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 サービスの推進

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」を開催している1。同研究会は、平成21年8月に第一次提言を、平成22年5月には第二次提言をそれぞれ取りまとめ、公表した。

また、同研究会においては、平成22年9月より、

「青少年インターネット WG」、「プロバイダ責任制限法検証 WG」、「電気通信サービス利用者 WG」、「迷惑メールへの対応の在り方に関する検討 WG」の4WGを新たに開催し、①青少年インターネット利用環境の整備、②プロバイダ責任制限法の検証、③更なる利用者の権利確保のための取組の在り方、④迷惑メール対策のそれぞれの第二次提言策定後の課題に対する検討を行っている。

(2) 電気通信サービスにおける消費者保護の推進

総務省は、消費者が安心して電気通信サービスを利用できるようにすることを目的として、平成16年3月に「電気通信事業法の消費者保護ルールに関するガイドライン」を策定し、平成16年4月の電気通信事業法施行に併せて運用している。

また、平成21年2月に公表された「電気通信サービス利用者懇談会報告書」において、電気通信サービスの契約締結時における説明事項として、契約変更、解約時の連絡先、連絡方法を追加することや、利用者の特性に配慮した勧誘を行うという適合性の原則の推奨等を同ガイドラインに盛り込むこと等が提言され

た。この提言を受け、平成 21 年 7 月に、電気通信事業法施行規則の一部を改正するとともに、同ガイドラインを改正した 2 。

平成 22 年9月には、これらの取組状況や効果を検証するとともに、電気通信サービスが更に高度化、多様化している状況を踏まえ、「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」の下に「電気通信サービス利用者 WG」が設置され、今後対応すべき新たな問題等を確認し、更なる利用者の権利保障のための取組の在り方について検討されている。。

(3) インターネット上の違法・有害情報への対策

我が国におけるインターネットの普及はめざましく、国民の社会・文化・経済活動等あらゆる活動の基盤(社会インフラ)として利用され、国民生活に必要不可欠な存在となっている。一方で、急速なインターネットの普及は、違法・有害情報の流通等、負の側面

も拡大させている。

総務省では、これらの問題に対処することとして、これまで、以下の取組を実施し、引き続き今後も推進していくこととしている(図表 5-3-1-1)。

2 参考:「電気通信事業法の消費者保護ルールに関するガイドライン」(改正):http://www.soumu.go.jp/menu_news/s-news/16063.html

3 参考:「電気通信サービス利用者 WG」:http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html

