JPCERT/CC Updates

パネルディスカッション

脆弱性情報の一般公開前の提供について

株式会社インターネットイニシアティブ
プロダクト推進部
齋藤　衛

パネリスト紹介

- 有限責任中間法人JPCERTコーディネーションセンター
  水越一郎
- 株式会社インテック・ネットコア
  近藤邦明
- 株式会社インターネットイニシアティブ
  齋藤　衛

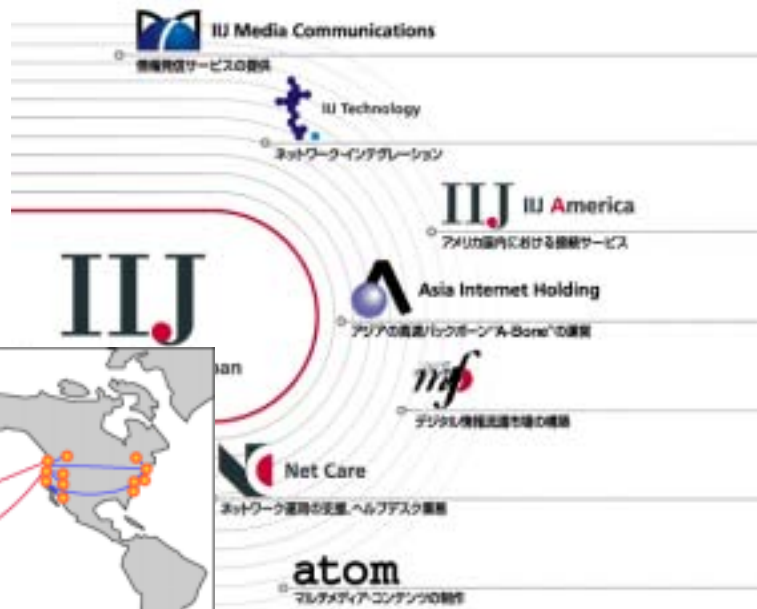
IIJ

Private CSIRT
IIJ-SECT
(IIJ Group SEcurity Coordination Team)

製品ベンダ

ISP
MSSP
xSP

SIer,IX,Callcenter,...



