CySec

初学者向けの基礎的なセキュアインフラ構築の実践

○津田 侑(Turnt Up Technologies株式会社/東京電機大学CySec)
寺田 真敏(東京電機大学未来科学部情報メディア学科)
柿崎 淑郎(東海大学/東京電機大学サイバーセキュリティ研究所)

本資料について

- 本資料は、一般社団法人 情報処理学会 情報処理教育委員会 情報システム教育委員会主催による第18回情報システム教育コンテスト(ISECON2025) の本審査用資料を元に再編集されたものです。
- 本資料（津田 侑, 「初学者向けの基礎的なセキュアインフラ構築の実践」, ISECON2025, 2026.3.8）は、クリエイティブ・コモンズ表示4.0 国際ライセンスの下に提供されています。

関連するJ17-IS LU

- 1108　　通信ネットワークにおけるサービス、信頼性、セキュリティ
- 1122　　ネットワークセキュリティ
- 1613　　セキュリティ機器
- 1905　　セキュアシステム設計

教育の対象者と目標

- 対象者
  - ジュニアレベルのシステムエンジニア・インフラエンジニア

- 目標
  - エンジニアとしてのキャリア形成に必須な土台を形成
    - サイバー攻撃の現状把握と対策に必要な情報収集の修得
    - セキュアインフラ構築のためのセキュリティ機能・ログ分析の基礎知識の習得
    - グループ対抗の競技型演習を通じた基礎知識の実践力の養成

本実践の特徴

- 本講座は「座学」と「競技型演習」の二部構成で実施
  - 座学1.5コマ、競技型演習2.5コマの**4コマ**を1日で実施

- **座学**（知識のインプットと意識付け）
  - サイバー攻撃の現状から「攻撃者の視点」を伝達し、日常的に発生しがちな問題の提示
  - システム堅牢化のための基礎知識の提示
    - 対策のための情報収集方法、システム堅牢化のためのコマンド群、システム異常の発見のためのログ閲覧方法
- **競技型演習**（実践力の養成と評価）
  - **グループ対抗戦形式**で、ウェブサーバ管理者としての基礎知識の実践
    - 実施内容: 座学で得た知識に基づき、システムを「安定稼働させつつ堅牢化する」ことを要求
    - 評価基準: 堅牢化の達成度は加点する一方で、システムの停止、およびサイバー攻撃の兆候の見逃しは減点とし、総合的にスコアリング

