提供先第三者に係る情報銀行の認定・運用上の課題について
－1.PマークとISMS認証に加えて許容される第三者認証等について
- 提供先第三者の選定条件に係る事例とその課題
- 解決の方向性と新たな第三者認証等に必要とする基本要件
- 許容される新たな第三者認証等（候補）
- 認定指針への記載方法（案）

当該指針ver2.0の記載

（事業者の適格性 ②業務能力など の3）

・個人情報の取り扱いの業務を的確に遂行することができる知識及び経験を有し、社会的信用を有するよう実施・ガバナンス体制が整っていること

（例）類似の業務経験を有する、プライバシーマーク・ISMS認証などの認証を有している 等

（事業者の適格性 ②業務能力など の4）

・情報提供先との間でモデル約款の記載事項に準じた契約を締結することで、情報提供先の管理体制を把握するなど適切な監督をすること、情報提供先にも、情報銀行と同様、認定基準に準じた扱い（セキュリティ基準、ガバナンス体制、事業内容等）を求めること（※）等

（事業者の適格性 の欄外）

（※）情報銀行は、提供先がPマークまたはISMS認証を取得していない場合・・・（以下略）

PマークとISMS認証に加えて許容される第三者認証等について

認定審査の過程で出てきた 提供先第三者の選定条件に係る事例とその課題

※構成員限り

PマークとISMS認証に加えて許容される第三者認証等について

認定および認定情報銀行の普及における課題（まとめ）

指針および認定基準の「提供先第三者の選定基準」が厳しく、提供先が限られてしまうことが、認定取得および認定情報銀行の普及拡大の妨げになっている

1.提供先第三者の実態

- 提供先第三者は、自社のブランド（信用）で商いをするB2C事業者であるため、Pマーク等第三者による認証（信用）を取得する動機が低い
- 提供先が第三者認証を取得する場合、ISMS(情報セキュリティ)よりも、プライバシー保護認証の方がニーズが高い
- 提供先第三者には、大企業の“一店舗・一部門”や “中小企業(店舗)”が一定数存在するが、企業の“一店舗・一部門”単位では、原則Pマークを取得できない
- ISMSは部門単位での取得は可能であるが、前述の通りISMSを取得する動機が低い

2.解決の方向性

- 先ずは、大企業の“一店舗・一部門” を想定した、Pマーク、ISMS認証に加えて許容される新たな“プライバシー保護認証”を、提供先選定条件に加える。

3.新たな第三者認証等に必要とする基本要件（案）

- プライバシー保護に関する認証であること（JIS Q15001、JIS X9250ベース）
- 企業の“一店舗・一部門”での認証取得が可能であること
- 一定の対外的信頼がある 第三者＊認証機関による認証であること（＊IT連盟以外）

PマークとISMS認証に加えて許容される第三者認証等について

4.許容される新たな第三者認証等（候補）※詳細は別紙ご参照

以下が候補としてあげられており、基準の正当性×認証の対外信頼性×普及可能性にて、許容の可否を検討したい。また、情報銀行自体の認証としても検討したい。
（進め方：認定団体等により詳細検討を行い 総務省での検討を経て、指針検討会WGに諮る）

	基準の正当性	認証機関	認証実績(ISMS)	認証の対外信頼性等
FISC安全対策基準	金融検査・監督の考え方と進め方（検査・監督基本方針）	金融庁による検査	–	FISC基準を基に、検査機関や監査法人が内容を解釈して、適合性を評価
①Pマーク情報銀行版(仮称)	JIS Q 15001:2017（ISMSを包含）	JIPDEC	–	Pマークの部門認証の例外措置を適用し、情報銀行の特性を見定めて審査項目を取捨選択して“パッケージ化”した『Pマーク情報銀行版』
②既存の部門JIS Q 15001	JIS Q 15001:2017（ISMSを包含）	ア 日本規格協会ソリューションズ	97件	認証機関の社会的認知は高いが、認証制度の社会的認知*がPマークやISMSに劣る *例）官公庁等の入札要件になっていない また、ISMSのオプションの位置付けが多く、審査機関によっては認証よりも評価に近い場合がある
		イ BSIグループジャパン	1,652件	
		ウ 日本品質保証機構（JQA）	1,159件	
		エ SGSジャパン	375件	
ア. JIS・ISO規格を作成している日本規格協会のグループ企業。ISMS等との組合せや、JIS Q 15001単独取得も可。 ~~イ. 世界初の国家規格協会(英)BSIの日本法人。ISMSのアドオンとしてJIS Q 15001認証が可能。~~ ウ. 品質(ISO 9001、PSC等)を中心とした認証・検査等実施企業。JIS Q 15001単独、他規格との組合せ取得も可。 ~~エ. 世界100か国以上で規格の認証等行う(仏)SGS社の日本法人。ISMSにJIS Q 15001を取入れた認証を実施。~~				
③ISO 27701	ISMS+JIS X 9250	未定	–	策定中に付き認証開始はしばらく後となる
④独自基準	JIS Q 15001ベース	未定	–	第三者認証機関による認証が必要（IT連による認証は“第三者認証”ではない）

