「記録媒体紛失」による情報漏洩事故を減らす現実的方法について

JNSA 組織で働く人間が引き起こす不正・事故対応 WG
セコム IS 研究所　甘利　康文

1．はじめに

筆者らは、JNSA Press Vol.33で「セキュリティ実現の原点から見た内部要因事故抑制手法」と題して、内部不正および従業員のヒューマンエラー抑制に関する問題提起と提言を行う小論[1]（以下、内部要因事故抑制手法論）を発表した。これに対しては、情報セキュリティ分野に留まらない複数の関係者より問合せを頂戴した他、JNSAにおいても、この小論を契機として「組織で働く人間が引き起こす不正・事故対応WG[2]」が発足した。本稿は、このWGにおける筆者の発言を元とし、「私有デバイスによる情報持ち出しがなぜ起きるのか」についての仮説を述べると共に、世の中に対して、その対策に関する現実的方法を提言することを目的としたものである。

2．私有デバイスによる情報持ち出しという「内部不正」

ネット検索すると、機密情報の入ったデバイスの紛失事故が、多くの組織で起きていることが見て取れる。そして、紛失したデバイスのうちの少なくない数が私物、すなわち私有デバイスである。私有デバイスは、パスワード設定や情報暗号化など、紛失や盗難の場合に備えた対策が行き届いていないことも多い。そのため、組織で働く従業員が、私有デバイスを業務に用い、仮に、それが紛失や盗難事故にあった場合、情報流出のリスクは相当高いものとなる。

実際、「情報持ち出しを禁止する」という職場のルールがあるにもかかわらず、そこで働く人間がその「ルールを無視」し、アングラで、もしくは公然と、私有デバイスを使ってそれを行っているという事例は少なからず存在する。これは、少なくない組織で、ルールに抵触する「不正行為」が行われているということである。そして、この行為が元となって、ある割合で、私有デバイスの紛失や盗難といった実際の事故が発生している。

一方、ネットを見る範囲では、組織の情報が記録された私有デバイスの紛失事故が発生した場合、それを発生させた組織における再発予防対策は、「情報の取扱い要領を定める」、「取扱注意を徹底する」、「研修会を開催する」、「職場内ルールを厳格化する」など、一言で言うと「運用を再徹底する」に留まるものが多い。

3．なぜ私有デバイスが用いられるのか？

筆者らは、先の内部要因事故抑制手法論[1]の7.5.4項、「ルール遵守への支援」において、以下のように指摘した。

> 組織で働く人間は、その組織のオペレーションの一部を担い、なんらかの価値を作り出すことをそもそもの目的として働いているのであり、ルールを守るために働いているのではない。そのため、ルール遵守に相当の手間が掛かり、組織のオペレーションをスムーズに行うことを必要以上に阻害する場合、やがてそのルールはオペレーション優先の形で形骸化し、守られなくなっていく。

「情報持ち出しを禁止する」という職場のルールが

● 本稿の内容は、筆者の個人的見解であり、必ずしも筆者が奉職する組織の見解と一致するものではない。
● 本稿では、ノートPCや、USBメモリ、デジタルカメラなどの「情報を記録し、それを持ち出すことのできるIT機器全般」を「デバイス」、そのうち「個人が所有するもの」を「私有デバイス」、業務上の必要性からの情報持ち出しのために組織が用意し、万が一の紛失や盗難などに備えて暗号化などの情報漏洩対策を施したデバイスを「公用デバイス」と呼ぶ。

