資料２－２

サイバー空間の安全性・信頼性向上のための課題等について

2011 年 3 月 25 日

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

目次

はじめに

本調査は、「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、「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）」こととされたことを受け、内閣官房情報セキュリティセンターの委託を受け、NRI セキュアテクノロジーズ㈱において実施したものである。

調査にあたっては、「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」を設置し、委員による検討を行った。本文書は、検討会における検討結果を踏まえたものである。

本調査では、サイバー空間の安全性・信頼性を向上させる上で重要となる制度的課題に関し、従来の情報セキュリティ政策の枠組みにとらわれず幅広い観点から検討を行い、海外動向等も踏まえながら、今後我が国において対応が求められる課題について、論点整理を行った。

その結果、論点を「サイバー空間の悪用を抑止するための取組」、「組織における情報セキュリティ対策を推進するための取組 」に大きく分け、さらに、組織だけではなく社会として対応を検討すべき課題については、「新たな課題への対応」としてまとめることとした。

１．サイバー空間の悪用を抑止するための取組

(1)　マルウェアの作成や頒布を抑制する上での課題

我が国においては、マルウェアによる被害が多発しており、特にファイル共有ソフトを媒介として感染が拡大し、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が猛威をふるってきた。

こうしたマルウェアが国内において作成されるケースは現に存在している。例えば、実際に国内で作られたことが判明している悪質なマルウェアとして、感染したパーソナルコンピュータ内のハードディスクに記録された情報を破壊･転送するなどの機能を有する「原田ウイルス」がある((参考1）に原田ウイルス事件判決要約を記載する)。同一の作成者が関与したいわゆる「イカタコウイルス」も、ファイルをイカやタコの画像に書き換えてしまい、データを復旧できなくしてしまうという悪質なマルウェアであった。

いわゆるワクチンソフトの改良は進んでいるものの、マルウェアの種類数（亜種を含む。）の急増と複雑化等[1]により、ワクチンソフトによるマルウェアの検出率低下[2]の傾向は年々強まっている[3]。ワクチンソフトのような技術的な対策は重要である半面、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。

他方で、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。マルウェアがファイルの損壊等を伴う場合には、電子計算機損壊等業務妨害罪（刑法第 234 条の 2）や電磁的記録毀棄罪（同法第 258 条・第 259 条））等を適用しうる場合がある。しかし、これらの刑法規定には他にも固有の要件（例えば、前者については業務妨害のおそれが要件となり、後者についても客体が限定）があることから、これらを必ずしも適用しうるとは限らない。そのような場合であっても、前述した原田ウイルスの場合には、特定人の氏名・顔写真画像情報や、他人の著作物である静止画像情報等が同ウイルスに添付されていたという特殊な構造であったことから、これを作成した者に対し、名誉毀損罪・著作権法違反の罪で有罪判決が言い渡された。これに対し、そのような特殊構造を有しないイカタコウイルスの場合には、これらの罰条を適用することができなかった。この事件にも示されているように、現状では、マルウェアの作成や頒布に対する直接的な処罰規定が置かれていない点においても限界がある。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、さらに広範かつ深刻な被害が多発している。より当罰性が求められるべきこれらの暴露ウイルスについては、前述した刑法規定はもとより、原田ウイルス事件のような罰条を適用することすら、困難であると予測されることから、これらを含んだマルウェア全体について、制度的な対応が必須となる。

---

[1] マルウェア数の経年変化の統計データとしては、たとえば、AV-Test(http://av-test.org/)によるものの他、大手ウイルス対策ソフトウェアベンダによるデータ(http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1038)がある。

[2] 主な理由として、亜種マルウェアを大量に生成する技術の普及により、マルウェアの数が急激に増加したことに伴い、パターンマッチング用データベースを生成するための検体マルウェアを全て収集することが困難となったこと等が挙げられる。

[3] ワクチンソフトのマルウェア検出率についての第三者機関によるテスト結果としては、たとえば、AV-Comparatives.org (http://www.av-comparatives.org/)によるものがある。

ところで、現在、マルウェアは、サイバー犯罪だけでなく、国家を対象とした DDoS 攻撃[4]にも利用されるようになっている。つまり、犯罪者・攻撃者が、インターネットを経由してボーダレスに犯罪や攻撃を行う際のツールとして、国内外において作成・頒布されたマルウェアが利用され、国境を超えて直接的・間接的に被害をもたらすケース[5]が通常となっている。そのような被害[6]を少なくする上で、マルウェアの作成・頒布を規制することが有効であるといえる。しかし、マルウェアの作成・頒布それ自体を規制する法律が我が国には存在しない現状においては、そうした場合に外国法執行機関からの協力要請に対して、国内で強制力を伴った捜査ができない状況にある。我が国がサイバー犯罪のループホールにならないよう、このような面からも国内の法制度を整備することが必要である。

