セキュリティインシデントおよびソフトウェア脆弱性の取り扱いとその課題

歌代 和正
(株)インターネットイニシアティブ
JPCERT コーディネーションセンター

JPCERT CC

JPCERT/CC概要

- Japan Computer Emergency Response Team Coordination Center
  - 緊急事態 (Emergency) への対応 (Response)
  - コンピュータセキュリティインシデントに関する調整、対応の協調、連携など
- 1996年10月設立
  - 1992年ころにボランティアではじまったグループを起源とする　エンジニア集団
  - 非営利目的、国からの予算で運営
- 2003年3月有限責任中間法人に
- 日本で最初に ('98) FIRST に加盟した CSIRT
  - 日本のPOC(窓口) CSIRTとして国際的に認知
- 2004年7月8日 経済産業省告示にて脆弱性情報流通調整機関として指定

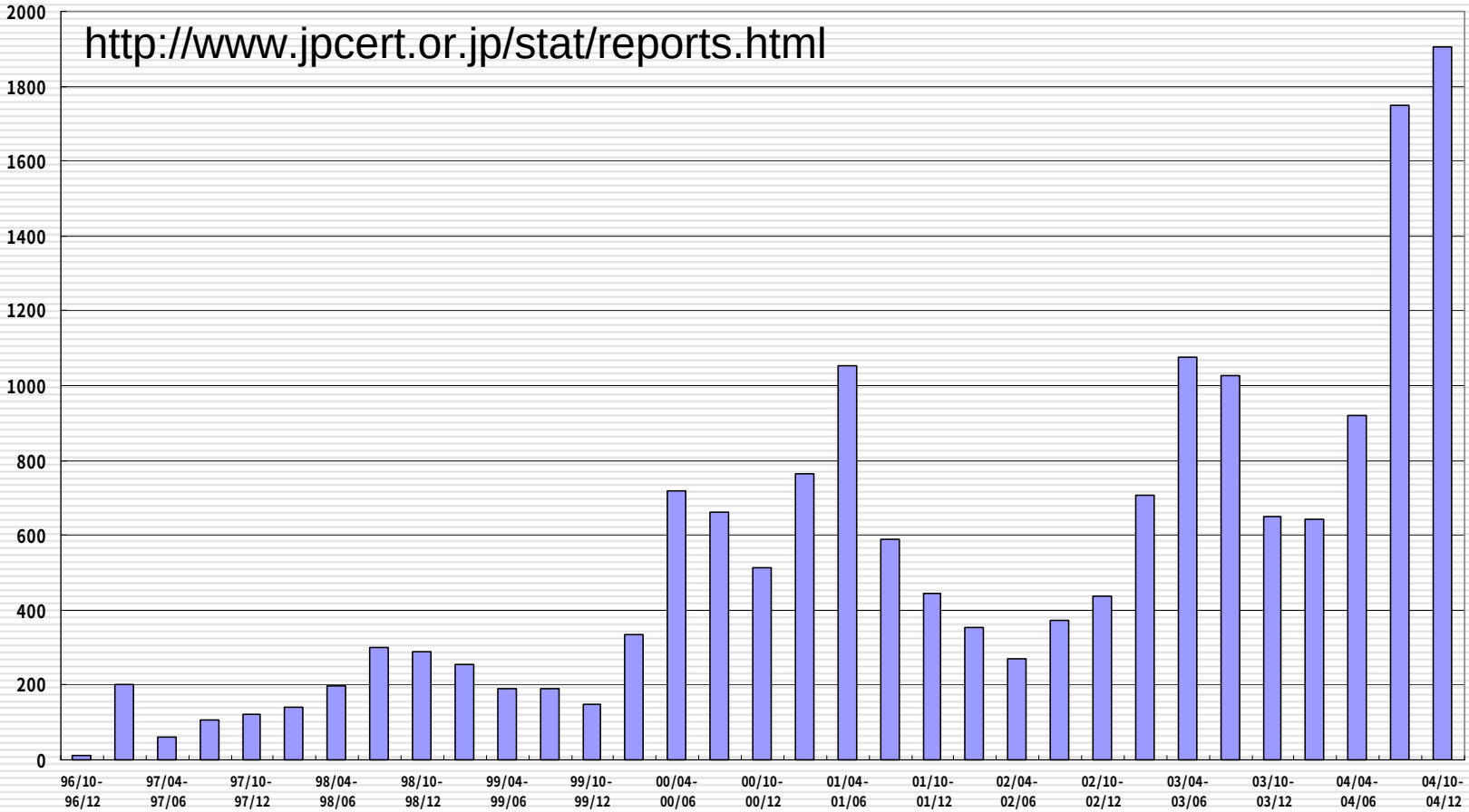
JPCERT CC

事後対応から事前対応に

JPCERT/CCの活動

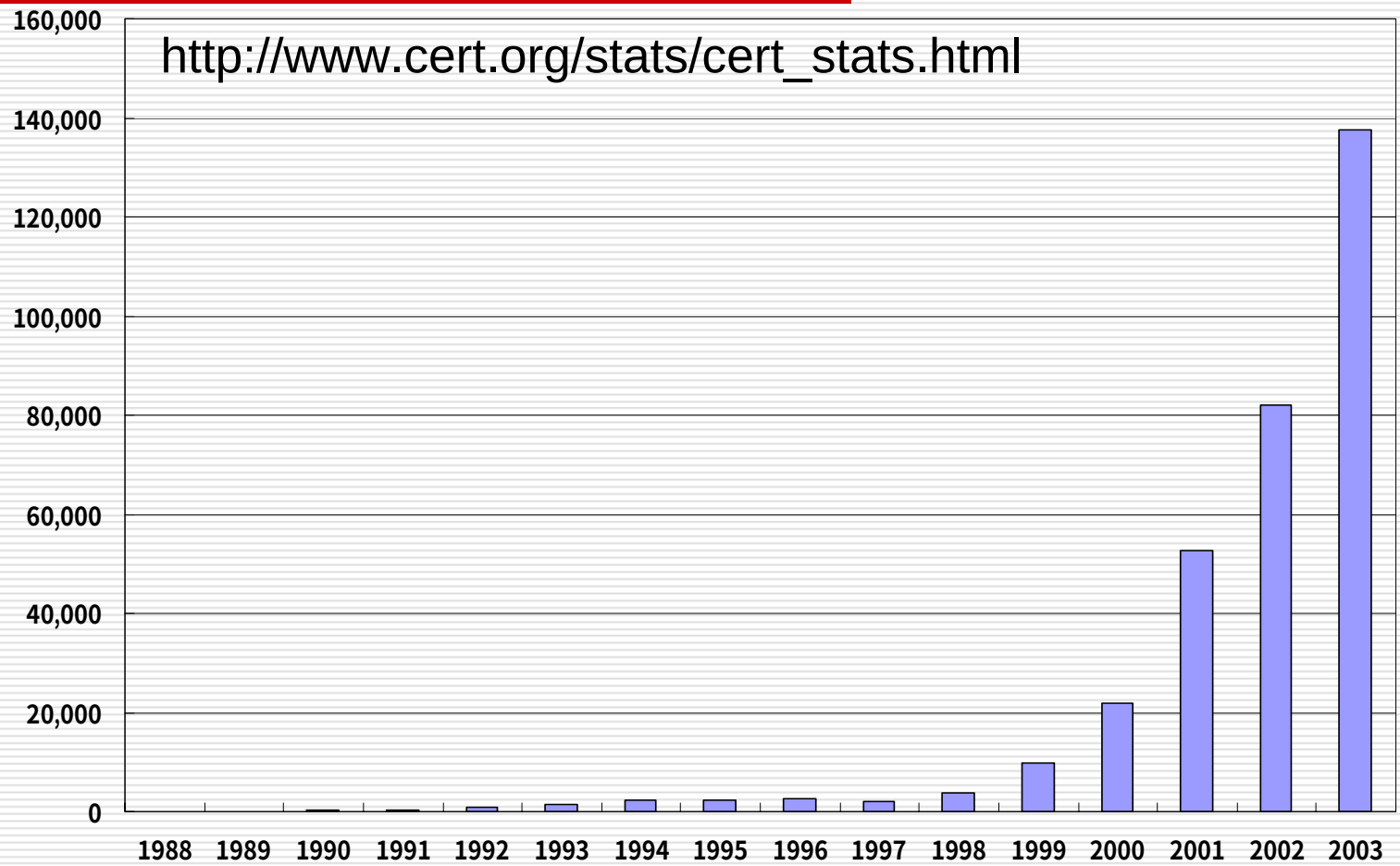
JPCERT CC

JPCERT/CC へのインシデント報告件数の推移



JPCERT CC

米国 CERT/CC へのインシデント報告件数の推移



JPCERT CC

脆弱性情報ハンドリング

JPCERT CC

ソフトウェア等脆弱性関連情報取扱基準

- 2003/11-2004/03
  IPA (**情報処理推進機構**) **主催の研究会**
- 2004/04-05
  パブリックコメント･･･募集
- 2004/07
  経済産業省告示
  情報セキュリティ早期警戒パートナーシップ運用開始
- **ソフトウェアとウェブアプリケーションに分けた届け出体制**

