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

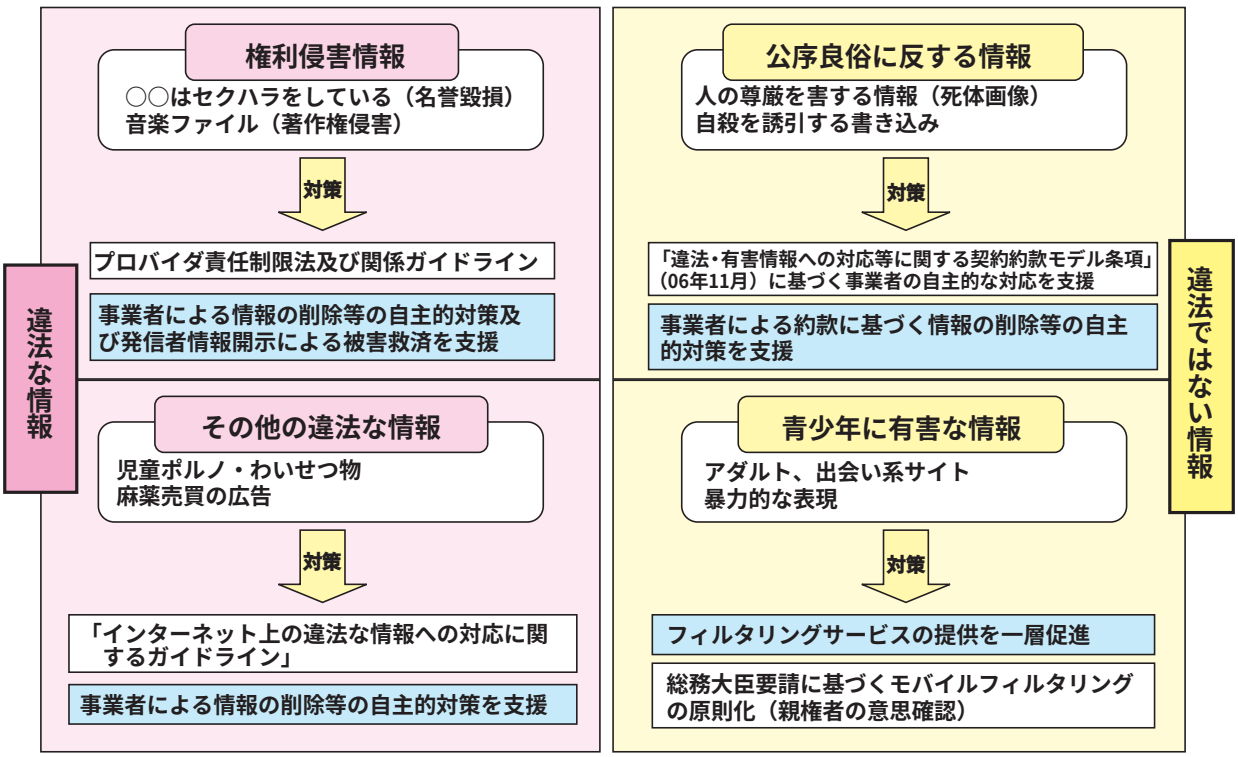
（1）インターネット上の違法・有害情報対策

ア　インターネット上の違法・有害情報への対応

インターネットの急速な発達・普及は、利用者である国民に大きな利便性をもたらす一方で、インターネット上では、いわゆる「闇サイト」が社会問題となっているとともに、青少年が有害サイトにアクセスして犯罪に巻き込まれたりするなどの問題が発生している。

総務省では、平成17年8月から平成18年8月まで開催された「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」における、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・方策に関する検討等を通じて、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取り組んできている。さらに、平成19年11月からは、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うため、「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」を開催しており、平成20年4月、携帯電話等のフィルタリングの改善策等に関して中間取りまとめが行われた。

図表3-3-1-1　インターネット上の違法・有害情報に対する総務省の取組



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、社団法人テレコムサービス協会内に設置されている「プロバイダ責任制限法ガイドライン等検討協議会」に対する支援や周知を行っている。

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」、平成19年10月に「インターネット上の違法・有害情報に関する集中対策」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。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・問い合わせ等を受け付ける「違法・有害情報事業者相談センター」をテレコムサービス協会内に設置した。

