IETF報告会 (101st ロンドン)
Security Area および 暗号技術に関する動向

株式会社レピダム
菅野 哲

目的

- IETF101におけるSecurity Areaおよび暗号技術に関する動向をお伝えします！(`･ω･´)ゞ

- 「いや～セキュリティとか興味なくて・・・」という方も、ぜひ聞いていただけたらと思います
  - 大きな流れを知って、もし興味をもっていただけたら参考情報などから詳細を！

おしながき

- 目的
- Agendaから振り返るIETF101
- Security Areaに関する動向
- 暗号技術に関する動向
- まとめ

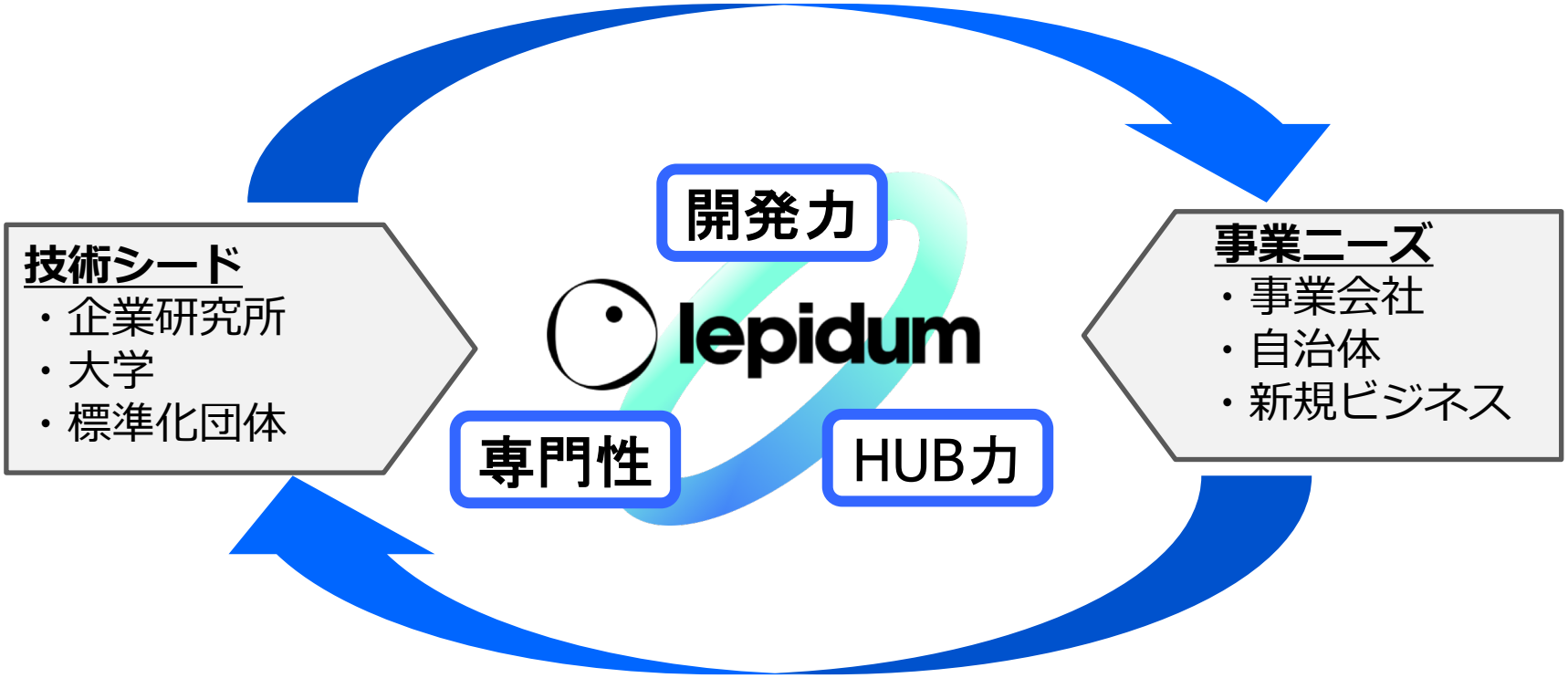
この人、誰よ？

- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - 株式会社 レピダム 

- どんなことやっていた／やっているの？
  - 学生時代～現在
    - 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
      - RFCを何本か発行
    - 今は会社のことなら何でもやっているw

株式会社レピダムって・・・？

最先端技術でお客様の想いを実現させる集団



具体的な技術領域：

「標準化支援、アイデンティティ、プライバシ、認証・認可、情報セキュリティ」に関する開発、調査・コンサル

おしながき

- 目的
- Agendaから振り返るIETF101
- Security Areaに関する動向
- 暗号技術に関する動向
- まとめ

IETF101 Agenda

毎度のことながら大量のWG/RGがセッションが開催

https://datatracker.ietf.org/meeting/101/agenda.html

様々なWG/RGでセキュリティに関する話題はあるけど
囲ったところにフォーカス！

おしながき

- 目的
- Agendaから振り返るIETF101
- Security Areaに関する動向
- 暗号技術に関する動向
- まとめ

Security Areaに関する動向（1/6)

