暗号技術による個人情報保護の制度と技術の動向

セコム株式会社 IS 研究所
松本　泰、伊藤　忠彦

1. はじめに

個人情報を適切に保護するための暗号技術については、個人情報保護法が施行された当時から現在に到るまで、様々な議論があったようです。個人情報に限らず、暗号技術により情報を保護するためには、「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」、それらすべてが適切である必要があります。

7月3日に開催された「JNSA ／第2回 鍵管理勉強会」ではこうした暗号技術・鍵管理技術のあるべき姿と、これらの技術が制度にどう組み込まれていくべきか等を念頭に、「暗号技術による個人情報保護の制度と技術の動向」を勉強会のテーマとして取り上げ、議論を行いました。

本稿では、鍵管理勉強会の議論も踏まえ、日本と米国の状況を説明し、今後の日本における課題を考察します。

2. 我が国における議論と現状

我が国の個人情報保護法は、2003 年に成立し、2005 年から全面施行されましたが、同法の施行は、情報セキュリティ業界に対しても非常に大きなインパクトがありました。こうした中、同法第 2 条第 1 項と第 20 条について、個人情報の解釈と暗号技術の扱いに対して、過去からいくつかの議論があったようです。以下に同法第 2 条 1 項と第 20 条を示します。

法第 2 条第 1 項
この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

法第 20 条
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

同法に対しては、主務官庁が作成するガイドラインが 40 以上存在し、その中でそれぞれが第 2 条第 1 項と第 20 条の解釈を示しています。例えば、「個人情報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」（経済産業省 2009 年改訂）では、同法第 2 条第 1 項の「個人情報」について「暗号化等により秘匿化されているかどうかを問わない」としています。同時に、同ガイドラインは同法第 20 条の対策として「高度な暗号化等による秘匿化を講じる事は望ましい」としています。また、漏えい時には「影響を受けた本人及び主務大臣に報告することが望ましい」としていますが、「高度な暗号化等の秘匿化が施されている場合」は本人への連絡は省略して構わないとしています。

一方「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（厚生労働省）では、個人情報の定義として「暗号化されているか否かを問いません」としていますが、別紙の Q & A では、「『個人に関する情報』であっても、暗号化により特定の個人を識別できなければ『個人情報』に該当しません」としています[1]。他にも多くの主務官庁毎のガイドラインがありますが、「安全管理措置」における暗号化等の扱いについては、様々な解釈がなされており、かつ、曖昧な扱いになっているように見受けられます。例えば、経済産業省のガイドラインでの「高度な暗号

[1] 厚生労働省の Q&A では、医療情報を 2 次利用する場合の、連結可能匿名性のために識別子の暗号化を意識したものだと思われます。

化」や厚生労働省のQ＆Aにある「特定の個人を識別できない暗号化」が何を指すかは明確に規定されていません。

2010 年 5 月に総務省の「利用者視点を踏まえた ICT サービスに係わる諸問題に関する研究会」の第二次提言では、安全管理措置を講じる際の考え方や技術的保護措置について、暗号技術のみでなく、認証、鍵管理等についても触れています。しかし技術紹介に留まっており、それらの技術を活用させる制度については触れていません。こうした状況に対して内閣官房情報セキュリティセンター（NISC）が主催する「情報セキュリティ政策会議」が 2010 年 5 月に公表した「国民を守る情報セキュリティ戦略」には、以下の記述があります。

> **個人情報保護の推進**
> 各事業分野ごとの個人情報保護に関するガイドラインの見直し、企業から個人情報等の情報の漏えいを防止する観点から、情報の適切な暗号化等を促進するため、漏えいした個人情報に適切な技術的安全管理措置が施されていた場合の手続の簡略化等、各事業分野の特性を踏まえつつ、事業者に暗号化等を行うインセンティブを付与するための見直しを行う。

「国民を守る情報セキュリティ戦略」の指摘は、内閣府の個人情報保護専門調査会でも検討されたように見受けられますが、この調査会が 2011 年 7 月に発行した報告書には、以下のような記述があります。

