信頼される安心を、社会へ。
SECOM

第３回　鍵管理勉強会概要（オンライン開催）

2020年10月13日

セコム（株）IS研究所　松本　泰

第３回　鍵管理勉強会概要（オンライン開催）

- 自動車、暗号資産システム等の様々な分野のシステムに暗号技術が組み込まれ／利用されると同時に、様々なシステムの至る所に「暗号鍵」が組み込まれるようになってきました。
- この際、暗号鍵管理は、これらのシステムのセキュリティの要となります。しかし、この暗号鍵管理がどのように設計され運用されるべきか、なかなか分かりづらいところがあるのではないでしょうか。
- こうしたことを背景に2020年7月7日に、CRYPTREC/IPAから暗号鍵管理ガイドラインが公開されました。
- 本勉強会では、この暗号鍵管理ガイドラインを中心に、暗号鍵管理のあるべき姿、設計の方法論、実装のあり方などを議論します。

第３回　鍵管理勉強会概要（オンライン開催）　本日のAgenda

- 【講演1】「暗号鍵管理の重要性」
  - 講師：JNSA 標準化部会PKI相互運用技術WGリーダー／セコム株式会社IS研究所　松本 泰 氏
- 【講演2】「暗号鍵管理システム設計指針（基本編）概要」
  - 講師：IPA(独)情報処理推進機構　神田 雅透 氏
- 【講演3】「暗号鍵管理に必要な仕組み 」
  - 講師：IPA(独)情報処理推進機構/セコム株式会社 IS研究所　伊藤 忠彦 氏
- 【講演4】「暗号鍵管理のためのHSM（仮題）」
  - 講師：タレスジャパン株式会社　舟木 康浩 氏
- 【パネルディスカッション】「様々なシステムにおけるセキュリティの要となる暗号鍵管理」
  - ファシリテーター
    - 松本 泰氏　（JNSA 標準化部会PKI相互運用技術WGリーダー／セコム株式会社IS研究所）
  - パネリスト
    - 林 浩史氏（デロイト トーマツ サイバー合同会社）
    - 神田 雅透氏（IPA(独)情報処理推進機構）
    - 伊藤 忠彦氏（IPA(独)情報処理推進機構/セコム株式会社IS研究所）
    - 舟木 康浩氏（タレスジャパン株式会社）

暗号鍵管理の重要性

2020年10月13日

セコム（株）IS研究所　松本　泰

暗号鍵管理の重要性

- (1) 過去の鍵管理勉強会
- (2) 暗号鍵管理の歴史
- (3) 暗号鍵管理ガイドラインとPKIの鍵管理
- (4) 暗号鍵管理の現在、未来
- (5) まとめ

過去の鍵管理勉強会

- 第１回　鍵管理勉強会
  - 2010年11月22日（月）
  - https://www.jnsa.org/seminar/seckey/101122/
- 第２回　鍵管理勉強会
  - 2012年7月3日（火）
  - https://www.jnsa.org/seminar/seckey/120703/

第１回鍵管理勉強会　10年前の2010年11月22日に開催

【第1回 鍵管理勉強会資料】

- 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」
  kanaoka.pdf [195KB]

- 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
  shindo.pdf [2.2MB]

- JPRS　民田雅人
  「ＤＮＳＳＥＣの鍵管理」
  minda.pdf [443KB]　※2010.11.25更新

- 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」
  ogawa.pdf [544KB]

- パナソニック電工　福田 尚弘
  「クラウドでの鍵管理」
  ※当日配布のみ

https://www.jnsa.org/seminar/seckey/101122/

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　by　金岡 晃 先生　（現東邦大学）

第１回鍵管理勉強会
2010年11月22日に開催

https://www.jnsa.org/seminar/seckey/101122seckey/kanaoka.pdf

第2回 鍵管理勉強会概要

2012年7月3日（火）開催

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」[PDF 859KB]

株式会社トヨタIT開発センター　小熊　寿　氏 [資料なし]
「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）
「DB暗号化と鍵管理の重要性」[PDF 1.87MB]

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[PDF 4.65MB]　※2012.7.10更新

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」
[PDF 556KB]　※2012.7.5更新

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認証制度の動向」
～国産暗号技術はどこに向かえばいいのか？～　[PDF 2.01MB]

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

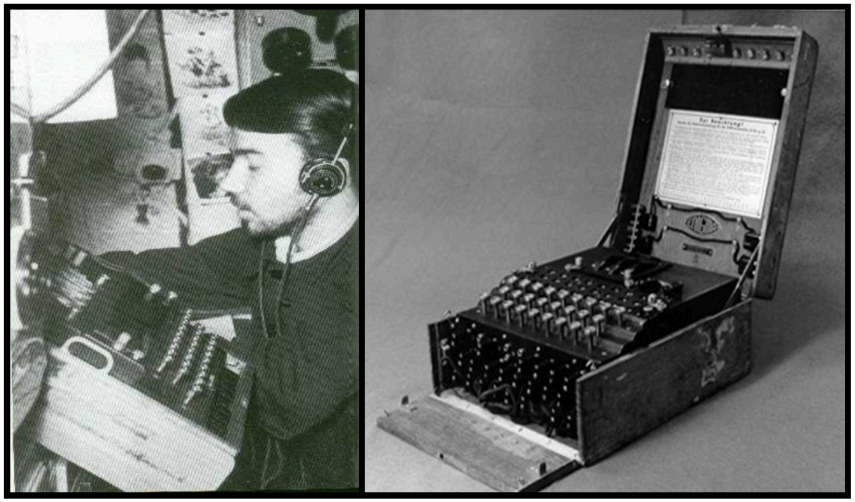
暗号鍵管理の歴史？？

暗号の歴史の話はよく語られるけど

暗号アルゴリズムは秘密、暗号鍵管理も秘密の時代
＃その存在自体も秘密？？？

信頼される安心を、社会へ。
SECOM

GERMAN ENIGMA



A RICH LEGACY

SIGABA

SIGSALY

出典：　NIST　Cryptographic Key Management Workshop 2009
https://csrc.nist.gov/csrc/media/events/cryptographic-key-management-workshop-2009/documents/gillman_petrina_kmwjune09_nsakeymgmt.pdf

