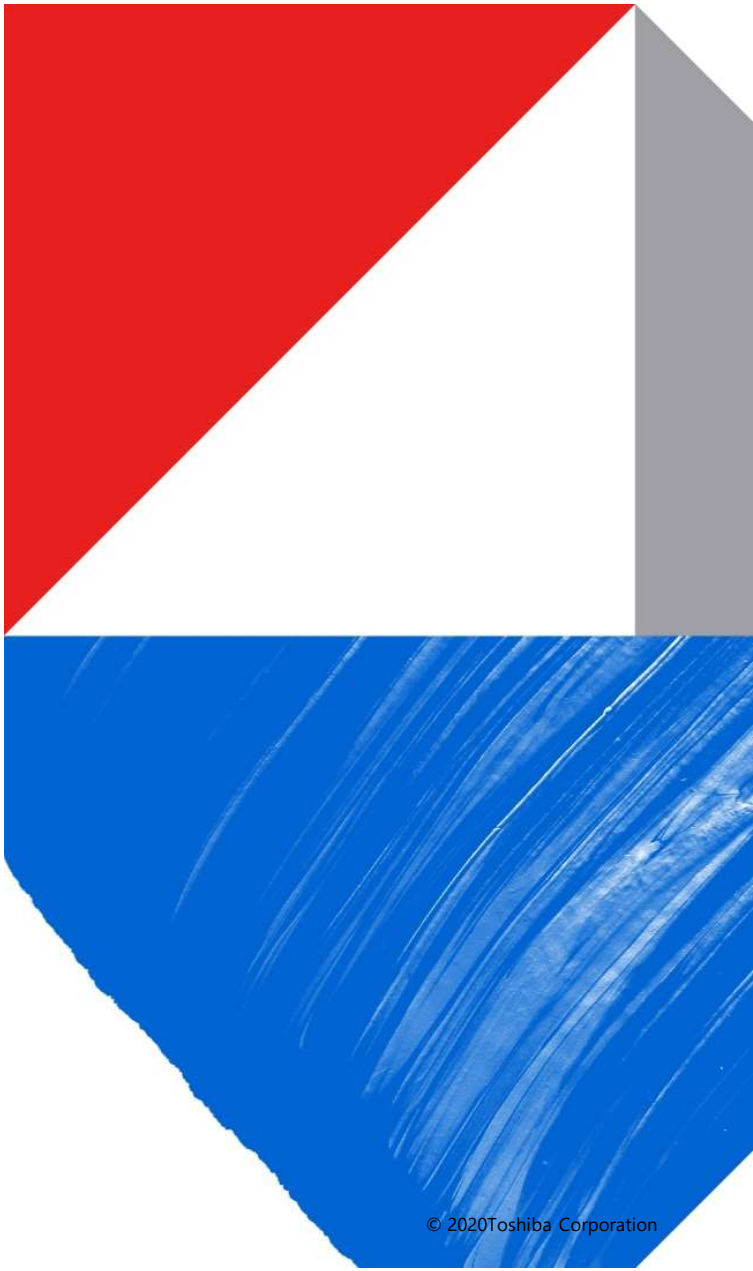
TOSHIBA

OWS2020
ファームウェア更新向けOSSのセキュリティベンチマーク



2020/10/27

東芝
東芝研究開発センター
〇小池竜一，藤松由里恵，蒋丹，金井遵，鬼頭利之

自己紹介

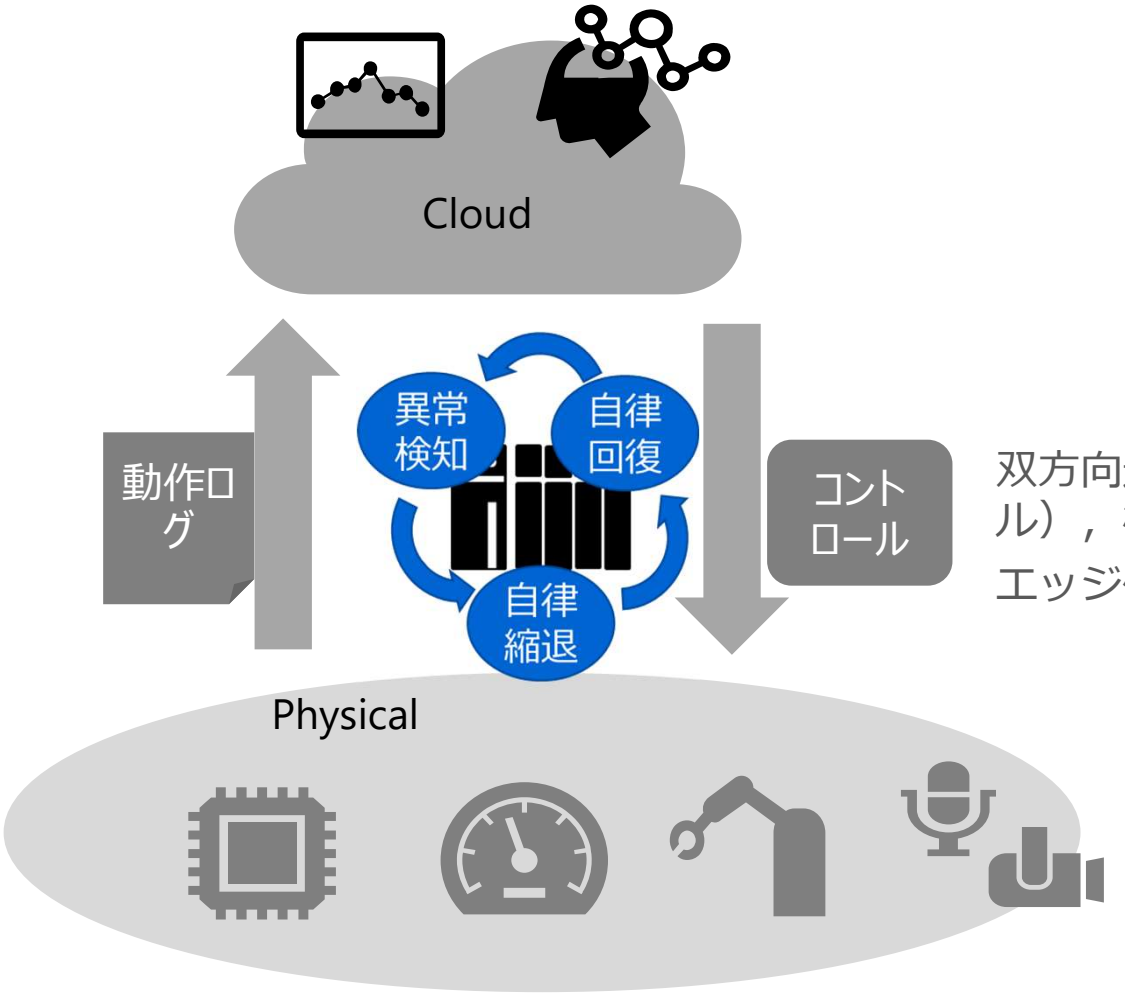
- 名前: 小池 竜一
- 所属: 東芝・東芝研究開発センター
- 業務内容: セキュリティに関する研究・開発
- これまでの経歴
  - P2Pコンテンツセキュア配信
  - Androidにおけるアクセス制御拡張
  - 組み込み機器セキュリティ
  - CSIRT（インシデント対応チーム）

