2011.7.1

中国風険消息＜中国関連リスク情報＞ 特別号2

＜2011 No.4＞

「風険消息＜中国関連リスク情報＞」は、中国に拠点をお持ちの企業の皆様にお届けするリスク情報誌です。「月刊」と「特別号」の２種類に分けて発行し、「月刊」では、中国における種々のリスク（自然災害、法令違反、情報漏えい、労務リスク等）について、発行の前月に公表・報道された主要ニュース一覧と、ニュースに関連するお役立ち情報を簡潔に記載しています。また、「特別号」では、時節に応じた話題や、社会の関心が高いトピックを取り上げて解説しています。

今号のお役立ち情報： 中国の情報セキュリティ事情について

情報セキュリティにおいては維持すべき３つの特性がある。「完全性」、「機密性」、「可用性」である。なかでもシステム停止による「可用性」の喪失や、個人情報漏えいなどに代表される「機密性」の喪失は、影響範囲の広くビジネスの停止やレピュテーションの低下につながり、企業経営への影響が大きなリスクである。

本稿では、この２つのリスクに着目して、中国における情報セキュリティ事情と対応策についてご紹介する。

１． システム障害

最大のインターネット利用人口を誇り、巨大情報化社会となった中国においても、情報システムは多くの企業活動のベースとなっている。情報システムの重要性はここ数年で急速に高まり、それにあわせてシステム障害は企業活動の停止に直結するリスクとなっている。他方で、日本企業の多くでは、海外進出に際し、現地でスピードとコスト最優先でシステム構築を行ってきたケースも多く、システム障害のリスクの発生可能性は低くない状態である。

このため、まずはシステム障害の事例をご紹介しつつ、システム障害への対応策をご案内しよう。

（１）中国におけるシステム停止事例

日本においては、この 3 月に発生した大手金融機関のシステムトラブルにより、数日間振込み業務ができなくなり、多くの企業の決済や資金繰りに多大な影響が生じたことは記憶に新しいが、中国においても、ここ数年、システム停止によるトラブル事例がいくつも発生している。こうした事例をいくつかご紹介すると、以下のとおりである。

＜事例１：北京五輪入場券の申込受付システムトラブル＞

2007 年 10 月 31 日、システムの処理能力を超える規模の五輪入場券の申込が殺到し、システムがダウン。申込受付を一時停止した。配布予定分１８５万枚に対して、申込方式が先着順であったため瞬時に 800-万件もの申込アクセスが殺到したことが原因と考えられている。

＜事例２：航空会社のシステム障害＞

2010/1 中国大手航空会社のオンラインチケット購入システムで障害が発生。一定期間、すべての航空券がわずか 300 円未満で販売された。但し、同社では購入した乗客数百人から追加料金を取らない方針を発表した。

このように利用者数が多く公共性の高いサービスに関連したシステムが中断した場合、その影響は大変大きなものになる。場合によっては、社会的な問題にも発展する可能性も否定できない。また、インターネットがサービス提供の主要インフラとしている企業の場合は、事業そのものが立ち行かなくなる危険性もある。

（２）事前に検討しておくべきリスクへの態勢

システムの停止を誘発する要因はいくつか存在するが、中国でのシステム障害の特徴としては、事前のシステム要件定義の検討が十分でなかったことが想定される。稼動させるシステムが重要であればあるほど、システムが見舞われるリスクについての洗い出し・分析を十分に行うことが必要である。サービスの内容や利便性といった観点だけでなく、リスクに対する態勢についても十分な検討を行ったうえで要件定義を取りまとめることが重要である。以下、システムの稼動前に検討しておくべきリスクへの態勢について紹介するので参考にしていただきたい。

①　システム障害が発生した場合のサービスの継続態勢（バックアップ体制）

システムの重要性が高ければ、遠隔地の代替拠点に有事の際に相互運用が可能なバックアップサーバーを保有するなどの対策が挙げられる。近年ではクラウドコンピューティングサービスの充実化に伴って、自国以外の海外でバックアップサーバーを保有する企業も多数見受けられる。新たに自社の拠点を構築するだけではなく、専門に代替サーバを保有するＩＴベンダーのサービスを活用することはコスト面では有効でもある。但し、バックアップサーバーの拠点選定においては、セキュリティ対策の充実度、緊急時のメンテナンス体制、データの保管管理体制といったリスク対策にも十分配慮しておくことが重要である。

