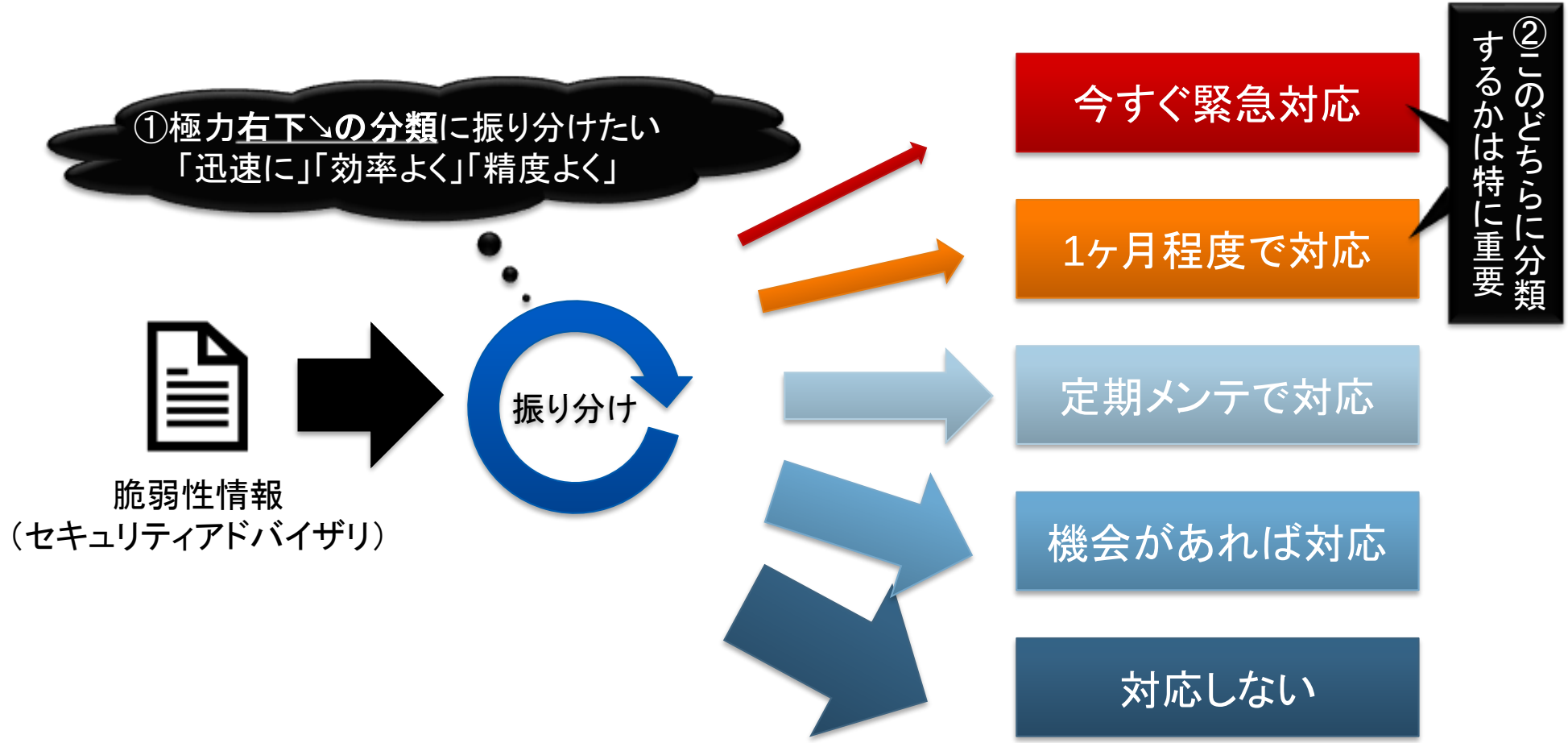
はじめに) JANOG39 脆弱性ハンドリングを楽にするBoF頭出し

運用者目線の脆弱性ハンドリング、トリアージ



対応の緊急度を下げるための判断材料探しが重要

問題意識①

■運用者にとって大事なこと

- (**できるだけ**)攻撃の被害が生じる前に対処
- (**できるだけ**)攻撃の被害が生じても極小化
- (**できるだけ**)低工数、低コストで対応
- **従業員のQOL(生活の質)を守る**(=事業は従業員の幸福実現の手段である)

■求める情報と世の中で流通する情報とのギャップ、温度感の差

- 「危ない！」「対策はパッチ適用」だけ言って騒がれても困る
  確率は？難易度は？想定される被害は？Workaroundは？
- タイムラインが盛り上がってると、「それ、本当に危ないの？」
  はなかなか言えない、言っても理解を得られにくい

