世界各国の個人情報保護制度の調査及び解決方法の提案

リスク工学グループ演習２班
太田諭　崔 子歆　QIN QIWEN 田口 渉
アドバイザー教員：西出 隆志

1. 研究背景

近年，モバイルインターネット，ビッグデータ，クラウドコンピューティング，人工知能などの新世代の情報技術の急速な発展に伴い，ネットワークとデータを取り巻くサービスとアプリケーションが爆発的に増加し，ますます多くのアプリケーションシナリオが公開されている．コンピュータを用いた通信技術の発達とともに，情報の重要性が高まり，攻撃技術が発達している．サイバーセキュリティのリスクと問題，及び近年の頻繁なランサムウェア攻撃，国境を超えた通信詐欺，データ侵害，サイバー攻撃など，世界規模で個人情報保護の分野に大きな影響を及ぼしている．

個人情報は，社会が各個人を理解または識別し，活動を実行するための基盤である．ただし，個人情報の不適切な使用は，個人の権利を侵害し，人々の尊厳と自由を危険に晒す．さらには個人及び財産の安全上のリスクをもたらす可能性がある．したがって，個人情報の保護は個人情報の使用の前提条件であり，ビッグデータの時代において，ますます重要な問題となっており，それに伴い個人情報を取り扱うＩＴ 企業が法律違反となるリスクが増加している．

2. 研究目的

本研究では，諸外国で個人データ保護に関する法律の制定が増加していることに着目し，その法律ごとにどのような特性があるのか，調査・分類を行うことで，ＩＴ企業が諸外国でビジネスを行う際に，プライバシー保護に関する法律に対してどのように行動すべきか考察を行い，提案することを本研究の目的とする．

3. インターネット上での個人情報の侵害

3.1 個人情報が侵害されやすい理由

電子ネットワークはオープンスペースであり，それを境界のない「第七大陸」と呼ぶこともある．電子ネットワークによって，人々は情報に自由にアクセスできる．

デジタル技術とインターネットにより，デジタル情報をコピーして瞬時に世界中のあらゆる場所に送信することができ，個人のプライバシーが転送されると，地理的な制限なしにタイムリーにダウンロードすることが可能である．情報を広めるためのより単純な方法は，情報所有者に多くのリスクをもたらす．

また，インターネット上の多数の消費者の個人情報は，ネットワーク経済の時代に企業間の競争のための戦略的無形資源となり，これが多数のオンライン個人情報の侵害を引き起こす可能性がある．

3.2 個人情報を侵害する主な方法

3.2.1 個人の侵害

インターネット上での侵害は，個人的な形式が最も一般的であり，その形式は多様である．主な特徴としては，個人がインターネット上で他人の個人情報を不正に宣伝，開示，または譲ることが挙げられる．

海外では個人のプライバシーが侵害されているという事例がある．1996 年 1 月，フランスのミッテラン大統領に解任された私立の医者が，ミッテランの健康記録を公開したドキュメンタリー本「最高の秘密」を発表した．その本はミッテランド大統領のプライバシーを侵害し，医師の職業倫理も侵害したため，パリの裁判所はその本の出版を禁止した．しかし，この本の全文を電子ファイルの形でインターネットに公開している人々がいるため，それが誰でも読むことができる「開かれた秘密」となった．

3.2.2 ハッカーの侵害

ハッカーとは，コンピュータ情報システムへの不正アクセスを行うものと定義され，通信ソフトウェアを使用して違法なネットワークを通じて公衆またはそのコンピュータ上の情報を傍受または改ざんし，情報システムのセキュリティを危険に晒す．

ハッカーの攻撃は他の人々のコミュニケーションのセキュリティを危険に晒す可能性があり，ハッキングソフトウェアは暗号化されていない e-メールを容易に入手し，e-メールの内容を改ざんする可能性がある．ハッカーによる攻撃は，個人情報のセキュリティを侵害する可能性があり，一部の Web サイトでは不完全なセキュリティ対策やコンピュータプログラムの抜け穴があり，クレジットカードの口座の機密情報，投資有価証券情報などの情報を妨害されずに盗取できる．

3.2.3 Web サイト運営者による侵害

Web サイト運営者によるプライバシーの侵害には，主に Cookie が用いられる．Cookie は Web ユーザが閲覧したサイトや商品を記録することができる追跡技術である．

そのため，多くの Web サイト運営者は，Cookie を用いてユーザを違法に監視し，情報を収集することでビジネス目的を達成する大規模な個人データベースを構築している．

3.2.4 ソフトウェア及びハードウェアの提供者による侵害

一部のソフトウェア及びハードウェアの提供者は，製造する機器のシリアル番号を無差別に識別し，個人情報を収集する．有名な事例として，1999 年に Intel が販売した商品に識別可能なシリアル番号を付け加えたことが挙げられる．この時，反対者はシリアル番号の本質は Cookie であると述べた．

