

# Hello, Tablet!

今からでもできるICT活用

## CONTENTS

vol.4

- | 簡単なことからICT活用！
  - ・フォームを活用しよう
  - ・連絡でクラウドを活用しよう
- | あると便利な外部機器
- | 接続コネクタの豆知識
- | コンピュータウイルスに注意

見たい項目をクリック 



ご意見、ご感想をこちらのフォームからお寄せください。→

# 1人1台タブレット端末

## 今からでもおそくない！ 簡単なことからICT活用！

### 1人1台端末整備から約1年

2021年は、GIGAスクール元年と呼ばれ、1人1台タブレット端末が整備されました。クラウドや学習支援アプリケーションをはじめとするICT活用において、マニュアルがない中で、まさに試行錯誤の連続だったのではないのでしょうか。

また、非常時において、オンライン授業は欠かせないものとなっています。学びの保障という側面においても、ICT活用の必要性と利便性を感じたことも多かったと思います。

しかしながら、ICTを使うと児童・生徒が操作に苦勞して授業が進まないという声も聞かれます。ICT活用を進めるには、児童・生徒、教員が使い慣れていくことが大切です。

### 児童・生徒が使い慣れるように

vol.1では、児童・生徒が端末に触れる機会を増やし、日常的に使っていく習慣を作ろうということをお伝えしました。教員の教具ではなく、児童・生徒が文具として使うことができるように、使う機会を増やすことが大切です。デジタルの課題を使ったり、連絡やアンケートをクラウドで行ったりして、使用頻度を増やしましょう。

### 今からでも遅くない

このvol.4では、普段の学校生活で、デジタル化に取り組みやすい事柄について紹介させていただきます。

今からでも遅くありません。やってみることが大切です。

# フォームを活用しよう

## アンケートフォームのメリットとデメリット

アンケートフォームを健康観察や小テストなどに活用されている先生方は多いと思いますが、出欠連絡や懇談の日程調整にまで活用を広げることに抵抗を感じてはいませんか。

アンケートフォームはデータの収集や集計が手軽にできる一方で、本当に本人が入力しているのか確認することが難しいという課題があります。特に出欠連絡や懇談の日程などは確実に保護者に入力してほしいものでしょう。

## ひと工夫で簡単にパスワードをかけられる

この課題を解決する方法の一つとして、フォームの回答項目にパスワードの入力欄を設けるといことがあります。保護者にだけパスワードを通知しておき、回答する際に入力してもらうことで、パスワードを知らない人は回答を完了できないようにすることができます。可能であれば、入力結果を入力者にメール送信する設定にしておけばより安心です。

アンケートフォームを出欠連絡に活用することで、電話対応の時間を減らすことができ、連絡の内容もデータとして自動的に保存されるので、児童・生徒に対して改めて連絡する際のデータベースとして役立てることができます。

作り方はリンク先の動画をご覧ください。

Googleフォームでパスワード保護する方法

<https://youtu.be/s1y-PfvvJjA>



# クラウドで連絡を取り合おう

## 掲示板・ストリームの機能を活かそう

Microsoft Teams や Google Classroomの掲示板やストリームは、文字列やデータファイルを投稿でき、たくさんのメリットがあります。操作も簡単ですので、積極的に使っていきましょう。

## 掲示する順番や場所を変えて効果的に

掲示板機能をもつアプリケーションでは、通常は投稿日時が新しいものが一番上に表示されます。行事予定など一定期間掲示しておきたい情報は、掲示場所を変えて一番上に移動するなど、必ず目にとまるようにしておくことで、見る人が情報を確認しやすくなります。



## 掲示板やストリームのメリット

- ・手書きして紙での提出が必要な書類のデータを投稿  
→児童・生徒がその書類を紛失した場合も家庭で印刷できる。
- ・様式が決まっている進路調査などは入力可能なファイル形式で投稿  
→生徒が各自で入力して提出することができる。
- ・アンケートフォームURLなどの複雑な文字列を投稿  
→クリックのみで様々なデータに簡単にアクセスできる。

## 児童・生徒とともに使い慣れよう

クラウド活用の利点はいつでもどこでもアクセスできる点にあり、長期休業や臨時休校での連絡では、特に効果を発揮することができます。そのためにも簡単な操作から始め、使い慣れていくことが大切です。

使い方に慣れたら、委員会や係からの連絡という形で児童・生徒がクラスに対してお知らせを投稿するという運用の仕方も主体的な活用を促す一つの方法になります。

# あると便利な外部機器

タブレット端末で入力したり、テレビ会議をしたり、画面を投影したりする場合に、外部機器を使うことで活用の幅を広げることができます。あると便利な外部機器を紹介します。

## スタイラスペン（タッチペン）



タブレット端末用のペンです。画面の細かい部分をタッチすることが可能で、細い線や細かい絵を描くことができます。手書き入力のスピードも上がり、作業効率を上げることができます。

## スプリッター



情報を分配する機器です。写真は、ピンプラグで入力された音声データを5つに分配することができます。HDMIの分配器もあり、映像を分配することができます。

## イヤホンマイク・ヘッドセット



オンライン会議をするときには必須の機器です。ハウリングを防いだり、音声をクリアに伝えたりできます。接続方法はピンプラグやUSBがあります。

## ビデオキャプチャ



オンライン会議でホームビデオカメラを使用したいときに使います。HDMI端子はカメラと接続、USB端子はPCのポートに挿し込んで使用します。

# 接続コネクタの豆知識

外部機器をタブレット端末と接続して使用する際には、様々な接続コネクタを利用します。外部機器、端末によって接続可能なコネクタが違いますので、購入の際には気を付けましょう。ここでは、一般的な接続コネクタを紹介します。

