

Classi

セキュリティ ガイド

安全にご利用いただくために



Classi はセキュアなクラウドサービス^{※1}です

「Classi」は、各基準・ガイドライン^{※2}に沿ったクラウドサービスを利用した安全なオンラインサービスです。また、より安心してご利用いただけるよう、セキュリティ対策会社から定期的に監査およびセキュリティ診断を実施しております。IDおよびパスワードや、ダウンロードしたデータのお取り扱いについては学校様で管理していただく必要がございますので、この冊子をよくお読みになって、各先生にセキュリティ対策の周知・徹底をお願いいたします。

※1)クラウドサービスとは、インターネット(クラウド)上にデータを保存するサービスです。パソコンのハードディスク等の記録媒体にデータを保存せずご利用いただけます。

※2)Classiは各基準・ガイドラインに沿ったクラウドを利用しております。安全にサービスを提供するよう、セキュリティ・品質マネジメント資格としては各種基準・ガイドライン(以下①-④)に準拠している「日本国内エリア」を利用します。

①PCI DSS (ペイメントカード業界データセキュリティ基準)レベル1 ②情報セキュリティ ISMS(ISO/IEC27001) ③品質マネジメント (ISO9001) ④ISMSクラウドセキュリティ認証(ISO/IEC 27017) 等

安心・安全への取り組み

SSL/TLS通信と厳重なデータ保管ルールで、大事な情報を守ります。



- Classiは、SSL/TLS方式の通信で暗号化しデータを保護しています。通信時に悪意ある第三者に内容を覗かれることはありません。

SSL/TLSはインターネットバンキングやインターネットショッピングの際のクレジットカード情報転送にも利用される、信頼性の高い通信技術です。

- 学校の指示があれば、校外からのアクセスを制限することもできます。公衆無線WiFiや自宅などからはアクセスができなくなり、盗聴の危険性が低減します。

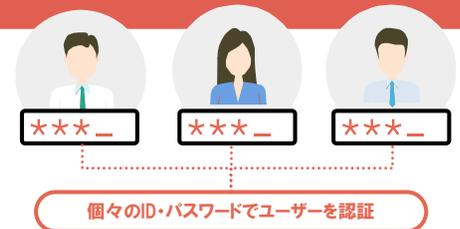
→ p.7参照

- Classiに保存された個人情報を含むデータは、安全なデータ格納方式で管理しています。
- また、ユーザーがClassiにアップロードするデータは、暗号化されているなどの特定の場を除き、アンチウイルスソフトウェアで自動的にウイルスチェックされます。
- Classiのデータベースは、権限を持つごく一部の社員しかアクセスできません。作業内容は記録され、厳重に管理されます。

Classiにアクセスするには、IDとパスワードが必要です。

Classiへのログインは、ユーザー個人にそれぞれ発行されるID・パスワードで認証されます。(発行された後はユーザーが各自でID・パスワードを自由に変更できます) ログイン後も、特に重要な個人情報を表示・入力する画面ではパスワードを再入力していただけます。ID・パスワードの管理・お取扱いは各位でご確認ください。

→ p.6参照



Classiは安全にご利用いただくための取り組みを各種おこなっておりますが、学校様でもセキュリティにご配慮いただき、対策を徹底していただく必要がございます。高度な技術や悪意を持った侵入者による学校への不正アクセスを完全に防ぐことはできませんが、二重・三重の安全管理によって万が一の被害を最小限に抑えることができます。

生徒が職員室などに簡単に入室することができる環境では、ID・パスワードが他人の目に触れる場所に貼ってあったり、推測され

やすい安易なパスワードが設定されているといった「ふとしたはずみ」や「不注意」から不正アクセスに繋がるケースもあります。このガイドは、学校にどのような情報セキュリティリスクが潜んでいるかを把握していただき、各自での対策と周知をお願いするためのものです。また、校内の情報管理運用規定を策定することもおすすめいたします。

安全にご利用いただくために、Classiでは以下のような取り組みをおこなっております。



先生ごとに「Classi管理者権限」と「閲覧権限」を設定できます。

Classiは「Classi管理者権限」と「閲覧権限」の二種類の設定によって先生ごとに操作できる機能や扱える生徒の範囲を限定できます。先生のそれぞれの立場に応じて、操作・閲覧できる範囲を最小限に設定しておけば、不必要に生徒の個人情報や学校の機密情報が人目に触れることはありません。万が一パスワードが流出したときにも、被害の範囲を狭められます。

