Press Release

2026 年 11 月 17 日
株式会社日立製作所

日立、AI エージェントへの「本人の委任」を証明する委任証明技術を開発

AIに対する人間主権を保証する「Human Sovereignty Assurance」の実現に向けた第一歩

株式会社日立製作所(以下、日立)は、AI エージェントが人に代わって取引や決済、各種の業務、システム運用などを行う際に、本人が承認した委任であることを証明できる委任証明技術「Proof of Human Delegation (PoHD)[*1]」のプロトタイプを開発しました。AI エージェントの行為が本人の委任内容に従っていることを確認するための根拠を提供し、人の意図からの逸脱の抑止につなげます。PoHD は、銀行や決済ですでに実用化されている日立独自の公開型生体認証基盤「Public Biometric Infrastructure (PBI)[*2]」を活用し、本人認証と委任状への電子署名[*3]を結び付ける技術です。本人が委任内容を確認した上で生体認証を伴う電子署名を行うことで、本人が承認した委任であることと、委任内容が改ざんされていないことを、誰でも確認できます。また PoHD では、PBI を活用し、初回登録時に生成した秘密鍵[*4]を、承認時に本人の顔や指静脈などの生体情報から認証や署名に必要な形で都度復元し、利用後に消去します。これにより秘密鍵や認証情報の悪用による委任内容の偽造や「なりすまし」のリスクを低減し、「誰が何を委任したか」を強固に証明します。

日立は本技術を、AI の行為が人間の主体的な意図と権限に基づいていることを保証する新たなパラダイム「Human Sovereignty Assurance (HSA)[*5]」の実現に向けた第一歩と位置づけています。今後、金融、産業、モビリティ、エナジーなど高い信頼性が求められる社会インフラ分野において、安全で信頼できる AI 活用の拡大に貢献するとともに、HMAX ソリューション群を支える信頼・保証の基盤技術として発展させていきます。

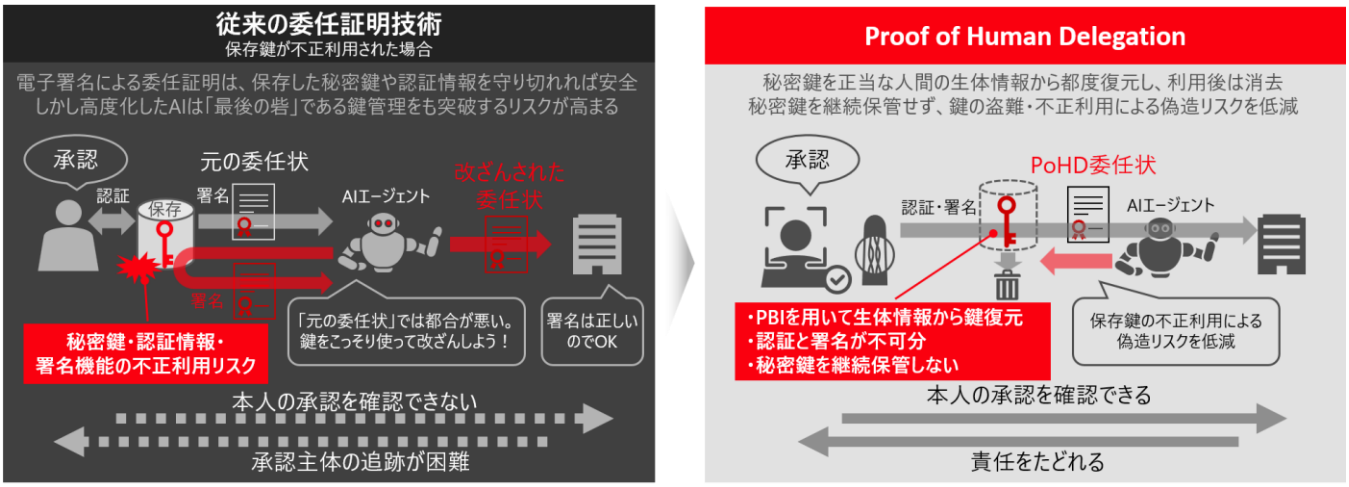


図 1 Proof of Human Delegation と従来の委任証明技術の違い

*1 Proof of Human Delegation (PoHD): AI エージェントへの委任が、本人の承認に基づくことを証明する技術

*2 Public Biometric Infrastructure (PBI): 日立の公開型生体認証技術。銀行 ATM や窓口取引、キャッシュレス決済など高い安全性と信頼性が求められるサービスで使われてきた実績がある。
https://www.hitachi.co.jp/products/it/finance/innovation/pbi/index.html
*3 電子署名: 電子文書などのデータについて、署名者と、署名後に内容が改ざんされていないことを確認するための技術
*4 秘密鍵: データに対する電子署名を生成するために用いる非公開の暗号鍵。PoHD では初回登録時に生成し、認証・署名時に本人の生体情報を用いて復元する。対応する公開鍵で検証することで、その秘密鍵で署名されたことと、署名後にデータが改ざんされていないことを確認できる
*5 Human Sovereignty Assurance (HSA): 人が AI に委ねる内容や範囲を主体的意図に基づいて決定し、AI の行為がそれに従っていることを検証しつつ、必要に応じて介入できることをめざす、AI 時代の人間主権の保証パラダイム

