2011. 2.24

情報セキュリティニュース ＜2010 No.5＞

情報処理実態調査等から見る企業に必要な情報セキュリティ対策のポイント ～効率的な対策を目指して～

１．はじめに

2010 年度になってからも、お客さまから情報セキュリティ対策や個人情報漏えい事故の事後処理の相談をいただくことが相変わらず多い。2005 年の個人情報保護法施行から約 6 年が経過し、企業・組織の情報セキュリティ対策は進んでいるはずであるが、個人情報漏えい事故は少なからず起きており、また、企業・組織は自社の情報セキュリティ対策が十分でないと感じている。

情報セキュリティ対策には「これでいい」という限度がなく、コストとロードがかかるものであるが、限りある企業・組織の資源の中で効率的に対策を講じるにはどうしたらいいだろうか。

そこで本稿では、個人情報漏えい事故の傾向と企業・組織における情報セキュリティ対策の取組傾向を見ながら、効率的な情報セキュリティ対策について考えていきたい。

２．個人情報漏えい事故の傾向

（１）事故件数と漏えい情報

NPO 日本ネットワークセキュリティ協会の「情報セキュリティインシデントに関する調査報告書」では、新聞、インターネットニュース、組織のリリース文書などで公表された情報漏えい事故が集計されている。これによると 2009 年に発生した個人情報漏えい事故は 1,539 件と、１日あたり約 4.2 件もの事故が発生していることになる。

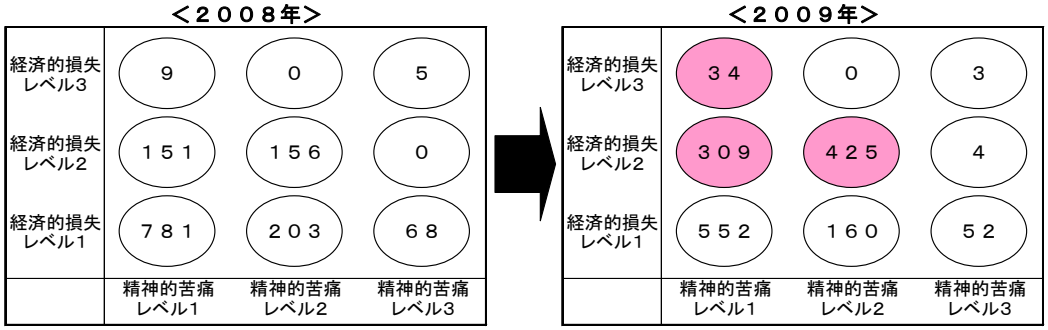
また、2009 年の事故による漏えい人数合計は 5,721,498 人であり、事故１件あたりの漏えい人数は約 3,924 人と多い。

