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

(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

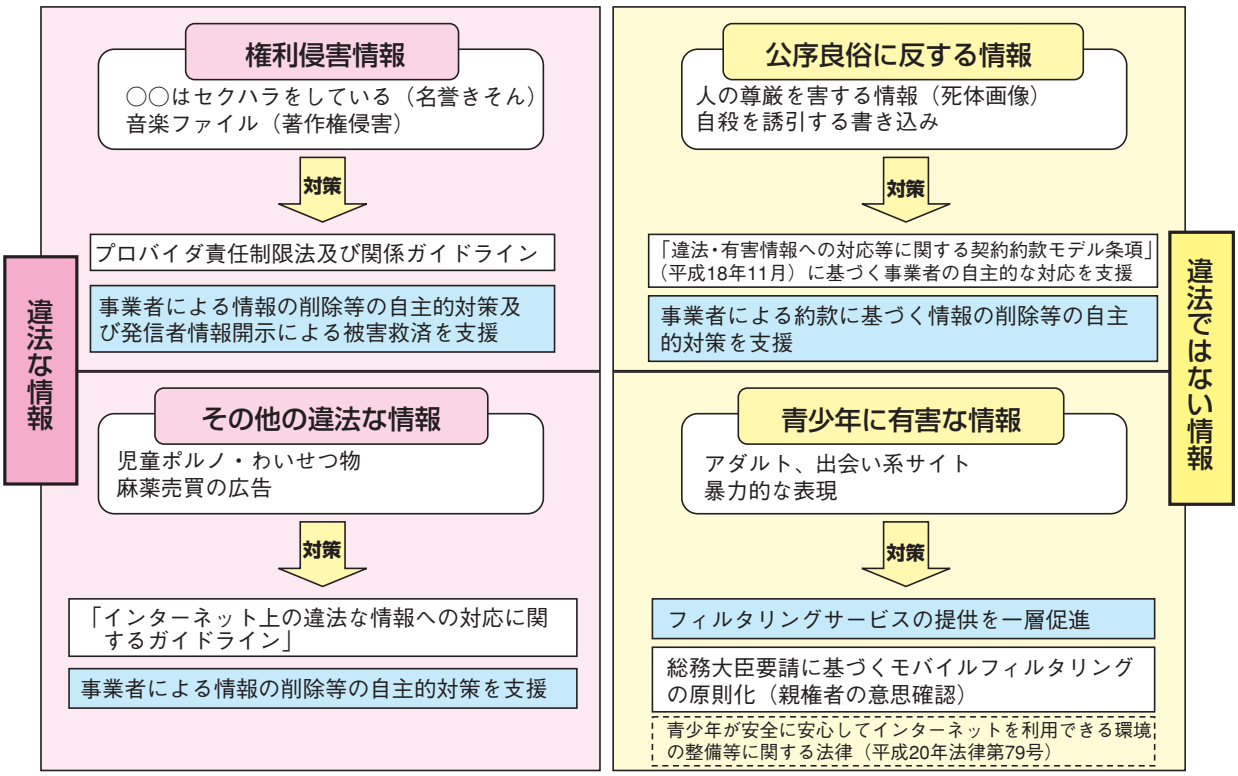
我が国におけるインターネットの普及はめざましく、国民の社会・文化・経済活動等あらゆる活動の基盤（社会インフラ）として利用され、国民生活に必要不可欠な存在となっている。一方で、急速なインターネットの普及は、違法・有害情報の流通等、負の側面も拡大させている。

総務省では、これらの問題に対処することとして、平成17年8月から18年8月まで「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」[1]を開催し、主に民間事業者の自主的対応を中心として具体的な施策について提言してきたところである。しかしながら、その後も、主に携帯電話からの出会い系サイトの利用を通じて青少年が犯罪に巻き込まれる事件や、いわゆる「学校裏サイト」におけるネットいじめ等の問題が発生し、効果的なインターネット上の違法・有害情報対策の立遅れや法規制の導入も含めた対応策の強化の必要性を指摘する声が高まった。

こうした声を受け、総務省では、平成19年11月から、「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」[2]を開催し、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の措置の支援、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を行い、21年1月に最終取りまとめを公表した（図表5-3-1-1）。

また、インターネット上の違法・有害情報対策に関する包括的な政策パッケージとして、平成21年1月に「安心ネットづくり」促進プログラムを策定した。

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



1 参考：「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～）」：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/internet_ihoyugai/index.html
2 参考：「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～）」：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/internet_illegal/index.html

イ　「青少年インターネット環境整備法」の成立

第169回国会において、議員立法により、「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）が成立し、平成21年4月1日より施行された。

同法は、インターネット上の違法・有害情報対策のうち、青少年（18歳未満）を有害情報から保護することに目的を絞り、インターネットの利用環境整備の在り方について、今後の取組の方向性を明確化したものである。基本理念として、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（国・地方公共団体は支援）を掲げており、民間事業者の自主的な取組やリテラシー教育の重要性を強調している。また、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ている。

