

Webサイト開発者向けセキュリティ・トレーニング  
ご案内資料

0. 本トレーニングの概要
1. STEP1 - Webサイトとサイバーセキュリティ
2. STEP2 - Webサイトへの攻撃手法と脆弱性対策
3. STEP3 - Webサイトへの検査手法とセキュリティ対策
4. 研修構成



## 0. 本トレーニングの概要

本トレーニングでは、「Webサイトのセキュリティ品質向上 & 保証を担う」中心的人材の育成を目指します。

1

STEP1  
Webサイトと  
サイバーセキュリティ

攻撃者の手口やインシデントの事例などを交え、ネットワークセキュリティからWebアプリケーションセキュリティまでサイバー攻撃の実態を幅広く学びます。

2

STEP2  
Webサイトへの攻撃手法と  
脆弱性対策

Webサイトに対する攻撃手法の学習を通じて、発生しうる被害、攻撃を可能にする脆弱性、およびその対策方法について詳細に学びます。

3

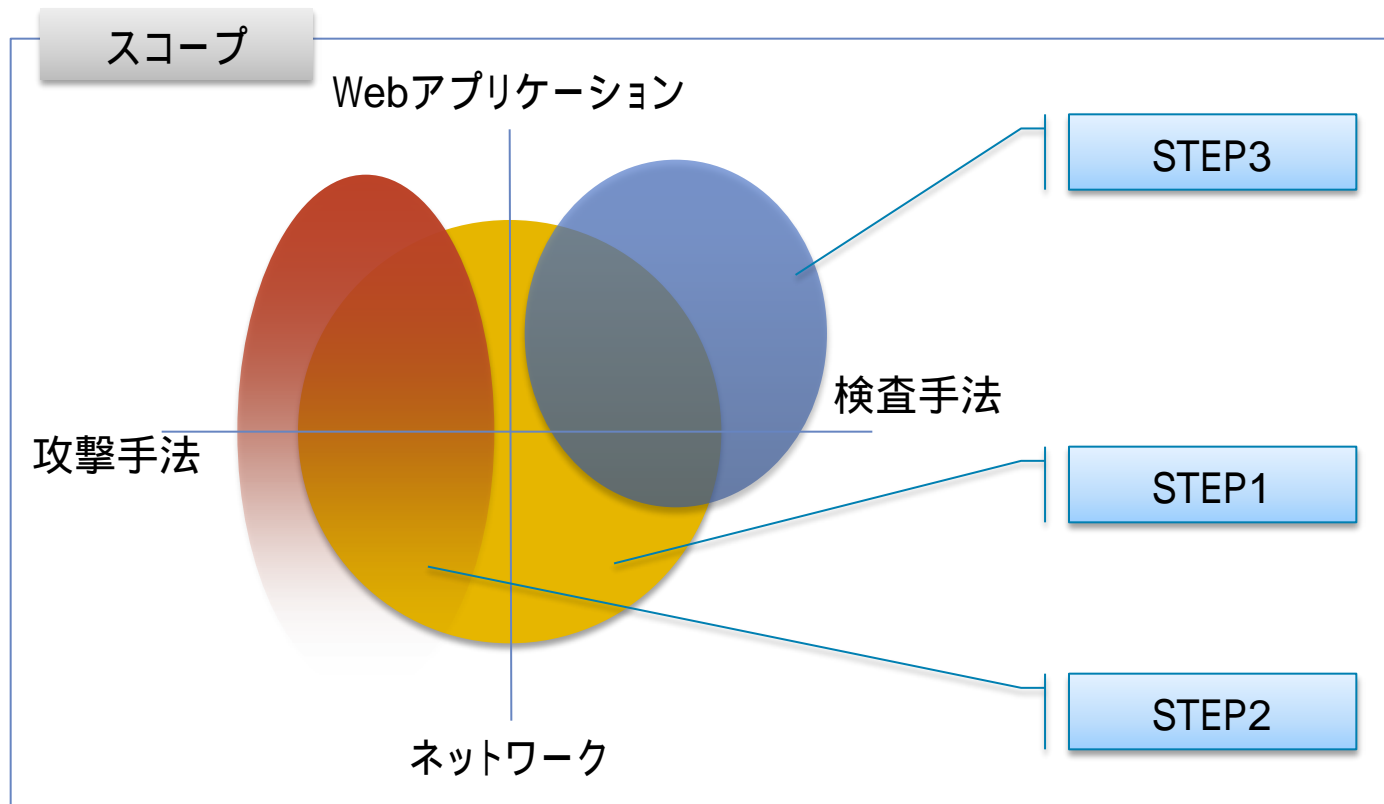
STEP3  
Webサイトへの検査手法と  
セキュリティ対策

Webサイトに対する検査手法の学習を通じて、脆弱性の判定方法、正しい対策の取り方、Webサイト構築におけるセキュリティ上の推奨事項などを学びます。

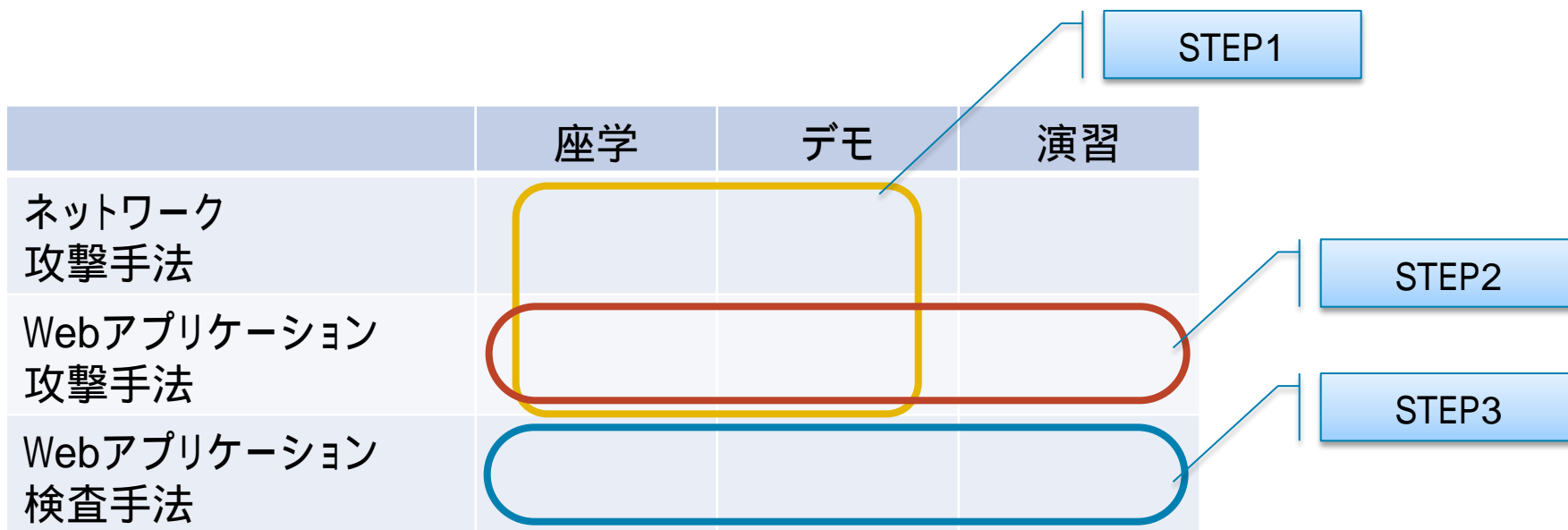
## 【研修受講者の到達目標】

- ・攻撃者の視点、攻撃に使用される手法を意識したセキュリティ対策ができる。
- ・Webサイトにおけるセキュリティ対策の必要性を説明できる。
- ・セキュアなWebサイト構築のために必要な観点を理解する。
- ・Webサイトのセキュリティ品質を向上するための手法を習得する。

