ソフトウェア技術者は
脆弱性のない世界を夢にみるか

歌代和正
株式会社インターネットイニシアティブ
有限責任中間法人 JPCERT/CC

脆弱性の事例

ウェブカレンダーの入力チェック不備が原因で、細工されたURL経由で任意のコードが実行される。※1

攻撃者が細工したJPEG画像をMMSメッセージで送りつけることで、携帯電話がのっとられてしまう。※2

世界各国の石油、ガス、食品・飲料などの工場でつかわれている制御システムに脆弱性。細工されたパケット1つで、システムがクラッシュ。※3

※1 CVE-2006-2261, ※2 CVE-2008-2548, ※3 CVE-2008-2005

脆弱性とは？

- 経済産業省告示
  - ソフトウェア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。
  - ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

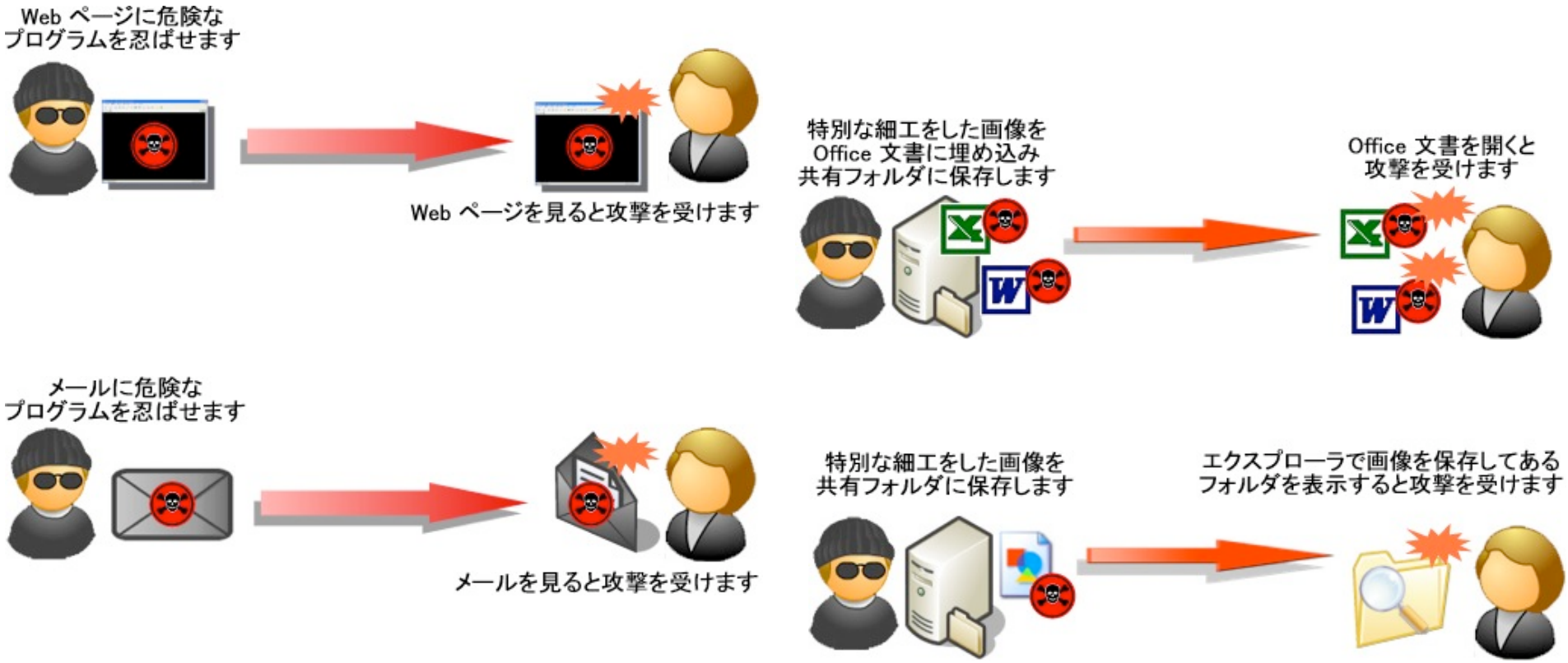
脆弱性とは？

- マイクロソフト *TechNet*
  - **セキュリティの脆弱性とは、製品の適切な使用による場合でも、攻撃者によるユーザーシステムに対する特権の不正行使、操作の制限、システム上のデータの損傷、および許可されていない信頼の偽装を防止不能にする、製品に含まれる問題である。**

- 解説
  - 製品には、仕様上の弱点を伴うことがありますが、このような弱点はセキュリティの脆弱性でありません。
  - 製品の不完全さによって問題があったとしても、広く受け入れられている標準であれば、セキュリティの脆弱性ではありません。
  - 問題がセキュリティの脆弱性となるには、相当の防止手段にもかかわらず、攻撃者が攻撃対象を屈服させることができる可能性がなければなりません。
  - 問題がセキュリティの脆弱性となるには、想定された方法、要求された方法、あるいは正当な方法で製品が使用されている際に発生する必要があります。
  - お気づきと思いますが、定義には判断の余地が大いにあります。ただし、最終的には、お客様の保護という良識と願いから判断しています。