エ　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、フィルタリングの研究開発を行い、平成17年7月から携帯電話事業者はフィルタリングサービスの提供を開始している。

フィルタリングに関係する業界団体は、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」を策定し、普及啓発活動に努めているところである。

総務省は、フィルタリング導入促進のため、平成18年11月に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ほか、平成19年2月に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、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した。

さらに、総務省では、平成19年12月に携帯電話事業者等に対し、青少年が利用する携帯電話等に関し、フィルタリングサービスの利用を原則とした形で親権者の意思確認を行う等のフィルタリングサービス導入促進活動の強化をするよう要請したほか、平成20年4月には、「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」中間取りまとめに示された方向性を踏まえ、フィルタリングの改善等に取り組むよう、携帯電話事業者等に対し、要請したところである。

総務省では、今後も引き続き業界や関係省庁等と連携し、青少年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・フィッシング対策

ア　迷惑メール対策

迷惑メール対策については、総務省では、「特定電子メールの送信の適正化等に関する法律」や、電気通信事業者による自主的な取組、迷惑メール対策技術の導入の促進、国際連携の推進等に努めており、我が国の国際的な迷惑メール送信国順位が大幅に低下するなど、一定の成果を収めている。しかしながら、迷惑メール全体の流通量は依然増加傾向にあり、また、迷惑メールの巧妙化・悪質化が進み、さらに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。

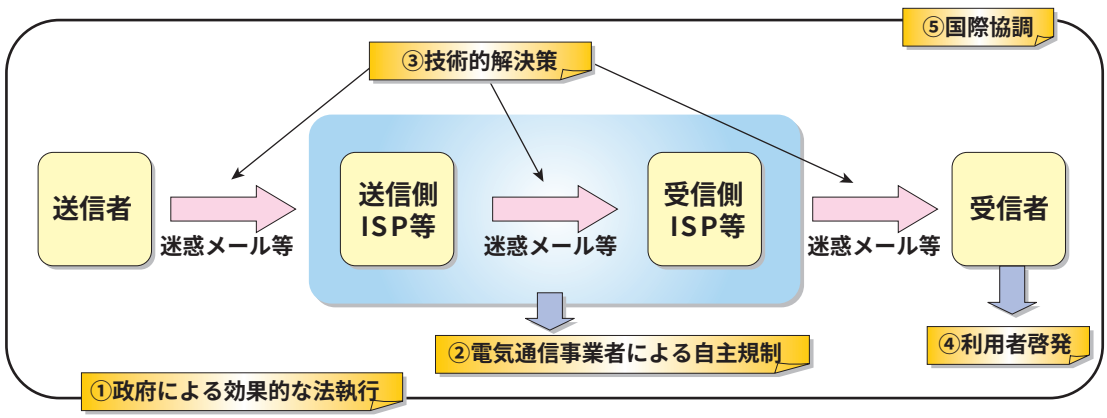
このため、総務省では平成19年7月から「迷惑メールへの対応の在り方に関する研究会」を開催し、総合的な迷惑メール対策を検討しており、同年12月には法制度の在り方の見直しを中心とする同研究会中間取りまとめが公表された。平成20年2月29日にはこの中間取りまとめを踏まえた「特定電子メールの送信の適正化等に関する法律の一部を改正する法律案」が閣議決定され、国会に提出された。同法案は、①原則としてあらかじめ同意をした者に対してのみ送信を認めるオプトイン方式の導入、②法人に対する罰金額の引き上げや報告徴収の範囲の拡大等による法の実効性の強化、③迷惑メール対策を行う外国執行当局に対し必要な情報の提供を可能とすること等の国際連携の強化を内容としており、衆議院及び参議院とも全会一致で可決され、平成20年5月30日に成立し、6月6日に公布されたところである。

迷惑メールに関しては多面的に対策を講じることが重要であることから、「迷惑メールへの対応の在り方に関する研究会」では引き続きオプトイン規制の運用の在り方や技術的対策、国際連携の在り方等について検討を進めている。

イ　フィッシング対策

金融機関等信用のある者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。上記「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おり、この結果に基づく上記改正法案では、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3-3-1-2　迷惑メール対策の全体像



→スパム対策は‘ No silver bullet ’(特効薬はない)であり、多面的な対応が不可欠。
できるところから行動すべき(2004年2月開催のOECDスパムワークショップ)

