第3節　国民の暮らしを守る安心・安全

1　電気通信サービスに関する消費者行政

（1）利用者視点を踏まえたICTサービスに係る諸問題への対応

ICT関連の新たなサービスの登場や新技術を活用した情報の流通等により、知的財産権をはじめとする諸権利との関係を整理する必要が生じてきたことから、総務省では、平成21年4月から「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[1]」を開催している。同研究会において、平成22年9月から「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（平成13年法律第137号。以下「プロバイダ責任制限法」という。）の検証、迷惑メールへの対応の在り方、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及び電気通信サービス利用者の利益の確保・向上について、各WGを開催の上検討を行い、平成23年度中に各課題に対する提言を取りまとめ、公表した（図表5-3-1-1）。

図表5-3-1-1　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の概要

➢　近年のインターネット・携帯電話の発展普及に伴う諸課題について、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するため平成21年4月から開催。

Ⅰ　プロバイダ責任制限法検証WG

✓プロバイダ責任制限法（ネット上の権利侵害情報へのプロバイダの対応の在り方を規定）に関し、その運用状況や諸外国動向を踏まえ、同法改正の必要性等を検討し、平成23年7月に提言を取りまとめ。

Ⅱ　迷惑メールへの対応の在り方に関する検討WG

✓平成20年12月の改正特定電子メール法附則の施行3年後の見直し規定を受け、今後の迷惑メール対策として必要な措置を検討し、平成23年7月に提言を取りまとめ。

Ⅲ　青少年インターネットWG

✓携帯電話のフィルタリングの更なる普及等を図るため、スマートフォン等の新たな端末の登場に伴う課題等を検討し、平成23年10月に提言を取りまとめ。

Ⅳ　電気通信サービス利用者WG

✓電気通信サービス利用者保護に関する関係者の取組状況や効果を検証し、利用者に対する契約締結前の情報提供の在り方、契約締結時の説明の在り方、契約締結後の対応の在り方について検討し、平成23年12月に提言を取りまとめ。

（2）スマートフォン時代の安全・安心な利用環境整備

総務省では、「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」で取りまとめた「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に関する提言～スマートフォン時代の青少年保護を目指して～」を受け、スマートフォンの青少年への普及を踏まえ、リテラシーの向上とフィルタリングの改善に官民連携で取り組むとともに、実効的な青少年保護を組み込んだ形で、機器の設計、サービスの設計、事業者内部及び事業者間の体制の整備等を行うことを示す概念として、「青少年保護・バイ・デザイン」を提唱している。

また、平成24年1月からは同研究会に開催した「スマートフォンを経由した利用者情報の取扱いに関するWG」において、スマートフォンにおける利用者情報が安全・安心な形で活用され、利便性の高いサービス提供につながるよう、諸外国の動向を含む現状と課題を把握し、利用者情報の取扱いに関する必要な対応等の検討を行っている。同年4月には、中間取りまとめ[2]を公表し、①スマートフォンを巡るサービス構造、②利用者情報の取扱いに関する現状、③今後の論点について整理を行った。また、併せて、スマートフォンの利用に際し、利用者自身で少なくとも注意すべき事項について整理された「スマートフォン プライバシー ガイド」を作成した（第2章第2節2（2）囲み記事参照）。

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：http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html
2「スマートフォンを経由した利用者情報の取扱いに関するWG中間取りまとめ」：http://www.soumu.go.jp/main_content/000154856.pdf

スマートフォン プライバシー ガイド

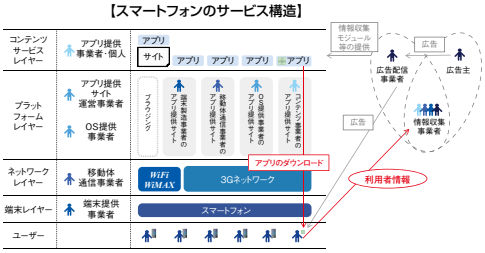
スマートフォンが急速に普及する中、スマートフォン上の利用者情報が様々なサービス提供等に利用されています。利用者情報の取扱いは、関係する事業者において適正に行われるべきものですが、スマートフォンの利用には自己責任が求められる側面もあります。

