IPA
Information-technology Promotion Agency, Japan

インターネットセキュリティの観点からの標準化動向

第60回IETF報告会
2004年10月13日 (水) 14:35-15:20

みやかわ やすお
宮川 寧夫

独立行政法人 情報処理推進機構
セキュリティセンター
情報セキュリティ技術ラボラトリー

1

講演内容

- **一般教養**
  - **歴史と古文**
  - **政治**
- **専門基礎**
  - FYIシリーズ　(近代)
  - BCPシリーズ　(現代)
    - **強いセキュリティ要件**
    - **「セキュリティについての考慮事項」**
  - **セキュリティチュートリアル**
- **専門応用**
  - **セキュリティエリア**
    - PKI X.509

2

一般教養

- **歴史と古文**（RFC 1500まで；1993年 8月以前）
  - RFC 602
    - 「暖炉のそばに靴下を吊るす際にはご注意」
      ("The Stockings Were Hung by the Chimney with Care")
  - RFC 1087
    - 倫理とインターネット
      (Ethics and the Internet)
  - RFC 1108 RFC 1038 を廃止
    - 米国国防総省 インターネットプロトコルについてのセキュリティオプション
      (U.S. Department of Defense Security Options for the Internet Protocol)
  - RFC 1135
    - インターネットの寄生虫病
      (The Helminthiasis of the Internet)
  - RFC 1281
    - インターネットのセキュアな運用のためのガイドライン
      (Guidelines for the Secure Operation of the Internet)

3

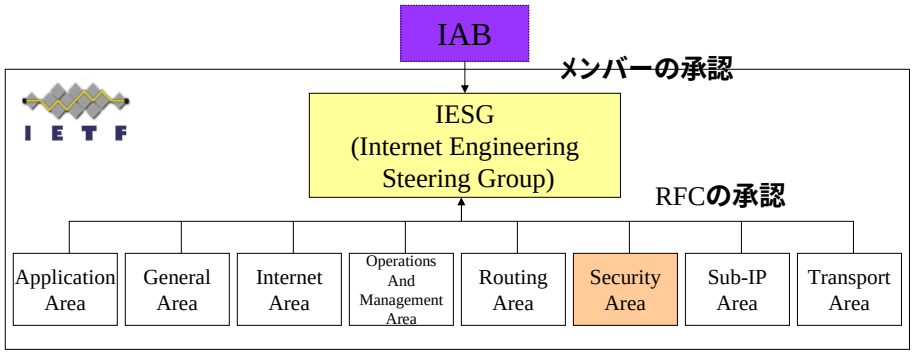
一般教養

- **歴史と古文**（RFC 2000まで；1997年 1月以前）
  - RFC 1535
    - 広く採用された DNS ソフトウェアについてのセキュリティ問題と提案された修正
      (A Security Problem and Proposed Correction With Widely Deployed DNS Software)
  - RFC 1636
    - IAB インターネットアーキテクチャのおけるセキュリティについてのワークショップの報告（1994）
      (Report of IAB Workshop on Security in the Internet Architecture)
  - RFC 1675
    - IPng についてのセキュリティの関心事
      (Security Concerns for IPng)
  - RFC 1750
    - セキュリティのための乱雑性についての推奨事項
      (Randomness Recommendations for Security)
  - RFC 1858
    - IP フラグメントフィルタリングについてのセキュリティ上の考察
      (Security Considerations for IP Fragment Filtering)
  - RFC 1948
    - シーケンス番号攻撃を防ぐ
      （Defending Against Sequence Number Attacks）

4

一般教養

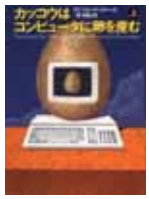
- 政治



5

一般教養の参考文献

- 歴史と古文：時代背景
  - カッコウはコンピュータに卵を産む（上・下）
    - クリフォード・ストール 著（池央耿 訳）
    - 草思社 (ISBN：4-7942-0430-2)
    - 1991年 9月
  - テイクダウン（上・下）
    - 下村 努, ジョン・マーコフ 著（近藤 純夫 訳）
    - 徳間書店(ISBN：4-19-860501-7)
    - 1996年 5月