①～⑤の総合的な対応策を検討し、一層の利用者保護の強化等電子メールの利用についての良好な環境の整備を図る

（３）携帯電話の安全・安心な利用

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利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利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　携帯電話のパケット通信料金の高額利用についての注意喚起

近年、消費者から総務省に対して、携帯電話の高額なパケット通信料金に関する相談事例が増えている。

パケット通信料金は、データ量が大きいサービスの利用やインターネットウェブページの閲覧、パケット通信料金の定額制の対象外となるインターネット接続の利用等によって、思いがけず高額となる可能性があることから、総務省では、利用方法にあった料金プランの選択や、定額制の対象外となるパケット通信料金の確認、通信料金が一定額を超えた場合に、利用者に通知されるサービスや利用が制限されるサービスの利用等の対策方法の周知を行っている。

（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、同ガイドラインの改定を行っている。

また、平成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た。

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

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月から平成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、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た。

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1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。

そのため、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」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、平成18年度から平成20年度までの3年間の我が国全体の情報セキュリティ問題全般についての戦略として、「第1次情報セキュリティ基本計画」が決定されており、また、同計画に基づいた平成19年度の具体的な年次計画として「セキュア・ジャパン2007」が平成19年6月に決定されている。その主な内容は次のとおりである。

（ア）平成19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 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 政策の推進体制と持続的改善の構造

（イ）平成20年度における重点施策の方向性

「情報セキュリティ人材の育成・確保、情報セキュリティ政策の国際展開、電子政府等の情報セキュリティ強化を中心とした情報セキュリティ基盤の強化に向けた重点的取組み」を重点とし、以下の施策を推進することとしている。

① 情報セキュリティ人材の育成・確保に向けた集中的な取組み
② 情報セキュリティ政策の国際展開に向けた集中的な取組み
③ 電子政府等の情報セキュリティ強化のための総合的な取組み

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、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月には改訂第2版が、平成20年2月には改訂第3版が決定されている。

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している。

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。

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な演習の実施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（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。

また、同計画の計画年度が平成20年度までであることから、平成21年度以降の計画策定に向けて、同計画の見直し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

総務省では、u-Japan政策及び「第一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。

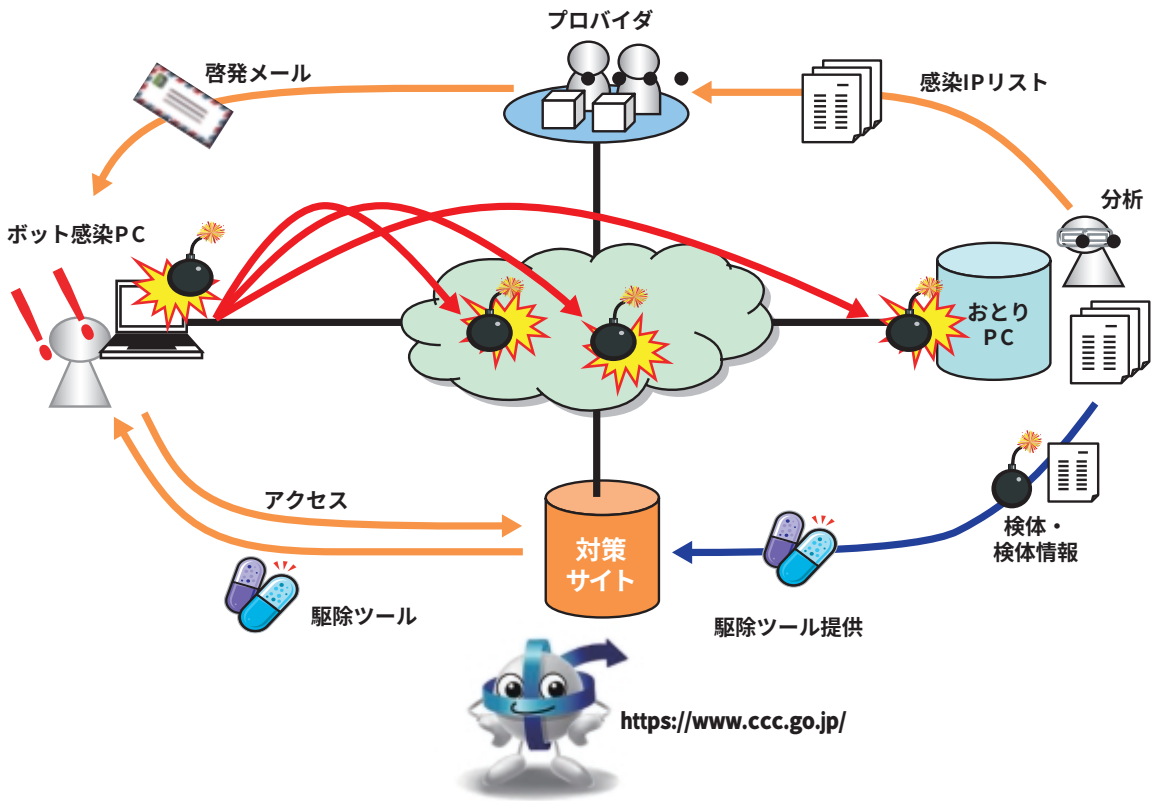
そのため、総務省では、経済産業省と連携して、①ボットネットの要因となるボットプログラムの収集・分析・解析を行うシステムの開発及び試行運用、②ボットプログラムを削除するソフトウェアの開発、③ISPを通じた一般ユーザへの配布・適用等の対策を講じているほか、平成18年12月にボット対策プロジェクトとして、両省共同運営のポータルサイト「サイバークリーンセンター」を開設し、ボット対策情報を発信するとともに、駆除ツールの提供等を行っているところである（図表3-3-2-1）。

