National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-84
国土安全保障省による後援

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

米国国立標準技術研究所による勧告

Tim Grance
Tamara Nolan
Kristin Burke
Rich Dudley
Gregory White
Travis Good

この文書は下記団体によって翻訳監修されています。
IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
NRI SECURE TECHNOLOGIES

NIST Special Publication 800-84

IT 計画および IT 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

米国国立標準技術研究所による勧告

**Tim Grance, Tamara Nolan,
Kristin Burke, Rich Dudley,
Gregory White, Travis Good**

コンピュータセキュリティ

米国立標準技術研究所
情報技術研究所
コンピュータセキュリティ部門
Gaithersburg, MD 20899-8930

2006 年 9 月

米国商務省　長官

Carlos M. Gutierrez

技術管理局　技術担当商務次官

Robert C. Cresanti

米国国立標準技術研究所　所長

William A. Jeffrey

コンピュータシステム技術に関する報告書

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下、NIST と称す）の情報技術ラボラトリ（ITL:Information Technology Laboratory）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシーを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動ならびに産業界、政府機関および教育機関との共同活動について報告する。

米国国立標準技術研究所、Special Publication 800-84
米国国立標準技術研究所、Special Publication 800-84、97 ページ（2006 年 9 月）

謝辞

本文書執筆陣である Tim Grance（NIST）、Tamara Nolan、Kristin Burke、Rich Dudley（左記 3 名とも Booz Allen Hamilton）、および Dr. Gregory White、Travis Good（左記 2 名とも UTSA（University of Texas-San Antonio））は、本書草稿のレビューと技術内容に関して協力してくれた同僚に感謝の意を表したい。次に、本書作成の過程全体を通じ、鋭く、洞察に満ちた助言を与えてくれた、Joan Hash、Karen Kent、Peter Mell、Matt Scholl、Marianne Swanson、Mark Wilson（左記 6 名ともNIST）、Dick Broome、Kara Crawley、Courtney Hawkins、Munir Majdalawieh、Zara Pyatt（左記 5 名とも Booz Allen Hamilton）、Dwayne Williams（UTSA）に感謝したい。さらに、貴重なコメントや提案を寄せていただいたことに対し、Glenn Fiedelholtz、Annabelle Lee、Jefferey Wright（左記 3 名、米国国土安全保障省国家サイバーセキュリティ部門（National Cyber Security Division of the Department of Homeland Security））、および米国国務省と MITRE Corporation の代表者にも感謝の意を表したい。

米国国立標準技術研究所は、NIST SP 800-84 に対する国土安全保障省の後援と支援に対しても深く感謝する。

目次

付録

図

表

要旨

さまざまな組織において、緊急時対応計画やコンピュータセキュリティインシデント対応計画などの情報技術（IT：Information Technology）計画が整備されている。こうすることで、企業に損害を及ぼすような IT に関わる不測の状況に対処することが可能となる。IT 計画は、準備の出来ている状態で維持されるべきである。例えば、計画における役割と責任を果たせるよう担当者のトレーニングを行ったり、内容を検証するために計画の実施演習を行ったり、計画に指定されている運用環境でシステムとシステム構成要素の運用性を確認するテストを実施する、といった準備がなされているべきである。これら 3 つの準備作業は、TT&E（Test, Training and Exercise：テスト、トレーニング、演習）プログラムを作成、遂行することにより、効率的かつ効果的に実行できる。テスト、トレーニング、演習は密接に関連しているため、組織は TT&E のようなプログラムの作成を検討すべきである。たとえば、演習とテストを実行することにより、IT 計画、手順、トレーニングに存在する問題点を明らかにするさまざまな方法が得られる。

この文書は、TT&E イベントの設計、作成、実施、評価に関する指針を示し、組織の活動に悪影響を及ぼしかねない出来事に対して、組織が備え、状況を把握、対処し、その出来事から復旧できるようにする能力の向上を目的としている。この文書の対象範囲は、複数組織が関わる大規模イベントではなく、単一の組織を対象とし、緊急時における内部の IT 運用手順を含む TT&E イベントに限定する。この文書は、特定の種類の IT 計画を対象とした TT&E を扱うものではない。この文書で解説する TT&E の方法論は、どのような IT 計画に基づく TT&E イベントにも、そして計画内で必ずしも文書化されていない IT の緊急時対応能力（例：コンピュータセキュリティインシデント対応）に関して作成された TT&E イベントにも適用することができる。

総合的な TT&E プログラム作成の一環として、とるべき手順をまとめた TT&E 計画を作成するべきである。TT&E 計画では、組織のロードマップを定義して実現可能な能力を確保し、計画の維持に加え、能力の強化と管理を実現するための、組織の取り組みについてまとめるべきである。緊急時対応の計画、ポリシー、手順を強化することにより、サイバー攻撃に対抗する能力をより効率よく利用できるようになる。さらに、TT&E 計画では、組織が実効的で実証済みの機能を実現できるようなリソースと予算の要件を明確にし、さまざまな種類の TT&E イベントについて実施スケジュールを示すべきである。TT&E プログラムの作成では、TT&E ポリシーの作成、役割と責任の明確化、TT&E イベント方法論の文書化など、他にいくつかの手順を実施する必要もある。

TT&E プログラムには、計画された内容が妥当であるかを必要に応じて幅広い視点で検証できるよう、サイバーインシデントが発生する状況を想定した各種のイベントを盛り込むべきである。本書で取り上げるイベントの種類は次のとおりである。

- **テスト**[1]。テストは、定量化可能な測定基準を用いて、IT 計画に指定されている運用環境において IT システムまたはシステム構成要素の運用性を検証するための評価手段である。たとえば、組織であれば、所定の時間内に連絡網によって、全員に連絡が行きわたるかどうかをテストしたり、システムやシステム構成要素から電源を抜いてどうなるかをテストしたりすることが可能である。テストは、できる限り実際の運用環境に近づけて実施する。もし可能であれば、組織の日常業務遂行に使用する構成要素またはシステムを実際にテストするべきである。テストの範囲は、個々のシステム構成要素やシステムを対象としたテストから、IT 計画に関わるすべてのシステムと構成要素を対象とした総合的なテストに至るまでさま

[1] 「テスト」と「演習」という用語は、たとえば「演習を通じてテストを行う」のように、互いに入れ替えても変わらないような使い方をされることが少なくない。しかし、この 2 つの用語には違いがある。本書の目的上、「テスト」という用語はシステムまたはシステム構成要素を対象とするテストの場合に使用し、計画実施の「演習」を表す場合には使用しないものとする。

ざまである。テストは、復旧やバックアップの作業を対象とすることが多いが、テストの内容は、テスト自体の目標や特定の IT 計画との関係に応じて変化する。

- **トレーニング。**この文書の目的をふまえ、トレーニングとは、担当者に、ある特定の IT 計画における役割と責任を伝達し、その役割と責任に関わる技能を教えて、IT 計画に関連する演習やテストへの参加の準備、および実際の緊急事態への対処のための準備を整えさせることのみを指すものとする。演習やテストに先立って実施される、役割と責任に関する担当者のトレーニングは一般に、役割と責任に関する発表と、担当者がトレーニング内容を理解したことを確認するための活動とに分けられる。

- **演習。**演習とは、緊急事態のシミュレーションのことで、IT 計画の 1 つ以上の側面について、その実用性を検証することを目的とする。演習では、ある特定の IT 計画で役割と責任を与えられている担当者が集まり、緊急事態における役割と対応に関する議論、シミュレーション用運用環境における対応策の実施、実際の運用環境を用いずに対応策の有効性を確認するその他の手段を通じて計画の内容の有効性を検証する。演習は、組織が利用するデータセンタでの停電やシステムの損傷につながる火災など、シナリオに基づいて実施され、演習を進めるなかで何らかの状況設定が追加されることも多い。演習にはいくつかの種類があるが、本書では、単一の組織が TT&E プログラムで広く用いている、次の 2 種類を取り上げる。

  - **机上演習。**机上演習は、議論ベースの演習で、担当者が会議室に集まったり、その場でグループを作ったりして、緊急時の役割や、ある特定の緊急事態への対応策を議論する形をとる。進行者はシナリオを提示し、それに関する内容を演習の参加者に質問する。質問をきっかけに、役割、責任、連携、意志決定について参加者間で議論を開始する。机上演習は、議論ベースのみの演習であり、設備やその他のリソースの配置を要しない。

  - **機能演習。**機能演習を実施することで、担当者はシミュレーション用運用環境のなかで自らの責務を果たすことにより、緊急時のための運用面の備えを検証できる。機能演習は、計画における、1 つ以上の機能的側面（通信、緊急事態の通知、IT 設備の設定など）に関わりのある、特定のチームメンバ、手順、および資産についての役割と責任の演習を行うことを目的とする。機能演習の複雑さと範囲は、計画の特定の側面の有効性確認から、計画の全要素を対象とした全面的な演習に至るまで、さまざまに異なる。機能演習を実施することで、スタッフは実際の緊急事態における役割と責任を、シミュレーション環境のなかで実践することが可能となる。

組織は、TT&E イベントを定期的に実施するべきである。組織の変更や IT 計画の改定、新たな TT&E 指針の発行、その他の必要性に応じて定期的に実施する。TT&E イベントの定期的な実施は、組織が IT 計画が適切かつ効果的で一貫していることを確認したり、各 IT 計画を実施するなかですべての担当者が自らの役割を確実に認識することに役立つ。TT&E イベントのスケジュール決定には、組織的要件が一部関連する場合も少なくない。たとえば、NIST SP 800-53 では、少なくとも 1 年に 1 回、国の機関が、システムの緊急時対応計画とインシデント対応能力について演習やテストを実施することを要求している。

1. はじめに

1.1 作成機関

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下 NIST と称す）は、2002 年施行の連邦情報セキュリティマネジメント法（FISMA: Federal Information Security Management Act、以下 FISMA と称す）、公法 107-347 に基づくその法的責任を推進するために、この文書を作成した。

NIST は、すべての連邦政府機関の運営および資産に適切な情報セキュリティをもたらすために、最低限の要求事項を含んだ標準およびガイドラインを作成する責務があるが、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局（OMB; Office of Management and Budget）Circular A-130、第 8b(3)項、『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項に一致しており、これは A-130 の付録 IV「重要部門の分析」で分析されているとおりである。補足情報は、A-130、付録 III に記載されている。

このガイドラインは連邦政府機関が使用する目的で作成されている。非政府組織が自由意志で使用することもでき、著作権の制約はない（翻訳者注:著作権に関するこの記述は、SP800-53 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する）。

本文書における一切は、商務長官が法的権威に基づき連邦政府に対して義務および拘束力を与えた標準および指針を否定するものではない。また、これらの指針は、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わるものと解釈してはならない。

1.2 目的と範囲

組織が、計画を整備し、情報技術（IT：Information Technology）に関わるさまざまな状況に対応し管理できるようにすることは重要であるが、それと同じくらい重要なのが、このような計画を準備の出来ている状態に維持しておくことである。こうした準備には、役割と責任を果たせるよう IT 担当者をトレーニングしたり、計画を実際に演習してポリシーと手順の有効性を確認したり、システムをテストして運用性を確認したりする作業が含まれる。これら 3 つの準備作業は、TT&E（Test, Training and Exercise：テスト、トレーニング、演習）プログラムを作成、遂行することにより、効率的かつ効果的に実行できる。

この文書は、IT に悪影響をもたらす状況に備える担当者を支援するため、TT&E イベントの設計、開発、実施、評価に関して組織の参考となることを狙いとしている。TT&E イベントは、組織が、その活動を脅かされる可能性のある災害に備え、対応、管理、復旧を行う能力を最大限発揮できるようにすることを目的として、担当者のトレーニング、IT 計画の演習、そして IT システムのテストを行うために設計されている。本書では、複数の組織が関与するような大規模イベントではなく、単一の組織におけるイベントの設計、開発、実施、評価について解説している。この文書で紹介している TT&E という方法論は、緊急時対応計画（例：災害復旧計画）やコンピュータセキュリティインシデント対応計画をはじめとする、あらゆる種類の IT 関連計画に基づいて構築された TT&E イベントに適用することができる。TT&E に関連する語彙は、組織ごとに異なる。この文書では、TT&E 関連の活動やチームにおいて最も一般的に使用される用語の定義を示す。

1.3 対象とする読者

この文書は、所属する組織の TT&E プログラムに関する責任を担う個人を対象として作成されたものである。特に、その責任を効果的に果たせるよう、TT&E イベントの設計、開発、実施、評価について IT 担当者を支援することを目的としている。

1.4 本書の構成

この文書の以降の内容は、大きく 5 つのセクションで構成されている。セクション 2 は、TT&E プログラムの確立に関する情報を示している。特に、TT&E プログラムの必要性、そして TT&E プログラム作成の手順（TT&E ポリシーの策定、役割や責任、活動の明確化、イベントスケジュールの設定、TT&E イベント方法論の文書化など）について解説している。

セクション 3 は、TT&E プログラムにおけるトレーニングの役割と、トレーニングが演習とテストにどう関連するかについて簡単に説明している。セクション 4 は、机上演習の必要の有無の決定に関する情報、そして演習イベントの設計、作成、実施、評価に関する情報を示している。このセクションでは、設計フェーズについて詳しく説明する。トピックと範囲の決定、目標の明確化、参加者とトレーニングスタッフの選定、実行計画の調整について取り上げる。セクション 5 およびセクション 6 では、それぞれ機能演習とテストについて同様の情報を提供する。

この文書には、付録も含まれている。付録 A、付録 B、付録 C は、順に机上演習、機能演習、テストに関する文書のサンプルである。付録 D は用語集、付録 E は頭字語の一覧である。付録 F は、TT&E イベントの範囲決定、計画作成、文書化、実施、評価に役立つ印刷物とオンライン情報を紹介している。付録 G には、この文書の索引を示す。

2. テスト、トレーニング、演習プログラムの確立

組織の IT 計画は、その活動に影響を及ぼすような災害に備え、対応能力、管理能力、復旧能力を組織が維持できるよう管理する必要がある[2]。この目的のために利用される IT 計画は、主に次の 2 種類がある。

- 緊急時対応計画：IT システムの復旧と再構成[3]。緊急時対応計画には、運用継続計画、事業継続計画、災害復旧計画が含まれる。
- インシデント対応計画：コンピュータセキュリティインシデントについての報告と管理[4]。

緊急時対応計画とインシデント対応計画の維持に用いられる主なイベントは、次のとおりである。

- **テスト。***テスト*は、定量化可能な測定基準を用いて、IT 計画に指定されている運用環境において IT システムまたはシステム構成要素の運用性を検証するための評価手段である。[5]。たとえば、組織であれば、所定の時間内に連絡網によって、全員に連絡が行きわたるかどうかをテストしたり、システムやシステム構成要素から電源を抜いてどうなるかをテストしたりすることが可能である。定量化可能な測定基準は、テストの対象となるシステムまたは構成要素（およびテストの対象となるシステムの構成要素）とテストの全体的な目標を明記した*テスト計画*を作成することで決められる。テストの結果、構成要素やシステムが誤作動したり、動作不能になったりした場合、それは担当者のトレーニングにおける問題や IT 計画・IT 手順に存在する問題を示している可能性がある。テストは、復旧やバックアップの作業を対象とすることが多いが、テストの内容は、テスト自体の目標や特定の IT 計画との関係に応じて変化する。セクション 6 で、テストについて詳しく説明する。
- **トレーニング。**このガイドでは、*トレーニング*とは、担当者に対し、特定の IT 計画における担当者の役割と責任（意志決定など）を伝達し、それらの役割と責任に関連する技能を教えることのみを指すものとする[6]。トレーニングは、IT 計画に関連する演習、テスト、そして実際の緊急事態に担当者が臨むための準備である。演習やテストに先立って実施される、役割と責任に関する担当者のトレーニングは一般に、役割と責任に関する発表と、担当者がトレーニング内容を理解したことを確認するための活動とに分けられる。セクション 3 では、トレーニングイベントの概要について簡単に取り上げている。トレーニングイベントについては、他の NIST 刊行物ですでに詳しく解説している。
- **演習。***演習*とは、緊急事態のシミュレーションのことで、IT 計画の 1 つ以上の側面について、その実行性を検証することを目的とする。演習は、IT 計画・IT 手順におけるギャップや矛盾点はもちろん、担当者に追加のトレーニングが必要となる状況やトレーニング内容の変更が必要な場面を明らかにするのに役立つ。演習では、ある特定の IT 計画で役割と責任を

---

2 組織は、インシデント対応能力など、計画内に必ずしも文書化されない IT 能力を維持する必要もある。わかりやすさを考慮し、このガイドでは「IT 計画・IT 能力」とせず、「IT 計画」と表記する。

3 緊急時対応計画に関する追加情報は、NIST SP 800-34『IT システムにおける緊急時対応計画ガイド（Contingency Planning Guide for Information Technology Systems）』に記載されている。

4 インシデント対応に関する追加情報は、NIST SP 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（Computer Security Incident Handling Guide）』に記載されている。

5 「テスト」および「演習」という用語は同じ意味で用いられることが少なくないが、この 2 つの用語には違いがある。本書の目的上、「テスト」という用語はシステムまたはシステム構成要素を対象とするテストの場合に使用し、計画実施の「演習」を表す場合には使用しないものとする。

6 トレーニングイベントは、本書に取り上げられていない種類のものも数多く存在する。一部については、NIST SP 800-16『Information Technology Security Training Requirements: A Role- and Performance-Based Model』および SP 800-50『IT セキュリティの意識向上およびトレーニングプログラムの構築（Building an Information Technology Security Awareness and Training Program）』で詳しく解説している。どちらの文書も http://csrc.nist.gov/publications/nistpubs/index.html より入手できる。

与えられている担当者が集まり、緊急事態における役割と対応に関する議論、シミュレーション用運用環境における対応策の実施、そして担当者の配置に関して実際の運用環境を用いずに対応策の有効性を確認するその他の手段を通じて計画の内容の有効性を検証する。演習は、組織が利用するデータセンタでの停電やシステムの損傷につながる火災など、シナリオに基づいて実施され、演習を進めるなかで何らかの状況設定が追加されることも多い。演習にはいくつかの種類があるが、本書では、単一の組織が TT&E プログラムで広く用いている、次の 2 種類を取り上げる[7]。

- **机上演習。***机上演習*は、議論ベースの演習で、担当者が会議室に集まったり、その場でグループを作ったりして、緊急時の役割や、ある特定の緊急事態への対応策を議論する形をとる。進行者はシナリオを提示し、それに関する内容を演習の参加者に質問する。質問をきっかけに、役割、責任、連携、意志決定について参加者間で議論を開始する。机上演習は、議論ベースのみの演習であり、設備やその他のリソースの配置を要しない。セクション 4 で、机上演習について詳しく説明する。
- **機能演習。***機能演習*を実施することで、担当者はシミュレーション用運用環境のなかで、緊急時のための運用面の備えを検証できる。機能演習は、IT 計画における、1 つ以上の機能的側面（通信、緊急事態の通知、IT 設備の設定など）に関わりのある、特定のチームメンバ、手順、および資産についての役割と責任の演習を行うことを目的とする。機能演習の複雑さと範囲は、計画の特定の側面の有効性確認から、計画の全要素を対象とした全面的な演習に至るまで、さまざまに異なる。機能演習を実施することで、スタッフは実際の緊急事態における役割と責任を、シミュレーション環境のなかで実践することが可能となる。セクション 5 で、機能演習について詳しく説明する。

テスト、トレーニング、演習を、何の連携もなしに独立した活動として実施することは可能だが、これら 3 つは互いに密接に関連しているため、この 3 つをまとめて扱うプログラムを整備することを組織として検討すべきである。たとえば、演習とテストを実施することにより、IT 計画、手順、トレーニングにおける問題を特定するさまざまな方法が得られる。効果的な TT&E プログラムは、トレーニング、演習、およびテストの各イベントの組合せで構成されるべきである[8]。プログラムには、TT&E 計画、ポリシー、イベント方法論、手順を含める。これらの要素を用いることで、TT&E イベント実行の一貫性と効果が高まり、特に作業の重複を減らせる。さらにプログラムは、リソースと予算の要件も取り上げ、TT&E の各イベントの実施スケジュールを示すべきである。このセクションでは、TT&E プログラム作成の手順について説明する[9]。

