三重大学における最近のセキュリティ情勢について

総合情報処理センター　堀川慎一

はじめに

当センターでは、基本的なセキュリティ対策として、2004 年より全学に向けてウィルス対策ソフトの無償提供を行ってきました。また、2006 年には侵入検知防御システム（IPS）の運用を開始し、公開サーバへの不正アクセスの防御を図っています。以下では、これらの統計量に基づき、三重大学における 2010 年度から 2011 年度に渡る 2 年間のセキュリティ情勢の概要をご紹介したいと思います。

エンドポイントのセキュリティ情勢

当センターでは 2009 年 5 月より、ESET NOD32 Antivirus を主たるウィルス対策ソフトとして全学に提供しています。このウィルス対策ソフトでは、マルウェアを検知すると管理サーバへ通知するよう初期設定を施しており、学内で利用されている Windows 端末の概況を随時確認できるようになっています。

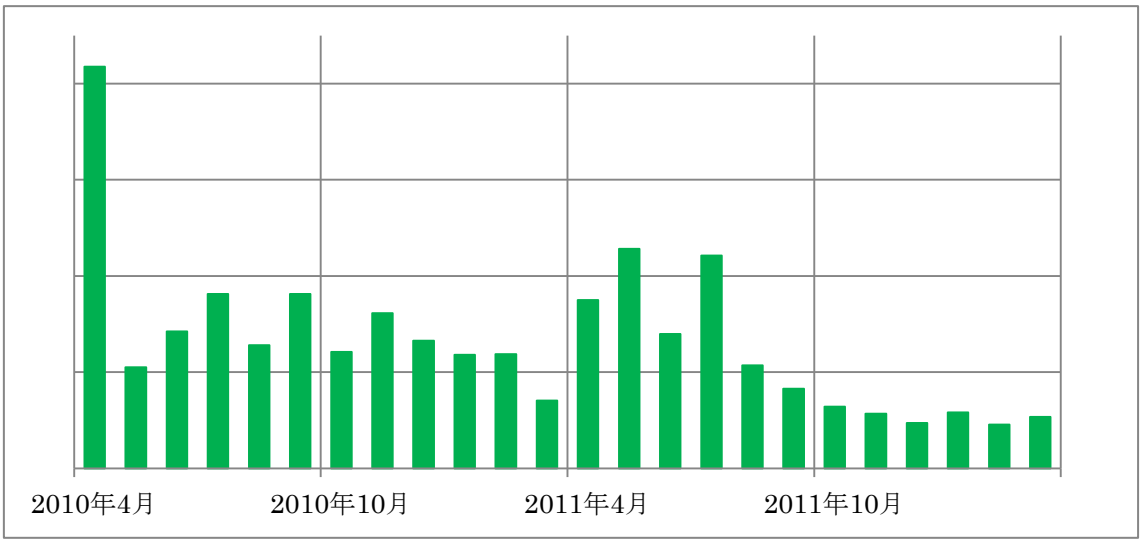

図 1　マルウェア検出数の推移

図 1 は、ESET NOD32 Antivirus の管理サーバにて確認されたマルウェア検出数の月別推移を示します。縦軸は 0 を起点とする線形軸です（以下同じ）。

上図では 2010 年 4 月に突出した値を記録していますが、これはオンラインゲームのパスワードを盗み出そうとする USB メモリウィルスが集中的に検出されたことによるものです。

このUSBメモリに代表されるリムーバブルメディアは現在でもマルウェアの検出場所として大半を占める状況にあり、実ユーザー数が一気に増加する年度初めに多くの検出が観測される傾向が見て取れます。また、2011 年度の夏休み以降は検出数が著しく減少していますが、こちらは Windows に加えて各種アプリケーションソフトでも自動更新機能が備えられるようになり、危険なセキュリティホールが長らく放置されにくくなったことが大きく貢献しているのではないかと考えられます。

ゲートウェイのセキュリティ情勢

当センターでは 2010 年 3 月より、スタンドアロン型の IPS を運用しています。この IPS では、公開サーバを個別に狙い撃ちするようなサイバー攻撃の防御と合わせて、ポートスキャン（アドレススープ）により標的を探し出そうとする不正アクセスを妨害する仕組みを取り入れています。

