HITACHI
Inspire the Next

ビッグデータビジネスにおける
日立のプライバシー保護の取り組み

― 日立「データ・アナリティクス・マイスターサービス」を例として ―

平成 25 年 5 月 31 日

株式会社　日立製作所　情報・通信システム社
スマート情報システム統括本部

Human Dreams.
Make IT Real.

はじめに

近年のITの進展等に伴い、ビッグデータビジネスが注目を集めており、ビッグデータの蓄積の進展、価値の顕在化に伴って、データマーケットプレイス等の新しいビジネスや組織を跨ったデータの融合も進みつつあります。

株式会社日立製作所 情報・通信システム社 スマート情報システム統括本部では、ビッグデータ利活用の専門家が、事業者のお客さまのビッグデータの利活用をトータルに支援するデータ・アナリティクス・マイスターサービスの提供を開始しています[1]。

一方で、ビッグデータという言葉は、雑誌やテレビ番組において個人情報を利用した行動ターゲティング広告やマーケティングの話題として登場することも多く、知らぬ間に個人のプライバシーが侵害されているのではないかという懸念を指摘する声も根強くあります。実際に、ビッグデータビジネスにおいてプライバシーの侵害が問題化する事例も発生しています。

このような状況に呼応して、EU におけるデータ保護規則案や米国における消費者プライバシー権利章典等、プライバシー保護を強化する動きが世界的に進んでいます。我が国においても経済産業省や総務省が個人に関するデータ（パーソナルデータ[1]）を利活用する際のプライバシー保護について検討を始めています。

これらの背景から、データ・アナリティクス・マイスターサービスにおいては、事業者のお客さまが安全に、かつ安心してパーソナルデータを含むビッグデータを利活用できるよう、プライバシー保護のための様々な取り組みを行っています。

本書では、ビッグデータの利活用を検討されている事業者のお客さまに、データ・アナリティクス・マイスターサービスにおいてプライバシー・バイ・デザイン[2][2]の概念を参考にしながら実施しているプライバシー保護の具体的な取り組みをご紹介します。

[1] 個人に関連するデータの総称であり、個人情報保護法上の個人情報に該当するかどうかを問わないとされています。

[2] システムやビジネスプロセスの設計段階からプライバシー対策を考慮し、企画から保守までのライフサイクル全体で一貫したプライバシー保護を行うという概念であり、プライバシー保護における世界的な標準となりつつあります。

Contents

適用範囲

本書は、ビッグデータの利活用を検討されている事業者のお客さまを対象に、株式会社日立製作所　情報・通信システム社　スマート情報システム統括本部が、データ・アナリティクス・マイスターサービスにおいて実施しているプライバシー保護の取り組みを整理し、説明するものです。

1. ビッグデータとプライバシー

1.1 ビッグデータ化に伴うプライバシーの状況の変化

ビッグデータは、一般的に「大量（Volume）、多様（Variety）、高速（Velocity）」という、いわゆる3V の特性をもつデータ、およびそれらデータを処理する新技術の総称として用いられます。

SNS 等によって個人の情報発信が飛躍的に拡大し、スマートフォン、IC カード型電子マネーなどのデバイスの普及によりデータの収集パターンも多様化したことで、大量かつ多様なビッグデータが蓄積されるようになっています。また、クラウド化と並列分散技術の進展が大量のデータを高速に分析することを可能にしたことで、これら蓄積されたビッグデータを分析し、ビジネスに利活用しようという機運が高まりつつあります。

ビジネスへの利活用が期待される一方で、ビッグデータについてはプライバシー侵害の懸念も根強く指摘されており、実際に、ビッグデータの利活用においてプライバシーを侵害しているとして問題化する事例が発生しています。従来は、個人情報保護法に基づいて個人情報（特定の個人を識別できる情報）を保護していればプライバシーの問題はあまり発生していませんでしたが、ビッグデータのビジネス展開に際して、必ずしも個人情報ではないと考えられる情報からプライバシーの侵害が発生するといった事態も起きています。

