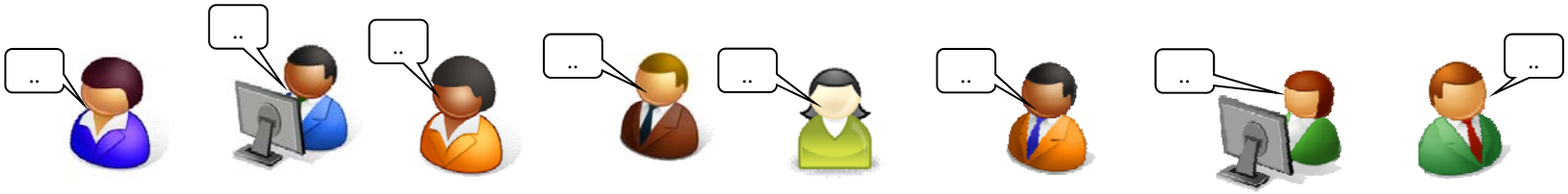
第2回鍵管理勉強会

セコムIS研究所
Intelligent Systems Laboratory

「鍵管理に係る技術と制度の動向」

2012年7月3日

セコム(株)IS研究所　松本　泰



鍵管理に係る技術と制度の動向

セコム IS 研究所
Intelligent Systems Laboratory

- 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。

セコムIS研究所
Intelligent Systems Laboratory

鍵管理に係る技術と制度の動向

- (1) なぜ「鍵管理」なのか？
- (2) 組み込み機器の鍵管理
- (3) 暗号技術を利用した個人情報保護
  - データセキュリティのドメイン
  - Data at Restのセキュリティと 自己暗号化ストレージ
  - 米国 HITECH法の個人情報漏通知ルール
- (4) ディスカション・日本での課題

セコムIS研究所
Intelligent Systems Laboratory

なぜ「鍵管理」なのか？

なぜ「鍵管理」なのか？

セコム IS 研究所
Intelligent Systems Laboratory

- 「鍵管理」は、セキュリティ上の暗黙の前提になっていることが多い。
  - Ex. 「SSLにより経路が暗号化されトラフィックが秘匿される」
- 現状の「鍵管理」は、秘密？が多い？　例えば B-CAS
  - なのでプラクティスが少ない？ノウハウが広く知られていない。
- 「鍵管理」により信頼関係モデルが作られる
- 「鍵管理」はロングタームセキュリティ的課題が多い
- 「鍵管理」は、クラウドコンピューティングの鍵？
  - 「鍵管理」もパラダイムシフト
- 「鍵管理」を制するものは、ビジネスを制する（かもしれない）
  - NFCとか。。。（もしかしたら。。も？？）
- セキュリティアーキテクチャは「鍵中心」「鍵管理」の設計が必要
- 「鍵管理」は、多くの技術的なチャレンジのある領域

（第１回）鍵管理勉強会

セコムIS研究所
Intelligent Systems Laboratory

- 筑波大学　金岡晃
  - 「NIST SP 800-57, SP 800-130ドラフトとそのコメントから鍵管理の全体像を見る」
- タレスジャパン(株)インフォメーションシステムセキュリティ事業部プロダクトマネジャ Jiro Shindo
  - 「鍵管理の標準化動向と必要性」
  - -Global Standard and technology trend for key management, such as KMIP, FIPS 等の動向と技術的なトレンドについて
  - -鍵管理に対する市場からのニーズ、利用のトレンド、必要性について
- JPRS　民田雅人
  - 「DNSSECの鍵管理」
- パナソニック電工　福田 尚弘
  - 「クラウドでの鍵管理」
- みずほ情報総研　　小川 博久
  - 「鍵管理に関する2つの第三者認証制度」

