

# Vulnerability Handling in Japan

Yozo TODA  
Information Coordination Group  
JPCERT/CC

CNCERT/CC conference 2005, 桂林, China  
March 25th, 2005

## What is JPCERT/CC? (1)

- started as a voluntary group in 1992
- Officially established as JPCERT/CC in 1996, with funding from MITI (Ministry of International Trade and Industry - predecessor of METI)
- Not-for-profit organization
- Budgeted by METI, MEXT
- Non-governmental Organization
- No law-enforcement

## What is JPCERT/CC? (2)

- National CSIRT in Japan (Point of Contact for International relations)
- FIRST(Forum of Incident Response and Security Team) Full member since 1998
- APCERT(Asia Pacific Computer Emergency Response Teams) SC member, Secretariat

Reactive to Proactive

# JPCERT/CC Services



# Vulnerability Handling

- What is Vulnerability Handling
- Coordination
- Vulnerability related information

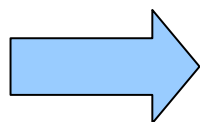
# What is Vulnerability Handling

## □ Players

- person/groups who find vulnerability
- Software vendors
- customers/users
- Bad guys/kiddies

# What is Vulnerability Handling

- person/groups want to disclose to the public what they found
- Vendors should provide upgrades/workarounds
- Users are affected; risk for exploit grows
- Kiddies want to play with it

