第3節 安心・安全なユビキタスネット社会の構築

1 電気通信サービスに関する消費者行政

情報通信分野の急速な技術革新と規制緩和による競争の進展等により、高度化・多様化した電気通信サービスが国民各層に広く普及・浸透し、国民生活に大きな利便性をもたらす一方、電気通信サービスに関するトラブルや、電気通信サービスを悪用する事例も急増し、その内容も年々複雑になってきていることから、総務省では、消費者が安心して電気通信サービスを利用できるための施策を積極的に推進している。

(1) インターネット上の違法・有害情報対策

ア インターネット上の違法・有害情報への対応

インターネット上を流通する情報のうち、

① 違法な情報（児童ポルノ、麻薬売買等）

② 特定の者にとって有害と受け止められる情報（アダルト画像、暴力的画像等）

③ 公共の危険や生命に対する危険を引き起こす原因となる情報（爆発物の製造・使用、自殺等を誘発する情報等）

等が近年大きな社会問題となっている。

総務省では、平成17年8月から、有識者及び電気通信事業者団体等で構成される「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」を開催し、同研究会は、インターネット上の違法・有害情報へのプロバイダ等による自主的対応及びこれを効果的に支援する制度・方策について検討を行い、平成18年1月に中間取りまとめを、続いて同年8月に最終報告書を、それぞれ取りまとめた。

最終報告書においては、

① プロバイダや電子掲示板の管理者等が他人の掲載する違法な情報を放置した場合の刑事責任

② インターネット上の違法な情報に対するプロバイダや電子掲示板の管理者等による自主的対応及びこれを支援する方策

③ インターネット上の有害情報に対するプロバイダや電子掲示板の管理者等による自主的対応及びこれを支援する方策

④ 「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。）における発信者情報開示の運用

等の論点について、提言を行っている。

総務省では、同研究会の提言等を踏まえ、インターネット上の違法・有害情報に対して、行政の支援の下、電気通信事業者及び利用者による自主的な対応が促進され、表現の自由に最大限配慮しつつ、利用者各人がインターネットの利便性を享受できるような環境の整備に引き続き取り組んでいくこととしている。

イ プロバイダ責任制限法関係ガイドラインの策定・改定の支援

ウェブページや電子掲示板等における他人の権利を侵害する情報の増加への対策として、平成14年5月に、

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対する発信者情報の開示請求権

を規定するプロバイダ責任制限法が施行されたことを受けて、総務省では、同法が適切に運用されるよう、業界団体による同法のガイドラインの策定に対する支援や周知を行ってきている。

なお、ガイドラインについては、業界団体等により、社団法人テレコムサービス協会内に「プロバイダ責任制限法ガイドライン等検討協議会」が組織されており、これまでに、

① プロバイダ責任制限法名誉毀損・プライバシー関係ガイドライン（平成14年5月。平成16年10月改定）

② プロバイダ責任制限法著作権関係ガイドライン（平成15年11月）

③ プロバイダ責任制限法商標権関係ガイドライン（平成17年7月）

が策定されているほか、今般、「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」最終報告書（平成18年8月）の提言を受けて、

④　プロバイダ責任制限法発信者情報開示関係ガイドライン（平成19年2月）

が策定されたところである。

ウ　インターネット上の違法・有害情報に対するプロバイダ等の自主的対応に関する支援

政府は、「IT安心会議」（インターネット上の違法・有害情報等に関する関係省庁連絡会議）において、平成17年6月に「インターネット上における違法・有害情報対策について」を取りまとめるなど、インターネット上の違法・有害情報対策を推進しているところである。

総務省においても、「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」最終報告書（平成18年8月）の提言を踏まえ、平成18年9月から、社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本インターネットプロバイダー協会及び社団法人日本ケーブルテレビ連盟とともに、インターネット上の違法な情報及び公序良俗に反する情報に対するプロバイダ等による適切かつ迅速な対応を促進するための方策について検討を行った。

その検討結果を踏まえ、上記4団体は、平成18年11月に、インターネット上に掲載された情報の違法性の判断基準及び送信防止措置等の手続を定めた「インターネット上の違法情報への対応に関するガイドライン」並びにプロバイダ等が違法・有害情報に対して契約約款に基づく自主的な対応を行うための「違法・有害情報への対応等に関する契約約款モデル条項」を策定した。これにより、プロバイダ等によるインターネット上の違法・有害情報への適切かつ迅速な対応が促進されることが期待される。