（第2回）鍵管理勉強会

セコム IS 研究所
Intelligent Systems Laboratory

- セコム（株） ＩＳ研究所　松本　泰
  - 「鍵管理に係る技術と制度の動向」（仮題）
- 株式会社トヨタIT開発センター　小熊　寿　氏
  - 「自動車におけるITセキュリティ」（仮題）
- 日本セーフネット　高岡 隆佳 氏
  - （データベース・セキュリティ・コンソーシアム・DB暗号化WGリーダ ）
  - 「データベース暗号化ガイドラインにおける鍵管理」
- 富士通　小谷 誠剛　氏
  - （TCG常任理事、TCG組込み系WGおよび日本支部共同議長）
  - TCG*関連から見る鍵管理
    - Opal HDD(暗号化ディスク)
    - 欧米における個人情報扱い/考え方
- みずほ情報総研　　小川 博久　氏
  - 「暗号化ストレージのプロテクションプロファイルとFIPS140認定の動向」（仮題）
- IPA 独立行政法人情報処理推進機構.　神田雅透　氏
  - 「暗号アルゴリズムと暗号モジュール認証制度の日米共同認証の動向」

セコムIS研究所
Intelligent Systems Laboratory

組み込み機器の鍵管理

様々なデバイスがネットワークに
接続されるM2M時代の鍵管理？？

セコムIS研究所
Intelligent Systems Laboratory

暗号技術を利用した個人情報保護

1. データセキュリティのドメイン
2. Data at Rest と自己暗号化ストレージ
3. 米国 HITECH法の個人情報漏通知ルール

セコムIS研究所
Intelligent Systems Laboratory

暗号技術による秘匿に係るデータセキュリティのドメイン

暗号技術の適応以前に、データセキュリティの要求が整理されないと議論が交錯する？？

セコムIS研究所
Intelligent Systems Laboratory

データセキュリティのドメイン

HITECH Breach Notification Interim Final Rule-(Ⅱ) Guidance Specification（2009年8月24日）

- データ移動（Data in motion）
  - ネットワークを移動中のデータなど
  - ワイヤレスネットワークでのデータ転送も含む
- 保管データ(Data at rest)
  - データベース、ファイルシステム、フラッシュドライブ、メモリ、などのストレジに保管されているデータなど
  - ストレージ盗難対策
- 使用中のデータ (Date in use)
  - 作成、変更、更新、消去の処理を行っている最中のデータなど
  - ＃（主にFIPS140で規定される）
- データの処分(Data disposal)
  - 紙媒体の廃棄、または電子媒体の再利用など

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

セコムIS研究所
Intelligent Systems Laboratory

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)	#DBSCのガイドラインなどが近い	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

