ICTビジネス戦略オンラインセミナー
「デジュール及びフォーラム標準に関する 国際標準化活動動向調査（第1回）」

IETF が策定する国際化技術の標準化推進と国際化技術を活用するIoT 技術の動向調査

2022/01/28(金)

根本 貴弘

国立大学法人東京農工大学

調査概要

- **調査機関**
  - Internet Engineering Task Force(IETF)
- **調査テーマ**
  - **IETFが策定する国際化技術の標準化推進と国際化技術を活用するIoT技術の動向調査**
- **調査概要**
  1. **IETFが策定する国際化技術の標準化推進としてIETFの主要な国際化技術である** PRECIS Framework**のUnicode 7.0以降への対応提案**
  2. **IoTサービスの情報資源参照時における利便性や安全性，相互運用性の向上に必要となる国際化技術の観点からみた課題の共有**

IETF(Internet Engineering Task Force)とは

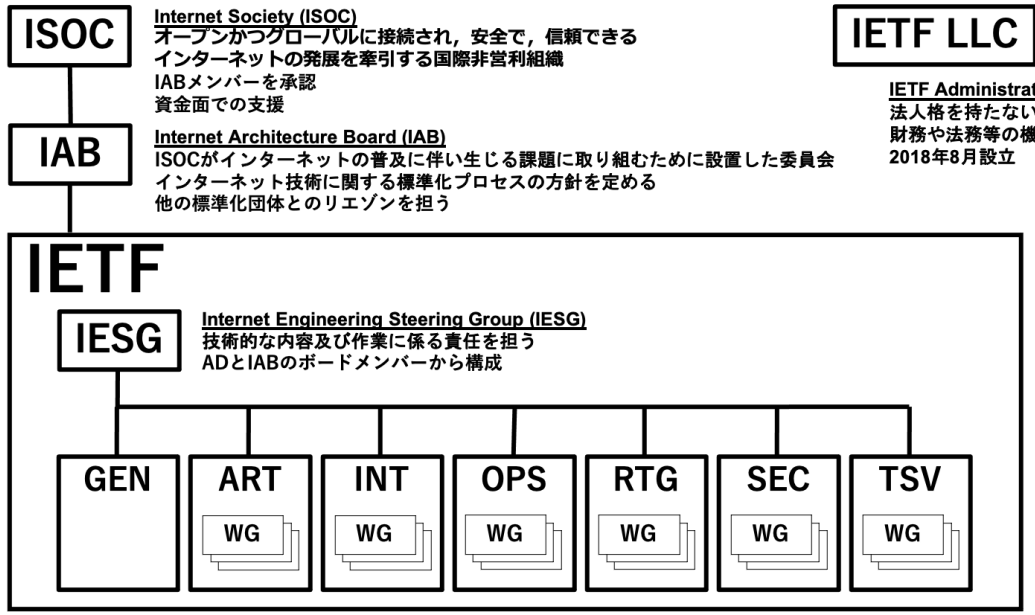
- **インターネット技術に係る仕様と，その仕様策定のプロセスに責任を持つ標準化団体**
  - 1986年に設置
  - **年3回開催されるIETF会合やメーリングリストでの議論**
- **特徴**
  - “Open”**な参加・標準化過程・標準仕様**
  - “Rough Consensus, Running Code”**を重視**
  - **標準化された仕様の普及は市場次第**
  - **多様性を大切にしている会議運営**

