TRANSITS

運用について

v6.2 2017/3/30

代表執筆者: : Olivier Caleff
共同執筆者: Don Stikvoort, Baiba Kaskina

目次

1. インシデントレスポンス入門
目次

最初のエクササイズ

- サンプルケース – 緊急時のハンドリング

1.インシデントレスポンス入門
1 – エクササイズ

- シナリオ:
  - **反対側の部屋の倉庫が燃えている。**
  - **水が入ったタンク、グラスがある。**
  - **私たちで火を消さなければいけない!**

- アクション:
  - 何とかしよう
  - 倉庫に水をかけよう

- 前提条件:
  - 条件 #1:タンクに入った水は運べない。グラスしか運べない。
  - 条件 #2: エクササイズは5分以内。
  - 条件 #3: みんなパニックになっている!

1.インシデントレスポンス入門
2 –エクササイズの振り返り

エクササイズの振り返り

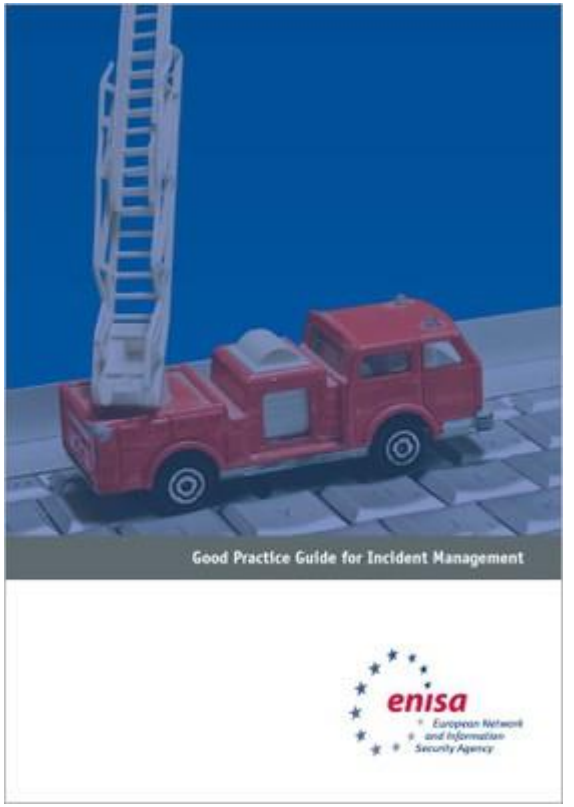
- 何ができたか?
- 何が失敗したか?
- またの機会があればどんなことをしたいか?
- インシデントに関連付けられた行動の名前は?

1.インシデントレスポンス入門

- 消防士は どんな規模、場所そして”可燃物”に一人で対応し火を消しているわけではない。
- 1人1人そして、誰もが “他の誰か” に協力するということがチームの努力の成果だということを理解する。
  → 1 + 1 > 2
- 問題を解決する新しい方法を作成するのではなく、プロセスに従って行動する。
  → 準備は重要
- 今日のメッセージ:
  - 車輪を再発明しない。
  - ルールに従うと、操作はよりスムーズかつはるかに良くなる。

1.インシデントレスポンス入門

ENISAからの問いかけ…
私たちは消防士!



抜粋:

あなたは、疑問を持つかもしれない –
インシデント管理がなぜ効果的であるのか、
なぜCERTが重要なのか、ということを尋ねられることがある。
実際、それはどの組織にとって不可欠なのか？

答えは簡単：火があるときは、それは消されなければならない。
これまでに火の中にいたことがある人は誰でも次回にそれを防止したい。

1.インシデントレスポンス入門
3 – その他の例

- 問＃1：あなたが消防士で、午前6時に仕事場に到着したとする。
- それぞれの問いであなたはどういった行動するか?

- 問＃2：午前11時45分、消防署から200メートル離れたオフィスビルで火事が発生する。

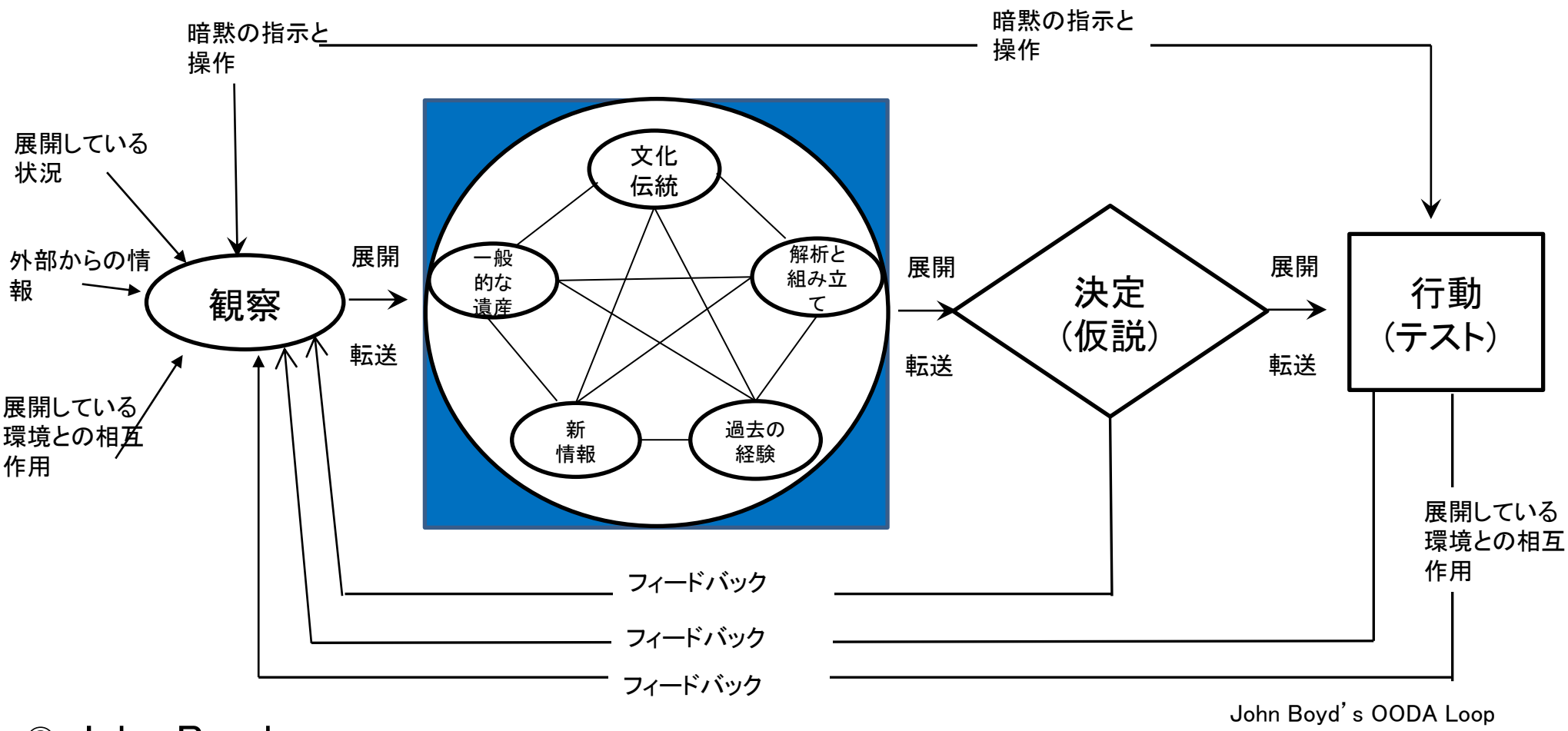
- 問＃3：午後12時30分に、現場のチームは火災が激しくなり、ブロック全体に広がり始め、道路の向こう側の他の建物に達すると可能性があるため、支援を求める。

- 問＃4：午後12時45分に、車の事故が発生する。火事を見ていたドライバーが原因。何台かの車が燃えている...