- **トピック１**：Area Directorが変わりましたっ！
  - Kathleen Moriarty ⇨ Benjamin Kaduk に交代
  - みんな、大好き EKRは続投です

sec active WGs

Group	Responsible AD	Name	Chairs
ace	Benjamin	Authentication and Authorization for Constrained Environments	Roman Danyliw, Jim Schaad
acme	Eric	Automated Certificate Management Environment	Yoav Nir, Rich Salz
curdle	Eric	CURves, Deprecating and a Little more Encryption	Daniel Migault, Rich Salz
dots	Benjamin	DDoS Open Threat Signaling	Roman Danyliw, Tobias Gondrom
emu	Eric	EAP Method Update	Joseph Salowey
i2nsf	Eric	Interface to Network Security Functions	Linda Dunbar, Yoav Nir
ipsecme	Eric	IP Security Maintenance and Extensions	Tero Kivinen, David Waltermire
kitten	Benjamin	Common Authentication Technology Next Generation	Benjamin Kaduk, Matthew Miller
lamps	Eric	Limited Additional Mechanisms for PKIX and SMIME	Russ Housley
mile	Alexey	Managed Incident Lightweight Exchange	Nancy Cam-Winget, Takeshi Takahashi (Assigned AD: Alexey Melnikov)
oauth	Eric	Web Authorization Protocol	Rifaat Shekh-Yusef, Hannes Tschofenig
sacm	Benjamin	Security Automation and Continuous Monitoring	Christopher Inacio, Karen O'Donoghue
secdispatch	Benjamin	Security Dispatch	Richard Barnes, Roman Danyliw
secevent	Benjamin	Security Events	Dick Hardt, Yaron Sheffer
suit	Eric	Software Updates for Internet of Things	Russ Housley, Dave Thaler, David Waltermire
teep	Benjamin	Trusted Execution Environment Provisioning	Nancy Cam-Winget, Dave Thaler
tls	Benjamin	Transport Layer Security	Joseph Salowey, Sean Turner
tokbind	Eric	Token Binding	John Bradley, Leif Johansson
trans	Eric	Public Notary Transparency	Melinda Shore, Paul Wouters

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

Security Areaに関する動向（2/6)

トピック2：流行りテーマに関するWGが開始＆興味深いテーマを取り扱うBoFが開催

- 流行りのテーマに関するWG
  - suit （Software Updates for Internet of Things)
    - IoT機器のファームウェアアップデート
  - teep (Trusted Execution Environment Provisioning)
    - TEEによる安全な初回のインストールやブート後のアプリ利用
- 興味深いテーマを取り扱うBoF
  - mls （Messaging Layer Security)
    - 今風なセキュリティ要件を満したイケてる仕様を作っちゃう

Security Areaに関する動向（3/6）

- 似ているようでターゲットの異なるteepとsuitだけど、どちらもWG化されて間もないので今なら追いつける！

IETF101における状況

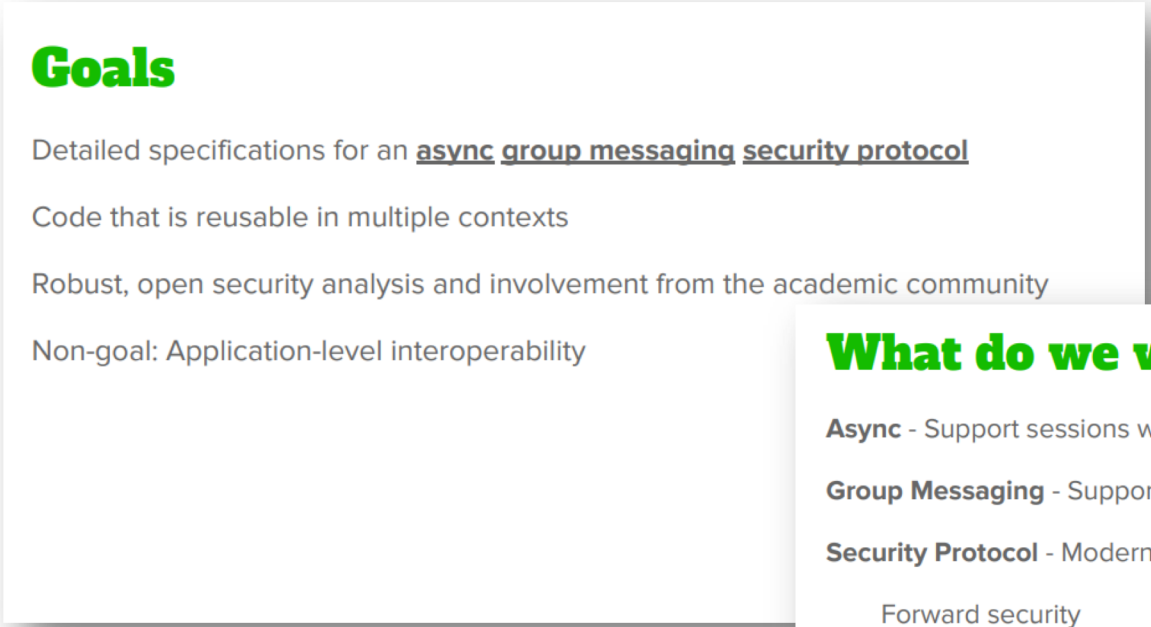
- suit
  - Charterとmilestoneのレビュ
  - ハッカソンレポート
  - アーキテクチャ
    - 「A Firmware Update Architecture for Internet of Things Devices」がWG itemに採択
  - Manifest Format
- teep
  - Charterとmilestoneのレビュ
  - 議論対象のDraft
    - The Open Trust Protocol (OTrP)
    - A Protocol for Dynamic Trusted Execution Environment Enablement

