当社作成の制御セキュリティ規格 IEC 62443 に準拠したセキュリティコンセプト文書の国際認証機関による技術レビュー結果として「技術的に正しい」とのコメントを取得

～戦略的基盤技術高度化支援事業の成果を利用して国際認証機関から取得～

株式会社ヴィッツ
執行役員　武田英幸

開催場所：ESEC会場内 Press room

御説明内容

株式会社 ヴィッツ

■セキュリティコンセプト文書の国際認証機関による技術レビュー結果

1. 社会的背景：JEEPへのサイバー攻撃（ハッキング事例）
2. TÜV SÜDの技術レビューについて
3. TÜV SÜDの認証について
4. IEC 62443全体像
5. システム構成
6. SafetyとSecurityの違い
7. 組み込みセキュリティのポイント 1/2
8. 組み込みセキュリティのポイント 2/2

■組込みセキュリティ導入支援サービス 正式開始

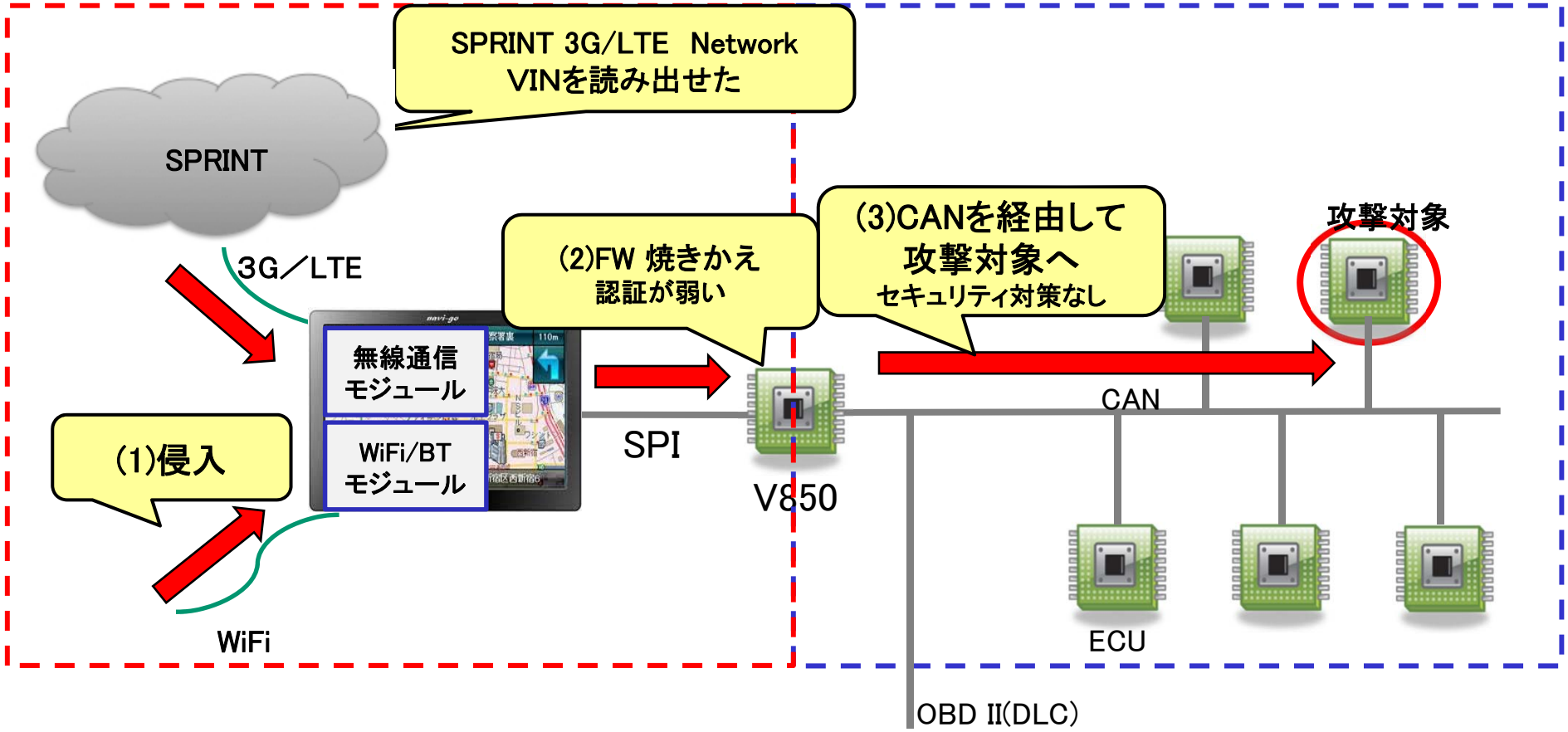
1. サービス内容 1/3
2. サービス内容 2/3
3. サービス内容 3/3

