ISBN978-4-89078-038-9
C3004

電子記録管理に関する調査検討報告書 2014

－　電子記録の利活用と情報セキュリティ　－

電子記録応用基盤研究会（eRAP）

電子記録利活用ワーキンググループ

平成 27 年 3 月

一般財団法人日本情報経済社会推進協会

序　文

高度に情報化された現代において、情報の生成、利活用は様々な社会活動の場面において急速に普及してきている。こうした中で、「情報の信頼性」、「安全な保管」、「安心できる取扱い」を保証できる仕組みを確立することが喫緊の課題といわれて久しい。組織として記録を電子化し適切に管理、活用することによるメリットは多い。例えば、監査における説明責任を果たす際に利用する、あるいは新たな業務を行う際に過去似たような業務で作成した記録を活用し、効率的にかつ質の高い業務活動につなげる、法律等の要求する情報を電子的に保存し必要な際に利用するなどである。

そこで、一般財団法人日本情報経済社会推進協会(JIPDEC)では、平成 22 年 4 月に電子記録応用基盤フォーラム(eRAP)を立ち上げ、これを引き継ぐ形で平成 25 年 4 月に電子記録応用基盤研究会(eRAP)と名前を変え、平成 26 年は、研究会の中に 2 つのワーキンググループ（WG）（ケース指向管理ハンドブック製作 WG、電子記録利活用 WG）を設置して活動を行った。

本報告書は、電子記録利活用 WG が平成 26 年度に実施した活動をまとめたものである。

本年度は電子記録利活用の際の「個人情報保護」、「プライバシー保護」、「マイナンバー法（番号法）」への対処に焦点を当てて活動を行った。

本報告書が、電子記録管理・利活用の発展の一助になれば幸いである。

平成 27 年 3 月

一般財団法人日本情報経済社会推進協会

目　次

まえがき **1**
第 1 章 2014 年度の活動方針 **3**
1.1　電子記録利活用における情報セキュリティ技術 3
1.2　セキュリティ対策推進の阻害要因 4
第 2 章 情報セキュリティ導入検討のための指針 **9**
2.1　情報セキュリティ対策の指針の必要性 10
2.1.1　車両の運転におけるセキュリティ 10
2.1.2　情報セキュリティ導入のための必要な体制 11
2.2　安全安心な電子記録利活用に向けた制度の構築の必要性 11
2.2.1　関連法律の理解 11
2.2.2　IT を用いたシステムやサービスを供給しようとする提供者への指針 13
2.2.3　IT を用いたシステムやサービスを適切に用いて対処しようとする利用者への指針 14
2.2.4　目的別カタログ 15
2.2.5　インシデント発生後の対応 15
第 3 章 電子記録利活用の情報セキュリティ推進の検討 **17**
3.1　電子記録利活用のための情報セキュリティ対策事例 17
3.1.1　モバイルネットワーク、事業継続（閲覧） 17
3.1.2　機密情報の参照（閲覧） 18
3.1.3　機密情報のアップロード（交換） 19
3.1.4　組織外との情報共有（交換） 20
3.1.5　機密情報移送時のセキュリティ・モバイル PC からの情報漏洩防止（持ち出し） 21
3.2　インシデント対応と証拠保全 22
3.3　個人情報の非個人情報化 27
3.4　防止策及びインシデント対応策 30
3.4.1　漏えいや流出事故等を起こさない対策を行う（残存リスクを正確に把握する） 30
3.4.2　漏えいや流出事故等が発生しても実害が生じない対策を実施する 32
3.4.3　日常的に安全管理措置を徹底していることの証拠を残す 35
3.4.4　不幸にして事故等が発生した際には、迅速に必要な対処を行う 36
あとがき **42**
メンバリスト **43**

まえがき

ICT 技術を活用することにより、多くのサービスは時間的、空間的制限がなくなり、いつでもどこからでもサービスを利用することが可能になった。しかしながら、電子記録の分野では、紙媒体で管理していたものを、電子媒体に移してそのまま管理・運用しているレベルにとどまっているものが多く、紙媒体ではできなかった新たな魅力的なサービスの享受にはなかなか至っていない。

今後、電子記録を対象とした様々なサービスが出現することが期待される。しかし、このようなサービス等を安心して利活用していくには、そこで運用管理される「情報」に対し、一般に言われる「情報セキュリティ」が必要不可欠であることは言うまでも無い。但し、この「情報セキュリティ」という単語は、非常に幅広く多くの意味を持っている。

不正に見られてしまうことへの対策(秘匿性)、紛失及び盗難への対策(アクセスコントロールや認証・機密性)、書き換えられてしまうことへの対策(真正性・完全性)、情報自体が破壊・消滅してしまうことへの対策(事業継続や可用性)といったこと等が挙げられ、前年度は特に秘匿性、真正性、気密性について、技術的な検討を行った。

今後、電子記録の利活用における情報セキュリティの導入・強化を図っていく必要があるが、多くのガイドラインが出ているにもかかわらず、導入責任者にとって、セキュリティを導入及び強化をすべきか否か、そのためにどの程度のコストを投入すべきかなどの相場観が形成されているとは言えない。

そこで、今年度は、電子記録の利活用においてどのレベルの情報セキュリティが必要かの議論を行い、議論の結果として、情報セキュリティの導入・強化が必須な場合として以下の 2 点に整理された。

① 法令の遵守

② 企業活動の維持

今年度はまず、「①　法令の遵守」に絞り、さらに「個人情報保護法」と「行政手続における特定の個人を識別するための番号の利用等に関する法律（以下　マイナンバー法（番号法））」への対応に絞って検討を進めることにした。

また、電子記録の利活用におけるセキュリティに対する理解を深めるため、具体的な事例の調査を行った。

「第 1 章　2014 年度の活動方針」では、前年度の活動成果の概要を示すとともに、情報セキュリティ対策推進の阻害要因について説明し、個人情報保護法、マイナンバー法（番号法）の罰則規定について解説する。

「第 2 章　情報セキュリティ導入検討のための指針」では、中小企業の経営者が情報セキュリティの導入を検討する際の必要な情報を整理し、その概要を示す。

「第 3 章　電子記録利活用の情報セキュリティ推進の検討」では、

・望ましくない、かつ陥りやすい電子記録利活用トラブル例（無過失　/　過失　/　悪意）について紹介する。特に、個人情報、マイナンバー、プライバシーを扱う際のトラブルに

ついて、取り上げる。
・トラブル例に対応できるユースケースについて紹介する。
・トラブルを解決するための技術を紹介する。

なお、本報告で使われる用語について以下のとおり、定義する。

① 電子記録

FDA(Food and Drug Administration:米国食品医薬品局) 21 CFR（the part of Title 21 of the Code of Federal Regulations）Part 11 では「電子記録とはコンピュータシステムにより作成，修正，維持，保管，復元および配布されるデジタル形式の文章，図，記録，音，画像およびその他の 情報表示のあらゆる組み合わせを意味する」と定義されている。

http://www.an.shimadzu.co.jp/apl/medicine/eres1.htm

② 秘密分散技術

秘密にすべき情報をビットレベルで複数の割符ファイルに分割して管理し、その分割した割符ファイル単体では原本情報を導き出すことが出来ないようにし、割符ファイルのすべてあるいは一部の複数の割符ファイルを用いると原本情報を復元することができるような情報の運用管理手法を秘密情報分散運用管理手法といい、秘密情報分散運用管理手法を実現するためのソフトウェア等の工学的成果は、秘密分散技術と呼ばれている。

本報告で扱う、個人情報の非個人情報化については、実際に電子情報の分割処理を行うのはソフトウェア等の技術である為、秘密分散技術についてのみ扱う。

また、秘密分散技術は、電子割符（一般名称）とも呼ばれることがあるが、代表的な秘密分散技術の供給会社である GFI 社の製品名 GFI 電子割符（R）と混同する恐れがあるため、本報告では「秘密分散技術」を使っている。引用する文章の中で「電子割符」と表記されている場合は、そのままにしてある。

③ マイナンバー法

正式名称は、「行政手続における特定の個人を識別するための番号の利用等に関する法律」。

社会保障と納税に関する情報を連携するために国民全員に割り振られた番号「共通番号(マイナンバー)制度」を導入及び運用するための法律。

また、年の表示は西暦を用いるが、法令など慣行的に和暦を用いているものはそのまま和暦で表示している。

第1章　2014 年度の活動方針

電子記録利活用における情報セキュリティ課題については、前年度に検討を行い、報告書としてまとめた［1-1］。まず、その概要を紹介するとともに、よりユーザがセキュリティに取り組むために必要な環境の検討を行った。

1.1　電子記録利活用における情報セキュリティ技術

クラウド/モバイル端末環境での電子記録の利活用におけるセキュリティ問題は、制度面、技術面、運営体制面から検討する必要がある。クラウドコンピュータのような仮想化環境かつマルチテナントの場合は、ユーザ間またはプロセス間での、漏洩、盗み見などが起きる恐れが指摘されている。また、クラウドコンピュータ運営企業における不正利用の恐れもある。モバイル端末を利用する際、重要なデータを保存して持ち歩くことができるため、紛失や盗難に対する対策の必要がある。

このほか、電子記録の利活用場面を想定すると多くのセキュリティの課題が考えられるが、前年度は次の 3 つの点に絞り、クラウド上でのサービスの提供、モバイル端末での利用も考慮して技術調査を行った。

①　開示データの真正性の確認手法
②　開示のためのアクセス制御方法
③　盗聴・盗難対策としての暗号/秘密分散技術の利用方法

下の図に、それらの課題の関連を示す。

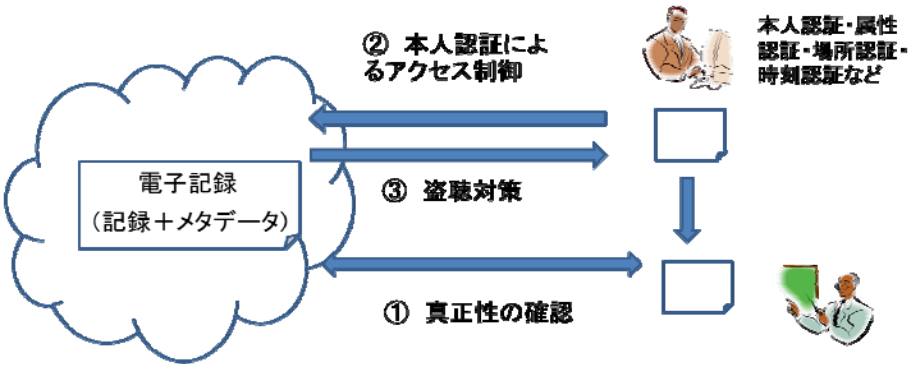


図 1-1　セキュリティ検討項目

①　開示データの真正性の確認手法

受け取ったデータがいつ、どこから取り出され、その後、改ざんされていないことを確認するしくみを検討した。オープンガバメントなどでも必要になる。

②　開示のためのアクセス制御方法

アクセス制御は、個人ごとに（ID/PW（パスワード）、生体認証、PKI（public key infrastructure：公開鍵基盤）など)を用いて制御する場合と、役職などの属性情報により制御する場合がある。

また、アクセス制御をシステム単位、サービス単位に加えて、電子記録単位に行うこともでき

るため、検討を加える必要がある。

③　盗聴・盗難対策としての暗号技術/秘密分散技術の利用方法

盗聴や盗難されても、暗号技術、秘密分散技術で平文になることを防ぐための検討を行った。

1.2　セキュリティ対策推進の阻害要因

2013 年度の調査で､セキュリティ対策のための技術メニューが豊富に準備されていることが確認できた。しかしながら、実際にセキュリティインシデント等に係る報道等が後を絶たないのが実情である。一つには企業におけるセキュリティ対策が進んでいないことによる。

今年度は、セキュリティ対策を推進するための検討を行った。

（1）セキュリティ対策の状況

2013 年度に警察庁生活安全局情報技術犯罪対策課が特定の業種、地域に偏りのないよう 3,313 件を無作為に抽出しておこなったアンケート調査の実施報告書［1-2］によれば、情報セキュリティ対策実施上の問題として、「費用対効果が見えない」が 53.7%で最も多く、「どこまで行えば良いのか基準が示されていない」が 45.5%、「コストがかかりすぎる」が 42.4%、「教育訓練が行き届かない」が 37.3%で続いている。

また、定性的観点から、セキュリティ対策上の問題点・不安点としては、「不正アクセス対策に係るコスト」、「知識や認識の不足」、「対策の限界」等に分けられる、としている。

「不正アクセス対策に係るコスト」としては、「セキュリティ対策の予算確保が難しい」、「対策経費が高い」といった声が挙げられている。

「知識や認識の不足」としては、「経営層の理解が得られない」、「全体的なリテラシーの不足」といった意識の問題などが挙げられた。

「対策の限界」としては、「どこまで対策をすれば完全なのかわからない」、「想定外のセキュリティの穴が発生する」、「公開 Web サーバの公共性が高く、不正の可能性が高い IP アドレスを安易に遮断できない」といった、対策の範囲や有効性についてのものが寄せられている。

