車載セキュリティの基礎技術

2021-11-29 - 2021年度第3回ASIFスキルアップセミナー

ルネサスエレクトロニクス株式会社
オートモーティブソリューション事業本部
車載コアテクノロジー開発統括部
車載システムセキュリティ部
セキュリティ技術マーケティング＆支援課
山中 聡

AST-AA-21-0030_00

アジェンダ

- ルネサスエレクトロニクスについて
- セキュリティとは
- 暗号の基礎
- 車載セキュリティ動向
  - 標準化・法令化
  - 車載マイコンの標準化
- まとめ

ルネサスエレクトロニクスについて

ルネサスとは

ルネサス エレクトロニクスは、グローバルな半導体会社です。
人々が安心・安全に暮らせる社会を実現するために、あらゆるモノとモノをつなぎインテリジェント化することを通して、組み込み機器に進化をもたらしています。

そして、無限の未来をカタチづくるために、自動車、産業、インフラ、IoT分野に対して、世界的に高いシェアを誇るマイコンに加え、アナログ&パワーデバイス、SoCなどの各種半導体と幅広いソリューションを提供しています。

本社所在地
東京都江東区

連結従業員数 *
～ 21,000人

関連会社所在国数
30+ 国

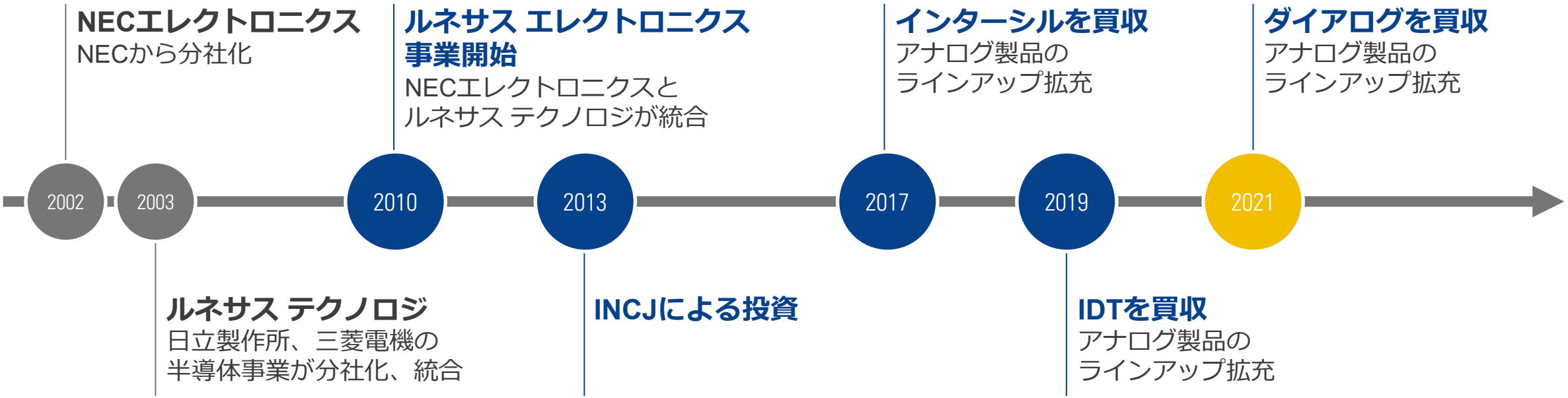
2020年売上収益
7,157億円

特許取得数および出願中件数
約20,000件

SoC: System-on-a-chip　*連結 2021年9月30日時点

沿革

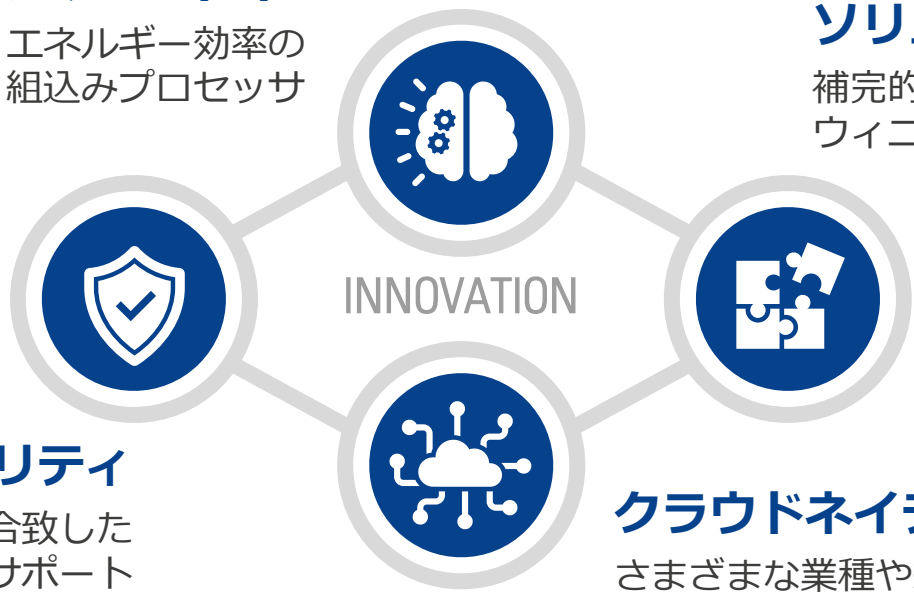
ルネサスは、日立製作所、三菱電機、NECを起源とする歴史ある強力な技術革新基盤を有しています。Intersil、IDTおよびDialogとの統合により、インフラ、データセンターなど飛躍的に成長するデータエコノミー関連分野へ事業領域を拡大するとともに、産業・自動車分野でのポジション強化を図っています。



IDT: Integrated Device Technology

コアテクノロジー

ルネサスでは、「AI」、「セーフティ＆セキュリティ」、「デジタル＆アナログ＆パワーソリューション」、「クラウドネイティブ」の4つのコアテクノロジーを柱に、あらゆる業界のニーズに応え、将来の持続的な成長に向けてきめ細かく対応し、イノベーションを起こしていきます。



人工知能（AI）

幅広い高出力・エネルギー効率の
組込みプロセッサ

デジタル＆アナログ＆パワーソリューション

補完的な製品ポートフォリオを組み合わせた
ウィニング・コンビネーション

セーフティ＆セキュリティ

業界の厳しい安全・安心基準に合致した
包括的な技術とサポート

クラウドネイティブ

さまざまな業種や組織のパートナーと連携した
クロスプラットフォーム

セキュリティとは

*1 翔泳社　情報セキュリティスペシャリスト　より一部引用し作成

セキュリティとは？ *1

- 「セキュリティ」は安全を意味する。安全とは、守らなければならない大切なものが、危害や損傷を受けない正常な状態にある事である。
- 安全を表す言葉には「セキュリティ」以外に「セーフティ」がある
  - 「セーフティ」は交通事故や災害など、**悪意の介在しない自然現象や偶発的・突発的に発生する脅威**に対する安全としての意味合いが強い。
  - 「セキュリティ」は侵入、盗難、攻撃、破壊といった**悪意をもって行われる人的な脅威**に対する安全の意味合いが強い。