> 公的な認証制度がないため、法令で求めるレベルに十分な安全管理措置の判断基準はどのように確保するのかが課題である。

現在の我が国において、暗号技術による個人情報の保護は有用だという認識はあり、様々な活動はあるのですが、それを支えるスキームが不十分といった状況にあるのではないでしょうか。

3. 米国 HITECH 法の事例

前節で、日本における「暗号技術による個人情報保護」の状況について説明しましたが、では海外ではどういう状況なのか気になるところです。ここでは、米国の医療分野の事例、具体的には、米国 HIPAA/HITECH 法の事例を説明します。

米国においては、1996 年に医療情報のプライバシー保護等を包括する法律である HIPAA[2] が成立しました。しかしながら、適用対象事業体が医療機関のみ、取り締まり権限を保有するのが健康福祉省[3] のみ、情報漏えいに対する罰則が軽いなど、その適用対象や権限が十分でないという指摘がありました。それらを受け、2009 年に米国再生・再投資法[4] の一部として成立した HITECH 法[5] では、HIPAA 適用対象事業体に対し機密性に関する追加要項が課せられました。HITECH 法では HIPAA の罰則規定も大幅に拡大されました。例えば、個人識別可能な医療情報を漏えいした場合は、最大で 10 年の懲役及び 150 万ドルの罰金（1 件については最大 5 万ドル）が課せられる可能性があります。また、健康福祉省以外に州の司法長官にも取り締まり権限が与えられました。

HITECH 法の漏えい通知ルール

HITECH 法おいて、特に個人情報・プライバシー保護との関連性が高い要項として、保護医療情報[6] が漏えいした場合に対象者全員への通報を義務付け

[2] Health Insurance Portability and Accountability Act
[3] HHS：Department of Health and Human Services
[4] ARRA：American Recovery and Reinvestment Act
[5] Health Information Technology for Economic and Clinical Health Act)
[6] PHI：Protected Health Information

るとともに、うち 500 人分以上の保護医療情報が漏えいした場合に、健康福祉省、連邦取引委員会[7]及びメディアに対して通報を行うよう義務付けている点があります。

HITECH 法における個人情報漏えいとは

HITECH 法において、情報が安全でなく（unsecure）、健康福祉省及び連邦取引委員会に通報義務が発生する事態を明示するため、健康福祉省は保護医療情報についてのガイドラインを更新し、無権限者による使用、判読、及び復号をできなくするための、暗号化と破棄についての技術と方法論を記載しています。
同法では、それらの技術と方法論で守られた情報が漏えいしても、NIST[8] の技術ガイドラインに記載される方法（表 1）による暗号化又は破棄が為されているならば、安全（secure）な医療情報であるとしています。

HITECH 法のスキーム

HITECH 法において適用対象事業体（Covered entity）に対する主務官庁は健康福祉省なのですが、技術的なガイドライン、HITECH 法で要求される情報システムの試作、技術や啓発活動促進のための R & D プログラム、テストデータ等を NIST が提供しています。また、個人情報を適切に保護するための暗号技術、その暗号モジュールの安全性を試験する CMVP[10] も NIST が行っています。このように、医療サイドの要望ベースの法案を、NIST が技術的にサポートするスキームになっています。（図 1）

CMVP は、米国政府機関が暗号技術ソリューションを調達する際の基準ですが、客観的な評価がもとめられる暗号技術ソリューションでは、評価の難しさもあり、CMVP のような評価・認証制度が重要な意味を持つ様になりました。CMVP の基準達成は、暗号技術ソリューションベンダーにとって高いハードルだったのですが、そのハードル越えを米国政府が支援することにより、ベンダーを育成した側面もあります。HITECH 法の法制度においても、高額な罰金などの刑事罰を規定する一方で、通知義務を守れば一定の範囲内で罰が軽減される可能性があり、CMVP により認証された暗号技術ソリューションの選択は利用者（適用対象事業体）のインセンティブとして働いているようです。

4. 自己暗号化ストレージ（記憶媒体）

前節では、米国 HITECH 法の事例を説明しま

表 1：HITECH 法が引用するガイドライン一覧[9]