■戦略的基盤技術高度化支援事業

1. 謝辞および前提条件
2. 研究プロジェクトの概要
3. 開発体制(川下産業と川上産業のコンソーシアム)

社会的背景 JEEPへのサイバー攻撃（ハッキング事例）

株式会社 ヴィッツ



http://illmatics.com/Remote%20Car%20Hacking.pdf

TÜV SÜDの技術レビューについて

株式会社 ヴィッツ

■国際認証機関の技術レビューを受けた目的

- （株）ヴィッツが国際標準規格であるIEC 62443が求める技術水準を有する事を国際認証機関に客観的に認めてもらう事。
- 技術レビューは、Certificate同様、アセッサ2名がアセスメントの形式で行う。また、上流工程のセキュリティコンセプトに対して、実施される。
- 現在、自動車向けに特化したセキュリティ規格はない為、IEC 62443のプロダクト認証、プロセス認証ではなく、技術レビューまでで妥当と判断。
- ISO 15408(Common Criteria)は、PP(Protection Profile)即ちセキュリティ要求以降を規格化しており、上流工程が規格化されているIEC 62443を選択。

■技術レビュー結果の抜粋

5.2 Review result

		Decision:	Yes	No
Review accepted			☐	☐
	With modifications		☒	

5.3 Review summary and next steps

This review shows that in general the SMP now is correct (only two minor findings 107/108). The review of the SRS and SAD shows that in general

- the approach of the security requirement specification and the derivation of security countermeasures is understandable and correct
- the security architecture is described quite well

