JC-STARと連携したECHONET Lite DA仕様のご紹介

一般社団法人　エコーネットコンソーシアム
技術委員長　村上　隆史

2026年3月5日

① ECHONET Liteの位置づけ

【前提】ECHONET Liteを用いたシステム構成について

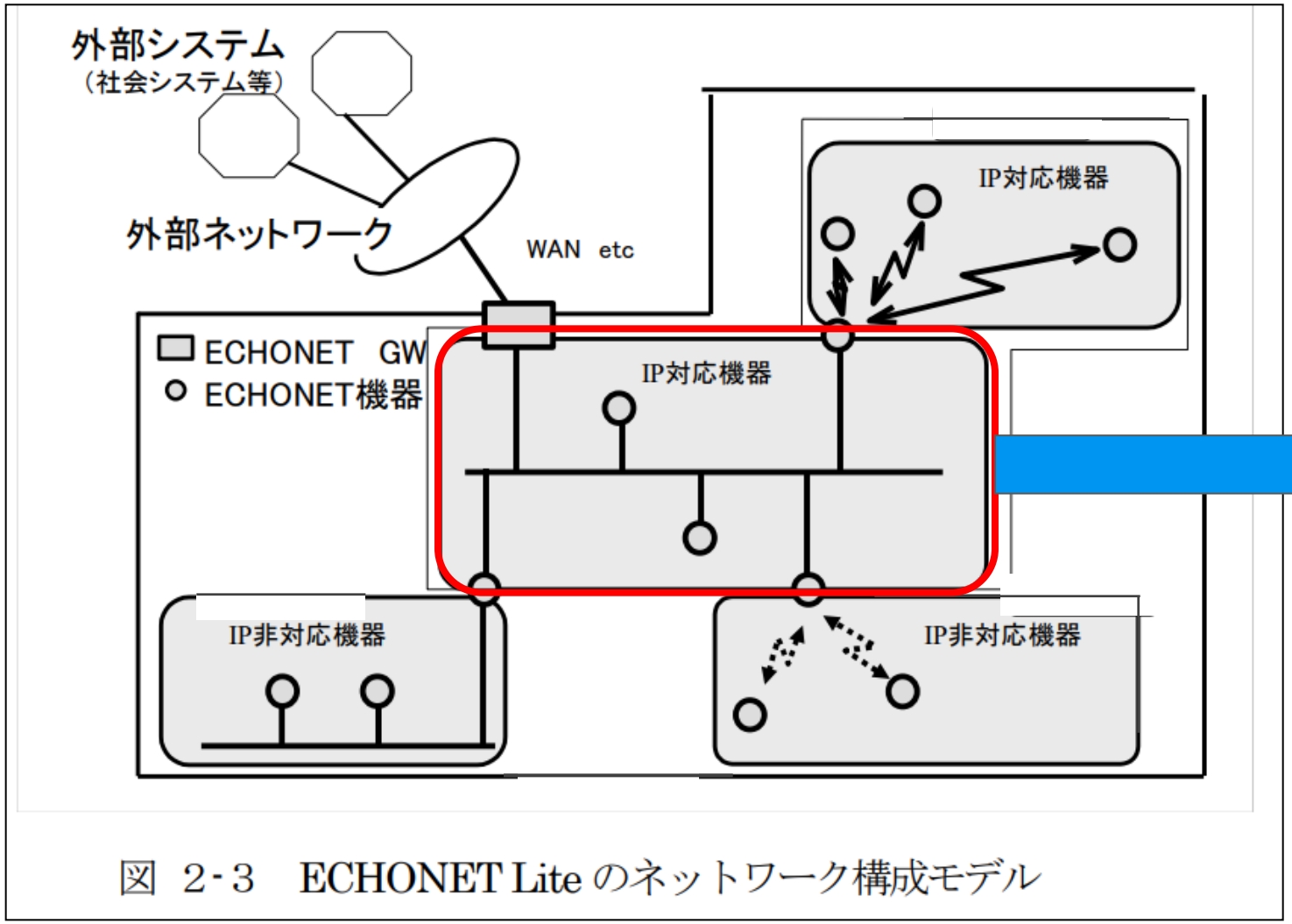


図 2-3 ECHONET Lite のネットワーク構成モデル

- ECHONET Lite対応機器はLAN内での通信機能を保持する
  - ECHONET LiteはLAN内の機器を前提に設計しており、ネットワーク境界防御は仕様外（想定外の機器がLANポートやWi-Fiなどのネットワークに侵入しないことを前提）
  - 無線は暗号・認証されている環境（例：WPA2以上）での利用を想定
- インターネットなどの外部ネットワークとの接続する機能である「ECHONET GW」をコントローラは搭載するケースが多い
  - 外部ネットワークと接続する機器にてセキュリティを担保する

- ECHONET Lite DA仕様を追加することで、
  - 対応機器は、暗号通信、メッセージ認証、送信元認証などによって、「改竄防止」「盗聴防止」「リプレイ攻撃防止」などに対応が可能
  - ペアリング機能によって、不当な機器の参入を抑制

様々な方によるECHONET LiteとJC-STAR★１等との関係に関する「発言」について

- 色々な方々のご意見を伺う中で、JC-STARとECHONET Liteとの関係について、様々な「ご発言」がされていると認識

- 事実
  - ECHONET Liteを搭載した機器について、適合要件を満たすことでJC-STAR★１を取得可能（実績あり）
  - セキュリティの観点において、証明書を用いた暗号通信（例：ECHONET Lite DA）は通常のECHONET Liteよりセキュリティ機能は高い

- 誤った意見
  - ECHONET Liteの認証を取得すればJC-STARの★1の取得が可能
    - ECHONET Liteだけでなく、「特定の通信仕様の認証取得を取ることでJC-STAR★１の取得が可能」、となることはない
  - ECHONET Lite搭載機器はJC-STARの★１の取得ができない
  - ECHONET Liteは★１を満たさない
    - JC-STARの対象は機器であって、プロトコルの評価をするものではない

【参考】JC-STARにおける「守るべき資産」について

- JC-STAR ★1における守るべき情報資産
  （参照：セキュリティ要件適合評価及びラベリング制度（JC-STAR）★1 レベル適合基準・評価手法）

【用語定義：守るべき情報資産】

以下のすべての情報：

- 通信機能に関する設定情報
- セキュリティ機能に関する設定情報
- IoT 機器の意図する使用において、IoT 機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報

- JC-STAR スマートホーム★2における守るべき資産（想定）
  （参照：スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン　添付G）

IoT 製品において守るべき資産	★1 で想定する守るべき資産	スマートホーム分野★2 で想定する守るべき資産
1. IoT 機能 機器やシステムが IoT につながるための機能	・ 有線通信機能 ・ 無線通信機能	・ 有線通信機能 ・ 無線通信機能
2. 本来機能 「モノ」本来の機能、セキュリティ対策・セーフティ対策のための機能	・ セキュリティ機能	・ セキュリティ機能 ・ 制御指示
3. 情報 ユーザの個人情報、収集情報、各機能の設定情報など	・ 通信機能に関する設定情報 ・ セキュリティ機能に関する設定情報 ・ 機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	・ 通信機能に関する設定情報 ・ セキュリティ機能に関する設定情報 ・ 機器が保存又は通信する、動作情報およびセンサ収集情報 ・ ユーザに関する設定情報 ・ 機器の初期ネットワーク設定情報 ・ 機器のファームウェア
4. その他の物理的資産 ユーザの健康・生命や IoT 機器が内蔵する物理的資産	－	－