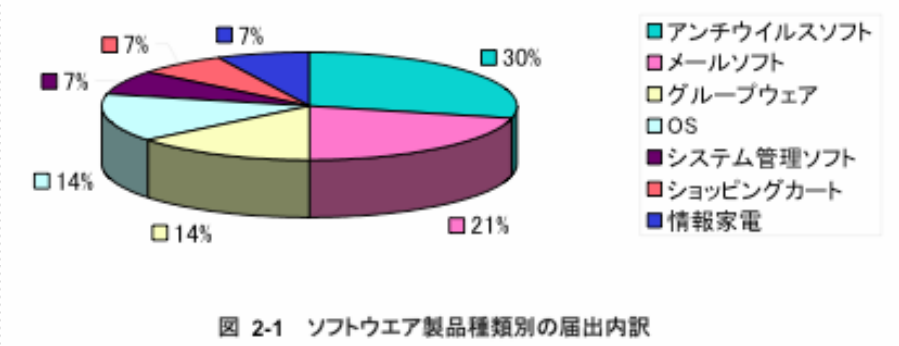


図 2-1 ソフトウエア製品種類別の届出内訳

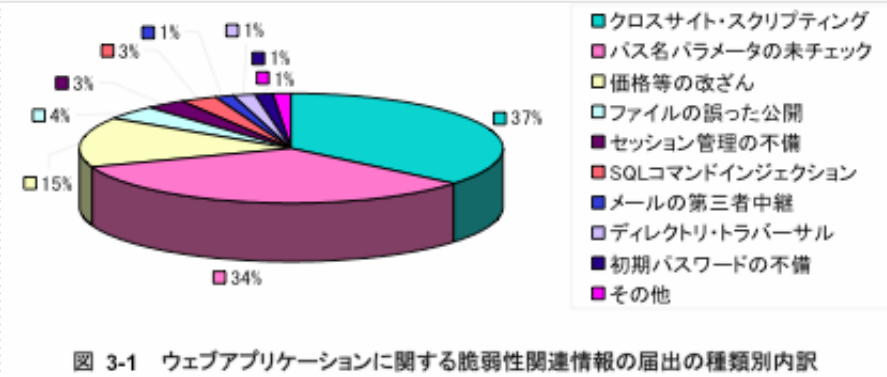


図 3-1 ウェブアプリケーションに関する脆弱性関連情報の届出の種類別内訳

2004**年第3四半期の届出状況**

JPCERT CC

脆弱性情報ハンドリング

- 脆弱性情報ハンドリングとは
  - 脆弱性関連情報を必要に応じて開示することで、脆弱性情報の　悪用、または障害を引き起こす危険性を最小限に食い止めるためのプロセスです。JPCERT/CCは、このプロセスの調整役(コーディネーター)として、影響のある製品を持つ製品開発者に脆弱性情報の連絡、対応を依頼します。
- 一般公開前の脆弱性情報を機密情報として扱いそれを製品開発者に伝えることで、製品の対策情報等を事前に作成してもらう
  - 取り扱う脆弱性情報
    - 特定の製品開発者の特定の製品に関わる脆弱性
    - 複数の製品開発者にまたがる、公開技術の根本的な問題による脆弱性
- 脆弱性情報の一般公開と同時に、対応策等も一般に公開されるようにするための仕組み

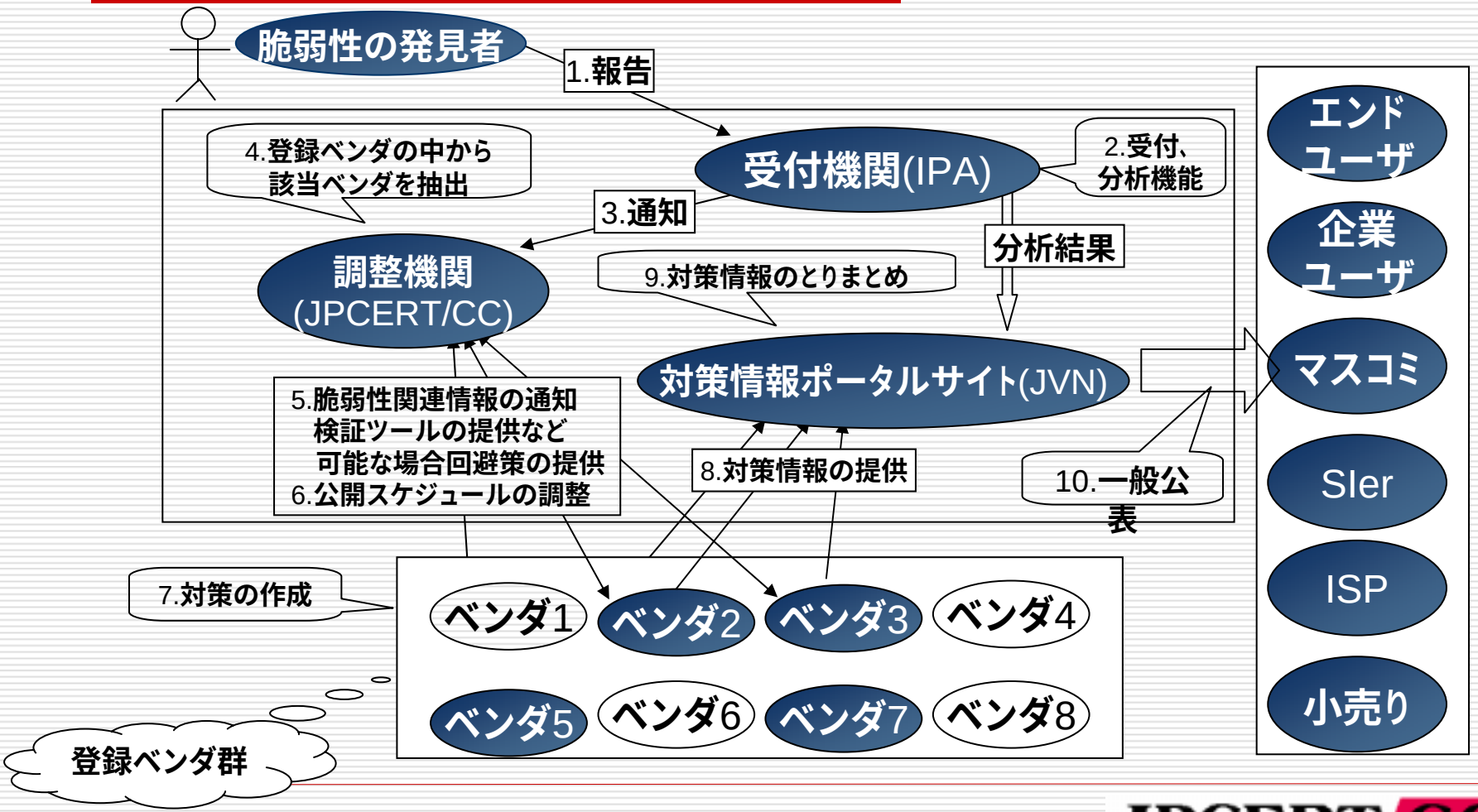
JPCERT CC

国際的な調整機関の必要性

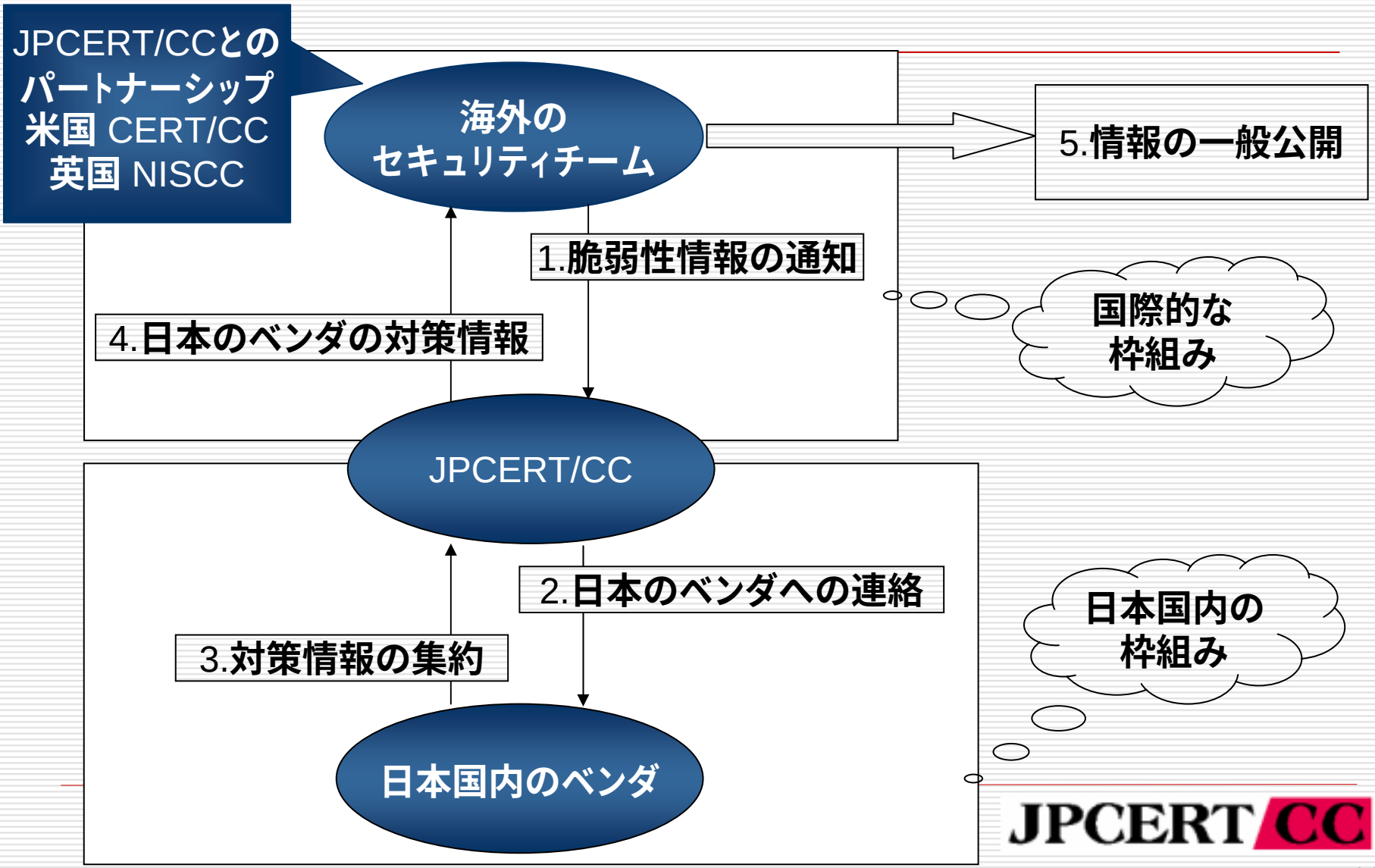
- 公表日一致の原則
  - 脆弱性情報と、製品開発者の対応状況は同時に公表
  - 影響が複数の製品開発者に及ぶ場合、特に同時公表のための、中立な第三者機関によるスケジュール調整が必要
- 製品開発者へのコンタクト
  - 影響のある製品を持つ製品開発者を、一社でも多く把握
    - 可能な限りの範囲への、公平な情報提供
    - 各組織内の、正しい連絡窓口の確保
      情報が適切かつ有効に使われる窓口の構築
- 発見者、製品開発者間の調整
  - 異なるモチベーションの調整
- 機密性の高い情報の、安全な取り扱い

