情報公開ポリシーと、対策情報流通体制について(JVN)

JPCERT コーディネーションセンター
寺田真敏

JPCERT CC

目次

- 脆弱性情報の取り扱いに関する歴史
- JPCERT/CCにおける脆弱性情報公表の考え方
- 対策情報流通体制について(JVN)

JPCERT CC

1. 脆弱性情報の取り扱いに関する歴史

1988年	CERT/CC 設立
1993年	Bugtraq メーリングリスト創設
1997年	NT Bugtraq メーリングリスト創設
2000年	SecurityFocus.com VulnHelp (2000年7月) CERT/CC 脆弱性情報公開ポリシー改訂 (2000年10月9日以降)
2002年	IETF におけるインターネットドラフトの提案棄却 (2002年2月) OIS (Organization for Internet Safety)設立 (2002年9月) ISS 社の脆弱性開示ガイドライン (2002年11月)
2003年	OIS が“Security Vulnerability Reporting and Response Process” を公開 (2003年7月)
2004年	ソフトウエア等脆弱性関連情報取扱基準 (2004年7月)

JPCERT CC

1. 脆弱性情報の取り扱いに関する歴史
Bugtraqメーリングリスト

- フルディスクロージャ(Full Disclosure)という考え方に基づいて運用されているメーリングリストであり、脆弱性に関する詳細情報の交換に利用されている。

- フルディスクロージャとは、セキュリティに関するひとつの考え方であり、「真にセキュアなシステムとは、プロトコル、ソースコードなどすべての視点でオープンレビューに耐えうること」「脆弱性に関する詳細情報はすべてのユーザが利用できること」としている。

1. 脆弱性情報の取り扱いに関する歴史
CERT/CCのアプローチ

- CERT/CCが報告を受けてから45日後を目安に脆弱性を公表する。深刻な脆弱性に関しては公表までの期間を変更する場合もある。
- 脆弱性を除去するための調整作業
  - 報告を受けた脆弱性の影響を受ける製品開発者と連絡を取りながら公表の日程を調整する。
- 対策情報の発信形態
  - 深刻な脆弱性に関してはCERT Advisory (現US-CERT Technical Cyber Security Alert) で公表し、その他の脆弱性に関してはCERT Vulnerability Notes (現US-CERT Vulnerability Notes) で公表する。

