ブロックチェーンネーミングサービスにおける名前衝突が引き起こす誤送金リスクの評価

小林 蒼一朗[1,a)]　伊藤 大貴[1]　渡邉 卓弥[1]　高田 雄太[1]　熊谷 裕志[1]　神薗 雅紀[1]

概要：暗号資産の取引におけるブロックチェーンネーミングサービス（BNS）の利用が進んでいる．BNSを用いることで，ウォレットアドレスの代わりに可読性の高いブロックチェーン上の名前（BN）を利用できるため，誤送金の防止が期待できる．一方で，異なるBNS間の名前衝突という問題が知られており，同一のBNでも意図しないウォレットアドレスに変換されてしまう事象が確認されている．そこで本研究では，BNS間の名前衝突による誤送金リスクを検証し，その影響を明らかにする．具体的には，複数のBNSに同じBNを登録して意図的に名前衝突を発生させた状況下で，ウォレットアプリおよびBNSプロバイダが提供する拡張機能を用いて名前解決の挙動を調査した．その結果，接続ブロックチェーンに依存しない名前解決や，名前解決後のアドレスの省略表示といった問題を特定し，現実的な誤送金リスクがあることを明らかにした．そして，誤送金を誘発する現実的な脅威モデルについて，SNSアカウントのなりすましや偽装アドレスの作成という観点から検討した．本研究の結果を踏まえ，誤送金のリスクを低減させるためにウォレット開発者，BNSプロバイダおよびユーザに向けて対策を提言する．

Risk Analysis of Misdirected Payments Caused by Name Collisions in Blockchain Naming Services

Soichiro Kobayashi[1,a)]　Daiki Ito[1]　Takuya Watanabe[1]　Yuta Takata[1]　Hiroshi Kumagai[1]
Masaki Kamizono[1]

Abstract: The use of Blockchain Naming Services (BNS) in cryptocurrency transactions has been increasing. By utilizing BNS, users can replace wallet addresses with human-readable blockchain names (BNs), which is expected to reduce the risk of misdirected payments. However, a known issue is name collisions across different BNSs, where the same BN may be resolved to an unintended wallet address. In this study, we examine the risk of misdirected payments caused by name collisions between BNSs and clarify their impact. Specifically, we intentionally registered the same BN across multiple BNSs to cause name collisions, and investigated the behavior of name resolution using wallet applications and browser extensions provided by BNS providers. Our results reveal issues such as name resolution that is independent of the connected blockchain, and truncated display of resolved addresses, both of which present a realistic risk of misdirected payments. We also discuss practical threat models that could induce such payments, focusing on impersonation of social media accounts and the generation of spoofed addresses. Based on these findings, we propose countermeasures for wallet developers, BNS providers, and users to mitigate the risk of misdirected payments.

1. はじめに

ブロックチェーン技術の進展および社会的関心の高まりにより，暗号資産をはじめとする分散型アプリケーション（DApps）の利用が拡大している．中でも，暗号資産の取引においては，ユーザが長く複雑なウォレットアドレスを直接入力・管理する必要があることから，誤送金の問題や，可用性およびユーザビリティの観点で課題が指摘されてきた．このような背景の下，ブロックチェーンネーミングサービス（BNS）と呼ばれる技術が注目を集めている．

[1] デロイト トーマツ サイバー合同会社，Deloitte Tohmatsu Cyber LLC
[a)] soichiro.kobayashi@tohmatsu.co.jp

BNS は，ブロックチェーン上のウォレットアドレスやスマートコントラクトアドレス，IPFS ハッシュなどに対して，人間にとって読みやすい `alice.eth` や `bob.bnb` といったブロックチェーンネーム（BN）を付与し，それらを対応するアドレスのエイリアスとして利用可能にする仕組みを提供する．BN はトップレベルドメイン（TLD）とセカンドレベルドメイン（SLD）に大別され，ユーザは複雑な 16 進数のアドレスを記憶・入力する代わりに，可読性の高い BN を使って暗号資産の送受信等を行うことが可能となる．なお本研究では，TLD（例：`.eth`）とその配下にユーザが登録した任意の名前（例：`alice`）を結合した BN（例：`alice.eth`）を SLD と定義する．

代表的な BNS には，Ethereum Name Service (ENS) [1], Unstoppable Domains (UD) [2], Handshake (HNS) [3], Freename (FNS) [4] などがあり，それぞれ異なるブロックチェーン基盤や管理方針に基づいて運用されている．ENS や UD が，`.eth` や `.crypto` 等あらかじめ TLD が固定された BNS であるのに対し，HNS のようにユーザが任意の TLD を登録できる BNS も存在する．著名な組織名や `.com` 等の ICANN 管理の TLD 登録には一定の制限があるものの，TLD 登録可能な BNS はより中央集権的要素が排除されたサービスといえる．