はじめに

- ファームウェア更新の位置づけ
  - ファームウェア = デバイス上で動作するソフトウェア全般
- ファームウェア更新に関連する脅威
- ベンチマーク対象オープンソースソフトウェア（OSS）
- ベンチマーク結果
  - 企業としてのベンチマーク軸

Cyber Physical System（CPS）な世界

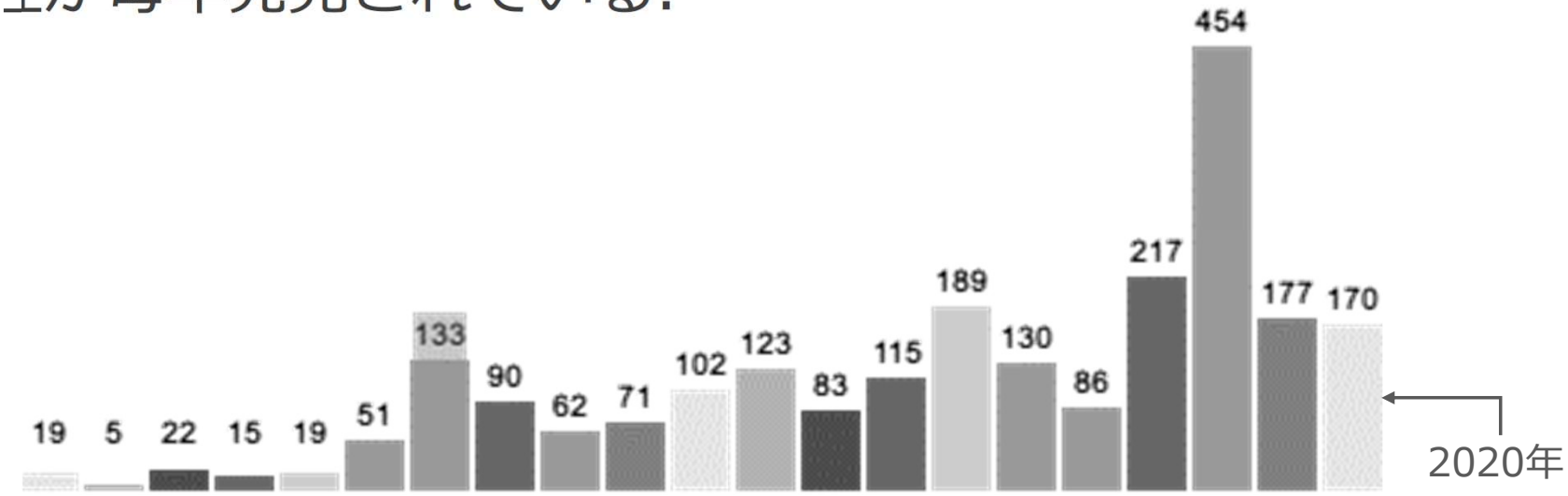
CPSサービスでは**双方向通信**によりサイバー攻撃のリスクが増大



双方向通信における下り制御（コントロール），機器の動作と密接に関連しておりエッジ側のリスクが増大.

ソフトウェア脆弱性をゼロにすることは不可能

- セキュリティ事故の原因: 脆弱性，バグ
- ソフトには必ず脆弱性が含まれる.
- 世界で最も監視の目の多いはずの Linux Kernelも
  脆弱性が毎年発見されている.

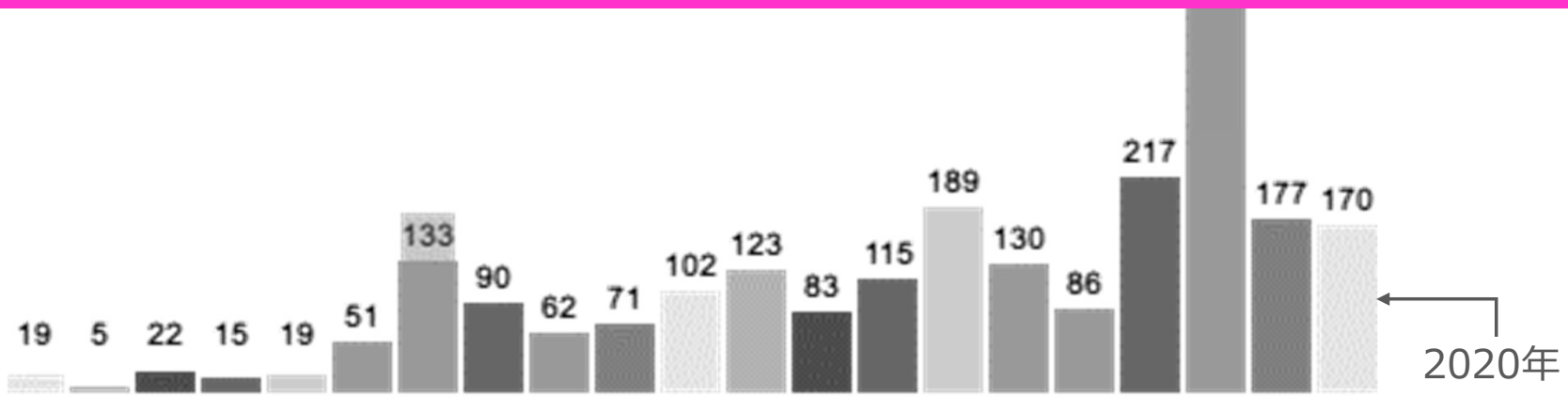


Linux Kernelの脆弱性発見数 (CVEDetails調べ)

ソフトウェア脆弱性をゼロにすることは不可能

- セキュリティ事故の原因: 脆弱性，バグ
- ソフトには必ず脆弱性が含まれる

人類の科学力では脆弱性の無いソフトはまだ作れない



Linux Kernelの脆弱性発見数 (CVEDetails調べ)

ファームウェア更新の必要性とOSS

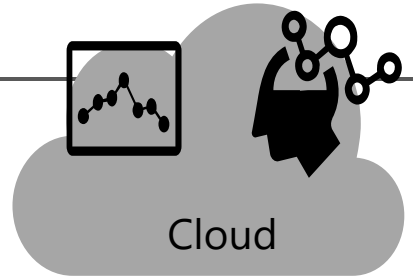
- **セキュアかつ低コストなファームウェア更新（FW更新）が必須.**

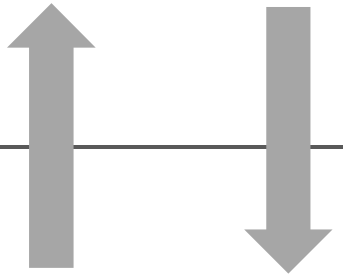
- 一方，現場においては製品・システムのセキュリティ機能は差異化ポイントと認められにくい現実がある.
  - 「セキュリティの確保は当たり前だよね」
  - 「これ自体に大きな開発コストはかけてほしくないね」