表 1-1 プライバシー侵害が問題化した事例（ビッグデータ関連）

事例	概要
AppLog （日本）	・ミログ社が提供していた携帯電話の動画配信アプリ app.tv をインストールすると、AppLog というプログラムにより、当該端末における他アプリのインストール状況、起動状況等が無断で収集されることが発覚しました。 ・これらデータは、必ずしも個人情報保護法上の個人情報とは言い切れないものでしたが、無断収集がプライバシーの侵害であるとして問題視されました。
Netflix （米国）	・米国の DVD レンタル会社 Netflix が、匿名化した 50 万件のレンタル履歴を公開し、レコメンドアルゴリズムの開発コンテストを開催しましたところ、Narayanan らは履歴データと映画レビューサイトのデータを突合した結果、個人が特定できたと発表しました。 ・このように、匿名であったはずのデータから解析によって個人を識別する再特定の危険性についての研究が進められています。
Carrier IQ （米国等）	・2011 年、複数の Android 端末や iPhone に Carrier IQ 社が提供する携帯電話のモニタリングソフトがプリインストールされていることが判明し、利用者に無断で携帯電話の利用状況をモニタリングしている可能性があるとして問題化しました。

出典：IPA「パーソナル情報保護と IT 技術に関する調査」[3]

このような動向を受けて、各国では国民・消費者のプライバシーを保護するため、法規制面の検討が進められています。我が国においては、番号制度の導入に伴い、番号の利用そのものを規制する新しいプライバシー保護制度の検討されました。また、海外においては、EUでデータ保護規則案、米国連邦政府で消費者プライバシー権利章典が提案されるなど、プライバシーの保護を強化する方向性が示されています。

表 1-2 プライバシーの保護に関連して検討されている主な法規制

法規制	概要
行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法）（日本）[4]	・2013 年 5 月、番号法が成立しました。 ・同法では、全国民に個人を識別するための個人番号が付与され、個人番号を含む個人情報（特定個人情報）の適切な取扱いを確保するために特定個人情報保護委員会が設置されることが規定されています。 ・同法では、法律施行後一年を目途に、特定個人情報以外の個人情報についても特定個人情報保護委員会の監視対象に含めることを検討することが示されています。
消費者プライバシー権利章典（米国）[5]	・2012 年、米国ホワイトハウスは消費者プライバシー権利章典を発表しました。 ・同権利章典では、「個人によるコントロール」、「透明性」、「アクセス及び正確性」等、7 つの原則が示され、「個人によるコントロール」では事業者による情報の収集や利用を消費者がコントロールする権利を持つべきであるとされています。 ・同権利章典と併せて、実効力を担保するために米国連邦取引委員会による執行権限が強化されることも謳われています。
データ保護規則案（EU）[6]	・2012 年、欧州委員会はデータ保護規則案を公表しました。 ・同規則案では、個人の権利の強化として、新たに、忘れられる権利、同意を撤回する権利、データポータビリティの権利等が規定されています。 ・また、規則に違反した場合、100 万ユーロあるいは国際的な売上の 2%を上限に罰金が科せられることも盛り込まれています。

1.2 個人情報とプライバシー

ビッグデータビジネスにおいてプライバシーの侵害が問題化した事例を参照すると、個人情報保護法を遵守していれば確実にプライバシー侵害を防ぐことができたというわけではありません。

個人情報は、個人情報保護法第 2 条において「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」と定義されています。

一方で、プライバシーについては、法令上の定義はありません。ただし、判例等を参照すると、「個人に関する情報をみだりに第三者に開示又は公開されない自由」などと解されています。

前述の問題化事例のうち、AppLog が収集していたデータは、パーソナルデータではありますが、必ずしも個人情報保護法上の個人情報に該当するわけではないと考えられ、データの収集方法や取扱い方法がプライバシーを侵害しているとされた例と言えます。

個人情報とプライバシーに関する情報は重複している部分もありますが、必ずしも両者は一致しておらず、ビッグデータビジネスを安全・安心に推進するためには、個人情報保護に加えて、プライバシー保護に配慮することが不可欠です。