— ECHONET Liteで扱う情報
→★２を対象にする場合、
ECHONET Lite DA仕様への対応が必要

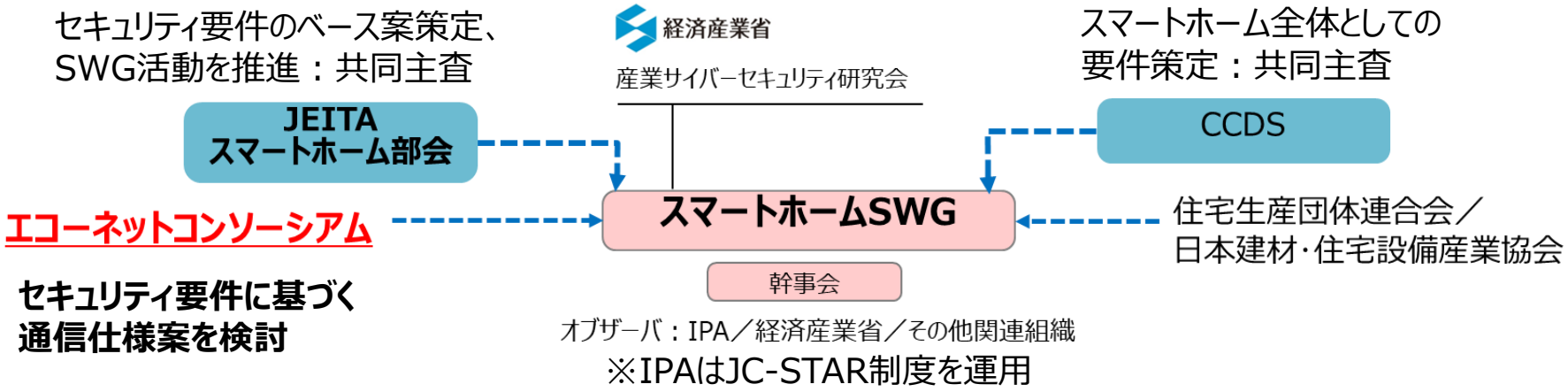
② ECHONET Lite DA仕様の導入について

JC-STAR制度　スマートホーム分野の制度検討状況

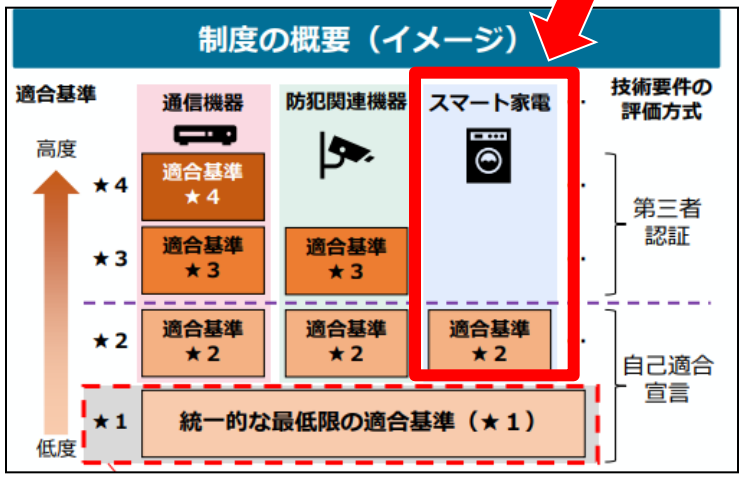
- JC-STAR制度 スマートホーム分野について、経産省　産業サイバーセキュリティ研究会傘下のスマートホームSWGに参画。昨年度、セキュリティ要件案（★2）まで検討完了。
- 今年度もスマートホームSWGに参画中。IPAでの適合基準検討について連携予定。

【JC-STAR制度】

インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的とした制度



検討範囲



エコーネットコンソーシアムはスマートホームSWG 幹事会に代表を派遣

JC-STAR スマートホーム分野★2セキュリティ要件案への対応

- スマートホーム分野★2 セキュリティ要件案（特に通信路保護）をふまえて、過去検討済の仕様をベースに、実運用を想定して改善した「ECHONET Lite Device Authentication(DA)仕様書」を策定中
- DA仕様の★2適合基準の達成可否確認について、スマートホームSWG等にご相談・確認実施

【スマートホーム分野★2 セキュリティ要件案（抜粋）】

特に「制御指示」、「機器が保存又は通信する、動作情報およびセンサ収集情報」に関わるセキュリティ要件案を以下に抜粋

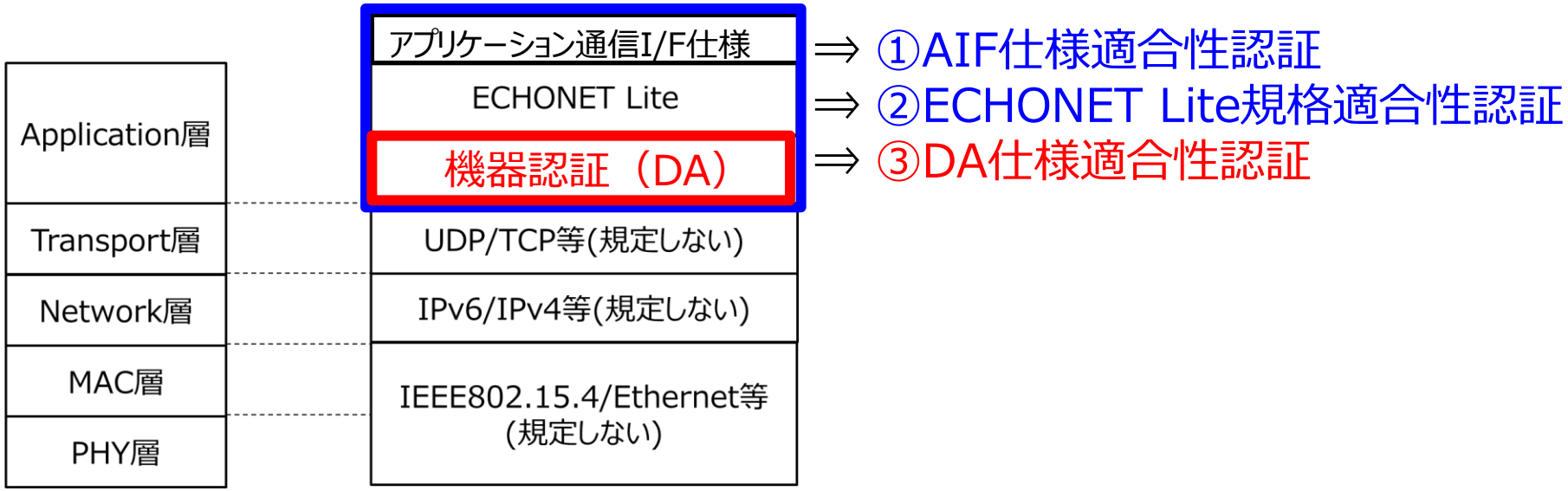
番号	分類	要件内容		適合基準	DA仕様での対応
1-5	技術要件	IoT機器	IoT機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。	IPA様にて検討開始（DA仕様が基準を満たすことをスマートホームSWGで確認）	ペアリング（期間制限、電子証明書を用いた相互認証）
5-1	技術要件	IoT機器	IoT機器は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。		暗号通信・メッセージ認証、送信元認証（AES-CCM、ECDSA）
8-2	技術要件	IoT機器	IoT機器と他のIoT機器や必須付随サービスとの間で通信されるIoTデータ(機器の動作情報やセンサ収集情報)の機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。		暗号通信（AES-CCM）

出典：https://home.jeita.or.jp/smarthome/pdf/security/guideline.pdf（付録3.セキュリティ要件の分類）

Device Authentication(DA)仕様の位置付け

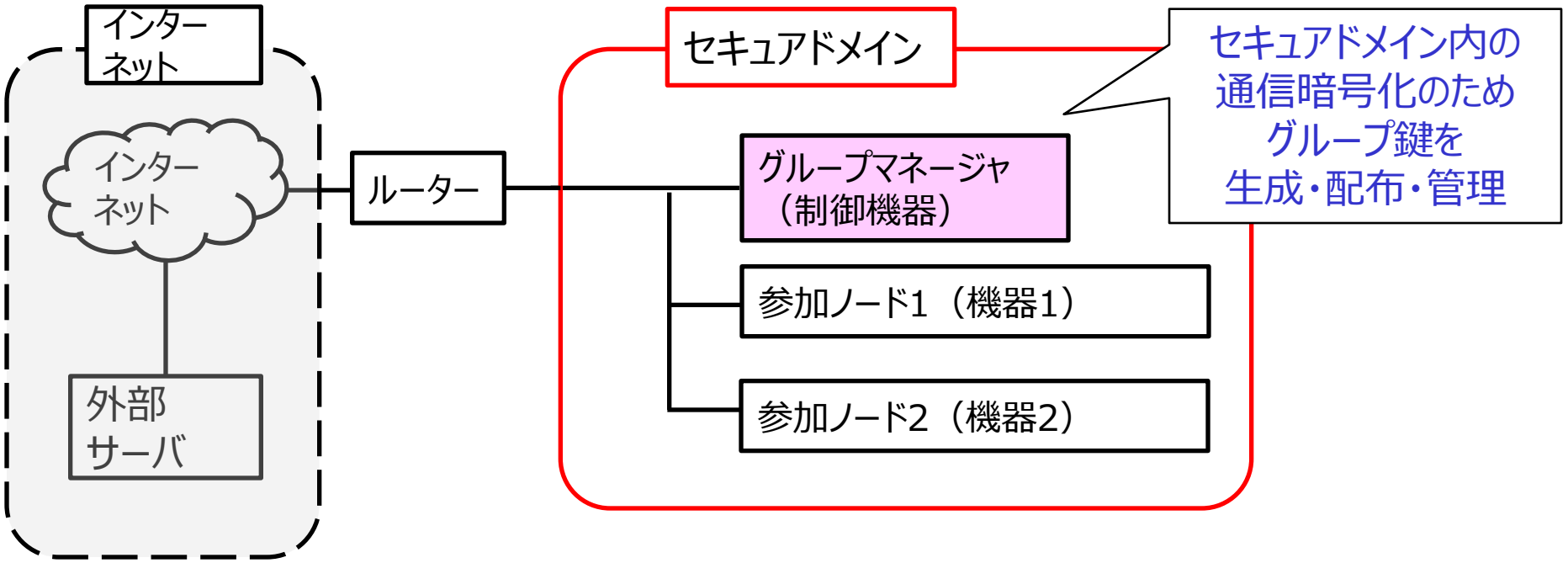
◆ 本仕様は、ECHONET Lite機器間において、機器がお互いを識別し、通信対象を適切に限定して安全に通信を行うための機能を提供

