ＩＴの活用と情報セキュリティ対策について

産業観光局産業戦略部産業政策課

近年のIT（情報技術）の進歩と低価格化に伴い，経営にITを利用する企業が増えてきました。自社でITシステムを導入し，経営・組織情報の管理，インターネットによる情報発信，ビッグデータの収集・分析を行ったり，さらに進んだIT活用形態として，自社でITシステムを保有せず，インターネットを介して外部のサーバやシステム・ソフトを使用できるクラウドサービスを利用するなど，ITを活用して経営を効率化し，ビジネス拡大につなげていくことが企業の競争力を高める上で必要不可欠となっています。

一方で，ITの活用は様々な危険性も併せ持っています。情報システムの停止による損失，顧客情報の漏洩や不適切な情報発信による企業のブランドイメージの失墜など情報システムに関連する事故は，自社のみならず取引先や顧客などの関係者へも波及します。また，スパイ行為などによって流出した先端技術が，テロや軍事用途に転用される恐れもあります。

また，オリンピック開催国においては，サイバー攻撃の増加が懸念されることから，2020年の東京オリンピック開催に向けて情報セキュリティ対策の強化が喫緊の課題となっており，国においては，政府機関や電力会社，金融機関など重要インフラをサイバー攻撃から守るための「サイバーセキュリティ基本法」が平成26年11月６日に成立しました。

このような状況の下，企業経営において，情報セキュリティに対するリスクマネジメントは重要な課題のひとつと考え，ITの導入と併せて，情報セキュリティ対策をしっかりと行うことが必要です。今回は，企業における情報セキュリティに係る主要な被害の例と，その対策を紹介します。

１．セキュリティ対策不足による被害の例

情報セキュリティに関わる事故には，様々な要因があります。ここでは，代表的な被害例を紹介します。

（１）ウイルスへの感染

ウイルス感染は以下で紹介するさまざまなトラブルの原因になります。ウイルスに感染したパソコンなど情報セキュリティ対策の不十分な機器を保有，使用することで，結果的に他者に損害を与えてしまい，社会的な非難や損害賠償請求を受ける可能性もあります。

近年，標的型攻撃（※）に代表される非常に巧妙な手段によるウイルス感染が急増しており，これまで以上の注意が必要です。

※　標的型攻撃

特定の組織を狙ったサイバー攻撃のこと。攻撃者は，標的とした組織の従業員にコンピューターウイルスを添付したメールを送信し，“言葉巧み”にウイルスを実行させる。

具体的には，メールの送信者や件名などを偽装するとともに，添付したウイルスを有用なファイルに見せかける。

（2）システムの停止

ウイルス感染，人的ミス，自然災害などにより社内の基幹システムが停止すると，データの毀損のみならず，最悪の場合，業務自体が停止してしまうこともあります。その間に顧客を奪われ，販売機会を失うことになるかもしれません。

（3）機密情報，個人情報の漏洩

機密情報や個人情報の漏洩には，ウイルス感染や外部からの不正アクセスなど情報システムを介したもの，社員による不正な情報の持ち出し，記録媒体の紛失，飲食店やタクシーでの会話やトイレでの立ち話といった人為的なものなど，さまざまな原因があります。また，結果的に情報漏洩にならなくても，社員が興味本位で個人情報を閲覧したことで，企業のブランドイメージが大きく毀損するケースもあります。

近年の個人情報保護に対する関心の高まりと相まって，個人情報を流出させてしまった場合，賠償や訴訟などの大きな問題にまで発展することがあり，顧客離れや多額の賠償金の支払いなどで，経営に大きな影響が出る可能性があります。

（4）ホームページやデータの改ざん

ホームページやサーバ内のデータを不正に改ざんされることは，企業活動に影響を及ぼすだけでなく，企業イメージの毀損にもつながります。さらに，ウイルスを埋め込まれてしまった場合には，ホームページの閲覧者に感染を拡大させてしまうこともあります。

これらのことは，企業としてのセキュリティ対策不足を露呈し，取引相手の信頼を失い，取引停止などにつながる可能性もあります。

（5）ソーシャルメディアへの不適切な投稿

ツイッターやフェイスブックに代表されるソーシャルメディアの爆発的な普及を受けて，アルバイト店員等が店内で悪ふざけを行う様子をツイッターなどに投稿することで，当該店舗の社会的イメージが大きく毀損した例が頻発しています。このような行為は，店舗のイメージダウンだけでなく，返金や商品の返品・交換及び消毒といった金銭的負担や，最悪の場合，店舗の閉店など巨額の損害が発生する可能性もあります。

2．企業で取り組んでいただきたい対策

このように情報セキュリティに係る被害には様々なものがあり，必要な情報セキュリティ対策も多様です。それでは，組織の限られた経営資源の中で最大限の対策効果を上げるためには，どうしたら良いのでしょうか。

以下では，組織としてとるべき対策，情報管理担当者がとるべき対策，職員一人ひとりが取り組むべき対策例について紹介します。

（1）組織としてとるべき対策

まずは，組織としてあらかじめ情報セキュリティポリシー（情報セキュリティ対策の方針や行動指針）を定めることが必要です。

その上で，すべての職員に教育を行い，情報セキュリティポリシーに沿った行動を意識付けすることが必要です。組織の実態や社会の変化に合わせた定期的な情報セキュリティポリシー