PマークとISMS認証に加えて許容される第三者認証等について

5.認定指針への記載方法（案）

１）考え方

・WGおよび検討会親会にて決定された具体認証については、その具体名を追加する。
・上記を含め明示された認証に加え、認定の運用上、認定団体が許容すると判断する認証等が生じた場合は【等】の中に読み込むことを可能とし、その後認定指針においても明示するか否かは検討会において議論することとする。
※【等】には、準ずる第三者認証または第三者による監査証明書等が該当。

２）指針の記載方法（案）

１）事業者の適格性 ②業務能力など（3）

・個人情報の取り扱いの業務を的確に（中略）実施・ガバナンス体制が整っていること
（例）類似の業務経験を有する、プライバシーマーク・ISMS認証・【追加認証の具体名】などの第三者認証等を有している 等

１）事業者の適格性 ②業務能力など（4）

・情報提供先との間でモデル約款の（中略）適切な監督をすること、情報提供先にも、情報銀行と同様、認定基準に準じた扱い（セキュリティ基準、ガバナンス体制、事業内容等）を求めること（※）等

１）事業者の適格性 の欄外

（※）情報銀行は、提供先がPマークまたはISMS認証、【追加認証の具体名】などの第三者等を取得していない場合であっても（以下略）

提供先第三者に係る情報銀行の認定・運用上の課題について
－２.提供先第三者の選定に係る記載の明確化について
・情報銀行事業者におけるサービスの事例
・事例を踏まえた上での認定審査運営上の課題
・認定指針の記載についての具体例（案）

当該指針ver2.0の記載（事業者の適格性 ②業務能力など）

・情報提供先との間でモデル約款の記載事項に準じた契約を締結することで、情報提供先の管理体制を把握するなど適切な監督をすること、情報提供先にも、情報銀行と同様、認定基準に準じた扱い（セキュリティ基準、ガバナンス体制、事業内容等）を求めること（※）等

（※）情報銀行は、提供先がＰマークまたはＩＳＭＳ認証を取得していない場合であっても、

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

②提供先において特定の個人を識別できないよう、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

③情報銀行の監督下で、提供先からＰマークまたはＩＳＭＳ認証を取得している者に個人情報の取扱いを全て委託させる

のいずれかの対策を講じた上で、それぞれのケースにおいて求められる情報セキュリティ・プライバシーに関する具体的基準を提供先が遵守していると認められる場合には、「認定基準に準じた扱い」であるとすることができる。

