# CNDv2 のリリース

## 日本では、2021 年 6 月に CNDv2 がリリースされました。

CNDv2 は、ネットワークセキュリティ問題を効果的に対応するための包括的なトレーニングとなっています。CNDv2 は、CNDv1 では「防御」「検出」「対応」の 3 つの範囲でしたが、それに「予測」が追加されました。

- モジュール　：14 モジュール→20 モジュールにリニューアル
- iLabs 数　：42 個　→　79 個へ大幅に増加

**1．Protect:防御**
- 多層防御セキュリティ
- 適切な設計・設定・施工されたセキュリティポリシー
- セキュリティアーキテクチャ
- 適切なコンフィグレーション
- セキュリティコントロール

**2．Detect:検出**
- トラフィックモニタリング
- ログ管理
- ログ監視
- 異常検出

**3．Respond:対応**
- インシデントレスポンス
- フォレンジック調査
- ビジネス継続性（BC）
- ディザスタリカバリ（DR）

**4．Predict:予測**
- リスクと脆弱性の評価
- 攻撃対象領域分析
- 脅威インテリジェンス

- CNDv1→CNDv2 の モジュール変更

以下の通り、モジュール変更いたしました。

◇v1

| | |
|---|---|
| 01 | コンピュータネットワークと防衛の基礎 |
| 02 | ネットワークセキュリティの脅威、脆弱性、攻撃 |
| 03 | ネットワークセキュリティのコントロール、プロトコル、デバイス防御 |
| 04 | ネットワークセキュリティポリシーのデザインと実装 |
| 05 | 物理セキュリティ |
| 06 | ホストセキュリティ |
| 07 | ファイヤーウォールの安全な構成と管理 |
| 08 | IDSの安全な構成と管理 |
| 09 | VPNの安全な構成と管理 |
| 10 | 無線ネットワークの防御 |
| 11 | ネットワークトラフィックのモニタリングと分析 |
| 12 | ネットワークリスクと脆弱性の管理 |
| 13 | データのバックアップとリカバリ |
| 14 | ネットワークインシデント対応と管理 |

v2

| | |
|---|---|
| 01 | ネットワーク攻撃と防御戦略 |
| 02 | ネットワークセキュリティ管理 |
| 03 | 技術的なネットワークセキュリティ |
| 04 | ネットワーク境界セキュリティ |
| 05 | エンドポイントセキュリティ - Windowsシステム |
| 06 | エンドポイントセキュリティ - Linux |
| 07 | エンドポイントセキュリティ - モバイルデバイス |
| 08 | エンドポイントセキュリティ - IoT |
| 09 | アプリケーションのセキュリティの管理 |
| 10 | データセキュリティ |
| 11 | エンタープライズ仮想ネットワークセキュリティ |
| 12 | エンタープライズクラウドネットワークセキュリティ |
| 13 | エンタープライズ無線ネットワークセキュリティ |
| 14 | ネットワークトラフィックの監視と分析 |
| 15 | ネットワークログの監視と分析 |
| 16 | インシデントレスポンスとフォレンジック調査 |
| 17 | ビジネス継続性とディザスタリカバリ |
| 18 | リスク管理によるリスク予測 |
| 19 | 攻撃表面分析による脅威評価 |
| 20 | サイバー脅威インテリジェンスによる脅威予測 |

# CND v2 の特徴

認定ネットワークディフェンダーCND v2 は、今日のネットワークセキュリティ問題に効果的に対処するための実践的なトレーニングを提供します。

**1.徹底したジョブタスク分析**

CNDv2は、NICE2.0フレームワークのサイバーセキュリティ教育フレームワークに基づいたプログラムとなっています。
米国国防総省のDoDDの4つの役割の推奨資格となっています。

**2.IoTセキュリティを追加**

IoTセキュリティが今や大きな懸念事項になっています。IoTデバイスをネットワークに接続する際の深刻な脆弱性があります。IoTデバイスの様々な課題とそれを軽減するために必要なセキュリティ対策について学ぶことができます。

