JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

暗号技術と情報セキュリティの ミッシングリンク

2013 年 6月 7日

松本 泰 セコム(株) IS研究所

暗号技術と情報セキュリティのミッシングリンク

- 昨年12月に開催したPKI day 2012 の午後の部では、「PKIへの攻撃とその対応」というテーマで、講演とパネルディスカションを行いました。
- ここでは、PKIの仕組みが世の中の信頼の起点となっているが故に攻撃の対象になっている実体と、この対応等の議論を行いました。この対応の難しさの背景の一つに、暗号技術の分かりにくさ、複雑さがあります。
- 今回は、PKIというよりは、社会基盤となるべき暗号技術、社会に役立つ暗号技術を念頭に、「暗号理論からみた理想のセキュリティ」と「実体としての情報セキュリティのベストプラクティス」の間には、大きなギャップがあるのではないか。このギャップを埋める活動が必要ではないかとの認識の元、議論を行います。

暗号技術と情報セキュリティのミッシングリンク

- コーディネータ
  - 松本　泰　セコム（株)ＩＳ研究所/ＰＫI相互運用技術ＷＧリーダ
- パネリスト
  - 神田 雅透 氏　　（独）情報処理推進機構 セキュリティセンター 暗号グループ 研究員
    - 「暗号技術」と「暗号の利用者の視点」（とのギャップ）？？
  - 須賀 祐治 氏　　（株）インターネットイニシアティブ セキュリティ情報統括室 シニアエンジニア
    - 「暗号技術」と「多様化するサイバー攻撃」(とのギャップ)
  - 宮内　宏氏　宮内宏法律事務所
    - 「暗号技術」と「情報セキュリティに関係する法制度」(とのギャップ)

ＪＮＳＡにおける暗号技術関連の活動

- ＰＫＩ day ２０１２　２０１２年１２月13日
  - 午前の部
    - 「我が国における信頼基盤の連携に向けて」
    - モデレータ　松本　パネリスト　宮内宏氏他
  - 午後の部
    - 「ＰＫＩへの攻撃」
    - モデレータ　須賀 祐治 氏　パネリスト神田 雅透 氏 他
- 第２回鍵管理勉強会　２０１２年７月３日
  - 「暗号鍵管理」の技術を中心にした勉強会
- ＪＮＳＡ Press　第３４号　２０１２年９月発行
  - 「暗号技術による個人情報保護の制度と技術の動向」
  - セコム　松本、伊藤

最近の暗号技術に関連する(JNSA以外の）活動

- 新しいCRYPTREC暗号リスト
  - 2002年度策定の電子政府推奨暗号リストを改定
    - その背景
  - 今後の体制？？
- 「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル ～安心・安全のための暗号利用法～」　2013年4月26日　公開　By IPA
  - 「暗号利用マニュアル」として作成
- 暗号の社会的利用推進フォーラム
  - 中央大学の辻井重男先生らが設立
  - MELT upの会（　Management /Market , Ethics, Law system, Technology）
  - 安心・安全の向上には、管理、倫理、法制度、技術を強く連携・融合（melt up）することが不可欠
- 「インフラのゲームチェンジを考えよう　～泥船PKI号、本当に大丈夫？～」
  - 「情報セキュリティシンポジウム道後２０１３」 2013年2月28日～３月1日
  - 司会 ： 株式会社インターネットイニシアティブ　須賀　祐治 氏
  - 司会 ： セコム株式会社　島岡　政基 氏

社会基盤としての暗号技術
Big Picture

デジタル時代の日本の社会？

効率的で、透明性があり競争力のある社会？

目的

デジタル時代の社会サービス

Trust が必要な様々な社会サービス

デジタル時代の社会基盤

暗号技術を利用したエコシステム (のための基盤)

デジタル時代の(信頼のための)フレームワーク

標準化

実装

法制度

デジタル時代の要素技術

コアとなる暗号技術 etc..