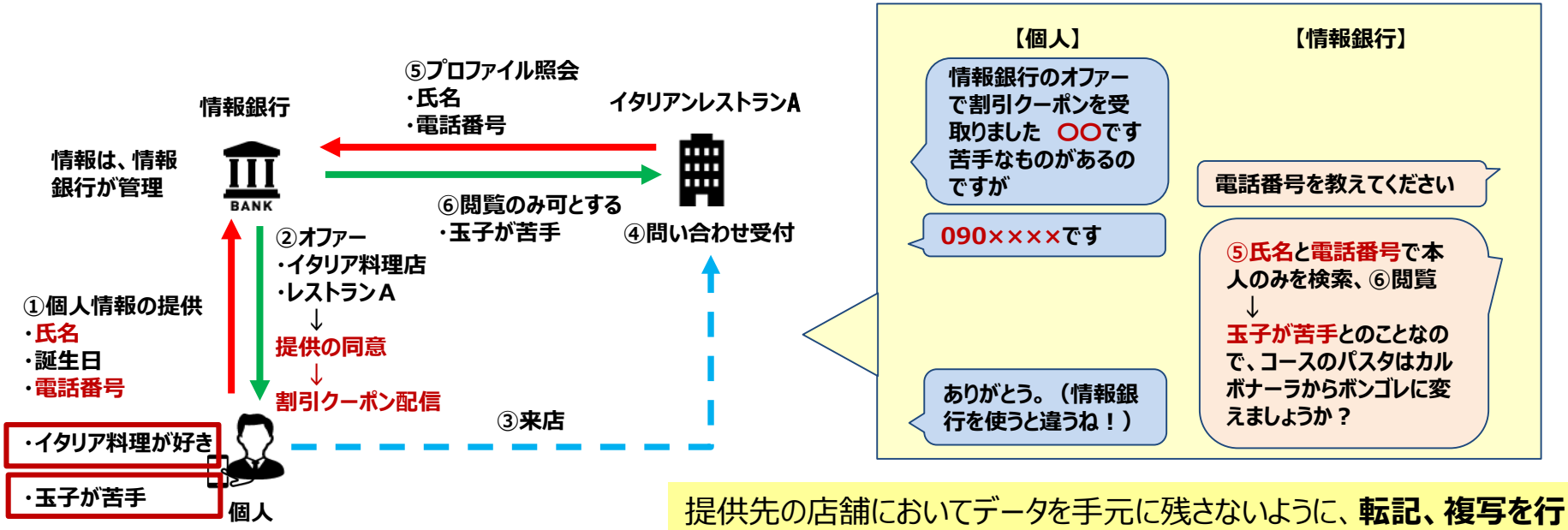
提供先がPマークまたはISMS認証を取得していない場合①　事例1

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点	どのような情報・手法であれば提供先が閲覧しても問題ないか？（転記、複写等の目的外利用を排除）

①事例１（提供先の店舗で 個人のプロファイルを確認する場合）

提供先の店舗において、本人からの申し出により、本人が提示するアクセスキーを用いて本人確認する場合。提供先は、直接本人から取得した個人情報を用いて、情報銀行に保管してある本人の個人情報を閲覧する。
（提供先に本人が、直接問い合わせを行い、本人の登録情報を確認する場合など、以下図解参照）



提供先の店舗においてデータを手元に残さないように、**転記、複写を行わない契約を締結した上で、一覧での閲覧は不可とする必要がある。**

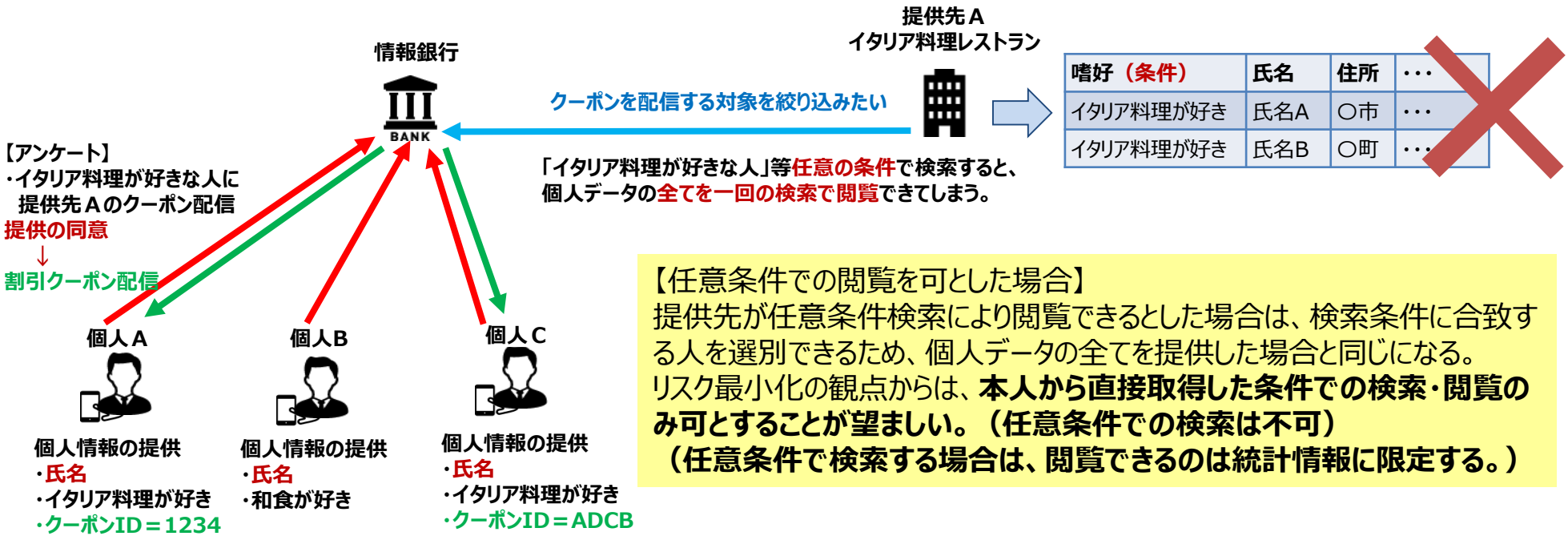
提供先がPマークまたはISMS認証を取得していない場合①　認められない事例1

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点	どのような情報・手法であれば提供先が閲覧しても問題ないか？