ウ　フィルタリングの普及促進

近年、青少年がいわゆる出会い系サイト等のインターネット上の有害サイトにアクセスし、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、利用者の意思によって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の一つであると考えられる。

総務省では、従来から、携帯電話事業者等に対し、携帯電話フィルタリングの導入促進及び改善等に関して要請を行うなどなどさまざまな取組を実施している。また、業界団体も、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」を策定するなど、普及啓発活動に努めてきたところである。

前出の「青少年インターネット環境整備法」により、21年4月1日から、携帯電話事業者は青少年（18歳未満）がインターネットへの接続に用いる携帯電話等について、原則フィルタリングを設定した上で提供すること、プロバイダは利用者からの求めに応じてフィルタリングを提供すること、パソコン等のインターネットと接続する機能を有する機器を製造する事業者はフィルタリングの利用を容易にする措置を講じた上で販売すること等が義務づけられるとともに、保護者はその保護する青少年によるインターネットの利用を適切に管理する責務があるとされることとなった。総務省、内閣府、内閣官房IT担当室、警察庁、文部科学省及び経済産業省は、平成21年2月、青少年が安全に安心してインターネットを利用できるようにするため、連名により、都道府県、教育委員会、都道府県警察及び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推進するため、学校関係者や保護者をはじめ住民に対する啓発活動に取り組むよう依頼したところである[3]。

また、平成21年3月には、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の連名により、青少年におけるフィルタリングの普及促進その他のインターネットの適切な利用を推進するため、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した[4]。

総務省では、今後も引き続き業界や関係省庁等と連携し、青少年が安心してインターネットを利用できる環境の整備に取り組んでいくこととしている。

エ　「安心ネットづくり」促進プログラムの策定

第169回国会において、「青少年インターネット環境整備法」及び「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」（通称：特定電子メール法）が成立したことを受け、総務省は同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として、「安心ネットづくり」促進プログラムを策定した[5]（図表5-3-1-2）。

本プログラムは、「青少年インターネット環境整備法」第3条の基本理念と方向性を共有し、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の3つを柱とした総合的な政策パッケージである。

3 参考：「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」：http://www.soumu.go.jp/menu_news/s-news/090210_4.html
4 参考：「フィルタリング普及キャンペーン」の実施：http://www.soumu.go.jp/menu_news/s-news/090304_2.html
5 参考：安心ネットづくり促進プログラムの公表：http://www.soumu.go.jp/menu_news/s-news/2009/090116_2.html

オ　プロバイダ責任制限法関係ガイドラインの策定・改定

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、「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）が施行された。本法律においては、

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

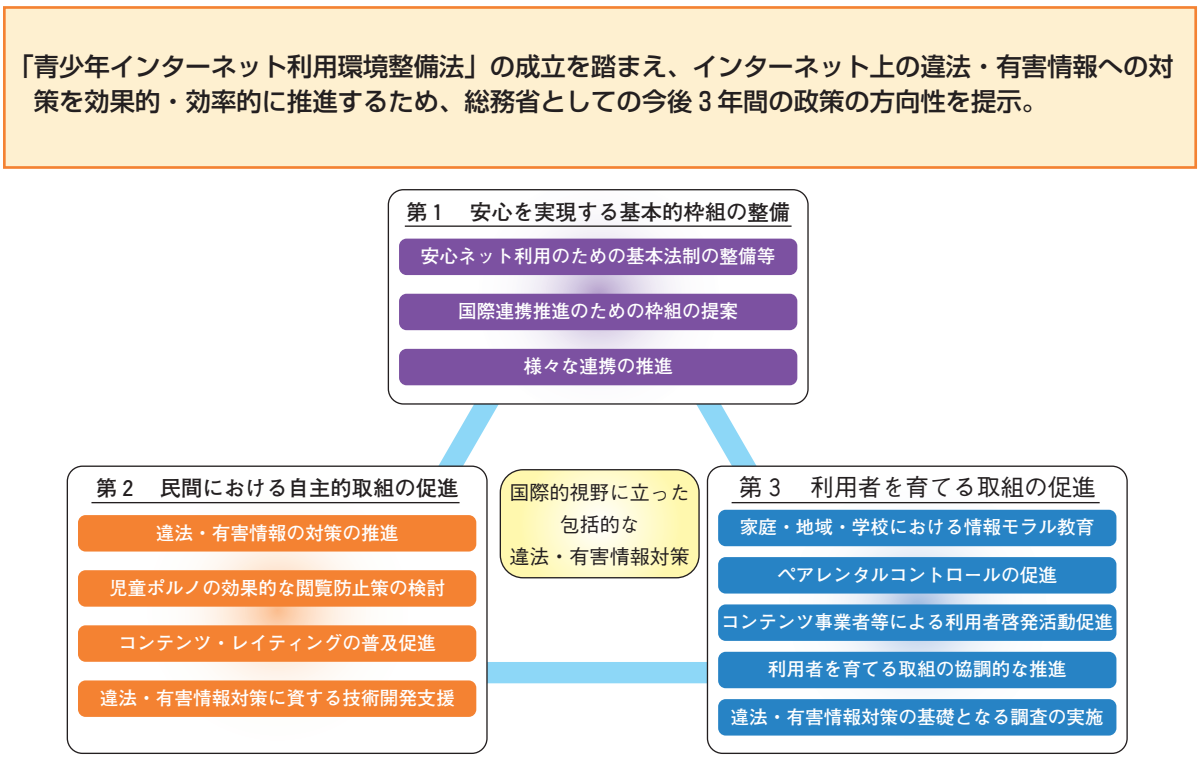
を規定しており、これを受けて、総務省では、同法が適切に運用されるよう、業界団体や権利者団体等から構成される「プロバイダ責任制限法ガイドライン等検討協議会」[6]に対する支援や周知を行っている。同検討協議会では、セミナー等を開催するほか、「発信者情報開示関係ガイドライン」「著作権関係ガイドライン」「名誉毀損・プライバシー関係ガイドライン」「商標権関係ガイドライン」を策定・公表するとともに、定期的に意見交換を行っている。