「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・スマートフォンを経由した利用者情報の取り扱いに関するWG」においては、事業者における利用者情報の適正な取扱い方策について検討してまいりますが、現時点でもスマートフォンを利用者が一定程度安心して利用できるよう、利用者自身で少なくとも注意すべき事項について、「スマートフォン プライバシー ガイド」として、中間取りまとめに際して整理しました。

1　スマートフォンのサービス構造を知りましょう

- スマートフォンは携帯電話事業者のみによるサービスではありません。アプリケーション（アプリ）提供者やアプリ提供サイトの運用者など多くの事業者が、それぞれ役割を持ちサービスを提供しています。
- スマートフォンでは、インターネットを経由して多様なアプリを自ら選択してダウンロードの上利用することができます。その一方、利用者の自己責任が求められる側面もあります。
- 無料のアプリ等の中には、広告主からの広告収入等によって収益を得ることによりアプリの提供を実現しているものもあります。このような場合、アプリに組み込まれた「情報収集モジュール」と呼ばれるプログラムなどを通じ、利用者情報が情報収集事業者や広告配信事業者等へ送信される場合もあります。

【スマートフォンのサービス構造】



【スマートフォンにおける主な利用者情報】

2　アプリの信頼性に関する情報を自ら入手し理解するように努めましょう

- スマートフォンには、電話番号、メールアドレスなど連絡先の情報、通信履歴、ウェブページの閲覧履歴、アプリの利用履歴、位置情報、写真や動画など様々な利用者情報が蓄積されます。アプリをインストールすると、これらの情報は、アプリを通じたサービス提供に活用されるほか、広告配信事業者等へ送信され、利用者の趣味・趣向に応じた広告の表示等に利用される場合もあります。
- このように利用者情報が収集・送信されて利用されることについてプライバシー上の不安がある場合、利用者も受け身ではなく、アプリの機能や評判、提供者など、アプリの信頼性に関する情報を自ら入手し、理解に努めるようにしましょう。
- その場合、評価サイトの評価や利用者のコメント等を参考にすることもできますが、それでも不安な場合には利用を避けることも大切です。
- 携帯電話事業者及び端末ベンダーなどが安全性を確認しているアプリ提供サイトなども必要に応じて活用しましょう。

【利用者情報の利用許諾画面の例】
<iPhoneで位置情報を利用する場合>

（※App storeから入手したアプリをもとに総務省作成）

3　利用者情報の許諾画面等を確認しましょう

- アプリの信頼性を確認するためには、利用者情報がどのような目的で収集されているか、必要以上の利用者情報が収集されていないかなどもヒントになります。
- アプリをダウンロードする時や利用（起動）する時などに、収集される利用者情報に関する利用許諾を求める画面が表示される場合があります。また、アプリの利用規約やプライバシーポリシーが定められ公表されている場合もあります。
- 利用許諾画面や利用規約等において、収集される利用者情報の範囲などをよく確認し、内容を理解した上で、同意・利用するよう努めましょう。
- なお、利用許諾画面等が表示されない場合には、上記２の様々な方法によりアプリの信頼性の確認に努めましょう。

<Android OS搭載スマートフォンでアプリをダウンロードする場合>

（※Google Playから入手したアプリをもとに総務省作成）

（3）インターネット上の違法・有害情報への対策

総務省では、平成23年7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」で取りまとめた「プロバイダ責任制限法検証に関する提言」を踏まえ、開示の対象となる発信者情報に携帯電話端末等の個体識別番号を新たに追加するため、同年9月に「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第四条第一項の発信者情報を定める省令」（平成14年総務省令第57号）を改正した。

