

災害時のスマートフォン上の属性証明機能分析 — STAMP/STPA を用いた安全性分析 —

中野 幸子^{1,*} 金子 朋子¹

概要：2025年6月より、マイナンバーカードの属性証明機能と電子証明書機能がiPhoneに搭載され、物理カードを用いずに本人確認や行政手続が可能となった。本研究の目的は、このスマートフォン上の属性証明機能を、災害時の避難所運営に活用することを想定し、その安全性と運用上のリスク分析を行うことである。分析対象とするのは、避難者がiPhoneを用いて自身の属性情報を提示し、受付職員がPoCシステムに登録までの一連のプロセスである。分析にはSTAMP/STPAを用い、アクシデント・ハザード・安全制約を整理し、UCAおよびHCFを抽出した。その結果、Face IDが使用できない状態での認証失敗、情報登録ミスといった具体的なリスク要因が確認された。この一連の分析により、災害時にスマートフォンで属性証明を行う仕組みを実際に活用するための課題の明確化を行う。

キーワード：STAMP/STPA, マイナンバー, 事故分析, システム理論

Analysis of Smartphone-Based Attribute Certification in Disasters: A Safe and Secure Analysis Using STAMP/STPA

Sachiko NAKANO^{1,*} Tomoko KANEKO¹

Abstract: In June 2025, the My Number Card's attribute certificate and electronic certificate functions became available on iPhones, enabling identity verification and administrative procedures without a physical card. This study evaluates the safety and operational risks of using this smartphone-based attribute certification in disaster shelter operations. Focusing on the process whereby evacuees present their attribute information via iPhone and staff register it using a PoC system, the analysis applies STAMP/STPA to identify accidents, hazards, and safety constraints, and to extract Unsafe Control Actions (UCAs) and Hazardous Control Factors (HCFs). Key risk factors identified include failed authentication when Face ID is unavailable, misidentification, and information registration errors. This analysis clarifies practical issues that must be addressed to ensure the reliable use of smartphone-based attribute certification in emergency contexts.

Keywords: STAMP/STPA, My number, Accident Analysis, System Theory

1. はじめに

2024年12月に健康保険証がマイナンバーカードと一体化し、翌年3月には運転免許証の一体化が施行されるなど、マイナンバーカードの利用範囲が拡大しつつある。加えて、政府はマイナンバーカードの主要機能である①電子証明機能および②属性証明機能をスマートフォンに搭載するサービスを開始した。2023年5月からAndroid端末で電子証明機能の利用が可能となり、2025年6月24日にはiPhoneでも両機能の提供が始まった。これにより、物理的にカードを携帯せずに本人確認が可能となり、スマートフォンが日常生活における不可欠な認証手段となりつつある。

こうしたデジタル技術の進展に伴い、災害時の活用に向けた実証実験も進められている。2024年度には、石川県においてマイナンバーカードを活用した避難所での本人確認・支援判断に関する技術検証が実施された[1]。災害時における活用例としては、①避難所の入退所手続き、②入所

後の属性登録、③行政サービスの受領、④診療・薬剤情報の取得などが想定されており、避難支援業務の高度化・効率化が期待されている。これらの実証は物理カードを前提としていたが、現実的にはカードを携帯していないケースも多く、今後はスマートフォンにカード機能が搭載されている場合の対応も想定する必要がある。

特に大規模災害時には、避難所の運営や物資配布、安否確認といった場面において、被災者の氏名、住所、生年月日などを迅速かつ正確に把握することが求められる。しかし、災害時には通信の断絶や電源の喪失、職員のITスキル不足などが伴う。そのため、スマートフォンによる属性証明の活用においても、リスクを事前に分析し、安全な運用体制を構築することが重要である。

本研究では、スマートフォンに搭載された属性証明機能を用いて、災害時に避難所で属性証明を行うプロセスに着目し、そこに内在する構造的なリスクと運用上の制約を明らかにする。分析には、システム理論に基づくリスク分析

¹創価大学
Soka University

* e24m5312@soka-u.jp

手法である STAMP/STPA（System-Theoretic Accident Model and Processes / System-Theoretic Process Analysis）を用い、安全な活用方針の検討を行う。対象とするシナリオは首都圏における地震災害を想定し、避難所運営の場面を中心とする。本研究は、災害対応におけるスマートフォン型マイナンバーカード活用の可能性と限界を明らかにし、安全性向上に向けた知見を提供することを目的とする。

