



国立研究開発法人

情報通信研究機構

National Institute of Information
and Communications Technology

ナショナルサイバートレーニングセンターにおける
若手セキュリティイノベーター育成の取組みについて
～SecHack365～

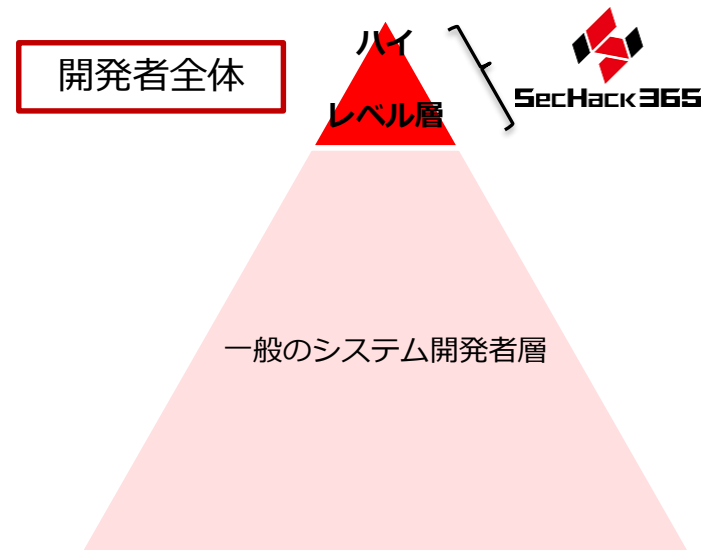
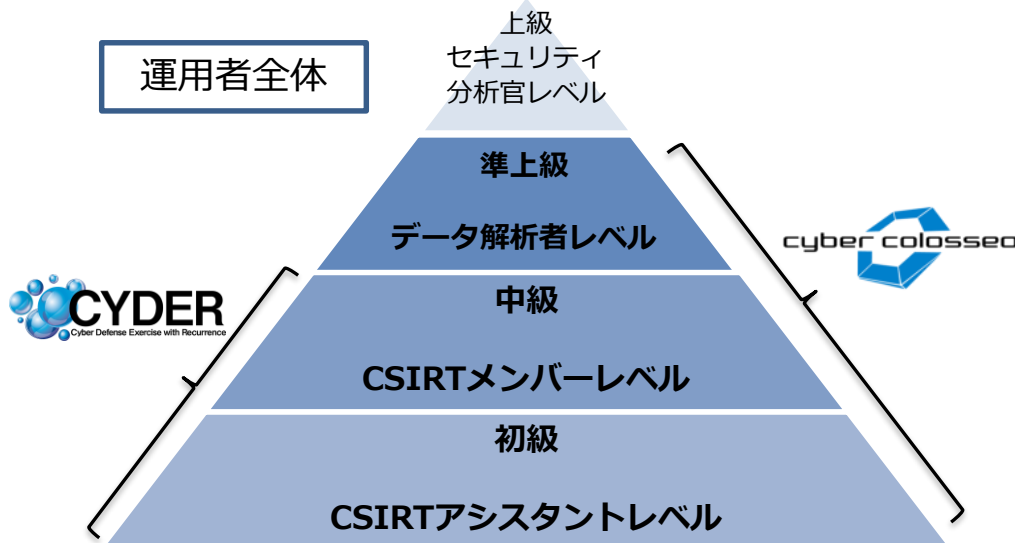
○ 情報通信分野を専門とする我が国唯一の公的研究機関であるNICTの技術的知見、研究成果、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進する組織として、「ナショナルサイバートレーニングセンター」を設置（2017.4.1）

セキュリティオペレーター（実践的運用者）の育成

- ✓ 行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象
- ✓ 所属組織が深刻なサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成

セキュリティイノベーター（革新的研究・開発者）の育成

- ✓ セキュリティマインドを持ち、既存ツールを単に「ユーザー」として利用するだけではなく、革新的なセキュリティソフトウェア等を自ら「研究・開発」していくことができるハイレベルな人材を育成



