フィッシングメールの特徴

■フィッシングメールの特徴１

同志社大学のシステム管理者を騙ったメールで，ユーザ ID やパスワードの返信を要求するフィッシングメールが確認されています。同志社大学 IT サポートオフィスでは，利用者個別にユーザ ID やパスワード等といった重要な個人情報の返信をメールにて要求をすることは一切ありません。

「フィッシングメール（例 1）メール返信要求型」のようなメールはフィッシングメールですので返信せずに破棄ください。

■フィッシングメールの特徴２

フィッシングメールは海外から送付されてくる場合が多くあります。海外の言語で作成した文章を，翻訳エンジンにて日本語に翻訳しているためか，日本語の文章がおかしい場合があります。

「フィッシングメール（例 2）Web 入力誘引型」、「フィッシングメール（例 3）Web 入力誘引型」のように日本語がおかしな文章の場合は，フィッシングメールの疑いが強いと言えますが，日本人が関与する事も否定できませんので，必ず内容も確認してください。

■フィッシングメールの特徴３

フィッシングメールは「HTML 形式」で作成されていることがあります。メール本文中に「ここへクリック」などといった文章で外部リンクを設け，本当の URL は伏せたままフィッシングサイトへ誘導するためです。この細工は，「テキスト形式」で受信すれば，「フィッシングメール（例 2）Web 入力誘引型」のようなメールの「ここへクリック」を選択しても，外部サイトにリンクされません（リンク先の URL がテキストで記載される形となります）ので，比較的被害を防ぎやすいと言えるでしょう。

もし，HTML 形式での受信が必要な場合は十分に注意してください。また，リンク先の URL が正規のものかどうかの判別には，後述の「URL 判断方法の一例」、「SSL 証明書の確認方法」を参照ください。

■フィッシングメールの特徴４

フィッシングメールにはメール本文に URL を記載するなど，外部サイトでの Web 入力を誘引する場合もあります。（例：「フィッシングメール（例 2）（例 3）Web 入力誘引型」）

リンク先の URL が正規のものかどうかの判別には，後述の「URL 判断方法の一例」、「SSL 証明書の確認方法」を参照ください。

■フィッシングメールの特徴５

フィッシングメールは，メールの送信元情報を詐称していたり，海外から送付されていたりするなど，メールのヘッダ情報に怪しい点があります。

メールヘッダの確認方法については後述の「メールヘッダの確認方法」を参照ください。

参考ページ

・警視庁フィッシング 110 番
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku406.htm

・フィッシング対策協議会
http://www.antiphishing.jp/

フィッシングメールの例

■フィッシングメール（例 1）メール返信要求型

ACTIVEMAIL 2013.
Dear Account User,

You have reached the limit of your email quota, You will not be able to send or receive new mail until you boost your mailbox size. To complete your Account Verification process, you are to reply this message & enter your ID and PASSWORD in the space provided below to avoid account De-activated and erased from our database.

*Full Email:.....
*User ID:.....
*Password:.....
*Confirm Password:.....
Warning!!!
Account owners that refuses to update his or her account within Four days of receiving this warning will lose his or her account permanently.
Reply us via this email:フィッシング先メールアドレスが記載されていたため削除

Thanks,
Web Administrator

■フィッシングメール（例 2）Web 入力誘引型

注意：doshisha.ac.jp ユーザー、 あなたは、250 メガバイトのあなたの doshisha.ac.jp 電子メールアカウントの制限クォータを超えて、あなたは 48 時間以内にそれを拡大したり、他のあなたの doshisha.ac.jp 電子メールアカウントは、当社のデータベースから無効にされ要求されます。完全な情報を単に（ここをクリック）は 450 メガバイトにあなたの doshisha.ac.jp 電子メールアカウントのクォータを拡大するよう要請した。doshisha.ac.jp 電子メールサービスをご利用いただきありがとうございます。

著作権（C）2013Doshisha 大学情報センター。

■フィッシングメール（例 3）Web 入力誘引型

同志社大学電子メールユーザー各位、

このメッセージは、同志社大学の電子メール管理者からのものである。すべて同志社大学電子メールユーザーは、アカウントを迅速かつ最大限のセキュリティを確保するための新しい 2013 年の電子メール版に彼ら同志社大学電子メールアカウントを更新する必要があることを通知すること。あなたは以下のリンクをクリックし、アカウントをアップグレードするには、同志社大学のユーザーID とパスワード（パスフレーズ）でログインすることが期待されることに注意してください。
http://フィッシングサイトの URL が記載されていたため削除
あなたの理解をありがとう。
Doshisha University
著作権（C）同志社大学すべての権利予約。