4. 世界のプライバシー保護法律の現状

世界中の国々でのプライバシー保護の法律は，基本的に直接保護と関節保護の 2 種類に分けられている．

4.1 直接保護

この種の保護は，米国で発生したもので，プライバシー権の侵害を独立した権利の侵害として直接認識し，加害者が負担する．このようにして，被害者のプライバシーの損

失が補償される．

米国では，プライバシーを保護する法律は，1967 年の情報自由法と 1974 年のプライバシー法の 2 つに基づいている．プライバシー法は，連邦政府が情報を扱う際の様々なことや機密性に関する詳細な規則を定めている．

プライバシーに関する法律は，多くの国際法がある．カナダ，スウェーデン，ドイツ，フランス，ノルウェー，デンマーク，オーストリアなどの国では，個人情報の取り扱いに関する法律が多くある．例えば，カナダ人権法，スウェーデンデータ法などがある．

4.2 間接保護

このような保護方式は，プライバシー権は独立した人格権とはみなされず，プライバシー権を含む事件は他の侵害に別々に含まれ，法律的な保護を求めることができる．もし侵害を訴える場合，プライバシーに対する独立した訴訟はない．

中国のプライバシー保護方式は間接保護となっている．例えば，民法では，市民の名前，肖像，評判，名誉に対する権利を侵害した場合の民事責任はそれぞれ第９９条，第１００条，第１０１条，第１０２条に規定されている．

5. 各地域の法律及び条例

ここでは，世界各地の個人情報保護制度に関する法律，及び条例について調査した結果を示す．調査対象とした地域はヨーロッパ（EU），中国，ブラジル，アメリカ（カリフォルニア州），ロシア，オーストラリア，の 6 つである．各地域の調査結果を項目ごとにまとめた表を，それぞれ表１から表６に示す．

表１：ヨーロッパ（EU）

国	EU, GDPR
制定,施行日	2018/5/25施行
責任主体	EEA内在住のユーザーを対象にしている企業
概要	加盟国が国ごとに整備していた個人情報保護法を加盟国全てで統一 個人の情報のコントロール権を個人に戻すことを目的とする EUが認めていない国への情報移転を認めない
提訴権利者	加盟国の国民
権利	アクセス権, 訂正権, 削除権等
罰則	初回かつ意図的でない場合書面での警告 2000万ユーロもしくは前会計期間の売上の4%, どちらか高い方

表２：中国

国	中国, 中華人民共和国サイバーセキュリティ法
制定,施行日	2017/6/1 施行
責任主体	中国国内のネットワーク事業者
概要	インターネットで業務を行う個人, 組織の素性を明確化 回線の提供、ドメイン登録等を行う場合、事業者は個人確認をしなければならない 真実の身分情報を公開しない場合サービスを提供できない
提訴権利者	中国政府
権利	本人確認の義務化, 虚偽申告を受領した際企業にも責任があると明示 中国国内の情報インフラを攻撃する組織、個人に対する処罰の明確化
罰則	罰金, 業務改善要求
特記事項	個人情報の使用に関する責任が明確化されていない
罰則適用事例	2017/9 阿里雲計算有限公司が真実の身分証明書未提示のユーザにネット接続サービスを提供 即時改善と登録情報の真実性確認を要請

表３：ブラジル

国	ブラジル, Lei Geral de Proteção de Dados
制定,施行日	2018年8月 成立
責任主体	ブラジル国内でデータ処理を行う組織
概要	「機微データ」というカテゴリを作り それらを本人の明示的な同意なしの商用利用を禁止 収集した情報の国外持ち出しは政府が認めた場合のみ可能
提訴権利者	ブラジル国民
権利	収集した情報に関して本人がアクセスできるようにする
罰則	データベースの破棄 罰金5000万レアル(約14億5000万円), もしくは年間売上高の2%の低い方
特記事項	機微データ：人種, 思想, 宗教観, 健康状態 EUのGDPRを参考にしている

表４：アメリカ（カリフォルニア州）

国	アメリカ, CCPA
制定,施行日	2020/7施行予定
責任主体	カリフォルニア州居住者の個人情報を取得する者
概要	取得・利用する情報に関するプライバシーポリシーを公開 オプトアウト権行使のためのページの作成を義務化
提訴権利者	州の住民
権利	個人情報に関する被害を受けた場合 厳格な証明なしに救済を求めることができる
罰則	一件あたり最高7,500ドルの罰金
特記事項	適用対象者の所在地を限定しないため州外にも適用されるリスク
罰則適用事例	なし

表５：ロシア

国	ロシア, No242-FZ
制定,施行日	2015/9/1施行
責任主体	ロシア国内向けのウェブサイトを通じて ロシア国民の個人情報を収集するウェブサイト
概要	ロシア国民の個人情報を扱う会社は 原則ロシア国内に置かれたデータベースを使用する
提訴権利者	ロシア政府
権利	違反者への訴訟を起こすことができる
罰則	ブラックリストへの登録, 罰金 ブラックリストに登録されたwebサイトは ロシア国内からのアクセスを遮断される
特記事項	十分に個人情報を保護できていると判断した国には持ち出し可能 それ以外の国へは権利者が同意している場合可能
罰則適用事例	2016/10 アメリカLinkedInに対し データ保護庁がロシア国内からの接続を遮断

