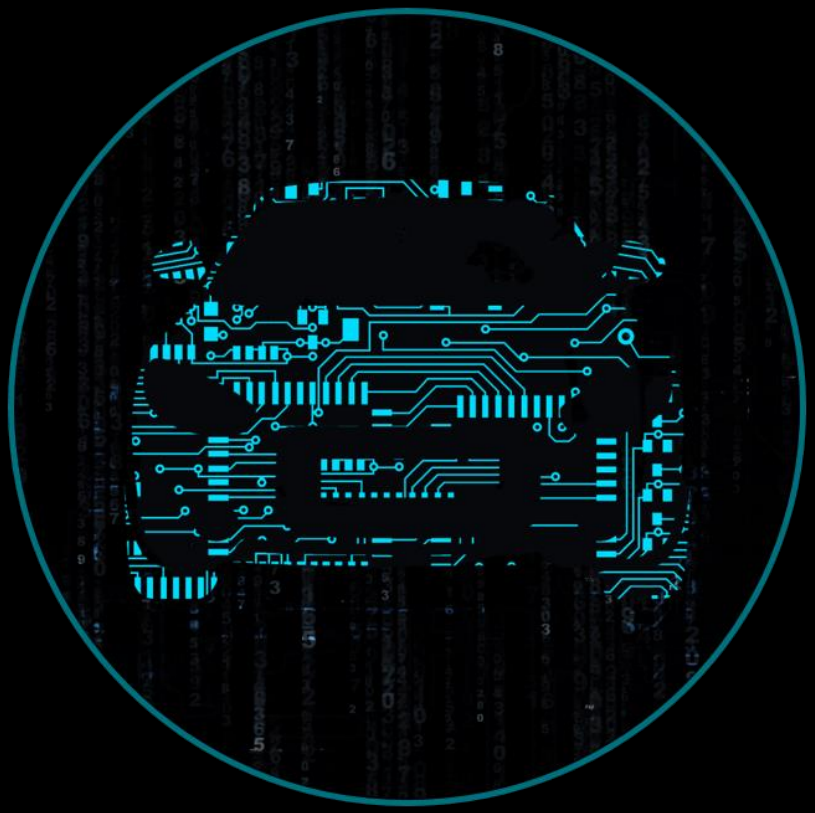
Deloitte.
デロイト トーマツ



IPA 第3回 STAMPワークショップ：
Connect Carを対象としたSTAMP/STPAの事例紹介

デロイト トーマツ リスクサービス株式会社　林　浩史
東京電機大学　金子朋子

Making another half century of Impact
デロイト トーマツ 50周年 次の50年へ
50th Deloitte Tohmatsu

Agenda

はじめに

STAMP/STPAでサイバーセキュリティを
扱うときの考え方

Virtual Car Keyとは

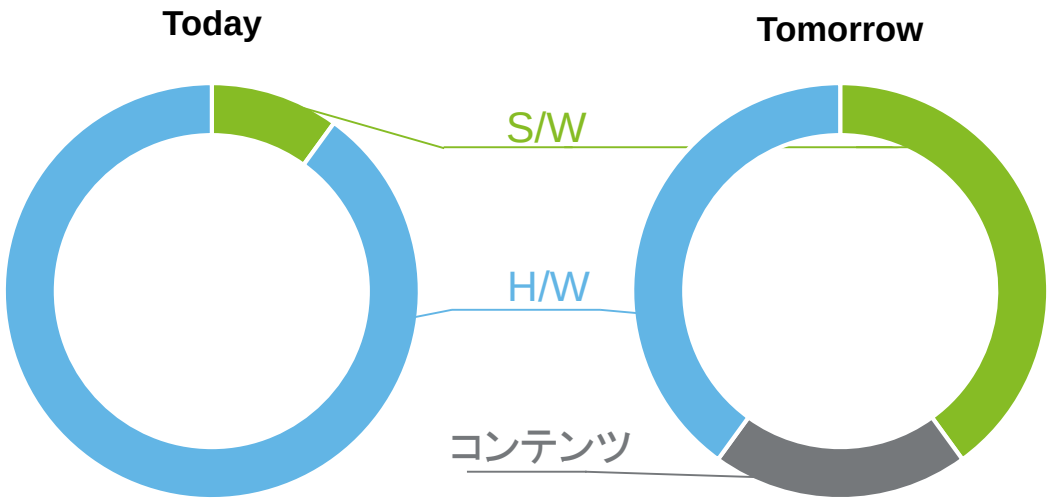
STAMP/STPAを用いた
VCKへサイバーリスクアセスメント

まとめ

はじめに

今後予想される車両開発でのバリューチェーンは、従来モデルとは異なる

コネクティビティ、自動運転、シェアード・カーなどにより、プレーヤーが増え、自動車に期待される価値観も劇的に変化



主に OEMや Tier1 が提供
- ボデー
- パワートレイン
- 電装系
- シート
- コンポーネント & HMI

多くの企業が参加
- OEM
- サプライヤ
- OSベンダー
- チップベンダー
- ISP、ISV
- In-car-アプリ
  – コネクテッドカーを実現するためのビルディングブロック