これらの BNS は暗号資産や Web3 サービスにおけるユーザ体験の向上に寄与する一方で，分散型管理に由来する問題も抱えている．各 BNS プロジェクトは独立して名前空間を管理しており，中央集権的な調整機関が存在しないため，異なる BNS 間で同一の BN が登録される「名前衝突」の問題が発生している [5]．具体的には，特定の BN がある BNS ではアドレス A を指す一方で，別の BNS ではアドレス B を指すという事象が発生している．このような名前衝突は，ウォレットアドレスの打ち間違えではなく BNS の仕組み上の問題に由来する，誤送金やなりすましといったセキュリティリスクを引き起こす可能性がある．

我々の過去の研究をはじめ，セキュリティ上の問題として名前衝突やドメインの悪用といった観点で BNS に着目した研究が進められている [6], [7], [8], [9]．一方で，これらの先行研究は，特定の BNS 内における BN の登録状況や名前衝突状況に関する多角的な調査であり，名前衝突の悪用シナリオの検討やリスク評価までは実施されていない．

そこで本研究では，暗号資産取引時における BNS の名前衝突が実際にどのような影響を及ぼすか明らかにすることを目的とする．具体的には，主要ウォレットアプリである MetaMask [10] 上で名前解決可能な HNS や FNS 等の BNS を対象に，名前衝突の実態を調査した．また，ユーザが実際に誤送金やなりすましの被害を受ける可能性について，名前衝突発生時におけるウォレットアプリの名前解決時の挙動確認や，SNS アカウントのなりすましといった脅威モデルを通じて評価した．本研究の貢献は以下のとおりである．

- MetaMask に対応した複数の BNS において，同一の SLD を登録して意図的に名前衝突を発生させ，ウォレット上における名前解決の挙動を調査する．その結果として，ウォレット本体および名前解決を実行する拡張機能のいずれにおいても，送金先 SLD の衝突に関する対策が施されていないことを明らかにし，誤送金リスクが現実的であることを示す．
- 誤送金を引き起こす脅威モデルを検討する中で，SNS アカウントのなりすましや偽装アドレスの生成に着目し，悪意ある名前衝突を利用した誤送金が誘発されるリスクがあることを示す．
- 名前衝突による誤送金リスクを低減させるために，ウォレットアプリ開発者，BNS プロバイダ，ユーザの三者に向けた提言を，本研究の調査結果をもとに示す．

2. 背景

2.1 ブロックチェーンネーミングサービス

ブロックチェーンネーミングサービス（BNS）は，ブロックチェーン上で人間にとって可読性の高い名称をアドレス等に紐付ける分散型ネーミングサービスである．BNS を利用することで，従来のように複雑な 16 進数形式のウォレットアドレスを直接入力することなく，可読性の高い文字列を使用してトランザクションを実行できる．この仕組みにより，暗号資産取引や Web3 アプリケーション利用時のユーザビリティが大幅に向上するとともに，入力ミスによる誤送金などのリスクも軽減される．

BNS には大きく分けて 2 つのタイプが存在し，それらの一例を表 1 に示す．ひとつは，特定の TLD 配下の SLD を登録できるタイプであり，ENS [1] や UD [2]，SPACE ID [11]，ONEID [12] などがこれに該当する．これらは，BNS プロバイダ側が定めた TLD 配下の SLD を登録し，ウォレットアドレスなどと紐付けて利用する方式である．もう一方は，TLD そのものをユーザが自由に登録・所有できるタイプであり，HNS [3] や Decentraweb [13]（DWEB），Freename [4] などがこの方式を採用している．これらのサービスでは，DNS におけるルートゾーンのような構造をブロックチェーン上に展開しており，ユーザが任意の文字列を TLD として登録し，その下に独自のドメイン空間を構築できる．また，基本的に ENS の `.eth` や UD の `.crypto` といったの著名な TLD は，著名な組織名や ICANN 管理の TLD などと同様に登録が制限されている．

HNS や FNS のような TLD 登録可能な BNS では，複数の BNS が互いに独立した名前空間を管理しているため，異なる BNS 間で同一の TLD，およびそれに紐づく同一の SLD が登録される，名前衝突が発生する可能性がある．たとえば，ある BNS においてユーザ A が `.wallet` 配下の `example.wallet` という SLD を登録した場合でも，別の

表 1: 各 BNS の特徴の比較

サービス名	ENS	HNS	UD	DWEB	SPACE ID	FNS	ONEID
公開時期	2017	2018	2019	2021	2022	2022	2023
ブロックチェーン	Ethereum	Original	Ethereum, Polygon	Ethereum, Polygon	Ethereum, BSC, Story 他	Base, BSC, Polygon 他	Viction
サービス上で利用可能な TLD	`.eth`	ユーザが登録した任意の TLD	`.crypto`, `.wifi`, `.wallet` 他	ユーザが登録した任意の TLD	`.bnb`, `.eth`, `.floki` 他	ユーザが登録した任意の TLD	`.c98`, `.hodl`, `.boss` 他
MetaMask Snaps の提供有無	✓	✓	✓	–	✓	✓	✓