セキュリティ技術の導入

起きるか起きないかは攻撃者が決める

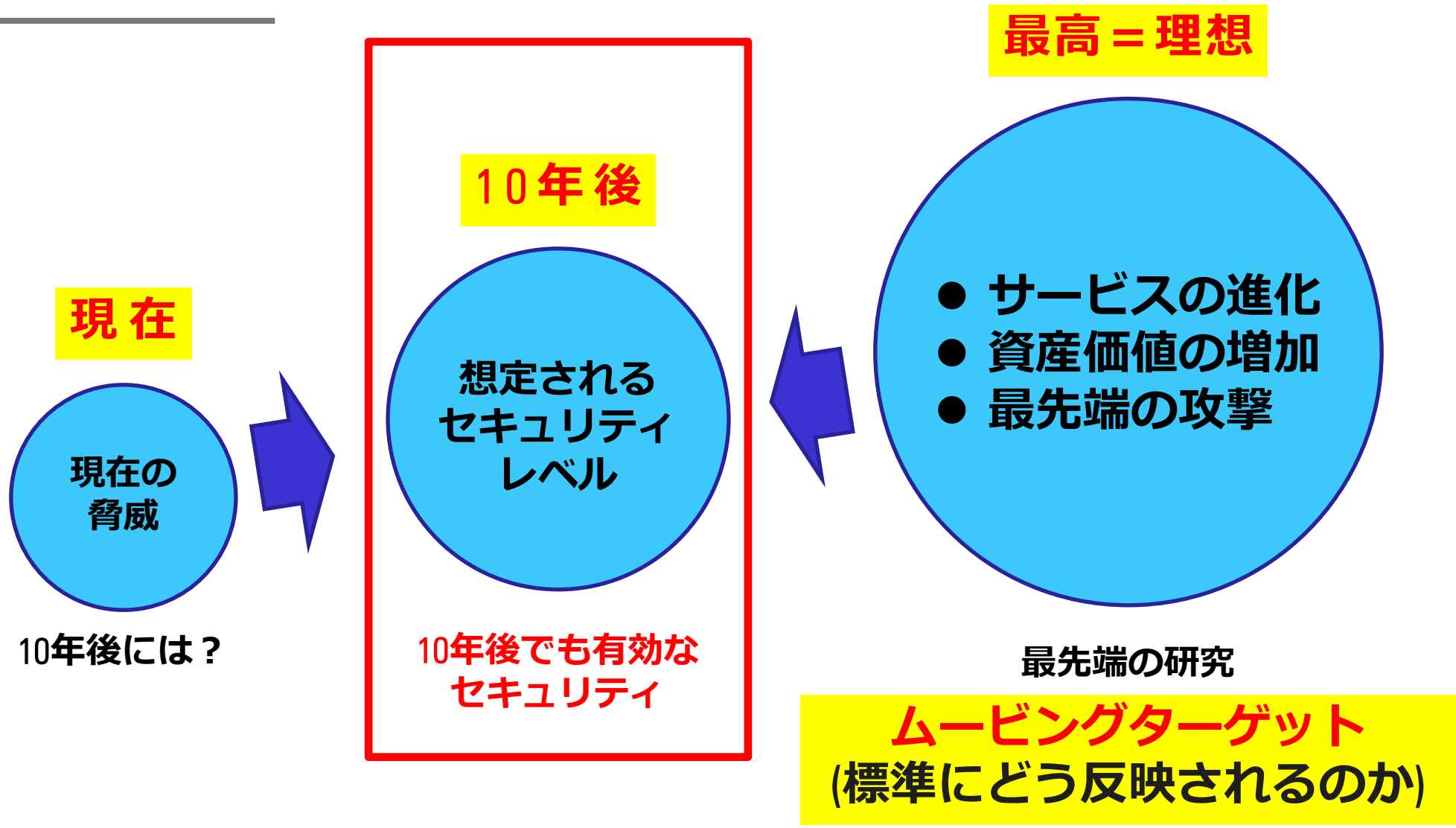
セキュリティ技術の導入

セキュリティ対策の導入は被害にあうメーカーの被害度による

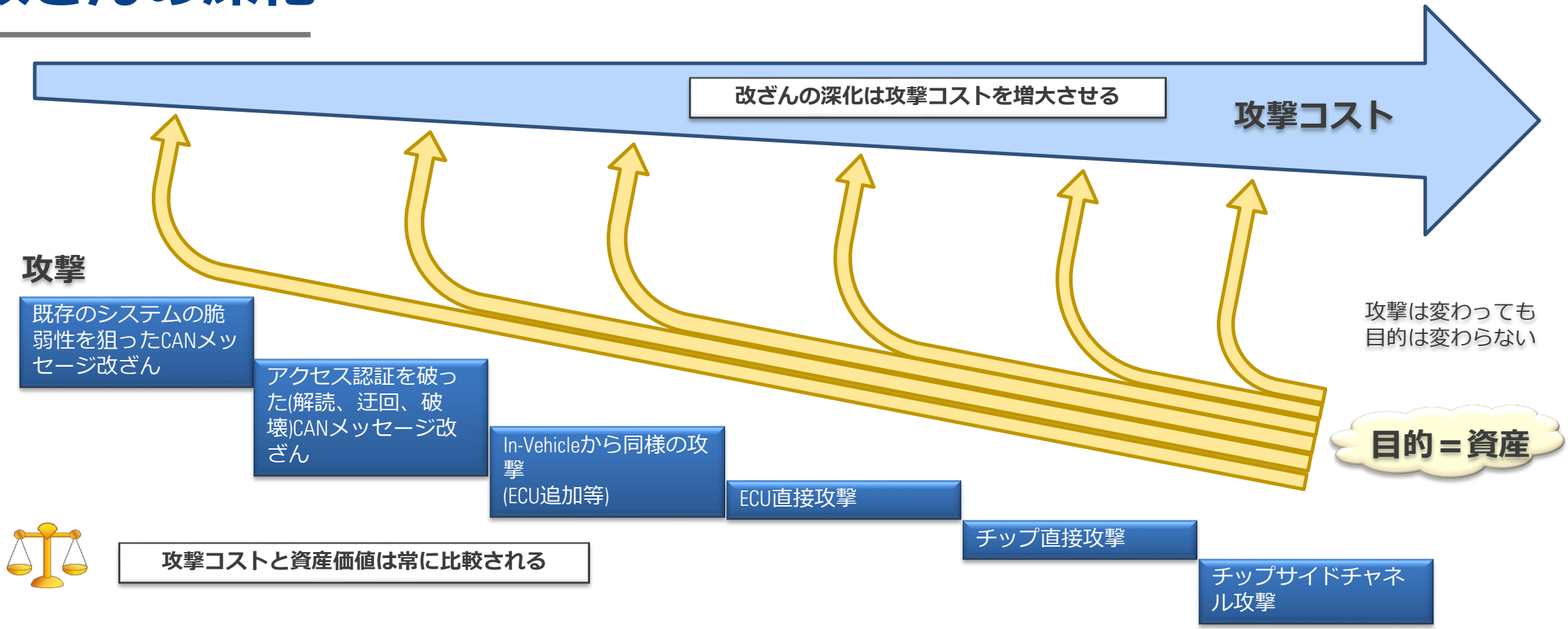
セキュリティ技術の導入

セキュリティ導入の波はもはや止められない

今、どう設計するのか



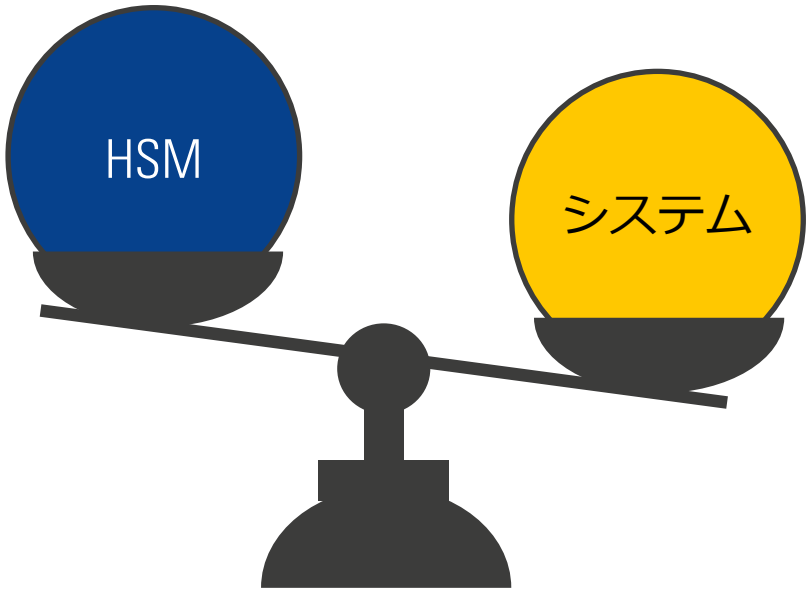
改ざんの深化

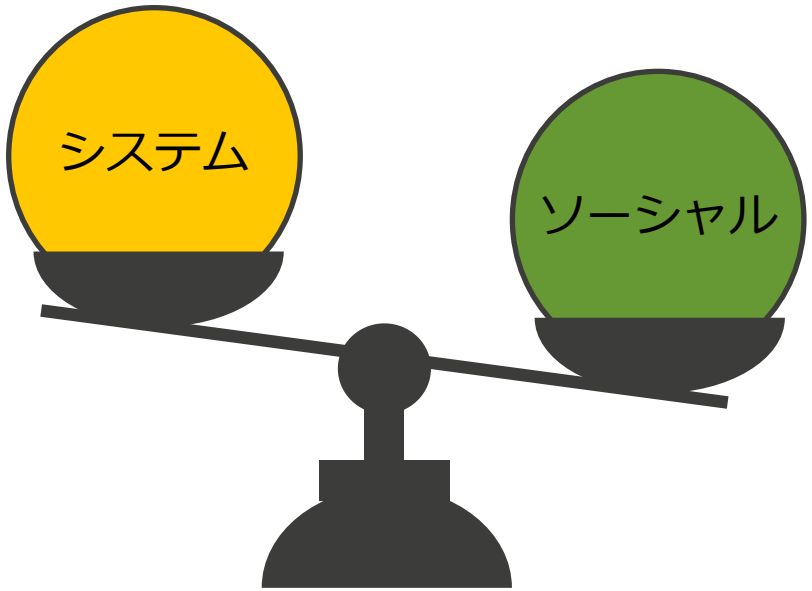


【重要】被害の深刻度を考えるとき資産の大きさだけでなく
発生確率(成功確率)の考慮も必要。
＊メッセージ改竄した結果、人命への影響が本当に起きるかどうか

システムのセキュリティ

- システムとしてHSMを正しく使用しているかどうか
- システムの環境がソーシャル攻撃から守られるようになっているか
  - ➢もっとも弱いところが狙われる





もっとも弱いところを補強し続ける必要がある

*NIST(National Institute of Standards and Technology)
=アメリカ国立標準技術研究所

（参考） NIST*推奨鍵長

https://www.keylength.com/en/4/

Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Group	Elliptic Curve	Hash (A)	Hash (B)
Legacy [1]	80	2TDEA	1024	160	1024	160	SHA-1 [2]	
2019 - 2030	112	(3TDEA) [3] AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128	
2019 - 2030 & beyond	192	AES-192	384	7680	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

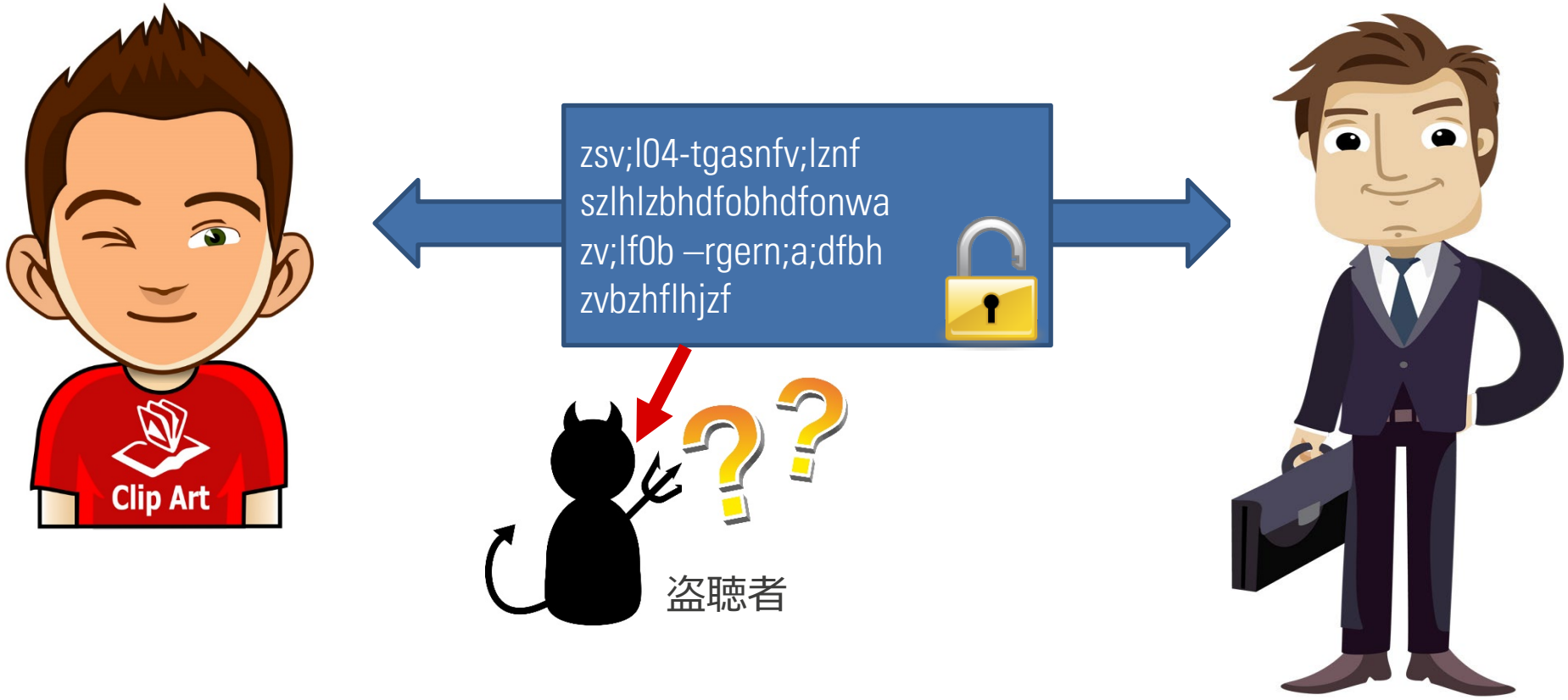
All key sizes are provided in bits. These are the minimal sizes for security.
Click on a value to compare it with other methods.