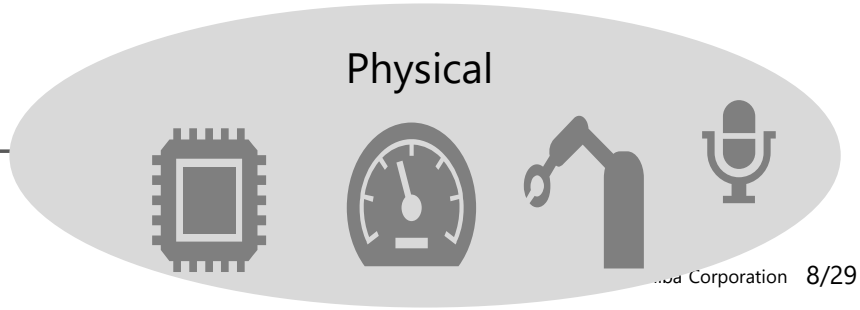
- → **FW更新に関するOSSのベンチマークを実施**

FW更新共通プラットフォームの全体像

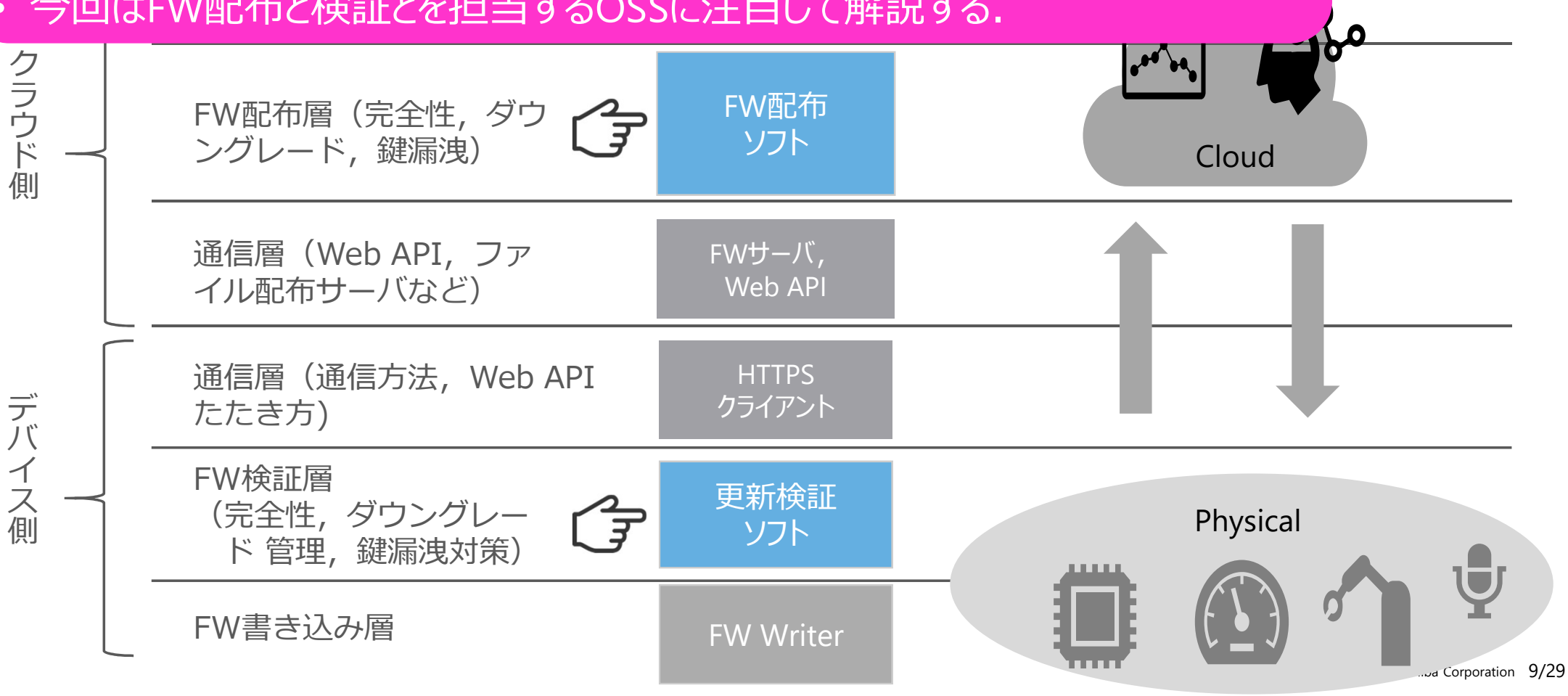
	機能	実装
クラウド側	FW操作・指示層（GUI）	FW管理 コンソール
	FW配布層（完全性，ダウングレード，鍵漏洩）	FW配布 ソフト
	通信層（Web API，ファイル配布サーバなど）	FWサーバ， Web API
デバイス側	通信層（通信方法，Web API たたき方）	HTTPS クライアント
	FW検証層 （完全性，ダウングレード 管理，鍵漏洩対策）	更新検証 ソフト
	FW書き込み層	FW Writer







- コンソールにあたる部分のOSSは数が少なく，当然デファクトなものは存在しない.
- コンソールとFW Writerとが密結合しているものが多く汎用性がない点.
  - 多様なデバイスを抱える当社としては活用が難しい.
- 今回はFW配布と検証とを担当するOSSに注目して解説する.