カ　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

「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、総務省は、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」及び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。その後、闇サイトや硫化水素による自殺方法の流通といった新たな問題の発生を受け、平成20年12月に上記ガイドライン及びモデル条項の改訂が行われている。また、平成20年1月には、プロバイダ等の事業者からの違法・有害情報に関する相談・問合せ等を受け付ける「違法・有害情報事業者相談センター」[7]をテレコムサービス協会内に設置した。

図表5-3-1-2　安心ネットづくり促進プログラム



6 参考：プロバイダ責任制限法検討協議会（（社）テレコムサービス協会）：http://www.telesa.or.jp/consortium/provider/index.html
7 参考：違法・有害情報事業者相談センター：http://www.isplaw-c.jp/

(2) 迷惑メール対策・フィッシング対策

ア　迷惑メール対策

迷惑メールについては、これまでも「特定電子メール法」や、電気通信事業者による自主的な取組をはじめ、様々な対策を行ってきた。しかしながら、迷惑メールの送信手法が巧妙化・悪質化し、海外から送信される迷惑メールが増大するなど新たな問題が顕在化している。

そこで、総務省は、平成19年7月から「迷惑メールへの対応の在り方に関する研究会」を開催し、迷惑メールについて総合的な検討を行った。同研究会は、平成19年12月に中間取りまとめを、20年8月に最終取りまとめを作成し、公表した[8]。

中間取りまとめにおいては、「特定電子メール法」の改正についての提言が行われ、これを踏まえ、迷惑メールに対するオプトイン方式による規制の導入等を盛り込んだ「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」が平成20年6月に成立し、同年12月1日より施行された（図表5-3-1-3）。

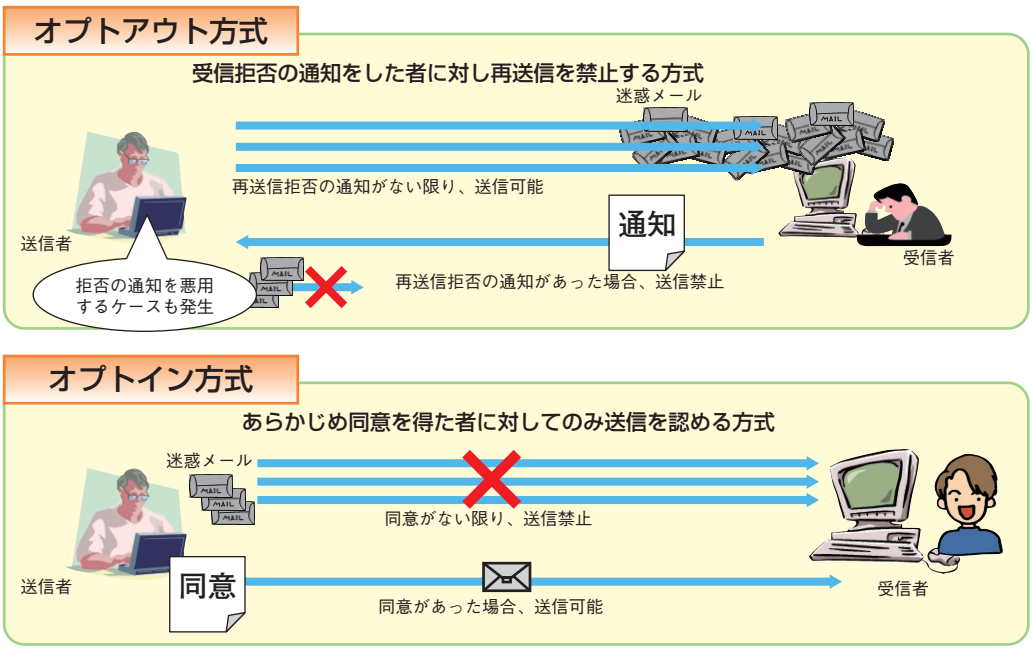
また、最終取りまとめにおいては、①総合的な迷惑メール対策の枠組、②オプトイン方式による法規制の運用と執行の在り方、③技術的対策の在り方、④電気通信事業者による自主的な措置の在り方、⑤利用者への周知啓発と相談体制の充実の在り方、⑥国際連携の推進の在り方、⑦総合的な迷惑メール対策推進のための体制について提言されており、総務省では、最終取りまとめを踏まえ、平成20年11月に「特定電子メールの送信等に関するガイドライン」を作成し、公表した[9]。当ガイドラインにおいては、改正された法律及び関係省令の解釈、特定電子メールの送信にあたって推奨される事項等がまとめられている。