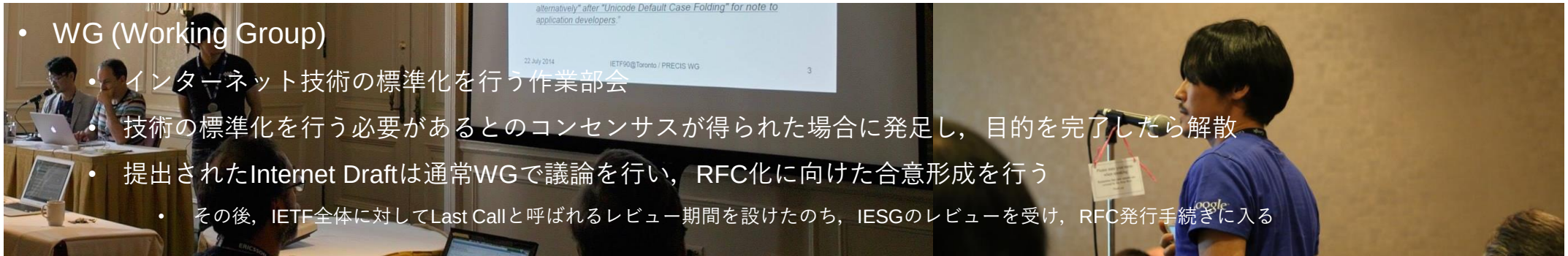
“ We reject kings, presidents and voting.
We believe in rough consensus and running code ”
By David Clark, MIT

- RFC (Request for Comments)
  - **インターネット技術に関連した技術（プロトコル）や運用に関する文書等ある**
  - **代表的なRFC例：**IP (RFC791), TCP (RFC793), DNS (RFC1034, RFC1035)…**等々**

技術範囲と標準化プロセス

- **インターネットに関連すること技術や運用管理等を幅広く扱う**
  - **主にOSI参照モデルのL2-L7とそれ以上で動作する技術が対象**
  - **エリア毎に分類された作業部会にて標準化作業を行う**
- **IETF Areas**
  - GEN：General （IETF**全体の管理・運営分野**）
  - ART：Applications and Real Time（**アプリケーション・リアルタイムコミュニケーション技術分野**）
  - INT：Internet （**インターネット技術分野**）
  - OPS：Operations & Management （**運用管理分野**）
  - RTG：Routing （**ルーティング技術分野**）
  - SEC：Security （**セキュリティ技術分野**）
  - TSV ：Transport and Services （**トランスポート技術分野**）

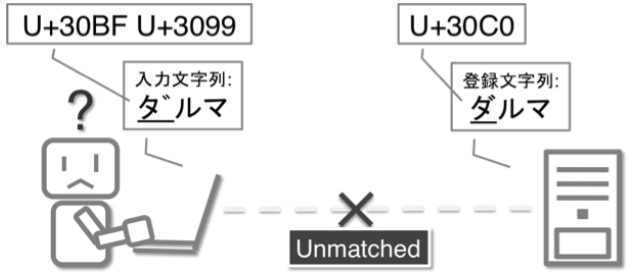


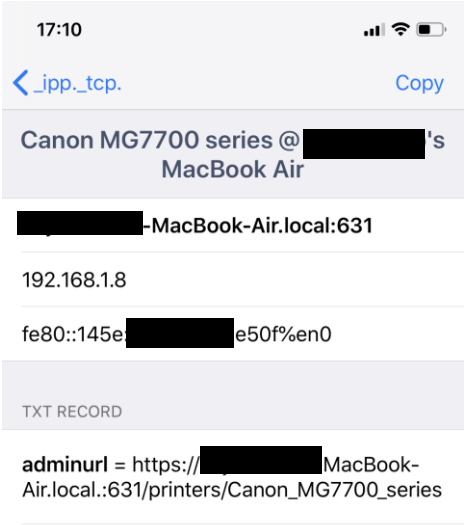


- WG (Working Group)
  - インターネット技術の標準化を行う作業部会
  - 技術の標準化を行う必要があるとのコンセンサスが得られた場合に発足し，目的を完了したら解散
  - 提出されたInternet Draftは通常WGで議論を行い，RFC化に向けた合意形成を行う
    - その後，IETF全体に対してLast Callと呼ばれるレビュー期間を設けたのち，IESGのレビューを受け，RFC発行手続きに入る