図表 5-3-1-1 インターネット上の違法・有害情報に関する総務省の取組

No.	項目	開催日等	概要
1	「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」 (通称:プロバイダ責任制限法)	平成14年5月施行	①他人の権利が侵害された場合におけるプロバイダ等の損害賠償 責任の制限・明確化。 ②権利侵害を受けた者のプロバイダにおける発信者情報の開示請 求権を規定。
2	「インターネット上の違法・有害情報への対応に関する研究会」	平成17年8月~18年8月	違法・有害情報に対する民間事業者の自主的対応を中心とした具体 的施策について提言。
3	「インターネット上の違法・有害情報への対応に関する検討会」	平成19年11月~21年1月	青少年に向けたフィルタリングの更なる導入促進、プロバイダ等による削除等措置の支援、インターネットリテラシーの普及啓発等の違法・有害情報に対する総合的な対応について検討。
4	「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」 (通称:青少年インターネット環境整備法)	平成20年6月成立 (平成21年4月1日施行)	①青少年自身がインターネットを適切に活用する能力を習得すること ②青少年による有害情報の閲覧の機会を少なくすること ③民間による自主的・主体的取組を尊重すること を基本理念とする。 具体的な有害情報対策として、フィルタリングの普及とその性能向上 に取り組むことを求める。
5	安心ネットづくり促進プログラム	平成21年1月	総務省における、今後のインターネット上の違法・有害情報対策の包括的政策パッケージ ①安心を実現する基本的枠組の整備 ②民間における自主的取組の促進 ③利用者を育てる取組の推進 を3つの柱とする。
6	青少年のインターネット利用におけるフィルタリングの普及促進 及び適切な利用のための啓発活動の都道府県等への依頼	平成21年2月	総務省、内閣府、内閣官房IT室、警察庁、文部科学省及び経済産業省が連名で、各都道府県、教育委員会、都道府県警察、PTA等に対し、青少年のインターネット利用におけるフィルタリングの普及促進及び適切な利用を促進するため、学校関係者や保護者をはじめ住民に対する存発活動に取り組むよう依頼。
7	フィルタリング普及キャンペーン	平成21年3月	総務省、内閣府、内閣官房、警察庁、文部科学省及び経済産業省が連名で、パーソナルコンピュータの製造事業者、携帯電話・PHS事業者、フィルタリングソフトメーカー、家電販売店等と連携して、フィルタリング普及のためのキャンペーンを実施。
8	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	平成21年4月	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 性が生じてきたため、開催。
9	安心・安全なインターネット環境整備に関する戦略対話	平成21年6月	総務省とITU(国際電気通信連合)の共催で、インターネット上の違法・有害情報への適切な対応について、国際連携を推進するとともに、世界における安心・安全なインターネット環境整備を促進するため、平成21年6月2日及び3日に、東京において明騰。本戦略対話では、安心を実現する基本的枠組の整備等についての議論が行われ、成果物として議長報告及び「東京声明」が取りまとめられた。
10	違法・有害情報相談センターの開設	平成21年8月	中小のプロバイダ、サイト管理者、学校関係者等を対象に、インターネット上の違法・有害情報や、いじめ等への適切な対応について助言する違法・有害情報相談センターの開設を支援。
11	「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」配下に新規4WGを設置	平成22年9月~	青少年インターネットWG、プロバイダ責任制限法検証WG、電気通信サービス利用者WG、迷惑メールへの対応の在り方に関する検討WGを設置し、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第二次提言策定後に設定されたそれぞれの課題について検討。

(4) 迷惑メール対策

迷惑メールについては、これまで「特定電子メールの送信の適正化等に関する法律」に基づく法執行や、電気通信事業者による自主的な取組、利用者への周知啓発、国際連携の推進等、総合的な対策を行ってきた(図表 5-3-1-2)。

また、平成22年9月には、特定電子メール法の平成20年改正(平成20年12月1日施行)附則において、施行3年後の見直し規定が盛り込まれていることを踏まえ、特定電子メール法の施行の状況等を検証し、今後の迷惑メール対策として必要な措置の検討を行うため、「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」の下に「迷惑メールへの対応の在り方に関する検討 WG」が設置された 4。同WGでは、日本における迷惑メールの現状、迷惑メール対策関係者からのヒアリング、諸外国の状況等を踏まえ、幅広い観点から検討を行っている。

さらに、平成23年4月から、特定電子メール法違 反者への措置等に活用するため、迷惑メールを受信さ れた方から、迷惑メールに関する情報提供をしていた だくこととして、迷惑メール情報提供用プラグインソ フトを開発し、専用ウェブサイトで配布している5。

5 参考:迷惑メール情報提供用プラグインソフトの配布: http://www.soumu.go.jp/menu_news/s-news/01kiban08_01000022.html