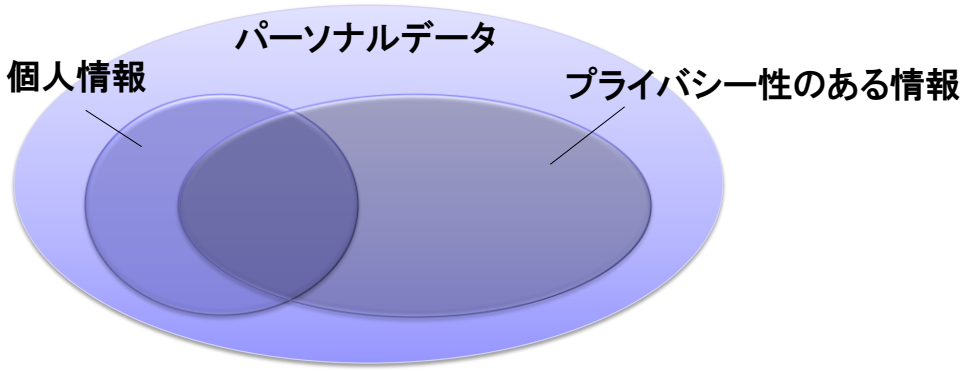
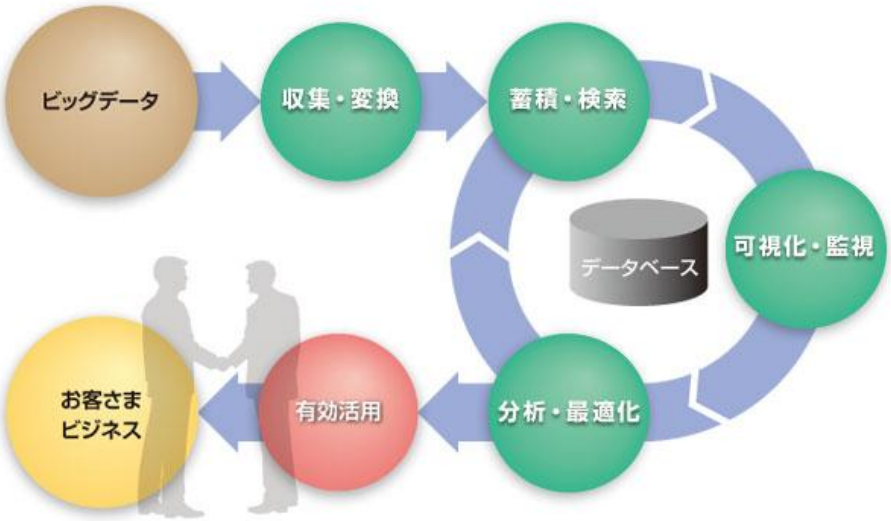


図 1-1 パーソナルデータ、個人情報、プライバシーに関する情報の関係性

1.3 ビッグデータ特有のプライバシーリスク

ビッグデータの利活用には、ライフサイクルがあると考えられます。まずビッグデータを効率的に収集し、その多様で莫大なデータを統一的に蓄積・管理し、その中からビジネスにとって価値のあるデータを抽出し、分析・シミュレーションにより、ビッグデータに適用できるよう情報化を行い、その結果を実ビジネスで有効活用します。



出典：株式会社日立製作所「日立のビッグデータ利活用プラットフォーム」[7]

図 1-2 ビッグデータ利活用のライフサイクル

このライフサイクルを、データ・アナリティクス・マイスターサービスにおいてビッグデータを取扱う場合に適用すると、ビッグデータの利活用プロセスを以下のような 4 つに分けることができます。

① ビッグデータの取得・変換（お客さまにて収集されたビッグデータを預かり、必要に応じてデータを変換する）
② ビッグデータの蓄積（取得・変換したデータを蓄積する）
③ ビッグデータの分析・活用（データを分析してお客さまのビジネスにとって価値のある知見を抽出し、その結果のビジネス活用を支援する）
④ ビッグデータの廃棄・返却（利用が終了したデータは廃棄または返却する）。

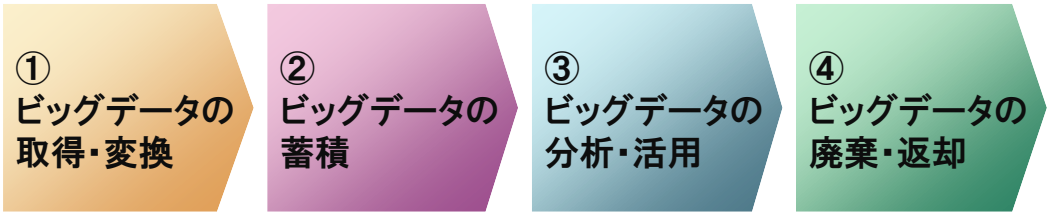


図 1-3 本書で想定するビッグデータの利活用プロセス

各プロセスには、ビッグデータならではの特徴があり、特有のプライバシーリスクが存在します。

例えば、「①ビッグデータの取得・変換」では、特徴として、取得するデータの中に様々なパーソナルデータが含まれる可能性があります。この場合、パーソナルデータの主体である個人が実態を理解していないままお客さまとデータをやり取りすることは、プライバシーの侵害ととらえられるリスクがあります。