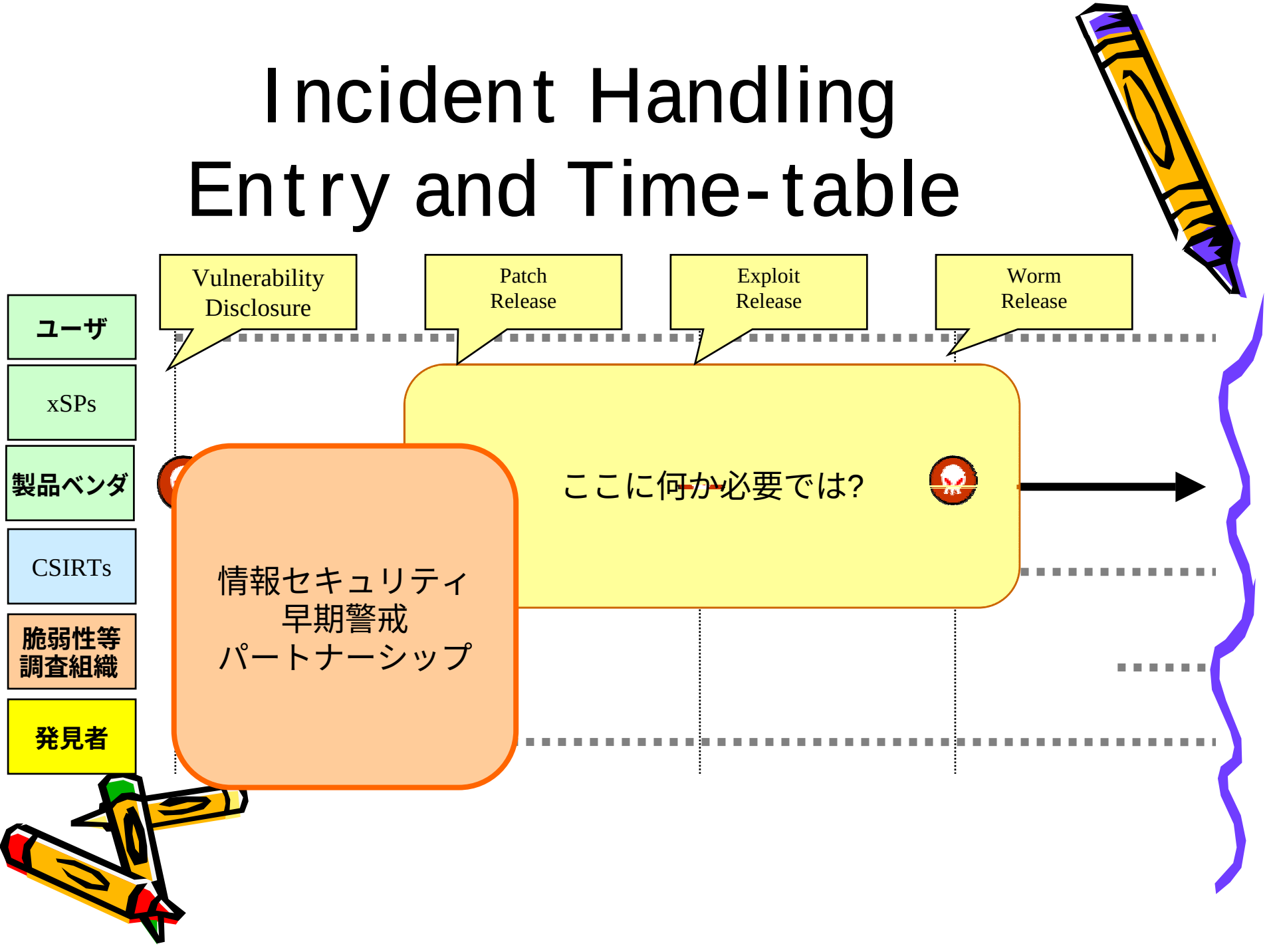
情報セキュリティ早期警戒パートナーシップ

- 経済産業省告示第235号
- 製品開発者に対する脆弱性情報の優先提供
- IPAとJPCERT/CCの協力関係で実現

本日の前提

- 製品の脆弱性対策については情報セキュリティ早期警戒パートナーシップが動くだろう。
- 脅威情報の流通について同じような枠組みは欲しくない？

Incident Handling Entry and Time-table



本日の議題

- では、
  - 誰に対して
  - いつ
  - どのような情報を

提供すればよいか

優先提供の問題点

- なにもしなくても
  - 対策と攻撃プログラムの開発競争
  - 製品開発者に対する優先提供で多少余裕ができる(かも)
- 優先提供自体の問題
  - 提供先の選定(誰が重要か?)
  - 優先提供先からの漏洩
  - 提供内容の選定
    - 対策情報(何を、どうやって守る)
      攻撃情報(何を、どうやって攻撃する)

JPCERT CC

脆弱性情報の
一般公開前の提供について

JPCERT/CC

水越一郎

背景その1：脆弱性情報

JPCERT CC

- 脆弱性情報
  - 悪意ある側に伝わると危険
  - 開発者に事前提供し対策情報の作成を促したい

これを実現するために

経済産業省告示
「ソフトウエア等脆弱性関連情報取扱基準」

この中でJPCERT/CCは開発者との調整を行う役割
{脆弱性、対策}情報の両方を事前に知りうる立場

Case 1:事前情報提供なし

JPCERT CC

Sendmailのヘッダー解析部に
buffer overflow…

http://www.jpcert.or.jp/at/2003/at030002.txt

2003/2/28JPCERT/CCが情報入手

2003/3/4　日本時間深夜一般公開

出社したら、大騒ぎだった…っていう人
いませんか？

背景その2:対策情報

JPCERT CC

- 対策が実施されて初めて、安全なシステム
- 対策を実施するまでのスピードが重要
- 「ＩＰＡは、（中略）、脆弱性関連情報と対策方法を、政府機関や重要インフラ事業者等に対して優先的に提供することがあります」

  情報セキュリティ早期警戒パートナーシップガイドラインより

{脆弱性、対策情報} の提供

JPCERT CC

前

重要インフラには、IPAから
優先的に提供の可能性

一般公開

後

一般に対して、JVN，Spread
などを通じて広く普及活動

上手な情報提供とは？

Case 2:事前提供あり

JPCERT CC

TCP プロトコルに潜在する信頼性の問題

http://www.jpcert.or.jp/at/2004/at040003.txt

2/下旬	情報の入手、公開は7月に設定
3/上旬	公表日が4月21に変更
4/7	TCP MD5をWeekly Reportで紹介
4/19	ASミーティング
4/21	一般公開

