In the Future 2013

21 世紀型企業への転換を図る

■　情報管理の実効性を向上させるためには ？！ ②

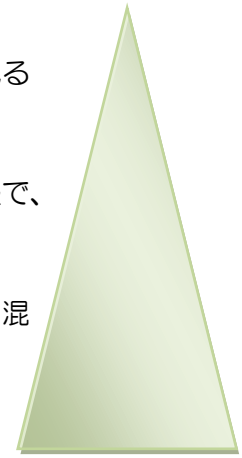
～　情報を管理する方法を考える ～

機密情報の整理　　？！

機密情報は、業界や業種、そして企業規模等によりその定義や区分が異なるものと思います。
いずれにしても、まず最初に管理しなければならないのが、その情報の漏えい・喪失によって、企業の信用が大きく失墜する恐れがあるものでしょう。

- ◆　個人情報の漏えい
- ◆　財務会計情報の改ざん
- ◆　設計図面、調合配分情報の紛失、破損・焼失

また、自社の機密情報だけではなく、取引先の情報・取引先から預かった情報の管理も忘れないようにしなければなりません。
つぎに、どのような「情報」を重要な「情報資産」として把握・管理するのか、という区分が必要となります。
ここでは、情報区分を「極秘」「厳秘」「部外秘」「社外秘」とわけて考えてみます。



【極秘情報】
目的外に使用された場合には、企業の信用に重大な影響を及ぼすことが想定される情報で、ごく限られた関係者のみに開示される情報

【厳秘情報】
目的外に使用された場合には、企業の信用に影響を及ぼすことが想定される情報で、一部の関係者のみに開示される情報

【部外秘情報】
部内者には開示するが、部外者には開示しない情報で、部外に開示した場合に、混乱を招く恐れがある情報

【社外秘情報】
社内では共有し、活用される情報であるが、社外には開示してはならない情報

実際に情報を区分する際には、経営トップ・役員・情報管理者が、企業のポリシーをもとに分類し、管理方法等を決めておきます。
また、各情報については、組織や環境変化に対応しつつ、随時区分を見直すことが必要です。
そして、最も重要なことが、<u>全社員に対して、これらを周知・教育しておく</u>こととなります。

日常的な管理ポイント

利用者毎にアクセス可能な情報、情報システム、業務アプリケーション、サービス等を決めておきましょう。
職務の変更や異動をチェックポイントとして、利用者のアクセス権限を見直しましょう。

社員採用時の適性診断実施 ⇒ ﾌﾘｰﾀﾞｲﾔﾙ 0120-81-4864

事故の可能性と影響を考える　！

重要な情報資産を把握することができたら、つぎは、情報資産がどのような脅威（事故の可能性）にさらされているかを検討することです。

◇　外部の要因（コンピュータウイルス、不正アクセス、サービス妨害など）
◇　内部の要因（セキュリティ対策の不備、ソフトウェアの欠陥、操作ミスなど）

そして、これらの脅威について評価してみましょう。

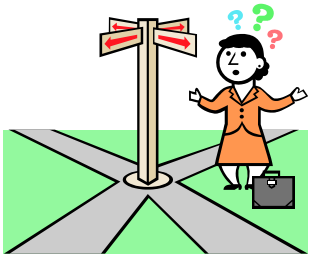
ステップ Ⅰ　どの程度起こりうるか？

頻繁におこる（月１ 回程度） ⇔ たまに起こる（年１ 回程度） ⇔ ほとんど発生しない

ステップ Ⅱ　どの程度の影響を受けるか？

影響大		影響中		影響小
会社の存亡にかかわる	⇔	業務が停止する	⇔	業務効率が低下する

脅威への対応　！



事故が発生した場合の影響の大きさと発生する頻度が把握できたら、企業としての対応方針を決めなければなりません。

しかし、あらゆる脅威に対して対策を講じるのは、コストも時間もかかりますので現実的ではありません。よって、業務に影響があり、ある程度、発生する可能性のあるものに、情報セキュリティ対策への投資を行うようにします。

良く用いられる考え方としては、以下のような４通りの対応方針に分類して、対策を検討することがあげられます。

■ 方針Ⅰ　*リスクを低減する！*
影響度中で、たまに発生するものについては、情報セキュリティ対策を実施することで、影響や発生確率を下げる対策の実施

■ 方針Ⅱ　*リスクの回避！*
影響度大で、頻繁に発生するものについては、業務の方法を変更したり、あるいは、そのような業務を実施しない、という対応

■ 方針Ⅲ　*リスクの移転！*
影響度大だが、めったに発生しないものについては、他社に委託したり、保険などをかける、という対応

■ 方針Ⅳ　*リスクの保有！*
影響度小で、めったに発生しないものについては、無視する、という対応
この場合は、定期的に残存リスクに対して評価することが必要です。

脅威への対応がコスト削減に　？！

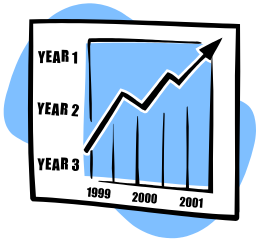
情報セキュリティ対策の実施にはコストがかかりますが、一方で情報セキュリティ対策を実施することで、業務効率化が図られ、結果として全社的なコストの削減に繋がる場合があるといわれています。

◆ ***作業効率の向上や、ミスの削減***

情報セキュリティ対策のため、業務フローやシステムの見直しにより、見せなくて良い人に対するデータの隠蔽や、同じデータを重複して入力する等の無駄な作業をなくすことができる可能性があります。これらによって、作業効率の向上や、ミスの削減に繋がることがあります。

◆ ***システム運用コストの削減***

情報セキュリティ対策を厳格に行うため、管理対象となるサーバを統合し削減することで、システム運用コストの削減などに繋がることがあります。



ケーススタディ　！！

【普段の状況】

〇〇株式会社の情報システムは、Ａ課長がすべてを管理しています。Ａ課長は、システムの設定や各社員のパスワードなどの情報を自分の業務用 PC に保存していました。

【発生した事故】

Ａ課長が結婚することになり、１週間の新婚旅行で海外に出発しました。その間に、〇〇株式会社の電子メールサーバに障害が発生し、電子メールの送受信がまったくできなくなりました。Ｂ部長が業者を呼びましたが、システムの設定等はマニュアル化されていないため、誰も再設定できず、またバックアップデータの復旧もＡ課長以外にできる人がいないので、**結局Ａ課長が帰国するまで、会社では電子メールを使用することができませんでした**。

【危険要因】

① 特定の個人のスキルに依存しすぎている
② 代替要員やマニュアル等が未整備

この問題に限らず、「その人しかできない仕事」を極力なくすようにしなければなりません。忙しさから、ついつい任せっぱなし、という例はよくあるものと思いますが、このケーススタディのような事故が発生したら大変なことになります。

【対　策】

■ どのようなシステムも複数人（代行者）が管理できるようにしておく
■ 情報システムの運用手順書（マニュアル）を整備しておく
■ 運用手順については、情報システムが停止時した際に備えて、紙に印刷しておく
■ 情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握しておく

労働基準監督署への是正報告対応 ⇒ ﾌﾘｰﾀﾞｲﾔﾙ 0120-81-4864