また、文献［1-3］では、セキュリティ対策推進の阻害要因を以下のようにまとめている。

A) セキュリティ対策の必要性が不明

－　どのような危機があるのか。

－　その危機の影響は

－　遭遇する頻度は

B) セキュリティ対策の効果が不明

－　不利益は何か

－　ご褒美は何か

C) 必要なセキュリティ対策が不明

－　実施すべき対策と費用が分からない

さらに、阻害要因解消についての必要な対策が分からない原因として以下をあげている。

・　曖昧で網羅主義的ガイドラインが多すぎる。

読む人、特に経営層には理解不能/　実装まで踏み込んだ説明書が必要/

・ 公的機関・重要インフラの率先垂範
　想定するリスクと対策を公開すべき
・ 結果ではなく対策決定の経過
　リファレンスモデルとなるべき

一方、データベス･セキュリティ・コンソシアムが 2014 年に発表した「DBA 1,000 人に聞きました」（注：DBA（DataBase Administrator））アンケート調査報告書[1-4]では、まとめのなかで「また今回の調査結果から DBA 自らが内部不正の可能性を自覚しており、約 10%が不正をする可能性があるというのは、従来の予想を上回るものであろう。このことは、現在多くの情報システムの安全性が多くの管理者の方々の善意で支えられており、雇用・人事・職場環境の改善といった、一見情報セキュリティとは直接関係がなさそうに見える経営的な施策と企業・組織の健全化そのものが、結果として情報保護のためにも有効であるということを示していると考えられる。」と述べている。

これら、セキュリティ対策推進の阻害要因に対応するための活動として文献［1-5］の中で、「IT 技術対策には、ソフトウェアや通信プロトコル、システムの脆弱性や脅威への対応があり、セキュリティマネジメント対策には、セキュリティポリシーの作成、運用、監査などを通しての組織の PDCA サイクルの確立と維持などがある。

IT 技術的な視点とマネジメント的な視点とからセキュリティ対策を考えるだけでは限界があると考える。そこで、情報セキュリティに経済的視点を加えた、情報セキュリティエコノミクス（Information Security Economics）を提案する」

としている。さらに、

「サービスや財などの商品の品質に関して買い手の情報が乏しいために適正な価格が分からず、売り手の持つ情報と、買い手の持つ情報に差がある状態、つまり情報の非対称性が存在する状態を解消する必要がある。

・ 品質に関する情報をわかりやすく説明する手段を用意する。
・ 一般の利用者よりも高度な知識を持つ公正な第 3 者が品質に関する何らかの保証を行ったりする。

等の対策が考えられる。」

といった提案を行っている。

そこで、我々はユーザの理解を深めるためには、具体的な事例を集めて紹介することが、有効な手段の一つになるはずであると考える。

（2）法令上対応せざるを得ないリスク

もう一つの視点として、「法令上対応せざるを得ないリスク」がある。セキュリティ対策を行わずに情報流出などのインシデントにあった場合に、法的な処分を受けるため、セキュリティ対策は必須項目になる。情報管理に関する主要な法律として以下のものがある。

・個人情報保護法
・マイナンバー法（番号法）
・不正競争防止法　など

企業が保護すべき主要な情報を図 1-2 に示す

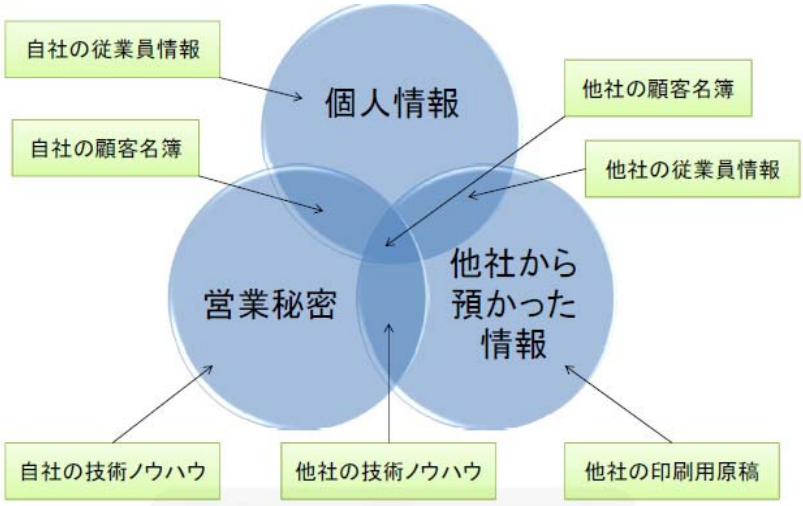


図 1-2　企業が保護すべき主要な情報（文献 1-6 より引用）

今年度は電子記録の利活用にかかわる法律として、個人情報保護法とマイナンバー法（番号法）に注目して検討を進めることとした。

（3）個人情報保護法の罰則規定

個人情報保護法が、約 10 年ぶりに改正されようとしている。政府の高度情報通信ネットワーク社会推進戦略本部（以下、IT 総合戦略本部）では 2013 年 12 月 20 日に「パーソナルデータの利活用に関する制度見直し方針（以下、制度見直し方針）を決定しており、その後 2014 年 6 月 24 日に「パーソナルデータの利活用に関する制度改正大綱」を決定している。ここでは大綱にそって、個人情報保護法の改正が、ビジネスの現場にどのような影響を及ぼすかについて見ておきたい。

罰則規定は、三十万円以下の罰金、または六ヶ月以下の懲役。

（4）マイナンバー法（番号法）の罰則規定

マイナンバー法（番号法）とは、国民一人ひとりに番号を割り振り、社会保障や納税に関する情報を情報連携可能なかたちで管理するための法律。2013 年 5 月 24 日に国会で成立した。

マイナンバーは、平成 2015 年 10 月以降、市区町村から住民票の住所に送られる「通知カード」で通知される予定で、マイナンバーの利用については、平成 2016 年 1 月以降、社会保障、税、災害対策の分野で行政機関などに提出する書類にマイナンバーを記載することが必要になる。

年金や納税など異なる分野の個人情報を照合できるようにし、行政の効率化や公正な給付と負担の実現を図ることなどが目的。個人番号カードは、通知カードとともに送付される申請書を郵送するなどして、平成 2016 年 1 月以降、交付を受けることができる。自治体は、申請者に対して、氏名や顔写真、個人番号などが記載された個人番号カード（マイナンバーカード）を交付する。番号の利用範囲は、社会保障と税の分野だが、他分野へのマイナンバーの利用拡大も検討する予定である。また、個人情報の漏洩や不正利用を監視する第三者委員会を設け、違反者にはそれがたとえ 1 件であっても 4 年以下の懲役、更に 200 万円以下の罰金等の重い罰則が科せられる。

罰則規定の詳細を図 1-3 に示す。

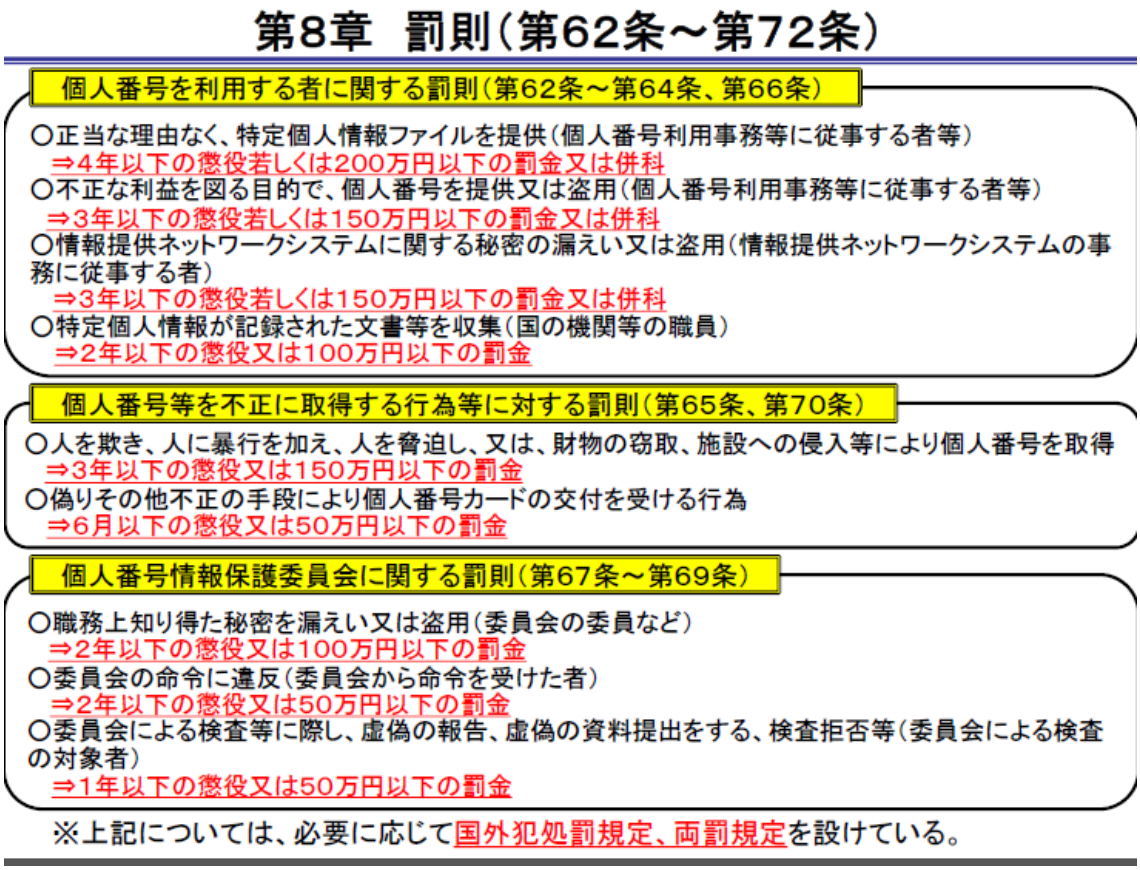


図 1-3　罰則規定（「マイナンバー法案」の概要［1-7］：内閣官房社会保障改革担当室より）

（５）2014 年度の検討項目

「電子記録の利活用における情報セキュリティ」を推進していくうえで、1.２節で述べたように、推進の阻害要因のなかで、情報セキュリティ対策をとるべきか否かが判断できない、どのように情報セキュリティ対策をとるべきかわからない、といった声に注目し、情報セキュリティ対策の普及について、以下の２項目について検討することにした。

① 全ての企業が対応する必要のある個人情報（特定個人情報も含む）を含む電子記録の利活用における情報セキュリティ対策の検討項目の指針

② ユーザの理解を深めるための電子記録の利活用におけるセキュリティ事例の充実などの対策

それぞれの項目について、２章、３章で検討内容を報告する。

参考文献

［1-1］　「電子記録管理に関する調査検討報告書 2013　－　ケース指向管理のユースケースとセキュリティ　－」　2014 年 3 月

［1-2］　「不正アクセス行為対策等の実態調査 報告書」　警察庁生活安全局情報技術犯罪対策課　2014 年 2 月

［1-3］　下村 正洋「セキュリティ産業が情報セキュリティエコノミクスに期待すること」 情報セキュリティエコノミクスシンポジウム 2013」講演資料

［1-4］　「DBA 1,000 人に聞きました」アンケート調査報告書　2014 年 9 月 10 日　データベス･セキュリティ・コンソシアム

［1-5］　杉浦ほか　「情報セキュリティエコノミクスの挑戦」情報処理学会第 11 回コンピュータセキュリティシンポジウム．コンピュータセキュリティ シンポジウム 2008（CSS2008）（改）．

［1-6］　岡村 久道「組織における内部不正防止ガイドラインの公表に向けて」「情報セキュリティエコノミクスシンポジウム 2013」講演資料

［1-7］　「マイナンバー法案」の概要　内閣官房社会保障改革担当室

第2章　情報セキュリティ導入検討のための指針

「行政手続における特定の個人を識別するための番号の利用等に関する法律」(通称マイナンバー法）では国民に付番される「個人番号（マイナンバー)」と、その個人番号（マイナンバー）の対象となる本人の個人情報が付されている情報を、「特定個人情報」と定義している。この情報管理に関し民間事業者に既存の個人情報保護法よりも厳格な情報管理を要求しており、その管理を怠った場合等には、前述の重い罰則が適用されることとなっている。過去の個人情報保護法では、5000 件という情報件数で一定の線引きが行われていたが、マイナンバー法（番号法）では１件から同法が適用されることとなっている。

同法はどんなに小さな組織であっても「個人番号（マイナンバー)」を含む「特定個人情報」を管理する組織は対象となる。今後同法への理解度の低い組織等が出てくることの懸念もあるが、生業としてマイナンバー法（番号法）の規定する個人番号や特定個人情報等を扱う組織等は、組織の規模の大小を問わずしっかりとした準備が必要となる。マイナンバー法（番号法）は、昨今の社会の実状を踏まえ情報管理を電子的に行なうことを相当意識した内容となっている。しかし、問題なのは現場実務では IT がすでに広く普及していても、適切な IT を含めた同法対処を具体化できない事業者や組織等が出現してしまう危惧があることである。それは、組織にとって IT は重要なツールではあることは事実であるが、あくまで事業活動を支援するツールである為、経営者や従業員が必ずしも IT に詳しいとは限らないことと、法律に関しても詳しいとは限らず、同法が法令上要求する厳格な情報管理や安全管理措置を具体化できないことが容易に予想できるためである。