JPCERT CC

国内体制での調整機関のポジション



国際的な枠組みについて



ベンダにとってのメリット

- 脆弱性関連情報を事前に入手することで、情報が公開されてから対応を始めるやりかたではなく、情報公開前から対応を始めることができる
- 上記理由によって、余裕のある対応ができる
- 脆弱性情報の一般公開と同時に対策情報を公開することで、ユーザへの影響を低減できる
- JPCERT/CCが各製品開発者の対応状況を考慮し、一般公開スケジュールを調整することが可能
- 脆弱性情報への対応状況を、ポータルサイトを通して、周知できる
  - http://jvn.jp

JPCERT CC

枠組みへの参加：
JPCERT/CC 製品開発者登録リストに登録

- JPCERT/CC 製品開発者登録リストとは
  - JPCERT/CCが、脆弱性情報を製品開発者に連絡する際、影響を受ける可能性のある製品開発者を特定するためのリスト
- 登録手順
  - 製品開発者はPOC仮登録情報を提出する
    - 製品開発者リスト仮登録申請様式
      http://www.jpcert.or.jp/form/poc.txt
  - JPCERT/CC から、POC本登録に必要な書類を提示する
  - 製品開発者はPOC本登録のための必要書類を作成し提出する
  - JPCERT/CCと製品開発者の間でミーティングを行う
  - JPCERTコーディネーションセンター製品開発者リスト登録規約への合意
  - 実際に登録をする

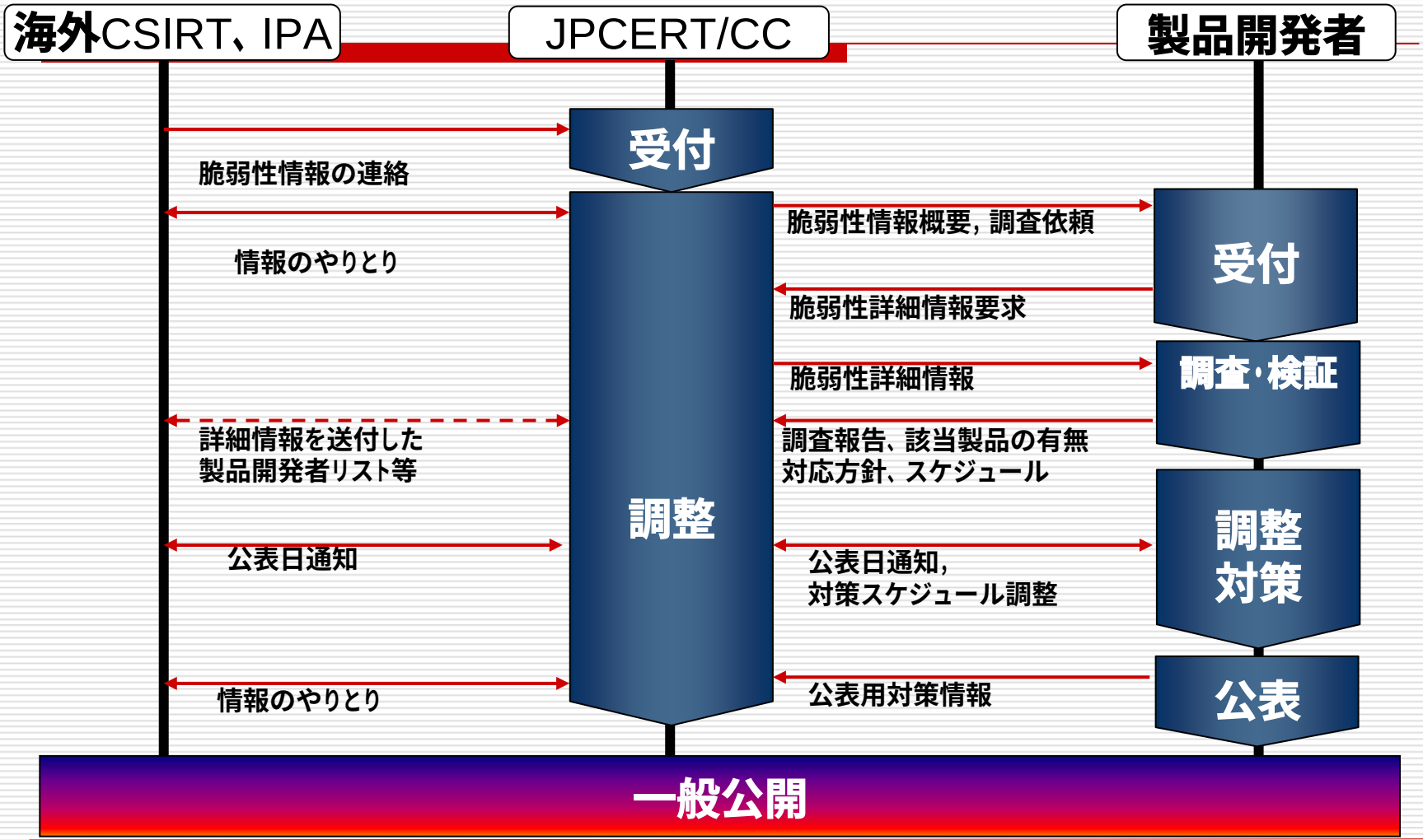
製品開発者の作業

- 社内体制の構築と窓口の登録
- 受付：脆弱性概要情報の取り扱い
- 検証：脆弱性詳細情報の取り扱いと製品の調査、JPCERT/CC への連絡
- 調整：公表日時の決定
- 対策：対策情報の作成
- 公表：対応状況の連絡と公表

脆弱性情報の公表

- 脆弱性情報を公表する理由
  - 汎用目的のソフトウェアの脆弱性は公開される必要がある
  - 悪意のある第3者が、脆弱性情報を発見し、対策情報なく公開してしまうケースを防ぐ
  - 管理者に、パッチの適用を動機付けさせる
  - 全ての安全性の懸念を認識しきれない
- 製品開発者支援
  - 製品開発者、研究者、関係者と調整し、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開をサポートする

JPCERT/CCと製品開発者のハンドリング(やり取り)概要図



JVN


JP Vendor Status Notes
http://jvn.jp/
Google
JVN
JP Vendor Status Notes
Last updated: 13:31
2004/11/30
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
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#7C9208F1: Becky! Internet Mail におけるS/MIME の署名検証に脆弱性 [2004/11/25 09:00]
JVN#B410A83F: Shuriken Pro3 のS/MIME機能で署名検証時にFromアドレスが確認されない [2004/11/22]
JVN#F88C2C13: desknet's に脆弱性(JVN#89DE2014の情報を追加) [2004/11/16]
Vendor Status Notes — CERT/CC
INDEX
JVNTA04-315A: Microsoft Internet Explorerにバッファオーバーフロー [2004/11/28 14:02]
JVNVU#457622: Samba QFILEPATHINFO 処理にバッファオーバーフロー [2004/11/28 14:02]
JVNVU#557062: CUPS にてユーザアカウント情報がログファイルに平文で保存される [2004/11/22]
Vendor Status Notes — NISCC
INDEX
NISCC-380375: MIME に関する複数の脆弱性 [2004/11/30 14:00]
NISCC-190204: Timbuktu for Mac OS X における脆弱性 [2004/11/25 10:00]
NISCC-841713: Hummingbird 製品に関する脆弱性 [2004/11/12]
Status Tracking Notes
INDEX
メニューを表示