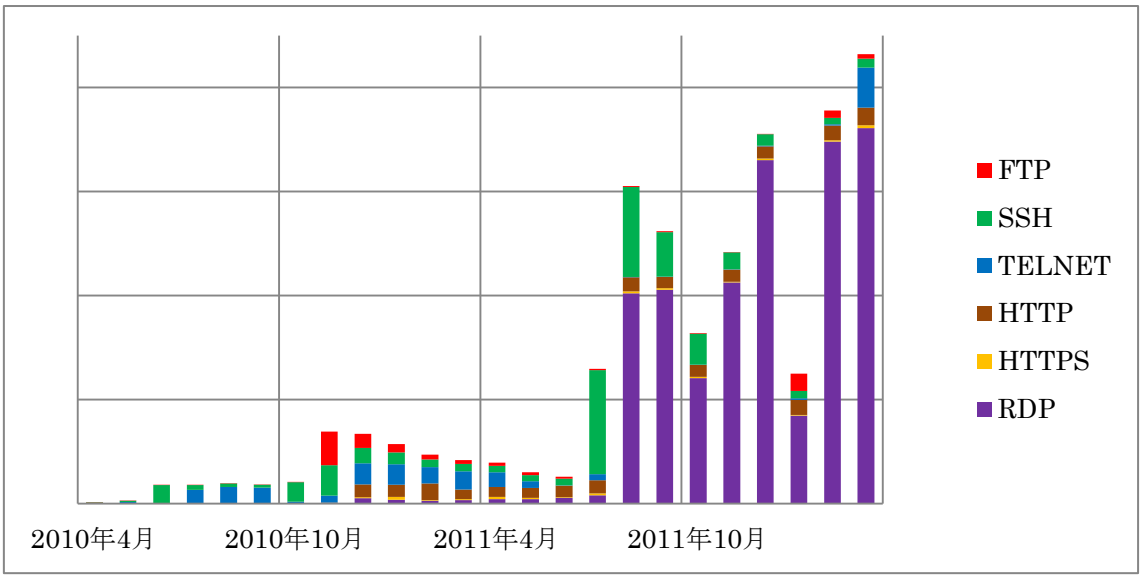

図 2　探索型不正アクセス遮断件数の推移

図 2 は、後者の探索型不正アクセス遮断件数の月別推移を示します。対象プロトコル（ポート番号）として当初は FTP（21/tcp）・SSH（22/tcp）・TELNET（23/tcp）の三つを遮断していましたが、2010 年 11 月からは HTTP（80/tcp）・HTTPS（443/tcp）・RDP（3389/tcp）を加えて対策を強化しています。

上図では 2011 年 8 月以降に RDP の遮断件数が激増していますが、これは RDP を悪用する Morto ワームの出現と拡散が大きく影響しています。しかしながら、その膨大な件数に目を奪われがちではあるものの、特に深刻な脅威とは認識していません。unix 系のサーバに対してリモートから管理操作を行う場合、まずは一般ユーザーでログインして su コマンドにより管理者権限を得るのが一般的ですが、Windows では管理者アカウントで直接ロ

グオンする方が普通ではないかと思います。このため、攻撃側の狙いは管理者アカウントに集中することとなり、実際のパスワード総当たり攻撃でも「Administrator」もしくはそれを書略したと思しき「a」というユーザー名しか確認していません。さらに、これらの不正アクセスはセキュリティホールを悪用するものではありませんので、パスワード管理に怠りがなければ十分に防御が可能と言えます。