6

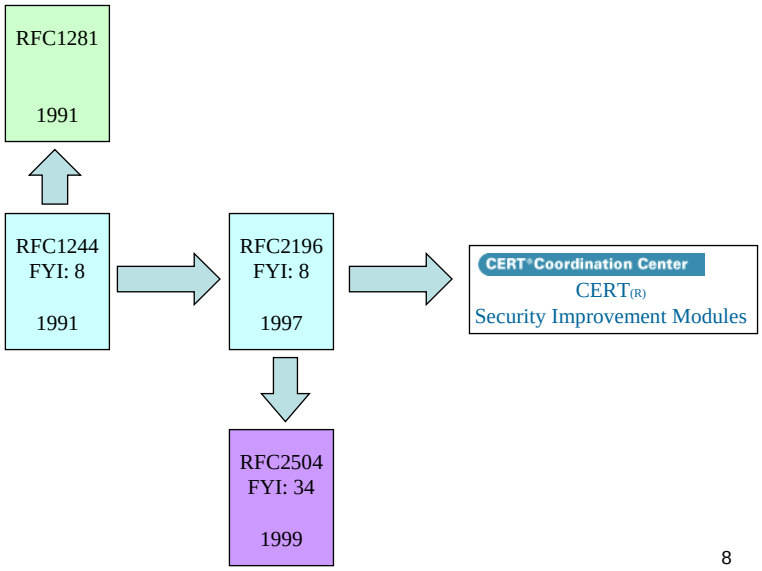
専門基礎 (1)

- FYIシリーズ（近代）
  - 確認：FYIシリーズとは？（RFC 1150; FYI 1）
    - For Your Information/Interest
    - ご興味があれば・・・
    - 情報の中央リポジトリ
    - User Service Area（2002年10月21日をもって終了）
  - FYI: 8 Site Security Handbook の系譜
  - FYI:36 Internet Security Glossary

IETF User Services Area

7

FYI: 8 Site Security Handbook の系譜



8

FYI:36 Internet Security Glossary

インターネット セキュリティ小辞典

- **要旨**
  - **この小辞典** (191**ページの定義と** 13**ページの参考文献**) **は、情報システムセキュリティ用語法について、略語、説明および推奨事項を提供します。**
  - **この意図は、インターネットセキュリティを扱う記述の理解しやすさ** (**特に「インターネット標準文書」の理解しやすさ**) **を向上すること**にあります。
  - **混乱を避けるため、インターネット標準文書は、同じコンセプト** (**概念**) **が述べられているとき、常に同一用語もしくは同一定義を使う必要があります。**
  - **国際的理解を向上するため、インターネット標準文書は、最も分かりやすく辞書のセンスで用語を使う必要があります。**
  - **インターネット標準文書は、特定ベンダー固有または特定ベンダーを選好する用語、あるいは、特定のセキュリティ技術もしくはメカニズムについて既存もしくは将来開発される競合技術に対してバイアスをかける** (**歪める**) **用語を避ける必要があります。**

9

専門基礎 (2)

- BCP**シリーズ** (**現代**)
  - **確認**：BCP**シリーズとは？** (RFC 1818; BCP 1)
    - Best Current Practice：**ベストカレントプラクティス**
    - **現時点における最善の実践**
    - IETF **が支持する技術的関連情報**
  - BCP**の策定状況**
    - **仕様の標準化において**
      - **強いセキュリティ要件**
      - **「セキュリティについての考慮事項」**
    - **セキュリティを確保する運用等のについての**BCP
    - **セキュアプロトコルの相互運用可能性を確保するための**BCP

10

BCPの策定状況

- RFC 2350 BCP：21
  - コンピュータセキュリティインシデント対応への期待
    (Expectations for Computer Security Incident Response)
- RFC 2505 BCP：30
  - SMTP MTA についての spam 対策推奨事項
    (Anti-Spam Recommendations for SMTP MTAs)
- RFC 2644 BCP：34（RFC 1812 を更新）
  - ルーターにおいて指図されるブロードキャストについてのデフォルトを変更する
    （Changing the Default for Directed Broadcasts in Routers）
- RFC 2827 BCP：38（RFC 2267 を廃止）
  - ネットワークのイングレスフィルタリング：発信元 IP アドレスを偽ったサービス妨害攻撃をくじく
    (Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing)
- RFC 3013 BCP：46
  - 推奨される ISP セキュリティサービスと手順
    (Recommended Internet Service Provider Security Services and Procedures)

