平成27年2月12日

各位

横浜市立大学　事務局長

サイバー攻撃に対するセキュリティ対策実施について【依頼】

最近、Web サーバーや NAS （Network Attached Storage：ネットワークに直接接続して利用するファイルサーバ）を対象としたサイバー攻撃が多発し、多くの大学や研究機関などで、Web サイトの改ざん、ウイルスの組込、大量の迷惑メールの送信の踏み台とされるなどの被害が発生しています。
これらの多くは、サーバーOS（Linux や WindowsServer など）の脆弱性、初期値のままのパスワード、不適切なアクセス権の設定などが原因となっており、機器の設定や必要なセキュリティ対策を適切に行っていれば、防御できたと考えられるものも多く、改めて、それらの対応の重要性が指摘されている所です。

本学においても、Web サイトを利用して様々な情報発信を行っていたり、NAS で重要なファイルを保存、共有していることが多いと思われますので、再度、各研究室、部署においてどのようなものがあるか確認し、以下の対策を行ってください。（特に Linux のサーバー、端末などについては、確実に対応願います。）

No.	項目	説明
1	**こまめに OS ・アプリケーションのアップデート、セキュリティパッチの適用を行う**	WindowsUpdate を行ったり、各種の脆弱性対策のためのセキュリティパッチを適用すると共にOSだけではなく、利用しているアプリケーションのアップデートも行う。 導入が義務づけられているウィルス対策ソフトの導入を行う。 特にLinux等のOSの対策は、細かい場合もあるので、十分な情報を集め対応すること。
2	**NAS やルーター、無線 LAN アクセスポイントなど各種の機器の管理者パスワードを初期値のままにしておかない。**	パスワードを初期値から変更すると共に、NASだけでなく、その他の機器も、同様の問題により乗っ取られる場合がある事を認識しておくこと。
3	**パスワード設定のないユーザーアカウントや、現在は所属していない職員などの不要なユーザーアカウントの抹消、適切なアクセス権の設定をする。**	ユーザーアカウントは必要な人に必要な範囲で付与し、こまめにメンテナンスを行うこと。 パスワードは十分な強度（一定以上の文字数、文字、数字、記号などの混在したもの）を設定すること
4	**個人情報や機密情報が含まれるファイルにパスワードを設定する。**	万一ファイルが流出しても、内容を守ることのできる可能性が高いため、重要なファイルにはパスワードを設定しデータの暗号化を行う。（詳細は後日行われる個人情報保護研修の中で説明します。）

※参考に BUFFALO の LinkStation のアクセス制限方法を紹介します。
http://buffalo.jp/download/manual/html/lsv1/にアクセスして、左側の項目の下、「その他の設定」のメニューの中で「アクセス制限を設定したい」をご覧ください。ただし、各機器によって設定は異なり、内容を十分に理解して行わないと、正常な利用に支障を来す場合もあります。ご注意ください。
※本学のネットワークについては、ファイアウォールなどにより、外部からの侵入や攻撃を防ぐ対策を行っていますが、全ての攻撃を防止することはできません。また、学外のサーバーなどを利用している場合は、個別に対策を行う必要があります。
※攻撃の為の手段は、電子メールなどの情報から、攻撃の為のサイトへの誘導やウィルスを感染される事などにより行われることもあります。利用しているPC等について、設定などを十分に理解し、適切な対策を行ってください。

具体的な対策がわからない場合や、サーバ攻撃を受けているかもしれないと考えられる場合は、以下の問合せ先まで、ご連絡ください。

【問い合わせ先】
八景キャンパス経営企画課IT推進担当　787-2340　787-2341（平日 8時半 ～ 17時）

◆参考◆

【最近のサイバー攻撃/個人情報漏洩の事例】

慶応義塾大学

「看護職キャリアシステム構築」という特設ページの一部が改ざんされ、ウイルスが組み込まれていた（H27.1.23 日本経済新聞）

産業技術総合研究所

研究員が内部で作った資料等を保管するサーバーに侵入されウイルスに似た不正ファイルを組み込まれた（H27.1.23 日本経済新聞）

城西国際大学

千葉県内の 13 市町村と共同で運営するサイトが改ざんされ、無関係なサイトに誘導される（H27.1.23 日本経済新聞）

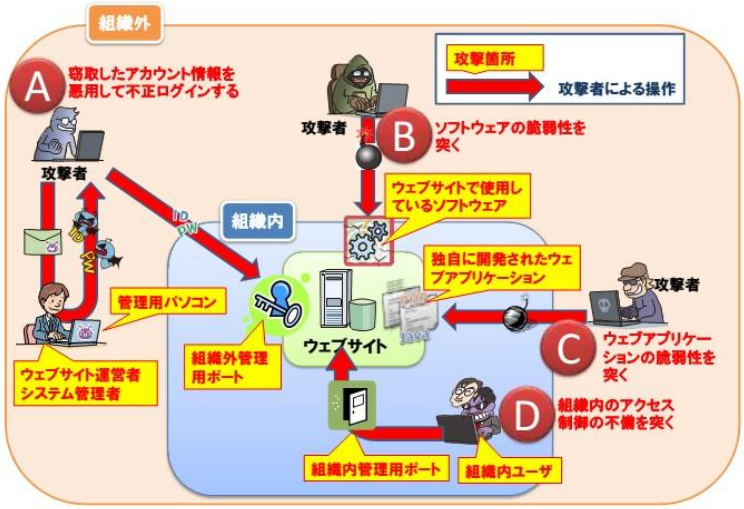
国立障害ﾘﾊﾋﾞﾘｾﾝﾀｰ

一部のサイトを管理するサーバーに侵入され、英語で「侵入成功」と記された不正なファイルが置かれた（H27.1.23 日本経済新聞）

首都大学東京

各部署や各研究室に設置されている NAS の設定ミスにより学生など 5 万 1 千人分の個人情報を載せたサーバーが外部から閲覧できる状態にあり、流出した可能性があると公表した。また、大学内に設置された NAS に外部から接続された形跡があり、当該 NAS から約 10 万 8000 通の迷惑メールを不特定多数に送信していたことが発覚した(2/2 首都大学東京プレスリリース)

【サイバー攻撃の一般的な手口】



（図１）情報処理推進機構ＨＰより引用

今回報道されたサイバー攻撃による被害は、どのような脆弱性をつかれたのかについて詳しい情報は公開されていませんが、サーバの基本ソフト(OS)の１つである「Linux」（リナックス）の脆弱性を突かれたものであることや（上記手口 B に該当）、NAS の設定不備（上記手口の D に該当）が原因であるとの報道もあります。