エ　フィルタリングの普及促進

近年、未成年者がいわゆる出会い系サイト等インターネット上の有害な情報にアクセスし、事件に巻き込まれるケースが多発しており、社会的な問題となっている。インターネット上の有害情報への対応については、受信者側で情報の取捨選択を可能とするフィルタリングが有効な対策であり、総務省では、平成16年度から、携帯電話事業者と連携して、携帯電話向けのフィルタリングの研究開発を行い、携帯電話事業者は、この研究成果を活かして、平成17年7月からフィルタリングサービスの提供を開始している。

また、平成18年3月、フィルタリングに関係する業界団体[1]は、フィルタリングの一層の普及を図るため、総務省及び経済産業省と連携して「フィルタリングの普及啓発アクションプラン」を公表し、普及啓発活動に努めているところである。

しかしながら、フィルタリングの認知率及び普及率は低水準にとどまっており、特に、保護者の目が届きにくい携帯電話からのアクセスについては、未成年者を保護する観点から早急な対策が必要となっていたことから、平成18年11月、総務省は携帯電話事業者等に対し、フィルタリングサービスの普及促進に向けた自主的取組を強化するよう要請した。

さらに、フィルタリングの普及には、草の根的な周知啓発が重要であるため、平成19年2月、総務省は、警察庁及び文部科学省と合同で、都道府県知事、教育委員会及び都道府県警察等に対し、携帯電話のフィルタリングについて学校関係者や保護者をはじめとする地域住民への周知啓発活動に取り組むよう要請を行ったところである。

総務省では、今後も引き続き業界や関係省庁等と連携し、未成年者が安心してインターネットに接続できる環境の整備に取り組んでいくこととしている。

（2）迷惑メール対策

総務省では、受信者の同意を得ずに一方的にパソコンや携帯電話に送信される広告・宣伝目的の電子メール（いわゆる迷惑メール）に対して、次のような総合的な対策に取り組んでおり、今後も、着実に進めていくこととしている。

ア　「特定電子メールの送信の適正化等に関する法律」の適切な執行

「特定電子メールの送信の適正化等に関する法律」（平成14年法律第26号）は、一時に多数の者に対してされる広告・宣伝メールの送信等による電子メールの送受信上の支障を防止するため、広告・宣伝メールの送信者に対して、表示義務、受信拒否者に対する再送信禁止、架空電子メールアドレスあての送信の禁止、送信者情報を偽った送信の禁止といった義務を課しており、総務省ではその適切な執行に努めている。

1 社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本インターネットプロバイダー協会、社団法人日本ケーブルテレビ連盟、社団法人電子情報技術産業協会及び財団法人インターネット協会の6団体

イ　「迷惑メール追放支援プロジェクト」の推進

総務省では、経済産業省と連携して、平成17年2月から、「迷惑メール追放支援プロジェクト」を開始している。同プロジェクトでは、総務省において財団法人日本データ通信協会に設置されたモニター機で受信した迷惑メールの違法性を確認し、当該電子メールに関する情報が送信元プロバイダに通知されることにより、契約約款等に基づく迷惑メール送信回線の利用停止等電気通信事業者の自主的な迷惑メール対策の円滑な実施を促すこととしている。

ウ　技術的解決策の推進

迷惑メールは、発信元を偽る送信や自営で設置するメールサーバー等からの送信が多いため、その防止には、発信元の情報を確認する「送信ドメイン認証技術」や、動的IPアドレスを割り当てられた自営サーバー等から直接外部に送信するメールを遮断する「25番ポートブロック」が有効であると考えられている。このため総務省では、このような迷惑メール対策技術の導入に当たっての法的留意点をHP等において公表するなどして、その導入を促進している。

エ　迷惑メール対策に関する国際協調の推進

近年では、国境を越えて送信される迷惑メールが大きな問題となっていることから、総務省では、迷惑メール対策に関する国際連携を強化している。具体的には、平成17年4月に、韓国、中国等のアジア・太平洋地域の国々と覚書（MoU）を交わす一方、平成18年5月にはフランスと、9月にはイギリス、10月にはカナダと迷惑メール対策における協力推進についての共同声明を発出するなど欧米諸国との協力も推進している。

