

IEEE 802における 標準化の基礎

IEEE P3800 Chair/ex 802.11ai Chair 眞野 浩

AGENDA

IEEE-SAにおける標準化の基礎

IEEE P802.11
標準化

IEEE802.11bcとは

標準化の成功とは



標準化の成功とは、市場形成をリードし**ブルーオーシャン**を作ること。



標準化の成功者は、市場成長モデルを示し、世界の流れを作るリーダーというプレゼンスを得る。



ICT技術の**C**ommunication は、Proprietary では成立しない。
使われる標準=つながる標準=つながる相手がある標準

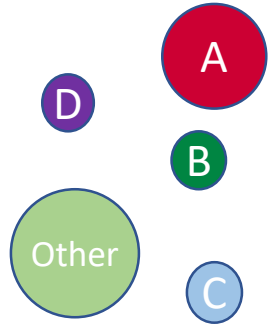


市場をつくり市場をリードすることで、日本の経済成長を牽引することこそが、技術の基盤を強化する。

標準化は、新しい市場を喚起する

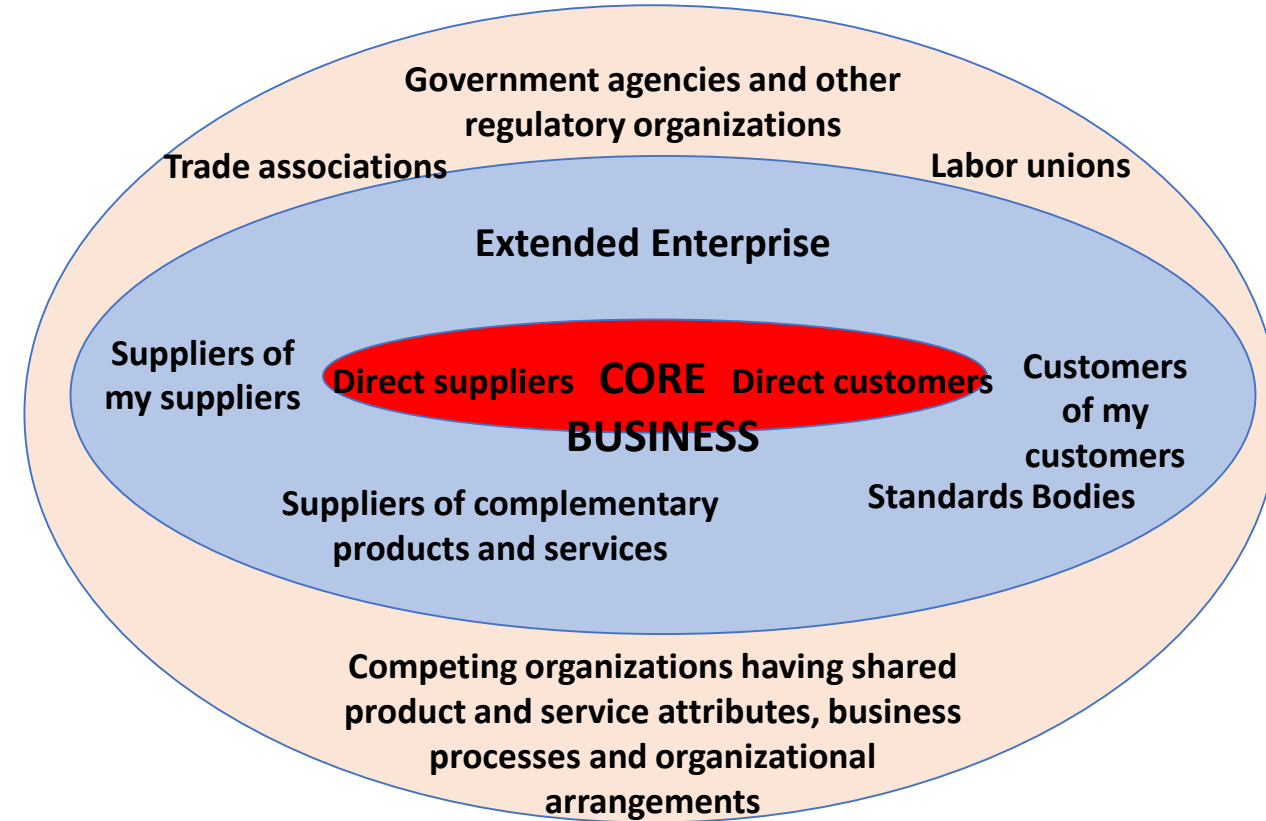
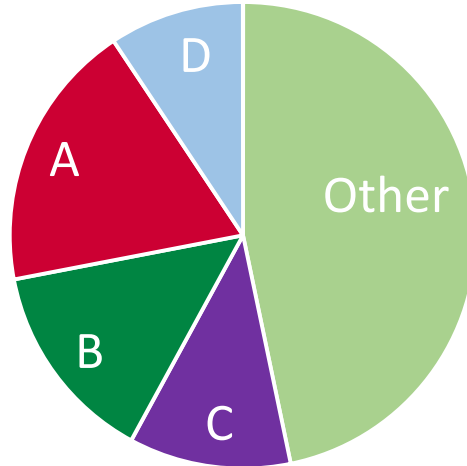
• 競争社会 → 協創社会

各社は、独自の市場を開発



より大きな市場を
生み出す

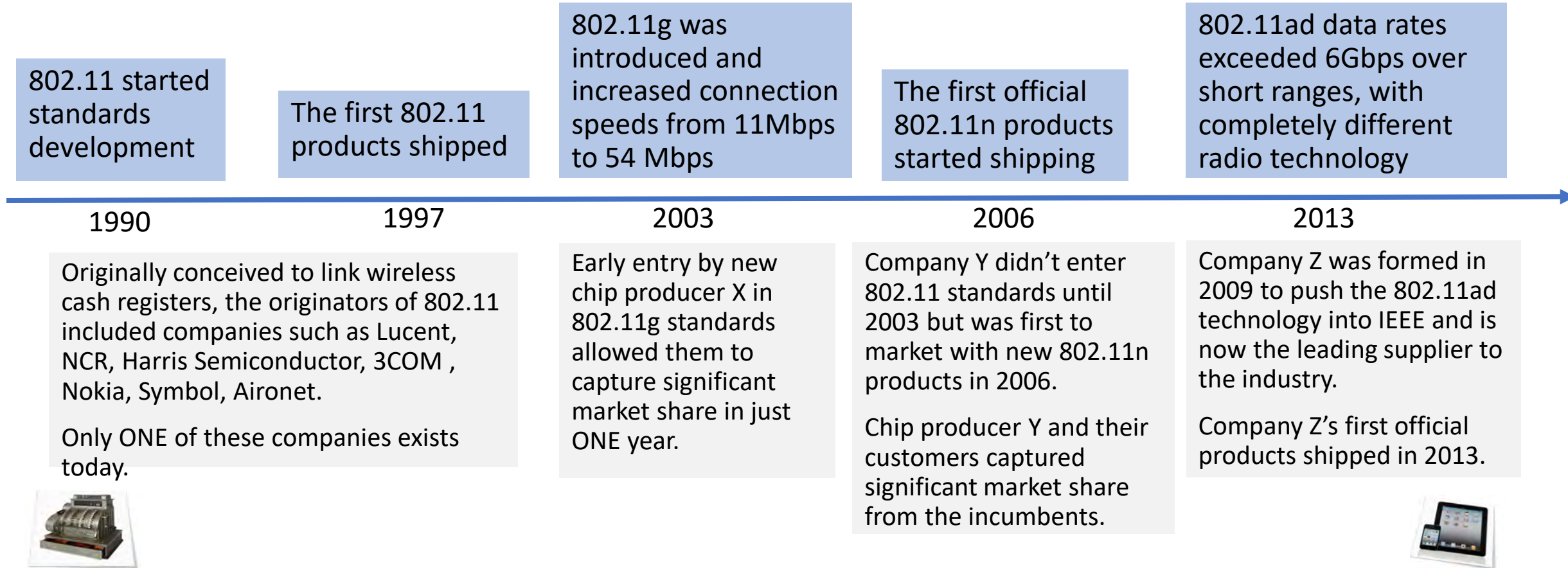
標準化による協業社会



Moore, James F. (1996). *The Death of Competition: Leadership & Strategy in the Age of Business Ecosystems*.

802.11デバイスの成長事例

IEEE-SA & DTA セミナ資料から



IEEE-SAにおける 標準化の基礎

IEEE-SAの仕組みとルール

IEEEについて

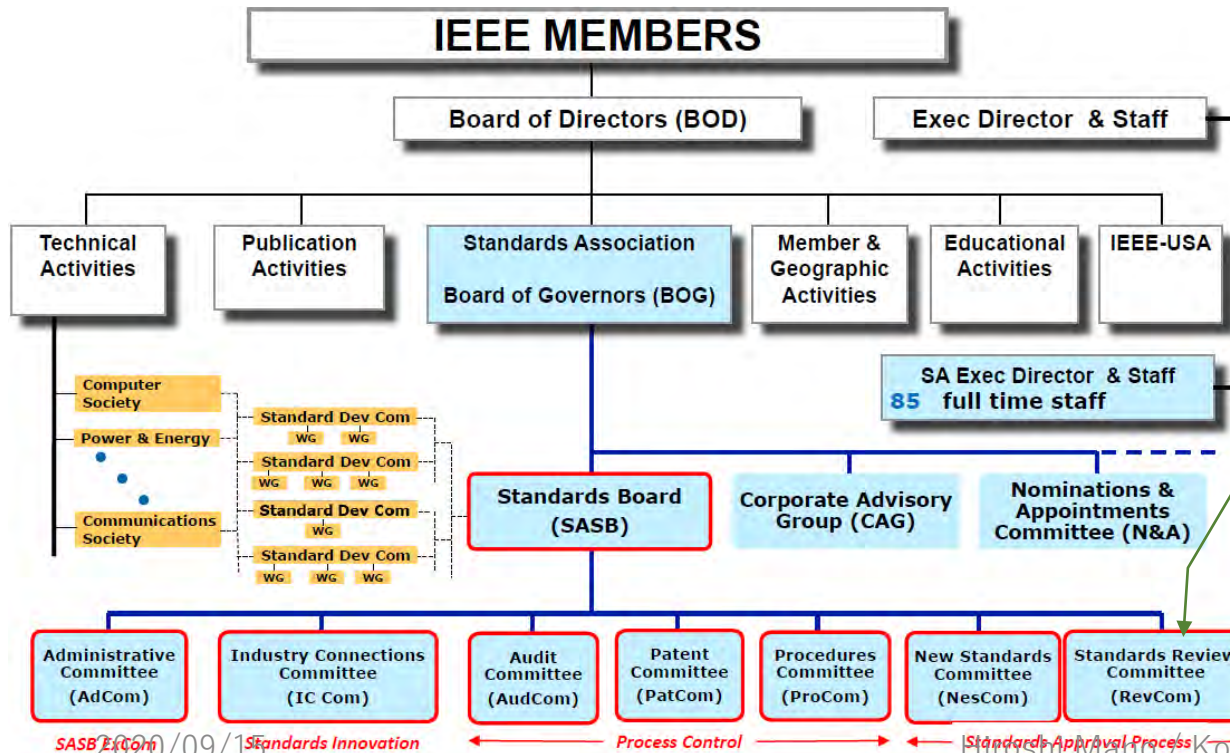
<https://standards.ieee.org/about/sasb/index.html>

■世界最大クラスのSDO

- Globally recognized standards
- 1256 active standards
- 718 standards under development
- 7264 individual members and approximately 20,000 standards developers from every continent
- 280 corporate members

■IEEE規格の強みと影響力

- Leverages the breadth of 40+ technical areas
- 100+ Smart Grid standards
- Flagship transport layer standards in communications (IEEE 802)
- 400-500 standards focused on the power and energy sector, etc.
- Independent global community
- Open standards development process
- IEEE-SA Strengths



標準化活動はIEEE-SAの下における
SASB(Standard Board)の指揮下で行っている。

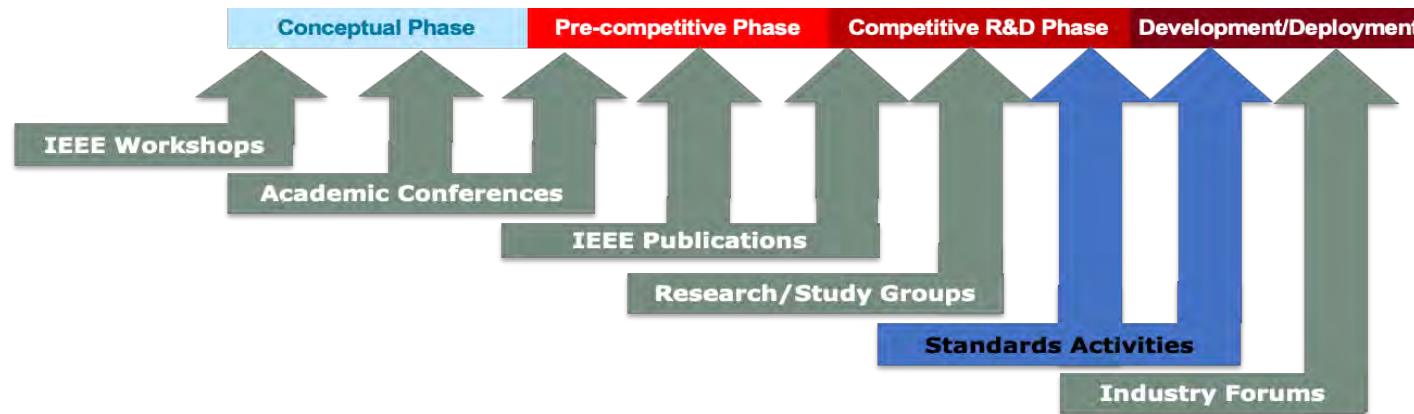
標準承認：新規標準委員会 (NesCom)、
標準レビュー委員会 (RevCom)

進捗制御：手続き委員会 (ProCom)
特許委員会 (PatCom)
監査委員会 (AudCom)

標準革新：業界連携委員会 (ICCom)
管理監督：管理委員会 (AdCom)

IEEE-SAの概要(1/2)

- IEEE (Institute of Electrical and Electronics Engineers)は、アメリカ合衆国に本部を置く電気・情報工学分野の学術研究団体（学会）であり、SA(Standard Association)は、この IEEE配下の標準化を担う機関である。
- この母体であるIEEEは、160か国以上で422,000人以上の会員を有しているが、その50%以上が米国以外の国と地域に属している。
- 標準化は下図に示すように、開発過程から社会実装展開へと移行する段階の活動として捉えている。



IEEEの活動のタイムライン (2018/03/05 IEEE-SA共催データ流通と標準化シンポジウム配布資料より)

IEEE-SAの概要(2/2)

・ビジョン&ミッション

- ・ビジョン：世界クラスの標準開発組織になること。
- ・ミッション：世界的に尊敬される、高品質で市場に関連する標準化環境を提供する。

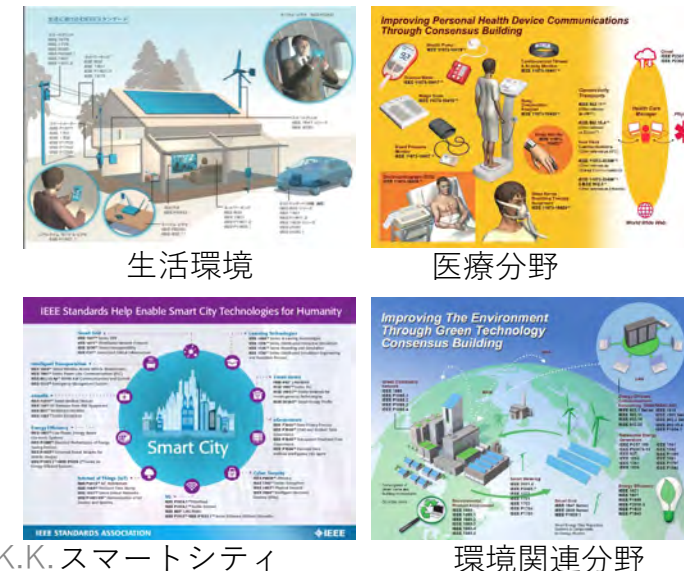
・実績

- ・累計20,000を超える国際標準仕様の開発実績。
- ・内1,200を超える標準仕様は、現時点でも有効に160カ国以上で批准されている。また、600を超える標準仕様の策定が現在進行中。



IEEE-SAの現状と活動範囲

<https://mentor.ieee.org/802-ec/dcn/19/ec-19-0098-00-00EC-ieee-802-orientation-2019.pdf#search='http%3A%2F%2Fieee802.org+ec1900980000EC'>



SASB(Standards Board) (1/2)

