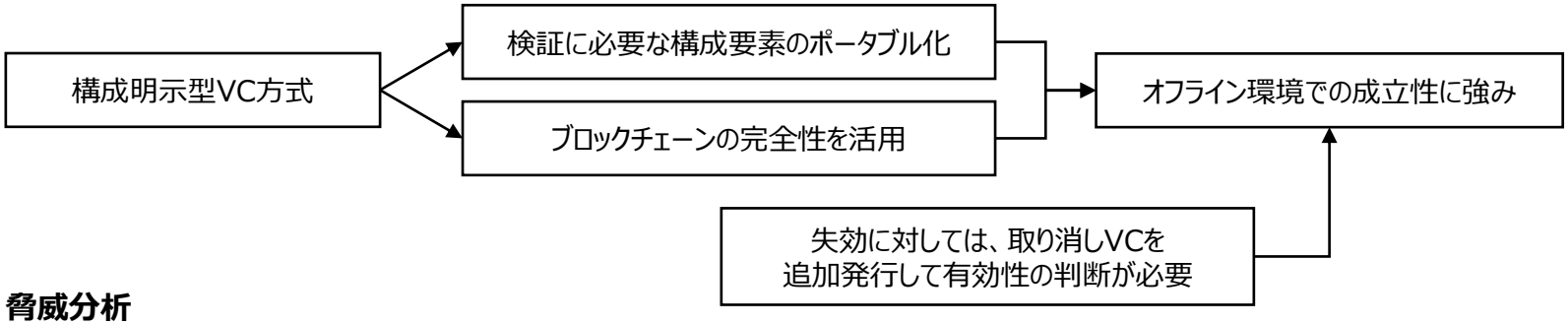
構成明示型VCの信頼性

総合評価

比較評価

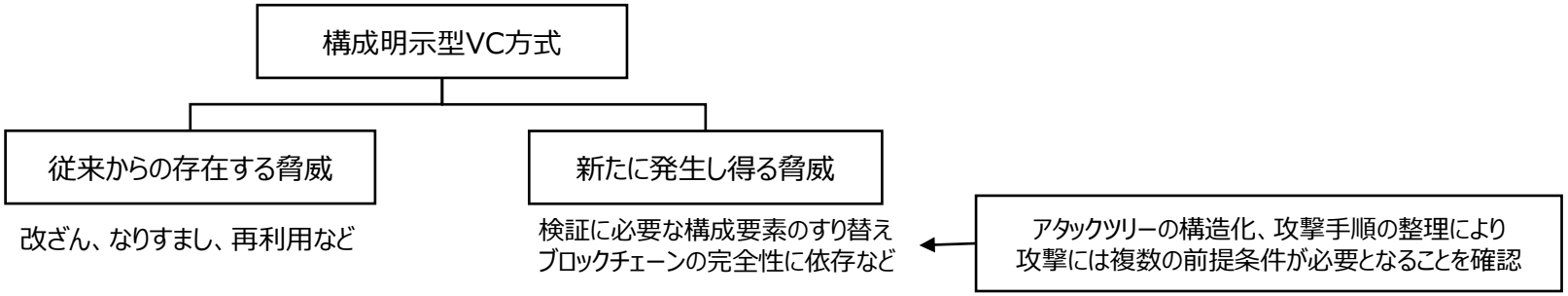
構成明示型VCを用いた検証方式は、発行行為そのものをブロックチェーン上の記録として保持し、発行時点単位で検証を行う構造を有している点に特徴がある。この構造により、時間の経過や運用変更、突発的な事象が発生した場合であっても、影響範囲を整理しながら検証を継続できる可能性が示された。

特に、災害時などの通信環境の制約や運用体制の変化が同時に発生し得る状況下においては、オフライン環境でも検証を継続できることに加え、影響をどの範囲まで切り分けられるかという点が重要となる。本評価の範囲においては、構成明示型VCを用いた検証方式は、このような観点において相対的に親和性が高い特性を有していることが示された。



脅威分析

アタックツリーの構造化、攻撃手順の整理の過程で、改ざん、なりすまし、再利用といった従来から存在する脅威に加え、検証に必要な構成要素のすり替えや、ブロックチェーンの完全性に依存する点など、構成明示型VC方式に固有の観点を含む脅威が確認された。しかしながら、当該検証基盤における重大な悪影響は、技術的な脆弱性のみならず、運用や利用の前提条件が複合的に崩れた場合にのみ成立し得るという性質を有することが示された。



目次

1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

5-1. 社会実装に向けた取組の全体像

社会実装に係る取組・成果の全体像

本開発・実証期間において、放送とブロックチェーンを組み合わせた対策技術を実際の運用環境へ展開することを見据え、社会実装に向けた取組を段階的に実施した。

まず、**放送局内設備検証**として、実際の放送局内設備を使用し、本放送に影響を与えない形でデータを重畳する検証を行った。これにより、実運用中の放送システムへの影響や調整事項を整理した。これにより次フェーズとなる実電波を活用したフィールド実証への道筋をつけることができた。なお、本実証では送出設備から局内設置の検証用送信機器を経由して有線で受信機に接続することで、電波を用いず局内で完結する構成により検証を行った（以下、本報告書内に「放送」と記載されている箇所はこの検証構成を意図するものとする）。

次に、**IPDC受信機の普及を見据えた環境整備**として、受信機から検証システムまでのデータ接続の開発を行った。放送から受信したデータをスマートフォンなどの端末へリアルタイムに転送する方式や、安定した検証機能を維持するために必要な実装構成の整理を進めた。これにより、実運用に耐えうる受信機に必要な要件を整えることができた。

また、ブロックチェーン活用に伴う**運用コストを抑制するための環境整備**として、暗号資産を利用者が直接保有しない運用スキームについて検討・開発を行った。暗号資産手数料を代替的に処理する仕組みを導入することで、自治体や防災組織が暗号資産管理を意識することなく本技術を利用できる構成とし、導入・運用のハードルを低減できることを確認した。

これらの取組を通じて、本事業で開発した対策技術が、放送現場および防災分野の実運用環境において適用可能であることを、設備面・運用面・コスト面の観点から確認した。本成果は、今後のフィールド実証や本格的な社会実装に向けた重要な基盤として位置づけられる。

放送局内設備検証	IPDC受信機普及に向けた環境整備	運用コスト軽減に向けた環境整備
実運用中の放送システムへの影響や調整事項を整理	実運用に耐えうる受信機に必要な要件の整理	自治体や防災組織が暗号資産管理を意識することなく本技術を利用できる構成の確認