あるにもかかわらず、少なくない組織の中で、私有デバイスを使い、それに抵触する「不正」が行われている主な理由はここにあるものと考えられる。

「情報持ち出しを禁止する」というルールを制定した組織においては、そのルールゆえ、暗号化など万が一の紛失や盗難による情報漏洩対策を施した「情報持ち出しを前提とした公用デバイス」を用意できないのが普通である。情報を持ち出さないと業務が回らない組織で、「情報持ち出し禁止ルール」が策定された場合、そこで働く人間は「背に腹は代えられない」ことから私有デバイスを用いてルールに抵触する行為を行わざるを得なくなる。実際、「情報持ち出し禁止」ルールがあるにもかかわらず、私有デバイスによる情報持ち出しという「不正」が行われている組織の多くでは、「それをしないと仕事にならない」状況が発生していることを仄聞している。「組織のルールを遵守すると、仕事にならない」という状況では、そのルールは守られるはずもない。ルールが組織のオペレーションの実態に合わないのである。

そして、公然とルール違反が行われている組織の中では、多かれ少なかれ、以下の状況が発生しているはずである。

> ルールが形骸化し、守られない状況が常態化すると、ルール違反をすることに口実を与えてしまう。また、ルールが一旦形骸化すると、それを超える行動のガイドラインが存在しないことから、事実上ルールが無い状態にもなる。[1]

4.「個人情報保護法のガイドライン」によって立ち現れるリスク

個人情報保護法がきっかけとなって、社会の情報漏洩に対する意識は高まり、「機密情報が入った可搬デバイスの紛失や盗難」が、「情報漏洩事故」として報道されることが多くなった。

経済産業省が2009年10月に発表した「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」では、法による保護の対象とする個人情報について、以下のように定義している。

> 「個人情報」とは、生存する「個人に関する情報」であって、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ものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、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。）

このガイドラインを拠り所として、社会一般では、「生存する『個人に関する情報』であって、特定の個人を識別することができる情報」は、暗号化されている、いないにかかわらず「個人情報」であると認識されている。そのため、個人情報が入ったデバイスを紛失したり、それが盗難にあったりした場合には、たとえその中の情報がどんなに強固に暗号化されていたとしても、「個人情報漏洩事故」とされる。

このような「事故」は、マスコミなどでも取り上げられ、世間から組織の不祥事として扱われる。事故発生後に、それを起こした組織が「暗号化などの情報漏洩対策を施している」と広報したとしても、社会は「その情報漏洩対策がどの程度安全か」を知るすべはない。社会からは、「暗号化等によって秘匿化されているかどうかを問わず」（個人）情報漏洩と見なされるため、事故を起こした組織に対する信用は毀損される。個人情報が入ったデバイスの紛失、盗難に関しては、情報暗号化の有無にかかわらず、組織として

は、大きな風評リスクを抱えていることになる。

5.「現在起こっていること」に関する仮説

本項では、「生存する『個人に関する情報』であって、特定の個人を識別することができる情報」を、それが暗号化されている、いないにかかわらず、一律に「個人情報」とみなし、「漏らしてはいけない」とすることから生じる問題について考える。このことが、万が一のデバイス紛失に備えた暗号化処理など、情報漏洩に対するためのセキュリティ対策に関する組織のモチベーションを削ぐ要因になっている可能性は否定出来ない。

情報がデバイスに格納された形で持ち出されて、それを紛失した場合、たとえデバイスや情報にどのようなセキュリティ対策が為されていたとしても「情報漏洩事故」と見なされる。この現状においては、組織の情報セキュリティ担当者としては、情報漏洩事故を起こさないようにするためには「『情報持ち出し禁止』のルールを策定すること」以外に打つ手は無い。

＜コラム＞

情報が暗号化されていようがいまいが、それがデバイスに格納された形で持ち出され、紛失した場合、その組織は「情報漏洩事故」を起こした組織として誹りをうける。持ち出されたデバイスは、常に「紛失のリスク」にさらされる。この状況では、組織の情報セキュリティ担当者は、情報持ち出しに関して「（実質）禁止」というルールを作らざるを得ない。「情報持ち出し禁止」のルールさえあれば、たとえ私有デバイスで情報が持ち出されて紛失事故に至ったとしても、情報セキュリティ担当者としては「その責の多くは持ち出した人間にある」と、ある程度責任回避することが出来る。その後の対応も「運用面を再徹底する」ということで釈明することが可能となる。このように、組織にとっては、現状で唯一採れる手段である「『情報持ち出し禁止』のルールを作ること」は、コストもかからない、一番簡単な自らを守るための手段となる。
これは相当に斜めからの見方ではある。しかし、少なくない組織において、「当たらずといえども遠からず」なのではないだろうか。