「Classi管理者権限」とは

操作できる**機能の範囲**を限定するためのものです。Classiは「管理責任者・管理者／機能限定管理者／一般（初期設定）」の4種類の権限が設定できます。例えば、時間割など学校や学年全体に関わる設定は「管理責任者・管理者」権限の先生しかおこなえません。

「閲覧権限」とは

閲覧・出力できる**生徒の範囲**を限定するためのものです。「権限」とは別に、管理責任者の先生は、それぞれの先生の立場に合わせて、閲覧・出力できる生徒の範囲を細かく設定できます。例えば、野球部顧問の先生は「担当クラスの生徒」と「部活の生徒」のみ閲覧・出力できるように設定しておけば、他のクラスや他の部活の生徒の情報は表示されなくなります。

管理者の任命権限	学校全体に関する設定権限	成績や志望校の登録権限	自分に関する設定権限	〈 設定例 〉					
				学年・クラスの閲覧範囲	部活の閲覧範囲	成績の閲覧	指導要録の閲覧	通知表の閲覧	...
管理責任者	管理責任者	管理責任者	管理責任者	Classi管理責任者の先生	全員	全員	✓	✓	✓
×	管理者	管理者	管理者	学年主任の先生	全員	全員	✓	✓	✓
×	×	機能限定管理者	機能限定管理者	クラス担任の先生	全員	全員	✓	×	×
×	×	×	一般ユーザー	教育実習生	担当クラスの生徒のみ	担当部活の生徒のみ	×	×	×

初期設定ではClassiお申し込み時に設定していただいた先生が「管理責任者」です。

その他、「委員会」で閲覧範囲を制限したり、志望校、学籍情報、調査書等の閲覧を制限したり、帳票出力の禁止などが設定できます。

→ 詳しくは別冊子「設定・登録ガイド」をご覧ください。

学校にはこんな情報セキュリティリスクがあります！

学校内にあるリスクを把握し、対策と周知の徹底をお願いいたします。

レベルの見かた



全員
Classiをご利用のすべてのユーザーが対象となる項目です。



管理者
Classiの「管理責任者」「管理者」「機能限定管理者」権限の先生が対象となる項目です。



IT担当者
学校でのIT（通信、パソコン）を管理する先生が対象となる項目です。

次ページへ



学校に
潜む

情報セキュリティリスク



Classiの

IDとパスワード の管理不足で…



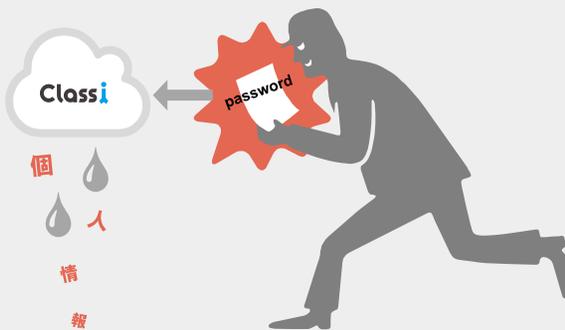
パソコン スマートフォン、 タブレット の管理不足で…

不正にアクセスされて



個人情報・機密情報の流出

IDとパスワードが漏洩してしまうと、「なりすまし」による不正アクセスにつながります。
パスワードをメモした紙やテキストファイルを盗まれることで漏洩するケースのほか、推測されやすいパスワードだったために簡単に見破られてしまうケースなどが考えられます。
また、Webブラウザにはパスワードを保存しておける機能がありますが、Classiなど個人情報を扱うサイトのパスワードには絶対に使わないようにしましょう。



対策しましょう ▶

p.6

パソコンを盗み見られて



個人情報・機密情報の流出

Classiにアップロードされた情報は、IDとパスワードが無いと閲覧できませんが、パソコン上に保存したダウンロードファイル類は学校・各先生の手任せられます。
パソコンやタブレットなど個人情報を保存している端末には必ずパスワードをかけ、秘匿性の高いファイルは暗号化するなど、二重・三重の安全管理をおすすめします。

ウィルス感染して



個人情報・機密情報の流出

ウィルスの感染経路にはさまざまなものがあります。不審なメールの添付ファイルをクリックすることで感染するタイプや、メールに記載されたリンクをクリックするとマルウェアをダウンロードさせるタイプ、ソフトウェアの脆弱性を悪用し感染するもの、外部記憶媒体経由で感染するもの、偽のソフトウェアをダウンロードさせインストールさせるもの…。手口は年々複雑に、巧妙になっています。いったん感染してしまうと、除去が難しく被害が拡大するおそれがあります。感染する前に信頼できるウィルス対策ソフトをインストールしておくことが肝要です。

