

# SOCが悩むセキュリティ対応の現実 2015

**阿部 慎司**

日本セキュリティオペレーション事業者協議会  
NTTコムセキュリティ株式会社

## 自己紹介

### 阿部 慎司

- 日本セキュリティオペレーション事業者協議会(ISOG-J) 運営委員
- NTTコムセキュリティ SOC所属 高度分析チーム (L3) リーダー / シニアアナリスト

- NTT出版「.com Master★★ 公式テキスト」の執筆
- 技術評論社「Software Design」2015年7月号の執筆
- 日経BP社「経営としてのサイバーセキュリティ」に掲載

### ● Internet Week プログラム委員

#### ● 「Internet Week 2014」での講演

- CSIRT時代のSOCとの付き合い方: <https://www.nic.ad.jp/iw2014/program/s13/>

#### ● 「Internet Week 2015」での講演

- 150分でわかるセキュリティ対応できる組織にする10のコツ: <https://internetweek.jp/program/s13/>
- CSIRT時代のSOCとの付き合い方 2015: <https://internetweek.jp/program/s14/>



## 本日のお話

SOCの現場での実例をもとに

 **失敗パターン**

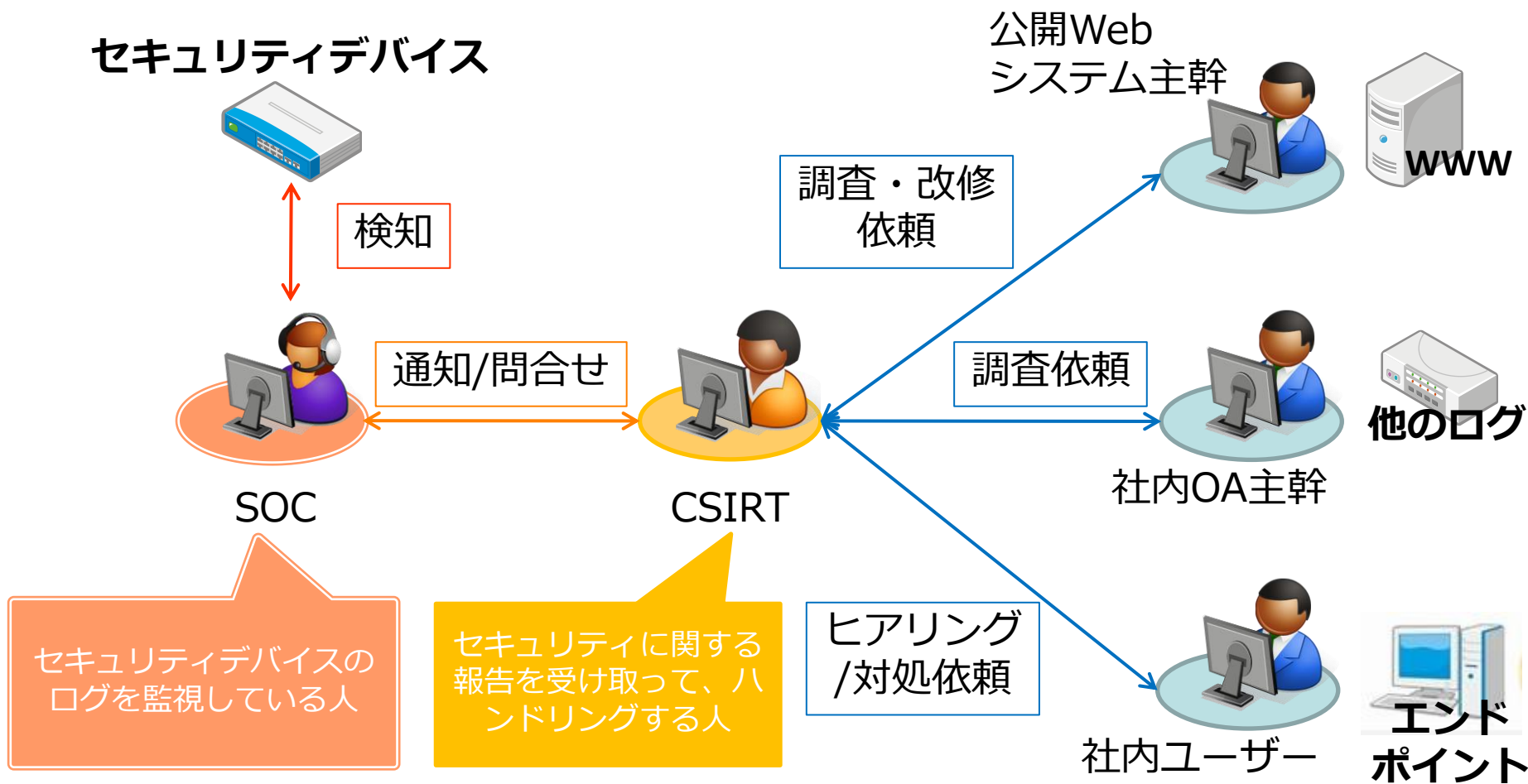
 **成功パターン**

をまとめながら、セキュリティ対応の難しさ、

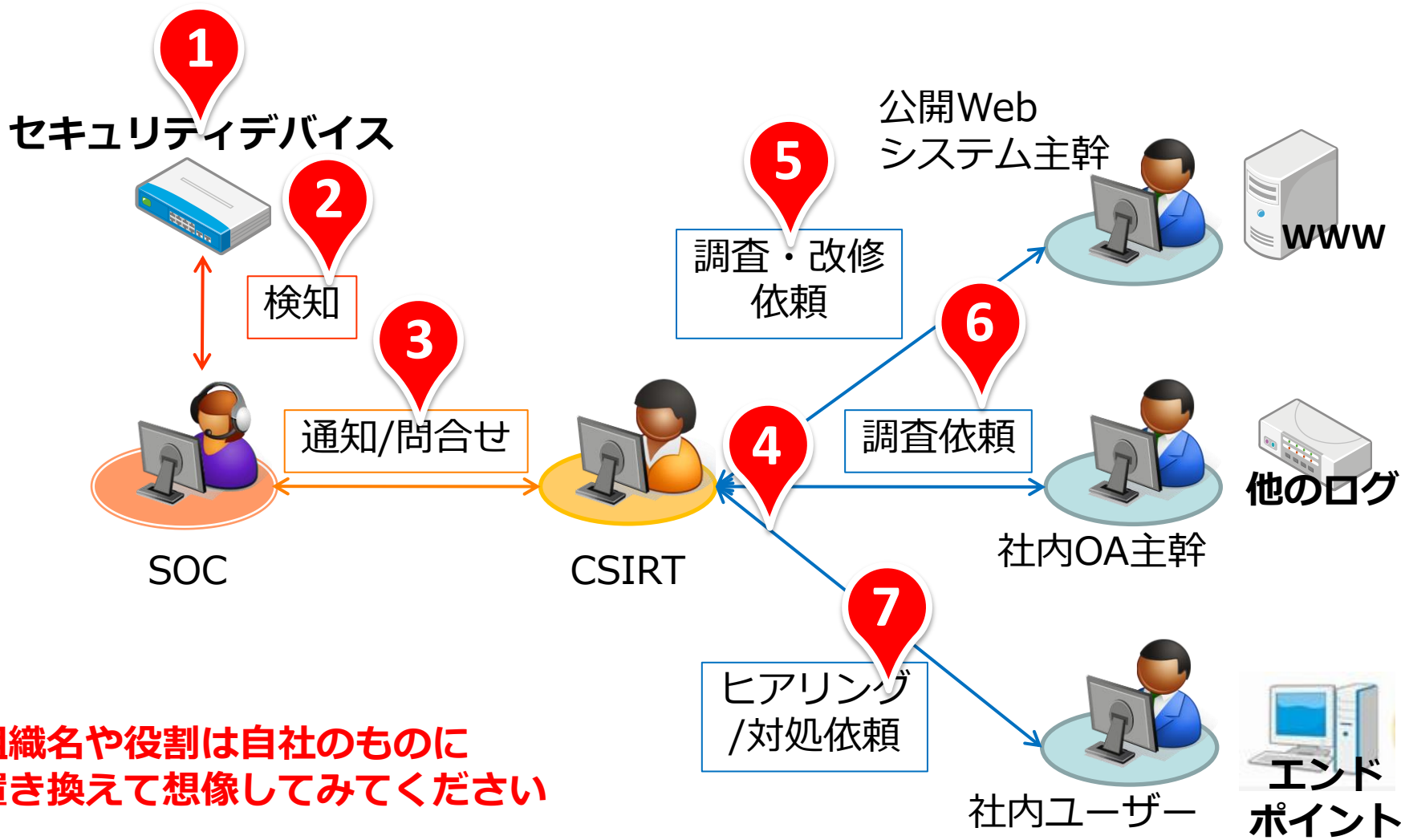
それをうまく解決していくための教訓を見出していきます。

# 今回想定するセキュリティ対応のモデルケース

※組織名や役割は自社のものに置き換えて想像してみてください



# 落とし穴がありがちな場所は・・・



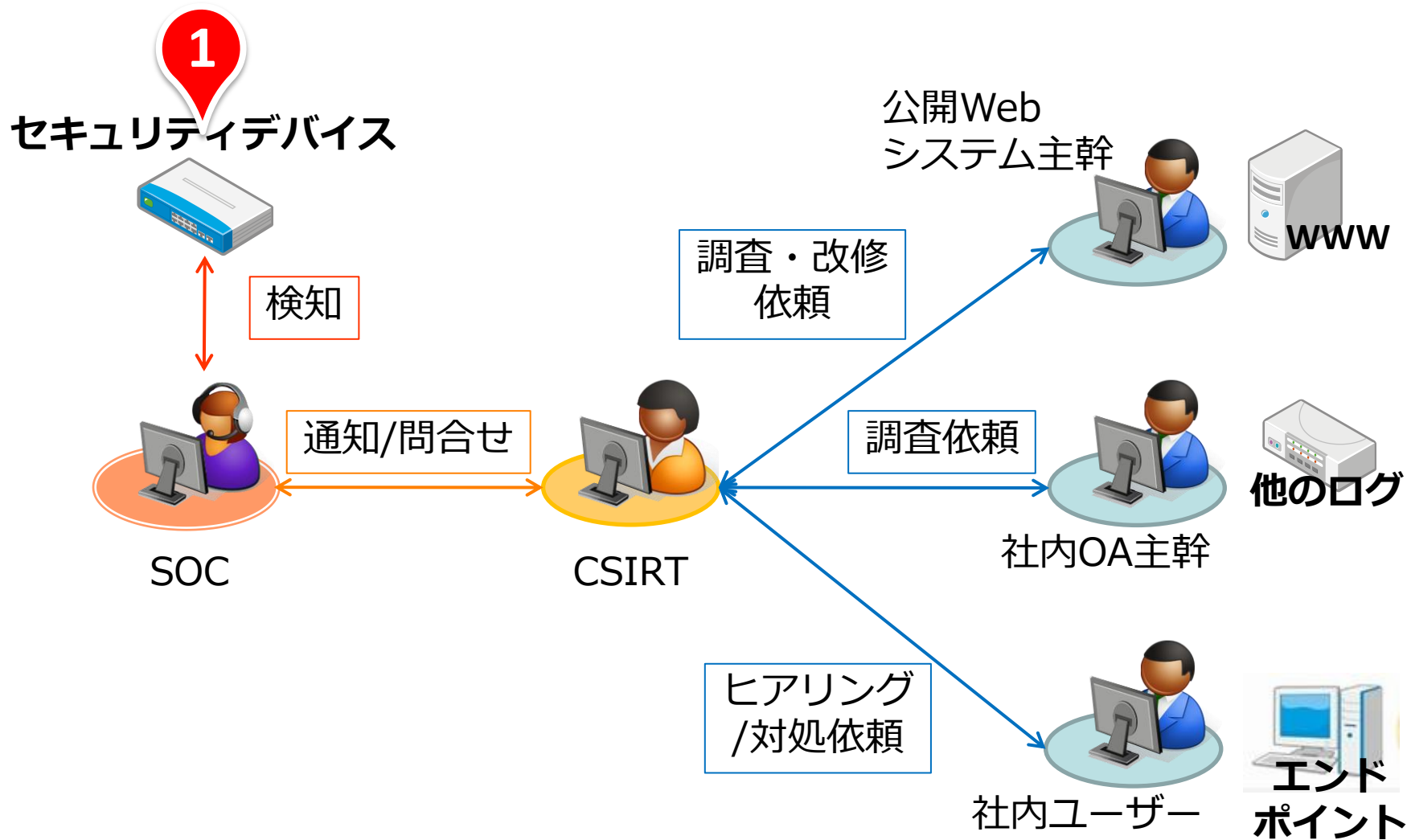
※組織名や役割は自社のものに置き換えて想像してみてください

# 落とし穴がありがちな場所は・・・



※組織名や役割は自社のものに置き換えて想像してみてください

# ①セキュリティ製品選択は適切？



## ①セキュリティ製品選択は適切？



- 偉い人に何とかしろと言われたので、取りあえず何か入れてみた
- セキュリティのセールスマンが良いって言うからそれにしてみた
- システム保守ベンダーにまるっとお願いしておいた