鍵の危殆化の理解 - プエブロ号事件の例

セコムIS研究所 Intelligent Systems Laboratory

信頼される安心を、社会へ。 SECOM

- 1968年に、USSプエブロ号（米海軍情報収集船）が北朝鮮に拿捕されました。当時、海軍の船舶はすべて、各種の暗号機のための対称鍵をさまざまなセキュリティレベルで扱っていました。
- それぞれの鍵は毎日変更されました。これらの鍵がどのくらいプエブロ号の乗組員によって破られず、北朝鮮の手に落ちたのかを知る方法がなかったので、海軍はプエブロ号が所持していたすべての鍵が信用できなくなったと仮定しなければなりませんでした。
- 太平洋戦域のあらゆる船舶と沿岸基地（つまり、航海中の船舶を含む数千の施設）は、各施設にコードブックとパンチカードを物理的に運んで、すべての鍵を取り替えなければなりませんでした。

出典：https://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/IW2008-H10-03.pdf

出典： セキュリティの概要 April 29, 2004

http://developer.apple.com/documentation/Security/Conceptual/Security_Overview/Concepts/chapter_3_section_4.html

5

NSA、プエブロ号事件の関連文書を公開　2012年に公開

出典 http://blog.livedoor.jp/intel_news_reports/archives/20385459.html

- 1968年1月、日本海を航行していた米海軍の通信情報船「プエブロ号（USSPueblo）」が、領海侵犯を理由に、北朝鮮の警備艇によって拿捕され、乗組員82名がそのまま連行されるという事件が起きた。いわゆる「プエブロ号事件」と呼ばれるものだが、米国家安全保障局（National Security Agency、NSA）は、このほど、プエブロ号事件に関する文書を自らのウェブサイト上に公開した。
- 文書は、大きく7つのセクションに分けられている。「Background」のセクションでは、プエブロ号が担当した「ピンクルート作戦（Pinkroot Operation）」について、事前に行なわれたブリーフィングなどの文書が紹介されている。この作戦は、1968年1月、長崎の佐世保基地から出航し、日本海において、ソ連海軍の動向監視や北朝鮮軍への通信傍受などを目的としたもので、作戦遂行上、どういったリスクがあるかといったことについて説明されていたことが分かる。
- 「Cryptologic History」のセクションでは、NSA暗号史センター（Center for Cryptologic History）のロバート・ニュートン（Robert E. Newton）によって、1992年に作成されたプエブロ号事件のレポート「The Capture of the USS Pueblo and Its Effect on SIGINT Operations」が公開されている。250ページを超えるもので、プエブロ号の乗組員が事前に十分な訓練を受けていなかった点を批判しながらも、北朝鮮が計画的に拿捕を行なったことも指摘している。

U.S.S. Pueblo

Please Note: These historical documents are PDF images of formerly classified carbon paper and reports that have been declassified. Due to the age and poor quality of some of the PDF images, a screen reader may not be able to process the images into word documents. In accordance with Section 504 of the Rehabilitation Act of 1973, as amended, individuals may request that the government provide auxiliary aids or services to ensure effective communication of the substance of the documents. For such requests, please contact the Public Affairs Office at 301-688-6524.

- U.S.S. Pueblo Release Summary
- U.S.S. Pueblo Release Summary #2
- U.S.S. Pueblo Release Summary #3
- U.S.S. Pueblo Release Summary #4
- U.S.S. Pueblo Release Summary #5

History Papers

- Background
- Cryptologic History
- Damage Assessments
- Director's Material
- Congressional Actions
- Patrol & Capture
- SIGINT Posture
- Pueblo Crew Release & Debriefing
- Lessons Learned
- Questions & Answers
- Chronologies
- North Korean News Broadcasts
- Press Releases & Reactions

https://www.nsa.gov/news-features/declassified-documents/uss-pueblo/

DOCID: 3997434

ACC# 24105
CBoJ 36

~~TOP SECRET~~

38

National Security Agency

Fort George G. Meade, Maryland

CRYPTOLOGIC/CRYPTOGRAPHIC DAMAGE ASSESSMENT

USS PUEBLO

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~LIMITED DISTRIBUTION~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~NOFORN~~

~~TOP SECRET~~

Paper

出典： https://www.nsa.gov/news-features/declassified-documents/uss-pueblo/

現代暗号と暗号鍵管理

- 現代暗号　≒　暗号アルゴリズムは公知
  - 暗号アルゴリズムの客観的な評価
    - #CRYPTREC とはCryptography Research and Evaluation Committees
  - 暗号システム／暗号技術の実装が広く普及するためには、暗号アルゴリズムが秘密でないことが非常に重要
  - → ありとあらゆるものに暗号技術が実装されていった
  - 暗号アルゴリズムは公知　→　守るべき対象としての暗号鍵
- 暗号鍵管理も公知の時代へ　（もしくは客観的評価可能な時代へ）
  - ＃共通鍵系の暗号システムの鍵管理は、現在でも秘密の場合が多いが
  - 暗号鍵管理の客観的な評価が出来なければ、暗号技術に基づくトラストの確立はあり得ない
    - しかし、暗号鍵管理のHowToは、元々、軍／国防上の秘密
    - CRYPTREC も、かつては、暗号鍵管理はスコープではなかった

NISTにおける暗号鍵管理関係のイベント

出典：https://csrc.nist.gov/Projects/Key-Management/Cryptographic-Key-Management-Systems

- Key Management Workshop 2000
- Key Management Workshop 2001
- Cryptographic Key Management Workshop 2009
- Cryptographic Key Management Workshop 2010
- Cryptographic Key Management Workshop 2012
- Cryptographic Key Management Workshop 2014
  - NIST SP 800-152

Key Management Workshop 2000

出典：
https://csrc.nist.gov/Events/2000/Key-Management-Workshop-2000

This workshop focused on the security and interoperability requirements of the Federal government, the key establishment options available, and the planned development of a FIPS that will address those needs.

