

# 情報セキュリティと情報倫理

## 第6回

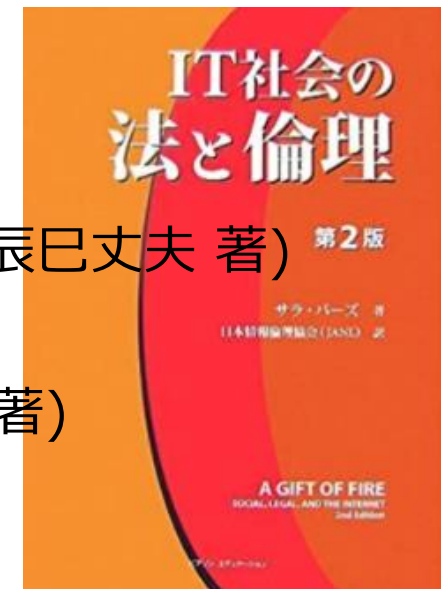
### ウィルスと不正アクセス技術

(教科書： 2 サイバー犯罪とマルウェア)

2022/11/4

# 概要

- 全学共通科目 1 年生後期
- 金曜日 5 時限 (16:10-17:40)
- 担当 :
  - 梶田秀夫・永井孝幸・森真幸 (情報科学センター)
- 評価方法 (予定)
  - 毎回のミニレポート (20%)
    - 講義ビデオを前提とした課題内容 (予定)
  - 1 回程度の課題レポート (30%)
  - 期末テスト (50%)
- **参考書** : 情報セキュリティと情報倫理 (山田恒夫 辰巳丈夫 著) 第2版
  - ISBN978-4-595-31897-9 C1355 ¥2600E
- 参考書: IT社会の法と倫理 第二版 (サラ・バーズ 著)
  - ISBN978-4-89471-430-4 C3032 ¥3900E



## 第6回

# ウィルスと不正アクセス技術 (教科書：2 サイバー犯罪とマルウェア)

# ウィルスと不正アクセス技術

## • シラバスより

- コンピュータウィルスおよびコンピュータワームの実例とそれらが利用している技術, 不正アクセスの実例とその技術について議論する.

## • 目標・ポイント

- インターネットの一般利用者の立場に立ってサイバー犯罪とは何かを理解する.  
次に, それらの犯罪から身を守るために, マルウェアの種類や感染経路を学習し, パソコンやネットワークを利用・管理する際の注意点を考える.

# サイバー犯罪

# サイバー犯罪とは

- コンピュータを利用した犯罪の総称
  - クレジットカード番号を盗み取られて不正利用された
  - 自宅のパソコンがウイルスに感染して機密情報が流出した
  - 中高生が出会い系サイトを使って犯罪に巻き込まれた
- 知能犯（窃盗，詐欺，横領，背任，偽造）
  - コンピュータ技術の進歩に伴う新しい手口

# サイバー犯罪の分類

- 不正アクセス行為の禁止等に関する法律違反
- コンピュータ・電磁的記録対象犯罪
- 不正指令電磁的記録に関する犯罪
- ネットワーク利用犯罪

# 不正アクセス行為の禁止等に関する法律違反

- 不正アクセス行為の禁止等に関する法律  
(通称：不正アクセス禁止法)

- 2000年に施行

- これに違反する犯罪

- コンピュータの欠陥を利用して、アクセス権限がないはずのコンピュータを利用

- フィッシング詐欺

- 不正アクセスのために他人のIDやパスワードを取得する行為
- 2013年の不正アクセス禁止法の改正で禁止行為となった



# コンピュータ・電磁的記録対象犯罪

- 1987年に刑法に新設
- 電子計算機損壊等業務妨害罪
  - コンピュータやデータの損壊
  - 虚偽のデータや不正なプログラムで業務を妨害
- 電子計算機使用詐欺罪
  - 虚偽のデータや不正なプログラムで事実でない記録データを作成し，財産上不法な利益を得る犯罪

# 不正指令電磁的記録に関する犯罪

- 2011年の刑法改正で新設
- コンピュータウイルスに関する犯罪
  - 他人のパソコンの動作不良を起こさせたり，データを破壊するために，ウイルスを作成し保存することやインターネット上にばらまくこと

# ネットワーク利用犯罪

- 犯行の手段としてコンピュータネットワークを利用する犯罪
  - インターネットでの詐欺行為
  - 出会い系サイトやSNSを使った犯罪
  - 電子掲示板などで犯罪予告
  - Webページ上で人を侮辱したり誹謗中傷
  - 違法な猥褻画像や映像を不特定の人に閲覧させる

# ウイルス届け出件数とその傾向

## 情報セキュリティ

### コンピュータウイルス・不正アクセスに関する届出について

最終更新日：2021年8月23日  
独立行政法人情報処理推進機構  
セキュリティセンター

1990年4月に通商産業省(※1)が告示した「コンピュータウイルス対策基準」(※2)、および「コンピュータ不正アクセス対策基準」(※3)に基づき、IPAでは国内のコンピュータウイルス(以下、ウイルス)の感染被害やコンピュータ不正アクセス(以下、不正アクセス)被害の届出を受け付けています。

