NRIセキュアテクノロジーズ

JANOG34 Meeting

Security Issuesへの取り組みと対応
～キャッシュポイズニングの手法を題材に～

2014年7月17日

NRIセキュアテクノロジーズ株式会社
テクニカルコンサルティング部
セキュリティコンサルタント
中島　智広

はじめに

■本セッションの目的は、下記について議論することです。

- ●問題を解決しより良い結果を導くために必要なこと
- ●今後必要になること

■車輪の再発明をしながら議論をするのは効率が悪いので、今回のJPRSさんの取り組みについて話をする前に、一般的な指針や枠組みを紹介しながらいくつかの論点を提示します。

[参考]

- ●ソフトウエア等脆弱性関連情報取扱基準(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ガイドライン(IPA)

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

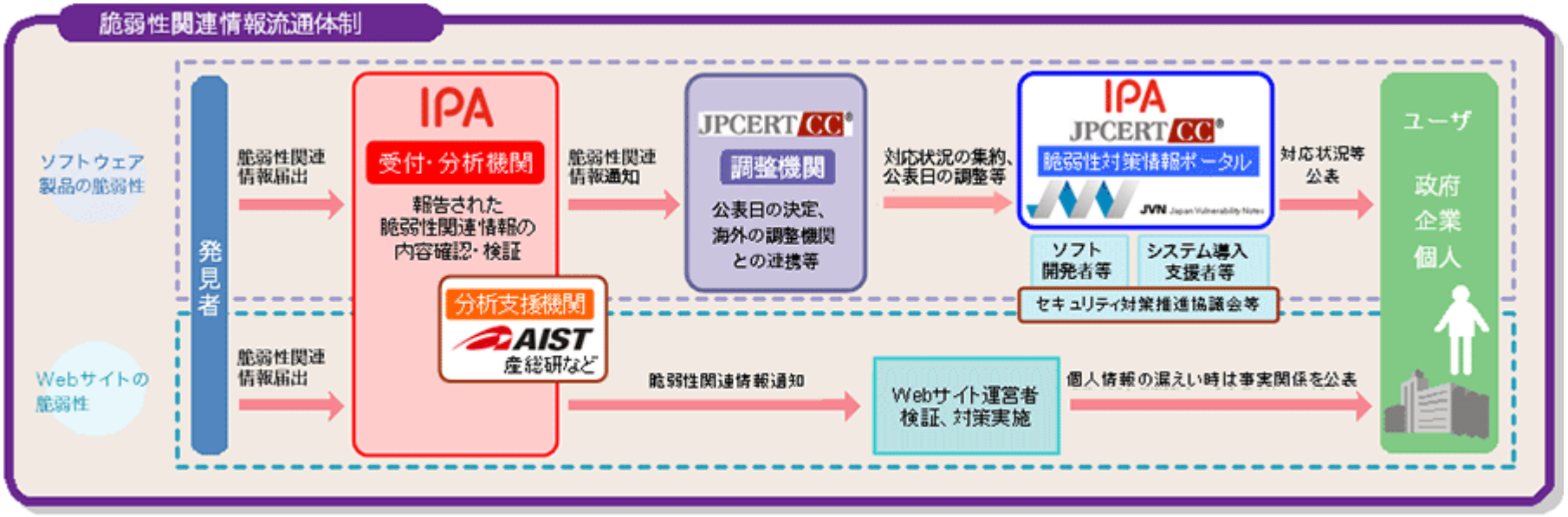
■概要

- 「ソフトウエア等脆弱性関連情報取扱基準(経済産業省告示)」に基づき、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルスなどによる被害発生を抑制するために、関係者に推奨する行為をとりまとめたもの

■対象

1. 日本国内で利用されているソフトウエア製品
   (ソフトウエア製品において通信プロトコル等の仕様を実装した部分を含む。)※厳密な意味での「プロトコル」は含まれない
2. 主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーション

情報セキュリティ早期警戒パートナーシップ



※JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:独立行政法人 産業技術総合研究所

IPA「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」より引用

- 受付・分析機関で内容確認・検証を実施(誤報、から騒ぎ抑止)
- 公表方針について調整を実施(不必要な被害、揉め事を抑止)
- 国外のCERT組織とも連携(世界的な問題にも寄与)

本事例の前提整理

対象	問題点	対策状況
プロトコル	悪用されうる問題が内在	未
実装	対策済 ※緩和策であり本格対策ではない	済
運用	危険な実装が10%残存	実施中

■根本たる問題(プロトコルの不備)は、実装により対策済
■このため、先述の枠組みに**そのまま適用されるものではない**
■あるべき論はあるにせよ、**運用の問題は無視できない**