組織が作成した IT 計画の種類に関係なく、組織は IT 計画の実効性を検証し、計画が維持されるよう管理するための仕組を持つ必要がある。TT&E プログラムを確立しようとする組織はまず、IT 計画における役割と責任についての担当者のトレーニング、IT 計画の有効性を検証するための IT

---

7 演習の分類の仕方は、数多く存在する。たとえば、「机上演習」を議論ベースの演習全般を指すために用いる場合もあれば、ある特定の種類の議論ベースの演習を指すのに用い、それ以外の演習（トレーニングの講義とグループディスカッションを合わせた「セミナー演習」など）には別の用語を用いる場合もある。同様に、「機能演習」という用語は、運用のシミュレーションを行う演習を表す一般用語として考えることもできる一方、特定の種類の運用演習を表していて、他の種類の演習（上級管理職の意志決定に焦点を合わせた、機能演習によく似た「本部演習」など）には別の用語を用いる場合もある。本書で使用している定義は、絶対的なものではなく、以降、本書において演習について議論する場合の土台を提供するためのものである。他の種類の演習については、Homeland Security Exercise and Evaluation Program（HSEEP）Web サイト https://www.hseep.dhs.gov/で提供している文書を参照のこと。

8 「TT&E」は「テスト、トレーニング、演習（test, training, and exercise）」を表しているが、本書の以降のセクションでは、特に断りのないかぎり、1）トレーニング、2）演習、3）テストの順でこの 3 種類のイベントを取り上げる。これは、この 3 つのイベントが通常この順番で実施されるためである（担当者をトレーニングしてから演習に参加させるべきであり、演習は通常、テストより先に実施される）。

9 このセクションは、TT&E プログラムを作成する個人が、上位管理職による支持と支援を求め、それらを獲得出来ていることを前提としている。

計画の演習、および IT 計画の状況における IT 構成要素またはシステムの運用性を確認するためのテストの実施をそれぞれ確実に行うための手順の概要を示す TT&E 計画を作成するべきである。TT&E 計画では、プログラムを構成するすべての要素を要約し、プログラムに関連する情報を確実に文書化する必要がある。TT&E 計画の作成に加え、TT&E プログラム作成の他の主な手順は次のとおりである。

- 総合的なポリシーの作成
- 役割と責任の明確化
- 全体スケジュールの作成
- 方法の文書化

上記の手順については、2.1 項から 2.4 項にかけて詳しく説明する。

2.1 総合的な TT&E ポリシーの作成

TT&E プログラムには、担当者のトレーニング、計画の演習実施、構成要素とシステムのテストに関連する、組織の内部および外部の要求を含んだポリシーを盛り込むべきである。このポリシーは、プログラムの目的と目標の枠組みを形成し、該当する国の指針や組織内部の指針を引用するものである。ポリシーはさらに、TT&E イベントを組織がどのように構築し、管理するかを規定する枠組み、つまり「規則」を示すものである。このポリシーによって、TT&E イベントに関連するすべての文書を作成するための明確かつ一貫性のある枠組みが確立される。

TT&E ポリシー作成の主な手順は次のとおりである。

- 作成にあたっては、上級管理職の支援と関与を受ける。これは、上級管理職にプラグラムの内容、プログラムを成功に導くために必要なリソース、プログラム実施のメリットと必要性、そしてプログラム作成に関わる潜在的リスクを理解してもらうことを含む。
- 内部、外部を問わず、計画に関連するすべての文書（過去のトレーニング記録、組織のポリシー、連邦政府の指針、他の組織や業界のパートナーから得た実践情報）を明らかにする。
- 必要な文書をすべて収集し、それらを一箇所で一元管理する。

TT&E ポリシーに盛り込むことが推奨される要素は次のとおりである。

- 目的
- 発効日
- 目標
- 適用対象と範囲
- 権限および関連ポリシー
- 主要ビジネス部門および担当スタッフの職位ごとの役割と責任
- TT&E の要件
- TT&E の確認と承認
- 施行と遵守

- 関連情報の入手先
- 用語の定義

TT&E ポリシーの作成後は、新たな指針がプログラムに適用されたり影響したりしたときに、ポリシーステートメントを更新する。

2.2 TT&E における役割と責任の明確化

TT&E プログラムの監督と責任の主管部署は、組織の構造や要件に応じて異なる。多くの組織では、最高情報責任者室(OCIO: Office of the Chief Information Officer、以下 OCIO と称す)が TT&E プログラムの監督と責任を担っている。TT&E プログラムは、組織の IT 計画作成能力に関して直接の責任を有する人物またはチームが管理するべきである。TT&E プログラムでは、IT 計画作成のすべての側面(IT 計画の維持に関わる TT&E 要素を含む)について責任を担う *IT 計画コーディネータ*を置くべきである。IT 計画コーディネータは、作成、遂行、維持を含め、IT 計画について全体的な責任を負う。IT 計画コーディネータが担う責任の 1 つに、TT&E 計画の作成とイベントの調整を担当する *TT&E プログラムコーディネータ*の指名がある。TT&E イベントの計画を立て、実施するために、TT&E プログラムコーディネータはイベントの設計チームと連携する。組織は、必要に応じて専用のソフトウェアを購入したり、担当チームの結成または要員調達のために外部の協力を求めたりしてもよい。セクション 4 からセクション 6 にかけては、各イベントの設計チームとチーム内の役割について解説する。

2.3 TT&E の全体スケジュールの確立

TT&E 計画では、TT&E プログラムにおいて実施する活動のスケジュール案を文書化する。イベントは、必要に応じて実施するべきではあるが、組織ごとにイベントの求められる頻度を評価し、TT&E スケジュールに各イベントの頻度を文書化しておくべきである。たとえば、NIST SP800-53 では、少なくとも 1 年に 1 回、国の機関が、システムの緊急時対応計画とインシデント対応能力について演習やテストを実施することを要求している。セクション 4 からセクション 6 にかけて、組織固有の TT&E ニーズを評価する方法の詳細を記している。

2.4 TT&E イベント方法論の文書化

TT&E プログラム作成の一環として、組織は、TT&E イベントの計画と実行のための高いレベルの方法論を選択して文書化するべきである。図 2-1 は、よく利用される方法論の 1 つで、4 つのフェーズで構成されている。

- **イベントの設計。**TT&E プログラムコーディネータは、計画コーディネータと連携し、組織の最新の要望に基づいて TT&E イベントのトピックと範囲を決定する。決定するトピックとしては、IT 計画における個々の役割と責任に関する担当者のトレーニング、対応手順の演習、個別システムのテストなどがあげられる。次に、TT&E プログラムコーディネータは、トピックと範囲に基づいて目標を明確にし、イベントに参加すべき担当者を決定する。TT&E プログラムコーディネータは、イベント設計チームも決定する。イベント設計チームは、イベントの要件に応じて、1 人の場合もあればグループの場合もある。TT&E プログラムコーディネータは、イベントの実行計画を管理する。たとえば、文書の印刷、部屋の準備、食事や AV 機器の準備などを管理する。
- **イベント文書の作成。**設計フェーズが完了したら、TT&E プログラムコーディネータは設計チームと連携して、イベント前、イベント中、イベント後に使用する文書を作成する。文書の種類はイベント毎に異なるが、概要説明資料、参加マニュアル、インストラクタおよび進行者用ガイド、テスト計画とスクリプト、評価基準などの文書を作成する。

- **イベントの実施。**このフェーズでは、イベント（トレーニング、演習またはテスト）を実際に行う。実施の詳細は、イベントの種類と範囲によって大幅に異なる。
- **イベントから得られた教訓の評価。**評価フェーズは、イベントを分析し、得られた教訓を明確にして、IT 計画とその実行を改善し、TT&E プロセスを改善するためのものである。評価の方法は、以下に示すように、イベントの種類によって多少異なる。
  - トレーニング（Training）：参加者は通常、イベントの成否、およびトレーニングの主題に関し担当者の知識を強化する余地のある部分について、評価・意見を用紙に記入する。こうして得たフィードバックを分析し、トレーニング分析レポートとして文書化する。また、必要に応じて今後のトレーニングに修正を加える。
  - 演習またはテスト：参加者は通常、*ホットウォッシュ*と呼ばれる、反省会に参加し、特にうまくいった部分と、計画の内容やテスト対象のシステムに関し強化の余地がある部分について議論する。反省会で明らかになった事柄、イベント中の所見、強化のための検討事項を事後レポートとして文書化する。

各フェーズの詳細は、実施するイベントの種類によって異なるが、どのイベントでも同じフェーズを経るべきである。各イベントの詳細については、セクション 4 からセクション 6 で紹介している。

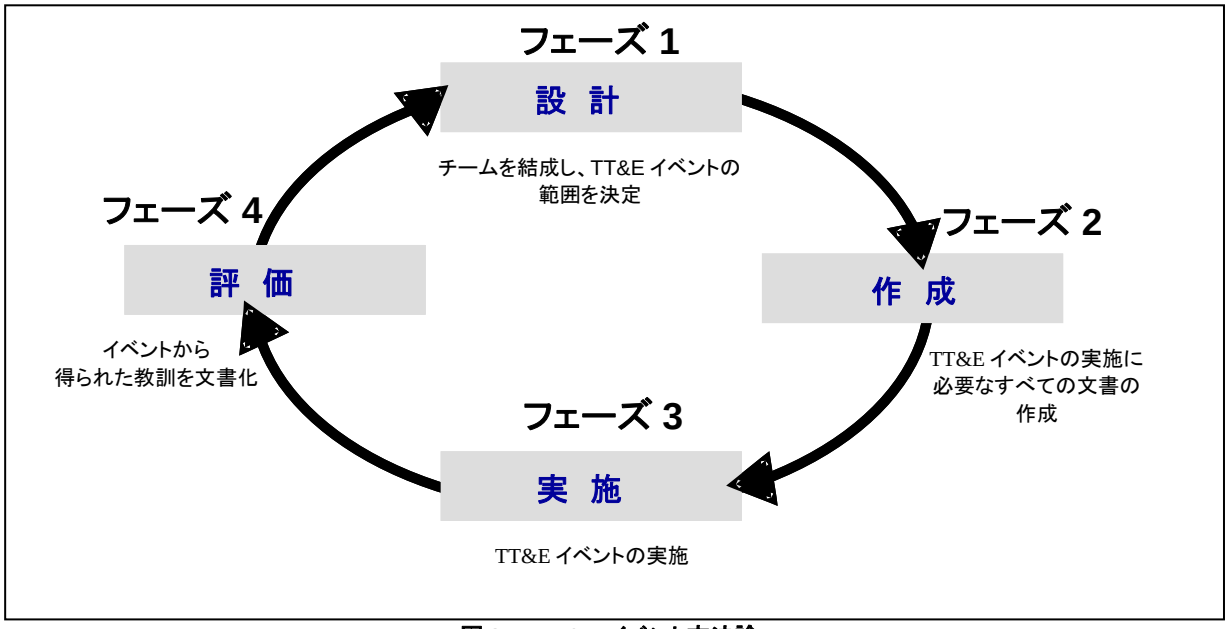

図 2-1 TT&E イベント方法論

2.5 推奨事項

組織は、緊急時対応計画やコンピュータセキュリティインシデント対応計画などの IT 計画の有効性を確認し、計画を維持するための TT&E プログラムの整備を検討すべきである。TT&E プログラムには、TT&E 計画、ポリシー、およびイベント方法論が含まれている必要がある。これらの要素を用いることで、TT&E イベント実行の一貫性と効果が高まる。TT&E 計画では、プログラムを構成するすべての要素を要約し、プログラムに関連する情報を確実に文書化する必要がある。TT&E 計画の作成に加え、TT&E プログラム作成の他の主な手順は次のとおりである。

- **総合的な TT&E ポリシーの作成。**このポリシーでは、担当者のトレーニング、計画の演習実施、構成要素とシステムのテストに関連する、組織の内部および外部の要求をまとめるべきである。

- **TT&E における役割と責任の明確化。**TT&E プログラムは、組織の IT 計画作成能力に関して直接の責任を有する人物またはチームが管理するべきである。TT&E プログラムでは、IT 計画作成のすべての側面（IT 計画の維持に関わる TT&E 要素を含む）について責任を担う計画コーディネータを置く必要がある。計画コーディネータは、作成、遂行、維持を含め、TT&E 計画について全体的な責任を負う。計画のコーディネータは、TT&E 計画の作成とイベントの調整を担当する TT&E プログラムコーディネータを指名する。実施するイベントの種類に応じて、TT&E プログラムコーディネータは、1 つ以上の設計チームと連携して作業を行う。

- **TT&E の全体スケジュールの確立。**TT&E 計画では、TT&E プログラムにおいて実施する活動のスケジュール案を文書化する。イベントは、必要に応じて実施するべきではあるが、組織ごとにイベントの求められる頻度を評価し、TT&E スケジュールに各イベントの頻度を文書化しておくべきである。

- **TT&E イベント方法論の文書化。**TT&E プログラム作成の一環として、組織は、TT&E イベントの計画と実行のための高いレベルの方法論を選択して文書化するべきである。各フェーズの詳細は、実施するイベントの種類によって異なるが、どのイベントでも同じフェーズを経るべきである。よく利用される方法論の 1 つは、次の各フェーズで構成される。

  – **設計。**TT&E プログラムコーディネータは、計画コーディネータと連携し、組織の最新の要望に基づいて TT&E イベントのトピックと範囲を決定する。次に、TT&E プログラムコーディネータは、トピックと範囲に基づいて目標を明確にし、イベントに参加すべき担当者を決定する。TT&E プログラムコーディネータは、イベント設計チームを決定する。イベント設計チームは、イベントの要件に応じて、1 人の場合もあればグループの場合もある。TT&E プログラムコーディネータは、イベントの実行計画も監督する。

  – **作成。**TT&E プログラムコーディネータは設計チームと連携して、イベント前、イベント中、イベント後に使用される文書を作成する。作成する文書としては、概要説明資料、参加マニュアル、評価基準などがあげられる。

  – **実施。**このフェーズでは、イベントを実施する。すなわち、担当者のトレーニング、IT 計画の演習、システムやシステム構成要素のテストを執り行う。実施フェーズの詳細は、イベントの種類によって大きく異なる。

  – **評価。**評価フェーズは、イベントを分析し、得られた教訓を明確にして、IT 計画とその実行および TT&E プロセスの両方を改善するためのものである。

3. トレーニングセッション

トレーニング とは、継続的な学習活動のことで、スタッフが自らの技能や技術力を維持、強化したり、最新の技術を習得したりすることを目的とするものである。この文書の目的をふまえ、トレーニングとは、参加者にある特定の IT 計画における役割と責任を伝達し、その役割と責任に関わる技能を教えて、計画に関連する演習やテストへの参加の準備、および実際の緊急事態への対処のための準備を整えさせることのみを指すものとする。[10]。トレーニングイベントは、インストラクタ主導型（教室形式やオンライン対話形式など）または自習型（学習プリントやオンライン画面などを使用）が可能である。

IT 計画を支えるトレーニングイベントのスケジュール設定は、TT&E プログラムの他のイベントのスケジュールとの間で綿密に調整する必要がある。たとえば、トレーニングセッションは通常、演習やテストよりも先に行う。これにより、IT 計画において割り当てられる役割と責任を把握してから、計画そのものの演習を行うことができる。トレーニング実施がもたらすもう 1 つの効果は、さらにトレーニングが必要な部分を明らかにできることである。

すでに発表済みの他の NIST 文書において、トレーニングプログラムおよびトレーニングイベントを詳しく取り上げている。トレーニングの詳細については、NIST SP 800-50『*IT セキュリティの意識向上およびトレーニングプログラムの構築（Building an Information Technology Security Awareness and Training Program）*』および NIST SP 800-16『*Information Technology Security Training Requirements: A Role- and Performance-Based Model*』を参照のこと[11]。

[10] トレーニングイベントのメリットの詳細については、NIST SP 800-50『*IT セキュリティの意識向上およびトレーニングプログラムの構築（Building an Information Technology Security Awareness and Training Program）*』を参照のこと。この文書は http://csrc.nist.gov/publications/nistpubs/index.html より入手できる。

[11] どちらの文書も http://csrc.nist.gov/publications/nistpubs/index.html より入手できる。

（本ページは意図的に白紙のままとする）

4. 机上演習

机上演習は、議論ベースのイベントで、特定の IT 計画における役割と責任を与えられた担当者が会議室に集まったり、その場でグループを作ったりして、緊急時の役割や、ある特定の緊急事態への対応策を議論する形をとる。机上演習は、形式ばらない環境で実施し、進行者が、あらかじめ定められた目的を達成するために参加者の議論を導く。1 回の机上演習につき、1 つのシナリオを議論する場合もあれば、複数のシナリオを取り上げる場合もある。机上演習の所要時間（通常 2～8 時間）は、対象者、演習のトピック、演習の目標によって異なる。机上演習は、緊急時対応計画やインシデント対応計画などの IT 計画の内容の有効性を確認し、計画内容が緊急時に確実に活用でき、実行可能であるようにするためのコスト効率の高い手段である。

このセクションでは、机上演習の必要性の有無についての判断基準、そして机上演習の設計、作成、実施、評価に関する指針を示す。その後、机上演習の実施前、実施中、実施後に検討すべき重要な要素をまとめている。付録 A は、机上演習の進行者用ガイド、参加者ガイド、事後レポートのそれぞれのサンプルを掲載している。

4.1 机上演習の必要性の判断およびスケジュールの作成

TT&E プログラムの一環として、プログラムコーディネータは、机上演習の実施における組織全体の目標を検討したり、以下の質問に回答したりすることで、特定の IT 計画の机上演習の必要性を定期的に判断するべきである。

- 机上演習に参加する担当者は、計画における自身の役割と責任に関するトレーニングをすでに受けているか。担当者がまだトレーニングを受けていない場合、TT&E プログラムコーディネータは、担当者が、より効果的に机上演習に参加でき、その有効性を高めるために、机上演習実施前にトレーニングイベントの実施を検討するべきである[12]。
- その計画について、組織が机上演習を最後に実施したのはいつか。
- 計画の内容に影響が及ぶ可能性のある組織上の変更が最近あったか。
- 計画の内容に影響が及ぶ可能性のある新たな TT&E 指針が発行されたか。

組織は、組織の変更や IT 計画の改定、新たな TT&E 指針の発行、その他の必要性に応じて、机上演習を定期的に実施するべきである。プログラムコーディネータは、机上演習ごとに、明らかにされた要望と目標に適した形式の机上演習を選択する必要がある。机上演習のスケジュールは、TT&E プログラムの他のイベントのスケジュールとの結び付きを考慮して調整する。TT&E プログラムコーディネータは通常、トレーニングイベント実施後の適切な期間内に机上演習のスケジュールを設定し、机上演習の参加担当者がその役割と責任についてトレーニングを受けてから時間が経過しすぎないようにする。演習のスケジュールが決定したら、管理責任者に通知し、承認を得ることが重要である。演習実施について管理責任者の同意を得ることは、演習イベント作成における重要なステップである。

4.2 机上演習イベントの設計

机上演習実施の必要性が確認されたら、TT&E プログラムコーディネータは、机上演習設計チームと連携して、演習イベントの設計を行う。設計フェーズは、机上演習の計画において最も時間のかかるフェーズであることが多い。計画は通常、大規模で複雑な演習の場合は実施日の少なくとも 3

[12] 組織によっては、机上演習の直前にトレーニングセッションを実施し、机上演習とトレーニングをひとまとめにした方がコスト効率が高いと判断する場合もある。

か月前、それほど複雑でない演習の場合は少なくとも 1 か月前に作成を開始する。4.2.1 項から 4.2.6 項では、演習設計プロセスの主な手順を示す。

4.2.1 トピックの決定

設計チームは、計画内容のうち演習の中心となる内容に基づいて演習トピックを決定する必要がある。総合トピックとしては、緊急時対応計画やインシデント対応計画が挙げられる。具体的トピックとしては、必須機能の維持から IT セキュリティインシデントへの対処と報告にいたるまで、さまざまなトピックが考えられる。たとえば、災害復旧計画の演習における議論のトピックであれば、組織の情報システム復旧のためのプロセスや手順に関わる担当者の役割と責任などが挙げられる。インシデント対応計画の演習における議論のトピックであれば、IT セキュリティインシデントへの対処と報告を行うプロセスや手順があげられる。

