真正性の文化

歴史的反省から現実世界×仮想世界の広がりの中で

3階層公開鍵暗号の提案

辻井重男

冒頭ご挨拶

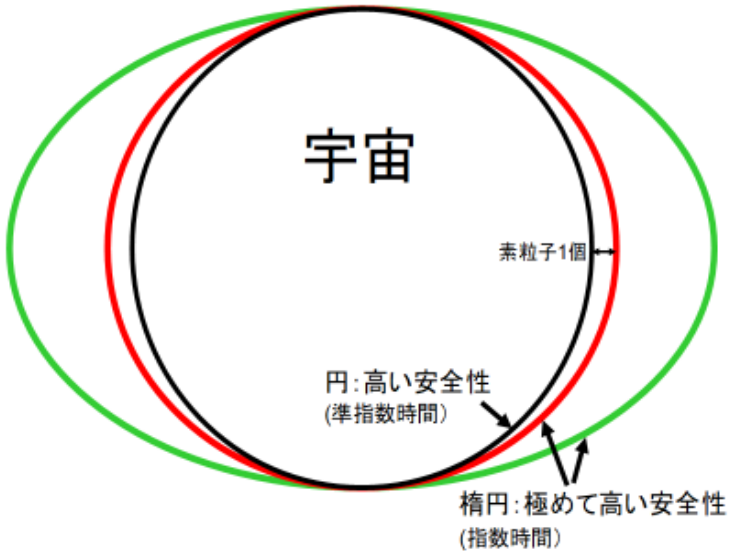
- S/MIME推進協議会の顧問を務めさせて頂くことになりました辻井重男です。
- よろしくお願いします。

- S/MIMEの意義・動向・期待・課題等については、佐々木良一会長、諸角事務局長
- の講演がありますので、辻井は、顧問の立場から、
  前半、現実×仮想世界が広がり偽情報などが氾濫する中で、
  S/MIME等の認証はもとより広く真正性文化の意義・重要性について、
  私見を述べさせて頂きます。

- 後半は、現在、提案中の個人的研究として「３階層公開鍵暗号の構想」について説明します。
- 「秘密鍵こそ命我が命」と言い続けて来ましたが、そうであれば、秘密鍵の中に、
- 本人を同定出来る情報を埋め込む必要があると考えている次第です。ご参考になれば幸いです。

- 略歴：
- 1979 年 東京工業大学教授、1994 年 中央大学教授、
- 1996 年 電子情報通信学会 会長
- 1999 年 中央大学研究開発機構 機構長
- 2003 年 日本学術会議 会員
- 2004 年 情報セキュリティ大学院大学初代学長
- 2004 年 中央大学研究開発機構教授
- 2007 年 日本ペンクラブ会員
- 2010 年 （一財）マルチメディア振興センター理事長
- 2013 年 （一財）放送セキュリティセンター理事長
- 2017 年 （一社）セキュア IoT プラットフォーム協議会理事長
- 瑞宝中綬章、NHK 放送文化賞、C＆C 賞、高柳記念賞、信学会功績賞、
- IEEE 第三千年記 記念賞、発明表彰等
- 郵政省 電波監理審議会会長、総務省・内閣等の諸官庁における、電子署名法、
- 住民基本台帳法等の多くの法制度創設に関する委員会委員長を歴任。

- 「真正性の文化」というタイトルについて、
- 「何が本物（真正）か？　は視野・分野によって異なる。」
- という例から始めよう。次の図をご覧下さい。
- 質問：　赤い図（宇宙のは半径位の広がりの横幅を素粒子1個程広げた曲線）は円でしょうか？楕円でしょうか？　　答えは次スライド



- 答え

質問が、人格の関する場合：　当然　円満な人格
楕円満な人格などと言う人はいない。

質問が、楕円曲線の安全性に関する場合：　楕円曲線暗号

黒色曲線（2次曲線 円）はRSA暗号に対応　鍵長2048ビット
赤色曲線（神様でなければ、円に見えるが）立派な楕円
楕円曲線暗号の3次曲線に対応する。　鍵長　約200ビット

緑色の楕円（横幅が縦幅の2倍）と赤色曲線の差は全く無し。

.