定義及び役割

- IEEE-SAにおける標準策定に関する最高意思決定機関。BOGによって設立および任命される。
- IEEE規格の開発と改訂の奨励および調整を行う。

構成員

- SASBは18人から26人の投票メンバーで構成される。
- 構成員はすべてIEEEかつIEEE SAメンバーである、
- 各スポンサーソサエティを管轄するIEEE Technical Activities Board Liaisonも投票メンバー。投票権のない名誉会員が1人含まれる。

2020 Roster 名簿

Gary Hoffman (Chair)	Jon Rosdahl (Vice Chair)	John Kulick (Past Chair)	Konstantinos Karachalios (Secretary, non-voting)
----------------------	--------------------------	--------------------------	--

Members メンバー

Ted Burse	Paul Nikolich [TAB Rep.]	David Law	Sha Wei
Doug Edwards	Damir Novosel	Howard Li	Philip Winston
Travis Griffith	Dorothy Stanley	Dong Liu	Daidi Zhong
Grace Gu	Mehmet Ulema	Kevin Lu	Jingyi Zhou
Guido Hiertz	Lei Wang		

Member Emeritus

IEEE Government Engagement Program on Standards (GEPS) Representatives

Administrator

名誉会員 Joseph Koepfinger (non-voting)

各国の政府関連プログラム代表 (省略)

管理者 Dave Ringle

SASB(Standards Board) (2/2)

構成される委員会とその役割

①AudCom (Audit Committee)

- 標準開発を行う機関(ワーキンググループや委員会) に対する監査機関。

②IC Com (Industry Connections Committee)

- 産業界との連携活動の開始を求めるICAID (Industry Connections Activity Initiation Documents) を調査し、その承認に関して IEEE SASBに勧告する委員会。

③NesCom (New Standard Committee)

- 提案された標準プロジェクトが適切なソサエティまたは他の組織に割り当てられたIEEEの範囲と目的の範囲内にあり、複数の団体がIEEE標準の開発に適切に参加していることを確認する責任を持つ委員会。

④PatCom (Patent Committee)

- IEEE規格の特許および特許情報の使用を監視する委員会。

⑤ProCom (Procedure Committee)

- SASBおよび標準化活動に従事する他のIEEE委員会による責任の効率的な遂行を促進するために、SASBの改善と手順の変更を推奨する責任を持つ委員会。

⑥RevCom (Standard Review Committee)

- IEEE SASBの承認または採択のために提出された規格の承認または不承認に関する勧告を行う委員会。

IEEE標準化の基本

運営

- WTO (World Trade Organization)/ TBT(Agreement on Technical Barriers to Trade)の原則に準拠すること。
- 厳格なピアレビューが行われること。
- 参加者の集合的なコンセンサスの見解を反映していること。
- 高品質でグローバルに関連する技術標準になること。

基本ポリシー

①Consensus 合意性

- 参加者の多数による合意がされていること。

②Due Process 適正な策定手順

- 全てにおいて適正な手順が取られていること。

③Openness オープン性

- 誰でもが、開発に参加する機会が与えられること。

④Right of appeal 異議申立ての権利

- 誰もが、規格の策定前、策定後でも意義を申し立てる権利があること。

⑤Balance バランス

- すべての重要な利害関係者メンバーからの意見が反映されていること。

Consensus

Due Process

Openness

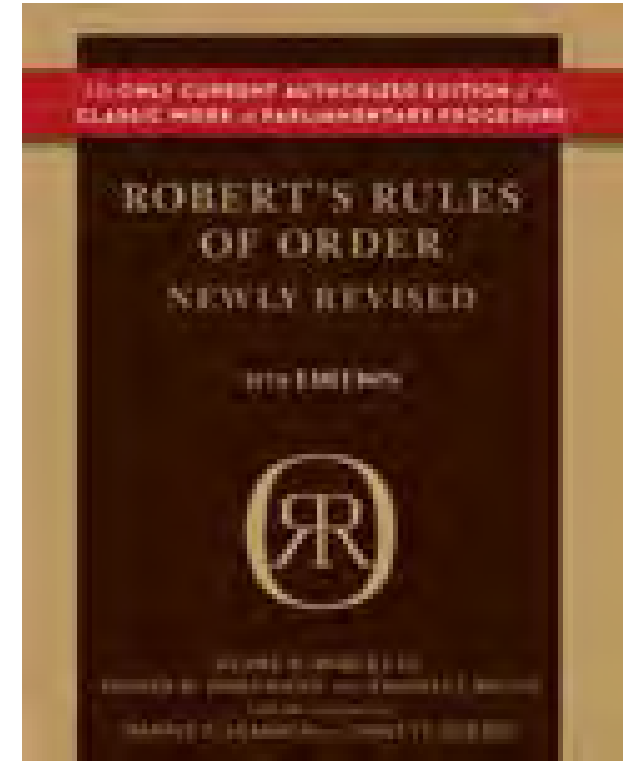
Right of Appeal

Balance



Robert's Rules of Order

- ロバートの会議規則 とは、
 - 1876年にアメリカ陸軍のヘンリー・ロバート将軍が作成。
- 会議規則が守るもの
 - (1) 多数者の権利（過半数の賛成）
 - (2) 少数者の権利（少数意見の尊重）
 - (3) 個人の権利（プライバシーの権利擁護）
 - (4) 不在者の権利（不在投票）
- 例えば
 - 発言者は、議長とのみ話せる
 - ローカルトークの禁止
 - 動議提案
 - 2人以上の賛同が必要
 - 審議棚上げ
 - 不十分な動議は、棚上げされる
 - 会期満了で失効
 - 一事不再議
 - 一度議決されたものは、審議できない



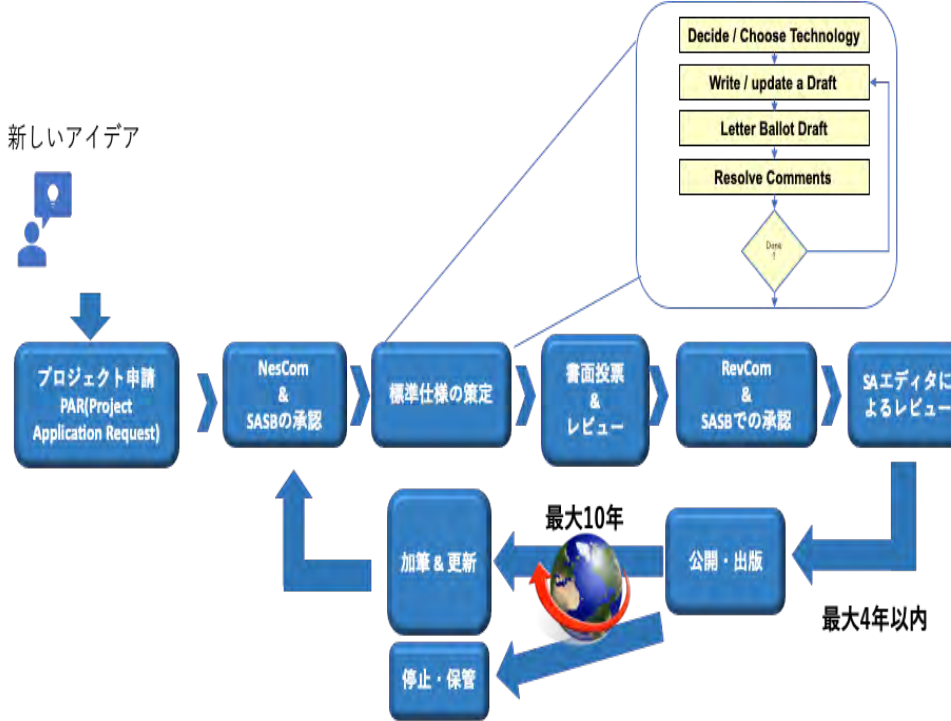
IEEE-SAにおける標準作成の流れ

標準化手順



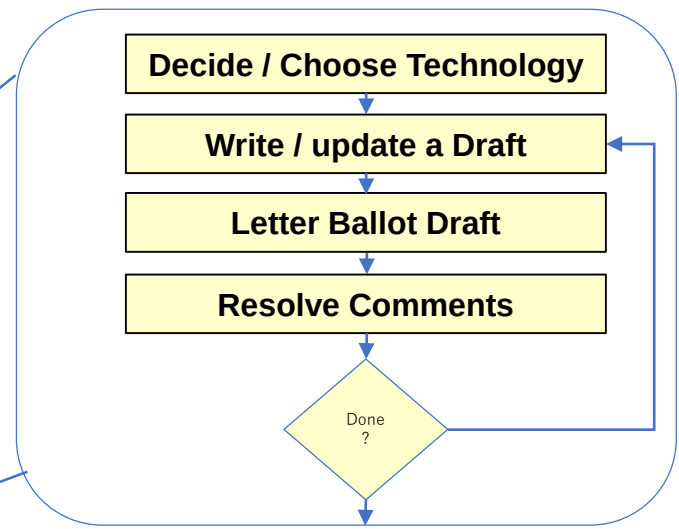
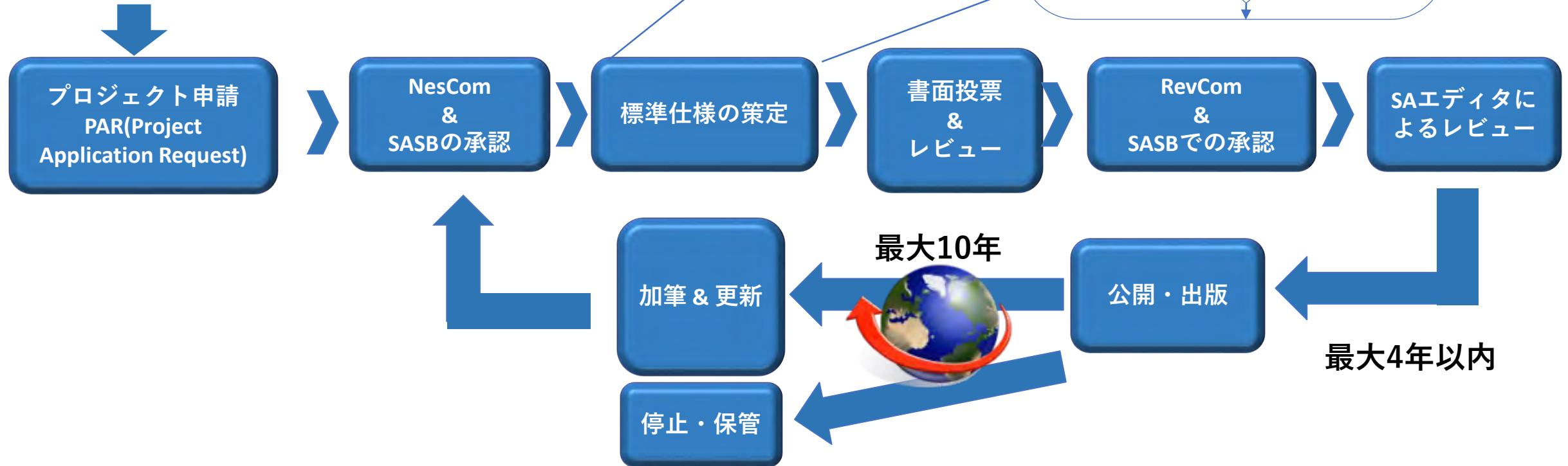
策定期間及び有効期限

- 策定はプロジェクト開始から4年以内
- 公開された標準は修正や改定がなければ10年で無効となる



IEEEにおける標準化手順

新しいアイデア



https://jp.ieee.org/activities/files/About_IEEE-SA_July2015.pdf

IEEEの標準化手順 2

個人標準化プログラム(Individual method) IEEE802等

- ⑩参加単位は、個人
- ⑩個人は、あくまで個人の利益代表
- ⑩各個人は、1投票権を有する
 - ⑩最低10人の投票権者による投票参加が必要
- ⑩投票権者は、IEEE-SA 個人会員であること (WGへの参加やWGの投票は、非会員でも可能)

法人標準化プログラム(Entity method) IEEE P2413等

- ⑩参加単位は、“entities=機関,” 例えば, 法人, 大学, 政府機関, など
- ⑩参加者は、機関に指定された代表者または代理人。
- ⑩各機関は、1投票権を有する
 - ⑩最低3機関による投票参加が必要
- ⑩各機関は、その利益代表者が会議に参加し投票権を行使する

The [IEEE-SA Standards Board Bylaws](#) require that “participants in the IEEE standards development individual process shall act based on their qualifications and experience”

This means participants:

- Shall act & vote** based on their personal & independent opinions derived from their expertise, knowledge, and qualifications
- Shall not act or vote** based on any obligation to or any direction from any other person or organization, including an employer or client, regardless of any external commitments, agreements, contracts, or orders
- Shall not direct** the actions or votes of other participants or retaliate against other participants for fulfilling their responsibility to act & vote based on their personal & independently developed opinions

By participating in standards activities using the “*individual process*”, you are deemed to accept these requirements; if you are unable to satisfy these requirements then you shall immediately cease any participation

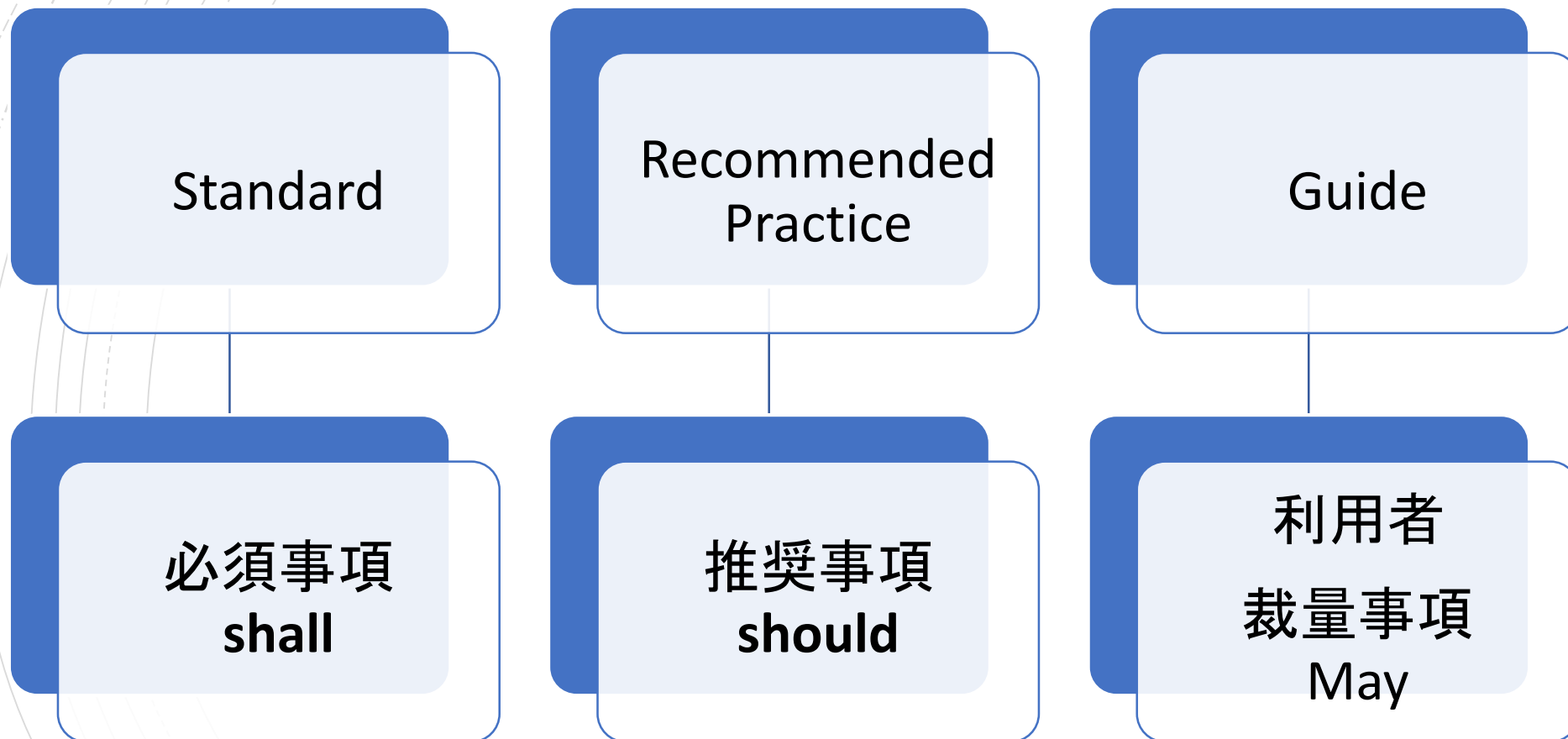


Individual
とは

IEEE SAの 標準必須特許

- FRAND: Fair, Reasonable And Non-Discriminatory (公平、妥当かつ差別のないライセンス)
 - 標準必須特許は、その標準を使用する者にたいして公平、妥当かつ差別がなく使用許諾をする。
 - ただし、その許諾条件は、当事者間の調整であり、無条件提供を求めるものではない。
- *If anyone in this meeting is personally aware of the holder of any patent claims that are potentially essential to implementation of the proposed standard(s) under consideration by this group and that are not already the subject of an Accepted Letter of Assurance, please respond at this time by providing relevant information to the WG Chair.*
- この会議に参加している誰かが、このグループが検討している提案規格の実施に不可欠となる可能性のある特許請求項の所有者を個人的に知っている場合で、まだ承認されたLoAの対象となっていない場合は、この時点でWG議長に関連情報を提供することで対応してください。