の見直しも必要です。

こうした情報セキュリティポリシーの策定から実際の運用・改善までを含めた活動全体を，情報セキュリティマネジメントといいます。企業経営者や幹部は，情報セキュリティマネジメントを確実に実行していくとともに，自社の情報システムの停止がどの程度許容されるのかを考慮した上で，情報セキュリティ対策への投資の必要性や規模を適切に判断していくことが必要です。

（2）情報管理担当者がとるべき対策

情報管理担当者は，情報セキュリティポリシーで定めた事項が組織全体で実際に実行されるように，社員への教育・監督を適切に行う必要があります。常に新しい脅威についての情報を収集し，必要に応じて組織幹部や外部の専門家とも連携しながら，継続的に組織全体の情報セキュリティ体制を見直していくことが必要です。

表　情報管理担当者が行う対策の例

対　策	例
技術的対策	ファイアウォール、侵入検知システム(IDS)、ウイルス対策システム、認証システムなど
物理的対策	防犯対策、入退管理、セキュリティワイヤーによる盗難防止など
人的対策	規程や手順書などのルール、従業員教育など

①　技術的対策

ウイルス対策などアプリケーションの適切な運用，導入している情報システムへの最新の修正プログラムの適用，Webサイトへの不正アクセスや改ざん対策，通信データの暗号化，システムや重要な情報へのアクセス管理（ID・パスワード設定，アクセス制限設定），ファイアウォールの導入などインターネット接続に関わる不正アクセス対策，無線LANのセキュリティ対策といった，情報システムや通信ネットワークの運用管理を行うことが必要です。このような運用管理を行える技術者が社内にいない場合，外部のシステム監査人に指導・監督を委託することも必要です。

また，自社で情報システムを保有せずにクラウドサービスを活用することで，情報セキュリティからの脅威を回避するとともに，経営効率化も図ることができます。ただし，クラウドサービスを利用する際は，事業者側の障害やメンテナンスなどによる利用の停止や，保存しているデータの消失といったリスクも考慮しておく必要があります。

②　物理的対策

情報を保管・使用する場所への入退管理，モバイルパソコンやUSBメモリなどの外部記憶媒体の管理・盗難紛失対策，他地域へのサーバ設置やデータセンターの活用による地震・水害への対策といった，物理的な対策を行うことが必要です。

③　人的対策

契約や業務委託における情報の取扱や社員の守秘義務を明確に規定するため，情報セキュリティポリシーに準拠した情報セキュリティルールを整備することが必要です。さらに，そのルールを職員に周知するだけでなく，実践するために必要な教育を定期的に行っていくなどの人的な対策を行うことが必要です。

また，企業が保有する高度な技術は常に外部

から狙われているということを，社員一人ひとりに自覚させることが必要です。

（3）社員・職員一人ひとりが取るべき対策

企業や組織においては，たった一人の不注意がウイルス感染や情報漏洩といった脅威につながることもあります。社員一人ひとりが，情報セキュリティ対策の必要性を十分に理解し，自覚をもって取り組むことが必要です。

3．企業の情報セキュリティ対策を支援する行政の取組

（1）「京（みやこ）サイバー犯罪対策協議会」の取組

京都府警察では，インターネット利用者の規範意識・防犯意識を醸成し，サイバー空間における安全・安心を確保するため，「京（みやこ）サイバー犯罪対策協議会」を設置しています。

産業界を始め，行政機関，教育機関等が緊密に連携して，インターネットの安全利用や日々進化するサイバー犯罪の被害防止等に関して情報交換や協議・検討をしています。

（2）「モノづくりプリザーブ」

企業が保有する伝統産業技術や先端技術をスパイ行為から守るため，京都の行政機関，産業界，約800社の先端技術保有企業等で構成する情報保全ネットワーク「モノづくりプリザーブ」を設置しています。府警の「京（みやこ）すぐメール」を活用した双方向型の情報ネットワークを構築し，サイバー攻撃やスパイ行為に係る情報提供・交換，注意喚起，助言等を行っています。

（3）京都高度技術研究所の取組

京都高度技術研究所（ASTEM）では，中小企業のクラウドコンピューティングの導入を支援することにより，企業競争力の強化を支えています。それに併せて，データベース等の活用を安全かつ積極的に推進していくための事業継続計画（BCP）の策定支援や，ITコンソーシアム京都と連携し，企業経営に必要な情報セキュリティ対策などのセミナーを開催しています。

参考資料

以下のホームページ等をもとに，京都市産業観光局が作成

1）「国民のための情報セキュリティサイト」（総務省）http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html
2）京都府警察のサイバー犯罪対策のホームページ
http://www.pref.kyoto.jp/fukei/anzen/cyber/index.html
3）中小企業における組織的な情報セキュリティ対策ガイドライン（独立行政法人情報処理推進機構）
4）公益財団法人京都高度技術研究所のホームページ
http://www.astem.or.jp/business/ict