2. 関連知識

2.1 マイナンバーカードのスマートフォン搭載

マイナンバーカードは、公的身分証明書であり、主に「電子証明書機能（公的個人認証サービス）」と「属性証明機能（カード代替電磁的記録）」の2つの機能を備えている[2]。

電子証明書機能には、電子署名および電子認証の機能があり、「署名用電子証明書」と「利用者証明用電子証明書」の2種類がカード内に格納されている。一方、属性証明機能では、氏名、生年月日、性別、住所のいわゆる「基本4情報」に加え、マイナンバーおよび顔写真のデータを格納し、これらの情報を読み取って本人確認に用いることができる。たとえば、スマートフォンを用いてマイナポータルにログインする際には、電子証明書機能を用いて本人であることを確認し、その上でマイナンバーカードを読み取って上記の券面記載事項（以下属性情報）を提供することで、さまざまな行政手続きが可能となる。

これらの機能をスマートフォンに直接搭載する取り組みが進展し、2023年5月にはAndroid端末における電子証明書機能の搭載が開始された。さらに2025年6月24日からはiPhoneでも電子証明書機能および属性証明機能の両方が利用可能となった。これにより、物理的にマイナンバーカードを携帯しなくとも、各種行政サービスの利用や本人確認が可能となる環境が整いつつある。

スマートフォンによる公的個人認証や本人確認は、従来必要であったICカードリーダーを用いずに本人確認を行えるため、利用者にとっての利便性が高く、今後の普及が期待されている。このような技術は日常の行政手続きのみならず、災害時や緊急時の迅速な本人確認手段としても大きな可能性を秘めている。

2.2 災害対応におけるマイナンバーカードの実証事例

2023年度には、神奈川県においてデジタル庁主導のもと、マイナンバーカードの災害時利用に関する実証実験が行われた[1]。2023年10月23日には、第一回実証実験が行われた。広域災害を想定し、避難所情報を連携するシステムが構築され、避難者がマイナンバーカードや交通系ICカードを提示することで基本情報を避難所運営システムに自動入力する仕組みが検証された。その結果、手書きによる手続きと比較して約9割の業務削減効果が見られ、災害対策本部への報告業務も約50%の業務削減が期待できるとされた。2024年2月28日に行われた第二回実証実験では、

第一回の検証を踏まえ、顔認証付き本人確認装置の利用や、マイナンバーカード搭載スマホの利用実験も行われた。

2024年度には、能登半島地震を踏まえた実証実験が石川県で実施された。この実証では、医療機関や福祉機関との情報連携、物資管理、安否確認などの多機能アプリ群とマイナンバーカードの連携が検証された。また、Starlinkや可搬型バッテリーによる通信・電源確保といった実用的条件下でも、避難所業務の効率化が確認されている。

これらの実証は、いずれもマイナンバーカードの物理的携帯を前提としていたが、今後はカード機能搭載スマートフォンの活用が求められる。とりわけ通信や電源の制約下において、スマートフォンによる属性証明がどのようなリスクを抱え、安全に運用できるかについての構造的な検討が必要である。

2.3 マイナンバーカード対面確認アプリ

デジタル庁は、マイナンバーカードのICチップを読み取り、格納された氏名などの本人情報を確認するためのアプリを2024年8月にリリースしている[3]。主な機能として、情報の読み取り表示機能と履歴機能を備えている。このアプリは、飲食店での年齢確認や、自治体窓口での本人確認、金融機関や携帯電話の契約のための本人確認などの利用が考えられている。なお、2025年7月31日現在の対面確認アプリはマイナンバーカードの直接読み取りに対応しているが、デジタル庁は2025年7月中旬に「iPhoneのマイナンバーカード」にも対応することを発表している。現状のアプリでは、物理カードに記載されている顔写真と、読み取りをしようとしている本人の顔を職員が確認することで、なりすまし防止などの観点も含め本人確認を行なっていると推察するが、今後iPhoneのマイナンバーカードに対応した場合、どのように整合性を保つかは現時点では不明になっている。

