2011年9月8日

インシデント発生を抑えるための取り組み

熊本大学総合情報基盤センター　　杉谷　賢一

Kumamoto University

はじめに

ファイヤウォールや侵入防止システムの導入
セキュリティポリシや個人情報保護基準の策定

↓

インシデントの発生は無くならない

↓

攻撃者の手口が巧妙だから？？

↓

利用者もしくはシステム管理者の
注意不足もしくは認知不足による行動が主原因

Kumamoto University

はじめに

［重要なのは］

各人の情報端末の取り扱いに関する
基本的な知識レベルの向上と
その知識に基づく行動

↓

サポートする組織の体制が必要

「教育」＋「（異常）通知システム」

↓

熊本大学での取り組みの紹介

Kumamoto University

インシデントとは

セキュリティの脅威となりうる事象

意図的な、偶発的な、疑いがある、…

重大事故につながりそうな事態

不正アクセス

ssh辞書攻撃、spamメールの大量受信、
Webページの改ざん、パスワード漏洩、
著作権違反ファイルのダウンロード、…

その他

ウィルス感染、情報漏洩、
ソフトウェアの不正コピー、…

Kumamoto University

インシデント発生要因

- サーバの乗っ取り、設定変更、他サーバへの攻撃
- ウィルス感染しボット化
- 可搬端末やストレージの紛失
- p2pソフトを利用し不正ファイルの共有
- ソフトウェアの不正コピー

Kumamoto University

インシデントへの対策

- パスワード管理の徹底
- セキュリティ設定の徹底
- サービスソフト管理の徹底
- OSを含むソフトのアップデートの徹底
- ウィルス対策ソフト導入の徹底
- 可搬端末やストレージの持ち出し管理の徹底
- ソフトウェアのライセンス管理の徹底

「xxxxの徹底」と言っても…

1）注意すべき事項を知らない

2）注意すべき事項をある程度知っているが、すべき行動をとらない

3）知っている注意すべき事項を基に行動するが、知識が少ない

4）注意すべき事項をほぼ把握しているが、行動が不完全である

5）注意すべき事項を基に（ほぼ）完全に行動する

「xxxxの徹底」をさせるには

知る

何をしなければならないのか
何に注意しなければならないのか
何をしてはいけないのか

（何が起きているのか）

↓

「教育」＋「（異常）通知システム」

熊本大学での取り組み [教育]

[1年次生全員への情報基礎科目の実施]

- ネットワーク上の法的責任
  - ・著作権侵害
  - ・名誉毀損
  - 実際に起こった訴訟の例を見ながら学習
- 情報倫理に関する商用コンテンツの学習
  - ・近年に発生した事例集
  - ・習得知識確認のためのオンライン問題集

熊本大学での取り組み [教育]

- ウィルス対策ソフトの紹介
  - ・サイトライセンス契約をしている
  - ・必ず導入すること
- メールの送受信の仕組み
  - ・熊大で作成したメールソフト(Seemit)による学習
  - ・送受信時の注意点の確認・対策の認識

熊本大学での取り組み [教育]

[サーバ管理者向けの講習会]

◆ 研究室でWeb等のサーバ等を作りたい人向け
- ・実習用PCを準備
- ・Linuxのインストール
- ・サーバソフトのインストール・設定・起動
- ・セキュリティ設定

要望がないので最近は行っていない
インターネット上に情報がたくさんあるため
管理上の重要なポイントが抑えられていない可能性も

熊本大学での取り組み [教育]

[情報セキュリティ対策パンフレットの配布]

◆ セキュリティポリシー策定WGで作成
- ・以前のものは、A4見開きで様々な場面を想定し沢山の脅威を示していた
- ・昨年度改定したものは、A4一枚で身近で特に重要な注意点に絞ってある
- ・1年次生の受講する情報基礎科目では講義中に説明

熊本大学での取り組み [教育]

[個人情報保護の学習コンテンツの提供]

- ◆ 商用の学習コンテンツをLMS上で提供
  - ・全教職員が受講対象となるコースを作成
  - ・提供初年度は、全員受講するように指導

残念ながら、全員受講には程遠い状況に...

[全教職員への各種注意喚起メール]

- ◆ セキュリティ、個人所法保護、ライセンス管理 ...
  - ・年に数度、不定期に
  - ・受信者の関心は低い

熊本大学での取り組み [system]

[DNSサーバのクエリログ監視による検知]

- ◆ 常時クエリログを監視
  - ・クエリログを統計処理することにより、攻撃元やウィルス感染端末を推定
  - ・必要に応じてFWでブロックしたり、DNSサーバでブロックしたりする
  - ・ウィルス感染等の疑いのある端末は、すぐに連絡し、必要があれば協力して対処する

熊本大学での取り組み [system]

[FWのアクセスログ等の監視による検知]

- ウィルス感染により使われるポートの監視
  - ・外に向かって大量にアクセスしている端末を特定し、ネットワーク管理者に連絡する
  - ・無線LANを利用している端末が感染している場合は、ユーザ名も判るため、直接端末の持ち主に連絡する

熊本大学での取り組み [system]

[主要サーバの定期的なセキュリティ監査]

- オープンソースの監査プログラムで定期的に
  - ・サーバを構築した直後に、まず監査
  - ・本稼働した後も、年に1，2度監査

[ソフトウェア管理システム]

- 導入アプリケーションとライセンスを登録
  - ・Windows PCは自動登録
    エージェントのインストールが必要

Kumamoto University

おわりに

- 当たり前のことを当たり前と思わせ、実行させる教育(体制)が必要
  - 何度も何度も繰り返し言うしか無い？
  - 常に言っていると「またか」と聞いてくれない？
- 当たり前のことを常に忘れずに行おう！
- サーバ管理者の養成が必要