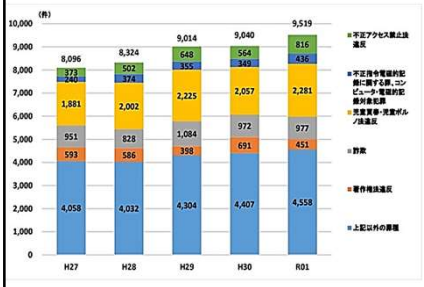
サイバー犯罪の現状 2015-2019(h27-r01)・他

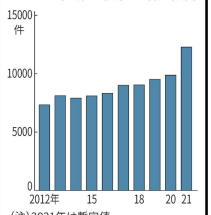
pp.16-17,25

サイバー犯罪の検挙件数の推移
（警察庁の発表資料より）



https://www.nikkei.com/article/DGXMZO56548840Z00C20A3000000/

サイバー犯罪の検挙は増加傾向



(注)2021年は暫定値
(出所)警察庁

サイバー犯罪に関する相談の推移

サイバー犯罪

pp.16-17,25

サイバー犯罪：ネットワークやコンピュータを悪用した犯罪。

サイバー攻撃とはサイバー犯罪を実行する具体的な手段を指す。

※ 安全対策の詳細は，第4章で。

種 類（一部の例）	例（下記も一例に過ぎない。これら以外にもさまざま…）
不正なアクセス	• 他人のユーザID，パスワード等を不正に利用する行為
データの改ざん	• 金融機関等のコンピュータを不正に操作し，無断で他人の口座から自分の口座に預金を移す行為 • ウェブページの改ざん
ネットワークを利用した詐欺や不正コピー	• ネットショッピングやネットオークションでの詐欺 • 映画や音楽などの不正コピーを販売したり広めたりすること

情報セキュリティの３大要素

pp.16-17

情報セキュリティ　コンピュータやネットワークを危険から守る

機密性 Confidentiality　特定人物のみにアクセス権限を許可すること
（不正アクセスや情報の漏えいがない）
• 対策例：**IDと<u>パスワード</u>**，**<u>生体認証</u>**等による<u>ユーザ認証</u>，暗号化等

完全性 Integrity　情報が正確かつ完全な状態で保持されること
（改ざんされていない・間違っていない）
• 対策例：<u>デジタル署名</u> 等

可用性 Availability　必要時に確実・安全に情報へのアクセスができる
（紛失・破損・システム障害等がない，障害復旧が高速）
• 対策例：ネットワーク回線・データ等の<u>二重化</u>，データ<u>バックアップ</u> 等

機密性の具体例を，少しだけ紹介しよう。　対策も含めた具体的説明は2学期以降。4章で！

機密性攻撃(認証突破)方法の例

pp.16-17,25

不正アクセス(クラッキング)：**サイバー攻撃**の一種
• **脆弱性**(セキュリティホール)を突いたり**マルウェア**を利用したり。
※ サイバー攻撃：ネットワーク上のコンピューターシステムへの破壊活動・データ窃取・改竄等

● **キーロガー**(入力履歴を記録するソフトやハード)　スパイウェアの一種…
• ネットカフェ等の不特定多数が使用するPCで注意！

● **ソーシャルエンジニアリング**（社会工学的手法）
• 話術，盗み見，盗聴等で保安上重要な情報を入手する。

● **スキミング**(読み取り装置を**スキマー**という)
• 磁気カード(クレジットカード等)の情報を複製してしまう。

機密性を保つ対策１　ユーザ認証(個人認証)

pp.16-17

● **ブルートフォース攻撃**(brute force attack)
「総当たり攻撃」ともいう。暗号やパスワードを解読する方法のひとつ。
成功するまで順に，すべての文字列を試していけば必ず解読できる。
例えば暗証が数字４桁の場合，１万通りである。
人が１万回入力するのは大変だが，プログラミングで自動化すれば**瞬時に完了**する。

● **<u>「もっとも使われた危険なパスワード」</u>**2021年版が発表！

問い：８文字でPWを作る。それぞれ何通り？
(1) 数字だけなら？　10^8＝1億
(2) 数字とアルファベット小文字なら？　36^8＝2兆8千億以上
(3) 数字とアルファベット大文字小文字なら？　62^8＝218兆以上
(4) 1秒に1000**万**パターン試した場合にPWを見つける**最長**時間は？
10秒　約3日　約8か月