図表 5-3-1-2 迷惑メール対策に関する総務省の取組

No.	項目	開催日等	概要
1	「迷惑メールへの対応のあり 方に関する研究会」(第1次)	平成13年11月~ 平成14年1月	・平成13年春頃から、携帯電話での利用を中心に、受信者の同意を得ずに、一方的、大量に送信される受信者が望まない広告宣伝目的のメールが、迷惑メールとして社会問題となったことから対応を検討。
2	「特定電子メールの送信の 適正化等に関する法律」	平成14年4月成立 (同年7月1日施行)	・営利目的の団体・営業を営む個人が広告宣伝の手段として、個人が私的に利用しているメールアドレス宛に送信する電子メールを特定電子メールとし、受信拒否の通知をした者に対する特定電子メールの送信の禁止(オプトアウト方式による規制)、架空電子メールアドレス宛の広告宣伝メールの送信の禁止等が定められた。
3	「迷惑メールへの対応のあり 方に関する研究会」(第2次)	平成16年10月~ 平成17年7月	・特定電子メール法の附則における施行3年後の見直し規定に基づき、特定電子メール法の施行の状況を踏まえ、今後の迷惑メール対策として必要な措置を検討。
4	「迷惑メール追放支援プロジェクト」の実施	平成17年2月	・総務省が設置したモニター機で受信した迷惑メールの違法性を確認し、当該メールに関する 情報を送信元プロバイダに通知することにより、迷惑メール送信回線の利用停止措置等の円 滑な実施を促す取組。
5	「特定電子メールの送信の 適正化等に関する法律の一 部を改正する法律」	平成17年5月成立 (同年12月1日施行)	・「迷惑メールへの対応のあり方に関する研究会」(第2次)の提言を踏まえ、特定電子メールの 範囲への企業や事業を営む個人が利用している事業用メールアドレス宛の広告宣伝メール の追加、送信者情報の偽装の禁止、罰則の強化等が行われた。
6	迷惑メールに関する共同声 明·共同宣言の締結	平成18年5月(フランス) 平成18年9月(英国) 平成18年10月(カナダ) 平成19年7月(ドイツ)	・迷惑メール対策について、連携して対応するため、共同声明・共同宣言を締結。
7	「迷惑メールへの対応のあり 方に関する研究会」(第3次)	平成19年7月~ 平成20年8月	・特定電子メール法の附則における施行3年後の見直し規定に基づき、特定電子メール法の施行の状況を踏まえ、今後の迷惑メール対策として必要な措置を検討。
8	「特定電子メールの送信の 適正化等に関する法律の一 部を改正する法律」	平成20年6月成立 (同年12月1日施行)	・「迷惑メールへの対応のあり方に関する研究会」(第3次)中間とりまとめの提言を踏まえ、あらかじめ同意した者以外の者への特定電子メールの送信を原則禁止するオプトイン方式による規制の導入、措置命令等の対象の送信委託者への拡大、特定電子メール法に相当する外国の法令を執行する外国当局に対する送信者の特定に資する情報の提供に関する規定の追加、罰則の強化等が行われた。
9	「特定電子メールの送信等に 関するガイドライン」公表	平成20年11月	・「迷惑メールへの対応のあり方に関する研究会」(第3次)提言を踏まえ、改正特定電子メール 法及び関係省令の解釈、特定電子メールの送信に当たって推奨される事項等を取りまとめ。
10	「消費者庁及び消費者委員会設置法」 「消費者庁及び消費者委員会設置法の施行に伴う関係 法律の整備に関する法律」	平成21年6月成立 (同年9月1日施行)	・消費者庁及び消費者委員会の設立。 ・消費者庁等の設立による、特定電子メール法に関する整備法による所要の改正の実施。
11	「迷惑メールへの対応のあり 方に関する検討WG」(第4 次)	平成22年9月~ 平成23年5月	・特定電子メール法の附則における施行3年後の見直し規定に基づき、特定電子メール法の施行の状況を踏まえ、今後の迷惑メール対策として必要な措置を検討。

(5) 情報通信分野における個人情報の保護

ア 「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」の策定・改定

電気通信事業における個人情報保護については、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、平成16年8月に策定し、運用している。

総務省は、平成22年5月に公表された「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」の第二次提言を踏まえ、平成22年7月、ガイドライン及び解説について、以下のとおり改定した6。

(ア) 利用目的の特定について (ガイドライン第5条 の解説)

第5条の解説に、特定の個人を識別できないよう にする加工(いわゆる匿名化)を行うことは、個人情 報の利用に当たらず、利用目的として特定する必要は ないことを明記する。

(イ) モバイル PC 等による個人情報の持出時に求められる安全管理措置(ガイドライン第 11 条の解説)

第11条の解説に、モバイルPC等による個人情報の持出時の漏えいリスクに対する安全管理措置の在り方及び個人情報の持出時の留意点について明記する。

(ウ) 個人情報の漏えい等発生時の手続の緩和(ガイドライン第22条及び同条の解説)

モバイル PC 等の紛失等に際して、漏えい等が発生した個人情報に対し適切な技術的保護措置が講じられていた場合には、事業者に求められる手続(本人への通知、事実の公表及び監督官庁への報告)の一部を緩和することを明記する。

⁶ 参考:「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」の改定 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html