ディスカッション

- 個人情報保護法と暗号技術
  - 経済産業省のガイドラインにある「高度な暗号化」の意味するところ
  - 通信中との暗号化(Data in Motion)と、保存されたデータの暗号化(Data at Rest)の違い、暗号化のセキュリティの理解
  - 個人情報保護法の技術ガイドラインは統一されないのか
    - 数多くの主務官庁毎の（技術も含む）ガイドライン
    - 米国の場合、技術ガイドラインは、NISTのガイドラインが参照されることが多い。日本にはNISTに相当する機関は必要ないのか？
  - 「暗号技術データ消去（ Cryptographic Erase ）」は法的に有効か？
    - 個人情報は、暗号化等によって秘匿化されているかどうかを問わない -- では、暗号化鍵を消去したら、個人情報を消去したことになるのか？ -- そもそも破棄のガイドラインがない？
- 暗号技術は本当に情報セキュリティの向上に寄与できるのか？
  - できるとするならば、
    - 何をするべきなのか？
    - どういった活動を行うべきなのか？

参考

PKI day 2013「PKIへの攻撃」2012年１２月13日開催

- 近年、PKIへの攻撃が顕著になっています。例えば、以下の事例があります。
  - 2011年3月Comodo事件：9件の証明書が不正発行
  - 2011年8月DigiNotar事件：500以上の証明書が不正発行
  - 2012年5月に発覚したFlame Malware
- これらの事例では、不正な証明書発行やX.509証明書の偽造等、PKIへの攻撃が行われています。こうして不正に取得された証明書は、Flameで見られるように複雑で高度な攻撃を行うために使われています。これらの事例はたまたま発覚されたに過ぎず、水面下ではもっと多くの攻撃が準備されている可能性もあります。
- また、SSL/TLS、SSHなどのセキュリティプロトコルで利用されている証明書を広く収集して様々な分析が行われています。今年8月にはUSENIX Security SymposiumおよびCRYPTOにて収集された公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題が指摘されました。この問題は正しく鍵生成を行っていないことに起因し、もちろん攻撃の糸口に利用される可能性があります。
- PKIが攻撃されるのは、現在の世の中において、PKIの仕組みが、世の中の信頼の起点として組み込まれていることに他なりません。PKIは、情報化社会の基盤技術ですが、このPKIを代替する技術は考えられず、今後の社会においても信頼の起点であり続ける必要があります。そのためには今後の攻撃に耐えうる技術・運用方法を確立する必要があります。
- 本セッションでは、
  - これらの事件の内容を、その背景も含め正確に理解し
  - 今後の考えられる攻撃を考察し
  - 今後の中長期的な対策について議論します。

http://www.jnsa.org/seminar/pki-day/2012/

情報漏えいを防ぐためのモバイルデバイス等設定マニュアル　２０１３年4月２６日　公開

- 解説編は、暗号設定を適切に実施するために、情報セキュリティの責任者や担当者のみならず、一般従業員層にも出来れば最低限知っておいてほしい暗号化の必要性や仕組み、情報漏えい対策として正しく安全に機能させるために必要なことなどを、平易な表現でまとめています。また、暗号化の設定によって「何をすれば守られ、何が守れないのか」を解説しています。
- 解説編の主な記載項目は以下のとおりです。
- ◆ 情報漏えい対策のために必要なこと
  - 端末ロックだけでは不十分（暗号化の必要性）
  - 暗号化のしくみ
  - 誤った対策により悪用されてしまうケース
- ◆ 正しい対策のために必要なこと
  - なりすましを避けるための利用者認証
  - 端末を常に最新の状態に保つこと
- ◆ 情報漏えい対策の考え方 ・情報価値レベルと対策の最低水準(ベースライン)について
  - 端末、過般媒体に対する対策のベースラインについて　　など

http://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html

ＪＮＳＡ　第２回鍵管理勉強会
２０１２年７月３日開催

- セキュリティプロトコル、デジタル署名、暗号化など暗号技術は、世の中の情報通信基盤に深く取り込まれつつあります。これらの安全性のかなりの部分は、暗号に利用する鍵、すなわち鍵管理の安全性に依存します。
- 例えば、最近話題になっているＢ-ＣＡＳ問題も、鍵管理の安全性の問題と捉えることも出来ると考えられるのではないでしょうか。
- 今回は、主に、デバイスに格納された鍵の鍵管理、および、暗号化による個人情報の保護に関係する、技術、制度の動向を中心に何人かの方にお話し頂き、それを元に今後のあり方をディスカッションします。