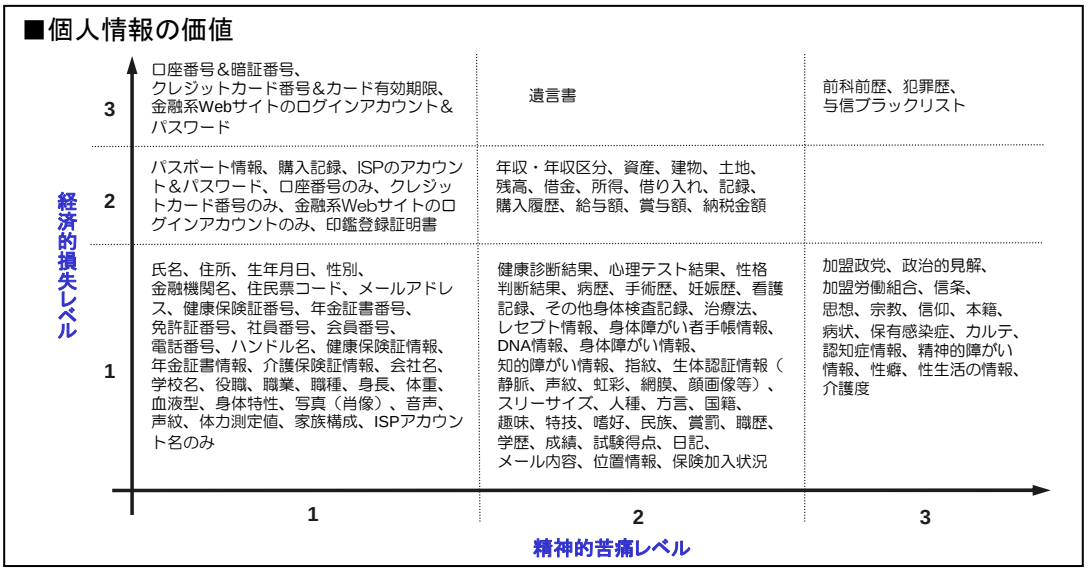
■個人情報漏えい事故の件数と漏えい人数

	2008 年	2009 年
事故件数	1,373 件	1,539 件
漏えい人数	723 万 2,763 人	572 万 1,498 人
事故１件あたりの漏えい人数	5,668 人	3,924 人

次に、漏えいした情報の内容を見てみると、2008 年と比較して 2009 年は漏えいした情報の価値が高い事故が増えている。これは経済情報（口座情報、クレジットカード情報、所得情報など）やセンシティブな情報（健康・医療情報、嗜好・思想情報など）等の重要な内容を含む個人情報漏えい事故が増えているということであり、事故によって被害者（個人情報の本人）に与える損害・苦痛はもちろん、漏えい元である企業・組織が被る損害も社会的信用や損害賠償の面で大きくなっていると言える。

■漏えい情報の価値分布（注：損失レベルの説明は次ページを参照）



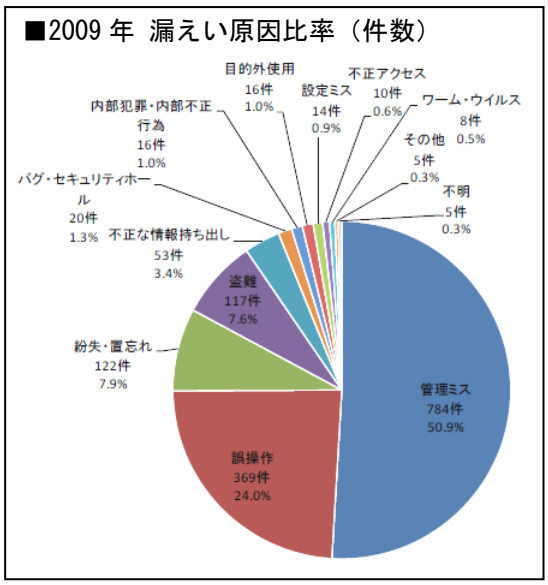


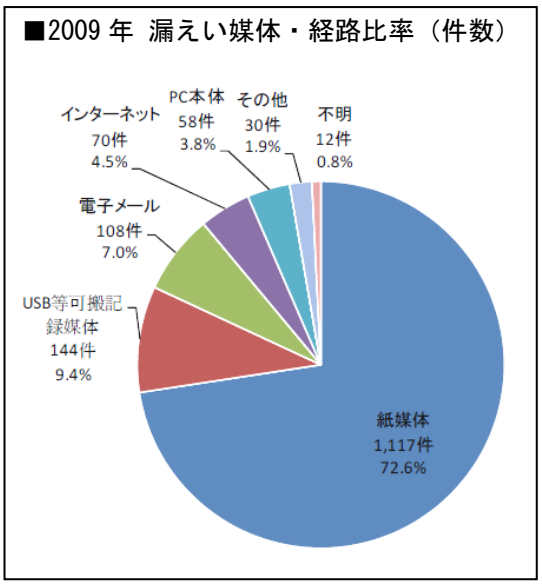
（２）事故の原因と媒体・経路

個人情報漏えい事故の原因（事故件数ベース）を見ると、「内部犯罪・内部不正」「不正アクセス」といった悪意によるものも一定数発生しているが、「管理ミス」「誤操作」「紛失・置忘れ」「設定ミス」といった意図しない基本的な過失の割合が全体の事故件数の約 84%と多いことがわかる。「管理ミス」は書類紛失など、「誤操作」はＦＡＸ・電子メール・郵便の誤送信など、「紛失・置忘れ」は外部の場所での紙資料・PC・USB の紛失などがあげられる。

