VI 情報漏えい時の「企業損害と責任」本論

弁護士
元東京地方裁判所非常勤裁判官
システム監査技術者
公認システム監査人
総務省行政管理局技術顧問
藤谷 護人（ふじたに もりひと）

1 漏えい事件は止まらず、件数が巨大化ーリスク見直しが必要

流出件数	発覚年月	原　因
35,040,000（48,580,000人）	2014年 7月	再々委託先SEが持出し
22,000,000	2013年 5月	外部不正アクセス
7,700,000	2011年 4月	外部不正アクセス
8,640,000	2007年 3月	委託先社員持ち出し
5,380,000	2006年12月	不明
4,000,000	2006年 9月	協力会社社員持ち出し
3,996,789	2006年 6月	不明、但し内部濃厚
1,760,000	2005年 4月	CD-ROM紛失
1,280,000	2005年 4月	CD-ROM紛失
2,200,000	2004年 4月	システム委託先から漏洩
1,400,000	2004年 3月	元社員持ち出し
6,60,0000	2004年 2月	外部不正アクセス
1,160,000	2004年 2月	内部犯行

表1　我が国で100万件を超える個人情報漏えい事件

我が国で初めて100万件を超える個人情報漏えい事件が発覚したのは、2004年2月のことである。さらに同じ月に、最大660万件の漏えい事件が起こり、翌2005年4月の個人情報保護法の完全施行を控えて大いに世間の耳目を集めた。そして10年後の2013年5月には一挙に2000万件を超え、2014年7月にはさらにそれを上回る漏えい事件が発覚した。

この10年間、個人情報保護法が施行され、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」（法第20条）義務が与えられ、企業も手を拱いていた訳ではないと思われる。

しかし、だとすれば何故漏えい事件が止まらないのか、何か根本的な原因の見落としがあるのではないか、見直しが必要である。

さらに、漏えい事件が発覚した後の企業の対応の失敗も10年前と変らず繰り返されている。何故なの

か。経営者が漏えい発表時に漏えいによる真の被害者は誰なのかについて不適切な発言をしてしまうことがあるが、損害と責任については、トップマネジメントレベルで根本的な意識変革が必要である。

2 「企業損害と責任」に関する問題点について

漏えい事件における企業損害と責任に関する主たる問題点は次のように整理できる。

- ●発覚直後のお詫び会見での対応ミスによる社会的信用の低下がなぜ繰返されるのか
- ●全顧客に対するお詫び金支出による損害の企業経営に及ぼす甚大な影響
- ●全顧客からの損害賠償(慰謝料)請求による賠償額の企業経営に及ぼす意外な小ささ
- ●漏えいによる社会的信用の低下による逸失利益はかなり大きい
- ●技術的セキュリティ対策は十分であっても、事故が起こるのはなぜか、なぜ漏えい事故が無くならないのか

以下、これらの問題点について、考察する。

3 発覚直後のお詫び会見での対応ミスによる社会的信用の低下がなぜ繰返されるのか

2004年2月の451万件[1)]の漏えい事件についてトップが記者会見したときに、「被害者は当社である」と公言して世間の批判を浴び、結局は一人500円の商品券を配布することとなってしまった。また、2014年7月の漏えい事件では、トップが(顧客に商品券を配布してお詫びする予定はないのかとの質問に対して)「漏えいした個人情報の機密度が低いのでそのような必要はない」と公言したもののマスコミからの追及もあり、結局7月末には「お詫びのために200億円用意した」と記者会見する事態となった。

なぜ個人情報保護法施行から10年を経過しても、対応ミスによる社会的信用の低下が繰り返されるのか。その根本的原因は、企業トップに「被害者は企業である」という意識が強く、「漏えい事件の第一の被害者は顧客であり、顧客との関係では企業は加害者である」という意識が欠落していることである。

