第4節 安心・安全ネットワークの構築

SECTION 04

1 電気通信サービスに関する消費者行政

（1）インターネット上の違法・有害情報対策

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で、電気通信サービスをめぐるトラブルも急増し、その内容も年々複雑になってきている。こうした状況の中、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取組を積極的に推進している。

1 プロバイダ責任制限法及び関係ガイドライン

インターネットの急速な普及に伴い様々な電気通信サービスの提供が可能となってきている一方で、他人の権利を侵害する情報の流通も増加してきている。その対策として、平成14年5月、インターネット上のウェブページや電子掲示板等による情報の流通によって他人の権利が侵害された場合について、（ア）プロバイダ等の損害賠償責任の制限・明確化、（イ）（被害を受けた者からの）発信者情報の開示請求権を規定する、いわゆるプロバイダ責任制限法（「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」）が施行された。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。

平成16年10月には、業界団体等により構成される「プロバイダ責任制限法ガイドライン等検討協議会」が策定した「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」が改訂され、①インターネット上の情報の流通による重大な人権侵害事案であって、②被害者自らが被害の回復・予防を図ることが困難な場合に、法務省人権擁護機関（各法務局長及び地方法務局長）がプロバイダ等に対し当該情報の削除依頼を行う手続等が新たに定められた。

また、インターネットオークション等における模倣品の流通が問題となっていることを受け、平成17年7月に同協議会において商標権侵害の具体例、インターネットオークション事業者等への削除要請の統一的手順・様式、信頼性確認団体を経由した削除の申出等について記述した「プロバイダ責任制限法商標権関係ガイドライン」が策定され、同年9月には、同ガイドラインに基づく信頼性確認団体が認定された。

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

インターネット上における違法な情報（児童ポルノ、麻薬販売等）や、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）、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）等の流通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、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公表した。今後も引き続き検討を進め、平成18年7月を目途に最終的な取りまとめを行う予定である。

また、最近、インターネット上の電子掲示板等で自殺の決行をほのめかす書き込みや集団自殺を呼びかける書き込みがなされ、これらの自殺予告を発見した者から通報を受けた警察による自殺を防止するため当該書き込みをした者の氏名、住所等（発信者情報）を緊急に入手することが必要な事案（自殺予告事案）が見られ、問題となっている。

こうした自殺予告事案におけるプロバイダ等の対応について、総務省では、電気通信事業者団体及び警察庁と共に検討を進め、平成17年10月に電気通信事業者団体4団体により、自殺予告事案に関してプロバイダ等が警察から発信者情報の開示を求められた際の情報開示の判断基準や手続等に関する行動指針となる「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」が策定、運用されている。

3 モバイルフィルタリング技術の研究開発

近年、携帯電話等を通じたインターネットが幅広い年齢層に急速に普及する一方、出会い系サイト等を通じた児童買春等が社会問題となっている。既にパソコン向けに実現している有害コンテンツのフィルタリング機能（インターネットのウェブページのうち特定の条件に合致する（しない）ページの閲覧を遮断等する機能）を、“モバイル”向けにも実現するため、総務省では、児童の健全育成の観点から、平成16年度から平成17年度にかけて、「モバイルフィルタリング技術の研究開発」に取り組んだ。なお、本研究開発の成果等を活かし、携帯電話事業者は、昨年から逐次、フィルタリングサービスの提供を開始している。

(2) 迷惑メール・フィッシング対策

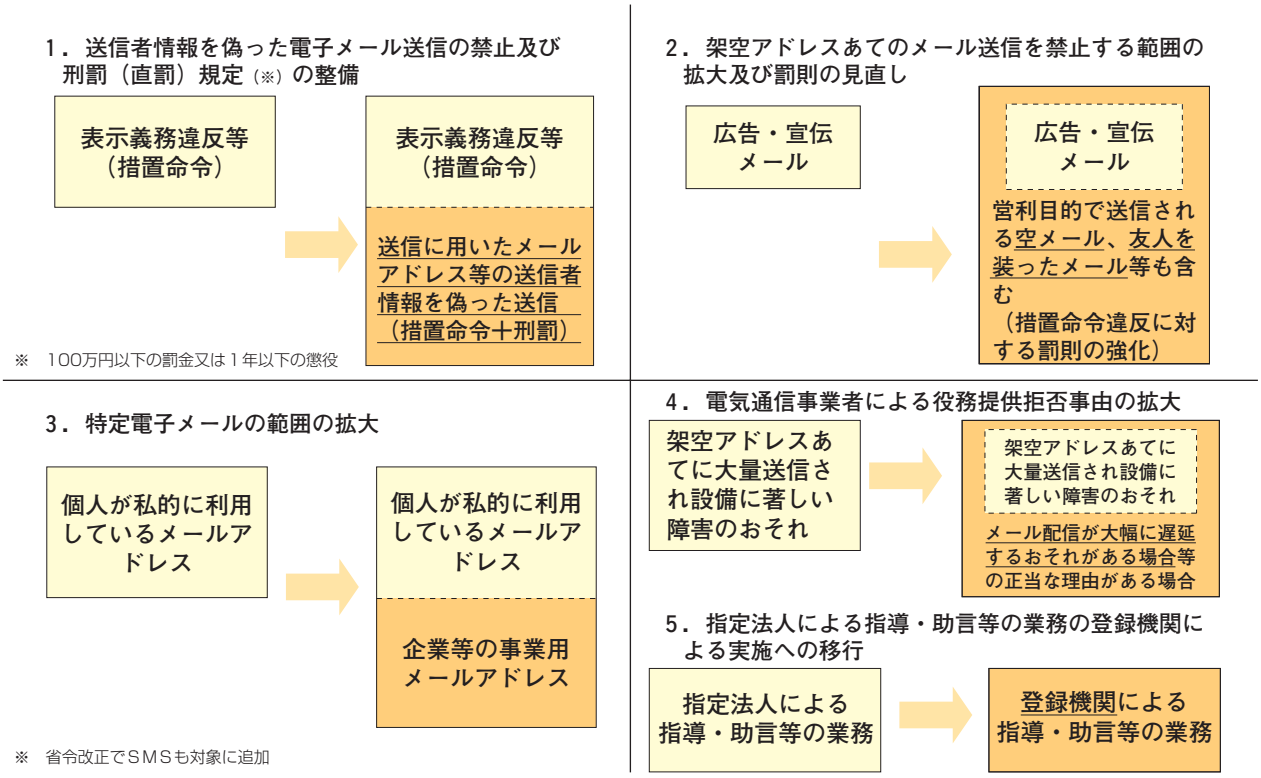
1 迷惑メール対策

携帯電話やパソコンに対し、受信者の同意を得ず一方的に送信される広告・宣伝目的の電子メール（いわゆる迷惑メール）について、総務省では、平成17年7月に取りまとめられた「迷惑メールへの対応の在り方に関する研究会」最終報告書に基づき、①政府による効果的な法執行、②電気通信事業者による自主規制、③技術的解決策、④利用者支援、⑤国際協調といった総合的な対策を推進している。

