個人情報の保護－サイバー法の観点から

あすか協和法律事務所弁護士
明治大学法学部教授
夏　井　高　人

１　はじめに

2005 年 4 月，民間事業者に適用される法律である個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号・以下，「個人情報保護法」という。）が完全施行された。これにより，一定数を超える個人情報を保有する者は，個人情報取扱事業者として個人情報を適法かつ安全に管理・運用するために必要な諸々の法的義務を負うとともに，主務大臣による監督に服し，そして，個人情報取扱事業者が主務大臣による監督に服しない場合には罰則が適用されることになった。

この個人情報保護法は，従来のいわゆる「業法」とは少し異なる。従来「業法」と呼ばれてきた法律は，特定の種類の業種に従事する事業者を適用対象とするものであったのに対し，個人情報保護法は，一定数を超える個人情報を取り扱う者であれば，原則として，業種の別を問わずに適用されるいわば横断的な性格をもった法律と言えるからである。

ところで，個人情報保護法は，電子化された個人情報についても電子化されていない個人情報について適用がある。しかし，電子化された個人情報は，無権限者による改ざん，破壊やその持ち出しが発覚し難いという側面を有すると同時に，それが電子化された情報であるがゆえに電子的な方法によって防御・管理することも可能だという側面も有している。前者の側面は法執行上の困難を痛感させることになり，後者の側面は情報セキュリティの重要性を認識させることになる。そして，その両者の側面において，「適法に行動していることの証跡（evidence）」をいかに確保するかが課題となるのであるが，そうした課題に対応しようとするのがコンピュータ法科学（Computer forensics）の重要な役割の一つである。

本稿では，そのような電子化された個人情報に焦点をあてながら，主としてサイバー法（Cyber law）の観点から問題点や課題などを指摘し，対応策を提示したいと思う。

２　法の効用と限界

個人情報保護法に定める行政監督権限や罰則などは，法の実効性を高めるために有用である。個人情報取扱事業者の義務を定めても，その違反に対するペナルティが存在しなければ実効性を欠くことになるだろうということは容易に想像可能だからだ。

しかしながら，電子化された個人情報を適正に管理・運用するためには，法的な保護・対処だけを考えていたのでは無力である。法は，それ自体としては，電子的な攻撃に対する現実の防御策となるものではなく，あくまでもその違反者に対して事後的に行政処分や罰則を適用するものに過ぎないからだ。換言すると，行政処分や罰則が適用されるのは，常に違反行為や事故が発生した後であることになる。このことは，個人情報の適正な管理・運用がなされなかった場合に適用可能な個人情報保護法以外の法令（刑法や民法など）でも全く同

じである。

とはいえ，法によって定められた義務を適正に履行することにより具体的な防御策が講じられれば，電子化された個人情報をより安全かつ適正に管理・運用できるようになることは疑いがない。

例えば，個人情報の取得は，適正になされなければならないが（17 条），適正な取得という義務を履行するために適正な契約書や約款等を整備し，取得時におけるミスやエラーなどを防止するための技術的防御手段がきちんと確保されるのであれば，法の求める理想が事故発生の前に実現され得ることになる。取得した個人情報の機密性を維持するために，組織の構成や職分の配分を見直し，電子化された個人情報を処理するためのシステムの情報セキュリティを徹底すれば，事故が発生する前に，個人情報取扱事業者が果たすべき安全管理措置義務（20 条）などの履行に寄与することになるだろう。

ただし，個人情報保護法がすべての業種に従事する者について適用されることから，法それ自体に定める義務の要件は一般的・抽象的にしか定められていない。これらの義務の具体的内容は，個々の業種や事業者毎に個別に検討・実施されなければならないのである。そのため，個人情報保護法の定める法的義務を遵守するための指針として，主務大臣などにより各種ガイドラインなどが定められている[1]。

これらのガイドラインは，個々の業種の特殊性などを考慮に入れたものであり，それぞれの該当業種において参考にすべき指針として重要なものだと言うことができる。そもそもガイドラインは任意的なものであり，「個人情報取扱事業者がそれに服すること」が法的に義務付けられているわけではない。しかし，当該主務大臣は自らが策定したガイドラインに従って個人情報保護法上の監督業務を遂行すべき義務を負う（当該主務大臣に対してのみ片面的に法的拘束力がある。）。

