情報リスクマネジメントと損害保険業界の情報リスクへの対応

H15.1.30　　卒業論文
日本大学　山田正雄ゼミナール
経営法　学籍番号 9940106
一期生　　平田　光二

目次

序論

現在、社会の情報化が急速な勢いで進んでいる。コンピュータの価格低下や高性能化、情報通信ネットワークの増大などに伴い、コンピュータは急激に普及してために企業のワークスタイルはこの 10 年で格段の変化を遂げた。大規模な情報システムやネットワークがビジネスの基盤となり、電子商取引も一般化するなか情報は企業にとって経営戦略の実現や日常業務の遂行において、今では必要不可欠なものになっている。そのため消費者ニーズの把握をはじめとした企業における個人情報の重要性はますます高まる傾向にある。その理由として情報は企業戦略上極めて利用価値の高い情報資産であることが挙げられる。

しかしその一方で、情報は不適切な取り扱いにより一度漏洩を起こすと、信用失墜をもたらしかねない危険性をも持ち合わせている。さらには情報システムに関する利便性からのトラブルなどの「情報リスク」が、コンピュータでの仕事量に比例して急増していることも事実である。今日、企業をはじめとした組織は、情報戦略投資の増加、不正アクセスや情報漏洩などの情報セキュリティの問題に直面しており、各企業はコンピュータ化によるコスト削減や業績の向上というプラス要素とともに情報セキュリティのリスク軽減への投資も必要になっている。

さらにこのような情報セキュリティのリスクをより効率的に防ぐにはシステム中心のセキュリティ対策だけではなく、より組織的・継続的なマネジメントが必要になってくるのである。これを「情報リスクマネジメント」という。

そこで本論文ではまずこの情報リスクとその被害や影響の内容を追っていき、さらには二次被害の内容やその対策方法を考えていきたいと思う。次に情報リスクの対策手段として、現在注目されている情報リスクマネジメントの概要やそのリスクコントロール方法の種類について検討し、その後は情報リスクマネジメントの運用方法の内容を見ていきたいと思う。そして最後に今後の情報リスクに対して損害保険業界の対応内容について検討し、この市場においての商業的な価値を含め、今後の損害保険業界の情報分野の発展方向について研究・発表をしていきたいと思う。

第Ⅰ章　情報リスクとその被害・影響

1．情報手段の発達とその変化

（1）情報手段の発達と社会の変化

現在、社会の情報化が急速な勢いで進んでいる。その理由としてコンピュータの価格低下による普及率の増加やコンピュータの処理能力の向上などが挙げられるが、それと同時に急激なＩＴ化に伴い、社会や経済に様々な変化を与えていることも見逃せない。その変

化とはＩＴ化により多くの情報がデジタル信号に変えられ、多数の人が同時に共通の情報にアクセスし、情報交換や加工をすることができるといったことや、単に一方向の情報発信だけでなく、ネット上での意見の交換など多様な情報のやりとりが可能になったことなどが考えられる。つまりこれらの変化に伴う社会のＩＴ化は、企業活動に対して以下の変化として表れているのである。

――社会のＩＴ化に伴った様々な変化――
①企業のワークスタイルの急速な変化
②情報システムやネットワークのＩＴ分野の発展
③企業間の消費者ニーズの把握手段として情報収集の激化などによる急激な変化

以上をふまえデジタルデータの発達により、膨大な量の情報処理を可能にし、大規模な情報システムやネットワークがビジネスの基盤となり、電子商取引や顧客とのオンラインアンケートなども一般化するなか、情報は企業にとって経営戦略の実現や日常業務の遂行において今では必要不可欠なものになっているのである。

しかし社会の急速な情報化に伴うＩＴに関わるトラブルから発生するリスクが、日増しに増大しているという事実も問題化している。これらは財務リスクのような従来型のリスクとは別に「情報リスク」と呼ばれている。

現在このような情報リスクに対しては多くの企業でユーザＩＤとパスワードによるログインが行われ、ファイアウォールなどが導入されている。またコンピュータウィルス対策としてワクチンソフトウェアを導入しており、マシンルームへの入退出管理も行われている場合が多い。他にもシステムの二重化やデータのバックアップ等もされているだろう。しかしそれだけでは十分ではない。それは今日での情報リスクによる被害例が後を絶たないことからも容易に想像することができる。

そのためこの第一章は情報リスクの発生原因からその種類や被害例を挙げ、情報リスクというものを詳しく考えていきたいと思う。

（２）情報リスクの発生原因

まず情報リスクの発生原因を考えてみることにする。

そもそもこのような情報リスクの発生原因としては、次の三点に大別することができる。

――情報リスク発生原因――
①法制度･社会ルールの未整備、組織体制の未対応、オープンなネットワークなどの、仕組みの変化のためのずれや隙間により発生
②セキュリティ技術の発展途上、ソフトウェアの欠陥などのネットワーク･インフラの脆

弱性の問題点により発生
③個人情報に関する認識の低さ、個人の情報活用能力不足などや犯罪により発生

以上の三点の共通点として情報リスクは1960年代以降のコンピュータ技術と通信技術が飛躍的に発展し、インターネットなどの社会のネットワーク化が急速に進展したことによる情報内容の増大から生じたと考えられる。つまりコンピュータの発展により、様々な分野に急激な利便性を与えたと同時に、その反面として急速な変化に対応しきれずにいる法整備・国家や企業などの組織のリスク管理に対する意識・セキュリティ技術・情報価値に対する個人意識など以上の全ての点で未熟であることが、情報リスクの存在を発生させている原因なのである。

そしてこの情報リスク管理への未熟な意識のまま現在の様に、今後も社会のＩＴ化が急速な勢いで進んでいくのであれば、企業活動において大変な問題になるはずである。

そのためまず次の項では、この情報リスクによる被害例を考えていきたいと思う。

２．情報リスクからの被害とその状況

（１）コンピュータウィルス被害

今日、最も日常的に被害が増大し続けている情報リスク被害例としてコンピュータウィルスが挙げられる。被害が増え続けている理由として、コンピュータウィルスの感染経路が犯人の匿名性に覆われており、かつ誰にでも製作が可能であるということが考えられる。

しかし企業にとっては、製造が容易であってもコンピュータウィルスによって被る被害は想像以上に大きい。例を挙げると社内ネットワークを通じ、コンピュータウィルスが撒き散らされ、ウィルス除去に多大な時間と手間を要すといったことやオペレーションシステムの破壊によりホストコンピュータのハードディスクが損傷し、ネットワークが数日停止するといったことなどが該当する。これらのダメージ例は具体的な企業のコストダメージとして表面化するために、その対処策を素早く適応すれば企業の被害は拡大しなくてすむが、さらにはこれらの被害によってその企業のブランドイメージが低下するといったことや、信用が低下するといった具体的に数値化できない二次被害が発生することも十分に考えられる。むしろ情報リスクとはこのような二次被害を含めたものであるため、その対処策を的確にまた迅速に適応していかなければならない。

そのため、この項ではコンピュータウィルスの被害パターンを分類し、その特徴的な感染形態や、被害形態、具体的なダメージを考えていく。

そもそも被害と一言で言っても種類としては、「感染被害」・「増殖被害」・「混入被害」の三種類に分けることができる。

――コンピュータウィルスの被害パターン――

①感染被害とは、感染したマシン自体が被るデータの消去といった被害のことである。被害影響例としてマシン復旧中は、代替機の導入、バックアップデータからの復元等のコストが生じる。

②増殖被害とは、ウィルスが電子メール等を経由し、顧客等に伝わってしまう被害のことである。被害影響例として送信した企業が信用を落とすといったケースもあり、ブランドイメージが低下するといったダメージが生じる。

③混入被害とは、製品にウィルスが混入し、製品購入者に被害を与えてしまい、信用低下などを招く被害のことである。被害影響例として企業側としては購買者に注意を促すための謝罪広告費やウィルスが混入した製品の返品手続に伴うコストが別途発生する。さらには製品への評判が落ち、社会的イメージの低下というダメージも生じる。

以上のようにウィルスによる被害一つを取ってみても、その種類によって様々なダメージを企業は受けてしまう。そのため被害種類を特定パターンとして分類することにより、被害影響での損失補填や機器への復元コストの投資などを、より効率化することにより、的確で、かつ迅速な対処策を講じることができるのである。またその企業の情報セキュリティやリスク意識などへの弱点を発見すると同時に、情報セキュリティやネットワークシステムにさらなる補強も迅速に行うことができるのである。

――参考例　　2002 年のコンピュータウィルスによる被害事件――

・コンピュータを起動するたびに感染メールを大量に送信する「フレゼム」の亜種が流行。
・実行するとパソコンのハードディスク内のほぼ全部のデータが削除される「デリオール」の国内での感染が確認される。
・ある会社の社員を装い、ウィルスに感染したファイルをメールで建設会社に送りつけていた男が逮捕される。
・「Klez.E」ウィルスが蔓延。メールを閲覧しただけで感染し、毎月６日にデータを破壊する。
・インターネットのＨＰのアドレスを装ったウィルスが蔓延。添付されたファイルに掲示されたＨＰのアドレスをクリックすると、アドレス帳に登録されている全ての宛先に同じウィルスを送付する。
・経済産業省の外郭団体であるＩＰＡ（情報処理振興事業協会）は、01 年 12 月のコンピュータウィルスの届出件数が、1 ヵ月間としては 1990 年に統計を取り始めて最悪の 3,900 件になったと発表。

三井住友海上火災保険株式会社　　資料『情報処理業のリスクマップ』

（２）情報の改ざん被害

情報の改ざんによる被害影響例として企業ＨＰを改ざんされた場合、そのデータの修復、犯人の特定などの労力とコストが発生する。また二次被害としてその改ざん後の情報を信用したことにより顧客が被害を被った場合や重要個人データが不正に改ざんされたということでのブランドイメージ低下などが考えられる。

以上の視点から情報とは完全であって初めて存在価値が生じるものである。つまりより堅実に情報のインテグリティ（完全性）を保障し、より迅速に情報を収集し、さらにはニーズに見合った情報をより的確に提供することが、今後の企業活動には求められているのである。そのため、企業はデジタルデータを効率的に使用することにより、情報交換や加工を迅速に行うといったことや、単に一方向の情報発信だけでなく、ネット上での意見の交換など多様な情報のやりとりを可能にすることを実現したのである。

しかし「情報とは、完全であって初めて存在価値が生じるもの」であり、情報インテグリティの確保は絶対条件であるため、企業の提供する情報に欠落や誤りがある場合はそのものに情報価値があるどころか、企業や顧客に大きな被害やダメージを被ったり与えたりしかねないということがあり得るのである。さらには企業がデジタルデータを積極的に使用した結果、情報のインテグリティを脅かす要素である、情報の改ざんや流出が発生しやすくなるという危険性も同時に存在することも考慮しなければならない。