3. 研究目的と分析手法

3.1 研究目的

本研究は、スマートフォンに搭載されたマイナンバーカードの属性証明機能が、災害時の避難所における本人確認手段としてどのように機能しうるかを明らかにし、その安全性と運用上の課題を評価することを目的とする。現在までに行われた実証実験では、マイナンバーカードを物理的に携帯していることを前提とした避難所運営が検討されているが、スマートフォンへの搭載が進んだ現状においては、カードを携帯しないまま被災したケースや、スマートフォンによる提示が必要となる場面も想定される。そのような状況下で、スマートフォンによる本人確認が円滑かつ安全に機能するためには、その運用プロセスに内在する構造的リスクをあらかじめ明らかにし、適切な制御・対策を講じる必要がある。

3.2 分析手法



図 1 : STAMP/STPA 分析の手順

本研究では、特に災害発生直後の避難所入所における属性証明プロセスに着目し、スマートフォンを用いた本人確認がどのような構造で機能し、どのような障害・ハザードが生じうるかをシステム的観点から分析する。上記の目的を達成するために、本研究では STAMP/STPA (System-Theoretic Accident Model and Processes / System-Theoretic Process Analysis) を用いてリスク分析を行う。STAMP は、従来の故障原因中心のリスク分析手法とは異なり、事故や障害を「不適切な制御」によって引き起こされるものと捉えるシステム論的アプローチである。その応用手法である STPA では、システム全体のコントロール構造を明確化した上で、Unsafe Control Actions (UCA : 不適切な制御行動) を抽出し、その背景にある Hazardous Control Factors (HCF : 因果要因) を特定していくことで、潜在的なリスクとその対策を体系的に導出できる。分析手順は、図 1[4]のように進め、導出された HCF の中から主要な対

策の例を示す。

3.3 分析シナリオ

本研究で想定するシナリオは、首都圏において大規模地震が発生し、被災者が避難所へ避難してくる状況を想定する。なお、分析対象とする端末は、属性証明機能が施されている iPhone に限定し、Android 端末との機能差異は考慮しない。被災者は、スマートフォンに搭載されたマイナンバーカード機能を用いて自身の属性情報を提示し、避難所の受付担当者（職員またはボランティア）がその情報をもとに入所手続きを行う。受付担当者が、被災者の情報を読み取る端末では、2.3 章に記載のマイナンバー対面確認アプリを使用することとし、被災者は iPhone のマイナンバーカードを使用することとし、受付側は、マイナンバー対面確認アプリを使用できる iPhone と、受付端末として使用されている IC カードリーダーを使用する。アプリから読み取った情報が PoC システムに入力されることで、避難所への入所及び支援を受け付けられる。

また、本研究では以下のようないくつかの前提条件を設ける。

- スマートフォン(iPhone)に属性証明機能が正常に搭載されている
- 通信環境は一部断絶しているが、一部の避難所では非常用通信手段が確保されている
- 職員は必ずしも IT に精通していない
- 災害による混乱や不明瞭な判断基準が存在している
- 対象端末は iPhone に限定し、Android 等他端末との違いは考慮しない

これらの条件下で、スマートフォン属性証明が正常に機能しないリスクや、誤った判断が下されるリスクがどこに潜んでいるかを分析対象とする。

4. 分析内容

4.1 準備 1 アクシデント等の抽出

Step0 では、STAMP/STPA の分析枠組みに基づいて、損失に関連するシステムとハザードを明らかにし、ハザード

表 1 : アクシデント・ハザード・安全規約の一覧

| アクシデントID | アクシデント | ハザードID | ハザード | 安全制約ID | 安全制約 |
|----------|------------------------------------|--------|----------------------------|--------|------------------------------------|
| A1 | 被災者の属性証明ができず、避難所の入所受付および支援が適切に行えない | H1 | 職員・被災者ともに正しく属性を提示・読み込みできない | SC1 | 職員・被災者ともに正しく属性を提示・読み込める状態でなければならない |
| A1 | 被災者の属性証明ができず、避難所の入所受付および支援が適切に行えない | H2 | 本人以外が属性証明できる状態である | SC2 | 本人以外は属性証明できない状態でなければならない |
| A2 | 他人の属性情報が登録される | H3 | 登録済みの属性情報が上書き・重複登録されている | SC3 | 登録済みの属性情報は上書き・重複登録されなければならない |
| A2 | 他人の属性情報が登録される | H2 | 本人以外が属性証明できる状態である | SC2 | 本人以外は属性証明できない状態でなければならない |
| A3 | 属性情報が漏洩する | H4 | 意図しない第三者が属性情報を確認できる | SC4 | 属性情報は意図しない第三者に提供されなければならない |
| A3 | 属性情報が漏洩する | H2 | 本人以外が属性証明ができる状態である | SC2 | 本人以外は属性証明できない状態でなければならない |