4.2.2 範囲の決定

机上演習の範囲は、対象者が誰であるかに基づいて決定する。IT 計画において責任が与えられている担当者は、全員が参加するべきであるが、管理職のチームと業務担当者のチームは、それぞれ責任のレベルが異なるため、最初の段階では、別々に机上演習を実施するのがよい。これら 2 つのチームがそれぞれ個別に演習を行ったら、両チームが合同演習に参加し、チーム間の連携を検証する。

演習は、演習実施対象の IT 計画における担当者の役割と責任に注目し、文書に明記されている役割、責任、依存関係が正確で最新のものであるかどうかの検証に重点を置く。演習実施時に参加者に尋ねる質問の種類は、演習の対象となっている参加者のレベルに合わせる必要がある。管理職の机上演習は通常、2～4 時間を要するが、業務担当者の机上演習の場合は 2～8 時間と幅がある。演習実施対象の計画に明記されている役割と責任について、確実に最新の内容を知るようにするために、4 時間を超える机上演習については、トレーニングセッションを併せて実施すると効果的であることが多い。

4.2.3 目標の決定

机上演習では、IT 計画および関連のポリシーと手順の内容の検証、計画に示されている参加者の役割と責任の検証、そして計画に明記されている依存関係の確認を目標とするべきである。演習のその他の目的としては、計画の演習に関連する規制やその他の要件を満たすことがあげられる。たとえば、NIST SP 800-53 では、連邦政府機関はシステムの緊急時対応計画について少なくとも年 1 回、演習またはテストを実施することを要件としている。

4.2.4 参加者の決定

設計チームは、演習のトピック、範囲、目標に基づき、演習参加者を決定する[13]。演習によって所定の目標を達成するために、参加者は、計画に明記されている役割と責任を持つ担当者で構成されるべきである。たとえば、管理職は、計画における意志決定プロセスや監督プロセスの検証が演習の主目的である場合は、参加を要請するべきである。主目的が運用手順の検証である場合は、業務担当者に演習への参加を要請する。両グループが机上演習を別々に実施済みである場合、合同セッションを実施することが推奨される。合同セッションでは、管理職と業務担当者が個人やチームの役割と責任、連携の要件について議論する。適切な参加者が明らかになったら、できるだけ速やかに演習への参加案内を書面で送付したり、通知したりする。これは通常、机上演習の設計チー

[13] 演習で達成しようとしている要件によっては、指名した人物の参加が必須となる場合もある。

ムの担当者が電子メールまたは書面によって伝達する。あるいは、いずれかの管理職から配布することが適切な場合はそれでもよい。

4.2.5 机上演習スタッフの決定

設計チームは通常、演習の進行者とデータ収集担当者を指名する。進行者は、演習参加者間の議論を促し、データ収集担当者は、演習時の活動に関する情報を記録する。進行者とデータ収集担当者は、演習対象の IT 計画と演習の目標を熟知していなければならない。そして、進行者とデータ収集担当者は、机上演習の前に、演習の範囲や目標を含め、演習に関する詳細について打ち合わせをするべきである。演習前の打ち合わせでは、進行者とデータ収集担当者は、以前の机上演習（実施されていた場合）の結果を確認して、問題発生の可能性をあらかじめ認識しておくようにする。

4.2.6 実行計画の調整

通常、設計チームのうちの 1 名が演習イベントの実行計画を調整する役割を担う。実行計画コーディネータは通常、机上演習実施の少なくとも 1 か月前から調整作業に着手する。表 4-1 のチェックリストは、実行計画コーディネータが、必要な作業が完了しているかどうかを確認するためのたたき台として使用できる。

表 4-1 机上演習イベント用実行計画チェックリストのサンプル

実行計画の内容	期限	完了
演習の実施日時の選定		
全参加者を収容できる会議室の予約		
AV 設備使用の有無の決定		
AV 設備の予約（必要な場合）		
進行者とデータ収集担当者の決定		
参加者の決定		
参加要請の実施		
進行者用ガイドと参加者ガイドの作成に関する調整		
名札印刷の手配		
演習の準備に必要な時間を含めた、会議室の利用時間の確認		
飲みもの、軽食の手配（必要な場合）		
すべてのファイルを CD-ROM や USB メモリなどのリムーバブルメディアにコピーしてバックアップを作成		

4.3 机上演習用資料の作成

イベントの設計が完了したら、設計チームはそのメンバーに役割と責任を割り当て、机上演習の資料を作成する。机上演習では通常、以下の文書を作成する。

- **概要説明。**概要説明資料は、参加者向けに作成する。本資料には、演習の予定と実行計画に関する情報を記載する。
- **進行者用ガイド**。進行者用ガイドには、以下の情報を記載する。
  - 演習実施の目的
  - 演習の範囲と目標

- 演習のシナリオ。仮想のインシデントを、順を追って説明するストーリーとして構成したもの。演習用の状況設定を定め、対応が必要となる状況を創り出し、演習の目標を実践できるようにすることを目的としている。
- シナリオに関連し、演習の目標に対応した質問のリスト[14]
- 演習の対象となる IT 計画のコピー

進行者用ガイドに記載する質問の種類は、参加者に合わせる必要がある。たとえば、参加者が管理職の場合の質問は、計画における役割と責任に沿って、より総合的で、俯瞰的なものにし、意志決定と監督に重点を置く。参加者が業務担当者が場合、通常、役割と責任を果たすために実行する特定の手順やプロセスに重点を置く。

- **参加者ガイド。**参加者ガイドには、質問のリストを除き、進行者用ガイドと同じ情報を記載する。参加者ガイドに記載する質問リストは、演習時に議論する可能性のある種類の問題に参加者の関心が向くよう手を加え、簡潔なものにする。
- **事後レポート。**事後レポートは演習イベント終了後に作成する。事後レポートには、あらかじめ定めておいた評価基準に基づく情報を記載する。評価基準は、演習前に作成しておき、データ収集担当者が演習中どのような種類の情報を収集して事後レポートに記載すればよいかわかるようにする。評価基準は、演習の目標に基づいて定め、演習の目標がどの程度達成されたかを評価し、さらなる演習が必要と考えられる部分を明らかにする手段とする。事後レポートについては、4.5 項でさらに詳しく説明する。

机上演習のサンプル文書は、付録 A に掲載してある。

よくある誤解は、シナリオをきめ細かく設定しなければ効果がないという認識である。実際には、短く簡潔なシナリオを作成する方がより効果的であることが多い。シナリオの設定が長く、細かな場合、机上演習中に参加者が演習の目標を達成することよりも、シナリオを分析して内容について議論したりすることに費やす時間が増えてしまうことが少なくない。詳細なシナリオが必要な場合、シナリオの精度を高めるために、計画および計画に示されているすべての手順について詳細な知識を有する信頼できる職員がシナリオの作成を支援するべきである。さらに、進行者は、参加者がシナリオの内容に意識を向けすぎている場合に、参加者の注目をシナリオから目標に向けるようにできなければならない。

4.4 机上演習の実施

机上演習は通常、会議室で実施する。これにより、進行者は演習を進行しながら、参加者 1 人 1 人にも参加者のグループにも対応することができる。また、会議室で実施する場合は、演習開始前に各参加者の席上に名札を置くことで、参加者間のコミュニケーションを促す。これは特に、参加者やチームが組織内の異なる業務領域で働いている場合に重要となる。参加者は通常、同じチームや部署の仲間とは隣り合わせに座らせず、思考プロセスを独立に行うことを促し、他の業務領域に触れることができるようにする。参加者ガイドは、各名札の横に置いておく[15]。

---

[14] 演習のシナリオおよび関連の質問リストのサンプルは、NIST SP 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(Computer Security Incident Handling Guide)*』および NIST SP 800-83『*悪意のソフトウエアによるインシデントの防止と対処のためのガイド(Guide to Malware Incident Prevention and Handling)*』に掲載されている。どちらの文書も http://csrc.nist.gov/publications/nistpubs/ より入手できる。

[15] 参加者は通常、演習実施日に参加者ガイドを受け取るが、参加者が演習のトピックをよく把握できるように、演習設計チームは、事前に参加者ガイドを配布してもよい。参加者ガイドを事前に配布する場合、演習の 1 週間前に配布するのが最も効果的である場合が多い。配布があまり早すぎると、演習の内容を忘れられてしまう可能性がある。また、演習日に近すぎても、参加者が参加者ガイドに目を通す時間をとれない可能性がある。

演習の開始時、進行者は参加者に対し、あいさつの言葉を述べた後、氏名と組織内での役割について簡単な説明を求める。次に、進行者は演習の概要を述べ、演習の範囲と実行計画の情報について説明する。さらに、参加者にシナリオを紹介し、進行者用ガイドに記載されている質問の 1 つについて話し合いを開始させ、意志決定や参加者間での意見調整を促す[16]。開始後、シナリオと目標に基づき、参加者間で自然と議論が始まる。進行者は、必要に応じて合間に進行者用ガイドの質問を挟む。議論が自然に始まらない場合、進行者はすべての目標が達成されるよう、進行者用ガイドに記載された補足の質問を行って議論を促す必要がある。演習のあいだ、データ収集担当者は事後レポートに記載する所見を記録する。

議論が終わったあとすぐ、進行者とデータ収集担当者は演習の反省会(「ホットウォッシュ」とも呼ばれる)を行う。反省会では参加者に対し、自分が優れていた部分、追加のトレーニングが必要な部分、および IT 計画の見直しが必要な部分について質問する。

4.5 机上演習の評価

反省会で出されたコメントは、演習時にデータ収集担当者が記録した演習の教訓とともに、事後レポートに記載する。事後レポートのはじめに、演習の目的や目標、参加者、シナリオなど、演習の背景情報について説明する。事後レポートには、進行者とデータ収集担当者による演習時の所見と、演習を行った IT 計画の強化につながる推奨事項も記載する。

事後レポート作成後、計画コーディネータは IT 計画を更新するために、担当者に宿題を割り当てることができる。計画コーディネータは、その場合、必要であれば事後レポートに記載された推奨事項を実施することで、計画を更新する。演習の結果について一部の管理職に概要を伝えたり、他のセキュリティ関連文書を改定したり、または演習に基づく他の行動を実行に移したりすることが必要な場合もある。

4.6 まとめ

机上演習は、議論ベースのイベントで、特定の IT 計画における役割と責任を与えられた担当者が会議室に集まったり、その場でグループを作ったりして、緊急時の役割や、ある特定の緊急事態への対応策を議論する形をとる。机上演習は、形式ばらない環境で実施し、進行者が、あらかじめ定められた目的を達成するために参加者の議論を導く。机上演習イベントの計画作成と実行によく利用される方法論の 1 つは、次の各フェーズで構成される。

- **設計。**TT&E プログラムコーディネータは、机上演習設計チームと連携して、演習イベントを設計する。設計フェーズは、しばしば最も時間を要し、演習の計画作成は少なくとも 1 か月前(複雑で大規模な演習の場合は 3 か月前)から開始する。イベント設計プロセスにおける主な手順は、次のとおりである。
  - 演習を行う対象となる計画の中心となる内容に基づいて、演習トピックを決定する。
  - 演習の対象者に基づいて、演習の範囲を決定する。
  - 演習の目標を決定する。
  - 演習に参加してもらう個人を決定し、演習への参加を要請する。
  - 演習のスタッフ(進行者とデータ収集担当者を含む)を決定する。

[16] 机上演習とトレーニングイベントを一緒に実施する場合、トレーナーはセッション開始時に、計画の概要、そして計画に参加する個人とチームの役割と責任について述べる。次に進行者進行者は、実践的活動を実施させてから、シナリオについて話し合いを開始して、議論を通じてチームで問題に取り組み、解決策をみいだすよう参加者を促す。

– 演習イベントの実行計画を調整する。

- **作成。**設計チームは、演習前、演習中、および演習終了後に使用する文書を作成する。通常、演習の概要説明、進行者用ガイド、参加者ガイド、事後レポートを作成する。
- **実施。**このフェーズでは、IT 計画を実際に試す。机上演習は通常、会議室で実施する。進行者は、参加者に概要を説明し、シナリオを流れに沿って一通り紹介し、進行者用ガイドの質問を利用してグループでの議論を開始させる。進行者は、議論を続けさせながら、必要に応じて追加の質問を挟む。データ収集担当者は、事後レポートに記載する内容を記録する。議論が終了したあとすぐ、進行者とデータ収集担当者は、演習の反省会を実施する。参加者に対し、自分が優れていた部分、追加のトレーニングが必要な部分、および IT 計画の見直しが必要な部分について質問する。
- **評価。**反省会で出されたコメントは、演習時に得られた教訓とともに、事後レポートに記載する。事後レポートには、演習に関する背景情報、進行者とデータ収集担当者による所見、そして演習を行った IT 計画の強化につながる推奨事項を記載する。評価の結果に基づき、IT 計画や他のセキュリティ関連文書を改定したり、結果について管理職に報告したり、その他の活動を行ったりする。

5. 機能演習

機能演習を実施することで、運用責任者は、シミュレーション用運用環境のなかで自らの責務を果たすことにより、IT 計画の検証、および緊急時のための運用面の準備状況を検証できる。機能演習に関する活動は、シナリオに基づいて実行される。たとえば、シミュレーション用環境において、あるビルの IT システムが利用できなくなり、参加者はそのビルに火災が発生していることを知る、というようなシナリオを利用する。演習時には、状況設定を追加してシミュレーションを行うことも多い。機能演習は、IT 計画における、1 つ以上の機能的側面（通信、緊急事態の通知、IT 設備の設定など）に関わりのある、特定のチームメンバ、手順、および資産に対する演習を行うことを目的とする。機能演習の複雑さと範囲は、計画の特定の側面の有効性確認から、計画の全要素を対象とした全面的な演習に至るまで、さまざまである。機能演習は、演習の目標、および演習の対象となる計画の複雑さに応じて、通常、数時間から数日間かけて実施する。

このセクションでは、機能演習の必要性の有無についての判断基準、そして機能演習の設計、作成、実行、評価に関する指針を示す。その後、機能演習の実施前、実施中、実施後に検討すべき重要な要素をまとめている。付録 B には、シナリオや追跡票、事後レポートなど、機能演習で使用する文書のサンプルを示す。

5.1 機能演習の必要性の判断およびスケジュールの作成

TT&E プログラムの一環として、プログラムコーディネータは、機能演習の実施における組織全体の目標を検討したり、以下の質問に回答したりすることで、特定の IT 計画の機能演習の必要性を定期的に判断するべきである。

- 機能演習に参加する担当者は、計画における自身の役割と責任に関するトレーニングをすでに受けているか。対象となる計画について、機能演習の基礎となる机上演習が実施済みかどうか。担当者がまだトレーニングを受けていない場合、または基礎となる机上演習がまだ実施していない場合、TT&E プログラムコーディネータはまず、機能演習実施前にトレーニングイベントと机上演習の実施を検討するべきである。これらを実施することにより、担当者はより効果的に機能演習に参加でき、その効果を高めることができる。
- その計画について、組織が機能演習を最後に実施したのはいつか。
- 計画の内容に影響を与えるような組織上の変更が最近、あったか。
- 計画の内容に影響が及ぶ可能性のある新たな TT&E 指針が発行されたか。

組織は、組織の変更や IT 計画の改定、新たな TT&E 指針の発行、その他の必要性に応じて、機能演習を定期的に実施するべきである。一般に、機能演習の前に、スタッフの十分なトレーニングと机上演習を実施しておくことが望ましい。機能演習のスケジュールは、TT&E プログラムの他のイベントのスケジュールとの結び付きを考慮して調整する。TT&E プログラムコーディネータは通常、机上演習実施後、妥当な期間内に機能演習のスケジュールを設定する。演習のスケジュールが決定したら、管理責任者に通知し、承認を得ることが重要である。演習実施について管理責任者の同意を得ることは、演習イベント作成における重要なステップである。

5.2 機能演習イベントの設計

機能演習実施の必要性が確認されたら、TT&E プログラムコーディネータは、機能演習設計チームと連携して、機能演習イベントの設計を行う。演習設計チームは、計画の内容に精通し、演習設計プロセスを促進することが可能な人物で構成する。機能演習の設計フェーズは通常、少なくとも実

施予定日の数か月前（演習の複雑さによって異なる）に開始する。5.2.1 項から 5.2.6 項では、演習設計プロセスの主な手順を示す。

5.2.1 トピックの決定

設計チームは、（たとえば、計画固有の要件に対応する、戦略的長期計画の一部として）IT 計画の演習における包括的な目標を決定する。これらの広範な目標は、演習で取扱われるトピックの範囲を表す。選択するトピックの範囲は、演習が計画全体を対象にするか、計画の特定の側面を対象にするかによって決まる。計画全体を対象とするトピックの範囲として、計画の手順の検証、組織の計画実施能力の評価、計画を実行する組織と要員の相互依存関係の評価などがあげられる。計画のある特定の側面を対象にするトピックの範囲としては、計画の警告と通知のプロセスの評価、計画の運用フェーズに関わる担当者の責任内容の検証、通常業務を再開するためのプロセスの評価などがあげられる。

5.2.2 範囲の決定

機能演習の範囲は、演習が IT 計画のどの部分（または全体）を対象としているかに応じて決定するべきである[17]。演習の対象が計画の一部だけの場合、設計チームは計画の遂行の特定のフェーズ（始動、運用、再構成など）または特定の機能の評価を検討するべきである。

機能演習の範囲を決定する際、設計チームは評価の対象となる、IT 計画の要素を明確にしてから、演習の実行に必要となる参加者のタイプを検討する。最終的には、しっかりした TT&E プログラムを作成することで、計画のすべての要素を試すが、初期の機能演習では運用チームの役割と責任に重点を置くことが多い。組織の TT&E プログラムが完成度を高めるのに従って、管理職も機能演習に参加し、計画の意志決定の側面をきめ細かく検証できる。

5.2.3 目標の決定

機能演習では、IT 計画の検証、計画に示されている参加者の役割と責任の検証、計画に示されている相互依存性の検証、そして参加者が自身の機能を実践的に訓練する機会の提供を目標とするべきである。演習のその他の目的としては、計画の演習に関連する規制やその他の要件を満たすことがあげられる。たとえば、NIST SP 800-53 では、連邦政府機関はシステムの緊急時対応計画について少なくとも年 1 回、演習またはテストを実施することを要件としている。個々の目標は、文書に記載し、演習参加者に明確に伝える必要がある。

5.2.4 参加者の決定

設計チームは、演習のトピック、範囲、目標に基づき、演習参加者を決定する[18]。演習によって所定の目標を達成するために、参加者は、計画に明記されている役割と責任を持つ担当者で構成されるべきである。たとえば、計画における意思決定プロセスや監督プロセスの研修が演習の主目的である場合は、管理職の参加を要請するべきである。主目的が運用手順の検証である場合は、業務担当者に演習への参加を要請する。最後に、主目的が計画全体の準備状況の検証である場合は、管理職と業務担当者の両方が参加する必要がある。適切な参加者が明らかになったら、できるだけ速やかに演習への参加案内を書面で送付したり、通知したりする。これは通常、機能演習の設計チームのメンバーが電子メールまたは書面によって伝達する。あるいは、管理職から配布する方が適切であれば、それでもよい。

---

[17] IT 計画全体を対象とする総合的な演習を、フルスケール演習と呼ぶこともある。

[18] 演習で達成しようとしている要件によっては、指名した人物の参加が必須となる場合もある。

5.2.5 機能演習スタッフの決定

設計チームは通常、*演習責任者*を指名する。演習責任者は、要員の確保、策定、実施、実行計画など、演習のあらゆる側面について責任を負う。演習責任者は、1 名以上の*演習管理者*(演習活動の監視、運営、管理を行う)、*データ収集担当者*(演習時に発生した活動の情報を記録する)、そして*シミュレーション担当者*(演習の進行に必要なインプットを提供する、演習に参加していない個人または組織の代理を務める担当者)を指名する。演習管理者、データ収集担当者、およびシミュレーション担当者は、演習対象の IT 計画と演習の目標を熟知していなければならない。

