IETF報告会 (98th シカゴ)
SEC関連
～TLS WGとBoF～

株式会社レピダム
菅野 哲

はじめに・・・

急なお客さまからの**招集**が掛かってしまいました・・・。
このことからIETF98 Security Area関連について**情報共有を行うことができません**・・・。

TLS WGの動向を追うのに役立つ情報仕立てで整理しました。参考にして頂けたら幸いです。

ぐぬぬぬ･･･

この人、誰よ？（いないけど）

- 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

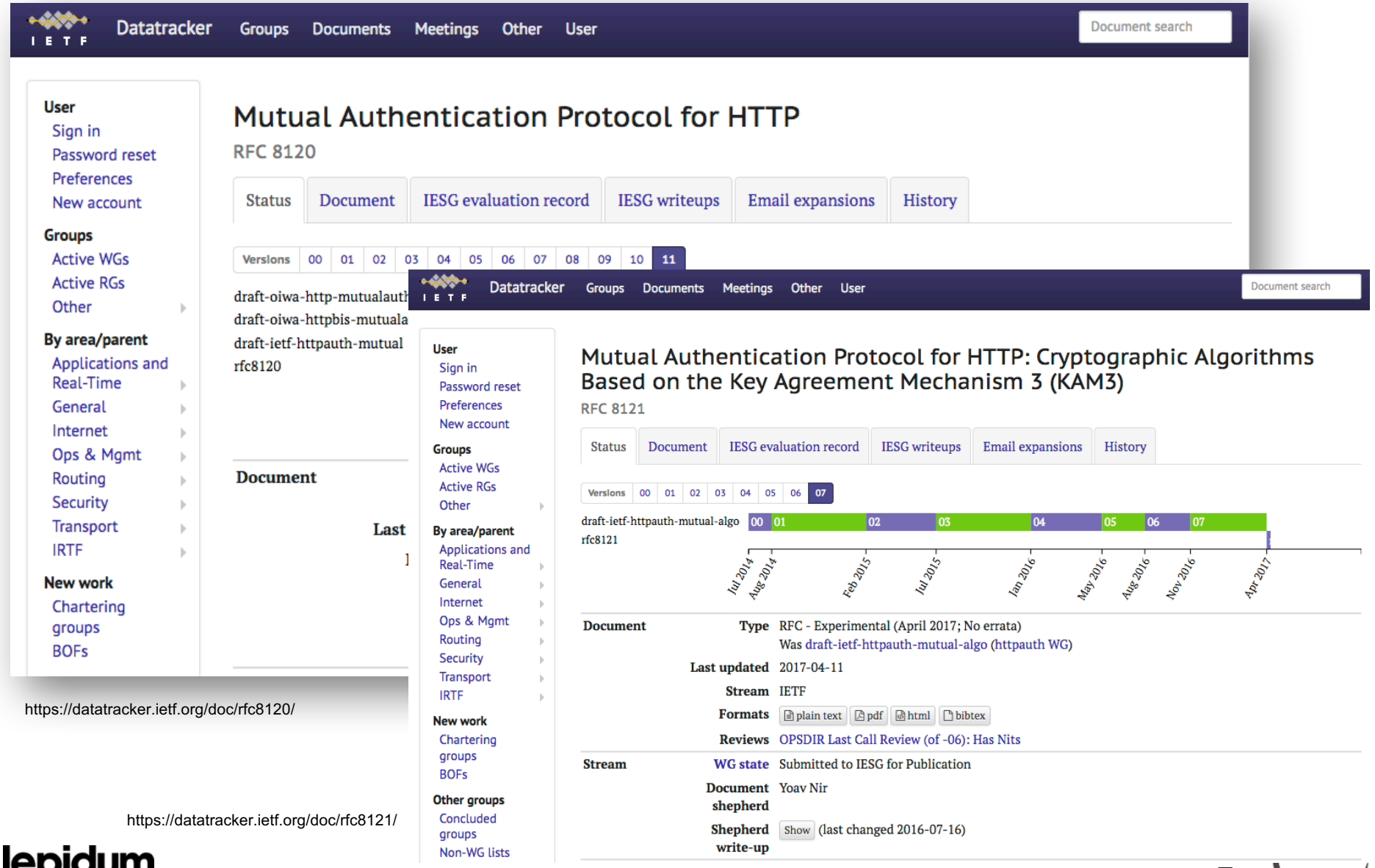
政策&研究アドバイザリ事業
- 事業ニーズの翻訳伝達
- 業界コミュニティからの産業課題摘出
- 諸外国の研究開発動向