（3）フィッシング対策

金融機関等からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページを通じてクレジットカード番号等の個人情報等を不正に詐取する「フィッシング」は、電子メールやウェブサイトが主要な手段となっている。そのため、総務省では、インターネットサービスプロバイダ（ISP）とともに、平成17年1月から「フィッシング対策推進連絡会」を定期的に開催し、情報共有を図るとともに、その効果的な対策等について検討を行っており、同連絡会は、平成17年8月に、それまでの検討状況と今後取り組むべき課題等を記した「フィッシングの現状及びISPによるフィッシング対策の方向性」を取りまとめている。

総務省は、この取りまとめに基づき、電気通信事業者団体、関係機関等とともに、実行可能なところから取組を開始するとともに、引き続きフィッシング対策の更なる検討、実施を進めていくこととしている。

（4）携帯電話の悪用対策

携帯電話の普及に伴い、携帯電話が振り込め詐欺や麻薬・覚せい剤の売買等の犯罪の手段として悪用されることが増えていることから、総務省では、次のような対策を講じている。

ア　「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な使用の防止に関する法律」（平成18年4月全面施行）の適切な執行

「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な使用の防止に関する法律」（平成17年法律第31号）は、携帯電話の悪用対策として、

① 携帯電話事業者に対し、契約締結時及び譲渡時の本人確認を義務付けること

② 犯罪に利用されている疑いがある携帯電話について警察署長が携帯電話事業者に契約者の確認を求めることができること

③ 相手方の氏名及び連絡先を確認しないで携帯電話を業として有償で貸与する行為等を処罰すること

等を定めており、総務省では、その適切な執行に努めている。

イ　プリペイド式携帯電話

犯罪に悪用されることの多いプリペイド式携帯電話について、総務省と携帯電話事業者等が対策を検討した結果、携帯電話事業者は、平成17年4月から、譲渡・転売等されたものを含むすべてのプリペイド式携帯電話について、契約者に対して契約者情報の届出義務を課すとともに、契約者情報の届出がないこと等により契約者の確認ができない場合には、利用停止措置を講じるなどの対策を実施した。その結果、平成18年3月

３１日までに、携帯電話事業者は、稼働しているすべてのプリペイド式携帯電話についての契約者確認を完了するとともに、契約者情報を確認できず名義不明のままであった約３０万回線について利用停止措置を講じた。

（5）情報通信分野における個人情報の保護

ア　「個人情報の保護に関する法律」の適切な執行

すべての分野を包括的に対象として個人情報の保護について定めた「個人情報の保護に関する法律」（平成１５年法律第５７号。以下「個人情報保護法」という）が平成１７年４月から全面施行されたことに伴い、同法に基づく認定個人情報保護団体として、電気通信分野においては財団法人日本データ通信協会（電気通信個人情報保護推進センター）、放送分野においては財団法人放送セキュリティセンター（個人情報保護センター）をそれぞれ認定するなど、同法の適切な執行に努めているところである。また、平成１９年３月には、大量の個人情報漏えい事案を発生させた電気通信事業者に対し、同法に基づく勧告（情報通信分野では初めて）を行っている。

イ　「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

総務省は、電気通信事業分野における個人情報保護のため、平成3年に「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」を策定、運用してきたが、個人情報保護法の全面施行を見据え、「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」（平成１５年2月から開催）において検討を行い、個人情報の適正な取扱いのより厳格な実施を図るため、平成１６年8月に、同ガイドラインの用語、定義等をできる限り個人情報保護法と統一のとれたものとするとともに、電気通信事業者がとるべき安全管理措置の具体化、個人情報保護管理者の設置、プライバシーポリシーの策定・公表等の規定を盛り込んだ改定を行っている。

ウ　「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

平成１７年４月から個人情報保護法が全面施行されるに当たり、総務省は、「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～平成１７年2月）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、「衛星放送の将来像に関する研究会」（平成１７年１０月～平成１８年１０月）の最終報告書等を踏まえ、見直しを行い、平成１９年3月に、