◆ 相互接続性が高いECHONET Liteプロトコルを使用できることを前提とした、**機器認証（Device Authentication：DA）機能**を備えた通信仕様をECHONET Lite Device Authentication仕様として規定



想定するシステム構成

◆ **グループマネージャ（GM）**によって鍵管理される1台以上の
参加ノードが同一セキュアドメイン上に存在



グループマネージャ（GM）の役割

・セキュアドメイン内に1台のみ存在し、各種グループとその所属メンバを管理
・新規メンバがユーザが意図した接続相手であることを確認（ペアリング）
・所属メンバにグループ鍵を配信・更新（グループ鍵管理）

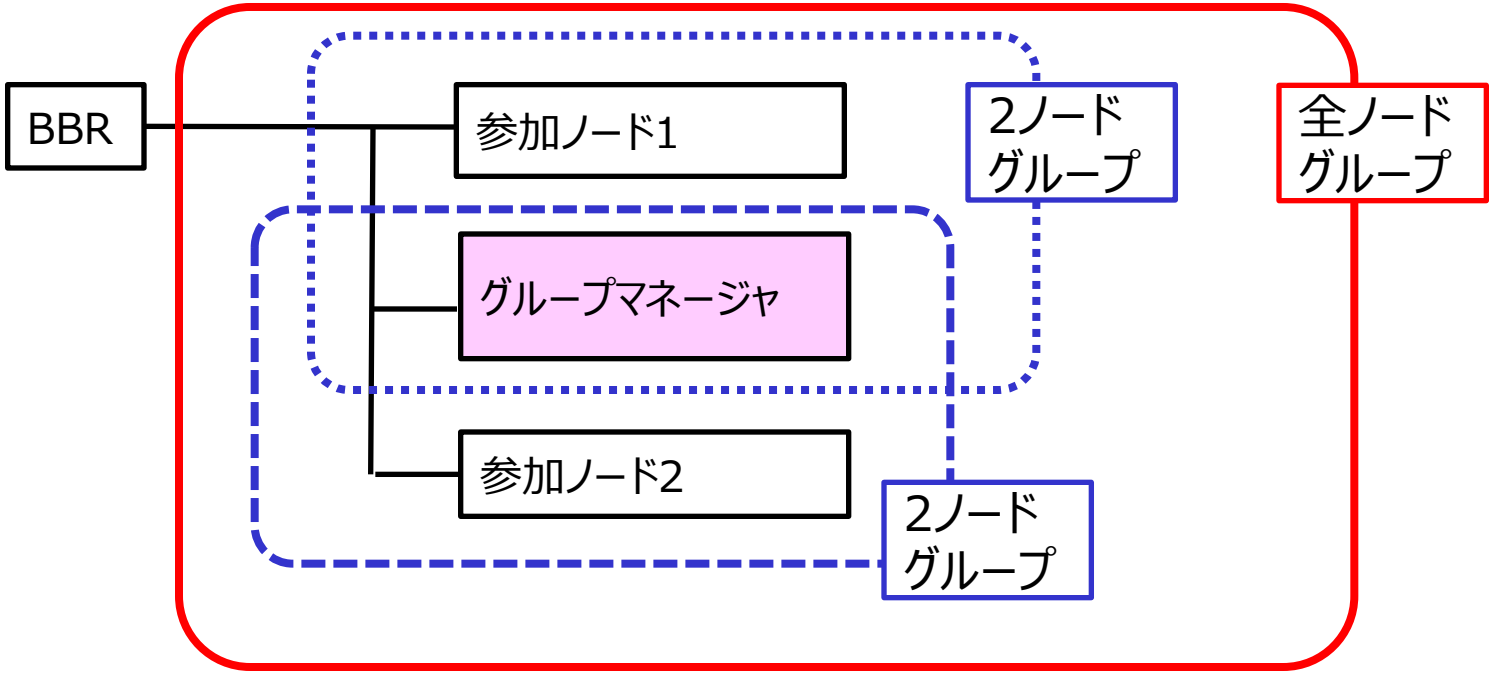
グループ構成

◆ **全ノードグループ：一斉同報などのマルチキャスト通信で使用**

グループマネージャ（制御機器）及び、グループマネージャとのペアリングに成功した全ての参加ノード（機器）の集合

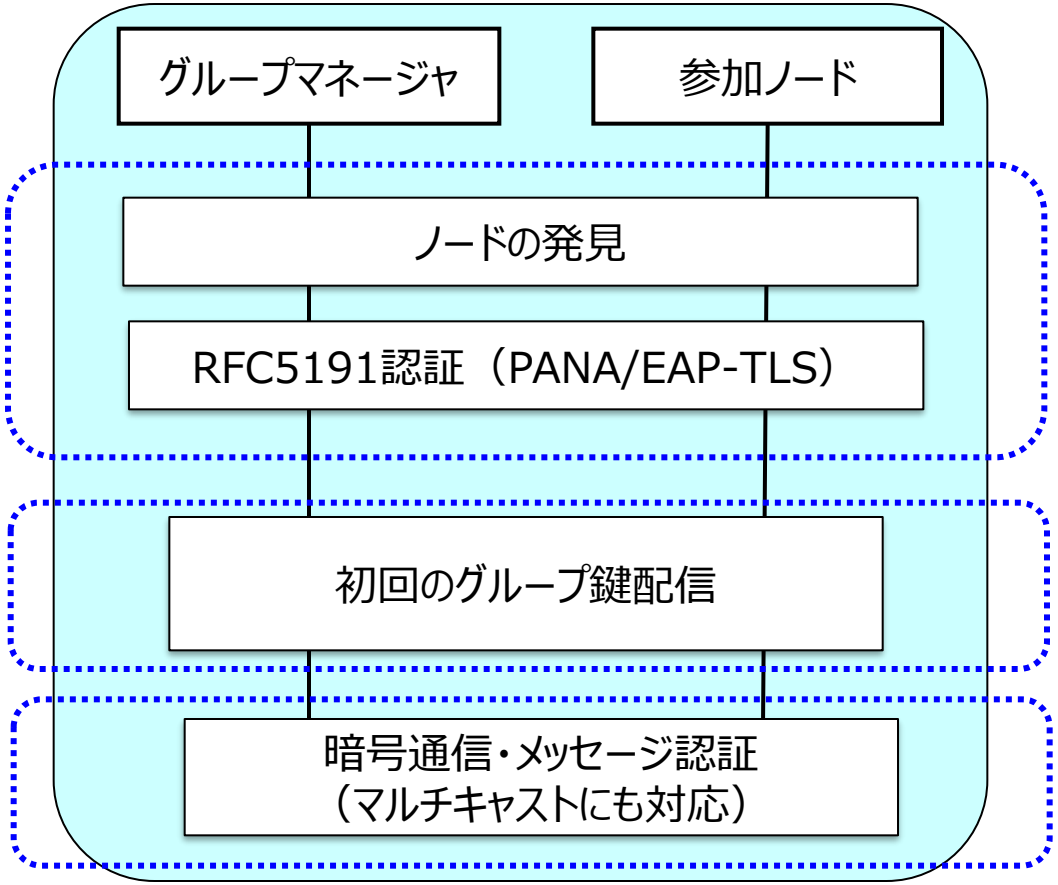
◆ **２ノードグループ：制御機器と機器とのユニキャスト通信で使用**

ペアリングに成功した参加ノードとグループマネージャからなる集合



機器認証の仕組み

「ペアリング」、「グループ鍵配信」、「暗号通信・メッセージ認証」の組合せにより
機器を識別し、ペアリング済の機器間のみに通信を制限



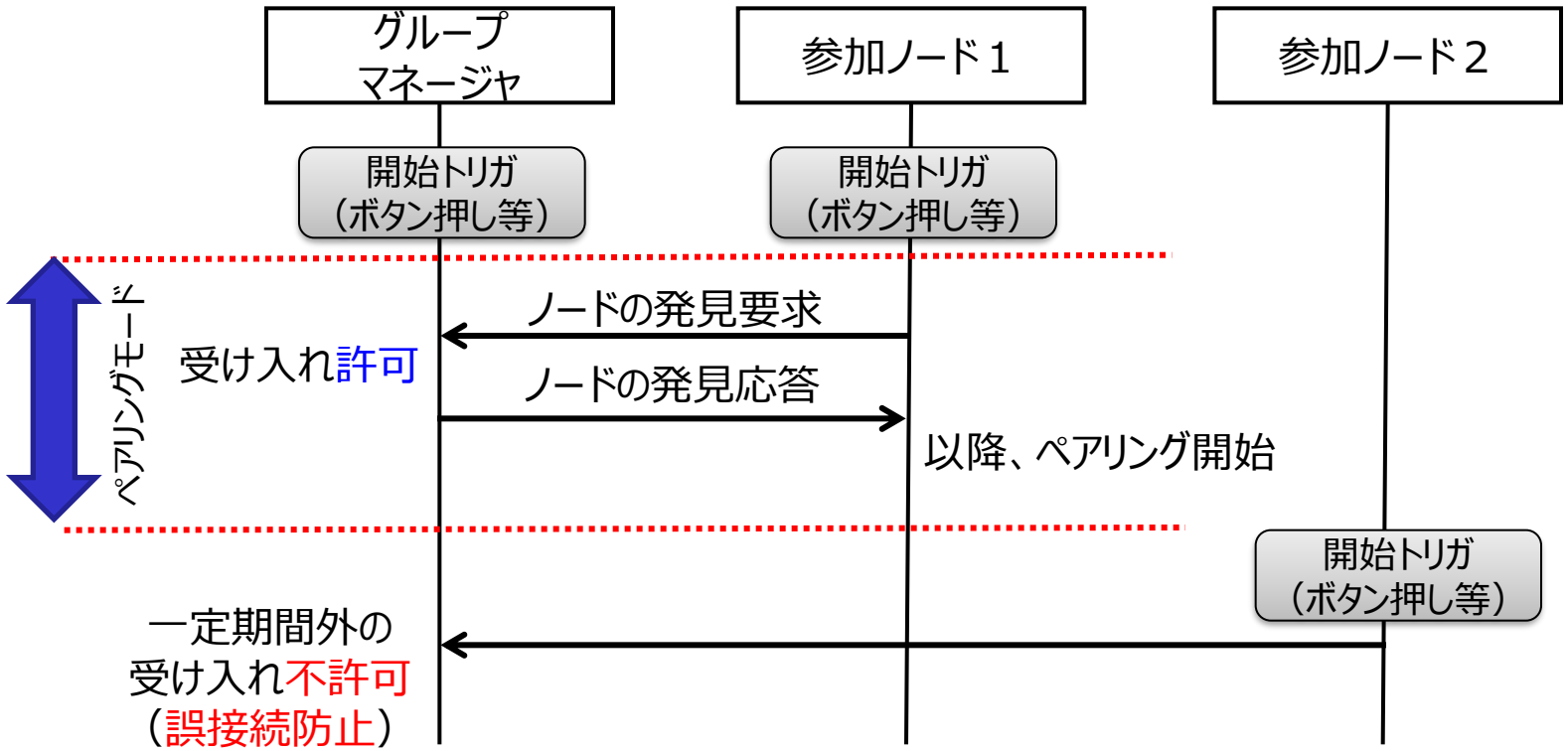
ペアリング：
ユーザが意図した通信相手とのみ接続（誤接続防止）
電子証明書による相互認証を実施

