これは三重大学の標的型攻撃メール訓練です！

このメールは三重大学　情報基盤センターが三重大学の教職員に対して、
標的型攻撃メールの訓練のために送信したものです。

あなたが今行った行為（本文中の　URL　を安易にクリックしてしまうという行為）は、コンピュータウィルスに感染してしまうかもしれない危険な行為です。

もし、これが訓練でなかった場合は、深刻な問題が発生する可能性が十分あり得ることを知って下さい。

標的型攻撃メールの怖さを知っていますか？

標的型攻撃メールは、特定の企業・官公庁・大学などを狙って学生・教職員や重要な社内情報などを盗み取ったり、学内システムに侵入して業務を継続できないようにします。感染すると業務に甚大な被害をもたらすことになります。

このメールは、この**「標的型攻撃メール」**による攻撃の手口の一例を模した訓練用のメールです。

今回は訓練なので実害はありませんが、もしこれが本当の標的型攻撃メールであった場合は、**「あなたのパソコンがコンピュータウィルスに感染し、学内に甚大な被害をもたらすきっかけ」**となっていたかもしれません。

標的型攻撃のターゲットになるのは、なにも政府や軍事関連の組織ばかりではありません。
三重大学もその標的とされる可能性は十分あります。

「ウチの大学には関係ない話」ではないのです。

【くどいようですが注意しましょう！】

大学に被害をもたらすことを目的とした、悪意を持ったメール（標的型攻撃メール）が、いつ送られてきても不思議ではありません。

標的型メールはとても巧妙になってきており、どうしても開いてしまうことは起こりえます。

※この場合の「開いてしまう」とは添付ファイルや URL をクリックする行為を指します

そのため、開いてしまった後の行動が大変重要になります。

「おかしいな？」と感じたら、直ちに以下のことを行ってください。

おかしいな？と感じたら・・・

① すぐにネットワークケーブルを抜く

感染したウィルスは、PC 内の情報を外に持ち出そうとしたり、横に感染を広げようとしたりします。
ひとまず**ケーブルを抜く**ことで、情報流出・感染拡大を防げます。無線 LAN を使っている場合は、**無線機能をオフ**にしてください。

② 管理者に連絡する

誤って開いてしまった場合、放置しておくと大きな問題に発展する可能性もありえます。

できる限り早急に
教員・学生は→　情報基盤センター　内線(9772)
事務職員は→　DX・情報チーム　内線(9773,9738)
医学部,病院は→　医療情報管理部　内線(5736)　に**必ず連絡をお願いします。**

今回のメールに関してはご連絡いただかなくて結構です。

③ ウィルス対策ソフトで感染をチェックする

管理者不在の場合は、インストールされている**ウィルス対策ソフトでチェック**してください。
大学内の PC の場合は、ウィルス対策ソフトを提供しております。

http://www.cc.mie-u.ac.jp/cc/i/sitelicense/ees_efsw.html よりインストールできます。

本訓練についてのお問い合わせ先

情報基盤センター 内線 9772
Mail: support@cc.mie-u.ac.jp