4. 付　録

付録A　インシデントハンドリングのシナリオ

インシデントハンドリングシナリオは、そのスキルの構築とプロセスの潜在的な問題点を特定するための軽易で効果的な方法を提供します。インシデントハンドリングチームまたはチームメンバーには、シナリオと関連する質問のリストが提示されます。その後、チームはそれぞれの質問について議論し、最も可能性の高い回答を決定します。ゴールは、チームが実際に何をするかを判断し、それをポリシー、手順、および一般的に推奨されている慣行と比較して、矛盾や欠陥を特定することです。例えば、ある質問への回答は、チームにソフトウェアがないために回答が遅れることや、他のチームが時間外のサポートを提供していないために回答が遅れることを示しているかもしれません。

以下の質問は、ほぼすべてのシナリオに当てはまります。各質問の後には、文書の関連するセクションを参照してください。質問の後にはシナリオがあり、それぞれの質問の後には追加のインシデント固有の質問が続きます。組織において、これらの質問とシナリオを、独自のインシデントハンドリング演習で使用するよう強く推奨します※。

※ 演習の詳細については、http://csrc.nist.gov/publications/PubsSPs.html#800-84 にある NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities を参照してください。

A.1 シナリオの質問

準　備

1. 組織はこの活動をインシデントと考えますか？その場合、この活動は組織のどの方針に違反していますか？(セクション2.1)
2. このタイプのインシデントの発生を防止するため、またはその影響を制限するために、どのような対策が講じられていますか？(セクション3.1.2)

検知と分析

1. インシデントの前兆があるとすれば、組織はどのようなものを検知する可能性はありますか? 前兆があれば、組織はインシデントが発生する前に行動を起こせますか? (セクション 3.2.2.2, 3.2.3)
2. どのような兆候があれば、組織はインシデントを検知できますか？どのような兆候があれば、インシデントが発生したかもしれないと誰かに思わせることができますか？(セクション 3.2.2.2、3.2.3)
3. この特定のインシデントを検出するために、どのような追加ツールが必要になるかもしれませんか? (セクション 3.2.3)
4. インシデント対応チームは、どのようにしてこのインシデントを分析し、検証しますか？どのような人員が分析及び検証プロセスに関与しますか？(セクション3.2.4)
5. チームは、組織内のどのような人々やグループにインシデントを報告しますか？(セクション 3.2.7)
6. チームはどのようにしてこのインシデントの処理に優先順位をつけますか？(セクション 3.2.6)

封じ込め、根絶、回復

1. このインシデントを封じ込めるために、組織はどのような戦略をとるべきですか？この戦略が他の戦略よりも望ましい理由は何ですか？(セクション 3.3.1)
2. インシデントが封じ込められなかった場合、何が起こりえますか？(セクション 3.3.1)
3. この特定のインシデントに対応するために、どのような追加ツールが必要になるかもしれませんか？(セクション 3.3.1、3.3.4)
4. 封じ込め、根絶、回復のプロセスにはどのような人員が関与しますか？(セクション 3.3.1 、3.3.4)
5. 組織は、もしあるならば、どのような証拠の情報源を取得すべきですか？どのようにして証拠を取得しますか？どこに保管しますか？どのくらいの期間保管されるべきですか？(セクション3.2.5、3.3.2、3.4.3)

インシデント後の活動

1. このインシデントに関する教訓を学ぶ会議には誰が出席します？(セクション3.4.1)
2. 今後同様のインシデントが発生しないようにするために、何ができますか？(セクション 3.1.2)
3. 同様のインシデントの検出を改善するために何ができますか？(セクション 3.1.2)

一般的な質問

1. このインシデントの対応には、何人のインシデントハンドリングチームメンバーが参加しますか？(セクション2.4.3)
2. インシデント対応チーム以外に、組織内のどのようなグループがこのインシデントの対処に関与しますか？(セクション2.4.4)
3. チームはどの外部関係者にインシデントを報告しますか? 各報告はいつ行われますか? 各報告はどのように行われますか？どのような情報を報告するか、あるいは報告しないか、その理由は？(セクション2.3.2)
4. その他、外部とのコミュニケーションはどのような場合に発生しますか？(セクション 2.3.2)
5. このインシデントに対処するために、チームはどのようなツールやリソースを使用しますか？(セクション3.1.1)
6. もしインシデントが別の日と時間に発生していたら、処理のどのような側面が違っていたでしょうか(時間内と時間外)？(セクション2.4.2)
7. インシデントが異なる物理的な場所で発生していたら、処理のどのような側面が違っていたでしょうか（オンサイトとオフサイト）？(セクション2.4.2)

A.2 シナリオ

シナリオ１：ドメインネームシステム(DNS)サーバのDoS(サービス拒否)

土曜日の午後、外部のユーザーが組織の公開ウェブサイトにアクセスする際に問題が発生します。その後1時間ほどで問題は悪化し、ほぼすべてのアクセスが失敗するまでになりました。一方、組織のネットワーキン

グ担当者の一人がインターネットとの境界ルーターからの警告に応答し、組織のインターネット帯域幅が、組織のパブリックDNSサーバーとの間のユーザー・データグラム・プロトコル(UDP)パケットの異常に大量のパケットによって消費されていると判断しました。トラフィックを分析すると、DNSサーバーは1つの外部IPアドレスから大量のリクエストを受信していることがわかります。また、そのアドレスからのDNSリクエストはすべて同じソースポートから来ています。
このシナリオに関する追加の質問は以下の通りです。

1. 問題の外部IPアドレスに関して、組織は誰に連絡すべきか?
2. 初期の封じ込め対策を実施した後、ネットワーク管理者が、9 台の内部ホストが DNS サーバーに同じ異常な要求を試みていることを検出したとします。
3. 9台の内部ホストのうち2台が、システムの所有者が特定される前にネットワークから切断されたとします。システム所有者はどのようにして特定されますか?