本トレーニングにより学習する範囲を下図に示します。  
本トレーニングでは、「Webアプリケーション」、「ネットワーク」、「検査手法」、「攻撃手法」を軸とし、STEP1では全体を広く範囲に、STEP2・3では攻撃手法・検査手法をそれぞれ深く学習します。



本トレーニングにおける学習方法の範囲を下図に示します。  
 本トレーニングでは、内容に応じて「座学」、「デモ」、「演習(ハンズオン)」を使い分け、学習していきます。





## 1. STEP1 - Webサイトとサイバーセキュリティ

## STEP1の到達目標

1

セキュリティの最新動向、インシデント事例を理解する

Webサイトに関する最新のセキュリティ動向、および、インシデント事例から、セキュリティ対策の必要性について理解します。

2

攻撃者の行動原理を理解する

攻撃者の行動に関する基本的な法則や規則について、攻撃対象の選定方法、セキュリティホールの識別、また、侵入方法、そして侵入後の振舞いについて理解します。

3

攻撃の原理原則を理解する

攻撃者の目的により選択される様々な攻撃手法 (STEP2で取り上げない、フィッシングやソーシャルエンジニアリングなどの手法も含む) と、その一般的な対策方法を理解します。

STEP1では、Webサイトのセキュリティに関して広く概念を学習していただき、セキュリティ対策の必要性や、セキュリティの基本的な考え方の理解を目標とします。



## 教材内容

攻撃者の手口やインシデントの事例などを交え、ネットワークセキュリティからWebアプリケーションセキュリティまでサイバー攻撃の実態を幅広く学びます。

The collage features several key diagrams and text elements:

- Webサイト開発者向けセキュリティトレーニング STEP1**: A title for the training course.
- 5-3-o. Web: 脆弱性を悪用した攻撃**: A diagram showing a cross-site scripting (XSS) attack. It illustrates how an attacker injects malicious code into a legitimate user's browser, which then executes it on the target website.
- 4-5-o. NW: 脆弱性を悪用した攻撃**: A diagram showing a network-based attack where an attacker exploits a vulnerability in a network device to execute arbitrary code on a target server.
- 7-3-a. 開発**: A diagram showing the development phase of a security program, including design, development, and testing.
- 2010年 [Gumlar] Webサイトを利用して感染を拡大したウイルス**: A diagram showing how a virus can spread by exploiting vulnerabilities in web applications.
- 脆弱性**: A central diagram showing various types of vulnerabilities (e.g., XSS, SQLi) and their potential impacts (e.g., data theft, service disruption).

## 講義形式

- ・教材による座学
- ・攻撃のデモンストレーション
- ・理解度テスト



## ボリューム

1.5日程度

第1章 セキュリティの最新動向とインシデント事例	1-1. セキュリティ最新動向 1-2. インシデント事例 1-3. 不正アクセス禁止法など
第2章 セキュリティの構成要素	2-1. セキュリティの構成要素 2-2. 構成要素の定義と関係性 2-3. 構成要素の具体例
第3章 攻撃者像と攻撃手法	3-1. 攻撃者像(攻撃者の分類、目的、視点) 3-2. 攻撃手法の全体像 3-3. 攻撃手法の変遷と傾向 3-4. 攻撃者の目的と行動パターン 3-5. 攻撃者と構築側の心理戦
第4章 ネットワークへの攻撃手法と手順	4-0. NW: 攻撃手順の全体像 4-1. NW: 攻撃対象の選定 4-2. NW: ネットワーク情報の収集 4-3. NW: システム情報の収集 4-4. NW: セキュリティホールの識別 4-5. NW: 脆弱性を悪用した攻撃 4-6. NW: 攻撃成功後の行動
第5章 Webアプリケーションへの攻撃手法と手順	5-0. Web: 全体像 5-1. Web: 攻撃対象の選定 5-2. Web: システム情報の収集 5-3. Web: 脆弱性を悪用した攻撃 5-4. Web: 攻撃成功後の行動
第6章 その他の攻撃手法	6-1. ユーザ/端末への攻撃 6-2. かんたんログインへの攻撃 6-3. ソーシャルエンジニアリング
第7章 セキュリティホールが作りこまれる理由	7-1. サイト構築のフェーズ 7-2. 設計 7-3. 開発 7-4. 導入 7-5. 運用
STEP1 理解度テスト	課題1 課題2 課題3 課題3 発表