本実践の特徴 – 座学パート

- 日常的に発生しがちな問題(サーバ構築あるある話)の提示

1. Linuxをインストールする
2. サービスをインストールして動かす
   - たとえば, Apache + WordPress
3. 動かない…

   ファイアウォール機能(iptables/firewalld)を止める
4. 動かない…

   OSのセキュリティ機能(SELinux)を止める
5. …動いた！！！**(アカン)**

なぜいろいろ無効にするのか

仮説1. 有効にしたせいで、どハマりした経験がある
仮説2.「とりあえず無効にする」と書かれた記事が多い
仮説3. いろいろめんどくさい

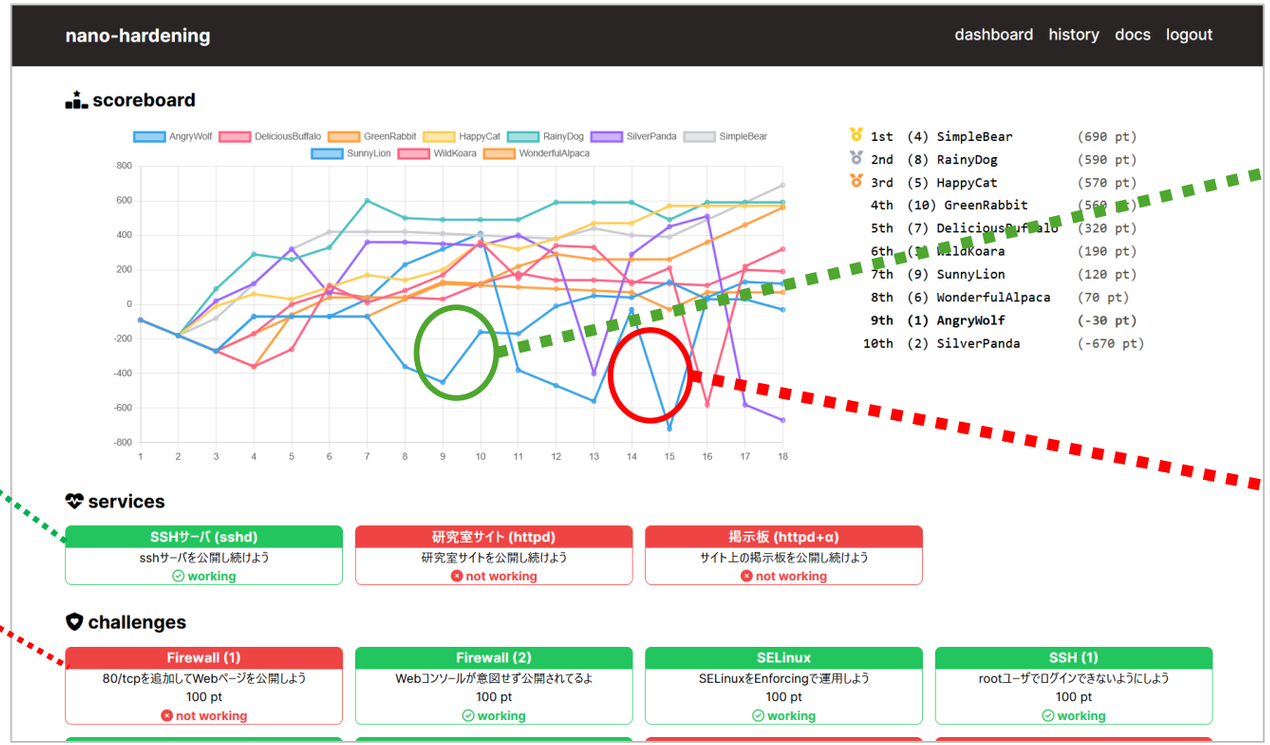
「とりあえず有効のままで」
最低限のことをキチンとやろう

本実践の特徴 – 座学パート

- サイバー攻撃の現状と情報収集
  - 攻撃者のモチベーション
  - 主な攻撃手法と被害
  - 脅威情報サービスの利用法と諸注意
- 安定稼働
  - ログを読めるようになろう
    - /var/logディレクトリのファイル群
      - テキスト形式のログ
      - バイナリ形式のログ
    - journalctl コマンド
- 堅牢化
  - firewalldの基礎
    - firewalldとは
    - 標準で用意されたゾーン
    - firewall-cmdコマンド
  - SELinuxの基礎
    - SELinux(Security-Enhanced Linux)とは
    - SELinuxのモード
    - SELinuxコンテキスト
  - その他の設定
    - sshd関連の設定ファイル
    - sudoの利用/rootでのログイン制限

本実践の特徴 – 競技型演習パート

- グループ対抗戦形式で、ウェブサーバ管理者としての基礎知識を実践
  - 実施内容: 座学で得た知識に基づき、システムを「安定稼働させつつ堅牢化する」ことを要求
  - 評価基準: 堅牢化の達成度は加点とする一方で、システムの停止、およびサイバー攻撃の兆候の見逃しは減点とし、総合的にスコアリングした様子をスコアボードで可視化