まず、政府による効果的な法執行については、平成17年11月1日に改正された「特定電子メールの送信の適正化等に関する法律」の着実な執行が挙げられる。同法は、平成13年頃迷惑メールが我が国において大きな社会問題となっていたことを受けて、議員立法により制定された。しかし、その後の送信行為の悪質化・巧妙化の進展等により、依然として迷惑メール問題が解決したとは言えない状況にあったことから、総務省は、「迷惑メールへの対応の在り方に関する研究会」の中間取りまとめを踏まえて作成した「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案」を平成17年3月に国会に提出、同法律は同年5月に成立、公布された。本改正により、自己又は他人の営業につき広告又は宣伝を行うための手段として送信者情報を偽って電子メールの送信をする行為の禁止及びその違反者に対する刑事罰、架空電子メールアドレスあての電子メール送信を禁止する範囲の拡大及び罰則の見直し、特定電子メールの範囲の拡大並びに電気通信事業者による電気通信役務の提供拒否事由の拡大等が行われた。

なお、上記の法改正に併せて、同法の対象に、

図表3-4-1 「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」の概要（平成17年5月13日成立、同年11月1日施行）



携帯電話同士で短い文字メッセージを電話番号により送受信する「ショートメッセージサービス」（SMS）を追加すること等を内容とする「特定電子メールの送信の適正化等に関する法律施行規則の一部を改正する省令」も制定され、改正法と同じく平成17年11月1日から施行された。

また、総務省及び経済産業省では、平成17年2月から、（財）データ通信協会及び（財）日本産業協会に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、当該電子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「迷惑メール追放支援プロジェクト」を推進している。

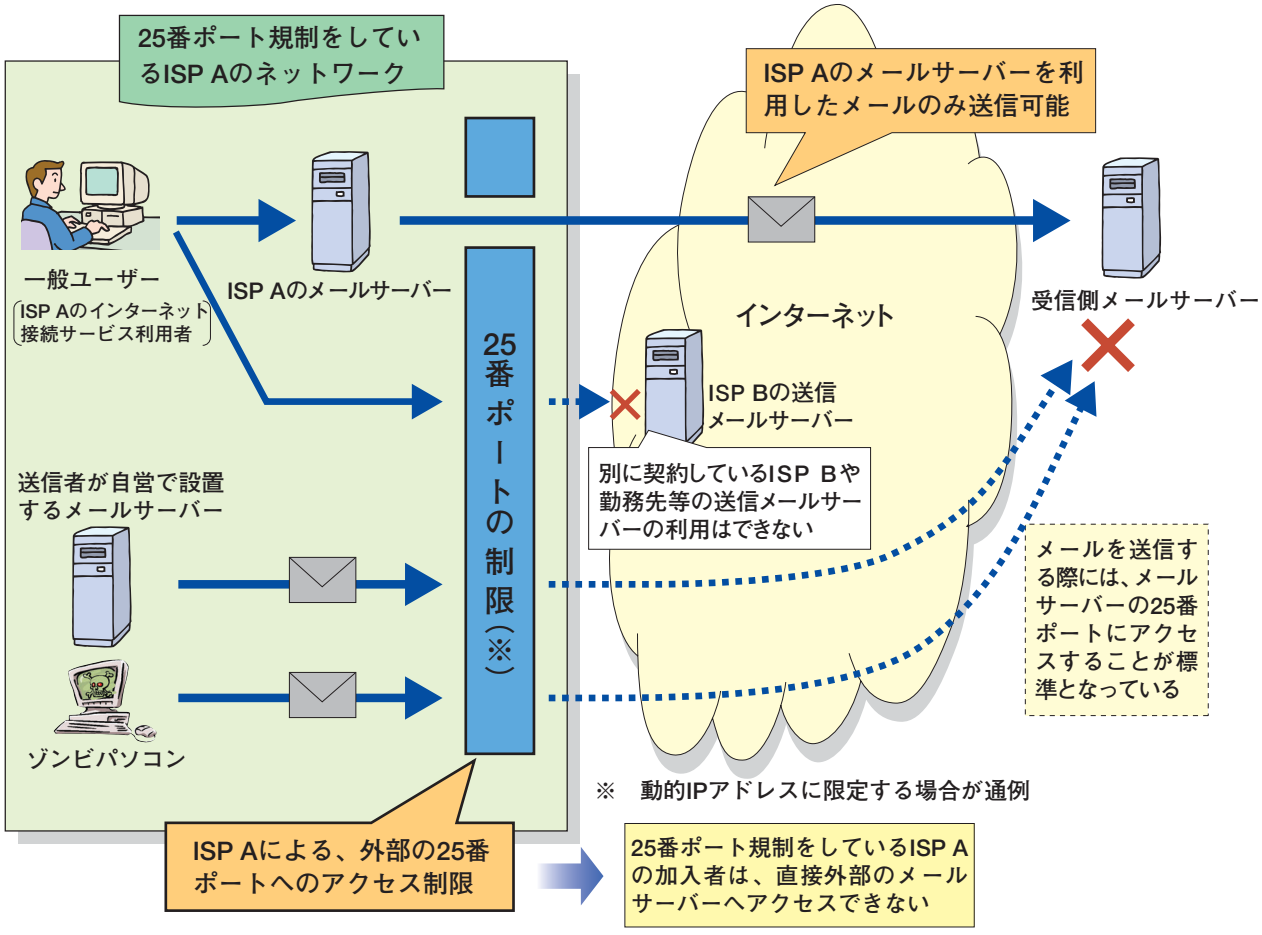
さらに、迷惑メールは発信元を偽るケースや自営で設置するメールサーバー等から送信されることが多いため、発信元の情報を確認する「送信ドメイン認証技術」や、動的IPアドレス[1]を割り当てられた自営で設置するメールサーバー等から直接外部に送信するメールを遮断する「25番ポートブロック」が有効であると考えられているが、総務省では、電気通信事業者の業界団体等と連携して、関係法令との整合性を確保しつつ、その導入促進策等に関する検討を進めている。

また、世界の中で、中国及び韓国が米国に次ぐ迷惑メール発信国となっている（Sophos社調査結果）こと等を踏まえ、総務省及び経済産業省は、平成17年4月、中国及び韓国を含むアジア太平洋地域の11機関との間で、「スパム対策の協力に関する多国間MOU（覚書）」を締結したが、今後、欧米諸国を含め、引き続き、国際連携を推進していくこととしている。

