LAC
ともに、イキル

実戦競技による高度セキュリティエンジニア人"才"育成

サイバー・グリッド研究所　仲上竜太

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
仲上竜太

サイバー・グリッド研究所

仲上　竜太

株式会社ラック
サイバー・グリッド・ジャパン
サイバー・グリッド研究所長
情報安全確保支援士(登録番号第005254番)

進化し続けるデジタルテクノロジーについて、サイバーセキュリティの観点から、「作る面」「使う面」からの安全な利活用方法を研究。

専門分野：脅威情報インテリジェンス
ブロックチェーン・スマートコントラクト
イマーシヴ・インターフェース

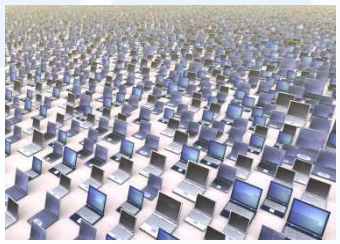
趣味は海釣り

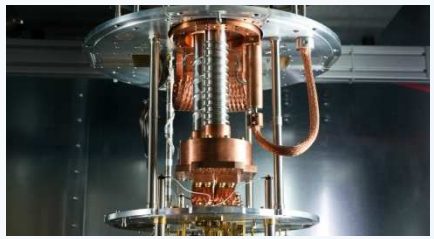
CYBER GRID JOURNAL Vol.4
2017.9.1
「攻撃者の先を行く！進化するサイバー攻撃から 日本を守る脅威情報の取り組み」

サイバー・グリッド研究所の紹介

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・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。