グループ鍵配信：
ペアリング済の証としてグループ鍵を配布

暗号通信・メッセージ認証：
ペアリング済の機器間のみに通信を制限するため、
グループ鍵を用いた暗号通信・メッセージ認証により
盗聴や改竄、なりすまし防止。

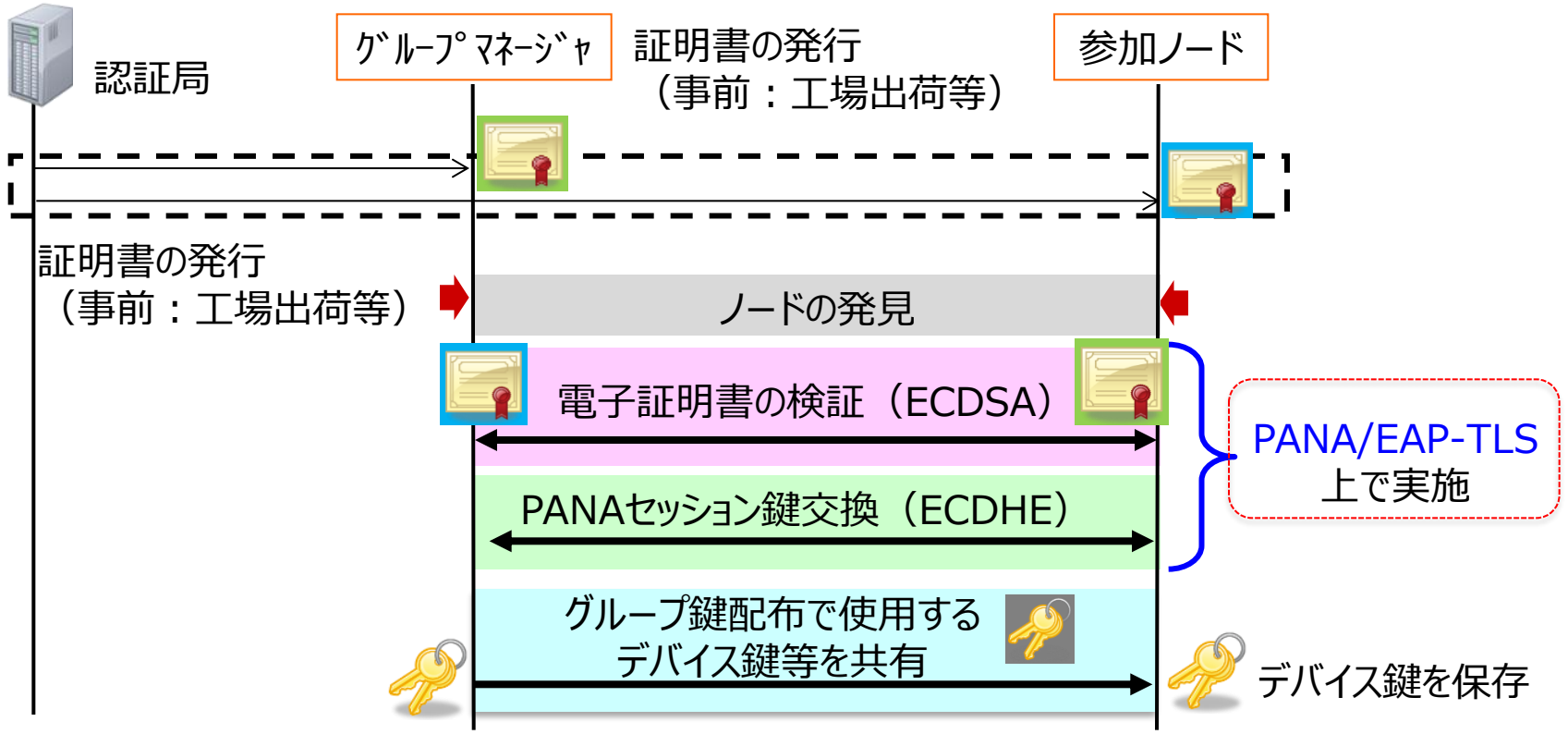
ペアリング：ノードの発見

ユーザ承認（ボタン押しなどのユーザからの開始トリガ）により
一定期間、ペアリングモードに移行する



ペアリング：RFC5191認証処理（PANA/EAP-TLS）

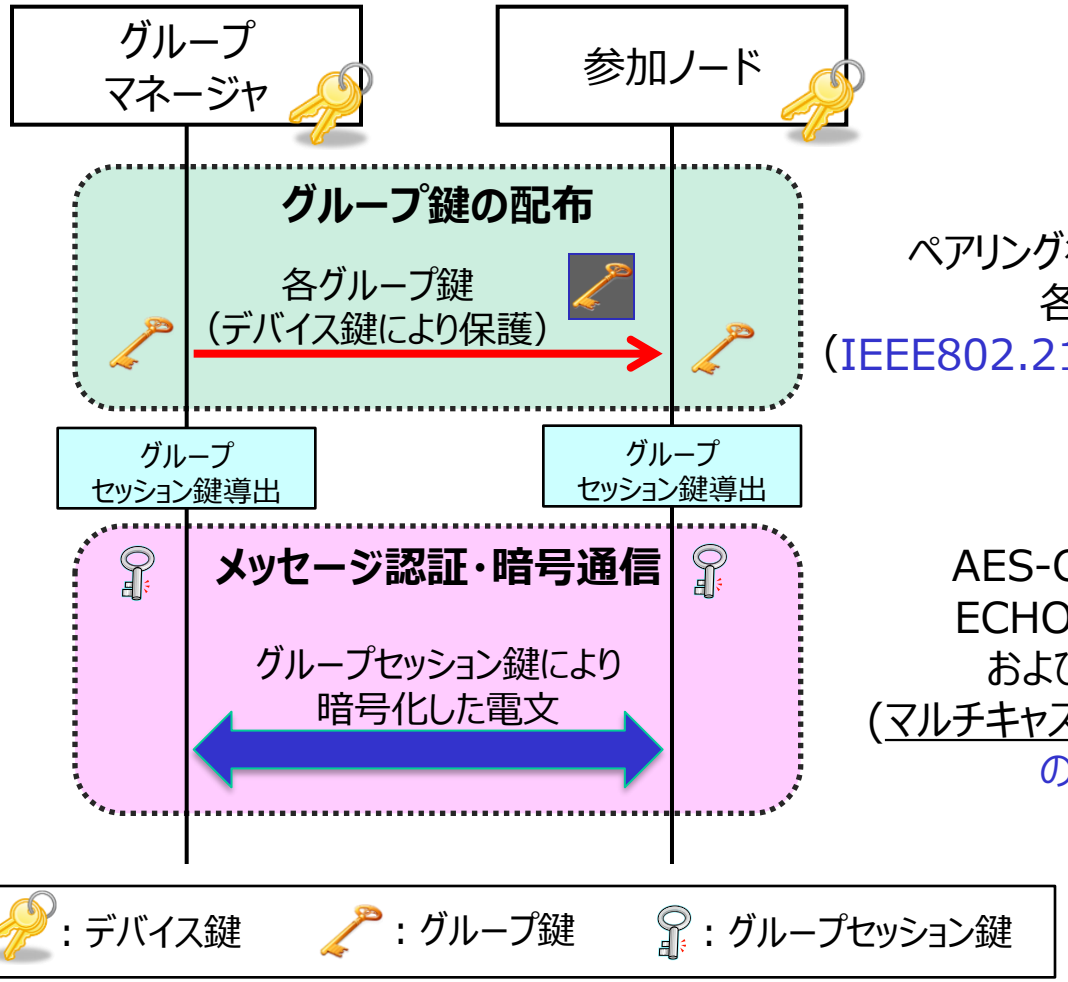
標準化されたプロトコルを使用し、電子証明書を用いた相互認証実施（PANA/EAP-TLS）



EAP-TLS：サーバ/クライアント双方の電子証明書を交換して認証を行うプロトコル。
PANA　　：UDP/IP上でEAPメッセージを効率的・安全に交換するためのプロトコル。Bルートで実績あり。

グループ鍵配信と暗号通信・メッセージ認証

・グループマネージャがペアリング済みの参加ノードに各グループ鍵を配布
・グループセッション鍵を用いて、ECHONET Liteフレームを暗号化して送受信

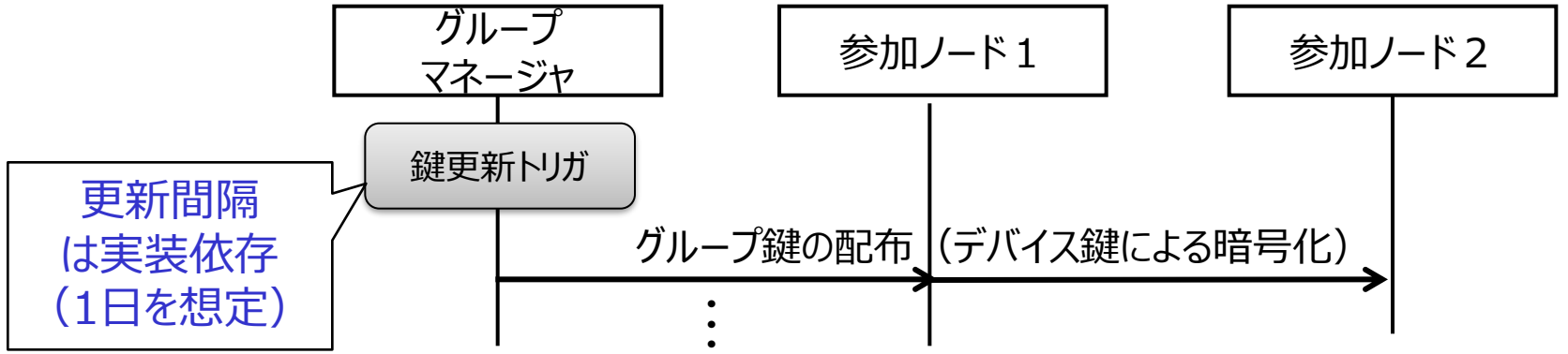


ペアリング後にグループマネージャから
各グループ鍵を配布
（IEEE802.21-2017の鍵配布機能を利用）

AES-CCM（鍵長128ビット）による
ECHONET Liteのフレームの暗号化
およびECDSAによる送信元認証
(マルチキャストに対応したIEEE802.21-2017
のフレームフォーマットを利用)