- 正しい答え（真正性）は視野によって異なる。

  赤は円満な人格（楕円満な人格ではない）
  S/MIME等に使われる暗号理論では、赤は緑と同じ安全性を持つ楕円

- 赤い曲線は、誰が見ても楕円ではなく円に見えますね。
- ところが、赤い曲線も緑の楕円と同じ楕円なのです。
- RSA暗号は　円（2次曲線）に対応。
- 楕円曲線暗号（ブロックチェイン等に利用）は楕円に対応する3次曲線。

- 数学的には当たり前ですが、念のため、様々な横幅の楕円、1万本について
- シミュレーションして、宇宙の広がり程大きな円の横幅を素粒子1個程～2倍に広げた
- 曲線から生成した楕円暗号3次曲線を比較してみた。
- 円（RSA暗号）の場合：鍵長が2048ビット必要なのに対して
- 横幅を素粒子1個程だけ広げた楕円に対応する楕円曲線暗号では、
- 鍵長は200ビット程度で済む。

真正性とは？　様々な視点

数学的視点　科学的視点　**歴史的視点　文学的視点　哲学的視点**

- **・・・等 多くの視点がある。それらの基盤となるのが、**
  認証的視点、要するに、本人・本モノ確認である。

S/MIME は送信者認証等として利用されており、佐々木会長のキーノートスピーチ、
S/MIME推進協議会　諸角昌宏事務局の「キックオフセミナー」にある通り
今後、より広い普及が期待される。

暗号としてはこれまで、主としてRSA暗号が用いられてきたが、
今後、楕円曲線暗号が利用されよう。

講演の流れ

- 現実世界×仮想世界の広がる中で、
- 何が事実で、それを関係者がどう解釈し利用し理念構築したのか
- を見極めることが重要である。

その基盤が、本人・本モノ性確認であり、その為、辻井は、

「秘密鍵の中に本人性・本モノ性を保証する為の極秘密鍵を埋め込む3階層公開鍵」

を提案しているが、先ずは、小学生時代に受けた、

{先生が「天皇」と言えば、さっと鉛筆を置いて姿勢を正す}太平洋戦争中の教育と

「白村江敗戦（663年）以降、明治維新までの事実と歴史理念の相克」

を振り返ることとしよう。

真正性の定義

- 奈良文書では下記のような主張が記されています。

- 遺産の保存は地理や気候、環境などの自然条件と、文化・歴史的背景などとの関係ですべきである。

  要するに、状況を考えてやむを得ないと判断された場合は

  遺産の保有国の伝統的な保存技術や修正方法を使って

  真正性を保つことを許すというものです！

  要するに　これは文化財として本物か。

  本物の継続性をどう保証するか。

真正性とは　　世界遺産分野では

- 文化財に使われている素材などが
- それぞれの文化的背景の独自性や伝統を継承している。

- 真正性の考え方に大きな影響を与えたのは”奈良文書”！
- 完全性は文化遺産＆自然遺産両方に求められる概念！

歴史に視る事実と解釈・利用

- 白村江の敗戦（663年） は事実。　唐への和解交渉に対して、
- 「付き合いたければ、文明国になれ。
- 仏教を広めよ。法制度を整備せよ。天皇制の正当性物語を作れ」
- ーー→　日本書紀　理念化・物語化

- 現実から物語・理念ーー→逆方向に作用　現実に影響
- 小学校教育：
- 日本は万世一系の天皇を頂く優れた国だ。大和魂があるから勝てる。
-
- 今後は、事実・現実を真正と観て、
- 高い視点・広い視野から考えていくことが必須では？
- 現実重視。常に現実に立ち返ることが必要。

