医学研究のための MMC 活用法と情報セキュリティ（講義）
Practical Use of MMC and IT Security for Medical Research (Lecture)

重歳 憲治（マルチメディアセンター）
Kenji Shigetoshi (MultiMedia Center)

マルチメディアセンターでは，利用者用端末として Windows 11 Pro 184 台および macOS Ventura 13 台を管理しており，利用者は，これらの端末で Microsoft Office 2021，SPSS 等のソフトウェアが利用可能となっている．また，センター内には研究発表用資料を作成するための設備があり，B0 サイズの大判印刷が可能なプロッター（普通紙，光沢紙，布の 3 タイプ），写真画質で A3 サイズまで印刷可能なインクジェットプリンタ，透過原稿対応フラットベッドスキャナおよび CD/DVD デュプリケータといった専用機器が設置されている．その他，ウイルス駆除ソフトの無料配布や VPN サービスによる学外からの文献検索，大容量ファイル転送サービスによる学内外者とのセキュアな大容量ファイルの受け渡し等，利用者の経済的負担の軽減および利便性の向上に資するサービスの提供を行っている．さらに，国立情報学研究所が運営するサービスの提供にも努めており，国際学術無線 LAN ローミング基盤「eduroam」，研究データマネージメントサービス「学認 RDM」の利用が可能となっている．また，2023 年 3 月の学術情報基盤システム更新に伴い，学内専用ストレージサービスの提供開始や個人所有端末に最新の Microsoft Office をインストールして利用することが可能となる等，サービスの拡充を行っている．

本講演では，マルチメディアセンターの設備および学内外で利用可能な各種サービスについて説明するとともに，情報セキュリティに関する自己点検項目等について紹介する．

Multimedia Center manages 184 Windows 11 Pro and 13 macOS Ventura terminals for users, and software such as Microsoft Office 2021, SPSS, etc. are available for these terminals.

In the Center, there is a facility for preparing materials for research presentations, and special equipment such as a plotter (Plain paper, Glossy paper, Cloth - 3 types) capable of large-format printing of B0 size, an inkjet printer capable of printing up to A3 size in photographic quality, a flatbed scanner compatible with transparent originals, and a CD/DVD duplicator are installed.

In addition, we provide services that help reduce the financial burden on users and improve convenience, such as the free distribution of the antivirus software, literature retrieval from off-campus through the VPN service, and the secure transfer of the large capacity file between people inside and outside of the university by the large capacity file transfer.

Furthermore, with the renewal of the computer and network system in March 2023, it has become possible to start providing on-campus storage services and to install the latest Microsoft Office software on personal devices.

We are also working to provide services operated by the National Institute of Informatics, making it possible to use an international academic wireless LAN roaming infrastructure "eduroam" and a research data management platforme "GakuNin RDM".

In this lecture, the facilities of the Multimedia Center and various services available on- and off-campus will be explained, and self-inspection items regarding information security will be introduced.

医学研究のための
MMC活用法と情報セキュリティ

2023年9月15日
マルチメディアセンター
重歳　憲治

目次

- MMC提供サービスの紹介
- MMC施設の紹介
- 外部サービスの紹介
- 情報セキュリティの脅威と対策
- CSIRT (Computer Security Incident Response Team)
- 参考資料
  - FileZen（めるあど便）：大容量ファイル転送サービス（利用方法）
  - パスワード強度の体験

MMC提供サービスの紹介

・メールアドレスの付与
・多要素認証
・Gmail
・VPNサービス
・ウィルス駆除ソフトの無償配布
・統計ソフトSPSS29, JMP Proの学内配布
・モノクロ／カラー印刷
・無線アクセスポイントの利用
・ノートPC、プロジェクター等の貸出
・大容量ファイル転送サービス
・学内専用ファイル受け渡しサービス
・学内専用データ保存サービス
・Office 365 A3 利用資格の付与
・WordPress学内ブログ利用登録
・その他
 - 個人ホームページの設置
 - 個人PCの学内LANへの接続
 - 新規メーリングリストの登録
 - 講習会の開催

メールアドレスの付与

- 半角8文字以下の任意の文字列で利用者IDを申請すると、以下のメールアドレスが付与される

  利用者ID@belle.shiga-med.ac.jp

  利用者IDは、病院システム（Niho）と同じだが、パスワードは異なるため管理に注意すること
- 一度発行された利用者IDは変更できない
- 学外からメールを利用するためには、多要素認証の設定が必要

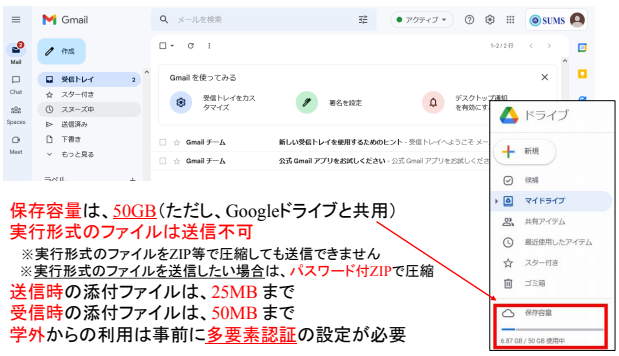
多要素認証

- セキュリティ上のリスクが高いサービスに、学外からアクセスする場合は、ID/PWの認証に加えて、もう一つの認証を要求
- もう一つの認証には、以下の3種類を用意
  - TOTP(Time-based One-Time Password)
  - FIDO(First IDentity Online)
  - イメージングマトリクス

多要素認証の設定

詳細は、MMCホームページ － 多要素認証
https://www.shiga-med.ac.jp/mmc/service/tayoso/

Gmail



保存容量は、50GB（ただし、Googleドライブと共用）
実行形式のファイルは送信不可
※実行形式のファイルをZIP等で圧縮しても送信できません
※実行形式のファイルを送信したい場合は、パスワード付ZIPで圧縮
送信時の添付ファイルは、25MB まで
受信時の添付ファイルは、50MB まで
学外からの利用は事前に多要素認証の設定が必要

VPNサービス

- 学外から以下のサービスが利用可能
  - e-Learning(WebClass)
  - オンラインジャーナル
  - まるっと滋賀医大
  - ウィルス駆除ソフトのダウンロード　等
- ただし、事前に以下の準備が必要
  - 「FortiClient VPN」、「CA証明書」のインストール
  - 多要素認証の設定