セコムIS研究所
Intelligent Systems Laboratory

Data at Restのセキュリティと自己暗号化ストレージ

エンドユーザ向けのソリューションとして、比較的「鍵管理」が容易な、「自己暗号化ストレージ」 の製品が多く出てきた。

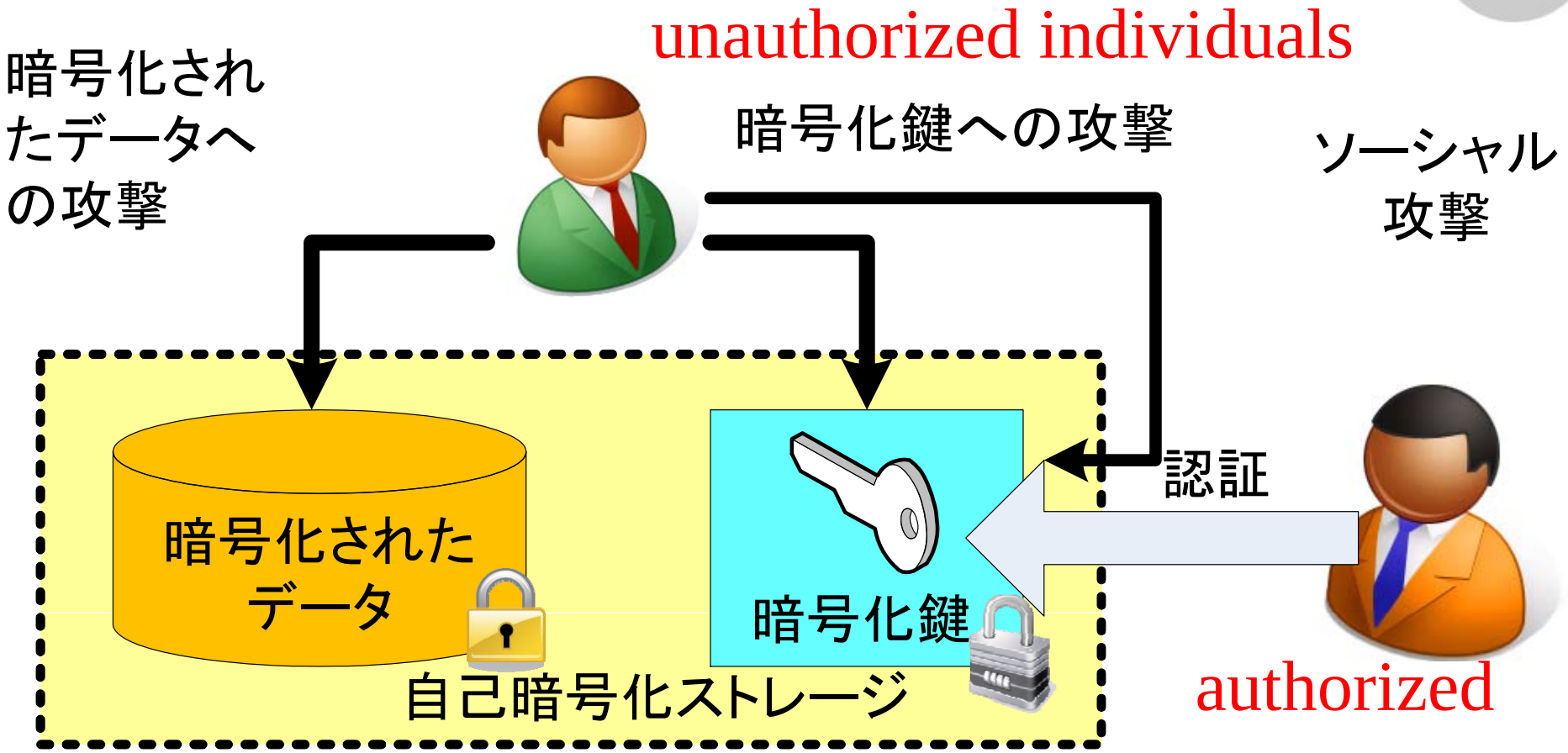
Data at Rest と自己暗号化ストレージ ガイドライン、仕様、ＰＰ、認定製品、、

セコム IS 研究所
Intelligent Systems Laboratory

- ガイドライン
  - NIST SP800-111 Guide to Storage Encryption Technologies for End User Devices 2007年
- 仕様
  - TCG OPAL 自己暗号化ディスク仕様
- プロテクションプロファイル
  - NSAの「暗号化ストレージ（Encrypted Storage）」のプロテクションプロファイル 2011年
    - フルディスク暗号化のプロテクションプロファイル、2011/12/1、バージョン1.0
    - USBフラッシュドライブ用のプロテクションプロファイル、2011/12/1、バージョン1.0
- 認定製品 FIPS140-2
  - TCG OPAL 仕様の自己暗号化ディスク
    - Seagateのハードディスク、サムソンのSSDなどの製品
  - 暗号化USB
    - Etc…

Data at Rest と自己暗号化ストレージ

セコム IS 研究所
Intelligent Systems Laboratory



データの強度　＝　暗号アルゴリムの強度　＋　暗号化鍵の強度

暗号化鍵の強度　＝　鍵管理装置の強度　＋鍵管理の運用の強度？
FIPS140-2的な強度

セコムIS研究所
Intelligent Systems Laboratory

米国 HITECH法の個人情報漏通知ルール
HITECH Breach Notification Interim Final Rule

- 個人情報漏洩に対して厳しい通知義務
- 「個人情報」が守られている状態の定義

米国のHITECH法 - 厳しい通知義務

セコムIS研究所
Intelligent Systems Laboratory

Health Information Technology for Economic and Clinical Health Act

- 2009年に成立した米国再生・再投資法（American Recovery and Reinvestment Act、ARRA）の一部として成立したHealth Information Technology for Economic and Clinical Health （HITECH） Actでは、HIPAA遵守義務がある医療機関・保険者などの組織に対して、情報通信の機密性に関する追加要項が課せられている。
- 中でも、特に個人情報・プライバシー保護との関連性が高い要項として、同法は**保護医療情報（PHI）が漏洩**した場合には**対象者全員への通報を義務付ける**とともに、うち**500人分以上のPHIの漏洩した場合に、HHS（Department of Health and Human Services）及びメディアに対して通報を行うよう義務付けて**いる、という点がある。