11

BCPの策定状況（続き）

- RFC 3227 BCP：55
  - 証拠収集とアーカイビングのためのガイドライン
    (Guidelines for Evidence Collection and Archiving)
- RFC 3365 BCP：61
  - IETF 標準プロトコルについての強いセキュリティ要件
    (Strong Security Requirements for Internet Engineering Task Force Standard Protocols)
- RFC 3552 BCP：72
  - RFC の「セキュリティについての考慮事項」についての文章を書くためのガイドライン
    (Guidelines for Writing RFC Text on Security Considerations)
- RFC 3704 BCP：84（RFC 2827 を更新）
  - マルチホームされたネットワークのためのイングレスフィルタリング
    (Ingress Filtering for Multihomed Networks)
- RFC 3766 BCP：86
  - 共通鍵を交換するために使われる公開鍵暗号の強度を判定する
    (Determining Strengths For Public Keys Used For Exchanging Symmetric Keys)

12

強いセキュリティ要件

RFC 3365 BCP：61

- IETF**標準プロトコルについての強いセキュリティ要件**
  (Strong Security Requirements for Internet Engineering Task Force Standard Protocols)

- **要旨**
  - IETF **標準プロトコルが適切な強いセキュリティメカニズムを利用しなければならない (MUST) ことは、**IETF **の総意（コンセンサス）です。**
  - **本書は、この信条についての経緯と理論を記述し、この信条をベストカレントプラクティスとして確立するものです。**

13

「セキュリティについての考慮事項」の書き方

RFC 3552 BCP：72

- RFC **の「セキュリティについての考慮事項」についての文章を書くためのガイドライン**
  (Guidelines for Writing RFC Text on Security Considerations)

- **要旨**
  - **すべての** RFC **には、「セキュリティについての考慮事項」の章をもつことが要求されています。**
  - **これまで、このような章の記述は、十分ではありませんでした。**
  - **本書は、**RFC **著者に良い「セキュリティについての考慮事項」の章の書き方についてのガイドラインを提供します。**

14

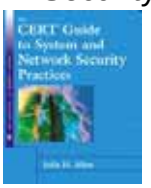
専門基礎 (3)

- セキュリティチュートリアル
  - Jeffrey Schiller版
    - 「セキュアプロトコルを設計する」
  - Radia Perlman版
    - 「ネットワークセキュリティプロトコル：入門編」
- 「第59回IETF韓国会合」SAAG
  - インターネットセキュリティプロトコルの自動検証プロジェクトが紹介された。
    - AVISPA (Automated Validation of Internet Security Protocols and Applications):
      - http://www.ietf.org/proceedings/04mar/slides/saag-1/index.html
      - http://www.avispa-project.org/

15

専門基礎の参考文献

- FYIシリーズ
  - CERT(R) Security Improvement Modules
    http://www.cert.org/security-improvement/
    1. Detecting Signs of Intrusion (1997)
    2. Security for Information Technology Service Contracts (1998)
    3. Securing Desktop Workstations (1999)
    4. Preparing to Detect Signs of Intrusion (1998)
    5. Responding to Intrusions (1999)
    6. Securing Network Servers (1999)
    7. Deploying Firewalls (1999)
  - The CERT Guide to System and Network Security Practices
    - by Julia H. Allen
    - Addison-Wesley Professional
      (ISBN: 020173723X)
    - June 7, 2001



16

専門基礎の参考文献

- BCPシリーズを読む前に
  - 基礎からわかるTCP/IPセキュリティ実験
    - 寺田 真敏, 萱島 信 著
    - オーム社 (ISBN4-274-06382-8)
    - 2000年 9月

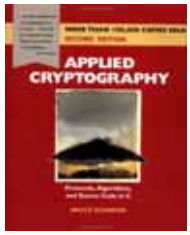
- セキュリティチュートリアルと共に
  - 図解雑学 暗号理論
    - 伊藤 正史 著
    - ナツメ社 (ISBN4-8163-3465-3)
    - 2003年 3月

17

専門基礎の参考文献

暗号技術の応用についての理解を深めるために

- Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition
  - by Bruce Schneier
  - Wiley (ISBN: 0471117099)
  - October 18, 1995
  - 邦訳版「暗号技術大全」



