V2X を見据えたゼロトラスト・アーキテクチャ “ZTA/SSI” の提案

Zero Trust Architecture for V2X Network, ZTA/SSI

三谷 陽 Akira MITANI
愛知 功 Isao AICHI
澤井 佑樹 Yuki SAWAI
石田 晋哉 Shinya ISHIDA
山下 克司 Katsushi YAMASHITA

In recent years, Vehicle-To-Everything (V2X) communication has attracted intense attention in the automotive industry. As the number of items connected to vehicles increases, many types of unexpected security threats be emerged. For society to safely and securely benefit from the convenience of V2X network services, countermeasures against such new threats are essential. In this paper, we propose a new extended zero-trust architecture (ZTA/SSI). ZTA/SSI supports V2X networks in which unspecified numbers of stakeholders participate.

Key words :
Security, V2X, Zero Trust, Blockchain, Self-Sovereign Identity

特集

はじめに

自動車産業界は 100 年に一度の変革期を迎えており，特に車両が社会の様々なモノと繋がる V2X（Vehicle to Everything）が注目されている．社会インフラ・他車両・歩行者・Web サービス等と車両がシームレスに情報をやりとりすることで，ユーザーの利便性や交通安全性の向上に繋がる様々なサービスが生まれるであろう．

一方で，車両が不特定多数の相手と繋がることは，車両だけでなく社会全体にこれまで想定していなかったセキュリティ上の脅威が生じることを意味する．そのため，社会が安心安全に V2X の利便性を享受するためには，そのような新たな脅威への対策が必須である．

本論文では，近年注目を集めている “ ゼロトラスト・アーキテクチャ ” と呼ばれるセキュリティ・アーキテクチャを不特定多数の参加者が参加する V2X のネットワークにおいて適用することを可能にする ZTA/SSI（Zero Trust Architecture over Self-Sovereign ID）を提案する．

複雑化する車両システムとネットワーク

車両が社会の様々なモノと繋がる V2X（Vehicle to Everything）が社会実装されていくに応じて，車両システムとそれが形成するネットワークは複雑化が避けられない．

車両はこれまでのように特定の対象と通信を行うのではなく不特定多数の相手と通信をすることが求められ始める．例えば，信号機などの交通インフラ，異なるメーカー製の車両，歩行者，更には Web サービス等と通信を行うことが考えられる．

それらの通信の実現とユーザーの利便性向上のため，車両には従来の OBD（On-Board Diagnosis）ポート

や CAN インターフェースに加え，Wi-Fi や 3G/LTE，Bluetooth，IVI デバイスタッチパネル，スマートキーなどの様々な外部インターフェースが追加されていく．

さらにそれらの通信を利用した高度なサービスを提供するため，車両ソフトウェアも複雑化していく．機能リッチな OS を導入し，その上に大規模なソフトウェアスタックを構築し，それらを高機能プロセッサ上で動作する必要が出てくる．

境界型防御の限界

現在の車両において主流のセキュリティ・アーキテクチャは多層境界型防御である．車両内部と車両外部との間にファイアーウォールとなる通信ゲートウェイを設けて通信を監視し，更に制御系へのアクセスには，もう一段のゲートウェイが通信を監視しアクセスを許すといった多層防御を行っている[i]．

しかし前述のように車両システムとそれを取り巻くネットワークが複雑化した V2X の環境の場合，多層境界型防御では脅威を排除しきれないことが知られている．

実際に，例えばセキュリティ研究者の C. Valasek と C. Miller は，実販売されている車両を対象にリモートからハッキングを試みて成功している[ii]．彼らは IVI システムへ Wi-Fi 経由で侵入し，そこを起点に多段的に各コンポーネントを攻撃することで，最終的に車両全体を制御する手段を不正に得ることが可能であることを実証したのである．

ゼロトラスト・アーキテクチャ

近年，リモートワークによる社外からのアクセスやクラウド移行などによりネットワーク構造が複雑化している背景から，企業内ネットワークの領域においても従来の境界型防御の限界が認識されている．