脆弱性ハンドリングにおける問題点

JPCERT CC

キーワードの整備

- 現在は、37の登録キーワードにしたがって、脆弱性の概要情報を送付している
- 問題点
  - キーワードが未整備なため、正確さにかける
  - 不要な情報を送付→情報漏洩の危険も
- ‥対応
  - CERT/CC の脆弱性 629件を基にキーワードを分析中

ベンダーキーワード TOP 20

	keyword (Vendor 情報)	該当件数	累積件数 (累積度数)	構成比率 (相対度数)	累積比率 (累積相対度数)	脆弱性(629 件)に対する構成比率	脆弱性(629 件)に占める累積比率
1	Microsoft	194	194	43.89%	43.89%	30.84%	30.84%
2	Cisco	35	229	7.92%	51.81%	5.56%	36.41%
3	Oracle	34	263	7.69%	59.50%	5.41%	41.81%
4	IBM	23	286	5.20%	64.71%	3.66%	45.47%
5	Sun	23	309	5.20%	69.91%	3.66%	49.13%
6	Hewlett Packard	17	326	3.85%	73.76%	2.70%	51.83%
7	Apple	9	335	2.04%	75.79%	1.43%	53.26%
8	SGI	8	343	1.81%	77.60%	1.27%	54.53%
9	Symantec	7	350	1.58%	79.19%	1.11%	55.64%
10	Real Networks	7	357	1.58%	80.77%	1.11%	56.76%
11	CheckPoint	5	362	1.13%	81.90%	0.79%	57.55%
12	Yahoo	5	367	1.13%	83.03%	0.79%	58.35%
13	Gaim	4	371	0.90%	83.94%	0.64%	58.98%
14	IPSWITCH	4	375	0.90%	84.84%	0.64%	59.62%
15	Alcatel	4	379	0.90%	85.75%	0.64%	60.25%
16	Network Associates	4	383	0.90%	86.65%	0.64%	60.89%
17	AOL	4	387	0.90%	87.56%	0.64%	61.53%
18	phpBB	3	390	0.68%	88.24%	0.48%	62.00%
19	Trend Micro	3	393	0.68%	88.91%	0.48%	62.48%
20	Macromedia	2	395	0.45%	89.37%	0.32%	62.80%

JPCERT CC

アプリケーションキーワード TOP 20

No	Keyword	該当件数	累積件数 (累積度数)	構成比率 (相対度数)	累積比率 (累積相対度数)
1	Windows	69	69	8.88%	8.88%
2	Internet Explorer	47	116	6.05%	14.93%
3	IIS	24	140	3.09%	18.02%
4	IOS	21	161	2.70%	20.72%
5	Solaris	18	179	2.32%	23.04%
6	Oracle Application Server	16	195	2.06%	25.10%
7	BIND	15	210	1.93%	27.03%
8	SQL Server/MSDE	14	224	1.80%	28.83%
9	Oracle Database Server	14	238	1.80%	30.63%
10	Instant Messenger	14	252	1.80%	32.43%
11	Lotus Domino/Notes	13	265	1.67%	34.11%
12	Kerberos	13	278	1.67%	35.78%
13	SNMP	10	288	1.29%	37.07%
14	FTP	9	297	1.16%	38.22%
15	OpenSSL	8	305	1.03%	39.25%
16	OpenSSH	8	313	1.03%	40.28%
17	Mozilla	8	321	1.03%	41.31%
18	IRIX	8	329	1.03%	42.34%
19	ActiveX	8	337	1.03%	43.37%
20	Windows 2000	7	344	0.90%	44.27%

JPCERT CC

その他のキーワード

- Server Service
- Network Protocol
- Web browser
- Web service
- Email service
- RPC service
- Utility
- RPC service
- Programming
- Library

JPCERT CC

その他の問題点

- 脆弱性情報の漏洩
  - 単一ベンダのフライング
  - 国際的な脆弱性の場合さらに難しい
- 定期的パッチによる調整困難
  - 月例パッチの衝突
- ベンダの知識不足
  - 根本的解決にならない場合も
- 開発者とベンダの意識差
  - 発見者：誇張気味、ベンダ：控えめ

ネットワーク家電における脆弱性

JPCERT CC

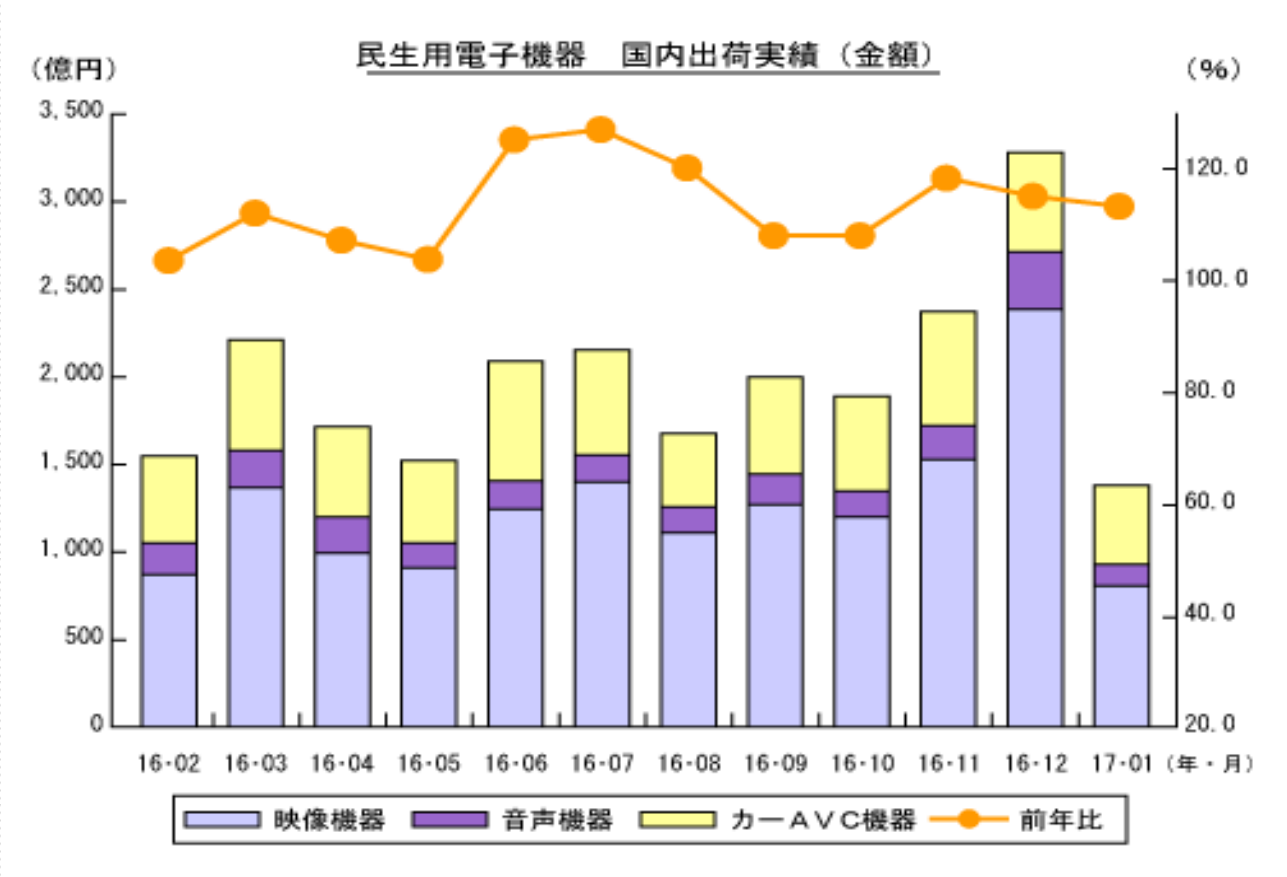
Index

- ネットワーク家電の全体動向
  - 市場動向
  - 業界構造
  - 技術概要
- ネットワーク家電に係わる脆弱性の動向
- ネットワーク家電に対する消費者の意識
- ネットワーク家電市場の拡大と発展のために
- 脆弱性克服のための具体的方策

