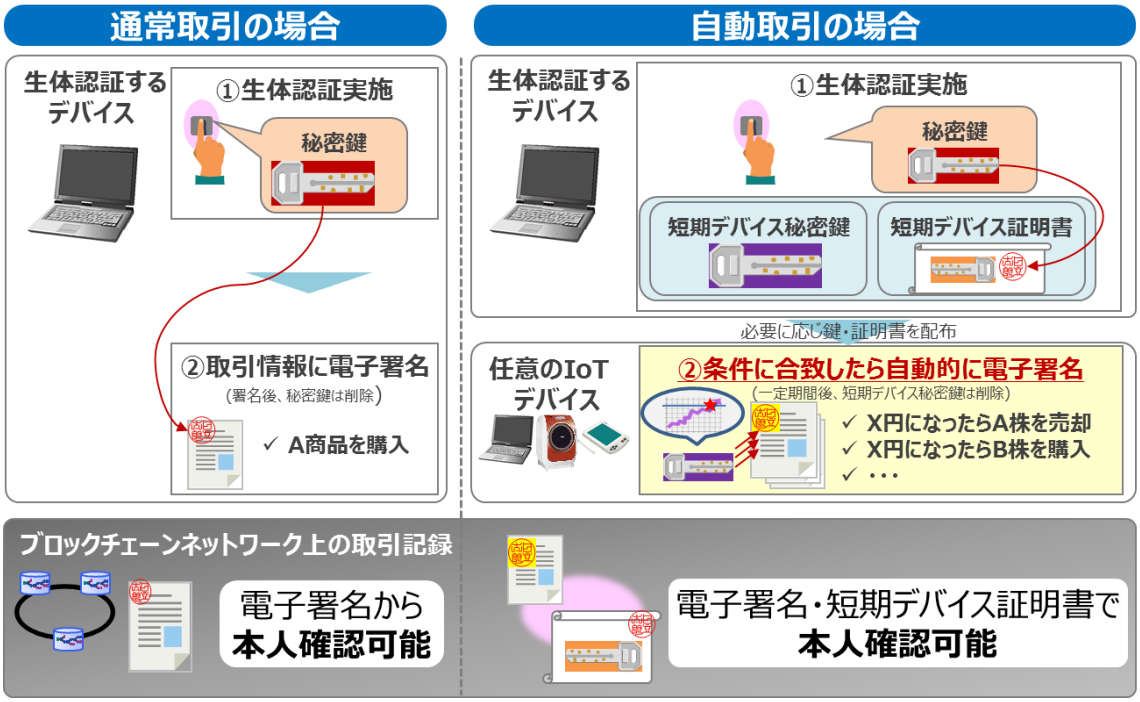
News Release

2017 年 10 月 5 日
株式会社日立製作所

ブロックチェーンにおけるセキュアな取引を実現する生体認証技術を開発

PBI-ブロックチェーン連携技術により、IoT 決済や自動取引を可能に



PBI-ブロックチェーン連携技術の概要

株式会社日立製作所(執行役社長兼 CEO:東原 敏昭／以下、日立)は、生体情報から電子署名*1を生成する日立独自の「公開型生体認証基盤(以下、PBI)」技術*2 を応用し、ブロックチェーンにおけるセキュアな取引を実現する PBI-ブロックチェーン連携技術を開発しました。本技術により、盗難や漏えいのリスクが低い指静脈などの生体情報を元にして電子署名を生成し、取引記録への付与が可能となるほか、設定した条件に従って電子署名を自動生成することができます。この結果、今後ブロックチェーン上での実現が期待される株や電力などのアルゴリズムトレードや、IoT デバイスによる自動取引などで必要となる、取引の際の本人認証を、手間無く行うことができます。日立は、今後、ブロックチェーンの利活用を検討するパートナーとの実証実験などを通じて、セキュアで利便性の高いブロックチェーン認証基盤の確立をめざしていきます。

ブロックチェーンは、第三者機関の仲介なしで取引が可能な取引基盤として、仮想通貨取引、商品売買、病院での受診履歴管理など多様な用途への活用が期待されています。ブロックチェーン上での取引の信頼性は、ユーザーが取引情報に対して公開鍵暗号技術*3 に基づく電子署名を付与し、その正当性を誰もが検証可能にすることで担保されています。一方で、ユーザーが電子署名を生成するための秘密鍵を紛失・漏えいした場合は、ブロックチェーン上の資産喪失や、なりすましによる不正取引被害のリスクがあります。そのため、現状の認証技術では、秘密鍵は IC カード内やサーバ