5-1. 社会実装に向けた取組の全体像

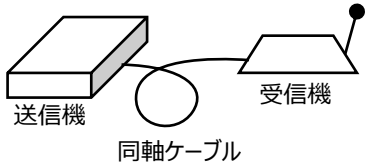
社会実装に係る取組・成果の全体像

放送設備検証

実電波での活用を見据えて、実際の放送設備に必要な設定内容や、放送設備及びテレビ受像機に与える影響を整理。

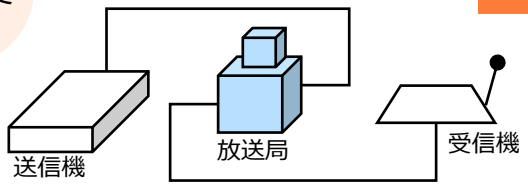
前年度

送信機と受信機を
有線で直接接続



今年度

送信機から局内放送設備を
経由して受信機へ有線接続



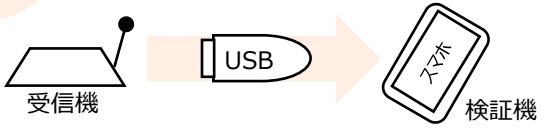
→ 実電波活用の
フィールド実証へ

IPDC受信機普及に向けた環境整備

カメラやセンサーなどの機能を持つ検証端末に受信データをシームレスに届ける仕様整理と開発。

前年度

受信機から検証端末へ
USBメモリで手動でコピー



今年度

IPDC受信機からIoT機器を
経由して検証機と無線で同期

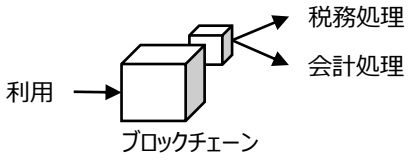
→ 量産を見据えた
受信機開発へ

運用コスト軽減に向けた環境整備

単方向配信データの信頼性確保に必要なブロックチェーン利用に伴う負担を軽減。

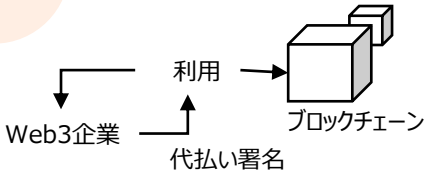
前年度

ブロックチェーンを利用するために
利用者負担が大きい



今年度

Web3企業を経由することで暗号
資産を所有しない利用環境の実現



→ ブロックチェーンを
災害に強いデータ
ベースとして活用

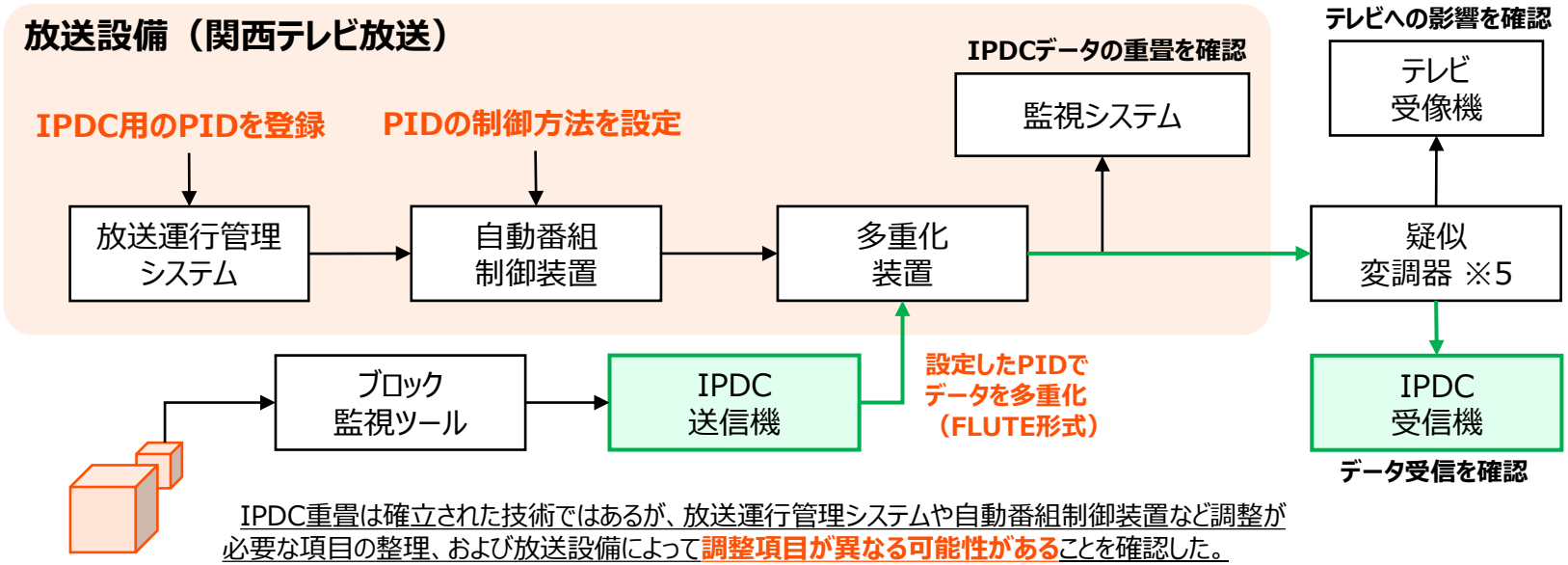
5-2. 社会実装に向けた取組の個別詳細

放送設備検証

放送設備への技術的適合

本実証では送出設備から局内設置の検証用送信機器を経由して有線で受信機に接続することで、電波を用いず局内で完結する構成により検証を実施。

IPDC送信機を**多重化装置**（※1）へ接続することで、放送のデータストリームに重畳できることを確認した。
放送設備の多重化装置を使用した重畳には**PID**（※2）の定義、**放送運行管理システム**（※3）への登録、**自動番組制御装置**（※4）でPIDごとの制御方法を設定することで多重化装置を適切に制御する必要がある。



IPDC重畳は確立された技術ではあるが、放送運行管理システムや自動番組制御装置など調整が必要な項目の整理、および放送設備によって**調整項目が異なる可能性がある**ことを確認した。

※1 多重化装置
放送設備において、番組映像・音声・字幕・データ放送など複数の信号を単一の伝送ストリームへ統合する装置。帯域制御やストリーム整形を担う。

※2 PID(Packet Identifier)
MPEG-TS方式のデジタル放送において、映像・音声・データなどを区別するための識別番号。受信機は設定されたPIDに基づき、対象のストリームのみを抽出して復号・処理する。

※3 放送運行管理システム
「番組編成」や「放送送出」などの業務を統合的に管理する基幹システム。

※4 自動番組制御装置
放送局において、放送をスケジュールに従って送信所に送り出す、あるいはその番組素材などをあらかじめ決めたスケジュールに従って送受するため、各種装置を制御する制御システム。

※5 疑似変調機
放送送出系から出力される伝送ストリームを、放送規格に準じた変調信号へ変換し、試験用に出力する装置。放送局内環境で受信確認や機器影響評価を行うために使用する。

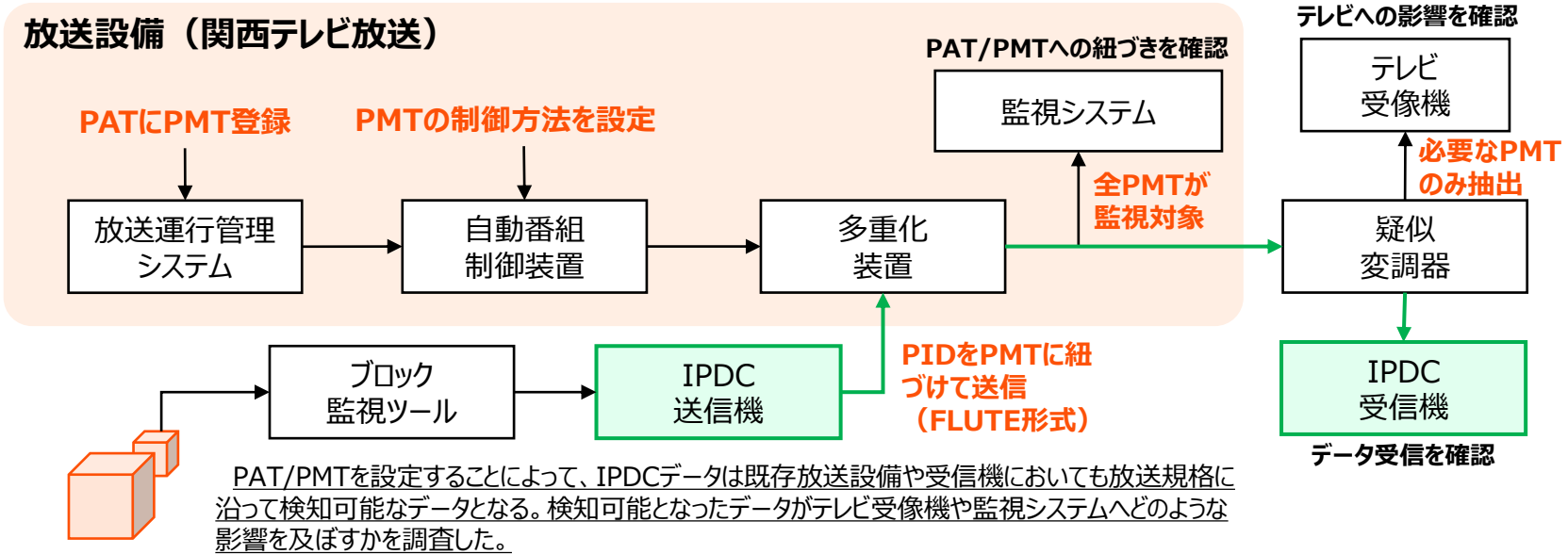
5-2. 社会実装に向けた取組の個別詳細

放送設備検証

放送規格への準拠

本実証では送出設備から局内設置の検証用送信機器を経由して有線で受信機に接続することで、電波を用いず局内で完結する構成により検証を実施。

既存放送機器に影響を与えないためにも、現在のARIB（一般社団法人電波産業会）によって整備された放送規格に準拠してIPDCを送出することが必要である。特に注意すべき点は、重畳するデータのPAT/PMTへの登録である。



PAT/PMTを設定することによって、IPDCデータは既存放送設備や受信機においても放送規格に沿って検知可能なデータとなる。検知可能となったデータがテレビ受像機や監視システムへどのような影響を及ぼすかを調査した。

PAT/PMTをたどって必要なPIDを検知する流れ
テレビ受像機・監視システム
（IPDCのPIDを5001とした場合）

PAT(PID = 0)	
番組1	PMT (PID = 1000)
番組2	PMT (PID = 2000)
番組3	PMT (PID = 3000)
番組4	PMT (PID = 4000)
番組5	**PMT (PID = 5000)**

PMT(PID = 1000)	
素材1	(PID = 1001)
素材2	(PID = 1002)
素材3	(PID = 1003)

PMT(PID = 5000)	
IPDC	(PID = 5001)

PAT (プログラム・アソシエーション・テーブル：Program Association Table)
伝送ストリーム内の番組一覧と、それぞれのPMTが格納されているPIDを示す管理テーブル。受信機はこの情報を基に番組構成を認識する。

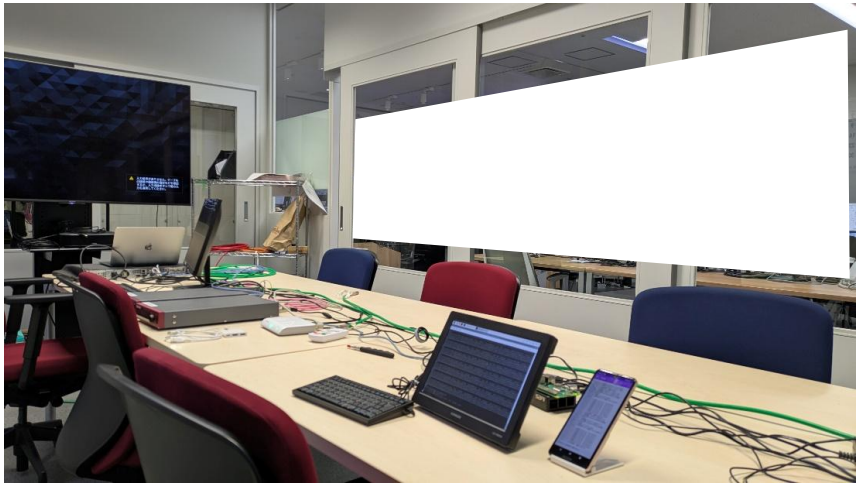
PMT (プログラム・マップ・テーブル：Program Map Table)
特定番組に属する映像・音声・データストリームのPIDを定義するテーブル。IPDCデータを送出する場合は、該当データのPIDをPMTに登録する必要がある。

