セキュリティ教育とイノベーション：SecHack365での取り組み

情報通信研究機構
ナショナルサイバートレーニングセンター
主任研究員 SecHack365担当
横山 輝明

自己紹介

- 自己紹介
  - 横山輝明、山口県出身、芦屋在住
  - 神戸情報大学院大学 情報技術研究科 特任准教授
  - 情報通信研究機構 主任研究員
  - サイバー関西プロジェクト, WIDE, AI3
- 経歴
  - 2007/3 奈良先端科学技術大学院大学 情報科学研究科 博士課程 卒業
  - 2007/4 サイバー大学 助教／講師
  - 2013/4 神戸情報大学院大学 情報技術研究科 講師／特任准教授
  - 2018/4 情報通信研究機構ナショナルサイバートレーニングセンター 主任研究員 SecHack365担当
- 専門
  - インターネット技術の教育（基盤から応用まで）
    - 途上国におけるIT基盤の整備
    - SDN, IoT, ネットワーク基盤, サービス基盤
  - ICT教育, 産学連携, 共同研究開発など

サイバーセキュリティ人材とは？

統合セキュリティ人材モデル

- 統合セキュリティ人材モデル
  - 実践的なスキルやノウハウを持つ技術者の育成
  - NEC・日立製作所・富士通の3社がとりまとめたセキュリティ技術者の共通人材モデル。サイバーセキュリティ人材育成スキーム策定共同プロジェクト」の成果物。2018年10月。
- 育成人材
  - 3社のセキュリティ対策の技術やシステム構築の実績、米国国立標準技術研究所（NIST） セキュリティ対策基準「NIST SP800-181」で定めるセキュリティ対策への対応
  - 14種類の人材像、必要なスキルセットを体系化

統合セキュリティ人材モデル

人材像	説明
【CT】セキュリティコンサルタント	セキュリティエンジニアリングの上流に位置し、経営課題や業務要件から、セキュリティに関するシステム仕様や運用仕様の方針を策定する。
【PL】セキュアシステムプランナー	求められるセキュリティ要件を満たすシステムやアプリケーションの上流設計を担当する。対象領域は、システムアーキテクチャー、ネットワーク、サーバ、アプリケーション、データベースなど。
【DV】セキュアシステムデベロッパー	セキュアシステムプランナーのアウトプットを引き継ぎ、セキュリティ要件を満たすシステム基盤の開発を担当する。対象領域は、システムアーキテクチャー、ネットワーク、サーバ、データベースなど。
【AD】セキュアアプリケーションデベロッパー	セキュアシステムプランナーのアウトプットを引き継ぎ、セキュリティ要件を満たすアプリケーションの開発を担当する。対象領域はアプリケーション、データベースアクセスなど。
【MG】セキュリティマネージャー	ISMSに代表されるセキュリティマネジメントシステムの整備および運用を担当する。
【AU】セキュリティオーディター	ISMSに代表されるセキュリティマネジメントシステムのマネジメント監査を担当する。
【SR】システムリスクアセッサー	対象のICTシステムが直面するセキュリティリスクを分析し、適切なセキュリティ対策選択の指針を示す。
【PT】ペネトレーションテスター	対象のICTシステムに対して攻撃者視点で攻撃を試み、ICTシステムの弱点（脆弱性や危険性等）を把握し報告する。
【NR】ネットワークリスクアセッサー	対象のICTシステムが直面するセキュリティリスクを分析し、適切なセキュリティ対策選択の指針を示す。
【RE】リサーチャー	セキュリティ技術に関する各種の研究を行う。
【FE】フォレンジックエンジニア	セキュリティインシデント発生時に、コンピュータ・フォレンジックプロセスに基づく詳細な調査を実施する。すでに侵害されたディスクイメージなどを採取し、また取得したイメージなどを解析し、攻撃者によっていつどのようなことが行われたのか解析を実施する。
【IA】インテリジェンスアナリスト	セキュリティに関する外部情報を収集・分析し、ICTシステムへの影響度を把握する。また、インシデント発生時にその背景などを分析し、インシデントの重大性に対する判断材料を提供する。
【IR】インシデントレスポンダー	セキュリティインシデントへの１次対処を行う。必要に応じて、インシデントハンドラーなどの他の人材像へのエスカレーション・引継ぎを行う。
【SP】セキュリティオペレーター	ICTシステムのセキュリティに関連する運用を担当する。

ICTシステムの関係者

- 開発者（システムの開発者）
  - システムを開発した単独・複数の開発者
  - 開発の内製／委託、完成物の購入の形態
- 利用者
  - システムの利用者
  - 複数の利用者・二次的な利用者が存在することも
- 運用者
  - システムの維持管理の担当者
  - 複数の運用者が存在することも
  - セキュリティ的な部分の維持管理も含む
- その他
  - 研究者はシステム要素や脅威を対象として研究
  - システムを取り巻く外部環境の調査や分析