FortiClient VPN, CA証明書のインストール

- 利用するには「FrotiClient VPN」と「CA証明書」のインストールが必要
- Windows, Mac, Android, iPhone 用のマニュアルを用意

ウィルス駆除ソフトの無償配布

- 自宅のコンピュータにもインストール可能

マルチメディアセンターのホームページからダウンロード
https://www.shiga-med.ac.jp/mmc/

- **Windows (10, 11)**
  - ESET Endpoint Antivirus
- **Windows Server (2012～2022)**
  - ESET File Security
- **MacOS (10.12～13.x)**
  - ESET Endpoint Antivirus
- **Android（OS5.x～13.x）**
  - ESET Endpoint Security

統計ソフト SPSS29 の学内配布

- **SPSS29 利用可能製品**
  - Statistics Base
  - Regression
  - Advanced Statistics
- **動作環境**
  - Windows 10, 11
  - Mac OS 10.13 ～ 12.0
- **注意事項**

学内利用限定
ネットワークライセンス（同時使用25ライセンス）のため、講義・講習会等でSPSSが使用される場合、一時的に利用できなくなります

詳細は、MMCホームページ
http://www.shiga-med.ac.jp/mmc/ → 各種サービス → SPSSダウンロード

統計ソフト JMP Pro の学内配布

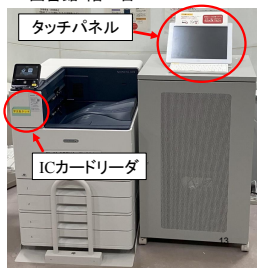
- **動作環境**
  - Windows 10, 11
  - Windows Server 2019, 2022
  - Mac OS 10.15 ～ 13
- **注意事項**
  - WebClassからダウンロード
  - ダウンロードする前に利用条件に同意する必要あり
  - 利用場所に制限なし

詳細は、MMCホームページ
http://www.shiga-med.ac.jp/mmc/ → 各種サービス → JMP Proダウンロード

モノクロ／カラー印刷

- プリンタは館内6箇所に設置
- オンデマンド印刷を採用しているので、空いているプリンタから出力できる
  - 図中のタッチパネルから利用者IDとパスワードでログイン
  - もしくは、ICカードリーダに学生証をかざす
- 利用可能ポイント：500/年
  [消費ポイント]
  カラー：4ポイント/枚
  モノクロ：1ポイント/枚

演習室：2台
ブラウジング室：1台
1階オープンフロア：1台
2階ブラウジングコーナー：1台
図書館2階：1台



無線アクセスポイントの利用

- 全学的に設置
- SSID: sums-wireless
- 認証： Mail Account/PW
- 無線LANカードのMACアドレスをMMCホームページから登録すれば利用可能
- コンピュータの設定方法については、MMCホームページを参照してください



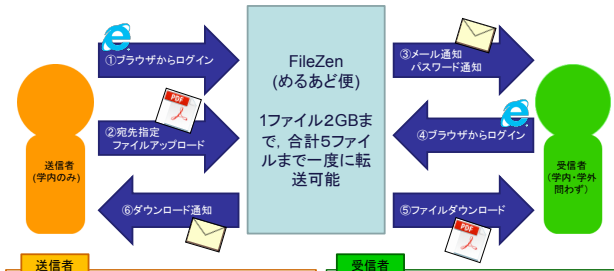
http://www.shiga-med.ac.jp/mmc/ → ネットワーク接続

ノートPC、プロジェクター等の貸出

- WindowsノートPC
  ・Windows 11 Pro
  ・Microsoft Office 2021
  ・Photoshop Elements2023
  ・SPSS 29 / JMP Pro 等
- MacノートPC
  ・macOS Ventura 13
  ・Office for Mac
  ・Adobe Creative Cloud
  ・SPSS 29 / JMP Pro 等
- プロジェクター
- Web会議用機材
  ・三脚付きカメラ
  ・マイク付きWebカメラ
  ・スピーカマイク

https://www.shiga-med.ac.jp/mmc/ → 予約→ 物品貸出

FileZen（めるあど便）：大容量ファイル転送サービス



送信者
①FileZenにログインする。
②宛先、メッセージ入力、パスワード、公開期間等を設定し、共有したいファイルをアップロードし送信する。
⑥ファイルがダウンロードされた旨、通知される。

受信者
③本文とログインURLが記載されたメールとダウンロード用パスワードが記載されたメールが届く。
④FileZenにログインする。
⑤ファイルをダウンロードする。

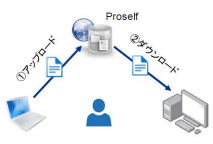
https://www.shiga-med.ac.jp/mmc/service/filezen/

学内専用ファイル受け渡しサービス(Proself)

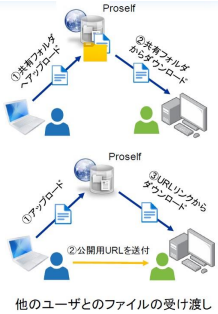
Proself

ファイル保存容量：10GB　ファイル保存期間：10日間（自動削除）

Proselfでできること



自分の端末間でのファイルの移動



他のユーザとのファイルの受け渡し

MMCホームページ
↓
各種サービス
↓
Proself（学内専用ファイル受け渡し用オンラインストレージシステム）

学内専用データ保存サービス(NextCloud)

Nextcloud

- 学内専用のオンラインストレージ
- 保存容量：5GB
- ファイル・フォルダの共有機能
- ブラウザ上でWord、Excel棟のファイルを共同編集できる
- 操作履歴の確認ができる　等

詳細は、MMCホームページ → 各種サービス
→ Nextcloud(学内専用データ保存サービス)

Office 365 A3 利用資格の付与

- 利用対象者：学部学生・大学院生・教職員
- Microsoft365ポータルサイト(https://login.microsoftonline.com/)にメールアドレスとメールのパスワードでサインイン
- 個人所有のPCでOffice365が利用可能
- 一人当たり、合計5台のPC（WindowsまたはMac）にWord・Excel・PowerPoint等のアプリをインストール可能
- PCとは別に、タブレット、スマートフォンにもそれぞれ最大5台までインストール可能
  ※PC、タブレット、スマートフォン全てにインストールする場合、最大15台まで可能
- OneDriveの保存容量：1TB

