日本におけるヘルスケアPKI（HPKI）の最新動向

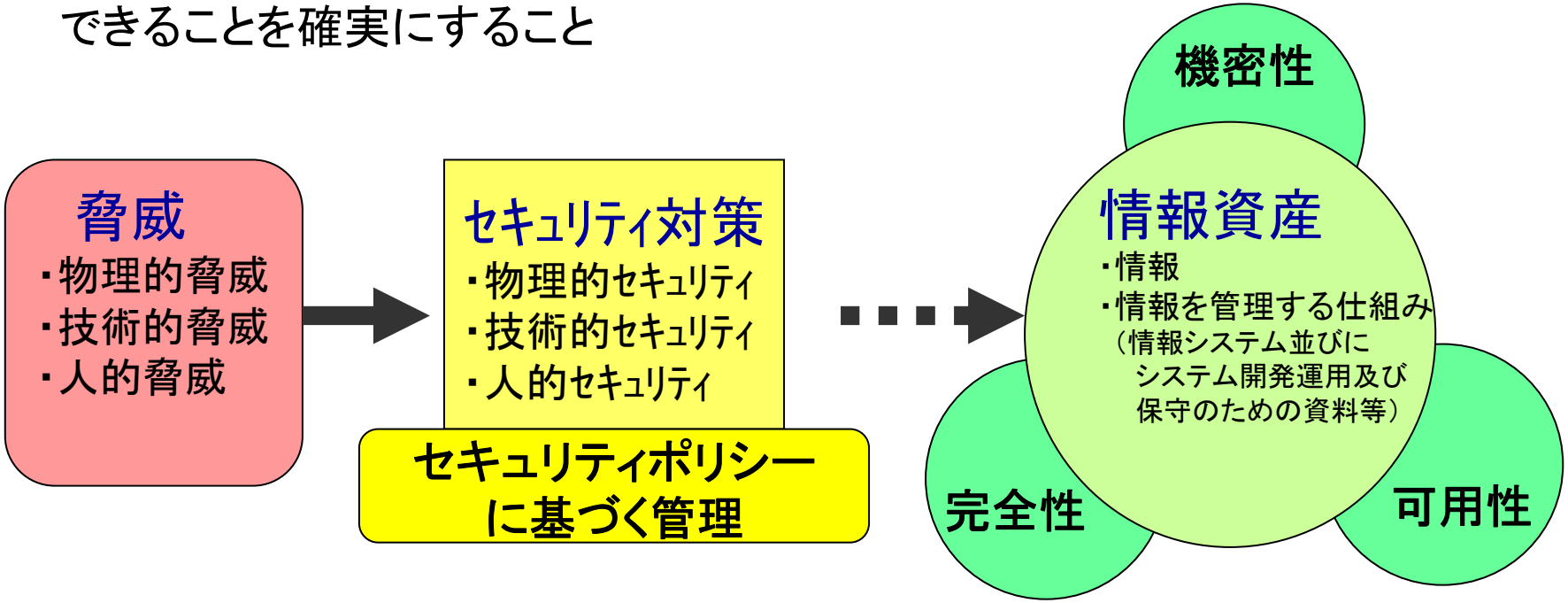
保健医療福祉情報システム工業会
セキュリティ委員会
委員長　茗原秀幸

１．情報セキュリティとは

情報セキュリティとは

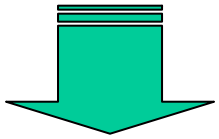
情報資産の機密性、完全性及び可用性を維持すること。

- 機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること
- 完全性（integrity）：情報及び処理方法の正確さ及び完全である状態を安全防護すること
- 可用性（availability）：認可された利用者が、必要なときに情報にアクセスできることを確実にすること



情報の保護を行うために必要なこと

- セキュリティポリシーの策定と施行
  - 組織の情報資産を適切に保護するための対策について組織的に取り組む統一基準
- セキュリティ対策技術の利用
  - アンチウイルスソフトやファイア・ウォール等の製品



セキュリティ対策には、
①ポリシー策定、組織運用などの組織的もしくは運用的対策
②ファイアーウオール、暗号化などの技術的対策
が必要で、全体の対策レベルは一番低いものに引きずられる!!

