別紙1

利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会

第二次提言(案)

平成２２年４月

はじめに

インターネットや携帯電話は急速に普及し、日常生活や経済活動に不可欠な社会基盤となっている。最近では、クラウドコンピューティング化や、携帯端末の高度化が進展し、欧米諸国や我が国においては、新たな ICT サービスが次々と登場している。しかしながら、新たに登場した ICT サービスが、通信の秘密、個人情報保護、プライバシー、知的財産保護等との関係において不分明な状況が生じ、利用者の不安が高まったり、事業者によるサービス展開が円滑に進まなかったりといった課題が指摘されるのも事実である。

総務省においては、こうした問題意識に基づき、適切な時期に、関係者間で速やかに問題を整理し、具体的な対応策を検討していくことが重要と考え、平成 21 年４月に利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会を設置して、課題ごとに WG を設けるなどして検討を行ってきた。

平成 21 年６月まで、①インターネット地図情報サービスについて、②違法音楽配信について、③ライフログ活用サービスについて、④個人情報保護ガイドラインの見直しについて、の４つの課題を設定して検討を行い、③を除く課題の検討結果を第一次提言として同年８月に取りまとめて公表した。

ここに提示する第二次提言は、第一次提言に含まれなかった課題の③と、第一次提言策定後に設定された２つの課題、すなわち⑤CGM について、⑥安全管理措置について、その検討結果を取りまとめたものである。この提言に基づき、関係者が協力し具体的な取組を行うことで、利用者が安心してサービスを享受し、サービス提供者が利便性に富んだ多様なサービスを提供できるような環境の構築が進むことが期待される。

目　次

Ⅰ　ＣＧＭに関する検討について……1
１．現状と課題について……2
２．青少年保護に向けた取組強化について……6
３．今後の課題について……27

Ⅱ　ライフログ活用サービスに関する検討について……29
１．はじめに……30
２．我が国のライフログ活用サービスの現状……31
３．諸外国の対応状況……35
４．我が国において懸念される法的問題……39
５．より信頼されるサービスに向けて（配慮原則の提言）……47
６．ディープ・パケット・インスペクション技術（DPI 技術：Deep Packet Inspection）を活用した行動ターゲティング広告について……54
７．おわりに……59

Ⅲ　安全管理措置に関する検討について……61
１．検討の背景……62
２．想定されるリスクと技術的対応策……66
３．求められる安全管理措置……76
４．漏えい等の発生時の手続の在り方……90
５．現行ガイドラインの改正の方向性……99

Ⅰ　ＣＧＭに関する検討について

１．現状と課題について

（１）青少年による CGM 利用の拡大

携帯電話の普及や家庭向けブロードバンドの進展に伴い、青少年のインターネット利用環境が整備されてきており、なかでも携帯電話保有率が着実に増加している。文部科学省の調査[1]によると、小学６年生では 24.7%、中学２年生では 45.9%、高校２年生では 95.9%の生徒が携帯電話を所有している。また、携帯電話からのインターネット接続については、中学２年生の 14.1%、高校２年生の 38.7%が１日平均１時間以上利用しており、さらに３時間以上利用している割合は、それぞれ全体の５%、11.5%となっている。

近時、利用者のサイトへの書き込みやメッセージの交換等の双方向コミュニケーションを可能とする CGM（Consumer Generated Media）の利用が拡大しており、以下特に断りがない場合、検討対象となるサービスは CGM 全般を指す。CGM には、青少年による携帯電話インターネットの利用用途として普及が進んでいる SNS（ソーシャル・ネットワーキング・サービス）に加え、プロフィールの交換を主とするプロフサイト、小説や動画等の投稿・交換を主とする投稿サイト等、多種多様なサービスが挙げられる。SNS は、利用者の経歴や顔写真又はアバター（サイト内の擬人キャラクター）を公開するプロフィール機能、日記や掲示板等の投稿を通じて双方向のコミュニケーションを行うコミュニティ機能、サイト内において利用者間でやり取り可能なメッセージ機能（いわゆる「ミニメール」機能）、その他利用者登録情報に基づいて利用者を検索する機能等も整備されてきており、青少年はリアルの世界で様々な場面や形で友人と交流するように、インターネット空間でも自由な表現活動やコミュニケーションを楽しんでいる。

主な SNS サービスである、mixi（株式会社ミクシィ）、GREE（グリー株式会社）、モバゲータウン（株式会社ディー・エヌ・エー）の会員数は、平成 21 年 12 月時点において延べ 5,112 万人（全体の利用者数は平成 19 年 12 月時点から倍増）となっており、青少年を含むインターネット利用者にとって当たり前の存在として普及してきていることが窺える。

（２）青少年被害の拡大

このように青少年による携帯電話からのインターネット利用が進む一方で、青少年の CGM サービス利用に伴う被害も増加している。主な被害としては、青少年保護育成条例違反や児童買春等の福祉犯被害、有料コンテンツの購入等による過剰消費等が挙げられるが、近年、特に青少年の福祉犯被害が増大し、社会問題となっている。

---

[1] 「子どもの携帯電話等の利用に関する調査」（平成 21 年５月 15 日公表）

警察庁の統計発表によると、平成 21 年中にいわゆる出会い系サイトに関係した事件の検挙件数は 1,203 件であり、前年と比べて 389 件（24.4%）減少している。また、被害児童数も 453 名と前年と比べて 271 名（37.4%）減少となっており、これらは出会い系サイト規制法（インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律）による規制強化の反映であるとの分析もなされている。

その一方、出会い系サイト以外のサイトを利用した福祉犯罪（児童福祉法違反、青少年保護育成条例違反、児童買春・児童ポルノ禁止法（児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律）違反）の検挙件数は 1,347 件、被害に遭った児童は 1,136 名で、前年と比べて 344 名（43.4%）増加となっている。なお、平成 21 年中のインターネット関連以外のものも含む少年の福祉犯事件の送致件数は 7,751 件（前年比 7.8%増）となっており、出会い系サイト以外のサイトを利用した福祉犯が占める割合が特に大きいというわけではないものの、児童ポルノ事件についていえば、インターネット利用に係る送致件数の割合は平成 20 年の 254 件（全体の 37.6%）から平成 21 年には 507 件（54.2%）と増加しており、被害児童数も 411 人（昨年比 21.6%増）と増加傾向にある。

他方、出会い系サイト以外のサイトにおける福祉犯被害全体に占める罪種の割合で見ると、青少年保護育成条例違反による被害児童数が 727 名（64.0%）と最大になっており、児童買春が最大の出会い系サイト関連事件とは異なる特徴が出ており、ことさらに出会い系サイト以外のサイトにおける被害を誇張して問題視していくべきかについては慎重な分析が待たれているものの、強姦や略取誘拐につながる被害も報告されている等、重要犯罪も根絶されているわけでもなく、福祉犯被害への有効な対策が求められている。

（３）福祉犯被害の防止に向けた効果的な対策の方向性

こうした現状に対し、多様な関係者によって青少年保護に向けた取組が進んできている。

まず、違法情報に対する取組としては、児童ポルノ禁止法、出会い系サイト規制法等に基づく取締りの強化が行われている。特に、出会い系サイト規制法については、平成 15 年の制定後も、出会い系サイトの利用に起因した犯罪が多発したことを踏まえ、平成 20 年に法改正が行われ、事業者に対する届出制の導入や不適格事業者に対する事業停止命令を含む執行の強化、児童誘引情報の削除等の規定が設けられる等、取締りの強化が図られている。その他、警察機関による福祉犯罪の取締りが強化されている。

青少年保護に関する基本的な法的枠組みとしては、青少年による安全・安心なインターネット利用環境の整備を目指し、「青少年インターネット環境整備法（青少年が安全

に安心してインターネットを利用できる環境の整備等に関する法律)」が平成 21 年４月から施行されており、青少年の適切なインターネット活用能力の取得（リテラシーの向上)、青少年の有害情報の閲覧機会の最小化（フィルタリングの普及促進)、民間主導による対策の推進が基本理念として明記される等、民間の自主的取組を主体とする対策の実施が図られている。

フィルタリングサービスの普及については、青少年インターネット環境整備法の施行以前より、総務省では過去３回にわたる総務大臣要請を携帯電話・PHS 事業者（以下「携帯電話事業者等」という。）に対して行っており、18 歳未満の青少年に対する携帯電話フィルタリングの原則適用、青少年利用への配慮に基づいて民間の第三者機関が認定したサイトのリストへの反映を初めとする携帯電話フィルタリングの普及・改善に努めてきた。これにより、フィルタリングの普及が着実に進展してきているとともに[2]、保護者によるサイトの個別閲覧可否設定が可能な「カスタマイズコース」や世代別フィルタリングの導入等使い勝手の良いサービスの開発も着実に進んできている。

その他、通信事業者や CGM 運営者等による出前講座（例：e-ネットキャラバン）の実施や、民間の関係団体（「安心ネットづくり促進協議会」等）による啓発イベントの開催等、青少年や保護者等を対象とした普及啓発活動も広がりを見せているところである。さらに、一般からの違法有害情報に関する通報を受け付ける「インターネット・ホットラインセンター」、サイト運営者や教員等にサイト上のトラブルへの対応策をアドバイスする「違法・有害情報相談センター」等の相談窓口も徐々に整備されてきている。

このように、青少年のインターネット利用環境整備については、必ずしもコミュニケーション活動に対する法規制に依拠することなく、それぞれの関係者が継続的に対策を講じているが、民間の自主的取組の促進を基本理念として掲げる青少年インターネット環境整備法の趣旨（同法第３条第３項）に照らし、今後も一層奨励されるべきアプローチといえよう。

また、同じく基本理念として掲げられているとおり、青少年が適切に情報を利活用できる能力の向上については、その重要性を強調してもしすぎるということはない。そもそも、青少年にとってのインターネットは、適切に利用される限りにおいては、他者とのコミュニケーション能力を涵養し、創意工夫ある表現行為を通じて経済的・文化的・社会的活動の基盤となる不可欠のツールと位置づけられるべきものである。青少年をリスクから守るために機能や利用を制限することの重要性は否定されるべきではないが、同時に、いずれ成年としてインターネットを活用していかなければならない青少年が、その発達段階に応じて適切な利活用能力を育成していくことが重要であることもまた

[2] 電気通信事業者協会発表の平成 21 年 12 月末時点での携帯電話フィルタリングの加入数は 623 万加入であり、青少年インターネット環境整備法の施行直前（平成 21 年３月）から 50 万加入の増加。

論を俟たないところである。とりわけ、青少年を取り巻くサービスや技術は不断に変化するものであり、技術的な対策や民間事業者による自主的取組による対応には自ずと限界があることから、利用者である青少年が自らリスクへの対応能力を高めていく必要性は、今後も一層高まっていくものと考えられる。そのため、既存の取組を一層強化するため官民が協力して国民の ICT リテラシーを高めていくことが求められている。

以上を踏まえつつも、青少年が判断能力の未成熟さゆえに様々なインターネット上のリスクに対して無防備な状態となっていることも事実であり、これまでに取り上げた様々な取組は引き続き効果的なものとして推進されるべきであるものの、全体としてはなお携帯電話インターネットを通じた CGM 利用を初めとする青少年被害が減少していないことにかんがみると、現状の取組をさらに進め、補完するために、関係者による一層の取組の強化が急務となっているといえる。

こうしたなか、安心ネットづくり促進協議会において、コミュニティサイト利用に関する青少年保護に向けて産学の関係者による集中的な検討が進められ、平成 21 年 10 月に報告書「子どもを護るために」がまとめられ、各関係者が果たすべき役割が整理された。

CGM 運営者による取組強化の方向性として、悪意のある大人が青少年にコンタクトできない仕組み作りが求められており、一定の機能制限やメッセージの同時多発送信者に対する注意喚起、利用者年齢に応じたサービスの設定等が例示されている。

また、携帯電話事業者及びフィルタリング提供事業者に対しては、青少年保護に対するフィルタリングの有効性確保が求められており、フィルタリングの一層の普及・改善を図るとともに、携帯電話利用者への啓発活動の充実等が課題とされている。

その他、第三者機関における青少年利用に配慮した運営管理体制構築に向けた認定基準の拡充、監視事業者における継続的な取組の向上、中小コミュニティサイトにおける運営体制の整備等、社会全体における啓発活動の推進等、様々なプレイヤーがそれぞれに果たしてきた役割を踏まえて、今後の取組強化の方向性を示したものとなっている。

同報告書では、被害防止に向けて有効な対策を講じるため、新たな対策を講じる必要性が提起されており、なかでも①CGM サービスにおける機能制限の前提となる年齢認証の確実化に向けた課題の整理、②悪意のある成年による青少年の誘引防止のための「ミニメール」内容確認の法的課題の整理等が政府に対して求められたところである。

本 WG は、CGM サービスに起因する青少年被害を少しでも減らしていくとともに、インターネット上における青少年の適切な利用環境を確保するため、法的関係や周辺環境が

不明確となっているがゆえに対策がためらわれている主な取組を取り上げ、法的整理等を通じて今後の方向性を明らかにすることを目的として検討を行ったものである。

２．青少年保護に向けた取組強化について

（１）フィルタリングサービスの普及改善

①　問題の所在について

青少年による有害情報の閲覧機会を最小化するための方策として、これまで携帯電話等のフィルタリングサービスの普及・改善が図られてきたことは既述のとおりであり、今後もフィルタリングの着実な普及に努めていくことが望ましい。

しかしながら、加入者数全体は増加しているものの伸び率が逓減しており、普及傾向に天井感が見られつつあるとも指摘されている。また、フィルタリング普及を含む利用者への啓発活動についても、事業者や業界団体を含む様々な主体によって継続的に行われているものの、いまだ「点」的な活動の集積に留まっており、「面」的な広がりが課題として指摘されている。

こうした現状を踏まえ、上記安心ネットづくり促進協議会の報告書においても、携帯電話事業者等に対して、フィルタリングサービスの加入促進や加入後の解除の抑制に向けた取組の加速とともに、携帯電話事業者等を含む各プレイヤーが自らの取組を検証するための指標として相応しい数値設定を行うべきであると提言されているところである。

②　更なる対策の方向性について

フィルタリングサービスの加入促進策としては、様々な取組の方向性が考えられるが、普及が進まない理由と考えられる要因を的確に見極めた上で、有効な対策を検討すべきである。この点については、これまで携帯電話事業者等においてカスタマイズや年齢層別等、多様な利用者ニーズにあわせる形でフィルタリングサービスの多様化が図られているものの、利用者の認知が十分に進んでいるとはいえず、普及の障壁となっているとの指摘もあることから、新規契約・機種変更時等の機会を捉えて一層の周知を図ることが求められる。また、新旧のフィルタリングサービスに対する利用者意識の調査・分析を行う等、利用者ニーズに更に応えたフィルタリングサービスの在り方について検討を進めることが求められる。

また、保護者名義で回線契約が締結されているが、利用者がその子等である携帯電話端末（いわゆる「親ケータイ」）の利用実態把握が進んでおらず、携帯電話事業者

等が青少年利用者に十分に訴求できないという点も、フィルタリング普及に向けた課題の一つとして指摘されている。本来であれば、青少年インターネット環境整備法第17条第２項に基づき、利用者が青少年である場合には当該保護者にその旨の申告が義務付けられているところであるが、保護者等の認知が十分に進んでいないことから、携帯電話事業者等において、保護者の意識向上や、新規契約・機種変更時等の機会を捉えた確認等により、利用者情報の確認強化を進めていくことが望ましい。

さらに、携帯電話フィルタリングの解除の抑制については、危険性を十分に認識しないことによる安易な解除を防ぐための取組が求められる。例えば、解除申告を受け付ける際に保護者に対する危険性の説明と明確な意思確認を行うプロセスを導入するといった解除受付方法の改善などが具体的には考えられる。また、解除理由の実態を踏まえ有効な対策を検討していくことも必要である。加えて、保護者になりすました子どもによる解除申告を防ぐための取組が求められる。例えば、解除申告を受け付ける際に、保護者に、架電での対応を含め、直接意思確認を行う対応や、保護者の本人確認書類の原本の確認等の対応が考えられる。

加えて、携帯電話事業者が自らの取組を検証するための指標については、これまで四半期ごとに電気通信事業者協会からフィルタリング加入者数の合計値が発表されてきたものの、今後の普及方策を検討する上で必要と考えられる年齢層別の加入状況といった指標についても、可能な限り公表されることが望ましい。

（２）青少年向けの機能制限等

①　問題の所在について

多くのCGM運営者は、危機対応能力が不十分な青少年の福祉犯被害への対策として、様々な自主的取組を実施している。例えば、フィルタリングの改善を目的として、民間の第三者機関による運用管理体制の審査・認定の仕組みが導入されているが、一部のCGM運営者は第三者機関認定に向けて青少年保護の取組を行う必要性に基づいて、自社の管理体制を強化することにより、インターネット利用環境の整備に貢献しているといえよう。また、CGM運営者のなかには、サービスの利用時に危険性の注意喚起（例：書き込み画面でのポップアップ表示）を行い、又は情報モラルコンテンツ（例：トップページからのリンク）を提供する等の普及啓発活動を行う者も少なくない。

そうしたなか、一部のCGM運営者は、悪意のある大人による出会いの誘引に悪用される可能性のある特定の機能について、青少年向けの提供を制限する取組を自主的に進めている。その仕様はサービスの種類や対象とするユーザにより異なるが、一般的には、コミュニティ機能や利用者検索機能、CGMサービス会員間のメッセージ機能（いわゆる「ミニメール」機能）等、面識のない他人同士の接触を容易にする機能につい

て、利用者の年齢に応じて利用可能な範囲を制限し、内容確認を行うなど、リスク低減に向けた手段を講じるものである[3]。

機能制限等の有効性等については、例えば、ある大手 CGM 運営者によると、平成 21 年上半期の警察機関からの捜査関係事項照会案件（福祉犯被害関係）のうち約８割は、検索機能により青少年利用者を捕捉し、プロフィール機能により利用者の属性を確認し（例：女子高生か否か）、ミニメールで直接のやりとりに持ち込むというパターンであり、これら特定の機能を制限することが被害防止の観点から有効と指摘されている。実際に、株式会社ディー・エヌ・エーでは、自社の運営するサイトで検索やミニメール機能の制限を開始した平成 19 年末以降、捜査関係事項照会数は大幅に減少したとの報告もある。

民間の第三者機関であるモバイルコンテンツ審査・運用監視機構（EMA）においても、コミュニティサイト運用管理体制認定基準のなかで、青少年利用を前提とした利用環境の整備を掲げた上で、概説書において、児童誘引行為等のトラブル防止策として、コミュニティサイト事業者に対し、サイトの規模や、サービス形態等に応じて、プロフィール検索やメッセージ等を含む関連機能の利用制限や重点的な監視体制の整備を行うことを求めている。また、フィルタリング提供事業者であるネットスター社は、平成 21 年 11 月に双方向利用型サイトにおけるリスク評価モデルの検討を通じたリスト分類基準の見直しを実施し、コミュニティサイトにおける児童保護のためにサイト側が配慮すべき事項として、提供機能の制限や書き込み内容の監視等の運営状況を外形的に評価する取組を行っている。

これら青少年向けの機能制限等は、福祉犯被害への引き金となる接触リスクについて、対応能力が十分育成されていない青少年を保護しつつ、発達に応じた適切な利用環境を確保するという点で効果的な対策であると指摘されていることから、既存の機能制限等の効果検証を踏まえつつ、今後も一層の取組強化が求められる。

機能制限等は究極的には利用者保護と事業者の信頼性向上に繋がるものであるが、一時的にはサービスの利便性を損なう側面もあることから、今後、自主的取組として機能制限等を行う主体をどのように拡大していくかが課題となる。この点については、本 WG での検討等も通じて、機能制限等の必要性や有効性についての周知を図ることにより、青少年を適切に守る観点から事業者の社会的意識を向上させるための環境づくりを進めていく必要があろう。

[3] SNS 大手３社では、一定年齢以下のサービス（コミュニティ機能）利用制限、一定年齢以下の利用者（又は一定の年齢差を有する利用者同士の）検索機能の制限、一定年齢以下のメッセージ交換機能の利用制限、一定年齢以下の利用者に対する啓発強化等を実施。

現在、青少年向けの機能制限等を進めていく上で、大きな課題として指摘されているのは、ア．法的関係が不明確であるために対策がためらわれている「ミニメール」内容確認についての考え方の整理、イ．機能制限等の前提となる年齢情報確認の確実化を通じた詐称リスクの低減である。イ．の年齢認証問題については次節に譲るとして、以下本節ではア.「ミニメール」内容確認と通信の秘密の保護等の法的関係の整理について述べることとする。

② 「ミニメール」内容確認について

いわゆる「ミニメール」は、CGM サイトに会員登録を行っている利用者の間でメッセージを交換するサービスであり、発信者が CGM 運営者の管理するサーバにメッセージを発信・記録し、受信者が当該記録されたメッセージを閲覧（受信）することによって通信が行われるものである[4]。上述のとおり、「ミニメール」を契機とする被害への対策として、一部の CGM 運営者や運営者から委託を受けた監視事業者は、「ミニメール」の通信内容を確認し、規約違反内容の削除等を実施している。内容確認の手法としては、発信時（サーバへの反映以前）にはあらかじめ設定された一定のキーワードを含む内容を機械的に検知して発信を防止し（ベイジアンフィルタリング）、発信後（サーバへの反映以後）は目視を含めた内容確認に基づき規約違反メッセージの削除等を行うというのが一般的である。

既述のとおり、「ミニメール」を通じた児童被害については、青少年の未熟な判断力に起因するものが多いと考えられており、事前・事後の内容確認により被害防止につながることが期待されている。他方、CGM 運営者等がサーバ上で内容確認を行うことから、通信の秘密その他利用者の利益を侵害するおそれが指摘されており、一部事業者においては取組がためらわれている例もあることから、速やかに法的関係を整理した上で、事業者が積極的に被害防止策を講じることができる環境づくりを検討することが必要である。

③「ミニメール」内容確認と通信の秘密の保護等について

ア 問題の所在

「ミニメール」内容確認を行うことが、通信の秘密の侵害に当たるかが問題となる。

通信の秘密は個人生活の安寧を保障するとともに、通信が社会経済文化活動にとって不可欠の基盤であることから、憲法上の基本的人権の一つとして憲法第 21 条第２項において保障されており、これを受けて、電気通信事業法においても、直接の

[4] 近時、CGM サイトの会員と非会員間で直接メッセージのやりとりを行う形態のコミュニケーションも登場している（例：ブログの閲覧者（非会員）が、同サイト上のコメント機能（管理者のみ閲覧可）を用いて、管理人である青少年利用者に直接アプローチする行為）。こうした「ミニメール」とは性質の異なるサービスの実態把握も必要との指摘があった。

罰則付きの保護規定が設けられている（同法第４条、第 179 条）。本規定は、電気通信事業に従事する者以外の者に対しても適用されるが、電気通信事業者等による侵害には特に重い罰則が科されており、厳格な規律として運用されてきている。

日本国憲法 第二十一条 ２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

電気通信事業法（昭和五十九年法律第八十六号） 第四条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。 ２　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。 第百七十九条　電気通信事業者の取扱中に係る通信（第百六十四条第二項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。 ２　電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。 ３　前二項の未遂罪は、罰する。

「通信の秘密」とは、（ア）個別の通信に係る通信内容のほか、（イ）個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号等の通信当事者の識別符号、通信回数等これらの事項を知られることによって通信の意味内容を推知される事項全てを含んでおり[5]、「ミニメール」の内容も、CGM 利用者間で交換される通信であることから、秘密の対象に含まれると解される。なお、ホームページに掲載された情報等、不特定者からの閲覧を前提とした通信は、発信者にその内容を秘密とする意思がなく、内容については法による保護の対象外とされている。

続いて、「電気通信事業者の取扱中に係る通信」とは、発信者が通信を発した時点から受信者がその通信を受ける時点までの間、電気通信事業者の管理支配下にある状態のものを指し、情報の伝達行為が終了した後もその通信内容等は保護の対象となるため、「ミニメール」を提供する CGM 運営者（又は業務委託を受けた者）が自ら管理するサーバ上で内容確認を行っている限りにおいては、原則として「電気通信事業者の取扱中に係る通信」に該当すると解される。

このように、「ミニメール」の内容は通信の秘密に該当するが、電気通信事業法上、事業者等が他人の通信を媒介する役務（いわゆる電子メール等）、事業者等が媒介を

[5] 東京地裁平成 14 年４月 30 日判決

行わずに自ら管理する電気通信設備を他人の通信のために運用する役務（いわゆる電子掲示板等）等がどのように位置づけられるかにつき議論が存在する。この点については、特段の前提なく「ミニメール」が提供される場合には、CGM 運営者が通信内容を変更することなく伝送・交換し、他人と他人の通信を仲介する立場に基づき、利用者の送信依頼を受けてメッセージを媒介する役務と解される一方、サービス提供に先立って、CGM 運営者が通信当事者となり内容確認を行い得る立場となることについて明確な通知及び同意取得が行われる場合は、その限りではないと解される。いずれにしても、通信の秘密との関係においては、電気通信事業法上どのように位置づけられるかが論点となるのではなく、通信当事者が何を秘密とする意思を有しており、その意思が誰によってどのように共有されているかにより保護の対象が異なってくるという点が重要である。

イ　通信の秘密の侵害該当性

以上を踏まえ、「ミニメール」内容確認が通信の秘密の侵害に該当するか否かが問題となるが、ここでの侵害行為は、（ア）通信当事者以外の第三者が積極的意思で通信の秘密を知り得る状態に置くこと（「知得」）、（イ）発信者・受信者の意思に反して通信を利用すること（「窃用」）、（ウ）他人が知り得る状態に置くこと（「漏えい」）に分類される。「ミニメール」内容確認は、CGM 運営者が積極的意思に基づいて通信内容を検知し、通信当事者の意思に反して処理（利用規約に基づく削除等）を行おうとする限りにおいては、知得ないし窃用に該当するといえるのであって、通信の秘密の侵害に該当する。

このように、通信の秘密の侵害に該当するか否かの判断において通信当事者の意思が論点となることを踏まえると、通信当事者以外の第三者が通信当事者から同意を得ずに内容確認を行う場合には侵害に当たる一方、通信当事者自身が内容確認を行う場合には侵害に当たらないと解することができる[6]。そうした観点から、「ミニメール」サービスにおける通信当事者の範囲が問題となる。

この点、広く一般に利用されているウェブメールサービスにおいて、通信当事者は送受信者であると解されていることを踏まえると、CGM 運営者が通信当事者として加わることによって「ミニメール」の内容確認を行おうとする場合、約款等を通じて通信当事者に加わることの意味を利用者が明確に理解できる環境が整備されていなければならない。

他方、CGM 運営者が通信当事者に加わることについて利用者の同意が得られておらずそのように評価できない「ミニメール」その他のメールサービスについては、

6 これは、通信の秘密の保護対象であるメッセージ内容は、通信当事者間で共有されている情報であり、その秘密性を当事者間で相手に委ねているため、第三者への関係で、一方当事者の同意により秘密性が解除されるためである。

CGM 運営者が内容確認を行うことについて発信者等から有効な同意がある場合には、通信当事者の意思に反しない利用であるため、通信の秘密の侵害に当たらない。そこで以下、同意取得の在り方について検討することにする。

ウ　通信当事者からの同意について

通信当事者ではない CGM 運営者が「ミニメール」内容確認を行うことが許されるかという点については、まず通信当事者から内容確認についての同意を得ているかどうかが論点となる。

この点については、「ミニメール」利用者の明示的な意思表示に基づいて行う必要があるため、デフォルトオフ（役務提供の初期設定では同意を推定しないこと）で個別の同意（例：発信時の画面表示での確認）を得ることを条件として内容確認を行うことが望ましい[7]。

他方、デフォルトオフの個別同意取得でなければ有効な同意と見なせないかという点については、過去、迷惑メールやウェブ閲覧のフィルタリングサービスと通信の秘密の保護の関係の検討において、原則としてデフォルトオフにより同意取得を条件として提供すべきとしながらも、以下の５要件全てを満たす場合には、例外的に通信当事者から同意が得られたものと同視し得るとして、フィルタリングをデフォルトオンの状態で提供することも可能とされてきた[8]。こうした整理が求められた背景としては、迷惑メールや有害情報のウェブ閲覧に対するフィルタリングにおいては、送信者から同意を得ることが期待できないため、受信者から同意を得て行う要請があることを踏まえ、受信者から事前に同意を得たと認められるための条件にはどのようなものが考えられるかについて整理することとしたものである。

以下、フィルタリングをデフォルトオンで提供するための５要件を掲げ、「ミニメール」内容確認の例にそれぞれ当てはめることにより、「ミニメール」の通信当事者から個別の同意が得られなかったとしても、周辺の利用環境等に基づきそのように考えることにより内容確認を行うことができるかどうかについての考え方を示したものである。