対策しましょう ▶

p.8

情報漏えいは、システムの脆弱性によるものだけでなく、パスワードの管理不足や、SNSの間違った使い方など「ちょっとした不注意」によっても引き起こされます。下記のようなセキュリティリスクにご留意いただき、**厳重な管理・対策**をお願いいたします。



印刷物

成績表や
評価の一覧等

の管理不足で…

Classiからダウンロードしたデータは、生徒に配布できる成績表や、会議に利用できる評価一覧など、さまざまな形でご利用いただけます。印刷された帳票にも個人情報が含まれていることにご留意いただき、厳重な管理をお願いいたします。

生徒を取り違えて

(間違った生徒に渡してしまう)



個人情報・機密情報の流出

生徒情報や成績の登録を誤ると、本来の生徒とは別の生徒に成績表が渡ってしまうことがあります(生徒の取り違え)。個人情報が意図しない生徒の目にふれることとなりますので、個人情報に関わるデータを登録するときは、先生同士のクロスチェックなどで入念に確認し、確実に登録するようにしてください。

紛失・盗難されて



個人情報・機密情報の流出

印刷したものを不用意に放置しておくことで、内容を盗み見られたり、紛失してしまうリスクが高まります。少しの間でも放置せず、カギ付きのキャビネットに保管するなど、厳重にお取り扱いください。

対策しましょう ▶ p.10

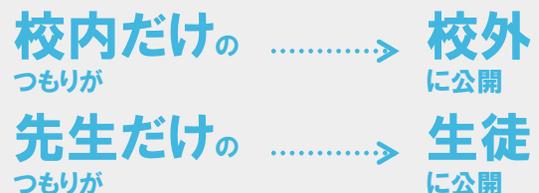


SNS

ソーシャル・ネット
ワーク・サービス

の使い方を誤って…

Classiのコミュニケーション機能では、校内の先生同士や生徒、さらに保護者や校外の先生ともコミュニケーションができます。スマートフォンからメッセージを送信したり、SNSに投稿したり、手軽にコミュニケーションをとれる反面、使い方を誤ると意図せぬ個人情報漏えいや「炎上」につながるおそれがあります。



個人情報・機密情報の流出

炎上・評判の低下



公開された情報は容易にコピーが可能のため、本人が投稿を削除しても、コピーされた内容で拡散が止まらない場合も考えられます。

SNSは多くの人の目にふれる公的な場であるという意識を持ち、投稿する内容や公開範囲には十分ご注意ください。



対策しましょう ▶ p.11



***_

ClassiのIDとパスワード

を管理しましょう

✓ パスワードは他人に推測されにくいものにしましょう



- ・他のサービスで利用しているものと同じID・パスワードを設定しないでください。
- ・推測されにくい文字列を使ってパスワードを設定しましょう。「自分の名前」「学校の名前」「クラス」「通し番号」「地域名称」の使用は避けてください。
- ・設定したパスワードを付箋でパソコンの周りに貼り付けるなど、第三者の目に触れる形でのパスワード管理は絶対にしないでください。
- ・パスワードを記載したテキストファイルを端末に保存することはしないでください。

注意 端末(パソコン、スマートフォン、タブレット等)にも必ずパスワードを設定してください。→ p.8

推測されてしまう例

複雑なパスワードは覚えてられないから…



田中さんの誕生日は1948年3月26日…



不正ログイン成功



😊 安全なパスワードの考え方

- ・パスフレーズ(好きな言葉や歌の歌詞など、ある程度長い日本語をローマ字に変換したもの)
- ・各サイトを示す識別子を付与して使いまわしを防ぐ

sukina1utano2kashi3#cl ←Classi用
sukina1utano2kashi3#tw ←Twitter用
sukina1utano2kashi3#tt ←TikTok用
!#%&…など使う記号を一つ決める」…など