18

専門応用

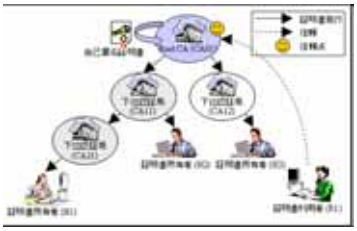
- **セキュリティエリアの今**
  - **ディレクター**：Russell Housley, Steven Bellovin
  - **ワーキンググループ**：
    - enroll Credential and Provisioning
    - idwg Intrusion Detection Exchange Format
    - inch Extended Incident Handling
    - ipsec IP Security Protocol
    - ipseckey IPSEC KEYing information resource record
    - ipsp IP Security Policy
    - isms Integrated Security Model for SNMP
    - kink Kerberized Internet Negotiation of Keys
    - krb-wg Kerberos WG
    - ltans Long-Term Archive and Notary Services
    - mobike IKEv2 Mobility and Multihoming
    - msec Multicast Security
    - openpgp An Open Specification for Pretty Good Privacy
    - pki4ipse Profiling Use of PKI in IPSEC
    - **pkix Public-Key Infrastructure (X.509)**
    - sacred Securely Available Credentials
    - sasl Simple Authentication and Security Layer
    - secsh Secure Shell
    - **smime S/MIME Mail Security**
    - stime Secure Network Time Protocol
    - syslog Security Issues in Network Event Logging
    - tls Transport Layer Security

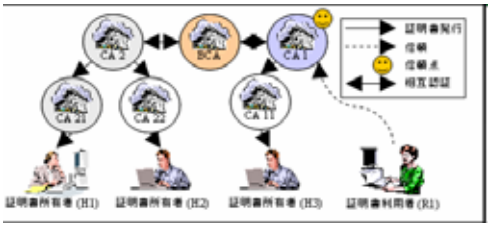
19

専門応用

- **セキュリティエリア**
  - PKI X.509（pkix-wg**は、終息させる予定。**）
    - PKI**は「単純な公開暗号技術の応用」ではない。**
      - **「信用モデル**（Trust Model）」
        - » **基本**：**「単独**CA（**認証局**）**の信用モデル」**
        - » **応用**：**「階層型の複数**CA**の信用モデル」**
          「ブリッジCA**モデル」**

BCPを確立しなければならない！





20

専門応用

- **セキュリティエリア**
  - PKI X.509
    - **ポリシー**（RFC 3647）
      - CP：**証明書ポリシー**
        - » **証明書の目的や利用用途を規定するもの。**
          （**例**：「**本人認証と経路の暗号化**」，「**デジタル署名の検証**」）
        - » **証明書の拡張領域に** OID **形式で記載される。**
      - CPS：**認証実施規定**
        - » CP **をどのように実施するかという、**CA **の運用規定を定めたもの。**
        - » CA **のシステムや運用手順を明示的な文書にして、証明書に記載された** URI **等で利用者に公開する。**
        - » **なお「**CPS **のセキュリティレベルに関する詳細な内容を、非公開とするか／一般に公開するか」は、**CA **のポリシーによって異なる。**

21

専門応用

- **セキュリティエリア**
  - PKI X.509
    - 「**第**60**回**IETF**サンディエゴ会合**」pkix-wg
      - **国際化ストリングマッチング**（UTF8String**文字列比較**）
        - » X.509**証明書上の項目**
        - » **信用パス構築／パス検証のために自動処理**
        - » **日本からの入力が期待されている。**
    - **相互運用可能性の検証には、ツールが必要。**
      - **テストツールおよびテストケースを用意できる主体は限られる。**
      - 「**電子政府情報セキュリティ相互運用支援技術の開発**」
        - » http://www.ipa.go.jp/security/fy14/development/pki/interop.html

22

専門応用

- セキュリティエリア
  - 「第60回IETFサンディエゴ会合」SAAG
    - “Easycert”メーリングリスト
      http://www.machshav.com/pipermail/easycert/
      - PKIやX.509証明書は、使いにくく、配備しにくい。
      - 容易にするためにIETFは何ができるか？
        - » いくつかのBCP（Best Current Practice）？

23

専門応用の参考文献

- PKI X.509
  - PKI技術解説
    - http://www.ipa.go.jp/security/pki/index.html
  - PKIと電子社会のセキュリティ
    - 青木 隆一, 稲田 龍 著（村井 純 監修）
    - 共立出版 (ISBN4-3201-2028-0)
    - 2001年10月
  - PKIハンドブック
    - 小松 文子 他 著
    - ソフト・リサーチ・センター (ISBN4-8837-3142-1)
    - 2000年11月

24

情報処理推進機構の参考ページ

- インターネットセキュリティに関する RFC の日本語訳
  - http://www.ipa.go.jp/security/rfc/RFC.html
- インターネットセキュリティに関する情報収集の報告
  - http://www.ipa.go.jp/security/ietf/ietf.html
- PKI 関連技術情報
  - http://www.ipa.go.jp/security/pki/pki.html

IPA
Information-technology Promotion Agency, Japan

25