信頼される安心を、社会へ。
SECOM

量子計算機時代のPKI

セコム株式会社 IS研究所
伊藤 忠彦

2018/04/17

自己紹介

信頼される安心を、社会へ。
SECOM

伊藤　忠彦

セコム株式会社　IS研究所　暗号・認証基盤グループ

- ～高校
  - 算数～数学を楽しむ（競技、日本・カナダ）
  - RSA暗号を実装
- 大学～大学院～
  - 10年くらい暗号（理論）を研究
  - 安全性証明、楕円曲線暗号、量子鍵配送
- セコムIS研究所（7年目）
  - ルート認証局構築
  - CA/BForum、IETF等で活動
  - IoT機器のセキュリティ（消費電力分析、L2暗号化、乱数）
  - 規格調査（米・日・欧）
  - 鍵管理・ライフサイクル管理

なぜセコムで量子コンピュータ？

- 認証局（CA）における「電子証明書」の発行業務に関与
- 特徴：
  - **鍵の価値が高い**
    - 不適切に利用された時のインパクトが大きい
    - 構築・運用コストも高い
  - **鍵のライフサイクルが長い**
    - 1度作ると、20-30年システムを保守しないといけない。
- 30年以内に暗号解読用の大規模量子コンピュータが登場するとビジネスに関わる

長期のライフサイクルをケアしなければいけない

量子コンピュータで暗号解読はいつできるのか疑問に思ったが. . .

- 世間では
  - 2020年にはできる？
    - たまに言う人がいる
  - 2030年にはできる？
    - 相当な数の人がそう言っている(いた)。
  - 30～50～年かかる？

根拠が不明な記事も多数存在する

PKI関係者は、どう量子コンピュータの向き合うべきか？

今日のスコープ:公開鍵暗号

- 共通鍵暗号
  - 鍵を長くすることで対応可能(AES256等)
    - AES256へ、何時移行するのか？
- ハッシュ関数
  - 出力を長くすることで対応可能(sha512, sha3)
    - sha384/512、512への移行は？
- 公開鍵暗号
  - **現状、効果的な対応ができない。**

