Risk Solution
News Today
No.19 2010/12/08

【ニュースに関するお問い合わせ】
銀泉リスクソリューションズ㈱
E-mail/ solutions@ginsen-risk.com
〒102-0074 東京都千代田区九段南3-9-14
TEL03-5226-2301 FAX03-5226-2609
〈メールマガジンでもお送りしています。ご希望の方は上記まで〉

## 情報漏洩 ― 貴方の会社は大丈夫ですか？

ウィキリークスによる米国国務省の機密事項漏洩が世界的問題となっているが、日本でも警視庁外事課の国際テロ関連情報の漏洩事件が先ごろ明らかになり、単なる流出ではなく意図的に誰かが秘密資料を漏洩し公開していた可能性が高いという。この件は、外国メディアでも取り上げられ、日本政府への信頼を大きく揺るがし、国益にも大きなダメージを与える事件となった。加えて、尖閣列島における中国漁船と海上保安庁の船の衝突を撮影していたビデオの公開を、外交上の配慮から政府が拒否していたにも拘わらず、海上保安庁の保安官によりインターネット上に公開され日本国民だけでなく全世界にあまねく知れ渡るところとなり、国会で政府としての失態および情報管理の甘さが指摘され、民主党政権の危機感の弱さが露呈する結果となっていることは皆さんも既承の通り。

民間でも、M社の社員が使用していたパソコンがウィルスに感染し、M社が請け負っていた原子力発電所の点検報告書や機密情報がWinnyを通じて流出した事件があった。 M社では、社内ネットワークについて、Winnyを利用したデータの送受信が行えない仕組みを設けており、更にデータの社外への持ち出しを原則禁止していたにも拘わらず、当該社員は報告書などのデータを外付けHDDにコピーして社外に持ち出し、自宅で個人的に使用しているパソコンに接続して作業を行っていたため、このパソコンがウィルスに感染し、データがWinnyを通じて流出したものであることが判明した。

ここ数年、日本では個人情報や企業情報の漏洩事件が多数発生している。実際、内閣府の調査によると、公表されているだけでも企業の17.5%が何らかの個人情報や企業情報の漏洩もしくは毀損を経験しているという。一昔前の産業スパイから、インターネットの普及後での情報漏洩事件は、外部の人間がシステムに不正な手段で侵入し情報を持ち出すという所謂不正アクセスが多くなってきていると思われがちだが、実際にはその原因の約8割は、メールや記録メディアを使った持ち出し、紙資料をコピーしての持ち出しなど、従業員や外注業者など内部の人間による盗難、流出であり、内部要因と言われている。外部要因に関しては、M社のように企業の側でも、ハッキング防止のためのファイアウォールや不正侵入検知システムなどの導入、外部からの訪問者の出入りを制限するためのIDカード採用、警備員の配慮など、既に実施されている企業も多いのではないでしょうか。

〈漏えい元・漏えいした者：平成19年度〉

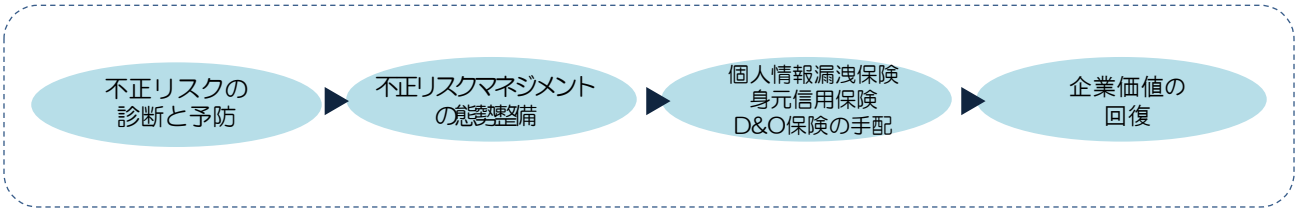
| 漏洩者 | 従　業　者 | | | | 第　三　者 | | | | その他 | 不明 | 合計 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 漏洩元 | 意図的 | 不注意 | 不明 | 計 | 意図的 | 不注意 | 不明 | 計 | | | |
| 事業者 | 6<br>0.7% | 517<br>61.0% | 32<br>3.8% | 555<br>65.4% | 43<br>5.1% | 1<br>0.1% | 12<br>1.4% | 56<br>6.6% | 23<br>2.7% | 13<br>1.5% | 647<br>76.3% |
| 委託先 | 4<br>0.5% | 113<br>13.3% | 14<br>1.7% | 131<br>15.4% | 23<br>2.7% | 5<br>0.6% | 1<br>0.1% | 29<br>3.4% | 15<br>1.8% | 5<br>0.6% | 180<br>21.2% |
| 不明 | - | - | - | - | - | - | - | - | - | 21<br>2.5% | 21<br>2.5% |
| 合計 | 10<br>1.2% | 630<br>74.3% | 46<br>5.4% | 686<br>80.9% | 66<br>7.8% | 6<br>0.7% | 13<br>1.5% | 85<br>10.0% | 38<br>4.5% | 39<br>4.6% | 848<br>100% |