シナリオ２：ワームと分散型サービス拒否（DDoS）エージェントの侵入

火曜日の朝、新しいワームがリリースされます。このワームはリムーバブルメディアを介して拡散し、自分自身をコピーしてWindowsの共有を開くことができます。ワームがホストに感染すると、DDoSエージェントをインストールします。ワームが拡散し始めてから数時間後のウイルス対策シグネチャが利用可能になる前に、組織はすでに広範囲の感染を起こしています。
このシナリオに関する追加の質問は以下の通りです。

1. インシデント対応チームは、感染したすべてのホストをどのようにして特定しますか?
2. ウイルス対策シグネチャがリリースされる前に、組織はどのようにしてワームが組織内に侵入するのを防止しようとしますか?
3. ウイルス対策のシグネチャがリリースされる前に、感染したホストによるワームの拡散をどのようにして防ぐことができますか?
4. 組織はすべての脆弱性のあるマシンにパッチを当てることを試みますか? その場合、どのようにしてパッチを適用しますか?
5. DDoS エージェントを受け取った感染ホストが、翌朝に別の組織のウェブサイトを攻撃するように設定されていた場合、このインシデントの処理はどのように変わりますか?
6. 感染したホストの 1 台以上に、組織の従業員に関する機密性の高い個人情報が含まれていた場合、このインシデントの処理はどのように変わりますか?
7. インシデント対応チームは、どのようにして組織のユーザーにインシデントの状況を通知しますか?
8. 現在ネットワークに接続されていないホスト(例: 休暇中のスタッフ、たまに接続するオフサイトの従業員)に対して、チームはどのような追加対策を行いますか?

シナリオ３：ドキュメントの盗難

月曜日の朝、組織の法務部門は、組織のシステムに関わる不審な活動について、連邦捜査局 (FBI) から電話を受けました。その日の後半、FBI捜査官が経営陣と法務部のメンバーと面会し、その活動について話し合うことになります。FBIは、機密性の高い政府文書の公開に関わる活動を調査しており、その文書の一部は組織のものであると報告されていました。捜査官は組織の支援を求め、経営陣はこれらの文書が正当なものであるかどうか、どのようにして漏洩した可能性があるかを判断するために必要な証拠を入手するために、インシデント対応チームの支援を求めています。
このシナリオに関する追加の質問は以下の通りです。

1. インシデント対応チームは、どのような情報源から証拠を収集する可能性がありますか？
2. 調査の秘密を守るために、チームは何をしますか？

3. チームが漏洩の原因となった内部ホストを特定した場合、このインシデントの処理はどのように変わるでしょうか?
4. チームが漏洩の原因となった内部ホストにインストールされたルートキットを発見した場合、このインシデントの処理はどのように変わりますか?

シナリオ４: データベースサーバの危殆化

火曜日の夜、データベース管理者は、いくつかの本番用データベースサーバのメンテナンスを時間外に行いました。管理者は、サーバの1つに見慣れない珍しいディレクトリ名があることに気付きました。ディレクトリのリストを確認し、いくつかのファイルを閲覧した後、管理者はサーバが攻撃されたと結論付け、インシデント対応チームに支援を要請しました。チームの調査では、攻撃者が6週間前にサーバへのルートアクセスに成功したことが判明しました。 このシナリオに関する追加の質問は以下の通りです。

1. チームはどのような情報源を使用して、侵害がいつ発生したかを判断することができますか?
2. データベースサーバがパケットスニッファーを実行し、ネットワークからパスワードを取得していたことをチームが発見した場合、このインシデントの処理はどのように変わるでしょうか?
3. サーバが毎晩、機密性の高い顧客情報(個人を特定できる情報を含む)を含むデータベースをコピーして外部アドレスに転送するプロセスを実行していたことをチームが発見した場合、このインシデントの処理はどのように変わるでしょうか?
4. チームがサーバ上にルートキットを発見した場合、このインシデントの処理はどのように変わりますか?

シナリオ５：不明な流出

日曜日の夜、組織のネットワーク侵入検知センサーの1つが、大規模なファイル転送を含む異常なアウトバウンドネットワークアクティビティを警告しました。侵入アナリストがアラートを確認すると、何千もの .RAR ファイルが内部ホストから外部ホストにコピーされており、外部ホストは別の国に位置していることがわかりました。アナリストは、インシデント対応チームに連絡して、その活動をさらに調査できるようにします。.RAR ファイルの内容は暗号化されているため、チームは .RAR ファイルが何を保持しているかを見ることができません。.RARファイルを含む内部ホストを分析すると、ボットのインストールの兆候が見られます。 このシナリオに関する追加の質問は以下の通りです。

1. . RARファイルの内部にある可能性の高いものをチームはどのように判断するのでしょうか？他のどのチームがインシデント対応チームを支援しますか？
2. インシデント対応チームが、最初の侵害が内部ホストのワイヤレスネットワークカードを介して行われたと判断した場合、チームはこの活動をどのようにしてさらに調査しますか?
3. インシデント対応チームが、内部ホストが企業内の他のホストからの機密ファイルのステージングに使用されていると判断した場合、チームはどのようにしてこの活動をさらに調査しますか?