脆弱性の例

MS04-028 : Windows の重要な更新JPEG 処理 (GDI+) のバッファ オーバーランにより、コードが実行される



脆弱なプログラムの例

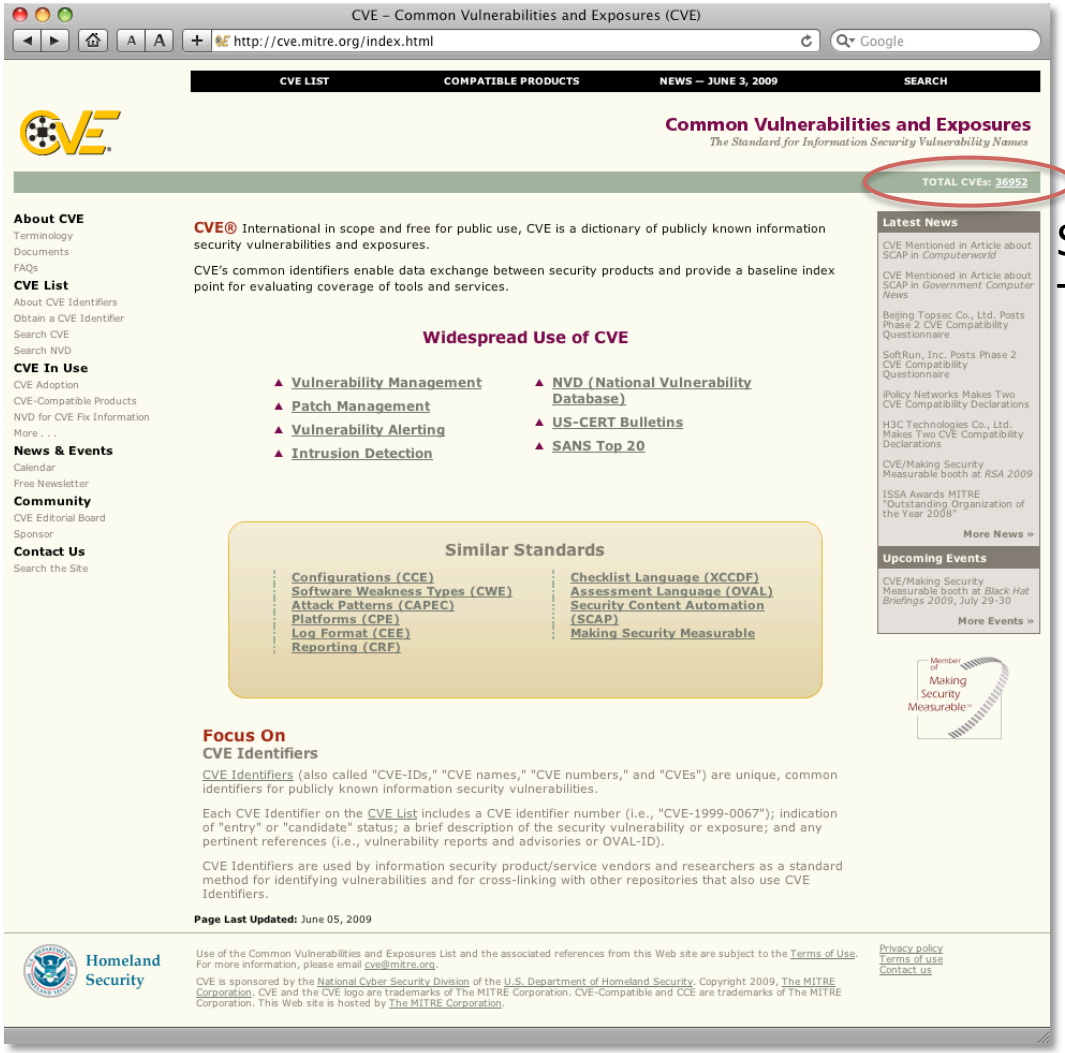
```
COMMENT FIELD
+------+------+------+------+------+------+------+------+
|     SIZE    |        COMMENT DATA ...                   :
+------+------+------+------+------+------+------+------+
```

```
void getComment(unsigned int len, char *src) {
   unsigned int size;

   size = len - 2;
   char *comment = (char *)malloc(size + 1);
   memcpy(comment, src, size);
   return;
}
```

どのくらいあるのか?

