IETFにおけるIoT/暗号技術に関する標準化動向

株式会社レピダム
菅野 哲

JNSA PKI相互運用技術WG・電子署名WG主催セミナー
PKI Day 2017「IoT・ブロックチェーン時代のPKI」

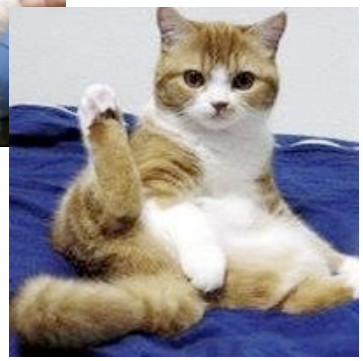
（個人的に期待する）聴講後の皆さまの状態

- IETFについて知っている！
  - 例：あのクッキーが配給されるところでしょ？
- IETFでのIoTと聞いたら、ピンと来る
  - 例：「あのWGを見れば、OK」という状態
- IETFでの暗号技術への取り組みも把握
  - 例：「IETF88がターニングポイントだよね～」と言える

参考：2017年2月27日に送付した講演概要

概要：
IETFにおいて様々なインターネットプロトコルが検討/標準化されていますが、
この組織においてもセンサーなどに代表されるIoT機器で利用されるプロトコルや暗号技術の利用が検討されています。
本講演では、ここ最近のIETFにおけるIoTで利用される暗号技術やプロコトルに関する標準化/技術動向を報告します。

この人、誰よ？



- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - 株式会社 レピダム
  - ISOC-JP プログラム委員
- どんなことやっていた／やっているの？
  - 学生時代～
    - 暗号製品を売り歩く
    - 暗号ライブラリや暗号関連システム開発
    - 人事部で人材開発
    - 標準化活動
  - 最近は会社に関することは何でも！？
    - かなり人が足りていない・・・Please, help us!! ☺

株式会社レピダムって・・・？

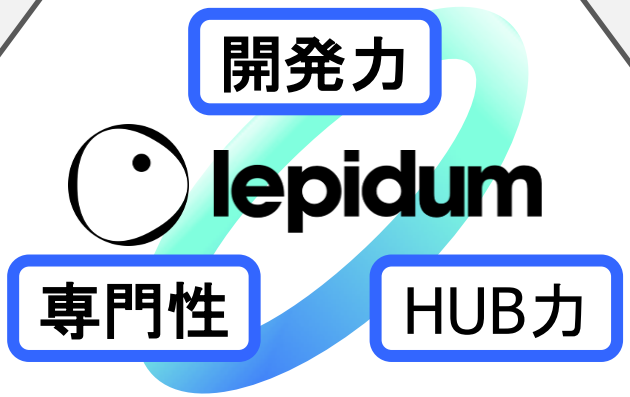
「エッジの効いた技術でお客様の事業を加速させる」燃料

ビジョン ： 世界を変革する技術イノベーション支援による付加価値創造

- 日本の課題　年間投資額18兆円の技術イノベーションの予算があるが、
  市場ニーズとタイミングを捉えての研究技術の送り出しが
  出来ていない=技術は良くても事業の芽が出ない

