情報システムの安全で適正な利用のお願い

1　白鷗大学のネットワーク

白鷗大学の白鷗情報ネットワークは、本キャンパス、大行寺キャンパスすべて、学内のネットワーク「ハークネット：HARCNET」に接続されています。
学内ネットワークは（本キャンパスは大行寺キャンパスを介して）インターネットへとつながっています。

2　セキュリティに関して

本学全体のネットワークである「ハークネット：HARCNET」 には、セキュリティ監視装置が設置され、全ての通信を 24 時間記録し、どのユーザーがいつどこのＰＣをどのように使用したかを「ログ」という履歴で管理をしています。学内のネットワーク利用状況を日常的に誰かが見ているということではありませんが、本学のネットワーク利用上の倫理基準の重大な違反や犯罪行為などが発生した際には、ユーザーを特定して対応することがあります。
（本学に限らず、アカウントを配布してネットワーク利用を許可している組織では、ユーザーの管理義務と犯罪などが起こった際に公的機関にログなどの記録を開示する義務があります。）

3　学内ネットワークを利用するには

白鷗大学では、学内ネットワークを利用するにあたり、次の 3 つのことを義務づけています。

3-1.「センターメール利用申請」をする。

利用規定を遵守するという誓約書として利用申請書を提出することによって、ユーザーID と有効化キー（パスワード）が発行されます。

3-2. 所定の講習を受ける。

入学時 PC 実習ガイダンスを受講し、ユーザーID（アカウントともいう）を受け取り、認証の為に独自に決めたパスワードを用いて学生アカウントの有効化を実施してください。この処理をしないと後述のサービスが利用できません。

3-3.「ネチケットテスト」に合格する。

学内ネットワークを利用するにあたり、基本的なルールを理解しているかを確認するため、「ネチケットテスト」を受験し、指定された期日までに合格することを必須としています。

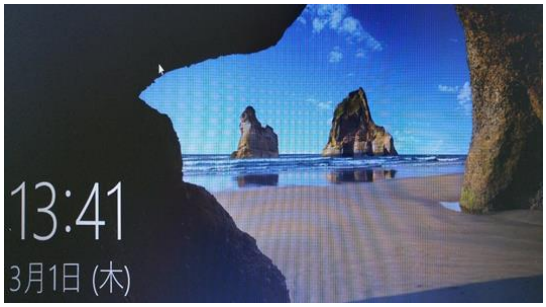
4　ID の取得（学生アカウントの有効化）

ユーザーID（学生アカウント）の設定方法

・ユーザーサインイン

① 発行されたユーザーID と有効化キー（パスワード）を準備します。

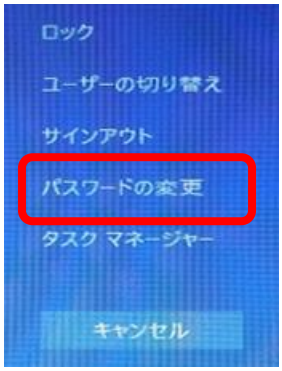
② 学内 PC を起動し下記の画面になりましたら、画面のどこかをマウスでクリックします。



③ サインイン画面が表示されたら、入手したユーザーID とパスワードでサインインします。

5　パスワードの変更

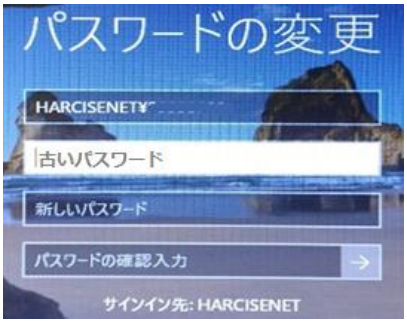
① サインイン後再度「Ctrl キー+Alt キー+Delete キー」を押し「パスワードの変更」を選択。



② 古いパスワードの欄をクリックし、4.（ID の取得）でサインインした際のパスワードを欄に入力してください。

③ 新しいパスワードの欄をクリックし、独自に決めたパスワードを入力します。

④ パスワードの確認入力欄をクリックし、もう一度新しいパスワードを入力します。



これで、ユーザーID とパスワードが有効になります。

※パスワードを忘れた場合、学生証を持参の上、次の場所で初期化してもらう必要があります。

本キャンパス：

東館 6F 情報システム室

大行寺キャンパス：

本館 1F 教務課内情報システム室ヘルプデスク

6　パスワードの適正な管理

本学のコンピュータシステムには、その利用を許可された者（利用者）のために、システムを利用する権利や利用者のファイル・情報などを保護することが求められます。そのためには利用者を特定する必要があり、その仕組みがユーザーID とパスワードになります。