ICTシステム導入

利用環境

ビジネス・目的

ワークフロー

利用者

外部環境

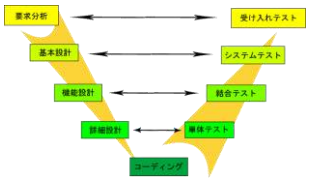
・法律
・社会常識
・技術変化

要求
仕様

開発者

機能要件

非機能要件



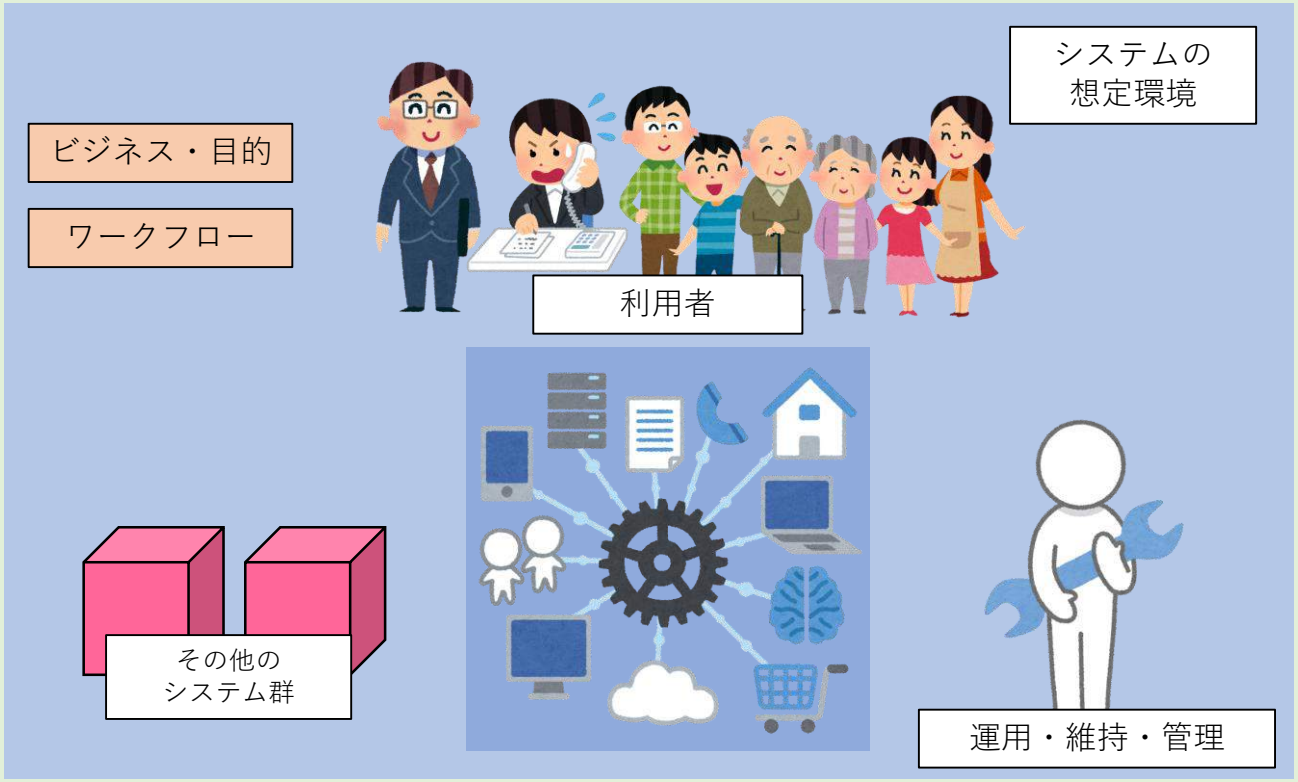
開発者

開発プロセス

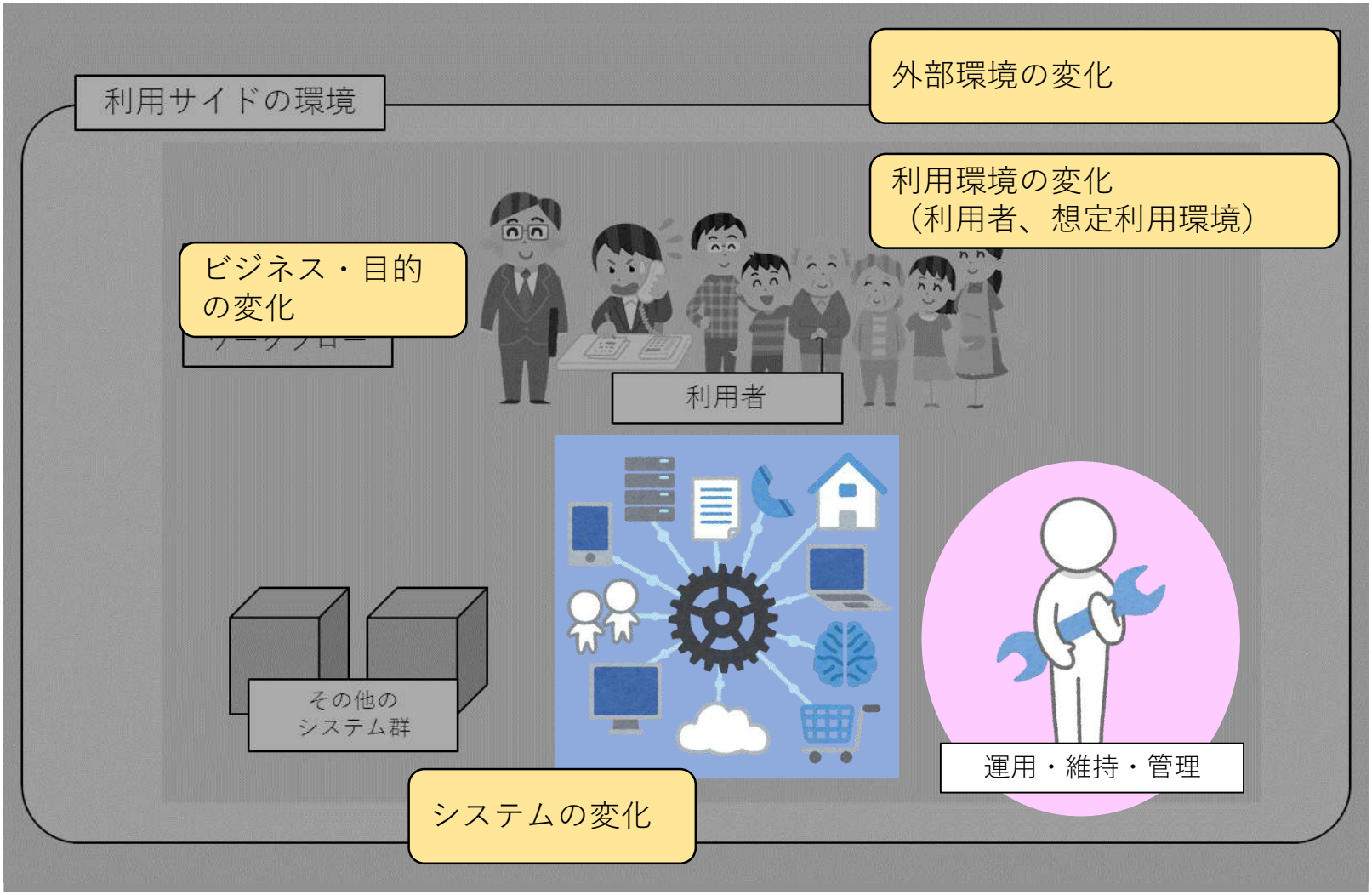
ICTシステム利用

外部環境

利用サイドの環境



ICTシステム運用


利用サイドの環境
外部環境の変化
利用環境の変化
（利用者、想定利用環境）
ビジネス・目的
の変化
利用者
その他の
システム群
運用・維持・管理
システムの変化

サイバーセキュリティ人材？

- システムについて
  - 機能要件・非機能要件（見えない、仕様漏れ）
  - 状況変化 （外部要因、脅威の発生）