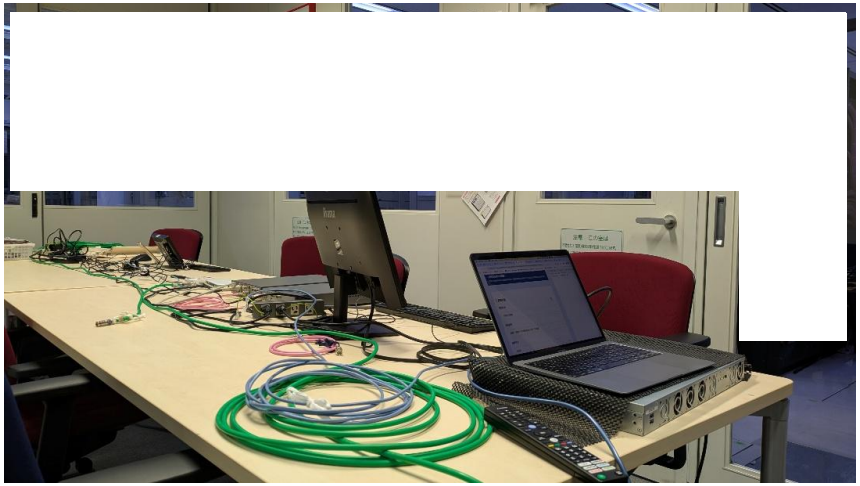
5-2. 社会実装に向けた取組の個別詳細

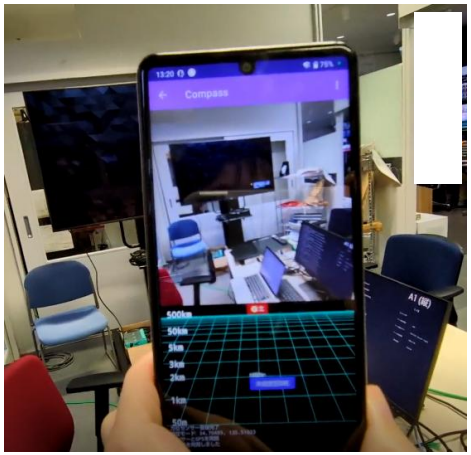
放送設備検証

実証実験の様子

関西テレビ放送マスタ設備に隣接した会議室にて、実証実験を実施。







受信機から取り出したデータで
アプリケーションを制御

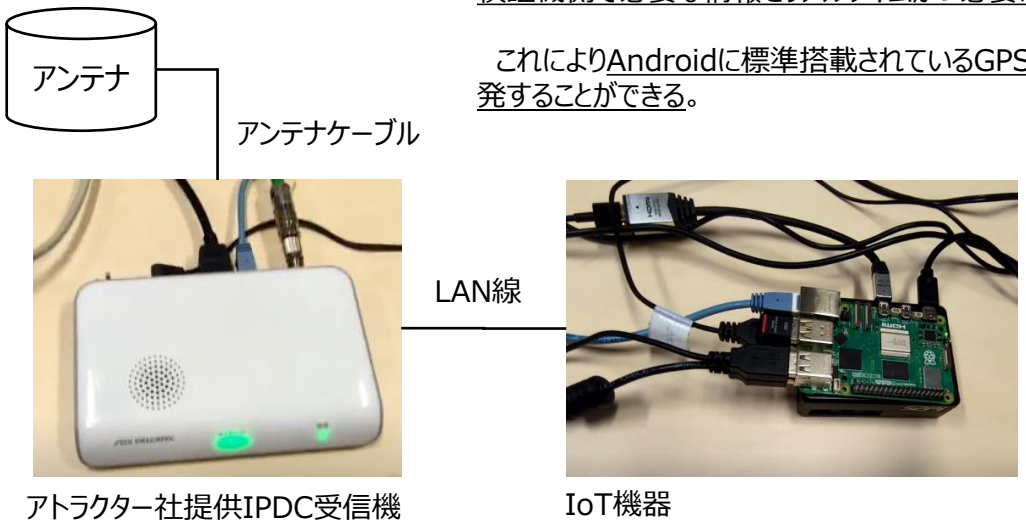
関西テレビ放送は本番系マスター（1/2系）とまったく同仕様の検証系マスター（3系）を持っている為、検証系での実験が本番系での挙動であるとみなせる。

また、本実証は、他の地上デジタル放送実施局への適用を想定し、地上デジタル放送の共通規定に基づいて構成されている。そのため、一定の技術的検討や調整を要するものの、放送局ごとの設備構成や運用差異を考慮した上での導入検討が可能な内容となっている。

5-2. 社会実装に向けた取組の個別詳細

IPDC受信機普及に向けた環境整備

IPDC受信機構成



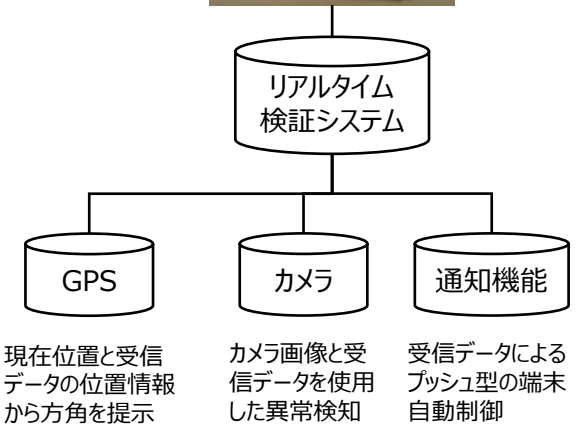
本実証では受信データをIoT機器に蓄積し、Androidスマートフォンとのローカル無線接続により、検証機側で必要な情報をリアルタイムかつ必要に応じてデータを取得できる構成にした。

これによりAndroidに標準搭載されているGPSやカメラなどを活用したアプリケーションを容易に開発することができる。

ユーザー体験を大幅に向上するリアルタイム検証の実現

IPDC受信機からAndroid検証機へのデータ転送時にIoT機器を中継させてデータの蓄積や無線配信機能を充実させることで、受信機の性能に依存しないリアルタイム検証を実現した。具体的には、IoT機器とAndroid検証機間の無線通信、送信機側からの配信間隔制御を実装（次頁参照）。また、検証結果キャッシュ機構の実装（次々頁参照）により、配信速度を大幅に向上させることができた。

上記機能を実装することにより、速報データが平均18秒で配信可能になり、今年度のKPI達成を確認（ネットワークの最適化により、最小7秒まで縮小可能であるが、受信機の負荷も増大するため、最適化の調整が必要）。また、ブロックチェーンへの登録を確実に行う場合は48秒での配信となるが、今後IoT機器機能を搭載した一体型受信機を開発することで、IPDC受信機とIoT機器間の通信ラグが解消され、さらなる速度向上が見込める。

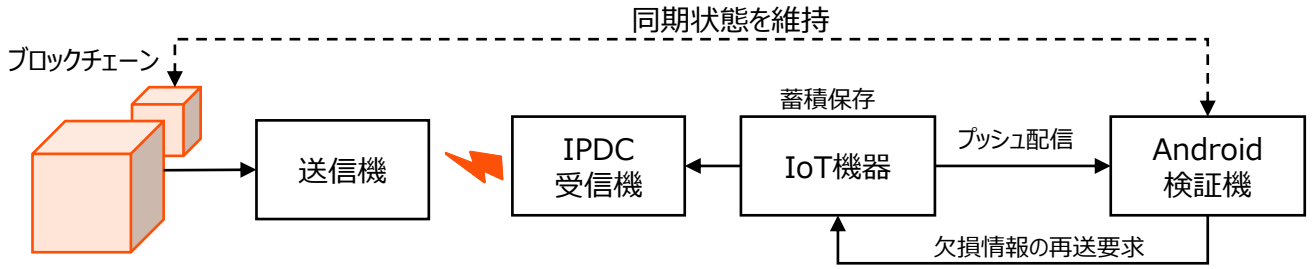


5-2. 社会実装に向けた取組の個別詳細

IPDC受信機普及に向けた環境整備

本実証で使用する信頼性検証では、信頼の基点となる特定の過去の情報から現在までの検証情報を連続的に受信していることが重要となる。そのため、放送受信後の**IPDC受信機とAndroid検証機間の無線通信**、および**送信機側からの配信間隔制御**によって、より柔軟な検証環境を整備した。

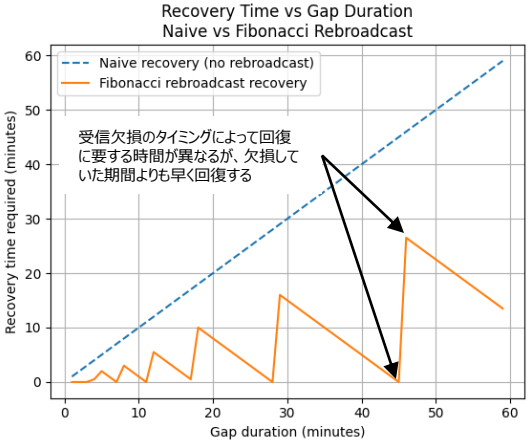
IPDC受信機とAndroid検証機間のローカル無線通信



受信したデータをIoT機器で**蓄積保存**する。IoT機器とAndroid検証機はローカル無線通信で接続し、IoT機器が放送から受信した最新情報は**プッシュ配信**し、Android検証機側での欠損情報は都度再送要求することで**ブロックチェーンと同期した状態を維持**する。