TÜV SÜDの認証について

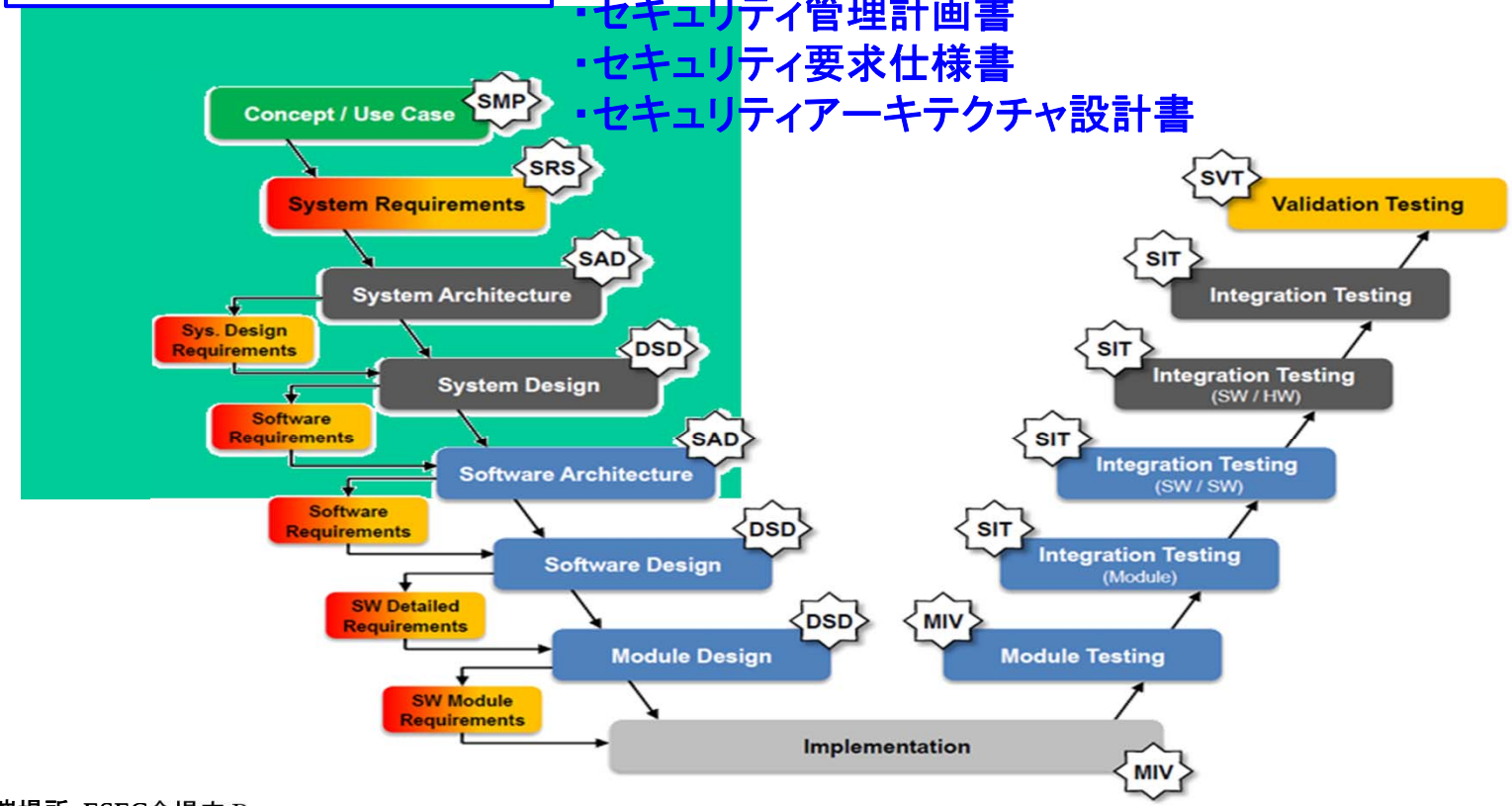
株式会社 ヴィッツ

■IEC 62443に対するアセスメント

- 製品認証（Product Certificate）
- プロセス認証（Process Certificate）
- 上記2つの認証の前に、上流工程のセキュリティコンセプトに対し、Certificate同様アセスメントの形式で技術レビューが行われる