したがって，個々の個人情報取扱事業者は，当該主務大臣の監督権限の行使を事前に予測するための基準として該当するガイドラインの存在及びその内容を尊重せざるを得ないという論理構造になっている。ただし，これらのガイドラインは，具体的な業務においてどのようにすべきかの細目まで定めるものではないので，個人情報保護法の完全施行後半年を経た時点においても依然として個々の個人情報取扱事業者の中にある種のとまどいや過剰反応などが見られるらしい[2]。

３　サイバー法の観点からみた課題

このようにして，個人情報保護法の運用は，各主務大臣の定めるガイドラインに沿いながら，業種毎に個別になされることになるのであるが，こと電子化された個人情報に関してはどの業種であっても共通に解決しなければならない法的または技術的な課題がある。それは，まさにインターネットやデータベースといった共通の技術基盤の上で個々の電子化さ

---

[1]「個人情報の保護に関するガイドラインについて」（平成 17 年 6 月 30 日・国民生活局）
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

[2]「最近の個人情報相談事例にみる動向と問題点－法へのいわゆる「過剰反応」を含めて－」（平成 17 年 11 月 7 日・国民生活センター）をあげることができる。
http://www.kokusen.go.jp/news/data/n-20051107_2.html

れた個人情報が処理されているからにほかならない。

検討・解決されなければならない共通の課題は無数に存在するが，サイバー法の観点からすると，問題を更に幾つかの局面に分けて考えることができる。例えば，サイバー空間における企業防衛という局面からの観察も可能であるので，そのような観点から類型化して事例を示してみると，次のようになる（網羅的ではない。）。

Ａ　単純な破壊行為

世間では，しばしば，いわゆる「ハッカー[3]」を含む情報犯罪者は愉快犯であるとか天才的な少年犯罪者であるとか言われやすいし，確かにそのような実例もたくさんある。しかしながら，いわゆる情報犯罪者の中には単なる「破壊」を目的とする者があることを忘れてはならない。彼らの目的は「破壊」のみであるので，電子的な手段と物理的な手段とを選ばない。そのような行為に対して電子的・技術的な方法による防御だけで足りると考えるのは誤りである。[4]

そして，この破壊行為はシステム，データ，通信のいずれに対してもなされ得る。その結果として，システム内の個人情報，個人情報であるデータ，通信中の個人情報などが破壊された場合において，相当と認められ得る程度の防御策が講じられていなければ，個人情報を安全に管理するための措置を講ずる義務を怠ったものとして，個人情報保護法に基づく行政監督に服するほか，民事上も債務不履行または不法行為として損害賠償責任を負うことになろう。

このタイプの破壊行為は，国際的なテロ行為として認識されることもある。

Ｂ　ビジネス犯罪（ライバル企業による妨害行為）

サイバー犯罪は，企業犯罪として実行されることがある。例えば，米国衛星テレビ業界の大物と呼ばれたジェイ・エシュアフニ（38 歳）が数名のハッカーを雇い，2003 年 10 月にライバル会社の Web サイトに DDoS 攻撃（分散サービス拒否攻撃[5]）をしかけたという事例[6]がある。2004 年にロサンゼルスで起訴された後に保釈されたジェイ・エ

---

[3] 「ハッカー（Hacker)」は，もともとは非常に能力の高くコンピュータ技術に精通した人のことを指す用語だったのだが，現時点では情報犯罪者一般を指すものとして世界的に定着してしまっているので，そのような意味でこの言葉を用いることにする。なお，本来の意味での「ハッカー」の概念については，白田秀彰「ハッカー倫理と情報公開・プライバシー」を参照されたい。
http://www.welcom.ne.jp/hideaki/hideaki/hacker.htm

[4] 爆弾や自動発火装置などを用いた攻撃に対しては，システム上のファイアウォールの設定などまるで無意味である。逆に，電子的な攻撃に対しては，警備員の配置や分厚いコンクリート壁の設置などまるで無意味である。