IEEE Standardの種類





IEEE Standardの 記載手法

Normative

- Information that is required in order to implement the standard
- The text that establishes requirements, recommendations, or alternative approach.
- 規格を実施するために必要な情報
- 要件、推奨事項、または代替的なアプローチを定めた文章

Informative

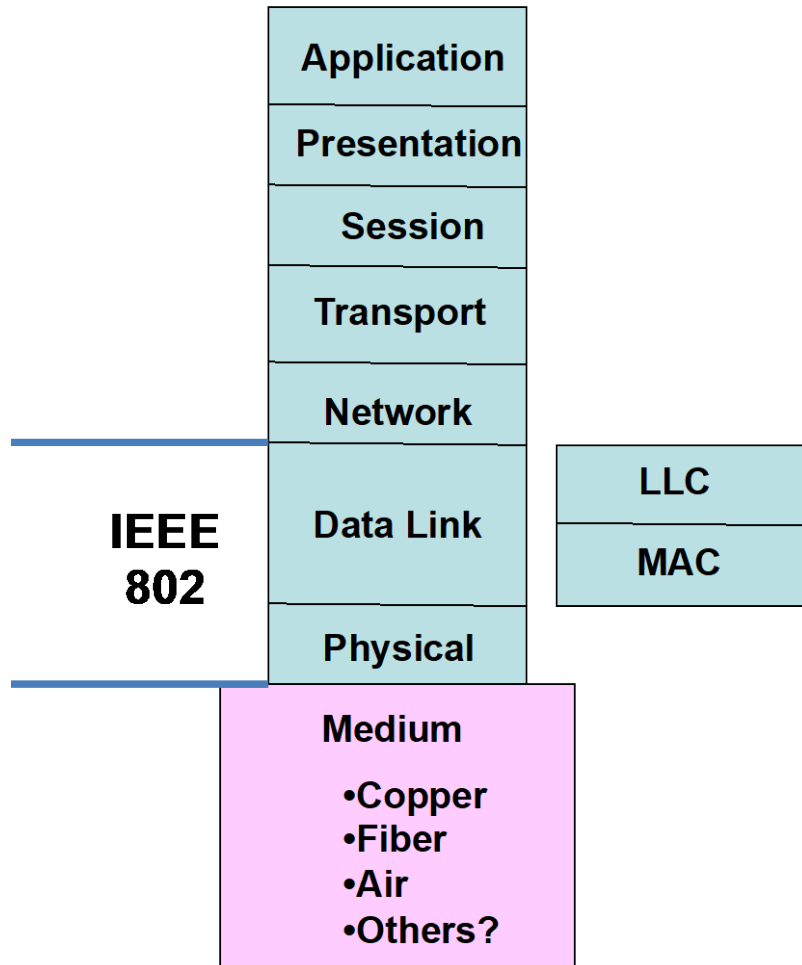
- Informative text is provided for background only and is therefore not officially part of the standard.
- Text that puts the processes and procedures in context, illustrates them, explains them
- 情報提供、背景説明だけに提供されており、正式な規格の一部ではない。
- プロセス及び手順を文脈に沿って説明し、図示し、説明する文章など

IEEE P802.11標準化

802 LMSC

802.11 WLAN

Reference Model for End Stations



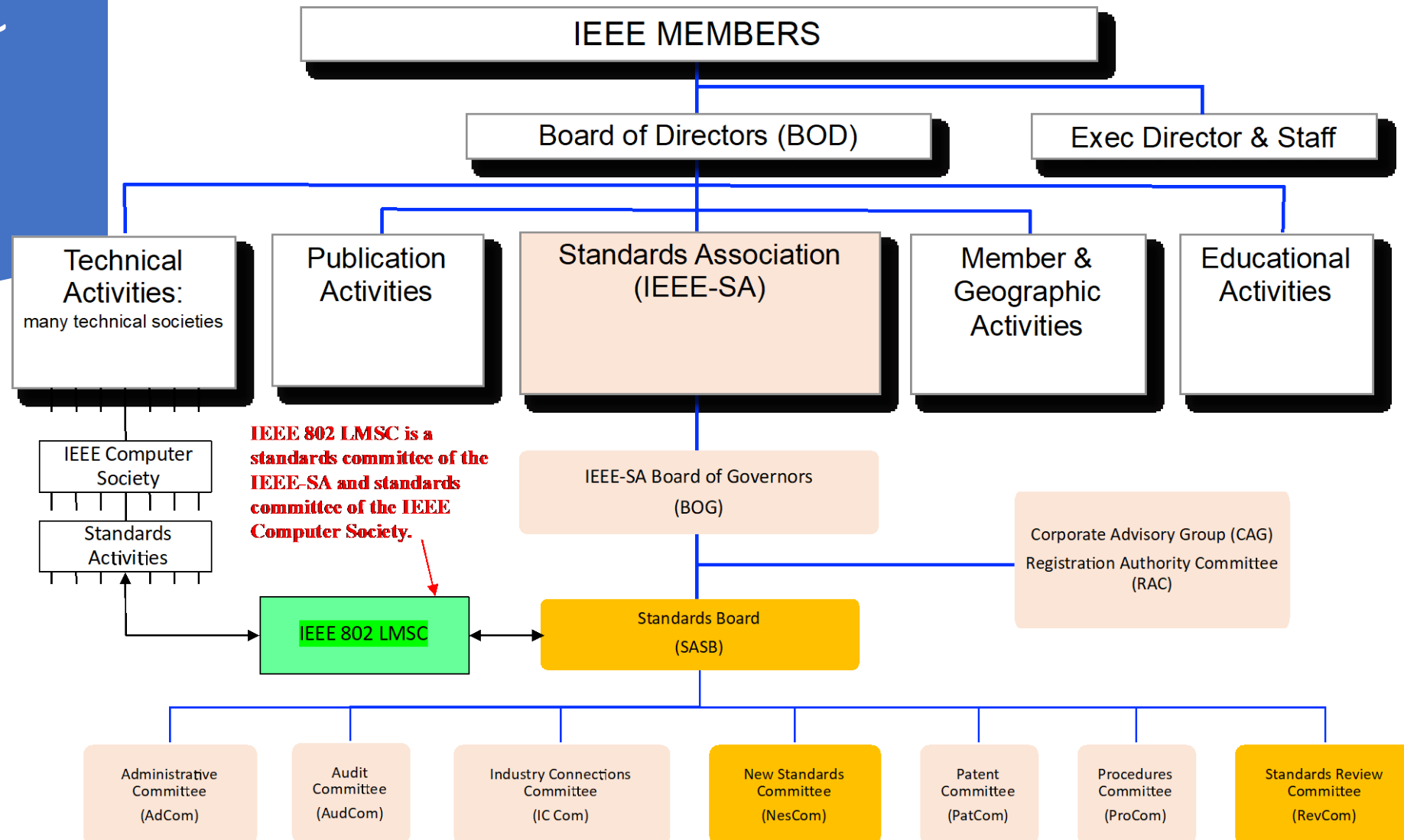
July 2020/ doc.: IEEE 802.11-20/0007r2

IEEE802の対象範囲

- IEEE 802 standards emphasize the functionality of the lowest two layers of the OSI reference model, and the higher layers as they relate to network management
 - physical layer (PHY, Layer 1)
 - data link layer (DLL, Layer 2)
- IEEE 802 divides DLL into:
 - Medium Access Control (MAC)
 - Multiple specifications
 - Common logical link control (LLC)
- See details in IEEE Std 802
 - “IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture”

IEEE802 LMSC と802.11WG

IEEE 802 within IEEE and IEEE-SA Structure



IEEE802 LMSC ECの構成

IEEE 802 EXECUTIVE COMMITTEE (EC)

CHAIR
Paul Nikolich

Working Group/TAG Chairs

802.1 Bridging/Arch Glenn Parsons	802.3 Ethernet David Law	802.11 WLAN Dorothy Stanley
802.15 WPAN Bob Heile	802.18 TAG Radio Regulatory Ray Holcomb	
802.19 Coexistence Steve Shellhammer	802.24 Vertical Applications Tim Godfrey	

Appointed Officers

1st Vice Chair James P.K. Gilb	2nd Vice Chair Roger Marks
Executive Secretary Jon Rosdahl	Recording Secretary John D'Ambrosia
Treasurer George Zimmerman	Member Emeritus (non-voting) Clint Chaplin
	Member Emeritus (non-voting) Geoff Thompson

Hibernating WG Chairs (non voting)

802.17 Resilient Packet Ring John Lemon	802.21 Media Indep. Handover Servs Subir Das
802.16 BWA Roger Marks	802.22 WRAN Apurva Mody

HIBERNATED

802.16 Broadband Wireless Access
802.21 Media Independent Handover Services
802.22 Wireless Regional Area Networks

DISBANDED

802.2 Logical Link Control
802.6 Distributed Queue Dual Bus
802.9 Integrated Service LAN
802.14 Cable Modems
802.20 Mobile Broadband Wireless Access

802.4 Token Bus

802.7 Broadband TAG

802.10 Security

802.5 Token Ring

802.8 Fiber Optic TAG

802.12 Demand Priority

802.23 Emergency Services

July 2020/ doc.: IEEE 802.11-20/0007r2

Participant 参加できるのは?

- For the development of standards, **openness** and **due process** are mandatory.
- Openness requires that any person who has, or could be reasonably expected to have an interest, and who meets the requirements of these procedures, has a right to participate by:
 - a) Attending Working Group meetings (in person or electronically)
 - b) Becoming a member of the Working Group
 - c) Becoming an officer of the Working Group
 - d) Expressing a position and its basis,
 - e) Having that position considered, and
 - f) Appealing if adversely affected.
- IEEE やIEEE SA の会員でなくても参加できます。

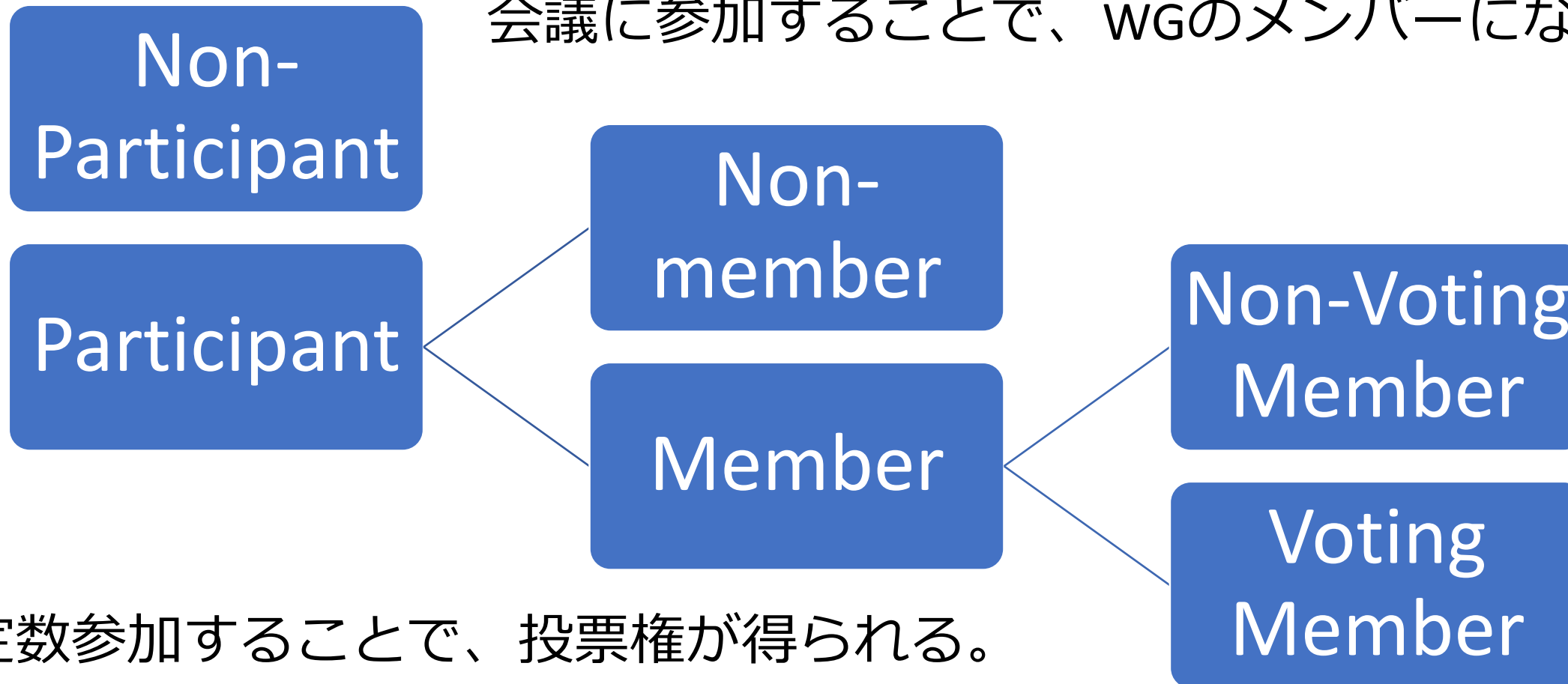
Working Group Responsibilities WGの役目

- a) Complete the project from Project Authorization Request (PAR) approval to IEEE-SA Standards Board approval as specified by the PAR, and in compliance with IEEE-SA policies and procedures.
- b) Use the IEEE-SA document template format.
- c) Submit to the Sponsor any documentation required by the Sponsor; e.g., a project schedule or a monthly status report.
- d) Notify the Sponsor of the draft development milestones.
- e) Notify the Sponsor when the draft is ready to begin IEEE-SA Sponsor ballot.
- f) Only those authorized to access and use IEEE's data, including personal data, from IEEE systems are permitted to do so, for the purposes intended, including to support the technical development work on the standard, and only in compliance with IEEE or IEEE- SA Privacy and data privacy policies.