URL 判断方法の一例

■共通ユーザ ID/パスワードを入力する学内システム URL には，以下の特徴があります。

▼本学学内システム

1)本学ドメイン名「.doshisha.ac.jp」が URL に含まれます。

2)URL において、「https:// 」から「.doshisha.ac.jp」の間に、「/」が存在しません。

3)「.doshisha.ac.jp」直後は、「/」か「文字列が無い」となります。

（例）○　https://webmail.doshisha.ac.jp

（例）○　https://webdisk.doshisha.ac.jp/proself/login/login.go?AD=init

▼不審な URL の特徴

・「doshisha.ac.jp」の文字列が「.」以外の記号で区切られている，もしくは区切られていません。

（例）×「https://webmail.doshisha-ac-jp.sample.ac.jp 」

・「doshisha.ac.jp」直後が「/」でなく，文字列が続いています。

（例）×「https://webmail.doshisha.ac.jp.sample.ac.jp 」

・「https:// 」から「.doshisha.ac.jp」の間に「/」があります。

（例）×「https://sample.ac.jp/webmail.doshisha.ac.jp/login.html」

▼注意事項

Web ページのリンク設定は，「こちら」の文字列をクリックすると特定の URL にアクセスするように，見かけの文字列とリンク先 URL を設定できます。以下は例です。

①ページ上では，　https://mikake.doshisha.ac.jp　と表示しつつ

②実際のアクセス先を　http://hontouha.doshisha.ac.jp　とした設定例です。

※下図のとおりマウスカーソルをリンクにあわせると，実際のアクセス先②が表示されています。

これと同様の設定が，HTML メールを利用すると可能です。

リンクをクリックして Web アクセスした際は，ブラウザのアドレスバーを確認すると良いでしょう。

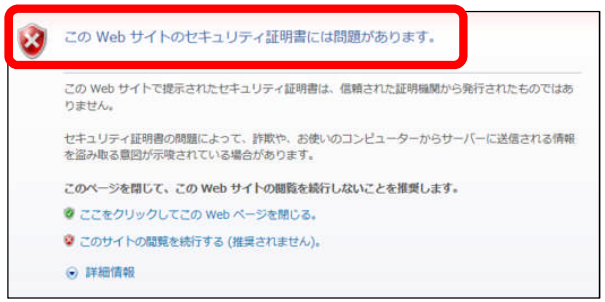
SSL 証明書の確認方法

■SSL 証明書の簡易なチェックが可能です。

インターネットで重要な個人情報などをやりとりする際，情報漏えいを防ぐために「暗号化」という技術を利用します。本学が提供する学内システムでも，共通ユーザ ID/パスワードを入力する必要がある場合はサーバにインストールされている SSL 証明書を利用して，通信内容を暗号化して盗聴や改ざんを防いでいます。

暗号化通信をする際には URL が「http://」ではなく、「https://」と表示されます。共通ユーザ ID/パスワードを入力するフォームがある場合は，まずは「https://」となっていることを確認ください。

次に，利用する SSL 証明書が問題ないかどうかは URL アクセス時にブラウザから簡易なチェックが可能です。アクセス時に以下のようなセキュリティ証明書に問題があるメッセージが出た場合は，アクセス先で利用している SSL 証明書もしくはサーバに何らかの問題があります。理由が明確でない場合は，Web ページを閉じることを推奨します。



セキュリティ証明書に問題があるメッセージが表示されてもサイトの閲覧を続行した場合は，以下のように SSL 証明書のエラーと表示されます。このような Web ページにおいて，エラーの原因が明確でない場合は，共通ユーザ ID/パスワードなどの重要な情報を入力せずに，Web ページを閉じてください。

※SSL 証明書を信頼できる証明書として，個別にインストールした場合はエラー表示されません。
個別にインストールする場合は十分に注意し、実行ください。

なお，ブラウザに表示された鍵マークやアドレスバーをクリックすると SSL サーバ証明書の内容を確認することができます。

参考ページ

・総務省　国民のための情報セキュリティサイト―SSL の仕組み
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/03.html

・サイバートラスト株式会社　SSL サーバ証明書の基礎知
https://www.cybertrust.ne.jp/ssl/beginner/ssl1.html

メールヘッダの確認方法

■メールヘッダから迷惑メールかどうかの簡易なチェックが可能です。

メールのヘッダ情報は，メールが「どこから」「どのような経路で」「いつ」送られてきたのかなどの一連の処理を記録した情報です。迷惑メールの場合でもヘッダ情報は記録されるため，迷惑メールかどうかのチェックに利用することが可能です。