NISTの見解

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

本日の目次

- 量子コンピュータがPKIへ与えうる影響
- 現在の性能・暗号解読に必要な性能
- 想定すべき脅威とは
- 今、なにができるか

量子コンピュータがPKIへ与えうる影響

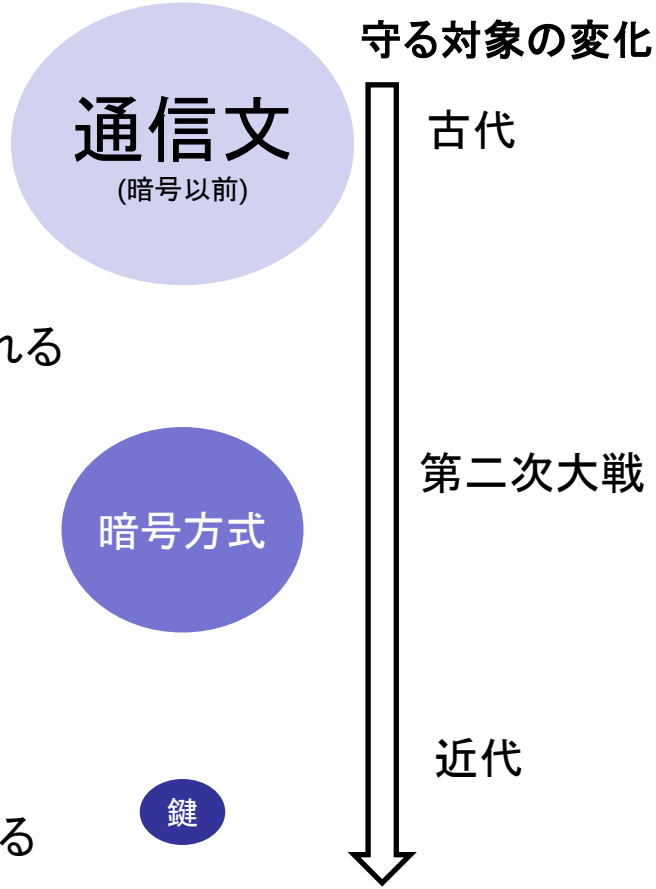
Society 5.0におけるPKI

信頼される安心を、社会へ。
SECOM

暗号技術の進展が「鍵」に及ぼす影響：

- 今まで
  - 守る対象の「価値」が鍵へ集約される
    - 守る対象が高価なほど、「鍵」の価値が上がる
    - 大規模になるほど、「鍵」の価値が上がる
  - 護る対象を「鍵」へ集約する事で、より効率的に護れる
    - 何も考えないと、価値が集約され過ぎる
    - 重要になるのが「鍵管理」

- Society 5.0
  - 暗号がより広く使われる
  - 暗号がより大規模に使われる
  - 鍵の価値が上がる
  - 鍵管理が、より重要となる
    - 何も考えないと、リスクがコントロール不能となる



量子コンピュータの影響

- （理想的な）量子コンピュータを利用すると
  - 素因数分解が効率的に解ける
  - 離散対数問題が効率的に解ける

- 公開鍵暗号（RSA、ECDSA、etc.）の鍵がわかる。
  - 暗号化したデータが読める
  - 署名されたデータが改ざんできる

社会へ非常に大きな影響を与えうる

現在の量子コンピュータの性能と暗号解読に必要な性能

今回の発表のスコープ

- 非ノイマン型チップ
  - 専用設計のチップ

スコープ外

- 量子イジングマシン
  - D-waveとか

スコープ外（次ページで概説）

- 量子コンピュータ

スコープ

量子アニーリングによる素因数分解

- 量子アニーリング(D-wave)を利用した因数分解(2017/1)
  - 200099(＜20bitの数)を因数分解
    - 20bit⇒2048bit は近く見える？
    - 現実的には、暗号に対する攻撃には利用できない。
      - 測定精度の問題

量子コンピュータの性能の指標

信頼される安心を、社会へ。
SECOM

qubit数	**:どれだけ大きなデータを扱えるか**
コヒーレンス時間 / 基本演算時間	:どれだけ複雑な計算ができるか
掛けたもの（不正確な表現ですが. . . ）	:量子ボリューム
演算精度（初期化・ゲート演算・測定）	:大規模化には非常に重要

分かりやすい

見通しが悪い
多くの知識や前提が必要

本命：量子コンピュータ（ゲート）

Company	Type	Technology	Now	Next Goal
Intel	Gate	Superconducting	49	TBD
Google	Gate	Superconducting	72	TBD
IBM	Gate	Superconducting	50	TBD
Rigetti	Gate	Superconducting	19	TBD
USTC (China)	Gate	Superconducting	10	20
IonQ	Gate	Ion Trap	7	20-50
Silicon Quantum Computing Pty	Gate	Spin	N/A	10
Univ. of Wisconsin	Gate	Neutral Atoms	49	TBD

https://quantumcomputingreport.com/scorecards/

暗号解読に必用な（論理）qubit

暗号プロトコル	解読に必用な論理qubit
RSA 2048	4098[1,2]
RSA 3072	6146[1,2]
ECC256	1800[1], 2330[2]
ECC 384	2700[1], 3484[2]

現状：～72qubit程度。
暫くしたら、現行RSA（2048bit）、ECC（256bit）の因数分解もできる？？

[1]A.Fowler, et al., "Surface codes: Towards practical large-scale quantum computation",
[2] M. Roetteler, et al., "Quantum resource estimates for computing elliptic curve discrete logarithms"