1. Algorithms and key lengths for 80-bit security strength may be used because of their use in legacy applications (i.e., they can be used to process cryptographically protected data). They shall not be used for applying cryptographic protection (e.g., encrypting).
2. SHA-1 has been demonstrated to provide less than 80 bits of security for digital signatures, which require collision resistance. In 2020, the security strength against digital signature collisions remains a subject of speculation.
3. Although 3TDEA is listed as providing 112 bits of security strength, its use has been deprecated (see SP 800-131A) through 2023, after which it will be disallowed for applying cryptographic protection. The use of a deprecated algorithm means that the algorithm or key length may be used if the risk of doing so is acceptable.

暗号の基礎

暗号とは

- 狭義には、通信路などで盗聴されないようにメッセージを変換する技術。

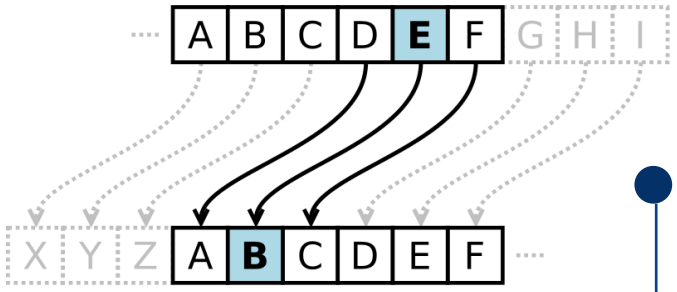


暗号の歴史

古代エジプト
- ヒエログリフ -

https://commons.wikimedia.org/wiki/File:Egypt_Hieroglyphe2.jpg

シーザー暗号



https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg

ヴィジュネル暗号

https://ja.wikipedia.org/wiki/ヴィジュネル暗号#/media/File:Vigenere-square.png

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

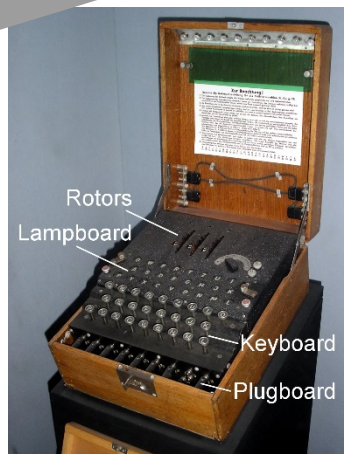
現代暗号

- AES暗号
- 量子暗号
- DES・RSA暗号

Future
2000
1977
1918
1400
B.C.100
B.C.600
B.C.3000

スキュタレー暗号

https://commons.wikimedia.org/wiki/File:Skytale.png

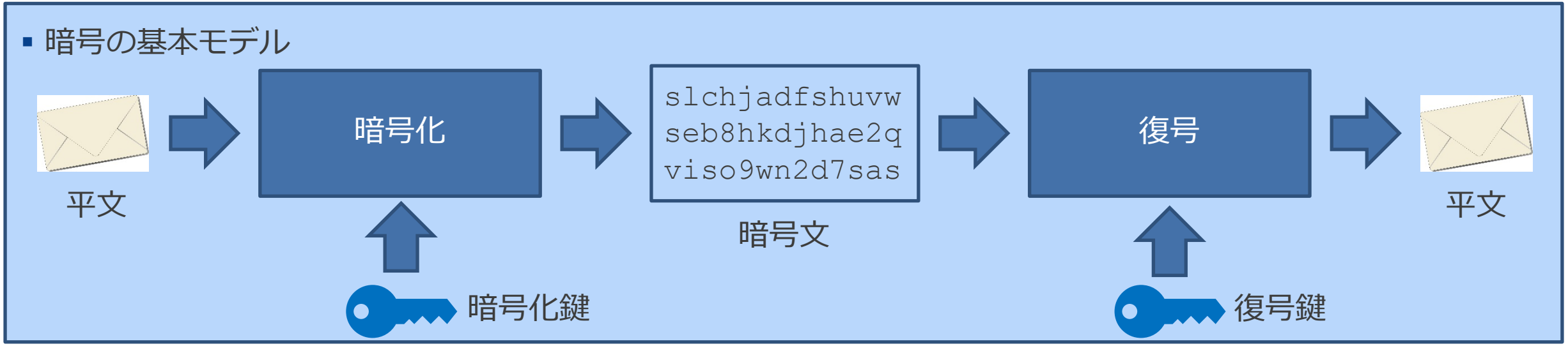


エニグマ暗号機

https://commons.wikimedia.org/wiki/File:EnigmaMachineLabeled.jpg

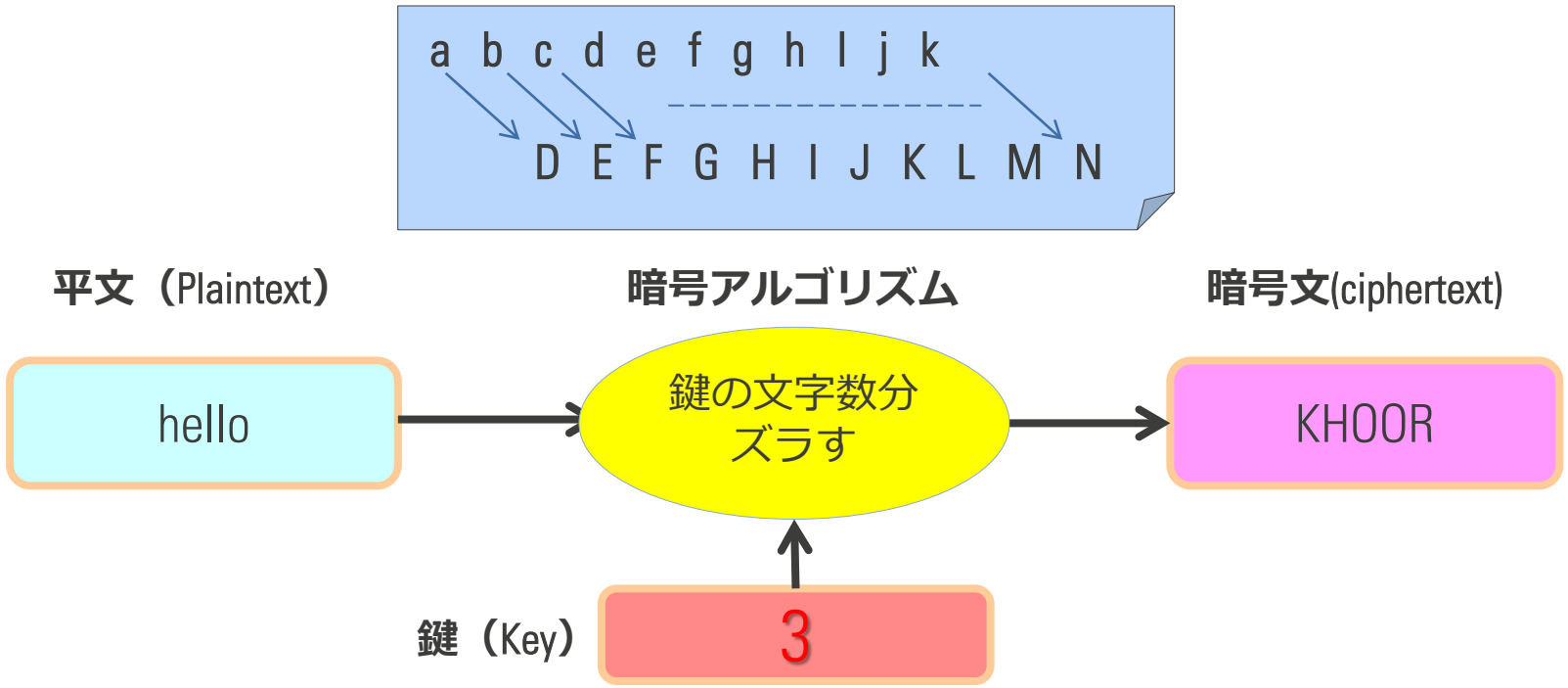
暗号用語

- 平文 (plaintext) 暗号化する前の元の文書、または暗号文を復号したあとの文書。
- 暗号文 (ciphertext) 平文を暗号化したもの。
- 暗号化 (encryption) 平文を暗号文に変換すること。
- 復号 (decryption) 暗号文を平文に変換すること。（復号化とは言わない）
- 暗号化鍵 (encryption key) 暗号化の際に利用される鍵
- 復号鍵 (decryption key) 復号の際に利用される鍵



古典的な暗号の例

- 暗号アルゴリズムと鍵　＜シーザー暗号を使った暗号化の例＞



※ 現代の暗号：アルゴリズム公開（裏を返せば鍵は秘密）
計算機による攻撃を想定した安全性を持つ

（参考）現代の暗号でアルゴリズムを公開する理由

■ 現代の暗号技術で暗号アルゴリズムが公開されるのは以下のような理由による。

- PCやスマートフォンなどで暗号化通信が利用されることが一般になっているため、アルゴリズムを公開してメーカーや国家を超えて同じアルゴリズムを使えるようにしておかないと、暗号通信ができない。

利便性

- アルゴリズムを公開することで多くの専門家による安全性検証が可能となり、アルゴリズムの信頼性が高まる。
- アルゴリズムの秘匿性を安全性の根拠としているような暗号では、一度アルゴリズムがばれてしまうと安全性が完全に失われる危険性がある。