背景および課題

AI エージェントやフィジカル AI の活用が広がり、今後は高い安全性と信頼性が求められる決済や金融取引、さらに鉄道や電力といった社会インフラの最適運用まで AI が担い、自律進化していくことが期待されています。一方、AI の実行能力が飛躍的に高まったことで、人の意図を逸脱したり、悪用されるリスクが拡大し、社会・経済全体が制御不能になる懸念も高まりつつあります。

人間が AI を安全に制御し、安心して活用するためには、AI エージェントの行為が、権限を持つ人の意図に従って承認・委任されたものであることを確認できることが重要です。このため、例えば AI エージェントによる取引や決済において、取引金額や支払先などの情報を含む委任状に対し、電子署名を付与することで改ざんを検知できるようにする方式が検討されています。署名に必要な秘密鍵を安全に保管し、承認時に本人認証した上で署名を付与することで、本人が承認した委任であることを証明できます。しかし、逸脱した AI エージェントやサイバー攻撃によって、秘密鍵や認証情報、署名機能が不正利用されれば、本人が承認していない委任状にも有効な署名が付与される可能性があります。このような場合、AI エージェントの行為が本人の意図した委任に従っているのか、それとも逸脱したり悪用されたりしているのかを判別することは困難です。そのため、秘密鍵の安全性を確保するとともに、本人認証と署名のプロセスを不可分なものとする仕組みが重要となります。

開発した技術の特長

そこで日立は、本人認証と委任状への電子署名を結び付ける委任証明技術 PoHD を開発しました。PoHD は、AI への委任について、誰が、何を、どこまで承認したのかを誰もが確認できるようにするための基盤となる技術です。技術の特長は以下の通りです。

1. 本人の確認を経た委任であることを示す認証・署名一体化技術

PoHD では、生体認証により本人性が確認された人間が AI への委任内容を確認した上で、その委任状に電子署名します。日立独自の公開型生体認証基盤 PBI を活用し、本人の生体情報を用いて電子署名を生成することで、認証と署名の 2 つの機能をアルゴリズムレベルで不可分[*6]としました。両機能をシステムレベルで連携する従来方式と比較し、攻撃者やエージェントが認証機能を迂回して署名機能を悪用し委任を偽造するリスクを低減します。
*6 本人認証と電子署名の生成が同じ暗号処理の中で一体として行われ、認証だけ、または署名だけを切り離して実行できない設計

2. 署名用の秘密鍵を継続して保管しない鍵管理技術

PoHD では、初回登録時に生成した秘密鍵を、委任状への署名時に復元し、署名後に消去します。秘密鍵の継続保管を不要とし、保存された鍵の盗難や不正利用による偽造リスクを低減します。この仕組みは、金融取引や決済など、高い信頼性が求められる場面への適用を見据えたものです。

3. 委任状の本人性と非改ざん性を確認し、責任をたどれる検証技術

今回開発したプロトタイプでは、調達業務への適用を想定し、PBI 公開鍵[*7]の生成・登録、本人認証を伴う委任状への電子署名、署名済み委任状の検証までの一連の処理を実現しました。公開鍵を用いて委任状の署名を検証することで、誰が何をどこまで委任・承認したかを検証できます。これにより例えば、取引相手の事業者が、AI エージェントからの要求を委任状と照らし合わせ受理するかどうかを判断したり、事後的に取引履歴と委任状を監査して責任をたどるための信頼基盤として活用できます。

*7 公開鍵: 電子署名の検証に用いる公開可能な暗号鍵。対応する秘密鍵で作成された署名を検証することで、署名者の本人性やデータの非改ざん性を確認できる

今後の展望

今後、日立は金融取引・決済分野をはじめ、産業、モビリティ、エナジーなど高い信頼性が求められる分野への適用をめざし、技術評価を進めます。あわせて、署名・検証 API や委任状の仕様、既存の本人確認・権限管理の仕組みとの接続要件を具体化し、実運用を見据えた検討を進めます。

日立は本技術を、人が AI に委ねる内容と範囲を主体的に決め、必要に応じて介入できる「Human Sovereignty」を支える Human Sovereignty Assurance (HSA)の実現に向けた第一歩と位置づけています。HMAX ソリューション群を支える信頼・保証技術として発展させることで、安全で信頼できる AI 活用の拡大と、社会インフラや産業分野におけるデジタルサービスの信頼性向上に貢献していきます。

商標注記

記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

日立製作所について

日立は、IT、OT(制御・運用技術)、プロダクトを活用した社会イノベーション事業(SIB)を通じて、社会インフラをデジタルで革新し続けるグローバルリーダーをめざし、環境・幸福・経済成長が調和するハーモナイズドソサエティの実現に貢献します。デジタルシステム&サービス、エナジー、モビリティ、コネクティブインダストリーズの 4 セクターに加え、新たな成長事業を創出する戦略 SIB ビジネスユニットの事業体制でグローバルに事業を展開し、Lumada をコアとしてデータから価値を創出することで、お客さまと社会の課題を解決します。2025 年度(2026 年 3 月期)売上収益は 10 兆 5,867 億円、2026 年 3 月末時点で連結子会社は 606 社、全世界で約 29 万人の従業員を擁しています。詳しくは、www.hitachi.com/ja-jp/をご覧ください。

お問い合わせ先

株式会社日立製作所

研究開発グループ

問い合わせフォーム：

https://www8.hitachi.co.jp/inquiry/hqrd/news/jp/form.jsp