エンターテイメント
音楽、ビデオなどのコンテンツ配信サービス

Social media
Facebook, Lineなどソーシャルメディアへの接続

カーシェアリング
所有から、サービスへの移行

宅配サービス
車両への荷物配達

Points of interest
スポンサード情報を含む目的地提案

福祉サービス
自動運転によるデイケア、過疎地の移動手段提供

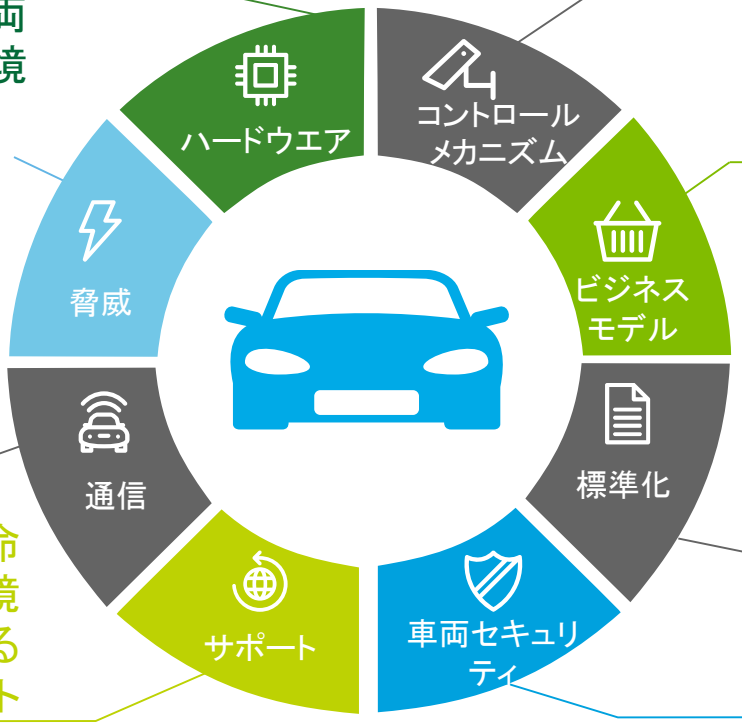
テレマティックス保険
ドライバや運転タイプによる保険料の最適化

緊急連絡、自動停車、自動搬送
ドライバーの異変などの緊急時に車両が自動対応

盗難防止
盗難にあった車両の位置情報を通知し、遠隔操作

コネクテッドカー、自動運転への挑戦

…サイバーセキュリティが新たなる課題に
従来の　E/Eアーキテクチャには存在しなかった脅威や攻撃面



多様化・複雑化する車両
の電装環境

攻撃手法は日々刻々
変化

車両内のコンポーネントや機能
間の通信は急激に増大

車両の長製品寿命
日々変化するリスク環境
常時接続、常時通電の車両に対する
ソフトウエアアップデート

サプライチェーン全体の
セキュリティ・モニタリング
ITのKnow-Howを活用

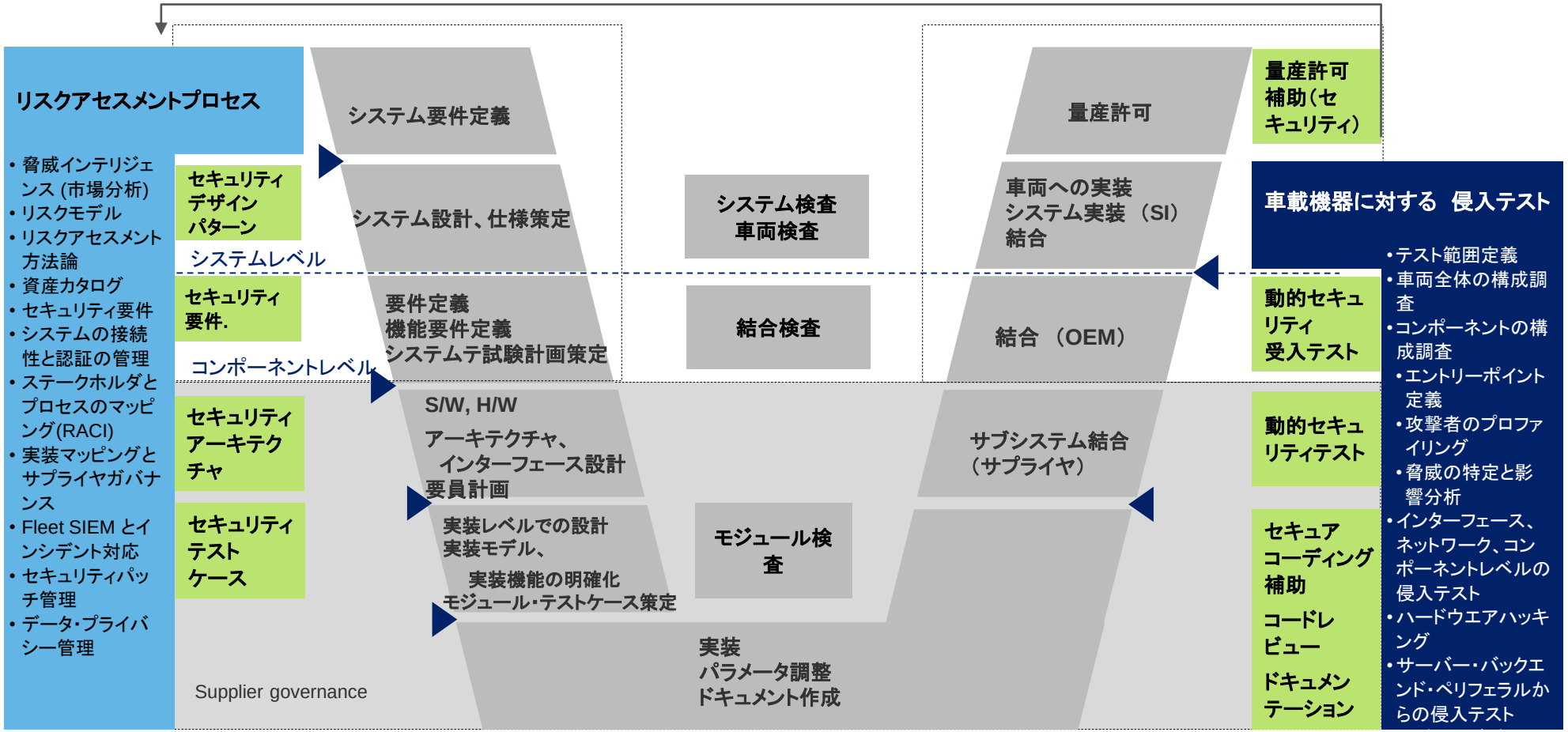
アフターセールス・
ビジネスモデルの変化
例：MaaS、テレマ保険など

車両のセキュリティ分野では
標準化やベストプラクティスが
整備途上

従来からの車両開発工程に
車両のセキュリティを実装

車両のV字開発におけるサイバーセキュリティ

デロイト　リスク　サービスは、車両を対象としたサイバーリスクに対するサービスを展開しています



最適なアセスメント手法の検討

単体でも、ハイブリッドでも、解析可能。 目的と対象に最適な手法を提案

TARA Threat Analysis and Risk Assessment	リスク指向による定量化分析手法。 自動車業界で実績。HARAのセキュリティ版。 特に上流 または 開発の前半での実施に適している
TVRA Threat, Vulnerability Risk Analysis	ETSIが策定した7ステップによるリスク評価アプローチ手法 ITSなど自動車業界で実績。 特に上流での分析が適している 半定量的なアセスメント結果。
STAMP / STPA Systems-Theoretic Accident Model and Processes	システムを対象に、安全＋セキュリティの視点で脅威を分析する手法 複雑なシステムでの実施に適している。 安全解析とセキュリティ解析を同時に行うことが可能
FTA / FMEA	脆弱性に対して、故障の木解析や故障モード影響解析のアプローチを適用 発生頻度の論理和、論理積などを使い、定量評価が可能 特に実装レベルや開発後期での評価に適している
Attack Tree Analysis	脅威視点による脆弱性と攻撃者目線での分析 基本構造は、FTAと同様。 定量評価が可能 他の手法とハイブリッドで使うことも可能