  - リスク、コスト便益評価、コスト転嫁
- 対応できる人材
  - 技術とビジネスの理解
  - デザイン、解決の提案
  - リスクアセスメント（特定・分析・評価）
- 人材活用の困難
  - スキル ↔ ポジション？
  - インソース？アウトソース？
  - 費用対効果？
  - 誰をどこに？役割分担？網羅性？

SecHack365について

セキュリティイノベーター育成プログラム「SecHack365（セックハックサンロクゴ）」の概要

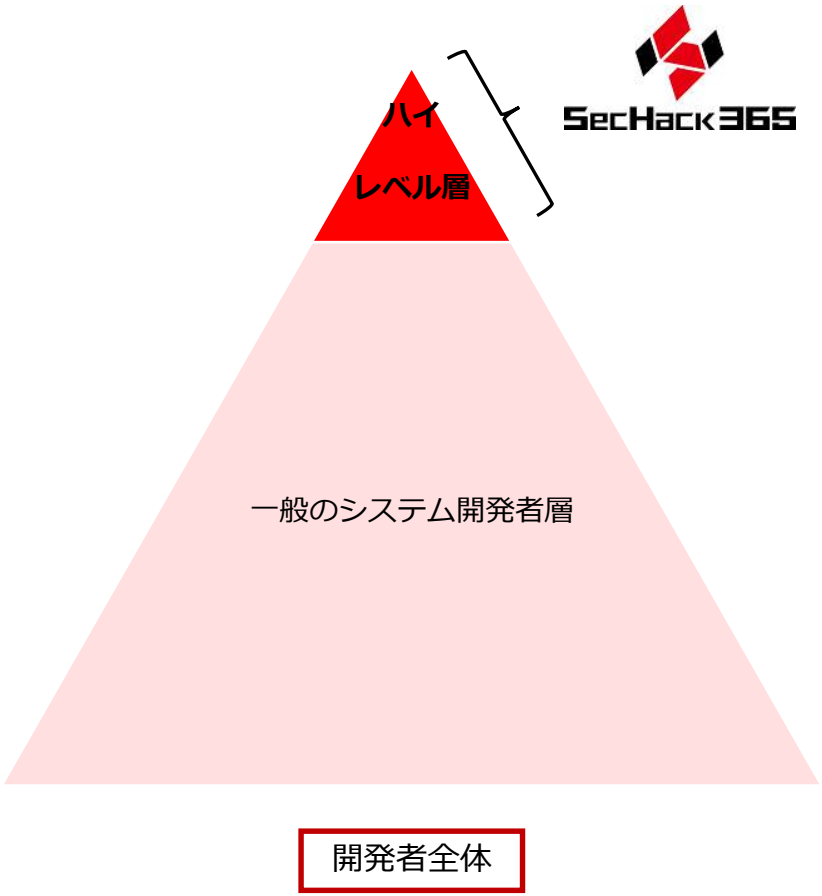
■ **未来のサイバーセキュリティ研究者・起業家の創出に向けて，NICTの持つサイバーセキュリティの研究資産を活用し，若年層のICT人材を対象に実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を1年をかけて本格的に指導する新規プログラム**