堅牢化の達成度は加点

うまく動作しているとき
workingと表示

動作していないとき
not workingと表示

システムの停止・
サイバー攻撃の兆候の
見逃しは減点

本実践の特徴 – 競技型演習パート

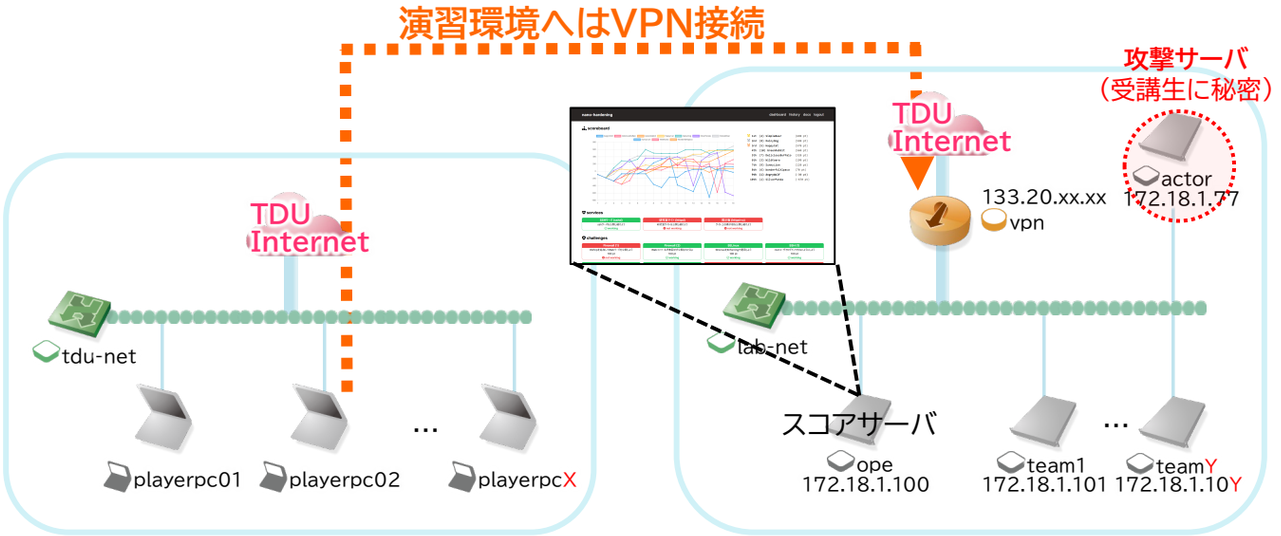
- 演習の進め方
  - 4～5人になるようにグループ分け
    - 研究室のウェブサーバ管理者をロールプレイ
  - サーバ設定経験者には、教える側に回ってもらう
    - 初学者が新配属学生、経験者は研究室の先輩役に

10分毎に減点されてしまうため
減点されないよう対応速度を
上げる必要がある。

グループ内で戦略を練りながら
座学で得た知識を
実践することが要求される。

- 演習シナリオ（受講生に配布）

- みなさんは大学の研究室のサーバ管理を新しく任されました
- このサーバは研究室のWebサイトを外部公開するもので、学生が主体となって管理されています
- 現状、「外部にWebサイトを公開する」のみが達成され、セキュリティ的な検討はされていません
- サーバの設定を改めて確認したところ、標準設定そのままの箇所や、あえて設定を弱めてしまっているところが多々発見されたため、修正することにしました
- 研究室に予算が全くなく設定変更の検証をするためのサーバを購入する余裕もなく、現在運用中のサーバに直接設定していくしかありません
- しかも、先生の講義資料へのリンク等も掲載されているため、ダウンタイムを最小限に留めなければ研究室（先生）の学内での評判に関わります
- このような状況から、みなさんは運用中のサーバのダウンタイムを最小に留め、素早くセキュアにする設定をしていくことに挑むのでした



本実践の特徴 – 競技型演習パート(課題)

