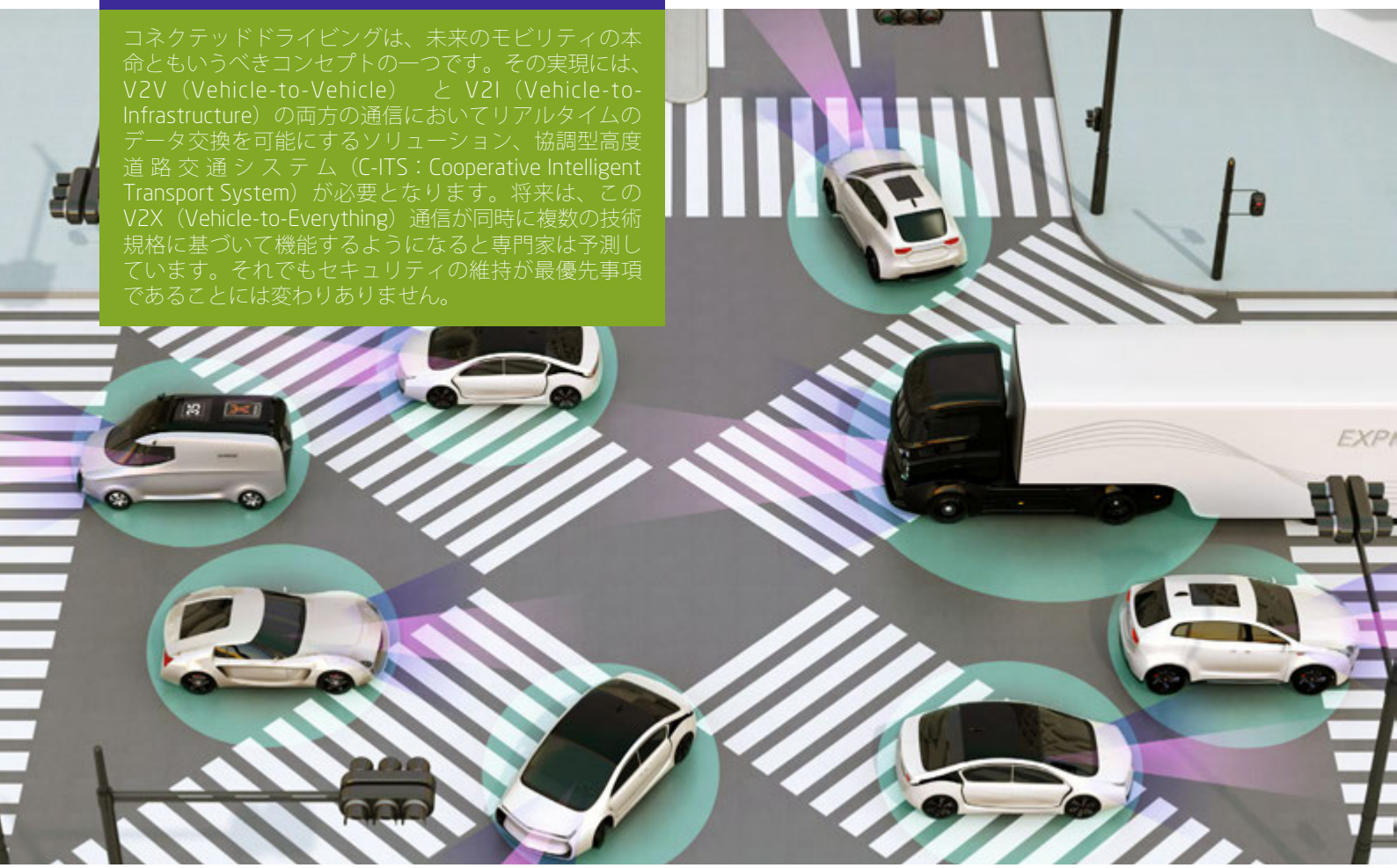
ハイブリッド V2X 通信のためのセキュリティ

コネクテッドドライビングの汎用データ通信を標準ソリューションで実現

コネクテッドドライビングは、未来のモビリティの本命ともいうべきコンセプトの一つです。その実現には、V2V（Vehicle-to-Vehicle）と V2I（Vehicle-to-Infrastructure）の両方の通信においてリアルタイムのデータ交換を可能にするソリューション、協調型高度道路交通システム（C-ITS：Cooperative Intelligent Transport System）が必要となります。将来は、この V2X（Vehicle-to-Everything）通信が同時に複数の技術規格に基づいて機能するようになると専門家は予測しています。それでもセキュリティの維持が最優先事項であることには変わりありません。



これまで V2X の直接通信には主に、ITS-G5 という、専用狭域通信（DSRC：Dedicated Short-Range Communication）規格が使用されてきました。つまり、沿道に設置された装置と車両とが基本的に直接無線 LAN 通信でデータを交換します。しかしこの状況は変わろうとしています。V2X データ通信に加え、高速無線通信のための LTE-V 規格（現在は 4G、間もなく 5G）を併用する取り組みが既に進んでいます。LTE-V 規格に準拠した無線チップがデバイスに搭載されていれば、デバイス同士が直接データを送受信する「アドホックデータ交換（C-V2X Autonomous）」という形で、車以外の道路利用者（歩行者、自転車など）を通信プロセスに含めることができるようになるのです。この混合通信のコンセプトは、今後も数多く標準化され、追加されていくでしょう。例えば、MEC（Mobile Edge Computing）を使い、近距離セルラーネットワーク経由でメッセージ（渋滞警告など）を配信したり、携帯電話の基地局を介した従来の無線通信を使ってバックエンドサービスやクラウドと通信を行ったりすることが挙げられます（図 1 参照）。

