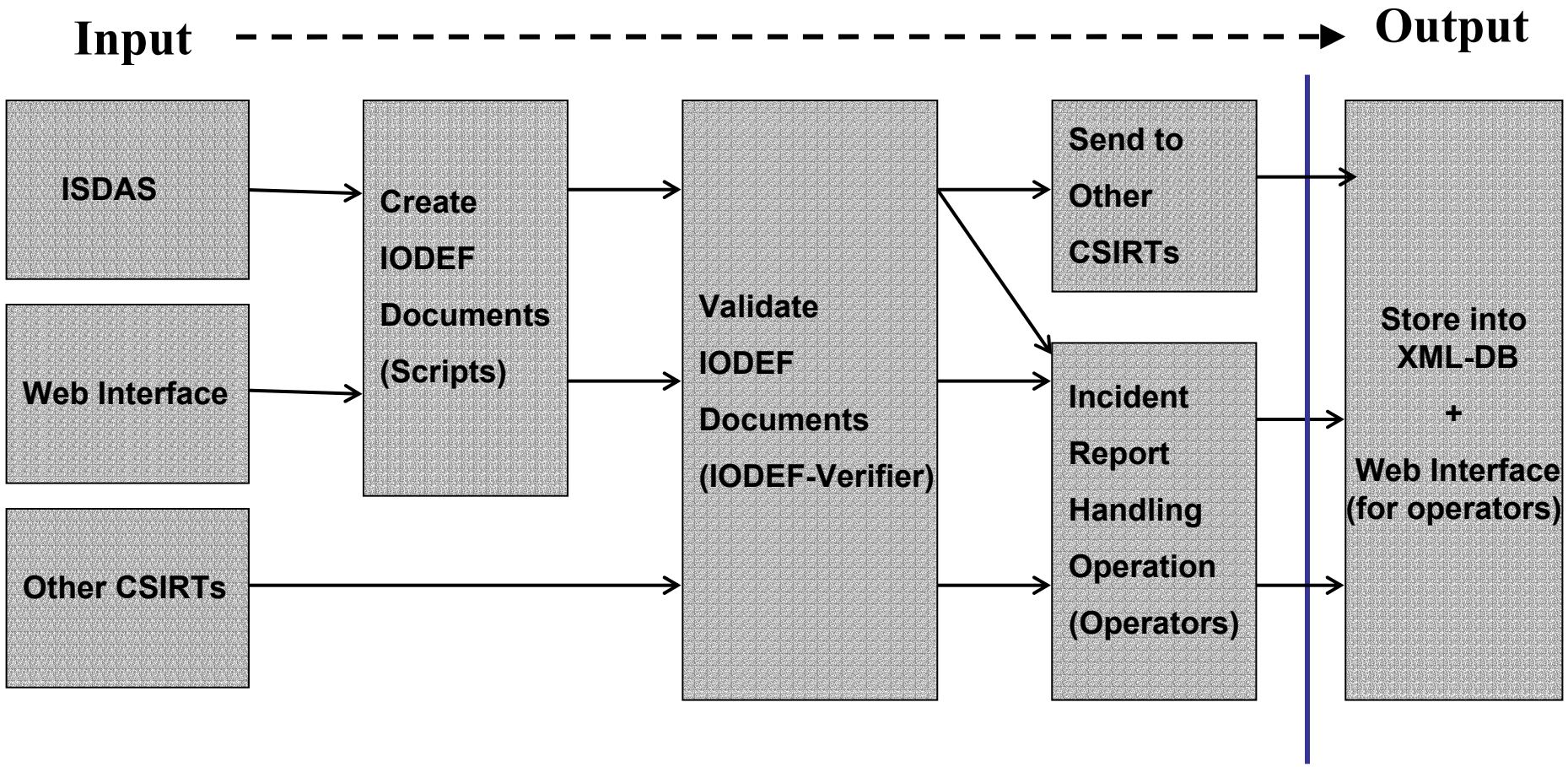
Early Experience from the JPCERT/CC IODEF Activity

JPCERT/CC: Hiroyuki Kido
Cyber Solutions: Glenn Keeni-Mansfield

Demostration

- Web Interface to gather Incident Reports as a form of IODEF (only in Japanese)
  - Prototype Implementation was Done
  - In phase of operational test by IR operators
  - Operation will begin around Aug 2004
- System to send scan data from data gathered by JPCERT/CC ISDAS (Internet Scan Data Acquisition System) in IODEF form
  - Experimental sending had already started !!
  - CERT/CC-KR, CNCERT, AUSCERT,….

