令和６年９月３０日

教職員　各位
学生　各位

最高情報セキュリティ責任者
寶珍　輝尚

【重要】メールの多要素認証の導入及び
令和６年１１月１日以降の利用必須化について

※(For an English version of this document, please scroll down.)

平素より本学メールサービスをご利用いただき、誠にありがとうございます。

なりすましによる不正利用を防ぐとともに、セキュリティの向上を図るために、メールサービスに多要素認証を導入しましたので、速やかに各自において多要素認証の機能を有効にしていただき、利用を開始してください。

また、**以下の実施日から、大学側で一斉にメールサービスの多要素認証の設定を有効にします。**それまでに、各自のタイミングで多要素認証の利用を開始していただき、操作方法に慣れていただきますようお願いいたします。

【メールサービスにおける多要素認証の必須化】

・実施日：**令和６年１１月１日（金）**

・多要素認証の利用方法：　https://info.cis.kit.ac.jp/wiki/x/rAJ8Bw

※　上記実施日以降は、**学外ネットワーク・eduroam**に接続している場合、**メールソフト及びWebメール**にログインする際に、多要素認証が必要となります。
※　学外ネットワーク・eduroamから、メールご利用されない方は、多要素認証にかかる設定は不要です。
※　学内ネットワーク（eduroam除く）に接続している場合のメールの利用や、ＶＰＮ接続中のメールの利用では、多要素認証は適用されません。これまでどおり、ＩＤ及びパスワードのみの認証となります。
※　事務局メールアドレス（@jim.kit.ac.jp）を利用している方は、既に多要素認証の

機能が有効となっています。
※　現在、メールソフトによる学外ネットワークからのメール送信については送信制限を行っていますが、多要素認証必須化以降、１１月中旬頃にこの制限を廃止する予定です。詳細が決まりましたら、改めて通知いたします。

【多要素認証の手順】
学外ネットワーク・eduroam に接続された端末から、メールを利用する際、Web メールを利用する場合もメールソフトを利用する場合も、まず、Web メールにアクセスしていただき、ID 及びパスワードの入力後、予め指定された方法で送られるワンタイムパスワードを用いて認証を完了させます。ワンタイムパスワードとは、1 回限り有効な使い捨てのパスワードです。ワンタイムパスワードの取得方法は、各自が所持しているスマートフォンに専用のアプリを入れて取得する方法と、本学のメールアドレス以外の、各自が所持している別のメールアドレスで取得する方法の２つです。
多要素認証の有効時間は 14 時間となりますので、使用時間が 14 時間を超過する場合には、14 時間後に再度 Web メールにログインして多要素認証を有効にしてください。

フィッシング攻撃等のサイバー攻撃で各種システムにログインするＩＤ・パスワードを窃取され悪用される事案が多発しており、本学においても情報科学センターアカウントのＩＤとパスワードが不正に窃取され、迷惑メール送信の踏み台にされる事案が発生しています。
複数の要素を組み合わせることでセキュリティを強化し、第三者からの不正ログイン・なりすましにさらされる危険性を下げることが目的です。
パスワードのみでセキュリティを保持することは大変厳しい状況にあり、何卒みなさまのご理解とご協力のほど、どうぞよろしくお願いいたします。

本件に関する問い合わせ先：情報科学センター
Web: https://helpdesk.cis.kit.ac.jp/
・トラブル → システム障害の問い合わせ
・その他 → 一般的な質問

Date: September 30, 2024

To: All Faculty, Administrative Staff and Students
From: Chief Information Security Officer, Teruhisa Hōchin

Re: [Important] Implementation of Multi-Factor Authentication for Email and Its Mandatory Use - Effective November 1, 2024

Thank you for using the KIT email service.

To prevent unauthorized access through impersonation and to enhance security, we have implemented multi-factor authentication for the email service. Please enable and make use of this feature right away.

From the implementation date below, multi-factor authentication settings for all email services will go into effect. We would like to encourage everyone to begin using multi-factor authentication at their own pace prior to this date, to familiarize themselves with the process.

Mandatory Multi-Factor Authentication for Email Services

- Implementation Date: November 1, 2024 (Friday)
- How to Use Multi-Factor Authentication: [Link to instructions in English]

  https://info.cis.kit.ac.jp/wiki/x/rAJ8Bw

Important Notes:

- After the November implementation date, multi-factor authentication will be required when logging into **email software and webmail** from **external (non-KIT) networks or eduroam.**
- If you do not use email from external networks or eduroam, you do not need to configure multi-factor authentication.
- Multi-factor authentication does not apply when accessing email from the university's internal network (excluding eduroam) or while connected via VPN. In these situations, continue to use your ID and password as before.
- For persons using the administrative email address (@jim.kit.ac.jp), multi-factor authentication has already been enabled.

- Currently, there are restrictions on sending emails from external networks, but these will be lifted around mid-November after multi-factor authentication is implemented. Further information will be provided as it becomes available.

Multi-Factor Authentication Steps: Whether you are using webmail or email software when accessing email from external networks or Eduroam, first, log in to your webmail account using your ID and password. You will then need to enter a single-use password to complete authentication. You can obtain this single-use password either by installing a dedicated smartphone app or through another of your email addresses.

Multi-factor authentication is valid for 14 hours. To exceed this, log in to your webmail account again after 14 hours to re-enable multi-factor authentication.

KIT has encountered numerous incidents of phishing and other cyberattacks that resulted in the theft and misuse of login IDs and passwords. These compromises led to the sending of spam emails. By implementing multiple authentication factors, we aim to enhance security and minimize the risk of unauthorized access and impersonation.

Relying solely on passwords for security has become increasingly challenging. We appreciate your understanding and cooperation in this matter.

For inquiries, contact the Center for Information Science

Online: https://helpdesk.cis.kit.ac.jp/

For Specific Breaches: “Having trouble with a system?”

For Other Issues: See “Get assistance with general IT problems and questions.”