こうしたマルウェアの作成行為や頒布行為について、英・仏・独等の欧州各国および米国では規制法が制定されている((参考２)にイギリス、フランス、ドイツおよび米国におけるマルウェアの作成行為や頒布行為を規制する法律を記載する)ものの、我が国においては現状において当該行為を直接規制する法律が存在していない。ワクチンソフトの改良等、技術的な対策を進めるとともに、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、マルウェアの作成や頒布行為を規制するにあたっては、ワクチンソフトの改良等をはじめ、ソフトウェアに関連する各種の正当な研究・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。

※ マルウェア：コンピュータウイルス、ワーム、スパイウェア等のコンピュータ及び利用者に害を与える悪意あるソフトウェアのこと

---

[4] この場合、マルウェアは、PC をボット化する(DDoS 攻撃を実行するためのボットネットを構築する)ために使用され、マルウェアに感染した PC は、所有者が気づかないうちに、所有者の意思とは無関係に DDoS 攻撃(の一部)を実行する。(この場合、感染した PC のユーザーは加害者となり、DDoS 攻撃を受けた側が被害者となる。)
大手マルウェア対策ソフトウェアベンダによれば、2010 年 10 月時点で、グローバルでのボット数は、340 万～510 万と推定されている。出所) http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened
ボットネットを根絶するためには、PC のマルウェアへの感染を抑止することが重要であるが、近年、ユーザーに気づかれないように感染するマルウェアが増加しており、マルウェア対策ソフトウェアの検知率が低下していることと相まって、エンドポイントにおける対策だけでは解決が難しい状況である。ネットワーク側におけるボットネット対策の取り組みの一つに、総務省・経済産業省の連携プロジェクトであるサイバークリーンセンター(CCC) があり、一定の効果をあげている。このような取り組みをグローバルに展開することも、マルウェアに起因する各種のサイバー犯罪の被害を少なくする上で有効ではないだろうか。

[5] たとえば、2010年10月に摘発された東ヨーロッパの国際的な犯罪組織は、米国の小規模な企業や個人のコンピュータに Zeus として知られるマルウェアを感染させ、コンピュータからユーザーのオンラインバンキングの口座の情報やパスワードを盗み出し、被害者の口座から米国内にいる仲介人の銀行口座に金を転送していた。http://www.bbc.co.uk/news/world-us-canada-11457611

[6] サイバー犯罪による被害額の具体的な例として、イギリス政府が 2011 年 2 月に、サイバー犯罪が同国経済にもたらす被害額は年間 270 億ポンド（約 3 兆 6000 億円）に達し、同国の国内総生産（GDP）の約 2%に相当すると発表している。
http://jp.wsj.com/layout/set/print/World/Europe/node_184751

（参考 1） 原田ウイルス事件判決要約

京都地裁平成 20 年 5 月 16 日判決（平成 20 年(わ)第 155 号，同第 232 号 著作権法違反，名誉毀損被告事件）

【判決要約】

本件は、被告人が、いわゆるコンピュータウイルス２種類を自ら作成した上、上記ウイルスの情報が記録されたハードディスク内蔵のパソコンを用いてインターネット接続した状態で、事前に起動させていたファイル共有ソフト「Winny」を作動させ、これらを不特定かつ多数の同ソフト利用者らにおいて受信・閲覧等が可能な状態にしたという事件である。以下、本判決が認定した事実に従って説明する。

被告人は、大学の同一学部・同一学科に当時在籍していた被害者甲に対する妬みなどから、甲をからかうとともに、被告人が作成したコンピュータウイルスが有名になることを企図して、次の各犯行に及んだものである。