②　想定外処理負荷が発生した場合のシステムの安定稼動（フェールソフト）

重要なシステムがシステムダウンに陥った場合は、たとえそれが短時間であっても大きな影響を及ぼす可能性がある。その意味では、想定外の処理負荷がかかった場合でもシステム全体の機能を完全に喪失するのではなく、可能な範囲で稼動機能を維持するような対策を施しておくことが重要である。それには、システム負荷の状況を監視する体制、状況に応じて縮退措置を講じることの出来る体制を平常時より整備しておく必要がある。

③　システム障害が発生した場合の情報伝達ルールと復旧対応組織の編成

万が一障害が発生した場合でも、サービスの早期復旧と悪影響拡大の防止に努める必要がある。その意味では、事業継続計画（BCP: Business Continuity Plan）を策定することが有効である。ＢＣＰの中で有事の際の復旧手順を明確化しておくことで、迅速かつ的確な復旧対応を実施可能となることが期待できる。近年では企業は事業継続の観点からも、いかにシステムを継続させるかが経営課題となっている。

２．個人情報管理

情報セキュリティにおける「機密性」を阻害する代表的なリスクといえば「情報漏えい」が挙げられよう。日本では個人情報漏えい対策は、2005 年の個人情報保護法施行以降、企業における情報セキュリティ対策の中心となっている。では中国の個人情報管理事情はどのようなものであろうか。ここでは中国での個人情報保護に関する意識と規制の動きにスポットをあてて紹介する。

（１）個人情報保護に関する中国の人々の意識

2010 年 11 月に、中国共産党機関紙・人民日報系の環球時報が、北京や上海など 7 都市で、18～64 歳の市民 1153 人を対象に実施した世論調査によると、個人情報保護に対して市民の 8 割が不満を抱いて

いる。回答者のうち、半数近くの 46.3%がプライバシーを侵害されたことがあり、このうち 4 割が、泣き寝入りしている実態も明らかになった。また、調査結果ではプライバシー保護の状況について、44.4%が「社会に保護意識はあるが、不足している」と回答、35.9%が「社会の保護意識に問題がある」としており、プライバシーを厳格に保護する法制定や法律による監督強化を求める意見が多かった。

中国国内での個人情報漏洩事件については目だって報道されることがないため、実体がなかなか把握しにくいが、実際には多くの国民が侵害をうけ、中国社会全体の個人情報保護への意識に懸念を抱いているという結果は注目すべきと考えられる。

（２）中国における個人情報漏えい状況

この調査結果を裏つけることができるような状況が垣間見られるのが、中国で 2008 年の流行語になった「人肉捜索」である。「人肉捜索」とは中国のインターネットで人気をよんでいる掲示板のことである。「人肉」は「人力で」、「捜索」は「ネット検索」を意味しており、必要な情報をみんなの手で探して公開するということから始まった。それが次第に関心のある人や物などについての情報交換へと代わり、2006 年ごろからは標的にした人物の個人情報を暴く形に変わってきた。現在では、ネット上で大勢の人間がよってたかって、個人情報を暴き出すというものとなっている。
人肉探索は、政府の統制のもとで既存メディアが報じない不祥事や腐敗をあぶり出す効果もあると言われているが、一方で、一般市民の個人情報も漏えいし、思わぬ中傷や非難を浴びせられる事例も散見されるようになっている。

＜事例１＞
2010 年 11 月、四川省成都市で開催された美女コンテストで、出演者の女性が突然、舞台上で全裸になった。中国の掲示板では「人肉捜索」が行われ、女性の身元（本名や年齢、生年月日、身長、体重、職業のほか、生まれ育った環境）がすべて明らかになってしまった。

<事例２＞
2010 年 5 月多数の女性との親密な関係を赤裸々につづった日記がネットで公開され、「人肉捜索」によって身元が明かされたことにより、広西自治区のタバコ専売局局長が免職。