※適用範囲や特徴は著者個人の理解によるものです。バージョンやアレンジによって異なります

For Discussion Purposes Only

STAMP/STPAで
サイバーセキュリティを扱うときの考え方

なぜサイバーリスクアセスメントにSTAMP/STPAを使うのか

STAMP/STPAの有効性と解析対象

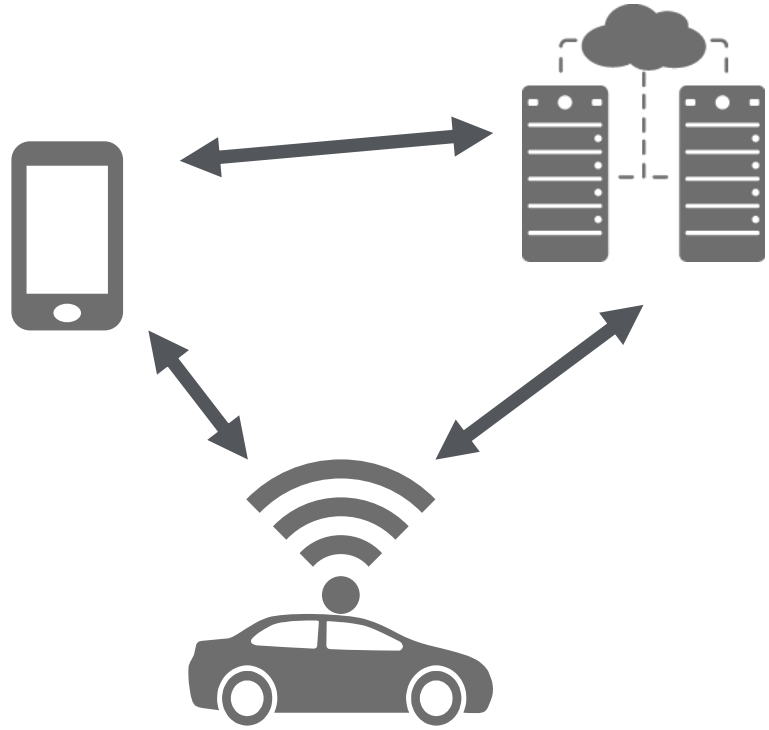
STAMP/STPAはサイバーにも活用できるといわれており、いくつかの活用法が提案されてます
(STAMP/STPA-sec, STAMP/STPA Safe-Secなど)
様々な提案をもとに、我々が、行ったサイバーセキュリティへの適用事例とその考え方を示します※

※適用範囲や特徴は著者個人の理解によるものです。バージョンやアレンジによって異なります

IoT
- コネクテッドカーをはじめとし、多くの機器がIoT化している
- セキュリティと安全(機能が共存)

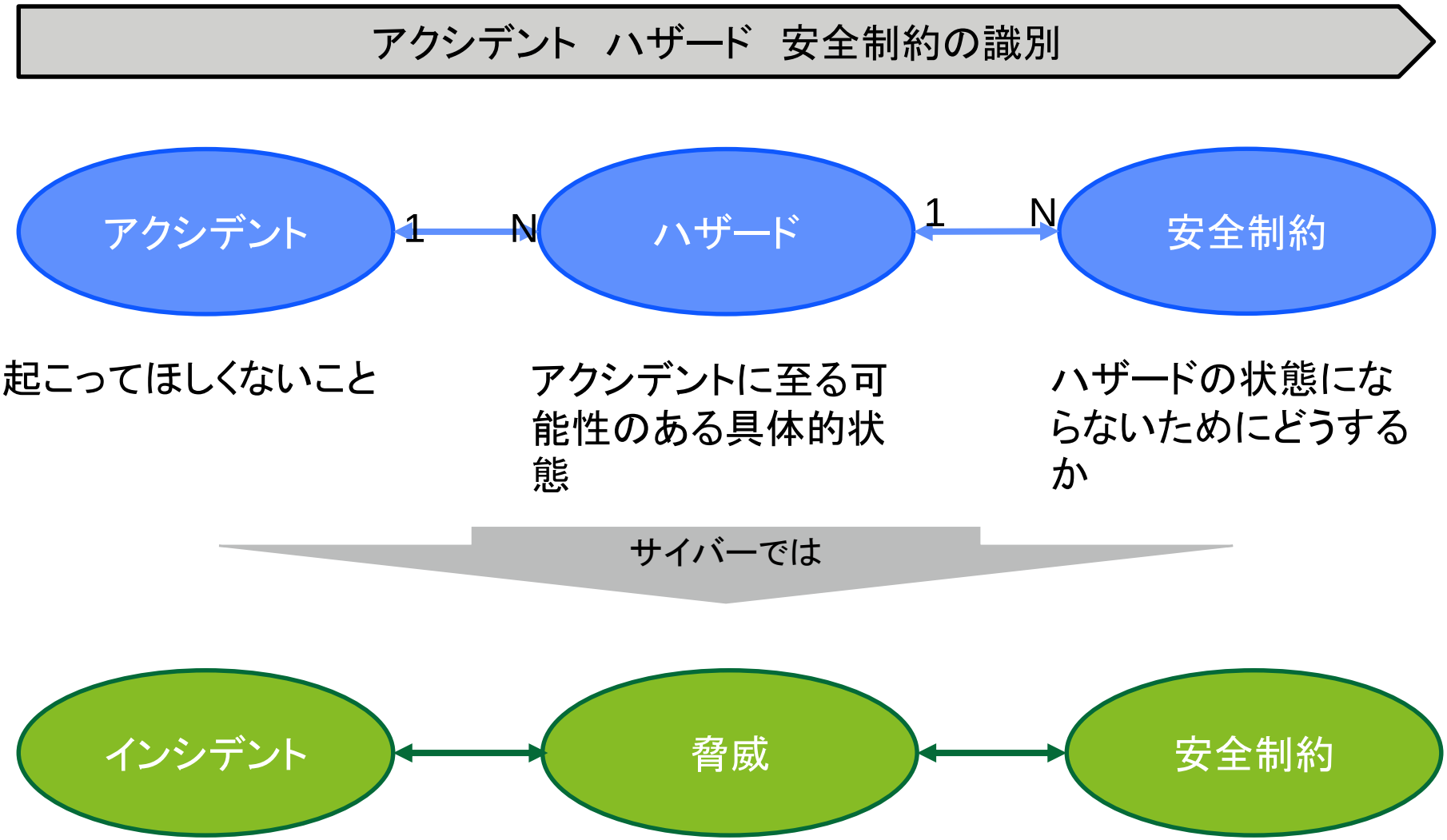
ネットワーク
- インターネットと接続
  より広い攻撃面

システム化
- 複数コンポーネントによる構成
- オープンソースや、3rd パーティー制部品



アクシデント・ハザード・安全制約の考え方

STAMP　STPAをサイバーセキュリティに活用



UCA・HCFの考え方

サイバーでUCA,HCFをどう扱うか

UCA（Unsafe Cause Action) :
　安全でなくなる原因となりうるアクション

（例えば） UnSecure Cause Action　:
　セキュアでなくなる原因となりうるアクション

HCF（ Hazard　Cause　Factor) :