最初に、被告人は、コンピュータウイルス A を作成した上、これを受信・閲覧可能な状態にした（第１の犯行）。ウイルス A は、利用者のパソコン内のハードディスク上の情報を破壊するなどの機能を有するものであった。ところが、ウイルス A は被告人の思惑通りに機能しなくなったことから、被告人は、別のコンピュータウイルス B を作成し、これを自動公衆送信した（第２の犯行）。ウイルス B は、上記「Winny」利用者のパソコン内のハードディスク上の情報を破壊・転送するなどの機能を有するものであった。しかし、被告人は、第１の犯行について、甲がウイルス A の作成者であると感染者に思わせるような文言や甲の実名、住所等を記載し、甲の顔写真を表示した画像情報をウイルス A に添付した上、アニメーション作品等の動画ファイルに偽装し、ファイル共有ソフト利用者らが受信・閲覧し得る状態にし、同利用者である乙らをしてこれを閲覧させたので、本判決は、この行為を、A に対する名誉毀損罪（刑法第２３０条第１項）に該当するものとした。

次に、上述のとおり、ウイルス A は被告人の思惑通りに機能しなくなったことから、被告人は、第２の犯行として、丙が制作し著作権を有する著作物であるアニメーション作品の静止画像情報にウイルス B を添付したものを画像ファイルに偽装した上、Winny 等で自動公衆送信するようになった。

本判決は、この行為が、著作権（公衆送信権）侵害（著作権法第１１９条第１項、第２３条第１項）に該当するとともに、上記著作者丙の名誉又は声望を害する方法により、その著作物を利用して著作者人格権を侵害したもの（同法第１１９条第２項第１号、第１１３条第６項）に該当するとした。本判決は、以上の判示第１、第２の犯行について、被告人に対し、懲役２年、執行猶予３年の刑を言い渡している。

【解説】

我が国にはコンピュータウイルスの作成、所持行為等を処罰の対象とする法律が存在しないので、本件でも、これらの作成、所持行為それ自体は起訴の対象とされていない。本件では、第１の犯行については甲の名誉を毀損する記載等を有するものであったことから名誉毀損罪の成立が、第２の犯行については丙の著作物の静止画像情報を用いたことから、著作権法違反の罪の成立が、それぞれ認められた。しかし、上記記載等、又は上記静止画像情報が存在していないような、一般的なマルウェアの事案では、当然のことながら、これらの罪の成立は認められない点で限界を有している。

（参考 2） ヨーロッパおよび米国におけるマルウェアの作成行為や頒布行為を規制する法律[7]

◆ イギリス

適用される法律 ： 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) コンピュータの作動を損なう

(b) コンピュータ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

適用される法律 ： 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 1 の未遂を既遂と同一の刑で罰することを規定する。

◆ ドイツ

適用される法律 ： 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取得させた者は、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。

適用される法律 ： 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

[7]『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で一部内容の追加・変更を行い作成。

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。

適用される法律 ： 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。

適用される法律 ： 刑法 303 条ａ データ変更

⑴ 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。

⑵ 本条の未遂は罰する。

適用される法律 ： 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）

⑴ 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

⑵ ⑴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。

⑶ 本罪の未遂は罰する。

⑷ ⑵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

⑸ 第 202 条ｃは、⑴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

適用される法律 ： 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。

⑵　その他の課題

我が国においては、不正アクセス禁止法が制定され、ID、パスワードを窃取した上で他人のコンピュータシステム等のアカウントにログインすることは禁止されている。他方で、サイバー空間においては、容易に外国の組織からも攻撃を受けうるところであり、国際的に協調してサイバー空間を一層安全にしていくことが重要である。この観点から、サイバー空間の悪用を抑止する制度に関しては、我が国と外国それぞれの制度の違いを常に検証していくことが重要である。

また、サイバー攻撃による被害を受けた場合のリカバリ策や事業継続性の確保策（事業継続計画（BCP）の策定等）も同時に充実させていくことが重要である。（その他の情報セキュリティ関連の事故対応の在り方については、次項においても触れることとする。）

２．組織における情報セキュリティ対策を推進するための取組

(1)　事故を前提とした対策実施を促す制度設計の必要性

情報セキュリティに係る事故の可能性を完全に排除する情報セキュリティ対策の実現は容易ではない。例えば、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。情報セキュリティ対策の実施にあたっては、事故の発生を前提として対応力を高めていく必要があり、事故が起こった際に被害の発生・拡大を防止するための取組も、事故の発生を未然に防ぐ取組と同様に重要である。

また、情報セキュリティ対策の観点からは、変化するリスクを把握し、それに見合った対策を実施することが重要である。こうした観点からは、法律等の制度設計においても、単に事故の発生を罰するという視点だけではなく、事故の発生も視野に入れた適切な対策の実施を促す視点が重要である。なお、欧州では、1995 年に発令された個人情報保護指令[8]の改定が議論されており[9]、この中で事故発生時の公表義務等の軽減[10]と、企業による情報セキュリティ対策の適切な実施の推進[11]が併せて議論されているところである。

