IPDCとブロックチェーンを活用した災害現場での信頼性検証システム

横島 裕明　大山　悟

はじめに

関西テレビソフトウェアでは、2019年より改ざんに強いとされるブロックチェーンと広範で安定したカバレッジを実現する放送波を組み合わせることで、災害時やより高度な通信インフラが必要となる環境でのコミュニケーション手段について、調査・研究を進めている。例えば、災害時はネットワーク環境が不安定となるため、インターネット上で公開鍵認証基盤を使用した信頼性検証が困難になる。そこで、ブロックチェーンにおいてノード間でやりとりされている信頼性検証情報を、放送波に重畳してエリア一帯にブロードキャスト（IPDC）することで、特定のサービスプロバイダに依存することなく検証に必要な情報をダイレクトに受信機へ届ける手法を提案する（図1）。

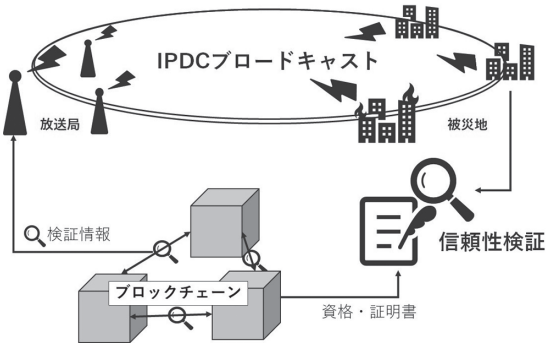

図1　IPDCでエリア一帯に信頼性検証情報をブロードキャストする

これにより、インターネットから分離された被災地の現場やアドホックネットワークへ、検証が必要な証明書を接近時通信あるいは直接搬送などでポータブルに移動させることが可能になり、激甚化しつつある災害環境においても「検証可能な証明書」の存在を根拠としてエリア一帯での経済活動が部分的に維持可能となる。

よこじま　ひろあき・おおやま　さとる：関西テレビソフトウェア株式会社　ソリューションセンターデジタルデザイングループ

今回、これら一連の仮説について机上での検証と有線での実証実験を株式会社アトラクター（以下、アトラクター社）と行ったので紹介すると共に、この手法は平常時におけるラストワンマイルやマルチネットワークなど双方向通信のみで運用した場合にかかるコストを削減できる可能性もあり、放送と通信の課題を補い合えるハイブリッドインフラとしての提言を最後にまとめさせていただきたい。

1．信頼性検証の範囲

本稿における「信頼性」とは公開鍵暗号方式（図2）の電子署名によって作成された証明書が間違いなく発行者が作成したものであるという真正性のことを指す。さまざまな経済活動において、利害関係者間での支払いや契約、決裁など自分の意思を表明する最小単位を「証明書」とし、その証明書データを発行・所有（提示）・検証できることで信頼性検証を可能とする。

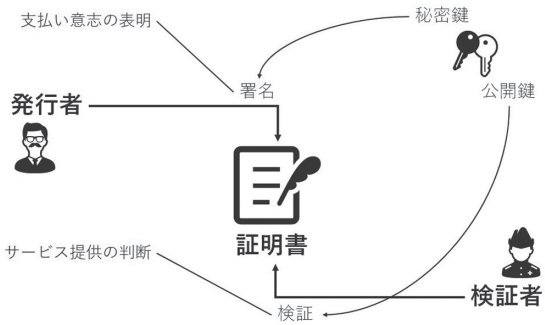

図2　公開鍵暗号方式

1．1．従来形式の課題

電子署名された証明書の信頼性検証、という観点では公開鍵認証基盤（PKI）が存在している。本稿では災害時のようなインターネットが利用できない状況においてもエリア一帯で共有するという要件を定義するため、第三者による認証局を必要としないスキームを検討したい（図3）。また、災害時という環境を想定

している以上、発行担当者の罹災による証明書発行業務への支障や、本人以外の人が証明書を提示するなりすましになどもできるだけ考慮し、より実運用に適した検証基盤としての実用可能性も重視する。

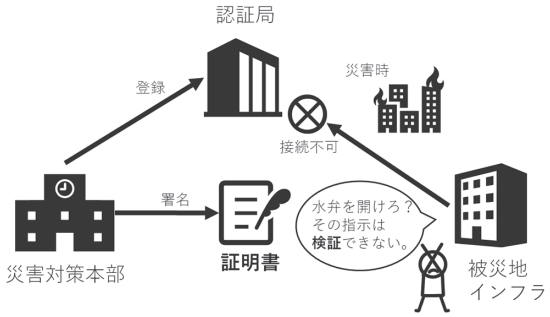

図3　災害時は認証局への確認が困難

1．2. DIDsとVCデータモデル

昨今、ブロックチェーンなどの特徴を活かしたDIDs(Decentralized Identifiers：分散型ID）によるVC(Verifiable Credentials：検証可能な資格情報）などのデータモデル策定がW3C(World Wide Web Consortium）で進められている。DIDsでは特定のサービスプロバイダがIDを定義するのではなく、ブロックチェーンを利用してユーザーが準備したIDにさまざまな証明書を紐づけて、そのIDを所有していることをユーザーが証明することで認証などを行う。VCのデータモデルによると、証明書にかかわる利害関係者には証明書を作成する「発行者（Issuer)」、証明書を所有する「所有者（Holder)」、証明書を検証する「検証者（Verifier)」を定義している。例えば、就職活動サービスの場合、卒業証書を作成するのが大学（発行者)、所有して就職活動で企業に提示するのが学生(所有者)、どの大学を卒業したのかを検証するのが企業（検証者)、と読み替えることができ理解しやすい（図4)。