①認められない事例1　任意条件での検索を可とした場合

任意条件での検索を可とした場合、以下の事例のように対象者の個人データを「提供」した結果と同じになる。
転記・複写禁止を契約条項に含めても、違反時の罰則は適用できるが、違反を止めることはできないためリスク対策が必要



【任意条件での閲覧を可とした場合】
提供先が任意条件検索により閲覧できるとした場合は、検索条件に合致する人を選別できるため、個人データの全てを提供した場合と同じになる。
リスク最小化の観点からは、**本人から直接取得した条件での検索・閲覧のみ可とすることが望ましい。（任意条件での検索は不可）**
（任意条件で検索する場合は、閲覧できるのは統計情報に限定する。）

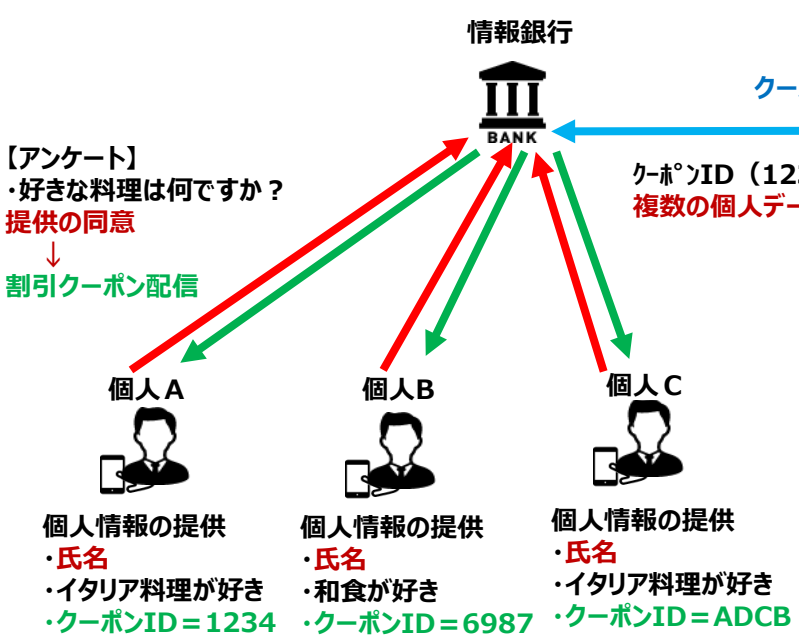
提供先がPマークまたはISMS認証を取得していない場合①　認められない事例2

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点	どのような情報・手法であれば提供先が閲覧しても問題ないか？

①認められない事例2　一度に複数人の検索を可とした場合

一度に複数人の閲覧を可とした場合、以下の事例のように対象者の個人データを「提供」した結果と同じになる。
転記・複写禁止を契約条項に含めても、違反時の罰則は適用できるが、違反を止めることはできないためリスク対策が必要



クーポンID（条件）	氏名	嗜好
1234	氏名A	イタリア料理が好き
6987	氏名B	和食が好き
ADCB	氏名C	中華料理が好き

【複数人の閲覧を可とした場合】
複数人の検索を可とすると、一回の検索で条件に該当した複数の個人情報を一覧で閲覧できることとなるため、個人データの全てを提供した場合と同じになる。
転記・複写禁止を契約条項に含めても、違反時の罰則は適用できるが、違反を止めることはできないため、**一人分のみ閲覧とすることが望ましい。**
（複数人の同時閲覧は不可）

提供先がPマークまたはISMS認証を取得していない場合①　論点

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点	どのような情報・手法であれば提供先が閲覧しても問題ないか？（転記、複写等の目的外利用を排除）

