3. OTAテストベッドの概説

経済産業省
Ministry of Economy, Trade and Industry

国土交通省

本章の目的

- OTAテストベッドの基本的な構造を理解する
- OTAテストベッドで出来ること／出来ないことを理解する

アジェンダ

1. 概要
   OTAテストベッドとは，出来ること／出来ないこと
2. OTAテストベッドの全体構成
   全体構成図
3. メタデータについて
   構成と依存関係，ダウンロードと検証，フォーマット
4. OTAテストベッドのシーケンスについて
   OTAテストベッドのシーケンス説明
   - OTA Update
   - Arbitrary software attack(鍵流出無し)
   - Arbitrary software attack(鍵流出有り 片方)
   - Arbitrary software attack(鍵流出有り 両方)

アジェンダ

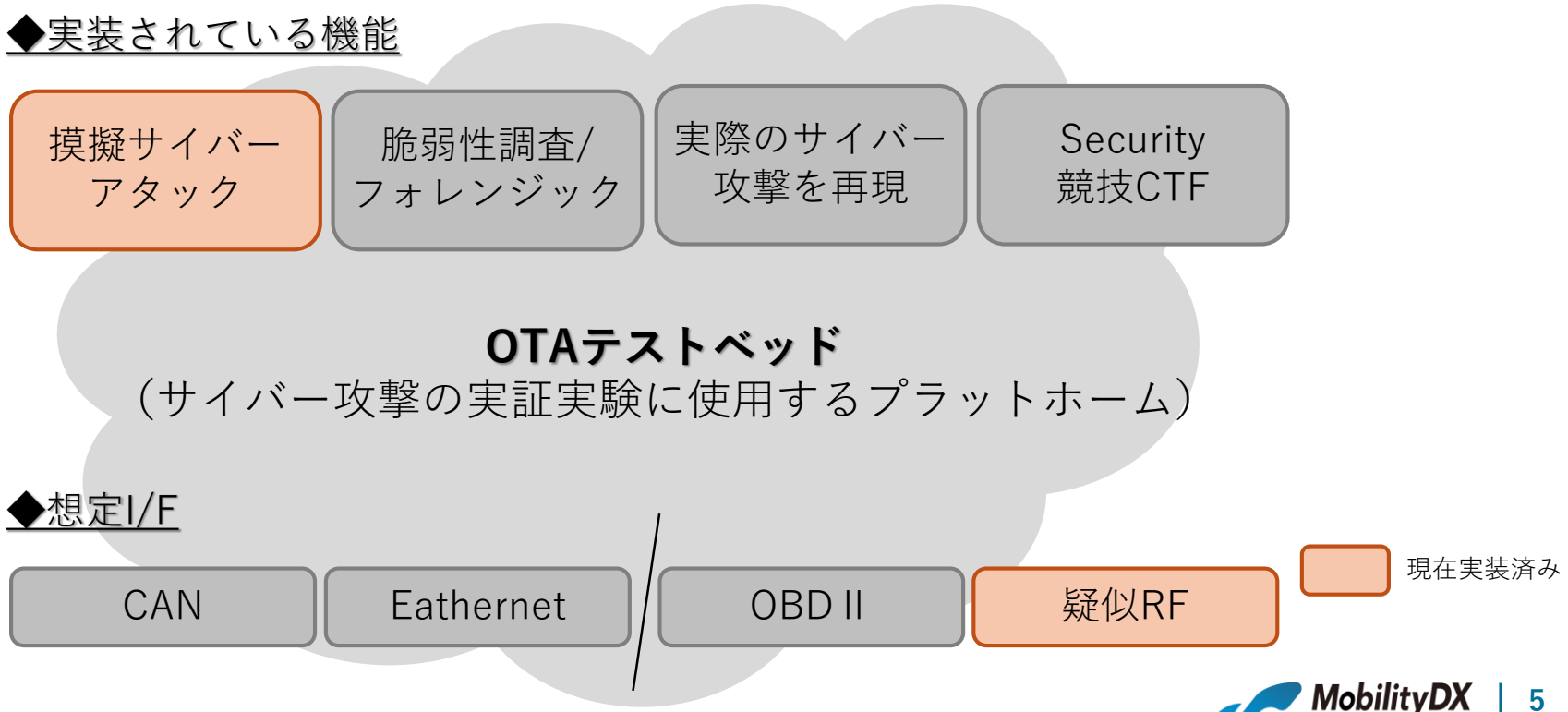
1. 概要
   OTAテストベッドとは，出来ること／出来ないこと
2. OTAテストベッドの全体構成
   全体構成図
3. メタデータについて
   構成と依存関係，ダウンロードと検証，フォーマット
4. OTAテストベッドのシーケンスについて
   OTAテストベッドのシーケンス説明
   - OTA Update
   - Arbitrary software attack(鍵流出無し)
   - Arbitrary software attack(鍵流出有り 片方)
   - Arbitrary software attack(鍵流出有り 両方)