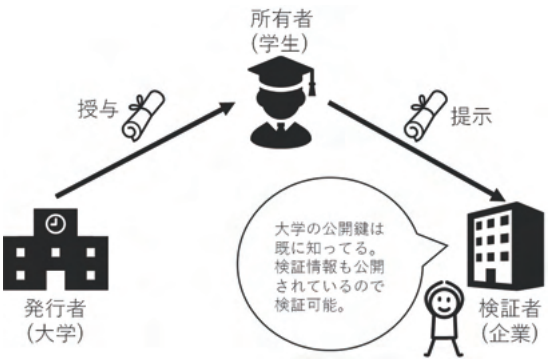

図4　VCデータモデル

前節の公開鍵認証基盤では第三者認証局によって認証されたサービス提供会社がサーバーにSSL/TLS証明書を配置し、サービス提供会社への信頼の元で証明書の信頼性を保証してきたが、DIDsは検証手段をブロックチェーン上に発行者自ら公開することで、第三者認証局やサービス提供者に依存しない検証手段を実現することができる。本稿においてもVCデータモデルの考え方に倣い、サービス提供会社への依存をせずに証明書を検証する手法をとる。

1．3. 証明書の検証

以下4つの事象が証明されていることを確認することで証明書の検証とする（図5)。

- 発行証明
- 非改ざん証明
- 所有証明
- オンチェーン証明

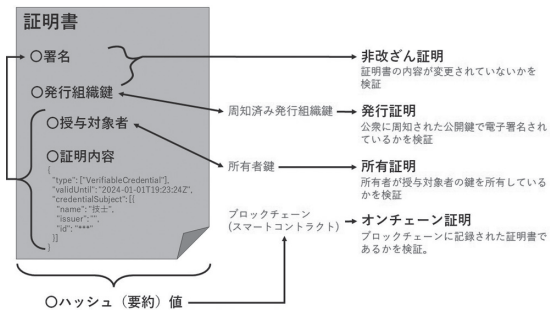

図5　検証する4つの証明

1．3．1．発行証明

事前周知された公開鍵と証明書の発行者が一致することを確認する。本稿が想定する災害時の環境では第三者認証局の最新の証明書を確認することはできない。そのため、証明書の発行組織は事前に公開鍵を周知し、固定しておく必要があるが、一般的な公開鍵認証基盤では、セキュリティ上公開鍵の定期的な更新を求められ、事実上1年程度が有効期限となっている。そこで、ブロックチェーンのAA技術等（Account Abstraction：アカウント抽象化）を用いて公開鍵を固定したまま、秘密鍵の実体を証明書発行の実務を担当する担当者間で分散管理する。これにより鍵の定期的なローテーションを実現し、紛失や漏洩時、または担当者罹災による証明書発行機能不全状態に陥ってもソーシャルリカバリ（分散管理されている他の担当者による復旧作業）によって鍵を差し替えることで失効リスト（CRL：Certificate Revocation List）を使用することなく対策を行うことができる。

1．3．2．非改ざん証明

発行者の作成した証明書が、検証者の検査対象となる証明書と一致することを確認する。署名は発行担当者によって実施され、発行組織の公開鍵と証明書の内容が共に署名対象となる。ブロックチェーンによって発行組織から発行担当者への委任関係を改ざんできないスマートコントラクトとして定義づけておくことによって、発行組織の作成した証明書とみなすことができる。

1．3．3．所有証明

検証者へ証明書を提示する者が、証明書内に記載された所有者（証明書授与対象者）と一致することを確認する。証明書はパブリックチェーン上で公開管理されているので、証明書自体の複製は容易である。なりすましを防ぐためには、証明書内にて指定された授与対象者と提示者の関係性を確認することが重要となる。本稿の実証実験では、災害現地で所有者と検証者が対面していることを条件としてPIN番号（Personal Identification Number：個人識別番号）を正しく署名できることで、提示者が所有者であることの証明とする。所有証明の確認方法については、パスワードやゼロ知識証明を使用するなど、ユースケースはさまざまでありこの限りではない。

1．3．4．オンチェーン証明

証明書がブロックチェーンに記録されていることを確認する。この確認には、ブロックチェーンが出力するブロックヘッダーを監視する必要があり、このデータの送受信にIPDCを使用する。オンチェーン証明により、証明書が単なる電子署名による証明書ではなくブロックチェーン上のスマートコントラクトの制約を満たした証明書であることが確認できる。本稿では、周知済み公開鍵を固定し、秘密鍵を担当者間で分散管理させるために使用する。

2. IPDCとブロックチェーンの特性

2．1．IPDCの特性

IPDCとはIP Data Castの略であり、データをIPパケット形式で分割し放送波に重畳して一斉配信する放送サービスの総称である。放送で使用する帯域の一部を使用するため大きなサイズのデータを常時放送することはできない。また、放送は災害時でも比較的安定してエリア一帯に情報を伝送することができる。

2．1．1．FLUTE

IPDCのファイル転送はRFC6726に規定されているFLUTEプロトコルを使用している。このプロトコルでは送信機から受信機へ向けて単方向のファイル転送を可能にする。今回の実証実験ではJSON形式のテキストファルを証明書として転送したが、FLUTE自体はデジタルデータであればテキスト・バイナリ問わず、いかなる形式のファイルでも分割して転送可能である。

2．2．ブロックチェーンの特性

ブロックチェーンとは情報通信ネットワーク上にある端末同士を直接接続して、暗号技術を用いて取引記録を分散的に処理・記録するデータベースの一種であり、「ビットコイン」等の暗号資産に用いられている基盤技術である。計算された時間ごとにブロックが生成され、トランザクションと呼ばれる電子署名されたデータベースを更新する指示情報を格納する。それらの指示情報はブロックチェーン内部のデータを更新すると共にブロックヘッダーという数KB程度の要約値にまとめ上げられて、P2Pネットワーク内でブロードキャストを繰り返し、全ノード間で合意を形成する。合意形成されたブロックの要約値は次に生成されるブロックに記録され、すべてのブロックの存在が前ブロックの存在に支えられるというチェーン構造が形成される。