2 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個人情報等を不正に詐取する「フィッシング」については、電子メールやウェブサイトが主要な手段となっていることから、総務省では、インターネット接続サービスを提供するプロバイダ（ISP）とともに「フィッシング対策推進連絡会」を平成17年1月から定期的に開催し、情報の共有を図るとともに、その効果的な対策等に

図表3-4-2 25番ポートブロックのイメージ



（出典）総務省「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」

1 一定期間ごとに変更されるなど一つに固定されていないIPアドレス。通常のインターネット接続サービスは動的IPアドレスを割り振る形態となっている

ついて検討を進めている。

「フィッシング対策推進連絡会」は、同年8月に、こ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、公表した。

本取りまとめでは、プロバイダによるフィッシング対策の方向性について、①プロバイダ間の情報共有及びユーザーへの周知啓発スキームを、電気通信事業者4団体を軸としてスタート、②発信元を偽るケースが多いフィッシングメールへの対処としては、送信者（ドメイン）認証技術の採用が有効であり、業界全体の課題として取組を進めるべき、③自営設置サーバー等から直接外部に送信されるケースの多いフィッシングメールへの対処としては、「25番ポートブロック」が有効、④フィッシングサイトと考えられるサイトの削除・閉鎖に関する手続き等については、「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」での検討を踏まえつつ引き続き議論、としている。

総務省は、電気通信事業者団体、関係機関等とともに、上記方向性に基づき、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。

（3）振り込め詐欺等対策

振り込め詐欺等の犯罪に利用されることの多いプリペイド式携帯電話については、その匿名性を排除するため、これまで携帯電話事業者において販売（契約）時の本人確認が自主的に行われてきた。

これに加えて、総務省では、譲渡・転売等された場合の利用者（契約者）の把握について、携帯電話事業者等と共に新たな対策を検討し、平成17年4月から、携帯電話事業者は、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き契約者に対して契約者情報の届出義務を課し、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、当該契約者について利用停止措置を講じるなどの対策を実施している。

その結果、平成18年3月31日までに、携帯電話事業者は、稼動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。

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利用の防止に関する法律

携帯電話事業者による契約者の管理体制の整備の促進及び携帯音声通信役務の不正利用の防止を徹底するため、「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」が平成17年4月8日に成立し、4月15日に公布され、同年5月5日一部施行、平

図表3-4-3　携帯電話不正利用防止法の概要（平成18年4月1日全面施行）

目　的

携帯電話（PHSを含む。）の事業者に対して携帯電話の契約締結時及び譲渡時の本人確認を義務付けたり、携帯電話の不正な譲渡・貸与行為等を処罰することで、携帯電話の不正な利用を防止する。

契約時・譲渡時の本人確認

○携帯電話事業者や代理店は、契約締結時、携帯電話の譲渡時に、運転免許証の提示を受けるなどの方法により、契約者の氏名・住居・生年月日を確認しなければならない。

○契約者は氏名、住居及び生年月日を偽って申告してはならない。

警察からの通知に基づく確認

○警察署長が、犯罪に利用されていると判断した携帯電話について、携帯電話事業者が契約者の確認を行い、確認できないときは利用停止等ができる。

譲渡・貸与等の制限

○自己名義の携帯電話を携帯電話事業者に無断で譲渡してはならない。

○他人名義の携帯電話を譲渡したり、譲り受けてはならない。

○携帯電話のレンタル行為を業として行う者は、借りる人の氏名や連絡先を確認しなければならない。

成18年4月1日全面施行された。

同法は、携帯電話事業者に携帯電話の契約の締結時及び譲渡時の本人確認を義務付けること、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確認を求めることができること、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が定められている。

また、同法の全面施行に合わせて、「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施行規則」を全面改正し、平成17年12月26日に公布し、平成18年4月1日から全面施行し、同施行規則では、同法の対象とする携帯音声通信役務の定義、相手方等の本人特定事項の確認方法、本人確認記録の作成方法等を定めている。

2 情報セキュリティ及びプライバシー保護対策の推進

(1) 政府全体での情報セキュリティ対策

近年、高度情報通信ネットワーク社会が現実のものとなり、我が国の国民生活・社会経済活動において情報技術への依存度が深まっている。

こうした状況の下、昨今、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、行政機関の重要情報の流出や企業からの大量の個人情報の漏えい等が社会問題化してきており、情報技術を安全・安心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、我が国にとって喫緊かつ重要な課題になっている。

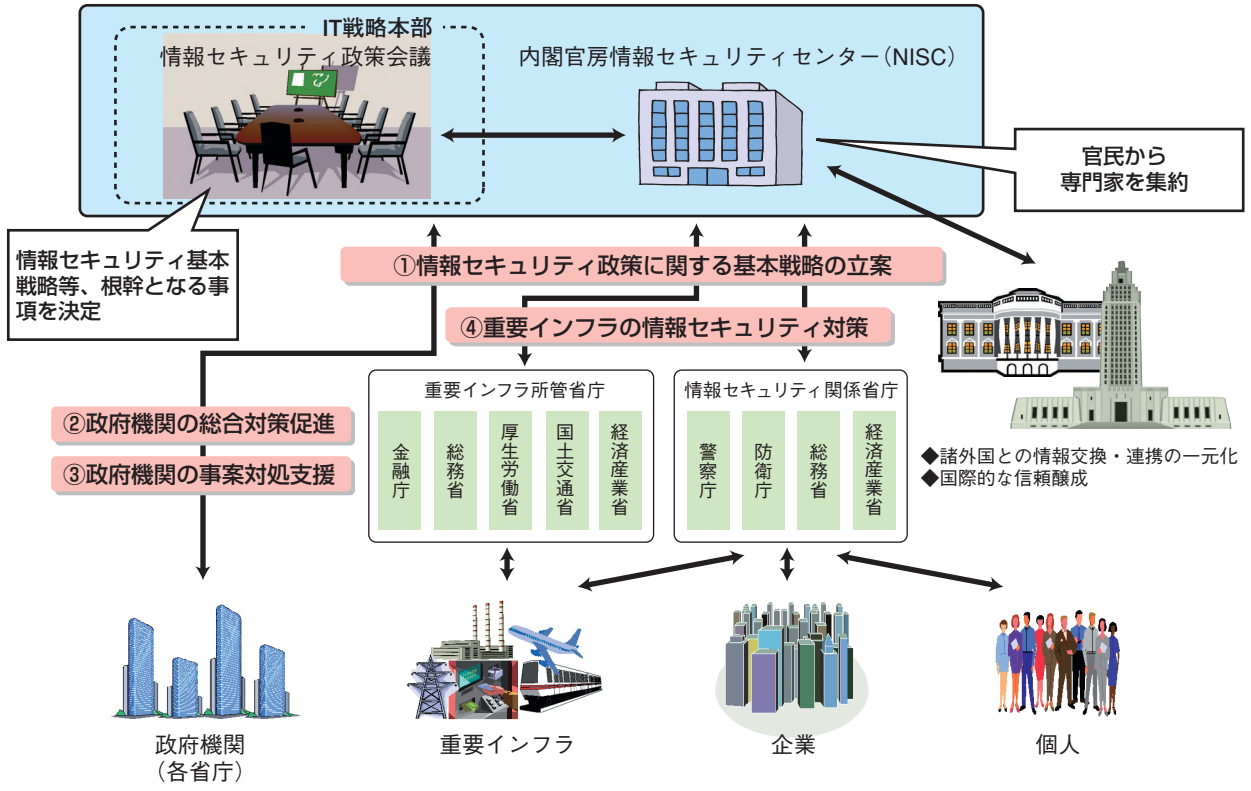
このため、政府は情報セキュリティ対策の中核機関として、2005年4月に内閣官房に「情報セキュリティセンター（NISC）」を、同年5月に高度情報通信ネットワーク社会推進戦略本部に「情報セキュリティ政策会議」（議長：内閣官房長官）を設置し、我が国全体としての情報セキュリティ対策を推進している。