また、「個人情報のオーナーは個人本人であり、企業は本人から預かっているのである」という個人情報保護法の革命的な根本理念が未だに理解されていないことが大きな要因であると思われる。

個人情報漏えいについては、「組織のリスクマネジメント」ばかりでなく、「トップのリスクマネジメント」を強化することが抜本的な課題である。

4 全顧客に対するお詫び金支出による損害の企業経営に及ぼす甚大な影響

2004年に漏えい事件が発覚した企業では、金券33億円分(500円×660万件)とお詫び文と金券の郵送費6.6億円(100円×660万件)の合計約40億円を出費した。また、2014年の漏えい事故では、漏えい件数は、2014年9月現在で3,504万件(4,858万人)と公表されている。この数字を前提に計算すると、金券242億9,000万円分(500円×4,858万人)とお詫び文と金券の郵送費48億5,800万円(100円×4,858万人)の合計約292億円となる。これらは言うまでもなく漏えい件数が多いほど増加するものであり、お詫び金の

1) 記者会見当時の件数。後日、660万件に訂正された。

支出は企業経営に甚大な影響を及ぼす可能性がある。

なお、過去の漏えい事件においては、数百億円のお詫び金を見積もり特別損失として計上した例もあるが、漏えいした件数によっては企業が見積もった範囲を大きく超えた損失に繋がり、見込んでいた純利益が消失してしまうおそれもある。あくまで他の経営努力がなければという仮定の話ではあるが、お詫び金だけで、数十億円～数百億円といった黒字決算が一気に赤字決算に転落するリスクも発生する可能性があることを肝に銘じる必要がある。

5 全顧客からの損害賠償(慰謝料)請求による賠償金の企業経営に及ぼす意外な小ささ

最高裁判決2002年7月11日では、自治体の住民基本台帳の情報の漏えいに対して1件1万円、また別の判決で企業における顧客の住所氏名およびメールアドレスの漏えいに対しては1件5,500円の慰謝料を認定している事例がある。1件あたりの慰謝料に、漏えい件数を乗じたものが「理論的損害額」となる。信用情報等の機微な情報を大量に漏えいさせてしまった場合や、漏えいした情報が回収不能の場合、1件あたりの慰謝料はより高く認定されると考えられる。仮に、顧客の住所氏名およびメールアドレスを1,000万件漏えいした場合、理論的損害額は最高裁判例を基に550億円(5,500円×1,000万件)と算出できる。これは、年間の純利益が50億円の企業の場合、11年間は純利益が出ないという超巨大リスクである。

しかし、「現実的損害額」は、理論的損害額に「訴訟提起率(訴訟提起者の数を被害者全体の数で除した数字)」を乗じることになる。あくまで報道ベースではあるが、前述の住民基本台帳の情報漏えい事件では21万人の被害者のうち訴訟を提起したのは3人であり、訴訟提起率は0.00143%、また、前述の企業の住所氏名およびメールアドレスの漏えい事件では660万人のうち訴訟を提起したのは5人であり、訴訟提起率は0.0000757%となる。つまり、「理論的損害額」である550億円に「訴訟提起率」を乗じると、「現実的損害額」は41,635円～786,500円に過ぎない。

これでは、企業にとって取るに足らないリスクでしかない。法律的に考えれば、法律的に保護されるべき被害者の救済を求める権利が実現されないことの反射的利益として企業が現実的リスクを免れている。これは不正義であるし、結局は、企業の正義適合経営を妨げているのではないのか、という疑念を払拭できない。「我が国はアメリカのような訴訟社会ではないこと」、「アメリカのように多額の懲罰的損害賠償が認められないこと」、「我が国の集団訴訟は損害賠償請求の場面には適用できないこと」、「訴訟のためには弁護士費用が必要であるが、一人当たり1万円程度の損害賠償額では弁護士費用が捻出できないこと(前述の判例では、住民基本台帳の情報漏えい事件で5,000円、顧客情報漏えい事件で1,000円の弁護士費用が認められてはいるが)」、「被害者が全国に分散していて弁護士が対応し難いこと」などが隘路となっている。