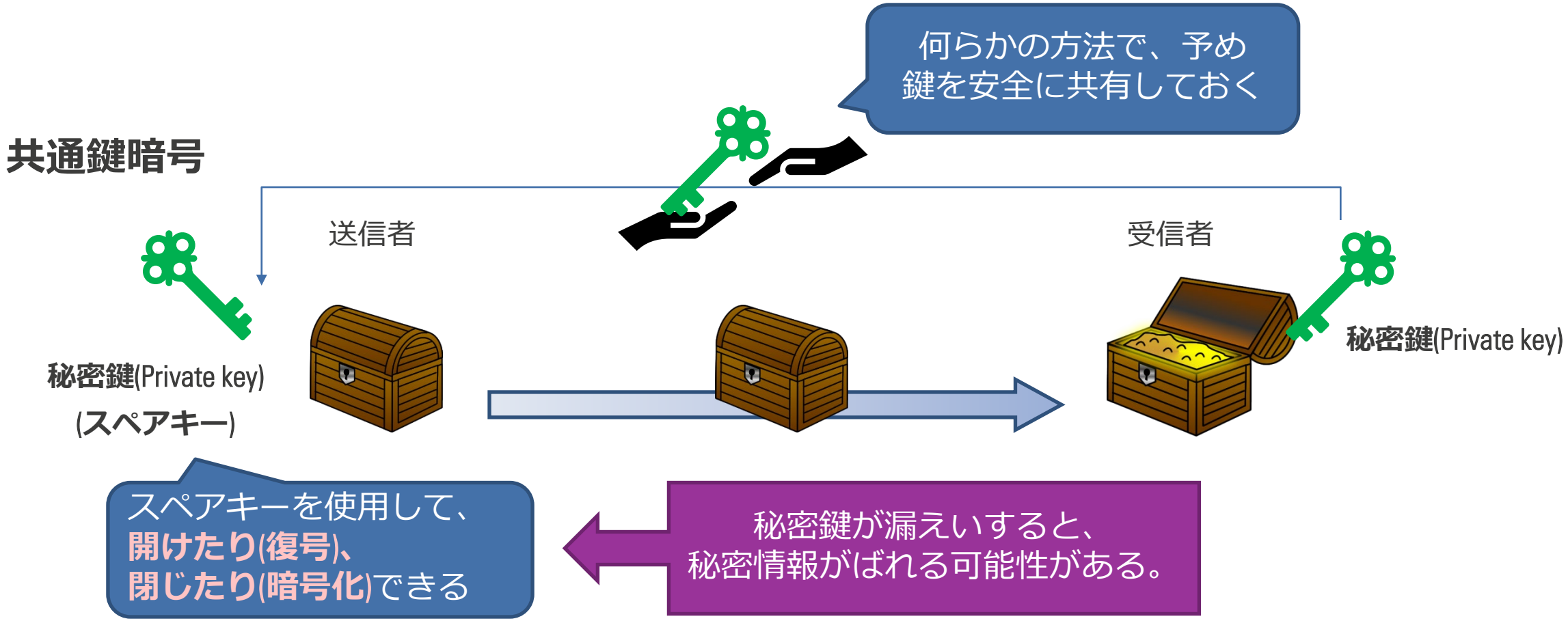
安全性

暗号化アルゴリズムを秘匿することを暗号の安全性の拠り所にしてはいけない。

共通鍵暗号と公開鍵暗号（共通鍵暗号）

- 代表的なアルゴリズム：
  - DES (Division of Employment Security)
  - AES(Advanced Encryption Standard)

- **共通鍵暗号：スペアキー**、公開鍵暗号：南京錠　と考えると分かり易い

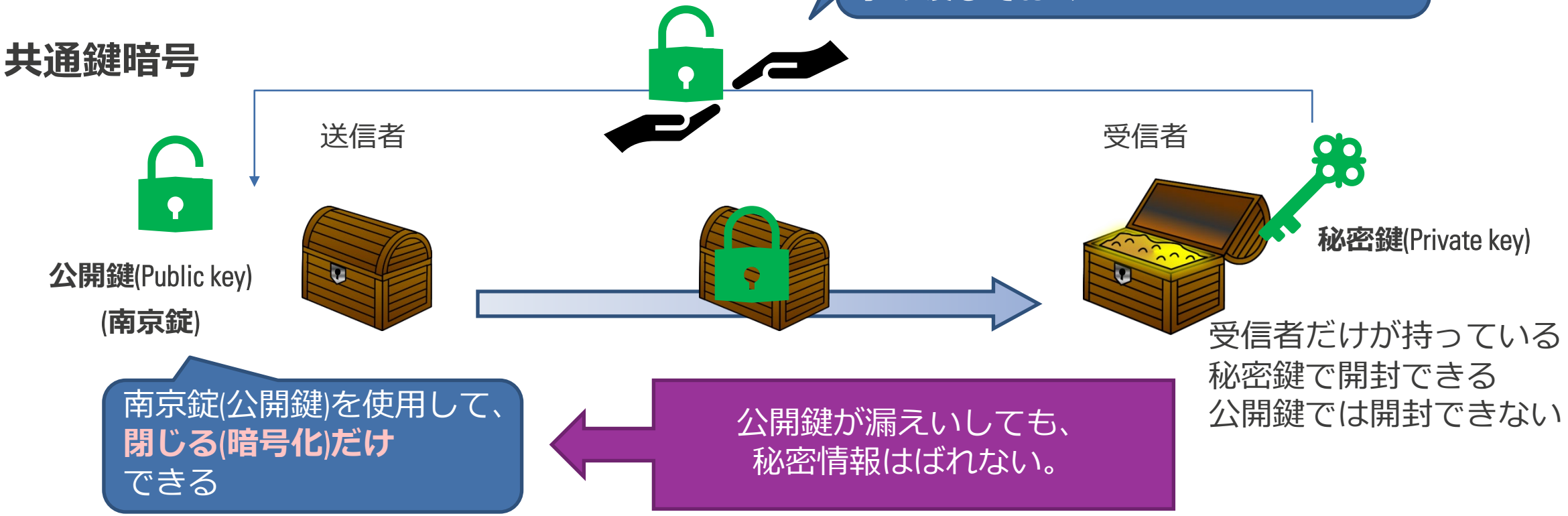


共通鍵暗号と公開鍵暗号（公開鍵暗号）

- 代表的なアルゴリズム：
  - RSA (Rivest–Shamir–Adleman)
  - ECC (Elliptic-curve cryptography)

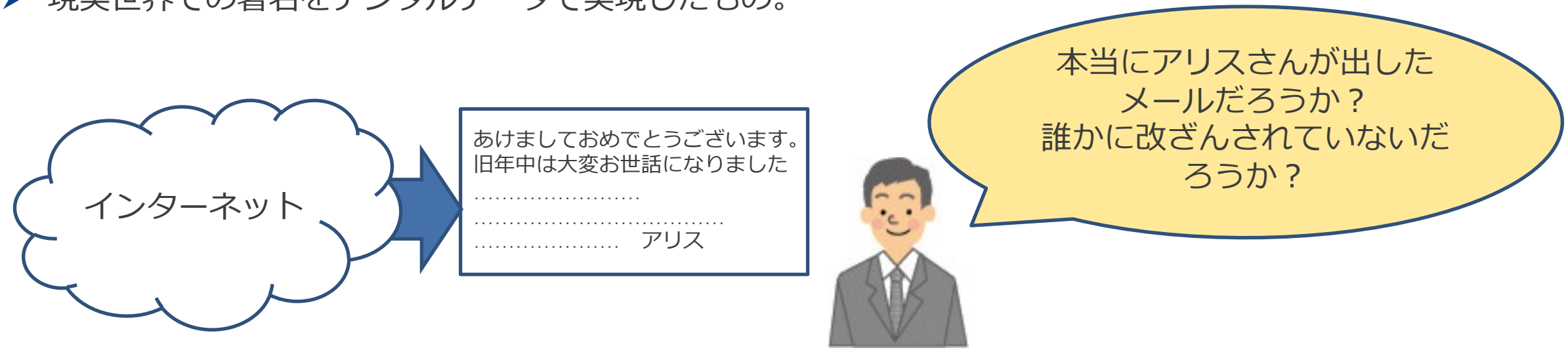
- 共通鍵暗号：スペアキー、**公開鍵暗号：南京錠**　と考えると分かり易い

受信者だけが持っている秘密鍵でのみ開けることのできる南京錠(公開鍵)を予め渡しておく



MACと電子署名 （MESSAGE AUTHENTICATION CODE）

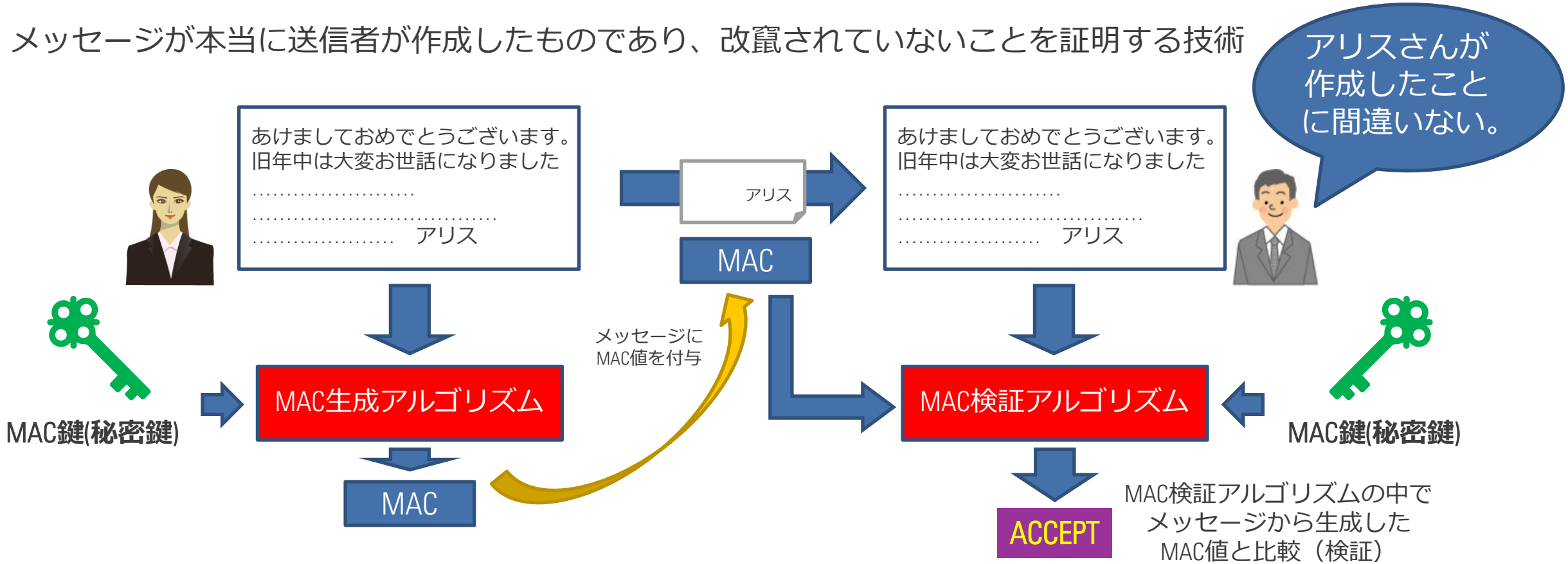
- 電子データが本当に意図した相手が作成したものか、改竄されていないかを保証する技術。
  - 現実世界での署名をデジタルデータで実現したもの。



