

やってみようCTF

WEST-SEC-CTFからはじまるSECCON登頂への道

九州大学サイバーセキュリティセンター)

学術研究員 藤岡 福資郎

特別インタビュー編「SECCON誕生」

教授 小出洋



AGENDA

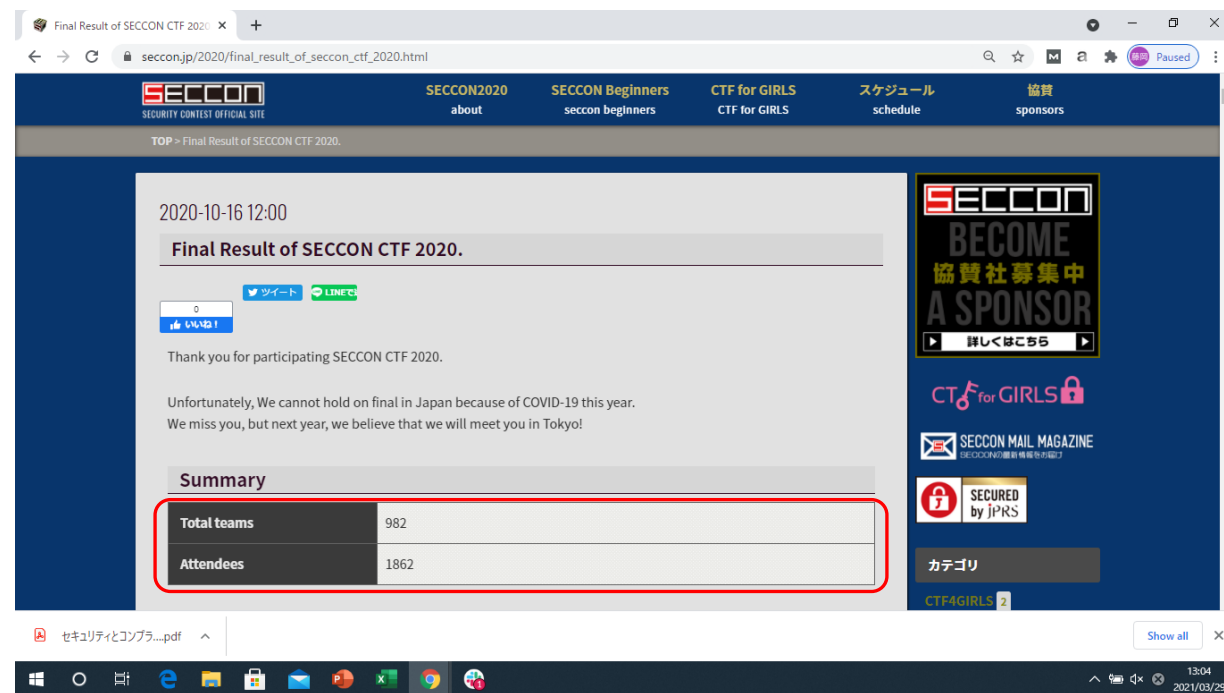
1. CTFとは？
2. CTFを通じて得られるもの
3. CTFを攻略するには？
4. CTFにチャレンジ！
5. まとめ

1. CTFとは？

1. CTFとは？

- Capture The Flagの略称。直訳をすると旗取りゲームです。
- 準備された多岐にわたるセキュリティに関する問題を解くと「Flag」(=回答となる文字列)が表示されます。
- 文字列を問題の解答欄に投入すると「正解！」となり、スコアが加算されます。制限時間内にスコアの合計点を競います。
- 世界各地でCTFは、実施されています。(https://ctftime.org/)