そのため、前項でのコンピュータウィルスの被害種類を大別したのと同様、企業情報インテグリティの不安要素を詳細に見分け、かつその対処法について効率よく考える目的として、情報の流れを段階別に分けて見ていくことにする。

――参考資料　　情報の完全性が失われる要素――

・情報の入手の段階…入手元の信頼性（専門業者、信用調査機関等）
　　情報の鮮度（情報の有効期限）
・情報の加工の段階…加工による情報の分割（一部分のみの場合等）
　　加工過程による情報の変化（電子情報が入手し易いため、加工される回数が増加し、本来の情報が変化する可能性）
・情報の移動の段階…情報の移動における盗聴
・情報の出力の段階…外部委託を利用した情報出力に関わる問題

『すぐわかる！情報リスクマネジメント』（Ｐ.41）

つまり情報の流れを「入手段階」・「加工段階」・「移動段階」・「出力段階」に分けることにより、その企業の問題点を洗い出すことが出来ると同時にその問題点を効率よく対処することが可能になるのである。

またさらに情報を確保するためには、その企業の内部体制の強化を外すことはできないであろう。そのためには情報管理体制・情報システム・業務プロセスのそれぞれの立場か

ら常に情報を検討することが必要になる。情報管理体制とは情報に関する責任者を明確化にし、情報システムにおいては技術的なセキュリティ対策を強化し、業務プロセスとは情報を取り扱う流れを明確化するということで、情報を異なった側面から捉えることができるようになるために、正確な情報を保持することができるのである。

最後に以上のように情報の完全性が失われる要素を段階別に踏まえ、企業の内部を考えていくことにより、企業のセキュリティの弱点や犯人の特定などをより迅速に発見・補強することができ、事件を阻止、または被害を最小限に抑えることができるのである。

――参考例　　改ざんによる被害事件――

・2002　警視庁が、他人のＨＰを勝手に書き換えるなどインターネット上の不正アクセスが急増していると警告。不正アクセスの認知件数は、01 年の 12 倍。

・2001　官庁や企業、自治体とさまざまな団体のＨＰが立て続けに改ざんされる事件が起こる。

三井住友海上火災保険株式会社　　資料『情報処理業のリスクマップ』

（３）情報漏洩被害

社会の情報化が進むことによって、情報漏洩のリスクは急増した。それは情報システムの急速な発展により、情報の交換や加工を迅速に行うことや、相互の意見交換など多様な情報のやりとりが可能になったことが、その利便性や急速な発展に反して様々な情報リスクを生み出したと考えられる。その理由として情報システムの発達による「複写可能」・「遠隔操作可能」・「法的整備の遅れ」の三点が挙げられる。

まず複写が可能であるために情報漏洩被害が拡大した理由として、電子データは全く同様のものを複写することが可能ということと、オリジナル情報においても変化がないため情報所有者が漏洩事実を気づきにくいということが挙げられる。

次に遠隔からの操作が可能であるため、ネットワークを経由して視界の範囲外での情報を盗み出すことが可能になったことが挙げられる。

最後に法的整備の遅れとは、電子データの価値が法律で定められていない場合、電子データとして格納されている情報の漏洩を法律で取り締まれないことが挙げられる。そのため電子データの価値とその漏洩後の企業へのリスクダメージのバランスとの違いにより、企業のセキュリティ意識と法律制度に大変な差が発生することになったのである。またその悪意の第三者である漏洩者だけでなく、漏洩発生の該当企業への具体的なペナルティが未熟であることも、その理由の一つとして考えられるであろう。

このようにして情報漏洩事件が発生するのだが、その発生原因と漏洩した情報は、様々な企業により異なってくる。その内容をまとめた資料として以下を参考にしたい。

――参考資料　　情報漏洩事件の主なパターン――

・人材派遣業者、サービス業、オンラインアンケートショッピングサイトで、従業員や業務委託先の悪意により、会員、顧客の個人情報、クレジットカード番号が盗み出され、インターネットで公開される。
・通信業、自治体で、従業員や業務委託先の悪意により顧客、住民の個人情報が盗み出され、販売される。
・オンラインアンケートで、第三者の不正アクセスにより、会員の個人情報が流出し、インターネットで公開される。
・インターネットプロバイダ、サーチエンジンで、ダウンロードした不正なプログラムにより、個人のＰＣからパスワードが流出する。
・大学で、第三者の不正アクセスにより、ユーザＩＤ、パスワードが流出し、インターネットで公開される。
・インターネットプロバイダ、仮想コミュニティサイトで、作業員の無知やミスにより、会員のパスワードが公開サーバや検索エンジンで一般へ公開される。
・インターネットプロバイダ、オンライン証券で、従業員の無知により、会員のメールアドレスが他の会員にメールで送信される。
・政府で、第三者の悪意により、ノートＰＣ上の機密データが、ノートＰＣごと盗難にあう。

『企業を守るセキュリティポリシーとリスク評価』（Ｐ.19）

以上の結果から見ても情報漏洩が発生した場合によって、様々なパターンが考えられる。業種ごとに原因が分かれ、漏洩した情報やその結果も多種多様である。中でも注目なのは、不正アクセスによるケースよりも、従業員や業務委託業者の悪意による情報漏洩のケースの方が原因として多いことである。また、インターネットプロバイダやコミュニティサイトなどの従業員の無知による事件も見逃すことができないであろう。

しかし全ての情報漏洩事件を通しての共通内容として、企業へのダメージが考えられる。その企業への被害影響例として、データの回収、犯人の特定などの労力、時間、コストなどの発生がまず挙げられる。さらに二次被害として、企業が社会的信用を落とすといったケースからブランドイメージが著しく低下するといったダメージや謝罪広告費、さらには情報資産としての損害賠償が発生することも十分に可能性がある。

――参考例　　2002 年の情報漏洩による被害事件――

・テレビ局が視聴者約 1,900 人のメールアドレスを、誤って外部に流出。
・地方自治体のＨＰから、自治体が運営する美術館の入場者など約 6,500 人の個人情報が流出。
・テレビ局のＨＰから、視聴者約 280 人の個人情報が流出。

・地方自治体のＨＰから、数名の個人情報が流出。
・私立大学のＨＰから、約 1,800 名の個人情報が流出。
・テレビ局関連会社のＨＰから、約 240 人の個人情報が流出。
・旅行会社のＨＰから、約 1,500 人の個人情報が流出。
・建材メーカーのＨＰから、約 45,000 人の個人情報が流出。
・エステティックサロンのＨＰから、約 50,000 人の個人情報が流出。

三井住友海上火災保険株式会社　　資料『情報処理業のリスクマップ』

参考例として 2002 年のみの情報漏洩被害例を列挙したが、非常に多くの事件が発生している。管理者の不注意から始まり、数名の個人情報から約 50,000 人の個人情報の流出までと幅広く起こっているが、やはりこれらは情報システムの発達とデジタルデータの利便性である遠隔操作と複写が可能であることと、未整備な法律制度が情報漏洩を助長しているのであろう。

しかしシステムや法律だけでなく、無論企業側の情報リスクへの管理意識とセキュリティ技術が未熟であることも否めないであろう。繰り返しになるが現在の様に今後も社会のＩＴ化が急速な勢いで進んでいくのであれば、情報漏洩問題は企業活動において大変な問題になっていくはずである。それは企業が経済競争の中で生き残るためには、他社との差別化を計る必要があり、いかに的確な情報を迅速、かつ大量に収めるかにかかっているからである。そのため現在の企業はまず情報漏洩の理由や原因をふまえ、自社の弱点を洗い出す必要があるだろう。

（４）情報リスクによる被害の可能性とその二次被害

第二章として「情報リスク」からの被害とその状況についてコンピュータウィルスの被害、企業情報の改ざん被害、企業情報の漏洩被害に的を絞り、順に考えてきた。

改めて情報リスクとその被害について列挙していくと、まず重複になるがコンピュータウィルスリスクによる被害では、マシン復旧中の代替機の導入やバックアップデータからの復元等のコスト発生、謝罪広告費やウィルスが混入した製品の返品手続に伴うコストの別途発生などが考えられる。情報改ざんリスクによる被害では、企業情報を改ざんされた場合、そのデータの修復、犯人の特定などの労力とコスト、同じく謝罪広告費などが発生する。情報漏洩リスクによる被害としてデータの回収、犯人の特定などの労力、時間、コスト、セキュリティ設備の見直しと再構築費などが発生する。他にも火災、落雷、地震などの天災によるコンピュータ損傷リスクのために、業務停止やサービスの提供延期に伴う企業ダメージも発生し得る。また企業側のオペレーションミスにより社内基幹システムが使用不可となり業務継続不能となるといった場合や、同じくオペレーションミスによる機密情報漏洩なども最近よく耳にする話題である。さらに細かい情報リスクとその被害例は

それこそ星の数ほど存在するが、今回本論文の問題点の一つである情報漏洩による被害の有無やその内容を考えるならば、「今後企業はいかに情報リスクによる一定のダメージを被る可能性が存在するか」、「常時企業に対して存在している状態で企業情報の流出被害の可能性から自社の重要情報を守れるか」が、今後の企業のポイントになっていくだろう。

その理由として現在における情報そのものの価値が、企業戦略上極めて重要な企業資産であるからだ。企業が経済競争の中で生き残るためには他社との差別化を計る必要性があり、そのためにはいかに的確な情報を迅速、かつ大量に収めるかにかかっているのである。また昨今における様々な情報システムによる事件が発生している背景からも改めて情報の資産価値の高さを伺うことも出来るであろう。

その情報の資産価値の中でも最も重要視され保護され得るべき情報は、個人情報と営業機密の二点である。まず企業のビジネスとして消費者や取引相手企業が信頼してくれなければ、商売を始めとした経済活動は成立しない。その企業ビジネスの基盤はシステムの安全性や情報保護対策に基づいた消費者の信頼によって構築していくのであろう。そのため個人情報の保護は企業活動の前提条件でもあり、必須条件なのである。次に企業のノウハウや新製品情報、企業戦略、業績、契約内容、ネットワーク情報などが営業機密に属する。さらに企業内での情報共有が進むほど情報漏洩のリスクが高まるのも現実であるが、これらの企業の原動力となる営業機密情報から企業価値や利益が生まれるため、絶対的に保護する必要性がある。

――参考例　　個人情報の定義（JIS Q 15001 の「3.定義」より引用）――

・個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号、画像若しくは音声により該当個人を識別できるもの。

『企業を守るセキュリティポリシーとリスク評価』（P.66）

しかし現実問題としてこれほどの重要な企業資産である情報の漏洩などの情報リスクによる被害が、発生していることを前項までに記してきた。今回はその情報リスクからの被害影響における二次被害を考えてみる。

