セキュリティ・キャンプミニ

2025（北海道開催）

振り返りレポート

セキュリティ・キャンプミニ2025（北海道開催）実施概要

2025年11月15日（土）～11月16日(日)
北海道大学 情報基盤センター 南館

専門講座 プログラム 1日目

13:00～13:20『オープニング』『セキュリティ・キャンプ紹介』
13:20～13:50『情報倫理とサイバーセキュリティ』
佐々木 祐伴 氏　北海道警察サイバーセキュリティ対策本部　対策・官民連携班長
14:00～16:30『Binary Breakdown: Analyzing Malicious Code』
首浦 大夢 氏
13:50～16:20『新スパコン見学会』

2日目

09:30～12:00『インシデントレスポンスにおけるフォレンジック入門』
扇沢 健也 氏、黒澤 南月 氏
さくらインターネット株式会社情報システム統括室 SIRT
13:00～15:30『攻撃者視点から学ぶサーバーの堅牢化』
蔀 綾人 氏　株式会社フォアーゼット
15:30～16:00『クロージング』

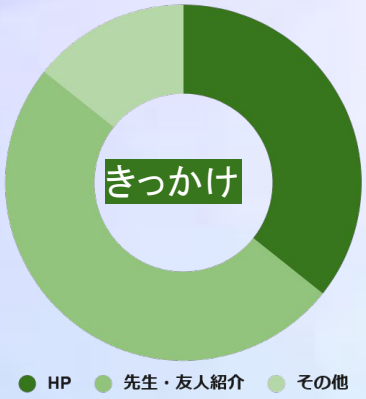
https://www.security-camp.or.jp/minicamp/hokkaido2025.html

セキュリティ・キャンプ2025ミニ(北海道開催)実施概要

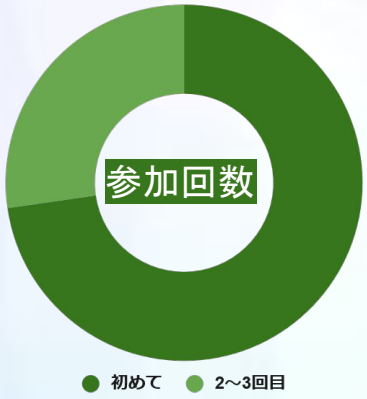
参加学生数

11名

それぞれのきっかけから



ほとんどんの受講生が
初参加



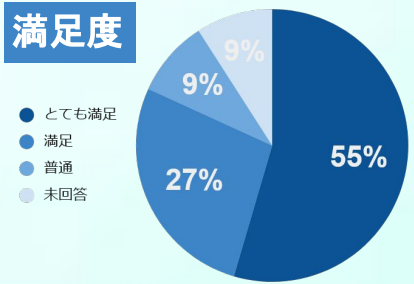
【講義１】
佐々木 祐伴 氏　北海道警察サイバーセキュリティ対策本部　対策・官民連携班長
『情報倫理とサイバーセキュリティ』

受講生の声

- ただ技術力を高めていくだけでは不十分で、その技術を利用する際に伴う責任などを考え、理解する必要があるのだとわかりました。
- 特に印象的だったのは、「誰も見ていないのではなく、自分の行動は常に自分が見ている」という事実です。これまで自分の行動が自分の将来を変えるということはほとんど意識したことがなかったため、今後の自分の身の置き方を考え直すきっかけとなりました。貴重なお話をありがとうございました！

難易度

満足度



講義内容

正しい倫理観をもって技術を使う重要性にフォーカスし、受講生が当事者としてイメージしやすいよう、具体例を交えて説明いただきました。

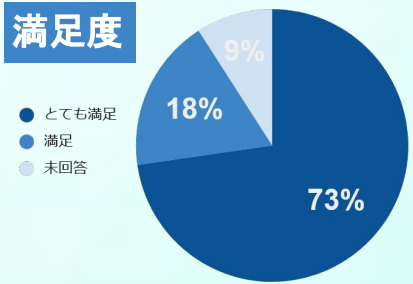
【講義2】首浦 大夢 氏
『Binary Breakdown: Analyzing Malicious Code 』

受講生の声

- 一見ただの文字列の羅列に見えるコードを、どのような順番で解析していくのかを学ぶことができました。今回学んだ解析順序を生かして、自分なりに他の検体の解析にもチャレンジしようと思います。
- マルウェア解析におけるGhidraの使い方とPEファイルの構造、さらにマルウェアの暗号化に関する挙動の分析を学べました。実際のマルウェアを自分で解析できただけでなく、解析できなかった部分については講師の解析ファイルを参照することで、講義後も継続して学習できる点が非常に有意義でした。

難易度

満足度



講義内容

マルウェアの基礎から解析フレームワーク、バイナリ解析手法まで幅広く実践的に学びました。グループ内で意見交換をしながら実際の検体を解析し、攻撃者の意図や行動を読み解くことで、脅威の理解と対策の構築に役立つスキルを身につけました。