上手な情報提供とは？

JPCERT CC

- 悪意ある側への攻撃情報の漏洩を防ぎつつ

- システムへの速やかな対策実施を勧める
  - 適切な人･組織に対して、
  - 速やかに、
  - 説得力のある情報を提供

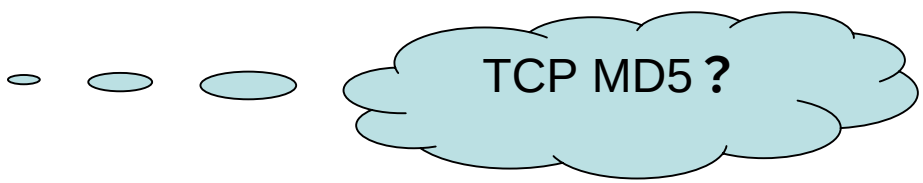
情報提供を考える上での要素

JPCERT CC

- 提供対象の選び方
  - 影響の大きさ

- タイミング
  - 対策実施に必要な準備期間

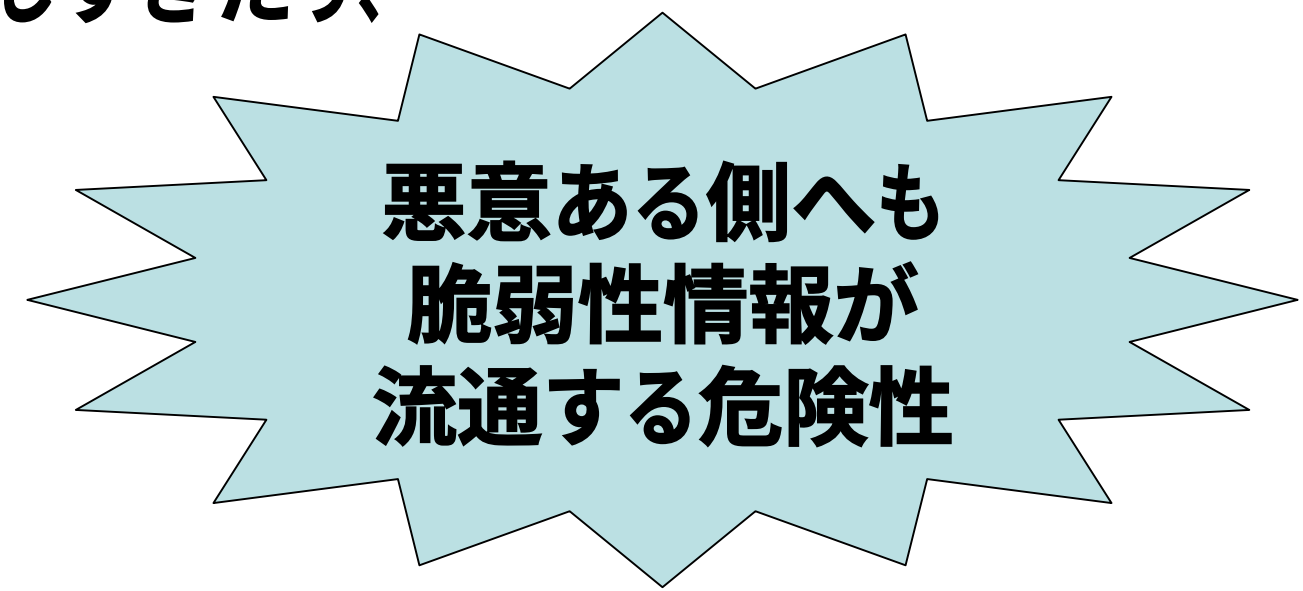
- 内容
  - 危険度の推定



しかし・・・

JPCERT CC

- 広すぎたり、
- 早すぎたり、
- 詳しすぎたり、



補足　Case 3:情報提供の内容

JPCERT CC

Cisco IOS Interface Blocked by IPv4 Packtes

時系列：http://jvn.jp/tr/TRCA-2003-17.html

2003/7/17 09:00 Cisco **初版公開**

　バージョンアップか、大量のACL**設定を推奨**

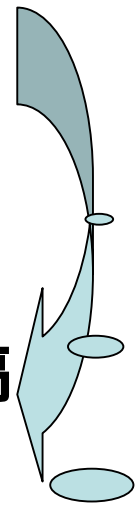
2003/7/18 08:00 Cisco **第三版公開**

　影響を受けるプロトコルフィールドを提示

2003/7/18 13:42 Full-Disclosure**に攻略コードが投稿**

2003/7/18 19:00 Cisco **第四版公開**

　攻略コードの存在を提示



こういう情報は有益？

この他、攻撃が開始された情報とかも有益？

この27時間をどう考える？

全部出したら駄目なの？

株式会社インテック・ネットコア
近藤邦昭

脆弱情報と脅威情報

- 脆弱情報
  - 脆弱について詳しく述べるため、その情報をつかって、その脆弱を突く可能性あり。
  - このため、通知範囲を限定する必要あり。

ん～それは出すのは難し～ね～

- 脅威情報
  - なにかがあることだけがわかる。実質的な対策が打てないが準備はできる。
  - 攻撃者にとって、なにをどう突いてよいかわからないので、情報とならない。

だったらだせばいいじゃん

でてこないとどうなる？

- 出てくる場合
  - 情報の順序：脅威情報　⇒　脆弱情報
  - 脅威情報に基づき対策準備が可能
  - 脆弱情報発表タイミングにあわせて、対応体制を組める。
- 出てこない場合
  - 情報の順序：脆弱情報のみ
  - 準備なしに脆弱情報のみが与えられる
  - 突然情報が出て、対応が十分にできないでオペレーターは右往左往…
    - せめて、何人体制の対応体制が必要か知りたい。
    - たとえば、「脅威度１０」だったら10人用意する。とか…

全部じゃないとだめなの？

- 全部じゃない場合
  - だれかが、これは重要じゃないって判断するんですよね？
    - それってだれの基準ですか？
    - その基準からはずれたのが、重要だと思ってるひとっていないのかなぁ～
- 全部の場合
  - 受けた側が重要かどうか判断できる
    - 受けた側の判断する重要度で対応体制を作ることができる。
    - でも、具体的な情報がないと判断できない

やっぱ全部だしてほしぃ～なぁ～