



2021年度 経済産業省・総務省・JIPDEC共催プライバシーガバナンスセミナー

パーソナルデータの利活用における JCBのプライバシー保護の取り組み

2021/9/14

株式会社ジェーシービー
コンプライアンス部情報管理室 主幹
日辻 治彦

1. JCBについて
2. プライバシーリスク評価体制
3. JCB消費NOWにおけるリスク評価例
4. プライバシーガバナンス構築に向けた課題

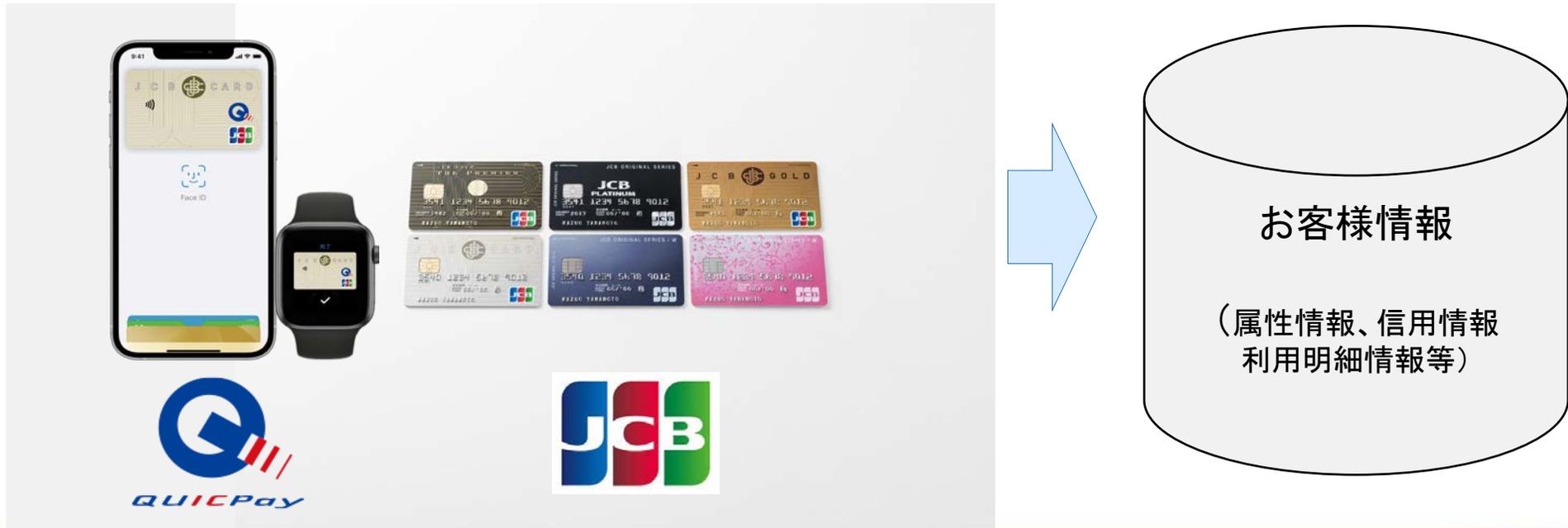
1. JCBについて (1) 企業概要

項目	内容
設立	株式会社ジェーシービー (JCB Co., Ltd.)
従業員数	4,375名
事業内容	クレジットカード業務、クレジットカード業務に関する各種受託業務、融資業務、集金代行業務、前払式支払手段の発行ならびに販売業およびその代行業
当期取扱高	33,825,514百万円 (2020年4月～2021年3月)
JCB加盟店数	約3,600万店
JCB会員数	141,025千会員