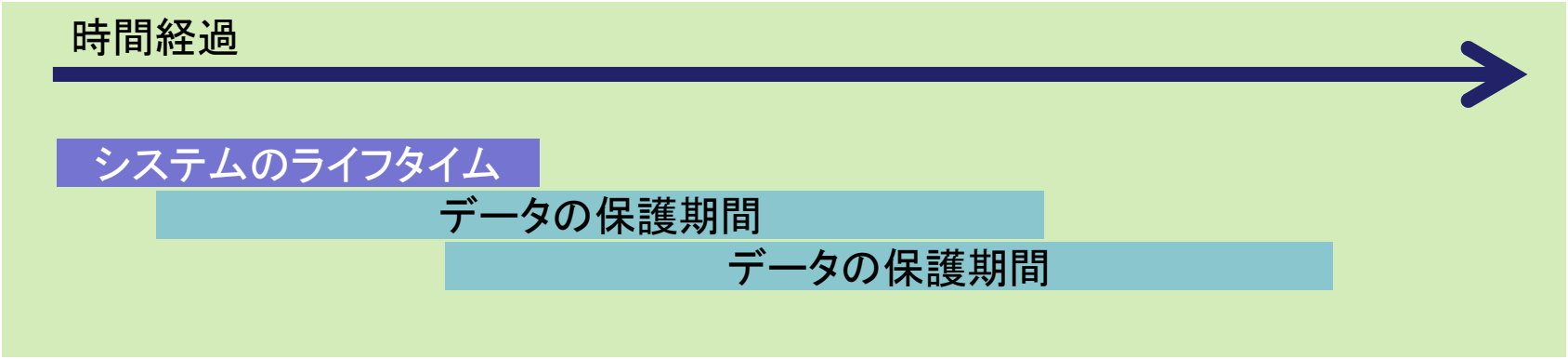
論理qubitと物理qubitの違い

- 論理qubit = 理想的なqubit
- 実際のqubit（物理qubit）は理想的とは言えない
  - 現状の試算
    - エラー率を抑えるために、qubit数を$10^{3\sim4}$倍にして対応
    - Fault Tolerantにするためには、qubit数を数十倍にして対応
    - 因数分解に必要な物理qubitは10^{8}～
  - 大幅な演算精度の向上が必要。
  - コヒーレンス時間の問題もある（今回は省略）