情報セキュリティの目標（例）
【何のためにセキュリティマネジメントを実施するのか】

（１）個人情報の保護

医療・健康情報は個人情報のなかでも特に重要な情報であり、情報の漏洩が本人の人生を大きく左右することも考えられる。情報提供機関は取り扱う情報の重要性を認識し、適切に管理しなければならない。

特に重要な対策（管理策）例としては以下のようなものがあげられる

個人情報保護の観点から医療・健康情報の機密性の維持をおこなうこと

（２）誤った情報による事故の予防

医療・健康情報の完全性が維持されない場合、誤った情報に基づく業務が実施される恐れがある。情報提供機関は事故防止の観点から社会保障情報の完全性の維持に努めなければならない。

特に重要な対策（管理策）例としては以下のようなものがあげられる

適切な業務を行なう観点から医療・健康情報の完全性の維持をおこなうこと

（３）サービス機能の維持

情報提供機関は社会インフラが多大なダメージを受けても速やかに機能回復し、継続して業務を行なえるようにする必要がある。また、悪意を持った攻撃に対する適切な防御手段を用意し、サイバーテロなどに対処できるようにしなければならない。

特に重要な対策（管理策）例としては以下のようなものがあげられる

情報提供機関の機能維持のために情報システムの可用性の維持をおこなうこと

ITを活用した、安全、安心な仕組み

- 個人情報の保護のために必要なこと
  利用者が間違いなく本人だと確認するための手段の整備
  →なりすましの防止
  →アクセス時の本人**認証**手段の整備
- 誤った情報による事故の予防のために必要なこと
  情報の作成が本人の手により間違いなく行われたと確認するための手段の整備
  →偽造、改ざんの防止と否認防止
  →医療・健康情報作成時の電子**署名**の手段の整備

情報セキュリティマネジメントの結果としての
管理策として選択されるべきもの

2.技術的対策としてのPKIの利用

PKIとは何か

PKI : Public Key Infrastructure（公開鍵基盤）

電子署名（デジタル署名）、電子認証、親展（暗号化）を実現するための公開鍵暗号を利用したセキュリティ基盤

情報セキュリティの「技術的セキュリティ対策」の有力な手段

各種セキュリティ機能を、高度なセキュリティ水準で実現

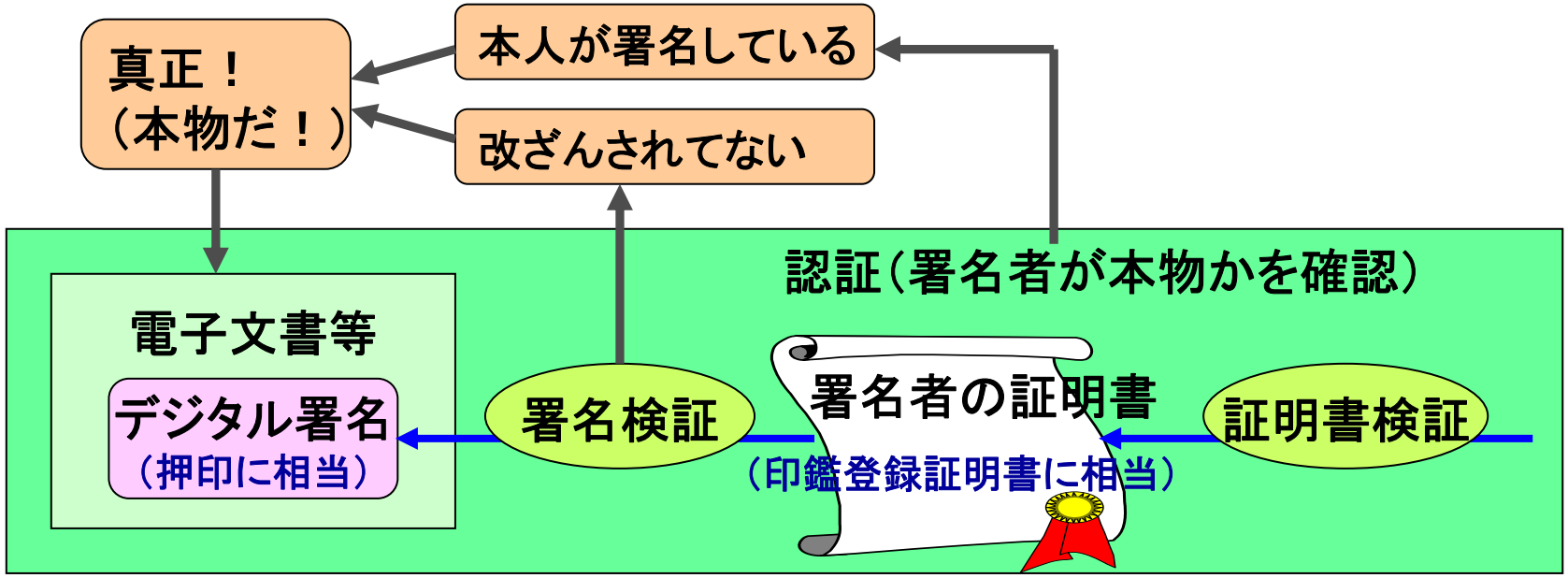
改ざん対策　→　デジタル署名
成りすまし対策　→　認証
盗聴対策　→　暗号化
否認対策　→　デジタル署名