- 何を守りたいのか明確になっている
- 守るに当たり、現状の環境、状況を理解している
- 各セキュリティ製品が得意な部分、苦手な部分を把握できている



## ①セキュリティ製品選択は適切？



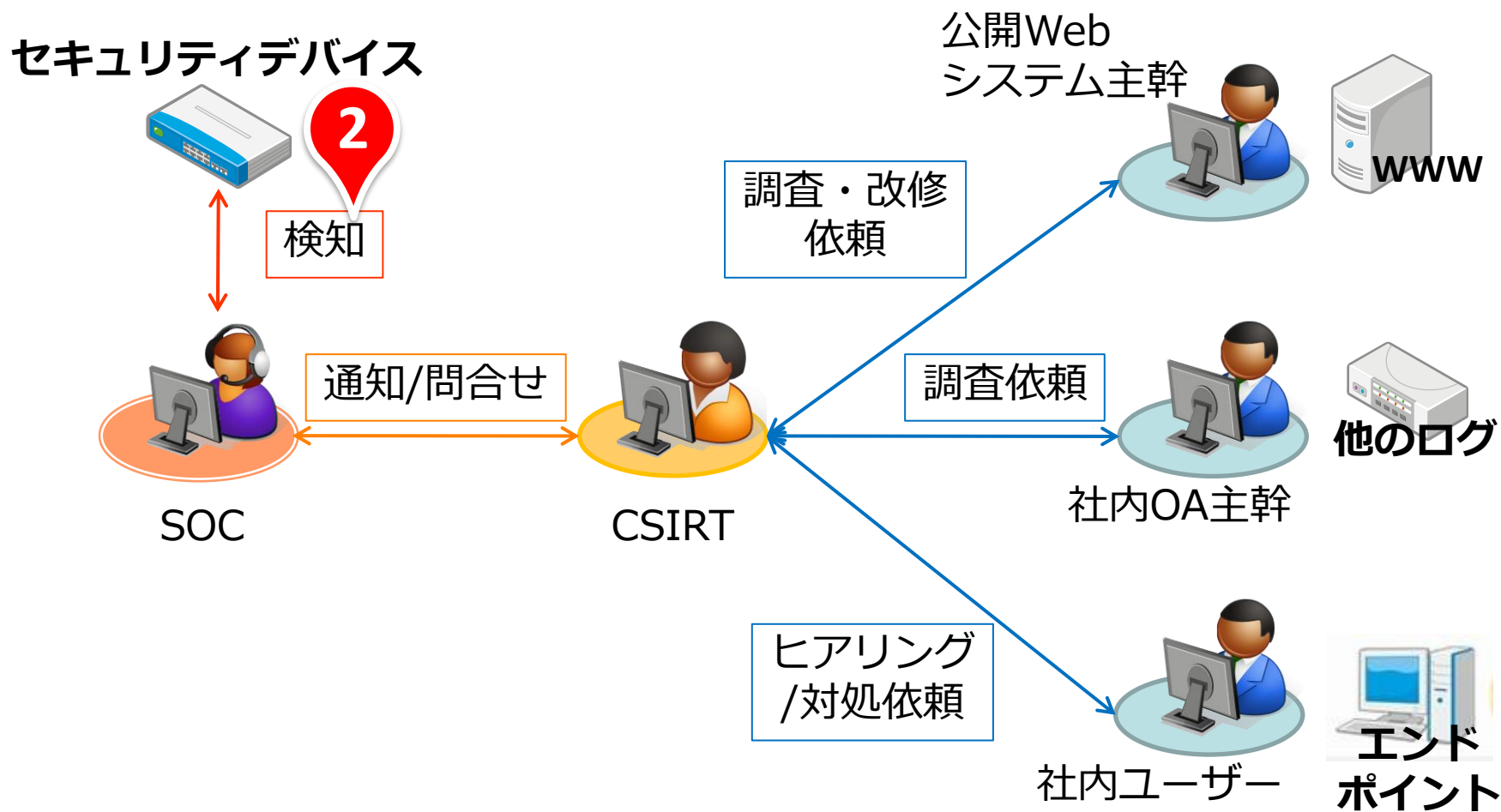
### 例

- 何を守りたいのか明確になっている
  - **自社の公開Webシステムを守りたい**
- 守るに当たり、現状の環境、状況を理解している
  - **自社の公開Webシステムは、実はWebサーバーだけではなく、メール配信サーバーも内包されている。また、外部からの作業用にFTPやSSHが一部許可されている状態。**
- 各セキュリティ製品が得意な部分、苦手な部分を把握できている
  - **「WAF」は基本的にHTTPに特化しているので、今回のシステムのように監視すべきプロトコルが幅広い場合は適さない場合がある。このようなシステムでは「IPS」の方がカバー範囲が広く有効。**

## ～ 教訓 ①セキュリティ製品選択は適切？ ～

- どんなシステムにもマッチするような魔法のセキュリティ製品はない
  - だからこそ防御目的に合ったものを選ぶ必要がある
- セキュリティ製品だけ横並べにした比較表に右往左往しない
  - 自社の環境、運用に合うかの方が大切
  - さらに言うと、使いこなせなければ本来の効果さえ引き出せない
- セキュリティベンダーにトライアルを依頼するもよし
  - 単なる機器のお試しにならないよう注意
    - 運用も意識したトライアルをして、自分たちには何ができて、どこをアウトソースすべきか検討する

## ②セキュリティ製品は嘘つき！？



## ②セキュリティ製品は嘘つき！？



- 危険度が高いと判定されたら無条件で対応している
- 危険度が低いものは件数も多くてキリがないので見ていない
- デフォルトの検知設定のまま使っている



- 危険度が高くても誤検知の可能性を理解している
- 危険度が低くても、その中に隠れた脅威を把握している
- 自社の環境に合わせ、検知設定を適切にチューニングしている

【参考】

セキュリティデバイスによる検知数

12,000,000

※infoレベルのシグネチャを除いても1,200,000



アナリストによる通知数

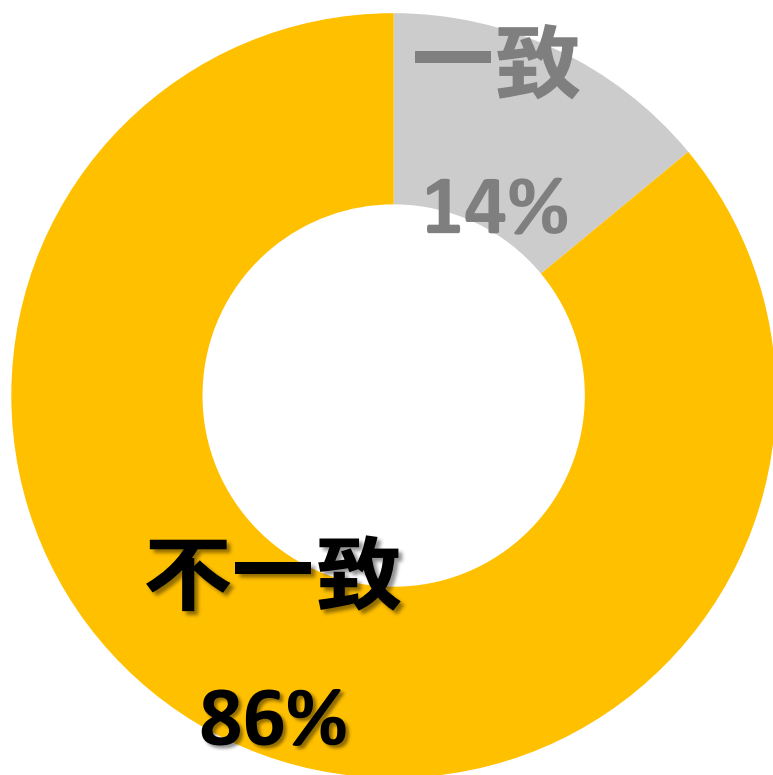
10

(1案件1か月あたりの平均値)