[5] 「サービス拒否（Denial of service)」とは，攻撃相手が提供すべき役務を提供できないような状態にすることを意味する。米国では「サービス拒否」を犯罪として処罰する立法例が多い。

[6] Kevin Poulsen「DoS 攻撃の罪を認めたハッカー、首謀者は逃亡中(上)」

シュアフニは，海外逃亡してしまったと報じられている。このタイプの事件は，電子的な方法以外の方法（デマや虚偽の風説など）によってもしばしば実行されるものであるが，電子的な方法によっても実行されることがあるということが明らかになったと言える。

この事例のような場合，攻撃をしかけられた企業は，まともに企業活動を行うことができなくなるだけではなく，その企業が保有する個人情報を満足に管理できない状態に陥ってしまうことがある。

C　ビジネス犯罪（産業スパイ）

競争相手の保有する新製品の開発計画や発明などの機密情報を盗み出すため，競争相手のスキャンダルを見つけ出すため，他の企業の顧客を奪い取るためその他の違法な目的で，特定の企業のシステムに対して電子的な侵入が実行されることがある。同様の目的は，相手企業の従業員を買収して機密資料を買い取るような行為によっても達成可能である。このような産業スパイ行為は，比較的古典的な犯罪類型に属する。

このようなタイプの行為が電子化された個人情報（顧客情報や閉鎖会社における株主情報など）への無権限アクセス及び無権限複製[7]というかたちで実行されると，当該攻撃を受けた企業などの保有する個人情報が意図せずに第三者に移転してしまうことになる。

そのような個人情報取扱事業者が意図しない個人情報の第三者移転が容易に起き得ないようにするための相当の注意が払われていない場合には，個人情報を安全に管理する措置を講ずべき義務の懈怠があるものと判断されることになろう。

D　ホワイトカラー犯罪（粉飾）

企業経営者は，株価の下落や自分に対する評価の低下を恐れ，粉飾決算をしたいという誘惑にとらわれてしまうことがある。そのようなことを防止するために，株式会社内には監査役が存在しているし，会計監査法人による外部監査も実施されることになっている。しかしながら，監査役がその職責を十分に果たすことができず他の取締役による支援も得られないような場合，あるいは，監査役や公認会計士も共犯者であるような場合には，粉飾を阻止することができない。米国エンロン社の粉飾決算事件はその中でも最も大規模なものであったが，世界的にも著名な会計監査法人であったアーサーアンデーセンは，エンロン社の粉飾に加担していたことが発覚し，そのことが厳しい社会的批判を浴びて消滅することになった[8]。日本国でも類似事例が幾つか発覚している。

---

http://hotwired.goo.ne.jp/news/culture/story/20050912204.html

[7] 欧米ではこのような電子データへの無権限アクセスや電子データの無権限複製行為についても犯罪として処罰する立法例が多い。この点については，拙稿「アメリカ合衆国におけるコンピュータ犯罪立法動向－無権限アクセスを中心とする比較法的検討と日本法への示唆」判例タイムズ 1008 号 106 頁を参照されたい。

[8] スーザン・E. スクワイヤほか著『名門アーサーアンダーセン消滅の軌跡―公正な監査

このような粉飾の過程で，顧客や従業員などの電子化された個人情報が本来の取得目的とは無関係の目的で用いられることがある。これは，個人情報保護法に定める個人情報の目的外使用に該当すると解される[9]。

D　ホワイトカラー犯罪（背任・横領）

企業の資産や財産などを私物化する背任や横領のような行為は，かなり古典的な犯罪類型に属する。財産の存在するところ，それを管理すべき立場の者が権限を濫用して当該財産を私物化したいという欲望を阻止することはかなり困難なことである。そのような欲望を実現化させないためには，相互監視と内部統制[10]の徹底が図られなければならない。

このような背任や横領などの行為は，電子化された個人情報の目的外使用や本人の同意のない第三者提供という形で実行されることがある。例えば，2004 年 1 月に発生した Yahoo BB の顧客情報流出事件などをその例としてあげることができよう。