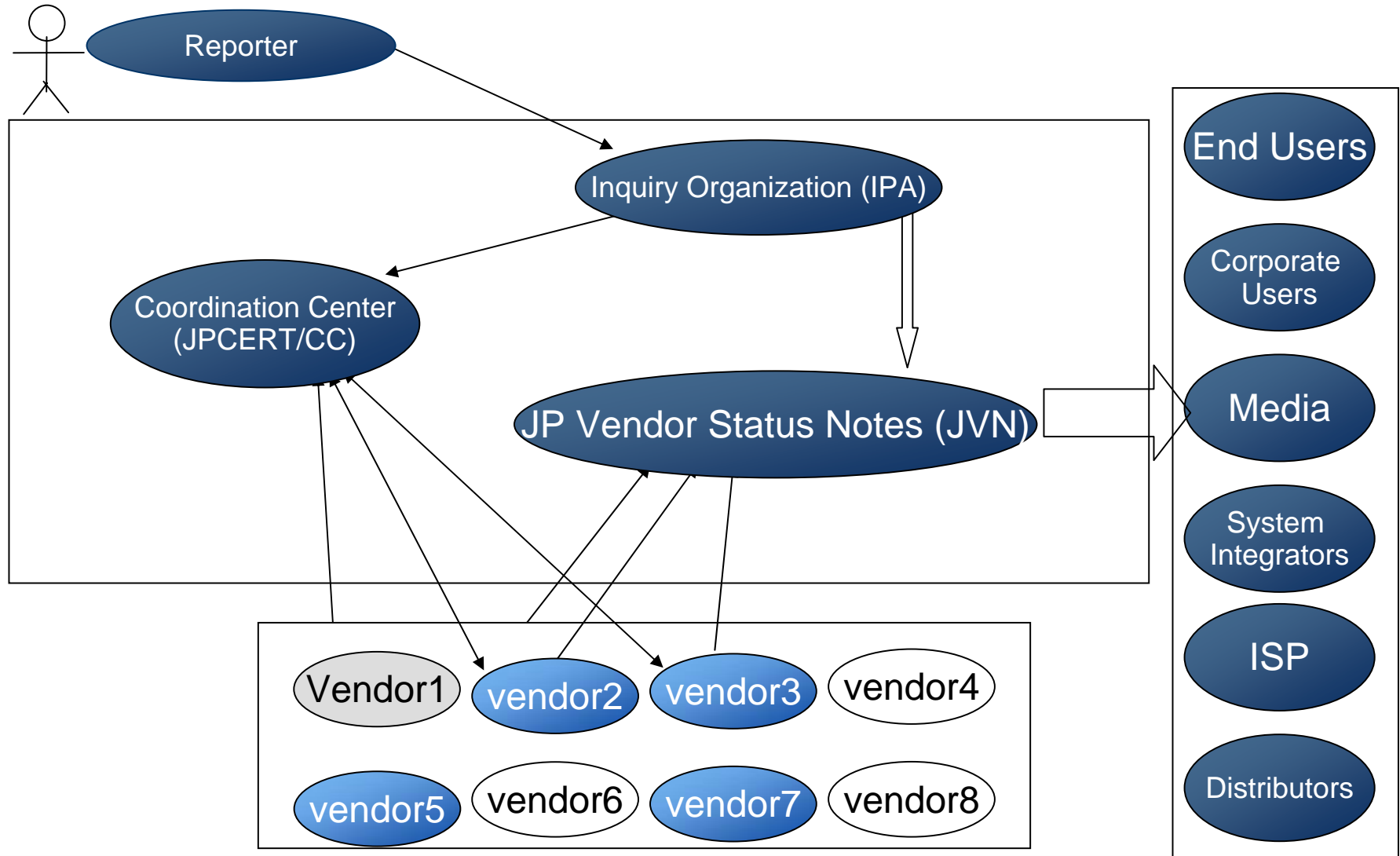


***Needs for coordination!!***

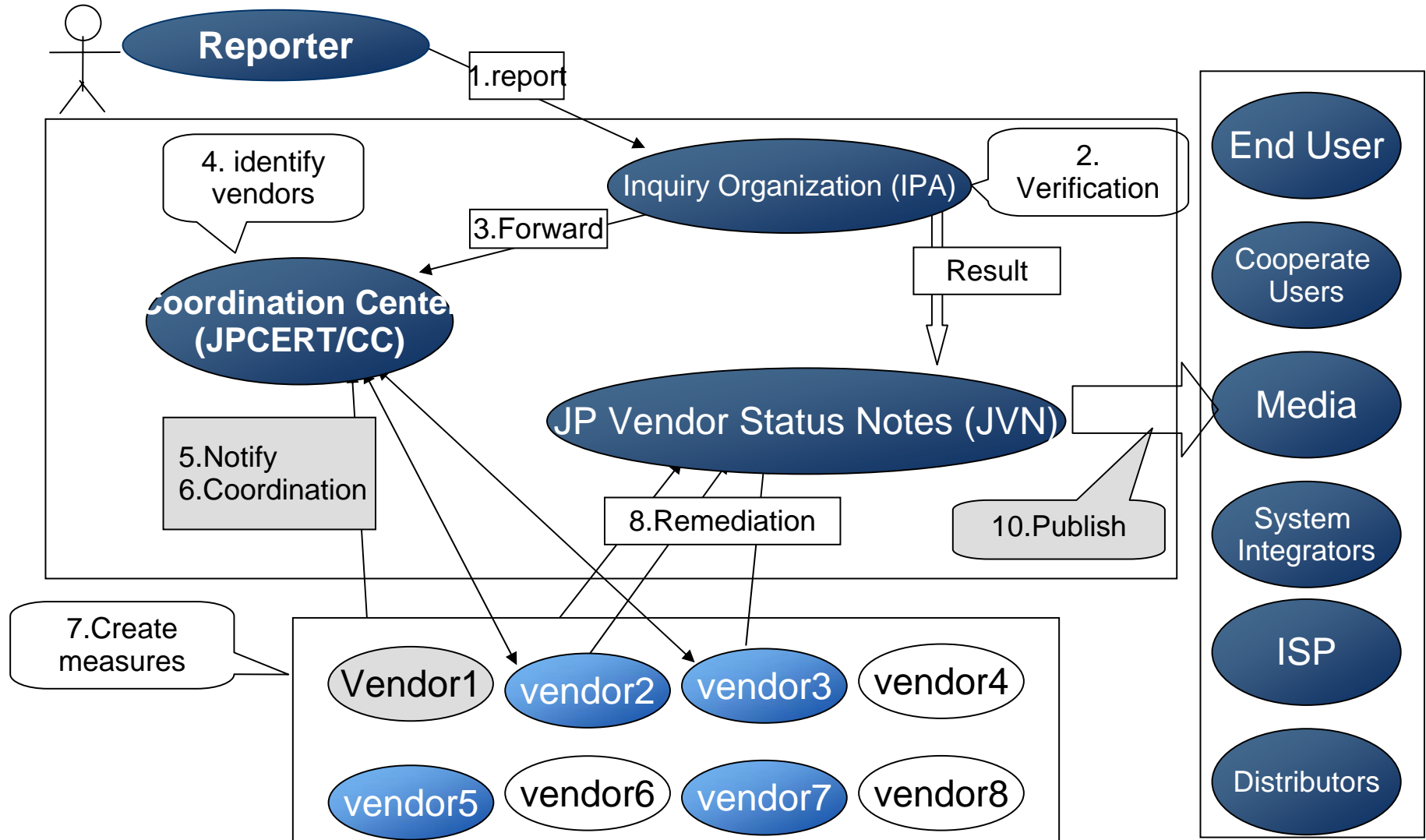
# Coordination Tasks

- **Receive vulnerability related information**
- **Notification to vendors**
- **Coordination on publishing date**
  - Multiple vendors may be involved
- **Help publicize the counter-measure**

# Vulnerability Handling Framework



# Vulnerability Handling Framework



# Portal site JVN <http://jvn.jp/>

JP Vendor Status Notes - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://jvn.jp/

