1. 序 章

1.1 権 限

国立標準技術研究所（NIST）は、2002 年の連邦情報セキュリティ管理法（FISMA）（公法 107-347）に基づく法的責任を推進するために、この文書を作成しました。NIST は、すべての機関の業務と資産に適切な情報セキュリティを提供するために、最低限の要件を含む標準とガイドラインを策定する責任がありますが、このような標準とガイドラインは、国家安全保障システムには適用されないものとします。本ガイドラインは、管理予算局（OMB）通達 Circular A-130 の第 8b(3)項「省庁情報システムのセキュリティ確保」の要求事項と一致しており、A-130 の付録 IV: 重要な項の分析で分析されています。補足情報は、A-130「付録III」に記載されています。本ガイドラインは、連邦政府機関が使用するために作成されたものです。非政府組織が任意で使用することができ、著作権の対象とはなりませんが、帰属表示が望まれます。また、これらのガイドラインは、商務省長官、OMB長官、またはその他の連邦職員の既存の権限を変更したり、それに取って代わるものとして解釈されるべきではありません。

1.2 目的と範囲

本書は、インシデントへの効果的かつ効率的な対応に関する実践的なガイドラインを提供することで、コンピュータセキュリ ティインシデントによるリスクを軽減するための組織を支援することを目的としています。本書には、効果的なインシデント対応プログラムの確立に関するガイドラインが含まれていますが、本書の主な焦点は、インシデントの検出、分析、優先順位付け、および対応です。組織は、推奨されるガイドラインとソリューションを、特定のセキュリティとミッションの要件を満たすように調整することが推奨されます。

1.3 対象者

この文書は、コンピュータセキュリティインシデント対応チーム（CSIRT）、システムおよびネットワーク管理者、セキュリティスタッフ、技術サポートスタッフ、最高情報セキュリティ責任者（CISO）、最高情報責任者（CIO）、コンピュータセキュリティプログラムマネージャー、その他セキュリティインシデントへの準備や対応に責任を持つ人々のために作成されました。

1.4 文章構成

本書の残りの部分は、以下のセクションと付録で構成されています。

■ セクション2では、インシデント対応の必要性について議論し、可能なインシデント対応チームの構造を概説し、インシデントハンドリングに参加する可能性のある組織内の他のグループを強調しています。

■ セクション3では、基本的なインシデント対応のステップをレビューし、インシデント対応をより効果的に行うための アドバイス、特にインシデントの検出と分析を提供しています。

■ セクション4では、インシデント対応の調整と情報共有の必要性を検討しています。

■ 付録Aには、インシデント対応の卓上ディスカッションで使用するためのインシデント対応シナリオと質問が含まれています。

■ 付録Bは、各インシデントについて収集すべきデータフィールドのリストを提供しています。

■ 付録CとDには、それぞれ用語集と頭字語のリストが含まれています。

■ 付録Eは、インシデント対応の計画と実行に有用なリソースを特定しています。

■ 付録Fでは、インシデント対応に関するよくある質問を取り上げています。

■ 付録 G には、コンピュータ・セキュリティ・インシデント関連の危機に対処する際に従うべき主な手順が記載されています。

■ 付録 H には、前回の改訂以降の重要な変更点をリストアップした変更ログが含まれています。

抄　録

コンピュータセキュリティのインシデント対応は、情報技術（IT）プログラムの重要な要素となっています。インシデント対応を効果的に行うことは複雑な作業であるため、成功するインシデント対応能力を確立するには、相当な計画とリソースが必要となります。本書は、コンピュータ・セキュリティ・インシデント対応能力を確立し、インシデントを効率的かつ効果的に処理するために、組織を支援するものです。本書は、特にインシデント関連データを分析し、各インシデントへの適切な対応を決定するためのインシデント対応のガイドラインを提供します。このガイドラインは、特定のハードウェアプラットフォーム、オペレーティングシステム、プロトコル、またはアプリケーションに依存せずに使用することができます。

キーワード

コンピュータセキュリティインシデント
インシデントハンドリング
インシデント対応
情報セキュリティ