解決案：転記、複写等の目的外利用を排除するリスク対応が必要

組織的対策	**転記、複写を行わない契約**を締結する
技術的対策	**一覧での閲覧は不可とする**技術的対策を講じる（転記、複写リスク）
	一人分のみ閲覧とする技術的対策を講じる
	任意検索不可とする＊（本人が提示したアクセスキーで検索。このアクセスキーは提供先が事前に知り得ないもの）
	複写ができないよう技術的対策を講じることが望ましい
物理的対策	提供先のサービスモデルに応じて、必要な情報のみ閲覧ができるよう表示項目を限定することが望ましい

＊プロフィール等の条件を指定して、該当者複数名を一覧検索する「任意検索」は不可とする
＊プロフィール等の条件を指定して検索する場合、該当者人数等の個人データに該当しないよう統計情報のみを閲覧可とする。
＊対面での対応に対して、本人からの申し出により、本人が提示するアクセスキーを用いて本人確認する場合であって、氏名、生年月日など２要素を聞いて検索することとする（類似例：コールセンターでの応対システム）

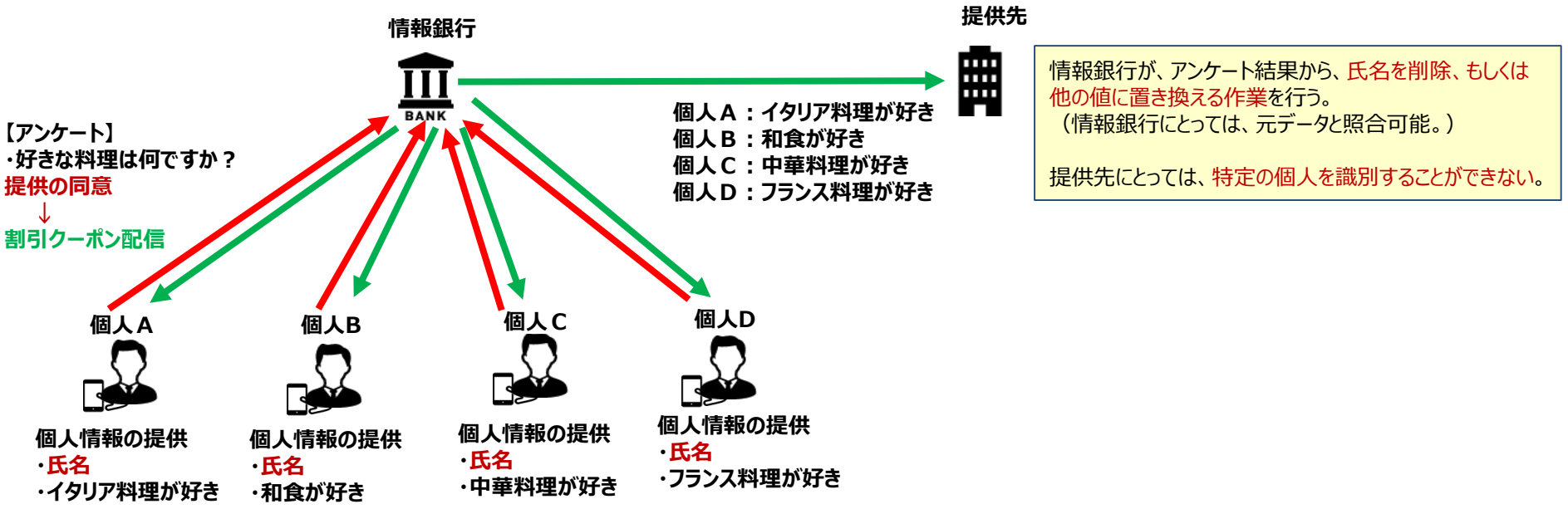
提供先がPマークまたはISMS認証を取得していない場合②　事例1

②提供先において特定の個人を識別できないよう、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

課題・論点	提供しても安全といえるような処理はどのようなものか、議論が必要ではないか？

②事例１（記名アンケートの情報を提供する場合）

情報銀行が、アンケート調査対象者の属性情報、アンケート回答内容、ウェブサイトへのアクセスログ等、**当該情報のみでは直接特定の個人を識別することができない情報を、提供先に提供する場合。**



提供先がPマークまたはISMS認証を取得していない場合②

②提供先において特定の個人を識別できないよう、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

課題・論点	「特定の個人を識別できない」ための要件とは何か

特定の個人を識別する情報を除くこと（規則19条1号の加工）

「匿名加工情報の適正な加工の方法に関する報告書」（2017年2月21日版　国立情報学研究所「匿名加工情報に関する技術検討ワーキンググループ）を参照すると、組み合わせによって特定の個人を識別することができる記述等となる項目を以下のとおり、限定的に考えることが望ましい。

