CSIRT 上級トレーニングプログラム

虎術（トランジュツ）開催概要

一般社団法人 日本シーサート協議会

チームトレーニング委員会

Ver 1.1

目 次

虎術について

CSIRT の構築・運用に悩まれている方、CSIRT のリーダー、もしくは今後リーダーになる方、新たなネットワーキングの機会を模索している方に向け、さらなる成長の機会を提供する内容となっています。また、既に CSIRT 運営に豊富な経験をお持ちの方にも、新たな視点や気づきを得られる多角的な学びの機会を提供します。

トレーニングコンテンツは、NCA が長年培ったノウハウを凝縮し、多様なモジュールをパッケージ化したものです。実践的な演習やディスカッションを通じて、日ごろの業務に直結するスキルを習得できます。また、参加者同士および講師陣との交流を通じて、CSIRT 間の連携や幅広いネットワークの構築も期待できます。

このトレーニングプログラムは、NCA が提供する夏・秋の「TRANSITS ワークショップ（TRANSITS-I）」に参加された方や、同等の知識とスキルを既に習得済みの方にも、新たな学びの場を提供します。また、すでに豊富な経験をお持ちの方にとっても、多角的なモジュール構成を通じて、新たな気づきを得られる機会となります。

受講対象者

- CSIRT の構築・運用に悩まれている方
- CSIRT のリーダ、もしくは今後リーダになる人
- 新たなネットワーキングの機会を模索している人

講義時間

- Day1 13:00-21:00　（講義、演習及びネットワーキング）
- Day2 9:00-21:00　（講義、演習及びネットワーキング）
- Day3 9:00-16:00　（講義、演習）

注意事項

- 体調管理には充分注意し、自己の責任においてトレーニングに参加願います。
- マスク着用は個人判断としますが、周りの方へのご配慮をお願いいたします。
- 災害等による開催の中止や規模の縮小については、NCA チームトレーニング委員会にて決定します。

- トレーニング期間中は講師及びスタッフの指示には必ず従ってください。もし従わなかった場合、状況によりワークショップの中断や中止を行うことがあります。その場合でも参加費の返金はいたしません。
- 会場、宿泊施設内での盗難・事故・怪我などのトラブルに関しましては、当委員会は一切の責任を負いません。
- 現地参加で規定人数に達しない場合は中止となる場合があります。
- 中止の場合は参加費を返金いたします。
- 申込後は、開催概要を一読し、全てに同意したものとします。
- 講義・演習中の写真撮影・録画はご遠慮願います。(記録・報告のため予め認められたスタッフのみ撮影・録画を行います)
- トレーニングモジュールの提供資料、開催中の講師及び参加者からのお話、提供される情報は、明確に指定があるもの以外は、すべて TLP:AMBER で取り扱いをお願いします。
- 講義・演習中に 講義 と無関係の作業や内職等はご遠慮ください。
- ゴミを捨てられる場合は会場設備の分別にご協力ください。
- 喫煙される方は必ず指定の喫煙場所でお願いします。
- モジュールごとに通知される注意事項を別途ご確認ください。

提供モジュール

CSIRT 記述演習

RFC2350 を記述しよう。

組織対象	マネジメント層、CSIRT/PSIRT（セキュリティチーム）		
レベル（段階）	準備、基礎	組織体系	組織

概要

CSIRT を、RFC2350 を利用して記述し、CSIRT を外部に向けて説明・公表できるようにします。このプロセスにより、対象の CSIRT がどのようなものか整理でき、自らの活動やステークホルダーとの関係を明確にすることができるようになります。

- [RFC2350]: https://www.nic.ad.jp/ja/tech/ipa/RFC2350JA.html

受講対象者

- CSIRT を構築しようとされている方
- 既に CSIRT のメンバーの方
- CSIRT とは何かをより理解したい方
- CSIRT とすでに関わりのある方

必要な知識

- サイバーセキュリティ用語一般
- CSIRT の単語レベルでの理解
- 技術等の詳細は必要なし

得られる内容

- CSIRT の概要
- RFC2350 の具体的記載内容
- CSIRT への理解の促進

トレーニングに含まれる可能性のある方法

講義、演習

SIM3 導入講習

SIM3 の概要を学び、演習を通じて理解を深めます。

組織対象	マネジメント層、CSIRT/PSIRT（セキュリティチーム）		
レベル（段階）	発展	組織体系	組織、機能（運用、技術）

概要

本トレーニングでは CSIRT の成熟度を評価するためのモデルである SIM3 の概要を学びます。SIM3 は FIRST では加盟時に使用して自チームを評価し、結果を提出することが必須となっています。また、NCA でもチームを効率的に運用するために、評価して使用することが推奨されています。

- SIM3(英語) https://opencsirt.org/csirt-maturity/sim3-and-references/
- FIRST(英語) https://www.first.org/