-

-

- 明治維新・植民地化対応が行き過ぎた　ーー→西南戦争・日清・日露・太平洋戦争

- 西郷死するも清の為、大久保殺すも清の為？　　歴史的慣性が禍？　・・・
- 日露戦争勝利を祝う博覧会などでは、植民地化の正当性を主張
-

- 太平洋戦争前後の文化人の現実認識

- フェイクとの闘いー暗号学者が見た大戦からコロナ禍まで
（辻井重男　コトニ社　2021年秋出版）
第2章　「戦時中の文化人・作家たちの現実認識を問う」参照

吉川英治、高村光太郎、亀井勝一郎　他

戦争協力への批判ではなく、日米の経済格差と言う現実を観ていたのかを問う。

サラリーマンだった父ですら、連戦連勝の昭和17年の頃から
「こんな戦争は負けるに決まっている。」
母「なんで？こんなに勝っているのに。」

- 小学生時代の教科書

- 敵高射砲弾は汝が機の胴体を貫きつ　汝　にっこりとして天蓋を押し開き
- 仁王立ちとなって僚機に別れを告げ　天皇陛下万歳を奉唱
- 若き血潮に大空の積乱雲を彩りぬ（高村光太郎？）

- 学童疎開時代　覚えないと食事抜きだったが、
- 恰好良いので、いっぺんで覚えてしまった。
- 自分がその身になった場合のことも考えず、恥ずかしい限りだが、
- 小学生教育の影響は深刻。「自分がその身になった場合のことも考えろ」が大事。
- 高村光太郎は、戦後反省したとも聞いているが、ここでは、戦争賛美の是非は不問。
- 日米の現実（経済力の差）を考えたのか？
-

- 現実（事実）を高い視点・広い視野の中で見極めた上で、真正性を把握することの重要性

- 真正性と真理の関係は？
- 数学・科学分野では、客観的に考え易いが。
- 文学・芸術分野では、虚構の中に主観的真正性・真理？
- 主観的真理（正義）は、認めるとして
- 真正性には客観性を持たせたい。
- 歴史的事実:　今後、歴史に残すには、本人性・本モノ性が基盤

本人性・本モノ性が基盤

- 1970年代　　デジタル署名　公開鍵暗号
- （火薬の発明に匹敵するとも言われるが、
- 物理・化学と違い、数学的構造の発明は理解され難い）

- 現実世界×仮想世界の拡大に伴って、秘密鍵の重要性が増大

- 「秘密鍵こそ命　我が命」と言う環境になった。

- だが、秘密鍵の中に、本人証明が入っていないではないか？

・日本経済新聞社説　２０２２ー７－１９

「個人情報持ち歩かぬ役所に」

・・・個人情報の管理は住民の生命や財産を守ることに直結する
・　　重要な責務であると、自治体は肝に銘ずるべきだ。・・・

・　　その通り。

- 例えば、岡崎祐史著「ブロックチェーン」講談社（2019年）135頁に

- 「トランザクションデータとデジタ署名を辻妻が合うように作ることができるのは、
- 秘密鍵を持っている本人だけだからである。
- もちろん、本人だけが秘密に管理しているはずの秘密鍵が漏洩していた場合には、
- すべての前提が崩れてしまう。これは公開鍵全般に言えることだ。」
- と記されている。

- 公開鍵暗号とその秘密鍵は、今後のメタバースでは、より広い社会基盤となる。
- その状況下で、盗難されても、運用時、盗用されないような対策が必須である。
- その為には、面前確認時のPKI認証だけでは盗用されるリスクがある。
- さればと言って、運用時に毎回、面前確認することは勿論不可能。
- では、そうするか？貴重な通信に対しては、
- 面前確認してあることを、remoteで、零知識証明（シュノア署名）すればよい。

3階層公開鍵方式の運用システム構成

- 利用者間通信には、利用者と管理者との間で、
  スマホ・パソコン等により、本人確認（シュノア署名）をした上で、
- マイナンバーカードの秘密鍵を使用する（秘密鍵盗難者には不可能）。

