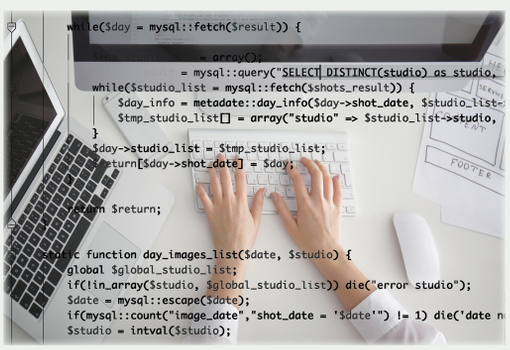
セキュリティ対策の不備は不法行為？

契約時に合意すべき事項

・納入後に公表された新規の脆弱性対策
・既知の重要な脆弱性対策
・脆弱性 検査の実施の有無
・緊急事態時の費用負担

（引用元：『セキュリティ担当者のための脆弱性対応ガイド』 IPA）



アウトソーシング先との確認

モニタリング
第三者監査
情報セキュリティ要求事項への
遵守状況に関する検収・評価

カード情報流出による個人情報漏洩などのセキュリティ事故は、多くの被害を引き起こし場合によっては裁判による闘争となってしまいます。
企業が被害者から賠償責任を問われる場合が多いのですが、企業がシステム開発を外部に委託している場合は、そのセキュリティ事故について、委託先企業と裁判で争うケースもあり、その中には、開発が終了し運用に入ってから、その作られたシステムの脆弱性に気づき、それを改修するためには費用もかかるためその責任について開発会社と争うということもあります。
ある SQL インジェクションの判例では、セキュリティ事故として実質的な被害があったわけではなく、サイトに脆弱性があると指摘を受けて SQL インジェクション対策の不足が発覚し、このセキュリティ対策不備については故意過失によって生じた不法行為（使用者責任）だと認定され、最終的には委託先企業に対してサーバの移転に必要な費用や、対策にのために停止した金額等での損賠賠償の支払いが確定しました。
つまり、セキュリティの脆弱性が見つかると、手抜き工事が見つかったマンションのように目に見えた損害がなくても責任追及されてしまうということです。
判例では、開発を請負った時点で IPA（独立行政法人情報処理推進機構）が公開している SQL インジェクションなどのセキュリティ対策は、仕様書記載の有無に拘わらず開発の必須条件として委託先に責任があるとしていることです。
ここで問題なのは、両者は確認書でセキュリティ対策を規定していたにもかかわらず 4 年以上にわたって運用されていたことです。被害がなかったからよかったものの、IPA も、稼動中の ウェブサイトに対し 脆弱性 検査を行 い、脆弱性が 見つかった場合にはその対策を施すことを契約に含めるべきだと、「脆弱性対応ガイド」に明記しています。
経済産業省が出している「アウトソーシングに関する情報セキュリティ対策ガイダンス」でも、情報セキュリティに係る要求事項については、管理策を示すだけでなく、実施状況の確認方法や、不備があった場合の対応にまで踏み込んだ明確な取り決めを行うべきだとアドバイスしています。
このように、企業も受注する側も、お互いにリスクを回避するためには、契約時の取り決めをしっかりすることと、セキュリティ対策についてもっと意識と知識を高めることが重要となります。

© CEC Customer Service Ltd.