- **Federal Register Notice**
- **Background and Objectives**
- **Workshop Report**

Presentations

- Government User Perspective (Richard Guida, Treasury)
- Wireless Applications (Doug Rahikka, NSA)
- ANSI X9.42 (Sharon Keller, NIST)
- ANSI X9.44 (Burt Kaliski, RSA Security)
- ANSI X9.63 (Simon Blake-Wilson, Certicom)
- Internet Key Exchange (Sheila Frankel, NIST)
- TLS Protocol (Chris Hawk, Certicom)

Patent Statements

- ANSI X9.42 (Certicom)
- ANSI X9.42 (IBM)
- ANSI X9.63 (Certicom)
- ANSI X9.63 (IBM)

この頃は、
PKI/認証局の鍵管理の標準化が課題だった？？？

暗号鍵管理ガイドラインと PKIの鍵管理

- 2020年公開された「暗号鍵管理ガイドライン」
- このガイドラインは、暗号鍵管理のチュートリアルではない？？
- このガイドラインはPKI・認証局的には、それほど重要じゃない。
- それでは、なぜ「暗号鍵管理ガイドライン」は重要なのか？

暗号鍵管理ガイドライン　2020年7月7日

https://www.ipa.go.jp/security/vuln/ckms.html

- 実際の暗号システムがセキュアに動作し続けるためには、暗号アルゴリズム自体がセキュアであるだけでは不十分で、データが保護される期間中、その暗号アルゴリズムが使用する暗号鍵もセキュアに管理されている必要があります。そのため、暗号鍵やデータのライフサイクルを踏まえた運用、安全な暗号鍵の保管、暗号鍵危殆化時の対策などを行う上で参考となるガイドラインを取りまとめています。
- 「暗号鍵管理システム設計指針（基本編）」の内容
  - 「暗号鍵管理システム設計指針（基本編）」は、あらゆる分野・あらゆる領域の全ての暗号鍵管理システムを対象に、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項を網羅的に提供し、設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を取りまとめたガイドラインとして作成されたものです。
  - 具体的には、暗号鍵管理の必要性を認識してもらうために「暗号鍵管理の在り方（暗号鍵管理の位置づけと検討すべき枠組み）」と、NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の解説書・利用手引書として活用できるように構成した「暗号鍵管理についての技術的内容」とで構成されています。

