

「第2次情報セキュリティ基本計画」(案)及び「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」(案)に関する意見書

2009年(平成21年)1月9日
日本弁護士連合会

第1 「第2次情報セキュリティ基本計画」(案)の基本的な考え方について

1 「第2次情報セキュリティ基本計画」(案)の概要

「第2次情報セキュリティ基本計画」(案)(以下「基本計画案」という。)は、「第2次基本計画における重要なメッセージの一つは、『事故前提社会』への対応力強化(第2章第1節を参照)である。これは、第1次基本計画の下での取組みが、事前対策に重点を置くような形で進められたことを受けて、万が一の事態における広い範囲での対応や復旧の準備にも注力することを意味する。もちろん、引き続き、あらゆる主体が情報セキュリティ上の問題の発生を防止するべく事前対策について最大限の努力を行う必要があることは言うまでもない。第2次基本計画を受けて、あらゆる主体は事前から事後まで、一貫した情報セキュリティ対策を進めることが期待される。」(基本計画案3頁)としている。

2 当連合会の基本的立場

このような基本的な考え方自体については、当連合会は賛成である。当連合会はトラブルは起きるという前提で対応を考えなければならないという意見を述べてきた。個人情報の漏洩などのトラブルが起きた際のことを考え、そのための予算、人員の確実な手当がなされる必要がある。

第2 国の政府機関間、国と地方の機関間、官民間の情報の共有の範囲を明確にする必要がある。

1 政府機関・地方公共団体の重要インフラについて

政府機関・地方公共団体の重要インフラについて、基本計画案では次のように記述している(基本計画案54-55頁。なお、「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」(案)(以下「行動計画案」という。)15-20頁は、基本計画案を敷衍してやや具体的な記述がなされている。)

「重要インフラ

重要インフラの情報セキュリティ対策に関する関係主体は、第2次行動計画に基づいて、各々重要インフラサービスの維持に努め、またIT障害発生時の迅速な復旧等を確保することに努めることとする。また、情報セキュリティ対策の実施状況について指標を用いた検証を毎年実施するとともに、行動計画の評価を実施し、各々の取組みの継続的改善を図ることとする。これらについての具体的な取組みは第2次行動計画に詳述しているが、以下にその概要を示す。

(ア)「安全基準等」の整備及び浸透

第1次行動計画で策定された指針について、事業継続の観点からの具体的内容の補充を含め、指針の位置づけや記載内容の具体性のレベルの見直しを行う。また、重要インフラ事業者等のPDCAサイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず、3年毎に個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する。

(イ) 情報共有体制の強化

第1次行動計画で構築されたセプター、セプターカOUNシルを含む関係主体間で共有する情報についての整理を行い、情報提供、情報連絡等に必要な環境整備等を推進するとともに、各セプター、セプターカOUNシルの自主的な活動の充実強化を推進する。

(ウ) 共通脅威分析

第1次行動計画で実施してきた、ある重要インフラ分野にIT障害が発生した場合に他のどの重要インフラ分野に影響が波及するか、という相互依存性解析を継続するとともに、重要インフラ分野共通に起こりうる脅威が何であるかを把握するための検討を行う。

(エ) 分野横断的演習

第1次行動計画において得られた分野横断的な演習手法に関する知見を踏まえ、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のセプター等の協力を得て、IT障害の発生を想定した、重要インフラ分野横断的な演習を実施する。

(オ) 環境変化への対応

社会環境や技術環境等の状況の変化に合わせて情報セキュリティ対策を機敏に対応させていくために、第2次行動計画策定時に想定しなかった環境の変化を察知する能力の向上に努める。また、こうした環境の変化に対して第2次行動計画の枠組みだけでは十分に対応できない場合は、内閣官房は必要な対応が可能となるような体制の検討を行う。」

2 国家機関内における情報共有についての懸念

この基本計画案及び行動計画案で議論されていることは情報セキュリティの強化についてであり、ここで議論されている「情報共有」や「共通脅威」、「分野横断的演習」などもあくまで、情報セキュリティに関する技術的なものであると理解される。

しかしながら、当連合会は国や地方公共団体に蓄積されている情報が横断的に共有されることについては、一貫して個人のプライバシーの権利への大きな侵害となる可能性を指摘し、警鐘を述べてきた。

例えば、第50回人権擁護大会(2007年11月2日)における「人権保障を通じて自由で安全な社会の実現を求める宣言」の本文においては、「国や地方自治体が、住民基本台帳ネットワークシステムや外国人の入国・在留管理などを通じて、また、国家間の情報の共有によって、あるいは市民や事業者からの報告を義務付けることにより個人情報を取得する制度が創設されつつあり、その情報を統合し、利用することが模索されている。憲法13条の個人の尊厳、幸福追求権の保障に含まれる自己情報