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

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

宣伝？：10年越しで、こんな成果が出ました～！



https://datatracker.ietf.org/doc/rfc8120/

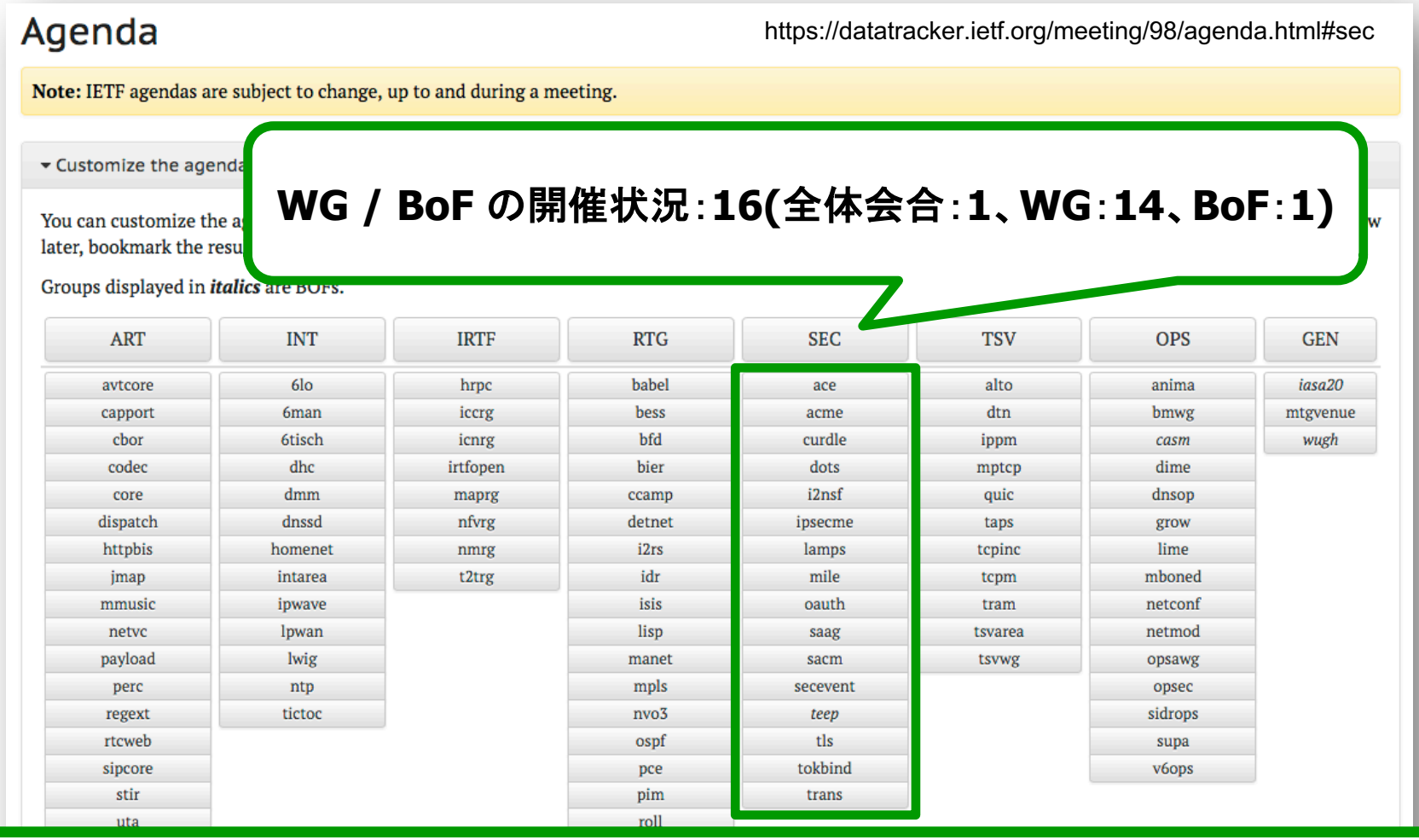
https://datatracker.ietf.org/doc/rfc8121/