詳細は、MMCホームページ
http://www.shiga-med.ac.jp/mmc/ → 各種サービス → Office365

WordPress学内ブログ利用登録（1）

WordPressの特徴

- ホームページ／ブログの作成が簡単
- メールアカウントによる閲覧・編集制限が可能
- ただし、学内専用

WordPress学内ブログ利用登録（2）

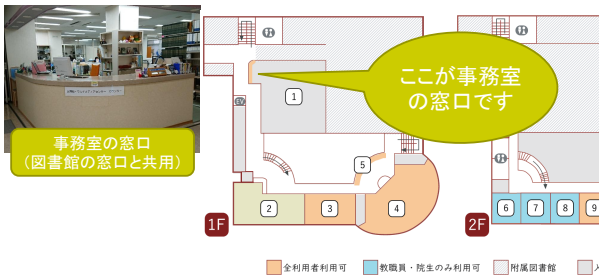
その他

- 個人ホームページの設置
  ・MMC HP → ホームページ設置
- 個人PCの学内LANへの接続（要登録）
  ・MMC HP → ネットワーク接続 → 学内ネットワーク接続申請
- 新規メーリングリストの利用登録
  ・MMC HP → メールサービス → メーリングリスト
- 講習会の開催
  ・セキュリティ講習会
  ・医療統計（SPSS）等

MMC施設の紹介

・MMC事務室の場所
・マルチメディアセンターに設置のコンピュータで利用可能なソフトウェア例
・演習室
・ブラウジング室
・オープンフロア
・MMC会議室 赤，青，緑，黄
・入出力室
・その他学内のコンピュータ設置場所
・館内での禁止事項

MMC事務室の場所



マルチメディアセンターに設置の コンピュータで利用可能なソフトウェア例

Windows 11 Pro

- MS Office 2016
- SPSS 29
- JMP Pro
- Visual Studio Code
- Google Chrome
- Moilla Firefox
- VLC

macOS Ventura 13

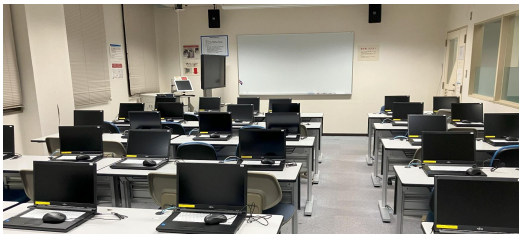
- Office for Mac
- SPSS 29
- JMP Pro
- Google Chrome
- Mozilla Firefox
- VLC

演習室（1階）

- 利用時間： 平日8:30～19:00
- 82台のWindowsノートパソコン（OS:Windows 11）
- 注）講義優先。講義使用以外は自由に利用可。

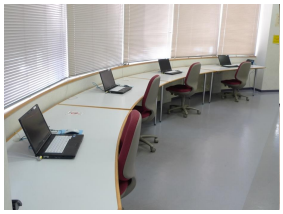
ブラウジング室（1階）

- 利用時間： 平日・土日祝7:00～24:00
  ※平日7:00～8:30, 19:00～24:00, 土日祝終日は要職員証・学生証
- 36台のWindowsノートパソコン（OS:Windows 11）
- 注）講義優先。講義使用以外は自由に利用可。



オープンフロア（1階）

- 24時間利用可能

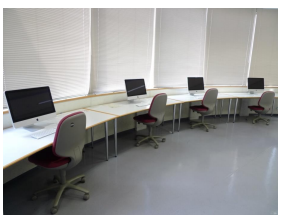


1階ホール
・WindowsノートPC 4台

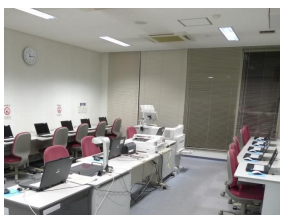
1階ホール
・iMac 2台
・オンデマンドプリンタ 1台

オープンフロア（2階）

- 24時間利用可能



2階ホール（iMac 6台）



2階ブラウジングコーナー
（WindowsノートPC 12台・スキャナ 3台）

会議室 赤，青，緑（2階）

- 利用時間： 平日8:00～24:00
- 収容人数12人
- LANコンセント
- ホワイトボード
- スクリーン（手動）
- 60インチ液晶モニタ
- Zoom Rooms

MMCホームページから利用予約が必要

会議室 黄（2階）

- 利用時間：　平日8：00～24：00
- 収容人数34人
- LANコンセント
- ホワイトボード
- 天吊プロジェクター
- 電動スクリーン
- Zoom Rooms

MMCホームページから利用予約が必要

入出力室（2階）

- 利用時間：24時間利用可能（要職員証・学生証）
  ※用紙交換・トラブル等の対応は、
  平日9:00～20:00、土曜日13:00～17:00
- ポスター印刷、CD/DVDデュプリケータ等

その他学内のコンピュータ設置場所

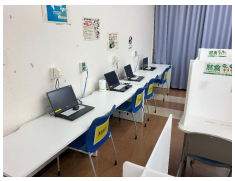
- 附属図書館1、2階　MMCサテライト

附属図書館1階参考図書エリア
Windows 4台

附属図書館2階エレベータ横
・Windows 2台
・オンデマンドプリンタ 1台

その他学内のコンピュータ設置場所

- 福利棟1、2階
- 看護学科棟1階ラウンジ

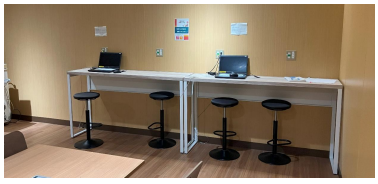


福利棟1階　Windows 4台
福利棟2階　Windows 3台

看護学科棟1階
Windows 4台
プリンタ　1台

その他学内のコンピュータ設置場所

- 一般教養棟1階学生ラウンジ
  利用時間：　8：00～22：00
  2台のWindowsノートパソコン



（備考）学生ラウンジの利用についてのルール
https://sumsdoc.shiga-med.ac.jp/ASTRUX2/ID_guest.aspx?did=137455