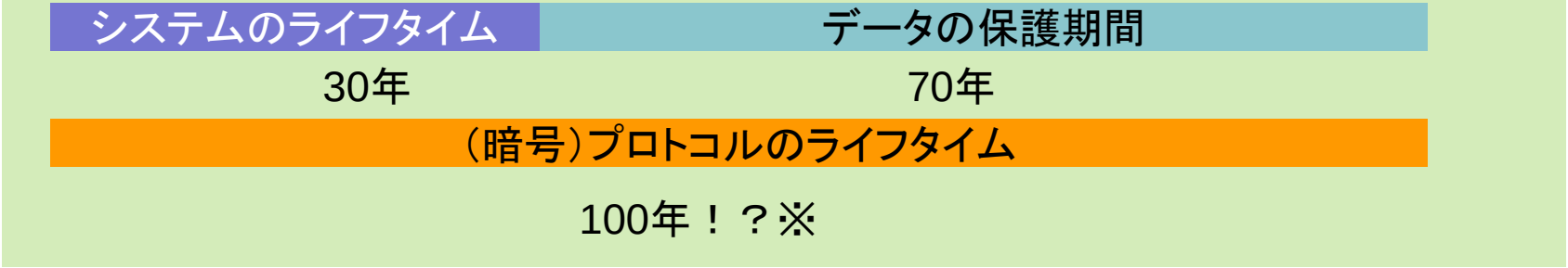
直ちに脅威とならない？？

想定すべき脅威とは

PKIへの脅威：鍵のライフサイクル管理は大変



例：仮に30年稼働するシステムで、人の寿命程度の期間に渡りデータを保護する必要がある場合



量子コンピュータ以前の米国の移行方針

- 米国の情報公開規定：50年（一部75年）
  - 暗号化したデータを、クラウドに保管する時等に重要な観点。

【RSA】2048⇒3072移行

誰でも手軽に2048が解けるようになるのは、この頃？

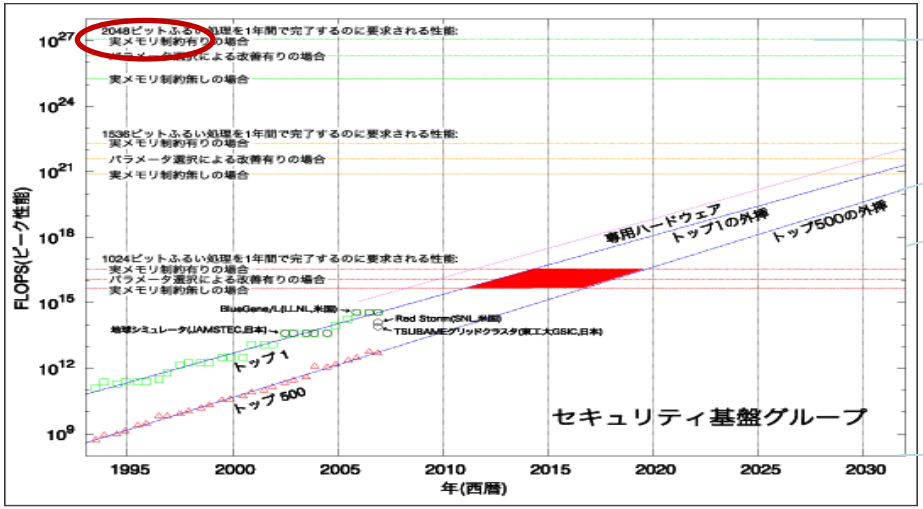
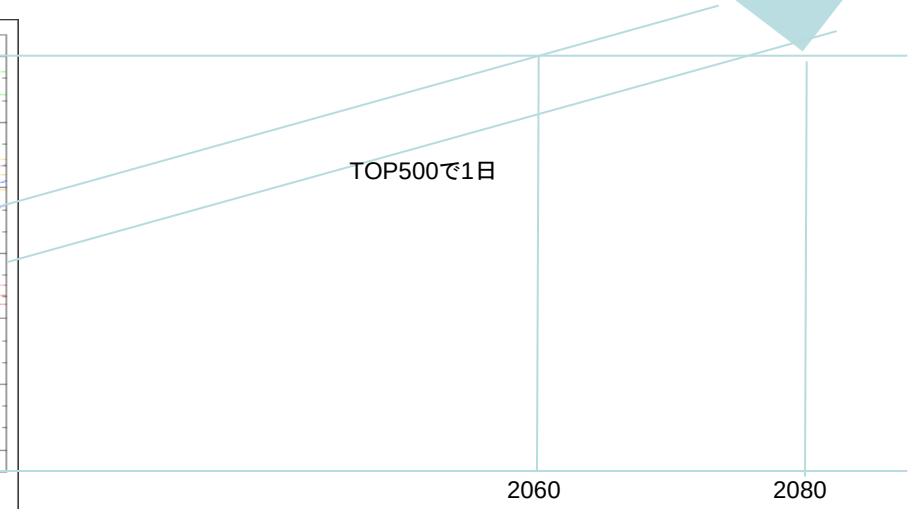