「暗号鍵管理ガイドライン」の意義　--　松本の理解

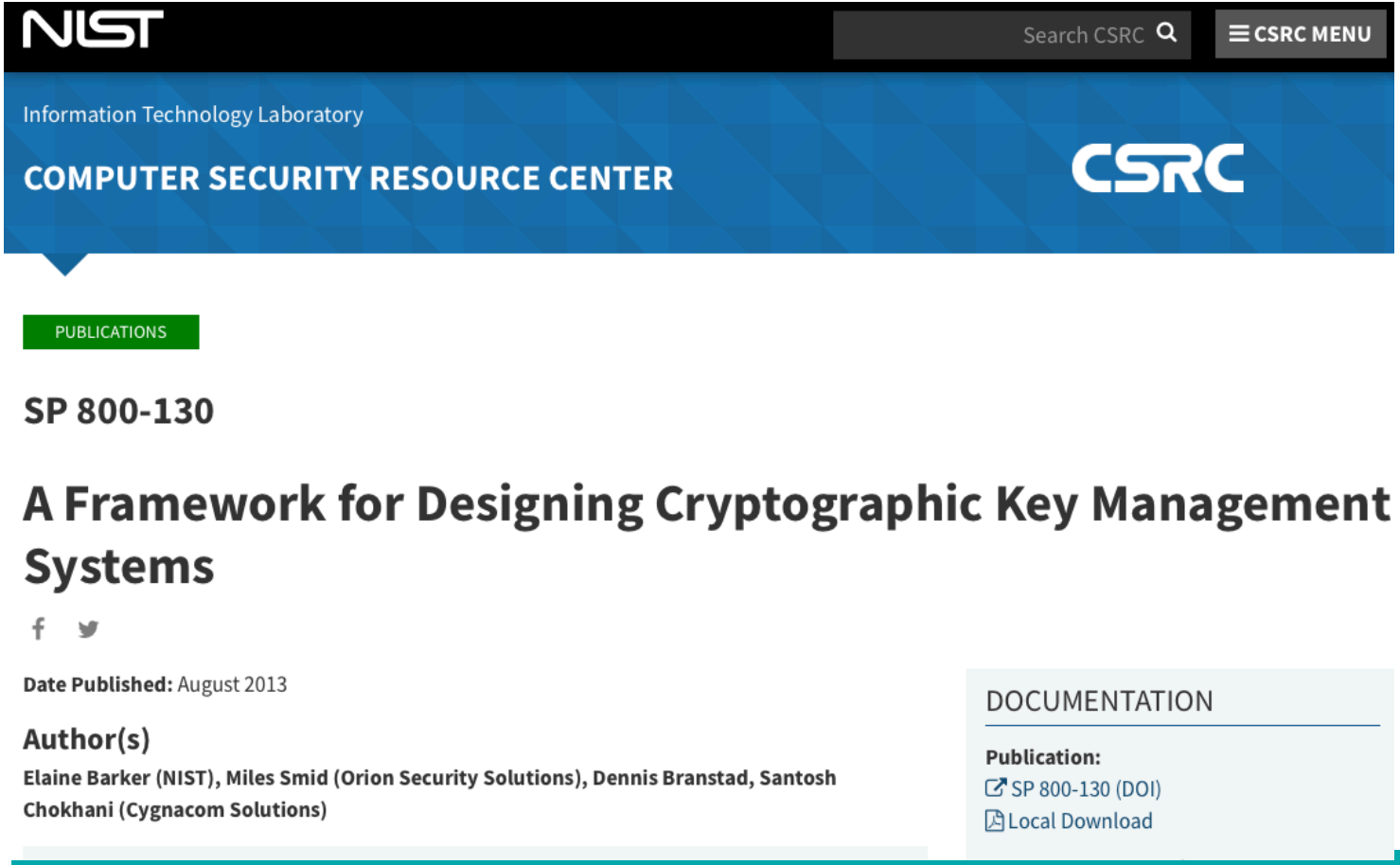
信頼される安心を、社会へ。
SECOM

- 暗号システムにおける暗号鍵管理システム(CKMS)の重要性以前に
  - あらゆる情報システムに暗号システムが組み込まれつつある（ただし多くの場合アドホックに）
  - 現在の情報システムにおいて、暗号鍵管理は、クレデンシャル管理のベースとなり、またこのクレデンシャル管理をベースとして様々なアクセス制御が行われている。
  - そのため、暗号鍵（管理）を中心に添えた情報システムの設計がなされるべきであり、そのためには暗号鍵管理システム(CKMS)が重要な役割を果たす。
  - さらに、Society5.0等の要求に見られるような、多様な分野、多様なステークホルダー間の連携が要求は、（そのためのトラスト確立が必要であり、これには、）今までにない暗号鍵管理システム（の設計）が要求される。　--　自動車/MaaS 、暗号資産、サイバーフィジカルシステム/デジタルツイン、etc..
- フレームワークの重要性
  - 「暗号鍵管理システム設計指針（基本編）」は、SP800-130 のフレームワークを説明するガイドラインであり、そのため、個々の「鍵」の管理方法等について記述されている訳ではないことに注意する必要がある。
  - なので、HowToだけを求める読者の要求には答えられていない。
  - しかし、Society5.0時代における、多様なステークホルダー間のトラストの確立の要求に応えるためには、今までにない新たな情報システム／暗号システムのための「暗号鍵管理システムの設計」が必要であり、フレームワークは、こうした新しい分野においてこそ、非常に重要な役割を果たす。

PKI／認証局の鍵管理（の標準化）-- CPSの公開と基準のためのフレームワーク

- RFC 2527　1999年　-- RFC 3647(2003年)
  - インターネット X.509 PKI 証明書ポリシーと認証実施フレームワーク
    (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework ）　1999年 3月
    - https://www.ipa.go.jp/security/rfc/RFC2527JA.html
  - Santosh Chokhani　CygnaCom Solutions, Inc.,　W. Ford　VeriSign, Inc.
  - 4.6　技術的なセキュリティ統制
    - https://www.ipa.go.jp/security/rfc/RFC2527JA.html#46
    - 4.6.1 鍵ペア生成とインストール
      4.6.2 プライベート鍵の防護
      4.6.3 鍵ペア管理の他の側面
      4.6.4 アクティヴェーション データ
      4.6.5 コンピュータ セキュリ統制
      4.6.6 ライフサイクル セキュリティ統制
      4.6.7 ネットワーク セキュリティ統制
      4.6.8 暗号化モジュール エンジニアリング統制
- RFC 2527に基づき作成されたCP（ Certification Practices ）
  - 米国　FPKI　CP　　→　1999年頃から