- 様々な方法
  - Observe Orientate Decide Act (OODA loop)
    - June 1995, John R. Boyd
  - “Computer Incident Response Guidebook”
    - US Navy, August 1996

- 3つの最もよく知られたモデル
  - SANS “6-steps Incident Handling”
    - Early 1990s
  - NIST SP800-61 “Computer Security Incident Handling Guide”
    - January 2004, latest update in August 2012 (release v2)
  - ENISA ”Good Practice Guide for Incident Management”
    - December 2010

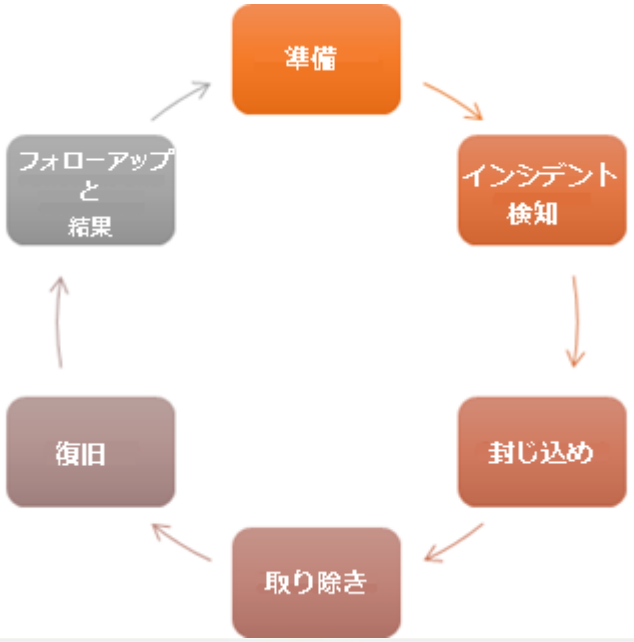
- OODA Loop: Observe Orientate Decide Act(観察 方向づけ 決定 行動)