技術シード
- 企業研究所
- 大学
- 標準化団体

事業ニーズ
- 事業会社
- 自治体



政策&研究アドバイザリ事業
- 事業ニーズの翻訳伝達
- 業界コミュニティからの産業課題摘出
- 諸外国の研究開発動向

事業化コンサルティング
- 政策動向への深い知見
- 研究者ネットワークへの窓口代理
- 先進技術の事業化目利き

IETFとIoTと暗号技術の関係を紐解く

- 一見関係がありそうでモヤモヤしている、
  この3つの関係を紐解く

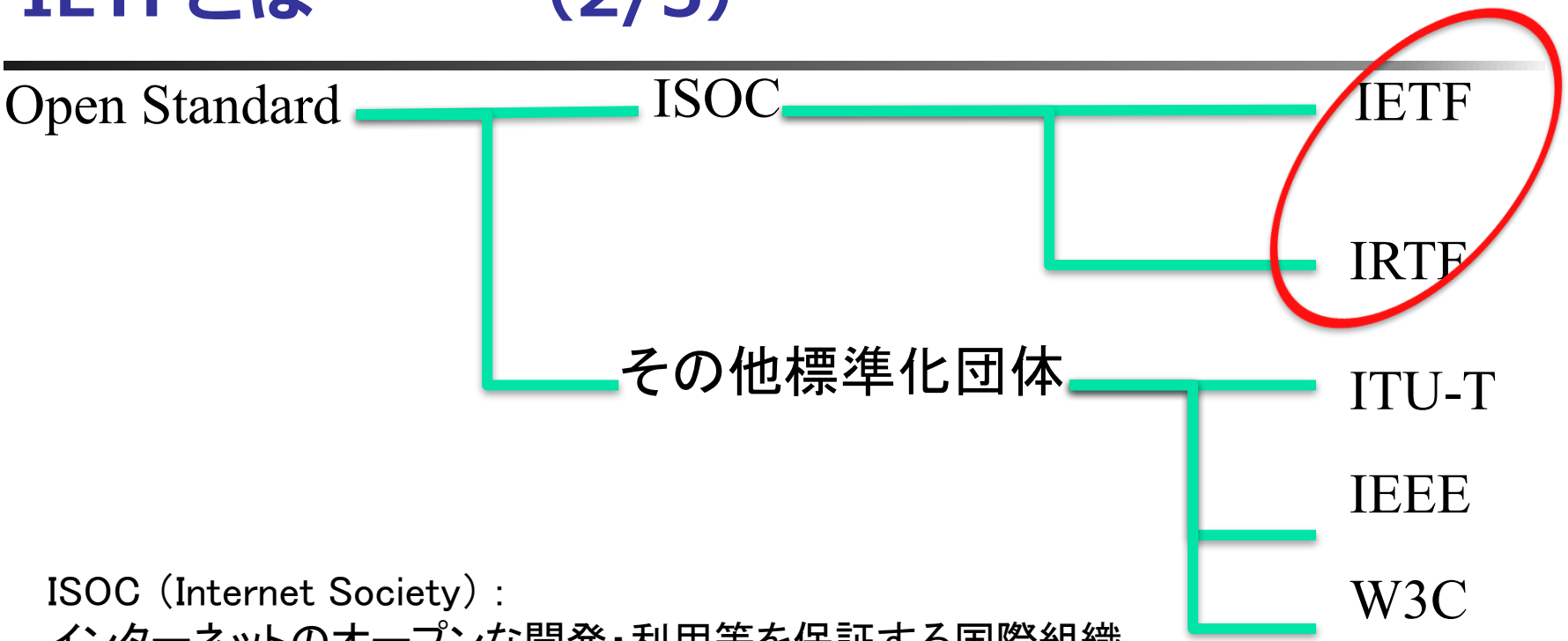
IETFとIoTと暗号技術の関係を紐解く

- 一見関係がなさそうな、この3つの関係を紐解く

IETFとは・・・（1/5）

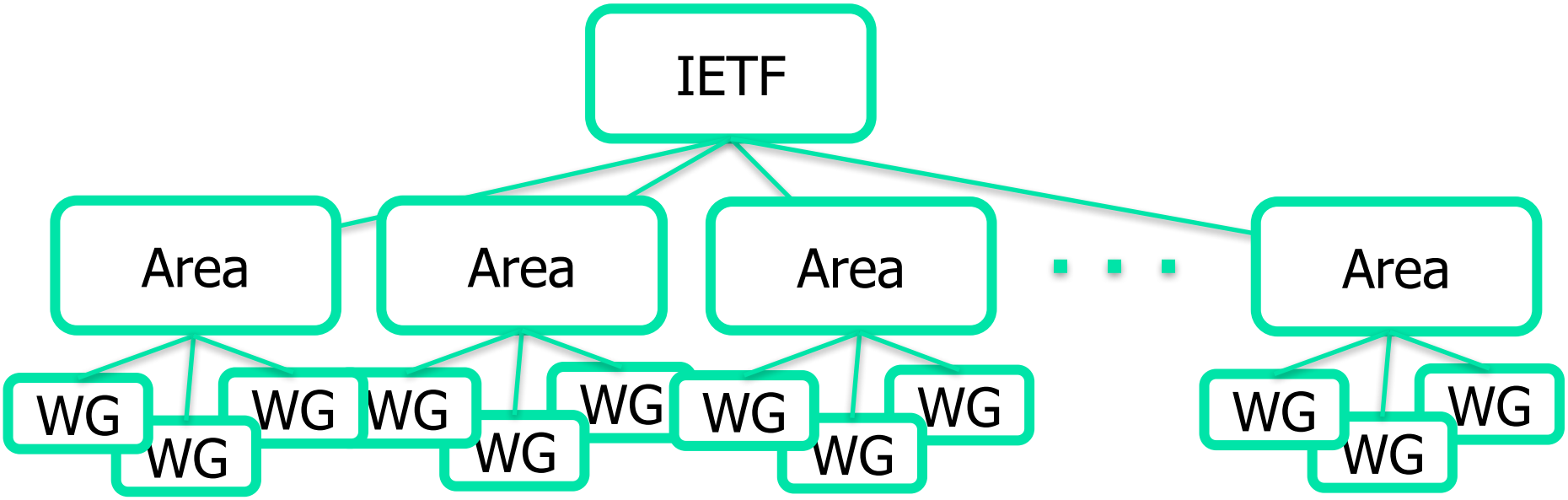
- **I**nternet **E**ngineering **T**ask **F**orce
  - **インターネットに関する技術**の国際標準を策定する組織
- 理念
  - “We reject kings, presidents and voting. We believe in ***rough consensus*** and ***running code***.” David Clark (1992)
- 生産物
  - RFC （Request for Comments）を発行
  - インターネットを技術的な側面を支えられている

IETFとは・・・（2/5）



- ISOC（Internet Society）：
  インターネットのオープンな開発・利用等を保証する国際組織
- **IRTF（Internet Research Task Force）：**
  インターネットの未来において重要と思われる研究を推進する組織
- ITU-T：
  国際電気通信連合において通信分野の標準化策定を担当する電気通信標準化部門
- IEEE：
  アメリカに本部を持つ電気電子技術学会
- W3C：
  World Wide Webで使用される各種技術の標準化の推進を目的に設立された団体

IETFとは・・・（3/5）



7 Area
129WGs
(2017.4現在)

- GEN（General）: 1
- ART（Applications and Real-Time）:38
- INT（Internet）: 19
- OPS（Operations and Management）: 17
- RTG（Routing）: 25
- SEC（Security）:16
- TSV（Transport Services）: 13

https://datatracker.ietf.org/wg/

IETFとは・・・（4/5）

メカっぽい参加者や所構わず議論する場面も

IETFとは・・・（5/5）

会場にはマイクが立ってて所属を超えて活発な議論！

世の中的に見てIETFって影響はあるの？

めちゃくちゃ影響を受けています！

- 身の回りのセキュアプロトコルだと・・・

TLS/DTLS

IPsec

SSH

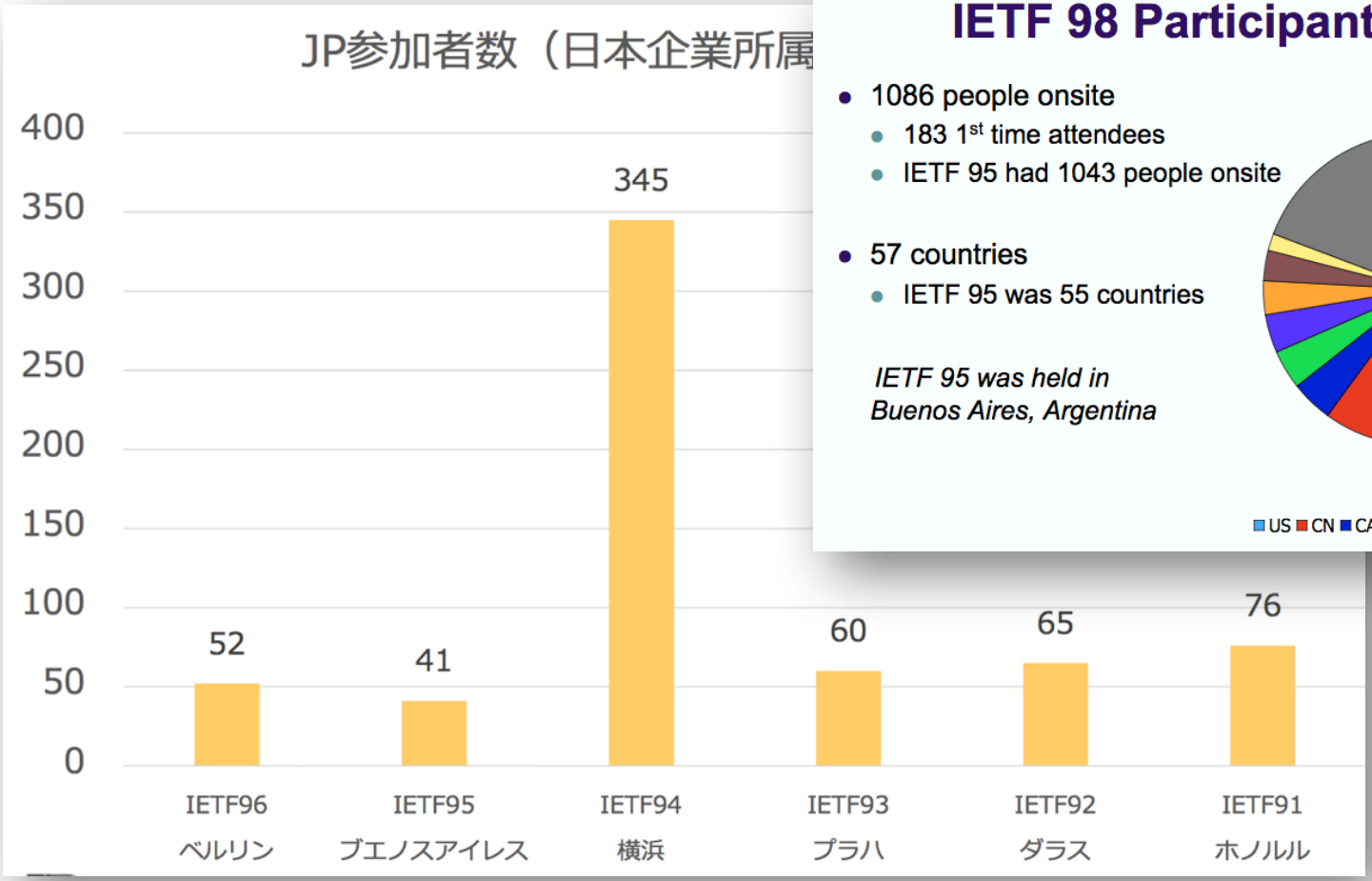
実社会に影響はありそうだけど・・・

暗号を使うプロトコルはあるけど、
暗号技術に関する議論とかしているの？

- 安全に暗号技術を利用するための鍵長などの議論
- Research Group（CFRG）やSAAGにて、インターネットで利用するアルゴリズムの選定を実施
  - 新たな暗号プリミティブの検討
    - 楕円曲線パラメータ
    - Post-Quantum　などなど