また、「③ビッグデータの分析・活用」では、パーソナルデータを含む大量のデータが分析対象となるという特徴があります。この場合、高度な分析技術を駆使すれば個人を高精度に推定できてしまう可能性があり、このような精度の高い推定結果をビジネスに活用することでプライバシーを侵害するリスクがあります。

パーソナルデータの主体である個人のプライバシーを保護し、安全・安心なビッグデータ利活用を推進するためには、このようなビッグデータ特有のプライバシーリスクを把握し、適切にプライバシー保護のための施策を講じていくことが非常に重要になります。

1.4 プライバシー・バイ・デザイン

このようなプライバシーリスクに対し、近年、組織におけるプライバシー保護検討のための基礎的概念としてプライバシー・バイ・デザインが注目されています。

プライバシー・バイ・デザインは、カナダオンタリオ州のプライバシーコミッショナーであるアン・カブキアン博士によって提唱されたものであり、「システムやビジネスプロセスの設計段階からプライバシー対策を考慮し、企画から保守までのライフサイクル全体で一貫したプライバシー保護を行う」という考え方です。

プライバシー・バイ・デザインでは、以下の 7 原則が提案されています。

表 1-3 プライバシー・バイ・デザインの 7 原則

No	原則
1	事後的ではなく事前的：プライバシー侵害の救済策を考えるのではなく予防策を考える。
2	デフォルト設定：デフォルト状態のシステムやビジネスプロセスでプライバシーが保護される。
3	設計に組み込まれるプライバシー：設計段階からシステムやビジネスプロセスにプライバシー対策が組み込まれる。
4	ゼロサムではなくポジティブサム：セキュリティ対策等とプライバシー保護はトレードオフではなく、Win-Win の関係である。
5	最初から最後まで：データのライフサイクル全体でプライバシーが保護される。
6	可視性と透明性：プライバシー対策は全てのステークホルダーから可視的、透明である。
7	利用者のプライバシー尊重：システムやビジネスプロセスの設計者、管理者は、利用者のプライバシーを最大限に尊重する。

出典：Information & Privacy Commissioner, Ontario, Canada「7 Foundational Principles」[8]

プライバシー・バイ・デザインは、EU のデータ保護規則案や総務省が取りまとめたスマートフォン・プライバシー・イニシアティブ[9]等、各国の政策検討の際に参照されているとともに、実際に大規模なパーソナルデータを扱う企業においても考え方として採用されるなど、プライバシー保護施策の世界的な標準となりつつあります。

個人のプライバシーを尊重し、プライバシーの侵害を予防するという概念は、パーソナルデータを利活用する際に重要であり、ビッグデータの利活用支援事業の展開にあたって、プライバシー・バイ・デザインの概念を参考にします。

2. 日立のプライバシー保護の取り組み

2.1 プライバシー保護に対する基本的な考え方

パーソナルデータには、個人情報保護法が定義する個人情報だけでなく、個人に関する様々な情報が含まれます。そこで、パーソナルデータの安全・安心な活用を図るため、従来の個人情報保護対策に加えてプライバシー保護のための対策を行います。

個人情報を含むデータを取扱う場合、まずは、個人情報保護法を遵守することが必須です。株式会社日立製作所はプライバシーマークを取得しておりますので、JISQ15001 に則って構築している個人情報保護マネジメントシステムに従ってデータを取扱います[10]。さらに、これらの個人情報保護対策に加え、ビッグデータビジネスにおけるプライバシー保護を堅固なものとするため、プライバシー・バイ・デザインの概念に基づくプライバシー保護のための対策を行います。

また、個人情報は含まれなかったとしても、パーソナルデータを取扱う場合には、プライバシー・バイ・デザインの考え方、それに基づくプライバシー保護のための対策を徹底し、データの安全・安心な活用に努めます。

