

パートナー企業と情報セキュリティ対策

野村総合研究所 末廣義人

インターネットの普及・定着にともない、企業運営における情報セキュリティへの関心はたいへん高まっており、情報セキュリティガイドラインの制定やマニュアルの整備も進んでいる。本稿では、とくにシステム開発のパートナー企業に対して、具体的にどのような対策が必要かについて考察する。

情報セキュリティ意識の高まり

最近、NRI（野村総合研究所）の主要パートナー企業の経営者の方にお話を伺う機会があった。そのなかで企業の重要施策としてあげられたのが次の4点である。

品質向上

生産性向上（コスト競争力強化）

上流工程への取り組み

情報セキュリティ対策

また、パートナー企業のなかで、セキュリティポリシーやセキュリティガイドラインを制定し、品質管理認証のISO 9001と同様に日本情報処理開発協会によるPマーク（JISQ 15001）を取得するところが増えている。

これらのことから、システム関連企業の間で、情報セキュリティ対策がいかに重要なものと認識されているかがうかがえる。

情報セキュリティ問題に対しては、システム関連企業にとどまらず一般企業においても、コンピュータウイルス、情報漏洩、個人情報保護に関する法案をめぐる議論などが社会問題として大きくとり上げられていることなどから、経営の意識は急速に高まっていると言えるであろう。

オフショア開発での指導の重要性

NRIでは、中国でのオフショア（海外拠点）開発の有効性に関する調査を目的に、2000年3月に北京、大連のソフトウェア企業を訪問した。その際に、他社の日本向け開発の実績を詳細に説明されたことや、関係者以外でも自由にオフィスに出入りできる様子を目のあたりにしたことで大きなショックを受けた。そして、中国オフショア開発の前提として、日本語や品質管理・進捗管理に関する教育や、標準化といった課題より前に、情報セキュリティガイドラインの制定とその指導が優先的な課題であると強く感じながら帰国したものである。

この経験から、実際に中国での開発を開始するにあたっては、セキュリティガイドライン制定と指導、品質・進捗などのプロジェクト管理ガイドライン制定と指導を行った。2002年春に中国の開発現場を訪問した際には、当社専用のセキュリティルームが整備され、当社のプロジェクト関係者以外が出入りできないシステムが導入されていた。また、日本の他社が当社の委託先を訪問した際、「この部屋はNRI専用なので入室禁止です」

「プロジェクト内容は一切説明できません」とあっさり断られたという話も聞いている。

オフショア開発で、委託先（リモート開発場所）に対するセキュリティ対策の徹底と指導がいかに大切かを示す出来事である。

対策の実効性を高めるために

一般に大手ソフトウェア企業では、セキュリティポリシーやセキュリティガイドラインを制定し、ファイアウォールの構築などの情報セキュリティ対策を実施している。またパートナー企業に対しては、プロジェクト実施時のセキュリティ対策の実効性を高めるため、たとえば次のような対策をとっている。

入館チェックシステム

入館許可カードシステムを導入し、ビルの入館チェックおよび所定場所の入室チェックを行う。さらに入館・入室ログを保存する。

エリア分離の徹底

委託外の他の業務との混在を避けるため、当該業務の要員のフロアあるいは入り口を分離してエリア分離を実施する。

PCの完全貸与

データ漏洩防止とセキュリティ対策を施したPCを貸与し、PCの持ち込みを禁止する。またアクセスできるデータを制限する。

業務委託契約書の機密保持条項の拡充

従来の機密保持条項に、機密情報の定義、セキュリティの確保方法、従業員の義務などの詳細事項を追加する。さらに、重要な役割

をもつ従業員には機密保持誓約書の写しの提出を求める。

再委託先の把握

再委託先の使用については書面による承諾を原則とする。また、再委託先の要員に対して、ビルへの入館証発行時などに本人確認を実施する。さらに、定期的に再委託先名や人数の実績を報告させる。

セキュリティ研修

委託元のセキュリティガイドラインについてパートナーメンバーに研修を行う。海外のパートナー企業についても現地を訪問して研修を実施する。

パートナーエリア管理

パートナー企業の委託業務エリアに管理者を置く。またルール・問題点を周知徹底させる会議を定期的で開催したり、巡回などの日々の管理を実施する。

実効性あるセキュリティ対策が肝要

企業にとって、セキュリティポリシーやセキュリティガイドラインの制定、パートナー企業に対するルール作り、機密保持契約の締結といった対策は、必要最低限の対策である。しかし、制度やルールを作るだけでは十分でなく、それが実効性をともなわなくては意味がない。そのために、他社を含めた事故事例の検証、教育や指導、そして監視・監査の充実、開発に携わる一人ひとりのモラルアップなどを図ることも忘れてはならない。