同法で法令上の義務を最終的に課せられているのは、結局は事業者、組織の経営陣（者）である。経営陣（者）は、自らの事業所・組織が導入する（している）情報システムが法令等に対しどれだけの範囲をどういったレベルでカバーしていて、対処できていない残存部分がどれだけあるのかを知った上で、その残存部分をリスクとして人的、組織的、物理的にどのように法令対処しなければならないのかを把握し、現実的な対処策を講じなければならない。

IT を用いたシステムやサービスは今後自らが役立つ範囲やレベルを明示していく必要があると考えられるが、多くの場合自らが役立つ範囲を明確に示すことが困難なことが多い。それは、IT を用いたシステムやサービス自体がハードやソフト、周辺サービス等で構成される巨大な複合体であり明確な表現がしにくいからである。しかしながら、IT を用いたシステムやサービスを導入判断し、対価を支払う利用者はどのようにして同法対処を具体化すれば良いか。特に、マイナンバー法（番号法）では、法の要求する安全管理措置は既存の個人情報保護法よりも厳格な対象情報の管理義務をクリアできるものでなければならない。

ここで必要なのは、"他人任せ"では本当の解決はできないことを自覚することである。このように法令遵守に対し、利用者（ユーザ事業者等）と IT を用いたシステムやサービス供給者（IT 事業者等）で協力して対処を具体化するという考え方は、決してマイナンバー法（番号法）に限ったことではないが、IT を適切に用いて法令遵守する際に資する、基本原則を指針として策定することが必要である。

2.1 情報セキュリティ対策の指針の必要性

電子記録の利活用において、個人情報や特定個人情報を扱うことも考えられ、情報セキュリティ対策が必須になってきているにもかかわらず、1 章で述べたように情報セキュリティ対策については、ユーザにとって受け入れやすい状況になっていないのが状況である。そこで、セキュリティ対策が進んでいる「車両の運転におけるセキュリティ対策」を整理したうえで、それと対比して情報セキュリティのあるべき対策の検討を進める。

2.1.1 車両の運転におけるセキュリティ

道路網や標識・信号等のインフラ整備、及びそれ利用するための法律の整備は国や地方自治体が行う。それらのインフラ上で車両の運転する場合、事故を起こさないため、あるいは事故後の対応を行うための社会的な体制が整っている。まず、これらについて確認を行う。

（1）関連法律の理解

一般に、「関連法律の学習」については、自動車教習所で受講料を支払い、試験に合格して初めて運転免許を受け取ることができる。この場合、「道路運送車両法」、「自動車損害賠償保障法」や「道路交通法」を各々すべて学習するのではなく、必要な部分をわかりやすく説明したテキストが準備される。

（2）運転技術の教習

一般に、自動車教習所で教官の指導の下で、自動車の構造を学んだうえで運転の訓練をする。自動車教習所の道路は私道であるため、法律は及ばない。一定の技術に達したと認められたのち、実技試験を受けることができる。

（3）自動車の購入

一般に、自動車ディーラから購入する。自動車ディーラは自動車のカタログを準備しその機能性能と価格について説明を行う。ここで、不正な表示・説明を行うことは禁じられている。

ユーザは、自分のニーズ、予算に合わせてカタログから購入候補を選択し、自動車ディーラから説明を受けて、購入する車両を判断する。

（4）自動車のメンテナンス

自動車のメンテナンスは、国家試験の資格である「自動車整備士」が行う。乗用車には「車検制度」があり、定期的に検査を受ける必要がある。また、トラブルがあると適宜整備、修理及び部品交換を行い、その作業は整備記録として残される。

（5）事故対策としての保険制度

一般的に、任意の自動車保険に加入する。任意の自動車保険は民間の保険会社が多く扱っているが、保険内容、価格などの相場はほぼ決まっている。ただし、運転者が飲酒運転をするなど契約を守らなかった時には、保険金は支払われない。

（6）事故対策としての証拠保全

一般的に事故が起きた時に、どちらに過失があったのかを証明するのは困難である。そこで、商業車だけでなく、ドライブレコーダ（車載カメラ）を搭載することができるようになってきている。

このように、車両を運転する場合、車両の種類（2 輪車、乗用車、大型車、特殊車両）に合わせた教育・訓練が行われ、事故後の対応にも体制ができている。

2.1.2 情報セキュリティ導入のための必要な体制

車両の場合を参考にすると、以下の項目を利用者に提供することにより、より情報セキュリティの導入の敷居が低くなると考えられる。

例えば、「電子記録利活用システム」を導入する場合

① 関連する法律、ガイドラインのわかりやすい資料、セミナ
② 「電子記録利活用システム」に特化した、情報セキュリティマネジメント
③ 「電子記録利活用システム」のわかりやすい事例集・カタログ
④ システムのメンテナンス体制
⑤ 事故が起きてしまった時の損害保険
⑥ 事故が起きてしまった時の自己防衛（証跡管理）

電子記録利活用のセキュリティ対策の指針を作成する際に考慮すべきものとして、事業者間の責任分界点の問題がある。実際にインシデントが起こった際に、システムの不備なのか、ユーザ側の操作ミスなのか、明確になるようにしておかなければならない。

そのため、ここでは、「法令遵守しようとする事業者に対し、IT を用いたシステムやサービスを供給しようとする供給者（IT 事業者等の経営層）への指針」と「法令遵守に IT を用いたシステムやサービスを適切に用いて対処しようとする利用者（ユーザ事業者等の経営層）への指針」に分けて検討を行った。

検討内容は、電子記録利活用における、個人情報保護法、マイナンバー法（番号法）を遵守するための指針に絞っている。個人情報保護法やマイナンバー法（番号法）に関するガイドラインはすでにあり、2.2 節でその概要を紹介するが、電子記録利活用における対応の具体的検討が必要となる。

2.2 安全安心な電子記録利活用に向けた制度の構築の必要性

2.2.1 関連法律の理解

電子記録を利活用するための、サービス提供者、サービス利用者ともに、関連する法律はもちろん、関連のガイドラインも理解しておく必要がある。しかしながら、以下に示すガイドライン、認証制度があり、それらを経営者が自ら読んで理解することは、困難である。

そこで、目的対応、たとえば「電子記録を利活用」する場合に限って理解しておく必要のある法律、ガイドライン、認証制度の検討が必要である。また、理解度を図る認定制度の検討も必要である。

検討分野に関する既存のガイドライン、認証制度として、ISMS（情報セキュリティマネジメントシステム）［2-1］、プライバシーマーク［2-2］及びマイナンバーのガイドライン［2-3］についてその概要を説明する。このほか、クラウド業者に対しては「クラウドサービス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」［2-4］についてその概要を紹介する。

(1) ISMS（情報セキュリティマネジメントシステム）［2-1］

ISMS とは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することである。

ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることにある。そのためには、ISMS を、組織のプロセス及びマネジメント構造全体の一部とし、かつ、その中に組み込むことが重要である。

JIS Q 27001（ISO/IEC 27001）は、ISMS の要求事項を定めた規格であり、組織が ISMS を確立し、実施し、維持し、継続的に改善するための要求事項を提供することを目的として作成されている。

(2) プライバシーマーク［2-2］

プライバシーマーク制度は、日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度である。

個人情報の保護に関して国の行政機関においては、「行政機関が保有する電子計算機処理に係る個人情報の保護に関する法律」（昭和 63 年 12 月法律第 95 号）が制定され、平成 15 年 5 月 30 日に改正（平成 15 年法律第 58 号）された。

(3) 特定個人情報の適正な取扱いに関するガイドライン（事業者編）［2-3］

番号制度の導入に伴い、国家による個人情報の一元管理、特定個人情報の不正追跡・突合、財産その他の被害等への懸念が示されてきた。

個人情報の適正な取扱いという観点からは、個人情報の保護に関する一般法として、「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「個人情報保護法」という。）、「行政機関の保有する個人情報の保護に関する法律」（平成 15 年法律第 58 号）及び「独立行政法人等の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号。以下「独立行政法人等個人情報保護法」という。）の三つの法律があり、また、地方公共団体では個人情報の保護に関する条例等において各種保護措置が定められている。

マイナンバー法（番号法）においては、一般法に定められる措置の特例として、個人番号をその内容に含む個人情報（以下「特定個人情報」という。）の利用範囲を限定する等、より厳格な保護措置を定めている。

本ガイドラインは、個人番号を取り扱う事業者（独立行政法人等個人情報保護法第２条第１項

に規定する独立行政法人等及び「地方独立行政法人法」（平成 15 年法律第 118 号）第２条第１項に規定する地方独立行政法人を除く。以下「事業者」という。）が特定個人情報の適正な取扱いを確保するための具体的な指針を定めるものである。

番号法では、前述のように一般法である個人情報保護法よりも厳格な情報管理を義務付けており、この事務処理等に関与する事業者の違反に厳しい罰則規定が定められている。尚、番号法は両罰規定があることや刑事罰以外にも民事訴訟等への対処も想定されるため、その経営陣は非常に厳しい経営努力を要求されることとなる。（善管注意義務や忠実義務等）

(4) クラウドサービス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［2-4］

本ガイドラインを情報セキュリティ管理、及び情報セキュリティ監査に活用することにより、クラウド利用者とクラウド事業者における信頼関係の強化に役立てることを目的とする。

本ガイドラインは、組織事業の基礎を成す情報資産の多くを、外部組織であるクラウド事業者が提供するクラウドサービスに委ねようとする組織が、 JIS Q 27002（実践のための規範）に規定された管理目的を達成するための管理策を実施しようとする場合を想定している。

全面的にクラウドサービスを利用する際の JIS Q 27002（実践のための規範）の管理目的達成という究極的な状況を想定することにより、クラウドサービスの利用において変化するシステム環境、責任の所在、事故や事象の判断基準を明確にする。

クラウドサービスを全面的に利用することにより生ずるリスクの変化に対応するため、JIS Q 27002 （実践のための規範）の管理策に、「クラウド利用者のための実施の手引」と、「クラウド事業者の実施が望まれる事項」を追加している。

2.2.2 IT を用いたシステムやサービスを供給しようとする提供者への指針

法令遵守しようとする利用者に対し、IT を用いたシステムやサービスを提供しようとする提供者（IT 事業者等の経営層）への指針について述べる。

これは、いわば車のディーラが客に車を薦める場合に近い。

（１）商品等の説明を適切に行なう責任

システム・サービスを供給しようとする供給者として、以下の項目について、対応しなければならない。

① 説明義務、説明責任
② 不当表示の禁止
③ スコープ範囲の明確化

上記のポイントは、一般消費者の利益を保護するための法律が「景品表示法（正式名称：不当景品類及び不当表示防止法)」でも要求され厳しい罰則も定められているところであるが、前述のように IT を用いたシステムやサービスを供給する側からすれば、非常に表現等に困るところである。何故ならば商品の設計開発や販売等の仕方にまで影響を及ぼす可能性のある事柄だからである。しかし、自らがそうした IT 等を導入する側に立って考えれば、自社での投資判断を行なう際に当然提供されるべき情報等であることは自明であり、今後特に法令対処に関する IT 等を市場に供給する者は、積極的にこうした取り組みをしなければならない。できる範囲、できない

範囲等を明確化し、利用者が納得できる商品を市場に供給しなければ、市場の選択に耐えられなくなる。

（2）第３者機関が認証した性能の提示

提示するソフトウェアの性能については、第３者機関による性能確認が望ましい。また、第３者機関は、提示された性能が出ない場合の駆け込み先としても必要である。

2.2.3 IT を用いたシステムやサービスを適切に用いて対処しようとする利用者への指針

法令遵守に IT を用いたシステムやサービスを適切に用いて対処しようとする利用者（ユーザ事業者等の経営層）への指針として、以下の項目について対応しなければならない。

① 善管注意義務
② 忠実義務
③ 適切な IT ソリューションを導入する責任

上記のポイントも、仮に事故が発生してしまうと取締役は、法律上、会社に対する善管注意義務（会社法３３０条、民法６４４条）及び忠実義務（会社法３５５条）を負っているので、会社や第三者に対する損害賠償責任等を負う可能性があり、取締役会設置会社である場合には、業務の適正を確保するための体制の整備についての決定は、取締役会によって行わなければならないとされている（会社法３６２条４項６号)。更に、従業員等の違法行為に関しては使用者責任も問われる可能性がある（民法７１５条、使用者責任)。企業・組織の経営者が、法令等の対処で IT 等を導入・投資検討をしている場合に重要視すべきことは、当然ながら、法令違反にならないような IT 等でなければならない。いい加減な導入判断を行なえば株主等を含めた利害関係者への説明責任も果たせない。例えば、マイナンバー法（番号法）の罰則は重く、違反者個人に加え違反者を雇用していた法人にも罰則が適用される。今後は、既存インシデント等の事例を調査することも含め、今まで以上に高い当事者意識を持って経営者としての適切な判断を行なうことになると考えられる。

3.4 節で、具体的な対策について述べる。

注：善管注意義務

民法 644 条で規定されている「善良な管理者としての注意義務」であり、業務を委任された人の職業や専門家としての能力、社会的地位などから考えて通常期待される注意義務のことである。