JPCERT CC

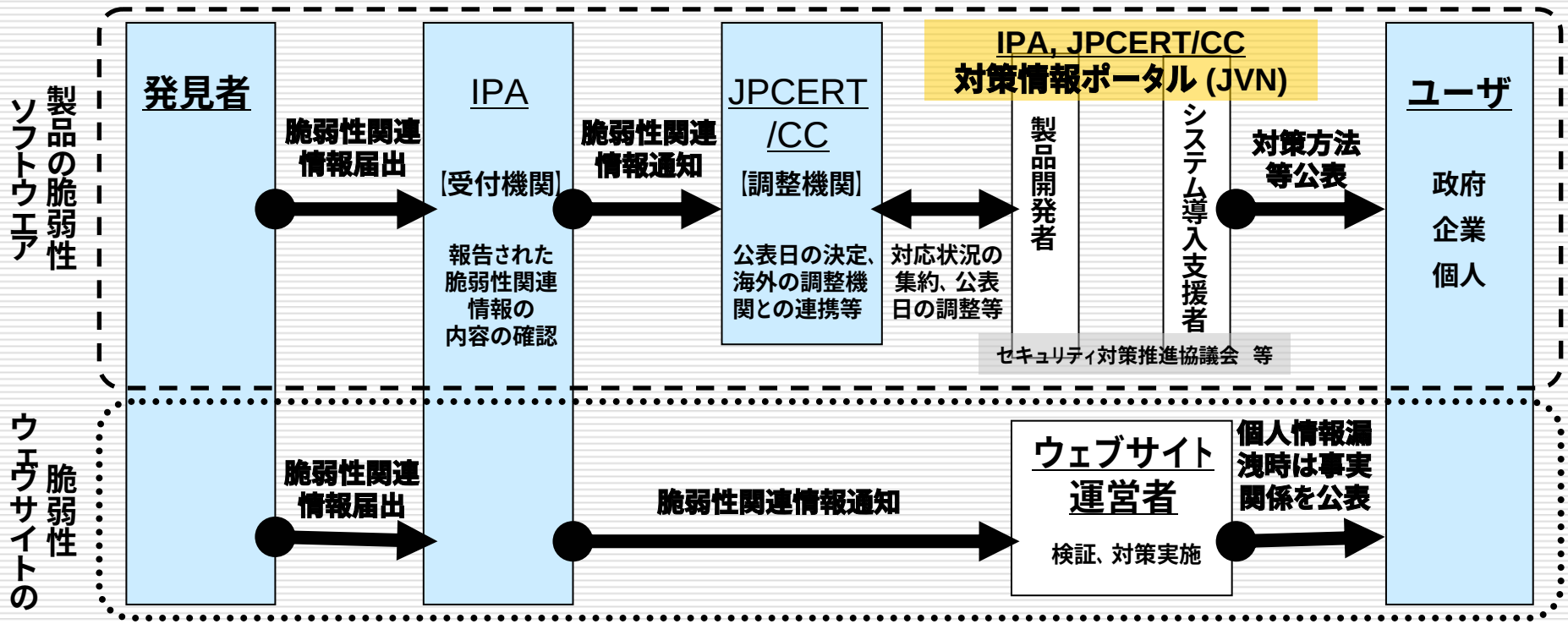
2．JPCERT/CCにおける脆弱性情報公表の考え方

- 脆弱性情報を公表する理由
  - 対策のないまま脆弱性が放置されてしまうことを防ぐ
  - 管理者に対策推進の動機付けを行う
  - 潜在的に存在する脅威に対して理解を深める
- 製品開発者の対策活動の支援
  - 公表日程のスケジューリング
  - 脆弱性情報と対策情報の同時公表
  - 影響を受ける製品開発者の情報公表