■全ての組織にセキュリティに精通した人がいるわけではない

問題意識②

■重要なのは解釈ではないか

- ●一次情報入手のタイミングの格差はほとんどない
- ●どのように解釈し対処するかが分かれ道

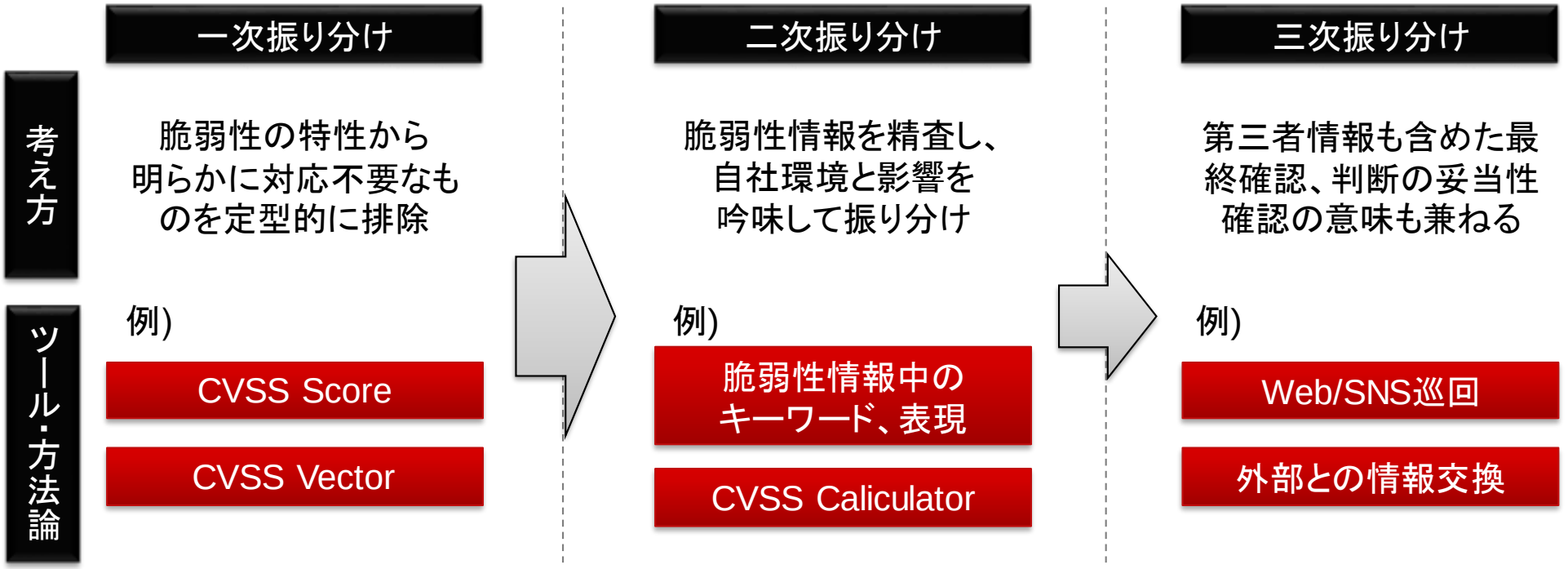
■みんな解釈に困ってないか？

- ●自分はこう考えるが正しいのだろうか？
- ●(自分の英語力では)このように書いてあるように見えるが間違ってないか？
- ●冷静に考えれば考えるほど世の中が危ないと騒いでいる理由がわからない

脆弱性ハンドリングの流れ

はじめに) JANOG39 脆弱性ハンドリングを楽にするBoF頭出し

BoF主催のモチベーション



- ひとつひとつのツールや方法論にきちんと広く共通認識はあるだろうか？
- 情報や知見の差によって無駄な苦労や非効率性が生まれていないだろうか?

みんなで議論して共有して共通ノウハウを底上げしたい！

本BoFの議論テーマ

実践！脆弱性ハンドリングの効率化手法

脆弱性のハンドリングの効率化手法全般について議論します。その一環として脆弱性の評価手法であるCVSSを取り上げます。脆弱性情報には数値(Score)と中身(Vector)が記されており、数値の大小だけでなく、意味と仕組みを理解することで効率が格段に向上します。このような方法論や観点について紹介や議論を行いノウハウの共有を行います。

運用者のためのイマドキの情報共有

脆弱性情報の収集や解釈は各組織の自助努力に依存しています。また、外部から情報を得ようとしても運用者にとって有用な情報を得にくい方向に向かっています。外況認識をふまえながら、問題意識の共有と運用者にとって有益な方法論の議論を行い、具体的な施策につなげます。