概要

OTAテストベッドとは

Uptaneが『OTAを利用したECU Update』確認用に公開しているデモプログラム[*1]をベースに，本講座のサイバー攻撃の実証実験用として用意.

[*1] 公開先：https://github.com/uptane/obsolete-reference-implementation



概要

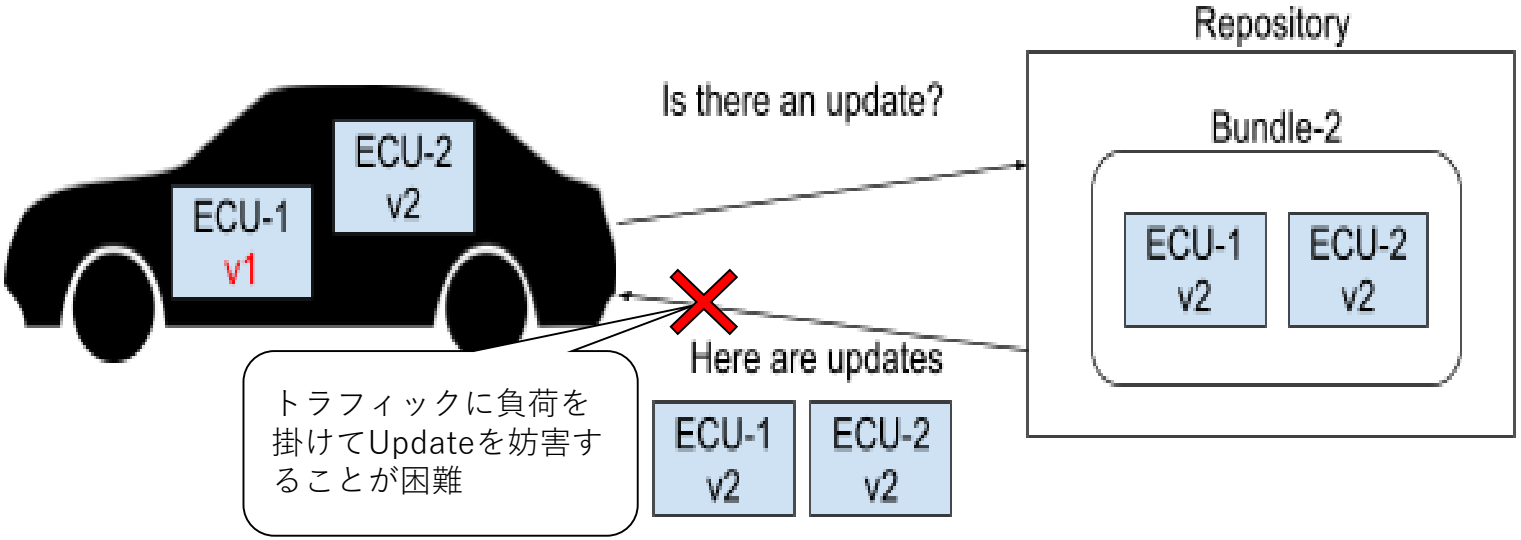
OTAテストベッドで出来ること／出来ないこと

OTAの脅威	対抗策	Uptaneの対象範囲	OTAﾃｽﾄﾍﾞｯﾄﾞ実装	演習1 演習で実施した攻撃	演習2 OTAの要求
Eavesdrop attack (更新内容の盗聴)	暗号化	×	―		
Drop-request attack (ドロップリクエスト攻撃)	再送	×	―		
Slow retrieval attack (遅延攻撃)	デッドライン監視	×	―		
Freeze attack (フリーズ攻撃)	バージョン監視	×	―		
Partial bundle installation attack(部分的なバンドルインストール攻撃)	レポート監視	○	×		
Rollback attack (ロールバック攻撃)	バージョンダウン禁止	○	○		
Endless data attack (エンドレスデータ攻撃)	デッドライン監視 2面持ち	×	―		
Mix-and-match attack (ミックスアンドマッチ攻撃)	デジタル署名	○	○		
Arbitrary software attack (任意のソフトウェアへの攻撃)	デジタル署名	○	○	(署名生成鍵の流出無し)	
				(１つの署名生成鍵が漏洩)	
				(複数の署名生成鍵が漏洩)	