イ　フィッシング対策

「フィッシング」は、金融機関等信用のある者からの電子メールを装い、電子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住所、氏名、銀行口座番号、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ものであり、電子メールの送信がフィッシングサイトへの誘引の主要な手段の一つとなっている。

「迷惑メールへの対応の在り方に関する研究会」においては、フィッシングメール対策を含む迷惑メール対策全般についての検討を行っている。また、改正特定電子メール法においては、送信者のメールアドレス等送信者情報を偽った電子メールの送信がなされた場合に電気通信事業者がサービスの提供を拒否できる旨の規定を盛り込んでいることから、フィッシングメール対策としても効果があることが期待される。

図表5-3-1-3　オプトアウト方式とオプトイン方式の違い



8 参考：「迷惑メールへの対応の在り方に関する研究会」（最終取りまとめの公表）：http://www.soumu.go.jp/menu_news/s-news/2008/080828_8.html
9 参考：特定電子メールの送信に関するガイドラインの公表：http://www.soumu.go.jp/menu_news/s-news/2008/081114_4.html

(3) 携帯電話の安全・安心な利用

ア　「携帯電話不正利用防止法」の適切な執行と改正

「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」（通称：携帯電話不正利用防止法）は、振込詐欺などの携帯電話の不正利用対策として、

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レンタルする行為や携帯電話の無断譲渡等を処罰の対象すること

などを定めており、総務省では、平成20年度中に2件の是正命令を発するなど、その適切な執行に努めている。

しかしながら、同法により携帯電話事業者による本人確認が徹底されているものの、近年、レンタル携帯電話が振込詐欺等の犯罪に使用されるケースが増加したことや、携帯電話端末ではなくSIMカード単体の取引を行うことにより同法の規制を逃れるケースが発生したことなど、既存の条文では対応できない事例が多く発生した。そこで、その対策として、平成20年6月に同法が一部改正され、改正省令とともに同年12月1日から施行されている。改正法においては、

① 携帯電話のレンタル契約締結時の本人確認義務を強化すること及び本人確認記録の保存を義務付けること

② SIMカードの無断譲渡を処罰の対象とすること

③ 政府が情報提供及び国民の理解を深めるための措置を講じること

が定められた[10]。

(4) 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

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・運用している。

また、平成15年2月から、「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」[11]を開催し、個人情報の適正な取扱いについて、より厳格な実施を図るため、個人情報保護法の成立等を踏まえた検討を行い、16年8月に、同ガイドラインの全面改訂及び解説の追加を行った。

さらに、平成17年10月には、「特定電子メール法」を踏まえ、迷惑メール等送信行為を理由として利用停止措置を受けた加入者情報の交換等に関する条文追加及び解説の改訂を行い、19年9月には、位置情報サービスの多様化やGPS機能付端末の普及を受けて、位置情報サービスを提供する際に電気通信事業者が講じるべき必要な措置の内容を明確化するため、同ガイドラインの解説の一部改定を行っている[12]。

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」[13]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い、①視聴者等の個人情報を取得する者を明示すること、②受信機に記録された個人情報を安全に管理することの2点について一部改定を行っている。

10参考：携帯電話不正利用防止法のページ：http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.html
11参考：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：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/privacy/index.html
12参考：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：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html
13参考：放送分野における個人情報保護：http://www.soumu.go.jp/main_sosiki/joho_tsusin/040831_1.html

