標的型攻撃メールへの対処について

標的型攻撃メールとは SPAM メールとは異なり、実際に存在するユーザに対して、いかにも業務上のメールであるかのように装って送られる悪意のあるメールで、メール中に URL が記載されているか、添付文書がついています。

標的型攻撃メールの本文中の URL をクリックする、あるいは添付文書を開くと、直接あるいは間接的に不正ソフトが入り込み、その PC やネットワークで接続された他の PC に悪意のあるソフトウェア（マルウェア）が感染します。
かなり巧みに文章が作られているメールもあり、URL のクリックや添付文書を開くことを完全に防止することは困難です。もちろん、少しでも怪しいところがあれば、URL をクリックしない、添付文書を開かない、という対策は大変重要ですが、業務でメールを使用する以上、100%防止することは困難です。

また、標的型攻撃メールで送り込まれたマルウェアに PC が感染した場合、その感染 PC は外部から自由に操作されると考えなければなりません。したがって感染 PC 内のファイルや感染 PC から直接アクセスできる共有フォルダにあるファイルは最悪の場合、瞬時に漏洩してしまいます。出ていってしまったファイルを確実に取り返す、あるいはインターネット上から削除する手段はありません。ここではこのような前提で、被害を最小限に食い止めるための予防措置、並びに事後措置について述べます。

予防措置１：インターネットでやりとりされるメールを読むことができる PC と、その PC から直接アクセスできる共有フォルダには患者情報を置かない。
やむを得ず患者情報を置く場合は、そのまえにマルウェアの感染がないことを管理者への問い合わせも含めて確認し、どうしても必要な期間だけに限定し、患者情報がある間はその PC ではメールを読まないようにします。なお、必要な期間が終わり患者情報を消去しても通常の消去では復元できる可能性があるので、復元不可能な消去ツールを使うことが必要です。
患者情報を含むファイルのパスワードロックも必要です。ただし、ファイルが盗まれた場合、パスワードロックがあるから絶対に安全というわけではありません。短いパスワードでは簡単に解読されてしまいますので、長い（できれば１２文字以上）パスワードにすることが必要です。また、例えば Windows OS では基本機能でのサポートはありませんので専用ソフトの導入が必要ですが、フォルダのパスワードロックを行うことも有効な対策です。

予防措置２：OS のセキュリティパッチは確実に適用する。
マルウェアの多くは最終的には OS の脆弱性を利用します。OS には常に最新のセキュリティパッチを適用しておくことが必要です。Java や Adobe flash player をインストールしている場合は、これらの最新のパッチの適用も必要です。なお、Adobe flash player は多くの場合、業務では不要です。したがって、インストールしないほうが安全です。インストールしている場合は削除しておくほうが無難です。Java も業務で使わないなら削除しておくほうが安全です。

予防措置３：メール送信する際に添付文書の使用や URL の埋め込みはできるだけしない。
よく業務でメールをやりとりする関係者間で協議し、添付文書の使用や URL の埋め込みはできるだけしないようにします。簡単な内容なのに、添付文書にする人がいますし、また紙の書類の信奉者は２行で済む内容をわざわざ PDF にして添付文書にすることもあります。このようなことは避けるべきで、メールの本文に書けば標的型攻撃メールかどうかの心配をしなくて済みます。また URL を埋め込む場合も本当に必要かどうか、よく検討してください。「『XXX』で検索すれば簡単にヒットします。」と書けばすむ場合はそうすべきです。また、メールソフトでメール作成の書式の標準設定が HTML モードになっている場合が多いですが、HTML モードでは意図せずに外部リンクを作成しまう可能性がありますので、可能であれば書式の標準設定をテキストモードに変更して利用することも有効です。

予防措置４：メールソフトで感染を予防するための設定をする。
　メールソフトの設定が適切にされていない場合、メールを受信した際にマルウェアに感染する可能性があります。受信したメールをプレビュー表示する機能がありますが、開くつもりのないメールも表示してしまう可能性があるため、プレビュー表示機能を使用しないようにし、必要なメールだけ表示するようにすることが有効な対策です。また、HTML メールを受信した際にテキストモードで表示されるよう設定することも有効です。

予防措置５：（システム管理者向け）外部とのネットワークコネクションを監視する。
　一般ユーザではなく、管理者の業務ですが、外部とのネットワークコネクションの監視や端末の監査証跡の定期的なチェックが必要です。マルウェアは情報を踏み台にされたサーバに対して転送することが多いと言われています。通常は行われないサイトへの転送を発見するためには、普段の状況を把握しておくことが必要です。２４時間常に監視することは普通の医療機関には不可能ですが、時折分析をしておくだけでも、被害の未然防止や実際に被害にあった時の初動対応の役に立ちます。

予防措置６：（システム管理者向け）ホワイトリストを活用する。
　業務で利用する外部サイトが特定できる場合は、それ以外のサイトをアクセス不可にすることで標的型メールの攻撃用のサーバとの通信を遮断することができます。ルータの接続相手先の制限や、ブラウザの接続先の制限などによってホワイトリスト以外接続を制限できます。

予防措置７：（システム管理者向け）セキュリティ情報を収集する。
　少なくとも管理者（担当者）は、以下の３つのサイトは定期的にチェックし、最新の脆弱性情報等を確認してください。
　JPCERT コーディネーションセンター
　IPA（独立行政法人　情報処理推進機構）
　NISC（内閣サイバーセキュリティセンター）
　また、厚生労働省から出されている最新の「医療情報システムの安全管理に関するガイドライン」を確認してください。

事後措置１：怪しいと気づいた時
　メールを見ただけでは標的型攻撃メールによる攻撃かどうかわからなくても、URL をクリックする、あるいは添付文書を開いた際に何かおかしいと気がつくことがあります。もし何かおかしいと思ったら、すぐに PC をネットワークから切り離します。そして管理者あるいは担当者に直ちに連絡してください。管理者（担当者）は連絡を受けたら、ネットワークの監視を直ちに開始すると同時に、これまでのログがあれば保存します。異常を感じた PC と同じセグメントにある PC やサーバはできるだけ早く LAN から切り離します。そして、LAN から隔離した状態で、それぞれの PC やサーバの状態を調査します。安全と確信できない間は絶対 LAN につないではいけません。自分たちで十分な調査ができない場合は外部の専門家に依頼します。

事後措置２：データの流出を外部から指摘された時
　すでに情報が流出してしまっている場合、この時点では被害の拡大を食い止めることしかできません。まずマルウェアの感染状況が完全に把握できるまで、組織全体をインターネットから切り離します。管理者は必要に応じて関係先（地域医療連携の接続先や所管省庁、JPCERT など）への連絡を行います。その後、インターネットへの接続は安全性が確かめられたセグメントから再開しますが、安全性は確実に確かめる必要があります。不安がある場合は専門家に依頼してください。