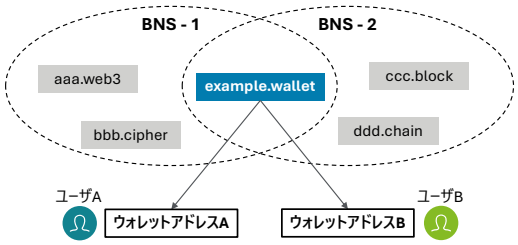

図 1: 名前衝突した SLD の解決先アドレス

BNS においてユーザ B が `example.wallet` を登録してしまう可能性がある．このような状況下では，同じ SLD にもかかわらず，その名前解決結果が BNS やウォレット環境ごとに異なるという問題が生じる．この名前衝突は，ウォレットアドレスの打ち間違えではなく BNS の仕組み上の問題に由来する暗号資産の誤送金やなりすましといったセキュリティリスクを引き起こす要因となり得る．

2.2 MetaMask

MetaMask [10] は，Ethereum をはじめとする EVM 互換ブロックチェーンに対応した代表的な暗号資産ウォレットであり，Web ブラウザの拡張機能やモバイルアプリとして広く利用されている．ユーザは MetaMask を通じて，ウォレットアドレスの生成・管理，トークンの送受信などを実行でき，Web3 エコシステムにおける主要なインターフェースの一つとして位置づけられている．

従来の MetaMask はウォレット機能に特化していたが，2023 年に「MetaMask Snaps」と呼ばれる拡張機能の仕組みが導入された [14]．Snaps を利用することで，Solana 等の EVM 互換ではない L1 ブロックチェーンへの対応，トランザクション署名のカスタマイズといった多様な拡張が可能である．Snaps は MetaMask 本体とは独立して開発・配布されるため，多様な拡張性とユーザ主導の機能選択が実現されている．執筆時点では，Snaps はブラウザ拡張機能にのみ対応しており，モバイルアプリでは非対応である．

MetaMask 本体は ENS にのみ標準対応しているが，Snaps により他の BNS にも対応できる．例えば，UD や FNS などはそれぞれ独自の Snap を提供しており，ユーザはこれをインストールすることで，MetaMask 上で特定の BNS の名前解決が可能となる．なお，表 1 中の BNS のうち，DWEB のみ Snap を提供していない．また，HNS の TLD を持つ SLD について，HNS TLD のオーナーがステーキングした場合にのみ，HNS.ID [15] という BNS に登録可能となることから，名前解決用 Snap も HNS.ID が提供している．

2.3 関連研究

多くの研究者が，BNS に対してセキュリティ的観点からの研究を進めている．Muzammil らは，複数 BNS におけるタイポスクワッティングの実態を分析し，数千件におよぶ誤送金の発生を明らかにしている [7]．また，ENS のドロップキャッチに関する研究では，期限切れのドメインが再登録されたことで誤送金が発生するケースが確認されている [8]．吉田らは，Handshake 上の TLD を対象に，既存の商用ドメインに類似する「ドッペルゲンガードメイン」を定量的に抽出・分析した結果を報告している [9]．これらの研究は BN の悪用に注目したものであるが，異なる BNS 間で同一 BN が重複登録される名前衝突の実態や，それによって発生し得る誤送金やなりすまし等のリスクについては，十分に検証されていない．

我々の過去の研究では，BNS 間における TLD レベルでの名前衝突に着目し，暗号資産の誤送金といったリスクが生じ得ることを指摘しているが，具体的なリスクの検証までは行っていない [6]．本研究では，BNS 間の名前衝突に着目し，名前衝突の発生実態および暗号資産取引における具体的なリスクを実証的に明らかにすることを目的とする．

なりすましの観点では，偽装アドレスを利用してユーザのトランザクション履歴を汚染し，攻撃者への送金を仕向ける「アドレスポイズニング」の研究が進められている．Tsuchiya らは，Ethereum と BSC 上でアドレスポイズニングによる被害状況の調査のほか，偽装アドレスの生成コストの定量的評価も実施している [16]．本研究では，偽装アドレスの生成が名前衝突に起因する誤送金リスクにどのような影響を与えるのかについても，具体的なリスクシナリオを検討した上で考察する．

3. BN の名前衝突に関する調査

本章では，誤送金リスクを評価する前段階として実施した，BN の名前衝突に関する調査について述べる．名前衝突の現状を把握するために，まず 3.1 節では DWEB，FNS，HNS という TLD 登録可能な BNS 同士の衝突状況を調査

表 2: BN の収集結果

	DWEB	FNS	HNS
TLD の合計	14,440	17,806	25,430
有効期限内の TLD	1,338	17,806	15,515
SLD の合計	487,311	266,683	6,291
有効期限内の SLD	487,283	266,683	5,557

表 3: BNS 間における名前衝突件数

	DWEB ∩ FNS	DWEB ∩ HNS	FNS ∩ HNS	DWEB ∩ FNS ∩ HNS
TLD	213	1,253	10,926	206
SLD	46	1	1	0

した．これらの BNS を調査対象にすることで，ユーザによって登録された TLD および SLD の両方の衝突状況を確認できる．また，3.2 節では，FNS などの TLD 登録可能な BNS と，UD などの TLD 固定の BNS 間における，TLD 衝突状況の調査について述べる．

