第15回 脆弱性対応勉強会

IPA ｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄ対応机上演習教材 体験会

2025-04-19

脆弱性対応勉強会

hogehuga

初めに

今回は、2025-04-15にIPAから公開された「セキュリティインシデント対応机上演習教材」を体験してみる勉強会、です。

おそらく、**教材が想定したユーザ ではない ような方**が参加されていると思います。
本教材を通して、以下が得られれば良いかと思っています。

- そもそも、世の中はこのレベルに達していないことを知る
- 中小企業向け教材をより高度な環境で実施する場合、どの点に気を付けたほうが良いのか
- 自社に持ち帰って実施をする場合の、気付きを得る

About Me

hogehuga（INOUE Kei）

- 脆弱性対応研究会主催
  - 一応、研究会の中の勉強会が”脆弱性対応勉強会”
- 趣味
  - バイク、水風呂
- 経歴等
  - 情シス、MSP、重要インフラ運営、コンサル、セールス/マーケ、を経験
  - 最近KDDI買収で話題になっている会社で、脆弱性管理等の研究職
- 発表歴
  - Code Blue Open Talks(2022)
  - Internet Week2023,2024
  - Internet Week SHOWCASE IN 福岡
  - NCA Annual Conference 2023,2024
  - OWASP (Japan|Kansai|Nagoya)
  - OWASP Hardening Conference
  - 塩尻サイバーセキュリティ勉強会
  - 脆弱性対応勉強会
- その他
  - ISOG-J WG1 “脆弱性トリアージガイドライン作成の手引き”
  - ISOG-J WG1/OWASP “セキュリティエンジニアの知識地図”
  - ISOG-J WG6 “セキュリティ対応組織の教科書 第3.x版”

DALLE-Eが表現する
登壇者が後ろから刺される絵

https://zeijyakuseitaioukenkyukai.connpass.com/

hogehuga / vulnRespStudyGroup

https://zeijyakuseitaioukenkyukai.connpass.com/

脆弱性対応研究会
公開グループ · メンバー260人

https://www.facebook.com/groups/zeijyakuseitaioukenkyukai/

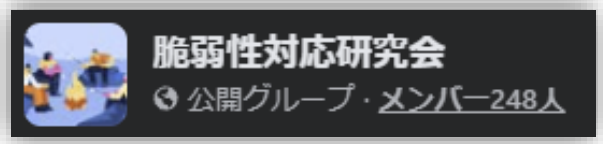
脆弱性対応勉強会は個人で行っている活動であり、会社とは無関係です。
私の発言は、会社及び組織を代表する見解ではないことがあります。

間違いや最新の情報は、後ろから刺さずにご共有いただければ幸いです。

脆弱性対応勉強会とは

2019年から開催している、セキュリティに関する勉強会です。

- connpass/Facebook/github で活動しています。
  - connpass: メンバーは1,050人(2025-04-18現在)で、勉強会の告知に利用
    - https://zeijyakuseitaioukenkyukai.connpass.com/
  - Facebook: メンバーは260人(2025-02-11現在)で、イベント告知と相談的に利用
    - https://www.facebook.com/groups/zeijyakuseitaioukenkyukai
  - github: ファイル置き場
    - https://github.com/hogehuga/vulnRespStudyGroup/
  - 勉強会としては、28回？ほど実施実績があります



- 活動拠点は東京（神田付近？）ですが、県外でも活動をしています。
  - 出張ついでに「出張版 脆弱性対応勉強会」を実施
    - 大阪 2回、名古屋/長崎 1回、札幌 1回（但し誰も現地に来なかった…）
  - VR（アバターを使った録画）も増やします
    - 2回ほど実施

- 2022-04-01 出張版 脆弱性対応勉強会 #01（札幌）
- 2022-07-08 出張版 脆弱性対応勉強会 #02（大阪）
- 2023-03-15 出張版 脆弱性対応勉強会 #03（長崎）
- 2023-06-01 出張版 脆弱性対応勉強会 #04（大阪）
- 2024-02-09 出張版 脆弱性対応勉強会 #05（名古屋）

要望があればどこにでも駆けつける勉強会です！

次回予告

脆弱性
対応
勉強会

TLP:CLEAR

cveTreage

- 脆弱性対応勉強会
  - 1か月以内？：本勉強会実施結果を基に、再度同じ内容を実施
    - どのようにファシリテーションすべきか、の知識をまとめるために実施し、後ほど公開する
  - 未定：使って学ぶ、SSVCと脆弱性トリアージ
    - https://github.com/hogehuga/cveTreage/tree/nightly-dev を用いたSSVCの活用
- JNSA教育部会
  - 2025-05-28：総関西サイバーセキュリティLT大会（第51回）
  - 2025-08-23：【ハンズオン】第13回サイバーセキュリティ勉強会2025夏 in 塩尻
- ISOG-J
  - 脆弱性管理プロジェクト（WG6配下の新プロジェクト）
    （05月頃から始動）

塩尻

SosaiLT

以降、IPAの教材で進めます

目的（実施マニュアル　3章）

TTX は技術的なスキル向上を目的としたものではなく、意思決定のプロセスを体験することを通じ、以下のような目的を達成するために行うものである。

1. 理解の促進
   - サイバー攻撃やリスクに対する組織の対応能力を向上させるため、参加者が自らの役割や責任を理解する。
2. コミュニケーションの強化
   - 関係者間の情報共有やコミュニケーションを促進し、チームワークを強化する。
3. 戦略の検証
   - 既存のインシデント対応計画や戦略が効果的であるかを検証し、改善点を見つける。

今日はここが目的

進行例

時間	内容
0:00～0:05(5分)	オープニング（主催者挨拶、講師紹介、目的説明等）
0:05～0:25(20分)	**講習（座学）** 「中小企業のためのセキュリティインシデント対応の手引き」をベースにインシデント対応のポイントを学ぶ。
0:25～1:25(60分) ※説明、発表時間を含む	**演習 1** 発生した事案の初動対応について、グループディスカッションにより対応方針等を検討する。
1:25～1:35(10分)	(休憩)
1:35～2:35(60分) ※説明、発表時間を含む	**演習 2** 業務・システムの復旧や再発防止、公表等について、グループディスカッションにより対応方針等を検討する。
2:35～2:50(15分)	振り返り
2:50～3:00(10分)	質疑応答・各種案内・クロージング

図 5-2 TTX のタイムスケジュール例

当日の進行状況

10:00-10:10	オープニング	弊勉強会の趣旨、本勉強会の趣旨
10:10-10:35	座学	講師用資料を基に概要説明（w/事例）
10:35-11:10	演習1	状況1の議論後、状況2の議論 当初、15分程度を想定したが、不足していた
11:10-11:25	発表	各グループ発表と議論/講評
11:25-11:55	演習2	状況1の議論後、状況2の議論 講演1を踏まえて時間を取りたいが、会議室利用時間により短縮
11:55-12:15	発表	各グループ発表と議論/講評

Thank you!

Any Questions?

オープンな議論としてお話ししたい場合は、Facebook/X/LinkedIn/Eight 等でご連絡下さい。

仕事として議論をしたい場合は、 kei.inoue@lac.co.jp までご連絡ください。

（どちらもお金が貰えるわけではないので、どっちでもいいです…）