2.2 プライバシー・ガバナンス

プライバシー保護に対するガバナンスの確立のため、プライバシー保護のための組織・体制を構築するとともに、ビッグデータビジネスにおけるプライバシー保護方針を定め、社員に遵守させます。また、このようなプライバシー保護の取り組みについて、お客さまに情報を公開するとともに、継続的な改善に努めます。

データ・アナリティクス・マイスターサービスでの取り組み

- **プライバシー保護責任者**：株式会社日立製作所 情報・通信システム社 スマート情報システム統括本部では、プライバシー保護責任者を選任しています。プライバシー保護責任者は、プライバシー保護に関連した活動全体を統括し、次のような職務を担っています。
  - ✓ 各種プライバシー保護施策の決定
  - ✓ プライバシー保護方針の制改定
  - ✓ 社員におけるプライバシー保護施策の遵守徹底
  - ✓ プライバシー保護施策の実施状況の監査
  - ✓ 社員へのプライバシー保護教育
- **プライバシー保護方針**：プライバシー保護責任者の監督のもと、ビッグデータビジネスにおけるプライバシー保護方針をまとめています。以下に、プライバシー保護方針を記載します。

ビッグデータビジネスにおけるプライバシー保護方針

1. プライバシー・バイ・デザインの概念に則り、個人のプライバシーを尊重し、プライバシーの侵害の予防に努めます。
2. お預かりするデータのプライバシーリスクを把握し、データを適切に取扱います。
3. お預かりするデータについて利用目的を明確にします。
4. 目的の達成に必要なデータのみを取得します。
5. プライバシーリスクを軽減するために必要な場合には、データの匿名化やあいまい化といった加工を行います。
6. 個人からの同意なく個人を特定する分析、プライバシーを侵害する分析を行いません。
7. お預かりするデータの正確性を確保します。
8. お預かりするデータの機密性を確保します。
9. データの二次提供またはデータの分析結果の公表等を行う場合、お客さまと事前合意した範囲内でのみ行います。
10. お客さまに対して個人からデータに関する問い合わせ等があった場合、当該案件におけるデータの取扱いについての情報を提供するなど、お客さまが行う問い合わせ対応を支援します。

- **運用**:プライバシー保護方針をはじめとするプライバシー保護に関する各種施策、各種決定は、プライバシー保護責任者の責任のもと、ビッグデータビジネスに携わる社員に周知、徹底されます。社員は、各々がプライバシー保護方針を遵守するように心がけるとともに、プライバシー保護責任者は、適切にプライバシー保護に各種施策が実施されていることを定期的にチェックし、運用の改善に努めます。

2.3 プライバシー影響評価

プライバシー影響評価（Privacy Impact Assessment、以下 PIA）は、「パーソナルデータを取扱うシステム、事業、サービス等において、プライバシーへの影響を事前に評価し、プライバシーの侵害を防ぐために運用面、技術面での対策を講じる一連のプロセス」と考えられ、諸外国では、パーソナルデータを取扱う組織に PIA の実施を義務付けている国もあります。

我が国では、番号法で行政機関に対し特定個人情報を扱うにあたって特定個人情報保護評価を行うことが義務付けられました。一方で、民間事業者が PIA を実施する根拠となる法令等はありませんが、ビッグデータビジネスにおけるプライバシー保護のための自主的取り組みとして PIA の実施に努めています。

データ・アナリティクス・マイスターサービスでの取り組み

- **PIA の期待効果**：ビッグデータを取扱う案件の開始に先立って PIA を実施し、適切な改善策を行っていくことで、円滑なビジネスの遂行とプライバシー保護が両立できると考えられます。特に以下の効果が期待されます。
  - ✓ プライバシー侵害の防止
  - ✓ プライバシー侵害の嫌疑等からのお客さまの保護
  - ✓ PIA の評価結果をお客さまに報告する等、プロセスの透明性確保
  - ✓ プライバシー保護のための事後的なサービス変更、システム改修等の防止
- **PIA の内容**：PIA の実施にあたっては、諸外国の PIA 制度において設定されている評価項目をベースに、ビッグデータ特有のプライバシーリスクを評価するための項目や、昨今問題化したプライバシー侵害に関する事例を参照してチェックが望ましい項目等を追加することで、独自のチェックリストを作成しています。以下に、チェックリストの一部を抜粋して示します。