http://www.jnsa.org/seminar/seckey/120703/

暗号技術による個人情報保護の制度と技術の動向
JNSA Press　第３４号　２０１２年９月発行

- 個人情報を適切に保護するための暗号技術については、個人情報保護法が施行された当時から現在に到るまで、様々な議論があったようです。個人情報に限らず、暗号技術により情報を保護するためには、「**暗号アルゴリズム**」、「**暗号モジュールの実装**」、「**暗号化に利用する鍵の管理**」、それら全てが適切である必要があります。
- 　7月3日に開催された「JNSA／第2回 鍵管理勉強会」ではこうした暗号技術・鍵管理技術のあるべき姿と、これらの技術が制度にどう組み込まれていくべきか等を念頭に、「暗号技術による個人情報保護の制度と技術の動向」を勉強会のテーマとして取り上げ、議論を行いました。
- 本稿では、鍵管理勉強会の議論も踏まえ、日本と米国の状況を説明し、今後の日本における課題を考察します。

http://www.jnsa.org/jnsapress/vol34/index.html
http://www.jnsa.org/jnsapress/vol34/3_kikou.pdf

インフラのゲームチェンジを考えよう
～泥船ＰＫＩ号、本当に大丈夫？～
「情報セキュリティシンポジウム道後２０１３

- 【ナイトセッション②】
- 「インフラのゲームチェンジを考えよう　～泥船ＰＫＩ号、本当に大丈夫？～」
- 司会 ： 株式会社インターネットイニシアティブ　須賀　祐治 氏
- 司会 ： セコム株式会社　島岡　政基 氏
- ＜概要＞　今のインフラは多様な技術と利害関係者が複雑に絡まり、その世代交代はますます難しくなっています。　このセッションではＰＫＩへの攻撃を起点に暗号やセキュリティプロトコルの世代交代の現状を理解し、各参加者の身近な事例になぞらえるなどして共通的な成功事例を見い出すことを試みます。　さらに、我々はどこまでＰＫＩを捨てられるのか、それとも泥船から抜け出し新たな信頼基盤となる船を模索すべきか皆で想いを膨らませましょう！

http://ehime-it.org/ssd/index.php/progrum-29

個人情報保護法と暗号技術
個人情報保護法の条文

2条 第1項	この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。
20条	個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.htm

個人情報保護法と暗号技術
「個人情報」（法第２条第１項関連）

- 法第２条第１項
  - この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。
- METIのガイドライン
  - **暗号化等によって秘匿化されているかどうかを問わない**（ただし、「2-2-3-2.安全管理措置（法第２０条関連）」の対策の一つとして、高度な暗号化等による秘匿化を講じることは望ましい。）。

http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.htm

個人情報保護法と暗号技術
「安全管理措置」（法第２０条関連）

- 法第２０条
  - 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
- ＭＥＴＩのガイドライン
  - (エ)影響を受ける可能性のある本人への連絡
    - 事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。
    - 高度な暗号化等の秘匿化が施されている場合