このように、いとも簡単に個人情報がネットで幅広く公開されるという現状は、日本では理解しにくいものである。しかしながら、中国においては、個人の非公開の情報を広く開示することに対しての抵抗感が比較的低く、制御が働きにくい実状にあることがわかる。

（３）個人情報保護に関する規制の動向

このような実態に対し、個人情報漏えいに規制をかける動きもでてきている。

＜事例１：浙江省「信息化促進条例（情報化促進条例）」＞
2010 年、浙江省が、インターネットを通じて他人の個人情報を広めることを禁止すべく、「信息化促進条例（情報化促進条例）」の草案を作成した。当初は「社会組織または個人の情報を得るためには、合法的な経緯によらねばならず、法にもとづき合理的な利用をしなければならない。法人、個人ともに、インターネットを利用して、権利人に関連する情報を許可なく発表、伝播（でんぱ）、削除、修正してはならない」との文章が盛り込まれた。但し、最終的には「業務上個人情報を扱う企業は、情報を第３者に販売・不法提供してはならない」に変更された。

＜事例２：江蘇省徐州市＞

江蘇省徐州市は 2009 年、「人肉捜索」を禁止する条例を制定した。住所をはじめ、財産・収入状況、女性の年齢など他人の個人情報をネットを通じて公表・流布した場合、最高 5000 元の罰金を科す。また、情状が重大なら、半年間のネット接続禁止も命じるといった内容。

中国においては、中央政府レベルでの明確な個人情報保護の法令は制定されていないが、このように、地方自治体レベルで、個人情報保護に向けた規制の動きが出てきている。浙江省のように、最終的には人肉探索のような個人による情報漏えいに対しては規制をかけることを断念したケースもあり、この問題への対処がなかなか難しくこのため、市民の不安はなかなか解消されないのが実情である。

但し、企業に対する個人情報漏えいを規制する動きは着実に高まっており、企業においては個人情報を含めた情報漏えいリスクに取組む必要性がある。特に世界的に注目されている中国企業に対し、企業における情報漏洩事故に対する社会の関心や意識はグローバルで非常に高くなっており、企業が個人情報漏えい事故を発生させると、「事故対応に関する直接的・間接的コスト」以外にも、「企業の信用の失墜」といったレピュテーションリスクにまで影響することが考えられる。

（４）企業における情報漏洩対策

深刻な影響をもたらす個人情報漏洩の多くは、不正アクセスなどの意図的な要因による情報漏えいによるものである。

不正アクセスによる情報漏えいの代表的なケースは、企業がサーバ内に保有する情報が不正に取得されるといったもので、そのアクセスルートは、外部からのものと内部からのものと２通りがある。

①外部からの不正アクセス

外部からの不正アクセスは、悪意をもった者が企業内ネットワークにおける脆弱性をついて、外部ネットワークから企業内ネットワークに侵入するものである。通常、多くの企業はネットワーク構成の中でファイヤーウォールを設置しているため、外部からの不正な侵入を容易に許すことはない。しかしながら、近年では外部からの侵入手口が高度化し、企業内ネットワークにおける僅かな脆弱性が巧みに利用されて不正にネットワークにアクセスされ、企業内の機密情報・個人情報が取得される事件が発生している。特に、企業が運営するＷｅｂページ（ホームページ、ショッピングサイト、等）が持つ脆弱性を利用した事故が近年多く見受けられる。中国国内でもショッピングサイトでの被害は多くなっているという。

外部アクセスによる情報漏えいを防止する対策としては、「ネットワーク上からの侵入対策」に注力する必要がある。基本的には、侵入検知のツールを社内ネットワーク内に設置するのが有効である。その代表的なものが不正侵入検知システム（ＩＤＳ：Intrusion Detection System）及び不正侵入予防システム（ＩＰＳ：Intrusion Prevention System）である。ＩＤＳは不正侵入を検知するシステムで、ネットワーク型ＩＤＳ（ＮＩＤＳ:Network-Based IDS）とホスト型ＩＤＳ（ＨＩＤＳ:（Host-Based IDS）の２種類がある。ＮＩＤＳは、監視対象となるネットワーク上に設置され、ネットワーク内の通信パケットを監視の対象としている。監視対象ネットワーク内における不正な通信パケットを検出する。一方、ＨＩＤＳは，監視対象となるホストサーバ上にインストールされ、受信データやアクセスログを自動解析して不正侵入を検出するが、ＨＩＤＳの中にはサーバ内にあるファイルの改ざんを検知する機能を持つものある。ＮＩＤＳ，ＨＩＤＳどちらも不正侵入の検知後は即刻、管理者へメールを発信するなど警告措置が自動設定で行われる。ＩＤＳにより不正侵入の検知がリアルタイムで行われることで、管理者は警告を受け取ったのち、被害拡大の防止に向けて迅速な措置をとることができる。