2．2．1．消すことのできない存在証明

ブロックチェーンで最も核となる考え方が「消すことのできない存在証明」である。ノード間で共有された情報はたとえ大規模なネットワーク障害が発生したとしてもすべてのノードを同時に消去するなどしない限り、消滅することはない。このブロックチェーンのデータを更新するための最小単位となるトランザクションに証明書などを付記しておけば、誰でも検証可能な消すことのできない証拠としてさまざまな経済活動に使用することができる。また、処理されたトランザクションはその要約値となる情報がブロックごとに小さくまとめ上げられ、ブロックヘッダーに格納される。ブロックヘッダー内に存在の証拠を見つけることができれば、「消せない存在証明」により、そのトランザクションはブロックチェーン内部に必ず保存されていると考えてよい。一方でブロックヘッダーが共有されないネットワーク外では、存在を検証することは困難である。

2．3．IPDCとブロックチェーンを組み合わせる

ブロックヘッダーのサイズはIPDCで常時放送できる送信サイズに十分収まり、IPDCはブロックチェーンがネットワーク内でブロードキャストしている情報

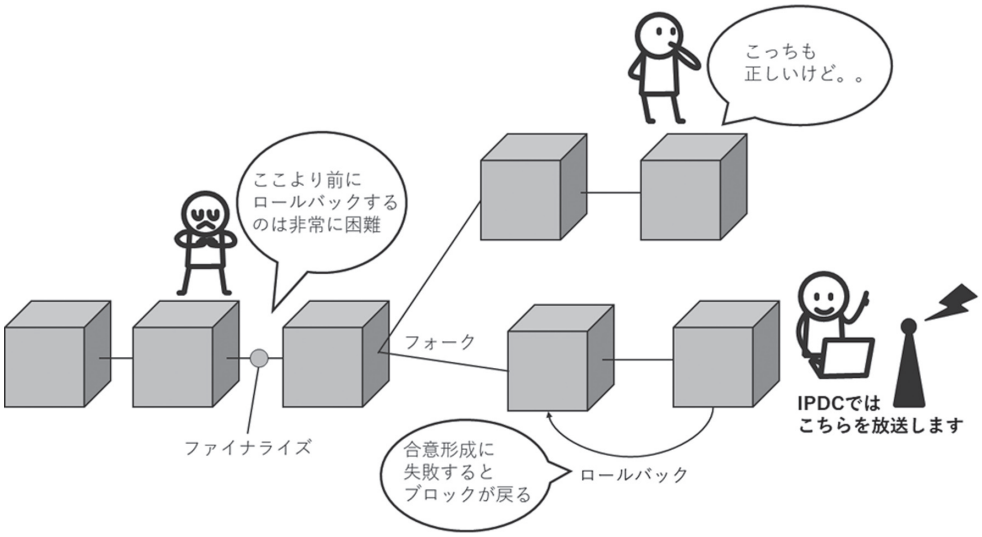

図6　ブロックチェーンの注意点

を放送可能なエリア一帯に拡散することができる。双方の特性の組み合わせにより、その地域が関わる重要な決定事項についての検証手段をエリア一帯で共有することが可能になると考える。

2．4．注意点

2．4．1．ロールバック／ファイナライズ

ブロックチェーンは分散型ノードのネットワークで合意形成されるため、合意形成に失敗したノードがデータを更新し直すために時折ロールバックが発生する。また、チェーンが分岐するハードフォークが発生する場合もあり、フォークした場合はどの分岐チェーンをIPDCで送出するのかを明確にしておく必要がある。いずれもファイナライズしたと想定されるブロックを超えてロールバックすることは困難であるために、検証側は平常時にあらかじめ、「このブロックまでチェーンを遡って検証できれば問題なし」ということを定期的に送信側と合意しておく必要がある（以下、本稿ではファイナライズ合意ブロックと表記）。（図6）。

3．実証実験

本稿の仮説を検証するために実施した実証実験のアーキテクチャや実施内容について解説する。

3．1．想定シナリオ

実証実験は災害時のボランティアスタッフが所有する資格を現地の作業監督者が確認するシナリオを想定した。ボランティアセンターにてスタッフが申告した資格を確認した証拠を証明書とすることで、その事実を現地で確認する。発行者がボランティアセンター、所有者がボランティアスタッフ、検証者が現地作業監督者とする。この想定は阪神淡路大震災において、ボランティアスタッフに電気工事士がいたために捜索作業が捗ったという当時の実体験に基づいて考案したユースケースである。電気工事士のみならず、重機の扱いや医療従事者など専門スキルを持ったボランティアスタッフが現地で迅速な救助に当たることができることを想定した。

3．1．1．想定する被災状況

- 被災現場でインターネットは使用できない。
- 受信機や検証機を動かすための電源設備は使用できる。
- IPDCを送出する放送局、また被災現場への支援指示を行う自治体などの本部組織は災害現場から少し距離が離れているため、インターネットが使用できる。
- IPDC受信機は被災地に配備されている。