要件１）利用者が、いったんフィルタリングの提供に同意した後も、随時、任意に同意内容を変更できること

---

[7] 役務提供契約約款等に基づく事前の包括同意のみにより通信の秘密の利益を放棄させることができるかどうかについては、①約款は当事者の同意が推定可能な事項を定める性質であり、通信の秘密の利益を放棄させる内容はその性質になじまないこと、②事前の包括同意は将来の事実に対する予測に基づくため対象・不明確となることから、一般的には有効な同意と解されていない。

[8] 「電気通信事業分野におけるプライバシー情報に関する懇談会」第 18 回会合（平成 18 年 1 月 23 日）

→（当てはめ）特段の前提なく提供される「ミニメール」につきデフォルトオンで内容確認を行った後、利用者の明示的な意思表示に基づいて、当該同意内容は変更できるようにする必要がある。他方、CGM 運営者が内容確認を行う前提で提供される「ミニメール」につき、利用者が内容確認に同意しなくなった場合、当該利用者は事実上「ミニメール」を利用できなくなるが、（ア）認定電気通信事業者でないCGM運営者に役務提供義務はないこと、（イ）青少年保護のための限定的な内容確認を条件として役務を提供することは不当な差別的取扱にならないことから許容されると考えられる。ただし、（イ）について、利用者視点を踏まえれば、青少年保護という目的や内容確認の手法（出会いを誘引するキーワードによる抽出等）がある程度可視化されている環境が存在することが望ましい。

要件２）フィルタリング提供に対する同意の有無にかかわらず、その他提供条件が同一であること

→（当てはめ）利用者が「ミニメール」内容確認に同意しないからといって、その他の提供条件を変更することは通常は想定されないと考えられる。

要件３）フィルタリングの内容等が明確に限定されていること

→（当てはめ）「ミニメール」内容確認の中身は約款等により明確に規定される必要があるのではないか。

要件４）通常の利用者であれば同意することがアンケート結果等により合理的に推定されること

→（当てはめ）CGM 運営者が通信当事者とならない場合の「ミニメール」内容確認について、利用者の包括同意は推定されにくいため、個別のサービスについて利用者啓発等を通じて、同意が合理的に推定される環境を整備していく必要がある。

要件５）利用者に対して、フィルタリングの内容等につき事前の十分な説明を行うこと（重要事項説明に準じた手続）

→（当てはめ）ユーザアカウント作成時等に周知を行う仕組みを整備する必要がある。

このように、「ミニメール」については、例外的に利用者同意が合理的に推定される環境が実現している場合には、CGM 運営者が通信当事者でない形で提供されているとしても、デフォルトオンにより内容確認を行うことができると解される。

上述のとおり、デフォルトオンによるフィルタリングと通信の秘密の関係の整理は、受信者からの有効な同意取得の在り方について検討されたものであり、「ミニメール」のように、送信者から内容確認を役務提供の条件とし又は個別通信の際の同意事項として得ることが可能であるサービスとは、検討の前提を異にする点に留意する必要がある。すなわち、青少年被害の防止という観点から「ミニメール」内容確認を行おうとするCGM運営者は、基本的には送信者からの事前の同意の取得（青少年保護目的の内容確認を条件としてサービスが提供されることを含む）を目指すことが想定され、実際には、５要件を満たすことによりデフォルトオンで内容確認を行う場面は限定的とも考えられる。

エ　違法性阻却事由について

通信当事者の同意がない場合でも、正当行為（刑法第35条）、正当防衛（同第36条）、緊急避難（同第37条）のいずれかの要件を満たす場合には、侵害行為の違法性が阻却され、内容確認を行うことができる。ここでは、「ミニメール」の送達以前にCGM運営者が常時行う内容確認を対象としており、送達後の通報に基づいてCGM運営者が行う内容確認については、通信当事者たる受信者の同意があること等から、通信の秘密の侵害に該当しないと考えられる[9]。従って、以下、「ミニメール」の送達以前にCGM運営者が網羅的に行う内容確認が、「正当行為」又は「緊急避難」に該当するか否かが論点となる。

まず、刑法第35条に基づき、法令に基づく行為及び正当業務行為については違法性が阻却される。「ミニメール」内容確認は民間の自主的取組であるため、ここでは正当業務行為といえるかどうかが問題となる。

CGM運営者の正当業務性の内容について直接に考え方が整理された例はないが、電気通信事業者による通信の秘密の侵害行為が正当業務行為に該当するか否かについては、実務上の運用や裁判例を通じて一定の考え方が整理されてきている。これまでに正当業務行為が認められた事例は、（ア）通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為、（イ）ISPがルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為に加え、（ウ）ネットワークの安定的運用に必要な措置であって、目的の正当性や行為の必要性、手段の相当性から相当と認められる行為（大量通信に対する帯域制御等）といったものが挙げられる。こうした事例の根底にある基本的な考え方によれば、正当業務行為性は、それによって得ようとする利益の一般的な意味での正当性の有無により判断

[9] 正当防衛については、侵害者（送信者）に対する反撃行為である必要があるところ、CGM運営者による内容確認は、一概に発信行為そのものに向けられた反撃行為ともいえず、また実際の成立要件は後述する緊急避難の検討により実質的に満たされ得ることから、ここで検討する必要はないと考えられる。

するのではなく、国民全体が共有する社会インフラとしての通信サービスの特質を踏まえ、誰もが自由に通信を支障なく利用できる環境を確保する観点から、そうした通信役務の提供にとっての正当性の有無により判断しているといえる[10]。

この点については、利用者保護のための行為には正当業務性が認められるのではないかとの指摘があるが、「ミニメール」内容確認はその仕様上、網羅的・機械的に行われざるを得ない一方、発信される通信の全てが違法行為を構成するわけではなく、発信者が加害者となることや受信者が被害者となることから一般的に利用者を保護することを理由として、違法性が阻却されると解することは相当ではない。

こうした考え方を敷衍すると、「ミニメール」内容確認は、役務提供にとっての正当性が一般的には認められず、正当業務行為性を認めることは困難であると考えられる[11]。

さらに、通信当事者の同意がない場合の違法性阻却事由として、緊急避難の成立の可否が問題となる。

刑法第 37 条に基づく緊急避難が認められるためには、（ア）法益侵害に対する現在の危難の存在、(イ)危難を避けるためにやむを得ずした行為であること(補充性)、（ウ）避難行為による害が避けようとした害の程度を超えないこと（法益の権衡）が求められる。(ア）現在の危難の存在とは、法益の侵害の危険が緊迫した状態を意味するが、「ミニメール」の流通により侵害される法益が何かが問題となる。(ウ）法益の権衡の考え方に基づけば、「ミニメール」内容確認により侵害される法益が通信の秘密の保護という重大な利益であることにかんがみると、現在の危難の内容も、生命又は身体に対する重大な危険に比肩するものに限られるべきである[12]。こうした点を踏まえると、CGM 利用を通じて強姦や略取誘拐等の重要犯罪による被害が生じている例はあるものの、緊急避難法理を用いて内容確認が許容される場合は、これらの犯罪の発生が受信予定者に切迫していることにつき客観的に信じるに足りる

---

[10] この点に関して、電気通信事業者に脅迫的内容の電報を差し止める義務があるかどうかが争われた判例において、電気通信事業者が電報の内容を確認することにつき否定的な判断を行ったものがある（「NTT 脅迫電報事件」)。原審判決（大阪地裁平成 16 年７月７日判決）においては、通信媒介者である NTT に対していわゆる脅迫電報の検知と差し止めを求めることは、適当でないだけでなく、公共的な通信事業者の職務の性質から許されない違法な行為であり、通信役務は物理的な通信伝達の手段として発信された通信内容をそのまま受信者に伝達することである旨判示されている。なお、控訴審判決（大阪高裁平成 17 年６月３日判決）において原告の控訴は棄却されている。

[11] なお、刑法第 35 条等により、法令行為、正当業務行為以外の一般的違法阻却事由が認められるとする見解があるが、この見解に立ったとしても、前記 NTT 脅迫電報事件判決の趣旨に照らせば、ミニメールの内容確認行為が、一般的違法阻却事由により違法性を阻却されると解することは困難である。

[12] 過去に緊急避難による違法性阻却が認められた事例として、人命保護の観点から緊急に対応する必要のある自殺予告事案につき、ISP が警察機関に発信者情報を開示する場合が存在（「インターネット上の自殺予告事案への対応に関するガイドライン」平成 17 年５月）

場合であって、内容確認以外に取るべきより侵害性の少ない手法（事後的な通報に基づく削除等）が存在しない場合など、極めて限定的な場面であると考えられる。

このことから、「ミニメール」内容確認は、発信行為の危険性等を理由として行うことが緊急避難に該当する可能性もあるが、内容確認を行う時点で現在の危難が認められる場面は極めて限定的であると考えられる。

オ　その他の論点

CGM 運営者が電気通信事業者である場合、電気通信役務の提供について不当に差別的取扱いをしてはならないとされている（電気通信事業法第６条）。また、通常は考えにくいが、仮に CGM 運営者が認定電気通信事業者（公益事業特権に基づいて電気通信回線を敷設して役務提供を行う者）である場合、正当な理由なく役務提供を拒否してはならないこととされている（同法第 121 条）。いずれの場合も、「ミニメール」内容確認に正当な理由の存在が認められるかが問題となるが、利用者の有効な同意に基づいている限りにおいては、利用の公平や役務提供義務に反しないと解される。

④　まとめ

これまでは、「ミニメール」が青少年に提供される場合に、その内容確認と通信の秘密の関係を法的に整理してきた。この整理は、そもそも「ミニメール」サービスが青少年の利用に供されるべきか否かという問題に直接応えるものではなく、「ミニメール」利用が様々なリスクをもたらすことを認識しつつ、青少年のコミュニケーションにもたらす影響について冷静な検討をしていくことも求められよう。

「ミニメール」内容確認については、危機対応能力の低い青少年の CGM 利用に伴う被害防止策として有効と考えられており、法的関係を明確化した上で実施していくことが望ましい。

この点については、「ミニメール」が通信当事者の範囲について特段の前提条件なく提供されている場合、内容確認を追加的に行うに際しては、利用者から有効な同意を取得することにより、通信の秘密の保護との関係で問題なく実施することができる。

また、サービス提供に先立って CGM 運営者が通信当事者として加わることについて利用者からの明確な同意が得られている場合も、内容確認を行うことができると解される。

CGM 運営者は、内容確認を行うことによって取得した情報については、電気通信事

業における個人情報保護に関するガイドライン[13]を遵守し、適正に管理することが求められる。

CGM 運営者によるメッセージ内容の確認は、通信の秘密との関係で一部に懸念が指摘されてきた一方、児童の福祉犯被害に対する有効な対策であるとされていることから、実施に当たっては不当な利益侵害とならないように配慮を行いつつ、被害防止に向けた社会的な環境づくりを図るとともに、利用者への周知・啓発に努めていくことにより、取組に対する理解の醸成と取組主体の拡大を図っていくことが求められよう。

（３）利用者年齢認証の確実化

①　年齢認証の確実化を巡る課題について

機能制限等の前提となる利用者の年齢認証については、悪意のある成年が青少年と偽り、又は青少年が成年と偽ることにより機能制限等を免れるといった年齢詐称に伴う弊害が指摘されており、年齢認証の確実化に向けた取組の強化が求められている。

ア　年齢認証の主体

誰が年齢認証を行うべきかについては、本来年齢情報を青少年向け機能制限等に活用しようとする CGM 運営者が自ら行うことが望ましいといえ、既に大手 CGM 事業者による年齢認証の改善に向けた自主的取組の例もあるところである（後述）。

しかし、CGM 運営者のみが認証行為を行うことに対しては、CGM サービスがオンラインコミュニケーションの機会を提供するものであり、通常は利用者情報もオンライン上で確認することとなるため、対面確認に比べて詐称の可能性が高まるという実効性の面からの指摘がある。この点について、たとえオンラインサービスであっても対面確認や書面確認を行うことが可能であるとの指摘があり、そうした取組の可能性については引き続き追求していく必要があるが、（ア）商取引等の契約を伴わない一般のコミュニケーションについてもあまねく対面確認等を求めることが有効かつ妥当か、（イ）青少年の CGM 利用の実態として、特定の CGM サービス（プロフ等）を中核としつつ複数の CGM を機能ごとに使い分けるのが主流であり、一つのサイトで年齢認証を行うことがどれほど有効か等の課題も指摘されている。現在、オンラインで行われている年齢認証は、主として成年向けに役務利用を制限することを目的として、成年の証憑（例：クレジットカードや運転免許証）を用いるものであり、そうした考え方が青少年による CGM 利用に適用できるかどうかについては、青少年のオンラインコミュニケーションをどのように位置づけるか等も踏まえたバランスの取れた検討が求められる。

---

[13] 平成 16 年総務省告示第 695 号。最終改正平成 21 年総務省告示第 543 号

また、CGM 運営者のみによる年齢認証については、厳格な年齢認証を行うサイトとそうではないサイトの間で利便性の面で差が生じ、青少年利用者が前者を避けることは極めて明確であること等から、認証を行わないサイトが潜在化し、却ってそれらの利用が増えることにより CGM 運営者の自主的取組の促進が阻害されるおそれも存在するところである。

したがって、CGM 運営者による年齢情報の取得を含めた自主的取組が推奨されるべきことを前提としながらも、より実効性の高い年齢認証の実現に向けて、CGM 運営者のみによる認証に伴う諸課題を克服するための工夫が求められる。その際、実効性の観点から青少年利用者本人やその保護者と対面で接する可能性が比較的高い主体として、インターネット回線契約を締結する携帯電話事業者等について検討することが有益と考えられる。

イ　年齢認証の客体

誰の年齢を認証すべきかについては、一義的には CGM を利用する青少年となるが、認証する主体が CGM 運営者の場合には当該サイトの閲覧者となり、通信回線契約の提供者の場合には（携帯電話）インターネット接続役務の利用者となる。

インターネット接続役務の青少年利用者に対して年齢認証を行う場合については、インターネットに関係した青少年の福祉犯被害の多くが携帯電話等からのアクセスとも指摘されており[14]、青少年被害の防止に向けた取組が喫緊の課題となっていることからすれば、少なくとも現時点における検討としては、まずは携帯電話等の利用者を対象とすることを検討することが考えられる。

ウ　既存の取組について

平成 21 年６月以降、大手 SNS 運営者３社は、年齢認証の確実化に向けた取組として、フィルタリングを実装した携帯端末からのアクセスを認識し、利用者のサイト上での申告年齢の如何にかかわらず、当該利用者を 18 歳未満と見なして機能制限等を行う「フィルタリング連動型年齢認証」を行っている。こうした年齢認証システムは、自己申告に基づくオンライン認証よりも情報の真正性が高い取組として評価することができるが、以下のとおりいくつかの課題も指摘されている。

まず、携帯電話フィルタリングは高校生を中心として未だ普及率が十分に高いとはいえず、この仕組みでは少なくないフィルタリング非実装者を補足することができない。フィルタリングを実装していない利用者ほど、インターネット上の違法・有害情報への危機対応能力や問題意識が低いことも予想されるため、本取組のみに

[14] 上記平成 22 年２月 18 日警察庁統計によれば、出会い系サイトへのアクセス手段として携帯電話を利用した被害児童は 99.3%（平成 21 年中）

依拠することは保護の必要性が高い利用者層を除外するおそれにもつながる。

また、携帯電話フィルタリングには、法人契約や青少年であった者が成年となっても継続利用するといった利用形態を含んでおり、青少年以外からの利用に対しては必要以上の制限となりかねない。

さらに、フィルタリング実装の有無では18歳未満か否かしか見分けることができないため、CGM 運営者の側でより細かい年齢設定に基づく機能制限を行おうとしても必要な情報が取得できないとの指摘もあるが、実際にどの程度の年齢情報が必要かはサイトごとに異なるため一概に必要な情報が不足するともいえず、今後カスタマイズや年齢層別のフィルタリングが普及し、当該情報が活用可能となる余地がある。

加えて、本取組では、成年が青少年のふりをするためにフィルタリングを実装することによる詐称を判別することができないが、悪意のある成年による詐称リスクは、この仕組みに限らず存在するとの指摘も可能である。

いずれにせよ、青少年保護の見地に立ち、CGM 運営者が自ら年齢認証の確実化に向けた取組を強化することは推進されるべきであり、上記の様々な課題を踏まえつつ、より確実な認証システムの構築に向けて、現行の取組の効果検証を適切に行った上で、CGM 運営者が主体的に更なる改善やその他主体への普及等を強化していくことが求められる。

しかし、フィルタリングの十分な普及により、青少年に配慮していないCGMサイトの閲覧が原則不可になっていくことにかんがみれば、フィルタリングの普及に伴って本認証システムの意義は薄まっていくことも予想される。また、中期的には、フィルタリングでも閲覧可能なサイト（例：第三者機関認定サイト）において機能制限を重畳的に行っていくためには、フィルタリングの有無より粒度の小さい年齢情報が求められるともいえよう。したがって、本取組はフィルタリング普及の過渡期の取組として位置づけ、より確実な年齢認証の実現に向けた関係者による取組の強化が望まれる。

以下、新たな取組の方向性について検討していくに先だって、それぞれの関係者が、引き続き既存の取組を強化する努力の必要性について付言したい。現在、一部の携帯電話事業者等は、青少年保護やサービス改善等を目的として利用者年齢情報の任意申告を求めているが、携帯電話事業者等が利用者年齢情報を把握することは、青少年インターネット環境整備法において、携帯電話事業者等に対して利用者の発

達段階に応じたフィルタリングサービスの提供が努力義務となっていること[15]等にかんがみれば、フィルタリングの一層の普及に向けた自主的取組の一環として推進されることが望ましい。同様に、CGM 運営者の側でも年齢認証に基づく機能制限等、青少年を有害情報から守る取組が進展していくことが期待されている。それぞれの関係者が既存の取組をしっかりと継続・強化していくことの必要性については、今後も確認されなければならない。

エ　新たな取組の方向性について

CGM 運営者のみによる認証に一定の限界があることを踏まえ、携帯電話インターネット経由の CGM 利用に伴うことから、携帯電話事業者等も含めた関係主体の協調による新たな取組の検討の必要性が指摘されている。

上記のように、回線契約の締結主体である携帯電話事業者等のなかには、自主的取組として利用者年齢情報を取得している者もあるが、そこで得られた情報については、サイト上で利用者が登録する情報との比較でいえば真正性が高いと想定されている。

こうしたことから、CGM 運営者のみによる情報取得に対する補完的役割として、携帯電話事業者等が取得した比較的真正性の高いと想定される年齢情報を CGM 運営者が活用する方策について検討することが求められている。

②　携帯電話事業者等と CGM 運営者の協調による年齢認証の課題について

新たな協調的取組の実施に際しては、年齢情報と個人情報保護法との関係について整理した上で、個人情報の取得・活用に伴う関連法令を遵守しつつ、利用者保護に向けた配慮が適切に確保されることを条件として、青少年保護に向けた民間による自主的取組として実施されることが望ましい。

ア　利用者年齢情報の位置づけについて

利用者年齢情報の取扱いの在り方を検討するに際して、当該情報と個人情報保護法が規定する個人情報等との関係について、取り扱う主体や態様別に整理することが求められる。

---

[15] 青少年インターネット環境整備法（平成二十年法律第七十九号）
第二十条　青少年有害情報フィルタリングソフトウェアを開発する事業者及び青少年有害情報フィルタリングサービスを提供する事業者は、青少年有害情報であって閲覧が制限されないものをできるだけ少なくするとともに、次に掲げる事項に配慮して青少年有害情報フィルタリングソフトウェアを開発し、又は青少年有害情報フィルタリングサービスを提供するよう努めなければならない。
一　閲覧の制限を行う情報を、青少年の発達段階及び利用者の選択に応じ、きめ細かく設定できるようにすること。
二　（略）

まず、年齢情報を取得する主体である携帯電話事業者等においては、年齢情報を的確に更新していくためには、利用者や保護者に対して、青少年利用者の生年月日又は実年齢の申告を求めることが想定される。この場合、年齢情報は利用者の氏名等との照合により特定の個人を識別し得る属性情報となるため、個人情報として個人情報保護法の関連規定の規律が及ぶと考えられる。さらに、携帯電話事業者等は当該情報をデータベース化することが想定されるため、通常は個人情報取扱事業者[16]として、利用目的による制限（個人情報保護法第 16 条）や適正な取得（同法第 17 条）等の義務を負うほか、電気通信事業における個人情報保護に関するガイドライン（以下「ガイドライン」という。）の関連規定に服するものと考えられる。

他方、年齢情報の提供を受けて機能制限に活用する主体である CGM 運営者については、情報提供を受ける態様により法的位置づけが変わり得る。生年月日や実年齢、一定の年齢層（例：18 歳未満か否か）等の年齢情報を特定の個人が識別可能な形（例：氏名との関連付け）により提供される場合には当該情報は個人情報となり、CGM 運営者による年齢情報の取扱いは個人情報保護法の適用を受ける[17]が、特定の個人が識別できない形（例：携帯電話サービスの契約者固有 ID とは関連付けられているが、氏名等との結合が不可能なもの）により提供される場合にはその限りではない。ただし、単独では特定の個人を識別できなくても、他の情報と容易に照合することにより個人を識別可能な場合については個人情報保護法の適用を受けるため、例えば、CGM サイトにアクセスした携帯端末の契約者固有 ID に基づいて、CGM 運営者が携帯電話事業者に対して行う照会に対して年齢情報が提供される場合に、CGM 運営者が自ら管理する利用者情報（例：会員氏名）と関連づけることが可能である場合、当該情報には容易照合性が認められると考えられる。

このように、CGM 運営者が年齢情報を取り扱うに当たって、それが個人情報保護法の適用を受ける個人情報の取扱いに当たるかどうかは、具体的な年齢情報の取扱態様により異なってくるものと考えられるが、年齢情報を活用される立場の利用者視点を踏まえれば、当該 CGM 運営者が個人情報保護法の義務規定の適用を受ける個人情報取扱事業者に該当するか否かにかかわらず、年齢情報の適正な取扱いや利用者への説明等について一定の配慮が求められるであろう。

なお、年齢情報の粒度（実年齢か、18 歳未満か否かといったきめの細かさの程度）によって、当該情報の法的位置づけが変わるかどうかについては、個人情報保護法上は個人識別性の有無に影響しないため関係がないと考えられるが、プライバシー保護やセキュリティ確保の観点からは、必要以上の情報のやりとりが行われること

[16] 個人情報保護法第２条第３項。個人データベース等を事業の用に供する者のうち、政令で定める小規模事業者を除いた者。

[17] 当該 CGM 運営者が電気通信事業を行う場合には、保有する個人情報の数にかかわらず電気通信事業における個人情報保護に関するガイドラインの対象となる。

は望ましくないと考えられる（詳細は後述）。

イ　携帯電話事業者等による年齢情報の取得時について

携帯電話事業者等による利用者年齢情報の取得に際しては、情報の利用目的等について顧客に十分な説明を行うことが必要である。すなわち、個人情報保護法第 15 条（利用目的の特定）、第 16 条（利用目的による制限）、第 17 条（適正な取得）、第 18 条（取得に際しての利用目的の通知・公表）及びガイドラインの関連規定（第５条、第６条、第７条、第８条。ただし、第 14 条はプライバシーポリシーの策定に関する上乗せ規定）を遵守する必要があり、具体的には、店頭での情報取得時の説明ツール（年齢情報の利用目的や用途、機能制限等の必要性等に関する注意喚起を含む）の開発や、プライバシーポリシーにおける個人情報取得等に関する規定の改訂といった取組が求められる。

青少年の利用者や保護者の視点を踏まえれば、自ら提供した個人情報については的確に把握・管理していくことが望ましいものの、年齢情報の提供先主体である CGM 運営者の適格性や情報の活用方策について個別に判断することは困難であること、提供先主体の範囲は不断に変わり得ること等から、実運用上は携帯電話事業者等による管理に委ねられる部分が多くなるため、提供先主体の選定基準（適格性の判断基準）等については、なるべく明確かつ透明であることが望ましい。例えば、携帯電話事業者等としては、顧客からの照会に対して、当該契約端末の利用者年齢情報の提供先主体である CGM 運営者の名称を開示する等の取組が考えられる。

また、年齢情報を CGM 運営者に対して第三者提供する際には、個人情報保護法第 23 条（ガイドライン第 15 条）に基づく同意取得を行うことが求められる。同法は、第三者提供の事実や情報の種類、第三者提供の手段方法等の事前通知等を要件として、オプトアウトの手続も定めているが、（ア）携帯電話事業者等にすれば、年齢情報の取得時に利用者と接触することから、その際に第三者提供の同意を取得するのが合理的であること、（イ）利用者視点を踏まえればオプトインの方がより丁寧な対応であることから、オプトインによる同意取得がより望ましいと考えられる。

具体的に求められる対応は、年齢情報を取得する対象により異なる。新規契約や端末の機種変更等、青少年利用者又は保護者が販売店等に来店する場合、利用者年齢情報の取得等について説明するとともに、第三者提供に関する同意を取得することが考えられる。他方、一部携帯電話事業者に見られる利用者年齢情報を既に登録済みの青少年利用者又は保護者に対しては、第三者提供についての同意を取得する必要があるため、利用者本人に対して行う手法（例：携帯電話事業者が顧客端末に送付する SMS での案内等）や保護者に対して行う手法（例：請求書同封物を通じた

案内等）等何らかの手法を講じる必要がある[18]。また、利用者年齢情報を取得していない既存の契約者に対しては、機種変更等に先だって直ちに情報を取得するかどうかについては、費用対効果や利用者の利便性等に配慮しつつ検討を進める必要があると考えられる。

ウ　携帯電話事業者等から CGM 運営者へ年齢情報の提供時について

上記イで述べたとおり、利用者にとっては、自らの年齢情報の提供先の選定基準（適格性の判断基準）が明確かつ透明となっていることが望ましいが、それに加え、実際に年齢情報が提供される際には、現にどのような主体に提供されているか等の関係主体による取扱いについても、それが適切であることが確保され、そのことにつき容易に知り得る状態にあることが期待される。また、提供時の仕様が決定される際には、セキュリティ確保の観点から、専門家による点検や確認といったプロセスを踏まえる等、年齢情報の適切な取扱いが行われるよう、あらかじめ検討に必要かつ十分な準備期間を置くことが求められる。

さらに、携帯電話事業者等から提供を受ける年齢情報について、どの程度の粒度が望ましいかが問題となる。年齢情報の取得時には、取得主体の如何にかかわらず、正確性や更新可能性の観点から生年月日が取得されることが望ましいが、当該情報の活用時については、きめ細かい対策を行う上での必要性と個人情報（又はプライバシー）保護の要請のバランスを適切に確保する水準を見いだしていくことが求められる。この点については、年齢情報が個人の属性に関する重要な情報であることや本取組のそもそもの目的に照らし、青少年の福祉犯被害防止の観点から各 CGM 運営者が行おうとする機能制限や注意喚起等の取組にとって必要最小限の粒度に留めることが必要と考えられる。

機能制限等の在り方は、各 CGM 運営者の提供するサービスの仕様により異なるため、一義的に定めることは適切ではないが、例えば携帯電話事業者等においてデータベースを一定の年齢層に分類した上で提供に供する、CGM 運営者から携帯電話事業者等への照会に対し一定の年齢層による回答が行われる等といった適切な運用を行うとともに、そうした年齢情報の活用方策について容易に知ることのできる状態を確保することが望ましい。

エ　CGM 運営者による年齢情報の活用時について

CGM 運営者による利用者年齢情報の活用に際しては、当該運営者が個人情報取扱

[18] 未成年者による同意の効力については、その結果もたらされる効果が CGM サービス上で利用可能な機能の制限等という事実行為であることから、基本的には有効と見なすことができる。他方、個人データの第三者提供という法律行為に着目すれば、民法第５条による未成年者の法律行為に対する制限や第 820 条による親権行使に関する一般規定に基づいて、青少年から同意取得できない場合の保護者による同意も有効と解される。

事業者に該当し、利用する年齢情報が個人情報に該当する場合は個人情報保護法の関連規定（電気通信事業者でもある場合にはガイドライン）を遵守する必要があるため、サイト上における年齢情報の利用目的の明記やプライバシーポリシーの改訂等の対策を講じる必要がある（関連規定は年齢情報取得時の携帯電話事業者の場合と同じと考えられる）。また、仮に個人情報取扱事業者に該当しない場合であっても、年齢情報は利用者にとってセンシティブな情報の一つでもあることから、個人情報の適正な取扱いを求める個人情報保護法の基本理念に基づき、適正な取扱いや利用者への周知について配慮することが求められるのは前述のとおりである。