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

ア　「第2次情報セキュリティ基本計画」と「セキュア・ジャパン」

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。

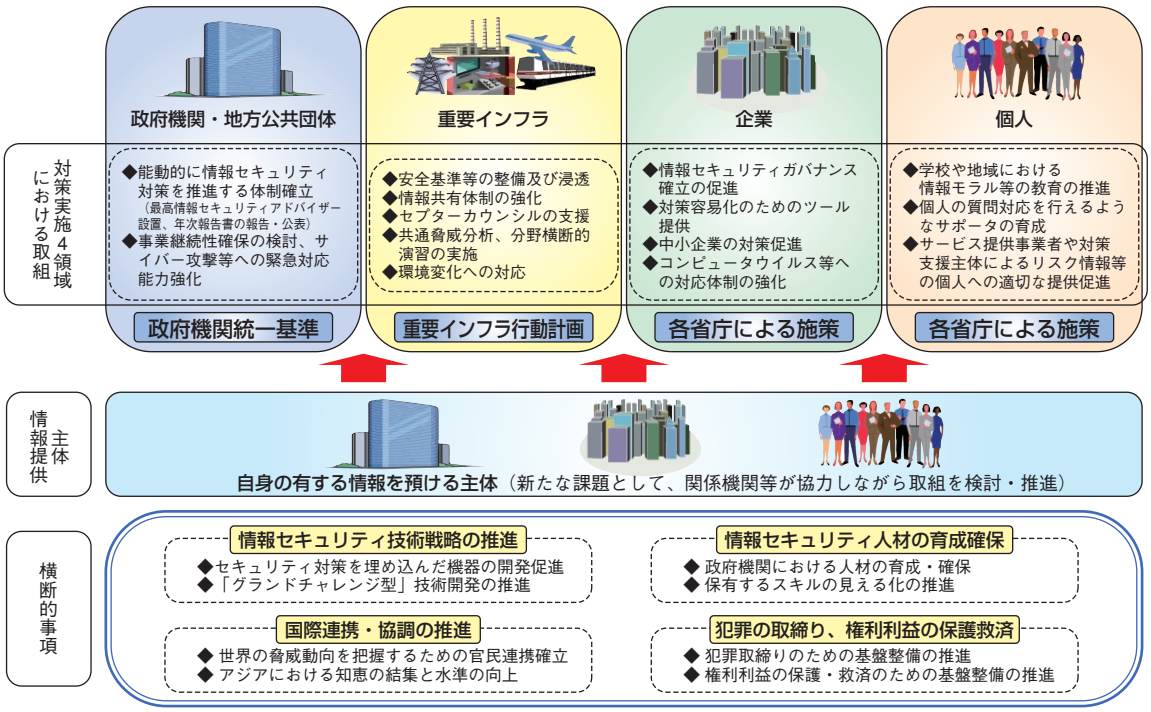
我が国の情報セキュリティ問題への取組としては、平成17年4月に内閣官房に「情報セキュリティセンター（NISC）」が、同年5月に高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）に「情報セキュリティ政策会議」が設置され、強化された。

平成18年2月、情報セキュリティ政策会議において、平成18年度から20年度までの3か年の中長期の戦略である「第1次情報セキュリティ基本計画」が決定された。また、同計画に基づいた年度ごとの推進計画として、平成18年6月に「セキュア・ジャパン2006」、19年6月に「セキュア・ジャパン2007」、そして20年6月に「セキュア・ジャパン2008」が決定されている。

この第1次基本計画に基づく各種の取組の進展や社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組を力強く推進するため、平成21年2月、「第2次情報セキュリティ基本計画」が決定された[14]（図表5-3-2-1）。本基本計画は、平成21年度から23年度までの3か年を対象としている。また、本基本計画に基づき、「セキュア・ジャパン2009」が、平成21年6月に決定された（図表5-3-2-2）。

情報セキュリティ第2次基本計画においては、「ITを安心して利用できる環境」の構築を基本目標に、「セキュリティ立国」の思想の成熟を取組に当たっての基本理念としている。また、基本目標の実現に向けた取組として、官民の各主体が適切な役割分担を果たす「新しい官民連携モデル」に加え、（対策実施側のみならず）情報提供側も視野に入れた取組を推進することとしている。

図表5-3-2-1　「第2次情報セキュリティ基本計画」に基づく取組ー今後3年間の重点政策ー



※　その他、対策支援主体（「情報セキュリティ対策を実施する主体の取組を支援する主体」）の取組も促進する

14参考：第2次情報セキュリティ基本計画：http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf

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」[15]を決定し、同年12月には「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。）を決定している。この政府機関統一基準については、技術や環境の変化を踏まえ見直しを行うこととされており、平成19年6月に改訂第2版、20年2月に改訂第3版が、21年2月に改訂第4版が決定されている。また、平成21年2月に、「政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針」[16]が改訂された。

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している。また、政府機関に対するサイバー攻撃等によるIT障害の発生をより確実に防止し、発生した場合にはより迅速かつ的確に対応するため、政府横断的な情報収集、攻撃等の分析・解析、各政府機関の連携促進等を行う体制を整備することにより、政府横断的な問題解決機能の強化とともに、各政府機関における緊急対処能力の強化支援を行っている。