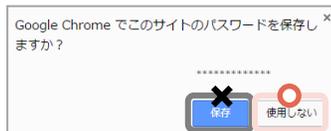
☹️ 危険なパスワードの例

- ・名前と誕生日の組み合わせ
- ・「P@ssw0rd」など、単語ひとつだけ
- ・ペットや好きな芸能人の名前など、容易に類推ができるもの

✓ ブラウザのパスワード保存機能は利用しないでください



Classiのような個人情報を扱うサイトでは、WebブラウザのID・パスワード保存機能は利用しないようにしましょう。



✓ IDの貸し借りは絶対に行わないでください



一時的であっても、自分のIDとパスワードを貸して他の先生にログインさせる「IDの貸し借り」はしないようにしてください。(例:教育実習生に自分のIDでログインさせるなど)



不正アクセス？
なりすまし？
おかしいと思ったら…



身に覚えのない操作がされていたり、意図しないデータの変更を発見した場合は、すみやかに「管理責任者」の先生とIT担当の先生に連絡して下さい。IDとパスワードが他人に知られてしまっており、なりすましでアクセスされている可能性があります。パスワードをそのままにしていると他人からアクセスされ続けてしまいますので、気付いたらすぐにパスワードを変更しましょう。

Classiには自分のログイン履歴を確認できる画面がありますので参考にしてください。

「Classi管理者権限」と「閲覧権限」を適切に設定しましょう



Classiは、前述(p.3)のとおり、ユーザーに「Classi管理者権限」と「閲覧制限」を設定できます。業務上必要のない情報を閲覧したり、登録できないようにすることで、パスワード流出など万一のときの被害範囲を狭めることができます。誰にどの権限を付与するか、プランをたててから設定してください。どの権限を与えるべきかわからないときは、**最も閲覧・出力範囲の狭い権限を付与しておき、必要に応じて段階的に範囲を広げていくこと**をおすすめします。年度変わりの時期には、学校の状況にあわせて権限の内容を見直してください。

Classi管理者権限

利用できる機能を制限するためのものです。例えば、「管理者」になると学校全体や学年全体に関わる操作ができるようになります。

→ 権限の種類と設定方法は、別冊子「設定・登録ガイド」の「管理者権限の付与」を参照

管理責任者・管理者

Classiのすべての設定をおこなうことができる先生です。

機能限定管理者

成績・授業に関する設定をおこなえます。
「成績と授業」または「成績のみ」の2種類設定しています。

一般(初期設定)

個人設定と、座席表の作成のみおこなえます。
権限を付与されていない場合は、すべてこちらに設定されています。

閲覧権限

閲覧・出力できる生徒の範囲を限定できます。担当クラスの生徒のみ表示したり、担当クラスでなくても顧問をしている部活に所属する生徒は閲覧できるようにするなど細かく設定できます。あらかじめサンプルとしてよくある閲覧範囲の設定が登録されています。自由に設定を変更したり権限を追加したりできますが、あまり増やしすぎると管理がかえって難しくなることがあります。

	A	B	C	D	E	閲覧権限
1 権限名	顧問担当学年・クラス	顧問担当 授業	顧問担当 部活	顧問担当 委員会	顧問担当 委員会	閲覧権限
2 管理権	全員	授業の条件を使わずに	部活の条件を使わずに	部活の条件を使わずに	委員会の条件を使わずに	○
3 部活	全員	授業の条件を使わずに	部活の条件を使わずに	部活の条件を使わずに	委員会の条件を使わずに	○
4 学年主任の先生	担当学年まで	担当する授業の生徒のみ	担当する部活の生徒のみ	担当する委員会の生徒のみ	担当する委員会の生徒のみ	○
5 高校担当の先生	担当クラスのみ	担当する授業の生徒のみ	担当する部活の生徒のみ	担当する委員会の生徒のみ	担当する委員会の生徒のみ	○
6 中学校担当の先生	担当クラスのみ	担当する授業の生徒のみ	担当する部活の生徒のみ	担当する委員会の生徒のみ	担当する委員会の生徒のみ	○
7 担任先生以外	担当クラスのみ	担当する授業の生徒のみ	担当する部活の生徒のみ	担当する委員会の生徒のみ	担当する委員会の生徒のみ	○
8 講師の先生	学年・クラスの条件を使わずに	授業の条件を使わずに	部活の条件を使わずに	委員会の条件を使わずに	委員会の条件を使わずに	×
9 事務長、事務の担当役員	授業の条件を使わずに	授業の条件を使わずに	部活の条件を使わずに	委員会の条件を使わずに	委員会の条件を使わずに	×