オ　携帯電話事業者等と CGM 運営者の役割分担について

携帯電話事業者等が取得した情報が CGM 運営者に提供される場合には、取り扱われる情報の信頼性を確保し、利用者に対する説明責任の所在を明確化していくことが求められる。また、本取組を実施するに当たっては、利用者への通知や取得した年齢情報の登録・管理、情報提供システムの構築等のコストが発生することが見込まれる。本取組は、CGM 運営者による年齢認証を補完する取組であるため、携帯電話事業者等のみがそのコストを負担することは望ましくなく、関係者間で適正なコスト分担の在り方も整理される必要がある。

以上を踏まえ、年齢情報の提供に際して、携帯電話事業者等と CGM 運営者の間で締結される契約において定められるべき基本的要素として考えられる以下の項目について、可能な限り明確化が図られる必要がある。

（ア）提供システムの構築等に伴うコスト負担

年齢情報の取得に伴うコストについては、携帯電話事業者等と CGM 運営者の間で協議し、適正なコスト分担の在り方が整理されることが望ましい。

（イ）年齢情報の真正性に関する挙証責任の所在

本取組は、CGM 運営者による年齢認証を補完する自主的取組であり、利用者等に対して強制力を持つものではなく、任意の年齢情報の申告を求めていくため、完全な真正性を担保することは不可能である。したがって、取得・提供される情報の真正性について、携帯電話事業者等が挙証責任を負うことのないようにすべきである。

（ウ）個別サイトの顧客対応の所在

実際に本取組が実施された場合、個別のサイト利用において、利用者からの問い合わせに対応する必要が生じる。個人情報取扱事業者は、個人情報保護法第 31 条等に基づいて苦情の適切かつ迅速な処理を行うように努めることとさ

れており、関係主体がそれぞれの責任を適切に果たしていくことが求められる。例えば、個人情報が活用される場面での苦情対応は当該サイトにおいて処理することが望ましい。

（エ）年齢情報の利用目的、目的外利用の禁止

個人情報取扱事業者として当然に遵守すべき義務であるものの、両者間においてあらかじめ禁止事項や利用目的等を明記することにより責任の所在や内容を明確化することも有効である。

（オ）年齢情報の安全な管理

利用者年齢情報が複数の主体間によって活用される取組であることから、それぞれの取扱主体が年齢情報について適切な安全管理措置を講じることが望ましい。

（カ）適格性判断基準の遵守

当該 CGM 運営者に対して利用者年齢情報を提供するに当たって考慮された適格性の判断基準を、当該 CGM 運営者が契約期間中、遵守し続けることが保証されるべきある。

③ その他の課題について

ア 確実性の向上に向けて

新たな取組が民間の自主的取組として実施される場合、年齢情報の真正性を完全に担保することは原理的に不可能であるが、年齢認証の確実性を少しでも高める観点から、関係者が協力して漸進的な取組を進めていくべきである。

例えば、年齢情報の任意申告要請に応じない青少年利用者への対策として、携帯電話事業者等においては、新規契約等の店頭での説明時に、機能制限を実装しないことによる福祉犯被害の危険性を説明すること等により申告を促していく方法、CGM運営者においては、年齢情報を登録していない利用者の端末からアクセスに対して、年齢情報を申告すべき旨画面上で表示し、デフォルトで機能制限を行う等の手法により申告を促していく方法も考えられる。具体的な取組の方向性については、費用対効果を見極めつつ、新たな年齢認証の仕組みがより実効性あるものとなるよう、関係者による更なる検討の深化が求められる。

イ 利用実態の把握に向けて

また、携帯電話端末が家族によって共有され、名義人と利用者が分かれることにより、青少年の利用実態が不明確となっている事例（「親ケータイ」等）が指摘されており、利用者年齢情報の取得のみならず、フィルタリングの普及にとっても障壁となっていることから、100%の確実性は担保できないながら、漸進的な実態把握に

努めていくことが期待される。

今回の新たな取組は、サイト上では例えば 18 歳以上と詐称されていたとしても、年齢認証の結果、実際には 18 歳未満であると判別された端末の実利用者を本人（18 歳未満の青少年）と判定することが目指されており、当該利用者が、実際には未成年であるにもかかわらず成年のふりをして利用しようとした機能等を制限するものである。これは、危機対応能力が低い青少年が、被害に対する問題意識の欠如から成年のふりをすることに伴う被害を防止する上では有効な取組であるといえる。

他方、サイト上では 18 歳未満であると詐称している利用者が、年齢認証の結果 18 歳以上の利用であると判別された端末からアクセスしている場合、CGM 運営者としては、当該利用者が本人（18 歳以上）なのかその子ども（18 歳未満）なのかを判定することは非常に困難である。これは「親ケータイ」の実態把握が進むことにより徐々に改善していくことが期待されるが、悪意のある成年が未成年のふりをして異性交際を誘引しようとする行為を有効に阻止できないとも指摘されており、何らかの方策の検討が求められている。

３．今後の課題について

（１）更なる取組の推進に向けて

青少年の CGM 利用に関連する事業者は、本 WG における法的整理等を踏まえ、青少年を被害から保護しつつ、適切な利用を一層高めていくという観点から、各自の取組を一層強化していくための検討を進めることが求められる。とりわけ、CGM 運営者においては、管理体制や機能制限の実施状況等青少年保護に向けた取組において事業者間に差が存在しており、中小事業者の事情にも配慮しつつ、業界全体として社会的要請に十分に応えていくべく、取組の底上げにつながるような方策の検討が求められている。

また、実際に新たな取組や、既存の取組の強化が検討されるに当たっては、一定の社会的コストを払って導入される枠組みであることに留意しつつ、既存のものを含めた各取組によりどの程度の被害防止の効果があったのか、利用者や保護者の意識にどのような変化が生じたのか、また実運用上どのような課題が生じたか等について、一定の期間を置いた上で客観的な検証を行っていく必要がある。

（２）様々な環境変化への対応

青少年のインターネット利用を巡る被害状況は、喫緊の社会的課題であり、関係者はできる対策から可及的速やかに講じていくことで、被害低減という結果を生み出していくことが求められている。その一方、技術革新やサービスの進展により、青少年のインターネット利用環境は不断に変化していることを踏まえ、必要に応じて青少年保護対策の在り方について定期的に振り返るなどの柔軟性が求められることも事実である。

例えば、携帯電話利用については、これまでとは異なり携帯電話事業者等によってネットワークや端末の基本仕様をコントロールされないスマートフォンの登場や、Wi-Fi 接続を標準装備した端末の普及など、携帯電話事業者等がフィルタリングの提供や顧客情報管理を行う前提としてきた環境が変化しつつある。また、CGM 利用についても、SNS のような緩やかな会員制を前提としたサービスだけでなく、近年ではツイッターやプロフといったサイトのオープン性が高く、即時性の高いコミュニケーションも爆発的に普及してきており、内容確認や機能制限等の観点から課題を投げかけている。

今回の検討は、あくまで、青少年被害の防止が喫緊の課題となっている社会情勢を背景として、現在の利用環境に即した対策の在り方について検証することとしたものであることから、CGM 利用のなかでも、特に携帯電話経由の CGM に代表されるサービスの利用を念頭に置いている点を再確認しておきたい。

関係主体は、このような利用環境の変化に配慮しつつ、被害実態と活用実態の適切な把握に努めるとともに、有効な対策の在り方について不断の検討を行っていくことが必要である。また、冒頭で述べたとおり、中長期的な観点からは、利用者に対する啓発や保護者に対する意識の向上も極めて重要であり、被害に遭わない、遭いにくい青少年利用者を育成していく観点から、社会全体で取組を強化していくことが重要である。

Ⅱ　ライフログ活用サービスに関する検討について

１．はじめに

ネットワーク機器や携帯端末の高機能化、普及に伴い、個人の生活の履歴であるライフログを利活用したビジネスが注目されてきている。例えば、過去の閲覧履歴等に応じた広告を配信する行動ターゲティング広告や、年齢階層等の属性情報で統計処理した位置情報や購買履歴などである。こうした新ビジネスは今後発展が期待される分野である一方、個人情報保護やプライバシーの保護の点で利用者に不安感や不快感（以下「不安感等」という。）が存在し、新規サービスの展開が円滑に進まない可能性が指摘されている[19]。こうした問題意識に基づき、本研究会では、以下のとおり検討を行った。

まず、我が国と海外の、ライフログを活用したサービス（以下「ライフログ活用サービス」という。）の現状について概観した。

次に、我が国において懸念される法的問題点について、主に個人情報保護とプライバシー保護の観点から検討を行った。この検討を受けて、利用者の不安感等を緩和し、安心なインターネット利用環境を確保する観点から、事業者に一定の配慮を求める原則集（配慮原則）を策定した。ライフログ活用サービスは揺籃期にあり、事業者に過度の負担を課し、当該サービスの発展を妨げることは避けるべきであることから、規制色の強い行政等によるガイドライン化を避けて、緩やかな配慮原則を策定することとし、その上で、事業者における自主的なガイドラインの策定を促すこととした。また、ライフログ活用サービスの態様が多岐に渡ること、今後の発展形態が現段階では想定し難いことも、緩やかな配慮原則の策定にとどめ、各業態における業態固有の事情を加味した自主的なガイドラインの策定を促すこととした理由の１つである。

最後に、ディープ・パケット・インスペクション技術を活用した行動ターゲティング広告について、その態様を概観するとともに、法的課題を整理した。

我が国では、ネットワーク機器や携帯端末の高機能化が進み、先進的なライフログ活用サービスの進展が期待できる環境整備が世界に先駆けて整う一方、利用者の不安感等から新規サービスの展開が円滑に進まない現状が浮かび上がってきた。本提言が、利用者の不安感等の軽減への道しるべとなることで、ライフログ活用サービスの更なる促進を促していく一助となれば幸いである。

---

[19] この点は「通信プラットフォーム研究会」（座長：相田　仁　東京大学大学院教授。平成 20 年２月 27 日から開催。平成 21 年１月 30 日に最終報告書公表。）においても、「・・・こうしたパーソナライズされた（情報を利用する）新ビジネスは潜在的に高い市場性があるものと考えられるが、他方、利用者個人の属性、履歴（検索履歴、購入履歴、行動履歴）のデータやそのデータの分析結果を活用することとなるため、どこまで利用が許容されるかについては、慎重な検討が必要である。」と指摘されている。

２．我が国のライフログ活用サービスの現状[20]

これまで、ライフログは積極的な利活用がほとんどなされてこなかったが、ネットワーク機器や端末の高機能化に伴い、行動ターゲティング広告への利用や、統計情報への加工などに積極的に利活用されるようになってきた。以下では、ライフログを定義した上で、現時点でのライフログ活用サービスについて、（１）利用者の興味・嗜好にマッチした情報を提供するサービス、（２）統計情報を提供するサービスの２つに区分して概観する。

（１）ライフログとは何か

ライフログは、蓄積された個人の生活の履歴を指す。ライフログは広範な概念であり、およそ考え得る蓄積された個人に関する情報の全てが含まれる。デジタル化されたものに限っても、ウェブサイトの閲覧履歴、電子商取引サイトにおける購買・決済履歴、携帯端末の GPS（Global Positioning System 全地球測位システム）により把握された位置情報、携帯端末や自動車に搭載されたセンサー機器により把握された情報、デジタルカメラで撮影された写真、ブログに書き込まれた日記、SNS(Social Networking Service)サイトに書き込まれた交友関係の記録、非接触型 IC を内蔵した乗車券による乗車履歴等から抽出された情報が含まれる。

従来、デジタル化されたライフログの取得シーンは、利用者による契約者情報の入力やクッキー技術を用いた閲覧履歴等の把握に限られ、その利活用も積極的なものではなかった。しかし、近年の技術革新により、多様なライフログを簡便に取得し積極的に利活用したサービスが可能になりつつある。例えば、ライフログを分析し利用者の興味・嗜好にマッチした広告等の配信や、複数のライフログを集約した統計情報の作成など、積極的な利活用が行われつつある。

ライフログの積極的な取得・利活用を支える技術は以下のとおりである。まず、センサー機器の発達と端末への実装により、多様なライフログを簡便に取得することが可能になった。次に、大容量のストレージが安価に利用できるようになったことにより、ライフログの大量取得・保存が可能になった。さらに、大容量のデータを検索、分析、送付、公開する技術が進展したことにより、より洗練された情報を提供できるようになった[21]。これに加え、ネットワークの高度化と低廉化により、大量のデータを安価に流通させることができるようになったことが、ライフログの積極的な取得・利活用を進展させている。

---

[20] 本節の記述は、寺田オブザーバ提出資料を基にしている。なお、詳細は、寺田眞治『ライフログビジネス』(平成 21 年、インプレスＲ＆Ｄ)を参照。

[21] Gordon Bell and , Jim Gemmell *“Total Recall: How the E-Memory Revolution Will Change Everything”* (Dutton Adult)(2009)

（２）ライフログ活用の２つの方向性

上述のとおり、ライフログを積極的に利活用したサービスが行われるようになってきたが、現在、技術革新に伴い、サービスの態様が不断に変化、発展、多様化している状況である。よって、現時点でライフログ活用サービスの外縁を画定することは困難であると言わざるをえない。本提言では、便宜的に、①利用者の興味・嗜好にマッチした情報を提供するサービスと、②統計情報を提供するサービスに区分して整理することとした。この区分にそぐわないサービスも存在するものの、当面の分析を行う上で有益と考えられるため、以下では、この２つのサービスについて、例を挙げながら概観する。

①　利用者の興味・嗜好にマッチした情報を提供するサービス

利用者のライフログを取得・蓄積し、そこからの興味・嗜好を分析し、これにマッチした広告等を表示したり、アドバイス等の情報を提供したりするサービスである。このサービスで提供される広告やアドバイスは、単純な広告やアドバイスと比較して、より利用者の嗜好を踏まえたものとなっている。現状、行動ターゲティング広告及び位置情報を用いた行動支援型サービスが代表的なサービスだが、今後、センサー機器の発達に伴って多様なライフログが取得できるようになることが想定され、これに伴って、先進的なサービスが発展することが期待されている。例えば、体内に微細なセンサーを埋め込み、生体データを取得・分析することで、健康維持に係るアドバイスを提供する等の先進的なサービスが検討されている。

以下では、現在の代表的なサービスである行動ターゲティング広告及び位置情報を用いた行動支援型サービスについて概観する。

ア　行動ターゲティング広告

行動ターゲティング広告[22]とは、蓄積されたインターネット上の行動履歴（ウェブサイトの閲覧履歴や電子商取引サイト上での購買履歴等）から利用者の興味・嗜好を分析して利用者を小集団（クラスター）に分類し、クラスターごとに広告を出し分けるサービスを指す。なお、通常、広告媒体であるウェブサイトの管理者が、自らのウェブサイト上のスペースを、広告掲載スペースとして対価と引き替えに提供する場合のみを「広告」と呼び、自らのウェブサイト上のスペースを自らの宣伝のために利用している場合は、「レコメンド」[23]と呼ぶ[24]。

---

[22] 行動ターゲティング広告とは言えないが、ターゲットを絞り込んだ広告としては、検索結果に応じて広告を表示する検索連動型広告（例：グーグル(株)の Google AdWords）や、ウェブページの内容に応じて広告を表示するコンテンツ連動型広告（例：グーグル（株）の Google Adsense）がある。行動ターゲティング広告に検索連動型広告やコンテンツ連動型広告の要素を組み合わせた広告も存在する。

[23] レコメンドの中には、このように個人の興味・嗜好を分析する行動ターゲティングを行うものもあるが、閲覧ページや閲覧ページ内の商品に合わせて情報を表示するコンテンツ連動型が大半である。

[24] 例えば、新聞社の提供するウェブサイトは、通常、対価をとってそのスペースを他者に提供しているため、そのウェブサイト上では広告が提供されていることになる。個人のウェブサイト上に掲載されるバナー広告も広告となる。これに対し、電子商取引サイト上で提供される、商品についての宣伝は、通

広告であろうとレコメンドであろうと、取得・蓄積される行動履歴や、その利活用の方法に大きな違いはない。その手法はおよそ以下のとおりである。利用者が、広告が掲載された媒体にインターネットを通じてアクセスした際に、クッキー技術等を利用して、利用者の使用するブラウザや携帯端末等に固有の識別番号を割り振る[25]。利用者が媒体上でウェブページの閲覧、情報の入力等の行動を行うたびに、その履歴を識別番号に紐づけて保存・蓄積する。その保存・蓄積された行動履歴を利用して、何らかのプログラムに基づいて利用者の興味・嗜好を分析して利用者をクラスターに分類する。クラスターごとに、興味・嗜好にマッチした広告や情報をブラウザや携帯端末等に配信する。

なお、行動ターゲティング広告を配信する事業者と、広告スペースを提供する媒体を管理する事業者は異なる場合が多い。この場合、通常、配信事業者は、複数のウェブサイトの広告スペースに広告を配信するアドネットワークを形成している。こういった第三者による広告配信（第三者配信）には、広告配信事業者にとって、複数のウェブサイトへの訪問履歴を把握し[26]、より詳細に個人の興味・嗜好を分析することで、効果の高い広告を配信できるようになることや、媒体にとっては、コストのかかる分析や広告配信をアウトソースできるようになること等の利点があり、今後も発展していくことが予想される。ただし、一方で、個人の興味・嗜好がより詳細に分析されることをプライバシーへの脅威ととらえる向きもあり、米国を含む海外では、プライバシーの観点から第三者配信についての議論がなされている。

イ　行動支援型サービス

携帯電話事業者は、利用者がほとんど常に携帯端末を携帯しているという利点を生かし、利用者の行動を支援する先進的なサービスを展開しつつある[27]。行動支援型サービスも、行動ターゲティング広告と同様、保存・蓄積された行動履歴や属性情報を基に、何らかのプログラムに基づいて利用者の興味・嗜好を分析し、分析結果に基づいて、興味・嗜好にマッチした情報をブラウザ、携帯端末や機器等に配信するものである。しかしながら、行動支援型サービスでは、携帯端末に GPS をはじめとした各種センサー機器を実装することにより、より現実世界に近いライフログが取得可能になっていること、利用者が常に携帯している携帯端末というインター

常、対価をとってそのスペースを他者に提供しているわけではないからレコメンドとなる。ただし、電子商取引サイトの中でも、複数の電子商取引サイトをまとめたサイト（電子市場）の場合は、スペースを他者に提供しているとも考えられ、広告とレコメンドの区別は困難な場合がある。

[25] 携帯電話を利用したインターネットの場合は、通常、クッキーは用いられず、いわゆる契約者固有 ID を用いて端末等の識別を行っている。

[26] 配信事業者は、自ら訪問履歴を取得する場合と、他の事業者から訪問履歴の提供を受ける場合がある。

[27] 現在、展開されている位置情報を用いた行動支援型サービスの代表例には、（株）NTT ドコモの「i コンシェル」がある。また、実験として、総務省のユビキタスネットワーク制御・管理技術の研究開発(Ubila プロジェクト）の一環として行われたケータイ de ライフログ（(株)KDDI 研究所）や、経済産業省の情報大航海プロジェクトの一環として行われたマイ・ライフ・アシストサービス（(株)NTT ドコモ）がある。

フェイスを利用できることから、利用者に対してタイムリーに情報を提供することが可能になっている。

現在では、GPS 等を通じて取得した位置情報を用いた行動支援型サービスが実用段階に入っているが、今後は、センサー機器の発達に伴って、生体情報や環境情報を活用したサービスも可能になるだろう。センサー機器の実装対象も、携帯端末だけでなく、カーナビゲーションシステムやゲーム機器に拡がりつつある。今後の発展が期待される分野である。

② 統計情報を提供するサービス

個人からライフログを取得し、それを集約して統計処理することにより、統計情報を作成、提供するサービスである。従来から、契約者情報等から統計情報を作成し、これをマーケティングデータとして利用することは行われてきたが、収集されるライフログの数や種類が少ないことから、その利用は限定的なものにとどまっていた。

しかしながら、携帯電話事業者や SNS 事業者に代表されるライフログの大規模収集者の出現、センサー機器の発達と端末への実装による取得可能なライフログの種類の多様化等により、より正確かつ多様な統計情報をより効率的に作成することが可能になってきている。

携帯電話事業者に関していえば、例えば、携帯電話端末への GPS の実装により取得された位置情報を、性別や年齢等の属性情報と組み合わせることができれば、人々の行動に関する正確な統計情報を作成することが可能となる。今後、センサー機器の発達と端末への実装化が進めば、例えば、気象情報、渋滞情報等の正確な統計情報を効率的に作成することが可能になってくるだろう。

また、携帯電話事業者と同じく、大手 SNS サイトも、大規模な顧客数を有する[28]点で、統計情報の提供事業者としてのポテンシャルを有している。大規模 SNS サイトは、年齢、住所といった情報のみならず、細かな興味・嗜好に関する情報[29]を取得しており、多様で良質な統計情報を作成することが可能であろう。

---

[28] 例えば、大手 SNS サイトである(株)ミクシィの mixi の利用者数は約 1,858 万人、グリー(株)の GREE は約 1,673 万人、(株)ディー・エヌ・エーのモバゲータウンは約 1,581 万人となっている。(いずれも平成 21 年 12 月末現在。各社 IR 情報による。)

[29] 例えば、mixi では、趣味は必須項目として登録し、好きな映画・スポーツ・音楽・休日の過ごし方といった嗜好情報を任意で登録できるようになっている。

３．諸外国の対応状況[30]

諸外国においても、ライフログを積極的に収集して利活用する取組が行われつつある。米国におけるLifelog project[31]やMy LifeBits Project[32]など、先進的なライフログ活用サービスの研究も行われているが、現状、サービスとして最も普及しているのは、日本と同様に、ウェブページ上での行動ターゲティング広告やレコメンド機能（行動ターゲティング広告等）の利用者の興味・嗜好にマッチした情報を提供するサービスの提供である。行動ターゲティング広告等に対する諸外国の対応状況は以下のとおりである。

（１）米国

行動ターゲティング広告とプライバシーの関係は、2000年に発生したいわゆるDouble Click事件[33]以来注目され、2007年には米国連邦取引委員会（FTC）が、事業者が自主的なガイドラインを作成するに当たっての根本的な原則となる「オンライン上の行動ターゲティング広告に関するプライバシー原則」（Online Behavioral Advertising Privacy Principles）の案を公表するに至った。この原則は、その後、パブリックコメントを経て修正され、2009年に「スタッフレポート：オンライン上の行動ターゲティング広告に関する自主行動原則」（FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising）として公表されている。原則は、データ収集の詳細の明示や収集の可否に対する利用者による決定を内容としている。

複数の業界団体が、FTCによる原則を受けて自主的なガイドラインを策定した[34]。表１は、FTCによる原則と業界団体による代表的なガイドラインとの比較を示したものであ

---

[30] 本章の記述は、総務省情報通信政策研究所『行動ターゲティング広告の経済効果と利用者保護に関する調査研究報告書』（平成22年３月）を基にしている。

[31] 国防総省国防高等研究計画局によるLifelog projectは、個人の生活における全行動を記録したデータベースを構築するという、野心的なプロジェクトであった。なお、本プロジェクトは、市民団体等からプライバシーに関する激しい抗議を受け、2004年にプロジェクトは中止されている。

[32] マイクロソフトによるMy LifeBits Projectは、閲覧したウェブページ、本、視聴したDVDやCDなど、個人の生活の所作の全てをデジタル化してデータベースを構築し、後からアクセスできるシステムを構築する試みである。
My LifeBits, http://research.microsoft.com/en-us/projects/mylifebits/default.aspx（最終訪問日2010年４月２日）

[33] Double Click社のサービスとプライバシーの関係が問題となった事件。同社において、インターネット利用者が同社の提携するウェブサイトにアクセスした際に、ハードディスクにクッキーを埋め込んだ行為が、電子通信プライバシー法等に違反するとして訴訟が提起された。FTCによる調査、利用者団体（EPIC）による連邦地裁への集団訴訟及び10州の検事総長による調査に発展したが、いずれも2002年に和解により終了している。

[34] Interactive Advertising Bureau(IAB)による”Interactive Advertising Privacy Principle)”、Network Advertising Initiative(NAI)による”The Network Advertising Initiative`s Self-Regulatory Code of Conduct”、４団体（American Association of Advertising Agencies(4A`s)、Association of National Advertisers(ANA)、Direct Marketing Association(DMA)、Council of Better Business Bureaus(CBBB)、IAB）による共同ガイドライン”Self-Regulatory Principles for Online Behavioral Advertising”がある。

る。

Double Click 事件の他にも、2007 年の Facebook 社のサービスをめぐる紛争事例[35]、NebuAd 社や AdZilla 社による DPI 技術を用いた行動ターゲティング広告をめぐる紛争事例[36]など、2000 年代後半以降、行動ターゲティング広告とプライバシーをめぐる紛争が複数発生している。

表１　FTC による原則と各業界団体よるガイドラインの比較

	FTC	IAB	NAI	４団体共同
対象データ	利用者をターゲットとした広告に提供するためのデータ。ただし、①第三者の手にデータが渡らないもの、②データが蓄積されない、コンテクスト広告は対象外。	インタラクティブ広告に用いるデータ	行動ターゲィング広告、マルチサイト広告、及び、広告デリバリー＆リポート行為のための情報 （個人識別情報と個人を識別しない情報を区別）	オンライン上の行動ターゲティング広告に関わるデータ。ただし、①第三者の手にデータが渡らないもの、②データが蓄積されない、コンテクスト広告は対象外。
対象事業者	・Web サイトの開設者 ・行動ターゲティング広告向けデータの保持者	インタラクティブ広告の実施者	行動ターゲティング広告の実施者	・Web サイトの開設者（「開設者」） ・Web サイトの開設者からデータを受け取り行動ターゲティング広告を提供する者（「広告実施者」） ・インターネットアクセス、ツールバー、ブラウザ、その他の上記に類する機能を提供するアプリケーション等のサービスの提供者（「サービス提供者」）
内容				
データ収集の詳細の明示及び収集の可否に対する利用者による決定	・Web サイトの開設者に対し、データ収集の詳細の明示及び収集の可否に対する利用者による決定を要求	・データ収集の詳細の明示及び収集の可否に対する利用者による決定を要求	データ収集の詳細の明示、及び、個人識別性の有無によりオプトイン又はオプトアウトが出来なければならない場面を区分して明示	・「開設者」、「広告実施者」に対し透明性の原則を要求 ・「広告実施者」に対して、利用者による管理の原則を要求

[35] Facebook 社の提供するソーシャルネットワークサービス Facebook において提供された行動情報の共有機能”Beacon”が利用者の反発を招き、カリフォルニア州北部地区連邦地裁に集団訴訟が提起された事件。2009 年に和解が成立している。

[36] 利用者の同意なく利用者のインターネット上での行動をマーケティングに利用する行為が、電気通信におけるプライバシー保護法、コンピュータ詐欺と濫用に関する法律及びカリフォルニア州法に違反するとして、NebuAd 社を相手取った集団訴訟がカリフォルニア州北部地区連邦地裁に提起された事件。2009 年に NebuAd 社が破産したため訴訟が中断されている。AdZilla 社とその親会社の Conductive Corporation 社も、NebuAd 社と同様の理由で 2009 年に訴訟が提起されている。

データセキュリティ及び保持期間の限定	・行動ターゲティング広告のためのデータを保持する事業者に対して、適切なセキュリティを要求 ・行動ターゲティング広告のためのデータを保持する事業者に対して、当該データの保持期間を正当な業務に用いる範囲内又は司法上必要な範囲内に限定	適切なデータセキュリティをデータの機微の程度に応じて要求	・適切なデータセキュリティをデータの機微の程度に応じて要求 ・データの保持期間を当該データの保持期間を正当な業務に用いる範囲内又は司法上必要な範囲内に限定	・「サービス提供者」等に対してデータセキュリティの原則を要求。
ポリシー変更時の同意の再取得	行動ターゲティング広告のためのデータを保持する事業者に対して、ポリシーの実質的な変更時の同意の再取得を要求	（記載なし）	個人識別情報と非識別情報で扱いを分けオプトイン又は、オプトアウトにより利用者の同意を取るようになっている	全ての者に、実質的変更に関する原則を要求
機微情報の対象及びその保護	・機微情報の収集であることに関する利用者の事前の同意を要求 ・定義は厳密に定めず、意見招集を行い続ける	（記載なし）	・機微の程度により適切なデータセキュリティの実施を要求 ・子供のデータに関し、保護者の同意を追加的に要求。	全ての者に、機微情報に関する原則を要求。とりわけ、子供のデータに関しては、保護者の同意を追加的に要求。
ＦＴＣ原則にない、その他の行動原則		・政府機関に対する説明責任を果たすことを要求 ・利用者に対する教育の実施を要求（教育の原則）	・利用者に対する教育の実施（透明性の原則）	・全ての者に、利用者に対する教育の実施（教育の原則） ・関連団体に、原則の見直し及び改善の実施を要求（説明責任の原則）