PKIの主な働き　（デジタル署名、認証、親展（暗号化）について）

(1) デジタル署名（以降、単に署名とも称す）

利用者の意思に基づき、アプリケーションによって、承認、検認、文責等の意味で署名する。
署名された電子文書等を署名検証することによって、電子文書等の改ざんを検出できる。また、併せて署名者の証明書を証明書検証することによって、署名者を認証し否認（作成者が知らないと言い逃れる）を防ぐことができる。

★ 電子文書等の真正性確認のための働き　（電子署名法に対応）

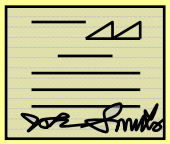


電子署名認証業務法

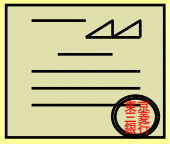
「電子署名及び認証業務に関する法律」 平成12年5月31日成立、平成13年4月1日施行

- ●郵政省（現総務省）・通産省（現経済産業省）・法務省の3省庁の共管、共同製作
- ●2000年5月成立、2001年4月から施行
- ●電磁的記録の真正な成立の推定と特定認証業務の認定及び国の役割、罰則

民事訴訟法第228条第4項



署名

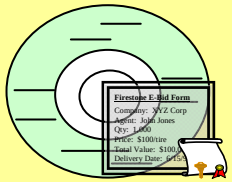


押印

「本人または代理人の署名又は押印がある時」 → 「私文書は、真正に成立したものと推定」

電子署名に対する法律上の取り扱いを明確化

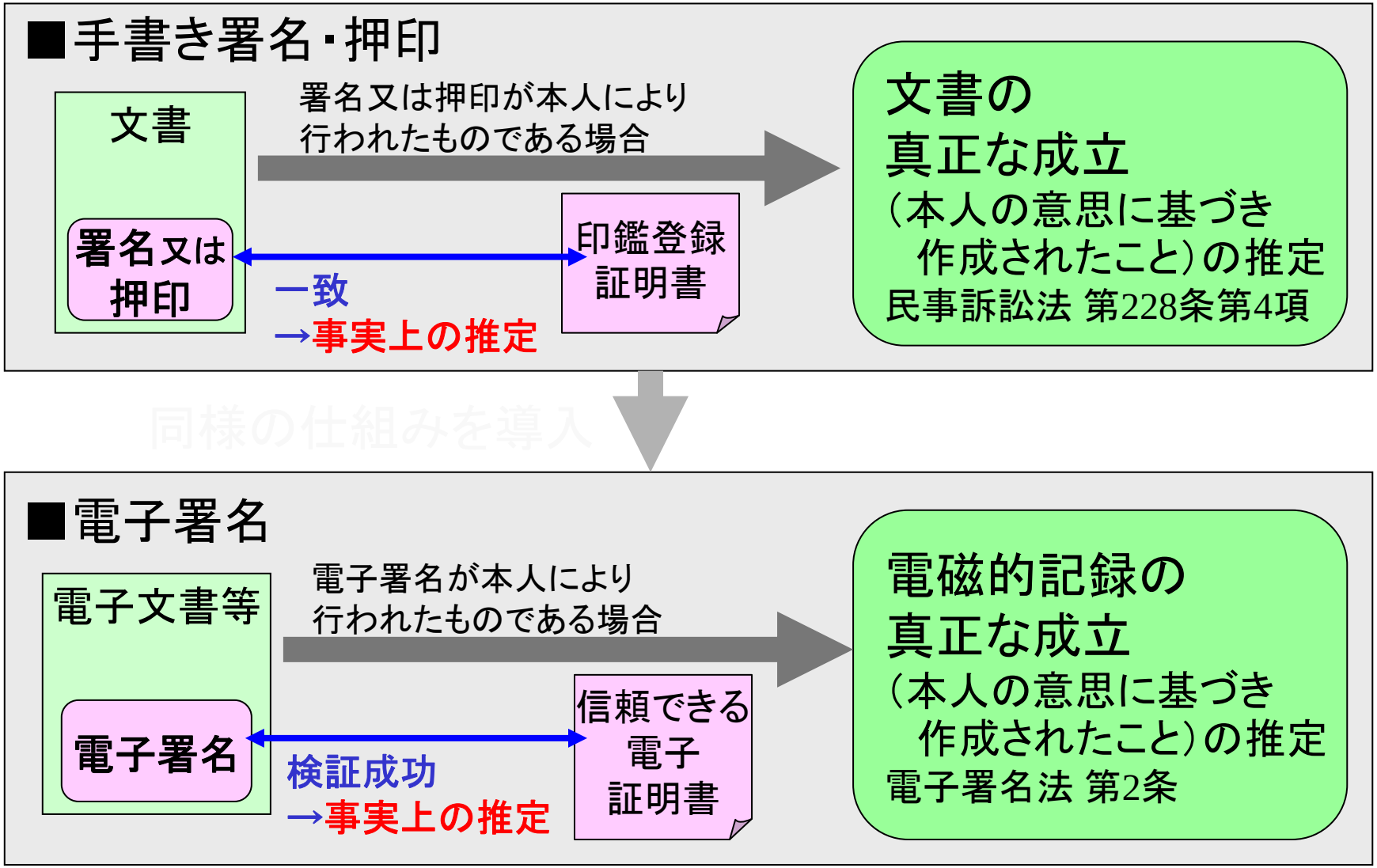
電子署名及び認証業務に関する法律第3条



電子署名

「本人による電子署名が行われている時」 → 「電磁的記録に記録された情報は、真正に成立したものと推定」

電磁的記録の真正な成立の推定



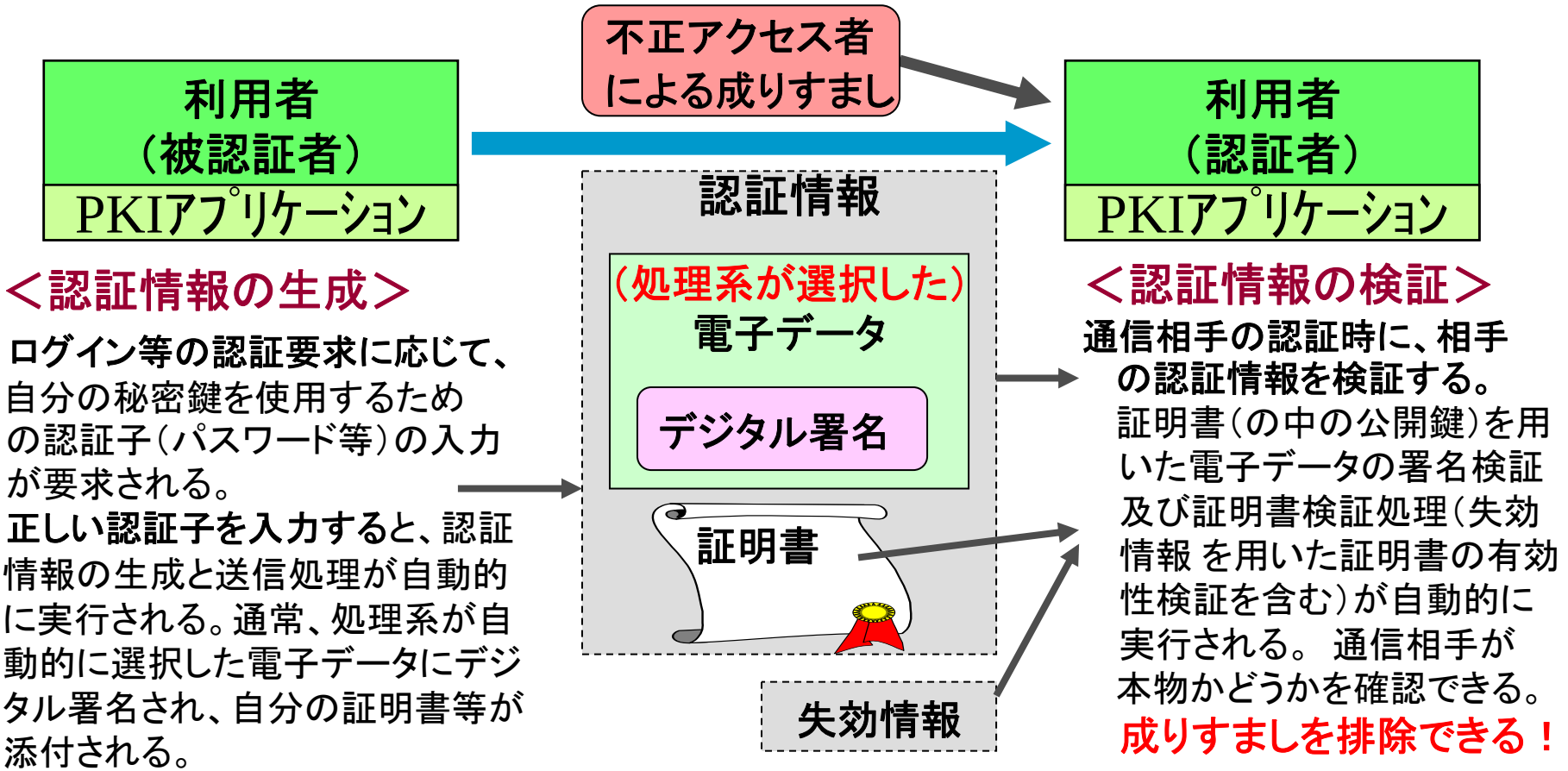
(2) 認証

成りすまし対策手段。