プライバシー影響評価チェックリスト（抜粋）

1. **全般**（プライバシー保護体制等について確認する）
   - ✓ 案件においてプライバシー保護対策の実施責任者が決まっているか。 等
2. **データ**（データの内容や出所等が適切であることを確認する）
   - ✓ 取得するデータは、いつ、誰が、どのように収集したものか確認しているか。 等
3. **目的**（データの利用目的が特定され、適切であることを確認する）
   - ✓ データの利用目的を特定しているか。
   - ✓ データの利用目的についてお客さまと合意しているか。 等
4. **取得**（データを適切に取得し、必要以上のデータを取得しないことを確認する）
   - ✓ 取得するデータは、お客さまと合意した利用目的の達成に必要とされる内容と量に限定しているか。 等

5. **利用**（データの利用は目的の範囲内で、プライバシーを侵害しないことを確認する）
   - ✓ 個人を特定するための分析を行わないか。
   - ✓ 個人のセンシティブな属性を推定する分析を行わないか。 等

6. **正確性**（データの保管や更新にあたって正確性が維持されることを確認する）
   - ✓ データを更新する場合に、その記録を残すようにしているか。 等

7. **安全管理**（データの取扱者を限定し、セキュリティ対策を行うことを確認する）
   - ✓ データを取扱う者は限定されているか。
   - ✓ データを取扱うシステムは、不正アクセスを防止できるようになっているか。 等

8. **二次提供、分析結果の公表**（データを二次提供等する場合の留意事項を確認する）
   - ✓ データを二次提供する場合、お客さまとの合意があるか。
   - ✓ データを二次提供する場合、提供先におけるデータの利用を契約等で制限するようにしているか。 等

9. **問い合わせ等対応**（問題発生時の対応手順を確認する）
   - ✓ プライバシーの観点から発生しうる問題を想定し、対応手順を定めているか。 等

10. **廃棄・返却**（データの廃棄方法または返却方法について確認する）
    - ✓ データの廃棄方法または返却方法を定め、お客さまと合意しているか。 等

- **PIA の運用**：パーソナルデータを取扱う案件の開始に先立って、各案件の責任者がチェックリストに基づいて案件におけるプライバシーリスクを評価します。

  評価の結果、プライバシーリスクがあると判断された場合には、適切な改善策を講じ、改めてチェックリストによる評価を行ってリスクが十分に下がっていることを確認します。

  その後、プライバシー保護責任者が評価結果に基づきプライバシーリスクが十分に下がっていることを確認、承認した後、初めて当該案件を開始することが可能になります。

2.4 各プロセスにおけるプライバシー保護

1.3 にて前述したように、ビッグデータの利活用プロセスは、「①ビッグデータの取得・変換」、「②ビッグデータの蓄積」、「③ビッグデータの分析・活用」、「④ビッグデータの廃棄・返却」というプロセスに分けることができます。

このような各プロセスにおいては、ビッグデータを取扱うことによる特有のプライバシーリスクが発生します。そこで、各プロセスにおいて、プライバシーリスクを踏まえた適切なプライバシー保護対策を行います。

データ・アナリティクス・マイスターサービスでの取り組み

- **各プロセスにおけるプライバシー保護対策**：前述のプライバシー保護方針を詳細化し、各プロセスにおける具体的なプライバシー保護対策を定め、それらの対策が適切に実施されるよう努めています。以下に、具体的なプライバシー保護対策の一部を抜粋します。

各プロセスにおける具体的なプライバシー保護対策（抜粋）

① ビッグデータの取得・変換
- ✓ お客さまのデータを取得する場合、お客さまがいつ、どこで、どのように収集したデータなのかを確認し、データの取得が適切であるかどうかを確認すること
- ✓ お客さまからデータを取得するにあたり、取得日、取得方法等を記録すること
- ✓ あらかじめデータの利用目的を特定してお客さまと合意し、利用目的の達成に必要以上のデータは取得しないこと
- ✓ 個人情報やプライバシーに関する情報が、必ずしも利用目的の達成に必要ない場合、匿名化や仮名化等の加工を行ってデータを保管すること　等

② ビッグデータの蓄積
- ✓ データを保管するにあたり、取扱者を限定し、システムでアクセス制御をかけること
- ✓ データに対する処理（更新、削除、複製等）を行うにあたり、記録を残すこと　等

