ICTビジネス戦略セミナー 「デジュール及びフォーラムの最新標準化動向と今後の取組」

IETFが策定する国際化技術とそれらを活用するIoT技術

2020/01/29(水)

根本 貴弘

国立大学法人東京農工大学

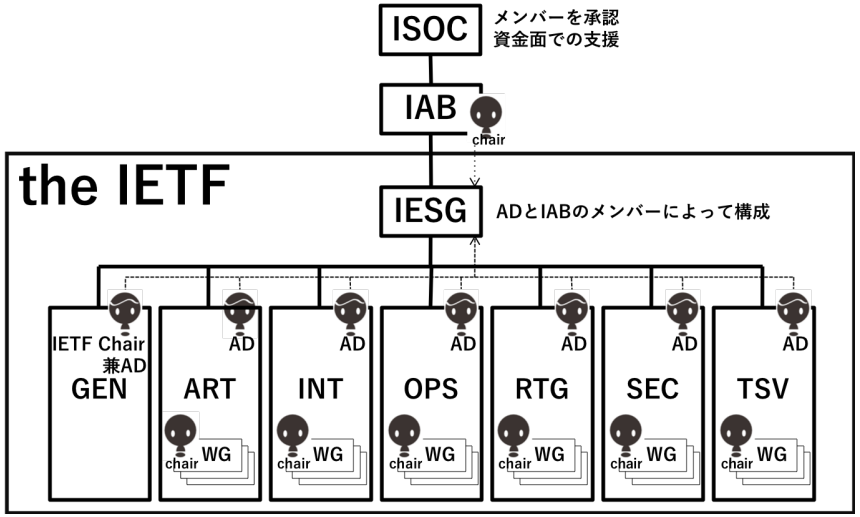
目次

- **IETF**及び**IETF**における**IoT**関連技術の外観
- **IETF**における**IoT**サービスディスカバリ
- **i18n**の観点からみたサービスディスカバリの課題
- まとめと今後の展望

IETF及びIETFにおけるIoT関連技術の外観

IETF概要

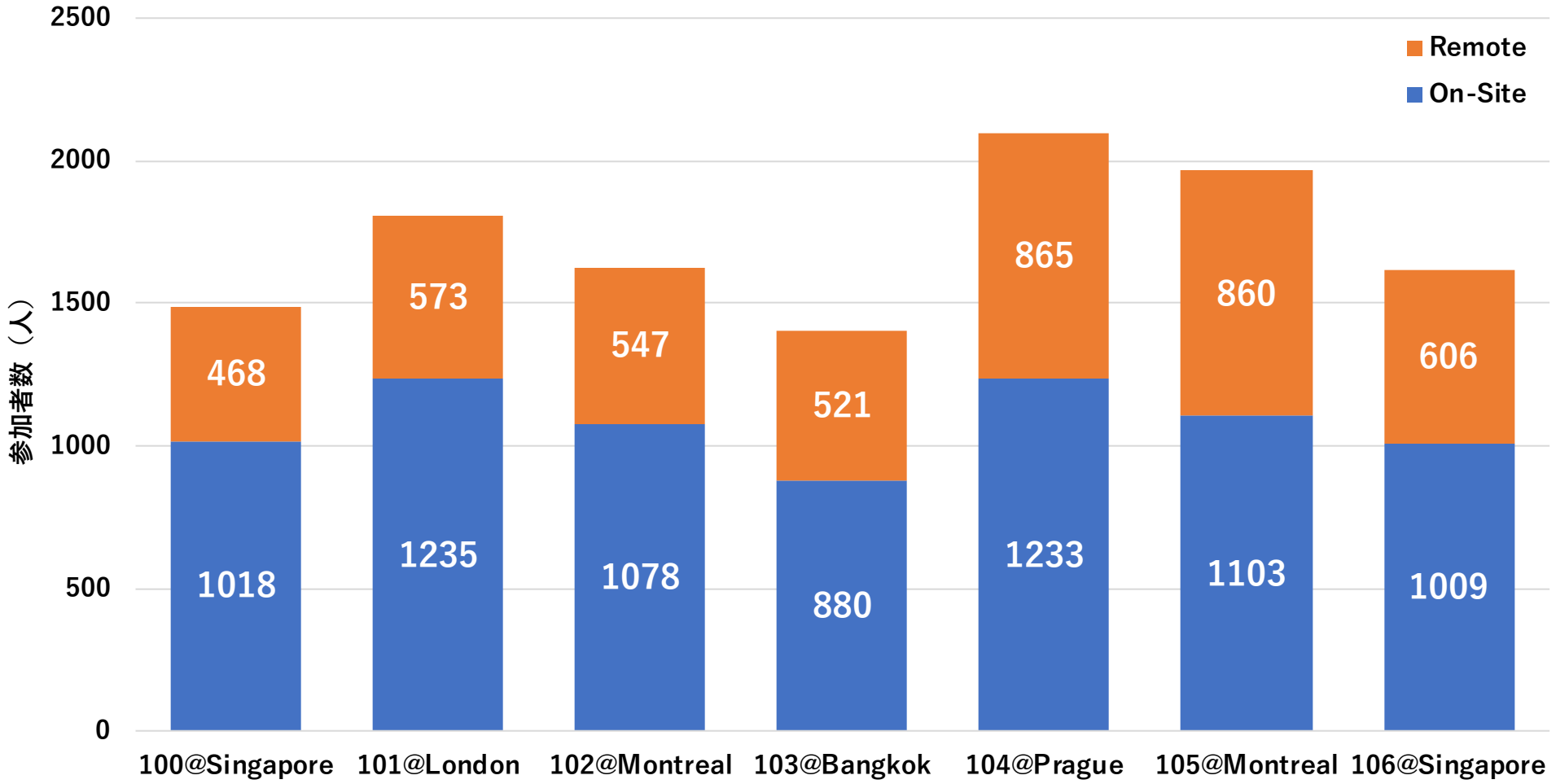
- **Internet Engineering Task Force (IETF)**
  - インターネット技術に係る技術標準としての**Request for Comments (RFC)**の仕様策定のプロセスに責任を持つ団体
  - 技術的な内容及び作業に係る責任は**Internet Engineering Steering Group (IESG)**が担う
  - **Internet Architecture Board (IAB)**のタスクフォースの一つであり，**IAB**が定めるインターネットの標準化プロセスの方針に従い活動を行う
  - **IAB**の上位組織の**Internet Society (ISOC)**は資金面での支援
- 代表的な**RFC**例
  - **IP (RFC791), TCP (RFC793), DNS (RFC1034, RFC1035)**．．．
- **IETF**の標準化過程に関する情報は全て公開
- **IETF**での標準化作業は，年**3**回開催される**IETF**会合中の**WG**会合や**WG**のメーリングリストでの議論を通じて行う