この点、情報セキュリティ対策のうち、特に個人情報保護の漏えいについては、個人情報保護法に基づく主務官庁のガイドラインにおいて、二次被害の防止等の観点から、本人への連絡、公表、そして主務官庁への通知が求められてきたところである。一方、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きている。

この点について、例えば、総務省が平成 22 年 7 月に改訂したガイドライン[12]においては、情報漏えいを起こした本人に対して二次被害が生じないよう適切な技術的保護措置が講じられている一定の場合において、本人連絡、公表の義務を除外し、主務大臣への報告も四半期ごとの報告に義務を緩和している。また、経済産業分野ガイドライン[13]においても、情報漏えいを発生させた事業者が行っていた対策や情

---

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

[9] Consultation on the Commission's comprehensive approach on personal data protection in the European Union
COM(2010) 609 final：A comprehensive approach on personal data protection in the European Union
http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[10] 事故発生時の公表義務の軽減に向けた施策として以下が挙げられている。
- 独立したデータ保護責任者の任命を義務化し、彼らの業務と能力に関連するルールの整合性を確保する。その際には、特に小規模企業や零細企業について、過度の管理負荷がかかることを避けるために、適切な閾値を設けることについても考慮する。
- 法的なフレームワークに、特定の状況において、データコントローラがデータ保護影響評価を実施することを義務化する。特定の状況とは、たとえば、機微性の高いデータを処理する場合、あるいは、処理のタイプが特定のリスクに関わるものである場合、特にプロファイリングやビデオによる監視を含む特定の技術やメカニズム、手続きを使用する場合である。
- さらなる プライバシー強化技術(Privacy Enhancing Technologies) の使用と、システムの構築や手続きの設定において予めプライバシーを考慮する(Privacy by Design)コンセプトの具体的な実装を推進する。

[11] 企業による情報セキュリティ対策の適切な実施のための具体的な施策として以下が挙げられている。
- 行動規範(Codes of Conduct)の積極的な推進を含む自発的な規制に向けたイニチアチブのさらなる促進のための方法の検証
- プライバシーおよびデータ保護の分野における EU 認証スキームの確立が現実的かどうかの検証。認証スキームとは、たとえば、プライバシー保護に準拠した手続き、技術、製品、サービスに対してプライバシーシールを付与するというものである。

[12] 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（平成 22 年 7 月 29 日総務省告示第 276 号）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html

[13] 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン(平成21年10月9日厚生労働省・経済産業省告示第2号)
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

報漏えいの態様に応じて本人連絡、公表の義務を緩和しているところである。

いわゆる「漏えい」が発生した場合に行うべき対応として、本人通知や公表といった二次被害防止策に加えて、事前対策として、暗号化等の技術的な二次被害防止策の実施についても選択肢とすることによって、事故発生後の被害を防止するための技術的対策の実施を促すことが可能になると考えられる。こうした観点から、消費者庁の標準ガイドライン[14]や主務省庁のガイドラインが検討されていくことが望まれる。

なお、技術的な対策の普及を推進していく上では、情報の重要度に応じた対策を実施していくことが重要であり、関係省庁において適切な技術的保護措置の在り方を具体的に示していくことも重要である[15]。

⑵ クラウドコンピューティングを巡る課題

複数国間にまたがってクラウドコンピューティングシステムを構築することは、今や現実のものになっているが、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は確認することができない。このため、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。

このため、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しておくことが重要である。同時に、クラウドコンピューティングには、事業者が倒産するリスクや外国政府による介入を受けるリスク（カントリーリスク）等が存在するところであり、かかる重要データの処理をクラウドコンピューティング事業者に委託する際は、適切にリスクアセスメントを行っておくことも重要である。

これに関連して、地方自治体における ASP・SaaS の導入の際の参考に資するため、「地方公共団体における ASP・SaaS 導入活用ガイドライン」（総務省　平成 22 年 4 月）[16]がまとめられ、ASP・SaaS における情報の取扱いに関して事前に調整すべき事項や予期せぬ脅威への対応などについても触れられている。また、総務省内に設置された「自治体クラウド推進本部」における「有識者懇談会取りまとめ（案）」（平成 23 年 1 月 20 日）[17]でも、クラウド導入に係る諸課題として、情報セキュリティに係る法的留意点に触れられている。また、政府機関の情報セキュリティ対策のための統一基準群においても、

