

Internet Week 2025

セキュリティの仕事、どんなことをしているの？どうしたらなれるの？

ペネトレーションテスターのお仕事

2025年11月20日

NEC サイバーセキュリティ技術統括部

リスクハンティンググループ

中島春香



中島 春香 (Haruka NAKASHIMA)

所属

日本電気株式会社
サイバーセキュリティ技術統括部
リスクハンティンググループ アナリスト

業務内容

脆弱性診断/ペネトレーションテストを通じたセキュア開発支援
セキュリティ人材育成

社外活動

CTF for GIRLS 代表
SECCON実行委員会 メンバ
経済産業省商務情報政策局サイバーセキュリティ課
情報セキュリティ対策専門官

今日話すこと

セキュリティの仕事、どんなことをしているの？どうしたらなれるの？

脆弱性診断/ペネトレーションテスト
セキュリティ人材育成



ペネトレーションテストや脆弱性診断って
どんな仕事なの？というお話

学生時代からやってきたこと



私はこうして今ペネトレーションテストのお仕事
をしていますよ、というお話

NECでセキュリティの仕事、どんなことをしているの？

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

基本情報

事業内容

IT サービス

- システム・インテグレーション
(システム構築、コンサルティング)
- サポート (保守)
- アウトソーシング・クラウドサービス
- システム機器
- ソフトウェア・サービス

主要顧客

- 官公庁、自治体・医療、インフラDX(消防防災、交通、メディア)、企業(金融、製造、流通・サービス)、他

社会 インフラ

- テレコムサービス
ネットワークインフラ (コアネットワーク、携帯電話基地局、光伝送システム、海洋システム)、通信事業者向けソフトウェア・サービス (OSS*1 / BSS*2)
*1 OSS: Operation Support System, *2 BSS: Business Support System
- 航空宇宙防衛
システム機器、システム・インテグレーション (システム構築、コンサルティング)、およびサポート (保守)

