サイバー空間の安全性・信頼性向上のための課題等に関する検討会の概要

2011年3月25日

◆ 検討の背景および目的

「情報セキュリティ2010」（平成22年7月22日情報セキュリティ政策会議決定）においては、内閣官房において、「機微な情報へのアクセス権限を明確化するための方策や情報漏えい等を防止するための方策等サイバー空間の安全性・信頼性を向上させる制度に係る課題について検討を行う（P63）」ことや、「大規模な個人情報漏えいを防止する観点から、アクセス権の設定、認証情報の管理、暗号化、匿名化等のプライバシー保護技術の適切な利用方法について検討する（P45）」こととされている。

本検討では、海外におけるサイバー空間の安全性・信頼性に係る制度についての調査を通じて、我が国において今後検討が望まれる制度的課題について、論点の整理を行った。

◆ 検討会委員（敬称略）

岡村久道	弁護士・国立情報学研究所客員教授（座長）
石井夏生利	筑波大学准教授 （IT本部電子行政タスクフォース構成員）
ジョン・キム	慶応大学准教授（ハーバード大学客員研究員）
鈴木正朝	新潟大学教授
高木浩光	（独）産業技術総合研究所　主任研究員

◆ 検討会の開催経緯

第1回検討会　2011年2月10日（木）
第2回検討会　2011年2月24日（木）
第3回検討会　2011年3月9日（水）

◆ 事務局における調査

以下の項目に関し、事務局（NRIセキュアテクノロジーズ）において、インターネットによる公開情報ベースの調査を行うとともに、有識者へのヒアリングを実施した。

（1） 個人のIT利用に係るセキュリティ対策
（2） 組織における情報セキュリティ対策
（3） 情報セキュリティに関係する制度の国際的調和（サイバー空間における安全保障等の論点を含む）

論点整理の結果：課題と背景、解決策のまとめ (1) 早急に取り組むべき課題①

早急に取り組むべき課題	背景及び 解決策
情報漏えいやデータ消去を引き起こすような凶悪なマルウェアによる被害を防ぐ取組が必要である（特に、我が国では、ファイル共有ソフトに関連した、いわゆる暴露ウイルスによって深刻な被害が発生している）	● 英・仏・独等の欧州各国及び米国では規制法が制定されている一方で、我が国ではマルウェアの作成や頒布を直接規制する法律が存在していない（マルウェアによっては、電子計算機損壊等業務妨害罪や電磁的記録毀棄罪を適用しうるとは限らない。） ● ワクチンソフトの改良は進んでいるものの、ワクチンソフトによるマルウェアの検出率低下の傾向は年々強まっており、それだけによってマルウェア被害を抑制することには限界がある。 ● サイバー攻撃はボーダーレスに行われるため、我が国がサイバー犯罪のループホールにならないようにする必要がある。（参考資料参照） → **マルウェアの作成や頒布行為を規制するための法律の早期の制定が望まれる。** → なお、規制にあたっては、ソフトウェアに関連する正当な研究・開発行為を規制することがないよう、**法律の普及・啓発活動等を通じて規制範囲を明確にしていく**ことが望まれる。
情報セキュリティ事故が起こった際に、被害の発生・拡大を防止するための対策の実施を促す制度設計が必要である	● 企業等による個人情報の漏えいは、繰り返し発生しているが、情報セキュリティ対策の観点からは、これを完全にゼロにすることは困難であると言わざるをえない。 ● 個人情報漏えいについては、二次被害の防止等の観点から、本人への連絡、公表、主務官庁への通知が求められてきたところであるが、現在では、暗号化等の技術的手段によっても、情報漏えい時の二次被害の防止等を図ることができるようになっている。 ● いわゆる「漏洩」が発生した場合に行うべき対応として、本人通知や公表等に加えて暗号化等の技術的対策の実施についても選択肢とすることにより、対策の実施を促すことが可能となると考えられる。 → **上述の観点から、個人情報保護に係る主務省庁のガイドライン等が検討されていくことが望まれる。**