→（例えば） Threat Cause　Factor　:
　脅威シナリオ、攻撃シナリオなどの結果
　具体的に発生する状態

安全制約を破る可能性のあるアクション

ヒントワードの拡張　（STRIDEの適用）

- なりすまし
- 改ざん
- 否認
- 情報漏洩
- DoS
- 権限昇格

を追加する

Virtual Car Keyとは

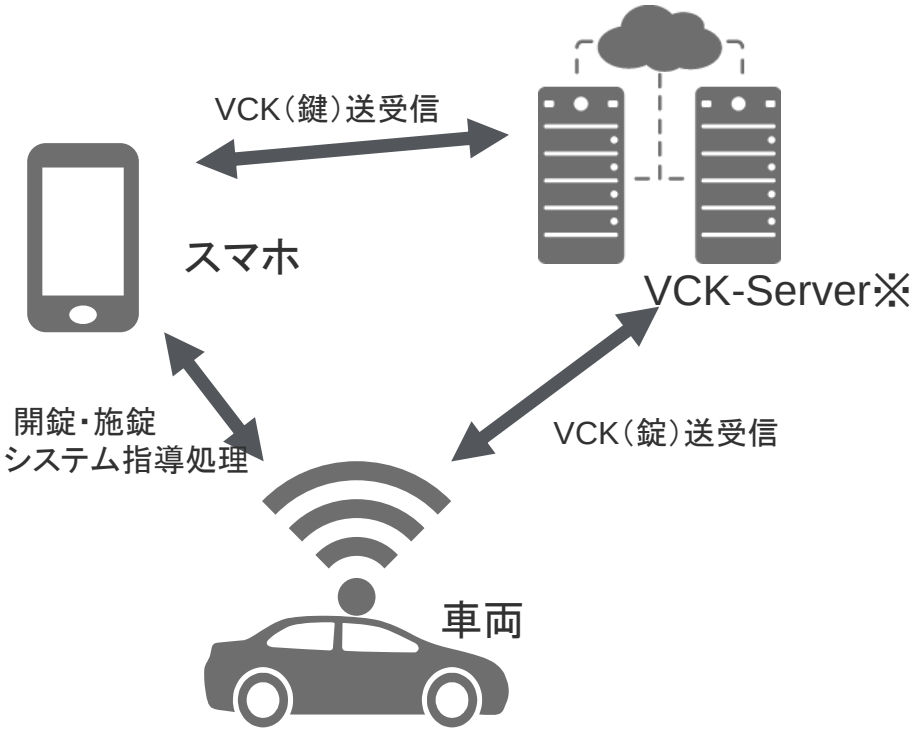
VCKの特徴と要件

スマホで車両を開錠・施錠・起動などを行う

スマホに、車両用キーフォブと同様の機能を実装する

- VCK単位での権限付与や制限が可能
- One time VCK などの利用が可能
- Car Sharing、宅配サービスなどの基本技術

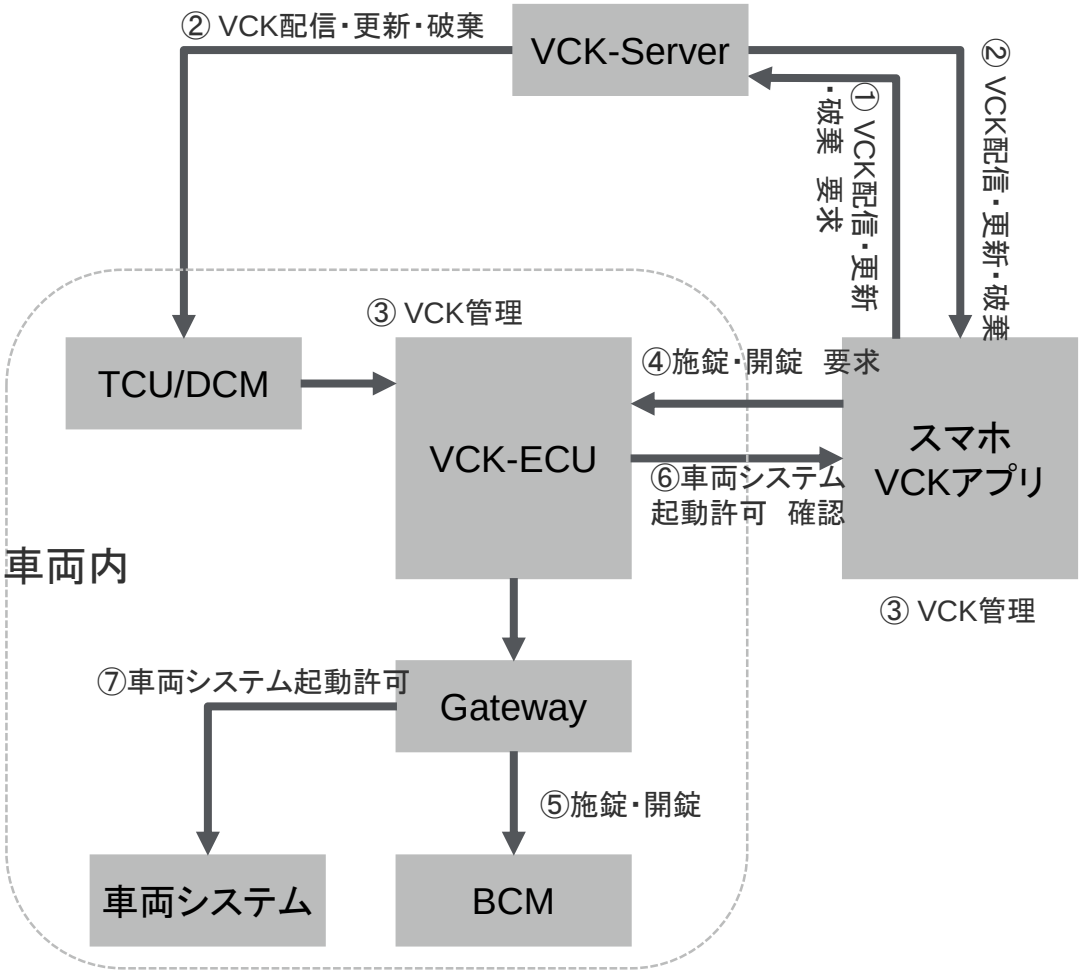
- 実装パターン
  - スマホ内に鍵を格納
    - ✓ 地下駐車場や、携帯通信網の外部でも利用可能
    - ✓ スマホ内でVCKを守る必要
スマホに特殊なセキュリティ対策が必要
  - サーバー上に鍵を格納
    - ✓ サーバーへの認証情報をスマホ内に保存
    - ✓ 携帯通信網圏外での利用に問題