主要顧客

- テレコムサービス：通信キャリア (国内、海外)
- 航空宇宙防衛：中央省庁、宇宙事業者

Security By Design

安全・安心なデジタル社会への架け橋となる

Technical Consultancy

コンサルティング

- Security By Design提案
- セキュリティ要件定義/設計支援
- セキュリティ認証取得支援

Risk Assessment

リスクアセスメント

- 脆弱性診断/ペネトレーションテスト
- リスクハンティング
- セキュリティ監査

System Integration

システム インテグレーション

- 高度セキュリティSI
- セキュリティソリューション設計/構築

Solutions

ソリューション開発・ サポート

- セキュリティ製品/サービス開発
- セキュリティオフリング/保守

Managed Service

マネージドサービス

- セキュリティ運用/監視サービス
- MDR*サービス
- セキュリティリスクマネジメント

Incident and Response

インシデントレスポンス

- インシデント発生時 初動対応支援
- フォレンジック調査/分析/アドバイザリ
- CSIRT構築/運用支援

SOC Platform

SOC基盤開発・運用

- 24時間365日 自社SOC基盤運用

Training

教育・人材育成

- セキュリティウェアネス
- セキュリティ演習

* MDR: Managed Detective and Response

中島の業務領域

Security By Design

安全・安心なデジタル社会への架け橋となる

Technical Consultancy

コンサルティング

- Security By Design提案
- セキュリティ要件定義/設計支援
- セキュリティ認証取得支援

Risk Assessment

リスクアセスメント

- 脆弱性診断/ペネトレーションテスト
- リスクハンティング
- セキュリティ監査

System Integration

システム インテグレーション

- 高度セキュリティSI
- セキュリティソリューション設計/構築

Solutions

ソリューション開発・ サポート

- セキュリティ製品/サービス開発
- セキュリティオフリング/保守

Managed Service

マネージドサービス

- セキュリティ運用/監視サービス
- MDR*サービス
- セキュリティリスクマネジメント

Incident and Response

インシデントレスポンス

- インシデント発生時 初動対応支援
- フォレンジック調査/分析/アドバイザリ
- CSIRT構築/運用支援

SOC Platform

SOC基盤開発・運用

- 24時間365日 自社SOC基盤運用

Training

教育・人材育成

- セキュリティアウェアネス
- セキュリティ演習

* MDR: Managed Detective and Response

脆弱性診断・ペネトレーションテスト（リスクハンティングサービス）

セキュリティのスペシャリストがおお客様のシステムのリスクを評価、対策を提示
ビジネス継続に関わるリスクを包括的に評価し対策を提示することでリスク低減を支援



セキュリティ
スペシャリストチーム

専門資格*を保有

国内外コンテストで表彰



お客様のご要望に応じて、様々なテスト/診断サービスをご提供
目的に応じてスペシャリストによる手動検査/ツールでの自動検査を実施

システム全体から見たセキュリティリスクを包括的に評価し対策を提示

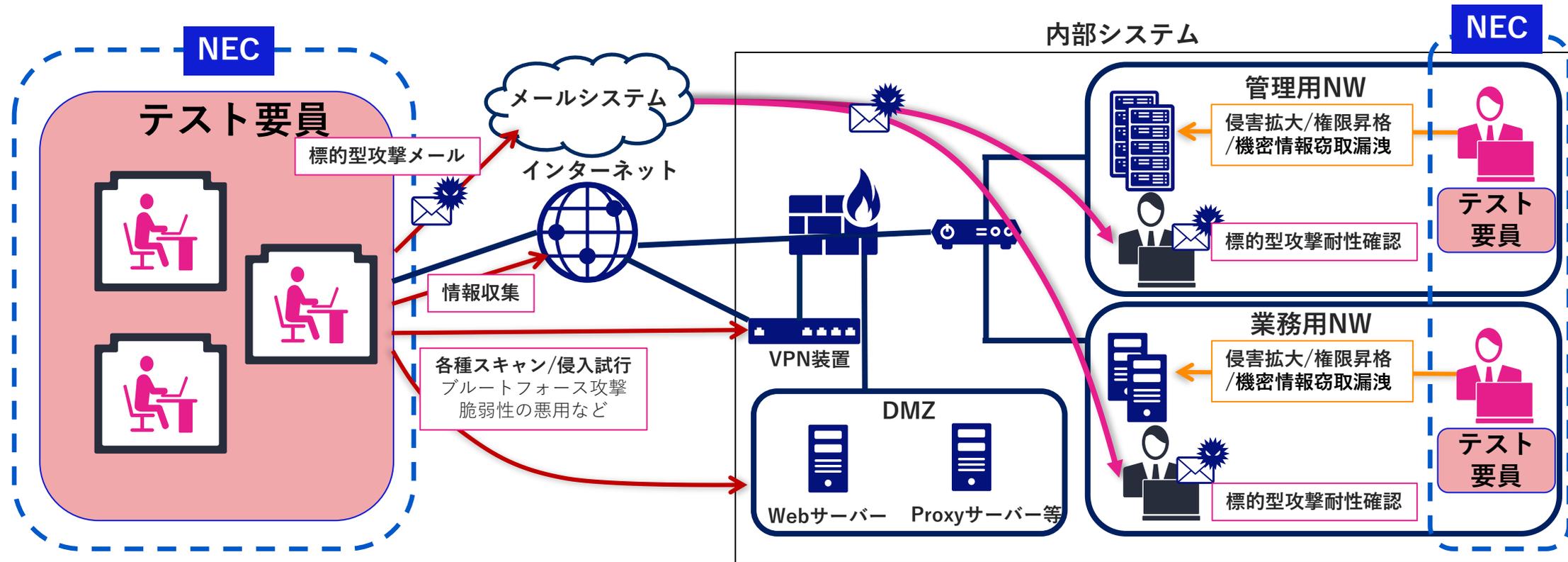
*CISSP, GIAC, 情報処理安全確保支援士等

ペネトレーションテストのイメージ

システム構成やお客様のご要望に応じたテストシナリオを設定し、
攻撃目標の達成可否を評価

- 外部テスト  : インターネット経由で外部公開サーバー等への侵入を目的としたテスト
- 内部テスト  : システム内部へ侵入済の攻撃者（または内部不正）による影響評価を目的としたテスト