PHI：protected health information

出典： ニューヨークだより 2012 年 6 月
米国における個人情報・プライバシー保護・活用の動向
http://www.ipa.go.jp/about/NYreport/201206.pdf

セコムIS研究所
Intelligent Systems Laboratory

HITECH Breach Notification Interim Final Rule

- 情報が安全でなく(unsecure)、HHS 及び FTC (Federal Trade Commission)に通報義務が発生する事態を明示するため、HHSはPHIについてのガイドラインを更新し、認証されないユーザが使用、判読、または復号できなくするための、暗号化と破棄についての技術と方法論を記載している
- 上記でHHSとFTCは、それらの情報が漏洩しても、ガイドラインに記載される方法による暗号化又は破棄が施されているならば、安全(secure)な医療情報であるとしている

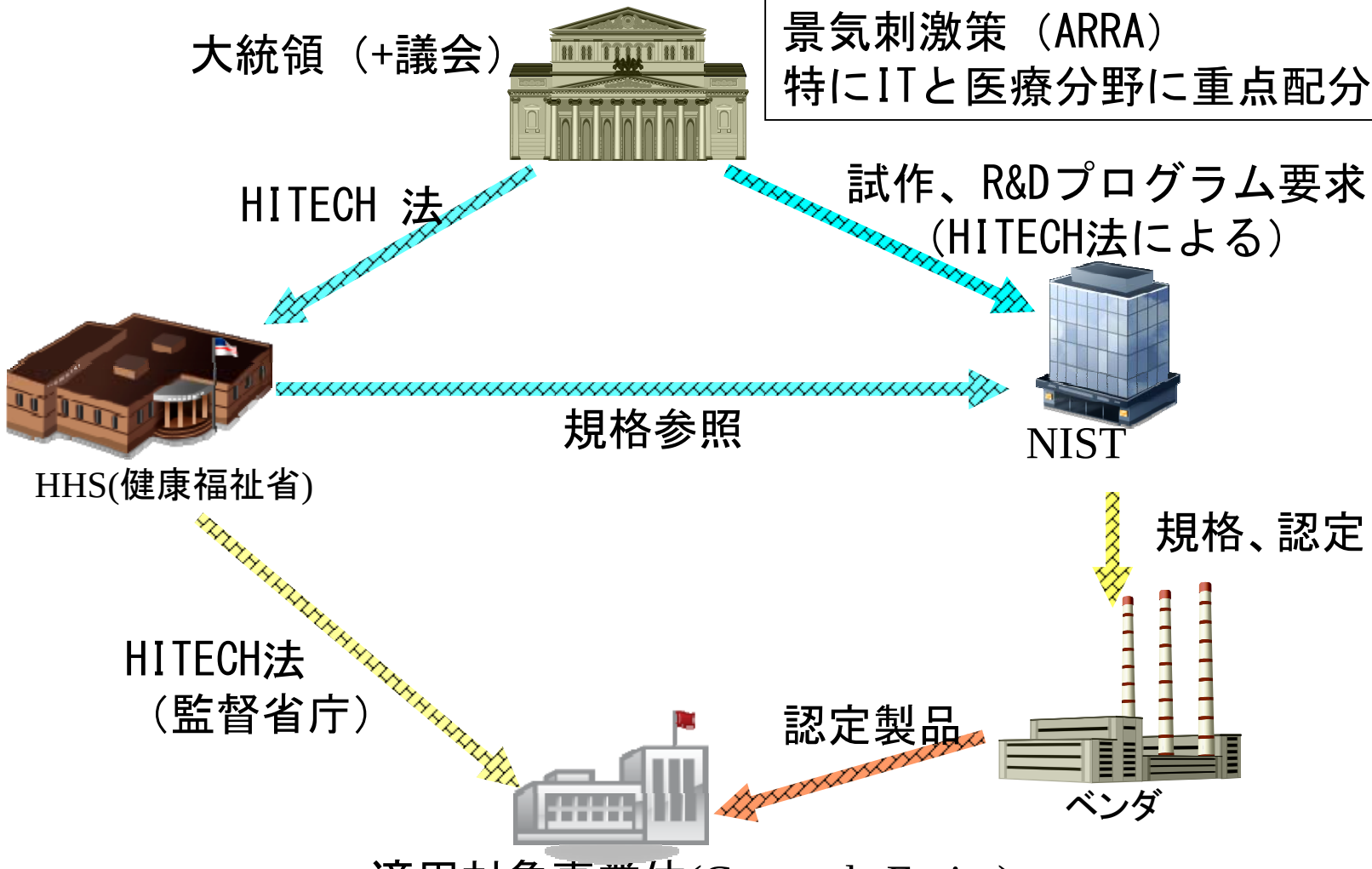
HITECH Breach Notification Interim Final Rule