に関連したシステムの安全制約やシステム要求を明らかにし、安全コントロールストラクチャー図を書き出す。

まず、アクシデントとは、本来避けるべき望ましくない結果であり、本研究では3つを定義した。次に、これらのアクシデントを引き起こす危険な状態（ハザード）を4つ定義し、これらのハザードを回避するための安全制約を4つ定義した。表1にアクシデント、ハザード、および安全制約の対応関係を示す。

4.2 準備2 安全コントロールストラクチャーの構築

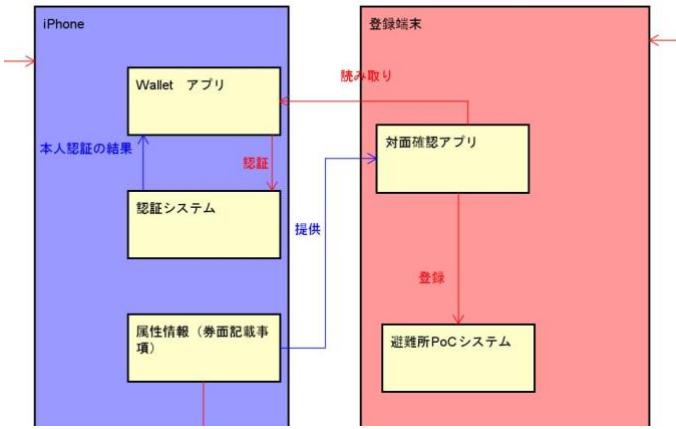


図2：コントロールストラクチャー図（CS図）の抜粋

準備2では、ハザードを制御し安全制約を課すよう整備された安全コントロールストラクチャーを図(以下CS図)として示し、システム全体のモデル化を行う。被災者はWalletアプリ上でマイナンバーカードが登録されていることが前提であり、対面確認アプリにiPhoneをかざすとFace IDによって本人認証を行った上で、属性情報の提示が許可される。提示された情報は、受付担当職員が対面確認アプリまたは支援端末を用いて読み取り、避難所PoCシステムに登録される。

4.3 Step1 UCAの抽出

Step1では、STAMP/StPAの手法に基づき、5つの制御行

動（CA）に対してUCA（不適切な制御行動：Unsafe Control Actions）を抽出した。その結果、操作の不実行、誤認証、誤読み取り、重複登録など、計13のUCAが特定された。

特に、認証が正しく行われない場合（UCA2-N-1）、本人以外が属性証明を提示できるリスク（UCA2-P-2）、属性情報が誤って読み取られたり、重複登録されるケース（UCA4-P-1、UCA4-D-1）が顕著であり、災害時におけるシステム運用の信頼性を損なう要因となる。詳細は、表2に表す。

4.4 Step2 HCFの特定

Step2では、各UCAに対してStPAに基づくHCFの抽出を行った。HCF（Hazardous Control Factors）とは、Unsafe Control Action（UCA）がハザードに結びつく原因となる要因を指し、システム構造や運用環境に内在するリスクを構造的に明らかにするものである。

代表的な例として、まずバッテリー残量の低下により被災者側ではWallet機能が利用できず、本人認証が失敗する要因が挙げられる。受付側の端末の電源がなくなった場合も、読み取りができなくなる。これは災害時における端末電源の制約に関するもので、認証機構の確実性に影響を及ぼす。特に、Wallet機能に関して、Bluetoothの使用が求められており、バッテリーを減らす要因にもなっている。デジタル庁が述べている通り[3]、インターネットに接続できる場所でのみ機能するため、災害時の一時的な通信断絶環境下での使用は困難になると予測される。