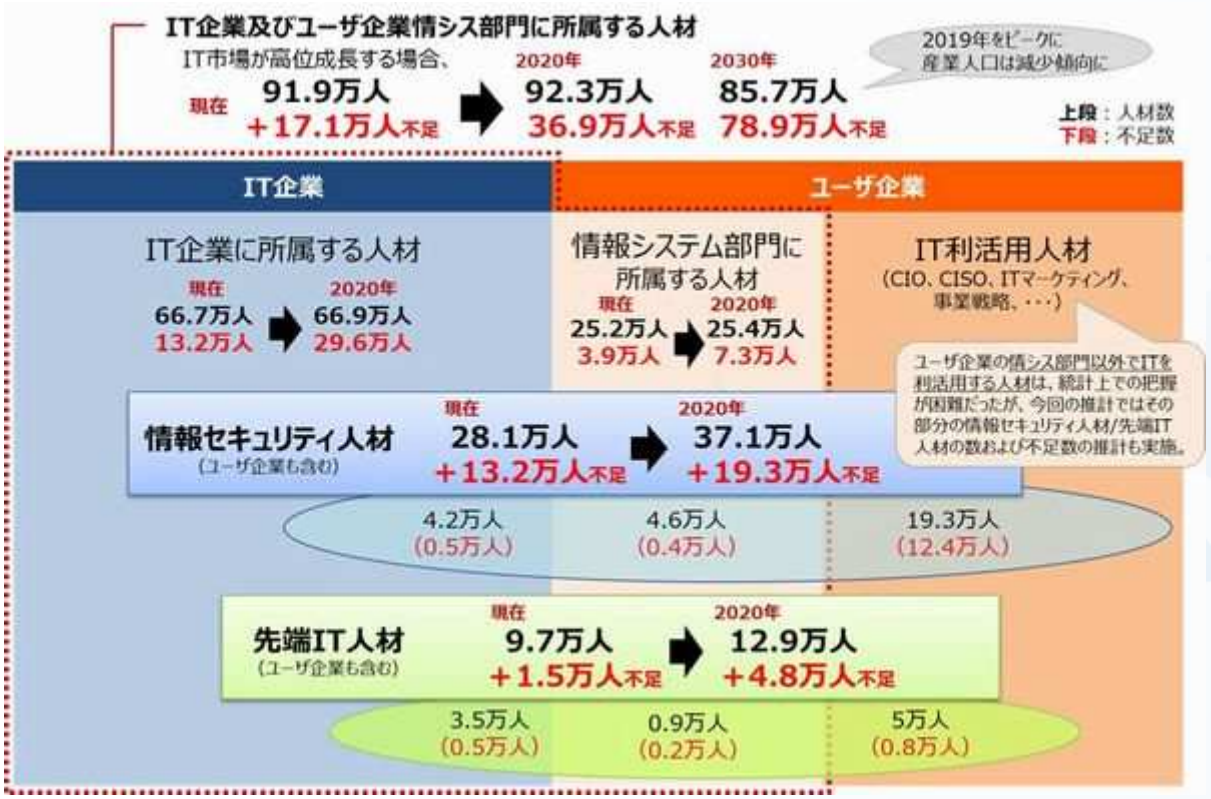




☜☜☜☜☜☜研究テーマの紹介は展示ブースにて

セキュリティ人材不足！？

情報セキュリティ人材の不足が大きな課題となっています。



情報セキュリティ人材
2016年：
28.1万人
13.2万人不足

2020年：
37.1万人
19.3万人不足

よく言われる

2020年に情報セキュリティ人材19万人不足説

出典：経済産業省のIT人材の最新動向と将来推計に関する調査(2016)

セキュリティ人材不足！？

情報セキュリティ10大脅威（組織）

脅威に対応するためのセキュリティ人材の不足

2018(2018/4/27発表)

順位	組織
1位	標的型攻撃による被害
2位	ランサムウェアによる被害
3位	ビジネスメール詐欺による被害
4位	脆弱性対策情報の公開に伴う悪用増加
5位	脅威に対応するためのセキュリティ人材の不足
6位	ウェブサービスからの個人情報の窃取
7位	IoT機器の脆弱性の顕在化
8位	内部不正による情報漏えい
9位	サービス妨害攻撃によるサービスの停止
10位	犯罪のビジネス化（アンダーグラウンドサービス）

2019(2019/1/30発表)

順位	組織	昨年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
5位	内部不正による情報漏えい	8位
6位	サービス妨害攻撃によるサービスの停止	9位
7位	インターネットサービスからの個人情報の窃取	6位
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開に伴う悪用増加	4位
10位	不注意による情報漏えい	12位

ランク外!?

情報セキュリティ10大脅威 2018
https://www.ipa.go.jp/security/vuln/10threats2018.html

情報セキュリティ10大脅威 2019
https://www.ipa.go.jp/security/vuln/10threats2019.html

セキュリティ人材不足！？

セキュリティー人材、消えた「19万人不足」

NIKKEI BUSINESS DAILY 日経産業新聞

https://www.nikkei.com/article/DGXMZO34590330U8A820C1X11000/

サイバー攻撃の増加を背景に、情報セキュリティー人材の不足を指摘する声が多い。経済産業省の2016年の調査では「20年に国内で19万3000人が不足する」と予測したほどだ。だがサイバー防衛の現場からは「不足感はない」との反論が多い。

不足感がない理由：

セキュリティベンダーへの委託

AI活用セキュリティサービスの導入

事案発生頻度によるもの

現場に必要なセキュリティ人材とは？

組織の持つ情報資産には「全員」が関与している


サービス開発者


運用担当者


情報システム担当者


営業担当者


総務担当者


経営者

…

現場に必要なセキュリティ人材とは？

組織の持つ情報資産には、「全員」が関与する状況


システム開発者


運用


情報


営業


務担当者

者

情報インシデント発生時、突然当事者に。

情報漏洩

WEB改ざん

機密情報窃取

内部不正

不正送金

IT設備破壊

現場に必要なセキュリティ人材とは？

必要なのは
「セキュリティ意識を持った」人材


サービス開発者　＋セキュリティ


運用担当者　＋セキュリティ


情報システム担当者　＋セキュリティ


営業担当者　＋セキュリティ


総務担当者　＋セキュリティ


経営者　＋セキュリティ

…

現場に必要なセキュリティ人材とは？

平時も含めた指揮官と実務担当者による規模に応じた体制

CISO

最高情報セキュリティ責任者

企業・組織内で情報セキュリティを統括する担当役員。
セキュリティポリシーの策定や情報運用の管理、情報漏洩などのインシデント発生時の対応施策決定など組織における情報セキュリティの全領域において管理責任を持つ。