※上記計数はいずれも2021年3月期

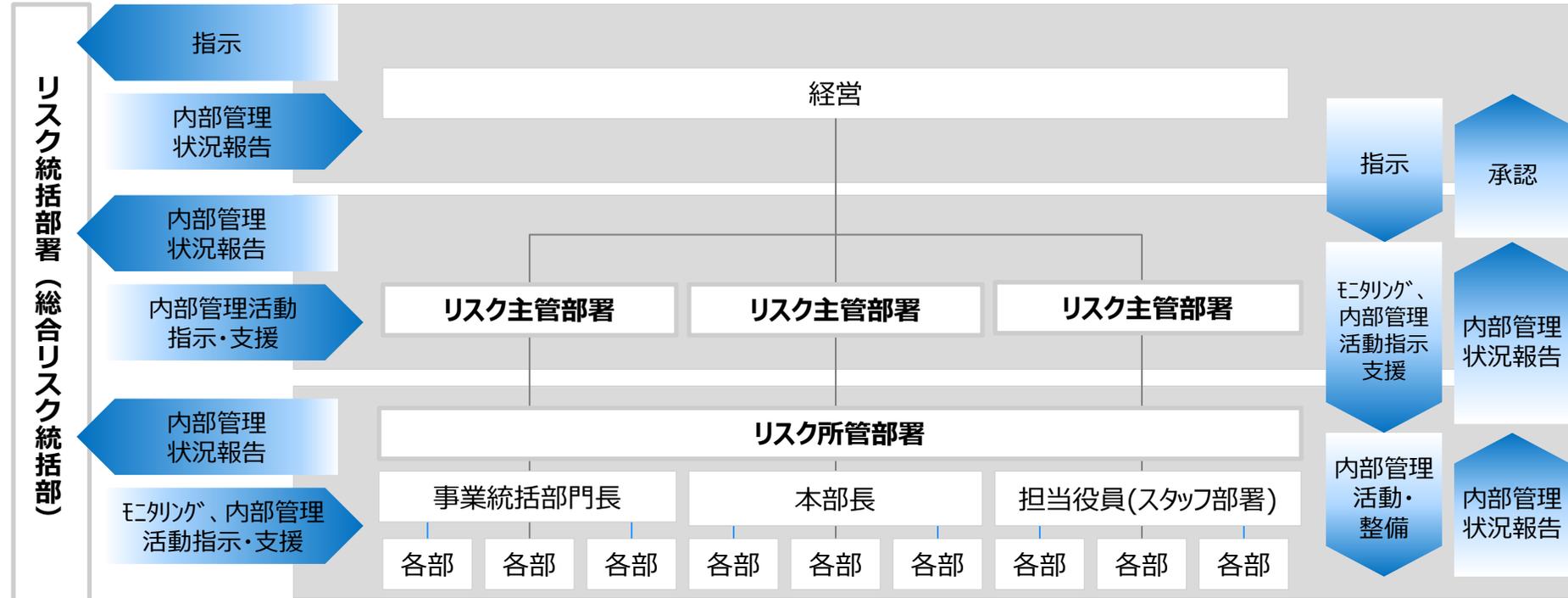
1. JCBについて (2) JCBにおけるプライバシー

- ・クレジットカードをはじめとした各種決済サービスを提供するため、お客様の属性情報、信用情報、カード利用明細情報、サービス利用履歴等プライバシーに関わる情報を大量に取り扱い。
- ・お客様の情報を漏えい、もしくは新商品・新サービスで不適切な利用を行なった場合、お客様のプライバシー侵害につながる可能性。
- ・プライバシー侵害につながる事象防止のため、情報漏えい防止のための安全管理措置と新商品・新サービス導入時のリスク評価を情報セキュリティの枠組みの中で実施。



2. プライバシーリスク評価体制 (1) 全社リスク管理態勢

- リスクに取り組むにあたり、役割ごとに『**リスク統括部署**』・『**リスク主管部署**』・『**リスク所管部署**』を定め、役割に応じたリスク管理を実施



- **リスク統括部署**：全社の内部統制の整備および運用を推進し、リスク主管部署あるいはリスク所管部署に対して指示、支援等を行う。
- **リスク主管部署**：**主管するリスクの内部統制の整備および運用を推進**し、リスク所管部署に対して指示、支援等を行う。
 リスク統括部署に対して、適宜状況を報告する。
 内部統制を効率的に推進すべく合理的な判断に基づき、リスク所管部署に自らの役割の一部を分担することができる。
- **リスク所管部署**：**組織内の内部統制の整備および運用を推進**する。
 リスク統括部署あるいはリスク主管部署に対して、適宜状況を報告する。