現状

我が国のセキュリティ・ベンダーの存在感は、世界規模で見ると決して大きいものではなく、ブラックボックス化した海外製品を利用することが多いのが現状



私たちが、自らの手で自らの社会の安全を守っていくためには、既存のセキュリティソフトウェア等を単に「ユーザー」として利用するだけではなく、新たに自ら「研究・開発」していくことができる人材の育成が必要

課題

革新的なセキュリティソフト等を研究・開発する実践的なトレーニングを行うためには、

- ✓ マルウェア検体やその痕跡データなど関連データと、それらを安全に利用して研究・開発を行うことができる「研究・開発環境」が必要
- ✓ 実績・経験がある一線級の「研究者・技術者」から、「技術指導・助言」を得る必要

マルウェア検体等を安全に利用して研究・開発を行う「研究・開発環境」を構築する必要性



ノンストップ
NICTが有する遠隔開発環境「NONSTOP」の活用

実績・経験がある一線級の「研究者・技術者」から、「技術指導・助言」を得る必要性



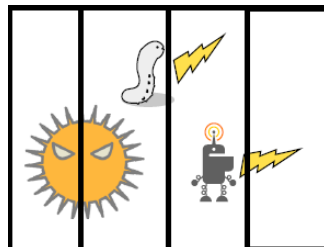
NICTの研究開発に関する知見・人的資源の活用

NICTによるセキュリティイノベーターの育成

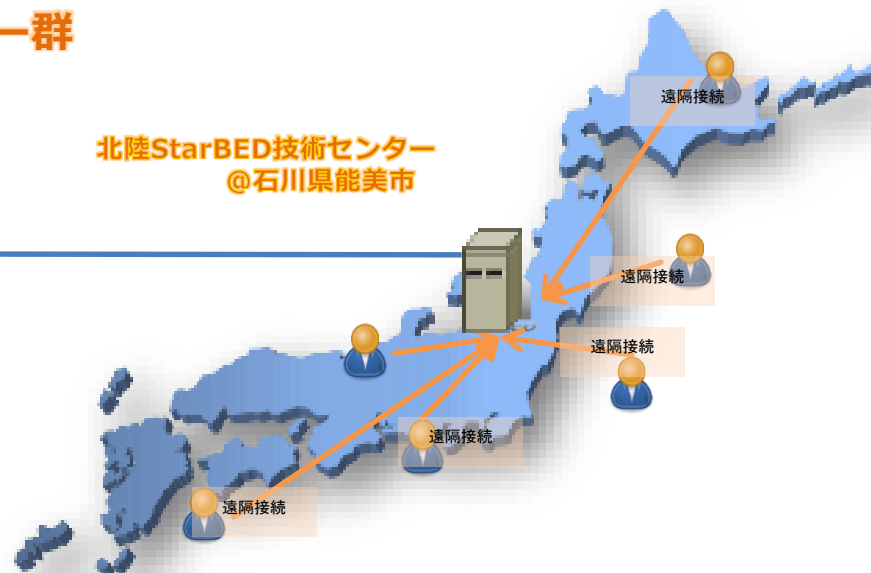
～①遠隔開発環境「NONSTOP」～

- ・ NICTは、サイバーセキュリティ研究用に、クラウド型で遠隔からも安全にマルウェア研究等を行うことができる遠隔開発環境「NONSTOP」を開発し、NICT自身の研究に利用
- ・ NONSTOPには、NICTが長年続けてきた大規模なサイバー攻撃観測網により収集した現実の攻撃データ等が数十万規模でデータベース化され、研究用に活用できる形式で蓄積
- ・ トレーニング受講生に対しても、この「NONSTOP」へのアクセス権を特別に付与することで、いつでもどこからでも安全な環境下で、豊富なマルウェア検体等を使用しつつ研究・開発の実践的トレーニングを行うことが可能