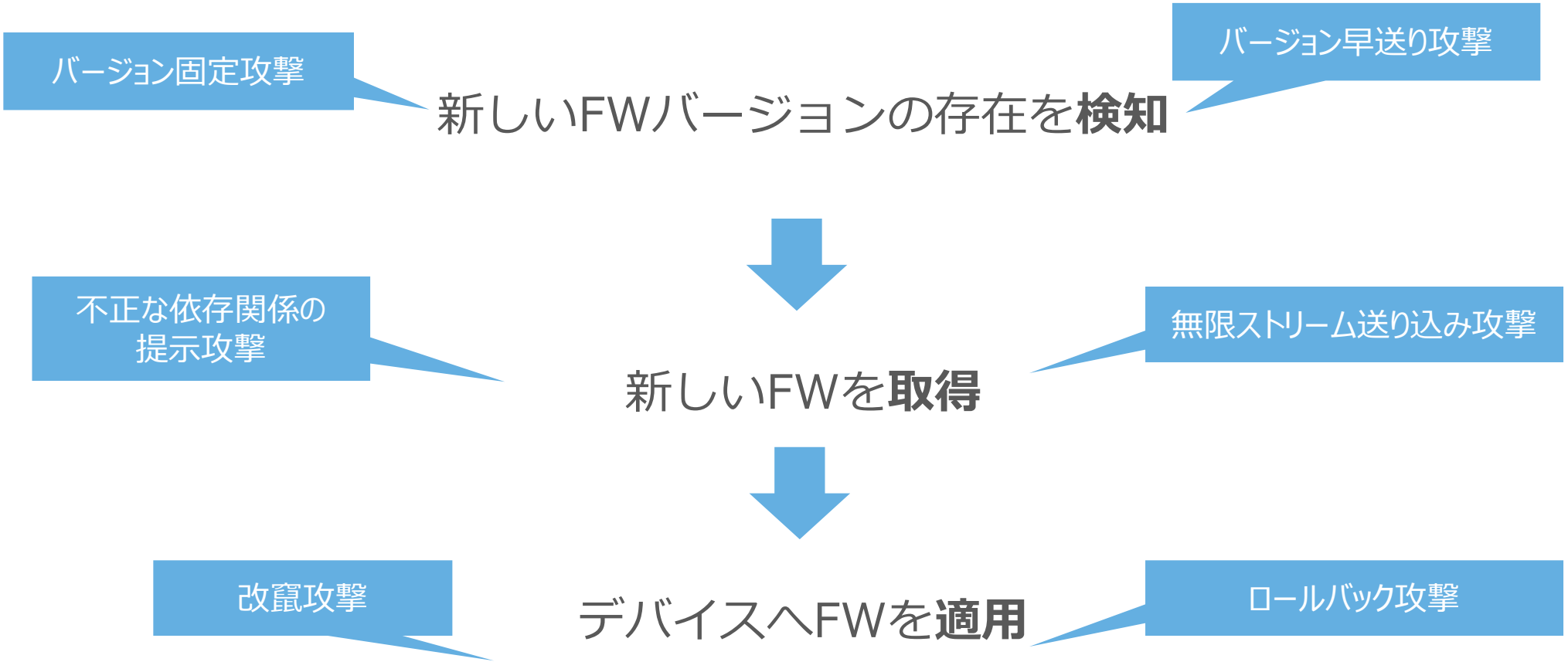
ファームウェア（FW）更新とは

新しいFWバージョンの存在を**検知**

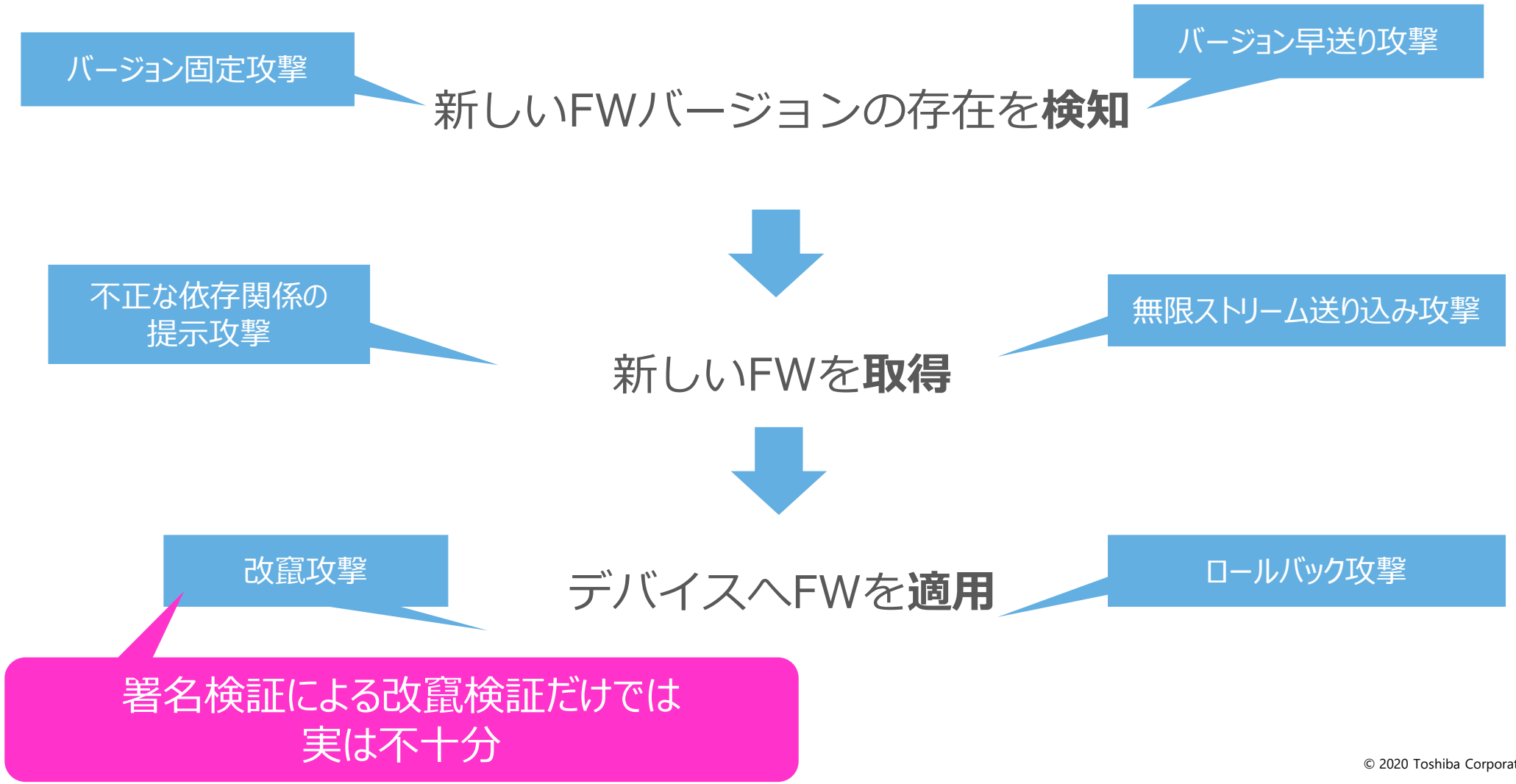
新しいFWを**取得**

デバイスへFWを**適用**

FW更新に関する脅威は改竄だけではない

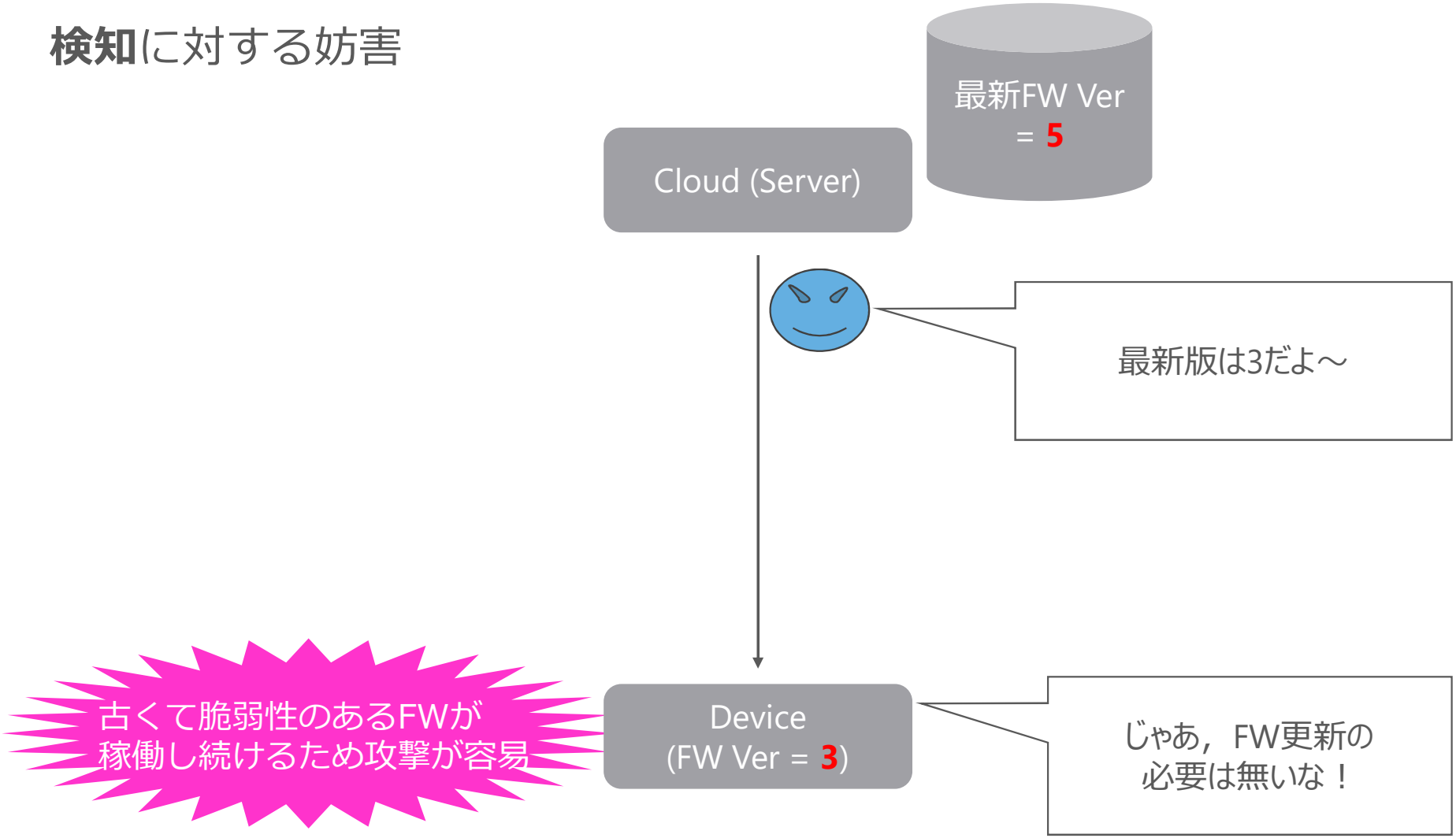


FW更新に関する脅威は改竄だけではない



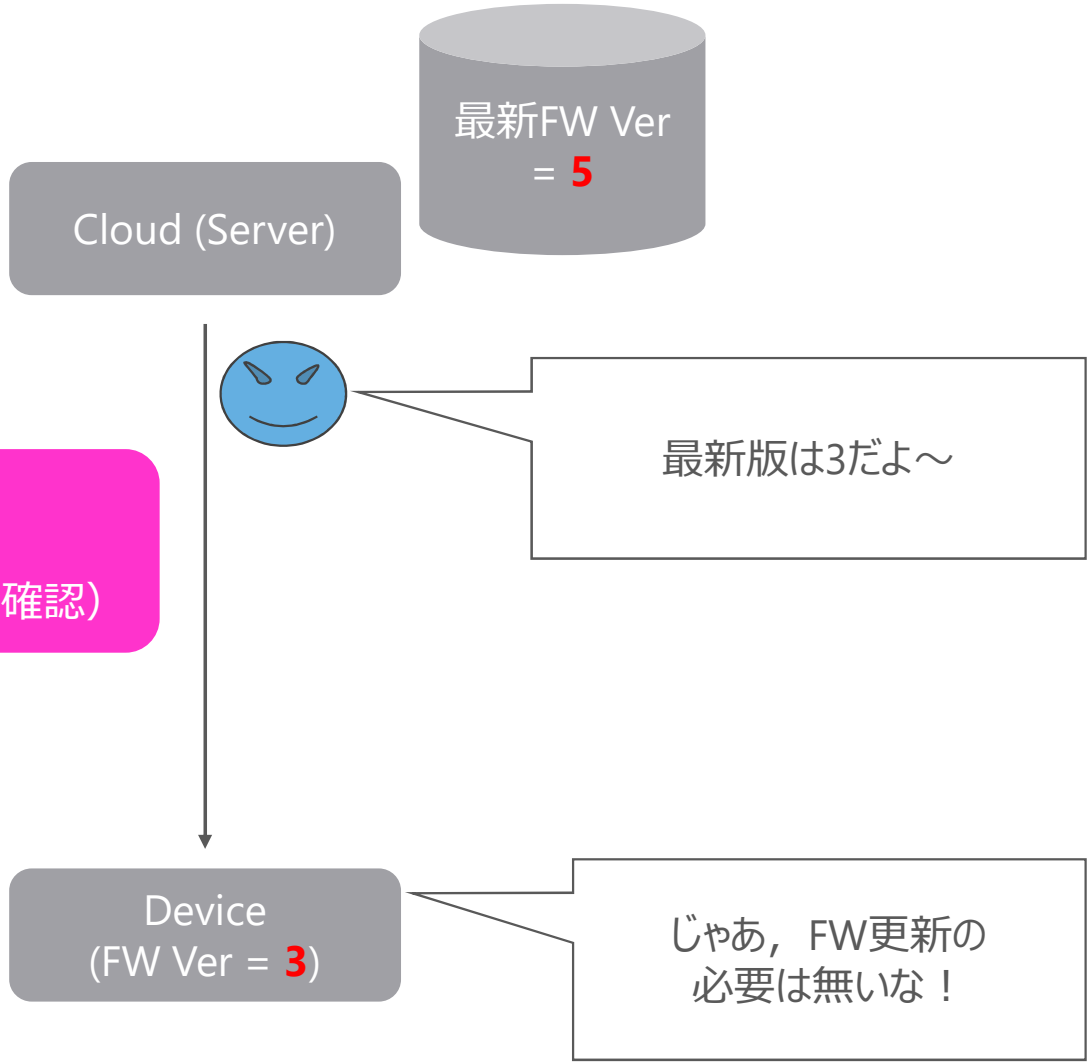
例1: FWバージョン固定攻撃（デバイスに嘘のバージョンを伝える）

検知に対する妨害



例1: FWバージョン固定攻撃（デバイスに嘘のバージョンを伝える）