**3.iLabsが充実**

CNDv2のプログラムは、CNDv1と比較してより実践的なトレーニングとなっており、iLabsが79(v1では42）と大幅に増設し充実をした内容となっています。

**4.リモート環境および仮想環境を保護**

セキュリティアプリケーションとリモート作業環境の構成を追跡することは非常に困難です。CNDv2は仮想化環境を保護するための完全なセキュリティ基準をカバーします。

**5．モバイルセキュリティ対策**

Gartnerは2021年までに企業のデータトラフィックの27%が境界セキュリティをバイパスし、モバイルデバイスやリモート端末からクラウドに直接流れると予測しています。CNDv2ではこのエンドポイントが安全案状態を維持する方法を学習します。

**6．クラウドセキュリティ対策強化**

企業、組織でのクラウドコンピューティングの利用は拡大している一方で、課題も増加しています。AWS、Azure、Googleなどのクラウドプラットフォームでセキュリティを確保するための方法について説明をします。

**7．脅威インテリジェンスの紹介**

セキュリティに対する予防的なアプローチが必要となっています。脅威インテリジェンが」なければサイバーセキュリティ対策は受け身になります。CNDv2は、脅威インテリジェンスを使用し、より効果的なプロアクティブなアプローチを取ることに役立ちます。

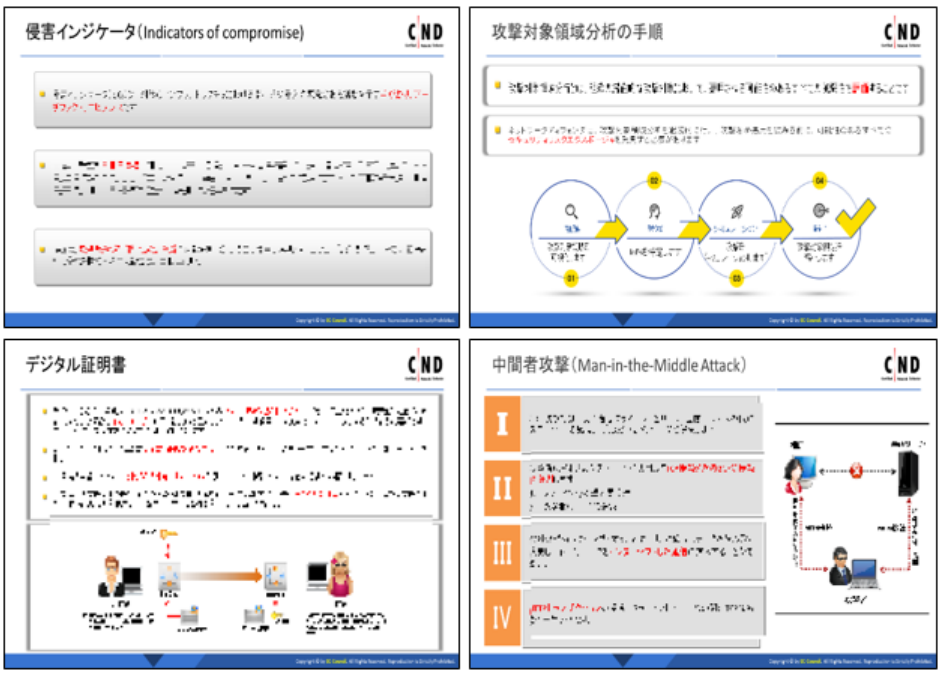
**8．詳細な攻撃の解析**

サイバーリスク管理のカギは、詳細な攻撃対象領域の分析である。。CNDv2は、セキュリティの脆弱性について組織のどの部分をレビュー・テストする必要があるかを特定数方法とネットワークのリスクを軽減、防止する方法を提供する

**9、最新の技術**

SDNセキュリティ、NFVセキュリティ、コンテナセキュリティ、Dockerセキュリティ、Kubernetesセキュリティなどの最新のテクノロジーにも対応しています。

# CND v2 テキストイメージ




**テキスト内容**

- ✓ **20のモジュール**
- ✓ **約1600のスライド**
  (v1は80 0 のスライド)
- ✓ **日本語対応**

**実践的なセキュリティについて、効率よく学習することが可能**

**BSI Professional Services Japan 株式会社 へのお問い合わせ先：**

BSI.PSJ@bsigroup.com

お急ぎの方は、下記弊社営業担当へのご連絡も受け付けております。

弊社主催有料研修担当：

◆三森　優（Yu, Mitsumori）070-1640-8511