セキュリティコンセプトの範囲

- セキュリティ管理計画書
- セキュリティ要求仕様書
- セキュリティアーキテクチャ設計書

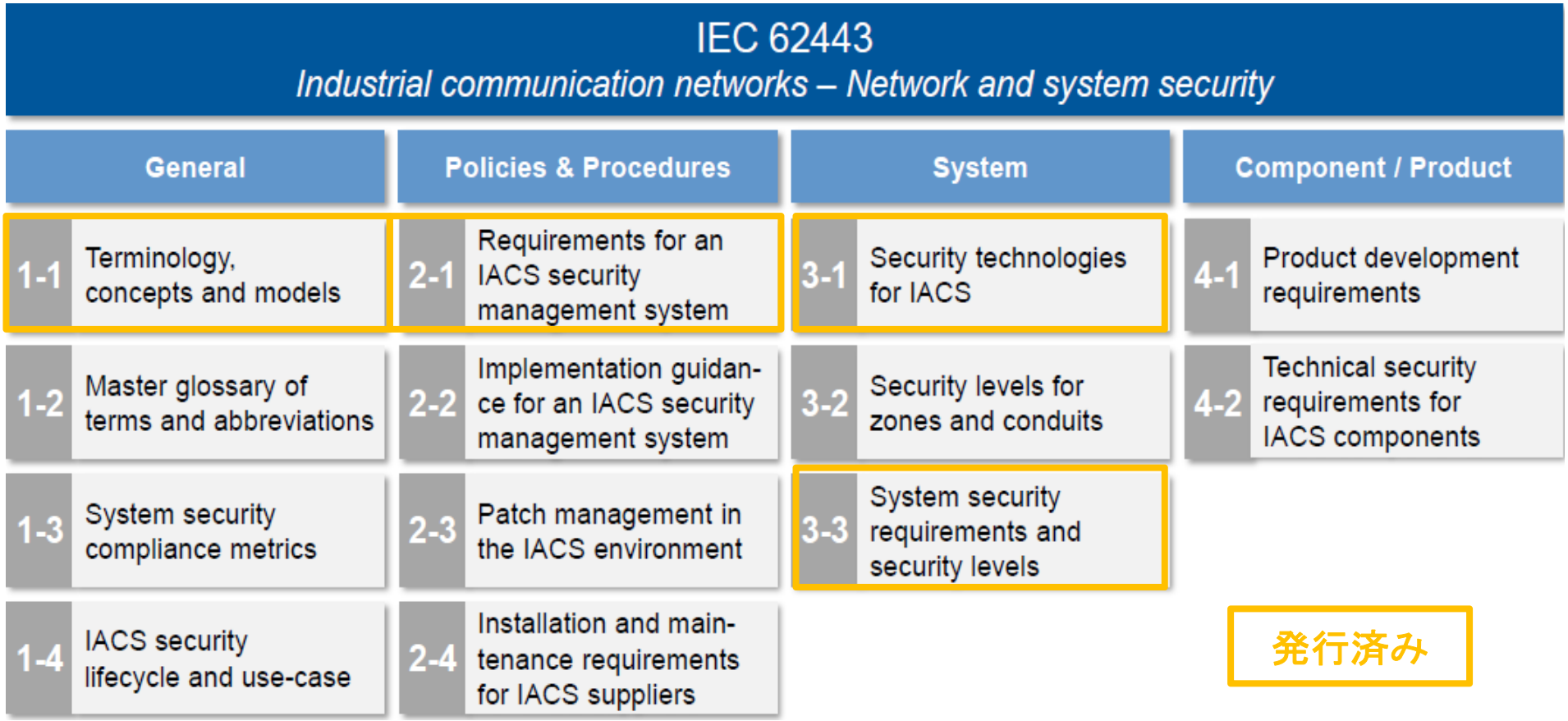


IEC 62443　全体像

株式会社 ヴィッツ

■IEC 62443はPart 1～Part 4の4シリーズが存在する。

- シリーズがさらに細分化されている。
- 発行済みのもの以外は、規格化が進行中。



IACS：Industrial Automation and Control System

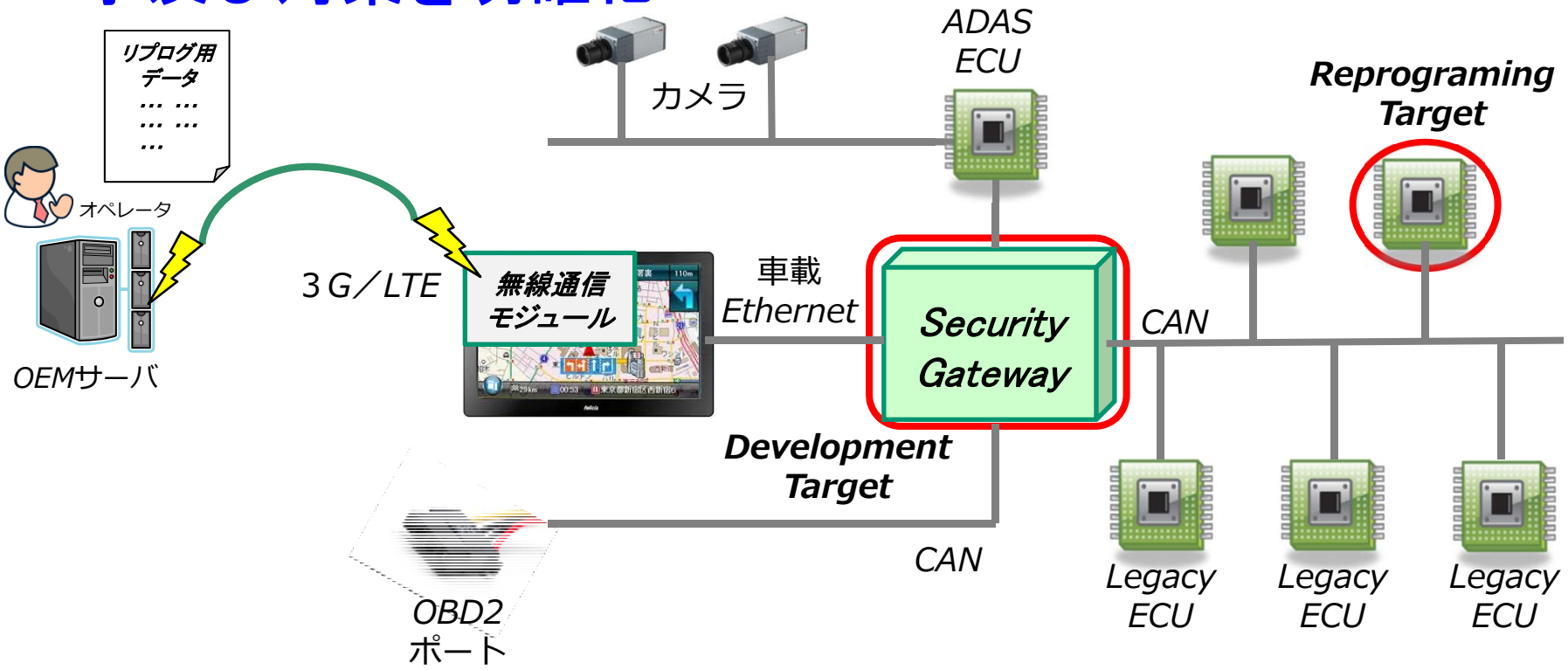
システム構成

株式会社 ヴィッツ

■遠隔リプログラミングシステム

– 「車両整備工場へ行かずに自宅等でECUのリプログラミングを可能にする」

このシステム構成でSecurity Gatewayのセキュリティ要求及び対策を明確化



SafetyとSecurityの違い

株式会社 ヴィッツ