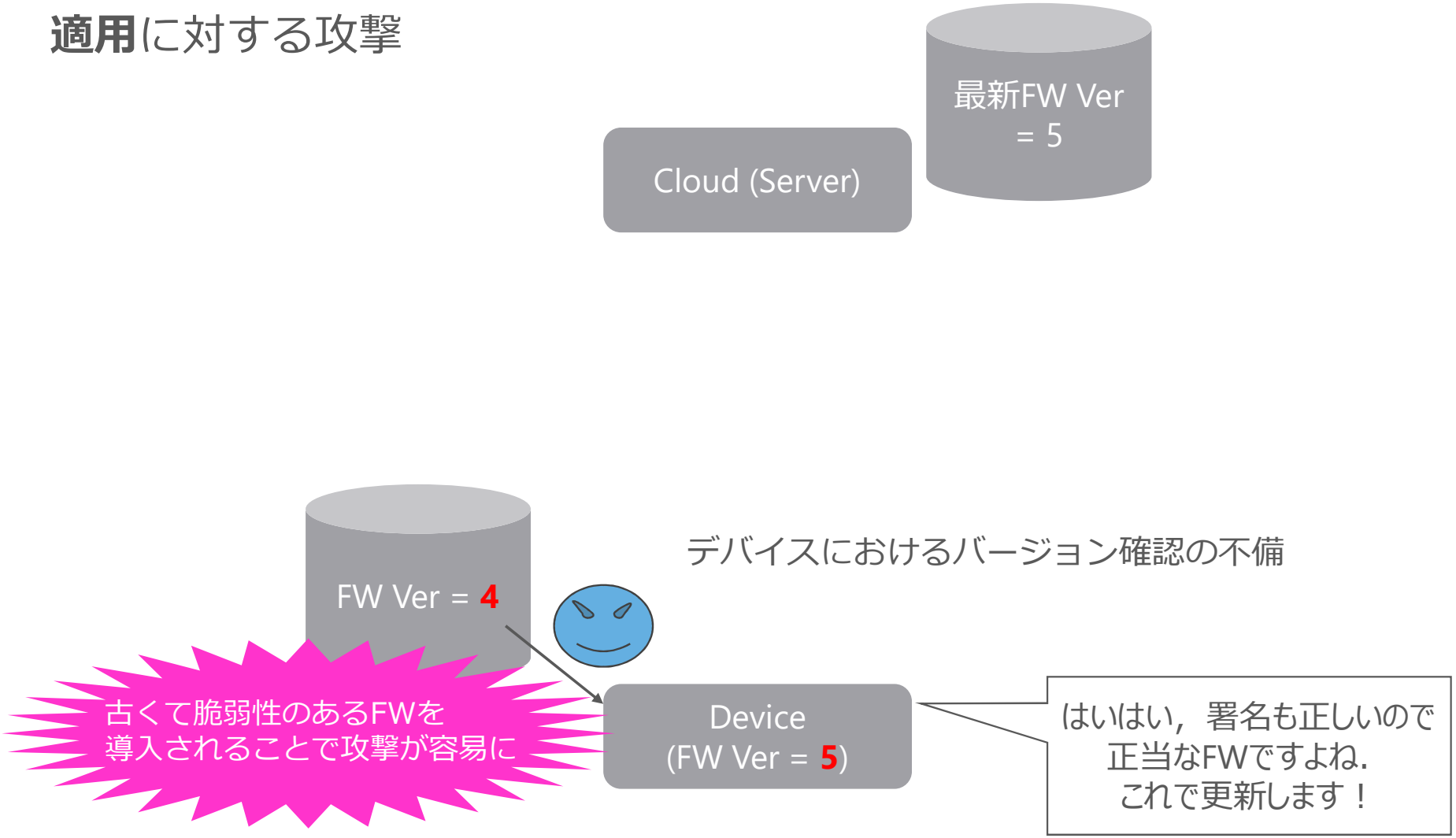
検知に対する妨害



対策
フレッシュネスの確認
（返答が古いものの使い回しでないことの確認）

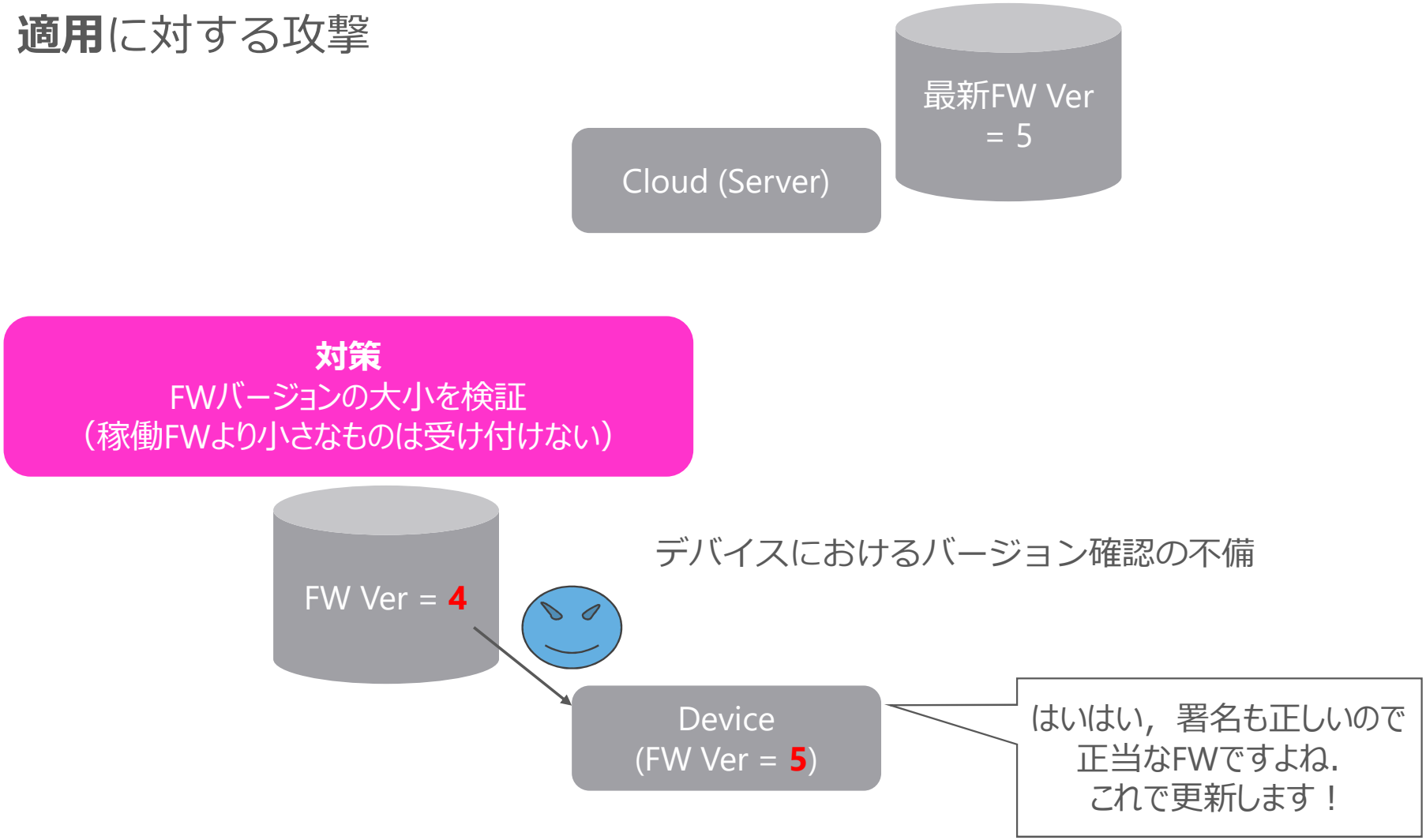
例2: ロールバック攻撃（デバイスに古いFWを導入させる）

適用に対する攻撃



例2: ロールバック攻撃（デバイスに古いFWを導入させる）

適用に対する攻撃



攻撃と対策との対応関係

	署名検証機能	バージョン 大小検証機能	フレッシュネス 強制機能	依存ファイルの 定義機能	サーバ分離構成	署名の複数化	帯域＆サイズ制御
改竄攻撃	○	×	×	×	×	○	×
ロールバック攻撃	×	○	×	×	×	×	×
早送り攻撃	○	×	×	×	×	○	×
バージョン固定攻撃	×	×	○	×	×	×	×