このような流れの中で、2006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今後3年間（2006年度～2008年度）の中長期戦略として、「第1次情報セキュリティ基本計画」が決定された。

また、政府機関自身の情報セキュリティ対策については、2005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」等が、2005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（2005年12月版（全体版初版））」（以下「政府機関統一基準」という。）が情報セキュリティ政策会議において決定された。

さらに、重要インフラの情報セキュリティ対策について、2005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」が情報セキュリティ政策会議において決定された。

図表3-4-4 政府全体の情報セキュリティ推進体制

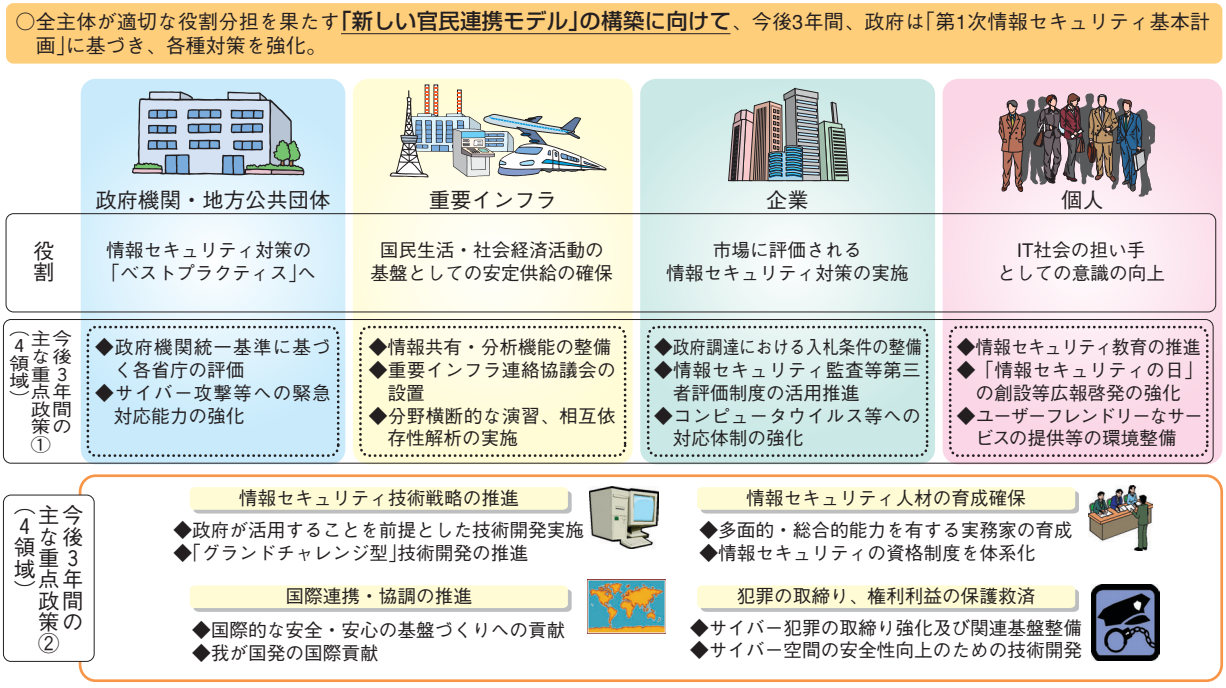


1 第1次情報セキュリティ基本計画

第1次情報セキュリティ基本計画では、
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

という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を提示している。

図表3-4-5 第1次情報セキュリティ基本計画ー今後3年間の重点政策ー



2 政府機関統一基準

政府機関の情報セキュリティ対策については、①情報セキュリティ水準の高い省庁と低い省庁の格差が大きい、②急激に変化するIT環境に対応した情報セキュリティ対策を実施する人材が全体的に不足しているなどの問題が指摘されている。また、昨今、政府機関へのサイバー攻撃が増加し、重要情報の流出事案が相次ぐなど、情報セキュリティ関連の事案が多発している状況にある。

こうした状況を受けて、政府機関全体の情報セキュリティ水準の向上を図るため、政府機関統一基準が策定され、これに基づき各省庁の情報セキュリティポリシーの整備が図られた。

内閣官房情報セキュリティセンターは、各省庁の対策状況を政府機関統一基準に基づき必要な範囲で検査し、評価を行い、これを基に情報セキュリティ政策会議が各省庁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。

3 重要インフラの情報セキュリティ対策に係る行動計画

重要インフラは、文字通り国民生活・社会経済活動の基盤であり、あらゆる脅威からその安定的供給を確保することが最優先の課題である。昨今の各重要インフラ分野におけるIT利用の飛躍的進展とITへの依存度の増大、各重要インフラ分野間での相互依存性の増大等を踏まえ、「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」（2005年9月情報セキュリティ政策会議決定）に基づき、本行動計画が策定された。

内閣官房情報セキュリティセンターは、本行動計画に基づき、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を重点政策として掲げ、人為的ミス、災害等への対策も含め、国民生活・社会経済活動の基盤としての安定的供給の確保を推進する。

(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、経済活動に大きな恩恵をもたらす一方、社会全体の情報通信システムへの依存度の高まりによって、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こともあり得ることになる。

このため、今後のICT社会の推進に当たっては、情報セキュリティの向上が不可欠であり、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、平成16年12月から開催している「次世代IPインフラ研究会セキュリティWG」における検討等を踏まえ、「ネットワーク」、「人」、「モノ」の三つの面から、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。以下、主な施策について述べる。

1 ネットワークの強化・信頼性の確保

「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。

(1) 乗っ取った多数のパソコン（ボットネット）を悪用した一斉攻撃の対策

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の集合体であり、悪意の者の命令に従い、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などの窃盗、等を行い、様々な情報セキュリティ上の問題を引き起こしている。