→ 設定方法などは別冊子「設定・登録ガイド」の「閲覧権限の設定・登録」を参照

退職・異動した先生はすぐに**利用停止**にしましょう



退職、異動した先生のアカウントは速やかに「**利用停止**」にして、ログインできなくしましょう。

「**削除**」ではなく「**利用停止**」にしましょう。

「削除」してもログインできなくなりますが、その先生が作成・共有したコンテンツも引き続き利用する為に、「利用停止」にすることをおすすめします。
([設定・登録]>[先生情報]画面で「利用停止」にできます。)



IPアドレス制御もご利用ください



IPアドレス制御のオプションサービス(無償)にお申し込みいただくと、ClassiにアクセスできるIPアドレスを制限できます。IPアドレス制御を利用すれば、先生機能全体あるいは特に秘匿性の高い機能(設定・登録、生徒カルテ、帳票出力、ポートフォリオ)に指定外のIPアドレスからアクセスできなくなります。お申し込みに関してはお問い合わせ窓口までご連絡下さい。





パソコン

スマートフォン、
タブレット

を管理しましょう



端末にパスワードをかけましょう



全員

パソコンの場合

- ・パソコンの**起動時のパスワード**を必ず設定しましょう。
- ・パソコン操作中に**離席する時は、画面をロック**するようにしましょう(Windows®の場合は、「Windowsキー+L」でロックできます)。**ロック解除のときもパスワードを求められるよう設定しておきましょう。**

タブレット・スマートフォンの場合

手軽に使えるのがタブレットやスマートフォンの良さですが、同時に盗み見られるリスクも高いものです。個人情報を扱う端末であることを念頭に置いて、**端末には必ずパスワードを設定**しましょう。

注意 端末には必ずClassiのパスワードとは別のパスワードを設定してください



すべての端末にセキュリティソフトを入れましょう



IT担当者

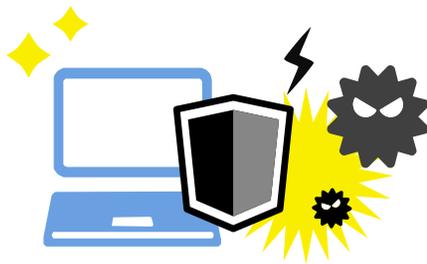
パスワードを厳重に管理していても、ウイルスに感染してデータが搾取され、外部に漏れ出せば意味がありません。ウイルスの脅威から重要な情報を守るには、**感染する前に信頼性の高いセキュリティソフトを導入**しておきましょう。また、フリーウェアのセキュリティソフトは信頼性に問題があるものもありますので、利用しないようにしてください。



セキュリティソフトを常にアップデートし、定期的にスキャンしましょう



全員



ウイルス対策には、セキュリティソフトを導入しておくのはもちろんのこと、ウイルスを検出する定義ファイルを常に最新にアップデートし、定期的なウイルスチェック(スキャン)をすることが大切です。

- ・ウイルスは日々進化しており、その進化に対応するために定義ファイルも**更新**されます。手動での更新は、忙しいと怠りがちになり、バージョンの劣化を招きますので、**自動更新されるよう設定**しておきましょう。
- ・セキュリティソフトの**ライセンス有効期限**に注意しましょう。
- ・「毎月1日」など、**日を決めて端末内をフルスキャン**するようにしましょう。リアルタイム検出をONにしても、検出が漏れる場合があります。
- ・**修正プログラムを適用**しましょう。セキュリティに関する脆弱性が改善されます。アップデートを怠ると脆弱性が放置され、ウイルスに感染しやすくなります。
- ・その他にインストールしているソフト(ブラウザなど)も同様に、**最新版にアップデート**しておきましょう。

感染した?と思ったら

ウイルスの型には、他の端末へ感染を拡大する「感染拡大型」、端末内の情報を盗み取る「情報窃取型」、遠隔から自由に端末を操作できる「遠隔操作型」などがあります。感染するとネットワークを経由して被害が拡大するおそれがありますので、動きがおかしいと思ったら**すぐにネットワークから隔離**し、原因を調査してください。