シナリオア６：給与記録への不正アクセス

水曜日の夕方、組織のフィジカルセキュリティチームは、給与計算の管理者から「見知らぬ人物がオフィスを出て廊下を駆け下り、ビルから出ていくのを見た」と電話を受けました。その管理者は、数分間だけ自分のワークステーションの鍵を開けたまま放置していました。給与計算プログラムは放置したままログインし、メインメニューに表示されていましたが、管理者はマウスが移動したように見えることに気付きました。インシデント対応チームは、インシデントに関連する証拠を取得し、どのような行動が行われたかを判断するように求められています。 このシナリオに関する追加の質問は以下の通りです。

1. どのようにして、どのようなアクションが実行されたかを判断するのでしょうか?

2. 給与管理者が、退社した人物を元給与計算部門の従業員と認識していた場合、このインシデントの処理はどのように違っていたのでしょうか？
3. その人物が現役の従業員であると信じるに足る理由があった場合、このインシデントの処理はどのように異なるでしょうか？
4. フィジカルセキュリティ・チームが、その人物がソーシャル・エンジニアリング技術を使って建物に物理的にアクセスしたと判断した場合、このインシデントの処理はどのように異なるでしょうか?
5. 前週のログに、給与管理者のユーザーIDを使用したリモートログインの試みに異常に多くの失敗があった場合、このインシデントの処理はどのように異なるのでしょうか?
6. 2週間前に、インシデント対応チームがコンピュータにキーストロークロガーがインストールされていたことを発見した場合、このインシデントの処理はどのように異なるでしょうか？

シナリオ７：消えるホスト

木曜日の午後、ネットワーク侵入検知センサーが、内部IPアドレスによって生成された内部ホストに向けられた脆弱性スキャン活動を記録します。侵入検知アナリストは、許可され、かつスケジュールされた脆弱性スキャンがないことを知っているため、その活動をインシデント対応チームに報告します。チームが分析を開始すると、アクティビティが停止しており、そのIPアドレスを使用しているホストが存在しなくなっていることがわかります。 このシナリオに関する追加の質問は以下の通りです。

1. どのようなデータソースが脆弱性スキャンホストの身元に関する情報を含んでいる可能性がありますか?
2. チームは、どのようにして脆弱性スキャンを実行していた人を特定するのでしょうか？
3. 脆弱性スキャンが組織の最も重要なホストに向けられていた場合、このインシデントの処理はどのように異なるでしょうか?
4. 脆弱性スキャンが外部ホストに向けられていた場合、このインシデントの取り扱いはどのように異なるでしょうか?
5. 内部IPアドレスが組織の無線ゲストネットワークに関連付けられていた場合、このインシデントの処理はどのように異なるでしょうか?
6. フィジカルセキュリティスタッフが、脆弱性スキャンが発生する30分前に誰かが施設に侵入したことを発見した場合、このインシデントの処理はどのように異なるでしょうか?

シナリオ８：在宅勤務の妥協点

土曜日の夜、ネットワーク侵入検知ソフトウェアは、ウォッチリストのIPアドレスから発信されたインバウンド接続を記録します。侵入検知アナリストは、その接続が組織のVPN サーバーに行われていると判断し、インシデント対応チームに連絡します。チームは、侵入検知、ファイアウォール、および VPN サーバーのログを確認し、セッションで認証されたユーザー ID と、そのユーザー ID に関連付けられたユーザー名を特定します。
このシナリオに関する追加の質問は以下の通りです。

1. チームの次のステップは何ですか? なぜこのステップを最初に実行する必要があるのでしょうか? 次に実行すべきステップは何ですか?
2. 外部IPアドレスがオープンプロキシに属していた場合、このインシデントの処理はどのように異なるでしょうか?
3. ユーザーが知らないうちに、そのIDが複数の外部IPアドレスからVPN接続を開始するために使用されていた場合、このインシデントの処理はどのように異なるでしょうか?
4. 特定されたユーザーのコンピュータが、家族のメンバーによってダウンロードされたトロイの木馬を含むゲームによって危険にさらされていたとします。これは、証拠の収集と処理にどのような影響を

与えますか？ユーザーのコンピュータからインシデントを根絶するという点で、チームは何をすべきでしょうか?
5. ユーザーがウイルス対策ソフトをインストールし、トロイの木馬にキーストロークロガーが含まれていたと判断したとします。このことは、インシデントの処理にどのような影響を与えますか? ユーザーがシステム管理者であった場合、このことはインシデントの処理にどのような影響を与えますか? ユーザーが組織内の高位幹部であった場合、このことはインシデントの処理にどのような影響を与えるでしょうか?