不正な依存関係の 提示攻撃	×	×	×	○	×	×	×
ユーザ保有鍵の漏洩	×	×	×	×	×	△（被害軽減）	×
サーバ保有鍵の漏洩	×	×	×	×	△（被害軽減）	×	×
無限ストリーム攻撃	×	×	×	×	×	×	○

OSSベンチマークの軸

- **実装品質**
  - すぐに使える稼働実績のあるコードが存在すること.
  - ソースコードや規格のコミュニティが活発であること.

将来にわたって実用レベルの実装が維持されて欲しい

- **オープン性＆認知度**
  - オープンな規格に準拠していること.
  - 産業界で認知・採用されていること.

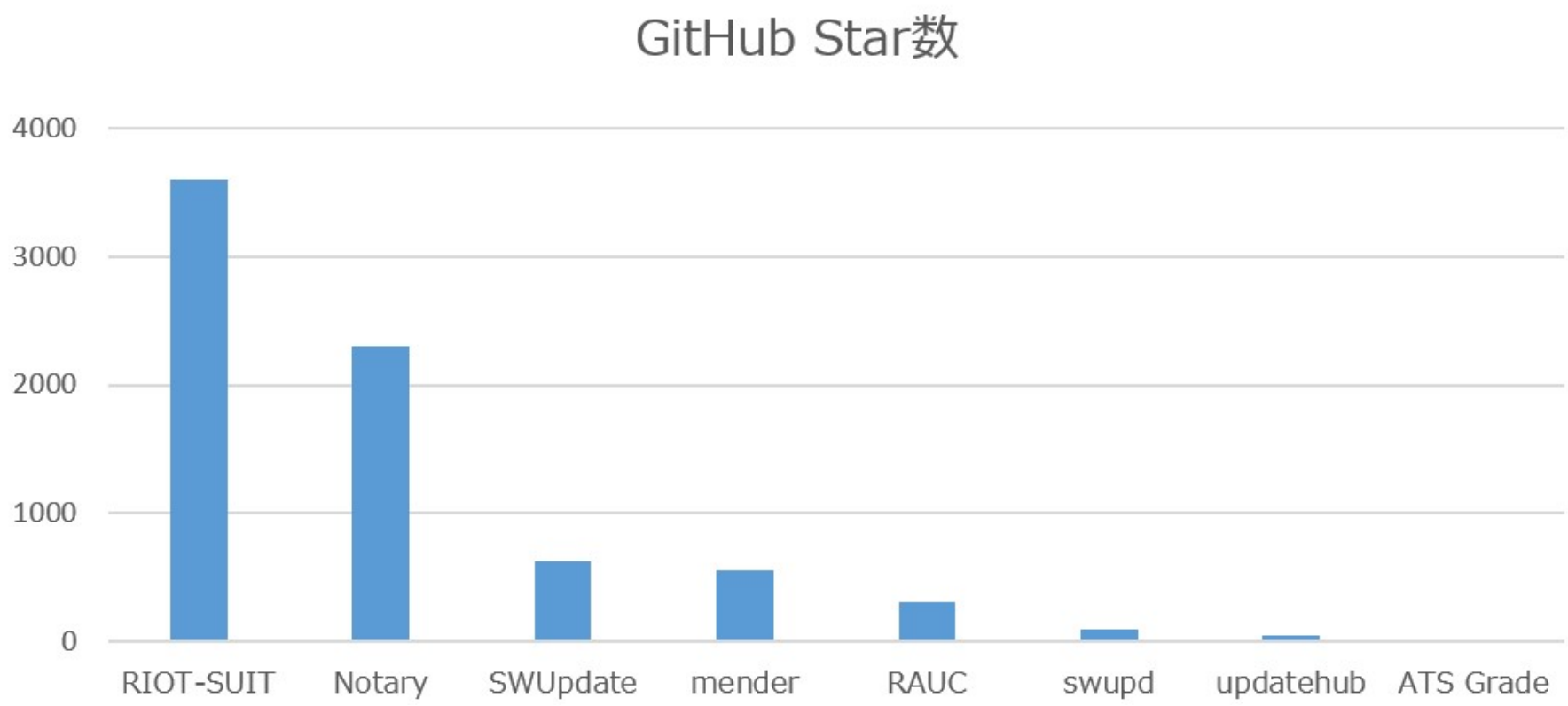
ベンダーロックインの排除＆ガラパゴスは避けたい

- **セキュリティ**
  - 前スライドの対策を可能な限り網羅的に持つこと.

高セキュリティ

コミュニティの活発さ（ベンチマーク対象の絞り込み）

- 実装の品質や継続性を加味するとコミュニティの活発度は重要指標.
- 定性的には500 Starを越えると開発がそれなりに継続しているとの感触あり.



ベンチマーク対象（1）

- **RIOT-SUIT（Software Updates for IoTの実装）**
  - Internet Engineering Task Force（IETF）で規格化が進んでいるSoftware Update for IoTと呼ばれるFW更新規格の実装.
  - 規格の実用化はまだ数年かかる見込み.
  - マニフェスト（記述法）が主な標準化対象で実現方法はスコープ外.
  - 組み込み向けOSであるRIOT上に試作機能（RIOT-SUIT）が存在する程度で実用的な実装はない.