余談：IETFでの日本の存在感は？

https://www.ietf.org/proceedings/98/slides/slides-98-ietf-sessc-chair-report-00.pdf



https://www.isoc.jp/wiki.cgi?page=IETF96Update&file=20160912%5FIETF96update%5F01%5Fplenary%5Ftaiji%2Dk%2Epdf&action=ATTACH

日本の存在感が消えつつ・・・ orz

IETFとIoTと暗号技術の関係を紐解く

- 一見関係がありそうでモヤモヤしている、
  この3つの関係を紐解く

IETFで暗号って意外かも・・・と言う方も

IETF88 Technical Plenary (Nov, 2013)

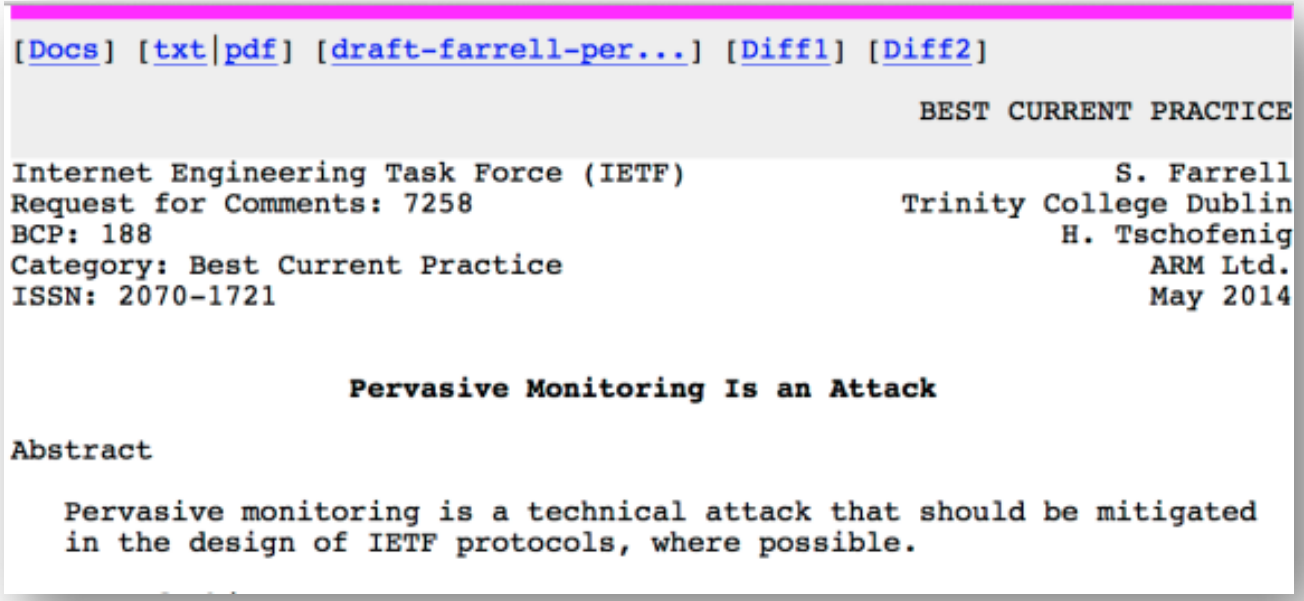
2013年6月に明らかになった「Pervasive Surveillance」に対してどうすべきかを検討！

IETF93（July, 2015）ではEdward Snowden氏も遠隔で登場

https://www.internetsociety.org/publications/ietf-journal-november-2015/snowdon-meets-ietf

SurveillanceとIETFにおける技術的対処方針

広域への監視行為をインターネットへの攻撃として合意



[Docs] [txt|pdf] [draft-farrell-per...] [Diff1] [Diff2]

BEST CURRENT PRACTICE

Internet Engineering Task Force (IETF) — S. Farrell
Request for Comments: 7258 — Trinity College Dublin
BCP: 188 — H. Tschofenig
Category: Best Current Practice — ARM Ltd.
ISSN: 2070-1721 — May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

http://tools.ietf.org/html/rfc7258

IETFが採用した技術的な方針

脱・米国標準

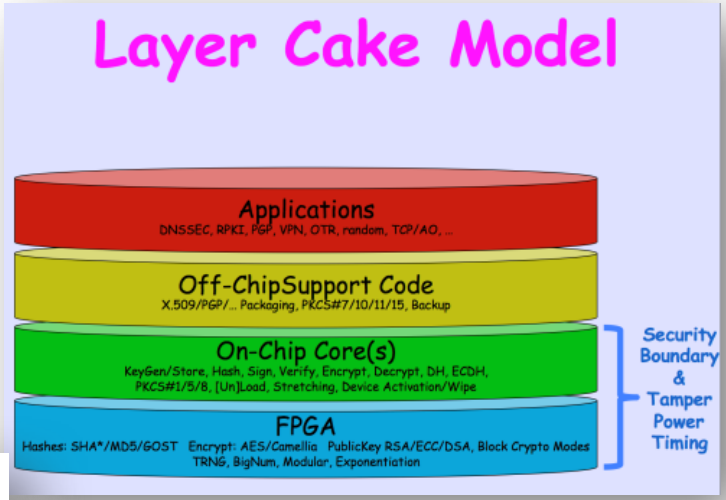
Forward Secrecy

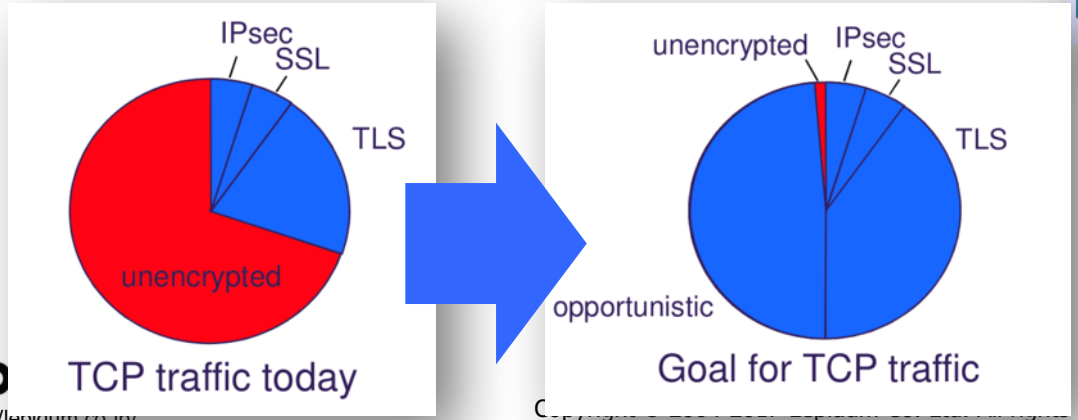
End to End Enc

対抗策として検討した結果は？

- 脱・米国標準以外のアルゴリズムの選定
  - 楕円曲線パラメタ：Curve25519
  - ストリーム暗号：ChaCha20+Poly1305
  - 署名アルゴリズム：EdDSA
- HSMも信じられない！
  - CrypTech Project
- 「とりあえず、暗号化！」
  - Opportunistic Encryption