ウイルス感染被害の拡大や再発の防止、不正アクセス被害の実態把握と同様の被害発生防止に役立てるため、届出にご協力をお願いします。

(※1) 2001年1月6日より、通商産業省は経済産業省に移行しました。

(※2) URL : <https://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm>

(※3) URL : <https://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm>

#### 届出方法(ウイルス発見・感染)

#### 情報セキュリティ

##### > 脆弱性対策情報

##### > 届出・相談・情報提供

##### > ウイルスの届出

##### > 不正アクセスの届出

##### > 脆弱性関連情報の届出

##### > 情報セキュリティ安心相談 窓口

##### > 標的型サイバー攻撃の特別 相談窓口

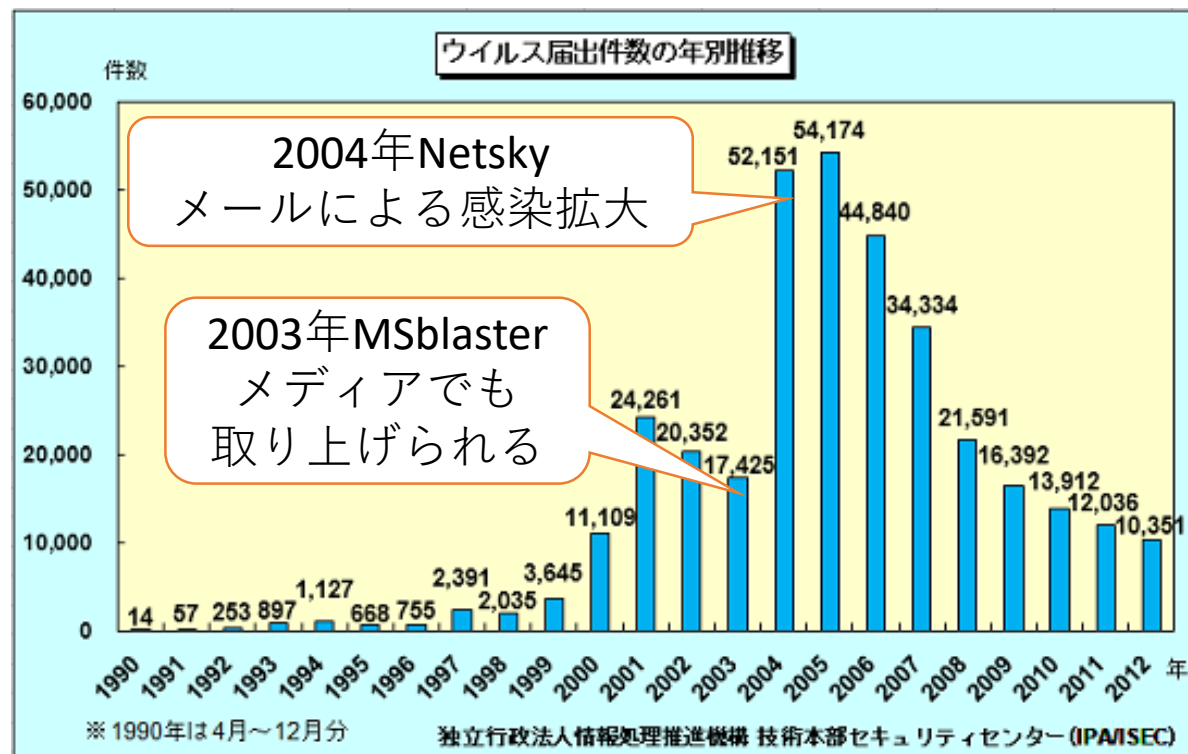
##### > 情報提供受付

##### > 特集コンテンツ

##### > 情報セキュリティ啓発

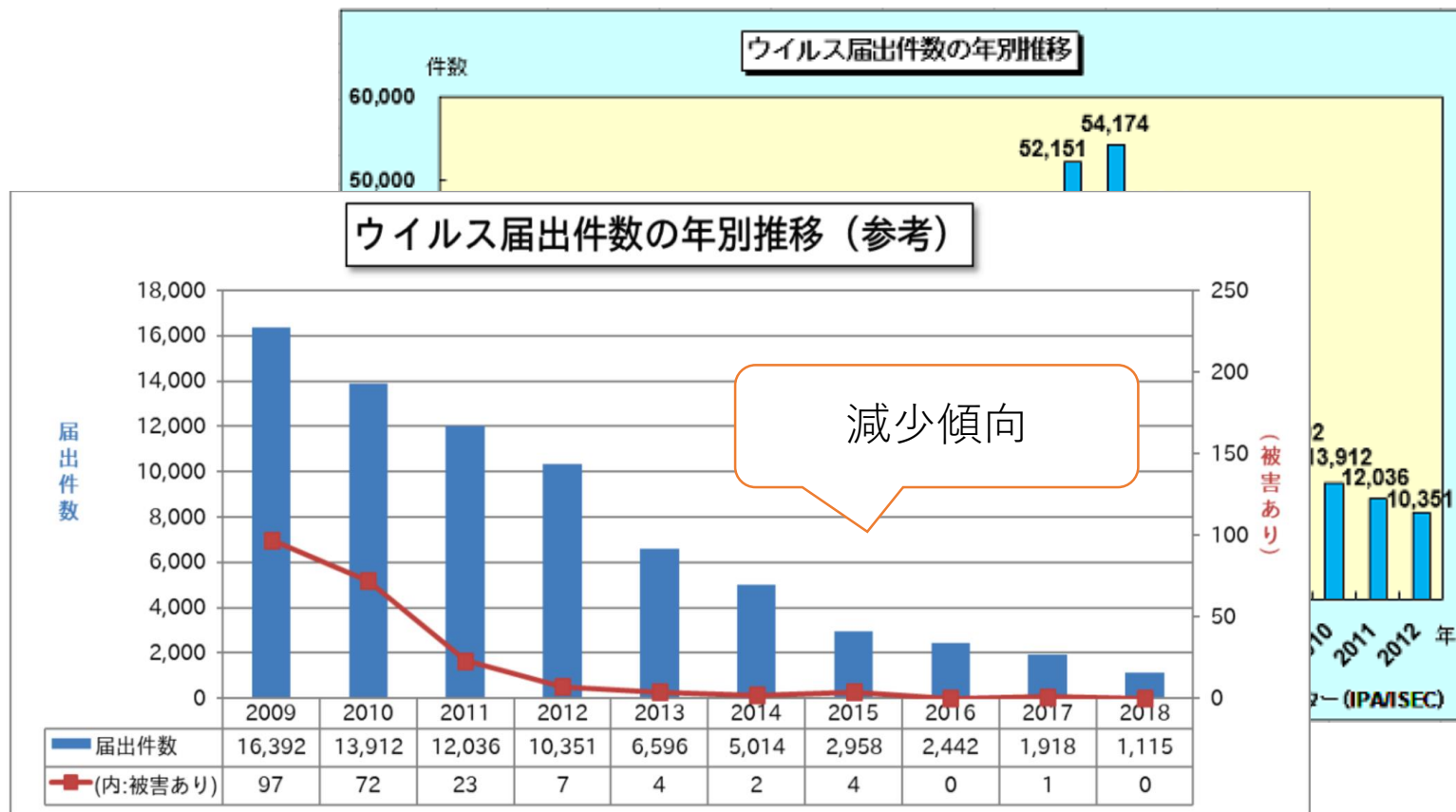
##### > 情報セキュリティ対策

# ウイルス届け出件数の年間推移



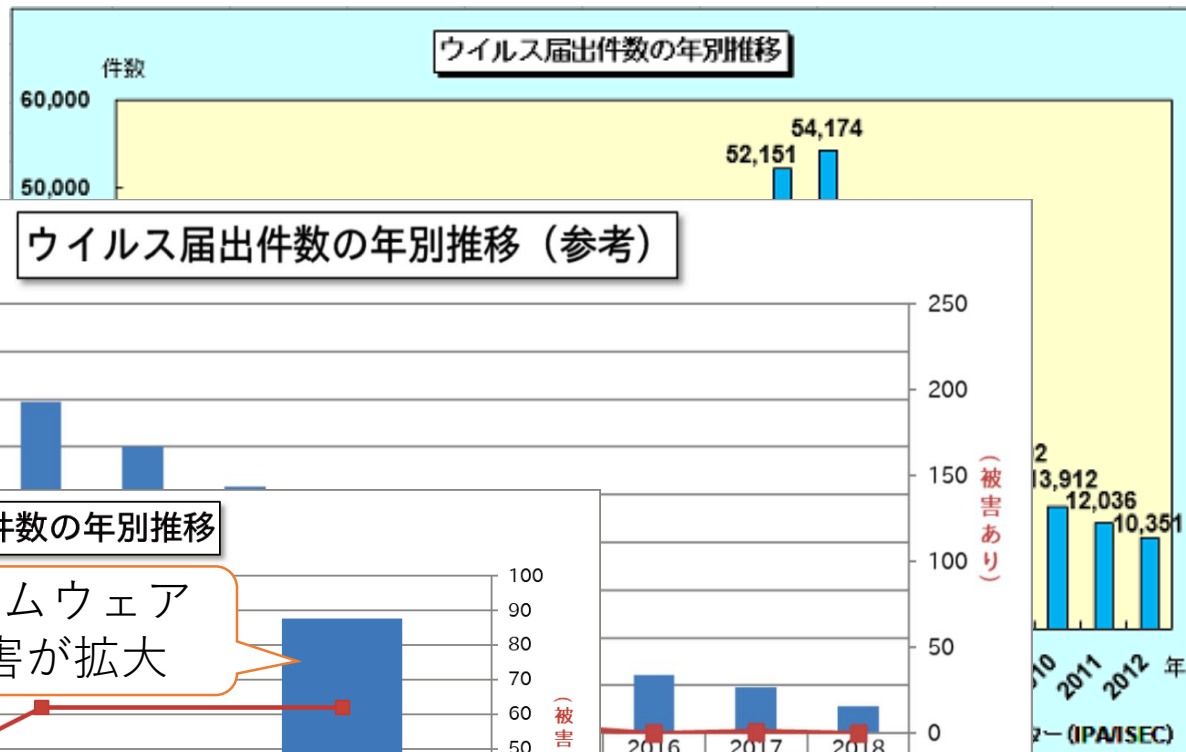
<https://www.ipa.go.jp/security/outline/todokede-j.html>