注意義務を怠り、履行遅滞・不完全履行・履行不能などに至る場合は民法上過失があると見なされ、状況に応じて損害賠償や契約解除などを受ける可能性がある。

また会社法 330 条においても株式会社の取締役は会社から経営の委任を受けているとされており、会社法 355 条においても「取締役は、法令及び定款並びに株主総会の決議を遵守し、株式会社のため忠実にその職務を行わなければならない」と規定されている。

また、法人及びその経営陣が、法律の要求する電子的な情報資産管理に必要以上に留意することで、経営判断が萎縮してしまうようなことがあっては経済活動自体がシュリンクしてしまい経

済崩壊を招きかねないことを回避するために、日本版ビジネスジャッジメントルールを市場啓発・普及も検討する必要があると考えられる。

注：ビジネス・ジャッジメント・ルール（business judgement rule）

経営判断の原則．アメリカの各州の判例法の中で発展してきた経営判断の法理である．その内容をどう解するかについては，アメリカにおいても変遷を経験してきた．最近のアメリカ法律協会のリステイトメントによると，取締役または会社役員は，自らが情報を得て合理的な調査をなし，誠実にかつ利害対立なく行動し，判断の合目的根拠を有する場合には，経営判断の結果について責任を負わないとする原則であると解している．たとえば，銀行の取締役がある会社に融資の決定をなす場合，その取締役がその会社の財務状況を適切に調査し，私欲ではなく誠実に行動した結果に基づいて融資をしたが，その融資が不良債権化してしまったとしても，その取締役の経営判断を尊重して取締役は経営責任を問われないとする考え方である．

わが国においては，経営判断の原則を肯定する最高裁判所の判決はなく，下級審裁判所ではこれを採用する判決がなされているに留まっている．また，学説の中でもこの原則を採用すべきだとする見解が次第に有力になりつつある．［黒木松男］

出典：学文社　増補版　現代経営用語の基礎知識
http://www.gakubunsha.com/manage-dic2/dataindex_ha.html

2.2.4 目的別カタログ

ユーザにとって、目的別の情報セキュリティ対策のためのカタログが必要である。できれば、各社のカタログを見比べることができることがよい。

その中には、以下の項目が必要となる。

① 情報システムの実現目的
② 個々の情報セキュリティ技術の解説
③ 利用実績
④ 価格

3.1 節で、事例を紹介する。

2.2.5 インシデント発生後の対応

特定個人情報の漏えいなどのインシデントが起こった場合、以下の対応が必要となる。

① 証跡管理
② インシデント発生の機関への報告
③ 保険支払いの問題

3.2 節で、検討内容を紹介する。

参考文献

［2-1］　「情報セキュリティマネジメントシステム(ISMS)とは」
http://www.isms.jipdec.or.jp/isms/index.html

［2-2］　「プライバシーマーク制度」　http://privacymark.jp/

［2-3］　「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」
平成 26 年 12 月 11 日　特定個人情報保護委員会

［2-4］　「クラウドサービス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」
2013 年度版　経済産業省

第3章　電子記録利活用の情報セキュリティ推進の検討

本章では、まず、「電子記録利活用セキュリティ対策事例」を示すとともに、「インシデント対応と証拠保全」、「個人情報の非個人情報化今後」、「防止策・インシデント対応」について述べる。

3.1　電子記録利活用のための情報セキュリティ対策事例

昨今、スマートデバイス、BYOD (Bring Your Own Device) [3-1]での電子記録利活用が増え、とても便利になってきている。しかしながら、セキュリティインシデントは後を立たない。電子記録利活用における企業の課題は様々であり、またその対策としても様々な方法がある(電子記録管理に関する調査検討報告書 2013 参照のこと)が、本項では、電子記録利活用における課題と対策を、先進的なユースケースにフォーカスして紹介する。

なお、電子記録利活用における事例の利用用途として大きく以下の類型がある。

- 閲覧(メールやスケジュールなどの編集も含む)
- 交換
- 持ち出し

なお、本節では、秘密分散技術で分割生成された電子ファイルを「割符ファイル」といい、分割生成することを「割符化」という。

3.1.1 モバイルネットワーク、事業継続（閲覧）

（1）課題

スマートデバイス、モバイル PC から安全に組織内の情報を閲覧・参照したい。

ワークスタイルの変革をしたい(スケジュールや掲示板、Web メールなどの編集をしたい)。

（2）解決策

クライアント証明書でデバイス認証が可能なセキュアブラウザにて実現。出先機関への出張中や自席を離れていても、モバイル PC やスマートデバイスで、スケジュールのチェックや情報の確認ができるようになった。

① セキュアブラウザ

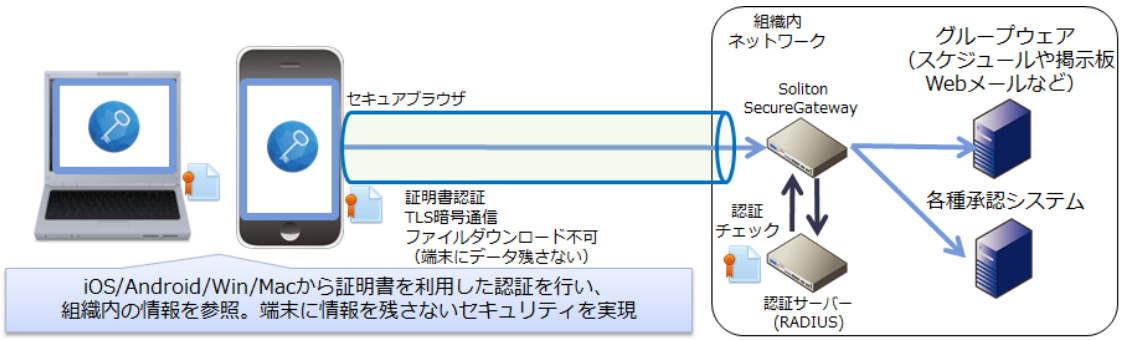
セキュアブラウザは､外部から受け取ったプログラムを保護された領域で 動作させるサンドボックス技術[3-2]を利用してブラウザ内のデータをアプリケーション外に取り出せない様に配慮された Web ブラウザである。閲覧、ダウンロードしたコンテンツは、セキュアブラウザの利用を終了すると同時に自動的に削除されるよう実装されていたり、さらに、アクセスできるサイトを制限する機能を搭載したりする製品もある。

電子記録管理システムや、業務用システムの多くがサービスを Web で提供する現在、外出先など外部から自組織内やクラウド上の電子記録管理システムへのアクセスも Web ブラウザをアクセスツールとして利活用することが想定される。

利用者が外出先や自宅などで利用する端末は、PC に限らずスマートデバイスなど多様な端末

が想定される。しかし、いずれを利用しても、扱った電子記録は利用端末内に残置されないことがセキュリティ対策面で重要視される。このため、自組織内やクラウド上にある特定の電子記録へのアクセスツールとしてセキュアブラウザが注目され、導入されつつある。現在では、すでに国内外を問わず複数の製品が提供されている。

（３）事例



※「政府機関の情報セキュリティ対策のための統一基準群」平成 26 年度版(案) 7.1.1(1)-4 e）、8.2.1(1)-3 等では、「セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境の構築。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする」方式が基本対策事項として取り上げられている。[3-3]

図 3-1 モバイルワーク、事業継続（閲覧）

3.1.2 機密情報の参照（閲覧）

（１）課題

個人情報を含む、機密情報へのアクセスをセキュアに行いたい（マイナンバーに備えたセキュリティ対策）。

（２）解決策

端末利用時の多要素本人認証（IC カード等のデバイス認証）、端末操作ログの導入、電子証明書を利用したネットワーク認証により、要機密情報へのアクセスを透明化し、監査にも対応できるようになった（証跡管理）。

①IC カード認証

セキュリティ対策において、基盤となるのは「本人認証」である。たとえログ管理や暗号化などの情報セキュリティ対策が施されていても、ID とパスワードの貸し借りや漏洩などによって、簡単にユーザの成りすましができてしまう環境では、情報へのアクセスが不正に行われる危険がある。IC カード認証は、社員証やビルの入館証、通勤で使用している交通系の電子マネーなどの IC カードを使って、端末利用時の本人（ユーザ）認証を強化し、データへのアクセス制御とログ管理をトータルに実現する端末セキュリティシステムである。

②ネットワーク認証

会社のネットワークは、企業に蓄積されたあらゆる情報への出入り口である。誰もが無秩序に接続できる状態ではなく、決められた人、決められた PC・スマートデバイスだけが接続できるように鍵をかけておく必要がある。その中でも電子証明書認証は一番セキュリティ強度が高く、

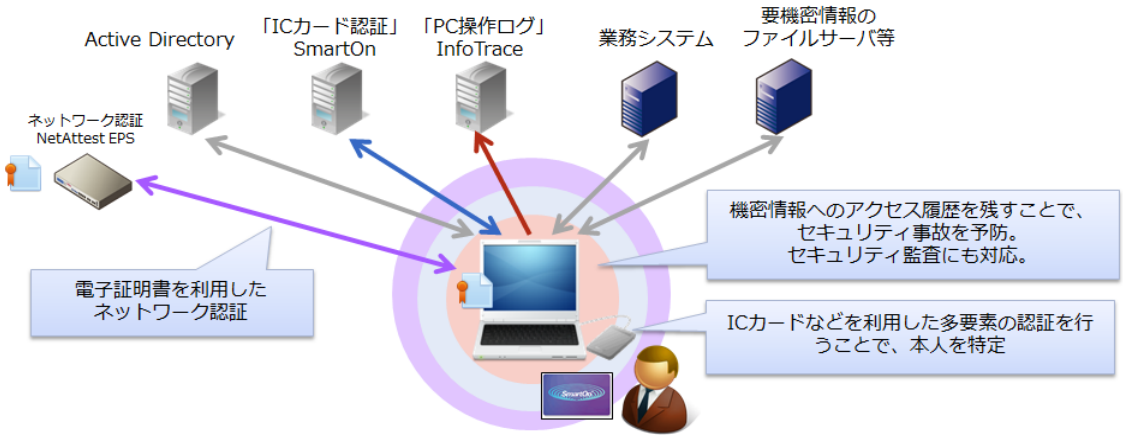
また確実に端末認証を行うことができる。証明書を「認証」、「電子署名」、「暗号化」に使用することで「なりすまし」、「データの改ざん」、「盗聴」を防止できる。これによって、IT セキュリティを確保するとともに、IT 統制への対応に役立てることができる。

③端末操作ログ

端末の操作ログを取得することにより、情報漏洩行為の抑止効果が期待でき、日々のログ運用はレポートでチェックできる。また、カーネルレベルでの検出が行える製品であれば、「誰が」「いつ」「何をしたのか」を正確に把握できる。

（3）事例

公共・民間でのユーザ事例



※「組織における内部不正防止ガイドライン」 Ver 1.2（IPA、2013.12）「情報システムにおける利用者の識別と認証」[3-4]

図 3-2　機密情報の参照（閲覧）

3.1.3 機密情報のアップロード（交換）

（1）課題

災害・事故現場・工事現場などの写真をセキュアに共有したい。

（2）解決策

セキュアブラウザ＋秘密分散技術や、ファイル共有アプライアンス等で実現(以下は前者の例)。

①電子割符ゲートウェイ

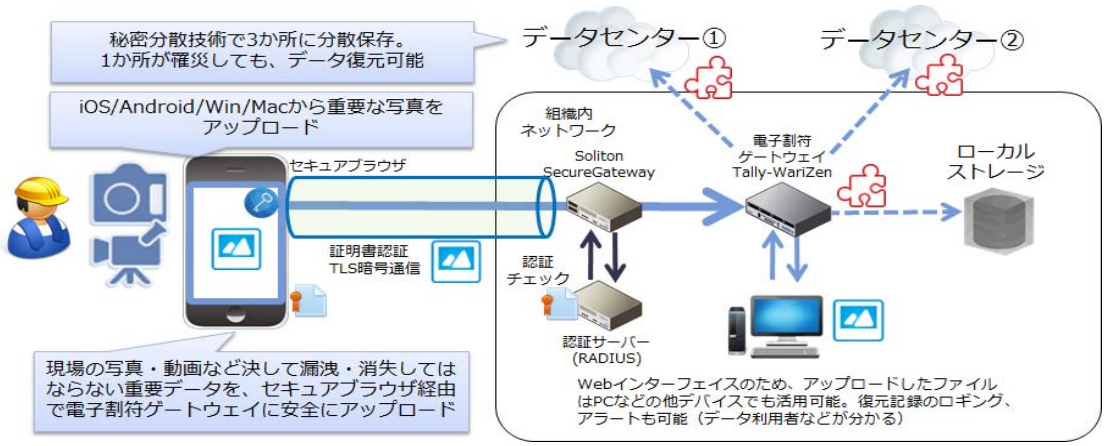
電子割符ゲートウェイとは、秘密分散技術を用い、1 つのデータを元データとは全く関係のない複数の割符ファイルに分割し保護する技術を用いた装置である。元データはビットレベルで分割・割符化される。1 つの割符ファイルからは、元の内容が一切分からないため、個人情報等の機密データを安全に保管することができる。また、元データを復元するためには、基本、すべての割符ファイルが必要であるが、割符化する際に割符ファイルに冗長を持たせることで、一部の割符ファイルが欠けても元データを復元することが可能である。