3.1 TLD 登録可能な BNS 同士の名前衝突

3.1.1 調査手法

3 件の TLD 登録可能な BNS に登録された BN の収集方法を示す．DWEB については，Dune Analytics [17] を利用し，DWEB のスマートコントラクトによって発行された BN のトークン ID を収集した．Dune Analytics では，ブロックチェーン上のデータが内部データベースに整形した上で保存されており，SQL クエリで検索・分析できる．そして，DWEB の API を利用してトークン ID に対応する BN の文字列を収集した．

FNS については，FNS が提供する API を用いてブロックチェーン上に発行済みの BN のリストを収集した．なお，FNS の BN は，サービスへの登録とブロックチェーン上への発行が別々の処理である．発行トランザクションの実行はユーザの任意であり，発行時は対応するブロックチェーンの中から一つを選択し，FNS の UI 上で実行する必要がある．本調査では，この発行済みの BN を対象とする．

HNS については，DWEB および FNS に登録された TLD を対象に，HNS 上での登録状況を調査する．我々の過去の研究と同様に，HNS のフルノード `hsd` とクライアント `hsd-cli` を利用し，`getnameinfo` コマンドにより対象 TLD のメタデータの一つであるオークションステータスが `CLOSED` のものを有効期限内の登録済み TLD として収集する．なお，HNS TLD 配下の登録済み SLD は，HNS.ID が提供する Subgraph API [18] を用いて収集する．

3.1.2 調査結果

BN の登録状況． 2025 年 2 月 25 日から 2025 年 4 月 17 日までの間に，各 BNS に登録された BN を収集した．BNS ごとの収集結果を表 2 に示す．DWEB SLD の有効期限はユーザが登録時に設定有無を選択できるが，DWEB TLD および HNS TLD/SLD は登録時に必ず有効期限が設定される．一方で FNS においては，TLD/SLD ともに有効期限は設定されないため，有効期限内の BN と合計の件数は一致している．

DWEB TLD に関して，我々の過去の研究 [6] では登録数が 11,889 件，その中でも有効な件数が 8,134 であったことを踏まえると，登録数は増加したものの，有効な件数は大幅に減少している．DWEB TLD は更新ごとに追加費用を支払う必要があるため，更新せずに所有権を放棄したユーザが一定数存在していると考えられる．また，SLD に関しては HNS SLD が最も登録件数が少ないが，先述のとおり HNS.ID において SLD を登録するには，該当する HNS TLD のオーナーが別途ステーキングする必要がある．本調査の BN 収集期間内では，ステーキング済みで SLD を登録可能な状態にあった HNS TLD は 48 件と非常に少ない件数であったため，その点が SLD 登録数にも影響していると考えられる．

BN の名前衝突状況． 表 3 に，TLD 登録可能な BNS 間の名前衝突件数を示す．なお，この衝突件数は表 3 中の有効期限内の BN の衝突件数を示している．HNS は DWEB，FNS に登録済みの TLD を収集対象にしており，FNS の TLD は 17,806 件中 10,926 件（61.4%）と半数以上が HNS に登録されている．さらに，DWEB の TLD は 1,338 件中 1,253 件（93.6%）と，有効期限内の TLD のほとんどが HNS に登録されていることが確認できた．その一方で，DWEB と FNS 間では 213 件と少ない件数に留まっていた．

SLD の名前衝突は，DWEB と FNS 間で 46 件，HNS と他の BNS 間で 1 件ずつと TLD よりも少なかった．DWEB と FNS 間の衝突件数に関しては，SLD 登録費用の決定方法の違いが原因と考えられる．DWEB では，TLD オーナーが SLD の登録費用を文字列に関わらず一律で決定できるが，FNS は SLD 中の文字列によって登録費用が変動し，文字数が増加するほど費用が下がる．例として本調査で収集した SLD に着目すると，TLD を除いた文字列の長さが 10 文字を超える SLD は，DWEB が 487,283 件中 108,963 件 (22.4%) であるのに対し，FNS は 266,683 件中 197,538 件 (74.1%) であった．したがって，FNS ユーザは文字数が多い SLD を登録する傾向にあり，文字列の構成がより複雑になることから，DWEB との SLD 衝突件数が少なくなったといえる．HNS に関しては，先述のとおり HNS.ID における SLD 登録可能な TLD は 48 件であり，DWEB，FNS の TLD との衝突件数は 2 件および 10 件と少数であった．そのため，SLD の衝突が発生しにくいと考えられる．

3 件の BNS 全てにおいて衝突している BN は，SLD が 0 件である一方で，TLD は 206 件確認できた．その中の一つに `.hodl` があり，これは TLD 固定の BNS である ONEID

表 4: TLD 固定の BNS と FNS の TLD 衝突件数

	UD	SPACE ID	ONEID	ZNS Connect
TLD	78	23	36	23
衝突 TLD	10	3	2	3

にも登録されている．この結果から，ある BNS に固有の TLD に関しても名前衝突は発生するといえる．

3.2 TLD 登録可能な BNS と TLD 固定の BNS 間における名前衝突

3.2.1 調査手法

本節では，TLD 登録可能な BNS として FNS を対象とし，TLD 固定の BNS と FNS 間での TLD 名前衝突に関して調査した．なお，DWEB は Snap をリリースしておらず，HNS は TLD のオーナーがステーキングすることで SLD を登録可能になることから，本調査では TLD 登録可能な BNS の対象外とした．