そして、演習責任者、演習管理者、データ収集担当者、およびシミュレーション担当者は、演習前に、演習の範囲や目標を含め、演習に関する詳細について打ち合わせをするべきである。演習前の打ち合わせでは、演習責任者、演習管理者、データ収集担当者、およびシミュレーション担当者は、以前の机上演習と機能演習(実施されていた場合)の結果を確認して、問題発生の可能性をあらかじめ認識しておくようにする。

5.2.6 実行計画の調整

通常、設計チームのうちの 1 名以上のメンバーが演習イベントの実行計画を調整する役割を担う。実行計画コーディネータは通常、機能演習実施のおよそ 3 か月前から調整作業に着手する。表 5-1 のチェックリストは、実行計画コーディネータが、必要な作業が完了しているかどうかを確認するためのたたき台として使用できる。

表 5-1 機能演習イベント用実行計画チェックリストのサンプル

実行計画の内容	期限	完了
演習の実施日時の選定		
演習を実施する施設の施設管理者との調整		
演習管理者、データ収集担当者、シミュレーション担当者の決定		
参加者の決定		
参加要請の実施		
演習管理者、データ収集担当者、シミュレーション担当者、および参加者が使用する文書の作成に関する調整		
演習時に役割をわかりやすくするため、演習管理者、データ収集担当者、シミュレーション担当者の名札印刷の手配		
移動や宿泊に関する手配(必要な場合)		
演習場所の必要な設備が利用可能であり、機能が正しく設定されていることの確認		
飲みもの、軽食の手配(必要な場合)		
電源タップ、延長コード、マーカ、テープなどの品目を記載した備品チェックリストの作成		
すべてのファイルを CD-ROM や USB メモリなどのリムーバブルメディアにコピーしてバックアップを作成		

5.3 機能演習用資料の作成

イベントの設計が完了したら、演習責任者は設計チームのメンバーに役割と責任を割り当て、機能演習の資料を作成する。機能演習では通常、以下の文書を作成する。

- **概要説明。**概要説明または概要説明書は通常、参加者と演習スタッフ向けに作成する。概要の説明は、対象者に直接行う場合と、事前に概要を配布しあらかじめ目を通しておいてもらう場合がある。演習の性質に応じて、1 回または複数回の概要説明を実施する。1 回の場合は、演習の約 1 週間前に実施する。複数回の場合は、演習までの各月や各週に行い、演習の少なくとも 1 週間前までに最後の概要説明を実施する。概要説明書には、演習の範囲と目標、守るべき規則、および演習イベントの管理的側面に関する情報を記載する。さらに、演習スタッフに対して概要説明を行い、演習イベントの運営面、シミュレーションを行う活動のレベル、および参加者の行動に応じて生じる活動のレベルに関する情報を提供する。

- **シナリオ。**シナリオは、参加者が演習の目標を達成しやすいように、対応が求められるような状況を演出して、演習に現実味を加えるように作成する。選択されたシナリオは、設計フェーズで選択した広範なトピック部分と具体的な目標を十分網羅していなければならない。さらに、演習の作成担当者は、シナリオが演習の範囲を逸脱しないよう注意しなければならない。演習のシナリオは、最悪の状況を試すよう作成することもできるが、参加者が現実において遭遇し、対応する可能性の高い状況をシナリオとして作成すると有用である。たとえば、自然災害が原因で業務中断に見舞われる可能性のある組織向けの IT 緊急時対応計画の演習では、ハリケーンが原因で大規模な停電が発生するシナリオを検討してみるとよい。物語形式のシナリオを文書化し、通常、参加者に資料として配付するか、演習当日に口頭で説明する。

- **マスタシナリオイベントリスト（MSEL：Master Scnenario Event List）。**MSEL は、参加者が演習時に対応を求められることになる、シミュレーションイベントおよび主要イベントの内容を時系列に従って一覧にしたものである。また MSEL には、これらイベントの結果として期待される行動のリスト、およびイベントを拠り所として達成すべき目標を記載する。MSEL は、参加者の行動を調整し、イベントのスケジュールを定めることで、シミュレーションイベントを統制する。MSEL の計画は注意深く行い、主要イベントによって演習目標が達成され、すべての参加者がイベントの間、活動し続けられるようにする。MSEL は、演習内容の作成と演習の運営のためにだけ使用する。

- **投入メッセージ。**投入メッセージは、インプリメンタまたは投入イベントとも呼ばれ、演習中参加者に示される、あらかじめ用意されているメッセージのことである。たとえば、「システムの復元が必要な現場にバックアップテープを運ぶ車両が渋滞につかまり、当初の予定より 3 時間遅れで到着する見込みである」というようなものが投入メッセージである。投入メッセージの伝達は、電子メール、手紙、メモ、電話連絡、無線連絡など、さまざまな形式が考えられる。それぞれの投入メッセージには、シナリオを補完し、追加の行動を促す情報が含まれる。投入メッセージは、MSEL に示される主要イベントの概略を展開するものである。そのため、MSEL の 1 つの項目に対し複数の投入メッセージが対応する場合もある。投入メッセージの目的は、シナリオ全体と MSEL の流れに沿ったものであり、最終的に、演習の目標達成につながる行動を参加者に促すところにある。投入メッセージは、メッセージを投入する時刻、メッセージを伝える相手、メッセージの発信者、メッセージの伝達手段（FAX、電話、電子メールなど）、そして実際のメッセージ本文で構成される。選択する投入メッセージの数は、参加者に余裕を与えない数にする。ただし、参加者が困惑するほど多くならないように注意する。そのため、選択する投入メッセージの数は、演習の所要時間によって異なる。

- **投入メッセージ追跡票。**投入メッセージ追跡票には、投入番号、メッセージ投入の予定時刻、メッセージ投入の実際の時刻、メッセージの要約、そしてメッセージを投入する担当者へのコメントを記載する[19]。

[19] 投入メッセージおよび投入メッセージ追跡票は、MSEL の文書に含まれる場合もある。

- **演習管理者、データ収集担当者、シミュレーション担当者の資料。**これらの資料には、演習スタッフに関係のあるすべての情報を記載する。演習管理者、データ収集担当者、シミュレーション担当者は通常、演習時の役割に関する情報を記載した資料を演習日（または、適切と考えられる場合は概要説明の日）に受け取る。資料には、演習のシナリオ、MSEL、投入メッセージを含める。

- **事後レポート。**事後レポートは演習イベント終了後に作成する。事後レポートには、あらかじめ定めておいた評価基準に基づく情報を記載する。作成フェーズでは、演習の実施中にデータ収集担当者が使用することになる演習の評価基準を決定し、文書化することも重要となる。評価基準は、演習の目標との関連性を重視して作成し、データ収集担当者が演習中に記録し、最終的に事後レポートに掲載する情報の種類を判断しやすいようにする。評価基準を作成したあとは、データ収集プロセスの役に立つ様式やその他のツールを作成するとよい。こうした様式は、データ収集担当者に対し、注目すべき担当者の特定の活動を指示する。また、特定の演習目標が達成されたかどうか、どのように目標が達成されたか、演習の対象である計画にどのような改善が必要か、そしてどの部分で追加の演習が必要か、といった判断のロードマップとしても利用できる。事後レポートについては、5.5 項でさらに詳しく説明する。

機能演習のサンプル文書は、付録 B に掲載してある。

機能演習の資料作成では、先に述べた設計チームのメンバーに加えて、他の担当者の協力が必要となる場合がある。たとえば、精度を高めるために、IT 計画や関連の手順について詳細な知識を有する信頼できる職員が、シナリオや MSEL、投入メッセージの作成を支援できる。4.3 項で説明したように、参加者がシナリオそのもののあら探しに終始しないように、シナリオは多くの場合、短く、簡潔にするのが最も有効である。

5.4 機能演習の実施

機能演習は通常、リアルタイムに（または、リアルタイムに近い状態で）実施し、参加者が自分の役割と責任をできるかぎり現実と同じように実行するよう促す。機能演習は、電話または他の適切な手段により、特定の IT 計画の発動または遂行を、選択した人物に警告するところから開始することが多い。この警告を受け、計画に指定されている手段によって、通知を受けるすべての担当者への通知が行われる。通知のプロセスが完了すると、参加者は計画に記されている運用上の活動または意志決定活動の実行を求められる。演習の範囲に応じて、活動の範囲は、通知手続きの実施から、代替施設への展開、スタッフと設備を含むリソースの動員にまでおよぶ可能性がある。展開または動員をシミュレーションで行うか、実際に行うかは、演習の範囲によって決まる。参加者は、居場所に関係なく、演習対象の計画に従って、割り当てられている活動を実行に移す。演習における人為的要素については、演習の概要説明時に参加者に伝える必要がある。

演習管理者、データ収集担当者、およびシミュレーション担当者は、演習の実施場所に事前に配置する。演習管理者は、コントロールセル（演習の調整を行う中心的な場所。通常、演習参加者から離れた場所に配置）を設置する。演習参加者は、コントロールセルからシナリオと投入メッセージを参加者に伝える。演習管理者は、投入メッセージ追跡票と MSEL を参照し、演習がスケジュールどおり、予定の範囲内で行われるよう監視する。

データ収集担当者は、演習の間、参加者の活動を直接観察する。データ収集担当者は、データ収集チームの作成した評価基準様式などの評価様式を参照する。シミュレーション担当者は、他の政府機関や一般市民、法執行機関など、演習イベントに参加していない内部および外部のさまざまな存在の役割を演じる。シミュレーション担当者が提供する情報は、シミュレーション対象の組織の方法に従って提供する。シミュレーション担当者は、演習管理者および演習責任者と綿密に連携して、

彼らの対応と MSEL との一貫性を確保する。さらには、演習管理者と同じ場所に配置したり、別の部屋に対応用の個室を設置したりしてもよい。演習中、演習責任者、演習管理者、データ収集担当者、およびシミュレーション担当者は相互に継続的に連絡を取り合い、演習の連携を保ち、スケジュールどおりに進行するよう努める。

演習責任者は、演習の終了をアナウンスする。一般に、演習に割り当てられた時間が経過した時点、すべての目標が達成された時点、または MSEL と投入メッセージがすべて演習で実行された時点で演習を終了する。演習中に現実の緊急事態が生じた場合は、演習責任者の責任で演習イベントをただちに中止する。演習の終了後すぐ、演習責任者、演習管理者、およびデータ収集担当者は参加者とともに演習の反省会(「ホットウォッシュ」とも呼ばれる)を行う。演習責任者は、反省会の推進役を務め、参加者、演習管理者、シミュレーション担当者、そしてデータ収集担当者にフィードバックを求める。反省会の終了直後、演習中と反省会のあいだに記入したメモや用紙を演習責任者に提出するよう、演習管理者、データ収集担当者、シミュレーション担当者、および参加者に求める。

5.5 機能演習の評価

評価フェーズでは、演習責任者が設計チームまたは他の指定の演習スタッフとともに、機能演習で明らかになった点や推奨事項をまとめた事後レポートを作成する。事後レポートは、演習中および反省会のあいだに作成されたメモ、様式、その他の資料を基にする。事後レポートのはじめに、演習の範囲や目標、シナリオなど、演習の背景情報についてまとめる。事後レポートには、演習時の演習スタッフと参加者による所見と、演習の対象となった IT 計画の強化につながる推奨事項も記載する。さらに、演習参加者のリストも含め、反省会時にフィードバックを得るために実施した参加者向けの調査で得た情報も必要に応じて掲載する。

事後レポート作成後、計画コーディネータは選択した担当者に活動項目を割り当てて、演習を実施した IT 計画を更新することができる。その場合、計画コーディネータは、必要であれば事後レポートに記載された推奨事項を反映することで、計画を更新する。演習の結果について一部の管理職に概要を伝えたり、他のセキュリティ関連文書を改定したり、または演習に基づく他の行動を実行に移したりすることが必要な場合もある。

5.6 まとめ

機能演習を実施することで、運用責任者は、シミュレーション用運用環境において、IT 計画の検証、および緊急時のための運用面の備えを検証できる。機能演習に関する活動は、シナリオに基づいて実行される。たとえば、シミュレーション用環境において、あるビルの IT システムが利用できなくなり、参加者はそのビルに火災が発生していることを知る、というようなシナリオを利用する。演習時には、状況設定を追加してシミュレーションを行うことも多い。機能演習は、IT 計画における、1 つ以上の機能的側面に関わりのある、特定のチームメンバ、手順、および資産に対する演習を行うことを目的とする。機能演習の複雑さと範囲は、計画の特定の側面の有効性確認から、計画の全要素を対象とした全面的な演習に至るまで、さまざまに異なる。

機能演習の計画作成と実行によく利用される方法論の 1 つは、次の各フェーズで構成される。

- **設計。**TT&E プログラムコーディネータは、機能演習設計チームと連携して、演習イベントを設計する。設計フェーズは通常、演習イベントの 3～6 か月前に開始する。イベント設計プロセスにおける主な手順は、次のとおりである。
  - IT 計画の演習を行う上で中心となる目標に基づいて、演習のトピックを決定する。
  - IT 計画のどの部分を対象に演習を行うかに基づいて演習の範囲を決定する。

- 演習の目標を決定する。
- 演習に参加してもらう個人を決定し、演習への参加を要請する。
- 演習責任者、1 名以上の演習管理者、データ収集担当者、シミュレーション担当者など、演習を実行するスタッフを決定する。
- 演習イベントの実行計画を調整する。

■ **作成。**設計チームは、演習前、演習中、および演習終了後に使用する文書を作成する。一般に、参加者と演習スタッフ向けの概要説明、シナリオ、MSEL（Master Scenario Events List：マスタシナリオイベントリスト）、投入メッセージと投入メッセージ追跡票、事後レポート、演習管理者向け資料、データ収集担当者向け資料、シミュレーション担当者向け資料を作成する。

■ **実施。**機能演習は通常、リアルタイムに（または、リアルタイムに近い状態で）実施し、参加者が自分の役割と責任をできるかぎり現実と同じように実行するよう促す。機能演習は、電話または他の適切な手段により、特定の IT 計画の発動または遂行を、選択した人物に警告するところから開始することが多い。参加者は、計画に記されている運用上の活動または、意志決定活動の実行を求められる。演習管理者は、参加者へのシナリオの説明や投入メッセージの提示を含め、演習を指揮する。データ収集担当者は、演習の間、参加者の活動を直接観察する。シミュレーション担当者は、外部の組織や一般市民など、演習イベントに参加していない存在の役割を演じる。演習責任者は、演習の終了をアナウンスする。演習責任者、演習管理者、およびデータ収集担当者は、演習直後に参加者と反省会を開き、演習スタッフと参加者からフィードバックを得る。

■ **評価。**反省会で出されたコメントは、演習時に得られた教訓とともに、事後レポートに記載する。事後レポートには、演習に関する背景情報、演習スタッフによる所見、そして演習を行った IT 計画の強化につながる推奨事項を記載する。評価の結果に基づき、IT 計画や他のセキュリティ関連文書を改定したり、結果について管理職に報告したり、その他の活動を行ったりする。

（本ページは意図的に白紙のままとする）

6. テスト

テストは、定量化可能な測定基準または予測される結果を用い、IT 計画内で重要と位置づけられている 1 つ以上の IT システムまたはシステム構成要素（オペレーティングシステム、アプリケーション、ページャ、Blackberry）の運用性を検証するための評価手段である[20]。テストは、以下に示すように、さまざまな形式で実施することができる。

- **構成要素テスト**は、ハードウェアやソフトウェアの個々の構成要素、または関連する構成要素のグループを対象に実行するテストである。構成要素テストは、組織の IT 計画の一部を構成しているプロセスや手順をテストする場合もある。ハードウェアおよびソフトウェアの構成要素は、完成した時点でのテストも実施されるが、そうしたテストは本文書の対象外である。この文書に登場する構成要素のテストは、組織を効果的に運営するために重要であり、定期的なテストが必要とされる、すでに運用されている個々の構成要素を対象とする。
- **システムテスト**は、システム全体が、指定された要件を満たしているかどうかを評価するためのテストである。システムテストでは、テスト対象のシステムに関連するプロセスや手順の調査も行う。
- **総合テスト**は、IT 計画に関わるすべてのシステムと構成要素を対象としたテストである。総合テストは一般に、複数の構成要素とシステムが対象となり、テスト範囲は非常に広くなる可能性がある。たとえば、メインのサイトにおける停電が長引いた場合に、バックアップサイトでの IT 業務の再開が可能であることを確認するテストが、総合テストの例として挙げられる。

テストは、できる限り運用環境に近づけて実施する。つまり、テストは、システムや構成要素が設置されている日常の作業環境を再現する形で実施する必要がある。可能であれば、組織の日常の業務遂行に用いられる構成要素やシステムを実際にテストすることが望ましい。テストの実施は、組織の業務を中断させる可能性がある。そのため、特にテストが何の問題も起こさずに完了するという強い確信が持てない場合は、実際の運用システムをコピーしたシステム上でテストを実施する場合もある。

このセクションでは、テストの必要性についての判断、テスト計画の作成、そしてテストの設計、作成、実施、評価に関する指針を示す。その後、テストの実施中および実施後に検討すべき重要な要素をまとめている。付録 C に、テスト計画、テストの概要、テスト結果の検証・評価用ワークシート、事後レポートなど、テストに関する文書のサンプルを示す。

6.1 テストの必要性の判断およびスケジュールの作成

TT&E プログラムの一環として、プログラムコーディネータは、テスト実施における組織全体の目標を検討したり、以下の質問に回答したりすることで、テストの必要性を定期的に判断する必要がある。

- テスト対象のシステムまたは構成要素はインストールされ、運用可能な状態か。
- システムまたは構成要素のプロセスと手順は確立されているか。

[20] この文書で説明するテストと、システムの承認および運用認可（C&A：certification and accreditation）を受けるために実行するテストを混同してはならない。C&A のためのテストでは、通常の条件下におけるシステムの安全性に重点が置かれているが、TT&E テストイベントは、緊急時対応計画やインシデント対応計画など、IT 計画に定義されている、システムに悪影響をもたらす条件下でのシステムの機能性に重点が置かれている。通常、C&A および TT&E のテストイベントの要件は大幅に異なるが、C&A と TT&E の要件の両方を包含する単一のテストイベントを実施して、重複する部分の労力を軽減する場合もある。

- 担当者は、システムまたは構成要素の使用についてトレーニングを受けているか。トレーニングの効果はあったか。
- NIST SP 800-53 への準拠など、特定の頻度でテストの実行が要求される要件（法令や規制への遵守など）が存在するか。
- 対象の構成要素、システム、構成要素とシステムのグループを最後にテストしたのはいつか。前回のテスト終了後、重要な変更や更新が行われたか。

テストは通常、組織のセキュリティ状況やその他の運用面に悪影響を及ぼさないように、テスト対象のシステムや構成要素の使用方法について担当者のトレーニングが終了し、システムや構成要素の運用を開始する前に実施される。担当者のトレーニングが完了していない場合、システムテストは、トレーニングが完了するまで延期する。運用の開始後、定期的にテストを行って、システムまたは構成要素の適切で安全な利用が継続するようにする。総合テストも定期的に実施するようスケジュールを設定し、IT 計画を適切かつ効果的で完全な状態で維持し、担当者が計画を実施するなかで自らの役割と責任を認識するようにする。担当者の異動が多い場合、組織が要求する準備レベルを維持するために、必要に応じてテストの実施頻度を高める。

テストのスケジュール設定では、利用可能なリソースや組織に与える可能性のある影響などの要素も検討する必要がある。テストのスケジュールを設定するとき、管理職に通知すること、そしてテスト実施の最適な時期を決定するために、業務に与える可能性のある影響を考慮することが重要となる。たとえば、組織の業務に影響を与える可能性のあるテストを、あらかじめわかっている業務のピーク時に実施することは勧められない。多くの従業員が休暇を取っている時期に総合テストのスケジュールを設定すれば業務への影響は最小限に抑えられるかもしれないが、テストに参加できる担当者の人数が制約を受ける可能性がある。組織の上層部にテスト、特に総合テストの実施を承認してもらうことは、テストを作成する上で重要な手順である。