ー上に格納した上で、ID やパスワード、生体認証などでのみアクセス可能にするなど、秘密鍵の安全な管理と、なりすまし防止のための確実な本人確認が課題でした。

そこで日立は、生体情報から電子署名を生成することができる、日立独自の PBI をブロックチェーン上で利用するための PBI-ブロックチェーン連携技術を開発しました。本技術では、従来の生体認証技術と異なり、生体情報自体を秘密鍵として利用できるため、秘密鍵を外部管理する必要がなく、セキュアな取引が可能です。また、今回、設定した条件に従って電子署名を自動生成可能な、自動取引向け短期デバイス証明書生成技術を開発することで、自動取引を実現し、取引のたびに認証を行わなくてはならない煩わしさを解消しました。開発した技術の特長は以下の通りです。

1.PBI-ブロックチェーン連携技術

代表的なブロックチェーン基盤である Hyperledger Fabric[*4]に対し、PBI を用いて取引時の電子署名を生成・検証することのできる連携技術を開発しました。通常の Hyperledger Fabric アプリケーションは、サーバー上でユーザーの秘密鍵の管理と署名生成を行うシステムでしたが、日立が構築した Hyperledger Fabric の環境に本技術を適用することで、ユーザー端末側で電子署名を生成し、本人確認することが可能だと確認できました。また、本技術では生体認証のたびにユーザーの体から都度、一時的に秘密鍵を抽出するため、秘密鍵を管理する必要がなく、紛失や漏えいによる不正利用といった課題を解決します。本人でなければ電子署名を生成できないため、確実な本人確認に基づく取引であることが保証されます。

2.自動取引向け短期デバイス証明書生成技術

株や電力のアルゴリズムトレードのように、PC やスマートフォンをはじめとした IoT デバイスが、ブロックチェーンに対して自動的に取引情報を送信する際に、電子署名を自動生成する技術を開発しました。具体的には、ユーザーがデバイスに対して「いくらになったらこの株をいくつ売る」といった取引条件のロジックを指示する際に、短期間だけ有効な「短期デバイス秘密鍵」を生成し、それと対になる公開鍵に対し電子署名を付与した「短期デバイス証明書」を生成します。デバイスは、「短期デバイス秘密鍵」と「短期デバイス証明書」を一定期間保管し、取引条件が成立した場合のみこれらを用いて、電子署名を生成します。これにより、取引のたびにユーザーが本人認証する必要なく、自動で取引可能です。「短期デバイス秘密鍵」と「短期デバイス証明書」を任意のデバイスに配布すれば任意の IoT デバイス上で決済などが可能なほか、証明書の有効期間は短期間に設定可能なため、「短期デバイス秘密鍵」が漏えいした際のリスクも低減されます。

日立は、今後、ブロックチェーンの利活用を検討するパートナーとの実証実験などを通じ、本技術の 2018 年度中での実用化をめざすとともに、本技術を活用して、ブロックチェーン上でユーザーが電子署名方式を選択・変更できる API[*5]機能を OSS[*6]として展開し、セキュアかつ利便性の高いブロックチェーン認証基盤の確立をめざしていきます。

本成果の一部は、2017 年 10 月 11 日(水)に東京都にて開催される「Blockchain EXE[*7]」で発表する予定です。

*1 電子署名： 紙文書における印章やサイン（署名）に相当する役割を果たすもの。主に本人確認や、偽造・改ざんの防止のために用いられる。

*2 PBI(Public Biometrics Infrastructure)技術： 静脈パターンなどの生体情報の「揺らぎ」を補正することで秘密鍵を抽出し、公開鍵暗号方式に基づく電子署名を生成する日立独自の技術。従来技術では生体情報は「揺らぎ」を持つため毎回同じデータが取得できず、一意なデータである暗号鍵を生成することはできなかった。IC カードやパスワードに依存した鍵管理が不要となり、便利で低コストかつ確実な本人確認が可能な電子認証基盤が実現できる。また生体情報は「一方向性変換」により暗号学的に復元困難なデータ（PBI 公開鍵）に変換して登録・照合されるため、元の生体情報はどこにも保存されず、漏えいリスクを最小化することができる。

*3 公開鍵暗号： 広く公開された公開鍵と本人だけが管理する秘密鍵を組み合わせる暗号化方式。公開鍵で暗号化されたものは、その対となっている秘密鍵でしか復号化できない。

*4 Hyperledger Fabric: The Linux Foundation が設立した、ブロックチェーン技術の共同開発プロジェクト「Hyperledger」にて開発されたオープンソースのブロックチェーンフレームワーク。

*5 API: Application Programming Interface

*6 OSS: Open Source Software

*7 https://blockchainexe.com/

■照会先

株式会社日立製作所 研究開発グループ 技術統括センタ [担当：阿部、藤原]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話：050-3135-3409 (直通)

以上