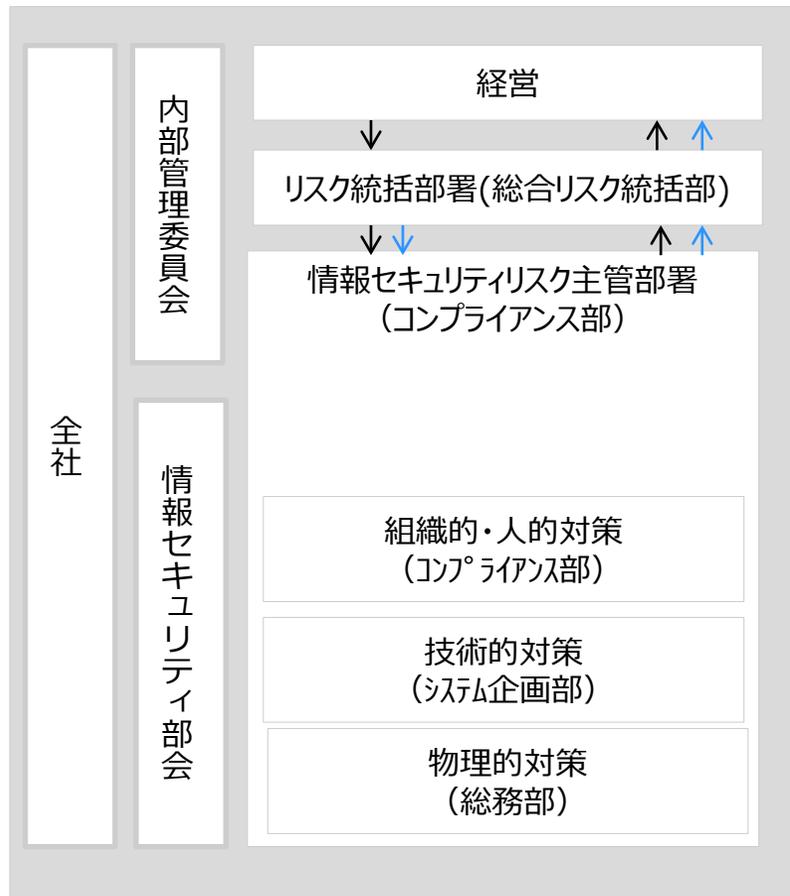
2. プライバシーリスク評価体制 (2) 全社リスク分類

- 事業に関連して発生する**12種類のリスク**と、**リスク毎にリスク主管部署**を定め、リスク毎のリスク管理を実施。
- プライバシーに関するリスクは**情報セキュリティリスク**として管理。

	リスク分類	リスク主管部署	リスク例
①	経営戦略リスク	総合企画部	事業戦略リスク、ビジネスパートナーリスク
	レピュテーションリスク	広報部	レピュテーションリスク
②	信用リスク	信用企画部	信用リスク、不正被害リスク
③	法令リスク	コンプライアンス部	-
④	契約リスク	コンプライアンス部	契約リスク、紛争リスク
⑤	財務リスク	経理部	金融市場リスク、資金流動性リスク
⑥	会計・税務リスク	経理部	会計リスク、税務リスク
⑦	資産ファシリティリスク	総務部	調達リスク、資産・在庫管理リスク
⑧	人的リスク	人事部	人材開発リスク、労働環境リスク
⑨	情報セキュリティリスク	コンプライアンス部	機密性毀損リスク、完全性毀損リスク
⑩	事務リスク	事務企画部	-
⑪	システムリスク	システム企画部	開発リスク、運用リスク
⑫	事故・災害リスク	総合リスク統括部	自然災害リスク、人的災害リスク

2. プライバシーリスク評価体制 (3) 内部管理委員会、情報セキュリティ部会

- 経営・リスク関連部の連携を目的に、**内部管理委員会・情報セキュリティ部会**を活用した相乗的なリスク管理を実現



弊社および関係会社における全社および組織内のリスク管理に関する基本方針の構築および運営を行なう場として、四半期ごとに内部管理委員会を開催
(毎回、10～15程度のテーマを報告)

- ・全社リスク管理・組織内リスク管理の管理状況の報告
⇒リスクレポート、内部管理状況(自己点検・モニタリング)
- ・主要リスクへの対応方針・実施施策内容の報告
⇒法令・情セ・反社・海外リスクなど各施策の活動報告

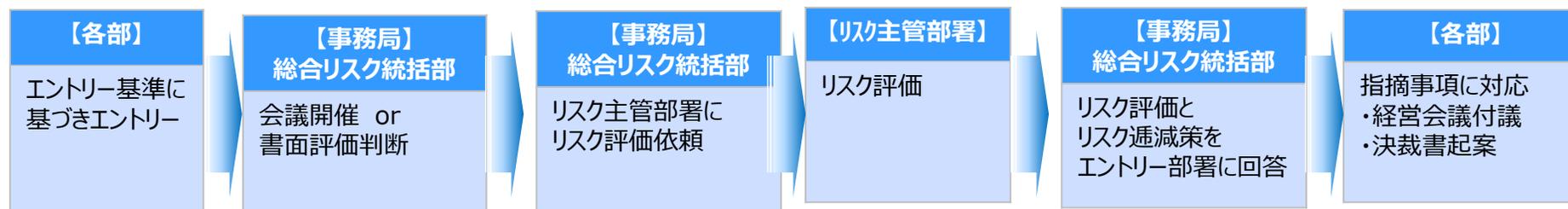
情報セキュリティリスク主管部署であるコンプライアンス部から情報統括責任者(コンプライアンス部担当役員)への報告の場として、毎月情報セキュリティ部会を開催
(毎月、数件程度のテーマを報告)