ベンチマーク対象（2）

- **Notary (The Update Framework: TUF規格の実装)**
  - Cloud Native Computing Foundation（CNCF）の主要プロジェクト（卒業済み）.
  - 規格であるTUFと実装であるNotaryとの関係性.
  - Dockerにおけるセキュアなイメージ配布の仕組みContent Trustでも採用されており汎用性がある.
  - TUF規格自体は自動車向けのAutomotive Grade Linuxでも採用.

- **SWUpdate**
  - 組み込みLinux向けのFW更新ソフトとして実績がある.
  - 一方で動作環境は限定される（Yocto Linux）
  - 既存のFW管理コンソール（hawbit等）との接続が可能.

ベンチマーク結果（セキュリティ面）

	TUF （実装:Notary）	SUIT (実装SUIT-RIOT)	SWUpdate
改竄攻撃	○	○	○
ロールバック攻撃	○	○	○
早送り攻撃	○	○	○
バージョン固定攻撃	○	X (nonceで対応可？)	×
不正な依存関係の提示攻撃	○	×	×
ユーザ保有鍵の漏洩	△（仕様上は複数人署名による対策があるが，実装はまだ）	×	×
サーバ保有鍵の漏洩	△（サーバ分離構成で影響の緩和までは可能）	×	×
無限ストリーム攻撃	○	△（manifestにファイルサイズ併記で対応可能)	○

ベンチマーク結果（セキ

脅威に対する対策の網羅性からはTUF仕様の実装であるNotaryが好ましい．一部TUF規格に存在するものの機能が未実装という範囲があるが，それらに対して課題意識は持ってくれている．

	TUF（実装:Notary）	（実装SUN-RIOT）	e
改竄攻撃	○	○	○
ロールバック攻撃	○	○	○
早送り攻撃	○	○	○
バージョン固定攻撃	○	X (nonceで対応可？)	×
不正な依存関係の提示攻撃	○	×	×
ユーザ保有鍵の漏洩	△（仕様上は複数人署名による対策があるが，実装はまだ）	×	×
サーバ保有鍵の漏洩	△（サーバ分離構成で影響の緩和までは可能）	×	×
無限ストリーム攻撃	○	△（manifestにファイルサイズ併記で対応可能）	○

ベン

標準化が進みつつあるという点では，SUITの動向も要チェック．ただし，現時点での実装はRIOT上のモックレベルのものしか存在せず，すぐに使える状況にはない．即効性のある活用は難しい．

	（実装:Notary）	SUIT （実装SUIT-RIOT）	SWUpdate
改竄攻撃	○	○	○
ロールバック攻撃	○	○	○
早送り攻撃	○	○	○
バージョン固定攻撃	○	X (nonceで対応可？)	×
不正な依存関係の提示攻撃	○	×	×
ユーザ保有鍵の漏洩	△（仕様上は複数人署名による対策があるが，実装はまだ）	×	×
サーバ保有鍵の漏洩	△（サーバ分離構成で影響の緩和までは可能）	×	×
無限ストリーム攻撃	○	△（manifestにファイルサイズ併記で対応可能）	○

ベンチマーク結果

更新対象が組み込みLinux向けに固定されるのであれば，
稼働実績の豊富なSWUpdateを使うのはあり．ただし，
脅威対策の網羅性という観点ではTUF系に劣る．

	TUF （実装:Notary）	（実装SUIT-RIOT）	SWUpdate
改竄攻撃	○	○	○
ロールバック攻撃	○	○	○
早送り攻撃	○	○	○
バージョン固定攻撃	○	X (nonceで対応可？)	×
不正な依存関係の提示攻撃	○	×	×
ユーザ保有鍵の漏洩	△（仕様上は複数人署名による対策があるが，実装はまだ）	×	×
サーバ保有鍵の漏洩	△（サーバ分離構成で影響の緩和までは可能）	×	×
無限ストリーム攻撃	○	△（manifestにファイルサイズ併記で対応可能）	○

ベンチマーク結果（Notary）

	セキュリティ対策網羅性	汎用性(部品としての使い勝手)	実装品質＆開発継続性	既存クラウドコンソールOSSとの接続性	ライセンス
Notary	○	○	○	X	Apache 2.0
RIOT-SUIT	△	△	?	X	LGPL 2.1
SWUpdate	△	△	○	○	GPL 2.0

- **CPSの部品としての使い勝手が良い.**
- セキュリティ重視で汎用的なファイル配布に特化.
- TUF規格自体は自動車業界でも採用されており信頼感あり.
- ただし，クラウド側などの周辺を固めるOSSが見当たらない.

ベンチマーク結果（RIOT-SUIT）

	セキュリティ対策網羅性	汎用性(部品としての使い勝手)	実装品質＆開発継続性	既存クラウドコンソールOSSとの接続性	ライセンス
Notary	○	○	○	X	Apache 2.0
RIOT-SUIT	△	△	?	X	LGPL 2.1
SWUpdate	△	△	○	○	GPL 2.0

- **IETFという主要団体で規格化される毛並みの良さで将来性に期待.**
- ARM等の有力ベンダも規格化に協力.
- 一方，規格のFIXまで数年かかる模様で実装は試作レベル.
- すぐに使えるという段階では無いが，要継続ウォッチ.

ベンチマーク結果（SWUpdate）

	セキュリティ対策網羅性	汎用性(部品としての使い勝手)	実装品質＆開発継続性	既存クラウドコンソールOSSとの接続性	ライセンス
Notary	○	○	○	X	Apache 2.0
RIOT-SUIT	△	△	?	X	LGPL 2.1
SWUpdate	△	△	○	○	GPL 2.0

- **組み込みLinux向けに特化して良いのであれば有力な選択肢.**
- 使い勝手も現状でこなれている.
- ただし，環境が限定され汎用性は低い.
- Hawkbitなどのクラウド側の管理コンソールとの接続性も高い.

まとめ

- CPSな世界で必須と思われるFW更新についてとりあげた.
- FW更新という改竄チェックにばかり目が向くことが多いが，ロールバック攻撃，バージョン早送り攻撃など，改竄以外にも多様な脅威があることを紹介した.
- CPS向けのFW更新OSSとしてデファクトといえそうなものはまだ無い.
- ベンチマーク結果.
  - Notary: セキュリティ対策の網羅性あり．部品としての汎用性.
  - RIOT-SUIT: 規格としての毛並みの良さ．良い実装はまだ無い.
  - SWUpdate: 組み込みLinux向け．クラウドの管理コンソールと接続性.

END

商標について

- Linuxは，Linus Torvalds氏の商標です.
- その他本スライドに掲載の商品，機能等の名称は，それぞれ各社が商標として使用している場合があります.
- また本文および図表中では，「™」，「®」は明記しておりません.