送信機側からの配信間隔制御

受信欠損期間と回復に必要な期間の対比グラフ



放送休止や移動中の受信など、受信環境によりデータ欠損が生じた場合、双方向通信では欠損分をサーバに問い合わせて補完できるが、放送では過去情報を再送する仕組みが必要となる。そのため、直近情報の早期回復と、長期間欠損した情報の最終的な補完を両立する再送方式として、再送間隔を緩やかに拡大させていくフィボナッチ数列に基づくカルーセル方式を設計・評価した。

評価：

フィボナッチ数列の間隔で過去のブロックヘッダーを再送しておくと、
1時間以内の受信時間の欠損を平均8.45分で解消（最遅26.5分）、
1日以内の受信時間の欠損を平均3.26時間で解消（最遅12.85時間）、
2週間以内の受信時間の欠損を平均2.24日で解消（最遅6.1日）できる。

フィボナッチ数列

前の2つの数を足し合わせて次の数を作る数列。1, 1 から始まり、1, 1, 2, 3, 5, 8, 13, 21, 34 …のように続いていく。この並びは、増え方が緩やかに加速するため、特定の範囲に偏りにくい構成になる。植物の葉の並びなど自然界にも見られることが知られており、このような「重なりにくさ」「偏りにくさ」の性質を持つとされる。この性質を再送間隔の設計に応用することで、直近の受信欠損は高頻度で補完しつつ、長期欠損も時間の経過とともに無駄を抑えながら回復できる。

カルーセル方式

同じデータを一定周期で繰り返し放送する方式。放送は単方向通信であり、受信側から再送要求ができないため、送信側があらかじめデータをループさせる構造をとる。受信者は途中から受信を開始しても、時間の経過により必要なデータを取得できる。

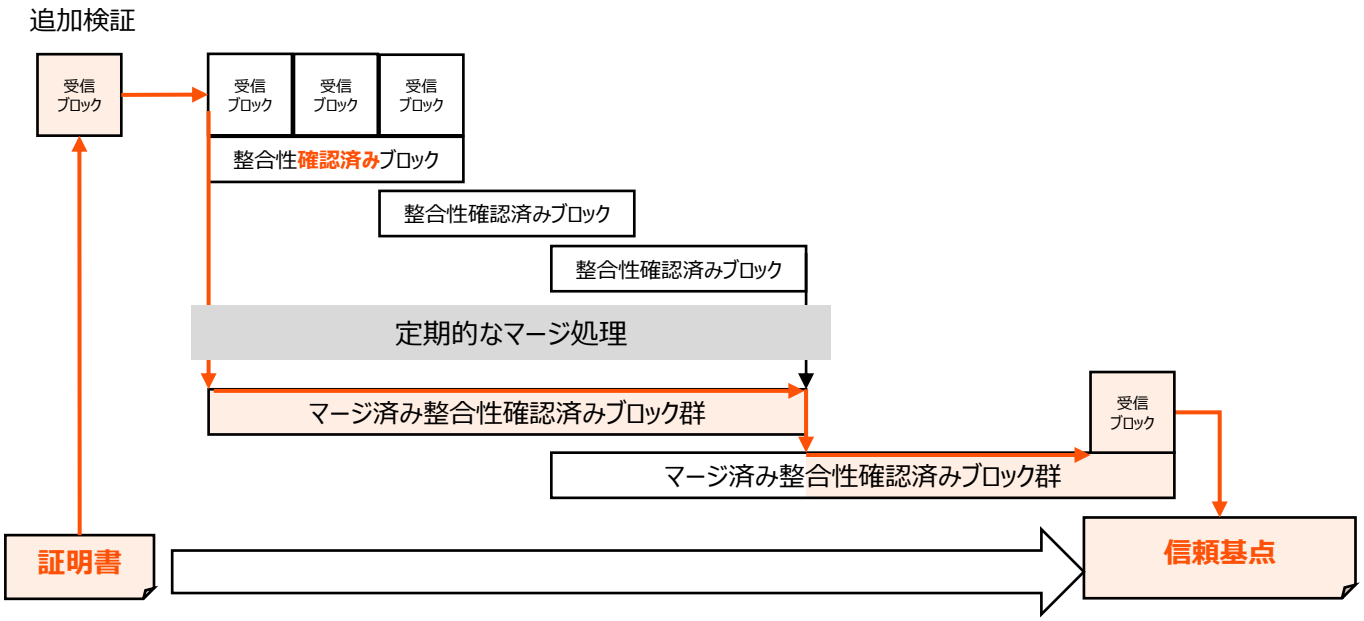
5-2. 社会実装に向けた取組の個別詳細

IPDC受信機普及に向けた環境整備

検証結果のキャッシュ機構

放送で受信したデータの信頼性検証には、**証明書**の存在がブロックチェーンによって保証され、あらかじめ周知された**信頼基点（基準となる公開情報）**まで検証連鎖を辿れる必要がある（詳細は3-2. 技術開発の個別詳細：ブロックチェーンへデータ（証明書）の記録と検証の仕組み、および4-2. 検証及び調査の個別詳細：構成明示型VCを参照）。

しかしながら、検証を行う度にこの一連の**受信ブロック**の**整合性確認**を都度最初から実施するのは計算量が大きい（Symbolブロックチェーンの場合は2週間で約40,320ブロックが蓄積される）。そこで、受信したブロックの整合性確認結果を定期的に蓄積保存する仕組みを実装した。これにより、最新情報受信時には整合性未確認の差分のみを**追加検証**すれば十分となる。このキャッシュ機構の実装により、トラストアンカーからの完全な検証連鎖を維持しつつ、リアルタイムでの信頼性確認を実現した。



検証者は**証明書**から**信頼基点**までのつながりを確認

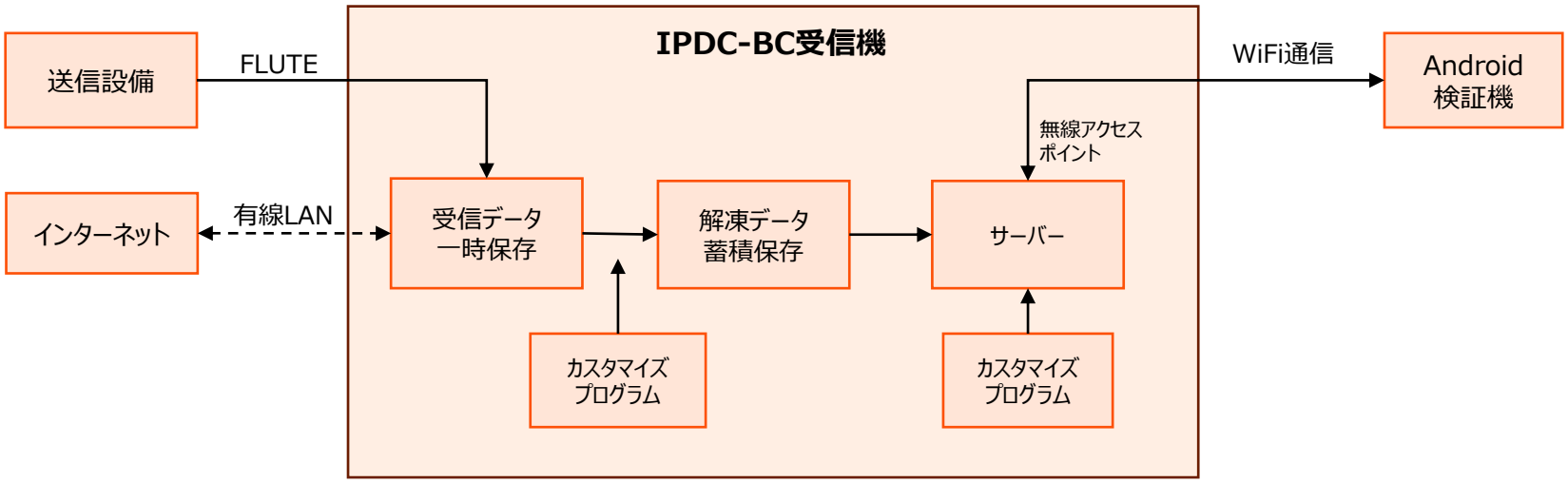
5-2. 社会実装に向けた取組の個別詳細

IPDC受信機普及に向けた環境整備

IPDC受信機開発に向けた整理

本実証では、受信機からAndroid検証機までのリアルタイム配信を実現するとともに、放送機器メーカーへのヒアリングを実施した。これにより、今後の実証を進める上でIPDC受信機に求められる機能要件を整理することができた。
まず、量産による低コスト化を見据えた設計としつつ、IPDC受信機の試作機を開発し、一定のカスタマイズ余地を残すことで、フィールド実証時に発生する課題を洗い出せる構成としておく必要がある。また、普及段階を考慮すると、受信機とIoT機器は一体型の構成とし、設置を行う自治体の作業負担を軽減するような設計上の工夫も必要となる。