調査背景

- 使用者が任意に命名可能なモノを情報資源として扱う可能性のある，IoTサービスにおいて情報資源参照時や認証時における利便性及び安全性の向上のためには適切な国際化技術を使用する必要





2つの課題

- Unicode 7.0以降への対応
  - Unicode 10.0で戸籍統一文字や住民基本台帳ネットワーク文字等の行政システムで利用される文字はほぼ一通り収録された文字も利用できない

IDNA/PRECIS

- 情報システムにおける相互運用性を考慮し文字情報の整備が必要
  - IoTサービスに関するプロトコルで，ホスト名にUTF-8が使用可能（しかし，適切な国際化技術が検討されていない）

mDNS/DNS-SD

IETFにおけるi18n

- i18n = internationalization，**国際化技術**
- **（主にアプリケーション）プロトコルで非ASCII文字集合を扱えるようにすること**
  （RFC 6365: Terminology Used in Internationalization in the IETF (BCP 166)）
- **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**
- **近年の課題は**Unicode7.0**以降への対応**

文字の方向	例
左から右（ラテン文字）	nemoto
右から左（アラビア文字）	نيموتو
右から左（ターナ文字）	ތެސްޓް
双方向（アラビア文字・ラテン文字）	تو0نيم
双方向（アラビア文字・数字）	نمو١٠

必要な変換処理	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゛ (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)
区切り文字	。(U+3002)	． (U+03C2)
空白文字	(U+3000)	(U+0020)
見た目に見えない文字	SHY (U+00AD)	(Nothing)

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 ，RFC8753
- 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

IDNA2008/PRECIS Frameworkの課題

- Unicode 7.0.0以降への対応（現在最新のUnicodeは14.0.0）
- IANAがUniocde 7.0以降のUniocdeのバージョンのIDNA2008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 14.0でも問題が継続している

  - Unicode 10.0で戸籍統一文字や住民基本台帳ネットワーク文字等の行政システムで利用される文字はほぼ一通り収録された文字も利用できない

IETFにおける国際化技術の動向

行政システムで利用される文字はUnicode 10.0でほぼ一通り収録されているため，それらの文字も利用可能となる

- IDNA2008のUnicode 7.0以降への対応に進展
  - IDNA Rules and Derived Property ValuesはUnicode 11.0まで更新完了
    - Unicode 12.0以降には未対応
  - RFC8753: Internationalized Domain Names for Applications (IDNA) Review for New Unicode Versions (Standards Track)の発行
    - IANA registryに登録されているIDNA Derived Propatyの更新方法を定義
    - 最新のIDNA Derived Propatyで古いIDNA Derived Propatyと互換性のない変更がないかを確認
    - 最新のUnicode PropatyでIDNA Derived Propatyの算出方法に整合しない登録されていないかを確認
    - IETGまたは専門チームによる指摘がない限り，原則Unicodeのメジャーバージョンに対してのみレビューを行う
- PRECIS FrameworkのUnicode 7.0以降への対応提案
  - RFC8753により生じた新規課題
  - draft-nemoto-precis-unicode12-00の更新対応

RFC8753により生じた新規課題

- draft-nemoto-precis-unicode12の内容を踏まえ，RFC8753の前身であるdraft-klensin-idna-unicode-reviewの修正とdraft-faltstrom-unicode12への統合が検討されていたが，draft-klensin-idna-unicode-reviewがRFC化したことにより， RFC8753への修正対応が難しくなった