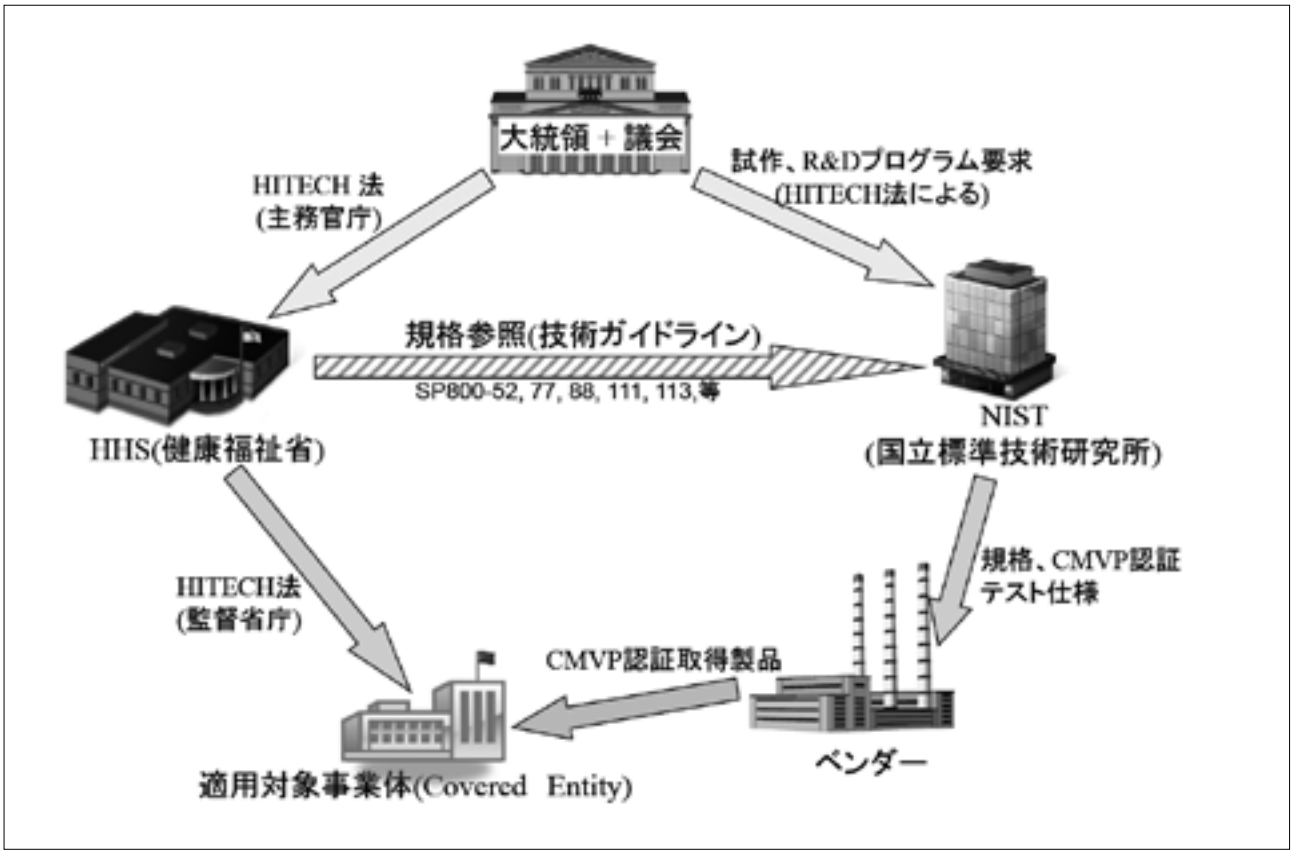
セキュリティのドメイン	ガイドラインの例	内容
移動中のデータ（Data in Motion）	NIST SP800-52 （2005）	安全な TLS の利用法
	NIST SP800-77 （2005）	安全な IPsec VPNs の利用法
	NIST SP800-113（2008）	安全な SSL VPNs の利用法
保管データ（Data at Rest）	NIST SP800-111（2007）	エンドユーザ向けのストレージ暗号化
使用中のデータ（Data in Use）	なし	処理中の秘密情報の扱いなど
データの処分（Data Disposed）	NIST SP800-88 （2004）	電子メディアの破壊など

