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

NTT DATA

ver.20120130

INDEX

0. 本トレーニングの概要

0-1. 本トレーニングの概要

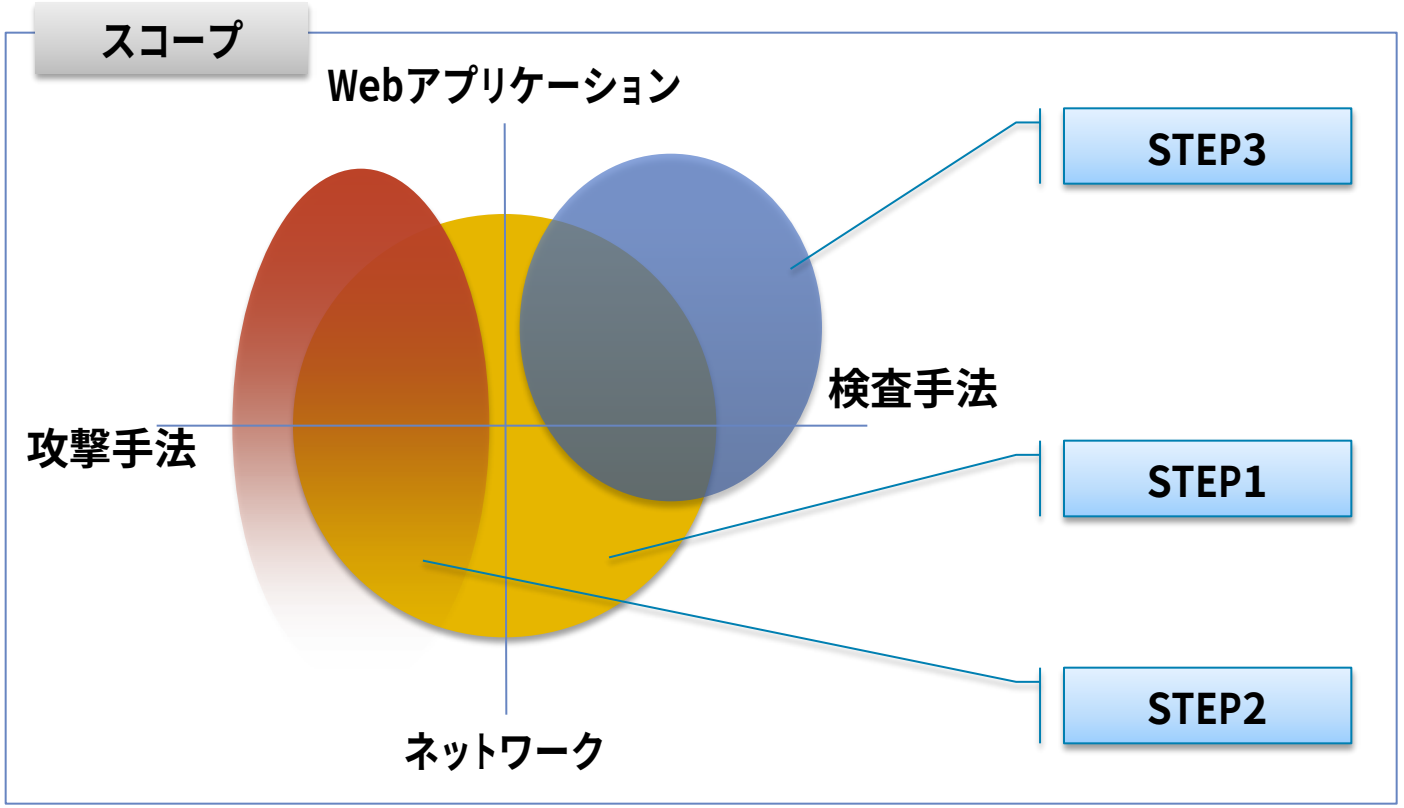
本トレーニングでは、「Webサイトのセキュリティ品質向上＆保証を担う」中心的人材の育成を目指します。