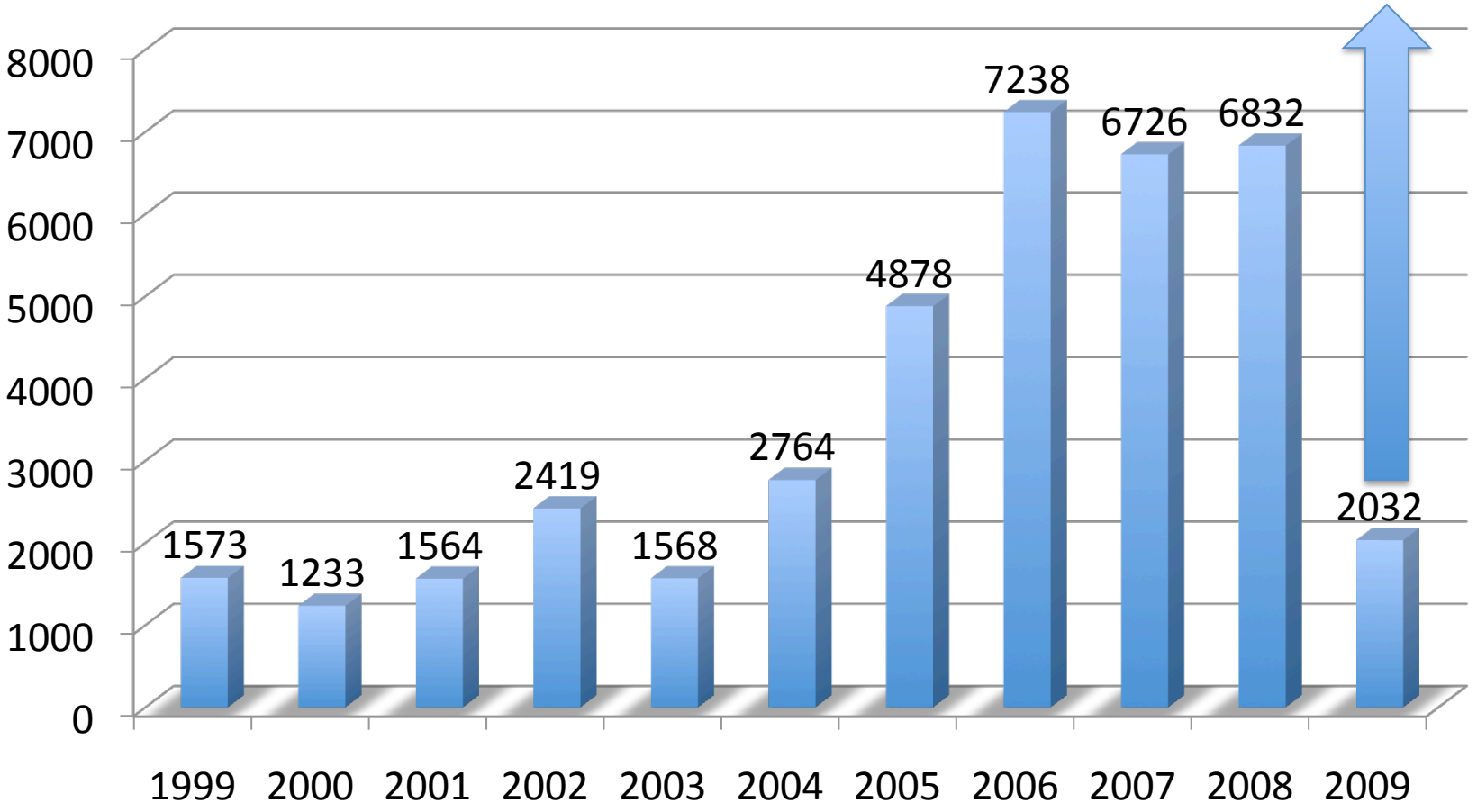
CVE:
Common Vulnerability and Exposures



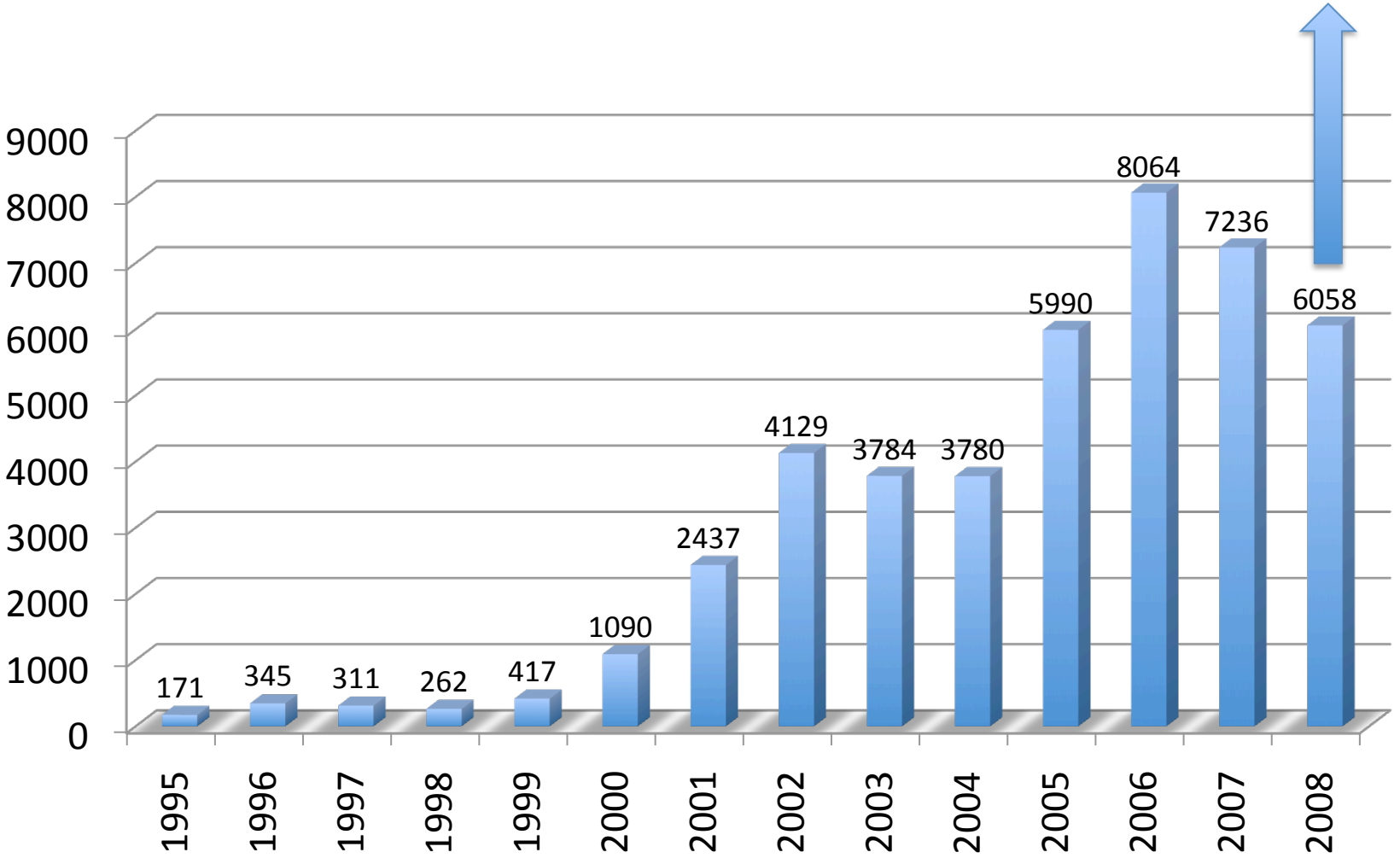
Since 1999

Total CVEs: 36952

CVE 登録件数


8000
7000
6000
5000
4000
3000
2000
1000
0
1573
1233
1564
2419
1568
2764
4878
7238
6726
6832
2032
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009

