情報漏洩対策

－喜んでやる情報漏洩対策－

アブストラクト

1. 研究の目的

2005 年 4 月の個人情報保護法施行後も情報漏洩事故は後を絶たない。各社様々な情報漏洩対策を実施しているが、それらの対策は本当に有効なのであろうか。そこで当分科会では、情報漏洩事故の現状や対策の実施状況を調査し、**「やっているフリ」**ではなく、**「本当に社員が喜んでやる対策」**の提言を目的とし、研究を行った。

2. 研究の進め方

既に公表されている様々な調査報告およびメンバ各社の状況調査の結果を踏まえ、情報漏洩事故の主な原因を「技術的側面」、「人的側面」に分類し、以下①～③のステップで有効な改善策の検討を行った。さらに「情報価値の可視化」に着目した近未来の情報漏洩対策について検討し、要望として提案する。

① 現状調査（本当にやっている？）
② 課題の抽出（問題はなに？どこ？）
③ 課題に対する改善策の検討と提言

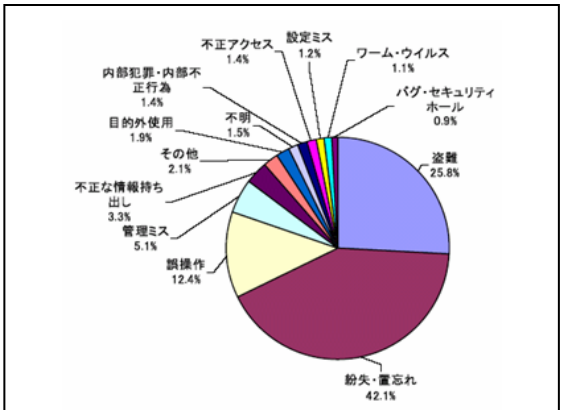
3. 研究成果

(1) 情報漏洩事故の現状

個人情報漏洩に代表される情報漏洩事故の主な原因は、ヒューマンエラーであり、実に全体の 6 割程度を占める。（図表 1）

つまり、これらのヒューマンエラーに対する有効な対策が実施できれば、情報漏洩事故は確実に減少すると思われる。そこで、当分科会では「技術的対策」については、各社の導入状況および現状調査に留め、主たるテーマとして事故原因の大部分を占める「人的対策」について取り上げることとした。

図表 1 個人情報漏洩原因の件数割合



※JNSA2005 年度 情報セキュリティインシデントに関する調査報告書

(2) 技術的対策の現状

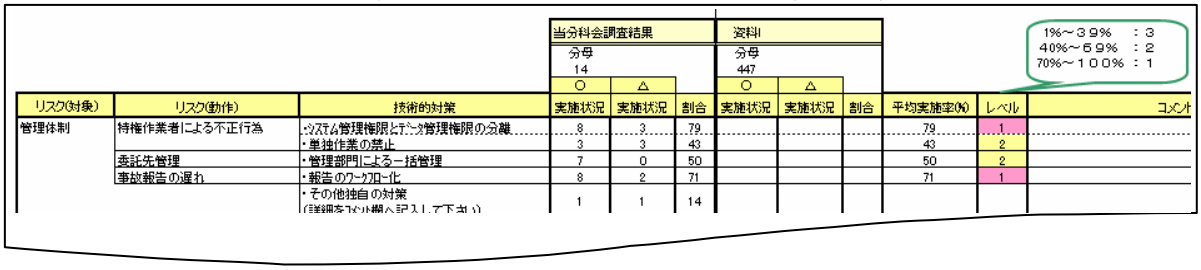
情報漏洩経路に着目し、それぞれに対する技術的対策を調査するため、メンバが実際に体験した「ヒヤリ・ハット」事例を中心に、想定される原因と経路の一覧表を作成した。（図表 2）

図表 2 情報漏洩の原因と経路集　抜粋

No.	誰が	何を	どうした	原因	リスク(対象)	リスク(動作)	技術的対策	残存リスク
1	システム管理者	ID・パスワード	本人確認せず他の人に開示	管理ミス 確認手順を怠った、あるいは詳細な確認手順が無い	ID・パスワード	確認もれ(公開相手)	・生体認証システム	・退職者、異動者のアクセス権限削除漏れ
2	メールマガジンの送信先が	発先に個人のメールアドレスを	掲載したため、送信先全員にメールアドレスを通知した (普通はBCCにする)		メールアドレス	eメール送信時の送信先の設定ミス	・メールシステムによる自社(または認可された)ドメイン以外へはBcc送信のみを許可	・認可ドメインの無秩序な登録
3	営業企画部員	一時使用アクセスID	一時使用アクセスIDを複数の関係者から申し込まれた際、	⑫eメールの送信方法-ツール	ID・パスワード	eメール送信時の送信内容の間違え	・メール送信のシステム化 ・重要情報の添付ファイル化、	・添付ファイル化の漏れ ・添付ファイル化対象の誤認