このため、総務省では、「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、ボットプログラムを削除するソフトウェアの開発、電気通信事業者を通じた一般ユーザーへの配布・適用等を行うこととしている。

(2) 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しており、各ネットワークでは、通信経路を確立するための経路情報を保持・交換している。一部の国内ISPでは、不正な経路情報が交換されることにより、経路ハイジャックが実際に発生しており、障害の検知・回復にかなりの時間を要しているのが実情である。このため、総務省では、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行うこととしている。

(3) トラヒック急増への対応

今後のトラヒックの急増に対応し得る情報通信インフラを強化するため、地域に閉じるトラヒックを当該地域で交換することを可能とする技術等の確立を目指し、次世代バックボーンに関する研究開発を平成17年度から推進している。

(4) 通信業界における情報セキュリティ対策に向けた取組

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、電気通信事業者等が中心となって、平成14年7月に「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）」が任意団体として発足（平成17年1月、（財）日本データ通信協会に編入）された。これにより、これまでの各々の電気通信事業者が自らのネットワークごとで対応する形態から、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可能な体制へと進化した。

(5) 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

ネットワークの強化・信頼性の確保に向け、上記の取組のほか、広域モニタリングシステム、IPトレースバック技術、高度ネットワーク認証基盤技術の研究開発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。

2 人的能力の向上

「人」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。

(1) サイバー攻撃対応演習

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ず、事業者間及び事業者と行政との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や緊急対応体制の強化が求められている。

このため、総務省では、平成18年度から電気通信事業者等を中心に、各重要インフラに跨る情報通信ネットワーク上で発生するサイバー攻撃等への緊急対応体制が実際に機能するかなどについて検証し、事業者間及び事業者との間の緊急対応体制を強化するとともに、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としている。

(2) 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

総務省では、インターネットの急速な普及を踏

まえ、情報通信システムの安全・信頼性対策に関する指標「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）の情報セキュリティ対策に関する項目の見直しを行い、安全・信頼性対策に関する理解の増進や電気通信事業者による同指針の活用の促進を図ってきた。

特に、自らの電気通信設備をユーザーの通信の用に供する電気通信事業者は、「通信の秘密」に属する情報をはじめとして多くのユーザー情報を取り扱っており、情報をより適切に管理することが求められることから、組織における情報セキュリティマネジメントを確立することが重要である。

このため、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）を基本としつつ、電気通信事業者が守るべき法令上の要求事項等を踏まえ、特に電気通信事業者において考慮することが望ましい事項を「電気通信事業における情報セキュリティマネジメント指針」として取りまとめている。

(3) 情報通信セキュリティ人材育成センター開設支援

情報通信セキュリティ侵害事案に対する実践的な対処方法を習得するための研修設備を整備する第三セクターや公益法人に対し、整備に必要な初期費用を補助することにより、情報通信セキュリティ人材の育成を促進している。

(4) 個人向け教育・啓発活動強化

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」を平成15年3月より開設しており、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。

また、一般ユーザーへの啓発として、総務省、文部科学省及び関係公益法人が協力し、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のキャラバンである「e-ネットキャラバン」を実施している。平成17年度は、関東及び東海地域（71講座を実施）で試行し、平成18年度からは、全国規模で3年間にわたり本格実施することとしている。

さらに、インターネット、携帯電話等のICTメディアの健全な利用の促進を図るため、総務省では、子供の利用実態等について調査・分析するとともに、これらICTメディアの利用に当たって必要とされるICTメディアリテラシーに係る指導マニュアルや教材の開発等、「ユビキタスネット時代における新たなICTメディアリテラシー育成手法の調査・開発」に取り組んでいる。

3 ネットワークに繋がるモノの多様化への対応

「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、電子政府で利用するOSに関する評価尺度の策定に向けた取組等を実施している。

(1) 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

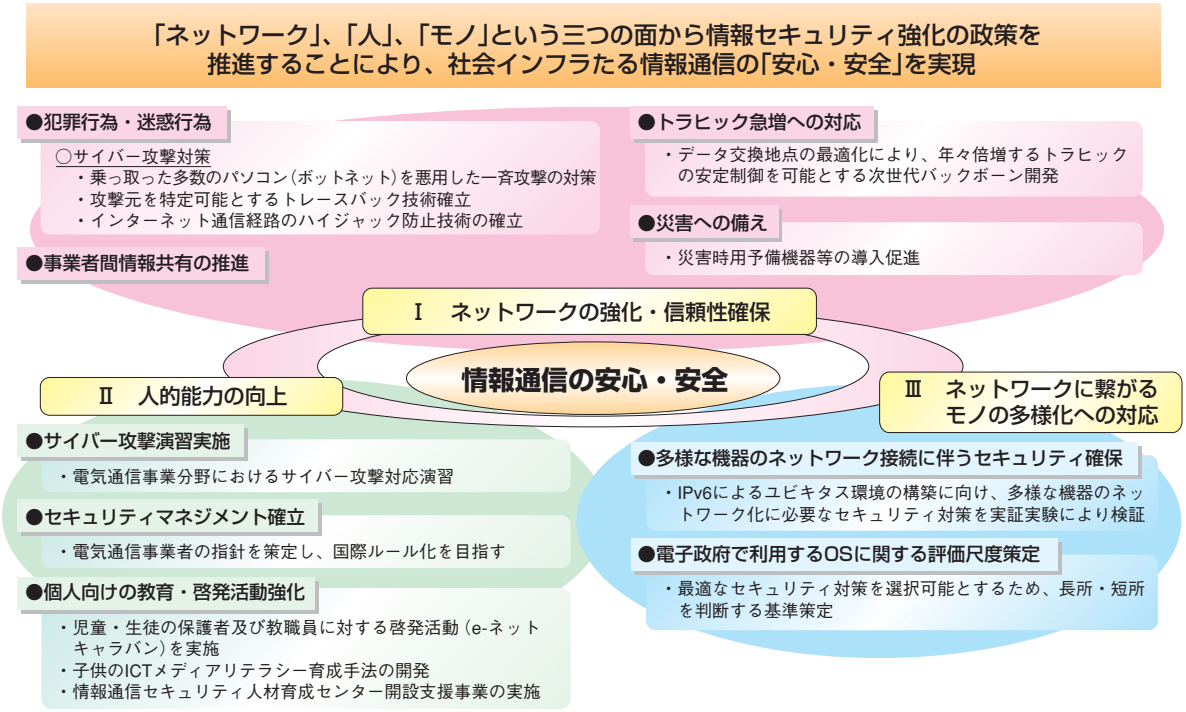
身の回りのあらゆるモノが通信機能を持つ、いわゆる“ユビキタス環境”の構築に向けて、膨大なアドレス空間を持ち、高いセキュリティを実現するIPv6インターネット網の利用が必要である。