ただし，現在の刑法上の横領罪は「財物」の横領のみを犯罪行為として規定しており，特定のデータを複製して持ち出す行為のように財物の占有移転を伴わない行為については横領罪が成立しない。また，職務上の義務違反行為としての背任罪についても法解釈論上様々な難点があることは否定できない。このことから，個人情報を複製したりして持ち出す行為について罰則を定めるべきだという意見がある。

なお，このようなタイプの事案では，無権限で取得した顧客情報などの個人情報の買取りを求める恐喝行為やその事実を暴露するという脅迫行為に発展することが少なくない。

E　ネット詐欺

詐欺は，ありとあらゆる手段によって実現されようとする。インターネットを含む情報ネットワークもその手段となり得る。

最も簡単な事例では，ネットオークション，電子掲示板，メーリングリスト，電子メールなどの情報伝達手段を用いて相手を信用させ，金銭や財物を騙し取るということが行われる。このようなタイプの詐欺は，古典的な詐欺行為とほとんど変わることがなく，単に欺罔のための手段としてネットが利用されているだけである。しかし，ネット上で伝達可能な情報が基本的には文字と画像だけに限定されているため，人間のもつ

とリスク管理のプロ集団に何が起こったか元社員らが書いた内幕ストーリー』（シュプリンガーフェアラーク東京）

[9] 一般に，犯罪などの違法な行為を目的として個人情報を取得することそれ自体が許されていないのは当然のこととして，何らかの犯罪を実行するための手段として保有個人データを流用・悪用した場合には，個人情報の本来の取得目的が適法であったとしても，常に保有個人データの目的外使用となると解される。

[10] 2005 年 11 月現在で審議中の会社法施行規則（法務省令）には，企業の内部統制に関する重要な条項が盛り込まれる予定である。

五感の作用すべてを駆使して詐欺であるかどうかを見破ることが困難であるという特徴がある。これらの行為については，刑法の定める通常の詐欺罪が成立することが多い[11]。

また，ネット詐欺は，スパイウエア（Spyware）やボット（bot）などのいわゆる「悪意あるソフトウェア（Malicious Software）」[12]を利用して実行される場合がある。日本国においても，スパイウエアを用いた詐欺事犯で 2005 年 11 月に容疑者が逮捕された[13]。これらの行為については，通常の詐欺罪が成立する場合と電子計算機使用詐欺罪が成立する場合とがある。

そして，ほぼすべてのタイプのネット詐欺事犯において，被害者となる者の個人情報（氏名，住所，電話番号，銀行口座の所在及び口座番号，ID，パスワードなど）が加害者の手に渡ることになり，更に加害者から犯罪者グループなどの手に渡ることも珍しくない。したがって，ネット詐欺事犯を単に単発的な加害行為としてのみ理解することは間違いであり，サイバー空間における個人情報の保護という観点からは重大な脅威の一つとして理解されるべきである。

F　フィッシング（Phishing）

フィッシングは，本物の Web サイトとそっくりの偽物のサイトを構築し，そのサイトを本物のサイトと誤認してアクセスする被害者から個人情報など様々な情報を入手するために用いられる違法な技術の一つである。

フィッシングは，詐欺行為の手段として利用されることが多いとされ，そのような場合を「フィッシング詐欺（Phishing fraud）[14]」と呼ぶのが通例である。しかし，その実態には依然として不明な部分がある。情報セキュリティ専門家の推測によると，いく

---

11 詐欺目的でネットオークションに出品しているような情報を掲示するといった事案の場合，最初から商品を出品する意思がなく代金を詐取することが目的である以上，そのような行為は民法上公序良俗違反として無効である。そのような行為について特商法のようないわゆる業法を適用して適正な業務を行うことを期待するのは無理なだけでなく，違法・無効な行為を形式的には適法行為として扱うことにもなり著しく不適切である。罪数論としては，このような詐欺行為については，特商法などのいわゆる業法違反の罪が成立することはなく，専ら刑法に定める詐欺罪のみが成立すると解すべきである。