CSIRT・実務担当

サイバーセキュリティ
インシデントレスポンスチーム

PoC（Point of Contact）・リーガルアドバイザー・ノーティフィケーション担当・リサーチャー・キュレーター・脆弱性診断士・セルフアセスメント担当・ソリューションアナリスト・コマンダー・インシデントマネージャー・インシデントハンドラー・インベスティゲーター・トリアージ担当・フォレンジック担当

組織の規模に応じて機能をアウトソースしつつ即応体制として組織。
まずは実務担当兼PoCの設置から。

現場に必要なセキュリティ人材とは？

セキュリティ人材不足に対して、できること。

高度セキュリティ人材の**発掘**

セキュリティ意識・能力の全体的**底上げ**

インシデント発生時の**訓練**(サイバー防犯訓練)

実戦競技による
高度セキュリティエンジニア
人才育成

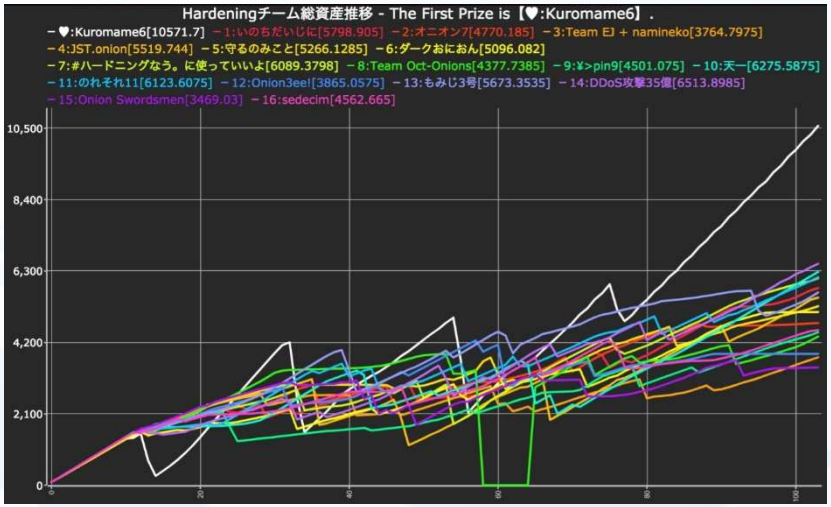
実戦競技による
高度セキュリティエンジニア
人才育成

実戦競技による人才育成

CTF(Capture The Flag)