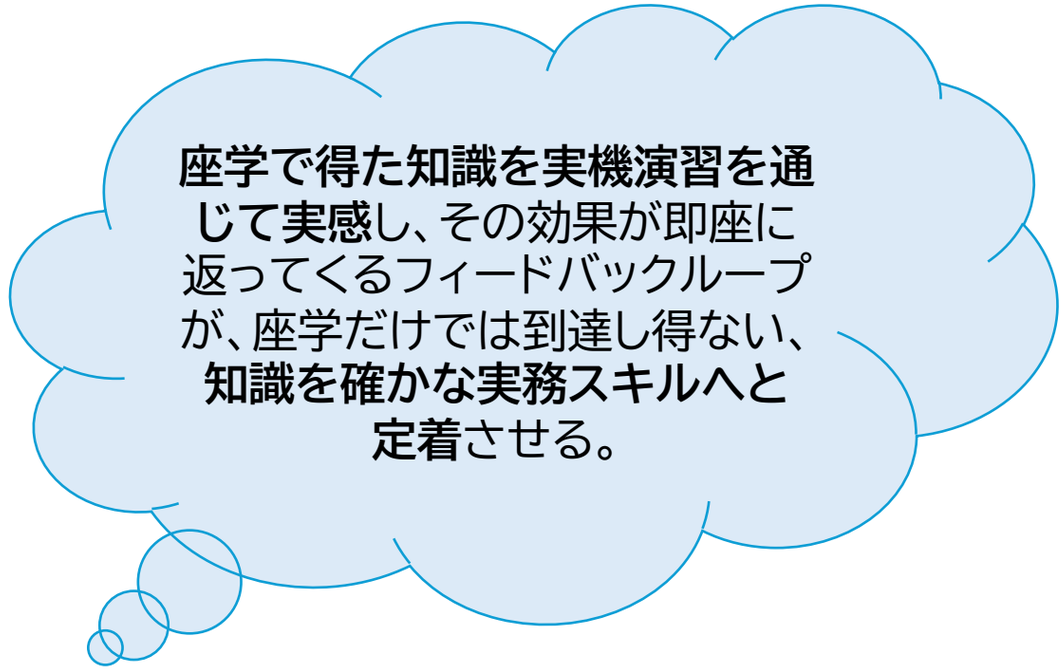
- 安定稼働（3課題）
  - SSHサーバ（sshd） sshサーバを公開し続けよう
  - 研究室サイト（httpd） 研究室サイトを公開し続けよう
  - 掲示板（httpd+α） サイト上の掲示板を公開し続けよう
- 攻撃兆候（1課題）
  - 攻撃をとめろ!! 特定のIPアドレスからの攻撃かも
    （攻撃発生のタイミングは受講生に事前に通知せず）
- 堅牢化（11課題）
  - Firewall（1） 80/tcpを追加してWebページを公開しよう
  - Firewall（2） Webコンソールが意図せず公開されてるよ
  - SELinux SELinuxをEnforcingで運用しよう
  - SSH（1） rootユーザでログインできないようにしよう
  - SSH（2） 公開鍵認証を有効にしよう
  - SSH（3） パスワード認証を無効にしよう
  - Web（1）「研究室限定」が公開されちゃってるよ
  - Web（2）「講義資料」の公開設定がおかしいよ
  - sudo cysecユーザのsudoを許可しよう
  - RFC 9116 脆弱性報告窓口をつくろう
  - マルウェア?? 見覚えのないファイルがある...

教育効果

- ウェブサーバ管理者としての基礎知識を問うものであり、
  システムの堅牢化に向けた基本的な設定に関する出題としている。

【受講者の声】

- 公開鍵の設定については知識として理解していたものの、実際に設定を行った経験はありませんでした。そのため、今回の演習を通じて具体的な手順を学ぶことができ、大変有意義でした。
- SSH 設定、Firewall、SELinux、Web 公開制御など、実務で必要となる基本的なサーバセキュリティ対策を実機で体験できた点が特に良かったです。設定内容がスコアとして可視化されることで、対策の効果を実感しながら学習でき、座学だけでは得られない理解が深まりました。チームで協力しながら課題を解決する流れも、実業務を想定した良い訓練になったと感じます。