しかし、前述した1,000万件の情報漏えいを起こした企業が、550億円の法律的責任を微々たる現実的損害額のみで済まそうとする、それで社会的責任を果たしたのだと胸を張るとしたら、それは褒められたものではない。この例においては、少なくともトップマネジメントは「理論的損害額」を意識し、550億円の法的に償うべき責任を負ってしまったという心理的な「負い目」はきっちりと自覚して経営に当たってほしいものである。

6 漏えいによる社会的信用の低下による逸失利益はどれくらいか

「お詫び金」や「慰謝料」の金額については、算定するための考え方や実例も揃っている。しかし、顧客情報を漏えいしてしまった企業において、おそらく、実際の経営上のダメージは金額的にそれらよりも断然大きいと思われるのに、具体的な金額を算定することが難しいのが、「漏えいによって、社会的信用が低下し、それによって、同業他社との競争上、不利な評価を受けることになり、新たな受注案件を失注したり、既存案件の解約を受けた」という「逸失利益」である。

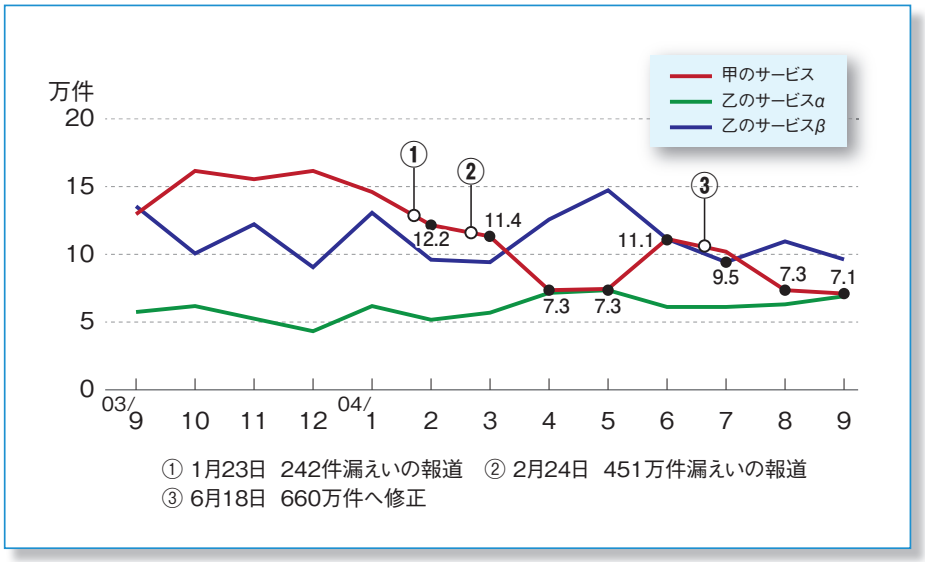

図1　甲対乙の契約対前月比増加数の推移比較と漏えい事件の影響

逸失利益の金額を算定する元になる数字を入手した。それが図1「甲対乙の契約対前月比増加数の推移比較と漏えい事件の影響」というグラフである。これは2003年9月～2004年9月までの13か月にわたり、同業である甲のサービスと乙のサービスの毎月の契約者数の増加数をドットし、それを直線で結んだものの折れ線グラフに、①2004年1月23日、②2004年2月24日、そして③2004年6月18日の報道内容をプロットしたものである。

2004年1月における甲のサービスの契約増加数は15万件であったが、2月には2.8万件、3月には3.6万件、4月には7.7万件、5月7.9万件、6月3.9万件、7月3.9万件、8月7.7万件、9月7.9万件減少したことが見て取れる。この8か月間の減少数の合計は45万4千件、年間の減少数に引き延ばすと68万1千件である。1件当たりの月額料金を5,000円だとすると年間料金は6万円、減少契約数を乗じるとすると409億円。これが、甲が逸失した年間売上額ということができる。甲全体での逸失利益は、この3倍額と見て1,227億円と算定できる。2003年度の甲の売上額は5,173億円である。対前年度売上で23.7%も逸失利益が発生したことになる。