前述した内容ではあるが情報リスクによる直接的な被害を簡単にまとめると、データの修復、労力とコストの発生が考えられる。さらにはそのときの企業から個人情報や営業機密が流出した情報漏洩事件による二次被害は、管理不徹底という信用低下に伴うブランドイメージの低下といったダメージが企業に発生する。また個人情報であればその情報価値に見合った損害賠償の発生可能性があり、漏洩した情報内容によっては悪用された場合の個人へのダメージは計り知れない。また外部からの不正アクセスによる漏洩なのか、内部犯行による漏洩なのか、はたまた従業員の無知やミスによる漏洩なのかという事実によってさらなる変化も考えられる。

――参考例　　情報漏洩による被害賠償問題――

・2000 年 5 月　京都府宇治市での住民情報流出事件が発生。宇治市の使用者責任を認め、慰謝料 1 人あたり 15,000 円の支払い判決。

三井住友海上火災保険株式会社　　資料『ネットセキュリティ総合保険　ホームページプランのご案内』

近年の情報漏洩による損害賠償代表例として、上の京都府宇治市の住民情報流出事件が挙げられる。流出情報内容として宇治市住民基本台帳のデータには約 19 万人分の氏名、住所、生年月日、世帯主名が記述されていた。この情報が光磁気ディスクによって持ち出され、名簿業者に 258,000 円で売却されたのである。その結果裁判所は宇治市の使用者責任を認め、被害者一人あたり 15,000 円の慰謝料支払いを国の決定とした。

この事件は現在の世間一般の個人情報価値への関心の低さと情報リスクの不透明性がはっきりと露呈したと思われる。なぜなら名簿業者はこれらの情報を 258,000 円で購入ということは、この金額を元手に利益を上げることが可能と判断したからである。そこで一人あたりの情報価値の原価は約 14,000 円前後になる。さらに被害者側からすると情報の資産価値の中でも最も重要視され、保護され得るべき情報である個人情報である上、名簿業者の悪用可能性や個人の機密情報の流出による精神的ダメージを考慮すると、被害者一人あたり 15,000 円の慰謝料金額は少なすぎるという意見が存在するのも十分にうなずける。しかし現時点では情報リスクの不透明性により、その後の二次被害などを含めると明確に数字化することができないのである。

だからこそ個人や企業は情報という資産価値に着目し、システム中心のセキュリティ対策にとどまらず、情報リスクは常時存在することを踏まえ、より効率化を目的としたマネジメントを実践していくことが現在の企業や個人には必要不可欠になっていくであろう。またこの京都府宇治市住民情報流出事件による 15,000 円という我が国初の県責任による慰謝料金額がコンピュータウィルスの被害、企業情報の改ざん被害、企業情報の漏洩被害といった情報リスク事故における損害賠償金額として、今後のベースとなるかどうかということも注目である。

第Ⅱ章　情報リスクへの対策手段

１．情報リスクに関する法律内容

1960 年代以降コンピュータ技術と通信技術が飛躍的に発展し、インターネット等による社会のネットワーク化が急速に進展した。その結果社会では情報量が増大し、その情報の

内容も様々な分野に広がっていった。

しかしその反面、急速な情報関連技術の発展に法制度等の整備が追いつかず、情報漏洩等の事件が数多く発生したことも今までに見てきた。

このような状況から近年情報自体の取り扱いについての問題意識は高まり、情報資産の保護に基づいた情報リスクへの対策手段の一つとして、法制度整備の必要性が求められてきたのである。

そのためこの項では現在日本において進められている法整備を見ていきたいと思う。

（１）個人情報保護基本法

「個人情報保護基本法」は、主に民間企業を対象に個人情報の利用制限や適正な収集、個人への利用目的の通知、適正な管理などを義務付ける法律である。現在は国会への提出延期などで施行時期が当初の予定より大幅に遅れを取っているが、この法律では罰則規定も盛り込まれる予定のため、施行後には情報漏洩などの被害に対して抑止効果が発生するとの期待を持たれている。

本法の制定目的としては高度情報通信社会の進展の下、個人情報（Ｐ.10　個人情報の定義参照）の流通や利用の増大に伴う個人情報の適正な取り扱いに関し、基本となる事項を定めることにより「個人情報の有用性に配慮しつつ、個人の権利利益を保護する」こととしている。

また上段でも述べたが、法案では「個人情報取扱事業者の義務等」において全二十二条にわたる事業者の義務を定め、違反した場合や義務違反改善勧告に従わなかった場合に科せられる懲役刑や罰金刑が「罰則」において定められている。ここでいう義務について簡単に説明すると、例えば個人情報を取り扱う事業者が個人情報を取得する際に取得する情報をどのような目的で利用するのか特定し、本人に公表・通知しなければいけないといったことや、個人情報取得後にも本人による情報開示・訂正・利用停止の依頼があれば必ず対応しなければいけないといったことが記述されている。

さらには、これらの義務を果たさなかった場合、その事業者には 6 ヶ月以下の懲役又は 30 万円以下の罰金が科せられることになる。

（２）電子署名および認証業務に関する法律

日本の情報化が遅れる原因として法的な一つの要因となる理由に、正式な契約書として電子媒体が認められていなかったことも挙げられる。高度情報通信社会が急速な勢いで進展しているにも関わらず、電子的な契約書では裁判上証拠とならないのであれば結果的に企業側は力を入れることができないことは明白である。

このような動きから 2001 年４月に施行された「電子署名および認証業務に関する法律」は

情報通信社会の新しい商取引のルールとして注目された。つまり本法は電子的な契約書でも紙による契約書と同様の効力を持たせる法律である。

従来の電子情報交換では通信傍受やデータ改ざんなどの可能性が示唆されていたが、同法に基づいて作られたシステムでは暗号技術によって不正防止を実現させている。使用する暗号技術は複数の方式から選択することが決められており、利用者の確認は主務大臣認定民間企業による特定認証業務として認定する方式がとられている。また対象は私文書であり、定義として本人性が確認できるものと非改ざん性が確認できるものが必要である。

しかし現段階では、本法の施行によって身の回りの環境が大きく変わったわけではなく、まだ電子証明書や電子署名が一般的に使われているとは言いがたい状況である。さらには電子証明書の互換性、対応アプリケーションの拡大といった基本的な部分、さらにコストの低下配慮といったクリアしなければならない課題が多々存在していることも事実である。

しかし情報通信社会として今後必要なルールである以上、本格的な検討や導入は今後の課題でもある。

（3）不正アクセス禁止法

2000 年 2 月 13 日に施行された「不正アクセス禁止法」は、変化の激しい情報技術分野において先端技術を駆使する新しい犯罪を視野に入れた法律である。

まず本法制定の背景には、一つ目として国内のコンピュータ犯罪の急増が挙げられる。以前までパソコン通信においてＩＤとパスワードを盗む行為そのものに対しては法的な罰則を設けることができなかったのである。また二つ目に情報化社会の進歩により、インターネットの商用利用が増加すると同じ様にネットの安全を脅かすトラブルが急増したことが考えられる。

次に本法の特徴を大別すると「不正アクセス行為の禁止」・「不正アクセス行為を助長する行為の禁止、処罰」・「アクセス管理者の防御措置」・「都道府県公安委員会による援助等」の以上の四つに分けることができる。

では順に見ていくことにする。

そもそも不正アクセス行為とは、アクセス制限する機能を持っているコンピュータを不正な手段でアクセスできる状態にする行為を指す。

まず「不正アクセス行為の禁止」として、第三条に不正アクセス行為の処罰される内容が書かれている。その該当行為として、他人のＩＤやパスワード、音声認識や網膜識別などの「識別符号」（『不正アクセス禁止法』第二条定義）を使用した不正アクセス行為がその内容にあたる。また識別符号を使用せず、コンピュータアクセス機能を利用せずに不正アクセスをする行為についても同様である。

次に「不正アクセス行為を助長する行為の禁止」として、第四条ではこの行為を禁止し、さらには処罰する内容が書かれている。その助長する行為とは識別符号による制御コンピ

ュータに対し、不正アクセスが可能目的で他人に識別符号を教えることをいう。ここでの注意点として金銭授受の存在なくしても処罰の対象となることである。

三つ目は「アクセス管理者の防御措置」として第五条に記述している。その内容はコンピュータ管理側にも不正アクセスに対して、防御することに努める義務を設けるということである。つまり第五条では具体的な措置内容に関して記述はないのだが、コンピュータ自体への防御措置やネットワークに対しての防御措置が相当するであろう。

最後の「都道府県公安委員会による援助等」としてその名の通りであるが、不正アクセス被害のコンピュータ管理者は援助を申し出ることが出来ると同時に、承認された場合は国から援助が行われるといった内容である。

また本法の罰則として､1年以下の懲役又は50万円以下の罰金が科せられることになる。

この本論文では、情報リスクに関する法律として個人情報保護基本法・電子署名および認証業務に関する法律・不正アクセス禁止法を取り上げた。

個人情報保護基本法のみ現段階では施行されていないが、民間企業を対象にした個人情報の適正な管理などを義務付ける法律内容であるため、個人情報の資産価値を今後は左右していくことになるだろう。つまり個人情報を委託する側として、最も必要不可欠な法律であるだろう。また受託する側の企業にとって罰則も存在するため、特に大きな影響を受けることになる。

電子署名および認証業務に関する法律は、新しい商取引のルールとして注目されている。未だ課題が多々存在していることも事実であるが、情報通信社会の急速な成長の中では企業にとって今後の顧客層拡大の重大な鍵になり得るだろう。

不正アクセス禁止法においては、検挙数を見た限りでは現在既に効果を挙げている。この法律制定はインターネット社会に向けた新しい第一歩となったのである。

以上の様に情報リスクに対する法の考えとして、個人情報においては委託する側と受託する側の双方に対して責任と正しい知識を各自持たさなければならないと同時に国家としての価値観を明確に打ち出す必要があるだろう。

２．システム中心のセキュリティ対策

そもそも世の全てのリスクに共通していることだが、情報リスクはテクノロジーと法律が噛み合わなければコントロールすることができない。さらにはその場の状況を加味し、企業や個人である個々が意識的にそれらを踏まえた上でマネジメントしていく必要がある。この項では情報リスク防止としてセキュリティテクノロジーの種類と内容について、検討していきたいと思う。

（1）ウィルス対策ソフト

いまやどの企業でも一度は被害にあったことがあると言っても過言ではない情報リスクとしてコンピュータウィルスが挙げられる。このコンピュータウィルスによる被害を防ぐ方法の一つとして、現在ではほぼ多くの企業が導入しているウィルス対策ソフトが必要不可欠になっている。

この爆発的な感染被害の背景にはインターネットの普及が考えられる。その以前までは主な感染経路はフロッピーディスクであり、一定した潜伏期間と物理的な感染経路が存在していた。しかしフロッピーディスクから電子メールへと感染経路が移行すると、ウィルス配布者の逃走時間が必要無くなり、感染と同時に発症するタイプが流行し、かつデジタルデータの発達による電子メールの大量送信に乗じて急速に被害が増大していった。

