CSIRT からみたインシデント対応

Nov. 20, 2014

奥村 祐則　GREE-IRT

Agenda

1. Introduction

2. GREE-IRT のあゆみ
    1. Phase 0 – 混沌の時代
    2. Phase 1 – GREE-IRT 黎明期
    3. Phase 2 – SOC さんと二人三脚
    4. Phase 3 – SOC さんとのこれから

3. Wrap up

1. Introduction

スピーカー紹介

氏名：奥村 祐則
所属：グリー株式会社
　　開発統括本部
　　インフラストラクチャ本部
　　セキュリティ部
社歴：丸3年が見えてきた
仕事内容：
　　おおよそセキュリティならなんでも
　　CSIRT への関与＝社歴

職歴：セキュリティエンジニア
　　→セキュリティ監査/コンサル
　　→社内セキュリティ（いまココ）

メディア掲載歴：
　　NY times, AERA（上）, 広報しながわ（下）

会社紹介

社名	グリー株式会社（英名：GREE, Inc.）
設立年月日	2004年12月7日
連結従業員数	1,882人（2014年6月末時点）
主要事業内容	ソーシャルゲーム事業、広告事業、ベンチャーキャピタル事業 等
売上高・営業利益	売上高 1,256億　営業利益 350億（2014年通期）
上場市場	東京証券取引所第一部上場