JPCERT CC

1. ネットワーク家電の全体動向

情報家電市場の全体動向

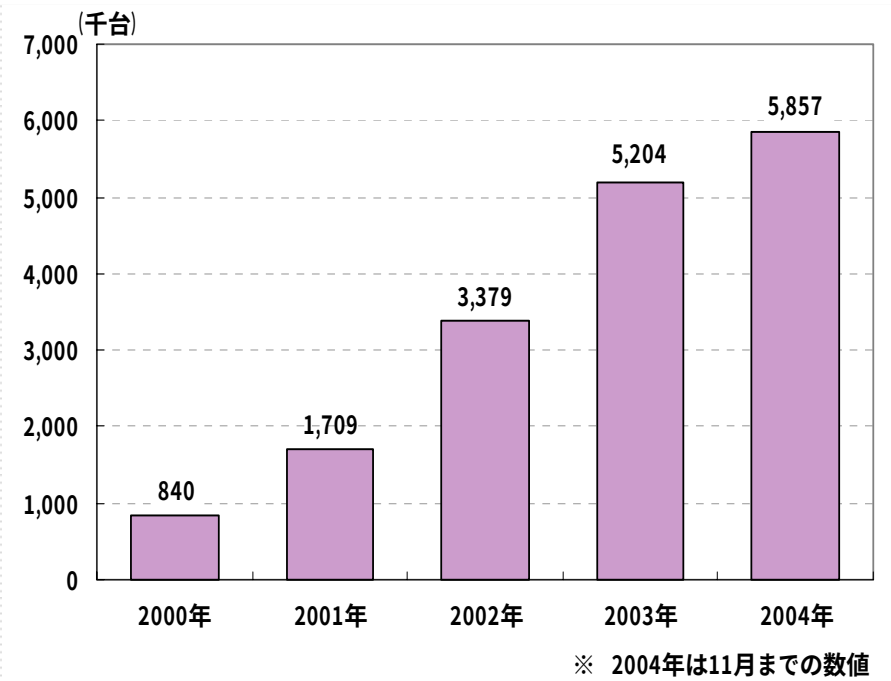


情報家電を含む民生用電子機器は対前年比14ヶ月連続でプラス成長している　　出展：JEITA

JPCERT CC

DVD Player/Recorderにおける製品市場

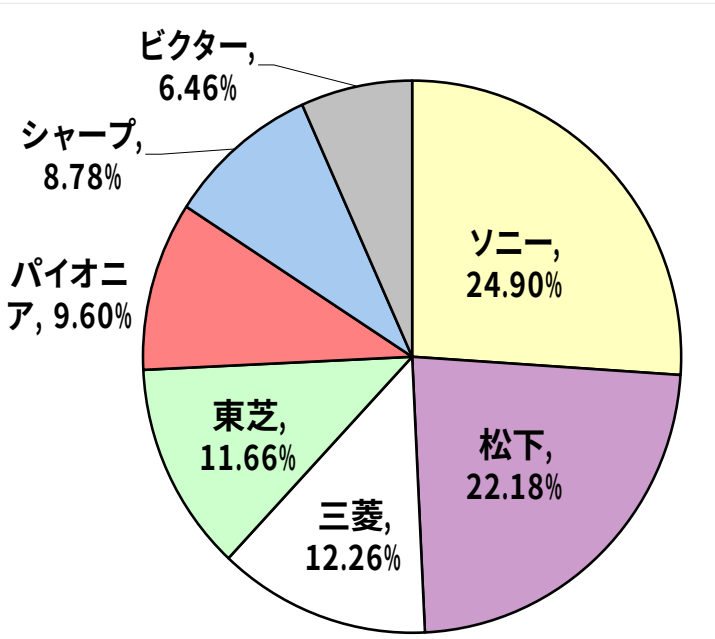
【市場規模（国内出荷台数）】



資料：JEITA

【参入事業者の動向】

DVD録画再生機のベンダ別全国販売シェア
（数量・2004年10月次）



資料：BCN総研

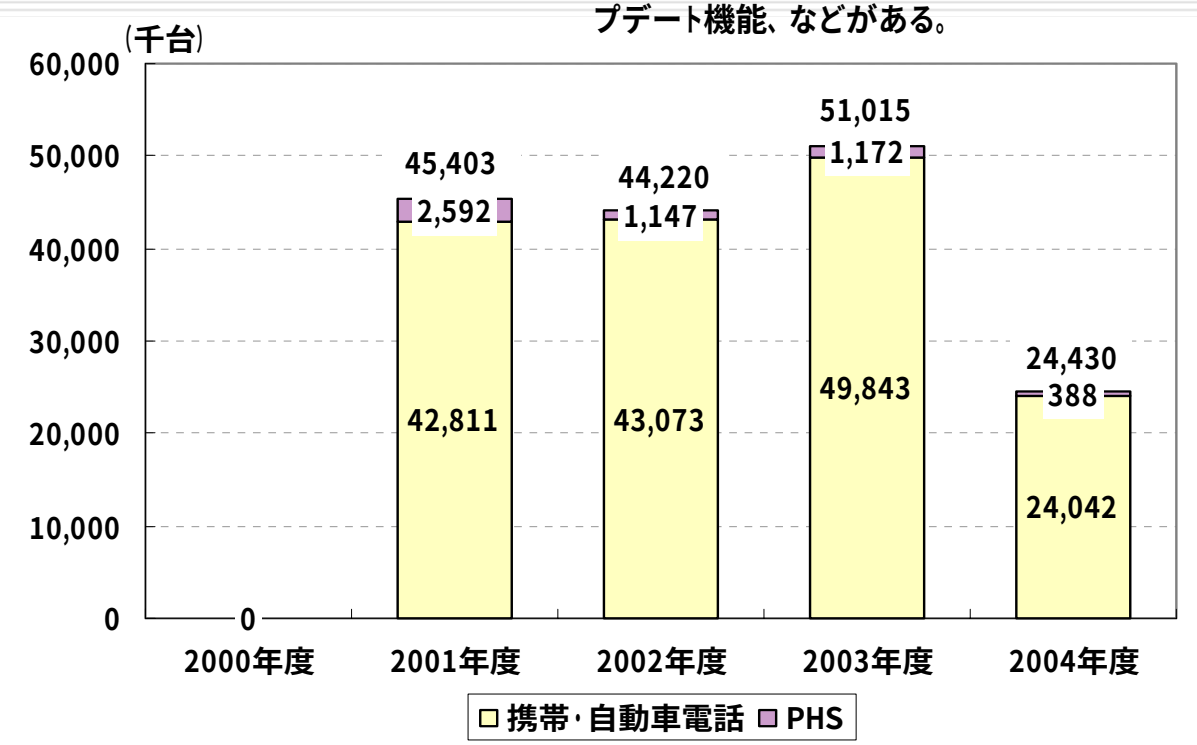
- DVD/HDD Player/Recorderにおける主なネットワーク機能は、電子番組表（iEPG等）、AVサーバ機能、外出先からの番組予約機能、ネットワークを介したファームウェアアップデート機能、などがある。

JPCERT CC

携帯電話における製品市場動向

[市場規模（国内出荷台数）]

•携帯電話における主なネットワーク機能は、WEBブラウザ、電子メール、Javaアプリ等により実現される機能、通信網を介したファームウェアアップデート機能、などがある。



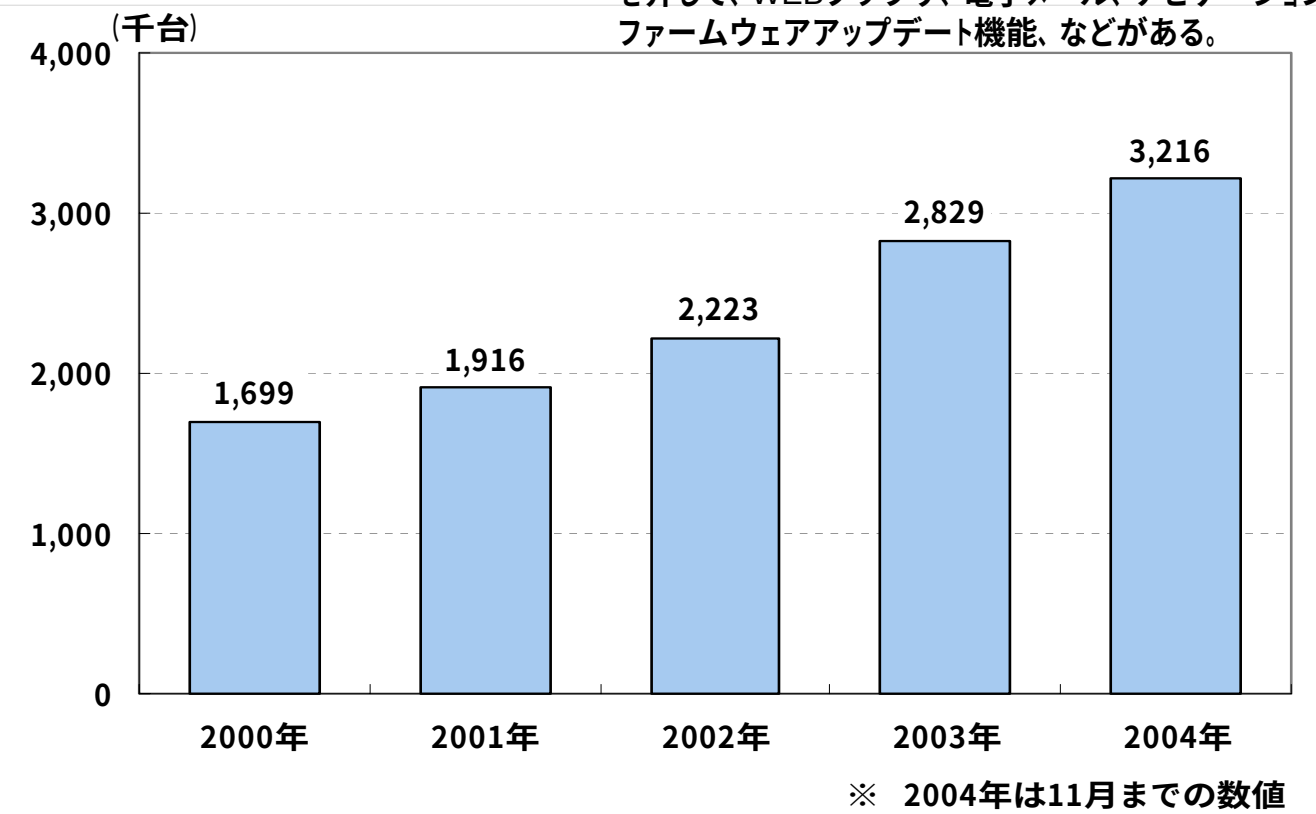
※　2004年度は10月までの数値

資料：JEITA

JPCERT CC

カーナビゲーションシステムにおける市場動向

[市場規模（国内出荷台数）]