この他、「不正な情報持ち出し」「目的外使用」といった、情報管理ルールがあるにもかかわらず安易なルール違反をしたことによって発生する事故もある。

次に、漏えい媒体・経路（事故件数ベース）では、「紙媒体」「USB 等可搬記録媒体」「電子メール」「インターネット」「PC 本体」など日常業務で使用しているものがほとんどを占めている。





（３）事故の傾向のまとめ

- 個人情報漏えい事故は少なからず発生しており、漏えいした情報の価値が高くなることにより事故発生時の損害も大きくなってきている。
- 事故の多くは日常業務の中でのふとした過失や安易なルール違反によって発生している。
- 事故の漏えい媒体・経路のほとんどは日常業務で使用しているものによる。
- システム技術の進歩に伴い、大容量の USB や PC の軽量化などによって業務を効率化できている反面、事故が発生しやすく、発生した場合の損害も大きくなる環境にある。

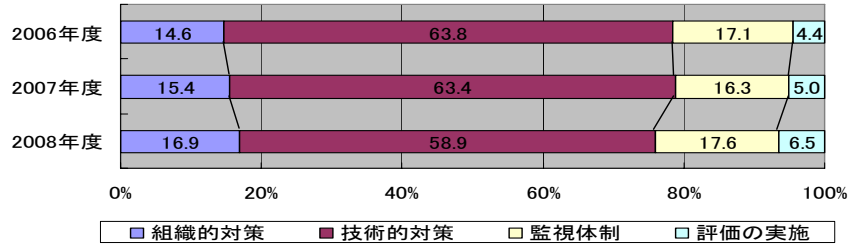
３．企業の情報セキュリティへの取組

（１）情報セキュリティ対策の費用内訳と対策実施状況

経済産業省が 2010 年 8 月にリリースした「平成 21 年情報処理実態調査結果報告書」では、アンケート（大企業から中小企業まで約 5,000 社が回答）により企業の情報処理の実態を把握・集計しているが、その中から情報セキュリティ取組に関する部分を見ていきたい。

企業が情報セキュリティ対策にかける費用の内訳を見てみると、「技術的対策」の割合が約６割と半分以上を占める。データ暗号化や内部アクセス管理などのシステム的な技術対策や、重要なコンピュータ室への入退室管理などの物理的な対策にはコストがかかるためにこのような結果になっていると考えられる。

■情報セキュリティ対策費用の内訳構成比の推移



次に企業の情報セキュリティ対策の実施状況とセキュリティ向上への寄与状況を見てみる。全体の約 87%が何らかの情報セキュリティ対策を実施していると回答している。対策の種類別では、「技術的対策」の実施率は約 81%と高いが、「組織的対策（約 66%）」「監視体制（約 57%）」の実施率はさほど高くなく、「評価の実施」の実施率は約 39%と低い。ここで気をつけたいのは、自社では対策を実施していても、取引先や外部業務委託先では対策を実施できていない可能性があるということである。

情報セキュリティ対策がセキュリティ向上に寄与したと回答した企業の割合は全体で 89%と高く、対策の種類別でも、「組織的対策（約 81%）」「技術的対策（約 89%）」「監視体制（約 86%）」「評価の実施（約 83%）」いずれも高く、どの種類の対策も実施すればセキュリティ向上に有効であると言える。