- (a) HIPAA遵守義務で記述される暗号化された電子PHIについて、…（略
  - (i)有効な手続きで暗号化された「保管データ(data at rest)」はNIST SP800-111 “Guide to Storage Encryption Technologies for End User Device”が該当する
  - (ii)有効な「移動中のデータ(data in motion)」は、NIST SP800-52 “Guideline for the Selection and Use of Transport Layer Security (TLS) Implementation”, 800-77 “Guide to IPsec VPNs”, 800-113 “Guide to SSL VPNs”,その他FIPS 140-2認定を適切に使う事により満たす
- (b)PHIが保存または記録された媒体は、以下の方法の何れかで破壊されないといけない、これは「データ破棄(data destruction)」を意味する
  - (ii)電子媒体は、NIST SP800-88 “Guidelines for Media Sanitization”により、PHIが復元できないように、削除、消去、又は破壊されなければいけない。

情報セキュリティからみた HITECH 法のスキーム

セコムIS研究所
Intelligent Systems Laboratory

2009年、オバマ政権下の
景気刺激策（ARRA）
特にITと医療分野に重点配分



セコムIS研究所
Intelligent Systems Laboratory

ディスカション・日本での課題

技術と法制度を噛み合わせることは
可能なのか？

日本における課題

セコム IS 研究所
Intelligent Systems Laboratory

- 暗号技術に対する誤解？
  - （学術系における）「暗号が破られた」という意味
    - ex.　SHA-1が破られた。
  - 所詮、暗号は破られると言う認識
    - B-CASの暗号が破られた！！
  - 「所詮、技術（だけ）では情報は守れない」という意見
    - これは正しいが、「暗号鍵管理技術」による運用、管理（含む証跡管理）の重要さが認知されていない。
- 暗号技術のバランスの悪さ（鍵管理の観点が希薄）
  - 「鍵管理」の観点が希薄
    - なので、実際に暗号技術を応用したシステムのセキュリティが破られる。

日本における課題　その2

セコムIS研究所
Intelligent Systems Laboratory

- 強制力のないガイドラインや認定制度
  - 「民間を規制しない」「技術の中立性」等という理由
- 技術のガイドラインも管轄官庁毎
  - 似て非なる技術ガイドライン
- その結果？？
  - 国内は、レモン市場化？？、オレオレ化？？
  - 対外的には、競争力のあるソリューションが出てこない？
- 暗号技術に係る政策的判断の不在???
  - CRYPTRECの推奨暗号リスト,JCMVP,CC
- その他
  - Cryptographic Eraseの法的な扱い

参考文献

- HITECH法, PUBLIC LAW 111-5, Sec.13400, 123 STAT. 258, FEB. 17, 2009
- HITECH Breach Notification Interim Final Rule, Federal Register, Vol. 74, No. 162, Monday, August 24, 2009.
- 個人情報保護に関する法律についての経済産業分野を対象とするガイドライン, 厚生労働省・経済産業省告示第2号, 2009年10月9日.

セコムIS研究所
Intelligent Systems Laboratory

BackupSlide

個人情報保護法
「個人情報」（法第2条第1項関連）

セコム IS 研究所
Intelligent Systems Laboratory

- 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。）。

個人情報保護法
「安全管理措置」(法第20条関連)

セコムIS研究所
Intelligent Systems Laboratory

- 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

電子署名ってどうして
こんなに面倒なの？

セコムIS研究所
Intelligent Systems Laboratory

「電子署名法等の課題」

（標準）技術
はあります

法律は
こうなってます

ギャップ

2012年現在の状況？

？？？

セコムIS研究所
Intelligent Systems Laboratory

"Rough consensus and running code"