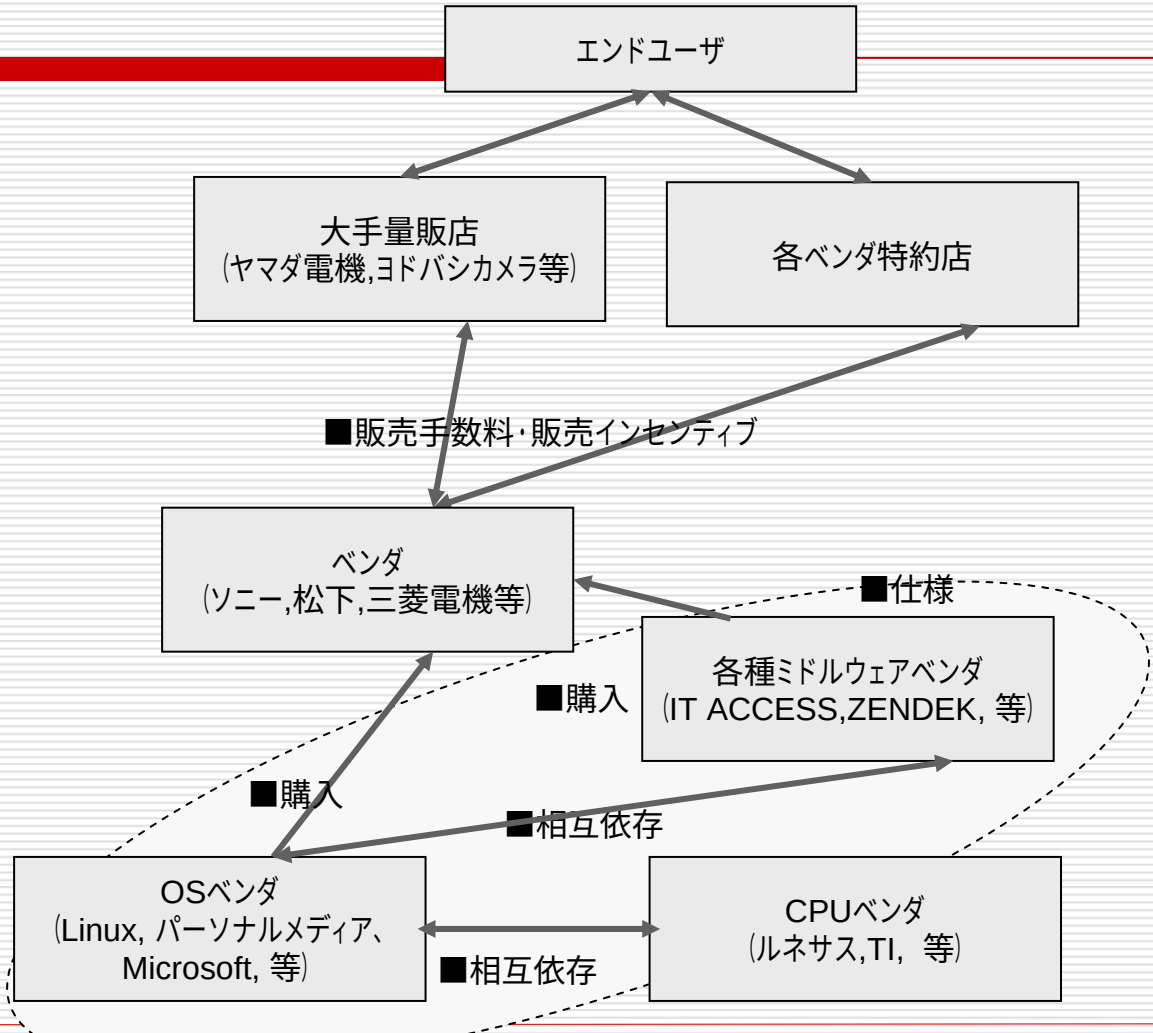
※　2004年は11月までの数値

資料：JEITA

•カーナビゲーションシステムにおける主なネットワーク機能は、携帯電話を介して、WEBブラウザ、電子メール、ナビゲーションデータの送受信、ファームウェアアップデート機能、などがある。