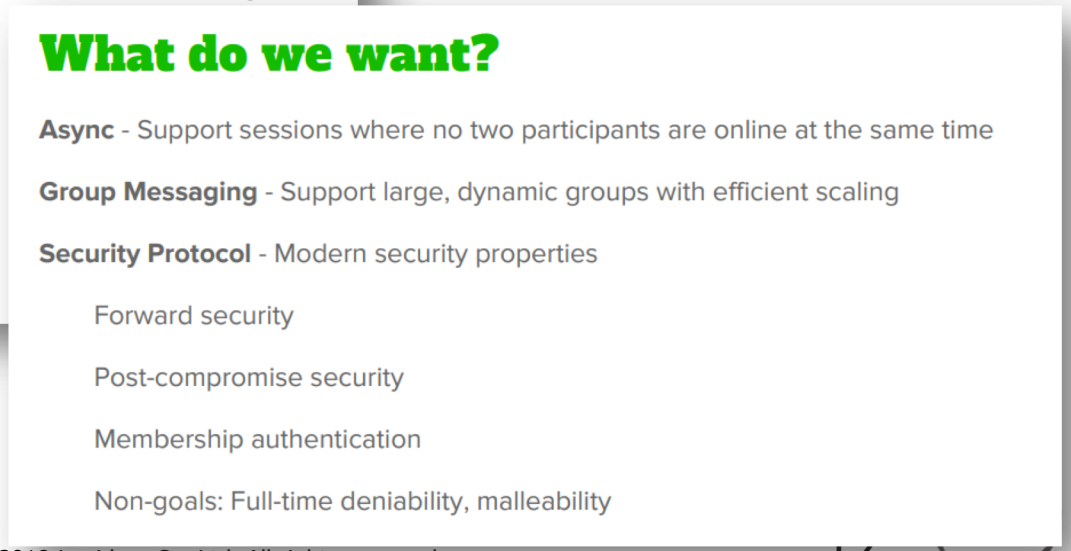
NICT高橋さんの「IETFにおける IoTソフトウェアアップデートに関する検討状況」を参照すると雰囲気が掴めます！

https://www.nic.ad.jp/ja/materials/ietf-report/20171215/20171215-1-takahashi.pdf

Security Areaに関する動向（4/6）

- **トピック3**：Messaging Layer Security
  - モチベ：たくさんメッセージングアプリあるよね？でもプロトコルは同じだったり全く違うものを使っている。それに自分たちで実装はメンテしてて大変そう・・・





https://datatracker.ietf.org/meeting/101/materials/slides-101-mls-mls-bof-slide-deck-00

Security Areaに関する動向（5/6)

- 今回のmls BoFで実施されたことは以下の感じ
  - 既存技術の振り返り＆スコープ
  - アーキテクチャ
    - Google、INRIA、Twitterなど中の人たちが執筆
    - https://datatracker.ietf.org/doc/draft-omara-mls-architecture/
  - プロトコル
    - Cisco、Facebook、Googleなどの中の人たちが執筆
    - https://datatracker.ietf.org/doc/draft-barnes-mls-protocol/
  - 形式検証
  - 恒例の Charterをすり合わそう

メッセージングの主要キャラが登場
&
形式検証を事前に考慮してて素敵！(๑•̀ㅂ•́)و✧

Security Areaに関する動向（6/6)

- BoFなのでWGへ繋がるかどうか・・・
  - 会議室でのコンセンサスとしてはWG化には賛成多数
  - ⇨ IETF102 以降が楽しみ

- 個人的に思うところ
  - モダンな要件を満たすために1970年代に考案された技術を組合せて頑張っている・・・
  - これって「高機能暗号の使うチャンス」なんじゃない？！