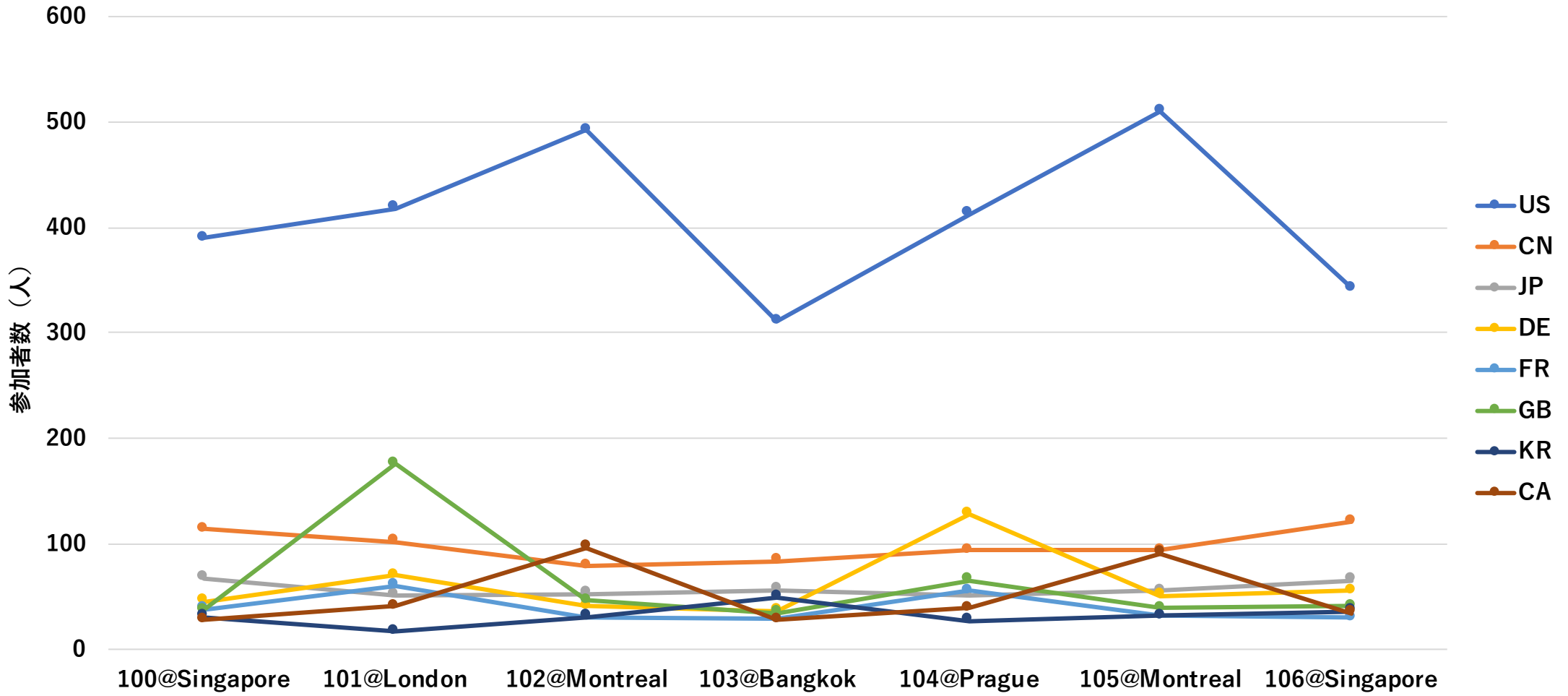
IETF Areas

GEN	• General(統括的技術分野)
ART	• Applications and Real Time(応用・リアルタイム分野)
INT	• Internet(インターネット分野)
OPS	• Operations & Management(運用管理分野)
RTG	• Routing(ルーティング分野)
SEC	• Security(セキュリティ分野)
TSV	• Transport and Services(トランスポート分野)

近年のIETF会合開催規模

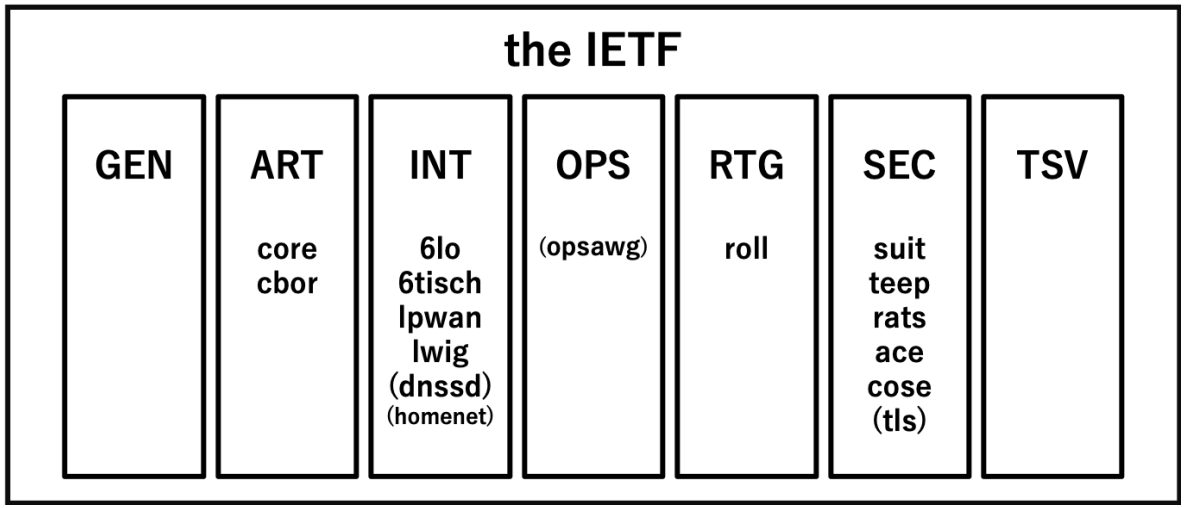


IETF会合現地参加者数の国別推移



IETFにおけるInternt of Things(IoT)

- **IETF**が想定する**IoT**環境
  - バッテリーの駆動時間や**CPU**の処理能力，メモリ量，通信速度等が制限された環境
  - 想定する主なデバイス（**Constrained Device**）性能
    - **RAM:**～**10KiB**，**ROM:** ～**100KiB**（**RFC 7728**にて，**Class1**として定義）
- **Constrained**な環境で動作するためのプロトコルの標準化
  - **XML/EXI -> JSON/CBOR**
  - **HTTP -> CoAP**
  - **TLS -> DTLS**
  - **TCP -> UDP**
  - **IPv6 -> 6LoWPAN**



