組織対応力ベンチマーク解説書

一般社団法人オープンガバメント・コンソーシアム
Open Government Consortium （略称：OGC）

目次

1. 本書の概要

1.1. 背景

来る 2020 年東京オリンピック・パラリンピックの開催に向け、サイバー攻撃への対応能力を強化するための方策が急務となっている。サイバー攻撃への対応能力については、個々の企業体の能力強化のみならず、サプライチェーンを構成する企業群全体としての能力強化も重要な課題である。例えば、重要インフラ企業及び関連する企業（以下：サプライチェーン企業）によって構成される企業群が提供する重要インフラ機能に対するサイバー攻撃を想定した場合、重要インフラ企業に比してサプライチェーン企業の対応能力の脆弱性が課題となっており、この脆弱性が重要インフラ機能のセキュリティホールになりかねない状況である。このため、企業群全体としての早急な対応力強化が必要と考えられる。

サイバー攻撃への対応能力を強化するための重要な要素として、組織のセキュリティインシデント対応能力の強化が挙げられる。セキュリティインシデント対応については、これを専任とする Computer Security Incident Response Team（以下、CSIRT という）を組織化する場合があるが、CSIRT に代表されるインシデントレスポンス対応組織の設立、及び有効な運営は重要なポイントであり、これを支援する施策が必要である。「組織対応力ベンチマーク」はこの施策の一環であり、組織のセキュリティインシデント対応能力の現状を評価するとともに、対策立案のための指針を提供することを目的としている。

1.2. 組織対応力ベンチマークについて

「組織対応力ベンチマーク」は、2014 年 4 月にセキュリティベンダを主として結成された連合体（以下、コンソーシアム）によって提言された施策ツールである。一般社団法人オープンガバメント・コンソーシアムが、組織の情報セキュリティインシデント対策の実施状況を診断するツールとして開発を進め、2015 年 7 月より Web 上で提供している。

「組織対応力ベンチマーク」は、情報セキュリティインシデントに対応するための組織能力を評価することを目的として、米国国立標準技術研究所（National Institute of Standards and Technology）（以下、「NIST」という） が公表している Special Publication 800-61 「コンピュータセキュリティインシデント対応ガイド」（Revision 1）を参考にしている。「コンピュータセキュリティインシデント対応ガイド」（以下、「NIST SP800-61」という）は、情報セキュリティインシデントに効果的かつ効率的に対応するための実用的な手引きとなることで、各組織が情報セキュリティインシデントによるリスクを軽減するのに役立てることを意図したものであり、効果的なインシデント対応プログラムの策定に関するガイドラインを含んでいる。「NIST SP800-61」は、独立行政法人情報処理推進機構（以下、「IPA」という）が翻訳編集し、ホームページ上で公開している。「組織対応力ベンチマーク」は、この IPA による公開資料を基に作成されている。

「組織対応力ベンチマーク」は、情報セキュリティインシデント対策の計画段階におい

ても、運用段階においても、組織の情報セキュリティインシデント対策を向上させるために使うことができる。「組織対応力ベンチマーク」は、対象とする組織全体のセキュリティインシデント対応力を評価しようとするものであるが、CSIRT を組織化している企業の場合には、CSIRT の対応力を評価することにも使用することができる。

「組織対応力ベンチマーク」は、セキュリティインシデントに対応するための基礎的要素が網羅的に実施されているかを評価しようとするものである。このため、中小企業や大企業といった組織の大小を問わず利用することができる。

1.3. 対象とする読者と本書の目的

本書は、組織内においてセキュリティインシデントへの対応を担い、組織対応力ベンチマークを利用して評価を実施する方々を対象として書かれている。本書で想定している主な対象者は、具体例としては以下の通りである。

- 最高情報責任者(CIO)、マネジメント層
- セキュリティインシデントに備えて対応する責任を持つ者
- CSIRT（コンピュータセキュリティインシデント対応チーム）
- システム管理者と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

本書は、組織対応力ベンチマークの使い方を指南するものである。このため、組織対応力ベンチマークの構成に沿って質問内容の解説を記載している。なお、組織対応力ベンチマークの利用者は、必ずしもコンピュータに精通していない場合がある。このような状況に鑑み、本書は、コンピュータに精通していない利用者にもわかりやすいよう、可能な限り平易かつ端的な表現による「組織対応力ベンチマーク」の解説を目的としている。

1.4. 本書の概要

組織の情報セキュリティインシデント対策は広範囲にわたり、その評価については専門的な知識や多くの手順が必要なことから、難しいというイメージがある。そこで、本書では、「組織対応力ベンチマーク」の設問項目の解説という視点から、情報セキュリティインシデント対策状況の評価について、具体的に、わかりやすい説明をこころがけた。

1 章では、本書の背景、対象とする読者および目的、および本書の概要について述べている。2 章では、情報セキュリティインシデント対策状況を評価する「組織対応力ベンチマーク」を利用するに際して、その質問構成、評価基準、および評価結果の利用方法ならびに留意点を説明する。3 章では、「組織対応力ベンチマーク」の各質問事項について、その背景や意義を解説している。

2. 組織対応力評価について

2.1. 組織対応力ベンチマークの構成

組織対応力ベンチマークは、6 分野の質問について計 25 問の設問から構成されている。6 分野の質問構成は、以下の通りである。

問 1．文書類の整備状況（4 設問）
問 2．インシデント対応チームの構成（3 設問）
問 3．インシデント対応の準備（4 設問）
問 4．予防（6 設問）
問 5．検知と分析（4 設問）
問 6．封じ込め・根絶・復旧および事後活動（4 設問）

2.2. 評価の実施方法

2.2.1. 評価方法

評価は、各設問に対して以下の選択肢の中からあてはまる回答番号を選択させる形式としている。

１．全くできていない。（設問事項がまったく満たされていない。）
２．内容に漏れがある。（設問事項が部分的に満たされている。）
３．概ねできている。（設問事項の全項目が満たされている。）
４．内容も十分なレベルである。（設問事項の全項目が満たされており、内容も十分なレベルに達している。）
５．定期的に見直しをしている。（設問事項の全項目が十分なレベルで満たされており、定期的な確認及び見直しをしている。）

各設問はいくつかの設問項目から構成されており、回答の観点はこの設問項目の達成度合いとなる。例えば、回答「２」または「３」に関して、「設問事項が満たされている」とは、各設問項目に対して何らかの検討が為されており、達成度合いが不十分であったとしても対応ができている状況を意味している。また、回答「４」または「５」に関して、「内容が十分なレベルに達している」とは、組織が直面する脅威の大きさや脆弱性対策への対応状況を鑑みて概ね十分と判断されている対応ができている場合を意味している。

2.2.2. 評価結果の利用に際して

組織対応力ベンチマークは、全ての組織のインシデント対応についての検討が、NIST SP800-61 に照らして網羅的に実施されることを目標として作成されている。このため、各

設問の回答が「３」の状態に到達しているかが評価の目安となる。回答「３」の状態とは、各設問の設問項目についてすべて検討がなされている状態であり、内容に不足はあるもののインシデント対応の必要事項について漏れなく考慮されている状態である。このため評価結果「２」の場合には、漏れのある事項について速やかに検討を開始することを推奨する。

回答「４」の状態とは、設問項目の実施内容についても十分なレベルに達しており、インシデント対応が概ね良好である状態である。このため評価結果「３」の場合には、実施内容が十分でない項目についての施策の再検討が必要となる。実施内容については、組織が直面しているリスクの大小等により達成レベルが異なるため、評価の際には注意が必要である。

回答「５」の状態とは、回答「４」の状態に加え、定期的に内容の評価や見直しを実施するいわゆる PDCA サイクルが実行されている状態である。

なお、全ての設問項目について回答「３」の状態を実現することが、重要インフラ企業及び関連する企業（以下：サプライチェーン企業）によって構成される企業群が目指すべきセキュリティインシデント対応の一旦の目標となるが、当該企業群にとってより重要性が高い項目や、より重要性が高い企業群については、回答「４」または「５」を目指すことが望ましい。

2.3. 評価結果の利用方法と留意点

組織対応力ベンチマークは、自組織のインシデント対応状況の評価の他に、サプライチェーン企業のインシデント対応状況の評価に用いることができる。組織対応力ベンチマークを複数企業で共有することにより、インシデント対応状況の比較評価が容易になるという利点がある。

3. 組織対応力ベンチマーク解説

3.1. 文書類の整備状況

3.1.1. インシデント対応ポリシー

① マネジメント層の責任表明を含む「インシデント対応ポリシー」を策定し、組織全体に周知徹底していますか？

以下の要素を含む、インシデント対応ポリシーを作成していますか？

- □ マネジメント層の責任表明。（1-1-1）
- □ ポリシーの目的と目標。（1-1-2）
- □ ポリシーの範囲。（1-1-3）
- □ インシデントの定義※注)と、それらのインシデントが自組織にもたらす影響（1-1-4）
- □ インシデント対応チームの組織構造と、役割、責任、権限レベルを表す記述。（1-1-5）
- □ インシデントの優先順位付けまたは重大さの格付け。（1-1-6）
- □ インシデント対応についての事後評価の方法。 （1-1-7）
- □ 報告および連絡のための必要事項の明確化。（1-1-8）

※注）インシデントの定義：どのような事象をもって「コンピュータセキュリティインシデント」とするかを定義付けすること。本書におけるインシデントの単語自体の意味は、用語集を参照のこと。

インシデント対応を左右するポリシーは、組織ごとに異なったものになる。ただし、組織がインシデント対応能力を自前で用意するか外部委託するかにかかわらず、ほとんどのポリシーの基本要素は同一である。

本設問では、インシデント対応についてマネジメント層が責任表明をすべき事項がポリシーとして文書化され、組織全体に周知徹底されているかを確認する。

解説

□ マネジメント層の責任表明。[2)]

インシデント対応は、マネジメント層（代表取締役、取締役、役員等）が適法性・適正性のいずれの観点からも責任を持って取り組まなければならない、リスク管理活動の重要な要素である。すなわち、マネジメント層は、自らの経営課題の一つとして、情報資産に係る機密性、完全性、可用性の観点からのインシデント対応を捉え直すことが重要であり、情報資産に係るリスクの管理を狙いとして、インシデント対応に関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み（マネジメント層が方針を決定し、組織内の状況をモニタリングする仕組み及び関係者に対する開示と関係者による評価の仕組み等）を構築・運用する責任がある。このため、インシデント対応ポリシーには、マネジメント層の責任表明が不可欠である。マネジメント層の責任表明においては、特定

部署のミッションとしてではなく、代表者自らが組織全体としてインシデント対応に取り組むことを明示することが重要である。

解説

□　ポリシーの目的と目標。

インシデント対応ポリシーの目的としては、以下が挙げられる。

- 体系的にインシデントに対応する仕組みの構築
- 組織内の状況をモニタリングする仕組みの構築
- 利害関係者に対する適切な情報の開示
- 利害関係者による評価の仕組みの構築

インシデント対応ポリシーの目標としては、上記の目的の達成の他に、インシデントが発生した際における SLA（合意されたサービスレベル）の順守が含まれる。また、ポリシー自体が継続的に実行され、必要に応じて見直されることも目標に含まれる。

解説

□　ポリシーの範囲。

インシデント対応ポリシーの範囲には、対象となる人員、設備、どのような状況で適用されるかについて、等が含まれる。ポリシーの適用範囲は、マネジメント層の責任の及ぶ範囲であり、個別組織（企業）の範囲を超えない場合が多い。一方で、インシデント対応が連結企業集団、さらにバリューチェーンを形成する企業集団に及ぶ場合も有り得る。前者の場合には、適用範囲に相応しいマネジメントである必要があり、例えば、連結親会社社長をマネジメント層とするポリシーを策定する必要がある。後者の場合には、例えば、協力会社に対して「要請していく」あるいは「（取引条件として）義務付ける」といった適用の程度を考慮する必要がある。

解説

□　インシデントの定義と、それらのインシデントが自組織にもたらす影響。[3)]

どのような事象をインシデントと判断するかについての定義付けを行い、定義付けたインシデントが自組織にもたらす影響を分析し、文書化する必要がある。以下にインシデントの例を示す。

- サービス不能攻撃によるサービス拒否（DOS）
- 悪意のコードによるシステムハードウェア、ソフトウェア、データへの不正な変更（ウイルス、ワーム、トロイの木馬に挙げられるような悪意のあるプログラムによるもの）
- システムまたはデータへの不正アクセス
- 情報資産の不適切な使用
- 上記インシデントの複合

これらについて、対象となる情報資産や情報システムを考慮したうえでの自組織への影響度合いを評価し、文書化する。この評価は、後述する「インシデントの優先順位付けまたは重大さの格付け」の根拠となるものであり、この目的に則した粒度および詳細度で評価を行う。

解説

□　インシデント対応チームの組織構造と、役割、責任、権限レベルを表す記述。

インシデント対応チームを組織化し、自組織におけるインシデント対応チームの位置付けと役割を明らかにする。また、インシデント対応チームの責任を明示し、インシデント対応チームが装置を確保したり、または接続を切断したり、疑いのある活動を監視したりする権限を明示する。事象発生時において、チームのみの判断でシステムの停止や回線のシャットダウンをできないと封じ込めができないため、権限レベルの記述は重要となる。また、インシデントに発展した場合にマネジメント層へ報告する義務等も含める必要がある。

解説

□　インシデントの優先順位付けまたは重大さの格付け。

定義付けを行ったインシデントについて、自組織の活動を踏まえたうえでインシデントの重大さの格付けを行い、対応する際における優先順位付け、あるいは優先順位付けを実施する際の考え方を記載する。