一貫性のあるインテリジェントな構造のプロトコルスタック

特定のユースケースとエンティティに応じて、異なるチャンネルや規格への対応を意図したさまざまな V2X 通信が登場すると考えられます。そうなれば当然、そのようなハイブリッド V2X 通信のセキュリティを最も効率のよい方法で確保するにはどうすればよいか、という問題が浮上します。異なる伝送チャンネルにそれぞれ独自のセキュリティソリューションを適用するのは、どう見ても正しいやり方ではないでしょう。そこで求められるのは、ユースケースの違いにかかわらず V2X 通信の全領域で効果的に作用するセキュリティの概念なのです。

そうなれば当然、そのようなハイブリッド V2X 通信のセキュリティを最も効率のよい方法で確保するにはどうすればよいか、という問題が浮上します。

解決の鍵は、あらゆる V2X デバイスとエンティティ間の V2X 通信で用いられるプロトコルスタックに、一貫性のあるインテリジェントな構造を持たせることにあります（図 2 参照）。V2X メッセージは、アプリケーションレベルまたはデバイスレベルで生成されて、トランスポート／トランスミッションレベルに中継されます。そこで各 V2X メッセージに、セキュリティコンポーネントインターフェースを介してセキュリティヘッダが追加されます。ヘッダには、メッセージの署名や関連する証明書が含まれています。また必要であれば、第 2 のステップでメッセージを対称的に暗号化することもできます。V2X メッセージを受信者が復号できるよう、ヘッダには対称キーに関連した情報が追加されます。V2X ネットワーク経由で通信を行うエンティティの

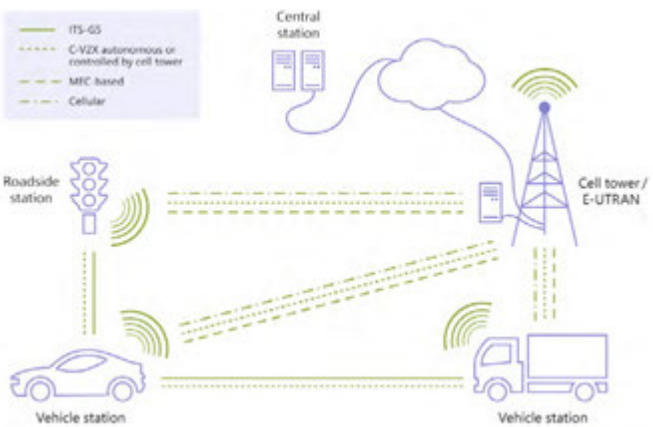


図 1：ハイブリッド V2X 通信のアーキテクチャ

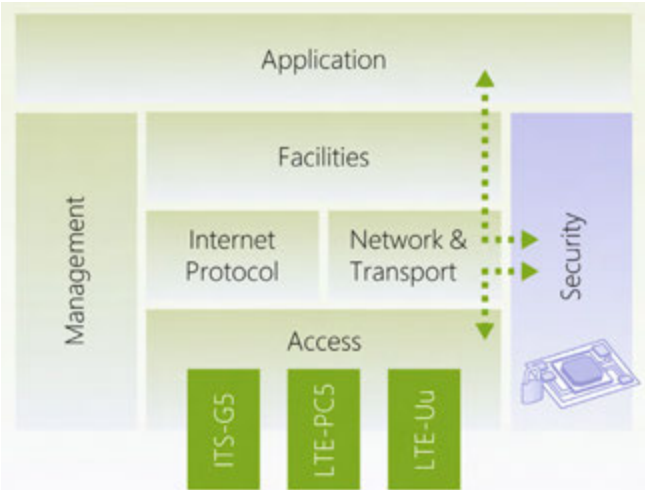


図 2：ハイブリッド通信での一貫した V2X セキュリティを実現するソフトウェアスタック

データを確実に保護するために、各 V2X メッセージには、暗号化の前に署名が追加されます。ハイブリッド通信ネットワーク内であっても、この方法なら、V2X データ交換に求められるセキュリティ要件（データの完全性、送信者の信憑性、送信者の認証、再生検出、機密性、プライバシー保護、信頼性、信頼の失効）はすべて満たされます。

CONCORDA プロジェクトでの路上試験

車両のハイブリッド通信は、コネクテッドドライビングのための実用的で役に立つ技術です。より多くのシステムや道路利用者、サービスを V2X データ交換に統合するための道を開くことになります。同時に IT セキュリティは、これまでも、そしてこれからも、V2X にとって必要かつ最も重要な条件であり続けるでしょう。インテリジェントな概念を確立すれば、結果として、V2X のさまざまな通信チャンネルと規格の垣根を越え、均質で一貫した効率的な IT セキュリティがもたらされます。

オランダ、ベルギー、ドイツ、フランス、スペインでは現在、CONCORDA（Connected Corridor for Driving Automation）プロジェクトとして、テストルートで実験が進められています。CONCORDA は欧州連合から一部資金提供を受けており、ESCRYPT、Deutsche Telekom、Nokia、Bosch、Volkswagen を含む複数の企業が協同で行っています。2020 年の半ばまでには、ITS-G5、LTE 接続、そして一貫性のある IT セキュリティアーキテクチャを備えたハイブリッド V2X 通信システムが、その役割を実際にどのように果たすかが、CONCORDA によって示されるでしょう。

執筆者

Dr. Norbert Bißmeyer、ESCRYPT、プロジェクトマネージャ
Jan-Felix van Dam、ESCRYPT、セキュリティエンジニア