会社紹介 / ソーシャルゲーム事業

事業の柱：ソーシャルゲーム / Native Gameの潮流

消滅都市
Everything in its right place

CROSS SUMMONER クロスサマナー

※株式会社ポケラボのタイトル

会社紹介 / 消費者向けサービス

新たな柱を目指して積極的に新規事業を展開

GREE-IRT という組織

組織名：GREE-IRT

沿革：　2011年ころ 設立
　　2012年1月 日本シーサート協議会加盟
　　2013年2月 社外SOC導入

組織形態：社内横断バーチャルチーム

活動内容：インシデント対応
　　脆弱性対応

売上高：ありません

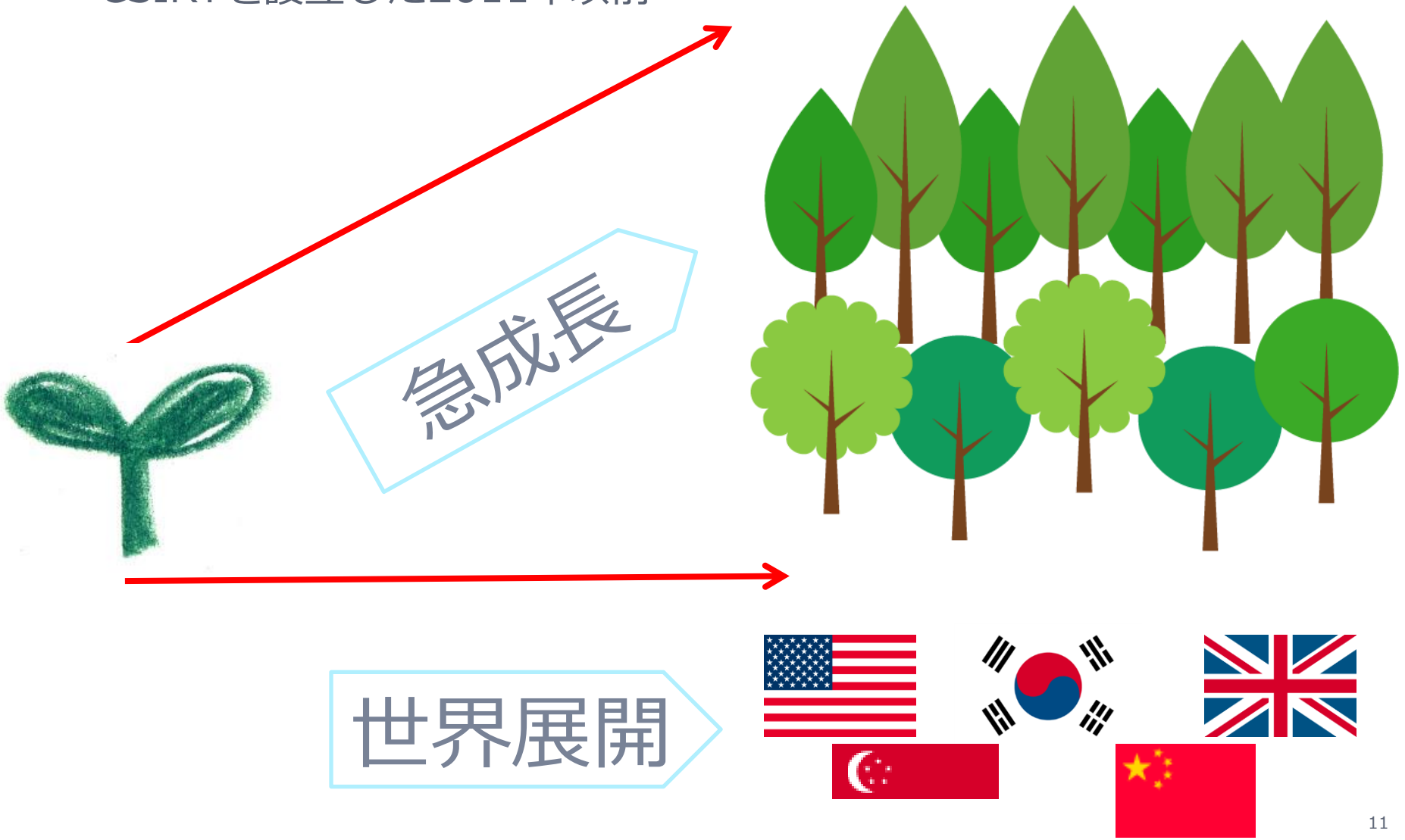
担当者：10名いかないくらい

2. GREE-IRT のあゆみ

Phase 0 – 混沌の時代

Phase 0 – 混沌の時代

- CSIRTを設立した2011年以前



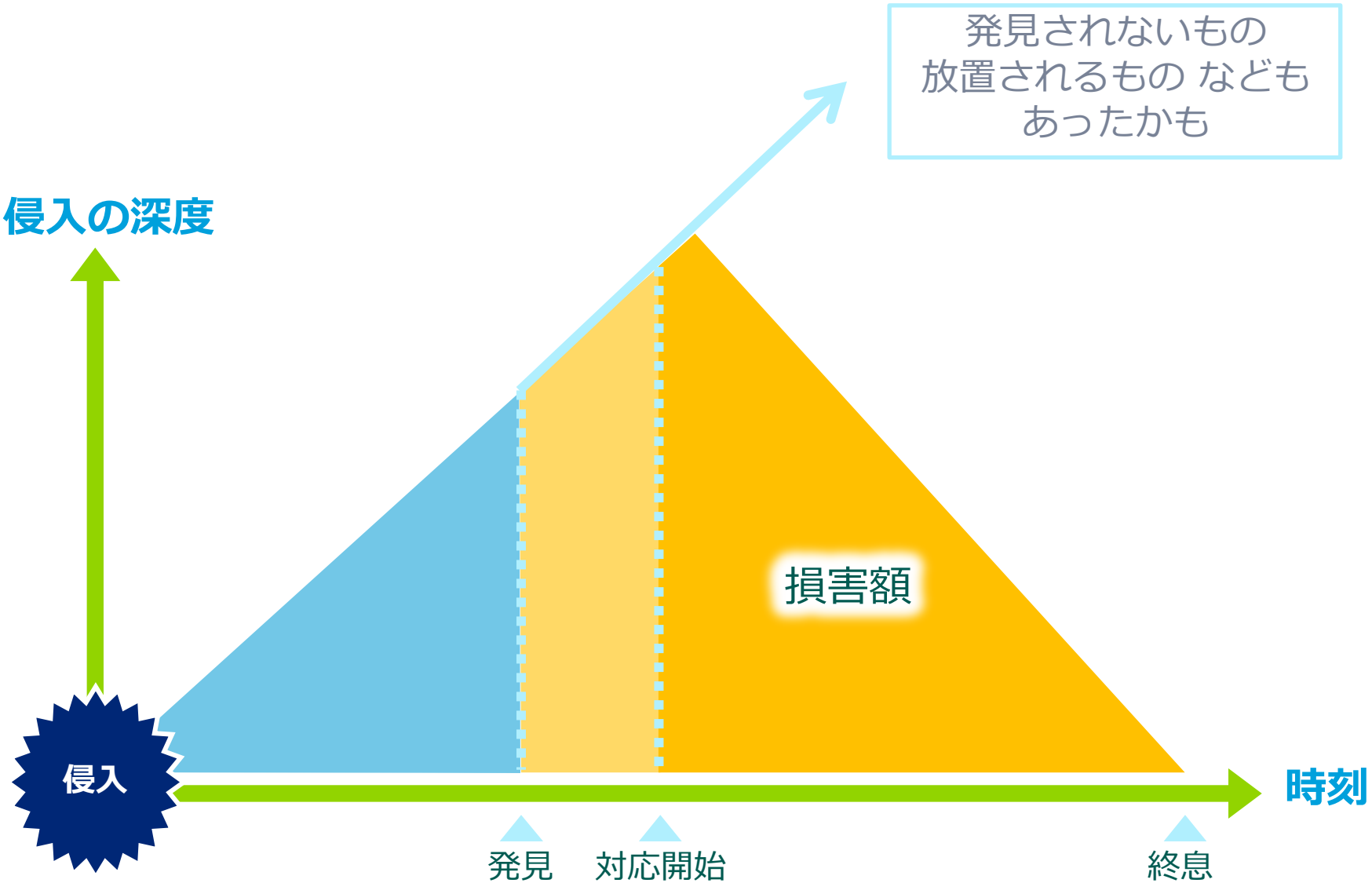
Phase 0 – 混沌の時代

1. 個々人の温度感/スキルに依存した対応レベル