FNS SLD に対して送金する手段は，MetaMask のブラウザ拡張機能で FNS Snap を有効にするか，FNS が独自に提供するブラウザ拡張機能を利用するかのいずれかとなる．名前衝突による誤送金リスクを評価することを考慮し，TLD 固定の BNS は名前解決用の Snap をリリースしているものに限定した．それらの BNS 固有の TLD をリストアップし，FNS に登録されているかを確認した．

3.2.2 調査結果

TLD 固定の BNS と FNS の TLD 名前衝突に関する調査結果を表 4 に示す．なお，TLD 固定の BNS のうち，FNS との TLD 衝突件数が 0 件だったものは除外している．表 4 より，4 件の TLD 固有の BNS において，合計 18 件の TLD が FNS と衝突していることが確認できた．先述した ONEID の `.hodl` をはじめとし，UD の `.moon`，SPACE ID の `.floki`，ZNS Connect [19] の `.speed` 等の TLD が挙げられる．また，除外した BNS も含め，衝突していないが FNS 上でユーザが登録できる状態の TLD も確認されており，登録制限の対象外であることから，FNS TLD との衝突リスクがあるといえる．本結果を踏まえると，誤送金リスクを評価する上では，TLD 登録可能な BNS，および TLD 固定の BNS で実際に SLD の名前衝突が発生した際のウォレットアプリの挙動を確認する必要がある．

4. 誤送金リスクの評価手法

本章では，MetaMask Snaps を提供する複数 BNS において衝突 SLD を登録することで，名前衝突が引き起こす MetaMask 上での誤送金リスクを評価する．

4.1 調査対象 BNS の選定

Snap を提供している BNS のうち，TLD 登録可能な BNS としては FNS と HNS を対象とした．TLD 固定の BNS は，表 4 に示す BNS のうち，SPACE ID と ONEID を選定した．SPACE ID は，TLD 登録可能な BNS および表 4 に示す BNS の中で，唯一 Snap 動作時に MetaMask アプリの接続ブロックチェーン情報を利用せず，常に名前解決結果が表示される仕様であることが選定理由である．また，ONEID は固有の TLD である `.hodl` が FNS と HNS に登録されており，3 件の BNS で名前衝突が発生している場合の挙動を確認するために選定した．

表 5: 評価用に衝突させた SLD の発行先ブロックチェーン

TLD	FNS	HNS	SPACE ID	ONEID
`.floki`	Base	–	BSC	–
`.hodl`	BSC	Optimism	–	Viction

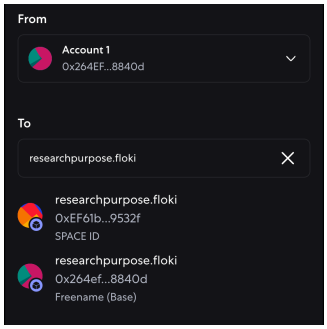

図 2: `researchpurpose.floki` の名前解決時の送金先選択画面（接続ブロックチェーン：Base）

4.2 衝突 SLD の登録

本評価の対象 BNS である FNS，HNS，SPACE ID，ONEID 間で共通の SLD を登録することで，意図的に名前衝突を発生させた．FNS と SPACE ID 間で共通の TLD として `.floki` を，FNS と HNS，および ONEID 間で共通の TLD として `.hodl` を選択し，衝突 SLD として `researchpurpose.floki` および `researchpurpose.hodl` を登録した．各 SLD の発行先ブロックチェーンを表 5 に示す．表 5 中の BNS のうち，FNS のみ発行先ブロックチェーンを対象の中から選択でき，本評価では `.floki` 配下の SLD を Base 上に，`.hodl` 配下の SLD を BSC 上に発行した．これらの SLD を利用し，MetaMask アプリ上で名前解決が実行される際に，名前衝突が発生した場合に生じうる誤送金リスクについて評価する．なお，評価は名前解決の役割を担う Snap，およびウォレット本体に対して実施する．