# ウイルス届出件数の年間推移



<https://www.ipa.go.jp/security/outline/todokede-j.html>

# ウイルス届出件数の年間推移

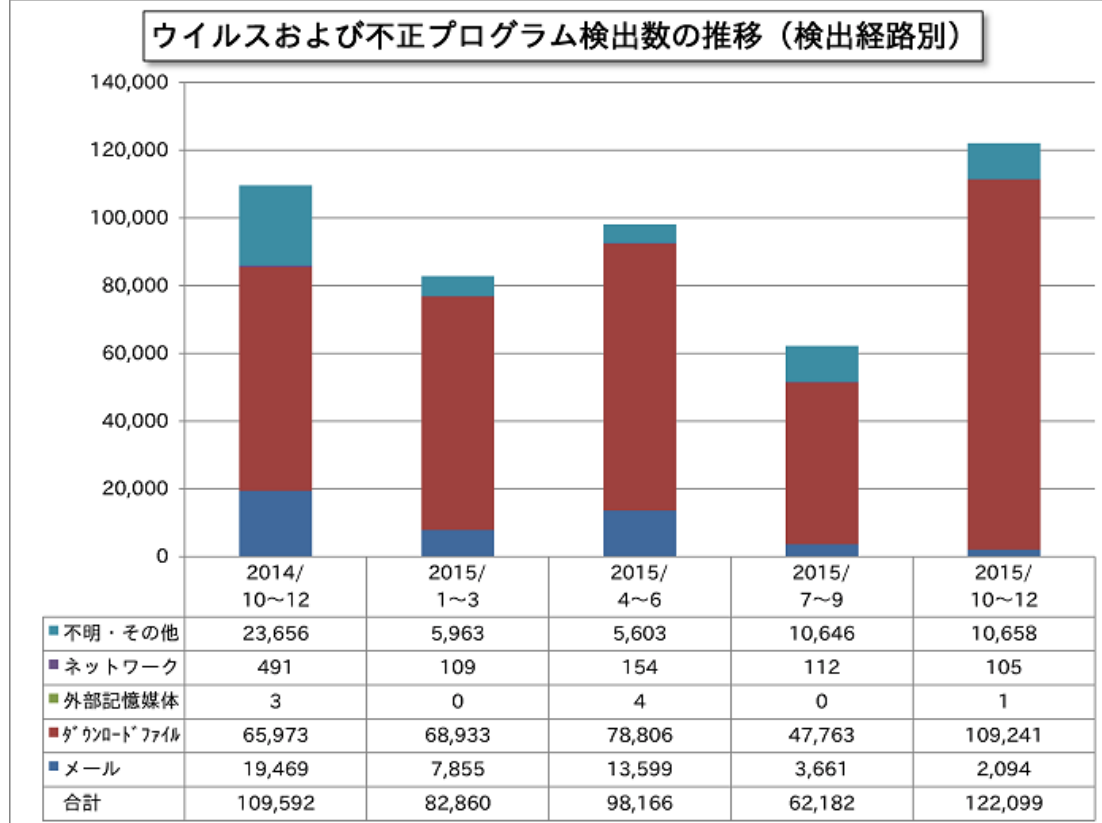


\* 2019年より集計方法が異なる

<https://www.ipa.go.jp/security/outline/todokede-j.html>



# ウイルスおよび不正プログラムの検出経路



<https://www.ipa.go.jp/security/txt/2015/q4outline.html>

<https://www.ipa.go.jp/security/txt/2016/q4outline.html>

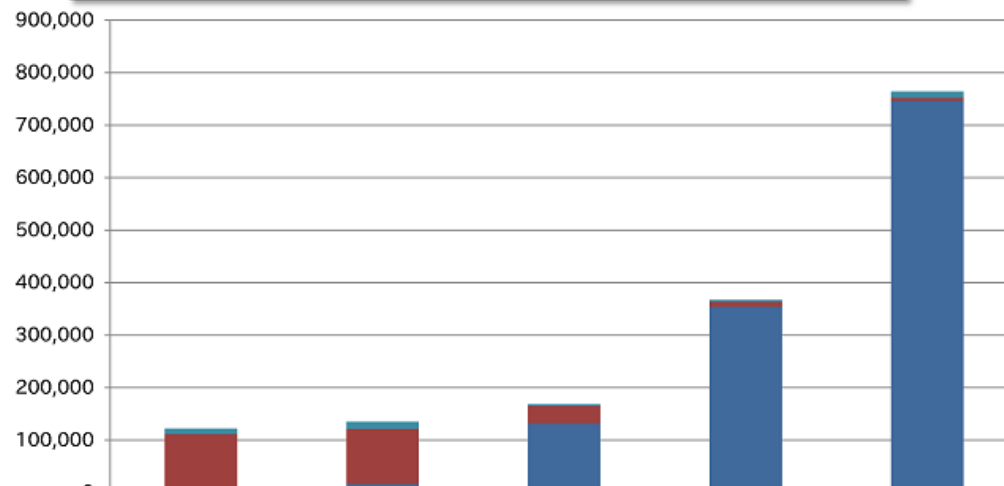
<https://www.ipa.go.jp/security/outline/todokede-j.html>

# ウイルスおよび不正プログラムの検出経路

ウイルスおよび不正プログラム検出数の推移（検出経路別）



ウイルスおよび不正プログラム検出数の推移（検出経路別）



不明・その他	10,658	13,839	3,072	3,634	11,818
ネットワーク	105	79	31	614	592
外部記憶媒体	1	1	1	0	3
ダウンロードファイル	109,241	105,006	34,027	8,870	5,832
メール	2,094	16,293	131,599	354,208	746,035
合計	122,099	135,218	168,730	367,326	764,280

2015/7~9	2015/10~12
10,646	10,658
112	105
0	1
47,763	109,241
3,661	2,094
62,182	122,099

<https://www.ipa.go.jp/security/txt/2015/q4outline.html>

<https://www.ipa.go.jp/security/txt/2016/q4outline.html>

<https://www.ipa.go.jp/security/outline/todokede-j.html>

# ウイルスおよび不正プログラムの検出経路

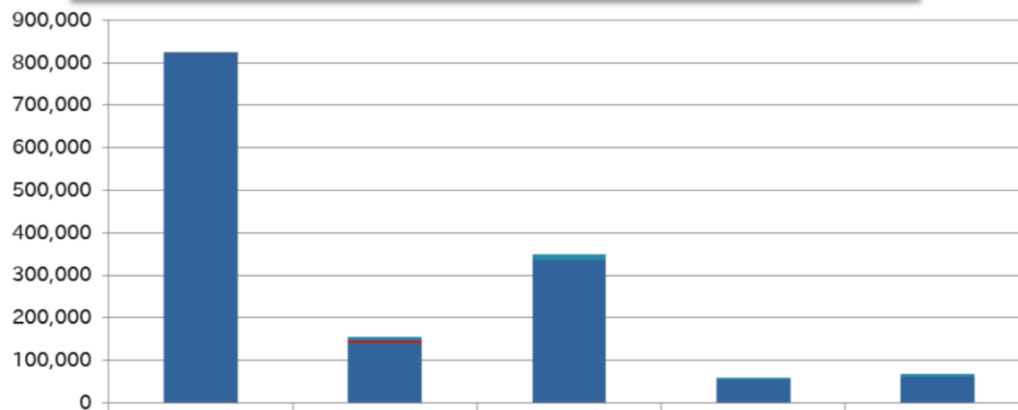
ウイルスおよび不正プログラム検出数の推移（検出経路別）



ウイルスおよび不正プログラム検出数の推移（検出経路別）



ウイルスおよび不正プログラム検出数の推移（検出経路別）



	2017/ 10~12	2018/ 1~3	2018/ 4~6	2018/ 7~9	2018/ 10~12
■ 不明・その他	3,281	5,973	14,334	2,840	6,892
■ ネットワーク	1,139	2,213	579	447	341
■ 外部記憶媒体	3	0	0	1	0
■ ダウンロードファイル	1,115	8,606	589	365	258
■ メール	820,029	138,417	334,732	54,608	61,180
合計	825,567	155,209	350,234	58,261	68,671

	2016/ 7~9	2016/ 10~12
不明・その他	3,634	11,818
ネットワーク	614	592
外部記憶媒体	0	3
ダウンロードファイル	8,870	5,832
メール	354,208	746,035
合計	367,326	764,280

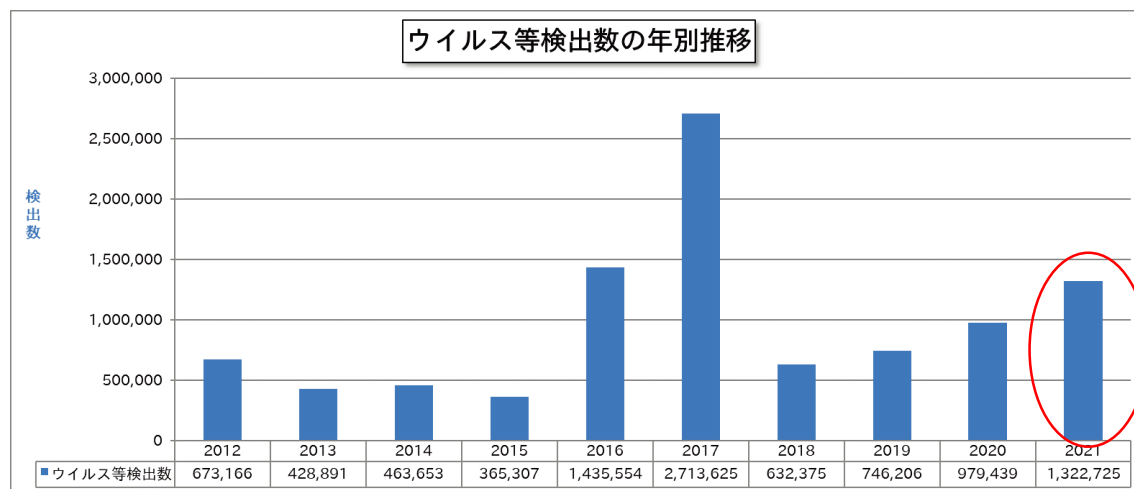
	2015/ 7~9	2015/ 10~12
不明・その他	10,646	10,658
ネットワーク	112	105
外部記憶媒体	0	1
ダウンロードファイル	47,763	109,241
メール	3,661	2,094
合計	62,182	122,099

<https://www.ipa.go.jp/security/txt/2015/q4outline.html>

<https://www.ipa.go.jp/security/txt/2016/q4outline.html>

<https://www.ipa.go.jp/security/outline/todokede-j.html>

# ウイルスおよび不正プログラムの傾向



## • 2021年の検出数

- 前年より約35%増加(2年連続3割越)し、1,322,725個
- Emotet と呼ばれるウイルスの検知・感染被害の届出が年間を通じて寄せられた
- Emotet
  - 2019年ごろに猛威を振るったコンピュータウイルス
  - 2021年1月に欧州刑事 警察機構 (Europol) を中心とした活動により、攻撃基盤の停止に成功 → **その後、活動再開**