✓ 個人情報・機密情報を含むデータを管理しましょう

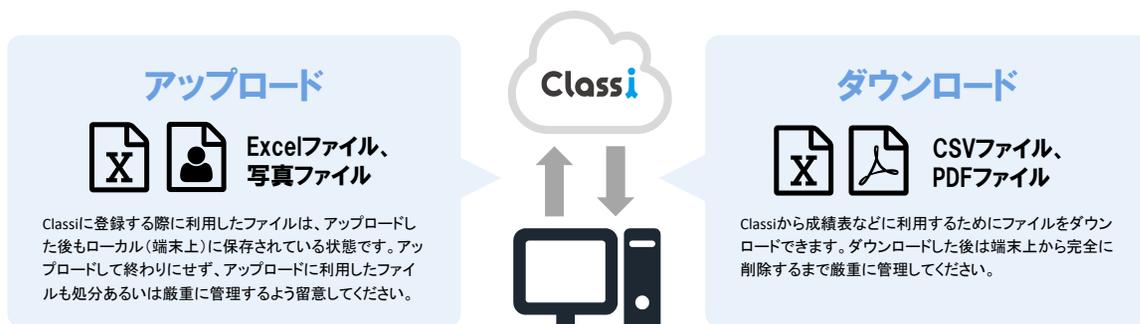


Classiからダウンロードしたファイルや、Classiに一括登録するために作成したCSVファイルなど、パソコン上に保存したデータについては、各先生の手で管理していただく必要があります。

無造作にデスクトップに放置したり、ゴミ箱に移動してそのままにしたりすることのないよう注意してください。

データを削除せずに保存しておく場合は、パスワード付きのファイルにしたり、パスワード付きのフォルダに保存して、第三者が簡単に閲覧できない形で保管してください。

※重要情報が記載されたエクセルファイル等をUSBメモリやSDカードなどの外部記録媒体に保存して持ち歩く場合も、端末上のデータと同様に注意してお取り扱いください。



登録後(または印刷後など)、使い終わったファイルを…

<div style="background-color: #0070c0; color: white; padding: 5px; font-weight: bold;">残したい</div>	または	<div style="background-color: #0070c0; color: white; padding: 5px; font-weight: bold;">廃棄する</div>
<p>パスワード付きファイルにする</p> <p>パスワード付きZIPファイルにまとめる</p> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> </div>		<p>ファイルを「ゴミ箱」に移動したあとは、「ゴミ箱を空にする」で完全に削除してください。</p>

自動で同期されるデータにもご注意ください

スマートフォンやタブレットをパソコンに接続したときに自動的に同期されるデータの管理にもご注意ください。充電目的で接続した場合であっても、データが知らず知らずのうちに同期されていることがあります。学校管理のセキュリティ対策がされていない端末と安易に接続しないようにしてください。





Classiから印刷した印刷物を管理しましょう

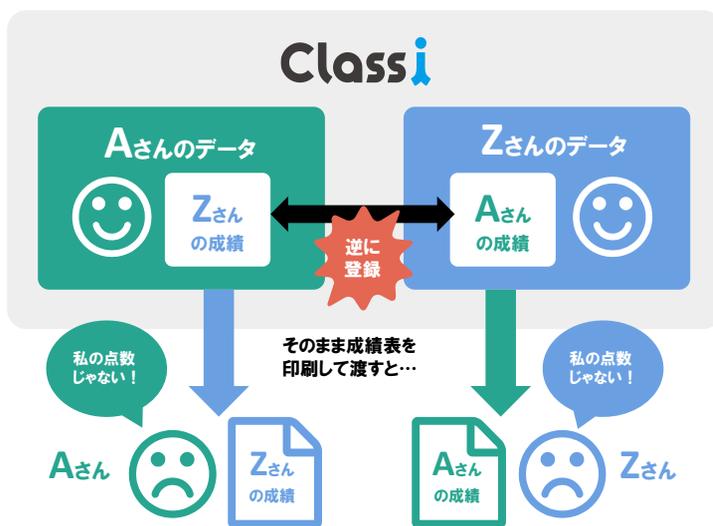
**必ず確認！** 成績表など個人情報配付する前に、確実にその生徒のものであることを確認しましょう

全員

Classiでは、登録されたデータの正誤についてはチェックされません。成績を登録すべき生徒を間違ってしまったら、本来の生徒とは別の生徒の手に個人情報が渡ってしまいます。登録ミスが無い先生同士でクロスチェックするなど、細心の注意を払って作業するようにしましょう。