2. ほぼ “response” のみ

3. 売上とか数字とかいろんなものを追いかけている
   スピードで振り切る作戦？？

Phase 0 – 混沌の時代



Phase 1 – GREE-IRT 黎明期

Phase 1 – GREE-IRT 発

- もう個人レベルでの対応は限

Phase 1 – GREE-IRT 黎明期

組織的な対応がスタート

- CTO を中心とした
  CSIRT 的なネットワーク

- セキュリティチームの発足

- プロセスの整備

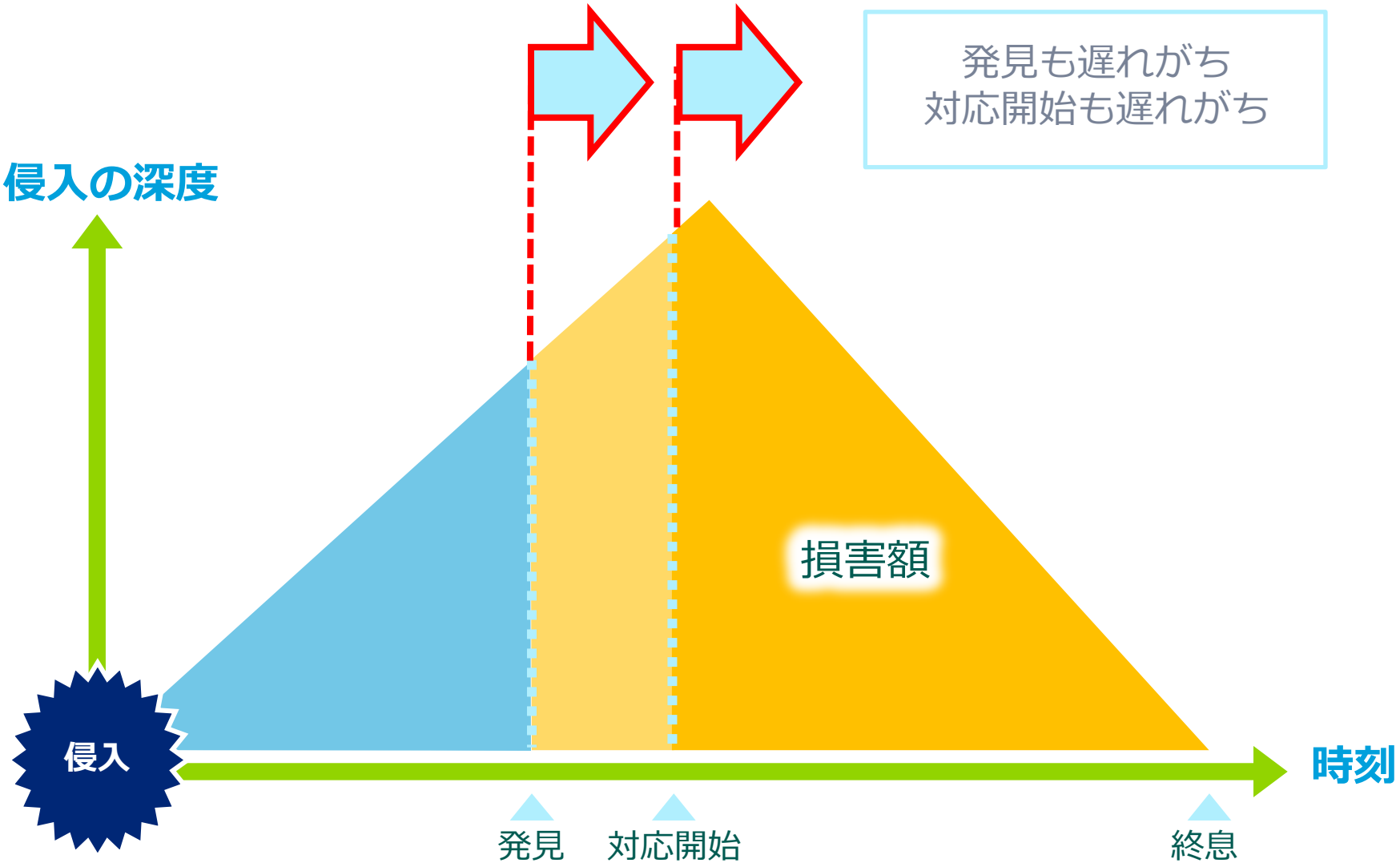
Phase 1 – GREE-IRT 黎明期

- とはいえ、まずは可視化大事

Phase 1 – GREE-IRT 黎明期

そして、すぐには結果が出ない・・・山積する課題

Phase 1 – GREE-IRT 黎明期



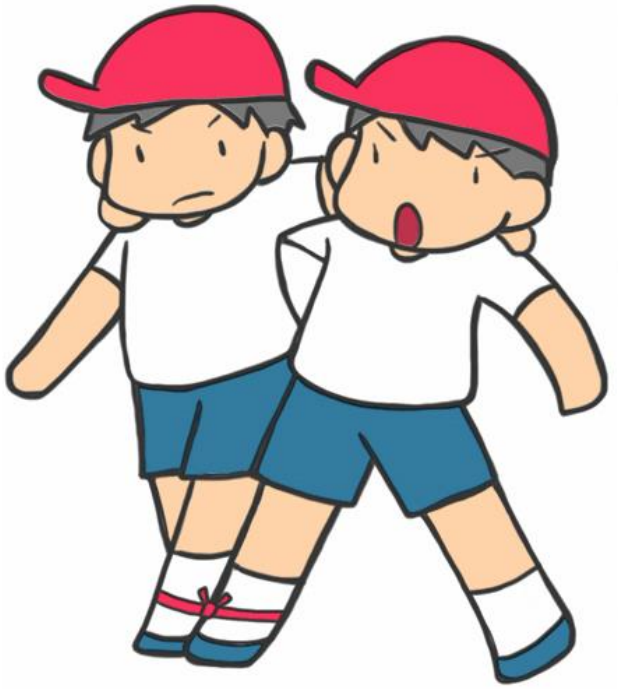
Phase 1 – GREE-IRT 黎明期

1. 組織はあるものの個人への依存度が高い
2. なにかと後手にまわりがち
3. 次々と新事実が判明し課題が増えていく