http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.htm

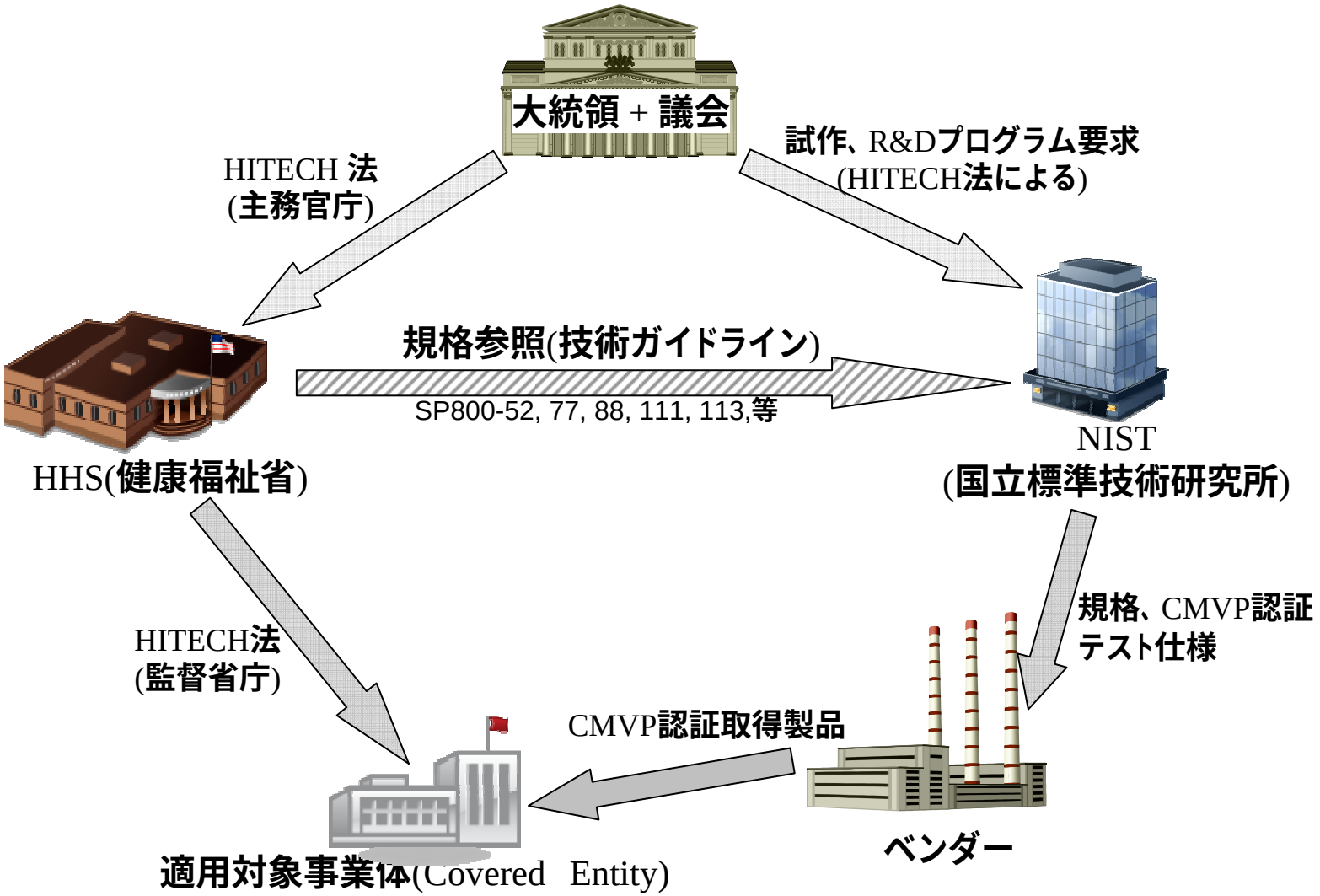
個人情報保護法と暗号技術
データセキュリティのドメインに対応したガイドラインの例

ドメイン	ガイドラインの例	対象
移動中のデータ (Data in Motion)	NIST SP800-52	TLS
	NIST SP800-77	IPsec VPNs
	NIST SP800-113	SSL VPNs
保管データ (Data at Rest)	NIST SP800-111	Storage Encryption for End user
使用中のデータ (Data in Use)	なし **	処理中の秘密情報の扱いなど
データの処分 (Data Disposed)	NIST SP800-88 ***	電子メディアの破壊