イ 「放送受信者等の個人情報の保護に関する指針」 の策定・改定

総務省は、平成17年4月の個人情報保護法の全面施行に当たり、「放送分野における個人情報保護及びIT時代の衛星放送に関する検討会」(平成16年5月から17年2月まで開催)で取りまとめられた「放送分野における個人情報保護の基本的な在り方について」(平成16年8月)を踏まえ、平成16年8月に、「放送受信者等の個人情報の保護に関する指針」(平成16年総務省告示第696号)を策定した(平成17年

4月施行)。

同指針については、平成 19年7月に施行後の実態を踏まえた見直しを行ったほか、平成 21年9月に、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)の一部変更等を踏まえ、受信者情報取扱事業者が策定する基本方針(プライバシーポリシー等)において定めるよう努めるべき事項(個人情報の取得元等の明記、委託処理の透明化等)の追加や、漏えい等があった場合の認定個人情報保護団体への報告の努力義務について新たに規定する等の改正を行った7。

2 情報セキュリティ対策の推進

(1) 政府の情報セキュリティ対策

[国民を守る情報セキュリティ戦略]

近年、情報通信基盤の急速なブロードバンド化や電子商取引の浸透に伴い、世界規模でのコンピュータウイルスのまん延、サイバー犯罪の増加、国民生活・社会経済活動の基盤となる重要インフラにおける情報システムの障害、大量の個人情報の漏えい等が社会問題化し、情報セキュリティ対策の強化が重要な課題となっている。

我が国の情報セキュリティ問題への取組としては、 平成 17 年 4 月に内閣官房に「情報セキュリティセンター(NISC:National Information Security Center)」が、平成 17 年 5 月に高度情報通信ネットワーク社会推進戦略本部(IT 戦略本部)に「情報セキュリティ政策会議」が設置され、強化された。

情報セキュリティ政策会議において、平成18年度 から20年度までは、「セキュア・ジャパン」の実現 を目指した「第1次情報セキュリティ基本計画」(平成18年2月)により、平成21年度からは、同計画を継続・発展させることとした「第2次情報セキュリティ基本計画」(平成21年2月)に基づき、官民の各主体によって取組を推進するなど、これまで以下の取組を実施している(図表5-3-2-1)。

また、平成 22 年 5 月には、同政策会議において、多様化・高度化・複雑化している情報セキュリティをめぐる環境の変化に的確に対応するために、「国民を守る情報セキュリティ戦略」を策定したところである。同戦略は、平成 22 年~ 25 年の 4 年間について、「第2次情報セキュリティ基本計画」に規定された施策に加え、年度計画である「セキュア・ジャパン 2010」改め「情報セキュリティ 2010」(平成 22 年 7 月)8に基づいた全 196 の具体的な取組施策を推進するものである(図表 5-3-2-2)。

図表 5-3-2-1 我が国の情報セキュリティ対策の歩み

年月日	項目等
平成17年4月	「内閣官房情報セキュリティセンター(NISC)」設置
平成17年5月	IT戦略本部に「情報セキュリティセンター」設置
平成18年2月	「第1次情報セキュリティ基本計画」
平成18年6月	「セキュア・ジャパン2006」
平成19年6月	「セキュア・ジャパン2007」
平成20年6月	「セキュア・ジャパン2008」
平成21年2月	「第2次セキュリティ基本計画」
平成21年6月	「セキュア・ジャパン2009」
平成22年1月	「情報セキュリティ月間」の新設
平成22年5月	「国民を守る情報セキュリティ戦略」
平成22年7月	「情報セキュリティ2010」

7 参考:「放送受信者等の個人情報の保護に関する指針」(改定): http://www.soumu.go.jp/menu_news/s-news/02ryutsu07_000018.html

8 参考:「情報セキュリティ 2010」:http://www.nisc.go.jp/active/kihon/pdf/is_2010.pdf

図表 5-3-2-2 「情報セキュリティ 2010」概要

「情報セキュリティ2010」の内容

2010年度及び2011年度に実施する具体的な取組の重点の詳細を記載したもの。 全 196 施策のうち、主な施策を以下に示す。

1 大規模サイバー攻撃事態への対処態勢の整備等(19施策)

(1) 対処態勢の整備(12施策)

- ○適切な初動対処のための態勢の整備 (内閣官房) 【年度内に能勢を整備、訓練を実施】
- ○サイバーテロ対策に係る体制の強化、重要インフラとの連携強 化 (警察庁)
- ○サイバー攻撃 (インシデント) 対応調整支援 (経済産業省)
- ○サイバー攻撃に対する防衛分野での体制の強化・研究等の推 進(防衛省)【年度内にサイバー企画調整官(仮称)を配置】

