これは標的型攻撃メールの訓練です。

不審なメールには注意しましょう。

1. メールを怪しい（タイトル、送信者/アドレス etc.）と判断したら開封しない。

2. 開封して、怪しければ（業務や組織を騙っている、心当りのない組織から etc.）、添付ファイルや記載リンクをクリックせず、破棄する。

3. 開封して、怪しければ（業務や組織を騙っている、心当りのない組織から etc.）、添付ファイルや記載リンクをクリックせず、システム管理部門に報告する。

4. 誤って添付ファイルや記載リンクをクリックした際、表示内容が業務外であったり、適切な表示がなかったり、動作に違和感を覚えたら、即座にシステム管理部門に報告し、指示を仰ぐ。

【標的型攻撃メール】

情報窃取等を目的として、ごく少数または多数ながら特定された範囲のみに対して送られる、利用者のPCをマルウェアに感染させることを目的としたメールを標的型攻撃メールと呼んでおり、 次のような特徴があります。

- メールの受信者に関係がありそうな送信者を詐称する
- 添付ファイルや本文中のURLリンクを開かせるため、件名・本文・添付ファイルに細工が施されている（業務に関係するメールを装ったり、興味を惹かせる内容や、添付ファイルの拡張子を偽装するなど）
- ウイルス対策ソフトで検知しにくいマルウェアが使われる

【標的型攻撃メール対策に関する情報】

・総務省 国民のための情報セキュリティサイト 標的型攻撃への対策
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_staff_05.html