■情報セキュリティ対策の実施状況とセキュリティ向上への寄与状況の比較（2008 年度）

対策の種類		対策の実施率	セキュリティ向上に寄与した割合
＜情報セキュリティ対策＞計		**86.6%**	**89.1%**
組織的対策の実施	**＜組織的対策の実施＞計**	**65.5%**	**80.8%**
	リスク分析	33.8%	76.5%
	セキュリティポリシーの策定	49.3%	75.6%
	セキュリティポリシーに基づいた具体的な対策の検討	42.2%	79.1%
	情報セキュリティ報告書の作成	15.9%	64.3%
	事業継続計画（BCP）の作成	18.3%	59.4%
	全社的なセキュリティ管理者の配置	47.9%	77.6%
	部門ごとのセキュリティ管理者の配置	34.6%	75.1%
	従業員に対する情報セキュリティ教育	43.5%	79.7%
	取引相手における情報セキュリティ対策実施状況の確認	26.5%	74.0%
	内部統制の整備強化	38.6%	71.4%
技術的対策の実施	**＜技術的対策の実施＞計**	**81.3%**	**88.8%**
	重要なコンピュータ室への入退室管理	52.7%	85.5%
	重要なシステムへの内部でのアクセス管理	64.7%	84.8%
	データの暗号化（PKIを含む）	33.4%	83.6%
	外部接続へのファイアウォールの配置	72.7%	88.4%
	ISO/IEC15408認証取得製品の導入	8.1%	62.6%
	シンクライアントの導入	11.2%	66.7%
	生体認証の導入	12.4%	81.9%
監視体制	**＜監視体制＞計**	**57.2%**	**86.0%**
	セキュリティ監視ソフトの導入	56.0%	85.8%
	外部専門家による常時セキュリティ監視	12.2%	83.8%
評価の実施	**＜評価の実施＞計**	**38.9%**	**82.8%**
	情報セキュリティ対策ベンチマークの活用	7.6%	71.7%
	外部専門家による定期的なシステム監査	17.3%	86.4%
	内部による定期的なシステム監査	28.1%	80.1%
	外部専門家による定期的な情報セキュリティ監査	14.2%	85.3%
	内部による定期的な情報セキュリティ監査	26.7%	83.1%
	情報セキュリティマネジメントシステム（ISO/IEC27001）認証の取得	7.0%	84.5%

（２）企業の情報セキュリティ取組状況のまとめ

・情報セキュリティ対策費用では、「技術的対策」に多くのコストをかけている。
・多くの企業が何らかの情報セキュリティ対策を実施している。対策の種類別では、「技術的対策」の実施率は高いが、「組織的対策」「監視体制」の実施率はさほど高くなく、「評価の実施」の実施率は低い。
・セキュリティ対策は総じてセキュリティ向上に寄与している。対策の種類別でも、「組織的対策」「技術的対策」「監視体制」「評価の実施」いずれも実施すればセキュリティ向上に有効である。
・対策の実施状況とセキュリティ向上への寄与状況を比較すると、「組織的対策」「監視体制」「評価の実施」は実施すればセキュリティが向上するはずなのに、実施率がさほど高くない。特に、「評価の実施」はその傾向が顕著である。

