第2回大学情報サミット大会

セキュリティ検討プロジェクトグループ報告

趣旨

参加各大学における情報セキュリティ上の個別・共通の課題や問題点に対し、参加大学の知を結集・共有して課題の検討や問題の解消を目指し共同研究を行う

プロジェクトの始動

- 「情報セキュリティ」とは？？？
  - あまりにも広義な言葉
  - テーマの絞込み
- 定常業務との共存
  - 限られた人的資源・予算
- 業務へのフィードバック
  - 技術・知識・現場勘・モチベーション

今年のテーマ

- ネットワーク上の脅威を知る
  - もっともポピュラーな脅威
    - SSHポートスキャン
    - SSHブルートフォースアタック
  - 複数の観測点
    - ネットワークブロック的に離散
      - 複数参加大学のネットワーク
      - 攻撃に相関関係が見出せるか？

定常業務と共存しつつ脅威の観測

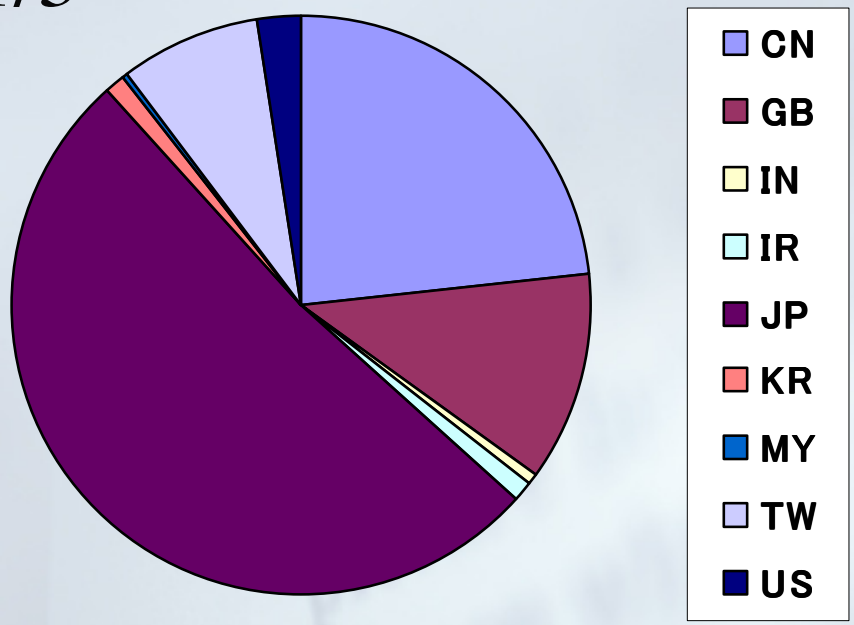
- 限られた資源
  - 人的資源
    - ログの自動収集
  - 予算
    - 余剰（型落ち）機材の再生利用
    - バンドルあるいは無料のOS
    - 無料のパケットキャプチャソフトウェア

観測要領

- Wiresharkによるパケットのキャプチャ
- 観測期間：2007/10/10～2007/11/17の中の一ヶ月間
- 観測点は大学の事情に合わせ決定
  なるだけ外からのトラフィックが到達する場所が望ましい