概要

Partial bundle installation attackの実装について

OTAテストベッドはHTTPプロトコルを利用して，リポジトリ⇔自動車間の通信を行う．この攻撃は通信経路に対してトラフィック等に負荷を掛けて実行する事が一般的な手法だが，通信経路とデータを特定してそれを落とすことが難しいため，本研修のデモでは未実装.



Partial bundle installation attack

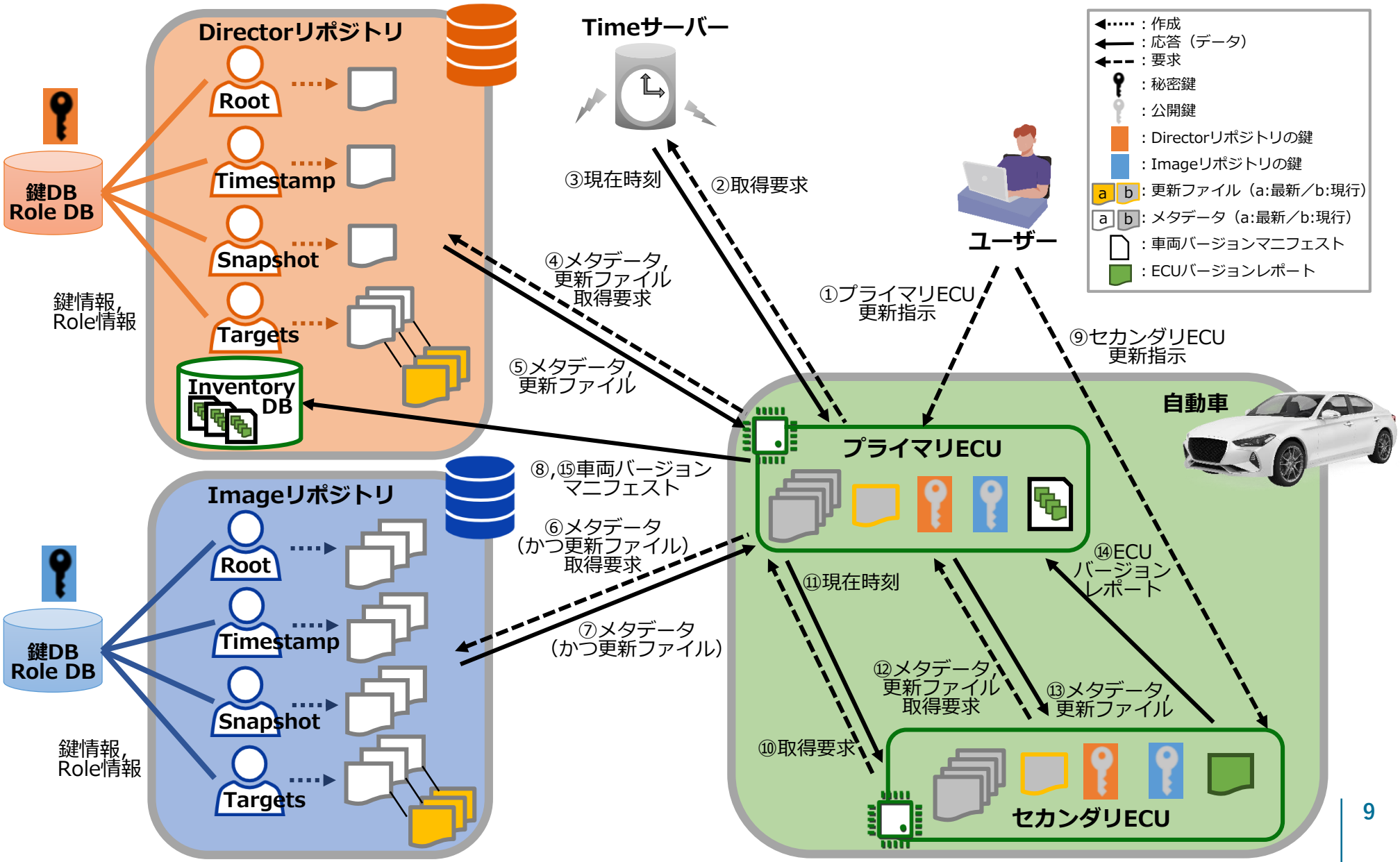
Uptane Design Overview (v2019.02.21)より図を引用

