TOSBAC

MANUFACTURING FIRST ≫ TOSBAC

capter
#01

情報漏洩の恐怖

社会的責任の遂行と利益の確保

情報の電子化により、様々な種類の、かつ大量な
情報を利活用できるようになり、非常に便利になりましたが
その反面、便利さに比例して
「情報漏洩」のリスクが高まっています。

企業では、様々な情報を保有しておりますが、中でも秘匿性の高い情報が漏洩してしまった場合、企業存続にも影響するようなダメージを受ける可能性があります。
例えば、顧客の作成した図面データや仕様書データが漏洩してしまった場合、直接的には取引中止や、損害賠償を請求されてしまったり、間接的には、業界に情報漏洩の事実が認知されてしまい、新規取引の機会が逸失してしまうというリスクがあります。

さらに、漏洩した情報が個人情報であった場合、国内では個人情報保護法に準じて会社、または経営者に対する刑事罰が科せられてしまうリスクがありますし、EUに拠点あるいは、取引がある企業においては2018年5月施行の「GDPR(EU一般データ保護規則)」への準拠が求められ、従わなかった場合、最大で企業の全世界年間売上高の4%以下、もしくは2000万ユーロ(おおよそ23億円)以下のいずれか高い方が適用されるという非常に大きな罰則が科せられます。

一方で、情報漏洩はあらゆる可能性が想定されることから、すべてに対策を講じると対策費が莫大になってしまいますし、業務の可用性も著しく低下してしまうといった「どこまで」「どのような」対策を講じるかの判断が非常に難しいテーマです。

弊社は、ISO27001(ISMS)の認証を取得しており
その知見を活かし、リスク評価から対策の支援まで対応可能です。

株式会社 神奈川トスバック
お問い合せ システム営業部
045-662-1335
http://tosbac.co.jp

漏えいの原因と手口

外部からの攻撃

CASE **ウイルスに感染させ、ウイルスに仕込まれた機能を用いてデータへアクセスするパターン**

- ▶ メールへのファイル添付し、リンク先へアクセスさせウイルスに感染させる
- ▶ ウェブサイトを改ざんし、アクセスしたPCへウイルス感染させる
- ▶ セキュリティ対策の浅いIoT機器の脆弱性の利用し、ウイルス感染させる など

CASE **窃取した認証情報を利用して不正アクセスするパターン**

- ▶ メールサーバーやクラウドサービスへ不正アクセスをし、認証情報を窃取する など

内部からの漏洩

CASE **ウイルスに感染させ、ウイルスに仕込まれた機能を用いてデータへアクセスするパターン**

- ▶ インターネットを介さず、USBメモリやDVDなどの記録媒体を利用して持ち出し可能

CASE **紙媒体の情報を持ち出すパターン**

CASE **不注意による漏えいのパターン**

- ▶ 落としたり、忘れたり など

対　策

- ☑ 各情報に対して漏えいした場合の影響度を精査し分類する。
- ☑ 分類された情報ごとに持ち出しルール（規定）を定める。
- ☑ 定めたルール（既定）を従業員へ周知徹底させる。
- ☑ USBメモリやDVDが不正利用できないよう対策製品を導入する。
  - ▶ エンドポイント監視・防御製品など
- ☑ 外部からの攻撃経路へ対策製品を導入する
  - ▶ ネットワーク監視・防御製品など
  - ▶ エンドポイント監視・防御製品など

弊社は、ISO27001（ISMS）の認証を取得しており、その知見を活かし、リスク評価から対策の支援まで対応可能です。

JQA-IM1644

関心をお持ちいただけましたら、下記までご連絡ください。

株式会社 神奈川トスバック
〒231-0032 横浜市中区不老町1丁目1番地5号
横浜東芝ビル7F
お問い合せ システム営業部
045-662-1335
トスバック 検索
http://tosbac.co.jp