- (1) 情報セキュリティマネジメントシステムの構築状況
- (2) 情報管理に関する社内規程類、社内基準ならびに情報セキュリティ対策の策定、周知、実行の状況
- (3) 情報の紛失、漏洩、改竄その他事故等における危機対応と再発防止対策の実行状況
- (4) 各部署からの情報管理に関する報告の徴収、助言、指導状況等

2. プライバシーリスク評価体制 (4) SCM (Service Control Meeting)

- **商品・サービスの立案時に、リスク懸念事象を早期検知することによるリスクの抑制を目的**とし、SCM事務局やリスク主管部署等がSCM起案部署とリスクの共有や洗出し、リスク評価を行なうプロセス。(年間約数百件程度実施)
- 経営会議付議、決裁書起案される案件は、SCMにて可視化されたリスクと当該リスクに対する対応方針を明記させることで、**決裁者の適正な判断を実現させる。**

【SCMフロー】



【SCMエントリー基準例】

エントリー基準	エントリー条件(除外条件)
新規商品・サービス・ビジネス開発	全件(除外条件無し)
商品・サービス終了	全件(除外条件無し)
新規カード立上げ	全件(除外条件無し)
提携カード解消	消費者不利益に該当しない場合を除く
DM・キャンペーン・施策	景品表示法などの法令評価が済んでいる場合を除く
情報システム・機器の導入および更改	インターネットなどの外部接続をしない場合・ハード単体の導入を除く
個人情報を取扱う業務委託	既存業務委託のうち、個人情報取扱の変更が無い場合を除く

2. プライバシーリスク評価体制 (5) パーソナルデータ管理細則

- パーソナルデータ利活用ビジネスを推進するにあたり、**お客様の適切なプライバシー保護を図るための社内ルール。**
- **OECD8原則、その他各種プライバシーに関する法令等から利活用の原則を策定。(第2章)**
- **個人情報保護法、ガイドラインに定められた匿名加工情報に関するルールを反映(第3章)**
 識別可能性、および復元リスクを極力排除するために当社独自の対策を追加している他、
 匿名加工情報に含める情報項目・加工方法について弁護士、または個人情報保護委員会へ法令上問題ないか
 確認する手順を追加。

パーソナルデータ管理規則	条
第1章 総則	1. 目的
	2. 定義
第2章 パーソナルデータ利用時の原則	3. 顧客心情の尊重
	4. 顧客によるコントロール
	5. 明確でわかりやすいポリシー
	6. プライバシーリスクの大きさに応じた対策
第3章 匿名加工情報の利用	7. 匿名加工情報の利用
	8. 匿名加工情報の作成等
	9. 識別行為の禁止、
	10. 匿名加工情報の提供
	11. 社内手続

2. プライバシーリスク評価体制 (6) パーソナルデータ利活用チェックリスト

- **パーソナルデータ管理細則の準拠状況を確認するためのチェックシート。**
- **SCMエントリー後、SCM起案部署は、コンプライアンス部の指示にしたがって準拠状況を以下の観点で確認。**
準拠状況をコンプライアンス部に報告するとともに、不足事項があれば対策を立案。

#	原則	基準
1	経緯（コンテキスト）の尊重	お客様に不安を抱かせない、予期できる範囲で利用すること
		お客様がパーソナルデータを提供した際の経緯（コンテキスト）に沿って、本人の期待と合致する形態で利活用を行うこと
2	個人によるコントロール	お客様に、自分のデータをコントロールする機会（どのように利用されるかについて関与する機会）を確保すること
		サービスに応じて、オプトイン・オプトアウトを適切に使い分けること
3	明確でわかりやすいポリシー	お客様に、何のデータをどのように使うかわかりやすく伝えること
4	プライバシー・リスクの大きさに応じた対策	データ種別ごとのプライバシー性、データ利用形態のリスク度合に応じて、プライバシーへの影響を事前に評価して対策すること

3. JCB消費NOWにおけるリスク評価例 (1) JCB消費NOWとは①

- 東大発統計ベンチャー(株) ナウキャストとの共同開発による、当社決済データを活用した独自の消費統計。
- 既存政府消費統計比で、正確性(実取引データ)・速報性(月2回)・網羅性(EC業種カバー)が優位となるよう設計。
- 消費統計はWEBサイトにて公開し、官公庁や金融機関、投資会社等へ提供することにより収益化を企図した事業。