図1●1年間で解(ふるい)処理を完了するのに要求される処理性能の予測

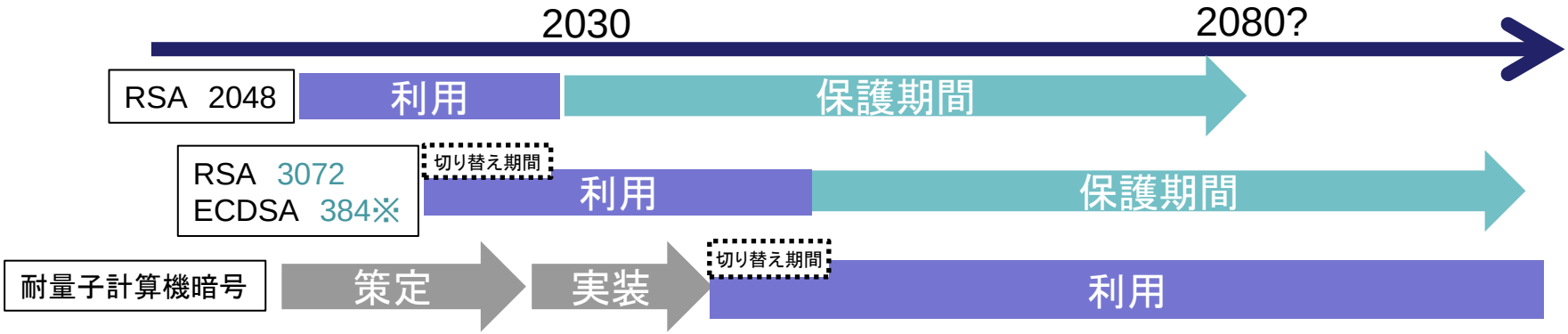


http://www.nict.go.jp/publication/NICT-News/0904/04.html

2048の利用

50年

最近の米国の移行方針？（量子コンピュータも考慮）



考察

- 耐量子計算機暗号の脅威は、データの保護期間次第
- 保護期間が長い場合、脅威は無視できない

何ができるか（対策）

汎用的対策：耐量子計算機暗号

利点：**汎用的かつ根本的な解決**

欠点１：**移行に時間が掛かる**

- 過去実績
  - sha1⇒sha2(web)
    - 2001年（ Sha2規格決定）～ 2017年（Sha1をwebで使わなくなる）～（一部、まだ使われている。）
  - (T)DES⇒AES
    - 1997（AES公募開始）～2000（AES仕様決定）～2030（NIST：TDESからAESへの完全移行予定）