論点整理の結果：課題と背景、解決策のまとめ (2) 早急に取り組むべき課題②

早急に取り組むべき課題	背景及び 解決策
クラウドコンピューティングにより海外にデータが移転する可能性があることへの対応策を検討する必要がある	● クラウドコンピューティングにおいては、データがどのサーバに存在するかを容易に確認することができず、国境をまたぐクラウドコンピューティングを利用した場合、特段の対策を講じない限り、異なる法制度や個人情報保護制度を有する国にデータが移転することとなる。（さらに、事業者の倒産リスクやカントリーリスク等もある。） → 特に公的分野において個人情報等の重要なデータを処理する部門においてクラウドコンピューティング事業者が提供するサービスを利用する際には、**クラウドコンピューティング事業者が適切に情報セキュリティ対策を講じていることを委託元において確認**するとともに、**適切なリスクアセスメントを行う**ことが重要。
ネットワーク接続可能な家電製品が増加し、道路交通システムと連携した自動車の自動運転システムが実用化されつつあることに、どのように対応するか	● ネットワークに接続された家電製品（ネットワーク家電）については、情報セキュリティ上の脅威に対応するために、内蔵された組み込み機器のソフトウェアのアップデート等の対策が必要となるが、ネットワーク家電には、ハードウェアを前提とした製造物責任法や消費生活用製品安全法の規制の適用対象となる可能性があるほか、従来PC等で採られてきたような、画面上での約款承認という方式の採用が困難である。 ● 道路交通システムと連携した自動車の自動運転システムなどは、関係主体が複雑化し責任分担が不明確になる一方で、セキュリティ上の問題が発生した際に各主体が適切に連携しながら対処・復旧策を講じることが必要。 → **ネットワーク家電に対して適用される情報セキュリティに関するルールを早急に明確化**するとともに、**国際標準化の動きにも的確に対応**できるようにしていく必要がある。 → **近未来の社会像を予想した上での情報セキュリティに関する制度を検討**していくことも課題である。

論点整理の結果：課題と背景、解決策のまとめ (3) 早期に取り組むべき課題

早期に取り組むべき課題	解決策
情報セキュリティやプライバシーに関わる分野について、近年、次々と新たな課題が生じてきていることにどのように対応するか	● 欧米では、「プライバシーを予め考慮しシステムや手続きを設定すべき」との考え方(Privacy by Design)、「行動ターゲティング広告において自らが追跡されることを許可するかどうか消費者が選択することができるようにする」との考え方(Do not track原則)、情報を「忘れてもらう権利」(Right to be forgotten)等の議論が行われている。 ● 情報セキュリティ対策は従来、「機密性」「完全性」「可用性」の確保によるデータの保護という観点が強く、上述の論点は、少なくとも情報セキュリティ政策の観点からは、国内で活発に議論がなされてこなかった。 ➔ これらの課題は、将来の情報セキュリティ対策にも大きな影響を及ぼしうることから、**情報セキュリティ政策担当部局（NISC）においても、プライバシー問題・個人情報保護制度に係る議論の動向を踏まえて政策を立案**していくことが重要である。
情報セキュリティ対策について、「何を、どこまで行ってよいか分からない」との指摘にどのように対応するか	● 個人情報保護法において実施が求められている安全管理措置について、法律や同法に基づくガイドラインにおいても、どのような事項について対応を行うべきかについては触れられていても、どのような形で実施すべきか、といった点にまでは触れられていない。 ➔ 仮に一律の対応を求めた場合には却って弊害が多くなるとも考えられることから、民間分野を中心に、リスクの分析方法について一定のガイダンスを示し、さらに、リスクの大きさに応じた**適当な対策を例示する形でガイドラインが整備されていくことが望まれる。** ➔ また、官民ともに、リスク分析に基づいた情報セキュリティ対策を実施していくための、**人材育成**を進めていくことが望まれる。

（参考）イギリス、フランス、ドイツ、米国において制定されているマルウエア作成関連の法律 ①

	適用される法律	法律の内容
イギリス	Section 3 of Computer Misuse Act of 1990	(1) 以下の行為をなしたものは有罪である。 (a) 無権限で、コンピューターのコンテンツに改変を加えるいかなる行為をした場合かつ (b) その行為の時点で、必要な意図と必要な認識を有している場合 (2) 意図的に以下の行為を行った場合 (a) コンピューターの作動を損なう (b) コンピューター内のデータないしはプログラムへのアクセスを妨害し、または、遅延させる (c) コンピュータプログラムの動作を損ない、またはコンピュータに記録されているデータの信頼性を損なう
フランス	刑法323条	▪第323 - 1条〔不正アクセス等〕 不法に、コンピュータ（自動データ処理システム）の全体又は1部にアクセスし又は滞留する行為は、2年以下の拘禁刑又は3万ユーロ以下の罰金で罰する。前項の行為により、システム中のデータの消去若しくは改変、又はシステムの動作の悪化が生じた場合、刑は3年以下の拘禁刑又は4万5千ユーロ以下の罰金に処する。 ▪第323 - 2条〔コンピュータ業務妨害〕 コンピュータの動作を妨害し、又は不調にする行為は、5年以下の拘禁刑又は7万5千ユーロ以下の罰金に処する。 ▪ 第323 - 3条〔データの不正操作〕 不法にコンピュータへデータを入力し、又は、そのシステムが収納するデータを不法に消去若しくは改変する行為は、5年以下の拘禁刑又は7万5千ユーロ以下の罰金に処する。 ▪ 第323 - 3条1 法的な権限なしに、第323 - 1条ないし第323 - 3条により禁止されている一つ以上の行為を行うために作成あるいは特に変更された機器、器械、コンピュータプログラムまたは情報を持ち込み、所有し、提供し、送信し、または利用可能な状態にした者は、行為に対して規定された刑罰あるいは最も重い刑罰により処罰される。 ▪第323 - 7条 第323 - 1条ないし第323 - 3条の未遂を既遂と同一の刑で罰することを規定する。