[7] FTC：Federal Trade Commission
[8] 国立標準技術研究所 (National Institute of Standards and Technology)
[9] HITECH Breach Notification Interim Final Rule -（Ⅱ）Guidance Specification より抜粋。
[10] Cryptographic Module Validation Program：FIPS 140-2 に基づいて米国・カナダで運用されている暗号モジュール評価制度であり、米国及びカナダ政府による、セキュリティ機器の調達基準として用いられています。

したが、このHITECH法における「データ保管」（Data at Rest）の技術的なガイドラインは、SP800-111（Guide to Storage Encryption Technologies for End User Device）になります。米国においては、このガイドラインに沿ったデータ保管のエンドユーザ向けのソリューションとして、比較的「鍵管理」が容易な、「自己暗号化ストレージ」なる製品カテゴリの暗号技術ソリューションが数多く出現しています。これは、ディスクの盗難や置き忘れ等への対策であり、日本においても、その扱いが課題となっています。例えば、PCを持ち出す際にどの程度の保護措置を行うのか、デバイス紛失時の対処方法、完全に持ち出し禁止にすると利便性の問題が生じる、などが課題として指摘されていました。

自己暗号化ストレージ製品としては、HDD、SSD、USBデバイスがあります。ここでは最初にSP800-111における自己暗号化ストレージの概念を紹介します。また、自己暗号化USBデバイス実装におけるCommon Criteria（ISO/IEC 15408）のプロテクションプロファイルとして、2011年にNSA[11]が発行した、Protection Profile for USB Flash Drive[12]（以下PP for USB）を紹介します。

図1：HITECH法のスキーム



[11] アメリカ国家安全保障局：National Security Agency

[12] このPP for USBは、CCRA（CCに基づいたセキュリティ評価結果の相互認証に関する協定）加盟国のグローバルな政府調達要件として発行されています。

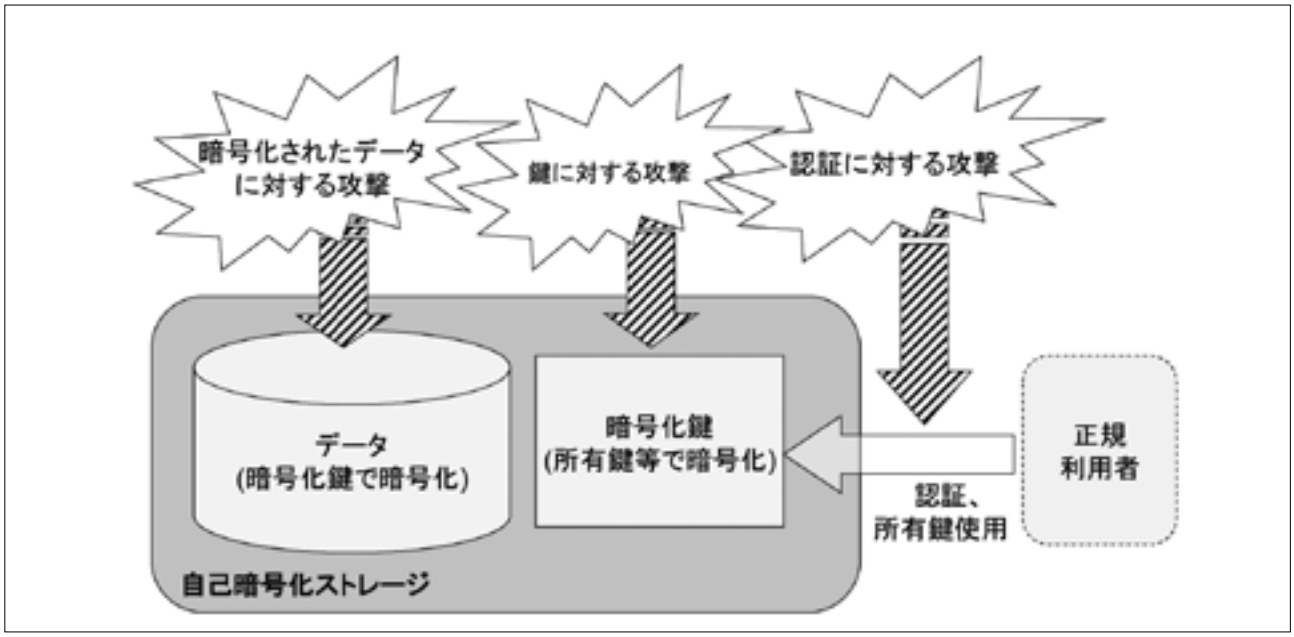
SP800-111 における自己暗号化型ストレージの概念は図 2 で示されています。保管データはデータ暗号化用の鍵（以下 DEK）で暗号化されストレージに保管され、データ暗号化鍵は正規の利用者が所持する鍵暗号化用の鍵（KEK）により暗号化され保管されます。利用者は KEK を複数の認証要素に分散することも可能です。正規の利用者は認証要素を使い認証 [13] された後に、KEK を使う事で DEK を取り出し、DEK を使い復号することでデータを取り出します。SP800-111 では暗号化されたデータ及び暗号鍵に対する安全性については言及されていましたが、鍵管理や認証構造については十分言及されていなく、CMVP と各ベンダーの実装に任されているようです。SP800-111 を受け、2008 年以降、多くのベンダーが、自己暗号化機能付き USB フラッシュデバイスを製品化しており、また CMVP の認証を取得しています [14]。