Participant

参加者の種類

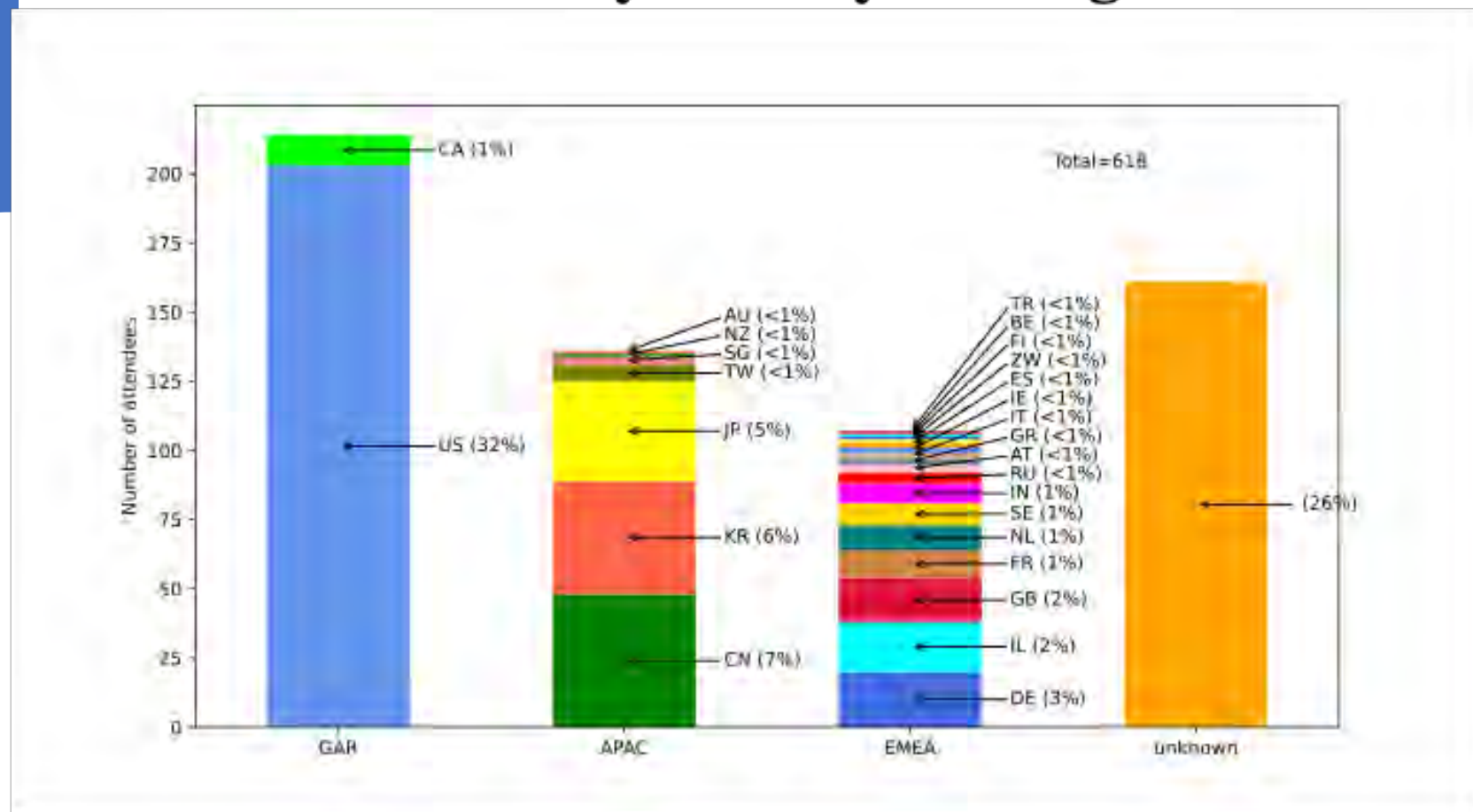
会議に参加することで、WGのメンバーになれる。



一定数参加することで、投票権が得られる。

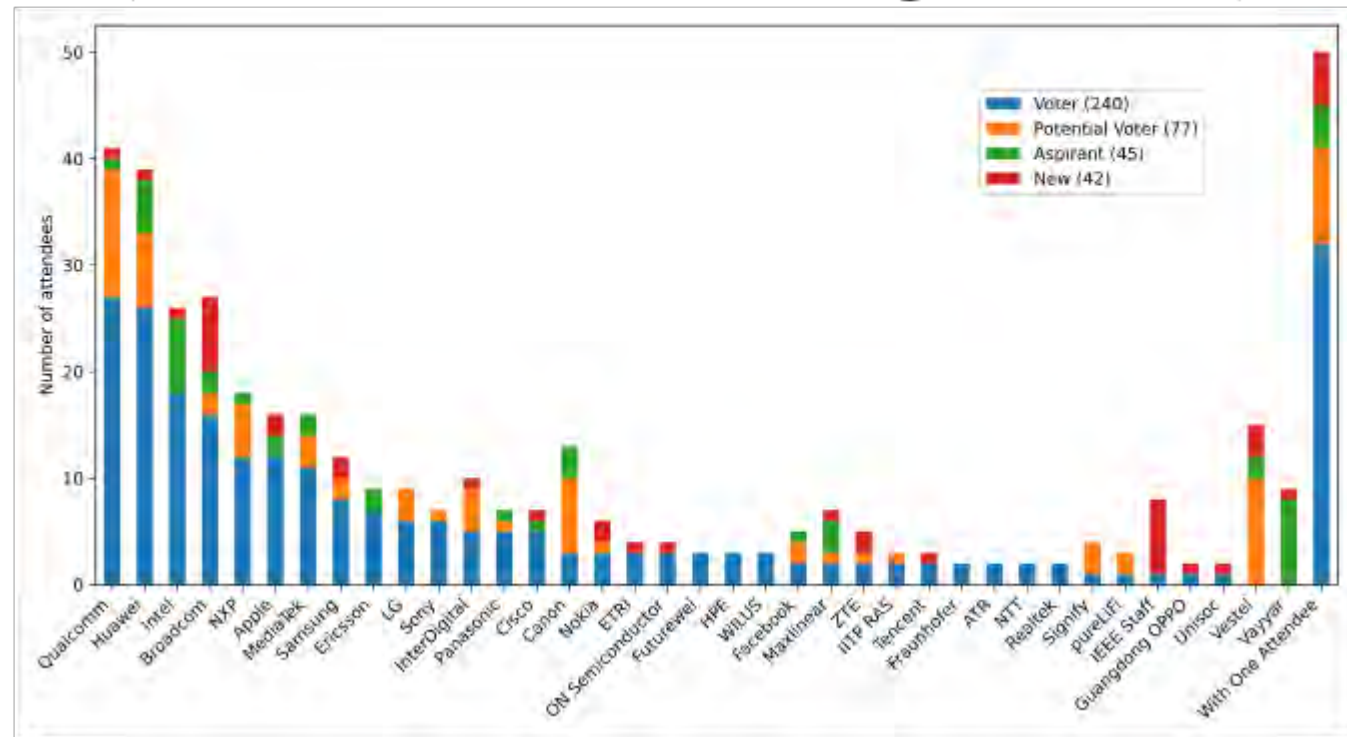
地域別参加者

Members by country and region



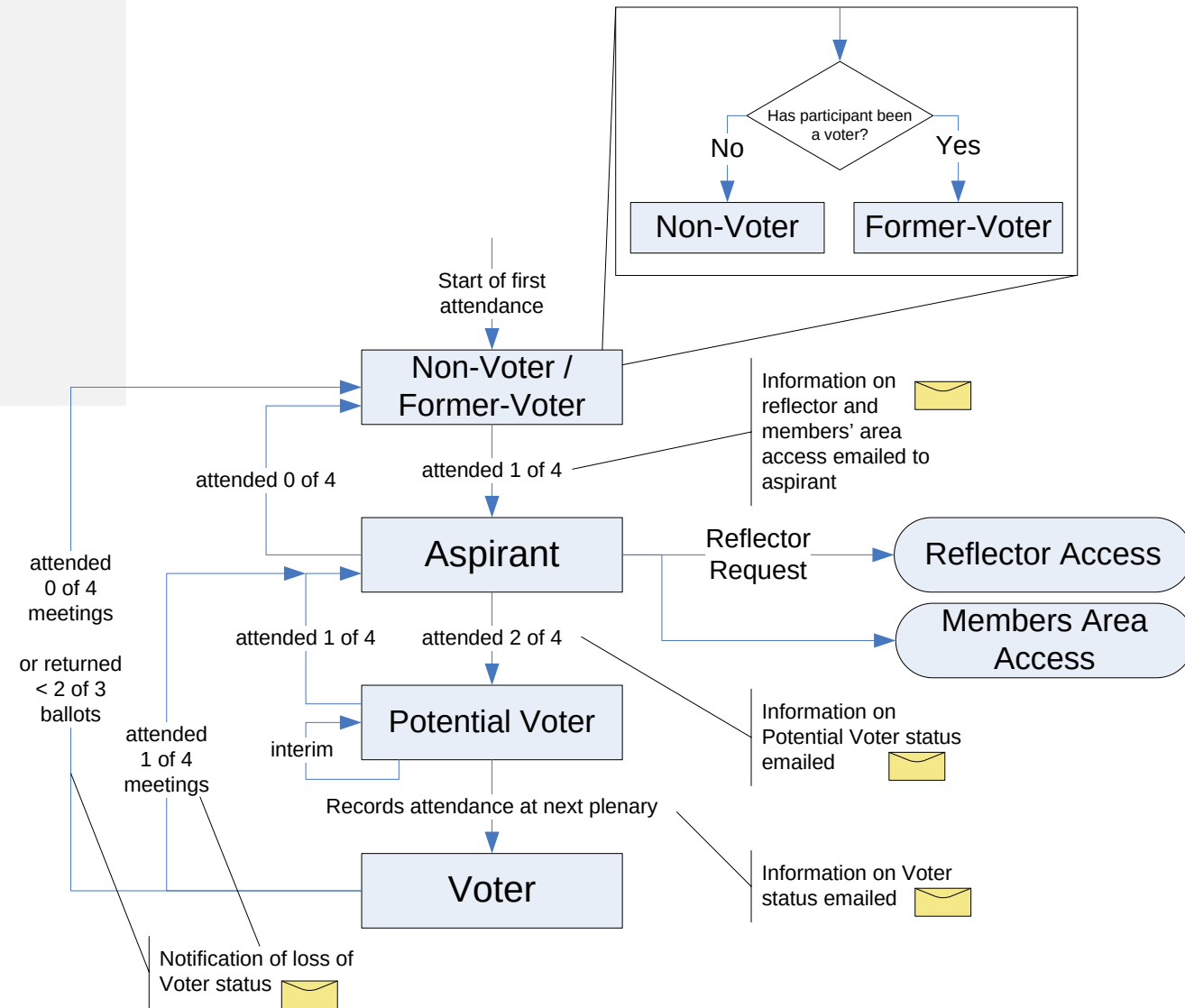
Affiliation

Attendees by affiliation (attended at least one meeting Nov to Jan)

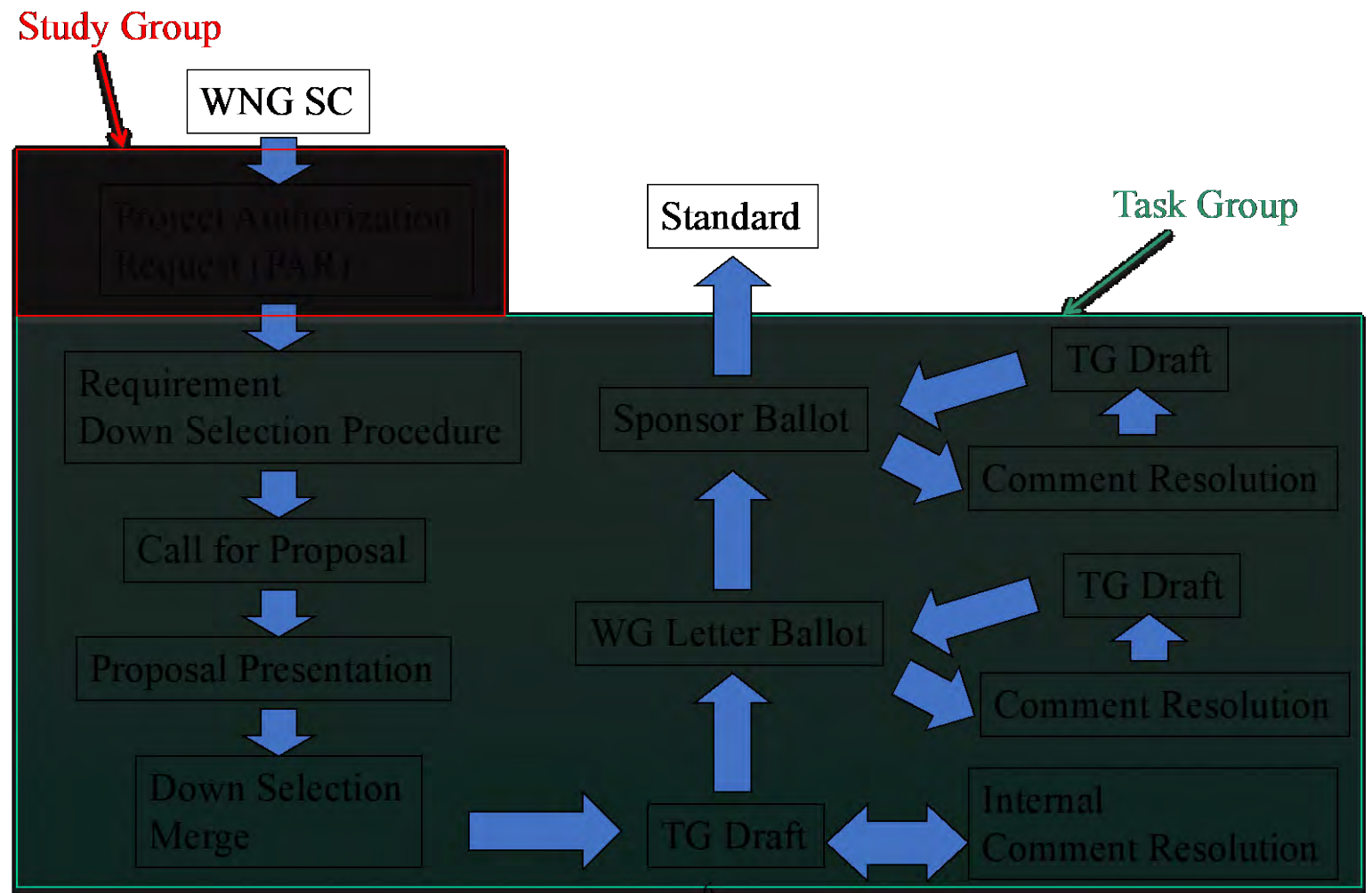


IEEE802 の投票権

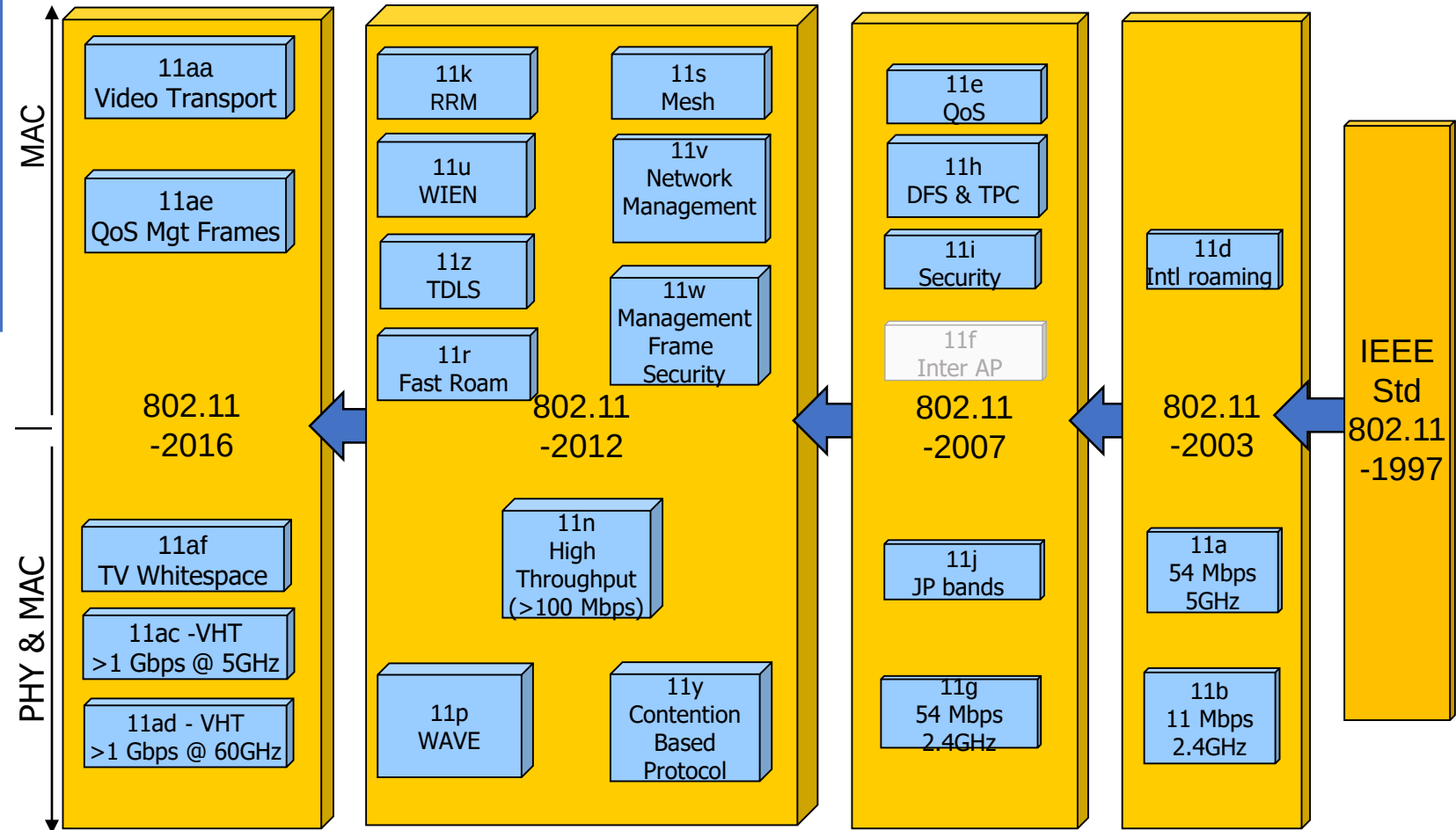
- 意思決定は、多数決で決めるため投票権が必要
- 投票権取得条件
 - 投票権は4回の連続する Plenary のうち3回目の出席で取得
 - 3回のうち1回は Interim で代替可
 - 投票権付与は Plenary のみ
 - セッションの75%以上出席しないと出席とは認められない
 - Base Slot が18コマだと14コマ以上出席
- 投票権維持
 - 直近4回の Plenary 中2回(1回は、Interim でも可能)に出席が必要
 - 書面投票による投票権の行使が義務