このように、社会的信用の低下によって既存の顧客が離れていくことはもちろん、当該企業が新規の営業活動を自粛した例もあり、漏えい事件は将来にわたって算定できないレベルの影響を及ぼすものと考えられる。

7 技術的セキュリティ対策は十分であっても、漏えい事故が起こるのはなぜか、なぜ漏えい事故が無くならないのか

2005年個人情報保護法に「安全管理措置義務」(20条)が規定され、企業も漏えい防止策に取り組んできているのに、漏えい事故が止まらないのはなぜか。過去の漏えい事故では、個人情報を預かる企業や、その委託先企業、さらに再委託先企業等における情報セキュリティ対策は十分だったと報道されたことが多いが、事故が起こったのはなぜか。

これまでの情報セキュリティにおいて、重大で客観的かつ構造的なリスクが見落とされていた、と言わざるを得ない。それは①「委託による内部統制力の喪失」によるリスク(図2　アウトソーシング・セキュリティ構造式)であり、②「労働力形態による内部統制力喪失」によるリスク(図3　労働力形態による内部統制力喪失関係)であり、③「内部的脅威による客観的防止策の喪失」によるリスク(図4　「リスク」定義図)である。

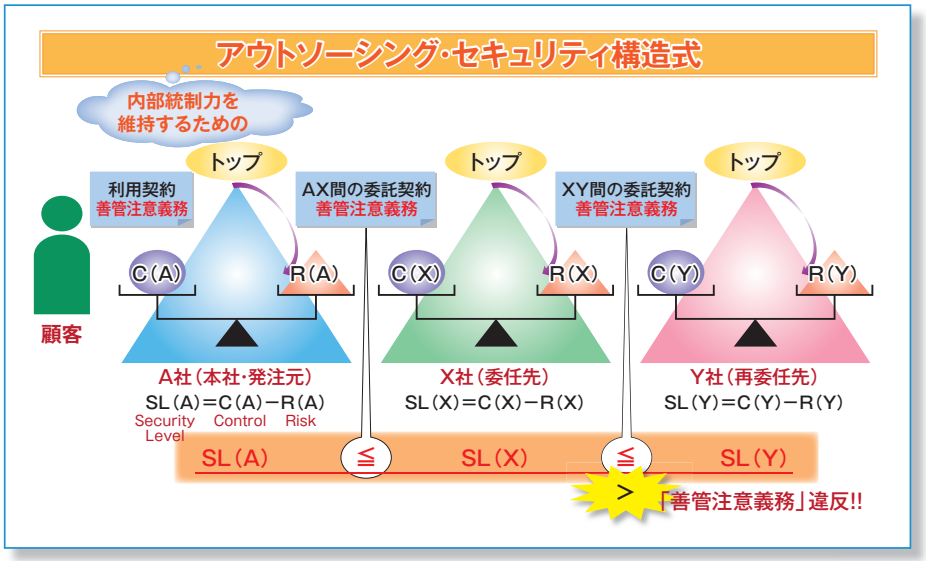

図2　アウトソーシング・セキュリティ構造式

(1)「外部委託による内部統制力の喪失」によるリスク

まず、図2の左端の三角は、顧客から個人情報を預かったA社だとする。顧客とA社との間には利用契約があり、その利用契約上の義務としてA社は顧客から預かった個人情報を「善良なる管理者としての注意義務(善管注意義務)」によって管理する債務を負っている。そのA社が当該個人情報を自社内で管理する場合には、「A社のセキュリティのレベル」は、A社における上皿天秤の向かって左側の上皿に乗っている「A社におけるコントロール(管理策)の大きさ」から、A社における上皿天秤の向かって右側の上皿に乗っている「A社におけるリスクの大きさ」を引いたものであると表わすことができる(「SL(A)=C(A)- R(A)」)。そして、当該個人情報を漏えいさせないためには、C(A)≧ R(A)の状態となるような内部統制力を確保することが必要である。