SP800-130　2013年8月発行

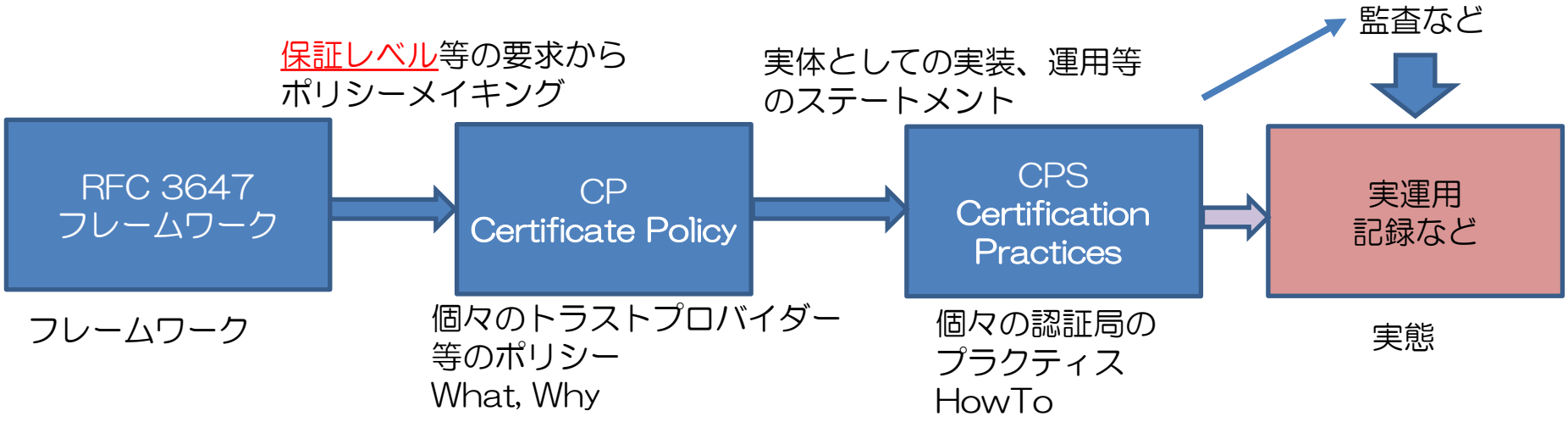


- Elaine Barker
- Santosh Chokhani

フレームワークはとっても難しい

＃肝心なことが書いてない？？？、その価値もすぐにはわからない？？？

- PKIの場合
  - RFC 2527　1999年　 --　RFC 3647(2003年)
    - インターネット X.509 PKI 証明書ポリシー(CP)と認証実施(CPS)フレームワーク



RFC 2527に基づき作成されたCP　証明書ポリシー

米国FPKI CP　--　４つの保証レベルのCP

4.6.2 プライベート鍵の防護

US Federal PKI　のCPの例

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic module

Assurance Level	Certification Authority	Subscriber	Registration Authority
Rudimentary	FIPS 140-2 Level 1 (HW or SW)	N/A	FIPS 140-2 Level 1 (HW or SW)
Basic	FIPS 140-2 Level 2 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)
Medium	FIPS 140-2 Level 2 (HW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 2 (HW)
High	FIPS 140-2 Level 3 (HW)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (HW)

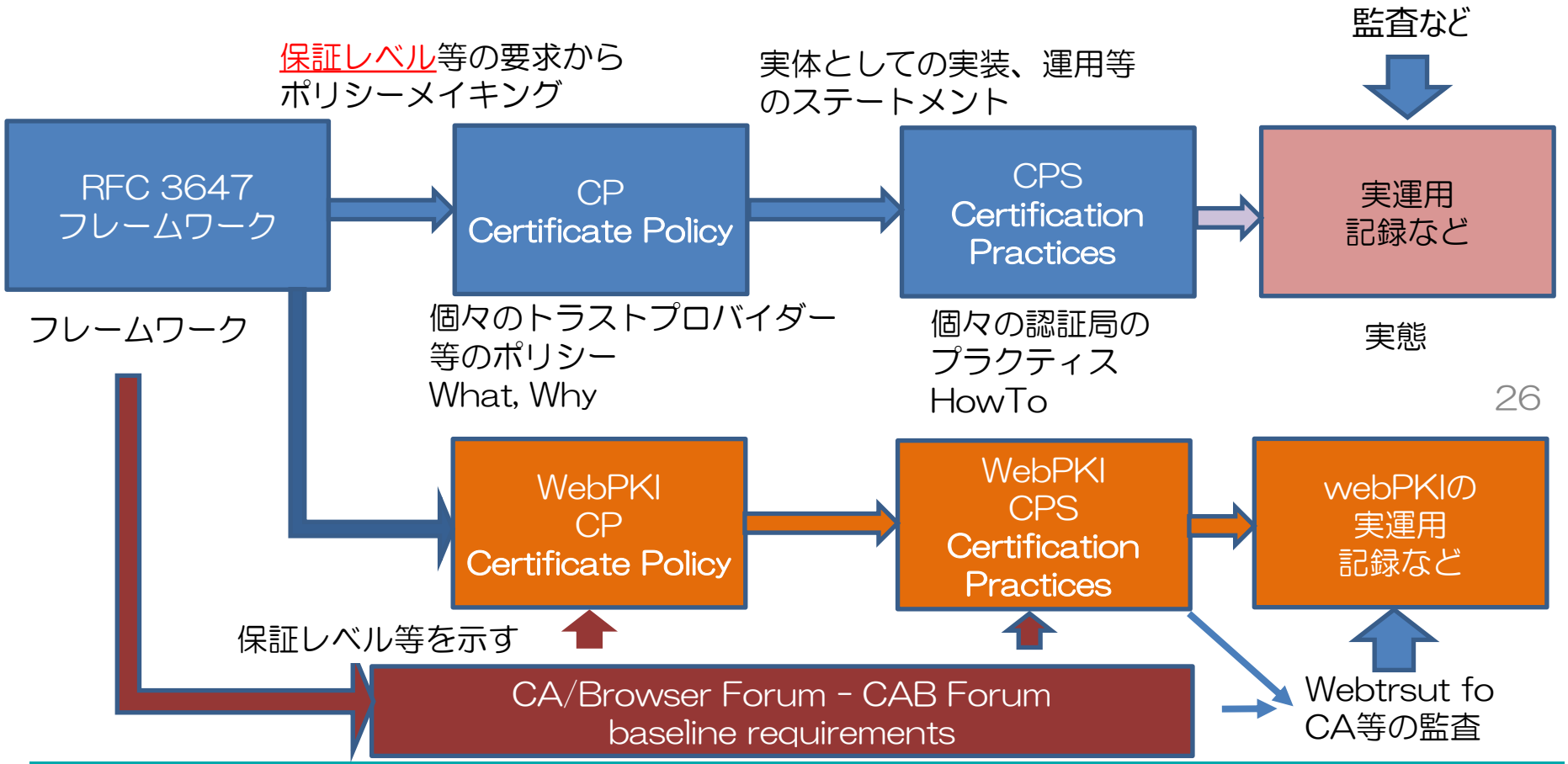
Federal PKI (FPKI) Policy Authority
http://www.cio.gov/fpkipa/policies.htm