JCB会員



JCBカードでお買い物



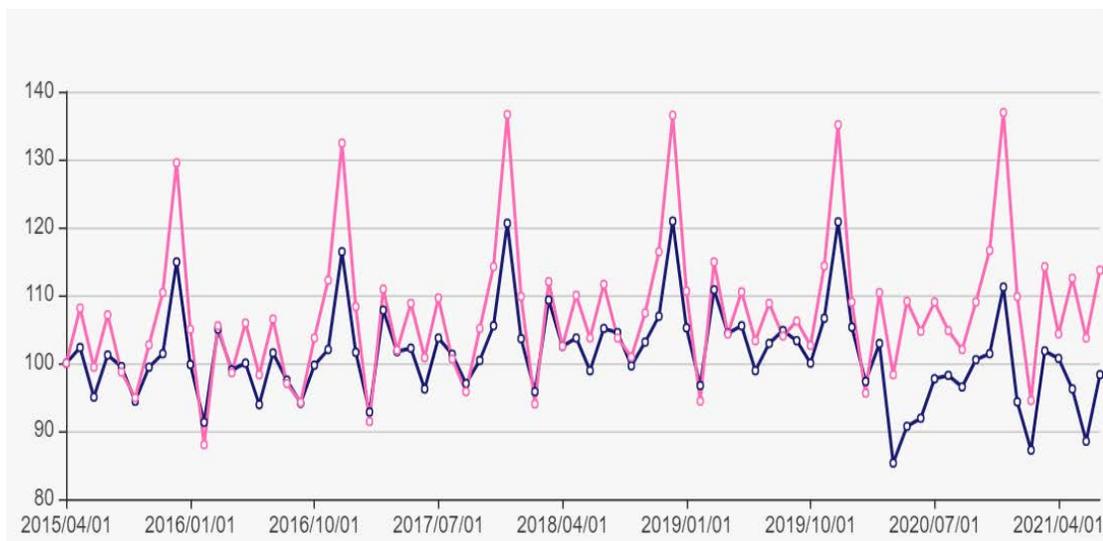
JCB/ナウキャスト



消費統計を作成



JCB消費NOW



「JCB消費NOW」サイトで公開

統計閲覧会員



分析・活用

3. JCB消費NOWにおけるリスク評価例 (1) JCB消費NOWとは②

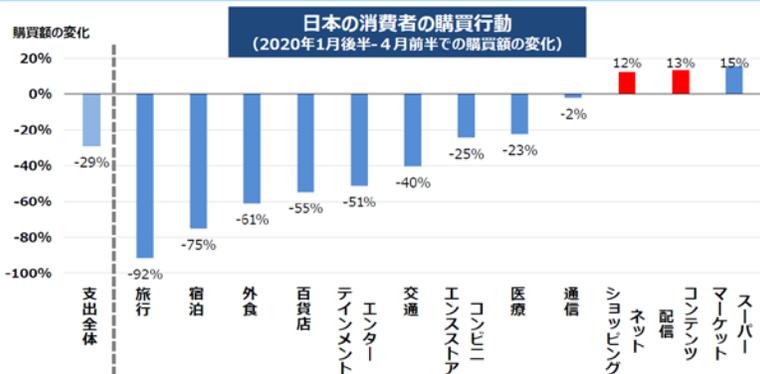
➤ 官公庁作成資料をはじめ、多方面での引用実績あり。

■ 経産省「産業構造成長戦略部会」基礎資料 (2020/5/1)

日本の消費者の購買行動

新たなビジネス

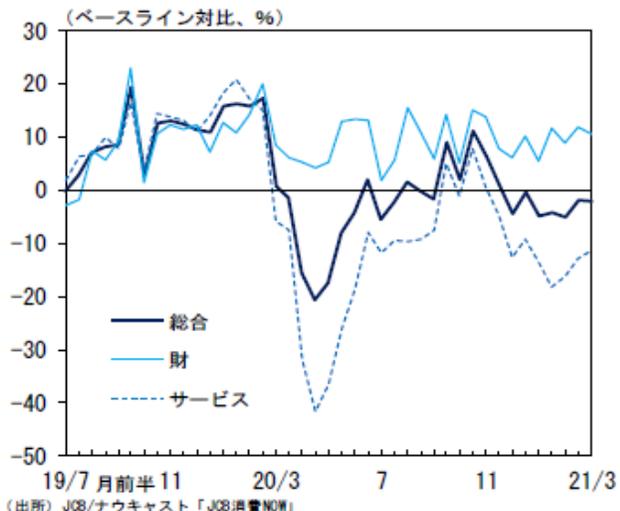
- 日本のクレジットカード購買額を見ると、2020年1月後半から4月前半にかけて、旅行 (▲92%)、宿泊 (▲75%)、外食 (▲61%) など大きく減少したのに対し、ネットショッピング (+12%)、コンテンツ配信 (+13%) が増加。