先に指摘した通り、「形骸化したルール」の存在は、事実上「ルールが無い状態」を作り出す。「情報持ち出し禁止ルール」のある組織では、論理上、情報持ち出しを前提とした、暗号化などの対策をされた公用デバイスを準備できない。一方、そこで働く人間は、「情報を持ち出さないと仕事にならない」から、そのルールに抵触することにさほど抵抗感を感じずに、十分な情報漏洩対策がなされていない私有デバイスを用いて情報を持ち出す。このような状況では、組織の情報セキュリティ担当者が、「私有デバイスを用いて（不正に）情報を持ち出す場合には、最低限パスワードの付与や暗号化をお願いします」という呼びかけを行うといった、笑い話のようなことは出来る訳もない。組織のルールとして「情報持ち出し禁止」にもかかわらず、「情報を持ち出さないと仕事にならない」という理由で、私有デバイスによる情報持ち出しが行われている。このような状況下では、情報セキュリティに関わるIT産業界としても、技術的に出来ることに限りがあることがお解り頂けるだろう。

現在の暗号技術のレベルに鑑みると、一般に推奨されている暗号がテクニカルに破られるリスクと、外部に持ち出されたデバイスを紛失するリスクを比べた場合、はるかに大きいのは後者である。仕事上の必要性から、暗号化などのセキュリティ対策が行われない形で、情報が私有デバイスに入れて持ち出され、万が一それを紛失した場合、そのデバイス内部の情報は「だだ漏れ」である。それに加え、持ち出された情報は、公式に管理されているわけではないため、組織として、その影響を正確に把握することも困難となる。

この場合、情報を持ち出した当事者は、ルールに抵触する「内部不正」を行った者として組織内部で何らかの処分を受け、事故を起こした組織も世間から相応の誹りを受ける。組織は、「情報の取扱い要領を定める」、「取扱注意を徹底する」、「研修会を開催する」、「職場内ルールを厳格化する」などの再発防止の対策を打ち出すだろう。しかし「情報を持ち出さないと仕事にならない」状況がある以上、私有デバイスを使って情報は持ち出され続ける。「情報持ち出し禁止」に関するルール違反は、構造的に、起こるべくして起こっているという見方ができるのである。

6. 提言

ここまでで、「情報持ち出し禁止」に関するルール違反（内部不正）では、いわゆる「三すくみの状態」が発生していることがお解り頂けるだろう。その大元は、組織における「守れないルール」にある。そして、多くの組織において「守れないルール」を策定せざるを得ない根本は、社会のルールが「守れないルール」であることによる。

本稿では、社会のルールを「守れるルール」とするために、先にあげた「ガイドライン」を以下のように変更することを提言したい。

> 「個人情報」とは、生存する「個人に関する情報」であって、特定の個人を識別することができるものをいう。・・・（中略）・・・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、暗号化等による高度な秘匿化とその運用が共に適正になされている場合は、たとえ情報媒体の紛失、盗難、情報の誤送信等の事象が起こったとしても、それを情報漏洩事故とはみなさない。）

個人情報保護法の運用ガイドラインにある「但し書き」を上記のように変更することで、情報セキュリティに携わるIT産業界は、「情報を持ち出さないと仕事にならない」という必然的な必要性がある「情報持ち出し」に関して、「暗号化等による高度な情報秘匿化とその運用によって、その利用を特定の者に限る」ための技術的なソリューションを提供することが可能となる。