Phase 2 – SOC さんと二人三脚

Phase 2 – SOC さんと二人三脚

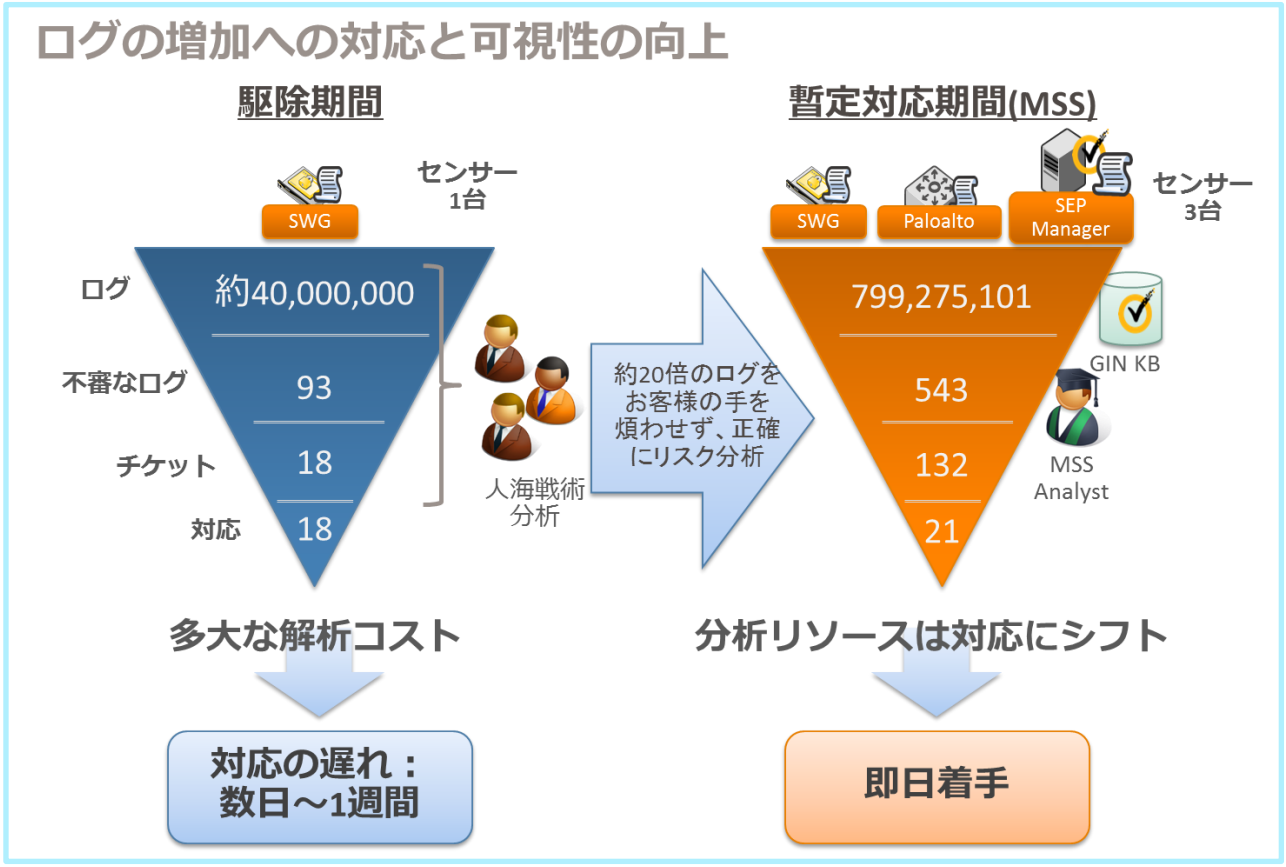
- どうすれば、もっと早く発見できるか
- どうすれば、もっと早く対応できるか



Phase 2 – SOC さんと二人三脚

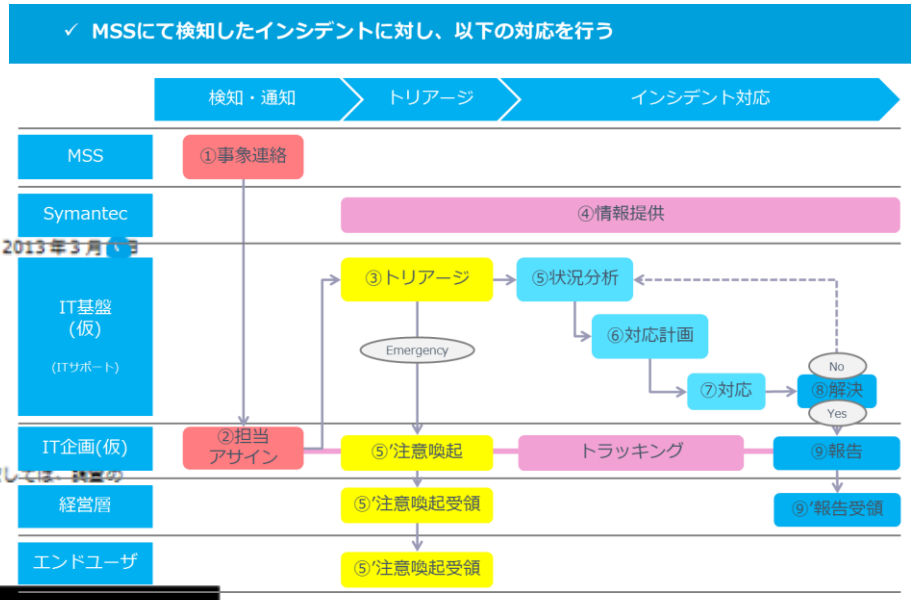
- どうすれば、もっと早く発見できるか
  - 見つけるためのセンサー追加
  - 発見に十分なログの取得
  - 相関分析と監視