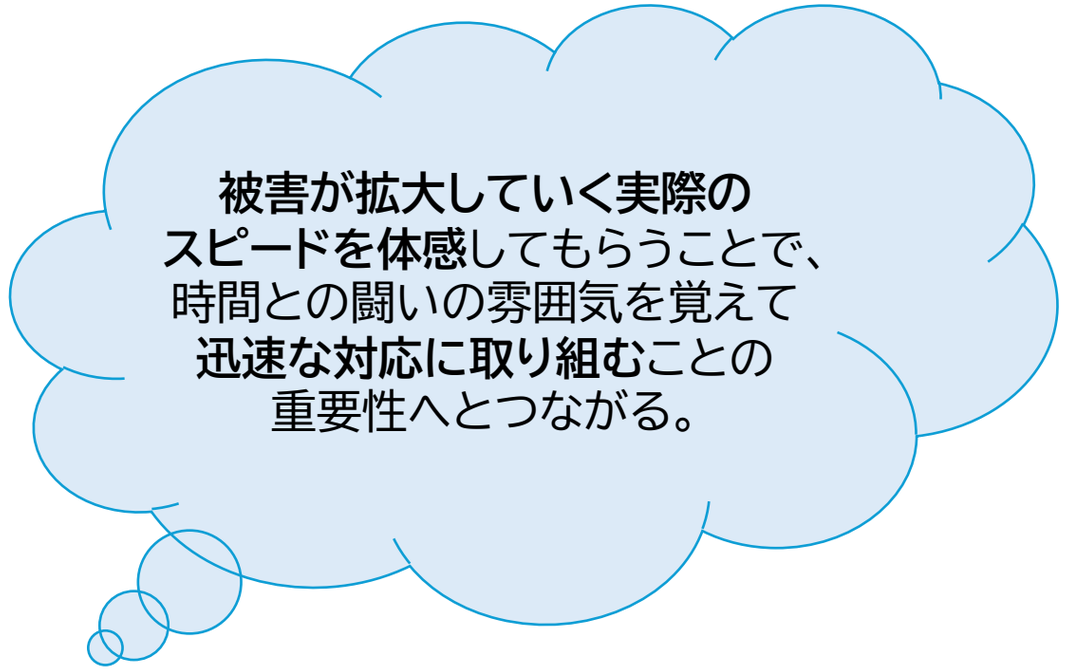


教育効果

- 各グループには座学で得た知識を基にシステムを「安定稼働させつつ堅牢化する」ことを求め、堅牢化できれば加点、システムの停止およびサイバー攻撃の兆候の見逃がしは減点となる。

【受講者の声】

- 演習の最中に演習用サーバ攻撃が起こるイベントに実際の臨場感をもって体験することができた。
- どんどんマルウェアにやられる？状況が可視化されていたので、実際のインシデントのスピードを体感できたため、今後の業務においてもこの雰囲気を覚えて取り組みたいと思った。