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。

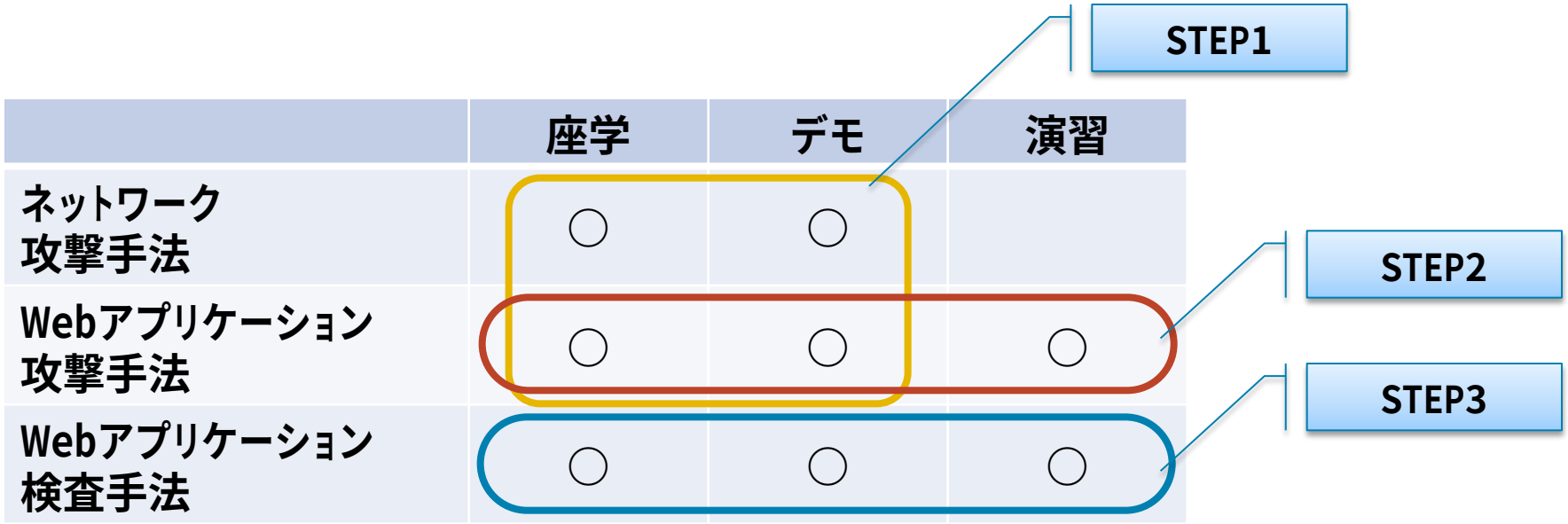
0-2. トレーニング内容のスコープ定義

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。



0-3. トレーニング方法について

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

1-1. STEP1　到達目標

■STEP1の到達目標