12 ここでいう「悪意」とは民法上の概念である「悪意」ではなく「害意」のことを意味する。英語の「Malicious」に日本語の「悪意ある」をあてることは，通常の法律家の視点からすると不適切であると考えられないが，訳語として事実上既に定着してしまっているので，本稿でもやむを得ずこの語を用いることにする。今後あるべき姿としては，情報セキュリティ関連の書籍の翻訳の際には，サイバー法と日本国法の理論と実務すべてに通暁した法律家の監修を経ることが望ましい。

13 CNET Japan 2005 年 11 月 11 日「警視庁、スパイウエア初摘発　ネット銀から 1140 万円詐取」
http://japan.cnet.com/news/sec/story/0,2000050480,20090677,00.htm

14 米国における fraud には日本国における窃盗罪に該当する行為も含まれることがあるので，正確には「フィッシング詐欺」という訳語は適切ではないが，この語も事実上既に定着していしまっているので，本稿でもやむを得ずこの語を用いることにする。

つかのパターンがあり得るということである。例えば，財産獲得目的で実行される場合にはフィッシングによって得た個人情報（ID，パスワード，クレジットカード番号など）をブローカーに売り渡す目的であることがあるとされている。また，他のコンピュータシステムに無権限でアクセスするための各種アクセス管理用情報を違法に入手する目的でフィッシングが実行される場合もあるということである。更に，騙されてアクセスした者の保有するコンピュータに即時に無権限でアクセスしたりスパイウエアなどを送信したりするための特殊な仕掛けがしてある場合などもあるようで，多様である。

フィッシングにより直接に財産権の侵害が発生する場合も重大な危害であると言える。しかし，それ以上に，フィッシング・サイトの存在は，適正なネットビジネスのためのサイトに対する信用を低下させたり，ネット上での重要な情報のやりとりに対する信頼性を低下させたりすることが十分に予想される。そして，その結果として，ネットビジネス（電子商取引）全体に対して大きな悪影響を及ぼすことになるのではないかと懸念されている。

４　分析の視点

以上に述べてきたように，サイバー法の観点の中でもサイバー空間における企業防衛という局面のみから観察してみても，サイバー犯罪がネットを利用した経済活動に大きな脅威を与えるものであり，しかも，その過程で顧客情報などの個人情報が違法に加害者などの手に渡ってしまうことが多いため，個人情報保護法上の問題も発生することになる。

これらの問題は，個々の個人情報取扱事業者の業態などとはあまり関係がなく，専らネットワークシステムを用いてビジネス運営をすることに起因するものである。

その意味で，これらの脅威は，業種の相違を超えた横断的なものとして理解されるべきである。そして，その脅威の分析もまた，横断的・共通のものとしてなされる必要があろう。

そこで，試みに脅威のタイプに分けて分析してみると，次のようになると考えられる（網羅的ではない。）。

①　個人情報取扱事業者のシステム管理上の懈怠

個人情報取扱事業者の運営するシステム内に記録・保存された個人情報を含むデータを安全に管理する措置を構ずるべき義務の懈怠として理解可能である。

②　個人情報の本人であるユーザの側での不注意

個人情報に関する権利や法的利益を守るためには，まず本人が自分でなすべき保護手段を講ずるのが第一である。しかし，自分の個人情報を安易に他人に提供してしまうことがしばしばある。

③　通信への無権限による介入

個人情報を含むデータは，通信中に無権限で介入（intercept）されることがある。これは，ディスクなどに記録されているデータへの無権限アクセスと同様の意味で伝送中のデータに対する無権限アクセスとして理解される。

④　トリック

スパイウエア，ボット，フィッシングなどは，技術的なトリックの一種である。コンピュータシステムが正常に動作しており適切に処理されているように見せかけることをその本質的要素としてもっている。

これらの諸要素に対応する法律上及び情報セキュリティ上の要求事項は，次のとおりであると考えられる（網羅的ではない。）。

①　個人情報取扱事業者のシステム管理

法的な要求事項としては，個人情報保護法の定める個人情報取扱事業者としての義務を履行することを意味し，義務違反があった場合には，主務大臣による行政監督権限の行使があり，主務大臣の命令に対する違反があれば罰則の適用がある。
また，民法や商法（会社法）に定める「善良な管理者の注意義務」等としてもそれを履行することに尽きる。義務違反があった場合には，債務不履行責任または不法行為責任として民事上の損害賠償責任が発生する。
具体的な内容については既に述べたものを含め，標準的な情報セキュリティの基準[15]を満たすものであることをもって「なされるべき相当の注意」を尽くしたと評価されることになろう[16]。