lepidum
https://lepidum.co.jp/

IETF98 Security Area

lepidum
https://lepidum.co.jp/

眺めてみると・・・



勢いのある技術分野：
Security Automation関連　と　暗号技術&PKI関連

とは言え・・・注目を集めているのは・・・？！

なんだかんだ言って

TLS 1.3

ですよね～

IETF98 TLS WG（Chair slides）

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

Agenda

Administrivia (5 min)	30min	TLS1.3
Note Well	30min	DTLS1.3
Blue Sheets	15min	A DANE Record and DNSSEC Authentication Chain Extension for TLS
Scribes	15min	Certificate Compression
Document Status (5 min)	15min	Delegated Credentials
	15min	Disposition of additional drafts

30分で終わるくらいにまで収束しつつある！
もう一息！！(`･ω･´)ゞ

Document Status

Adopted Since Last Meeting:
- Example Handshake Traces for TLS 1.3
- Applying GREASE to TLS Extensibility

With/Through IESG:
- ECC CSs for TLS v1.2 & earlier
- RFC 5289 to PS

Completed 2nd WGLC:
- TLS 1.3

Completed WGLC:
- ECDHE_PSK w/ AES-GCM & AES-CCM CSs

In-Progress:
- A DANE Record and DNSSEC Authentication Chain Extension for TLS
- D/TLS IANA Registry Updates

WG Adoption Call ongoing:
- DTLS 1.3

Patiently waiting:
- Exported Authenticators in TLS
- Delegated Credentials
- TLS 1.2 Update for Long-term Support
- TLS Server Identity Pinning with Tickets

2nd WGLC!!

5つのitem候補

雰囲気的には、大きなタスク（TLS1.3）の終わりが見えてきた！
少しのんびりする感じ？

IETF98 TLS WGを大胆にサマる！

- メインな議題であるTLS 1.3の動向は？！
  - 会合では19版について以下の項目について議論し、結果を踏まえて検討しつつ20版で2nd WGLCを終え、IESG へ！？ そろそろ大丈夫・・・？
    - PR #768: D-H key re-use considerations => 棄却
    - PR #762: Short Headers => 棄却
    - Non-X.509 Certificates
      => IoTで使いたいという声やopenpgp cert実装では非推奨やでという意見あり
    - Post handshake client auth
      => オプトアウトするために拡張を送信することで合意
  - Draft-18の実装を確認して先に進めるかどうかを判断する

- その他で更新のあったWG item（I-Ds）
  - DTLS、DNSSEC Chain extension、Certificate Compression、Delegated Credentials について議論を実施

- WG item候補に関する採択における明暗
  - 採択：
    - draft-rescorla-tls-dtls13
    - draft-ghedini-tls-certificate-compression
    - draft-rescorla-tls-subcerts
    - draft-sullivan-tls-exported-authenticator
  - 棄却：
    - draft-gutmann-tls-ltss
    - draft-sheffer-tls-pinning-ticket