JPCERT CC

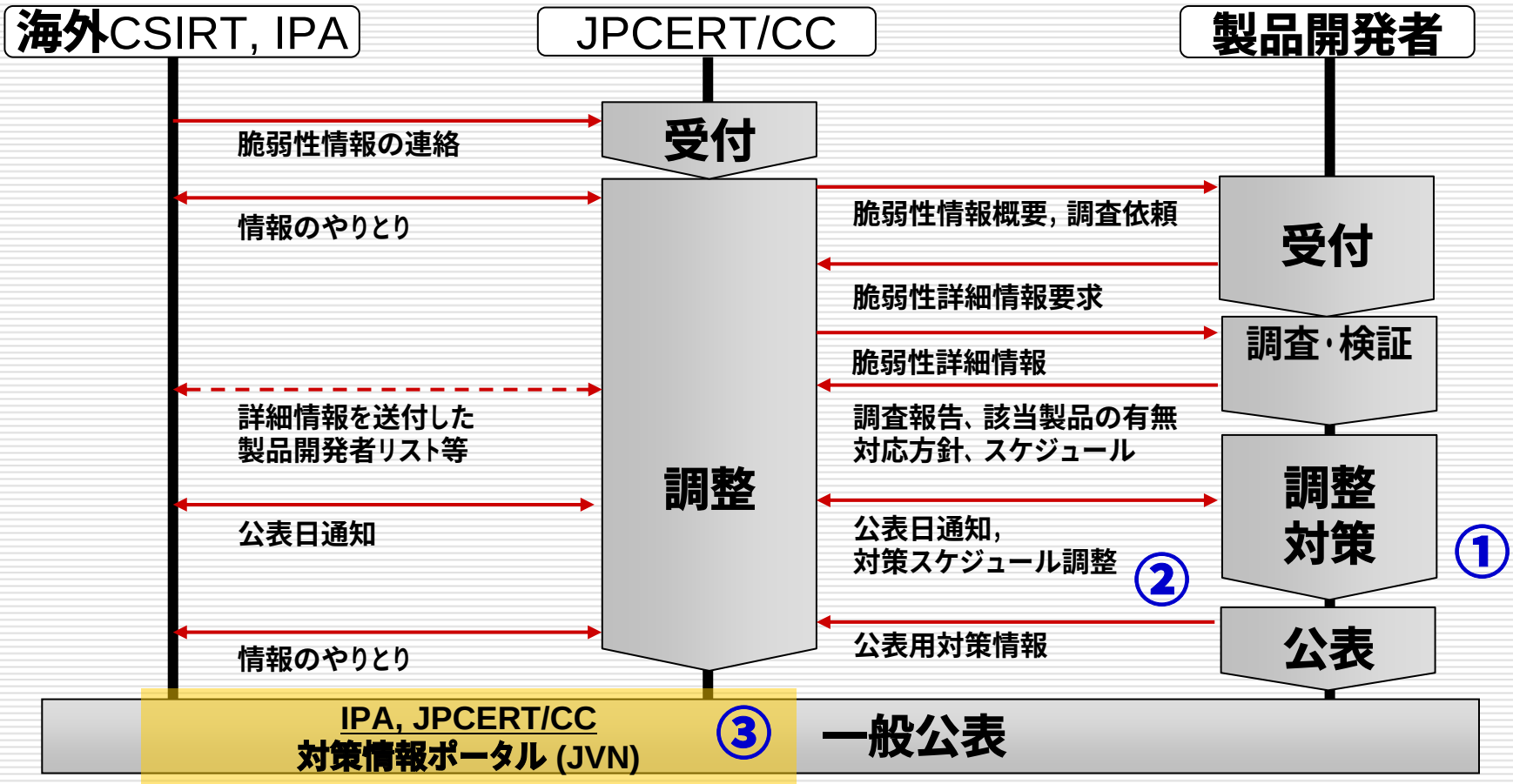
3. 対策情報流通体制について
JVN: JP Vendor Status Notesの位置付け

- 製品開発者の情報公表の支援
- システム導入支援者ならびにユーザへの対策情報提供



JPCERT CC

3. 対策情報流通体制について
製品開発者との脆弱性ハンドリングの概要



３．対策情報流通体制について
① 製品開発者における公表情報の作成

- 脆弱性に関して公表可能な情報がある場合には、一般公表日までに公表情報を作成
- 製品開発者が作成する公表情報の主な項目
  - 脆弱性に該当する製品名およびバージョン
  - 脆弱性の概要
  - 脆弱性への対応状況　⇒「製品開発者の対応状況(p10)」参照
  - 回避方法や修正方法などの対策方法
  - 関連情報へのリンク
  - 当該脆弱性情報に関する連絡先
  - 発見者への謝辞 (発見者が望んだ場合)

JPCERT CC

3. 対策情報流通体制について
① 製品開発者の対応状況

- 対応状況は下記の5項目の中から選択

表現方法	内容
該当製品あり	脆弱性該当製品がある場合
該当製品あり：調査中	脆弱性該当製品があり継続して調査を行っている場合
該当製品なし	脆弱性該当製品がない場合
該当製品なし：調査中	脆弱性該当製品は見つかっていないが、継続して調査を行っている場合
不明	脆弱性への対応状況の連絡がない場合

JPCERT CC

3．対策情報流通体制について
② 製品開発者からJPCERT/CCへの対応状況連絡

- 脆弱性の一般公表に向けて、製品開発者の対応状況をJPCERT/CCに連絡
- 主な連絡項目
  - JPCERT/CCが発行した識別番号
  - 製品開発者名称(会社名)
  - 製品の該当状況　⇒「製品開発者の対応状況(p10)」参照
  - 公表情報に記載するフリーフォーマットの文章