50

- FPKI CP (Certificate Policy)
  - FPKIは、米国連邦 PKI
- なんのためのCP
  - ブリッジ認証局とのCross Certificateのためのcp
  - 実質的には、ブリッジ認証局とのCross Certificateする認証局に対する要求
  - Cross Certificateする認証局は、このCPに基づきCPSが作成され、そして監査される
- 4つの保証レベル
  - 現在は、MediumとHighと、そのバリエーションのみ機能している。
  - 4つの保証レベルは、その後、SP800-63(2004年）に引き継がられる。

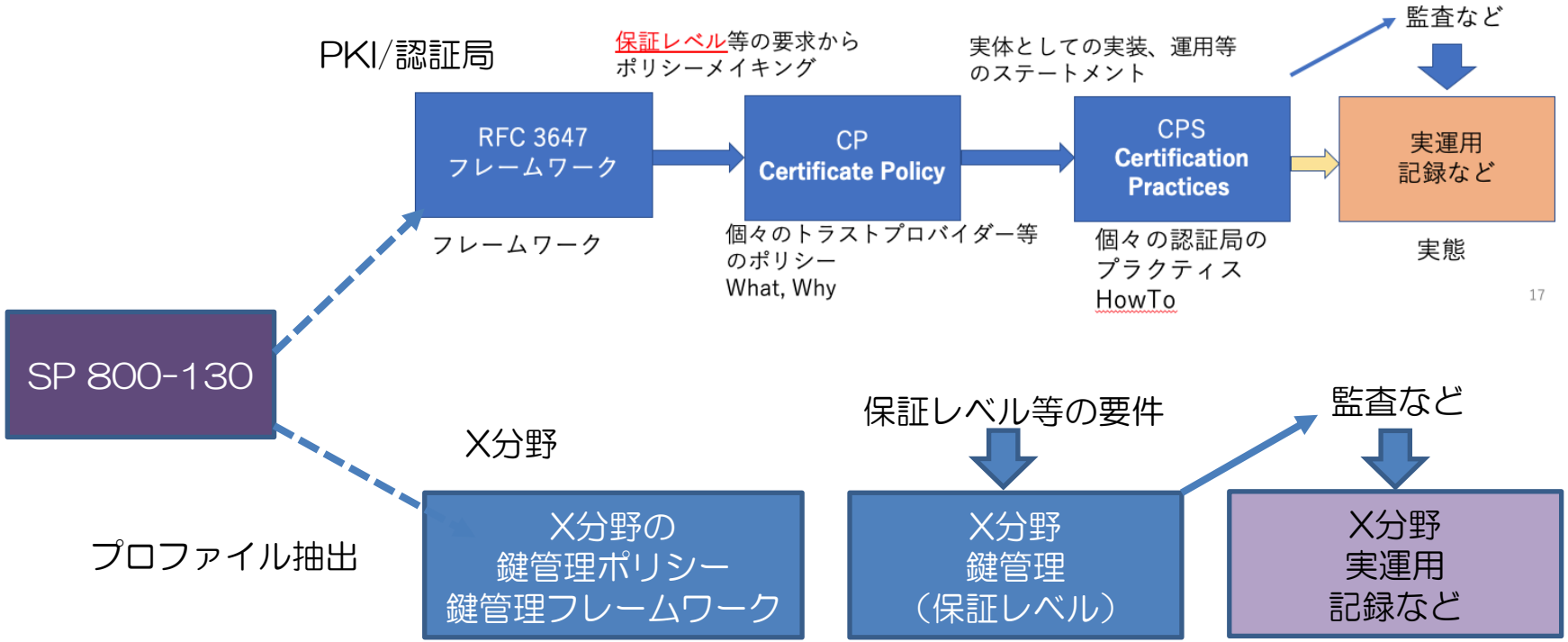
出典：インターネット上の信頼を確立する PKIの技術と運用」(基礎編)
https://www.nic.ad.jp/ja/materials/iw/2005/proceedings/T12-1.pdf