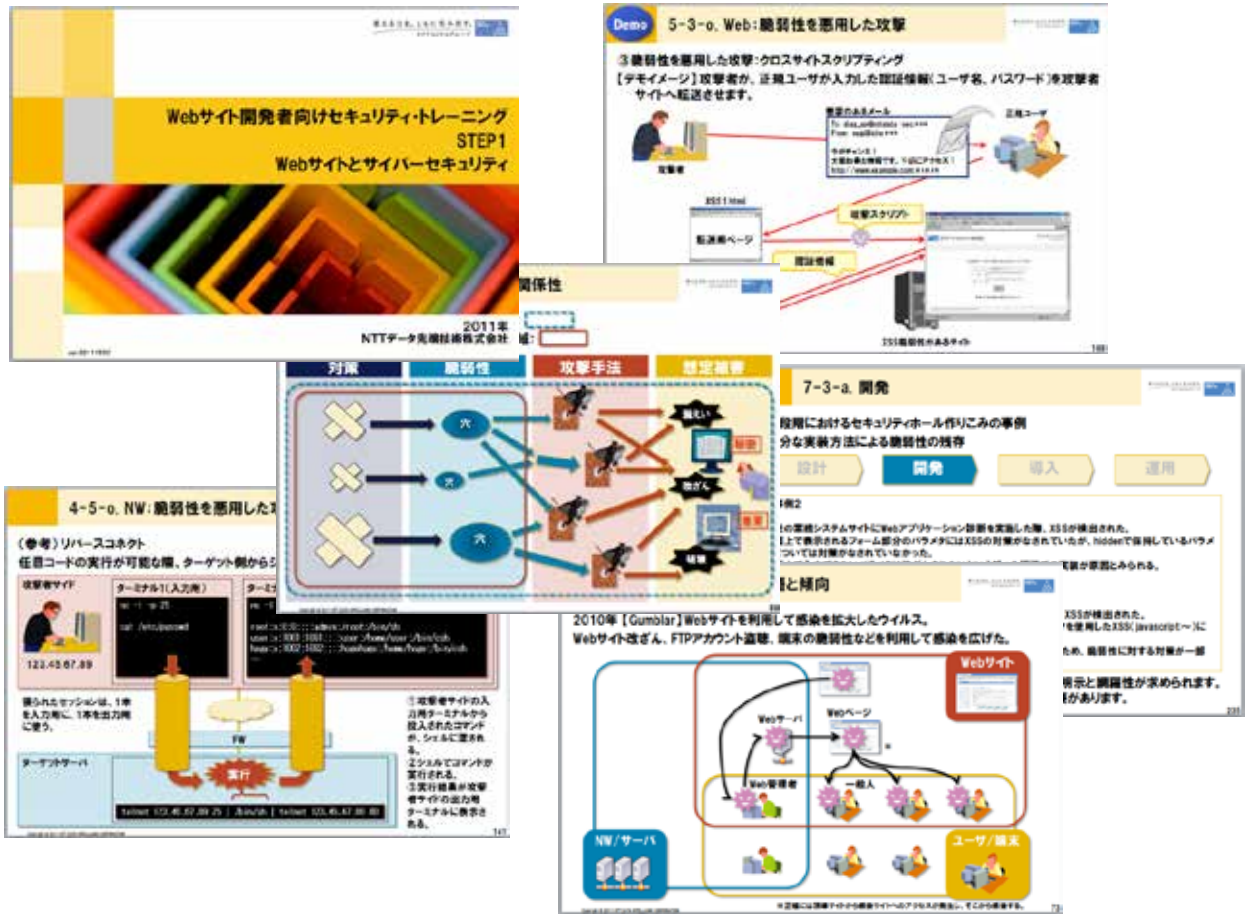
1	セキュリティの最新動向、インシデント事例を理解する	Webサイトに関する最新のセキュリティ動向、および、インシデント事例から、セキュリティ対策の必要性について理解します。
2	攻撃者の行動原理を理解する	攻撃者の行動に関する基本的な法則や規則について、攻撃対象の選定方法、セキュリティホールの識別、また、侵入方法、そして侵入後の振舞いについて理解します。
3	攻撃の原理原則を理解する	攻撃者の目的により選択される様々な攻撃手法（STEP2で取り上げない、フィッシングやソーシャルエンジニアリングなどの手法も含む）と、その一般的な対策方法を理解します。