- RFC8753に相当するPRECIS Derived Propatyの更新方法を定義するためのRFCが必要となる見通し

draft-nemoto-precis-unicode12-00の更新作業

- draft-nemoto-precis-unicode12-00に対する関係者からのコメント対応及び更新版I-D（draft-nemoto-precis-unicode13-00）の執筆
  - 議論に参加してもらっている主な関係者
    - Peter Saint-Andre (RFC8264 Author / i18ndir chair)，John C. Klensin (eai WG Chair / i18ndir reviewer)，Marc Blanchet (precis WG Chair / i18ndir reviewer)，Patrik Fältström (RFC5892 Author / i18ndir reviewer)，Barry Leiba (ART Area Review Team (artart) Chair)
  - 関係者からの主なコメント
    - draft-nemoto-precis-unicode12の内容をdraft-faltstrom-unicode12に移し，統合すべきか統合可能性について調査する
    - RFC8264の更新が必要か否かについての検討
    - 標準化を進める上での議論の場所についての検討

I-D更新に向けた主な取り組み (1/3)

- draft-nemoto-precis-unicode12とdraft-faltstrom-unicode12の統合可能性についての調査
  - 各Unicodeのバージョンにおける IDNA2008 Derived Property ValueとPRECIS IDNA2008 Derived Property Valueの差分を調査するためのプログラムの開発
  - 上記プログラムを用い，Unicode 7.0からUnicode 13.0までの各Derived Property Valueの差分を調査
    - その結果，IDNA2008では仕様が禁止されている一部の文字が，PRECISでは利用可能となっていた（PRECISで禁止されている文字がIDNA2008で利用可能となる変更はなかった）
    - これは各Derived Property Valueの算出方法の違いによるものであるため統合することによる維持は比較的容易

```
11,373 characters in Unicode 6.3.0
12,281 characters in Unicode 7.0.0
13,129 characters in Unicode 8.0.0
13,369 characters in Unicode 9.0.0
13,470 characters in Unicode 10.0.0
13,830 characters in Unicode 11.0.0
14,103 characters in Unicode 12.0.0
14,403 characters in Unicode 13.0.0
```

RFC8753により困難に

  - IDNA2008を使用するドメイン名をPRECISを使用する他のプロトコル要素として利用することは可能だが，PRECISを使用する識別子をIDNA2008を使用するドメイン名で使用する場合，制限を受ける可能性があることがわかり，適切なマッピングが必要となる可能性がある（RFC8264だけでなくRFC7790の更新についても検討が必要）

I-D更新に向けた主な取り組み (2/3)

- RFC8264の更新が必要か否かについての検討
  - RFC8264の内容の再調査を行った
    - その結果，UnicodeにIETFの国際化技術と整合しない変更が生じた場合のPRECIS Derived Property Valueの更新手続きについて記載がないことがわかった

  - RFC8753と同様のPRECIS Derived Propatyの更新方法を定義するためのRFCが必要となることがわかった

- 標準化を進める上での議論の場所についての検討
  - draft-nemoto-precis-unicode12とdraft-faltstrom-unicode12の統合が難しいことと，現在適切な提案場所となるWGがないことを受け，専門家等に相談したところ，

    Internationalization Directorate（i18ndir）のMLで本I-Dについて議論をすることを提案頂いた

I-D更新に向けた主な取り組み (3/3)

draft-nemoto-precis-unicode13-00 (Informational Document)

- PRECIS FrameworkがUnicode 13.0に対応可能か，Unicode 6.3からの各Unicode(各1,114,112文字)のPRECIS Derived Property Valueの差分について説明
  - Unicode12.0から13.0への変更については特殊な変更はなかった

```
3.7.  Changes between Unicode 12.0.0 and 13.0.0

   Change in number of characters in each category:

      PVALID changed from 124,415 to 130,049 (+5,634)

      UNASSIGNED changed from 836,537 to 830,606 (-5,931)

      CONTEXTJ did not change, at 2

      CONTEXTO did not change, at 25

      DISALLOWED changed from 140,439 to 140,439 (+0)

      ID_DIS or FREE_PVAL changed from 12,694 to 12,991 (+297)

      TOTAL did not change, at 1,114,112

   Code points that changed derived property value from other than
   UNASSIGNED: 0

   There are no changes made to Unicode between version 12.0.0 and
   13.0.0 that impact PRECIS calculation of the derived property values.
```