『コンピュータウイルス等有害プログラムの法的規制に関する国際動向調査』(IPA)
(http://www.ipa.go.jp/security/fy11/report/contents/virus/law243.html) をもとに
NRI セキュアテクノロジーズにおいて一部内容の追加・変更を行い作成。

（参考）イギリス、フランス、ドイツ、米国において制定されているマルウエア作成関連の法律 ②

	適用される法律	法律の内容
ドイツ	刑法202条a データの探知	(1) 権限がないのに、自己のために予定されておらずかつ無権限のアクセスに対して特別に保護されているデータを取得しまたは他人に得させた者は、3年以下の自由刑または罰金に処する。 (2) 1項の意味におけるデータは、電子的、磁気的またはその他直接認知しえない形態で貯蔵されまたは伝送されるものに限られる。
	刑法202条b データの獲得	権限がないのに、自己のために予定されていないデータ（第202条a第2項）を、公開されていないデータの伝達又はデータ処理装置の電磁的放出を通じて、自ら取得しまたは他人に取得させた者は、当該行為が他の規定により重く処罰される場合でない限り、2年以下の自由刑又は罰金刑に処する。
	刑法202条c データの探知又は獲得の準備	(1) 第202条または第202条bに規定する行為の準備として、次に掲げるものを製造し、自ら入手しもしくは第三者をして入手・譲受・譲渡・頒布またはその他使用できるようにした者は、1年以下の自由刑又は罰金刑に処する。 1 パスワードその他のセキュリティコードであって、データ（第202条a第2項）の入手を可能にするもの 2 前2条の行為の実行を目的とするコンピュータプログラム (2) 第149条第2項及び第3項は、前項の場合に準用する。
	刑法303 条a データ変更	(1) データ（第202 条a 第2）を違法に消去し、隠蔽し、使用不能にし、または変更した者は、2年以下の自由刑または罰金に処する。 (2) 本条の未遂は罰する。
	刑法303 条b コンピュータサボタージュ（コンピュータ妨害）	(1) 他人にとって本質的に重要であるデータ処理を次に掲げる行為によって妨害した者は、3年以下の自由刑または罰金に処する。 1 第303 条a 第1項の行為をおこなうこと 2 損害を生じさせることを目的としてデータを入力または送信(第202 条a 第2)すること 3 データ処理施設またはデータ貯蔵媒体を破壊し、毀損し、使用不能にし、除去しまたは変更すること (2) (1)において、データ処理が、他人の経営体、他人の企業または官庁にとって本質的に重要である場合、5年以下の自由刑または罰金に処する。 (3) 本罪の未遂は罰する。 (4) (2)において、特に重大な結果を招いた場合、6ヶ月以上10年以下の自由刑に処する。特に重大な結果を招いた場合とは、以下のような場合である。 1 大きな経済的損失を生じさせた場合 2 業務上またはコンピュータ妨害を目的とする集団のメンバーとして実行した場合 3 国民に対する生活必需品または不可欠のサービスの供給、あるいは、ドイツ連邦共和国の国家安全保障を危険にさらす場合 (5) 第202 条cは、(1)の実行の準備活動に対して、必要な変更を加えて適用される。
米国	合衆国法典第18編第47章第1030条(a)(5)(A)	▪ 故意にプログラム、情報、コード、コマンドを送信し、または、保護されたコンピュータにアクセスし、意図的に権限無しで、保護されたコンピュータに損害を与えた場合、処罰される。

『コンピュータウイルス等有害プログラムの法的規制に関する国際動向調査』(IPA) (http://www.ipa.go.jp/security/fy11/report/contents/virus/law243.html)
をもとにNRI セキュアテクノロジーズにおいて一部内容の追加・変更を行い作成。