Firefox Help Firefox Support Plug-in FAQ

JVN  
JP Vendor Status Notes

Last updated: 15:30 2005/03/18

Home

- JVNとは
- VN - JP
- VN - CERT/CC
- VN - NISCC
- TRnotes
- ベンダ情報一覧

関連サイト

- JPCERT/CC
- ISDAS
- IPA/ISEC
- 脆弱性情報の届出
- CERT/CC
- NISCC
- CVE

JPCERT/CC

IPA

Done

Topics

- 2004年07月08日 : 本運用開始
- 2004年07月20日～ : [脆弱性関連情報取り扱い説明会](#) (終了致しました)

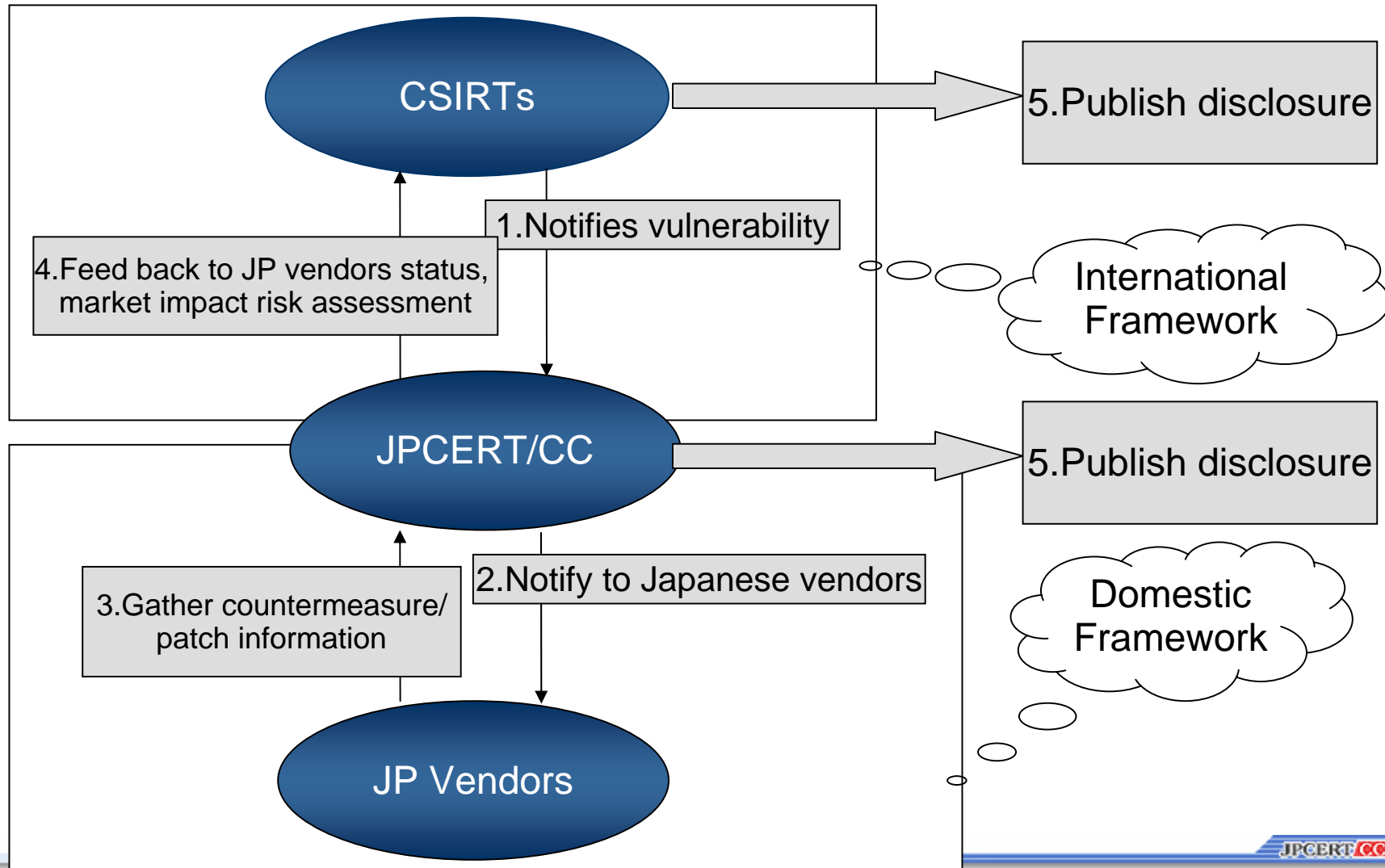
Vendor Status Notes — JP [INDEX](#)