---

[14] 個人情報の保護に関するガイドラインの共通化について
http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou2.html
http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou/kyoutuuka2.pdf

[15] 総務省の『利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会』の第二次提言では、手続(本人への通知、事実の公表、監督官庁への報告)の簡略化が可能となる適切な技術的保護措置が実施されているのは、以下のすべてが満たされた場合であるとしている。
① 公的機関が推奨する暗号アルゴリズム（電子政府推奨暗号リスト、ISO/IEC 18033 に掲載されたもの）による情報の暗号化
② 暗号化された情報及び復号鍵の適切な管理
③ 個人情報の漏えい等に際し、①、② の措置が有効に実施されていること
また、技術の安全性が変化することや、より安全性の高い技術が登場することも考えられ、適切な技術的保護措置については、必要に応じて見直しを実施することが適当であるとしている。

[16] http://www.soumu.go.jp/main_content/000061414.pdf

[17] http://www.soumu.go.jp/main_content/000099227.pdf

統一管理基準及び統一技術基準に、クラウド技術を活用するにあたっての情報セキュリティ上の配慮事項を追加することが検討されている。（平成 22 年 12 月 28 日パブリックコメント募集開始）[18]

クラウドコンピューティングにおける情報セキュリティに関しては、総務省の「スマートクラウド研究会」（平成 22 年 5 月報告書とりまとめ）[19]や、経済産業省の「クラウドコンピューティングと日本の競争力に関する研究会」（平成 22 年 8 月報告書公表）[20]など、国内で活発な議論が行われ、ジャパン・クラウド・コンソーシアム[21]などの産官学連携のための組織も設立されているところである。また、経済産業省の「クラウドサービスの利用のための情報セキュリティマネジメントガイドライン」（平成 22 年 11 月パブリックコメント募集開始）[22]のような、委託先のクラウドサービス事業者も対象として包括的に JIS Q27000 シリーズを適用するための手引き書も作成し、ISO の場での国際規格化を目指しているところである。

(参考 3)に、国内におけるクラウドコンピューティング関連の取り組みの概要をまとめる。

（参考 3）国内におけるクラウドコンピューティング関連の取り組みの概要（一部抜粋）

◆ 【総務省】「地方公共団体における ASP・SaaS 導入活用ガイドライン」（平成 22 年 4 月）

地方公共団体がインターネット ASP を導入し、個人情報などの機密性の高い情報の処理などを行う場合は、インターネットが不特定多数の者に利用されているものであることに十分に留意する必要がある。具体的には、インターネットで行政情報の処理などを行う場合は、地方公共団体組織認証基盤（LGPKI）から発行された電子証明書による暗号化やアクセス制御を行ったり、あるいは VPN（仮想専用網）などを取り入れたりするなど、情報セキュリティの確保に配慮が必要である。（報告書ｐ17）

地方公共団体が住民情報などの機密性が求められる情報を扱う業務にインターネット ASP を活用する場合、事業者のデータセンターやバックボーンの構成についても留意した慎重な検討が必要である。（報告書ｐ18）

LGWAN-ASP は、サービスの提供にあたり、LGWAN への接続要件を満たすことについて所定の審査を受けた上で LGWAN への接続許可を受けることが必要である。この点からも、LGWAN-ASP のサービスは一定のセキュリティの要件を満たしていることが保証されているといえる。LGWAN を利用できるのは地方公共団体のみであり、機密性の高い情報を取り扱うことの多い地方公共団体の業務に対して、ASP･SaaS を導入する場合、まずは LGWAN-ASP の活用を検討することが望ましい。（報告書ｐ19）

ASP･SaaS のサーバは庁舎外のデータセンターで管理されているため、庁内システムと外部の接続にあたっては、ASP･SaaS までのネットワーク回線について、セキュリティポリシーに則したセキュリティが保証されていることを確認する必要がある。（報告書ｐ44）

◆ 【自治体クラウド推進本部】「有識者懇談会取りまとめ（案）」（平成 23 年 1 月 20 日）

➢ 情報セキュリティ等向上効果（システムの性能向上効果）

⑤ 安全性（セキュリティ）

[18] http://www.nisc.go.jp/active/general/kijun5.html
[19] http://www.soumu.go.jp/menu_news/s-news/02ryutsu02_000034.html
[20] http://www.meti.go.jp/press/20100816001/20100816001.html
[21] http://www.japan-cloud.org/
[22] http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595210034&Mode=0