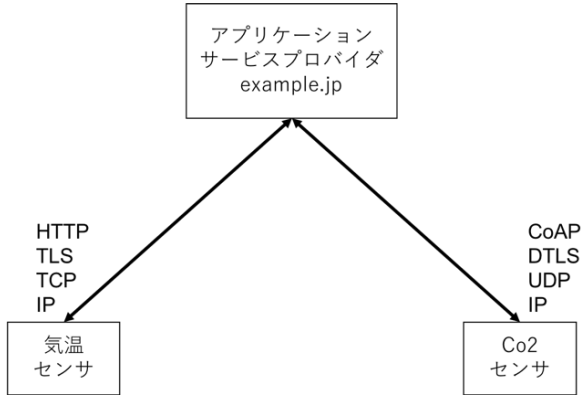
IETF106で開催されたIoT関連技術Working Group（WG）

IoT関連技術WG抜粋

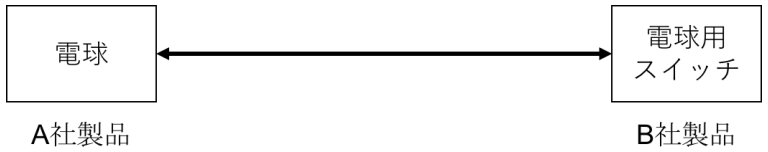
Area	WG	Name	概要
ART	core	Constrained RESTful Environments	制限された環境下でのRESTfulアクセス可能なアプリケーション技術について検討．CoAP（RFC 7252）等を策定
	cbor	Concise Binary Object Representation Maintenance and Extensions	JSONベースのバイナリフォーマット等について検討
INT	6lo	IPv6 over Networks of Resource-constrained Nodes	リソースに制限があるノードで構成されたネットワークでIPv6を使用するための手法について検討．6Lowpan WGの後継
	6tisch	IPv6 over the TSCH mode of IEEE 802.15.4e	IEEE 802.15.4eのTSCHモードでIPv6ネットワークを構築する方法等を検討
	lpwan	IPv6 over Low Power Wide-Area Networks	広域かつ低消費電力のネットワーク実現に向けたIPv6向けプロトコルについて検討
	lwig	Light-Weight Implementation Guidance	リソースに制限がある機器に対するプロトコル実装ガイダンスを検討
	dnssd	Extensions for Scalable DNS Service Discovery	DNSを使ったサービスディスカバリとその拡張手法について検討．mDNS（RFC 6762），DNS-SD（RFC 6763）を基に，複数ネットワークセグメントへの対応を検討
OPS	opsawg	Operations and Management Area Working Group	OSP Area全体に関わるWG．その一部として，Constrained Devicesが関わるネットワークの問題や要件の整理，そのユースケースについて議論
RTG	roll	Routing Over Low power and Lossy networks	リソースに制限があるノードで構成されたネットワークにおけるルーティング手法を検討
SEC	suit	Software Updates for Internet of Things	IoT機器の安全なファームウェアの更新手法について検討．デ ジタル署名を付与可能なファームウェアのメタデータに関するフォーマット等の定義等
	teep	Trusted Execution Environment Provisioning	信頼できる実行環境（Trusted Execution Environment (TEE)）でのアプリケーションのライフサイクル管理（インストール・実行・削除）のプロトコルについて検討
	rats	Remote ATtestation ProcedureS	あるエンティティがIoT機器等のシステムコンポーネントを利用する際，その正当性を検証する仕組みについて検討
	ace	Authentication and Authorization for Constrained Environments	制限された制限された環境下での認証・認可の方式について検討
	cose	CBOR Object Signing and Encryption	CBORを利用したデジタル署名等のフォーマット等，CBORの拡張方式について検討

IoT機器の通信パターン例

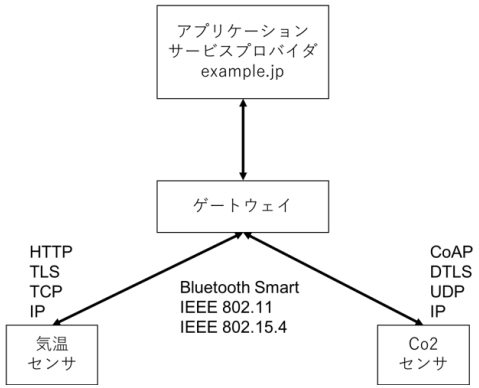
- **RFC7452: Architectural Considerations in Smart Object Networking**にて，**IoT**機器の通信パターンの例が紹介