多様化する脅威に対して企業内ネットワークのセキュリティをどのように確保するか，その対応方針として近年注目を浴びているのが「ゼロトラスト・アーキテクチャ（Zero Trust Architecture：ZTA）」と呼ばれるアーキテクチャである．2020 年 8 月，米国国立標準技術研究所（NIST）が SP800-207 としてゼロトラスト・アーキテクチャ導入のガイドラインを発行し[iii]注目され始めた．

ZTA の中核となる論理コンポーネントを Fig. 1 に示す．ZTA では「決して信頼せず，常に検証する」という原則に従いアクセス制御が行われる．

企業リソースに対してアクセス要求元がアクセス要求する度に，ポリシー実施ポイント（PEP）を経由し，ポリシー決定ポイント（PDP）でアクセス許可が判断される．PDP では，アクセス要求元やアクセスされる企業リソースのネットワーク上の「場所」を基準にするのではなく，アクセス要求元の役割やデバイス情報，要求している企業リソース等のコンテキストに基づいたアクセスポリシーを適用する．これにより不適切なアクセスや環境内での水平移動をブロックすることを可能にする．

アクセス要求元が，要求するリソースにアクセスするための権限を持っているか？その権限が正当に与えられたものか？といったアイデンティティの管理が ZTA を実現するうえで根幹となる．

エンタープライズ NW では ZTA を実現するための様々なサービスが提供され，多くの企業で ZTA が採用され始めている[iv]．

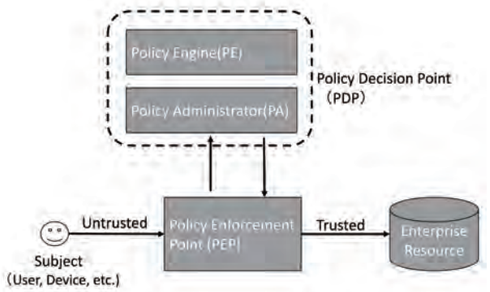

Fig. 1 Core components in ZTA

V2X ネットワークでのアイデンティティ管理

前述したように V2X ネットワークにおいて，境界型防御ではセキュリティの確保が困難となることが想定される．そこで企業内ネットワークと同様に，ZTA に準じた V2X ネットワークを実装することで安心・安全なモビリティ社会が実現できると考えられる．

しかし V2X ネットワークは，アイデンティティ管理の面で企業内ネットワークにない困難がある．

企業内ネットワークはその所有者である企業そのものが単一のアイデンティティ管理主体として運営される．そのため管理者が NW 内の全エンティティのアイデンティティ情報を Identity and Access Management System（IAM）等により把握・管理するすることが可能である（Fig. 2 左）．

一方で V2X ネットワークは，Fig. 2 の右図のように不特定多数の独立した運営主体が各々管理するべきエンティティを管理しており，異なる運営主体のエンティティ間で通信を行う必要があるのが特色である．このような状況ではエンティティのアイデンティティ情報をお互いに正確に把握することが困難という課題がある．

この課題に対して回避方法として考えられるのは，各運営主体が共通して信頼できるサードパーティーの運営主体を立て，そこで全エンティティのアイデンティティ情報の管理を行う方法である（Fig. 3）．

しかしこの方法は以下のような課題があり，決して好ましくない．第一に，サードパーティーの管理システムが単一障害点となりうる．第二に，サードパーティーにアイデンティティ情報が集約されるため，サードパーティーが情報を独占し，サードパーティーの力が強まる懸念がある．第三に，V2X ネットワークは国家を跨り構築されるものであり，国家間の競争などに巻き込まれ，サードパーティーの独立性を確保し続けるのが困難であると考えられる．

そこで我々は，中央集権的なアイデンティティ管理ではなく，自己主権型の ID 管理機構を用いて V2X ネットワークのアイデンティティ管理を行う方法を検討した．それが今回提案するアーキテクチャ ZTA/SSI となる．まずは自己主権型 ID の概要について説明する．