日本の代表的なCTF「SECCON」には、毎年1000近いチームが参加。技術力を切磋琢磨している。



【出所】https://www.seccon.jp/2020/

【WORK】SECCONには、どんな問題がでるのか？また、ctftime.orgで過去3年間のCTFの開催回数の推移を調べてみましょう【制限時間30分】

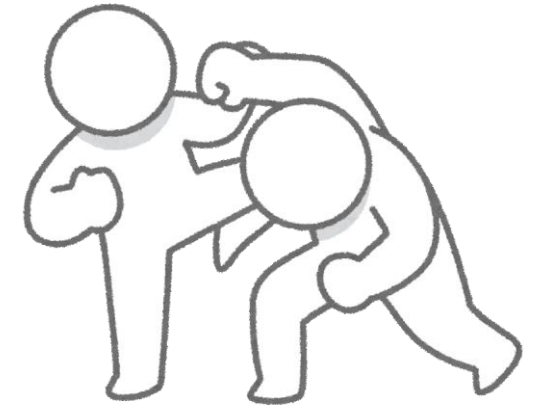
1. CTFとは？

Capture The Flag, サイバーセキュリティ技術を中心とした情報系の技術コンテスト

コンテストによりルールはさまざま(後述)

さまざまな技術を駆使して未知の課題に取り組む必要がある

- プログラミング, 暗号, ネットワーク, OS, バイナリ, ...
- 場合により技術以外(マネジメント, ビジネス系)のスキルも



→ 技術系総合格闘技とも呼ぶ人もいる

SECCONは政府のサイバーセキュリティ戦略本部からで
てくる年次報告などに載っている日本最高峰のCTF.
情報セキュリティ白書や世界先端IT国家創造宣言にも紹
介。 千里の道も一歩から登頂を目指しましょう！



九州大学



1. CTFとは？（特別インタビュー編）

SECCON誕生

サイバーセキュリティコミュニティへの参入

- 「九工大に特別講師としてきていた日立システムズ本川さんからの紹介で「脅威と対策研究会(岡谷隊長が代表)」に参加
- 当時IPAセキュリティキャンプ実行委員長だった宮本久仁男氏と再会(電通大で同期だった)
- サイバーセキュリティコミュニティの要人と知り合いになる

福岡の勉強会にて園田道夫氏に合う

- サイバーセキュリティ人材育成に課題があるという問題意識を共有
- 日本でもCTFをやりたい
→小出が初回のローカルアレンジを担当

第一回 SECCON CTF を開催

- 2012年2月九工大飯塚キャンパス(SECCON CTF 福岡大会(九州地区予選))
- メディアからの取材が殺到するなど反響が大きかった
- その後の多くの課題を洗い出すことができた



1. CTFとは？ ～九州大学での実施の様相

攻防戦型CTF(Capture The Flag)

Hiroshi Koide
@hirosk

今日の九大 ProSec-ITは服部祐一さんをお招きして、ちょっとすすんだ攻防戦演習です！
#enpit



10:41 - 2018年12月15日

2件のリツイート 2件のいいね



🗨️ 2 🍷 2 📊

Hiroshi Koide
@hirosk

いやあ攻撃防戦CTF楽しそう！ #九大
ProSecIT #enpit



14:23 - 2018年12月15日

2件のリツイート 4件のいいね



🗨️ 1 🍷 2 🍷 4 📊



Hiroshi Koide @hirosk · 2018年12月15日
結果はこんな感じ。振り返り中！



🗨️ 1 🍷 1 📊



九州大学



1. CTFとは？ ～九州大学と大阪大学連携型での実施の模様

阪大との連携CTF(Capture The Flag)