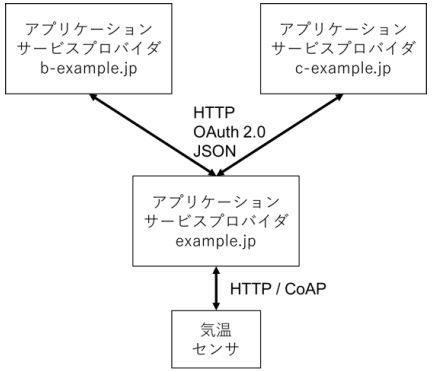
IoT機器とクラウド間の通信



IoT機器同士の通信



IoT機器とゲートウェイ間の通信



バックエンドでのデータ共有の通信

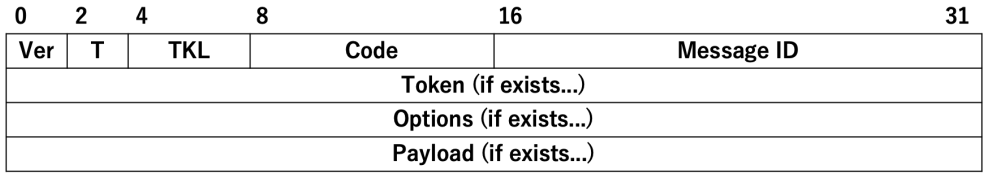
IETFにおけるIoTサービスディスカバリ

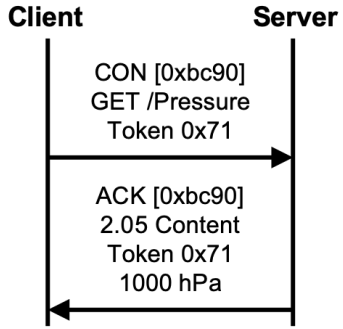
core WG (1/3)

- **WG**概要
  - **IoT**デバイスのように，バッテリーの駆動時間や**CPU**の処理能力，メモリ量，無線通信速度等が制限された環境下で，必要な情報を効率的に交換を行うための**RESTful**アクセス可能なアプリケーション技術の標準化を策定している**WG**
- **RFC7252：The Constrained Application Protocol (CoAP)**が主要プロトコル
  - **HTTP**や**TLS**を利用できる性能を持たない機器に対して**RESTful**アクセスを実現
  - **UDP**ベースの非同期通信
  - コンパクトなワイヤーフォーマット
  - **URI**及びメディアタイプのサポート
  - プロキシ及びキャッシング機能

[URI]
coap://a.example.jp/light
coaps://a.example.jp/light

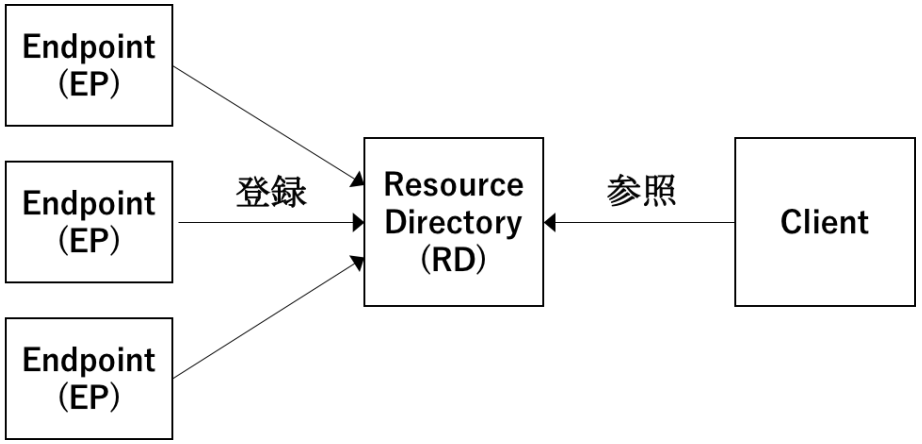
[デフォルトポート番号]
coap: 5683
coaps: 5684





core WG (2/3)

- **draft-ietf-core-resource-directory-23：CoRE Resource Directory**
  - スリープ状態のノードや分散ネットワーク等の制限のある環境下における
    直接機器を見つけることが困難な機器を発見可能とする方法の提案
    - **Endpoint(EP)**機器のリソース情報を**Resource Directory(RD)**サーバに登録し，クライアント端末からの参照（**UTF-8**が使用可能）
    - **CoAP**の**Well-Known URI**「**/.well-known/core**」を使いクライアント端末から**RD**サーバに**GET**リクエストを行う



core WG (3/3)

- **draft-ietf-core-rd-dns-sd-05：CoRE Resource Directory: DNS-SD mapping**
  - 既存の**DNS**インフラストラクチャを使用してサブドメイン内の**CoAP**サーバ等のサービスを検索するための**PTR**及び**SRV**，**TXT RR**の記述方法を定義する提案
  - **CoRE Resource Directory**と補完的な関係にある
  - **CoRE Resource Directory**で定義されるリソース情報を**DNS-SD**のサービス名にマッピングを行う