このA社が当該個人情報の管理をX社との委託契約によって、X社に委託した場合、A社は顧客の個人情報を管理するための自らの「内部統制力を喪失」することになる。このままでは、A社は顧客に対する善管注意義務を果たすことが出来ないので、A社はX社との間の委託契約の内容として、内部統制力を利かせていた時の自社のセキュリティのレベルSL(A)と委託先X社のセキュリティのレベルSL(X)が、SL(A)≦SL(X)であることをX社の善管注意義務として約定しなければならない。もし、A社が、委託先X社がY社へ再委託することを認める場合には、SL(A)≦SL(X)≦SL(Y)であることをY社の善管注意義務として約定しなければならない。確かに契約書の文言に、

「再委託する場合には、X社の善管注意義務と同等の善管注意義務をY社に負わせるものとする」という規定は見かける。

しかし、問題は、①契約の文言通りにSL(A)≦SL(X)≦SL(Y)のセキュリティのレベルが確保されているのかどうかについて、委託・再委託の我が国の現実(より低価格化=セキュリティレベルの低下)に照らして、戯言化している、あるいは漏えいリスクが顕現しないだけで、状態としては、既に、善管注意義務違反状態にあることに目を瞑っている。赤信号が点滅しているのに皆で渡れば怖くないと衆愚化して対応策を取ってこなかった。そんなことに目くじらを立てていたら、我が国のこの業界における「系列」を否定することであり、ドロップアウトするしかないぞとの居直りの声すら聞こえる。

さらに、②外部委託に出すということは、それが守られるための担保は、債務不履行解除と損害賠償しか存在していない。これだけで、内部統制力と同等のリスクコントロールが存在すると言えるだろうか。不十分である。自治体等においては外部委託の場合には、地方公務員としての刑罰的コントロールを個人情報保護条例の中で、委託先社員にも刑罰を規定して、コントロールを確保しようとする方法も行われている。民間企業においても、内部統制力が直接及ぶ場合には、懲戒解雇までの心理的抑止力があるが、外部委託契約には当然ながらそのコントロールは及ばない。債務不履行解除と損害賠償にプラスアルファで何らかの抑制力を盛り込むことが不可欠である。今までは、この点の認識が甘すぎ、対策が緩すぎたと言わなければならない。

(2)「労働力形態による内部統制力の喪失関係」によるリスク

現在は、企業における労働力の調達は複雑化しており、一つの職場に、自社常用社員、自社契約社員、自社パート/アルバイト社員、派遣社員、委託先社員、再委託先社員など様々な労働力形態が混在している。この職場において、顧客の個人情報を取り扱う場合、リスクコントロールの「抑制策」の観点から、各社員に対する心理的抑制力は同じなのか、漏えい防止のための必要なレベルの心理的抑制力が確保できているのか、という分析を行ったのが、図3である。

		自社常用	自社契約	自社パ/ア	派　遣	委　託	再委託
帰属・服従意識		○	△	△	×	×	×
兼・競業禁止権		○	○	×	×	×	×
懲戒解雇権		○	○	○	×	×	×
懲戒権		○	○	○	×	×	×
研修命令権		○	○	○	×	×	×
規範遵守要求権		○	○	○	○	×	×
守秘要求権		○	○	○	○	○	△
誓約書徴求権		○	○	○	△	×	×
業務指揮命令権		○	○	○	○	×	×
監査権		○	○	○	×	×	×
改善指導命令権		○	○	○	×	×	×
損害賠償請求権	契約	○	○	○	×	○	×
	不法行為	○	○	○	○	○	○