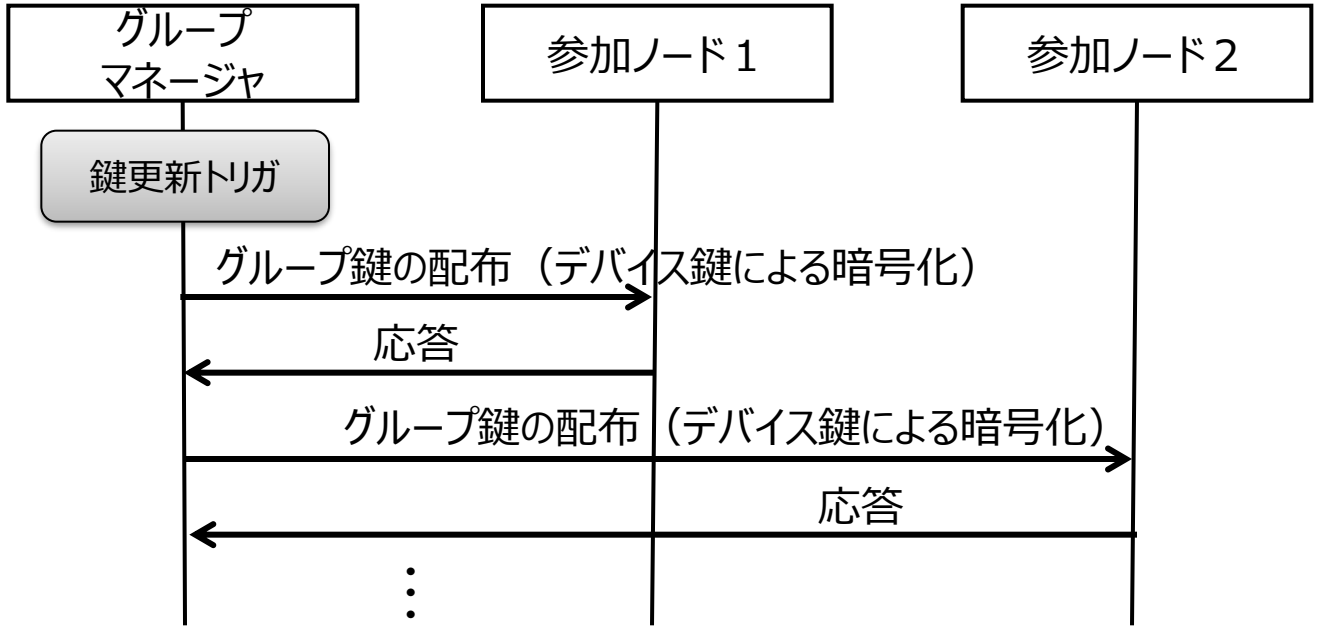
グループ鍵の更新

■マルチキャストによる鍵更新



※鍵を取りこぼした場合、機器側から再取得する仕組み有

■ユニキャストによる鍵更新

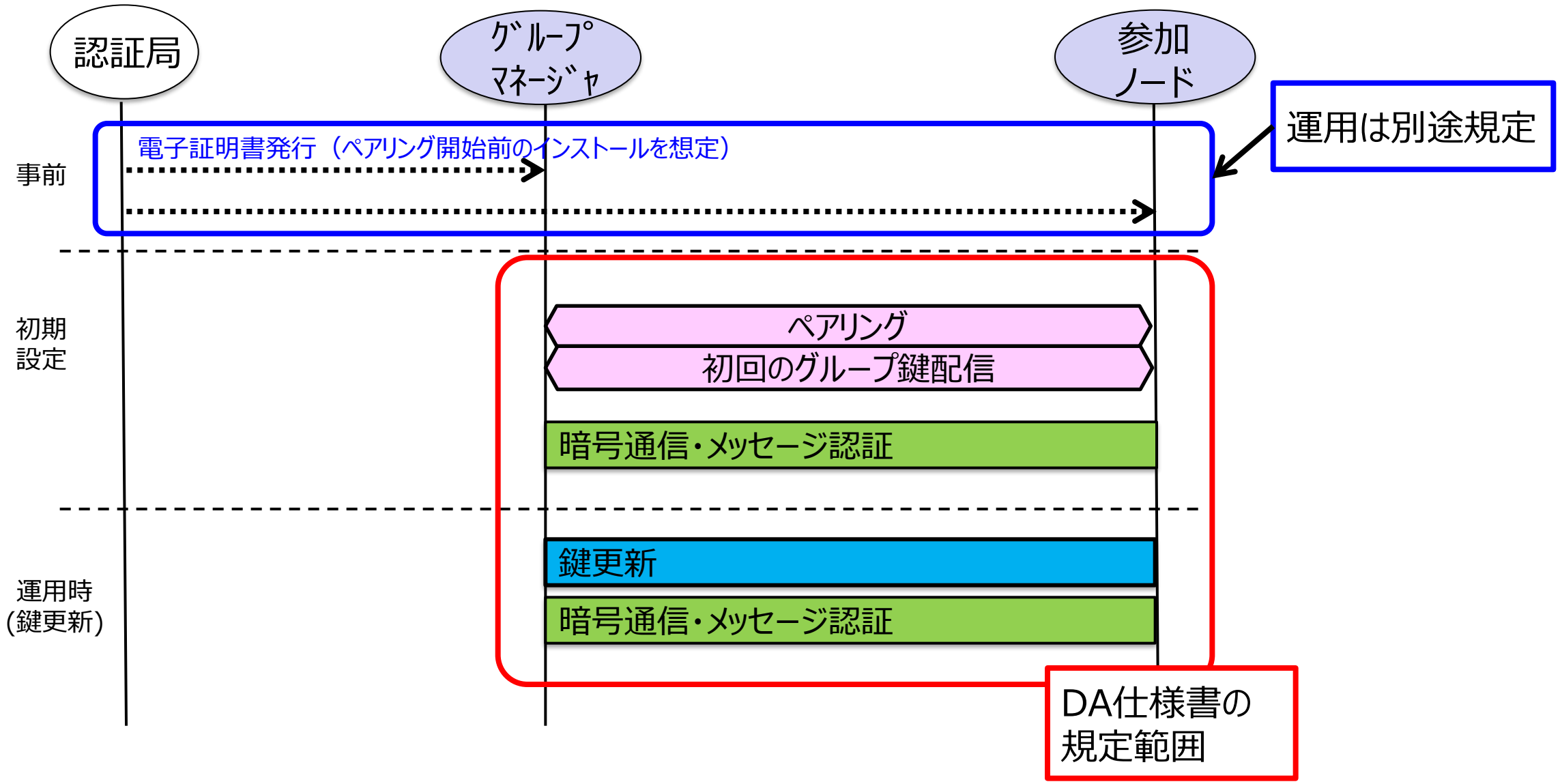


機器認証（DA）仕様の構成

グローバルでの活用も視野に入れ、仕様に標準規格を採用
→IEEEとMOUを締結し、仕様策定にあたり情報共有を実施

項目		仕様
システム構成		セキュアドメイン内にグループマネージャ1台と 参加ノード1台以上で構成
ペアリング （相互認証）	認証手段	電子証明書（X.509 Ver.3形式）を使用
	通信 ﾌﾟﾛﾄｺﾙ	PANA/EAP-TLS
	ｱﾙｺﾞﾘｽﾞﾑ	ECDSA，ECDHE（secp256r1） （楕円曲線暗号による署名検証、鍵交換）
鍵配信・ 更新	鍵管理 （ｸﾞﾙｰﾌﾟ管理）	ECHONET Lite向けプロファイルを策定
	鍵配布 ﾌﾟﾛﾄｺﾙ	IEEE802.21-2017