## 2. STEP2 - Webサイトへの攻撃手法と脆弱性対策

### STEP2の到達目標

1

WEBサイトへの攻撃手法を理解する

ネットワークからアプリケーションレイヤまでの攻撃手法について理解します。

2

WEBサイトへの攻撃手順を理解する

攻撃者視点による、調査フェーズから侵入フェーズにいたる一連の攻撃手順とその対策について理解します。

3

不正アクセスの影響、被害を理解する

不正アクセスに対する影響や被害について理解します。

STEP2では、攻撃者が使用するツールを利用し、調査フェーズから侵入フェーズにいたる一連の手順について、ネットワークレイヤからアプリケーションレイヤまでの攻撃手法、および、その対策方法について網羅的に理解することを目標とします。

## 教材内容

Webサイトに対する攻撃手法の学習を通じて、発生しうる被害、攻撃を可能にする脆弱性、およびその対策方法について詳細に学びます。

The collage features several key diagrams and text blocks:

- 4-3-d クロスサイトスクリプティング攻撃手法**: A flowchart showing the attack process from the attacker's site to the user's site and then to the target website. It highlights the injection of malicious scripts and the resulting actions on the target site.
- 4-4-1 クロスサイトリクエストフォージェリ攻撃を可能にする脆弱性への対策**: A diagram explaining the vulnerability of session cookies and how CSRF attacks exploit them. It includes a table with columns for '脆弱性' (Vulnerability) and '対策' (Countermeasure).
- インジェクション攻撃**: A diagram detailing SQL Injection attacks, showing how malicious SQL code is injected into a web form to manipulate the database. It includes a table with columns for '脆弱性' (Vulnerability), '攻撃手法' (Attack Method), and '想定被害' (Expected Damage).

## 講義形式

- ・教材による座学
- ・攻撃のデモンストレーション
- ・研修環境でのハンズオン
- ・理解度テスト



## ボリューム

1.5日程度

第1章 インシデントの原因となる脆弱性	1-1. インシデントの原因となる脆弱性
第2章 Webサイトの攻撃手順	2-1. サイト構成の把握(クロール) 2-2. アプリケーションに関する情報収集 2-3. 攻撃
第3章 攻撃ツールの種類と使い方	3-1. 攻撃ツールの種類と使い方 3-2. HTTP通信 3-3. BurpProxy説明
第4章 Webサイトの脆弱性を狙った代表的な攻撃手法、対策方法、被害事例	4-1. SQLインジェクション攻撃 4-2. OSコマンドインジェクション攻撃 4-3. クロスサイトスクリプティング攻撃 4-4. クロスサイトリクエストフォージェリ攻撃 4-5. セッションフィクセーション攻撃 4-6. アクセス制御の回避攻撃 4-7. ディレクトリトラバーサル攻撃 4-8. レスポンスヘッダインジェクション攻撃 4-9. 任意のサイトヘリダイレクト攻撃 4-10. 強制ブラウジング攻撃 4-11. その他の攻撃 4-12. 診断における事例解説
STEP2 理解度テスト	課題A 課題B 課題B 発表