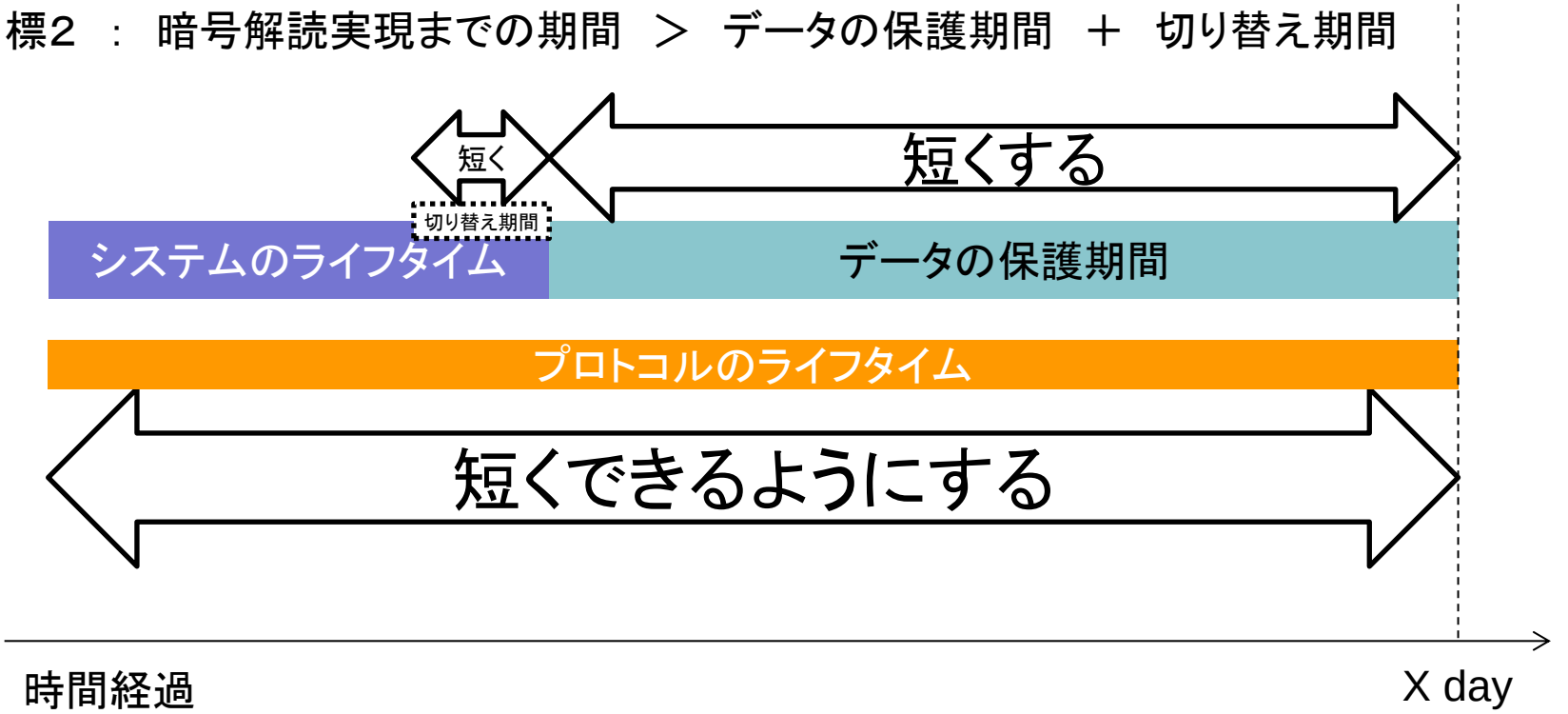
欠点２：**既存暗号に比べ、パフォーマンスは（ほぼ確実に？）落ちる**

- セキュリティと計算量やデータ量のトレードオフ

既存の公開鍵暗号を長く使いたい！

既存の公開鍵暗号を長く使うための方向性①

目標1 ： 暗号解読実現までの期間 ＞ プロトコルのライフタイム
目標2 ： 暗号解読実現までの期間 ＞ データの保護期間 ＋ 切り替え期間



（攻撃者が量子計算機を利用可能になる時）

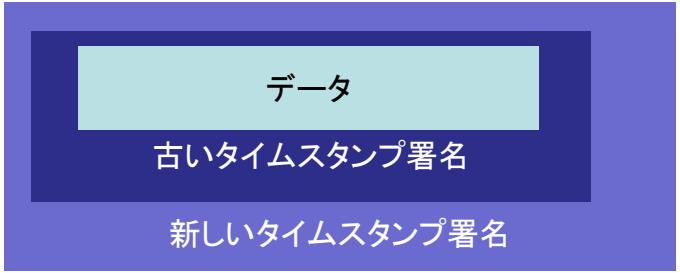
期間の短縮（秘匿・署名）

（Security and）Crypt Agilityが大事

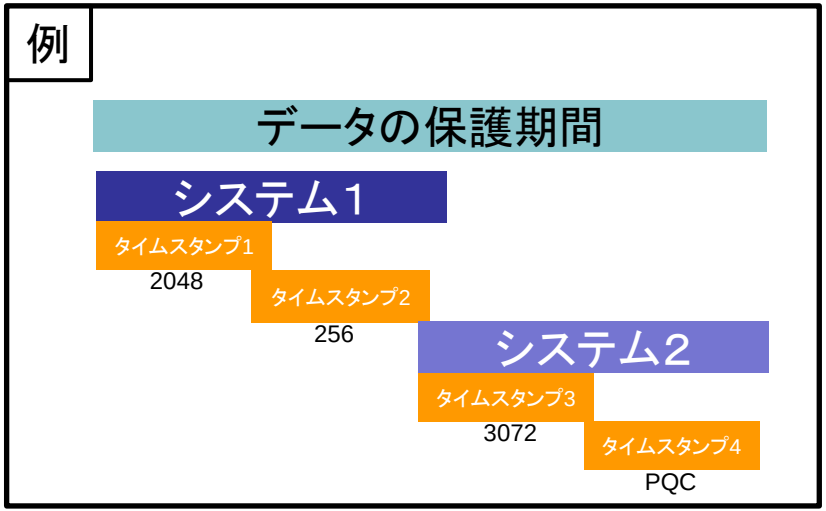
- データの保護期間を短縮する試み
  - webPKI
    - 証明書の有効期間を短縮
      - 証明書の有効期間が長いと、脆弱な証明書を市場から回収するのに時間がかかる
      - サーバ証明書の有効期間が5年⇒3年⇒2年⇒1年？
      - Let’s Encryptの有効期間は3カ月
    - ACME
- 切り替え期間を短縮する試み
  - クレジットカード
    - カードを5年で再発行
  - 相互運用性
  - 暗号部分のモジュール化
  - OTAアップデート
  - etc.

既存の公開鍵暗号を長く使うための方向性②（署名）

- データに対し、タイムスタンプを何度も付与
  - データのライフタイムとプロトコルのライフタイムを分離
  - 一番外側のタイムスタンプ署名が耐量子であれば良い

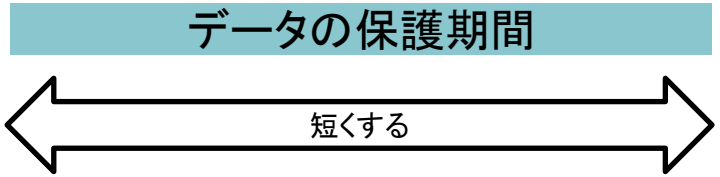


- 懸念点
  - 多数のタイムスタンプ署名の保管方法
  - 大量のドキュメントに対してのタイムスタンプ
  - 途中、修正された場合の対応