解説

□　インシデント対応についての事後評価の方法。

インシデント対応についての事後評価の方法として、実施の時期、評価結果の報告対象、等を記載する。

解説

□　報告および連絡のための必要事項の明確化。

インシデント対応についての報告および連絡のための必要事項について記載する。

3.1.2. インシデント対応計画

② インシデント対応にかかわる組織の役割や目標を明記した「インシデント対応計画」を策定し、インシデント対応機能の確立を推進していますか？

以下の要素を含む、インシデント対応計画を作成していますか？

- □ インシデント対応チーム※注) の役割。(1-2-1)
- □ 戦略および目標。(短期および長期の目標) (1-2-2)
- □ マネジメント層による承認。(1-2-3)
- □ インシデント対応への組織的な取り組みの内容。(1-2-4)
- □ インシデント対応チームによる他の職員への連絡方法。(1-2-5)
- □ インシデント対応機能を評価するためのチェックリスト。(1-2-6)
- □ インシデント対応機能を向上させるための手引き。(トレーニングの実施等) (1-2-7)
- □ インシデント対応計画をどのようにして組織全体に適合させるかの方法。(1-2-8)

※注) インシデント対応チーム：インシデントへの対応を支援する目的で発足させた要員の集合体のこと。

組織にとって、インシデントに対応するための正式な機能を確立することは、重要である。この機能は、対象が絞られて明確になっており、組織内での調整がなされたものであるべきである。このような機能を効果的に活用するためには、インシデント対応計画の策定が必要になる。インシデント対応計画は、インシデント対応機能を有効活用するための手引きを提供し、インシデント対応機能を組織全体に効果的に適用するための高いレベルの手法を提供する。それぞれの組織は、自身のミッション、組織の規模、組織の構造、および組織の機能に見合った独自の要求事項を満たすための、計画を策定しなければならない。また、組織が作成し、マネジメント層の承認を得たインシデント対応計画は、定期的（少なくとも年に 1 回）に見直される必要がある。この見直しにより、組織は、インシデント対応機能の成熟を確実にし、インシデント対応に関する組織の目標を達成できるようになる。

本設問では、インシデント対応にかかわる組織の役割や目標について対応計画として文書化され、インシデント対応機能の確立がマネジメント層によって推進されているかを確認する。

解説

□ インシデント対応チームの役割。[4)]

インシデント対応チームの基本的な役割は、組織において発生したインシデントに対応することであるが、組織の事業内容、規模、部署構成、業務遂行形態、組織や事業に対する脅威及びリスクが異なるため、自組織の状況に合った役割を検討する必要がある。

【参考】

インシデント対応チームの基本的な役割の例を以下に示す。

(1) インシデント報告の受理

発生したインシデントについて、サービス対象（一般ユーザなど）からの報告を受理すること。インシデントに係る情報保全（デジタルフォレンジック）を行うこと。

(2) 外部組織との連携

外部のインシデント対応チーム等、外部組織がどのように対応するかを理解した上で、適切な依頼をすることができる関係を構築すること。

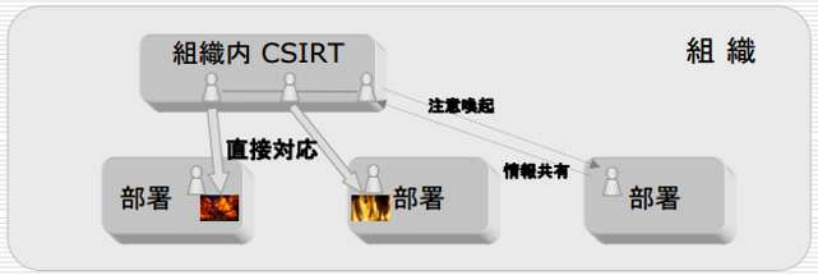
(3) インシデント関連情報の伝達経路の保全

インシデント関連情報のやり取りは、通常のインターネット回線を使用することが多いため、なりすまし、改ざん、或いは盗聴などがされないことを確保すること。

インシデントへの対応の役割については、組織の状況をもとに、マネジメント層やサービス対象からの期待によって定義される。以下にその例を示す。

(1) インシデントへの「直接」対応

組織において、各部署内でのインシデント対応能力が十分ではないので、インシデント対応チームが 主として／直接 インシデント対応する場合がある。この場合には、インシデント対応チームは、組織内のコンピュータシステム及びネットワークなどで発生するインシデントの被害を局限化し、迅速に復旧させる役割を担う。また、インシデントが早期に発見され、迅速に対応できる仕組み（各部署等との情報共有及び連携など）を整備及び維持する役割を担う。



（出典：組織内 CSIRT の役割とその範囲、JPCERT コーディネーションセンター）

(2) インシデントへの「支援的」対応

組織において、既に部署内で発生するインシデントへの対応能力はあるが、組織全体で（各部署を横断して）はインシデントの対応能力が十分ではないので、インシデント対応チームにその 発生したインシデント対応の支援及び調整 を期待する場合がある。この場合には、インシデント対応チームは、部署内で発生したインシデントへの（各部署等による）対応活動に対して、技術的支援及び組織内全体の調整及び統制等

をすることにより、迅速な被害の局限化及び迅速な復旧を支援する役割を担う。

（出典：組織内 CSIRT の役割とその範囲、JPCERT コーディネーションセンター）

(3) インシデントへの「調整役としての」対応

組織において、外的要因に基づくインシデント（DoS 攻撃、Phishing 詐欺等）に対する対応能力が十分でない場合は、インシデント対応チームにそのインシデントへの対応及び調整と、それに必要な組織内外への調整を依頼することがある。このような場合には、インシデント対応チームは、外的要因に基づくインシデントに対応する責任を持ち、外部のインシデント対応組織との連携及び組織内における必要な調整をすることにより、被害を局限化し、迅速な解決に努力する役割を担う。

（出典：組織内 CSIRT の役割とその範囲、JPCERT コーディネーションセンター）

解説

□　戦略および目標。（短期および長期の目標）

インシデント対応にかかわる組織のミッション、戦略および目標を明確にすることにより、インシデント対応機能の構造を決定しやすくなる。このような戦略および目標に関しては、インシデント対応計画の中で論じるべきである。

解説

□　マネジメント層による承認。

インシデント対応計画は、マネジメント層による承認が必要である。

解説

□　インシデント対応への組織的な取り組みの内容。

インシデント対応計画では、インシデント対応機能を効果的に維持・向上させるためのリソースおよびマネジメント層のサポートに関して、明確に記述しなければならない。

解説

□　インシデント対応チームによる他の職員への連絡方法。

インシデント対応計画には、組織内の他の職員への連絡方法を記載する。連絡については、それぞれ起票部署および提出先部署を明示する。また、連絡の種別に応じて書式を定めておくことが望ましい。

解説

□　インシデント対応機能を評価するためのチェックリスト。

インシデント対応計画には、対応機能を評価するためのチェックリストを記載する。

解説

□　インシデント対応機能を向上させるための手引き。（トレーニングの実施等）

インシデント対応計画には、トレーニングの実施等、対応機能を向上させるための手引きを記載する。この場合における「トレーニング」は、CSIRT チーム内のトレーニング、CSIRT と連携してインシデント対応に当る組織内の関係職員のトレーニング、および組織内全体の要員トレーニングの全てを対象とする必要がある。

解説

□　インシデント対応計画をどのようにして組織全体に適合させるかの方法。

インシデント対応計画には、組織全体に適合させるかの方法を記載する。例えば、組織のイントラネット上にインシデント対応計画を掲載するとともに定期的に閲覧を促す通知を出す、等の方法を検討し、その方法自体をインシデント対応計画に記載する。

3.1.3. インシデント対応手順

③ 「インシデント対応ポリシー」と「インシデント対応計画」に基づき「インシデント対応手順」を策定し、標準となる対応手順を関係組織に周知徹底していますか？

以下の要素を含む、インシデント対応手順※注) を作成していますか？

- □ 各手順は、インシデント対応ポリシーとインシデント対応計画を踏まえている。（1-3-1）
- □ 特定の技術手順、手法が記載されている。（1-3-2）
- □ インシデント対応についてのガイドライン※注) が記載されている。（1-3-3）
- □ チェックリストや確認のための様式が記述あるいは添付されている。（1-3-4）
- □ 組織の優先順位が反映された対応活動が記載されている。（1-3-5）
- □ テストを行い、正確さと有用性を検証した後、チームの全メンバーに配付されている。（1-3-6）

※注）インシデント対応手順：インシデント対応における標準運用手順(SOP: Standard Operating Procedures)のこと。特定の技術手順、手法、インシデント対応チェックリスト、フォームが記述されている。

※注）ガイドライン：組織の行動に具体的な方向性や縛りを与えるための規範（ルール等）や目標など。

インシデント対応を実施するに際しては、標準となる運用手順(SOP: Standard Operating Procedures)を作成し、平常時よりその組織にとっての標準的な対応手順を関係部署に周知しておくことが必要である。インシデント対応手順は主としてインシデント対応チームが使用するものであり、対応が標準化されていることで、誤り(特に事件処理のペースやストレスからくる誤り)を減らすことができる。

本設問では、インシデント対応にかかわる標準手順が文書化され、関係部署に周知徹底されているかを確認する。

解説

□ 各手順は、インシデント対応ポリシーとインシデント対応計画を踏まえている。

各手順は、インシデント対応ポリシーを踏まえ、迅速かつ効果的にインシデントを解決するために、組織風土に適合したグッドプラクティスとなっていることが必要である。また、インシデント対応計画に基づいた対応手順を詳細に記したものであり、属人的な要素を排除し、誰が実行しても同等の結果が得られるように標準化されたものでなければならない。

解説

□ 特定の技術手順、手法が記載されている。

□　インシデント対応についてのガイドラインが記載されている。
□　チェックリストや確認のための様式が記述あるいは添付されている。

各手順は、特定の技術手順や手法について、作業担当者のスキルレベルに寄らず同一の結果が得られる程度に詳細化されている必要がある。また、証拠保全の観点から時間の許す限り、手順に従った順序で実行することが強く推奨されるものである。また、守るのが好ましいとされる規範（ルール等）や目指すべき目標などを明文化し、組織の行動に具体的な方向性を与え、時には何らかの「縛り」を与えるものであることが必要である。

解説

□　組織の優先順位が反映された対応活動が記載されている。

複数のインシデントが同時に発生したような場合を想定して、組織の優先順位や事象の重大性を考慮した対応活動を行うためのルールが記載されていること。

解説

□　テストを行い、正確さと有用性を検証した後、チームの全メンバーに配付されている。

各手順は、テストを行い、正確さと有用性を検証した後、チームの全メンバーに配付する。各手順の利用者は、手順ドキュメントを教育ツールとして使用したトレーニングに参加すること。また、定期的にインシデント対応チーム全員参加によるリハーサルを実施し、実際のインシデント発生時にスムーズな対応ができるように日常的に訓練を実施すること。さらに、環境の変化や攻撃手法の変化によって、手順書は随時改善し続ける必要がある。そのプロセスを盛り込んでおくこと。

3.1.4. インシデント関連の情報共有に関するポリシーと手順

④ インシデント関連の情報共有に関するポリシーと手順を策定し、組織外に向けた情報提供について関係組織に周知徹底していますか？

以下の要素を考慮して、インシデント関連の情報共有に関するポリシーと手順を作成していますか？

- □ 記載内容についてマネジメント層と合意している。(1-4-1)
- □ 記載内容について組織の広報部門と合意している。(1-4-2)
- □ 記載内容について組織の法務部門と合意している。(1-4-3)
- □ （マスコミ等の外部関係者とやりとりする際に使用する）組織の現行ポリシーと手順に従っている。(1-4-4)

組織は、外部の関係者にインシデントについて連絡しなくてはならない場合がある。また、場合によっては、組織が他の関係者にも連絡することがある （たとえば、法執行機関への連絡、マスコミの問い合わせへの対応など)。インシデント処理担当者は、組織のインターネットサービスプロバイダ(ISP)、攻撃者が使用している ISP、脆弱性があるソフトウェアのベンダー、担当者が理解しようとしている異常な活動に詳しいインシデント対応チームなど、その他の関係者と事件について話し合わなくてはならない場合もある。さまざまな理由から、インシデントの詳細を外部の組織に連絡したい(または連絡しなくてはならない)ことがある。このような場合には、連絡対象ごとに開示可能範囲が定められている必要がある。

本設問では、インシデント関連の情報共有にかかわるポリシーと手順が文書化され、関係部署に周知徹底されているかを確認する。

解説

- □ 記載内容についてマネジメント層と合意している。
- □ 記載内容について組織の広報部門と合意している。
- □ 記載内容について組織の法務部門と合意している。

インシデント対応チームは、事件が起きる前に、組織の広報部、法務部、マネジメント層と連携し、情報共有に関するポリシーと手順の確立に関与しておく必要がある。インシデント対応の知見をもったメンバーが関与しない場合には、事件に関する機密情報が権限のない者に提供され、事件そのものよりも大きなダメージや経済的な損失が起こる可能性がある。また、インシデント対応チームは、責任の所在の明確化と証拠を残す目的で、外部関係者とのすべての連絡およびやりとりの内容を文書化するべきである。

【参考】

情報共有を行う必要が外部組織の候補を以下に示す。

(1) マスコミ

マスコミへの対応は、組織の広報部が窓口となる場合が多い。マスコミへの対応は、インシデント対応の重要な部分である。インシデント対応チームは、マスコミとのやりとりや情報の公開について、組織のポリシーに合った手順を確立しておく必要がある。