① キャンペーン応募等の際に個人情報を取り扱う者を視聴者に明確に了知させることができるよう対象事業者の取組を確保するための規定

② 受信機に記録された個人情報の安全管理について対象事業者が講ずべき措置の規定

の２点を追加する改定を行った。

2　情報セキュリティ対策の推進

近年、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、企業等からの大量の個人情報の漏えい、サイバー攻撃（情報通信ネットワークや情報システムを利用した電子的な攻撃）等が社会問題化しており、国民、企業、行政機関等が、安全にICTを活用するためには、情報技術を安心・安全に活用するための取組、すなわち情報セキュリティ対策の強化が、喫緊かつ重要な課題になっている。

そのため、政府では、官民における統一的・横断的な情報セキュリティ対策を推進しており、総務省においても重点的に取り組んでいるところである。

（1）政府の情報セキュリティ対策

ア 「第１次情報セキュリティ基本計画」と「セキュア・ジャパン」

政府では、情報セキュリティ対策の中核機関として、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)」を、同年5月に高度情報通信ネットワーク社会推進戦略本部に「情報セキュリティ政策会議」（議長：内閣官房長官）を設置し、我が国全体としての情報セキュリティ対策を推進しているところである。

平成18年2月に、情報セキュリティ政策会議において、我が国全体としての情報セキュリティ問題全般についての3年間（平成18年度～平成20年度）の戦略として、「第１次情報セキュリティ基本計画」が決定されており、同計画においては、

① 経済国家日本の持続的発展を支える情報セキュリティ
② 安全・安心で、より良い国民生活を実現するための情報セキュリティ
③ 我が国の安全保障におけるITに起因する新たな脅威に対応するための情報セキュリティ

の三つの基本理念の下、今後3年間で官民の全主体が適切な役割分担を果たす「新しい官民連携モデル」を構築し、その結果、我が国が「情報セキュリティ先進国」へ進展することを目指し、政府が取り組む重点政策の方向性及び政策の推進体制が提示されている。

その後、平成18年6月には、平成18年度における具体的な施策の実施計画である「セキュア・ジャパン2006」を決定した。その主な内容は次のとおりである。

（ア）平成18年度における我が国の情報セキュリティ対策の重点施策

「官民における情報セキュリティ対策の体制の構築」を重点とし、以下の施策を推進することとしている。

① 対策実施4領域（政府機関・地方公共団体、重要インフラ、企業及び個人）における情報セキュリティ対策の強化
② 横断的な情報セキュリティ基盤の形成（情報セキュリティ技術戦略の推進、情報セキュリティ人材の育成・確保、国際連携・協調の推進、犯罪の取締り及び権利利益の保護・救済）
③ 政府の推進体制と持続的改善の構造

（イ）平成19年度における重点施策の方向性

「官民における情報セキュリティ対策の底上げ」を重点とし、以下の施策を推進することとしている。

① 模範となる領域（政府機関、重要インフラ）の情報セキュリティ対策の底上げ
② 企業及び個人のうち取組が遅れがちな主体の対策の底上げ
③ 横断的な情報セキュリティ基盤の底上げ

これらの決定を受け、政府では、総合的な情報セキュリティ対策を推進、平成19年4月には、この「セキュア・ジャパン2006」に基づく施策への取組及び取組を受けた現状について評価等を実施のうえ、平成19年度における年度計画「セキュア・ジャパン2007」の案を取りまとめたところである。

イ 政府機関の情報セキュリティ対策の推進

情報セキュリティ政策会議は、政府機関の情報セキュリティ対策について、平成17年9月に「政府機関の情報セキュリティ対策の強化に関する基本方針」等を、また、同年12月に「政府機関の情報セキュリティ対策のための統一基準」（以下「政府機関統一基準」という。）を決定しており、この政府機関統一基準に基づき、各府省による情報セキュリティポリシーの整備が図られている。

また、内閣官房情報セキュリティセンターは、各府省の情報セキュリティ対策の推進状況について、政府機関統一基準に基づき、必要な範囲で検査・評価を行っており、これを基に情報セキュリティ政策会議が各府省の対策の改善を勧告することにより、政府全体としてのPDCAサイクルの実施を推進することとされている。

なお、政府機関統一基準については、定期的に見直しを行うこととされており、平成19年4月、その改定案が取りまとめられたところである。

ウ 重要インフラに関する情報セキュリティ対策の推進

我が国の国民生活・社会経済活動を支える「重要インフラ」（現在、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）、医療、水道及び物流が対象とされている。）については、安定的供給の確保が最優先の課題であり、そのためには、サイバー攻撃等の意図的要因だけではなく、人為的ミス等の非意図的要因や地震・津波等の自然災害等、あらゆる脅威から適切に防護される必要がある。情報セキュリティ政策会議は、近年の各重要インフラ分野におけるICT利用の進展を踏まえ、平成17年9月に「重要インフラの情報セキュリティ対策に係る基本的考え方」を、また、同年12月に「重要インフラの情報セキュリティ対策に係る行動計画」を決定している。

