実戦競技による高度セキュリティエンジニア人才育成

株式会社ラック
サイバー・グリッド・ジャパン
サイバー・グリッド研究所

**実際のサイバー攻撃手法を、
自分の手で「試す」・自らのサービスで「受ける」。
実戦型セキュリティ人才育成。**

自主開催社内CTF競技会による サイバー攻撃知識の向上

社内CTF競技会”LACCON”の開催

ラックグループ全社員が参加できるセキュリティ競技会「LACCON」を開催しています。
LACCONは、競技運営・問題作成ともに当社社員有志によるボランティアで運営されている競技会です。過去3回が開催され、のべ500人が参加しています。

CTF(CaptureTheFlag)とは

セキュリティの知識を駆使して「フラグ」を取得し、合計得点を競う技術競技です。国内ではSECCON、海外ではDEFCONやBLACKHATなどが有名なCTFとして知られています。

Jeopardy（ジョパディ）形式
カテゴリごとにクイズ形式表示される問題を解いて得点を重ねる方式です。

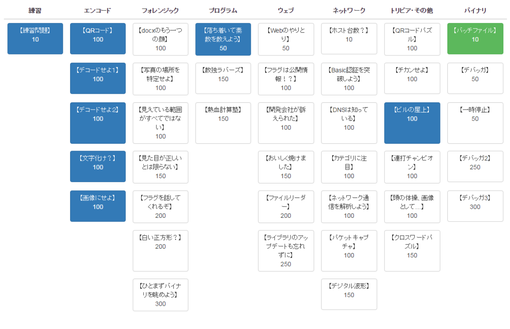
Attack-Defense
攻防戦と呼ばれる、脆弱なサーバにある情報を争奪する形式です。

出題ジャンル

実際の攻撃や分析手法のカテゴリに応じ、多岐にわたります。問題カテゴリごとに必要なスキルが異なり、多様な攻撃手法に触れることができます。

- ✓ ネットワークWeb
- ✓ バイナリ、Exploit
- ✓ 脆弱性
- ✓ プログラミング
- ✓ フォレンジック
- ✓ トリビア

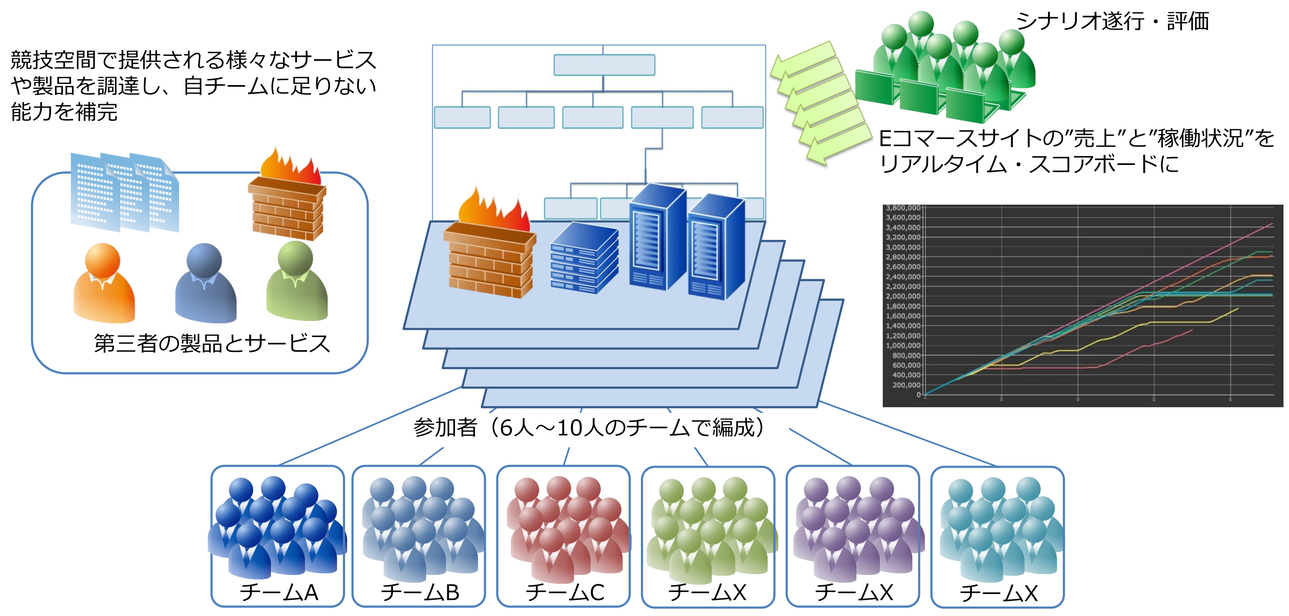
など



サイバー攻撃体験によるインシデント レスポンスの実践

Hardening Project

サイバー・グリッド研究所は、WAS Forum主催のHardening Projectの開催に協賛・技術協力を行っています。
Hardeningは、インターネットの縮図を実現した環境で、11時間にわたる競技時間中、限られたリソースを最大限に生かしビジネス価値の最大化を競う実践競技です。



仮想ECサイトへの攻撃対処・報告・対策から学ぶ

Hardeningでは、参加者の運営する仮想ECサイトへの断続的なサイバー攻撃が行われます。参加者はこのサイバー攻撃に対処しながら、適宜上層部役への報告、世間への公表、報道対応などを実際に体験することができます。