館内での禁止事項

- 喫煙
- 食物の持ち込み
- 携帯電話の使用（中庭での使用は可）
- 大声での雑談等、他の利用者への迷惑行為
- 設置機器へのソフトウェアのインストール

※飲物はOK（ただし、ペットボトル等のフタのできるものに限る。また、飲んでいない時はフタを閉めることが条件）

外部サービスの紹介

国立情報学研究所（NII）提供サービス

・eduroam（国際学術無線LANローミング基盤）

・GakuNin RDM（研究データ管理基盤）

eduroam（国際学術無線LANローミング基盤）

国内230機関(46都道府県)、世界約90か国(地域)が参加

利用方法

1．SSID

「eduroam」あるいは「eduroam-XXX」

(XXXは任意の文字列)

2．IDとパスワード

ID：xxxxxx@shiga-med.ac.jp

（xxxxxx: 本学のメールアドレスの@より前の部分（メールのID））

パスワード：

本学のメールのパスワード

国立情報学研究所提供　https://www.eduroam.jp/about/

GakuNin RDM（研究データ管理基盤）

■GakuNin RDM ログインURL■
https://rdm.nii.ac.jp/

■GakuNin RDM とは

2021年2月から本運用が開始された国立情報学研究所が運用する研究データ管理基盤で、公表前の非公開の研究データの管理と共有を目的としており、Webブラウザから操作することができるWebアプリケーションとしてサービスが提供されるシステム

■主な機能

・研究プロジェクト単位でデータへのアクセス権を設定し、研究室内や共同研究者間でデータを共有できる
・大学の認証システムと連携させるため、大学で普段用いているIDとパスワードでログイン可能
・ファイルへタイムスタンプを付与し、システム外でのデータの変更を検出することにより研究の証跡を管理
・研究者1人当たり100GBまで利用可能な無料ストレージ

■e-Learning (WebClass)

国立情報学研究所の講師が説明する講習会の録画映像及び資料をWebClassにて提供中

情報セキュリティの脅威と対策

・情報セキュリティとは
・セキュリティインシデント
・外部記憶媒体について
・コンピュータおよび外部記憶媒体のセキュリティ対策
・記憶媒体を廃棄するときの注意
・外部記憶媒体の廃棄方法
・情報セキュリティ10大脅威2023
・フィッシングとは
・ランサムウェアとは
・標的型攻撃
・医療機関でのウィルス感染、情報流出例
・脅威への対策
・情報セキュリティに関する自己点項目

「情報セキュリティ」とは、情報資産の機密性、完全性、可用性 を確保すること！

- 機密性（Confidentiality）

  情報に関して、アクセスを認められた者だけが、これにアクセスできる状態を確保すること。
- 完全性（Integrity）

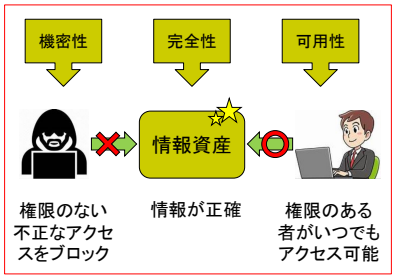
  情報が破壊、改ざん、または、消去されていない状態を確保すること。
- 可用性（Availability）

  情報へのアクセスを認められた者が、必要時に中断することなく、その情報にアクセスできる状態を確保すること。

情報資産とは

- 情報の内容
- 情報を作成・利用・管理するための仕組み
  - ハードウェア
  - ソフトウェア
  - ネットワーク
  - 記録媒体　等

情報セキュリティの侵害例

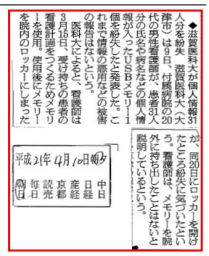


- コンピュータがウイルスに感染して個人情報が漏洩した（機密性）
- 不正アクセスにより大学のホームページが改竄された（完全性）
- メールサーバが故障して電子メールの送受信ができなくなった（可用性）

情報セキュリティが維持されている状態

セキュリティインシデント

帰宅時や外出時に学外で使用するノートパソコンやUSBメモリ、外付けハードディスクなどの持ち運び可能な外部記憶装置の盗難や紛失により、そこに保存された情報が漏洩するなどの問題が起きている。



外部記憶媒体について

- ノートパソコン
- USBメモリー
- 外付けハードディスク
- クラウドストレージ　等

2019年4月1日よりUSBメモリの学内での使用が禁止になりました！

コンピュータおよび外部記憶媒体のセキュリティ対策

- コンピュータには必ずログインパスワードを設定する
  コンピュータを使う上で必須のセキュリティ対策
- ファームウェアに起動パスワードをかける
  パスワードを知らない第3者によるコンピュータの起動を防止
- ハードディスク、USBメモリーにパスワードをかける
  ソフトウェアによってハードディスクやUSBメモリーに対してパスワードをかけることができる（暗号化）
- ファイルを暗号化する
  暗号化パスワードを英数字および記号を含め12文字以上にする

記憶媒体を廃棄する時の注意

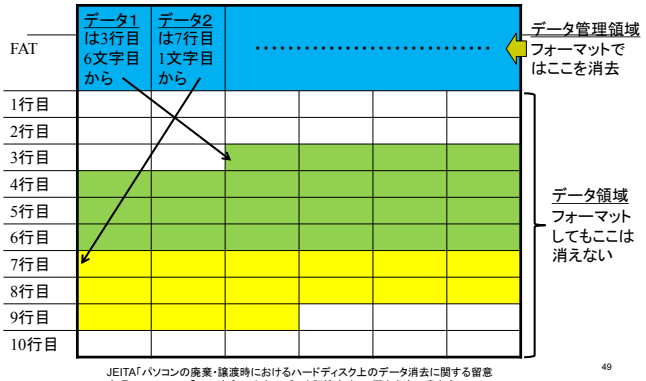
使用済みのパソコンやサーバ、または記憶媒体などを返却/破棄する際には、そこに保存されているデータを確実に消去する必要がある。データ復旧用ソフトウェアなどを使うと、削除されたファイルを再び読み取ることが可能になる場合があるためである。

削除したデータの復活 ～フォーマットでデータは消えない～

- ファイルの削除やディスクのフォーマットをすると、一見データが消去されたように見える
- しかし、消去されているのはデータの管理情報だけであり、実データは残る
- Windowsのクイックフォーマットはもちろん、標準のフォーマットを使っても実データは消えない

WindowsでUSBメモリをフォーマットするとき

FAT (File Allocation Table)