また、内閣官房情報セキュリティセンターは、同計画に基づき、重要インフラにおける情報セキュリティ確保に係る安全基準等の整備、情報共有体制の強化、相互依存性解析及び分野横断的演習に重点政策として掲げ、人為的ミス、災害等への対策も含め、重要インフラによる安定的供給の確保を推進しており、重要インフラ所管省庁（総務省、経済産業省、国土交通省、厚生労働省及び金融庁）も、それぞれの所管分野において、安全基準等の策定、情報共有・分析機能の整備等を進めているところである。

（2）インターネットの安心・安全な利用環境の実現

ICT化の進展は、国民生活、経済活動に多大な利便向上等をもたらす一方、情報通信システムへの攻撃により社会全体に重大な事態が引き起こされる可能性も増大することから、今後の高度情報通信ネットワーク社会の形成の推進に当たっては、情報セキュリティ対策の強化による安心・安全な利用環境の実現が不可欠である。

総務省では、政府全体の情報セキュリティ対策の取組状況や、「次世代IPインフラ研究会」（平成16年2月～平成17年6月）の第二次報告書「「情報セキュリティ政策2005」の提言」（平成16年7月）等を踏まえ、

① ネットワークを通じた障害の広域化への対応
② ネットワークにつながるモノの多様化への対応
③ 人材面の脆弱性の克服

の三つの面から、次のとおり、情報セキュリティ対策の強化に向けた取組を行っている。

ア　ネットワークの強化・信頼性の確保

総務省では、「ネットワーク」面からの情報セキュリティ対策として、犯罪行為・迷惑行為やトラヒック急増への対応、災害への備え、事業者間情報共有の推進等を実施している。

（ア）ボットネットを悪用した一斉攻撃への対策

「ボットネット」とは、一種のウイルスである「ボットプログラム」に感染した多数のパソコン及び攻撃者の命令を送信する指令サーバーからなるネットワークであり、悪意のある第三者の命令に従って、

① 特定のウェブサイトへのサイバー攻撃
② スパムメールの送信やフィッシング用ウェブサイトの開設
③ 感染したパソコン内の個人情報等の漏えい

を行うなど、様々な情報セキュリティ上の問題を引き起こしている。

そのため、総務省では、経済産業省と連携して、

① ボットネットの要因となるボットプログラムの収集・分析・解析を行うシステムの開発及び試行運用
② ボットプログラムを削除するソフトウェアの開発
③ ISPを通じた一般ユーザーへの配布・適用

等の対策を講じている。

また、平成18年12月には、ボット対策プロジェクトとして、両省共同運営のポータルサイト「サイバークリーンセンター」を開設した。両省は、このサイトを通じて、

① ユーザーのコンピュータからのボット駆除方法の提供
② ISPの協力を得て、ボット感染ユーザーに対し、感染事実の通知や駆除方法の提示、再感染防止の促進

等の活動を行っているところである。

（イ）情報漏えい対策技術の研究開発

ファイル共有ソフトの利用等による情報漏えいが大きな社会問題となっており、利用者の自助努力のみでは対処が困難な状況となっている。そのため、総務省では、平成19年度から情報漏えいの予防・対策の高度化・容易化を図る技術開発を行うこととしている。

（ウ）インターネットにおける経路ハイジャック防止技術の確立

インターネットは、ISP、大学、企業等の主体が運営するネットワークが相互に接続されており、各ネットワーク間において通信経路を確立するための経路情報の保持・交換が行われている。一部の国内ISPにおいては、不正な経路情報の交換による「経路ハイジャック」が発生し、障害の検知・回復にかなりの時間を要する事例が起こっている。そのため、総務省では、平成18年度からこうした「経路ハイジャック」を検知・回復・予防するための研究開発を推進している。