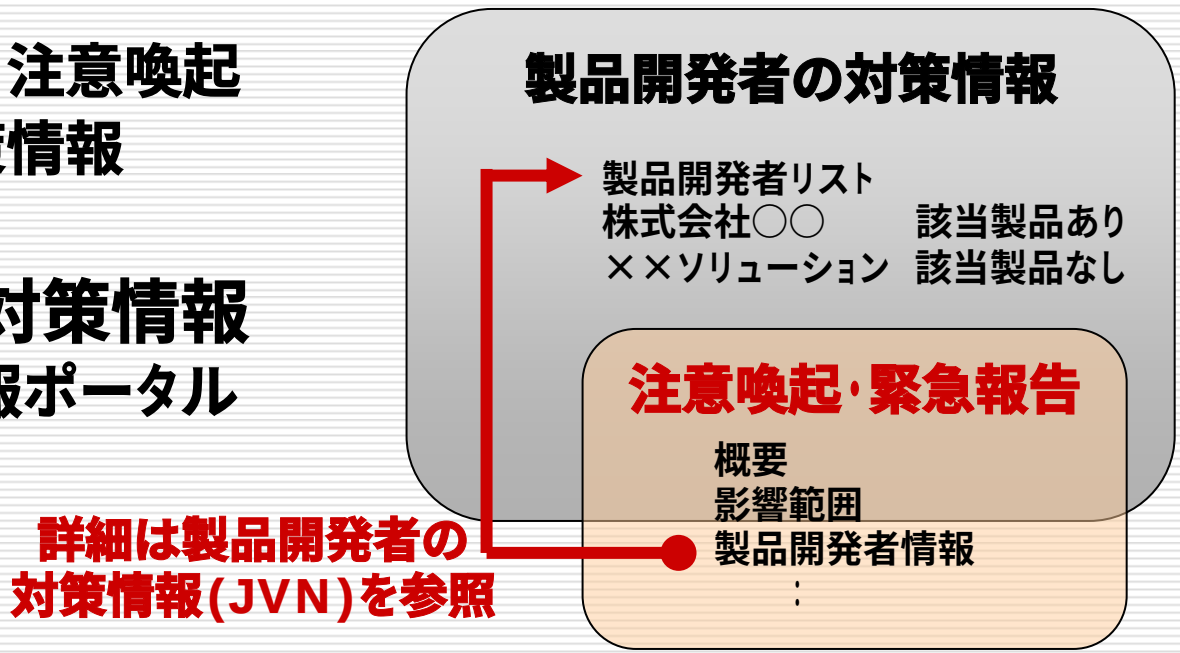
⇒JPCERT/CCでは製品開発者の対応状況を元に公表情報(③)を作成

JPCERT CC

3．対策情報流通体制について
③ 対策情報の発信形態

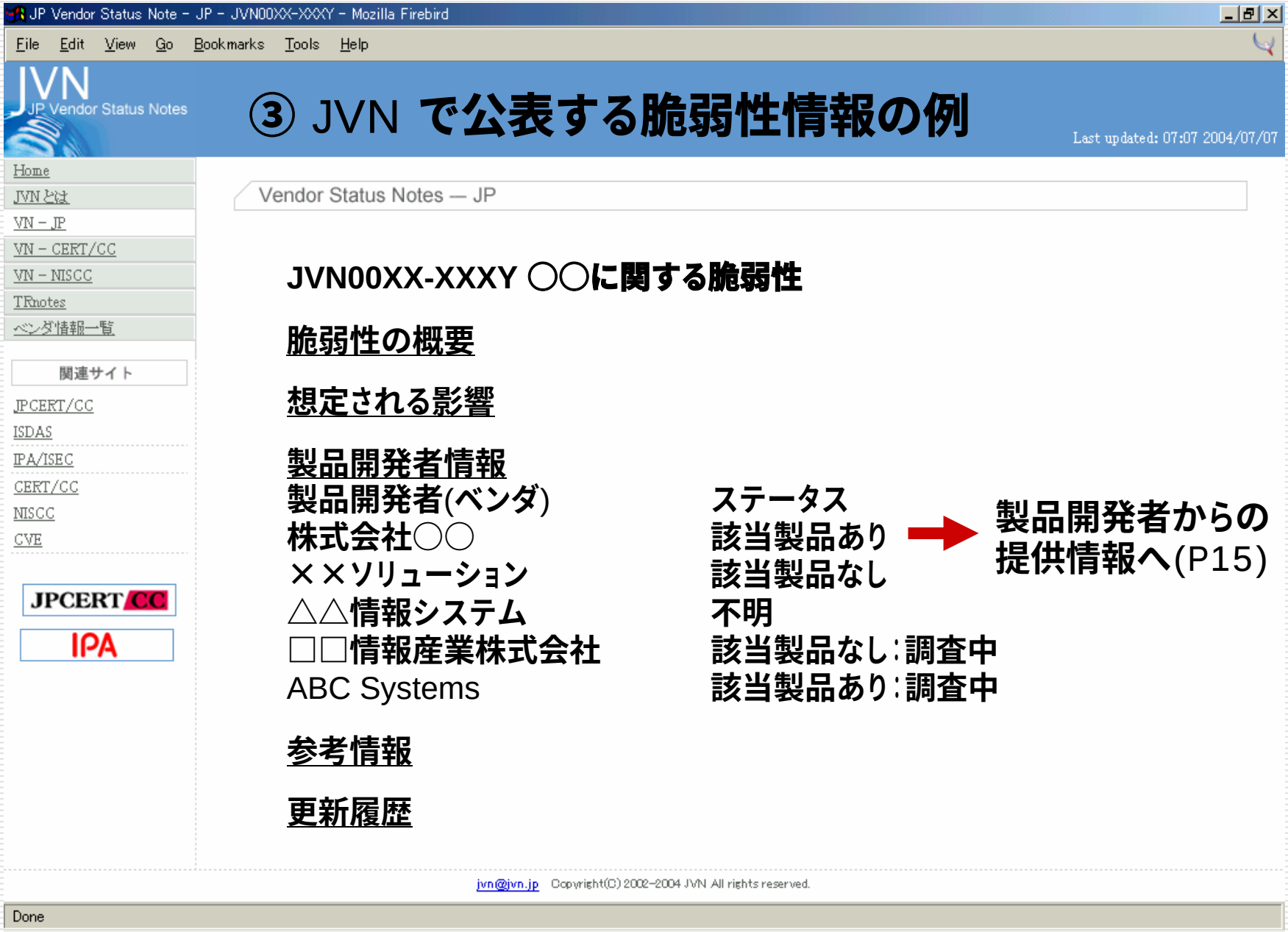
- **注意喚起ならびに緊急報告**
  「深刻且つ影響範囲の広い脆弱性に関する情報」「インシデント報告に基づき、同種のインシデントの発生を防止するための情報」
  - JPCERT/CC：**注意喚起**
  - IPA：**緊急対策情報**