シナリオ９：匿名の脅威

木曜日の午後、組織のフィジカルセキュリティチームは、IT マネージャから「従業員2名が組織のシステムに対する匿名の脅迫を受けた」との報告を受けました。調査に基づき、フィジカルセキュリティチームは、脅威を真剣に受け止めるべきだと考え、インシデント対応チームを含む適切な内部チームに脅威を通知します。
このシナリオに関する追加の質問は以下の通りです。

1. インシデント対応チームは、脅威の通知に対応して、何かあるとすれば、どのように異なる行動をとるべきでしょうか？
2. フィジカルセキュリティ管理の強化は、インシデント対応チームの対応にどのような影響を与える可能性がありますか？

シナリオ１０：ピアツーピアによるファイル共有

この組織では、ピアツーピアのファイル共有サービスの使用を禁止しています。この組織のネットワーク侵入検知センサーは、複数の一般的なピアツーピアファイル共有サービスの使用を検知できるシグネチャを有効にしています。月曜日の夕方、侵入検知アナリストは、過去3時間の間に複数のファイル共有アラートが発生し、すべて同じ内部IPアドレスが関係していることに気付きました。

1. このインシデントの処理に優先順位をつけるには、どのような要因を使用すべきでしょうか(共有されているファイルの内容など)。
2. どのようなプライバシーへの配慮が、このインシデントの処理に影響を与える可能性がありますか?
3. ピアツーピアのファイル共有を実行するコンピュータにも機密性の高い個人情報が含まれている場合、このインシデントの処理はどのように異なるでしょうか?

シナリオ１１：不明な無線アクセスポイント

月曜日の朝、組織のヘルプデスクは、ビルの同じフロアにいる3人のユーザーから、無線アクセスに問題があるとの電話を受けました。問題解決の支援を依頼されたネットワーク管理者は、無線アクセスが可能なノートパソコンをユーザーのフロアに持ってきました。無線ネットワークの設定を見ていると、新しいアクセスポイントが利用可能であることに気付きます。チームメイトに確認したところ、このアクセスポイントは自分のチームでは配備されていないため、許可なく設置された不正なアクセスポイントである可能性が高いと判断しました。

1. このインシデントに対処するための最初の主要なステップは何でしょうか（不正アクセスポイントを物理的に見つける、アクセスポイントに論理的に接続するなど）？
2. アクセスポイントを見つける最も早い方法は何ですか? アクセス・ポイントの場所を特定する最も内密な方法は何ですか?
3. アクセスポイントが外部の関係者（契約者など）によって一時的に組織のオフィスに配置されていた場合、このインシデントの処理はどのように異なるでしょうか？

4. 侵入検知アナリストが、ビルの同じフロアにあるいくつかのワークステーションに関係する不審な活動の兆候を報告した場合、このインシデントの処理はどのように異なるでしょうか?
5. チームがまだ物理的にアクセスポイントの位置を特定しようとしている間に、アクセスポイントが取り外されていた場合、このインシデントの処理はどのように異なるでしょうか?

付録B インシデント関連データ要素

組織は、各インシデントについて収集すべきインシデント関連のデータ要素の標準的なセットを特定すべきです。この取り組みは、より効果的で一貫性のあるインシデント処理を促進するだけでなく、適用されるインシデント報告の要件を満たすために組織を支援することにもなります。組織は、インシデントが報告されたときに収集される基本的な要素（例えば、インシデント報告者の名前、 電話番号、および場所）のセットと、インシデント対応者が対応中に収集する追加の要素のセットを指定すべきです。2つの要素のセットは、前にセクション3.2.5で議論したインシデント報告データベースの基礎となります。以下のリストは、インシデントに対して収集すべき情報の提案であり、包括的なものではありません。各組織は、そのインシデント対応チームのモデルと構造、および "インシデント "という用語の定義を含むいくつかの要因に基づいて、独自のデータ要素リストを作成するべきです。

B.1 基本データ要素

■ インシデントレポーター・ハンドラーの連絡先
– 名 前
– 役 割
– 組織単位（例：代理店、部署、部署、チーム）と所属
– メールアドレス
– 電話番号
– 所在地（住所、事務所の部屋番号など）

■ インシデントの詳細
– 状態変化の日付/タイムスタンプ（タイムゾーンを含む）：インシデントが開始されたとき、インシデントが発見/検出されたとき、インシデントが報告されたとき、インシデントが解決/終了したとき、など
– インシデントの物理的な場所（例：市、州）
– インシデントの現在の状況（進行中の攻撃など）
– ホスト名とIPアドレスを含む、インシデントの発生源/原因(既知の場合)
– インシデントの説明（例：どのようにして検出されたか、何が起こったか）
– システムのホスト名、IP アドレス、機能を含む、影響を受けるリソース（ネットワーク、ホスト、アプリケーション、データなど）の説明
– 既知の場合は、インシデントのカテゴリー、インシデントに関連する攻撃のベクトル、およびインシデントに関連する指標（トラフィックパターン、レジストリキーなど
– 優先順位付けの要因（機能的な影響、情報への影響、復旧可能性など）
– 緩和要因（例：機密データを含む盗まれたノートパソコンが完全なディスク暗号化を使用していたなど）
– 実行されたレスポンスアクション（例：ホストのシャットオフ、ネットワークからのホストの切断）
– 連絡を取った他の組織（例：ソフトウェアベンダー）

■ General Comments 総評

B.2 インシデントハンドラのデータ要素

■ インシデント対応の現状
■ インシデントの概要
■ インシデント対応アクション
– すべてのハンドラーが実行したアクションのログ
– 関係者の連絡先
– 集められた証拠の一覧 ■ インシデントハンドラのコメント
■ インシデントの原因（アプリケーションの設定ミス、パッチが適用されていないホストなど）
■ インシデントの費用
■ インシデントのビジネスへの影響※