3．2．アーキテクチャ

本実証のアーキテクチャは大きく分けて、IPDCとブロックヘッダーの同期部分、証明書発行部分、証明書検証部分に分かれる（図7）。

- IPDCとブロックヘッダーの同期
- 証明書の発行
- 証明書の検証

本実証では、被災地現場でインターネットが使用できないという想定により、検証時の認証局への問い合

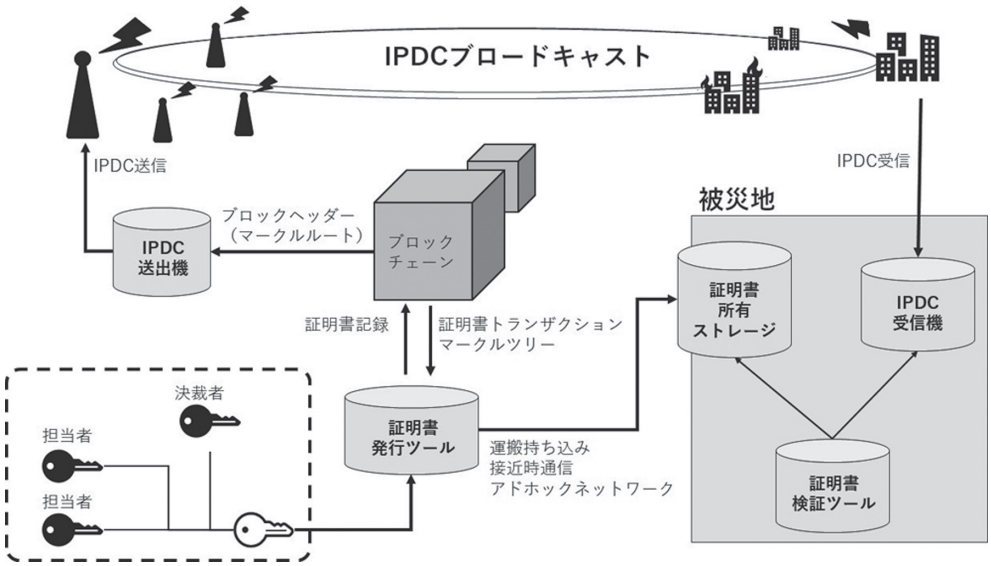

図 7　アーキテクチャ概要図

わせは不可能であり、発行時に使用した公開鍵の変更は固定されているという制約を課す。公開鍵の固定には、ブロックチェーンのアカウント抽象化技術でマルチシグを構成し、周知済みの発行組織の公開鍵を固定したままで、分散管理された発行担当者の鍵を定期的に差し替えることにより代替運用が可能である。しかしながら、署名検証だけでは信頼性の検証が十分ではなくなってしまうため、証明書がチェーン上に記録されている事実まで検証する必要性が新たに生じる。

3. 2. 1. IPDCとブロックヘッダーの同期

ブロックチェーンを構成するノードへ接続し、IPDCを通じて最新のブロックヘッダー情報を送出する。ブロックチェーンがフォークした場合は都度、ロールバックで修正されたブロックヘッダーで上書き更新する。またブロックヘッダーを取得するノードがネットワークの同期に失敗していたり、フォーク後に主流ではないチェーンに追従していたりする可能性もあるので、複数のノードから分散取得してチェーンの同期状況を随時確認する必要がある。

3. 2. 2. 証明書の発行

以下の手順により、証明書を発行する。

- マルチシグ設定
- 証明書作成
- 署名
- ネットワークアナウンス

ボランティアセンターはマルチシグ設定を行い、複数の証明書発行担当者間で秘密鍵を分散管理する。証明書発行担当者は、ボランティアスタッフの所有する資格・認定書などを確認し、ボランティアセンターの公開鍵を指定して証明書トランザクションを生成する。トランザクションを発行担当者の秘密鍵で署名してブロックチェーンに登録した後、ブロックチェーン上でのトランザクションの存在証明となるマークルツリー情報と共に証明書をボランティアスタッフに通知する。

3. 2. 3. 証明書の検証

ボランティアスタッフが提示する証明書の真正性を検証する。

- 署名検証
- マークルパス検証
- ブロックヘッダー整合性検証
- PIN認証

署名検証では証明書内に記載された電子署名により証明書が改ざんされていないことを検証する。マークルパス検証ではブロックヘッダーとマークルツリーによって証明書がブロックチェーン上に存在していることを確認する。 マルチシグの署名条件を満たした証明書でなければブロックチェーン上に記録することが出来ないため、証明書内の発行組織鍵と事前周知された公開鍵と照合して証明書がボランティアセンターとして発行されたことが確認できる。また、ブロックヘッダー整合性検証により、証明書の存在を記録したブロックが意図したチェーンに紐づいているかを確認

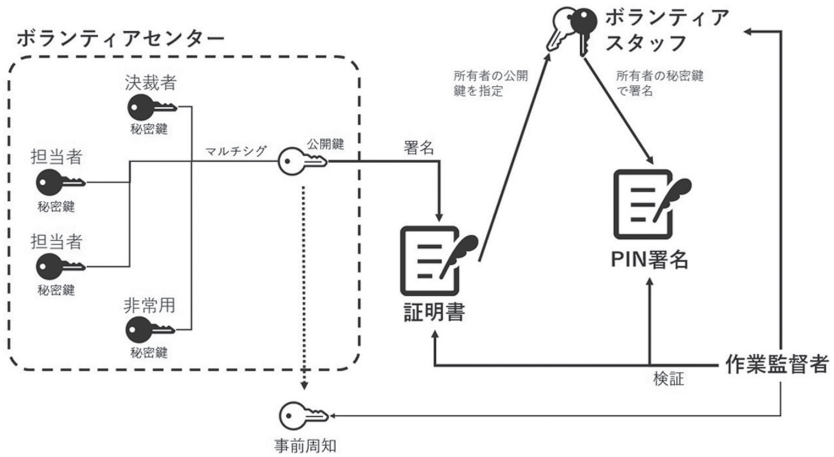

図8　本実証での公開鍵検証の活用方法

する。PIN認証では検証者が提示するPIN番号を証明書内で記載された授与対象者の公開鍵で正しく署名できるかどうかにより証明書提示者が所有者であることを確認する（図8）。