http://trac.cryptech.is/attachment/wiki/DocMeet/140109.cryptech.pdf





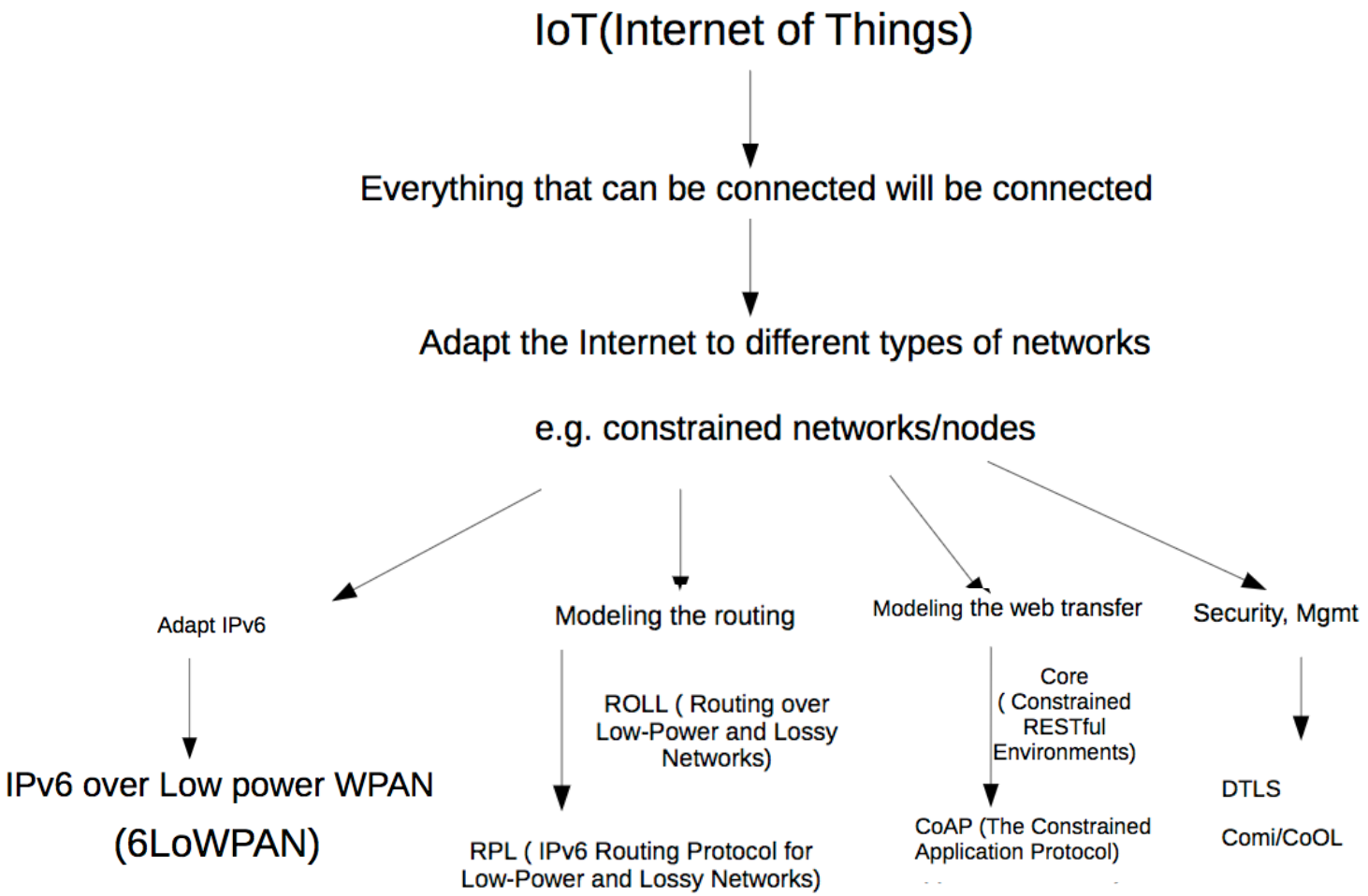
http://www.ietf.org/proceedings/91/slides/slides-91-tcpinc-1.pdf

