

# Collaborative Vulnerability Analysis

## JPCERT/CC and CERT/CC

---

Art Manion  
CERT/CC

Yurie Ito  
JPCERT/CC



CarnegieMellon  
Software Engineering Institute  
CERT<sup>®</sup>Coordination Center

---

**JPCERT/CC**

# Motivations

---

## □ CSIRT motivations

- Better contact with Japanese and U.S. vendors
  - Language, time zone, culture
- Model for sharing vulnerability handling capability across multiple coordination centers
- Share resources/load balance
- Reduce duplication

## □ Vendor motivations

- Awareness of new vulnerability information
- Dissemination of vendor information



# Timeline

---

- 2003 Oct First discussions, process mapping
- 2004 Mar Vulnerability Handling Workshop with Japanese vendors in Tokyo
- 2004 Aug Coordination centers meeting in Seattle
- 2004 Dec-2005 Mar CERT/CC team members mentor JPCERT/CC in Tokyo
- 2005 Aug JPCERT/CC visits CERT/CC
- 2005 Nov "Vultures" meeting in San Mateo
- 2006 Feb Decision Support System (DSS)
- 2006 Oct Secure Coding tutorial in Tokyo
- 2006 Nov "Vultures" meeting in Pittsburgh



# Communication

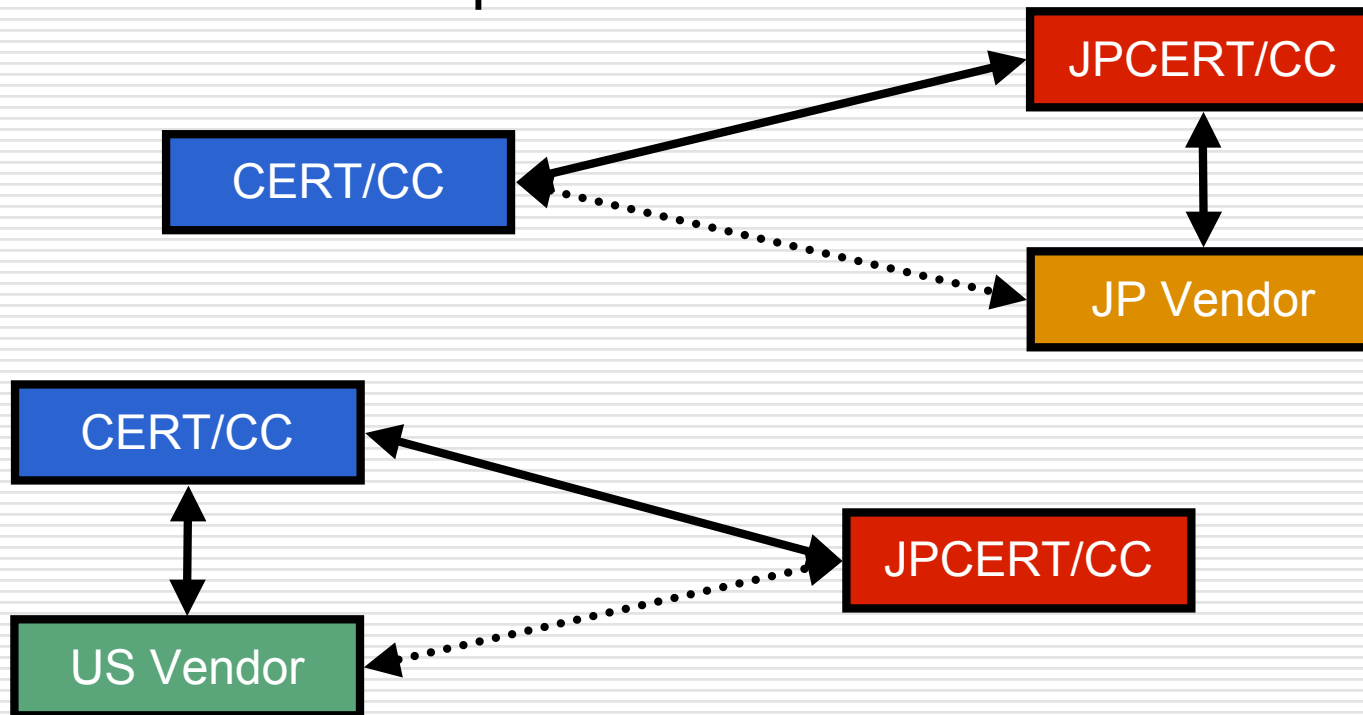
---

- ❑ Direct communication between teams
  - Email, telephone, video conference, meetings
  - Daily operations, out-of-hours warning