  PKI 面前認証のみでは、運用時には、盗用されるリスクがある。

- 秘密鍵に極秘密鍵を埋め込む。極秘密鍵には、本人の真正性情報
- （マイナンバー・DNA？ ＆ 乱数）

DX環境の本人確認に向けて－３階層公開鍵暗号の提案

秘密鍵が紛失・盗難されても　盗用されない為に

DX環境・

Beyond 5G
ブロックチェーン
ゼロトラスト

one stop service

IOWN

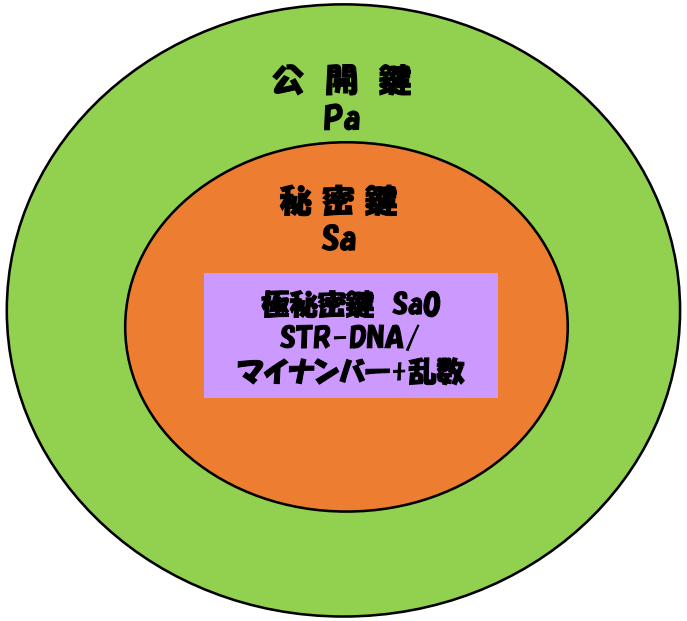
テレワーク

DID/VC

SSI(自己主権型
アイデンティティ)

・・・

メタバース・・



必要な特性（下表は顔認証等の
アナログ生体認証では不可能。
デジタル生体認証が不可欠）

完全性	Aである場合は必ずAと認定
健全性	A以外は絶対にAと誤認定されない
零知識性	A は秘密を見せずに、 管理者に秘密を保持している ことを信用させることが可能

本人確認手順：登録時は面前で。
運用時はシュノア署名に拠る
零知識証明で。

図1　３階層公開鍵暗号の構造

Analog　VS　Digital

アナログ

利点　　社会的認知度が高い
　　一般の人が、扱いやすい。分かり易い

欠点　　完全性・健全性に欠ける　　成り済まし
　　完全性と健全性　いたちごっこ
零知識証明等の高度な技術は利用できない。

アナログの心受け継ぎデジタルへ（ある標語から）

マイナンバーの完全性・健全性の課題

マイナンバーカード保険証に　別人番号登録が33件。
（厚生労働省2021－12－23日発表）

マイナンバーカードと健康保険証連携の際の人為的ミス、
家族の個人番号 →　勤務先 で取り違い→ 健康保険事業者 → 登録。

このような誤りを起こさない為にも、マイナンバーを極秘密鍵
とすることは有効であると考え、以下の運用方策を提案する。

学会発表文献

辻井重男他、
究極の本人確認のための3層型公開鍵暗号の提案
ーマイナンバー・STRの秘密鍵への埋め込みと
その利用に向けてー第２報　電子情報通信学会
SCIS2020

3階層公開鍵方式の運用システム構成

利用者間通信時には、利用者と管理者との間で、
スマホ・パソコン等により、本人確認（シュノア署名）
をした上で、
マイナンバーカードの秘密鍵を使用する
（秘密鍵盗難者には不可能）。