© John Boyd

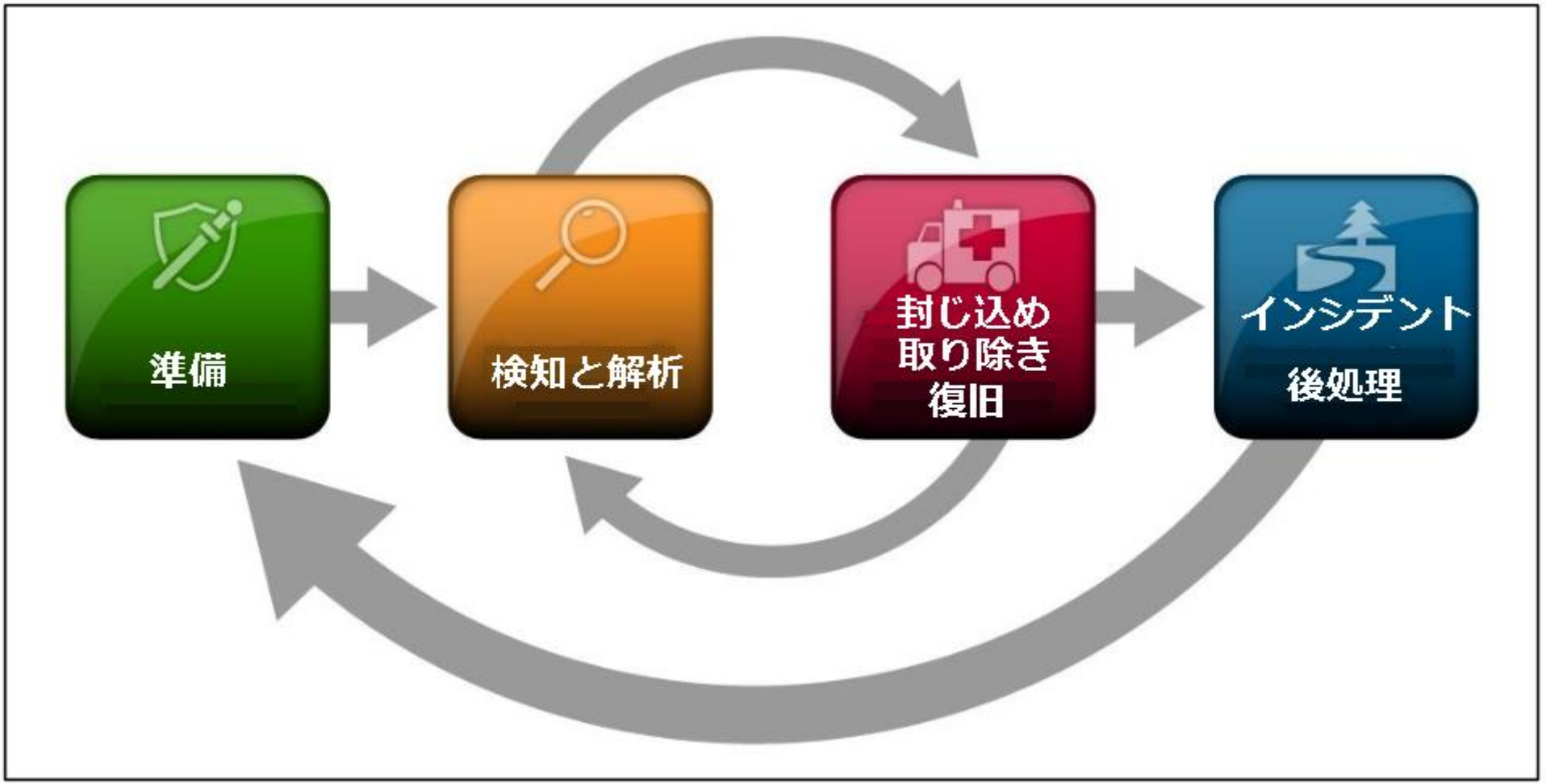
1.インシデントレスポンス入門

SANS

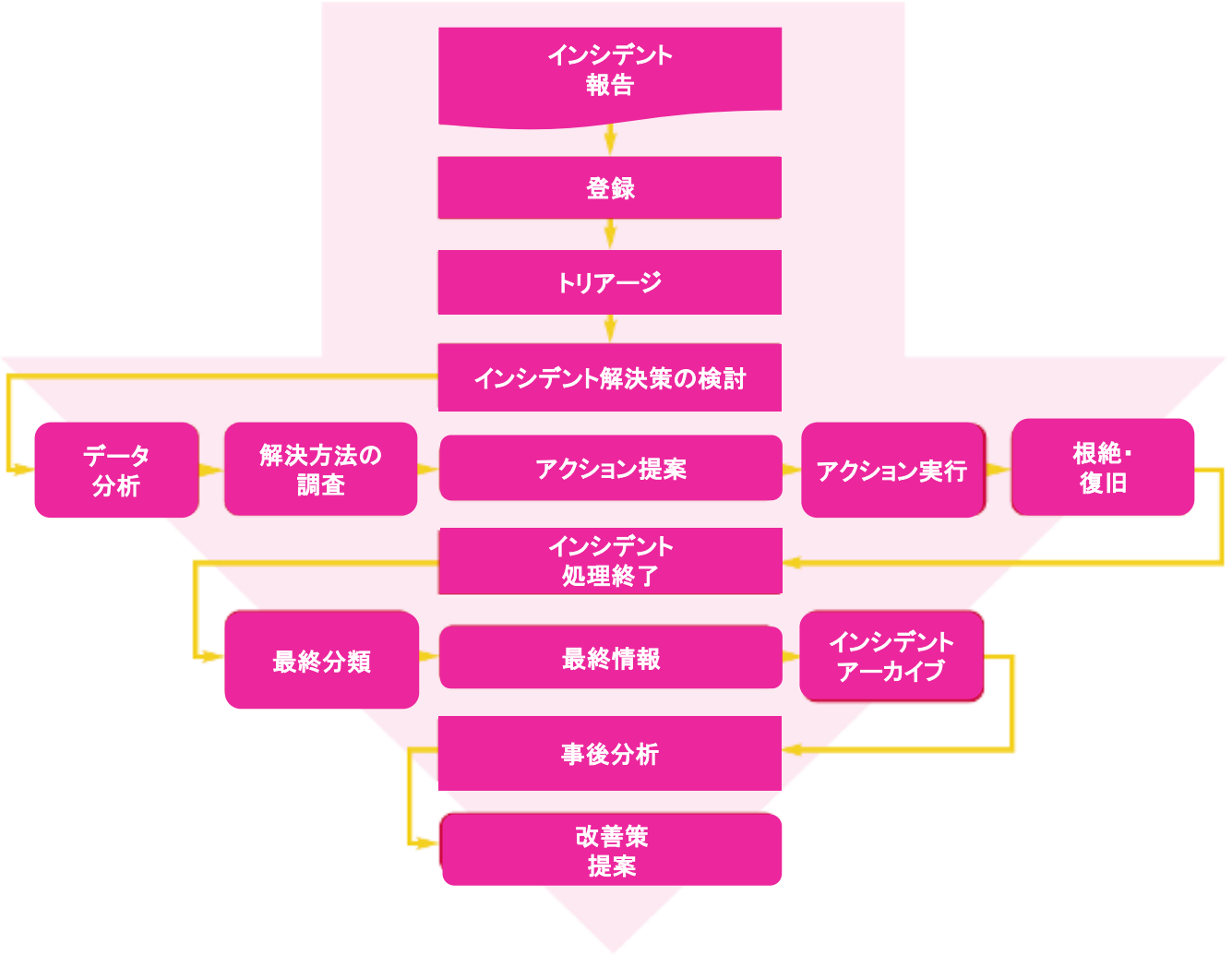


1.インシデントレスポンス入門

NIST SP 800-61 rev 2 (2012)



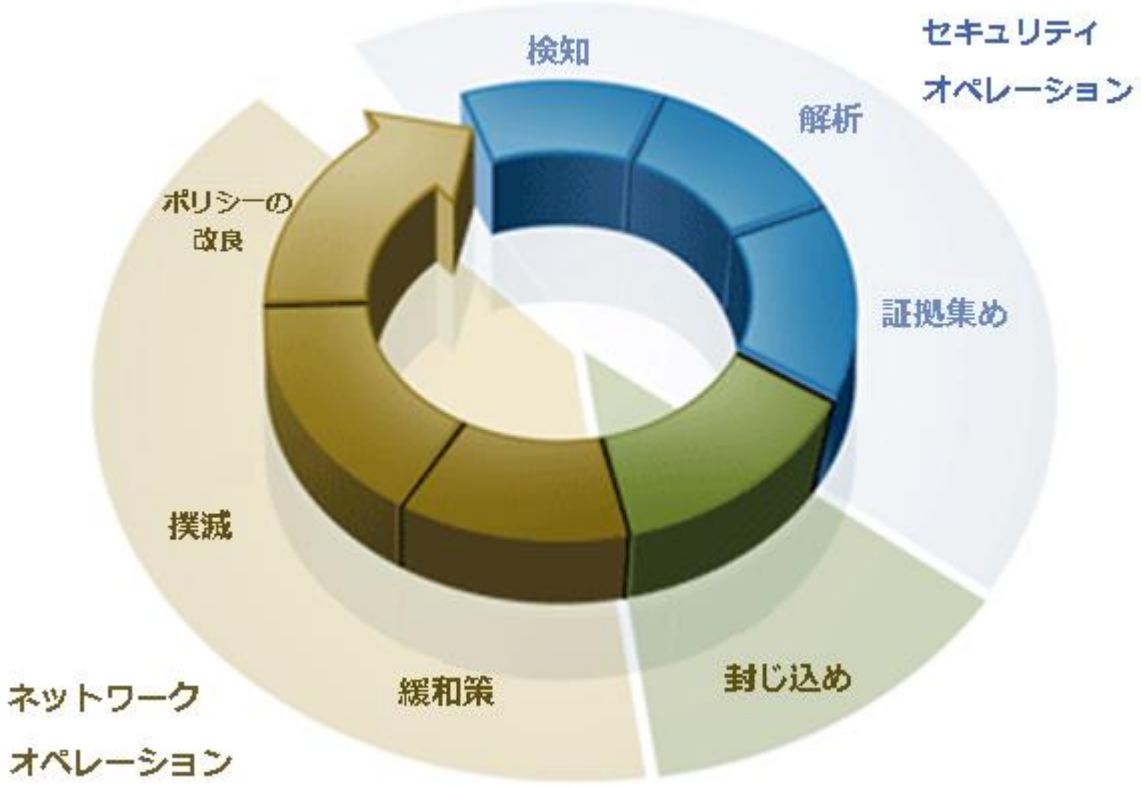
ENISA “Good Practice Guide for Incident Management” (p.34)



© ENISA

別の例（広告ではない！）

BlackStratus’ Multi-Tier Security Incident Management Solution



責任はどのように分かれているのか？

© BlackStratus

消防

消防の歴史

http://www.emergencydispatch.org/articles/historyoffirefighting.html

組織での火との戦い: Summing It All Up

http://netage.com/pub/books/TeamNet/CHAPTERS%20PDF/CHAPTE~3.pdf

緊急

IT インシデントマネジメント

ENISAによる” Good Practice Guide for Incident Management”

- https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

CERT-CCによるCSIRT構築ページ

- https://www.cert.org/incident-management/index.cfm

FIRSTによるインシデント分類例

- http://www.first.org/resources/guides/#bp19

- RFCs
  - RFC 2350 – expectations for computer security incident response
    - http://www.ietf.org/rfc/rfc2350.txt (BCP 21)
  - RFC 2196 – site security handbook (rfc1244)
    - http://www.ietf.org/rfc/rfc2196.txt (FYI 8)
  - RFC 3013 – Recommendations for ISP security services and procedures
    - http://www.ietf.org/rfc/rfc3013.txt (BCP 46)
  - RFC 3227 – Guidelines for evidence collection and archiving
    - http://www.ietf.org/rfc/rfc3227.txt (BCP 55)
  - RFC 2142 – Mailbox names for common services, roles and functions
    - http://www.ietf.org/rfc/rfc2142.txt

1.インシデントレスポンス入門
結論

- 原則
  - 消防士の仕事を理解する
  - あなたの周辺を知る
  - あなたのチームを知る
  - プロセスを知る

- 3つのステージ:
  - “準備” → 準備を整える
  - “行動” → ルールに従って
  - “投資する” → 準備とプロセスの向上

目次

2. インシデントハンドリング
目次

1 – グループ討論
2 – インシデントハンドリング V.S.インシデントレスポンス
3 – 小さい CSIRT チームの運用例

- 役割を相互で補う
  - インシデントレスポンス
    - 解析と封じ込め
  - インシデントハンドリング
    - 情報管理とコミュニケーション
    - 計画と調整
    - プロセスと手順
- 異なる技術セット

- インシデントが大きくなればなるほど,より複雑に:
  - 活動の整理
  - 実践的な分析と技術的作業には専門知識が必要
  - インシデント対応者をサポートを行う

2. インシデントハンドリング
2 – インシデントハンドリング *V.S.* インシデントレスポンス
活動の形

- リアルタイムアクティビティ
  - 検出
  - インシデント処理
  - インシデントリカバリ
  - 調査
  - 管理
  - 法的措置
  - コミュニケーション
- オフライン アクティビティ
  - ポリシー
  - 準備
  - インシデント情報の追跡、インシデントの報告と処理の手順
  - インシデントの後処理

2. インシデントハンドリング
3 – 少人数のチーム向け

- 二人くらいのインシデントハンドリングチーム
  - 情報連携と記録のためのかんたんなツール
    - 範囲がない問題
    - Excel スプレッドシート, Wiki