ＩＰＳは不正侵入を予防するシステムで、監視対象ネットワーク内における不正な通信パケットがあればそれ以上のネットワーク内への到達を遮断することで、不正侵入や攻撃を防止する。

従来からの通信制御機能をもつファイアウォールに、こうしたＩＤＳ、ＩＰＳを組み合わせて形での企業内ネットワークへの不正侵入への対策が講じることが望まれる。

②内部からの不正アクセス

一方、内部からの不正アクセスは、企業内組織に所属する従業員がデータへのアクセス権限を不正利用して情報を取得するといったものである。中には企業に雇用されている期間に正規のアクセス権限でデータを取得し、退職後にそれを持ち出して不正利用するといったケースや、企業内ネットワークへのアクセス権限が付与された外部委託社員により、正規のアクセスルートからの不正に情報が持ち出されるケースも発生している。

内部からの不正アクセスを防止するに当たっては、まず、そもそも、なぜ機密情報の持ち出しや他社への提供がいけないのか、社内ルールも含めて従業員を教育し周知することが重要である。また教育実施後には、従業員へ「教育内容を理解し、機密情報を漏えいした場合は損害賠償請求されることを理解した」などを明記した書類に署名を求め、契約の上でも機密保持義務を明確にすることも効果的である。また、退職者による内部犯行の防止の観点からは、退職後でも在職中に知りえた個人情報や重要情報について不正利用しないことを誓約させるなど、退職者に関しての情報管理ルールを明確化しておくことよいだろう。

内部犯行による情報漏えいについては、100%防止することは不可能である。しかしながら、企業の取り組みとしては、社内規定やルールを整備し、従業員への教育を徹底するなど、最低限、抜け漏れがないようにしておくことが望まれる。

３．まとめ

中国国内での実施すべき企業の情報セキュリティ対策のポイントは、「意識啓発」にあると考えられる。「システム障害」であっても「個人情報管理」であっても。情報セキュリティリスクへの意識レベルの底上げがなければ実効性のある取組みができないだろう。その意味では、企業の情報管理責任者が、中国国内の情報セキュリティ事情、自社の情報セキュリティリスクの対策の現状などについて積極的に情報発し、意識啓発に努めることが望まれる。その際、マンパワーの不足によって取組みが足踏みしてしまうようであれば、外部コンサルティング会社の簡易診断や現場調査などを有効活用していただくことを是非検討いただきたい。

株式会社インターリスク総研は、MS&AD インシュアランスグループに属する、リスクマネジメントに関する調査研究およびコンサルティングを行う専門会社です。中国進出企業さま向けのコンサルティング・セミナー等についてのお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、お近くの三井住友海上、あいおいニッセイ同和損保の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
㈱インターリスク総研　コンサルティング第二部
TEL.03-5296-8918　　http://www.irric.co.jp/

瑛得管理諮詢（上海）は、中国 上海に設立されたＭＳ＆ＡＤインシュアランスグループに属するリスクマネジメント会社であり、お客様の工場・倉庫等へのリスク調査や、ＢＣＰ策定等の各種リスクコンサルティングサービスを提供させて頂いております。お問い合わせ・お申し込み等は、下記の弊社お問い合わせ先までお気軽にお寄せ下さい。

お問い合わせ先
瑛得管理諮詢（上海）有限公司 （日本語表記：インターリスク上海）
上海市浦東新区陸家嘴環路 1000 号　恒生銀行大廈 24 楼 142 室
TEL:+86-(0)21-6841-0611（代表）