StarBED 大規模高性能サーバー群



北陸StarBED技術センター
@石川県能美市

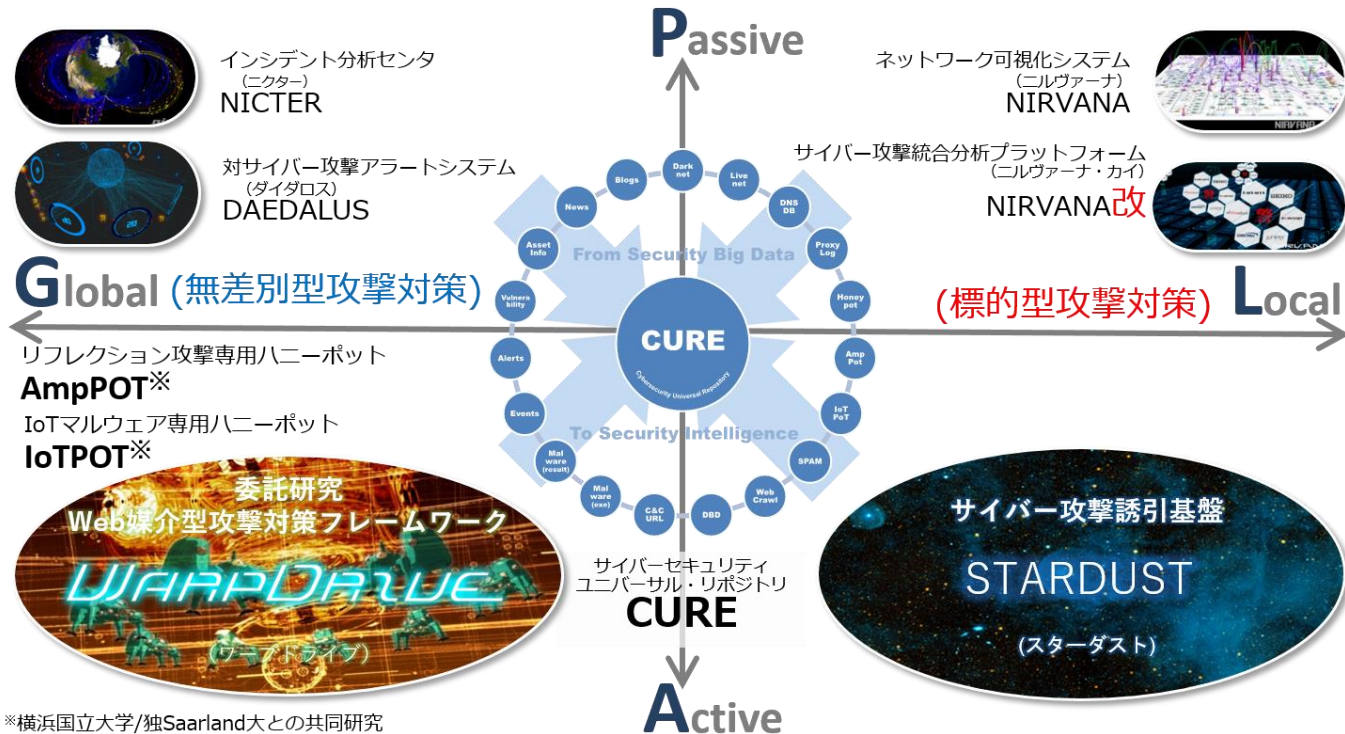


NICTによるセキュリティイノベーターの育成

～②研究・開発に関する知見・人的資源～

・ NICTの研究者・技術者は、長年のサイバーセキュリティ研究を通じて、NICTER, NIRVANA, DAEDALUS, STARDUSTといった、最先端の研究・開発の「モノづくり」を行い、そのノウハウを蓄積

・ これらNICTの研究者・技術者を核として、NICTの研究分野における人的ネットワークを活用し、外部の有志の研究者・技術者の協力をも得ることにより、一線級の研究者・技術者陣による本格的な技術指導・助言を行うことができる。



セキュリティイノベーター育成プログラム「SecHack365」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。