(2) 法執行機関

法執行機関への窓口は、マネジメント層あるいは法務部となる場合が多い。インシデント対応チームは、さまざまな法執行機関と関係を持ち、インシデントを報告する条件、その方法、どのような証拠を収集するか、それをどのように収集するかについて情報を共有しておくべきである。

(3) インシデント報告組織

インシデント報告組織への窓口は、インシデント対応チームとなる場合が多い。組織によっては、インシデントを報告するよう義務付けられている場合がある。

(4) その他の外部関係者

その他の外部関係者への窓口は、インシデント対応チームあるいは情報システム部となる場合が多い。

- 組織が加入する ISP
- 攻撃元アドレスの所有者
- ソフトウェアベンダー
- 他のインシデント対応チーム
- 影響を受ける外部関係者

解説

□ （マスコミ等の外部関係者とやりとりする際に使用する）組織の現行ポリシーと手順に従っている。

組織は、マスコミ等の外部関係者とやりとりする際のポリシーや手順を有している場合が多いため、インシデント関連の情報共有もこれらのポリシーや手順に従う必要がある。この手順には、対外発表前において、法務部あるいはマネジメント層のチェックを受ける仕組みが明記されている必要がある。対外発表においては、社会的不安を引き起こさないように、通常のプレスリリース以上に注意を払う必要がある。また、つかんでいる情報の確からしさに基づいて、インシデント発生原因や攻撃元情報の公開をどうするかについても指針を決めておくことが望ましい。発生してしまった事故は早期に終息させる必要があるが、その過程でいかに迅速かつ的確に対外的な情報発信を行ってきたかについては、事後においてマスコミや第三者機関によって評価されることに留意すべきである。

3.2. インシデント対応チームの構成

3.2.1. インシデント対応チームの構成検討

① インシデント対応チーム構成を検討する際に、適切なインシデント対応チームモデルを選択し、適切なスキルをもった人材要員を検討していますか？

以下の要素を考慮して、インシデント対応チームの構成を検討していますか？

- □ 組織の現状を踏まえたうえで、インシデント対応チームの組織体制を決定している。（2-1-1）
- □ 組織の要件や利用できるリソースに照らし、慎重に検討を行ったうえで、要員配置を行っている。（2-1-2）
- □ チームリーダーは、インシデント対応における組織内外との調整能力、コミュニケーション能力を有する。（2-1-3）
- □ チームメンバーは、システム管理、ネットワーク管理、プログラミング、技術サポート、セキュリティ管理、いずれかのスキルを有する。（2-1-4）
- □ 各メンバーのスキルを総合し、チーム全体として上記スキルを網羅している。（2-1-5）
- □ 各メンバーは、スキルの向上や獲得、最新の知識習得のための教育研究を行っている。（2-1-6）
- □ チームワークを尊重できる要員であること。（2-1-7）
- □ チーム内だけでなく、組織内の他のグループや外部組織とも円滑なコミュニケーションを図ることができる。（2-1-8）

インシデント対応チームの構成においては、その組織にとって最適なモデル（分散／集中）を選定し、チームの役割に合った人材を招集して組織化を行うことが重要である。

本設問では、組織の現状を踏まえたうえで、インシデント対応チームの組織体制および要員配置を行っていることを確認する。

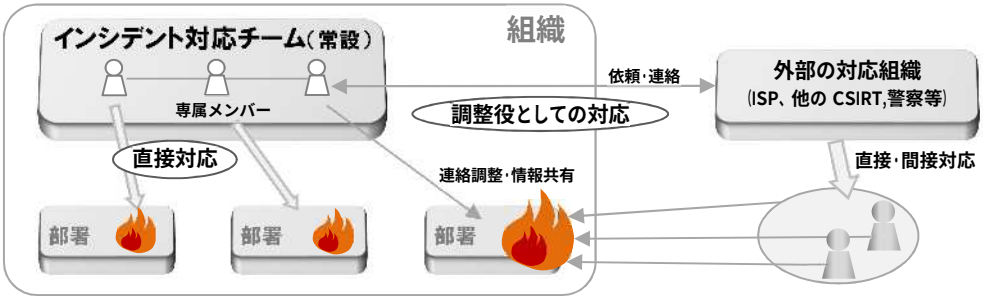
【補足】

「インシデント対応チームモデル」とは、不正攻撃や情報漏えい等のセキュリティ事故に対応する組織の“構成の特徴”をモデル化したもので、「集中型」「分散型」という 2 つのモデルに分けられる。

「集中型」「分散型」それぞれの特徴を以下に示す。

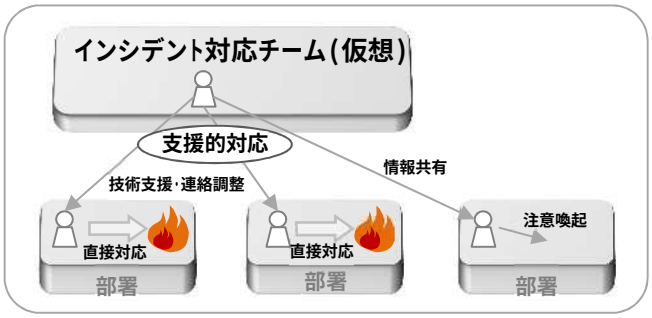
「集中型」

- 正式に対応チームが組織化されている。
- 専属メンバーで構成される。
- インシデント対応チームの役割（設問 1-2-1 解説）のうち、「直接対応」または「調整役としての対応」の役割を担う。



「分散型」

- インシデントが発生した際、解決までの一定期間だけ仮想的に対応チームを作る。
- チームメンバーは有事の際に参画する（兼務者も含む）
- インシデント対応チームの役割(設問 1-2-1 解説)でのうち、「支援的対応」を担う。



解説

□ 組織の現状を踏まえたうえで、インシデント対応チームの組織体制を決定している。

インシデント対応チームを構成するにあたり、組織規模や部署構成・人材リソースといった環境条件と、インシデント対応の現状課題のバランスを取りながら、「分散型」「集中型」どちらが実務上適しているのかを見極めて、体制を決定している。

解説

□ 組織の要件や利用できるリソースに照らし、慎重に検討を行ったうえで、要員配置を行っている。

組織における「インシデント対応チーム」の役割と責任範囲を明確にしている。例えば、インシデント対応のライフサイクルから、「日常運用」「情報収集」「検知」「調査分析」「復旧」「復旧後の対応」など実務要件を洗い出し、何をどこまで担うのか定義することで、組織要件が明確になる。その明確になった役割において、適する人材がどこにいるのか、現在の担当業務との兼ね合いなどを慎重に考慮の上、アサインを行い配置するなど、現状の

組織体制にマッチするチーム作りが行われている。

解説

□ チームリーダーは、インシデント対応における組織内外との調整能力、コミュニケーション能力を有する。

インシデント対応チームのチームリーダーは、マネジメント層や他のグループ、外部組織などと調整を行い、危機を打開するために必要な要員、リソースを確保し、短時間で意思決定できることが求められる。そのため、優れた調整能力、コミュニケーション能力を有することが重要である。

解説

□ チームメンバーは、システム管理、ネットワーク管理、プログラミング、技術サポート、セキュリティ管理、いずれかのスキルを有する。

□ 各メンバーのスキルを総合し、チーム全体として上記スキルを網羅している。

組織の役割定義に基づき選定したメンバーは、ここに挙げた５つのスキルのうち 1 つ以上は専門知識を有しており、インシデント発生時には率先して対応し、チームを牽引することが可能なレベルの能力を有している。同時に、一人で５つのスキル全てを保有することは難しいため、チーム全体として 5 つのスキルを網羅できていることが重要である。

【参考】

セキュリティの観点から５つのスキルの「例」を以下に示す。

- 「システム管理」の例
  対象機器（ソフトウェア、ハードウェア）の管理を行う中で、システムの脆弱性を見極め、セキュリティの脅威情報を元に影響範囲を切り分けることができる等のスキルを有する。
- 「ネットワーク管理」の例
  管理対象のネットワーク上のセキュリティ脅威を見極めることができ、適切な対応策を打ち出すことができる。また、インシデント発生時には、セキュリティ対策製品等を活用してネットワークの遮断や設定変更が行える、といったスキルを有する。
- 「プログラミング」の例
  Web システムにおける SQL インジェクションのように、システムを構築する際に注意すべきポイントを認識し、セキュリティを意識したプログラミングを行えるスキルを有する。
- 「技術サポート」の例
  システム運用中の技術的な問題やユーザからの問い合わせに対処でき、インシデントが発生した場合には的確な初動対応の指示が行える等のスキルを有する。

- 「セキュリティ管理」の例
  セキュリティ対策製品を使用して不正行為の監視・検知を行うことができ、インシデントが発生した場合には調査すべきシステムやログが分かり、適切な対処が実行できる等のスキルを有する。

解説

□ 各メンバーは、スキルの向上や獲得、最新の知識習得のための教育研究を行っている。

スキルの向上やスキルを獲得するために、技術カンファレンスへの定期的な出席や、最新の知識を習得するために、技術関連資料の入手、ワークショップの開催など継続的な教育研究を行っていることが望ましい。

解説

□ チームワークを尊重できる要員であること。
□ チーム内だけでなく、組織内の他のグループや外部組織とも円滑なコミュニケーションを図ることができる。

インシデント対応は、チームメンバーとの共同作業を行う機会が多い。また、インシデント対応のライフサイクルに則り、様々な部署と連携することも必要になるため、協調性やコミュニケーション能力があることが望ましい。

3.2.2. インシデント対応の参加グループ

② インシデント対応※注) に参加してもらう必要がある、組織内の他のグループが明確になっていますか？

以下の要素を考慮して、インシデント処理の参加グループを明確にしていますか？

- □ 参加を依頼する組織の役割が明確になっている。（2-2-1）
- □ 上記組織には、マネジメント層、情報セキュリティ部門、IT サポート部門、法務部門、広報部門、設備管理部門が含まれる。（2-2-2）

※注）インシデント対応：インシデントの影響を軽減するための施策のこと

インシデント対応に係る活動のなかには、インシデント対応チームだけでは対応が難しい場合がある。そのため、どの部署と連携をする必要があるのか予め明確に整理しておき、インシデントが発生した場合には協力してもらえるよう、事前に支援要請を行っておくことが重要である。

本設問では、インシデント対応に参加してもらう必要がある、組織内の他のグループが明確になっていることを確認する。

【補足】

インシデント対応チームの基本的な役割は、設問 1-2-1 解説から以下の 6 つに整理できる。

技術的な役割

(1) 直接対応
(2) 支援的対応
(3) 調整役としての対応

管理的な役割

(4) インシデント報告の受理
(5) 外部組織との連携
(6) インシデント関連情報の伝達経路の保全

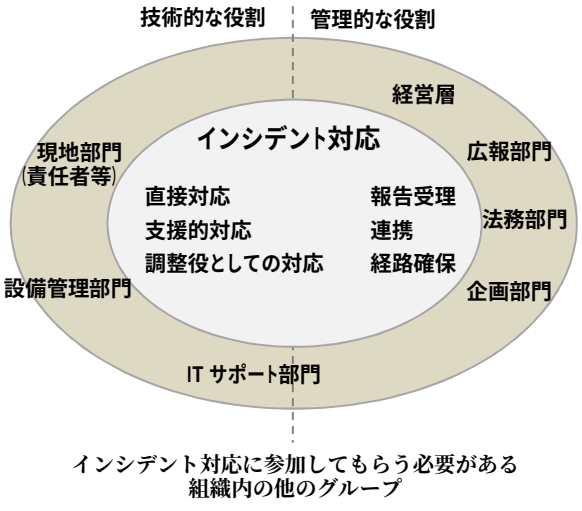
上記(1)～(6)の活動はインシデント対応チームだけでは対応が難しい場合がある。そのため、どの部門と連携をする必要があるのか予め明確に整理しておき、インシデントが発生した場合には協力してもらえるよう、事前に支援要請を行っておくことが重要である。

例えば、

- インシデント対応チームのメンバーが直接現地に赴いて技術的な対応を行う場合では（直接対応）、部門の PC 管理者や業務システムの運用管理者等と連携を行い、バ

ックアップデータの提供やログ収集を伴う現地調査に協力してもらう必要がある。

- 現地部門が直接インシデント対応を行い、インシデント対応チームは後方から支援を行う場合では（支援的対応）、現地で作業する IT サポート部門と連携を行い、技術情報のやり取りを行う必要がある。
- 外部の対応組織にインシデント発生の連絡や対応依頼を行う場合では（調整役としての対応）、自組織と外部の対応組織とをつなぐ窓口の設置や、技術情報をやり取りするための安全なネットワークの敷設など、企画部門や IT サポート部門との連携が必要となる。
- インシデント報告を受理する窓口を設置する際には、組織内外からの通報を一時的に受け付けるコールセンターの設置や、専用の電話番号・メールアドレスの取得、これらの情報を Web サイト等へ掲載して周知するなど、広報部門を含めた関係各所との連携が必要となる。
- インシデントが発生した場合に組織外にどう公表するか（組織外サイトへの経緯・状況の掲示やマスコミ向けの会見調整など）、また、その後の対応（法的対処、ステークホルダーへの補償など）については、法務部門等と連携を行う必要がある。
- インシデント情報の伝達経路については、特に外部の対応組織に支援を依頼してインシデント対応を行う場合などに、機密情報を依頼先と安全にやり取りするための経路の確保が必須となる。2 組織をつなぐセキュアなネットワークの敷設調整など、IT サポート部門と連携を行う必要がある。