※ インシデントのビジネスへの影響は、インシデントの影響の説明（例えば、会計部門が2日間タスクを実行できないなど）か、コストに基づく影響のカテゴリー（例えば、「重大な」インシデントは10万ドル以上のコストがかかるなど）のいずれかである可能性があります。

付録C 用語集

本資料で使用されている用語は以下の通りです。

バーゼルニング
リソースを監視して典型的な利用パターンを判断し、重大な逸脱を検出できるようにすること。

コンピュータセキュリティインシデント
「インシデント」を参照

コンピュータセキュリティインシデントレスポンスチーム（CSIRT）
コンピュータセキュリティ関連のインシデントへの対応を支援する目的で設置された機能。コンピュータインシデントレスポンスチーム（CIRT）またはCIRC（コンピュータインシデントレスポンスセンター、コンピュータインシデント対応能力）とも呼ばれる。

イベント
ネットワークまたはシステムで観察可能なあらゆる出来事

偽陽性
悪意のあるアクティビティが発生していることを誤って示すアラート

インシデント
コンピュータ セキュリティ ポリシー、許容される使用ポリシー、または標準的なセキュリティ慣行に対する違反による差し迫った脅威。

インシデントハンドリング
セキュリティポリシーおよび推奨されるプラクティスの違反を緩和すること。

インシデント対応
「インシデントハンドリング」参照

インジケータ（兆候）
インシデントが発生した可能性がある、または現在発生している可能性があることを示す兆候。

侵入検知および侵入防止システム
コンピュータシステムまたはネットワークで発生しているイベントを監視し、インシデントの可能性のある兆候を分析し、検出されたインシデントを停止させようとするプロセスを自動化するソフトウェア。

マルウェア
ウイルス、ワーム、トロイの木馬、またはその他のコードベースの悪意のある存在で、ホストに感染することに成功したもの。

前　兆 攻撃者がインシデントを引き起こす準備をしている可能性のある兆候。

プロファイリング
予想される活動の特性を測定して、活動の変化をより容易に特定できるようにすること。

シグネチャ
ウィルスのバイナリ文字列や、システムへの不正アクセスに使用される特定のキーストロークなど、攻撃に関連した認識可能で識別可能なパターン。

ソーシャルエンジニアリング
システムやネットワークを攻撃するために使用できる情報（パスワードなど）を明らかにしようと誰かを騙そうとする試み。

脅　威
不利な事象の潜在的な発生源。

脆弱性
システム、アプリケーション、またはネットワークの弱点で、悪用されたり悪用されたりする可能性があるもの。

付録D 頭字語（略語）集

この文書で使用されているいくつかの略語は、以下に定義されています。 **CCIPS**
Computer Crime and Intellectual Property Section
コンピュータ犯罪・知的財産部門

CERIAS
Center for Education and Research in Information Assurance and Security
情報セキュリティ教育研究センター

CERT®/CC CERT® Coordination Center
CERT®コーディネーションセンター

CIO
Chief Information Officer
最高情報責任者

CIRC
Computer Incident Response Capability
コンピュータインシデント対応能力

CIRC
Computer Incident Response Center
コンピュータインシデント対応センター

CIRT
Computer Incident Response Team
コンピュータインシデント対応チーム

CISO
Chief Information Security Officer
最高情報セキュリティ責任者

CSIRC
Computer Security Incident Response Capability
コンピュータセキュリティインシデント対応能力

CSIRT
Computer Security Incident Response Team
コンピュータセキュリティインシデント対応チーム

DDoS
Distributed Denial of Service
分散型サービス拒否攻撃

DHS
Department of Homeland Security
国土安全保障省

DNS
Domain Name System
ドメインネームシステム

DoS
Denial of Service
サービス拒否攻撃

FAQ
Frequently Asked Questions
よくある質問

FBI
Federal Bureau of Investigation
連邦捜査局

FIPS
Federal Information Processing Standards
連邦情報処理規格

FIRST
Forum of Incident Response and Security Teams
インシデントレスポンス・セキュリティチームフォーラム※

FISMA
Federal Information Security Management Act
連邦情報セキュリティマネジメント法

GAO
General Accountability Office
米国会計検査院

GFIRST
Government Forum of Incident Response and Security Teams
インシデントレスポンス・セキュリティチーム政府フォーラム※

GRS
General Records Schedule
米国記録スケジュール　←要修正

HTTP
HyperText Transfer Protocol
ハイパーテキストトランスファープロトコル

IANA
Internet Assigned Numbers Authority
インターネット割当番号公社

IDPS
Intrusion Detection and Prevention System
侵入検知・防止システム

IETF
Internet Engineering Task Force
インターネット技術特別調査委員会

IP
Internet Protocol
インターネットプロトコル

IR
Interagency Report
内部機関報告書

IRC
Internet Relay Chat
インターネットリレーチャット

ISAC Information Sharing and Analysis Center
セキュリティ情報共有組織

ISP Internet Service Provider
インターネットサービスプロバイダ

IT
Information Technology
情報技術

ITL
Information Technology Laboratory
情報技術研究所

MAC
Media Access Control
媒体アクセス制御

MOU
Memorandum of Understanding
基本合意書、了解覚書

MSSP
Managed Security Services Provider
マネージドセキュリティサービスプロバイダ

NAT
Network Address Translation
ネットワークアドレス変換

NDA
Non-Disclosure Agreement
秘密保持契約、秘密保持契約書

NIST
National Institute of Standards and Technology
アメリカ国立標準技術研究所

NSRL
National Software Reference Library
ナショナルソフトウェアリファレンスライブラリ
NISTのプロジェクトで、法執行機関やコンピュータ・フォレンジック調査に関与する他の組織が使用する既知のソフトウェア、ファイルプロファイル、ファイル署名のリポジトリを維持・提供している。