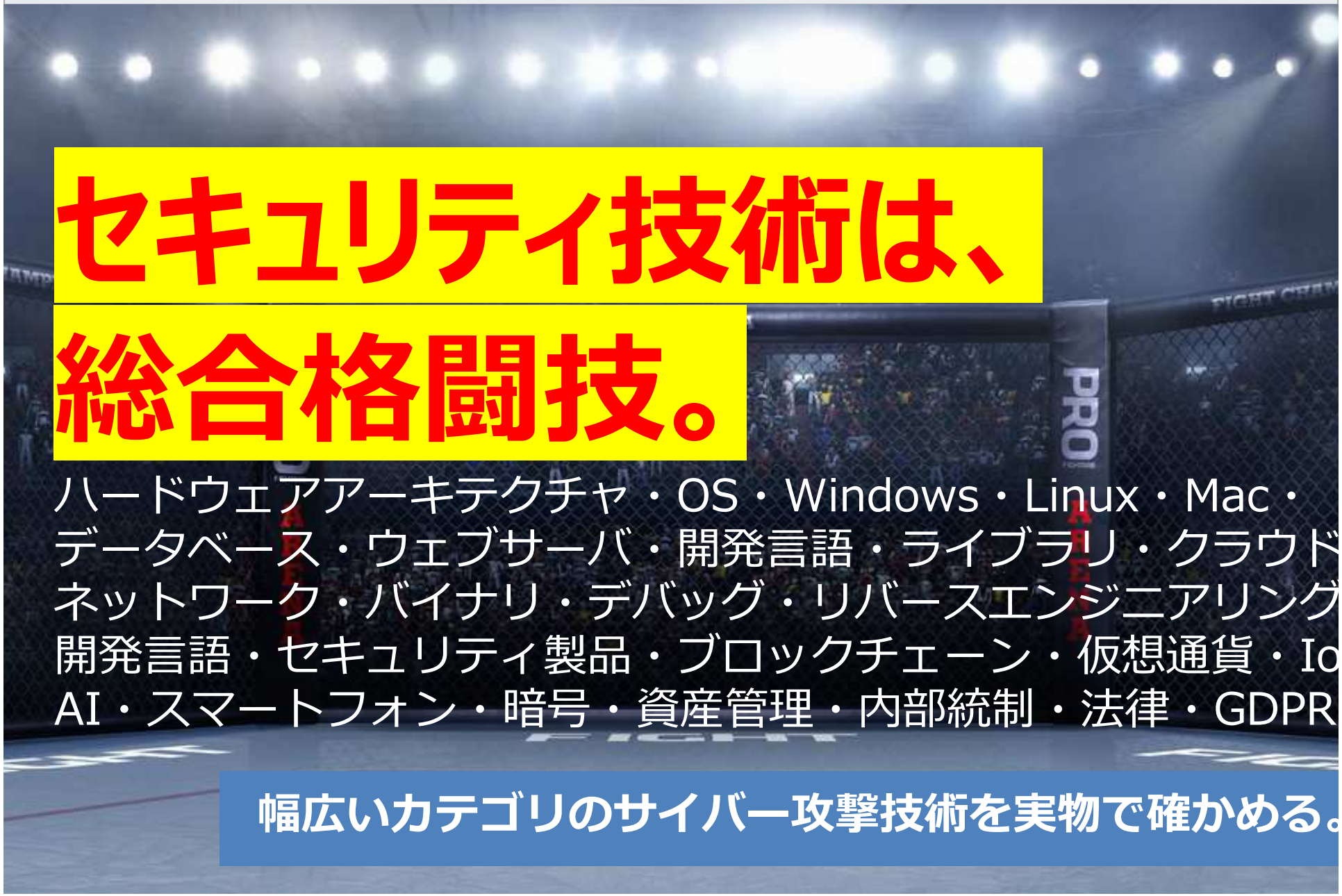
クイズ形式の競技による、
自主的な実戦技術の体験。
幅広いカテゴリのスキルを
体験的に学ぶことが可能。

Hardening



ECサイトを、サイバー攻撃から
防衛しながら売上を競うゲーム。
インシデントがリアルタイムに
発生し、サイバー攻撃の当事者
を疑似的に体験。

実戦競技による人才育成



CTF（Jeopardy形式）

練習	エンコード	フォレンジック	プログラム	ウェブ	ネットワーク	トリビア・その他	バイナリ
【練習問題】 10	【QRコード】 100	【docxのもう一つの顔】 100	【落ち着いて素数を数えよう】 50	【Webのやりとり】 50	【ホスト台数？】 10	【QRコードパズル】 100	【バッチファイル】 10
	【デコードせよ1】 100	【写真の場所を特定せよ】 100	【数独ラバーズ】 150	【フラグは公開情報！？】 100	【Basic認証を突破しよう】 100	【チカンせよ】 100	【デバッガ】 50
	【デコードせよ2】 100	【見えている範囲がすべてではない】 100	【熱血計算塾】 150	【開発会社が訴えられた】 100	【DNSは知っている】 100	【ビルの屋上】 100	【一時停止】 50
	【文字化け？】 100	【見た目が正しいとは限らない】 150		【おいしく焼けました】 150	【カテゴリに注目】 100	【連打チャンピオン】 100	【デバッガ2】 250
	【画像にせよ】 100	【フラグを話してくれるぞ】 200		【ファイルリーダー】 200	【ネットワーク通信を解析しよう】 100	【頭の体操、画像として…】 100	【デバッガ3】 300
		【ひとまずバイナ			【デジタル波形】		