解説

□ 参加を依頼する組織の役割が明確になっている。
□ 上記組織には、マネジメント層、情報セキュリティ部門、IT サポート部門、法務部門、広報部門、設備管理部門が含まれる。

インシデント対応の６つの役割を実行する上で、それぞれの役割ごとに協力が必要な部門を整理し、リスト化するなどの準備を行っている。また、どのような支援が必要か具体的に必要な作業を明確にし、インシデント発生時には対応に参加してもらうよう事前の調整を行っている。

3.2.3. インシデント対応チームが担うインシデント対応以外の役割

③ インシデント対応チームが担う、インシデント対応以外の役割を明確にしていますか？

以下の要素を考慮して、インシデント対応チームが担うインシデント対応以外の役割を明確にしていますか？

- □ インシデント対応チームがインシデント対応以外に行う業務や役割が明確になっている。（2-3-1）
- □ インシデント対応以外で情報共有及び連携する組織内の他のグループや外部組織との協力関係が明確になっている。（2-3-2）

インシデント対応に直接は関係しないものの、インシデントの発生を抑制したり、問題を早期解決し被害の甚大化を防ぐための活動が必要である。このような活動をインシデント対応チームの役割とする場合には、そのことを明確にしておくことが必要である。

本設問では、インシデント対応チームのインシデント対応以外の役割が明確になっていることを確認する。

【補足】

例えば、いち早く危険な攻撃を察知するための情報収集

・最新の脆弱性情報や攻撃情報の収集

・IPA や JPCERT、セキュリティベンダー等が発信する情報の収集

組織内の脆弱性を解消したり、攻撃を早期発見するための調査

・対策状況の一元管理と未対策 PC 等への対策徹底

・トラフィックの監視などシステム全体の運用管理

セキュリティに関する意識付けを行うための啓発活動

・教育の実施

・インシデント情報の共有

などについて、役割を担う部署が必要である。

解説

- □ インシデント対応チームがインシデント対応以外に行う業務や役割が明確になっている
- □ インシデント対応以外で情報共有及び連携する組織内の他のグループや外部組織との協力関係が明確になっている

日常的な調査・啓発活動について、「何をやるか」「誰がやるか」「インシデント対応チームとどう連携するか」といった事を定義し、組織図のような目に見える形でまとめ、共有している。

3.3. インシデント対応の準備

3.3.1. インシデント対応担当者への連絡と設備

① 社内外からのインシデントに関する情報について、インシデント対応チームへの連絡手段が準備されていますか？

以下の要素を考慮して、インシデント対応担当者への連絡手段を準備していますか？

- □ インシデント発生時の連絡先が明確である。（3-1-1）
- □ 社内のエスカレーションルートを整備している。（3-1-2）
- □ 社内及び社外からのインシデント報告窓口を用意している。（3-1-3）
- □ 携帯電話等、リモートでインシデント対応チームと連絡をとる手段を用意している。（3-1-4）
- □ チームのメンバー間、組織内、外部の関係者との間で情報伝達を行う場合に使用する暗号化ソフトウェア※注）を準備している。（3-1-5）
- □ インシデント対応の中心となって組織内外の連絡・調整を行うための対応本部が常設されている。または、常設ではないが必要時に対応本部を確保する手順を策定している。（3-1-6）

※注）暗号化ソフトウェア：秘匿性の高い連絡用のメッセージを暗号化するためのソフトウェア

情報漏えい・Web 改ざん・ウイルス感染など、何らかのインシデントが発生した場合に、その事象を発見した人から速やかに、インシデント対応組織・対応者に対して、正確な情報の伝達がなされることが、被害拡大防止と早期解決のために重要である。

本設問では、インシデント対応担当者への連絡手段および設備が準備されていることを確認する。

解説

□ 連絡先情報を整備している。

インシデントを通報する（受け付ける）全社的な窓口が設置されており、その連絡先（外線番号、Mail アドレス、Web フォーム等）が周知されている。

【補足】

例えば窓口としては、情報システム部門や警備部門などがあげられる。また、連絡手段（電話なのか、メールなのか）はルール化されていることが望ましい。

解説

□ 社内のエスカレーションルートを整備している。

インシデントが発生した場合、各部門において上司、上位上司、情報セキュリティ管理

者など、インシデント情報をいち早く把握し、何らかの対処が求められる責任者については、漏れなく連絡先をリストにまとめ、内部で共有している。
その際、どのようなルートでインシデント対応組織まで情報を報告していくのか、フロー図などを用いて整理し、関係者に周知している。

解説

□　社内外からのインシデント報告手段を作成している。

社内外問わず、通報を受け付ける窓口を用意している。また、報告手段（電話、メール等）についてルールを定め、Web サイトへ掲載するなどして周知を行っている。

【補足】
Web サイトの改ざんといったインシデントの場合、第一発見者は外部の一般ユーザであることが多いため、外部に開かれた窓口は必要である。

解説

□　携帯電話等、リモートでインシデント対応者と連絡をとる手段を持っている。

外出先の関係者と連絡が取れるよう、携帯電話などの連絡手段を確保している。

【補足】
インシデント対応は迅速に行うことが求められるため、現地への移動中に情報をやり取りする事も多い。また業務時間外にメンバーが招集されるケースもある。

解説

□　チームのメンバー間、組織内、外部の関係者との間での連絡で使用する、暗号化ソフトウェアを準備している。

インシデント対応の過程でやり取りするデータは、情報漏えいを考慮した適切な手段でやり取りを行っている。

【補足】
解析に用いるログファイルや、マネジメント層への報告レポートなど、インシデント対応の過程でやり取りするデータは「機密情報」にあたるため、情報漏えいを考慮した適切な手段でやり取りを行う必要がある。暗号化はその手段の一つであり、専用ソフトウェアや ZIP 暗号等によってデータを保護することが不可欠である。

解説

□ インシデント対応の中心となって組織内外の連絡・調整を行うための対応本部が常設されている。または、常設ではないが必要時に対応本部を確保する手順を策定している。

インシデント対応に関わる全ての関係者を統括し、情報を取りまとめ、交通整理を行う窓口を用意することができる。

【補足】

インシデント対応は、マネジメント層、情報セキュリティ部門、IT サポート部門、法務部、広報部、設備管理部門など複数の組織が関係する。また、監督省庁やマスコミなどとの調整も必要になるため、全体をマネジメントする要員が必要になる。

3.3.2. インシデント分析のためのハードウェアとソフトウェア

② インシデント分析のためのハードウェアとソフトウェアが準備されていますか？

以下の要素を考慮して、インシデント分析のためのハードウェアとソフトウェアの準備を実施していますか？

- □ 証拠物や機密物を安全に保管するための手段を用意している。（3-2-1）
- □ コンピュータフォレンジックワークステーション※注) とバックアップ装置を用意している。（ディスクイメージ作成、ログファイル保存、その他データ保管用）（3-2-2）
- □ インシデント分析のための PC を用意している。（3-2-3）
- □ 予備のワークステーション、サーバ、ネットワーク機器を用意している。（3-2-4）
- □ 未使用媒体を用意している。（証拠保全用の CD-R、DVD-R 等）（3-2-5）
- □ 簡単に持ち運びができるプリンターを用意している。（3-2-6）
- □ パケットスニファとプロトコルアナライザを用意している。（3-2-7）
- □ コンピュータフォレンジックソフトウェア※注) を用意している。（3-2-8）
- □ インシデント分析に利用するプログラム・ツール用の CD 等を用意している。（3-2-9）
- □ 証拠収集アクセサリを用意している。（3-2-10）

※注）コンピュータフォレンジック：データの完全性を維持しながら、調査目的でコンピュータ関連のデータを収集、保管、分析すること。

※注）コンピュータフォレンジックワークステーション：コンピュータフォレンジック用の PC 等

※注）コンピュータフォレンジックソフトウェア：コンピュータフォレンジックを実施するためのソフトウェア

インシデント分析を行うには、証拠保全や情報収集、解析環境のための環境を事前に用意することが求められる。

本設問では、インシデント分析のためのハードウェアとソフトウェアが準備されていることを確認する。

解説

□ 証拠物や機密物を安全に保管するための手段を用意している。

バックアップを行うための手段、環境を用意している。

解説

□ コンピュータフォレンジックワークステーションとバックアップ装置を用意している。（ディスクイメージ作成、ログファイル保存、その他データ保管用）

ディスクのコピーを取ったりするのに必要なハードウェア、ソフトウェアの指定がある

場合は、それに準拠した環境の用意を行っている。

解説

□　インシデント分析のための PC を用意している。

インシデント分析のための PC を用意している。

解説

□　予備のワークステーション、サーバ、ネットワーク機器を用意している。

マルウェアの動きを確かめるなど、何らかの再現環境を持っている。

解説

□　未使用媒体を用意している。（証拠保全用の CD-R、DVD-R 等）

バックアップ用に、書き換え禁止の媒体を用意している。

解説

□　簡単に持ち運びができるプリンターを用意している。

簡単に持ち運びができるプリンターを用意しており、調査結果のスクリーンショット等を保存しておくことができる。

解説

□　パケットスニファとプロトコルアナライザを用意している。

WireShark などの情報取得ツールを用意している。

解説

□　コンピュータフォレンジックソフトウェアを用意している。

インシデント発生時の証拠保全を行うために、コンピュータフォレンジックソフトウェアを用意している。

解説

□　インシデント分析に利用するプログラム・ツール用の CD 等を用意している。

証拠収集や分析に使うためのプログラム・ツール類を入れた CD を用意している。

3.3.3. インシデント分析のための準備

③ 重要資産の一覧を準備する等、インシデント分析のための準備がされていますか？

以下の要素を考慮して、インシデント分析のための準備を実施していますか？

- □ 一般に使用されるポートとトロイの木馬のポートリスト※注）を用意している。（3-3-1）
- □ OS、アプリケーション、プロトコル、侵入検知とアンチウイルスシグネチャなどのマニュアルを用意している。（3-3-2）
- □ ネットワーク図と重要な資産の一覧を用意している。（3-3-3）
- □ 予想されるネットワークの活動、システムの活動、アプリケーションの活動の基準を整備している。（3-3-4）
- □ インシデントの分析、検証、根絶を迅速に行うための、重要なファイルのハッシュリストを準備している。（3-3-5）

※注）トロイの木馬のポートリスト：見かけとは別の悪意のある目的を持ったプログラム（トロイの木馬）が使用するポートの一覧

インシデント分析に役立つ情報、例えば、攻撃パターンのリストや、通常時（正常時）のデータを蓄積しておくことで、分析作業が効率的に進む場合がある。

本設問では、インシデント分析のための準備がされていることを確認する。

解説

□ 一般に使用されるポートとトロイの木馬のポートリストを用意している。

トロイの木馬が一般的によく使うポートのリストを保有している。

【補足】

ポートリストは、Google やセキュリティベンダの Web サイトから検索できるので、必要な際に検索する方法を知っておくこと。

解説

□ OS、アプリケーション、プロトコル、侵入検知とアンチウイルスシグネチャなどのマニュアルを用意している。

分析ツールの操作に困らないよう、プロトコルアナライザのマニュアルや、アンチウイルスシグネチャソフトのマニュアルを用意すると共に、ツール類の使用方法について日常的なトレーニング等によって習熟しておく。

解説

□ ネットワーク図と重要な資産の一覧を用意している。

システムの全体構成を把握するためのネットワーク図と、組織内で守るべき資産のリストを持っている。

【補足】
守るべき資産とは、文書であれば技術情報や経営機密など。機器であれば、基幹業務サーバやデータベースなど。情報漏えいやシステム障害といったインシデントにより事業に何らかの影響がでる資産を洗い出し、整理しておくことで、インシデントの影響範囲の特定や被害状況の判断に役立つ。またハッシュ値などを取っておけばファイルが変更された際の分析にも役立つ。

解説

□　予想されるネットワークの活動、システムの活動、アプリケーションの活動の基準を整備している。

資産の一覧を元に、現状のベースライン（正常値）を測定し、それを超えた場合に異常を検知できるよう、事前の準備を行っている。

解説

□　インシデントの分析、検証、根絶を迅速に行うための、重要なファイルのハッシュリストを準備している。

ファイルが変更された際に、それを検知することができる何らかの手段を用意している。（ハッシュ値はその一例）
なお、構築完了の段階のマスターイメージについては、すべてのファイルのハッシュ値を取得しておくことが望ましい。

3.3.4. インシデント鎮静化のためのソフトウェア

④ インシデント鎮静化（対処・復旧）のためのソフトウェアが準備されていますか？

以下の要素を考慮して、インシデント鎮静化のためのソフトウェアを準備していますか？

- □ OS のブートディスクや CD-ROM、OS の媒体、アプリケーションの媒体などを用意している。（3-4-1）
- □ OS やアプリケーションのセキュリティパッチを用意している。（3-4-2）
- □ OS、アプリケーションおよびデータのバックアップイメージを用意している。（3-4-3）

インシデントの調査分析により、原因や影響範囲が特定され、対処方法が確定した後、パッチ適用や設定変更、復旧などの具体的な作業を実施することになるが、その際、作業に必要なツール類や環境等を予め準備しておくことが重要である。

