

電子私書箱(仮称)による社会保障サービス等のIT化に関する検討会報告書
参考資料2

技術検討ワーキンググループ 報告

平成20年3月17日

1. 検討の方針
2. 電子私書箱の全体像
 1. 電子私書箱の実現のイメージ
 2. アクタの定義
3. 主な検討課題
 1. 主な課題の位置づけ
 2. アカウント管理
 3. 情報取扱制御
 4. セキュリティレベルを反映した情報の構造化
 5. 送受信確認
4. 課題に対する方向性及び実現案の例示
 1. トラストの考え方
 2. アカウント管理
 3. 情報取扱制御
 4. セキュリティレベルを反映した情報の構造化
 5. 送受信確認
 6. 全体像の例示

付録

電子私書箱の情報の持ち方

技術検討参考資料

1.検討の方針

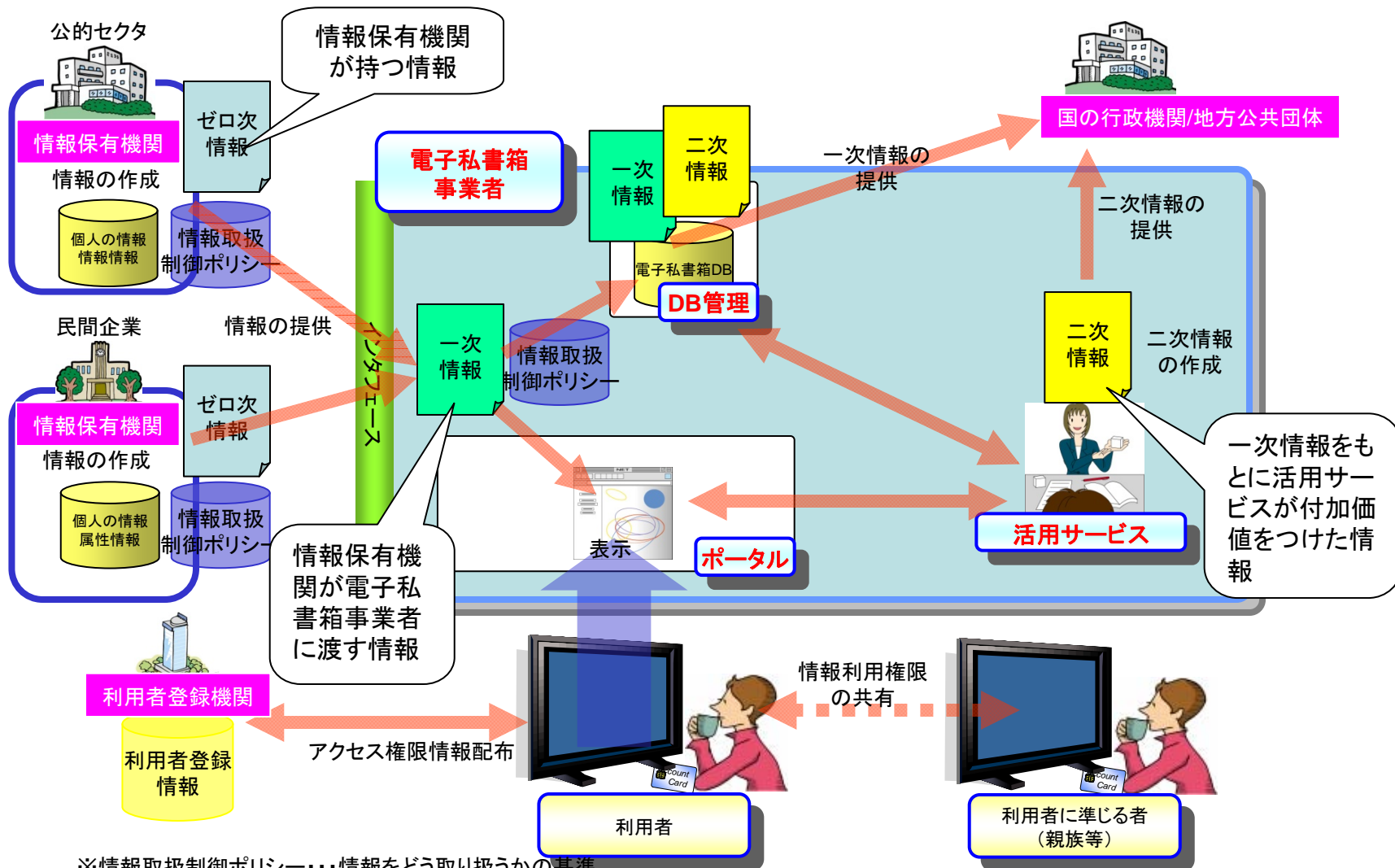
電子私書箱の技術的課題について以下の基本的な方針に従い検討する。

- ◆ 情報セキュリティを確保し、かつプライバシー保護を目的とした課題のうち、特に情報の流通の観点における「主な課題」を検討する。その他の課題については、今後の検討に委ねるが抽出のみ行う。
- ◆ 現在想定できる社会保障関連の電子私書箱のサービスだけでなく、将来の情報活用の様々な可能性を排除しない拡張可能な仕組みとする。
- ◆ 標準規格に準拠した技術又は、実用化されている技術を採用する(技術について特定するが、製品選定は行わない)。

なお、「4.6全体像の例示」の「4.6.2トラストによる情報管理モデル」については、本検討における仮定をもとに作成したモデルの一例であり、引き続き検討が必要。

2.電子私書箱の全体像

◆ 電子私書箱を「個人が保有もしくは個人に付帯する情報を物理的もしくは仮想的に集約し、活用する場を提供するサービス」と定義。



※情報取扱制御ポリシー…情報をどう取り扱うかの基準

※利用者登録情報…利用者を識別する情報を管理する。公的個人認証などの認証局が考えられる。

※電子私書箱事業者が、ポータル、DB管理、活用サービスを含めて一体の事業として行うかどうかは別途検討が必要。

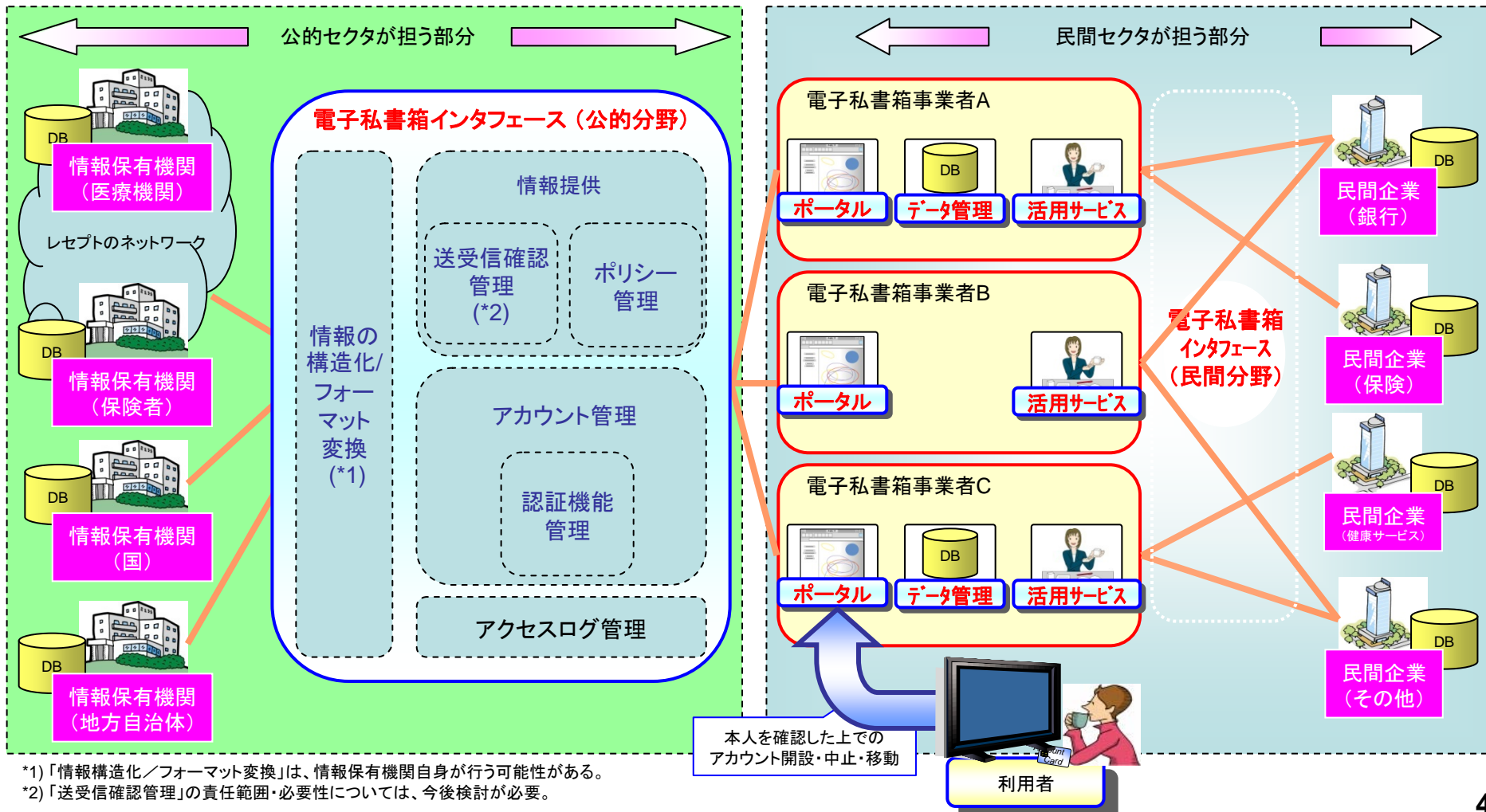
2.1 電子私書箱の実現のイメージ

【全体的な特徴】

- ◆ 公的セクタの情報保有機関に存在する情報を公的セクタが責任をもって、電子私書箱事業者を利用する利用者へ届ける

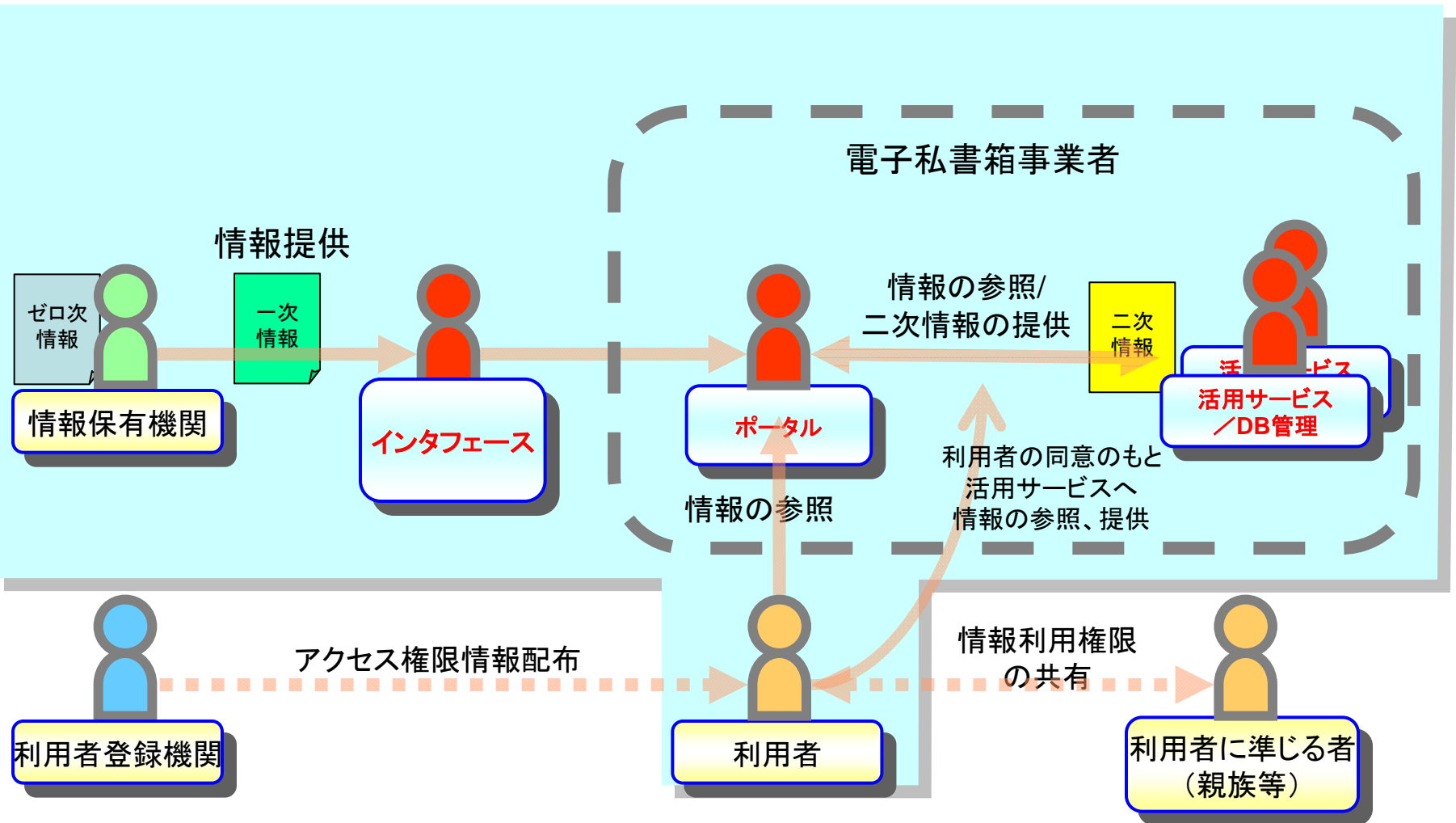
【公的セクタの取り組み】

- ◆ 電子私書箱インタフェース（公的分野）は公的分野の各情報保有機関と電子私書箱の間でデータを送受信
- ◆ 電子私書箱インタフェース（公的分野）ではデータを蓄積しない
- ◆ 制度、（電子私書箱事業者等への）ガイドラインは国が整備



2.2 電子私書箱を構成する関与者をアクタとして定義

- ◆ アクタ間の関係や各アクタ間の相互作用を表すために、全体像を簡略化
 - 赤のアクタは一体の事業者が行う場合、別々の事業者が行う場合が考えられる。
 - 利用者の同意のもと活用サービスへ情報の参照、提供も考えられる。



3. 主な検討課題

◆ トラストの考え方

- 電子私書箱サービス全体の中で、情報の配送に責任をもつアクタについて、電子私書箱サービスの枠組みに従って確実に動作するパーティの範囲をトラストと呼ぶ。この前提が個人のIDや機微な情報をいかに管理するかに影響を与える。

◆ アカウント管理

- 利用者が正しく電子私書箱を通して情報保有機関に保存されている利用者の情報を取得する必要がある。
- 情報保有機関等の利用者情報を入手するために必要とされる「情報」（例：基本4情報など。検索キーと呼ぶ）と利用者が電子私書箱に作成するアカウントとの結合手段（アカウント管理）を検討する。