ビジネスの視点
Focus on prevention techniques and process

守る技術の顕彰
Engineering awards and talent discovery

利用者視点の認識向上
Perspective for stakeholder communication

理論だけでは分からない、発覚からの対処

現実に業務の中で体験できる機会はなかなか存在せず、体制構築を行っていてもどのように対処を行うべきか、運用上の考慮不足などに気が付きにくいのがサイバー攻撃です。
現実の攻撃手法を反映した模擬攻撃に対処することで、インシデントレスポンスの実践的活動を体験的に理解することが可能になります。

サイバー・グリッド研究所／個別研究テーマの紹介

株式会社ラック
サイバー・グリッド・ジャパン
サイバー・グリッド研究所

**デジタル化する社会が、
安全・安心であるために。
先端テクノロジー×サイバーセキュリティ研究。**

サイバー・グリッド研究所について

サイバー・グリッド・ジャパンに所属しているサイバー・グリッド研究所は、最先端のサイバー攻撃事例研究、人材育成、セキュリティコミュニティ活動支援、学校・官公庁・民間企業向け講演・授業、執筆活動などを通じてデジタル社会の安全形成に努めています。

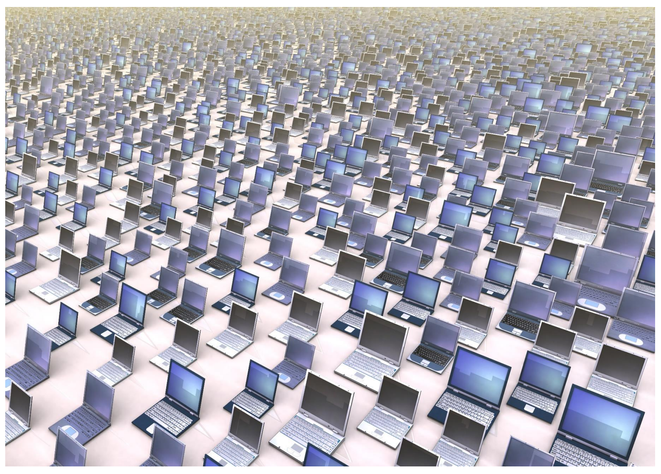
サイバー・グリッド研究所の研究活動

サイバー・グリッド研究所では、デジタル化する社会に求められる基礎的テクノロジーについて、今後重要視される重点技術分野に対して利活用やセキュリティ観点での調査・研究を外部組織とともに行っています。

ブロックチェーン・スマートコントラクト研究

非中央集権的な金融テクノロジーとして利活用が進んでいる、ブロックチェーン・スマートコントラクトについての研究を行っています。

- 暗号通貨への攻撃と防御
- スマートコントラクトを活用した社会システムの実証研究
- スマートコントラクトへの攻撃と防御
- 介護・ヘルスケアへの応用
- 偽造データの検出・排除



サイバー攻撃・脆弱性検知即応環境研究

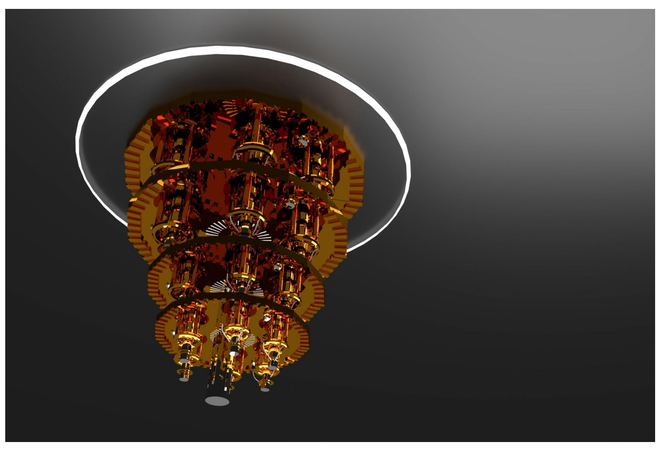
シミュレーション実務環境下における、新規脆弱性の即時検証実施と回避策の即時立案支援研究を行っています。

- 脆弱性の発表された内容に対して影響度調査や再現確認を行える、一般的なオフィス環境を模したネットワーク環境を構築
- 環境（OSアップデート適用状態）に合致したゼロデイ回避策の即時立案を支援
- HardeningやCTF環境等セキュリティ実戦学習への応用

イマーシヴ・インターフェース研究

IoTの進化によってデジタル・ツイン化（フィジカル空間のデータ化）する社会における、コンピュータ環境遍在化のためのユーザインターフェース研究を行っています。

- バーチャルリアリティシステム研究
- MixedRealityインターフェース研究
- VRコンテンツセキュリティ研究
- AR利活用研究
- ビジネスコミュニケーションにおけるテレイグジスタンス・テレプレゼンス研究



量子コンピュータ研究

量子ゲートによって、量子力学的な重ね合わせを用いた演算が可能な量子コンピュータ利活用やセキュリティ面からの調査研究を行っています。

- 量子アニーリング(D－Waveマシン）で解決できる最適化組合せ問題設定研究
- 交通量最適化問題研究
- 量子コンピュータによるセキュリティ・量子暗号通信
- 接続機器の負荷分散