PKI 面前認証のみでは、
運用時には、盗用されるリスクがある。

３層構造の公開鍵暗号の構成

エルガマル暗号、または楕円エルガマル暗号を利用するものとする。
以下、エルガマル暗号を利用する場合について記述する。

極秘密鍵　Sa ＝H(Nm ＋Ra ）　mod p

秘密鍵　　Sa1=gSa）　mod p
公開鍵　　Pa1=gSa１　　mod p

H(　　)：ハッシュ関数（公開）

マイナンバーカードには：
　現在と同様に　秘密鍵を耐タンパー領域に内蔵。
（秘密鍵には、当然、極秘密鍵が内蔵されるが、秘密鍵を知っていても
　極秘密鍵（マイナンバーと乱数から成る）は、数理的に求められないように構成す

スマホ・パソコン等には：
- 極秘密鍵を耐タンパー領域に内蔵する。
- 極秘密鍵は、秘密鍵のハッシュ値であり、極秘密鍵から秘密鍵を求めることは
- ハッシュ関数の一方向性により不可能である。
- 従って、スマホ・パソコンが盗難されても、秘密鍵を求めることは不可能であり
- （マイナンバーカードが同時に
- 盗難されなければ）秘密鍵が盗用されることはない。
-

図において　管理所Dは、現在のマイナンバーカードの管理所に対して、
秘密鍵３層構造に変更したものである。
秘密鍵の構造は、現状のままでも良いし、3層構造でも良い。

１）現在のマイナンバーカードの利用者（現在の秘密鍵構造の所有者）
　　については勿論、
２）3層構造秘密鍵をマイナンバーカードに導入した利用者についても
　　運用時の本人確認を必要としない場面では、
　　管理所Dだけを利用すれば良い。

　管理所 C は、秘密鍵の運用時にも（面前登録時だけでなく）
　本人確認を望む場合に使用される。

面前登録・運用プロセス

- 面前登録（図2）
  ①　利用者aは管理所Cの窓口 において、マナンバーNaを登録する。
- ②　管理所Cは、乱数Ra を発生し、

- 以下、図2　面前登録手順　に示す通り。

- ネットワーク上の運用手順（図3）
- ①　管理所Cは、利用者aとの間で、シュノア署名を行い、
- 利用者aが面前登録済の極秘密鍵を所有していることを確認し、
- 認証結果をaに送信する。
- ②　利用者aは、利用者bに　認証結果を付してメールを送信する。
-