WebPKIの場合



SP 800-130　2013年

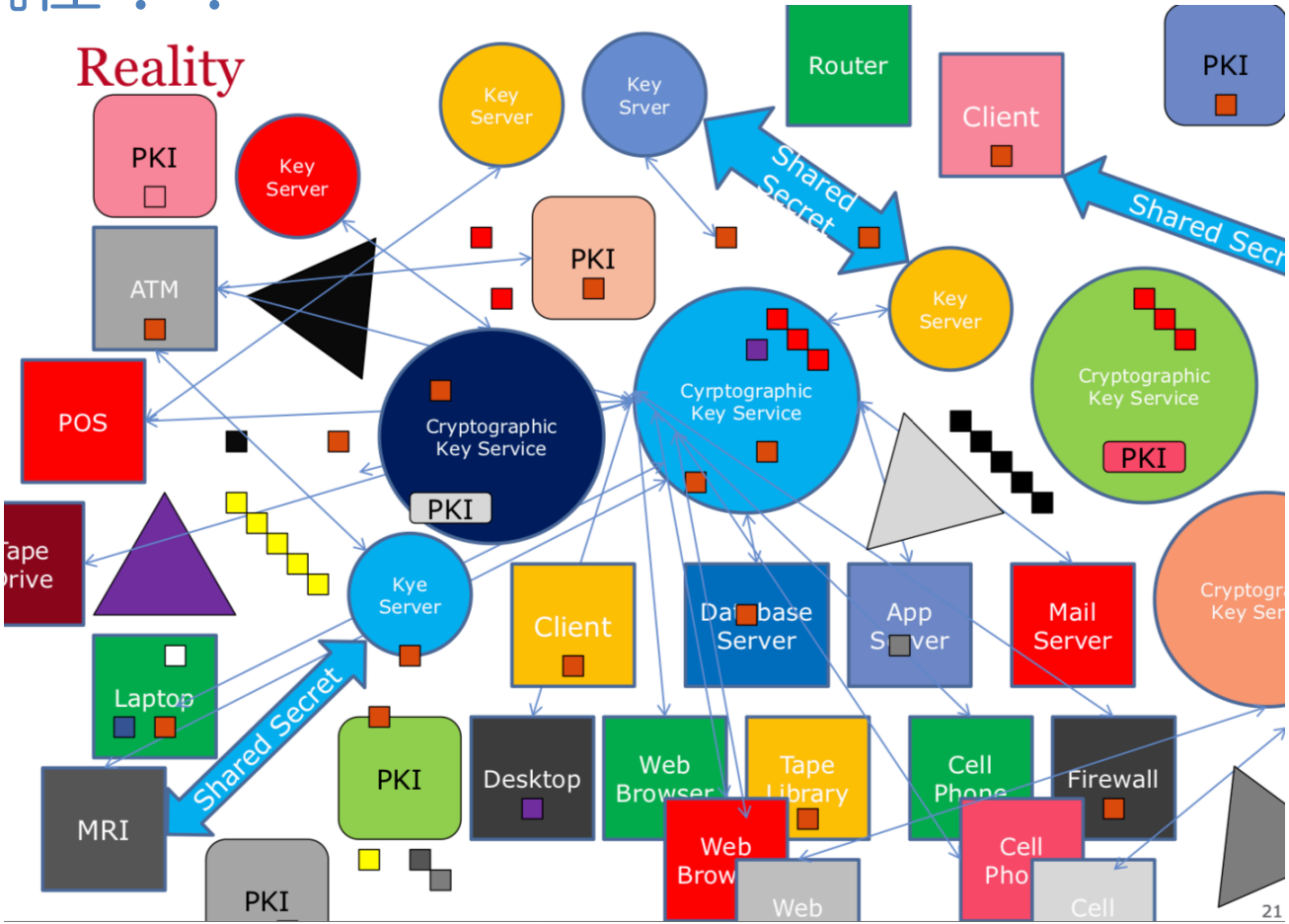
A Framework for Designing Cryptographic Key Management Systems



暗号鍵管理の現在、未来

- 境界線防御からゼロトラストアーキテクチャへ
  - 膨大な数のクレデンシャル管理・暗号鍵管理が要求される時代へ
- サイバーフィジカルシステムもゼロトラストアーキテクチャへ
  - フィジカル空間の至るところに暗号鍵が組み込まれてく

現在？？



出典：
IEEE
Key Management Summit 2010
Enterprise Cryptographic Key Management Realities and Issues
https://storageconference.us/2010/Presentations/KMS/9.Stieber.pdf