<https://www.ipa.go.jp/files/000088692.pdf>

# コンピュータウイルス

# コンピュータウイルス

- コンピュータを操作する人の意図に反して悪意ある動作をさせる
- 総称 マルウェア
  - ワーム
  - ボット
  - スパイウェア など
- 狭義のコンピュータウイルス
  - ワードプロや表計算ソフトなどのファイル, あるいはUSBフラッシュメモリなどリムーバブルメディアに寄生
- 広義のコンピュータウイルス
  - 寄主が不要で単体で動作「トロイの木馬」

# ワーム(worm)

- 寄生するファイルを必要とせずに，不要で単体で活動できる形態プログラム
- ウイルスと同様の不正な動作
  - データの改ざんや流出
  - メール送信
  - システムファイル破壊
  - 他のコンピュータへの攻撃

# ボット(bot)

- ロボットのようなプログラム

- インターネットを通じて別のコンピュータから操作されるか、自身でインターネット上の特定の掲示板などに書かれた指令を参照し動作する

- 被害例

- サーバのサービスを不能にするDoS (Denial of Service) 攻撃
- スパムメールの送信

- ボットネット 教科書p32

- ボットに感染したコンピュータ群に対して攻撃を指令するコンピュータをあわせネットワーク化したもの
- 多数のコンピュータが攻撃の踏み台に



# スパイウェア(spyware)

- キーボード入力やマウス操作, 画面そのものなどを記録し, あるいはひそかに送信する
- 被害例
  - 利用者認証時のID, パスワードやクレジットカードの番号, PINコードなどの外部への送信
  - 情報漏洩

# アドウェア

- 広告を表示する

- ある機能を持ったソフトウェアを提供する対価に広告を見せる様式のもので、それ自体に不正な要素はない
- ただし、偽ショッピングサイトへの誘導や、告知なしにユーザの情報を収集するような機能を持つ場合は、広義のスパイウェアに該当する

# クラッキングツール(ルートキット rootkit)

- ワームやボットなど，侵入した不正プログラムが利用するプログラム群
- OSの一部を書き換えてバックドア(裏口)を作り，外部から侵入しやすくするなど

# ウイルスの種類

- 商用サイトでの情報

- <https://www.mcafee.com/jp/threat-center.aspx>
- <https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/>

# 情報処理推進機構(IPA) 新種ウィルス情報

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 1999年

- 2月24日掲載  W32/Ska (Happy99)
- 4 月 8日掲載 W97M/Melissa
- 4月15日掲載 W32/CIH
- 6月17日掲載 W32/ExploreZip
- 10 月 8日掲載 W32/PrettyPark
- 11月12日掲載 VBS/BubbleBoy
- 12月28日掲載 W32/Fix2001

<https://www.ipa.go.jp/security/topics/newvirus/newvirus-top.html>

<https://www.ipa.go.jp/security/txt/list.html>

# 情報処理推進機構(IPA)：新種ウィルス情報

- 2000年

- 1 月 8日更新 VBS/LOVELETTER (掲載2000年, 更新2002年)
- 7月24日更新 VBS/Stages
- 10月31日更新 W32/QAZ
- 11 月 9日更新 W32/MTX

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2001年

- 1月8日更新 W32/Zoher (掲載 2001年 更新 2002年)
- 1月8日更新 W32/Maldal (掲載 2001年 更新 2002年)
- 1月8日更新 W32/Nimda (掲載 2001年 更新 2002年)
- 1月8日更新 W32/Magistr (掲載 2001年 更新 2002年)
- 1月8日更新 W32/Apost (掲載 2001年 更新 2002年)
- 1月8日更新 W32/Sircam (掲載 2001年 更新 2002年)
- 1月8日更新 W32/Badtrans (掲載 2001年 更新 2002年)
- 1月8日更新 VBS/Haptime (掲載 2001年 更新 2002年)
- 1月8日更新 VBS/Homepage (掲載 2001年 更新 2002年)
- 1月8日更新 VBS/SST (AnnaKournikova) (掲載 2001年 更新 2002年)
- 1月8日更新 W32/Hybris (掲載 2001年 更新 2002年)
- 1月11日更新 W32/Aliz (掲載 2001年 更新 2002年)
- 1月15日更新 W32/Navidad (掲載 2001年 更新 2002年)
- 3月28日更新 W32/Badtransの亜種 (掲載 2001年 更新 2002年)
- 5月31日更新 W32/Klez (掲載 2001年 更新 2002年)
- 8月16日更新 W32/CodeRed



# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2002年

- 1月29日掲載 W32/MyParty
- 3 月 8日掲載 W32/Gibe
- 3月15日更新 W32/Fbound
- 5月31日更新 W32/Klezの亜種
- 7月18日更新 W32/Frethemの亜種
- 10 月 8日更新 W32/Bugbear
- 11 月 8日掲載 W32/Opaserv
- 11月12日掲載 W32/Brid

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2003年

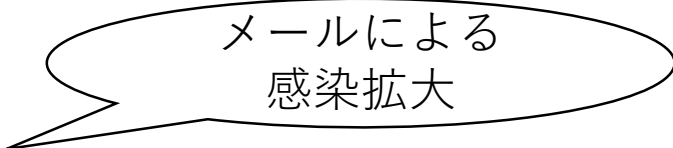
- 1月16日掲載 W32/Sobig
- 1月31日更新 W32/SQLSlammer worm
- 2月 7日掲載 VBS/Redlof
- 2月25日更新 W32/Welchia (掲載 2003年 更新 2004年)
- 2月25日更新 W32/**MSBlaster** (掲載 2003年 更新 2004年)
- 3月13日掲載 W32/Deloder
- 3月25日掲載 W32/Lovgate
- 5月14日更新 W32/Fizzer
- 5月28日更新 W32/Sobigの亜種 (別名：W32/Palyh)
- 6月 9日更新 W32/Bugbearの亜種
- 8月22日掲載 W32/Sobigの亜種 (Sobig.F)
- 9月22日更新 W32/Swen
- 12月 3日掲載 W32/Mimailの亜種

メディアで大きく  
取り上げられる

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2004年

- 1月21日掲載 W32/Bagle
- 1月29日更新 W32/Mydoom
- 2月18日掲載 W32/Bagleの亜種
- 3月3日更新 W32/Netskyの亜種
- 3月22日更新 W32/Bagleの新しい亜種
- 4月6日更新 W32/Netskyの亜種(Netsky.Q)
- 5月7日更新 W32/Sasser
- 6月16日掲載 W32/Zafiの亜種
- 8月17日掲載 W32/Mydoomの亜種 (Mydoom.S, Mydoom.Q, RatOS)



メールによる  
感染拡大

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2005年

- 4月12日掲載 W32/Mytobの亜種
- 8月18日更新 W32/Zotob
- 8月18日更新 W32/IRCbot
- 8月19日掲載 W32/Bobaxの新しい亜種
- 11月24日掲載 W32/Soberの亜種

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2006年

- 1月 更新 W32/Feebs
- 2月 更新 W32/Rontokbro, W32/Sality, W32/Honk, OSX/Inqtana,
- 4月 更新 W32/**Antinny**の亜種, W32/Areses, W32/Tufik, W32/Olmi, W32/Kidala, W32/Bhound, W32/Scanbot
- 5月 更新 W32/anwarum
- 6月 更新 W32/Ranchneg, W32/Looked, W32/Sixem, W32/Bacterra, JS/Yamanner
- 8月 更新 W32/Stration, W32/Womble, W32/Virut
- 9月 更新 W32/Naras
- 10月 更新 W32/Wikedir, W32/Bacalid
- 11月 更新 W32/bodgy, W32//Chiton
- 12月 更新 W32/Fujacks, W32/Nuwar, W32/Dzan, W32/Kraze

ファイル共有ソフトウェアを介した感染

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2007年

- 1月 更新 W32/Allapple, W32/Madangel, W32/Koddro, W32/Lewor
- 2月 更新 W32/Zhelatin, W32/Fukustog, W32/Rahack, W32/Detnat, W32/Bustoy, W32/Sohanad,
- 3月 更新 W32/Rinbot, W32/Vutsog, W32/Huegone, W32/Piggi, W32/Lunalight, VBS/Solow
- 4月 更新 W32/Almanahe, W32/Resik
- 5月 更新 W32/Validin, W32/Uisgon, W32/Whybo
- 7月 更新 W32/Wuke, W32/Dotex, W32/Gammima, W32/Fakerecy
- 8月 更新 W32/Resourcer, W32/Gexin, W32/Mumawow, W32/Hitapop, W32/Xirtam
- 9月 更新 W32/Autorun, W32/Neeris, W32/Expiro, W32/Kespo, W32/Reyds, W32/Vispat, VBS/Lido
- 10月 更新 W32/Grum, W32/AHKHeap, W32/Winko
- 11月 更新 W32/Knight, W32/Scrimge
- 12月 更新 W32/Blastclan, W32/Kalel, W32/Niuniu