インターネットからダウンロードしたプログラムやアップデータなどの場合、
本当に正しい発行者（マイクロソフトなど）が作ったもので、
改ざんされていないか保証できなければ、恐ろしくて実行できない。

MAC(MESSAGE AUTHENTICATION CODE)（メッセージ認証符号）

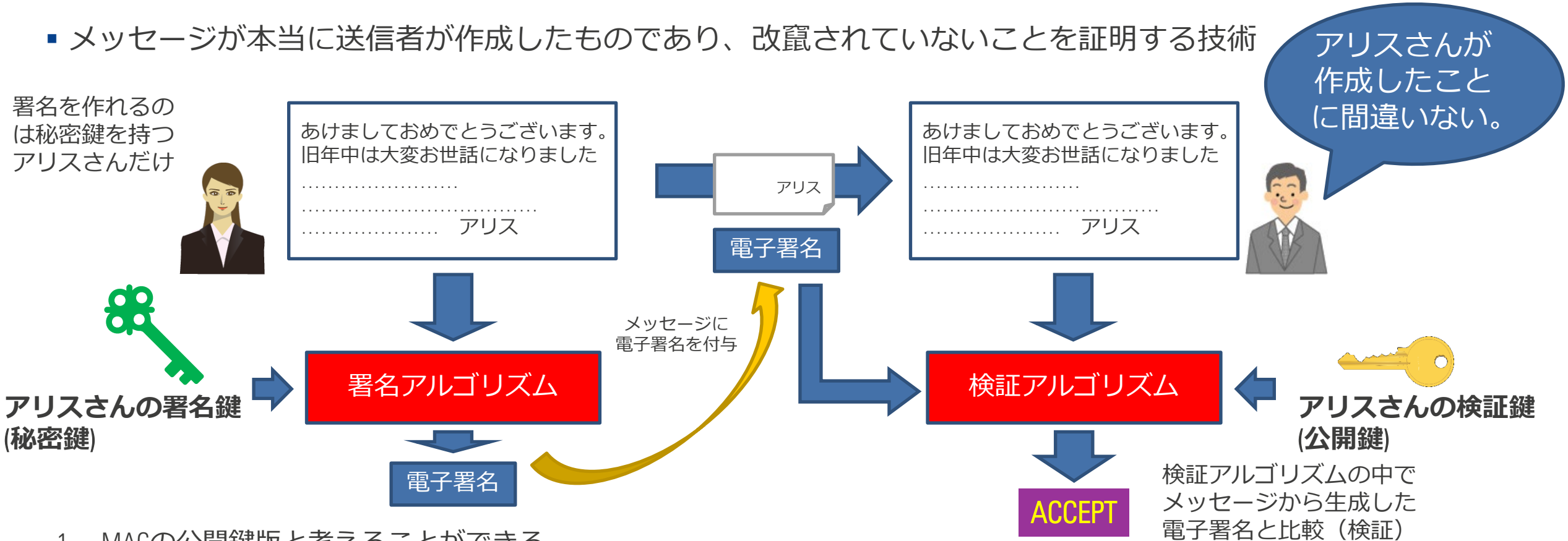
- メッセージが本当に送信者が作成したものであり、改竄されていないことを証明する技術



1. 送信者と受信者で鍵を共有しておく。メッセージに対して、鍵を使ってMACを作成する。
2. MAC鍵を共有している相手だけが検証可能。
   - 代表的なアルゴリズム：HMAC, CMAC

電子署名(DIGITAL SIGNATURE)

- メッセージが本当に送信者が作成したものであり、改竄されていないことを証明する技術



1. MACの公開鍵版と考えることができる。
2. 署名は署名鍵（秘密鍵）を用いて作成する。検証は検証鍵（公開鍵）を使って行う。
3. 検証鍵が公開なので、誰でも検証できる。
   - 代表的なアルゴリズム：RSA**署名**、ECDSA

他の人は同じ署名を作れない（検証のみ可能）

MACと電子署名の使い分け

- MACと電子署名の違い
  - 電子署名はMACが持っていない以下の３つの特徴を持っている。
    1. Public Verifiability : 誰でもメッセージに対する署名の検証が可能である性質。検証鍵が公開鍵であることからこの性質を持つことができる。
    2. Transferability : メッセージと署名を受け取った人が、そのメッセージと署名を第３者に対して署名の正当性を示すことができる。
    3. Non-repudiation（否認不可性） : 署名者が一度署名を作成して公開してしまうと、後から署名を作成したことを否認できない。
  - MACを使うほうがよい場合は以下の両方を満たすとき。（MACの方が電子署名より非常に処理が速い）
    1. 電子署名の持つ３つの特徴が不要な（もしくは持っていてほしくない）とき
    2. 鍵の共有が可能なとき。

乱数生成器

- パスワードや鍵の生成のためには、良質な乱数が必要。
- 第三者に予測されるとセキュリティ上問題になる。
- 乱数は下記に分類することが出来る。

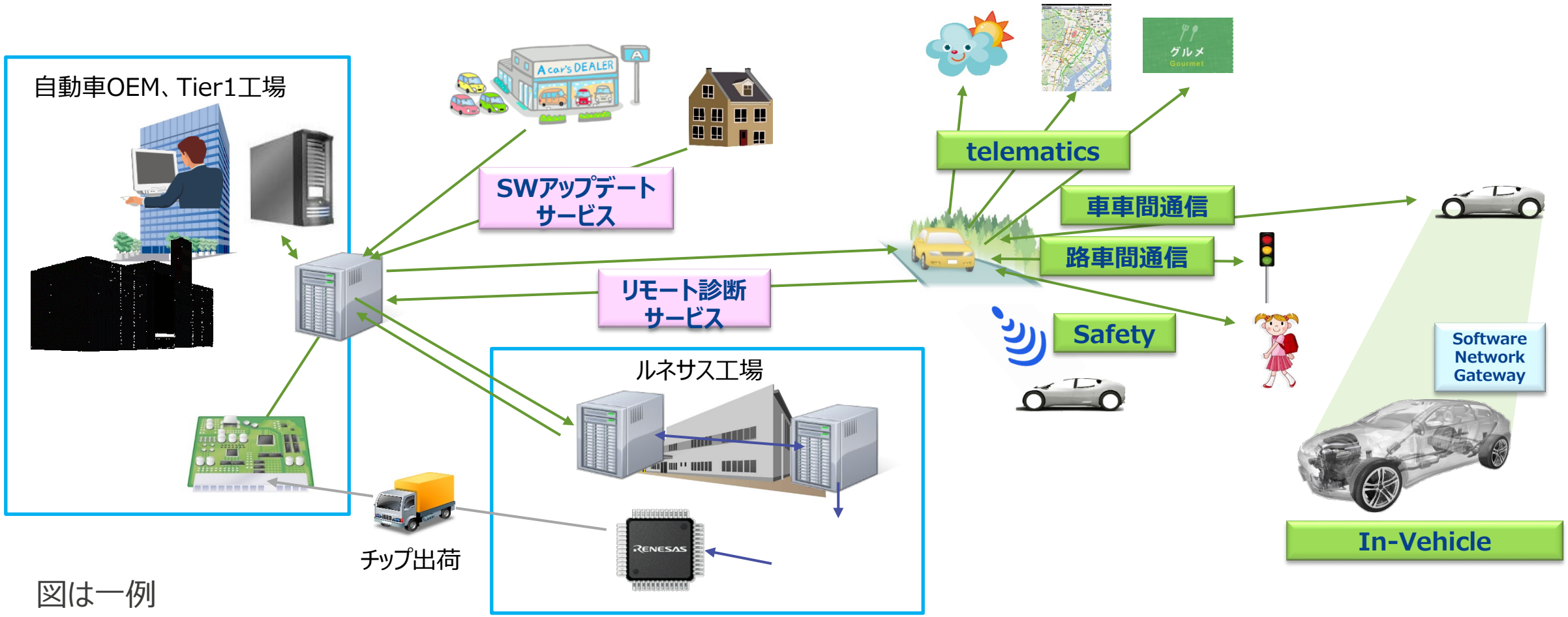
ランダムな値を用いることで、パスワードや鍵の推測を難しくする。

	疑似乱数 (Pseudo Random Number)	真性乱数 (True Random Number)
生成方法	アルゴリズムに基づいた計算により生成。短い乱数値（シード：真正乱数から生成）から長い乱数を生成する。回路規模は比較的小さい。 高速処理が可能。	物理的なランダム要因(回路の熱雑音等)から生成。アナログ回路が必要。高速化が難しい。
周期性	必ず周期性を持っている	各ビットが互いに独立
再現性	初期値とアルゴリズムを与えれば、全ビットが再現可能	1/0の発生確率が等しく、予測不可能性を持つ
用途	暗号で用いる秘密鍵、パスワード等（より長い鍵長、パスワード長）	暗号で用いる秘密鍵、パスワード等 疑似乱数のシード
主な規格	AIS20, NSIT SP800-90A	AIS31, NSIT SP800-90B

クルマのセキュリティ動向

自動運転時代のサービスとセキュリティ

- 自動運転の時代には各種サービスとクルマが相互に接続され情報が相互にやり取りされる(クルマのIT化)



図は一例

クルマのセキュリティ インシデント

Experimental Security Analysis of a Modern Automobile

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno
Department of Computer Science and Engineering
University of Washington
Seattle, Washington 98195–2350
Email: {supersat,aczeskis,franzi,shwetak,yoshi}@cs.washington.edu