(2) 平素からの情報収集・共有体制の構築・強化 (7 施策)

- ○対処に資する情報の収集、内閣官房への集約、適時・適切 な共有のための体制を強化 (内閣官房、全府省庁) 【年度内に情報収集・共有のための体制を強化】
- ○サイバー攻撃に関する諸外国等との情報共有体制の構築・強 化(内閣官房、関係府省庁)【年度内に情報共有体制の在り方を検討】

筀

2 新たな環境変化に対応した情報セキュリティ政策の強化(177施策)

(1) 国民生活を守る情報セキュリティ基盤の強化(102施策)

①政府機関等の基盤強化(39施策)

- ○最高情報セキュリティ責任者(CISO)連絡会議等の開催(内 閣官房、全府省庁)【7月に設置し、速やかに開催】
- ○政府横断的な情報収集・分析システムの充実・強化(内閣官房、 全府省庁)【年内に訓練等を実施】
- ○「情報セキュリティに係る年次報告書」の作成(内閣官房、全 府省庁)【年度内に報告書を作成】

②重要インフラの基盤強化(22施策)

- ○重要インフラセプターカウンシルの支援 (内閣官房)
- ○リスクコミュニケーションの充実(内閣官房、重要インフラ所管省庁) 【年度内に推進方策を検討】
- ○事業継続計画 (BCP) の充実 (内閣官房) 【年度内に課題を抽出】

等

③その他の基盤強化等(41施策)

- ○クラウド化に対応した情報セキュリティ確保方策の検討(内閣 官房、総務省、経済産業省)【年度内にガイドライン策定の体制整備】
- ○IPv6 運用技術習得のためのテストベッドの整備 (総務省) 【年度内にテストベッドを整備】
- ○医療・教育分野における ASP・SaaS の普及に向けた取組 (総務省) 【年度内にガイドライン等を作成】
- ○中小企業に対する情報セキュリティ対策支援(経済産業省)等

(2) 国民・利用者保護の強化(29施策)

-) 「包括的な普及・啓発プログラム」の策定 (内閣官房) 【年度内にプログラムを策定】
- ○情報セキュリティ安心窓口(仮称)の検討(内閣官房、経済産 業省、総務省、関係府省庁)【年度内に窓口の在り方を検討】
- ○各事業分野における個人情報保護ガイドラインの見直しの検 討(内閣官房、関係府省庁)
- 【2011年6月までに暗号化等のインセンティブの在り方を検討】 ○デジタルフォレンジック等、サイバー犯罪の取締りのための態 勢の強化 (警察庁)

(3) 国際連携の強化(15施策)

- ○情報セキュリティ政策に関する二国間政策対話の強化(内閣 官房、関係府省庁)【年度内に日米サイバーセキュリティ会合を開催、 2011年3月に日・ASEAN情報セキュリティ政策会議を開催】
- ○多国間の枠組み等における国際連携・協力の推進(内閣官房、 関係府省庁)【MERIDIAN、FIRST 等の会合に参加】

(4) 技術戦略の推進等(24施策)

- ○新たな情報セキュリティ研究開発戦略の策定 (内閣官房) 【2011年6月を目途に戦略を策定】
- ○情報セキュリティ人材育成に係る工程表の策定の推進 (内閣) 官房) 【2011年6月を目途に工程表を取りまとめ】 等

(5) 情報セキュリティに関する制度整備 (7 施策)

- ○サイバー犯罪に適切に対処する法整備等の推進(法務省)
- ○各国のセキュリティ法制度の調査 (内閣官房) 【年度内にアジア諸国の法制度の調査に着手】 等

(2) 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「第2次情報セキュリティ基本計画| 等を踏まえ、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、以下 のような取組を実施している。

ア ネットワークの強化、信頼性の確保 (ア)「サイバークリーンセンター」

平成18年12月に、総務省及び経済産業省の共管 により開設。平成23年3月まで、ボット対策情報を

発信するとともに、効率的にボットを捕獲することで ボット感染パソコンユーザーを特定し、特定したボッ ト感染パソコンユーザーに対する駆除ツールの提供等 を行っていた⁹。平成23年度以降は、民間を中心に 運営する予定であり、現在準備が進められている。