（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（平成17年1月に財団法人日本データ通信協会に編入）され、活動を行っている。

また、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、「T-CEPTOAR」が平成19年4月から運営を開始している。

図表3-3-2-1　ボット対策プロジェクトの概要



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」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、平成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。

適切な情報セキュリティ対策が施されたASP・SaaSサービスの提供が促進され、ASP・SaaSが企業の生産性向上の健全な基盤となるよう、ASP・SaaS業界における当該ガイドラインの普及促進活動や継続的な見直し・改善に向けた取組の支援を行っている。

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、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いる。

（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。また、同指針を国際電気通信連合（ITU）に提案し、平成20年2月にISM-TG（Information Security Management Guideline for Telecommunications、X.1051）として国際標準化が了承された。ISM-TGについては、国際標準化機構／国際電気標準会議（ISO/IEC）においてもISO/IEC27011として国際標準化が進められており、平成20年3月末現在、国際標準化に向けた最終投票が行われている。

（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」を開設し（平成19年6月リニューアル）、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。同活動は、「生活安心プロジェクト 緊急に講ずる具体的な施策」において青少年を有害情報から守るための代表的な国民運動として位置付けられており、平成19年度においては、全国で1,089講座を実施した。

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」を開催し、現状のインターネット等の利用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ている。

平成20年4月に公表された中間報告書では、「重点的に検討・実施すべき項目」として以下の5点が挙げられている。

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 産学官連携による先進的な研究開発の実施
③ 関係機関における連携強化
④ ユビキタスネットワーク社会における情報セキュリティ対策に関する業界横断的な検討体制の整備
⑤ 利用者、情報通信環境、情報セキュリティが共生するICT社会モデルの検討

同研究会では、本中間報告書に基づき更に検討を重ね、平成20年7月を目途に最終報告書を取りまとめる予定である。

（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、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ところである。しかしながら、近年、これまでの安全・信頼性を確保するための対策が適切に実行されているにもかかわらず、ネットワークのIP化の過程において、事故・障害等の件数が増加するとともに、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、総務省は、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」、平成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。

総務省では、これらの答申を踏まえ、

① 事故の報告基準及び管理規程の見直し、事故の定期報告化等を内容とする省令等の改正

② ガイドラインの見直し

等を行ったところである。

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月から平成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。

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。

（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）

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」を平成１５年２月から公表しているところである。

平成１９年度は、これらの暗号技術を正しく利用するためのガイドブックとして「電子政府推奨暗号リストガイド」を作成し、また、電子政府推奨暗号リストの見直し方針を決定したところである。

今後はこの方針等を受けて、電子政府推奨暗号リストの改訂に向けて暗号技術の公募の準備を進めるとともに、引き続き、電子政府推奨暗号に関連する調査等を進めることとしている。

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」（平成12年法律第102号）が平成13年4月から施行されており、平成20年4月末現在、18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ほか、諸外国との国際協調にも積極的に取り組んでいるところである。

（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20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）したほか、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。