出典：  NTT Com Security

## 【参考】

## アナリストによる危険度判断とセキュリティデバイスによる 機械的な危険度判定が揃う割合はわずか14%



### • 25%は最悪の過小判定

- アナリストが**Critical**と判定したイベントのうち**25%**はセキュリティデバイスで**infoレベル** ⇒ 見逃しに直結

### • 全体的に過剰判定気味

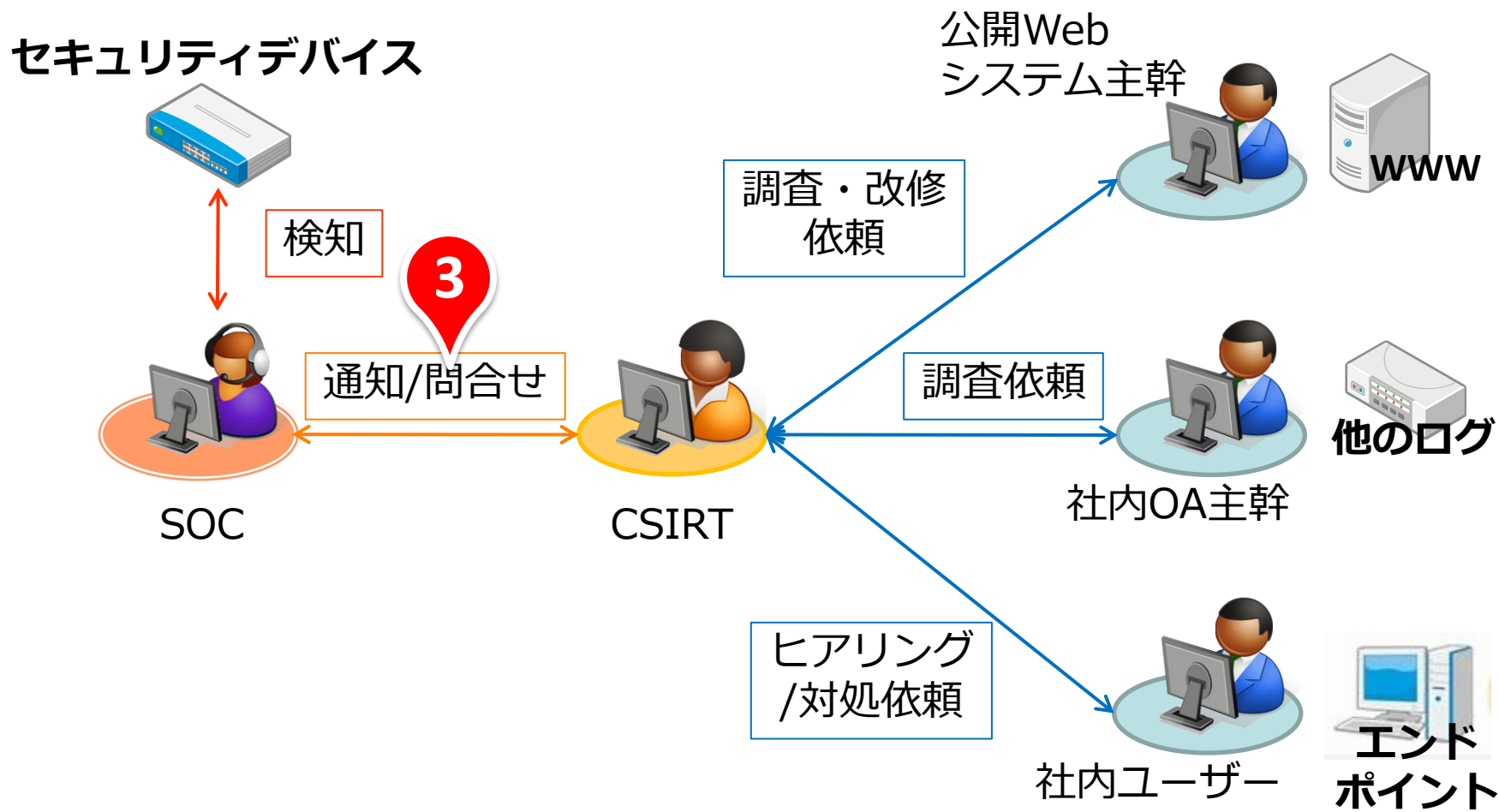
- 全てのアナリスト通知対象イベントのうち**81%**がセキュリティデバイスの方が危険度高め ⇒ 無駄な対応

出典：  | NTT Com Security

## ～ 教訓 ②セキュリティ製品は嘘つき！？ ～

- セキュリティ製品が必ずしも正解を出してくれているわけではない
  - 検知内容を理解し、**本当の危険度を見抜けるスキル**が必要
    - さもなくば、見逃しや無駄なセキュリティ対応が発生
- セキュリティ製品をデフォルト設定のままにするのはもったいない
  - **自分の環境に合わせた設定をしていくことがセキュリティ強化の面**  
でも対応の効率化という面でも大切
- 有スキル者がいなければアウトソースも検討

### ③通知と問合せに潜む罠





### ③通知と問合せに潜む罠



- とにかく早い方が良いのだから内容はさておき通知は早く！
- 問合せは、聞きたいことだけ聞きっぱなし
- 外部からの情報がトリガーになって問合せ祭り



- きちんと分析したうえで適切な通知を行う
- 問合せは、お互いの情報共有の場ととらえて対応する
- 外部情報はしっかり咀嚼して、冷静な対応

### ③通知と問合せに潜む罠



例

◆ とにかく早い方が良いのだから内容はさておき通知は早く！

s: 「（まだ良くわかってないけど...）取り急ぎ通知します」

c: 「至急詳細な報告を！（なんだかわからん...）」

s: 「（んー調査が不完全...でも至急って言われた）こんな感じです」

c: 「対応は必要なのでしょうか？（はっきりしないな...）」

s: 「（調査終わった!）こういう事象なのでこう対応してください」

c: 「了解しました。対応開始します。（やっとわかった!）」

**誰も得をしていない無駄な対応...むしろ  
問合せ対応のために余計に時間がかかっている...**

### ③通知と問合せに潜む罠



例

◆問合せは、聞きたいことだけ聞きっぱなし

c: 「○○はどうすればよいでしょうか。」

s: 「（急にどうしたんだろう）□□□がよいかと。」

c: 「聞きたいのは△△です。（伝わらない...）」

s: 「（ん？なんか背景があるのかな？）であれば◇◇◇ですね！」

c: 「理解しました！（なっとくなっとく。おわりー。）」

s: 「（最終的にどうなったのだろうか...）」

**問合せの背景や、対応の結果などは  
お互い共有しないと、すれ違いが発生する**

### ③通知と問合せに潜む罠



#### ◆外部からの情報がトリガーになって問合せ祭り

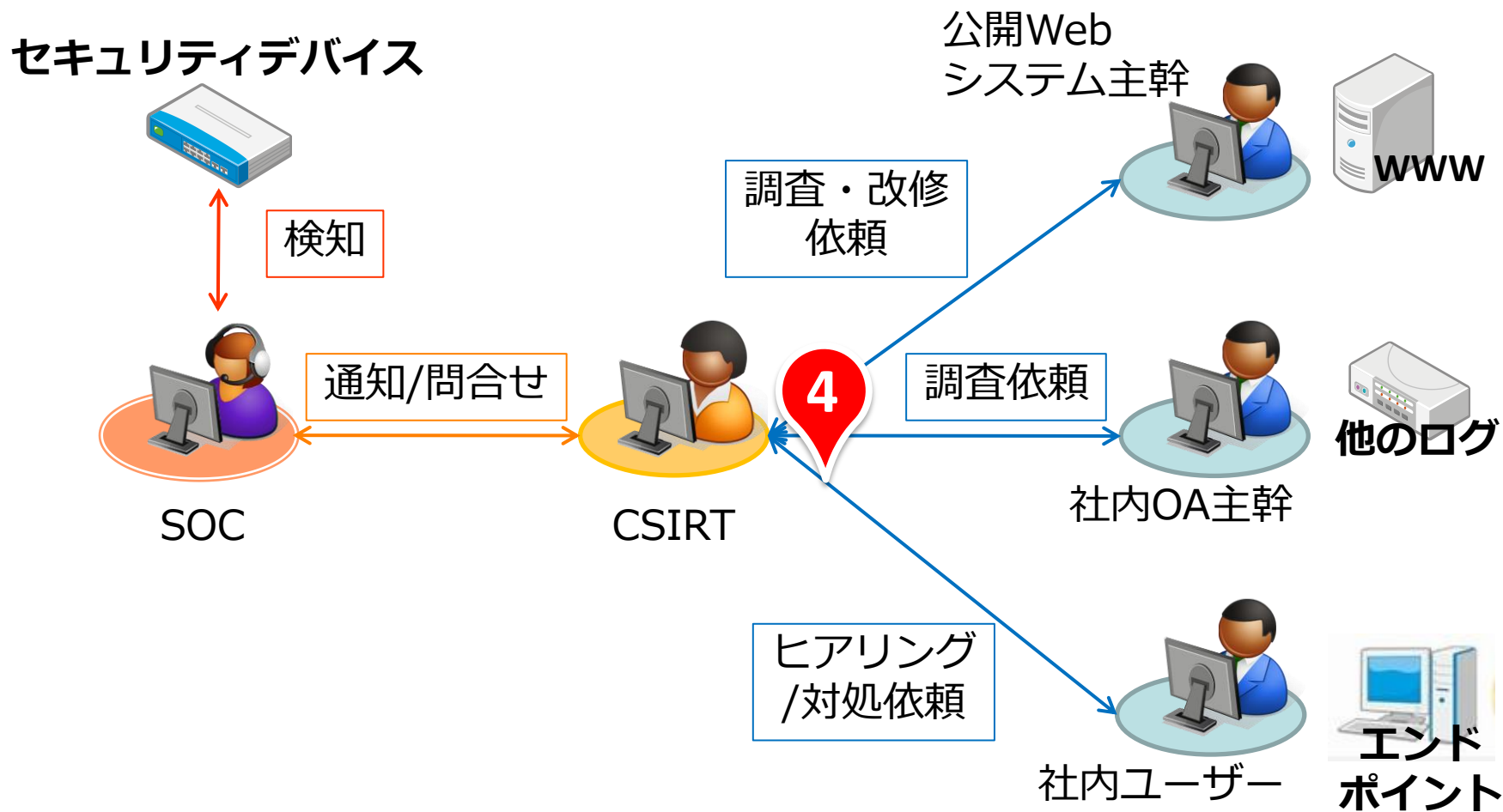
- あるある その1
  - 何かのニュースを見た偉い人が心配しだして、急に口を出し、社内騒然
- あるある その2
  - たいした攻撃でもないのに、いつのまにか「標的型攻撃だ」と煽られて、セキュリティ界隈がざわざわする
- あるある その3
  - 外部機関から、システムが踏み台にされている等の連絡が来る