IETFとIoTと暗号技術の関係を紐解く

- 一見関係がありそうでモヤモヤしている、
  この3つの関係を紐解く

IETFでの暗号の話はわかった・・・IoTの話は？

- IoTにおける”制約“が発生する場所を捉える

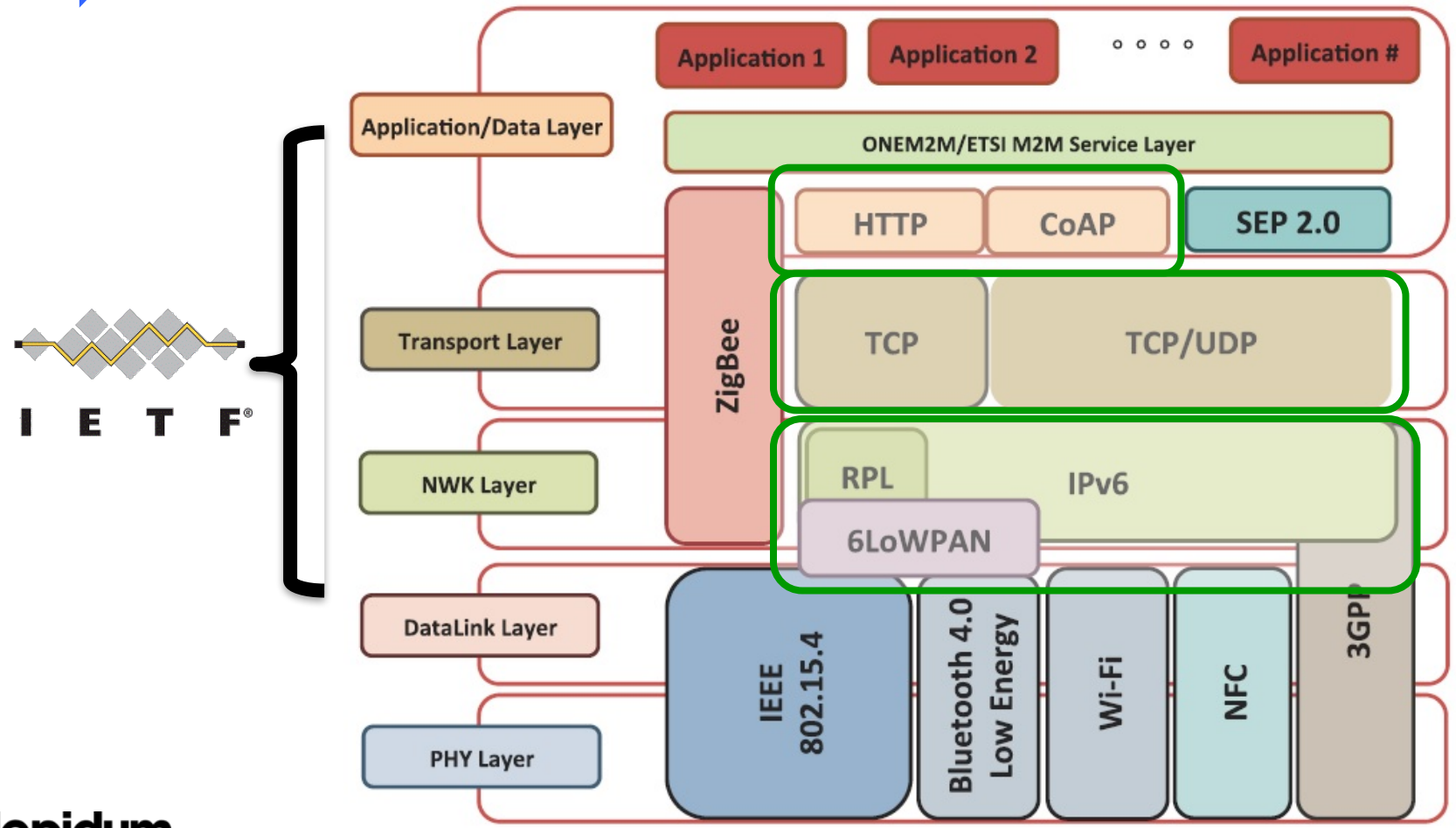


http://seminar-materials.iijlab.net/iijlab-seminar/iijlab-seminar-20161122.pdf

IoTから見たIETFの成果

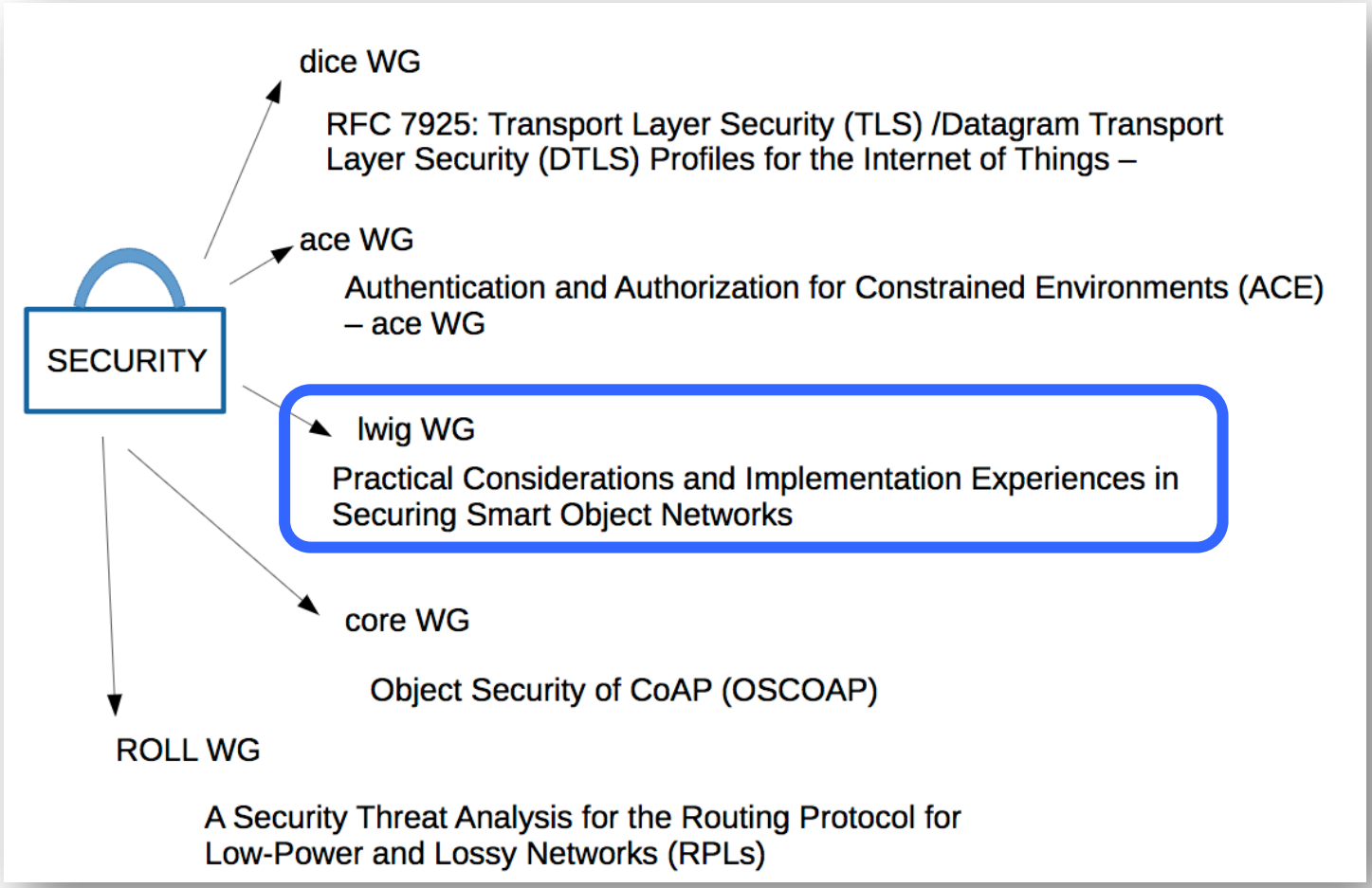
OSIに基づくレイヤとプロトコルスタック的に見てみると・・・

➡ NW層～アプリケーション層は、ほぼIETFの独壇場！



https://connectedtechnbiz.wordpress.com/tag/iot-standards/

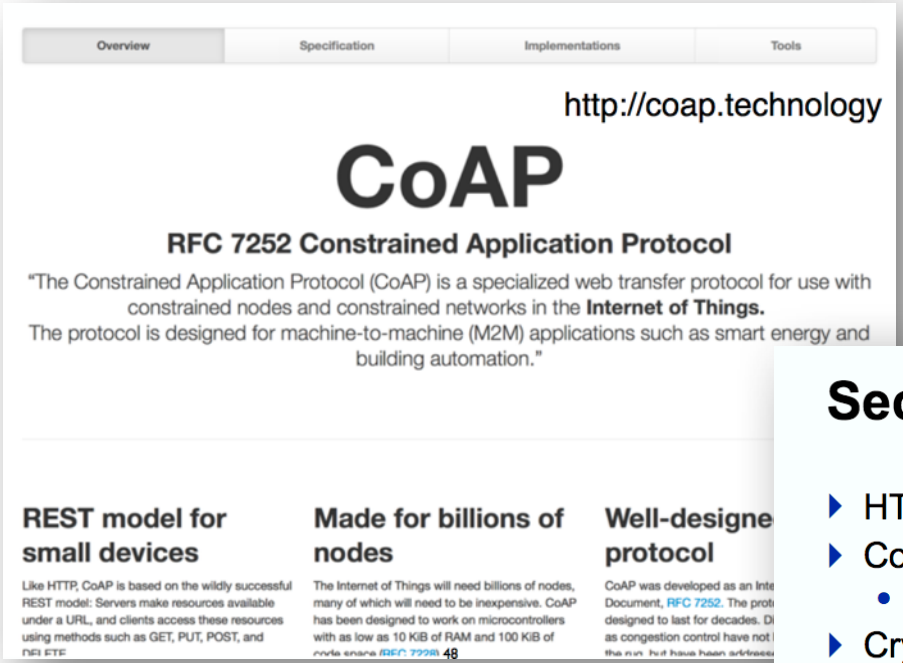
IETFでIoT Securityを検討しているWG



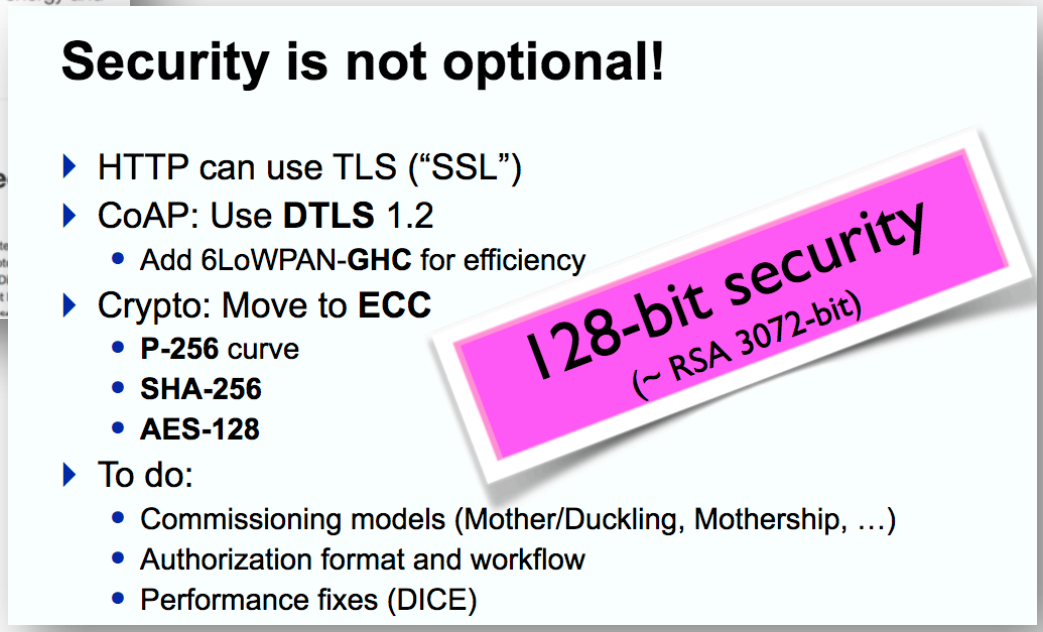
http://seminar-materials.iijlab.net/iijlab-seminar/iijlab-seminar-20161122.pdf

lwigでIoTでの実装についてガイダンスを検討

IoTでのセキュリティに関する取り扱い



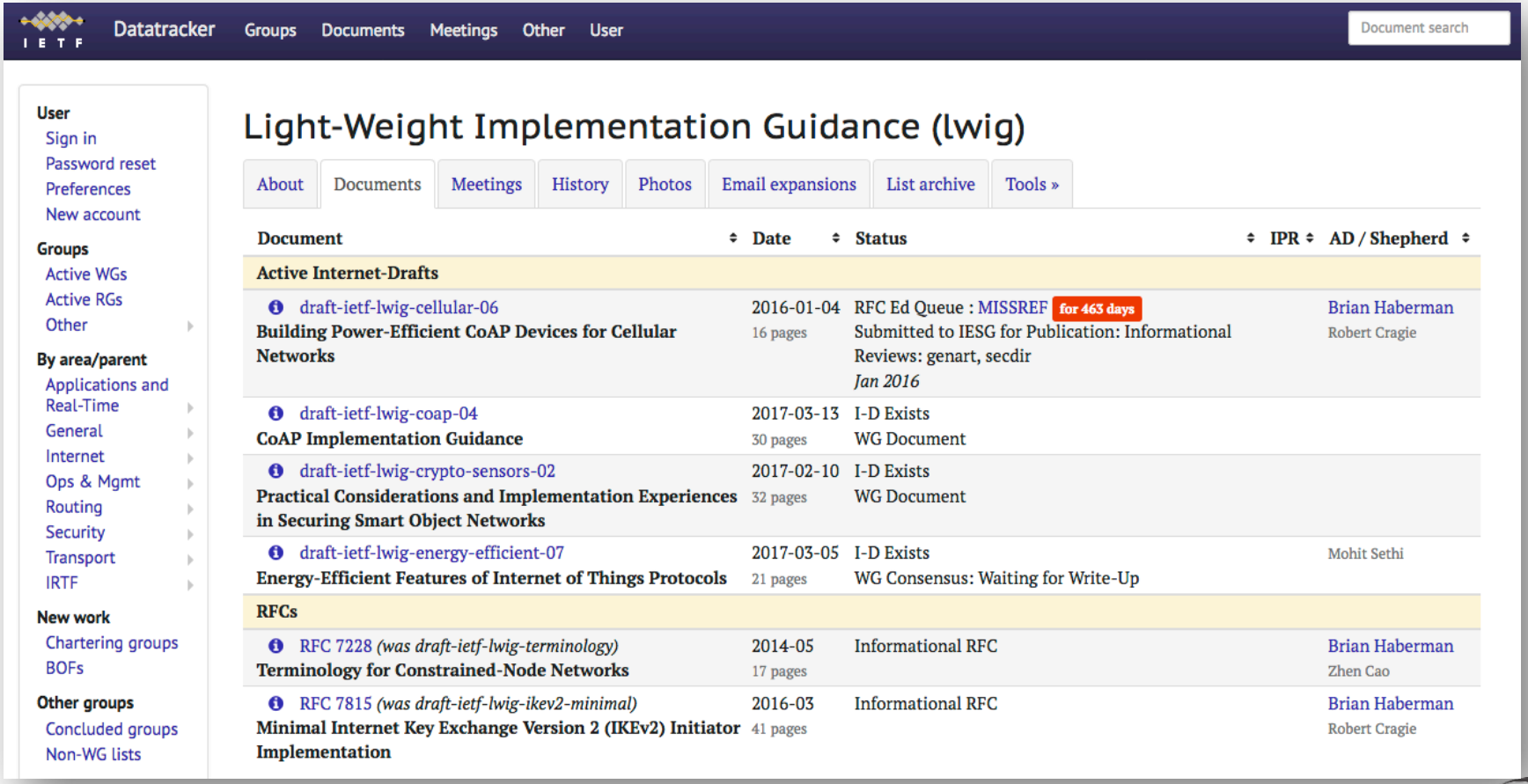
https://www.w3.org/2015/04/munich/bormann.pdf



制約された機器で128ビットセキュリティ可能なの？！

Light-Weight Implementation Guidance (lwig)

2011年3月にlwig WGが発足され、制約された機器での利用を想定したガイダンスを検討



https://datatracker.ietf.org/wg/lwig/documents/

lwigにおけるドキュメント（1/4）

コミュニケーションの基本として用語の統一（超大事）

From: draft-ietf-lwig-terminology-07 Informational

Internet Engineering Task Force (IETF)
Request for Comments: 7228
Category: Informational
ISSN: 2070-1721

C. Bormann
Universitaet Bremen TZI
M. Ersue
Nokia Solutions and Networks
A. Keranen
Ericsson
May 2014

Terminology for Constrained-Node Networks

Abstract

The Internet Protocol Suite is increasingly used on small devices with severe constraints on power, memory, and processing resources, creating constrained-node networks. This document provides a number of basic terms that have been useful in the standardization work for constrained-node networks.