コントロール権尊重の見地から、『改正』入管法などの制度の見直しを行うとともに、このような個人情報の統合、利用を厳格に規制し、特に警察などが市民の生活や思想を監視するために情報を利用することを防止すること。

また、国及び地方自治体などによる個人情報の取得、保管、利用に対する調査、是正命令などを行う権限を持つ、政府から独立した機関を設立すること。」を求め、決議理由においては、「警察は、通行する車両の移動をテレビカメラとコンピューターによって監視・記録・保存するNシステムによって、車両の位置情報を全国規模で入手することができる。また、国や地方自治体は、住民基本台帳ネットワーク（以下「住基ネット」という。）によって様々な個人情報を統合して利用することが可能となっている。

テロや犯罪を防止する社会体制を構築するためとして、『改正』入管法によって国が取得した外国人の指紋情報、顔情報と在留関係の様々な情報が、統合されて利用されることが可能となっている。さらに、銀行などが取得した個人の金融取引情報、監視カメラなどで取得した人の顔貌や所在などの情報、外国人の就労、就学情報などが国に集積され、市民の生活状況が国によって詳細に把握される可能性が高まっている。これらの情報は『改正』入管法の国際的な情報提供の規定などを通じて、国際的にも統合される可能性が生じている。このように、市民の生活情報、思想傾向などのデリケートな自己情報が、知らないうちに警察などの国の機関に集積され、名寄せされて、市民の行動や思想などが容易に把握されるという監視社会化が進む可能性が生じている。

これに対して、行政機関の保有する個人情報の保護に関する法律は、行政機関の取得した個人情報について法律の規定さえあれば、その実質的な理由の有無や相当性などにかかわらず他の行政機関に提供することを可能としており（同法8条）、取得した情報の保有期間やデータの個人ごとの集約による生活状況の分析に対する規制も何ら規定していない。

この結果、市民は、一方で政治過程へ民主的に参加する上で必要不可欠な公益的情報から閉ざされながら、他方で個人のプライバシー権ないし自己情報コントロール権が侵害されるおそれが強まっている。」としている。

3 基本計画案及び行動計画案についての当連合会の疑問と見解

上記のような当連合会の基本的な立場から検討すると、基本計画案及び行動計画案には次のような疑問と懸念があると言わざるを得ない。

基本計画案及び行動計画案においては、国家機関間、国家機関と地方公共団体の間、官民間の情報共有の方法やそのためのルールについての考え方を述べたものとは理解されない。

しかしながら、基本計画案及び行動計画案の前記の部分を注意深く読めば、背後に何らかのデータベース結合の計画ないし実体が既に存在し、これらが現実に運用されるような状況の下で、このような統合されたネットワーク全体の情報セキュリティの向上を図ることを念頭に置いた計画となっているのではないかとの疑問を表明せざるを得ない。なぜならば、国家機関間、国家機関と地方公共団体の間、官民間の情報共

有がなされていなければ、「情報共有」や「共通脅威」、「分野横断的演習」を議論する実益もないのである。

少なくとも、当連合会としては、国家機関間、国家機関と地方公共団体の間、官民間の情報共有の方法については、その考え方やそのルールを明確にする必要があり、共有される情報がどのような性格を持った情報を含み、どのような情報は含まれないのかを明らかにすべきであると考えます。

また、「共通脅威」や「分野横断的演習」を問題とするのであれば、なぜ一つの脅威が共通の脅威となるのか、「各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のセクター等の協力を得て」行われるとされる「重要インフラ分野横断的な演習」が必要である技術的な背景として、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のセクターがネットワークを通じてどのような結合・相互連携の状況にあるのかを明確にすることが必要であると考えます。

そして、情報セキュリティの向上を図るだけでなく、このような活動を通じてプライバシー権ないし自己情報コントロール権に対する侵害が発生しないように、当連合会は前記の宣言において以下のとおり独立の第三者機関の設立を求めている。

「これに対して、EUでは、加盟各国に対して政府から独立した、情報保護に関する第三者機関の設置を指示し、各国においてデータ保護監察官（ドイツ連邦共和国）などが設置されている。多岐にわたるプライバシー権ないし自己情報コントロール権に対する侵害の問題については、その専門性、人権保障という準司法的性格に鑑み、日本においても、プライバシー権ないし自己情報コントロール権を保護する観点から、国及び地方自治体などによる個人情報の取得、保管、利用に対する調査、是正命令などを行う権限を持つ、政府から独立した第三者機関を設立すべきである。」

よって、このような情報セキュリティについての基本計画を立案する際には、この問題と密接に関連する自己情報コントロール権を保護する観点から、国及び地方自治体などによる個人情報の取得、保管、利用に対する調査、是正命令などを行う権限を持つ、政府から独立した第三者機関の設立を前向きに検討すべきである。

以上