IEEE802 WGの 標準化手順



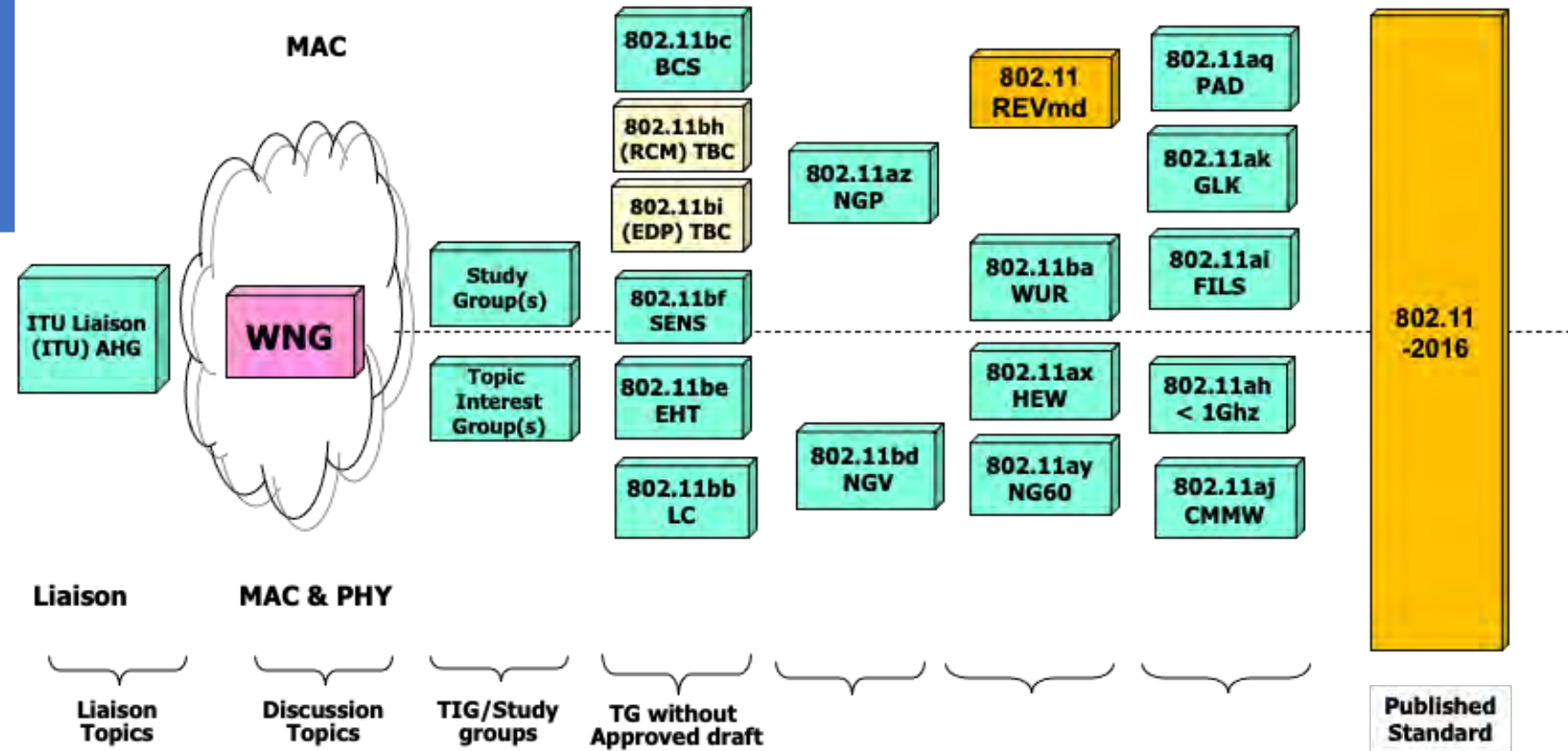
IEEE 802.11 Revisions



Jan 20201/ doc.: IEEE 802.11-20/1905r1

IEEE 802.11 Standards Pipeline

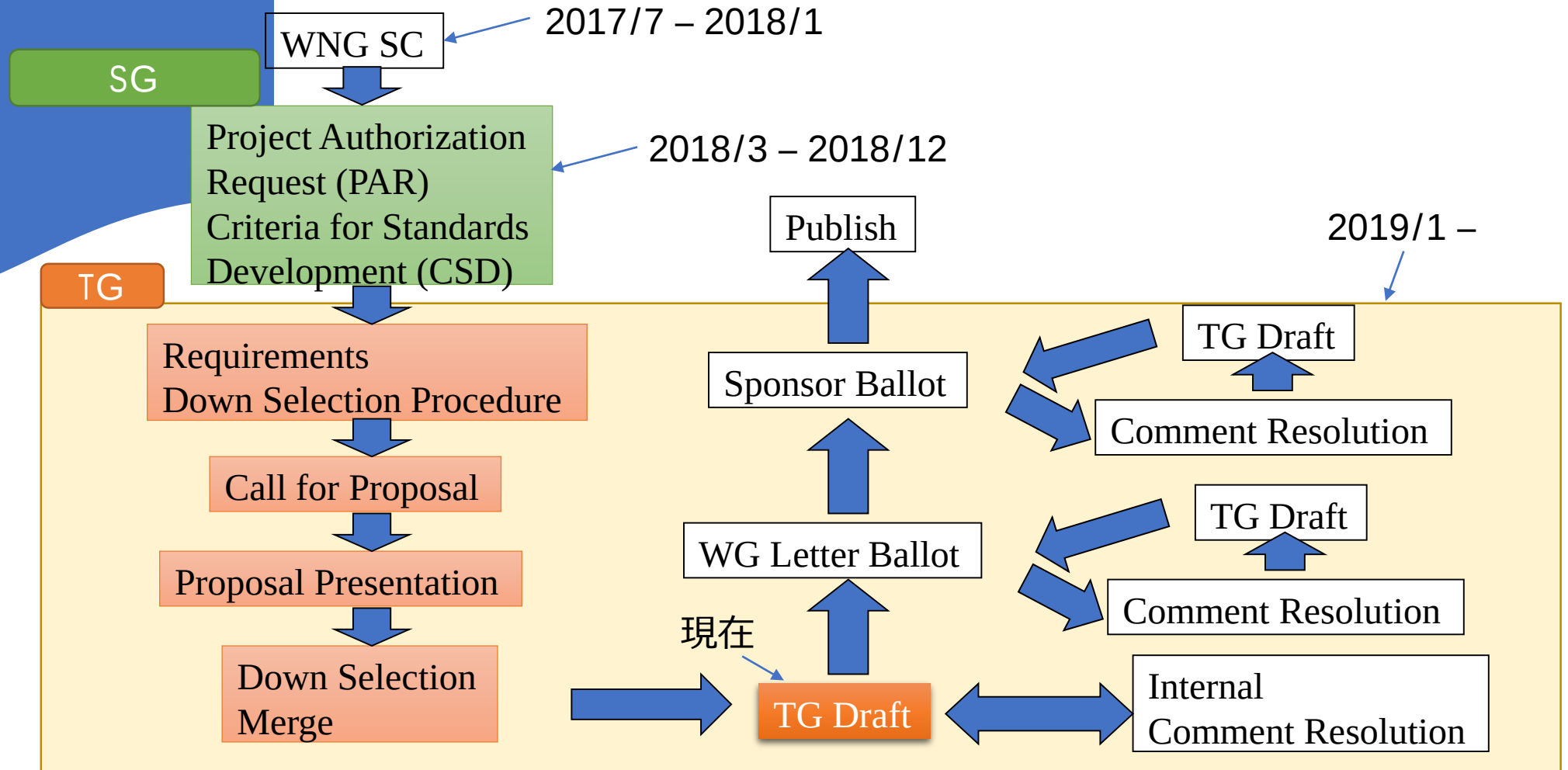
M4.1.4 IEEE 802.11 Standards Pipeline



July 2021/ doc.: IEEE 802.11-20/1905r1

IEEE802.11bc

IEEE 802.11bc のステータス

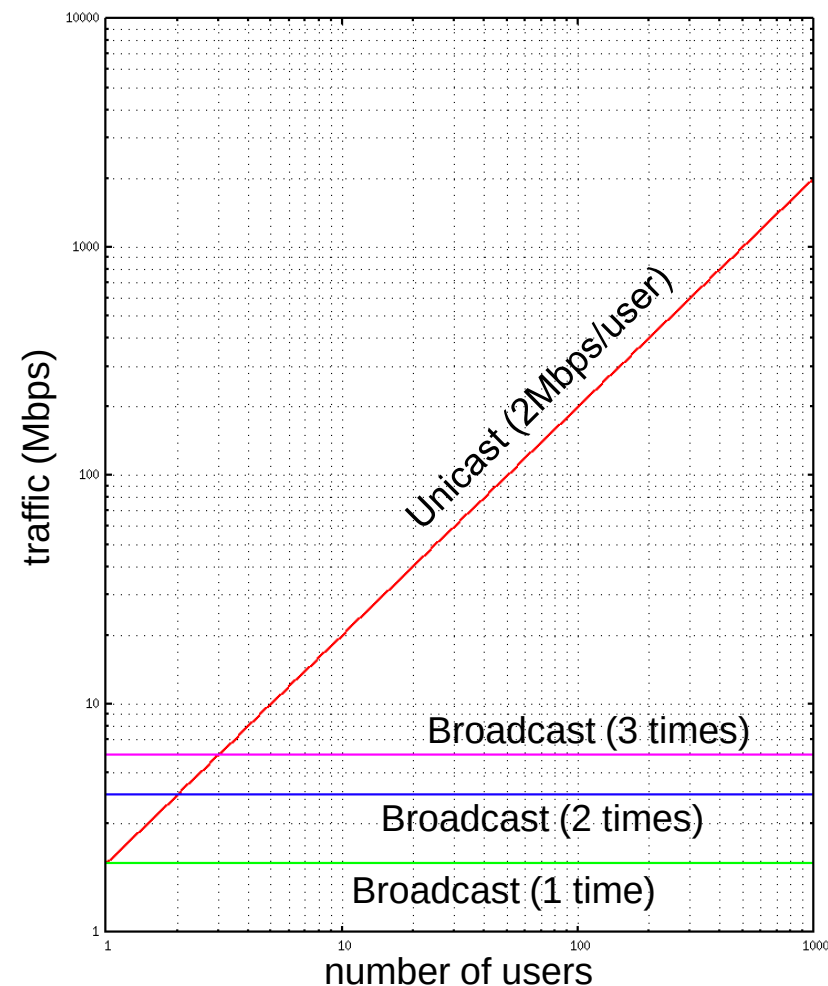


なぜ無線LANで放送？

- 無線はそもそも放送向き。(範囲内のデバイスは受信できる)
 - ブロードキャストの仕組み(グループアドレス)はすでにある
 - コンテンツはリアルタイムで送信可能
 - 免許不要
 - セル範囲は広すぎず狭すぎず (半径数十m程度)
 - 高速 (～数百Mbps)
 - 低コスト
-
- 現在このように手軽な放送手段はない

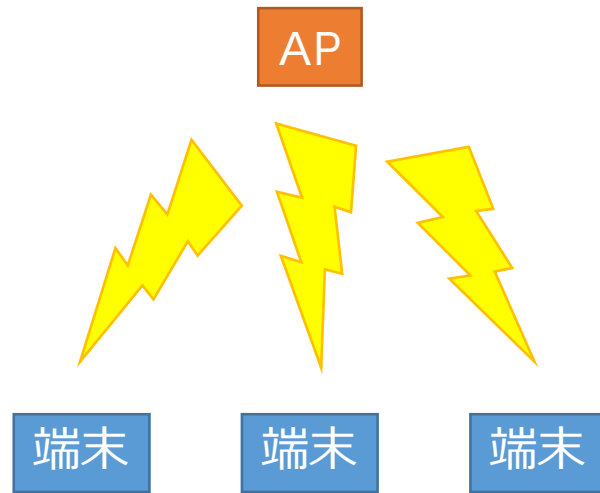
ブロードキャストのメリット

- ユニキャストではトラフィックがユーザー数に比例
- ブロードキャストではユーザー数に関わらず一定
 - ただしACKが使えないのでパケットロスに対する対策が必要

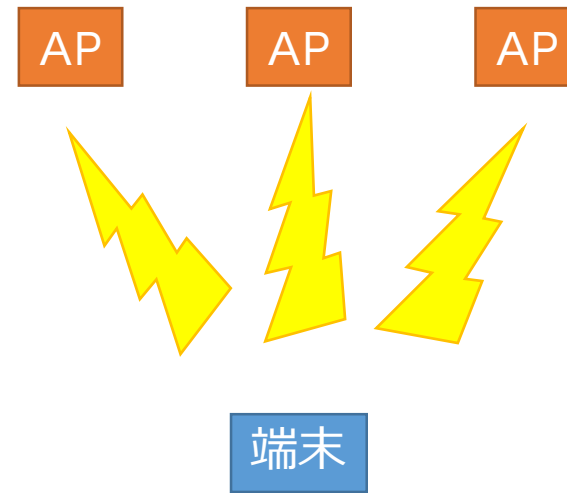


ユースケース

Downlink (DL) と Uplink (UL)



Downlink
APから多数の端末に送信

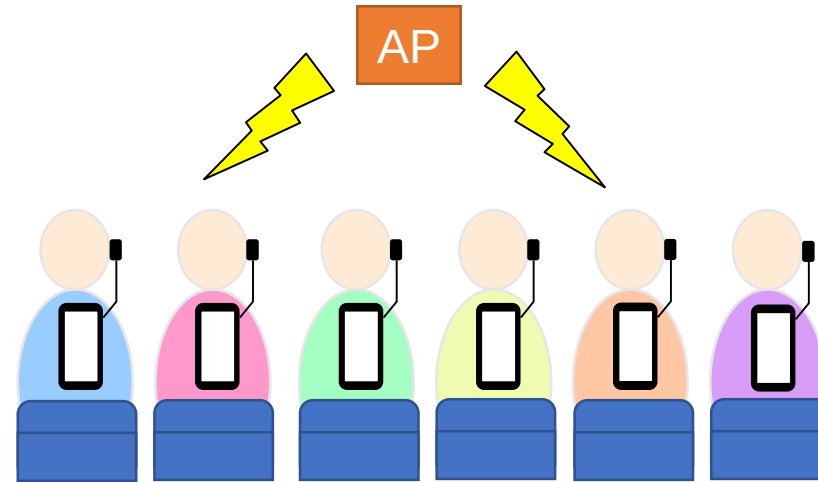


Uplink
端末から複数のAPに送信

ユースケース1

スタジアムライブストリーミング (DL)

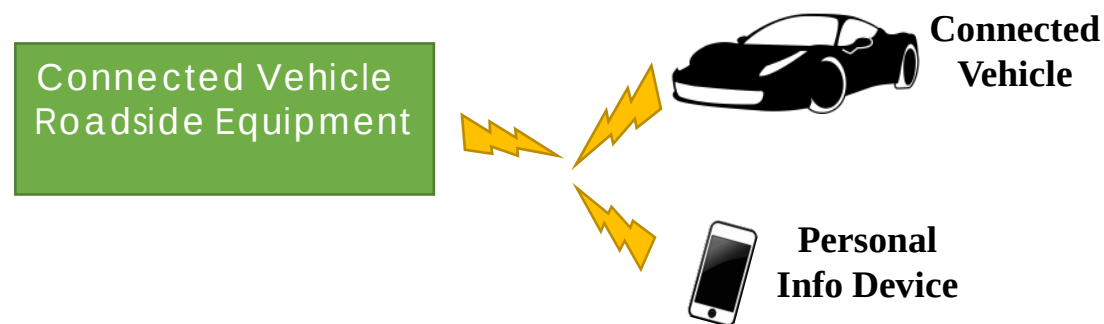
- ハイライトのリプレイ動画配信
- 様々なアングルの動画同時配信
- 並行して行われている競技の動画配信 (体操・陸上競技など)



ユースケース 2

I T S (DL)

- 踏切で列車接近を知らせる
- 旅行情報の配信



路側→車両ブロードキャスト

ユースケース 3 イベント (DL)

- コンサート会場でスタッフ向けのステージ動画配信
- イベント入場待ち客へのコンテンツ提供



ユースケース 4

緊急情報 (DL)

