NTTソフトウェア

IETF 報告会 - IETF85@アトランタ編 - SEC関連

菅野　哲

2012.12.21

NTT Software Corporation

http://www.ntts.co.jp/

http://www.nttsoft.com/

Copyright©2012 NTT Software Corporation. All rights reserved.

発表の流れ

- 自己紹介
  - この登壇者って誰よ？
- IETF Security Area
  - どんなところなの？
  - 他Areaとの関係は？
  - 最近のSecurity Areaの動向
- IETF 85
  - どんな雰囲気だったの？
- 参加して考えたこと
  - 最近のSecurity Area は？
- まとめ

Copyright©2012 NTT Software Corporation. All rights reserved.

自己紹介

- 名前
  - 菅野 哲（かんの さとる）
- 所属：
  - NTTソフトウェア株式会社
    - たぶん8年目くらい
  - PKI48暫定センタ
- 主な活動
  - 暗号技術関連のお仕事が中心
    - NTT＆三菱電機が開発したCamelliaの標準化活動
  - IETF初参加は？
    - 72nd Dublin, Ireland

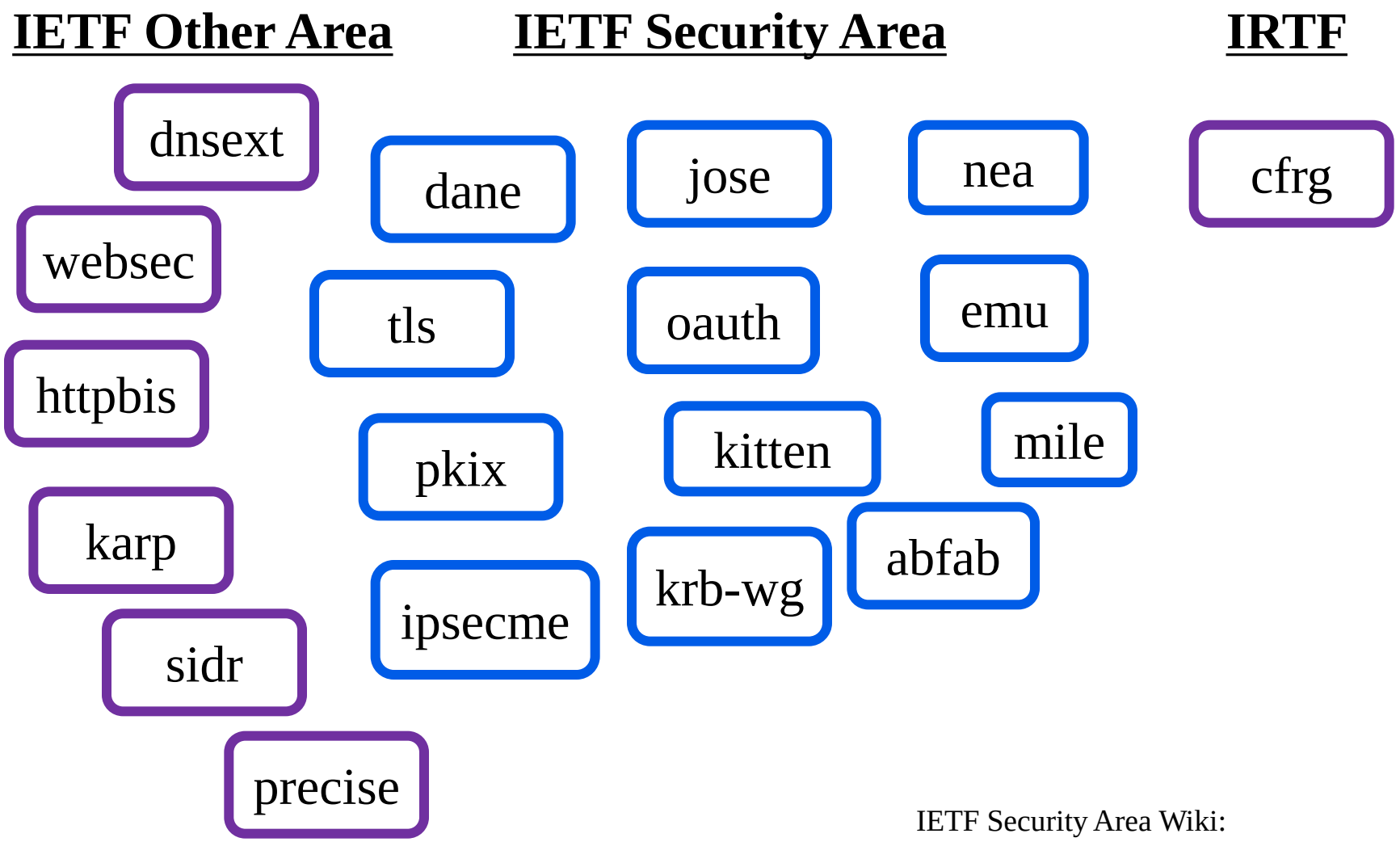
Copyright©2012 NTT Software Corporation. All rights reserved.