- インシデントレスポンスとインシデントハンドリングは分ける
  - IR: 技術的問題
  - IH: 顧客/執行部/運営について考える

- 情報連携

- インシデント対応者をすべてから守ることがさらに重要
  - 「実践的な」スタッフを気にしない
  - 消防士の話を思い出してみる

2. インシデントハンドリング
3 –少人数のチーム向け– 5つの制約

1 – リソース/人材/ソフトウェア/ハードウェア

- より小さなタスク
  - チームの柔軟性に関する問題
  - いくつかの側面（法的な）
  - 役割は明確に分割する必要があります
    - 意思決定者と技術部門

- ソフトウェアとハードウェアをすぐに使えない場合
  - 運用、調査どちらにおいても

- 使用可能なリソースの量を予想する
  - フルタイムとパートタイム

- 不足している部分を特定し、レンタルまたはアウトソースする準備ができている
  - 訓練, ハード/ソフト/アプリケーション, ディスク・スペース

2. インシデントハンドリング
少人数のチーム向け

1 – リソース/人材/ソフトウェア/ハードウェア

2 – 資金

3 – 専門技術

- 正しいトレーニング方法を見つけ、実践する
- ドキュメント、ベストプラクティス、フィードバックを共有するリポジトリを構築する…

4 – ツール化と自動化

- 潜在的なインシデントを簡単に特定できる
- 反復作業の労力を削減
- 既存のツールまたはカスタマイズされたスクリプト

5 – 時間

- 最も限られた資源
- 後で時間を浪費することを避けるために、準備する時間を作る

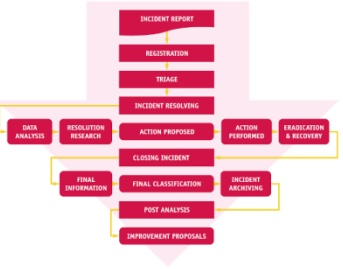
2. インシデントハンドリング
Mike Alexiouの原則

- コンピュータのフォレンジック研究者によってよくある間違いは、**明確な方向性の欠如**
  - 事実 → 犯人の存在
  - 行動 → 痕跡を探す
  - エラー → 最初に調査計画を立てない
  - 結果 → 時間の浪費、答えのない疑問

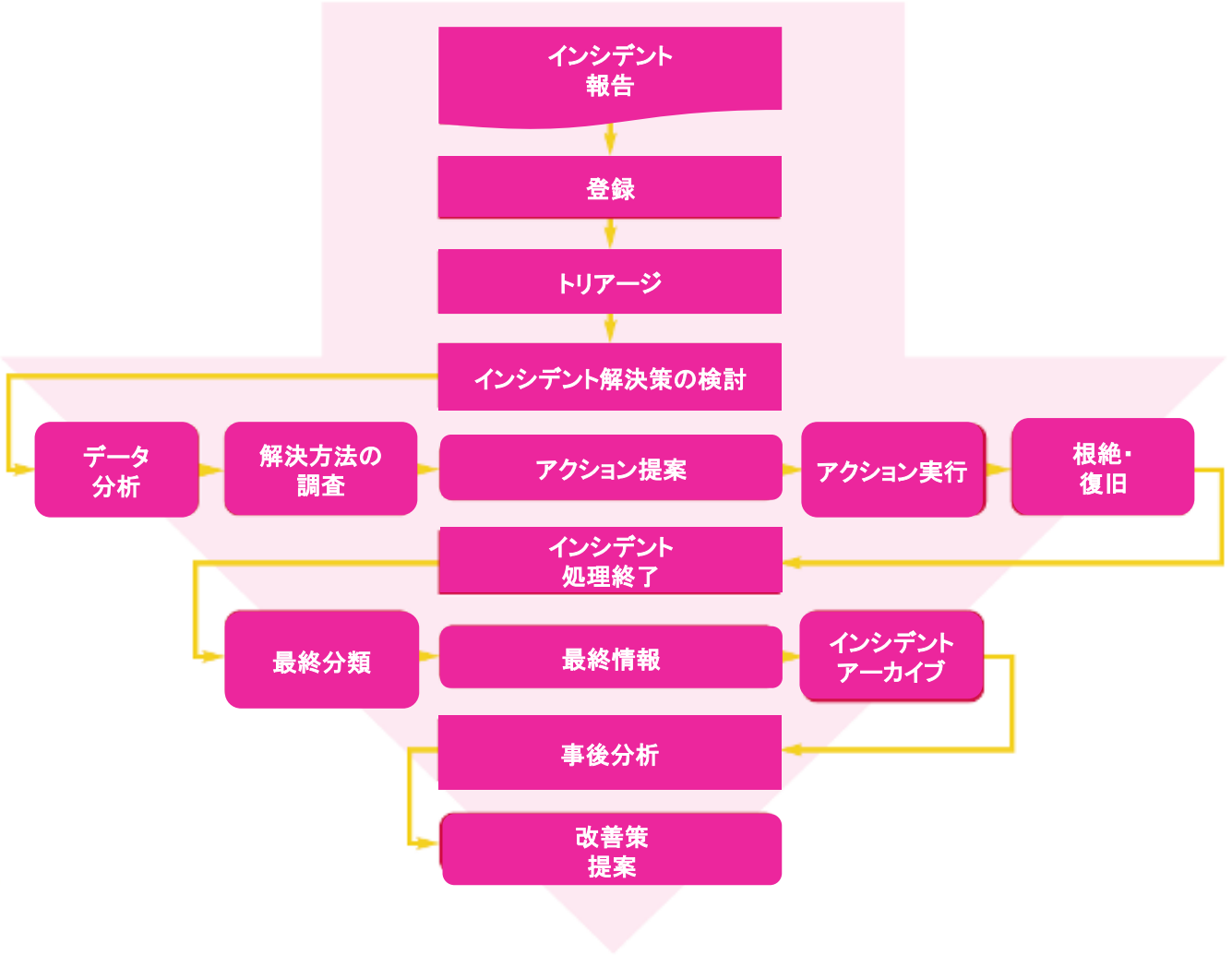
- Mike Alexiou原則は4つの疑問を研究者に問いかけている:
  1 – あなたは何の質問に答えようとしてるのか？
  2 – その質問にはどのようなデータが必要か？
  3 – どのようにデータを抽出するのか？
  4 – そのデータはあなたに何を伝えるのか？

目次

4. インシデントマネジメントモデル– ENISA プラン

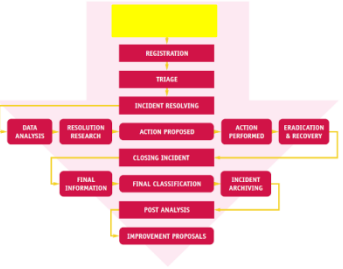


ENISA “Good Practice Guide for Incident Management” (p.34)



© ENISA

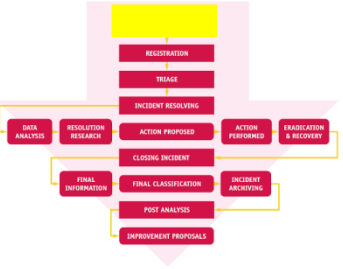
4. インシデントマネジメントモデル– ENISA
1 – インシデント報告



- 入り口(Initial Input)
  - CSIRTが受領した発生事象/問題/インシデント
  - CSIRTに到達するために複数の経路を確保しなければならない。様々な停止や攻撃などの場合に備えて、、、