**いずれのパターンもとにかく冷静に  
淡々と情報整理と現状把握を最優先**

## ～ 教訓 ③通知と問合せに潜む罠 ～

- 通知が早ければ早いほど良いというのは幻想
  - 対応の開始、対応の完了まで含めて全体が早くなることが大切
    - 「15分で通知」のような画一的なルールは、無駄な通知を増やしたり、問合せが増えてしまったりと、かえってその後の対応に悪影響を及ぼす
    - 特に昨今の高度な攻撃は15分で調査が終わるほど甘くない
- 問合せの際は、お互い仲間なので、しっかりと背景や、対応の結末を伝え合い、円滑なコミュニケーションを心がけるべし
  - 最終的なコミュニケーション総コストを低減できる
  - 同じレベルで会話できるということも重要なので、互いにしっかり勉強すべし
  - 両組織が社内にあるなら一つの組織のように振る舞えるとベスト
- 外部からの情報こそ冷静に対応し、踊らされず、確実に対処
  - 特に、インパクトがわからないときは、「何が何でも対策だ！」の前に、「ぶっちゃけどのくらい影響のある話ですかね？」とsocに聞いてみるのが吉
    - 冷静な意見が聞けるはず

# ④通知きたけど何するんだっけ？



## ④通知きたけど何するんだっけ？



- 通知がくるたびに、何をどこまで対応するか苦悩する
- 通知がくるたびに、誰と話をするべきなのか苦悩する



- 通知内容、危険度に則した対応を行う
- 問題発生個所に対応する管理責任者を明確にしておく

# 【参考】アクションカード

簡易的な対応表を作っておくだけで大違い

#	タイプ	説明	危険度			
			Informational	Medium	Serious	Critical
100	不正アクセス	脆弱性を突く攻撃や、認証突破を試みるアクセス	-	-	攻撃成功の可能性が高い場合	攻撃成功が明白な場合
200	DoS攻撃	サービス不能状態に陥れるような通信	-	影響は見られていないがDoS攻撃が発生している場合	-	サービス不能状態が確認された場合
300	マルウェア	マルウェアのダウンロードおよび感染後挙動	-	アドウェア等好まれざるプログラムの挙動が確認された場合	マルウェアのダウンロード成功が確認された場合	マルウェアの感染が確認された場合
400	不自然な通信	一般的なポリシーに違反するような通信や設定不備が疑われるような通信	不自然な通信が確認された場合	-	-	-
500	調査行為	ネットワークスキャン、脆弱性スキャンなどの調査行為	-	継続	-	-
600	その他	上記に分類されないもの	その他	-	-	-

#	タイプ	説明	Informational	Medium	Serious	Critical
100	不正アクセス	脆弱性を突く攻撃や、認証突破を試みるアクセス	-	-	-	-
200	DoS攻撃	サービス不能状態に陥れるような通信	-	-	-	-
300	マルウェア	マルウェアのダウンロードおよび感染後挙動	-	-	-	-
400	不自然な通信	一般的なポリシーに違反するような通信や設定不備が疑われるような通信	-	-	-	-
500	調査行為	ネットワークスキャン、脆弱性スキャンなどの調査行為	-	-	-	-
600	その他	上記に分類されないもの	-	-	-	-