(a)氏名以外の基本4情報（住所、生年月日、性別）
(b)現在所属するまたは過去に所属した会社、学校等の団体、職歴および学歴であって、具体的な会社名、団体名を含むもの
(c)本人到達性のあるメールアドレス、SNSのID
(d)本人到達性のある電話番号（スマートフォン、自宅の電話番号、職場等の電話番号）
(e)クレジットカード番号
これらに(f)単体で特定の個人を識別することができるもの(氏名、顔画像）を合わせた特定の個人を識別することができる記述等を構成する項目を、以下「特定対象項目」という。
※(a)のうち、住所については市区町村、生年月日については年までとする。性別はそのまま残してよい。

同報告書では、個人情報保護委員会規則第19条第1号の措置の対象となる情報については、「全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）」を求めている。

提供先等で個人情報と照合ができない状態にすること（規則19条5号の加工）

情報又はその組み合わせが一意で、その情報と氏名等が紐づく情報が提供先等にとって入手可能な場合、そのような情報又はその組み合わせは、提供先等で個人情報になる。たとえば、アプリベンダーAが保有するユーザーのGPS移動履歴は多くの場合一意である。アプリベンダーAはユーザーの氏名等を保有しないが、アプリベンダーBはGPS移動履歴と氏名を保有しているとき、アプリベンダーAの保有するGPS移動履歴は、アプリベンダーBにとって個人情報である。

提供先がPマークまたはISMS認証を取得していない場合②　論点

②提供先において特定の個人を識別できないよう、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

課題・論点	提供しても安全といえるような処理はどのようなものか、議論が必要ではないか？

解決案：提供しても安全といえる処理（１）or（２）

（１）匿名加工情報相当のものとする
1号加工から5号加工までのすべてを行うが、匿名加工情報作成の意図がないため作成時公表義務等の対象にはならない。

（２）NIIの報告書を参考に、1号加工、2号加工（個人識別符号の削除等）、4号加工（一般的に特異な情報の削除等）を行うが、履歴は原則としてそのままとする。
特定の個人を識別する可能性がないとは言えないが、現在の履歴には要配慮個人情報が含まれていないことから、個人識別のリスクは許容される範囲と考えていいか？

※指針の記載文言のうち「個人情報の暗号化処理または」は、削除する
（IT連盟の認定基準「認定申請ガイドブック」ではパブコメでの指摘もあり 削除済み）

<u>個人データの再提供の制限への該当性について</u>

「提供先第三者において個人情報を統計情報等個人情報ではないデータに加工し、別の第三者に提供する」場合には、指針2.0によって再提供禁止が緩和されている。（１）の場合は情報銀行によって匿名加工情報相当の加工が行われているため、特定の個人を識別するおそれはなく、再提供は認められる。（２）の場合、特定の個人を識別するおそれがないとはいえないことに加えて、提供先が通常の要件を満たしておらず、再提供先との契約等について不備があるおそれがあるため、再提供は禁止とする。