４．効率的な情報セキュリティ対策

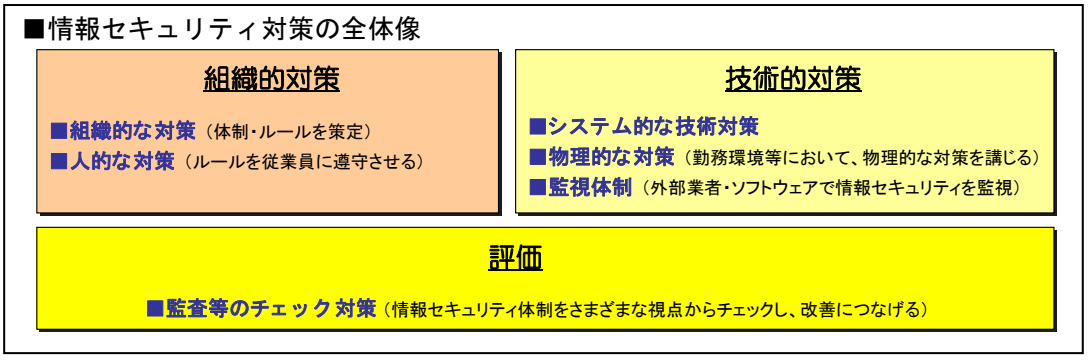
（１）情報セキュリティ対策の全体像

情報セキュリティ対策は、大きく「組織的対策」「技術的対策（監視体制を含む）」「評価」の３つに分けられる。

「組織的対策」は、情報セキュリティの体制・ルールを構築し、従業員に遵守させることで、例えば、情報の社外持ち出しルール策定、従業員への教育研修、外注委託先への対策確認などがあげられる。

「技術的対策」は、システム的な技術対策、勤務環境等の物理的な対策、外部業者またはソフトウェア等での監視体制構築のことである。具体的には、適切なアクセス権限の付与、USB メモリ使用の制御、ウイルス対策ソフト、監視カメラ、部外者の侵入を予防する執務室レイアウトなどがあげられる。

「評価」は、「組織的対策」「技術的対策」にまたがる情報セキュリティ対策を様々な視点からチェックし、改善につなげるもので、内部監査・外部監査の実施などがあげられる。



上記対策をすべてバランスよく実施することが理想であるが、本稿では、限られた予算と人的資源の中で効率的に対策を実施することを考えたい。

前記「３．企業の情報セキュリティへの取組」で見たように、実施すればセキュリティ向上が見込めるのに実施率が高くない「組織的対策」と「評価の実施」に着目する。この２つは、「技術的対策（監視体制を含む）」に比較してコスト面での負担は小さいと考えられるため、取り組みやすい。また、前記「２．個人情報漏えい事故の傾向」で見たように、情報漏えい事故のほとんどは、日常業務の中での意図しない基本的な過失や安易なルール違反によって、日常業務で使用している媒体・経路から発生しているため、「組織的対策」によって身近な情報セキュリティ体制・ルールを構築・見直しして実効性を確保することと、「評価の実施」によって日常業務実施状況をチェック・改善することは、情報漏えい事故防止に有効であると考えられる。

では、「組織的対策」と「評価の実施」のポイントをこれから見ていくこととする。

対策の種類	対策の実施率	セキュリティ向上の割合	人的なロード面	コスト面
組織的対策	中（65.5%）	高（80.8%）	中～大	小～中
技術的対策	高（81.3%）	高（88.8%）	小～中	大
監視体制	中（57.2%）	高（86.0%）	小～中	大
評価の実施	低（38.9%）	高（82.8%）	小～大	小～中

（２）「組織的対策」のポイント

情報セキュリティ対策のうち「組織的対策」は組織と人に関する対策であるが、この組織と人に関する対策は両方できて初めて有効に機能するため、簡単なようで完全にできている企業・組織はほとんどないのではないだろうか。対策のポイントは次の３点になる。