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage
Department of Computer Science and Engineering
University of California San Diego
La Jolla, California 92093–0404
Email: {s,dlmccoy,brian,d8anders,hovav,savage}@cs.ucsd.edu

***Abstract*—Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced a range of new potential risks. In this paper we experimentally evaluate these issues on a modern automobile and demonstrate the fragility of the underlying system structure. We demonstrate that an attacker who is able to infiltrate virtually any Electronic Control Unit (ECU) can leverage this ability to completely circumvent a broad array of safety-critical systems. Over a range of experiments, both in the lab and in road tests, we demonstrate the ability to adversarially control a wide range of automotive functions and completely ignore driver input—including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on. We find that it is possible to bypass rudimentary network security protections within the car, such as maliciously bridging between our car's two internal subnets. We also present composite attacks that leverage individual weaknesses, including an attack that embeds malicious code in a car's telematics unit and that will completely erase any evidence of its presence after a crash. Looking forward, we discuss the complex challenges in addressing these vulnerabilities while considering the existing automotive ecosystem.**

***Keywords*—Automobiles, communication standards, communication system security, computer security, data buses.**

I. INTRODUCTION

Through 80 years of mass-production, the passenger automobile has remained superficially static: a single gasoline-powered internal combustion engine; four wheels; and the familiar user interface of steering wheel, throttle, gearshift, and brake. However, in the past two decades the underlying control systems have changed dramatically. Today's automobile is no mere mechanical device, but contains a myriad of computers. These computers coordinate and monitor sensors, components, the driver, and the passengers. Indeed, one recent estimate suggests that the typical luxury sedan now contains over 100 MB of binary code spread across 50–70 independent computers—*Electronic Control Units* (*ECUs*) in automotive vernacular—in turn communicating over one or more shared *internal network buses* [8], [13].

While the automotive industry has always considered *safety* a critical engineering concern (indeed, much of this new software has been introduced specifically to *increase* safety, e.g., *Anti-lock Brake Systems*) it is not clear whether vehicle manufacturers have anticipated in their designs the possibility of an adversary. Indeed, it seems likely that this increasing degree of computerized control also brings with it a corresponding array of potential threats.

Compounding this issue, the attack surface for modern automobiles is growing swiftly as more sophisticated services and communications features are incorporated into vehicles. In the United States, the federally-mandated *On-Board Diagnostics* (*OBD-II*) port, under the dash in virtually all modern vehicles, provides direct and standard access to internal automotive networks. User-upgradable subsystems such as audio players are routinely attached to these same internal networks, as are a variety of short-range wireless devices (Bluetooth, wireless tire pressure sensors, etc.). Telematics systems, exemplified by General Motors' (GM's) OnStar, provide value-added features such as automatic crash response, remote diagnostics, and stolen vehicle recovery over a long-range wireless link. To do so, these telematics systems integrate internal automotive subsystems with a remote command center via a wide-area cellular connection. Some have taken this concept even further—proposing a "car as a platform" model for third-party development. Hughes Telematics has described plans for developing an "App Store" for automotive applications [22] while Ford recently announced that it will open its Sync telematics system as a platform for third-party applications [14]. Finally, proposed future vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2X) communications systems [5], [6], [7], [25] will only broaden the attack surface further.

Appears in *2010 IEEE Symposium on Security and Privacy*. See http://www.autosec.org/ for more information. 1

http://www.autosec.org/pubs/cars-oakland2010.pdf

DEFCON

http://illmatics.com/car_hacking.pdf

BlackHat

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

2010

2011

2012

2013

2014

2015

2016

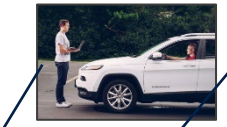
2017

https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/

クルマのセキュリティ動向
標準化・法制化

クルマのセキュリティ標準化動向






2000~ 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

日本

IPA

JSAE ▼TP-15002

JASPAR

ISO26262 2nd Edition

欧州

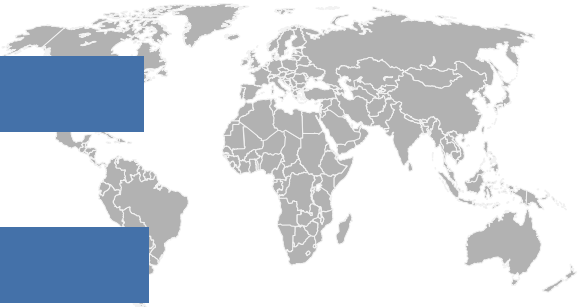
Car2Car Communication Consortium

HIS/SHE

PRESERVE

EVITA

AUTOSAR



ISO/SAE21434 IS▼

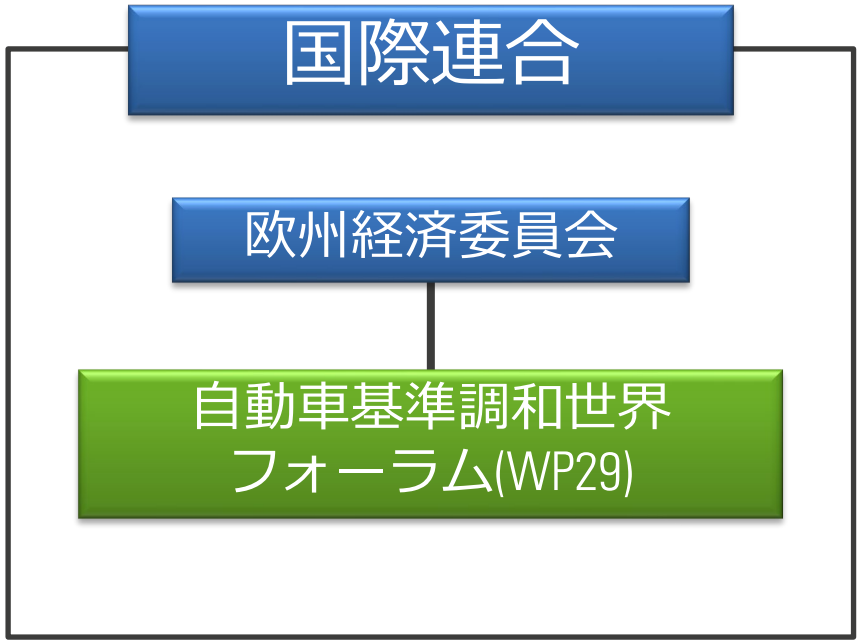
UNR R155▼

北米

SAE TEVEES18 ▼J3061

自動車基準調和世界フォーラム（WP29）

- **サイバーセキュリティ及びデータ保護に係るガイドライン**　(2016 Nov)
  - 通信利用型自動運転車へのリモートアクセスに係るオンラインサービスについては、強力な相互認証を持たなければならない旨規定。