IETF Security Area

- ミッション
  - 名前からセキュリティに関する技術を議論／検討
    - 有名どころだと･･･
      - TLS，IPsec，
  - 最近のSecurity Area内の動向
    - プロトコルのメンテナンスを行っているWGが多い
      - tls, ipsecme, pkix, …
- どのくらいWGがあるの？
  - 12WG
    - 通信プロトコル，認証関連，関連する技術
- Security Areaが関係あるWG等は？
  - CFRG（Crypt Forum Research Group）

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF Security Areaとその周辺



IETF Security Area Wiki:
http://trac.tools.ietf.org/area/sec/trac/wiki

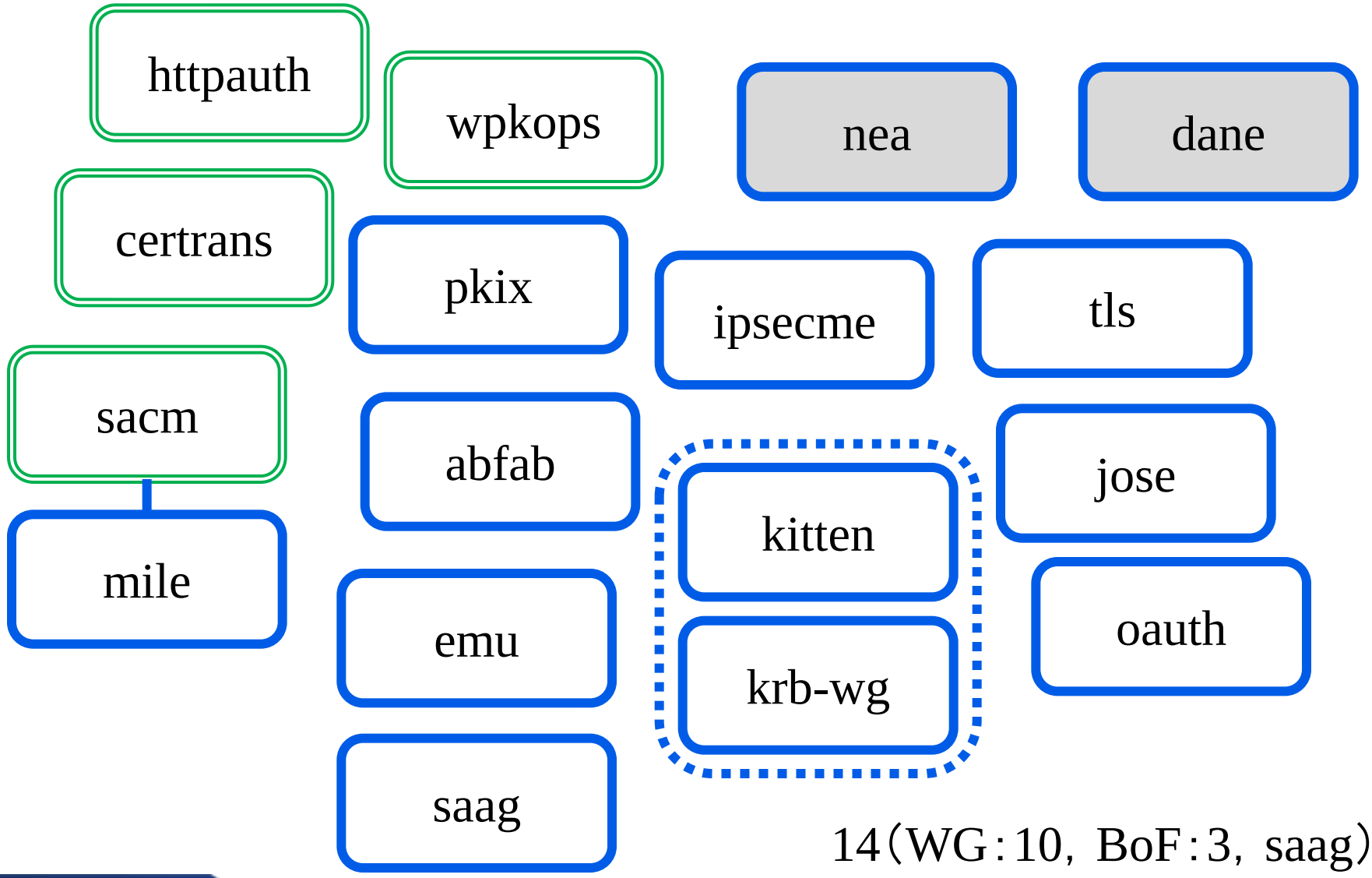
Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th：どんな感じだったの？