◆ 情報取扱制御

- 情報への参照や設定などの処理の許可・不許可などのアクセスコントロールは、情報の特性（セキュリティレベル又はプライバシーレベル）に依存すると考えられる。
- 情報に関するアクセスの制限、制限の設定方法、設定可能な者（医療従事者、公務員、利用者本人など）の関連とその判断処理等を検討する。

◆ セキュリティレベルを反映した情報の構造化について

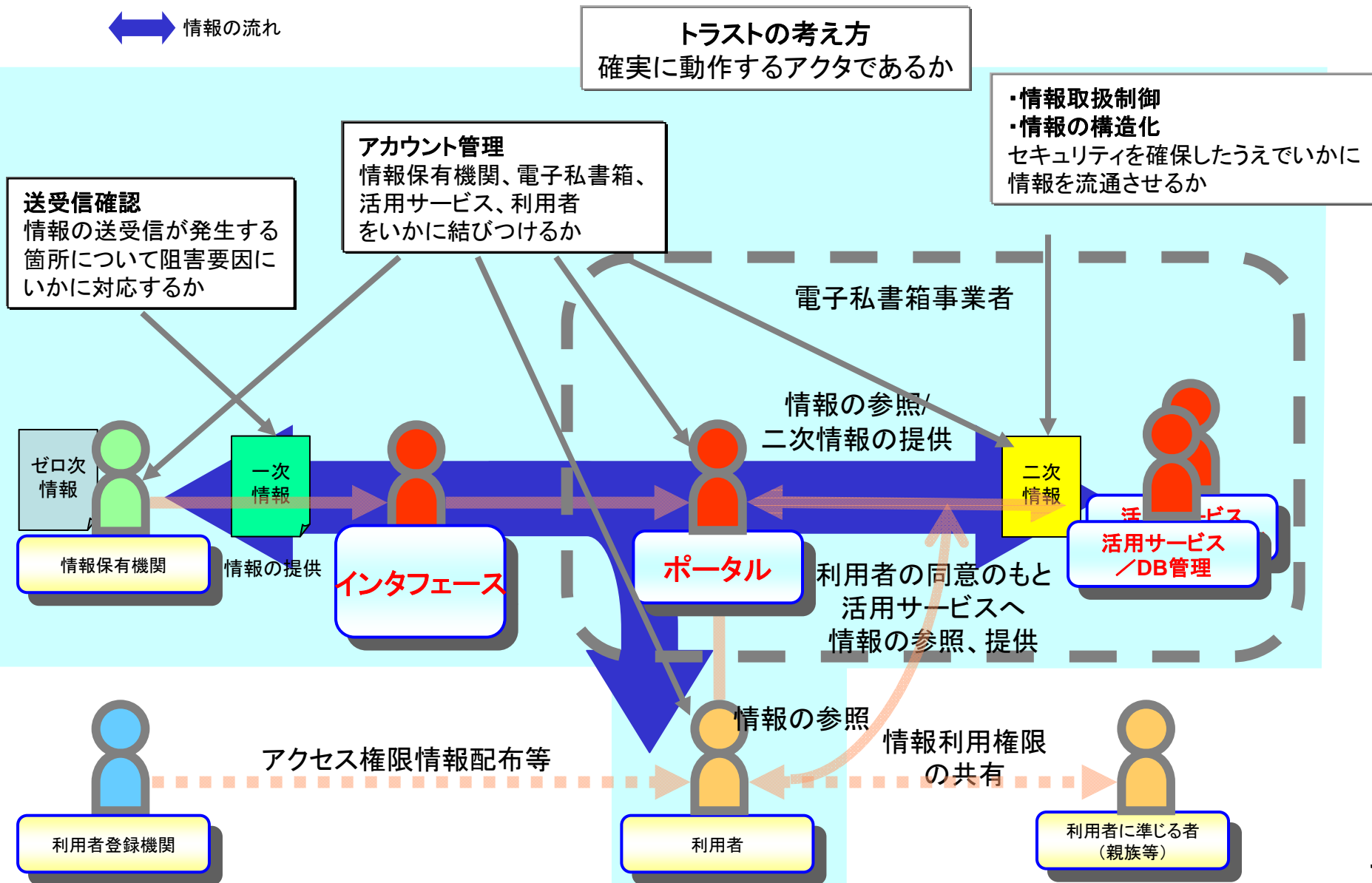
- 複数の異なる処理システムが解釈可能な情報として活用でき、また、処理する情報のセキュリティレベルをアクタ間で適切かつ確実に引き継げるようにするため、情報の構造化が有効ではないかと考えられる。
- 情報保有機関が提供する情報について、セキュリティレベルを反映できる構造化のための取組みについて検討する。

◆ 送受信確認（送受信証明）

- 特に機微な情報に関して、送受信の事実の保証について検討する必要がある。
- 複数のアクタ間における、送信・受信した事実及び許可された相手のみへの送受信の確認手段について検討する。

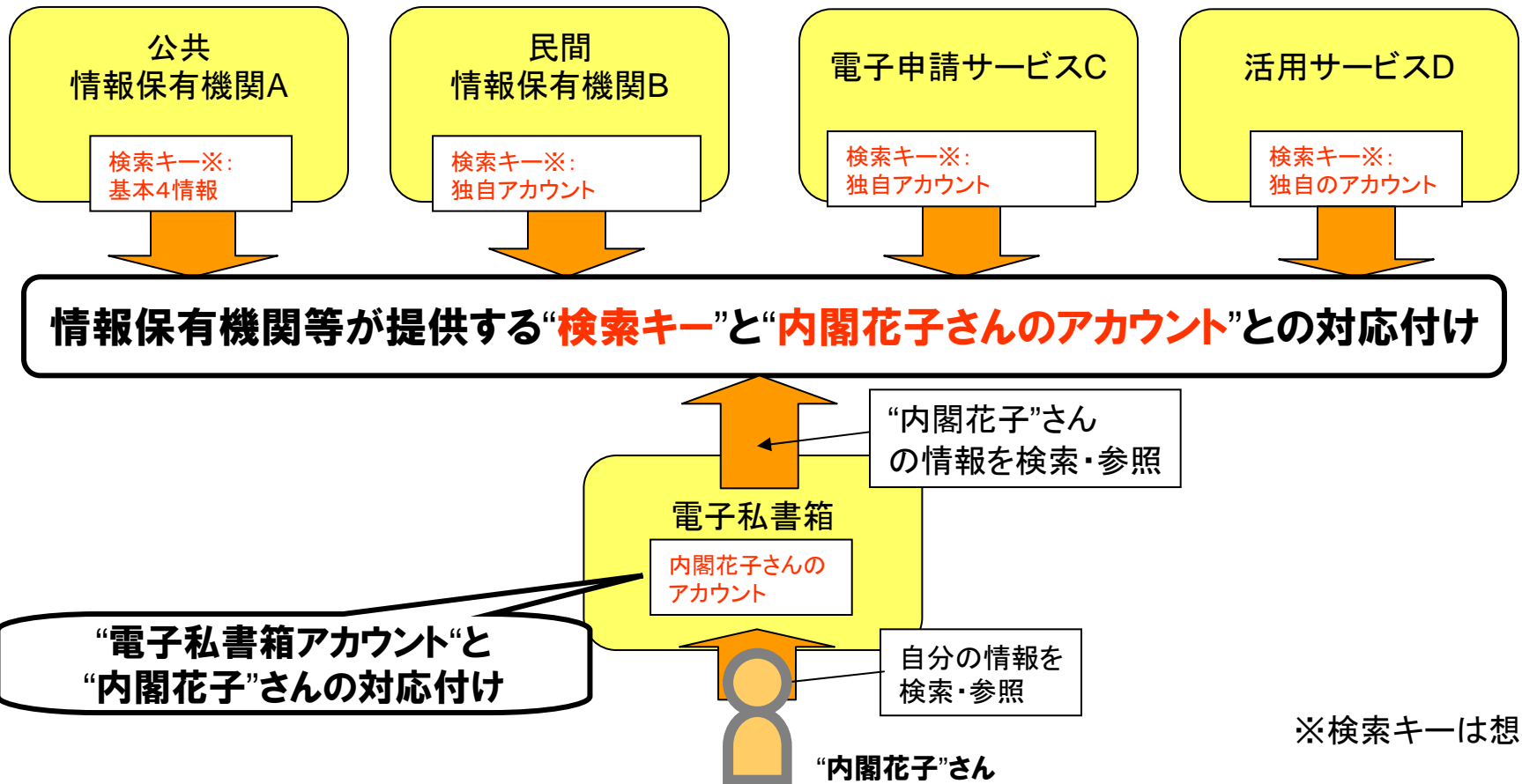
3.1. 主な課題の位置づけ

◆ 主な課題をアクタ定義の図に表す。



3.2 アカウント管理

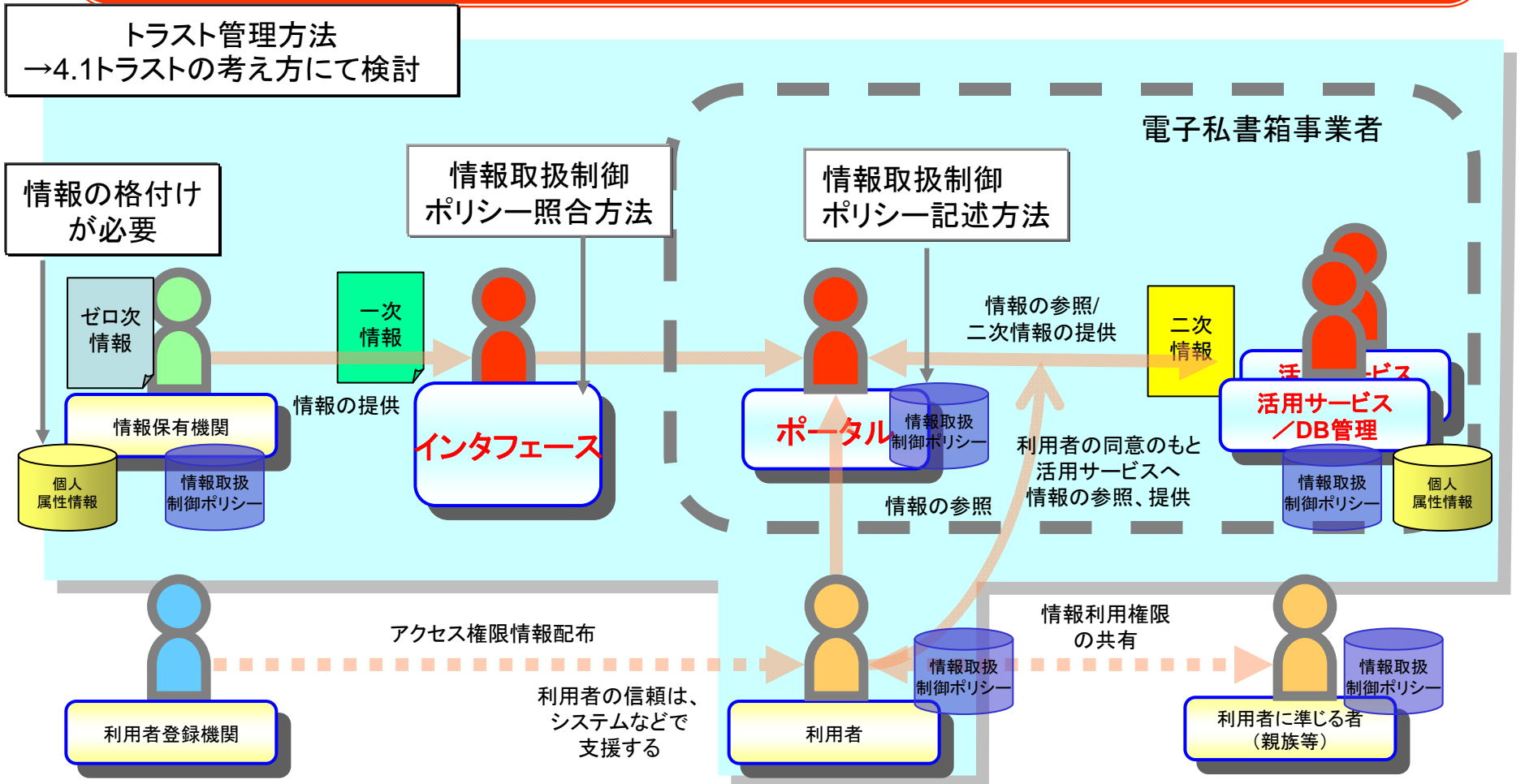
- ◆ 情報保有機関、活用サービス等において、特定の個人の情報をどのキーで検索可能かは、異なる可能性がある。
- ◆ 電子私書箱のアカウント・情報保有機関・利用者間の関連付けが必要である。
- ◆ 電子私書箱アカウントの管理と複数の情報機関の検索キーをいかに対応付けるかが課題となる。



“内閣花子”⇔“本人の電子私書箱のアカウント”⇔“検索に必要な情報(検索キー)”

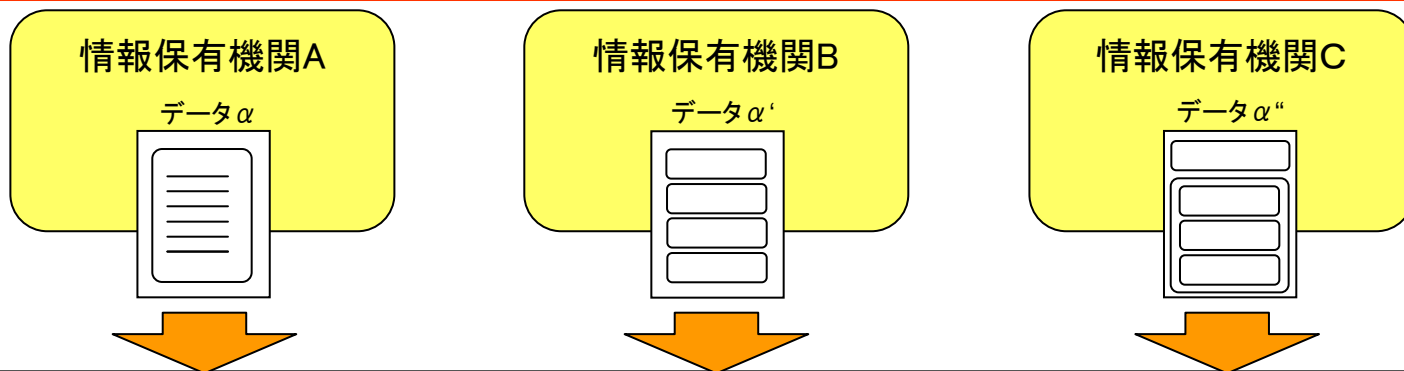
3.3 情報取扱制御

- ◆ 利用者の情報は、それぞれの情報保有機関で格付けされて取り扱われており、情報の流通時に情報取扱について合意を形成しなければならない。
 - 情報取扱制御ポリシー記述方法
電子私書箱の要件を満たす情報の取り扱いを制御する記述方法の検討が必要。
 - 情報取扱制御ポリシー照合方法
異なる情報の取扱制御ポリシーの照合方法の検討が必要。