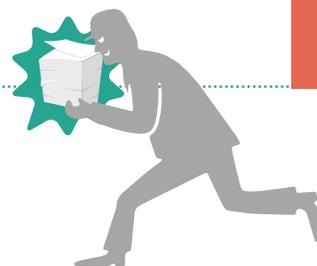
**登録ミスを防ぐために、権限は最低限に設定しましょう**

登録できる範囲が限定されていれば、間違いの範囲も狭められます。→ p.7参照

**印刷物の紛失・盗難・放置に気をつけましょう**

全員

- ・教室、部室、車の中などに放置しないようにしましょう。
- ・職員室などにある施錠できるキャビネット等に保管しましょう。
- ・不要になったものは機密文書として慎重に処分してください。

**生徒・保護者にもセキュリティについて周知を**

全員



IDやパスワード等の情報を印刷して生徒や保護者へ周知する場合、配付時に、その紙は慎重に取り扱う必要があることを説明しましょう。配付時は、資料と配付対象生徒に相違がないよう確認しながら配付し、配付し終わったら全員に自分の名前が記載されているか確認させましょう。また、生徒には、友だち同士で見せ合ったり、交換してはいけないこと、他のプリントなどに紛れて紛失することのないよう持ち帰るなど指導してください。保護者にも同様に適切な保管を依頼しましょう。欠席した生徒への配付は、後日渡すか郵送にするなどし、友達に預けることは避けましょう。



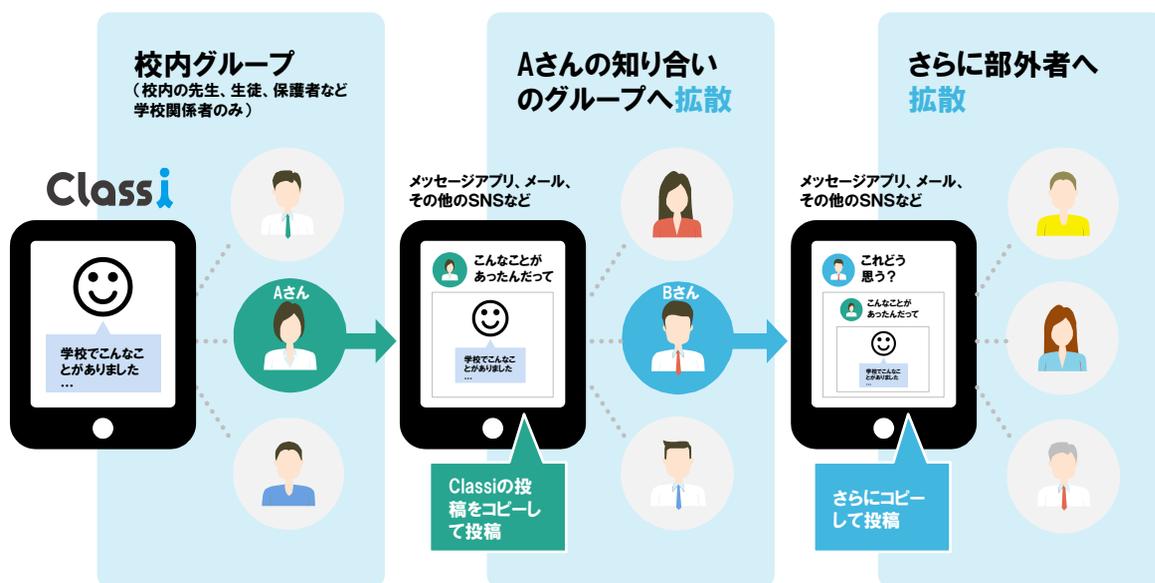
SNS(ソーシャル・ネットワーク・サービス)を適切に使いましょ

投稿内容に注意を払いましょ



ClassiのSNS機能では、校内の先生、生徒、保護者、校外の先生とコミュニケーションが図れます。多くの人とコミュニケーションができる分、公開する内容を注意深く選んでください。一度投稿されたものは、一瞬でも他人の目に触れてしまいますので、不適切な投稿などにご留意ください。投稿を削除しても、コピーされた内容が拡散されてしまうことがあります。

投稿が外部に拡散されてしまうパターン例



プロフィールの公開範囲と内容に注意を払いましょ



先生方のプロフィールは、初期設定では校内にのみ公開されますが、「すべての先生」に設定を変更すると、Classiをご利用のすべての先生方(校外の先生を含む)に公開されます。プロフィールには自己紹介文のほか、自分の写真も登録できます。多くの方の目に触れる情報であることを意識して、ふさわしい内容で登録してください。