** 暗号化状態処理などは、 Data in Use に対応した技術になり得る？？？

*** NIST SP800-88 rev.1 draft 2012年9月 このDraftには、暗号技術による消去 Cryptographic Eraseが記述されている。

個人情報保護法と暗号技術
米国HIPAAにおけるスキーム重要なNISTの役割



「暗号技術による個人情報保護の制度と技術の動向」より

個人情報保護法と暗号技術
ＪＣＭＶＰ・ＣＭＶＰとISMSの日米比較

	JCMVP 日本	CMVP 米国
開始	2006年	1995年
試験機関	4	21 (日本に2)
認証取得組織	10	485
2011年認証数	0	186
2012年認証数	4	70
総認証数	15	1733 (2012.6.20)

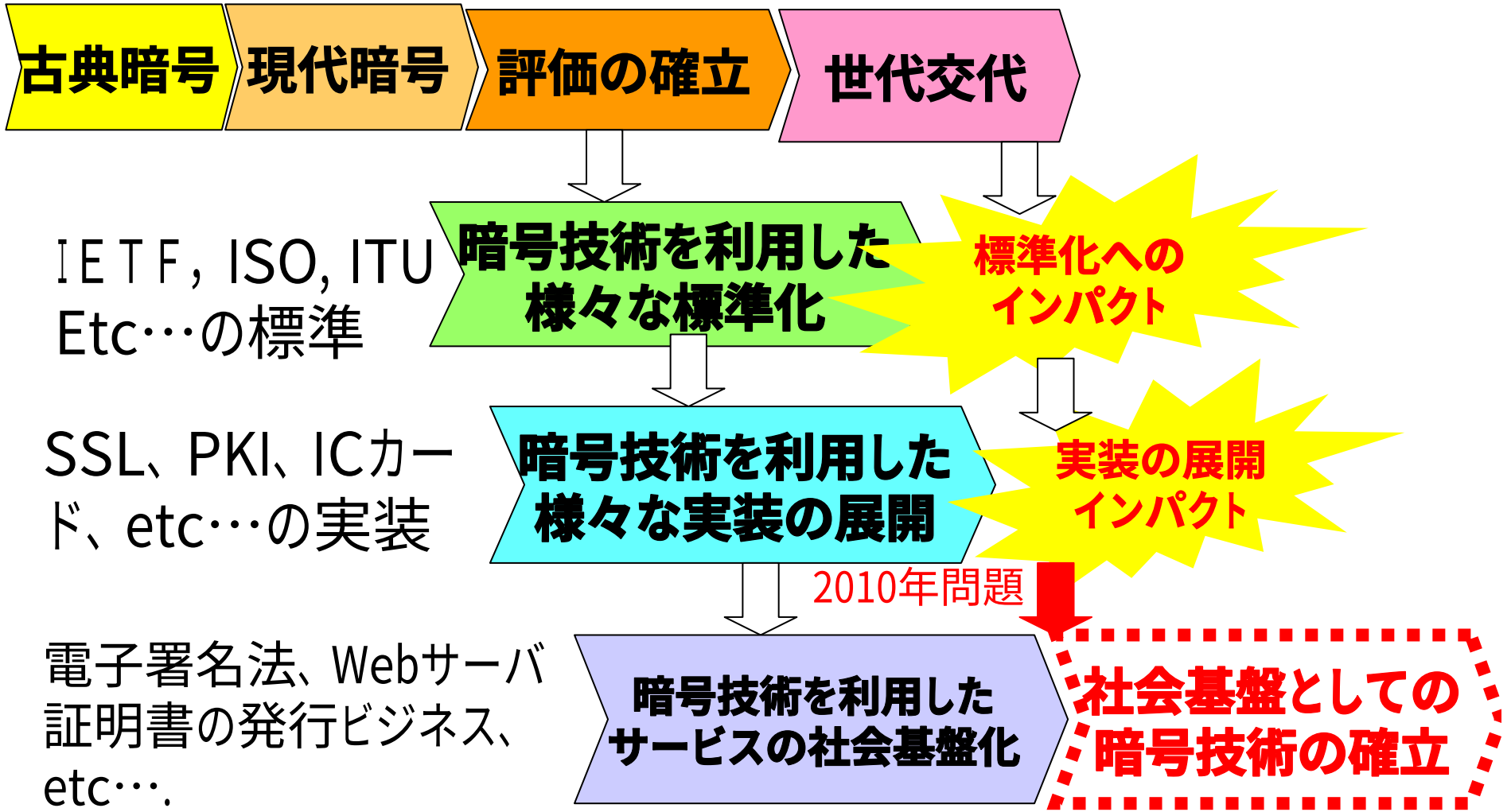
	ISMS 日本 (JIPDEC)	ISMS 米国 (ANAB)
認証機関	26	7
認証取得組織	4061	104

