情報セキュリティ

1. サイバー犯罪にはどのようなものがあるのだろうか
警察白書には不正アクセス禁止法違反，コンピュータ・電磁的記録対象犯罪等，ネットワーク利用犯罪，の三つが挙げられている．インターネットの利用者数が世界中で増加していることに伴い，サイバー犯罪は年々増加し，多様化・高度化している．ネットワークの利便性が上がった一方で，サイバー犯罪の脅威が増加している．

ネットワークの特徴として，匿名性が高い，痕跡が残りにくい，不特定多数が利用する，時間と空間の制約がないという特徴が挙げられ，サイバー犯罪はこの特徴を用いた手段である．ネットワーク犯罪の一例として，他人の個人情報を勝手にネットワーク上に掲載したり(いわゆる晒し行為)や無責任な噂を流す行為をしたり，他人の名誉を毀損したりというものが挙げられる．

2. 情報システムを安心して利用するにはどうすればいいのだろうか
情報システムを安全に利用するためには，情報セキュリティが必要である．
情報セキュリティ：情報の機密性・完全性・可用性を確保すること

しかし，現実的に全てを最大限に確保することはできない．例えばパスワードをいちいち難解なランダムな記号にしても覚えることはできないし，一人一人を認証しようとしても莫大な人員が必要となるからである．よって情報セキュリティは運用コスト，導入コストを考慮して重要度を考える必要がある．また，真正性，責任追跡性，信頼性，否認防止の 4 要素を加えて情報セキュリティの 7 要素という．これらの実現には，パスワードをたくさんの種類の文字を用いることにより，他者から容易に推測できないようにすることや，他者がアクセスできる箇所にパスワードを保存しないようにすることなどが必要である．

安全なパスワード	危険なパスワード
・個人情報から推測できない	・Yukinori など個人情報から推測できるもの
・英単語などをそのまま使用していない	・apple など辞書に普通に載っている単語
・アルファベットと数字が混在している	・aaaaa などの同じ文字の繰り返しや 0123 などのわかりやすい並びの文字列
・適切な長さの文字列	・pass1 など短すぎる文字列
・類推しやすい並び方やその安易な組み合わせでない	・yukinori2023 のように類推しやすい文字列の組み合わせ

ネット上でのサービスが多くなり，登録する認証情報が増加しているため，複数のサービスで同じパスワードを使い回すことがあるが，他のサービスから情報が漏れた際に別のサービスにも不正ログインされてしまう可能性があるため，それぞれのサービスで異なるパスワードを使うことが望ましい．また，定期的にパスワードを変更することによってもそのような事態に備えることができる．また，サービスによっては生体認証や二要素認証の導入が進んでいる．

生体認証：人間の身体的特徴や行動の癖などを用いて行う個人認証技術のこと
　　例：指紋，声紋，虹彩，静脈，顔認証や歩き方など
二要素認証：知識情報．所持情報，生体情報のうちの二つを組み合わせて行う認証のこと

3.　セキュリティを確保するために必要なことを考えよう
コンピュータウイルスはインターネットが普及する前から存在しており，ネットワークが普及する前はフロッピーディスクなどを媒体としていた．しかし，ネットワークが発達した現在では，インターネットを通して侵入するものが多い．

コンピュータウイルス：第三者のプログラムやデータベースに対して意図的に何らかの被害をもたらすように作られたプログラムのうち，自己伝染機能，潜伏機能，発病機能のうちの一つ以上を備えるもの．
マルウェア：コンピュータに入り込んで不正行為を行う悪意のあるプログラム
※マルウェアも広義ではコンピュータウイルスに当たる．

マルウェアはファイルやシステムに悪い影響を与え，データ漏洩の原因になることがある．
具体的には，トロイの木馬，ワーム，狭義のウイルスがマルウェアに当てはまる．

種類	特徴
トロイの木馬	無害なソフトウェアになりすまして存在し，自己増殖しない
ワーム	独立して活動し，自己増殖する
狭義のウイルス	他のファイルに寄生して活動し，自己増殖する

コンピュータウイルスに対する対策としては，ウイルス対策ソフトウェアの導入と，OS やアプリケーションを最新の状態に保つということが効果的である．また，ファイアウォールを導入し，ネットワークへの不正侵入を防ぐことも有効な手段である．
ファイアウォール：コンピューターやネットワークを，外部からの不正な侵入から守るための防御システム。ファイアウォールは英語の防火壁から名が来ている．

1. 組織としての対応

基本的にどのような方針でセキュリティを確保するのかを組織内で共有し，それを守る必要がある．基本方針は，なぜ情報セキュリティが必要か，をはっきりさせ，責任の所在や情報資産について明確にする．それをもとに，対策基準を作り，その中では，何を実施するのか，そして実施手順としては，どのように実施するのか，を取り決める必要がある．また，常に改善していくという心構えが必要である．

2. 個人としての対応

個人に対して，他者になりすましたメールが送られてきたり，ウイルスが添付されたメールが送られてきたりすることがある．組織としてそのようなメールを開かないなどのルールを決めることや，怪しいメールをチェックするツールなどを導入することも必要だが，個人としてもそのような悪意あるメールが送られてくる可能性があることを理解しておくことが必要である．パスワードなどの情報を偽サイトに誘導することにより盗む手法やゴミ箱を漁ってパスワードや IP アドレス一覧などの機密情報を盗み出す手法など多種多様な手法がある．

また，公衆無線 LAN いわゆるフリーWi-Fi が最近街中に増えてきているが，無線 Wi-Fi の性質上通信内容が盗み見られることがあるということを理解しておく必要がある．また，悪意の第三者が公開無線 LAN を設置していることもあるため，信頼できる機関, 企業の無線 LAN かどうかを確認する必要がある. また, 無線 LAN の暗号化技術は進化しているが，古いものを使っている場合だと暗号が一瞬で解読される可能性もあるため，できるだけ最新の暗号方式を利用すべきである．公衆無線 LAN を利用する際には，できるだけ自分の情報が特定されにくい状態にし，大切な情報や機密性の高い情報などの送受信には使用しないなどの対策が必要である．