（エ）次世代バックボーンに関する研究開発、ネットワークセキュリティ基盤技術の研究開発等の推進

総務省では、今後のトラヒックの急増に対応し得るよう、情報通信インフラ強化の一環として、地域に閉じたトラヒックについては当該地域内で交換することを可能とする技術等の確立を目指して、平成17年度から次世代バックボーンに関する研究開発を推進している。

また、ネットワークの強化・信頼性の確保に向け、IPトレースバック技術等ネットワークのセキュリティを確保するための基盤技術の研究開発を推進している。

（オ）通信業界における情報セキュリティ対策に向けた取組

インターネットサービスを提供する電気通信事業者を中心に、平成14年7月に、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、セキュリティ情報を業界内で共有・分析する組織として、「インシデント情報共有・分析センター」（Telecom-ISAC Japan。ISAC：Information Sharing and Analysis Center）が設立された（同センターは、平成17年1月に、当初の任意団体から財団法人日本データ通信協会内の組織に移行）。これにより、それまでの各々の電気通信事業者が個別に対応する形態から、我が国のネットワーク全体にわたるセキュリティ情報の収集・共有・分析を行うとともに、機動性及び実効性のある情

報セキュリティ対策を共同して実施することが可能な体制が確立された。

また、電気通信分野の民間企業や業界団体等から構成される「電気通信分野における情報セキュリティ対策協議会」において、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：Capability for Engineering of Protection, Technical Operation, Analysis and Response）」の整備に向けた検討が行われ、平成19年4月から、「T-CEPTOAR」が運営を開始している。

イ　ネットワークにつながるモノの多様化への対応

総務省では、「モノ」面からの情報セキュリティ対策として、多様な機器のネットワーク接続に伴うセキュリティ確保等を行っている。

（ア）多様な機器のネットワーク接続に伴うセキュリティ確保

身の回りのあらゆるモノが通信機能を持ついわゆる「ユビキタス環境」の構築に向けて、膨大なアドレス空間を持ち、高いセキュリティを実現するIPv6インターネット網の利用が必要となっている。また、誰もが容易に、かつ安心・安全に、膨大な数の「ユビキタス機器」を利用可能とするためには、複雑なセキュリティ対策をIPv6インターネット網側からサポートするシステムが求められる。

そのため、総務省では、平成18年度からこのようなセキュリティサポートシステムの構築に向けた実証実験を実施し、IPv6によるユビキタス環境構築に向けたセキュリティ確保上の課題解決を図るとともに、ガイドラインを策定することとしている。また、実証実験の成果を国内外に広く公表し、IPv6によるユビキタス環境の構築を促進することとしている。

ウ　人的・組織的能力の向上

総務省では、「人材・組織」面からの情報セキュリティ対策として、サイバー攻撃対応演習の実施や情報セキュリティマネジメントの確立、個人向けの教育・啓発活動の強化等を実施している。

（ア）サイバー攻撃対応演習

国民の社会生活インフラとして定着しているインターネットにおいて広域的・組織的なサイバー攻撃が発生した場合には、個々の電気通信事業者のみでは対応できないことから、組織横断的な緊急対応体制の強化や事業者間及び事業者と行政間で連携してセキュリティ対策を講じることのできる人材の育成が求められている。

そのため、総務省は、電気通信事業者等とともに、サイバー攻撃等に備えた緊急対応体制が実際に機能するかなどについて検証し、

① 組織横断的な緊急対応体制を強化する
② 緊急時の対応において調整力を発揮できる高度なICTスキルを有する人材の育成を図る

ことを目的として、平成18年度から3箇年計画で「電気通信事業分野におけるサイバー攻撃対応演習」を実施している。

（イ）電気通信事業における情報セキュリティマネジメントの確立

インターネットの急速な普及を踏まえ、情報セキュリティの確保が強く求められる中で、特に、自らのネットワークをユーザーの通信の用に供する電気通信事業者については、「通信の秘密」に属する情報をはじめ多くのユーザー情報を取り扱うことから、情報をより適切に管理するための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、国際電気通信連合（ITU）において勧告化されている情報セキュリティマネジメント規格（X.1051）をもとに、法令上の要求事項等、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事項について「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」（ISM-TG：Information Security Management Guideline for Telecommunications）として取りまとめ、ITUにおいて、国際標準化に向けた提案を行うとともに、国内では、「電気通信分野における情報セキュリティ対策協議会」において、同指針を「電気通信事業における情報セキュリティマネジメントガイドライン」として業界ガイドライン化し、公表した。また、「重要インフラの情報セキュリティ対策に係る行動計画」を受け、電気通信分野において必要な又は望ましい情報セキュリティ対策の水準を明示し、対策強化を図るため、同協議会において、「電気通信分野における情報セキュリティ確保に係る安全基準（第1版）」を策定し、電気通信分野における情報セキュリティの確保に向けて業界をあげた取組を行っている。