- [JVN#1F649902](#): McAfeeウイルススキャンエンジンにバッファオーバーフローの脆弱性 [2005/03/18 15:30]
- [JVN#8BAAAB4E](#): msearch におけるディレクトリトラバーサル脆弱性 [2005/03/16 11:00]
- [JVN#DD18AD07](#): Tomcat におけるサービス拒否の脆弱性 [2005/03/16 11:00]
- [JVN#67B82FA3](#): SSL-VPN製品におけるCookieの脆弱性
- [JVN#8F8B1C85](#): サイボウズ Office におけるブラウザスクリプト実行の脆弱性

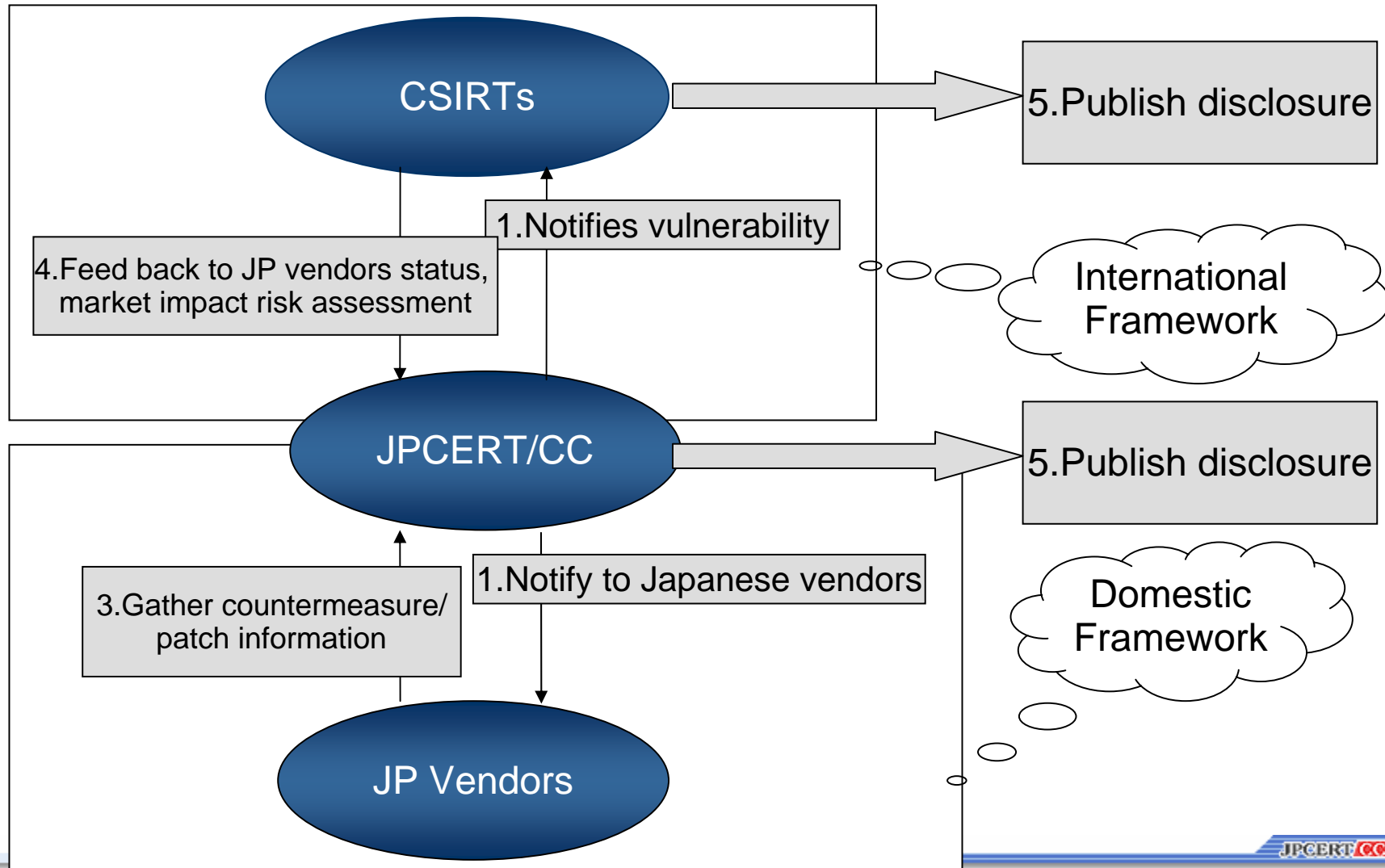
Vendor Status Notes — CERT/CC [INDEX](#)