JEITA「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」, p.7, 2010「ハードディスク中のデータ記憶方法」の図を参考に書き直し

外部記憶媒体の廃棄方法

- ソフトウェアによるデータ消去が手軽であるが、物理的に破壊することが望ましい
- マルチメディアセンターでは、ペーパーシュレッダー兼フロッピーディスク、CD/DVD、MO破砕装置がカウンター前に設置されており、自由に利用できる
- また、マルチメディアセンターでは、パソコンのハードディスク破壊処理も受け付けている

詳細は、MMCホームページ
http://www.shiga-med.ac.jp/mmc/
→ 各種サービス → HDD/SSD等破壊依頼申請

情報セキュリティ10大脅威 2023（IPA）

前年順位	個人	順位	組織	前年順位
1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
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3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	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5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	4位
7位	不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8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	脆弱性対策の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不正請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

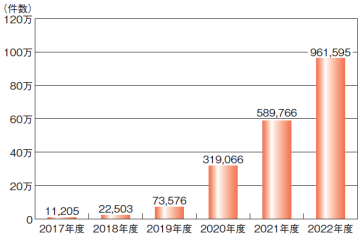
https://www.ipa.go.jp/security/10threats/10threats2023.html

フィッシングとは

実在する組織を騙って、ユーザネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人情報を詐取すること。電子メールのリンクから偽サイト (フィッシングサイト) に誘導し、そこで個人情報を入力させる手口が一般的

フィッシング対策協議会ホームページより抜粋
https://www.antiphishing.jp/consumer/abt_phishing.html

フィッシングによる被害



■図 1-1-10　年度別フィッシング報告件数（2017 ～ 2022 年度）
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2023 年 3 月）を基に IPA が作成

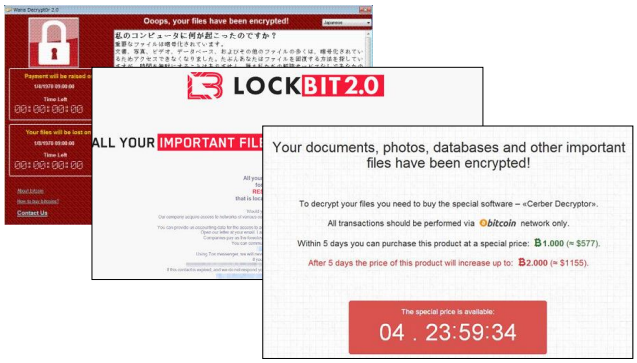
出典：IPA「情報セキュリティ白書2023」, p.11

ランサムウェアとは

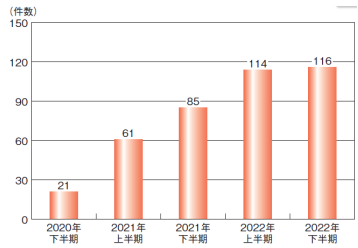
ランサムウェアとは、ファイルを勝手に暗号化するなどパソコンに制限をかけ、その制限の解除と引き換えに金銭を要求する不正プログラムの総称

出典：IPA 情報セキュリティ2015年6月の呼びかけ
https://www.ipa.go.jp/security/txt/2015/06outline.html

ランサムウェアに感染すると



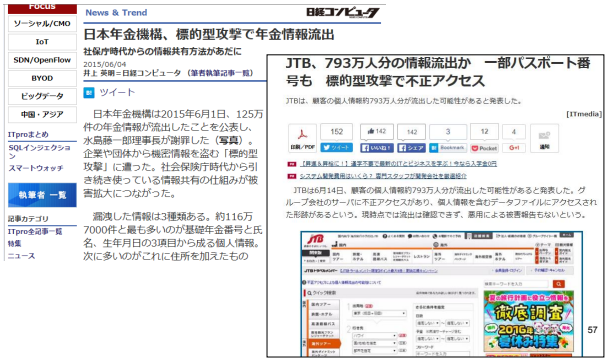
ランサムウェアによる被害



■図 1-2-1　企業・団体等のランサムウェア被害の報告件数の推移
(出典)警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について[※11]」を基に IPA が編集

出典：IPA「情報セキュリティ白書2023」, p.15

標的型攻撃



特定個人を狙う標的型攻撃

●ユーザーをだましてウイルスに感染させる

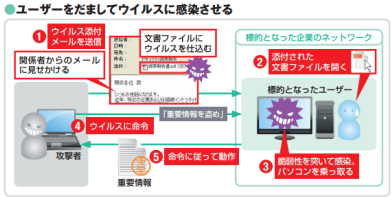


図 1　標的型攻撃の典型例。攻撃者は、標的とした企業や組織の従業員に対して、関係者などを装ったウイルス添付メールを送付する。添付ファイルを開くとウイルスに感染し、パソコンを乗っ取られてしまう

●政府機関や防衛関連企業が狙われる

公表時期	攻撃を受けた時期	攻撃対象	被害
2011年9月	同年8月	三菱重工業	製品に関する情報が流出、機密情報は未流出
2011年10月	同年8月	衆議院	全議員のユーザーIDやパスワードが流出
2011年10月	同年6月	外務省や在外公館	機密情報の流出は未確認
2012年2月	同年2月	特許庁	機密情報の流出は未確認

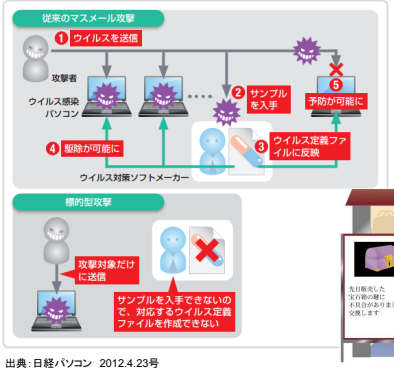
表 1　ウイルス感染が確認されている標的型攻撃の例

出典：日経パソコン　2012.4.23号

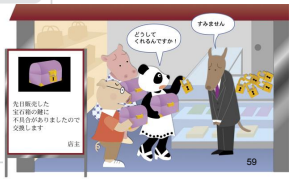
2004年（平成16年）以降、陸上自衛隊・海上自衛隊・航空自衛隊の各自衛隊員が職場に私物のパソコンを持ち込み、業務に利用していたが、秘密のデータを保存したまま自宅へ持ち帰りWinnyその他のファイル共有ソフトを使用したため、Antinnyをはじめとする暴露ウィルスに感染する事案が多発。これにより装備品の性能諸元・コールサイン等の軍事機密情報が漏洩した。