これまでの CMVP 認証取得製品では、利用者（役割）認証構造をはじめ詳細な仕様については各社が独自に実装していましたが、2011 年 NSA により作成された PP for USB では、SP800-111 の概念を実装する方式が述べられています。（図 3）具体的には、鍵及び秘密情報の管理や、それらの強度を同程度にすることにより暗号モジュール全体の安全性を確保する方法が述べられています。

PP for USB では、2 種類の鍵（DEK 及び KEK）と最大 3 種類の認証要素が秘密情報として用いられます。それらの関係は以下のようになります。

データは AES（Advanced Encryption Standard）[15] により暗号鍵 DEK を用いて暗号化され、暗号化された状態でデバイスに保存されます。DEK は AES 又は排他的論理和によりは暗号鍵 KEK を用いて暗号化され、暗号化された状態でデバイスに保存されま

図 2：自己暗号化ストレージが対応する攻撃



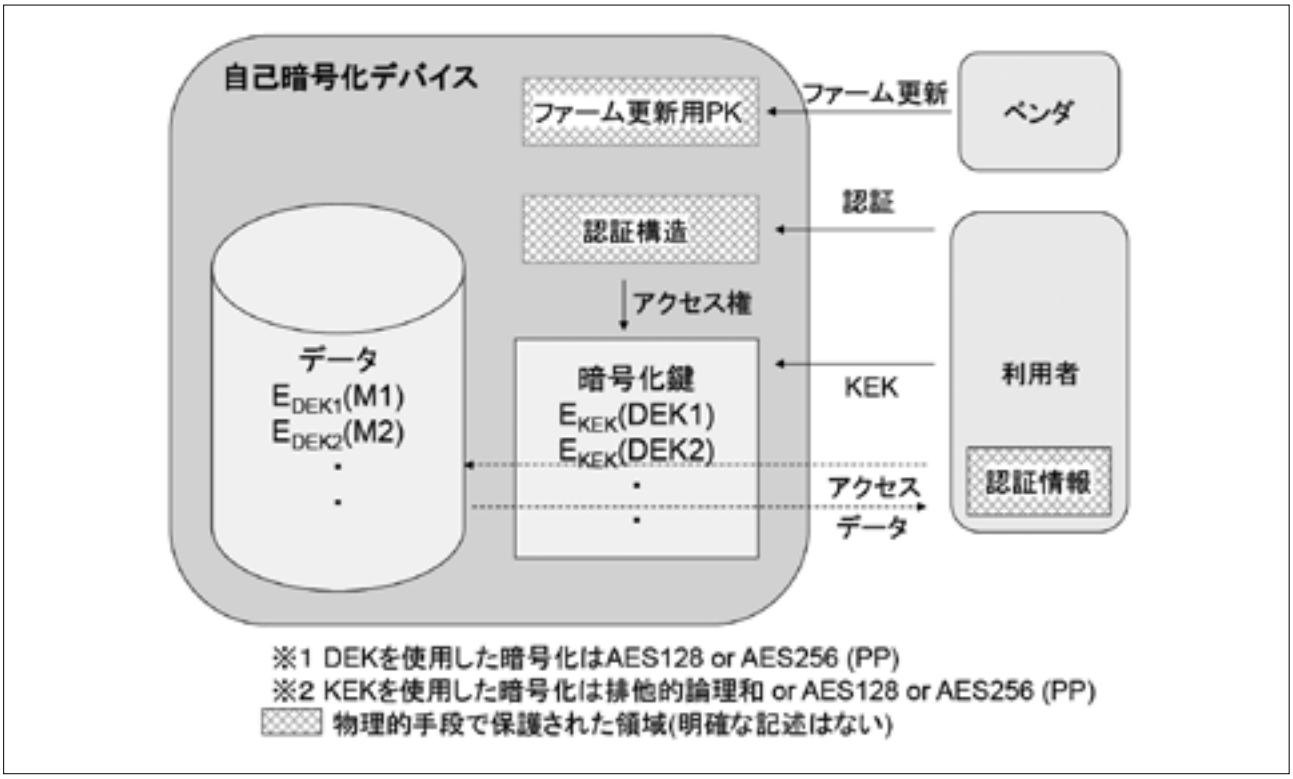
[13] ここでの認証は Authentication の意味ですが、CMVP 等に関する記述における認証は Certification の意味なので注意願います。
[14] IPA の「暗号モジュール試験及び認証制度のご紹介」では、USB フラッシュドライブとして、セキュリティレベル 2 のものが 8 件、セキュリティレベル 3 のものが 13 件、CMVP 認証されていると紹介されています。
[15] 米国政府標準暗号。

す。KEK は①辞書にある単語 9 個以上からなるパスフレーズ（を一方向関数で処理したもの）、② 2^256 以上の情報量を持つトークン、③その他の認証要素、の排他的論理和により使用の度に計算されます。ここで①又は②は必ず含まれなければいけませんが、3 種類全て用いる必要はありません。ここで注目したいのは、DEK を 256 ビットとしても、①～③全てと KEK が同程度の鍵空間を持つ事です。