5. 評価結果

5.1 SLD へ送金する際の Snap の挙動

意図的に衝突させた SLD について，送金先選択画面における `researchpurpose.floki` の名前解決結果を図 2

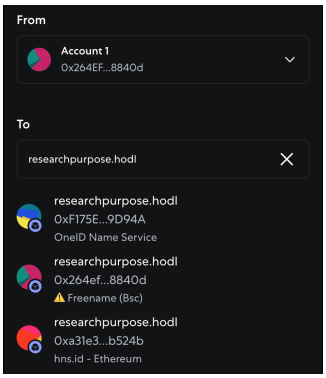

図 3: researchpurpose.hodl の名前解決時の送金先選択画面（接続ブロックチェーン：Ethereum）

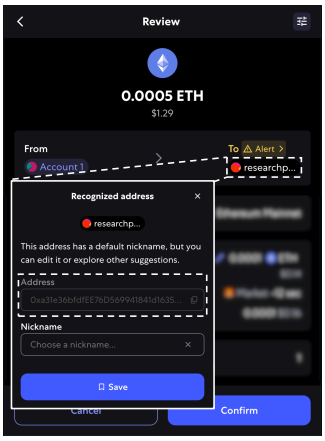

図 4: researchpurpose.hodl（HNS）への送金確認画面

に，researchpurpose.hodl の名前解決結果を図 3 に示す．図 2 は FNS SLD の発行先である Base に接続した際の結果であり，FNS と SPACE ID の両方の解決結果が並列に表示された．表示内容は，それぞれ SLD，解決先アドレスに加え，アドレス識別用のアイコンと登録先 BNS の名称であった．また，FNS Snap に対応していないブロックチェーンに接続した場合は，FNS の解決結果は表示されず，接続ブロックチェーンに依存しない SPACE ID の解決結果のみが表示された．

3 件の BNS 間で衝突させた researchpurpose.hodl について，それぞれの Snap が対応しているブロックチェーンである Ethereum に接続した場合，図 3 のように 3 件の名前解決結果が並列に表示された．これら 3 件の BNS Snap は全て名前解決に接続ブロックチェーン情報を利用するため，名前解決結果を表示する Snap の件数は接続ブロックチェーンによって変化する．また，FNS の名前解決結果は図 2 とは異なり，BNS 名の横に警告マークの表示が確認できた．これは FNS Snap 固有の機能であり，SLD の発行先ブロックチェーン（BSC）と MetaMask アプリの接続ブロックチェーン（Ethereum）が異なることを示している．

これらの結果から，送金先 SLD に関して名前衝突が発生している状況下では，接続ブロックチェーンや Snap の導入状況によって解決先が一意に定まらないことが確認できた．各 Snap の解決結果には登録先 BNS 名も表示されるため，正規の送金先 SLD の BNS を認識しており，該当する Snap を有効にしている場合は誤送金リスクが低いといえる．しかし，正規 BNS の認識を誤ったり，当該 Snap ではなく間違った Snap のみを有効にしている場合は，正規の解決結果が表示されず，意図しない相手への誤送金が発生するリスクが高い．

5.2 SLD へ送金する際のウォレット本体の挙動

図 2 および図 3 の送金先選択画面では，各 BNS Snap の名前解決結果が表示されるのみで，名前衝突が発生していることに対する警告表示等は確認されなかった．また，解決先アドレスの詳細を確認するためには，送金先選択後に表示される図 4 の送金確認画面において，送金先 SLD をクリックするという複数回の UI 操作が必要になる．そのため，名前解決結果で表示される略記が類似している場合，ユーザが誤った解決先を選択し，誤送金が発生してしまう可能性がある．なお，図 4 では SLD の上部に警告が表示されているが，これは当該送金先との初めての取引の際に表示されるものであり，名前衝突とは関連性がない．

6. 脅威モデルの検討

本章では，名前衝突による誤送金に関して，実際に発生しうる脅威モデルを検討する．基本的な脅威モデルとしては，「SLD の名前衝突による，ウォレットアプリの UI 上での誤った送金先の表示」が挙げられる．この脅威による誤送金の実現可能性を高めるために、標的ユーザが偽装 SLD の登録先である BNS の Snap を有効にしている前提のもと，脅威モデルの拡張を検討する．なお、標的とする正規ユーザが所有する SLD を正規 SLD，攻撃者が正規 SLD と衝突させる目的で登録した SLD を偽装 SLD と定義する。また，ここでの攻撃者とは，ネットワークを介した標的ユーザのウォレットアプリが動作する端末へのアクセスを実行できないオフパス攻撃者である．各種 BNS の SLD 登録状況をブロックチェーンや BNS の UI から監視することで，攻撃者は任意のタイミングで SLD を登録できる．

6.1 SNS アカウントのなりすましによる誤送金の誘発

X [20] をはじめとする SNS では，アカウント名に SLD を利用するケースが確認できる．アカウント名としての SLD は，自身が所属する暗号資産コミュニティを明示するほか，暗号資産の送金先を公開する役割を担っている．そのようなアカウントは，BNS の中でも特に著名な ENS の SLD を利用するケースが多く見られるが，本調査においては，.floki 配下の SLD をアカウント名に利用している X アカウントを確認した．ここでは，攻撃者が以下に示すフ

ローに則って，当該 SNS アカウントのなりすましを実行するケースを検討する．

(1) SLD を名前に設定した SNS アカウントを探索し，当該 SLD の登録先 BNS について調査する．
(2) 登録先 BNS を特定できた場合，当該 SLD に含まれる TLD が衝突している他の BNS 上で，偽装 SLD を登録するとともに，偽装 SNS アカウントを作成する．
(3) 偽装 SNS アカウントに偽装 SLD の登録先 BNS を明示し，当該 BNS の Snap をインストールするよう，標的ユーザを誘導する．

まず，攻撃者は発見したアカウント名に利用されている SLD の登録先 BNS を特定する必要がある．アカウントのプロフィール情報や投稿，および BNS の UI から得られる情報から登録先 BNS を特定することで，攻撃者は当該 SNS アカウントをなりすましの標的として選定できる．実際に，本調査で発見した SNS アカウントは，SPACE ID に登録された `.floki` 配下の SLD をアカウント名として設定していることを確認した．