(注) 株式会社ナウキャスト、株式会社ジェシービー「JCB消費NOW」(JCBカードの利用者約100万人の購買を集計したデータ)
(出所) Tsutomu Watanabe「The Responses of Consumption and Prices in Japan to the COVID-19 Crisis and the Tohoku Earthquake」作成、35

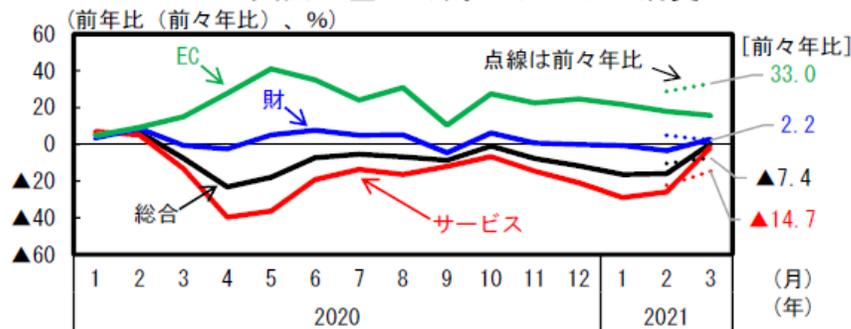
■ 日本銀行「経済・物価情勢の展望」資料 (2021/4/28)

図表35: カード支出に基づく消費動向



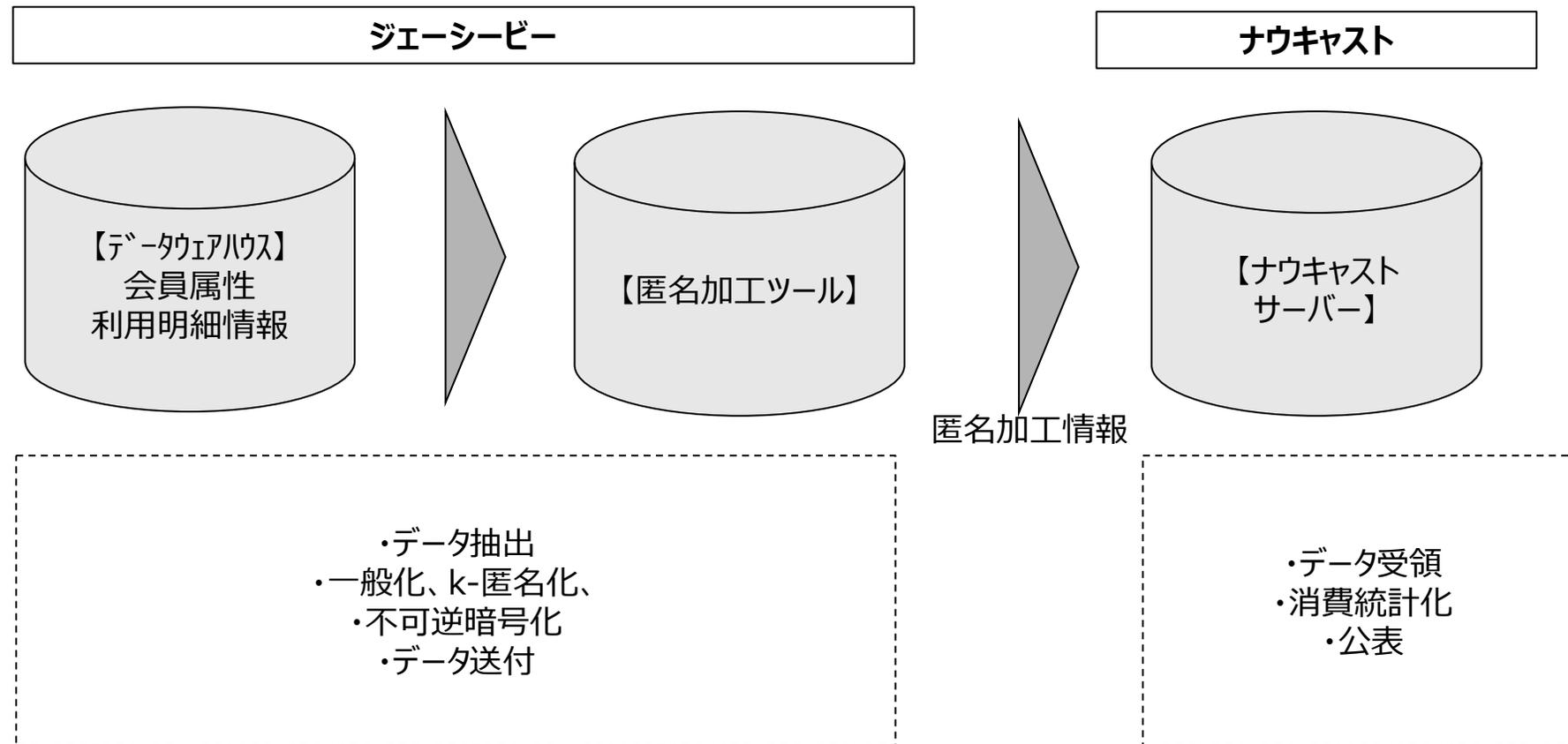
■ 内閣府「月例経済報告等に関する関係閣僚会議」資料 (2021/4/22)