- ❑ Shared infrastructure
  - Integrated database
  - Discussion forum
  - Planning to cross-certify CAs
- ❑ Vendor communication
  - Direct coordination
  - Indirect coordination



# Direct Vendor Coordination

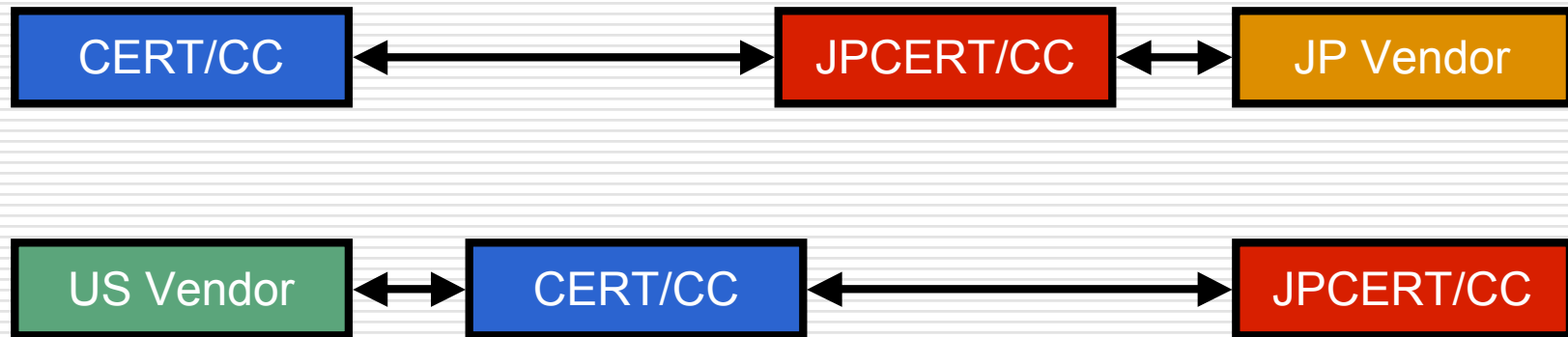
- ❑ Contact vendor and local CSIRT
- ❑ Local CSIRT works with vendor, vendor and/or local CSIRT respond



# Indirect Vendor Coordination

---

- ❑ Contact local CSIRT, local CSIRT contacts vendor
- ❑ Local CSIRT works with vendor, local CSIRT responds on behalf of vendor



# Vulnerability Policy

---

- ❑ FIRST Vendor SIG (SIGIIV)
- ❑ APECTEL Vulnerability Handling Workshop
- ❑ Vendor contacts meetings in Tokyo
- ❑ GFIRST workshop (U.S. government CSIRTs)
- ❑ Comparable vulnerability disclosure policy



# Publication

---

## □ CERT/CC

- Vulnerability Notes (web)
- Technical Alerts (web, email)

## □ JPCERT/CC

- Japanese Vendor Notes (JVN)
  - JVN-VU, JVN-TA (web)
- Alerts (web, email)



# Success Stories

---

- ❑ Localized threat analysis
- ❑ Reaching more vendors
- ❑ Patch verification
- ❑ WinNY vulnerability
- ❑ Secure Coding Initiative
- ❑ Vulnerability analysis/reproduction
- ❑ Multiple coordination center model
- ❑ Trust, comparable policies