＜認証の利用イメージ＞

署名意思を伴なわない認証モデル

利用者は署名するという意識を持たない。内部的には、PKI処理系が自動的に署名対象データを選択して署名を行う。（電子署名法の対象外）



＜認証情報の生成＞

ログイン等の認証要求に応じて、自分の秘密鍵を使用するための認証子（パスワード等）の入力が要求される。

正しい認証子を入力すると、認証情報の生成と送信処理が自動的に実行される。通常、処理系が自動的に選択した電子データにデジタル署名され、自分の証明書等が添付される。

＜認証情報の検証＞

通信相手の認証時に、相手の認証情報を検証する。

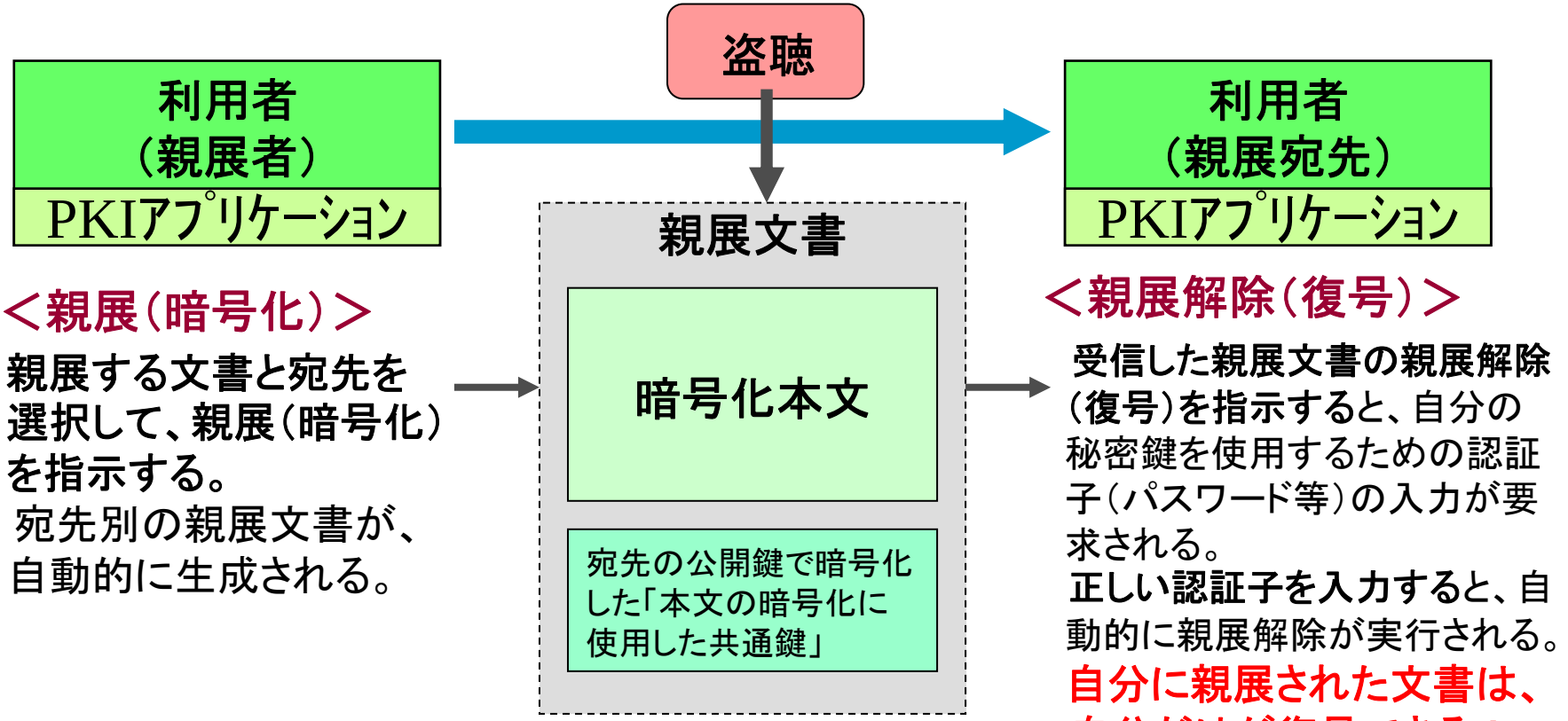
証明書（の中の公開鍵）を用いた電子データの署名検証及び証明書検証処理（失効情報 を用いた証明書の有効性検証を含む）が自動的に実行される。 通信相手が本物かどうかを確認できる。