ユーザーID は利用者個々に対応しており、これによりシステムはどの利用者が利用するのかを知ることができます。パスワードは利用しようとする者が、その人のみが知りえる情報としてシステムに伝えることにより、本人であることをシステムに示すためのものです。

本学コンピュータシステムはユーザーID とパスワードにより、利用者を特定し、利用を許可します。パスワードが正しければ本人が利用しているものとみなされます。このため、ユーザーID とパスワードは適正に管理する必要があります。

パスワードは他人に絶対教えない。

他人にパスワードを知られると、他人があなたのユーザーID を使って本学のコンピュータシステムや提携するサービスにアクセスし、あなたになりすまし、以下のような行為を行うことが可能になります。

・メールや保存してあるファイルを覗き見たり、勝手に変更したり削除したりされる。

・信用を貶めるようなメールの送信や、SNS への書き込み。

・ほかのコンピュータへの侵入など、迷惑行為、犯罪行為をする。

コンピュータでの行動は顔が見えないので、行為者はユーザーID によって特定されます。このため、あなたのユーザーID を使って行われた行為はすべてあなたの行為とみなされ、あなたが責任を負うことになります。

本学の学内ネットワークでは、「パスワードを他人に教えてしまう」ことは、セキュリティ面から「機密の保護・維持に個人が努める」という規約に違反してい

るとみなされ、処罰の対象となりますので注意してください。

「使い回しのパスワード」は絶対にやめましょう。

複数のサービスで同じユーザーID とパスワードを利用すると、万が一、ユーザーID とパスワードが漏洩した際、その ID とパスワードを利用してほかのサービスへの不正ログインを試みる「リスト型アカウントハッキング」の攻撃にあう可能性もあります。

パスワードの保管方法に気をつけましょう。

パスワードの管理はすべて自己責任となります。
メモに記述等の場合紛失の恐れがあります。
完全に暗記する。ID とパスワードを別々に所持する。
など個々に対策をしておきましょう。

7　ネットワーク利用上の注意

インターネットを利用しているときは、常に現実社会で行動しているのと同じであるという自覚を持ちましょう。インターネットが整備され、PC やスマートフォンの普及とともに、情報の受発信が誰でも容易にできるようになりました。しかしその反面、「コンピュータウイルス」や「迷惑メール」、「ネットワークへの不正侵入」や「なりすまし」、「情報漏えい」、「SNS の炎上」、「いじめ」、など、実にさまざまな問題が生じています。このような状況から私たちは加害者とならず、また被害者とならない為に情報社会の一員であることを自覚し、その規範に則って行動することが求められています。

情報セキュリティについて

インターネットはとても便利な道具ですが、セキュリティについては利用者側も注意をしないと、思わぬ事故（セキュリティ・インシデント）になってしまう可能性があります。本学でのパソコンには、ウイルス対策ソフトがインストールされていますが、あくまでも善良な利用をしているにも関わらず、PC にウイルスが侵入してきた場合に有効なものです。ユーザーの積極的な行動で感染した場合、検出・駆除できないことがあります。

8　ネットワークセキュリティを守るために

パスワード漏えいについて

本学のコンピュータシステムやメールでは、ユーザーID とパスワードで利用者を特定し、学内ネットワーク、その他のサービスを提供しています。パスワードは推測されにくいものにすることはもちろん、みだりに教えたり、見られたり、知られることのないよう、適切に管理してください。

コンピュータウイルスについて

コンピュータウイルスとは、電子メールの添付ファイルや Web サイトの閲覧、USB 等の外部記憶メディアなどから感染する悪意のあるコンピュータプログラムです。ネットワークや USB などの外部記憶媒体を介して感染が広がります。感染しないために、次の点に注意が必要です。

・不審なメールは開かない。
・怪しい Web サイトに誘導されない、行かない。
・出所のはっきりしないファイルは開かない。
・USB を接続する際は必ずウイルスチェックをする。

利用者自身のパソコンのセキュリティについて

利用者自身が自宅または個人で使用しているパソコンついても次のようなセキュリティ対策をお願いします。

・ウイルス対策ソフトを導入し。定期的に検査、常に最新の状態に更新する。
・Windows、Office などソフトウェアは常に最新の修正プログラムを適用する。

個人情報について

自分を含め、ネットワーク上で個人、プライバシーにかかわる情報を扱う際は慎重に行ってください。

Web で個人情報を入力が必要な際は、信頼できるサイトか、情報を安全に取り扱われているか、よく確認してください。特にクレジットカード番号や個人情報を入力する際は、暗号化通信や、なりすましを防ぐ証明書が発行されているかの確認など安全を確認してください。