またインターネットの普及はウィルスの悪質化を助長したことも否めない。ウィルス作成者がウィルス作成プログラムをホームページで公開し、さらに他者がそのウィルスを改良し凶悪化していくという悪循環に陥っているのである。

次々とコンピュータウィルスが進化していくことに対して、対策ソフトも新しい技術で対抗している。例えば顧客から届けられた未確認のファイルやプログラムを自動解析するシステムを備えているソフトウェアなどが挙げられる。

さらに現在では消費者のニーズに応えて、ウィルス対策ソフトを供給するメーカーによる 24 時間体制でコンピュータウィルスへの被害を最小にする努力を行っているのである。

（2）ファイアウォール

そもそもファイアウォールとは、企業内ＬＡＮのような機密性の高いネットワークを外部のネットワークと接続する時に使用するシステムのことである。つまり悪意を持つ第三者によるサイバー攻撃から、機密性の高いネットワークを守る防火壁の役割を果たすシステムである。

そのファイアウォールの機能として複数のネットワークの間に設置することで互いに流れるデータをコントロールし、不当アクセスを防止することができるのだが、データコントロール方法として「経路制御」・「フィルタリング」の二種類に分けることができる。

――ファイアウォールの機能――

①経路制御とは、ファイアウォールを経由して送られるデータの送信元と送信先を判断してアクセスをコントロールすることである。つまり個別に設定することにより、経路を制御することで、社内の不特定なマシンに外部からアクセスすることを不可能にするということである。

②フィルタリングとは、経路制御で許可したマシンに対して、アクセス方法のサービス

内容である権限の上限を個別に設定することである。

またセキュリティ技術の一つであるファイアウォールにも多くの種類が存在する。大きく分類するとハードウェアとソフトウェアを組み合わせたファイアウォールと、ソフトウェアのみのファイアウォールに分けることができる。

ハードウェアとソフトウェアを組み合わせたファイアウォールはネットワークからの妨害を防ぐだけでなく、盗難や破壊といった物理的な接触にも対応できるようになっている。そのため改ざんの可能性やセキュリティホールが少ないという利点が考えられる。しかしその欠点として高価であり、代替機が必要ということがある。

一方ソフトウェアのみのファイアウォールは商用ソフトウェアタイプとフリーソフトウェアに分類できる。商用ソフトウェアの利点として操作性に優れており、バージョンアップが容易であることが挙げられる。欠点としては物理的接触による攻撃とハードウェアに関して別途考慮する必要があるということが考えられる。フリーソフトウェアではソースプログラムが無料で使用することができるため、自社のセキュリティ事情に合わせたカスタマイズが可能という利点がある。しかし無料であるためにサポート機能はなく、ソースプログラムがオープン化しているために常時セキュリティ情報に注意を払わなければならないということが欠点として考えられる。

またその反面として、ファイアウォールでは防御しきれない攻撃も存在する。例を挙げるとアクセス権限が与えられている電子メールといったサービスを経由して侵入した攻撃に対しては、制御することができないことである。そのため他のセキュリティ技術と組み合わせることも必要になってくるのである。

（３）侵入検知システム「ＩＤＳ」

ＩＤＳ（Intrusion Detection System）とは外部ネットワークからの不正なアクセスに備えて、侵入を検知する製品のことである。ＩＤＳにもファイアウォールと同様に専用のハードウェアからソフトウェアまで様々なタイプが存在する。

そのＩＤＳが侵入を検知する仕組みを見ると、まずネットワークに接続されたＩＤＳがネットワーク上に流れるパケットを監視するスキャンを始め、得られたパケットを侵入パターンと比較し、一致した場合や不可解なデータを照合していくのである。そして侵入と確認するとその情報をログファイルに記録し、ＩＤＳ設定にしたがってシステム管理者や別のシステムに通知するのである。ここで注意することとして、基本的にＩＤＳの役割として侵入者に対してアクセスを切断するようなコンピュータそのものを守る機能を備えているわけではないことを忘れてはならないのである。

続いてＩＤＳの構成機能と種類について分類すると「ホスト型」・「ネットワーク型」・「複合型」の三つのタイプに大別することができる。

――ＩＤＳの種類の分類――

①ホスト型ＩＤＳは、外部からの侵入を防ぐ全マシンにインストールすることで、直接マシンへの侵入を検知するタイプである。ホスト型ＩＤＳは主に、システムのエラーログ、イベントログを監視するツールとして利用されている。

②ネットワーク型ＩＤＳは、ログを消されるリスクを回避するようにしたＩＤＳである。ネットワーク型は同一ネットワーク内のマシンをすべて含めて、ネットワークをスキャンするのである。ネットワーク型の設置箇所は、マシン間を超えて侵入されないよう監視する目的で、インターネットと社内ＬＡＮとの間や部署間に設置されるのである。

③複合型ＩＤＳは、ホスト型ＩＤＳとネットワーク型ＩＤＳの双方の利点を取り入れた、現在最も多く販売されているタイプである。

――参考資料　　ＩＤＳを構成する機能――

○スキャン機能

ネットワークを監視し、パケット（データの塊）を取り出す。ネットワーク回線が太くなり、大量のデータが流れるようになると、安価なＩＤＳではパケットの取りこぼしが発生する。スキャン機能はネットワークのモニタリング（監視）とも呼ばれる。

○解析機能

スキャンされたデータを解析して、データの送受信先、時刻、データサイズなどを解析する。会席機能はＩＤＳによって異なる。

○ルールＤＢ

解析機能によって取り出された情報をＩＤＳが持っている侵入パターンと比較して侵入か否か判断する。この侵入パターンをルールＤＢと呼び、シグネーチャと呼ばれることもある。

○通知機能

ＩＤＳが不正侵入と判断した時、画面にメッセージを出す、電子メールを送信してシステム管理者に通知する他、他のアプリケーションへ指示を出す。ＩＤＳによっては、特定のファイアウォールと連携して侵入を防止することができる。

○ログ機能

ＩＤＳが検知した侵入を証拠として残すために、日時、送受信先、侵入方法、などをファイルやイベントログに出力する。ＩＤＳは未知の攻撃分析するためにも、ログ機能は大切。

○制御部

起動、中断、停止、ルールＤＢの更新、ログファイルの切り替え等の制御を行う。

『すぐわかる！情報リスクマネジメント』（Ｐ.41）

しかしＩＤＳにおいても問題点も多数存在している。そもそも技術的に発展途上であるため、異なったベンダー間で互換性がないという点もその一つである。また知名度が低いという点も見逃せない。しかしウィルス対策ソフトやファイアウォールなどのセキュリティ技術と併用することによって、今後さらに重要性は増していくだろう。

（４）その他のセキュリティ技術

その他にも様々なセキュリティ技術が存在する。ここではさらにセキュリティ監視・監査ツールと電子署名について簡単に挙げていく。

まずセキュリティ監視・監査ツールとはセキュリティ対策に特化した機能を持つ専門のツールである。現在の情報システムの複雑化に対応していくためには、システムに備わっている管理機能だけでは困難になっているというニーズから誕生したのである。その監視ツールは 24 時間常時稼動してシステムのリソースを最小に抑えるということや、安全性の確保を重視するように作られており、セキュリティの脆弱性を調査する監視ツールは最新のセキュリティ情報を搭載することによって、最新の攻撃手法から防御する方法をアドバイスしてくれるのである。

またネットワーク監視ツールの他に、マシンのＣＰＵ稼動、リソースを監視するツール、アプリケーションのライセンス監視ツール、コンテンツの監視ツールなどが存在している。これらはそれぞれのシステムの脆弱性を発見するということや、さらには個々の弱点を補うといった目的で幅広く導入され始めているのである。

次に電子署名であるが現在既に多くの企業が電子商取引を取り入れ、大幅なコストダウンを実現している。しかし同時に多くの問題点も存在している。その根底にある問題点として、相手を確認できないということと証拠が残らないという二点が考えられる。この問題点を解決すべく注目されているのが「電子署名」である。電子署名とは現実社会で利用される判子、サインに相当する効力を電子的にも実現させる技術のことで、ネットワーク上の交渉にも法的効果をもたせようとしているのである。

以上の他にも様々なセキュリティ技術が存在するが、企業がどの程度の情報セキュリティ対策を行っているかは事業や提供サービスによって千差万別である。今後ＩＴ関連技術が発達していくことは明白であるためコストやスキル、その他全ての問題で、情報リスクとのバランスを取っていくことが重要になっていくだろう。

３．情報リスクへの総合的な対策手段

今までに見てきたように、多くの情報リスクが存在し、多くのセキュリティ技術対策方

法や法制度整備の必要性が高まってきたが、情報リスクを始めとした存在リスクに対してはテクノロジーと法律が噛み合わなければコントロールすることができない。さらにはその場の状況を加味し、企業や個人である個々が情報資産の保護に基づいた情報リスクへの対策手段の一つとして、組織的・継続的なマネジメントを行うことが必要になっていくだろう。そもそも情報リスクを踏まえたリスクという存在を完全に無くすことができない中で、企業が最大のリターン（利益）を確保しつつ、リスクを最小限に抑えるようにコントロールすることが今後の企業活動に必要不可欠なのである。

次項から今までの情報リスクやセキュリティ技術、ＩＴへの法律内容を踏まえた上で効率的なマネジメントとして「情報リスクマネジメント」の内容や方向性を検討していく。

第Ⅲ章　情報リスクマネジメントの内容と形態

1．情報リスクマネジメントの概要

そもそも情報リスクマネジメントの概念としては企業を脅かす情報リスクをトータルで捉え、多岐にわたる対策や手段を効果的・効率的に組み立てることである。リスクという存在を認める中で目的がリスクを無くすことではなく、情報リスクをコントロールするということに焦点を当てることによって、情報リスクを最小限に抑えた上でそのリスクをビジネスで必要不可欠なものとして取り入れるようになるのである。

（1）情報リスクマネジメントのメリット

情報資産を保有している以上、必ず情報リスクは存在する。しかも個人と違い、企業に至っては個人情報と営業機密の二点を保持しており、特に前者は顧客との信用関係によって構築されていった情報資産である。そのため情報漏洩等の問題を起こした場合、企業に与えるダメージは計り知れない。そうした状態で経営側の立場から、継続的に情報リスクを把握（リスクモニタリング）し、適切な経営判断（リスクテイクやリスク回避）や対策（リスクコントロール）を実施することが必要になっていくのである。