（出典：総務省情報通信政策研究所『行動ターゲティング広告の経済効果と利用者保護に関する調査研究報告書』(平成 22 年３月) 94～95 ページより抜粋）

（２）欧州

欧州においても、行動ターゲティング広告等を含むライフログ活用サービスに関するプライバシーの課題に関心が払われている。例えば、近年では、2009 年 11 月に、クッキー及び個人情報の利用の事前通知を分かりやすい説明によって行うことを義務づけた Telecoms Reform Package が、欧州議会で採択されている[37]。

[37] これにより、加盟国諸国は、18 ヶ月以内に国内法にする義務を負う。

欧州域内では、特にイギリスにおいて、行動ターゲティング広告とプライバシーの問題が顕在化している。2008 年に発生したいわゆる Phorm に関する事例[38]では、欧州委員会が、Phorm 社の DPI 技術を用いた行動ターゲティング広告サービスについて、1995 年 EU 個人データ保護指令や 2002 年 EU 電子通信プライバシー指令に違反するとして侵害手続を進めている。とりわけ、イギリスの国内法では、①通信傍受に対する苦情に対応するための独立した監督機関が設置されていない、②通信当事者が同意を与えたと信じる合理的な理由があれば傍受が可能である、③意図的な傍受のみが規制されている点が問題視されている。

また、イギリスにおいては、2009 年に業界団体が Internet Advertising Bureau(IAB)が、オンライン上の行動ターゲティング広告に関する行動原則”Good Practice Principles for Online Behavioural Advertising”を公表している。原則は、情報提供の原則、選択の原則、教育の原則、機微な情報区分を内容としている。

[38] Phorm 社が、2008 年に英国の大手 ISP である BT、VirginMedia、TalkTalk に対して DPI 技術を活用した行動ターゲティング広告の技術を提供することを公表した事例。これに先駆ける 2006 年と 2007 年に、すでに BT と試験運用を実施していた。

４．我が国において懸念される法的問題

第２章において概観したとおり、ネットワーク機器や端末の高機能化に伴い、ライフログは、行動ターゲティング広告への利用や、統計情報への加工など、積極的に利用されるようになっている。一方で、ライフログ活用サービスについて、個人情報保護やプライバシー保護の観点から懸念が指摘されている。以下では、この２点について法的課題を整理することとする。

なお、先述のとおり、ライフログ活用サービスの態様は不断に変化、発展、多様化しており、現時点でライフログ活用サービスの外縁を画定することは困難である。よって、最も主要なサービスである行動ターゲティング広告、レコメンド機能及び位置情報を用いた行動支援型サービス（以下「行動ターゲティング広告等」という。）を念頭において、懸念される法的課題を検討することとする。

（１）個人情報保護法との関係

「個人情報の保護に関する法律」（以下「個人情報保護法」ないし単に「法」という。）は、「個人情報取扱事業者」に対して、「個人情報」、「個人データ」及び「保有個人データ」の取扱いに関して様々な義務を課している。ライフログ活用サービスの提供者が、同法にいう「個人情報取扱事業者」に当たる場合、法第15条以下の義務規定[39]が適用される。

以下では、行動ターゲティング広告等の提供者が「個人情報取扱事業者」として個人情報保護法上の義務が課せられるかについて検討する。行動ターゲティング広告等の提供者が「個人情報取扱事業者」に当たるのは、「個人情報データベース等を事業の用に供している」場合である[40]から、まず取り扱う情報が個人情報に当たるかを検討する。次に、行動ターゲティング広告等の提供者が事業の用に供しているデータベースが、個人情報データベース等（「個人情報を含む情報の集合物」であって、「特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの」（法第２条第２項））に当たるか否かについて検討することとする。

---

[39] 個人情報の取扱いについて、利用目的の特定（第 15 条）、利用目的による制限（第 16 条）、適正な取得（第 17 条）及び取得に際しての利用目的の通知等（第 18 条）が、個人データの取扱いについて、データ内容の正確性の確保（第 19 条）、安全管理措置（第 20 条）及び従業者の監督（第 21 条）、委託先の監督（第 22 条）及び第三者提供の制限（第 23 条）が、保有個人データの取扱いについて、保有個人データに関する事項の公表等（第 24 条）及び開示、訂正等、利用停止等（第 25～27 条）が、それぞれ適用される。

[40] ただし、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６か月以内のいずれの日においても 5 千を超えない者は除く。法第２条３項、個人情報の保護に関する法律施行令第２条）

① 個人情報に当たるか

ア 個人情報とは

「個人情報」とは、「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。）」（法第２条第１項）をいい、個人識別性の有無が「個人情報」該当性の要件となる。

イ 行動ターゲティング広告等への適用

一般に、行動ターゲティング広告等においては、利用者の興味・嗜好の分析に必要な、（ア）ウェブページ上の行動履歴（閲覧履歴、購買履歴等）や（イ）位置情報と、行動履歴の取得及び広告等の配信に必要な、（ウ）クッキー技術を用いて生成された識別情報や(エ)携帯端末の識別に必要な契約者固有IDのみが必要であり、特段の事情がない限り、これらの情報自体は個人識別性を具備しない。よって、通常、行動ターゲティング広告等の事業者は個人情報取扱事業者には該当しないと考えられる[41]。

ただし、他の情報と容易に照合して特定の個人を識別できる場合には、（ア）～（エ）の情報は個人情報に該当する。例えば、コンピュータ上に保存された（オ）氏名等の契約者情報のデータベースと（ア）～（エ）の情報とを容易に連係して用いることができる場合にあっては、（ア）～（エ）の情報は個人情報に該当する。（表２は、行動ターゲティング広告等の事業者が取得し得る情報に個人識別性が認められるかをまとめたものである。）また、他の情報と容易に照合して特定の個人を識別できる立場で、第三者から（ア）～（エ）の情報を取得した場合（いわゆる「名寄せ」）にあっても、（ア）～（エ）の情報は個人情報に該当する[42]。

また、（ア）ウェブページ上の行動履歴（閲覧履歴、購買履歴等）が相当程度長期間にわたって大量に蓄積された場合等、個人が容易に推定可能になる可能性がある。また、（イ）位置情報も、相当程度長期間にわたって時系列に蓄積された場合等、個人が容易に推定可能になる可能性がある。

41 もちろん、行動ターゲティング広告等の事業者が、行動ターゲティング広告等以外において、何らかの個人情報データベース等を事業の用に供している場合には、個人情報取扱事業者に該当することとなる。

42 個人識別性の有無は、個々の事業者を基準として相対的に決せられる。岡村久道「新訂　個人情報保護法」（商事法務、平成 21 年）76 頁参照。

表２　行動ターゲティング広告等の事業者が利用者から取得し得る情報

	情報	含まれる情報	個人識別性
行動ターゲティング広告等に必要な情報	（ア）ウェブページ上の行動履歴（閲覧履歴、購買履歴等）	利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴。	通常、個人識別性を有しない。 （相当程度長期間にわたって大量に蓄積される場合等、その態様によっては個人が推定可能になる可能性がある。）
	（イ）位置情報	携帯端末やカーナビゲーションシステムに搭載されるGPS機器によって計測される位置情報 携帯端末から基地局に送信される位置登録情報	通常、個人識別性を有しない。 （相当程度長期間にわたって時系列に蓄積された場合等、その態様によっては個人が推定可能になる可能性がある。）
	（ウ）クッキー技術を用いて生成された識別情報	ポータルサイト、CGMサイト等、各種サービスをネット上で提供するサイトにおいて、ログインなしに利用者（正確にはブラウザ）を特定するために利用される情報	個人識別性を有しない。
	（エ）契約者固有ID	利用者が、携帯電話インターネット上のウェブサイトを閲覧した際に、ウェブサイト側に送信される、ブラウザや端末を特定する情報[43]	個人識別性を有しない[44]。
行動ターゲティング広告等に必ずしも必要ではない情報	（オ）氏名、住所等の契約者情報	電子商取引や電気通信役務等の契約において、電子商取引事業者や電気通信事業者が契約者から取得する情報。一般的に、氏名、性別、住所、年齢、電話番号等の情報や、クレジットカード番号等の個人信用情報が含まれる。	個人識別性を有する。
	（カ）ログインの際に用いる識別情報	ポータルサイト、CGMサイト、電子商取引サイト等、各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報	利用者がID自体に氏名等の個人識別性を有する情報を使用していない場合等を除き、個人識別性を有しない。

② 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したものに当たるか

①で検討したとおり、通常、行動ターゲティング広告等の事業者が取得・利用する情報は個人情報に該当しない。しかし、個人情報[45]に該当する前述の例外的なケース

[43] 契約者固有 ID の機能や利用方法は、携帯電話事業者ごとに差異がある。

[44] 契約者固有 ID については、複数のコンテンツプロバイダに対して同一の契約者固有 ID が送出されるため、各コンテンツプロバイダが各々保有するウェブページ上の行動履歴や位置情報を、同一 ID に紐付けて集積することが極めて容易との指摘がある。また、各コンテンツプロバイダにとっては、契約者固有 ID を、契約者情報等の個人情報と紐付けることが容易に可能であり、同一の契約者固有 ID に紐付けて集積されたウェブページ上の行動履歴等が比較的容易に個人識別性を獲得するとの指摘がある。

[45] この場合は、通常、個人情報を含む情報の集合物にも該当する。

の場合であって、（オ）を含む各構成要素を連結して管理して、お互いに電子計算機を用いて検索することが可能な態様で取り扱っている場合には、行動ターゲティング広告等の事業者は、個人情報データベース等を事業の用に供しているといえる。

③　まとめ

通常、行動ターゲティング広告等の事業者の取り扱う情報は、それ単独では個人情報に該当しないため、行動ターゲティング広告等の事業者は個人情報取扱事業者には該当しないと考えられる。しかしながら、例外的なケース（（オ）氏名等の契約者情報のデータベースと（ア）～（エ）の情報を容易に連係して用いることができる場合等、他の情報と容易に照合して特定の個人を識別できる場合や、（ア）ウェブページ上の行動履歴（閲覧履歴、購買履歴等）が相当程度長期間にわたって大量に蓄積されて個人が容易に推定可能になる可能性がある場合）には、各構成要素を連結して管理して、お互いに電子計算機を用いて検索することが可能な態様で取り扱っている場合に限り行動ターゲティング広告等の事業者は個人情報取扱事業者に該当し同法に基づく対応が求められることとなる。

＜参考：匿名化＞

行動ターゲティング広告や統計情報を提供するサービスについては、必ずしも個人を識別する必要がないことから、個人識別性を具備する情報に対して匿名化[46]を行うことで個人識別性を喪失させ、流通や利活用を容易にする取組が検討されている。

個人識別性を備える情報には、（オ）契約者情報等の、それ単独で個人識別性を有する場合と、（ア）利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴から生じ得る場合が存在する。

現在、個人識別性の獲得リスクを回避するために、各方面においてk-匿名化[47]等の処理のアプローチが検討されているが、課題も指摘されており、客観的に、完全に個人識別性を喪失させるのは容易ではなく、結局、ケースバイケースの判断によらざるを得ない。

なお、匿名化を行って個人識別性を喪失させる行為は個人情報の利用に当たらない

[46] なお、正確には、匿名化には、契約者情報のような個人識別性のある情報を完全に抹消する方法（連結不可能匿名化）と、同情報を番号・符号に置き換えて分離する方法（連結可能匿名化）がある。前者の場合には、匿名化によって個人識別性を喪失し個人情報への該当性を失う。これに対し、後者の場合は個人情報に該当する場合と該当しない場合がある。番号・符号を他の情報と容易に照合することによって特定の個人を識別し得る場合は、個人情報に該当する。詳細については、「経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン」（平成 17 年）参照。

[47] 行動履歴の一部を一般化やあいまい化することにより、組み合わせることで個人を推定できる可能性のある情報（準識別子と呼ぶ。）の組み合わせ（準識別子群）と同じ準識別子群を少なくともｋ個以上存在する状態を作り出す処理。この状態をｋ-匿名性と呼び、このデータ処理をｋ-匿名化と呼ぶ。

ため、個人情報取扱事業者は、匿名化を個人情報保護法上の「利用目的」として、特定する必要はないと解される[48]。

個人情報保護法の規定する利用目的の特定（法第15条）[49]の趣旨は、不必要に又はみだりに個人情報を取り扱うことを制限するとともに、個人情報の取扱いの透明性を図り、本人自らが権利利益の侵害を未然に防止するために必要な対応をとることができる環境を整備しようとするものである[50]。一方、匿名化を行って個人識別性を喪失させる行為は、個人の権利利益の侵害のおそれを小さくするものであり、利用目的の特定等の義務を課さない方がむしろ法の趣旨に沿うと考えられる。

この点について、従来必ずしも明確ではなかったため、電気通信事業における個人情報保護に関するガイドライン（平成16年総務省告示第695号）の解説に明記することが求められる[51]。

[48] 利用目的に係る個人情報取扱事業者の義務は、利用目的の特定（法第 15 条）の他、利用目的による制限（法第 16 条)、取得に際しての利用目的の通知等（法第 18 条）がある。

[49] 電気通信事業における個人情報保護に関するガイドラインにあっては、第 5 条で利用目的の特定が規定されている。

[50] 園部逸夫編集、藤原靜雄＋個人情報保護法制研究会著「個人情報保護法の解説」（株）ぎょうせい、平成 15 年を参照。

[51] 匿名化処理を利用目的として特定する必要がないことを定めたガイドラインには、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成 16 年 12 月、厚生労働省）がある。

（２）プライバシー等との関係

プライバシーについて一般的に規定した法律は存在しないが、判例法理上、プライバシーは法的に保護されるべき人格的利益として承認されてきた。

プライバシー侵害の問題を扱ったリーディング・ケースは、『宴のあと』事件である[52]。東京地方裁判所は、昭和 39 年 9 月 28 日の判決の中で、プライバシー権を「私生活をみだりに公開されないという法的保障ないし権利」と定義づけ、その侵害が認められるための要件を、「公開された内容が（イ）私生活上の事実または私生活上の事実らしく受け取られるおそれのあることがらであること、（ロ）一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められることがらであること、換言すれば一般人の感覚を基準として公開されることによって心理的な負担、不安を覚えるであろうと認められることがらであること、（ハ）一般の人々に未だ知られていないことがらであることを必要とし、このような公開によって当該私人が実際に不快、不安の念を覚えたことを必要とする」と述べている。

『宴のあと』事件の判断基準は、その後の裁判実務で長期間にわたり採用されてきたが、最近では、プライバシーの対象となる情報は拡大傾向にある。例えば、早稲田大学講演会名簿提出事件[53]において、最高裁判所は、平成 15 年９月 12 日判決において、氏名、住所、電話番号等の単純な個人識別情報であったとしても、「本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり、そのことへの期待は保護されるべきものであるから、本件個人情報は、上告人らのプライバシーに係る情報として法的保護の対象となるというべきである」と判示している。現在では、前掲『宴のあと』事件の裁判例に掲げられた要件は必ずしも踏襲されてない。

①　プライバシー侵害の有無・程度

前述のとおり、行動ターゲティング広告等においては、一般的に、ウェブページ上の行動履歴（閲覧履歴、購買履歴等）や位置情報が取得・利活用されている。

ウェブページ上の行動履歴は、閲覧履歴や購買履歴等が相当程度蓄積された場合には、個人の関心事、嗜好、思想傾向や主義を推し量ることが可能であるため、個人の内面に関わるような秘匿性の高い情報と考えられる[54]。また、位置情報も、その情報が相当程度の期間にわたって時系列に連結された場合には、個人の生活の態様が明ら

[52] 東京地裁昭和 39 年 9 月 28 日判決。

[53] 最高裁平成 15 年 9 月 12 日第二小法廷判決。

[54] 最高裁平成 20 年 3 月 6 日第一小法廷判決（住基ネット事件）では、住基ネットによって管理、利用等される本人確認情報について、「個人の内面に関わるような秘匿性の高い情報とはいえない」といえるか否かに触れており、要保護性の高低に関する判断要素としている。岡村久道「新訂　個人情報保護法」（商事法務、平成 21 年）35 頁参照。

かになる可能性が高い。したがって、これらの情報は、他人にみだりに知られたくないと考えることは自然なことであるということができる。よってウェブページ上の行動履歴や位置情報は、その取扱いの態様によっては、プライバシーに係る情報として法的保護の対象となる可能性がある。

なお、ウェブページ上の行動履歴や位置情報は、一般にそれ単独では個人識別性を有しないため、特定個人のプライバシーの侵害が成立しないとの指摘がある[55]。確かに、個人の興味・嗜好や生活の態様がある程度明らかであったとしても、それらが誰の情報であるかが他者から判断できない場合には、特定個人のプライバシー侵害が問題となる場面は限定されると解される。しかしながら、個人識別性のない情報であっても、行動履歴等の情報が大量に蓄積されて個人が容易に推定可能になるおそれがあることや、転々流通するうちに個人識別性を獲得してしまうおそれがあることから、現時点で情報に個人識別性がないことをもって、プライバシーとしての保護が完全に失われると考えるのは相当ではない。

具体的なプライバシーの侵害の有無と程度は、ライフログの取扱いの態様を総合考慮する必要があるところ、行動ターゲティング広告等の提供に係るライフログの取扱いの態様は多岐に渡るため、その判断はケースバイケースとせざるを得ない。主要なケースについて検討してみると、例えば、相当程度長期間にわたって行動履歴や位置情報を蓄積して特定個人の嗜好や生活の態様を詳細に分析する場合には、プライバシー侵害が成立する可能性がある。また、利用者の許諾のない行動履歴や位置情報の第三者への提供や、インターネット上での公開の場合にも、プライバシー侵害が成立する可能性がある[56]。

そこで、かかるリスクを低減すべく、事業者には、行動履歴や位置情報等の取扱いについて透明性を高めることや、利用停止や取得停止等の利用者関与の手段を提供することなど、相応の配慮が求められる[57]。

---

[55] 新潟地裁平成 18 年 5 月 11 日判決（防衛庁リスト事件）は、「原告のプライバシー等が侵害されたというためには、そのリストに記載された原告に関する個人情報が個人識別性を有することが必要である。」と判示して、プライバシーと個人識別性の関係に言及している。

[56] プライバシーに関連する問題の 1 つに、いわゆる「肖像権」の侵害がある。最高裁平成 17 年 11 月 10 日第一小法廷判決は、「人は、みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する。もっとも、人の容ぼう等の撮影が正当な取材行為等として許されるべき場合もあるのであって、ある者の容ぼう等をその承諾なく撮影することが不法行為法上違法となるかどうかは、被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様、撮影の必要性等を総合考慮して、被撮影者の上記人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかどうかを判断して決すべきである」と判示し、違法性阻却の要件を含めた判断基準を示した。

[57] 東京地裁平成 16 年 2 月 20 日判決は、高層マンション建設による近隣住民のプライバシー侵害の有無・程度について、被告（マンション建設事業者）が原告（近隣住民）の求めに応じて手すりや窓ガラスの変更、目隠しの設置を行ったことが「事業者がプライバシーについて相応の配慮、努力をしたものと認められるから、プライバシー侵害の程度は受忍限度を超えるものとは認められない」と判示している。

② 利用者の不安感等

仮に個人識別性を獲得する可能性がなく、プライバシーの侵害が想定されない場合であっても、端末、機器及びブラウザ等を識別する情報等、利用者本人にとって自らの情報であることが自明な情報については、その情報の取扱いの態様を知らないことや取扱いに関与できないことが利用者の不安感等を惹起する可能性がある。また、単に行動履歴を取得するだけでも、事業者による情報の取扱いに透明性が確保されていない場合や利用者が情報の取扱いに関与できない場合に、利用者の不安感等を惹起する可能性がある。

そこで、かかる不安感等を軽減して円滑なサービス展開に資するため、事業者には、行動履歴や位置情報等の取扱いについて透明性を高めることや、利用停止や取得停止等の利用者関与の手段を提供することなど、相応の配慮が求められる。

③ まとめ

これまで述べてきたとおり、ライフログ活用サービスは、その態様によっては、プライバシーを侵害し、かつ、利用者の不安感等を惹起し得る。しかしながら、事業者がプライバシーについて相応の配慮をなした場合は、プライバシー侵害となるおそれは限定的なものとなり、利用者の不安感等は相当程度軽減されることとなる。よって、事業者は、利用者の信頼に裏付けられた円滑なサービスの提供に資するため、ライフログの取扱いに関し、一定の配慮をなすことが求められる。

本章では、主に行動ターゲティング広告等に焦点を当てて検討してきたが、次章ではライフログを取得・利活用するサービスに対する一般的な配慮について検討することとする。

５．より信頼されるサービスに向けて（配慮原則の提言）

これまで検討してきたとおり、ライフログ活用サービスは、その態様によっては、プライバシーを侵害し得るし、利用者の不安感等を惹起し得る。よって、ライフログを取得・保存・利活用する事業者は、利用者に対して一定の配慮をなし、円滑なサービスに資するための対策を取ることが望ましい。

事業者のなすべき配慮についてガイドライン等を行政が示すことも一手段として考えられる。しかし、ライフログ活用サービスは揺籃期にあり、事業者に過度の負担となってサービスの発展を妨げることは避けるべきであることから、まずは、規制色の強い行政等によるガイドラインではなく、事業者による自主的なガイドライン等の策定を促すべきであろう。よって、本研究会では、こういった自主的なガイドライン等の策定の指針となる緩やかな配慮原則を策定することとした。各業態[58]においては、本配慮原則を踏まえ、業態固有の事情を加味した自主的なガイドライン等を策定することが期待される[59]。

なお、ライフログ活用サービスが、今後、技術革新に伴って急速に発展することが想定されること、サービスのボーダレス性から国際的なハーモナイゼーションに対応する必要があること等から、定期的に本配慮原則を見直す必要がある。また、事業者による取組を促進するため、総務省において、本配慮原則を踏まえた事業者の取組を定期的に調査し、これを公表する必要がある。

（１）対象

①　対象情報

配慮原則の対象となる情報は、特定の端末、機器及びブラウザ等（以下「端末等」という。）を識別することができるものとする。対象情報は、個人情報保護法上の個人情報であるか否かを問わない。

例えば、クッキー技術等を用いて生成された識別情報、携帯電話端末に係るいわゆる契約者固有 ID、ログイン中の利用者を識別する ID、端末等のシリアル番号、MAC アドレスや IC タグの ID も、特定の端末等を識別することが可能であるから対象情報と

---

[58] 具体的には、現時点では、行動ターゲティング広告を配信する広告事業者、レコメンド機能を営む電子商取引サイト、ディープ・パケット・インスペクション技術を活用した行動ターゲティング広告を配信するインターネット・サービスプロバイダ、行動支援型サービスを行う携帯電話事業者等を想定している。

[59] FTC による「スタッフレポート：オンライン上の行動ターゲティング広告に関する自主行動原則」（FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising）も、事業者が自主的なガイドラインを作成するにあたっての根本的な原則であり、本配慮原則と同様のアプローチを採用している。

なる。また、これらと結びつけることが可能な閲覧履歴、検索履歴、購買履歴等の行動履歴も対象情報に含まれる。

前述したとおり、ライフログ活用サービスの提供に当たっては、個人識別性のない情報を取り扱う場面が多いと考えられる。個人識別性のない情報の取扱いについては、特定個人のプライバシーが侵害される場面は比較的限定されるとはいえ、プライバシー性が完全に失われていると考えるのは相当ではない。例えば、転々流通するうちに個人識別性を獲得してしまうおそれがあるし、大量に蓄積されて個人が容易に推定可能になるおそれがある。また、対象情報を取り扱う事業者にとっては個人識別性がないとしても、利用者本人にとって自らの情報であることが自明な情報については、その情報の取扱いに関与できないことが利用者の不安感等を惹起する可能性がある。

他方で、特定の端末等を識別することすらできない情報については、他の情報との照合や大規模な蓄積がなされたとしても、個人識別性を獲得する可能性は低く、プライバシー侵害の可能性は極めて低いと考えられる。また、特定の端末等を識別できない情報は、利用者本人にとっても自らの情報であることが判然としないため、利用者の不安感等は相当程度減じていると考えられる。

なお、対象情報が個人情報に該当する場合は、別途、個人情報保護法及び関係各ガイドラインの遵守が必要であることはいうまでもない。

② 対象事業者

対象となる事業者は、対象情報を事業（ただし、対象情報を蓄積せずに行う事業は除く。）の用に供している者とする。

「事業」とは、単に一定の目的をもって反復継続的に遂行される同種の行為であることだけでは足りず、社会通念上それが事業とみられる程度の行為であることを要する。例えば、個人でウェブサイトやブログを開設している場合では、対象情報が取得・保存・利活用されることもあるが、通常、電子商取引サイト等の事業を営んでいない限り、社会通念上事業とみられる程度の行為ではないことから、本配慮原則の対象となる事業者には含まれない[60]。

対象情報を蓄積せずに行うサービスについては、利用者の嗜好の分析の程度が低いこと、対象情報が保存されないことから、プライバシーが侵害されたり、利用者の不安感等が惹起されたりする場面は極めて限定的であり、配慮原則の対象としないこと

[60] もっとも、事業者ではない個人であっても大規模に対象情報を取得・保存・利活用している者も考えられる。こういった者は、対象事業者には含まれないとはいえ、自主的に配慮原則を踏まえたプライバシーポリシー等を整備することが望ましい。

が適当である[61]。

（２）配慮原則

具体的な配慮原則は以下の６つである。
① 広報、普及・啓発活動の推進
② 透明性の確保
③ 利用者関与の機会の確保
④ 適正な手段による取得の確保
⑤ 適切な安全管理の確保
⑥ 苦情・質問への対応体制の確保
以下、配慮原則の具体的な内容について説明する。

① 広報、普及・啓発活動の推進

対象事業者その他の関係者は、利用者のリテラシーの向上や不安感や不快感の払拭に資するべく、対象情報を活用したサービスの仕組みや、本配慮原則に基づく取組について、広報その他の啓発活動に努めるものとする。

対象情報を取り扱う事業者その他の関係者に対し、広報、普及・啓発活動の推進に努めるよう配慮を求める原則である。本原則は、大きく分けると、利用者に対する広報、普及・啓発活動と、ライフログ活用サービス事業者への広報、普及・啓発活動で構成され、２つの広報活動が相まって利用者のリテラシーの向上や不安感等の払拭に資することが期待されている。なお、事業者以外の関係者としては、具体的には、消費者団体、公益法人、国や地方公共団体が考えられる。

１点目の利用者に対する広報活動についてであるが、これは後述する配慮原則「透明性の確保」の目的をより実効性のあるものにするために提言するものである。ライフログ活用サービスは、利用者から取得したライフログを利活用してサービスを提供するものであるが、プライバシー、個人情報保護の観点からすれば、ライフログを提供するかどうかは利用者の判断に委ねられるべきである。そして、その判断材料を提供するためには、サービスの仕組みについての透明性が確保されるべきである。そこで、本研究会では、透明性を確保すべく、事業者がサービスの仕組みについて利用者に明らかにするよう求めることとした。（「②透明性の確保」を参照。）

広報活動に係る本原則は、ライフログ活用サービスの認知度が低いことにかんがみ、事業者その他の関係者が、受動的にサービスの透明性を確保するのみならず、より積極的にサービスの仕組みについて利用者に広報、普及・啓発していくよう配慮を求め

[61] 対象情報を蓄積せずに行うサービスとしては、例えば検索連動型広告が挙げられる。（一般的に、検索連動型広告は検索キーワードを蓄積せずに行われている。）

ることにしたものである。

２点目の対象情報を取り扱う事業者への広報、普及・啓発活動についてであるが、ライフログ活用サービス事業者の中には、ライフログの取得・保存・利活用に当たって、利用者への配慮を行っていないか十分でない事業者が多数存在する。こういった事業者に対し、すでに配慮原則を踏まえたガイドライン等に基づいた取得等を行っている事業者やその他の関係者が、配慮原則について広報、普及・啓発を行うことによって、本配慮原則を踏まえたガイドライン等の普及を促し、ひいては利用者の不安感等の払拭に資することが期待される。

② 透明性の確保

対象事業者その他の関係者は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知り得る状態に置く（以下「通知等」という。）よう努めるものとする。通知等に当たっては、利用者が容易に認識かつ理解できるものとするよう努めるものとする。

前記のとおりライフログを事業者に提供するかどうかは利用者の判断に委ねられるべきである。その判断材料を提供するため、利用者関与の手段を含むサービスの仕組みについての透明性が確保されるべきである。本研究会では、透明性の確保を達成するために、事業者がサービスの仕組みについて利用者に明らかにすることを求めることとした。本原則は「③利用者関与の機会の確保」と相まって、事業者による対象情報の適正な取扱いを促すものであり、６つの原則の中核をなす。