PP for USB では、データを暗号化する鍵である DEK が取りうる領域を「エントロピ」という概念で表現し、KEK や認証要素も DEK と同程度のエントロピ（≒鍵強度）を持つ事を要求しています。また、デバイスや利用者の OS 内に秘密情報を残さないような細かな規定をし、アクセス制御についても言及しています。暗号技術ソリューションの安全性は、設計、実装、運用、管理のうち一番低いものに落ちることは以前から頻繁に指摘されていましたが、実際には徹底されているとは言いがたい状況でした。PP for USB では、暗号モジュールの各段階における強度を「鍵のエントロピ」という形で統一することを要求しており、鍵管理という点でも参考になります。

表 2 は米国における自己暗号化ストレージの規格、認証基準等です。これらの規格群により個人情報を安全に保護するための技術要求を明確にし、また、要求を満たした暗号技術ソリューションへの認証制度等が整備され、そうした製品の利用にインセンティブを付与する法制度があり（HITECH 法等）、また、実際に利用できる暗号技術ソリューションが多く出現しています。これは、適切な暗号技術に対してベンダーと利用者へのインセンティブを与える制度的なスキームが機能している結果ではないでしょうか。

図 3：PP for USB における自己暗号化デバイスの概念図



5. 日本における今後の課題

米国においては、先に示した「自己暗号化ストレージ」は暗号技術を利用した適切な個人情報保護のための暗号技術ソリューションとして確立しつつあるようです。

我が国において、2005 年に全面施行された個人保護法は、社会に大きなインパクトを与え、また、情報セキュリティ業界においても個人情報保護バブルとも揶揄されるほどに大きな影響がありました。しかし、施行から 8 年も経過したにも係わらず、個人情報を適切に保護するための暗号技術ソリューションの状況は、米国の状況とは大きく異なるように見受けられます。