※VCK-Server： VCKの管理を行う
鍵を発行、 送信、 管理、 廃棄などを行う
通常、車両の管理や、ユーザー管理、
課金なども行う

VCKシステムのコントロールストラクチャ

簡略化したVCKシステム



説明のため簡略化しています

通常VCKの分析を行う場合には

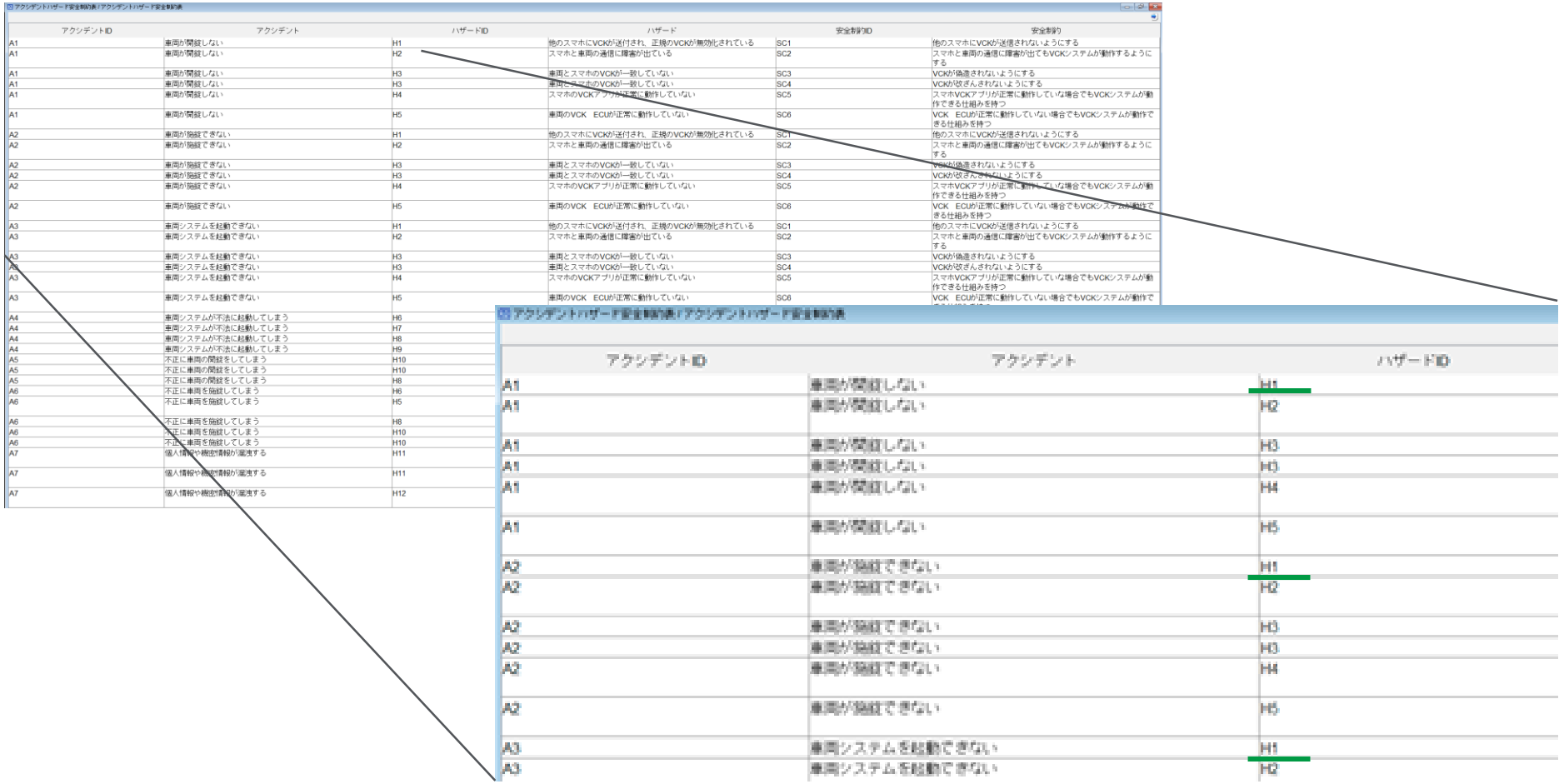
- 二次的に影響を受けるECUの考慮
- VCK-ECU内の機能（セキュアストレージなど）の詳細化
- スマホ内の機能（セキュアストレージ、暗号エンジンなど）を詳細化

などを行います

VCKはスマホ、車両内で管理されているパターンを想定しています

STAMP/STPAを用いた
VCKのサイバーリスクアセスメント

アクシデント・インシデント　－　ハザード・脅威　－　安全制約



アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	車両が開錠しない	H1	他のスマホにVCKが送付され、正規のVCKが無効化されている	SC1	他のスマホにVCKが送信されないようにする
A1	車両が開錠しない	H2	スマホと車両の通信に障害が出ている	SC2	スマホと車両の通信に障害が出てもVCKシステムが動作するようにする
A1	車両が開錠しない	H3	車両とスマホのVCKが一致していない	SC3	VCKが偽造されないようにする
A1	車両が開錠しない	H3	車両とスマホのVCKが一致していない	SC4	VCKが改ざんされないようにする
A1	車両が開錠しない	H4	スマホのVCKアプリが正常に動作していない	SC5	スマホVCKアプリが正常に動作していな場合でもVCKシステムが動作できる仕組みを持つ
A1	車両が開錠しない	H5	車両のVCK　ECUが正常に動作していない	SC6	VCK　ECUが正常に動作していない場合でもVCKシステムが動作できる仕組みを持つ
A2	車両が施錠できない	H1	他のスマホにVCKが送付され、正規のVCKが無効化されている	SC1	他のスマホにVCKが送信されないようにする
A2	車両が施錠できない	H2	スマホと車両の通信に障害が出ている	SC2	スマホと車両の通信に障害が出てもVCKシステムが動作するようにする
A2	車両が施錠できない	H3	車両とスマホのVCKが一致していない	SC3	VCKが偽造されないようにする
A2	車両が施錠できない	H3	車両とスマホのVCKが一致していない	SC4	VCKが改ざんされないようにする
A2	車両が施錠できない	H4	スマホのVCKアプリが正常に動作していない	SC5	スマホVCKアプリが正常に動作していな場合でもVCKシステムが動作できる仕組みを持つ
A2	車両が施錠できない	H5	車両のVCK　ECUが正常に動作していない	SC6	VCK　ECUが正常に動作していない場合でもVCKシステムが動作できる仕組みを持つ
A3	車両システムを起動できない	H1	他のスマホにVCKが送付され、正規のVCKが無効化されている	SC1	他のスマホにVCKが送信されないようにする
A3	車両システムを起動できない	H2	スマホと車両の通信に障害が出ている	SC2	スマホと車両の通信に障害が出てもVCKシステムが動作するようにする
A3	車両システムを起動できない	H3	車両とスマホのVCKが一致していない	SC3	VCKが偽造されないようにする
A3	車両システムを起動できない	H3	車両とスマホのVCKが一致していない	SC4	VCKが改ざんされないようにする
A3	車両システムを起動できない	H4	スマホのVCKアプリが正常に動作していない	SC5	スマホVCKアプリが正常に動作していな場合でもVCKシステムが動作できる仕組みを持つ
A3	車両システムを起動できない	H5	車両のVCK　ECUが正常に動作していない	SC6	VCK　ECUが正常に動作していない場合でもVCKシステムが動作できる仕組みを持つ
A4	車両システムが不法に起動してしまう	H6			
A4	車両システムが不法に起動してしまう	H7			
A4	車両システムが不法に起動してしまう	H8			
A4	車両システムが不法に起動してしまう	H9			
A5	不正に車両の開錠をしてしまう	H10			
A5	不正に車両の開錠をしてしまう	H10			
A5	不正に車両の開錠をしてしまう	H8			
A6	不正に車両を施錠してしまう	H6			
A6	不正に車両を施錠してしまう	H5			
A6	不正に車両を施錠してしまう	H8			
A6	不正に車両を施錠してしまう	H10			
A6	不正に車両を施錠してしまう	H10			
A7	個人情報や機密情報が漏洩する	H11			
A7	個人情報や機密情報が漏洩する	H11			
A7	個人情報や機密情報が漏洩する	H12			

アクシデント・インシデント

アクシデント・インシデントは発生して欲しくないことを記載

アクシデント
車両が開錠しない
車両が施錠できない
車両システムを起動できない
車両システムが不法に起動してしまう
不正に車両の開錠をしてしまう
不正に車両の施錠をしてしまう
個人情報や機密情報が漏洩する