①現場の業務内容および情報管理実態の把握
②有効な「体制」・「ルール」の構築
③「ルール」を従業員に徹底させる

まず、「①現場の業務内容および情報管理実態の把握」「②有効な「体制」・「ルール」の構築」について考える。

現在の多くの企業・組織ではトップダウンで体制・ルールが策定されており、このため、体制・ルールと現場の業務内容・情報管理実態との間に乖離があり、せっかく策定した体制・ルールに実効性が伴っていないケースがある。例えば、ルールが現場の業務オペレーションやシステム実態に即していないために現行ルールに従った管理が不可能になっているケース、従業員が業務効率を優先して現行ルールから逸脱した運用をしてもチェックできていないケース、業務上どうしても発生するヒューマンエラー（意図しない基本的な過失）をチェックできていないケースなどがあげられる。やはり、ルール策定者サイドの視点だけでルールを定めるのは限界があるため、現場の業務オペレーションと情報管理実態を再確認し、現場の実情・声を反映させるように体制・ルールを見直すことによって、より実効性のある情報セキュリティ対策が実施でき、ヒューマンエラーやルール違反を予防することができる。これには、管理部門と現場が一体となってルールを策定していくために、現場でのヒヤリ・ハット事例、現場での疑問点や工夫している点を現場へのアンケート・ヒアリング等で収集して活用するなど、体制・ルール策定においてトップダウンだけでなくボトムアップの要素を取り入れることが有効である。

次に「③「ルール」を従業員に徹底させる」であるが、これは地道な継続的な取組によって従業員の情報セキュリティ意識を向上・維持させていくほかない。ｅラーニングや研修を継続して実施することにより、日常業務で扱う情報の重要性や情報漏えい事故が発生した場合の影響を従業員にしっかりと認識させるとともに、日常業務遂行時にもあたりまえのように情報セキュリティ対策が実施できるような環境を作ることが必要になる。

参考までに、「組織的対策」において、効果的な取組の具体例を紹介する。

■組織的対策の効果的な取組具体例

◇封入時に2名が確認・押印することでミスを軽減

・郵送物の封入のダブルチェックをしている。封入前に2人で確認し、封入時にも2回以上確認するようにしている。封入の袋にあらかじめ印鑑を押す場所を2つ印刷しており、必ず2名が押印するようにしている。

◇職員個々人が自己診断を実施し、取扱責任者が定期的にチェックする目標管理的な運用で自己点検の実効性を確保

・自己診断書をツールとして準備している。個人情報保護管理者が自分の担当する事業所の状況について定期的（半期に1回程度）にチェックを行い、本社に報告するようにしている。
・個人については、年に2回は個人情報保護に関する「自己診断」をさせている。年に2回、時期を指定して（GW 前、年末・年始直前など）実施している。
・自己診断後、取扱管理者が見てチェックをすることになっており、その際に、問題があれば取扱責任者が指導を行ったり、できていないにも関わらず「できている」としていることなどについては指摘をするように、目標管理制度的に運用することで、単なる書類としての「自己診断」に留まらないようにしている。

◇管理を極めて厳格に行っていることを明確にアナウンスすることで緊張感を醸成

・ログの管理（どのファイルをコピーしたのか、どのホームページを閲覧したのかということ等）を行っていること、日常的に事務所を回りながらチェックを行っていることについては広く従業者に公表している。従業者はいつも見られている、チェックされている、という認識を持っているようであり、「常に見ている」という姿勢を広く公表することで効果的な従業者教育になっている。

◇内部点検の際に委託先職員に同道してもらい、自社のチェックの厳しさを伝える

・内部点検の際に、委託先企業の職員を同道している。自分たちがどれほどキッチリしているかということを見せることで、要求される水準を示すことができ、暗に個人情報保護に関する努力を促すことができていると考えている。

【参考】 経済産業省「平成 21 年度「個人情報の適正な保護に関する取組実践事例調査」」

（３）「評価の実施」のポイント

外部監査や内部監査による「評価の実施」では、情報セキュリティの実態をチェックしていくが、構築した体制・ルールとその実施状況を改めて確認することは情報セキュリティ対策を徹底していくうえで不可欠である。そのポイントはシンプルに次の３点である。

①ＰＤＣＡサイクル	・情報セキュリティに関するＰＤＣＡサイクルが構築され、きちんとまわっているか。
②ルール遵守	・業務がルールどおりに運用されているか。 ・策定されたルールは形骸化していないか。
③ルールの有効性	・策定されたルールは、本当に効果があるか。 ・策定されたルールは、現状（業務内容、システム最新技術等）に対応しているか。