（ウ）情報通信人材研修事業支援制度

総務省では、情報通信セキュリティ人材を含む情報通信分野の専門的な知識や技術の向上を図る情報通信人材研修事業を実施する第三セクターや公益法人等に対し、当該事業に必要な経費の一部を助成する「情報通信人材研修事業支援制度」を平成13年度から実施している。

（エ）個人向け教育・啓発活動強化

総務省では、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。平成１８年6月には、総務省のホームページにインターネット利用者への「情報セキュリティ対策のお願い」を掲載するなどの「情報セキュリティ対策の集中啓発」を行った。

また、総務省及び文部科学省並びに関係公益法人等が協力し、主に保護者及び教職員向けにインターネットの安心・安全利用に向けた啓発を行う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。平成１８年度においては、全国で４５３講座を開催した。

さらに、総務省においては、今後のICTメディアの健全な利用の促進を図り、子どもが安全に安心してインターネットや携帯電話等を使用できるようにするため、平成１８年度に総合的なICTメディアリテラシーを育成するプログラム「伸ばそうICTメディアリテラシー　～つながる！わかる！伝える！これがネットだ～」の開発を行い、平成１９年度にその普及を図ることとしている。

（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、情報通信システムの安全・信頼性対策に関する指標として「情報通信ネットワーク安全・信頼性基準」（昭和６２年郵政省告示第７３号）を策定し、電気通信事業者による同指針の活用の促進を図っているところである。

しかしながら、ネットワークのIP化が進展し、新しいICTサービスの利用が拡大する中で、昨今、これらのサービスにおける通信障害等の事故件数が増加する傾向にある。

また、事故の特徴についても、従来のネットワークと異なってきており、

① 人為的要因による事故の増加
② ソフト的な不具合に起因する事故の増加
③ 事故の大規模化と復旧の長時間化

といった傾向が表れてきている。

このような状況を踏まえ、平成１８年8月から、ネットワークのIP化に対応した安全・信頼性対策について、情報通信審議会において審議がなされているところである。

イ　重要通信の確保

火災、事故、人命に関わる事態における救援、救助等に直接関係ある機関等が行う通信や治安の維持のために緊急を要する事態における警察相互間の通信等の重要通信については、災害等の非常時においても、その疎通を確保する必要がある。重要通信の確保については、従前から、電気通信事業者により、

① 電気通信設備の安全・信頼性対策
② 通信の輻そう対策
③ 通信手段の確保

等の観点から対策が講じられてきているが、近年、ネットワークのIP化、情報通信サービスの高度化、多様化の進展や、重要通信に対するニーズの変化に対応していくことが求められており、上記の審議会の中で審議されたほか、緊急通報高度化の制度整備を行った。

ウ　緊急通報機能等の高度化

携帯電話やIP電話からの緊急通報が急増していることから、総務省では、平成１５年１１月、情報通信審議会に「電気通信事業における緊急通報機能等の高度化方策」について諮問し、同審議会から、

① 「携帯電話からの緊急通報における発信者位置情報通知機能に係る技術的条件」（平成１６年6月）
② 「IPネットワークにおける緊急通報等重要通信の確保方策」（平成１７年3月）

について答申を受けた。

これらを踏まえ、総務省は、平成１８年1月に関係省令及び告示の改正を行い、電気通信事業者が緊急通報を取り扱う場合においては、

① 携帯電話については、GPS（Global Positioning System）等を利用した位置情報（緯度経度等）を緊急通報受理機関へ通知すること
② 固定IP電話については、住所情報等を緊急通報受理機関へ通知すること

とし、平成１９年4月から施行したところである。

（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、客観的にその安全性が評価され、実装性に優れた暗号技術を採用することが重要である。