インシデントの種類

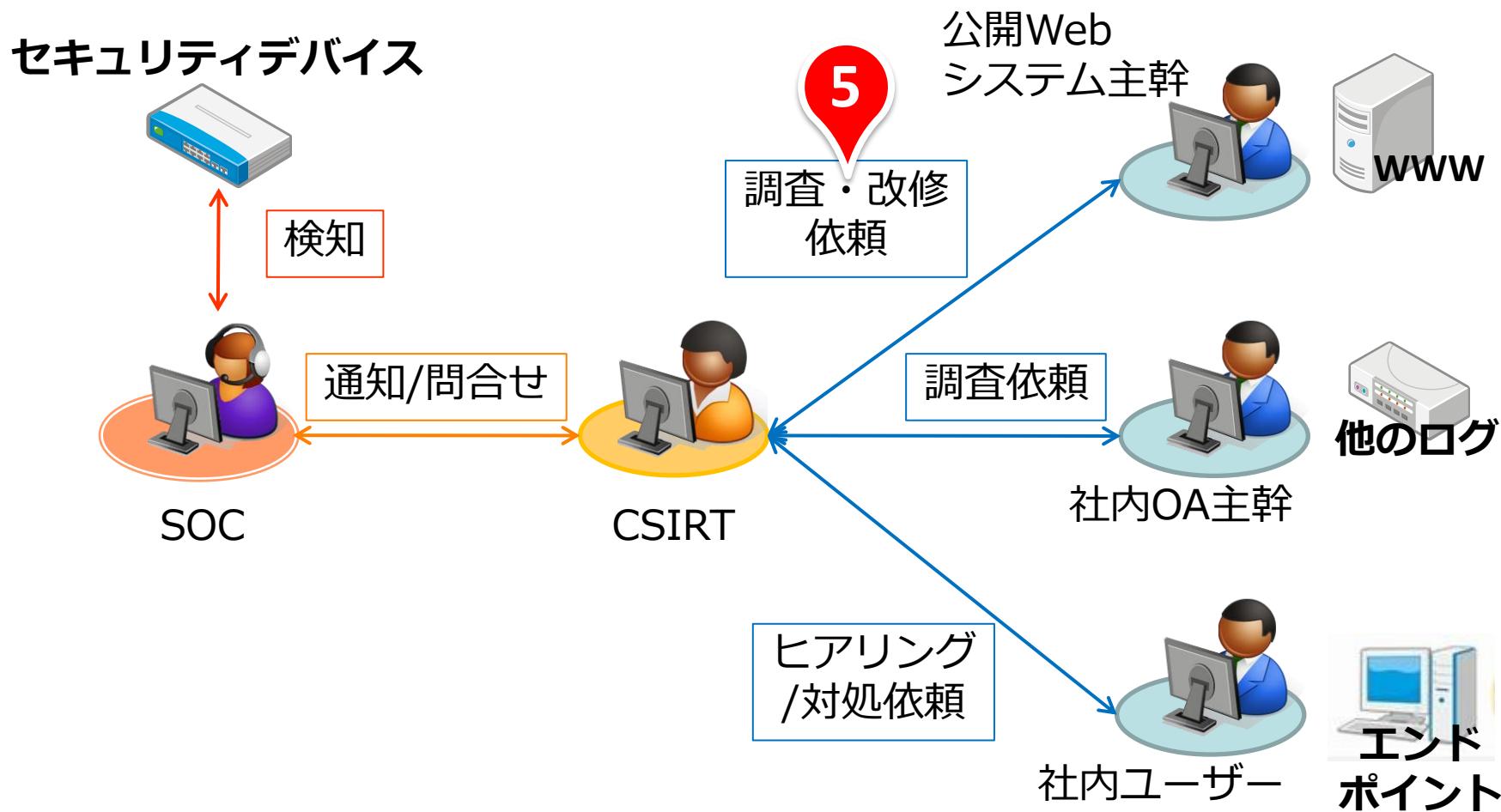
誰がどのシステムに対して何を対応するのか対応表を作る



## ～ 教訓 ④通知きたけど何するんだっけ？ ～

- 想定可能な範囲で構わないので、発生する事象、**危険度に応じたアクションを決める**べし
  - 初めから完璧を目指して、細かな対応表を作ろうと思わない
    - おそらく関係者との調整だけで疲弊しきってしまう...
    - とにかくまずはアクションのトリガーを引ける重要人物を味方にする
- 必ず想定外のことが起こるので、その都度、アクションの内容等を見直し、**反映、浸透させる営み**も事前に定めておくこと
- 定期的なセキュリティ対応演習を行うこと
- 本格的な営みとしては、BCP（事業継続計画）へ「サイバーセキュリティ」を組み込むことが目標となりえる

# ⑤脆弱性にはすぐに対応できない？！



## ⑤脆弱性にはすぐに対応できない？！



- 脆弱性が見つかり連絡したのに、気にしてもらえない
- どうにか理解してもらえたのに、今期は直せないと言われる



- 脆弱性を連絡すると、すぐに調査が開始される
- 脆弱性が明確になり次第、すぐに改修が開始される

## ⑤脆弱性にはすぐに対応できない？！



- 脆弱性が見つかり連絡したのに、気にしてもらえない
- どうにか理解してもらえたのに、今期は直せないと言われる

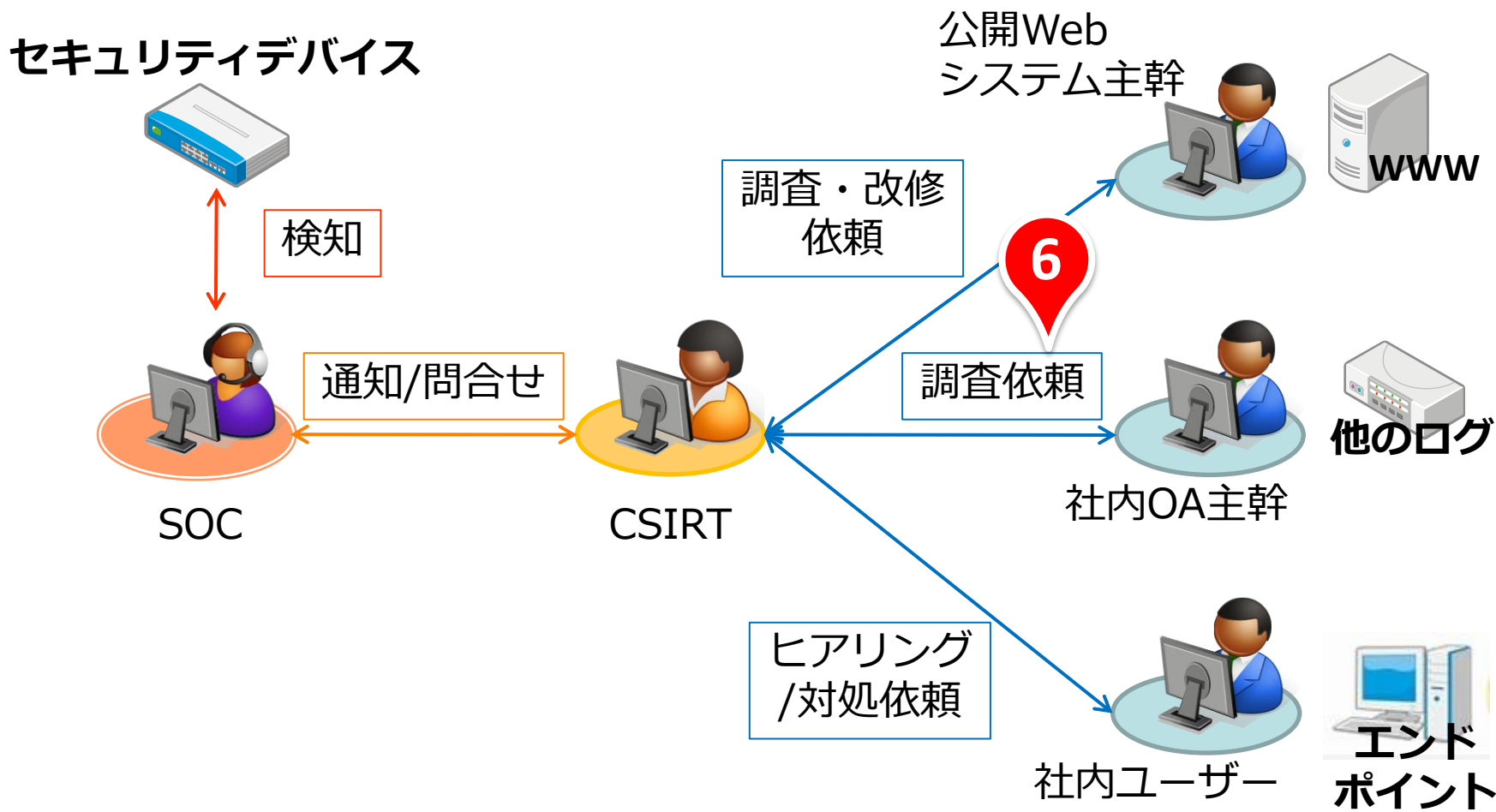
- **意識の低さ**
  - ✓ 「今まで特に何も起きてないし、うちは大丈夫でしょ」
- **権限の不足、権限が及ばない**
  - ✓ 開発、保守が別会社でストレートに命令できない
  - ✓ 相手が親会社なので意見を通しにくい…
  - ✓ 同じ社内だが、こちらの方が組織的な地位が低い…
- **コスト/リソースの問題**
  - ✓ 「今期予算取ってないので…」
  - ✓ 「新機能リリース直前で稼働が無いから、ちょっと今は…」

**適切な権限、予算、体制/ルール整備が大切**

## ～ 教訓 ⑤脆弱性にはすぐに対応できない?! ～

- まずはセキュリティに対する意識改革
  - 事故が起これば嫌でもわかる（が、そういうわけにもいかないで...）
  - 社内にすでにある開発ガイドライン等にセキュリティの項目を組込めないか検討
    - 新規、追加開発時など、節目でのセキュリティチェック等
  - 開発や保守、運用に関する契約に、セキュリティ対応を含める
- 本格的には、**権限の明確化**が必要
  - きっちりドキュメント化する（アクションカードを発展させ公式な文書に昇華）
  - 予算やリソース配分にパワーを持つ組織/役職の直下に対応の起点となる組織を作り、  
配置できると理想的
- **セキュリティ対応に敏感に反応し、自然と対応が走る組織文化に変える**