https://docs.google.com/document/d/1pBK--40BCg_ofww4GES0weYFB6tZRedAjUy6PJ4Rgzk/

アジェンダ

1. 概要
   OTAテストベッドとは，出来ること／出来ないこと
2. OTAテストベッドの全体構成
   全体構成図
3. メタデータについて
   構成と依存関係，ダウンロードと検証，フォーマット
4. OTAテストベッドのシーケンスについて
   OTAテストベッドのシーケンス説明
   - OTA Update
   - Arbitrary software attack(鍵流出無し)
   - Arbitrary software attack(鍵流出有り 片方)
   - Arbitrary software attack(鍵流出有り 両方)

OTAテストベッドの全体構成



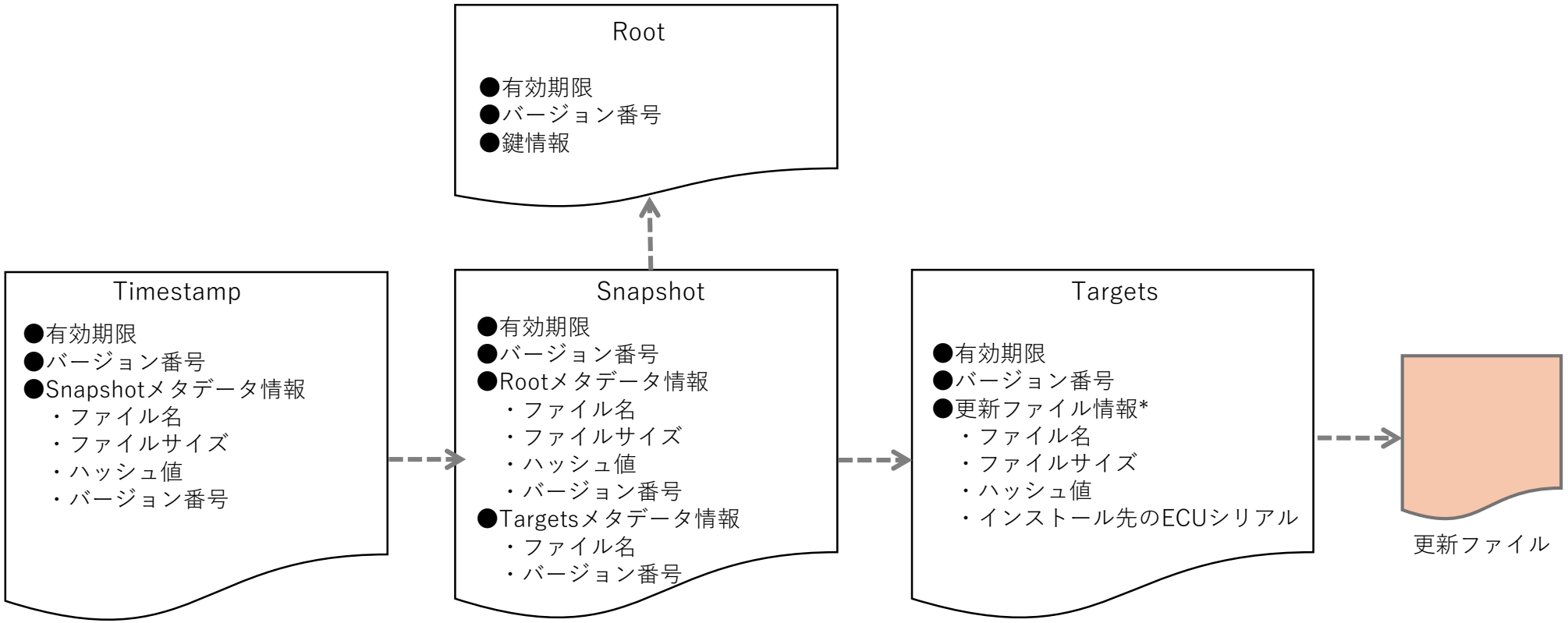
アジェンダ

1. 概要
   OTAテストベッドとは，出来ること／出来ないこと
