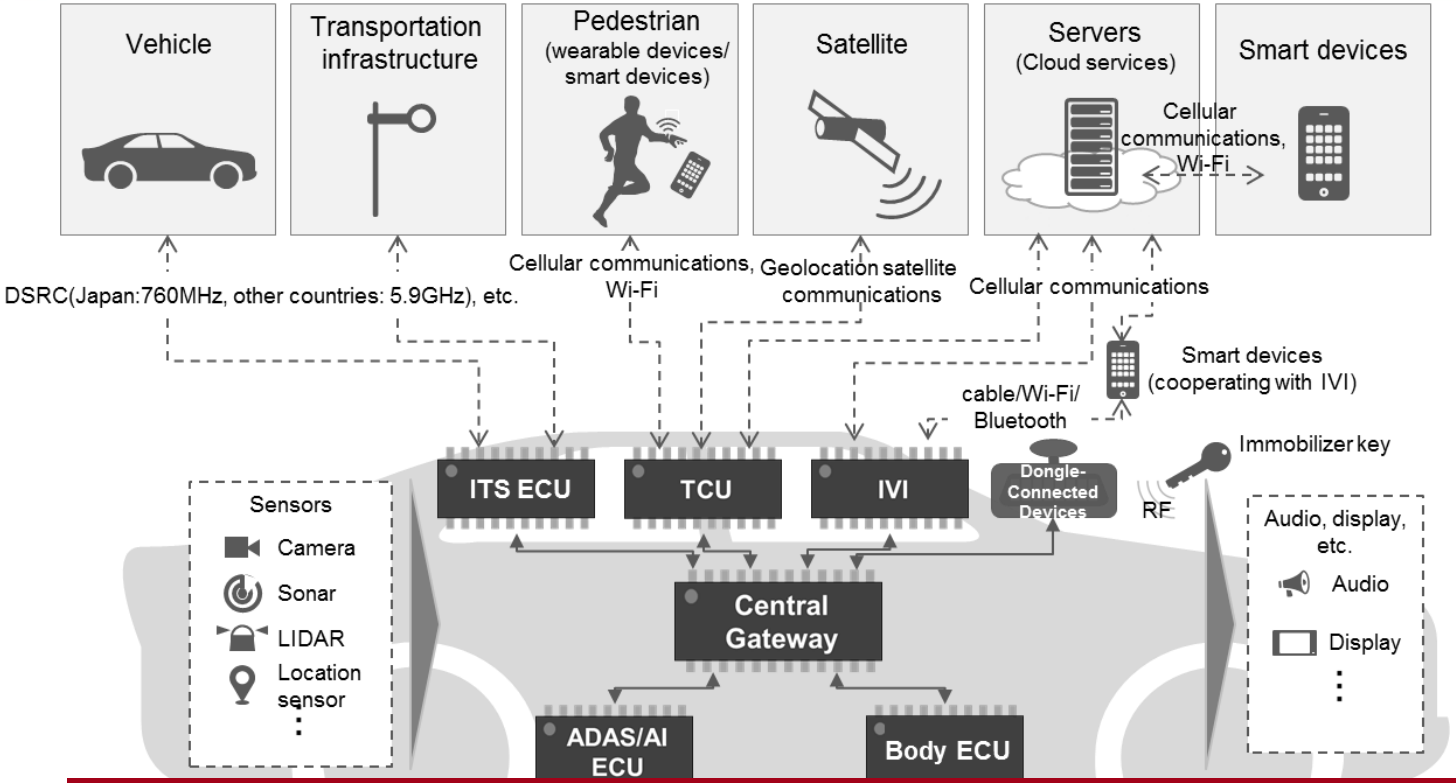
Cybersecurity

J-Auto-ISAC / トヨタ自動車　上原　茂

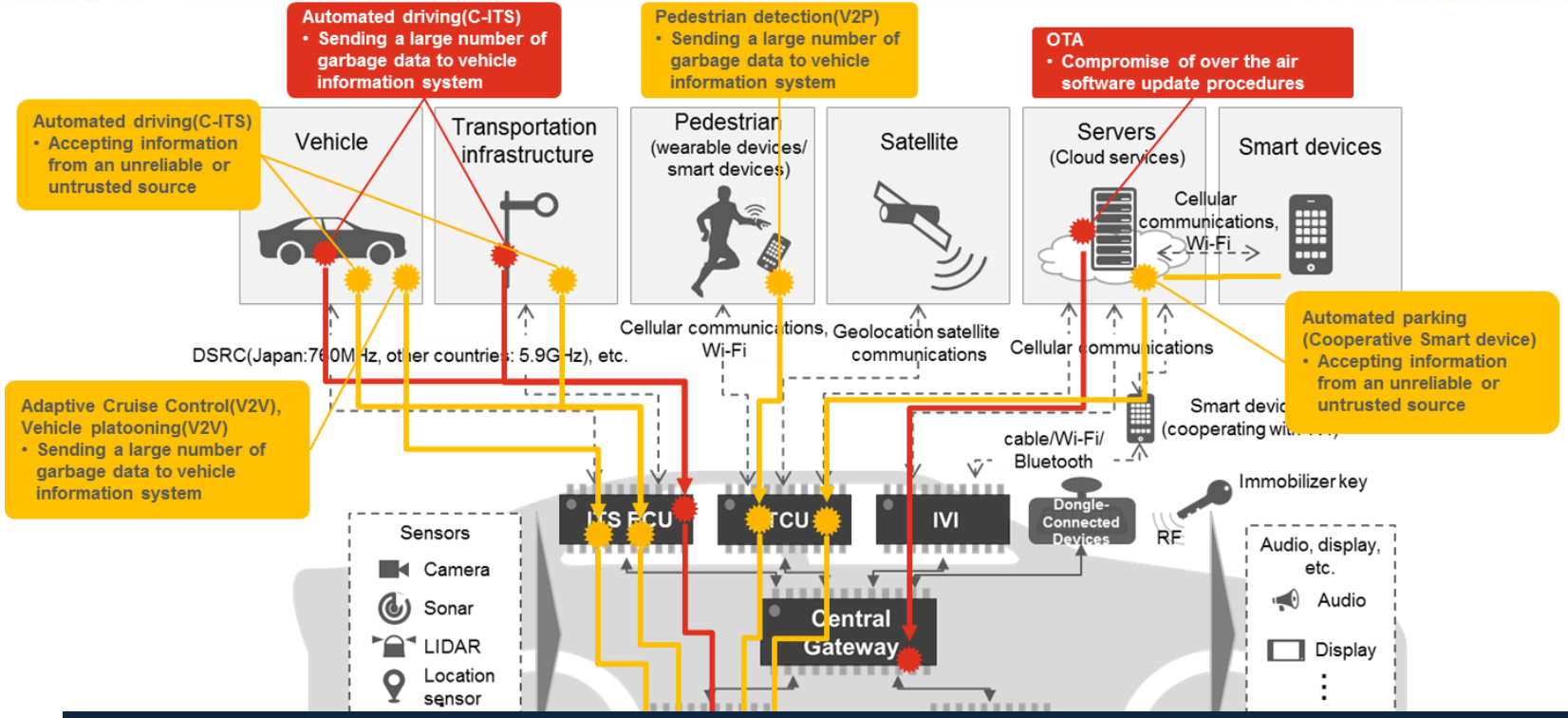
NEDO SIP Cabinet Office

自動運転機能のシステム構成



外部インフラとの通信で自動運転は成立している

多岐に渡る侵入経路



攻撃者は常に新たな攻撃手法を見つけ侵入してくる
我々は攻撃され被害が出るまで気がつかない

攻撃者の視点：クルマを攻撃する動機

金銭目的

金融システムにおける不正送金などとは違い、
車両への攻撃によって直接お金が儲かるという事はなく
金儲けが目的であれば、車両を攻撃するという事は
プライオリティ的には高いとは言えない

（金銭を受け取り、犯罪を犯すような受託犯罪は除く）

攻撃者の視点：クルマを攻撃する動機

愉快犯

取り締まり当局の捜索技術も向上しており、その状況下で
愉快目的だけで 敢えてリスクを冒すとは考えにくい

また、いたずら程度のサイバー攻撃では社会的に注目されなくなってきているのが現状

愉快目的という動機は弱い

攻撃者の視点：クルマを攻撃する動機

売名目的

売名目的のケースを考えると
売名目的の多くのケースは　攻撃者が自分の技術力を誇示し
関係者にそれを見せつけ　最終的に何らかの利益を合法的に得よう
というもの（その会社とサイバーセキュリティの技術コンサルタントとして契約するなど）