Hiroshi Koide
@hirosk

今日は阪大と連携してのCTF大会事前準備勉強会です。トレンドマイクロの新井さんNICTの藺田さんが登場！ #enpit



10:50 - 2019年1月26日

4件のリツイート 5件のいいね



4

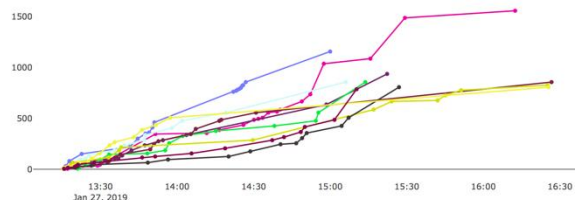


5



Prolog CTF Notifications Users Scoreboard Challenges Profile Settings Logout

Top 10 Teams



enPiTCTF{XXXXXX}

Web, バイナリ, フォレンジクスなどさまざまなジャンルから出題

阪大と連携して遠隔講義, クラウドを活用して実施

トレンドマイクロ, 日本総研, NICTが実施協力



九州大学



Challenge & Training Fukuoka

【WORK】SECCONには、どんな問題がでるのか？また、
ctftime.orgで過去3年間のCTFの開催回数の推移を調べて
みましょう【制限時間30分】

1. CTFとは? ~演習

https://CTFtime.org

The screenshot shows the CTFtime.org website. The top navigation bar includes links for CTFs, Upcoming, Archive, Calendar, Teams, FAQ, Contact us, and About, along with a Sign in button. The main content area is divided into three sections: Team rating, Past events, and Upcoming events.

Team rating

2020 2019 2018 2017 2016 2015 2014 2013 2012 2011

Place	Team	Country	Rating
1	perfect blue	USA	769.384
2	More Smoked Leet Chicken	Russia	756.889
3	A*0*E	China	602.892
4	Plaid Parliament of Pwning	USA	593.144
5	p4	Russia	485.792
6	OpenToAll		459.087
7	justCatTheFish	Russia	430.399
8	redpwn	USA	419.301
9	TokyoWesterns	Japan	408.608
10	Corrupted Pwnis	Russia	402.766

Full rating | Rating formula

Past events

With scoreboard All

UNICORN CTF 2020
8月 10, 2020 10:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points *
1	YummyTacos	Russia	0.000
2	cpls	Russia	0.000
3	Платцкартный вагон #49		0.000

285 teams total | Tasks and writeups

DEF CON CTF 2020
8月 09, 2020 21:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points
1	A*0*E	China	192.000
2	Plaid Parliament of Pwning	USA	143.802
3	HITCON x Balsn		115.233

16 teams total | Tasks and writeups

Upcoming events

Open Academic Finals

PoseidonCTF 1st Edition
8月 09, 2020 17:00 UTC | On-line | Weight voting in progress

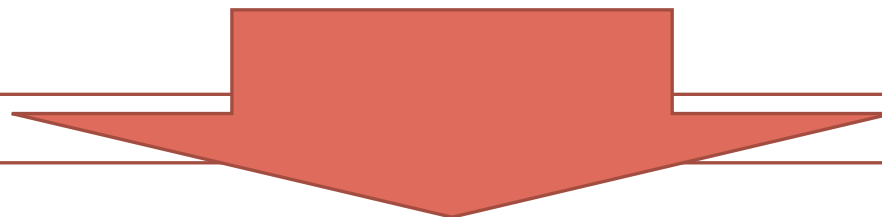
世界中のCTFの日程
CTFのランキング
チームのランキング



2.CTFを通じて得られるもの

1. どのような問題がでるのか？ 何が身につくのか？ 【メモを取りましょう】

- **【WORK】**どんなジャンルの問題がでるか？その内容は何か？ など技術的な出題が主です。
- **【WORK】**どんな形式があるか3種類は何か？ 2種類があります。
- CTFの大会には、様々なレベルがあります。初心者むけ(for ビギナー等)を選ぶとよいでしょう。
- 特に記載のないものは、非常にレベルが高いものもあり、参加したけれどほとんど解けなかったということがあります。



-
- **【WORK】**何を得られそうか？得てみたいか？ 3つ予想してみましょう。【10分】
-

2. CTFの実施形式

Jeopardy形式

個人プレイあるいはチーム形式

最も一般的な形式(この形式のCTFが多い. オンラインだとまずこの形式)

プレイヤはフラグを答え, 正解するとポイントが入る

フラグは一定の形式のキーワード

プレイヤ(あるいはチーム)はポイントを競い合う

AROUND THE WORLD	RECENT MOVIES	STAMPS	BRAND NAMES	THE BIBLE	BEFORE & AFTER
\$200	\$200	\$200	\$200	\$200	\$200
\$400	\$400	\$400	\$400	\$400	\$400
\$600	\$600	\$600	\$600	\$600	\$600
\$800	\$800	\$800	\$800	\$800	\$800
\$1000	\$1000	\$1000	\$1000	\$1000	\$1000