■SafetyとSecurityの文化

- 機能安全対応は難しい。しかし、Securityはその100倍は難しい。
  なぜなら対象範囲を絞ることが出来ず、システム全体と、
  その全てのユースケースを想定して考えなければならない。
  その上、クレイジーな悪人を相手にしなければならない。

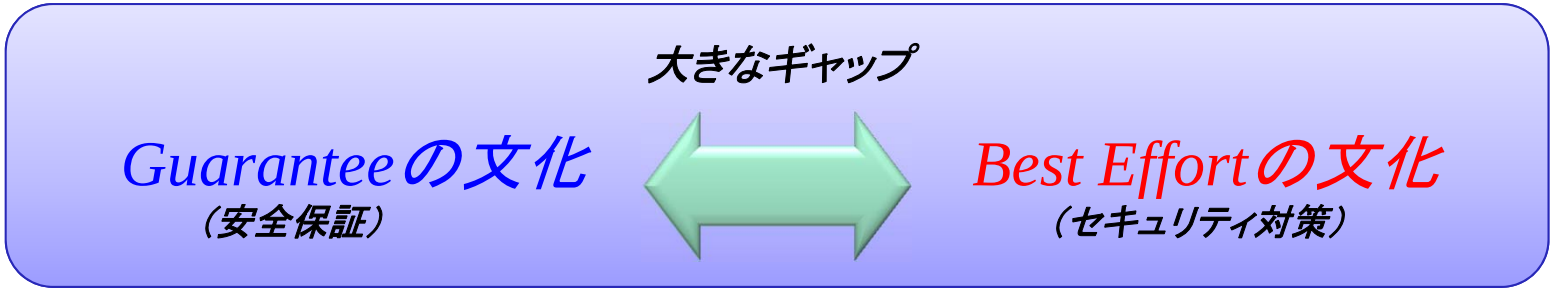
※TÜV SÜDアセッサのコメント

Safety

- *Precise targets because of well understood threats.*

Security

- *Moving targets because of new threats from malicious people result in less practical guidance.*
- *Application engineers ask, however, for more practical guidelines.*