(イ)「インシデント情報共有・分析センター (Telecom-ISAC Japan)]

平成14年7月に、ISPを中心として設立(平成 17年2月に財団法人日本データ通信協会に編入)。

9 参考: サイバークリーンセンター: https://www.ccc.go.jp/

情報通信ネットワークの安全性・信頼性を向上させるため、情報セキュリティに関する情報を業界内で共有・分析する組織として、活動を行っている¹⁰。

(ウ) [T-CEPTOAR]

Telecom-ISAC Japan の枠組みも活用し、固定系、アクセス系、携帯電話事業者にも範囲を拡大した電気通信分野の「情報共有・分析機能(CEPTOAR)」として、平成19年4月から運営。

イ ネットワークにつながるモノへの多様化への対応 (ア) ASP・SaaS の利用の促進

平成20年4月から、(財)マルチメディア振興センターにおいて、「ASP・SaaS 安全・信頼性に係る情報開示認定制度」が開始されている¹¹。これは、今後、ASP・SaaS サービスの利用を考えている企業や地方公共団体等が、事業者やサービスを比較、評価、選択する際に必要な「安全・信頼性の情報開示基準を満たしているサービス」を認定するもので、平成23年3月31日現在で、127件のASP・SaaSを認定している。

ウ 人的・組織的能力の向上

(ア)「電気通信事業における情報セキュリティマネジ メント指針」

インターネットの急速な普及を踏まえ、電気通信事業者にとっては、情報をより適切に管理するための組織体制を確立することが急務となっている。そのため総務省では、特に電気通信事業者において遵守又は考慮することが望ましい対策事項について、平成18年3月、「電気通信事業における情報セキュリティマネ

ジメント指針」を策定、平成18年6月に業界ガイドライン化している。

同指針は2008年(平成20年)2月に国際電気通信連合(ITU:InternationalTelecommunication Union)において、また同年6月に国際標準化機構/国際電気標準会議(ISO/IEC)において、ISM-TG (Information Security Management Guideline for Telecommunications, X.1051|ISO/IEC27011)として国際標準が決定された。

また、現在、ITUにおいては、中小企業の電気通信事業者による ISM-TG の実施を促進することを目的とした標準化の検討が進められており、我が国として、平成 23 年 4 月の ITU の場に、中小企業を対象とした情報セキュリティマネジメントガイドラインに係る寄書を提出する等、主導的に貢献している。なお、本ガイドラインは、平成 24 年 2 月の勧告化を目指しているところである。

(イ) 「総務省 国民のための情報セキュリティサイト」

平成 15 年 3 月から、総務省ホームページ内に「総務省国民のための情報セキュリティサイト」を開設し、国民一般向けに情報セキュリティに関する知識や対策等の周知・啓発を継続的に実施している ¹²。

(ウ) [e- ネットキャラバン]

平成 18 年 4 月から、総務省、文部科学省及び通信関係団体等が連携し、子どもたちのインターネットの安心・安全な利用に向けて、おもに保護者及び教職員を対象とした啓発講座を全国規模で行う「e-ネットキャラバン」を実施している ¹³。

(3) 電気通信サービスにおける安全・信頼性の確保

ア 安全・信頼性の確保

総務省では、電気通信サービスの安全・信頼性を確保するため、法令において設備の技術基準を定め、これを担保するために電気通信主任技術者の選任義務や管理規程の届出義務を課し、さらには、ガイドライン(「情報通信ネットワークの安全・信頼性基準」(昭和62年郵政省告示第73号))の活用の促進を図ってきた14。

ネットワークの IP 化が進展し、様々な新しい IP 系サービスの利用が拡大する一方で、IP 系サービス における通信障害が増加、大規模化、長時間化するな

どの傾向にあることを受け、平成 20 年 4 月に Γ IP ネットワーク管理・人材研究会」を開催し、平成 21 年 2 月に最終報告書を取りまとめ、公表した。

総務省は、平成22年2月に当該報告書を踏まえ、電気通信事業者に課している事業用電気通信設備の監督を行う電気通信主任技術者の選任の要件を見直し、複数の都道府県を業務区域とする場合には、設備を直接管理する事業場への選任に加え、原則、設備を設置する都道府県ごとに電気通信主任技術者を選任することを義務付けるため、電気通信主任技術者規則(昭和60年郵政省令第27号)の一部改正等を行った。