  - 墨塗り等への対応
  - 耐量子計算機暗号に変更する事での
    - 署名サイズの増加
    - 鍵サイズの増加 etc.
- 長期署名等で解決できる課題も多い



【懸念】秘匿については

- 保護期間を短縮しない場合
  - より強い鍵で再度暗号化
    - 色々と大変
  - 保護期間の上限が存在しない場合、対応が難しい。
  - 暗号文を適切にアクセス制御
    - クラウド保管は望ましくない？
- 保護期間を短縮するアプローチ
  - 情報公開する
    - 公開してしまえば、「秘匿情報」ではない
  - データを消去する
    - 鍵・暗号文
    - Cryptographic Eraseは利用しない
- 鍵・データのライフサイクルを予め考えておく必要あり
  - 秘密を「墓場まで持って行く」思想とは相性が悪い事にも留意



現状の対策まとめ

- 耐量子計算機暗号
  - 移行期間が長い、移行コストが高い
- データの保護期間短縮
  - ポリシー（場合によっては法令も）変更が必要
  - 適切な鍵管理、破棄方法、公開方法もセットで検討する必要あり
- 切り替え期間を短縮
  - 設計思想の変更が必要な場合もある
- （署名のみ）タイムスタンプを定期的に付与
  - 既存の仕組み（長期署名等）も利用できる
  - 署名/鍵データサイズ増加については要検討

耐量子以外のセキュリティ上の恩恵も有る

まとめ～量子コンピュータ時代のPKI～

- 鍵の「価値」が上がり、鍵管理の重要性も上がる
- 鍵/システムのライフサイクル管理の重要性も向上
  - キーワード
    - データのライフタイムが重要
      - 破棄・公開の年限・手段を明確化する事が重要
    - 移行についての検討
    - Security and crypt agility
  - 用途に合わせ、アクセス制御も適切に組み合わせる

- その上で、量子コンピュータの開発動向を注視する