https://datatracker.ietf.org/doc/html/rfc7228

※ すでに改訂版のI-Dが投稿されている

lwigにおけるドキュメント（2/4）

皆んなの心の中で想定が違うデバイス性能を整理

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB

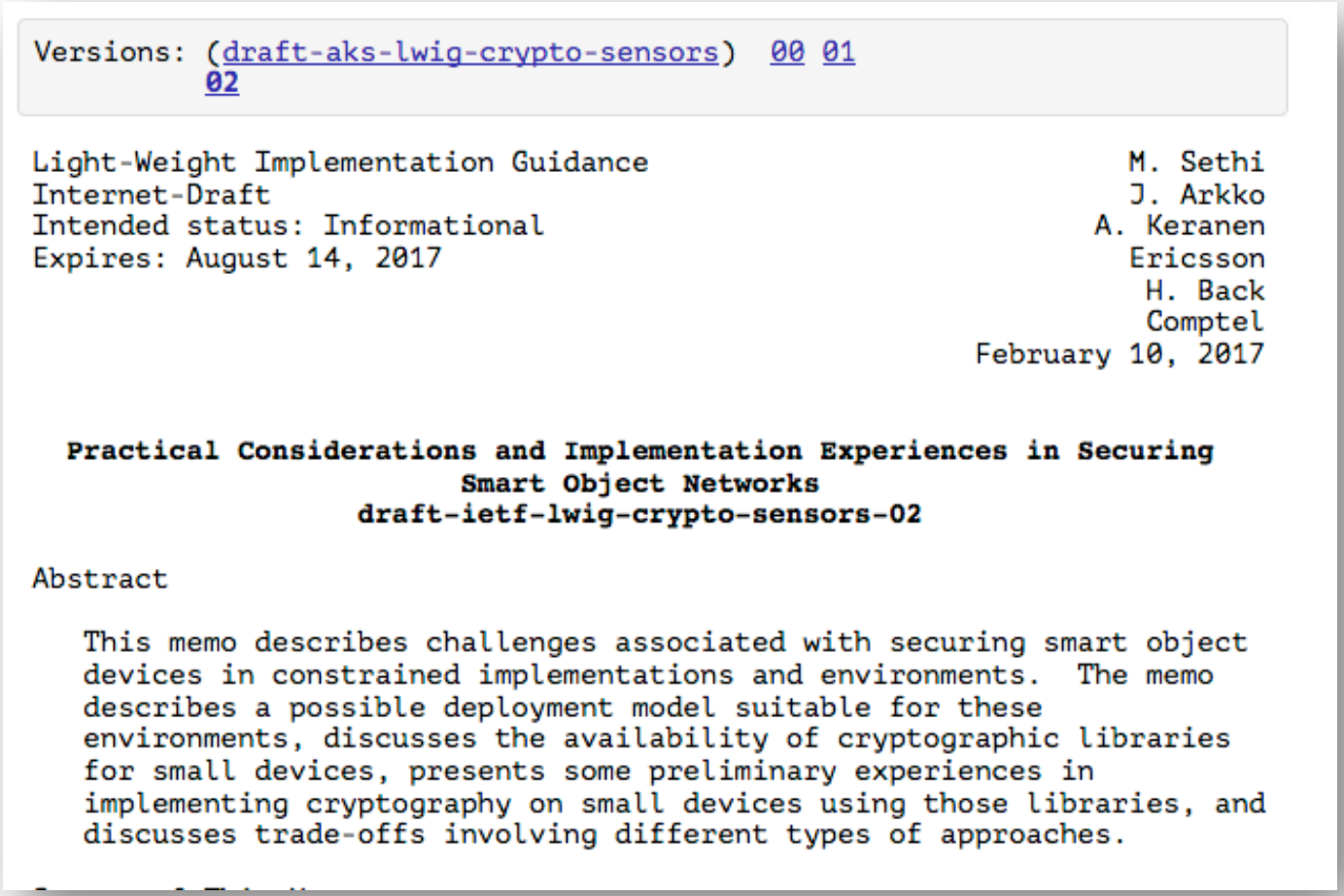
Table 1: Classes of Constrained Devices (KiB = 1024 bytes)

https://datatracker.ietf.org/doc/html/rfc7228

- **Class 0 :**
  - メモリ＆処理の制約が非常に厳しい。通信に必要なリソースもない。
  - プロキシ、ゲートウェイなどのサポートによりインターネットへ接続
- **Class 1 :**
  - コードスペースと処理に制約がある。フルスタックプロトコル（HTTP、TLSなど）を容易には利用できない。CoAPで通信したり、ゲートウェイのサポートなく通信可能。
  - 大規模ネットワークでのセキュリティ機能が利用可能
- **Class 2 :**
  - ノートPCやサーバで利用されるプロトコルスタックを利用可能。

lwigにおけるドキュメント（3/4）

個人的には実装者向けには有力なRFCになると予想！



Versions: (draft-aks-lwig-crypto-sensors) 00 01
02

Light-Weight Implementation Guidance
Internet-Draft
Intended status: Informational
Expires: August 14, 2017

M. Sethi
J. Arkko
A. Keranen
Ericsson
H. Back
Comptel
February 10, 2017

Practical Considerations and Implementation Experiences in Securing Smart Object Networks
draft-ietf-lwig-crypto-sensors-02