本設問では、インシデント鎮静化（対処・復旧）のためのソフトウェアが準備されていることを確認する。

解説

□ OS のブートディスクや CD-ROM、OS の媒体、アプリケーションの媒体などを用意している。

OS やアプリケーションの再インストールが行えるよう、必要な媒体を用意している。

解説

□ OS やアプリケーションのセキュリティパッチを用意している。

パッチ未適用のシステムを更新できるよう、最新のセキュリティパッチを保有している。

解説

□ OS、アプリケーションおよびデータのバックアップイメージを用意している。

定期的にシステムのバックアップを行い、バックアップイメージから速やかに復旧できる手段が整っている。

3.4. 予防

3.4.1. リスク評価

① システムとアプリケーションのリスク評価を定期的に行っていますか？

以下の要素を考慮して、リスク評価を実施していますか？

- □ 保護すべき情報資産を把握している。（4-1-1）
- □ 脅威※注）と脆弱性※注）の組み合わせから、どのようなリスク※注）があるかを判断している。（4-1-2）
- □ 明らかになったリスクへの対応方針を明確にしている。（4-1-3）

※注）脅威：リスクを引き起こす原因。

- DOS 攻撃（サービス不能攻撃）
- 改ざん（ハードウェア、ソフトウェア、データの不正変更）
- 不正アクセス（業務システムや機密データへの不正アクセス）
- 情報資産の不適切な使用

※注）脆弱性：システムやアプリケーションにおけるセキュリティ上の弱点。攻撃の入口となるセキュリティホールなど。

※注）リスク：組織に損害や影響を発生させる可能性。システム停止や情報漏えいなど。（脅威が脆弱性を利用して組織にリスクをもたらす）

リスク評価とは、保護すべき情報資産を明らかにし、それらに対する脅威と脆弱性の分析を行い、インシデントが発生した場合の影響度を「見える化」することをいう。これにより、リスクが高いシステムへの対策強化や、万一インシデントが発生した場合の対処法を想定することができ、より的確な対応が行えるようになる。

本設問では、システムとアプリケーションのリスク評価を定期的に行っていることを確認する。

解説

□ 保護すべき情報資産を把握している。

重要なシステムを構成するサーバ、クライアント端末、アプリケーション、個人情報等の重要なデータ資産について、管理場所や数、バージョン等の基本情報を把握している。

解説

□ 脅威と脆弱性の組み合わせから、どのようなリスクがあるかを判断している。

脅威の定義に基づき、脆弱性がもたらす組織のリスクを整理している。例えば、

- DOS 攻撃（脅威）に対する脆弱性がある場合、システム停止や遅延のリスクが顕在化する可能性がある。

- システム改ざん（脅威）に対する脆弱性がある場合、誤作動や誤ったデータの流出、復旧のための業務遅延などのリスクが顕在化する恐れがある。
- 機密システムへの不正アクセスに対する脆弱性がある場合、非公開情報の閲覧やそれに伴う情報漏えいのリスクが顕在化する可能性がある。
- 情報資産（個人情報・技術情報など）の不正利用に対する脆弱性がある場合、流出に伴う信用の失墜、ビジネス競争力の低下、補償等による経営の圧迫といったリスクが顕在化する恐れがある。

解説

□　明らかになったリスクへの対応方針を明確にしている。

リスクを低減する対策をとるのか（パッチ適用などによる脆弱性の解消）、影響度の低いリスクについては保有するのか（特に対処は行わない）、リスクを回避する手段をとるのか（根本原因を取り除く）など、個々のリスクに対してどのような対応を行うか、方向性を共有している。

3.4.2. パッチ管理

② パッチ管理ができていますか？

以下の要素を考慮して、パッチ管理を実施していますか？

- □ 対象の分類分けができている。（4-2-1）
- □ 全ての対象に対して確実に実施している。（4-2-2）
- □ パッチ管理プログラムを使用し、システム管理者によるパッチの識別、取得、テスト、配布を支援している。（4-2-3）

パッチ管理は、セキュリティ事故の要因の一つである「システムの脆弱性」を解消するために必要なプロセスである。パッチ適用を漏れなく行うためには、どの資産に対してパッチ適用を行う必要があるのか把握するため、あらかじめ対象資産の洗い出しを行い、優先順位づけを行っておくことが重要である。パッチ適用対象が多い場合は、システム管理者の作業を支援する管理プログラムを活用することも有効である。

本設問では、適切なパッチ管理が実施できているかを確認する。

解説

□ 対象の分類分けができている

パッチ適用をすぐに実施すべきものと、すぐに実施できないもの（評価やスケジュール調整等が必要なものなど）を分類し、優先順位づけを行っている。また、すぐに実施できないものについても、脆弱性がもたらす事業への影響度によって、その後の対処方針を定めている（例：定期メンテナンスで実施。バージョンアップ時に実施。リスクの受容。等）

解説

□ 全ての対象に対して確実に実施している。

パッチ適用対象の分類に基づき、パッチ適用を行う全ての対象に対して、確実にパッチ適用を実施している。また何らかの方法で適用済みである事を客観的に判断できる。

解説

□ パッチ管理プログラムを使用し、システム管理者によるパッチの識別、取得、テスト、配布を支援している。

システム管理者が、パッチ適用対象のハードウェアやソフトウェア等の情報を管理し、現在適用されているパッチのバージョン情報やパッチ適用有無について、効率的に把握することができるような管理プログラムやツールの導入を行っている。その上で、システム管理者が、適用すべきパッチをベンダーから取得しテストできる仕組みや、各担当者への配布を支援する仕組みが取り入れられている。

3.4.3. ホストのセキュリティ管理

③ ホスト（クライアント端末／サーバ等）のセキュリティは適切に管理されていますか？

以下の要素を考慮して、ホストのセキュリティ管理を実施していますか？

- □ 各端末に対し、適切にパッチが適用されるよう管理している。（4-3-1）
- □ 最低限のサービスが適切なユーザと端末だけに提供されるよう設定している。（4-3-2）
- □ 安全でないデフォルト設定(デフォルトのパスワード、安全でない共有など)を変更している。（4-3-3）
- □ セキュリティ対策が実施されたリソースにユーザがアクセスしようとした場合、警告バナーが表示されるようにしている。（4-3-4）
- □ 端末の監査が実施できるようになっており、重要なセキュリティ関連のイベントについてはログを取得している。（4-3-5）
- □ 管理者が端末のセキュリティ対策を首尾一貫して効果的に実施できるよう、オペレーティングシステム（以下、「OS」という）とアプリケーションの管理手順を用意している。（4-3-6）

インシデントの発生を抑制するためには、クライアント端末およびサーバのセキュリティ対策を実施する必要がある。

本設問では、クライアント端末、サーバ、及びその上で動作するアプリケーションについてのセキュリティ対策について確認する。

解説

□ 各端末に対し、適切にパッチが適用されるよう管理している。

各端末に適用されているパッチのバージョンを把握し、適切なパッチが当たっていない場合には、確実に適用されるよう配布等の手段を確保し、状態のフォローを行っている。

解説

□ 最低限のサービスが適切なユーザと端末だけに提供されるよう設定している。

許可された関係者だけが、必要な業務システムにアクセスできるよう、認証等によるアクセス権の強化を行っている。

解説

□ 安全でないデフォルト設定(デフォルトのパスワード、安全でない共有など)を変更している。

パスワードなしや推測しやすいパスワードは変更を促すなどのフォローを行っている。

また、アクセス制限が設定されている共有フォルダについては、関係者以外がアクセスできないよう、共有フォルダの設定をこまめに見直し最新化を行っている。（プロジェクトを離れた元関係者がアクセスするケースもあるため）

解説

□　セキュリティ対策が実施されたリソースにユーザがアクセスしようとした場合、警告バナーが表示されるようにしている。

ポップアップメッセージや、アラート画面への遷移など、注意喚起の仕組みが導入されている。

解説

□　端末の監査が実施できるようになっており、重要なセキュリティ関連のイベントについてはログを取得している。

インベントリ情報や syslog など、監査に必要な情報を効率的に取得するための支援ツールが導入されている。アプリケーションログについてはサーバ上に蓄積できる仕組みが導入されている。

解説

□　管理者が端末のセキュリティ対策を首尾一貫して効果的に実施できるよう、OS とアプリケーションの管理手順を用意している。

初期設定については、ポリシーに基づいたサーバ設定、OS・アプリケーションのインストールが実行されるよう、手順が共通化されている。変更を行う場合の管理手順（OS、アプリケーションのバージョンアップ、ライセンス追加など）についても、評価や実装、運用手順などについて文書化されている。監査においては、監査手順やログの保存期間など、組織内でルールが整理され文書として共有化されている。

3.4.4. ネットワークのセキュリティ管理

④ ネットワークセキュリティは適切に管理されていますか？

以下の要素を考慮して、ネットワークのセキュリティ管理を実施していますか？

- □ ネットワークの境界※注)では、明示的に許可されていないすべてのアクセスを拒否するように設定している。（4-4-1）
- □ 組織が適切に機能するために必要な活動だけを許可している。（4-4-2）
- □ VPN (virtual private network)、ほかの組織への専用線接続といったすべての接続ポイントのセキュリティを高めている。（4-4-3）

※注）ネットワークの境界：一般的に、組織内のネットワーク（イントラネット）とインターネットが接する部分を「ネットワークの境界」と表わす。また、組織内においても、ネットワークのセキュリティレベルが切り替わる部分（例えばオープンネットワークとクローズドネットワークの接点）も境界と表現することがある。

ネットワークのセキュリティ管理は、外部からの不正行為（クラッキング等）を防ぎ、内部からの情報流出を防止するなど、組織内のネットワークの安全性を維持し、情報資産を守るために重要である。特に、インターネットを経由して内部に入ってくる通信および、内部から外部に出ていく通信に不正なものが含まれていないかを見定め、適切に対処することが求められる。そのためには、業務に関係のない通信をブロックしたり、不正な第三者のアクセスを排除したりするなどの対策が有効である。

本設問では、ネットワークのセキュリティが適切に管理されていることを確認する。

解説

- □ ネットワークの境界では、明示的に許可されていないすべてのアクセスを拒否するように設定している。
- □ 組織が適切に機能するために必要な活動だけを許可している

組織内のネットワークがインターネットに繋がる部分は、外部からの不正アクセスや情報流出の出入口となるため、適切な対策が必要である。ファイアウォールや UTM およびサンドボックスなどの製品を用いて業務に関係ないアプリケーションや不正な通信を止めるなどの制御を行う事が重要である。

解説

- □ VPN (virtual private network)、ほかの組織への専用線接続といったすべての接続ポイントのセキュリティを高めている。

VPN や専用線など信頼している関係者からの接続においても、踏み台攻撃やネットワーク探査による不正攻撃により被害を受ける可能性があるため、接続ポイントには適切な対

策が求められる。たとえば、UTM による不正通信の遮断や、認証権限強化によるなりすましの防止などが有効である。

3.4.5. 悪意のコードを予防する仕組み

⑤ ウイルスなどの悪意のコードを予防する仕組みを導入していますか？

以下の要素を考慮して、悪意のコードを予防する仕組みを導入していますか？

□ ウイルス、ワーム、トロイの木馬などの悪意のコードを検知して阻止するソフトウェアを組織全体に配布している。（4-5-1）

□ 悪意のコードの予防策を行っている。（4-5-2）

悪意のコードとは、ウイルス、ワーム、バックドア、キーロガーなどに代表される不正なプログラムのことで、システムの停止／遅延や、権限の奪取、ID パスワードの搾取など、直接的または間接的にシステムへ影響を及ぼす。この悪意のコードを実行させない、もしくは早期に検知するために、必要な対策を行うことが重要である。

本設問では、悪意のコードを予防する仕組みが導入されていることを確認する。

解説

□ ウイルス、ワーム、トロイの木馬などの悪意のコードを検知して阻止するソフトウェアを組織全体に配布している。

ウイルス対策ソフトやスパイウェア検出駆除ソフトなどの専用ツールを適用している。その際、定義ファイルは常に最新のものに更新している。

解説

□ 悪意のコードの予防策を行っている。

例えば、以下のような取り組みが予防策に該当する。

- 最新パッチを迅速に適用するなど脆弱性の早期解消を行っている。
- システム管理者は、悪意のコードを早期に識別するために、適切な情報源（例えば、IPA やセキュリティベンダなど信頼できる Web サイトや定評のある刊行物等）からの情報収集を行っている。
- 悪意のコードの検出や、復旧のための管理策を事前に整備し共有している。
- 利用者に対して、悪意のコードが検出された場合の手順について周知展開している。

3.4.6. ユーザのセキュリティ意識向上

⑥ トレーニングや訓練によって、ユーザのセキュリティ意識向上に努めていますか？

以下の要素を考慮して、ユーザのセキュリティ意識向上を実施していますか？

- □ ユーザに対し、ネットワーク、システム、アプリケーションの適正な利用に関するポリシーや手順について情報提供を行っている。（4-6-1）
- □ 過去の事件の教訓をユーザ間で共有し、自分たちの行動が組織にどのような影響を与えるかを認識させるようにしている。（4-6-2）
- □ 悪意のコードに関係する事件や、利用ポリシー違反に関係する事件を共有し、事件に関するユーザの意識向上に努めている。（4-6-3）
- □ 情報技術(IT)スタッフは、ネットワーク、システム、アプリケーションを組織のセキュリティ標準に従って維持できるように訓練を行っている。（4-6-4）

セキュリティ対策は、システムの強化だけでなく、システムを使う作業者一人一人の意識付けを行うことで効果を発揮する。なぜセキュリティ対策が大切なのか、どのような行動がインシデントの発生に繋がるのか、インシデントが発生すると事業や関係者にどのような影響があるのか、等について、できる限り具体的にイメージできるよう啓発活動を行うことが重要である。