カード支出に基づく財・サービス消費



3. JCB消費NOWにおけるリスク評価例 (1) JCB消費NOWとは③

- 当社で元データとなる対象データ（会員属性情報、利用明細情報）を抽出し、匿名加工情報化。
- 提携先であるナウキャスト社に匿名加工情報を提供。
- ナウキャスト社で当社から提供した情報をもとに消費統計化しWEBサイトにて公開。



3. JCB消費NOWにおけるリスク評価例 (1) JCB消費NOWとは④

- JCBからナウキャスト社に提供する匿名加工情報は以下の通り。
- 当社会員データベースからサンプル会員を無作為に抽出。各項目に対して匿名加工化を実施。

データ種別	データ項目	加工方法	表示形式
個人識別子	個人番号	不可逆暗号化	仮ID (ハッシュ化された個人番号)
属性情報	居住地	一般化	都道府県
	年代	一般化	5歳刻み (例: 20~24歳) ※90歳以上は削除
	性別	加工なし	1 (男性) または2 (女性) の数字
	契約年月日	一般化	年月 (yyyymm)
利用情報	利用年月日	一般化	15締or未締 (2019年10月16日⇒2019年10月末締)
	利用金額	加工なし	数字
利用加盟店情報	加盟店番号	加工なし	数字14ケタ
	加盟年月日	一般化	年月 (yyyymm)
	加盟解約年月日	一般化	年月 (yyyymm)
	業種コード	加工なし	数字5ケタ
	店頭通販契約区分	加工なし	数字1ケタ

3. JCB消費NOWにおけるリスク評価例 (2) 各部リスク評価

- 企画段階で、施策実施部署が他社のプライバシー侵害事案における課題を整理し、プライバシー保護対策を立案。
- 法令遵守をしても風評リスクが残存することを前提に、法令順守だけでなく、お客様の心情に寄り添った対応 (+α) を行う必要があると評価。
- 今回の評価は重要な案件としてリスク主管部署であるコンプライアンス部と一緒に実施。

#	当社で考えた他社プライバシー侵害事案の課題	プライバシー保護対策
1	顧客への事前説明が十分にされていなかった	顧客目線のわかりやすい説明ページを設置するとともにeメール等の各種媒体でサービス内容を周知 ・JCB消費NOWとは？ https://www.jcb.co.jp/service/pop/jcbconsumptionnow.html ・匿名加工情報とは？ https://www.jcb.co.jp/service/pop/tokumeikakou.html
2	オプトアウト機能があるもののわかりにくかった	オプトアウト機能設置と会員目線での周知
3	適切で客観的な法令評価がされていなかった	個人情報保護委員会に事前相談し法令違反にならないことを確認する。
4	匿名加工化が十分でないため識別可能性が残存していた	個人情報保護委員会ガイドラインに準拠した匿名加工を実施する。
5	データ提供先における情報取扱方法が明確でなかった	データ提供先に目的外利用禁止、安全管理措置を契約で義務付けるとともに、契約遵守状況を確認するためにオンサイト・オフサイトモニタリングを実施。
6	顧客からみてデータ利活用目的が納得できるものでなかった	一企業の利益ではなく <u>公共度の高い利用目的</u> であることを説明する。 ・経済指標高度化

3. JCB消費NOWにおけるリスク評価例 (3)SCM・経営会議

- 施策実施部署が立案した対策をSCMで各リスク主管部署が評価し、リスク低減のための指摘を実施。
- S C M指摘事項に対し、施策実施部署とコンプライアンス部で対応方針を策定。
- サービス開始を審議する経営会議で、S C M指摘事項を残余リスクとその対応方針として報告し経営陣の承認を取得。
- さらにリリース前に、マスメディア、個人ブログ・SNS等でのネガティブな掲載、会員からの苦情等の発生状況を確認。リスクが発生していないことを確認して、再度経営会議で報告のうえリリースをしている。