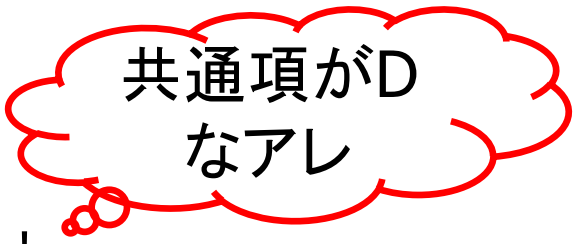
暗号研究者のみなさん･･･今がチャンス！

おしながき

- 目的
- Agendaから振り返るIETF101
- Security Areaに関する動向
- 暗号技術に関する動向
- まとめ

暗号技術に関する動向（1/4）

- 最近のIETFでの暗号技術に関する注目事項は**「耐量子暗号」**になっている
  - 少し前のブーム（？）
    - 安全な楕円曲線パラメータを決めようぜ！
    - ChaCha20-Poly1305をどうするんだぜ？！



- IETFで標準化されている「耐量子暗号」
  - RG itemになっているのはハッシュ関数ベースの署名アルゴリズムたち
    - XMSS: Extended Hash-Based Signatures
    - Hash-Based Signatures
  - 比較
    - IETFではハッシュ関数ベースが人気だけど、NISTのPQCコンテストの応募状況は格子ベース（24件）、符号ベース（16件）、多変数多項式ベース（10件）、同種写像（1件）、その他（16件）という結果であり、格子ベースが大人気

暗号技術に関する動向（2/4）

- 実社会に近づきつつある耐量子暗号
  - secdispatchで「Use of the Hash-based Digital Signatures in the Cryptographic Message Syntax (CMS)」を発表し、lamps WGが適切となる
    - 「これ自体重要な活動だが、Post-Quantum WGを作るようなものではない」by EKR と釘を刺す発言があり、グッときた
- みんな忘れかけているSHA-3（SHAKEだけど）
  - CMSとX509向けのSHAKEに関する準備も進行中
    - Internet X.509 Public Key Infrastructure: Additional SHAKE Algorithms and Identifiers for RSA and ECDSA
    - Use of the SHAKE One-way Hash Functions in the Cryptographic Message Syntax (CMS)

暗号技術に関する動向（3/4)

- Crypto Review Panel 爆誕してた٩(｡•ω•｡)و

Crypto Review Panel

- Formed in September 2017
  - Wiki page for the team: <https://trac.ietf.org/trac/irtf/wiki/Crypto%20Review%20Panel>
  - Mailing list for internal communications was requested
- May be used to review documents coming to CFRG, Security Area or Independent Stream.
- **Lots of good reviews done!**

https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-chairs-slides-00

I-Dを書いていて暗号に困ったら相談ができる仕組み！

暗号技術に関する動向（4/4)

- cfrgについて気になること
  - cfrgってこのスタンスでいいんだっけ？？
    - 将来のインターネットに必要になるような暗号技術を研究しているのか・・・？
    - 新規に考案されたプロトコルとかをレビュするというスタンスで良いのか？
  - もっと効果を考えるのであれば・・・
    - 国際会議で専門家たちのレビュを終え、お墨付きを得た技術をインターネットにどう活かすか？を検討した方がいいなじゃないかなと思った

おしながき

- 目的
- Agendaから振り返るIETF101
- Security Areaに関する動向
- 暗号技術に関する動向
- まとめ

まとめ

- IETF101 Security Areaと暗号関連について注目ポイントとして気になるところと暗号技術の動向について報告
- 今回、取り上げたテーマ以外にも様々な技術について議論しているよ
  - Security Automation mile, sacm など
  - DDoS対策　dots など
  - セキュアプロトコル　tls, ipsecme など
  - 証明書関連　lamps, acme など

気になるテーマがきっとあるので
気軽にIETFのページを覗いてください！

連絡先

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

お気軽にご連絡ください！

参考情報

- IETF 101
  - https://www.ietf.org/how/meetings/101/
- IETF 101 Agenda
  - https://datatracker.ietf.org/meeting/101/agenda
- IETF 101 Materials (Chair's slide)
  - suit
    - https://datatracker.ietf.org/meeting/101/materials/slides-101-suit-chairs-slides-00
  - teep
    - https://datatracker.ietf.org/meeting/101/materials/slides-101-teep-chairs-slides-02
  - mls
    - https://datatracker.ietf.org/meeting/101/materials/slides-101-mls-mls-bof-slide-deck-00
  - cfrg
    - https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-chairs-slides-00
  - secdispatch
    - https://datatracker.ietf.org/meeting/101/materials/slides-101-secdispatch-chairs-overview-02.pdf