暗号通信	フレーム フォーマット	IEEE802.21-2017で規定された フレームフォーマット（AES-CCM）を使用 （マルチキャスト通信に対応）
	暗号化	
	ﾒｯｾｰｼﾞ認証	

運用を含むECHONET Lite DA仕様の全体像



ドキュメント類における現在の状況

■ ECHONET Lite DA仕様書／DA仕様適合性試験仕様書
- 「ECHONET Lite DA仕様書　Ver.1.00 Ready版」および「DA仕様適合性 認証試験仕様書 第1版　Ready版」をエコーネットコンソーシアム会員に対して公開実施（1月22日）。

■ 試験ツール
- DA仕様適合性 認証試験仕様書対応の試験ツール開発着手
- DA仕様搭載時におけるECHONET LiteおよびAIF仕様に関する試験ツールに関する検討着手
- 会員とのプラグフェストのようなイベントも要検討

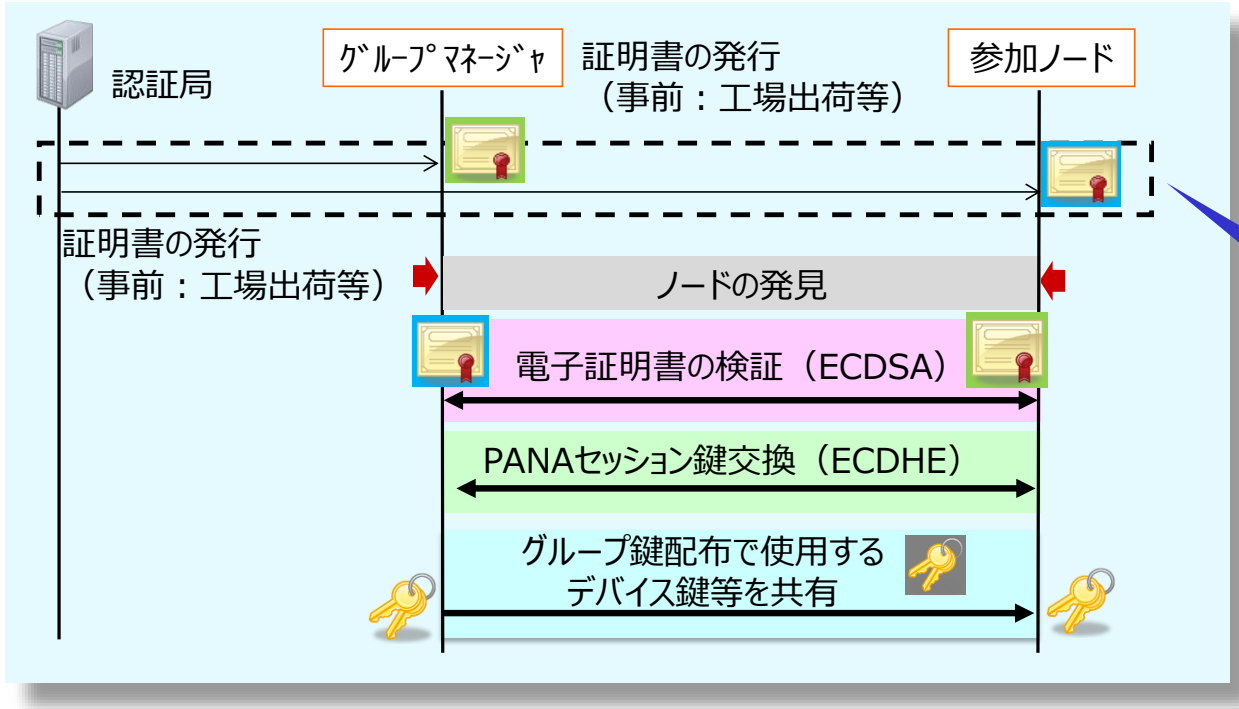
■ 認証制度
- WG設立し、認証局の在り方、DA仕様適合性試験の方法などについて議論着手
- ロゴの検討を通じ、DA仕様搭載／非搭載を分かりやすい施策を検討