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2008年

- 1 月 更新 W32/Imaut, W32/Kaxela, W32/Polip, W32/Trats
- 2 月 更新 W32/Joydotto, XF/Helpopy
- 3 月 更新 W32/Mabezat
- 4 月 更新 W32/Blune, W32/Dizan, W32/Dronzho
- 5 月 更新 W32/Selex, W32/Nomvar
- 6 月 更新 W32/Saros, VBS/Mondezimia
- 7 月 更新 W32/Uporesc
- 8 月 更新 W32/Agist, W32/Niumu
- 12 月 更新 W32/Downad, W32/Flob

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2009年

- 1月 更新 W32/Harakit, W32/Pinit, W32/Waledac
- 2月 更新 W32/Mercel
- 6月 更新 X97M/Ecmetsys
- 8月 更新 W32/Induc
- 10 月 更新 W32/Toal, W32/Palevo
- 11 月 更新 W32/Koobface



# 情報処理推進機構(IPA)：新種ウィルス情報

- 2010年

- 7月 更新 W32/Slugin
- 8月 更新 W32/Stuxnet, W32/Blakcont
- 11 月 更新 W32/Ramnit, W32/Changeup

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2011年

### スマホのウィルスの増大

- 3月 更新AndroidOS/**Lotoor**
- 4月 更新W32/Wapomi, DIR-Byway, Diskkiller, W32/Vbsclick, WM/Spenty
- 6月 更新W32/Defo, VBS/Near, AndroidOS/**Lightdd**, AndroidOS/**Smspacem**, AndroidOS/**Smstibook**
- 8月 更新W32/Ganelp, AndroidOS/**Walkinwat**
- 9月 更新XM/Slide
- 10 月 更新W32/Vbmania
- 11 月 更新AndroidOS/**Rootcage**, W32/Morto, W32/Pykspa
- 12 月 更新Squeaker, AndroidOS/**Rooter**

# 情報処理推進機構(IPA)：新種ウィルス情報

## • 2012年

- 1月 更新 W32/Gramos, WM/Swlab
- 2月 更新 W32/Spyrat, AndroidOS/SmsSend
- 4月 更新 AndroidOS/Fakeinst, XM/Mailcab
- 5月 更新 W97M/Dotor
- 7月 更新 AndroidOS/Adware,  
AndroidOS/Fakeflash, Linux/Adore,  
W97M/Antisr1

# コンピュータウイルスの歴史

# コンピュータウイルスの歴史

- ブレインウイルス 1986年

- フロッピーディスクに感染
- ソフトウェアの不正コピーに対する警告プログラムだった

- モリスワーム事件 1988年

- インターネットを通じて拡散したワーム
- 作成者がプログラムのパラメータ値設定を誤り、予想外に大きな影響を与えた

# W97M/Melissa( メリッサ) 1999/03

- Word97/98/2000文書に感染（マクロ機能）
- メールの添付文書としてやってくる.
  - 受け手が、文書ファイルを開くと起動.
- Wordのマクロウィルス保護機能を無効にする
  - ( 警告メッセージを出なくする) .
- ツールメニューの「マクロ」の項目を無効化
  - 現在登録されているマクロの確認ができなくなる.
- Outlook (メーラー)を操作する.
  - アドレス帳の上位50件にメール送信(ウィルスつき)
  - バックグラウンドで行なうため、利用者は気がつきにくい.
- 大量のメールでシステム麻痺
  - たとえば『全社員』という項目が登録されていたら  
⇒ これも『1件』に

# VBS/LOVELETTER ( ラブレター) 2000/01

- メールの添付ファイル (スクリプトタイプ)
  - 巧妙なファイル名 「LOVE-LETTER-FOR-YOU.TXT.vbs」
- 自分自身をコピー, 自動実行の登録
  - Outlook のアドレス帳を元に再配布
  - mIRCというIRCソフト(チャット)の起動スクリプトにも感染
- チャット参加者に対して,  
LOVE-LETTER-FOR-YOU.HTM ファイルを送信
  - 拡張子が, 以下のファイルを破壊  
.vbs , .vbe , .js , .jse , .css , .wsh , .sct , .hta ,  
.jpg , .jpeg , .mp3 , .mp2

## W32/CIH ( シーアイエイチ, チェルノバイリ) 1999/4

- ファイル感染型ウイルス(.EXE ファイルに)
  - メモリに常駐
  - プログラムの実行, ファイルのコピー等で開く操作をしたプログラムファイルに感染
- ハードディスクの先頭部分を無意味なデータで上書き
  - ディスク内容がアクセス不能に
  - コンピュータによってはBIOS ROM (基幹部分)のブートブロックの内容を破壊(Intel 430TX互換のもののみ)
- 4月26日発病, 6月26日発病等の種類あり
  - 1986年4月26日チェルノバイリ原発事故



# W32/Hybris(ハイブリス) 1999/12～

- 電子メールの添付ファイルで感染

- すべての通信に利用される基本ライブラリである Wsock32.dll ファイルを書き換え
- 受信したメールや, 閲覧したWebサイトを監視
- 取得したアドレス宛にウイルス自身を添付したメールを送信
- メールソフトに依存しない

## W32/MTX (エムティエックス) 2000/8～

- 実行形式のファイルに感染
- 感染したマシンを再起動しメールを送信すると、もう1通、同じアドレスに、ウイルスを添付した件名・本文が空白のメールを送信
  - Wsock32.dllを改変
  - ウィルス対策WWWサイトとの通信を遮断
    - nii. nai. avp. f-se mapl pand soph  
ndmi afee yenn lywa tbav yman
- メール送信を妨害
  - mcafee.com\*, earthlink.\*, symantec.c\*, trendmicro\*, sophos.com\*, maple.com.\*, netsales.n\*, f-secure.c\*

# W32/Sircam (サーカム) 2001/7～

- メールの添付ファイルを介して感染

- 宛先

- Outlook, Outlook Express のアドレス帳の登録アドレス
    - 「テンポラリ・インターネット・ファイル」フォルダ (Web ブラウザのキャッシュフォルダ)にあるファイルの中から任意に取得したアドレス

- 同じアドレスに何度でも送信するため, 相手先に多大な迷惑をかける

- 10月16 日にC ドライブのすべてのファイルとディレクトリを削除. 起動時にハードディスクの未使用スペースを埋める( 回復不能に)

# W32/Nimda (ニムダ) 2001/9 (1)

- MS 社のIIS (Internet Information Server)に感染
  - IIS . . . Webサーバ
  - WWWページを改ざん (セキュリティホールについて)
- Internet Explorer で改ざんされたWWWページを見ると感染 (セキュリティホールについて)
- PC が感染すると, Outlook のアドレス帳に登録されているアドレス等にウイルスを送信
- ウイルス付メールを受け取ると, Outlook ではメールを開いただけで, OutlookExpress ではプレビューしただけで感染

添付ファイルを「実行」しなくても感染！

# W32/Nimda (ニムダ) 2001/9 (2)

- IIS (Webサーバ) を攻撃
- Web改ざん
  - ホームページをみるだけで感染
  - IEのセキュリティホールを突く
- システム改変：
  - 「登録されているファイルの拡張子は表示しない」, 「隠しファイルおよび隠しフォルダを表示しない」の設定を有効に

# W32/CodeRed (コードレッド)2001年夏～秋

- MS社のIISの脆弱性を利用して感染

- メモリ上で動作し, Webを改ざん
- インターネット上のセキュリティホールのあるIISサーバを検索, 発見するとそのマシンに侵入
- ホワイトハウス(<http://www.whitehouse.gov/>) を攻撃 (DDoS攻撃)
- バックドアプログラムをインストールする亜種(CodeRed II)

- 副作用

- ネットワーク混雑
- 他のWWWサーバも停止

# CodeRed の示した問題点

- IISのセキュリティホール

- パッチを当てていないところが多かった
- 過去にパッチを当てて障害が起こった経験も
- IISを稼働させている自覚がない
  - 勝手にインストールされるから
  - 他のサービスに付属して非自覚的に

- ファイアウォールに欠陥がないのに侵入

- ノートPCのIISが社外で感染
- (その後)社内ネットに接続

# W32/MSBlaster (エムエスブラスター)

## 2003年8月12日午前2時～

- RPCインターフェイスのバッファオーバーランによりコードが実行される脆弱性[MS03-026]がある環境で感染
  - Port 135に攻撃データを送信し, 侵入できると, ワーム本体をコピーして実行
  - 毎月16日以降または9月以降に発病
- windowsupdate.comにDoS (サービス妨害) 攻撃を仕掛ける
  - ネットワーク混雑
  - PCが異常終了/再起動を繰り返す (ウィルス自体のバグ)  
→これにより顕在化(?)