②　個人情報の本人であるユーザ

個人情報の本人に対して「自己責任」として自己の個人情報を自ら防御すべきことを命ずる法律は存在しない。現時点では一般常識の範囲内にとどまる。ただし，現実に事故が発生した場合には，本人が「うかつに行動したこと」が過失相殺のための事情

---

15 財団法人日本情報処理開発協会 ISMS 制度推進室「ISMS 認証基準(Ver.2.0)について」（2003 年 4 月 21 日）
http://www.isms.jipdec.jp/v2/v2.html

16 個人情報保護や情報セキュリティなどに関連する規格や基準に限定されることではないが，「第三者認証を受けることが重要である」と誤解されることがしばしばあるし，そのように宣伝しているコンサルタント業者なども多数存在する。しかし，第三者認証制度は，ある基準を満たす実務対応の達成度を第三者機関が客観的に評価するために存在しているのであって，個人情報などの保護のための実務（プラクティス）それ自体ではない。したがって，第三者認証を受けることを第一の目的とするのは適切ではなく，基準を満たすような適正な実務環境の確立・実現をめざすべきである。

として考慮されることがあり得る。
情報セキュリティのための要求事項としても基本的には存在せず，また，一般市民に対してそれを要求することは非現実的なことである。

③　通信への無権限による介入

電気通信事業者に対しては電気通信事業法に定める法的義務と罰則が適用され，電気通信事業者以外で有線電気通信を行う者については有線電気通信法の定める法的義務と罰則が，無線通信を行う者については電波法の定める法的義務と罰則がそれぞれ適用される。また，当該通信を直接に取り扱う者及び通信当事者以外の第三者による通信への無権限介入については，「通信の秘密」を侵害するものとして罰則が適用されることがある[17]。
通信を媒介する者についても一般的な情報セキュリティの基準や規格が適用される。なお，電気通信事業者については，2005 年 11 月現在，ISMS の特別のバージョンの策定作業が進められている[18]。

④　トリック

トリックは，専ら犯罪その他の違法行為を実行しようとする者によって設置・実行されるものである。彼らに対して個人情報保護法などの遵守を求めることは最初から期待できないだけでなく，彼らの行動は個人情報の侵害を直接の目的の中に含んでいるため理論的にも自己矛盾であることになる。一般的には，刑法その他の法令に定める犯罪を処罰するための法令が直接に適用される。
　トリックを防御するためには，①の事業者，②のユーザ及び③の通信媒介者がそれぞれの立場で導入・実施可能な情報セキュリティの基準や規格によることになる。犯罪者その他の違法行為を行動目的とする者に対して情報セキュリティの要求事項の実現を求めることは，理論的にも自己矛盾となる。

５　課題に対する今後の対応

---

[17] RFID チップを内蔵した無線タグをビジネスに利用する場合，そのタグとリーダーとの間の無線通信に対する無権限介入も考えられる。この場合において通信事業者等が介在しないときは，当該無線タグを利用する個人情報取扱事業者など自身の義務が最前面に現れることになる。なお，そのような無線通信が電気通信事業者によって媒介される場合であっても，当該無線タグ及びリーダーの安全を確保する措置を構ずるべき当該個人情報取扱事業者の法的義務が減免されるわけではない。なお，RFID タグとプライバシー問題に関しては，Simson Garfinkle, Beth Rosenberg ed, RFID: Applications, Security, And Privacy, Addison-Wesley Pub，拙稿「トレーサビリティシステムと個人情報保護上の問題点」情報ネットワーク・ローレビュー第 3 巻 113 頁を参照されたい。
[18] 中尾康二「ITU-TSG１７（データネットワークおよびテレコミュニケーションソフトウェア）における ISMS-T 標準化動向と今後」
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/pdf/050120_1_s1.pdf