2012年4月での情報
認証収得組織は世界全体で7840

暗号アルゴリムの２０１０年問題
暗号技術の歴史の変遷

JNSA

暗号アルゴリズムの歴史



暗号アルゴリズムの２０１０年問題
ＳＳＬ証明書の暗号アルゴリズムの移行問題
ステークホルダーの声？？

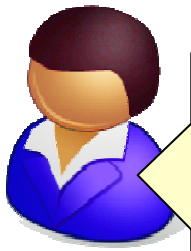
モバイル
キャリア

メモリの関係から、よく使われるルート証明書だけを格納したい。

認証局

「全ての端末をサポート」して欲しいというお客様がいる限り古いルート証明書を使うしかない。

ブラウザベンダ



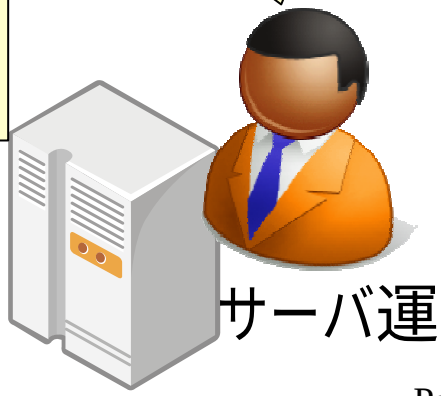
基準を満たしている限り、証明書リストに入れていくけど、暗号のことはどうしましょーね。
後、古いOSは、勘弁してね？

信頼できる証明書なんて分らないからブラウザを信頼するしかない

利用者

ＳＳＬ

ともかくＰＣも携帯も全ての端末をサポートして欲しい



サーバ運営者

暗号アルゴリムの２０１０年問題
暗号技術のレイヤーと移行問題

レイヤー	関係者	一般的な課題	TLS/SSLの事例
アルゴリズム	CRYPTRECやNISTなどの暗号アルゴリズム評価機関	暗号アルゴリズムの評価期間等	N/A
標準	IETFなどの標準化団体	暗号移行可能性の確保	プロトコルの暗号アルゴリズム移行可能性
実装	マイクロソフト社などの製品ベンダ オープンソース	暗号移行可能性の確保	携帯電話の2048ビットやSHA-256対応等
社会基盤	暗号技術を利用する関係者	多数の関係者間の調整	CA/Browser Forumなどの合意の場

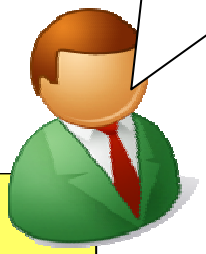
暗号技術と情報セキュリティに関係する法制度のギャップ　--　電子署名法の場合

JNSA

"Rough consensus and running code"

民事訴訟法は228条4項　「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立。。」

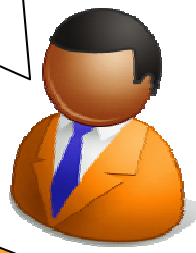
法制度等からニュートラルな技術標準



技術標準

ギャップ

噛み合わない会話
共有されないビジョン



・既存のレガシーな法制度
・様々な管轄官庁の様々な業法

デファクト標準としての実装

対極の実装

紙前提の制度(の電子化)

強い影響

現実の実務からの乖離という問題

「電子署名法」、「e文書法」、「電子公証人制度」、「商業登記に基づく電子認証制度」、「住民基本台帳制度」、etc…

既存の慣習、権益が強すぎる問題

「光の道」で医療問題も教育問題も解決する？

番外編

現在の医療の問題点は、デジタル化以前の問題