平成22年1月25日

サブネットワーク管理者各位

ネットワーク管理委員会
委員長　板野 肯三

SSHサービスに関する注意喚起

本学において，学外からログインして計算機を利用する手段として，Telnet等より安全なSSHを用いることが推奨されています．

この数年来，インターネット全体でSSHによる不正ログインの試みが続いております．本学におきましても，いくつかの計算機がSSHサービスを経由して侵入され，侵入された計算機が踏台として利用されて，さらに他の計算機へSSHでの侵入を試みるという事例が継続して起きています．従来にも同様の主旨の注意喚起を行っておりますが，依然として同様の事例が毎年継続して起きており，今年度だけでも新たに10件が報告されている状況に鑑みて改めて管理者の方々の注意をお願いするところです。

これらの事例は，"root"，"test"，"admin"，"pgsql" といった一般的ユーザ名や，よくある人名などに対して，総当たりや辞書を用いたパスワードの推測を行ない，ログインを試みる手口により侵入を許したものと思われます．

これはSSHの脆弱性を用いた攻撃ではないため、最新のSSHサーバを用いていても，設定によっては，このような侵入を許してしまう可能性があります．単にセキュリティ・パッチの適用やソフトウェアの更新を行っているというだけで安心せず今一度アカウントやログイン設定の確認をお願いします．

Unix系のOSでは，インストールした初期状態でSSHサービスが稼働し，テスト用のユーザアカウントが作られているような場合があるようですので注意が必要です．

まず何よりも、ネットワーク経由でのログインが必要ないサーバではSSHサービスを稼働させないという点を徹底願います．

次に，どうしてもSSHサービスを稼働させる必要があるサーバに関しましては、
http://www.jpcert.or.jp/at/2005/at050003.txt を参考に，以下のすべての対策をお取りいただくようお願いいたします．

1. TCP wrapper 等を用い，ログインを許可するクライアント計算機を可能な限り制限する．（できれば少数の計算機、学内等に制限する。そのような制限が難しい場合でも，例えば.jpドメインに制限するだけでも攻撃を受ける頻度を大きく減らすことができる．）

2. rootによるSSHログインを無効にしておく．

3. 不要なユーザアカウントを無効にする．

4. パスワードによる認証でSSHログインを許可することはなるべく避け，公開 鍵認証などの，より安全な認証手段のみ許可するようにする．パスワード認証を用いる場合は，すべてのユーザアカウントに対して，十分な強度のパスワードが設定されていることを確認する．

5. SSHその他OSのソフトウェアは，なるべく最新のものを使用し，脆弱性が発見された場合は速やかに更新する．

以上