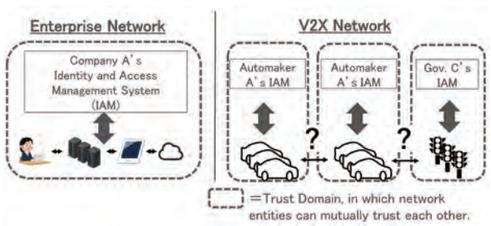

Fig. 2 Difference between Enterprise and V2X Network

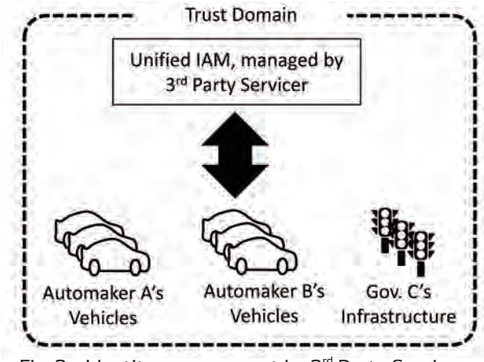

Fig. 3 Identity management by 3rd Party Servicer

自己主権型 ID の概要

自己主権型 ID（Self-Sovereign ID：SSI）とは現在主流の中央集権的なアイデンティティ管理と対極をなすアイデンティティ管理手法の枠組みである．中央集権的な存在を介さずにユーザー自らが自身のアイデンティティ情報を管理しコントロールすることを目指すものである．

自己主権型 ID を構成する要素とその関係性を，Fig. 4 に示す．

ISSUER は HOLDER のアイデンティティ情報に関する証明書（Verifiable Credential：VC）を発行する機関である．ISSURE は事前に自身を示す DID（Decentralized IDentifier）とそれに紐づく秘密鍵と公開鍵を生成し，そのうち DID と公開鍵を DID Document として Verifiable Data Registry に登録しておく．HOLDER への VC の発行の際，Verifiable Data Registry に登録しておいた公開鍵に紐づく秘密鍵で VC をデジタル署名する．

HOLDER はアイデンティティの管理主体であり，様々な ISSURE から発行された自身のアイデンティティに関する VC を保管・管理する．

VERIFIER は HOLDER がアイデンティティ情報を証明したい相手であり，HOLDER は VERIFIER に対して VC の内容を Verifiable Presentation（VP）として提示する．VERIFIER は VP の発行元として記された ISSURE の公開鍵を Verifiable Data Registry から取得し，証明書の署名の正当性を確認する．VERIFIER は，ISSURE を信用していれば，その示されたアイデンティ

ティ情報を信用することが可能になる．

以上のようなスキームにより，HOLDER が自身のアイデンティティを管理し，証明することが可能になる．

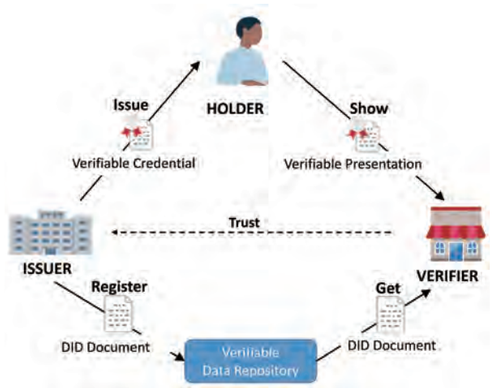

Fig. 4　Relationship among core components in SSI

ZTA/SSI

ここで我々は自己主権型 ID を応用することで V2X ネットワークの参加者が各々で自身のアイデンティティを管理し，その情報に基づいて通信の可否を都度判断するアーキテクチャを検討した．このようなアーキテクチャにより，前述のような V2X ネットワークで不特定多数のステークホルダが存在することの困難を解消しつつ，ZTA に基づいた強固なセキュリティを確保できると考えている．我々はこのようなアーキテクチャを ZTA/SSI と呼んでいる．