ここまで述べたことにより，マクロ的に観察した場合，個人情報保護のための諸施策の中で最も大きな穴（セキュリティホール）となっているのは，実は，「個人情報の本人」であることが明らかとなった。そして，「この穴を少しでも小さくするためにはどのようにすべきか」が最も重要な課題の一つであることになる。

また，同様の問題は，組織における個人情報の保護や情報セキュリティの実現においても別のかたちをとって出現することがある。それは，組織の構成員（企業の従業員など）が生きた人間として記憶してしまっている他人の個人情報や私物ＰＣに記録してしまっている他人の個人情報の管理の問題である。このような個人情報は，法的には当該組織の管理の問題となるはずなのであるが，現実を直視すれば，個々具体的な構成員（企業の従業員など）の知識，意識，意欲，能力，技量などによって圧倒的に支配されてしまう。同様の問題は，企業からデータ処理を委託された受託者の従業員などについても発生する。

その意味において，個人情報の本人に関する課題と組織構成員に関する課題等は，共通の要素をもった問題であり，情報セキュリティの分野において一般に「人間系」と呼ばれている脅威の問題とほぼ同一の問題であると理解することが可能である。人間系の問題に対する対応としては，システム内に何らかの仕組みを導入するだけでは決して適切に対処し切ることができないという共通の問題が発生し得る。

この問題に対する対応として，現在，様々のことが提案され実施されてきている。例えば，ＰＣ内にディスクを持たず一定の手順の下でホストコンピュータと通信している時にのみ顧客データ等にアクセスすることのできる「シンクライアント（thin client）」と呼ばれるタイプのコンピュータシステムの導入，特定の一個のＰＣの中には，個人情報を含むデータの中の数学的に分解され暗号化された一部分だけが記録され，万が一にもそのＰＣが盗まれたとしてもその暗号化されたデータの解析が非常に困難な「秘密分散法（Secret Sharing Scheme）[19]」の応用導入などがその例である。

しかし，これら既に導入されている手法それぞれには長所と短所とがある。また，企業の命令によってそれらの手法を導入することを強制できない一般市民のシステムやＰＣについては，全く異なるアプローチが必要となる。

そこで検討されるべきものは，プロバイダなどによるネットワーク監視の一部として脅威の発見と抑制を実現するという手法の導入である。この手法を実効的なものとして導入・運用するためには，必然的に，事前の監視（monitor）と不審なパケットなどの追跡（trace）という技術的要素を実現することも必要となる。

ところが，そのような事前の監視と追跡については，様々な法的問題が伴うことにもなる。例えば，そのような監視が同意に基づく場合には比較的問題も少ないが，同意に基づかないで監視をする場合にはユーザなどのプライバシーや個人情報の保護の観点から見て法的問題が発生する余地がある。また，追跡の場合には，原則として，事前の同意ということがあ

---

[19] What are some secret sharing schemes?
http://www.rsasecurity.com/rsalabs/node.asp?id=2259
山本博資ほか「一般アクセス構造に対する秘密分散法の情報理論的性能解析と応用に関する研究」
http://research.nii.ac.jp/kaken-johogaku/reports/H15_A04/A04-01.pdf

り得ない。

そのような事前の監視や追跡が個人情報取扱事業者によって実行される場合において，個人情報保護法に「本人の同意を得ることができない場合」に同法の所定法条を適用しないという例外規定が幾つか存在するので，当該個人情報取扱事業者によって本人の同意を得ることが社会通念上不可能である場合には，むしろ同法に定める例外規定の適用の可否の問題として理解され得るし検討の対象ともなり得るだろう。

これに対し，本人の同意を得ることができる場合でも，それを得ることにより事前の監視や追跡という業務に支障が生じ得る場合が一番問題となる。この文脈では，脅威や事故などが発生しつつある時点などでは正当防衛や緊急避難として違法性阻却を考えることができるが，そうでない場合には「正当業務行為（正当行為）」として違法性阻却を考えることができるかどうかが今後の非常に重要な法的検討課題の一つになることは疑いない。そしてまた，その場合における適法化要件のひとつとして，手段の「相当性」の基準が検討されることになるであろう。