１３．ネットワークの危険性と対策

◆インターネットの不正利用
・盗聴

・なりすまし

・改ざん（データの無断書き換え）

◆考えられる対策
（１）パスワード

（２）身体的特徴によるチェック

（３）暗号

◇暗号の基本的考え方　---　鍵（暗号 Key）による計算

たとえば、Key＝１のとき

ＨＥＬＬＯ　⟶　ＩＦＭＭＰ　⟶　ＨＥＬＬＯ

平文　（暗号化）　暗号文　（複合化）

Key＝１２にするとどうなる？

◇暗号の方式
①秘密鍵方式　送信者と受信者が同一の秘密 Key を持つ
→　単純だが不特定多数のユーザに対応できない

②公開鍵方式（暗号化用と複合化用の２つの鍵を用意する）

秘密鍵　所有者だけが保管

公開鍵　ネットワーク上に公開（誰でも入手可能）

（例１）暗号化Keyを公開鍵にする場合（一般的な暗号化通信）

（例２）複合化Keyを公開鍵にする場合（デジタル署名＝なりすまし対策）

◇公開鍵の原理

一方通行関数を利用　Ｘ→Ｙ　簡単　Ｙ→Ｘ　非常に困難
（例　素数の積）