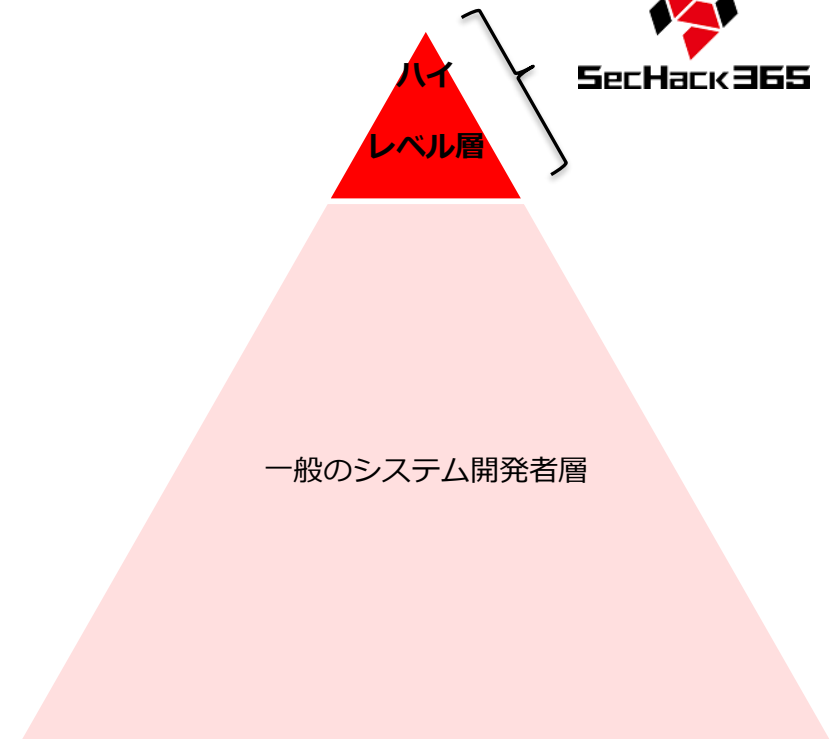


対象者

- ✓ 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
- 募集人数 : 40名程度



開発者全体

プログラム概要

NICTの強みを活かした育成事業

- ✓ アイディアソン, ハッカソン, 遠隔研究・開発, 演習の組み合わせによる**総合的能力開発**
- ✓ NICTの研究者・技術者を核とした, 一線級の研究者・技術者陣による, **1年を通じた**本格的な技術指導・助言
- ✓ NICTが有する研究資産(攻撃データ等)の活用

! 継続的な研究開発環境の提供

- ✓ 受講者はハッカソンの実施日以外の期間も, 北陸 StarBED 技術センター(石川県)に整備された遠隔開発環境("NONSTOP")に自宅等から接続し, 研究・開発を継続
- ✓ 北陸 StarBED 技術センターに NICT が収集したサイバー攻撃の実データを集約し研究・開発に活用

! 反復的なイベントによる技術の深掘り

- ✓ 受講者で構成されたチームごとにサイバーセキュリティ関連システムの議論と研究・開発を行う(計6回+成果発表会1回)
- ✓ セキュリティ倫理教育, 研究者による最新のセキュリティ技術の講義も実施
- ✓ 実施回ごとに開催地を変えるなど, 趣向を凝らしたイベントで柔軟な発想, 議論を誘起

| 月 | SecHack365 年間プログラム [2018] | | | 遠隔開発 実習環境 NONSTOP |
|------------|---------------------------|--|--|----------------------------|
| 4月 Apr | 2 | 応募期間 20 課題フォーム配布期間 17 応募締切 2018年4月20日(金) | 選考期間 | いつでもどこでもライブスタイルにあわせて遠隔開発実習 |
| 5月 May | 2 | 5月2日(水)までに 可否ご連絡 | 第1回 神奈川 18~20 5月18日(金)~5月20日(日) 横浜市 | |
| 6月 Jun | | 6月29日(金)~7月1日(日) 札幌市 | 第2回 北海道 29~ | |
| 7月 Jul | 1 | | | |
| 8月 Aug | | 8月22日(水)~24日(金) 福岡市 | 第3回 福岡 22~24 | |
| 9月 Sep | | | | |
| 10月 Oct | | 10月12日(金)~14日(日) 山形市 | 第4回 山形 12~14 | |
| 11月 Nov | | 11月30日(金)~12月2日(日) 松山市 | 第5回 愛媛 30~ | |
| 12月 Dec | 2 | | | |
| 1月 Jan | | | | |
| 2月 Feb | 1~3 | 2019年2月1日(金)~3日(日) 南城市 | 第6回 沖縄 | |
| 3月 Mar | 8 | 東京 成果発表会 3月8日(金) 東京会場 | | |