WP29の主な活動
- 安全一般
- 衝突安全
- ブレーキと走行装置
- 排出ガスとエネルギー
- 騒音
- 灯火器

WP29で定められたUNR-155で車両型番を得るために必要な要件を定義。

ISO/SAE 21434は上記要件の具体的な実施例（参照資料）の位置づけ

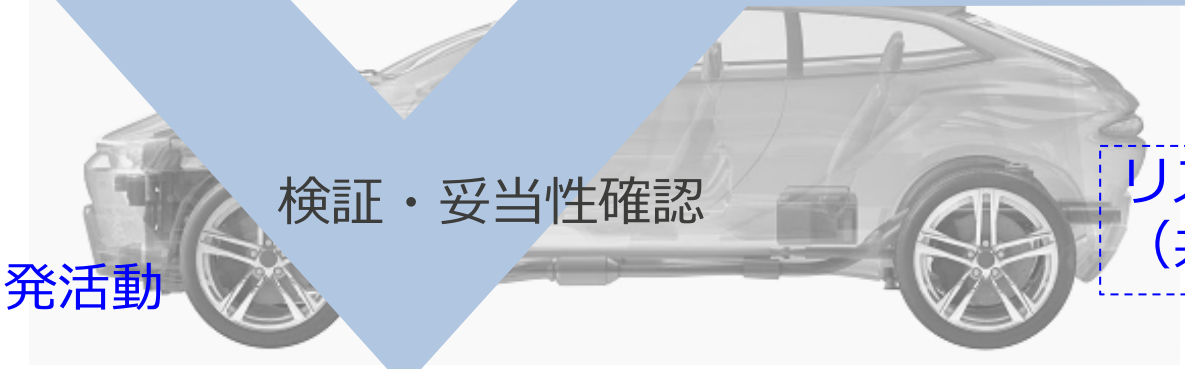
ISO/SAE 21434 概要

組織活動

セキュリティ管理（組織定義・監視・一般管理等）
生産・運用・メンテナンス・廃棄

コンセプト
製品開発

インシデント対応



検証・妥当性確認

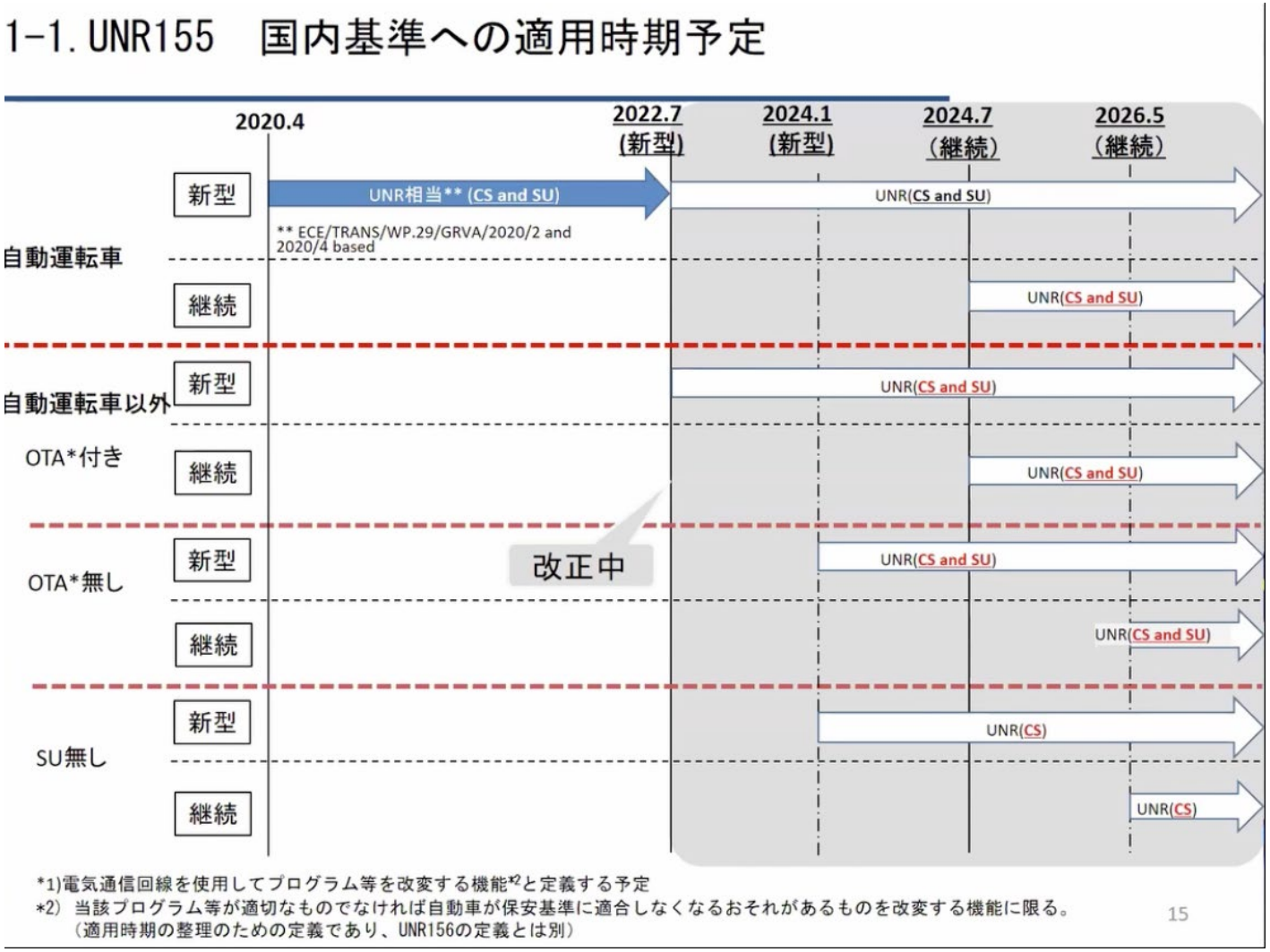
開発活動

リスク管理
（共通部品）

ISO規格は購入時に公開範囲が定められるため、詳細をお話しすることはできません。

ご興味のある方は、ご購入を検討ください。

ISO/SAE 21434 （UNR155 国内対応スケジュール）



https://media.dglab.com/2020/12/16-cs-01/

クルマのセキュリティ動向
車載マイコンの標準化

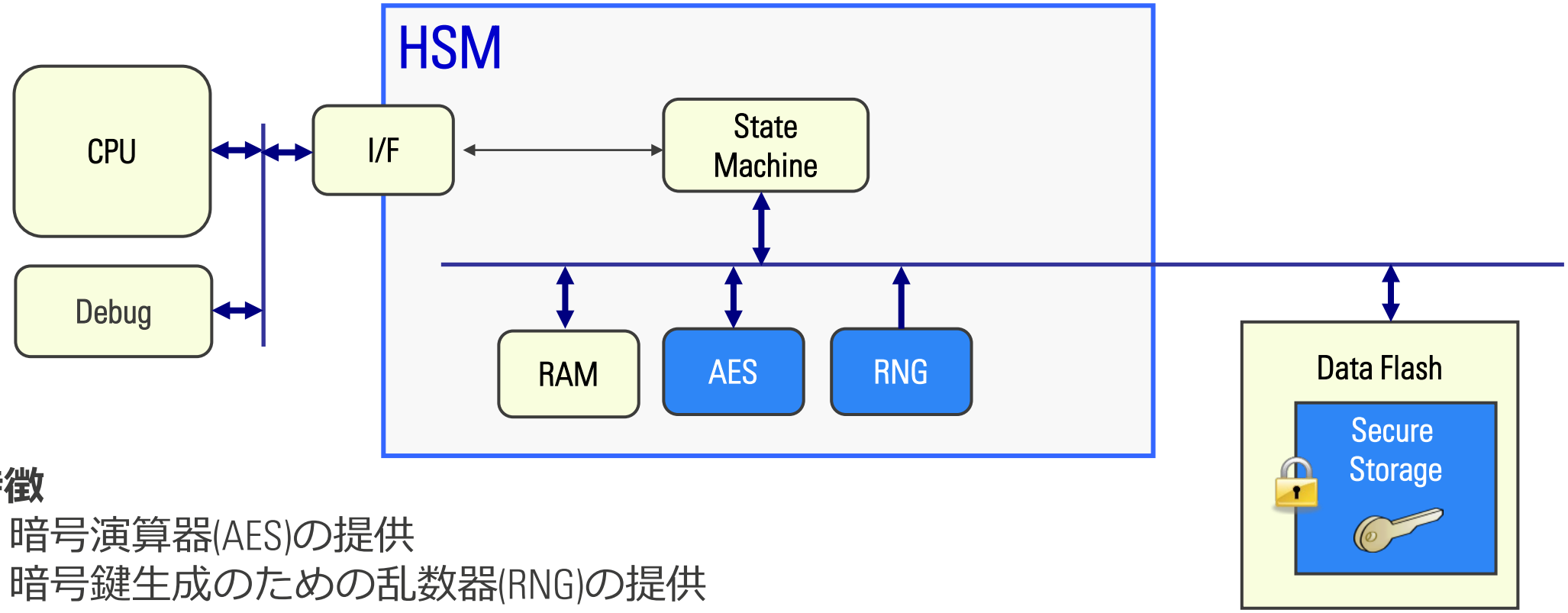
EVITA/SHE MCU 機能要求

HSM(Hardware Security Module)に求められるセキュリティ機能をガイド

	EVITA full	EVITA medium	EVITA light	SHE
Assumption Use case	V2X	Automotive ECU	Automotive ECU	ECU
Internal CPU	Yes	Yes	No(state machine)	No(state machine)
Code Flash	Yes	Yes	No	No
RAM	Yes	Yes	Option	Yes
EEPROM (Data Flash)	Yes	Yes	Option	Yes
HW crypto algorithms	AES-128, ECC-256, WHIRLPOOL	AES-128	AES-128	AES-128
Random Number Generator	AES-PRNG w/ TRNG seed	AES-PRNG w/ TRNG seed	AES-PRNG w/ external seed	AES-PRNG w/ TRNG seed

AES : Advanced Encryption Standard (Key size 128 bit), ECC : Elliptic Curve Cryptography (Key size 256 bit), PRNG : Pseudo Random Number Generator
TRNG : True Random Number Generator, WHIRLPOOL : One of Hash function

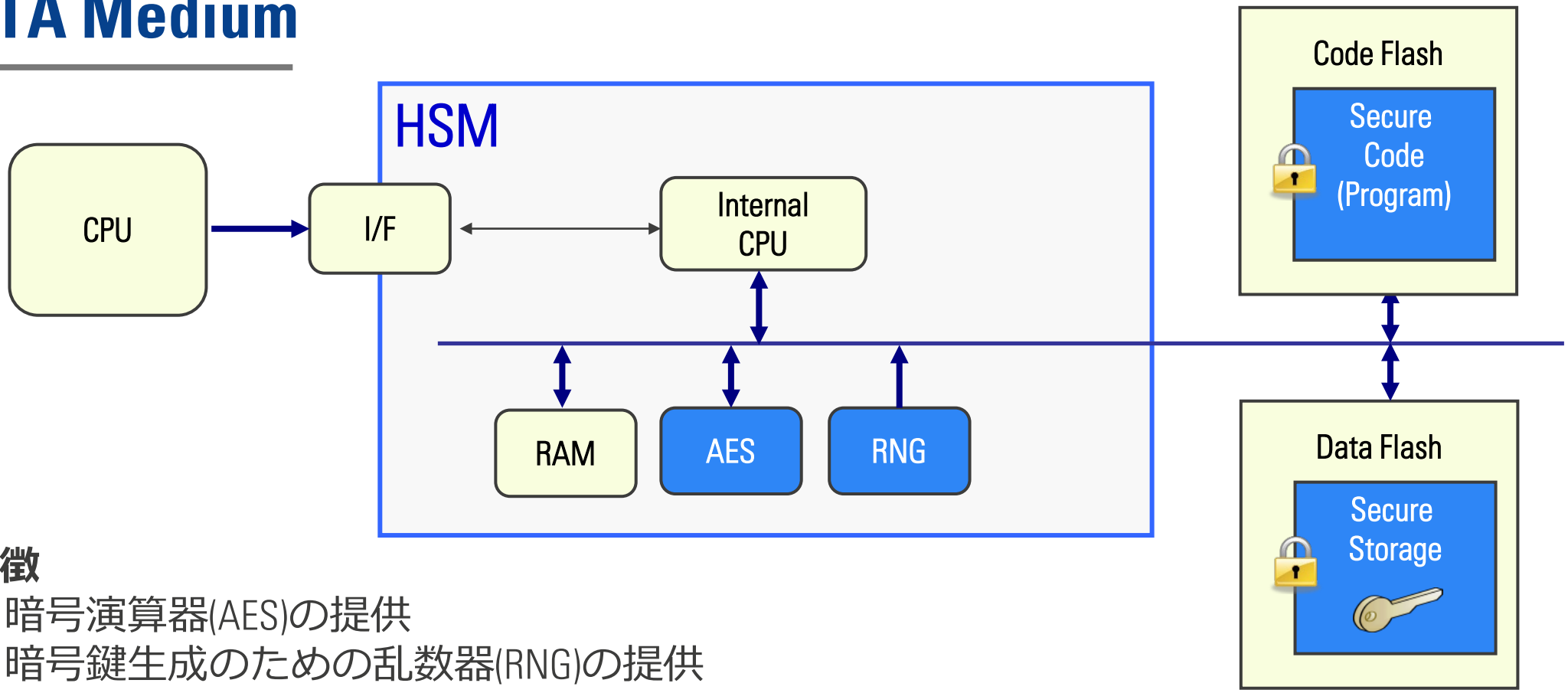
EVITA Light



特徴

- 暗号演算器(AES)の提供
- 暗号鍵生成のための乱数器(RNG)の提供
- 暗号鍵(AES)保存の為のセキュアストレージの提供
  （CPUから暗号鍵を読み出すことはできない）