本設問では、トレーニングや訓練によって、ユーザのセキュリティ意識向上が成されているかを確認する。

解説

- □ ユーザに対し、ネットワーク、システム、アプリケーションの適正な利用に関するポリシーや手順について情報提供を行っている。

組織全体でポリシー（セキュリティを維持するためのルール）を定め、それを周知し、実際に守られているかどうか定期的にチェックしている。例えば、フリーソフトの使用条件や申請手順、パスワード設定のルール（○文字以上など）、個人情報の取り扱い、外出時のルール（社外からの接続条件）など、その組織の事業を遂行する上で必要なセキュリティの規則を文書化し、共有している。

解説

- □ 過去の事件の教訓をユーザ間で共有し、自分たちの行動が組織にどのような影響を与えるかを認識させるようにしている。
- □ 悪意のコードに関係する事件や、利用ポリシー違反に関係する事件を共有し、事件に関するユーザの意識向上に努めている。

過去のヒヤリハットを含む事故事例を、関係者が集まる場で共有し、何がいけなかったのか、防ぐにはどうしたら良いのか、討論を行うなどして自ら考えさせている。

解説

□ 情報技術(IT)スタッフは、ネットワーク、システム、アプリケーションを組織のセキュリティ標準に従って維持できるように訓練を行っている。

システムの環境設定がポリシーに沿って適切に行えるよう、ツールの操作に関する教育や実機演習などに参加している。

3.5. 検知と分析

3.5.1. 攻撃検知

① IDS などの攻撃を検知する仕組みがありますか？

以下の要素を考慮して、攻撃を検知するための対策を実施していますか？

- □ 組織内には、IDS/IPS やウイルス対策ソフトウェア、ファイル完全性チェックソフトウェア、もしくはパケットフルキャプチャ製品※注) が導入されており、セキュリティインシデントを検知することができる。(5-1-1)
- □ 新しい脆弱性とエクスプロイトに関する情報や他組織でのセキュリティインシデントに関する情報を定期的に収集している。(5-1-2)
- □ ポリシーに準拠し、主要なシステムに対してログ取得に関する基準が策定されている。(5-1-3)
- □ ポリシーに準拠し、主要なシステムで監査機能を有効にし、監査イベントを取得している（5-1-4）
- □ 主要なシステムにおいて、ログ取得が適切に機能していること、及びログ取得の基準に準拠していることを定期的に確認している。(5-1-5)
- □ 取得したログを保存する際は、ファイルの完全性チェックを行い、ログが改ざんされていないことを確認している。(5-1-6)

※注）パケットフルキャプチャ製品：ネットワーク上で実際に流れるトラフィックのパケットを全て採取する製品

インシデント対応チームが有効に活動するためには、システム的にセキュリティインシデントを検知する仕組みの構築が必要となる。一般的には「ログ分析」と呼ばれるセキュリティ対策で、IDS/IPS やウイルス対策ソフト等のセキュリティ製品のアラートを分析する。また、システムのログを分析してセキュリティインシデントを検知することが重要となる。

本設問では、セキュリティインシデントを検知する仕組みがあるかを確認する。

解説

- □ 組織内には、IDS/IPS やウイルス対策ソフトウェア、ファイル完全性チェックソフトウェア、もしくはパケットフルキャプチャ製品が導入されており、セキュリティインシデントを検知することができる。

IDS/IPS やウイルス対策ソフトウェアは一般的なセキュリティ製品である。IDS/IPS は主に外部サーバへの不正アクセスを検知・防御を行い、ウイルス対策ソフトウェアはゲートウェイ、もしくはエンドポイント（ホスト上）で不正なプログラムを検知・駆除を行う。両製品とも不正な事象をアラートとして出力するため、インシデントを検知するために非常に有効な製品といえる。

ファイル完全性チェックソフトウェアはファイルの変更を管理し、完全性をチェックするための製品であり、ファイル改ざん等を検知するために有効な製品となる。ファイルの変更は通常の業務でも発生するため、前述のセキュリティ製品のアラートをトリガーに分析する必要がある。

パケットフルキャプチャ製品は、ネットワーク上に送り出された全ての通信データをキャプチャ（取得）する製品で、インシデント発生時に事象の分析を行うために利用される。ファイル完全性チェックソフトウェアと同様に製品単体で脅威を発見することはできないが、トリガーとなる情報を基に分析を行う際に有効なツールとなる。

解説

□　新しい脆弱性とエクスプロイトに関する情報や他組織でのセキュリティインシデントに関する情報を定期的に収集している。

新しい脆弱性とエクスプロイトに関する情報や他組織でのセキュリティインシデントに関する情報を定期的に収集することで、自組織でのセキュリティインシデント検知を補完することができる。また、脆弱性やエクスプロイトの情報については自組織に関連するものを特定する必要がある。

解説

□　ポリシーに準拠し、主要なシステムに対してログ取得に関する基準が策定されている。

多くのシステムを利用している場合、全てのログを取得するとログが膨大となり、有効な分析ができない可能性がある。そのため、ログの取得に関する基準を作成し、意図したログを取得することが重要となる。

解説

□　ポリシーに準拠し、主要なシステムで監査機能を有効にし、監査イベントを取得している。

監査イベントは各ホストやサーバの動作の記録（ログ）となる。監査機能を有効にし、監査イベントを取得することでインシデントが発生した際に、原因究明の分析に利用できる。但し、全てのホストで監査機能を有効にした場合にログが膨大となるため、監査ポリシーを作成し、ポリシーに準拠したホストで利用することが重要となる。

解説

□　主要なシステムにおいて、ログ取得が適切に機能していること、及びログ取得の基準に準拠していることを定期的に確認している。

主要なシステムにおいて、ログ取得が適切に機能しているかを定期的に確認することで、

実際にインシデントが発生した場合にも効果的に分析作業が実施できる。また、確認時にはログのサイズやディスク容量等に問題が無いかを確認する必要がある。

解説

□　取得したログを保存する際は、ファイルの完全性チェックを行い、ログが改ざんされていないことを確認している。

ログ自体が改ざんされた場合、ログ分析やインシデント時の分析が不可能となる。そのため、定期的にファイルの完全性チェックを行い、ログが改ざんされていないことを確認する必要がある。

3.5.2. 異常検知

② ネットワークとシステムの使用率や、正常な動作を把握し、異常を検知できる仕組みがありますか？

以下の要素を考慮して、異常を検知できる対策を実施していますか？

- □ ネットワークの帯域使用率を監視している。（5-2-1）
- □ 各ホストのリソース使用率を監視している。（5-2-2）
- □ ネットワークや各ホストにおける、平均及びピーク時の使用率レベルを把握している。（5-2-3）
- □ ネットワークにおける、正常時の動作を把握している。（5-2-4）
- □ 各ホスト及びホスト上で稼動するアプリケーションにおける、正常時の動作を把握している。（5-2-5）

ネットワークやシステムのプロファイリングを行い、期待される（正常な）活動レベルの特性を測定しておくことで、期待される活動レベルからのズレを素早く検出して管理者に報告することができる。また、正常な動作とはどのようなものなかのを理解すれば、異常な動作をより簡単に認識することができる。なお、正常な動作として、システムの仕様や運用形態、データフロー等を把握しておく必要がある。

本設問では、異常を検知できる仕組みがあるかを確認する。

解説

□ ネットワークの帯域使用率を監視している。

「異常検知」とは、「正常な動作」から外れる動作を検知することで、まずは「正常な動作」を把握し、そこからどこまで外れると「異常」になるかを明確にすることが重要となる。ウイルスの中には Bot として外部サイトを攻撃するものやワームのように自己増殖するものが存在する。その場合、ネットワークの帯域が増加する傾向があるため、帯域使用率を監視することで異常検知を行うことができる。また、平均時やピーク時の使用率レベルを把握することも有効となる。

解説

□ 各ホストのリソース使用率を監視している。

各ホストのリソース使用率では、ウイルスを含む不正プログラムの影響でトラフィックや CPU の使用率等が増大することを検知することが可能となる。また、平均時やピーク時の使用率レベルを把握することも有効となる。

解説

□ ネットワークにおける、正常時の動作を把握している。

ネットワークにおける正常な動作を可視化することで、異常時の検知ができる。正常な動作を可視化する方法としては、通信プロトコルやアプリケーションを特定し、どの時間帯に利用があるかを把握することが有効となる。

解説

□ 各ホスト及びホスト上で稼動するアプリケーションにおける、正常時の動作を把握している。

アプリケーションの動作では、ホスト上で稼働するアプリケーションの正常な動作を可視化することで、外部からの不正アクセス等による不正な動作を検知できる。正常な動作を可視化する方法として、発生する通信や稼働するプログラム、また前述の CPU 使用率等を把握することが有効となる。

3.5.3. ログの管理と相関分析

③ ポリシーに基づくログの取得と保管を実施するとともに、各イベントを相関分析※する仕組みがありますか？

以下の要素を考慮して、ログの管理と相関分析を実施していますか？

□ 各システムで取得したログはログサーバに送信し、管理している。（5-3-1）

□ ログの保持期間等を規定したログ保管ルールを策定し、準拠している。（5-3-2）

□ 複数のシステムで検知したイベントの相関分析※注）を実施している。（5-3-3）

□ すべてのシステムで時刻の同期ができている。（5-3-4）

※注）相関分析：脅威と思われる兆候を見つけ出す等を目的として、多種多様なシステムのログを一元的に集めて相関的な分析を行うこと。

インシデントは、いくつものログで捕捉される可能性がある。複数のソースのイベントを相関させることは、インシデントに関して入手できるすべての情報を収集し、インシデントが発生したかどうかを検証する上で重要である。

本設問では、インシデントを発見するために、ログの相関分析をする仕組みがあるかを確認する。

解説

□ 各システムで取得したログはログサーバに送信し、管理している。

各システムで取得したログを一括で管理することで後述の相関分析が容易となる。また、各ホストでログを保存せずログサーバに送信することで、ホストが攻撃を受けていた場合にもログの改ざんを防止することができる。尚、大量のアラートやログの保管、分析に SIEM（Security Information and Event Management）を使うケースも多くなっている。

解説

□ ログの保持期間等を規定したログ保管ルールを策定し、準拠している。

ログの保持期間はインシデント発生時にどこまで遡って分析する必要があるかを考慮することが重要となる。

解説

□ 複数のシステムで検知したイベントの相関分析を実施している。

相関分析は、各イベントの相関性からセキュリティ上の事象や状況（影響の有無や度合）を分析する手法である。例えば IDS/IPS で検知したイベントと関連するサーバのログを確認することによって攻撃が成功したかどうかを判断することが可能となる。

相関分析は「3.5.1. 攻撃検知の仕組み」のログ分析を効率的、かつ脅威の発見を容易に

するが、効果を発揮するためには相関分析を行うロジックが重要となる。ロジックについては「3.5.4. 知識やスキルの向上」で形式知化するナレッジを利用し、自社で取得するログに適した相関処理を構築する。

解説

□　**すべてのシステムで時刻の同期ができている。**

取得するログは時刻同期により正確性を担保する必要があり、また改ざん等を防止するために専用サーバに保存する必要がある。

3.5.4. 知識やスキルの向上

④ インシデント対応に必要な知識やスキルを向上し、攻撃検知の仕組みに反映していますか？

以下の要素を考慮して、知識やスキルの向上の対策を実施していますか？

- □ インシデント対応に有用なナレッジ（セキュリティベンダーサイトの情報、過去のインシデント情報等）を二次利用し易い方法（Excel、データベース、専用ツール等）でまとめ、定期的に更新している。(5-4-1)
- □ 検出されたインシデントの分類や確認に係る方法を明文化した、チェックリストが整備されている。(5-4-2)
- □ インシデントが検出された時点から、最終的に解決されるまでのすべてのステップを記録し、タイムスタンプを付加している。(5-4-3)
- □ インシデントに係るデータは、許可された人間だけがアクセスできるように論理的かつ物理的に制限されている。(5-4-4)
- □ 影響のあるリソースの重要性やインシデントの技術的な影響に基づき、ビジネスインパクトごとに対処するインシデントの優先順位をつけている。(5-4-5)

検出されたインシデントの分類方法や確認方法など、インシデント対応に有用なナレッジは形式知化すると共に、最新の脅威に対処できるように定期的に更新する必要がある。

本設問では、インシデント対応に必要なナレッジの形式知化等が、攻撃検知に反映されているかを確認する。

解説

□ インシデント対応に有用なナレッジ（セキュリティベンダーサイトの情報、過去のインシデント情報等）を二次利用し易い方法（Excel、データベース、専用ツール等）でまとめ、定期的に更新している。

セキュリティベンダーサイトの情報、過去のインシデント情報等は、インシデント対応時に有用なナレッジ（情報）となる。そのため、定期的に内容を更新し、常に参照が可能な状態とする。

解説

□ 検出されたインシデントの分類や確認に係る方法を明文化した、チェックリストが整備されている。

インシデント対応の属人化を防ぐため、インシデントの分類（情報漏えい、Web 改ざん、マルウェア感染、サービス不能攻撃等）や確認に係わる方法を明文化したチェックリストを作成する。また、チェックリストは定期的に見直すことが必要となる。

解説

□　インシデントが検出された時点から、最終的に解決されるまでのすべてのステップを記録し、タイムスタンプを付加している。

インシデントの結果を報告する、また外部に公表する場合には、「時間軸」が重要となる。そのため、対応した内容を記録する際にはタイムスタンプを付加し、必ず「いつ」「何をしたか」を明確にする。