- 関係者からのコメントの反映として以下の点を修正
  - 各UnicodeのバージョンにおけるIDNA2008 Derived Property ValueとPRECIS IDNA2008 Derived Property Valueの差分結果とそれに対する考察を追記
  - RFC8264の更新の必要性について追記
- 従来の調査結果で得た知見の反映として以下の点を修正
  - INDA2008やPRECISを相互に使う可能性のあるプロトコル要素に関する問題点を記載

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

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

- ホスト名にUTF-8による名前を許容するmDNS/DNS-SDを使用する提案がある

dnssd WG（1/2）

- 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＋DNS-SD
  - 同一ネットワークセグメント内における，サービスディスカバリ手法を提案
    - 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

```
hoge@hogehoge-PC  ~ % dns-sd -B _ipp._tcp
Browsing for _ipp._tcp
DATE: ---Wed 26 Jan 2022---
22:28:50.871  ...STARTING...
Timestamp     A/R    Flags  if Domain               Service Type         Instance Name
22:28:50.872  Add        2   6 local.               _ipp._tcp.           Canon MF650C Series
```

- 近年発行されたRFC
  - RFC8765: DNS Push Notifications
  - RFC8766: Discovery Proxy for Multicast DNS-Based Service Discovery
  - RFC8882: DNS-Based Service Discovery (DNS-SD) Privacy and Security Requirements

dnssd WG（2/2）

- RFC8765 ：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
- RFC8766 ：Discovery Proxy for Multicast DNS-Based Service Discovery
  - DNS-SDを複数ネットワークセグメントへの拡張方式
  - 異なるネットワークセグメント（netB.example.jp）のサービスを使用する場合,「_ipp._tcp.netB.example.jp」として探す
- RFC8882：DNS-SD Privacy and Security Requirements
  - draft-ietf-dnssd-privacyの著者によるDNS-SDにおけるプバイバシーやセキュリティに関する要件について説明をしている
  - いくつかのシナリオを用いてDNS-SDにおける脅威モデルとその課題解決に必要となる要件を整理している

国際化技術を利用するIoT技術の課題共有

- 国際化文字列の処理に課題があったUTF-8を識別子として利用するIoTサービスディスカバリ技術
  - dnssd WG（RFC6763，draft-ietf-dnssd-hybrid），homenet WG（draft-ietf-homenet-simple-naming），core WG（draft-ietf-core-rd-dns-sd）等で， mDNS（RFC6762）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がある
- 本課題について，国際化技術側の関係者等に情報提供
  - 国際化技術の専門家グループである，i18ndirの関係者に共有
  - dnssd WGにて課題の共有
    - rfc6762：Multicast DNSやrfc7558：Requirements for Scalable DNS-Based Service Discovery (DNS-SD) / Multicast DNS (mDNS) Extensions等の著者のStuart Cheshire（Apple社）にから回答を得た

まとめ

1. IETFが策定する国際化技術の標準化推進としてIETFの主要な国際化技術であるPRECIS FrameworkのUnicode 7.0以降への対応提案
   - INDA2008やPRECISを利用するプトロコルを相互に行き来するプロトコル要素に関する問題点と今後の検討事項（RFC8264だけでなくRFC7790の更新についての検討）の明確化
   - RFC8753の発行の影響を受けて方針転換が生じたが，RFC化を進める上での議論の場の提案を受けた
2. IoTサービスの情報資源参照時における利便性や安全性，相互運用性の向上に必要となる国際化技術の観点からみた課題の調査と情報提供
   - INDA2008やPRECISを相互に使う可能性のあるプロトコル要素で生じる問題点をdraft-nemoto-precis-unicode13-00に記載し公開した
   - dnssdWGでは， INDA2008やPRECISへの参照がないため，dnssdを使用する技術では国際化技術の観点からみた問題が生じる可能性がある