IODEF Data Flow in JPCERT/CC

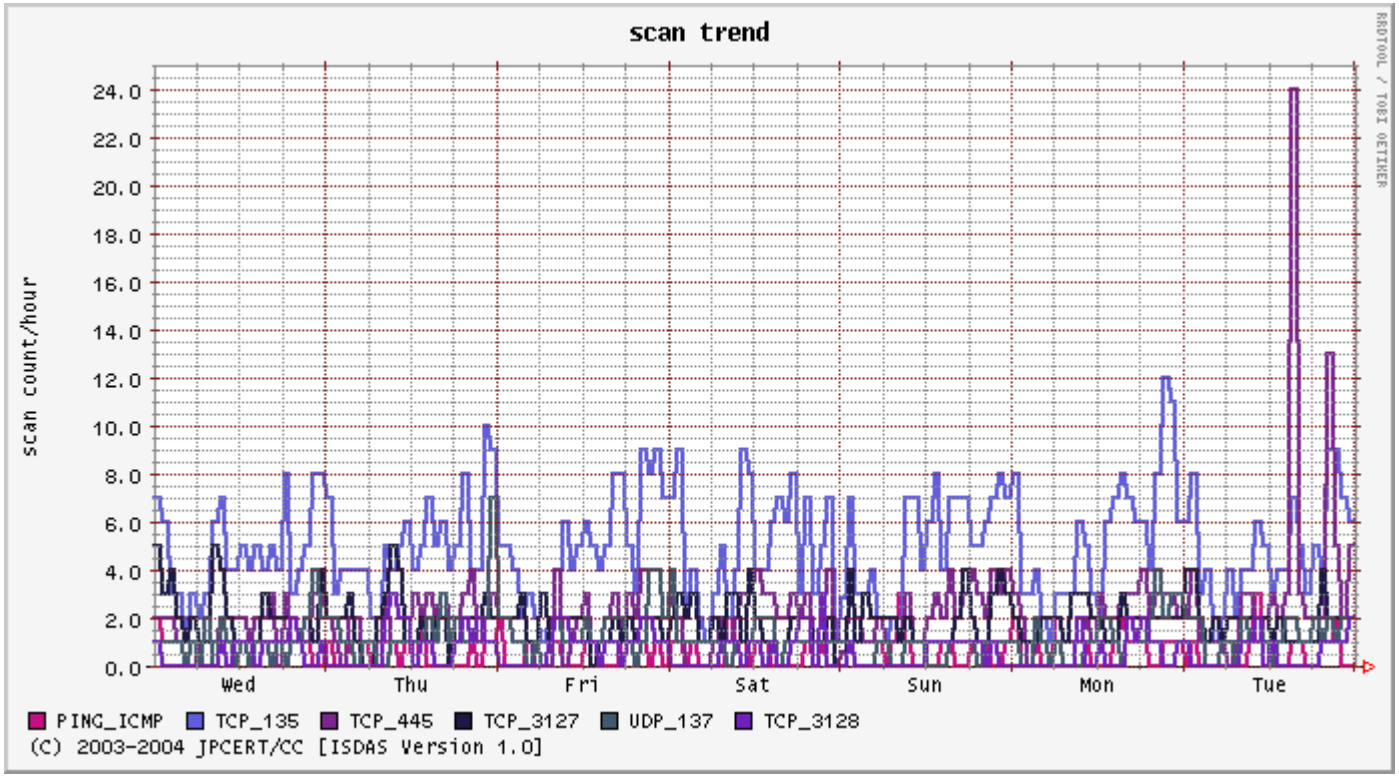


Web Interface

- Gather Incident Report in Following Category
  - Scan/Probe
  - Intrusion/Abuse
  - Relay
  - DoS
  - Forged
  - Worm/Virus