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。

1-2. STEP1　研修イメージ

◆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。



◆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

1-3. STEP1　目次

2. STEP2 - Webサイトへの攻撃手法と脆弱性対策

■STEP2の到達目標

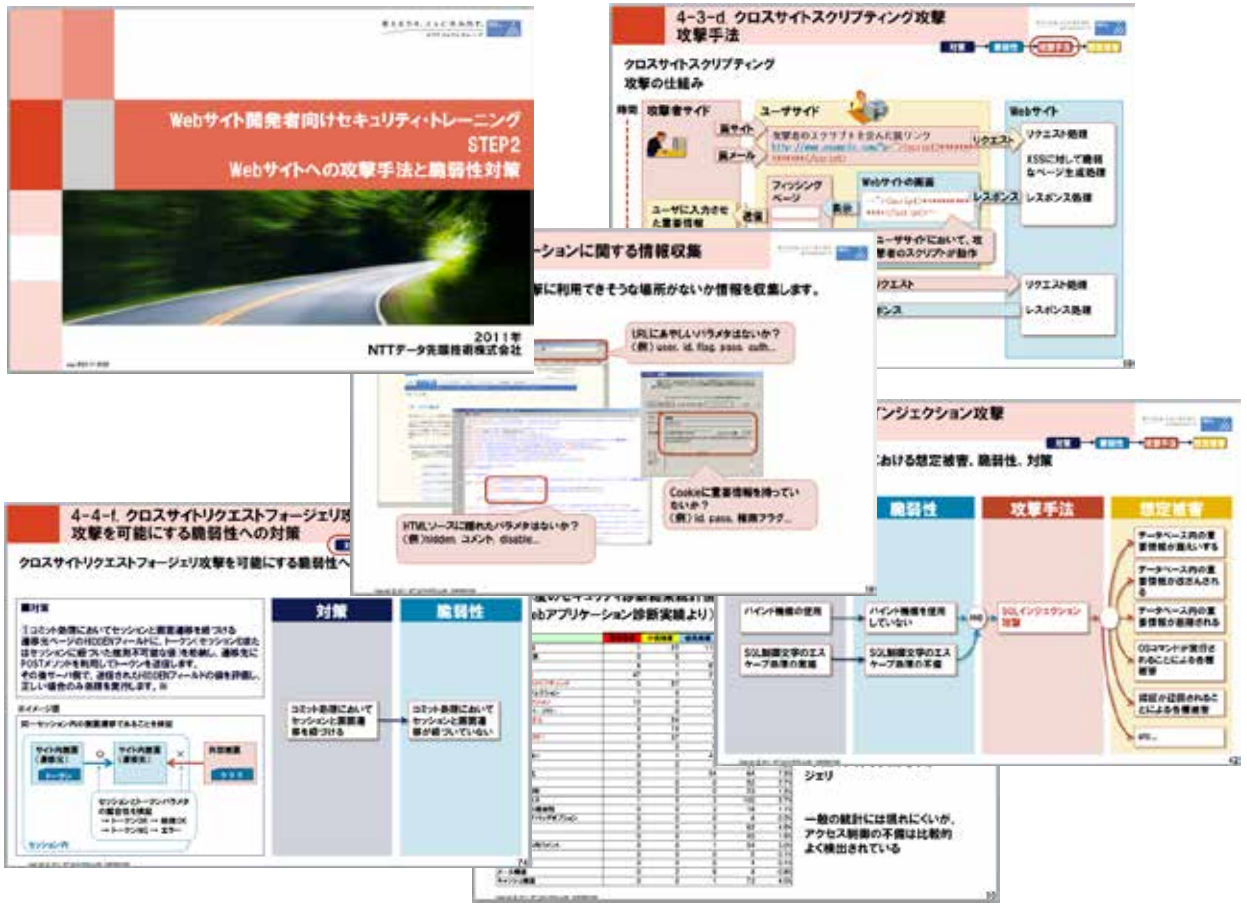
1	WEBサイトへの攻撃手法を理解する	ネットワークからアプリケーションレイヤまでの攻撃手法について理解します。
2	WEBサイトへの攻撃手順を理解する	攻撃者視点による、調査フェーズから侵入フェーズにいたる一連の攻撃手順とその対策について理解します。
3	不正アクセスの影響、被害を理解する	不正アクセスに対する影響や被害について理解します。

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。

2-2. STEP2　研修イメージ

◆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。



◆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

2-2. STEP3　目次

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. 任意のサイトへリダイレクト攻撃
	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