# ⑥ログをください！



## ⑥ ログをください！



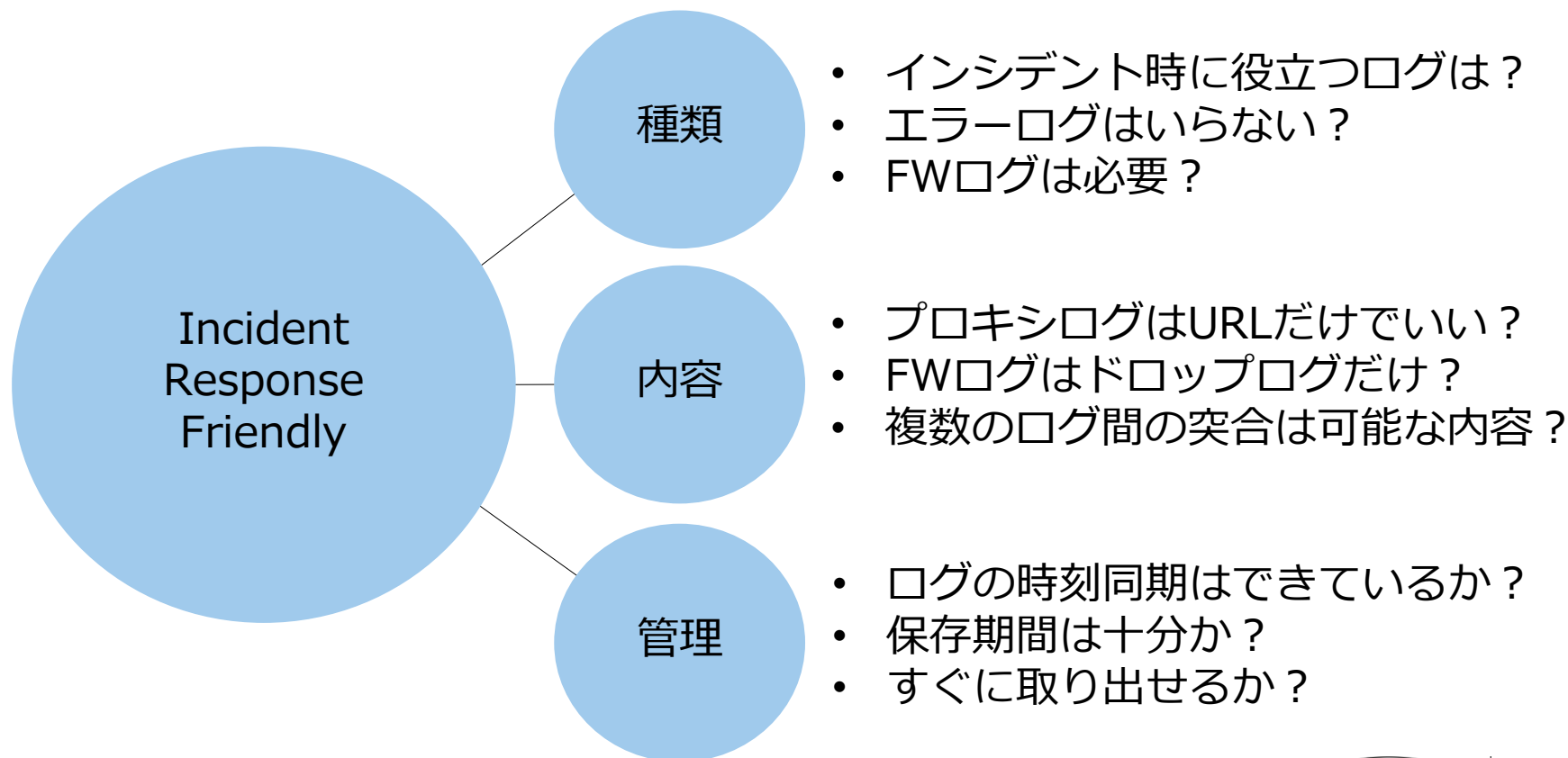
- 詳細な調査のために必要なログがない...
- ログはあるのに手に入れるまでにすごく苦勞する



- セキュリティ対応に必要なログが、種類、保持期間ともに十分
- 必要なときに必要な分、ログを手に入れることができる

## × 詳細な調査のために必要なログがない…

### インシデントレスポンスを意識した (Incident Response Friendly) ログの収集が必要



出典：  NTT Com Security



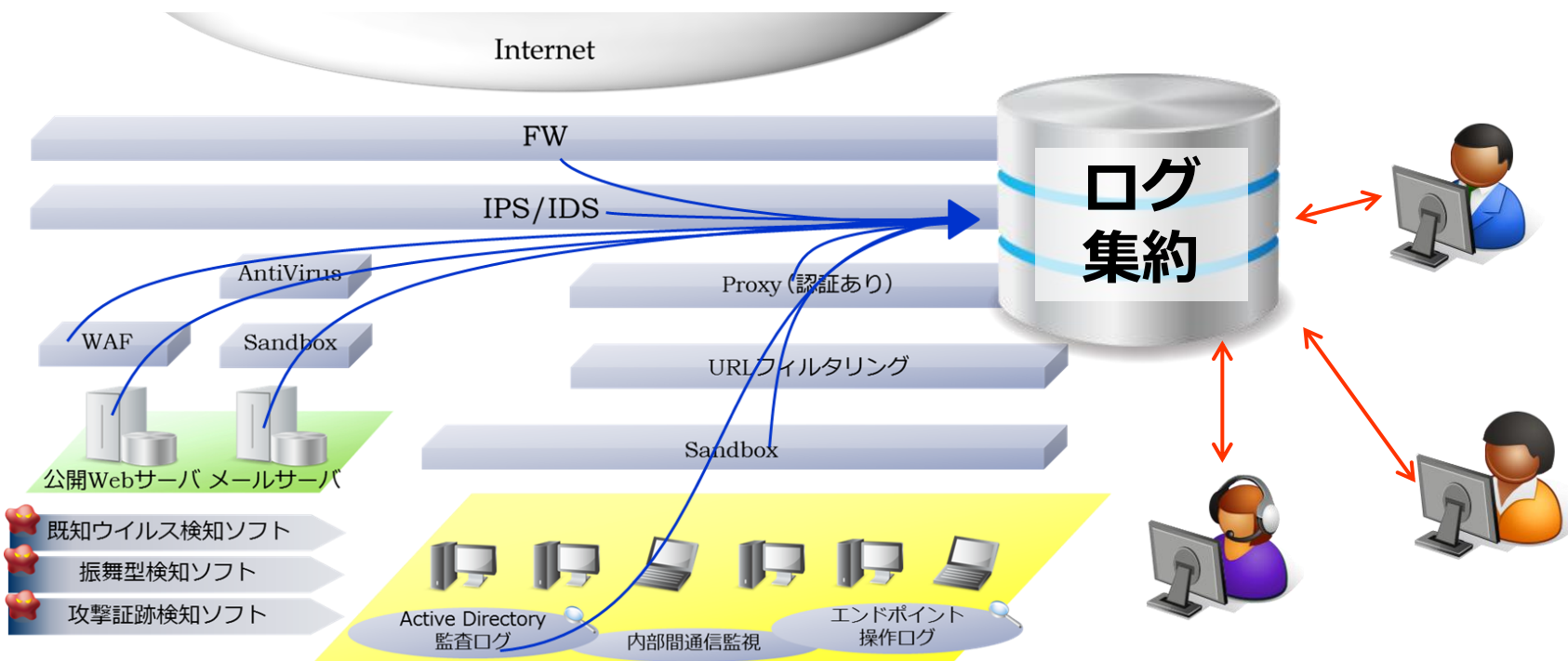
# × ログはあるのに手に入れるまでにすごく苦勞する…

## 原因 3例

- **体制面（組織の壁）**
  - ✓ ログ取りが依頼先にとっては面倒な作業でしかなく敬遠される
- **制度面**
  - ✓ ログの管理規定が厳しく、手続きが難しいいうえ、時間がかかる
- **システム面**
  - ✓ テープバックアップなど取り出しにくい形で保管されている
  - ✓ 膨大なログがあり、単純に抽出処理に時間がかかる