必要な利用制限の設定と不正アクセスの防止等の技術的な管理策とともに、情報セキュリティ教育等を体系的に実施し、安全性を確保できること。(報告書案ｐ5、ｐ6)

➢ 情報セキュリティに係る技術的対策

自治体クラウドの安全安心確保のために必要なものとして以下の 3 つがある。

ⅰクラウドの狭義のセキュリティ対策（Security）

ⅱバグや故障・災害などへの対策（Dependability）

ⅲサービス提供者へのトラストの確保対策（Trust）

このうちここで扱うセキュリティに関してはクラウドへの攻撃とクラウドを用いた攻撃の両方を考えておく必要がある。(報告書案ｐ8)

➢ 情報セキュリティに係る法的留意点

自治体とクラウドサービス事業者間の権利義務関係は、原則としてサービス提供契約の内容によって定まるので、必要な情報セキュリティに係る項目をあらかじめ契約内容に盛り込んでおかなければならない。しかし、契約によるコントロールには一定の限界もあることから、次のような点にも留意すべきである。

例えば、サーバ所在地国の法令によって、当該国の政府に対して通信の内容を開示する義務が課されている場合には、データの機密性が保たれない場合がある。これは、当事者の合意の有無に関わらず存在するリスクである。このような課題に対応し、SLA 等を確実に担保するためには、契約における規定でデータセンターの設置場所やアクセス可能な区域を国内に限定する必要がある。また、民事裁判管轄・準拠法についてもサービス提供契約に特約が置かれることが一般的であるが、国内でなければ事実上の限界が生じる場合がある。(一部抜粋)（報告書案ｐ9)

◆ 【総務省】 スマートクラウド研究会」（平成 22 年 5 月報告書とりまとめ）

消費者（利用者）の権利を保障する観点から、クラウドサービスの種類に応じたメリットやデメリット、クラウドサービスを利用する際のリスクと責任等、消費者の権利や資産を適切に保護しつつ、クラウドサービスの利用を促進するための指針策定等について、クラウド事業者、利用者、監査法人等の有識者により、民間主導で進めることが適当である。その際、大地震の発生などによるネットワークの分断に対処するための BCP の策定など、リスク分散の対処方法についても指針に盛り込むことが必要である。

こうした取り組みを通じ、データ流出の懸念などセキュリティを重視したクラウドサービスについては日本のクラウドサービスを利用するなど、利用者のニーズに沿ったクラウドサービスの利用が可能となる。(報告書ｐ25)

◆ 【経済産業省】クラウドコンピューティングと日本の競争力に関する研究会」（平成 22 年 8 月報告書公表）

➢ クラウドサービスの技術的標準化の動向

ベンダロックインを回避するため、クラウドコンピューティング間の相互接続性を確保しようとする動きが活発になり、いくつの標準化団体がその検討を行っている。

CSA(Cloud Security Alliance)は、クラウドコンピューティングにおけるセキュリティのあり方を提唱。ユーザーとプロバイダ両方に向けて教育の場所を提供。(報告書ｐ41)

➢ 情報セキュリティ監査制度の検討

クラウド利用者がクラウドコンピューティング環境のセキュリティレベルを比較検討することができるよう、クラウド事業者がセキュリティ対策の概要を表明するための標準様式を検討し、この様式に準拠した情報公開を促進する。

上記の表明が正しく実装、運用されていることを客観的に確認するため、既に一般に利用されている情報セキュリティ

監査制度を活用し、クラウド事業者のセキュリティレベルに一定の保証を不えることで、企業ユーザのクラウドコンピューティング移行を促進する。（報告書ｐ57、ｐ58）

- 適用範囲

ガイドラインは，クラウドサービス利用における情報セキュリティ管理の確立、導入、運用、監視、見直し、維持及び改善のための実施の手引を提供するものである。JIS Q27002:2006 に加え、クラウドサービス利用時に実施することが望ましい管理策及び実施の手引について記述している。

他方で、海外に目を転じれば、米国 NIST が公的分野でクラウドコンピューティングを利用するにあたってのセキュリティ確保及びプライバシー確保に関するガイドライン[23]を策定しつつある。

クラウドコンピューティングについては、現時点で未だサービスや技術の発展期であり、クラウドコンピューティングを利用したサービスや技術の振興という視点も持つ必要がある。

他方で、クラウドコンピューティングを巡る規格化の動きについては、我が国としての立場を積極的に反映させるため、国際的な基準策定の動きに積極的に参画していくことが望まれる。