3. 3. データ構成

扱う情報は以下の通りである。

- 証明書（vc.json）
- ブロックヘッダー情報（{height}.json）
- ファイナライズ合意ブロック
- 所有者情報（holder.json）
- 提示者情報（persenter.json）
- 発行組織公開鍵（well-knownkeys.json）

証明書には証明書本文と特定ブロック高のブロックヘッダーを根とするマークルツリーを記載する。ブロックヘッダー情報はブロックチェーンでブロックが生成されるたびに付与されるヘッダー情報である。ブロックが処理したトランザクションの要約値がツリー状にまとめ上げられてその根となる部分がブロックヘッダーに記録されている。前ブロックの要約値も記録されおり、生成されたブロックは前ブロックと処理されたトランザクションの存在に支えられて生成されているため、検証したいトランザクションからマークルツリーをたどってマークルルートにたどり着けた場合はそのトランザクションはブロックチェーンに記録されていると判断することができる。また、ファイナライズ合意ブロックは検証者がブロックをどこまで遡って確認すれば、チェーンの一部とみなしてよいかを定期的に確認するために使用する。特に取り決めの無い場合はブロックチェーンが最初に生成したジェネシスブロックがそれにあたる（図9）。

所有者情報は、証明書内で指定された授与対象者に紐づく秘密鍵を暗号化して記録されており、この秘密

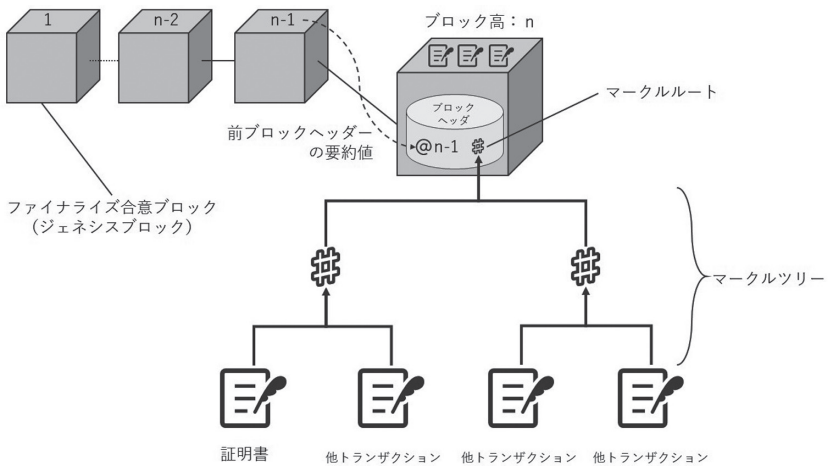

図9　ブロックヘッダーとマークルツリー

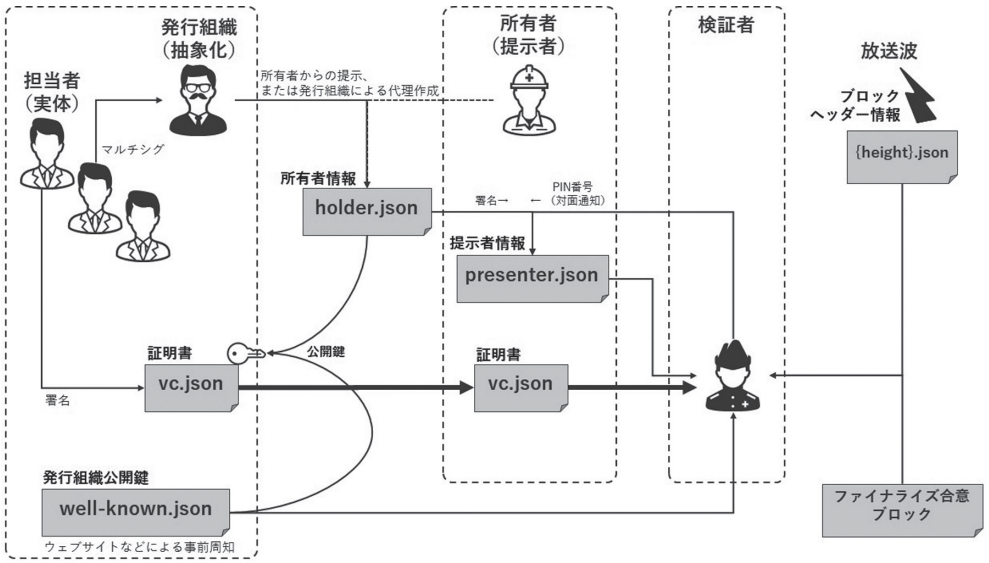

図10　データの流れ

鍵にアクセスできる者が証明書の所有を主張することができる。提示者情報は、検証者が対面で通知したPIN番号に対する所有者の電子署名が記録されており、授与対象者の公開鍵で署名検証に成功すれば、その相手は所有者であると見なすことができる。発行組織公開鍵は、マルチシグ構成を取る証明書発行組織の公開鍵が記録されている。発行組織の秘密鍵はブロックチェーンへの記録には使用できないように無効化されており、証明書発行担当者の署名によってトランザクションを実行することができる（図10）。

3. 4. サブシステム

本実証では以下5つのサブシステムを開発した。

- 証明書発行ツール
- 証明書所有ストレージ
- 証明書検証ツール
- IPDC送出機
- IPDC受信機

証明書発行ツールは証明書を発行する（図11）。証明書所有ストレージは証明書と証明書内に記載された授与対象者情報を所有するためのストレージである（図12）。検証者が提示したPIN番号を署名して提示する機能を持つ。証明書検証ツールは証明書を検証する（図13）。IPDC受信機が蓄積しているブロックヘッダーを検証する。IPDC送出機はブロックチェーンから随時ブロックヘッダーを取得し、IPDCを通じて送出する。機器はアトラクター社の「IPDC編成／TS送出システム」を使用した。IPDC受信機はIPDCからデータを受信し、蓄積する。機器はアトラクター社の「IPDC受信システム」を使用した。