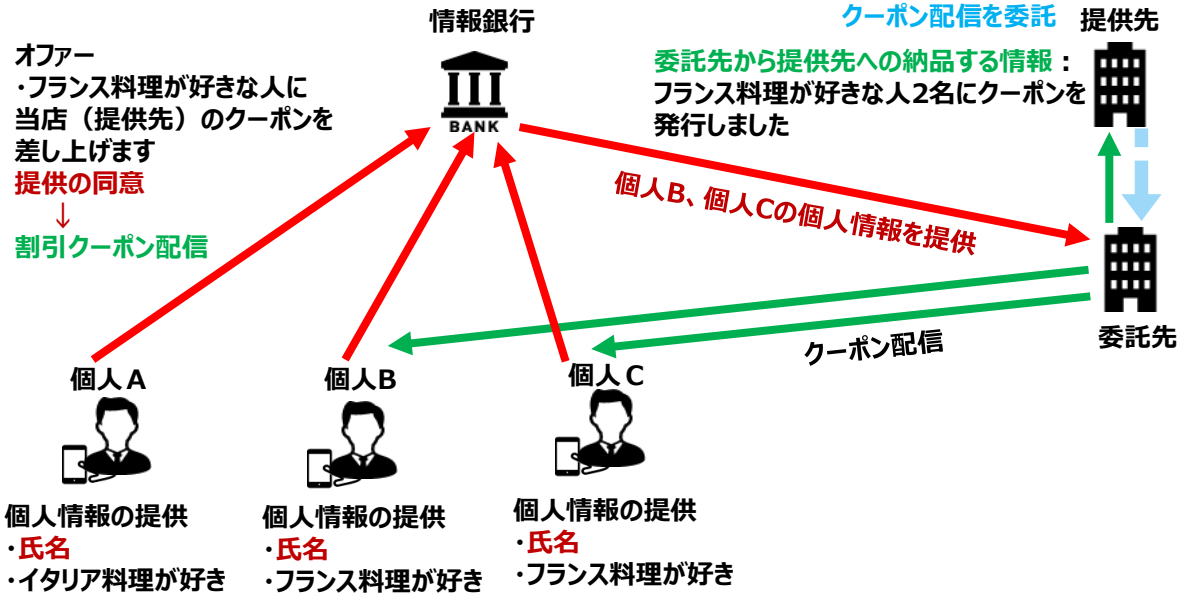
提供先がPマークまたはISMS認証を取得していない場合③　事例1

③情報銀行の監督下で、提供先からPマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる

課題・論点	提供先（委託元）と委託先のスキームと情報銀行の役割を具体化する必要があるのではないか？

③事例１（委託先にクーポン配信を委託する場合）

提供先が、委託先に個人情報の取扱いの全てを委託しているケース（委託先にクーポン配信を委託）
・提供先(委託元)は、委託先に個人データの取扱いを委託するため、提供先に個人データへのアクセス権限は付与しなくて良い。



・提供先はクーポンIDのみを受取る
「提供先において特定の個人を識別できないよう、個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する」に該当する