テストのスケジュールは、組織外部の要素に影響される場合もある。たとえば、特定のテストを定期的に実施するよう法令や規制で定めている場合がある。さらに、環境や安全上の問題がスケジュールに影響する場合がある。たとえば、ある施設から別の施設にスタッフが業務を移転することを求めるテストの場合、激しい吹雪など極端な条件下で従業員が移動したりする必要がないように、天候の予測がつく時の方がより効果的にテストを実施できる可能性がある。

6.2 テストイベントの設計

テスト実施の必要性が確認されたら、TT&E プログラムコーディネータはテスト設計チーム[21]を結成して、個々の具体的なテストを設計する。いくつかの要素が、テストのレベル（構成要素テスト、システムテスト、または総合テスト）、テストに関与する組織の部門・部署、テストの範囲など、テストの設計にとって大きな意味を持つことがある。これらの要素は、テストの作成に必要な期間、テストの複雑さのレベル、およびテストの所要時間に影響を与える可能性がある。設計プロセスの早い段階で、テストに参加する担当者を決定し、テストの影響を受ける部分の管理職に連絡する。6.2.1 項から 6.2.6 項では、テスト設計プロセスの主な手順を示す。

6.2.1 範囲の決定

テストの範囲は、現行のシステムまたは、セキュリティ要件、および法令や規制の遵守事項に基づいて決定するべきである。テストの範囲は、テストの種類によって直接決まってくる。構成要素テストは、範囲が絞られ、一般に、関わる担当者や組織の部門・部署は少なくなる。システムテストの場合、

[21] テスト設計チームは、チームリーダと、テスト対象の領域ごとの専門家で構成する。チームリーダと専門家で協力しながらテストの内容を作成する。

範囲は広くなり、より多くの担当者と複数の構成要素が関わる。総合テストでは、組織の関与する割合がはるかに大きくなり、組織の全員が参加する場合もある。また、より広範な調整と計画作成が必要となる。

6.2.2 目標の決定

設計チームは、実施するテストの内容を決定し、期待される結果や成果を具体的に定める。テスト計画は、一連の小規模なテストで構成することができる。1 つ 1 つのテストは、構成要素やシステムの一部、または対象の構成要素やシステムで構成されるグループの一部を検証するよう設計する。各テストの目標は、構成要素、システム、または構成要素とシステムのグループが所定の目的と機能を十分果たしているかどうかを測定、確認、検証するものでなければならない。可能であれば、期待される結果や成果を客観的かつ測定可能な形で表現し、主観に基づく測定を最小限に抑える。結果はできるだけ、定量化可能かつ再現可能であることが望ましい。

テストはしばしば、標準的な運用の一環として、例えば、バックアップからの復旧、別の場所へのサーバの移動、オペレーティングシステムやアプリケーションのアップグレードやパッチの適用、ハードウェア構成要素の交換（ハードドライブの交換、故障した電源の交換など）などが実施される。テストと運用活動を一緒に実施することは、それぞれ個別に実施する場合よりも一般的に効率的であり、運用に悪影響を及ぼす可能性も低い。

他によく行うテストとしては、連絡網にて、連絡を開始して、所定の制限時間内に連絡が行き渡るかどうかの確認や、システムやシステム構成要素の電源を抜くことなどがある。

6.2.3 テストツールの決定

設計チームは、テストに必要となる、評価用のツールと手順を決定する必要がある。必要となる具体的なツールは、テストの範囲に応じて大きく異なる可能性がある。ソフトウェアまたはハードウェアによる専用ツール（ネットワークスニファ、脆弱性スキャナなど）から、計測装置や記録装置（ストップウォッチ、カメラ、ビデオレコーダなど）、確定したプロセスや手順への遵守度の測定に用いるチェックリストに至るまで、さまざまなツールを利用する。さらに、実行面を支援するために、テストチームに必要となる用品（ラジオ、携帯電話、バッジなど）もツールに含まれる場合がある。

6.2.4 参加者の決定

テストへの参加者は、実行するテストの範囲に応じて異なる。テストイベントへの参加には、次に示す 2 つのレベルがあると考えられる。

- 第 1 レベルの参加者は、テスト対象の構成要素またはシステムを操作する担当者で構成する。
- 第 2 レベルの参加者は、テストには直接関与しないが、テストまたはテスト関連の活動に影響を受ける可能性のある者で構成する。たとえば、テストに避難訓練を含める場合、参加者は避難せざるを得ない状況に置かれるすべての人々となる。そして、テストの影響を受ける者には、避難する人に連絡をとろうとするものの、オフィスにその人がいないために連絡ができない者も含まれる。

設計チームは、両方のレベルについて参加者の決定を試みるべきである。ただし、規模の大きいテストの場合、場合によっては、影響を受ける者は個人単位ではなくグループ単位で指定しなければならないことがある。第 1 レベルの参加者に含まれる個人は、電子メールまたは書面により、日数に十分な余裕を持たせて事前に通知する必要がある。第 2 レベルの参加者に含まれる個人とグループには、テスト実施前に通知する。例えば、テスト対象のシステムが中断する可能性のあることを

参加者にアナウンスしたり、ある時間帯にテスト対象のシステムが中断する可能性のあることや、ヘルプデスクの電話番号を伝えたりする。

6.2.5 テストスタッフの決定

設計チームは通常、*テスト責任者*を指名する。テスト責任者は要員の確保、計画や文書の作成、テストの実施、実行、設計チームの監督など、テストのあらゆる側面について責任を負う。テスト責任者は、1 名以上のデータ収集担当者を指名し、テストの結果の監視と記録を担当させる。テスト責任者とデータ収集担当者は、テストの前に、テストの範囲や目標を含め、テストに関する詳細について打ち合わせをするべきである。テスト前の打ち合わせでは、テスト責任者ディレクタとデータ収集担当者は、以前の演習とテスト（実施されていた場合）の結果を確認して、問題発生の可能性をあらかじめ認識しておくようにする。

設計チームには、テスト対象の特定の領域に詳しい専門家を 1 名以上置くことも少なくない。これらの専門家は、テスト計画の作成および必要なテストツールの決定を支援する。専門家は、テストの詳細を把握しているため、テストの参加者にするべきではない。ただし、テストの監視役、進行者、データ収集担当者、またはテスト管理者を担当することはできる。

6.2.6 実行計画の調整

設計チームは、テストが滞りなく完了するよう、事前に十分な時間の余裕を持って実行面の支援の調整を開始する。テスト前の調整に必要な時間は、テストの範囲によって異なる。通常、構成要素テストの場合は 1 か月、災害復旧計画やインシデント対応計画などの大規模 IT 計画における構成要素とシステムの総合テストの場合は数か月を要する。表 6-1 のチェックリストは、実行計画面について実行する必要があると考えられる行動の例である。具体的な実行要素は、テストの設計フェーズで明確化するが、実行要素に関する必要なリストは頻繁に更新する必要がある。これは特に、テストの作成が完了したあとに重要である。

表 6-1 テストイベント用実行計画チェックリストのサンプル

実行計画の内容	期限	完了
テストの実施日時の選定		
テスト対象の構成要素の決定		
参加者の決定		
組織のミーティングへの中核的な参加者の招待		
テスト計画およびその他の必要な文書の作成に関する調整		
全参加者を収容できる会議室の予約		
準備に必要な時間を考慮し、会議室が少なくとも 1 日前から確保出来ているかの確認		
AV 設備、録音・録画機器の使用の有無の決定		
AV 設備、録音・録画機器の予約（必要な場合）		
飲みもの、軽食の手配（必要な場合）		
必要なテストツール、測定・記録の機器、名札や名札ホルダ、クリップボード、ペンなどの項目を含む、備品チェックリストの作成		
テストに関するすべての文書とファイルを CD-ROM や USB メモリなどのリムーバブルメディアにコピーしてバックアップを作成		
テスト機器の正しい操作の確認、評価担当者へのテスト機器の操作方法の伝達		
テストの予行演習やリハーサルの実施（必要な場合）		

実行計画の内容	期限	完了
業務上の問題で中止が必要になった場合のための、テスト中止手順の確認		

6.3 テスト用資料の作成

テストの設計が完了したら、設計チームはテスト用文書を作成する必要がある。文書作成の規模は、テストの範囲によって異なる。テスト用文書には、次のものがある。

- **概要説明。**大規模なシステムテストまたは総合テストの場合、テストの最初にミーティングを行って、テストイベントの開始を知らせてもよい。上級管理職およびテストの影響を受ける可能性のあるほかの管理職への具体的な概要説明は、テストの内容とその重要性を理解してもらえるよう作成する必要がある。

- **テストガイド。**テストガイドは、テスト実施の基本的な手順をまとめたもので、参加者のリストも掲載する。さらに、テストによって影響を受ける可能性のあるすべての個人とグループのリストも掲載し、中止の必要が生じた場合のテスト中止手順についても説明する。テストガイドにより、テスト時に生じる事柄を総合的に把握できる。

- **テスト計画。**実施する具体的なテストそれぞれについて、実行する具体的な手順をまとめたテスト計画を作成する必要がある。各手順には、必要な実行項目のリストを示し、その手順を実行したあとに期待される結果や対応を記す。テスト中止の手順は、テスト計画にも記載する必要がある。なぜなら、評価担当者またはテストを実施する担当者は、テスト中にテスト計画を使用するからである。緊急時の連絡先（携帯電話やポケベルの番号など）も記載する。

- **事後レポート。**テスト完了後に事後レポートを作成する。事後レポートには、個々のテストの結果の他、テスト活動全体の概要を記載するべきである。また、是正措置や推奨事項も事後レポートに記載する。大規模なテストの場合、テストの概要、結果、改善に向けた推奨事項を含む、上級管理職向けの要旨も作成する。

IT 計画を対象に総合テストを作成するとき、同じ計画を対象とした機能演習を作成するときに発生する事柄と多くの部分が重なることがある。実際、総合テストのテスト計画は多くの場合、機能演習で使用する資料（シナリオ、MSEL、投入メッセージなど）と同様の資料を含む。たとえば、テスト中、特定のバックアップテープが損傷したこと、特定のサーバが利用できないこと、バックアップ施設への道路が閉鎖されていることなどが資料を通じて参加者に伝えられる。機能演習とテストの主な違いは、テストはできる限り実際の運用環境で実施される点である。そして、計画に記されているシステムの復旧と復元のプロセスと手順はもちろん、実施されたトレーニングについても実際の有効性を検証することを目的とし、担当者が自身の責任を把握し、所定の状況でどう対応すべきかを把握できるようにしている点が異なる。

6.4 テストの実施

テストの実施場所は、実施するテストの種類と範囲に応じて異なる。たとえば、小規模の構成要素テストは、1 つの事務室で実施できるが、IT 計画に含まれる構成要素とシステムの総合テストは、さまざまな場所に存在する、組織のさまざまな部門・部署が多数関わる可能性がある。

安全とセキュリティの 2 つは、いかなるテストの場合でも確保しなければならない要素である。組織の運用システムとネットワークは、実害を受けないように保護する必要がある。テストが原因で、組織が機能しなくなり、提供すべきサービスを提供できなくなるようなレベルで組織の中核的な機能や活動が途絶するようなことがあってはならない。こうした理由から、テスト責任者は、あらゆるテスト

を詳細に監視する必要がある。大損害をもたらしかねない中断の兆候がみられたり、個人の安全が脅かされたり、組織またはそのデータのセキュリティに問題が生じたりした場合に、テスト責任者およびテストチームのメンバーがただちにテストを中止できる態勢になっている必要がある。

テストの終了後すぐ、テスト責任者とデータ収集担当者は参加者とともに、テストの非公式の反省会（「ホットウォッシュ」とも呼ばれる）を行う。テスト責任者は、反省会の推進役を務め、参加者とデータ収集担当者にフィードバックを求める。反省会の終了直後、テスト中および反省会の間に記入したメモや用紙をテスト責任者に提出するよう、データ収集担当者および参加者に求める。

6.5 テストの評価

評価フェーズでは、設計チームのメンバーまたは別途選ばれたスタッフメンバーが事後レポートを作成し、テスト対象のシステムまたは構成要素が問題なく機能しているかどうかについて記載する。事後レポートのはじめに、テストの範囲や目標、シナリオなど、テストの背景情報についてまとめる。事後レポートには、テストチームによるテスト中の所見、そしてテストした構成要素またはシステムが含まれる IT 計画の強化につながる推奨事項も記載する。さらに、テスト参加者のリストも含め、反省会時にフィードバックを得るために実施した参加者向けの調査で得た情報も必要に応じて掲載する。

事後レポートは通常、作成に数日を要する。セキュリティまたは安全上、重大な不備のある場合、テスト責任者はレポートの完成を待たずに上層部にそのことを伝えるべきである。重大な不備を記載した非公式のレポートはただちに作成する必要がある。完全版のレポートはその後、妥当な期間内に提出する。適宜、正式な反省会を実施し、テスト責任者、計画コーディネータ、およびその他のテスト運営スタッフがテストの結果について議論する機会を設ける。利害関係者は一般に、事後レポートに目を通し、特定の推奨事項の重要性を明確にするために、その内容を強調するなど、細かな言葉遣いの変更を提案することがある。

事後レポート作成後、計画コーディネータは選択した担当者に活動項目を割り当てて、テストした構成要素またはシステムを含む IT 計画を更新できる。計画コーディネータは、その場合、必要であれば事後レポートに記載された推奨事項を実施することで、計画を更新する。テストの結果について他の管理職に概要を伝えたり、他のセキュリティ関連文書を改定したり、またはテストに基づく他の行動を実行に移したりすることが必要な場合もある。

6.6 まとめ

テストは、定量化可能な測定基準または予測される結果を用い、IT 計画内で重要と位置づけられている 1 つ以上の IT システムまたはシステム構成要素の運用性を検証するための評価手段である。テストにはいくつかの形態があり、たとえば、構成要素テスト（ハードウェアまたはソフトウェアの個々の構成要素、または互いに関連のある構成要素のグループのテスト）、システムテスト（システム全体のテスト）、総合テスト（IT 計画に盛り込まれているすべてのシステムと構成要素のテスト）がある。テストは、できる限り運用環境に近づけて実施する。つまり、テストは、システムや構成要素が置かれている日常の作業環境を再現する形で実施する必要がある。もし可能であれば、組織の日常業務遂行に使用する構成要素またはシステムを実際にテストするべきである。。テストの実施は、組織の業務を中断させる可能性がある。そのため、特にテストが何の問題も起こさずに完了するという強い確信が持てない場合は、実際の運用システムをコピーしたシステム上でテストを実施する場合もある。

テストイベントの計画作成と実行によく利用される方法論の 1 つは、次の各フェーズで構成される。

- **設計。**TT&E プログラムコーディネータは、テスト設計チームと連携して、テストイベントを設計する。いくつかの要素が、テストの形態（構成要素テスト、システムテスト、または総合テスト）、テストに関与する組織の部門・部署、テストの範囲など、テストの設計に影響を与える可能性がある。イベント設計プロセスにおける主な手順は、次のとおりである。
  - 現行のシステム要件またはセキュリティ要件、および法令や規制の遵守事項に基づいてテストの範囲を決定する。
  - テストの目標を決定する。
  - テストに必要な評価ツールと手順を決定する。
  - テストに参加してもらう個人を決定し、テストのスケジュールを参加者に伝える。
  - テスト責任者、1 名以上のデータ収集担当者など、テストを実行するスタッフを決定する。
  - テストイベントの実行計画を調整する。
- **作成。**設計チームは、テスト前、テスト中、およびテスト終了後に使用する文書を作成する。通常、テストの概要、テストガイド、テスト計画、事後レポートを作成する。一部のテスト、特に総合テストでは、シナリオや MSEL、投入メッセージなど、機能演習で用いるものと同様の資料が必要となる場合がある。
- **実施。**テストの実施場所は、実施するテストの種類と範囲に応じて異なる。たとえば、小規模の構成要素テストは、1 つの事務室で実施できるが、IT 計画に含まれる構成要素とシステムの総合テストは、さまざまな場所に存在する、組織のさまざまな部門・部署が多数関わる可能性がある。テスト中、組織が機能しなくなり、提供すべきサービスを提供できなくなるようなレベルで組織の活動が中断されるようなことがあってはならない。テスト責任者は、すべてのテストを詳細に監視し、大きな損害をもたらしかねない中断の兆候がみられたり、個人の安全が脅かされたり、組織またはそのデータのセキュリティに問題が生じたりした場合に、テスト責任者およびテストスタッフのメンバーがただちにテストを中止できる態勢になっている必要がある。テストの完了後、テスト責任者とデータ収集担当者は、テストの非公式の反省会を開き、スタッフと参加者からフィードバックを得る。
- **評価。**反省会で出されたコメントは、テスト時に得られた教訓とともに、事後レポートに記載する。事後レポートには、テストに関する背景情報、テストスタッフによる所見、そしてテストを行った構成要素またはシステムが含まれる IT 計画の強化につながる推奨事項を記載する。評価の結果に基づき、IT 計画や他のセキュリティ関連文書を改定したり、結果について管理職に報告したり、その他の活動を行ったりする。

（本ページは意図的に白紙のままとする）

付録A—机上演習用文書のサンプル

付録 A では、以下のサンプル文書を示す。

- 机上演習進行者用ガイド
- 机上演習参加者ガイド
- 机上演習事後レポート

これらのサンプル文書は、机上演習用文書の設計と作成の担当者がテンプレートとして使用できるよう構成されている。この付録に示す文書の他に、演習次第と実行計画に関する情報を含む概要説明を作成し、演習開始時に提示する。

A.1 机上演習進行者用ガイドのサンプル

［組織名を挿入］
［机上演習のタイトルを挿入］

進行者用ガイド

［実施場所を挿入］

［実施日を挿入］

[目次を挿入]

[サンプル]はじめに

*[組織名を挿入]*の*[演習の対象となる計画の名称を挿入]*の有効性確認を目的として、*[組織名を挿入*[22]*]*において机上演習を実施し、*[計画名を挿入]*の遂行に関わるプロセスと手順を検証する。議論をベースに行うこの演習は、*[開始時刻を挿入]*に開始し、*[終了時刻を挿入]*まで行う*[所要時間を挿入]*時間のイベントである。

この演習は、*[施設名を挿入]*に設置されているミッションクリティカルなシステムの停止を引き起こすイベントの発生を受け、*[組織名を挿入]*における復旧業務の遂行に関し、選ばれた担当者どうしのコミュニケーションを促すことを目的としている。さらにこの演習は、*[組織名を挿入]*の準備状況を改善し、既存の*[計画名を挿入]*の手順の有効性確認に役立つことを目的とする。

参加者は、*[施設名を挿入]*のミッションクリティカルなシステムの復旧に関連する問題を高い視点から議論する準備をして演習に参加するべきである。演習の目標を達成するため、以下に示す、*[施設名を挿入]*の緊急時対応計画の要素を中心に議論を行う。

- *[施設名を挿入]*のシステムの各機能(メッセージング、Web など)を復旧するため何を行うか。
- どのようにしてシステムを復旧するか。復元の優先度や最適な順番は何か。
- 復元にどれくらいの時間が必要か。どのようにすれば復元を最適化できるか。
- 期待される結果、そしてシステムチームの役に立ち、演習後の準備状況を改善する活動項目は何か。

参加者は、上記の質問への回答に役立てるために、必要に応じてバックアップの参考資料を持参してもよい。

[サンプル]運用の概念

机上演習は、議論をベースに行うイベントで、参加者は会議室に集まり、緊急時にとる行動について議論する。机上演習は、危機のシナリオに関するさまざまな問題を担当者が議論する最初のステップとして効果的である。机上演習は、役割と責任の検証、相互依存関係の発見、そして計画の評価を行う優れた場を提供する。

参加者には、*[施設名を挿入]*に影響を与える内容のシナリオが提示される。進行者が、演習の目標に結び付くような質問をすることで、議論の進行を促す。進行者は、議論を活性化するために、適宜シナリオに変更を加えることもある。参加者同士でも互いに質問しあうことが推奨される。

[サンプル]目標

この演習の目標は、次のとおりである。

22 ここでは、IT 緊急時対応計画の机上演習をサンプルとして示す。

- チームが代替施設において IT 業務を再開できることの検証。
- *[計画名を挿入]*に記されている復旧手順の正確さの検証。
- 緊急時対応計画で修正が必要な領域の特定。