九州大学



Challenge & Training Fukuoka

2. CTFの実施形式

攻防戦形式(Attack & Defense)

チーム形式が多い

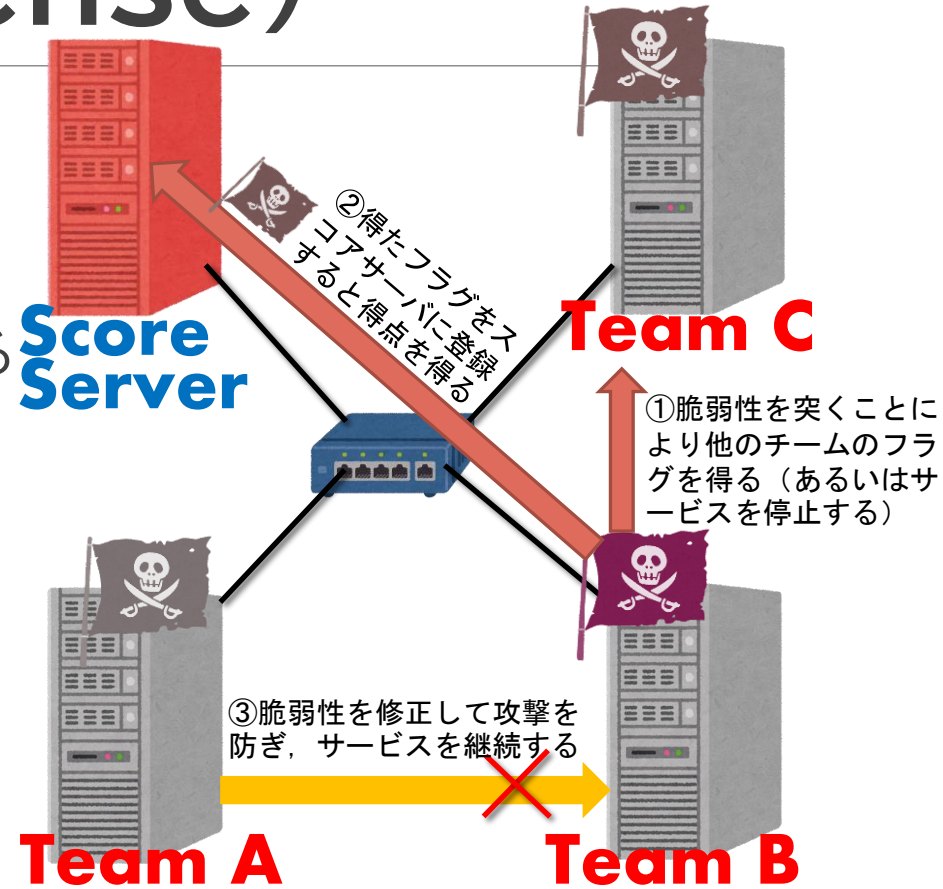
各チームに割り付けられた脆弱性を持つサーバを守り、
かつ他のチームのサーバを攻撃する

チームで脆弱性が仕込まれたサーバの脆弱性を修正することで守る
また他のサーバに仕込まれている脆弱性を突くことにより攻撃する

他のサーバへの攻撃が成功することによりポイントを得る
(Attack Point)

自分のサーバのサービスを停止させず長く継続することにより
高いポイントを得る(Defense Point)