## 一般的に広く使われているコネクタ

USB Type-A



Type-B



mini-B



micro-B



Type-C



USBは、WindowsやChromebookなど、多くのタブレット端末、パソコンで接続が可能です。最近では、USB Type-Cが使えるiPadもあります。

## iPhoneやiPadで使われているコネクタ

Lightning



iOS端末でのみ使われています。このコネクタで様々な外部機器を接続でき、充電ケーブルとしても使用されます。

## 音声や映像を転送するコネクタ

モニター、プロジェクター、ヘッドセットなどと接続するコネクタです。

HDMI



音声と映像を1本のケーブルで転送できます。写真のように、コネクタはサイズの違いで3種類あります。

VGA



映像のみを転送できます。最近ではHDMIに置き換わりつつあり、あまり見られなくなってきました。

3.5mmピンプラグ



音声のみを転送できます。ピンプラグには極の数が違うものがあり、極数によって用途が違いますし、プラグを差し込むジャックにも極数に対応したものがああります。詳しくは、別で紹介しています。↓こちらからどうぞ

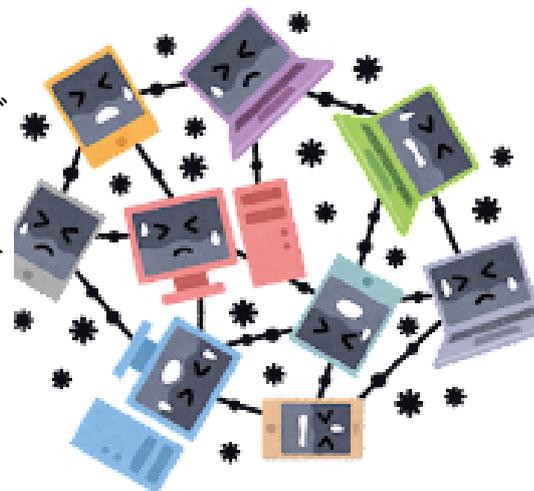


<https://www.fukui-c.ed.jp/~fec/wp-content/uploads/2022/02/tab4-2-220224.pdf>

# コンピュータウイルスに注意

## コンピュータウイルスとは・・・

風邪ウイルスがヒトの体内に侵入して細胞で増殖し、ヒトからヒトへ感染していくように、パソコンなどの端末内にあるドライブに侵入し、知らない間にインストールされるプログラムのことです。



## コンピュータウイルスの種類

コンピュータウイルスにもさまざまな種類があり、それによって引き起こされる被害もそれぞれ違います。

パソコン上の実行プログラムに感染し、プログラムを書き変えて本来と違う動作をさせるものや、悪意のあるプログラム自身がコピーされ増殖していくものがあります。

さらに、ウイルスプログラム自身は増殖せず、インストールされた状態で静かに潜んでいて、メールアプリを開いたときに動作してメールアドレスなどの情報を抜き取るものや、ExcelやWordのファイルに悪意のあるマクロを組み込み、開いたときに動作するものがあります。

## おもな感染経路は

ウイルスを含んだプログラムデータは、おもに次のような経路で端末内に侵入してきます。

- ・ Webサイトからファイルをダウンロードしたとき
- ・ USBメモリや外付けドライブなどを接続したとき
- ・ E-mailに添付されているファイルを開いたとき

E-mail本文にURLが掲載されていてWebサイトへ誘導するものもあります。



## 騙されやすいウイルス感染パターン

悪意のあるマクロが組み込まれたExcelなどのファイルは、E-mailによって送信されることがほとんどです。

このようなウイルスを送りつけてくるメールは、メール本文やファイル名、ファイル拡張子を偽装してあるため、受け取った人は、あたかも知っている人から届いたメールのように思ってしまいます。このようなメールは、特定の人のアドレス帳に載っているメールアドレスをもとに作られていることが考えられます。



## 感染しないために注意すること

アップデート、ウイルススキャンをまめに行う

端末のOSには、ウイルスをブロックする仕組みがあります。その仕組みを活用するためにもOSを常に最新の状態に保つ必要があります。OSやウイルス対策ソフトの更新（アップデート）は必ず行いましょう。また、USBメモリについてもウイルス対策ソフトでUSBメモリを「スキャン」してから使用すると安心です。



不審なメールに記載されたURLや添付されたファイルを開かない

知らないアドレスから送信されたメールや、本文がたどたどしい日本語で書かれているメール、信頼できる署名がないメールなど、不審なメールに記載されたURLや添付されたファイルは開かずに削除しましょう。

また、上述の騙されやすい感染パターンのように、知人を装ったメール（ドメインが違うなど）を受け取った場合は、偽装されている本人に連絡を取りましょう。同一グループのアドレスに一斉送信されている可能性があるため、危険を共有し、注意喚起することができます。特に、学校で使っているアドレスに不審メールが届いた場合は、ネットワーク管理者や教育委員会にも連絡しましょう。

おかしいかな？不審メールかな？と思ったら検索する

巧妙に偽装し業者や公的機関になりすましてメールが送られてくることがあります。このメールあやしいかな？と感じたら、書かれているメール本文をインターネットで検索すると、過去の被害情報と一致することがあり、有害なメールであると気づくことができます。