- 目的:
  - 最初に最適を得るために
  - 早く情報を集約するために
  - 通知してくれる人のために簡単に、シンプルな電子メール

4. インシデントマネジメントモデル– ENISA
1 – インシデント報告

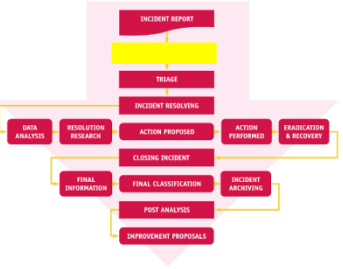


- インシデントハンドリングシステムとメールシステム間の連携を推奨します。

- 何かが起こるのを待つ対応から積極的な対応へ:
  - ツールを統合化する (IDS probes, scanners, feeds...)
  - 第三者からのインシデントを(自動的)にレポートを統合化する
  - ツールを統合化する(IDS probes, scanners, feeds...)
  - 集めた情報をWeb上で統合化する (forums, file repository)

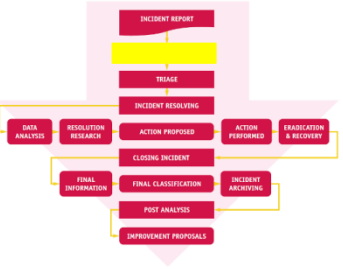
- インシデントの詳細を完全に自動化するのは夢かもしれない、しかし
  - 様々な人、ケース、ツールに合う共通の単語集を見つけることが必要。。。
  - 相関関係と通知の相似性を考慮して対応することが必要
  - 営業日に報告されるインシデントレポートをちゃんと引き受けること。。。
    そして価値をみること
  - 広く影響を与えるインシデントケースの大規模発生はどうでしょう？

4. インシデントマネジメントモデル– ENISA
2 – 登録



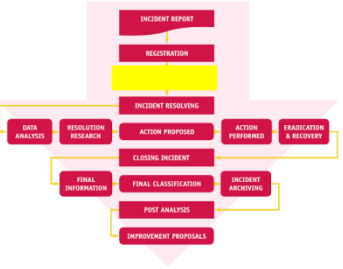
- インシデント報告フォームはインシデント登録プロセスを簡単にする
    - 使用頻度が高い、必須項目を定義すること
- トラッキング可能な一意の番号を振る
- 集約するために上から眺める・一つのインシデントでは複数のチケットをマージする。。。
- しかしながら、最初に一つのインシデントとして捉えたものが複数のケースになることも。。。

4. インシデントマネジメントモデル– ENISA 2 –登録



- 登録システムへの攻撃:
  - 不正な入力: システムへのあらゆるインプット、すべての入力は最初に検証されなければならない
    - メールサーバのパンク
    - スパム
    - 漏洩
- 異常検知を設定すべき、そして登録されたタグ付けされたインシデント初期フィルタリングを実施
- 幾つかのタスクは自動化できない。時間がかかる、人的リソースも消費

4. インシデントマネジメントモデル– ENISA
3 – トリアージ

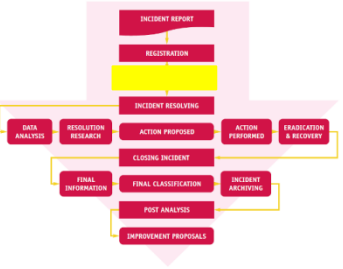


- トリアージはフランスの医療用語から
  - 多数の被害者が到着し対応する時に、医療のリソースが足りない時に
  - ベストな方法ですべてのケースを処置するために必要な方法
  - 時間が限られている中で

  - 解決策:
    - 重要性、診断、治癒を考慮に入れる
    - 例えば、傷害の重大度による正式な判断基準による優先度を設定する

- インシデントハンドリングは3つのステップもある
  - 評価
  - 初期判断
  - 担当割当

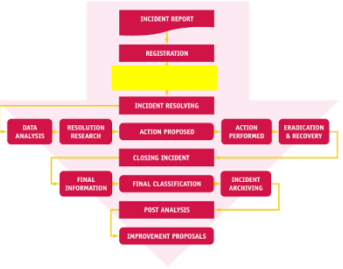
4. インシデントマネジメントモデル– ENISA
3 –トリアージ



1 – 評価する

- 対象外ではないか・扱えうるしきい値を超えてないか
- 通常スキャンやウイルス検知の場合多くのメッセージが出力される
- 他の対象とならないケース
  - 外国語や暗号のような文字で書かれたメッセージ
  - CSIRTの基準ではインシデントとならないイベント
  - CSIRTの対象とするコンスティチュエンシではない
  - 疑わしい発信元からの通知
- 対象とならない通知のポリシーは何になるか?
- 返信をする準備はできているか?

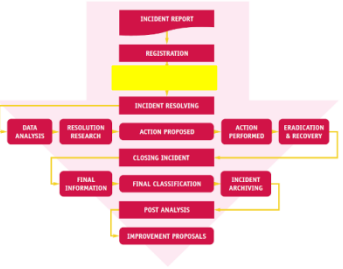
4. インシデントマネジメントモデル– ENISA
3 –トリアージ



2 – 初期のインシデントの分類 / 重大度の評価

- CSIRTの分類体系に適合するように、コンスティテュエンシのためのCSIRTの役割に基づいた評価をする
- より詳細は分類を助ける
- 初期の分類は正しくないかもしれない
  - 追加の情報は分類の変更を促すかもしれない
- 初期報告者にACK(受領確認)を返すのがいい
  - チケット番号
  - 移行のステップのヒントなどを添えて
- **<u>優先順位付け</u>**
  - 最も重大なケースを最初に対応すること

4. インシデントマネジメントモデル– ENISA
3 –トリアージ



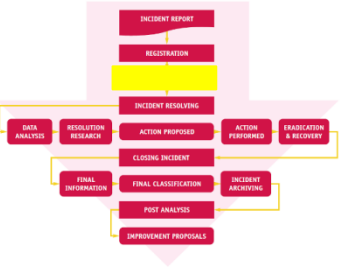
2 – 初期インシデント分類 / 重大度調査 / 優先順位付け

- 幾つかの優先順位付けの基準:
  - 対象のセキュリティ要件
  - ビジネスへの影響
  - 攻撃の種類
  - 攻撃の大きさ
  - 単一の攻撃なのか複数可
  - コンスティチュエンシとのSLA

- 基準はCSIRTの役割や活動に依存する可能性が大きい
  - 政府系CSIRTと企業 CSIRT
  - 組織内CSIRTとプロダクト対応 CSIRT(PSIRT)

- 分類はインシデントハンドリングすることによる努力によって決められるだろう

4. インシデントマネジメントモデル– ENISA
3 –トリアージ

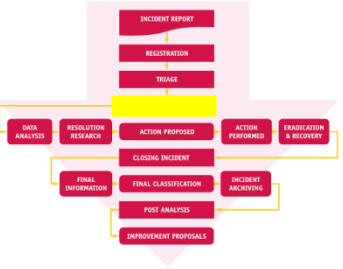


3 – 案件の割当

- 分類が終わり、努力のほどが計られるであろう
- … チケットはインシデントハンドラーにアサインされる

- 割当の判断基準
  - 専門性もしくは能力
  - リソース
  - 知識
  - 言語

4. インシデントマネジメントモデル– ENISA
4 – インシデント解決

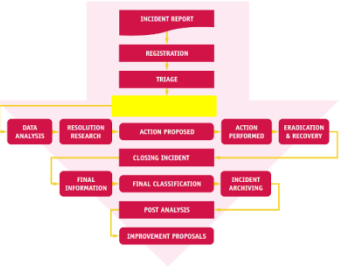


- 実践的なインシデントハンドリングフェーズ
- 6ステップ:
    - データ分析
    - 解決先検討
    - アクションの提案
    - アクションの実行
    - 根絶
    - 復旧

- 逐次の流れではない

- CSIRT外のリソースを依頼する必要があるかもしれない
- 時間とともに、追加の詳細が収集されるだろう
    - 他のインシデントが関連すれ場合も
    - 新たな被害者が見つかるかも

4. インシデントマネジメントモデル– ENISA
4 – インシデント解決



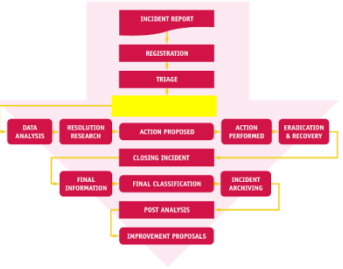
ガバナンスの課題　#1:

あなたはインシデントを処理したいかもしれない。でも、実際の被害者は何を望んでいるのだろう?