DNS-SDサービス名　＝　<Instance>. <Service>. <Domain>
↑ 「ins」属性　↑ 「rt」属性　↑ 「d」属性　マッピング

dnssd WG (1/3)

- **WG**概要
  - **RFC6763**：**DNS-Based Service Discovery (DNS-SD)**の拡張を行う**WG**
  - **DNS-SD** では，**RFC6762**：**mDNS**を使用し，**IP**アドレスやホスト名を知らなくても同一ネットワークセグメント内のサービスを発見する手法標準化しており，これを複数のネットワークセグメントに拡張するための手法が検討されている
- **mDNS**
  - 「ホスト名**.local**」の名前解決をするとホストの**IP**を引ける
  - ホスト名には，**UTF-8**が使用可能
- **DNS-SD**
  - **DNS**を使ってサービスを特定するためのドメイン名の構造を定義「**<Instance> . <Service> . <Domain>** 」
  - サービスに対応するサービスインスタンス名を**PTR**レコードに記述し，サービスへのアクセスには**SRV RR**を使用する
    - **example.jp**の**http**サービスは「**_http._tcp.example.jp**」，
    - 「**_http._tcp.example.jp RTP OfficialWebPage._http._tcp.example.jp.**」とすると，
    - 「**OfficialWebPage._http._tcp.example.jp SRV 0 100 80 www.example.jp.**」が返される

dnssd WG (2/3)

- **mDNS＋DNS-SD**
  - 同一ネットワークセグメント内において，サービスの発見を実現
    - プリントサービスを発見したい場合，「**_ipp._tcp.local**」としてプリントサービスを探す
- 複数ネットワークセグメントへの対応
  - **draft-ietf-dnssd-hybrid-08：Discovery Proxy for Multicast DNS-Based Service Discovery**
    - ネットワークセグメント毎にドメイン名を用意し，**DNS**及び**mDNS**プロキシとしての機能をディスカバリプロキシとしてルータに追加する提案
      - ネットワークセグメント**A**からネットワークセグメント**B**のサービスを使用する場合，「**_ipp._tcp.netB.example.jp**」というクエリをディスカバリプロキシが受信
      - クエリをネットワークセグメント**B**に対して「**_ipp._tcp.local**」クエリを送信
      - その応答クエリをネットワークセグメント**A**に返す
    - 米**Apple**社では既に実装が行われている

dnssd WG (3/3)

- その他の議論
  - **draft-cheshire-dnssd-roadmap-03：Service Discovery Road Map**
    - **DNS**ベースのサービスの整理とその情報提供
    - **DNS**ベースのサービスと**dnssd**の取り組みの関係がわかるようする方針で修正し**WG I-D**とする
  - **draft-ietf-dnssd-push-25：DNS Push Notifications**
    - **DNS**プッシュ通知の提案
    - レコード情報の頻繁な更新に対応するために，レコード情報の更新時にサーバからクライアントに対してその変更を通知する仕組み
    - **Github**や**apple.com**等で実装が公開されている
  - **draft-ietf-dnssd-privacy-05：Privacy Extensions for DNS-SD**
    - **DNS-SD**におけるプバイバシー問題解決方法の提案
    - **mDNS**では対応する全てのホストが応答するためプバイバシー上の問題がある
    - 許可されたホスト間のみで名前解決として許可されたホストグループのみが持つ共有鍵を使い**mDNS**のメッセージを暗号化するという方法が提案されたが採用に至らず
    - 何かしらの方法で暗号化したホスト情報をサーバに登録し，復号方法を知っている端末のみ名前解決する方法について検討することとなった
    - **WG LC**まで行ったがまとまらず， **draft-ietf-dnssd-prireq-03： DNS-SD Privacy and Security Requirements**としてサービスディスカバリに求められる要件定義から仕切り直し中

homenet WG

- **WG**概要
  - **homenet WG**では，**IPv6**環境をはじめとした次世代家庭用ネットワークに関する様々な技術について議論を行う**WG**
    - 企業や大学等の管理されたネットワークと比べて，ネットワーク運用者がいない比較的小規模な私的ネットワークでの利用を想定
    - プライベート用，ゲスト用といった複数セグメントを持つネットワークも想定
    - **RFC8375**：**Special-Use Domain ‘home.arpa.’** で，**Homenet**を示す予約済みドメイン名は「**home.arpa**」が定義
    - リンク名は**RFC7788**：**Home Networking Control Protocol**の**HNCP**によって機械的に生成された文字列を使用
- **draft-ietf-homenet-simple-naming-03**：**Homenet Naming and Service Discovery Architecture**
  - **Homenet**上のサービス名とサービスディスカバリ方法の提案
  - 名前の登録に**dnssd WG**の**draft-sctl-service-registration-02**：**Service Registration Protocol for DNS-Based Service Discovery**の利用し動的に**DNS**レコードを更新
  - 名前解決は，ローカルなサービスについては**mDNS**及び**DNS-SD**を使用，それ以外では**ISP**のフルリゾルバを使用
- 市場に受け入れられる仕様にすることが今後の課題