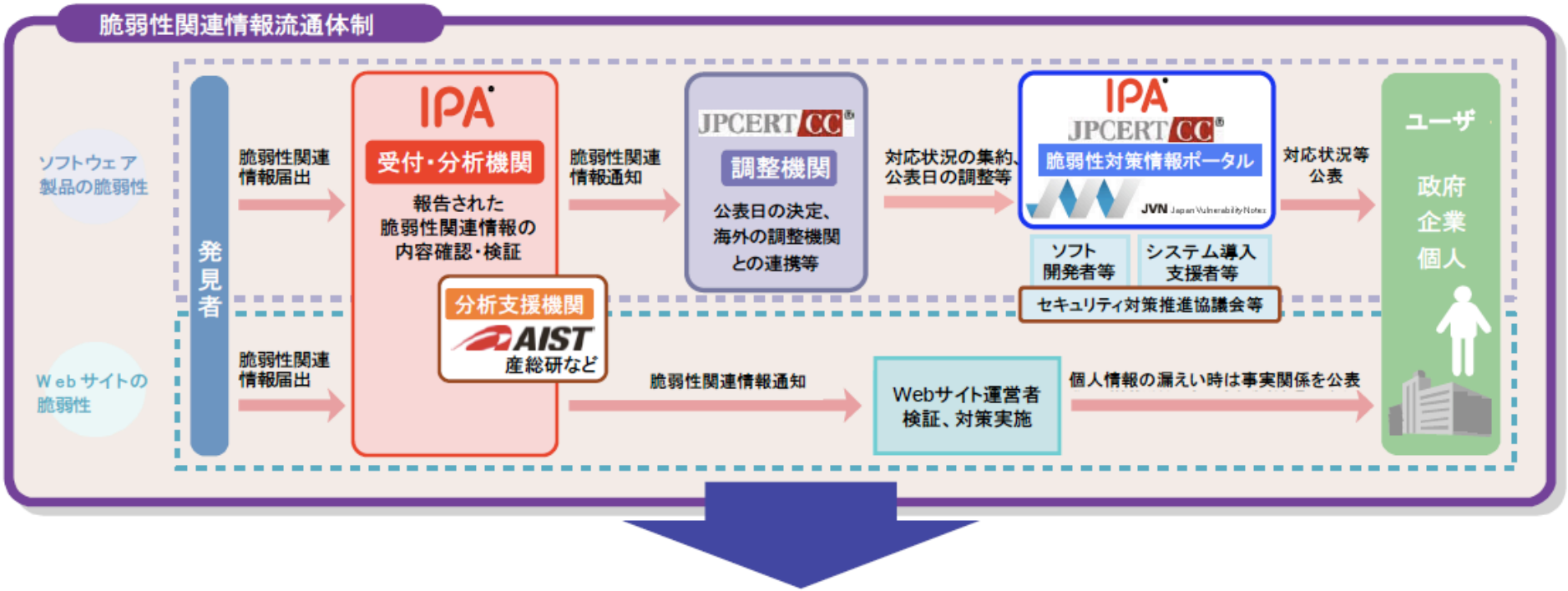
CERT/CC への脆弱性届け出件数



まあ、とにかく増えてます

日本では…

情報セキュリティ早期警戒パートナーシップ



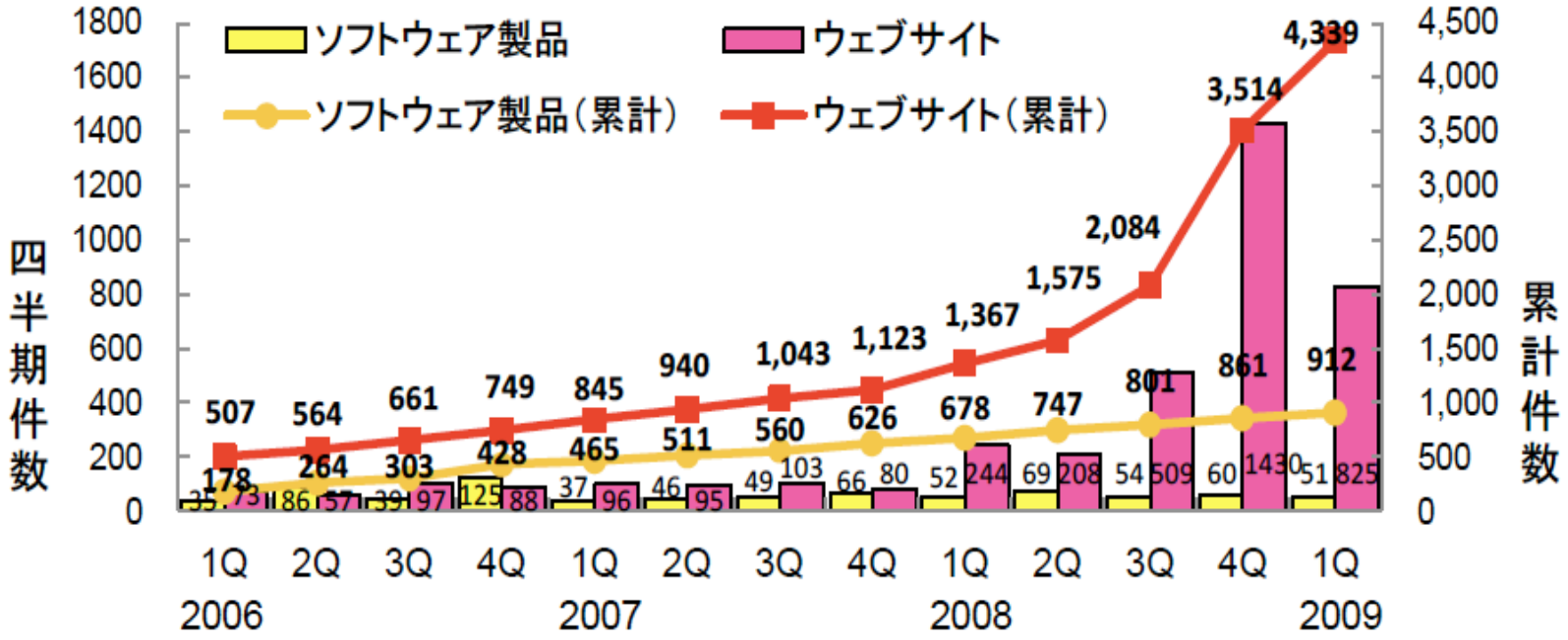
【期待効果】

①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②不用意な脆弱性関連情報の公表や脆弱性の放置を抑制
③個人情報等重要情報の流出や重要システムの停止を予防