個人情報保護法第 20 条の「個人データの安全管理のための必要かつ適切な措置」は、様々な観点があり単純な日米比較が出来る訳ではありません。しかし、データ保管のための暗号技術ソリューション確立という観点からは、我が国は、米国より大きく遅れているように見受けられます。日米の比較から、今後、我が国で検討されるべきことは、以下の 3 点になるのではないでしょうか。

(1) 個人情報保護法に関連する技術ガイドラインの統合
(2) 暗号技術における鍵管理技術の重要性の周知と施策
(3) 情報化社会における技術と制度の整合

個人情報保護法に関連する技術ガイドラインの統合

我が国において、個人情報保護法のガイドラインは、各業界の主務官庁毎に作成されています。確かに、業界毎に守るべき組織や情報が異なるため、個別のガイドラインの必要性はあります。

米国の個人情報保護法は、セクトラルモデルであり、やはり、そのガイドラインは個別の業界毎に作成されているようです。しかし、個人情報を適切に保護するための技術ガイドラインとしては、NIST が作成しているもの（SP800 シリーズ）が参照されている場合が多いようです。

NIST の SP800 シリーズに近いものとしては、我が国の内閣官房情報セキュリティセンターの「政府機関の情報セキュリティ対策のための統一基準群」等がありますが、これは、政府機関向けのものであり、民間の規範となるものを目指している訳ではないように見受けられます。こうしたこともあり、個人情報保護法に関しては、各業界向けには統一された技術ガイドラインが整備されていません。各技術ガイドライン要求は業界毎に作成され、統合されていませんし、既存の各ガイドラインにしても技術要件が明確に規定できていません。これが「個人データを安全管理するた

表 2：自己暗号化ストレージを取り巻く規格、標準、認証制度

類　別	規格、標準、認証制度
ガイドライン	NIST SP800-111
仕様	TCG Opal[16] 自己暗号化ディスク仕様など
プロテクションプロファイル	NSA フルディスク暗号化のプロテクションプロファイル、2011/12/1、バージョン 1.0
	NSA USB フラッシュデバイス用のプロテクションプロファイル、2011/12/1、バージョン 1.0
FIPS140-2　認証製品（CMVP）	TCG Opal 仕様の自己暗号化ディスク（Seagate のハードディスク、Samsung の SSD などの製品）
	多くの暗号化 USB デバイス

[16] 標準技術を策定する業界団体である TCG（Trusted Computing Group）によるストレージ暗号化に向けての規格のこと。

めの必要かつ適切な措置」に対応した適切な暗号技術ソリューションが確立しない原因のひとつになっているのではないでしょうか。

暗号技術における鍵管理技術の重要性の周知と施策

暗号技術ソリューションが適切に機能するには、「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」全てが適切に機能しないといけません。

暗号アルゴリズムが安全でも、例えば暗号鍵を管理するパスワードに脆弱なものを使用したり、実装に脆弱性が存在すれば、データが漏えいする可能性は高まり全体として十分な強度が保てません。つまり、暗号アルゴリズムの強度だけでなく、暗号化に利用する鍵管理の運用や実装も含めて適切なレベルになるよう考える必要があります。我が国においては、この部分の認識が希薄であり、特に鍵管理に関する技術や運用のプラクティスもおざなりになっていたのではないでしょうか。

エンドユーザ向けの自己暗号化ストレージ等の暗号技術ソリューション利用において、「暗号アルゴリズム」に関しては電子政府推奨暗号アルゴリズムを参照すればよいのですが、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」に関しても我が国の制度は十分機能してないように見受けられます。今後は、利用者レベルの鍵管理を提供する仕組みや、その実装の安全性を保証する認証制度を整備するべきではないでしょうか。