例えば、機密データを秘密分散技術で分割し、各種ストレージに分散保管する。分割したファイル（割符ファイル）からは、元データの内容が一切分からないため、クラウドストレージを安

全に利用できる。さらには、機密データを割符化する際にデータに冗長を持たせることで、一部の割符ファイルが不測の事態で消失しても元データを復元することができる。決して失ってはならない機密データの災害対策に有効である。

（3）事例

公共・建設など



※電子割符ゲートウェイ単体でも、クライアント証明書認証を行うことは可能だが、この提案では、安全な接続経路の確保のためにセキュアブラウザを併用している。

※電子証明書による端末認証は不要で、ユーザ認証のみで良い場合は、セキュアブラウザや認証サーバ（RADIUS)を無しとし、電子割符ゲートウェイにアップロードさせる構成も可能。

図 3-3　機密情報のアップロード（交換）

3.1.4 組織外との情報共有（交換）

（1）課題

組織外の取引先と安全に機密情報のやり取りを行いたい。

USB 接続機器は利用させたくない。

（2）解決策

ファイル共有・転送アプライアンスを利用。メールとは異なり送信履歴が残り、大容量のファイルも USB ストレージを利用せずにやり取りできた。

①ファイル共有アプライアンス

画像や動画を貼りこんだリッチなプレゼン資料、音声ファイル、印刷データや CAD データなど、業務で扱うデータは年々大容量化している。組織を跨いだ協業が当たり前となった今、こうした大容量データのやり取りに多くのユーザが苦労している。

その問題を解決するのが、ファイル転送アプライアンスである。一般的なファイル転送サービスは既に存在するが、アプライアンスであれば自社で運営できるのでセキュリティ面でも安心できる。

例えば、禁止しているはずなのに、USB メモリやフリーのファイル転送サービスでデータを持ち出す、大量のファイルをメールに添付して何度も送信、はたまた輸送コストをまったく意識せ

ずディスクでやり取りする組織のユーザ。 たとえ悪意がなくとも、こんな状況は決して見過ごせるものではない。 しかし、業務で必要なデータのやり取りを禁止するわけにもいかず、ユーザの教育には時間も根気もいる。そのような時に有用なのがファイル共有アプライアンスである。

（3）事例

府中市（国体（スポーツ祭東京 2013）での利用）など

建設（協力会社との設計図面などの情報共有）

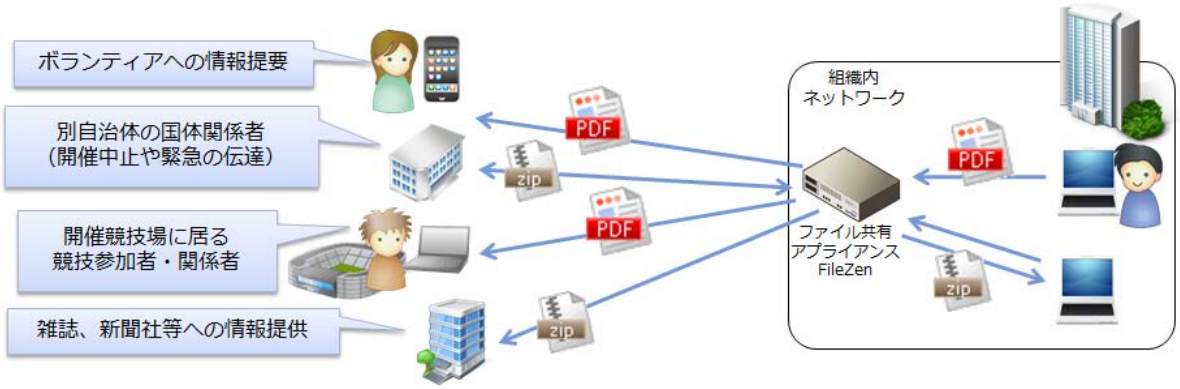


図 3-4　組織外との情報共有（交換）

3.1.5 機密情報移送時のセキュリティ・モバイル PC からの情報漏洩防止（持ち出し）

（1）課題

PC や USB メモリ等外部メディアに保存される個人情報を含むデータを保護したい。

ファイルや HDD の暗号化対策は、万一の紛失時でも情報流出にあたるため、法令上の対策が行えるソリューションを探していた。

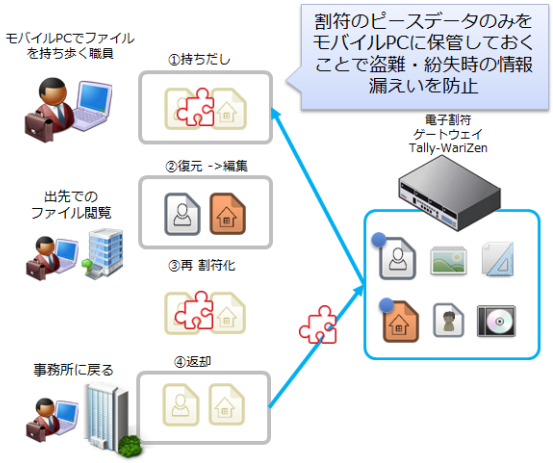
インターネット接続がない環境でファイルを利用する必要がある。

（2）解決策

電子割符ゲートウェイ経由で割符化されたデータを用いて運用することで課題をクリア。

（３）事例

某公共団体



電子割符に対する法的見解 単体としての電子割符情報は、他の割符と容易に結合できる状態でない限り、個人情報とはいえない※

※JIPDEC 次世代電子商取引推進協議会（ECOM）が 2010 年 3 月に発表した「EC における情報セキュリティに関する活動報告書 2009」の「情報分散管理技術（電子割符技術を利用した情報管理）に関する法的意見書」[3-5]

図 3-5 機密情報移送時のセキュリティ・モバイル PC からの情報漏洩防止（持ち出し）

3.2　インシデント対応と証拠保全

昨今、内部犯行やインシデントなど、顧客データ、機密データの漏洩が後を絶たない。

特に機微情報の漏洩は企業内外に大きな損害をもたらすため、「誰が」「いつ」「どこで」「何をして」など、企業がすぐに把握し、インシデント対応する必要性がある。

マイナンバー法(番号法)施行では、罰則規定がありシステム操作者や特定個人情報に関わる人達のインシデントの把握、解析、対応が重要になり、事案の内容によっては、証拠保全なども必要になってくる。

特に注目したい対策法では、現行法である個人情報保護法でも利用実績が高く、追跡手段や監査的にも利用される「端末認証」と「端末操作ログ」である。

（１）端末認証と端末操作ログへの対応

端末等のネットワーク接続に対しては、昨年の報告書「電子記録管理に関する調査検討報告書 2013」にもあるように、電子証明書がインポートされていない端末を社内ネットワークに不正アクセスさせない等の対策がある。しかし、正規の接続端末における操作がポリシーに準拠しているかどうかは、端末上で操作ログを取得して把握する必要がある。例えば、暗号化されたファイルによる情報漏洩などはネットワーク監視では把握できない。　また、記憶媒体に対しては、USB メモリや CD、スマートデバイス等を社内端末で使用禁止にする対策もあるが、この方法では「内部」の者が意図的にデータを持ち出すことへの対策にはならない。内部の者は「許可された人」であり、「許可された端末」を使用している。もしかしたら、許可された人であれば USB メモリなどの記憶媒体も使用できるかもしれない。このように内部の者が情報を持ち出すことを完璧に対策することは難しいため、「誰が」「いつ」「何をして」情報を持ち出したのかを正確に把握する

必要がある。

（２）マイナンバー法(番号法)への対応

さて、昨今話題となっている、マイナンバー（番号法）に係るセキュリティに関する注意点として、2014 年のパブリックコメント版からいくつか挙げたい。

「どこまで対策すれば良いのか？」といった関心の高い疑問への答えとして、パブリックコメント上で発表された「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」［3-6］から抜粋する。

今回のガイドライン［3-6］では、例示など様々されているが、事業者（個人事業主を含む）を対象にし、大企業から小企業まで対応を求められている。ガイドラインの対応をした場合、大企業のように大きな予算を持って対応が出来ない。専任担当者をアサインできない。専用の物理区画や情報機器（PC 等）を用意できない。等の多くの声も多く聞こえている。

しかし、ガイドライン［3-6］の P1 では、

「本ガイドラインの中で、「しなければならない」及び「してはならない」 と記述している事項については、これらに従わなかった場合、法令違反と判断される可能性がある。一方、「望ましい」と記述している事項については、 これに従わなかったことをもって直ちに法令違反と判断されることはないが、番号法の趣旨を踏まえ、事業者の特性や規模に応じ可能な限り対応することが望まれるものである。」

とある。

上記、前段の、**【これらに従わなかった場合、法令違反と判断される可能性がある。】**と記載された内容で特に注意が必要な点を記載した。

また、実際の法令違反となる場合の罰則規定も記載しておく。

以下が「マイナンバー法(番号法)」における罰則である。

罰則(第 62 条～第 72 条)

[個人番号を利用する者に関する罰則(第 62 条～第 64 条、第 66 条)]

- 正当な理由なく、特定個人情報ファイルを提供(個人番号利用事務等に従事する者等)
  ⇒4 年以下の懲役若しくは 200 万円以下の罰金又は併科
- 不正な利益を図る目的で、個人番号を提供又は盗用(個人番号利用事務等に従事する者等)
  ⇒3 年以下の懲役若しくは 150 万円以下の罰金又は併科
- 情報提供ネットワークシステムに関する秘密の漏洩又は盗用(情報提供ネットワークシステムの事務に従事する者)
  ⇒3 年以下の懲役若しくは 150 万円以下の罰金又は併科

上記に即罰の可能性も示唆されているなか、注意が必要な点について、「特定個人情報ファイル」「個人番号(データ)」「情報提供ネットワークシステム関する秘密(データ)」の提供、漏洩等の調

査が必要になることが分かる。しかし、以下に抜粋した「(別添) 特定個人情報に関する安全管理措置)」[3-6]の「2-C-b 取扱規程等に基づく運用」にもある「特定個人情報ファイルの削除・廃棄記録・削除・廃棄を委託した場合、これを証明する記録等・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況(ログイン実績、アクセスログ等)の記録」に関して、一般的なアクセスログ、認証のログを取っているだけではインシデント対応が難しいため、調査においても端末操作ログを取得しておかなければならない可能性が高いと考えられる。

（3）一般的なインシデント対応

その例として､一般的なインシデント対応の流れを以下に示す｡調査に対する内容は様々あり、実際の調査と言う意味で、このようなケースが現在でも考えられる。

① 重要なファイルがコピーされたようだ。(インシデントの露見)
② イベントとして、ファイルが USB に書かれた？（インシデントの推定）
③ いつ、だれが、どのように？どこで？どこから？（原因追究）
④ なぜ？　本当に書き込まれているのか？？（インシデント発生の確認）
⑤ 保全活動・証拠保全（悪意、善意、過失など関係なく）

上記について、ガイドライン［3-6］では情報漏洩防止策があるなか、調査に必要なポイントの記述は少ない。そこで以下に例示する。

マイナンバーデータの操作者がオペレーションミスにより、個人情報ファイルを USB にコピーしそうになったが､それに気づき中断した｡しかしながら､管理者にコピーしたと誤認された。

何故このようなことが起きてしまったのか。簡単に解説すると、コピーイベントのみが管理者に通知され、コピーしたと疑われた。実際には書き込んだファイルのバイト数が 0 バイトであるにも関わらず、カーネルレベルでログを取得しないシステムを導入した例では、個人情報ファイルが USB に書かれた(COPY)としか判断していないため、事実と違うことが分からなかったのである。

誤認については以下にも参考出典を示す。[3-7]

後を絶たない「監視カメラ誤認逮捕」不鮮明な映像根拠に自白強要

監視カメラは全国に 500 万台以上設置されていると見られ、その映像が犯罪調査の重要な根拠となる機会も増えている。しかし、監視カメラ映像による誤認逮捕が全国で相次いでいるという。NHK の調べでは、2011 年以降、コンビニ、路上、ATM、ガソリンスタンド、リサイクルショップ、スーパー、パチンコ店などの映像をもとにした誤認逮捕が起きている。

設定時間のズレに気付かず別人逮捕

2014 年春、パート店員の女性は客として訪れたパチンコ店で、別の客がパチンコ台の上に置き忘れた財布を盗んだ疑いで逮捕された。財布を忘れた客の後に座ったのがこの女性で、台の上に手を伸ばすような仕草をしていた。「クローズマップ現代」が検証すると、カメラの画質や設置場所などから、女性が財布を取ったかどうかまでは映っていないはずだが、警察は「何回もビデオを見てもあなたが盗っているように見える」などと自白を迫った。

しかし、結局は 7 日後に釈放された。女性が席を離れた後に座った人物が財布をゴミ箱に捨てる映像や財布を手にする映像があり、真犯人だと判明したのだ。警察は映像を一部しか見ておらず、ずさんな捜査だったと謝罪した。