※提供先がクーポンIDすら受取らない場合、委託先は提供先に個人情報を納品しないことになるが、情報銀行は個人情報を提供したといえる（提供元基準）

・Pマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる
情報銀行で委託を受けても良い

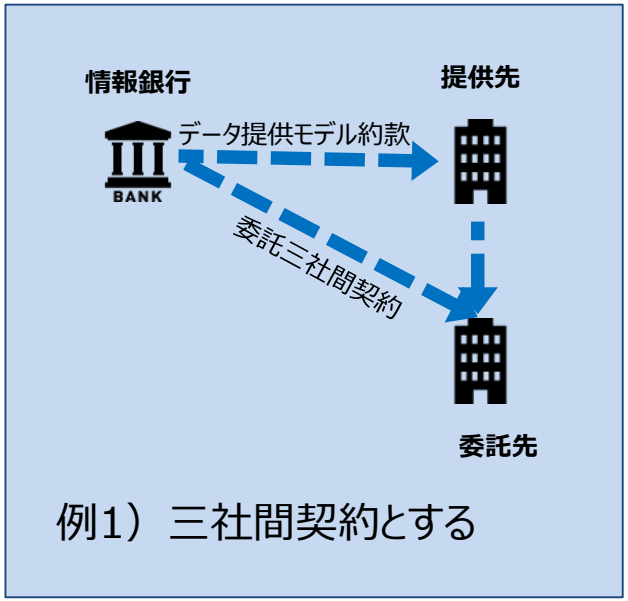
提供先がPマークまたはISMS認証を取得していない場合③　事例1

③情報銀行の監督下で、提供先からPマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる

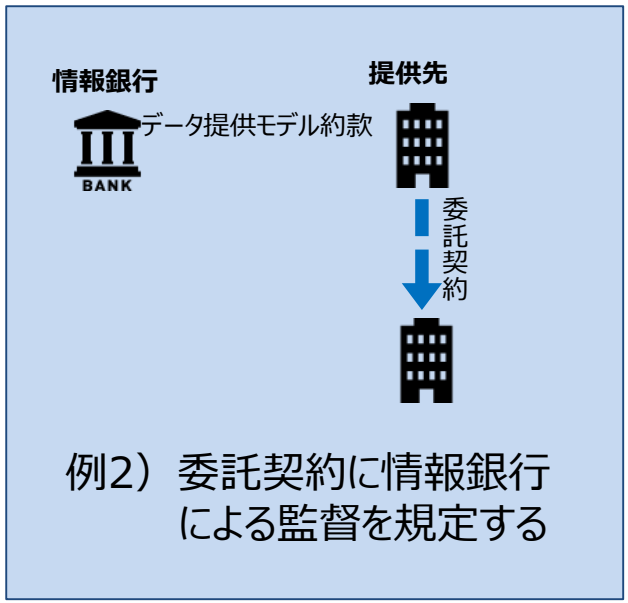
課題・論点	「情報銀行の監督下で委託させる」とは、どのような契約が必要か

③事例１（委託先にクーポン配信を委託する場合）

三社間契約または、委託契約にて「情報銀行の監督下」とする場合



例1）三社間契約とする



例2）委託契約に情報銀行による監督を規定する

情報銀行の監督が及ぶために
委託契約に盛り込むべき要件

b) 個人データの安全管理に関する事項
d) 個人データの取扱状況に関する情報銀行への報告の内容及び頻度
e) 契約内容が遵守されていることを情報銀行が，定期的に，及び適宜に確認できる事項
f) 契約内容が遵守されなかった場合の措置
g) 事件・事故が発生した場合の報告・連絡に関する事項

提供先がPマークまたはISMS認証を取得していない場合③　論点

③情報銀行の監督下で、提供先からPマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる

課題・論点	提供先（委託元）と委託先のスキームと情報銀行の役割を具体化する必要があるのではないか？

解決案：委託元(提供先)と委託先のスキームの整理

リスク対応として、**提供先(委託元)には、それ単体で個人情報となる情報へのアクセス権限を付与しない**

本人に対するオファーや提供先で利用するクーポン発行は、**提供先(委託元)の個人情報の利用目的の中で委託を受ける**

提供先(委託元)には、提供元で個人情報となる情報を納品しなくても、提供先の利用目的で個人情報を扱う場合には、提個人情報の提供に該当する

情報銀行事業者が委託を受けても良い（情報銀行サービスとは別サービスとする）

解決案：情報銀行の役割を具体化

「情報銀行の監督下で、委託させる」場合の具体的条件を提供先の委託契約に規定する

例1）情報銀行、提供先、提供先の委託先間での三社契約

例2）提供先が委託先と締結する委託契約に情報銀行の監督が及ぶように規定する

a) 委託者及び受託者の責任の明確化
b) 個人データの安全管理に関する事項
c) 再委託に関する事項
d) 個人データの取扱状況に関する委託者への報告の内容及び頻度
e) 契約内容が遵守されていることを委託者が，定期的に，及び適宜に確認できる事項
f) 契約内容が遵守されなかった場合の措置
g) 事件・事故が発生した場合の報告・連絡に関する事項
h) 契約終了後の措置

前述の事例を踏まえた上での認定審査運営上の課題

認定における課題：事業者が企画するビジネスモデルは多様であるため、基本的な考え方と照合し安全管理措置の十分性を審査する。事業者の企画が一見して基本的な考え方を満たさない場合でも、直ちに修正要請や認定の拒否を行うのではなく、各々のビジネスモデルとの関係で安全管理措置が十分かを審査する必要がある。

1.基本的な考え方を示す必要性

前述した事例における対策は、安全管理措置として十分なレベルに該当するため、これらの事例を事業者理解のために基本的案考え方として示すことが必要。なお、全く同一のサービスモデルは存在せず、多少の差異は生ずるので、この差異部分に対しては、慎重な審査が必要となる。

2.認定指針の記載の具体化

認定指針では現行の記載内容を分かりやすく修正することに留めるのが妥当。（次ページにて提示）

3.事例の公表

事業者の理解を進めるためにも事例の公表が必要と考える。
なお、該当する事例及び該当しない事例のそれぞれにつき、“典型的な例”を示すものとする。幾つかの業種の例を取り上げたもので、すべての業種の例を網羅しているわけではないことを前提とする。（実際には個別事案ごとに検討が必要）

※事例の公表方法

事例等解説を加えるのは「ガイドライン(手引き)」等の役割となるため、IT連盟の認定基準「情報銀行認定申請ガイドブック」の下位に位置する「データ倫理審査会人材育成プログラム」等への記載が相当と考える。

認定指針の記載についての具体例（案）

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

⇒情報は情報銀行が管理し、**提供先には転記・複写禁止の契約を締結し、一覧での閲覧や任意検索ができない方法で、一人分のみ検索できる技術的対策を施した上で、**必要な情報の閲覧のみができることとする。

②提供先において特定の個人を識別できないよう、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

⇒提供先において特定の個人を識別できないよう、**当該個人情報に含まれる記述等の一部を削除（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）処理を行い**、提供先に提供する　［暗号化処理を削除］

③情報銀行の監督下で、提供先からＰマークまたはISMS認証を取得している者に個人情報の取扱いを全て委託させる

⇒［追加］**提供先の委託先に対して情報銀行の監督が及ぶよう提供先の委託契約に規定する**