また情報リスクをマネジメントしていくことによって、企業にとって様々なメリットが生じていく。その内容は次の四点に大別することができる。

――情報リスクマネジメントによる企業のメリット――

①情報システムや情報資産を効果的に管理できる点

②リスクを数値化して把握することで、判断材料となる点

③トラブル発生時に、素早い対外的な応対ができる点

④新分野への参入調査に対して、能率の良い調査を行える点

以上の様にまずセキュリティの視点から資産を分類する。それに応じた企業の情報資産を効果的に管理することができ、同時にリスク分析を行うことによってリスク脅威を数値化することができる。そのためリスク値削減コストと処理結果の利潤の関係を明確に把握でき、効率的な投資を行えるのである。また企業に対してリスクが顕在化した場合、ダメージへの対処、情報収集、分析、決定などの仕事を明確化することで迅速な応対が可能となることや、既存の業務外での分野に対しても同様に仕事を明確化することによってリスク内容の把握を行えるようになるのである。

（２）情報リスクマネジメントの立場別役割

情報リスクを回避する手段はコンピュータウィルス対策や、マシン故障に備えてのバックアップデータを常時保存するなどという、個別の手段を取ることも必要である。しかし企業経営側が個々のリスクや対策手段だけに着目していては、幅広い情報リスクの脅威を防ぐことができないであろう。つまり企業内部のそれぞれ立場から企業を脅かす情報リスクを幅広い観点から把握し、効果的な対策を選択していかなければならないということである。

ここでは企業内部の「部門」ごとに、情報リスクマネジメントにおいて「やるべき内容」と「具体的な作業」の一例を挙げ、検討していきたいと思う。まず経営者層のやるべき内容としてＩＴ統治であり、その具体的な作業としてＩＴ投資事業戦略やシステムの統合などが考えられる。つまり具体的なセキュリティ等に焦点を絞るのではなく、その企業の方向性を導き出す役割を担うのである。次に情報システム部門管理職のやるべき内容こそ、第一にセキュリティ管理である。その具体的な作業として情報分析やシステムの企画･設計および人員整理などが必要になるだろう。またシステム管理者での行う事項としては、無論セキュリティ対策を構築することであろう。具体的な作業は前述したように、バックアップ、ウィルス対策やライセンス管理などがそれにあたる。

以上の様に情報リスクマネジメントにおいて、どの分野にどのようなリスクが存在しているかをいかに迅速に分析し、いかに迅速に対処することが求められる。そのためにはそれぞれの立場や役職に見合った判断や対策を行うことが必要不可欠なのである。

２．情報リスクマネジメントの方法とその内容

情報リスクマネジメントにおいてはいくつかの方法が存在する中で、トータルでリスクをコントロールするには色々なマネジメント手法を企業規模や目的に応じて、総合的に組み合わせる必要がある。そこでこの項では情報リスクマネジメントの代表的な方法とその

内容について検討していく。

（１）情報資産評価

企業が自社の情報資産を情報リスクから守るためには、自社の情報資産について正確に知ることが大切である。なぜなら情報資産価値や情報システムの運用状況を踏まえておくと、企業の対策が安全水準に達していることを常時チェックすることが出来るようになるからである。しかし情報資産価値によってＩＴの価値を正確に把握することができなければ、価値のないものを高コストで守るという非効率なセキュリティ対策をとらなければならなくなる。

そこで情報資産評価を的確に行うためには、まず情報資産というものを分類することが必要になる。その情報として挙げられるのが、個人データに該当する顧客データや取引先データと営業機密である設計図面や特許、経理情報、資料などである。同時にパーソナルコンピュータやネットワークケーブル、ルータ、プリンタなどのハードウェアや、ＯＳやソフトなどのソフトウェアなども情報資産として含まれるであろう。また電話や建物自体の設備も情報資産が発生し得ると考えられる。

次に以上の情報資産に対して、正確にその価値を評価することが求められる。そのためには情報資産を監査し、情報システムの状態を公正・中立に評価をする「情報システム監査」にて、信頼性・安全性・効率性の観点から問題点を発見・指摘して改善をしていくのである。

（２）情報セキュリティ

自社の情報資産の価値を情報資産評価によって把握すると同時に、それに対する脅威を洗い出した上で、セキュリティ方針や対策を選択することがマネジメントとして求められる。つまり現時点での自社のセキュリティ能力を把握することによって、情報リスクに対する脆弱性を見出すことができるのである。そのための手段の一つとして「ペネトレーションテスト」という診断方法が代表的である。

ペレトレーションテストとは、外部から情報システムに対して擬似的に攻撃する立場で情報システムを診断することである。この診断手順として顧客の同意・情報収集・サービスチェックを踏まえた上で、システムへ擬似攻撃を試しみる。その結果を報告書にまとめ、企業運営側の今後の方針を仰ぐという結論を導くのである。

また情報セキュリティの種類やその対策としては、前項（Ⅱ.情報リスクへの対策手段２.システム中心のセキュリティ対策）にて取り上げてきた。電子認証システムやファイアウォールなどの情報セキュリティもそのニーズに見合ったマネジメントをしていかなければならない。

（３）災害復旧･業務継続計画

企業にとって避けることが出来ないリスクが顕在化した場合に対して、企業は業務を継続するために備える必要がある。つまり地震や落雷、火災等の災害に備えるために情報リスクマネジメントでは、事前に「災害復旧計画」・「業務継続計画」を作成し、常時リスクに備えておくべきである。

その災害復旧・業務継続計画とは災害時に業務を元の状態に戻す計画と災害発生時において業務を継続するための計画の双方を指す。具体的には従業員の生存確保から、復旧に必要な人員、宿泊施設などの確保や復旧手順などを検討するということである。また企業内の部門別、担当別などの責任の相違点からも業務継続計画を用意しておくことも必要であろう。災害時復旧計画を整備するには多くの確認事項が存在すると同時にあらゆるリスクを想定し、対策を考えなければならない。

つまり企業の情報資産を堅持するためには、情報リスクのみに対策を講じるだけではなく、多角化したリスクに対して視野を広げていなければならないのである。

（４）情報価値管理

実際に企業においては必要なセキュリティに有意義な投資を行うことや、自社の情報資産を的確に把握をすることがマネジメントの土台であろう。同時に緊急事態に備えた費用の有効な運用も必要であることも前述した。

しかし企業というものは常に経済活動によって利潤を発生させていかなければ会社規模を維持できない。そのため急速に成長していく情報通信社会に対しても、セキュリティ対策を含めて的確な投資をしていかなければならない。また企業の情報戦略に基づいた投資を行わなければ、効率に結びつかないこともあり得る。このように投資価値を見極めることもマネジメントの一つであり、情報投資対象をどのように選択するかという考え方を「情報価値管理（Information Value Management）」という。

この情報価値管理を実施するための代表例としてバランススコアカードという手法が存在する。これは費用対効果を「コスト」・「顧客」・「プロセス」・「教育・成長」という四つの視点から投資の妥当性を評価する方法である。

第一にコストの視点から考える。例えるならセキュリティ対策にもコストがかかるが、対策を怠った場合の企業へのダメージと差し引いた場合、無論対策を維持すべきであるためコスト面において投資する価値があると言えるのである。

第二に顧客の視点から考える。セキュリティ対策が不完全であった場合のリスクにおいては、顧客においても企業においても被害を与えかねないため投資をしなければならないであろう。

第三にプロセスに対する影響を考える。新しく投資を行った場合に従業員の作業量増加について検討するのだが、新システムを導入することによって、研修などのコストや時間が当然必要になる。何日も業務を離れなければ習得し得ない新システムから数時間のガイダンスで終了する企画も存在する。現在の企業活動において、重度の支障を期さず、かつ先見的に利用できる投資を行わなければならないであろう。

第四に教育・成長の視点から考える。この投資を行うことで社員は知識や技能のレベルを向上することが出来るかどうかといったことや、その教育において企業の今後の経済活動に効果を発揮することが出来るかどうかということを検討するのである。

以上四つの視点から検討をすることで費用対効果を明確に測定することができ、企業にとっての必要性を調べることができるのである。さらに情報価値管理は情報システムの拡張に伴う投資の判断材料のみならず、事業の安全な縮小対策や拡大指標においても有効な手法として注目されるのである。

この項の最初で述べた通り、情報リスクマネジメントとはトータルでリスクをコントロールする目的で、色々なマネジメント手法を企業規模や方針に応じて総合的に組み合わせて結論を導き出すものである。つまり第一段階として自社の情報資産の価値や中身を客観的に評価して全体像を的確に把握することによって、第二段階の情報セキュリティを種類や能力に応じた効率的な対策を講ずることができるようになる。そして第三段階として企業にとって避けることが出来ない緊急事態などのリスクが顕在化した場合に対して、業務を継続するために安全を保障した必要内容を備えると同時に、無駄が生じないための効率的な運営が必要になる。ここまでの段階では企業活動においての最低限存在するリスクに対する準備であり、その後の経済活動に対するリスクを考慮すると、第四段階として今後の必要とされる投資を見極めるために情報価値管理を行うのである。以上の様に段階的に必要・不必要、効率的・非効率的などという観点から、企業に存在する情報リスクを減少させると同時に、常時リスクが顕在化しないためにコントロールを行うことを情報リスクマネジメントというのである。

しかし情報リスクマネジメントの立場別役割として前述した通り、企業としての目的が情報リスクマネジメントであっても企業での役割において仕事内容が変わってくる。その役職や部門ごとに応じた仕事とは、企業方針に基づいた統括的な仕事の一つである必要がある。そのため全ての従業員に企業のマネジメント方針を把握させる必要が生じてくるのである。これが次項のセキュリティポリシーなのである。

３．情報リスクマネジメントの運用形態

前項では主に情報リスクマネジメントにおけるマネジメントの種類や内容に焦点をあてたが、次にどの程度のセキュリティを確保するのか、そのために誰が何をするのかといっ

た情報リスクに対する企業としての方針が必要になってくる。これを「セキュリティポリシー」と言い、経営責任者の承認印のある企業としての正式な文書のことである。つまり情報リスクマネジメントを行うには、まずセキュリティポリシーを適切に策定していくことから始めるのである。

（1）セキュリティポリシーの策定

企業や組織の情報資産を守るために方針を示したものであるセキュリティポリシーの策定によって得られる効果やその策定意義とは何なのであろうか。

――参考資料　　セキュリティポリシー策定の意義――

意義	目的
1.経営者の意思表示	効果的なセキュリティ対策の実施
2.従業員のセキュリティ意識の統一	
3.情報資産の統一的な取り扱い	
4.セキュリティ製品導入の際の指針	
5.取引相手、顧客へのセキュリティ対策の開示	外部からの信用を得る
6.情報漏洩の立証	
7.インターネット保険への加入	