自分のプライバシー設定の公開範囲を確認するには

ホーム画面の[設定・登録]ボタン>[プライバシー]で公開範囲の設定を確認できます。

プライバシー

メッセージと校外グループでの公開情報を設定します。

検索結果に自分を表示できる人 すべての先生 校内の先生

学校名を開覧できる人 すべての先生 校内の先生

プロフィールを開覧できる人 すべての先生 校内の先生

キャンセル 保存

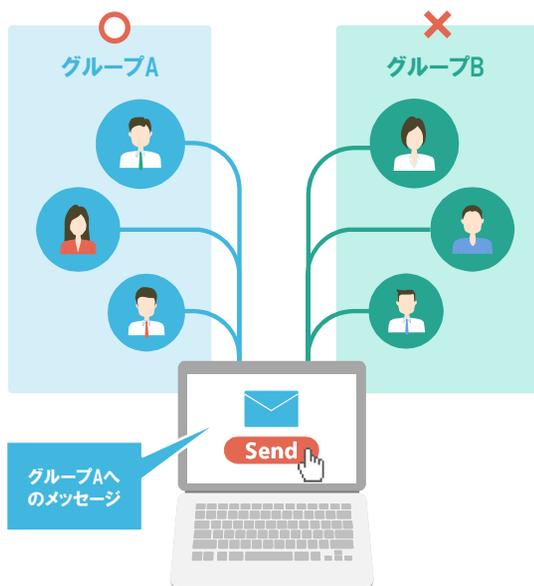
詳しい手順は別冊子「各機能ご利用ガイド」の「初回ログイン」を参照



公開先をよく確認しましょう



Classiでは、校内の資料を「校内グループ」機能を利用して共有できます。共有する資料の秘匿性が高いときは、公開するグループの選択に間違いのないよう、特に注意してください。特定の先生や生徒、保護者に関する資料やコメントが、他の人に見られてしまうと大きなトラブルに発展します。また、校外グループを利用する場合には、面識のない先生も多く閲覧しています。不適切な投稿により、学校や先生ご自身の評判を損なうことになりかねません。投稿する前に、そのグループに含まれているメンバーを確認してください。



そのグループに参加しているメンバーを確認するには



グループページの右上[編集]ボタンをクリックすると、そのグループに誰が含まれているか確認できます。

グループの設定方法などは別冊子「各機能ご利用ガイド」を参照



個人情報保護方針(プライバシー・ポリシー)などと同様に、あらかじめ**ソーシャル・メディア・ガイドライン**を策定しておくなどして、先生、生徒、保護者など学校関係者の中で、SNSなどの利用についてルール作りとその周知しておくことも対策の一つです。

ソーシャル・メディア・ガイドラインとは、ソーシャル・メディア・ポリシーともいわれ、企業や自治体などの組織において、私的にソーシャル・メディア(SNSなど)を利用する場合の、一定のルールを定め、それを遵守することで、私的な利用が組織の情報漏えいや炎上によるトラブルに発展することなどを防ぐためのものです。

Classiの個人情報ポリシーについて

- 個人情報保護方針は、Classiのコピーサイトをご確認ください。 <https://classi.jp/privacy.html> Classi 検索
- 個人情報取得に当たり、サービス申込時にClassi管理責任者の先生のご同意を確認させていただいております。ご同意いただけない場合は当サービスをご利用いただけません。ほかの先生については、その先生のサービス利用開始時(初回ログイン時)にご同意を確認させていただきます。
- 個人情報の利用目的について
 - 「管理責任者」について、先生を識別するために、以下の情報を利用しています。
 - 取得情報:先生が本サービスの利用者として登録する先生のお名前、学校・学科名
 - 利用者については、閲覧・利用・ダウンロード等の履歴などを機械的に取得し、本サービスの向上、研究・開発のために利用しています。
- 個人情報の扱いを懸念される場合
 - 個人情報の扱いを懸念される場合には、よりセンシティブな個人情報を扱う一部機能を制御してご利用いただけます。お申し込みに関してはお問い合わせ窓口までご連絡下さい。

・Internet Explorer®、Microsoft®、Windows®は、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

・Google Chrome™およびロゴは、Google Inc. の国際登録商標です。

Classi

お問い合わせ **0120-755640** 通話料 無料

受付時間 月～金8:00～19:00 土8:00～17:00 (祝日、年末・年始を除く)

※タブレットのご利用方法に関しては、ご契約される通信事業者または販売店等にお問い合わせ下さい。