教育効果

- グループ内で戦略を練りながら座学で得た知識を実践することが要求されるため、コミュニケーション能力と基礎的な技術力を養成できる。

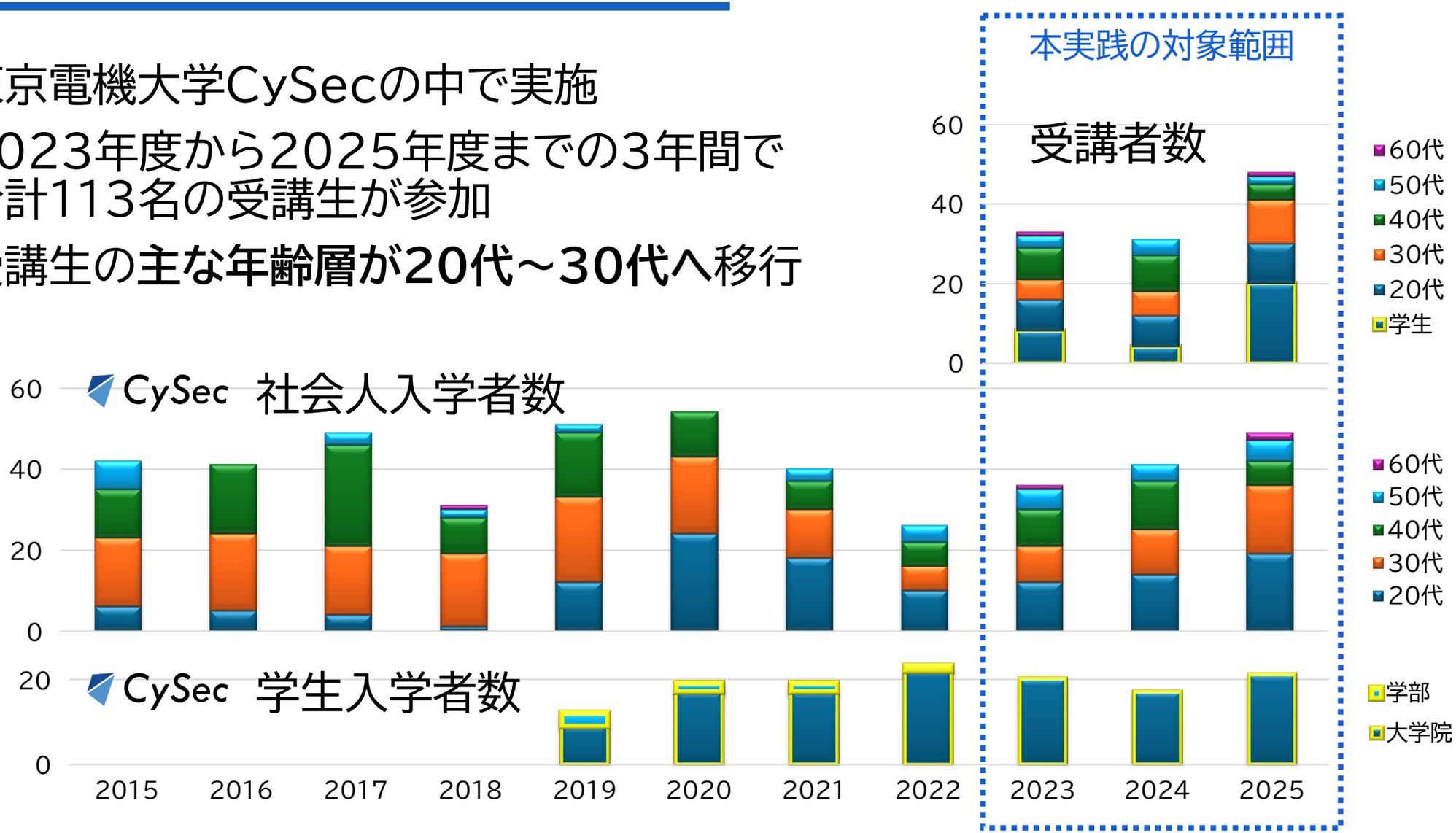
【受講者の声】

- システムの把握から、同じチームメンバーとの意思疎通など、役割分担の重要性も痛感しました。
- インシデントが発生した際の役割分担や、チームで対処する連携などを学ぶことができました。
- 競い合う感覚よりもチーム内の連携がより重視されていた点も良かったです。
- 実際の業務においても、窓口対応や調査・復旧対応などを役割分担して進める場面が多いと思いますが、今回の演習ではそのような動きを疑似的に体験できた点も良かったと感じています。

多岐にわたるタスクを**チームで連携して対処する流れを疑似体験**することで、「競い合う」よりも**「連携する」ことの価値を再認識**し、今後の業務に活きる協調性を養う。

受講生アンケート

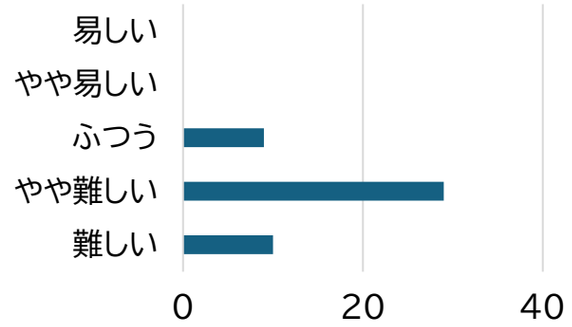
- 東京電機大学CySecの中で実施
- 2023年度から2025年度までの3年間で合計113名の受講生が参加
- 受講生の**主な年齢層が20代～30代へ移行**