チームは総合ポイントを競い合う



九州大学



Challenge & Training Fukuoka

2. CTFの実施形式

King of the Hill

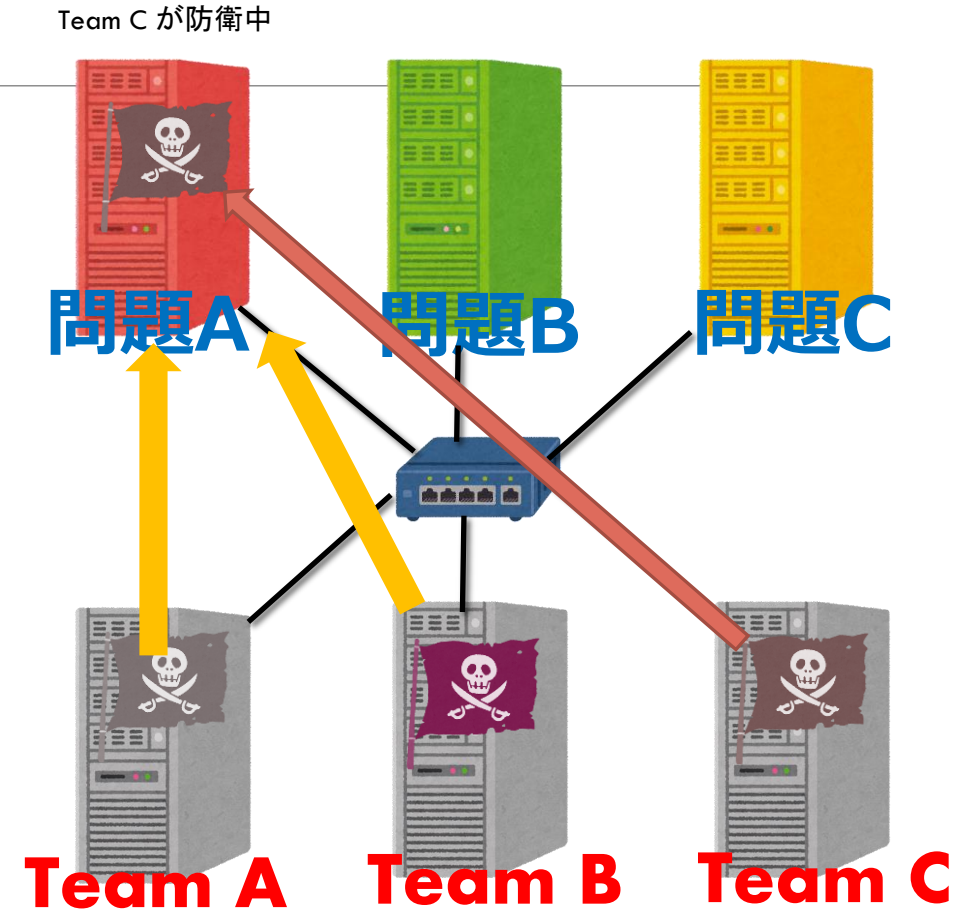
SECCON Final の方式

Attack & Defenseと似ているが問題サーバは独立に置かれる

各問題サーバの問題を解きフラグを見つけるとポイントが得られる(Attack Point)

各問題サーバに自チームのフラグを書き込み, 長時間防衛するとより高いポイントが得られる(Defense Point)

チームは総合ポイントを競い合う



九州大学



Challenge & Training Fukuoka

3. 出題される問題の種類

サイバーセキュリティは総合技術→情報技術全般

Crypto…… 暗号技術

Network ……ネットワークセキュリティ

Web …… Webセキュリティ

Binary ……バイナリ解析

Programing・ プログラミング

Pwn ……プログラムの脆弱性

Forensic ……フォレンジクス, 攻撃などの情報を収集

Hardware ……ハードウェア, IoT技術

Misc ……その他

プレイヤー, コンテストにより得意不得意が存在

チームではお互い補い合うと良い

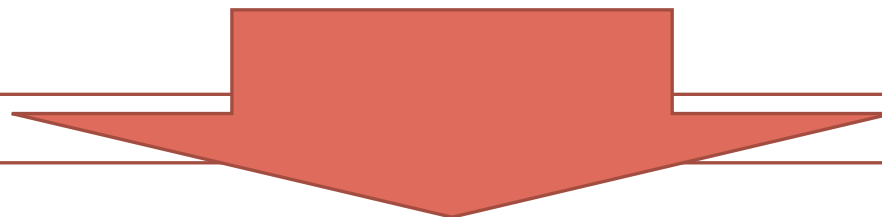


九州大学



1. どのような問題がでるのか？ 何が身につくのか？

- 暗号、フォレンジック解析、Webアプリケーション解析、バイナリ解析 など技術的な出題が主です。
- Jeopardy形式(クイズ形式の問題に回答するもの)、Attack & Defense形式(チーム対チームの攻防戦)、King of the Hillの2種類があります。
- CTFの大会には、様々なレベルがあります。初心者むけ(for ビギナー等)を選ぶとよいでしょう。
- 特に記載のないものは、非常にレベルが高いものもあり、参加したけれどほとんど解けなかったということもあります。