③ ビッグデータの分析・活用
- ✓ 分析を行うにあたり、分析担当者を限定すること
- ✓ 分析を行うにあたり、あらかじめ特定した利用目的の範囲を超えないこと
- ✓ 個人を特定する目的での分析は行わないこと　等

④ ビッグデータの廃棄・返却
- ✓ データの取得時にデータ提供者とデータの保管期間、廃棄方法について合意しておき、それを遵守すること　等

2.5 プライバシー保護のための技術的対策

日立グループでは、種々のセキュリティ関連技術、プライバシー強化技術（Privacy Enhancing Technology、以下 PET）[3]の開発を行っており、お客さまからのご要望や取扱うデータの実態に応じてこれらの技術を活用することで、パーソナルデータの利活用とプライバシーの保護のより最適なバランスを実現します。

パーソナルデータを含んだビッグデータを預かるにあたり、お客さまのプライバシー保護ニーズに応えるためには、以下のような要件を満たすことが必要と考えられます。

- データの漏えいを防止すること
- データを分析・利用する過程でプライバシーの侵害が起きないようにすること
- お客さまへの透明性を確保すること

このような要件を満たすため、各種セキュリティ対策を施したデータ分析環境で、データを管理・分析します。また、日立グループが有する PET についても適宜、適用します。

データ・アナリティクス・マイスターサービスでの取り組み

- **シンクライアント**：データ分析環境をシンクライアントで構築し、パーソナルデータを含むビッグデータを当該環境で管理します。なお、当該環境は、クラウド型サービスである「SecureOnline」[11]上で構築し、以下に示すような特長を有しています。
  - データの一元管理：このようなデータ分析環境を利用することで、データはデータセンタで安全に一元管理されるようになります。
  - ローカル端末のデータレス：分析を行うにあたって、担当者はデータセンタにリモートログインし、データセンタ上でデータを取扱います。このとき、分析担当者によるローカル端末へのデータ保存を禁止することができます。
- **アクセス制御**：データ分析環境においては、厳重なアクセス制御を行っています。
  - 二重の認証：ID／パスワードに加え、ワンタイムパスワードによる二重認証を行います。
  - ログ取得：データ分析環境に対するアクセスについて、自動的にログを取得します。
- **データ移送時のセキュリティ**：分析のためにお客さまからデータを移送する場合においてもセキュリティ対策を行います。
  - データ移送時のセキュリティ対策：お客様の環境からデータを抽出する端末において情報漏洩防止ソリューション「秘文」[12]を導入し、安全に暗号化した状態で移送するようにしています。
- **PET の適用**：前述のセキュリティ対策に加え、パーソナルデータを利用する際のプライバシー侵害のリスクを低減するため、適宜、匿名化技術等の PET を適用します。

---

[3] プライバシー保護の向上を目的として利用される暗号化、匿名化等の技術の総称とされています。

匿名化技術の例として、データに氏名や住所など、個人を識別できる情報が含まれている場合に、個人を識別できる情報とその他属性情報を切り離し、属性情報に代替 ID を振ることで個人の識別を防止するものが挙げられます。

また、個人を識別できる情報を切り離したとしても、属性情報の値の組み合わせが一意になるデータがある場合などは、個人が特定されてしまうリスクが残ってしまいます。株式会社日立製作所では、このようなデータに対し、属性値のあいまい化等を行うことで個人の特定を困難にする高度な匿名化技術（k-匿名化技術）を開発しています[13]。

2.6 プライバシー保護教育

適切なプライバシー保護とビッグデータの利活用の両立を図るためには、プライバシー保護方針を定めたり、プライバシー保護技術を活用するだけではなく、社員がプライバシーについて正しく理解し、各々がプライバシーの保護を心がけることが非常に重要です。