犯行現場のカメラの設定時刻がずれていたのを警察が確認しなかったため、違う時間にたまたま映っていた男性を逮捕した例もあった。取材した NHK 記者は「ビデオを操作に活用しているわりには、ずさんな扱いをしている例があると感じる」と話す。

このように、ひとつの映像のみでの判断や、時刻のずれを確認していなかったことによって誤認されることが日常的に起こりうる。特定個人情報の取扱いにおいては特に厳格な管理が必要である。例えば、証拠保全の観点から端末操作ログの取得は不可欠だが、時刻を正確に記録することと、コピーイベントにおいて「読み込んだファイルのバイト数」と「書き込んだファイルのバイト数」のログをカーネルレベルで取得可能な端末操作ログシステム(株式会社ソリトンシステムズの InfoTrace など)が製品選定において重要である。

（4）誤認への対策

IC カード認証による個人特定、秘密分散技術によるマイナンバー記載書類の保管、情報漏洩が無過失であることの証明に役立つ、正確な端末操作ログの取得を組み合わせることにより、安全にマイナンバーを取り扱うことができると考える。

では、もしも実際にインシデントが発生した場合は、どのように対応すれば良いのか。ここからはインシデント発生時における証拠保全の必要性について話を進める。

以下にインシデントレスポンスに必要な項目と流れを示す。

1. 端末・サーバアクセスの状況把握
2. ネットワークアクセスの状況把握

3. ログの検索、調査、確認
4. 保全活動(証拠保全＜状況保全) ※ガイドライン[3-6] P53 の d 参照
5. コンピュータフォレンジック
6. インシデント内容による各種対応
7. 各種、安全管理措置の確認、修正、更改等

実際のインシデント調査では以下が必要になる。

- 被害内容(情報漏洩、システム破壊、不正操作、データ改竄…)
- 被害原因(マルウェア、内部犯行、システム障害、人為的ミス…)
- 被害範囲(何台、どの端末/サーバ、関連・協力会社は？…)
- 被害時期(数時間前、先週、昨年…)

しかしながら、昨今のサイバー攻撃や不正利用などの全容把握は困難になりつつある。コンピュータフォレンジックと、ネットワークフォレンジックを行なったうえで相関分析し、ようやくインシデントの全容把握が可能となる。

それでは、どのような端末操作ログなら役に立つのか？

- 確実な端末操作ログ取得のための措置(ログ取得は不正停止されていないか？)
- 相関分析のためのキー情報(動作時端末の持つ複数の IP アドレス、タイムスタンプ、ホスト名、認証の情報等)が正しく記録・保存されていること
- 例として操作したファイル名だけではなく、本当に書きだしたのか？読み込んだファイルのバイト数・書き出したファイルのバイト数が取得でき、正しく判断できること(いわゆるカーネルレベルのログ取得)
- リモートデスクトップ等からの接続時間

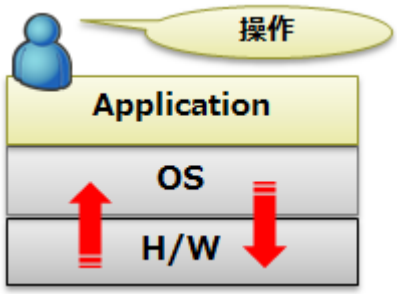


図 3-6　カーネルレベルでの端末操作ログの取得

インシデント発生時の証拠保全とは、調査対象のコンピュータ等を現状のまま確保し、原本と同一性を保ちつつ電子データをコピーする行為である。証拠となるコンピュータ等をすぐに現状のまま確保しておかないと、「共謀して証拠データを改竄しているのでは？」や「証拠を隠すためにデータを削除しているのでは？」と疑われる場合がある。電子データは改変しやすく、コンピュータを起動しただけでも電子データは変化し、対応を協議している間でも、対象端末を使用し

ていると証拠隠滅の疑いがもたれる場合もある。

注意点としては、インシデント発生時に問題の端末に対し、以下のような対応をとると、専門調査に支障をきたし、データ改竄を疑われるので厳に避けなければならない。

- 使い続ける
- 廃棄する
- 初期化、フォーマット
- 内部で直接端末に対して調査
- ウイルススキャンをかける
- 再起動や電源 ON/OFF の繰り返し

それでは、証拠保全を意識した対応とはどのようなものか。インシデントが発生した時点で、すぐに以下の対応を取れば専門調査もしやすくなる。

- 問題となる機器をすぐに確保
- 問題となる機器を使わせない、使わない
- 問題となる機器のネットワークケーブルを抜く
- 再起動、電源 ON/OFF をしない
- 内部だけで調査しようとしない
- 電子データ調査の専門家に相談

その際証拠保全の対象として、組織が所有するスマートデバイス、携帯電話、デスクトップ・モバイル PC、USB メモリ・SD カード、CD・DVD-ROM などの電子機器を確保する必要がある。

このように、インシデントが起きないためのセキュリティ確保はもちろんのこと、インシデントが起きてしまった場合の対応についても、マイナンバーを取り扱うことにおいて十分注意する必要がある。

※参考出典［3-8］「証拠保全ガイドライン 第 3 版」

3.3 個人情報の非個人情報化

秘密分散技術により、個人情報や特定個人情報を処理し生成された個々の割符ファイルを適切に管理することにより、個々の割符ファイル単体は個人情報保護法、マイナンバー法（番号法）の対象外（非個人情報化）にすることができるため、単体からの復元可能な情報も含む完全な情報を一元管理するような通常の情報管理に比べ、情報漏えい等に対する耐性を向上させ、事故発生によるリスク顕在化を未然防止するだけでなく、対象情報の委託・受託時の監督責任や管理責任を全うする際にも役立つ。また副次的効果として、割符ファイル単体が法令上の定義項から除外されることから、海外のサーバに単体の割符ファイルを置くことも可能になる。

（１）暗号化された個人情報や個人番号及び特定個人情報の扱い

個人情報保護法において、既公開の「経済産業省個人情報保護法ガイドライン」（平成２６年１２月、以下、「経済産業省個人情報保護法ガイドライン」とする）定義項解説部分に記載の「～、

暗号化等によって秘匿化されているかどうかを問わない（ただし、「2-2-3-2.安全管理措置（法第２０条関連)」の対策の一つとして、高度な暗号化等による秘匿化を講じることは望ましい。)。」
の記述は組織として個人情報を暗号化等を実施して管理していても、それが漏洩等した場合には個人情報漏洩とみなすことが明記されている。

また、2014 年 10 月 27 日に特定個人情報保護委員会が開催した本法に関する給与計算等ソフトウェア制作事業者向け説明会で、暗号化してあっても個人番号であり特定個人情報であるとの認識が明確に示された。(個人番号のマスキングに暗号利用した場合も含む)

マイナンバー法（番号法）はその法律の一般法である個人情報保護法よりも厳格な管理を要求しており、更なる情報管理の厳格性を要求することが示されたと言える。また、生業として個人番号や特定個人情報を管理する事業者は、どんなに自らの事業規模、組織規模が小さなものであっても、しっかりとした法対処をしなければならないことも明確に示された。(注１)

このことは現実に漏洩してしまった際のリスク顕在化の懸念を考えると、これは暗号の誕生経緯を振り返ると納得できることでもある。

暗号は主として戦場での情報伝達を主眼に工夫されてきたのである。つまり、作戦実行するまでの間に敵に傍受等されても解読されない「時間を稼ぐ」ことが最重要な機能であり、長期的な秘匿性よりも最前線での復号速度等の方が重要であることは改めていうまでも無い。こうしたことから暗号化は秘匿化技術の一つであり、非個人情報化を実現する技術ではないと言える。

（２）組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置

既公表のガイドライン等も暗号化した際の鍵管理も完璧にできていた場合に、解読までの時間を稼ぐことで、攻撃者に解読する為の時間と労力を費やさせる。という暗号化による効果を得るための投資をすること自体の意義は認めるものの、法律の求める期間の安全性確保という観点からは、様々なリスクも考慮しなければならない。こうした行政判断上致し方の無い見解として記載された文言のひとつの例が後述する「望ましい」という表現と言えるであろう。更に、鍵管理が徹底できていない場合の安全性の問題も実際の暗号利用現場においては頭の痛い事実である。但し、管理対象となる情報自体の安全性を直接向上させる手段（技術的安全管理措置のうち、暗号や秘密分散技術等を指す）は、様々なセキュリティ対策の最後の砦と言えるもので、非常に大事なものであることは普遍であり本項で取り上げている秘密分散技術等の新たな特性を持つセキュリティ技術等の一般化が望まれるところである。

ちなみに、「経済産業省個人情報保護法ガイドライン」記載の高度な暗号化等の暗号は、政府推奨暗号かＩＳＯ等の国際機関に登録されているものが対象である。(秘密分散法コンソーシアム（注２）による経済産業省確認 2014 年 12 月 04 日)

総合すると、現実的な対処法はその他の「組織的安全管理措置、人的安全管理措置、物理的安全管理措置」と「技術的安全管理措置」を事業者自身の現場工夫で効果的・合理的に組み合わせ運用することで、法の要求が強化されたことによってこれから様々な現実的な対処事例が出てくるのではないかと考えられる。

（３）暗号技術と秘密分散技術

マイナンバー法（番号法）での暗号技術と秘密分散技術の比較を表 3-1 に整理する。

	秘密分散技術	暗号技術
個人情報か否か	秘密分散技術で作成された「割符ファイル」単体は個人情報の定義項から除外されているが、復元に足る数の「割符ファイル」があり容易に照合・復元できれば、個人情報に該当	個人情報及び特定個人情報は、暗号化後も個人情報及び特定個人情報に該当
原理的背景	集合論（部分集合）や秘密分散法等	集合論（写像）や素因数分解の困難性等

表 3-1　暗号技術と秘密分散技術

表 3-1 のうち、原理的背景部分は、「そもそも現時点で解法が想定できているものと、そうではないもの」との違いが根底にあることがポイントで、この原理的特性が様々な解釈等の際の違いに出てきているところに注意したい。暗号化された特定個人情報は特定個人情報のままであるが、秘密分散技術で処理された特定個人情報の各々の割符ファイル単体は特定個人情報ではないといった特徴があり、暗号技術も含め他の安全管理措置と組み合わせることで、より効果的且つ合理的な利活用が可能である。

（注１）

「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」の

（別紙）ガイドライン（事業者編）（案）に関する意見募集結果について

http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=240000003&Mode=2

の No,60 の回答では、

「～なお、上記における個人番号をその内容に含む電子データは、仮に暗号化等により秘匿化されていても、その秘匿化されたものについても個人番号を一定の法則に従って変換したものとして、個人番号として取り扱われます。」と記載されている。

（注２）秘密分散法コンソーシアム：

秘密分散法コンソーシアムは、秘密分散法の広範な社会的有効活用及び秘密分散技術の健全な市場普及とを目的として、2002 年 10 月 10 日の創設した非営利の民間団体。

（http://www.gfi.co.jp/01news20141112_361.html）

（http://www.gfi.co.jp/01news20140926_358.html）

3.4 防止策及びインシデント対応策

「2.3.3　IT を用いたシステムやサービスを適切に用いて対処しようとする利用者への指針」では、その概要を示したが、ここでは防止策及びインシデント対応策について検討を進める。

実際に法令上安全管理義務を要求されている情報が漏えい等した際に、どのように解釈されるのかを把握しておくことは重要である。

本節では、個人情報保護法[3-9]とマイナンバー法（番号法）[3-10]への対応を主として扱う。

防止策、インシデント対応に関するポイントは、以下のとおりである。

（1）　漏えいや流出事故等を起こさない対策を行う（残存リスクを正確に把握する）

（2）　漏えいや流出事故等が発生しても実害が生じない対策を実施する

（3）　日常的に安全管理措置を徹底していることの証拠を残す

（4）　不幸にして事故等が発生した際には、迅速に必要な対処を行う

以下、それぞれについて詳しく説明する。

3.4.1 漏えいや流出事故等を起こさない対策を行う（残存リスクを正確に把握する）

先ず、対象となる情報の管理の仕方は以下が考えられる。

A：対象情報を自らの組織で管理する

B：対象情報を外部委託する

C：非個人情報化を利活用する

D：そもそも対象となる情報は取得しない

D に関しては本報告書の対象とはならないので除外すると、A か B、または C のいずれかとなる。

そもそも漏えいや流出事故等を起こさないというのは、言うまでも無く大原則なのであるが、内部統制問題等も絡み非常に大きな経営課題である。現実の姿として、外部委託先の作業員等も含め、結局はいずれかの組織に属していることから単独の窃盗犯等以外は実際のところ内部犯行とも考えられる。そうしたことを考えると、前述の「1.2　セキュリティ対策推進の阻害要因」で触れたように、「～現在多くの情報システムの安全性が多くの管理者の方々の善意で支えられており、雇用・人事・職場環境の改善といった、一見情報セキュリティとは直接関係がなさそうに見える経営的な施策と企業・組織の健全化そのものが、結果として情報保護のためにも有効であるということを示していると考えられる。」というデータベースコンソーシアムの報告内容[3-11]は、非常に経営陣にとって重いものである。