Clash of Cultures *(Rainer Faller氏(exida社)の資料より)*

組込みセキュリティのポイント 1/2

株式会社 ヴィッツ

■開発技術

（1）セキュリティ要求の導出には、脅威分析が必要。

脅威分析には、前提となるユースケース、想定システムの定義が必要であり、また、脅威分析での抽象化のレベル、相場観の把握が困難。更に攻撃手法の知識が必要。

=> 戦略的基盤技術高度化支援事業の採択テーマとして実施している「高度IT融合社会の安心安全を支える次世代自動車用セキュリティ・ゲートウェイ・ECUの開発」にて、脅威分析に対するセキュリティエキスパートのアドバイザー様によるレビュー、TÜV SÜDのレビューにより獲得。

=> 攻撃手法は、論文、CWE(Common Weakness Enumeration)を調査。

（2）セキュリティ対策の実現には、他の規格に精通しなければならない。

※ IEC 62443のみで、セキュリティコンセプトは作成できない

BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

SHE(Security Hardware Extension)

ISO/IEC 11770-2 Information technology Security techniques Key management Part 2: Mechanisms using symmetric techniques

組込みセキュリティのポイント 2/2

株式会社 ヴィッツ

■組込みセキュリティ実現の困難性

－システムが持つ処理性能の違い

Item	ITシステム	組込みシステム
CPU (Clock)	1~8 Core (~3GHz)	1Core (80MHz)
Memory	Main Memory (~8GB)	Internal RAM (256KB)
Storage	HDD / SSD (256GB)	Flash ROM (2MB)
User Interface	GUI	Not supported
Boot Loader	Using	Not used
Execution	On the Main Memory	On the Flash ROM

ITシステムの分野では古くからセキュリティに対する取り組みが成されており、多くの技術（ノウハウ）が集められている。しかし、それらの技術はITシステム環境上で実行することを前提に考えられており、スペックに大きな差がある組込みシステムにそのまま適用することは困難である。

=> ヴィッツでは、長年経験してきた組込みシステムのリソースを考慮した最善のセキュリティアーキテクチャの提案が可能。

組込みセキュリティ
導入支援サービスについて

株式会社ヴィッツ
執行役員　武田英幸

開催場所：ESEC会場内 Press room

サービス内容　1/3

株式会社 ヴィッツ

■概要

株式会社 ヴィッツ（本社：愛知県名古屋市、代表取締役社長：服部 博行、以下ヴィッツ）は、自社が事業管理法人を勤めている平成26～28年度 戦略的基盤技術高度化支援事業（中小企業基盤整備機構）「高度IT融合社会の安心安全を支える次世代自動車用セキュリティ・ゲートウェイ・ECUの開発」での組込みセキュリティの開発経験及びその活動の上流工程で作成したセキュリティコンセプト文書のドイツ TÜV SÜD（ミュンヘン）による技術レビュー経験を活かして、組込みセキュリティの導入支援サービスを2016年5月より正式に開始。

■サービス内容

(1)教育

分類	内容
Step1:イントロダクション	自動車セキュリティ概論
Step2:業界動向の解説	IEC 62443の解説
	ISO 15408の解説
	SAE J3061の解説
	EVITAの解説
	AUTOSARの解説（特にSecOC）
Step3:セキュリティ方法論	脅威分析方法の解説
	セキュリティアーキテクチャの組み方
	暗号鍵の管理方法の解説

サービス内容 2/3

株式会社 ヴィッツ

■サービス内容

(2) 開発技術

工程	固有技術
SRS:Security Requirement Specification	脅威分析によるセキュリティ要求の導出
SAD: Security Architecture Design DSD: Detailed Software Design MIV: Module Implementation Verification	CWE(Common Weakness Enumeration)を用いた既知の脆弱性チェック
MIV: Module Implementation Verification	CERT-C、セキュアコーディング
SIT: Security Integration Test	Fuzz、Penetrationを用いた脆弱性検証