NTP
Network Time Protocol
ネットワークタイムプロトコル

NVD
National Vulnerability Database
脆弱性情報データベース

OIG
Office of Inspector General

監察総監室 OIG は、全米の事業所における監査・調査・評価を通して、事業とマネジメントの問題点を長官及び議会の両方に対して報告し、改善を勧告している。

OMB
Office of Management and Budget
アメリカ合衆国行政管理予算局

OS
Operating System
オペレーティングシステム

PII
Personally Identifiable Information
個人情報、個人を特定できる情報

PIN
Personal Identification Number 個人識別番号

※和名不明

付録E 情報源

以下のリストは、インシデント対応能力の確立と維持に役立つ情報源の一例です。

インシデント対応組織

組　織	URL
Anti-Phishing Working Group (APWG) フィッシング対策実務者グループ	http://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice アメリカ合衆国司法省コンピュータ犯罪および知的財産担当課	http://www.cybercrime.gov/
CERT® Coordination Center, Carnegie Mellon University (CERT®/CC) カーネギーメロン大学CERT®コーディネーションセンター	http://www.cert.org/
European Network and Information Security Agency (ENISA) 欧州ネットワーク・情報セキュリティ機関	http://www.enisa.europa.eu/activities/cert
Forum of Incident Response and Security Teams (FIRST) インシデントレスポンス・セキュリティチームフォーラム※	http://www.first.org/
Government Forum of Incident Response and Security Teams (GFIRST) インシデントレスポンス・セキュリティチーム政府フォーラム※	http://www.us-cert.gov/federal/gfirst.html

組　織	URL
High Technology Crime Investigation Association (HTCIA) ハイテクノロジー犯罪捜査協会※	http://www.htcia.org/
InfraGard インフラガード※	http://www.infragard.net/
Internet Storm Center (ISC) インターネットストームセンター※	http://isc.sans.edu/
National Council of ISACs ※	http://www.isaccouncil.org/
United States Computer Emergency Response Team (US-CERT) 米コンピュータ緊急事態対策チーム	http://www.us-cert.gov/

※和名不明

NIST出版物

情報源名	URL
NIST SP 800-53 Revision 3, 連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策	http://csrc.nist.gov/publications/PubsSPs.html#800-53
NIST SP 800-83, マルウェアによるインシデントの防止と対応のためのガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-83
NIST SP 800-84,IT計画およびIT対応能力のためのテスト、トレーニング、演習プログラムのガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-84
NIST SP 800-86,媒体のサニタイズに関するガイドライン	http://csrc.nist.gov/publications/PubsSPs.html#800-86
NIST SP 800-92, コンピュータセキュリティログ管理ガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-92
NIST SP 800-94, 侵入検知および侵入防止システム（IDPS）に関するガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-94
NIST SP 800-115, 情報セキュリティのテスト・評価のための技術的ガイド※	http://csrc.nist.gov/publications/PubsSPs.html#800-115
NIST SP 800-128,情報システムにおけるセキュリティを焦点とした設定・管理ガイド※	http://csrc.nist.gov/publications/PubsSPs.html#800-128

※筆者訳　他はIPAによる

インシデントハンドリングに適用されるデータ交換仕様

題名	説明	追加情報
AI	Asset Identification 資産の特定※	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7693
ARF	Asset Results Format 資産結果のフォーマット※	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7694
CAPEC	Common Attack Pattern Enumeration and Classification 共通攻撃パターン一覧	http://capec.mitre.org/
CCE	Common Configuration Enumeration 共通セキュリティ設定一覧	http://cce.mitre.org/
CEE	Common Event Expression 共通イベント記述	http://cee.mitre.org/
CPE	Common Platform Enumeration 共通プラットフォーム一覧	http://cpe.mitre.org/
CVE	Common Vulnerabilities and Exposures 共通脆弱性識別子	http://cve.mitre.org/
CVSS	Common Vulnerability Scoring System 共通脆弱性評価システム	http://www.first.org/cvss/cvss-guide
CWE	Common Weakness Enumeration 共通脆弱性タイプ一覧	http://cwe.mitre.org/
CybOX	Cyber Observable eXpression サイバー攻撃観測記述形式	http://cybox.mitre.org/
MAEC	Malware Attribute Enumeration and Characterization マルウェア特徴属性一覧	http://maec.mitre.org/
OCIL	Open Checklist Interactive Language 対話型チェックリスト記述言語	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7692
OVAL	Open Vulnerability Assessment Language セキュリティ検査言語	http://oval.mitre.org/
RFC 4765	Intrusion Detection Message Exchange Format (IDMEF) 侵入検知メッセージ交換フォーマット	http://www.ietf.org/rfc/rfc4765.txt