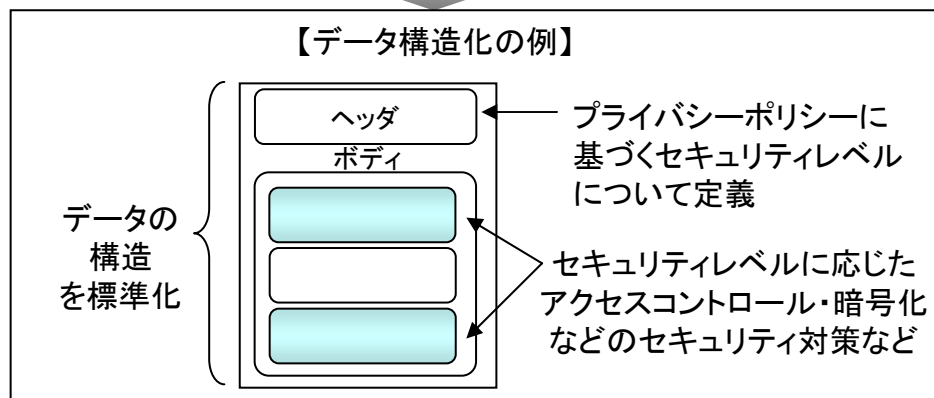


3.4 セキュリティレベルを反映した情報の構造化

- ◆ 電子私書箱、情報保有機関、活用サービスといった異なるアクタ間でデータ流通があるため、データ構造が統一されていないと、業務・システム双方の面で処理が煩雑となる。
- ◆ プライバシー情報を含むデータを異なるアクタ間で流通させるため、情報のセキュリティレベルを引き継ぐことが必要となるが、これを適切かつ確実にを行うためには、情報のセキュリティレベルを何らかの形で定義し、これをデータ構造のなかで表現することが考えられる。
- ◆ 異なるアクタ間でのデータ交換の効率性や利用者・活用サービスにおけるデータの利活用、さらには、プライバシーの厳格な保護を考慮すると、データ構造を整合させ、情報のセキュリティレベルも含めた標準化を図ることが望ましい。



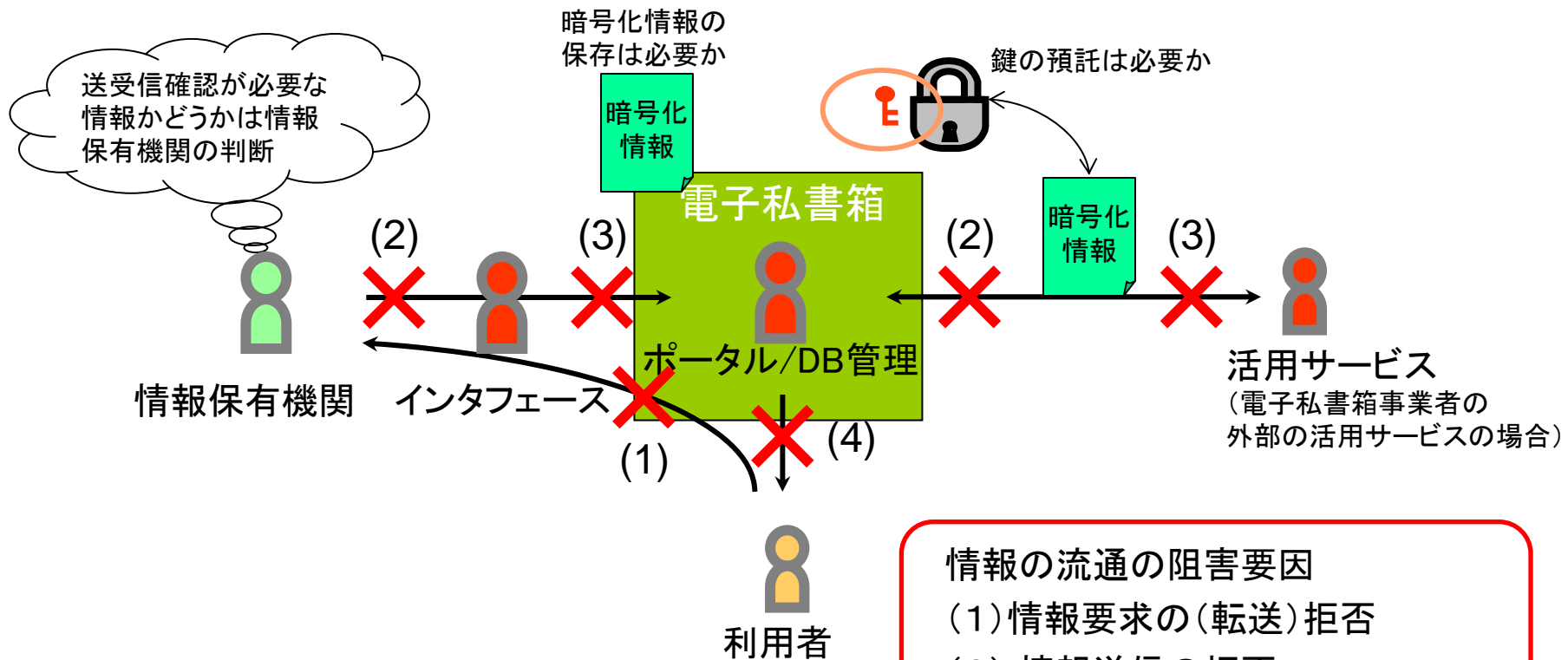
情報保有機関が提供するばらばらな**“データ構造”**を整合させることが望ましい



※情報の流通、活用のためには、民間セクタではデータ構造の整合が図られ、公的セクタではデータ構造の整合及びインタフェースの標準化がなされることが望ましい

3.5 送受信確認(送受信証明)

- ◆ 情報が、情報保有機関、電子私書箱、活用サービス、利用者間を流通する際に、情報要求の拒否、情報送信の拒否、情報受信の拒否、情報確認(提示)の拒否などが起き、情報の流通が阻害される可能性がある。
- ◆ ネットワークの安全性は確保されているなど、一定の前提を置いたうえで、(エラー処理も含めた)送受信確認の仕組みを技術的にどう対応ができるのかを検討する。
- ◆ 情報を秘匿(暗号化)し、相手に送信し、その暗号化情報を保存する場合は、鍵の預託について考慮する必要がある。



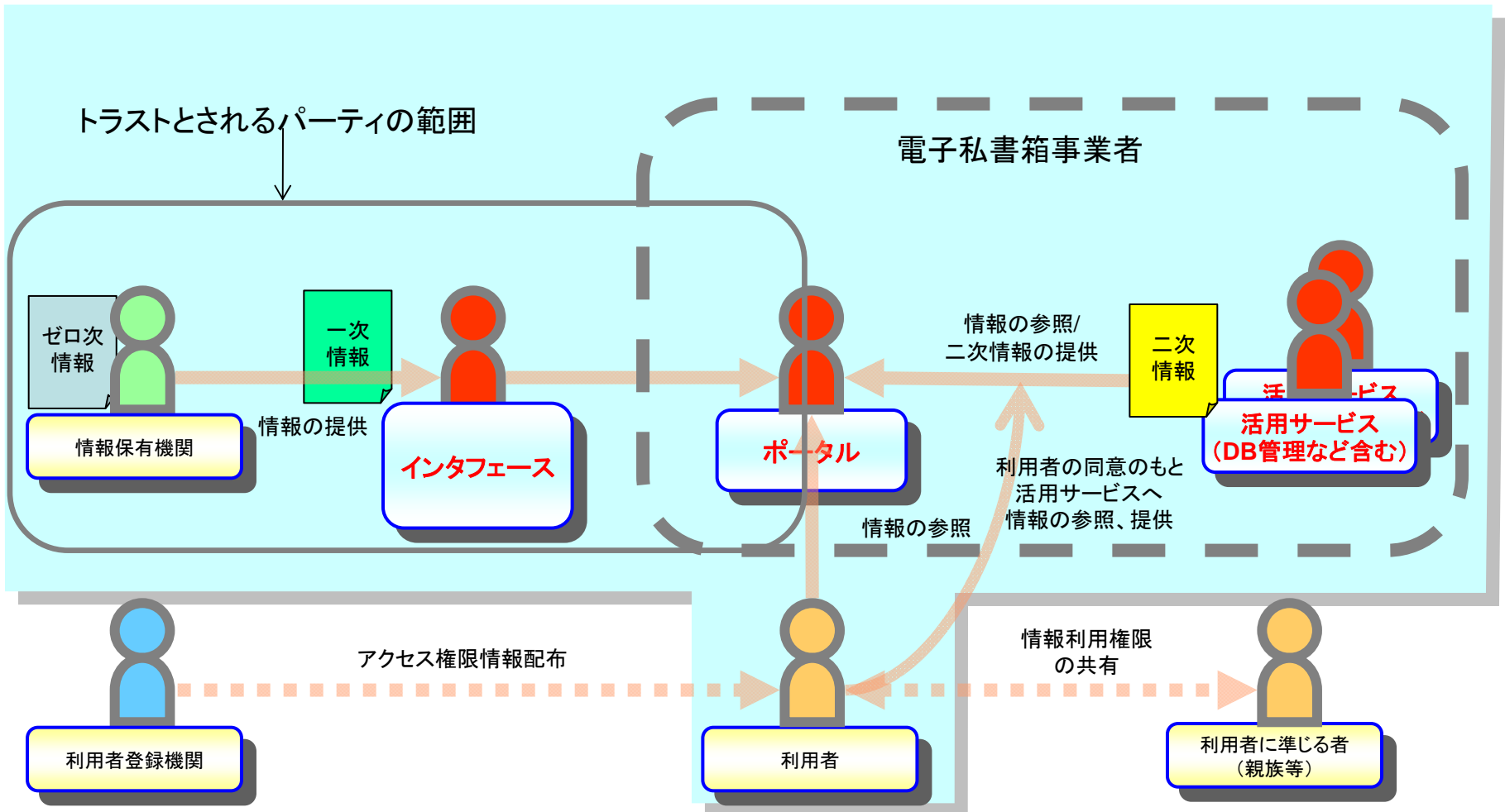
- 情報の流通の阻害要因
- (1) 情報要求の(転送)拒否
 - (2) 情報送信の拒否
 - (3) 情報受信の拒否
 - (4) 情報確認(提示)の拒否

4. 課題に対する方向性及び実現案の例示

4.1 トラストの考え方

4.1.2 トラストの定義

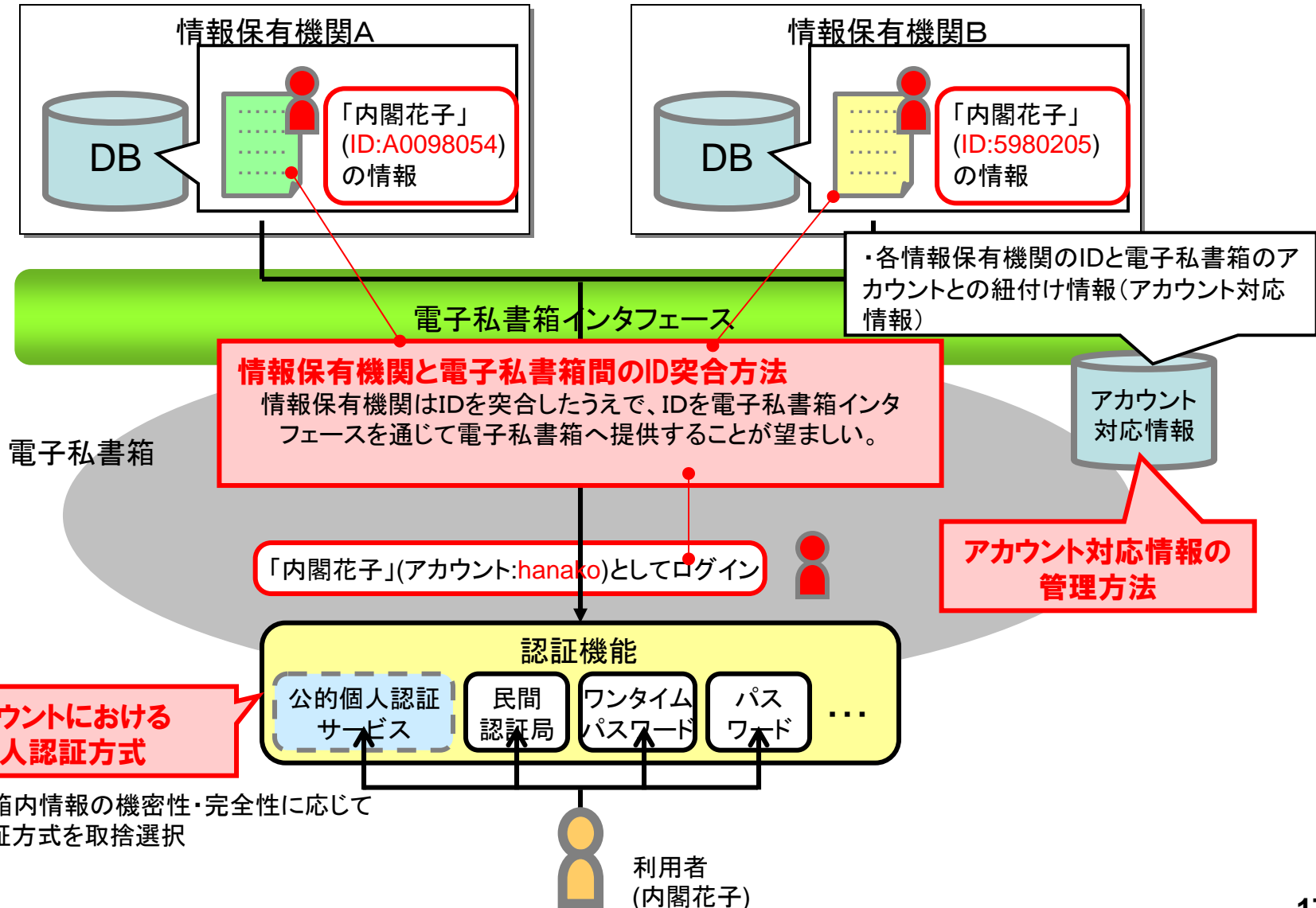
- ◆ 電子私書箱サービス全体の中で、情報の配送に責任をもつアクタについて、電子私書箱サービスの枠組みに従って確実に動作するパーティの範囲をトラストと呼ぶ。
 - システムのアーキテクチャを検討するうえでトラストを基点に機能の分担を行う。
- ◆ 電子私書箱サービスは、民間の参入を容易にするため、極度の厳密な制限を設けることは避けるべきだが、一定の確実な動作を保障できる仕組みを必要とする。