[サンプル]演習次第

日付:	*[日付を挿入]*
場所:	*[住所を挿入]*
午前 9:00～午前 9:15	あいさつと紹介
午前 9:15～午前 9:45	演習の概要説明（目標、遵守事項など）
午前 9:45～午前 11:30	シナリオに基づく議論
午前 11:30～午後 12:00	反省会

[サンプル]シナリオ

*[日付を挿入]*の*[時刻を挿入]*、*[施設名を挿入]*において発生した電気火災により大規模な被害が発生し、データセンタの業務が停止した。このインシデントに対応するため*[計画名を挿入]*が発動され、当面の間、*[代替施設名を挿入]*において業務を行う。*[組織名を挿入]*の職員は、煙、水、その他の健康に害を及ぼす危険がなくなるまで、ビルから退去する。*[施設名を挿入]*で問題が発生しているものの、取締役や管理職は予定を変更する様子はなく、IT 業務の*[代替施設名を挿入]*へのシームレスな切り替えを期待している。

[サンプル]進行者からの質問

以下の質問は、議論を促し、あらかじめ定められた目標を達成できるよう、進行者が使用するためのものである。演習の流れに応じて、以下の質問または、他のの質問を用い、議論を通じて参加者が目標を達成できるようにする。

1. *[計画名を*挿入]を発動する権限を持っているのは誰か。
2. 計画が発動された場合、*[施設名を挿入]*では、どのレベルのスタッフが対応すべきか。
3. 計画の発動をどのように、誰から通知を受けるか。
4. *[施設名を挿入]*におけるチームの役割と責任は何か。
5. 重要な担当者が火災でけがを負い、*[施設名を挿入]*に出向けない場合、どのようにして業務が移行されるか。
6. IT の復旧手順は、もれなく文書化されているか。その内容は正確か。緊急時対応計画に追加の手順を記載する必要はあるか。
   - *[計画名を挿入]*に示された時間内に復旧手順を完了できるか。
   - *[施設名を挿入]*において業務を再開するための手順はどのようなものか。

［サンプル］反省会で行う質問

優れている点および改善が必要と考えられる領域を明らかにする事後レポートを演習後に作成する。以下は、参加者からフィードバックを得て、事後レポートに盛り込むための質問である。

- 演習中に取り上げなかった事柄で、議論したい課題はあるか。
- 緊急時対応計画のよい点は何か。より詳細な検証が必要な領域はどれか。
- 演習のメリットはあったか。今後実施されるテストの準備に役立ったか。
- 演習から得たものは何か。
- 今後実施する演習とテストはどのように改善できるか。

A.2 机上演習参加者ガイドのサンプル

［組織名を挿入］
［机上演習のタイトルを挿入］

参加者ガイド

［実施場所を挿入］

［実施日を挿入］

[目次を挿入]

[サンプル]はじめに

*[組織名を挿入]*の*[演習の対象となる計画の名称を挿入]*の有効性確認を目的として、*[組織名を挿入]*[23]において机上演習を実施し、*[計画名を挿入]*の遂行に関わるプロセスと手順を検証する。議論をベースに行うこの演習は、*[開始時刻を挿入]*に開始し、*[終了時刻を挿入]*まで行う*[所要時間を挿入]*時間のイベントである。

この演習は、*[施設名を挿入]*に設置されているミッションクリティカルなシステムの停止を引き起こすイベントの発生を受け、*[組織名を挿入]*における復旧業務の遂行に関し、選ばれた担当者どうしのコミュニケーションを促すことを目的としている。さらにこの演習は、*[組織名を挿入]*の準備状況を改善し、既存の*[計画名を挿入]*の手順の有効性確認に役立つことを目的とする。

参加者は、*[施設名を挿入]*のミッションクリティカルなシステムの復旧に関連する問題を高い視点から議論する準備をして演習に参加するべきである。演習の目標を達成するため、以下に示す、*[施設名を挿入]*の緊急時対応計画の要素を中心に議論を行う。

- *[施設名を挿入]*のシステムの各機能(メッセージング、Web など)を復旧するため何を行うか。
- どのようにしてシステムを復旧するか。復元の優先度や最適な順番は何か。
- 復元にどれくらいの時間が必要か。どのようにすれば復元を最適化できるか。
- 期待される結果、そしてシステムチームの役に立ち、演習後の準備状況を改善する活動項目は何か。

参加者は、上記の質問への回答に役立てるために、必要に応じてバックアップの参考資料を持参してもよい。

[サンプル]運用の概念

机上演習は、議論をベースに行うイベントで、参加者は会議室に集まり、緊急時にとる行動について議論する。机上演習は、危機のシナリオに関するさまざまな問題を担当者が議論する最初のステップとして効果的である。机上演習は、役割と責任の検証、相互依存関係の発見、そして計画の評価を行う優れた場を提供する。

参加者には、*[施設名を挿入]*に影響を与える内容のシナリオが提示される。進行者が、演習の目標に結び付くような質問をすることで、議論の進行を促す。

[サンプル]目標

この演習の目標は、次のとおりである。

- チームが代替施設において IT 業務を再開できることの検証。
- *[計画名を挿入]*に記されている復旧手順の正確さの検証。

---

23 ここでは、IT 緊急時対応計画の机上演習をサンプルとして示す。

- 緊急時対応計画で修正が必要な領域の特定。

[サンプル]演習次第

日付:	*[日付を挿入]*
場所:	*[住所を挿入]*
午前 9:00～午前 9:15	あいさつと紹介
午前 9:15～午前 9:45	演習の概要説明（目標、遵守事項など）
午前 9:45～午前 11:30	シナリオに基づく議論
午前 11:30～午後 12:00	反省会

[サンプル]シナリオ

*[日付を挿入]*の*[時刻を挿入]*、*[施設名を挿入]*において発生した電気火災により大規模な被害が発生し、データセンタの業務が停止した。このインシデントに対応するため*[計画名を挿入]*が発動され、当面の間、*[代替施設名を挿入]*において業務を行う。*[組織名を挿入]*の職員は、煙、水、その他の健康に害を及ぼす危険がなくなるまで、ビルから退去する。*[施設名を挿入]*で問題が発生しているものの、取締役や管理職は予定を変更する様子はなく、IT 業務の*[代替施設名を挿入]*へのシームレスな切り替えを期待している。

[サンプル]参加者への質問

以下は、参加者ガイドに登場する可能性のある質問のサンプルである。

1. *[計画名を挿入]*を発動する権限を持っているのは誰か。
2. 計画の発動をどのように、誰から通知を受けるか。
3. IT の復旧手順はもれなく文書化されているか。*[計画名を挿入]*に示された時間内に復旧手順を完了できるか。

[サンプル]反省会で行う質問

優れている点および改善が必要と考えられる領域を明らかにする事後レポートを演習後に作成する。以下は、参加者からフィードバックを得て、事後レポートに盛り込むための質問である。

- 演習中に取り上げなかった事柄で、議論したい課題はあるか。
- 緊急時対応計画のよい点は何か。より詳細な検証が必要な領域はどれか。
- 演習のメリットはあったか。今後実施されるテストの準備に役立ったか。
- 演習から得たものは何か。
- 今後実施する演習とテストはどのように改善できるか。

A.3 机上演習事後レポートのサンプル

［組織名を挿入］
［机上演習のタイトルを挿入］

事後レポート

［実施場所を挿入］

［実施日を挿入］

[目次を挿入]

[サンプル]はじめに

[日付を挿入]、*[組織名の挿入]*は*[計画名を挿入]*に対する理解を確認する目的で*[演習の所要時間を挿入]*時間の机上演習に参加した。

[サンプル]目標

この演習の目標は、次のとおりである。

- チームが代替施設において IT 業務を再開できることの検証。
- *[計画名を挿入]*に記されている復旧手順の正確さの検証。
- 緊急時対応計画で修正が必要な領域の特定。

[サンプル]演習次第

日付:	*[日付を挿入]*
場所:	*[住所を挿入]*
午前 9:00～午前 9:15	あいさつと紹介
午前 9:15～午前 9:45	演習の概要説明（目標、遵守事項など）
午前 9:45～午前 11:30	シナリオに基づく議論
午前 11:30～午後 12:00	反省会

[サンプル]議論の成果

*[演習名を挿入]*により、*[関連情報を挿入]*に関する情報が得られた。この演習を通じて参加者が重要な質問、懸念事項、課題を明らかにする機会を得られたことは、大きな成果であった。演習終了時、事後レポートに盛り込むため、演習で得られた情報、必要な追加情報、そして演習自体や演習のトピックに関する考えについて、参加者に評価用紙への記入を依頼した。*評価用紙のサンプルについては、C-16 ページを参照。*

演習の議論で得られた成果、必要な推奨される行動は次のとおりである。

全般的な成果

今回の演習では、参加者は*[関連情報を挿入]*のよい機会を得た。演習の結果、参加者は*[関連情報を挿入]*に対する意識を高めた。

具体的な成果

演習時の所見、および計画の強化につながる推奨事項は次のとおりである。

所見 1　［全般的なトピック領域を挿入］

［所見を挿入］

推奨事項

［推奨事項を挿入］

***所見 2*　［全般的なトピック領域を挿入］**

［所見を挿入］

推奨事項

［推奨事項を挿入］

所見と推奨事項の例:

所見 1　コミュニケーション

緊急時対応計画のメンバーとコミュニケーションをとるための標準化されたシステムを確認する計画が存在しない。

推奨事項

- 対象組織は、標準化された通信要件の確立、予備通信システムの配置方法と配置場所の指定、および担当者による予備通信システムの利用手順の説明を内容とする通信計画の作成を検討するべきである。
- 組織は、冗長通信システムを明らかにして、緊急時に重要な担当者と連絡をとることができるようにするべきである。冗長通信システムは、家庭用電話や携帯電話、ノートパソコン、その他の通信システムなどで構成することができる。

所見 2　移動キット

重要な担当者に対し、緊急時に移動先の施設に運ぶ、業務遂行に必要な用品類の含まれた移動キットが支給されていない。

推奨事項

- 連邦政府機関は、緊急時に移動する担当者向けに、移動キットを作成して事前に配布する可能性を検討するべきである。長時間配置される場合に担当者に必要となる用品に加え、移動キットには担当者が自身の重要な機能を果たすために必要な情報が記録されたフラッシュドライブ、ディスクまたは CD-ROM を含める必要がある。

［サンプル］評価用紙

評価用紙記入へのご協力お願いいたします。

演習イベント名を挿入

演 習 評 価 用 紙

日付を挿入

演習に関する以下の質問にお答えください。

氏 名 _____

1)． 自分の責任を果たすために必要な情報とリソースはすべて手元にありましたか。

2)． 移動先施設で責任を果たすためのトレーニングは十分でしたか。

3)． 演習の構成は現実的でしたか。

4)． 演習中、うまく行った点、うまく行かなかった点について自由にお書きください。

5)． 緊急時に移動先施設で長期にわたって業務を継続するための準備は十分にできましたか？*いずれか1つに○をつけてください。*

準備できていない　多少準備はできた　準備できた　十分準備できた

6)． 演習全体をどう評価しますか。*いずれか1 つに○をつけてください。*

改善が必要　普通　良かった　非常に良かった

［サンプル］評価結果

*［日付を挿入］*に実施された*［机上演習名を挿入］*のあと、演習の感想を記入する評価用紙が参加者に手渡された。参加者は、評価用紙において、演習を数値で評価したり、事後レポートに記載する検討事項を記入したりできる。参加者の反応の詳細については「別紙 1」を参照のこと。*別紙はそれぞれ、個々の演習イベントの評価用紙の内容が反映される。評価用紙に、評価尺度で記入する項目があれば、円グラフや棒グラフで表現できる。*

質問は、取り上げるべき課題が他にあったかどうか、演習をやって良かったか、演習から得たものは何か、そして演習の改善に向けて何が出来るかを参加者に尋ねる内容となっている。*［パーセンテージの数値を挿入］*の参加者が評価用紙に記入した。

他に取り上げるべき課題があったかどうかに関する質問に対しては、評価を記入した参加者のうちおよそ*［パーセンテージの数値を挿入］*が、必要な課題が演習で網羅されていたと回答した。その他のコメントとしては、*［関連情報を挿入］などがあった。*

演習をやって良かったかどうかの質問に対しては、評価を記入した参加者のうち*［パーセンテージの数値を挿入］*が、演習をやって良かったと回答した。コメントとしては、*［関連情報を挿入（「初めてにしては良かった」、「非常に有益であった」などがあった）］*。

演習から何を得たかに関する質問に対しては、評価を記入した参加者のうち*［パーセンテージの数値を挿入］*が、*［関連情報を挿入］*と回答した。

別紙：参加者の回答

演習についての感想	演習から得たもの
■ *［コメントを挿入］*	■ *［コメントを挿入］*
■	■
■	■
■	■

全体として、*［机上演習名を挿入］*から得られたフィードバックは*［関連情報を挿入］*。

（本ページは意図的に白紙のままとする）

付録B—機能演習用文書のサンプル

付録 B では、以下のサンプル文書を示す。

- シナリオ
- マスタシナリオイベントリスト（MSEL）
- 投入メッセージ
- 投入メッセージ追跡票
- 事後レポート

これらのサンプル文書は、機能演習用文書の設計と作成の担当者がテンプレートとして使用できるよう構成されている。この付録に示す文書の他に、演習次第と実行計画に関する情報を含む概要説明を作成し、演習開始時に提示する。

B.1 機能演習用シナリオのサンプル

［組織名を挿入］
［機能演習のタイトルを挿入］

シナリオ

［実施場所を挿入］

［実施日を挿入］

シナリオは、作成フェーズにおいて機能演習チームが作成する。シナリオの文書には、簡単なシナリオの背景を記し、演習開始の数週間前または数か月前の時点における世界または各地域の状況を参加者に意識させる。背景情報は、演習前または演習開始時の概要説明で参加者に提供する。シナリオ自体は、演習実施中に発生する出来事を描いたものである。発生する出来事には、マスタシナリオイベントリストに記載されるものもあり、投入メッセージとして演習に盛り込まれる。

[サンプル]シナリオの背景

緊急事態発生 20 日前

米国の戦略的利害に関連し、国際的な緊張が海外において大幅に高まっている。対立を外交的に解決する試みにも関わらず、敵対国の軍隊が展開し、米国の同盟国に対する大規模な軍事侵攻の体勢を整えている。米国の諜報機関は、同盟国の政治経済を敵対国が混乱させる計画の文書の存在も把握している。同盟国の混乱は、当該地域における米国の軍事的および経済的な利益に悪影響を及ぼす可能性がある。

緊急事態発生 10 日前

緊張は引き続き高まり、敵対国は同盟国および海外に存在する米国の利権に対し、小規模な軍事行動を実施した。米国の偵察機が撃墜され、死亡した乗員の様子がテレビの画面に映し出された。緊急の閣議が招集され、同盟国政府と米国の利権を保護するため、当該地域に米国軍を展開することが決定された。米国の利権を守る、初期段階の作戦態勢は翌月までは整わないと予想されている。

緊急事態発生 5 日前

米国が当該地域に軍隊と物資を送ると宣言したのを受け、敵対国は「米国の帝国主義者に対し激しい一撃を加える」ために必要な、いかなる行動も辞さないことを宣言した。敵対国は、米国が引き起こすいかなる戦争も米国本土においても戦われると表明している。まもなく米国の諜報機関は、米国に対するサイバー攻撃の増加と米国政府に向けたテロリストによる攻撃実行の脅威の高まりを把握する。さらに諜報機関は、米国内における敵対国の海外利権の動きが盛んになり、他の国に存在するテロリストの拠点も、米国内外を問わず、米国に対する攻撃実行の動きを開始した兆候もつかんでいる。米国政府高官は、敵対国が大量破壊兵器の使用とサイバーテロリズムを含むさまざまな行動を実行に移すことにより、米国の一般の人々による支持を弱め、軍隊の展開力を阻害することを望んでいる疑いがあると述べている。にも関わらず、米国軍は当該地域への展開を継続した。

[サンプル]シナリオ

緊急事態発生当日

0900: 米国コンピュータ緊急対応チーム(US-CERT: United States Computer Emergency Readiness Team、以下 US-CERT と称す)は、最新のコンピュータワームと考えられる存在についての警告を発した。US-CERT は、このコンピュータワームがわずか 2 時間の間に世界各地の 50 万台を超えるコンピュータに感染したと推定しており、そのことから、ワームの感染拡大が電子商取引や電子メール、エンターテイメントなど、ビジネスや個人によるインターネットの利用を阻む可能性を警告するに至った。米国の諜報機関は、ワームの拡散を米国軍の展開に対するものと関連付け、特に、軍事展開を支援する政府機関同士の通信を阻害することを目的とした攻撃であると恐れている。

ここ数時間で、連邦政府機関の Web サイトへの侵入が多数報告されている。敵対国と結び付きがあると政府高官が考えているハッカーたちは、米国政府のさまざまな情報システムのセキュリティを侵害することに成功した。各省庁や政府機関の多数の Web サイト上でも反政府的破壊行為が報告されている。

*[組織名/データセンタ名を挿入]*は現在、ワームの影響への対処と、さらなる電子的侵入に対する防御を実施する過程にある。

1000: 差し迫ったテロリズムの脅威、および連邦政府機関の情報システムに対して継続している電子的侵入が計画的な情報戦争攻撃の一部である可能性があるという懸念から、国土安全保障省(DHS:Department of Homeland Security)は、国土安全保障勧告システム(Homeland Security Advisory System)の警告レベルを、「高」のオレンジからテロリストによる攻撃の危険を表す「危機」の赤へと変更した。

1200: 多数のタンク車を牽引する貨物列車が都市中央部をゆっくりと通過していた。タンク車の一部は、殺虫剤の製造に用いられ、爆発性の高い化学物質であるイソシアン酸メチル(MIC:Methyl Isocyanate)を積載していた。貨物列車が*[組織の施設名を挿入]*を通過する途中、あるタンク車がすさまじい爆発を起こした。爆風により施設の一部が崩落し、その周辺で停電が発生した。*[組織の施設名を挿入]*にいた人の多くが死傷した。

*[データセンタ名を挿入]*は爆風に耐え、緊急用電源が重要な IT システムに供給された。データセンタの職員数名が昼食のためデータセンタを離れており、彼らの安否はこの時点では不明である。管理責任者は、データセンタで緊急時対応計画を始動し、代替のコンピューター施設にデータセンタを再配置するよう指示した。管理責任者は、代替施設において重要なデータセンタ業務を復元するのに加え、さらなる電子的侵入から[組織名を挿入]を守ることも引き続き最優先であることを表明した。

緊急事態発生 1 日後

1000: 諜報機関および法の執行機関は、米国に対する数多くの脅威の追跡を継続している。連邦捜査局(FBI:Federal Bureau of Investigation)は、米国中の各省庁および連邦政府機関に対してさらなる攻撃の脅威が存在することを政府機関に通達した。*[組織名を挿入]*に向けた通知では、組織の代替コンピューター施設外でテロリストによる監視活動が行われている可能性が報告されていた。そのため、管理責任者は、データセンタの担当者に対し、脅威の存在が間違いないと判明した場合に備え、業務を予備の代替施設に移行する選択肢の検討を指示した。

B.2 機能演習用マスタシナリオイベントリストのサンプル

［組織名を挿入］
［機能演習のタイトルを挿入］

マスタシナリオイベントリスト（MSEL）

［実施場所を挿入］

［実施日を挿入］

マスタシナリオイベントリスト(MSEL)は、作成フェーズにおいて機能演習チームが作成する。MSEL には、シナリオの重要なイベント、主要なイベントに加えられる投入メッセージ、および各 MSEL 項目の目標を記載する。演習管理者、シミュレーション担当者、およびデータ収集担当者は、演習の実施フェーズの間 MSEL を参照し、演習の進行が順調に進むようにする。