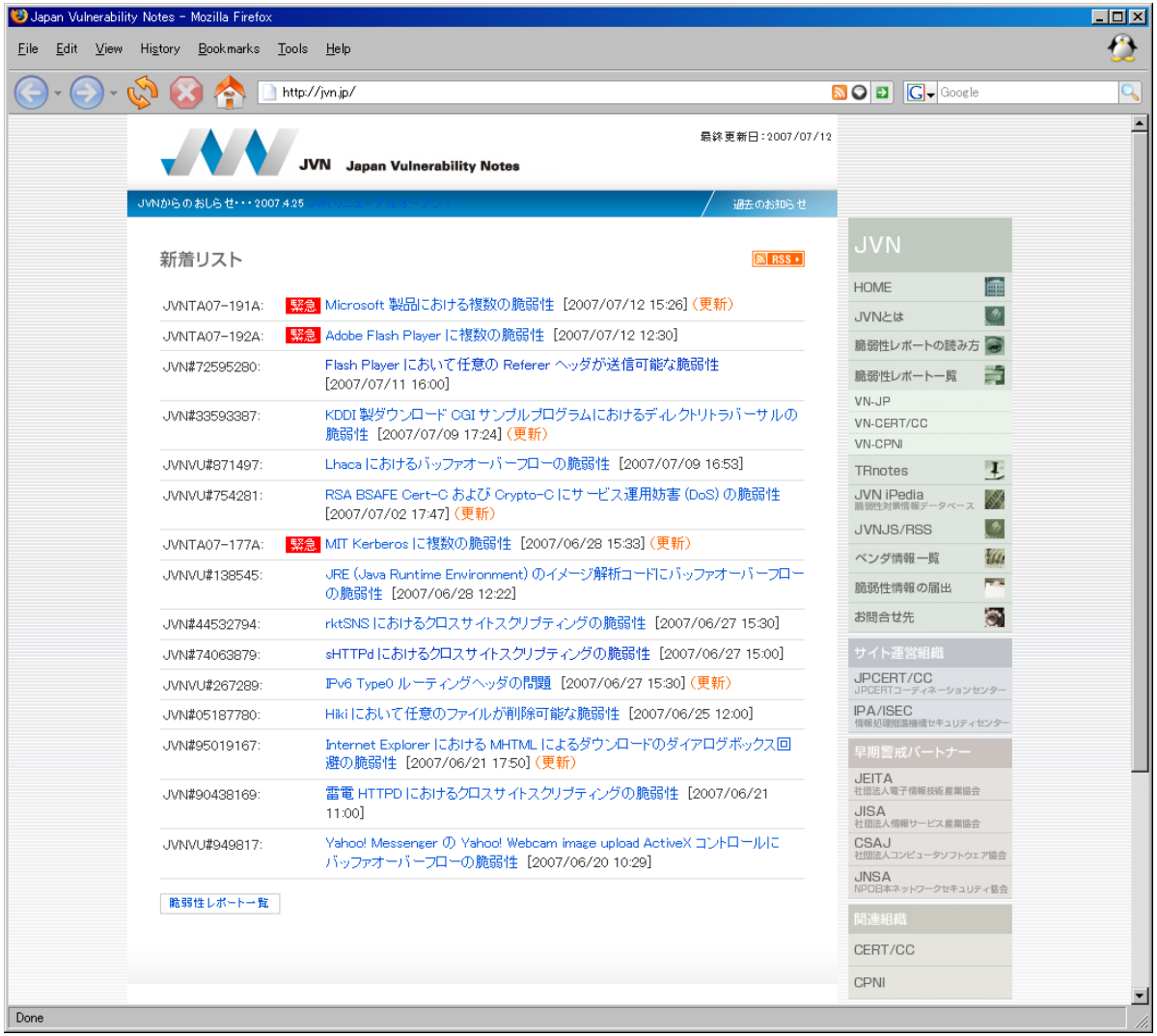
ソフトウェア等の脆弱性関連情報に関する届出状況 [2009年第1四半期]

脆弱性関連情報の届出件数の四半期別推移

	2006/1Q	2007/1Q	2Q	3Q	4Q	2008/1Q	2Q	3Q	4Q	2009/1Q
累計届出件数[件]	685	1,310	1,451	1,603	1,749	2,045	2,322	2,885	4,375	5,251
1就業日あたり[件/日]	1.61	1.95	1.98	2.03	2.05	2.24	2.38	2.79	4.00	4.55