- Security Area関連で開催されたWGおよびBoF
  - 14の会議が開催された
    - 内訳　WG：10，BoF：3，saag
- Securityに関連するWGおよびBoF
  - 6WG
    - Webアプリケーション
      - websec
    - 通信プロトコル
      - httpbis
    - ルーティング
      - karp，sidr
    - その他
      - precise

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th Security Area WG/BoF関係図



14（WG：10，BoF：3，saag）

Copyright©2012 NTT Software Corporation. All rights reserved.

今回ピックアップしたWG／BoF

- 取りあえずメジャーなところ
  - tls
- 他WGと毛色の違うもの
  - mile & sacm BoF
  - wpkops BoF & certrans BoF
    - （wpkopsはSecurity Area じゃないけど ☺）
- Security Area特有の議論や番外的な話題
  - ipsecme
  - krb-wg

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th：tls

- tls WG
  - TLSに関連する拡張や安全性等について議論

- 取り扱われたトピックス
  - TLS Cached Info
    - draft-ietf-tls-cached-info
  - The Certificate Status Extension
    - draft-ietf-tls-multiple-cert-status-extension
  - Out of Band Public key Validation
    - draft-ietf-tls-oob-pubkey
  - Origin Bound Certificates
  - DTLS Multicast Security
  - TACK
  - AuthZ extension to use DTCP certificates in TLS

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th：mile & sacm BoF

- mile & sacm
  - 各国・各機関が互いにサイバーセキュリティ情報を交換・共有するための技術
  - 自動的かつ継続的にセキュリティをモニタリング
    - 関連技術：Cybex，SCAP

- 今後，利用が促進されることが期待される分野
  - 攻撃が国境を超えるようなものに…
  - 高度化する脅威に対抗するための基盤

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th：mile

- Agenda
  - Call for Participation: IODEF-bis / IODEF Guidance Survey
    - IODEF（Incident Object Description Exchange Format）を修正したい
      - IODEFを用いて利用状況をヒアリング
      - どうやって利用したいのか
  - IODEF-extension to support structured cybersecurity information
    - IODEFを拡張してSCAPなどの各種セキュリティ関連情報をIODEFに埋め込み可能にする規格
    - 前回，懸念されていたIPR問題は解決
    - 残課題：Normative referenceについてMITRE規格を参照するか
  - IODEF Enumeration Reference Format
    - IODEFのReferenceクラスを利用してCVEなどのidentifierを記述可能とする
    - 今後、working group itemになる見込み
  - Resource-Oriented Lightweight Indicator Exchange
    - Incident情報交換をする際にRESTスタイルを用いてより一般的に適用できるようにする
    - mileで実施すべきことなのか，APP Areaにて議論すべきことなのか，sacmのcontent repository draftと重複がないか確認することに

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th：sacm BoF

- Agenda
  - Use Casesに関する議論
    - sacmで取り組む課題を明確化するためのUse case
    - Use Case
      - 組織内のポリシーなどを鑑みてシステムを評価
      - セキュリティコントロールを継続的にモニタリング
  - Asset Identification Draft
    - アセットを特定する記述手法を規格化
    - アセットはどの範囲を指すのか？
      - Virtual machineなども含まれるのか
  - Continuous Assessment Protocol Draft
    - neaの成果をSCAPにくっつけてできることを探索
      - 現時点でどのように連携するかの具体的な内容は未確定
  - Assets Summary Reporting
  - Content Repository Protocols
  - Vulnerability Model

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th：wpkops BoF & certrans BoF

- CAや証明書に関するBoFが同時開催！
  - wpkops: Web PKI operations
    - https://datatracker.ietf.org/meeting/85/agenda/wpkops/
  - certrans: Certificate Transparency
    - https://datatracker.ietf.org/meeting/85/agenda/certrans/