- **製品開発者の対策情報**
  - JVN：**対策情報ポータル**
    http://jvn.jp/



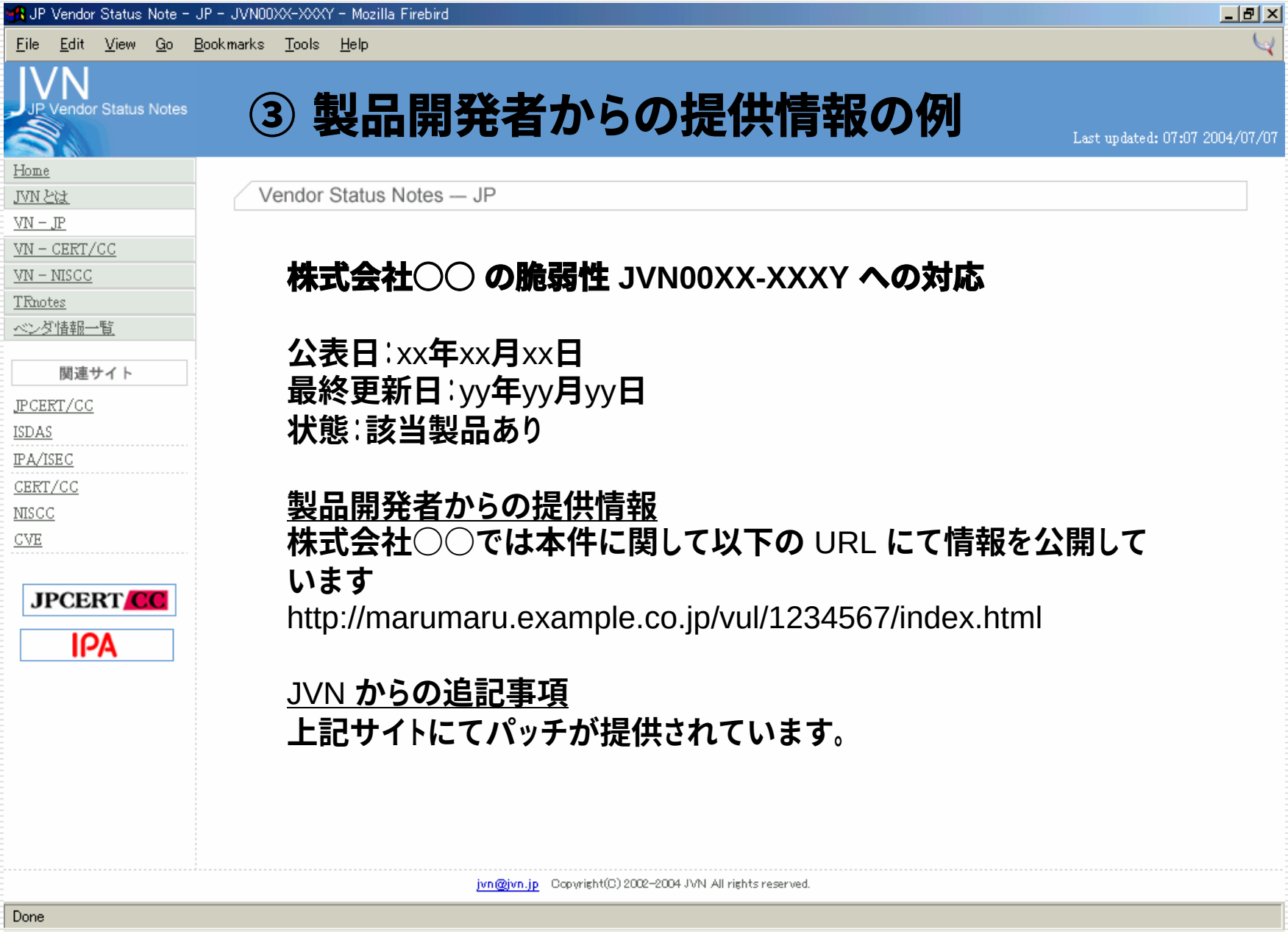
3. 対策情報流通体制について
③ JPCERT/CCにおける公表情報の作成と公表

- JPCERT/CCは、事前に設定された一般公表日時に、JVNを通じて脆弱性情報を一般に公表
- 脆弱性詳細情報を通知した全ての製品開発者をリストとして公表
- JPCERT/CCが作成する公表情報の主な項目
  - 脆弱性情報の概要
  - 脆弱性情報の影響範囲
  - 脆弱性情報に対する製品開発者の対応状況
  - 各製品開発者固有の情報



③ JVN で公表する脆弱性情報の例

JPCERT CC



③ 製品開発者からの提供情報の例

JPCERT CC

お問い合わせ先

- JPCERTコーディネーションセンター
  - Email：　office@jpcert.or.jp
  - Web：　http://www.jpcert.or.jp
  - Tel：　03-3518-4600