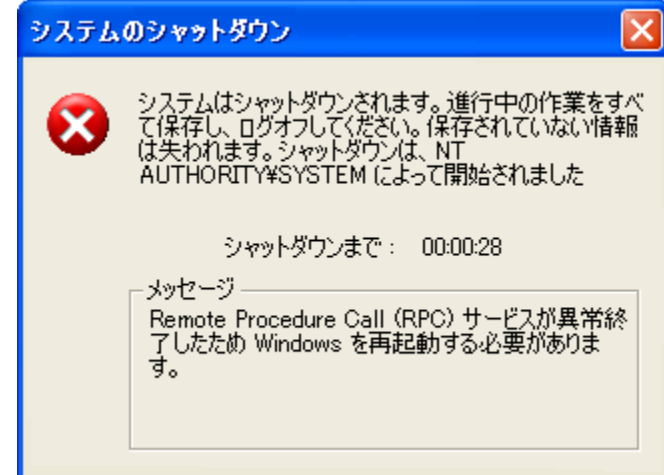
# W32/MSBlaster の示した問題点 (1)

- Windows RPCのセキュリティホール
  - (利用者が)何もしなくても感染する
    - PCをネットワークにつないで電源を入れているだけ
- RPC機能は全てのWindowsで動いている
  - 特に動作禁止しないかぎり
  - 修正パッチは公表済みだったが
- ノートPCも運搬役に
  - ファイアウォールが役に立たない
  - 日本では「お盆休み中」(だった)

## W32/MSBlaster の示した問題点 (2)

- 何もしなくても感染する
  - PCをネットワークにつないで電源を入れているだけ
- 電子メールやWWW等の手段での通知ではダメ
  - 通知を読んだ時点では感染している
- かなり大規模な被害
  - それでもマイクロソフトは動かず
- 警察庁，総務省，経済産業省の三省庁
  - 9月18日に，米マイクロソフト日本法人のマイケル・ローディング社長に対策の周知徹底を申し入れ
  - マイクロソフトが新聞広告，修正CD配布

# W32/MSBlasterの被害例



## • 2003年10月 夏休み明け

- コンピュータ系専門学校での授業中
- 注意喚起にウイルス対策ソフトウェアが必須という話をするも学生が誰も使っていないことが判明
- 動揺を治めるためトレンドマイクロのオンラインウイルススキャンを授業中に実行する事態に

## • 2003年11月 とあるイベント

- 急きょ必要になったWindows2000をイベント主催側から提供された有線LANに接続したままインストール
- インストール完了後、最初のログイン画面を待たずに感染
- 以後再起動を繰り返す

# W32/Netsky ( ネットスカイ) 2004/02

- メールの添付ファイルとして拡散
- 感染時に, Windowsのシステムファイルを改変 (services.exe)
- メールの添付ファイルを開いたとき, 偽のエラーメッセージを表示
  - 感染したことに気付かせないように
- 「share」「sharing」という単語を含むフォルダ名を検索し, 発見したフォルダに自分自身をコピー
  - ファイル共有も利用して拡散

# W32/Sasser（サッサー） 2004/05 ～

- Windows の脆弱性[MS04-011]を利用して感染
- ファイル共有が餌食に
- ポート445（ファイル共有サービス）を通じて侵入し、ワーム本体をコピー
  - 感染対象のコンピュータを任意に検索し、感染拡大を試みる

# W32/Mytob (マイトブ) 2005/05～

- メールの添付とネットワーク共有で感染拡大
- バックドアを仕掛け, 外部からパソコン内のファイルを削除されたり不正なプログラムを埋め込む
- Hostsファイル (システムファイルの一部) の改ざん
  - ホスト名からIPアドレスを調べる対応表
  - アンチウィルスベンダー等のセキュリティ関連サイトの閲覧を妨害

# W32/Antinny 2006/04～

- ファイル交換ソフトで流通

- クリック(実行)しようとするすると偽のメッセージを出す
  - 「無効なポインタ操作」
- 裏で、自身のコピーを作成する
- 勝手な公開用フォルダを作り、多くのファイル群をコピー
  - 通称 暴露ウイルス

- 特段新しい技術では無いが、被害が広まった.

- 官民間わず多数の組織の情報が流出して社会問題化
- 削除困難性が高い特性をもつネットワーク

# 原田ウイルス 2008

- ファイル共有ソフトウェアを媒介として感染
  - ファイル共有ソフトウェアでダウンロードしたファイルを削除
  - デスクトップ画面をキャプチャしてメール転送
- イカ・タコウイルス
  - 原田ウイルスの亜種
  - ファイルを特定の画像に置き替える  
OSのファイルを削除して修復不能に



# W32/Autorun 2007/11～

- リムーバブルメディアの自動起動を悪用
- 自身のコピーと構成ファイル(.inf)を作成して増殖
  - autorun.inf があると、メディア接続時に自動的に指定プログラムが起動
  - USBメモリなども媒介に
    - FirewallやIDSは効かない
- ネットワークに繋いでいないパソコンにも感染
  - 昔はフロッピーディスクだった(先祖返り?)
  - アンチウィルスソフトのパターンが未更新

# Gumbler/JS-Redir 2009/06～

- Webページの閲覧で感染拡大に加担
  - 不正なJavaScript (IFRAME)の実行
  - IE, Acrobat, Flashなどの脆弱性をつく
  - ウィルス(ダウンローダ)をインストール
  - パスワードを盗み, Webサーバを攻撃
  - 不正なJavaScript (IFRAME)を挿入
- 通販サイトGENOで最初に発覚
- 2009年末に多数のサイトがやられる
  - JR東日本, ホンダ, ローソン, ハウス食品…….

# Windowsでなければ良いのか

- Linux/Lion(ライオン) 2001/03～
  - BIND(DNSサーバ)のセキュリティホールを悪用
  - マシンのパスワードが特定のアドレスに送信
    - 特定のパスワードで外部からログイン可能に
    - インターネット上のセキュリティホールのあるサーバを検索し感染
- Linux/Slapper(スラッパー) 2002/09～
  - OpenSSLとApache(Webサーバ)のセキュリティホールを悪用
  - バックドアを作成
    - DDoS攻撃用Bot/Zombieになる
    - 他のサーバを攻撃し, 感染を拡大
- 2011年以降, スマートフォンを標的としたウイルスの増大



## Windowsユーザの方はこちら

» Windows向け

## Macユーザの方はこちら

» Macintosh向け

## ESET Endpoint Antivirus for Linux

【Ubuntu用プログラム : ESET Endpoint アンチウイルス for Linux (製品名)】

サポートするOS・動作環境に関する詳細は以下リンク (学外) をご参照ください。

[https://eset-info.canon-its.jp/files/user/pdf/support/esetbe\\_os\\_client.pdf](https://eset-info.canon-its.jp/files/user/pdf/support/esetbe_os_client.pdf)

ライフサイクルポリシーに関する詳細は以下リンク (学外) を参照してください。

<https://eset-info.canon-its.jp/business/info/lifecycle-eol/>

## ソフトのダウンロードとインストール手順

以下のリンクから、ESETインストーラをダウンロードしインストールしてください。

<https://confluence.cis.kit.ac.jp/x/Nu5DAw>

※Symantec Endpoint Protectionがインストールされている場合、ESETインストール後に以下の手順によりアンインストールしてください。

Uninstall Endpoint Protection 14 from Linux

## ESET Server Security for Linux

【RHEL, SUSE Linux, CentOS, Amazon Linux用プログラム : ESET Server Security for Linux (製品名)】

サポートするOS・動作環境に関する詳細は以下リンク (学外) をご参照ください。

[https://eset-info.canon-its.jp/files/user/pdf/support/esetbe\\_os\\_client.pdf](https://eset-info.canon-its.jp/files/user/pdf/support/esetbe_os_client.pdf)