さらに、PoCシステムへの登録操作が失敗し、属性情報が記録されないまま手続きが終了するケースも抽出された。

以上のように、各UCAに対して抽出されたHCFは、避難所における属性証明プロセスにおいて特定の誤動作や不備がハザードにつながる可能性を示している。

最後に、これらのHCFが発生する原因として考えられるシナリオを発想し、各シナリオに特化した対策を表3のようにまとめた。

表2：UCAの一覧

| No | CA | From | To | CA提供条件 | Not Providing | Providing causes hazard | Too early / Too late | Stop too soon / Applying too long |
|----|------|------------|------------|-------------------------|----------------------------|--------------------------------------------------|------------------------------------------|----------------------------------------------|
| 1 | 操作 | 被災者 | iPhone | | | (UCA1-P-1) 登録されているマイナンバー情報が本人のものではない [SC2] | | |
| 2 | 認証 | Wallet アプリ | 認証システム | Face ID / Touch IDによる認証 | (UCA2-N-1) 正しく認証されない [SC1] | (UCA2-P-1) 登録されているマイナンバー情報が本人のものではない [SC2] | | |
| 3 | 読み取り | 対面確認アプリ | Wallet アプリ | 本人認証が完了し、属性情報が表示されている | | (UCA4-P-1) 読み取って他人の情報を読みとる [SC3] | | (UCA4-D-1) 同一情報を読み取り、重複登録される [SC2][SC3][SC4] |
| 4 | 登録 | 対面確認アプリ | 避難所PoCシステム | | (UCA5-N-1) 正常に登録されない [SC1] | (UCA5-P-1) 重複登録が発生する [SC3] | (UCA5-T-1) システム上で未確認のまま誤登録される [SC3][SC4] | |
| 5 | 操作 | 受付担当職員 | 登録端末 | | | (UCA6-P-1) 職員の誤操作により、他人の情報登録や重複登録がされる [SC1][SC3] | | |

4.5 本章のまとめ

本章では、災害時におけるスマートフォンを用いた属性証明プロセスに対して、STAMP/STPA 手法を適用し、シナリオに基づいたアクシデント、ハザード、安全制約、UCA、およびHCFを抽出した。その結果、電源供給や通信環境の不安定性、本人認証における誤操作、情報登録時のヒューマンエラーなど、属性証明の信頼性を損なう複数のリスク要因が明らかとなった。次章では、これらの分析結果をもとに、災害時における属性証明の課題と今後の対策について考察する。

5. 分析結果と考察

5.1 分析結果

本分析では、STAMP/STPA の手順に沿って、災害時において iPhone に搭載されたマイナンバーカードの属性証明機能を用い、避難所で被災者情報の提示・登録などの運営及び災害支援が行われる一連のプロセスを分析した。分析の流れでは、アクシデント、ハザード、安全制約の抽出と、制御構造モデルを構築し、それに基づく UCA および HCF の特定を行った。

準備 1 として、このプロセスにおいて発生しうるアクシデント（事故・失敗事象）として、「属性証明ができず支援が受けられない」「他人の情報が誤って登録される」「属性情報が漏洩する」といった 3 種を想定した（表 1 参照）。それらのアクシデントを引き起こす原因として、「属性情報の提示・読み取りの失敗」「本人以外による認証の成功」「登録済み情報の上書き・重複」「属性情報の第三者への可視化」といった 4 つのハザードを特定した。これらに対応する安全制約として、以下を定義した：(SC1) 職員・被災者とともに正しく属性情報を提示・読み取りできる状態でなければならぬ、(SC2) 本人以外は属性証明できない状態でなければならない、(SC3) 登録済みの属性情報は上書き・重複登録されてはならない、(SC4) 意図しない第三者に属性情報が提供される。