4.2 アカウント管理

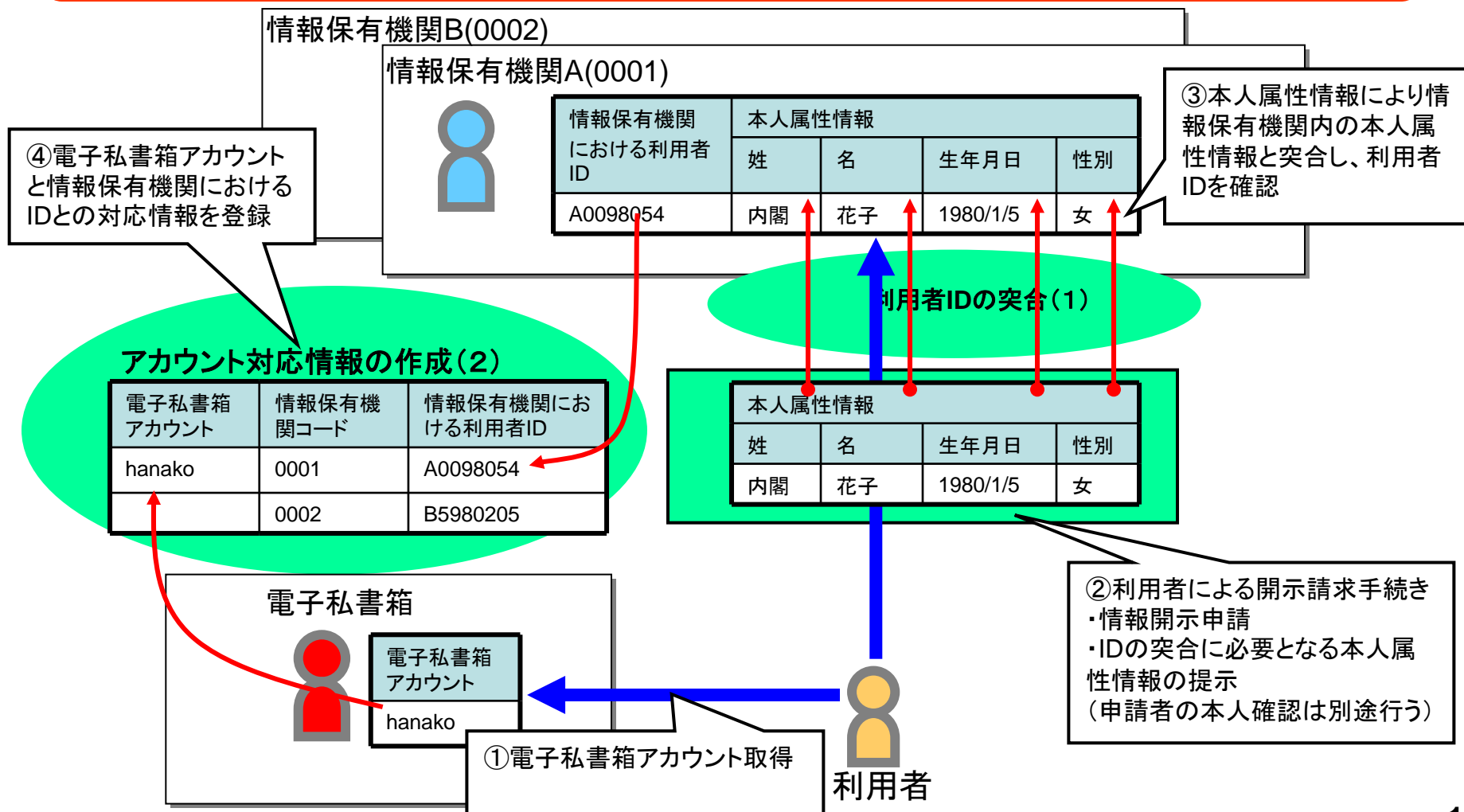
4.2.1 IDの突合の必要性

- ◆ 電子私書箱事業者が利用者のアカウントに対して、複数の情報保有機関から当該利用者に関する情報を収集する場合、各情報保有機関における当該本人のIDが異なる為、当該本人を特定できるよう、IDの突合を行う必要がある。



4.2.2 情報保有機関の利用者IDの突合例

- ◆ 情報保有機関が、利用者に利用者の情報を開示していない場合、利用者IDの突合が必要。(1)
 - 情報保有機関における利用者の特定(突合)に必要な本人属性情報は、開示請求手続き申請様式(紙面)もしくは当該情報を含む公的機関の発行する本人確認用ICカードを提示する運用が考えられる。
- ◆ 確認された利用者IDを電子私書箱アカウントと結びつける。(2)
 - アカウント対応情報の作成手順、管理場所については、第三者機関が作成する場合、利用者本人が情報を収集して作成する場合などパターンがあると想定。



4.2.3 アカウント情報管理におけるセキュリティ対策

- ◆ 情報を管理する機関の内部犯罪等による情報漏えいのリスクに対し対策を採る必要がある。
- ◆ 電子私書箱システムの中の情報管理の責任分担の考え方によって、これらのセキュリティ対策の必要性の程度が変化する。トラストの考え方と協調して公的セクタの役割など今後の検討が必要。

トラストモデルによる管理手法

アカウント情報の種類	例 アカウント:hanako	内部犯罪等による情報漏えいのリスク			リスクに対するセキュリティ対策
①各情報保有機関におけるID突合に必要な本人属性情報	<ul style="list-style-type: none"> 氏名:内閣花子 性別:女 生年月日:1980/1/5 	漏洩	一般の個人情報漏洩による被害レベルに準ずる	中	・共通セキュリティ対策※
②各情報保有機関におけるIDとアカウントとの対応情報	<ul style="list-style-type: none"> 情報保有機関AにおけるID:A0098054 情報保有機関BにおけるID:5980205 	漏洩	各情報保有機関から情報を引き出せる場合、IDの対応情報からプライバシー情報が不正に入手され、漏洩する	大	<ul style="list-style-type: none"> ・共通セキュリティ対策 ・アカウント情報漏えいに備えたプライバシー情報の暗号化 ・各情報保有機関と電子私書箱間のシステム間接続認証
③アカウントに対応する認証情報	<ul style="list-style-type: none"> ・ロック回数:3 ・認証方式1:パスワード ・認証方式2:電子証明書 ・認証方式3:MACアドレス 	漏洩 改竄	なりすましによりプライバシー情報が漏洩する	大	<ul style="list-style-type: none"> ・共通セキュリティ対策 ・アカウント情報漏えいに備えたプライバシー情報の暗号化
④アカウントのライフサイクル管理に必要な情報	<ul style="list-style-type: none"> ・ステータス:利用 ・再発行時の本人確認情報:運転免許証番号 ・連絡先情報:03-XXXX-YYYY, hanako@aaa.bbb.cc 	漏洩 改竄	ステータスの変更や再発行時のなりすましによりプライバシー情報が漏洩する	大	<ul style="list-style-type: none"> ・共通セキュリティ対策 ・アカウント情報漏えいに備えたプライバシー情報の暗号化

トラストで管理することが望ましい。

電子私書箱に厳密な管理を要求できない場合、アカウントの認証以外の手法による情報参照を検討する必要がある。

※共通セキュリティ対策の例

- ①アカウント情報そのものの暗号化
- ②アカウント情報の分散管理(情報分割、複数人認証)
- ③USBメモリやCD-R等の記録可能な可搬媒体の利用制御、施設への持込、持ち出しの禁止
- ④外部ネットワークへの通信制御

4.3 情報取扱制御

◆ 関連アクタとポリシー例

➤ 利用者

- 自らの個人属性を保有する利用者
(ポリシー例)

自分の医療情報は、家族と所定の医療サービスのみ参照可能だが、それ以外には参照不可。

➤ 情報管理者 (情報保有機関 / 電子私書箱事業者)

- 利用者から委託されて、個人属性情報を管理する。情報要求者からの情報参照要求に対して、開示の認可判断を行った上で、開示。
(ポリシー例)

医療機関は、急病の患者の処置のために、その患者の医療情報を参照することができる。

➤ 情報要求者 (電子私書箱事業者 / 活用サービス)

- 個人属性情報を活用したサービスを提供するために、情報管理者から個人属性情報を取得。
(ポリシー例)

患者の医療情報は、適した医療サービスを紹介する目的で参照するが、他の目的には参照しないし、第三者に提供しない。

➤ サービス代理要求者

- 利用者の個人属性に関するサービスに対して、利用者の代理でアクセスする。その際のアクセス権限は、前記利用者の権限に依存する。
(ポリシー例)

利用者が急病の場合、その利用者が認めて委任状に記載した代理人は、所定の医療保険サービスにアクセスできる。

- ◆ **情報取扱制御には、前述のような電子私書箱で想定されるポリシー要件を満たす十分な記述力を備えたポリシー記述を標準ポリシー記述言語を参考にし、規定する必要がある。**
 - 標準的な記述言語で、電子私書箱で想定されるポリシー要件を満たす十分な記述力を備えたものがない。

◆ 参考となる標準ポリシー技術言語

➤ P3P (Platform for Privacy Preferences)

- W3C勧告のXMLベースのプライバシーポリシー仕様。
- プライバシー情報の取扱いに関し、利用目的、配布先範囲などの要素で、プライバシーポリシーを記述可能。
- 利用者個人の情報に関する取扱いに関して、Webサイトがそのポリシーを公開。

➤ XACML (Extensible Access Control Markup Language)

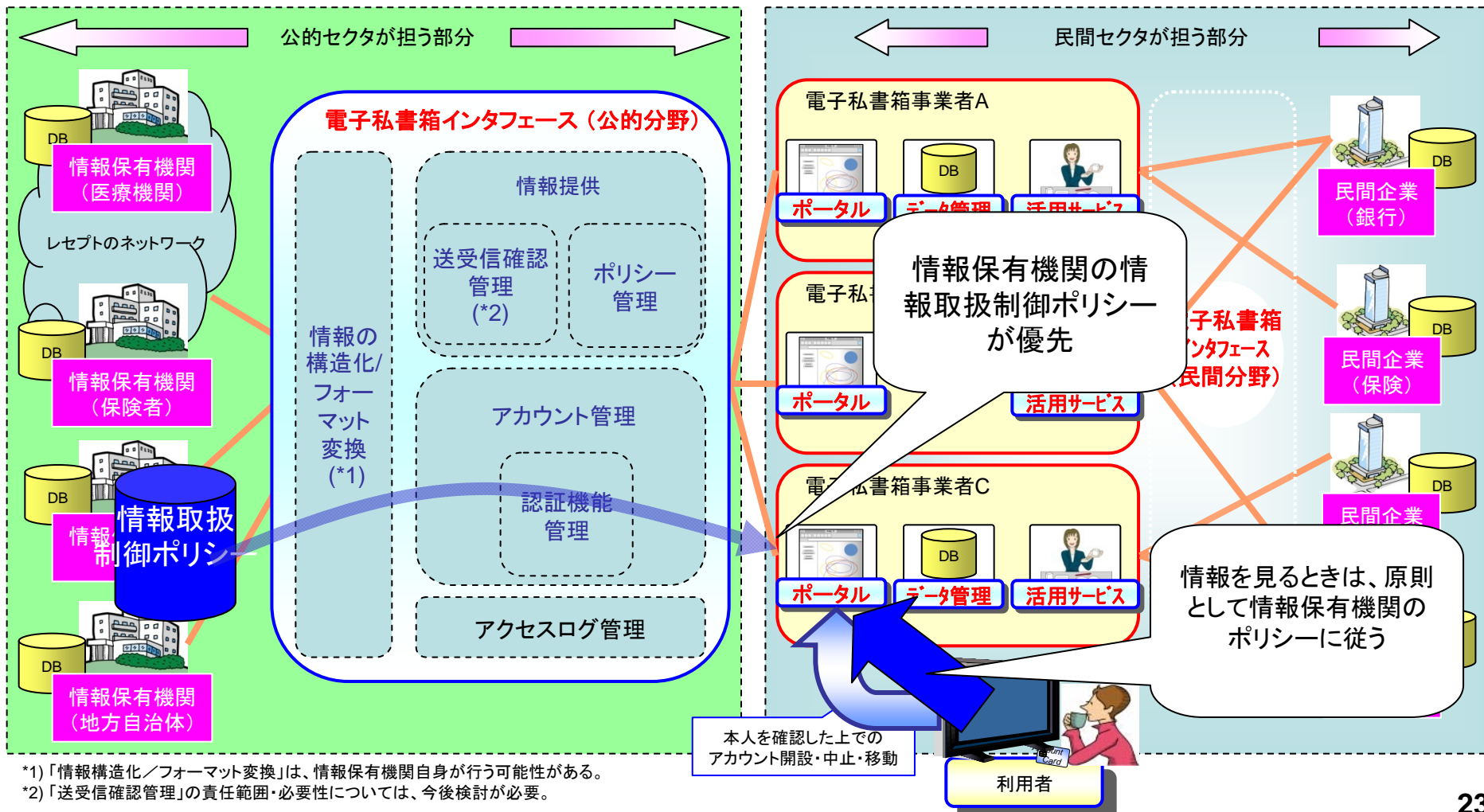
- OASIS標準のXMLベースのアクセス制御言語。
- セキュリティポリシーに特化するも、汎用的なルール記述とそのルール間の矛盾解決のためのメタルールも記述可能。

➤ WS-Policy/WS-SecurityPolicy

- 汎用的なポリシー言語。

4.3.3 情報取扱制御ポリシー—照合方法例(情報の閲覧)

◆情報の閲覧時は、基本的に情報保有機関の情報を閲覧しているため、電子私書箱事業者のポリシーより情報保有機関のポリシーが優先されると想定される。



4.4 セキュリティレベルを反映した情報の 構造化

4.4.1 健診情報に係るデータ構造に関する現状(1)