機密性を保つ対策

青少年科学館より

生体認証(バイオメトリクス)：
指紋・虹彩・網膜・静脈・掌形・顔・音声等

【参考】情報社会における法律

今，全てを覚える必要はないが，少しずつ理解を！

- 知的財産基本法　2003施行
- 著作権法　1970制定，1971施行，2004・2014・2016・2018・2020・2021改正等
- 個人情報保護法　2003一部施行，2005全面施行
- 不正アクセス禁止法　2000施行
- 特定商取引法　1976制定，2000名称変更
- 特定電子メール法　2002施行，たびたび改正
- 情報公開法　1999公布，2001施行

ネットワーク犯罪（よく耳にする言葉）

pp.16-17,25

- 迷惑メール　（対策：電子メールフィルタリング等）
- ワンクリック詐欺　p.25
- 架空請求　p.25
- ネットショッピングやネットオークションの詐欺　p.25
- フィッシング（phishing）詐欺　p.16
- ファーミング（pharming）詐欺

迷惑メールの例（2022年5月20日に送信された濱宛のメール）

- 差出人：HYOGO-C.ED.JP ポータル u1@tky.3web.ne.jp
- 宛先：　s000000@hyogo-c.ed.jp　（数字000000は参考例。@以降は実例）
- 件名：　【重要】【共用】【5月20日実施】サーバーメンテナンスのお知らせ
- 日時：　Fri, 20 May 2022 07:35:28

お客様各位

2022年5月19日（水曜日

インターネットサービスをご利用いただき誠にありがとうございます。
メールアドレスは【s000000@hyogo-c.ed.jp】で、削除のフラグが付けられています。
サービスの詳細は以下のURLをご参照ください。
http://support.hyogo-c.ed.jp.1stguardinguk.co.uk/bitdrive?uid=s000000@hyogo-c.ed.jp
お客様にはご迷惑をお掛け致しますが、ご了承くださいますようよろしくお願い申し上げます。
何とぞご理解ご了承の程、よろしくお願いいたします。
引き続き変わらぬご愛顧を賜りますようお願い申し上げます

Hyogo-c NET　お客さまサービスセンター

補足：広告メールに関する規制の流れ

- 広告メールが増加
- オプトアウト方式（拒否後再送禁止）・・・この方式問題あり
  （特定電子メール法 2002年施行）
- タイトルに「未承諾広告※」の表示が必要
  （特定商取引法 2002年改正）
- オプトイン方式（事前同意必要）
  （特定電子メール法 2008年改正）
- しかし，イタチごっこ

迷惑メールの一般的な対策

- **メールに返信や転送をしない。**
  例：一方的に送られたメールに「配信停止を希望される場合は返信して下さい」等と記載されているケースがあるが，返信すると実在するアドレスだと判断されて被害が拡大する可能性がある。
- **メールを開封しない。添付ファイルも開封しない。**
- **メール本文中のURLにアクセス(クリック)しない。**
  例：フィッシングサイトの場合あり。「同意した」等と表示⇒料金を請求。
  悪質なプログラムが埋め込まれたWebサイトへ誘導される場合もあり。
- **メールアドレスは，ホームページ等で公開しない！**
- **推測しにくいメールアドレスを利用する！**
  英字と数字を組み合わせて，推測されにくい長めのアドレスにする等の工夫を。
- **被害が拡大した場合は，メールアドレスを変更！**
  様々な対策を施しても迷惑メールが増えて支障が出る場合の最終手段。
  他者への変更通知に大変な労力がかかるが・・・。
- **迷惑メール対策(メールフィルタ,メール検知,メール遮断システム等)。**

マルウェア（コンピュータウイルス）の概要

情報セキュリティの3大要素すべてに悪影響を及ぼす！

マルウェア（コンピュータウイルス）とは？
- 悪意をもって作られたプログラム(malicious software)。
- データやプログラム，電子メール，Webページ，USBメモリ等から広がる。

マルウェアの機能
① 自己伝染機能：　他のシステムに自らの機能をコピーすること
② 潜伏機能：　ある時期まで，被害を及ぼさずに待機すること
③ 発病機能：　被害を及ぼす動作（ファイル破壊,データ流出,機能低下等）

マルウェアの分類（厳密な分類はない）

マルウェア（広義のウイルス）	ウイルス(狭義)	ファイルに寄生（例：マクロウイルス）
	ワーム	単独のファイルとして存在
マルウェア（広義のウイルス）	トロイの木馬 / スパイウェア / ボット	等

スパイウェア↑は一般に上記①の機能をもたない