準備 2 として、モデリングを行うことで、どのような仕組みでシステムが動いているかを確認した。

表 3：シナリオ及び対策案の抜粋

| HCFID | HCF | シナリオ | 対策 ID | 対策 | UCA | 対策対象コンポーネント | 備考 |
|------------|----------------------------|-----------------------------------------|-------|-----------------------------|--------------------------------------------|----------------------------|------------------------------------|
| HCF1-P-1-1 | 登録されているマイナンバーカードが本人のものではない | 家族や知人のカードを登録しているなど、意図して他人のカードを登録している | M1 | 本人のみ登録できる形にする | (UCA1-P-1) 登録されているマイナンバー情報が本人のものではない [SC2] | iPhone Wallet アプリ 登録端末 被災者 | 1台のスマホに対して登録できるマイナンバーは一台のみ |
| HCF2-N-1-1 | 認証に失敗する | FaceIDやTouchIDがうまく認証されない | M2 | 生体認証失敗時にパスコードでの認証ができるよう設定する | (UCA2-N-1) 正しく認証されない [SC1] | iPhone Wallet アプリ | 筆者の検証下では、顔認証に失敗すると、その場でエラーになってしまった |
| HCF2-N-1-3 | バッテリー低下で反応しない | スマホのバッテリーが不足している場合、Walletが開かず、認証画面も開かない | M3 | バッテリーがない状態でも認識可能な状態にする | (UCA2-N-1) 正しく認証されない [SC1] | Wallet アプリ 対面確認アプリ 登録端末 | モバイルSuicaは電源低下時でも読み取り可能 |
| HCF2-P-1-1 | 登録されているマイナンバーカードが本人のものではない | 家族や知人など他人のマイナンバーカードが意図した状態で登録されている | M1 | 本人のみ登録できる形にする | (UCA2-P-1) 登録されているマイナンバー情報が本人のものではない [SC2] | iPhone Wallet アプリ 登録端末 被災者 | 1台のスマホに対して登録できるマイナンバーは一台のみ |

Step1 では、各構成要素間の制御関係に着目し、UCA (Unsafe Control Actions) を抽出した。ここでは、「本人以外の情報がスマートフォンに登録されている」「「パスコード認証のなりすまし」「職員が誤って他人の情報を登録してしまう」「重複登録」など、4種の分類に従って、制御構造における不適切な振る舞いを 10 件以上特定した。

Step2 では、これらの UCA に至る背景要因を HCF (Hazardous Control Factors) として分類した結果、特に以下のようない要因がリスクの根源として確認された：

- ①家族や知人のカードを登録しているなど、意図して他人のカードを登録している、②Face ID (顔認証) 失敗時の処理中断③ネットワークの不安定さおよび電源制約による登録処理の中止、④正しい本人確認を挟まずに登録完了する

これらの結果から、スマートフォンによる属性証明機能は一定の利便性と即時性を提供するものの、災害という特殊な状況においては、本人認証の正確性、情報登録プロセスの安定性、運用者の理解と訓練の有無などが、その安全な活用の成否を大きく左右することが示唆された。

5.2 考察

本研究における分析から、スマートフォンに搭載された属性証明機能を災害時に活用する際には、いくつかのリスクが存在することが明らかとなった。特に、以下の点が実装・運用上の重要な論点として浮かび上がった。

①属性情報の読み取りと登録処理の信頼性

属性情報が正しく表示されていても、登録処理の中止や誤操作により、重複登録や誤登録が発生する可能性があり、職員側の操作における教育・訓練の必要性が示唆される。現状のアプリでは、履歴の確認として物理カードの読み取りでは、カードの有効期限およびセキュリティコードが保存される。また、iPhone のマイナンバーカードでは、読み取った情報の一部は履歴として残るが、どのシステムに登録したか、いつ属性情報を提示したかなどの履歴は本人から確認できない。そのため、本人が仮に避難所を移動した際や、確認ができない状況下で本人が誤って重複登録する場合なども考えられた。

特に 2023 年には、公金受取口座の誤紐付けなどさまざまな誤紐付けの問題が発生し、筆者はこれに関する事故分析を行ない[5]、その際の事故原因としても本人確認作業のミスが原因としてあがった。本件に関しては、重複登録や誤登録を防ぐために、カードリーダーで読み取った情報をそのまま反映させるだけでなく、特に入所登録や支援時には名前情報の確認など、本人確認の作業が必要なのではないかと考える。

③通信環境および充電の依存

本プロセスの成立には通信環境および電源の安定供給が前提となっており、これらのインフラが損なわれた場合には、スマートフォンによる本人確認そのものが機能しなくなるリスクがある。4.4 で述べたとおり、たとえば、避難中にスマートフォンのバッテリーが切れてしまう場面では、属性証明機能は利用できなくなる。また、大規模災害によりインターネット接続が不安定になる場面では、属性情報の読み取りができず、システムへの登録が困難になる。ただし、物理カードでの属性証明は、通信環境に影響されずに読み取りを行うこと自体は可能なので、まずはインターネット環境がない状態での提示を可能にすることが求められる。このような技術的前提への依存は、災害対応における公平性や継続性にとって重要な課題である。

