近年、情報の流出が社会的な問題となっており、流出を防ぐことは情報化社会の発達の上で重要なことである。情報の流出の発生原因について以下の2つが挙げられ、それぞれ対策を考える。

　1つ目はクライアント側の問題として、IDやパスワードの不適切な運用・管理である。単純なID・パスワードではたとえ適切な管理をしていても総当たり攻撃で不正なアクセスをされてしまう恐れがあり、他のサービスと共通したパスワードを設定している場合も一箇所で流出したパスワードで次々と流出してしまう。またショルダーハックやフィッシングなどでパスワードを騙し取られることは、直ちに情報の流出を招いてしまう。

この対策として複雑なパスワードをサービスごとに設定して、自分のみアクセスできるスタンドアローンなデバイスに保存しておく事が有効であると考えられる。

　2つ目はサーバー側の問題として、サービスの脆弱性である。クロスサイトスクリプティングや水飲み場攻撃、SQLインジェクションなどの攻撃はサイトの脆弱性を突いて行われる。またクライアントとの通信も秘匿性が十分に確保されなければ盗み見られる恐れがある。

この対策としてWEBサイトを作るときやデータベースへのアクセス部分はどのような攻撃があるのか想定し、脆弱性が生まれないように十分なテスト・ベンチマークをする事が必要である。また攻撃は日々新しい手法が生まれているため、一度作ったサービスは定期的にメンテナンスをしてセキュリティレベルをあげることが大切である。

情報流出は組織・個人問わず起こりうる事であり、情報流出の損害はその範囲に収まらないものである。ゆえに発生原因を考えその対策を行う事が大切である。