対象者

✓ **学生，若手社会人**を対象とした早期人材育成

H30年度 募集概要

募集期間　：　2018年4月2日 (月) ～ 2018 年4月20日 (金)
応募資格　：　日本国内に居住する25歳以下の若手ICT人材
応募数　　：　345名
受講決定数：　50名（内訳　成年37名/未成年13名・男性46名/女性4名　※2018.5.7受講者決定時点）



SecHack365

- SecHack365： https://sechack365.nict.go.jp/
  - U-25 若手セキュリティ系人材育成、公募
    - 25歳以下、50名程度を選抜
  - セキュリティ技術の研究開発、セキュリティ技術を用いたビジネス実現ができる人を育成
  - セキュリティイノベーターの育成

- プログラム内容
  - 1年間を通した人材育成プログラム
  - 年6回、2泊3日の集合イベント
  - 講師には研究者・実務家などを起用
    - アイデア発想、セキュリティ技術開発、セキュリティ研究 など

コースと全体評価

- 進め方の違いに基づく3コースを用意
  - コースマスターが主指導を担当
  - 他トレーナーも協力
- コース
  - 表現駆動コース：テーマや作品の表現を通じて推進
  - 思索駆動コース：テーマへの思索考察を通じて推進
  - 開発駆動コース：テーマや関連技術の実装を通じて推進
- 評価
  - アイデア：新規性や有用性などテーマの方向性
  - 技術　　：作品実装における技術力
  - 表現力　：テーマや作品を伝える能力

2018年度の審査

- 審査方針
  - 名前や所属などは考慮しないブラインド審査
  - 各コースでの選考
    - 各コースごとに課題を作成して審査
    - 各コースの進め方で作品づくりを達成できるか
    - 作って見せることについては全体として統一基準

- 応募の流れ
  - 募集開始日： 4月2日（月）
  - 課題フォーム提出期限： 4月20日（金） 17時
  - 4月27日審査、5月2日に連絡

2018年度の審査結果

- 応募数　345件 → 受講決定数　50件
  - コース別の内訳
    - 表現駆動コース 23名、思索駆動コース 11名、開発駆動コース 16名
  - 属性別の内訳
    - 成年37名／未成年13名、男性46名／女性4名
  - 所属別の内訳
    - 社会人　6人
    - 大学院　11人
    - 大学（学部）　20人
    - 高等専門学校　5人
    - 専門学校　1人
    - 高等学校　5人
    - 中学生　2人

2018年度 SecHack365 運営体制

NICTメンバ

トレーナー


園田 道夫


池田 克巳


衛藤 将史


笠間 貴弘


加藤 大貴


金濱 信裕


佐藤 公信


花田 智洋


安田 真悟


横山 輝明
(トレーナー長
／NICT主担当者)

SecHack365実行委員会

実行委員


小泉 カー
(実行委員長)
(IPU・環太平洋大学)


井上 博之
(広島市立大学)


猪俣 敦夫
(東京電機大学)


柏崎 礼生
(大阪大学)

推進委員


佳山 こうせつ
(富士通株式会社)


川合 秀実
(サイボウズ・ラボ株式会社)


坂井 弘亮
(富士通株式会社)


服部 祐一
(株式会社セキュアサイクル)


久保田 達也
(株式会社イッツ)


今 佑輔
(トレンドマイクロ株式会社)


仲山 昌宏
(株式会社WHERE)


神薗 雅紀
(PwCサイバーサービス合同会社)

事務局

NICT ナショナルサイバートレーニングセンター
塩山英里香、五十里治美、島田弘一 ほか (事業運営全般)
平田 真由美、鎌田 広子 (広報担当)、石川 大樹 (インフラ担当) ほか

運営支援事業者
株式会社　ナノオプトメディア

SecHack365の活動

- 開発テーマ
  - IoTモニタリング、自動車ハック、マルウェア解析
    攻撃トラフィックの可視化、ハニーポット などなど
  - セキュリティ技術／セキュリティ関連／サービス開発
  - 作る→見せる→評価される→ …（繰り返し）