詳細を知りたい場合は・・・
https://www.ietf.org/proceedings/98/minutes/minutes-98-tls-00.txt

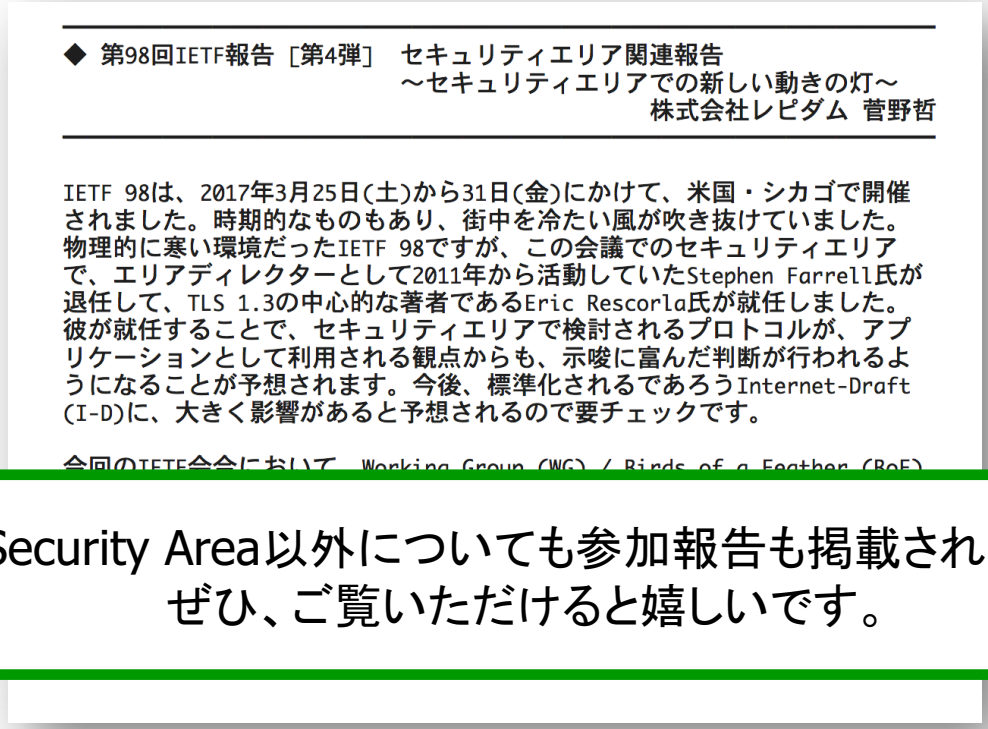
今後のTLS WGってどうなりそう？

- もうTLS 1.3は大丈夫じゃないかなー？
  - ほぼ確定してきたDraftを対象に様々な実装によって相互接続など確認が進んでいる
  - 実装例：
    - wolfSSL
    - https://www.wolfssl.com/wolfSSL/Blog/Entries/2017/5/11_wolfSSL_TLS_1.3_BETA_Release_Now_Available.html?utm_source=dlvr.it&utm_medium=facebook
- TLS 1.3がひと段落するとIoT機器などを考慮してDTLS 1.3にフォーカスが移るだろうなぁ～

暗号利用的な観点で、注目するような新しい技術的要素がないなぁ、、、と寂しい気持ちでいっぱいです。

もう一つのテーマ：Security AreaのBoF

- JPNICさんの第98回 IETF報告において、Security AreaでのBoFに関する動向を整理
  - 個人的に気になるトピックである「信頼」に関するのでとても興味深い！！



◆ 第98回IETF報告［第4弾］ セキュリティエリア関連報告
～セキュリティエリアでの新しい動きの灯～
株式会社レピダム 菅野哲

IETF 98は、2017年3月25日(土)から31日(金)にかけて、米国・シカゴで開催されました。時期的なものもあり、街中を冷たい風が吹き抜けていました。物理的に寒い環境だったIETF 98ですが、この会議でのセキュリティエリアで、エリアディレクターとして2011年から活動していたStephen Farrell氏が退任して、TLS 1.3の中心的な著者であるEric Rescorla氏が就任しました。彼が就任することで、セキュリティエリアで検討されるプロトコルが、アプリケーションとして利用される観点からも、示唆に富んだ判断が行われるようになることが予想されます。今後、標準化されるであろうInternet-Draft(I-D)に、大きく影響があると予想されるので要チェックです。

今回のIETF会合において、Working Group (WG) / Birds of a Feather (BoF)

IETF98 Security Area以外についても参加報告も掲載されているので、
ぜひ、ご覧いただけると嬉しいです。

https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1498.html

参考情報

- IETF98
  - https://www.ietf.org/meeting/98/
- IETF98 Meeting Materials
  - https://datatracker.ietf.org/meeting/98/materials#sec
- TLS WG : Internet Draft
  - TLS 1.3
    - https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/
    - https://github.com/tlswg/tls13-spec
  - DTLS 1.3
    - https://datatracker.ietf.org/doc/draft-rescorla-tls-dtls13/
- IETF98 BoF
  - https://trac.tools.ietf.org/bof/trac/#TimeframeIETF98Chicago

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！