ログの量は20倍に
発見までの時間は1/5に
＝100倍の効果！



Phase 2 – SOC さんと二人三脚

- どうすれば、もっと早く対応できるか
  - プロセスの細分化
  - 担当部門の役割と責任を明確化
  - 権限も必要（反発もある！



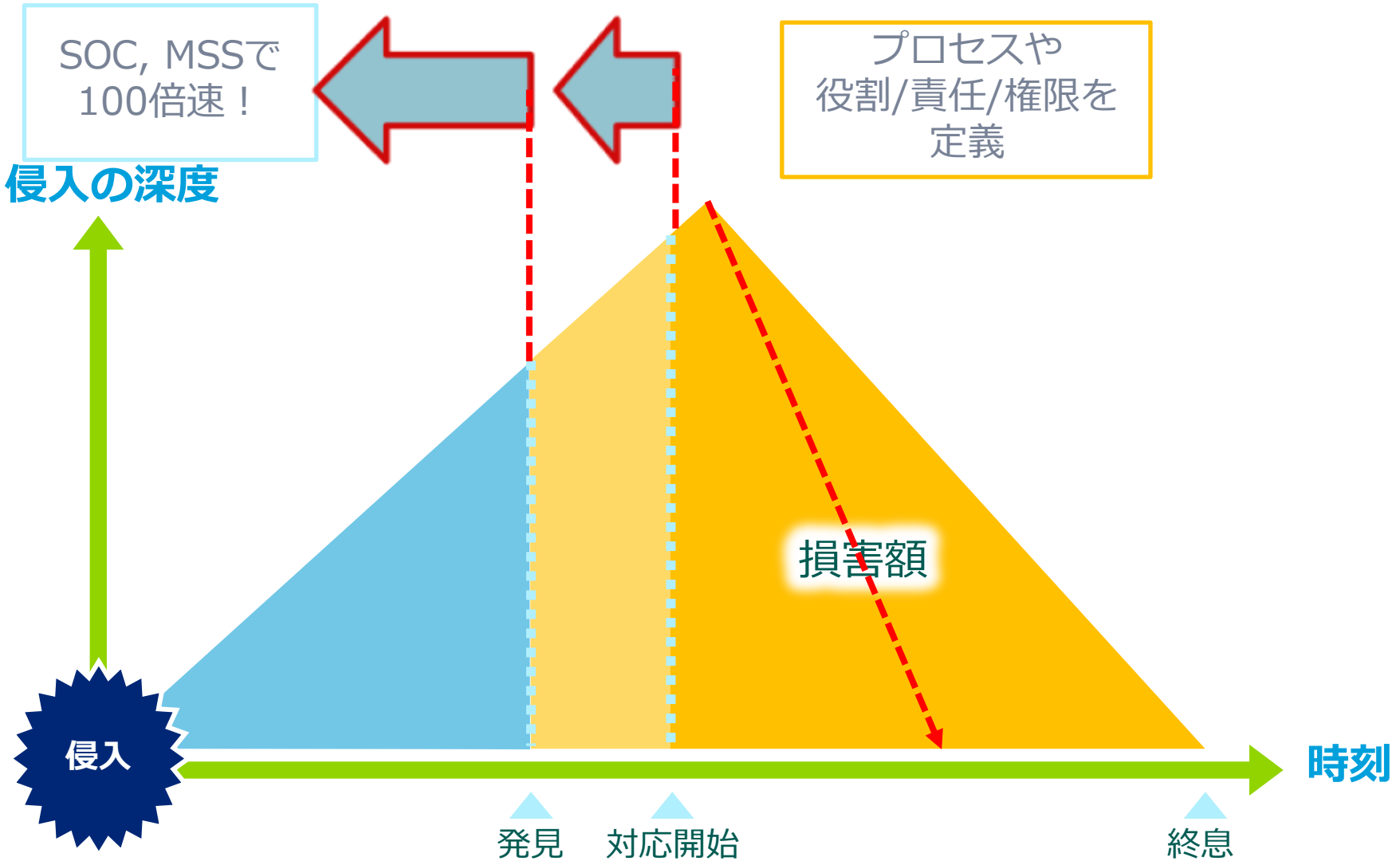
マルウェア感染調査協力依頼書

現在ご利用中の PC にウイルス/マルウェア感染の可能性が発見されました。つきましては、調査の
ためのご協力を賜りたく、お願い申し上げます。

記

	項目	情報
1	インシデント番号	インシデント番号を記入して下さい
	検知日時	2013 年 3 月 [redacted] 日 17:[redacted]
	ホスト名	[redacted] gree.jp
	ローカル IP	[redacted]
	インシデントカテゴリ （詳細は備考 1 参照）	☐ウイルス/マルウェア ダウンロード （ウイルス名：ウイルス名を記入して下さい） ☒ボット活動の疑い ☐不適切な PC の利用（ファイルのアップロード/アプリケーションの利用等）
2	登録された PC 使用者	使用者名：氏名を記入して下さい OS 種類：OS を選択してください
3	依頼事項 （詳細は備考 2 参照）	☒PC 使用状況のヒアリング ☐社内ネットワークからの隔離＋ウイルススキャンの実施

Phase 2 – SOC さんと二人三脚



Phase 2 – SOC さんと二人三脚

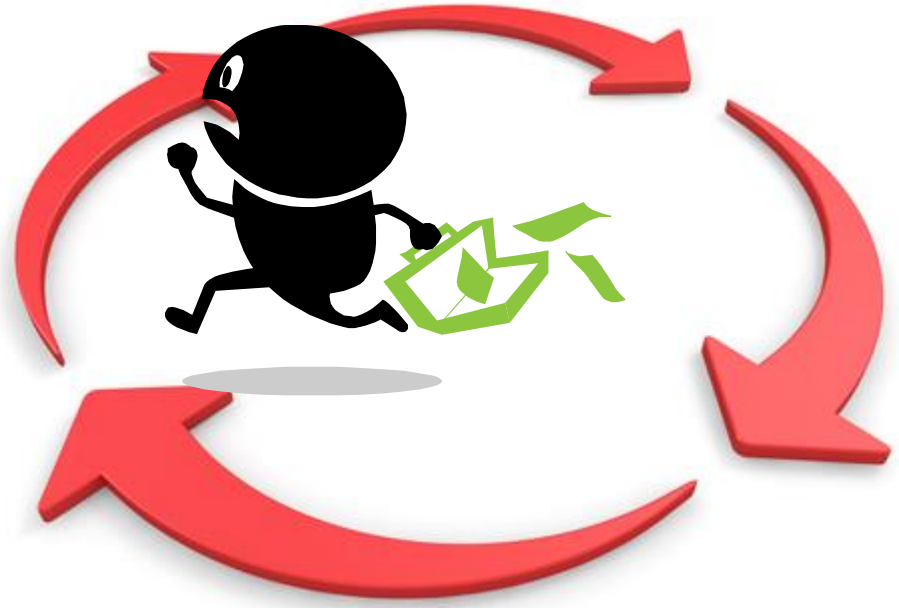
1. 専門家の活用による対応レベルの向上
2. タイムリーな対応
3. 現場からの反発に注意