これが動機としては一番高いと思われる

攻撃者の視点：クルマを攻撃する動機

さらに

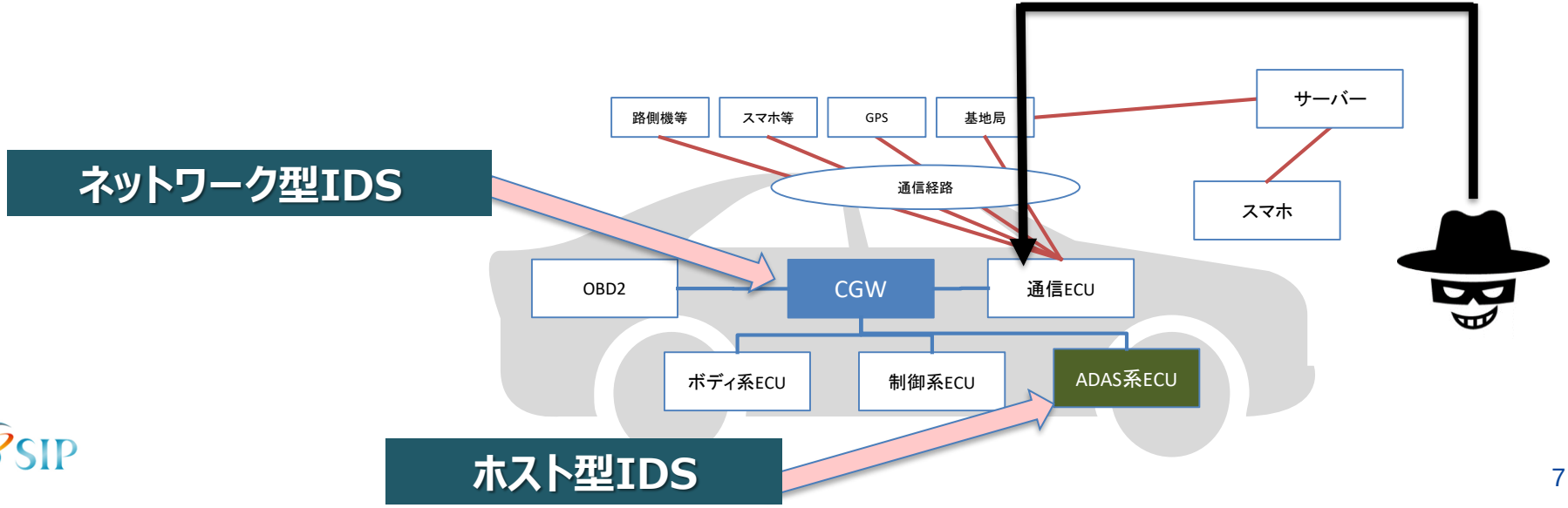
この売名目的のケースの多くは　技術的に高度な攻撃であり、
予測し先回りして防御する事は難しい

一方で　攻撃者は売名目的であるので、攻撃後 必ず名乗り出て来る
また、こちらからの連絡にも応答してくる

よって、
仮に我々が早期に攻撃を検出でき、攻撃者と連絡を取ることができ、
最終的に良い関係が構築できれば、サイバー攻撃による被害を出さずに
対策をうつ事ができる

防御側の視点：技術力の高い攻撃に対し何ができるか

防御側の我々には 外部から侵入された事を いち早く知る手段として
IDS (Intrusion Detection System)があり、
いち早く侵入を検知し、被害拡大・拡散を防止する為に開発者が
現状対応できる数少ない手段の一つと考えられる。



Video Plenary Session

まず最初に　IDSテストベッドを使った
デモVideoを見て頂いてから、
IDSの今後の“目指すべき方向性”などに
ついてサイバーセキュリティにおける各分野
の4名の専門家のプレゼンテーション動画
を見ていただきます

（ビデオ撮影協力 ： PwCコンサルティング、トヨタ自動車）

IDSテストベッド

講演者

◆ Mr.Nishant Khadria

Senior Manager,Risk Advisory, Deloitte Germany

◆ Mr.Robert Shein

Senior Manager,Consulting-Technology, PwC USA

◆ 川名茂之

日本自動車工業会　電子安全性分科会長

◆ 松本　勉

横浜国立大学　教授

セッション スタート

NEDO SIP Cabinet Office