

# Table of Contents 目 次

---

## Executive Summary 要 旨

### 1. Introduction 序 章

1. Authority 権 限
2. Purpose and Scope 目的と範囲
3. Audience 対象者
4. Document Structure 文章構成

### 2. Organizing a Computer Security Incident Response Capability コンピュータセキュリティのインシデント対応力の組織化

1. Events and Incidents イベントとインシデント
2. Need for Incident Response インシデント対応の必要性
3. Incident Response Policy, Plan, and Procedure Creation インシデント対応方針・計画・手順の作成
  1. Policy Elements ポリシーの要素
  2. Plan Elements 計画の要素
  3. Procedure Elements 手順の要素
  4. Sharing Information With Outside Parties 外部との情報共有
4. Incident Response Team Structure インシデント対応チームの構成
  1. Team Models チームモデル
  2. Team Model Selection チームモデルの選択
  3. Incident Response Personnel インシデント対応要員
  4. Dependencies within Organizations 組織内の依存関係
5. Incident Response Team Services インシデント対応チームサービス
6. Recommendations 推奨事項

### 3. Handling an Incident インシデントのハンドリング

1. Preparation 準 備
  1. Preparing to Handle Incidents インシデントハンドリングの準備
  2. Preventing Incidents インシデントの予防
2. Detection and Analysis 検出と分析
  1. Attack Vectors 攻撃手法
  2. Signs of an Incident インシデントの兆候
  3. Sources of Precursors and Indicators 前兆と兆候のソース
  4. Incident Analysis インシデント分析
  5. Incident Documentation インシデントの文書
  6. Incident Prioritization インシデントの優先順位付け
  7. Incident Notification インシデントの通知
3. Containment, Eradication, and Recovery 封じ込め・根絶・復旧
  1. Choosing a Containment Strategy 封じ込め戦略の選択
  2. Evidence Gathering and Handling 証拠の収集と処理
  3. Identifying the Attacking Hosts 攻撃ホストの特定
  4. Eradication and Recovery 根絶と回復
4. Post-Incident Activity インシデント後の活動
  1. Lessons Learned 教 訓

- 2. Using Collected Incident Data 収集したインシデントデータの利用
- 3. Evidence Retention 証拠の保持
- 5. Incident Handling Checklist インシデントハンドリングチェックリスト
- 6. Recommendations 推奨事項
- 4. Coordination and Information Sharing 連携と情報共有
  - 1. Coordination 連携
    - 1. Coordination Relationships 連携の関係
    - 2. Sharing Agreements and Reporting Requirements 協定と報告要件
  - 2. Information Sharing Techniques 情報共有のテクニック
    - 1. Ad Hoc アドホック
    - 2. Partially Automated 部分的な自動化
    - 3. Security Considerations セキュリティに関する考慮事項
  - 3. Granular Information Sharing 粒度の高い情報の共有
    - 1. Business Impact Information ビジネスへの影響情報
    - 2. Technical Information 技術情報
  - 4. Recommendations 推奨事項

List of Appendices 付録リスト Appendix A— Incident Handling Scenarios インシデントハンドリングのシナリオ A.1 Scenario Questions シナリオの質問

A.2 Scenarios シナリオ

Appendix B— Incident-Related Data Elements インシデント関連データ要素

B.1 Basic Data Elements 基本データ要素

B.2 Incident Handler Data Elements インシデントハンドラのデータ要素

Appendix C— Glossary 用語集

Appendix D— Acronyms 頭字語（略語）集

Appendix E— Resources 情報源 Appendix F— Frequently Asked Questions よくある質問

Appendix G— Crisis Handling Steps 危機対応のステップ

Appendix H— Change Log（省略）