- 11 参考:「ASP・SaaS 安全・信頼性に係る情報開示認定制度」:http://www.fmmc.or.jp/asp-nintei/
- 12 参考:「総務省国民のための情報セキュリティサイト」: http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm
- 13 参考:[e- ネットキャラバン]:http://www.e-netcaravan.jp/
- 14 参考:「情報通信ネットワークの安全・信頼性基準」:http://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/anshin/kijyun.html

また、当該報告書において、IP 化の進展に対応し た電気通信主任技術者に求められるスキルを具体的か つ体系的に整理、公表することで、人材の育成・確保 に役立てることが必要であるとの提言がなされたこと を受け、平成22年10月に「電気通信主任技術者ス キル標準」を公表した。

イ 公共ブロードバンド移動通信システムの推進

現在、災害等の現場において使用される警察、消防・ 救急等の公共通信システムは音声が中心であるが、被 災地等の正確な情報の共有のため、機動的かつ確実に 映像伝送を行う手段が求められている。

そこで総務省では、平成19年6月の情報通信審議 会一部答申を踏まえ、地上テレビジョン放送のデジ タル化により空き周波数となる VHF 帯の一部につい て、安全・安心な社会実現のためにブロードバンド 通信が可能な自営通信を導入することとし、平成21 年4月に「公共ブロードバンド移動通信システムの 技術的条件」について情報通信審議会に諮問した。平 成22年3月の情報通信審議会の答申に基づき、平成 22年8月には、公共ブロードバンド移動通信システ ムの導入に必要な関係規定の整備を行ったところであ る。

(4) 暗号技術の安全性評価と高度化の推進

ネットワークを利用した社会経済活動において不可 欠な情報セキュリティを確保するためには、安全で実 装性に優れた暗号技術を利用することが重要である。

- ① 「暗号技術検討会」(総務省及び経済産業省が共 同で開催) 15
- ② 「暗号方式委員会」((独)情報通信研究機構及 び(独)情報処理推進機構が共同で開催) 15
- ③ 「暗号実装委員会」(同上) 15
- ④ 「暗号運用委員会」(同上) 15

からなる暗号評価プロジェクト「CRYPTREC」

(Cryptography Research and Evaluation Committees)は、暗号技術を公募し、客観的な評価 を行った結果として、安全性及び実装性に優れている と認められた暗号技術をリスト化した「電子政府推奨 暗号リスト」16を、平成15年2月から公表している。

暗号技術検討会においては、電子政府利用等に資す る暗号技術の評価等を行っており、電子政府推奨暗号 リストを改訂するため、平成21年度には、電子政府 推奨暗号リスト改訂のための暗号技術の公募を実施 し、平成22年度及び平成23年度には当該公募技術 の評価を実施している。

電子データの信頼性の確保

(1) 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利用した社会経済活 動の更なる発展を図ることを目的として、電子データ に付される電子署名の円滑な利用環境を確保するた め、本人が行った電子署名が付された電子文書等につ いて、手書き署名や押印が付された紙文書と同様の法 的効力を認めること、特定認証業務に関する任意的認 定制度を導入すること等について定めた「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) が平成13年4月から施行されている。平成23年4 月末現在、18件の特定認証業務が認定を受けている。

電子署名法附則第3条においては、施行後5年を 経過した場合に、同法の施行の状況について検討を行 うものとされており、総務省、法務省及び経済産業省 は、平成19年12月から電子署名及び認証業務に関

する法律の施行状況に係る検討会を開催し、平成20 年3月に報告書を策定した 17。

平成 21 年度には、電子署名法に係る電子証明書に 使用されている暗号アルゴリズムに関して、より安全 性の高いものへの移行における技術面・制度面の課題 を調査・分析し、認定認証業務における暗号アルゴリ ズムの円滑な移行を可能とするために必要な実務面及 び移行スケジュールに係る検討を行うため、「電子署 名法における暗号アルゴリズム移行研究会 | を開催し、 検討を行い、暗号移行計画については平成22年3月 に報告書を策定した。また、平成22年度にも、引き 続いて同研究会を開催し、暗号危殆化時緊急時対応計 画や指定調査機関の調査の在り方等について検討を行 い、平成23年3月に報告書を策定した。