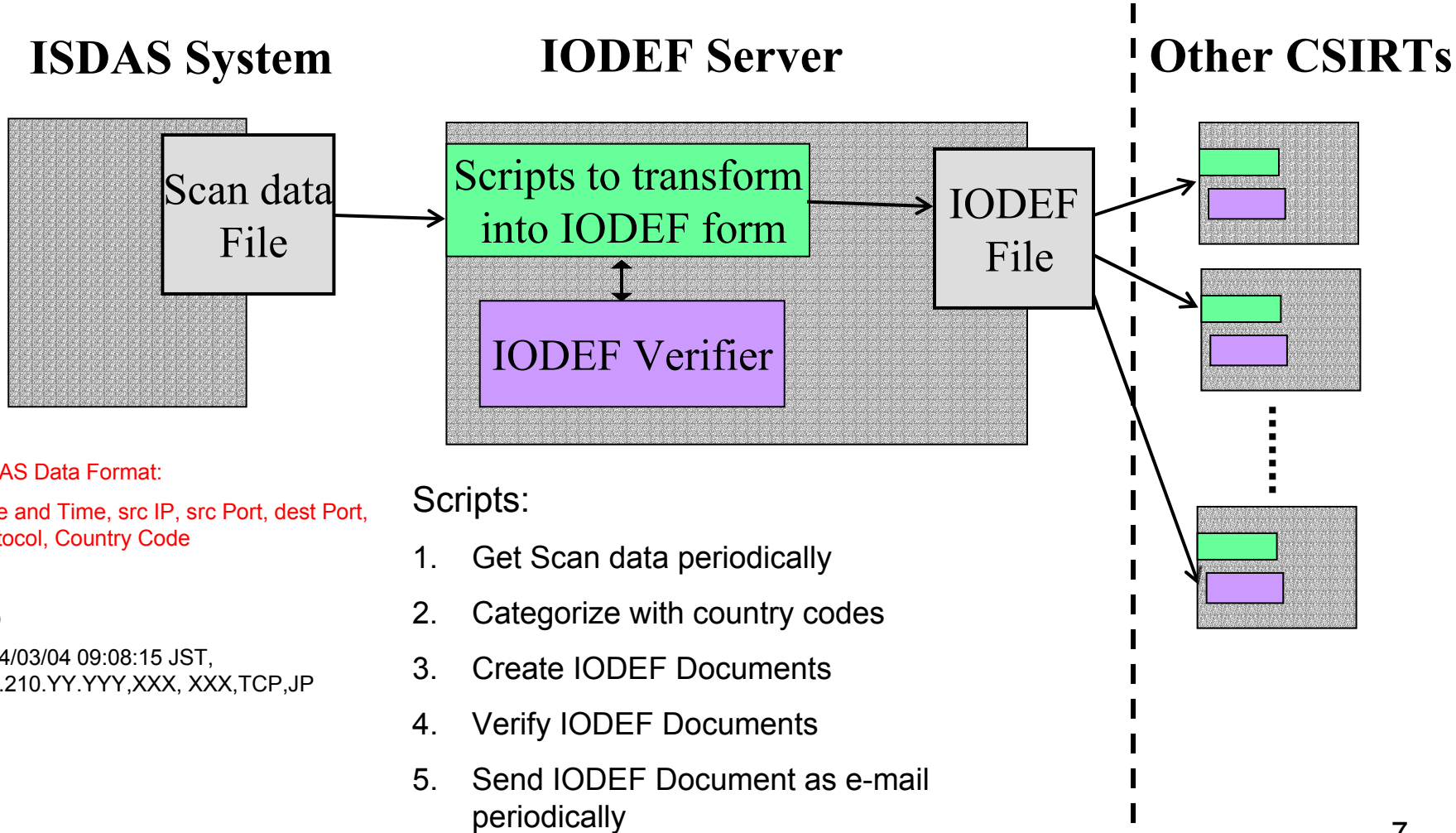
ISDAS

JPCERT/CC Scan Monitoring System



http://www.jpcert.or.jp/isdas/index-en.html

Outlook of System Architecture



ISDAS Data Format:

Date and Time, src IP, src Port, dest Port, Protocol, Country Code

Ex.)

2004/03/04 09:08:15 JST, 220.210.YY.YYY,XXX, XXX,TCP,JP

Scripts:

1. Get Scan data periodically
2. Categorize with country codes
3. Create IODEF Documents
4. Verify IODEF Documents
5. Send IODEF Document as e-mail periodically

IODEF Profile for Scan Data

- ISDAS Scan Data
  - Date and Time , src IP, src Port, dest Port, Protocol, Country Code
- IODEF Form

```
<?xml>
<IODEF-Document>
 <Incident>
  <IncidentID>JPCERT/CC#3001-XXXXXXXX</IncidentID>
  <IncidentData>
   <Description>YYYYYYYYYYYY</Description>
   <Contact role="tech" type="organization">
   XXXXXXXXXXXXXXXX
   </Contact>
   <ReportTime>2004-03-03T00:00:00-09:00</ReportTime>
   <StartTime>2004-03-02T18:00:00-09:00</StartTime>
   <EndTime>2004-03-02T19:00:00-09:00</EndTime>
   <Expectation>
    <Description>YYYYYYYYYYYY</Description>
   </Expectation>
   <Assessment><Impact severity="xxx“ type="x"/></Assessment>
   <EventData>

   </EventData>
  </IncidentData>
 </Incident>
</IODEF-Document>
```

```
<EventData>
 <DetectTime>2004-03-02T18:01:26-09:00</DetectTime>
 <System category="source">
  <Node>
   <Address category="ipv4-addr">
    <address>XXX.XXX.XXX.XXX</address>
   </Address>
  </Node>
  <Service>
   <port>XXX</port>
   <protocol>TCP</protocol>
  </Service>
 </System>
 <System category="target">
  <Service>
   <port>XXX</port>
  </Service>
 </System>
</EventData>
```

Future Work

- Web Interface in English
- Public Distribution
  - Web Interface (Input)
  - XML DB and Web Interface
- XML-Signature and XML-Encryption