#	各リスク主管部署からのSCM指摘事項	対応
1	匿名加工情報の利用について安全・安心であることを十分に告知すること	告知内容は、誤解を与えないようわかりやすい表記にする。
2	匿名加工情報の加工について個人情報保護委員会事務局レポートに沿った対応を行うこと	レポートに基づいた対応を行うとともに個人情報保護委員会にも適宜相談する。
3	社会的風評のモニタリングを実施するとともに、社外公知後の風評リスクを見極め、風評リスク大になった場合の対応・利用停止措置を講じる前提で進めること	開始前、開始直前、開始後それぞれにチェックポイントを設けて風評リスクを評価。
4	会員が拒否できる期間を一定期間設置後、運用を開始すること	オプトアウト受付開始後、一定期間を設け運用を開始する

4. プライバシーガバナンス構築に向けた課題

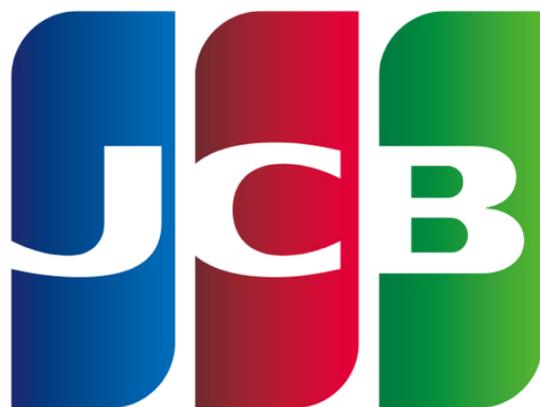
- ▶ 当社のプライバシーは、個人情報保護法に沿った対応をしつつ、OECDプライバシー 8 原則における「⑤安全保護の原則」に重点を置いた「情報セキュリティ」の枠組みでの取り組み。
- ▶ 世の中のプライバシー意識の高まりのなか、お客様の当社に対するプライバシーのニーズを見極め、当社ならではのプライバシーの概念・定義をつくり、情報セキュリティに限定されない、あらたなプライバシーへの取り組みをしていくことが必要。

OECDプライバシー 8 原則	個人情報保護法
①収集制限の原則	適正な取得（第17条）、取得に際しての利用目的の通知等（第18条）
②データ内容の原則	利用目的による制限（第16条）、データ内容の正確性の確保（第19条）
③目的明確化の原則	利用目的の特定（第15条）
④利用制限の原則	利用目的による制限（第16条）、第三者提供の制限（第23条）
⑤安全保護の原則	安全管理措置（第20条）、従業員の監督（第21条）、委託先の監督（第22条）
⑥公開の原則	保有個人データに関する事項の公表等（第27条）
⑦個人参加の原則	開示（第28条）訂正等（第29条）利用停止等（第30条）理由の説明（第31条）開示等の請求等に応じる手続き（第32条）手数料（第33条）
⑧責任の原則	個人情報取扱事業者による苦情の処理（第35条）

4. プライバシーガバナンス構築に向けた課題

- 当社は情報セキュリティに関して、ISMSをベースにした管理態勢の中で、従業員へ継続的な周知徹底を実施することで、従業員における情報セキュリティに関する意識は高く共通の目標を持っている
- 今後はプライバシーに関する意識も情報セキュリティと同様に高め、新たなプライバシーに関する目標に向けて取り組んでいくことが必要

#	情報セキュリティに関する研修プログラム	対象	内容
1	コンプライアンスの手引き	全従業員	情報セキュリティに関する基本ルールが掲載された従業員向ハンドブック 情報セキュリティだけでなくコンプライアンス全体を網羅。
2	情報セキュリティ教育研修 (全社E-Learning)	全従業員	情報取扱ルールの理解度を確認するもの。 部長向、一般従業員向と階層をわけて実施。
3	情報セキュリティ教育研修 (部門独自研修)	全従業員	各部の情報リスクアセスメント結果から各部におけるリスクと対応、 各部における独自情報取扱ルールについて説明する
4	新任管理職研修	管理職	新たに管理職に昇格した従業員に対して、管理職として情報管理を推進するため 留意すべき事項を説明する
5	リスク感度研修	管理職	情報セキュリティに関する喫緊の事例・重要事項の共有と注意喚起。管理職として 必要な組織運営や管理業務に係る知識・手法の「再確認」「情報のアップデート



世界にひとつ。あなたにひとつ。