(3) 車載技術

技術	内容
AUTOSAR	AUTOSAR SecOC
CAN通信	メッセージ認証
鍵管理、鍵交換	SHE(Security Hardware Extension) ISO/IEC 11770-2
認証	ECU相互認証

サービス内容 3/3

株式会社 ヴィッツ

■サービス内容

(4) プロセス構築

お客様の既存の開発プロセスとのギャップ分析を行い、プロセス構築のスタートなるSMP(Security Management Plan)の作成支援から開始し、各工程でのガイドライン作成を支援。

(5) 組織運用

製品を如何に堅牢に作ろうとも、開発中や製品リリース後に暗号鍵が漏洩してしまえば、セキュリティは保てません。
鍵管理の組織運用やインシデント発生時に対処を中心となっておこなうSIRT(Security Incident Response Team)の構築支援を実施。

■今後のサービス拡張について

株式会社ヴィッツでは、自動車業界向けの組込みセキュリティ支援から開始します。今後のIoT/CPS社会では、莫大な数の組込み製品がネットワークにつながります。今後、ドローン、ロボットなど様々な製品に対し、ヴィッツの組込みセキュリティ技術を適用する支援を行い、安心、安全な社会作りに貢献。

戦略的基盤技術高度化支援事業
「高度IT融合社会の安心安全を支える次世代自動車用セキュリティ・ゲートウェイ・ECUの開発」
について

謝辞および前提条件

株式会社 ヴィッツ

国際認証機関による技術レビューに際し、経済産業省・（独）中小企業基盤整備機構の戦略的基盤技術高度化支援事業の採択テーマとして実施している「高度IT融合社会の安心安全を支える次世代自動車用セキュリティ・ゲートウェイ・ECUの開発」の成果を活用しました。

研究実施プロジェクトのメンバならびにアドバイザ各位

<u>メンバ組織</u>

（株）ヴィッツ、立命館大学、（株）アトリエ、産業技術総合研究所

<u>アドバイザー組織</u>

スズキ（株）、アイシン精機（株）、アイシン・コムクルーズ（株）
三菱電機（株）、（株）KDDI研究所、名古屋大学

<u>オブザーバー組織</u>

ソニーデジタルネットワークアプリケーションズ（株）

研究プロジェクトの概要

株式会社 ヴィッツ

プロジェクト名

高度IT融合社会の安心安全を支える次世代自動車用セキュリティ・ゲートウェイ・ECUの開発

目的

東京オリンピックを4年後に控えた今、次世代自動車システムの制御乗っ取りを狙うインターネット等を介したサイバー攻撃は現実の脅威である。本研究では有効な防衛策として、わが国が先行する対攻撃性の高いハードウェア暗号技術とソフトウェアによる保護技術を効果的に組合せた「セキュリティ・ゲートウェイ・ECU」を開発する。国際規格にも準拠することで、高度IT融合社会の安全・安心を、国境を越えて築くための中核技術とする。

開発成果物

(1)IEC 62443準拠のセキュリティコンセプト文書(セキュリティ管理計画書、セキュリティ要求仕様書、セキュリティアーキテクチャ設計書)