ZTA/SSI の基本的な構成と処理の流れを Fig. 5 に示す．

ここでは簡単な例として異なる車両メーカーの車車間通信を考えている．メーカー A 製の車両 X からメーカー B 製の車両 Y に対して通信要求を行うことを想定する．この場合，ISSURE が A 社となり，HOLDER が車両 X，VERIFIER が B 社という関係となる．

以下にアクセス許可までのフローを示す．

1. A 社は予め自身の DID Document を Verifiable Data Repository に登録しておく（Fig. 5 ①）．
2. A 社は自身の IAM（Identity and Access Management system）で車両 X のアイデンティティ情報を管理しており，そのアイデンティティ情報を VC として車両 X に対して発行する．VC を受け取った車両 X は自身で VC を保持・管理する（Fig. 5 ②）．
3. 車両 X から車両 Y にアクセスを要求する．その際自身の管理している VC の中から，車両 Y へのアクセスに必要な情報のみを VP として抜き出し，車両 Y 上に配置された PEP に提示する（Fig. 5 ③）．
4. PEP は B 社の管理する PDP に VC の検証を依頼する（Fig. 5 ④）．
5. PDP は Verifiable Data Repository から A 社の DID Document を取得する（Fig. 6 ⑤）．
6. 取得した DID Document をもとに VP の署名を検証することで提示された VP が A 社により正しく署名されたものであることを確認する．署名の正当性が確認できれば VP の内容を確認し通信要求のための要件を満たしているか否かを判断し，結果を PEP に返す．PEP は PDP の判断をもとに車両 X からのアクセスを許可・拒否する（Fig. 5 ⑥，Fig. 5 ⑦，Fig. 5 ⑧）．

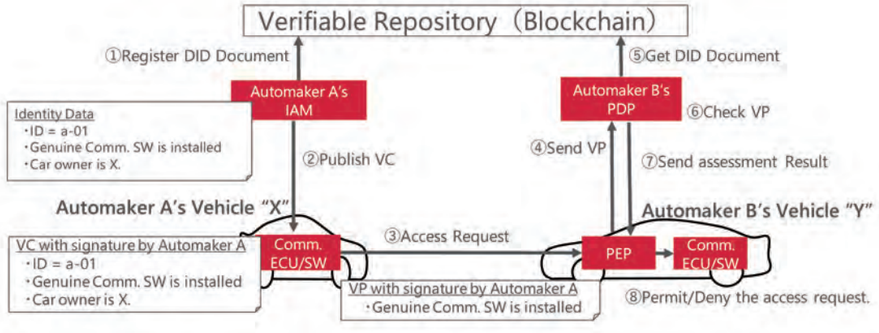

Fig. 5　Access control flow in ZTA/SSI

ZTA/SSI の嬉しさ

以上が ZTA/SSI の処理の流れであるが，対比として，同様の通信を A 社 B 社共通で信頼できるサードパーティーにより中央集権的に ID 管理した場合の ZTA の構成を Fig. 6 に示す．

この場合，A 社の持つ機密情報である A 社車両のアイデンティティ情報をサードパーティーに預ける必要がある．さらに A 社が預けた情報のうちどの情報を B 社に渡すかはサードパーティーがコントロールすることになる．つまり A 社が情報の流通を直接コントロールできないところが，サードパーティーによる管理の最大の難点となる．

一方で Fig. 5 からわかるように，ZTA/SSI を採用した場合，A 社の車両のアイデンティティ情報は A 社と A 社製の車両 X のみに閉じていることが分かる．不必要な情報を他社に渡すことなく，通信に必要な情報のみを公開して通信の信頼性を確保することが出来る．

V2X ネットワークにおいて，そのセキュリティを ZTA により担保しつつ，各ステークホルダが自身の持つ情報の流通をコントロールしたいという要求を同時に満たすのが ZTA/SSI のアーキテクチャである．