テーマ1）実践！脆弱性ハンドリングの効率化手法

脆弱性情報ちゃんと読めてますか？

CVE-2016-2776: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request

Author: **Brian Conry** Reference Number: **AA-01419** Views: ... Rating/ Voters

CVE: CVE-2016-2776
Document Version: 2.1
Posting date: 2016-09-27
Program Impacted: BIND
Versions affected: 9.0.x -> 9.8.x, 9.9.0->9.9.9-P2, 9.9.3-S1->9.9.9-S3, 9.10.0->9.10.4-P2, 9.11.0a1->9.11.0rc1
Severity: High
Exploitable: Remotely

Affected Version：対象

Description:

Testing by ISC has uncovered a critical error condition which can occur when a nameserver is constructing a response. A defect in the rendering of me... can cause named to exit with an assertion failure in buffer.c while constructing a response to a query that meets certain criteria.

This assertion can be triggered even if the apparent source address isn't allowed to make queries (i.e. doesn't match 'allow-query').

Description：解説

Impact:

All servers are vulnerable if they can receive requ...

CVSS Score: 7.8

CVSS Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:C)

For more information on the Common Vulnerability ... calculator&adv&version=2&vector=(AV:N/AC:L/Au:N/C:N...

Impact：影響

CVSS Score: 7.8

特にココとか

CVSS Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:C)

Workarounds:

No practical workarounds exist.

Active exploits:

A step-by-step breakdown of the issue has been published and working Metasploit code is available. Crashes have been reported that appear to be th... exploitation.

Workaround：回避策
Mitigation：軽減策

Solution: Upgrade to the patched release most closely related to your current version of BIND. These can all be downloaded from http://www.isc.org/downloads.

- BIND 9 version 9.9.9-P3
- BIND 9 version 9.10.4-P3
- BIND 9 version 9.11.0rc3

Solution：解決策

テーマ1）実践！脆弱性ハンドリングの効率化手法

やりたいこと、共有したいこと、議論したいこと

■ミニチュートリアル

- ●CVSSの解説とCaliculatorのハンズオン
- ●参加者全員がCVSSを活用した効率化ができるようになる

■共有・議論

- ●脆弱性情報のこんなところみてこんな風に考えるよ
- ●こんなところから情報収集してるよ、こんなことに困ってるよ
- ●その他効率化手法

テーマ2）運用者のためのイマドキの情報共有

情報共有の課題

■不文律のネチケットに基づくオープンな情報共有は限界

- ●janog@janogに脆弱性ネタを投げるのは相当に気を遣う
- ●「個人の見解」と前置かないと発言しにくい
- ●謎のクレームのようなものもしばしば

■ISAC※ってあるんだけど

※Information Shareing and Analysis Center

- ●上手くいっているところもある、敷居(お金の壁、業種の壁)はちょっとある
- ●早めに一次情報が来ることはあるらしい、でもパッチ提供が早いわけではない
- ●会社は加入してても現場担当者まで情報降りてこなかったり(組織内の問題)
- ●本来の情報共有の場、頑張ってほしいところ⊂(^･^)⊃フレーフレー

既存の枠組みだと現場の本音での解釈論議は難しそうだな

テーマ2) 運用者のためのイマドキの情報共有

目指すところ

お金で解決

- メーカーのプレミアムサポート
- スレットインテリジェンスサービス

運用者の助け合いによる情報と解釈の共有
- of the Ops, by the Ops, for the Ops -

組織に閉じた自助努力(我流解釈)

テーマ2) 運用者のためのイマドキの情報共有

議論にあたって

■前提

- ●各々の事業者で同じことをやるのは本当に無駄
  - ・組織に閉じた自助努力は限界
  - ・孤軍奮闘は寂しい
- ●共通のコンテキストがなければ議論は難しい
  - ・運用に疎い人たちに混ざって運用の議論ができるか？
  - ・運用に関しては、運用に理解ある間柄に閉じるのが基本ではないか？

■論点

これをどのように実現するか

運用者の助け合いによる情報と解釈の共有
- of the Ops, by the Ops, for the Ops -

Agenda

■CVSSミニチュートリアル

■Exploitablity(攻撃される可能性)をどう考えるか?

■BoF(バッファオーバーフロー)脆弱性は直ちに危険か?

■MITM前提脆弱性への対応温度感

■Internet Unreachableな脆弱性は放置できるか?

■セキュリティ原理主義とどう向き合うか～情報共有のすゝめ～