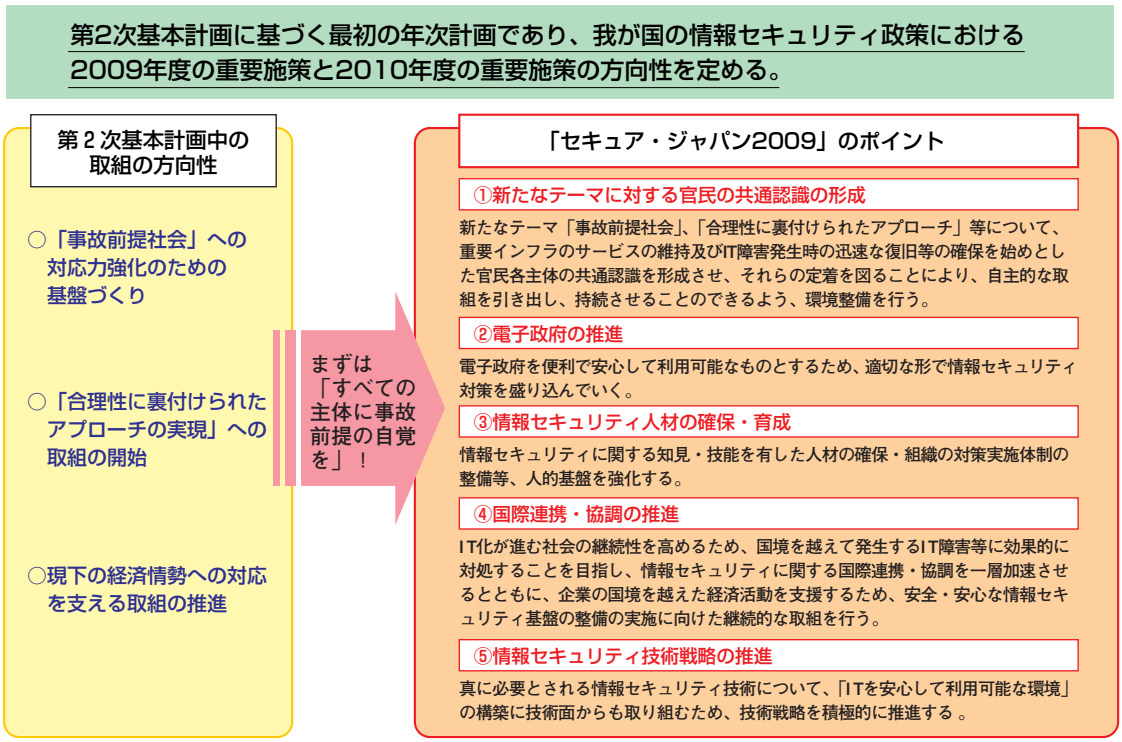
ウ　重要インフラに関する情報セキュリティ対策の推進

国民生活・社会経済活動の基盤である「重要インフラ」によるサービスの安定的供給を確保するためには、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12月に、平成18年度から20年度の3か年の行動指針を示した「重要インフラの情報セキュリティ対策に係る行動計画」を決定した。また、同行動計画を見直し、平成21年2月に「重要インフラの情報セキュリティ対策に係る第2次行動計画」[17]を決定した。

内閣官房情報セキュリティセンターは、同2次行動計画に基づき、安全基準等の整備及び浸透、情報共有体制の強化、共通脅威分析、分野横断的演習及び環境変化への対応を重点政策として掲げ、重要インフラによるサービスの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（金融庁、総務省、厚生労働省、経済産業省及び国土交通省）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。

図表5-3-2-2　「セキュア・ジャパン2009」のポイント



15参考：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：http://www.nisc.go.jp/active/general/pdf/2siryou04-1d.pdf
16参考：政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針：http://www.nisc.go.jp/active/general/pdf/4siryou04-2d.pdf
17参考：重要インフラの情報セキュリティ対策に係る第2次行動計画：http://www.nisc.go.jp/active/infra/pdf/infra_rt2.pdf

(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、u-Japan政策及び「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）ボットネットを悪用した一斉攻撃への対策

「ボット」とは、「ロボット」から取られた造語で、ある種のプログラム（ボットプログラム）を埋め込まれたコンピュータを指し、多数のボットが連携したものが「ボットネット」である。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。