標的の SLD が有する TLD の `.floki` は，SPACE ID の管理下にある一方で，FNS にも TLD として登録済みである．かつ，FNS 上に同一の SLD が登録されていなければ，攻撃者は偽装 SLD を登録することで，SPACE ID と FNS 間で SLD の名前衝突を発生させることができる．偽装 SLD 登録後，攻撃者は正規の SNS アカウントのなりすましとして偽装アカウントを作成する．

偽装アカウントには，偽装 SLD の登録先 BNS に関する情報を明記する必要がある．本節の例であれば，FNS SLD であることの明示に加え，自身への送金にはブラウザ拡張機能版の MetaMask を使用し，FNS Snap を有効にするよう促す必要がある．このような誘導により，標的ユーザが元から FNS を利用しているか否かに関わらず，送金先選択時に偽装 SLD の名前解決結果が表示され，誤送金を誘発することができる．

なお，正規 SLD の解決結果の表示は，標的ユーザの環境および Snap の仕様に依存する．本節の例では，正規 SLD の登録先は SPACE ID であり，標的ユーザが SPACE ID Snap を導入していない場合，送金先選択画面には偽装 SLD の解決結果のみが表示されるため，誤送金リスクは非常に高くなる．

6.2 MetaMask の UI 特性を利用したアドレスの紐付け

MetaMask の送金先選択画面では，名前解決結果として「SLD」「解決先アドレス」「登録先 BNS」「アドレス識別用のアイコン」の 4 項目が表示される．解決先アドレスは，42 桁のアドレスのうち `0x` を除いた先頭・末尾の各 5 桁，計 10 桁のみが表示される．また，アイコンはアドレスの文字列を入力として一意に生成される Identicon である．Snaps に対応しているブラウザ拡張機能版の MetaMask では Jazzicons [21] がデフォルトで利用され，アドレスの `0x` を除いた先頭 8 桁がアイコン生成のシードとなる．

標的ユーザの MetaMask UI に正規 SLD と偽装 SLD の名前解決結果が表示される場合を考えると，正規アドレスと先頭・末尾の計 10 桁が一致する偽装アドレスを紐付けた場合，表示内容のうち SLD と解決先アドレスが一致し，先頭・末尾の計 13 桁が一致する偽装アドレスを紐づけた場合，加えてアイコンまで一致する．したがって，攻撃者は偽装 SLD の解決先アドレスを操作することで，表示内容を正規 SLD に近づけることができる．この場合，登録先 BNS が異なっていても，標的ユーザは両方の SLD が同じアドレスに解決されていると誤認し，偽装 SLD の解決結果を送金先に選択する可能性が考えられる．上記のような偽装アドレスは，アドレスポイズニングの先行研究 [16] で実施されたシミュレーション結果から十分生成可能であり，偽装アドレスの紐付けは本章で設定した脅威モデルの実現可能性を高めるための一手法といえる．

7. 議論

7.1 提言

これまでの評価結果をもとに名前衝突が引き起こす誤送金リスクを低減させるための対策を，ウォレット開発者，BNS プロバイダ，ユーザの三者に向けて提言する．

ウォレット開発者． ウォレット開発者に対しては「名前衝突発生時の警告表示の実装」および「SLD 詳細情報表示の実装」を提言する．現在の MetaMask の仕様として，Snap は互いに独立して動作するため，送金先 SLD が名前衝突しており，それぞれの BNS の Snap が有効である場合，複数の名前解決結果が表示される．加えて，名前解決結果のフルアドレスは UI を複数回操作しないと確認できないため，6.2 節で述べた偽装アドレスを攻撃者が偽装 SLD に紐付けることにより，名前とその解決結果（略記アドレス）は完全に一致してしまう．提言のとおり，UI 操作なしに各解決結果に対する警告や詳細情報を表示することで，ユーザへの注意喚起につながると考える．表示すべき詳細情報としては，フルアドレスや発行先ブロックチェーンが挙げられる．

BNS プロバイダ． BNS プロバイダに対しては，「名前解決におけるウォレットの接続チェーン情報利用」を提言する．FNS や HNS など一部の BNS Snap は，名前解決時に接続ブロックチェーン情報を利用しており，Snap ごとに対応しているブロックチェーンは異なる．そのため，どの Snap の解決結果が表示されるかは接続ブロックチェーンによって変化するが，SPACE ID のように無条件で解決結果を表示する Snap も存在する．各 BNS の名前解決において，接続ブロックチェーン情報の参照を基本実装とすることで，解決結果の表示に関する制約が強まり，ユーザの