題 名	説 明	追加情報
RFC 5070	Incident Object Description Exchange Format (IODEF) インシデントオブジェクト記述法と交換フォーマット	http://www.ietf.org/rfc/rfc5070.txt
RFC 5901	Extensions to the IODEF for Reporting Phishing フィッシング報告用のIODEF文書クラス拡張	http://www.ietf.org/rfc/rfc5901.txt
RFC 5941	Sharing Transaction Fraud Data 取引詐欺のデータの共有	http://www.ietf.org/rfc/rfc5941.txt
RFC 6545	Real-time Inter-network Defense (RID)	http://www.ietf.org/rfc/rfc6545.txt
RFC 6546	Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS リアルタイムのネットワーク間防衛の交通HTTP / TLS経由（RID）のメッセージ	http://www.ietf.org/rfc/rfc6546.txt
SCAP	Security Content Automation Protocol セキュリティ設定共通化手順	http://csrc.nist.gov/publications/PubsSPs.html#SP-800126-Rev.%202
XCCDF	Extensible Configuration Checklist Description Format セキュリティ設定チェックリスト記述形式	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7275-r4

付録F よくある質問

組織内のユーザ、システム管理者、情報セキュリティ担当者などから、インシデント対応に関する質問を受けることがあります。以下は、よくある質問（FAQ）です。組織は、この FAQ をカスタマイズしてユーザーコミュニティで利用できるようにすることをお勧めします。

1. インシデントとは何ですか？ 一般的に、インシデントとは、コンピュータセキュリティポリシー、許容される使用ポリシー、または標準的なコンピュータセキュリティ慣行の違反のことです。インシデントの例としては、以下のようなものがあります。
■ 攻撃者がボットネットに命じて、組織の Web サーバーに大量の接続要求を送信し、クラッシュさせる。
■ ユーザが騙されて電子メールで送られてくる「四半期報告書」を開くと、実際にはマルウェアであり、ツールを実行することでコンピュータが感染し、外部ホストとの接続が確立されてしまう。 ■ 加害者が機密データへの不正アクセスを取得し、組織が指定された金額を支払わない場合は、詳細を報道機関に公開すると脅迫する。 ■ ユーザーが、ピアツーピアのファイル共有サービスを通じて、ソフトウェアの違法コピーを他人に提供する。

2. インシデントハンドリングとは？
インシデントハンドリングとは、インシデントを検知・分析し、インシデントの影響を限定するプロセスのことです。例えば、攻撃者がインターネットを介してシステムに侵入した場合、インシデントハンドリングプロセスはセキュリティ侵害を検知する必要があります。その後、インシデントハンドラーはデータを分析し、攻撃がどの程度深刻なものかを判断します。インシデントハンドラーは、インシデントに優先順位をつけ、インシデントの進行を食い止め、影響を受けたシステムが一刻も早く通常の動作に戻るように行動します。

3. インシデント対応とは何ですか？
「インシデントハンドリング」と「インシデントレスポンス」という用語は、本書では同義語です※。
※ 「インシデントハンドリング」と「インシデントレスポンス」の定義は、大きく異なる。例えば、CERT®/CC は、「インシデントハンドリング」を、インシデントの検出、報告、分析、および対応の全体的なプロセスを指すために使用しているのに対し、「インシデントレスポンス」は、具体的にインシデントの封じ込め、回復、および他者への通知を指しています。詳細については、http://www.cert.org/csirts/csirt_faq.html を参照してください。

4. インシデント対応チームとは何ですか？
インシデント対応チーム（Computer Security Incident Response Team [CSIRT]とも呼ばれる）は、組織の一部または全部にインシデント対応サービスを提供する役割を担っています。チームは、起こりうるインシデントに関する情報を受け取り、それを調査し、インシデントによる被害を最小限に抑えるための対策を講じます。

5. インシデント対応チームはどのようなサービスを提供しているのですか？
インシデント対応チームが提供する特定のサービスは、組織によって大きく異なります。ほとんどのチームは、インシデント対応を行うことに加えて、侵入検知システムの監視と管理の責任を負います。また、チームは、新しい脅威に関するアドバイスを配布したり、インシデントの予防と処理における役割についてユーザーやITスタッフを教育したりすることもあります。

6. インシデントは誰に報告すべきですか？
組織は、内部的にインシデントを報告するための明確な接点（POC）を確立すべきです。組織によっては、すべてのインシデントがインシデント対応チームに直接報告されるように、インシデント対応能力を構築する場合もあれば、IT ヘルプデスクなどの既存のサポート体制を初期のPOCに使用する場合もあります。組織は、他のインシデント対応チームなどの外部関係者が、一部のインシデントを報告することを認識すべきです。連邦政府機関は、法律に基づき、すべてのインシデントを米国コンピュータ緊急事態対応チーム（US-CERT）に報告することを義務付けられています。すべての組織は、適切なコンピュータ・セキュリティ・インシデント対応チーム（CSIRT）にインシデントを報告することが推奨されています。組織に連絡先となる CSIRT がない場合は、情報共有・分析センター（ISAC）などの他の組織にインシデントを報告することができます。

7. インシデントはどのように報告されますか？
ほとんどの組織では、インシデントを報告するための複数の方法があります。 活動を報告する人のスキル、インシデントの緊急性、およびインシデントの感度の違いにより、適切な報告方法が変わる場合があります。緊急事態を報告するための電話番号を設けるべきです。電子メール・アドレスは、非公式のインシデント報告に使用される可能性ありますが、正式なインシデント報告にはウェブベースのフォームが適切な場合があります 機密情報は、チームが公開した公開鍵を使用して資料を暗号化することで、チームに提供することができます。