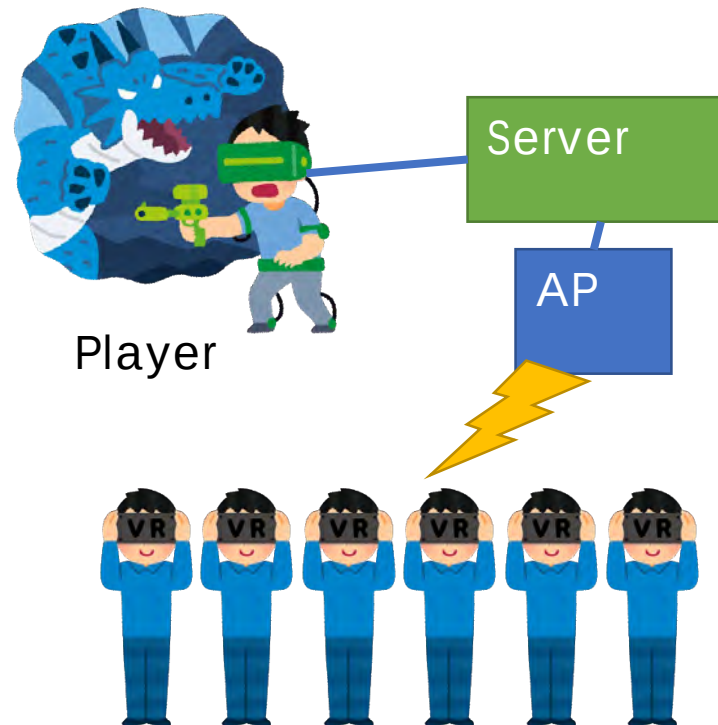
- ショッピングモールなどでの火災時の避難誘導
- 避難所での情報提供



ユースケース 5

eSports VR (DL)

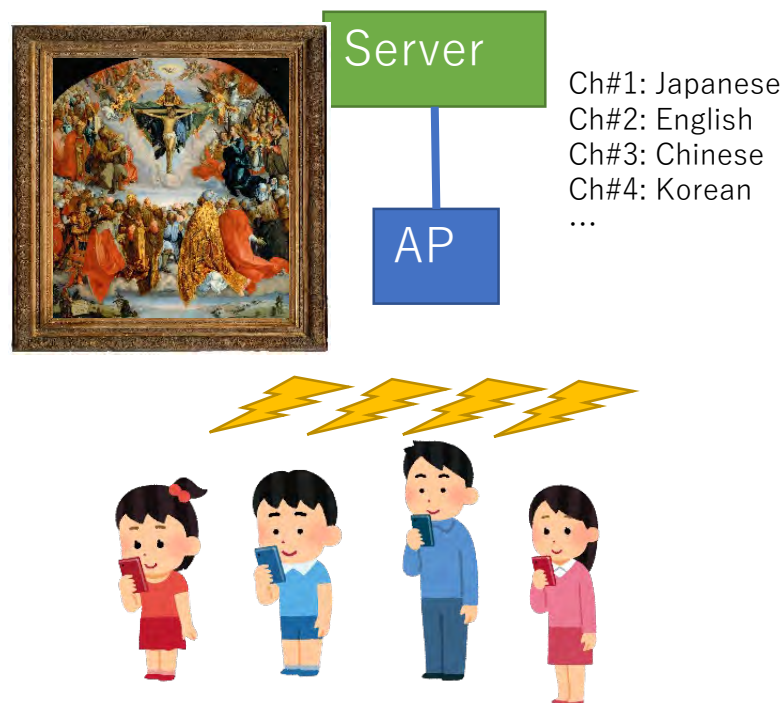
- eSportsイベントでのVRプレイ画像配信



ユースケース 6

多言語案内 (DL)

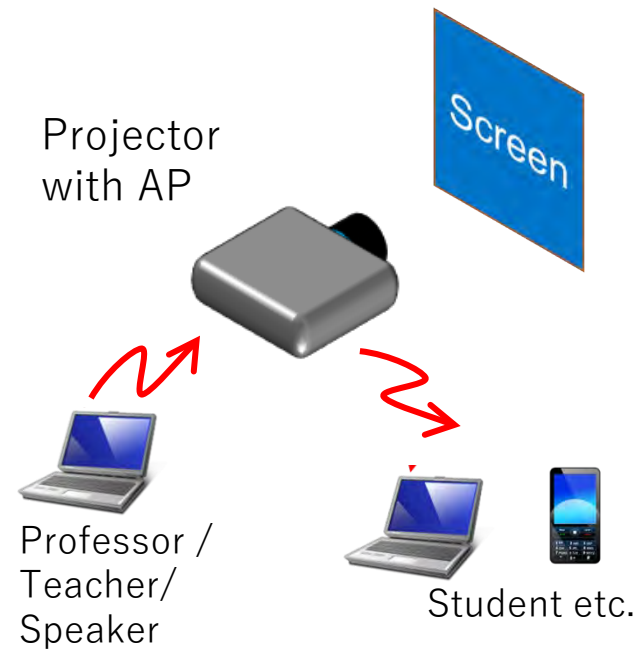
- 美術館・博物館などで多言語情報提供
- 国際会議での同時通訳配信



ユースケース7

講義 (DL)

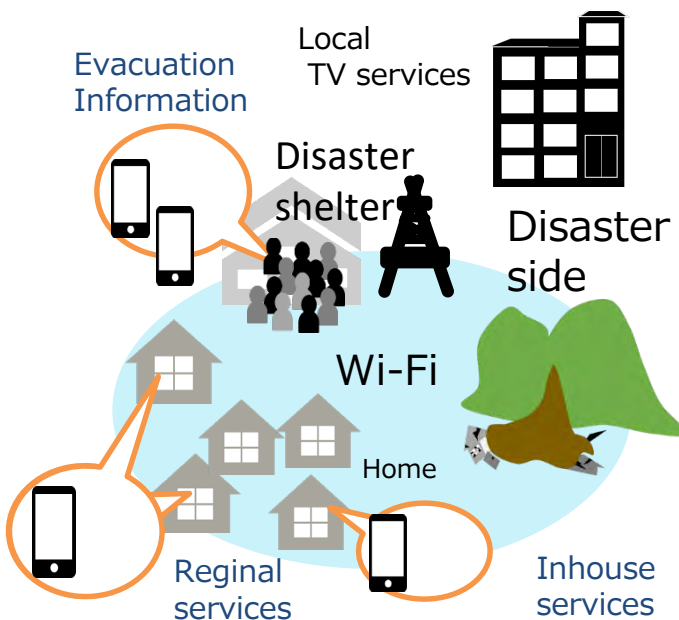
- 講師のスライドをスクリーンおよび各受講者に配信



ユースケース 8

ローカルTV放送 (DL)

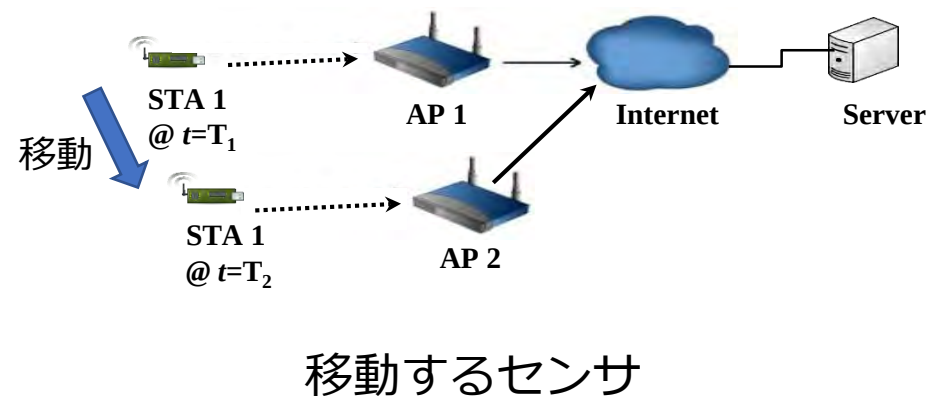
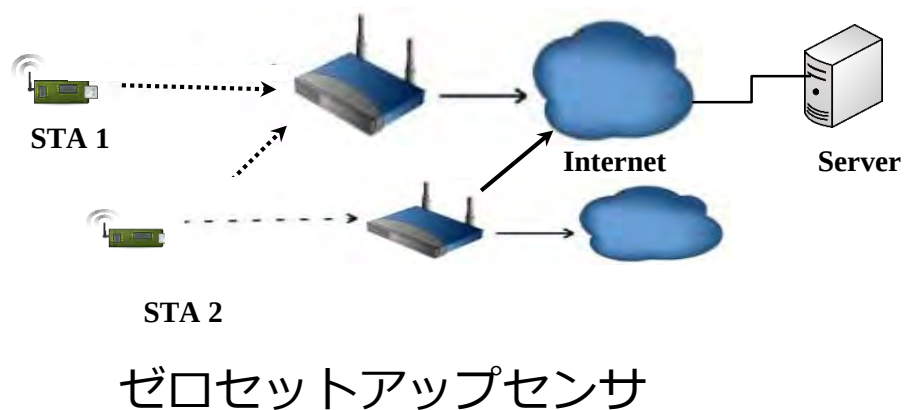
- 小規模なTV放送
- 災害時は避難情報などを放送



ユースケース9

センサデータアップロード (UL)

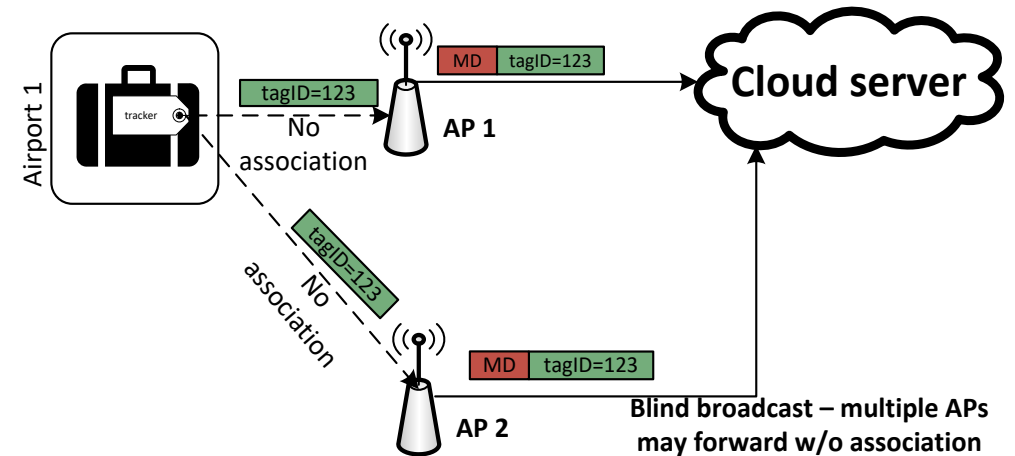
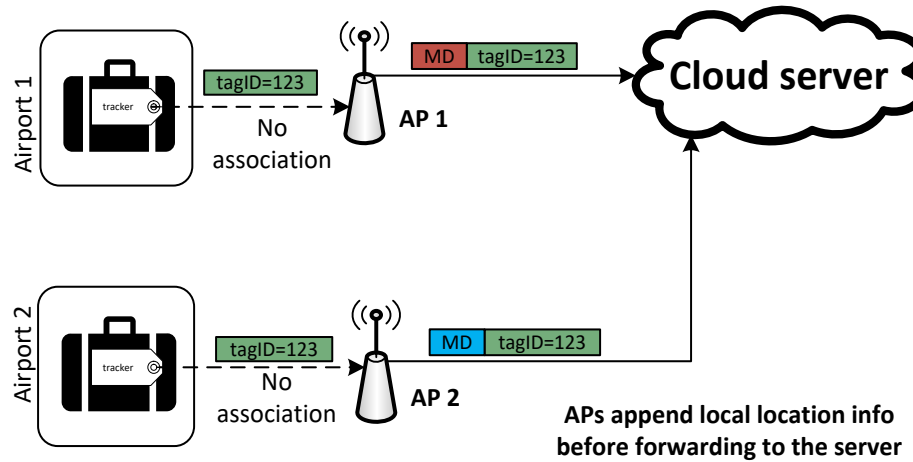
- アソシエーション無しでセンサのデータを上流にフォワード



ユースケース10

APタグ付けアップリンク転送 (UL)

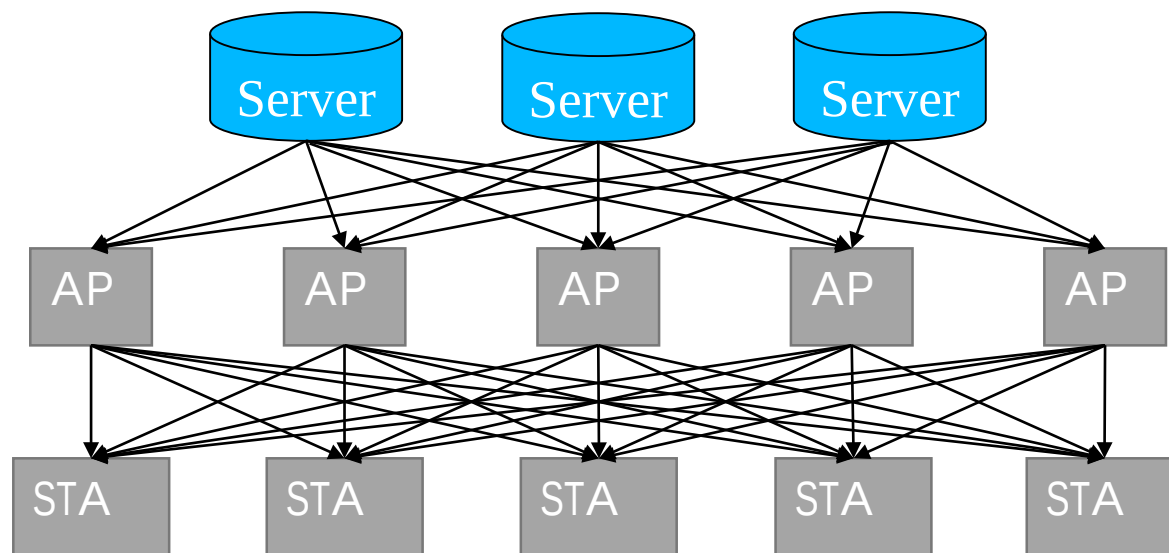
- アップリンクのデータにAPでタグ付け
- 荷物のトラッキング



想定しているシステム (DL)

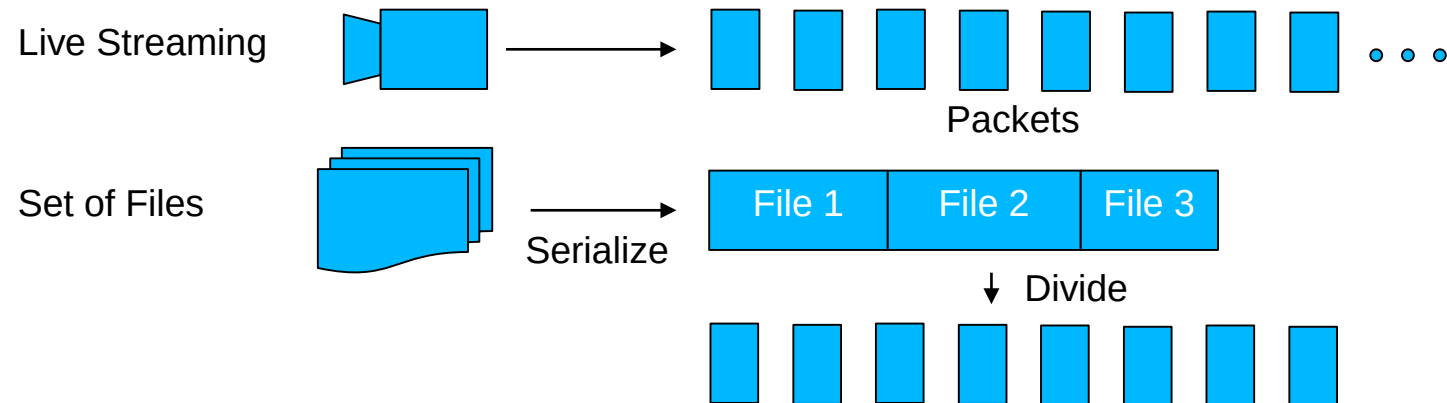
デバイス

- サーバ: コンテンツを配信する
- AP: eBCSフレームを送信する
- STA: eBCSフレームを受信し、ユーザにコンテンツを提供する



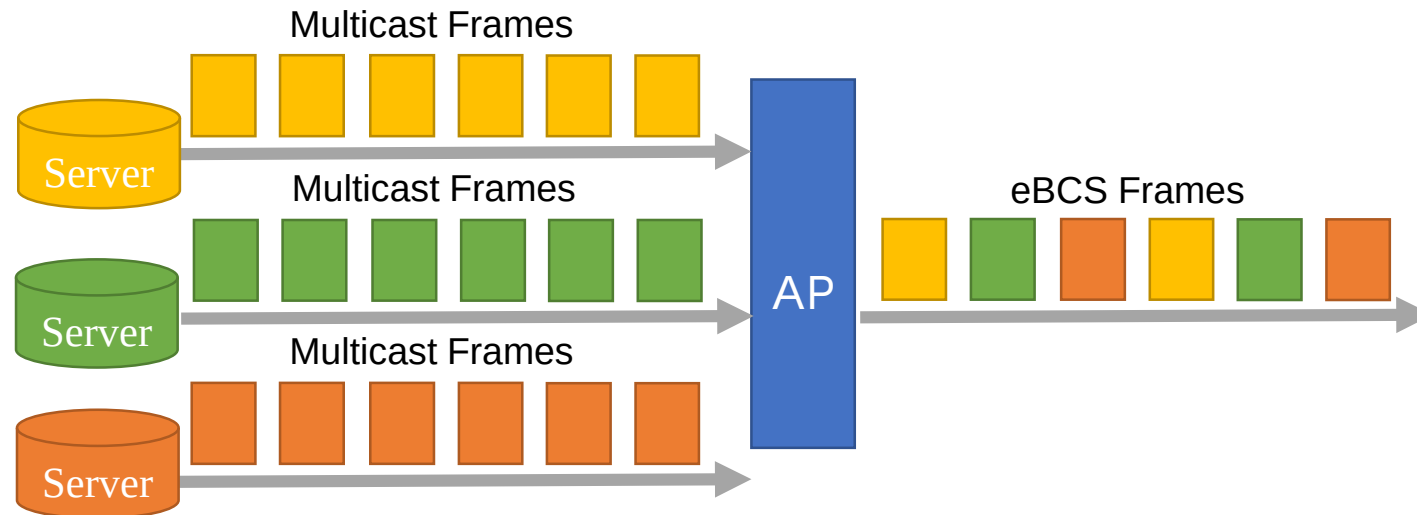
コンテンツ

- コンテンツはパケットのストリーム
 - ライブストリーミング
 - ファイルのセット (Webページ)
 - シリアルライズしてパケットに分割
- 各コンテンツはIDを持つ (IPアドレス・ポート, アプリケーション独自ID)