一般論として、雇用・人事・職場環境の改善等は一朝一夕に実現できるものではないことを考えると、法令対処を行う組織の経営陣は、内部犯行・漏えいや流出等は、想定の範囲として対策を検討しなければならない時代といえる。では、漏えいや流出事故等を起こさない対策を行うにはどうしたら良いのか。

「対象となる情報を持たない」のが、究極の対策と言えるのだが、多くの場合実務上不可能である。というのも、外部に委託して管理したとしても、個人情報保護法もマイナンバー法（番号法）も委託元による委託先の監督責任を課しているからで、委託元の管理責任は免れないからである。

―経済産業省個人情報保護法ガイドライン冒頭部の対象記述箇所抜粋部―

法第２２条

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（解説部抜粋）

～「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第２０条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取扱状況を把握することが含まれる。

なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。

―マイナンバー法（番号法）ガイドライン事業者編冒頭部の対象記述箇所抜粋―

（再委託）

第十条　個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）の全部又は一部の委託を受けた者は、当該個人番号利用事務等の委託をした者の許諾を得た場合に限り、その全部又は一部の再委託をすることができる。

２　前項の規定により個人番号利用事務等の全部又は一部の再委託を受けた者は、個人番号利用事務等の全部又は一部の委託を受けた者とみなして、第二条第十二項及び第十三項、前条第一項から第三項まで並びに前項の規定を適用する。

（委託先の監督）

第十一条　個人番号利用事務等の全部又は一部の委託をする者は、当該委託に係る個人番号利用事務等において取り扱う特定個人情報の安全管理が図られるよう、当該委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（解説部分抜粋）

～必要かつ適切な監督

「必要かつ適切な監督」には、①委託先の適切な選定、②委託先に安全管理措置を遵守させるために必要な契約の締結、③委託先における特定個人情報の取扱状況の把握が含まれる。

委託先の選定については、委託者は、委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。具体的な確認事項としては、委託先の設備、技術水準、従業者（注）に対する監督・教育の状況、その他委託先の経営環境等が挙げられる。

委託契約の締結については、契約内容として、秘密保持義務、事業所内からの特定個人情報の持出しの禁止、特定個人情報の目的外利用の禁止、再委託における条件、漏えい事案等が発生した場合の委託先の責任、委託契約終了後の特定個人情報の返却又は廃棄、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定等を盛り込まなければならない。また、これらの契約内容のほか、特定個人情報を取り扱う従業者の明確化、委託者が委託先に対して実地の

調査を行うことができる規定等を盛り込むことが望ましい。

上記のように、個人情報保護法もマイナンバー法（番号法）も対象となる情報の管理等を委託することは可能であるが、漏えいや流出等の事故に対し委託先に全責任を負わせるようなことはできない。しかも、委託先を適切に選定する義務と、監督責任も発生するのである。一概には言えないが、そこまでして費用を支払って外部委託しても、情報漏えいや流出事故等が発生した場合には委託元の管理責任問題と損害賠償対処の可能性があることは確かである。

A：対象情報を自らの組織で管理する
- １００％の管理責任を当初から自覚した対処を具体化する必要がある
- 単に情報管理だけを意識した対策では、内部犯行を未然防止できない

B：対象情報を外部委託する
- 委託元の監督責任を免れることはできない
- 委託先でも内部犯行の可能性があることを意識した監督が必要

C：非個人情報化を利活用する
- 組織として個人情報や特定個人情報として管理するが、個々の割符ファイル単体は法令の定義項から除外された状態で保存し、万が一の漏洩等を意識した安全管理措置
- 組織内であれ、委託先であれ単体の割符ファイルでは個人情報や特定個人情報に復元出来ないため、適切な割符ファイルの管理を行えば事実上対象となる個人情報や特定個人情報を複数の相互監視の下で管理する形となる

結論としては、漏えいや流出等の事故発生は、自社で情報管理を行おうと外部委託しようとも発生する可能性はあり、いずれの場合でもそうした事故が発生した場合には、経営陣にも責任問題が発生するということであり、昨今の一般常識と大きく乖離のない結果である。そうした際に個人情報や特定個人情報の法令上の定義項から除外されるような安全管理措置を実施することは非常に有力な対処法と考えられる。

3.4.2 漏えいや流出事故等が発生しても実害が生じない対策を実施する

法令上の要求事項である対象情報の安全管理措置をどのように実施すれば良いのかがについて述べる。

現実に漏えいや流出が発生しているのに実害が生じないとは、次の 2 つの場合が想定される。

（1）：事業者にとって実害が発生しないこと

（2）：情報の対象者等にとって実害が発生しないこと

（3）：法令上の解釈からも対象情報の漏えいや流出と看做されないこと

（1）：事業者にとって実害が発生しないこと

事業者にとって実害が発生しないとは、次の 2 つの場合が想定される。

①実害は発生しているが、事業者には全く関係の無い領域で発生している

②実害は発生しているが、その実害全てを賠償できる対策が整っている

①に関しては、元となる情報の漏えいや流出等を発生させたのが自らの組織であるとすれば、全く無関係な領域で発生したとは言いにくいと考えられる。しかし、情報漏えいや流出等は発生したものの、そのことには全く責任が無いと証明できる場合は対象となる可能性がある。前者と後者は大きな違いがある。

ポイントは個人情報保護法、マイナンバー法（番号法）の両方で規定されている「安全管理措置」である。

―経済産業省個人情報保護法ガイドライン冒頭部の対象記述箇所抜粋部―
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。

―マイナンバー法（番号法）ガイドライン事業者編冒頭部の対象記述箇所抜粋―
第４－２－⑵ 安全管理措置
安全管理措置（番号法第 12 条、第 33 条、第 34 条、個人情報保護法第 20 条、第 21 条）
個人番号関係事務実施者又は個人番号利用事務実施者である事業者は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の漏えい、滅失又は毀損の防止等、特定個人情報等の管理のために、必要かつ適切な安全管理措置を講じなければならない。また、従業者（注）に特定個人情報等を取り扱わせるに当たっては、特定個人情報等の安全管理措置が適切に講じられるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
（注）「従業者」とは、事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいう。具体的には、従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。

から考えると、「①　実害は発生しているが、事業者には全く関係の無い領域で発生している」状態というのは考えにくい。

2-2-3-4.　委託先の監督（法第２２条関連）
法第２２条
個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。
【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】
・　　契約内容が遵守されなかった場合の措置（例えば、安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項も含まれる。）

また、「②　実害は発生しているが、その実害全てを賠償できる」対策が整っているという状況

も、現実的な取引に関して言えば重要な観点であるうえに、見落とされることのある事項である。

しかしながら通常契約可能な会社役員賠償責任保険契約の上限は現状１０億円程度であり、１０億円で全ての損害賠償が可能かどうか判断する必要がある。

（２）：情報の対象者等にとって実害が発生しないこと

現実に漏えいや流出が発生しているのに、情報の対象者にとって実害が発生しない。とは一体どのような意味か。

① 対象となる情報を入手した全ての取得者が高いレベルの道徳観に基き行動する人達だけである場合

② 対象となる情報を入手したが、対象となる当事者やその近親者等が皆急死してしまったような場合

③ 対象となる情報を入手したが、対象となる情報自体に技術的安全管理措置を施してあり、容易に解読できない場合

といった場合が想定される。①に関しては現実問題として発生し得ない場合と言える。一方②は、激甚災害や航空機事故や海難事故等全く可能性が無いとは言い切れない。この場合、損害を被り訴訟を行うべき主体も存在しなくなっていると考えることもできる。③に関しては、その技術的安全管理措置の内容によって、以下のように場合分けができる。

ケース１：漏えいや流出した情報単体で復元可能性はあるものの、現実には時間を要する場合
ケース２：漏えいや流出した情報単体での復元可能性は無く、現実に解読できない場合

ケース１は、ガイドライン等で「望ましい」と記載されている安全管理措置の暗号化を実施している場合が想定できる。この場合、上記①、②以外のケースであることや IT 環境の実状を踏まえると、世界中のあらゆる攻撃者を前提として考える必要がある。例えば現在の標準的な公開鍵暗号技術のパラメータ選択においては、おおよそ 20 年程度以上の耐用年数が想定されていますが、不測の事態により耐用年数が短くなる可能性を完全には否定できません。また、前出の（注１）「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」の（別紙）ガイドライン（事業者編）（案）に関する意見募集結果について。なども踏まえた場合に想定されるケースというのは、

イ） 攻撃者のスキルが低く、事実上解読できない場合
ロ） 攻撃者のスキルが高く、時間を要するが解読できてしまう場合
ハ） 攻撃者に利用した暗号の解法（脆弱性など）が入手された場合
ニ） 攻撃者がすでに利用した暗号の解法（脆弱性など）を保有している場合

といったことが考えられる。

イ）の場合は、「望ましい」とされる安全管理措置を実施したことが良い結果を生じるケースとなる。

ロ）の場合は、「望ましい」とされる安全管理措置を実施していても攻撃者に個人情報等が入手

され悪用されることが考えられる。

ハ）の場合には、攻撃者のスキルが低くてもその暗号の解法（脆弱性など）が情報公開される等してしまえば､解読可能性が一気に高まり個人情報等が入手され悪用される可能性が出てくる。

二）の場合には、攻撃者は容易に解読し犯罪を犯す可能性が高い。

ケース２は、現状市場で入手可能な技術としては、秘密分散技術が想定される。この場合も、CASE１同様に解読可能性を検討してみる。

ホ）　攻撃者のスキルが低く、事実上解読できない場合

ヘ）　攻撃者のスキルが高く、時間を要するが解読できてしまう場合

ト）　攻撃者に利用した暗号の解法が入手された場合

チ）　攻撃者がすでに利用した暗号の解法を保有している場合

となるが､当該技術の場合は単体の割符ファイルでは個人情報や特定個人情報（個人番号含む）を導き出すことはできない。このことは、前述の表 3-1　暗号技術と秘密分散技術でも記載されているように、原理的背景が暗号と異なる為に出てくる特性である。

結論としては、①のような可能性は無いものと考え、更に②のようなケースも日常的に発生するとしないことが、基本となるので情報漏えいや流出が発生すれば情報の対象者等にとって実害が発生するのが常識としなければならない

（３）：法令上の解釈からも対象情報の漏えいや流出とみなされないこと

現実に漏えいや流出が発生しているのに、法令上の解釈からも対象情報の漏えいや流出と看做されない、とはどういう意味か。検討する際の前提条件として、法令はそもそも国民・市民の権利等を保証する為に存在し運用されている。よって法令とは実社会の実情を乖離したものであってはならないという基本がある。

「3.3　個人情報の非個人情報化」で述べたように､「秘密分散技術で作成された「割符ファイル」単体は個人情報の定義項から除外されているが､復元に足る数の「割符ファイル」があれば､個人情報に該当」であり、個人情報（特定個人情報を含む）を秘密分散技術により複数の「割符ファイル」にし､分けて適切に管理することにより､「割符ファイル」の一つが漏えいした場合でも、組織外の実社会から見た際にはそもそも内容の判別できない電子ファイルが出てきたとしか認識出来ず、組織内で適切に管理する残りの割符ファイルと容易に照合することもできないことから、法令上の解釈から組織外に出た割符ファイル単体は、個人情報や特定個人情報と看做されないこととなる。

3.4.3 日常的に安全管理措置を徹底していることの証拠を残す

組織的管理としての人的運用管理の記録とシステム上のログ、その質が問われる。

安全管理措置は、IT システムだけでは完結しないので、どうしても組織・人が絡む部分が発生する。そうすると、その組織に対する法令対処等の評価といったものがいずれ必要になると考えられる。組織としての総合的なリソースの問題や経営層の意識レベル等様々な課題があるが、少

なくとも法令対処を実践する組織として、どのくらいの取り組みを実際に行なっているのかを評価認証しておかないと、事故が発生した際にその組織としての最善の対処を本当にしていたかを示すことができないからである。

① IT システムが対処する部分

② 組織対処部分

こうした対処に関しては、昨年１２月に公開された特定個人情報ガイドライン（事業者編）[3-6]などに比較的詳しく解説されているが、

①では監査ログが相当する。本報告書の「3.2 インシデント対応と証拠保全」でも詳しく述べているように、質の良いログ管理をできるソリューションの導入が必要である。

②に関しては、ISMS 等組織としての情報マネジメントの中で人的・組織的な対処を行うことが良いと考えられる。特に、ISMS 等を取得していない組織等であっても一見面倒に見える組織としての対処を実践すべきである。

3.4.4 不幸にして事故等が発生した際には、迅速に必要な対処を行う

インシデントが発生した場合の対応については、「3.2 インシデント対応と証拠保全」において説明したが、ここでは以下のように対象の情報を委託管理の場合について述べる。

① 完全に委託先に預けていた場合

② 委託先に預けていたのだが、自社内にも残しておいた情報が漏えいした場合

（1）完全に委託先に預けていた場合

前出の「3.4.1 漏えいや流出事故等を起こさない対策を行う（残存リスクを正確には把握する）」でも記述したが、委託を行っている場合には委託元監督責任が発生する。そうした場合、どのような契約を締結しているかでそもそも対処が迅速にできるか疑問になるケースが出てくる。