インシデントハンドリングは被害者にとっての鍵とはならないかもしれない
被害者はすぐに運用を再開することを望んでいるかもしれない…
…Artifact(証拠など)の削除や台無しにすることとともに

ビジネス基本の判断基準、マネージメントの決断

4. インシデントマネジメントモデル– ENISA
4 –インシデント解決



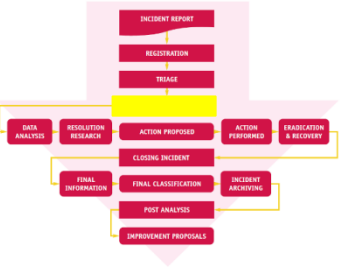
ガバナンスの課題 #2:

何がインシデントハンドリングの重要ポイントとなるか

インシデントから回復し、ビジネスを回復する?
インシデントの拡大を防ぐ?
インシデントの元を見つける?

ビジネス基本の判断基準、マネージメントの決断

4. インシデントマネジメントモデル– ENISA
4 –インシデント解決



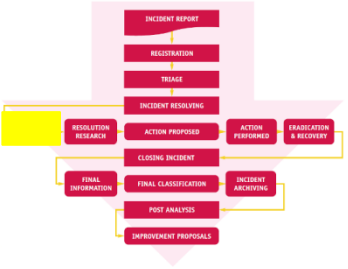
ガバナンスの課題　#3:

インシデントについて言えることは?

秘密のままにしておく
(制限の上で) 通知は法律や規定によって義務となっている
関係者に共有
一般に公開

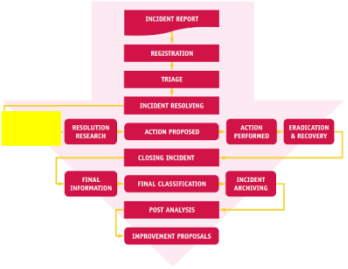
ビジネス基本の判断基準、マネージメントの決断

4. インシデントマネジメントモデル– ENISA
5 – インシデント解決 / データ分析



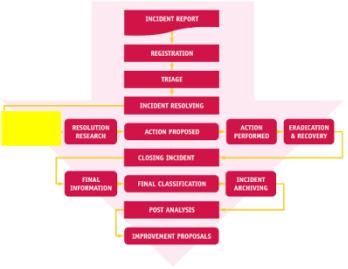
- インシデント対応の尽力を支援するための詳細を探す
- 被害者からのデータ収集と支援に寄与する
  - 連絡先、日付、対象環境のポイントを含む、通知フォームですぐに利用可能なデータ…
  - インシデント知識ベース
  - センサーやモニタリングシステムからのライブデータ
  - セキュリティシステムからのログ
- 他のまだ認知されてないインシデントの被害者を発見するかもしれない
- 次の潜在的な犠牲者を想起するかもしれない

4. インシデントマネジメントモデル– ENISA
5 –インシデント解決 / データ分析



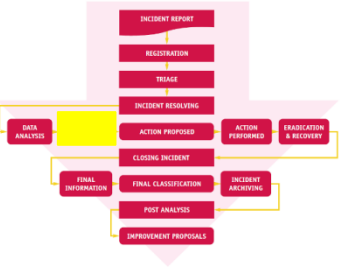
- 技術パートナーと連絡を取り合う必要があるかもしれない
  - ホスティング会社、ISP、コンテンツ・サービスプロバイダー
  - HW/SW 提供者、アプリケーションベンダー
  - サービスプロバイダー
- ビジネスパートナーと連絡を取り合う必要があるかもしれない
  - パートナー、下請け業者
  - サービスプロバイダー
- 当局と連絡を取り合う必要があるかもしれない
  - 警察など、法執行機関 (LEA)
- 準備無しでの良い意思でのポジティブなサポートレベル
- ***期待***

4. インシデントマネジメントモデル– ENISA
5 –インシデント解決 / データ分析



- 正式な手順
    - 文書化の必要性
    - 再生可能であるこれればベスト
    - 本来のデータで決して作業しないこと、常にコピーを使うこと
- ソースの選択
    - 人・スタッフ、コンポーネント、データ、時間割
- チームを作る
    - チームマネージャー
    - 以下に従い仕事を分けること
        - 手順・プロセス、専門性、可用性、負荷
    - チームによる努力
- 計画に従って進める

4. インシデントマネジメントモデル– ENISA
6 – インシデント解決 / 解決策調査



- 追跡でのグローバル調査
    - 独立した追跡と調査
    - プロジェクト管理
        - ブレインストーミング、タスク、会議...

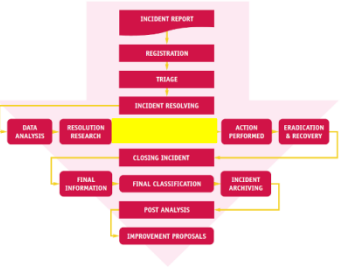
- 区切りでのレビューはとても重要
    - インシデントマネージャーの鍵となる役割

- 詳細まで掘り下げ分析する

あるいは

- 調査に対する分析のレベルを調整する

4. インシデントマネジメントモデル– ENISA
7 – インシデント解決 /提案アクション



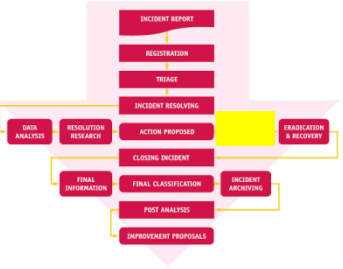
- 前のステップを基本とし、新しい方向性を提案する
    - 分析は継続すること
    - 他のコンポーネントに向かってみる
    - 時間を遡って、狙う
        - 一番最初のイベントまで

- 次のステップをビジネスマネージャーや意思決定者に提示する
- 提案されるアクションは聴衆者に関係あること
    - 技術、ビジネス、法律、リソース

例:

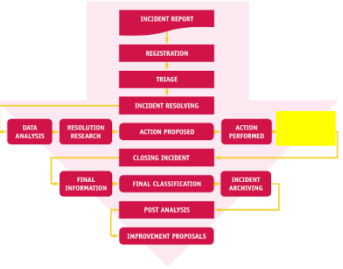
- 攻撃元を探すこと
- 攻撃の停止、対し、提言
- バックアップ環境に向かう

4. インシデントマネジメントモデル– ENISA
8 –インシデント解決 / 実施アクション



- アクションはインシデントチームの対応者、もしくは委託先などにより実施される可能性がある。
- すべてのケースで、計画に合致したものでなければならない
- 結果は選択に影響を与える

4. インシデントマネジメントモデル– ENISA
9 – インシデント解決 / 封じ込めと復旧

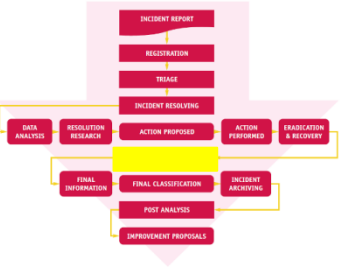


- 主たるゴール: インシデントを取り除くこと
  - 封じ込め
  - 復旧
  - ビジネスの回復

- 封じ込め:
  - 影響をなくすNo more effects
  - 新たな被害を発生させない
- 復旧
  - インシデント前の状況に戻ること

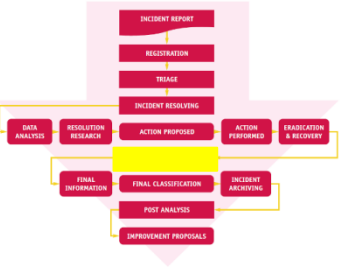
- ビジネスの回復
  - RTO: Recovery Time Objective(リカバリ時間目標)
  - RPO: Recovery Point Objective(過去のどの時点まで戻れるか)

4. インシデントマネジメントモデル– ENISA
10 – インシデントのクローズ



- 最後であるが決して軽んじてはいけない。これがインシデントの最後である。
- 問題がもはや何もないこと
- だれがクロースの決断をするのか?
- クロースの基準は何か?
- 法的立件があったら?
- センサーや検知システムに対して追加や調整をしたか?