さらに、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。このため、総務省においては、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。

(2) 電子政府で利用するOSに関する評価尺度の策定

電子政府の情報システムで利用するOSについて、そのセキュリティ品質に関する評価尺度の検討とその評価尺度の妥当性検証を実施することにより、実際のシステム調達に活用可能な評価尺度の確立を目指した検討を行っている。

図表3-4-6 情報通信の安心・安全確保に向けた取組の概要



（3）電気通信サービスにおける重要通信の確保

1 重要通信の確保

電気通信分野では、携帯電話やIP電話等の普及に伴う通信サービスの発展や利用形態の多様化等に応じ、国、電気通信事業者及び産業界が連携して災害等の非常時に備えて重要通信を確保するための効果的な仕組みを、我が国全体として整備する必要性が高まっている。こうした事情を踏まえて、総務省では、平成14年4月から「電気通信事業における重要通信確保の在り方に関する研究会」を開催し、平成15年7月に報告書を取りまとめた。

平成16年12月には、同報告書の提言等を踏まえ、その後の携帯電話事業者等の主な取組状況について同年1月に続き公表した。また、新潟県中越地震における電気通信事業者の設備やサービスへの被害及びその復旧等の対応について、電気通信事業者が取り組むべき今後の対応策を、主要電気通信事業者等関係者からなる「災害時の電気通信サービス確保に関する連絡会」の場を活用して検討し、その結果を取りまとめた。

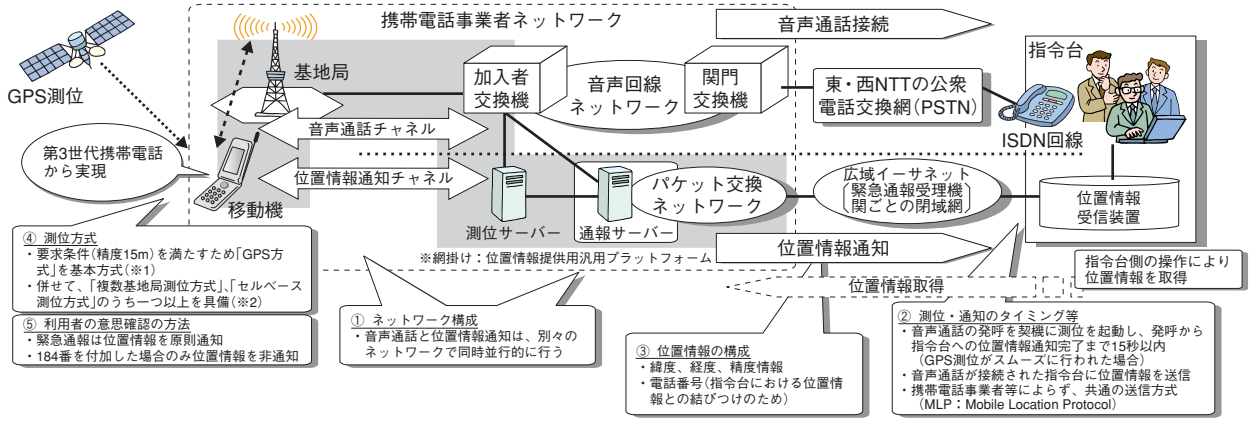
同取りまとめでは、災害時の電気通信サービス確保における技術面での対応策として、障害が発生した場合の携帯電話基地局への駆け付け時間を考慮した非常用電源の容量の再点検や保持時間の延長等が、また、体制・制度面での対応策として、道路管理者及びライフライン関係機関（電力事業者等）との情報共有・連絡体制の確立等が、今後の対応策として挙げられた。

2 電気通信事業における緊急通報機能等の高度化方策

携帯電話やIP電話の普及に伴い、これらの電話からの緊急通報が急増していることに対応するために、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、平成16年6月に、「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」について一部答申を受け（図表3-4-7）、また、平成17年3月に、「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」について答申を受けた。

同答申を踏まえ、平成18年1月に、緊急通報を取り扱う場合には、携帯電話においては、GPS等を利用した位置情報（緯経度等）を、IP電話（固定するもの）においては、住所情報等を緊急通報受理機関へ通知すること等について省令、告示の改正を行い、平成19年4月からの導入に向けた取組を進めている。

図表3-4-7 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



※1 GPS測位方式に限定せず、同等の測位精度等を有する他の衛星測位方式も想定
※2 複数基地局測位方式：3基以上の基地局からの同期信号をもとに位置を算出
セルベース測位方式：移動機が接続している基地局のセルの情報から位置を算出

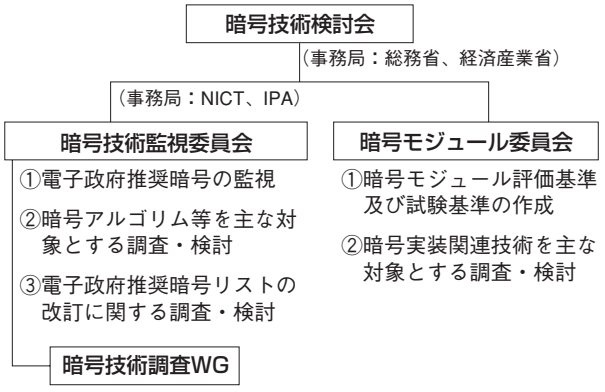
(4) 暗号技術の安全性評価と高度化の推進

「暗号評価プロジェクト（CRYPTREC）」

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、平成13年度から開始された総務省及び経済産業省が共同で開催する「暗号技術検討会」と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する「暗号技術評価委員会」の両研究会による暗号評価プロジェクトCRYPTREC（Cryptography Research and Evaluation Committees）において、平成15年2月に暗号技術を公募の上、客観的に評価し、安全性及び実装性に優れた暗号技術をリスト化し、「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）が決定された。これを踏まえ、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している。

その後、「暗号技術評価委員会」に代わり、図表3-4-8のとおり、「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。

図表3-4-8 CRYPTRECの体制図



NICT：独立行政法人情報通信研究機構
IPA：独立行政法人情報処理推進機構

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、基準の作成等を行う。また、電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進める。

(5) 情報通信分野における個人情報の保護

情報通信分野においては、その業務上、通信の秘密その他のプライバシーに関連する大量の情報を取り扱う機会が多いことから、従来からその厳正な扱いが求められてきたが、電子化された情報がネットワークを介して迅速に流通する高度情報通信ネットワーク社会においては、個人情報保護の必要性が一層高まってきている。

すべての分野を包括的に対象とした個人情報の保護については、平成15年5月、「個人情報の保護に関する法律」が公布され、平成17年4月から全面施行されている。

総務省でも同法の施行に伴い、個人情報取扱事業者の個人情報の取扱いに関する苦情の処理や個人情報の適切な取扱いの確保に関して必要な業務を行う認定個人情報保護団体を数団体認定している。