i18nの観点からみたサービスディスカバリの課題

IETFにおけるi18n

- **i18n = internationalization**，国際化技術
- **ASCII**文字集合の範囲外の文字を含む識別子の利用を可能とする技術
- **IETF**では，**ASCII**文字集合の範囲外の文字として**Unicode/UTF-8**を利用することを前提に標準化を行っている
- 識別子の国際化を実現するために検討すべき課題は多々ある
  - プロトコルで利用可能な文字の分類
  - 視覚的に紛らわしい文字の扱い
  - **bidi**文字列の扱い
  - **Unicode**の改版への追従方法

項目	例	
文字種（大文字・小文字）	A (U+0041)	a (U+0061)
文字幅（全角・半角）	ｱ (U+FF71)	ア (U+30A2)
合成済文字・結合文字列	ガ (U+30AB U+3099)	ガ (U+30AC)
文脈依存文字	σ (U+03C3)	ς (U+03C2)
言語依存文字	İ (U+0130)	i (U+0069)

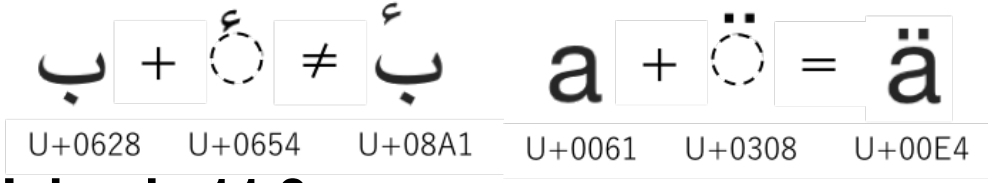
- 国際化技術に関する文書のレビューを行える専門家が少なく，国際化技術に関する課題解決に遅れが生じている
  - **draft-klensin-idna-unicode-review-05**として，**IDNA**に関する**Unicode**更新のためのレビュー枠組みを作ろうという取り組みが行われている

IETFが取り組んできた国際化技術における標準

- **Multipurpose Internet Mail Extensions (MIME)**
  - 電子メールや**HTML**の本文で**ASCII**文字集合以外の文字が扱うことが可能
  - **RFC2045**，**RFC2046**，**RFC2047**，**RFC2048(**現**RFC4288**，**RFC4289)**，**RFC 2049**
- **Internationalizing Domain Names in Applications (IDNA)**
  - 国際化ドメイン名（**IDNA2003**と**IDNA2008**がある）
  - **IDNA2003**：**RFC3490**，**RFC3491**，**RFC3492**
  - **IDNA2008**：**RFC5890**，**RFC5891**，**RFC5892**，**RFC5893**，**RFC5895**
- **Email Address Internationalization (EAI)**
  - 国際化電子メールアドレス
  - **RFC6530**，**RFC6531**，**RFC6532**，**RFC6533**，**RFC6855**，**RFC6856**，**RFC6857**，**RFC6858**
- **Stringprep**
  - 国際化文字列を扱うための枠組み
  - **RFC3454**
- **PRECIS Framework**
  - **Stringprep**に変わる国際化文字列を扱うための枠組み
  - **RFC8264**，**RFC8265**，**RFC8266**，**RFC6885**，**RFC7790**

i18n関連の課題：Unicode 7.0.0以降への対応

- **IANA**が**Uniocde 7.0**以降の**Uniocde**のバージョンの国際化ドメイン名及び**PRECIS Framework**のプロパティ情報を更新しないとしたことにより，**IETF**で策定された主要な国際化技術が**Uniocde 7.0**以降の文字集合に対応できない問題が起きている
  - **Uniocde 7.0**にて新たに収録された**ARABIC LETTER BEH WITH HAMZA ABOVE (U+08A1)** が等価とみなすべき文字コードのプロパティに等価性を示す情報が記載されていない（**NFC**により合成されない）
  - **Unicode 11.0**でも問題が継続している