（4）情報通信分野における個人情報の保護

総務省では、電気通信事業における個人情報保護について、電気通信サービスの利便性の向上を図るとともに、利用者の権利利益を保護することを目的として、「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」及び解説を策定している。平成23年11月に、電気通信事業者が取得する位置情報に関する関係省庁の協議結果を受けて、関係規定を整備するために同ガイドライン及び解説を改正した[3]。

2　情報セキュリティ対策の推進

（1）インターネットの安心・安全な利用環境の実現

総務省では、重要インフラの一つである情報通信分野の主管官庁という立場から、国民が安心して情報通信ネットワークを利用できる環境を整備するため、次のような取組を実施している。

ア　スマートフォンに関する情報セキュリティ対策

総務省では、平成23年10月から、スマートフォンやスマートフォンを通じたクラウドサービスの利用にあたっての情報セキュリティ上の課題を抽出するとともに、安全・安心な利用環境の構築のために講ずべき対策について検討すること等を目的として、「スマートフォン・クラウドセキュリティ研究会[4]」を開催してきた。同研究会においては、平成23年12月に、スマートフォンの情報セキュリティを確保するための事業者における当面の対策や、利用者に最低限守っていただきたい事項を記載した「スマートフォン情報セキュリティ3か条」（図表5-3-2-1）を含む中間報告を取りまとめ、利用者への普及啓発の取組等を推進してきた。平成24年6月には、中間報告の内容に加え、事業者・政府における中長期的対策を提示する最終報告を取りまとめ、公表した。今後、事業者等の取組について、利用者への啓発活動を含め、半年に一度程度のフォローアップを行っていくこととしている（第2章第2節2（2）囲み記事参照）。

図表5-3-2-1　スマートフォン情報セキュリティ3か条

スマートフォン情報セキュリティ3か条（利用者が最低限取るべき情報セキュリティ対策）

スマートフォンは、アプリケーションを活用することで、様々な機能を自由に追加できる便利な携帯電話です。しかし自由さの反面、その中には危険なアプリケーションが混じっている場合もあります。利用者自身で情報セキュリティ対策を取ることが必要です。

盗難・紛失対策や他人による不正利用防止対策など、従来の携帯電話と同様の対策が必要です。さらにスマートフォンにおいては、次の3つの対策が大切です。

1.OS（基本ソフト）を更新

スマートフォンは、OSの更新（アップデート）が必要です。古いOSを使っていると、ウイルス感染の危険性が高くなります。更新の通知が来たら、インストールしましょう。

2.ウイルス対策ソフトの利用を確認

ウイルスの混入したアプリケーションが発見されています。スマートフォンでは、携帯電話会社などによってモデルに応じたウイルス対策ソフトが提供されています。ウイルス対策ソフトの利用については、携帯電話会社などに確認しましょう。

3.アプリケーションの入手に注意

アプリケーションの事前審査を十分に行っていないアプリケーション提供サイト（アプリケーションの入手元）では、ウイルスの混入したアプリケーションが発見される例があります。OS提供事業者や携帯電話会社などが安全性の審査を行っているアプリケーション提供サイトを利用するようにしましょう。インストールの際にはアプリケーションの機能や利用条件に注意しましょう。

3 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及び解説：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html
4 スマートフォン・クラウドセキュリティ研究会：http://www.soumu.go.jp/main_sosiki/kenkyu/smartphone_cloud/index.html

（2）電子データの安全な利活用の推進

ア　暗号技術の安全性評価と高度化の推進

総務省では、電子政府等の安全性及び信頼性の確保を目的として、経済産業省と共同で暗号評価プロジェクトCRYPTREC（Cryptography Research and Evaluation Committee）[5]を実施し、「電子政府推奨暗号リスト」（平成15年2月策定）[6]の公表、暗号の安全性の評価・監視等を実施している。CRYPTRECは、総務省及び経済産業省が共同で運営する「暗号技術検討会」と、その下部委員会であり、独立行政法人情報通信研究機構及び独立行政法人情報処理推進機構が共同で運営する「暗号方式委員会」、「暗号実装委員会」、「暗号運営委員会」から構成されている。