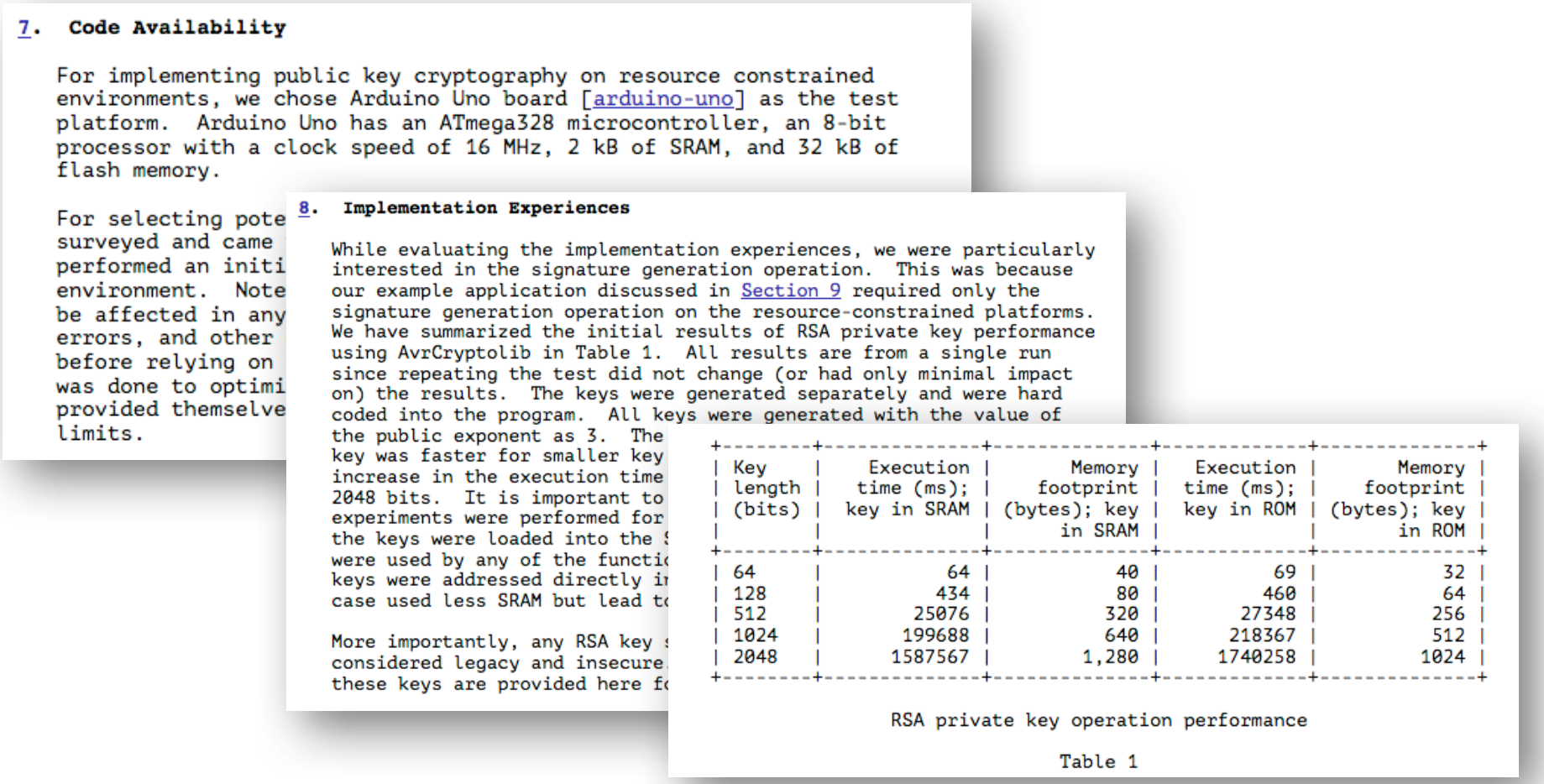
Abstract

This memo describes challenges associated with securing smart object devices in constrained implementations and environments. The memo describes a possible deployment model suitable for these environments, discusses the availability of cryptographic libraries for small devices, presents some preliminary experiences in implementing cryptography on small devices using those libraries, and discusses trade-offs involving different types of approaches.

https://datatracker.ietf.org/doc/html/draft-ietf-lwig-crypto-sensors

lwigにおけるドキュメント（4/4）

IoT機器で利用できる暗号ライブラリや実機での性能等を整理



7. Code Availability

For implementing public key cryptography on resource constrained environments, we chose Arduino Uno board [arduino-uno] as the test platform. Arduino Uno has an ATmega328 microcontroller, an 8-bit processor with a clock speed of 16 MHz, 2 kB of SRAM, and 32 kB of flash memory.

For selecting pote
surveyed and came
performed an initi
environment. Note
be affected in any
errors, and other
before relying on
was done to optimi
provided themselve
limits.

8. Implementation Experiences

While evaluating the implementation experiences, we were particularly interested in the signature generation operation. This was because our example application discussed in Section 9 required only the signature generation operation on the resource-constrained platforms. We have summarized the initial results of RSA private key performance using AvrCryptolib in Table 1. All results are from a single run since repeating the test did not change (or had only minimal impact on) the results. The keys were generated separately and were hard coded into the program. All keys were generated with the value of the public exponent as 3. The
key was faster for smaller key
increase in the execution time
2048 bits. It is important to
experiments were performed for
the keys were loaded into the
were used by any of the functi
keys were addressed directly i
case used less SRAM but lead t

More importantly, any RSA key
considered legacy and insecure
these keys are provided here f

Key length (bits)	Execution time (ms); key in SRAM	Memory footprint (bytes); key in SRAM	Execution time (ms); key in ROM	Memory footprint (bytes); key in ROM
64	64	40	69	32
128	434	80	460	64
512	25076	320	27348	256
1024	199688	640	218367	512
2048	1587567	1,280	1740258	1024

RSA private key operation performance

Table 1

https://datatracker.ietf.org/doc/html/draft-ietf-lwig-crypto-sensors

IETF98でのIoT関連WG開催状況

IETF98において、9 WG/RG も開催されており注目度は高い

- IRTF
  - t2trg (Thing-to-Thing) RG
- IETF
  - INT
    - 6lo (IPv6 over Networks of Resource-constrained Nodes) WG
    - 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) WG
    - lpwan (IPv6 over Low Power Wide-Area Networks) WG
    - lwig (Light-Weight Implementation Guidance) WG
    - ipwave (IP Wireless Access in Vehicular Environments) WG
  - ART
    - core (Constrained RESTful Environments) WG
  - SEC
    - ace (Authentication and Authorization for Constrained Environments) WG
  - RTG
    - roll (Routing Over Low power and Lossy networks) WG

余談としてのIETF動向（セキュリティ関連）

- IETF98では様々なBar BoF/BoFが開催
  - A Protocol for Dynamic Trusted Execution Environment Enablement (TEEP)
  - Firmware Update Description (FUD)
  - Internet-level consistency (ILC)

IETFで取り扱うべきテーマなのか？という議論を
実施しながら、実社会で必要な技術要素をピックアップ

Bar BoF/BoFから次のビックウェーブが？！

最近、IETFに参加して感じること

- 再度IETFに参加して強く感じるのは、実際に利用されるシチュエーションを意識している
  - 有用な情報を共有したり、Hackathon を開催したり
- セキュリティ領域を見ると高年齢化が進行
  - 日本からの参加者はそもそも少ない・・・
  - 日本企業・組織からの参加が少ない・・・
- みんなで楽しいことしたいよね

IETFにおけるIoTへの影響予想？！

DTLS 1.3

&

QUIC

現在、進行中のこれらの技術が影響を与えそう！

参考： IETFでのIoT関連RG/WG （1/2）

さらにIoT関連の議論を追っかけたい人向けのリンク集

- **t2trg (Thing-to-Thing) RG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/t2trg/
  Charter: https://irtf.org/t2trg
- **6lo (IPv6 over Networks of Resource-constrained Nodes) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/6lo/
  Documents: https://datatracker.ietf.org/wg/6lo/
  Charter: http://datatracker.ietf.org/wg/6lo/charter/
- **6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/6tisch/
  Documents: https://datatracker.ietf.org/wg/6tisch/
  Charter: http://datatracker.ietf.org/wg/6tisch/charter/
- **lpwan (IPv6 over Low Power Wide-Area Networks) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/lpwan/
  Documents: https://datatracker.ietf.org/group/lpwan/
  Charter: https://datatracker.ietf.org/group/lpwan/charter/
- **core (Constrained RESTful Environments) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/core/
  Documents: https://datatracker.ietf.org/wg/core/
  Charter: http://datatracker.ietf.org/wg/core/charter/

参考：IETFでのIoT関連RG/WG（1/2）

- **ace (Authentication and Authorization for Constrained Environments) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/ace/
  Documents: https://datatracker.ietf.org/wg/ace/
  Charter: http://datatracker.ietf.org/wg/ace/charter/
- **roll (Routing Over Low power and Lossy networks) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/roll/
  Documents: https://datatracker.ietf.org/wg/roll/
  Charter: http://datatracker.ietf.org/wg/roll/charter/
- **lwig (Light-Weight Implementation Guidance) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/lwig/
  Documents: https://datatracker.ietf.org/wg/lwig/
  Charter: http://datatracker.ietf.org/wg/lwig/charter/
- **ipwave (IP Wireless Access in Vehicular Environments) WG**
  Agenda: https://datatracker.ietf.org/meeting/98/agenda/ipwave/
  Documents: https://datatracker.ietf.org/wg/ipwave/
  Charter: http://datatracker.ietf.org/wg/ipwave/charter

まとめ

- こんな状態になっていますか・・・ドキドキ
  - IETFについて知っている！
  - IETFでのIoTと聞いたら、ピンと来る
  - IETFでの暗号技術への取り組みも把握

- 暗号技術を使った技術分野で何か一緒に活動しませんか？
  - JNSA PKI相互運用WGでIETFの情報共有・議論が実施

よろしくお願いします！(`･ω･´)ゞ

何か気になることなどあれば・・・

- E-mail
  - kanno@lepidum.co.jp
- SNS
  - Twitter(satorukanno)
  - Facebook(satoru.kanno)

お気軽にご連絡ください！