マスタシナリオイベントリスト			
イベント番号	**MSEL 主要イベントの説明**	**MSEL イベントの結果として期待される行動**	**目標**
1	***例*** *[組織名を挿入]*は、重要な情報システムに電子的侵入を受ける。	***例*** 投入:1 日目、0900～1700 ■ サイバーインシデント対応チームを始動 ■ サイバー侵入対応計画を遂行 ■ 顧客および利害関係者への通知と調整 ■ 感染したシステムの復旧	***例*** ■ サイバー侵入対応計画の下、スタッフに責任内容を周知 ■ サイバー侵入対応計画の有効性確認 ■ 連邦政府のサイバー関連機関、顧客、および主要な利害関係者との調整
2	***例*** 国土安全保障勧告システムの脅威レベルが「高」のオレンジからテロリストによる攻撃の危険を表す「危機」の赤に変更される。	***例*** 投入:1 日目、1000～1200 ■ 緊急時対応チームを始動 ■ ミッションクリティカルなすべての IT システムについてバックアップ手順を開始 ■ 重要な担当者を代替施設に再配置 ■ ホワイトハウスやその他の省庁、政府関連機関と調整し、業務再配置の決定を担当者に通知	***例*** ■ スタッフに緊急時対応の開始と通知の手順を周知 ■ IT 緊急時対応計画と手順の有効性確認 ■ 再配置計画と手順の有効性確認 ■ 主要な利害関係者との調整およびコミュニケーションプロセスの有効性確認
3	***例*** オフィスのあるビルの外で大規模な爆発が発生する。	***例*** 投入:1 日目、1200～1700 ■ ビルに供給されていた商用電力がすべて遮断 ■ サイトから、一部のデータ通信リンクに障害発	***例*** ■ IT 緊急時対応計画と手順の有効性確認 ■ 追加の緊急時対応計画を作成する必要の有無を確認

		生との報告 ■ 施設の管理者からビルの修復は不可能との報告	■ データセンタの業務復旧計画の検討
4	***例*** 代替施設に対するテロの脅威の可能性	***例*** 投入:2 日目、1000～1200 ■ 代替施設が機能停止した場合の選択肢の検討 ■ IT システム復旧の優先順位を決定する	***例*** ■ 代替施設用に追加の緊急時対応計画を作成する必要の有無を確認

B.3 機能演習用投入メッセージのサンプル

［組織名を挿入］
［機能演習のタイトルを挿入］

投入メッセージ

［実施場所を挿入］

［実施日を挿入］

投入メッセージは、作成フェーズにおいて機能演習チームが作成する。これらのメッセージは、実施フェーズにおいて、演習管理者が演習の参加者に対し、投入メッセージ追跡票に示す手段で提供する。以下に示すサンプルの投入メッセージの場合、演習管理者は最高情報責任者(CIO)の役割を演じ、演習チームの責任者を呼び、情報を提供し、以後の行動を要請する。チーム責任者または他の演習参加者に期待する行動は、このリストの下部にある「コントロールセル／対応セルへの注記」に示され、投入メッセージの結果、どのような行動がとられるかを想定する演習管理者、シミュレーション担当者、またはデータ収集担当者を支援する。

****演習**演習**演習**演習****

[演習名を挿入]の実装者
[日付を挿入]

例

*#15 ー[投入メッセージのタイトルを挿入]**(例:代替施設用災害復旧戦略の作成)***

投入日時: [*日時を挿入*] ***(例:緊急事態発生 2 日目 10:45)***

発信者: [*メッセージの発信者を挿入*]**(例:最高情報責任者(CIO))**

受信者: [*メッセージの受信者を挿入*]**(例:チーム責任者)**

伝達手段: [*メッセージの伝達手段を挿入*]**(例:電話)**

[*メッセージを挿入*]

例

ビルおよびデータセンタの損害の規模が判明した結果、この先しばらくの間、代替施設(AF)で業務を行うことになるのは明らかである。テロリストによる攻撃の脅威が継続しているなか、AF に影響を及ぼす大規模な停電の発生に備える緊急時対応計画を作成する必要がある。AF におけるミッションクリティカルシステムの運用継続性を確保するために、どのような戦略をとればよいか。優先して復旧するシステムとアプリケーションはどれか。それらのシステムの有効なバックアップシステムを構築するのにどれくらいの期間が必要か。

コントロールセル／対応セルへの注記:

[*コントロールセル／対応セルが、演習参加者の追跡、評価、対応のために検討する必要のある任意の種類の情報を挿入*]

例

AF チーム責任者が、AF 緊急時対応計画を参照し、適切なシステムエンジニアおよびアプリケーションエンジニアと調整して復旧戦略を立てることを想定する。

B.4 機能演習用投入メッセージ追跡票のサンプル

［組織名を挿入］
［機能演習のタイトルを挿入］

投入メッセージ追跡票

［実施場所を挿入］

［実施日を挿入］

*投入メッセージ追跡票は、作成フェーズにおいて機能演習チームが作成し、実施フェーズにおいて演習管理者が追加の情報を記入する。以下のサンプルでは、**太字**で示した文字が作成フェーズで作成されたもので、斜体の文字は実施フェーズで演習管理者が追加したものである。投入メッセージ追跡票は、どの投入メッセージをどのタイミングで参加者に示すかを記した「台本」を演習管理者に提供することを目的としている。そして、演習管理者は投入メッセージ追跡票を使用し、投入メッセージを提示した時刻、およびそれに応じて参加者がとった行動の要約を記録する。*

投入メッセージ追跡票				
投入メッセージ番号	**投入予定時刻**	**実際の投入時刻**	**投入メッセージの要約**	**コメント**
例 **1**	*例* **0900**	*例* *0901*	*例* **悪意のあるコンピュータワームによる DOS（サービス拒否）攻撃**	*例* *演習管理者からチーム責任者に対し投入。チーム責任者は、ただちにネットワーク管理者に行動を指示。ネットワーク管理者は、適切な行動をとり、管理責任者および顧客の代表者に連絡。ネットワーク管理者は、引き続き、演習の終了まで状況の監視を続行。*
例 **2**	*例* **1015**	*例* *1018*	*例* **リーダーへの状況報告のスケジュール**	*例* *演習管理者からチーム責任者に対し投入。チーム責任者が 10:20 に業務担当者に行動を指示。業務担当者は、標準業務手順に従ってチーム全員のスケジュールを記録し、提示。*
例 **3**	*例* **1025**		*例* **ホワイトハウスへ連絡**	
例 **4**	*例* **1200**		*例* **ビルの外で大規模な爆発**	

B.5 機能演習事後レポートのサンプル

［組織名を挿入］
［機能演習のタイトルを挿入］

事後レポート

［実施場所を挿入］

［実施日を挿入］

事後レポートは、評価フェーズにおいてデータ収集担当者が作成する。事後レポートには、演習イベントに関する背景情報、演習の範囲、目的、シナリオ、主な成果と推奨事項を記載する。その他に、事後レポートには演習の参加者のリストを掲載し、必要に応じて、演習終了時に参加者が記入したアンケートに基づく関連情報を記載する。

[サンプル]目次

[目次を挿入]

[サンプル]はじめに

[日付を挿入]、*[組織名の挿入]*はサイバー侵入対応計画および代替施設用緊急時対応計画に対する組織の理解を確認する目的で*[演習の所要時間を挿入]*時間の機能演習に参加した。*[演習の背景情報で、事後レポートに関連する追加の情報を挿入]*

[サンプル]範囲

この演習は、*[組織名を挿入]*が代替コンピューター施設より、計画的サイバー攻撃に対処する能力を検証することを目的としている。演習イベントでは、サイバー侵入対応計画および代替施設用緊急時対応計画の両方について、発動、運用、再開の各フェーズのあらゆる側面を検証した。2 つの計画の下で運用上の責任を持つ担当者全員が演習イベントに参加した。上位の意志決定担当者の演習は行わなかったが、管理責任者の行動を中心とする 2 回目の演習を翌月以降に予定している。

[サンプル]目標

この演習の目標は、次のとおりである。

- サイバー侵入対応計画および代替施設用緊急時対応計画の有効性確認
- 2 つの計画の間の相互依存関係、重複、矛盾の特定
- チームが代替施設において IT 業務を再開できるかどうかの検証
- 計画における責任をスタッフに周知
- *両計画*に記されている復旧手順の正確さの検証
- 連邦政府のサイバー関連機関、顧客、および主要な利害関係者との調整
- 両計画で修正が必要な領域の特定
- 追加の緊急時対応計画を作成する必要の有無を確認

[サンプル]シナリオ

[シナリオまたはシナリオの概要を挿入]

［サンプル］演習の成果

*［演習名を挿入］*により、*［関連情報を挿入］*に関する情報が得られた。演習では、代替施設で緊急時に対処する実践的トレーニングを参加者が受ける機会となったことが重要な成果であった。さらに、この演習では、参加者が重要な質問、懸念事項、課題を明らかにする機会を得られた。演習終了時、事後レポートに盛り込むため、演習で得られた情報、必要な追加情報、そして演習に関する考えについて、参加者に評価用紙への記入を依頼した。*［評価用紙のサンプルについては、B-17 ページを参照。］*

演習の成果および推奨される行動は次のとおりである。

全般的な成果

今回の演習では、参加者は*［関連情報を挿入］*のよい機会を得た。演習の結果、参加者は*［関連情報を挿入］*に対する意識を高めた。

具体的な成果

演習時の所見、および計画の強化につながる推奨事項は次のとおりである。

所見 1　［全般的なトピック領域を挿入］

［所見を挿入］

推奨事項

［推奨事項を挿入］

所見 2　［全般的なトピック領域を挿入］

［所見を挿入］

推奨事項

［推奨事項を挿入］

所見と推奨事項の例:

所見 1　コミュニケーション

緊急時対応計画のメンバーとコミュニケーションをとるための標準化されたシステムを確認する計画が存在しない。

推奨事項

- *[組織名を挿入]*は、標準化された通信要件の確立、予備通信システムの配置方法と配置場所の指定、および担当者による予備通信システムの利用手順の説明を内容とする通信計画の作成を検討するべきである。
- *[組織名を挿入]*は、冗長通信システムを明らかにして、緊急時に重要な担当者と連絡をとることができるようにするべきである。冗長通信システムは、家庭用電話や携帯電話、ノートパソコン、そのほかの通信システムなどで構成することができる。

所見 2　移動キット

重要な担当者に対し、緊急時に移動先の施設に運ぶ、業務遂行に必要な用品類の含まれた移動キットが支給されていない。

推奨事項

- *[組織名を挿入]*は、緊急時に移動する担当者向けに、移動キットを作成して事前に配布する可能性を検討するべきである。長時間配置される場合に担当者に必要となる用品に加え、移動キットには担当者が自身の重要な機能を果たすために必要な情報が記録されたフラッシュドライブ、ディスクまたは CD-ROM を含める必要がある。

［サンプル］評価用紙

評価用紙記入へのご協力お願いいたします。

演習イベント名を挿入

演 習 評 価 用 紙

日付を挿入

演習に関する以下の質問にお答えください。

氏 名 _____

1)． 自分の責任を果たすために必要な情報とリソースはすべて手元にありましたか。

2)． 移動先施設で責任を果たすためのトレーニングは十分でしたか。

3)． 演習の構成は現実的でしたか。

4)． 演習中、うまく行った点、うまく行かなかった点について自由にお書きください。

5)． 緊急時に移動先施設で長期にわたって業務を継続するための準備は十分にできましたか。*いずれか 1 つに○をつけてください。*

準備できていない　　多少準備はできた　　準備できた　　十分準備できた

6)． 演習全体をどう評価しますか。*いずれか 1 つに○をつけてください。*

改善が必要　　普通　　良かった　　非常に良かった

[サンプル]評価結果

*[日付を挿入]*に実施された*[機能演習名を挿入]*のあと、演習の感想を記入する評価用紙が参加者に手渡された。参加者は、評価用紙において、演習を数値で評価したり、事後レポートに記載する検討事項を記入したりできる。参加者の反応の詳細については「別紙 1」を参照のこと。*[別紙はそれぞれ、個々の演習イベントの評価用紙の内容が反映される。評価用紙に、評価尺度で記入する項目があれば、円グラフや棒グラフで表現できる。]*

質問は、取り上げるべき課題が他にあったかどうか、演習をやって良かったか、演習から得たものは何か、そして演習の改善に向けて何が出来るかを参加者に尋ねる内容となっている。*[パーセンテージの数値を挿入]*の参加者が評価用紙に記入した。

他に取り上げるべき課題があったかどうかに関する質問に対しては、評価を記入した参加者のうちおよそ*[パーセンテージの数値を挿入]*が、必要な課題が演習で網羅されていたと回答した。その他のコメントとしては、*[関連情報を挿入]などがあった。*

演習をやって良かったかどうかの質問に対しては、評価を記入した参加者のうち*[パーセンテージの数値を挿入]*が、演習をやって良かったと回答した。コメントとしては、*[関連情報を挿入(たとえば、「初めてにしては良かった」、「非常に有益であった」など)]などがあった。*

演習から何を得たかに関する質問に対しては、評価を記入した参加者のうち*[パーセンテージの数値を挿入]*が、*[関連情報を挿入]*と回答した。

別紙 1:参加者の回答

演習についての感想	演習から得たもの
■ *[コメントを挿入]*	■ *[コメントを挿入]*
■	■
■	■
■	■

全体的に、*[機能演習名を挿入]*から得られたフィードバックは*[関連情報を挿入]*。

付録C—テスト用文書のサンプル

付録 C では、3 種類のテスト（構成要素テスト、システムテスト、総合テスト）に対応する以下のサンプル文書を示す。

- テスト構成の説明
- テスト計画
- テストの概要説明（参加者用）
- テストの投入メッセージまたは行動
- テスト内容有効性確認ワークシート
- テスト内容評価ワークシート
- テストの事後レポート

これらのサンプル文書は、テスト用文書の設計と作成の担当者がテンプレートとして使用できるよう構成されている。

C.1 構成要素テスト用文書のサンプル

構成要素テストの例は、以前、緊急放送用ネットワーク（Emergency Broadcast Network）と呼ばれていた米国の緊急警報システム（Emergency Alert System）[24]の不定期テストである。このようなテストでは、機器のテストが行われ、緊急事態を伝える音とアナウンスがラジオやテレビで放送される。このテストでは、応答者による対処が必要な緊急事態のシミュレーションは、行われないが、メッセージによって、システムを構成する特定の構成要素がテストされる。

［サンプル］構成要素テスト計画

［テストの種類または名前を挿入］

構成要素テスト計画

テスト実施日：*［日付を挿入］*

期間：*［時刻を挿入］～［時刻を挿入］*

頻度：*［頻度を挿入］*

テストの重点：*［テストの重点を挿入］*

テストの目標：このテストの目標は次のとおりである。

- 実際の試験環境で緊急用放送システムのハードウェアを検査する
- 遅延、障害、および改善すべき領域を明確にする

テストの詳細：*［テストの詳細を挿入］*

参加者：*［参加者を挿入］*

トレーニングスタッフ：*［トレーニングスタッフを挿入］*

検証スタッフ：*［検証スタッフを挿入］*

評価スタッフ：*［評価スタッフを挿入］*

テスト中止手順：*［テストの中止手順を挿入］*

テストに関する中心的な連絡先：*［テストに関する中心的な連絡先を挿入］*

テスト実施許可者：*［テスト実施許可者を挿入］*

[24] 緊急警報システムの詳細については、http://www.fcc.gov/eb/eas/を参照のこと。

[サンプル]構成要素テストの概要説明(参加者用)

[日付を挿入]、*[時刻を挿入]*より*[時刻を挿入]*まで、[組織またはポリシーを挿入]の*[構成要素を挿入]*のテストを行う。参加者は、以下の作業を行うことが期待されている。

- *[作業を挿入]*
- *[作業を挿入]*

テスト中止手順: *[テストの中止手順を挿入]*

不明な点のある場合は、*[連絡先を挿入]*に問い合わせること。

[サンプル]構成要素テストの投入メッセージまたは行動

緊急警報システムを始動する。それに伴って以下の機能が実行される。

- 通常の番組の中断。
- 次のメッセージを放送する。*「これはテストです。お聞きの(ご覧の)放送局[任意 ー 放送局のコールサインを挿入]は、緊急放送システムのテストを行っています。これはテストです。」*
- EBS エンコーダから 2 音の警報信号を送信する。
- 次のメッセージを放送する。*「これは緊急放送システムのテストです。皆様の地域の放送局が、政府、州、地域の関係当局と自発的に連携し、緊急事態を皆様に伝えるこのシステムを開発しました。実際の緊急事態の場合、[任意 ー 放送局は必要に応じ、その地域で発生する可能性のある緊急事態の種類について触れる]、先ほどお聞きになった警報信号に続いて、公式の情報、ニュース、指示が放送されます。[任意 ー放送局のコールサインを挿入]お聞きの(ご覧の)放送局は[対象地域名を挿入]地域向けに放送をお送りしています。これで緊急放送システムのテストを終了します。」*

[サンプル]構成要素テストの結果の検証

構成要素のテストには、構成要素またはシステムが意図どおりに機能しているかどうかを判断するための検証基準が必要である。テスト結果の検証には、構成要素またはシステムが正常に機能していることを測定する指標が含まれる。さらに、期待される結果についても詳述する必要がある。この例の場合、2 音の警報信号とメッセージが明瞭に聞き取れることが該当する。

[サンプル]構成要素テストの有効性確認ワークシート

[テストの種類または名前を挿入]

構成要素テストの有効性確認ワークシート

テスト実施日:*[日付を挿入]*

期間:*[時刻を挿入]*～*[時刻を挿入]*

テストの重点:*[テストの重点を挿入]*

参加者:*[参加者を挿入]*

トレーニングスタッフ:*[トレーニングスタッフを挿入]*

検証スタッフ:*[検証スタッフを挿入]*

テストの目標:このテストの目標は次のとおりである。

- 実際の試験環境で緊急用放送システムのハードウェアを検査する
- 遅延、障害、および改善すべき領域を明確にする

検証方法:*[検証方法を挿入]*

テスト結果を検証することはできたか。*[回答を挿入]*

コメント:*[コメントを挿入]*

テストの中で検証できなかった部分はあるか。*[回答を挿入]*

コメント:*[コメントを挿入]*

推奨事項:*[推奨事項を挿入]*

[サンプル]構成要素テストの評価

テストは、目標および結果の判断基準に基づいて評価を行い、システムのテストおよび関連の構成要素とプロセスが適切に実行されたかどうかを判断する必要がある。考えられる改善点と推奨事項は、評価プロセスの重要な項目である。

[サンプル]構成要素テストの評価ワークシート

[テストの種類または名前を挿入]

構成要素テストの評価ワークシート

テスト実施日:*[日付を挿入]*

期間:*[時刻を挿入]*～*[時刻を挿入]*

テストの重点:*[テストの重点を挿入]*

参加者:*[参加者を挿入]*

トレーニングスタッフ: *[トレーニングスタッフを挿入]*

検証スタッフ: *[検証スタッフを挿入]*

評価スタッフ: *[評価スタッフを挿入]*

テストの目標:このテストの目標は次のとおりである。

- 実際の試験環境で緊急警報システムをテストする
- 遅延、障害、および改善すべき領域を明確にする

テストの目標は達成されたか。*[回答を挿入]*

コメント: *[コメントを挿入]*

テストの詳細: *[テストの詳細を挿入]*

テストの実施基準は適切であったか。*[回答を挿入]*

コメント: *[コメントを挿入]*

テストの実施基準は、改善可能か。*[回答を挿入]*

コメント: *[コメントを挿入]*

テスト結果の検証基準は適切であったか。*[回答を挿入]*

テスト結果の検証基準は、改善可能か。*[回答を挿入]*

コメント: *[コメントを挿入]*

テストは想定どおり実行されたか。*[回答を挿入]*

コメント: *[コメントを挿入]*

テスト中に障害が発生したか。*[回答を挿入]*

発生した障害が原因でテストは失敗したか。*[回答を挿入]*

コメント: *[コメントを挿入]*

推奨事項: *[推奨事項を挿入]*

構成要素テストの事後レポート

構成要素テストの事後レポートは、以下の内容で構成する。

- 全般的な成果(要旨の形式で作成することが多い)
- 具体的な成果

■ 裏付けデータ

構成要素テストの全般的な成果

「全般的な成果」のセクションでは、テストの結果に重点を置く。たとえば、以下に示すような記述で構成する。

> 今回の構成要素テストでは、参加者は*[関連情報を挿入]*をテストするよい機会を得た。構成要素テストの結果、参加者は*[関連情報を挿入]*の重要性に対する意識を高めた。*[組織名または部署名を挿入]*は全体として、*[関連情報を挿入]*をテストの結果として学んだ。