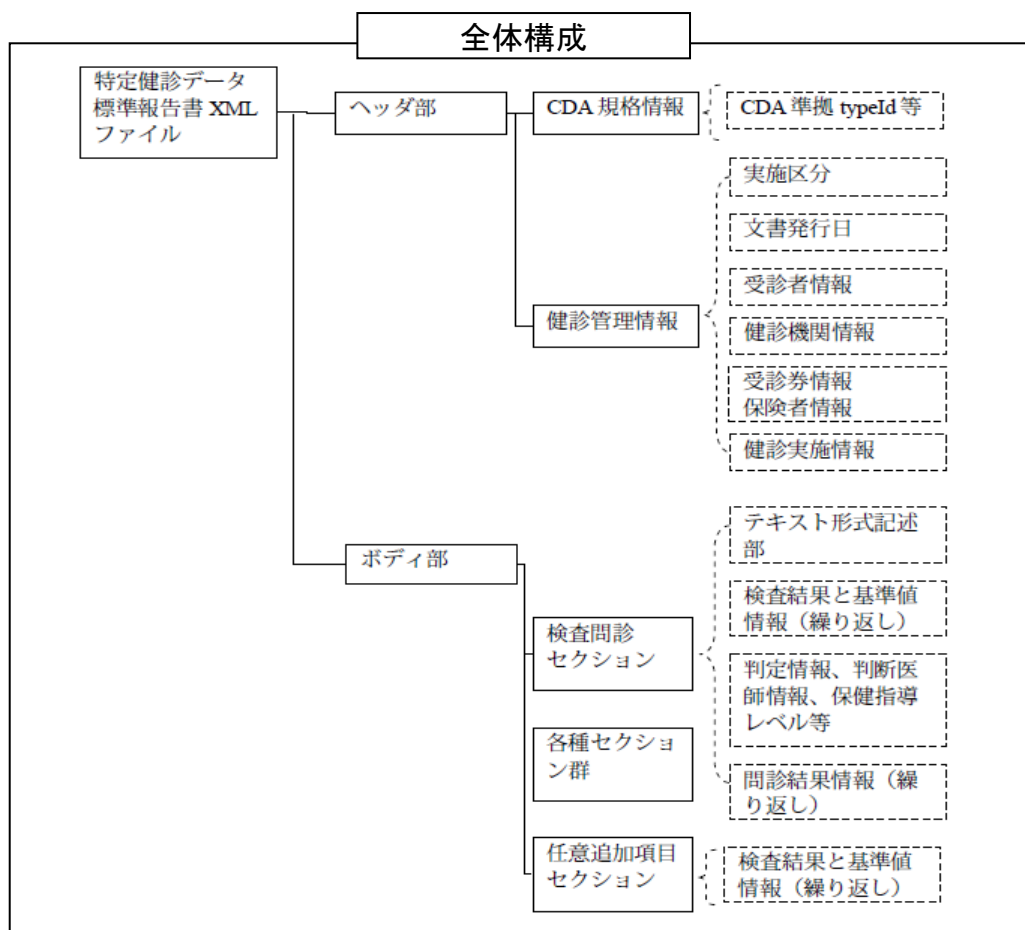
◆事例1：特定健診結果情報のデータフォーマットの標準化

➤厚生労働省は、2008年度から実施される特定健康診査について、特定健診結果の情報を電子的に作成するためのデータフォーマットを標準化。

➤当該標準フォーマットはXML形式であり、HL7 CDA（注）の規格に準拠。

（注）HL7 CDA（Health Level 7 Clinical Document Architecture）：システム間でのデータ交換を目的として、診療文書の構造等を標準化するための規格。

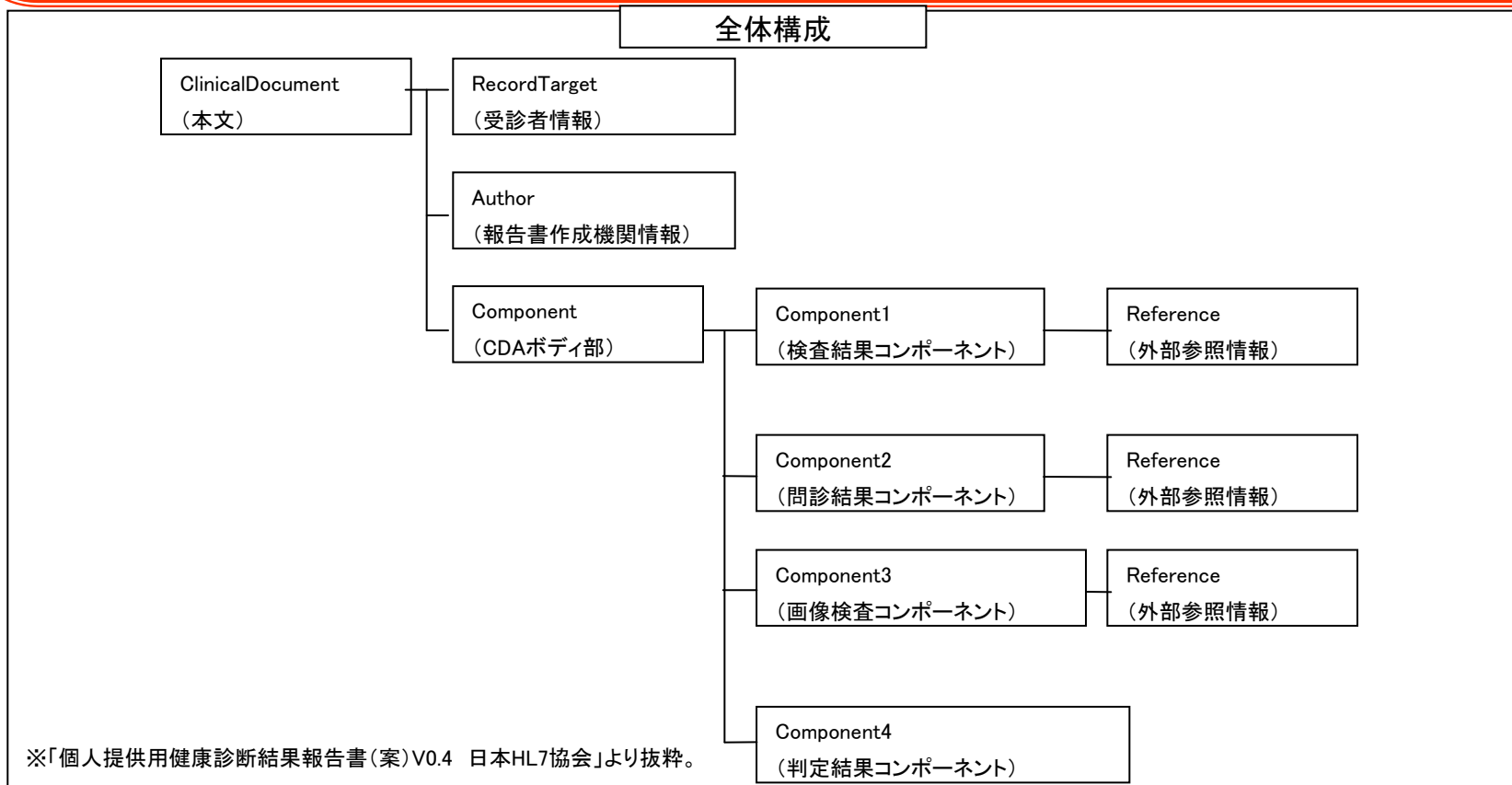
➤ただし、プライバシーポリシーを引き継ぐ構造ではない。



※「特定健診の電子的なデータ標準様式 仕様説明書 V1.26」より抜粋。

◆事例2：個人提供用健康診断結果情報のデータフォーマットの標準化

- 特定健診の標準フォーマットデータ（事例1）は、
 - ・ 基本的には、健診機関から保険者等に電子的に報告するためのもの。
 - ・ 内視鏡等による画像データや心電図等の波形データを外部参照情報としてリンク付け不可。
- 患者個人に提供することを目的としたフォーマットについて、日本HL7協会において標準化作業を実施中（現在、V0.4版を業界内でコメント募集中。）
- 当該個人提供用健康診断結果情報のデータフォーマットは、特定健診のものと同様、XML形式でHL7 CDA規格に準拠。
- 取り扱えるデータは、特定健診情報＋一般健診情報＋画像・波形。
- ただし、プライバシーポリシーを引き継ぐ構造ではない。



4.4.2 情報の構造化状況と対応方法

- ◆ 構造化している情報／されていない情報が混在するため、情報に応じて現状の評価、データ項目・構造の検討、構造化によるメリット等を十分に検討する必要がある。

現行の運用の中で情報保有機関がすでに保有している情報

構造化されている情報

電子私書箱の利活用を想定したデータ項目・構造になっているか評価が必要。
その上で見直しを行う。

プライバシーポリシーを引き継げる構造となっているもの

プライバシーポリシーを引き継げない構造となっているもの

例：特定健診結果情報のデータフォーマット

構造化されていない情報

今後構造化する見込みのあるもの

電子私書箱の利活用を想定したデータ項目・構造とするための取り組みが必要。

現時点では構造化の見込みのないもの

構造化によるメリットを十分に検討することが必要。

電子私書箱における利活用のために新たに作成し保有する情報

データ項目の標準化が必要。そのうえで電子私書箱での利活用を想定したデータ項目・構造とするための取り組みを推進。

今後構造化を想定して作成される情報

構造化を想定しない(そもそも構造化が必要ない)情報

◆ 構造化にあたっての要件

- 国際的な標準に準拠した構造形式を採用すること(特定のソフトウェアに依存しない構造形式を採用すること)
 - データ項目の追加、変更等が柔軟に行えるよう拡張性のある構造とすること
 - プライバシーポリシーを複数の異なる機関間で引き継げる構造とすること
 - 利用者や活用サービス事業者が編集・加工しやすい構造とすること
- 等

4.5 送受信確認(送受信証明)

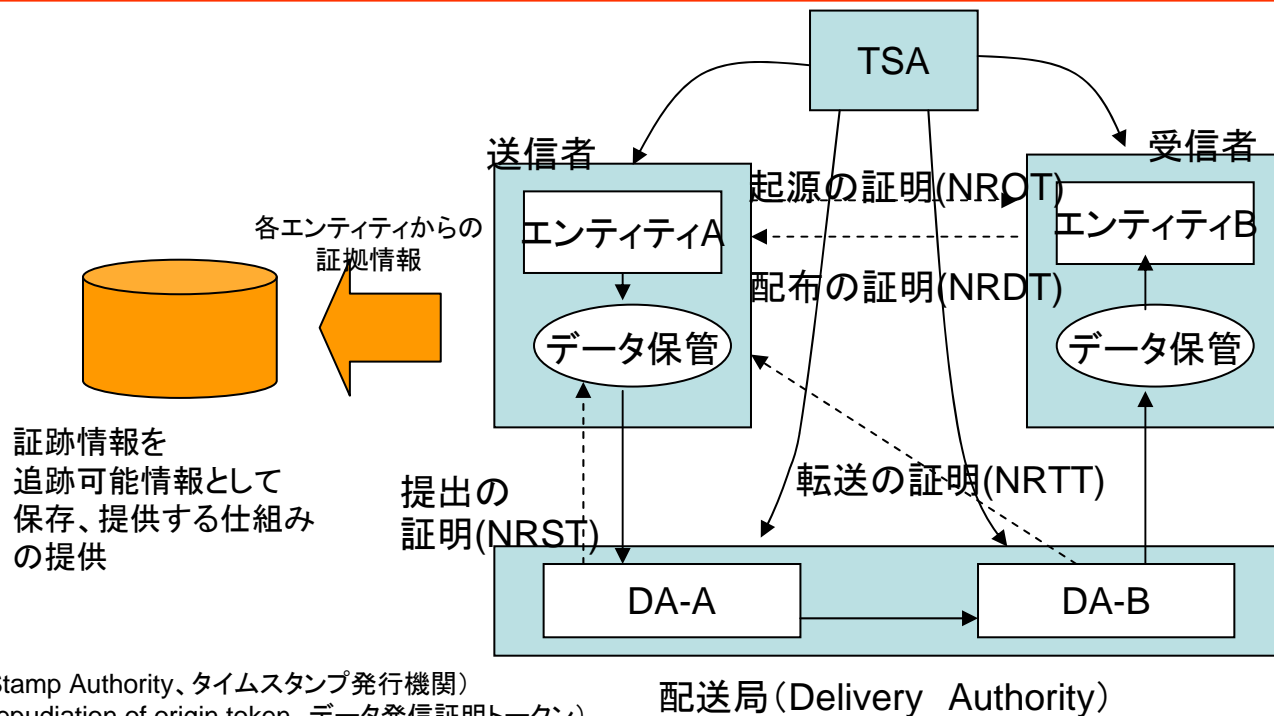
◆ 国際標準ではISO13888に送受信証明 (Non-repudiation) の形態を規定

➤ 特徴

- 各処理 (文章作成, 送信, 受信, 閲覧) ごとに電子署名付きの証跡情報を作成
- 証跡情報を追跡することで、送受信証明 (否認拒否を証明すること) を可能とする。

➤ 適用について

- インターネット上のサービスにおいて、すべての経由点に証跡情報の保管を要求するのは非現実的
- 証跡情報を保存するのは信頼があるアクタでなければならない。
- 証跡情報に対する攻撃に対し、運用を含むセキュリティ対策を十分に検討する必要がある。



【用語解説】

TSA (Time Stamp Authority、タイムスタンプ発行機関)

NROT (nonrepudiation of origin token、データ発信証明トークン)

NRDT (non-repudiation of delivery token、データ受領証明トークン)

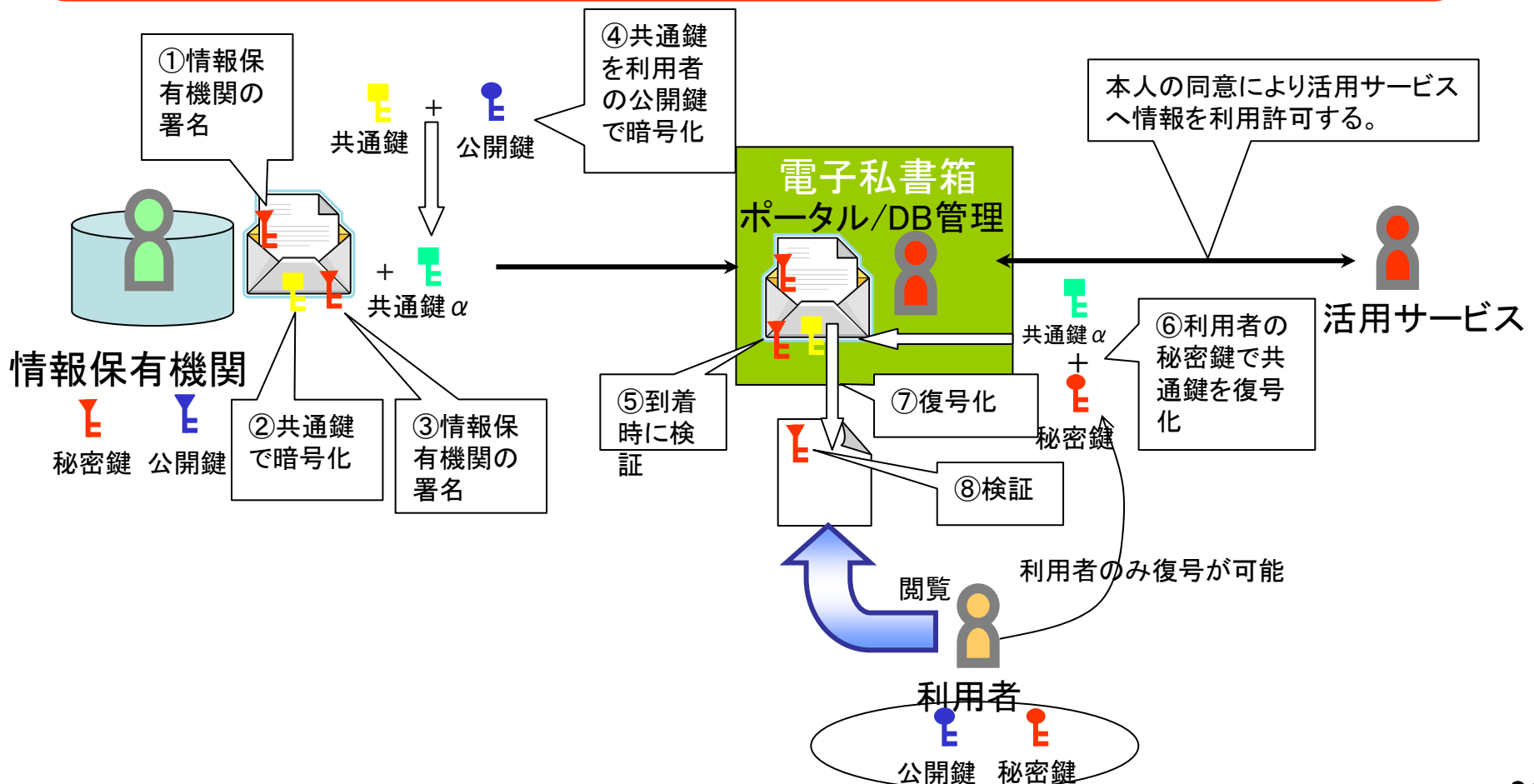
NRTT (non-repudiation of transport token、データ転送証明トークン)