15 参考: 「暗号技術検討会」: http://www.cryptrec.go.jp/

16 参考:電子政府推奨暗号リスト:http://www.cryptrec.go.jp/list.html

¹⁷ 参考:「電子署名及び認証業務に関する法律の施行状況に係る検討会」報告書の公表及び意見募集の結果: http://www.soumu.go.jp/menu_news/s-news/2008/080530_4.html

(2) 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ための 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きている。

総務省では、平成 16 年 11 月に、民間事業者が提供するタイムビジネスを国民が安心して利用できるよう、「タイムビジネスに係る指針」を策定・公表するなどタイムビジネスの利用促進に積極的に取り組んでいるところである 18。

この指針を受けて、(財) 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」を平成17年2月に創設(平成23年3月末現在、4件の時刻配信業務及び5件の時刻認証業務を認定)している¹⁹。また、平成18年7月には、民間において、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」が設立されている²⁰。

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 勧告の改訂案(日本提案)が SG7 において承認され、これ受けた時刻配信・監査の在り方の明確化、また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、当該認定制度の技術基準の改定(平成 24 年度)に向けて作業中である。

4 消防防災分野における ICT 化の推進

(1) 災害に強い消防防災ネットワークの整備

大規模災害時には、地方公共団体が把握した災害の 規模や被害の概況を国が迅速かつ的確に把握し、緊急 消防援助隊の出動その他の災害応急対策を迅速に講じ ることが重要である。このため、災害時においても通 信を確実に確保し、情報の収集及び伝達を迅速かつ確 実に行うべく、国、都道府県、市町村等においては、 加入電話、携帯電話等の公衆網及び専用線等を使用す るほか、災害に強く輻そうのおそれのない自営網である消防防災通信ネットワークを整備している。

総務省では、今後も、消防防災通信ネットワークの整備促進及び充実強化を図るとともに、非常通信協議会の活動等により、不通となった場合の通信の確保に努めている。

(2) ICT 化の今後の展開

全国瞬時警報システム (J-ALERT) 等の整備

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。

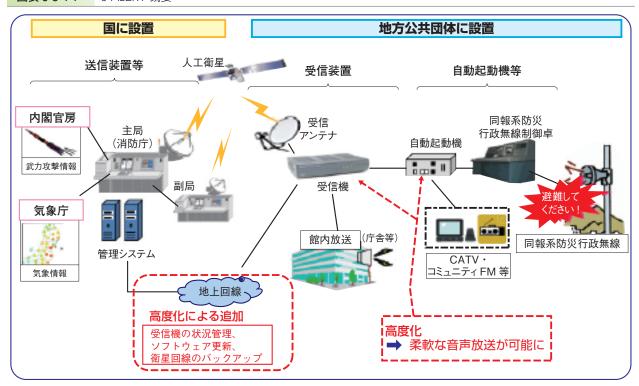
また、平成 22 年 12 月からは、状況に応じた内容の音声放送や、オンラインでのソフトウェア更新、システムの稼働状況の管理等を可能とするシステムの高度化を行ったところである(図表 5-3-4-1)。

18 参考:[タイムビジネスに係る指針]:http://www.dekyo.or.jp/tb/summary/data/MICguideline041105.pdf

19 参考:「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

20 参考:「タイムビジネス協議会」:http://www.dekyo.or.jp/tbf/guide/greeting.html

図表 5-3-4-1 J-ALERT 概要



国民保護法においては、総務大臣及び地方公共団体 の長は、武力攻撃事態等において、避難住民及び武力 攻撃災害により死亡又は負傷した住民の安否に関する 情報を収集・整理し、照会があった時は速やかに回答 することとされている。総務省では、安否情報の収集 及び提供を円滑に行うためのシステム(安否情報シス テム)を開発し、平成20年4月から運用している。 さらに、安否情報システムにおいて登録された安否情 報を検索する際に、曖昧検索可能な対象を拡大し、氏 名等の入力項目についても部分一致及び表記ゆれが あっても検索できるようシステム改修を行ったところ である。