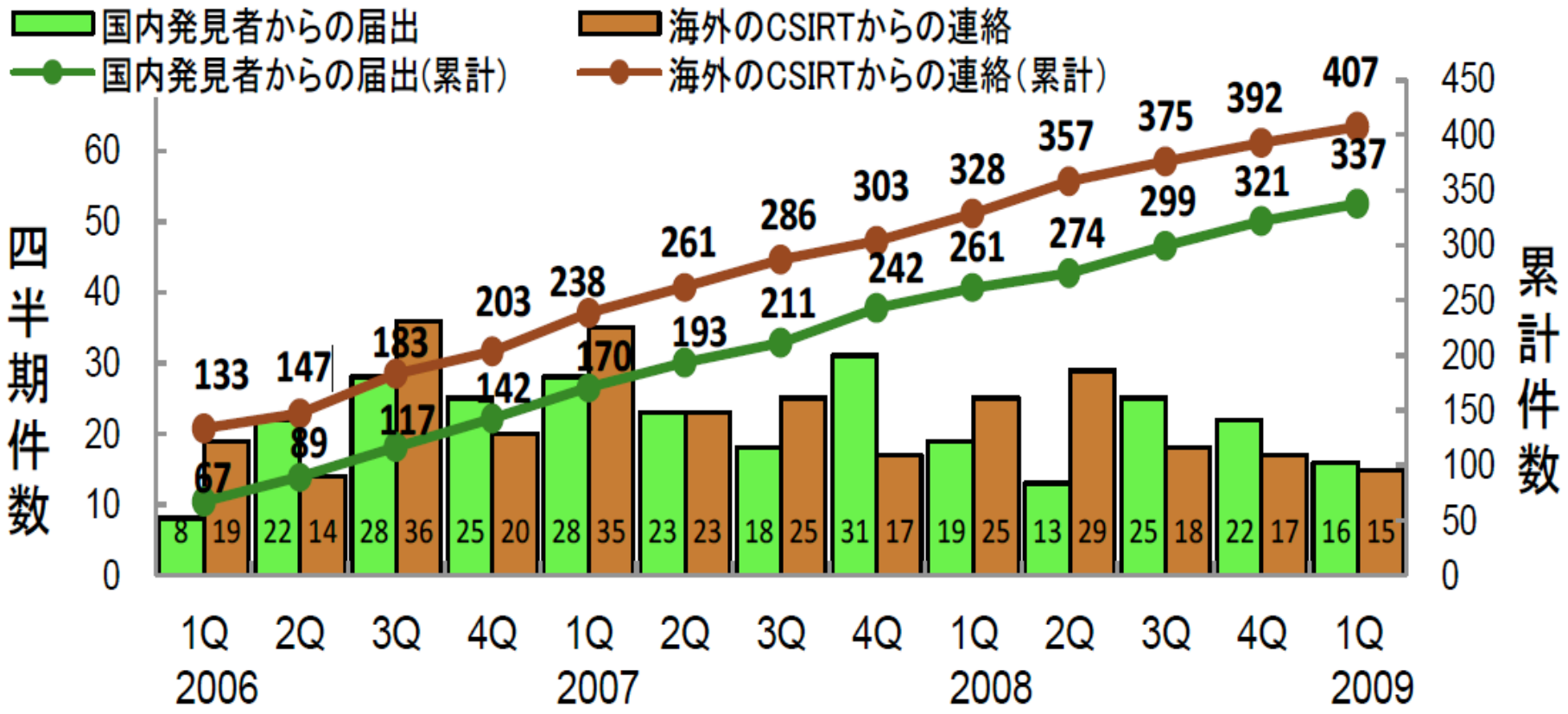


JVN: Japan Vulnerability Notes



ソフトウェア等の脆弱性関連情報に関する届出状況 [2009年第1四半期]

ソフトウェア製品の脆弱性対策情報の公表件数



脆弱性に当たる確率は?

- 日本のプログラマ人口は50～100万人
  - 情報サービス業では 25万人
  - H17年度国勢調査 SE+プログラマ 80万人超
- とりあえず50万人にしときましょう
- 世界で1年間に発見される脆弱性が10000件で、その1割の1000件が日本で発生すると仮定すると