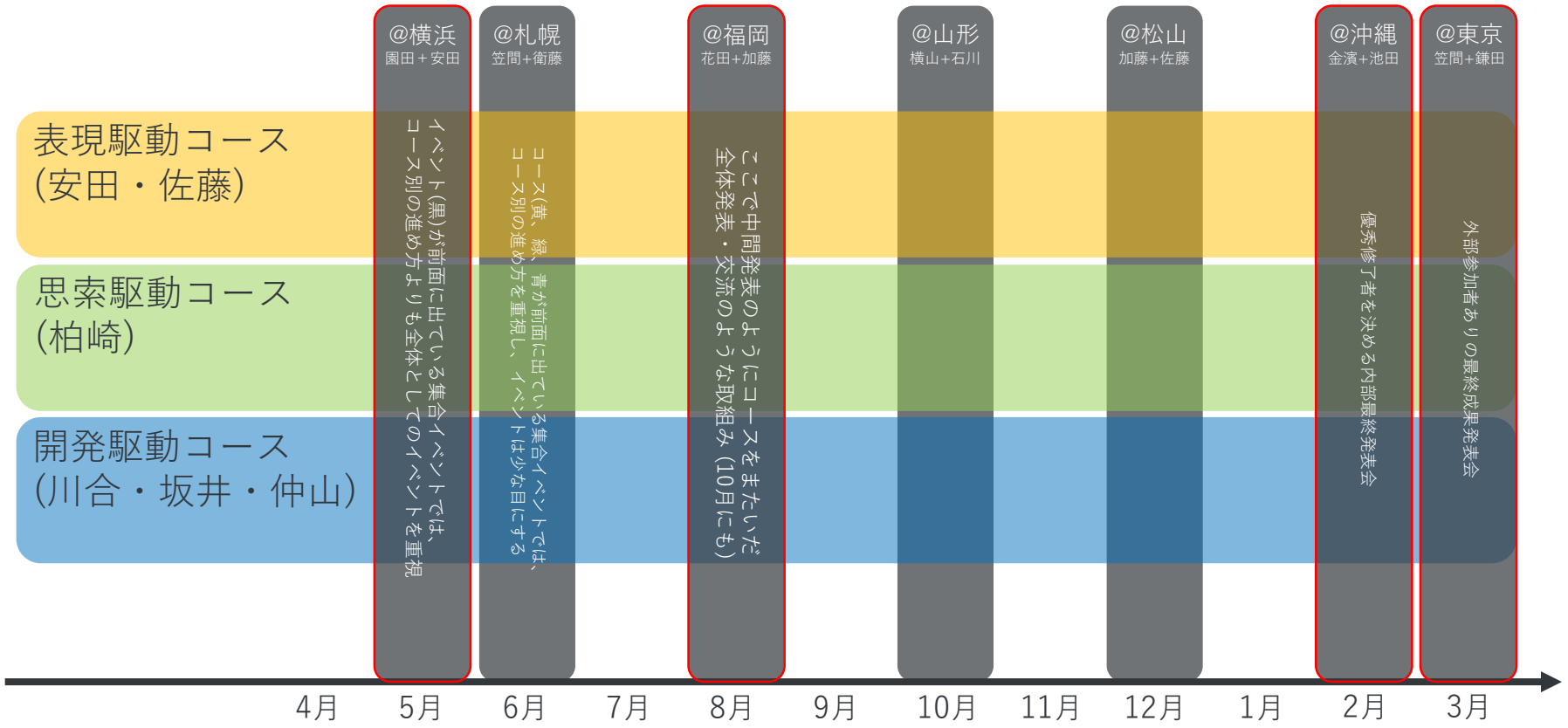





SecHack365 全体スケジュール 2018

National Institute of Information and Communications Technology

コース制の説明：コース制と集合イベント



テーマ例

- セキュリティ技術
  - 機械学習を用いたダークネットトラヒック解析
  - 囮ファイルによる攻撃検知システムの開発
  - シグネチャ共有に基づく分散フィルタ基盤
  - SNSにおける個人情報・プライバシーに配慮した画像共有
- セキュリティ啓発
  - セキュリティに対する意識向上～ARによるゲームアプリ～
  - Pythonで学ぶ情報セキュリティ入門本の執筆
  - ペンテスト学習プラットフォームの開発について
- サービス開発
  - Alt RequestBinの開発
  - 家事情報共有サービスUTIPSの進捗報告
  - 教育用（初心者向け）CanSatの開発環境をつくる