### 3. STEP3 - Webサイトへの検査手法とセキュリティ対策

## STEP3の到達目標

1

セキュリティ検査の評価項目を理解する

セキュリティ検査を実施する場合に使用する評価項目の意図や優先順位について理解します。

2

脆弱性の有無についての判断基準を理解する

セキュリティ検査を実施した場合に、どのような基準で脆弱性と判断するかを理解します。

3

Webサイト構築におけるセキュリティ対策の考え方を理解する

セキュアなWebサイトを構築するために必要となる、セキュリティ対策の考え方を理解します。

STEP3では、セキュリティ検査の手法、および、考え方を中心に習得していただき、STEP1、STEP2に学習した内容を合わせ、システム開発の際に検討する必要があるセキュリティ要求事項を理解します。



## 教材内容

Webサイトに対する検査手法の学習を通じて、脆弱性の判定方法、正しい対策の取り方、Webサイト構築におけるセキュリティ上の推奨事項などを学びます。

**Webサイト開発者向けセキュリティトレーニング STEP3 Webサイトへの検査手法とセキュリティ対策**

2011年 NTTデータ先端技術株式会社

**3-3. パラメータ操作**  
SQLインジェクション攻撃を可能にする脆弱性検査チャート

対象	検査	結果	判定
パラメータ値	ハイト機能を使用しているか?	使用している	OK
		使用していない	
SQL特殊文字のEscaping処理に不備はないか?	不備はない	NG-SQLインジェクション	
	不備がある		

**1-1. セキュリティ検査とは**  
セキュリティ検査の目的とは?  
→Webサイトへの攻撃を可能とする脆弱性を洗い出し

脆弱性の存在状況が不明な状態 → 脆弱性の存在状況が明らかになる → 脆弱性が覆われる

脆弱性の存在状況が不明な状態では、正しく対策を取ることができません。脆弱性の存在状況を洗い出すことで、正しく対策を取ることが可能となります。

## 講義形式

- ・教材による座学
- ・攻撃のデモンストレーション
- ・研修環境でのハンズオン
- ・理解度テスト



## ボリューム

1.5日程度

第1章 セキュリティ検査の概要	1-1. セキュリティ検査とは 1-2. セキュリティ検査の流れ
第2章 セキュリティ検査の手法	2-1. ブラックボックス検査とホワイトボックス検査 2-2. ツール検査とマニュアル検査 2-3. 手法ごとのメリット/・デメリット
第3章 セキュリティ検査における評価項目と判断基準	3-0. 検査項目一覧 3-1. セッション管理 3-2. 認証/認可 3-3. パラメータ操作 3-4. ユーザ管理 3-5. 暗号 3-6. 情報 3-7. 画面設計 3-8. サーバ設定 3-9. ロジック流出 3-10. その他
第4章 Webサイト構築におけるセキュリティ対策の考え方	4-1. セキュリティ対策の原則
STEP3 理解度テスト	課題 課題 発表



## 4. 研修構成

項目	形式	Aコース	Bコース	Cコース	Dコース	ボリューム
STEP1 Webサイトと サイバーセキュリティ	座学					1.0日
	デモ					
	理解度テスト	-				0.5日
STEP2 Webサイトへの攻撃手法と 脆弱性対策	座学	-	-			1.0日
	デモ	-	-			
	ハンズオン	-	-			
	理解度テスト	-	-			0.5日
STEP3 Webサイトへの検査手法と セキュリティ対策	座学	-	-	-		1.0日
	デモ	-	-	-		
	ハンズオン	-	-	-		
	理解度テスト	-	-	-		0.5日
価格 (税抜)	10名様まで 11名以上の場合、別途お問い合わせください	60万円	90万円	180万円	270万円	

会場は、弊社の月島セミナールームのほか、貴社ご用意の会場でも承ります。  
用意する物品、時間帯の調整など詳細は別途ご相談ください。  
研修内容および価格は、改定されることがあります。

**NTTデータ先端技術株式会社**

**プラットフォーム事業部 研修担当**

TEL: 03-5843-6845

Mail: [itil-info@intellilink.co.jp](mailto:itil-info@intellilink.co.jp)



# NTT DATA

Global IT Innovator