ライフサイクルポリシーに関する詳細は以下リンク (学外) を参照してください。

<https://eset-info.canon-its.jp/business/info/lifecycle-eol/>

## ソフトのダウンロードとインストール手順

以下のリンクから、ESETインストーラをダウンロードしインストールしてください

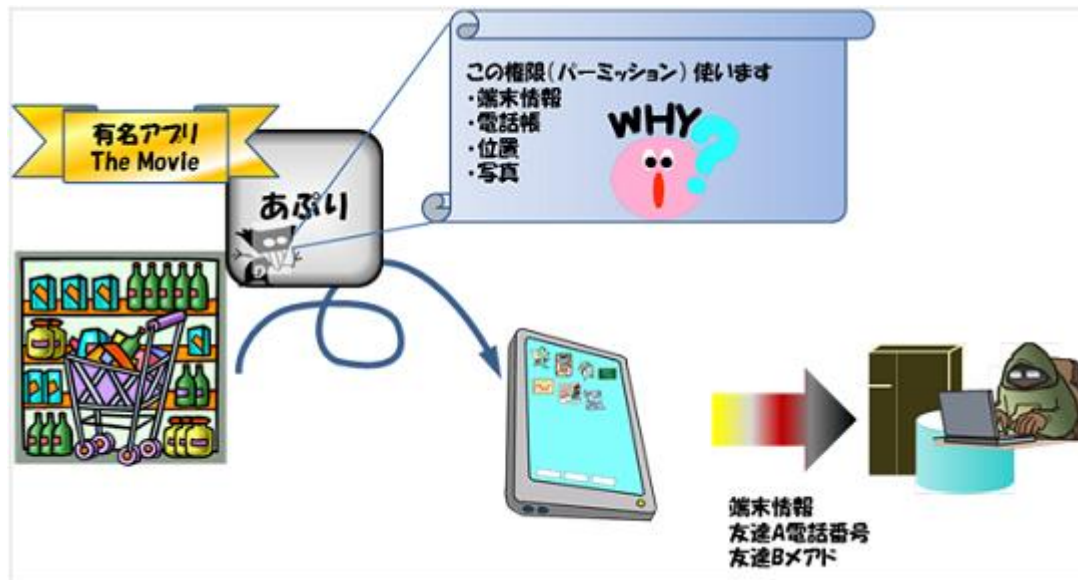
<https://confluence.cis.kit.ac.jp/x/Ou5DAw>

※Symantec Endpoint Protectionがインストールされている場合、ESETインストール後に以下の手順によりアンインストールしてください。

Uninstall Endpoint Protection 14 from Linux

# スマートフォン (iOS/Android 端末)

- 個人情報(電話帳)やプライバシー(行動履歴)が満載
- 公式マーケットによる囲い込み-セキュリティの担保
  - チェック(審査)は十分ではない
- 騙しテクニックを駆使
  - 「他のスマートフォンOSで人気のアプリ」
  - 「有名なアプリ名, アイコンの使用」
  - 「興味を持たせるキーワードを含む」など



不正なアプリが情報を流出させるイメージ図

<https://www.ipa.go.jp/security/txt/2012/05outline.html>

# スマートフォンにもセキュリティを

- モバイル端末(スマートフォン)が狙われている
  - いわゆる“ガラケー”では難しかった
    - 「追加」アプリの「実行」をさせることが困難
  - アプリの導入が容易 (App Store, Playストアなど)
- 正規(?)のアプリ(サービス)に問題がある場合
  - カレログ
  - AppLog (ミログ)
    - 端末内部のアプリ稼働状況を外部へ送信

# Miraiウイルス 2016/08～

- IoT機器を主なターゲットとする新しいタイプのマルウェア
- Linuxが搭載されたIoT機器に感染
  - ネットワークカメラ、家庭用ネットワークルータ、ビデオレコーダ等
  - 管理用IDとパスワードが工場出荷時設定のままになっていることが多いことを狙われた
  - 感染したIoT機器はボットネットを構成
    - 多数の機器同士がネットワーク上で連携
    - 遠隔で操作されてDDoS攻撃に利用される
- GitHub（プログラミングのソースコードを公開・閲覧できるサービス）で公開され、亜種が多数作られている

# 遠隔操作ウイルス事件 2012

- 2012年の初夏から秋に発生したサイバー犯罪
  - ボットに感染させた他人のパソコンを遠隔操作  
そこから犯罪予告を行った
- 感染したパソコンの所有者が誤認逮捕される事態に
- 遠隔操作は外国の複数のサーバを経由した巧妙なもの



# ウィルスの手口(まとめ)

- どうにかしてプログラムを実行させる
  - セキュリティホールについて
  - 利用者に操作させて(ソーシャルエンジニアリング)
    - 標的型攻撃は防ぎにくい
- プログラムが実行できたら、後はなんでもあり
  - 他のマシンへ感染の拡大, DoS攻撃
  - ファイルの消去, 放出, 改ざん
  - 入出力の監視(キーロガー)
  - 詐欺, 恐喝など非コンピュータな犯罪とも連携
- ウィルス自身の更新
  - ウィルス対策ソフトウェアへの対策!?

# デマウィルス (Hoax)

- 単なる嘘

- 「〇〇というSubjectのメールはウィルス」

- システム破壊をそそのかす

- 「〇〇というファイルがあれば、ウィルスだ」
  - 実は、もともとあるファイル(存在して正常)
  - 信じて、ファイルを消すとPCが動かなくなる

- ウィルス対策ウィルス

- 「添付のプログラムはウィルス除去ツールです」
  - 実はウィルス

<https://www.kaspersky.co.jp/threats/hoax>

# 近年の情報セキュリティの脅威

# 情報セキュリティ10大脅威 2018

昨年 順位	個人	順位	組織	昨年 順位
1位	インターネットバンキングやクレジットカード情報等の不正利用	1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	2位
7位	ネット上の誹謗・中傷	3位	ビジネスメール詐欺による被害	ラン ク外
3位	スマートフォンやスマートフォンアプリを狙った攻撃	4位	脆弱性対策情報の公開に伴う悪用増加	ラン ク外
4位	ウェブサービスへの不正ログイン	5位	脅威に対応するためのセキュリティ人材の不足	ラン ク外
6位	ウェブサービスからの個人情報の窃取	6位	ウェブサービスからの個人情報の窃取	3位
8位	情報モラル欠如に伴う犯罪の低年齢化	7位	IoT機器の脆弱性の顕在化	8位
5位	ワンクリック請求等の不当請求	8位	内部不正による情報漏えい	5位
10 位	IoT機器の不適切な管理	9位	サービス妨害攻撃によるサービスの停止	4位
ラン ク外	偽警告によるインターネット詐欺	10 位	犯罪のビジネス化 (アンダーグラウンドサービス)	9位

<https://www.ipa.go.jp/security/vuln/10threats2018.html>

# 情報セキュリティ10大脅威 2019

昨年 順位	個人	順位	組織	昨年 順位
1位 ( <a href="#">*1</a> )	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者への被害	3位	ランサムウェアによる被害	2位
<b>NEW</b>	メール等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	<b>NEW</b>
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

<https://www.ipa.go.jp/security/vuln/10threats2019.html>

# 情報セキュリティ10大脅威 2020

昨年 順位	個人	順位	組織	昨年 順位
<b>NEW</b>	スマホ決済の不正利用	<b>1位</b>	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	<b>2位</b>	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	<b>3位</b>	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	<b>4位</b>	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	<b>5位</b>	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	<b>6位</b>	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	<b>7位</b>	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正口グイン	<b>8位</b>	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	<b>9位</b>	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	<b>10位</b>	サービス妨害攻撃によるサービスの停止	6位

<https://www.ipa.go.jp/security/vuln/10threats2020.html>

# 情報セキュリティ10大脅威 2021

昨年 順位	個人	順位	組織	昨年 順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

<https://www.ipa.go.jp/security/vuln/10threats2021.html>

# 情報セキュリティ10大脅威 2022

昨年 順位	個人	順位	組織	昨年 順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

<https://www.ipa.go.jp/security/vuln/10threats2022.html>



# キャッシュレス決済サービス 「7pay」への不正利用事件

- スマホを利用したQRコード決済のサービス
  - 2019年7月1日に事業をスタート
  - 一部アカウントへの不正アクセスを確認
  - 7月4日にサービス停止
  - 9月30日にサービス終了
- 認証システムの不備
  - 2段階認証が未導入
  - パスワード再発行時に登録していないメールアドレスが指定できた
  - 会員登録時に生年月日を登録無しとした場合、2019年1月1日が自動入力され、実質的に生年月日抜きに再発行可能

# ランサムウェア

- マルウェアの一種
- 感染したコンピュータは利用者のシステムへのアクセスが制限される
- 制限解除に身代金を支払うよう要求する
- WannaCry 2017/5～
  - Microsoft Windowsを標的としたランサムウェア
  - 暗号化されたデータの身代金としてビットコインを要求
  - Microsoft社はサポートが終了していたWindowXPなどのOSに対してもセキュリティパッチを提供する異例の対応

# ランサムウェア



**Payment will be raised on**  
5/18/2017 10:57:16  
Time Left  
02:23:58:43

**Your files will be lost on**  
5/22/2017 10:57:16  
Time Left  
06:23:58:43

[About bitcoin](#)  
[How to buy bitcoins?](#)  
**Contact Us**

**Ooops, your files have been encrypted!** Japanese

**私のコンピュータに何が起きたのですか？**  
重要なファイルは暗号化されています。  
文書、写真、ビデオ、データベース、およびその他のファイルの多くは、暗号化されているためアクセスできなくなりました。たぶんあなたはファイルを回復する方法を探していますが、時間を無駄にすることはありません。誰も私たちの解読サービスなしであなたのファイルを回復することはできません。