幅広い出題ジャンル

実際の攻撃を伴う出題内容

実戦競技による人才育成（CTF）

- **実際の攻撃手法を自分で行うことで高い学習効果**

  実体験として広い範囲の技術や知識を学べる

  – 手を動かすことで、理解を深めることができる

  – 脆弱性や設定不備を狙い、フラグ(答え)を入手する問題が多い

  – 実際のWebサイトに対して実施すると、法に抵触する可能性が高い

  攻撃に類する行為は、
  許可された範囲でのみで行うよう注意が必要

  – 攻撃観点なので、守りの技術は他で学ぶ必要がある。

CTFの問題例（初級）

カテゴリ：フォレンジック

【写真の場所を特定せよ】

※ 本問題のフラグ形式は FLAG{} ではありません。
HINT: 19 26' 13.20" N 99 8' 27.60" E のような形式で、GPS情報から地図上の位置を検索できます。
HINT: 漢字8文字。Google Map 上の表記で建物の名称を入力ください

Flag

送信

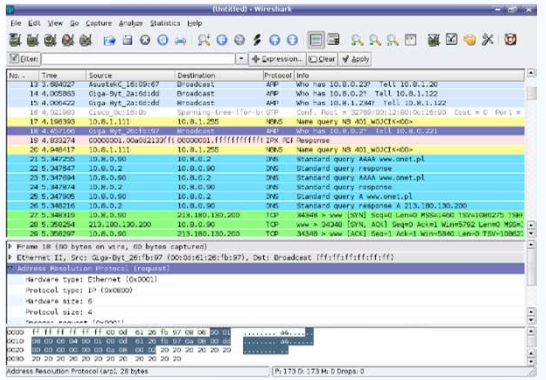
問題文を読んで答え（Flag）を探す
問題によっては脆弱なWebアプリを攻撃してFlagを入手するものもある

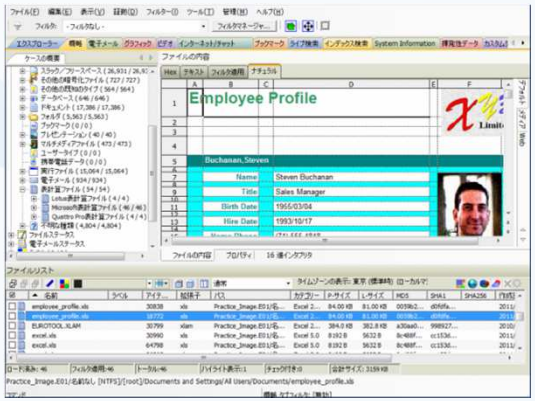
ここに答え（Flag）を入れる。
例題の画像にはGPS情報が含まれているので、そこから場所（Flag）を特定する

問題を解くためのツール例

- CTFで使うフリーツール
  - Wireshark, Network Minor
    パケットキャプチャ、パケットアナライザ
  - Cygwin
    Windows上で疑似Linux環境実現ツール
  - FTK Imager Lite
    簡易フォレンジックツール
  - OllyDbg
    プログラムのデバッグツール
  - Stirling
    バイナリエディタ

