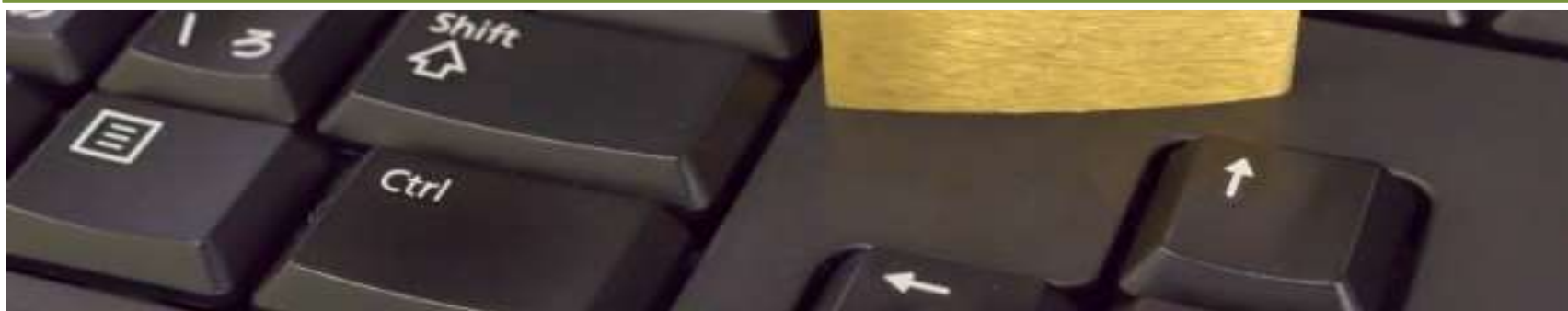




情報セキュリティの基礎概念





情報セキュリティの基本

情報セキュリティ対策では、

次の3つを維持する継続的な対策を求めています。

①重要な情報を漏らさない。盗まれない。

(許可された者だけが取扱える)

②重要な情報を改ざんさせない。取扱いを間違えない。

(厳重な保管、手順通りの実施、確認の実施)

③重要な情報を利用したい時に利用できる。

(整理整頓、問題時の準備)

いわゆる「①機密性」、「②完全性」及び「③可用性」を維持することです。

守るべき情報資産

情報資産

情報資産とは、保有するすべての情報及び情報システムを指します。

情報システム

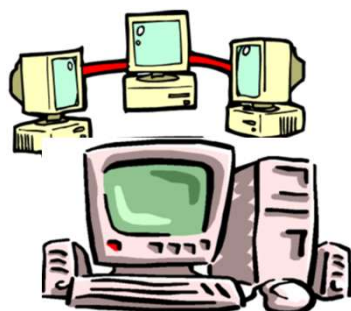
ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、処理を行う仕組み

パソコンデータ

ワープロや表計算ソフト等で取り扱うデータ（電子メールやFD・MO・CD等で外部より入手したデータ等）

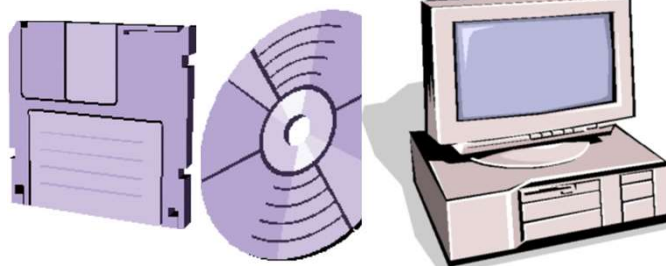
紙媒体

パソコンデータを利用後に出力された紙文書、業務で取り扱う紙文書



情報システム

パソコンデータ



紙媒体



情報資産分類の基準

情報セキュリティ対策基準

3. 1. 1 情報資産の分類 (P.34)

情報資産は、各情報資産の機密性、完全性及び可用性を踏まえ、リスクの大きさに応じて次のように分類する。

I	個人情報及びセキュリティ侵害が区民の生命、財産等に重大な影響を及ぼす情報
II	公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報
III	外部に公開する情報のうち、セキュリティ侵害が行政事務の執行等に軽微な影響を及ぼす情報
IV	上記以外の情報

- * 重要情報資産とは、分類 I 及び II の情報資産を指す。
- * 重要情報資産については、情報資産台帳の整備が必要である。
- * 情報資産の保有者（主管課）から、その情報を受け取る場合は価値分類を継承する。

【参考資料】個人情報価値

経済的損失レベル

3	口座番号&暗証番号、 クレジットカード番号&カード 有効期限、ネットバンキングの ログイン情報	遺言書	前科前歴、犯罪歴、 与信ブラックリスト
2	パスポート、口座番号のみ、 パスワードのみ、 クレジットカード番号のみ、 印鑑登録証明書	年収・年収区分、 所得(生活保護情報含む)、 資産、土地、建物、 給与額、納税額、未納金額	-
1	氏名、住所、生年月日、性 別、電話番号、会社名、メ ールアドレス、住民票コード、 健康保険証番号、免許証番 号、身長、体重、血液型、 身体特性、写真、家族構成	健康診断結果、病歴、 身体障がい情報、DNA情報、 生体認証情報 知的障がい情報、 レセプト情報、国籍・人種、 趣味、嗜好、成績、学歴、 メール内容、位置情報	加盟政党、思想、 信仰、本籍、病状、 保有感染症、 精神的障がい情報、 要介護度、カルテ、 プライベート情報
	1	2	3