※本スライドのテストシナリオは一例。



セキュリティ人材育成（CTF）

NEC-Gにおけるセキュリティウェアネス向上を目的としたプロジェクト
2021年から企画・運営リードとして参画し、社内外に向けてCTFを実施

“社内CTF”は”CTF”とは別物

スキル習得や技術力可視化の目的に沿った難易度設定と解説付きで実施

一般的なCTF

難易度の高い問題を競う

技術力の高さを競う目的であり
スキル習得の効率性は目的外

社内で開催するCTF

セキュリティの
スキル習得に繋げる

効率的にスキル習得する配慮を実施

- 誰もが解けない問題にならない難易度を設定
- 業務への関わりがわかるよう問題ごとに詳細解説を付与

© NEC Corporation 2022 ワークショップ実施要領 | Orchestrating a brighter world NEC

NECセキュリティスキルチャレンジ(CTF)の特徴

- ◆ NECグループ内のエンジニアが幅広いカテゴリから問題を作成
- ◆ 業務で使えるテクニックを問題に反映
- ◆ 問題の出題意図、学びを詳細に説明

問題カテゴリ(2022年度)



© NEC Corporation 2022 ワークショップ実施要領 | Orchestrating a brighter world NEC

NEC-GでのCTFに関する取り組み

セキュリティの初心者から上級者までの全ての層をカバーする。約800名が自主的に参加した社内CTF（第8回）実施の裏側

#プロジェクトの裏側 #セキュリティ #社内CTF

2023年2月9日 15時00分

日本電気株式会社

#プロジェクトの裏側 #セキュリティ #社内CTF

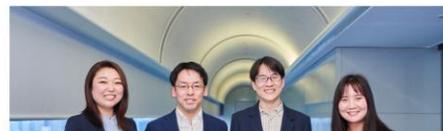
サイバー攻撃によるシステム破壊や個人情報の流出、度々流れてくるこのようなニュースを目にするたび、胸を痛めるセキュリティ技術者も少なくないのではないだろうか。

最近では、テレワーク等の場所や時間に捉われない働き方を狙った攻撃も増えており、技術者だけではなく、全社員がセキュリティを身近に感じて意識を高めることが、より一層重要になっている。しかし、全社員へ効率的にセキュリティウェアネス(注1)の向上を図っている企業は多いわけではない。

(注1)人がITシステムを利用する際にセキュリティリスクを理解し問題発生時の正しい対処が意識できること

そのような中、日本電気株式会社（以下、NEC）は、2015年からグループ全社員を対象に Capture the Flag（以下、CTF）を実施している。CTFとは、セキュリティ技術を競うオンラインコンテスト。ゲーム感覚で効果的に技術や知識の習得が可能だ。同社で実施されているCTFは「NECセキュリティスキルチャレンジ(以下、NSSC)」と呼ばれ、セキュリティ関連の仕事をする社員から普段馴染みがない部署の社員まで、幅広い職種の人々が参加している。2022年11月には8回を実施する等、文化としても根付きつつある。

社員が自主的に参加する形式をとっている社内向けのCTF（以下、社内CTF）は、どのように運営されているのか。NSSCの運営メンバーである、NEC サイバーセキュリティ戦略統括部の橋 龍太郎、中島 春香、水田 辰也、中川 紗菜美の4名に話を聞いた。