など





社内CTFイベントの開催

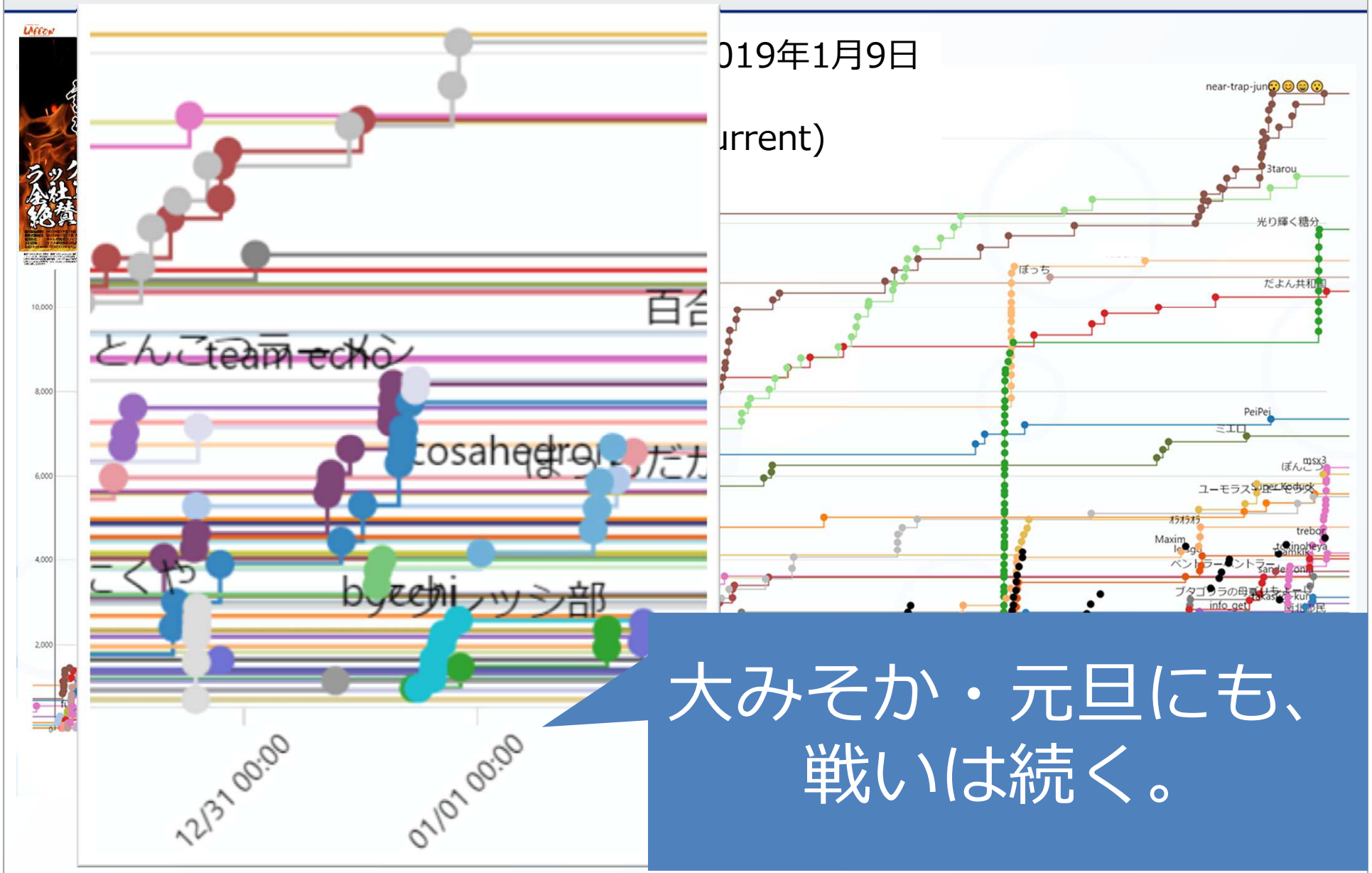
ラックグループ全社員が自由に参加可能

問題作成・大会運営はボランティアで実施

社内CTFイベントの開催

開催期間：2018年12月19日～2019年1月9日
参加：140名・76チーム
優勝：near-trap-junk(Japan Current)
準優勝：😮😊😄😮(Net Agent)