- 最終成果発表会
  - 優秀修了生の発表
  - 作品デモの展示
  - ポスターの展示

成果発表会(秋葉原)　2018/3/24

2017年度の成果

WEB: SecHack365 2017年度修了生作品
https://sechack365.nict.go.jp/2017artifact/

氏名	名称
上原瑛美	視て聴いて触るセキュリティ
小野諒人	ダークウェブ統合分析プラットフォーム
篠岡祐太	Mail Total - 分析・可視化で“わかる“スパムメール
高岡奈央，三須剛史	OS実装の自動化
安田昂樹	Secussion セキュリティについて議論するディスカッショントレーナー
青木克憲	シンボリック実行エンジンTritonのマルチアーキテクチャ対応
珊瑚彩主紀	サーバー管理をしてくれるLINE BOT彼女
千葉裕也	Raspberry Pi組込みOS
中村綾花	ネットワークカメラハニーポット
小林滉河，仲地駿人	深層学習を用いたフィッシングサイト検知システム
青池龍，市川友貴，小野輝也， 澤田拓弥，田中千尋，早坂彪流	IoTデバイス管理システム
大平修慈，草野清重，手柴瑞基，室田雅貴	車の情報×クラウドを使って安全・快適なカーライフをしたい！
酒井蓮耀	光を媒体とする電波を使わない無線通信の開発
湯川大雅	レーザポインタを使って便利に/安全に`モノ`を操作しよう
古謝秀人	機械学習を用いたマルウェア検知システム
江川達翔	Intel-PTを用いたバイナリのトレース
竹村太一，藤井翼	LOG VISUALIZATION　～攻撃の脅威度の分析と可視化～
石黒健太	仮想環境検知プログラムの解析環境の構築
榎本秀平	サンドボックス解析のための機能追加
三嶋秀宗	American Fuzzy Lopのheap canaryランダム化の実装
井上紘太朗，木下嵩裕	RasPiを用いたARM簡易プロトタイピング環境の構築
中島千咲	カラフルちゃん ～あなたの暮らしに彩りを～
澤佳祐，丸山泰史	分散Webプラットフォーム
二ノ方理仁	プログラミング言語開発
北村拓也，青木克憲，川島一記	Cyship：仮想空間でサイバー攻防を体験できるゲーム

Cyship

- SecHack365 2017年度受講生たちの作品
  - サイバー攻防をモチーフ
    - 攻撃・防御技術のイメージ
    - Unity利用のWebゲーム
  - 3名のグループによる作品
  - WEB: https://cyship.jp/

2017年度の成果

WEB: SecHack365 2017年度修了生作品
https://sechack365.nict.go.jp/2017artifact/

2017年度の成果

WEB: SecHack365 2017年度修了生作品
https://sechack365.nict.go.jp/2017artifact/

深層学習を用いたフィッシングサイト判定システム

小林 滉河　仲地 駿人

目的

本プロジェクトは，深層学習(LSTM)を用いることで従来の手法で対応が遅れていた未知のフィッシングサイト を検知し，手軽にフィッシングサイト判定を行えるGoogle extensionを開発し，フィッシングサイトの被害者を無くすことを目指した．

フィッシングサイトとは?

フィッシング(Phishing)とは，金融機関(銀行やクレジットカード会社)などを装った電子メールを送り，住所，氏名，銀行口座番号，クレジットカード番号などの個人情報を詐取する行為です．電子メールのリンクから偽サイト(フィッシングサイト)に誘導し，そこで，個人情報を入力させる手口が一般的に使われる．

従来手法

- ブラックリスト形式
  マルウェア配布先やフィッシングサイト といった悪質なサイトをデータベースに登録し，そこに含まれるサイトはアクセスできないようにする．
- ホワイトリスト形式
  安全と言えるサイトだけを集めたデータベースを作成し，そこに含まれるサイトのみアクセスを許可する．

従来手法の問題点

- ブラックリスト形式
  誰かがブラックリストに登録するまで，そのサイトは安全なサイトとして扱われる．
- ホワイトリスト形式
  限られたサイトにしか入ることができないため，色々なサイトを見たいユーザには有効的ではない．

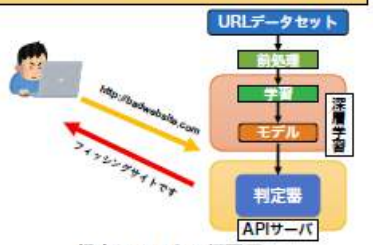
提案手法

- 深層学習(LSTM)を用いたURLベースの検知
  データベース更新が不要になり，次々と作成されるフィッシングサイトに対して対応することを目指す．

フィッシングサイトはどれだ！？

https://conselmypaypIresol.ddns.net/

https://www.paypal.com/signin?country.x=US&locale.x=en_US



提案システムの概要図

データセット

- フィッシングサイト
  フィッシングサイト 報告サイトから収集．
- 一般的なサイト
  Alexa ranking Top 50と日本の上場企業URLにスクレイピングを行い，URLを収集．

前処理

[h, t, t, p, :, /, /, e, x, a, m, p, l, e, ., c, o, m]
↓ ASCIIコード番号 に変換
[112, 58, 47, 47, 101, 120, 97, 109, 112, 108, 101, 46, 99, 111, 109]
↓ URLの長さを150に固定 前に-1を代入
[-1, -1, -1, -1, -1, -1, ・・・, 97, 109, 112, 108, 101, 46, 99, 111, 109]

結果

テスト用データ

クラス	データ数	不正解数	正解数	正解率
Phishing	7,857件	139	7,718	98.2%
Normal	88,173件	673	87,500	99.2%

まとめ

- 深層学習を用いることで，未知のフィッシングサイトに対する対策が可能になった．
- 実験だけではなく，Google extensionという形で提供することができた．

