プレスリリース

平成 30 年 6 月 25 日

報道関係者各位

国立大学法人 奈良先端科学技術大学院大学

仮想通貨のブロック･チェーンを応用し、IoT のセキュリティを保証する技術を開発
～莫大な数の接続機器への不正アクセスを個別に制御～
人とモノが安全につながる社会の実現へ

【概要】

奈良先端科学技術大学院大学（学長：横矢直和）先端科学技術研究科　情報科学領域　大規模システム管理研究室の笠原正治教授、張元玉（チョウエンユ）助教は、西安電子科技大学の沈玉龍（シェンユロン）教授らとの共同研究により、データを分散して管理する仮想通貨の基盤技術「ブロック・チェーン」を応用して、多数の機器が接続した「IoT（モノのインターネット）」ネットワークのセキュリティを保証するアクセス制御方式を開発しました。

莫大な数のセンサやユーザ･デバイス（装置）が連携して構成されるモノのインターネット（IoT）では、セキュリティが脆弱な IoT デバイスが存在すると、そのデバイスを介して不正な意図を持ったユーザがシステム内のリソース（データなど）やサービスに不法にアクセスできてしまう重大なセキュリティ問題が知られていました。本研究開発では、ブロック・チェーン上で機能し、個々のデータの信頼性をチェックするスマートコントラクト技術を応用しました。その結果、莫大な数の信頼し難い IoT デバイス群で構成されるネットワークシステム上で、信頼性が保証された分散アクセス制御を実現するフレームワーク（基本構造）の開発に成功しました。これにより、とてつもない数の IoT デバイスと多種多様なリソースやサービスを強固なセキュリティの下で連携させることが可能となり、人とモノがより簡単につながる政府提唱の「Society 5.0」の実現に向けた基盤技術として期待されます。

この研究成果は、平成 30 年 6 月 15 日付けで IEEE Internet of Things Journal にオンライン公開されました。

つきましては、関係資料を配付いたしますので、取材方よろしくお願いいたします。

【ご連絡事項】

(1) 本件につきましては、奈良先端科学技術大学院大学から奈良県文化教育記者クラブをメインとし、学研都市記者クラブ、大阪科学・大学記者クラブに同時にご連絡しております。
(2) 取材希望がございましたら、恐れ入りますが下記までご連絡願います。
(3) プレスリリースに関する問い合わせ先

奈良先端科学技術大学院大学　先端科学技術研究科　情報科学領域
大規模システム管理研究室　教授　笠原　正治
TEL　0743-72-5134　　FAX 0743-72-5369
E-mail kasahara@is.naist.jp

奈良先端科学技術大学院大学　先端科学技術研究科　情報科学領域
大規模システム管理研究室　助教　張　元玉
TEL　0743-72-5365　　FAX 0743-72-5369
E-mail yyzhang@is.naist.jp

【背景】

ワイファイ（WiFi)、ジグビー（Zigbee)、ブルートゥース（Bluetooth）に代表されるネットワーク通信技術の急速な発展により、数限りないセンサやユーザ・デバイスがインターネットを介して相互接続され、モノのインターネット（IoT）が形成されようとしています。このようなIoT環境では、接続された多くのIoT端末から大量のデータを収集・蓄積・加工することを可能にする一方で、セキュリティが脆弱なIoT端末が存在すると、その端末を介して不正ユーザがシステム内のリソースやサービスに不法アクセスできるようになり、重大なセキュリティ問題を引き起こす可能性があります。このように、莫大な数のIoT端末により構成されるIoTネットワークにおいて、IoT端末に対するアクセス制御は非常に重要な研究課題となっています。 ひとつのサーバに複数のユーザがアクセスする、既存のクライアント・サーバ型に代表される集中型アクセス制御方式では、サーバが悪意のあるユーザに侵入されるとアクセス制御自体が乗っ取られたり、自然災害や人為的災害でサーバが破壊されるとアクセス制御方式自体が機能しなくなったりする単一点障害の問題がありました。

【研究開発手法】

IoTシステムにおける不正アクセスを防止するためには、信頼できる分散型のアクセス制御方式が重要です。近年、ビットコインやイーサリアム等の仮想通貨の基盤技術であるブロック・チェーンが、信頼できないピア（端末）間で信頼性の高い分散コンピューティングを実現するアプローチとして注目を集めています。本研究ではブロック・チェーン上で機能するスマートコントラクトを利用して、莫大な数の信頼できないセンサ・デバイス群で構成されるIoTシステム上で、信頼できる分散アクセス制御方式のフレームワークを開発することに成功しました。

スマートコントラクトは、ブロック・チェーンに存在する実行可能なプログラミング・コードとして考えることができます（図1)。スマートコントラクトは、さまざまな端末で共通に使用できる多数のアプリケーションバイナリインターフェイス（ABI）を提供し、ブロック・チェーンシステムの任意のピアによって実行できます。 ABIに加えて、スマートコントラクトには、契約の状態とみなされるデータも含まれます。各スマートコントラクトは特定のアドレスに関連付けられており、このアドレスによって、システム内の任意のピアはこのコントラクトのABIを実行したり、状態を変更したりすることができます。また、 システム内の任意のピアの計算能力がシステム全体の計算能力の半分よりも少ない状況になっている限り、システム内のどのピアもそのABIを意図的に間違った形で実行することができず、結果としてそのスマートコントラクトの機能を改ざんすることができません。スマートコントラクトのこの特性に基づいて、本研究は、IoTシステム内の任意のピア間で強固なセキュリティをもつアクセス制御方式を実現しました。