一般的にアセスメント開始前に、システムとして守るべきものは何かを決定します。アクシデント・インシデントは、その軸にしたがって決定されます

（例）

- 生命・安全に関わるケース
  例えば　開錠しない場合　搭乗者が車内に閉じ込められ、怪我や病気に陥る可能性があります
- 個人情報・機密情報に関するケース
  例えば、 VCK発行時に決済情報や免許証情報を登録していた場合、これらが漏洩するケースです
- 経済的損失が発生するケース
  例えば、不正に開錠した場合、車両の盗難につながります
- システムの機能が十全に動作しなくなるケース
  例えば、車両システムが起動しなくなる場合、鍵として機能しません
- 外部環境への影響を考慮するケース
  例えば、攻撃によりエンジンパラメータが変更され、大気汚染につながるなどです

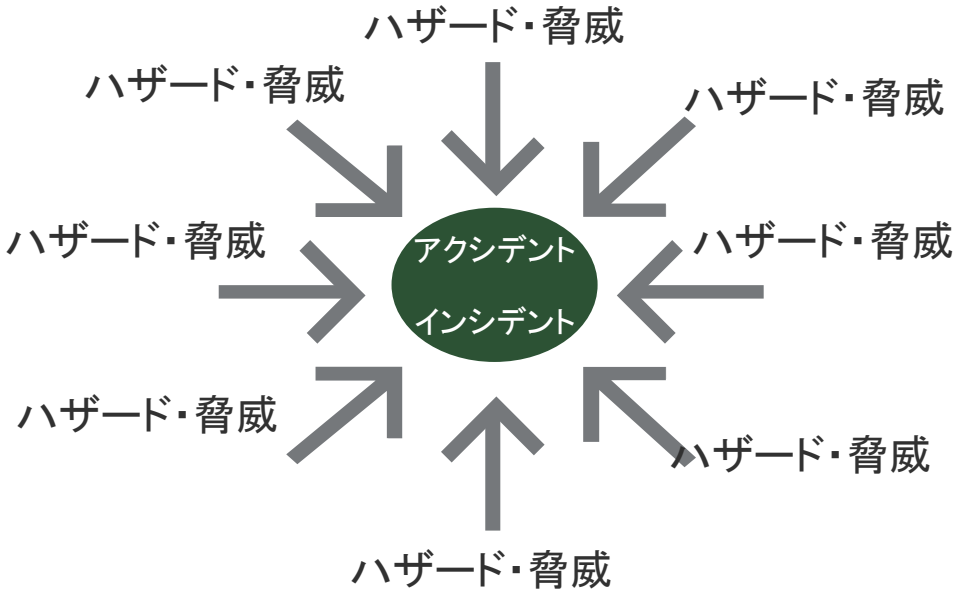
ハザード・脅威

本分析での脅威は、攻撃者により、何が行われたとき、インシデントに陥るか検討します

例： アクシデント “車両が開錠しない”

なぜ、車両が開錠しなくなっているのか？

車両が開錠しない　原因となっている事象を洗い出します

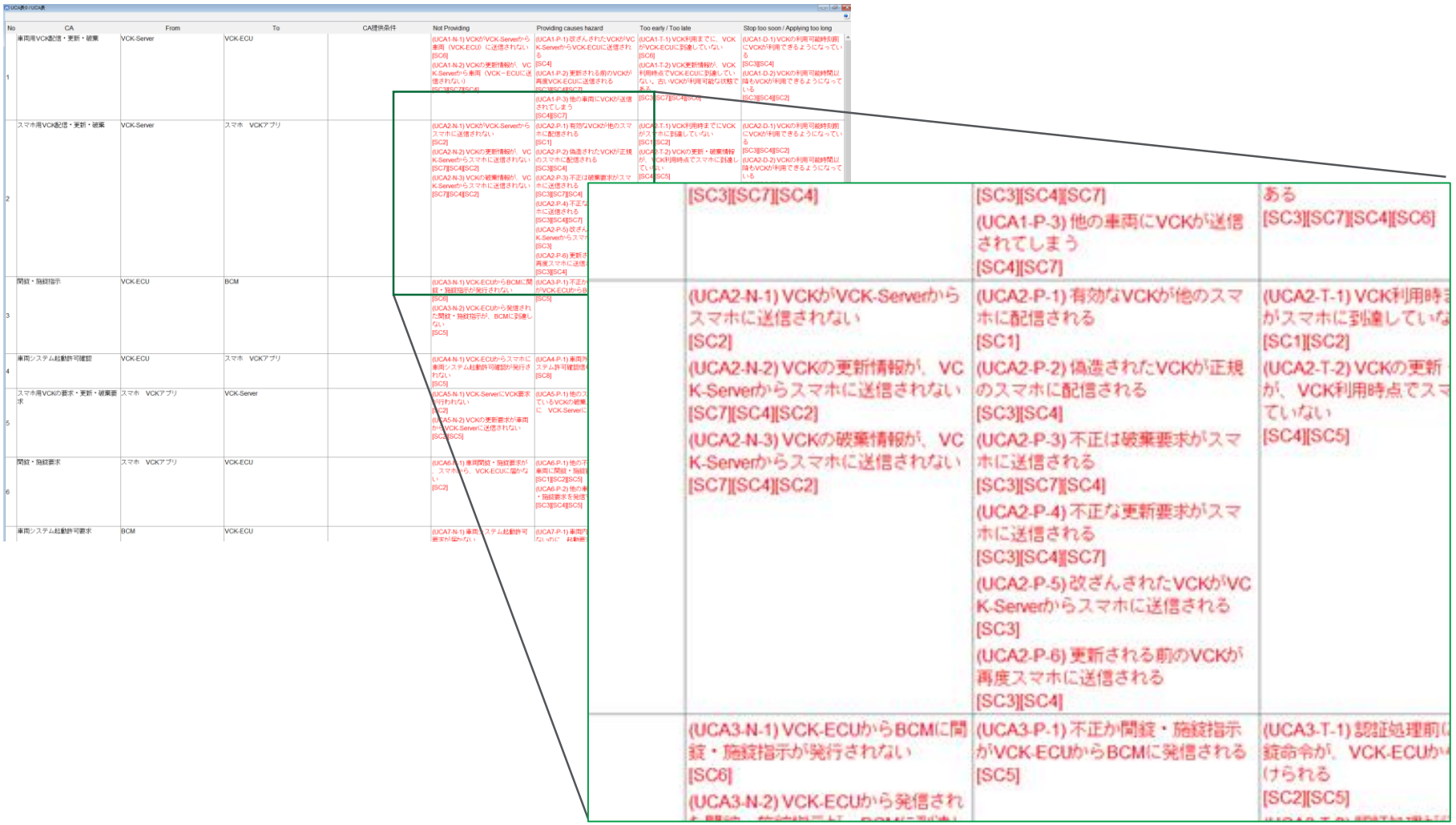


- ✓ “車両とスマホのVCKが一致しない”
- ✓ “車両とスマホの通信に障害が出ている”
- ✓ “他のスマホにVCKが送付され、正規のVCKが無効化されている”
- ✓ “スマホのVCKアプリが正常に動作していない”
- ✓ …….