■ 想定スケジュール
- 2026年秋に認証開始を目途に上記の取組を実施中

IPA様によるJC-STAR制度のスマートホーム★2の検討スケジュールと足並みをそろえて、仕様書・ツール類などの公開、規格適合性認証制度の運用を開始予定

③: ECHONET Lite DA仕様における制度設計

認証局について



DA仕様の動作のためには、
“認証局”から“証明書”を取得し、
証明書に対応する秘密鍵を
セキュアに保存・使用すること

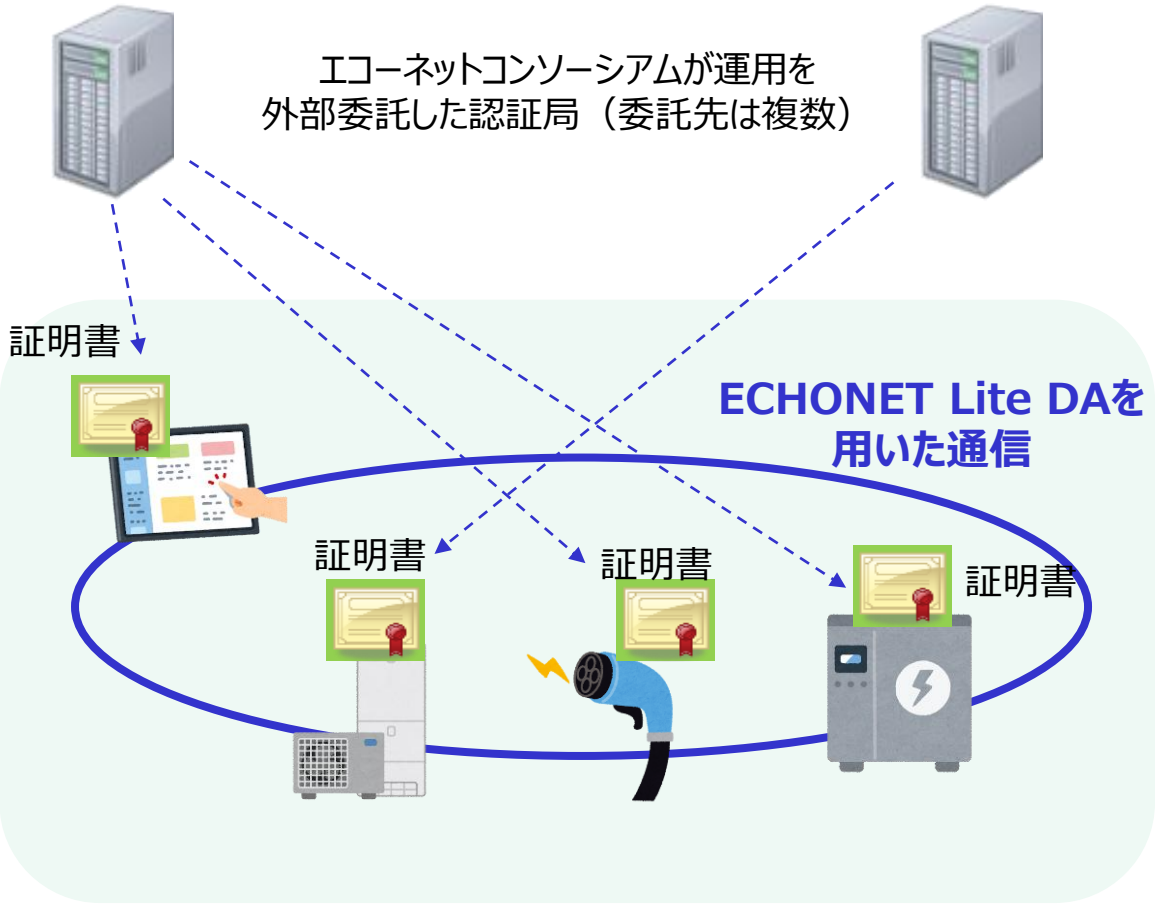
セキュリティの十分な確保のため、
認証局や証明書は一定の要件を満たすことが必要

エコーネットコンソーシアムでは、
認証局を指定すること、または、認証局や証明書に求める要件を定める予定です

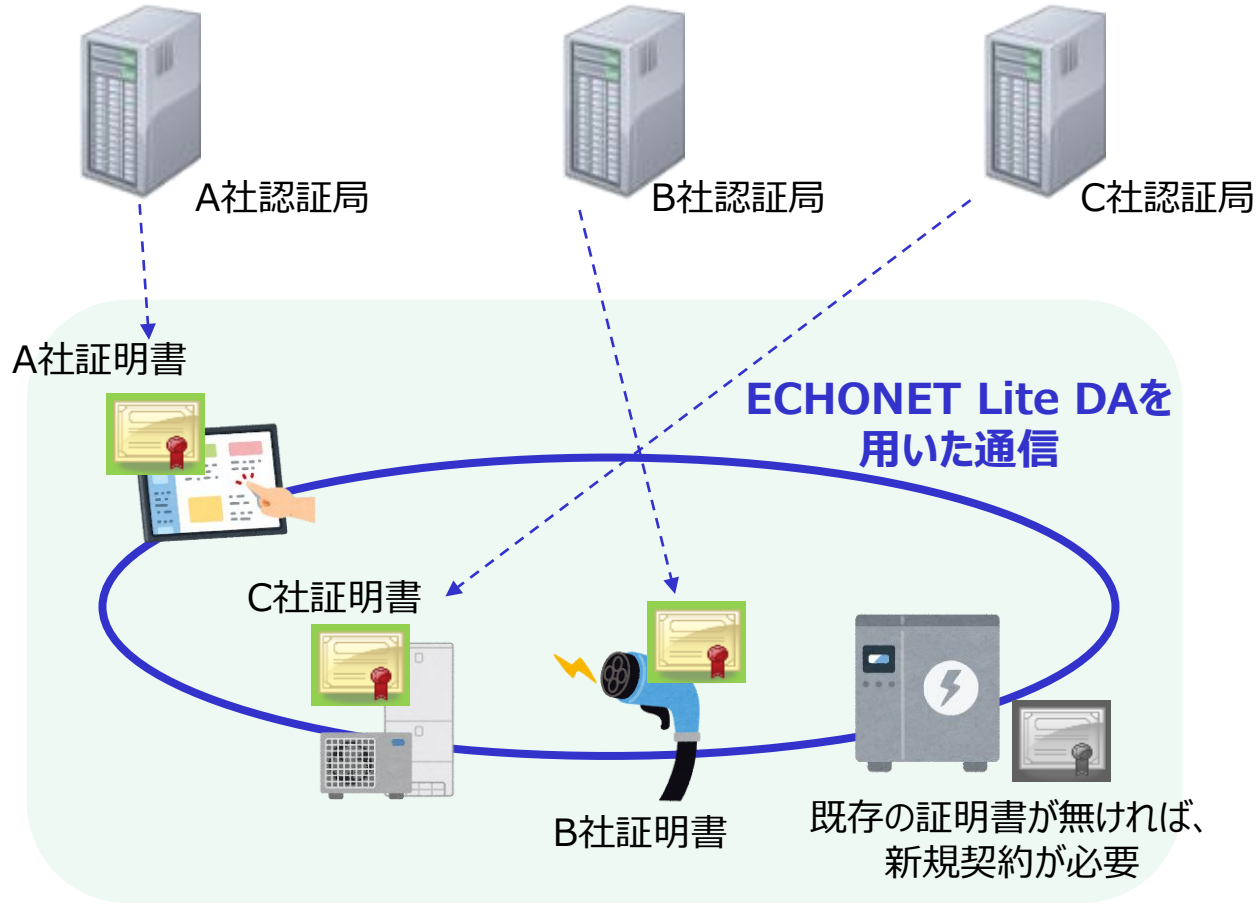
認証局について

認証局の信頼性や会員間の公平性、コストコンシャスの観点を鑑みながら２案を検討中

エコーネットコンソーシアムが運用を外部委託する認証局が発行する証明書を取得・使用



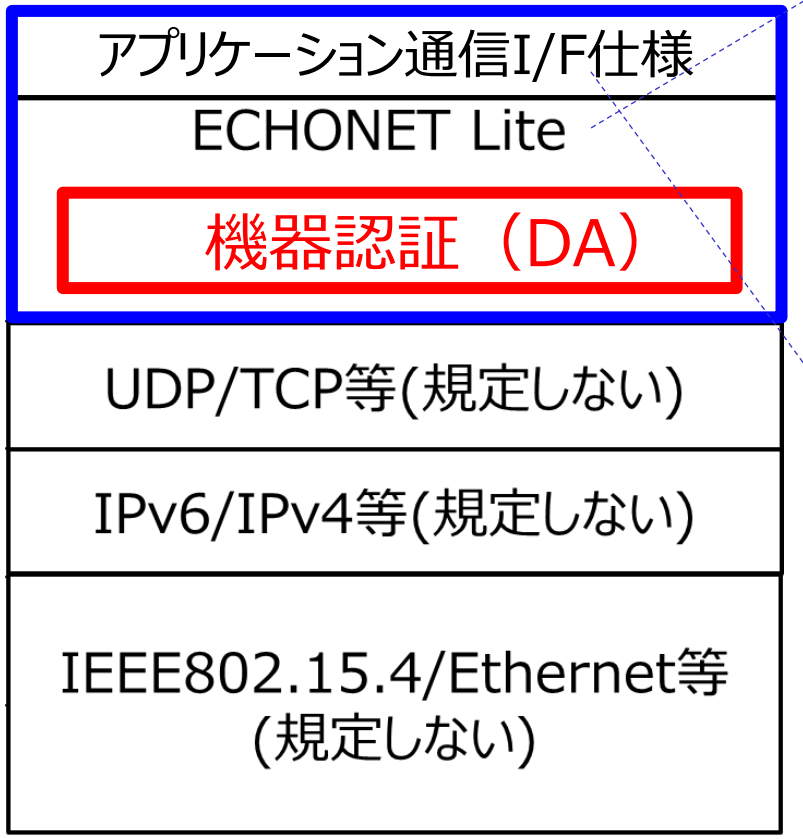
エコーネットコンソーシアムが認定した認証局から取得した証明書を使用



DA仕様に関する規格適合性試験・認証について

DA仕様に対応したECHONET Lite通信等の規格適合性認証を計画中

以下は検討中の一案であり、決定ではありません



ECHONET Lite規格適合性認証

DA非搭載

従来の試験仕様書に従い試験・認証を行うことで
“ECHONET Lite”の認証を取得できる

DA搭載

DA試験仕様書の内容を試験・認証した上で、