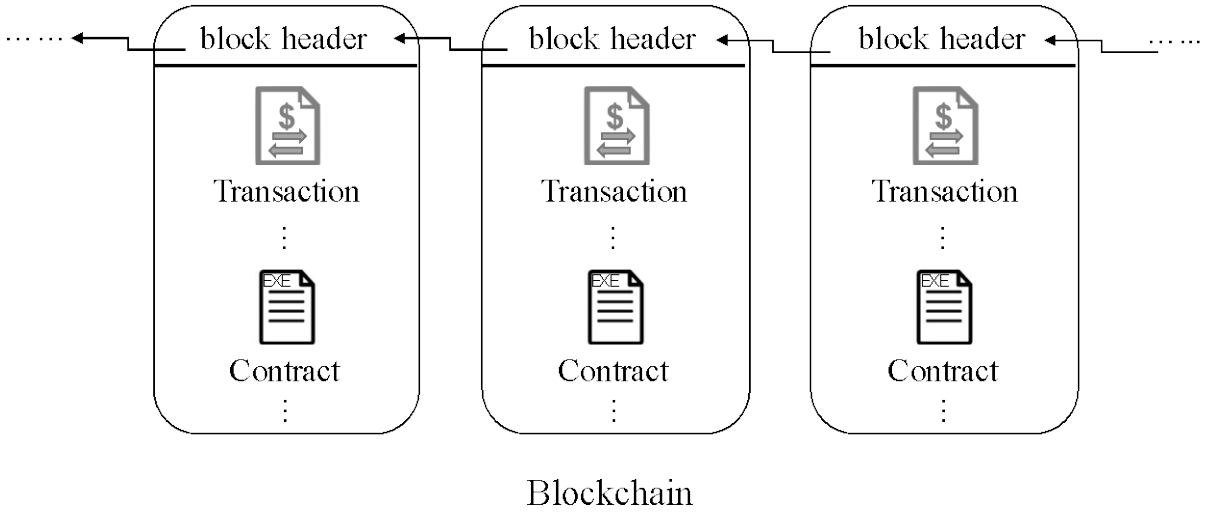

図１：ブロック・チェーンにおけるスマートコントラクト

【本技術の応用例】

本技術の簡単な応用例として、ガス検知器・アラーム・スマートフォンを備えた簡単な IoT システムを考えます。 スマートフォンはガス検出器からガス漏れ情報を取得し、ガス検出器にコマンドを送信してガスを遮断することができます。アラームはガス検出器からガス漏れ情報を取得し、警報を発することができますが、ガス検出器にコマンドを送ることはできません。この例は典型的なアクセス制御シナリオとして考えることができます。

このシナリオでは、ガス検出器はガス漏れ情報とガスを遮断する機能をリソースとして提供する IoT デバイス、スマートフォンとアラームはガス検出器のリソースにアクセスする IoT デバイスとして考えることができます。本技術では、次のようにアクセス制御を実現します。

最初に、ガス検出器はスマートフォンとアラームの両方にアクセス権を与えます。このとき、スマートフォンにはガス漏れ情報取得とガスの遮断の二つの機能についてアクセス権を付与します。一方、アラームに対してはガス漏れ情報取得の機能のみについてアクセス権を付与します。このアクセス権付与情報は、ブロック・チェーンのブロックに含まれるコントラクトとして記録されます。

次に、ガス検出器がアクセス要求を受け取ったとき、ガス検出器はその要求を発生させた IoT デバイスのアクセス権を検証します。これは、ガス検出器がブロック・チェーン上に記録されているコントラクトの内容を照会することでそのリソースにアクセスできる IoT デバイスかどうかを判断します。

リソースを要求した IoT デバイスが正当な端末であることをガス検出器が確認できた場合、ガス検出器は要求されたリソースを IoT デバイスに提供します。例えばアラームがガス漏れの確認を要求してきた場合、ガス検出器はその時点でのガス漏れ情報をアラームに返します。

【用語解説】

IoT：

Internet of Things の略で「モノのインターネット」と訳され、多種多様なモノがインターネットを介して接続され、大量の情報をやり取りするネットワークシステムを意味する。IoT デバイスは低コストで開発されることが多く、セキュリティの脆弱性が問題として指摘されている。

ブロック・チェーン：

ビットコインに代表される仮想通貨の基盤技術であり、通貨の取引がインターネット上の複数のノードに分散的に記録される取引台帳型データベース。イーサリアムという仮想通貨では、プログラムをトランザクション（一連の情報処理単位）に埋め込んでオークションやコントラクト（契約）といったサービスを提供することができる。

スマート・コントラクト：

コンピュータ・ネットワーク上で自動的に行う契約行為。ビジネス分野におけるブロック・チェーン技術の代表的な応用例として考えられている。

【掲載論文】

タイトル　：Smart Contract-Based Access Control for the Internet of Things

著　　者　：張元玉　（奈良先端科学技術大学院大学　先端科学技術研究科　情報科学領域）
笠原正治（奈良先端科学技術大学院大学　先端科学技術研究科　情報科学領域）
沈玉龍　（西安電子科技大学　計算機科学研究科）
姜暁鴻　（公立はこだて未来大学　システム情報科学研究科）
万剣雄　（内モンゴル工科大学　情報工学研究科）

論文掲載先　：IEEE Internet of Things Journal