本トレーニングでは SIM3 の概要をお伝えします。その後、SIM3 の組織、人材、ツール、プロセスの 4 領域の概要、さらにそれぞれの個々のパラメター、レベルを学びます。

受講対象者

- CSIRT を既に運用されている方
- CSIRT のメンバーではない場合、組織運営や改善を行った経験のある方
- セキュリティチームなどのマネジメントに関わられている方

必要な知識

- サイバーセキュリティ用語一般
- CSIRT の単語レベルでの理解
- 技術等の詳細は必要なし

得られる内容

- SIM3 の概要
- CSIRT の効率化、継続、信頼性向上に関する知見

- 世界の CSIRT コミュニティでの共通概念

トレーニングに含まれる可能性のある方法

講義、演習

コミュニケーション

連携のためのコミュニケーショントレーニング。

組織対象	経営層、マネジメント層、CSIRT/PSIRT(セキュリティチーム) 関連組織		
レベル（段階）	発展	組織体系	信頼(法制度、コミュニティ)

概要

CSIRT においてはコミュニケーションスキルが重要だと言われています。本トレーニングでは、なぜ重要なのか、コミュニケーションとはそもそも何なのか、CSIRT ではどのようにすべきなのか、実際に演習なども交えて実施します。

受講対象者

- どなたでも
- CSIRT のリーダーの方
- CSIRT をこれから始めようという方
- CSIRT の運用で悩んでいらっしゃる管理者

必要な知識

- サイバーセキュリティ用語一般
- CSIRT の単語レベルでの理解
- 技術等の詳細は必要なし

得られる内容

- CSIRT 活動における情報共有の重要性を理解します。
- 社内での情報共有の対象、手法、実践例を学習します。
- 社外連携先の確認、対応フローを学習します。

トレーニングに含まれる可能性のある方法

講義、演習

脆弱性管理

ユーザー（システム管理者）の立場での脆弱性管理の要点と関連演習。

組織対象	CSIRT/PSIRT（セキュリティチーム）		
レベル（段階）	基礎	組織体系	技術

概要

ユーザー（システム管理者）が脆弱性管理を行う際に、具体的に組織なかでどのようなことを実施すればよいのかの解説し、関連する演習により理解を深める

受講対象者

- 脆弱性管理を行う者または行うチームと業務上やり取りするシステム担当

必要な知識

- セキュリティ業務に関して TRANSITS Workshop 受講後程度の知識を有する者

得られる内容

- ユーザー（システム管理者）の立場で行う脆弱性管理の実践的な要点の把握

トレーニングに含まれる可能性のある方法

講義、演習

フォレンジック基礎

フォレンジックを基礎知識として学びます。

組織対象	CSIRT/PSIRT（セキュリティチーム）		
レベル（段階）	基礎、発展	組織体系	機能（運用、技術）、資源

概要

インシデント発生時に取るべき行動、取ってはいけない行動を再認識し、有効なフォレンジック結果を得るための初動対応のイロハを整理します。インシデント発生時に落ち着いて初動対応し、その後のフォレンジック担当者（業者）への依頼を効率的に実施できるようにします。

受講対象者

- 基礎的な技術としてフォレンジックを学びたい方
- 初動対応を現場で実施する方

必要な知識

- サイバーセキュリティ用語一般
- CSIRT の単語レベルでの理解
- 技術用語への理解

得られる内容

- 基礎技術としてフォレンジック

トレーニングに含まれる可能性のある方法

講義、演習、ハンズオン

※ハンズオンにおける注意点

コース 1：ハンズオンのため suspicious image/files を配布する場合があります。セキュリティ製品が導入されている場合は、解除できるようにご準備ください。

コース 2：解析用のイメージを安全な処理をして配布いたします。当日、テキストを読み取れる状態でご参加ください。

法制度

CSIRT 業務に関連する法制度について議論を交えて学ぶ。

組織対象	経営層、マネジメント層、CSIRT/PSIRT（セキュリティチーム） 関連組織		
レベル（段階）	発展	組織体系	信頼(法制度、コミュニティ)

概要

CSIRT 業務を運用する中で、取り扱う情報や業界に応じて様々な法令に従って対応をする必要があります。

このトレーニングでは、CSIRT 業務の中でどのように法令がかかわってくるのか、各種関連法令で抑えなければならないポイントや実際の取組みについて、参加者間での議論を通じて理解を深める。

受講対象者

- CSIRT 活動を実際に行っている人
- CSIRT 活動のマネージメントを行う人
- CSIRT 活動のプロセス/文書の整備・改善を行う人

必要な知識

- CSIRT 活動のプロセス・内容を大枠で理解している

得られる内容

- 自社の CSIRT 活動のプロセス上での法規上の課題/解決方法のヒント

トレーニングに含まれる可能性のある方法

講義、演習