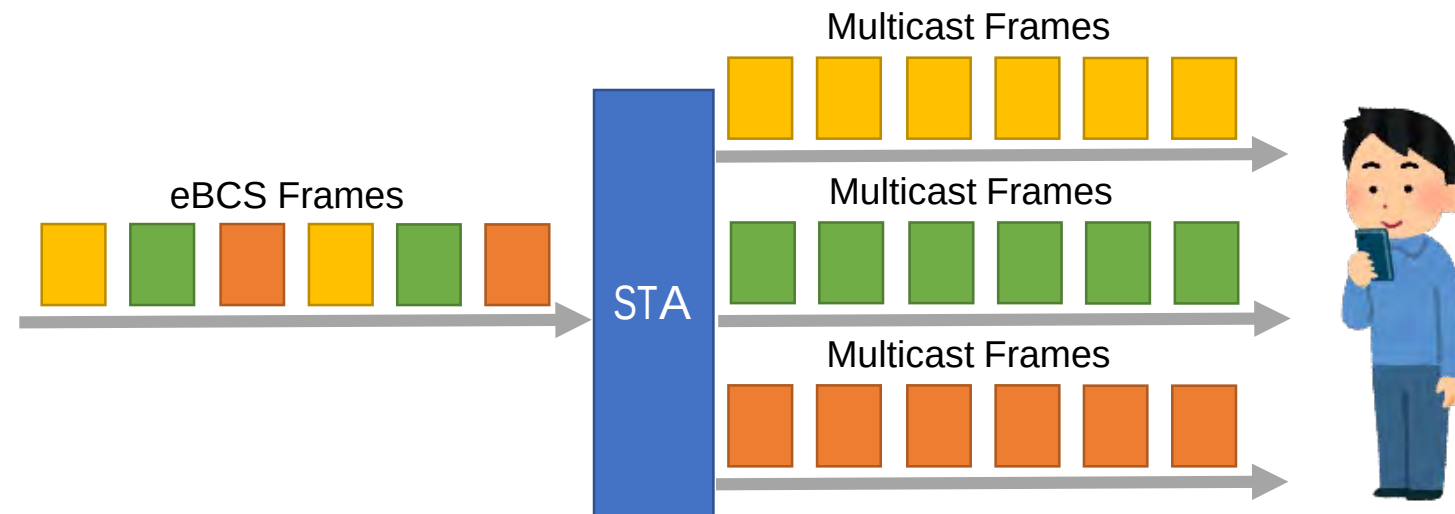
AP

- サーバから受信したパケットをeBCSフレームで送信する
 - 複数のコンテンツストリームを扱える
 - コンテンツのIDによってフィルタできる
 - 全てのコンテンツを対等に扱う
- 端末にコンテンツ情報(コンテンツID, 可読タイトルなど)を提供する



STA

- eBCSフレームを受信し、コンテンツを再構成する
- コンテンツをユーザに提供する
- 受信するコンテンツをユーザが選択する機能を提供する
- 同一コンテンツを複数のAPから受信できる
- 複数のコンテンツを単一・複数のAPから受信できる



必要となる機能

要求機能（抜粋）

- フレームの送信者を認証できること
- アソシエーションの有無に関わらず使用できること
- 端末は複数の放送サービスを同時に利用できること
- PHYは変更しないこと

現在のIEEE802.11での問題点

- アソシエーション
- 送信者認証

アソシエーション

- AP↔端末間で最低でも2往復のフレーム交換が必要
 - 端末もフレーム送信
- 接続端末数の上限2,007台/AP (プロトコル上の制限)
 - 実際は数百台程度 (かなり高性能なAP)
- セルサイズシミュレーション
 - アンテナ: 0dBi

Frequency	2.4 GHz		5.2 GHz	
TX Power	1 mW	10 mW	1 mW	10 mW
Distance (RX Power = -67dBm)	22 m	70 m	10 m	35 m
Cover Area	1,558 m ²	15,579 m ²	332 m ²	3,319 m ²

アソシエーションしない利点・欠点

- 端末がフレームを送信しなくてもよい
 - 帯域有効利用
 - 端末の消費電力低減
 - 端末のプライバシー確保
- 台数制限なし
- セキュリティネゴシエーションができない
 - Nonceを使った鍵生成ができない

IEEE 802.11 の現状の送信者認証

4.5.4.6 Data origin authenticity

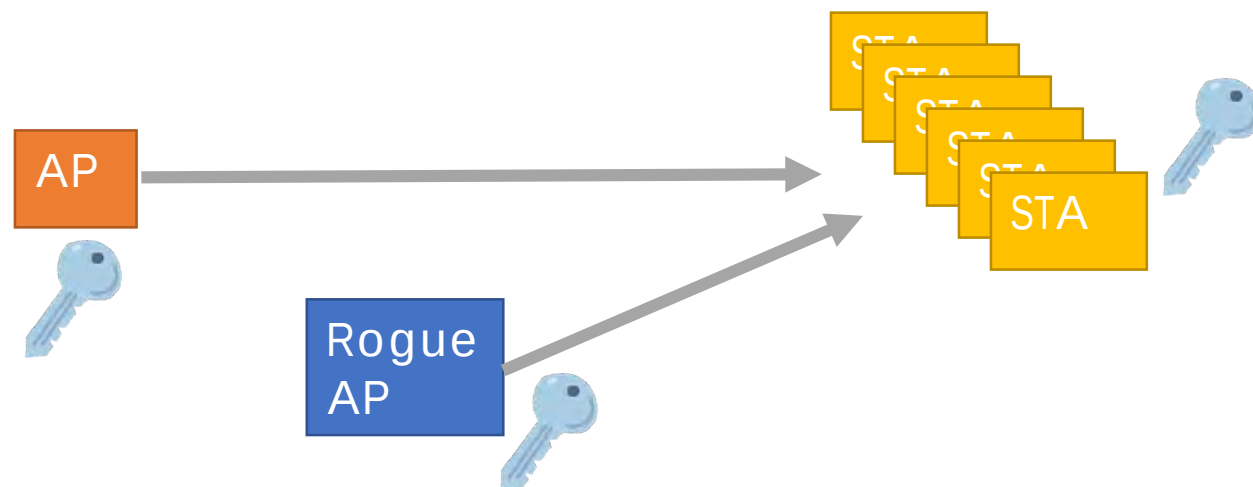
...

Data origin authenticity is applicable only to individually addressed Data frames, and individually addressed robust Management frames.

The protocols do not guarantee data origin authenticity for group addressed frames, as this cannot be accomplished using symmetric keys and public key methods are too computationally expensive.

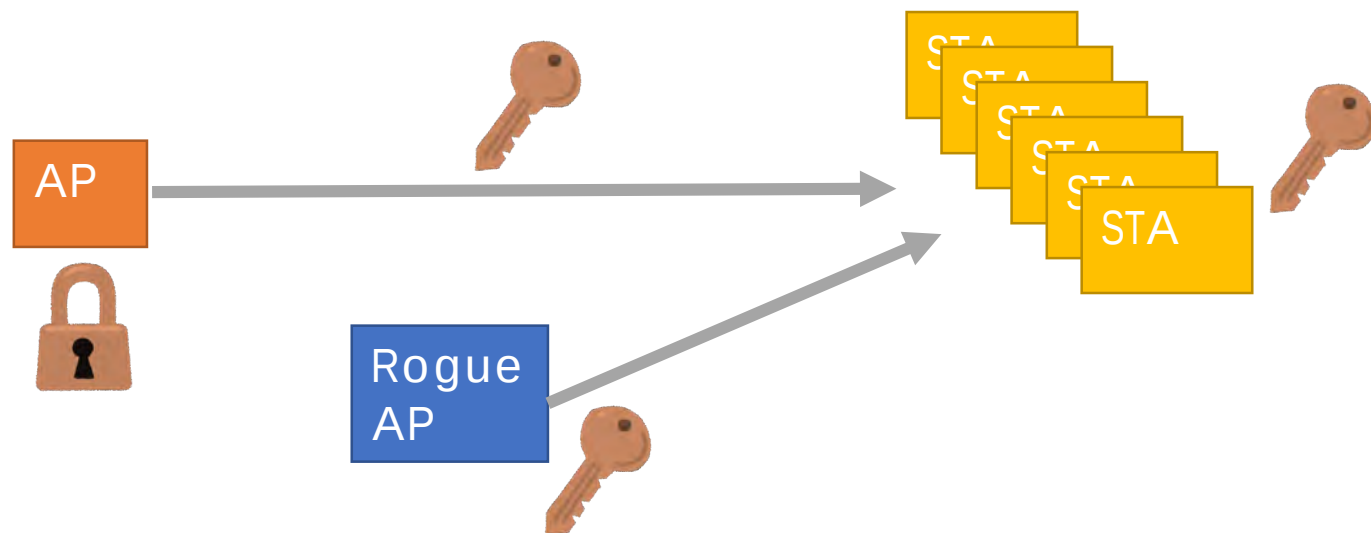
現状のブロードキャストの問題点

- GTKSA (Group Temporal Key Security Association)
- 対称アルゴリズム (AES)
- APおよびアソシエートしている端末すべてが同じ鍵を共有
- 悪意ある端末がAPになりすませる
- 全員が信用できる環境でないとセキュリティを確保できない



必要となるアルゴリズム

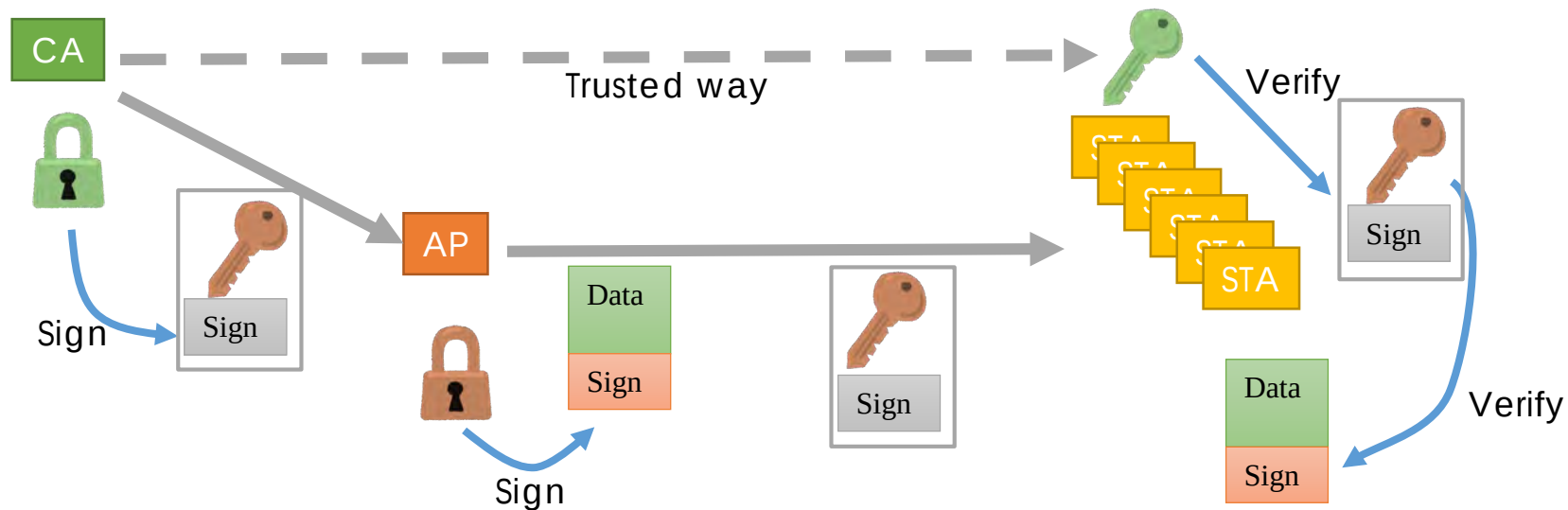
- **正規のAPのみ**がフレームに署名できる
- 端末が署名を検証できる



提案中の認証方式

Public Key Infrastructure

- 公開鍵アルゴリズム
 - 秘密鍵(署名用) と公開鍵(検証用)が別 (非対称アルゴリズム)
 - 秘密鍵で生成された署名は公開鍵でのみ検証可能
 - TLS, SSHなどで広く利用されている
- CA(認証局)の公開鍵はあらかじめ端末にインストール
- APの公開鍵はCAの秘密鍵で署名
- APは公開鍵と署名付きフレームを端末にブロードキャスト
- 端末はAPの公開鍵をCAの公開鍵で検証、フレームの署名をAPの公開鍵で検証



公開鍵アルゴリズムの欠点

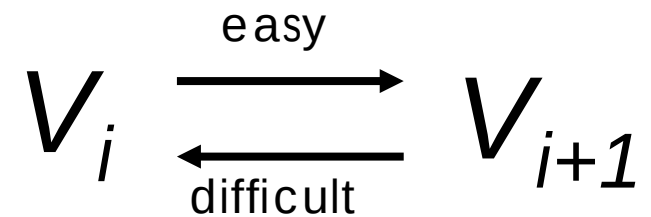
- 計算量が多い

	Intel Core i7 3.1GHz Linux		Intel Core i5 3.2GHz MacOS		AMD Turion II 2.2GHz FreeBSD		ARM Cortex-A7 1.1GHz Android	
	Sign	Verify	Sign	Verify	Sign	Verify	Sign	Verify
RSA 2048	2,651	77	2,502	72	6,580	188	94,073	2,460
RSA 4096	14,514	214	13,267	201	40,000	643	627,607	7,553
DSA L1024N160	225	426	206	390	599	1,098	7,274	13,942
DSA L2048N224	874	1,694	809	1,584	2,360	4,874	34,655	68,362
DSA L2048N256	873	1,695	799	1,548	2,436	4,702	39,672	77,262
DSA L3072N256	1746	3,496	1,605	3,173	4,896	9,674	84,727	169,804
ECDSA P256	37	91	33	87	138	247	5,027	14,792
ECDSA P384	4,459	8,588	4,324	8,560	17,160	35,719	94,448	184,409
ECDSA P521	8,321	16,538	8,147	16,479	35,759	49,511	190,014	360,304

μsec

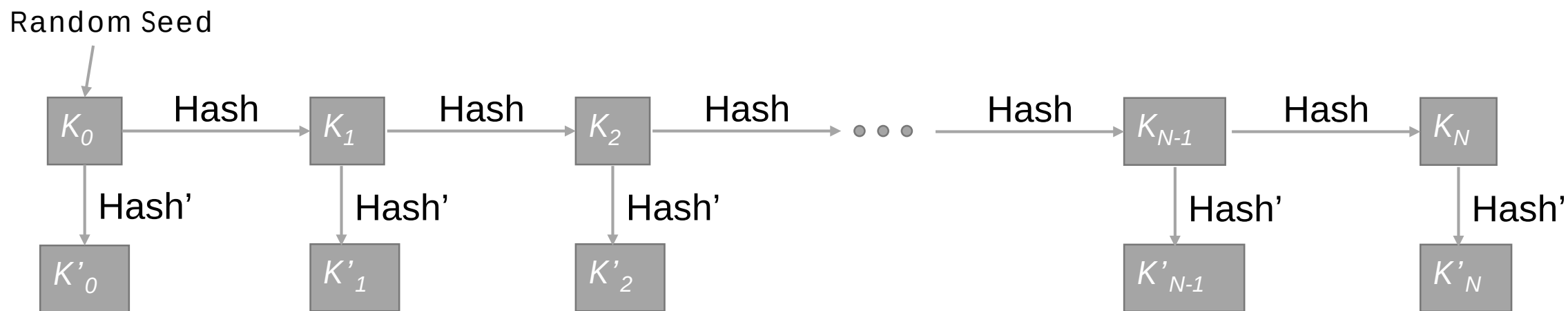
Timed Efficient Stream Loss-Tolerant Authentication (TESLA)