- 今年、脆弱性を発見されるプログラマは、500人に1人
- 10年に1度遭遇するプログラマは50人に1人
- 1000人規模の会社では、年間2件脆弱性事故発生

ビミョー…

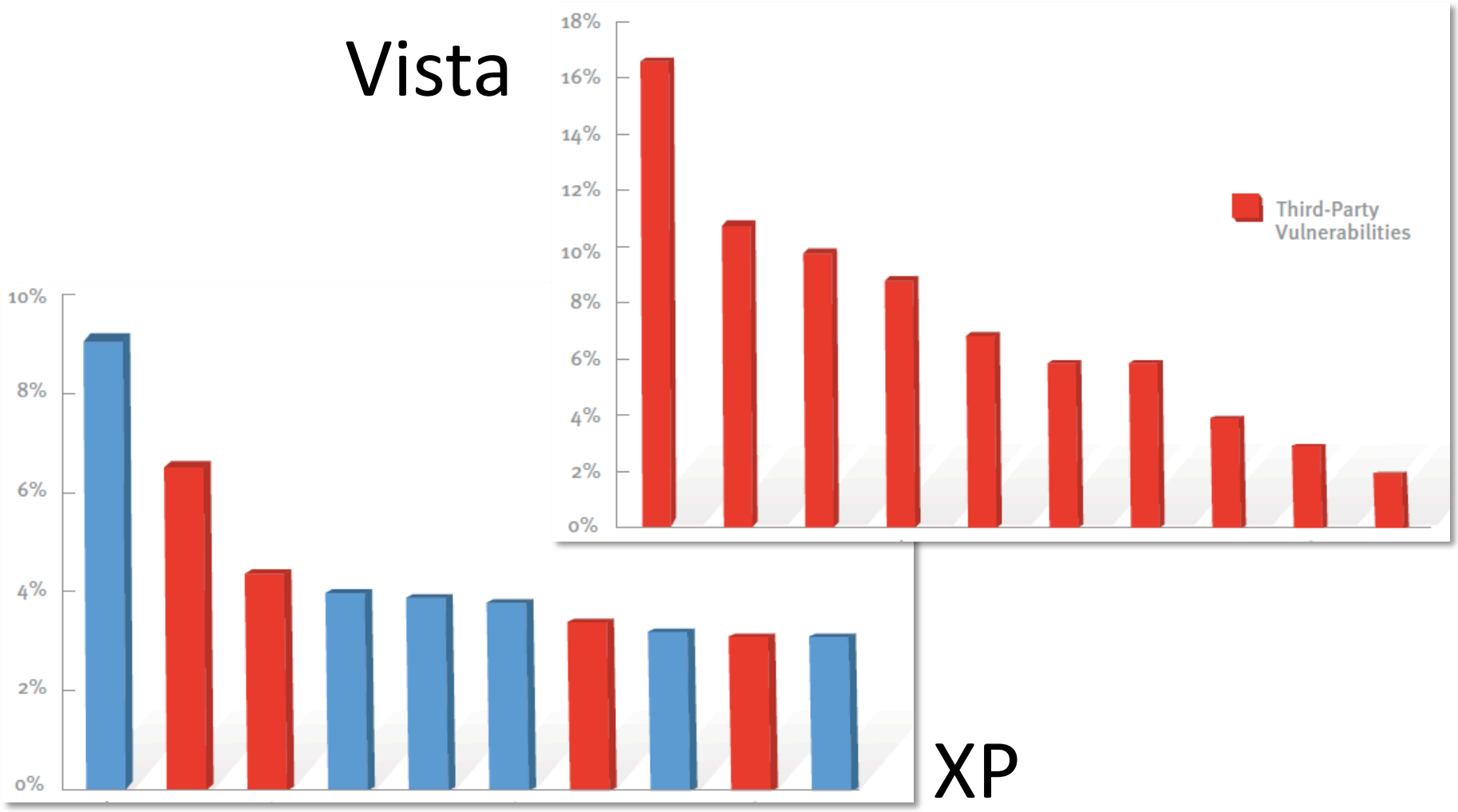
サービスを含めるともうちょい深刻

- 前のページは、ソフトウェア製品の脆弱性の話
- ウェブページに関する脆弱性報告は、ソフトウェア製品の20倍
- ウェブ以外のサービス提供形態の場合、届け出体制がないので、実態はもっと多いはず

- 1000人規模の会社では、年間数十件の脆弱性対応が発生
- おそらく、その数倍～数十倍の潜在脆弱性が存在

そうはいっても、マイクロソフトがちゃんとしなきゃ駄目だと思ってませんか?

Vista



XP

資料:セキュリティ インテリジェンス レポート 第6版

JVN で 2009年に公開された国内案件

1. CGI RESCUE 製 Webメーラーにおける HTTP ヘッダインジェクションの脆弱性
2. CGI RESCUE 製フォームメールにおけるメールの不正送信が可能な脆弱性
3. CGI RESCUE 製簡易BBS におけるクロスサイトスクリプティングの脆弱性
4. CGI RESCUE 製簡易BBS22 におけるメールの不正送信が可能な脆弱性
5. 一太郎シリーズにおけるバッファオーバーフローの脆弱性
6. futomi's CGI Cafe 製高機能アクセス解析CGI Professional 版における管理者権限奪取の脆弱性
7. futomi's CGI Cafe 製高機能アクセス解析CGI Standard 版 (Ver. 3.x 系) におけるクロスサイトスクリプティングの脆弱性
8. futomi's CGI Cafe 製 MP Form Mail CGI における管理者権限奪取の脆弱性
9. ソニー製ネットワークカメラ SNC シリーズの ActiveX コントロールにおけるバッファオーバーフローの脆弱性
10. Becky! Internet Mail におけるバッファオーバーフローの脆弱性
11. futomi's CGI Cafe 製全文検索CGI における管理者権限奪取の脆弱性
12. MyNETS におけるクロスサイトスクリプティングの脆弱性

なんか、おかしくないか?

発見される脆弱性の偏り

- 存在する脆弱性と発見される脆弱性の間には隔たりがある
- 発見者の意図
  - 発見しやすい
  - 目立つ
  - 自分で使っている
  - 入手しやすい
  - 数を稼ぎやすい
- 潜在的に存在するが発見の対象となっていない脆弱性は数多く存在すると予想される

攻撃にも流行がある

- ある画像ファイルの脆弱性が見つかると、他の画像形式についての脆弱性研究が進む
- あるハッシュアルゴリズムに衝突があることがわかると、他のハッシュアルゴリズムについても衝突の研究が進む
- ある機器で uPnP に関する脆弱性が見つかると、他の機器にもないかと探す

OS からアプリケーションへ

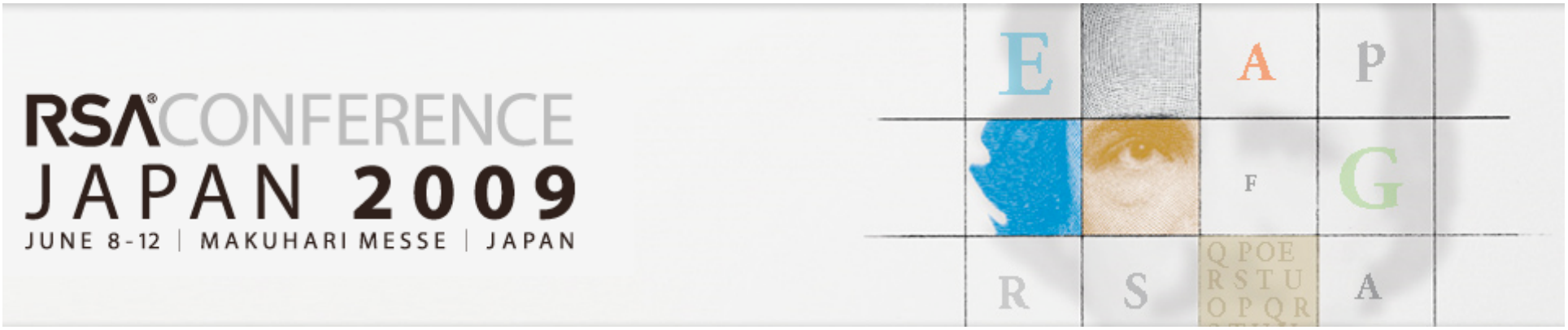
- 脆弱性の発生傾向はオペレーティングシステムからアプリケーションやサードパーティプラグインなどに移行してきている。