我々は安心安全 V2X ネットワークの実装に向けて，ZTA/SSI は必須のアーキテクチャとなると考えている．

おわりに

本論文では，車両が様々なモノと接続する V2X ネットワークが実装される時代見据えたとき，これまで主流であった境界型防御ではセキュリティを確保することが難しいこと，そして ZTA という新たなセキュリティの枠組みを導入することが必要であることを示した．

さらに V2X ネットワーク固有の問題として不特定多数のステークホルダが存在することを挙げ，そのような NW に ZTA を適用するための自己主権型 ID（SSI）を応用した新しいアーキテクチャ，ZTA/SSI を提案した．

これは V2X ネットワークにおいて，そのセキュリティを ZTA により担保しつつ，同時に各ステークホルダが自身の保有する情報の流通をコントロールしたいという要求を満たすことが出来るアーキテクチャとなっている．

本論文では ZTA におけるアイデンティティ管理部分のみを取り上げた．しかし V2X ネットワークへの ZTA の実装に向けては，車載 NW の ZTA の設計と車両のトラストスコアの計算手法，リアルタイム処理に対応したクレデンシャル情報の受け渡しの効率化など，検討するべき事項は多く残されている．

これらの多くは V2X ネットワークの仕様として標準化されていくものであると考えられる．そのため，標準化の動向を注視しつつこれらの課題に対する技術開発を行っていくことで安心安全な V2X ネットワークの実現に向けた基盤技術の更なる進化を図っていく．

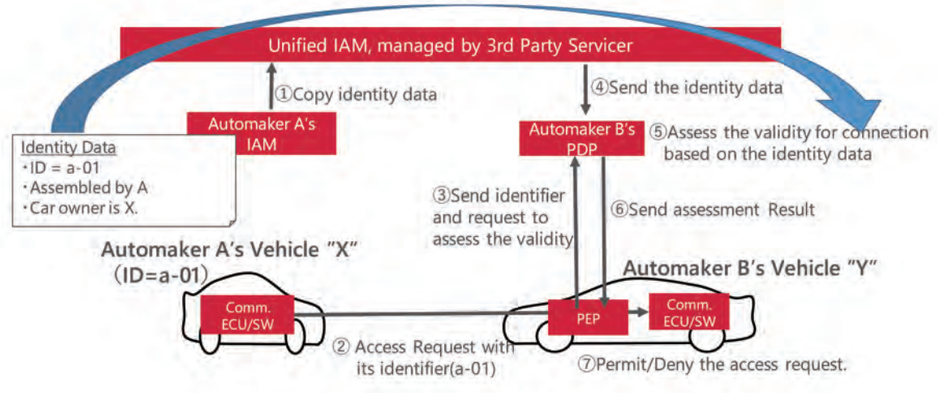

Fig. 6　Access control flow

参考文献

i　自動車部品メーカとしてのセーフティ & セキュリティの活動紹介
https://www.ipa.go.jp/sec/old/users/seminar/seminar_tokyo_20151207-04.pdf

ii　Remote Exploitation of an Unaltered Passenger Vehicle
https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

iii　SP 800-207 Zero Trust Architecture
https://csrc.nist.gov/publications/detail/sp/800-207/final

iv　ゼロトラストの現状調査と事例分析に関する調査報告書
https://www.fsa.go.jp/common/about/research/20210630/zerotrust.pdf

著者

三谷 陽
みたに あきら

AI 研究部 博士（理学）
データ分析や AI 技術の開発に従事

愛知 功
あいち いさお

AI 研究部
車両のセキュリティ・プライバシー保護
技術開発に従事

澤井 佑樹
さわい ゆうき

AI 研究部
車両のセキュリティ・プライバシー保護
技術開発に従事

石田 晋哉
いしだ しんや

クラウドサービス部 博士（情報科学）
クラウドサービスの開発，社内の開発現場・プロセスの改善に従事

山下 克司
やました かつし

山下技術開発事務所 代表
DENSO 技術顧問としてアーキテクチャと技術知見の提供に従事