ハッカソンのテーマ例 (H29 年度実績)

- AI(深層学習)による不正 Web サイト検知
- 広範なマシン環境で動作可能なプログラム解析エンジン
- 仮想空間でサイバー攻撃を体験できるゲーム
- 自動車データのクラウド解析によるドライバーアシスト
- レーザーポインタによる家電の「指揮」
- 不正 Web サイトの統合分析プラットフォーム

期待される成果等

研究者・起業家の育成

- ✓ 優秀な受講者に対し，受講者の志望に合わせた継続的なサポートを提供
 - ・ 海外のハッカソンイベントや大学の短期講座に国費で派遣
 - ・ 国内研究会等における研究発表を支援
 - ・ NICT自身がインターンとして受け入れ，研究を指導
 - ・ 起業を支援
 - ・ 企業関係者との交流の機会を設定 等

研究・開発へのフィードバック

- ✓ 有望なアイデア・研究成果があれば **NICTの研究開発に応用**

SecHack365コミュニティの形成

- ✓ SecHack365修了生が新たな受講生の相談相手となり関係を継続
 - ⇒ 各年度の修了生が楽しく集まる，持続的で厚みのあるコミュニティの形成
 - ⇒ 1年間の受講期間で終わるのではなく，長期的な能力開発を継続
 - ⇒ 将来的なトレーナー候補としても期待



2017年度 募集状況

募集期間 : 2017年4月3日(月) ~ 2017年4月28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 : 358名
 受講決定数 : 47名
 (内訳 成年30名/未成年17名・男性43名/
 女性4名 ※2017.5.9受講者決定時点)

SecHack365年間プログラム

| 月 | SecHack365 年間プログラム【2017】 | | | 遠隔開発環境 |
|------------|--------------------------------|---------------------------------|----------------------------|-------------------------------|
| 4月 Apr | 3 | 課題ファイル配布期間 | 25 | NONSTOP |
| | 3 | 応募期間 | 28 | |
| 5月 May | 選考期間 合否ご連絡 (5月12日までにご連絡) 12 | | 【合格者】東京 NICT見学会 19/20 | いつでもどこでもライフスタイルにあわせて遠隔研究・開発実習 |
| | | 5月19日(金) 5月20日(土) 東京都小金井市 | | |
| 6月 Jun | 第1回 東京 | 10/11 | 6月10日(土)~11日(日) 東京都大田区 | |
| 7月 Jul | | | | |
| 8月 Aug | | 8月23日(水)~25日(金) | 福岡県福岡市 | |
| 9月 Sep | | | | |
| 10月 Oct | 第3回 北海道 | 14/15 | 10月14日(土)~15日(日) 北海道札幌市 | |
| 11月 Nov | | | | |
| 12月 Dec | | 12月23日(土)~24日(日) | 大阪府大阪市 | |
| 1月 Jan | | | | |
| 2月 Feb | | 2月24日(土)~25日(日) | 沖縄県 | |
| 3月 Mar | | 3月24日(土) | 東京都 | |

第1回東京(蒲田)回 6/10-6/11

富士通株式会社の全面的な協力を得て ^{フジツウ}FUJITSU ^{ナレッジ}Knowledge ^{インテグレーション}Integration ^{ベース}Base ^{プライ}PLY
にて開催