8. インシデントを報告する際には、どのような情報を提供すべきでしょうか？ 情報は正確であればあるほど良いです。例えば、ワークステーションがマルウェアに感染しているように見える場合、インシデントレポートには、以下のデータをできるだけ多く含める必要があります。 ■ ユーザーの名前、ユーザーID、および連絡先情報（電話番号、電子メール アドレスなど ■ ワークステーションの場所、モデル番号、シリアル番号、ホスト名、および IP アドレス
■ インシデントが発生した日時 ■ 感染が発見された後にワークステーションに何が行われたかなど、何が起こったのかを段階的に説明します。 この説明は、マルウェアやウイルス対策ソフトの警告などのメッセージの正確な文言を含めて詳細に行う必要があります。

9. インシデント対応チームは、インシデント報告にどのくらいの早さで対応しますか？ 応答時間は、インシデントの種類、影響を受けるリソースとデータの重要度、インシデントの深刻度、影響を受けるリソースに対する既存のサービスレベル契約（SLA）、時間と曜日、チームが処理している他のインシデントなど、いくつかの要因に依存します。一般的に、組織または他の組織に最も大きな被害をもたらす可能性の高いインシデントを処理することが最優先されます。

10. インシデントに関与している人は、いつ法執行機関に連絡すべきか？ 法執行機関との連絡は、インシデント対応チームのメンバー、最高情報責任者（CIO）、またはその他の指定された関係者によって開始されるべきであり、ユーザー、システム管理者、システム所有者、およびその他の関係者は、連絡を開始すべきではありません。

11. システムが攻撃されていることを知った人はどうすればいいですか？ 直ちにシステムの使用を停止し、インシデント対応チームに連絡しなければなりません。また、発見した人物は、インシデントの初期処理を支援する必要があるかもしれません。例えば、インシデント・ハンドラーが到着するまでの間、システム上の証拠を保護するためにシステムを物理的に監視するなどです。

12. インシデントに関してメディアから連絡を受けた人は、何をすべきですか？ ある人物は、インシデントと外部関係者に関する組織の方針に従って、メディアの質問に答えることができます。また、その人が組織を代表してインシデントを語る資格がない場合には、その人はインシデントに関するコメントをしてはならず、通報者を組織の広報室に紹介する以外は、インシデントに関するコメントをしてはなりません。これにより、広報室はメディアや一般市民に正確で一貫性のある情報を提供することができます。

付録G 危機対応のステップ

これは技術専門家が重大なインシデントが発生し、組織にインシデント対応能力がないと考えた場合に実行すべき主な手順のリストです。これは危機に直面したときに、この文書全体を読み通す時間がない人のために何をすべきかの基本的な参考資料としての役割を果たします。

1. **すべてを文書化する。**
   この取り組みには、実行されたすべてのアクション、すべての証拠の断片、ユーザー、システム所有者、およびインシデントに関するその他の人とのすべての会話が含まれます。

2. **援助してくれる同僚を見つける。**
   例えば、一人が行動を行い、もう一人がそれを文書化するなどです。

3. **証拠を分析して、インシデントが発生したことを確認する。**
   必要に応じて、証拠をよりよく理解するために追加の調査(インターネットの検索エンジン、ソフ トウェアの文書など)を行います。組織内の他の技術専門家に連絡を取り、追加の支援を求めます。

4. **組織内の適切な担当者に通知する。**
   これには最高情報責任者（CIO）、情報セキュリティ責任者、現地のセキュリ ティ管理者が含まれるべきです。インシデントの詳細を他の人に話す場合は慎重に行い、知る必要のある人だけに伝え、合理的に安全なコミュニケーションメカニズムを使用します(攻撃者が電子メールサービスに侵入した場合は、インシデントに関する電子メールを送信しないこと)
   。

5. **US-CERT および/またはその他の外部組織に通知**し、インシデントへの対応を支援してもらう。

6. **インシデントがまだ進行中の場合はインシデントを停止する。**
   最も一般的な方法は、影響を受けたシステムをネットワークから切断することです。場合によっては、サービス拒否（DoS）攻撃など、インシデントの一部であるネットワークトラフィックを停止するために、 ファイアウォールおよびルーターの構成を変更する必要があります。

7. **インシデントの証拠を保存する。**
   影響を受けたシステムのバックアップ（ファイルシステムのバックアップではなく、ディスクイメージのバックアップが望ましい）を作成します。インシデントに関連する証拠を含むログファイルのコピーを作成します。

8. **インシデントのすべての影響を一掃する。**
   この作業には、マルウェア感染、不適切な素材（海賊版ソフトウェアなど）、トロイの木馬ファイル、およびインシデントによってシステムに加えられたその他の変更が含まれます。システムが完全に侵害されている場合は、ゼロからシステムを再構築するか、既知の良好なバックアップから復元します。

9. **悪用されたすべての脆弱性を特定し緩和する。**
   インシデントは、オペレーティングシステムやアプリケーションの脆弱性を利用して発生した可能性があります。そのような脆弱性を特定し、インシデントが再発しないように排除するか、または緩和することが重要です。

10. **操作が正常に復旧したことを確認する。**
    インシデントの影響を受けたデータ、アプリケーション、およびその他のサービスが通常の運用に戻ったことを確認してください。

11. **最終報告書を作成する。**
    この報告書には、インシデント処理プロセスの詳細を記載する必要があります。また、何が起こったのか、正式なインシデント対応能力があれば、どのように状況を処理し、リスクを軽減し、被害をより迅速に限定できたのかについての要約を提供する必要があります。