参考として秘密分散法コンソーシアム調査が想定した事例について、金融庁、経済産業省に等合わせた結果を示す。

想定した事例：
「経済産業分野の事業を営む企業が、個人情報を金融庁管轄の企業に委託管理してもらうとする。（株主名簿の管理委託等は、今後株主の個人番号も対象となると考えられる）」
回答
１、現状ガイドラインは、各省庁の管轄業界の事業者自身が個人情報を管理することに対する指針にはなっているが、今回のように他社から業務委託を受ける際の指針、特に委託元の監督責任を満たすような内容は、明確ではない。（金融庁）
２、現状の御社契約書に不足している、御社又は御社の委託先にて事故が発生した際や事故発生の懸念が生じた際の具体的対処方針に関しては、明文化した方が良い。（経済産業省）
（提供：秘密分散法コンソーシアム調査資料）

受託する側からすれば極力責任範囲が狭く軽い契約が良い。但し主務官庁の開示するガイドラインは遵守するという契約雛形が提示されることになる。すると、上記のように受託先が提示す

る契約書で契約締結すると、そもそもその業界のガイドラインでは受託することを前提としたガイドライン記載が抜けていることがあり、契約書は受託する事業者としてこんなことをする。といった契約条文に終始することになる。

これでは、委託元の委託先監督責任が果たせるかは疑問である。何故ならば、受託業者の側には委託元の監督責任を満たすような契約条項が詳細に記載されていない為、実際に事故が発生した場合や事故が予見できる状態になった場合に、連絡してくるのかさえも不明瞭になっているからである。

参考まで、経済産業省が昨年暮れ（平成２６年１２月）に公開した改正版の個人情報保護法ガイドラインを敢えて再掲抜粋する。

経済産業省ガイドライン抜粋

2-2-3-4.委託先の監督（法第２２条関連）

法第２２条

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

【委託を受けた者に対して必要かつ適切な監督を行っていない場合】

事例１）個人データの安全管理措置の状況を契約締結時及びそれ以後も適宜把握せず外部の事業者に委託した場合で、委託先が個人データを漏えいした場合

事例２）個人データの取扱いに関して定めた安全管理措置の内容を委託先に指示せず、結果、委託先が個人データを漏えいした場合

事例３）再委託の条件に関する指示を委託先に行わず、かつ委託先の個人データの取扱状況の確認を怠り、委託先が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

事例４）契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにもかかわらず、委託先に対して再委託に関する報告を求めるなどの必要な措置を行わなかった結果、委託元の認知しない再委託が行われ、その再委託先が個人データを漏えいした場合

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

・委託元及び委託先の責任の明確化

・委託先において、個人データを取り扱う者（委託先で作業する委託先の従業者以外の者を含む）の氏名又は役職等（なお、委託の実態に応じて、例えば、契約書とは別に、個人データを取り扱う者のリスト等により、個人データを取り扱う者を把握するなど、適切な対応を行うことが望ましい。）

・個人データの安全管理に関する事項

・個人データの漏えい防止、盗用禁止に関する事項

・委託契約範囲外の加工、利用の禁止

・委託契約範囲外の複写、複製の禁止

・委託契約期間

・委託契約終了後の個人データの返還・消去・廃棄に関する事項
・再委託に関する事項
・再委託を行うに当たっての委託元への文書による事前報告又は承認
・個人データの取扱状況に関する委託元への報告の内容及び頻度
・契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）
・契約内容が遵守されなかった場合の措置（例えば、安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項も含まれる。）
・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf

といった内容が記載されている、一方、金融庁ガイドラインを抜粋すると、

金融庁ガイドラインを抜粋
第 21 条 個人情報取扱事業者による苦情の処理（法第 31 条関連）
1 金融分野における個人情報取扱事業者は、法第 31 条に従い、個人情報の取扱いに関する苦情を受けたときは、その内容について調査し、合理的な期間内に、適切かつ迅速に処理するよう努めなければならない。
2 金融分野における個人情報取扱事業者は、苦情処理手順の策定、苦情受付窓口の設置、苦情処理に当たる従業者への十分な教育・研修など、苦情処理を適切かつ迅速に行うために必要な体制の整備に努めなければならない。

第 22 条 漏えい事案等への対応（基本方針関連）
1 金融分野における個人情報取扱事業者は、個人情報の漏えい事案等の事故が発生した場合には、監督当局に直ちに報告することとする。
2 金融分野における個人情報取扱事業者は、個人情報の漏えい事案等の事故が発生した場合には、二次被害の防止、類似事案の発生回避等の観点から、漏えい事案等の事実関係及び再発防止策等を早急に公表することとする。
3 金融分野における個人情報取扱事業者は、個人情報の漏えい事案等の事故が発生した場合には、漏えい事案等の対象となった本人に速やかに漏えい事案等の事実関係等の通知を行うこととする。
http://www.fsa.go.jp/common/law/kj-hogo/

となっている。

（2）委託先に預けていたのだが、自社内にも残しておいた情報が漏えいした場合
この場合は契約当事者間の信頼の上でも、先ずは委託元から委託先に情報漏えいが発生したことを伝えるべきである。
これは、自社の管理している情報が漏えいしたのだから、同じ情報を管理している委託先には特段伝える必要は無いなどと考えてはいけない。実社会に出てしまえば、どちらから漏えいした

のかは判別できないことも想定できるからである。

ここまで、「3.4　防止策及びインシデント対応策」では、経営者をインシデントから守るための方針について述べてきたが、セキュリティとはまさに実社会を反映しており、複雑系・非線形そのものであり、部分だけを見て解を求めようとすると、旧来の線形な解釈が通用しないくらいの前提条件が浮かび上がってきてしまい、結局正しい解を導けなくなる。少し一般的な感覚で表現すれば、硬直した思考では現代の要求しているセキュリティ要件に対処できないのである。少しでも有用な取り組みを積極的に自社に取り入れ､それでも尚残る残存リスクへの対処を怠らず、有用な情報を積極的に収集し、合理的な組織としての対処判断を行い実行しなければならない。そして、利害関係者や周辺、社会に安全・安心を示すことが事業者として肝要なところである。

現時点ですでに個人情報保護法とマイナンバー法（番号法）の一部改正法案が国会提出（第１８９回　通常国会　平成２７年3月１０日　内閣官房情報通信技術（IT）総合戦略室）されているが､法令遵守とはいかに多様な前提条件を想定し､全体を見て判断･対処しなければいけない。そうした事実が垣間見られるマイナンバー法（番号法）の条文の一部と昨年（平成２６年１１月）成立したサイバーセキュリティ基本法の条文は、比較的簡明な条文なので是非一読していただきたい。国、地方公共団体、重要社会基盤事業者の責務や、サイバー関連事業者その他の事業者の責務の他に、国民の努力といった条項もある。「木を見て森を見ず」といった事態にならないよう十分留意しなければならない。

（参考）

ガイドライン記載の「望ましい」とは

「ガイドラインの中で望ましいとして記載された内容に関しては、実際に漏えいや流出等の事故が発生した際に何ら問題の無い対処事例として記載したものではなく、あくまで事業者が自らガイドラインの対象となる法令対処を行う際に実施すべき内容に関し参考となであろう事例を示しただけのものである」であり、現実の事業者等の法令対処の際のリスク管理や訴訟・裁判での判断においては「望ましい」の実施で安心しきってはいけない。

特に、すでに同様の対策で法的な罰則を課せられているような判例が存在する場合は、経営判断上適切な安全管理措置を行っていなかったと解釈されるリスクを認識しなければならない。

―経済産業省個人情報保護法ガイドライン冒頭部の対象記述箇所抜粋部―
～一方、「望ましい」と記載されている規定については、それに従わなかった場合でも、法の規定違反と判断されることはない（３．参照）。しかし、「望ましい」と記載されている規定についても、個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに配慮して適正な取扱いが図られるべきとする法の基本理念（法第３条）を踏まえ、個人情報保護の推進の観点から、できるだけ取り組むことが望まれるものである。もっとも、個人情報の保護に当たって個人情報の有用性に配慮することとしている法の目的（法第１条）の趣旨に照らし、公益上必要な活動や正当な事業活動等までも制限するものではない。
なお、本ガイドライン中に事例として記述した部分は、理解を助けることを目的として、該当する事例及び該当しない事例のそれぞれにつき、典型的な例を示すものであり、すべての事案を網羅することを目的とするものではない。実際には個別事案ごとに検討が必要となる。また、幾つかの業種の例を取り上げたもので、すべての業種の例を網羅しているわけではない。

とあり、他方マイナンバー法（番号法）ガイドライン事業者編では、以下の通り述べている。

―マイナンバー法（番号法）ガイドライン事業者編冒頭部の対象記述箇所抜粋―
～一方、「望ましい」と記述している事項については、これに従わなかったことをもって直ちに法令違反と判断されることはないが、番号法の趣旨を踏まえ、事業者の特性や規模に応じ可能な限り対応することが望まれるものである。

参考文献

［3-1］ 「BYOD (Bring Your Own Device)」http://e-words.jp/w/BYOD.html

［3-2］ 「サンドボックス」
http://e-words.jp/w/E382B5E383B3E38389E3839CE38383E382AFE382B9.html

［3-3］ 「「政府機関の情報セキュリティ対策のための統一基準群 平成 26 年度版(案)」
http://www.nisc.go.jp/active/general/kijun7.html

［3-4］ 「組織における内部不正防止ガイドライン Ver 1.2（IPA、2013.12)」
http://www.ipa.go.jp/security/fy24/reports/insider/

［3-5］ 「EC における情報セキュリティに関する活動報告書 2009」
http://www.jipdec.or.jp/archives/ecom/results/results21.html

［3-6］ 「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（本文及び（別添）特定個人情報に関する安全管理措置） 2014 年 12 月 11 日」
http://www.ppc.go.jp/legal/policy/

［3-7］ 「後を絶たない「監視カメラ誤認逮捕」不鮮明な映像根拠に自白強要」
http://www.j-cast.com/tv/2014/10/16218534.html

［3-8］ 「証拠保全ガイドライン 第 3 版」 https://digitalforensic.jp/2013/09/30/guidelines-3/

［3-9］ 個人情報保護法：個人情報の保護に関する法律（平成 15 年法律第 57 号）

［3-10］ 番号法：行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

［3-11］ データベースのセキュリティ対策 および DBA 意識調査 DBSC による “DBA1000 人に聞きました” データベース・セキュリティ・コンソーシアム (DBSC)
http://www.db-security.org/report/dbsc_dba_ver1.0.pdf#search='DBA1000%E4%BA%BA+%EF%BC%92'

あとがき

2013 年に電子記録応用基盤研究会の中に、電子記録利活用 WG を立ち上げて活動を続けてきた。この間、マイナンバー法（番号法）が成立し、これまで以上に電子記録利活用の情報セキュリティ対策に対する関心が高まりつつある。

しかしながら、電子記録利活用のためのシステム提供者及びその利用者は、どのように情報セキュリティ対策をすればよいのか、手探り状態が続いている。

マイナンバー法（番号法）によれば、特定個人情報を扱うすべての事業者・個人にかかわる問題であり、事業者が情報セキュリティの導入に対して理解しやすい環境を作り出していく必要がある。

今年度は、理解しやすい環境を作り出していく流れの一つとして、中小企業の情報セキュリティ導入責任者に対してどのような情報を提供すべきかの検討を行い、用途ごとの、情報セキュリティ導入事例を示した。

今後、この流れが広がることを期待したい。

メンバリスト

顧問（敬称略、五十音順）

大山　永昭　　東京工業大学
辻　　秀一　　東海大学
米丸　恒治　　神戸大学大学院

執筆・レビュメンバ（敬称略、所属五十音順）

役　割	氏　名	所　属
メンバ	松山　博美	株式会社アコール
	野嶽　俊一	株式会社インテック
	内田　道久	株式会社エイエイエス
	保倉　豊	グローバルフレンドシップ株式会社
	荒木　粧子	株式会社ソリトンシステムズ
	渡邉　英美	株式会社ソリトンシステムズ
	粟野　真太郎	株式会社ソリトンシステムズ
	能勢　健一朗	東芝ソリューション株式会社
事務局	前田　陽二	一般財団法人日本情報経済社会推進協会

上記以外のメンバ（敬称略、所属五十音順）

役　割	氏　名	所　属
メンバ	中根　崇成	シヤチハタ株式会社
	田中　慎一郎	新日鉄住金ソリューションズ株式会社
	富本　正幸	株式会社ソリトンシステムズ
	石原　達也	東芝ソリューション株式会社
	高橋　英治	日本ユニシス株式会社
	三原　真	富士ゼロックス株式会社
有識者	佐藤　均	東海学院大学
	柿崎　淑郎	東京電機大学

電子記録応用基盤に関する調査検討報告書 2014　-電子記録の利活用と情報セキュリティ-

電子記録応用基盤研究会（eRAP）　電子記録利活用ワーキンググループ

平成 27 年 3 月 31 日　第 1 刷発行

発　行：一般財団法人日本情報経済社会推進協会

〒106-0032　東京都港区六本木一丁目 9 番 9 号　六本木ファーストビル内

TEL 03-5860-7557　FAX 03-5573-0561　　http://www.jipdec.or.jp


JIPDEC