想定するIPDC受信機



5-2. 社会実装に向けた取組の個別詳細

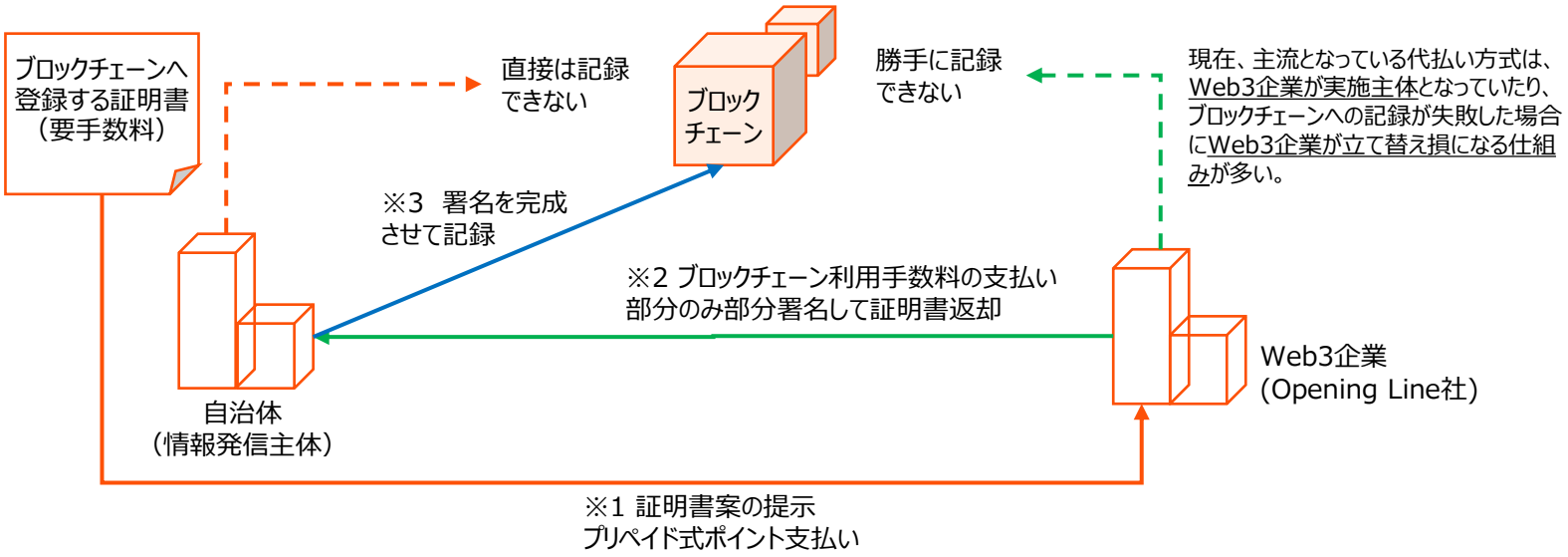
運用コスト軽減に向けた環境整備

本実証では、単方向で配信されるデータでも発信者確認を可能とするために、ブロックチェーンを信頼の土台として使う。しかし、ブロックチェーンに情報を記録するには通常、暗号資産が手数料として必要になるが、想定ユーザとなる自治体が暗号資産を保有すると、会計監査や税務処理の手続きが増え、運用コストが上がりやすい。

そこで本事業では、自治体が暗号資産を持たずに運用できるように、サービス利用料に相当する独自のポイント（手数料代替ポイント）を使う方式を採用する。自治体はあらかじめWeb3企業からこのポイントをプリペイドで購入しておき、ブロックチェーンに記録する証明書の中で手数料相当のポイントをWeb3企業へ支払う内容を明記する（※1）。Web3企業はその内容を確認して問題がなければ、実際のブロックチェーン利用手数料の支払い部分のみ電子署名を行う（※2）。

このときWeb3企業が行うのは、代払いを成立させるために必要な一部の署名だけである。記録するデータの内容や、記録するタイミングの判断には関与しない。最終的な実行（ブロックチェーンへの送信）は発信者側が行う（※3）ため、第三者が送信まで代行する方式とは異なり、実行の主体性は自治体側に残る。

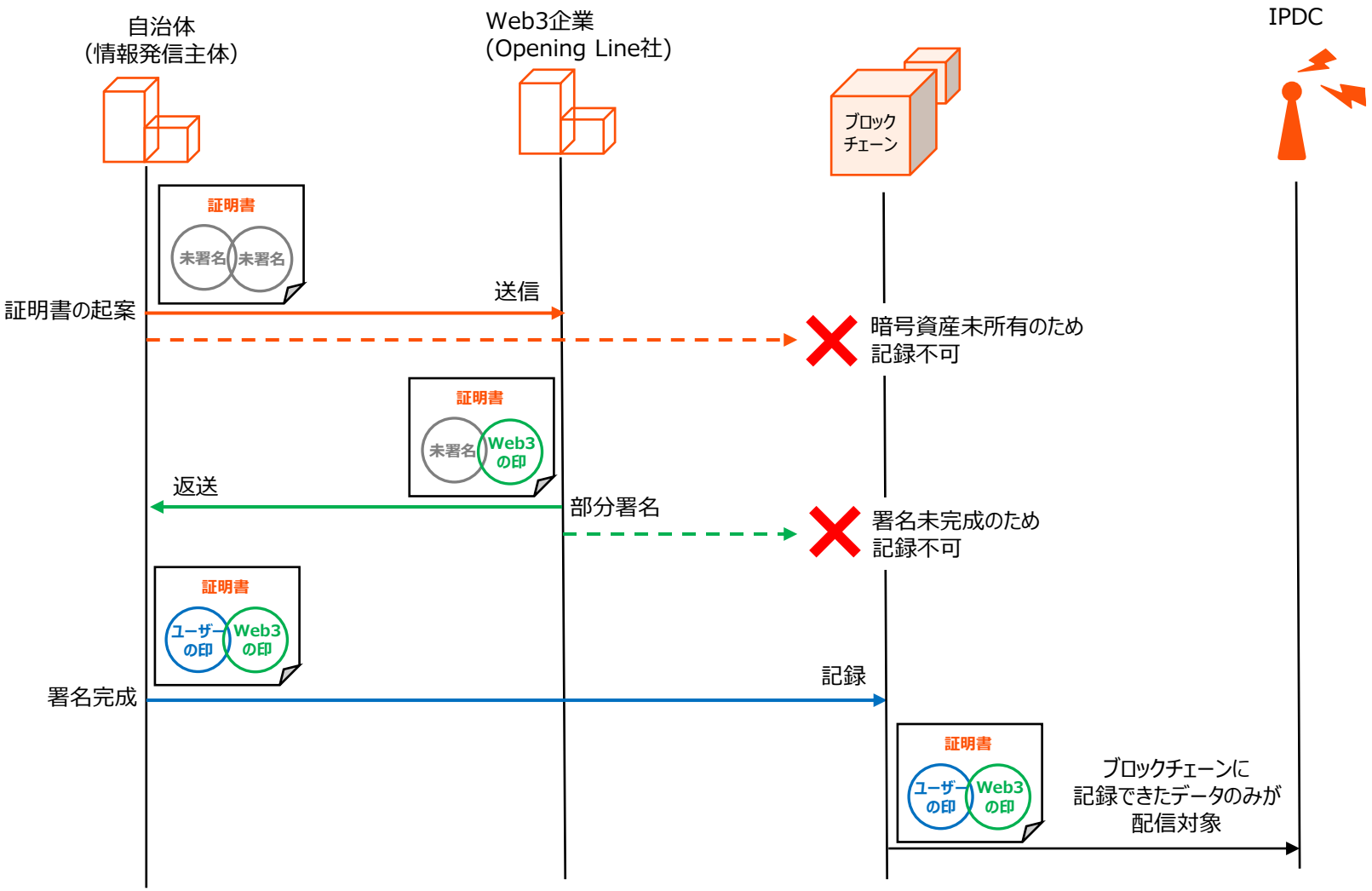
この方式により、発信者側は暗号資産を保有せずに証明書を作成・発行できる。つまり、情報システムの運用と、暗号資産に関わる会計処理を分離しやすくなり、ブロックチェーン活用の参入障壁を下げることができる。



5-2. 社会実装に向けた取組の個別詳細

運用コスト軽減に向けた環境整備

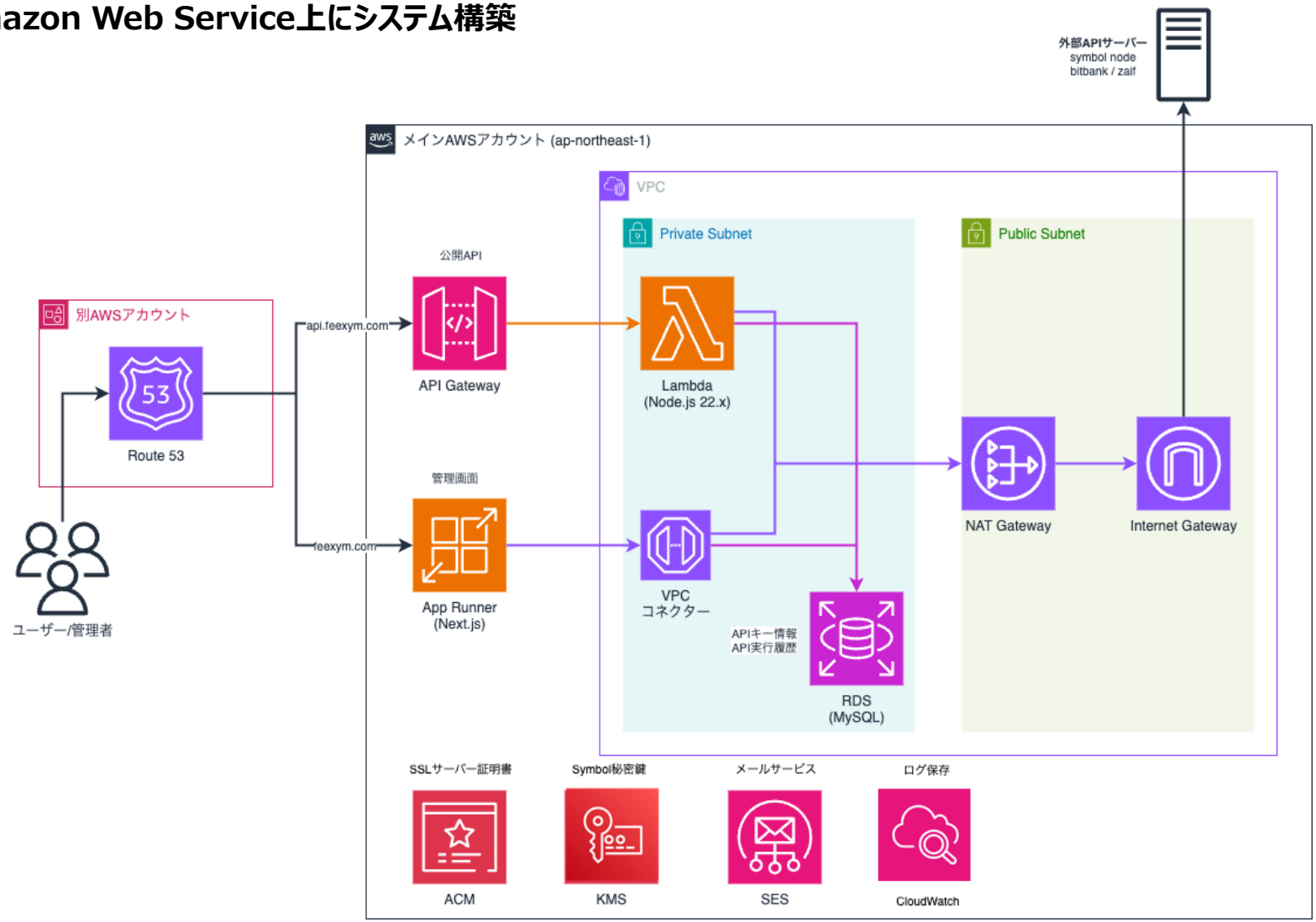
処理の流れ　自治体による証明書の起案から、ブロックチェーンへ記録してIPDCによる配信対象となるまでの流れ