図11　証明書発行ツール

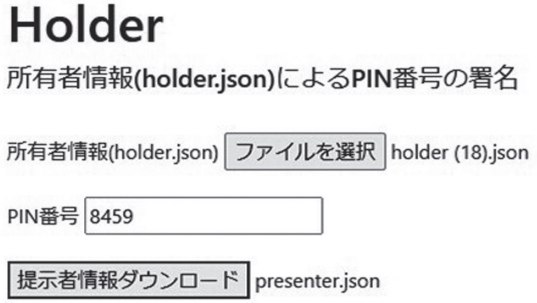

図12　証明書所有ストレージ

図13　証明書検証ツール

3. 5. ブロックチェーン

放送波という公共財で扱う特性上、接続するブロックチェーンはパブリックブロックチェーンとした。パブリックとは、誰もが自由にノードを追加してネットワークに参加することができ、特定少数の管理者による恣意的な合意を形成させることが極めて困難なネットワークである。またパブリックブロックチェーンの中でも、直接ノードに対してマークルツリーなどの検証情報を取得できるAPI エンドポイントを広く分散させているSymbolを採用した。Symbolは2021年のローンチ以降、ブロック生成が止まったことがなく、災害発生時など緊急を要する要件を満たしており、採用には即時性よりも安定性を重視している。即時性とは、合意形成に関与するノードを制限するなどしてブロック生成がロールバックしないことを保証する機構（即時ファイナリティ）を持つチェーンであるが、ブロック生成自体が停止してしまう不具合も散見されている。また、本実証では証明書発行組織の鍵を抽象化するためにスマートコントラクトを実装する必要があったが、Symbolは個別にテストされたプラグインを組み合わせることでスマートコントラクトの実行が可能であり安全性にも優れている。

3. 6. 実証実験

実証実験は事前準備、証明書発行、証明書検証の3つのプロセスで行った。今回は有線の実験であるため、本来放送波にあたる部分は、RFケーブルで直結している。ローカルPC間のデータ転送には、簡便化のためにUSBメモリを使用した。

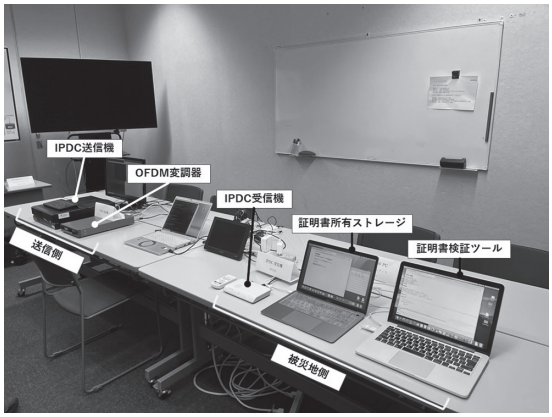

写真1　実証実験の様子

3. 6. 1. 事前準備

災害が発生する前の事前準備として、以下の事項について確認した。

- ボランティアセンターの公開鍵取得
- ブロックヘッダーの同期
- ファイナライズ合意ブロック確認

まず、周知されたボランティアセンターの公開鍵を取得し証明書検証ツールに配置、次に送信機・受信機間でのブロックヘッダーの同期を開始した。

ボランティアセンターの公開鍵はSSL/TLS証明書を付与したHTTPSアクセス可能なドメイン配下に.well-known/keys.jsonを配置し、事前周知した。このページは第三者認証局によって認証された組織の者しか更新することはできず、そのファイルに示された公開鍵で検証できる署名は、組織の決定とみなしても問題ない、と判断することができる。また、ブロックヘッダーの同期は、600以上の公開されたAPIエンドポイントからランダムに5つのエンドポイントを選択し、同期確認のため最新ブロックのハッシュ値を比較してから接続を行った。冗長性確保のため3つのプロセスで同様の処理を行い、ノードへの接続が切断された場合は、自動的にランダムにエンドポイントを再度選択しなおす処理で安定的なブロックヘッダーの同期を行った。IPDCの送信は定期的にまとめて行い、すでにロールバック前の情報をIPDCで送信してしまっている場合は、再度同じブロック高のブロックヘッダーを送信した。

また、受信機側ではファイナライズ合意ブロックに至る範囲までのブロックヘッダーを蓄積しておき、平常時に定期的にブロックチェーンへアクセスを行い、受信ブロックと比較し、ファイナライズ合意ブロックの更新を行った。

3. 6. 2. 証明書発行

ボランティアセンターによる証明書を作成した。証明書の本文はパブリックブロックチェーンに記録するので、情報漏洩のリスクを避けるために個人情報は記載せずに番号などを記録する。個人情報と紐づけが必要な場合は暗号化するか、あるいは添付ファイルの要約値をブロックチェーンに追記して、添付ファイル本体はオフラインで検証者に提示するなどの工夫が必要である。しかし、秘匿方法についてはユースケースに応じてさまざまな方法があるので、本実証においては実施していない。まず、証明書発行ツールに証明書本文を記入して、ブロックチェーンにマルチシグで発行担当者が署名して登録した。ブロックチェーンへの登録が完了した後、証明書と所有者情報をダウンロードして証明書所有ストレージにUSBメモリで転送した。なお、本実証では所有者情報はボランティアセンターが新規に発行したアカウントをパスワードで暗号化してボランティアスタッフに渡したが、DIDsの観点からボランティアスタッフが自身で作成した所有者情報に対して、発行者が証明書の授与対象者にその情報を記載してもよい。