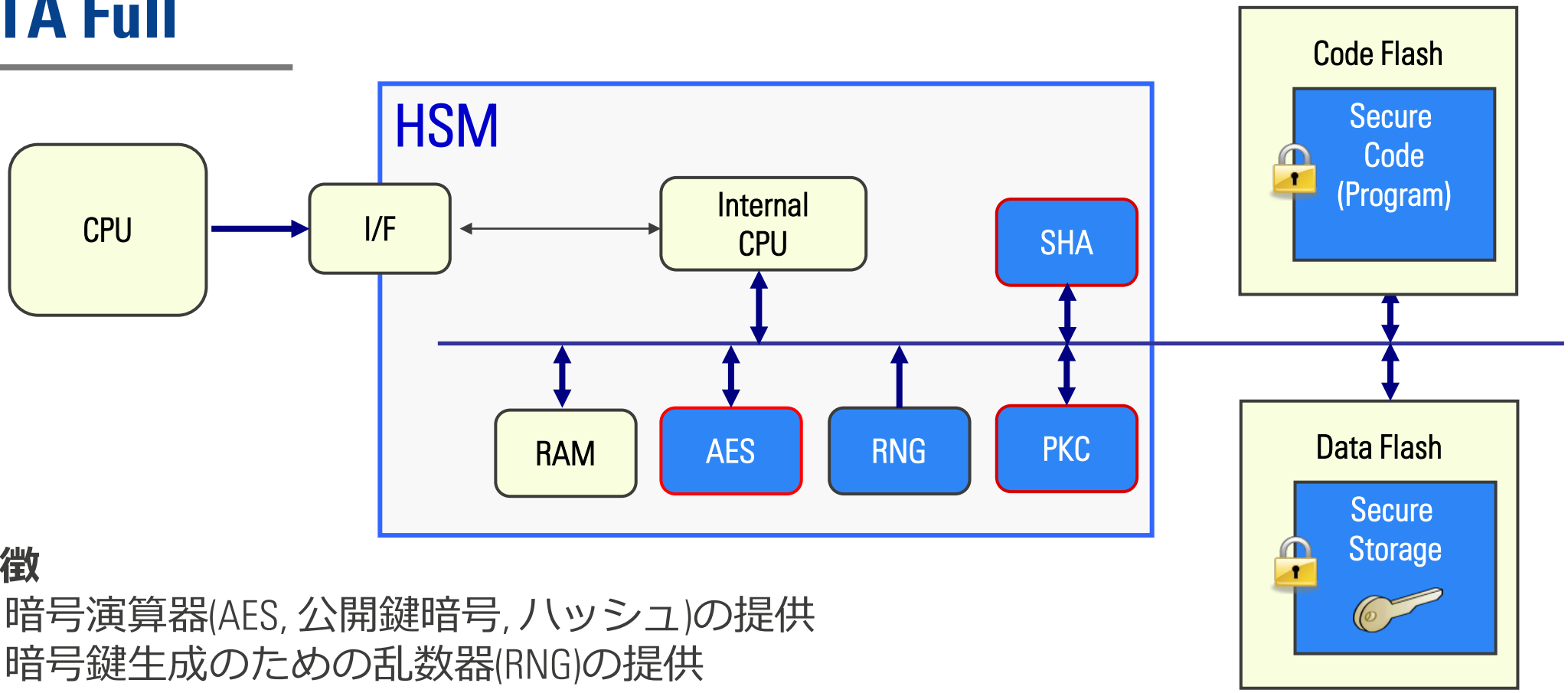
EVITA Medium



特徴

- 暗号演算器(AES)の提供
- 暗号鍵生成のための乱数器(RNG)の提供
- 暗号鍵等のセキュア情報保存の為のセキュアストレージの提供
  （CPUからセキュア情報を読み出すことはできない）
- セキュアプログラムを実行する為の専用Internal CPU，セキュアストレージの提供
  （CPUからInternal CPUのセキュアプログラムを読み出すことはできない）

EVITA Full



特徴

- 暗号演算器(AES, 公開鍵暗号, ハッシュ)の提供
- 暗号鍵生成のための乱数器(RNG)の提供
- 暗号鍵等のセキュア情報保存の為のセキュアストレージの提供
  （CPUからセキュア情報を読み出すことはできない）
- セキュアプログラムを実行する為の専用Internal CPU，セキュアストレージの提供
  （CPUからInternal CPUのセキュアプログラムを読み出すことはできない）

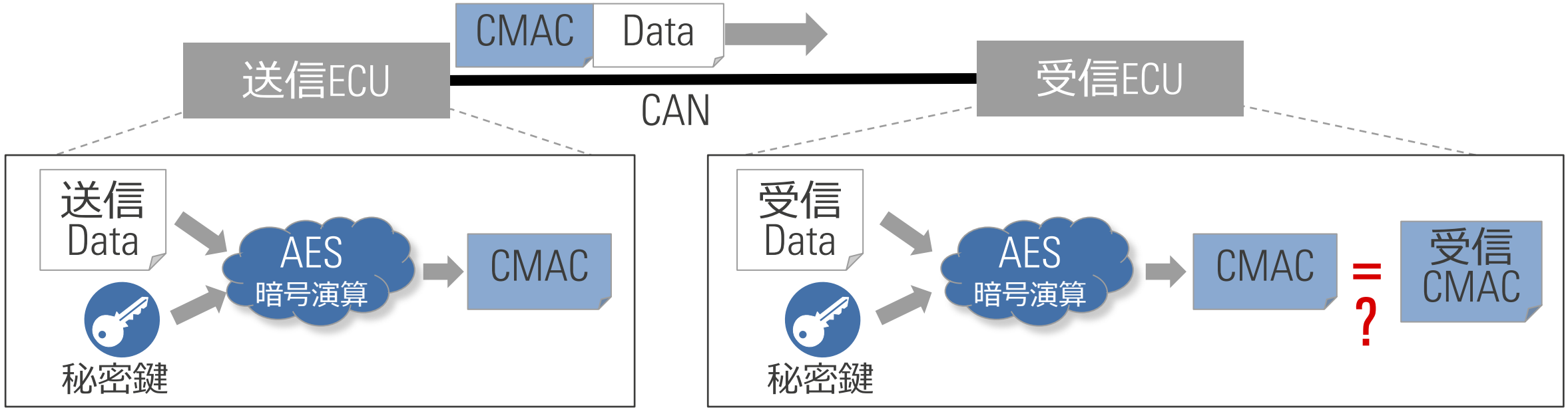
車載マイコン内蔵HSMによるセキュリティ対策実装例

#	手法例	説明
①	メッセージ認証	• 受け取ったメッセージが正しい相手から送られたものかどうかを検証できる • 受け取ったメッセージの改ざん有無を検証できる
②	セキュアブート	• プログラムが改ざんされていない事(改ざんされている事)を確認出来る

① メッセージ認証(CMAC)

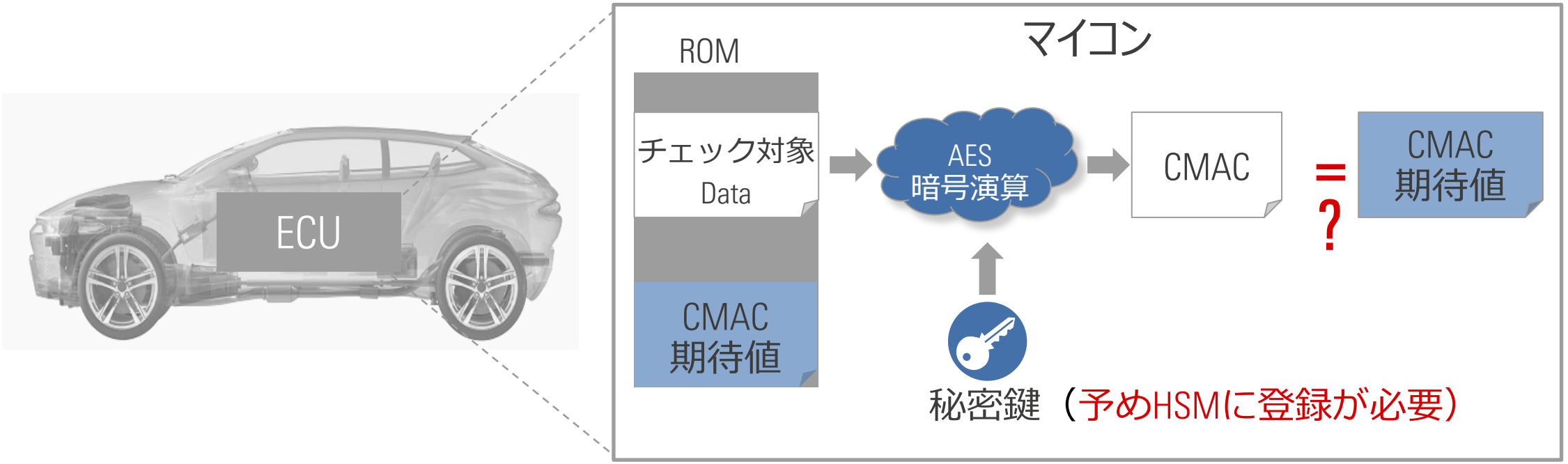
- CMAC: Cipher based MAC (Message Authentication Code)
- EVITA light要求のAES128ビットで実現可能

➢ネットワーク内部への不正アクセスを排除可能
➢上位のシステムを乗っ取られている場合排除不可能



② セキュアブート

- プログラムの更新とプログラム保護のセキュアブートはセットになる
- ブートアップ時に改ざんを防止したいROMデータのCMAC値をチェック
- チェック対象のプログラムが改ざんされていないことを確認
- 上位のシステムを乗っ取られている場合排除不可能



まとめ

まとめ

- 「セキュリティ」は安全を意味します。安全とは、守らなければならない大切なものが、危害や損傷を受けない正常な状態にある事です。（翔泳社　情報セキュリティスペシャリスト　より一部引用）
- 暗号とは、狭義には、通信路などで盗聴されないようにメッセージを変換する技術です。
- 近年車両に対するハッキング事例が増加しており、車載セキュリティの重要性が増しています。また、UNR-155やISO/SAE 21434にみられる車載サイバーセキュリティの法令化(2020年/7月～)によって、車両OEM/Tier1の車載セキュリティ対応が待ったなしの状況となっています。
- しかしながら、車載ECUに搭載されるセキュリティ技術も進化していますので、本日の講義が皆様のセキュリティ技術向上の一助になれば幸いです。

RENESAS

BIG IDEAS FOR EVERY SPACE