C2C CTF 2023 サイドチャレンジ提供

世界から大学生78名が日本へ集結！セキュリティ技術を競う国際イベントに、NECが大会“初”となる問題提供を行った理由。社内CTFで培った基盤活用の裏側。

#イベントの裏側 #セキュリティ #産学連携

2023年9月28日 11時00分

日本電気株式会社

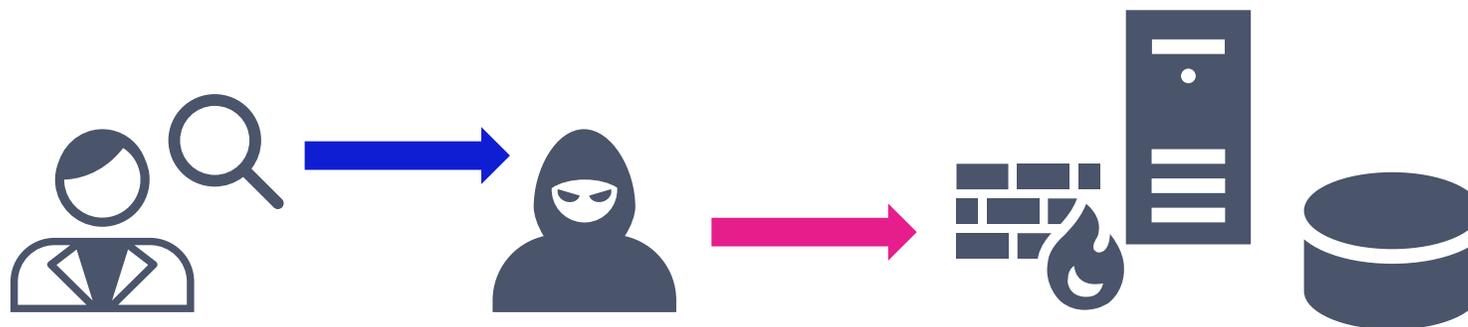
世界トップ大学が加盟するサイバーセキュリティ分野の産学連携組織「InterNational Cyber Security Center of Excellence (INCS-CoE)」が主催する国際イベント「Country to Country CTF 2023（以下、C2C CTF 2023）」が、8月1日から4日間にわたり開催された。CTF（Capture The Flag）とは、実際に手を動かしながらセキュリティ技術を駆使してフラグと呼ばれる答えを探し出し得点を競い合うもの。2020年から毎年、加盟大学が持ち回りオンラインで開催してきたが、2023年度は、慶應義塾大学がホスト校を務め、初めてオフラインでの開催となった。9カ国、33大学から総勢78名の大学生が参加し、日本に集結した。



セキュリティ人材育成（社内ハンズオン環境の構築・運用）

セキュリティ診断で得た知見を反映し、脆弱性の発生原理や影響、対策について効率的に学ぶことができるハンズオン形式の演習環境を社内に展開

- 対策を怠った場合の**社会的影響が大きく知名度の高い脆弱性**を再現
- 脆弱性の発生原理や影響、対策について手を動かして学ぶことで、**セキュアなシステム開発・運用を推進**することを目的に展開
- **影響や対策を含めて丁寧に解説**