(2)PUF(Physical Unclonable Function)を活用した暗号演算回路

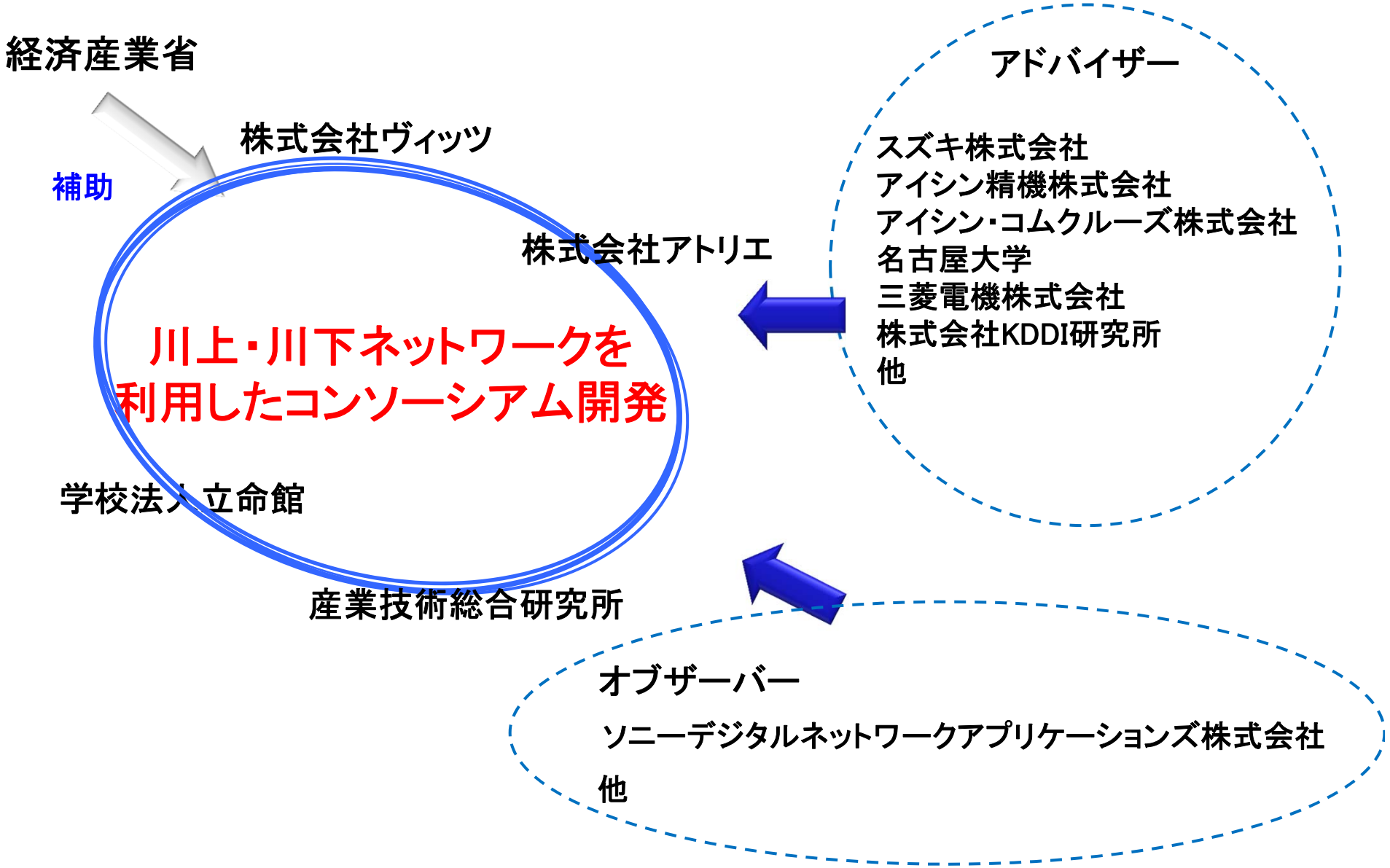
(3)遠隔リプログラミングシステム

予算

経産省からの補助金及び自社費用

開発体制（川下産業と川上産業のコンソーシアム）

株式会社 ヴィッツ



本発表への問い合わせ先

株式会社 ヴィッツ

総合問い合わせ先

株式会社ヴィッツ

総務部：脇田、佐藤　(052) 220-1218

技術的問い合わせ先

株式会社ヴィッツ

組込セキュリティPF開発部：　武田(takeda@witz-inc.co.jp)

(052) 220-1218

ご静聴ありがとうございました

本内容についてのご質問は下記にお願いします

株式会社ヴィッツ

Tel: 052-220-1218

武田英幸

takeda@witz-inc.co.jp