- ・オリエンテーション
- ・グループディスカッション
- ・トレーナーによる講義等
- ・アイデアソン
- ・発表
- ・倫理教育



第2回福岡回 8/23-8/25

- ライン
- ・LINE株式会社特別講義
 - ・緑日(トレーナーによるハンズオン演習)
 - ・ハッカソン
 - ・倫理教育



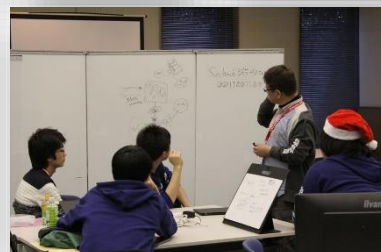
第3回北海道(札幌)回 10/14-15

- ・ハッカソン
- ・緑日(トレーナーによるハンズオン演習)
- ・株式会社さくらインターネット石狩データセンター見学
- ・特別講義: 北海道大学 町村教授(情報セキュリティと法)



第4回大阪回 12/23-12/24

- ・ハッカソン
- ・特別講義①：大阪大学 柏崎講師（研究ってなんだ（開発とのつながり））
- ・特別講義②：パナソニック株式会社
- ・発表, 展示
- ・トレーニーとトレーナーの相談タイム



第5回沖縄回 2/24-2/25

- ・大自慢会（成果発表）
- ・特別講義：学校法人KBC学園 国際電子ビジネス専門学校 淵上副校長（現 NEC サイバーセキュリティ戦略本部ご所属）
「これからの時代をどう生きるのか ～ セキュリティイノベーターというキャリア ～」



成果発表会(秋葉原) 3/24

成果発表会における全発表タイトルと発表者

| | |
|-----------------------------------|--|
| 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組み込み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 | レーザー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 |
| 井上紘太郎, 木下高裕 | 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 |



成果発表会(秋葉原) 3/24

成果発表会における優秀グループの発表タイトルと発表者

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

現在フィッシングサイトへの対策方法として、ブラックリスト方式、ホワイトリスト方式など様々なフィッシング検知方式が提案されている。本プロジェクトでは、リスト更新が不要になる新たな検知方法として、深層学習を用いたURLベースの検知方法を提唱し、実装、実験を行った。また多くのパソコン利用者が利用出来るようChrome拡張として公開している。

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

ターゲットはプログラミングや情報科学の知識は無いが、セキュリティを学びたい中高生。CTFに代表されるように、プログラミング知識なしにセキュリティを学ぶのは難しい。仮想空間でサイバー攻防を体験できるゲームプラットフォームCyshipを提案する。ゲームを進行するAIの作成をビジュアルプログラミング言語により可能で、やりこみ要素とプログラミング要素を備える。

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!

現在、自動運転車の普及が急速に高まっています。将来的にはゴーストカーと呼ばれる自動運転車が街を徘徊し、ゴーストカーが皆さんを行きたい場所へ連れていってくれる時代が予想されています。そういった時代には、現在の自動運転車の模範となる運転情報が明確でないという課題や、サイバー攻撃に対する安全性という課題が問題となります。そこで、私たちは自動車とクラウドを連携させた次世代型自動車サービスのプロトタイプを開発して、実際のデータを使った運転情報の定量的評価、ドライバーへのサイバー攻撃の通知・可視化を実現するシステムを開発しました。

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でき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減らすことを目指した。

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段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蓄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
悪質な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
信頼されたサイトしか入ることができないため、色んなサイトを見たいユーザー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!?

| クラス | データ数 | 不正数 | 正数 | 正精度 |
|----------|---------|-----|--------|-------|
| Phishing | 7,857件 | 130 | 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ド化
・世界のWebサイトの対応

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

CYSHIP

GA M E

サイバー攻防の仕組みを理解し、自分だけの最強のAIを作成せよ!

サイバー攻防をゲームで体験学習
ホワイトハッカーを目指せ

対人戦で負けるとあなたの秘密が漏洩する
情報漏洩を避け!

最強のAIをプログラミングで作成せよ

オフラインのカードゲーム作成
オンライン版作成
中学生や高校生に使ってもらいたい改善
SECCONデモ展示

2017.5 2017.10 2017.11~2018.1 2018.3

北村拓也, 青木克憲, 川島一記 連絡先:tkitamura@mitou.org

安全×快適なカーライフをしたい! ~自動運転の社会を目指して~

自動車のデータを取得 クラウド(AWS)で収集・分析

- セキュアに運転データをクラウドへ
- 運転データ...速度, 回転数, 位置情報, など
- 可視化・運転評価を提供

GPSアンテナ SORACOM Sim 自動車への接続点

データ Lambda (プログラム) 分析 保存 可視化 運転評価 異常通知 ユーザー

クラウドを使ってデータを収集! データを活用!