『企業を守るセキュリティポリシーとリスク評価』（P.122）

またセキュリティポリシーの策定によって得られる効果として、以下の資料を参考にしたい。

――参考資料　　セキュリティポリシーの策定効果――

□セキュリティポリシーを策定する過程で得られる効果

・セキュリティ組織の創設（ポリシー策定メンバーからセキュリティ対策実行組織へ）
・社内情報システムの整理（システム、アプリケーション利用状況、ライセンス等の管理）
・セキュリティトラブルの情報収集（ウィルス、電子メールトラブル、停電、機器の故障）
・リスク分析（無形資産、有形資産の洗い出し）
・業務の優先順位（業務遂行する上で優先するサービス、人員体制など）
・責任者の明確化

□セキュリティポリシーの策定によって得られる効果

・定期的なセキュリティ対策（トラブル報告、セキュリティ監査など）
・計画的なセキュリティ投資

・顧客、取引先への信頼性向上
・情報共有する関連会社と連携したセキュリティ維持体制
・新システム構築時にセキュリティ対策を反映
・従業員のセキュリティ意識向上、情報システムへの理解度向上

『すぐわかる！情報リスクマネジメント』（P.89）

参考資料から分かるようにセキュリティポリシーを施行すると、企業の方針として経営者による意思表明を行い、その方針に従業員が的確に従事する必要がある。また情報資産への取り扱いを含めた意識の向上やセキュリティ対策の効率的な導入、機密情報の明確性を公表できるために情報漏洩などの被害についても立証手段として考えられるようになる。また損害保険会社がその企業のセキュリティレベルを判断することにも役立つのである。

以上の様にセキュリティポリシーを策定し、実行することによってセキュリティ対策にも効果的であると同時に、外部からの信用を得ることにもつながるのである。

またセキュリティポリシーとは企業や組織の情報資産を守るために方針を示したものであるため、明文化した上で管理される。その構成として「セキュリティ基本ポリシー（基本方針）」・「セキュリティスタンダード（対策基準）」・「セキュリティプロシジャ（実施手順）」の三段階によって成り立っている。

基本ポリシーでは経営者の情報セキュリティに対する意思を示すもので、顧客や株主などに公開するものである。内容は 1 ページ程度で簡潔に記述したもので今後の方針の根底になるものである。

セキュリティスタンダードはセキュリティ基本ポリシーである基本方針に基づいて作成するもので、セキュリティを確保するための具体的な対策を 20 ページから 50 ページ程度にまとめて記述するものである。

セキュリティプロシジャはセキュリティスタンダードに基づいて作成するもので、システムや部門、管理者、利用者に分け、実際の運用や利用手順を詳細に明記するものである。

以上の三段階を踏まえた上で実行することにより、効率的なマネジメントを実践するための予定書を作成することができるのである。

（2）セキュリティポリシーの策定のステップ

つまり充実したセキュリティポリシーに基づいた役割ごとに的確な対策を行うことで、情報リスクマネジメントを実行でき、この情報社会の中で企業は経済活動をより安全に、より効率的にリスクに対応できるようになるのである。言い換えれば企業方針であるセキュリティポリシーが企業にとってそれだけ重要であると同時に、現状を的確に把握した上でポリシーを策定しない場合においてはセキュリティの効果を十分に得られない可能性も考えられる。

そのためセキュリティポリシーを「情報収集・資産分類」・「リスク分析、目標設定とセキュリティポリシーの策定」・「セキュリティポリシーの実施」・「セキュリティポリシーのモニタリング」という次の五段階のステップに分けて作成していくのである。

○ステップ１　「情報収集・資産分類」

まず企業が守るべき対象を正確に把握する必要がある。そこで企業の情報資産の情報収集とその分類によって、セキュリティで管理するべき対象範囲を定めるのである。次にその情報の価値や機密性に基づいてセキュリティレベルを三段階程度で設定する。例を挙げると管理者以上のみがアクセスできる情報、社内限定の情報、社外に公開できる情報といった様に分類するのである。同時にその情報資産の価値に応じたセキュリティ対策を施すといった管理も重要である。

このように情報資産に対する情報収集を行って資産を分類することによって、企業の情報資産が明確に把握することができる。その中でどの資産が大切であり、優先してセキュリティを講じるかという問題が明らかになるのである。

○ステップ２　「リスク分析」

企業にとって守る必要の高い情報資産を把握した後に、重要なことはその情報資産を脅かす情報リスクについて分析することである。このリスク分析において必要不可欠なポイントが三点ある。その第一に、分析する対象と範囲を明確にすることである。その第二に、セキュリティポリシーを策定する目的に合わせて、リスクを分析することである。その第三に、リスク分析の結果をセキュリティポリシーに反映させることである。つまり分析対象や範囲を絞り、セキュリティポリシーの目的に応じたリスク分析を行った結果を反映させるということである。

そのリスク分析の流れとしては、情報漏洩の洗い出しから情報の属性を明確化する情報資産分析から始める。次に多角的な視点からの脅威の洗い出しする脅威分析を行う。続いて企業の脆弱性分析や経営における重要性分析を、それぞれほぼ同時期に行う。そして揃えた分析結果に基づいた総合的なリスク分析を行うのである。

その結果自社のリスク分析による報告内容から、リスク分析報告書が作成される。この報告書に基づいて次のセキュリティポリシー策定の段階に進むのである。

○ステップ３　「目標設定とセキュリティポリシーの策定」

自社の守るべき情報資産とそれに被害を与える可能性のある情報リスクを分析し、双方共を把握することによってセキュリティポリシーを策定することができるようになるのである。つまり自社の情報資産とそのリスクを踏まえた上で具体的なセキュリティの目標を設定し、全社で統一するための明文化することをセキュリティポリシーの策定という。

リスク分析報告書による内容から企業はセキュリティポリシーの対象範囲を決定する。

例えば会社全体に対して行う一括的なマネジメントなのか、特別なシステム部門のセキュリティシステムを向上させるためのマネジメントなのかという観点により、対策内容が変わってくるからである。

その対象範囲を決定すると次に目標という具体的な内容を設定することができる。この具体的なセキュリティ管理策こそが完成したセキュリティポリシーなのである。つまりコンピュータウィルスというリスクは発生頻度と分析結果による被害影響度がともに高いために、ワクチンソフトの導入というセキュリティ対策を講じた結果、目標被害影響度を減少させるという会社の指針を打ち出すということである。

○ステップ４　「セキュリティポリシーの実施」

情報資産を把握し、そこに存在するリスクを分析した結果、セキュリティ対策を強化するという具体的な方針を企業が決定することをセキュリティポリシーの策定と言う。この時にもっとも重要事項の一つとしてその企業関係者全員に確実に認識させ、企業の方針として意思統一を行うことが挙げられる。そうした企業全体が一体となる体制を構築しなければ効果は得られないのである。

○ステップ５　「セキュリティポリシーのモニタリング」

最後に自社のセキュリティポリシーの策定内容とその実施方法に対して、問題点や不足点が存在しないかという視点から運用状況を確認するために、モニタリング（監視）を行うのである。

以上の五段階に基づいてセキュリティポリシーの運用が可能になるのである。つまり最初に自社の情報資産価値を正確に把握し、被害を被る可能性のある情報リスクを詳細に分析し、その分析結果によるハイリスクな箇所や脆弱なシステムをどのように強化していくかという具体的な企業の目標を定める。この目標をセキュリティポリシーと呼ぶのである。またその実施にあたり会社全体の従業員に対して、目標結果への意思統一を強化し、そのセキュリティポリシーの基づいた進行状況を常時確認しながら運用していくのである。

（３）情報リスクマネジメントの今後の必要性

私は「人・物・金」という時代は既に終わったと考えている。序論において前述したが、現在社会の情報化が急速な勢いで進んでおり、それに伴って企業のワークスタイルはこの 10 年で格段の変化を遂げている。その顕著な例として情報技術は企業にとって経営戦略の実現や日常業務の遂行において、今では必要不可欠なものになっていることが挙げられる。そのため消費者ニーズの把握をはじめとした、企業における個人情報の重要性はますます高まる傾向にあると同時に、情報は企業戦略上極めて利用価値の高い情報資産であること

が十分に考えられる。このことから見ても「人・物・金」の時代から、「人・物・金・情報」の時代にシフトする過渡期であると考えている。

こうした背景から他社との差別化を図るためにも、その企業の情報資産の質と量が鍵を握るのではないだろうか。つまりその企業資産である情報を、いかに効率よく保持していくことができるか、また運用していくことができるかということが求められているのである。そのニーズに応えるべく注目されているのが、本論分の主題である情報リスクマネジメントである。

この情報リスクマネジメントの目的は重要視されている情報に対するリスクをいかに安全で効率的に抑えた上で、いかにその情報資産を企業の運営に効率的に利用できるかということである。そのためには自社の情報資産の価値を正確に評価し、同時に存在し得るリスクに備えたセキュリティシステムの導入や会社の具体的方針であるセキュリティポリシーの策定に基づいて情報を保持していくことが求められる。また同時進行として企業の絶対条件である非常事態に備える準備やコスト・顧客・期間・効果などの複数の視点から検討していく必要もあるだろう。その結果により企業にとって最低のセキュリティ対策コストで最高の利潤をもたらすという、効率的なマネジメントを実践することができるようになるのである。

つまり今後の情報化社会の向上とともに企業活動においても情報の有無が重要性を増す中で、いかに効率的な情報リスクマネジメントを迅速に行うかどうかが今後の企業の方向性を決定づける重大な要因となるであろう。

第Ⅳ章　情報リスクへの損害保険業界としての対応

1．損害保険業界の情報通信分野への取り組み

（1）企業活動と情報リスク

本論分において情報リスクの種類やその被害、また様々なセキュリティ技術やシステムを検討してきた。そしてこれらを元に全体的に統括したマネジメントが企業活動において重要であると述べた。しかし企業活動を行うにあたり、他にもリスクが存在するのではないだろうか。また企業活動を行うからこそ発生するリスクも考えられるのではないだろうか。

その答えとして情報通信技術の発達による急激なネットワークの成長性やその利便性の裏側に存在し得るハッカーなどによる情報漏洩などの情報リスクは無論企業としては危惧するべき問題であるが、他にもコンピュータの発展に伴ったシステム依存の現在のオフィス環境にもリスク発生あるいはリスク拡大の様々な要因が考えられるのである。