ウェブアプリについては…

- 適当なソフトをダウンロードして検査すると、必ず脆弱性が見つかる (某F氏)

- ウェブサイトには100%脆弱性がある (某S社)

どうやら、きりがないらしい



RSA カンファレンスでパネルをやりました

「セキュアデベロップメントの現場を語る」

パネリスト

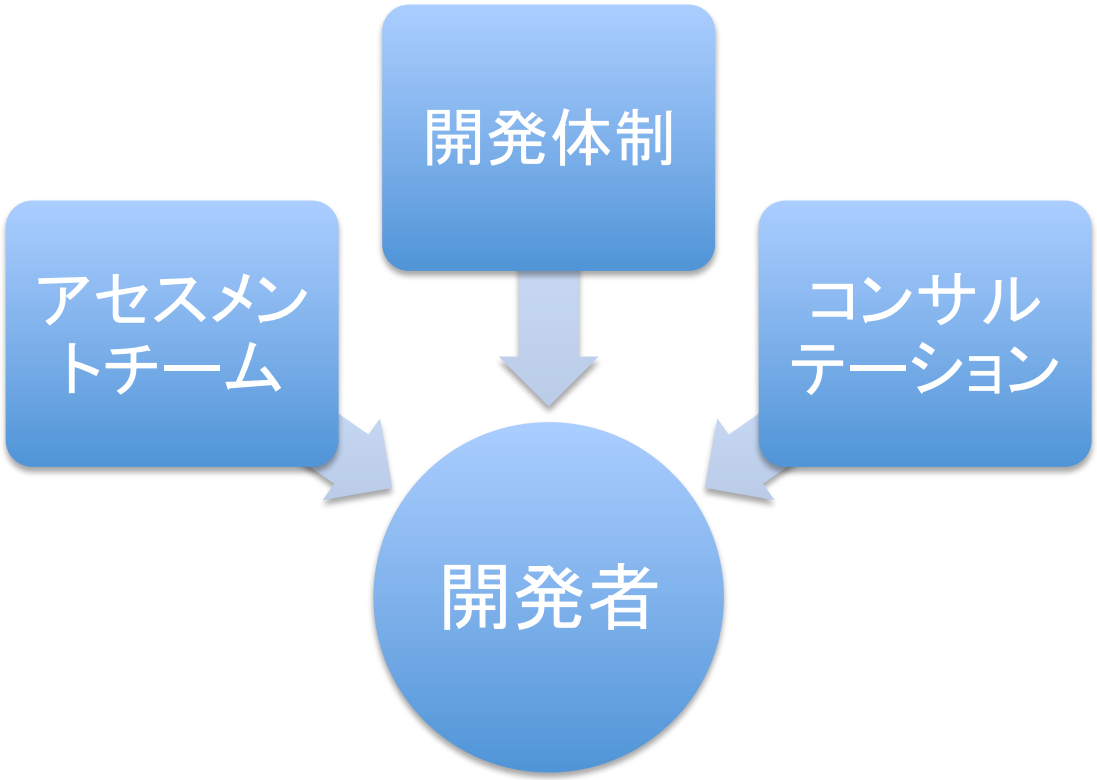
- 松並　勝
  - ソニーデジタルネットワークアプリケーションズ株式会社
- 加治佐　俊一
  - マイクロソフト株式会社
- 金谷　延幸
  - 株式会社富士通研究所

三者三様のアプローチ

	松並さん	加治佐さん	金谷さん
分野	組み込みソフトウェア開発	オペレーティングシステム、システムソフト	システムインテグレーション、システム開発
主張	限られたリソースの範囲内で、最も効果的な部分に集中して、足りない部分は諦める	トップダウンによる徹底的なセキュリティ指向の開発ライフサイクルの構築	SI の開発チャンスは一度きりなので、設計段階での判断ミスは致命的
手法	ドキュメントレビュー コードレビュー 静的解析ツール	Security by Design, by Default and in Development + Communication 脅威モデル	問診サービスによって、潜在的な問題を事前に察知

手厚い支援体制

ソニー	マイクロソフト	富士通研
•強制はしない •開発体制に口出ししない •社内インターン制度	•トップデシジョン •全社一丸 •確立した統一的メソドロジー	•開発者と信頼関係を構築 •非難しない •問題点を一緒に明らかにしていく



何が言いたいかというと

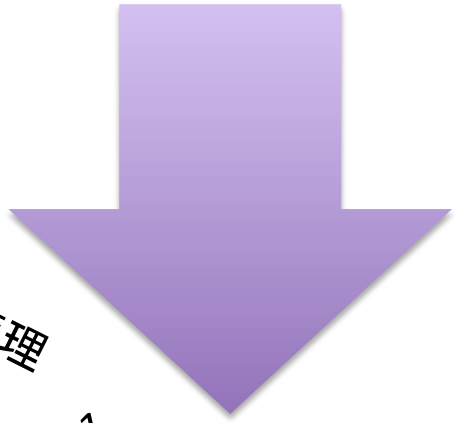
- セキュリティ担当者はものすごく気を使っている
- 当の開発者に危機感はあるのか?

- 脆弱性を作り出す本人に当事者意識がなければ問題は永遠に解決しない

とは言っても
開発者は、より優れたソフトを作りたい

スタック、なにそれ？
おいしいの？

アプリケーションの複雑化
高機能化
大規模開発
統合開発環境
複雑なGUI



スタック
ボット
マルウェア
バーチャルモニタ
レジスタ管理
スケジューリング
メモリ管理
アセンブラ
オペレーティングシステム
Ring -1
ルートキット
BIOS

下層へと移動する攻撃対象
巧妙化、高度化する攻撃手法

闘う条件はかなり不利

- 相手は、どこか１箇所でもいいから穴をみつければ勝ち
- こちらは、すべてを完璧に守らなければならない

とりあえず、夢くらいは見ましょうよ