また、情報通信分野における個人情報の保護のための格別の措置については、「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」及び「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」における検討を踏まえ、総務省は、平成16年8月、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3年に策定し、平成10年に改訂した「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」を再び改訂（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み）するとともに、「放送受信者等の個人情報の保護に関する指針」を制定した。これらのガイドラインも、平成17年4月から適用されている。

なお、情報通信分野における個人情報の保護のための法制上の措置についても、上記懇談会等において検討が行われ、それぞれ平成16年12月及び平成17年2月に公表された取りまとめにおいて、分野横断的に個人情報を漏えいする行為等を処罰できることとするための法制度の整備の検討を今後進めていくことが適当である旨提言されている。

「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」については、上記懇談会での議論を踏まえ、平成17年10月に「特定電子メールの送信の適正化等に関する法律」に違反する迷惑メール等の大量送信行為により利用停止措置を受けた加入者情報を、プライバシー及び個人情報の保護に配慮しつつ、電気通信事業者間で交換できる規定を追加するなどの改訂が行われた。

3 電子データの信頼性確保に資する取組

1 電子署名・認証の普及促進

(1) 電子署名及び認証業務に関する法律の施行

電子署名の円滑な利用環境を確保することにより、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一層の促進を図るため、平成13年4月に「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）が施行された。同法では、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とともに、②特定認証業務（省令で定める基準に適合する電子署名について行われる認証業務）に関し、業務に用いる設備や利用者の真偽の確認方法等の業務の実施方法が一定の水準を満たすものについての国による任意的認定制度を導入している。平成17年度末現在、19件の特定認証業務が認定を受けている。

また、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とともに、国境を越えた電子商取引を促進するため、諸外国との国際協調にも積極的に取り組んでいる。

(2) 高度ネットワーク認証基盤に関する研究開発

誰もが電子証明書を利用した厳格な認証機能を手軽に利用することが可能となり、ネットワークサービスを安心して提供・利用できるようにするため、総務省では、高度ネットワーク認証基盤に関する研究開発を平成16年度から実施している。従来の電子証明書を利用した通信では、電子証明書を受け取った側が自らその検証を行う必要があるが、本研究開発では、電子証明書の検証を行う機能をネットワーク自体に具備させることにより、誰もが簡便に利用できる高度な本人確認機能を有するネットワーク基盤の構築を目指している。また、民間における取組も活発になっており、平成15年12月に安心・安全インターネット推進協議会が設立された[2]。

2 タイムビジネスの利用促進

近年、電子商取引等の様々な分野において流通し又は保存される電子データに対して、一層の信頼を与えるため、時刻配信（ネット上で正確な時刻情報を配信）と時刻認証（電子データに付与し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）に関する業務であるタイムビジネスの重要性がますます高まってきている（図表3-4-9）。

総務省では、民間事業者が行う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」を平成16年11月に策定・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。

また、同指針を受け、(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与えることで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月に開始した。同制度に基づき、平成17年度末現在、3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ところであり、今後、タイムビジネスの利用促進が期待される。

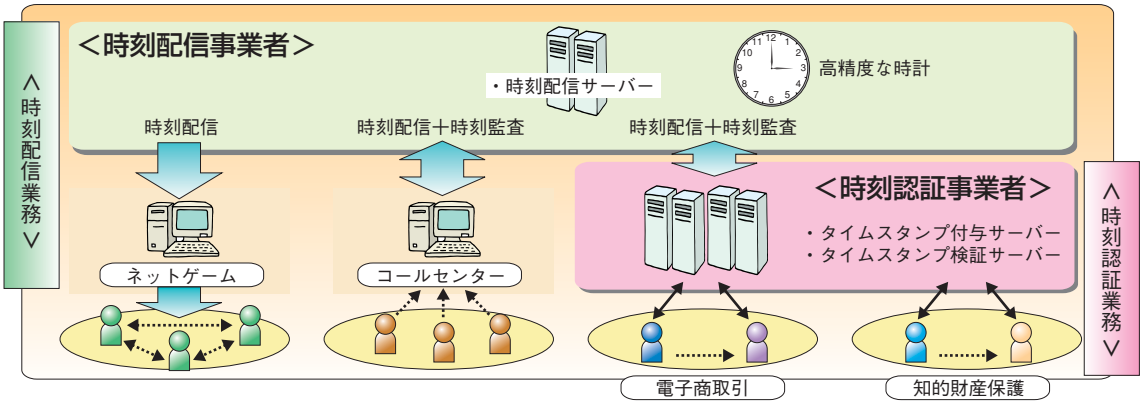
2 安心・安全インターネット推進協議会（http://www.scat.or.jp/stnf/）

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

平成17年4月に、民間における文書・帳簿の電子的な保存を、その内容・性格に応じた真実性・可視性等を確保しつつ、原則として容認する法律として、「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」及び「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の施行に伴う関係法律の整備等に関する法律」（以下e-文書法という。）が施行された。

e-文書法の成立により可能となった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係る電子保存の場合には、一定の要件を満たす措置（電子データに対する電子署名とタイムスタンプの付与）を行うことが必要となる。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によって認定された特定認証業務で発行されたものに、タイムスタンプは（財）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に限定され、信頼される電子署名やタイムスタンプの付与が求められている。

図表3-4-9 タイムビジネスのイメージ



4 電波利用環境の整備

（1）電波の与える影響からの人体の防護等

携帯電話をはじめとする電波利用の急速な普及・高度化に伴い、無線設備から発射される電波が人体に好ましくない影響を及ぼすのではないかという懸念や、心臓ペースメーカー等の医用機器に誤動作を引き起こす可能性が提起されている。

総務省では、こうした懸念を解消し、安心して安全に電波を利用できる環境を整備・維持するため、適切な基準の策定、継続的な研究等を実施している。

1 電波の人体に対する影響に関する基準の策定及び研究の推進

我が国では、旧電気通信技術審議会において「電波防護指針」を策定し、電波が人体に好ましくない影響を及ぼさない安全な状況であるか否かを判断する際の基本的な考え方や、それに基づく基準値等を示すとともに、この指針に基づく規制を導入することにより、安心して安全に電波を利用できる環境を整備している。

また、電波の人体への影響を科学的に解明するため、平成9年度から医学・工学の研究者等により構成される生体電磁環境研究推進委員会を開催している。同委員会では、世界保健機関（WHO）における国際電磁界プロジェクトと協調しながら実施した研究の成果に基づき、平成13年1月、「現時点では電波防護指針値を超えない強さの電波により、非熱効果を含めて健康に悪影響を及ぼすという確固たる証拠は認められない」こと等を内容とする中間報告を発表した。また、平成15年10月に「長期にわたる携帯電話の使用が脳腫瘍の発生に及ぼす影響は認められない」こと、同年12月に「携帯電話の電波が脳微小循環動態に及ぼす影響は認められない」こと、平成17年12月に「携帯電話の電波による脳内でのメラトニン合成への影響は認められない」ことを発表するなどし、現在は、携帯電話端末の使用と脳腫瘍との関係についての疫学調査、細胞内の遺伝子への影響調査等を実施している。

