JPCERT/CC に対する DoS 攻撃

小島肇
kjm@rins.ryukoku.ac.jp

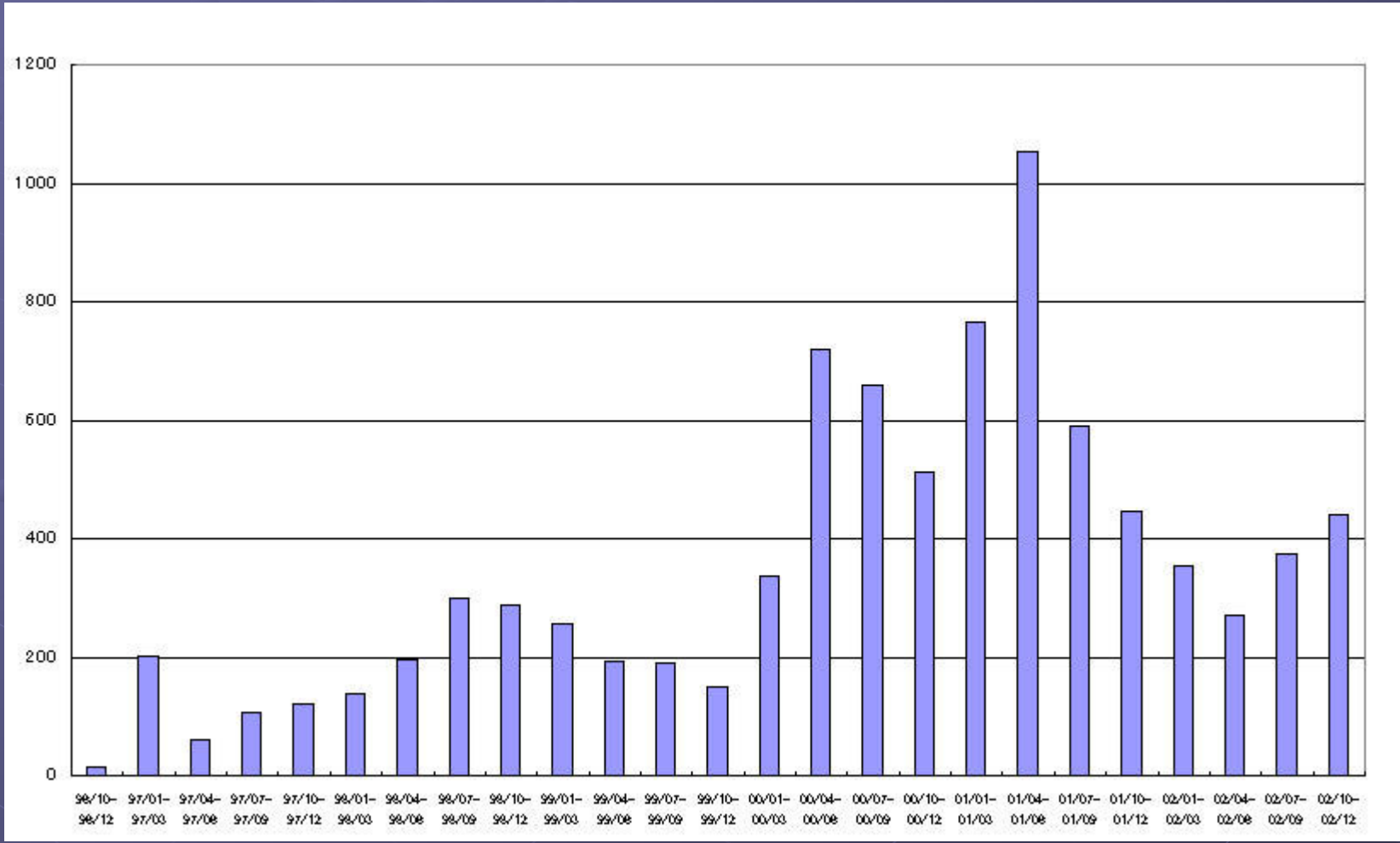
#include <std/desc.h>

- この発表はあくまで個人の立場で行うものであり (以下略)

JPCERT/CC に対する インシデント報告件数

- 現状 4～5 件 / day 程度。
- 報告に伴う関連サイトとのやりとりが 3 件 / day 程度。
- 一見減ってきているように見えるが、実は、…

- http://www.jpcert.or.jp/stat/reports.html より
（3 か月おき、いちばん上が 1200、一番右が 2002.10-12）



JP ドメイン総数（50 万）

- http://jprs.co.jp/press/030107.html
- 日本語ドメインがほとんど使われていないであろう一方、.com や .org を使ってる例も多いから、日本人が利用しているドメインの実数は 50 ± α 万か？

情報提供してくれとか言っているが…

- 日本人が利用している全ドメインから毎日報告が来たら、JPCERT/CC は耐えられるの?
  - 多分無理: JPCERT/CC はそれほど大きな組織じゃない
  - 1000 件 / day 程度でヒーヒーか?

役に立つ情報発信が JPCERT/CC から行われるには…

- 数千件 / day 程度は必要だろう…
- dshield.org は 400 万レコード / day 程度
- 十分な情報提供がなければ、役に立つ情報発信はできない。
  - 役に立つ情報発信がないので報告する気にならず…→ 負のスパイラル

みんなで JPCERT/CC が DoS になるくらいの情報を送ってあげよう!

- 悪意ある報告はダメよん
- 情報提供 として port scan log を送ろう。dial-up router や personal firewall の port scan log で ok
  - テキスト形式で送ってね…
- 使いにくいと評判の報告様式だが、連絡先などをあらかじめ記入したものをつくっておけば、それほど手間ではない。
- 新しい報告様式も近々登場予定! なかなかいいぞ。

Q. 報告様式がウザいんですが

- よほど変なものでない限り、log そのままとかでも受領される模様 (推奨されるわけではないが……)
- 私自身は、報告様式の 3-5 項に dshield.org 報告形式の log をそのまま張り付けて、毎日送りつける script を使っている。dshield.org にある client を改造して使うのもいいだろう。
  http://www.dshield.org/clients.html
- 「情報提供なのか、協力を依頼したいのか、どちらなのかを明確にしてほしい」（JPCERT/CC 談）
- 新しい報告様式は書きやすくなっているぞ。

その他の楽しみ方

- 反応時間から JPCERT/CC の状況を推測する(笑)
  - いや実際、妙に遅いときとかあるし…

定点観測システム？

- 経済産業省「世界規模で報告されたネット障害についての総括レポート～Slammerワームによる被害について～ 」から:
  http://www.meti.go.jp/kohosys/press/0003634/

今回のようなワームによる感染の急激な広まりに際しては、関係組織間での情報連携が重要である。したがって、今後、
・情報収集・相談窓口の強化 (JPCERT/CC、IPA)
・定点観測システムの構築 (JPCERT/CC)
・国際的連携の強化（特に時差の少ないアジア太平洋地域内での情報共有）
等が急務であると考える。

Links

- JPCERT/CC
  http://www.jpcert.or.jp/
- DShield.org
  http://www.dshield.org/