図3 労働力形態による内部統制力喪失関係

表頭には、各労働力形態を並べ、表側には、自社常用社員に対して、当該企業の社長が行使しうる内部統制力(心理的抑止力)を列挙し、各労働力形態ごとに、各心理的抑止力が有る場合には○印を、無い場合には×印を、中間の場合には△印を付けていった。

するとどうだろう。左上隅から右下隅への対角線の右上部分に×印が集中的に分布し、対角線の左下部分に○印が集中的に分布した。さらに、派遣社員・委託先社員・再委託先社員のグループは、他の労働

力形態とは明確に一線を画しており、これらのグループに対する内部統制力がほとんど喪失されており、心理的抑止力を利かせる人的基盤が存在しないことが明白である。さらに、派遣社員＜委託＜再委託と喪失の程度が拡大している。

このことから、これらの労働力形態の社員にも、他の社員と同様に個人情報を取り扱わせようとする場合には、この内部統制力の喪失状態を十分にリカバーするだけのリスクコントロール策を実施できていなければ認められないと判断しなければならない。

(3)「内部的脅威による客観的防止策の喪失」によるリスク～外部委託による脅威の内部化のリスクの大きさ

従前からの「リスク」は次のように定義されてきた。組織が用意している防壁(管理策)の穴や弱いところ（脆弱性）を外部からの「脅威」が突破して、組織の内部に侵入し、組織内にある「情報資産」を侵害し、「損害」を発生させるような状況のことを「リスク」という。（図4）

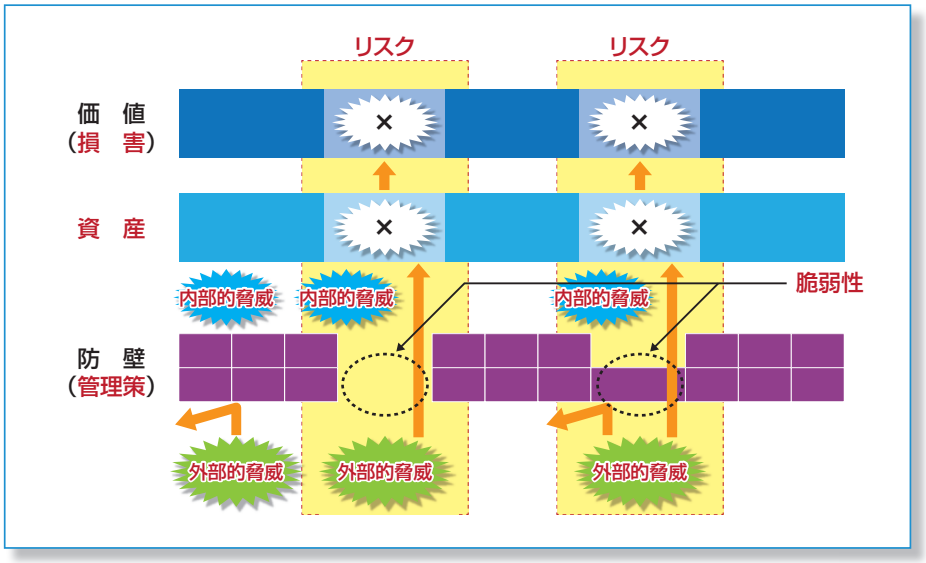

図4　「リスク」定義図

そして、このリスクをコントロールする方策は大きく分けて「防止策」と「抑制策」に区別される。「防止策」は、客観的な方法を用いて、脆弱性(脅威が外部から侵入しようとするチャンス)を可能な限り狭めることであり、「抑制策」は、まず「防止策」を実施した後において、残されたリスクに対して、主観的に心理的に抑圧を加えて、規範適合行動を取らせる方法である。リスクコントロールにおいて、「防止策」と「抑制策」は車の両輪であるが、まず「防止策」を十分実施して、残されたリスクに「抑制策」を実施することが効果的である。