# 生きたログにするために…

SIEMなどを活用し、複数の組織からアクセスでき、適切な管理権限を与えながら、スムーズなログ検索が可能となる仕組みを実現する

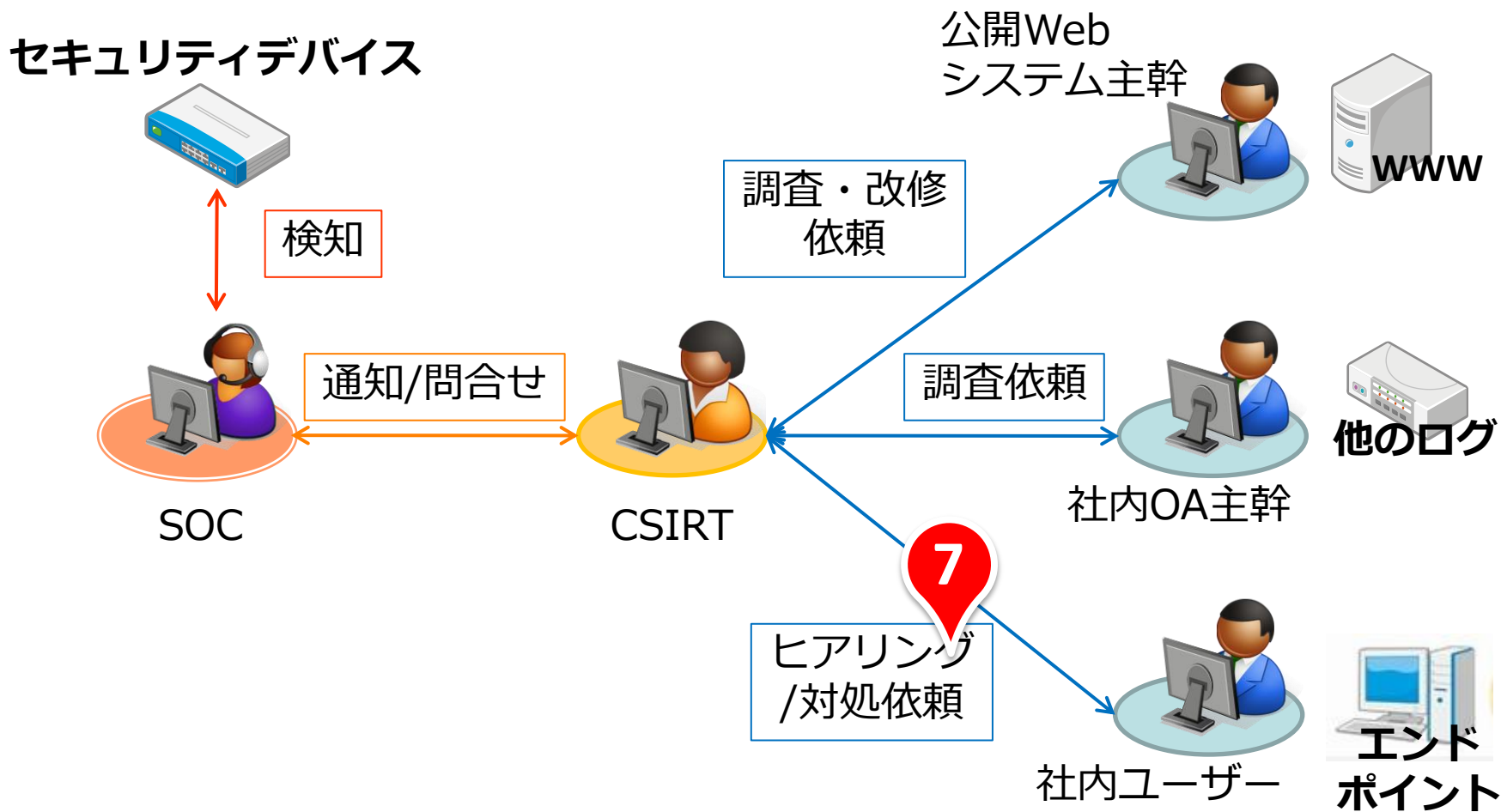


出典：  | NTT Com Security

## ～ 教訓 ⑥ログをください！ ～

- インシデントレスポンスを意識したログの収集を行う
  - まずは現状を把握。どんなログを、どのくらい保持しているか
  - セキュリティ対応の中で不足したログは取得を検討する
- 組織の壁は、権限の明確化や、緊密なコミュニケーションにより低くしていく
- 収集したログを「生きた」状態にするためSIEM等の活用を検討する
  - 様々な製品があるのできちんと活用シーンを踏まえて選択する
  - あるもの全部取る！というのはコスト的にもリソース的にも勿体ないので、上記の通り、自社でのセキュリティ対応に何が必要なのか良く考える
- 自社での検討が難しければ、セキュリティ事業者へ相談してみる
  - ログの分析への活用についても相談するとよい
  - 分析が難しいものはアウトソースも検討

# ⑦業務とセキュリティどっちが優先？



## ⑦業務とセキュリティどっちが優先？



- 端末を調査させてほしいというと怒られる
- セキュリティ製品で遮断設定を強めにしたらクレームの嵐
- 偉い人の端末だから対応しにくい



- 調査や通信遮断が、結局は身を守るためだと理解してもらう
- 役職は関係なく、淡々とアクションを行う

## ～ 教訓 ⑦業務とセキュリティどっちが優先？ ～

- 研修などを通して自社で行っているセキュリティ対策を全社員へしっかり伝える
  - そのうえで、各社員においてはどのような対応が求められるのか明確にする
  - 合わせて、その対応が会社や本人を助けるものであることを理解してもらう
  - ISMSなど、すでに社内に浸透している営みがあれば、そこへからめて理解促進を
  - セキュリティ対応に聖域なし
- 起きたインシデントは解決した後に、事例として公表する
  - セキュリティ対応についてよりリアルに感じてもらう
  - 毎月のインシデント件数などを定期的に公表するのもよし
- とにかく、どうにかセキュリティに対する意識を保たせる

## まとめの教訓

セキュリティ対応は落とし穴ばかり。

本当に困ったら誰かに相談しよう。



























**お金ある ⇒ コンサルを受けてみるべし**

**お金ない ⇒ コミュニティに参加して情報交換すべし**





参考：「セキュリティ対応できる組織にする10のコツ」対応表  
(<https://internetweek.jp/program/s13/>)

1. 防御から対応までのすべてをSOCに統合せよ  
2. 規模と透明性/俊敏性のバランスを取れ   
3. SOCに適切な権限を与えよ  
4. できる事をやろう       
5. メンバーは量より質を重視せよ  
6. 買った技術は最大限利用せよ   
7. データを集めて整理せよ  
8. SOCの任務遂行を保護する  
9. 脅威情報の賢い消費者であり供給者であれ   
10. 冷静に・計算高く、プロらしく対応せよ 