2. OTAテストベッドの全体構成
   全体構成図
3. メタデータについて
   構成と依存関係，ダウンロードと検証，フォーマット
4. OTAテストベッドのシーケンスについて
   OTAテストベッドのシーケンス説明
   - OTA Update
   - Arbitrary software attack(鍵流出無し)
   - Arbitrary software attack(鍵流出有り 片方)
   - Arbitrary software attack(鍵流出有り 両方)

メタデータについて

メタデータの構成と依存関係

４つのメタデータと更新ファイルは依存関係にあり，整合性を保つ必要がある．



メタデータの依存関係

*更新ファイル情報を検証するタイミングは全てのメタデータ検証後、更新ファイルのダウンロード時に実施

メタデータについて

メタデータのダウンロードと検証

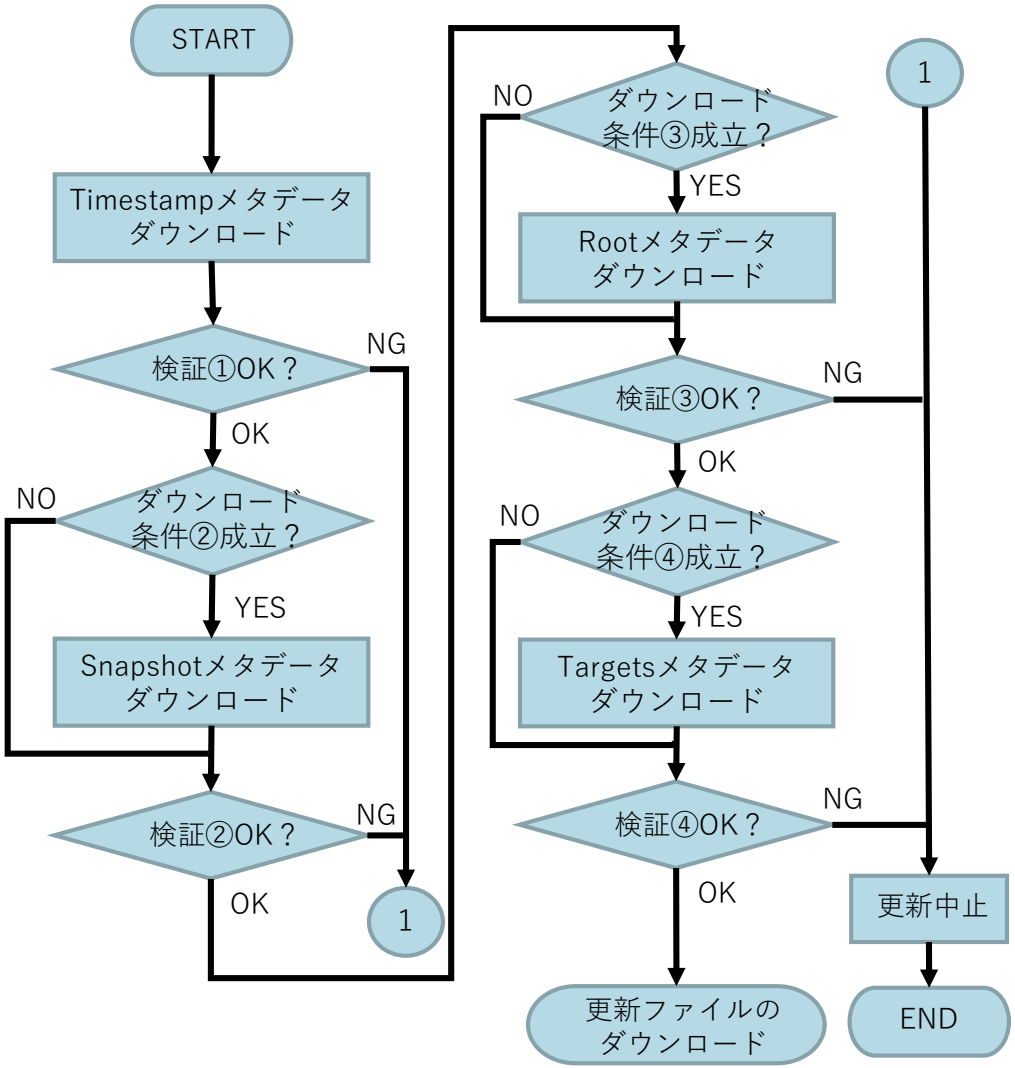
メタデータをダウンロードする際，次の手順を実施.