そこで、社員に対するプライバシー保護教育を継続的に行い、意識の普及啓発に努めます。

データ・アナリティクス・マイスターサービスでの取り組み

- **個人情報保護に関する教育**：株式会社日立製作所では、個人情報保護マネジメントシステムを構築しており、個人情報保護に関する社内教育が義務化され、社員全員が個人情報保護について学習し、理解を深めています。
- **プライバシー保護に関する教育**：社員がビッグデータビジネスに携わる際にプライバシーの観点から配慮するべき内容をまとめたテキスト（「ビッグデータビジネスにおけるプライバシー保護のための手引き」）を作成しており、ビッグデータビジネスに携わる社員はプライバシー保護について学習し、理解を深めています。
- **情報共有・啓発**：ビッグデータを取扱う他の部署やグループ会社を含めて、プライバシーに関する定例の勉強会、検討会を開催しています。プライバシーに関するビジネス動向、制度動向等について情報共有を行うとともに、プライバシーを保護するための対策等について検討を行っています。

おわりに

本書は、データ・アナリティクス・マイスターサービスを提供するにあたって、プライバシー保護の世界的な標準となりつつあるプライバシー・バイ・デザインの概念を参考にして、株式会社日立製作所 情報・通信システム社 スマート情報システム統括本部が行っている取り組みをまとめたものです。

プライバシーの保護においては、法制度、ビジネス、技術とも、まさに現在、世界的な検討が行われている状況にあります。株式会社日立製作所 情報・通信システム社 スマート情報システム統括本部では、お客さまに安心して利用いただけるサービスの実現をめざし、今後も、国内外の法制度、技術の変化の把握に努め、適時、サービスに反映していきたいと考えています。

また、今後、このようなプライバシー保護の取り組みを、ビッグデータビジネスに携わる各事業部や日立グループ各社に展開していくことについても検討したいと考えています。

参考文献等

[1] 株式会社日立製作所：データ・アナリティクス・マイスターサービス（2012 年 6 月）
http://www.hitachi.co.jp/products/it/bigdata/approach/service.html
[2] Ann Cavoukian：Privacy by Design … Take the Challenge（2009 年 1 月）
http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf
[3] IPA：パーソナル情報保護と IT 技術に関する調査（2012 年 8 月）
http://www.ipa.go.jp/security/fy23/reports/pdata/documents/pdata_report.pdf
[4] 参議院：行政手続における特定の個人を識別するための番号の利用等に関する法律案（番号法案）（2013 年 5 月）
http://www.sangiin.go.jp/japanese/joho1/kousei/gian/183/meisai/m18303183003.htm
[5] THE WHITE HOUSE：CONSUMER DATA PRIVACY IN A NETWORKED WORLD（2012 年 2 月）
http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[6] EUROPEAN COMMISSION：Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)（2012 年 1 月）
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[7] 株式会社日立製作所：日立のビッグデータ利活用プラットフォーム（2012 年 7 月）
http://www.hitachi.co.jp/products/it/bigdata/platform/
[8] Information & Privacy Commissioner, Ontario, Canada：. 7 Foundational Principles（2009 年）
http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
[9] 総務省：スマートフォン プライバシー イニシアティブ －利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－（2012 年 8 月）
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
[10] 株式会社日立製作所：情報セキュリティ報告書（2012 年 6 月）
http://www.hitachi.co.jp/csr/csr_images/securityreport.pdf
[11] 株式会社日立ソリューションズ：SecureOnline
http://www.hitachi-solutions.co.jp/so/
[12] 株式会社日立ソリューションズ：情報漏洩防止ソリューション秘文
http://www.hitachi-solutions.co.jp/hibun/sp/
[13] 藤井康広・佐藤尚宜・吉野雅之・原田邦彦：クラウドコンピューティング・ビッグデータ利活用を支える先進セキュリティ技術（日立評論 2012 年 10 月号）（2012 年 10 月）
http://www.hitachihyoron.com/2012/10/pdf/10a09.pdf

本書について

- 本書は、株式会社日立製作所 情報・通信システム社 スマート情報システム統括本部が提供するデータ・アナリティクス・マイスターサービスの 2013 年 5 月現在のサービス内容に基づきまとめたものです。
- 本書に記載されている情報は、今後、予告なく変更されることがあります。

ビッグデータビジネスにおける日立のプライバシー保護の取り組み
― 日立「データ・アナリティクス・マイスターサービス」を例として ―

2013 年 5 月 31 日　　初版発行

著者　　株式会社日立製作所　情報・通信システム社 スマート情報システム統括本部
　　株式会社日立コンサルティング
編集・　株式会社日立製作所　情報・通信システム社 スマート情報システム統括本部
発行　　〒140-8572 東京都品川区南大井六丁目 27 番 18 号 日立大森第二別館