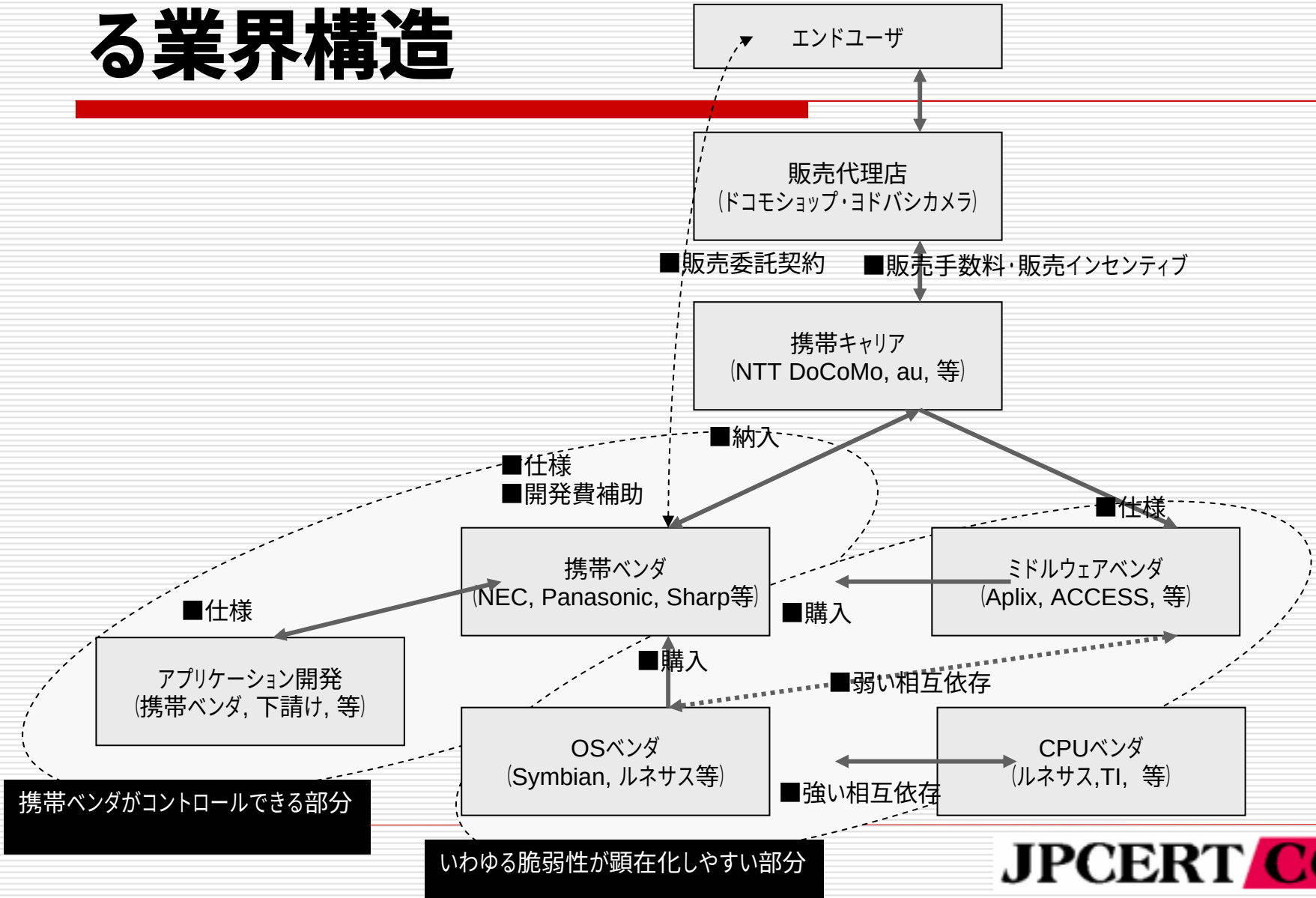
JPCERT CC

DVDプレイヤに代表されるAV系家電のソフトウェアに係わる業界構造



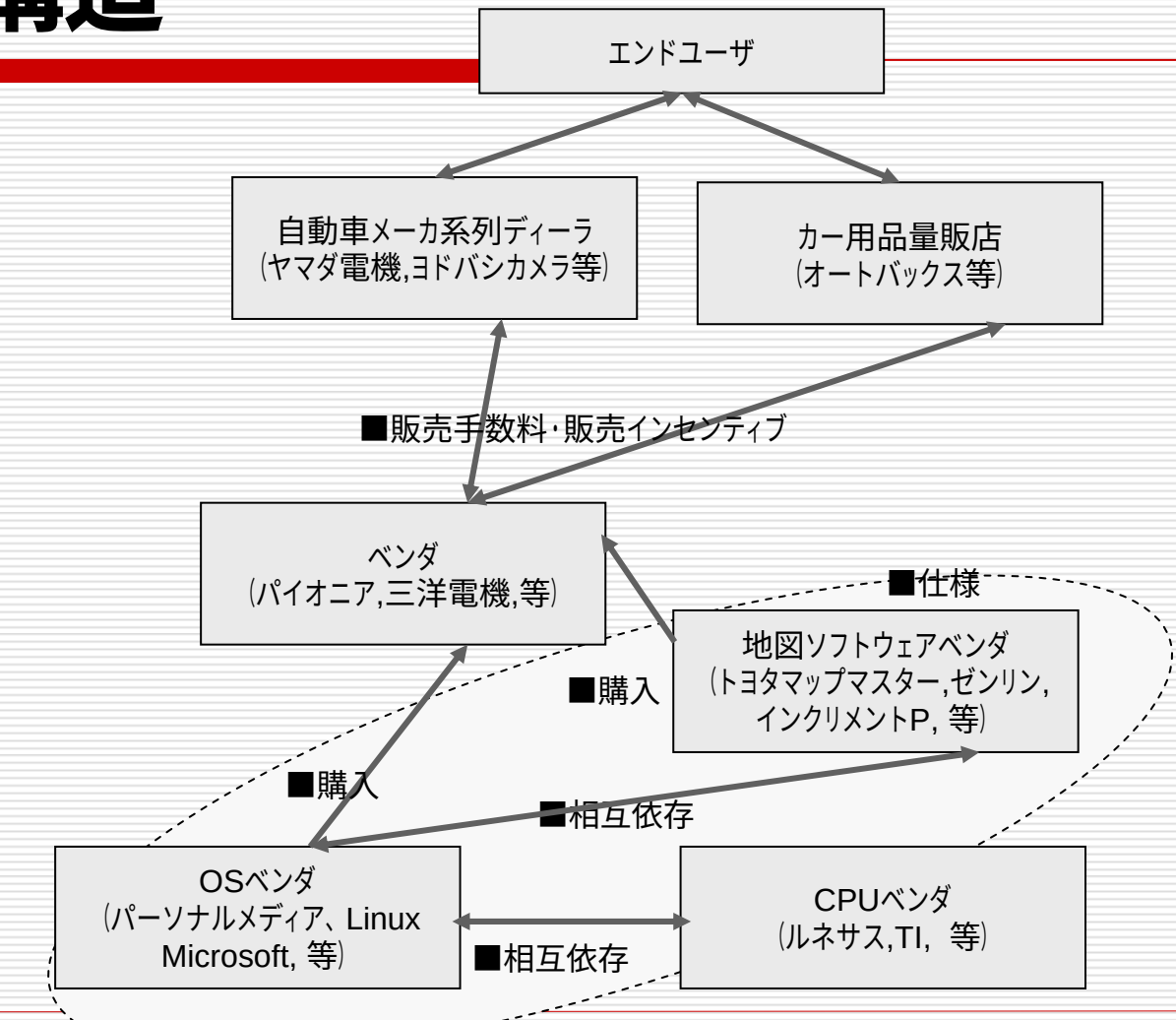
JPCERT CC

携帯電話におけるソフトウェアに係わる業界構造



JPCERT CC

カーナビにおけるソフトウェアに係わる業界構造



JPCERT CC

技術動向
情報家電の技術的アーキテクチャ

Application	アプリケーション	
Streaming	**Windows Media Player, Real Player**, EMMS, Open MG X	
Digital Rights Management Content Protection	WM-DRM, Helix DRM, EMMS, UDAC-MB, OpenMG/Magic gate ShellRights	
Media Transports	Image: **JPEG, GIF, TIFF, PNG** Music: AAC, MP3, TwinVQ, LPCM, WMA Video: MPEG-1/2/4/7, H.264, DivX, WMV	MPEG-21 ATRAC3
Media Transports	HTTP	
Appliance Control	ECHONET, HAVi	
Device Discovery and Control	UPnP Arch v1	
Network Protocol	**IPv6**	
Physical Network	電灯線, 特定省電力無線, IrDA, Bluetooth, Ethernet, Wired802.3u, **Wireless 802.11 a/b/g**, IEEE1394	
OS	**Linux**, ITRON, VxWorks, **Windows**	
Device Driver	デバイスドライバ	
CPU	CPU	
LSI/Device	I/F LSI	センサー

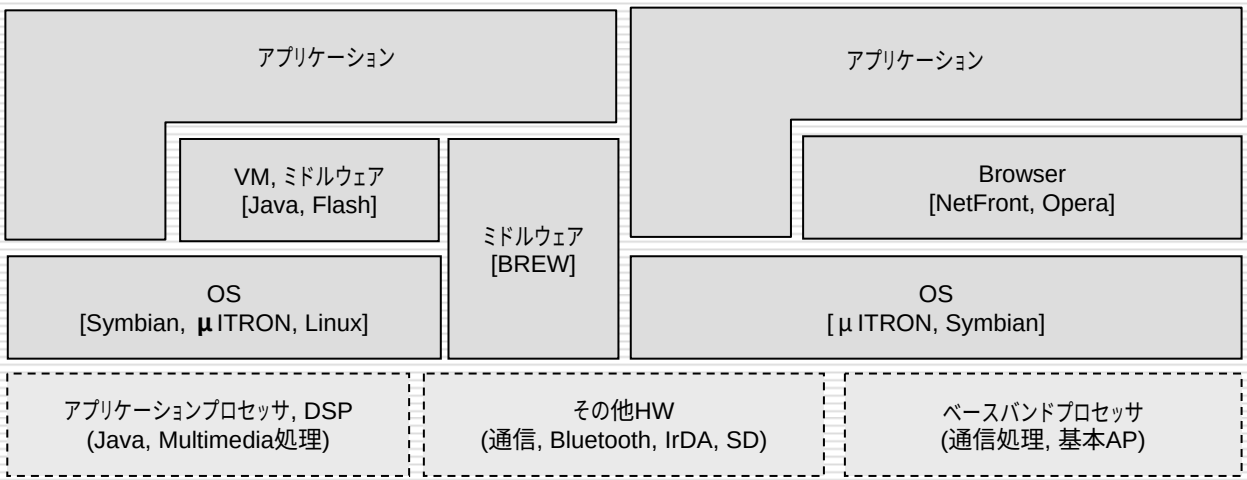
経済産業省資料より

JPCERT CC

技術動向
携帯電話

主要ソフトウェアコンポーネント

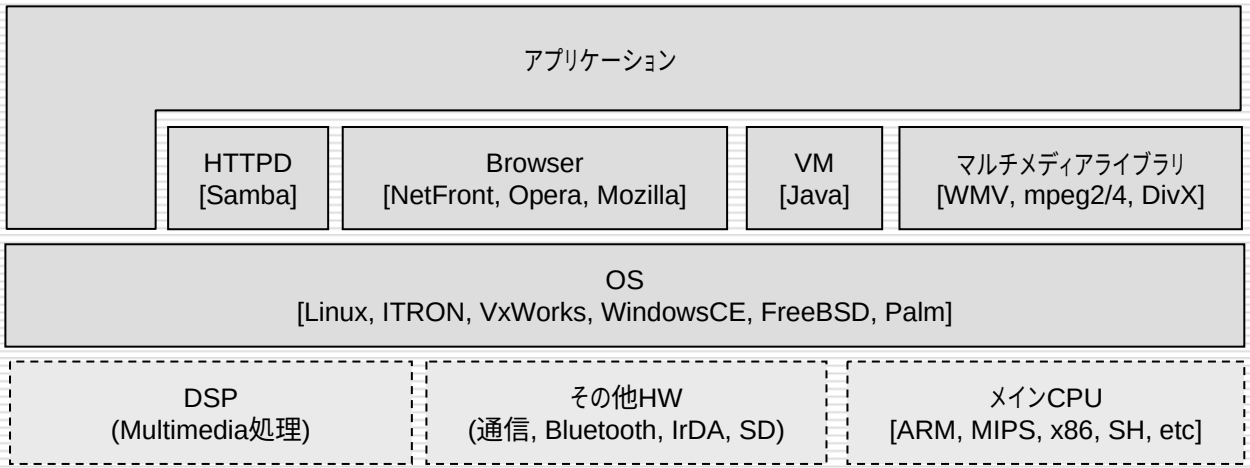
OS	Linux: montavista, CELF* ITRON: **パーソナルメディア** Symbian: Symbian PalmOS: PalmSource (**海外の携帯**) Windows Mobile: Microsoft
ミドルウェア	Flash: Macromedia Java: Aplix JBlend, Sun MIDP* BREW: QUALCOMM
ブラウザ	NetFront: ACCESS Opera: OPERA Software



技術動向
ネット家電・AV家電

主要ソフトウェアコンポーネント

OS	Linux: montavista, CELF* ITRON: **パーソナルメディア**, **ルネサス**, NEC, T-Engine* VxWorks: WIND RIVER Windows Embedded/CE: Microsoft PalmOS: PalmSource FreeBSD
ミドルウェア	Java: Sun , Aplix JBlend, ACCESS JV-Lite
マルチメディア	Windows Media Video: Microsoft
ブラウザ	NetFront: ACCESS Opera: OPERA Software Mozilla: Mozilla



JVN
JP Vendor Status Notes

Last updated: 16:00 2004/11/04

Vendor Status Notes — CERT/CC

JVNTA04-217A

libpng に複数の脆弱性

概要

PNG (Portable Network Graphics) 形式の画像処理ライブラリ libpng のバージョン 1.2.5 およびそれ以前には、バッファオーバーフローなど複数の脆弱性があります。この脆弱性は、脆弱な libpng ライブラリを使用しているプログラムの実装にも影響を与えます。