現在、近年の技術の進展により「電子政府推奨暗号リスト」掲載暗号の危殆化が懸念されていることから、平成24年度末までに当該リストを改訂すべく、CRYPTRECにおいて、安全性、実装性、運用性等の様々な観点から掲載候補の暗号の評価を実施している。

イ　電子署名・認証業務の普及促進

電子商取引等のネットワークを介した社会経済活動を安全に行うため、「電子署名及び認証業務に関する法律」（平成12年法律第102号）では、安全性の高い電子署名について行われる認証業務を「特定認証業務」と定義し、電子署名の真正性を担保している。平成24年4月末現在、16件の特定認証業務が認定を受けており、電子署名・認証業務の普及促進を図っている。

ウ　タイムビジネスの利用促進

電子商取引等の分野において、流通・保存される電子データの作成時期等に関する信頼性を高めるために、電子データに付されるタイムスタンプ及びそのサービスであるタイムビジネス（時刻配信業務と時刻認証業務の総称）の重要性が高まっている。

一般財団法人日本データ通信協会では、一定の基準を満たすタイムビジネスに対し認定を行うことで、国民に対し信頼性の目安を提供する「タイムビジネス信頼・安心認定制度」を運営し、平成24年3月末現在、3件の時刻配信業務及び6件の時刻認証業務を認定している。また、民間事業者やベンダー等で構成される「タイムビジネス協議会[7]」は、タイムビジネスの普及促進を目的として、セミナーやシンポジウム活動を行っている[8]。

また、平成22年4月に時刻のトレーサビリティの保証に関するITU-R（International Telecommunication Union Radiocommunication Sector）勧告の改訂案（日本提案）がSG7（Study Group 7）において承認されたことを受け、時刻配信・監査の在り方の明確化やタイムスタンプに使用される暗号アルゴリズムの脆弱化に対応するため、平成23年11月に当該認定制度の技術基準を改定し、平成24年10月より適用予定である。

3　消防防災分野における情報化の推進

（1）災害に強い消防防災通信ネットワークの整備

被害状況等に係る情報の収集及び伝達を行うためには、通信ネットワークが必要である。災害時においても通信を確実に確保するように、国、都道府県、市町村等においては、公衆網を使用するほか、災害に強い自営網である消防防災通信ネットワーク、非常用電源等の整備を行っている。

現在、国、消防庁、地方公共団体、住民等を結ぶ消防防災通信ネットワークを構成する主要な通信網として、①政府内の情報収集・伝達を行う中央防災無線網、②消防庁と都道府県を結ぶ消防防災無線、③都道府県と市町村等を結ぶ都道府県防災行政無線、④市町村と住民等を結ぶ市町村防災行政無線並びに⑤国と地方公共団体及び地方公共団体間を結ぶ衛星通信ネットワーク等が構築されている。