- それぞれBoFの主張は理解できる
  - あれれ？？　真逆な方向性なのでは？
    - wpkops：WebでのPKIを使いやすくしようぜ！
    - certrans：X.509証明書をもっと厳密に管理しょうぜ！
  - 属するAreaが異なるので何かが起きそう？

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th:（番外）ipsecme

- Security AreaのWGでよく話題に挙がる“暗号アルゴリズム”問題
  - 暗号アルゴリズムの危殆化の話？
    - その場合もあるけど「安全なアルゴリズムに乗り換えましょう！」なので話は簡単
  - バックアップ or 代替アルゴリズム選択問題
    - 世界中で利用される暗号技術は米国標準暗号AES？
      - ひとつだけのアルゴリズムに依存していて大丈夫？
      - 頼っている暗号アルゴリズムの安全性が担保できなくなると・・・
        - » 例えば，新しい攻撃が発明される
    - どのアルゴリズムを選択すれば良いの？
      - 米国標準暗号以外は利用されていない状況では・・・？

Copyright©2012 NTT Software Corporation. All rights reserved.

IETF85th:（番外）krb-wg

IETF85thの会議でRFC editor queueだったI-DがRFC化

Internet Engineering Task Force (IETF)
Request for Comments: 6803
Category: Informational
ISSN: 2070-1721

G. Hudson
MIT Kerberos Consortium
November 2012

Camellia Encryption for Kerberos 5

Abstract

This document specifies two encryption types and two corresponding checksum types for the Kerberos cryptosystem framework defined in RFC 3961. The new types use the Camellia block cipher in CBC mode with ciphertext stealing and the CMAC algorithm for integrity protection.

貢献できた！？

Appendix A. Acknowledgements

The author would like to thank Ken Raeburn, Satoru Kanno, Jeffrey Hutzelman, Nico Williams, Sam Hartman, and Tom Yu for their help in reviewing and providing feedback on this document.

Copyright©2012 NTT Software Corporation. All rights reserved.

参加して感じたこと

- 他エリアに比べて日本からの貢献度が低い？！
  - 標準化活動
    - 個人や他組織と共同での提案活動があまりない
  - Security Areaの日本人参加者が少ない
    - IETF的には日本人の参加者率は2 or 3位なのに･･･
- 若い世代の参加率
  - 欧米，アジア（特に中国）は若い人たちの参加が目立
  - 海外で活躍する技術者の高年齢化･･･
    - e.g., PKI業界

このような現状を打破したい！

Copyright©2012 NTT Software Corporation. All rights reserved.

まとめにかえて

- Security Areaでの活動を知り，興味を持ってもらいたい
  - Securityを軸に様々な領域の議論が行われている
    - 自分の関係するWGがあるはず！？
  - 資料化できないドロっとした話もあり
    - 標準化活動での苦労話…
- IETF Security Areaでの危機感を感じた人募集中

- IETF 86th はOrlandoです
  - 良いところらしいのでぜひ！
  - 登録はコチラ
    - https://www.ietf.org/meeting/register.html

Copyright©2012 NTT Software Corporation. All rights reserved.

ちなみに・・・

Attendance List

IETF 86

Orlando, FL, USA

March 10-15, 2013

Last updated Wednesday, December 19, 2012 at 16:48:42 PST

18 registrations:

Please log in to view profile data:	
Email Address:	
Confirmation Number:	
Submit Login	

Last Name	First Name	Organization	ISO 3166 Code	On-Site	Profile
Baker	Fred	Cisco Systems	US	No	
Barnes	Mary	Polycom	US	No	
Blanchet	Marc	Viagénie	CA	No	YES
Brim	Scott	Internet2	US	No	
Deen	Glenn	NBCUniversal	US	No	
Heron	Giles	Cisco	GB	No	
Housley	Russell	Vigil Security, LLC	US	No	
Jacobsen	Ole	Cisco Systems	US	No	YES
Kanno	Satoru	NTT Software	JP	No	
Lemon	Edward		US	No	YES
Muhanna	Ahmad	Award Solutions	US	No	
Oran	David		US	No	
Palet Martinez	Jordi	Consulintel, S.L.	ES	No	
Penno	Reinaldo	Cisco Systems, Inc	CA	No	
Perkins	Charles	Futurewei	US	No	YES
Resnick	Peter	Qualcomm Technologies, Inc.	US	No	YES
Roberts	Phil	Internet Society	US	No	
YUE	Peiyu		CN	No	

Copyright©2012 NTT Software Corporation. All rights reserved.