DA仕様が動作した状態で従来の試験仕様書に従い試験・認証を行うことで
“ECHONET Lite Secure”の認証を取得できる

注：DA仕様が停止した状態で試験・認証を行った場合は、ECHONET Liteの認証を付与

AIF仕様適合性認証

DA非搭載

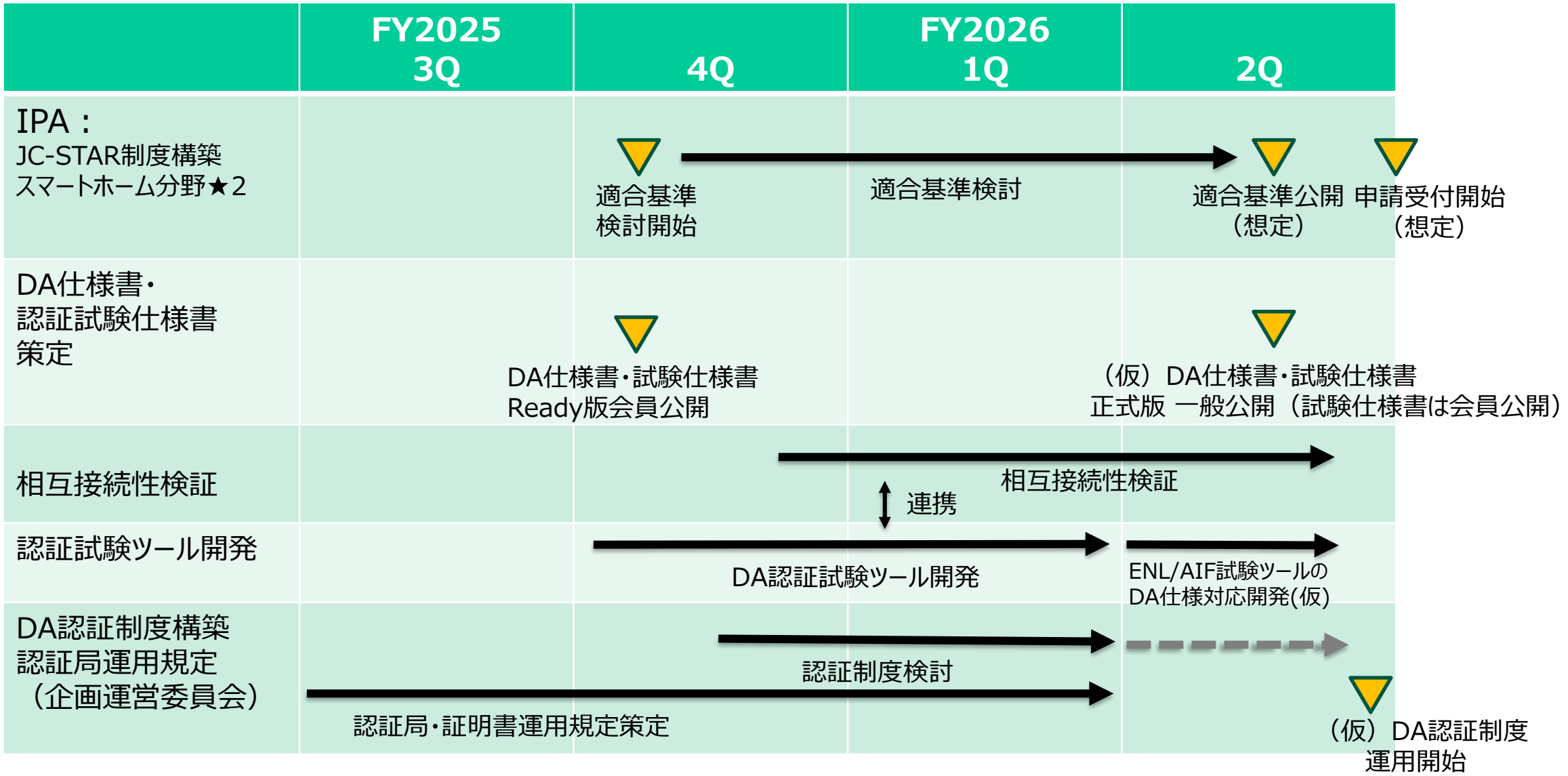
従来通りの試験仕様書に従い試験・認証を行うことで
“ECHONET Lite AIF”の認証を取得できる

DA搭載

DA仕様が動作した状態で従来の試験仕様書に従い試験・認証を行うことで
“ECHONET Lite AIF Secure”の認証を取得できる

注：DA仕様が停止した状態で試験・認証を行った場合は、ECHONET Lite AIFの認証を付与

今後のスケジュール（案）


FY2025
3Q
4Q
FY2026
1Q
2Q
IPA：
JC-STAR制度構築
スマートホーム分野★2
適合基準
検討開始
適合基準検討
適合基準公開
（想定）
申請受付開始
（想定）
DA仕様書・
認証試験仕様書
策定
DA仕様書・試験仕様書
Ready版会員公開
（仮）DA仕様書・試験仕様書
正式版 一般公開（試験仕様書は会員公開）
相互接続性検証
相互接続性検証
連携
認証試験ツール開発
DA認証試験ツール開発
ENL/AIF試験ツールの
DA仕様対応開発(仮)
DA認証制度構築
認証局運用規定
（企画運営委員会）
認証制度検討
認証局・証明書運用規定策定
（仮）DA認証制度
運用開始

【基本方針】関係者と連携しながら、ECHONET Lite DA仕様について、
円滑な活用に向けて整理と環境整備を進めていきます

引き続きご支援のほど
よろしくお願いいたします

ご清聴ありがとうございます