資料 4

日弁連総第８４号
２００８年（平成２０年）２月１３日

情報セキュリティ政策会議
基本計画検討委員会
委員長　須藤　修　殿

日本弁護士連合会
会長　平山　正剛

「第２次情報セキュリティ基本計画」（仮称）の検討に係る意見について

当連合会では，標記につきまして別紙のとおり意見をまとめましたので，ご検討いただきたく提出致します。

「第２次情報セキュリティ基本計画」（仮称）の検討に係る意見

２００８年（平成２０年）２月１３日
日本弁護士連合会

１　現在の社会環境とＩＴが果たす役割について

(1) ＩＴのような情報インフラは、水道、電気、ガス等に続く社会のインフラとして認識される時代となっている。個人情報保護法１条が「高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱い」をはかることを求め、また高度情報通信ネットワーク社会形成基本法２２条が「高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置を講じ」ることを求めているが、これらの観点は、現在の社会環境とＩＴが果たす役割についても、その前提条件と考えることができる。

(2) 当連合会は、１９９０年（平成２年）９月２８日に、国民の情報主権の確立という観点から、国が保有している国政関係の諸情報については、主権者たる国民のものであることを基本として、諸施策が実施されなければならない旨の宣言を採択した。

他方、個人のプライバシー権保護という観点から、個人情報の収集・管理・利用・閲覧・訂正等にわたって、個人の権利が保障されなければならない。当連合会は、２００１年（平成１３年）５月９日付け「個人情報の保護に関する法律案に対する意見書」において、当時提案されていた個人情報保護法について、「個人情報保護の名の下に民間の情報を国家がコントロールする民間規制法というべき極めて危険性の高い法案であ」る旨批判しており、民間部門における情報の流れを国家がコントロールすることは抑制されなければならない。

殊に、当連合会は、近年のデータ通信技術の急速な高度化と広がりをふまえ、２００２年（平成１４年）１０月１１日には、電子政府、電子自治体及び住基ネットの稼動に伴うプライバシー侵害の危険性を指摘し、国及び地方自治体が収集・管理する個人情報の分散管理を意識的に進めるとともに、統一的なセキュリティ基本法を定めることを求め、その後２００３年７月１８日には、国及び地方自治体のセキュリティ確保のための制度をさらに検討し、情報主権の確立とプライバシー保護を確保しつつ情報資産のセキュリティを確保するとの基本理念に基づき、国および地方自治体等の情報セキュリテ

ィポリシーを策定し、継続的かつ不断の努力によってセキュリティの水準を向上させるべき責務をさだめること等を骨子とした情報セキュリティ基本法の法文案(以下「日弁連案」という。)をとりまとめて、公表した。これらの政策提言の経過をふまえて、情報セキュリティとして取り組むべき範囲については、プライバシー保護を頂点として明確に位置づけ、情報セキュリティを環境マネージメントや品質マネージメントと一体のものとして取り組むべきである。

2　情報セキュリティ政策に関する現状認識と評価について

ＩＴの利用に絶対的な安全はない。実現可能なのは「より安全な環境」だけである。したがって、「ＩＴを安心して利用可能な環境の構築」という設定そのものが正確性を欠いているから、「ＩＴをより安全に利用可能にする環境の構築」とすべきである。この場合においても、上記１で述べた、情報主権の確立及び国家が情報をコントロールする民間規制法とならないようにする必要がある。

3　情報セキュリティ政策の理念について

当連合会は、日弁連案において、「情報セキュリティ」を「情報の機密性、完全性及び可用性の維持」と定義付けたが、現時点で、「情報セキュリティ」をどのような概念として定義づけ、その法律上の要件や効果をどのように考えるべきか、議論が尽くされていない。

日弁連案が公表された後、与党において個人情報保護法の罰則を強化しようとする試みがなされたことや、後記のとおりサイバー犯罪条約とその国内法化に問題点があることをふまえると、上記２のとおり、情報主権の確立及び国家が情報をコントロールする民間規制法にならないようにするとの観点から、限定的な定義付けが必要である。

また、情報セキュリティは、リスクマネージメント（危機管理）を政策の理念とすべきであり、企業・個人のコンプライアンス（法令順守）だけの問題と把握されてはならない。社会的コストがあるとしても、それを理由に隠蔽やリスク無視が正当化されることにはならない。さらに、過度の責任追及をおそれ隠蔽するとしても、責任追及を求めないというのは被害者救済の観点からも問題である。情報セキュリティポリシーの策定、不正アクセス対策の実施等の具体的な責務を定めることによって、世界最高水準の情報セキュリティ技術の形成を促進し、情報セキュリティを確保するための教育および学習を振興するとともに、情報セキュリティを担う専門的な知識または技術を有する創造的な人材を育成し、もって基本的人権を擁護し、高度情報通信