Phase 3 – SOC さんとのこれから

Phase 3 – SOC さんとのこれから

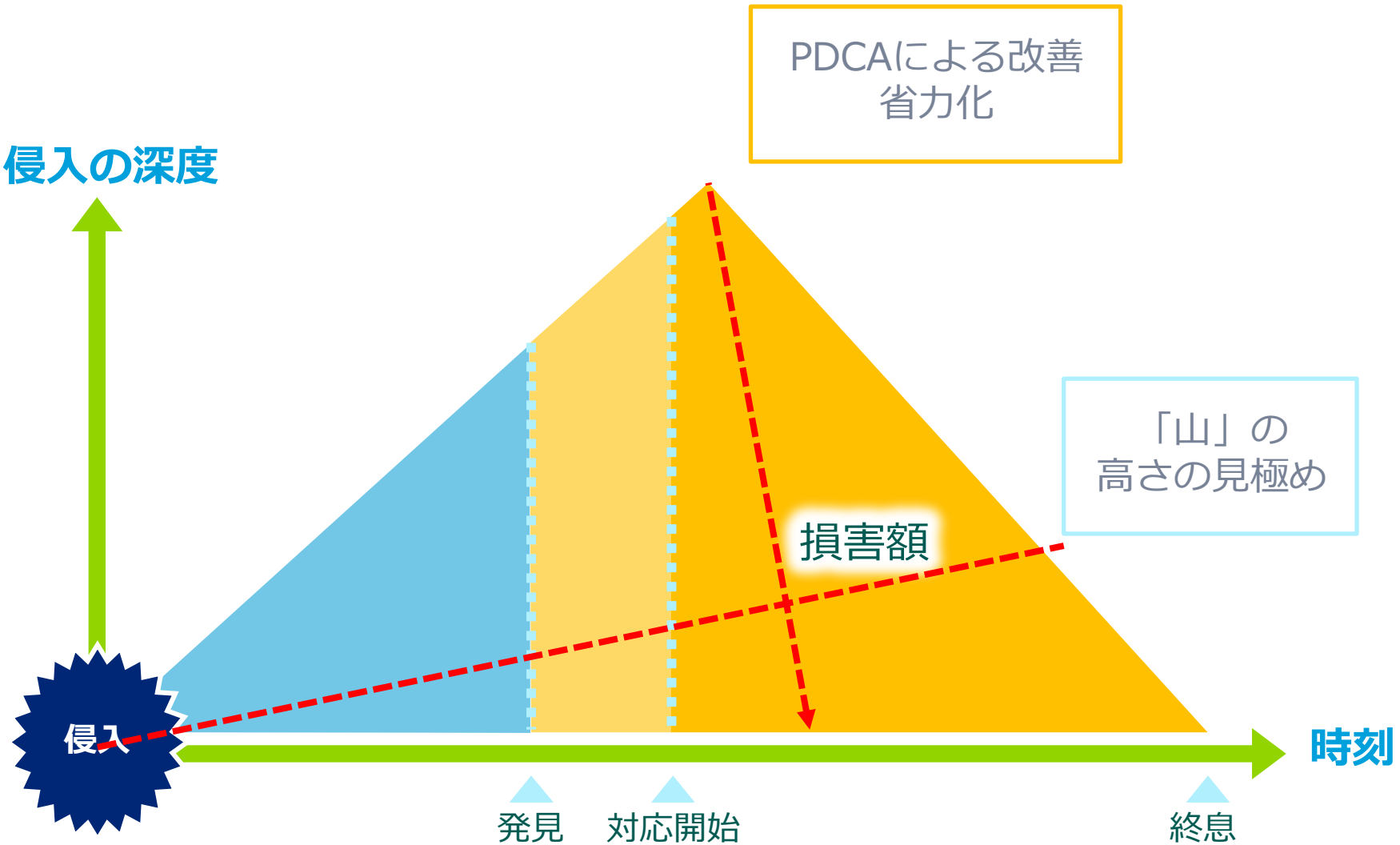
SOC + CSIRT の活動は、終わりなき戦い

- SOC + CSIRT の活動は、終わりなき戦い



Phase 3 – SOC さんとのこれから

Phase 3 – SOC さんとのこれから



Phase 3 – SOC さんとのこれから

1. 素早い発見、素早い判断、素早い対応
2. 先手が打てる体制へ
3. さらなる改善を目指す

3. Wrap up

Wrap up

- 頼れるところは頼るべし
- 可視化大事
- 特効薬はありません
  時間かかります

インターネットを通じて、
世界をより良くする。