解説

□　インシデントに係るデータは、許可された人間だけがアクセスできるように論理的かつ物理的に制限されている。

インシデントに係わるデータは機密性の高い情報となる。そのため、関係者以外がアクセスできないようにする。

解説

□　影響のあるリソースの重要性やインシデントの技術的な影響※注）に基づき、ビジネスインパクトごとに対処するインシデントの優先順位をつけている。

※注）インシデントの技術的な影響とは、インシデントの発生により受けるシステムの影響（システムの停止、アプリケーションの停止や情報漏えい等）を指す。

インシデントの重要度とは別に、システム停止に係わるビジネスインパクトも考慮して対処するインシデントの優先順位をつけることが重要となる。

3.6. 封じ込め・根絶・復旧および事後活動

3.6.1. インシデントの封じ込め

① インシデントを封じ込めるための手順や戦略・許容できるリスク定義は出来ていますか？

以下の要素を考慮して、インシデント封じ込めの対策を実施していますか？

- □ インシデントの種類（サービス不能攻撃・悪意のコード・不正アクセス・不適切な使用・複合要素）のいずれかまたは複数を想定して、検討が為されている。(6-1-1)
- □ インシデント発生時の封じ込めのための具体的な対応手順／想定フローが作成されている。(6-1-2)
- □ インシデント発生時の封じ込めのための意思決定プロセスが明確になっている。(6-1-3)
- □ インシデント発生時の封じ込めのための許容できる範囲／レベルが明確になっている。(6-1-4)
- □ インシデント発生時の封じ込めのための許容できる範囲／レベルを既存の SLA(合意されたサービスレベル）等と照らし合わせて決定し、実態に即した封じ込めとして実効性がある。(6-1-5)

インシデントを封じ込めるための手順や戦略・受容できるリスクが、インシデントが発生する前に決められていないと、事業継続や迅速なリカバリにおいて混迷を極めることになりかねない。また、被害が拡大する可能性が高くなり、収拾する時間や工数が業務を大きく逼迫するなど、業績下方修正等の最悪の事態を引き起こす可能性さえある。

本設問では、インシデントが発生した後のことを想定して、いかにリスクを最小化するか・どのように回避するかの封じ込めプランについて、組織全体で定義されているか、具体的な対応手順フローが作成され、許容できる範囲／レベルが明確になっているかを確認する。また、いずれにおいてもインシデント対応チームの独自判断で実行できる範囲を明確にしておくべきである。

解説

□ インシデントの種類（サービス不能攻撃・悪意のコード・不正アクセス・不適切な使用・複合要素）のいずれかまたは複数を想定して、検討が為されている。

インシデントの種類については、以下の 5 つのパターン例を参考にしながら想定や検討を行うことが必要である。

(1) サービス不能攻撃（DOS）

想定例：中央処理装置(CPU)、メモリー、帯域、ディスク領域などのリソースを枯渇させることで、ネットワーク、システム、アプリケーションの正規の使用を妨害する活動。

(2) 悪意のコード

想定例：別のプログラムにこっそりと埋め込まれたプログラムで、データを破壊したり、破壊的なプログラムや侵入目的のプログラムを実行したり、攻撃対象者のデータ、アプリケーション、またはオペレーティングシステムのセキュリティや機密性、完全性、可用性などを侵害したりすること。

(3) 不正アクセス

想定例：ユーザがアクセスを許されていないリソースへのアクセスを不正に得ることによって起こるもの。

(4) 不適切な使用

想定例：ユーザが適切なコンピュータの利用方針に違反した行動を取った場合に起きるもの。

(5) 複合要素

想定例：1 つのインシデントに 2 つ以上のインシデントを包含しているものである。

解説

□　インシデント発生時の封じ込めのための具体的な対応手順／想定フローが作成されている。

インシデントの種類によって、封じ込めの対応手順やフローが異なることが多くある。ここでは、以下の 5 つのパターン例を自社の事業と照らし合わせながら、以下の各項目に示す検討項目を参考にしつつ、実際の対応手順やフローを作成することが必要である。

(1) サービス不能攻撃（DOS）

㋐活動元からのすべてのトラフィックをブロックすることである。（注：しかし、この種の攻撃では送信元アドレスが偽装されているか、数千の侵入されたホストが使用されることが多く、送信元IPアドレスに基づく効果的なフィルタリングを実施するのは難しいか不可能なことが多い。）

㋑脆弱性／弱点を修正する。

A:起動しているサービス（一例：echo 等）の修正パッチによる対応。

B:起動しているサービス（一例：echo 等）の一時停止など。

C:関連ホストの切り離しなど。

㋒攻撃手法に有効なフィルタリングを行う。

A:攻撃が例えば ICMP echo 要求であれば、このプロトコル等をネットワーク／セキュリティ機器でブロックする。

B:攻撃手法が SYN フラッドの場合は、単にブロックするとそれ自体がユーザに対する攻撃（DOS）になり加害者になってしまうので注意を必要とする。

C:様々な攻撃手法に対するフィルタリング対応を想定しておく。

D:帯域制限することで、特定プロトコルや特定ホスト宛パケットを毎秒一定数し

か許可しない。

E:フィルタリングや帯域制限を行う場所／機器も封じ込め対応で重要となる。(例：境界ルーターやファイアウォールなど)

F:前述 A～E を実施できるセキュリティ機器の配備やアップグレードを行う。

㊓ISP にフィルタリングの実施を依頼する。

ISP へフィルタリング依頼できる仕組みなどがあり、実効ある対応が可能な形にしておく。

㊔ターゲットの再配置を実施する。

ほかの封じ込め戦略の効果がない場合、対象ホストをほかの IP アドレスに移動することも効果がある。

(2) 悪意のコード

㋐感染したシステムが重要でない場合は、すぐにネットワークから切り離すことが望ましいことが多い。一方、感染したシステムが重要な機能を実行している場合は、サービスが利用できないことによる組織への損害が、すぐにシステムを切り離さないことによるセキュリティ上のリスクを上回る場合のみ、ネットワークに接続したままにしておくことも選択肢として残る。

㋑感染範囲を調査して隔離する。

A:ポートスキャンでの感染ホスト発見と隔離

B:特定の悪意のコードへの対応が可能なスキャン／クリーンアップツールでの隔離

C:各種ログ（メール、ファイアウォール、システム、ホストログ等）による発見と隔離

D:ネットワーク及びホストへの侵入検知／防御ソフトの導入による発見と隔離

㋒不明な悪意のコードを分析依頼し隔離する。

分析結果から駆除ツールやシグネチャの提供を受けて隔離する。また、インシデント処理担当者は、不明な悪意のコードのコピーを分析依頼するための手順を確立しておく。

㋓電子メールサーバや電子メールクライアントによる発見と隔離

駆除ツールやシグネチャの提供を受けるまでのタイムラグや残存リスクをカバーする手段の１つとして、電子メールシステムでの発見と隔離も効果が出る場合がある。

㋔ネットワーク又はホストの隔離

例えばネットワークトラフィックなどにより、インターネットアクセスができない場合は、組織をインターネットから一時的に切断することもある。また、内部システムが他のシステムを攻撃してトラフィック輻輳（多量の通信を発生させ通常の送受信が困難な状態）やサービス停止などの被害拡大を増長させないために

も、該当ネットワークや特定ホストを隔離することも有効である。

㈎サービスの無効化

例えばマルウェアが悪用しているプロセスサービスを停止したり、ネットワーク周りの特定のサービスを停止／遮断することで、迅速かつ効果的に封じ込めができる場合がある。ただし、むやみにサービスを無効にすると、そのサービスに依存しているほかのサービスを誤って停止させてしまうこともあり、組織の活動にマイナス影響などが出る可能性があるので注意が必要である。

(3) 不正アクセス

㈀影響のあるシステムを隔離する。

不正アクセスを封じ込めるための最も簡単な方法の１つとして、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がある。しかし、影響を受けたシステムをすべて特定するのは難しい。多数のシステムを確認しなくてはならない場合が少なからずあるので、バックドアのポートスキャンなど、自動化された方法を使用することが望ましいときもある。

㈁影響を受けたサービスを無効にする。

悪用されている該当サービスの無効化もインシデントの封じ込めの１つとして有効である。たとえば攻撃者が FTP の脆弱性を悪用している場合などがある。

㈂侵入ルートを除去する。

例えば、特定のネットワークセグメントに対する受信方向のコネクションを一時的にブロックしたり、リモートアクセスサーバを切断したりすることである。

㈃悪用されている可能性があるユーザアカウントを無効にする。

悪用される／悪用されたアカウントは組織全体で無効にすることを強くお勧めする。また、見覚えのない新しいユーザアカウントなどについても、チェックして無効化などを行うことが望ましい。

㈄物理的なセキュリティ対策を強化する。

例えば、部外者がサーバルームにアクセスしたことが疑われる場合は、サーバルームのセキュリティを強化するだけでなく、関連設備を捜索して、侵入者がもうそこにいないことを確認することが望ましい。また、サーバールーム以外の物理的なセキュリティの変更も有効である。

(4) 不適切な使用

㈀基本的に、好ましくないファイルを削除したり、許可されていないソフトウェアをアンインストールする以外は、一般に封じ込め、根絶、復旧活動は必要ない。

㈁ただし、ユーザがほかの組織を攻撃している場合は例外であり、ユーザの特定や攻撃の停止などを通じて、ほかのシステムへのさらなる被害を防ぎ、最小化する。

㈂もうひとつの例外としては、インシデント対応チームが外部の組織に対して、その組織のホストに違法なファイル等があることを通知する場合である。

(5) 複合要素

㋐基本的に、インシデント処理担当者は、インシデントのすべての要素を特定することだけに注力すべきではない。なぜなら、すべての要素を調査・把握するまでには膨大な時間がかかるだけでなく、その間にも最初に発見したインシデントの初動対応が不十分になることで、被害拡大などの問題が進行してしまう可能性もあるからである。また、最初に発見したインシデント調査・対応の過程の中で、他のインシデント要素を特定できる場合があるからである。

㋑よって一般的には、最初のインシデントを封じ込めてからほかの要素の兆候を探すのがよいことが多い。

㋒もしも、インシデントの複数の要素に気づいたら、各要素の処理に個別に優先順位を付けるべきである。たとえば、現在起きている DoS 攻撃は、6 週間前に起きた悪意のコードの感染よりも、通常はより迅速に対処することが多い。

解説

- □ インシデント発生時の封じ込めのための意思決定プロセスが明確になっている。
- □ インシデント発生時の封じ込めのための許容できる範囲／レベルが明確になっている。
- □ インシデント発生時の封じ込めのための許容できる範囲／レベルを既存の SLA（合意されたサービスレベル）等と照らし合わせて決定し、実態に即した封じ込めとして実効性がある。

実際にインシデントを封じ込めるための対応手順やフローを実行・適用することについて、組織としての最終判断の所在（意思決定プロセス）が明確になっていないと、これまでの作業や努力は全く意味をなさないに等しい。また、その実行・適用を最終判断するにあたり、許容できる範囲／レベルを明確にしておかないと実効性がないだけでなく、事業継続などへの想定外の悪影響・副作用が起きるので、定期的に実効性確認や見直しが必要である。

なお、この３つについては各企業で SLA（合意されたサービスレベル）やサービス形態などが異なるため、それぞれの環境や事情に沿って各インシデント封じ込めへの対応として現実的な実行・適用可能な意思決定プロセス、許容範囲／レベルの設定、実効性確認などの整備状況のチェック及び推進を行うことが重要である。また、いずれにおいても、インシデント対応チームの独自判断で実行できる範囲を明確にしておくべきである。

3.6.2. 証拠保全

② 証拠保全（証拠収集や処理）の方法について、文書で確立された手順に従って対応できますか？

以下の要素を考慮して、証拠保全の対策を実施していますか？

- □ インシデントの種類（サービス不能攻撃・悪意のコード・不正アクセス・不適切な使用・複合要素）のいずれかまたは複数を想定して、検討が為されている。(6-2-1)
- □ 何を証拠とすべきかが明確になっている。(6-2-2)
- □ 証拠保全の方法について手順の作成等がされている。(6-2-3)
- □ 証拠保全の手順等の作成は、関係第三者機関（法執行機関等）や法務スタッフなどの組織内関係者との協議のもとで実施している。(6-2-4)

インシデントが発生した後で配慮しなければならないものに証拠保全（証拠収集や処理）の方法・手順がある。確かに組織にとってインシデントの封じ込めを行うことが最優先事項の１つではあるが、より的確な原因究明や正確な状況把握、効果的なインシデント対応のためには、証拠収集や処理の手順が適切でなければ意味がない。一定知識や準備がない状態で証拠保全及びインシデント対応を進めると封じ込めに時間がかかるだけでなく、封じ込め失敗による再発・被害拡大が延々と続くことになる。

本設問では、インシデントが起きた後で効果的な封じ込めを実施するための証拠保全の方法について、その手順が確立されているかを確認する。

解説

- □ インシデントの種類（サービス不能攻撃・悪意のコード・不正アクセス・不適切な使用・複合要素）のいずれかまたは複数を想定して、検討が為されている。
- □ 何を証拠とすべきかが明確になっている。

インシデントの種類によって、証拠保全の観点が異なることがある。ここでは、以下の 5 つのパターン例について、何を証拠にすべきなのかも含め、押さえるべきポイントを解説する。

(1)サービス不能攻撃（DOS）

DoS 攻撃の証拠収集や処理は、主に以下の３つの観点も鑑みながら、手順を作成すること。

㋐ログエントリーをレビューする

ほとんどの DoS 攻撃はリソースを逼迫させることで起きるため、異常に大量のログエントリーが生成される可能性がある。ログが上書きされたり、証拠が残らないことがないように、ログの収集方法や処理（証拠保全）の手順を確立しておく。