成りすましを排除できる！

(3) 親展（暗号化）

盗聴に対抗するデータ秘匿手段。
宛先別に暗号化されるので、宛先の人以外には復号できない。
（Aさんに親展した文書は、Aさんしか見れない。）

＜親展の利用イメージ＞



＜親展（暗号化）＞

親展する文書と宛先を選択して、親展（暗号化）を指示する。
宛先別の親展文書が、自動的に生成される。

＜親展解除（復号）＞

受信した親展文書の親展解除（復号）を指示すると、自分の秘密鍵を使用するための認証子（パスワード等）の入力が要求される。
正しい認証子を入力すると、自動的に親展解除が実行される。
自分に親展された文書は、自分だけが復号できる！

公的個人認証基盤の問題点

本人性・実在性を担保する電子署名（用途その１）として既に公的個人認証基盤が存在する。

しかし、

（１）検証者になれる者に制限がある。

（たとえば民間病院や調剤薬局、健保組合はNG）

（２）基本四情報が証明書に記載されているため、本来公開する必要のない情報が相手先に漏れる。（電子申請なら問題ないが、医療文書交換では問題になる可能性がある）

（３）医師資格などの国家資格が単独では確認できない。

たとえば、東京大学医学部附属病院の山元龍一先生（仮名）が
電子診断書に公的個人認証基盤で署名すると、
患者は山元龍一先生の基本四情報を知ることができる。

3.署名用HPKIの必要性と推進状況

署名用ヘルスケアPKI（HPKI）の推進

医療情報ネットワーク基盤検討会における検討
厚生労働省によるCP（証明書ポリシ）の策定
準拠性監査ルールの策定

HPKIにおける署名用途とそれ以外（認証用・暗号用）の分離
署名用途は全国統一のルールが必要
属性を含む個人認証用は全国統一ルール策定には時期尚早
暗号用は既に広く普及（SSL、IPSECなど）

属性つき署名用証明書が何故必要か
→国家資格の確認の必要性
→医療機関の管理者の確認の必要性

HPKIの狙い

一つの証明書検証で、本人性と属性を一度に確認できること。

国家資格の確認：診療情報提供書（紹介状）には医師の署名（もしくは記名押印）が必要。

医療機関の管理者の確認：電子契約への応用の可能性を開く。電子レセプトにおける発行責任者であるかの確認を行うことも技術的には可能となる。

HPKIの国際規格（ISO IS17090）
との整合性を取りつつ
日本の社会インフラとして整備する

ネットワーク基盤検討会最終報告書

今後の医療情報ネットワーク基盤のあり方について

ネットワーク基盤検討会最終報告

（平成16年9月30日）

署名用証明書のための公開鍵基盤の整備

診断書や診療情報提供書の電子化を認める

外部保存の受託可能機関の拡大

e−文書法への対応に関する指針の提示

HPKI認証局の準拠性監査基準の策定

- 保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議設置（平成17年7月）
  - 医療情報ネットワーク基盤検討会で策定された証明書ポリシに準拠した各認証局の準拠性を公正に審査するための体制等について検討を実施。
  - 当該会議の下に設置された専門作業班で準拠性監査基準を作成
  - 同時に、証明書ポリシのメンテナンス（改定、修正）を実施

IT新改革戦略重点計画2006

ITによる医療の構造改革

- 医療の情報化のための共通基盤の整備（以下演者が要約）
  - 個々のHPKI認証局が共通のHPKI証明書ポリシに準拠していることを示す証明書を発行する認証局を2006年度までに構築し運用を開始する。（厚生労働省）

厚生労働省が協力を依頼している日本医師会のHPKI認証局と医療情報システム開発センター（MEDIS-DC）のHPKI認証局が厚生労働省の定める証明書ポリシの準拠性監査に合格すれば厚生労働省のRoot－CAを信頼点として相互認証が可能となる

医療分野の申請の添付書類の電子化

医政発第0622010号　平成18年6月22日

厚生労働省医政局長

「書面に代えて電磁的記録により作成、縦覧等又は交付等を行うことができる医療分野に係る文書等について」

演者による要約:（正しい解釈は原文を参照願います）

医療分野における各種申請、請求などに関する手続きにおいて求められる医師などの証明書が必要と考えられる添付書類（診断書や証明書など）について電磁的記録により作成、交付および署名を認めることとする。

手続名と添付書類の例:(通知の別紙に記載されているものの抜粋)