▼メールヘッダ情報からわかること

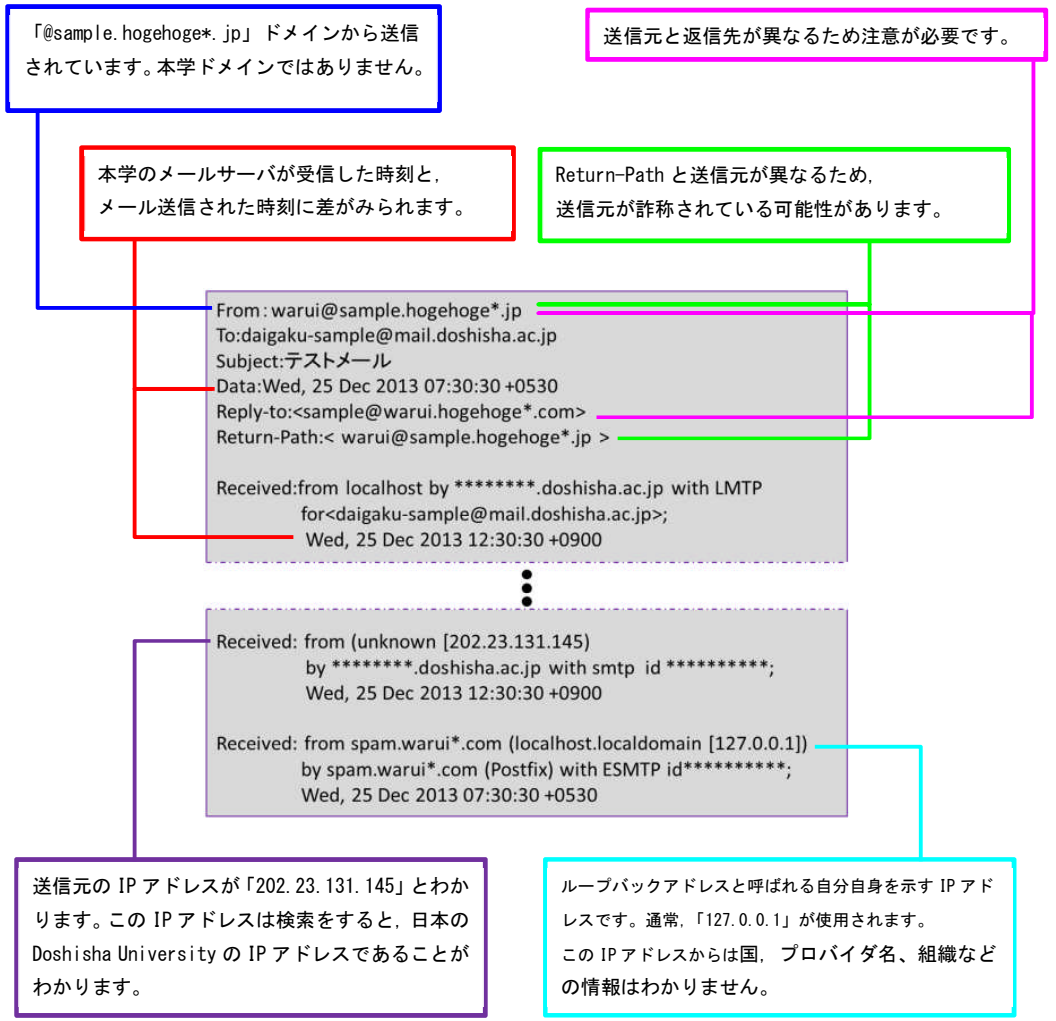
ヘッダ名	意味	チェックポイント
From （送信元）	送信者のメールアドレスです。 メールアドレスが詐称されている場合もあるため注意が必要です。	「@*.doshisha.ac.jp」以外のアドレスの場合は， 本学のドメインではありません。 しかしながら，From の詐称は可能なため，ご留意ください。
To（送信先）	宛先のメールアドレスです。	-
Subject（件名）	メールの件名です。	-
Date（時刻）	メールが送信された時刻です。	海外のプロバイダからメール送信された場合は，時差のためメールを受信した日時と若干のずれがある可能性があります。
Reply-To （返信先）	メールの返信先です。 メール送信者は Reply-To に指定のメールアドレスを設定することで，メール受信者が返信する際の宛先を指定することができます。	迷惑メールの場合，From（送信元）とは違うメールアドレスが設定されている場合が多くみられます。メール返信時には宛先アドレスをよく確認する必要があります。
Return-Path	メール配信エラーの際の差し戻し先です。	From（送信元）を詐称した迷惑メールの場合でも， 実際には Return-Path に記載されているメールアドレスからメールが送信されている可能性があります。 しかしながら，Return-Path の詐称は可能なため， ご留意ください。
Received	メールが配送されたルートです。経由したサーバの数だけ Received の情報が記載され，ヘッダの下から順に経由したサーバが記載されます。 ※ヘッダ記載の一番下の Received が送信元で、一番上の Received が自身のメールサーバとなります。	Received の“[ ]”内に記載されている 4 オクテットの数字は経由サーバの IP アドレスを示します。以下のようなサービスを利用して IP アドレスを検索することで，送信者の利用している国，プロバイダ名、組織などの情報がわかります。 参考：CMAN ドメイン / IP アドレス【whois 情報検索】 http://www.cman.jp/network/support/ip.html なお、本学保有の IP アドレスを検索した場合，国や組織名は以下のように表示されます。 country:JP → （日本） Organization：Doshisha University

※メールヘッダの表示方法は使用しているメールソフトやメールサーバによって異なります。

表示方法の参考：一般財団法人　日本データ通信協会　迷惑メール相談センター
http://www.dekyo.or.jp/soudan/ihan/header.html

▼メールヘッダのサンプル

メールヘッダ情報からわかることを，サンプルを使って示すと以下のとおりです。



参考ページ

・一般財団法人　日本データ通信協会　迷惑メール相談センター　E メールヘッダ情報の確認方法
http://www.dekyo.or.jp/soudan/ihan/header.html