**情報セキュリティ**

**情報セキュリティとは**

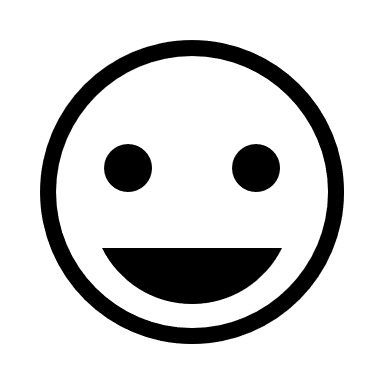
情報セキュリティの3要素である機密性、完全性、可用性を維持すること

これに加えて真正性(authenticity)や責任追跡性([accountability](http://e-words.jp/w/%E3%82%A2%E3%82%AB%E3%82%A6%E3%83%B3%E3%82%BF%E3%83%93%E3%83%AA%E3%83%86%E3%82%A3.html))、信頼性(reliability)、否認防止（non-repudiation）などの要素を情報セキュリティの要件の一部とする場合もある

・機密性…アクセスを認められた者だけがその情報にアクセスできる状態を保持すること

・完全性…情報が破壊、改ざん、消去されていない状態を確保すること

・可用性…必要な時はいつでも情報にアクセスできる状態を確保すること



ユーザ

可用性

Availability

第三者にアクセスさせない

機密性

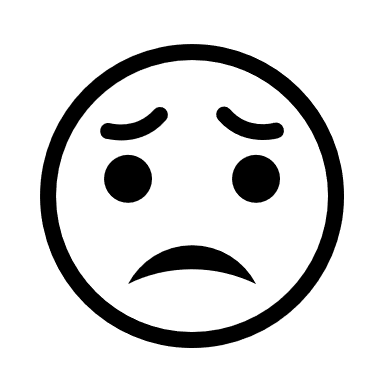
Confidentiality

情報が破壊・改ざん・消去されていない状態を確保

状態へのアクセス(閲覧・変更)がいつでもできる

完全性

integrity



攻撃者

情報の変更・削除

情報の閲覧

改ざんされていない

情報

情報システム

**リスク・脅威・脆弱性**

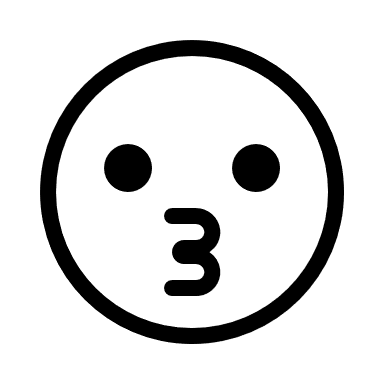
・リスク…情報セキュリティが維持できず、何らかの損失が発生する可能性

・脅威…リスクを実現化させる要因

・脆弱性…脅威に対する弱み

実際に不正アクセスを受け、損失が現実化することをリスクが顕在化するという。

情報セキュリティの維持には、脅威や脆弱性を洗い出しリスクの顕在化を防ぐための対策を行うことが必要。一般的にはリスクによる損失の度合いを算出し、それに応じて優先順位を決めたうえで対策を行う。



脅威

不正アクセス

脆弱性

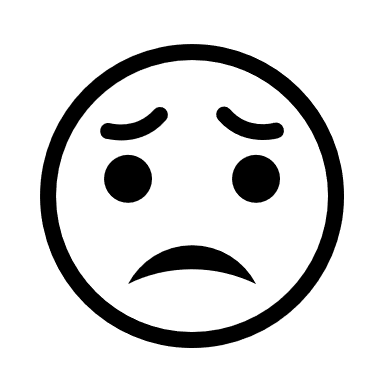
不正アクセスを許してしまうバグ

機密情報

情報システム

機密情報を持ち出されると信用を失う

リスク



管理者

※脅威や脆弱性への対応は費用や手間がかかるので、リスクが軽微な場合にはあえて対策を行わないこともある

**脅威の種類**

・技術的脅威…プログラムが介在する脅威のこと。ネットワーク上で行われるものも技術的脅威に含まれる。マルウェア、 フィッシング詐欺など方法は様々だが、メールを偽装したりソフトウェアやプログラムの脆弱性を狙ったりす るものが多く存在する。

・人的脅威…操作ミスや内部からの情報漏えいするケースなど、人の操作によって引き起こされる脅威のこと。メールの誤 送信や、内部関係者によるデータの抜き取りなどがこれに当たる。

・物理的脅威…地震・洪水・天災などによる、物理的な破損の脅威のこと。天災時には、落下によるPCなどの機器の 破損や浸水などが多く起こっている。経年による故障も物理的脅威に含まれる。

**リスクアセスメントとは**

インシデントを防ぐためにまず情報資産を洗い出し、情報資産に存在し得るリスクを調査、そしてリスクの発生頻度や影響などについても分析し、適切な対応を決定する一連の作業のこと

**リスクマネジメントとは**

リスクを排除したり最低限に抑えたりする作業のこと、リスクマネジメントにはリスク回避、リスク低減、リスク移転の3つがある。

・リスク回避…リスクを回避したり、排除したりすること

・リスク低減…リスクの起きる可能性やその規模を限りなく抑えること

・リスク移転…リスクを第三者に委託すること