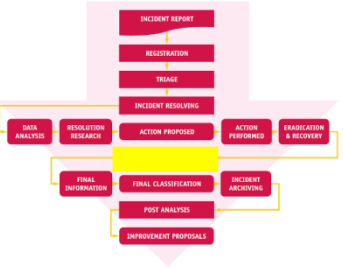
4. インシデントマネジメントモデル– ENISA
10 – インシデントのクローズ



- インシデントハンドラーに取ってインシデントが終了する時...
  - すべてのタスクが遂行された
  - 活動が文書化された
  - インシデントチケットがすべての詳細でクローズされる

- インシデントマネージャーにとってのインシデントが終了する時...
  - 必要とされるインシデントハンドリングタスクがすべて終了される
  - インシデントチケットが与えられた時間の中で再度オープンされない
  - チケットのクローズが確認された
  - 証拠(artifacts)や収集されたもの、ログ、文書が索引された... 安全に

4. インシデントマネジメントモデル– ENISA
10 – インシデントのクローズ



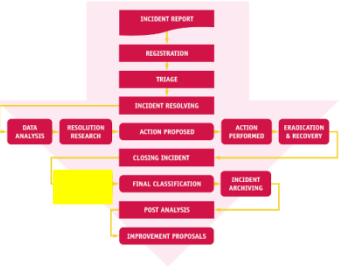
被害者にとって、インシデントが終了する時...

通常業務に戻る

被害者...

- 同じもしくは(同様の)インシデントが再度発生するとしても基本アクションを知るべし
- 同じもしくは(同様の)インシデントが再度発生するとしても、誰にコンタクトするかを確実にしておくべし、
- 被害者は正式なクローズの通知を受領する

4. インシデントマネジメントモデル– ENISA
11 – 最終情報



どんなメッセージをリリースするのか?

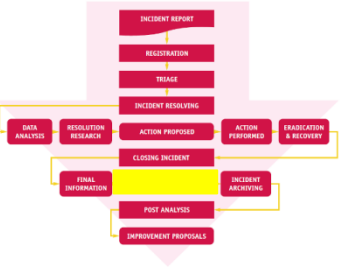
- 対象(インシデントの)、実及び可能性のあった影響、現在の状況
- 主たる発見事項
- 出会った問題と終了させた作業のサマリー
- 攻撃の複雑性と理解度のレベル
- 新しく評価されたセキュリティレベル
- 推奨とフォローのステップ
- 聴衆者とインシデントの複雑性のレベル、両方の理解への調整が必要

誰がメッセージを配布するのか?

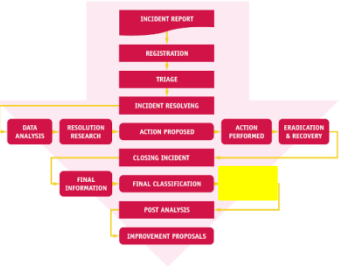
- インシデントマネージャかCSIRTリーダー
- 説明のレベルの違いを使用する可能性

誰が今後のサポートをするのか?

4. インシデントマネジメントモデル– ENISA
12 – 最終分類



- 最終分類は初期と違っているかもしれない
  - 初期: 最初に有効だった要素をベースとしている
  - 解決のステップ: 各アクションのフェーズの間、問題に取り組んでいる間
  - 最終: インシデントのグローバルで最終的な理解
- 分類はトリアージのスピードアップの助けとなる可能性がある
  - 追加の詳細情報が、正しい方向で開始するのに役立つ
- 最終分類のリスク
  - 分類のサブカテゴリーに注力してしまう
  - 分類を助ける基準や詳細を拡張するのに時間を費やす代わりに



保存(Archives)

- 簡単にアクセスできるようにするべき
  - インシデントが再度発生した時に、簡単に過去のケースに追従得できる
- アクセスはセキュアにかつ機密として取り扱われるべき
  - 保存されているものはインシデント解決までのすべてのステップが含まれている
- 保存物に対するあらゆセキュリティ侵害はそれ自身がインシデントとなる!

組み込み製品

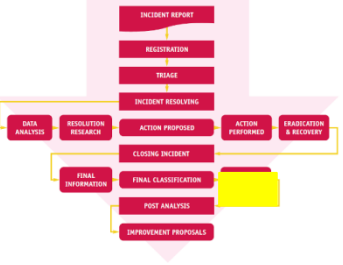
V.S.

CSIRT専用製品

V.S.

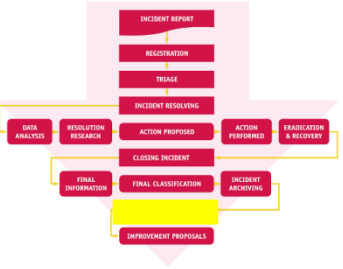
組織全体製品

4. インシデントマネジメントモデル– ENISA
13 – インシデントの保存



- データに対して多くの国々で法律が適用される
  - プライバシー保護やデータ処理
  - データ保持要件とデータ処理
- もちろん、各々の国で法律は異なる
- 時間経過後、データは削除されるとも推測される…
  - 法的なデータの保存期間は?
  - **数年前に**始まっているAPTインシデントを遡って調べなければ行かなかったら?

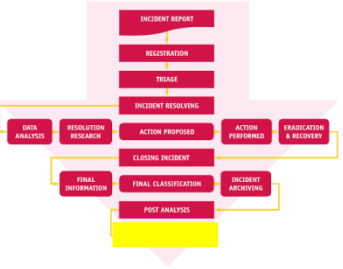
4. インシデントマネジメントモデル– ENISA
14 – 事後分析



- クローズ後に開始すべき
  - インシデントハンドラーたちからの抵抗:
    - *クローズしているのになぜ時間のムダをかけるの?*
    - *私達がやったんだ、なぜあなたは調査するのか、私達の活動を?*
    - *私たちは他のインシデントに対応中だ!*
    - *むむむむ…あなたは事務処理、私達は本来の仕事…*
    - *オフライン品質と生きたインシデント*

- 事後分析を開始する前に数週間待つか…
  - もしくは、専任の人々がその開始からの処理に従うようにする
  - 定期的な事後分析とフィードバックセッションを構成する
- 事後分析はすべての処理で実施されるべきである
- うまくいったもの、うまくいかなかったもの、両方に対処すべき?
- 学んだことは何なのか?

4. インシデントマネジメントモデル– ENISA
15 – 改善の提案



- この前の事後分析をベースにすべき
    - 何がうまくいかなかったか?
    - それを防ぐために何をすべきだったか?
    - 誰がこれらの改善からの利益があるのか?
        - 内部のチームに直接に
        - 内部のチームに間接的に
        - 外部のステークホルダー
- 利点
    - より良いインシデントハンドリングプロセス
    - CSIRTと他のステークホルダーに取ってよりよい関係に

目次

5. コミュニケーションと相互作用
1 – グループディスカッション

グループディスカッション

- あなたに連絡をとるためには、何時どのようにすればよいのか、どう簡潔に説明する?
- あなたの活動の概要をどう説明する?

- 様々なレベルの機密性を持つ事柄について、どのように説明する?
- “知る権限”を付与された小規模なリストからマスにまで、どのように通知・連絡する?