- 自分で勉強する力(=世界の最先端にとどまり続けるための基礎力)
- チームワーク(=人脈ネットワークの広がり。切磋琢磨する中での気づき)
- 最新の技術トピック(=事前準備での勉強やCTFの出題問題)

アウトプットから
入るから
CTFは、学習効
果が高い！

3. CTFを攻略するには？

1. CTFのサイバーセキュリティ教育への活用

サイバーセキュリティ

多岐にわたるさまざまな技術を駆使する総合技術

- プログラミング, 暗号, ネットワーク, OS, バイナリ, フォレンジクス, ハードウェア, Webセキュリティ, 技術以外...

CTFを教育に利用すると..

チームで身につけたいろいろな技術を駆使して限られた時間内で未知の課題に取り組むCTFはさまざまな理由により教育的な効果が高い

- ゲーム性がある(楽しい！)
- 切磋琢磨できる環境ができる(あいつには負けられない！)
- 同じ指向を持つ(学校では見つけられない)仲間を得ることができる
- **完全に身につけた情報技術をすばやく活用**

→ 現代の寺子屋



2. 「完全に身につけた情報技術をすばやく活用」の例

CTFの問題を効率良く解くにはエンジニアの通常業務でも必要な多くのTIPSを組み合わせる必要がある. 以下は例.

すばやくサーバを立てる(netcat/pythonなど)

```
% nc -l -p 2222
```

```
% python3 -m http.server 2222
```

すばやく基数変換を行う(python/web上のツール/関数電卓など)

```
$ python3 -c "print(int('c0ffebabe', 16))"
```

```
51807959742
```

```
$ python3 -c "print(format(11259375, 'x'))"
```

```
abcdef
```



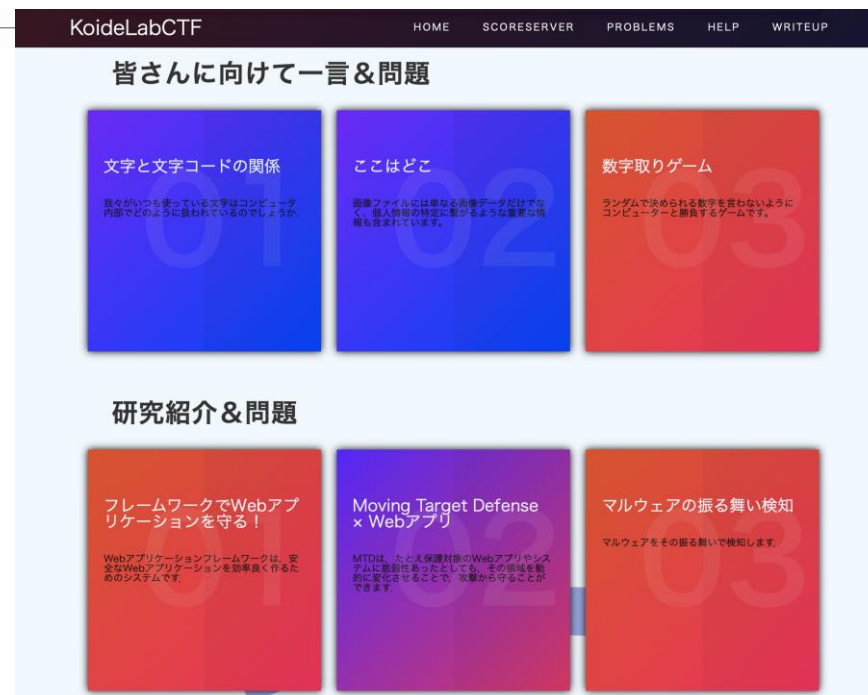
3. CTFのサイバーセキュリティ教育への活用 CTFは個人戦からチーム戦へ発展可能