健康保険疾病手当金請求書→疾病の状態に関する医師又は歯科医師の意見書

医療情報システムの安全管理に関するガイドライン第4 版（平成21年3月）

6.12 法令で定められた記名・押印を電子署名で行うことについて（抜粋）

（1）厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

1. 保健医療福祉分野 PKI 認証局については、電子証明書内に医師等の保健医療福祉に係る資格が格納された認証基盤として構築されたものである。保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、この保健医療福祉分野PKI 認証局の発行する電子署名を活用するのが望ましい。ただし、当該電子署名を検証しなければならない者すべてが、国家資格を含めた電子署名の検証が正しくできることが必要である。

（2）電子署名を含む文書全体にタイムスタンプを付与すること。

（3）上記タイムスタンプを付与する時点で有効な電子証明書を用いること。

デジタル新時代に向けた新たな戦略
～三か年緊急プラン～ （平成21年4月9日IT戦略本部）

日本健康情報コミュニティ（仮称）構想の実現

○ デジタル技術を活用した地域医療連携による地域医療の再生
○ 遠隔産科医療、遠隔画像診断等による安全・安心な医療
○ 健康情報の集積・活用の実現による医療の質の向上
○ 健康サービス産業の創出による生涯を通じた健康・疾病管理

２．取組みの概要

（３）医療機関等のデジタル基盤の整備

医療従事者間の情報伝達・共有のため、健康情報へのセキュアなアクセス実現に不可欠な認証基盤を整備するとともに、新規資格取得医師等及び希望する既取得者に対し、医療における公開鍵基盤（HPKI）を実装するHPKI カード等の適切な支給方法等を検討の上、必要な支援を行う。

4.認証用HPKIの検討のために

医療分野の属性認証の必要性

本人性の確認のみであれば、将来的には社会保障カード（仮称）などのフレームワークが利用可能かもしれないが…

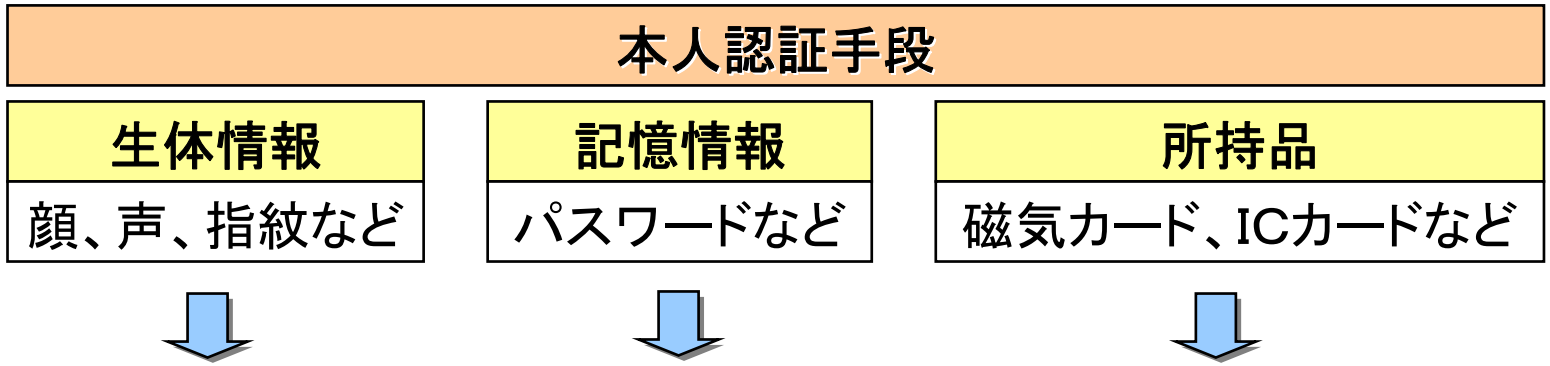
医療分野におけるITの利用においては、医療の専門家であることを担保する仕組みが必要になる

- 医師でなければ作成できない記録などが存在する
- 業務アプリケーションに対するより厳密なアクセス制御をする場合には、属性認証が必要になる

従来は、各医療機関内や地域ドメイン内で
独自の属性認証の仕組みを個別に構築していた.
→施設間や地域間での互換性なし

検討課題：全国統一の属性を含む認証基盤の構築は必要か！？

本人認証技術とICカード



安全管理のガイドラインでは2要素認証を要求しているため、
上記3要素のうち二つ以上を組み合わせて利用することになる

さまざまな認証手段があるが、認証する側は、上記情報が確かであることを何らかの形で管理、運用しなければならない。

医療機関内であれば、各医療機関が独自にルールを決めて採用すればよいが、全国共通ルールを策定する場合は、全国的に信頼されるスキームを構築する必要がある。

全国共通のなりすまし防止のために

- 生体認証やパスワード管理を全国統一で実施するためには全ユーザーの個人情報を統合管理し、メンテナンスする必要があるが、安全性の定量的な担保という点においてはPKIほど確立した手法は現状ない。
- また、生体情報やパスワードをセンターで管理する手法の場合、そこから情報漏えいした時点で機能不全となる。
- 現状、PKIに代わる適切なフレームワークは見出せていない。

