

標的型攻撃メールの見分け方（ご参考）

見分け方のポイント

①不明・不自然な差出人からのメール

※アマダ社員からのメールは XXXX@amada.co.jp です。

②興味を煽り、リンクのクリックへ誘導する文章

③不明・不自然なドメイン、暗号化されていないURLのリンク（httpsではなくhttp）

④不明または存在しない団体の署名

サンプルメール内容

各位

お疲れさまです。
新型コロナウイルス対策会議より、以下のとおり連絡がありました。

各自で内容を確認してください。

よろしくお願いいたします。

----- 転送メッセージ -----

From: 新型コロナウイルス対策会議 <1> covid19info@scrty-chk-sys.biz>

日付: 2020年7月17日(金) 9:59

件名: 新型コロナウイルスに関する対応について

各位

2 表題の件、以下のサイトに方針を記載いたしましたので、社内で共有ください。

3 http://covid19info.scrty-chk-sys.biz

体調に十分ご注意ください。今後とも三密を避けて日々の生活を過ごすよう改めて周知ください。

よろしくお願いいたします。

4 新型コロナ対策会議
covid19info@scrty-chk-sys.biz

標的型攻撃を受けないために

多くの標的型攻撃はOSやアプリケーションの脆弱性を利用して感染を拡大させます。

- ・ 毎月配信されるWindows／Officeの更新プログラムは必ずインストールし、PCを再起動して更新を適用してください。
- ・ ウィルス対策ソフトの定義が更新されているか定期的に確認してください。
- ・ その他ソフトウェア(GoogleChrome等)についても自動更新機能を無効にせず、常に最新版を保ってください。

標的型攻撃メールと疑われる、不審なメールを受信した際は・・・

- ・ 不審なメールに気がいたら、添付ファイルや本文中のリンクをクリックせず、速やかにメールを削除しましょう
- ・ 添付ファイルやリンクをクリックしてしまった場合は、直ちにLANケーブルを外し、無線LANをOFFにしてネットワークに接続できない状態にしましょう