ウィルス対策ソフトの抜け穴を狙う

・標的型攻撃



・ゼロデイ攻撃
OSやアプリケーションのセキュリティ・ホール（脆弱性のある不具合）を修正するパッチ（修正プログラム）が提供されるより前に、その脆弱性を突いて攻撃すること



出典：日経パソコン　2012.4.23号

医療機関でのウィルス感染、情報流出例

2009年3月11日	東大医学部付属病院院内の診療業務用の端末パソコン1,000台以上と複数のサーバーコンピューターが感染
2016年2月5日	ロサンゼルスにあるハリウッド長老教会派医療センターで院内のPCがウィルス（ランサムウェア）に感染し、PCを使った業務が停止。患者データへのアクセスを取り戻すために17,000ドル相当のビットコインを支払った
2017年5月12日	ランサムウェア（WannaCry）の感染により、英国の国民保健サービス（NHS）のコンピューターが多数停止
2021年10月31日～2022年1月4日	徳島県のつるぎ町立半田病院で院内の電子カルテサーバやパソコンがランサムウェア（LockBit）に感染し、新規患者の受け入れ停止等の被害が発生
2022年10月31日～2023年1月15日	大阪急性期・総合医療センターでランサムウェアによる重大なシステム障害が発生し、電子カルテを含めた総合情報システムが利用できなくなり、診療機能に大きな支障が生じた

脅威への対策

- OS、ソフトウェアのセキュリティアップデート（2012年の事例では99．8%が既知の脆弱性を悪用しているとのレポートあり（日本IBM））
- ウィルス駆除ソフトの導入と定義ファイルの更新
- メール、Web、スマートフォンアプリ利用において常に疑いの心を持ち、怪しいと感じたときは検索サイトで調べてからにするといったことを徹底
- パスワードの使い回しをしない

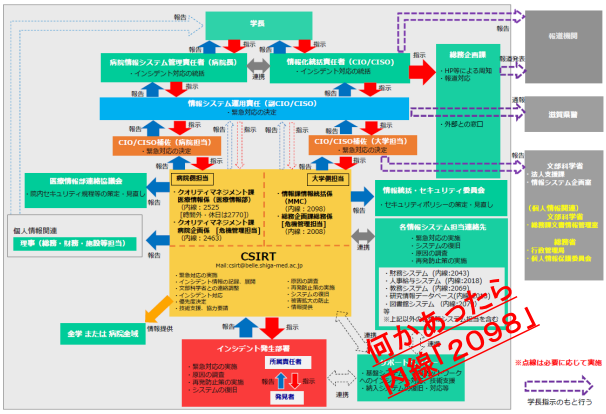
脅威への対策

- データのバックアップ（3－2－1ルール）
  - 3つ以上のコピーを作成
    →本来のデータ＋2つ以上のコピー
  - 2つの異なる種類のメディアに保存
    （例：クラウドおよび 外付けUSB-HDD等）
  - そのうちの1つは他の2つとは異なる場所に保存
    （例：自宅とクラウド等）

情報セキュリティに関する自己点検項目

1. パソコンやスマートフォン等の端末のOSやソフトウェアは、常に最新の状態にしていますか。
2. 本学のネットワークに接続する端末にはウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にしていますか。
3. 本学のメールアドレスを、学外のクラウドサービス等を利用する際のIDとして使用していますか。使用している場合、本学の認証システムで利用しているパスワードとは異なるパスワードを設定していますか。
4. 電子メールの添付ファイルや本文中のURLリンクを介したマルウェアの感染に気をつけていますか。
5. 離席する際は、情報を覗き見られたり、勝手に操作されないように、パソコンの画面をロックするように気をつけていますか。
6. 本学では、2019年4月より原則としてUSBメモリの利用を禁止しています。やむを得ない場合でも、暗号化機能つきのUSBメモリの使用しか認められていません。この方針を遵守できていますか。
7. 帰宅時にノートPCや備品等を施錠された場所に保管するか、アクセスが制限された部屋で管理する等、盗難に対する対策はされていますか。
8. 自分が所属している部署の情報セキュリティ担当者が誰か把握していますか。

CSIRT Computer Security Incident Response Team



参考資料

FileZen（めるあど便）：
大容量ファイル転送サービス（利用方法）

滋賀医科大学は学内における USBメモリの使用を禁止しました.

- 禁止日：2019年4月1日
- 院内，学内における度重なるUSBメモリの紛失事案により決断
- USBメモリの代替手段として FileZen: 大容量ファイル転送サービスの利用を推奨
- やむを得ずUSBメモリを使用する場合は，大学指定のものが使用可能

※使用可能なUSBメモリの詳細は以下を参照
MMC HP -> SUMS CSIRT -> 大学CSIRT -> USBメモリ使用禁止について(2019.4~)
http://isis.shiga-med.ac.jp/wp/csirt/usb_flash-drive_201904/

滋賀医科大学での現状

- 2017年5月～2019年1月(1年9ヶ月)で72件のUSBメモリ拾得物（病院は別）
  - 平均すると月3.4件
  - 患者情報を含むもの1件、患者さん以外の個人情報を含むもの14件
  - 暗号化されたUSBメモリはなし

マルチメディアセンターに届けられたUSBメモリの落とし物

USBメモリは小さくて便利だが紛失しやすい

情報の重要度に応じたファイルの取扱いを意識するようにしてください.