機密情報を扱うユーザー組織には、社会から認められている「安全な公的情報持ち出し手段」として、持ち出し情報を高度に暗号化したり、それを安全に管理運用したりするソリューションを適用したデバイス（公用デバイス）を用意し、それを現場で働く人間に対して提供する新たなインセンティブが生まれる。「業務上の必要性によって情報を持ち出す場合には、『ソリューションA』により暗号化を施し、『ソリューションB』により適正に管理された公用デバイスを用いること」のような形で、その組織で働く人間が「実質的に守れるルール」を策定することも可能となる。

この状態で、デバイスの紛失等の事象が起こったとしても、社会的に「情報漏洩事故」とは見なさない前提であるため、組織としては風評リスクを回避できる。加えて、各種のセキュリティ対策が施された公用デバイス内の情報は、現実的には、特定の人間以外の不正利用が不可能であることから、大きな実害も生じない。

「情報媒体の紛失、盗難、情報の誤送信等の事象が起こったとしても、それを情報漏洩事故と見なさないようにする」ためには、ユーザー組織において各種技術ソリューションの運用がきちんと行われているかどうかについての、第三者による認証も必要となるだろう。暗号の認証としては、現在、総務省および経済産業省が共同設立したCRYPTRECによるものがあるが、これは暗号化強度を技術的に評価するのが主目的である。デバイスに入れる情報に、どんなに強

い暗号化アルゴリズムを適用したとしても、パスワードなどの鍵の管理に不備があるなど、運用が徹底されていない場合、総体としての持ち出し情報のセキュリティレベル低下は免れない[3]。

そのため「暗号化等による高度な秘匿化とその運用が共に適正になされている」かどうかの認証は、「JIS Q 15001(個人情報保護マネジメントシステム)」のように、運用管理面の評価を重視する形にしなければならないだろう。これまでも「CRYPTRECで推奨された暗号化がなされていたならば、情報が流出した場合においても、情報漏洩とみなさないようにしては」という提言はあった[4]。しかし、いかに「推奨暗号化アルゴリズムによる強固な暗号化」がなされていたとしても、その暗号を解読するための鍵管理などの運用が杜撰であったとしたら、総合的観点からの情報の機密性は損なわれてしまう。本稿の提言は、技術のみならず、この運用までもを総合的に評価、認証し、問題が無ければ、たとえ、デバイスの紛失、盗難、情報の誤送信等が起きたとしても、それを「情報漏洩事故とは見なさない」とするものである。

＜コラム＞

十分強い強度で暗号化された情報であっても、それが流出した場合の世間の反応は、「極めて微小ではあるが、数学的にはゼロではない可能性」に対して、社会がミスリードに陥り、過剰反応しているためではないかと考えられる。現在利用が推奨されている暗号化アルゴリズムの多くは「十分に強く」、総合的観点からは、何らかの方法で「復号キー」を入手しない限り、一般の人間、環境では、実質上解読不能と言っても良い。多くの場合、心配すべきは「暗号化アルゴリズムの弱さ」ではなく、「何らかの方法で『復号キー』を知られてしまうこと」である。そのため、通常の場合においては、復号キーを知られてしまわないように管理運用に十分な注意を払わなければならない。

個人情報保護法の運用ガイドラインにある「但し書き」に、社会の現実にあった変更を加えることで、業務上の必要性から情報を持ち出さざるを得ない多様な業界のユーザー組織に、「情報に高度な秘匿化を施し、その利用を特定の者に限る」ための「技術的手段、管理運用的手段」を導入する強いモチベーションが発生する。当然、それを提供するIT産業界側にも具体的ソリューションを開発、提供する新しいインセンティブが生まれる。加えて、組織の管理運用状況を認証する公的体制に対する新しいニーズも生まれるだろう。ユーザー組織で働く個人の仕事が回る。組織のオペレーションが回り、風評リスクも抑えられる。情報セキュリティ分野や社会に新しい需要が生まれることでIT産業がさらなる発展をし、「本当の意味での情報漏洩」も抑えられる。良いことづくめである。