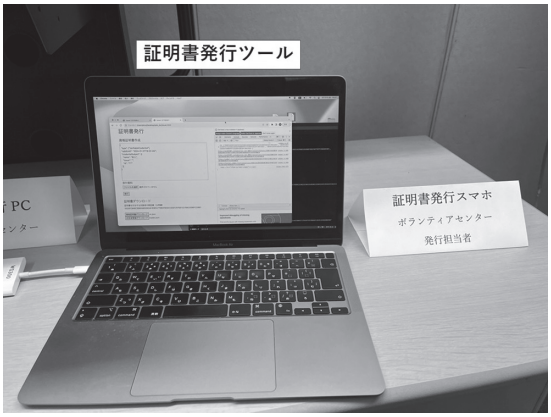

写真2　証明書を発行してボランティアスタッフに渡す

3. 6. 3. 検証

ボランティアスタッフは対面で被災現地監督者からPIN番号の通知を受け、証明書所有ストレージを使用してそのPIN番号の署名結果を提示者情報として出力した。次に、その提示者情報と証明書を被災現地監督者の証明書検証ツールにUSBメモリでコピーした。さらに、証明書のマークルツリーが指定するブロックヘッダーを受信機から取得、事前に取得していたボランティアセンターの公開鍵情報とあわせて検証を行った。また、被災現地監督者は受信機に蓄積されていたブロックヘッダーを一括で取得し、最新ブロックからファイナライズ合意ブロックまでの整合性を確認した。

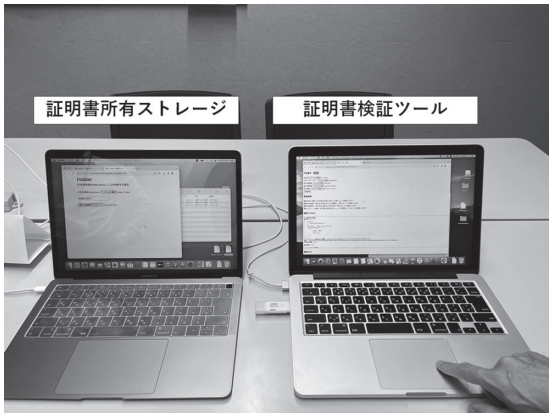

写真3　証明書検証ツールに必要なデータを集める

3. 7. 結果

実証実験の実施結果について、正常系と異常系に分けて説明する。

3. 7. 1. 正常系

ブロックヘッダーの同期について、24時間におよぶ同期の中で60回のロールバックが発生したが、受信機にて蓄積されたブロックヘッダーは問題無く実証実験開始時に起点として定めたファイナライズ合意ブロックまで整合性を確認することができた。また、インターネットとの接続を完全に遮断したPCに証明書をUSBで転送し、事前に与えられた情報と受信したブロックヘッダーのみで、証明書の真正性、発行組織、提示者の本人確認を実施することができた。さらに、分散管理されている発行組織の署名鍵の構成を変更して新規に発行担当者の秘密鍵を追加しても、信頼性検証が正しく行えることを確認した。

3. 7. 2. 異常系

異常系の検証として、証明書の内容を書き換える、周知済み発行組織の公開鍵を変更する、所有者の鍵を差し替える、PIN番号を間違える、異なるブロックヘッダーを使用する、などの状況下で検証を行った場合、証明書検証ツールで異常（検証失敗）として検知することができた。また、発行担当者をマルチシグから除外した後に証明書の発行手続きを行ったところ、除外した発行担当者がブロックチェーンへ証明書を記録することはできなくなった。

3. 8. 考察

今回の実証実験の設計あるいは実装中に浮上した懸念事項について、今後の課題として検討したい。

放送休止時などに生成されたブロックヘッダーなどはリアルタイムに送信することができず、送出タイミ

ングについては別途考慮が必要である。また、発行済みですでに被災地に持ち込まれた証明書の内容を訂正したい場合、被災地内から更新情報の検証は困難であるため、別途IPDCを使用して訂正情報を送出するなどの対策が必要である。さらに、証明書の秘匿化については注目・期待している企業も存在し、どのような実装にすれば汎用性が高いかユースケースを洗練させながら見極めていく必要がある。加えて、ブロックチェーンがロールバックすることを考慮して、放送波でファイナライズを待って送出すべきか、あるいは受信機側での再検証を必須とすべきかなど、放送として扱うデータの速報性・完全性の優先度について検討したい。

4. ハイブリッドインフラへの提言

実証実験の結果、インターネットが使えない被災地において放送波と同等の送受信設備により、現地に持ち込まれた証明書の信頼性を検証することができた。IPDCを用いてブロックチェーンに記録された信頼性検証のための情報をエリア一帯に共有する本手法は、災害等の有事だけではなく平常時においても利用価値のある放送と通信のハイブリッドインフラを実現できると考える。Beyond 5Gやトラステッドウェブなどさまざまなキーワードで通信の未来が語られるなか、放送の特性を活かした情報伝達手段を組み合わせることで実現するハイブリッドインフラがどのような課題を解決するのか検証してみたい。

4. 1. 共有リソースの動的割り当て

従来のDBシステムとブロックチェーン技術の大きな違いは、RWA(Real World Asset:現実資産）など、競合他社間で共有するリソースのシェアを実現できる点にある。十分に分散されたパブリックブロックチェーンを使用すれば記録されたデータは合意に基づいた書き換えしか許可されない。従来システムでも実現不可能ではないが、競合他社間での合意をまとめ上げるためには、より規模の大きなシステムインテグレータの仲介が必要となり、その開発規模は莫大に跳ね上がる。さらに、IPDCによりリソース割り当ての変更情報が共有されれば、たとえばエリア一帯に張り巡らされた信号機に対して気象やマーケットなどの状態変更に応じた割り込みや時間帯によっての交通制御変更などが可能になる。そして、対象となる機器が数億台に増えたとしても、現在の電波が受信可能な状況であれば基地局の増設などは必要なく、現状と同じ送信コストで制御することが可能である。また、パブリックブロックチェーンは記録されたデータを誰でも監査可能なのでセンサーや取引信用保険などを組み合わせることで、記録された情報を元にコンプライアンス遵守を条件とした融資や補償を伴う経済活動を行うことが可能であると考える（図14）。