NRST (non-repudiation of submission token、データ提出証明トークン)

※送受信証明とともに、親展通信 (秘匿) を実現する必要がある

4.5.2 親展通信(送受信確認例)

- ◆情報保有機関から電子私書箱に情報を確実に届け利用者のみが情報を確認できるようにする。
 - 情報保有機関は利用者の公開鍵を利用し、電子私書箱に送る。利用者のみが自分の秘密鍵で情報を閲覧することができる。
- ◆利用者が鍵の紛失、更新した際に情報の復号化ができなくなる恐れがあるが、鍵の預託を不要とする方策(再度更新した鍵で情報を送りなおすなど)を検討する必要がある。



4.6 全体像の例示

4.6.1 トラストの考え方を基にした全体像

- ◆ 電子私書箱インタフェースを電子私書箱サービスの枠組みに従って確実に動作するものと定義することにより、情報保有機関で持つアカウント対応情報、情報取扱制御、親展通信などの機能を電子私書箱インタフェースに代行させることが可能。
- ◆ 電子私書箱全体像の中での電子私書箱インタフェースの役割を明確化する。

◆ 電子私書箱インタフェースの役割案

◆ アカウント対応情報の中継

- 各情報保有機関における利用者のIDと電子私書箱アカウントの対応情報の中継。

◆ 情報取扱制御

- 公的セクタとして情報保有機関と電子私書箱インタフェースは同じ責任を有すると考えられ、ひとつの情報管理者エンティティとみなせる。
- 電子私書箱インタフェースは情報保有機関のポリシーを共有し、情報取扱制御を行う。電子私書箱インタフェースは情報保有機関の要求どおりに動作を行う。

◆ 親展通信

- 情報保有機関と電子私書箱インタフェースを一体とみなし、鍵の管理は電子私書箱インタフェースで行う。
- 本来親展通信は情報保有機関が秘匿して送るものであるが、インタフェースが信頼できるものとした場合、インタフェースで秘匿して送ることも考えられる。これにより、情報保有機関が、利用者の鍵を扱う作業から開放される。

- ◆ 電子私書箱で各情報保有機関におけるIDとアカウントとの対応情報（以下アカウント対応情報）をもたず、アクセスチケット（アクセス許可証）を利用する。
 - 「アカウント情報管理におけるセキュリティ対策」にて検討した②アカウント対応情報は、信頼できる主体が管理する必要がある。
 - アカウント対応情報を電子私書箱インタフェースが管理するモデルと利用者本人が管理するモデルを検討。

アクセスチケット発行モデルの主な主体について

◆アクセスチケット発行機関

- アクセスチケットの発行（後述する電子私書箱インタフェースでアカウント対応情報を管理するモデルの場合）と発行済みのアクセスチケットを管理する。
- 公的な機関またはそれに準じる機関とする。

◆アクセスチケット

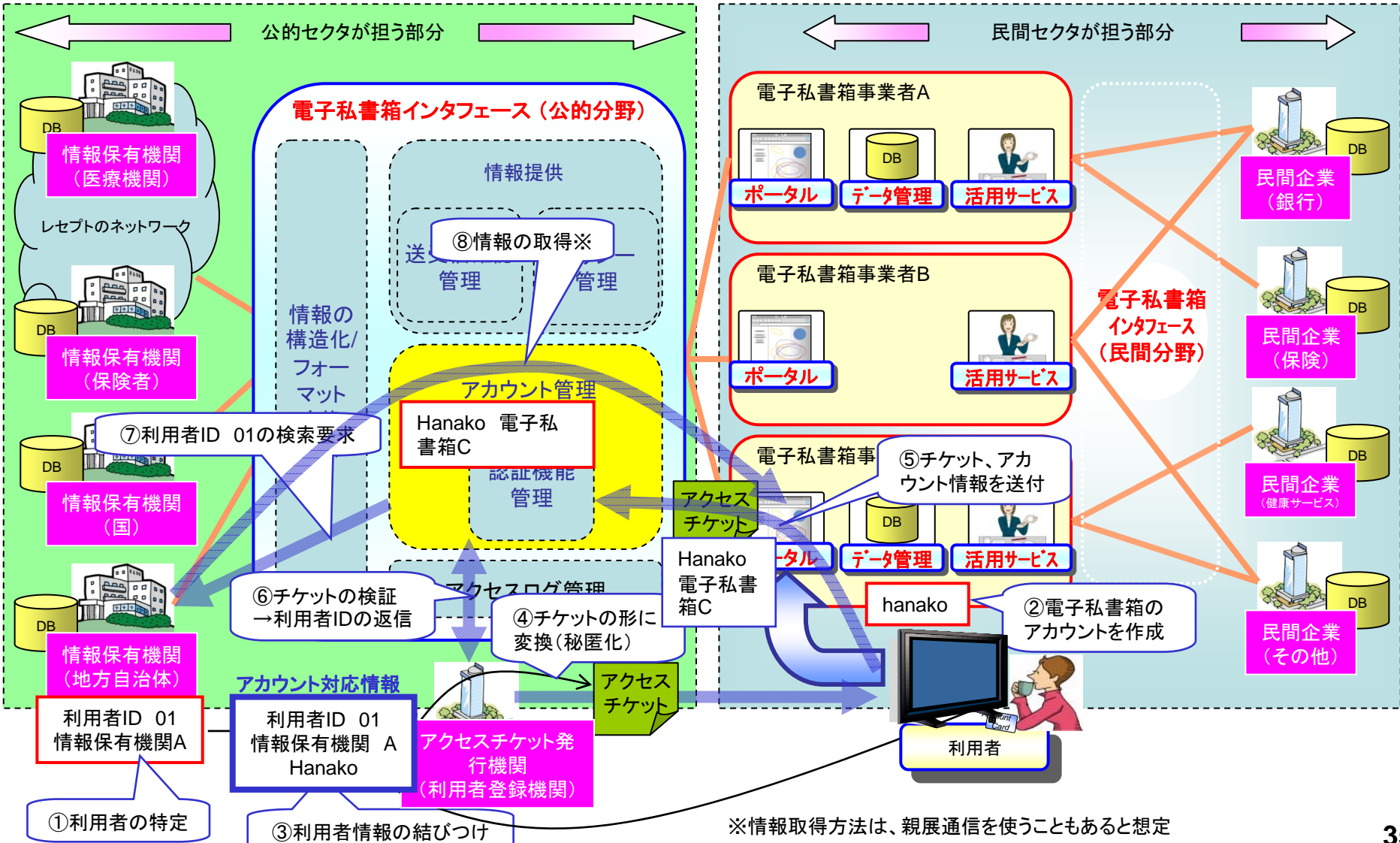
- アカウント対応情報に関連する情報を含み、内容が暴露されないよう、暗号技術を利用して秘匿化および電子署名を付与した情報。
- 本人を確認した上で、アクセスチケット発行機関により発行される。

◆電子私書箱インタフェース

- 情報保有機関と電子私書箱間をアクセスチケットを介して情報の送受信を行う。
- アクセスチケットの検証を行う（アカウント対応情報がアクセスチケット発行機関にある場合）。
- 履歴（証拠）の管理を行う。

4.6.3 アクセスチケットを利用したモデル（電子私書箱インタフェースで管理）

- ◆ アクセスチケット発行機関が発行するアクセスチケットを利用し、またアカウント対応情報をアクセス許可チケット発行機関で管理するため、電子私書箱事業者は、アカウント対応情報を所有しなくてよい。



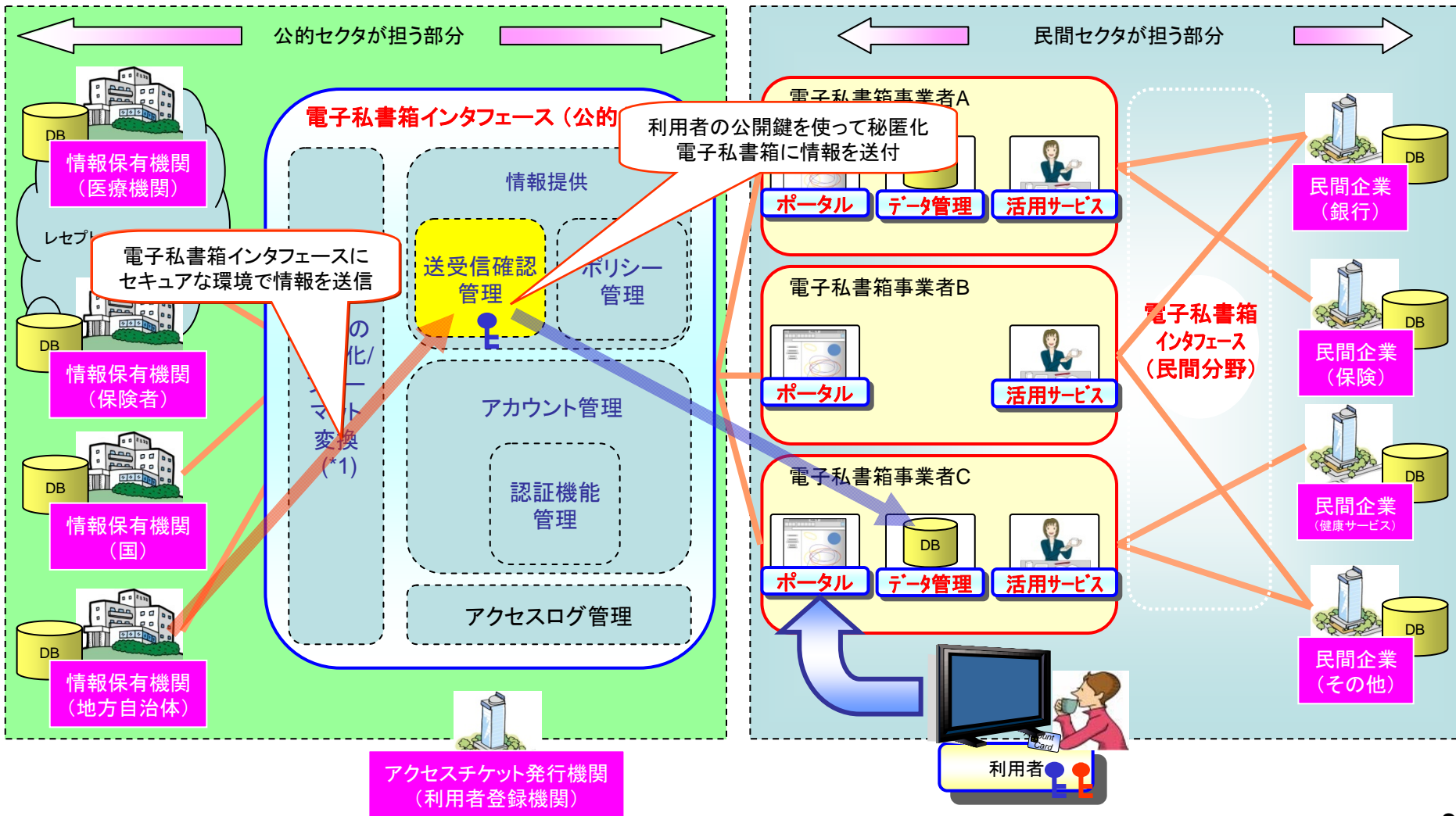
4.6.5 2つのモデルの特徴の比較

- ◆ アカウント対応情報を電子私書箱インタフェースで管理するモデルは、アクセスチケット発行機関による集中管理が必要であり、利用者が管理するモデルは、利用者個別の管理が必要となる。
- ◆ これらの実現に向けては、技術的な課題だけでなく制度的な視点、利用者の負担や利便性といった利用者視点、コスト等、多様な観点からの検討が必要となる。

項番	比較項目	電子私書箱インタフェースでアカウント対応情報を管理するモデル	利用者がアカウント対応情報を管理するモデル
1	トラスト主体	・アクセスチケット発行機関	・利用者
2	情報の持ち方	・アクセスチケット発行機関がアカウント対応情報を管理 ・電子私書箱事業者は、電子私書箱アカウントを管理	・利用者がアカウント対応情報を管理 ・電子私書箱事業者は、電子私書箱アカウントを管理
3	リスクの差異	・アクセスチケット発行機関への攻撃によるアカウント対応情報の漏えい	・利用者への攻撃によるアカウント対応情報の漏えい
4	システム構築上の課題	・利用者がアクセスチケット発行機関にチケット要求の通信が必要 ・アクセスチケット発行機関の応答性能、信頼性の確保	・利用者側でアクセスチケットを生成するための仕組みが必要
5	利便性	・利用者に準じる者の利用も技術的な対応により拡張が可能	
6	アクセスチケットの有効期間	・有限(短期間)としてチケット漏えいによる他人のなりすましのリスク低減を図ることが必要	

4.6.7 電子私書箱インタフェースの役割：親展通信

- ◆ 電子私書箱インタフェースが、情報保有機関に代わって情報を秘匿化し、電子私書箱事業者に送付する。
 - 電子私書箱インタフェースは情報配送の責任を負う。
 - 利用者の公開鍵は電子私書箱インタフェースで管理。



- ◆ チケット発行機関、電子私書箱インタフェースを利用することにより、電子私書箱事業者は、公的セクタの情報の入手、閲覧、活用において負担が軽減される。
 - アクセスチケット発行機関（又は利用者）によってアカウント対応情報を厳重に管理。

- ◆ 利用者の電子私書箱アカウントの管理
 - 電子私書箱事業者としてのルールによる本人確認、認証処理を実施したうえで利用者の電子私書箱アカウントを管理する必要がある。

- ◆ 情報取扱制御ポリシーの管理
 - 電子私書箱の情報取扱制御ポリシーについて利用者の自由なポリシーの設定が可能な環境を整備する必要がある。

- ◆ 電子私書箱インタフェースとの接続
 - 電子私書箱インタフェースとの通信制御を行う必要がある。
 - 電子私書箱インタフェースの情報取扱制御ポリシーと電子私書箱事業者の情報取扱制御ポリシーの調整を行う必要がある。