ところが、外部委託し、委託先社員に個人情報に対するアクセス権限を付与してしまった場合、当該委託先社員に対しては、「防止策」は無力である。委託先社員は「管理策」の内側に居るからである。委託先社員に対するリスクコントロールは、車の両輪であり、まず優先的に実施すべき「防止策」を最初から有していない。主観的な「抑制策」だけで、リスクを片輪走行でコントロールしなければならない、という例外的で異常で苦しい局面に立たされている。

同様に、客観的「防止策」が効かないために主観的「抑制策」のみによらなければならないセキュリティの場面として、社員が会社のシステム機器によらずに、自前のスマホとSNSを利用して情報漏えいをする場合があるが、この場合は社員が対象であるから、雇用契約上の就業規則などの義務を拡充強化することで対処することを提案したことがある。しかし、外部委託先社員に対しては、この方法も適用できない。俄

かには、十分なコントロールの方法を提示できないが、労働法学者が幾ら異を唱えようとも、「直接自筆の誓約書を不法行為による損害賠償義務を受忍する文言も入れて提出してもらうこと」、「外部委託先に対して、選定条件を厳しくし、万が一の場合には、損害賠償の他にペナルティを負わせる」位は早急に改善していくべきと考える。

(4) まとめ

先の(1)(2)(3)に述べたことは、少なくとも、現時点まで、漏えい事件における損害賠償と責任、リスクコントロールの場面でも、気付かれず、論じられていない問題点である。しかし、国民の多くが被害者となるような膨大な個人情報の漏えいが発生し、それらの個人情報が犯罪等に悪用される事態は近年ますます懸念されている。また、いったん流出した情報の完全な回収は不可能であり、漏えいの影響は広くかつ長きにわたって日本社会に大きな害悪を与え続ける。このような事態に至ってもなお手を拱いていることは許されない。

外部委託において顧客情報漏えい事件が頻発することに、構造的な本質的な原因があることに気付くべきである。「外部委託とは内部統制力を喪失することである」にも拘わらず、「それに代わる統制力が考えられていない」。そして「外部委託先の内部統制力が不十分である」現状がある。このような構造的要因を放置したまま外部委託をすることは、トップマネジメントの会社に対する「忠実義務」違反の違法な行為であり、喫緊に改善すべき法的責任というべきである。

<筆者プロフィール>
藤　谷　護　人（ふじたに もりひと）
【経歴】
1979年、東京都千代田区役所に入所し、千代田区住民情報システム開発プロジェクトをプロジェクトリーダーとして企画推進達成する。1991年に通産省システム監査技術者試験に合格、2002年に公認システム監査人認定取得、2008年にIT-ADRセンターのセンター長に就任し、IT分野の専門家として活躍。一方、1989年に司法試験合格後、弁護士活動を開始。1995年 藤谷護人法律事務所を設立。2002年に弁護士法人エルティ総合法律事務所（http://www.lt-law.or.jp）と法人化、2005年～2010年には東京弁護士会CIOに就任する。2006年から2年間は東京地方裁判所非常勤裁判官として従事。2010年に日本弁護士連合会システム監理者に就任。これまでの実績は、企業法務を始め、民事、刑事、行政法全般やコンピュター、ネットワーク、ニューメディアに関する法律関係全般（開発請負契約、著作権等知的財産管理等）、システム監理・監査、セキュリティ監査等、多岐にわたる。実践に裏打ちされた「システム技術（含むセキュリティ技術）と法律技術との融合」について取り組んでいる。また、近時注目されているシステム開発におけるプロジェクトマネジメント義務の先例判決（2004年3月10日）を獲得したことでも知られている。さらに、弁護士法人エルティ総合法律事務所はJISA（一般社団法人日本情報サービス産業協会）から、産業分類上の「情報サービス産業」業者であると認められ、正会員となっている唯一の法律事務所である。