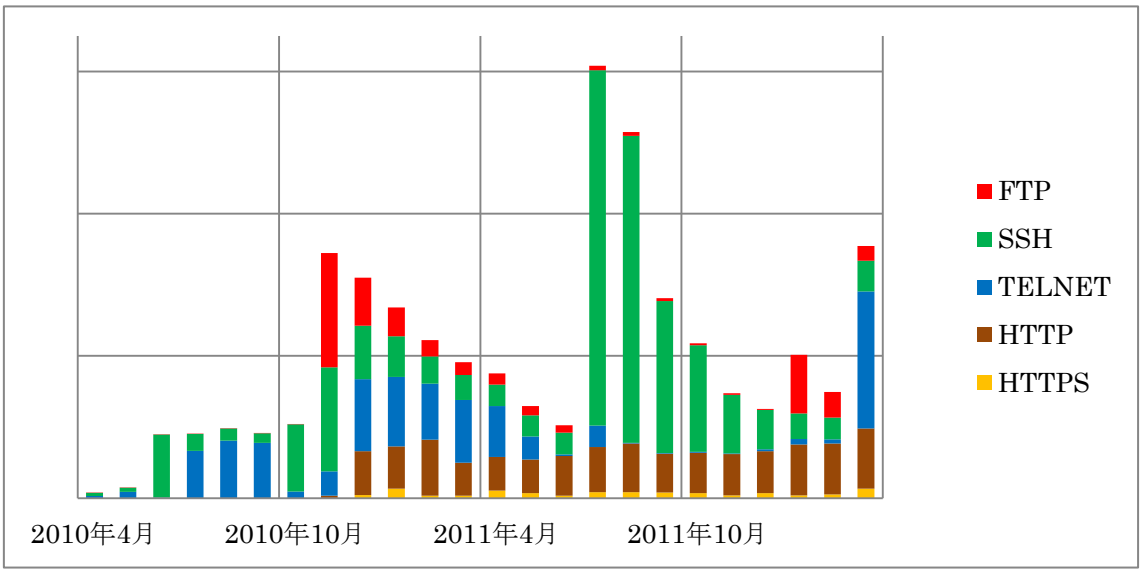

図 3　RDP を除く探索型不正アクセス遮断件数の推移

図 3 は、図 2 から RDP を除いた探索型不正アクセス遮断件数の月別推移を示します。これを見れば明らかなように、unix 系サーバへの一般的なリモートアクセス手段である SSH や TELNET に対する不正アクセスは全く衰えていません。unix 系サーバでは管理者以外の一般ユーザーが複数存在することが珍しくありませんが、その中の一つでも安易なパスワードが設定されていると、それを足がかりに管理者権限が奪われる危険性が存在します。このため、特に SSH におけるパスワード総当たり攻撃は、その内容が確認できないこともあり、依然として大きな脅威であると認識しています。

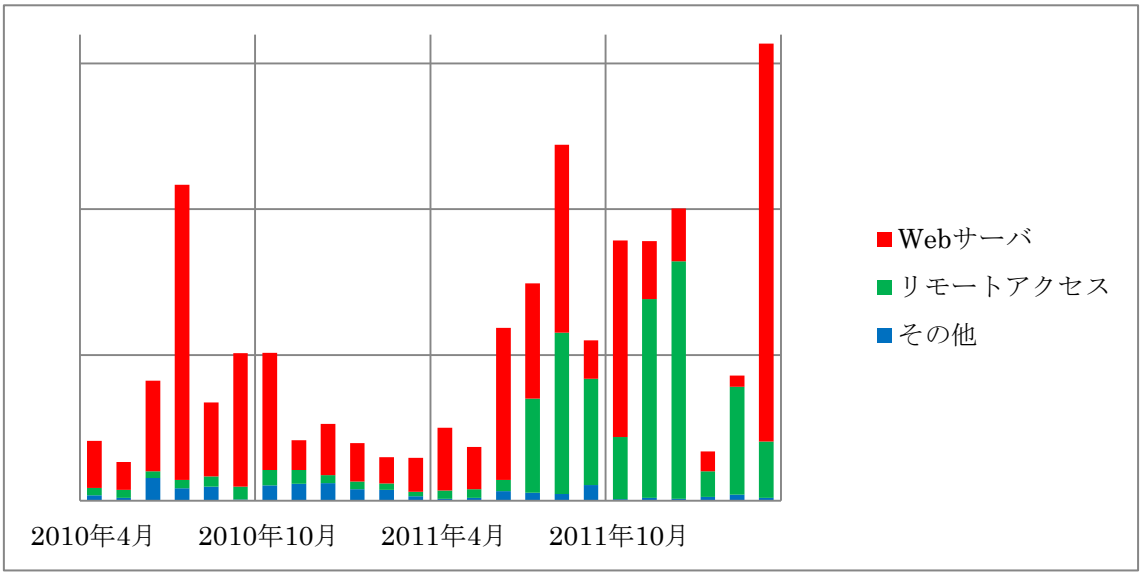

図 4　公開サーバに対する個別攻撃遮断件数の推移

図 4 は、当センターが運用する IPS によって遮断された公開サーバへの個別攻撃件数の月別推移を示します。

上図にて 2011 年 7 月以降にリモートアクセスの割合が増加しているのは、上述した RDP に対するパスワード総当たり攻撃が主たる要因となっています。しかし、こちらでは図 2 のように大半を占めるような状況になっておらず、むしろ Web サーバの方が多く狙われており危険性の高いことがわかります。具体的には CGI の隙を突いてコマンドを実行させるといった手口が目立つのですが、この種の攻撃はセキュリティホールがなくともスクリプトの不備等により成功してしまうケースがあり、IPS で防御しようにも一筋縄では行かないのが実状です。

おわりに

以上、簡単ではありますが、本学における最近のセキュリティ情勢をご紹介させていただきました。サイバー攻撃の手口は日々巧妙化しつつあるものの、それが悪用する基本的な技術にはここ数年間で特に目新しいものは現れていません。上述した傾向はあくまでも当センターが把握できる範囲内に限られたものですが、「システムを常に最新の状態に保つ」とともに「安易なパスワードは使用しない」という基本的なセキュリティ対策の重要性を、この機会に改めてご認識いただければ幸いです。