そこで、

① 「暗号技術検討会」（総務省及び経済産業省が平成

13年度から共同で開催）
② 「暗号技術評価委員会」（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開催）
の両者から構成される暗号評価プロジェクト「CRYPTREC」（Cryptography Research and Evaluation Committees）は、平成15年2月に暗号技術を公募し、客観的な評価を行った結果、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、平成15年2月に「電子政府における調達のための推奨すべき暗号のリスト」（電子政府推奨暗号リスト）を決定している。これを受けて、「各府省の情報システム調達における暗号の利用方針」（平成15年2月行政情報システム関係課長連絡会議了承）において、各府省は、情報システムの構築に当たり暗号を利用する場合には、可能な限り電子政府推奨暗号リストに掲載された暗号の利用を推進するものとされている。

その後、「暗号技術評価委員会」に代わり、「暗号技術検討会」の下に「暗号技術監視委員会」と「暗号モジュール委員会」が設置され、現在に至っている。

CRYPTRECでは、平成18年も引き続き、電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査、研究、基準の作成等を行った。

3 電子データの信頼性の確保

電子商取引や、電子申請・電子申告等のネットワークによる取引、手続等については、
① 「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律」（平成13年法律第95号）
② 「行政手続等における情報通信の技術の利用に関する法律」（平成14年法律第151号）
等の法制面の整備が行われ、また、電子データによる文書、帳簿等の保存については、
① 「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」（平成10年法律第25号）
② 「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号）（e-文書法）
等の整備が行われたところである。

これらの制度面の整備ともあいまって、今後、電子データによる取引、手続等や文書、帳簿等の保存が一層活発に行われていくこととなるが、その際、これらの電子データについて、
① 作成・送信した者が本人に相違ないこと
② 内容が改ざんされていないこと
③ ある時点において、存在したこと、送信されたこと
等が証明できる仕組みが整えられていないと、取引、手続、保存等の安全性が確保できないこととなり、ネットワークを利用した社会経済活動に支障が生じることとなる。

そのため、次のような様々な措置が講じられている。

（1）電子署名・認証業務の普及促進

「電子署名」は、電子データについて、本人が作成したものであることを示し、内容が改ざんされていないことを確認できるようにするための措置である。この電子署名の円滑な利用環境を確保するため、
① 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
② 特定認証業務（基準に適合した電子署名が行われることを認証する業務）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）（以下「電子署名法」という。）が、平成13年4月から施行されており、平成18年度末現在、18件の特定認証業務が認定を受けている。

総務省では、同法を共管する法務省及び経済産業省とともに、電子署名や認証業務に対する国民の理解を深めるため、広報活動等を通じた普及啓発活動を行うほか、国境を越えた電子商取引の促進に向け、諸外国との国際協調にも取り組んでいる。

なお、地方公共団体による公的個人認証サービスについては、第4節3（4）において記述している。

（2）タイムビジネスの利用促進

「タイムビジネス」とは、ネットワーク上を流通し、また、サーバー等に保存される電子データの信頼性を高めるために行われる、

① 時刻配信業務（ネットワーク上において正確な時刻情報を配信するサービス）

② 時刻認証業務（電子データに付与された「タイムスタンプ」の有効性を証明することにより、電子データの存在した時刻とその時刻以降の非改ざんを証明するサービス）

の総称であり、ネットワーク化の進展等に伴い、その重要性がますます高まってきている。

そのため、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。

なお、この指針を受けて、財団法人日本データ通信協会では、平成17年2月に、一定の基準を満たすタイムビジネスを同協会が認定することにより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」を創設しており、平成18年度末現在、4件の時刻配信業務及び5件の時刻認証業務が認定を受けている。

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」が設立された。同協議会では、より使いやすく信頼されるタイムスタンプ等の普及を目指し、セミナーの開催等啓発活動等を積極的に推進している。

（3）文書の電子保存における電子署名・タイムスタンプの利用

文書を電子保存する場合において、電子署名やタイムスタンプを利用することにより、非改ざん性や作成者・作成日時等の証明が容易になり、文書の信頼性が高まることになる。そのため、電子保存される文書のうち、高い信頼性が求められる国税関係書類及び地方税関係書類並びに医療分野における関係文書等については、関係省令やガイドラインにおいて電子署名及びタイムスタンプの付与を行うこととされており、このとき、電子署名に係る電子証明書は電子署名法に基づき主務大臣が認定した特定認証業務によって発行されたものであることが、また、タイムスタンプは財団法人日本データ通信協会が認定した時刻認証業務で提供されたものであることが求められている。