**ファイルを回復できますか？**  
確かに。すべてのファイルを安全かつ簡単に復元できることを保証します。しかし、十分に時間はありません。  
あなたは無料でいくつかのファイルを解読することができます。<Decrypt>をクリックして今すぐ試してください。  
しかし、すべてのファイルを解読したい場合は、支払う必要があります。お支払いを送信するのに3日しかかかりません。その後、価格は倍になります。また、7日間で支払いを行わないと、ファイルを永久に回復することはできません。私たちは6ヶ月で払うことができないほど貧しい人々のために無料イベントを開催します。

**私はどのように支払うのですか？**



**Send \$300 worth of bitcoin to this address:**

11 

Copy

Check Payment

Decrypt

# 標的型攻撃

- メール本文に、  
「人事異動の一覧を添付した」「見積書を添付した」等、  
特定の組織の構成員宛てのような、もっともらしい文面でコンピュータウイルスを添付して送るサイバー攻撃
- 受信者に業務メールと誤認されることで添付ファイルを開かせる
- メール本文は海外から送られてくることが多い
  - 従来は日本語表現が不自然ですぐに気づくことができた
  - 近年は日本語が「上達」してきている傾向がある
  - 実在の会社名、取引先名を使った巧妙なメール本文が送られることもある

# フィッシング

- 実在する銀行やクレジットカード会社を装ってパソコン利用者の情報を盗み取る行為
- もっともらしい文面や緊急を装う電子メール
  - “重要なお知らせ”, “パスワードが失効します”など
  - 近年ではスマートフォンのSMSからも
- メールに記述されたURLにアクセスしてしまうと
  - 偽のサイトに誘導
  - クロスサイトスクリプティングの脆弱性を利用して改ざんされた本物のサイトに誘導



# Emotet（エモテット）

- マルウェアおよびサイバー犯罪活動

- 感染したデバイスから情報を盗むのが目的
- 感染するとランサムウェアあと追加のマルウェアがダウンロードされる
- 他の端末に伝染。Emotet拡散の踏み台に。

- 主な感染経路

- メールに添付したMicrosoft WordやExcelファイルのマイクロ

- 経歴

- 2016年ごろ活動開始
- 2019年ごろに世界中で猛威を振るう
- 2021年1月に欧州刑事 警察機構（Europol）を中心とした活動により、攻撃基盤の停止に成功  
→ **その後、活動再開。現在も感染と攻撃は拡大。**

# ゼロデイ攻撃

- 特徴

- 対策が講じられていない脆弱性を狙った攻撃
  - OSやソフトウェアに脆弱性が発見される前
  - 既知の脆弱性に対して修正プログラムが提供される前

- 名称

- 修正プログラム提供日を「1日目（One Day）」  
とすると、提供前はいわば「0日目（Zero Day）」

- 対策

- アンチウイルスソフトウェア
- EDR（Endpoint Detection and Response）
  - デバイスの挙動を観測し、不審な動きを検知したら  
すぐに管理者や利用者に通知するシステム

# 個人でできる情報セキュリティ対策



# URLを確認すれば安心か

- 偽サイト

- 正しいURLを知っていれば見分けられる
- アドレスバーが偽装されている場合もある
- 短縮URLになっていると本来のアドレスがわからない
- URLとIPアドレスの対応が書き換えられている場合も

- 脆弱性を突かれて改ざんされた本物のサイト

- URLでは見分けられない

# 暗号化通信のサイトであれば安心か

- SSL (Secure Socket Layer)

- 重要な情報を送るときに使われる暗号化通信
- http**s**://から始まるURL
- サーバ証明書
  - 大手の証明書の会社（認証局, CA）であれば安心か
  - Webサーバがきちんと審査されて基準に合格したときに発行される証明書（Extended Validation SSL(EV SSL)）であれば安心か
  - 怪しい業者が発行したものも
    - ブラウザから証明書を確認するよう促す画面が出たらまず疑ってかかるべき

# そもそも

- 銀行からパスワード変更を促すメールが来ることはない
- 本物の銀行であれば必ず文書で通知される

参考 : <https://www.mizuhobank.co.jp/crime/email.html>

# コンピュータウイルスへの対策

- 電子メールの添付ファイルを不用意に開かないこと
- ウイルス対策ソフトウェア（アンチウイルスソフト、セキュリティソフト）
  - 調査対象とするファイルに、マルウェアの中からそれぞれに特徴的なプログラムコードを見つけて検出するためのパターンを照合
    - ウイルスが含まれていればファイルを隔離，削除
  - マルウェアは次々と新しいものが作られるのでパターンファイルが常に最新になるように「自動更新」の設定が必要
    - それでも新しいウイルスに感染することもある

# 認証パスワード

- 各種Webサービスで個人を認証するためにIDとパスワードは必須
- パスワードは英数字と記号を組み合わせたなるべく長いものが望ましい
- パスワードを一定期間ごとに変更することを推奨されることが多いが・・・
  - つい覚えやすい単純な文字列になりがちなので注意
- ID, パスワードの使いまわしの危険性
  - 一つのサービスのIDとパスワードが漏洩したときに、他社サービスで次々に利用される恐れがある
  - IDがメールアドレスであるサイトも多く、パスワードだけが認証の砦になっている場合は被害が大きくなる恐れも

# ソーシャルエンジニアリング

- 相手を騙して個人情報聞き出したり，不当な利益を得る方法
- LINE乗っ取り 2016年ごろ～
  - 他人になりすまし，自身の普段使っているLINEが凍結されたとAさんにメッセージを送る
  - 凍結解除に必要なだと携帯番号や認証コードをそれらしい理由で聞き出し，相手のLINEアカウントを乗っ取る
  - 乗っ取ったLINEアカウントは詐欺に利用
    - プリペイドカードを買ってきて詐欺
      - 他人を装って相手にプリペイドカードの購入を依頼
      - 購入させてたカードの番号を教えさせる

# ワンクリック詐欺

- リンクをクリックしただけで、金銭を要求するWebページ
  - 閲覧しただけでは閲覧者の個人情報には抜き取られない
    - IPアドレスや使用ブラウザなど、閲覧者を把握しているかのような情報が表示される場合がある
      - ・ 通常のウェブブラウジングでどのWebサイトでも確認できる閲覧者の情報であるため個人を特定できるような致命的な情報ではない
  - うかつに対応しない
    - 「お支払者を確認しますので、お名前と電話番号を入力してください」といった誘導に従い、入力してしまうと個人情報が取られる
    - 心配なことがあれば、警察や消費生活センターに相談

# パソコンの管理

- マルウェア対策

- ウイルス対策ソフト
- Microsoft WindowsパソコンであればWindows Updateを定期的に実施
  - OSやMicrosoft製ソフトウェアのセキュリティパッチが適用できる
- 他のアプリケーションソフトウェアもアップデートを行う
  - Adobe製品（Flash(2020年12月31日で配布と更新を終了)など）やJavaなど

- サポートの切れたソフトウェアやOSは使用しない

- 利用者の注意深さ

- 知らない人からのメールを安易に開かない
- 怪しげなWebサイトへは行かない



# 記憶媒体の管理, パソコン廃棄の配慮

- 個人情報や企業秘密情報の漏洩対策

- ウイルス対策ソフト
- 共有設定の安易な利用
- USBフラッシュメモリなどの外部記憶媒体の管理
- データの暗号化
- 廃棄時のデータ削除
  - HDDの物理破壊
  - 専用のソフトウェア/ハードウェアによるデータ完全削除

# 自宅のネットワーク管理

- 家庭用ルータの設定

- ファイアウォール

- 外部からの攻撃を防ぐ

- 無線LANの暗号化

- 暗号化なしで使用しない

- 高度な暗号化の規格であるWPA-PSKを使用する

- 暗号化にも脆弱性があるため、特に古いWEPは暗号として役に立たない

(WPAより強力なWPA2を使うことが推奨されている)

- 2017年10月16日、セキュリティ面でより強力とされたWPA2についても脆弱性

- 現在では新たな規格、WPA3を使用すべき

# 街中のアクセスポイントの利用

- 公衆無線Wi-Fi

- 喫茶店やホテルのロビー，空港や駅などに設置
- 盗聴の危険性を認識して利用すべき
  - 脆弱な暗号化方式または暗号化していない
- ネットバンキングなどの個人情報といった機密度の高いデータのやり取りはさける
  - どうしても必要な場合は通信内容が暗号化されるhttpsでアクセス
- ファイル共有機能は停止

# 総括

## • ウィルスと不正アクセス技術

### ➤ いたちごっこは続く

- ウィルスは日夜新しいものがばらまかれる
- フィッシングや乗っ取りなどは次々に新たな手法が出てくる

### ➤ 利便性との戦い

### ➤ 対策を講じることが大事

- ウィルス対策ソフトウェア
- ソフトウェアのアップデート
- 暗号化通信
- 場合によってはまず疑う