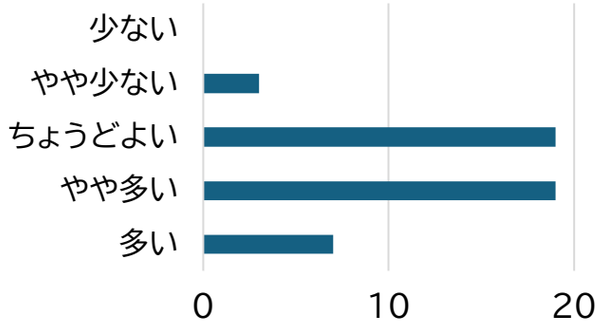
受講生アンケート

- 競技型演習パートでは、バランスのとれた課題レベルと分量であったと判断

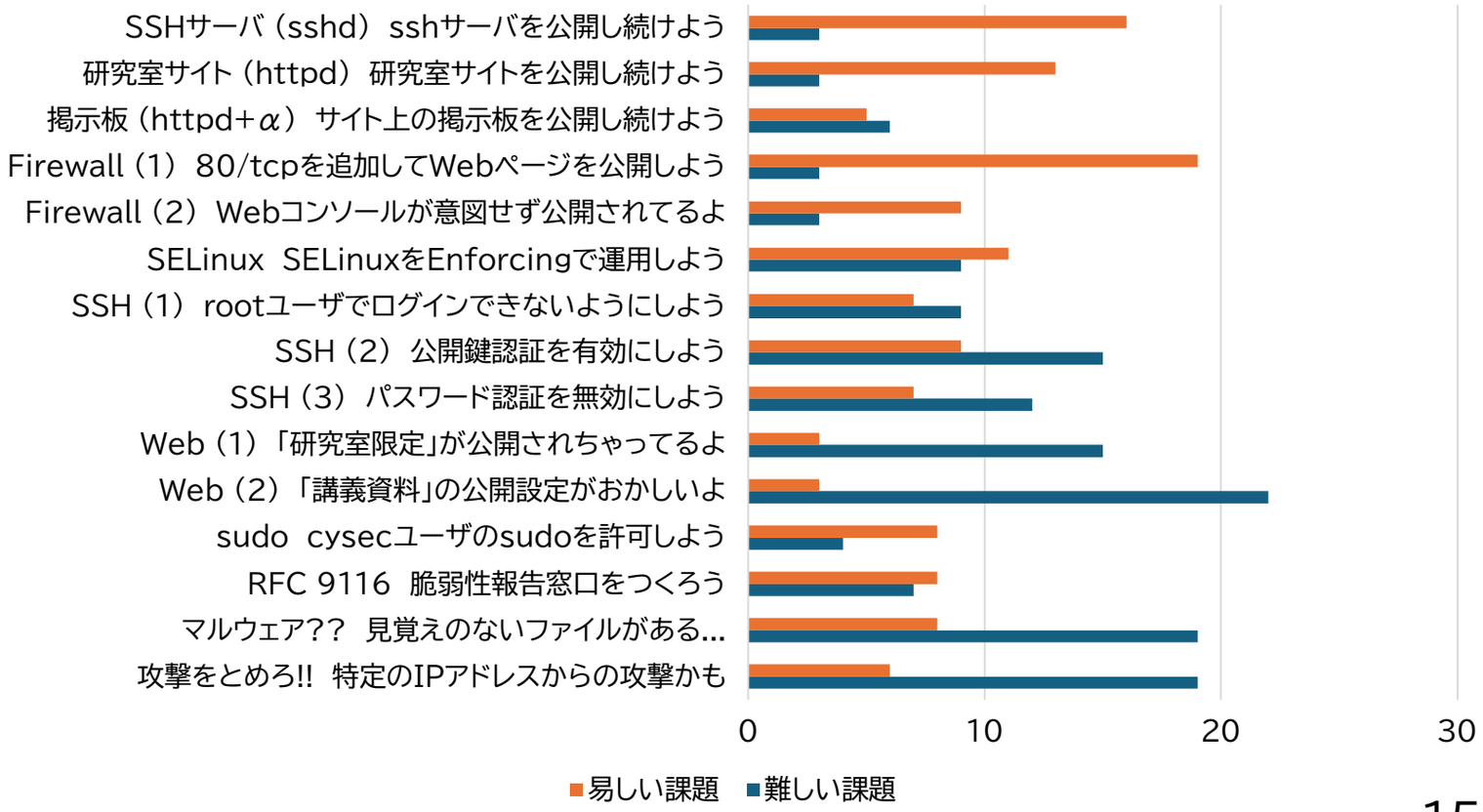
課題の全体レベル



課題の分量



難しい課題と易しい問題



受講生アンケート（自由記述）

- ポジティブな意見

本実践だけに寄らない一般的な意見

- 普段接点がないことを経験することができたこと
- 実体験をすることで、理解が深まった。
- グループを通して課題をやることで自分では解決できないところができるのがよかった

本実践だからこそに関する意見

- サーバの基本的な構築方法を再度学習できることが有意義である点
- 実務では専用のセキュリティ製品を操作することが多く、Linuxに標準で組み込まれているセキュリティ機能に触れる良い機会だった。

- 改善要望の意見

グループワークへの課題

- もう少し個人ワークを導入してほしい。
- 自身で最後までやり切りたかったが、同時編集の場合は、相互影響も発生してしまう恐れもあったので、各課題を難易度別に分けるなどしていただき、個人ワークでやったほうが達成感があったと思う。

Linuxという使い慣れていない利用環境への課題

- Linux操作になれてない受講者用に、その部分についての事前勉強資料があればありがたい。
- Linux全般の知識が不足しているので、同じチームの方に教わりながら実施することができた。

今後の改善

	座学	課題数	競技型演習		個人ワーク
			グループワーク	演習中のサイバー攻撃の発生	
2017年度～2019年度	firewalldの基礎 SELinuxの基礎 その他の設定 ログを読む	3	なし	なし	個人ワークのみ 仮想マシンを配布して個人PCにインポートする形態
2020年度～2022年度		5			
2023年度 2024年度		12	あり		なし
2025年度		15		あり	
2026年度以降	firewalldの基礎 SELinuxの基礎 その他の設定 ログを読む **Linuxコマンドの基礎**	15以上			**全員参加型課題の検討**