なお、行動ターゲティング広告やレコメンドについては、国内外のガイドライン[62]や主要事業者の現状を基に検討した結果、少なくともア．取得の事実、イ．対象情報を取得する事業者の氏名又は名称、ウ．取得される情報の項目、エ．取得方法、オ．第三者提供の事実、カ．提供を受ける者の範囲、キ．提供される情報の項目、ク．利用目的、ケ．保存期間[63]、コ．利用者関与の手段について、利用者に通知し、又は知り得る状態に置くことが望ましい[64]と考えられる。

対象情報の取得・保存・利活用及び利用者関与の手段の詳細について通知等を行っていたとしても、それが利用者にとって認識されにくいか又は難解なものである場合には、透明性を確保するという本原則の趣旨が達成されないことになる。よって、通

[62] 我が国では「行動ターゲティング広告ガイドライン」（インターネット広告推進協議会　平成21年6月）が、アメリカでは”Self-Regulatory Principles for Online Behavioral Advertising“(American Association of Advertising Agencies et al. 2009年7月)がある。

[63] 保存期間には、端末等の識別を継続して行う期間と、蓄積した対象情報を保管する期限の２つがある。

[64] 一部の構成員から、どの広告が対象情報を活用した行動ターゲティング広告等なのか、利用者に容易に認識かつ理解できるようにすべきとの指摘があった。

知等に当たっては、事業者は利用者が容易に認識かつ理解できるものとすることが望ましい。

利用者が容易に認識かつ理解できる通知等の具体的内容については、例えば、取得者のプライバシーポリシー等を掲載したページに、取得事実等を簡潔かつ目を惹きやすい形で掲載することを念頭に置いている。

行動ターゲティング広告においては、第三者による対象情報の取得や広告やウェブビーコンの配信が行われる場合等、広告の掲載者と対象情報の取得者や広告等の配信者とが異なる場合が考えられ、対象情報の取得者や広告等の配信者のウェブサイトに取得事実等を単純に表示しても、利用者が確認することが困難であり、透明性を確保したことにはならないのではないかという問題がある。この場合は、広告の掲載者のウェブサイトにおいて、第三者による対象情報の取得や広告等の配信が行われていることを明示した上で、取得者の名称、取得事実等に係る情報が掲載されたページへのリンクをはることが望ましい[65]。

③　利用者関与の機会の確保

対象事業者は、その事業の特性に応じ、対象情報の取得停止や利用停止等の利用者関与の手段を提供するよう努めるものとする。

対象情報に関して誤った取扱いがなされることに起因するプライバシー侵害や個人情報の不適切な取扱いを予防・是正する観点から、事業者に対し、対象情報を最もよく知り得る立場にある利用者が情報の取扱いに関与できる手段を提供するよう求める原則である。この原則は、透明性の確保の原則が適切に実現されていることが前提となる。

現在、行動ターゲティング広告では、行動ターゲティング広告配信停止手段[66]の提供が広く行われている。通常、この手段の提供は、行動ターゲティング広告の配信を拒否したブラウザであることを示すクッキー（オプトアウトクッキー）を発行することにより行われている。ただし、この手段は、クッキーが削除された場合にオプトアウトが解除されてしまうものであり、異なるブラウザの利用、端末の買換え、OS の再インストールの場合等に、再度、クッキー発行の手続をとることが必要となる一定の制約がある。事業者には、オプトアウトクッキーの制約について利用者に説明することが求められる。

---

[65] 第三者による対象情報の取得及び広告の配信については、プライバシーへの影響度合いが大きいため、どのウェブサイト上において行われているかを対象情報の取得者が明らかにすべきとの指摘があった。

[66] 通常、行動ターゲティングされた広告の配信が停止され、その代わりに行動ターゲティングされていない広告が配信される。

他には、プライバシーポリシー等のページで、クッキーの拒否、クッキーの削除について説明するとともに、その設定方法を掲載しているウェブサイトが散見される。クッキーの拒否、削除によりブラウザを識別することが出来なくなるため、取得情報は対象情報からはずれることになるとはいえ、通常のブラウザの設定では、個別のクッキーを拒否することが難しいことも考慮される必要があると思われる[67]。

また、携帯電話インターネットでは、契約者固有 ID の非通知について説明するとともに、その設定方法を掲載しているウェブサイトが散見される。契約者固有 ID の非通知により、同様にブラウザを識別することが出来なくなり、取得情報は対象情報からはずれるとはいえ、契約者固有 ID が非通知になっていると利用できないサイトやサービスが広く存在することも同様に考慮の必要があると思われる。

以上からすれば、結局、事業者は上記の行動ターゲティング広告配信停止手段の提供、クッキーの拒否・削除等の利用者関与の手段を、事業の特性に応じて総合的に提供することが求められる。「事業の特性に応じ」としたのは、ライフログ活用サービス事業者の事業は多種多様であり、利用者関与の手段も、その特性に応じて柔軟に提供されるべきだからである。

事業者には、今後、簡便に利用者が対象情報の取扱いを確認し、取得及び利用を停止させる手段を提供することが望まれる[68]。

④ 適正な手段による取得の確保

対象事業者は、対象情報を適正な手段により取得するよう努めるものとする。

不正手段による取得には、取得者や取得情報の範囲等を偽る場合（通常人が想定する範囲を大きく逸脱して取得される場合を含む。）、利用者が全く認識し得ない手段を用いる場合等が考えられ、かかる態様の取得に対する利用者の不安感等が高まっている。こういった事案に対応し、不安感等を払拭し、対象情報の適正な取扱いに対する利用者の信頼を確保する観点から、取扱いの起点である取得段階から適正性が確保されていることが重要である。よって、対象情報を適正な手段により取得するよう提言するものである。

具体的な適正性の判断については、ケースバイケースであり、各法令の趣旨や社会通念に委ねられる。

---

[67] この手段によると、例えば、Windows Internet Explorer 8 は、個別のクッキーを拒否するための機能を標準で用意している。また、Mozilla Firefox バージョン 3.0 系列や Google Chrome 4.0.249.89 ではアドオンを追加することによって個別のクッキーを拒否することが可能になる。

[68] 一部の構成員から、簡便に利用者が対象情報の取扱いを確認し、取得及び利用を停止させることが可能な技術的手段の発展が望まれるとの指摘があった。

⑤　適切な安全管理の確保

対象事業者は、その取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要かつ適切な措置を講じるよう努めるものとする。

対象情報が、不正に取得した者によって利用に供された場合、プライバシーの重大な侵害が惹起される場合が考えられる。このため、対象情報を取得した事業者に対し、その取り扱う対象情報が漏えい、滅失又はき損の危険にさらされることのないよう配慮を求めるものである。

⑥　苦情・質問への対応体制の確保

対象事業者は、対象情報の取扱いに関する苦情・質問への適切かつ迅速な対応に努めるものとする。

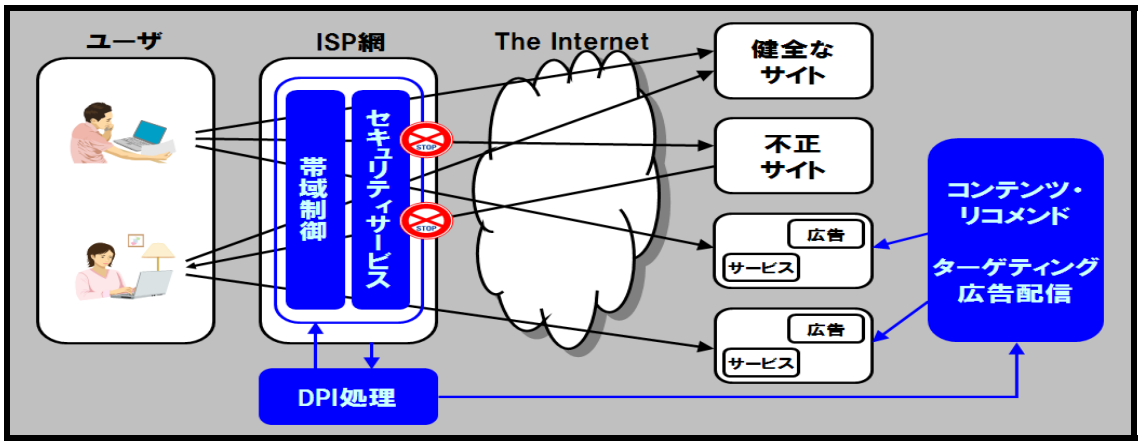
対象情報の取扱いをめぐるトラブルは、基本的に私人間の問題であるため、まずは当事者間で話し合うことで迅速な解決を図ることが望ましい。このため、事業者に対し、対象情報の取扱いに関する苦情や質問に対応する窓口を設け、適切かつ迅速な処理に努めるよう配慮を求めるものである。

６．ディープ・パケット・インスペクション技術（DPI 技術：Deep Packet Inspection）を活用した行動ターゲティング広告について

（１）DPI 技術を利用した行動ターゲティング広告の態様

DPI 技術を活用した行動ターゲティング広告は、通信プロバイダ（ISP）が、ネットワークを通過するパケットを解析して利用者の興味・嗜好を分析し、これにマッチした広告を利用者に配信するものである[69]。一般に、DPI 技術とはネットワークを通過するパケットのヘッダ情報やペイロード情報を解析し、通信の特徴や振舞いを分析する技術を指している。従来、DPI 技術は、帯域制御のための要素技術として利用されてきたが、現在、ファイアウォールでは防ぎきれないインターネット上の脅威に対する防衛手段のための要素技術として、より洗練された行動ターゲティング広告のための要素技術として、先進的な利用が検討されており、今後の展開が期待される技術である。

図１　DPI 技術を活用した行動ターゲティング広告のイメージ



[69] 現状の DPI 技術を用いたオンライン行動ターゲティング広告では、HTTP リクエスト及びレスポンスに係るパケットを解析して抽出された情報（アクセス URL 及び検索エンジンでの検索キーワード）を基に興味・嗜好を分析し、これにマッチした広告を配信している。なお、ブラウザ等の特定は、IP アドレス等から生成された ID により行われている。

（２）法的な課題

DPI 技術を活用した行動ターゲティング広告については、ISP によってネットワークを通過するパケットの解析が行われるものであるため、４．で検討した個人情報保護法やプライバシー保護の関係に加えて、通信の秘密の保護との関係で検討が必要となる。以下では、通信の秘密の保護との関係を整理するが、同技術を活用した行動ターゲティング広告の実施に当たっては、個人情報保護法及びプライバシーへの配慮も併せて必要であることは言うまでもない。

① 通信の秘密とは

通信の秘密は、個人の私生活上の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）とともに、通信が人間の社会生活にとって不可欠なコミュニケーション手段であることから、憲法上の基本的人権の一つとして憲法第 21 条第２項において保障されている。

日本国憲法 第二十一条 ２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

電気通信事業法では、憲法第 21 条第 2 項の規定を受けて電気通信事業者の取扱いに係る通信の秘密を保護している。（電気通信事業法第４条第１項）通信の秘密を侵害した場合には罰則が適用される（同法第 179 条）。また、電気通信事業者の業務の方法が通信の秘密の確保に支障があると認められるときは、総務大臣による業務改善命令が発動される（同法第 29 条第１項第１号）。このように、電気通信事業法上、通信の秘密は厳格に保護されている。

電気通信事業法（昭和五十九年法律第八十六号） 第四条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。 ２　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。 第二十九条　総務大臣は、次の各号のいずれかに該当すると認めるときは、電気通信事業者に対し、利用者の利益又は公共の利益を確保するために必要な限度において、業務 の方法の改善その他の措置をとるべきことを命ずることができる。 一　電気通信事業者の業務の方法に関し通信の秘密の確保に支障があるとき。 二～十二　（略） 第百七十九条　電気通信事業者の取扱中に係る通信（第百六十四条第二項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

2　電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。 3　前二項の未遂罪は、罰する。

「電気通信事業者の取扱中に係る」とは、発信者が通信を発した時点から受信者がその通信を受ける時点までの間をいい、電気通信事業者の管理支配下にある状態のものを指している。

「通信の秘密」は、通信内容はもちろんのこと、通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、通信回数等、これらの事項を知られることによって通信の意味内容が推知されるような事項全て（通信の構成要素）を含むものである。電気通信事業に従事する者に対しては、通信の秘密のほか、契約の際に入手した契約者の個人情報等、個々の通信の構成要素とはいえないが、それを推知する可能性のあるものに対しても、守秘義務を課している[70]。

通信の秘密を侵すとは、通信当事者以外の第三者が積極的意志をもって通信の秘密を知り得る状態に置くこと（「知得」）のほか、第三者にとどまっている秘密そのものを他人が知り得る状態に置くこと（「漏えい」）及び発信者・受信者の意思に反して自己又は他人の利益のために用いること（「窃用」）も、それぞれ独立して秘密を侵すことに該当する。

② 通信当事者の同意

通信当事者の同意がある場合には、通信当事者の意思に反しない利用であるため、通信の秘密の侵害に当たらない。もっとも、通信の秘密という重大な事項についての同意であるから、その意味を正確に理解したうえで真意に基づいて同意したといえなければ有効な同意があるということはできない。一般に、通信当事者の同意は、「個別」かつ「明確」な同意である必要があると解されており、例えば、ホームページ上の周知だけであったり、契約約款に規定を設けるだけであったりした場合は、有効な同意があったと見なすことは出来ない。有効な同意とされるためには、例えば、新規のユーザに対して、契約の際に行動ターゲティング広告に利用するため DPI 技術により通信情報を取得することに同意する旨の項目を契約書に設けて、明示的に確認すること等の方法を行う必要がある。

③ DPI 技術を活用した行動ターゲティング広告は通信の秘密を侵しているか

ISP による DPI 技術を活用した行動ターゲティング広告は、利用者の HTTP リクエスト及びレスポンスに係る全てのパケットを解析して利用者の興味・嗜好を分析し、これにマッチした広告を利用者に配信するものである。

[70] ただし、罰則は通信の秘密を侵した場合に限られる。（電気通信事業法第 179 条）

ISP が解析するパケットは、発信者たる利用者と受信者たるウェブサーバ間の通信（レスポンスの場合は発信者たるウェブサーバと受信者たる利用者間の通信）に係るパケットであり、当該通信は、電気通信事業者たる ISP の管理支配下の状態にある。よって、解析対象のパケットは、電気通信事業者の取扱中の通信に係るパケットである。

また、DPI 技術を活用した行動ターゲティング広告では、利用者の HTTP リクエスト及びレスポンスに係る全てのパケットから、利用者がウェブページにアクセスした際の URL や、利用者が検索エンジンにおいて検索にかけた検索キーワードを抽出して解析しているが、これらの情報は通信の構成要素若しくは内容に当たり、通信の秘密の保護対象に該当する。

さらに、DPI 技術を用いた行動ターゲティングでは、パケットを解析し、その解析結果を嗜好にマッチした広告の配信に利用しているが、パケットを解析する行為は「知得」に、解析結果を用いて広告の配信に利用する行為は「窃用」に該当し、通信の秘密の侵害行為となる。

④　違法性阻却が認められるか

上述のとおり、DPI 技術を活用した行動ターゲティング広告の実施は、利用者の同意を得ない場合は、通信の秘密の侵害に該当することとなるが、正当行為（刑法第 35 条）、正当防衛（同第 36 条）、緊急避難（同第 37 条）等の一定の事由が認められる場合には、その違法性が阻却され、例外的に通信の秘密を侵すことが許容されることになる。DPI 技術を活用した行動ターゲティング広告については、緊急避難や正当防衛の事由は想定しにくいため、ここでは正当行為について整理を行うこととする。法令に基づく行為及び正当業務行為については、正当行為として違法性が阻却されるが、DPI 技術を活用した行動ターゲティング広告は民間事業者による事業の一環であり、法令上に根拠のある行為ではないため、ここでは正当業務行為といえるかどうかが問題となる。

刑法 第三十五条　法令又は正当な業務による行為は、罰しない。

電気通信事業者による通信の秘密の侵害行為が正当業務行為となる場合については、実務上の運用事例を通じて一定の考え方が整理されてきている。これまでに正当業務行為が認められた事例は、ア．通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為、イ．ISP がルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為に加え、ウ．ネットワークの安定的運用に必要な措置であって、目的の正当性や行為の必要性、手段の相当性から相当と

認められる行為（大量通信に対する帯域制御等）といったものが挙げられる。こうした事例の根底にある基本的な考え方は、国民全体が共有する社会インフラとしての通信サービスの特質を踏まえ、利用者である国民全体にとっての電気通信役務の円滑な提供という見地から正当・必要と考えられる措置を正当業務行為として認めるものである。

こうした基本的な考え方に立って検討すると、ISP による DPI 技術を活用した行動ターゲティング広告の実施は、パフォーマンスの高い広告を配信することや、そのために利用者の嗜好を把握することを目的としており、ISP による電気通信役務（電気通信設備を用いて利用者をインターネットに接続させる役務）にとって、必ずしも正当・必要なものとは言い難く、正当業務行為とみることは困難である[71] [72]。

⑤ 運用基準等の策定

このように、DPI 技術を活用した行動ターゲティング広告の実施は、利用者の同意がなければ通信の秘密を侵害するものとして許されない。利用者の同意が明確かつ個別のものであることが必要なことは、前記②記載のとおりであるから、同意に当たっての判断材料を提供するという意味で、利用者に対してサービスの仕組みや運用について透明性が確保されるべきである。よって、DPI 技術を用いた行動ターゲティング広告については、各事業者は、透明性の確保に向けて運用に当たっての基準等を策定し、これを適用することが望ましい。

---

[71] 前述（脚注 10）でもふれたとおり、この点に関連する裁判例として、電気通信事業者に、脅迫的内容の電報を差し止める義務があるかどうかが争われた事案がある。原審判決（大阪地裁平成 16 年 7 月 7 日判決）においては、電気通信事業者が脅迫電報を把握して差し止める行為について、①通信事業者に求めることが適当でないのみならず、かえって公共的通信事業者としての職務の性質からして許されない違法な行為である、②電気通信事業者の提供する役務の内容として予定されているのは、あくまでも物理的な通信伝達の媒体ないし手段として、発信者から発信された通信内容をそのまま受信者に伝達することである、③ある電報が犯罪的な内容であるか否かを把握するためには、全電報を審査の対象としなければならず、結局、圧倒的に多数のその他の電報利用者の通信の秘密を侵害することになり、このことによる社会的な悪影響はきわめて重大である、④通信の内容が逐一吟味されるものとすると、萎縮効果をもたらし、自由な表現活動ないし情報の流通が阻害されるなどと判示している。同判決は、電気通信事業者が電報の内容を解析・把握することが正当業務行為に当たるか否かについて判断した事案ではないが、同判決に示された考え方を前提にする限り、通信内容を解析する行為が、正当業務行為に当たると解することは困難であろう。なお、控訴審判決（大阪高裁平成 17 年 6 月 3 日判決）において原告の控訴は棄却されている。

[72] なお、刑法第 35 条により、法令行為、正当業務行為以外の一般的違法性阻却事由が認められるとする見解があるが、この見解に立ったとしても、前記脅迫電報事件の趣旨に照らせば、通信内容の解析に当たる DPI 技術を活用した行動ターゲティング広告が、一般的違法性阻却事由により違法性を阻却されると解することは困難である。

７．おわりに

本研究会では、ライフログ活用サービスの更なる進展を促すために、事業者自らが、利用者のプライバシーや不安感等に対処することが必要と考え、その指針となる配慮原則を示した。しかしながら、ライフログ活用サービスの進展を促すためには、これだけでは十分ではなく、ライフログの利活用促進が必要であろう。

総務省においては、ライフログの利活用を促進し、ライフログ利活用サービスの更なる進展を促すための検討を進めることが求められる。

Ⅲ　安全管理措置に関する検討について

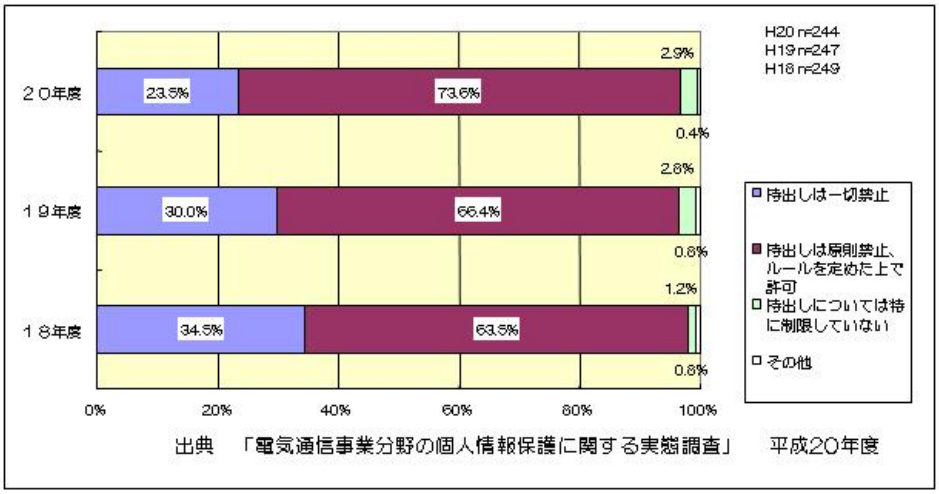
１．検討の背景

（１）モバイル PC 等による情報資産の社外への持出しの現状

企業は、顧客情報、財務企業情報等様々な情報資産を保有し、その活動において活用している。ICT 技術の進歩により、企業が保有し、活用する情報資産の量は膨大なものとなっている。さらに、近時はそれらの情報資産を社外に持ち出し、業務に活用することが増えている。

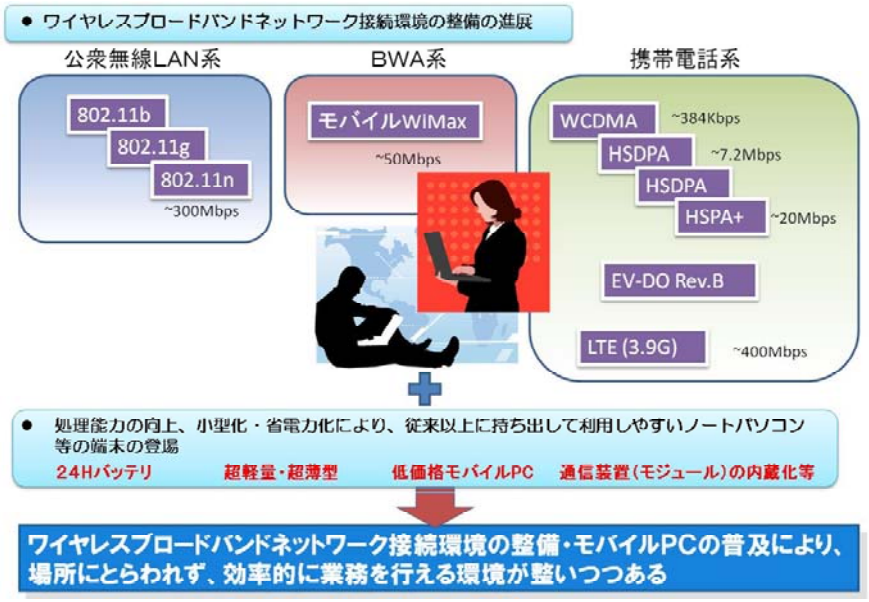
平成 20 年度に財団法人日本データ通信協会が電気通信事業者（以下「事業者」という。）を対象に実施した「電気通信事業分野の個人情報保護に関する実態調査」によれば、「個人情報が入ったノート PC、可搬型記録装置の外部持出制限」について、「持出しの一切禁止」とする事業者は減少傾向にある一方で、「持出しは原則禁止、ルールを定めた上で許可」とする事業者が年々増加してきている傾向が示されている。

図２　電気通信事業者の個人情報の入ったノート PC 等の持出状況



このように情報資産の社外への持出しが増えてきている背景として、まず、情報資産を社外で活用できる環境が整備されてきていることが挙げられる。処理能力の向上、小型・軽量・省力化が進むとともに、出荷段階から通信機能が内蔵されるなど、社外に持ち出して利用しやすいモバイル PC が提供されている。また、携帯電話を用いたブロードバンドサービスの進展、公衆無線 LAN の普及、BWA の提供開始等、ワイヤレスブロードバンド環境が整備されてきている。

図３　ワイヤレスブロードバンド環境の整備



次に、情報資産を社外に持ち出して活用する業務上の必要性が高まっていることが挙げられる。すなわち、業務効率化の必要性、従業員の多様な勤務形態の必要性等に対応する解決策として、営業先や従業員の自宅等社外での情報資産を活用した業務遂行を可能とすることが考えられている。また、新型インフルエンザの発生等に対応し、人的接触を最小限に抑えつつ継続的な業務遂行を可能とする方策の一つとしてのニーズも高まっている。社会全体としても、長時間の通勤時間の減少や、サテライトオフィス活用による地域雇用の確保、育児や在宅介護に対応可能な勤務形態の実現などに対する手段として、テレワーク等情報資産の社外での活用が有効なものと考えられている。

さらに、社外に持ち出した情報資産の安全性を確保可能とするサービスが出てきていることが挙げられる。すなわち、個人認証技術、暗号技術等の技術を組み合わせ、モバイル PC の紛失、盗難時においても、技術的に情報資産の安全性を確保するサービスが提供されるようになってきている。

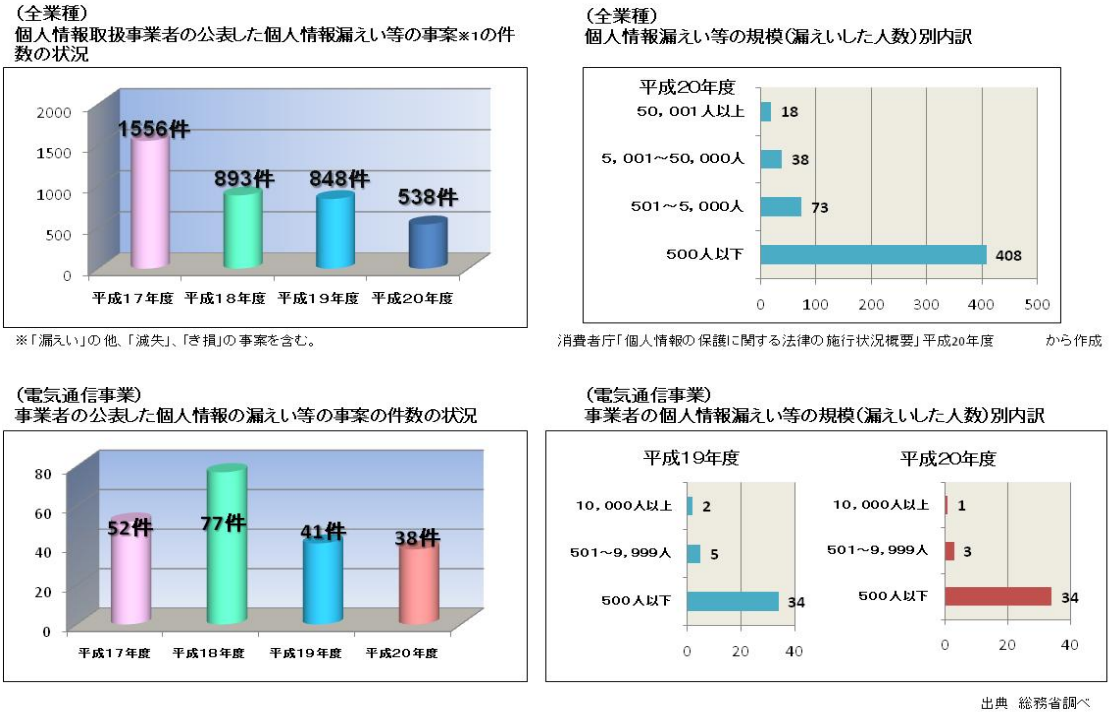
（２）モバイル PC 等による情報資産の社外への持出しに伴うリスク

社外への情報資産の持出しの機会の増加に伴い、持ち出したモバイル PC（携帯電話端末を含む。）、USB メモリ等のような記録媒体（以下「モバイル PC 等」という。）の紛失、盗難による個人情報の漏えいリスクが問題となる。

モバイル PC 等の紛失、盗難による個人情報の漏えいの場合には、書類等の紙媒体による個人情報の漏えいの場合に比べて、記録容量が膨大であること、コピー、頒布が容易であることから、権利利益の侵害を受ける本人が多数になる可能性が高く、また、被害が広範に拡がるおそれがあるなど、事業者にとってのリスクは相対的に大きいことが多い。さらに、社内データベースへのアクセス権限が付与されたモバイル PC を紛失、盗難した場合には、社外の第三者によって社内データベースにアクセス可能となるおそれもあり、そのような場合には、事業者にとってのリスクは格段に大きくなる。