今後の課題

- ブラックリスト形式やホワイトリスト形式とのハイブリット化
- 世界のwebサイトへの対応

ダークウェブ統合分析プラットフォーム

ダークウェブとは

仮想通貨取引所から盗難された通貨の交換所

違法ドラッグマーケット ヘロインやMDMAが誰でも買える

匿名性が高く実態が分かりにくい

統合分析プラットフォーム

ダークウェブの実態を解明する

違法なマーケットのトレンドを追える　　サイトの情報が収集できる

システム概要

アドレス収集システム

スキャナ

可視化システム

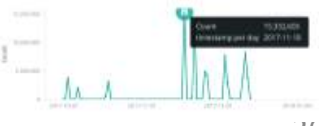
elasticsearch　kibana

実際のデータ

スキャンによるセキュリティ評価

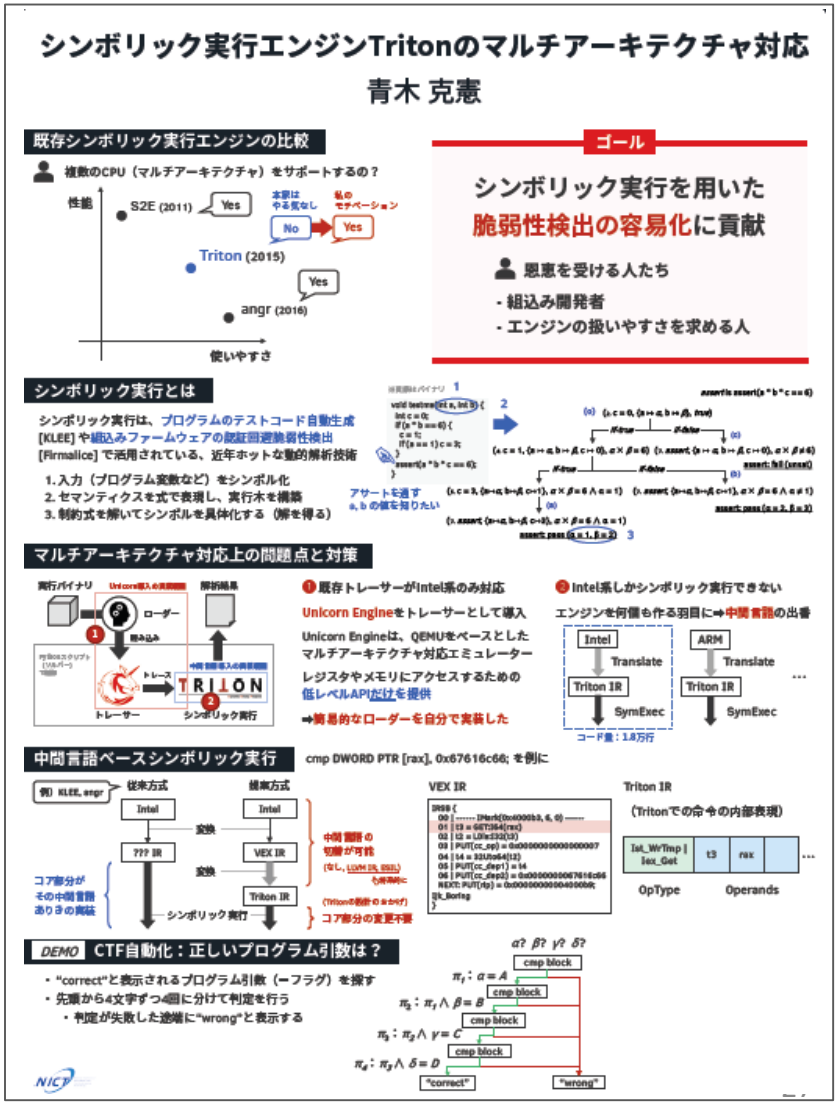
ダークウェブ版アクセスランキング

ダークウェブへのDDoS攻撃の観測



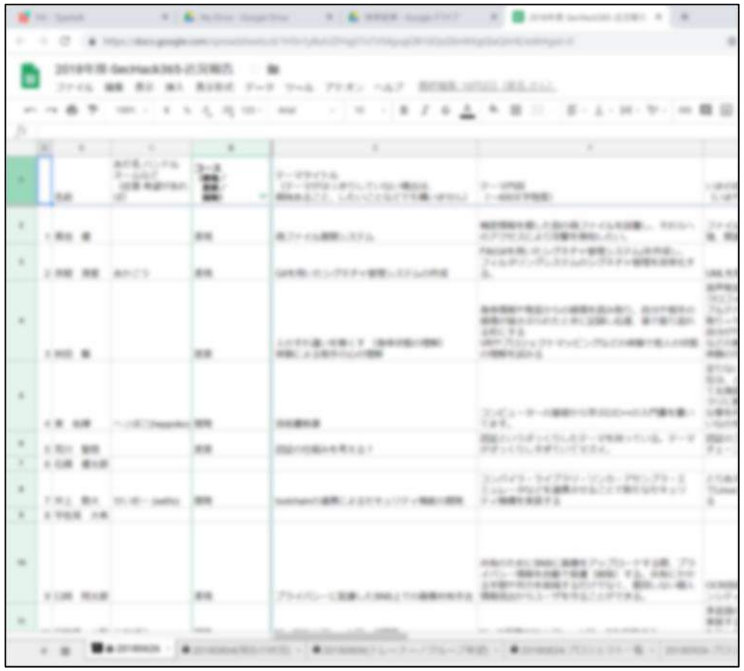
2017年度の成果

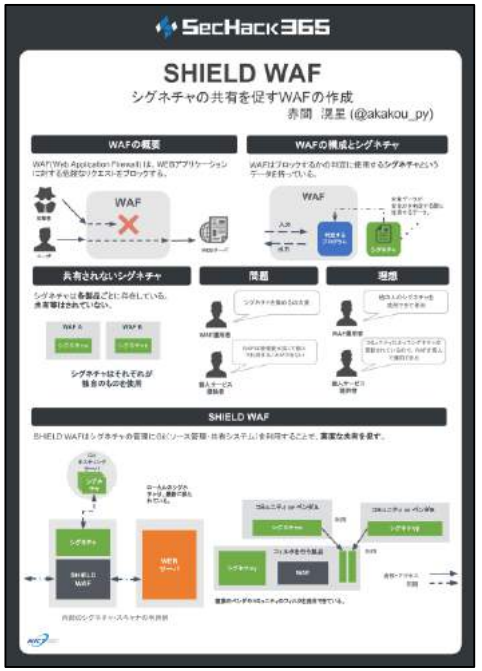
WEB: SecHack365 2017年度修了生作品
https://sechack365.nict.go.jp/2017artifact/



オンラインでの活動

- チャット等を通じてオンラインでの開発
  - 各コースやトレーナーからの指導
  - 日常のなかでの継続的な開発活動
  - 全体進行の管理、テーマや状態の共有





SecHack365での活動

- インプット
  - 各トレーナーからの知見、考え方、発想法など
    - 長期の開発を続けるための「習慣化」
    - 自分たちが作り上げるものに責任をもつ「倫理」 など
  - 企業等での事例見学、ディスカッション
  - アウトプットに対するフィードバック
- アウトプット
  - 持ち込む作りたい作品テーマ
  - 作品を説明する発表、プレゼンテーション、ポスター
  - デモンストレーション
- 進め方
  - イベント回にて発表
  - イベント回の間の期間は自主的に活動、オンラインでサポート

全体の進行

- 5月 神奈川回の実施 (2018年5月18日～20日)
  - 顔合わせとキックオフ
  - オリエンテーション（目標の確認、進め方）
  - 自己紹介、テーマ
- 6月 北海道回の実施 (2018年6月29日～7月1日)