また、分析で抽出されたリスクは、単なる技術的不備にとどまらず、倫理的観点からも検討が求められる。たとえば、本人確認に失敗することで被災者が支援を受けられないケースや、パスコード認証の曖昧さにより他者によって属性情報が誤って登録されるケースは、人権やプライバシー、支援の公平性を脅かすものもある。したがって、スマートフォンによる属性証明を実用化するにあたっては、技術・制度・運用・倫理の観点から包括的な設計が求められる。

これらの観点から、スマートフォンによる属性証明の災害時活用においては、利便性の追求と安全性の担保の間で適切な設計判断が求められることがわかる。実装側のシステム設計者だけでなく、運用に関わる自治体や災害対策本部の運用方針に対しても、重要な示唆を与えるものである。

6. まとめ

本研究では、2025 年 6 月より iPhone への搭載が開始されたマイナンバーカードの属性証明機能に着目し、災害時の避難所運営に活用する際の安全性と運用上のリスクについて、STAMP/STPA による分析を通じて評価を行った。具体的には、属性証明の提示・登録におけるアシデント・ハザード・安全制約の整理から始まり、コントロール構造モデルの構築、UCA および HCF の抽出と分類を通して、システムの構造的リスク要因を明らかにした。

分析の結果、顔認証の失敗時の処理中断や、職員による誤登録や情報重複などの具体的なリスクや、避難所という非常日常的かつ不安定な環境においては、通信環境や電源供給といった技術的前提が安全性に直結することも示唆された。これらの分析から、スマートフォンによる属性証明は、災害対応の即時性や利便性を高める一方で、本人性の担保や運用フローの整備といった観点で慎重な設計が求められることが明らかとなった。現時点では、物理カードの携帯も前提としながら災害対策を行わなければならないが、そもそもマイナンバーカード自体義務化されているわけではないため、より実現に時間がかかるかっていると考えられる。[1] の実証実験では、マイナンバーカードやスマートフォン、交通系 IC カードを携帯していなかった場合に、手書き情報を OCR 处理し、デジタルデータ化したものを NFC タイプのホワイトカードに読み込むことで、カードタッチによる災害対策が考えられていた。しかし、物理的なマイナンバーカードを作成しなくとも、いずれスマートフォンのみでカード機能が全て代用できる、もしくはスマートフォン自体が身分証明証になるような時代が来ると期待する。

今後の展望としては、本研究が対象とした避難所入所プロセスに限定せず、災害時に想定される多様な利用シナリオ（例：医療機関での本人確認、支援物資の受け取り、避難者台帳の統合管理等）における属性証明の応用可能性を検討する必要がある。また、2024 年 12 月より施行された健康保険証との一体化を踏まえれば、医療機関での属性確認や保険資格の提示といった新たなユースケースへの対応が求められることになる。これらを含めたより広範な制度設計と技術基盤の整備が、将来的なスマートフォン属性証明の信頼性確保に寄与すると期待される。

7. 参考文献

- [1] デジタル庁，“デジタル技術を用いた災害対策の高度化に関する実証事業”。

https://www.digital.go.jp/policies/disaster_prevention/demonstration-for-digital-response, (参照 2025-08-22).

- [2] デジタル庁, “マイナンバーカード機能のスマホ搭載について”.
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/fcb737a4-07b9-4abd-bdca-34af9c4f71a5/f6f1ad84/20240913_meeting_smartphone_mynumbercard_outline_01.pdf, (参照 2025-08-22)
- [3] デジタル庁, “マイナンバーカード対面確認アプリ”.
<https://services.digital.go.jp/mynumbercard-check-app/>, (参照 2025-08-22).
- [4] 情報処理推進機構, “はじめての STAMP : STPA (実践編)”,
<https://www.ipa.go.jp/archive/publish/qv6pgp00000010x0-att/000059652.pdf>, 2020 年 3 月.
- [5] 中野幸子, 金子朋子, “公金受取口座の誤紐付けに対する安全分析と設計提案” コンピュータセキュリティシンポジウム 2024(CSS2024)