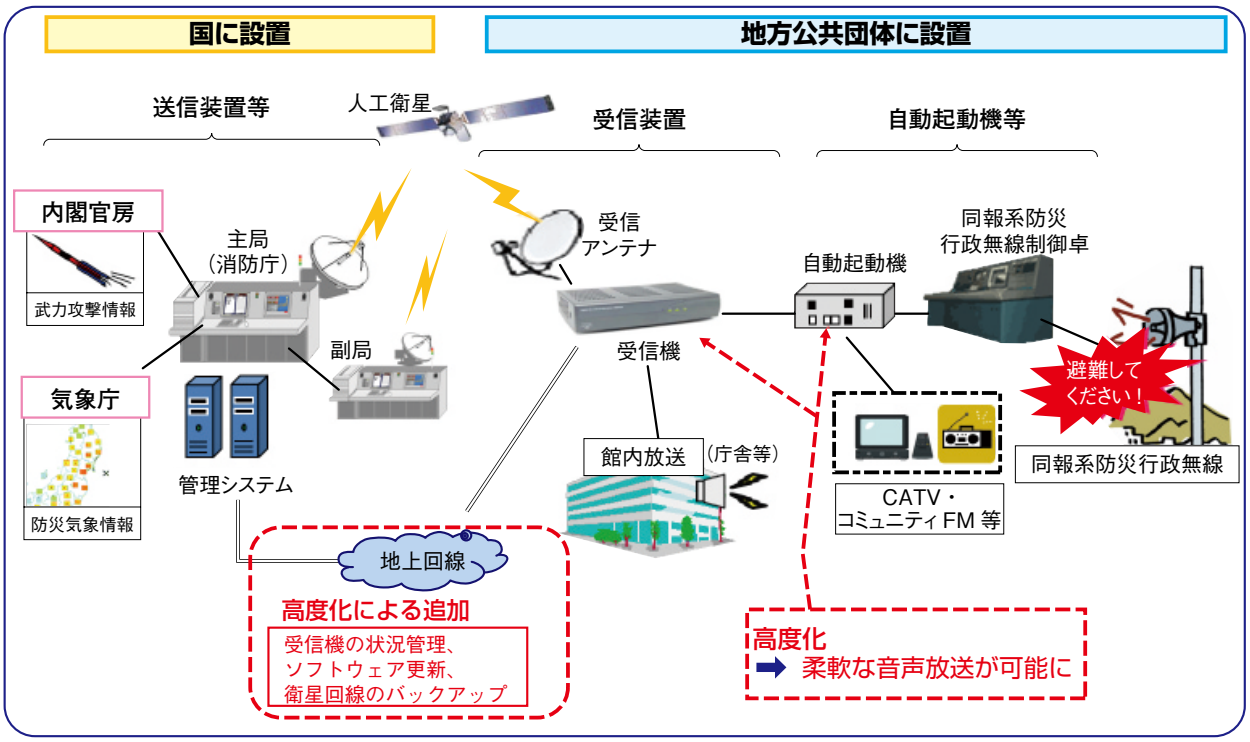
5 CRYPTREC：http://www.cryptrec.go.jp/index.html
6 電子政府推奨暗号リスト：http://www.cryptrec.go.jp/images/cryptrec_01.pdf
7 タイムビジネス信頼・安心認定制度：http://www.dekyo.or.jp/tb/summary/data/unyoukiyaku.pdf
8 タイムビジネス協議会：http://www.dekyo.or.jp/tbf/guide/greeting.html

（2）全国瞬時警報システム（J-ALERT）の整備

総務省では、津波警報、緊急地震速報、弾道ミサイル発射情報等といった、対処に時間的余裕のない事態に関する緊急情報を、国（内閣官房・気象庁から消防庁を経由）から人工衛星を用いて送信し、市町村防災行政無線（同報系）等を自動起動することにより、住民に緊急情報を瞬時に伝達する「全国瞬時警報システム（J-ALERT）」の整備を行っている。

また、平成 22 年 12 月からは、状況に応じた内容の音声放送や、オンラインでのソフトウェア更新、システムの稼働状況の管理等を可能とするシステムの高度化を行ったところである（図表 5-3-3-1）。

図表 5-3-3-1　J-ALERT 概要



（3）情報化の今後の展開

総務省では、ICT を積極的に活用し、①消防救急無線等のデジタル化、②市町村防災行政無線の整備促進、③住民への情報伝達手段の多様化、④ヘリコプターテレビ電送システム等に重点をおいて消防防災通信ネットワークの充実強化を推進することにより、地方公共団体と一体となって国民の安全・安心をより一層確かなものとすることとしている。