ネットワーク社会の安全性を確保することが求められる。

４　第２次情報セキュリティ基本計画の枠組みについて

当連合会は、上記３のとおり、現時点で情報セキュリティの概念について一義的な見解を有するものではないが、今般の提案にかかる第２次情報セキュリティ基本計画は、個人情報保護や不正競争防止法が規定する営業秘密保護の分野の政策と相当部分において重複するとも考えられるから、上記のとおり、国家が情報をコントロールする民間規制の計画とならないよう、個人情報保護や営業秘密保護の分野の政策との整合性を考えるべきである。

当連合会は、前述の２００１年（平成１３年）5月９日付け意見書により、民間部門における個人情報保護法の制度設計については、個人信用情報や医療情報など分野別個別法によるべきであることを指摘し、全分野に横断的に適用される一般法の制定には反対してきた。また、個人情報保護法が成立した２００３年（平成１５年）5月２３日にも、「個人情報保護関連法案の成立に関する会長声明」において、個人情報保護法によって情報の流通が妨げられ日本社会全体が委縮してしまう危険性を指摘したところである。今般の基本計画が、電気通信事業分野における個人情報保護等の個別的分野についての保護をはかるというものであれば、当連合会が求める個人情報保護のあり方等と方向性を同じくすることが期待される。

５　政府機関・地方公共団体における情報セキュリティ対策について

上記のとおり、国民の情報主権の確立という観点からは、情報公開法及び情報公開条例が前提とする公文書（公的情報）の管理が十分になされているかという観点もあわせ考えて、政府機関と地方自治体に個別具体的な統一基準をもって情報セキュリティのあり方を考えるべきである。安全保障・外交、犯罪関連等を理由とする機密情報の保護を当然の前提として、情報セキュリティを検討すべきではない。

内閣官房情報セキュリティセンターの強化、並びにサイバー犯罪条約の締結に伴う法制度の改正及び国際協力の強化によりサイバー犯罪の取締りを強化するということについても、上記の観点から慎重な検討が必要である。当連合会は、２００４年（平成１６年）４月１７日、サイバー犯罪条約は、人権保障の観点から、国民のプライバシーや通信の秘密に対する重大な制約となる危険性が大きく、その影響は極めて重大であるとして、その条約批准に反対した。

また、各府省庁が自らのセキュリティ対策をチェックできる仕組み（監査体制等）の構築については、府省庁で統一的にはなされていない。政府機関

の情報セキュリティ対策については、内閣府内にその推進組織を作り、外部に監査のための第三者機関を作るべきである。さらに地方自治体へは十分な予算配分を検討すべきである。

6　重要インフラにおける情報セキュリティ対策について

そのカテゴリーを設けること自体は認められるが、そもそも、「重要インフラ」というカテゴリーを法律用語として用いるとすると、これが何を意味することになるのか、その定義付けが極めて不明確である。

各業法の個別的適用範囲を検討することなく、「重要インフラ」の名の下で、各業法でカバーしていない部分を含む、罰則付きの一般法的な情報セキュリティの法規制はなされるべきではない。

これに関連して、情報の流出については、外部からの侵害による情報流出と内部からの漏えい（故意又は過失）がある。すなわち、政府機関と民間の何れにおいても、内部からの漏洩については、個人の不正な利益を目的としたものもあるが、職員や従業員などによる公益目的（国民の生命身体財産保護）の告発や企業のコンプライアンス違反の行為の告発などもある。公益通報者保護法（２００４年（平成１６年））の制定により、「事業者による国民の生命や身体の保護、消費者の利益の擁護等にかかわる法令遵守を確保することを目的」とする公益通報は法的に保護されることになった。ただ、この制度は「犯罪行為等の事実が生ずる場合」に限定している点などが不十分である。

情報セキュリティの名のもとに正当な内部告発などが抑制され、国民の知る権利が侵されることがあってはならず、そのような視点からも検討することが必要である。

7　企業や個人等の民間部門における情報セキュリティ対策について

上記６と同様、個人情報保護法、知的財産法、Ｊ－ＳＯＸ法、不正競争防止法等、情報資産の保護に関する制度や企業のコンプライアンスに関連する諸制度が、有効に機能しているかどうかの十分な分析検討なくして、国家が一般企業における情報セキュリティ対策を罰則付きで一般的包括的に規制することは避けるべきである。

その意味において、罰則付きの一般的包括的な「情報セキュリティ基本法」や「情報保護に関する一般的な法制度（罰則を含む）」というようなものは現段階では必要とはいえない。むしろ、日弁連案でも提案したとおり、内閣府内に情報セキュリティの推進組織とともに、外部に政府機関のセキュリティ対策を監査するための第三者機関を作るべきである。

また、個人のＩＴ安全利用環境のための制度、技術（フィルタリング、認

証制度等）と、既存のネットワークのアーキテクチャ（コンテンツの解放、匿名性等）との関係については、たとえば、有害環境対策が現になされている有害図書規制と同様、「有害」の定義が不明であるによって、知る権利や社会参加する権利の侵害が指摘されていることなどをふまえると、今後、個別具体的な法分野で十分に検討されるべきであり、現段階で早計な結論を導くことは望ましくない。