7. 本提言の別の視点 ～ 暗号化情報の扱いに関する矛盾 ～

現在、パブリックネットワークでは、VPN技術を用いることにより、ネットバンキングやクレジット決済、確定申告や医療情報など、相当な機微情報が、暗号化され、通信されている。このケースでは、情報がパブリックネットワークを流れるにもかかわらず、特定の人間以外にはそれが解読できないものとして扱われている。その情報がどのようなサーバーを経由して通信されているかなどについては、ほとんど気にされることもない。しかし、先の「ガイドライン」を杓子定規的に解釈するならば、たとえその暗号化強度がどのようなものであったとしても、個人を特定できる暗号化情報は「公にさらしてはいけない個人情報」であり、それがインターネットのようなパブリックネットワークを流れることは「個人情報流出」に当たるという解釈も可能となるのである。しかしながら、今現在も、暗号化された情報は、どんなに機微なものであったとしても、パブリックネットワークを介して公然とやり取りがなされており、社会はそのことから多大なる恩恵を受けている。

現在、たとえ同等の強さで暗号化された情報であったとしても、それが入ったデバイスが紛失や盗難に遭うと事故として扱われる一方で、それがパブリックネットワークを流れることについては、問題視されていないという状況が起きている。これは明らかに矛盾である。本稿の提言は、この矛盾を解消しようとするものでもある。

＜コラム＞

過去、事故発生に関して、「可能性が全くない時以外は、研究者は『ゼロではない』という表現をよく使う」という研究者の発言がマスコミに流れたことがあるが、「数学的にゼロではないもの」に対する専門家の見解を解釈する場合には十分な注意が必要であろう。世の中では、これが主な要因となって、暗号化された情報の解読可能性についての「過剰反応」が起こっているものと考えられる。「非常に微小で実質上無視できるものの、数学的にはゼロではないもの」を、「ゼロではない」と表現するのは、論理的な厳密性を論ずる際の「学術畑方言」、「研究者方言」である。「ゼロではない」という類の専門家の発言が、世間を混乱させている例はこれに限らない。人々は落ちる可能性が「ゼロではない」のに飛行機に乗る。現実的な議論では、このことを忘れてはならないだろう。

8．おわりに

先の、内部要因事故抑制手法論では、「組織として、従業員がルール遵守をする行為に必要以上の手間がかからないように支援する必要がある」旨について触れたが、これは「情報漏洩事故と見なす基準」についても同様である。

> 社会正義に反しない範囲で、組織のオペレーションの実態にあったルールを策定し、運用していくことである。そのためには、組織のオペレーションを熟知している人間が、ルール策定をする必要がある[1]。

この提言は、組織のルールという観点のものであるが、これは「世の中のルール」についても同様である。「普通では守れないルール」、これはルールに問題がある。社会のオペレーションの実態にあったルールを策定しなければ、守れるはずがない。

実社会で回っているオペレーションと、ルールとの乖離、矛盾。ここにメスを入れることにより、「ルール違反」という、組織内部で行われている「内部不正」は大いに減るはずである。

【参考文献】

[1] 甘利康文，新井真司，内田順一：セキュリティ実現の原点から見た内部要因事故抑制手法，JNSA Press Vol. 33, pp.3-29 (2012)

[2] 甘利康文：組織で働く人間が引き起こす不正・事故対応WG，JNSA Press Vol. 35, pp.6-7 (2013)

[3] 松本泰，伊藤忠彦：暗号技術による個人情報保護の制度と技術の動向，JNSA Press Vol. 34, pp.3-11 (2012)

[4] 辻井重男：情報社会のセキュリティと倫理の課題，Fundamentals Review Vol.1, No.3, pp.10-26 (2008)