認証用HPKIの狙い

HPKIであれば、一つの証明書検証で、HPKI認証局が信頼されていれば全国どの組織においても本人性と属性（国家資格）を一度に確認できる

本人性の確認：

本人性、実在性を認証用HPKIルート認証局が信頼点として保証することで、異なる組織間においても本人性が担保される。

国家資格の確認：

国家資格の保有についても、認証用HPKIルート認証局が信頼点として保証するため、異なる組織間において属性が担保される。

国際規格（IS17090）との整合性を取りつつ認証用においても日本の社会インフラとして整備する

何故認証用HPKIは平成16年のネットワーク基盤検討会最終報告で時期尚早とされたのか

全国レベルで属性を含む個人認証を実現するためには、その技術的基盤（例えばPKIやSAMLなど）が整備されるだけではなく、それぞれの医療機関の定義する役割が何らかの形で標準化され、医療機関同士で交換可能になるためのポリシ合意がないと不可能。

コンテナはあってもコンテンツがない。
先にコンテナを定義するのは無意味とは言えないが
具体的な業務運用イメージもない状況で
先に定義するのは時期尚早ということ

認証用HPKIだけでは不十分

- 日本のHPKIにおいては、長期的に変わらない属性を管理することとしている。
  - 認証局が担保する属性であるため、国家資格などの公的に確認できる属性でないと確認が難しい。
  - 証明書の有効期限は一般的に2年程度であり、短期的に保持する属性は証明しにくい。
- アクセス制御にはきめ細かに属性を定義する必要があるが、HPKI証明書がサポートする属性のみでは対応できないものがある。
  - 医療チームメンバーか？、当直医か？、麻酔科医か？、＊＊病院職員か？etc

第２１回医療情報ネットワーク基盤検討会資料
個人が自らの医療情報を管理・活用する基盤を構築する際に必要となる医療従事者の認証方式について

結論（抜粋）

・想定するユースケースにおいて本人性、実在性、国家資格保有を確認できる全国共通のフレームワークは有用であり、09 年度以降に具体化に向けた検討を行うことが求められる。特に認証ポリシの検討、運用方式の検討、署名用HPKI 発行主体との連携などについて検討を行う必要がある。

・国家資格をもつ医療専門職の本人性・実在性・国家資格を認証する仕組み以外の認証フレームワーク構築の必要性も考えられるので、継続して検討を実施する必要がある。

平成21年度の医療情報ネットワーク基盤検討会作業班の検討状況

- 当日最新動向をお話いたします。

4.JAHISセキュリティ委員会の取組み

HPKI電子署名規格検討WGの活動

- ガイドラインとの整合性を持つ電子署名規格を整備
- 厚生労働省によるHPKIルートCA構築に対応した産業界による標準規約を制定
- W3CやJISなどの標準規約を採用したルール化
- タイムスタンプや長期署名に対応
- HPKI対応ICカードガイドライン検討WGとの連携。
- 日医、MEDISなどの発行機関との連携をはかり実効性のある規約を作成

「医療文書に対するHPKI電子署名規格」の概要

- 長期署名規格としてヨーロッパのESTI、日本のJISで採用されたXAdES、CAdES方式をそのまま採用し日本の電子署名法やHPKIのCPを考慮した実装規格として規定
- タイムスタンプと組み合わせることにより半永久的に完全性（改ざんされていないこと）を担保することが可能。
- 医療分野の電子署名が必要となるユースケースを解説

主にPKIアプリケーションベンダー向けの実装規約だが
業務アプリケーションベンダーにおいても
電子署名を実装する際に参考になるように記載

HPKI対応ICカードガイドライン作成WGの活動

- 署名用HPKI証明書と私有鍵（秘密鍵）を格納するためのICカードのカードアプリケーションのガイドラインを策定。
- ISO／IEC7816part4,8,15に準拠
- HPKI秘密鍵、証明書を格納するデータモデルを提示
- HPKI電子署名を行う際のシーケンスを提示
- 発行（鍵・証明書の格納）はスコープ外

主にカードベンダー向けのガイドラインだが、
PKCS#11やCSPの開発ベンダーや上位PKIアプリケーション
ベンダーにも参考になる

認証用HPKIへの対応

- 今年度、署名用HPKI電子署名規格とは別の認証用HPKI電子署名規格を策定中
- 従来の署名用HPKIのために作成したHPKI対応ICカードガイドラインを認証用HPKIを含めたガイドラインに改定中。

厚生労働省の検討状況を反映し、
タイムリーなJAHIS標準の策定を目指す

ありがとうございました