参考資料「EP 図 (Economic-Privacy Map)」

出典・引用：NPO 日本ネットワークセキュリティ協会「2013年 情報セキュリティインシデントに関する調査報告書 Ver.1.2」

精神的苦痛レベル



重要ポイント

情報セキュリティ事故が発生すると

■ 情報漏洩

- 社会的**信用の失墜/低下**
- 漏洩情報による**実害**
⇒ 損害賠償の可能性や殺人事件に発展することも

「目的外利用」により信用失墜することもある
信用の回復には、長い年月を必要とする

■ 業務の中断

- 社会的**信用の失墜/低下**
- 業務中断による**行政サービスの遅延や停滞**

■ 復旧コスト

- ウイルス感染パソコン/サーバの初期化・再設定
- 関係各所への報告
- 被害者（がいれば）へのお詫び
- 再発防止策の考案と実施 など

⇒ **情報セキュリティ対策（人的物的技術的）が必要になる**

セキュリティ事故は常に起こっている

- 情報セキュリティに関連する事故は常に発生している
『そんなつもりはなかったのに…』
『この前は大丈夫だった…』



- 決して他人事ではない!!
 - **ヒューマンエラー**が大半である
 - **意識が低い**（セキュリティルールを知らない/守らない）ことで、自分自身が当事者となる
 - 常に自分も**セキュリティ事故を起こす危険性**があることを認識する

身と区を守る

情報セキュリティは、常に「性悪説」で考える

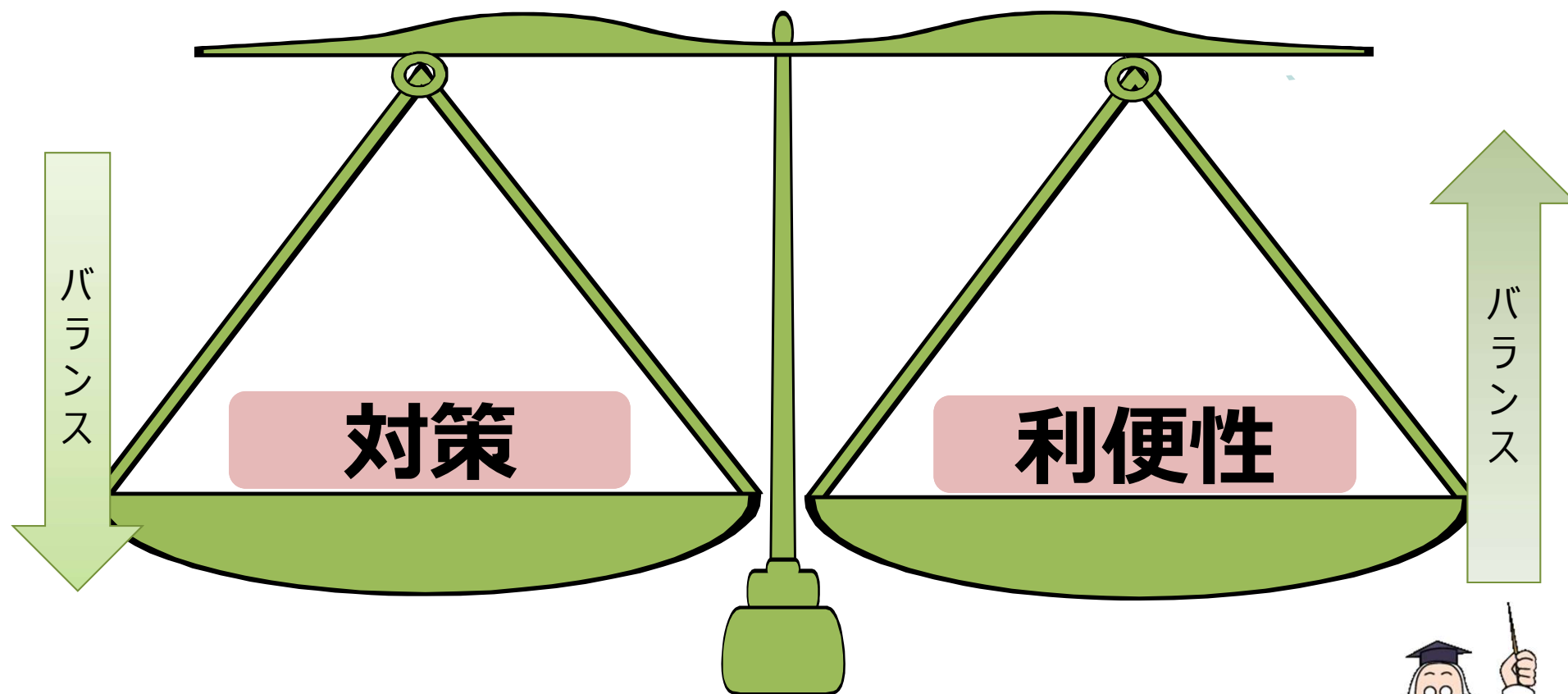
つまり、

- ・情報セキュリティ事故は必ず起こる、
- ・人は必ず不正をはたらく、
- ・情報システムは必ず障害で止まる、など



「不測の事態を前提にルールをつくる必要」

有効性を評価する視点



セキュリティは、常に「対策」と「利便性」が対の状態にあります。
必要な利便性を維持し、
運用可能な対策となっているかを見る視点も大切です。