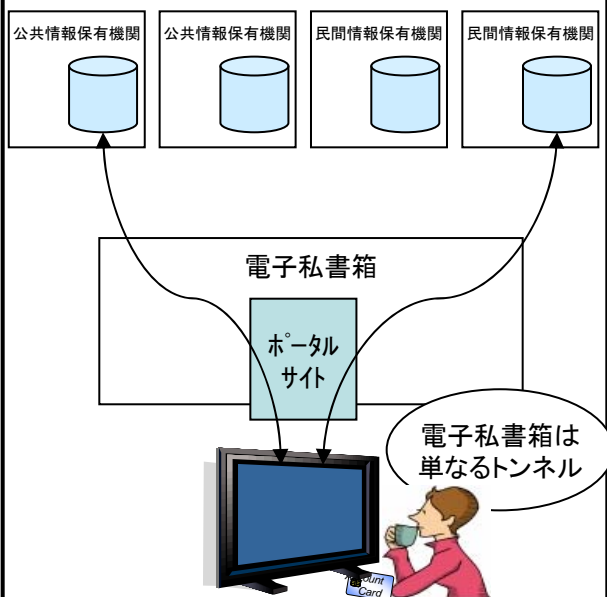
- ◆ 情報の取扱、管理
 - 構造化された情報のセキュリティレベルに応じた取扱いを行う必要がある。

付録

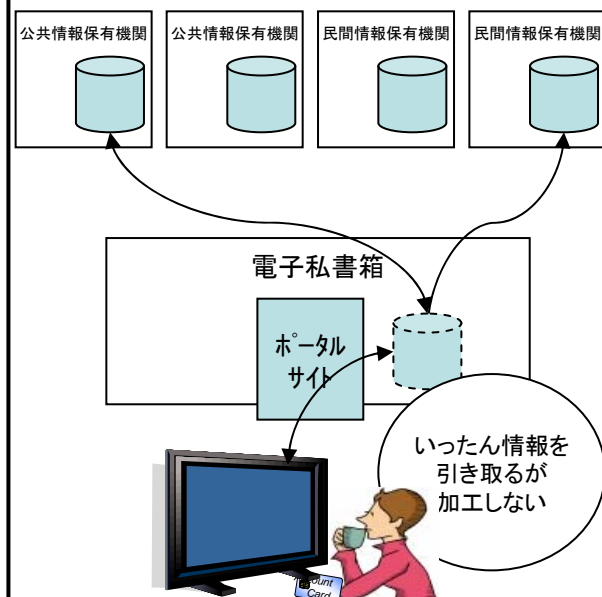
1. 電子私書箱の情報の持ち方

- ◆ 電子私書箱全体の構造を考える上で、扱う情報をどこで保有するかは、セキュリティ、プライバシー保護の観点から重要である。
- ◆ 情報の持ち方のモデルを示すとともに、各モデルの技術的課題を検討する。
 - 電子私書箱が情報を保有しないモデル
 - 情報保有機関の情報を一時的に保有するモデル
 - ・ サービス例：情報保有機関の最新情報を一元的に表示する場合
 - 電子私書箱に情報を保有するモデル
 - ・ サービス例：情報保有機関が情報を定期的に更新する場合

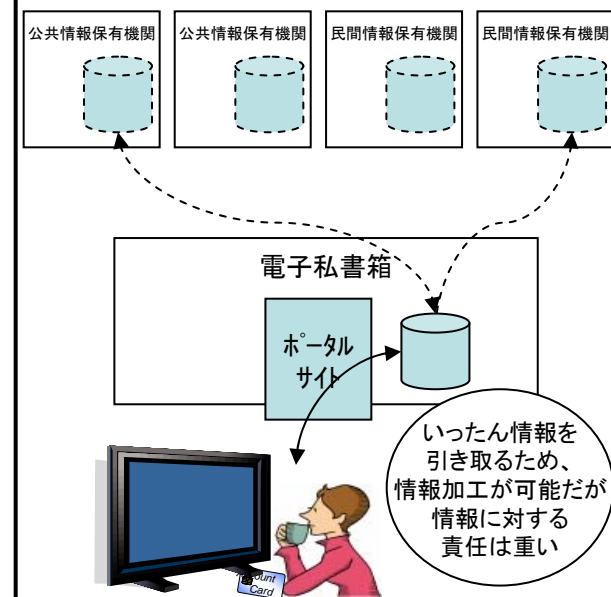
【電子私書箱が情報を保有しないモデル】



【電子私書箱が情報を一時的に保有するモデル】



【電子私書箱が情報を保有するモデル】



技術検討参考資料

1. アカウント管理の流れ

◆アカウント管理の流れを以下に示す。

①アカウント開設

電子私書箱サービスの利用を希望する情報保有者の申請に基づき、アカウント開設の手続きを行う。

②情報保有機関への情報開示請求とIDの突合

電子私書箱サービスへ情報開示を請求したい情報保有機関に対し、開示請求手続きを行う。また電子私書箱のアカウントに対して、情報保有機関における対応IDとの突合を行い名寄せ結果の確認を行うと共に、アカウントと情報保有機関におけるIDとの対応情報を登録する。

③アカウント利用

①②の手続きを行った後に、電子私書箱のアカウントを利用し、電子私書箱内の情報を利活用する。

④アカウント一時停止

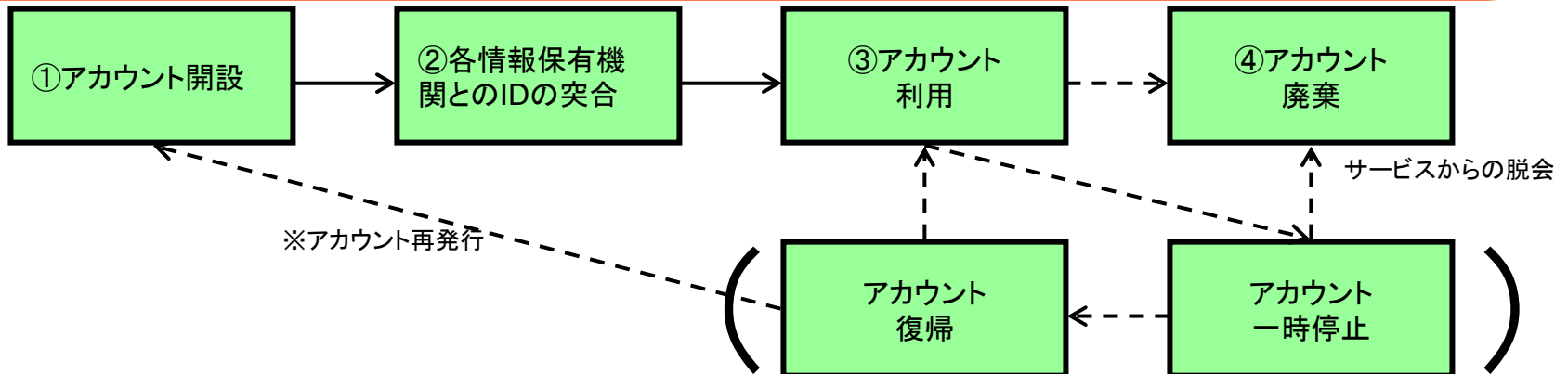
認証情報の盗難や紛失等の理由により情報保有者からアカウントの停止要請があった場合、要請した本人が当該情報保有者であることを確認した後に、該当アカウントの利用を停止させる。

⑤アカウント復帰

アカウントの停止後、情報保有者からアカウントの利用を復帰、継続の要請があった場合、要請した本人が当該情報保有者であることを確認した後に、アカウント復帰処理を行う。

⑥アカウント廃棄

情報保有者が電子私書箱サービスの脱会を要請する場合、要請した本人が当該情報保有者であることを確認した後に、当該アカウントに関するすべての情報を消去し、アカウントの廃棄処理を行う。



2. アカウント管理に必要な情報

- ◆ 電子私書箱サービスにログインする利用者を識別及び認証するために、電子私書箱内で一意に識別できる電子私書箱アカウントを開設する必要がある。
- 1. 各情報保有機関におけるID突合に必要な本人属性情報
 - 各情報保有機関におけるID突合の実施にあたり、突合に必要な情報(検索キー)。
- 2. 各情報保有機関におけるIDと電子私書箱アカウントとの対応情報
 - 初回のID突合後、各情報保有機関におけるIDと電子私書箱アカウントとの対応情報管理する必要がある。
- 3. 電子私書箱アカウントに対応する認証情報
 - 電子私書箱アカウントの認証に用いる情報(credential)を管理する。
 - ID/パスワード方式による認証方式の場合は、ハッシュ化パスワード文字列
 - PKIによる認証方式の場合は、電子証明書の主名(Subject)等
 - 端末認証による認証方式の場合は、端末特定情報(MACアドレス等)、もしくは端末認証用電子証明書情報等(TPM等)
- 4. 電子私書箱アカウントのライフサイクル管理に必要な情報
 - 認証情報の盗難や紛失、忘却に備えて、アカウントのステータス情報(利用、停止)やアカウントの認証情報リセット・再発行に必要な本人確認情報を管理する必要がある。またサービスの停止や周知に必要な連絡情報(住所、電話番号、メールアドレス等)もこれに含まれる。

3. IDの突合時の課題①

- ◆ 情報保有機関が情報を開示していない場合は下記の方策をとる必要がある。
 - ◆ ID突合を行う方法としては、各情報保有機関の管理するID以外の個人情報(以下、本人属性情報)を使用して、突合を行う方法が考えられる。
 - ◆ 突合に用いる情報は、情報保有機関が管理するDB内で本人を特定するために必要とする情報である。個人を一意に識別できるとされる基本四情報(氏名、性別、生年月日、住所)などが考えられる。
 - ◆ 但し以下のケースでは特定が困難。
 - ① 結婚による苗字の変更や引越し等による住所の変更等により、各情報保有機関における本人属性情報の該当箇所が一致しない場合(以下、図)
 - ② 突合に用いる情報の項目の一部が情報保有機関で管理されていない場合(例えば、生年月日を管理していない等)
 - ③ 突合に用いる情報の項目すべてが一致する人物が複数存在する場合

情報保有機関A	情報保有機関におけるID	本人属性情報				
		姓	名	生年月日	性別	住所
	A0098054	内閣	花子	1980/1/5	女	東京都中央区...

情報保有機関B	情報保有機関におけるID	本人属性情報				
		姓	名	生年月日	性別	住所
	5980205	内閣	花子	1980/1/5	女	東京都千代田区...

突合に用いる情報						
本人属性情報		姓	名	生年月日	性別	住所
		内閣	花子	1980/1/5	女	東京都千代田区...

情報保有機関Aに登録されている住所が古いため、基本四情報のAND条件では特定に失敗する

3. IDの突合時の課題②

◆住所表記の課題

- ▶日本の住所表記は自由度が高く、「丁番地」「地名」「異体字」「省略表記」などでの表記ゆれが発生するため、同じ住所でもまったく違う表記が可能となっている。また、住所表記にも、通常表記のほかに通り名表記がある地域があり、そのような地区では通り名表記が普及していることが多い。そのほか、マンション名表記の有無や区画整理や市町村合併等に伴う変更等もある。
- ▶各機関が登録している住所は、基本的に本人の申請に依存するため、住所表記が一致するとは限らない。

さらに住所表記が一致する前提であっても、次のように技術的にマッチングが困難となる事象が発生しうる。

◆情報保有機関と電子私書箱間の文字コード変換処理

- ▶情報保有機関で用いられている多くの基幹システムでは汎用機が使用され、氏名や住所に用いられるホストコードにおける機種依存文字の変換方式を決める必要がある。またシステムで独自にサポートされるシステム外字や独自に追加した外字をどのように規格表内文字に置き換えるか、ルールを決める必要がある。
- ▶電子私書箱における文字コード、フォントを取り決める必要がある。

◆本人属性情報の変更に対するロバスト(安定)性の確保

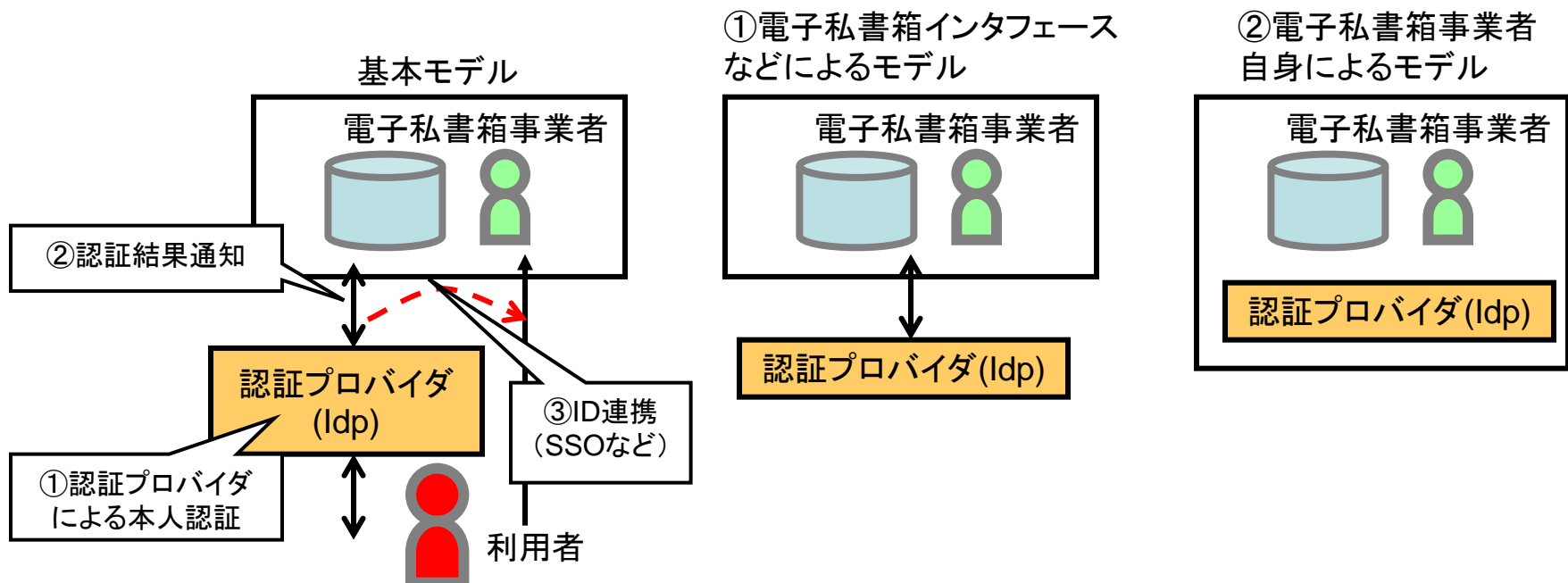
- ▶突合する情報間で、現住所の変更やその他属性情報の変更(結婚等による姓の変更等)があった場合においても、一致する突合候補を抽出できることが望ましい。
- ▶但し、プライバシー保護の観点から、利用者自身が操作し自身と対応するIDとの突合を行うのではなく、情報保有機関の職員による突合処理を基本としたモデルであるべきである。