米国の場合、暗号技術を利用したものに関しては、CMVP が認証制度として定着しており、利用者は多くのことを理解せずとも CMVP 認証製品リストから暗号技術ソリューションを選択すればよいことになります。個人情報保護専門調査会の報告書では、暗号技術ソリューションが定着しない理由として公的な認証制度がないことを挙げていますが、実際には、我が国においても、米国の CMVP に対応する JCMVP（Japan Cryptographic Module Validation Program）[17] があります。しかし、この JCMVP の認知度は非常に低く、また、認証製品も米国の CMVP に比べ極端に少ないのが現状です。これにはいくつかの要因がありますが、そのうちのひとつは、鍵管理技術の重要性が認識されていないことではないでしょうか。JCMVP の様な認証制度を機能させ、暗号技術ソリューションを活用する上でも、鍵管理技術の重要性を周知させることが必要でしょう。

情報化社会における技術と制度の整合

情報技術、情報通信技術が社会の基盤として不可欠となるにつれて、情報セキュリティと制度との関係が重要になっています。そのような状況で、2000 年以降、情報セキュリティにも関係の深い、様々な制度が施行されてきました。しかしながら、技術と制度が噛み合わないために、こうした制度が有効に機能していない面が多々あるのではないでしょうか。また、制度の見直し等の議論においても、技術と制度の関係者の間で意思疎通が成立していないように感じることがよくあります。本稿では、個人情報保護法に着目し、「情報化社会における技術と制度の整合」の必要性を考察することを試みているところがあります。

社会から、適切な個人情報保護の仕組みが求められており、実際に適切な暗号技術を利用すれば効果的な対策が可能なはずにも拘わらず、ベストプラクティスと言えるような暗号技術ソリューションが確立できていません。これは、個々の技術の問題というよりは、もう少し広い問題で、技術と制度を整合させるためのスキームに課題があるように感じられます。。このあたりの考察は、本稿において、まだまだ稚拙なところはあるかと思いますが、今後の情報化社会に対応した情報セキュリティの制度と技術のあるべき姿を議論する上で参考になれば幸いです。

[17] JIS X 19790 に基づいて IPA により運用される暗号モジュールの評価制度。2012 年より CMVP との共同認証も行っている。

参考文献

◇国内の法令・ガイドライン

個人情報保護法 , (2003)

個人情報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（2009 年改正）
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（2010 年改正）
http://www.ajha.or.jp/about_us/nintei/pdf/101014_1.pdf

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」に関するＱ＆Ａ（事例集）、(2010 年改正)
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805iryou-kaigoqa.pdf

◇国外の法令・ガイドライン

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)

American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5)（HITECH はこの一部）

HITECH Breach Notification Interim Final Rule, (2009)
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

NIST, Guide to Storage Encryption Technologies for End User Device（SP800-111）, (2007)
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

◇その他の参考資料

暗号モジュール試験及び認証制度のご紹介
http://www.ipa.go.jp/security/jcmvp/documents/open/jcmvp_session_20120312.pdf

「国民を守る情報セキュリティ戦略」における「情報セキュリティ政策会議」
http://www.nisc.go.jp/conference/seisaku/

個人情報保護専門調査会報告書
http://www.cao.go.jp/consumer/iinkai/2011/067/doc/067_110826_shiryou3.pdf

JNSA 第 2 回鍵管理勉強会（2012）
http://www.jnsa.org/seminar/seckey/120703/

NSA, Protection Profile for Full Disk Encryption,（日本語訳：フルディスク暗号化のプロテクションプロファイル）(2011)
原文：http://www.niap-ccevs.org/pp/PP_FDE_v1.0/
日本語：http://www.ipa.go.jp/security/publications/niap/spp-jp/pp_fde_v1.0-J0.1.pdf

NSA , Protection Profile for USB Flash Drives,（日本語訳：USB フラッシュデバイス用のプロテクションプロファイル）(2011)
原文：http://www.niap-ccevs.org/pp/PP_USB_FD_v1.0/
日本語：http://www.ipa.go.jp/security/publications/niap/spp-jp/pp_usb_fd_v1.0-J0.1.pdf

FIPS140-2, http://csrc.nist.gov/publications/PubsFIPS.html

謝　辞

本稿の執筆および、第二回鍵管理勉強会の企画では、みずほ情報総研の小川博久様に有益なご助言を頂きました。
ここに感謝致します。