出典：平成20年度　「個人情報の保護に関する法律施行状況の概要」平成21年11月消費者庁　参考資料より

**〈企業に必要とされる リスクコントロール〉**

1. 情報漏洩の原因が企業内部にあることを、経営者自身が認識すること。
2. 内部要因による漏洩を防ぐ対策に、経営者から従業員まで全社を挙げて取り組むこと。
3. 内部漏洩の原因経路を理解し、そのすべてに必要な対策を講じること。

〈不正リスクに対する最も有効な手段〉




**企業の社会的価値の確立・維持・向上**

情報漏洩によって企業は、被害者への損害賠償、謝罪費用、調査費用といったコスト面だけでなく、企業としての信頼やブランドイメージの低下など、企業への影響は計り知れず大きな損害を被ります。では、情報漏洩について、保険ではどこまで対応出来るのであろうか。個人情報漏洩についてはかなり対応できるようになっているが（参考例参照）、企業情報となると殆ど対応できていないのが実情です。

〈「個人情報漏洩保険」の参考例〉

| 保険手配のポイント | 引受例（※保険会社により異なる） |
|---|---|
| 情報管理システムを採用した場合、顧客の個人情報漏洩保険が割引対象か。 | 保険会社により異なるが、<br>プライバシーマーク、TRUST eシール、<br>ISMS等の情報管理体制で割引あり。 |
| 個人情報漏洩保険に加入した場合、企業情報漏洩も補償可能か。 | 企業情報漏洩にも対応可能な保険会社もある。 |
| 企業情報漏洩をカバーするために、別途保険（IT賠償責任保険）が必要か。 | 不要とする保険会社もある。 |
| 引受限度額 | 保険会社により異なるが、<br>個人情報　10億円<br>企業情報　10億円<br>共通限度額とする保険会社もある。 |
| 医療機関、病院、薬品治験業者等の引受規制 | 「なし」とする保険会社もある。<br>※地方公共団体、独立行政法人専門職業人、<br>は引受規制あり、とする保険会社もある。 |
| 電磁波による情報漏洩について | 契約者の過失により、情報漏洩と認定された場合、電磁波に起因しても情報漏洩事故として有責となる。契約者に過失がなく、単に電磁波のみ受信解析して情報漏洩となれば無責とする保険会社もある。 |

※従業員の不正「窃盗・強盗・横領・背任行為・詐欺」により、企業の財産上の損害に対して保険金が支払われる「身元信用保険」という保険がありますが、残念ながら、保険各社とも、「財産上」とは現金並びに有価証券に限定され、企業情報は入らないという解釈で統一されているためカバーされません。

◆身元信用保険（Fidelity Bond）
従業員が会社の事務を処理するに当たり、また事故の職務上の地位を利用する事によって行った窃盗、強盗、横領、背任、詐欺の結果生じた会社の財産上の損害に対して保険金が支払われます。第三者に損害をもたらした場合でも、会社の使用責任に基づく法律上の損害賠償責任が生じた場合、保険金が支払われます。

◆会社役員賠償責任保険（D&O）
会社役員としての業務の遂行に起因して、損害賠償請求がなされたことによって被る損害賠償責任が生じた場合、保険金が支払われます。

企業情報漏洩のように保険が十分に機能しないリスクについて、先ず、リスクの予防として様々な対策を講じつつ、不足の保険ヘッジ分をキャプティブ（レンタキャプティブ）のような手段で企業防衛を図ることも一考に値するのでは・・・。