4. 2. 分離されたネットワーク上での合意確認

現在、インターネットはグローバルで単一のネットワークとして機能している。しかしながら、今後さらに大容量で低遅延のストリーミングデータが求められると従来の転送方式ではいずれ限界が来ると考えられており、ICN(Information-Centric Networking：情報指向ネットワーク）など、インターネットとは異なるプロトコルのネットワークが広がりを見せる可能性がある。関係者間で主として使用するネットワークが異なっていたとしても、双方共に信頼性を検証できる情報を根拠に価値を伴う情報の交換が行われるべきで

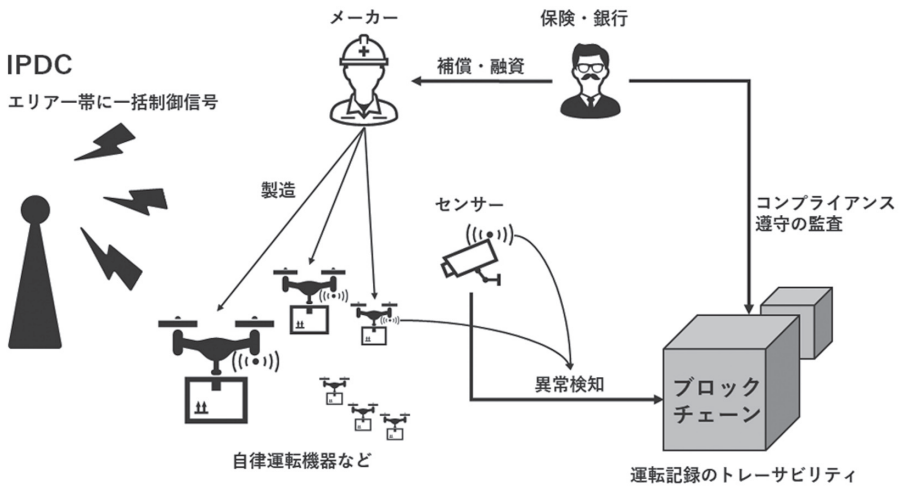

図14　リソースの割り当てと自動運転の監視

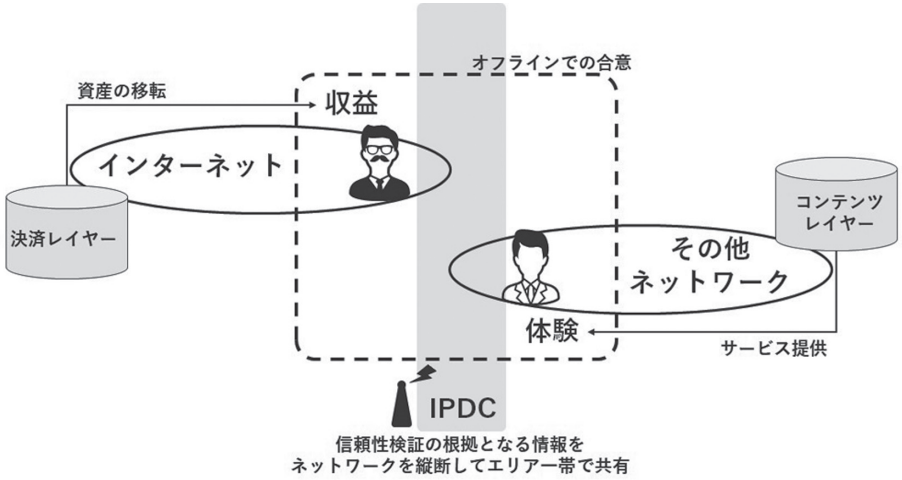

図15　マルチネットワーク間での合意形成

あり、特定のネットワークに依存すべきではない。合意形成された情報が放送波により受信可能であれば、取引の当事者は複数のネットワークに接続する必要なく、合意結果と検証手段のみを入手すればその情報を元に取引を開始することができ、さらに複雑なマルチネットワーク上でのインターオペラビリティ（相互運用性）構築に貢献することができると考える（図15）。

さいごに

今回の実証実験を実運用していくには一企業だけでは実施できないため、多くの賛同者を得ながら実現していきたいと考える。本稿の取り組みは、Inter BEE 2023で展示予定であり、本稿でも書ききれないユースケースも盛り込んで説明しようと思っているので、ぜひ株式会社アトラクターのブースをご訪問いただきたい。最後に本実証実験において、尽力いただいた株式会社アトラクター殿にこの場を借りて深く感謝申し上げる。

【参考文献】

New directions in cryptography
https://www-ee.stanford.edu/~hellman/publications/24.pdf

Internet X.509 Public Key Infrastructure　Certificate and Certificate Revocation List (CRL) Profile
https://www.ietf.org/rfc/rfc5280.txt

Digital Video Broadcasting (DVB);
IP Datacast over DVB-H: Architecture
https://www.etsi.org/deliver/etsi_tr/102400_102499/102469/01.01.01_60/tr_102469v010101p.pdf

FLUTE - File Delivery over Unidirectional Transport
https://www.ietf.org/rfc/rfc6726.txt

Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf

Account abstraction Ethereum
https://ethereum.org/en/roadmap/account-abstraction/

Symbol Technical Reference
https://symbol.github.io/symbol-technicalref/main.pdf

Decentralized Identifiers (DIDs) v1.0
https://www.w3.org/TR/did-core/

Verifiable Credentials Data Model v2.0
https://www.w3.org/TR/vc-data-model-2.0/

Information-Centric Networking (ICN) Research Challenges
https://www.ietf.org/rfc/rfc7927.txt