- ワンウェイキーチェーンの一種 (RFC4082)
- 少ない計算量でブロードキャスト・マルチキャスト通信におけるフレームごとの認証を実現可能
- ワンウェイキーチェーンはハッシュ関数の性質を利用
 - $V_{i+1} = \text{Hash}(V_i)$ の場合
 - V_i から V_{i+1} を計算するのは簡単
 - V_{i+1} から V_i を計算するのは困難(実質不可能)



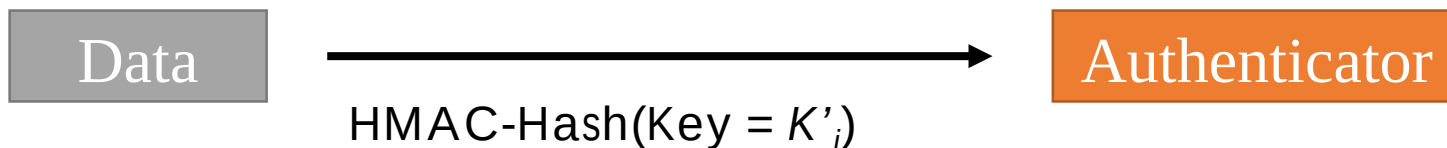
ワンウェイキーチェーン生成

- 送信者がハッシュ関数を使って一連の鍵を生成する

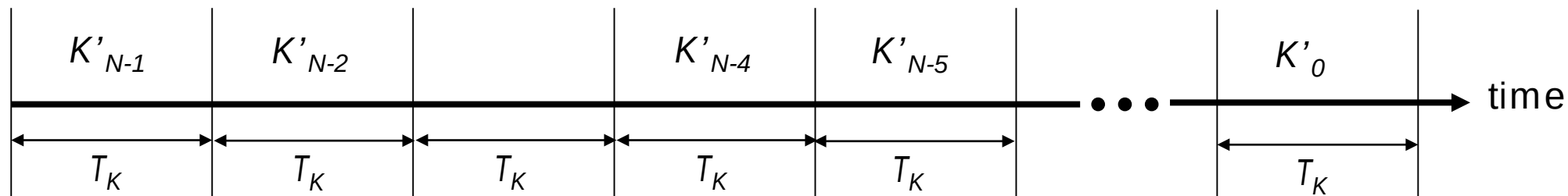


認証情報生成

- 送信者はHMACハッシュ関数を使って各フレームの認証情報を生成する

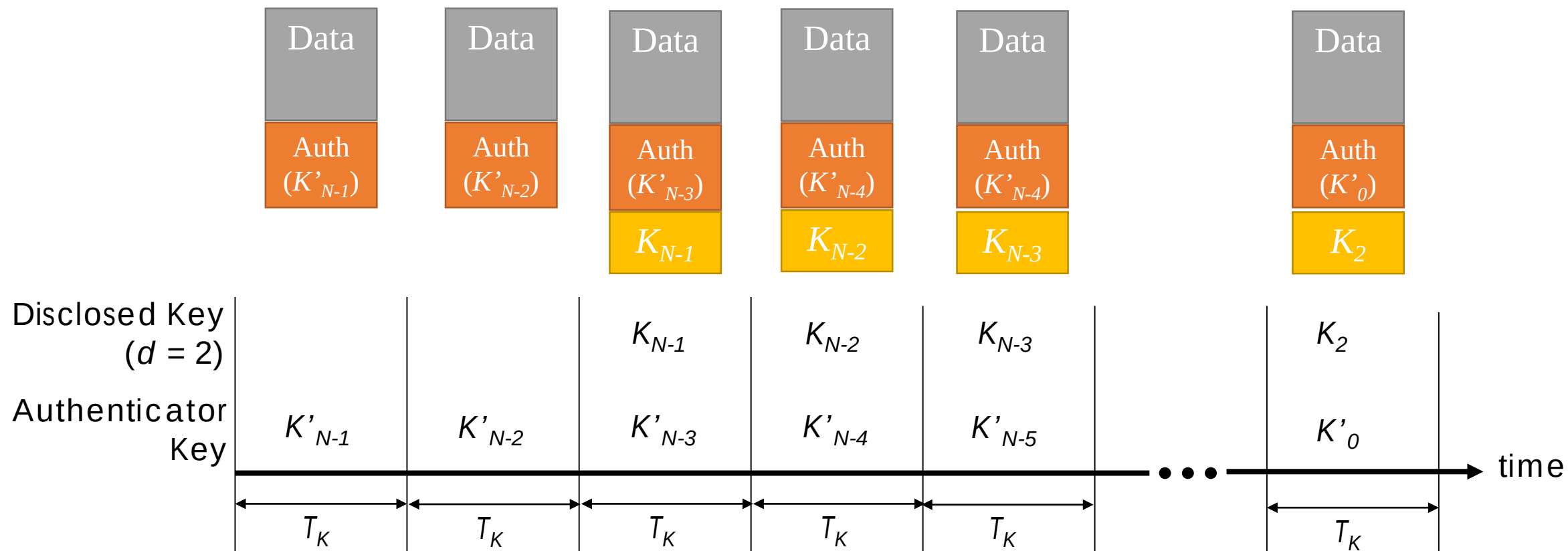


- 一定の時間 T_k で使用する鍵を切り替える
- 鍵は生成時とは逆順で使用する



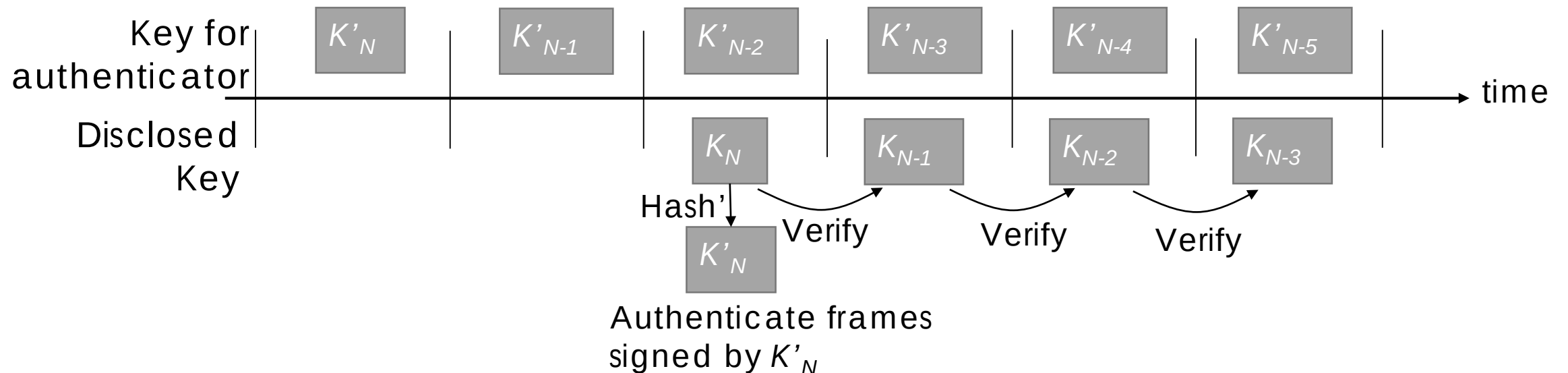
鍵開示

- 送信者は $d * T_k$ ($d \geq 2$) 後に鍵を開示する



フレーム認証

- 受信者は鍵が開示されるまでフレームをバッファ
- 開示された鍵は次のように検証する
 - K_i が検証済みで $\text{Hash}(K_{i-1}) = K_i$ ならば K_{i-1} は正しい
- 開示された鍵から生成した認証鍵でバッファしていたフレームを認証する



フレームシーケンス

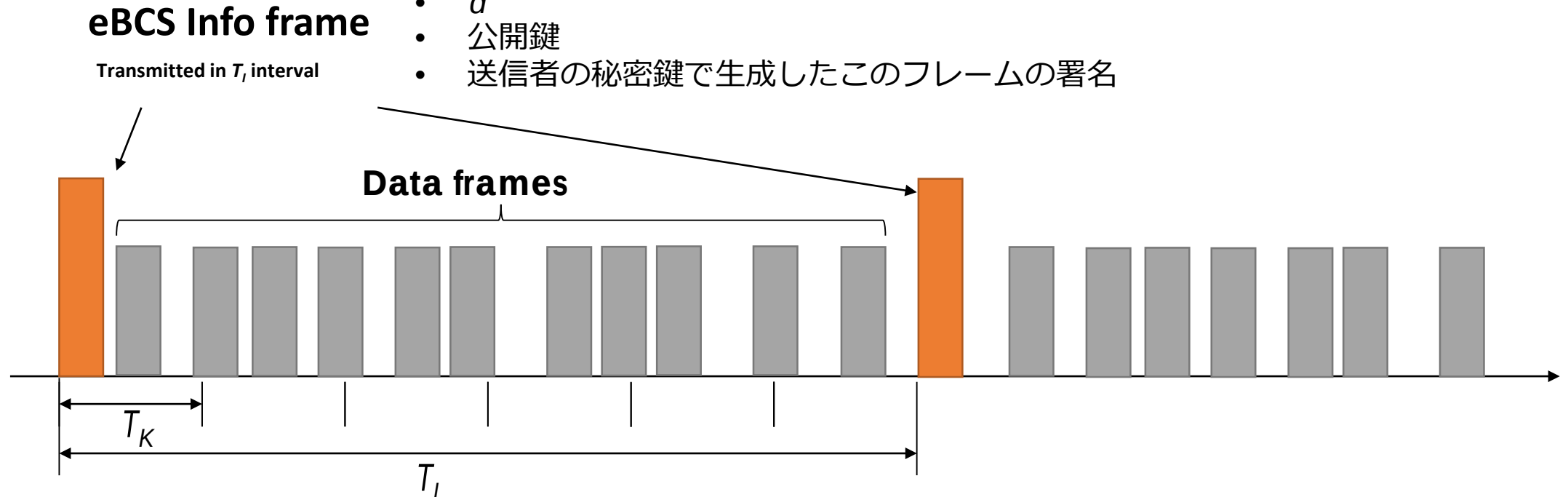
送信者はeBCS Infoフレーム送信前にキーチェーンを生成する
($K_{s,N}, K_{s,N-1}, K_{s,N-2}, \dots, K_{s,0}$)

eBCS Infoフレーム

- eBCS Info シーケンス番号
- $K_{s,N}$ (s : eBCS Infoシーケンス番号)
- $K_{s-1,L}$ (L : 最後に使用した鍵のインデックス)
- $K_{s-1,L+1}$ ($d = 2$ の場合)
- タイムスタンプ
- T_I
- T_K
- d
- 公開鍵
- 送信者の秘密鍵で生成したこのフレームの署名

eBCS Data フレーム

- データ
- $K_{s,i+2}$
- $A_{s,i}$ ($K'_{s,i}$ で生成された認証情報)
- 鍵のインデックス: i
- eBCS Infoシーケンス番号: s

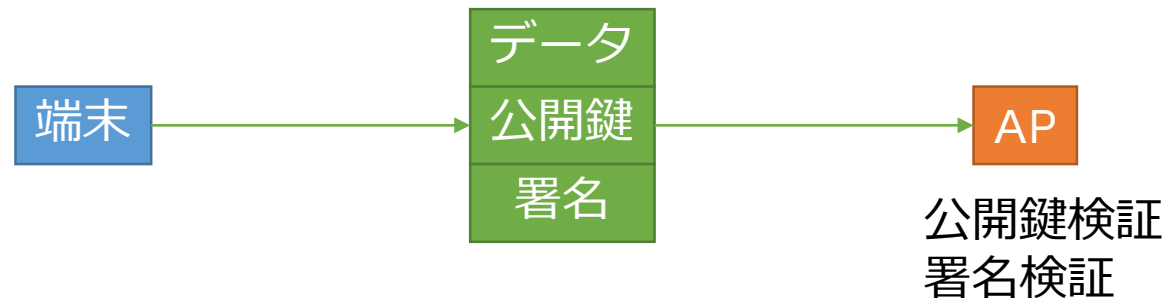


遅延を避けたい場合のオプション

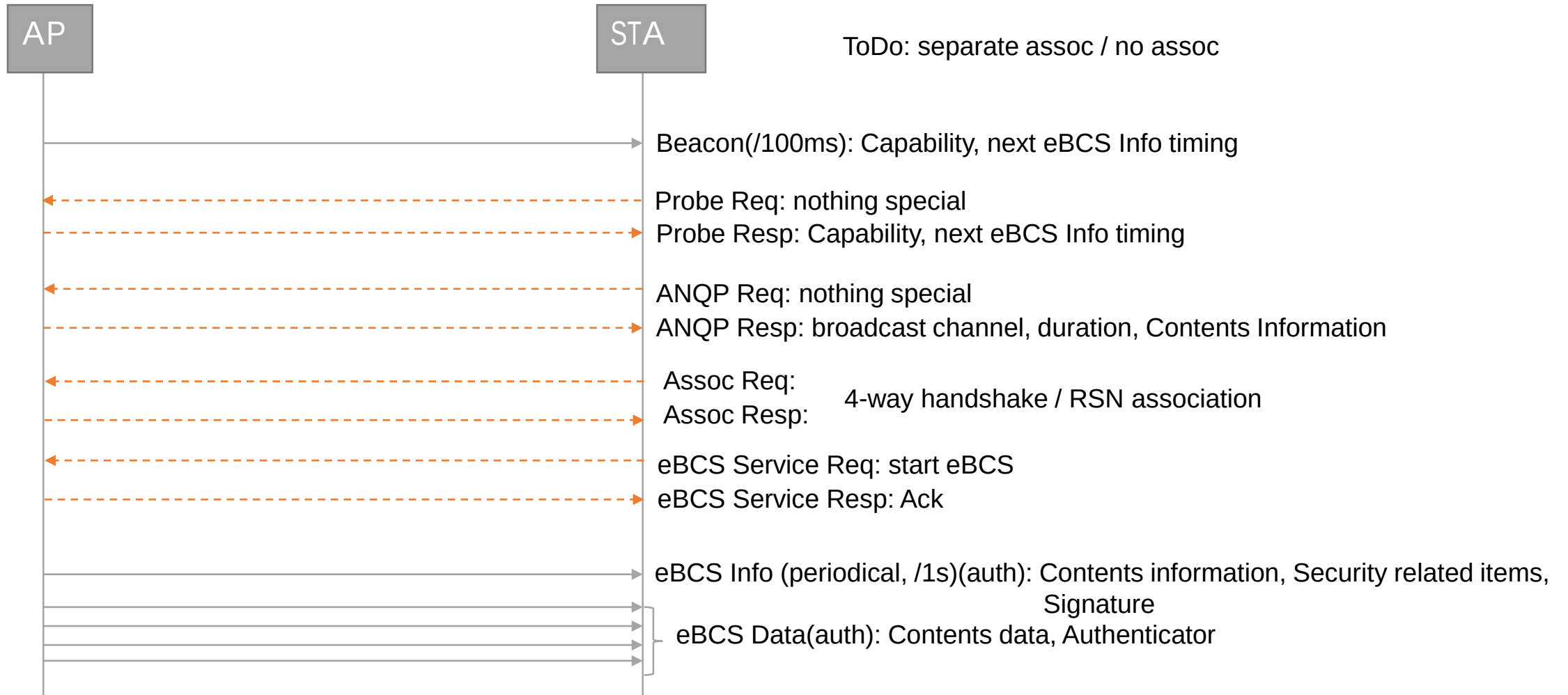
- TESLAでは最低でも $d * T_k$ の遅延が発生する
- 遅延を避けたい場合のためにすべてのフレームで公開鍵アルゴリズムを使用するオプションを用意する
- この場合、送信者・受信者ともに大量の計算が必要になることに留意する必要がある
- IEEE 802.11レイヤでは認証を行わず、上位レイヤで認証する。
 - 上位レイヤでの認証は必須。

ULでの認証

- 想定されるデータの性質
 - 散発的
 - データは小さい
- 公開鍵のみで認証



Downlink Frame Sequences



TGbc スケジュール

- January 2019 First meeting as a task group
- September 2020 Initial WGLB (D1.0)
- March 2021 D2.0 WGLB Recirculation LB
- September 2021 Form SB Pool
- September 2021 MEC/MDR done
- November 2021 Initial SB
- March 2021 Recirculation SB
- May 2022 Final WG/EC approval
- July 2022 Revcom/SASB approval