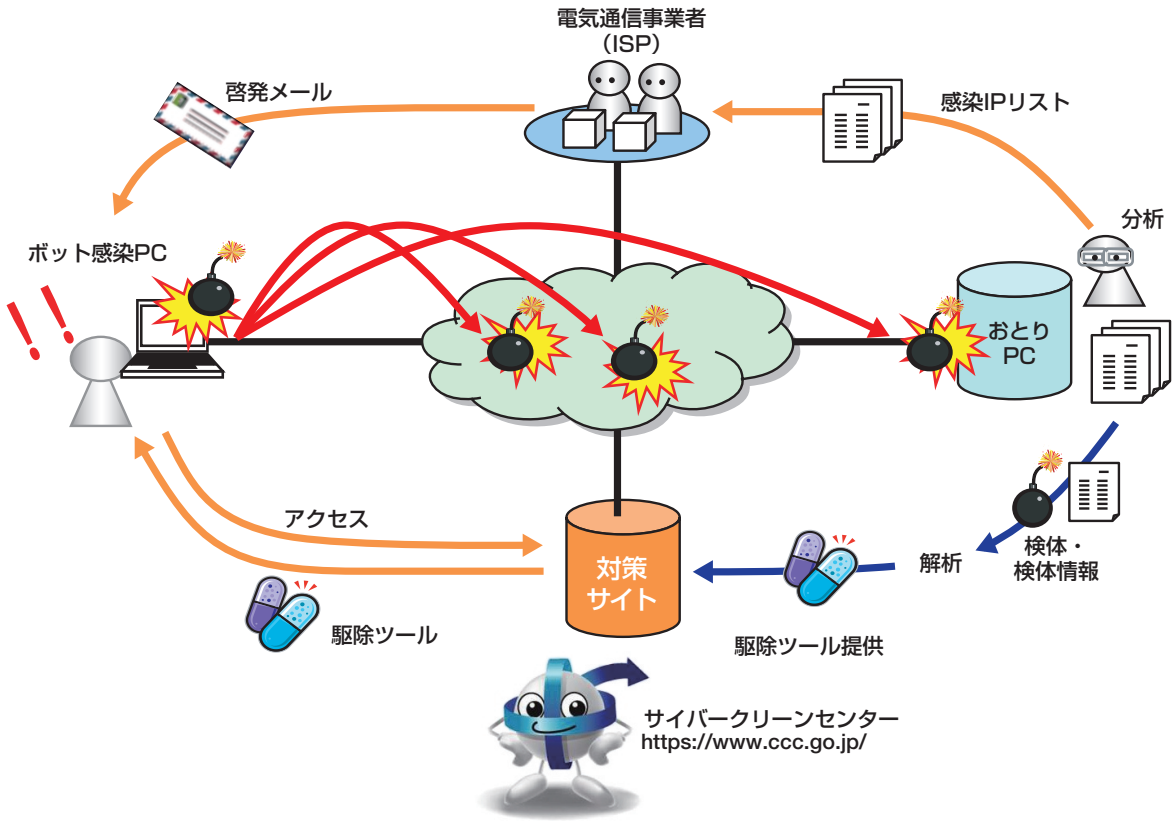
そのため、総務省では、経済産業省と連携して、①ボットネットの要因となるボットプログラムの収集・分析・解析を行うシステムの開発及び試行運用、②ボットプログラムを削除するソフトウェアの開発、③ISPを通じた一般ユーザーへの配布・適用等の対策を講じている。また、ボット対策プロジェクトとして、平成18年12月に、両省共同運営のポータルサイト「サイバークリーンセンター」を開設し、ボット対策情報を発信するとともに、駆除ツールの提供等を行っている[18]（図表5-3-2-3）。

（イ）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、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、平成14年7月にISPを中心として「インシデント情報共有・分析センター（Telecom-ISAC Japan）」が設立され（平成17年2月に財団法人日本データ通信協会に編入）、活動を行っている[19]。

また、Telecom-ISAC Japanの枠組も活用し、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、「T-CEPTOAR」が平成19年4月から運営を開始している。

図表5-3-2-3　ボット対策プロジェクトの概要



18参考：サイバークリーンセンター：https://www.ccc.go.jp
19参考：Telecom-ISAC Japan：https://www.telecom-isac.jp/

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における情報セキュリティ対策の促進

近年、ブロードバンド化の進展により、ネットワークを通じてオンデマンドにアプリケーションソフト等の機能を提供するASP・SaaS等の利用が進展している。

ASP・SaaSの利用は、システムの保守・運用・管理にかかる負担が軽減されるなどのメリットがある一方で、ASP・SaaS事業者に利用者の膨大な情報が集積されることとなることから、適切な情報セキュリティ対策の実施が重要となる。

総務省では、平成19年6月から「ASP・SaaSの情報セキュリティ対策に関する研究会[20]」を開催し、ASP・SaaSにおいて必要とされる情報セキュリティ対策について検討を行い、20年1月に報告書とともに「ASP・SaaSにおける情報セキュリティ対策ガイドライン」を公表したところである。

また、平成20年4月からは、（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。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21年5月15日現在で、71件のASP・SaaSを認定している[21]。

ウ　人的・組織的能力の向上

（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、総務省では、平成18年度～20年度の3か年計画で「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、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を図ってきた。

今後は、電気通信事業者やメーカー等から構成されるテレコムアイザック推進会議の中に、「サイバー攻撃対応演習WG」が演習実施主体として平成21年5月に設置されたことを踏まえ、総務省としても本WGと連携してサイバー攻撃対応演習に関する取組を推進する。

（イ）電気通信事業者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、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、同年6月に業界ガイドライン化した。

同指針は2008年（平成20年）2月に国際電気通信連合（ITU）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。