㋑観測されるトラフィックからの攻撃元の特定

ただし、送信元 IP アドレスは偽装されていることが多いので、特定に至らないこ

とが少なくないので注意が必要である。

㋐複数の ISP にまたがった攻撃の逆探知

各 ISP からの協力を取り付けるのに要する時間を考えると、逆探知できるようになるまでには攻撃が止まっている可能性が高い。現在進行中の攻撃を逆探知することよりも、はるかに難しい。

(2)悪意のコード

悪意のコードの証拠収集や処理は、主に以下の３つの観点も鑑みながら、手順を作成すること。

㋐フォレンジックによる証拠収集／識別

最近又は過去の感染の証拠を探し出すことによって、感染したシステムを識別する手法である。たとえば、ユーザまたは IT スタッフによる、マルウェアや感染の兆候に関する情報のほか、ウイルス対策ソフトウェア、スパイウェア検出／駆除ユーティリティ、コンテンツフィルタリング（スパム対策など）、ホストベースの侵入防止ソフトウェア、あるいはスキャンツールを駆使して、感染を特定するなどがある。

㋑リアルタイムでの証拠収集／識別

現在どのホストが感染しているのかを識別するのに使用する。たとえば、駆除ユーティリティを実行する、オペレーティングシステムやアプリケーションのパッチ・ウイルス対策の更新を配備する、感染しているシステムのための VLAN にホストを移動するなどである。

(3)不正アクセス

不正アクセスの証拠収集や処理は、主に以下の観点も鑑みながら、手順を作成することが望ましい。

㋐処理担当者はシステムの完全なバックアップイメージを取得する。

㋑ホストとアプリケーションのログ、侵入検知警報、ファイアウォールのログなど関連するほかのデータも取得する。

㋒インシデントの最中に物理的なセキュリティ違反が起きた場合には、物理的なセキュリティシステムのログ、監視カメラのテープ、目撃者の証言なども追加証拠として収集しておく。

㋓場合によっては、法執行機関へ連絡する。

(4)不適切な使用

不適切な使用の証拠収集や処理は、主に以下の観点も鑑みながら、手順を作成することが望ましい。

㋐証拠の改ざんや破壊に備え、組織の物理的なセキュリティを管理するスタッフとの連係を行い、証拠物のある場所へのアクセス制限を行うことなども含める。

(5)複合要素

複合要素の証拠収集や処理は、前述の(1)～(4)をもとに手順を作成することが望ましい。

㋐複数のインシデントがあった場合、より優先する証拠収集や処理を決めておくこと。

解説

- □ **証拠保全の方法について手順の作成等がされている。**
- □ **証拠保全の手順等の作成は、関係第三者機関（法執行機関等）や法務スタッフなどの組織内関係者との協議のもとで実施している。**

前述のインシデントの種類によって、証拠保全の観点や証拠とすべきものが明確になったことをベースに具体的な証拠保全の手順作成等を実施する必要がある。また、手順作成の際は組織内外の有識者とも協議のうえ行うべきである。

なお、具体的な証拠保全の手順については、各企業の業務やサービス形態などに依存する部分が大きいため、それぞれの環境や事情に沿って現実的に実行・適用可能なものを作成する必要がある。手順の作成にあたっては、IPA にて公開されている RFC3227「証拠収集とアーカイビングのためのガイドライン」を参考にするとよい。

3.6.3. 揮発性データ及び完全なディスクイメージの収集

③ 不用意に変更・破壊することなく、揮発性データを証拠としてシステムから取得することができますか？また、フォレンジックに適した完全なディスクイメージ（単なるファイルシステムのバックアップではなく）を収集できますか？

以下の要素を考慮して、揮発性データなどの収集について対応策がありますか？

- □ 保全すべき揮発性データを漏れなく迅速に収集できるように、収集過程がある程度自動化されている。（6-3-1）
- □ 揮発性データの証拠が不用意に変更や改ざんなどされないような媒体（再書き込み不可メディア：DVD、CD 等）に保存できる。（6-3-2）
- □ ディスクイメージを保存する先として、未使用（ゼロクリア、初期化済み）のデバイスを準備する。（6-3-3）
- □ ディスクイメージ取得時に元のディスクイメージデータが不用意に改変されないように、再書き込み・上書き禁止などの配慮ができている。（6-3-4）
- □ 完全なディスクイメージを取得するツールやコマンドを問題なく使用できる。（6-3-5）

インシデント発生後に収集する証拠としては、大きく分けて揮発性データと完全なディスクイメージがある。揮発性データとは、一般的に電源が入っているときだけデータが保持（保存）されるような例えばメモリー上に存在するものである。一方、完全ディスクイメージは、ハードディスクに保存されている全てのデータを丸ごと取得することで、通常のファイルコピーでは収集できない削除ファイルやブートセクター情報なども含めることができるため、より詳細かつ正確な証拠保全や分析・封じ込めに貢献できる。

本設問では、的確なインシデント対応に必要な証拠として、揮発性データやディスクイメージの情報が不用意に改ざんや消去等されないように正しく収集できる過程・保存方法が実現できることを確認する。

解説

- □ 揮発性データを漏れなく迅速に収集できるように、収集過程がある程度自動化されている。
- □ 揮発性データの証拠が不用意に変更や改ざんなどされないような媒体（再書き込み不可メディア：DVD、CD 等）に保存できる。

揮発性データ（例：ネットワーク接続の一覧、プロセス、ログインセッション、オープンされたファイル、ネットワークインタフェース設定、メモリーの内容など）を漏れなくかつ迅速に収集するためには、収集過程で使用する各コマンド・プログラムがバッチ等によって自動化することが良いとされている。また、収集した揮発性データの完全性を担保するために、証拠保全先の媒体は再書き込み不可メディアとする。

解説

- □ ディスクイメージを保存する先として、未使用（ゼロクリア、初期化済み）のデバイスを準備する。
- □ ディスクイメージ取得時に元のディスクイメージデータが不用意に改変されないように、再書き込み・上書き禁止などの配慮ができている。
- □ 完全なディスクイメージを取得するツールやコマンドを問題なく使用できる。

ハードディスクや他ストレージの証拠保全を実施する際は、完全なディスクイメージを取得することで、より確実な原因究明の確率が上がるだけでなく、効果的な封じ込めが実現しやすくなる。このため、元の証拠ディスクが不用意に改変等されないように、再書き込みや上書きがされないようにしておくことが重要である。また、証拠保全先については必ず未使用のデバイス（準備できない場合は全領域をゼロクリアしたもの）にする必要がある。なお、完全なディスクイメージを取得するには専用のツールやコマンドが必要なので、何度か事前にテストをしておくことが望ましい。

3.6.4. インシデント対応の事後活動

④ インシデント対応のレビュープロセスが入っていますか？

以下の要素を考慮して、インシデント対応の事後活動を計画していますか？

- □ レビュープロセスが定義されている。(6-4-1)
- □ レビューするための適切なメンバーが選出されている。(6-4-2)
- □ レビュー責任者が明確である。(6-4-3)
- □ レビューメンバーにマネジメント層が含まれている。(6-4-4)
- □ レビューのルールが決められている（再発防止のためにも建設的なレビューに努めることなど)。(6-4-5)

インシデント対応後のレビュープロセスがない又は形だけで進めてしまうことがある。レビュープロセス（事後活動）をしっかり計画することで、セキュリティ対策の再確認や改善が図れるだけでなく、インシデントレスポンス体制・対応手順・技術的課題の見直しなどにより、実害を最小限に抑えることができるようになる。

本設問では、レビュープロセス（事後活動）をしっかり計画し、実施できる体制を確立することで、組織的な対応及び解決方法・プロセスの改善活動が実施される状態であることを確認する。

解説

- □ レビュープロセスが定義されている。
- □ レビューするための適切なメンバーが選出されている。
- □ レビュー責任者が明確である。
- □ レビューメンバーにマネジメント層が含まれている。

組織的な対応及び解決方法・プロセス改善活動の効果を高めるためには、レビューの定義・目的を明確にし、メンバーにマネジメント層を含める必要がある。また、レビューは建設的なものにすることが重要であり、犯人捜しなどを必要以上に行うことはできる限り避けるべきである。またレビュープロセスには、事後活動のレビューによって定まった改善事項の実施状況や効果を定期的にモニタリングすることを含めることが望ましい。

解説

- □ レビューのルールが決められている（再発防止のためにも建設的なレビューに努めることなど)。

レビューを円滑に行うためには、ルールを事前に決めておくことが望ましい。

4. 付録

付録 I　用語集

項番	用語	意味
1	IDS/IPS	コンピュータシステムまたはネットワーク上の疑わしい活動の監視プロセスを自動化し、事件の兆候を分析して、検出された事件の防止を試みるソフトウェア。
2	インシデント	コンピュータセキュリティインシデントのこと。コンピュータセキュリティポリシーや情報利用規定等の違反、または違反が予測される差し迫った事象のこと。
3	インシデント対応	コンピュータセキュリティインシデントの影響を軽減するための施策のこと。
4	インシデント対応チーム	コンピュータセキュリティインシデントへの対応を支援する目的で発足させた機能。コンピュータインシデント対応チーム(CIRT)、CIRC(コンピュータインシデント対応センター、コンピュータインシデント対応機能)とも呼ばれる。
5	ウイルス	自己複製するプログラムで、ほかのプログラムやファイルを変更することで動作・拡散するもの。
6	エクスプロイト	プログラムのセキュリティ上の脆弱性（セキュリティホール）を攻撃するために作成された簡易なプログラムの総称であり、多くの場合、悪意を持って利用されるプログラムを指す。
7	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。
8	コンピュータセキュリティインシデント対応チーム(CSIRT)	「インシデント対応チーム」を参照。
9	コンピュータフォレンジック	データの完全性を維持しながら、調査目的でコンピュータ関連のデータを収集、保管、分析すること。
10	サービス不能攻撃(DoS)	リソースを枯渇させることで、ネットワーク、システム、アプリケーションの正規の使用を妨害または阻害する攻撃。多数のホストを使用して攻撃を実行する場合には、分散型サービス不能攻撃(DDoS)の用語を用いる。

11	シグネチャ	ある攻撃に関係する、認識可能で特徴的なパターン。ウイルス中のバイナリ文字列や、システムへの不正アクセスを得るために使用する特定のキーストロークなどがある。
12	スキャニング	その後の攻撃で使用する情報を得るために、ほかのシステムにパケットや要求を送ること。
13	トロイの木馬	自己複製不可能なプログラムで、便利な目的を持っているように見えて、実は別の悪意のある目的を持ったもの。
14	パケットスニッファ	ネットワークトラフィックを観察して記録するソフトウェア。パッチ管理パッチを入手、テストし、組織全体の該当する管理者やユーザに配布するプロセス。
15	ファイル完全性チェックソフトウェア	ファイルのメッセージダイジェストを生成、保存、比較して、ファイルの変更を検知するソフトウェア。
16	フォレンジック	「コンピュータフォレンジック」を参照。
17	プロファイリング	変更がより簡単に見つかるよう、予想される活動の特性を測定すること。
18	ベースライン	リソースを監視する際の典型的な利用パターン。これを確定することにより、大きなずれを検知できるようにする。
19	ポートスキャニング	プログラムを使って、システムのどのポートが開いているか(システムがこれらのポートを経由した接続を許しているか)をリモートから調べること。
20	ポリシー	方針、規定、など。
21	リスク	1 つ以上の不利な事象が起きる見込み。
22	悪意のコード	ウイルス、ワーム、トロイの木馬など、ホストに感染するコード型のエンティティ。
23	脅威	不利な事象を起こす可能性がある元凶。
24	事象	ネットワークまたはシステム内の目に見える出来事。
25	脆弱性	悪用や誤用の対象となるシステム、アプリケーション、ネットワークの弱点。
26	ワーム	自己複製し、自己増殖する、自己完結型のプログラムで、ネットワークの仕組みを利用して広まっていく。
27	兆候	インシデントがすでに起きたか、または現在起こっている可能性を示すサイン。
28	不正アクセス	許可なくネットワーク、システム、アプリケーション、

		データ等のリソースに論理的または物理的にアクセスすること。
29	不適切な使用	ネットワークやコンピュータの利用規定に違反すること。
30	複合要素のインシデント	1 つのインシデントで 2 つ以上のインシデントを包含しているもの。

付録II　参考資料

1) コンピュータセキュリティインシデント対応ガイド（Revision 1）、Special Publication 800-61、NIST（IPA 翻訳編集版）
http://www.ipa.go.jp/files/000015367.pdf

2) 情報セキュリティガバナンス導入ガイダンス、平成 21 年、経済産業省
http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf

3) IT システムにおける緊急時対応計画ガイド、Special Publication 800-34、NIST
https://www.ipa.go.jp/files/000025327.pdf

4) 組織内 CSIRT の役割とその範囲、JPCERT コーディネーションセンター
https://www.jpcert.or.jp/csirt_material/files/02_role_of_csirt.pdf

お問合せ先

■組織対応力ベンチマーク
一般社団法人 オープンガバメント・コンソーシアム
〒153-0051
東京都目黒区上目黒 3-12-24-306 ハートウエア 21 内
e-mail：info@ogc.or.jp
URL：http://ogc.or.jp/

【執筆者】
天田めぐみ、市川大輔、岩野圭一郎、久保善輝、
佐々木弘志、佐山享史、豊田祥一、星智恵

組織対応力ベンチマーク解説書
2015 年 7 月 初版

著作編者　　一般社団法人 オープンガバメント・コンソーシアム