- 自分が扱っている情報は機密情報に該当するのか
  - どのような情報が含まれているのか確認する
  - 漏洩した場合にどのような影響があるのか考える
- 持ち出しが認められた情報なのか
  - 大学の規程や運用規則に違反していないか確認する
  - データの管理責任者の許可は必要ないか確認する
- 重要度に応じたセキュリティを確保しているか
  - 外部記憶媒体、ノートPCは紛失・盗難のリスクがあることを認識する
  - 暗号化やパスワードの設定等のリスク軽減策を施す
  - 物理的な保管場所、ネットワークの設定等の確認

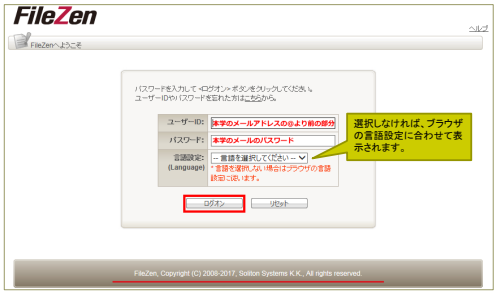
FileZen（めるあど便）とは

- FileZen(めるあど便)は、本学のアカウント（メールアドレス）を持つユーザから、一度に5つのファイル(1アカウントにつき1ファイル2GB:合計10GB※まで)を共有することができるシステムです。※すべてのめるあど便・受取フォルダの合計
- 学内・学外のどちらからもアクセスすることが可能です。
- 公開期間・ダウンロード上限回数・ダウンロード時に要求するパスワードを設定することができます。
- FileZen URL：https://porter.shiga-med.ac.jp/

注：タイムアウトまでの時間は60分です。

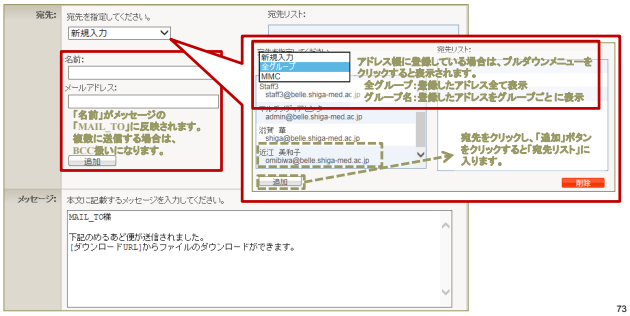
ファイルの送信の仕方

1. FileZen(https://porter.shiga-med.ac.jp/)にアクセスし、ユーザーIDとパスワードを入力し「ログオン」する。

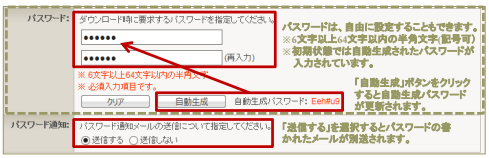


2. 「めるあど便」タブをクリックし「新規作成」を選択する。
   ※共有できるファイルの容量は、画面右上の「ディスク使用量」を確認する。

3. 件名、宛先(学外者可)、メール本文を入力する。
※メッセージ本文の「MAIL_TO」様の部分には宛先の名前が入力される。(複数に送信する場合は、BCC扱いになる。)



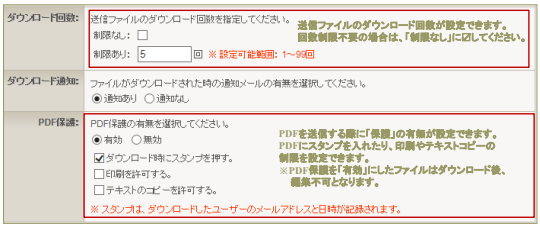
4. ファイルのダウンロード時に要求するパスワードを設定する。
- 「パスワード」
自由に設定したもの・自動生成したものどちらかを選択して使用する。
- 「パスワード通知」
「送信する」を選択するとパスワードの書かれたメールが別送される。
※「送信しない」場合は、別の手段でパスワードを通知してください。



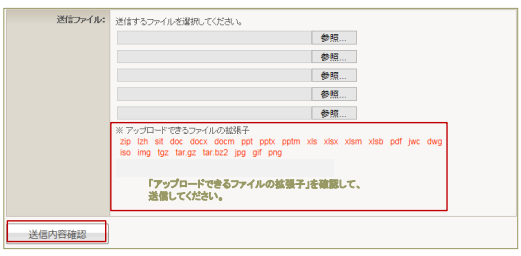
5. 「設定オプション」の「変更」ボタンをクリックし、「公開期間」を設定する。
- 公開期間は、デフォルト設定は3日間、1日～10日間までの設定が可能。
- 日付を指定して公開期間設定可能(上限10日)。

6. 「ダウンロード回数」を設定する。
- ダウンロード回数は、制限なし・1～99回までの任意回数を選択できる。
※受信者毎にダウンロード回数が設定される。

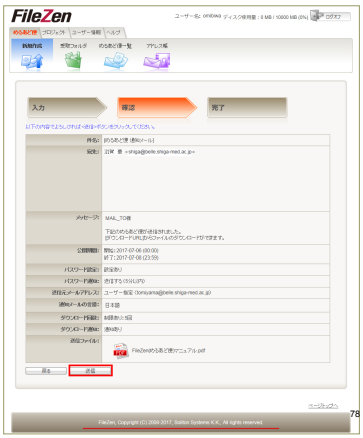
7. 「PDF保護」の設定をする。※PDFファイルを共有する時に使用。
- PDFの保護を有効にするとダウンロードしたPDFは編集不可、及び印刷・テキストコピーの制限等をかけることができます。



8. 「送信ファイル」を選択し、「送信内容確認」をクリックする。
- 一度に共有できるファイル数は5つまで。
- アップロードできるファイルの合計サイズは1アカウントにつき1ファイル2GB:合計10GB※まで。※すべてのめるあど便・受取フォルダの合計

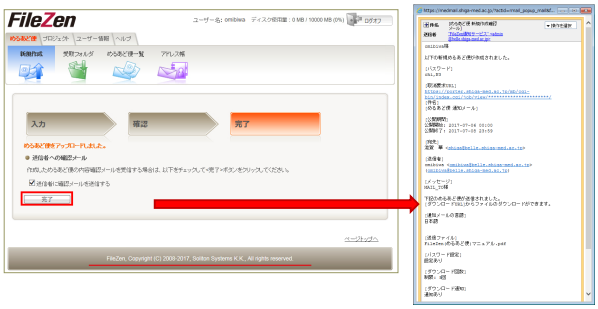


9. 送信内容を確認し、「送信」ボタンをクリックする。



10.「完了」ボタンをクリックすると宛先に送信される。

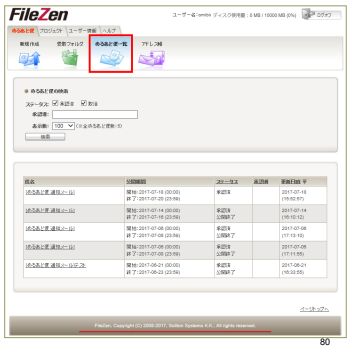
- 「送信者に確認メールを送信する」に☑が入っていると送信した内容を確認できるメールが届く。