  - 長期ハッカソンへの参加の習慣化の促進
  - 最初のスプリント、オンラインコミュニケーション／開発
  - さくらインターネット見学
- 8月 福岡回の実施 (2018年8月22日～24日)
  - 発表練習、テーマや作品の説明
  - テーマの共有、ディスカッション、指導
  - 見せる練習、フィードバック
  - Nulab見学

全体の進行

- 10月 山形回の実施 (2018年10月12日～14日)
  - ポスターとして作品を明示的に説明
  - 可能なトレーニーにはデモも求める
  - 作品に対しての意見などフィードバックの開始
- 12月 愛媛回の実施 (2018年11月30日～12月2日)
  - 最終発表に向けての練習、デモやポスターの展示
  - 2月に向けて、相談と意見をもらう大きな機会
- 2月 沖縄回の実施 (2019年2月1日～3日)
  - 最終発表、デモやポスターとして完成品の展示
  - 優秀修了者の選抜
- 3月 最終成果報告会 (2019年3月8日)
  - 優秀修了者による発表、修了者によるポスターやデモを予定
  - 秋葉原UDXで実施、一般公開なのでぜひご参加ください

「作ること」の変化

- 作ることがスタート
  - 昔は作ることがゴール
  - 今はただ動かすだけなら簡単

- 作ってからが大変
  - 何が売れるかわからない
  - マーケットニーズへの適合や変化
  - 機能要件の変更
  - 作ったあとから見つかる欠陥
    - ＝ セキュティ対応

作る・見せる

- 作る
  - プロトタイプ、仮説検証、作りすぎない
    - 作る目的の自覚、デモの工程管理、手抜きする
    - 非機能要件の絞り込み
    - 本当に必要な作業をしているのか？
  - 拡張性・使い捨てを考慮した設計
- 見せる （アイデア検証）
  - 見せ方、ストーリー、クエスチョンの明確化
  - 心理的安全、面の皮の厚さ
    - 途中でも見せる、正直に見せる
    - 締め切りよりも早くてよい
  - 意見の受け取り方、取捨選択
  - 見せるのが目的、コードは手段→捨てる勇気

→ セキュリティ／イノベーションへのプロセス
ICTの社会実装と維持を実現できる人材育成

今後の連携の可能性について

- キャリアパス
  - 研究、開発、応用への発展
  - 就職など、スキルや経験の活用の場
- 既存の教育カリキュラムとの親和
  - 学業との両立・連携
  - 学業側からの利用
- 今後ともよろしくお願いいたします