表６：オーストラリア

国	オーストラリア, Assistance and Access Bill 2018
制定,施行日	2018/12 可決
責任主体	オーストラリア国内のIT企業
概要	政府に製品へのバックドア設置を要求された場合 従わなければならない
提訴権利者	オーストラリア政府
権利	バックドア設置を強要
罰則	最高1,000万AUD(約7億7600万円)の罰金
特記事項	IT企業の製品はグローバル展開されるため 世界全体でセキュリティリスクが高まる恐れ
罰則適用事例	なし

6. 各地域の法律の比較

ここでは，5. の各地域の法律及び条例に基づいて比較をし，各地域の法律の相違点を表７に示す．アメリカ，ロシア，オーストラリア，中国，ＥＵ，ブラジルの６つの地域は，法律のタイプや対象，活動拠点によって，３つのグループに分けられる．

表７：各地域の比較

国	アメリカ	ロシア	オーストラリア
主体	国民	政府	政府
目的	国民の情報保護	国民の情報保護	治安維持
IT 企業限定か	限定しない	限定する	限定する
対象の活動拠点	国内外問わず	国外	国内
罰金以外の罰則	なし	あり	なし

国	中国	EU	ブラジル
主体	政府	国民	国民
目的	治安維持	国民の情報保護	国民の情報保護
IT 企業限定か	限定する	限定しない	限定する
対象の活動拠点	国内	国内外問わず	国内
罰金以外の罰則	あり	なし↓ (罰金もない場合がある)	あり

6.1 グループ１：アメリカ，ＥＵ

a. 活動拠点は国内外問わない
b. 対象がＩＴ企業に限らない
c. 国民の個人情報を不当に得ようとする組織への牽制目的であると考えられる
d. 国民情報保護タイプ

6.2 グループ２：オーストラリア，中国

a. 活動拠点は国内限定である
b. 対象がＩＴ組織に限る
c. 個人情報に対しての規制が目的ではなく，国に対して不利益になる行為を規制しようとしていると考えられる
d. 不利益規制タイプ

6.3 グループ３：ロシア，ブラジル

活動拠点，対象，目的，タイプがグループ

１とグループ２の中間である．

7. 考察

ここでは分類に対して企業が取るべき対策を考察する．

7.1 国民の個人情報を保護するタイプ

a. 情報流通の規制よりも，個人の情報は持ち主が操作できるようにすることを目的としている
b. 正当な手続きをすれば情報の持ち出しは可能である
c. 各国の規約を理解し手続きを行い，必要に応じて取り扱いに関する警告を表示すればこれまで通りの業務を行うことは可能である
d. サイトの規約，取り扱い指針，警告の整備を行えば比較的安価に業務継続は可能である

7.2 国に対する不利益を牽制するタイプ

個人情報保護よりも，国外への情報流出を止めることを目的としており，データベースなどを国内に設置する必要があるため資金や人員が必要になる．

a. 個人情報保護タイプよりも目的にばらつきがあり共通の対策を立てるのは難しい
b. 場合によっては対象国へのサービスを止めるのも選択肢に入る．例えば，オーストラリアに拠点を置くのはあまり望ましくないと言える．
c. 国への申請や設備の増設などが必要になり，業務継続にはコストがかかるため，場合によってはサービス停止も視野に入れたほうが良い可能性がある

8. 今後の課題

本調査では，グローバルＩＴ企業が海外に拠点を置く際にとるべき対応について考察し，まとめた．しかし，法律について不透明な部分が多くあり，考察の妥当性の確認が取れておらず，実際に提案した対応をとるだけで問題が解決するという確実な根拠が今のところない．したがって，今回の提案した対応が妥当であるのか日本企業へのヒアリングなどを通じてより詳しく調べていことが今後の更なる課題である．

参考文献

[1]IIJ.news vol. 150, https://www.iij.ad.jp/news/iijnews/2019/pdf/vol150.pdf, IIJ
[2] Financial and Social System of Information Security https://blog.goo.ne.jp/hosiei/e/fc1bfaf0921b6d3d06c0f45e73a273c2
[3] Client Alert ロシアにおける個人情報保護の強化 http://www.bakermckenzie.co.jp/material/dl/practice/intellectualproperty/ClientAlert_201410_IP_IT_EC_Personal_Data_in_Russia_J.pdf
[4] Brazil’s New General Data Privacy Law Follows GDPR Provisions, Melanie Ramey, CROSS-BORDER TRANSFERS, DATA PRIVACY, INTERNATIONAL
[5] EU 各国における個人情報保護制度に関する調査研究報告書，株式会社 IT リサーチ・アート
[6] 個人情報保護をめぐる国内外の動向（法の域外適用の在り方及び国際的制度調和への取り組みと越境移転の在り方関係）

https://www.ppc.go.jp/files/pdf/190304_shiryou1.pdf, 個人情報保護委員会
[7] データ越境移転に関するルールの動向 –対応を迫られる GDPR
https://japan.zdnet.com/article/35107016/, ZDNet Japan