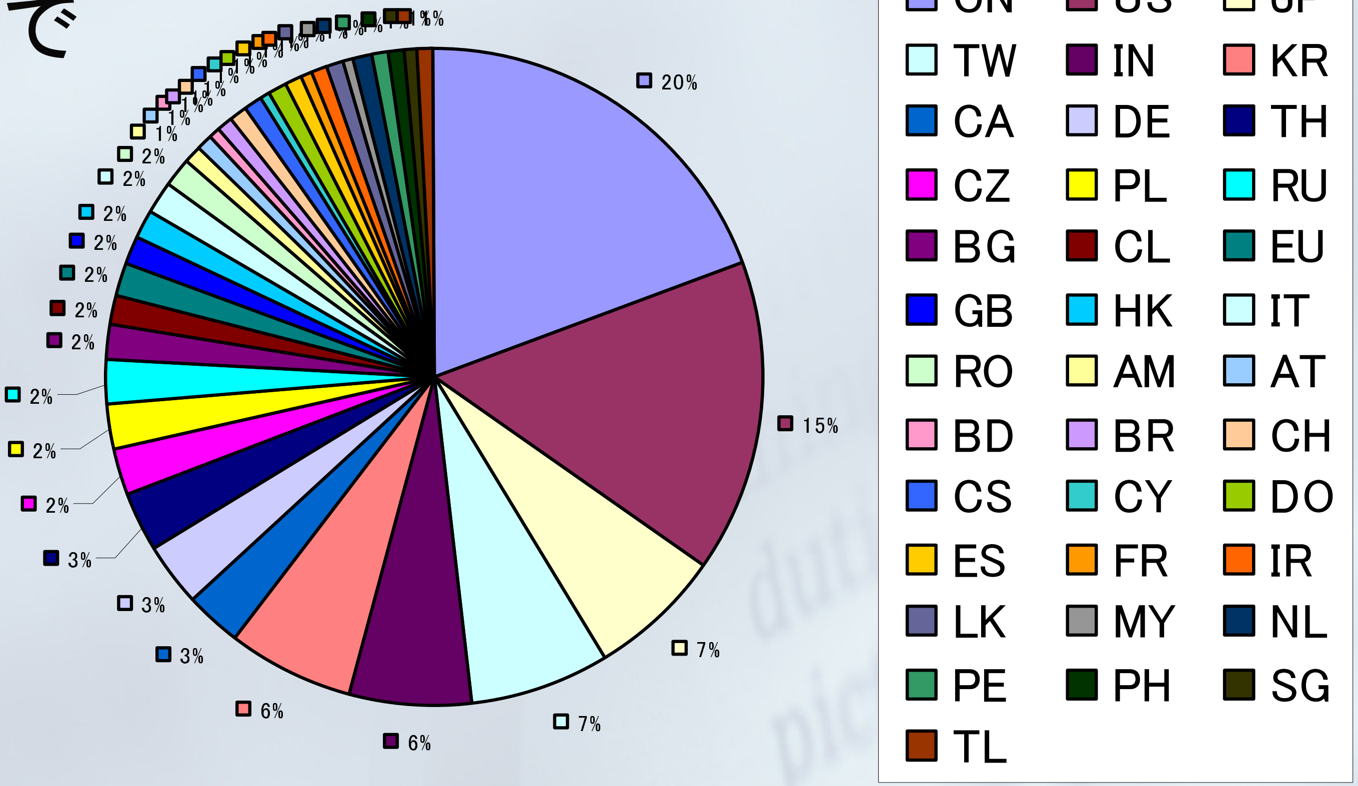
観測点Aにおける観測結果と傾向

- 観測期間（2007/10/11-11/10）
- SYNパケット数をカウント
- 半数以上が国内から
- アジア（中台韓）からが1/3



国別ユニークIP数

- 中国から20%
- 米国から15%
- 上位6カ国で 60%強

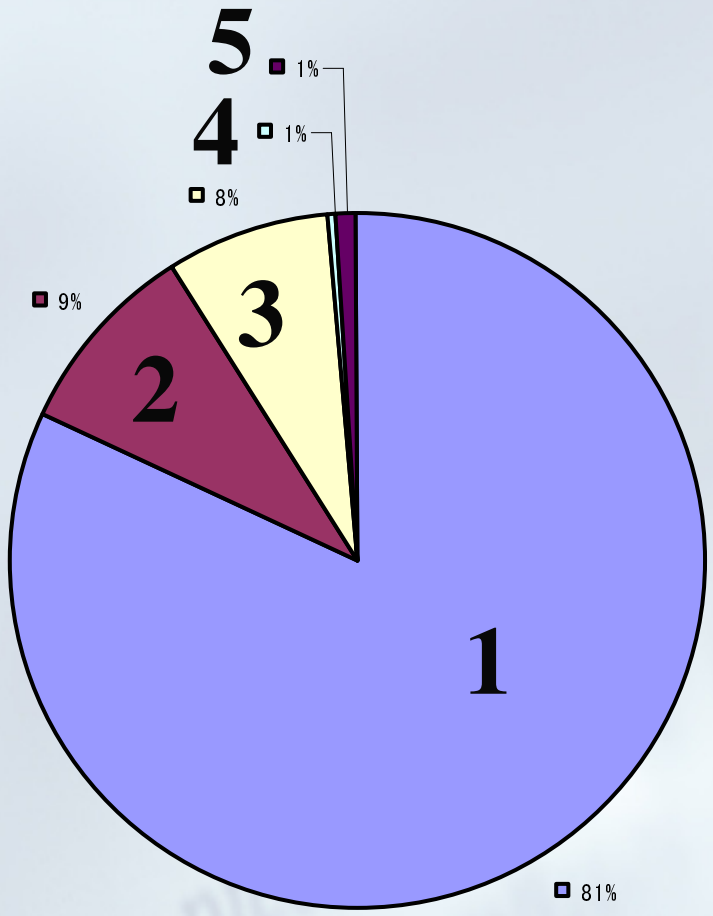


国別ユニークIP数に関する考察

- アジア圏、北米、インドからが多い
  - 単純に端末の絶対数が多い
    - 脆弱な端末の絶対数も多い
    - ほとんどが踏み台である可能性が高いと思われるが、実際のところ始点との区別はできない

ユニークIP別複数拠点への到来数比

- 133ユニークIPを観測
- 109が単一拠点へ
- 12が二拠点へ
- 10が三拠点へ
- 四拠点、五拠点は
  それぞれ1ユニークIP



複数拠点への到来数に関する考察

- 参加大学のすべてがクラスBのIPv4アドレス空間を持つ
- 第1オクテットが同じ大学が3大学（A群）
  - うち第2オクテットが連続している2大学（A1群）
- 二拠点に到来した場合の拠点の組は10/12がA群、うち8/10がA1群
  - A1群の場合到達間隔は28秒から24分20秒
- 三拠点に到来した場合の拠点の組は6/10がA群