- **draft-faltstrom-unicode11-05：IDNA2008 and Unicode 11.0**
  - **Unicode 6.3**と**Unicode 11.0**における**IDNA2008**のプロパティ情報の差分について報告
    - プロパティ情報に変更があったグルジア語や**Unicode7.0**以降に追加されたソヨンボ文字，シャーラダー文字等のプロパティ情報の差分は既存サービスへの影響はない
  - 問題があるのは**U+08A1**のみ
  - この**1**文字のために国際化技術の更新が行えないことは問題であるとし．**IDNA2008**の**Unicode 11.0**対応を目指し，**draft-faltstrom-unicode11-08**を**RFC**化する方針となった
  - **IDNA Rules and Derived Property Values**は**Unicode 11.0**に対応完了

i18nの観点からみたサービスディスカバリの課題 **(1/2)**

- サービスインスタンス名を構成するホスト名には，**UTF-8**が使用可能
  - 利用者が任意に決めた文字列が識別子として利用可能
- **UTF-8**が使用可能である一方で**i18n**に関する検討が乏しい
  - **dns-sd, homenet-simple-naming**
    - **RFC5198**の**Net-Unicode**に従い， **0x00-0x1F**及び**0x7F**の**ASCII**制御文字を禁止にする程度
    - 文字列の正規化等は行われないため，合成済み文字や結合文字列等の見かけ上同じ文字列を別の文字列として扱う
  - **core-rd-dns-sd**
    - 正規化**(NFC)** を行うため，**dnssd**での合成済み文字や結合文字列に関する問題は起こらない
    - 正規化**(NFC)**では，日本語の全角カタカナや半角カタカナの変換はされないため，日本語対応が不十分
    - 制御文字については**dnssd WG**の問題が起こる

i18nの観点からみたサービスディスカバリの課題 (2/2)

- 標準化された国際化技術を使用しないと独自実装等により意図しないサービスを参照してしまうことやサービスに到達できない可能性がある
- **ASCII**制御文字以外の制御文字が利用可能であるため，悪意あるインスタンス名を容易に作成可能
- 全角文字や半角文字，合成済み文字や結合文字列が入力可能な日本語に対する課題が残ってしまっている
- 国際化技術を使用する際の注意点
  - 文字列変換処理を行うことで，正しい情報資源であってもアプリケーション上での表示が利用者が意図した文字列と異なる場合があり，利用者を混乱させる可能性がある
    - ホスト名の設定時から共通した国際化技術を適応する等の検討が必要
    - **IDNA2003**及び**IDNA2003**との互換性を維持した**IDNA2008**の文字列変換処理には，句点**(。)**をドット**(.)**に変換する処理を実装可能としているため，ホスト名に句点が含まれていれている場合は名前解決が失敗する可能性がある

まとめと今後の展望

まとめ

- **IETF**では，**Constrained**な環境で動作するためのプロトコルに焦点を当てた標準化を進めている
  - **IETF106**では， **IoT**関連技術に関する**12**の**WG**が開催され注目度は高い
- **IoT**機器のサービスディスカバリに関しては，既存の技術の再利用として，**mDNS**を利用した手法が検討検討されている
  - **dnssd WG**や**core WG**，**homenet WG**にて， 識別子として利用する文字列に**UTF-8**による国際化文字列を許容する**IoT**サービスのサービスディスカバリが提案されており，その技術の国際化文字列の処理手法には利便性及び安全性の観点から課題がある
  - 国際化技術に関する文書のレビューを行える専門家が少なく，国際化技術に関する課題解決に遅れが生じている
    - **draft-klensin-idna-unicode-review-05**として，**IDNA**に関する**Unicode**更新のためのレビュー枠組みを作ろうという取り組みもある

今後の展望

- **IETF**における国際化技術に関する主要プロトコル**IDNA2008**の**Unicode 11.0**への対応の見通しが立った
  - **IDNA Rules and Derived Property Values**は**Unicode 11.0**に対応完了
  - 同様に**PRECIS Framework**においても**Unicode 11.0**への対応が可能か調査を行う必要がある
- **dnssd WG**や**core WG**，**homenet WG**では， **mDNS**が使用する国際化技術の影響を受けている
  - 特に日本語の文字列処理における**Width mapping**の必要性や制御文字に関する問題の提言が必要
  - **DNS**インフラストラクチャを利用する**IoT**サービスのサービスディスカバリでは，**mDNS**を使用していることから**mDNS**の国際化技術が及ぼす影響を整理しその問題を提言するとともに，それを解決するための方法を提案する必要がある
    - **draft-ietf-dnssd-mdns-dns-interop-04**にて，**mDNS**と**DNS**のラベルの相互運用生の問題が指摘されており，その中で国際化技術についても指摘されているが停滞している
- 日本語圏をはじめとした英数字以外の文字を使用する言語圏の利用者にも安全かつ便利に利用できる**IoT**技術を実現するには，国際化文字列のか使いに関する十分な検討も必要である