一方で、モバイル PC 等の紛失、盗難の場合には、適切な技術的保護措置を講じていれば、実際に個人情報が第三者により判読、解読されることを防止することができる。このため、鞄への施錠程度の措置しか講じることができない紙媒体の紛失、盗難の場合に比べて、実際の被害を大幅に減少させることが可能と考えられる。

図４　個人情報漏えい事故の状況



（３）モバイル PC 等による個人情報の持出し増加に伴う検討の必要性

このため、モバイル PC 等による情報資産の社外への持出しが増加している中で、それに伴う個人情報の保護という観点での検討が必要となる。

まず、モバイル PC 等による個人情報の社外への持出しに当たって必要とされる安全管理措置についての検討が必要である。個人情報の保護に関する法律（以下「法」という。）では、個人情報取扱事業者に対し、取り扱う個人データ[73]の漏えい、滅失又はき損（以下「漏えい等」という。）が生じないよう安全管理のために必要かつ適切な措置を講じることを義務付けており、「電気通信事業における個人情報保護に関するガイドライン」（平成 16 年総務省告示第 695 号。以下「現行ガイドライン」という。）では、個人情報[74]の持出しに関して、「個人情報の持出し手段の制限（みだりに外部記録媒体へ記録することの禁止、社内と社外との間の電子メールの監視を社内規則等で規定した上で行うこと等）」を規定している。しかし、これらの規定は、必ずしも通常業務時におけるモバイル PC 等による個人情報の社外への持出しが増加している現状に対応した内容になっていない部分もあることから、モバイル PC 等の紛失、盗難による個人情報の漏えいの被害の甚大性を考慮しつつ、想定されるリスクへの対応という観点から必要な安全管理措置について検証し、現行ガイドラインの見直しの必要性について検討することが求められる。

次に、モバイル PC 等の紛失、盗難があった場合の手続の在り方についての検討が必要である。個人情報の漏えい等が発生した場合の手続に関して、現行ガイドラインをはじめ、監督官庁で定める業種業態ごとのガイドラインの多くでは、個人情報取扱事業者に漏えい等の事案が発生した場合に、本人への通知、公表、監督官庁への報告という措置を講じることを求めており、モバイル PC 等による個人情報の社外への持出しの場合であっても、これらの手続は、同様に必要とされる。モバイル PC 等による個人情報の社外への持出しの場合には、仮に紛失、盗難があっても、適切な技術的保護措置が講じられていれば、通常、第三者により判読、解読されることはなく、本人への二次被害が発生することはないことから、手続が必要とされている理由を踏まえつつ、適切な技術的保護措置が講じられている場合の運用の在り方について検討することが求められる。

---

73 個人情報の保護に関する法律では、安全管理措置の対象を個人データ（個人情報データベース等を構成する個人情報）としている。

74 電気通信事業における個人情報保護に関するガイドラインでは、広く個人情報の安全管理措置について規定している。

２．想定されるリスクと技術的対応策

（１）想定されるリスク

モバイル PC 等により個人情報を社外に持ち出す場合に生じ得るリスクとしては、大きく分けて、①モバイル PC 等が権限のない者に使用されることによる漏えいリスク、②モバイル PC の記録媒体を物理的に取り出されることによる漏えいリスク、③ネットワーク上を流通する情報を盗み取られることによる漏えいリスクの３つが考えられる。

① モバイル PC 等が権限のない者に使用されることによる漏えいリスク

持ち出したモバイル PC 等が紛失、盗難にあった場合に、権限のない第三者に使用されることにより、そのモバイル PC 等の中に記録された情報を閲読されるおそれがある。また、モバイル PC に社内データベースへのアクセス権限が付与されている場合には、社内データベース上の情報まで閲読されるおそれがある。

② モバイル PC の記録媒体を物理的に取り出されることによる漏えいリスク

モバイル PC の内部にあるハードディスク等の記録媒体に情報を記録する場合には、その記録媒体を物理的に抜き出されることにより、他の PC に接続して情報を読み出されるおそれがある。

③ ネットワーク上を流通する情報を盗み取られることによる漏えいリスク

ネットワーク上で情報のやりとりをする場合には、ネットワーク上を流通する情報を盗み取られることにより、その内容を閲読されるおそれがある。例えば、電子メール等でのやりとりや、社内ネットワーク内に存在するデータへのアクセスなどの場合に、このようなリスクが生じることになる。

（２）リスクに対応する技術的保護措置

以上のようなモバイル PC 等により個人情報を社外に持ち出す場合に生じ得るリスクに対応するために用いることができる技術がある。具体的には、個人認証技術、暗号技術、シンクライアント、遠隔データ管理である。

① 個人認証技術

個人認証技術とは、本人のみが持ち得る情報等を用いて、本人であることを確認するための技術である。この技術を導入することで、モバイル PC 等が権限のない者に使用されることによる漏えいリスクに対応することができる。

個人認証技術を導入可能な部分としては、BIOS（Basic Input / Output System）等のハードウェアの起動時、オペレーティングシステム（Operating System : OS）やアプリケーション等のソフトウェアの起動時がある。これらの複数の段階で導入することも可能であり、その場合には、セキュリティ強度は、より強固なものとなる。

個人認証技術による認証方法としては、パスワード等の記憶により本人（利用者）を識別する方法、IC カード、USB（Universal Serial Bus）キー等の所有物により本人を識別する方法、静脈、指紋、顔等の生体情報により本人を識別する方法の３方式がある。これらの認証方式には、それぞれメリット・デメリットが存在する。

ア 記憶による認証

記憶による認証は、専用のハードウェアが不要である等、導入が容易という利点がある。一方で、パスワード等を忘却したり他人に教えたりするという本人による不適切な管理が起こりやすいという欠点や、桁数が少ないパスワードや辞書等に記載されている単語の組合せによるパスワードの場合等は、第三者に類推されるおそれがあるという欠点が指摘されている。また、長く類推されづらいパスワードになるほど、本人が忘却する可能性が高くなるという問題がある。

イ 所有物による認証

所有物による認証は、その所有物でなければ認証に成功しないことから、唯一性が高いという利点がある。また、記憶による認証と比べて忘却する可能性は低いという利点もある。導入の容易さについても、多くのノート PC には標準で USB ポートが搭載されているなど、媒体の選び方によっては、容易に導入することも可能である。その一方で、ノート PC とともに紛失、盗難にあった場合には、容易に認証を破られるという欠点が指摘されている。

ウ 生体情報による認証

生体情報による認証は、忘却や紛失、盗難のおそれがないという利点がある。一

方で、精度の設定次第では他人を受け入れてしまったり、本人を拒絶してしまったりするという欠点がある。生体情報による認証の中でも、指紋認証や静脈認証では、他人受入率が 0.001%～0.00001%程度であるのに対して、声紋認証や顔認証等では、他人受入率が 1%～0. 1%と相対的に高くなっている。また、一度登録した生体情報は本人が生涯変更することができないため登録情報の厳格な管理が求められるという留意点が指摘されている。

表３　個人認証方法とその特徴

	利点	欠点	認証の強度	利用形態	備考
記憶による認証					
パスワード	導入が容易	忘却、漏えい、類推等	管理・設定方法に依存	専用のハードウェア不要	BIOS、OS、アプリケーションソフトウェア等で対応
所有物による認証					
接触／非接触型ＩＣカード	唯一性が高い 忘却の可能性が低い	紛失、盗難等	情報とともに紛失、盗難に遭うと弱い （PIN併用で、強度向上）	PC内蔵/PC外付けのリーダライタ	交通系カード、携帯電話などで利用可能
USBキー	〃	〃	〃	USB インターフェース	ほとんどのPCにはUSB インターフェースが標準搭載
生体情報による認証					
指紋認証	忘却等のおそれがない	荒れた（磨耗した）指紋では認証率が低下	他人受入率:1/10万～1/1000万(※)	PC内蔵/PC外付けセンサ	PCによっては、センサーを標準搭載
静脈認証	忘却等のおそれがない 体内情報で偽造困難	直射日光下では認証率低下	他人受入率:1/10万～1/1000万(※)	PC外付けセンサ	銀行ATMで用いられている実績
顔認証	忘却等のおそれがない	照明変動、姿勢変動に弱い	他人受入率:1/100(※)	PC内蔵/外付けのWebカメラ	主にデジカメの顔識別で実績
声紋認証	忘却等のおそれがない	風邪、喉の酷使後の声質変化に弱い	他人受入率:1/100(※)	PC内蔵/外付けのマイク	電話による本人認証で実績

（※）認証の強度は、一般的なものであり、使用状況によって異なる

② 暗号技術

ア 暗号技術の動向

暗号技術とは、保護対象の情報について特定情報を用いて変換を施すことにより（暗号化）、その変換された情報を、特定情報を用いて元に戻さなければ（復号）、保護対象の情報の内容を知り得ないようにする技術である。

暗号技術では、暗号化に用いられる特定情報（暗号鍵）と復号に用いられる特定情報（復号鍵）で異なる鍵を用いる公開鍵暗号方式と、暗号鍵と復号鍵で同一の鍵を用いる共通鍵暗号方式がある。

現代社会では、インターネットでのショッピング、携帯電話での通信、地上デジタル放送の受信、電子メールへの電子署名等様々な場面で暗号技術が用いられている。

図５ 暗号技術の用いられる場面

暗号アルゴリズムについては、いくつかの公的機関が、その安全性等について客観的評価を行った上で、使用が推奨されるものを公表している。また、暗号アルゴリズムについては、解読技術の発展、コンピュータ能力の向上等によって、強度が弱くなる（危殆化が生ずる）ことから、不断に検証が行われており、より強度の高い暗号アルゴリズムへの移行スケジュールの公表や推奨の停止等が行われている。

国内では、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである CRYPTREC（Cryptography Research and Evaluation Committees）において、電子政府推奨暗号リストを公表している。また、暗号技術に関する国際標準規格としては、ISO（国際標準化機構（International Organization for Standardization））・IEC（国際電気標準会議（International Electrotechnical Commission））の策定した、ISO/IEC 18033 が存在する。その他、

米国をはじめとした諸外国でも、公的機関により、推奨される暗号アルゴリズムが公表されている。

表４　公的機関で客観的な評価・公表が行われている暗号アルゴリズム

	電子政府推奨暗号 （平成15年度版）(1) 公表元：総務省，経済産業省 原案策定：CRYPTREC (2)	ISO/IEC 18033シリーズ 国際標準規格 策定：ISO/IEC JTC 1/SC27 (3)	NIST SP 800-57 （2030年末期限の場合） 策定：米国立標準研究所
公開鍵暗号			
署名	RSA-PSS(1024bit)、 RSASSA-PKCS1-V1_5(1024bit)、 DSA(1024bit)、ECDSA(160bit)	記載なし（ISO/IEC 9796-2等で規定）	RSA(2048bit)、DSA(2048bit)、 ECDSA (224bit)
守秘	RSA-OAEP(1024bit)、 RSAES-PKCS1-V1_5(1024bit)	RSA-KEM、RSA-OAEP、 PSEC-KEM、ACE-KEM、 HIME(R)、ECIES-KEM	推奨なし
鍵共有	PSEC–KEM (160bit)、 DH(1024bit)、ECDH(160bit)	記載なし（ISO/IEC11770-3で規定）	DH、MQV
共通鍵暗号			
64 bitブロック暗号	3-key TDES、MISTY1、Hierocrypt-L1、CIPHERUNICORN-E	TDES(3-key推奨)、 MISTY1、CAST-128	3-key TDES
128 bitブロック暗号	AES、Camellia、SC2000、 CIPHERUNICRON-A、Hierocrypt-3	AES、Camellia、SEED	AES
ストリーム暗号	MUGI、MULTI-S01、RC4(128bit)	MUGI、MULTI-S01、 SNOW 2.0	推奨なし
ハッシュ関数			
	SHA-256、SHA-384、SHA-512、 SHA-1、RIPEMD-160	記載なし（ISO/IEC 10118 で規定）	SHA-224、SHA-256、 SHA-384、SHA-512

※　表中にあるそれぞれのアルゴリズムには、期限や条件が付されているもの等もあるため、実際に利活用する場合には、原典を確認すること
(1) 平成25年度から新たな推奨暗号の体系に移行することから、現在、リスト見直しのための検討が行われている
(2) CRYPTREC：Cryptography Research and Evaluation Committees　　事務局（総務省、経済産業省、NICT、IPA）
(3) ISO / IEC Joint Technical Committee 1 / SubCommittee 27 “IT Security techniques”
ISO：International Organization for Standardization（国際標準化機構）、IEC：International Electrotechnical Commission（国際電気標準会議）

イ　情報の暗号化

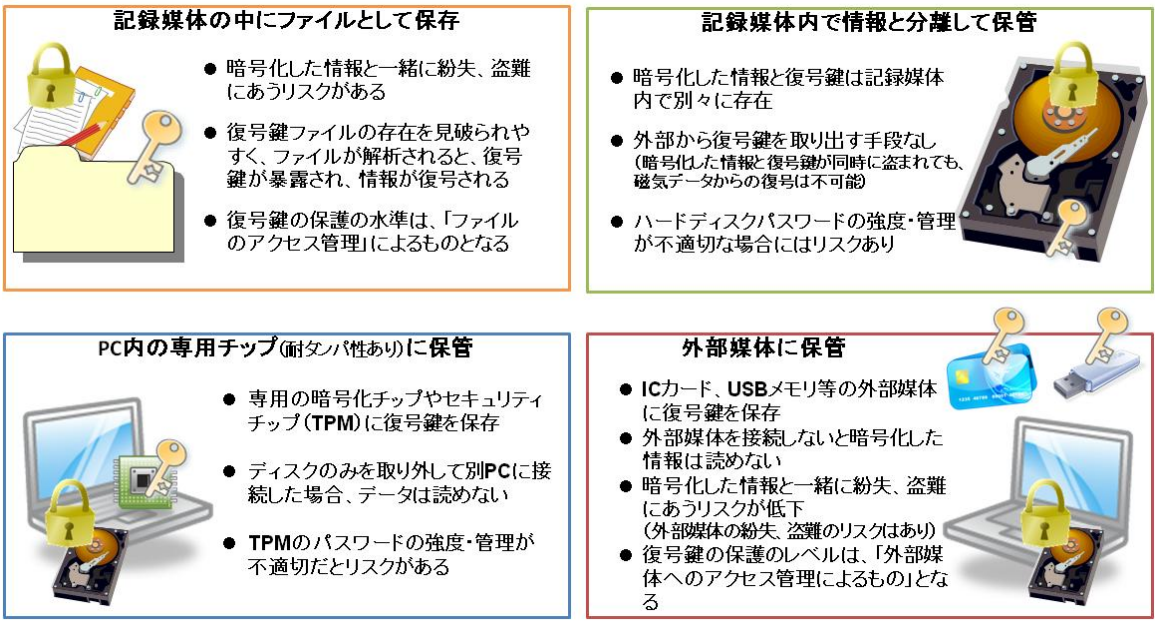
モバイル PC 等により社外に持ち出す情報を適切な暗号アルゴリズムを用いて暗号化することにより、モバイル PC の内部にある記録媒体を物理的に抜き出されることによる漏えいリスクに対応することができる。また、ネットワーク上でやりとりするファイルを適切な暗号アルゴリズムを用いて暗号化することにより、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクにも対応することができる。

暗号技術で重要となる復号鍵の管理については、暗号化した情報が存在する記録媒体の中に保存する方法では、記録媒体と一緒に紛失、盗難に遭うため、復号鍵を盗みだそうとする攻撃から守ることのできる耐タンパ性を持ったモバイル PC 等の中の独立したチップ上で管理する方法、IC カード等の別の媒体で管理する方法等、より適切に管理する方法がある。

復号鍵の適切な管理がなされている場合には、暗号化した情報が存在する記録媒体が紛失、盗難に遭ったとしても、第三者が復号鍵を手に入れることができないため、情報の内容を知られる可能性は極めて低い。

なお、暗号化する対象としては、個々のファイル、特定のフォルダなど記録媒体の特定の領域、記録媒体全体等が考えられる。

図６　復号鍵管理の方法



ウ　通信経路での暗号化

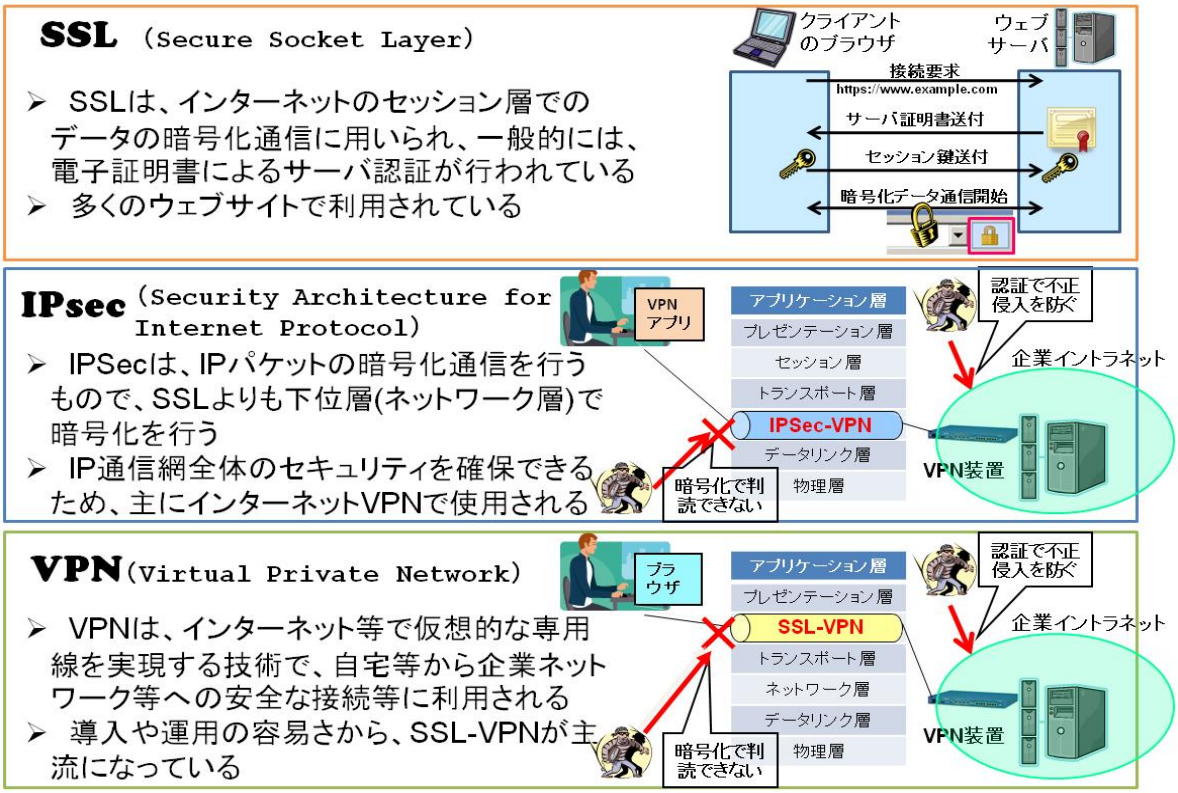
通信経路を暗号化することにより、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクに対応することができる。

通信経路での暗号化方法としてはさまざまなものがあり、その中で代表的な方法としては、SSL（Secure Socket Layer）、IPsec（Security Architecture for Internet Protocol）が挙げられる。

SSL は、一般的には証明書によるサーバ認証が行われるものであり、電子商取引や個人情報等の秘匿性のある情報のやりとりをするウェブサイトの多くにおいて利用されている。IPsec は、IP パケットの暗号化通信を行うものであり、セッション層において暗号化を行う SSL よりも下位層の IP 層において暗号化を行うものである。

VPN（Virtual Private Network）は、SSL 等による暗号化通信を行うことで、仮想的な専用線を実現する技術であり、自宅等の外部から企業ネットワーク等に安全に接続する場合等に利用される。

図７　通信経路での暗号化

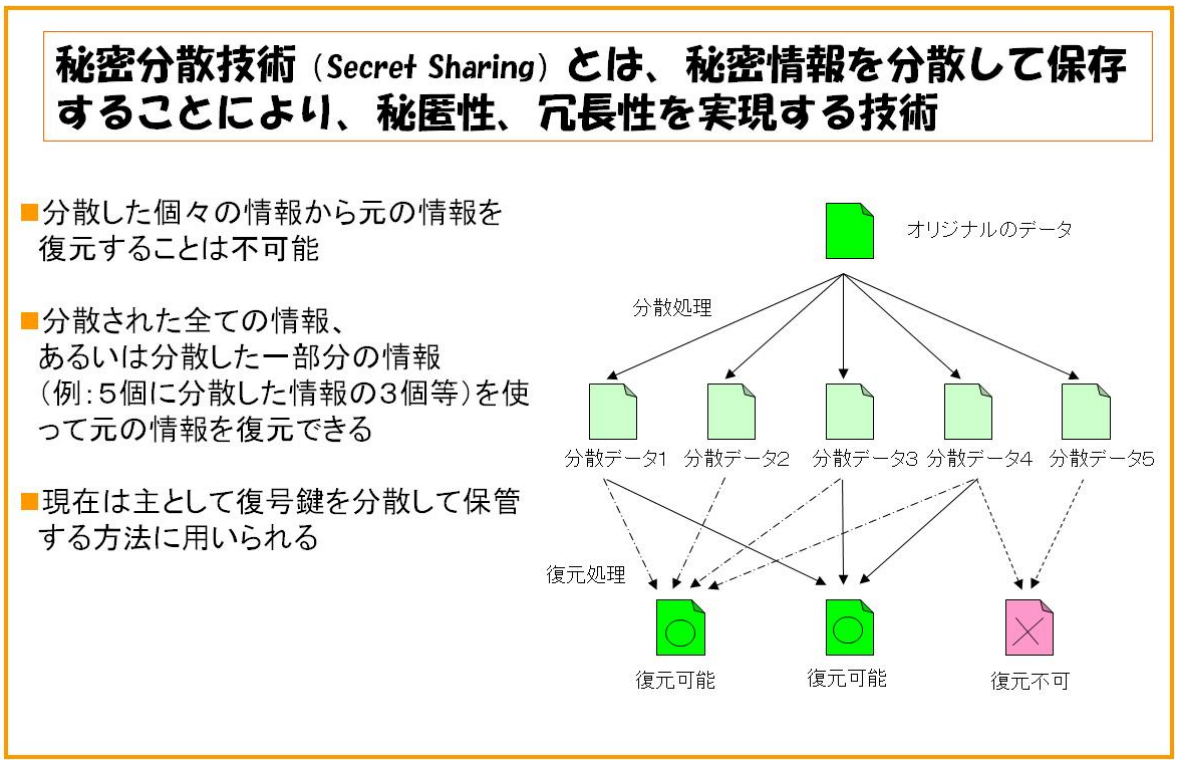


③　秘密分散技術

秘密分散技術（Secret Sharing）とは、秘密情報を分散して保存することにより、秘匿性、冗長性を実現する技術である。分散した個々の情報から元の情報を復元することは不可能で、分散された全ての情報、あるいは一部分の情報を使って元の情報を復元できる特長がある。なお、分散された各々の情報の大きさは、理論上、元の情報の大きさと同じである。また、分散された情報に復元処理に必要な情報が添付されている場合は元の情報よりも大きくなる。

秘密分散技術の応用により、複数の記憶媒体やネットワーク上のサーバに個々の分散した情報を保存し、盗難や漏えい及び災害や故障に対する安全性を保つことが可能である。また、分散した情報の一部をネットワーク上のサーバや、USB メモリ、IC カード等の他の媒体に格納することも可能である。現在は、主として復号鍵を分散して保管するために用いられることが多い。

図８　秘密分散法



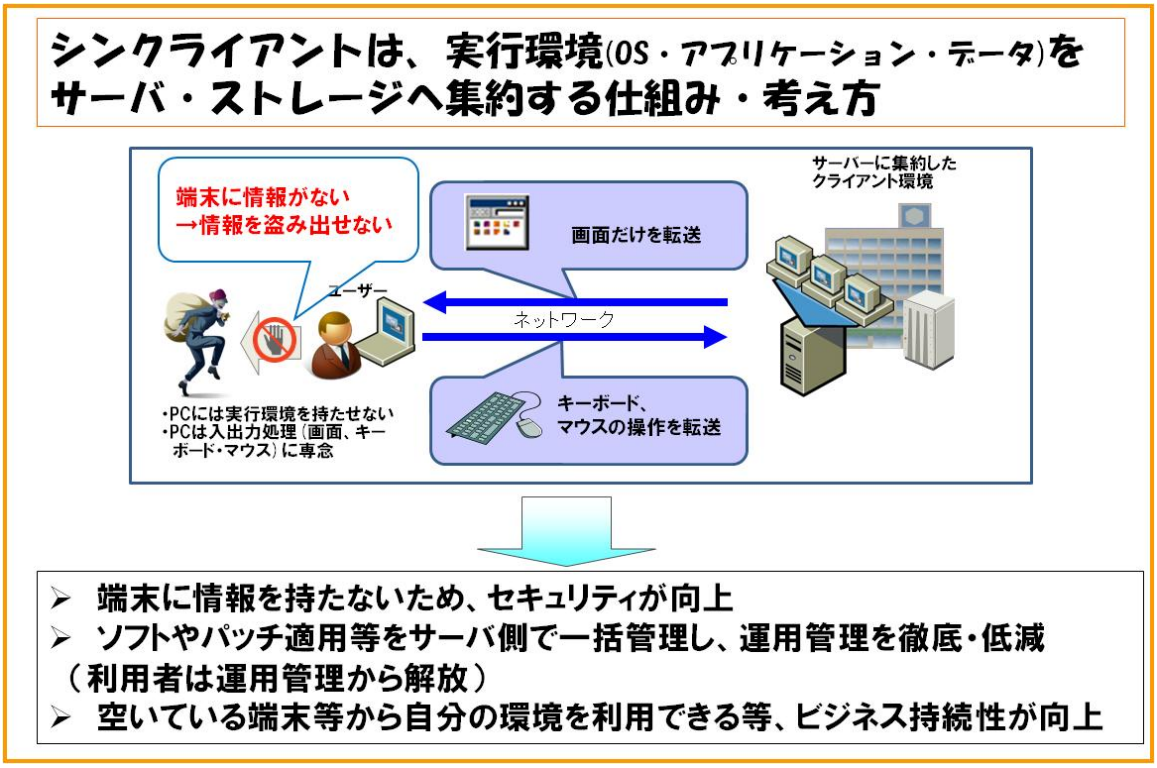
④　シンクライアント技術

シンクライアント技術とは、従業員等が使用する利用者側端末（クライアント）には最小限の機能（ネットワーク機能、画面表示・操作機能）のみを持たせ、アプリケーションやデータはサーバ側で管理する技術である。

シンクライアント技術により、利用者側端末の記憶媒体を物理的に取り出されることによる漏えいリスクに対応することができる。一方で、サーバと利用者側端末との間で情報が伝達されることになり、盗聴されにくくする配慮はなされているものの、不可能ではないため、通信経路の暗号化等による適切な対応が必要である。

なお、シンクライアント技術には、主に、サーバでアプリケーションを実行し、その画面情報を利用者側端末に転送する方式と、サーバにある OS やアプリケーションを実行するためのデータを利用者側端末に転送し、データ処理を利用者側端末で行う方式がある。前者の方式は、サーバの画面情報の転送であり、利用者側端末で処理が行われないため、情報漏えいのリスクは低いが、転送する情報量が多くなる。後者の方式は、データ処理を利用者側端末で行うため、転送する情報量は相対的に少ないが、利用者側端末でのデータ処理に際して情報が記録されることになるため、情報漏えいのリスクは相対的に高くなる。このため、採用するシンクライアント技術の方式に合わせて、適切なリスク管理が必要である。

図９　シンクライアント技術（画像転送方式）



⑤　遠隔データ管理技術

社外に持ち出したモバイル PC に対して、専用のソフトウェアやハードウェアによって遠隔操作する様々な仕組みも存在する。これらは、携帯電話や Wi-Fi 等の通信網を用いて、モバイル PC のアプリケーションや BIOS 等に対して指示を出すものである。

例えば、モバイル PC が紛失、盗難にあった場合に、そのモバイル PC の機能を制限したり、起動できないようにしたりすることや、内部の情報や暗号化された情報の復号鍵を削除し、第三者に閲読されることがないようにすること等が可能となる。この場合には、指示を出した者がそれらの措置の実行結果を把握可能とするサービスも存在する。