企業の情報セキュリティに関する監査について当社がご支援する場合があるが、その場合も上記の３点を中心に実態をチェックしている。監査を実施した中で出てきた気になる問題点を以下のとおり列挙する。内容を見てみると「あたりまえ」とされていることばかりだが、実態としてできていないケースが多いのである。

「評価の実施」はチェックを行い改善につなげることが目的であるため、上記の３つのポイントを中心に、体制・ルールおよび管理実態の両面から、以下の例のような問題点がないかをチェックし、前記「（２）「組織的対策」のポイント」を参考に改善されることをお勧めする。

■監査時における問題点の例

○各種ルールが異なる時期に策定されたために、整合性がとれていない。（つぎはぎだらけ）
○ルールは策定されているが、会社として実態をチェックできていない。
・ルールのつくりっぱなし
・ルール策定部門（総務部門等）が現場の実態を把握していない　… 等
○ルールはあるが、責任の所在があいまい。
・誰が承認するか、誰がチェックしてどの部門に報告するかが不明確
・組織改編・人事異動等により責任の所在がわからなくなっている　… 等
○業務の現場が、策定されたルールどおりの運用をしていない。
○ルールがシステム最新技術に対応しておらず、想定していない運用がされている。
○教育研修が不十分。
・以前実施したが、現在は実施していない
・中途入社社員への教育研修をしていない　… 等
○内部監査（社内での監査）は実施しているが、同じ社内でのチェックのため、馴れ合いのチェックになっている。

なお、参考までに、最近の監査において見落としがちなチェック項目（具体例）を紹介する。

■見落としがちなチェック項目（具体例）

◇重要データ（機密情報、個人情報等）が社内システムの共有フォルダに置かれていないか？
…必要な人以外から重要データが参照・取得できるようになっていないかを、「社内ルール」「アクセス権限」「実態」等の観点からチェックする。

◇社外持ち出し用のモバイルPCに必要以上のデータが置かれていないか？
…社外使用時のためにモバイルPCにデータを一時的に保存する場合、業務で使用する必要最小限のデータ以外のものがモバイルPCに保存されていないかを、「社内ルール」「実態」等の観点からチェックする。

◇オンラインストレージを使用不可にしているか？
…オンラインストレージを使用して自宅にデータを送付していないかを、「社内ルール」「オンラインストレージへのアクセス規制」「実態」等の観点からチェックする。

◇社内PCから個人所有のスマートフォンへのデータ転送を不可にしているか？
…社内PCから Bluetooth 等によりスマートフォンにデータが転送できないようになっているかを、「社内ルール」「実態」等の観点からチェックする。

５．おわりに

情報漏えい事故は人間が業務を行う限りなくなることはないが、事故が起きると被害者に大きな損害・苦痛を与え、漏えい元の企業・組織にとっても大きな影響を及ぼし、社会的信用の失墜は致命的なものになりかねない。本稿では、情報セキュリティ対策について、企業・組織の限りある予算と人的資源の中で効率的に取り組むポイントについて考えてきた。事故を予防するためには「これで十分」という限度はないが、まずは身近なできるところから取り組んでいくことをお勧めする。本稿の内容が皆さまの取組の一助となれば幸いである。

以　上

株式会社インターリスク総研
コンサルティング第二部
マネジャー・上席コンサルタント　野﨑　久之

［参考資料］

・NPO 日本ネットワークセキュリティ協会
「2009 年情報セキュリティインシデントに関する調査報告書」
「2008 年情報セキュリティインシデントに関する調査報告書」
・経済産業省
「平成 21 年情報処理実態調査結果報告書」
「平成 21 年度「個人情報の適正な保護に関する取組実践事例調査」」

株式会社インターリスク総研は、ＭＳ＆ＡＤインシュアランスグループに属する、リスクマネジメントについての調査研究およびコンサルティングに関する専門会社です。
弊社では情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、あいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
㈱インターリスク総研　コンサルティング第二部
TEL.03-5296-8918　　http://www.irric.co.jp/