V-Campus ID 認証時のセキュリティ強化
― 多要素認証とアカウントロック機能の導入 ―

V-Campus ID に対する不正アクセス防止を目的としたセキュリティ強化対策の一環として、多要素認証とアカウントロック機能を導入した。

近年、フィッシング、標的型攻撃による ID・パスワードの窃取、パスワード総当たり攻撃（ブルートフォースアタック）など、Web サービスのユーザーアカウントに対する不正アクセスの手口が多様化している。そのため、「パスワードをできる限り長く複雑なものにする」、「パスワードの使い回しをしない」などの従来の対策だけでは、ユーザーアカウントのセキュリティ確保が困難になっている。万が一、ユーザーアカウントに不正アクセスされた場合には、利用者の個人情報のみならず、教育研究・業務に関する機密情報の漏洩・不正利用にもつながりかねない。

これらのリスクを未然に防ぎ V-Campus の各種サービスを安全に利用するためにも、利用者に対して多要素認証の有効化を継続的に推奨していく。また、上述したパスワードリスト・パスワード総当たり攻撃などによる V-Campus ID への不正アクセスを防御するために、一定時間内に複数回パスワードを間違えた場合に V-Campus ID をロックする機能（アカウントロック機能）も併せて導入した。以下に概要を紹介する。

1. 多要素認証について

(1).多要素認証とは

多要素認証とは、V-Campus ID を認証する際に、ID・パスワードに加えて、認証コード（ワンタイムパスワード）を追加入力する認証方式を指す。認証コード（ワンタイムパスワード）は、スマートフォンの認証アプリか個人用メールアドレスを用いて受信する。

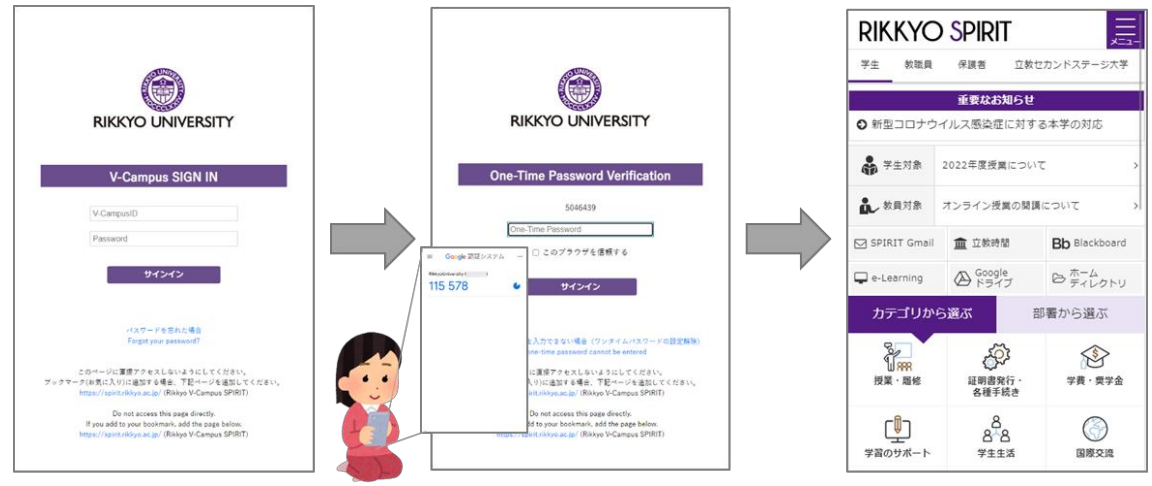
このように、二種類の認証方法を組み合わせることにより、万が一 ID・パスワードが他人に知られた場合にも、アカウントの不正利用を防ぐことが可能となる。

(2).対象

V-Campus ID を保有するすべての利用者が対象である。

初期設定では多要素認証は無効化されており、有効化するためには利用者自身による設定が必要である。多要素認証を有効化するまでは、ID・パスワードによる認証のみでサービスを利用可能である。

また、スマートフォンの紛失等により認証コード（ワンタイムパスワード）を受信できなくなった場合を考慮して、多要素認証を有効化した後に無効化することもできる。



V-Campus ID とパスワードを入力　　認証コード（OTP）を入力　　サインイン

図 1：多要素認証の利用イメージ

2.　アカウントロック機能について

(1). 概要

一定時間内に所定の回数以上、認証に失敗した場合、V-Campus ID を一時的に利用停止するアカウントロック機能を導入した。アカウントロック機能により、パスワードを 1 文字ずつ変えながら解読を試みるパスワード総当たり攻撃（ブルートフォースアタック）による不正アクセスを未然に防ぐことができる。

図 2：アカウントがロックされた際に表示される画面

(2).アカウントロックの解除

アカウントがロックされてから、一定時間経過するとロックが自動解除される。自動解除された後にV-Campusパスワードを再発行のうえ、再度V-Campus ID認証を試す必要がある。なお、利用者自身でパスワードを再発行する場合は、あらかじめ予備のメールアドレスの登録が必要となる。予備のメールアドレスを登録していない場合は、メディアセンターの窓口でパスワードを再発行する必要がある。