総務省では、今後も電波の人体安全性に関する研究等を継続し、我が国の電波防護のための基準の根拠となる科学的データの信頼性向上を図るとともに、その成果を公表することにより、安心して安全に電波を利用できる環境の整備を推進して

いくこととしている。

2 電波の医用機器等に与える影響の防止

平成9年3月、不要電波問題対策協議会（現電波環境協議会）において「医用電気機器への電波の影響を防止するための携帯電話端末等の使用に関する指針」が策定された。これを受けて、総務省（旧郵政省）では指針の内容を厚生労働省（旧厚生省）及び国土交通省（旧運輸省）へ通知するとともに、その効果的な活用について要請した。

その後、第3世代携帯電話等の新しい方式の携帯電話サービスの開始をはじめとする電波利用の拡大、心臓ペースメーカーのような医用機器等の妨害電波排除能力の向上等、電波利用をめぐる状況が変化してきている。

このため、総務省では、電波が医用機器等に及ぼす影響に関する詳細な調査を行い、電波を発射する側と医用機器等の影響を受ける側が安心して共存していける環境の確保を図っていくこととしている。具体的には、平成13年度までに、新方式の携帯電話端末等が植込み型心臓ペースメーカー等や病院内で使用される医用機器に及ぼす影響について調査を行い、平成9年の指針が妥当であることを確認したほか、平成16年度までに、新方式の携帯電話端末、ワイヤレスカードシステム、電子商品監視機器、無線LAN機器及びRFID機器から発射される電波が植込み型心臓ペースメーカー等に及ぼす影響について調査を行い、これらの結果を基に、平成17年8月、「各種電波利用機器の電波が植込み型医用機器へ及ぼす影響を防止するための指針」[3]を取りまとめた。さらに、平成17年度には、新たに実用化された携帯電話端末について上記同様の調査を行った。

(2) 不要電波対策

1 無線妨害波に関する規格の策定

電波利用の拡大、各種電気・電子機器等の普及に伴い、無線利用が各種機器・設備から電磁的な妨害を受けることが大きな問題となっている。

不要電波対策については、国際的には、IEC（国際電気標準会議：International Electrotechnical Commission）の特別委員会として、様々な機器・設備から発生する無線妨害波に関する許容値と測定法について検討し、国際規格を策定することを目的に、CISPR（国際無線障害特別委員会：Comité international Spécial des Perturbations Radioélectriques）が設置されている。

総務省では、情報通信審議会の中にCISPR委員会を設置し、CISPRにおける国際規格策定に寄与しているほか、CISPR国際規格との整合性を図りながら国内規格を策定している。平成17年度は、CISPR15「電気照明及び類似機器の無線妨害波特性の許容値及び測定法」について、150kHz未満の周波数における許容値及び測定法を追加する国内規格を策定した。

2 高速電力線搬送通信に関する検討

電力線搬送通信は、既存の電力線を使用することにより容易にネットワークを構築し、通信を行うことができるものであるが、無線利用への影響を考慮し、現在のところ10～450kHzの周波数を使用することが可能とされている。近年、この電力線搬送通信について、伝送可能な情報量を増大させるため、使用可能な周波数を拡大（2～30MHzを追加）することが要望されている。

使用可能な周波数の拡大により高速通信を可能とした電力線搬送通信については、漏えいする電波が無線利用に影響を及ぼすことが懸念されることから、これまで漏えい電波低減技術の開発が行われてきており、平成16年3月からは屋内電力線の使用を中心とした実験によるデータ取得も行われている。

このような状況を受け、総務省では、平成17年1月から「高速電力線搬送通信に関する研究会」を開催し、高速電力線搬送通信と無線利用との共存可能性・共存条件等について検討を行い、平成17年12月に報告書を取りまとめた。また、本報告書を踏まえ、平成18年1月から情報通信審議会において、「高速電力線搬送通信設備に係る許容値及び測定法」について審議が行われている。

(3) 適切な電波の監視・監理

1 正しい無線局運用の徹底

(1) 重要無線通信妨害への対応

電波利用の拡大とともに、電波の不適正な利用も増大し、電波利用における障害が多発している。このうち、総務省は人命や財産の保護、治安の維持、電気通信、気象、放送及び電気鉄道のための無線通信においては重要無線通信と位置付け、不法無線局等により電波障害が発生したときにはこれを排除するため、直ちに不法無線局の探査等を行っている。

3 「各種電波利用機器の電波が植込み型医用機器へ及ぼす影響を防止するための指針」（http://www.soumu.go.jp/s-news/2005/pdf/050811_2_1.pdf）

また、不法無線局の探査等を効果的に行うため、平成5年度から電波監視システム（DEURAS：Detect Unlicensed Radio Stations）の整備を進め、平成17年度末において、遠隔方位測定設備センサー341局、短波帯電波監視施設センサー5局及び宇宙電波監視施設1局を整備し、電波監視活動を強化するとともに、捜査機関との不法無線局の共同取締りを実施している。

平成17年度の電波障害に対する混信・妨害申告の総件数は2,666件であり、このうち重要無線通信に対するものは672件となっている。

なお、愛知県での「愛・地球博」の開催期間中や米国、ロシア大統領来日期間中等においては、重要無線通信の妨害に備えて電波監視体制の強化を行っている。

(2) 不法・違法無線局への対応

電波利用環境の維持に向けて、無線局の免許が必要でありながら免許を取得しないで開設、運用している不法無線局に対しては、これを探査し、告発等必要な措置を講じている。平成17年度の措置総数は4,642件であり、このうち告発は521件、行政指導は4,121件となっている。

また、電波法令に基づく合法な無線局に対しては、発射する電波の質や無線局の運用が電波法令どおりであることを監査し、違法無線局に対しては是正措置等を講じている。なお、平成17年度における監査総局数は438,461局であり、このうち違反局数は13,667局となっている。

(3) 電波利用環境保護のための周知・啓発活動

不法無線局等の電波利用のルールに違反する行為の未然防止を図るため、総務省は6月1日から10日までの間を「電波利用保護旬間」と位置付け、電波利用環境保護のための周知・啓発活動を強化している。

また、違法性のある無線機がインターネットオークション等で販売されるケースが増加していることから、平成17年度からインターネットバナー広告等を活用し、「技術基準適合マーク（〒）がない無線機は要注意！」等の周知広告を実施している。