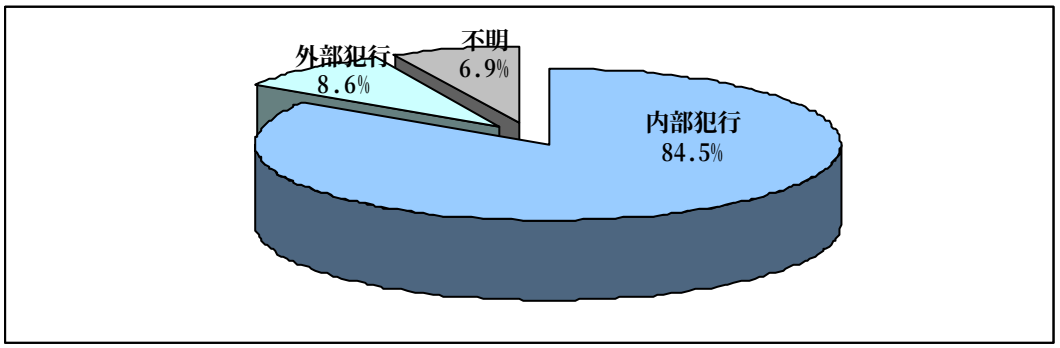
その第一の理由として、コンピュータの利便性が高まったことによるシステム依存度の

上昇リスクの拡大が挙げられる。第二に、コンピュータの存在が日常に溶け込むことによってリスク認識の低下を招いたことが挙げられる。第三に、コンピュータの使用が誰にでも使うことができるようになったという視点から、事務専門職の減少や分業処理による事務知識の低下のためにリスク拡大したことが挙げられる。つまり企業の大幅なコンピュータ導入による運営の効率化は、日常業務の処理能力の急激な成長を保障すると同時に企業の内外に問わない情報リスクを発生させる原因になったのである。

そこで企業内における情報リスクの代表的例として、情報漏洩などを含めたコンピュータ犯罪の内部・外部犯行別内訳を参考例として取り上げたい。一般的にコンピュータ犯罪のリスク可能性が考えられるのは、第一に職務上接する機会がある従業員、第二に職務上接する機会のない従業員、第三にアウトサイダーの三者に分けられるであろう。損害保険業界の日本興亜損害保険株式会社の調査によると、対象の半分以上がアウトサイダーと答える状況にあるという調査報告を発表した。しかし同社の以下のグラフ結果から分かるように圧倒的に内部犯行が比重を占めているのである。この結果一つ見ても情報提供者である個人、情報利用者である企業ともに情報リスクとそのセキュリティに対しての意識が低いことが見て取れる。

つまり三章で取り上げた企業のセキュリティ対策方針であるセキュリティポリシーにおいては、外部脅威と内部犯行の双方に対処する必要がある。また企業活動を行うにあたり情報リスクへのマネジメントが求められると同時に、企業は情報利用者との意識から責任と自覚を今以上に持つことが望まれる。

――参考例　　コンピュータ犯罪の内部・外部犯行別内訳――



日本興亜損害保険株式会社　　資料『リスクレビュー　オフィス・コンピュータの環境リスクを考える』

（２）損害保険業界各社の情報戦略

そもそも「リスク」とは偶然な事故により損失が発生する可能性や不確実性という意味である。現在では至る所に拡散するリスクから身を守る合理的な方法として、損害保険が存

在する。この損害保険は将来発生し得る可能性のあるリスクに備えており、経済的な損失を最小限に止めるための手段と言えるだろう。そのため万人が助け合いの精神のもとに、損害保険各社が代表して資金を徴収しているのである。だからこそ損害保険各社において、消費者や取引相手企業が信頼してくれなければ成立し得ないし、その信頼の基盤としてシステムの安全性や情報保護対策の充実に基づいた経営が必要なのである。

その一方で信頼の下で資金を運用している損害保険業界において、情報リスクの存在は無視できない存在である。その情報リスクによる被害を簡単にまとめるとデータの修復、労力とコストの発生という一次被害や、その企業から個人情報や営業機密が流出した情報漏洩事件による二次被害がその情報リスクにあたる。この二次被害とは管理不徹底という信用低下に伴うブランドイメージ低下といった企業へのダメージや、損害賠償の発生可能性、漏洩した情報内容によっては悪用された場合の個人や企業へのダメージなどが考えられる。特に二次被害の企業へのダメージは計り知れないため、企業においては無視できないのである。

その反面、情報は企業戦略上極めて重要な企業資産であることは明白であり、損害保険各社が経済競争の中で生き残るためには、他社との差別化を計る必要性があるためいかに的確な情報を迅速、かつ大量に収めるかがポイントになるだろう。

つまり顧客の信頼から成立している損害保険各社は、顧客や自社の営業機密などの情報資産を安全に保持すると同時に、経済競争を勝ち抜くために与えられた情報資産を常に利用していかなければならないだろう。そのため現在相反する両極の立場にある損害保険業界としては独自の情報戦略に取り組むことが課題になっている。そこでこの本論文では、損害保険各社が情報リスクを含めた情報戦略にどのように取り組んでいるか検討していく。

○東京海上火災保険株式会社の情報戦略

次世代ＩＴ基盤の強化として、契約管理システムの拡大化を促している。特に携帯電話でのコンテンツサービスは業界に先駆けて開始している。その内容は保険商品の紹介、資料請求や代理店紹介に加え、リスクソリューション分野を活かしたゲームや相談サービスも行っている。また対法人への情報戦略として、最も力を入れているのがリスクマネジメントコンサルティングである。そのため同社は 1996 年に完全子会社である東京海上リスクコンサルティング株式会社を設立している。この設立により多方面での専門分野で得た知識を活かすことができ、実践的で効果の高いリスク対策を実施することができるようになったのである。中でも他企業の情報リスクマネジメントやリスク評価、その企業にあったセキュリティポリシーの策定や検査までも行っている。これは情報化の変化に常に対応し、自社の情報リスクの評価や分析を的確に行っている証拠でもある。

リスクの専門的立場を利用し、他企業の情報リスクに対してもマネジメントサービスを実施している背景には、業界に先駆けて情報リスクに対し、最も早くから注目をしていたことが見て取れる。

○三井住友海上火災保険株式会社の情報戦略

インターネットを利用した保険販売やサービス提供の強化など、情報通信技術の戦略的活用を推進している。特に代理店業務のさらなる効率化を目指し、代理店と会社を結ぶパソコンネットワーク「代理店ＭＳ１」の拡大に力を注いでいる。つまり、ネットワーク基盤の強化により、代理店との業務の迅速化やサービスレベルの底上げに力を入れている。

また情報リスクにおいては、三井住友海上グループ「株式会社インターリスク総研」によるリスクマネジメントを行っている。株式会社インターリスク総研では、総合シンクタンク兼トータルコンサルティングを本分としているため、災害・環境・ＩＴなど企業・個人の各種リスクに関する調査研究の受託と総合的なリスクコンサルティング業務を行っている。つまり情報通信を含めた多様化するリスクに関して専門的に対応し、かつサービスを行うために子会社として設立したのである。こうしたことで親会社の情報リスクマネジメントを率先して行う場合に内部の守秘義務が守られ、客観性を保ちつつリスク評価を行えるという、他社によるマネジメントコンサルティング実行時よりもメリットが二点発生するのである。

消費者用の情報戦略において他社との差別化が少なく、今後自社の方向性を明確に提示する必要性があるであろう。しかしリスクマネジメントサービスやリスクソリューションサービスにおいてはグループ全体での取り組みを行っており、対法人向けの情報戦略には力を入れているという特色を持っている。

○日本興亜損害保険株式会社の情報戦略

情報通信技術の活用機能の発展により、将来の環境変化や事業拡大に柔軟かつ迅速に対応可能な時期システムの基盤の構築を目指している。具体的には次世代代理店システムの構築を想定したネットワーク基盤の強化・整備に力を入れている。国内初めてＨＰによる保険加入を可能にした株式会社損害保険ジャパンと日本興亜損害保険株式会社とあいおい損害保険株式会社の三社共同による「ＡＢＣシステム（Agent Business Cooperative System）」という次世代Ｗｅｂ型代理店システムを開発している。その内容としてＷｅｂ技術の採用により、契約データなどをサーバ上に展開し、高速なレスポンス・操作性を保証し、インターネット接続環境を用意するだけで業務を始めることができる初期導入の簡易性を実現ということである。また「安心 My.com」という個人用のサイトを設け、会社や保険情報を常時送るというサービスも開始している。

情報戦略は基本的に個人消費者用として新規格のサービスを始めているのは特徴的であるが、リスクソリューションという立場での情報戦略には力を発揮していないのが現状であろう。

損害保険業界の各社の情報戦略から急激な情報化に対応するために、次世代ＩＴ基盤の

設立を目的としていることが垣間見ることが出来た。特に営業業務から次世代契約管理システムや次世代代理店システムの構築、損害調査サービスの迅速化を想定したネットワーク基盤の強化・整備に共通して取り組んでいることが分かる。またインターネットを活用したサービス提供のレベルを向上することも一つの課題として取り組んでいる。

２．現在の情報関連リスクに対応している保険商品とその比較

（１）東京海上火災保険株式会社の保険商品

東京海上火災保険株式会社は、企業の情報化に関わるリスクに対応した専用商品として「e-クリック（e-リスク保険)」を 2002 年 12 月に発売した。

――参考例　　e-クリック――

○e-クリックに加入いただけるのは、売上高 200 億円以下で、対象外業種に該当しない企業となります。(対象外業種：ネット関連業・情報サービス業・金融業)

・火災・落雷、不正アクセス、コンピュータウィルス感染等の偶然な事故
＜基本補償＞コンピュータ等（除くリース機器)・通信用回線等の情報機器の記録媒体・記憶媒体に記憶されている情報（データ・プログラム・ソフトウェア）の消失
⇒修復・再作成費用
・偶然な事由によるコンピュータネットワークの停止
＜売上減少・営業継続費用特約＞売上減少・営業継続費用
・コンピュータネットワークを使用した営業活動
＜賠償責任特約＞顧客・取引先等の
・業務停止による経済的損失
・プライバシーの侵害
・名誉・信用の毀損
・データの消失
による賠償責任損害

東京海上火災保険株式会社　　資料『e-クリックのご案内』

（２）三井住友海上火災保険株式会社の保険商品

三井住友海上火災保険株式会社は、現在情報関連に対応している保険として「ネットガード」という新商品を開発している。そのため現時点では補償内容等は分からないのだが、前対応商品である「ネットセキュリティ総合保険」を見る限りでは、軽過失による情報漏洩での損害賠償責任の損害や、同様に第三者による情報漏洩での損害賠償責任の損害に対応していた法人向けの保険であった。またコンピュータのソフトウェアやハードウェアに