1. **ダウンロード条件確認**
   メタデータのダウンロードは前回更新時から変更が発生した場合のみ実施.
   - 条件成立：メタデータのダウンロード
   - 条件不成立：最新のメタデータを検証
2. **メタデータのダウンロード**
3. **メタデータの検証**
   ダウンロードしてきたメタデータに改ざんが無いか検証.
   - 検証OK：次のメタデータのダウンロード条件確認
   - 検証NG：更新を中止

これを４つのメタデータ分，繰り返す.

メタデータについて

- ４つメタデータのダウンロードと検証は左下のフローに沿って実施
- 各メタデータのダウンロード条件と検証内容は右表の通り



メタデータ	DL条件とメタデータの検証 ※メタデータの検証は検証内容が全てOKになること	
Time stamp	検証①	・バージョン番号が前回更新時より新しいこと ・メタデータの有効期限内であること ・メタデータが改ざんされていないこと
Snap shot	DL条件②	・Timestampメタデータ内のファイルサイズ，またはハッシュ値が前回更新時から変更していること
	検証②	・ファイルサイズとハッシュ値がTimestampメタデータ内の値と一致していること ・メタデータが有効期限内であること ・メタデータが改ざんされていないこと
Root	DL条件③	・Snapshotメタデータ内のファイルサイズ，またはハッシュ値が前回更新時から変更していること
	検証③	・ファイルサイズとハッシュ値がSnapshotメタデータ内の値と一致していること ・メタデータが有効期限内であること ・メタデータが改ざんされていないこと
Targets	DL条件④	・Snapshotメタデータ内のバージョン番号が前回更新時より新しいこと
	検証④	・バージョン番号がSnapshotメタデータ内の値と一致していること ・メタデータが有効期限内であること ・メタデータが改ざんされていないこと

メタデータについて

(補足)メタデータのフォーマット

OTAテストベッドのメタデータはpythonの辞書型というデータ型で登録．辞書型とは，keyとvalueの２つの値をペアで保持するデータ型．

{key:value，・・・}

(例)Timestampメタデータの赤枠内では，keyが’version’，valueが’1’となる．

```
'signed': {
            '_type': 'Timestamp',
            'version': 1,
            'expires': '2022-01-18T06:37:57Z',
            'meta': {'snapshot.der': {'length': 217, 'hashes': {'sha256': 'd760129727a630e53b948d66b798d58caa
                    813f828bbb5e5f98bbf4119b29e6b7'}, 'version': 1}}
},
'signatures': [{
            'keyid': 'da9c65c96c5c4072f6984f7aa81216d776aca6664d49cb4dfafbc7119320d9cc',
            'method': 'ed25519',
            'sig': 'fa48cf37e375ce44f2d922dd1066babb4cec97fa8cd4a9b205f184d3ad75ca8b964
                    5c3b01bb81a7e87f507bae2cb7196babb5fad3de1720092cd312853e0e806'
}]
```

keyが’version’，valueが’1’

timestampメタデータ

アジェンダ

1. 概要
   OTAテストベッドとは，出来ること／出来ないこと
2. OTAテストベッドの全体構成
   全体構成図
3. メタデータについて
   構成と依存関係，ダウンロードと検証，フォーマット
4. OTAテストベッドのシーケンスについて
   OTAテストベッドのシーケンス説明
   - OTA Update
   - Arbitrary software attack(鍵流出無し)
   - Arbitrary software attack(鍵流出有り 片方)
   - Arbitrary software attack(鍵流出有り 両方)

OTAテストベッドのシーケンスについて

メタデータが何を確認してUpdateの有効無効を判断しているか、シーケンス図を用いて説明する.

ファイル名：OTAテストベッド_シーケンス図_解説用.xlsx
シート名：「OTA Update」
「Arbitrary software attack (鍵流出無し)」
「Arbitrary software attack (鍵流出有り 片方)」
「Arbitrary software attack (鍵流出有り 両方)」