影響を受けるシステム
- libpng 1.2.5 ならびにそれ以前
- libpng ライブラリを使用しているアプリケーションならびにシステム

想定される影響

遠隔から第三者が、PNG 形式の画像ファイルを経由して、libpng を使用したアプリケーションを実行しているユーザの権限を取得する可能性があります。
なお、PNG 形式の画像ファイルは、Web ページや HTML 形式の電子メールに含まれている場合があります。

ネットワーク家電に係わる脆弱性の動向

JPCERT CC

ネットワーク家電における脆弱性のリスト：

2000年前後	タグメールと呼ばれるメールを送付することで、送付先携帯を操作できる問題	NTTドコモ の特定機種に採用されていたアクセス社製ブラウザに、制御用のHTMLタグを解釈する機能があり、これを利用することで、メールを開くだけで強制的に指定した先にメールを送信したり、電話を発信させることができる問題点が存在した。
NA	携帯電話をフリーズさせたり、暗証番号をクリアするコマンドが存在する問題	J-Phone (当時) のシャープ製携帯である特定のキー操作を行うことで、当該携帯がフリーズする問題点が存在した。同様の問題はauの東芝製携帯や松下製H"携帯端末にも存在する。
2003年8月	Windowsの脆弱性 (MS03-026) を悪用したウイルスの蔓延によるWindowsベース家電製品への影響 (国内)	PCだけでなくWindows NT 4.0/Windows 2000/XPベースのOSあるいは組込み専用OSを採用している家電製品やOA製品にも脆弱性が存在し、同Blasterウイルスへの感染の可能性があった。富士ゼロックスにおいては同社製品のコピー機等についての対策方法を公表した。
2003年11月報告 2004年7月に実証 等	携帯電話のBluetooth機能の脆弱性 (海外)	Bluetooth対応携帯電話の脆弱性をついて、アドレス帳、カレンダー予定表、メールメッセージ等を入手すること、メモリに偽のテキストメッセージを埋め込むこと、携帯を盗聴器に変え音声を拾うことが可能であることが実証された。これらの攻撃の大半の形跡を残さずに実行できる。
2004年10月	HDD＆DVDビデオレコーダへ認証なしでアクセス可能 (国内)	出荷時の設定では認証無しで同製品にアクセスが可能である。同製品にはHTTPプロキシサーバが実装されているため、インターネット接続を行い外部ネットワークから利用している場合に、第三者にコメントスパムの踏み台等に悪用される可能性がある。
2004年10月	携帯電話Javaに2件の脆弱性 (海外)	Java Bytecode Verifierの脆弱性。ユーザが悪質なJavaプログラムをダウンロードし実行した場合に、データの送信、メモリの消去、ネットへの接続等を行われる可能性がある。8月に発見者より通知を受けたSunは、Javaライセンス保有者に対し2週間以内に修正パッチを配布した。
2004年11月～12月	シンビアンOS搭載携帯電話アプリを破壊するプログラム (海外)	Skullsプログラム、METAL Gearプログラム。ユーザがそれと知らずに悪意あるプログラムをダウンロードしてインストールしてしまうと、不具合が起きる (トロイの木馬)。

JPCERT CC

脆弱性の事例1：
A社製 HDD＆DVDビデオレコーダへ認証なしでアクセス可能

■経緯

2004年9月中旬	報告者の個人のブログに大量の悪意ある書き込み（コメントスパム）が送りつけられ、この送信がオープンプロキシを用いたものであった旨が掲載された。
2004年9月22日	報告者よりIPAに報告者より同脆弱性に関する届出が行われ受理された。
2004年9月24日	大手IT関連ニュースサイトに、同問題に関するA社への取材に基づく記事が掲載された。
2004年10月4日	A社より「重要なお知らせ：セキュリティ設定のお願い」が発表された。
2004年10月15日	JVN に 脆弱性情報JVN#E7DDE712 として掲載された。

■脆弱性の概要

出荷時の設定では認証無しで同製品にアクセスが可能である。

■影響

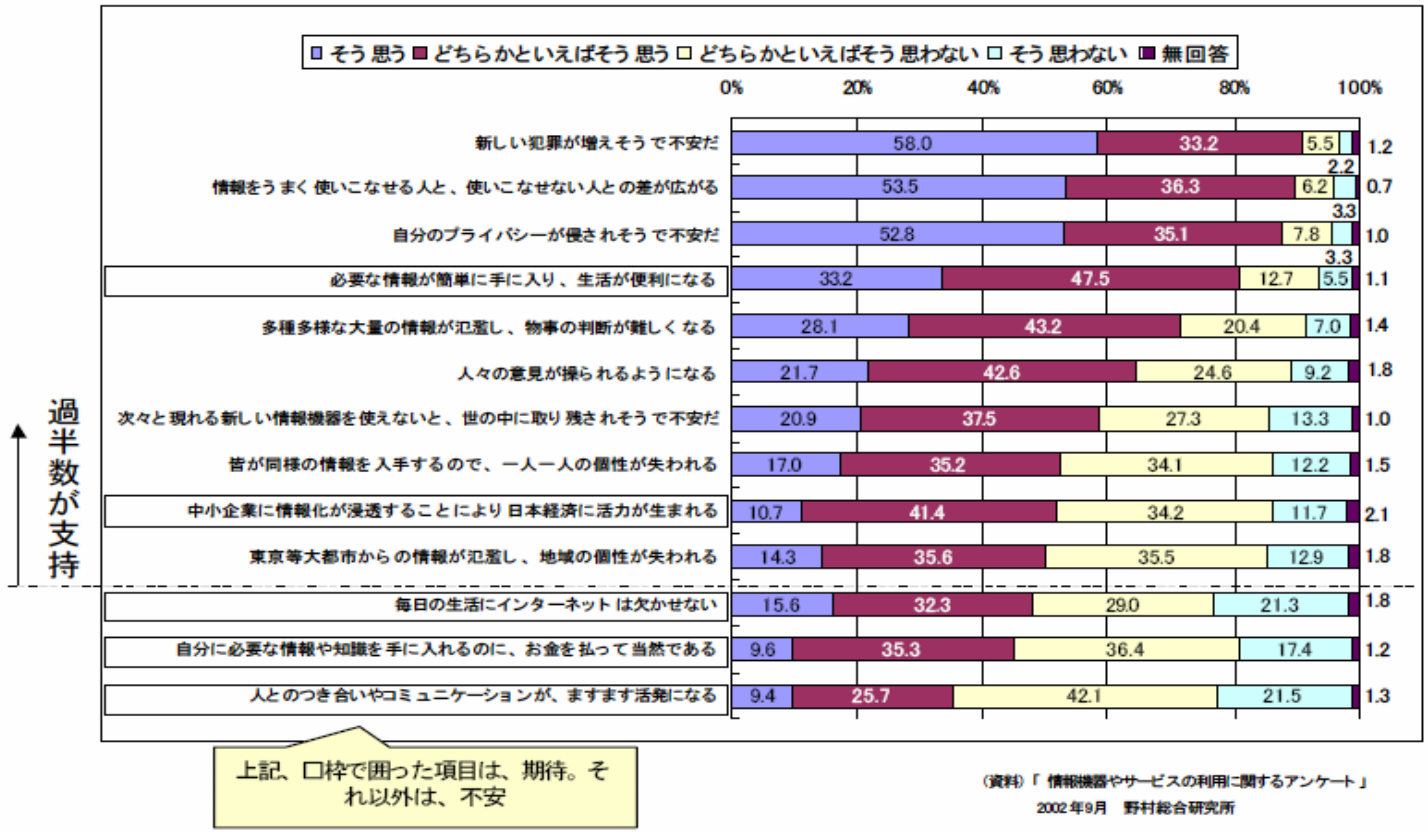
同製品にはHTTPプロキシサーバが実装されているため、インターネット接続を行い外部ネットワークから利用している場合に、第三者に公開された中継サーバ（オープンプロキシ）として悪用され、コメントスパムの踏み台等に利用される可能性がある。

■対策

ユーザは、インターネットの同社ホームページから最新の内蔵ソフトウェアを入手してバージョンアップした上で、同製品の設定画面でセキュリティ設定を有効に変更する。

家庭や企業の情報化に対する消費者の意識

- 消費者は、期待と不安が入り混じった意識を有している。



（資料）「情報機器やサービスの利用に関するアンケート」
2002年9月　野村総合研究所

ネットワーク家電市場の拡大と発展のために

- 消費者に対する脆弱性情報に関する適切な情報の提供
- ネットワーク家電における脆弱性情報の取扱体制の構築
- 消費者に対する脆弱性情報に関する適切な情報の提供においては、以下の点が重要
  - 脆弱性は、主としてネットワークを介した他の機器や利用者に迷惑をかける原因になることがあるが、ベンダの適切なサポートを受ければ、脆弱性を回避することや脆弱性自体を解消することが可能となり、安心してネットワーク家電を利用できること
  - 脆弱性とは、製造段階では検知が困難な問題であり、ネットワーク家電で発生をゼロとすることは困難であること
- ネットワーク家電における脆弱性情報の取扱体制
  - 業界が共同して脆弱性情報取扱体制を構築することにより、比較的低コストで体制を構築できること
  - 個々の製品毎に、製品開発者から消費者までに至る販売経路は異なっており、それに応じた体制が必要となること

JPCERT CC