水野施設長の介護マネジメント塾

5 月号

情報セキュリティインシデントとは

はじめに

皆さん、こんにちは。

組織が持つ情報は、経営を行う上で大切な「人・物・金」と並んで重要な資源といえます。中でも、ご利用者の情報の保護は、「個人情報保護」という観点からも、江戸川光照苑に限らず、あらゆる施設においても自施設の介護サービスを快適にご利用いただくための要件の一つであることは、いうまでもありません。

そこで、今回は、情報セキュリティに対する脅威とリスクについてお話ししたいと思います。

すでに情報セキュリティインシデントに脅かされている

ITが現代の企業経営のあらゆる分野に浸透し、企業の重要な経営資源や資産として認識されてきています。これは、企業に限らず介護・福祉の分野でも、生産性の向上や競争力の強化などを目指し、絶えず情報システムの刷新、構築を図ってきました。

しかし、単にシステムを活用するだけでは、顧客満足を実現することはできません。市場において競争優位を確立するためには、情報システムの安定稼働はもちろん、いかに情報セキュリティを確保するかが大きな課題となるのです。その一方でITは、セキュリティ対策の不備に起因する機密情報の漏洩、コンピュータウィルスや不正アクセスによる事業への影響など、さまざまな危険と脅威にさらされおり、これらを裏付けするように、セキュリティ関連の事件・事故が相変わらず発生し、組織のコンプライアンス経営を脅かしています。

事実、「2009 年　情報セキュリティインシデントに関する調査報告書　第 1.1 版」（NPO 日本ネットワークセキュリティ協会）においても、表のように、医療・福祉分野においても情報セキュリティインシデントが継続的に発生していることがわかります。

医療・福祉分野のインシデント件数の経年変化

年	件数
2005	54 件
2006	42 件
2007	73 件
2008	91 件
2009	64 件

「2009 年　情報セキュリティインシデントに関する調査報告書　第 1.1 版」（NPO 日本ネットワークセキュリティ協会）より筆者作成

情報セキュリティインシデントの実際

情報セキュリティが注目を集めたのは、以前発生した尖閣諸島の中国漁船衝突事件のビデオ映像が流出問題ではなかったでしょうか。これによって、新たな情報セキュリティリスクの出現を医療・福祉分野においても予想させるものになったといえます。

実際に、大阪府池田市で施設から備品のデジタルカメラが盗まれ、複数の幼児を撮影した写真200枚以上が路上にばらまかれた事件や、群馬県介護研修センターの職員が、旧高齢者介護総合センター利用者の個人情報や業務資料などが保存された USB メモリを紛失した問題、一昨年にも、千葉県で、県職員が、介護保険サービス事業者に関する個人情報など 9705 件含む USB メモリを持ち帰り、帰宅途中に紛失したなど、情報漏洩というリスクはご利用者に対する重大な人権侵害といえます。

このことからもわかるように、平成17年4月に完全施行された個人情報保護法をうけ、施設や事業者では、個人情報の適切な管理を行っているにも関わらず、あらゆる分野で個人情報の持ち出しやパソコンや USB メモリの盗難など個人情報漏えい事件が後を絶ちません。また、言い換えればそれだけ個人の情報は狙われているといえるのです。

特別養護老人ホームをはじめとする施設や事業者が保有する個人情報には利用者にとって極めて守秘性が高い、既往歴や現病歴、要介護状態、ケアプランメニュー、家族構成などが含まれています。特に、地域包括支援センターなど在宅の一人暮らし高齢者や高齢世帯の情報漏洩は、振り込め詐欺などの犯罪には絶好の情報であり、これら個人の情報を適正に管理することは、組織にとって最大の責務であるといえます。

このことは、万が一にでもご利用者の情報を漏洩してしまった場合、その性質上、ご利用者やそのご家族への影響はもちろん、社会的影響も非常に大きく、施設や事業者の信頼失墜はもとより、施設運営に深刻な問題が生じることはいうまでもありません。

情報セキュリティのリスク

ISO27001/ISMS における情報セキュリティマネジメントシステムにおいては、情報セキュリティのリスクを機密性のリスク、完全性のリスク、可用性のリスクと、大きく3つに分類しています。

機密性のリスクとは、組織内で話されたり、書かれたり、作成されたりする情報が、無許可のユーザーや悪意のあるコードからアクセスされることによって、組織の知的所有権が受ける脅威です。

また、完全性のリスクとは、組織の重要なデータの損傷を試みる無許可のユーザーや悪意のあるコードによって、ホームページや施設広報紙、調査報告書など、組織の経営に役立たせるため

の付加価値のある情報、いわゆるビジネスリソースが受ける脅威です。完全性のリスクでは、データベース サーバー、データ ファイル、電子メール サーバーなど、組織の重要な情報が含まれるビジネス資産を損失する可能性があります。

そして、可用性のリスクとは、業務やスタッフの作業の妨害を試みる無許可のユーザーや悪意のあるコードによって、業務プロセスが受ける脅威です。可用性のリスクによって、組織に蓄積されたデータや分析結果、マニュアルや手順書などのも業務プロセス、ワードやエクセルなどの市販のソフトはもとより、自施設独自で開発したデータソフトなどのアプリケーションの機能や能力など、業務を遂行する上において必要な行程はすべて、被害を受ける可能性があります。

この3種類すべてのリスクから組織を保護するために、ISO27001/ISMS つまり、情報セキュリティマネジメントシステムが有効といえます。

※参考文献

㈱インターリスク総研が発行している情報セキュリティニュース＜2010 No.2＞