安全 快適 安心

実際の運転データを利用!

Unityでの可視化 運転評価

- 車載ネットワークの直感的なイメージ
- 自動車への攻撃や異常の警告
- 速度, 回転数などを基に運転評価
- 未来の自動運転の指標に!

現在の車の情報を表示 優秀なドライバーのデータを収集

データの種類の色分け

92 69 79 72

安全・快適な自動運転社会を!

NICT 自動車セキュリティチーム: 大平修慈, 草野清重, 手柴瑞基, 室田雅貴

成果発表会(秋葉原) 3/24

成果発表会における優秀グループの発表タイトルと発表者

湯川大雅

レーザーポインタを使って便利に/安全に`モノ`を操作しよう

近年、IoT技術の需要が高まるとともに、音声認識やスマートフォン/タブレットを利用して家電や情報を操作することが一般に広まりつつある。しかし、音声やスマートフォンを用いる操作方法は、使用する場面や人によって不都合な点がいくつかある。そこで、そのような不都合な場面で家電や情報を操作する方法として、レーザーポインタを用いる方法を提案する。また、付随するセキュリティ問題について考察し、解決策を提案する。

小野諒人

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、近年急速に拡大している犯罪色の強いネットワークのことで、主にTor秘匿サービスのことを指します。また、このネットワークは匿名性が高く、捜査機関の方も困っていると聞いています。そこで、このTor秘匿サービスの観測や捜査の困難さを解決するために、分析システムを開発しました。このシステムにより、ダークウェブのトレンドの観測と、セキュリティ強度の評価が可能になります。

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

シンボリック実行エンジンが複数台頭する中で、扱いやすさと成果の観点において近年はangrが有力である。一方、シンボリック実行エンジンTritonは扱いやすく、拡張性が高いが、Intel以外のアーキテクチャに対応していなかった。本研究の目的は、Tritonをマルチアーキテクチャ対応することで、angrのライバルを立てることである。中間言語Vex IRベースのシンボリック実行に対応したところ、Vex IRに変換したIntelの機械語片のシンボリック実行に成功し、マルチアーキテクチャ対応の実現性が示された。

レーザーポインタを用いた家電操作

湯川 大雅

作品イメージ

家電と情報を光で操る指揮者になろう

背景

IoT技術が一般に広がるにつれて、タブレットや、スマートスピーカーなどを用いて家電を操作する機会が増えている。しかし、それらの方法では、使用者や環境によって、不都合な点がある。

- 直感性の欠如
- 声を発する必要がある
- 言語で表現しにくい命令

目標

レーザーポインタを用いた直感的かつ安全で汎用性の高い、家電等操作の仕組みを作成する。

結果・考察

- レーザーポインタで家電の操作できた。
- 第三者からの不正操作のリスクを軽減できた。
- レーザー光による事故のリスクを軽減できた。
- 使用方法をより簡単にする必要がある。
- 安全対策をより強固なものにする必要がある。

成果物

1. 家電操作の仕組み
 - ①レーザーで家電
 - ②カメラで家電の動作を確認
 - ③家電へ命令
2. 操作方法
 - ①目標に電気を送る
 - ②目標を確認
 - ③ジェスチャー
3. セキュリティと安全対策
 - ①自分のレーザーを認識する
 - ②認識しないレーザーをOFF
4. 専用レーザーポインタ
 - レーザーの出力状態を確認
 - 危険であるときは自動的に出力を停止
5. 開発用ライブラリ(Python)

開発者がプログラムを動かさなくても、レーザーポインタの動作を確認し上げられるよう工夫した。

ダークウェブ統合分析プラットフォーム

匿名性が高く実態が分かりにくい

ダークウェブとは

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

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

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

スクリー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

ダークウェブのDDoS攻撃の観測

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

青木 克憲

既存シンボリック実行エンジンの比較

性能: SZE (2011), Triton (2015), angr (2016)