次に、これらの原因と経路に対する有効な技術的対策としてどのようなものが存在するのか既存のセキュリティ製品について調査を行った。さらに、原因と経路に対するメンバ各社の対策実施状況および公表されている調査結果の中から、これら技術的対策の実施状況を調査し、その実施率から 3 つのレベルに分類し、自社の現状判断指標として参照できる一覧表を作成した。（図表 3）

図表 3 情報漏洩防止に関する技術的対策状況　抜粋



			当分科会調査結果 分母 14 ○	当分科会調査結果 分母 14 △		資料 分母 447 ○	資料 分母 447 △			
リスク(対象)	リスク(動作)	技術的対策	実施状況	実施状況	割合	実施状況	実施状況	割合	平均実施率(%)	レベル
管理体制	特権作業者による不正行為	・ｼｽﾃﾑ管理権限とﾃﾞｰﾀ管理権限の分離	8	3	79				79	1
		・単独作業の禁止	3	3	43				43	2
	委託先管理	・管理部門による一括管理	7	0	50				50	2
	事故報告の遅れ	・報告のﾜｰｸﾌﾛｰ化	8	2	71				71	1
		・その他独自の対策 (詳細をｺﾒﾝﾄ欄へ記入して下さい)	1	1	14					

1%～39%　：3
40%～69%　：2
70%～100%　：1

(3) 人的対策の現状

メンバ各社の実施状況を調査した結果、主な対策として以下のものが挙げられた。

「教育・訓練の実施」、「制度・ルールの策定（文書化）」、「各種認証の取得」、「セキュリティ対策専門部署の設置および担当者の任命」

(4) 課題の抽出

現状調査結果より「技術」、「人」それぞれの課題を抽出した。主な課題は以下の通りである。

技術

① 対策レベルを決められない・投資対効果が見えにくい（どこまでやる？いくらかける？）
② 技術的対策には限界がある（今現在、完璧でも新たな脅威に対応できる保障はない）
③ 運用に問題があると効果を十分に発揮できない（運用するのはやっぱり人である）

人

① 人である以上、過失・不注意によるヒューマンエラーを完全になくすのは不可能である
② 無事故が正しく評価されない（ルールを遵守していれば事故はなくて当たり前？）
③ 個人の処罰を恐れて正しく報告されない（事故を隠蔽していない？）

(5) 技術的対策の課題に対する改善策の提言　**～資産・リスクの可視化と投資判断～**

新たな脅威への対応までも視野に入れれば、技術的対策は日進月歩である。そのような状況下で重要なのは、リアルタイムで守るべき資産・リスクを可視化し、レベルに応じた対策を実施することである。その判断材料として、「技術的対策の実施状況」を参照頂きたい。

(6) 人的対策の課題に対する改善策の提言　**～喜んでやる情報漏洩対策～**

個人情報漏洩事故原因からもわかるように、人はミスを犯す存在である。しかし、その原因を科学的に分析し、人の意識に訴えかける対策を実施することができれば理想的である。その実現に向けた検討結果として、以下に主な改善策を提言する。

① 報奨金制度の導入　～モチベーションアップのために～

「無事故に対する報奨金」、「事故未然防止のための事例報告に対する報奨金」、「対策により増加した作業負荷への業務改善に対する報奨金」

② 経営層による「社員個人は必ず守ります」宣言　～風通しのよい組織作り～

個人を責める行為は、速やかなインシデント報告の阻害要因にもなりうる。ルールを遵守した上で発生した事故に対しては「当事者を責めないこと」、「組織として個人を守ること」を明確に宣言する。

(7) 近未来の情報漏洩対策への要望　**～「情報セキュリティタグ」の導入～**

近い将来、実現可能な技術的対策として、ファイルへ情報セキュリティタグを付けることを考案した。これは、ファイル作成時に付加されるタグに各自で情報の資産区分、重要度、属性等の管理情報を書き込むことで情報価値を可視化し、利用者のセキュリティ意識の向上を図るものである。また、情報資産の分類や違反操作等についてもリアルタイムに管理可能とする。

4. まとめ

当分科会では、技術的対策を施してもなお残存するリスクを中心に研究を進めてきた。

技術的対策によって防ぐことが困難なリスクについては、人的対策で補完する必要がある。また、技術的対策は、人的対策により適切な運用がなされることで有効となる。対策を実施する目的を明確にした上で、関係者の納得性を引き出すべきである。重要なのは人に対する働きかけであり、個人のやる気を引き出し、誇りをもてる組織作りが必要であることが改めて分かった。

有効な情報漏洩対策を行い、さらに従業者が「やる気になる対策」、「社会的に貢献できる対策」が進んでいくことを願う。