関して対応している商品も別に存在していたが、今後はこの双方を合わせた保険として「ネットガード」が発売されるだろう。

（３）日本興亜損害保険株式会社の保険商品

日本興亜損害保険株式会社による、情報システムを包括的に補償する商品として「e-Pa-So-Co-N 保険（コンピュータ総合保険)」が発売されている。

――参考例　　e-Pa-So-Co-N 保険（コンピュータ総合保険）――

○契約対象

・パソコン本体、サーバ機器、周辺機器、その他システム設備

・記憶媒体、データプログラム

・ネットワークの事故による喪失利益（オプション）

○契約内容

・ハードウェアの修理費･再購入費の補償。

・代替機のレンタル費･リース費の補償。

・データプログラムの修復、再入力費用の補償

・喪失利益の補償（通信回線、電気供給ネットワークが中断し、阻害されたことにより生じた損失分）

日本興亜損害保険株式会社　　資料『e-Pa-So-Co-N 保険』

（４）大手三社の情報リスク対応保険商品の比較

まず日本興亜損害保険株式会社の商品である「e-Pa-So-Co-N 保険」は、補償内容もコンピュータやデータといった、被害が発生した場合顕在化するリスクのみの対応商品である。本論分で扱ってきた内容で表現すると一次被害と同様である。つまり情報漏洩を起こした場合に、顧客からの損害賠償責任による損害額や企業業務が停止した場合の売上減少額などを補償することはできないということである。またその逆として、この保険の長所として考えられることは保険加入対象に制限を設けていないことである。

次に三井住友海上火災保険株式会社においては、情報リスク対応保険に関して新装販売するため一端販売が休止しているが、このことこそ現在の情報化社会を象徴している。社会の情報化が進むに連れて情報リスクもより複雑化していく。そのため企業を取り巻く環境も大幅に変化していくからこそ、現在存在するリスクに対応するために新たな保険が必要になってくるのである。

最後に東京海上火災保険株式会社の商品として「e-クリック（e-リスク保険)」を見ていく。現在考えられる保険商品の中では最も新しく、充実した内容であることは間違いない。

現段階では保険加入対象や損害賠償責任の損害額の双方に上限があるのだが、今後情報漏洩に関して損害賠償金額の一定の流れが決まれば、この上限もなくなることだろう。

３．今後の損害保険業界の情報分野の発展方向

現段階において損保業界全体が情報リスクに対しての一次被害については対応保険商品つくられているが、二次被害以降の問題には着手していない企業の方が多いのが現状である。私はそれには二点の大きな理由が存在すると考えている。第一の理由として、被害額や流出経路、商品価値が発生するか否かという次元での研究結果が明確に出されていないことが挙げられる。つまり急激な情報通信技術の進歩に、法整備の遅れやセキュリティ技術などの社会環境が追いついていないのである。第二に、損害保険業界として「被保険利益」による安定した利潤の確保が現在では難しいということが挙げられる。要はこれも被害額や流出経路が不透明であることが根底にあるのだが、例えば情報漏洩問題の損害賠償責任金額の判例が少なすぎることなどが二つ目の理由の要因になっている。

しかし今後も情報化の波は止まることはないであろう。そのため自社の情報資産を堅持しつつ、いかに企業活動に利用するかが企業の成長の鍵になるはずだ。無論情報を利用すればするほど脅威は比例して増していくため、情報の提供者である消費者は情報資産の価値に対して意識を高めなければならないし、情報の利用側は責任と義務に基づいて利用していかなければならない。そうした状況の中で、自社グループとしてリスクコンサルティングを専門的に扱う会社を損害保険各社が設立することにより、詳細な情報リスク分析から多岐にわたる対応策や発展策を生み出すことができるであろう。なぜなら情報リスクには二次被害という大きなリスクが存在しており、さらにはその補償を求めているニーズがあることも確かだからだ。

結論

情報とはそもそも何なのだろうか。

『広辞苑』では「①あることがらについてのしらせ。②判断を下したり行動を起こしたりするために必要な、種々の媒体を介しての知識」とある。人間においても、企業においても、色々な目的を持って行動している。それらの目的を達成するためには十分な知識である情報が必要不可欠である。本論文の後半にて記述した内容だが、私は「人・物・金」の時代から「人・物・金・情報」の時代に変革していると考えている。人間においては、国内過去最大の不景気であり、海外情勢に至っては戦争が再度行われる可能性すらある。企業においては、世界的な不況状態であり、国内・海外問わず深刻な経済状態の中での企

業活動を余儀なくされている。こうした中で人間はより充実した人生を、企業は常に成長し続けるという目的を持って行動しているのである。そして何よりその目的を達成するために必要なものが「情報」なのだ。だからこそ個人情報や企業の営業機密といった情報資産を大切にしなければならないと、私は思う。

現代の情報通信技術の進歩は、人々の生活から企業のワークスタイルまで様々な変化をもたらした。自社をより成長させたいと考える企業にとっては、情報化による情報収集の効率化は他社との差別化を図るには願ってもないチャンスであったろう。しかし顧客のニーズを逸早く押さえることができる情報資産は、企業拡大化の原動力となり得ると同時に、多くのリスクを併せ持つことは本論文で検討してきた通りだ。ウィルス被害や改ざん被害、さらには情報漏洩被害の事件は後を絶たないという事実からもいかに多くのリスクが存在しているか見ることができる。特に情報漏洩を起こした企業へのダメージは想像以上に大きいものだ。また誤って企業から送信されたウィルスにより顧客のコンピュータが停止する可能性だって考えられるし、改ざんされた企業の情報を信用したことによって発生する顧客の被害も侮れないであろう。つまり企業にとって大きなメリットである情報にも、巨大なデメリットである情報リスクが存在するのである。この情報リスクが顕在化した後では企業活動において莫大な損害を与えかねないであろう。だからこそこの情報リスクを企業ごとにコントロールするために、情報リスクマネジメントが必要になるのである。

しかし目に見えない情報リスクを企業ごとに対処しても、完全に把握しているか疑問が残る。そのためセキュリティポリシーという企業のセキュリティ対策方針を示した公式文書の内容が問われるのである。セキュリティポリシーとは本論文でも取り上げたセキュリティ技術導入を行うといったセキュリティ対策と従業員の意識の底上げや育成方法を組み合わせて構成していくものである。企業はこのセキュリティポリシーに基づいて情報リスクマネジメントを行うのである。

だが、どんなにリスクをマネジメントしたところで情報を利用している間はリスクをなくすことはできないのである。そのため企業側に過失がない場合においても情報漏洩問題等が発生する可能性があるのだ。だからこそ法律や環境の整備が早急に求められるのだが、同時に情報提供者も企業に対して全面的に委任するのではなく、自己管理や情報価値への意識の向上も同様に必要になる。この結論内の初めに記述したが、私は情報提供者の意識が甘すぎると思う。確かに法整備の遅れは問題である。であるが企業は営利目的による活動を行っているわけで、利潤を発生させるために情報を十分に活用する。勿論企業の管理能力とその責任も重大だがリスクは必ず発生してしまうのだからこそ、個人がさらに情報資産に興味を持ち、しっかりと管理しなければならなくなるであろう。

ここで私は以下の二点が今後の損害保険業界の差別化につながるのではないかと考えている。第一に、企業はどんな効率的な情報リスクマネジメントを行ったとしてもリスクを消滅させることができないため、企業は常時情報リスクの脅威に脅かされていなければならないこと。第二に、情報漏洩問題などに対する国家の対策の遅れから、今後は個人が情

報資産に興味を持ち、しっかりと管理しなければならない時代が来ることがその理由になるだろう。以上の二点から情報リスクに対して、個人・法人ともに自らの責任で対応しなければならない時代に成りつつあるが、情報リスクの被害は個人のみならず企業一社では負担しきれるレベルではないことが分かる。そのためこの情報リスクに対応していく商品へのニーズは今後急速に高まっていくと言えるのである。

しかし現段階において、損保業界全体が情報リスクの被害影響例を加味した対応保険商品がつくられていない。私見ではあるが、その理由に二点の大きな問題点が存在すると前述した。以下重複になるが第一の理由として、被害額や流出経路、商品価値が発生するか否かという次元での研究結果が明確に出されていないことが挙げられる。つまり急激な情報通信技術の進歩に法整備の遅れやセキュリティ技術などの社会環境が追いついていないのである。第二に、損害保険業界として「被保険利益」による安定した利潤の確保が現在では難しいということが挙げられる。要はこれも被害額や流出経路が不透明であることが根底にあるのだが、例えば情報漏洩問題の損害賠償責任金額の判例が少なすぎることなどが二つ目の理由の要因になっている。

逆に非保険利益の問題点さえクリアすれば、次期に必ず情報リスクに幅広く対応する保険商品が開発されるだろう。なぜなら国家政策に消費者が満足していない上、現在の損害保険各社の自動車保険を初めとした商品が既に飽和状態にあるからだ。ここ数年の損害保険業界の収入は全体の半分が自動車保険による売上である。しかし主要マーケットである自動車保険の成長率は伸び悩んでいるのが現状である。それに比べＩＴ化が謳われているにも関わらず、旅行保険や積立保険、ＩＴ関連保険を含めた新種保険の全体のシェアは 10%にも満たないのである。

現実に情報リスクの問題はいまや社会問題の一つである。それにも関わらず、法律や情報リスクを取り巻く環境は、目まぐるしく変化する情報化に対応しきれていないとも言われている。しかし複雑化する情報リスクに対し、多くの注目が集まっているのであれば飽和状態である損害保険業界において、情報リスクは大きなチャンスにもなり得ると、私は考えている。

「人」が「物」・「金」そして「情報」を正しく使用すればこその充実した人生であり、目に見えないリスクから身を守る手段の一つとして、損害保険が存在するのである。

以上

―――【参考文献】
著：古川泰弘
『すぐわかる！情報リスクマネジメント』　／かんき出版

著：株式会社オーエスケイ
『これで作れる情報セキュリティポリシー』　／ローカス

著：塚田孝則（日立ソフトウェアエンジニアリング株式会社）
『企業を守るセキュリティポリシーとリスク評価』　／日経ＢＰ社

著：小野覚
『金融リスクマネジメント』　／東洋経済新報社

監修：松田晃一　著：峰岸和弘・舟木春仁
『ｅセキュリティ』　／ダイヤモンド社

著：小泉修
『図解でわかるＷｅｂ技術のすべて』　／日本実業出版社

監修：赤堀侃司
『標準パソコン用語辞典』　／秀和システム出版編集部

社団法人　日本損害保険協会
『損害保険募集人教育テキスト』

三井住友海上火災保険株式会社
『三井住友海上の現状　2002』

―――【参考資料】
東京海上火災保険株式会社　　各種資料
『情報リスクマネジメントサービスのご案内』
『ｅ-リスク保険　ｅ-クリックのご案内』
『別紙　Ｅ－Ｒisk 対策保険』

日本興亜損害保険株式会社　　各種資料

『e-Pa-So-Co-N 保険（コンピュータ総合保険）』

『Ｒisk　Review』

『リスクインフォメーション』

三井住友海上火災保険株式会社　各種資料

『ネットセキュリティ総合保険　ホームページプランのご案内』

『ＮＥＴガード PRO のご案内』

『IT（情報技術）事業者賠償責任保険の特長』

『IT 関連事業者をとりまくリスク』

『ＲＭ　トピックス』

『情報処理業のリスクマップ』

株式会社インターリスク総研

『ネットセキュリティ情報』