現在、国際的な議論の場にお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に関する要求事項の国際標準化に向けた議論が行われており、我が国としても積極的に関与していく必要がある。このため総務省では、平成21年5月以降に安心・安全インターネット推進協議会の国際戦略検討WGに設置される、電気通信事業者等を中心とする検討会合と連携して本件に関する取組を推進することとしている。

（ウ）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」[22]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。

また、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協力し、主に保護者及び教職員を対象にインターネットの安心・安全利用に向けた啓発のための講座を全国規模で行う「e－ネットキャラバン」[23]を実施している。

20参考：ASP・SaaSの情報セキュリティ対策に関する研究会：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/index.html
21参考：ASP・SaaS情報公開認定サイト（（財）マルチメディア振興センター）：http://www.fmmc.or.jp/asp-nintei/index.html
22参考：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
23参考：e－ネットキャラバン：http://www.e-netcaravan.jp/

エ　次世代の情報セキュリティ政策の検討

昨今の、ネットワークを経由したウイルス感染の巧妙化・高度化、被害の深刻化や、次世代ネットワークの整備促進等、ICT利用環境が急速に進展している現状を踏まえ、総務省では、平成19年10月から「次世代の情報セキュリティ政策に関する研究会」[24]を開催し、20年7月に最終報告書を策定し、公表した[25]。

同研究会においては、現状のICT環境において継続的に対策を講じていかなければならない課題を明らかにするとともに、3年から5年後の近い将来におけるICT利用環境を想定し、今後、取り組むべき情報セキュリティ政策の在り方について検討を行った。

研究会報告書においては、重点的に検討・実施すべき主な項目として以下の4点を挙げている。

① 利用者を取り巻く環境における情報セキュリティ対策の徹底
② 業界横断的な検討体制の整備
③ 安心・安全なグローバルICT環境の実現に向けた国際連携の推進
④ 産学官連携による先進的な研究開発の実施

(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」の活用の促進を図ってきたところである。しかしながら、ネットワークのIP化が進展し、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等について、事故件数が増加、大規模化、長時間化する傾向にある。

このような状況に対応するため、情報通信審議会において審議がなされ、平成19年5月に「ネットワークのIP化に対応した安全・信頼性対策」、20年1月には「ネットワークのIP化に対応した安全・信頼性基準」について一部答申を受けた。これらを踏まえ、総務省は、IP化するネットワークのシステム管理・人材の在り方について意見集約することを目的に、平成20年4月に「IPネットワーク管理・人材研究会」[26]を開催し、21年2月に最終報告書を取まとめ、公表した[27]。

この中で、IP化の進展に対応した電気通信主任技術者のスキル、電気通信主任技術者資格試験等の見直し等について検討がなされている。

イ　重要通信の確保

災害の救援、社会インフラの確保、秩序の維持のために必要な通信等の重要通信については、天災、事変等の非常事態が発生した際においても、その疎通を確保する必要がある。

近年のネットワークのIP化の進展により、電気通信事業者が所有する設備も変化しつつある状況等を踏まえ、総務省では、電気通信事業においてIP化されたネットワーク等における重要通信の高度化の在り方について検討を行うため、平成19年11月から20年5月まで「重要通信の高度化の在り方に関する研究会」を開催した[28]。同研究会では、

① 重要通信の対象
② 重要通信の疎通の確保
③ 緊急通報等
④ 電気通信事業者間の連携・連絡体制

等について検討を行い、報告書を取りまとめたところであり、これを受けて、重要通信の高度化に向けた施策に積極的に取り組んでいるところである。

24参考：次世代の情報セキュリティ政策に関する研究会：http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/next_generation/index.html
25参考：次世代の情報セキュリティ政策に関する研究会報告書の公表：http://www.soumu.go.jp/menu_news/s-news/2008/080703_5.html
26参考：IPネットワーク管理・人材研究会：http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/ip_network/index.html
27参考：「IPネットワーク管理・人材研究会」報告書の公表：http://www.soumu.go.jp/menu_news/s-news/090218_5.html
28参考：重要通信の高度化の在り方に関する研究会：http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/jyuyou-t/index.html

(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。

そこで、

① 「暗号技術検討会」（総務省及び経済産業省が共同で開催）[29]

② 「暗号技術監視委員会」（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）

③ 「暗号モジュール委員会」（同上）

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」[30]を平成15年2月から公表しているところである。

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、平成14年度に発表した、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）の改訂のための暗号技術公募要項を、平成21年3月に取りまとめたところである。

3 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

我が国は、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、

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」（電子署名法）が平成13年4月から施行されており、21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「電子署名法」の施行状況に係る検討会を開催し、20年3月に報告書を策定した[31]。

(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。

この指針を受けて、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する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21年4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。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[32]。

29参考：暗号技術検討会：http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/ango/index.html
30電子政府推奨暗号リスト：http://www.cryptrec.go.jp/list.html
31参考：「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
32参考：タイムビジネス協議会：http://www.dekyo.or.jp/tbf/