CTFは個人戦からチーム戦へ発展可能

- チーム活動で培うスキルも得られる！
- 強いチームの形成が可能
 - ノウハウの蓄積
 - チーム内での切磋琢磨などの良い循環
 - ランキングでチームの客観的な評価

CTFの開催

- CTFのシステム運営(クラウドやサーバを複数運用)
- 問題作成(最新技術を問題に、プレイヤーからの評価)
- 組織運営



5. 参考になる文献一覧

令和3年3月29日
九州大学

NO	書籍名	著者
1	セキュリティコンテストチャレンジブック	碓井 利宣 (著), 竹迫 良範 (著), 廣田 一貴 (著), 保要 隆明 (著), 前田 優人 (著), 美濃 圭佑 (著), 三村 聡志 (著), 八木橋 優 (著), SECCON実行委員会 (監修)
2	セキュリティコンテストのためのCTF問題集	清水 祐太郎 (著), 竹迫 良範 (著), 新穂 隼人 (著), 長谷川 千広 (著), 廣田 一貴 (著), 保要 隆明 (著), 美濃 圭佑 (著), 三村 聡志 (著), 森田 浩平 (著), 八木橋 優 (著), 渡部 裕 (著), SECCON実行委員会 (監修)
3	サイバーセキュリティテスト完全ガイド	Peter Kim (著), 株式会社クイープ (翻訳), 保要 隆明 (翻訳, 監修), 前田 優人 (翻訳, 監修), 美濃 圭佑 (翻訳, 監修), 八木橋 優 (翻訳, 監修)
4	ハッキング・ラボの作り方	IPUSIRON (著)
5	はじめて学ぶバイナリ技術	小林 佐保 (著), 岡田 怜士 (著), 浅部 佑 (著), 満永 拓邦 (著)

4. CTFにチャレンジ！

1. CTFを攻略するためには？

- 書籍(＝問題集)による学習。
- 初心者向けのCTFに参加する。
- 分からなかったところを他の参加者から習う。(＝ミートアップ)

はじめての一步は、

- 例えば、クイズ形式、チーム対抗戦に加え、ゲーミフィケーションを用いたチームで回答する「8割」回答できるNTT西日本が提供する「WEST SEC CTF」
- 特に技術系以外のセキュリティを担当する仲間との協力やコミュニケーションが生まれる点が特徴。

2. 早速！WEST-SEC CTFにチャレンジしよう！

- WEST-SEC CTF サイト <https://west-sec.com/>
- 申込ページ <https://west-sec.connpass.com/>

助け合い、楽しむこと。
教えあうことに力点を置いてください！ ☆≡

初心者向け、学生向けなど目的にあわせたCTF大会と勉強コンテンツを体験しよう。



- 申込ページ <https://west-sec.connpass.com/>

3. 攻略のヒント ～ワークシートにグループ名と目標 担当者を決めよう

• グループ名

• 目標

NO	項目	担当
1	なぜなぜ、脳トレ	
2	暗号	
3	CASE STUDY	
4	法制度規制	
5	脆弱性管理・インシデント対応	
6	セキュリティ対策危機	
7	ログ分析	
8	認証とPKI	
9	サーバ	
10	セキュアプログラミング	
11	Fortigate	

5. まとめ

相互フィードバック

1. 輝いていた人と輝いていたところを書き出して褒め合いましょう☆彡

• グループ名

• 目標

NO	項目	輝いていた人	輝いていたところ
1	なぞなぞ、脳トレ		
2	暗号		
3	CASE STUDY		
4	法制度規制		
5	脆弱性管理・インシデント 対応		
6	セキュリティ対策危機		
7	ログ分析		
8	認証とPKI		
9	サーバ		
10	セキュアプログラミング		
11	Fortigate		