『新スパコン見学会』

講義内容

主催であり会場をご提供いただいた、北海道大学情報基盤センターによる「新スパコン見学会」も実施しました。新世代大規模計算機システムに関する解説の後、スパコン室や冷却システムを実際に見学しました。

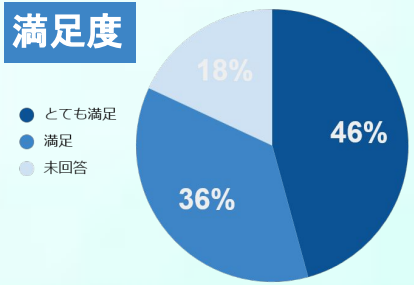
【講義3】扇沢 健也 氏、黒澤 南月 氏
さくらインターネット株式会社情報システム統括室　SIRT
『インシデントレスポンスにおけるフォレンジック入門』

受講生の声

- forensicも知ってはいたが、学んだことがなかったので、必要なツールや基本的な使い方など学ぶことができてよかったです。
- メモリフォレンジックの生の実務者からどこに最初に注目するべきでどこは見なくてもよいかという実務視点での書籍では得られない知識を得られた
- これまで「削除されたデータがよみがえる」というのは魔法のように感じていたのですが、今回の講義をきっかけに自分でもそれができると気付き、ハードルが下がった気がします。実際にメモリダンプなどを体験でき、すごく楽しかったです。

難易度

満足度



講義内容

デジタル・フォレンジックの視点から情報セキュリティを考え、技術を正しく活用するための倫理的観点とセキュリティリスクを学びました。さらに、演習を通してフォレンジック技術を体験しました。

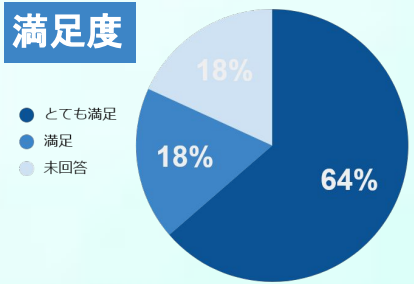
【講義4】蔀 綾人 氏　株式会社フォアーゼット
『蔀 綾人 氏　株式会社フォアーゼット

受講生の声

- hardeningを通じて、攻撃を受けないようにするためにどこを修正すればいいのか模索する過程が面白かったです。
- サーバーのログを確認すること、アクセス権の把握などサーバーを運用するために大切なことを学ぶことができ、競技形式で学ぶことができた点が面白かった。
- 将来redteamで働きたいと思っていたのでどのような脆弱性でどんな攻撃が可能か、などの話はかなり役に立ちました。

難易度

満足度

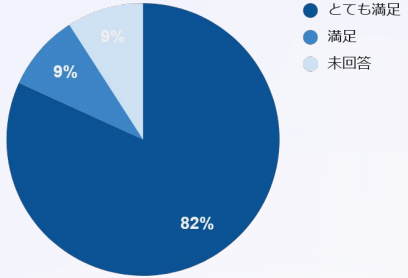


講義内容

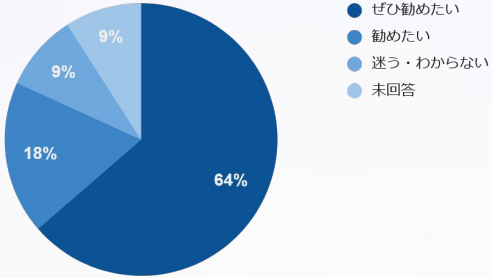
グループでのハンズオン演習を通じて、攻撃手法や検知、復旧について理解を深めました。さらに、 hardening演習を取り入れ、講師が仕掛ける攻撃に対して防御を競い合いながら、サーバーの堅牢化を実践的に体験しました。

事後アンケート

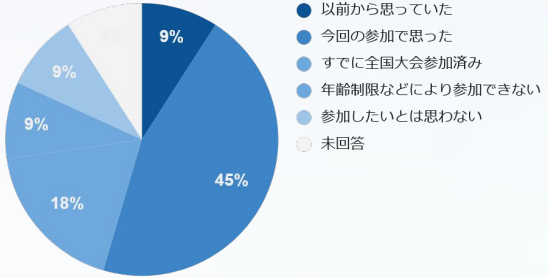
全体の満足度



受講を友人に勧めたいですか？



全国大会に参加してみたいと思いましたか？



受講生の声

- 実際に手を動かしながら学ぶことができ、かつわからないことがあれば講師やチューターの方々にすぐ質問ができるため、セキュリティに興味はあるけどなかなか手を出せなかった方におすすめかなと思います。
- マルウェア解析などを0から個人で始めるのは難しいと思っており、今まで敬遠してきました。本イベントをきっかけにその0を5くらいにすることができ、今後さらに学んでいけるための足掛かりになったと思います。参加できてほんとによかったです。

公式Webサイト・SNS

https://www.security-camp.or.jp/
https://x.com/security_camp
https://www.facebook.com/seccampjapan
https://www.youtube.com/user/securitycampjapan
https://blog.security-camp.or.jp/

次回の参加もお待ちしています！