また、海外にデータを移転することについてのリスクアセスメントを行う上で必要となる、諸外国の個人情報保護制度や司法制度の概要等については、欧米を除き分かりやすい形で国内に紹介されていないところである。この点に関し、例えば第 2 回日 ASEAN 情報セキュリティ政策会議（2010 年 3 月にバンコクにて開催）において、我が国と経済的なつながりの深いアジア各国との間で、国際的なデータの移転や関係する諸制度について調査等を検討することが提案されているところである。

（3） その他の課題

組織における情報セキュリティ対策については、「何を、どこまで行ってよいか分からない」との指摘が常に存在してきたところである。例えば、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は、法律上は詳しい内容が書き込まれておらず、詳細は主務大臣が定めるガイドラインに委ねられている。主務大臣が定めるガイドラインにおいても、一般的には、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、それを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。

他方で、（１）でも触れたように、本来、情報セキュリティ対策は、リスク分析の結果に基づき、リス

[23] NIST SP 800-144：Guidelines on Security and Privacy in Public Cloud Computing
http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf
クラウドサービスを利用する際の留意点として以下を挙げている。
- クラウドコンピューティングソリューションを利用する前に、そのセキュリティとプライバシーの側面について、注意深く計画する。
- クラウドプロバイダが提供するパブリッククラウドコンピューティング環境を理解し、クラウドコンピューティングソリューションが、組織のセキュリティおよびプライバシーに対する要求を満たすことを確認する。
- クライアント側のコンピューティング環境が、クラウドコンピューティングに対する組織のセキュリティおよびプライバシー要求を満たすことを確認する。
- パブリッククラウドコンピューティング環境において実装・導入されているデータやアプリケーションのプライバシーとセキュリティに関する説明責任を維持する。

ク相応の対策を行うべきものである。このため、どのような情報に対してどの程度の対策を講ずべきかといったことや、どのリスクに対してどのような対策を実施すべきかについての基本的な考え方が確定しない限り、規則として具体的な対策を示すことは難しく、仮に一律の対応を求め違反時に厳格なペナルティを課した場合には却って弊害が多くなるとも考えられる。

このため、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、現時点では、情報セキュリティ分野における人材が不足していることから、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。

また、社会保障・税に関わる番号制度についての基本方針（社会保障・税に関わる番号制度に関する実務検討会（平成 23 年 1 月 31 日））[24]では、「番号制度に係る個人情報保護法制の円滑な執行と適切な運用を担保するために設置される第三者機関の在り方について、具体的検討を行う」こととされている。その際、第三者機関の在り方の検討とあわせて、番号制度を運用するシステムの情報セキュリティ対策を一層推進する方策を整えることが重要である。

[24] http:/www.cas.go.jp/jp/seisaku/bangoseido/pdf/110131/honbun.pdf

３．新たな課題への対応

(1) 情報セキュリティ／プライバシー問題の急激な変化

情報通信技術分野における急速な変化を背景に、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は、近年、次々と新たな課題が生じてきており、欧米の関係機関による対応策の検討が行われている。例えば、米国の公正取引委員会(FTC)は、2010 年 12 月に、消費者のインターネット上における行動に関する情報の企業による収集・利用について、プライバシー保護の観点から企業が実施すべき対策や消費者に提供すべき選択肢に関する報告書[25]を公表しており、その中で、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であるとする Privacy by Design[26]という考え方や、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を消費者が選択することができるようにする（Do not track 原則）[27]という考え方について言及している。

一方、EU においても、技術革新や経済活動のグローバル化を背景として、2010 年 11 月に個人情報保護指令を改正し包括的なルールを策定するための伝達文書(COMMUNICATION)[9] を公表し、その中で情報を「忘れてもらう権利」（Right to be forgotten）[28]等について触れている。この文書では、1995 年の個人情報保護指令の目的および原則は現在においても有効であるとしながら、技術革新・グローバル化によって個人情報保護に関する新たな課題が提起されたことにより、個人情報保護指令の改正が必要になったとしている。特に個人情報の収集方法が精巧なものとなり、個人情報がいつどこで収集されているのかを検知することが難しくなったことにより、従来の個人情報保護指令が新たな課題に十分かつ効果的に対処することができるかどうかについて疑問が生じているとしている。さらに、OECD においても、情報セキュリティ／プライバシーガイドライン[29]の更なる改定に向けた作業が開始されようとしている。