この段階で、Securityと Safetyを区別する必要はありません
IoT 機器を分析する場合、Securityと Safetyは一般的に同時に考慮すべきです

UCA(UnSafe / UnSecure Cause Factor)

各ハザード・脅威（安全制約）を、CA毎に掘り下げます



No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	車両用VCK配信・更新・破棄	VCK-Server	VCK-ECU		(UCA1-N-1) VCKがVCK-Serverから車両（VCK-ECU）に送信されない [SC6] (UCA1-N-2) VCKの更新情報が、VCK-Serverから車両（VCK－ECUに送信されない） [SC7][SC4][SC2]	(UCA1-P-1) 改ざんされたVCKがVCK-ServerからVCK-ECUに送信される [SC4] (UCA1-P-2) 更新される前のVCKが再度VCK-ECUに送信される [SC3][SC4][SC7] (UCA1-P-3) 他の車両にVCKが送信されてしまう [SC4][SC7]	(UCA1-T-1) VCK利用までに、VCKがVCK-ECUに到達していない [SC6] (UCA1-T-2) VCK更新情報が、VCK利用時点でVCK-ECUに到達していない。古いVCKが利用可能な状態である。 [SC3][SC7][SC4][SC5]	(UCA1-D-1) VCKの利用可能時刻前にVCKが利用できるようになっている [SC3][SC4] (UCA1-D-2) VCKの利用可能時間以降もVCKが利用できるようになっている [SC3][SC4][SC2]
2	スマホ用VCK配信・更新・破棄	VCK-Server	スマホ　VCKアプリ		(UCA2-N-1) VCKがVCK-Serverからスマホに送信されない [SC2] (UCA2-N-2) VCKの更新情報が、VCK-ServerからスマホにVCKが送信されない [SC7][SC4][SC2] (UCA2-N-3) VCKの破棄情報が、VCK-ServerからスマホにVCKが送信されない [SC7][SC4][SC2]	(UCA2-P-1) 有効なVCKが他のスマホに配信される [SC1] (UCA2-P-2) 偽造されたVCKが正規のスマホに配信される [SC3][SC4] (UCA2-P-3) 不正は破棄要求がスマホに送信される [SC3][SC7][SC4] (UCA2-P-4) 不正な更新要求がスマホに送信される [SC3][SC4][SC7] (UCA2-P-5) 改ざんされたVCKがVCK-ServerからスマホにVCKが送信される [SC3] (UCA2-P-6) 更新される前のVCKが再度スマホに送信される [SC3][SC4]	(UCA2-T-1) VCK利用時までにVCKがスマホに到達していない [SC1][SC2] (UCA2-T-2) VCKの更新・破棄情報が、VCK利用時点でスマホに到達していない [SC4][SC5]	(UCA2-D-1) VCKの利用可能時刻前にVCKが利用できるようになっている [SC3][SC4][SC2] (UCA2-D-2) VCKの利用可能時間以降もVCKが利用できるようになっている
3	開錠・施錠指示	VCK-ECU	BCM		(UCA3-N-1) VCK-ECUからBCMに開錠・施錠指示が発行されない [SC6] (UCA3-N-2) VCK-ECUから発信された開錠・施錠指示が、BCMに到達しない [SC5]	(UCA3-P-1) 不正が開錠・施錠指示がVCK-ECUからBCMに発信される [SC5]		
4	車両システム起動許可確認	VCK-ECU	スマホ　VCKアプリ		(UCA4-N-1) VCK-ECUからスマホに車両システム起動許可確認が発行されない [SC5]	(UCA4-P-1) 車両システム許可確認信 [SC6]		
5	スマホ用VCKの要求・更新・破棄要求	スマホ　VCKアプリ	VCK-Server		(UCA5-N-1) VCK-ServerにVCK要求が行われない [SC2] (UCA5-N-2) VCKの更新要求が車両からVCK-Serverに送信されない [SC2][SC5]	(UCA5-P-1) 他のスているVCKの破棄に　VCK-Server		
6	開錠・施錠要求	スマホ　VCKアプリ	VCK-ECU		(UCA6-N-1) 車両開錠・施錠要求が、スマホから、VCK-ECUに届かない [SC2]	(UCA6-P-1) 他の不車両に開錠・施錠 [SC1][SC2][SC5] (UCA6-P-2) 他の車・施錠要求を受信 [SC3][SC4][SC5]		
	車両システム起動許可要求	BCM	VCK-ECU		(UCA7-N-1) 車両システム起動許可要求が届かない	(UCA7-P-1) 車両シ		

HCF, Threat Cause Factor

想定される具体的な攻撃の抽出

UCA： VCKの利用可能時間以降もVCKが利用できるようになっている

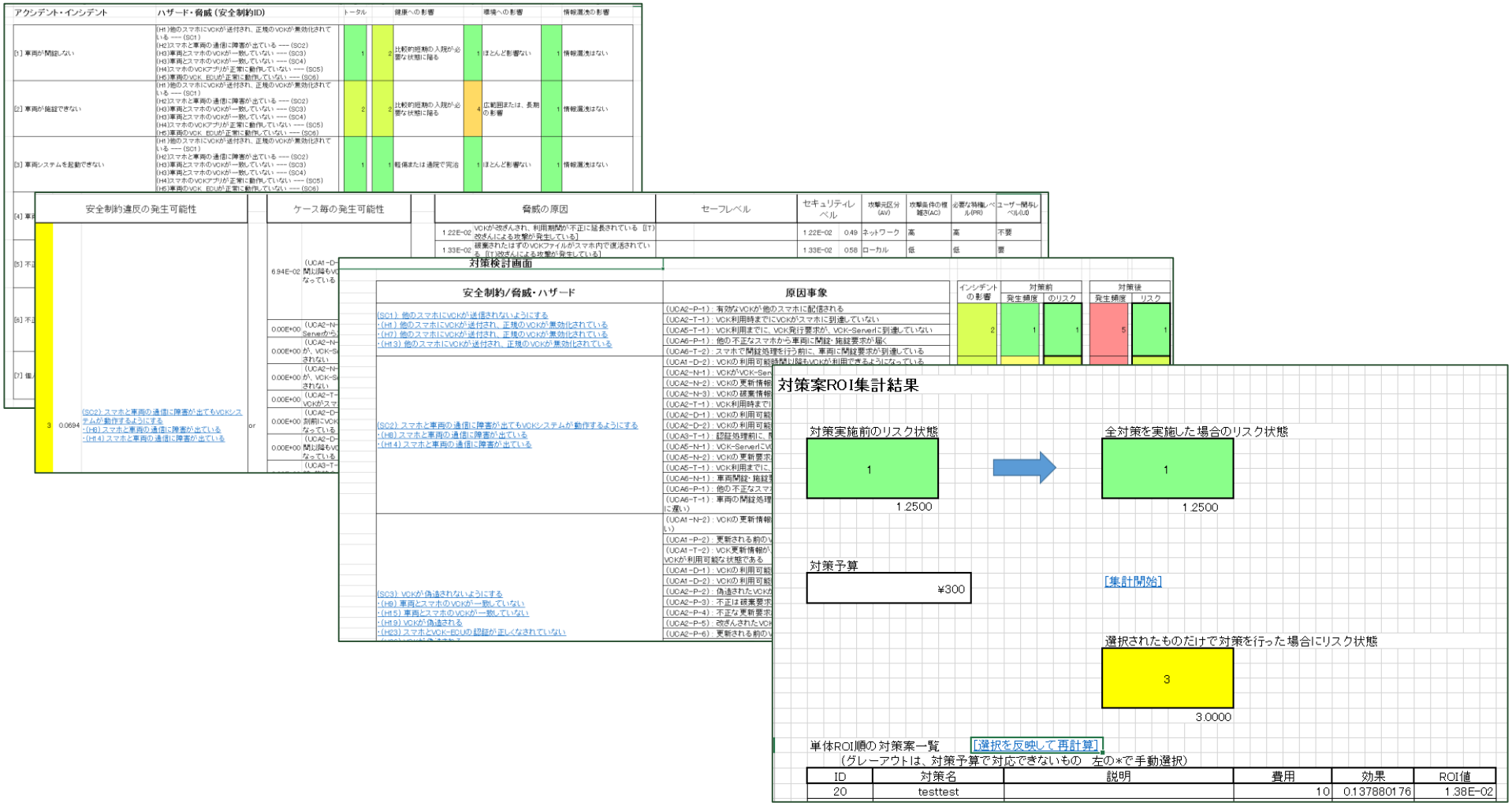
HCF/ Threat Cause Factor	ヒントワード	シナリオ
VCKが改ざんされ、利用期間が不正に延長されている	(T)改ざんによる攻撃が発生している	スマホーVCK-Server間、にMitM攻撃を行い、不正なVCKをスマホや端末に配布する スマホ内のVCKアプリや、保存されているVCK情報が改ざんされている
破棄されたはずのVCKファイルがスマホ内で復活されている	(T)改ざんによる攻撃が発生している	スマホの改ざんまたはスマホ内のVCKアプリが改ざんされて、消去されたファイルを復活させている
サーバーからのVCK破棄要求の受領を無視して利用している	(R)否認が行われている	サーバーから届いた、VCK破棄要求の受領を否認して、VCKを利用しつづけている
他のスマホにVCKをコピーして利用しているまたはスマホを複製している	(E)権限昇格を伴う攻撃または権限昇格を目的とした攻撃が行われている	他のスマホに、VCK情報をコピーして、または、スマホを複製して、正規のスマホ上で、VCKが破棄された後も、複製したスマホやVCKを利用している
次のユーザーや他のユーザーになりすまして、VCKを利用している	(S) なりすましによる攻撃が発生している	カーシェアリングなどのケースで、自分の利用時間中に、車両にリレー攻撃のデバイスを設置し、他のユーザーが利用しているときに、車両とスマホとの通信を傍受し、それを自己のスマホに送信する。この通信を再現して、不法に車両を利用する