  - 到達間隔は3時間51分59秒から5時間34分34秒

複数拠点への到来数に関する考察

- 四拠点に到来した場合の拠点の組はA群＋第1オクテットの類似度が高い1拠点
  - 到達間隔はA群で2時間42分08秒
  - 四拠点では3日と7時間04分25秒
- 五拠点に到来した場合
  - 到達間隔は2日と23時間27分06秒
- 単一拠点にしか到達していないものについてはランダム生成の可能性
- 複数拠点に到達しているものはリニアにプログラム生成
  - A1群の例からクラスBをなめるのに大して時間がかからない

今年の成果:フィードバック

- 最小限の資源の活用可能性
- 特定の脅威ではあるが傾向の把握
- 管理者育成への動機付け

今後に向けて

- 継続的観測の必要性
  - ハニーポットによる継続観測
    - 観測対象の拡大
    - 勘を研ぎ澄ます
    - ブラックリストの共有
- 管理者教育の重要性
  - 大学特有の問題：短い管理者サイクル
  - スーパーユーザの継続的確保
  - スーパーユーザの育成
    - 勉強会の開催、管理者心得の整備

ご清聴ありがとうございました

メンバー一同

林貞孝（慶應義塾：グループリーダー）
藤平貴久（明治大学：グループサブリーダー）
伊藤敦（早稲田大学）
河村学（立教大学）
清水正治（法政大学）
服部裕之（明治大学）
細川達己（慶應義塾）
吉野政美（法政大学）
若林久芳（早稲田大学）