「関係者に推奨する行為」とは

ひとことで言うと

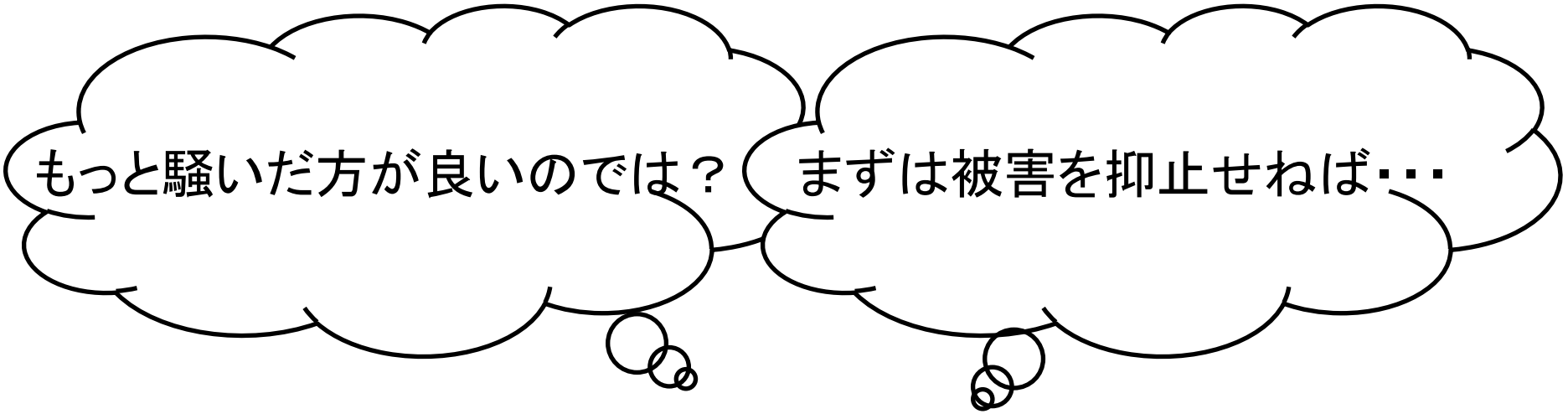
真摯な対応

- 発見者/通報者
  - 悪用のデメリットへの十分な配慮
- 開発者/提供者
  - サポートの約定の趣旨に従った対策

とはいえ・・・

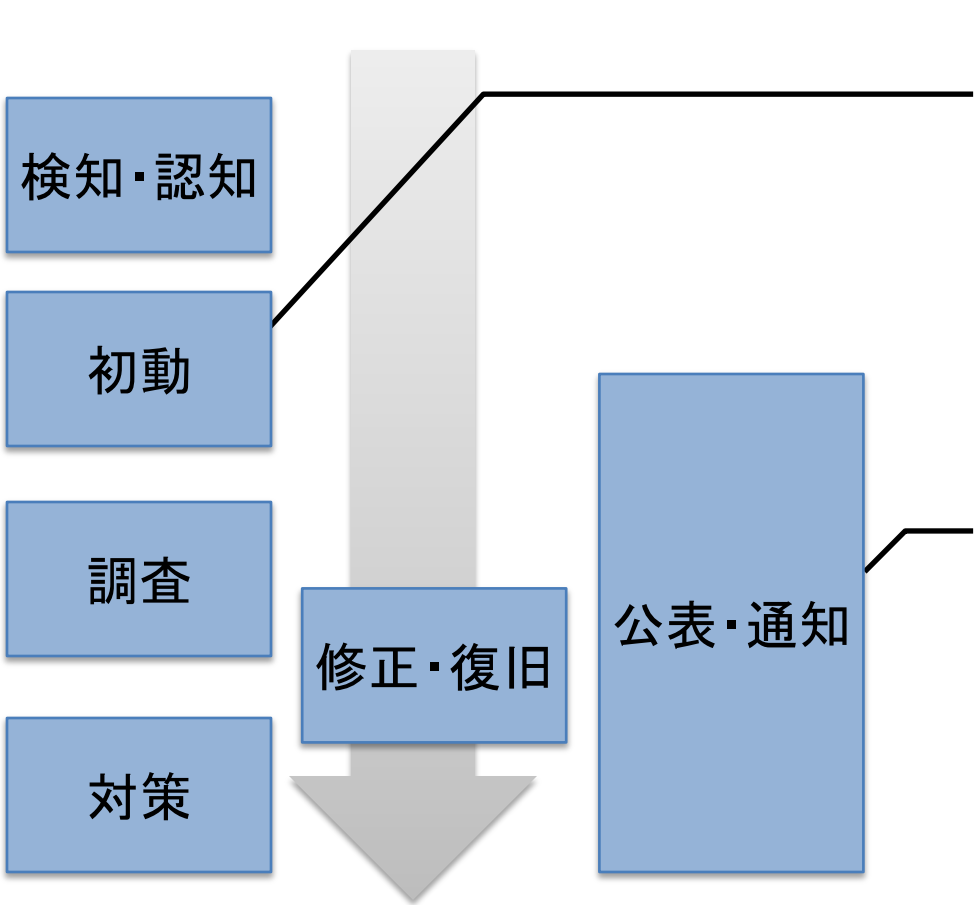
■皆、良かれと思ってやっている

●メリット/デメリットを認識した上で、各々の思いがある



収束に向けてステークホルダとの調整は重要かつ困難

インシデントハンドリングの一般的なプロセス



初動

- 対応方針の策定
- 応急措置
- 調査範囲の模索

重要

➔**遅れや間違い**があると、
その後の対応に影響大

公表・通知

■関係機関や、
ステークホルダへの公表

重要

➔**タイミングや温度感**を誤ると
不必要な不信や反感を買う

「初動」「公表・通知」のプロセスは特に重要

論点提示

- 何を最優先すべきか？
  - 利用者の安全性・被害の抑止
  - ステークホルダの思い
- インシデントハンドリングのプロセス、
  特に「初動」や「公表・通知」の方針はどうだったのか？
- そもそも何を、どんな場で問題とすべきだったのか？
  誰が、どう振る舞うとよりよかった、これからよいのか？
  - プロトコル、実装、運用
  - 発見者、通報者、調整者、運用者、研究者、専門家、etc…

これらを念頭に議論をしていきましょう

NRIセキュアテクノロジーズ