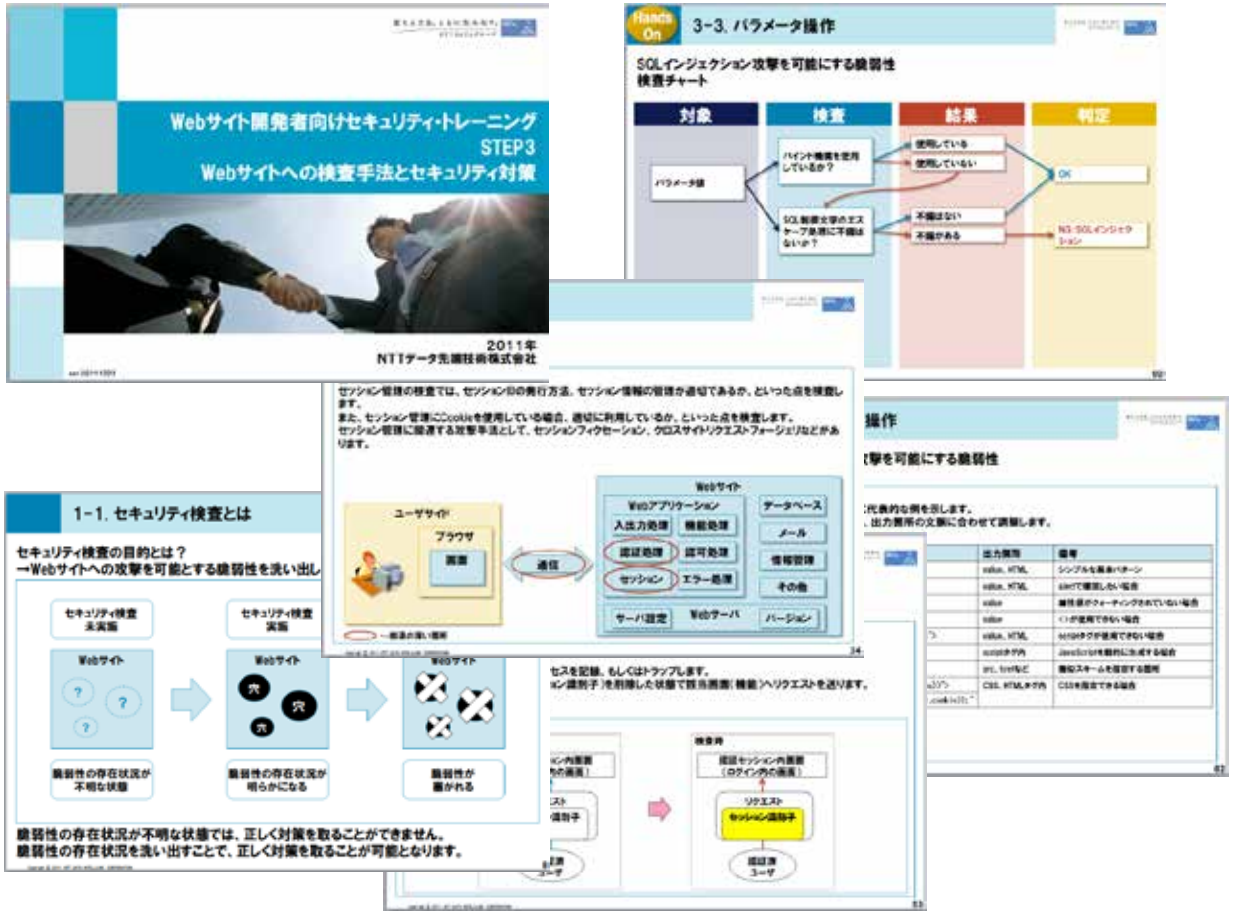
1	セキュリティ検査の評価項目を理解する	セキュリティ検査を実施する場合に使用する評価項目の意図や優先順位について理解します。
2	脆弱性の有無についての判断基準を理解する	セキュリティ検査を実施した場合に、どのような基準で脆弱性と判断するかを理解します。
3	Webサイト構築におけるセキュリティ対策の考え方を理解する	セキュアなWebサイトを構築するために必要となる、セキュリティ対策の考え方を理解します。

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のあるセキュリティ要求事項を理解します。

3-2. STEP3　研修イメージ

◆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。



◆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

3-3. STEP3　目次

4. 研修構成

4-1. 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、別途お問合せください	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。

お問い合わせ

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

NTT DATA

Global IT Innovator