扱いやすさ: Yes/No

シンボリック実行を用いた脆弱性検出の容易化に貢献

- 悪意を受ける人たち
- 組み込み開発者
- エンジンの扱いやすさを求める人

シンボリック実行とは

シンボリック実行は、プログラムのASTから自動生成されたASTから、プログラムの実行をシミュレーションする。

1. 入力 (プログラムのAST) をシミュレーション
2. セマンティクスで表現し、実行をシミュレーション
3. 制約式を用いてシンボリックを具体化する (解を得る)

マルチアーキテクチャ対応上の問題点と対策

- 既存のアーキテクチャがIntelのみ対応
- Intel以外のアーキテクチャで実行できない
- Unicorn Engineをレシーバーとして導入
- Unicorn Engineは、OS/ハードウェアと連携したマルチアーキテクチャ対応のレシーバー
- Unicorn Engineをレシーバーとして導入
- Unicorn Engineは、OS/ハードウェアと連携したマルチアーキテクチャ対応のレシーバー

中間言語ベースシンボリック実行

中間言語: VEX IR, Triton IR

中間言語ベースシンボリック実行

中間言語ベースシンボリック実行

中間言語ベースシンボリック実行

中間言語ベースシンボリック実行

海外派遣SXSW 3/10~3/17

- 訪問地** : アメリカ合衆国 オースティン
参加者 : 木下嵩裕, 酒井蓮耀, 澤田 拓弥, 早坂彪流, トレーナー3名, コーディネーター1名
海外派遣の目的 : 世界最大級のクリエイティブイベントに参加。海外トップクラスのイノベーター, クリエーターとの意見交換等を実施。今後のキャリア, セキュリティイノベーターに資するマインドセット・スキル習得を目指す。

SXSW (South by Southwest)

スポンサーであるAmazonのAlexa, Clouduary, Capitol Music Groupなどが提供する機能を用いてアイデアを24時間で実装するハッカソン。もともと音楽とテクノロジーの融合を目指して始まったイベントで, 近年はエンタテインメントとテクノロジーの融合がテーマになっている。



2017年度海外派遣SXSW Hackathon スポンサー賞を受賞

| | |
|-------|---|
| タイトル | emShare |
| コンセプト | 人間は言葉になる前の感情, 言葉にできない感情を秘めている。emShare はそういう感情を人間がアップロードした動画から読み取り, それに相応しい音楽を選んで動画に差し込むシステム。選んだ音楽が流れる動画を共有することで感情を共有する。 |
| 受賞者 | 木下嵩裕, 酒井蓮耀, 澤田拓弥, 早坂彪流 |

2017年度 修了者数

受講決定者 : 47名 (内訳 成年30名/未成年17名・男性43名/女性4名)
 修了者 : 39名 (8名は主に学業との兼ね合い等の理由により途中辞退)

実行委員 (4名)



小泉 カ一氏(委員長)

環太平洋大学 次世代教育学部 教育経営学科 教授
次世代情報センター センター長



井上 博之氏

広島市立大学大学院 情報科学研究科 准教授



猪俣 敦夫氏

東京電機大学 未来科学部 情報メディア学科 教授



柏崎 礼生氏

国立大学法人大阪大学 情報推進本部
兼 サイバーメディアセンター 講師

推進委員 (8名)



委員：神園 雅紀
PwCサイバーサービス合同会社
サイバーセキュリティ研究所 所長



委員：今 佑輔
トレンドマイクロ株式会社
プロジェクト推進本部 サイバーセキュリティ産学連携担当



委員：佳山 こうせつ
富士通株式会社 サイバーセキュリティ事業戦略本部
サイバーディフェンスセンター マネージャー



委員：坂井 弘亮
富士通株式会社 ネットワークサービス事業本部



委員：川合 秀実
サイボウズ・ラボ株式会社



委員：仲山 昌宏
株式会社WHERE IoT基板センター
サービスプロデューサー



委員：久保田 達也
株式会社イツ 代表取締役



委員：服部 祐一
株式会社セキュアサイクル 代表取締役