◆外国人に対する扱い

- ▶外国人登録制度を考慮した突合方式とすることが望ましい(名前をカタカナにしたものを登録しているケースが多い)。旧型のシステムでは氏名欄の字数に制限がある為、1文字の枠に2文字のカタカナを外字として割り当てて使用しているケースもある。

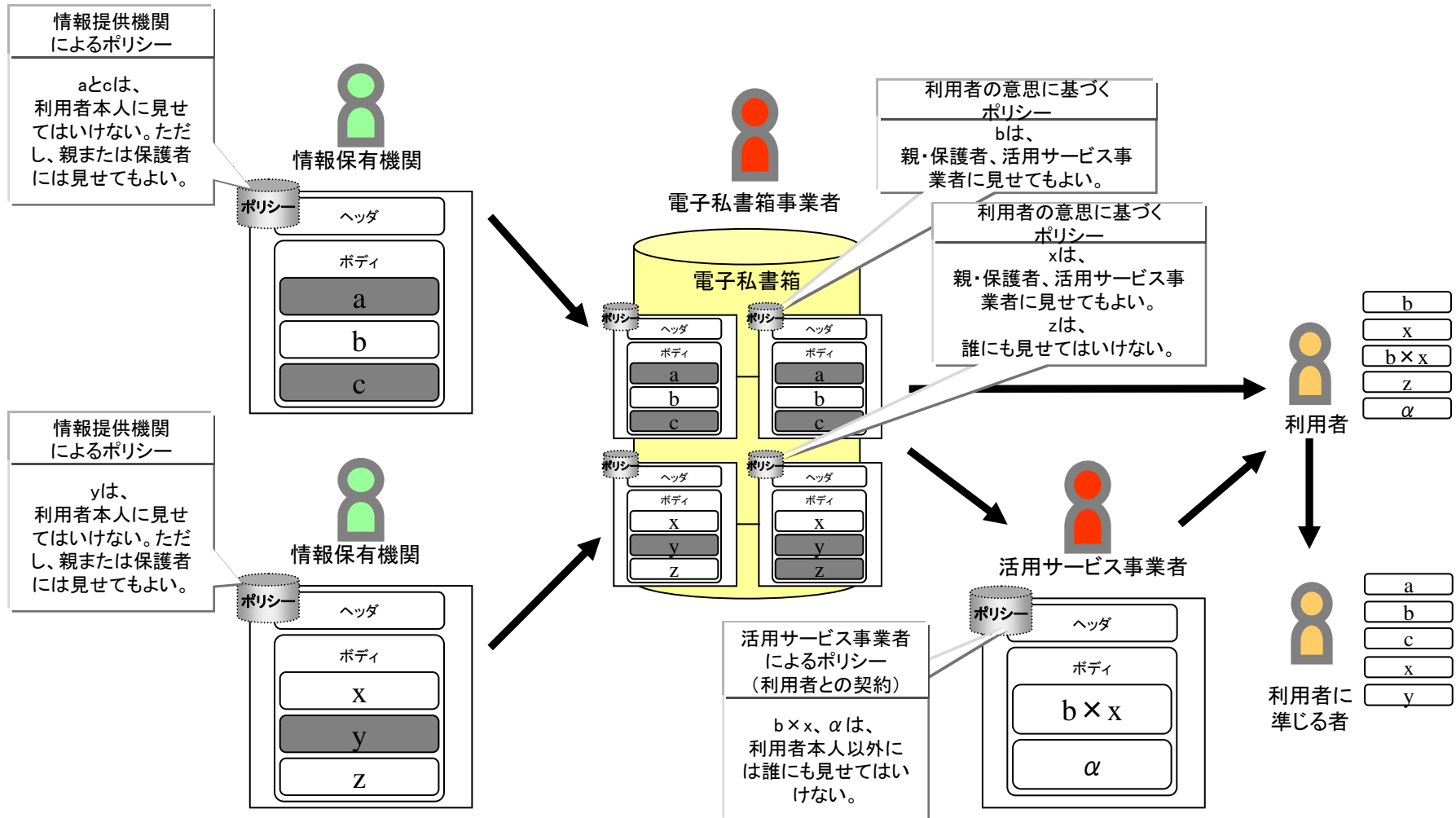
4. 認証処理の実装モデル

- ◆ 電子私書箱のアカウントに対する認証処理の実装モデルとしては、利用者における電子私書箱サービスの利用環境を考慮し、Webブラウザ(http)と親和性の高い下記の基本モデルになるものと考えられ、そのバリエーションとしては、①電子私書箱インタフェースなどに認証処理を委託するモデルと、②電子私書箱自身が認証処理を行うモデルの2つが想定される。
- ◆ 認証情報漏えいのリスクや電子私書箱のアーキテクチャ自体の認証処理のポリシー統一を行うならば、例えば電子私書箱インタフェースに認証プロバイダを整備する方式が考えられる。



5. データ構造によるポリシーの継承

- ◆ 情報提供機関から提供されるデータが様々な事業者等間を流通するため、ポリシーがどこかで継承されないこととなれば、想定外の者に情報が漏えいする恐れがある。
- ◆ このため、ポリシーを適切に継承していくための手立てが必要。
- ◆ これをどのような形で実装していくかということについて、データ構造そのものをセキュア化するというのであれば、データ標準化の取組のなかでそれを組み込むことが必要。



◆ 情報取扱制御ポリシーには以下のポリシーが含まれる。

➤ セキュリティポリシー

- 信頼できる相手とセキュアな通信路を確保するための要件。
- 安全にデータを保管するための要件なども含む。
- (例) SSL/TLSで通信可能な相手のみ通信する。

➤ アクセス制御ポリシー

- 情報管理者が、管理する情報を、不正なアクセスから保護するために、アクセスする情報要求者の属性やアクセス時のコンテキスト情報に基づき、情報へのアクセスの認可判断の基準とするポリシー。
- (例) 人事情報は、部長職以上の役職には開示可だが、それ以下は許可しない。

➤ プライバシーポリシー

- 情報が特に個人属性などの個人に関連する機密性を持つ場合に、その情報の取扱いに関する要件・方針を規定するポリシー。
- (例) サービス利用者の住所情報は、利用者が購入した商品の配送目的で利用するが、それ以外の目的には利用しない。

7. プライバシー制御

◆ 概要

個人情報取扱に関して、利用者と管理者と要求者との間で合意し、プライバシー漏えい・侵害を防止する。

◆ 課題

➤ プライバシーポリシー記述内容の規定

- 以下のような条件に関して、情報管理者、情報要求者、利用者は、取扱に関し規定する。
 - 対象個人属性
 - 利用目的
 - 利用期限
 - 配布範囲

➤ プライバシーポリシーの合意方法

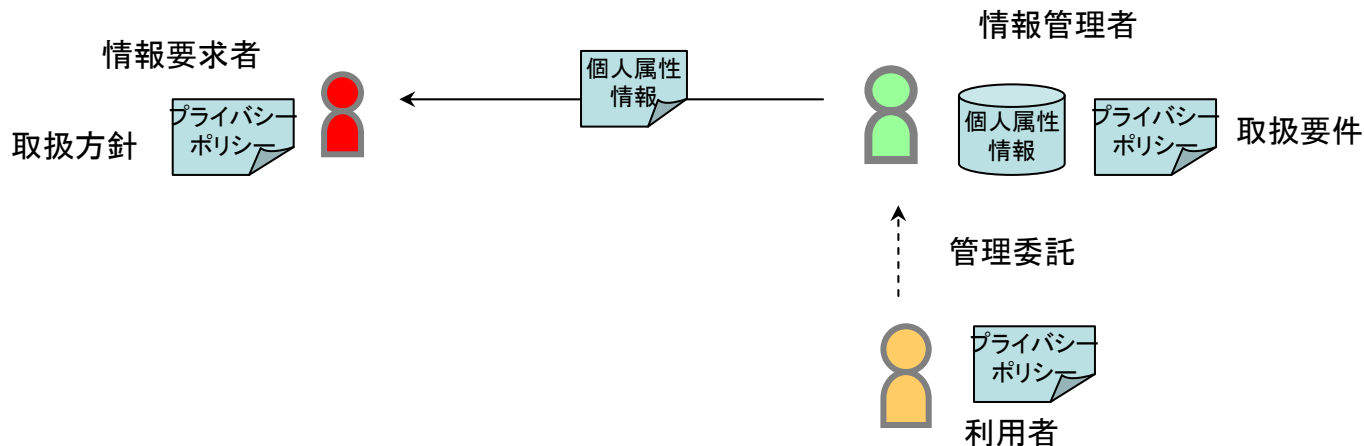
- オフラインで事前契約などの手法をとり、合意する。
- 動的に、必要時に交渉し、合意形成。

➤ アクセス制御ポリシーとの関係

プライバシー制御は、上記合意を形成して初めて、情報が送付されるべきものである一方、アクセス制御ポリシーは、情報管理者が主体的に認可判断を行うものである点で異なるが、情報制御の観点からは類似する。

注

- ここでは、情報を、「個人属性」として、利用者個人に関連する(プライバシーに関連する)情報に特化している。
- 情報管理者は、利用者から委託され管理する。情報管理者が情報要求者に対して提供する際の認可判断は、情報管理者のみならず、利用者本人のプライバシーポリシー(プリファレンス)を反映させる必要がある。



8. アクセス制御

◆ 概要

不正なアクセスからの情報保護。しかるべきアクセス者に対して情報を提供する。

◆ 課題

➢ 情報アクセス要求者の認証

- 情報アクセス要求者の認証が前提と考えられ、認証方式、認証レベルや強度の要件を整理する必要がある。
- 情報保有機関と情報保有機関との認証連携を伴う場合には、認証情報の交換プロトコル、認証方式・強度の合意が必要がある。

➢ アクセス制御ポリシー規定

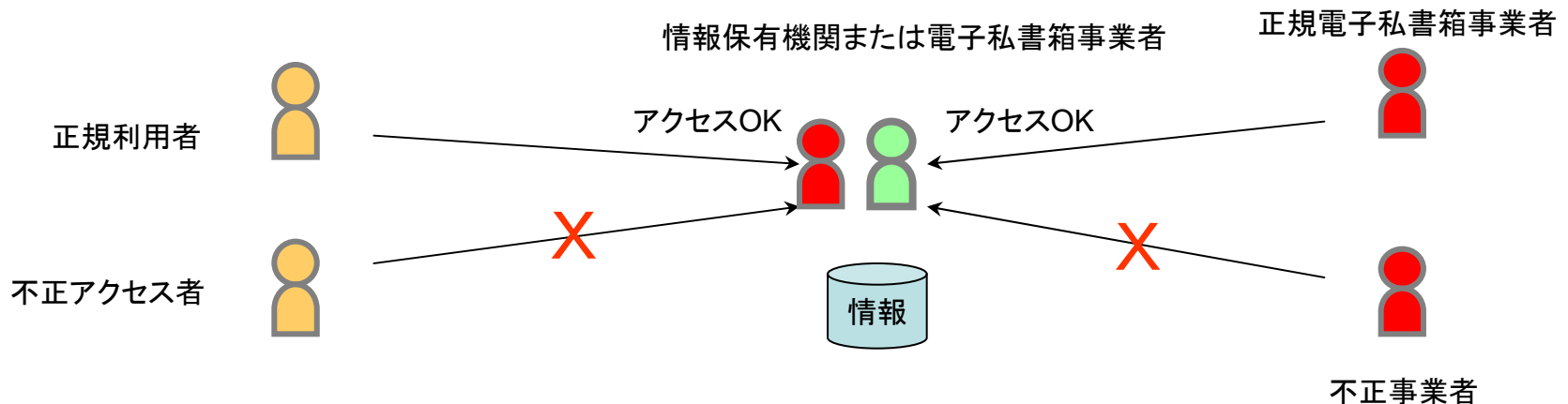
- 情報保有機関
情報アクセス要求者の属性、あるいは、コンテキスト情報などの認可判断基準を決める必要がある。
- 電子私書箱事業者
基本は、事業者固有のポリシーによる制御だが、電子私書箱サービスという公共的側面から、遵守が必要、あるいは、推奨されるポリシーを規定する必要があると思われる。

➢ アクセス制御方式

- ロールベース、属性ベースなど、数多くの制御方式から選定、あるいは、拡張方式を検討する必要がある。
- 代理アクセスを認める場合には、別途検討が必要がある。

注

ここでは、一般的な「情報」に言及しており、個人情報には特化していない。



◆ 情報の格付けと取扱制限の実施

すべての情報保有機関と電子私書箱により情報の格付けと取扱制限が行われることが必要である。

➤情報の格付け及び取扱制限は、その作成者又は入手者が、当該情報をどのように取り扱うべきと考えているかを他の者に認知させ、当該情報の重要性や講ずべき情報セキュリティ対策を明確にするための手段である。このため、情報の格付け及び取扱制限が適切に行われないと、当該情報の取扱いの重要性が認知されず、必要な対策が講じられないことになってしまう。

◆ 独自のポリシーによる情報の取扱い

情報保有機関と電子私書箱は、それぞれの情報セキュリティポリシーにもとづき情報を取り扱う(格付けの規定や格付けに応じた取扱いの規定など実施手順を整備する)。情報の格付けや取扱制限の方式は組織ごとに異なる。

➤考察

- ・情報の格付けと格付けに応じた取扱の基準は組織内に閉じており、組織間における格付けの相互運用性は期待できない。
- ・情報の取扱制限の方式は組織内に閉じているが、取扱制限の意図するもの(取扱いにおける留意事項)を組織の外部の者と共有することができる。

◆ 情報の取扱いの合意

情報保有機関が提供する情報が電子私書箱において適切に取り扱われるように、情報保有機関は、情報の取扱上の留意事項を電子私書箱へ確実に伝達し、必要に応じ、電子私書箱における当該情報の適切な管理のために必要な措置及び情報の利用目的を協議の上、合意・決定する必要がある。

➤実現における検討課題

情報保有機関と電子私書箱は、n:nの関係にある。参加組織が増えたときに、その都度協議の上で情報の取扱いにつき合意・決定する運用は負担が大きく検討が必要である。

10. サービスレベルと情報の持ち方の関係

- ◆ 各アクタのサービスレベルが異なることによって情報の持ち方に影響が生じると考えられる。
 - 自ら情報を保有すればサービスレベルは独立して担保可能である。
 - 他機関の情報に依存する場合は、相手先のサービスレベルに依拠することとなり、担保は不可能となる。
 - 従って、サービスの緊急性・重要性(国民の生命・財産に影響を与える可能性)の観点から、情報保有について整理する必要がある。
 - また、既存のサービスレベルが前提となると思われるので、民間事業者の現状を把握する必要がある。