5-2. 社会実装に向けた取組の個別詳細

運用コスト軽減に向けた環境整備

Amazon Web Service上にシステム構築



5-2. 社会実装に向けた取組の個別詳細

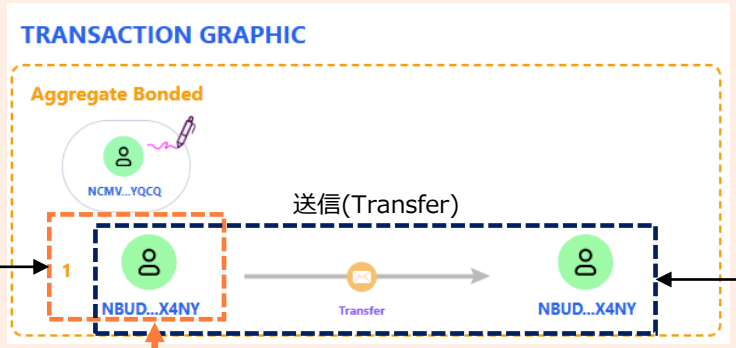
運用コスト軽減に向けた環境整備

実際に記録されたブロックチェーン上の処理詳細（トランザクション詳細）

前年度の登録方法

情報登録者が暗号資産を所有して
ブロックチェーンにデータを記録。

暗号資産の会計上および税務上の管理は
自治体にとっては通常業務とは異なる処理が発生し、
暗号資産の利活用が整備されるまで社会実装のハードルが高い。



NBUD…X4NY
情報登録者
（自治体）

手数料支払い
対象ユーザー

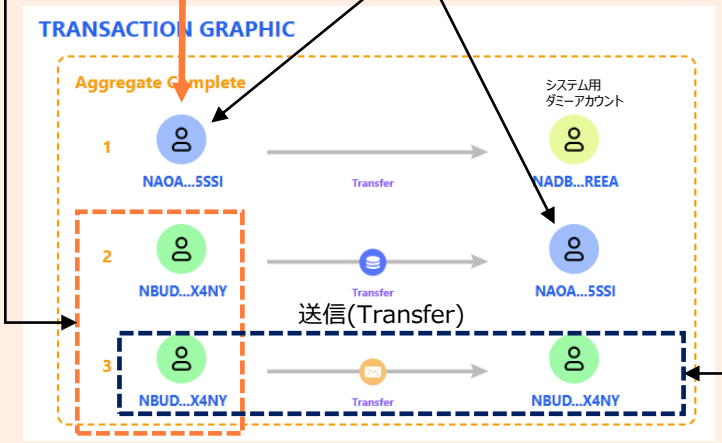
NAOA…5SSI
Web3企業

ブロックチェーンに
記録する処理
（データ）

本年度整備した登録方法
（手数料代払い）

Web3企業が暗号資産を所有して
ブロックチェーンにデータを記録。

暗号資産の会計上、および税務上の管理は
Web3企業にとっては通常業務処理。



5-2. 社会実装に向けた取組の個別詳細

運用コスト軽減に向けた環境整備

本事業で発行したプリペイド式ポイントが**資金決済法上の「暗号資産」に該当するか否か**については、不特定多数に対して使用可能であること、物品・役務の対価として利用できること、電子的に移転可能であること等の要件を総合的に勘案して判断される。暗号資産に該当する場合には、暗号資産交換業への該当可能性を含めた検討が必要となり、監督当局への報告義務等の体制整備が求められ、相応の運用負担が発生する。

＜資金決済法に抵触しない根拠＞

■暗号資産の定義

資金決済に関する法律（平成二十一年法律第五十九号）第２条１４項

１４　この法律において「暗号資産」とは、次に掲げるものをいう。ただし、金融商品取引法第二十九条の二第一項第八号に規定する権利を表示するものを除く。

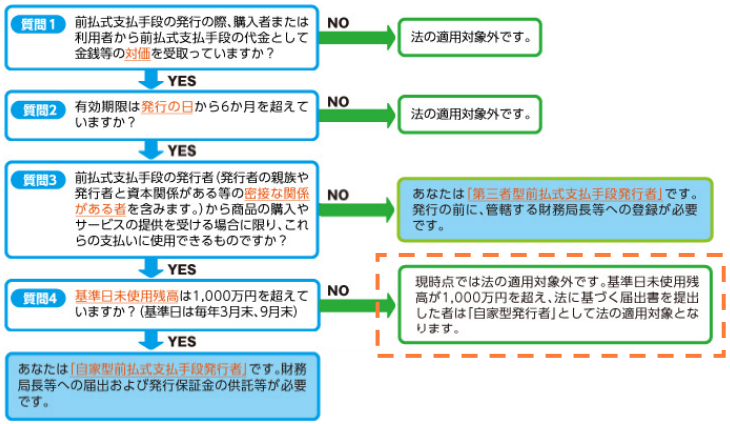
一　物品等を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨、通貨建資産並びに電子決済手段（通貨建資産に該当するものを除く。）を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの

二　不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの

事前に契約を結んだ相手との取引に該当するため、不特定多数に該当しない

前払式支払手段に該当するか否かについては、対価性の有無、有効期限、発行者との関係、未使用残高等の実態に基づいて判断される。前払式支払手段に該当する場合には、監督当局への報告義務等の体制整備が求められ、相応の運用負担が発生する。

＜前払式支払手段発行業として法の適用対象外である根拠＞



一般社団法人日本資金決済業協会｜前払式支払手段発行業の概要　より図を抜粋
https://www.s-kessai.jp/businesses/prepaid_means_overview.html

親密な関係者にあたると考えられるため、基準日（３月末、９月末）に残高１千万円を超えなければ適用外
ただし、１千万円を超える場合は「自家型」に該当する可能性あり

目次

1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

6-1. 普及啓発活動の全体像

普及啓発活動に係る取組・成果の全体像

令和7年10月に開催されたブロックチェーンEXPOを通じて、偽・誤情報への取り組みについての普及啓発活動を行った。

展示会名

NextTechWeek2025 第6回ブロックチェーンEXPO【秋】
会期：2025年10月8日(水)～10日(金)
会場：幕張メッセ　主催：RX Japan株式会社
展示会全体の来場者数3日合計：20,314名(前年度24,077名)

展示内容

「放送×ブロックチェーン 信頼で未来をつなぐ」 展示ブース：小間番号32-14

講演内容

「災害時に広がる“情報の二次災害”を防げ！放送×ブロックチェーンが挑む偽・誤情報対策」
Blockchain Case Studies 2025
セミナー番号：BC-6「Blockchain Case Studies 6」

ブース来訪者：235名、トークセッションの聴講者：50名
[業種別来場者数]
Web3：43名、**放送局・メディア：15名**、IT通信：29名、製造メーカー：38名、コンサル：18名、制作：12名
インフラ：12名、教育・研究：12名、広告：9名、AI：7名、官公庁：6名

関東圏の主要放送局3社を含む放送局・メディア業種の来場者15名に弊社の取り組みを詳しく知っていただくことができたため、
設定していたKPI「IPDCについて放送局や自治体への説明会実施（3件以上）」を達成。