5. コミュニケーションと相互作用
2 – RFC 2350

- RFC 2350 – BCP 21, June 1998
- コンピュータセキュリティインシデント対応への期待
  - http://www.rfc-editor.org/rfc/rfc2350.txt
  - https://www.rfc-editor.org/bcp/bcp21.txt
  - http://www.rfc-editor.org/pdfrfc/rfc2350.txt.pdf
  - Appendix D: CSIRT テンプレートについての骨子

- 2つの使用方法:
  - CSIRTの活動を構造化するため
  - 簡単に連絡が取れるように、CSIRTの詳細な連絡先を示すため

- 誰にでも共有可能な情報ですか?
  - 限定されたステークホルダーに共有する
  - パートナーに共有する
- 少数の関係者のみに共有可能な情報か?
  - (静的) 情報それ自体
  - (動的) 情報の流れ
  - 静的と動的なデータ保護
  - (制限) 情報の扱いを許可された人のリスト

- **TLP: https://first.org/tlp = TLP version “1.0”**
- 情報共有を促進するために作成された
  - 機微ではあるが、極秘ではない情報を共有する
- 受け手の垣根を越えて情報を広げるためにはどうすれば?
  - 受け手がTLPを理解し遵守することを確認し、情報のオーナーがTLPタグを付与する
  - 受け手がより広範囲に共有したい場合、送り主に許可を求めなければいけない
- TLP = 4つのタグ / 色
- Eメールの**件名と本文**が TLP:XXX で始まる

5. コミュニケーションと相互作用
4 – Information Sharing Traffic Light Protocol (TLP)

- TLP-RED: 情報源は、情報が関係者の協力なくして効率的に行動できない場合であり、かつ悪用された場合に関係者のプライバシー、風評、運用に影響が起こり得る場合、TLP-REDを使用する。受け手はTLP:REDの情報が開示された取引、会議、会話に参加していない部外者には情報を共有してはいけない。会議を例にした場合、TLP:REDの情報は会議の参加者のみに限定される。多くの場合、TLP:REDは口頭または直接に交換される。

- TLP-AMBER: 情報源は情報を関係する組織の外に共有した際にプライバシー、風評、運用に影響が起こり得る場合であっても、効率的に行動するためにTLP:AMBERを使用できる。受け手はTLP:AMBERの情報を自身の所属するメンバー、または被害を防止するためにその情報を知る必要のあるクライアント・顧客に共有することができる。情報源は共有に関して、意図的な制限を自由に追加することができる。この制限は遵守しなければならない。

- TLP-GREEN: 情報源は情報がすべての参加組織や広範なコミュニティ/セクター内の仲間の気づきとして有益な場合、TLP:GREENを使用できる。受け手はコミュニティ/セクター内の仲間とパートナーに情報を共有できるが、一般公開しているチャネルを通して共有しては行けない。TLP:GREENの譲歩はコミュニティの外に流れてはいけない。

- TLP-WHITE: 情報源は情報が悪用されるリスクが最小限または予知出来ない場合、一般公開するための適用規則・手続きに従ってTLP:WHITEを使用できる。一般的な著作権のルールに従って、TLP:WHITEの情報は制限無しで配布される。

5. コミュニケーションと相互作用
4 – チャタムハウス・ルール (CHR)

- 情報源は開示されない
  - 帰属は明示されない
- *会議全体またはその一部がチャタムハウス・ルールで行われる場合、参加者はそこで得た情報を自由に使用することができるが、会議における発言者およびそれ以外の参加者の身元や所属団体をいっさい明かしてはならない*
  - *https://www.chathamhouse.org/about/chatham-house-rule/*

- 最初の送信者がCHRタグの適用可否を決定する

- Eメールの件名は [CHR] か [TLP-XXX]タグの後から始まる

- CSIRTのメンバーは仲間と共有しようとする
- CSIRTのメンバーは仲間を助けようとする
- CSIRTのメンバーは多くのインシデントは自分たちのコンスティチュエンシーの中のみで発生しないことを理解している
- 情報を求めれば、CSIRTコミュニティから何らかのヒントまたは助けが得られる
- *私たちは同じボートに乗っている*、**ぜひ共有しましょう**
- **しかしながら …**

5. コミュニケーションと相互作用
5 – インシデント時のコミュニケーション方法

- CSIRTコミュニティ内での共有
  - プロトコル
  - ツール
  - 公的機関と法執行機関

- ENISA
  - ″A flair for sharing – encouraging information exchange between CERTs″, Nov 2011
    - 法律・規制の側面
    - 情報共有及びヨーロッパ内の国家・政府CSIRTによる国際的な協力

- 残念ながら、インシデント関連事例の共有には問題がある …
- 経営陣は問題を”コミュニティ”に共有することに同意するか?
- インシデント/問題/漏えいの影響は何か?
  - ビジネスの観点から
  - あなたの活動分野の文脈から
  - **規制・法律上**の観点から
  - 信頼/イメージの観点から
- 情報の**開示**はあなたの役割か?

5. コミュニケーションと相互作用
5 – インシデント時のコミュニケーション方法

- インシデントについて語ることはコミュニティに知らせること … しかし、そのコミュニティについてどの程度の信頼を持っているか?
  - コミュニティ内で共有されるメッセージはどの程度プライベートなものか?
  - 情報共有のルールは何か? 最適なTLPは何か?
  - 悪意のある人が(間接的に)コミュニティ内で聞き耳を立てている可能性がある

- 仲間に伝えると、敵に伝わることになるかもしれない
  - あなたが攻撃に気づいていること
  - あなたが敵への対応を進めていること
  - どのくらい敵の除外に近づいているか
  - どのくらいインシデントの解決に近づいているか

5. コミュニケーションと相互作用
5 – インシデント時のコミュニケーション方法

- どんなことが言えるか?
- 誰に対して伝えることが許可されているか?

- あなたは組織外の誰かに伝えることを許可されているか/準備ができているか?
  - IT技術向けまたはマスコミ向けのジャーナリストに対して伝えること、またはインタビューを受ける準備ができているか?

- インシデントに関する風評被害にどう対応するか?
- 偽情報にどう対応するか?

- 待って!
  - 広報はそのインシデントに気づいているか?
  - 所属組織のTwitterまたはFacebookアカウントを担当しているのは誰?

- ***あなたが担当すべきか?***

ルール #1: 発信できることを確認する
ルール #2: 発信できるならば、以下のことを確認する …
ルール #3: 発信できないならば、発信ができる人に情報を伝える準備を行い、コミュニケーションをとる
ルール #4: イライラする準備をしておく!

演習

- 組織内で情報漏えいが発生した。あなたならどうする?

- インジェクト #1: 5分
- インジェクト #2: 10分
- インジェクト #3: 10分
- まとめ: 10分

目次

8. まとめ
CSIRT Maturity

- CSIRT成熟度イニシアティブはCSIRTの成熟度を5つの領域で示している
  - 基盤: 法的制約を理解した上でのビジネスプラン
  - 組織: 内部組織への命令、他のCSIRTとの連携
  - 要員: チーム内の人員配置、構成、専門技術、行動規範、トレーニングオプション
  - プロセス: 脅威とインシデントのハンドリングまたはメディアとの対応

- *"CSIRT Maturity Kit – A step-by-step guide towards enhancing CSIRT Maturity"* NCSC-NL, Global Conference on Cyber Space 2015
  - https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf
- *"SIM3: Security Incident Management Maturity Model"*, Trusted Introducer
  - https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

8. まとめ & 最終演習
問題に対応するための組織の例

目次

- Part 1 – インシデントレスポンス入門
- Part 2 – インシデントハンドリング
- Part 3 – SANSのアプローチ
- Part 4 – ENISAのアプローチ
- Part 5 – コミュニケーションと相互作用
- Part 6 – オンサイトとオフサイトのインシデントハンドリング
- Part 7 – CSIRT運用のマネージャー
- Part 8 – まとめ
- Part 9 – ツール