法制度等から
ニュートラルな
技術標準

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。。」

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

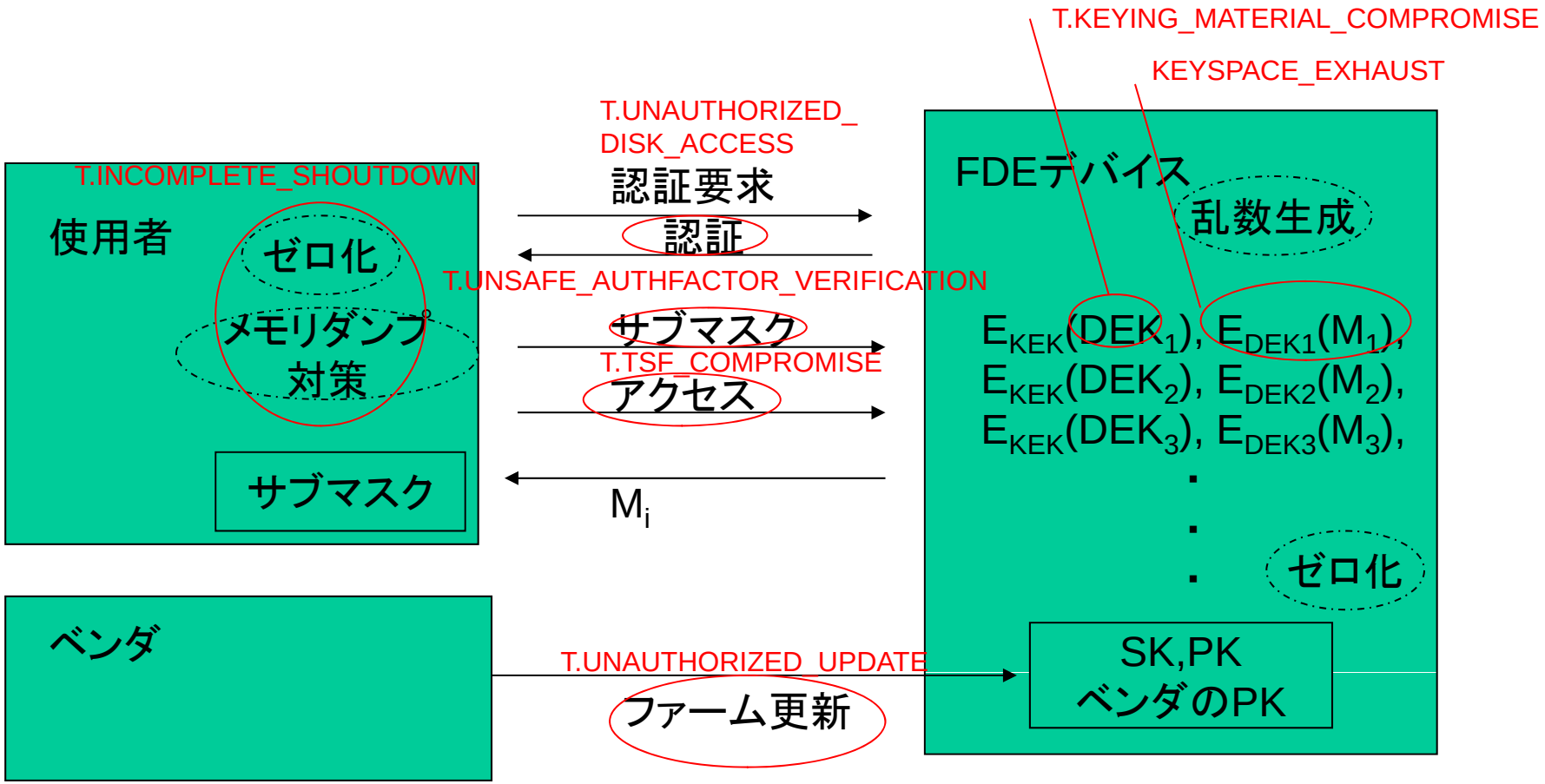
「光の道」で医療問題も教育問題も解決する？

番外編

現在の医療の問題点は、デジタル化以前の問題

セコムIS研究所
Intelligent Systems Laboratory

Data at Rest と自己暗号化ストレージ



※サブマスクを1つ以上使いKEK導出
※認証はサブマスクの安全性が下がらない方法で

JCMVP・CMVPとISMSの日米比較

セコムIS研究所
Intelligent Systems Laboratory

	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