誤送金リスクが低減できると考えられる．

ユーザ．自身の SLD を BNS に登録しているユーザに対しては，「登録先 BNS の周知」を提言する．SLD の名前衝突が発生しており，ウォレットの UI 上に複数の名前解決結果が表示された場合でも，送金者が正規 SLD の登録先 BNS を把握していれば，誤送金が発生するリスクは低くなる．また，ユーザは SLD への送金時に「登録先 BNS の確認」および「名前解決設定の適切な管理」を意識する必要がある．名前解決の際に表示される SLD と BNS 名の組み合わせが正しいかを確認することで，誤送金が誘発される可能性は低下する．加えて，MetaMask における Snaps のような名前解決を担う拡張機能は，必要な BNS の機能のみを有効にすることで，意図しない解決結果の表示を防ぐことができる．そのほかにも，多額の暗号資産を送金する前には「少額送金の試行による送金先の検証」を実行することで，誤送金による被害額を抑えられる．

7.2 制限事項

本研究の名前衝突調査では，FNS，HNS，DWEB の BN を一定期間内で収集しているが，それぞれの収集タイミングにはずれが生じている．そのため，BN の有効期間等を考慮すると，厳密な衝突件数は若干の変動が見込まれる．しかし，DWEB の BN は大半が期限切れになっており，活発な動きが見られないことなどを踏まえると，結果に大きな影響は及ぼさないと考えられる．

また，本研究で調査対象としたウォレットアプリは MetaMask の 1 種類のみである．現時点で我々が認識する限りでは，多数の BNS の名前解決に対応しているウォレットアプリは他に確認できないため，現実的な誤送金リスクを評価する上では問題ない認識である．

7.3 研究倫理

本研究では，誤送金リスク評価のために，我々自ら複数の BNS に SLD を登録した．当該 SLD は，確認している限りでは我々のみが登録している文字列であり，今後偶発的に名前衝突が発生し，ユーザが被害に遭う可能性は極めて低いといえる．

TLD 登録可能な BNS 上の BN を収集する際には，各 BNS の SDK および API を利用した．収集にあたっては，利用規約を遵守した上でレート制限を超過することなく利用し，既存ユーザのサービス利用に影響を与えるような行動は回避している．

8. まとめ

本研究では，BNS 間の名前衝突が引き起こす誤送金リスクを評価した．まず BN の名前衝突について，TLD 登録可能な BNS 間における TLD および SLD の衝突状況を調査したほか，BNS に固有の TLD に関しても衝突が発生しているかを確認した．また，主要ウォレットアプリである MetaMask に対応した FNS や SPACE ID 等の BNS 間で，我々自ら新規 SLD を登録することで名前衝突を発生させ，MetaMask 上で名前解決が実行される際の挙動を確認し，誤送金が発生するリスクが高いことを確認した．さらに，具体的な脅威モデルを検討し，攻撃者の悪意ある名前衝突による誤送金の誘発が十分現実的であることを確認した．

今後の展望としては，SPACE ID や ONEID といった TLD 固定の BNS に登録された SLD まで含めた，より広範な名前衝突調査や，オーナーアドレスなどの衝突 BN のメタデータを含めた詳細な分析の実施が挙げられる．

参考文献

[1] ENS: `https://ens.domains/` (2025).
[2] Unstoppable Domains: `https://unstoppabledomains.com/ja-jp` (2025).
[3] Handshake: `https://handshake.org/` (2025).
[4] Freename: `https://freename.io/` (2025).
[5] 神薗雅紀ほか：`https://faportal.deloitte.jp/institute/report/articles/000980.html` (2024).
[6] Ito, D. et al.: Investigations of Top-Level Domain Name Collisions in Blockchain Naming Services, *Proceedings of the ACM Web Conference 2024*, WWW '24, p. 2926–2935 (2024).
[7] Muzammil, M. et al.: Typosquatting 3.0: Characterizing Squatting in Blockchain Naming Systems , *2024 APWG Symposium on Electronic Crime Research (eCrime)*, Los Alamitos, CA, USA, IEEE Computer Society, pp. 94–108 (2024).
[8] Muzammil, M. et al.: Panning for gold. eth: Understanding and Analyzing ENS Domain Dropcatching, *Proceedings of the 2024 ACM on Internet Measurement Conference*, pp. 731–738 (2024).
[9] 吉田純一ほか：分散型ネーミングサービス Handshake に登録されたドッペルゲンガードメインの定量的調査，インターネットと運用技術シンポジウム論文集， Vol. 2024, pp. 41–48 (2024).
[10] MetaMask: `https://metamask.io/` (2025).
[11] SPACE ID: `https://www.space.id` (2025).
[12] ONEID: `https://www.oneid.xyz` (2025).
[13] Decentraweb: `https://decentraweb.org` (2025).
[14] MetaMask Snaps: `https://metamask.io/snaps` (2025).
[15] HNS.ID: `https://hns.id/` (2025).
[16] Tsuchiya, T. et al.: Blockchain Address Poisoning, *arXiv preprint arXiv:2501.16681* (2025).
[17] Dune Analytics: `https://dune.com/home` (2025).
[18] Subgraph(hns-id): `https://thegraph.com/explorer/subgraphs/6FAHdNZszs25J25NmjTc2de7nuQu2b4HRhGWsPWiKruh?chain=arbitrum-one&view=Query` (2025).
[19] ZNS Connect: `https://zns.bio` (2025).
[20] X: `https://x.com/` (2025).
[21] Jazzicons: `https://github.com/MetaMask/jazzicon` (2025).