-

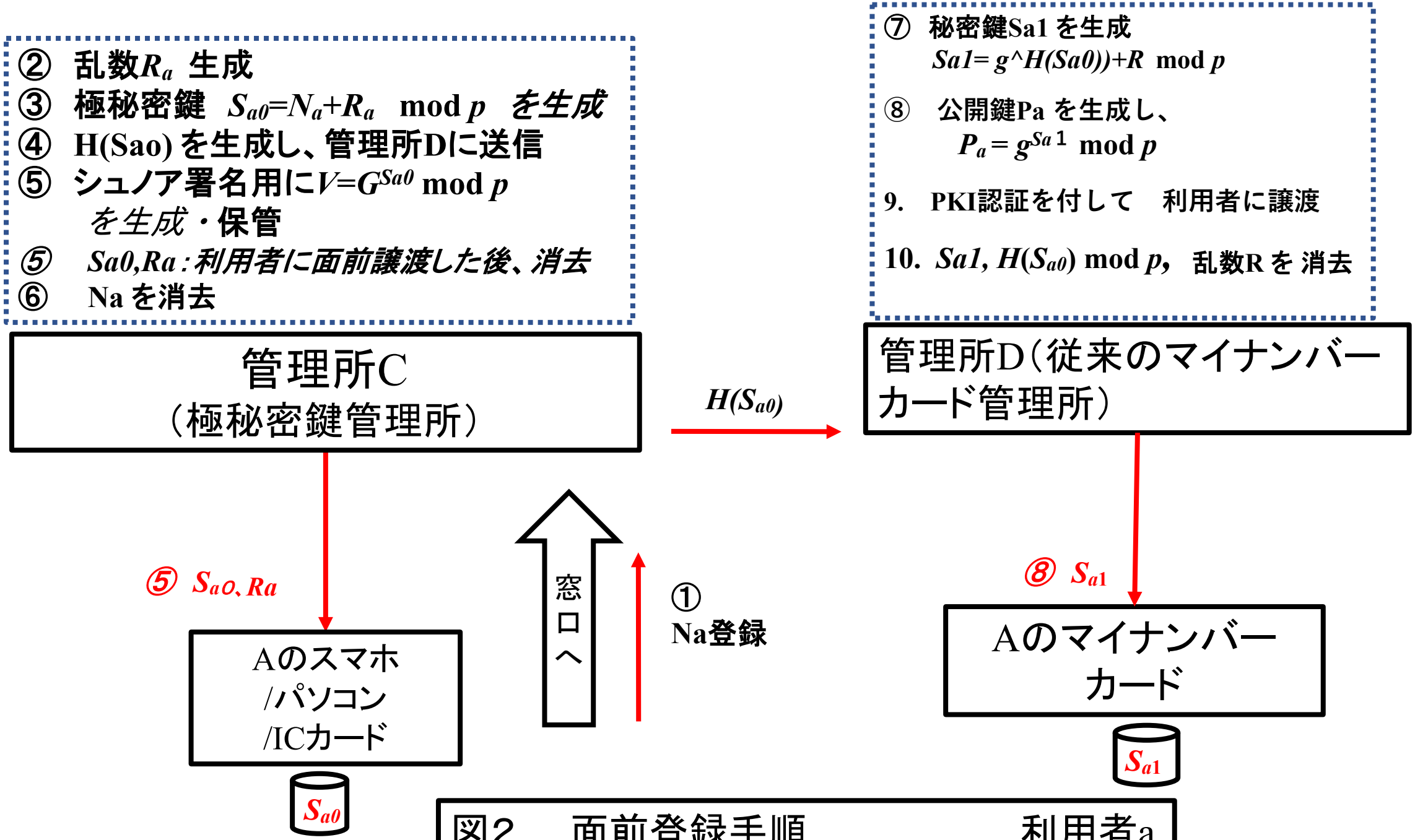


図２ 面前登録手順 利用者a

① シュノア署名による
極秘密鍵S_a所有の確認

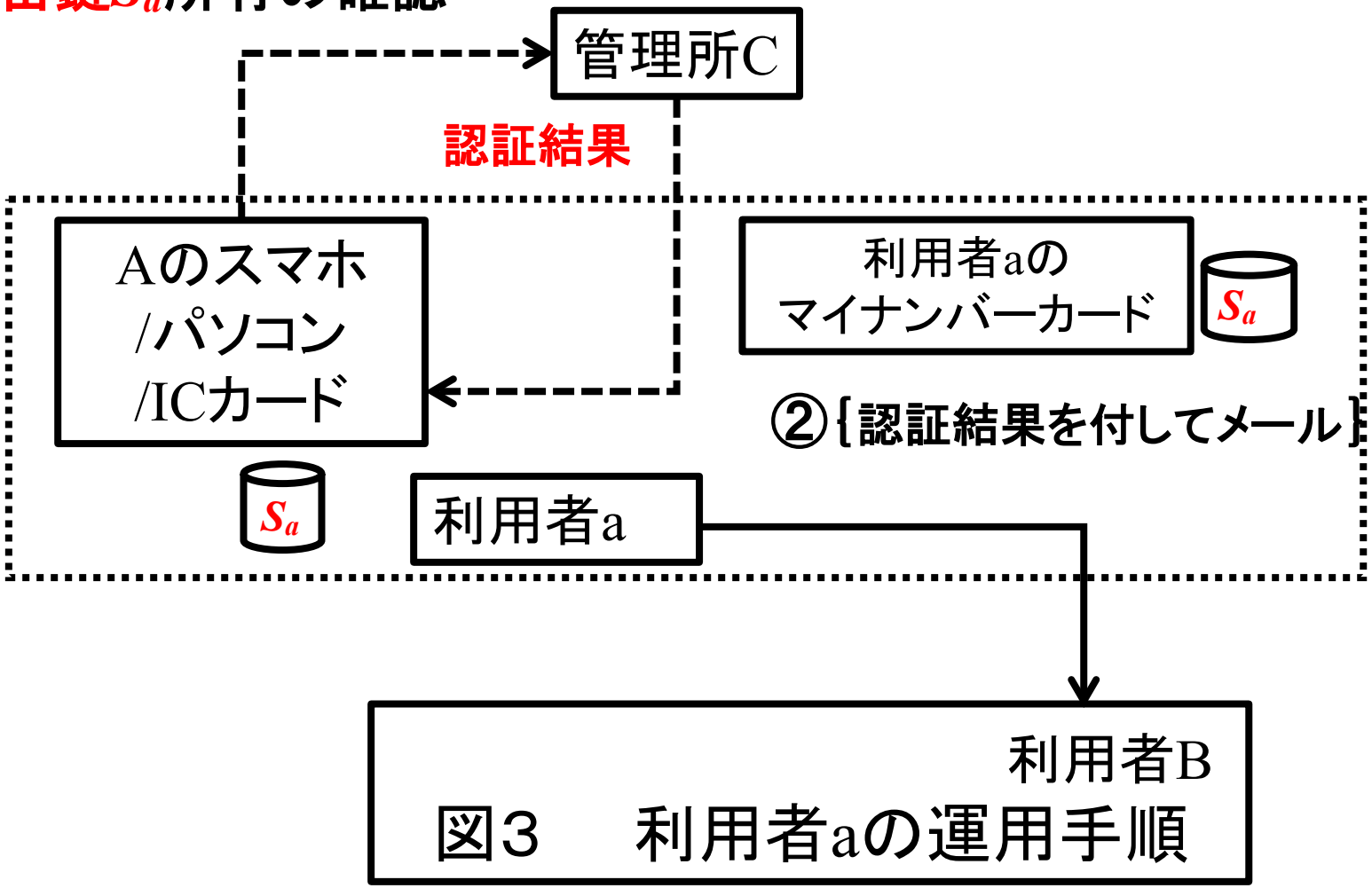


図３　利用者aの運用手順

6. 利用者の利便性の視点から

- 本研究で提案する、秘密鍵・極秘密鍵の2管理体制を
- すべての利用者に適用しようという訳ではない。

- 現状のマイナンバーカード運用管理で良いという人には、このままで良い。

- 秘密鍵が生命・財産に関わる状況下で、現状では不安であると感じている
- 組織・グループに利用して貰うために、図〇のようなシステム構成を提案する。

7.　安全性考察

暗号方式の安全性レベル（IND-CCA等）は、利用者が決定する。
離散対数問題の困難性を仮定する。
ハッシュ関数の1方向性を仮定する。

管理所C ,D ,利用者A のスマホ等、及び、マイナンバーカードの４者間
の情報漏洩についての安全性は下記の通り。

１）　管理所 C の　管理（消去・保管の秘密性）は完全とする。
２）　管理所 D の　管理（消去・保管の秘密性）は完全とする。
３）　秘密鍵 Sa1 から極秘密鍵 Sa を求めることは困難である。
４）　極秘密鍵 Sa から秘密鍵 Sa1 を、第3者が求めることは、管理所CがHc(　)
を秘密保管している 為、困難である。

付録１　　本提案に対するＱ＆Ａ

Q&A

Q　「極秘密鍵」の入ったスマホ・パソコンは盗難に遭わない
　と仮定するのでしょうか？

A　違います。
「極秘密鍵」の入ったスマホ・パソコンが盗まれた場合でも、
マイナンバーカードだけでは、remote 本人確認が出来ない
ように、
運用時も、シノア署名で極秘密鍵所持をremote 認証
するするわけです。

（マイナンバーカードには、秘密鍵は入っているが、
秘密鍵から極秘密鍵が　数理的にも割り出せない
ー図　2参照））