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かったが、情報を「忘れてもらう権利（Right to be forgotten）」は、個人による個人情報の削除権を明確化することを、「Do not track 原則」は、個人のインターネット上での行動を企業等が追跡すること

---

[25] Protecting Consumer Privacy in an Era of Rapid Change　http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[26] COM(2010) 609 final における(Privacy by Design)の定義は、以下のようなものである。
プライバシーおよびデータの保護が、技術のライフサイクル全体、つまり、初期の設計段階から技術の導入、使用、最終的な廃止の全ての段階にわたって組み込まれていること。

[27] FTC の報告書には以下の記述がある。
FTC は、これまで繰り返し企業等に対して、消費者がインターネットでどのサイトを閲覧したのかに関するデータの収集・利用を消費者自らの手によってコントロールすることができるツールを開発するよう要求してきた。これに対応して、いくつかの企業が、消費者がターゲティング広告を受信するかどうかをコントロールし、企業がターゲティング広告を行うために収集した情報の確認や操作を行うためのツールを開発した。行動ベースの広告がもたらすベネフィットを減じることなく、かつ、ユニークな識別子を登録することなく(プライバシー問題を避けるため)、消費者が、行動ターゲティング広告についてコントロールを行うことができるようにするための方法として、FTC は、ブラウザベースのメカニズムを推奨する。

[28] COM(2010) 609 final には、『忘れてもらう権利（Right to be forgotten）』について以下の記述がある。
『忘れてもらう権利』とは、個人が、自身に関する個人データが、もはや正当な目的のために必要ではない場合に、当該個人データが今後取り扱われることがないよう削除されるようにすることができる権利である。たとえば、データの取り扱いが個人の同意に基づいて行われていたが、個人が同意を取り下げた場合や、データの保存期限が経過した場合が該当する。

[29] プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告（1980 年 9 月）
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

に関して、どこまで追跡されることを許容するのかを個人が選択する権利を行使する方法を単純化することを意図したものである。少なくとも情報セキュリティ政策の観点からは、これらの論点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、現在、諸外国において議論が急速に動いている分野であり、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状況となってきていることから、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。

現在、欧州では、プライバシー保護についての規格化の議論が行われているところであり、端的には国際標準化という形で、国際的制度調和に向けた議論がスタートすることも考えられる。我が国として、これらの論点について国際的な議論にも積極的に参加できるよう、国内関係者による議論の開始などに早急に着手することが求められる。

（2） 情報通信技術の利用環境の変化に応じた対応

近年、ますます多くの組み込み機器がネットワークに接続されるようになってきており、ネットワーク接続可能なテレビ等の家電製品（ネットワーク家電）が増加しつつある。

ネットワークに接続された家電製品については、情報セキュリティ上の脅威に対抗するために、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ってくる。 他方で、これらの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、ソフトウェアアップデート時の画面上での約款承認といった方式を採用することが困難であるという側面もある[30]。

我が国において、こうしたネットワーク家電は今後も増加するものとみられ、また、今後我が国の主要な輸出製品となる可能性もある。このため、我が国において、ネットワーク家電製品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、それらのルールについて今後予想される国際標準化の動きに対しても的確に対応できるようにしていく必要がある。

また、将来において、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し、ネットワーク家電が多くの家庭に普及した場合には、各種製品の情報セキュリティを所管する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

---

[30] IPA の報告書『自動車と情報家電の組込みシステムのセキュリティに関する調査』に、情報家電のセキュリティ対策を考える上で検討すべき項目として、以下が記述されている。
a）情報リテラシーが充分でない利用者が存在する可能性
b）情報等資産の多種多様化、範囲拡大の可能性
c）オークションや譲渡による情報の漏洩の可能性
d）セキュリティ対策が不十分な情報家電が混在する可能性
e）何が繋がり、誰が利用しているか、把握できなくなる可能性
f）着脱機器やテレメトリングによる情報の拡散の可能性
g）偽のダウンロードパッチを受け入れてしまう可能性
h）情報家電経由でインターネットの不正サイトにアクセスしてしまう可能性
i）宅内ネットワークのセキュリティ設定が行われていない可能性

対処・復旧策を講じる必要性は一層高まるものと考えられる。

　また、製品の仕組みを熟知しないユーザーにおいても、容易にかつ間違いなく実施可能な情報セキュリティ対策を用意するとともに、ユーザーの意識向上・啓発を今まで以上に積極的に推進しなければならないという課題も想定される。こうした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今後の課題と考えられる。

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

委員名簿（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）