また、モバイル PC の位置情報を管理し、紛失、盗難時に発見に向けた対応を可能にするようなサービスも存在する。

なお、これらの遠隔データ管理技術では、対象となるモバイル PC が通信圏外に持ち出された場合には、遠隔操作ができないことや、遠隔操作結果を得られないことがある。このため、サービスによっては、断続的な指示の送信や、圏外での起動抑止等の補完的な対応が取られている。

図 10　遠隔データ管理技術

３．求められる安全管理措置

（１）現行ガイドライン等での安全管理措置の規定の概要

法第 20 条では、個人情報取扱事業者に対し、取り扱う個人データの漏えい等が生じないよう安全管理措置を義務付けている。法第７条に基づき策定された「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定。以下「基本方針」という。）では、「事業運営において個人情報の保護を適切に位置づける観点から、外部からの不正アクセスの防御対策のほか、個人情報保護管理者の設置、内部関係者のアクセス管理や持ち出し防止策等、個人情報の安全管理について、事業者の内部における責任体制を確保するための仕組みを整備することが重要である」として、安全管理措置の必要性を規定している。基本方針を踏まえ、監督官庁で定めるガイドラインで、個人情報の安全管理措置について具体的に規定している。

現行ガイドラインでは、「電気通信事業者は、個人情報へのアクセスの管理、個人情報の持出し手段の制限、外部からの不正なアクセスの防止のための措置その他の個人情報の漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講ずるもの」としている。現行ガイドラインの解説では、安全管理措置を大きく組織的保護措置と技術的保護措置の２つに分類し、その双方を適切に実行することが必要であるとしている。その中で、個人情報の社外への持出しについては、「個人情報の持出し手段の制限（みだりに外部記録媒体へ記録することの禁止、社内と社外との間の電子メールの監視を社内規則等で規定した上で行うこと等）」と規定している。

（２）諸外国等での状況

①　諸外国での状況

諸外国では、多くの国で個人情報の保護に関する法令において個人情報の安全管理についての規定がなされているものの、持出時の安全管理措置について明確な規定を設けているものは多くない。

イギリス及びオーストラリアでは、監督機関の定めたガイドラインで、社外に持ち出す情報には暗号化措置を講じるという持出時の安全管理措置に言及している。カナダでは、「個人情報保護法　自己評価ツール」で、企業に対してテレワーク等個人情報の持出しを想定した社内規則を作成するよう求めている。また、韓国では、持出時の安全管理措置について明確な規定を設けてはいないものの、情報通信網を通じて利用者の個人情報を送受信する場合には、暗号化して送受信することを規定している。

一方、ドイツ、フランス、アメリカにおいては、持出時の安全管理措置について、ガイドライン等の指針を含め、明確な規定は設けられていない。

表５　諸外国における個人情報の安全管理措置

	主な個人情報保護制度	安全管理措置及び持出時の安全管理措置に関する規定について
イギリス	● 「1998年データ保護法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、ガイドラインに規定
フランス	● 「情報処理、情報ファイル及び自由に関する1978年1月6日の法律78-17号」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関しても、法律でカバーしているとの見解
ドイツ	● 「連邦データ保護法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
EU	● 「個人情報の取扱いに係る個人の保護及び当該情報の自由な移動に関する欧州議会及び理事の指令（データ保護指令）」を制定	● 安全管理措置については指令で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
韓国	● 「情報通信網利用促進及び情報保護に関する法律」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置に関する明確な規定は存在しない
オーストラリア	● 「1998年連邦プライバシー法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、インフォメーションシートに規定
カナダ	● 「連邦個人情報保護・電子文書法」を制定	● 安全管理措置については法律で規定 ● 持出時の安全管理措置については、「個人情報保護法 自己評価ツール」により企業内で定めることを推奨
アメリカ	● 連邦法では、個別法にて個人情報保護を規定 ● 州法においては、個人情報保護法を制定	● 安全管理措置について個別の法律内で規定 ● 民間部門においては、持出時の安全管理措置に関する明確な規定は存在しない
（参考） 日本	● 個人情報の保護に関する法律を規定	● 安全管理措置については法律で規定 ● 持出時に関する規定は、各分野のガイドライン内において個別に規定

2009年　11月の状況

②　他分野のガイドラインでの状況

他分野のガイドラインでは、現在、持出時の安全管理措置について明確に規定しているものは少ない。そのような規定があるものとしては、金融分野のガイドライン

（「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」）及び医療・介護分野のガイドライン（「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」）が挙げられる。

金融分野のガイドラインでは、持ち出す個人データを必要最小限に限定する等の事項を盛り込んだ安全管理措置に関する規程を設けるよう規定している。医療・介護分野のガイドラインでは、持出しに関する方針や情報の管理方法を運用管理規程で定めること、情報機器に対して起動パスワード、情報に対して暗号化・アクセスパスワードを設定すること等を掲げており、人的・組織的安全対策の面に加えて、技術的安全対策の面からも対策を講じるよう規定している。

③　その他

個人情報保護のみを念頭に置いたものではないものの、安全・安心にテレワークを導入するための情報セキュリティ対策という観点から、総務省では、平成 16 年 12 月に、「テレワークセキュリティガイドライン」を作成している。平成 18 年４月の改訂の際には、同ガイドラインを援用しつつ、職場外でパソコンを使用する際に想定される様々な危険性を前提に、モデルケースとしての対策を例示した「職場外のパソコンで仕事をする際のセキュリティガイドライン」も作成している。同ガイドラインでは、必要な対策について、「ルール」についての対策、「人」についての対策、「技術」についての対策に分け、19 項目を規定している。

表６　テレワークセキュリティ対策１９か条

（「ルール」についての対策）
①管理規程（管理者の選任、情報資産の管理方法の策定等）を構築する。
②職場外でパソコンが使用される場合でも、管理規定が正しく守られているか、定期的なチェック（監査）を実施する。
③社内システムへアクセスするためのアカウントについては、管理方法を明確に定め、厳格に管理する。
④従業員にパソコンを貸し出す際には、「氏名」、「担当業務」、「パソコン機種」、「連絡先」、「返却期限」、「情報セキュリティ対策状況」 等を把握しておく。
⑤業務用に貸し出されたパソコンは許可された目的内で利用条件に従って適切に用いる。
⑥時的に職場外に持ち出す情報は原本ではなく、原本からの複製とする。
⑦私物のパソコンを業務に利用する場合には、インストールされているソフトを確認する等定められた利用条件に従う。
⑧ネットワークを用いて業務を実施する際には、指定された通信手段を用いる。

（「人」についての対策）
⑨トップダウンにより管理規程を周知・徹底する。
⑩従業員の情報セキュリティに関する認識を確実なものにするために、日々、教育・啓発活動を実施する。
⑪就業規則や外部委託契約に情報の持ち出しに当たっての許可等機密保持規定や罰則規定を設ける。
⑫漏えい事故発生時は、直ちに定められた担当者に連絡する。

（「技術」についての対策）
⑬ウイルス対策ソフトをインストールし、最新の定義ファイルに定期的に更新する。
⑭ＯＳ及びソフトウェアにおいては、パッチの更新を定期的に行う。
⑮ＯＳのログイン時等のパスワードは、他人に推測されにくいものとし、定期的に更新を行う。
⑯機密性の高い情報を持出・保存・送信する際には必ず暗号化する。
⑰社内システムと持ち出し用パソコンの環境の境界線にはファイアウォールやルータ等を設置し、不必要なアクセスを遮断する。
⑱社内システム内にある重要情報は、安全な領域に格納するとともにアクセス権限の付与は必要最低限とする。

※「職場外のパソコンで仕事をする際のセキュリティガイドライン（平成18年4月 総務省） 概要より抜粋

（３）持出時の安全管理措置を講じる際の考え方

モバイル PC 等による社外への個人情報の持出時に、個人情報の漏えいリスクに対応するために必要な安全管理措置を講じる場合には、リスクの評価、リスクに対応する措置の検討・決定、決定した措置の適切な運用、という手順で対策を行うことが必要である。

① リスクの評価

まず、持ち出す情報の種類、内容やその分量、持ち出す従業員の範囲や持ち出す方法、社内での管理状況等の関連する状況を踏まえ、どのようなリスクがどこで生じるのか等、個人情報の持出時に想定される具体的なリスクを網羅的に評価することが必要である。

② リスクに対応する措置の検討・決定

リスクの評価の後、それらのリスクに対応するために必要とされる安全管理措置を検討し、決定することが必要である。その際には、技術的保護措置と組織的保護措置との双方についての検討が必要となる。

まず、個々の技術的保護措置には、その技術の特性から強い点・弱い点が存在することから、それぞれの特性を把握した上で、リスクに適切に対応できるように具体的な措置を選択することが必要である。その際には、一つの措置で全てのリスクに対処するのではなく、複数の措置を適切に組み合わせることが重要である。

次に、講じようとする技術的保護措置の技術的に最も弱い部分を確認することが必要である。導入コストをかけて部分的にセキュリティ強度を強固にしても、相対的に技術的に弱い部分があれば、その部分から問題が生ずるおそれがあるため、技術的に最も弱い部分を把握し、その部分に対応する措置が十分なものなのかを検討することが必要である。

さらに、技術的保護措置の検討に当たっては、措置を講ずることによる利便性への影響及び導入コストと、持ち出された個人情報の安全性の双方を勘案することが重要である。一般に、利便性や導入コストと安全性とはトレードオフの関係にあるため、評価したリスクについて、利便性や導入コストと安全性の双方のバランスを判断して適切な措置を決定することが必要である。

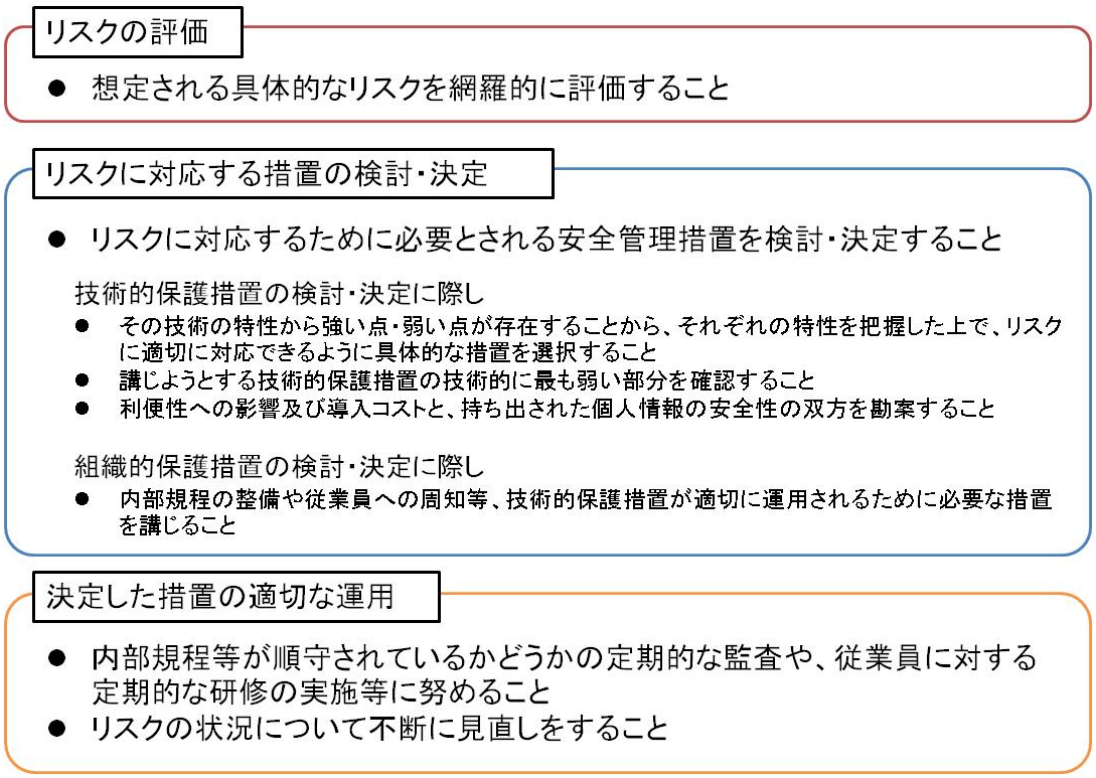
組織的保護措置については、内部規程の整備や従業員への周知等、技術的保護措置が適切に運用されるために必要な措置を講じることが必要である。

③ 決定した措置の適切な運用

リスクに対応する安全管理措置を決定しても、それが適切に運用されていないとリスクは低減されない。このため、内部規程等が順守されているかどうかの定期的な監査や、従業員に対する定期的な研修の実施等に努めることが必要である。さらに、持

出しの状況の変化や技術の進歩等、リスクの状況は変化していくものであるため、リスクの状況について不断に見直しをすることが必要である。

図 11　持出時の安全管理措置を講じる際の考え方



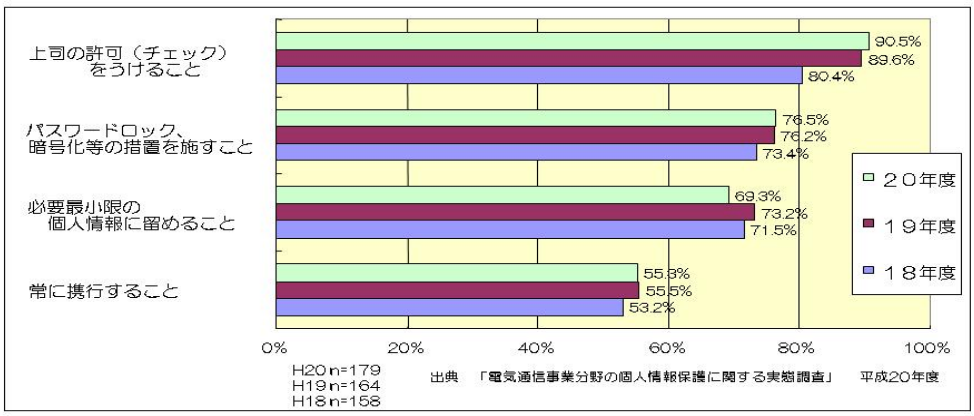
（４）技術的保護措置についての検討の必要性

安全管理措置は、前述のとおり、組織的保護措置と技術的保護措置の２つに大きく分けられる。モバイル PC 等による個人情報の社外への持出しに当たっての安全管理措置としては、その双方を一体的・総合的に講じることが必要である。

組織的保護措置については、内部規程の策定、適切な運用がなされているのかの監査、従業員の教育や監督等であり、講じるべき措置については、社内での個人情報の取扱いに関する措置と大きな相違点は存在しないものと思われる。ただし、具体的内容については、持出時にも対応するような内部規程の修正、持出時を対象とした監査、従業員の教育や監督等が必要になる。

一方で、技術的保護措置については、持出時の漏えいリスクに対応した技術的対応策がでてきており、それらは社内で用いられる技術的対応策とは異なるものも多く、具体的な留意点等も異なるものと思われる。また、現状としても、事業者によっては必ずしも適切な技術的保護措置が講じられていないものと思われる。前述の「平成 20 年度電気通信事業分野の個人情報保護に関する実態調査」では、社外に持ち出した業務用 PC で取り扱う個人情報に暗号化、パスワード設定等をしていると回答した事業者は 70%を超えており、ある程度の技術的保護措置が講じられている。しかし、法施行以来、電気通信事業分野における個人情報の漏えい事案として総務省に報告されたもののうち、ノート PC の紛失は 17 件あり、それらの事案で講じられていた技術的保護措置として、IC カードによる PC の起動制御に加え記録媒体の暗号化措置など、個人認証と暗号化による複数の安全管理措置を講じているケースが４件、暗号化措置のみを講じていたケースが１件、BIOS や OS へのパスワード措置を講じていたケースが 11 件、まったく措置をしていないものが１件で、必ずしも十分な安全管理措置が講じられているとはいえない状況である。

図 12　個人情報の入ったノート PC 等を社外に持ち出す場合のルール



このため、以下では、モバイル PC 等による個人情報の社外への持出しに当たって必要とされる安全管理措置について、技術的保護措置を中心に検討する。

（５）技術的保護措置を講じる場合の考え方

① 基本的事項

モバイル PC 等により個人情報を社外に持ち出す場合に必要とされる技術的保護措置に関する基本的事項として、次の事項が挙げられる。

ア モバイル PC 等を社外に持ち出す場合に必要な技術的保護措置

モバイル PC 等を社外に持ち出す場合には、常に紛失、盗難に遭うリスクがあり、その場合には、当該モバイル PC 等を権限のない者に使用されることによる漏えいリスクが生ずる。

このため、権限のない者に使用させないように、モバイル PC の BIOS、OS の起動時等で個人認証技術を導入することが必要である。

また、本来想定していなかった使用方法による個人情報の漏えいを防ぐため、通信カードや USB 等不必要な外部媒体について、内部規程で使用しないように定めるのみならず、物理的に接続を制限することが必要である。

さらに、持出先で通信カードや USB 等の外部媒体を接続する場合や、インターネットに接続する場合には、それらを通じてウイルスの侵入を受け、内部の情報が漏えいするおそれがある。そのような事態に備え、常にモバイル PC の OS・アプリケーションを最新のセキュリティ水準に維持するようにしておくことが必要である。

イ モバイル PC 等に情報を保存する場合に必要な技術的保護措置

モバイル PC 等に個人情報を含む情報を保存して社外に持ち出す場合には、紛失、盗難に遭った場合に、当該モバイル PC 等を権限のない者に使用されることによる漏えいリスクに加えて、記録媒体を物理的に取り出されることによる漏えいリスクも生ずる。

このため、持ち出す情報を暗号化することが必要である。その際、社外において個人情報を含む情報を保存することが考えられる場合には、保存した情報が常に暗号化されているようにし、暗号化されていない情報が持ち出したモバイル PC 等の内部に存在しないようにすることが必要である。

ウ モバイル PC をネットワークに接続する場合に必要な技術的保護措置

モバイル PC を用いて社外からネットワークに接続し、個人情報をやり取りする場合には、ネットワーク上を流通する情報を盗み取られることによる漏えいリスクが生ずる。

このため、第三者から通信内容を盗み見られないよう、暗号化通信を行うか、やり取りするファイル自体を適切に暗号化することが必要である。

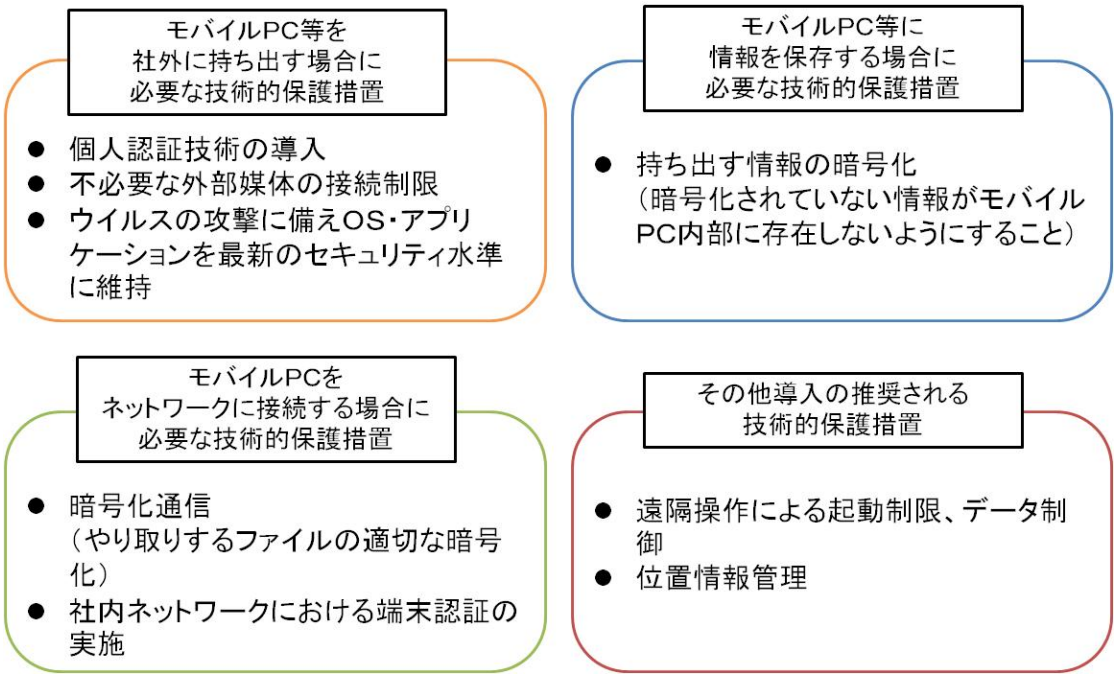
また、持ち出したモバイル PC から社内ネットワークに接続可能である場合には、第三者に社内ネットワークに侵入され、情報を盗み見られるおそれもある。

そのような事態を防ぐために、社内サーバ側においてクライアント認証を実施し、社内ネットワークに入る権限のある者だけが情報を見ることができるように措置を講じることが必要である。

エ　その他の措置

現在、モバイル PC の紛失、盗難に備え、遠隔操作によって起動制限、データ制御、位置情報管理等を行う技術も存在する。これらについては、導入することによりさらに個人情報の漏えいリスクに対応することが可能になるため、以上のような措置に加えて導入しておくことが推奨される。

図 13　利用状況に応じて必要とされる、持出時の技術的保護措置



② 個別技術に関する留意事項

それぞれの技術的保護措置を講じる場合には、適切な安全性を確保するために、その技術に応じ、以下のような点に留意する必要がある。

ア 個人認証技術

個人認証技術を講じるに当たっては、本人認証性を高め、第三者が簡単に個人認証を破ってモバイルPC等を使用することがないよう、それぞれの認証技術に応じ、以下の点に留意することが必要である。また、複数の認証技術を組み合わせ、二重三重の認証を講じることが望ましい。

（ア）パスワード等記憶による認証

認証に用いるパスワードは、第三者から容易に推測されないよう、辞書等に記載されている単語を避けること、複数の英数特殊文字を組み合わせること、適切な文字数以上の長さのものを使用すること等に注意することが必要である。また、定期的にパスワードを変更することが必要であり、その際には、少数のパスワードを定期的に使いまわすことは避けるべきである。これらの条件を満たしたパスワードを自動生成ソフトによって作成することや、また、システム的に不適切なパスワードは設定できないようにすることが可能な場合もある。

また、従業員によるパスワードの管理が適切に行われることも必要である。具体的には、メモ等に書き込んで放置したりしないこと、ソフトウェアに記憶させないこと等他人に知られないようにすることが必要である。

コンピュータを用いた総当たり攻撃によって権限のない第三者が認証を破ることも考えられるため、認証に複数回失敗した場合には、一定時間認証を不可能にすることや、その後の認証自体を不可能にする等の措置を講じることが望ましい。

（イ）ICカード等所有物による認証

所有物とモバイルPCを同時に紛失、盗難に遭った場合には、容易に認証を破られてしまうことから、同時に紛失、盗難に遭わないように適切に管理することが必要である。また、それに加えて、所有物による認証時に、パスワードによる認証も併せて実施することが望ましい。

（ウ）指紋等生体情報による認証

生体情報による認証の中でも、音声認証や顔認証のように他人受入率が１％～0.1%のものもあれば、指紋認証や静脈認証のように他人受入率が 0.001%～0.00001%のものもあるなど、その方式により本人認証性に差がある点に注意して、導入する方法を選択することが必要である。

イ　暗号化措置・鍵の管理

（ア）暗号アルゴリズム

暗号化措置を講ずるに当たっては、技術的な確証がある暗号アルゴリズムを用いることが必要である。具体的には、公的機関による客観的評価がなされているものとして、CRYPTREC で策定された電子政府推奨暗号リストや ISO/IEC で策定された国際標準規格 ISO/IEC18033 で公表されている暗号アルゴリズムを使用することが強く推奨される。

（イ）復号鍵の管理

情報を暗号化していたとしても、復号鍵が第三者に利用されては、暗号化は意味をなさない。そのため第三者が容易に復号鍵を入手できないように、復号鍵の管理を適切に行うことが必要である。

最も確実な方法として、復号鍵を暗号化された情報から物理的に分けて管理する方法がある。例えば、IC カード等の別の媒体の中に復号鍵を保管する方法や秘密分散法により復号鍵を分散する方法がある。この場合には、その媒体がモバイル PC と同時に紛失、盗難に遭うことがないよう管理を徹底すること、媒体による復号時にパスワードによる認証を併せて実施すること等の措置を講じることが望ましい。

復号鍵をモバイル PC と物理的に分けて管理しない場合には、常にモバイル PC と同時に紛失、盗難に遭うリスクが存在する。その場合には、復号鍵を盗みだそうとする攻撃から守ることのできる耐タンパ性を持った、モバイル PC 中のチップ上で管理する方法が考えられる。また、紛失、盗難に遭った際に、復号鍵を遠隔操作により削除し、第三者が復号鍵を入手できないようにすることも考えられる。

（ウ）暗号化の対象

暗号化の対象としては、個別のファイル、特定のフォルダ、記録媒体全体等の中から選択することになる。

ファイル、フォルダの暗号化の場合には、暗号化の対象外となる情報があるため、個人情報を含む情報が確実に暗号化されるようにすることが必要である。特に、自動的に生成される作業用ファイルやバックアップファイル等については、ソフトウェアによって格納される場所が異なることから、注意が必要である。

ウ　遠隔データ管理技術

遠隔操作によりモバイル PC を管理する場合には、通信可能な圏外に持ち出された場合等、遠隔操作が不可能となる事態や指示を実行するまでにモバイル PC を使用さ

れる事態をあらかじめ想定し、個人認証技術や情報の暗号化等の他の技術と組み合わせて対応することが必要である。

　また、遠隔操作の指示をしたとしても、それが正しく実行されない可能性もあるため、指示の実行状況を把握できるようにすることが望ましい。

（６）導入コスト等

以上で見てきた技術的保護措置については、現在、それほど多額の費用をかけることなく、最低限の安全性が確保できる措置の導入が可能である。

例えば、暗号化措置については、OS に標準装備されている機能や、一般に市販されているソフトウェアによって導入することが可能である。個人認証についても、パスワード認証は、モバイル PC の BIOS や多くの OS やソフトウェアで設定が可能である。また、多くのモバイル PC では USB ポートを標準装備しており、USB キーを利用した所有物による認証の導入のコストは大きくない。さらに、指紋認証のための読取機能があらかじめ内蔵されている PC も存在する。

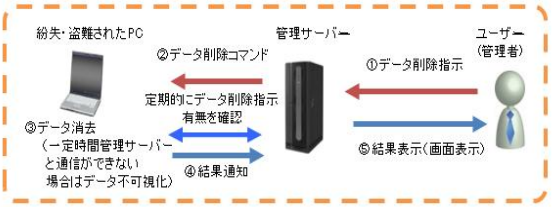
携帯電話端末については、現在、それぞれの事業者により具体的な機能は異なるが、紛失、盗難時に備え、端末のロック機能や指紋認証等、携帯電話端末に保存された情報を保護するための機能が提供されている。

さらに、様々な機能を組み合わせて、一定レベルの安全性を確保するサービスも存在している。それぞれのサービスにより対応するリスクや確保される安全性の程度が異なり、また、導入に係る費用も異なっている。このため、そのようなサービスを利用する場合には、どのような技術が組み合わされており、どのようなリスクに対して、どれだけの安全性が確保されているのか等を確認し、自社におけるリスクへの対応として十分であるのかを検討することが必要である。

図 14　現在あるソリューション事例

【ソリューション事例】（KDDI株式会社）　平成21年11月時点

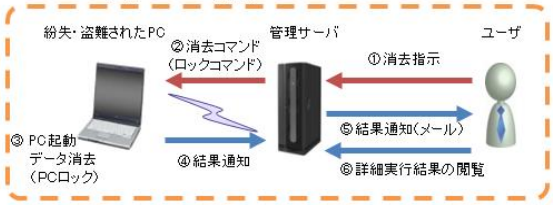
遠隔操作によって該当データの上書きを指示し、データを削除



- 遠隔操作でPCの指定されたデータを削除（データの上書き）
- インターネット接続中は、定期的に管理サーバーと通信し、データ削除指示有無を確認
  インターネット接続がない環境でも、PCにKDDI指定の通信カード等を使用の場合、電源ON時等に強制的に管理サーバーと通信し、データ削除指示有無を確認
- 一定時間管理サーバと通信ができない場合は、指定されたデータを不可視化

【ソリューション事例】（富士通株式会社、株式会社ウィルコム）

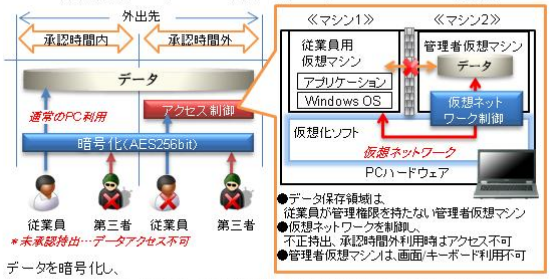
遠隔操作によって、PCの起動制限、データの復号鍵を消去し、ハードディスク内データを消去