- [JNVU#702777](#): UW-imapでユーザ認証が正しく行われない脆弱性 [2005/03/17 17:30]
- [JNVU#698302](#): nfs-utils にバッファオーバーフローの脆弱性 [2005/03/11 20:00]
- [JNVU#448384](#): ISC DHCP の enwarn.c にフォーマット文字列の脆弱性 [2005/03/10]
- [JNVU#125598](#): LibTIFF に整数オーバーフローの脆弱性 [2005/03/08]
- [JNVU#253024](#): Adobe Acrobat Reader for UNIX にバッファオーバーフローの脆弱性 [2005/03/08]

# International framework



# International framework(2)



## Requirements to Vendors

- **JPCERT/CC maintains the vendor list**
- **Ask vendors to register to the list**
- **But ! We require vendors to**
  - **Establish intra framework**
  - **the responsible Point-Of-Contact**
  - **Responsible information control**
  - **Agree to the JPCERT/CC vendor list registration rules**
  - **Agree to the information disclosure rules**
  - **Check the technology keywords**

## Recent JPCERT/CC experience 2004 July to 2005 January

- **Number of the whole coordination: 37**
  - **discovered in Japan and reported to IPA: 12 cases**
  - **From CERT/CC: 21 cases**
  - **From NISCC: 4 cases**
  
  - **Single vendor coordination: 8**
  - **Multiple vendors coordination: 22**
- **Non-coordinated information published on JVN: 20**
- **And on-going cases...**

## vulnerability handling capability is useful

- for vendors
  - to create patch in advance the disclosure
  - To minimize the users risk by distributing the counter-measure at the same time of disclosure
- for the CIP (Critical Infrastructure Protection)
  - To do risk/impact assessment
- for the System integrators and users
  - To know the counter-measure for software used

# International coordination is important

- Affected vendors may be within multiple countries
  - coordination centers should take a leading role to conduct schedule coordination.
- Vendors Notification
  - Notification of the sensitive information should be with safely and timely manner
    - Develop trust appropriate POC at local vendors
    - Notification with local language
    - There are large number of vendors in India, Kr, CN...
- Coordination between discoverer and vendor
  - Often different motivation
  - Share public monitoring resources

## International coordination is important(2)

- Information disclosure
  - Publishing in local language
  - Media correspondence
- impact/risk should vary for each economy/culture, etc.
  - Vulnerability in Ipv6 protocol
  - Some Localisation part have a vulnerability

# Thank you! 謝謝!!

## □ Contact

Yozo TODA

Information Coordination Group

JPCERT Coordination Center

- Email: office@jpcert.or.jp
- Tel: 03-3518-4600
- <http://www.jpcert.or.jp/>
- <http://jvn.jp/>