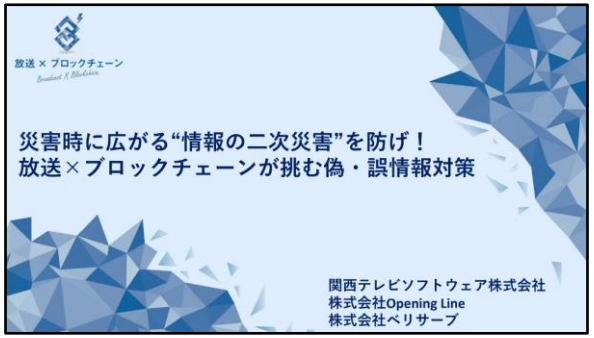
6-2. 普及啓発活動の個別詳細

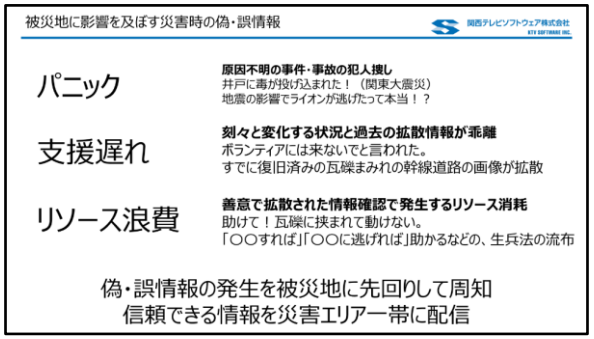
ブロックチェーンEXPO　展示概要

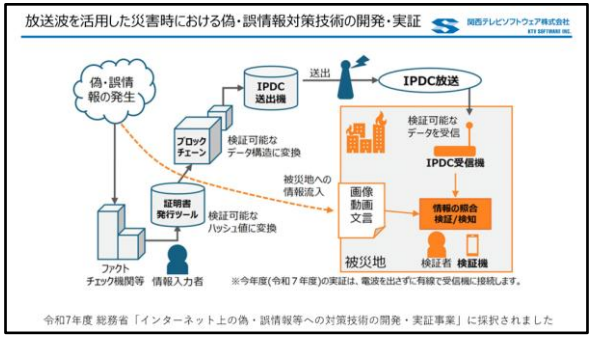
ブース展示の様子

トークセッションの様子

使用スライドの抜粋







アプリケーションのデモ

目次

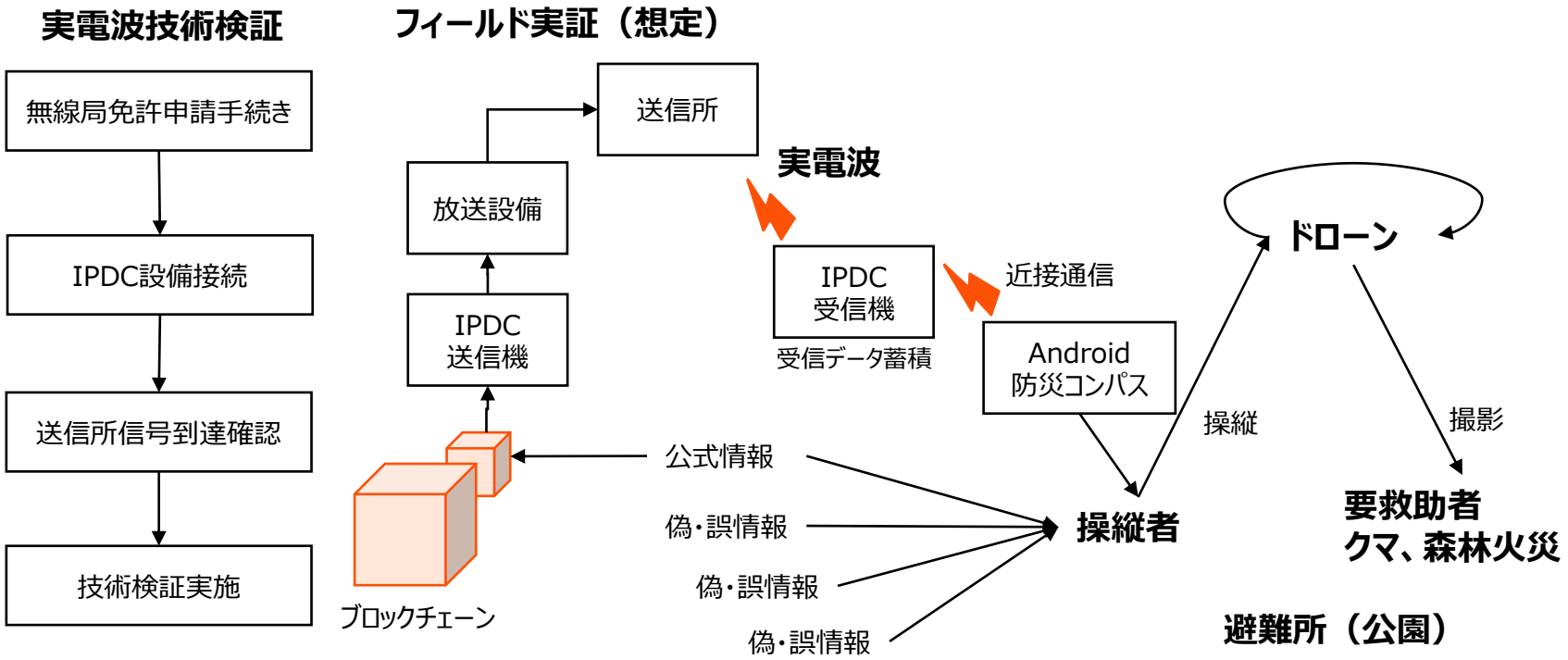
1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

7-1. 技術開発及び社会実装における課題・展望

技術開発及び社会実装にあたっての今後の課題およびそれらを踏まえた今後の展望

本開発・実証期間における検証は、有線接続による送受信環境を前提としたものであり、社会実装を見据えた場合には、実電波を用いたフィールド実証が不可欠となる。

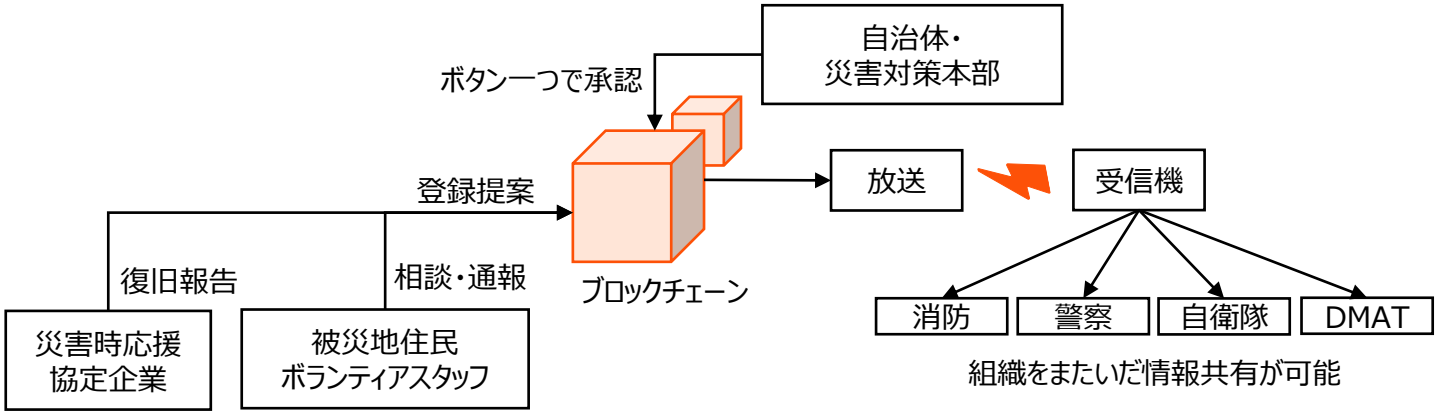
実際の放送環境において、送信から受信までを通して検証するための技術的・運用的課題について、送信基地局までのIPDC配信、放送休止中の技術検証実施と段階的に分けて整理する必要がある。
また、放送波で受信したデータをスマートフォン等のGPSやカメラを搭載した端末で活用するためには、受信機から取り出したデータの信頼性検証を安全かつ確実に実施する必要がある。実電波の技術検証フェーズは、送信設備のみならず受信機側におけるデータ蓄積・検証・端末連携までを含めての安定性を考慮する必要があり、今後の量産を想定した評価機としての受信機設計は重要な技術課題として位置づけられる。



7-1. 技術開発及び社会実装における課題・展望

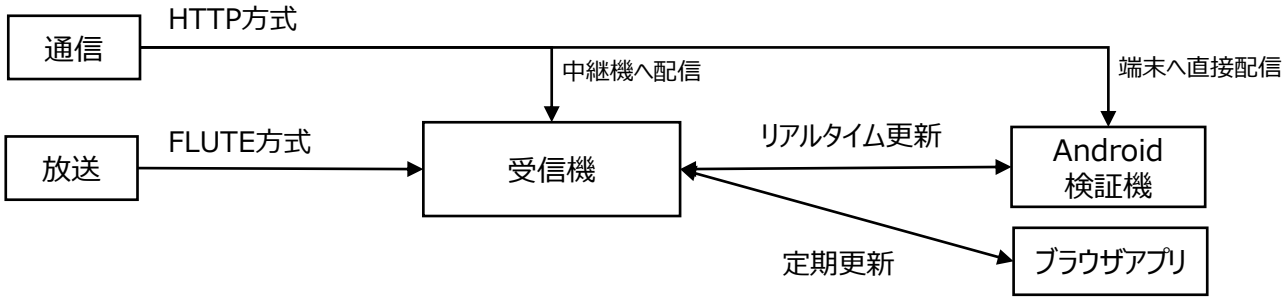
技術開発及び社会実装にあたっての今後の課題およびそれらを踏まえた今後の展望

災害時に登録・管理すべきデータが増加すると、現場の負担が増大するため、導入を妨げる要因となる。今後の展望としては、自治体が情報登録するだけではなく、**災害時応援協定企業**や**ボランティアスタッフ**による登録提案を可能とし、自治体が**ボタン一つで承認**可能な仕組みにより運用負荷を下げる方策を実現する。従来システムで不特定多数の登録提案を実現しようとするとセキュリティ対策や認証基盤の構築が必要となりシステム構築コストが大きなものになるが、ブロックチェーンを使用することで組織横断型の申請・承認システムが低コストで実現可能になる。