- 遠隔操作でPCの起動を制限（PCロック）
- 遠隔操作でPCのハードディスク内の全データを即時消去（復号鍵の消去）
- PCが電源オフ状態でも実行可能（専用の通信モジュールを搭載）
- 消去結果や、PCへのアクセス履歴を含むレポートを通知

【ソリューション事例】（株式会社 東芝）

データ保存領域のアクセスを制御し外出時のセキュリティを強化

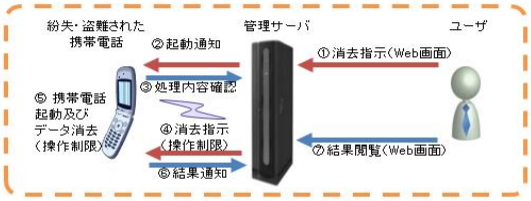


データを暗号化し、

- 承認時間内は、パスワード等がないと利用不可（パスワード等を持ち得ない第三者は、利用不可）
- 承認時間外は、パスワード等があっても利用不可（従業員であっても、利用不可）

【ソリューション事例】（株式会社NTTドコモ）

遠隔操作によって操作制限や、データ消去プログラムを起動し、携帯電話内のデータを消去



- 遠隔操作で端末の操作を制限
- 遠隔操作で携帯電話の全データを消去し、工場出荷時に戻す
- 本体のみならず、SIMカード内の電話帳データやmicroSD内も削除
- 消去指示結果を通知（５分程度で操作履歴画面に反映）

（７）個人情報の持出しに関する留意点

モバイル PC 等による個人情報の社外への持出しに際して、適切な技術的保護措置を講じることにより、モバイル PC 等が紛失、盗難に遭っても、被害を最小限に抑えることが可能な場合もある。

しかし、技術的保護措置を講じているからといって、紛失、盗難に遭っても良いものではなく、そのような事態にならないように、モバイル PC 等が適切に管理されるようにすることが必要である。

また、持ち出す個人情報は、業務上必要最小限の範囲にすることが必要である。例えば、業務上必要な分量を超えた個人情報や業務上必要でない種類の個人情報を持ち出すことは避けるべきである。その際、現行ガイドライン第４条で取得を制限しているいわゆるセンシティブ情報等、漏えいした場合に本人の権利利益の侵害の程度が大きい個人情報については、安易に外部に持ち出すことのないようにするとともに、持ち出す必要がある場合には、より高い安全性が確保されるような技術的保護措置を講じることが必要である。

４．漏えい等の発生時の手続の在り方

（１）現行ガイドライン等での漏えい等の発生時の手続の概要

個人情報の漏えい等の発生時の手続に関して、法には直接的な規定はない。基本方針では、「個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係を公表することが重要である」と規定している。監督官庁で定めるガイドラインの多くでは、基本方針の趣旨を踏まえ、個人情報取扱事業者に対し、本人への通知、公表、監督官庁への報告等、漏えい等の発生時の手続を求めている。

現行ガイドラインでは、個人情報の漏えいが発生した場合は、その個人情報の本人が適切に対応できるようにするため、事業者は本人の連絡先が不明である場合を除き、事実関係を本人に速やかに通知することを規定している。なお、個人情報の漏えいにはあたらない滅失又はき損の場合は、個人情報の本人の権利利益には影響がない場合もあるため、一律に本人への通知を要するものとはしていない。

また、個人情報の漏えい等が発生した場合には、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することを規定している。ここで、「可能な限り」とされている理由は、セキュリティの観点から公表するとかえって二次被害の拡大や類似事案の増大につながるようなものは公表することを要しないが、そのおそれのない場合については、二次被害の防止、類似事案の発生回避等に有用な情報をできるだけ公表すべきであるとの考え方によるものである。

さらに、個人情報の漏えい等が発生した場合には、事実関係を総務省に直ちに報告することを規定している。この報告が必要とされる理由は、監督官庁を通じた漏えい等の事案の周知等による本人への二次被害の防止や類似事案の発生回避、監督官庁による適切な技術的保護措置等の再発防止策の確認、今後の行政施策への反映等のために、行政が速やかに適切な対応をとることを可能とするものである。

（２）諸外国等の状況

① 諸外国での状況

ア 漏えい等の発生時の手続

諸外国では、多くの国の個人情報の保護に関する法令において、個人情報の漏えい等の発生時に、個人情報を取り扱う者が執るべき手続について規定されており、また、現在そのような規定がない国の多くにおいても、今後それらの規定の整備が検討されている。

ＥＵでは、「電子通信分野における個人データ処理及びプライバシー保護に関する2002 年７月 12 日の欧州議会及び理事会指令（電子プライバシー指令）」において、個人情報漏えい等の発生時に、個人情報を取り扱う者が権限のある当局へ遅滞なく通知を行うこと、本人へ影響を及ぼしそうな場合には、その本人へ遅滞なく通知を行うことを規定している。

イギリス、ドイツ、オーストラリアでは、法又はガイドラインにおいて、本人への通知、公表、政府等への報告等、個人情報漏えい等の発生時に個人情報を取り扱う者が執るべき手続を規定している。フランス、韓国、現在、そのような手続を規定していないが、本人及び監督機関への報告を法律等により義務化する方向で検討が進められている。

カナダでは、ガイドラインを根拠とした漏えい時の手続を法律で規定することが検討され、アメリカでは、これまで分野別個別法や州法により手続を求めていたものを連邦法で規定する動きもある。

イ 適切な技術的保護措置が講じられている場合の手続

紛失した個人情報に適切な技術的保護措置が講じられていた場合について特段の整理をしている国もある。

オーストラリア、カナダでは、ガイドラインで、紛失した個人情報に適切な暗号化がされており、その後回収され、調査の結果当該情報に手が付けられていないことが判明した場合には、本人への通知が不要である旨の考え方が示されている。

アメリカでは、「経済的・臨床的健康のための健康情報テクノロジー法」で、ガイダンスで特定するテクノロジー又は方法に基づいて、権限のない個人が利用、判読、解読できないよう保護された医療情報の漏えいに際しては、関係者への通知義務は発生しない旨の規定を設けている。

ＥＵでは、電子プライバシー指令において、個人情報を取り扱う者が適切な技術的保護措置を講じ、当該措置が漏えい等の発生した情報にも適用されていたことを権限のある当局に立証できた場合は、関係者への通知を求めないものとされている。

表７　諸外国における個人情報の漏えい時等に求められる手続

	主な個人情報保護制度	個人情報の漏えい等が発生した際に求められる手続について
EU	● 「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事の指令（データ保護指令）」を制定	● 電子通信分野における個人データ処理及びプライバシー保護に関する2002年7月12日の欧州議会及び理事会指令」（電子プライバシー指令）にて、本人及び監督機関への報告を義務化（2011年5月までに指令に関する加盟国は国内法制化） ● 漏えい等の発生した情報に適切な技術的な保護措置を講じていたことを、権限のある当局の得心のいくように立証できた場合は本人や関係者への通知は不要
イギリス	● 「1998年データ保護法」を制定	● 本人への通知、公表、監督機関への通知についてガイドラインにて規定 ● 通知の手続を緩和する規定は存在しない
フランス	● 「情報処理、情報ファイル及び自由に関する1978年1月6日の法律78-17号」を制定	● 現在、本人及び監督機関への報告を法律で義務化する方向で議論中
ドイツ	● 「連邦データ保護法」を制定	● センシティブ情報、銀行の口座情報等が漏えいした場合は、関係者への通知（もしくは公表）、監督官庁への報告を法律で義務化 ● 通知の手続を緩和する規定は存在しない
韓国	● 「情報通信網利用促進及び情報保護に関する法律」を制定	● 現在、本人及び監督機関への報告を法律で義務化する方向で議論中
オーストラリア	● 「1998年連邦プライバシー法」を制定	● 本人への通知（もしくは公表）、監督機関への通知についてのガイドラインにて規定 ● 同ガイドラインにおいて、漏えいした情報が適切に暗号化されており、その後回収され、調査の結果当該情報に手を付けられていないことが判明した場合は本人への通知不要との例示
カナダ	● 「連邦個人情報保護・電子文書法」を制定	● 本人への通知（もしくは公表）、監督機関への通知についてのガイドラインにて規定（法律化を検討中） ● 同ガイドラインにおいて、漏えいした情報が適切に暗号化されており、その後回収され、調査の結果当該情報に手を付けられていないことが判明した場合は本人への通知不要との例示
アメリカ	● 連邦法では、個別法にて個人情報保護を規定 ● 州法においては、個人情報保護法を制定	● 医療分野の個別法では本人への通知、公表、監督機関への通知を義務化（連邦法での規制化の動きがある）。 ● 同法では、権限のない個人が解読等できないよう保護された医療情報の漏えいに際しては、本人への通知、公表及び監督機関への通知不要との規定
（参考）日本	● 個人情報の保護に関する法律を規定	● 各分野の多くのガイドライン内において、本人への通知、公表及び監督官庁への報告を規定 ● 経済産業省のガイドライン等では、高度な暗号化措置が施されていた場合には、本人への通知及び公表が不要の規定（監督機関への報告は必要）

2009年　11月の状況（EUについては2009年　12月の状況）

②　他分野のガイドラインでの状況

個人情報の漏えい等の発生時に適切な技術的保護措置が講じられていたときの手続の在り方について、他分野のガイドラインでも、その一部において、特別の規定が設けられているものがある。

金融庁で公表している「金融機関における個人情報保護に関するQ&A」では、「漏えい事案が発生した場合において、高度な暗号化処理等が施されている場合等」、「本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さい場合等には」、「本人への通知を省略し得るケースもある」としている。また、経済産業分野のガイドライン（「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」）では、「高度な暗号化等の秘匿化が施されている場合」等、「本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には」、本人への通知、公表の手続を「省略しても構わないものと考えられる」ことが規定されている。

（３）簡略化可能な手続

① 手続の必要性

個人情報の漏えい等の発生時の手続として、現行ガイドラインで求められている事実関係の本人への通知、公表、監督官庁への報告については、二次被害の防止、類似事案の発生回避等の観点から、今後も原則として継続することが適当である。

一方で、モバイルPC等の紛失、盗難、破損等（以下「モバイルPC等の紛失等」という。）に際し、漏えい等が発生した個人情報に対して本人への二次被害が生じないよう適切な技術的保護措置が講じられている場合には、一部の手続の簡略化は可能と考えられる。

② 本人への通知

事実関係の本人への通知については、漏えいが発生した個人情報に対して本人への二次被害発生の防止のために求められているものであることから、漏えいが発生した個人情報に対して本人への二次被害が生じないよう適切な技術的保護措置が講じられている場合には、必要としないことができるものと思われる。

③ 公表

公表については、漏えい等が発生した個人情報に対して本人への二次被害発生の防止という観点からは、漏えい等が発生した個人情報に対して本人への二次被害が生じないよう適切な技術的保護措置が講じられている場合は、必要としないことができ、類似事案の発生の回避の観点からは、事業者それぞれの個別の公表ではなく、類似事案発生のおそれがある事案について監督官庁による発表等の手段により、これに代替することができると思われる。

④ 監督官庁への報告

監督官庁への報告は、監督官庁を通じた漏えい等の事案の周知等による本人への二次被害の防止や類似事案の発生回避、監督官庁による適切な技術的保護措置等の再発防止策の確認、今後の行政施策への反映等の観点から求められている。

まず、漏えい等が発生した個人情報に対して本人への二次被害が生じないような適切な技術的保護措置が講じられていたのか、監督官庁において確認することが必要である。

また、事案の発生に係る事実関係の確認や再発防止策について、単に事業者が自ら講ずるのみならず、監督官庁で確認、検証し、仮に再発防止策等が不適切な場合には、改善の指導や、場合によっては、法に基づく命令、勧告等を行うことも必要となる。

さらに、監督官庁において、問題事案を分析し、類似事案発生のおそれがある事案について発表を行う等、必要に応じて個人情報保護の施策に反映させること等も必要である。

以上のことから、適切な技術的保護措置が講じられていたとしても、講じられた技術的保護措置の内容、事案の発生に係る事実関係及び再発防止策等について、監督官庁への報告が必要である。

ただし、現行ガイドラインでは、漏えい等の発生時に「直ちに」報告することとされているが、本人への二次被害が生じないよう適切な技術的保護措置が施されている場合には、本人への被害が切迫している等の状況が存在しないことから、例えば、四半期ごとにまとめて報告することを認容する等、提出期限の緩和等の措置を講ずることは可能である。

⑤　なお、モバイル PC 等の紛失等に際し、適切な技術的保護措置が講じられていたと事業者が判断し本人への通知、公表を省略したが、その後、適切な技術的保護措置が講じられていなかったことが判明した場合には、当然のことながら、速やかに本人への通知や事実の公表を行う必要がある。

そのような場合には、監督官庁においても、適切な技術的保護措置が講じられていなかった原因等を究明することが必要となる。

表８　適切な技術的保護措置が講じられていた場合等の手続の在り方

	個人情報の漏えい		個人情報の滅失、き損	
適切な技術的保護措置の有無	現行ガイドラインにおける手続	適切な技術的保護措置が講じられていた場合	現行ガイドラインにおける手続	適切な技術的保護措置が講じられていた場合
本人への通知	事実関係を速やかに通知 →	省略可能	一律に本人への通知を要するものとはしていない	省略可能
公表	可能な限り事実関係等を公表 →	省略可能	可能な限り事実関係等を公表 →	省略可能
監督官庁への報告	監督官庁へ直ちに報告 →	監督官庁への報告期限を緩和	監督官庁へ直ちに報告 →	監督官庁への報告期限を緩和

（４）適切な技術的保護措置

手続を簡略化することが可能な「適切な技術的保護措置」が講じられている場合については、次のようにまとめることができる。

① 基本的な考え方

ア 単に「高度な暗号化等」というだけでは、技術的保護措置の内容の具体性に欠けること、また、高度な暗号化が施されていたものの個人認証であるパスワード等や復号鍵の管理が不十分な場合には暗号化措置を施していた意味がなくなることから、事業者がどのような技術的保護措置を講ずれば良いのかの判断基準としては適当ではない。

イ できる限り具体的な基準とするため、暗号アルゴリズムのように客観的な評価が既にあれば当該評価を参照するが、そのような客観的評価がない場合にはそのような具体的基準を設けることは困難であり、確実に二次被害が防止されるような定性的基準を採用する。

ウ 時間を経るごとに技術の安全性が変化することや、より安全性の高い技術が登場することも考えられるため、適切な技術的保護措置については、必要に応じて見直しを実施することが必要である。

② 上記の基本的な考え方を前提とした上で、モバイル PC 等の正規の利用者又は権限者（例えばシステム管理者）だけしか、紛失等にあったモバイル PC 等に搭載された情報を見ることや利用することができない適切な技術的保護措置として、次のア～ウのいずれを満たすものが考えられる。

ア 高度な暗号化措置が講じられていること

電子政府推奨暗号リスト又は ISO/IEC 18033 に掲げられている暗号アルゴリズムによって、記憶媒体内の個人情報の保存先として利用可能な全領域（使用者が意図しない自動保存を含む。）が自動的に暗号化されること

イ 適切な暗号化された情報及び復号鍵の管理がされていること

次の（ア）又は（イ）の方法によって暗号化された情報及びその暗号化された情報を復号可能な復号鍵の管理が適切にされていること。ただし、使用する暗号化措置は、（ア）の方法においては暗号化された情報から分離された復号鍵の、（イ）の方法においては遠隔操作により削除された復号鍵の権限者以外による不正な複製及び再生成ができないこと。

（ア）次のＡ又はＢの方法によって暗号化された情報と復号鍵が分離されていること

Ａ　復号鍵の全てが暗号化された情報と分離され、紛失した暗号化された情報の復号鍵が権限者の管理下に置かれるように構成されていること

Ｂ　公知の方式を用い、かつ分散された情報の一部からの全体の復元が不可能であることが立証された秘密分散技術によって復号鍵が分散保存され、当該復号鍵の構成部分のうち、紛失した暗号化された情報と分離されない構成部分では復号ができず、かつ、紛失した暗号化された情報と分離されている全ての構成部分は権限者の管理下に置かれるように構成されていること

（イ）遠隔操作により記憶媒体内の復号鍵又は暗号化された情報（あるいはその両方）を削除でき、かつ、記憶媒体内の復号鍵又は情報を削除するまでの間に、復号鍵の複製、情報の閲覧、複写がされていないことを権限者側で確認できること

ウ　個人情報の漏えい等に際し、ア及びイの技術的保護措置が有効に実施されていること。

（５）手続の簡略化に当たっての留意点

① 暗号技術の危殆化

適切な暗号アルゴリズムにより対象となる個人情報が暗号化されていれば、一般には第三者がその個人情報を取得しても、それを解読すること等は困難である。しかし、暗号技術は、設計時有効な暗号アルゴリズムであっても、解読技術の発展、コンピュータ能力の向上等によって、将来的には強度が弱くなる宿命にある。このため、将来にわたり 100%の安全性が確保されない限り、個人情報の漏えい等の発生時の手続の簡略化を認めるべきでないという考え方もあり得るが、そのような考え方は、次の点から適当ではないと考えられる。

ア 暗号技術は、インターネットでのショッピング、携帯電話での通信、地上デジタル放送の受信、電子メールへの電子署名等に用いられ、現代社会の必須技術ともなっており、関係者による検証が不断に行われていること、脆弱性が認知されても実害が生じるまでにはタイムラグがあり、現実的にセキュリティ上の問題が生じるおそれは極めて少ないこと（直ちに本人への二次被害が生じるものではないこと。）

イ コストや利便性を考慮すると、100%に限りなく近い安全性を求めることは現実的ではなく、この点は、他の技術でも同様で、個人情報漏えい等の発生時の技術的保護措置のみ将来にもわたって 100%の安全性を求めることは適当ではないこと。

② センシティブ情報について

個人情報のなかでも、いわゆるセンシティブ情報については、漏えい等が発生した場合に本人への二次被害の程度が大きいものと思われる。このため、センシティブ情報の有無やその内容により、手続の簡略化の是非を決めることも考えられるが、そのような考え方は、現時点においては、次の点から適当ではないと考えられる。

ア 現時点において、法は、「センシティブ情報」を定義しておらず、また、監督官庁が定めるガイドラインにおいても統一的な運用がなされていないこと。

内閣府が平成 18 年９月に実施した「個人情報の保護に関する世論調査」では、「他人に知られたくない個人情報」として上位を占める情報は、（ア）銀行口座番号、クレジットカード番号、取引履歴、（イ）年間収入、財産状況、納税額等、（ウ）顔写真等の画像、（エ）電話や電子メール等の通信記録、（オ）家族構成、結婚歴、離婚歴等、（カ）現住所、電話番号、（キ）年金、生活保護等の公的扶助の受給の有無、（ク）メールアドレス、（ケ）病歴、身体の障害等、（コ）学歴、職歴等であった。「他人に知られたくない情報」は、一般にセンシティブ度が高いほど本人への二次被害の程度が高くなるものと考えられるが、センシティブ情報については、それぞれの国、地域の固有の歴史、文化を背景とする側面もあり、また、個人の受け止め方も異なることから、定義は容易ではなく、現に法においても定義はなされていな

い。監督官庁が定めるガイドラインにおいては、センシティブ情報の取得制限を行う観点からセンシティブ情報の例を掲載することが少なくないが、統一的な見解によるものではない。

イ　個人情報保護に関しては、グローバルな視点も重要であることから、現行ガイドラインへのセンシティブ情報の適用については､上述の国際的な議論も踏まえつつ、今後検討することが適当であること。

国際的には、データ保護プライバシー・コミッショナー国際会議で、50 カ国のプライバシー保護機関が共同して「国際個人データ・プライバシー保護基準」を策定しようとする議論がなされている。センシティブ・データの定義に関しては、抽象的に､「a.データ主体の最も機微な領域に影響するデータ、又は b.悪用の場合に ⅰ.違法な若しくは恣意的な差別､又は ⅱ.データ主体に対する重大な危険を引き起こすおそれのあるデータ」を挙げるとともに、ＥＵデータ保護指令等で規定されているセンシティブ・データ（人種、民族、政治的見解、宗教、思想、信条、労働組合への加盟、健康又は性生活に関するデータ）に言及しているが、この基準が策定されるまでには、まだ期間を要するものといわれている。

ウ　適切な技術的保護措置が講じられていれば､モバイル PC 等の紛失等にあったとしても、含まれている情報の種類にかかわらず、現実的には個人情報が判読、解読されるおそれはないこと。

５．現行ガイドラインの改正の方向性

（１）モバイル PC 等による個人情報の社外への持出しの際に講ずるべき安全管理措置、適切な技術的保護措置が講じられていたときの手続の簡略化について、第３章及び第４章の検討結果に基づき、現行ガイドラインの改正を行うことが適当である。

具体的には、現行ガイドライン第 11 条（安全管理措置）で、持出時の漏えいリスクに対する安全管理措置に係る検討事項、漏えいリスクに対応する具体的な技術的保護措置及び個人情報の持出時の留意点について、明示することが適当である。

また、現行ガイドライン第 22 条（漏えい等が発生した場合の対応）で、モバイル PC 等の紛失等に際し、漏えい等の発生した個人情報に対して適切な技術的保護措置が講じられていた場合の本人への通知、公表、監督官庁への報告に関する手続の緩和措置を設けることが適当である。

（２）平成 21 年度「情報通信白書」において、国民は「情報通信利用」に関する不安を感じている傾向が高いという結果が示されているなど、国民には「情報セキュリティ」、「違法有害コンテンツ」、「プライバシー」に関する不安感があることから情報通信利用への国民への理解を高め、利用促進していくためにはこうした国民の不安を解消していく取組が、業界、行政にとって重要な課題であることはいうまでもない。

そのため、事業者は、情報資産が存在する環境には必ず何らかの弱点、想定外のリスクがあることを認識し、情報資産を守るための技術的保護措置を講じる努力を継続して進めていくとともに、想定外のリスクが発生した場合には、迅速な対応を行うことが重要である。

総務省は、電気通信事業分野における個人情報漏えい等の事故状況を分析、評価し、二次被害の防止、類似事案防止の観点から、国民、事業者への情報提供を行うことが求められる。

（３）なお、時間を経るごとに技術の安全性が変化することや、より安全性の高い技術が登場することも考えられるため、適切な技術的保護措置については、必要に応じて見直しを実施することが必要である。

（４）適切な技術的保護措置が講じられていたときの手続の簡略化の検討結果については、電気通信分野以外の分野でも同様であると思われることから、この提言が他分野における安全管理措置の在り方の検討に際し、参考とされることを期待する。

「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」開催要綱

１　目的

新たなサービスの登場や新技術を活用した情報の流通などにより、通信の秘密、個人情報保護、知的財産保護などの観点から、新たな課題が生じたり、深刻化したりといった状況がある。また、諸権利との関係が不分明なために、新規サービスの展開が円滑に進まないといった課題も生じている。

こうした課題について、利用者視点を踏まえながら、関係者間で、速やかに具体的な対応策を検討して実施するとともに、通信の秘密等との関係についても必要に応じて整理することを目的として、本研究会を開催する。

２　名称

本会は、「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」と称する。

３　検討事項

⑴ ＩＣＴサービスを展開するに際しての通信の秘密等についての考え方の整理
⑵ 個別課題の対応策の検討
⑶ その他利用者視点を踏まえたＩＣＴサービスに係る諸問題に対する対応策の検討

４　構成及び運営

⑴ 本会は、総務省総合通信基盤局長の研究会として開催する。
⑵ 本会の構成員は、別紙のとおりとする。
⑶ 本会には、座長及び座長代理を置く。
⑷ 座長は、研究会構成員の互選により定めることとし、座長代理は座長が指名する。
⑸ 座長は本会を招集し、主宰する。また、座長代理は、座長を補佐し、座長不在のときは、座長に代わって本会を招集し、主宰する。
⑹ 本会は、必要があるときは、外部の関係者の出席を求め、意見を聞くことができる。
⑺ 座長は、必要に応じて、ワーキンググループを開催することができる。
⑻ ワーキンググループの構成員及び運営に必要な事項については、座長が定めるところによる。
⑼ その他、本会の運営に必要な事項は、座長が定めるところによる。

５　開催期間

本会の開催期間は、平成 21 年４月から平成 22 年３月までを目処とする。

６　庶務

本会の庶務は、総務省総合通信基盤局電気通信事業部消費者行政課がこれを行うものとする。

「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」構成員

（敬称略・五十音順）

【構成員】

相田　仁	東京大学大学院新領域創成科学研究科教授
岡村　久道	英知法律事務所弁護士
木村　たま代	主婦連合会
清原　慶子	三鷹市長
桑子　博行	社団法人テレコムサービス協会サービス倫理委員長
國領　二郎	慶應義塾大学総合政策学部教授
長田　三紀	特定非営利活動法人東京都地域婦人団体連盟事務局次長
野原　佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
藤原　まり子	博報堂生活総合研究所客員研究員
別所　直哉	安心ネットづくり促進協議会調査企画委員会副委員長
堀部　政男	一橋大学名誉教授
松本　恒雄	一橋大学大学院法学研究科教授

【オブザーバ】

消費者庁企画課個人情報保護推進室長

ＣＧＭ検討ＷＧ　構成員

（敬称略　平成 22 年４月１日現在）

顧問	親会（利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会）構成員	
主査	宍戸　常寿	東京大学大学院法学政治学研究科　准教授
主査代理	曽我部　真裕	京都大学大学院法学研究科　准教授
	新保　史生	慶應義塾大学総合政策学部　准教授
構成員	森　亮二	弁護士　（英知法律事務所）
	青柳　直樹	グリー株式会社　取締役　執行役員 CFO
	小泉　文明	株式会社ミクシィ　取締役　経営管理本部長
	上林　靖史	株式会社ディー・エヌ・エー　執行役員 経営企画本部長
	関　聡司	楽天株式会社　執行役員　広報渉外室室長
	西野　茂生	ソフトバンクモバイル株式会社　渉外本部渉外部　部長 （社団法人電気通信事業者協会　青少年有害情報対策部会長）
	丸橋　透	ニフティ株式会社　法務部長 （社団法人テレコムサービス協会　サービス倫理委員会副委員長）
	高橋　誠	株式会社ライブドア　カスタマーサポートセンター長
	小田　志門	イーガーディアン株式会社　取締役　営業部長
	岸原　孝昌	一般社団法人モバイルコンテンツ審査・運用監視機構　事務局
	吉川　誠司	WEB110 代表

オブザーバ　内閣官房 IT 担当室
内閣府青少年インターネット環境整備推進室
警察庁生活安全局情報技術犯罪対策課
経済産業省商務情報政策局情報経済課

ライフログ活用サービスＷＧ　構成員

（敬称略　平成 22 年３月 31 日現在）

主査	上沼　紫野	虎ノ門南法律事務所　弁護士
主査代理	森　亮二	英知法律事務所　弁護士
構成員	石井　夏生利	情報セキュリティ大学院大学　准教授
	新保　史生	慶應義塾大学　准教授
	長田　三紀	東京都地域婦人団体連盟　事務局次長
	藤原　まり子	博報堂生活総合研究所　客員研究員
オブザーバ	楠　正憲	マイクロソフト株式会社　技術標準部　部長
	桑子　博行	社団法人テレコムサービス協会　サービス倫理委員長
	下島　健彦	ＮＥＣビッグローブ株式会社　執行役員 ポータル事業部長
	正垣　学	株式会社ＮＴＴドコモ　コンシューマサービス企画 コミュニケーションサービス企画担当課長
	寺田　眞治	株式会社オプト　海外事業本部　本部長
	中井　博胤	株式会社ぐるなび　総合政策室　次長
	別所　直哉	ヤフー株式会社　ＣＣＯ兼法務本部長

安全管理措置ＷＧ　構成員

（敬称略　平成 22 年３月 31 日現在）

主査	田島　正広	田島総合法律事務所所長　弁護士
主査代理	石井　夏生利	情報セキュリティ大学院大学　准教授
構成員	井上　大介	独立行政法人情報通信研究機構　情報通信セキュリティ研究センターインシデント対策グループ　主任研究員
	尾形　わかは	東京工業大学大学院イノベーションマネジメント研究科　准教授
	花木　親司	社団法人電気通信事業者協会　消費者支援委員長
	丸橋　　透	社団法人テレコムサービス協会サービス倫理委員会副委員長
オブザーバ	阿部　美雪	社団法人全国消費生活相談員協会　関東支部理事
	坂巻　健士	富士通株式会社パーソナルビジネス本部ソリューション開発統括部　統括部長代理
	三輪　真久	消費者庁企画課個人情報保護推進室　課長補佐
	山岡　正輝	株式会社 NTT データビジネスソリューション事業本部情報セキュリティ推進室長