ヒントワード： STRIDEを活用
デフォルト＋STRIDE
(S) なりすましによる攻撃
(T)改ざんによる攻撃
(R)否認
(I)情報漏洩が発生しているまたは
情報漏洩を目的とした攻撃
(D) DoS攻撃
(E)権限昇格をともなく攻撃または、
権限昇格を目的とした攻撃

ヒントワードとUCAの組み合わせから、想定される具体的な攻撃と、その背景にあるシナリオを抽出

MRC4IoTへの接続

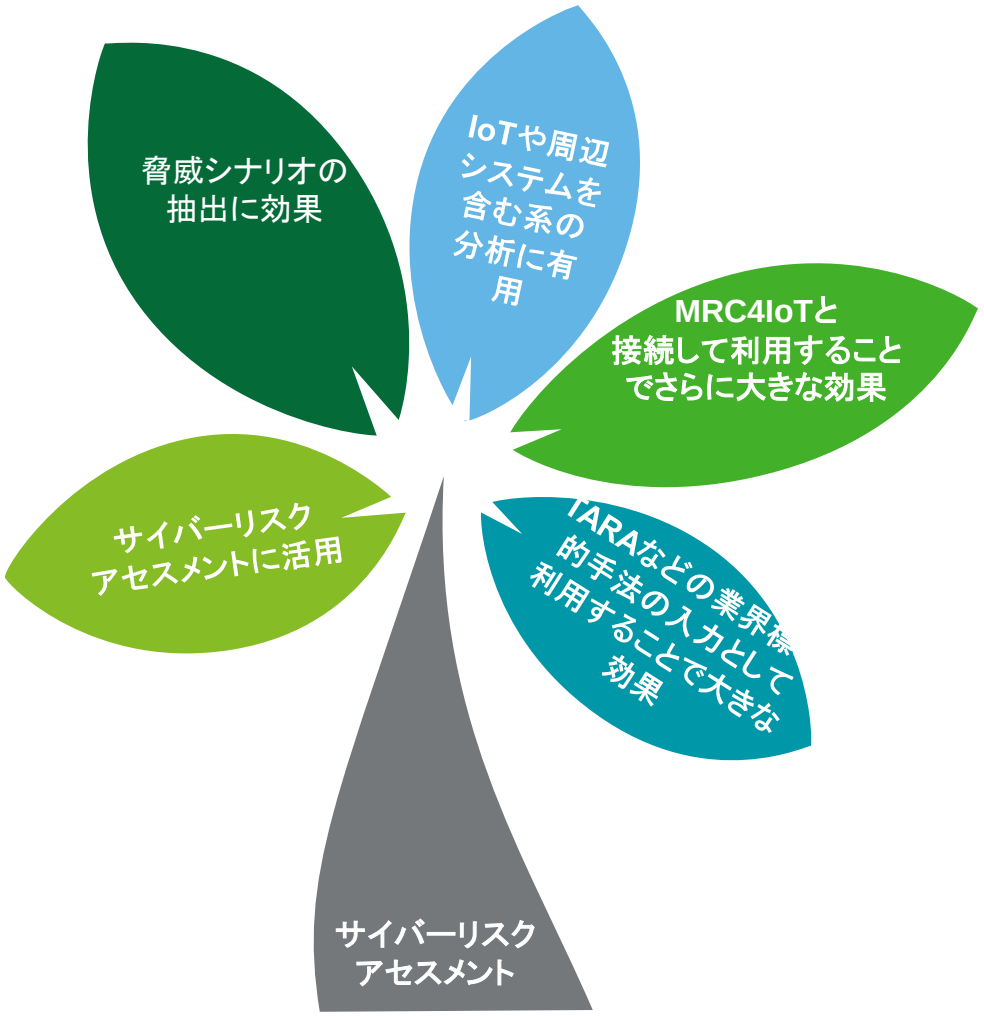
準定量化解析への活用



まとめ

STAMP STPAはサイバーリスクアセスメントにも活用可能

Header



STAMP/STPAをサイバーセキュリティ・アセスメントに活用しています

多くの脅威シナリオの抽出が可能であることが確認されました

アセスメント対象がシステムとして動作するIoT機器や、バックエンドシステムを含むサービスシステムの分析に効果があることがわかりました

MRC4IoTを用いてFTA、Attack Tree分析などと接続することで、より大きな効果が得られました

抽出された大量の脅威・攻撃シナリオをTARA（ Threat Analysis and Risk Assessment) などの一般的に標準的に用いられる手法の入力として利用することが可能であり、大きな効果が期待が得られました

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームであるデロイト トーマツ合同会社およびそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約40都市に約11,000名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクアドバイザリー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスをFortune Global 500®　の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約245,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細はwww.deloitte.com/jp/aboutをご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

IS 669126 / ISO 27001

Member of
Deloitte Touche Tohmatsu Limited