アドホックに、暗号システムが追加されてきた結果の現状？？？

IoT ・BD・AI ≒ サイバーフィジカルシステム

フィジカル空間の至るところに暗号鍵が組み込まれていく

信頼される安心を、社会へ。
SECOM

法と技術アーキテクチャ

技術

技術アーキテクチャと
ビジネス・デザイン

法制度

AIなどによる処理

ビジネス

ビッグデータの収集

情報と情報がつながるサイバー空間

フィジカル空間に還元
新たな価値の創造

デジタル・ツイン

高機能なエッジAI

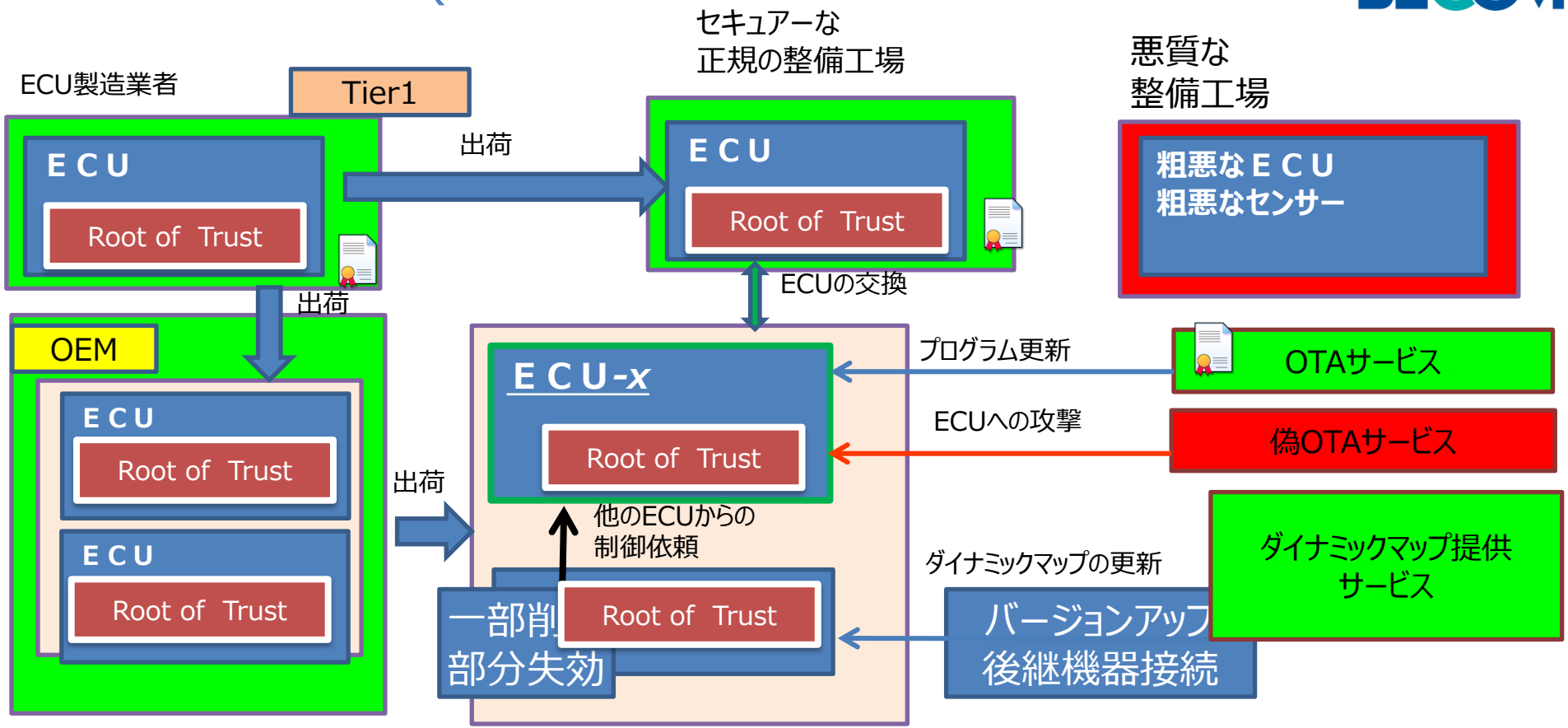
学習済
モデル

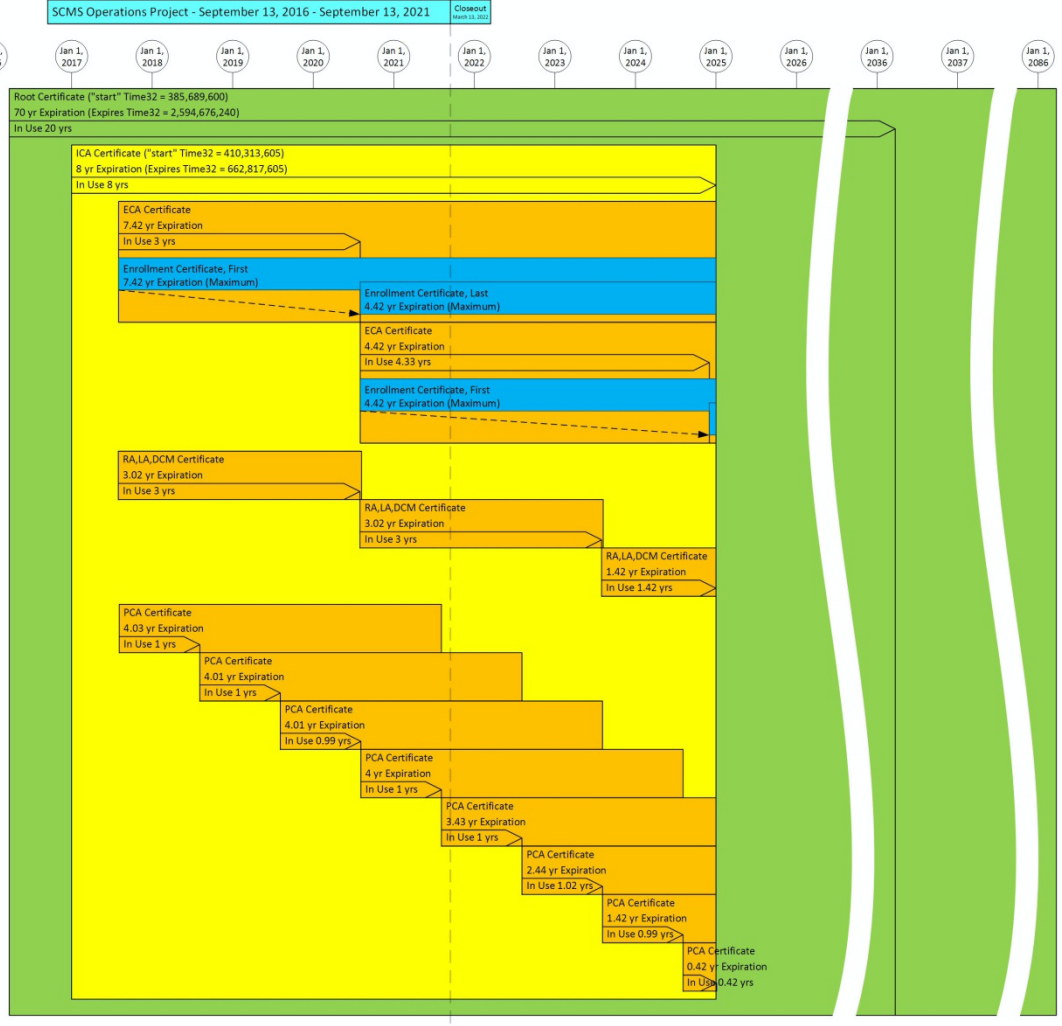
フィジカル空間における
サービスイノベーション

膨大な数のIoTデバイス

人と人、人とモノ、モノとモノがつながるフィジカル空間

ECUのアクセス制御(の今後？)





サイバーフィジカルシステムにおける暗号鍵管理システムのライフサイクル？？

出典：CV Pilot PROD Certificate Expiration Timelines
https://wiki.campllc.org/pages/viewpage.action?pageId=27427019

まとめ

- PKI／認証局に関する鍵管理は、2000年前後には、確立していた。
- 2020年現在、デジタル社会を迎え、非情報系も含め様々な産業分野（金融、仮想資産、自動車、etc…)において、新たなトラストの仕組みが必要になっている。
- こうした新たなトラストの仕組みには、暗号技術が欠かせず、そして、暗号鍵を中心としたアーキテクチャが、様々な産業分野に必要になっており、その中心的な技術として「暗号鍵管理」がある。
- こうした新しい分野にこそ、「暗号鍵管理」のフレームワークが重要な役割を果たす。

33