

機密性・完全性・可用性

情報セキュリティ対策は、情報資産の「機密性」、「完全性」、「可用性」の三要素を確保しつつ、企業や組織の正常な活動を維持するために実施されなければなりません。

【豆知識】

「機密性」(Confidentiality)、「完全性」(Integrity)、「可用性」(Availability)のそれぞれの頭文字をとって、CIA と呼ばれることもあります。米国の中央情報局(Central Intelligence Agency)になぞらえての呼び方なのかもしれません。

機密性

機密性とは、情報資産を正当な権利を持った人だけが使用できる状態にしておくことです。

情報漏えいが機密性を阻害する最大要因と言って過言ではなく、企業や組織は情報漏えいに対する様々な対策を講じなければなりません。

情報資産が含まれた情報機器や媒体(パソコン、スマホ・タブレット、USB メモリや CD-ROM、書類等)の紛失、置き忘れや、メールの誤送信など、悪意のないミスによる情報漏えい防止対策がまず重要です。(情報漏えいの防止)

また、そのような時に情報を再利用しにくくするために、データを暗号化するなどの対策も効果的です。(暗号化)

さらに、悪意のある者への対策も必要となります。

具体的には、外部の者が不正にネットワーク内に入ってこないようにする、パソコンやデータにパスワードを設定する、許可された者だけがその情報資産にアクセスでき、許可されていない者はアクセスできないか、データを閲覧することはできても書き換えることはできないように制御するなどの対策です。(ネットワーク管理、パスワードの設定、アクセス権の設定)

企業や組織により、機密性の高い情報は異なります。メーカーならば新製品の開発情報、小売店ならば顧客情報などがそれにあてはまりますが、社員や職員の個人情報はその企業でも保有する機密性の高い情報です。このような機密性の高い情報は、組織内でもできるだけ情報にアクセスできる人を減らすことで漏えいや悪用リスク

が減ることになります。ID やパスワードによる管理も重要ですが、特定のエリア入室者制限をするなどの対策も効果的でしょう。

完全性

完全性とは、保有する情報資産が正確であり、完全である状態を維持することです。情報が不正に改ざんされたり、破壊されたりしないことを指します。

悪意の有無によらずデータの管理ミスが起きれば、組織の信頼性が揺らぐこととなります。データを扱う社員のオペレーション教育が重要です。

火災や天災でデータが破損や損失することで企業の継続性が失われてしまうリスクにも目を向けなければなりません。システムのバグも時としてデータを不正確なものにしてしまうのでチェックが欠かせません。

重要な情報資産にはバックアップが欠かせません。

悪意を持った第三者による完全性の破綻の例として、サイバー攻撃(サーバやパソコンなどのコンピューターシステムに対し、ネットワークを通じて破壊活動やデータの窃取、改ざんなどを行うこと)による情報の改ざんが考えられます。サイバー攻撃というと個人情報の取得を狙ったものが多いのですが、最近は情報の改ざんにとどめる例もあります。つまりターゲット企業の経営のかく乱や信用の失墜を図るためです。ネットワーク管理、パスワードの設定、アクセス権の設定、データの暗号化など、機密性の項で述べた対策は完全性の面でも有効です。

さらに、利用者のアクセスやデータ変更の履歴を残し(ログと言います)、どのような処理がなされたのか遡れるようにする、データを正副2つ持つことで片方を喪失しても、またデータが改ざんされても置き換えたり、データマッチングで差異を検知できるようにするなどの対策で、悪意の第三者による改ざんや漏えいの際の被害を低減することができます。

可用性

可用性とは、情報資産を必要なときにいつでも使用できることです。つまり、可用性を維持するということは、情報を提供するサービス(システム)が常に動作するということを意味します。

前述の「機密性」と「完全性」の対策がここでも有効ですが、データのバックアップにしても、システムダウンや天災など大規模な災害時に、いかに早く復旧できるかが問われます。メインデータの複写をサブとして持つだけではなく、それがすぐに利用できないと企業や組織としての被害は甚大です。大規模な基幹システムはシステムを二重化し、例えば東京本社が機能停止しても大阪支社が肩代わりできる体制を構築しておくことなども検討すべきかもしれません。

いわゆる BCP (Business Continuity Plan: 事業継続計画) の一環として、災害復旧のための計画を立案し、バックアップに切り替えて運用するなどを定期的に試験しておくのが良いでしょう。