防災用途では、すべての状況で放送波受信を前提とするのではなく、導入条件や防災関連予算の規模に応じた柔軟な構成が求められる。配信方式の切り替え(HTTP/FLUTE)により放送と通信の双方で同一情報を配信できるハイブリッド構成を採用する。さらに、通信の場合は受信機を中継して利用する方式とAndroid検証機へ直接配信する方式を選択可能とすることで、導入環境に応じた段階的な社会実装を可能とする。

災害の規模に応じて通信でも接続可能なハイブリッド構成



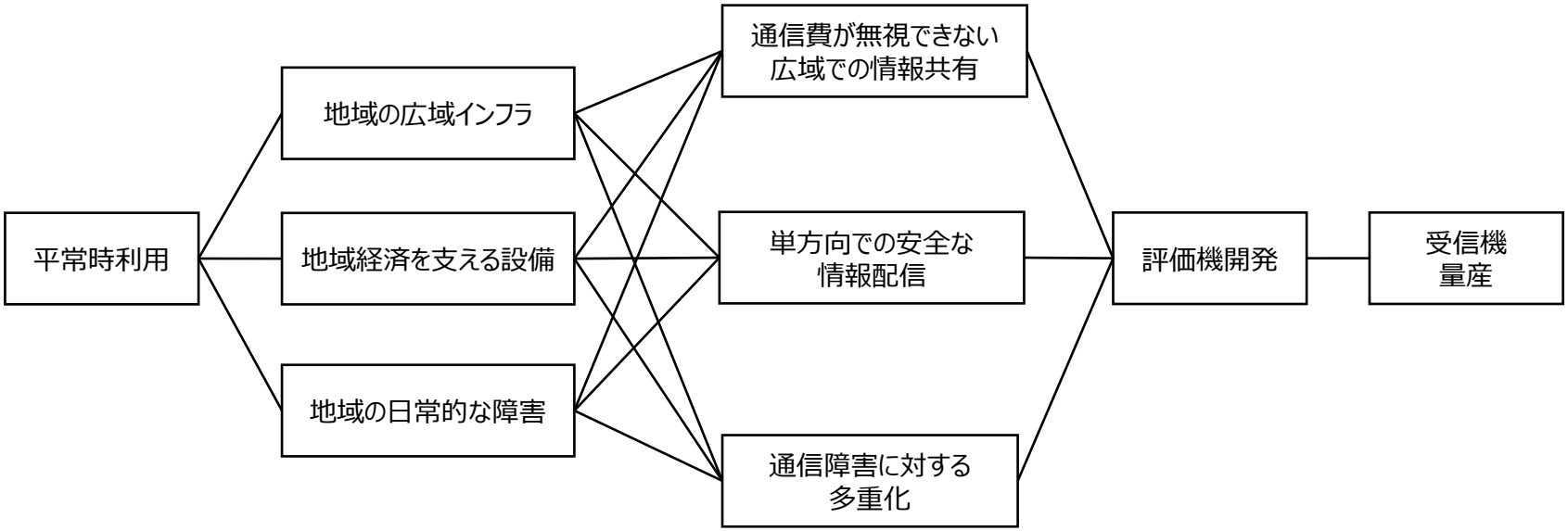
7-1. 技術開発及び社会実装における課題・展望

技術開発及び社会実装にあたっての今後の課題およびそれらを踏まえた今後の展望

ヒアリングや有識者からの助言を通じて、本実証を社会実装するうえでは、災害時に限らない**平常時活用**が重要であるとの意見が多く示された。本実証の根幹となるものは、偽・誤情報対策に限らず同一エリアで生活や経済活動を営む人々が、共通した判断基準を共有できる情報基盤を構築することにあるため、今後の展望としても平常時活用を視野に入れる必要がある。

放送インフラを活用した単方向かつ安全な情報配信は、通信費の制約を受けにくく、広域での情報共有を可能とする。また、通信障害時にも機能する多重化された情報伝達手段として、地域インフラの信頼性を高める役割を果たす。この特性を、平常時の**地域インフラ運用**や**地域経済を支える設備**、**日常的に発生する障害対応**に活用することで、継続的な利用価値を生み出す。具体的には、**通信費が無視できない広域での情報共有**が必要な場合、あるいは、双方向での通信による情報取得がセキュリティ的に課題が大きく**単方向での安全な情報配信**を行いたい場合、また住民の生活に直結していて損失リスクが大きいために**通信障害に対する多重化**が必要な場合などが考えられる。

そのために、要件を満たす受信機の開発を進め、評価・検証を経て**量産体制を整える**ことで、社会実装へと段階的に展開していく。結果として、平常時に使われ続ける情報基盤が、そのまま災害時にも機能する構成を目指す。

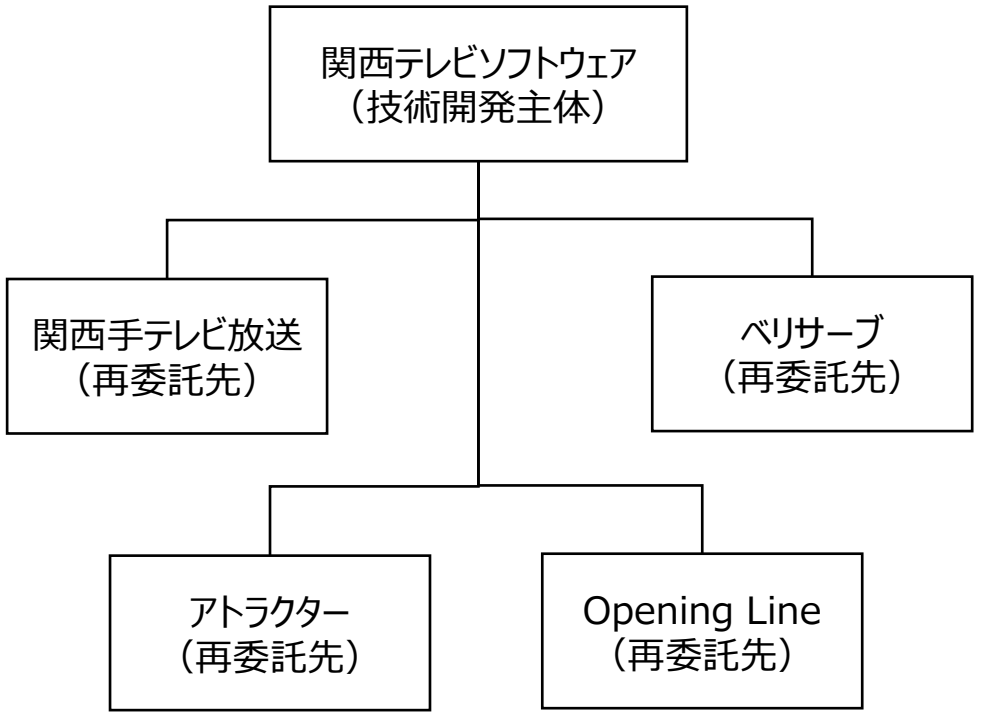


目次

1. 開発・実証のサマリ
    1. 開発・実証のサマリ
2. 開発・実証の背景・目的
    1. 開発技術によりアプローチする課題
    2. 開発技術により目指す姿・ゴール
    3. 開発技術により対処可能なユースケース
3. 開発・実証における「対策技術の開発」
    1. 技術開発の全体像
    2. 技術開発の個別詳細
4. 開発・実証における「対策技術の有効性等に関する検証及び調査」
    1. 検証及び調査の全体像
    2. 検証及び調査の個別詳細
5. 開発・実証における「対策技術の社会実装に向けた取組」
    1. 社会実装に向けた取組の全体像
    2. 社会実装に向けた取組の個別詳細
6. 開発・実証における「普及啓発活動への協力」
    1. 普及啓発活動の全体像
    2. 普及啓発活動の個別詳細
7. 開発・実証の課題・展望
    1. 技術開発及び社会実装における課題・展望
8. 開発・実証の実施体制等
    1. 実施体制及び役割分担
    2. 全体スケジュール

8-1. 実施体制及び役割分担

本事業の実施体制図



各団体の役割・業務範囲

関西テレビソフトウェア株式会社
災害時において、放送波を活用することにより偽・誤情報の拡散抑制を目指した開発実証・環境整備・社会実装の推進。

関西テレビ放送株式会社
IPDCデータを放送設備へ入力した場合の影響検証及び課題の解消に関する調査。

株式会社アトラクター
IPDC送受信に関わる環境の構築およびブロックチェーン分散環境との安定同期に必要な技術開発の実施。

株式会社ベリサーブ
IPDCによる単方向配信で構築される検証基盤の有効性・安全性についての調査・評価。

株式会社Opening Line
ブロックチェーン活用時に発生する暗号資産の運用コスト軽減に向けた環境整備。

8-2. 全体スケジュール

主な実施事項	令和7年					令和8年		
	8月	9月	10月	11月	12月	1月	2月	3月
インターネット上の偽・誤情報等への対策技術の開発								
位置情報と連動させたコンパス型アプリケーション	→	→	→					
前年度開発アプリケーションの効率化と精度向上			→	→	→			
評価・分析					→	→	→	→
インターネット上の偽・誤情報等への対策技術の有効性等に関する検証及び調査								
セキュリティ評価（構成明示型VC）	→	→	→	→	→	→	→	→
インターネット上の偽・誤情報等への対策技術の社会実装に向けた取組								
放送設備検証		→	→	→	→			
IPDC受信機普及に向けた環境整備（受信機側システム開発）			→	→	→			
運用コスト軽減に向けた環境整備（暗号資産手数料代替システム開発）		→	→	→	→	→	→	