学生時代からやってきたこと

学生の時何してた？

サイバーセキュリティを仕事にするまでの道のり

ハッカーって かっこいい

日本の高校生が
ハッキングスキルを
武器にテロリストと
戦う漫画、BLOODY
MONDAYに出会う



画像出典：
https://m.media-amazon.com/images/I/7116y4SW8nL_SL1200_.jpg

2009

大学入学 ふらふら期

1年目はまずいろいろ
触れてみようと思い、
心理学やプログラミ
ング、いろいろな
講義へ。

2014

コミュニティ 活動に参加

勉強会に参加したり、
CTF for GIRLS運営に
入ったり。
セキュリティ業界の
仕事や働くイメージ
がみえてきた

2015

NECに入社

ペネトレーション
テストに興味があり、
志望。日本のインフ
ラを支えている大き
な会社で働きたいと
思い、入社。

2019

プログラミング 面白いかも？

プログラムを書いた
り、バグを見つけた
りするのが楽しい
なーと感じていた頃

研究室でWeb セキュリティ

サイバーセキュリティ
の研究室に入る
Webセキュリティ
面白いなー
研究室起点で人との
繋がりができる

大学院 研究ちょっと辛い

大学院ネットワーク
の運用や企業との
共同研究などに参加。
伝える力の大事さを
より実感。

学生の時何してた？

サイバーセキュリティを仕事にするまでの道のり

転機1

ハッカーって カッコいい

日本の高校生が
ハッキングスキルを
武器にテロリストと
戦う漫画、BLOODY
MONDAYに出会う



画像出典：
https://m.media-amazon.com/images/I/7116y4SW8nL_SL1200_.jpg

2009

大学入学 ふらふら期

1年目はまずいろいろ
触れてみようと思い、
心理学やプログラミ
ング、いろいろな
講義へ。

2014

コミュニティ 活動に参加

勉強会に参加したり、
CTF for GIRLS運営に
入ったり。
セキュリティ業界の
仕事や働くイメージ
がみえてきた

2015

NECに入社

ペネトレーション
テストに興味があり、
志望。日本のインフ
ラを支えている大き
な会社で働きたいと
思い、入社。

2019

プログラミング 面白いかも？

プログラムを書いた
り、バグを見つけた
りするのが楽しい
なーと感じていた頃

研究室でWeb セキュリティ

サイバーセキュリティ
の研究室に入る
Webセキュリティ
面白いなー
研究室起点で人との
繋がりができる

大学院 研究ちょっと辛い

大学院ネットワーク
の運用や企業との
共同研究などに参加。
伝える力の大事さを
より実感。

学生の時何してた？

サイバーセキュリティを仕事にするまでの道のり

ハッカーって
カッコいい

日本の高校生が
ハッキングスキルを
武器にテロリストと
戦う漫画、BLOODY
MONDAYに出会う



画像出典：
https://m.media-amazon.com/images/I/7116y4SW8nL_SL1200_.jpg

2009

大学入学
ふらふら期

1年目はまずいろいろ
触れてみようと思い、
心理学やプログラミング、
いろいろな
講義へ。

2014

転機2

コミュニティ
活動に参加

勉強会に参加したり、
CTF for GIRLS運営に
入ったり。
セキュリティ業界の
仕事や働くイメージ
がみえてきた

2017

NECに入社

ペネトレーション
テストに興味があり、
志望。日本のインフラ
を支えている大きな
会社で働きたいと
思い、入社。

2019

2008

プログラミング
面白いかも？

プログラムを書いたり、
バグを見つけた
りするのが楽しい
なーと感じていた頃

2013

研究室でWeb
セキュリティ

サイバーセキュリティ
の研究室に入る
Webセキュリティ
面白いなー
研究室起点で人との
繋がりができる

2015

大学院
研究ちょっと辛い

大学院ネットワーク
の運用や企業との
共同研究などに参加。
伝える力の大事さを
より実感。

どうしたらなれるの？

「やりたいことをやる」がベースにあり、それを「どう社会に還元できるか、協力することでどう生かせるか」を考えて仕事をすることを意識しています



とりあえずやってみる 手を動かす

興味があることにはとりあえずチャレンジする。
手を動かしている見えるものが広がり、広がるとまた手を動かせるようになるの繰り返し。



狭い範囲にとどまらず コミュニティを広げる

何かものがあるって、その上にセキュリティがある。
なので、セキュリティにとどまらず、開発や運用も学ぶ。
様々な人と繋がりを持つ。



自分がやったことを どう生かすか考える

脆弱性を見つけて終わり、ではない。
それをどう生かしてシステムやサービスのセキュリティの向上につなげるのか、何のためにやっているのかを意識する。

NEC

\Orchestrating a brighter world