IODEF experience in JPCERT/CC

AGENDA

- Scan information reports
- Incident reports exchange
- (JVN: vendor status notes)
- How to proceed inch wg?

Small Update from INCHwg Seoul

Scan information reports

- JPCERT/CC ISDAS system gathers port-scan logs
- extracting allocated-country wise logs and send them periodically to the related “national” CSIRTs(KR,CN,AU,...)

Scan information reports(2)

- Want to see how useful this type of information for CSIRTs
- Feedback and discussion on the profile jut starting
- Aims to standardise the profile among APCERT...
  - ➔ Check the conference program!

Incident reports exchange

- Aims to setup “standard” profile among APCERT (asia-pacific CSIRT community)
- Start discussion on proile among KrCERT,CNCERT/CC,JPCERT/CC
- Just start now. We'll update later...

We assume a profile for each scan reports and incident reports

JVN: JPCERT/CC Vendor Status Notes

- Collaboration between JPERT/CC and Keio university (mainly one person, Terada)
- Based on CERT/CC advisories, gather information on JP vendors' correspondence
- http://jvn.doi.ics.keio.ac.jp/

JVN: JPCERT/CC Vendor Status Notes

- How can we ease the update process of vendors' information?
- VULDEF for information exchange
- Push updates from vendors
- (I'm not sure it's directly related to IODEF, but looking VEDEF, anyway introduce here. I'll kick Terada!)

How to proceed INCHwg

- Real usage necessary to discuss further
  - ➔ Current datamodel document should be informational RFC (version1)

- More experience reports, discussion on the usage and finally version2
  - Specific format for each scenario?
  - Basic part and additional option parts?
  - Universal format for any scenarios?