送信している「めるあど便」の確認方法

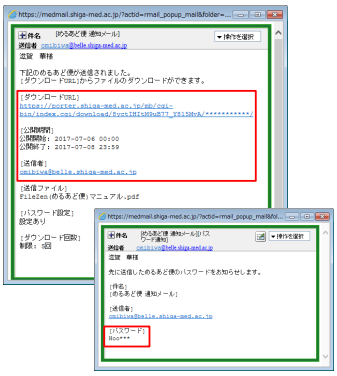
「めるあど便」タブの「めるあど便一覧」を選択する。

- 送信した履歴、ステータス等を確認することができる。
- 件名のリンクをクリックすると設定の詳細やファイルをダウンロードしたユーザー（アカウント）が確認できる。
  ※パスワードは確認不可
- めるあど便の取消・再利用することができる。
  ※再利用は宛先の設定を保持した状態で新規作成できる。

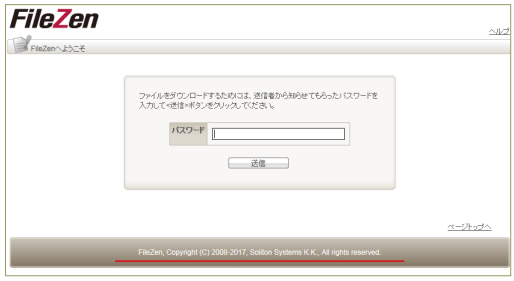


ファイルの受信の仕方

1. FileZen(めるあど便)から通知メールが届く。
2. 送信者、公開期間、パスワードを確認し、ダウンロードURLをクリックする。



3. パスワード入力画面が表示されるので、メールで通知されたパスワードを入力する。



4. ダウンロード画面が表示される。
   - ファイル名または、アイコンをクリックするとダウンロードが開始される。
   - 終了後は「ログオフ」してください。

ファイルがダウンロードされたら…

「ダウンロード通知」をデフォルト設定のまま「通知あり」にしておくと、ファイルがダウンロードされた際、送信者に「ダウンロード通知メール」が届きます。

パスワード強度の体験

ファイルのパスワードによる暗号化保護と解読の難易性についての実習資料

パスワード強度の体験（実習の流れ）

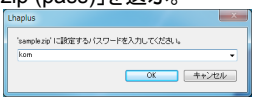
- 圧縮・解凍ソフト「Lhaplus」（フリーソフト）を使ったパスワード付き圧縮ファイルの作成
- 同ソフトを使ったパスワードの解読
- パスワードの文字数を変えるとパスワード解読に掛かる時間がどのように変化するか各自で確認してください

パスワード付き圧縮ファイルの作成

例として「sample.pdf」というファイルでパスワードをつけて圧縮する手順を示す。フリーソフトの「Lhaplus」を使う。

ファイルアイコンを選択し、右クリック

「圧縮」メニューを選び、「.zip (pass)」を選ぶ。

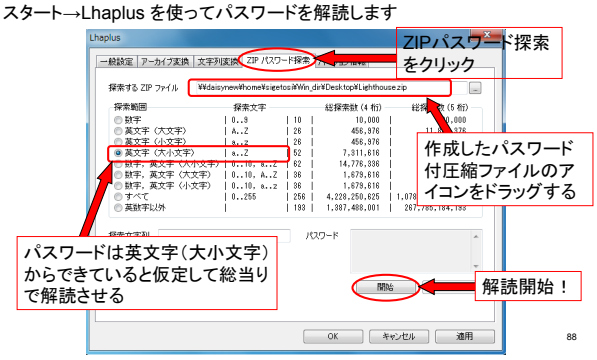


設定するパスワード(3桁)を入力する。

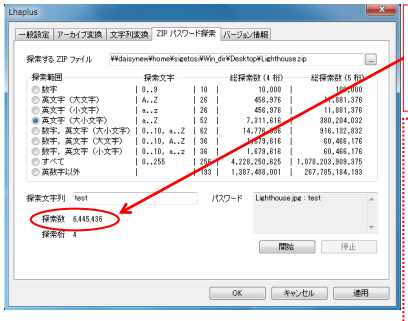
圧縮ファイルの完成。
ダブルクリックして確認。

圧縮ファイルのパスワード解読

スタート→Lhaplus を使ってパスワードを解読します



パスワード解読結果



総当り6,445,436回目で解読完了！

4桁程度であれば短時間で解読できました。

それでは、パスワードの桁数を5桁以上にすると解読にどのくらい時間がかかるか確かめてください。

パスワードに英数字や記号を組み合わせるとパスワード強度が上がる理由がわかりましたか？

パスワードの桁数と強度

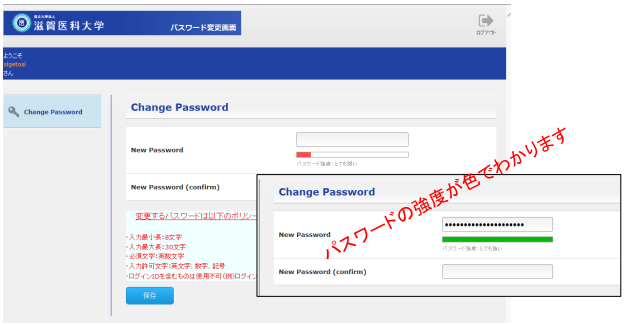
使用する文字の種類	使用できる文字数	最大解読時間 入力桁数 4桁	6桁	8桁	10桁
英字（大文字、小文字区別無）	26	約3秒	約37分	約17日	約32年
英字（大文字、小文字区別有）＋数字	62	約2分	約5日	約50年	約20万年
英字（大文字、小文字区別有）＋数字＋記号	93	約9分	約54日	約1千年	約1千万年

※すべての組み合わせを試すために必要な時間を計算。記号は31文字使用できるものとした。使用パソコンOS：Windows Vista Business 32bit版、プロセッサ：Intel Core 2 Duo T7200 2.00GHz、メモリ：3GB

上記の表は、情報処理推進機構（IPA）より転載
http://www.ipa.go.jp/security/txt/2008/10outline.html

パスワード強度の確認

パスワード強度の確認



92

END

93