社内CTFイベントの開催



大みそか・元旦にも、
戦いは続く。

CTFイベントを通じた技術力強化

作問者は問題作成を通して、新たなテクニックの習得と理解が可能

技術部門だけでなく、管理部門や営業部門からも参加することで、セキュリティ意識を向上

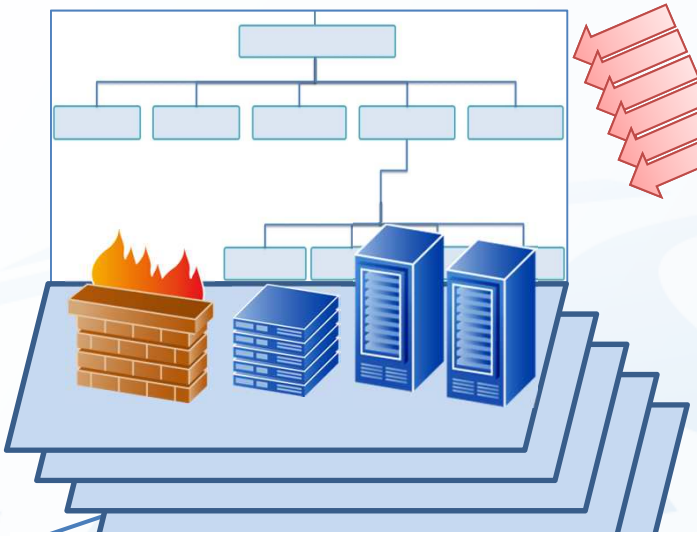
セキュリティ専門部署以外から、セキュリティスキルの高い社員を発掘できる

実戦競技による人才育成

Hardeningによる守りと対処の体験

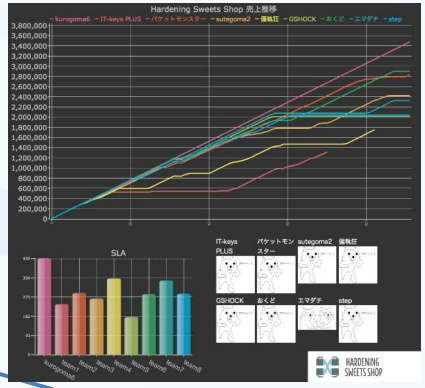
WAS Forum(Web Application Security forum)主催 Hardening Project

競技空間で提供される様々なサービスや製品を調達し、自チームに足りない能力を補完

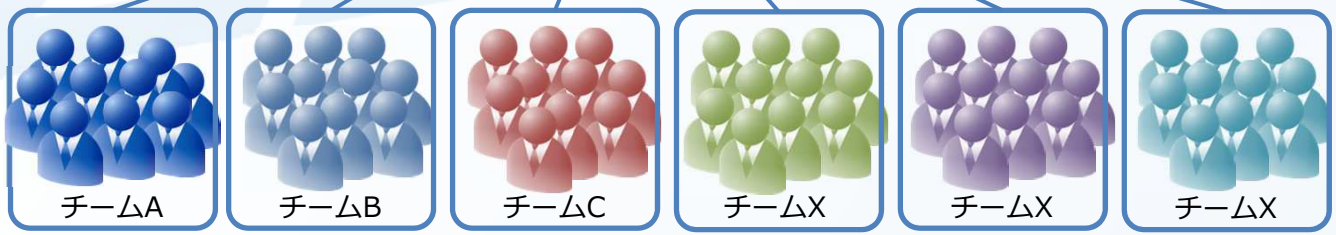


Hardening Project
シナリオ遂行・評価
kuromame6

Eコマースサイトの”売上”と”稼働状況”をリアルタイム・スコアボードに



参加者（6人～10人のチームで編成）



攻撃に対処しながら、売上を最大化。

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シナリオに沿って、リアルタイムに行われます

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。

Hardeningによる守りと対処の体験

攻撃分析	対処の実施	社内外対応	ビジネス視点

サイバー攻撃に対する組織的対応能力強化

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活動を体験的に理解することが可能。

ベンダーの活用など自組織の能力を見極め、外部の力を頼る判断も体験できる。

現場に必要なセキュリティ人材とは？

セキュリティ人材不足に対して、できること。

高度セキュリティ人材の**発掘**

セキュリティ意識・能力の全体的**底上げ**

インシデント発生時の**訓練**(サイバー防犯訓練)

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。

展示のお知らせ

- 展示ブースにてCTF体験を行っています。
- 是非お気軽にお声がけください。

サイバー・グリッド・ジャパン
サイバー・グリッド研究所
Cyber Grid Laboratory

Thank you. Any Questions ?