構成要素テストの具体的な成果

「具体的な成果」のセクションでは、テストの結果をより詳細に示す。具体的には構成要素の技術的側面を理解する者が、テストの結果を評価して構成要素またはプロセスを改善できるレベルの詳細さが求められる。以下は、具体的な成果を示すセクションの概要の例である。

> 演習時の所見、および計画の強化につながる推奨事項は次のとおりである。
>
> **所見 1　　*[全般的なトピック領域を挿入]***
>
> *[所見を挿入]*
>
> **推奨事項**
>
> *[推奨事項を挿入]*
>
> ***所見 2　　[全般的なトピック領域を挿入]***
>
> *[所見を挿入]*
>
> **推奨事項**
>
> *[推奨事項を挿入]*

裏付けデータ

事後レポートの「裏付けデータ」セクションには、テスト時に収集された具体的なデータを示す。データは、収集方法に関する簡単な説明を添えた添付文書に記載されることが多い。

C.2 システムテスト用文書のサンプル

システムテストの例は、組織のデータをバックアップし復元するシステムとその手順のテストである。このテストでは、データバックアップ機器、およびデータのアーカイブ作成と復元の手順のあらゆる側面をテストする。

[サンプル]システムテストの内容:

システムテスト(System Test):データのバックアップと復元

- データのバックアップ手順のテスト
- データのバックアップ機器のテスト
- バックアップデータの完全性検証手順のテスト
- ローカルのデータ保管手順のテスト
- ローカルのデータ取得手順のテスト
- オフサイトのデータ保管手順のテスト
- オフサイトのデータ取得手順のテスト
- UNIX システムのデータ復旧テスト
- Microsoft システムのデータ復旧テスト
- ネットワークシステムのデータ復旧テスト
- その他のシステムのデータ復旧テスト

[サンプル]システムテストの計画:

[テストの種類または名前を挿入]

システムテスト計画

テスト実施日: *[日付を挿入]*

期間: *[時刻を挿入]*～*[時刻を挿入]*

頻度: *[頻度を挿入]*

テストの重点: *[テストの重点を挿入]*

テストの目標: *[テストの目標を挿入]*

テストの詳細: *[テストの詳細を挿入]*

テスト対象の構成要素:

- *[構成要素を挿入]*
- *[構成要素を挿入]*
- *[構成要素を挿入]*

システムテスト構成要素 1: *[構成要素を挿入]*[25]

- **構成要素テストの参加者**: *[参加者を挿入]*
- **構成要素テストの検証スタッフ**: *[検証スタッフを挿入]*
- **構成要素テストの評価スタッフ**: *[評価スタッフを挿入]*
- **構成要素テスト中止手順**: *[テストの中止手順を挿入]*
- **構成要素テストに関する中心的な連絡先**: *[テストに関する中心的な連絡先を挿入]*
- **構成要素テスト実施許可者**: *[テスト実施許可者を挿入]*

システムテストに関する中心的な連絡先: *[システムテストに関する中心的な連絡先を挿入]*

システムテスト実施許可者: *[システムテスト実施許可者を挿入]*

[サンプル]システムテストの概要(参加者用)

[日付を挿入]、*[時刻を挿入]*より*[時刻を挿入]*まで、[部署またはポリシーを挿入]の[構成要素またはシステムを挿入]のテストを行う。以下に示す各構成要素をテストする。

- *[構成要素を挿入]*。日付: *[日付を挿入]*。時刻: *[時刻を挿入]*～*[時刻を挿入]*。
- *[構成要素を挿入]*。日付: *[日付を挿入]*。時刻: *[時刻を挿入]*～*[時刻を挿入]*。

*[システムを挿入]*システムテストにおける*[構成要素を挿入]*構成要素テスト[26]

[日付を挿入]、*[時刻を挿入]*より*[時刻を挿入]*まで、*[部署またはポリシーを挿入]*の*[構成要素を挿入]*のテストを行う。参加者は、以下の作業を行うことが期待されている。

- *[作業を挿入]*
- *[作業を挿入]*

テスト中止手順: *[テストの中止手順を挿入]*

不明な点のある場合は、*[連絡先を挿入]*に問い合わせること。

[サンプル]システムテストの検証

[25] このサブセクションは、必要に応じ、システムテストに含まれる構成要素テストごとに繰り返す。
[26] このサブセクションは、必要に応じ、システムテストに含まれる構成要素テストごとに繰り返す。

システムテストでは、システムテストおよび関連の構成要素テストまたは手順が意図どおりに機能しているかどうかを評価する方法と基準が必要となる。テスト結果の検証には、構成要素またはプロセスが正常に機能していることを測定する指標が含まれ、期待される結果の詳細が示される。システムテストが有効であったかどうかは、各構成要素テストの目標と検証結果を確認することで判断できる。

この例では、このシステムテストを検証するには、バックアップ手順の正確さの確認、バックアップシステムを構成する各機器のデータバックアップ機能の確認、データ完全性チェックの確認、ローカルおよびオフサイトのデータ保管・取得手順の確認、およびバックアップシステムを構成する各機器のシステム復元機能が期待どおり機能するかの確認を行う必要がある。

[サンプル]システムテストの有効性確認ワークシート

[テストの種類または名前を挿入]

システムテスト有効性確認ワークシート

テスト実施日:*[日付を挿入]*

期間:*[時刻を挿入]*～*[時刻を挿入]*

テストの重点:*[テストの重点を挿入]*

参加者:*[参加者を挿入]*

トレーニングスタッフ:*[トレーニングスタッフを挿入]*

検証スタッフ:*[検証スタッフを挿入]*

テストの目標:このテストの目標は次のとおりである。

- *[目標を挿入]*
- *[目標を挿入]*

テスト対象の構成要素:*[テスト構成要素を挿入]*

検証方法:*[検証方法を挿入]*

テスト結果を検証することはできたか。*[回答を挿入]*

コメント:*[コメントを挿入]*

テストの中で検証できなかった構成要素はあるか。*[回答を挿入]*

コメント:*[コメントを挿入]*

推奨事項:*[推奨事項を挿入]*

[サンプル]システムテストの評価

テストは、目標および結果の判断基準に基づいて評価を行い、システムのテストおよび関連の構成要素とプロセスが適切に実行されたかどうかを判断する必要がある。考えられる改善点と推奨事項は、評価プロセスの重要な項目である。

[サンプル]システムテストの評価ワークシート

[テストの種類または名前を挿入]

システムテスト評価ワークシート

テスト実施日:*[日付を挿入]*

期間:*[時刻を挿入]*～*[時刻を挿入]*

テストの重点:*[テストの重点を挿入]*

参加者:*[参加者を挿入]*

トレーニングスタッフ:*[トレーニングスタッフを挿入]*

検証スタッフ:*[検証スタッフを挿入]*

評価スタッフ:*[評価スタッフを挿入]*

テスト対象の構成要素:*[テスト構成要素を挿入]*

テストの目標:このテストの目標は次のとおりである。

- *[目標を挿入]*
- *[目標を挿入]*

テストの目標は達成されたか。*[回答を挿入]*

コメント:*[コメントを挿入]*

テストの詳細:*[テストの詳細を挿入]*

テストの実施基準は適切であったか。*[回答を挿入]*

コメント:*[コメントを挿入]*

テストの実施基準は、改善可能か。*[回答を挿入]*

コメント:*[コメントを挿入]*

テスト結果の検証基準は適切であったか。*[回答を挿入]*

テスト結果の検証基準は、改善可能か。*[回答を挿入]*

コメント:*[コメントを挿入]*

テストは想定どおり実行されたか。*[回答を挿入]*

コメント: *[コメントを挿入]*

障害の発生したテスト構成要素はあるか。*[回答を挿入]*

発生した障害が原因でテストは失敗したか。*[回答を挿入]*

コメント: *[コメントを挿入]*

推奨事項: *[推奨事項を挿入]*

システムテストの事後レポート

システムテストの事後レポートは、以下の内容で構成する。

- 全般的な成果（要旨の形式で作成することが多い）
- 具体的な成果
- 裏付けデータ

システムテストの全般的な成果

「全般的な成果」のセクションでは、システムテストの結果に重点を置く。たとえば、以下に示すような記述で構成する。

> 今回のシステムテストでは、参加者は*[関連情報を挿入]*のよい機会を得た。テストの結果、参加者は*[関連情報を挿入]の重要性*に対する意識を高めた。*[組織名または部署名を挿入]*は全体として、*[関連情報を挿入]*をテストの結果として学んだ。

システムテストの具体的な成果

「具体的な成果」のセクションでは、テストの結果をより詳細に示す。具体的には構成要素の技術的側面を理解する者が、テストの結果を評価して構成要素またはプロセスを改善できるレベルの詳細さが求められる。以下は、具体的な成果を示すセクションの概要の例である。

> 演習時の所見、および計画の強化につながる推奨事項は次のとおりである。
>
> **所見 1　　［全般的なトピック領域を挿入］**
>
> *［所見を挿入］*
>
> **推奨事項**
>
> *［推奨事項を挿入］*
>
> **所見 2　　［全般的なトピック領域を挿入］**
>
> *［所見を挿入］*

推奨事項

［推奨事項を挿入］

裏付けデータ

事後レポートの「裏付けデータ」セクションには、テスト時に収集された具体的なデータを示す。データは、収集方法に関する簡単な説明を添えた添付文書に記載されることが多い。たとえば、各構成要素テストで使用した用紙を裏付けデータとして添付することが考えられる。

C.3 総合テスト用文書のサンプル

総合テストの例では、組織の事業継続計画に含まれるシステムと構成要素すべてをテストする。このテストでは、各システムで使用されるすべての機器、プロセス、手順、および関連構成要素を 1 つの包括的単位としてテストする。

[サンプル]総合テスト計画の概要

総合テスト計画は特に、組織のセキュリティ計画や事業継続計画などの計画を中心に設計されているため、テスト用文書のサンプルすべてを示すことは実用的ではない。ただし、このセクションでは包括的な計画の一部として、システムと構成要素テストの内容をまとめた計画の概要を示す。付録 C.1 および付録 C.2 に示す、構成要素およびシステムのテスト用の用紙は、総合テストを構成する一部として使用できる。

[サンプル]総合テストの構成

総合テストは、いくつかの構成要素テストで構成された、複数のシステムテストで構成される。次の例は、ある総合テストの一部分の構成を示したものである。

総合テスト:事業継続計画

- **システムテスト**:データのバックアップと復元
  - **構成要素テスト**:データのバックアップ手順のテスト
  - **構成要素テスト**:データのバックアップ機器のテスト
  - **構成要素テスト**:バックアップデータの完全性検証手順のテスト
  - **構成要素テスト**:ローカルのデータ保管手順のテスト
  - **構成要素テスト**:ローカルのデータ取得手順のテスト
  - **構成要素テスト**:オフサイトのデータ保管手順のテスト
  - **構成要素テスト**:オフサイトのデータ取得手順のテスト
  - **構成要素テスト**:UNIX システムのデータ復旧テスト
  - **構成要素テスト**:Microsoft システムのデータ復旧テスト
  - **構成要素テスト**:ネットワークシステムのデータ復旧テスト
  - **構成要素テスト**:その他のシステムのデータ復旧テスト
  - **構成要素テスト**:遅延、障害、および改善すべき領域を明確にする

[サンプル]総合テストの計画

[テストの種類または名前を挿入]

総合テスト計画

テスト実施日: *[日付を挿入]～[日付を挿入]*

期間: *[時刻を挿入]～[時刻を挿入]*

頻度: *[頻度を挿入]*

テストの重点: *[テストの重点を挿入]*

テストの目標: *[テストの目標を挿入]*

テストの詳細: *[テストの詳細を挿入]*

テスト対象のシステム:

- *[システムテストを挿入]*
- *[システムテストを挿入]*
- *[システムテストを挿入]*

システム 1: *[システムテストを挿入]*[27]

システム 1 構成要素テスト:

- *[構成要素テスト項目を挿入]*
- *[構成要素テスト項目を挿入]*
- *[構成要素テスト項目を挿入]*

構成要素テスト 1: *[構成要素を挿入]*[28]

- 構成要素テストの参加者: *[参加者を挿入]*
- 構成要素テストの検証スタッフ: *[検証スタッフを挿入]*
- 構成要素テストの評価スタッフ: *[評価スタッフを挿入]*
- 構成要素テスト中止手順: *[テストの中止手順を挿入]*
- 構成要素テストに関する中心的な連絡先: *[テストに関する中心的な連絡先を挿入]*
- 構成要素テスト実施許可者: *[テスト実施許可者を挿入]*

総合テスト中止手順: *[テストの中止手順を挿入]*

総合テストに関する中心的な連絡先: *[テストに関する中心的な連絡先を挿入]*

総合テスト実施許可者: *[テスト実施許可者を挿入]*

[サンプル]総合テストの結果の検証

[27] このサブセクションは、必要に応じ、総合テストに含まれるシステムテストごとに繰り返す。
[28] このサブセクションは、必要に応じ、各システムテストに含まれる構成要素テストごとに繰り返す。

数多くのシステムおよびシステム構成要素を対象とする総合テストには、構成要素またはプロセスが意図どおりに機能しているかどうかを評価する方法と基準が必要となる。総合テストは、多数のシステムテストと構成要素テストを集めたものであり、テストでは、それぞれのシステムと構成要素の検証結果を総合的に評価する。

総合テストの結果の検証には、構成要素またはプロセスが正常に機能していることを測定する指標を含める必要がある。また、期待される結果を詳しく示す必要がある。

[サンプル]総合テストの結果の評価

総合テストでは、目標および結果の判断基準に基づいて評価を行い、総合テストおよび関連のシステムテストと構成要素テストが適切に実行されたかどうかを判断する必要がある。総合テストは、多数のシステムテストと構成要素テストを集めたものであり、テストでは、それぞれのシステムと構成要素の検証結果を総合的に評価する考えられる改善点と推奨事項は、評価プロセスの重要な項目である。

総合テストの事後レポート

総合テストの事後レポートは、以下の内容で構成する。

- 全般的な成果(要旨の形式で作成することが多い)
- 具体的な成果
- 裏付けデータ

総合テストの全般的な成果

「全般的な成果」のセクションでは、テストの結果に重点を置く。たとえば、以下に示すような記述で構成する。

> 今回の総合テストでは、参加者は*[関連情報を挿入]*のよい機会を得た。テストの結果、参加者は*[関連情報を挿入]の重要性*に対する意識を高めた。*[組織名または部署名を挿入]*は全体として、*[関連情報を挿入]*をテストの結果として学んだ。

総合テストの具体的な成果

「具体的な成果」のセクションでは、テストの結果をより詳細に示す。具体的には構成要素の技術的側面を理解する者が、テストの結果を評価して構成要素またはプロセスを改善できるレベルの詳細さが求められる。以下は、具体的な成果を示すセクションの概要の例である。

> 演習時の所見、および計画の強化につながる推奨事項は次のとおりである。
>
> **所見 1　　*[全般的なトピック領域を挿入]***
>
> *[所見を挿入]*
>
> **推奨事項**
>
> *[推奨事項を挿入]*

所見 2　　*[全般的なトピック領域を挿入]*

[所見を挿入]

推奨事項

[推奨事項を挿入]

裏付けデータ

事後レポートの「裏付けデータ」セクションには、テスト時に収集された具体的なデータを示す。データは、収集方法に関する簡単な説明を添えた添付文書に記載されることが多い。

付録D—用語集

付録 D では、この文書で使用している用語の定義を示す。

事後レポート（After Action Report）：演習またはテストによって明らかになった事柄や推奨事項が記された文書。

構成要素テスト（Component Test）：ハードウェアやソフトウェアの個々の構成要素、または関連する構成要素のグループを対象に実行するテスト。

総合テスト（Comprehensive Test）：ある特定の IT 計画（緊急時対応計画、コンピュータセキュリティインシデント対応計画など）を支援するシステムや構成要素のすべてを対象としたテスト。

コントロールセル（Control Cell）：演習の調整を行う中心的な場所。通常、演習への参加者から離れた場所に配置される。

演習管理者（Controller）：機能演習を担当するスタッフメンバの 1 人。設定された目標が達成されるよう、演習活動を監視、運営、調整する。

データ収集担当者（Data Collector）：演習中またはテスト中に生じた出来事や活動に関する情報を記録する人物。

演習（Exercise）：緊急事態のシミュレーションのことで、IT 計画の 1 つ以上の側面について、その実用性を検証することを目的とする。

演習概要（Exercise Briefing）：演習時に参加者に配付される資料。演習次第、演習の目的、シナリオ、その他の関連情報がまとめられている。

演習責任者（Exercise Director）：人員配置、演習計画の作成、実施、実行計画など、演習のあらゆる側面の責任を担う人物。

進行者用ガイド（Facilitator Guide）：演習において演習の進行者が必要とする文書。これには、演習の目的、範囲、目標およびそれらの目標の達成に必要なシナリオに加えて、シナリオに関する質問リストおよび IT 計画のコピーなどが含まれる。

進行者（Facilitator）：演習の参加者間の議論を促す人物。

機能演習（Functional Exercise）：運用の責任を担う担当者が、シミュレーション用運用環境において、IT 計画の検証、および緊急時のための運用面の準備状況の検証を行えるようにするための演習。

ホットウォッシュ／反省会（Hotwash）：演習またはテストの実施直後に、スタッフと参加者が行う報告反省会のこと。

マスタシナリオイベントリスト（MSEL：Master Scenario Events List）：参加者が演習時に対応を求められることになる、シミュレーションイベントおよび主要イベントの内容を時系列に従って一覧にしたもの。

投入メッセージ（Message Inject）：演習の実施中に参加者に与えられる、あらかじめ用意されたメッセージ。

参加者ガイド（Participant Guide）：一般に、演習の目的、範囲、目標、シナリオ、演習の対象となる IT 計画のコピーを含む、演習時に使用する文書。

計画コーディネータ（Plan Coordinator）：IT 計画作成のすべての側面（IT 計画の維持に関わる TT&E 要素を含む）について責任を持つ人物。計画コーディネータは、計画の作成、遂行、維持を含め、計画について全体的な責任を負う。

シナリオ（Scenario）：仮想のインシデントを、順を追って説明するストーリーとして構成したもの。演習用の状況設定を定め、対応が必要となる状況を創り出し、演習の目標を実践できるようにすることを目的としている。仮想のインシデントを、順を追って説明するストーリーとして構成したもの。

シミュレーション担当者（Simulators）：機能演習のスタッフメンバの 1 人。演習に参加していない個人または組織の代理を務め、演習の進行に必要なインプットを提供する。

システムテスト（System Test）：指定の要件を満たしているかどうか評価するために、完全なシステムを対象に実行されるテスト。

机上演習（Tabletop Exercise）：議論ベースの演習で、特定の IT 計画における役割と責任を与えられた担当者が会議室に集まったり、その場でグループを作ったりして、緊急時の役割や、ある特定の緊急事態への対応策を議論することによって、その IT 計画の内容を検証すること。進行者は、シナリオを提示し、シナリオに基づいた質問を行うことで議論を開始する。

テスト（Test）：定量化可能な測定基準を用いて、IT 計画に指定されている運用環境において IT システムまたはシステム構成要素の運用性を検証するための評価手段のこと。

テスト責任者（Test Director）：人員配置、計画や文書の作成、テストの実施、実行計画の調整など、ストのあらゆる側面について責任を負う人物。

テストガイド（Test Guide）：テストの実施に関する基本的な手順がまとめられ、参加者のリスト、テストの影響を受ける可能性のある個人およびグループのリスト、テスト早期中止の場合の手順が記載された文書。

テスト計画（Test Plan）：**実行**に関して必要な項目、および各手順について期待される結果または対応を含め、特定のテストにおいて実行される具体的な手順をまとめた文書。

TT&E イベント（Test, Training, and Exercise (TT&E) Event）：組織が IT 計画に関連する問題を明らかにし、不都合な状況が発生する前に対策を実施できるようにすることで、IT 計画の維持を支援するイベント。

TT&E 計画（Test, Training, and Exercise (TT&E) Plan）：IT 計画における役割と責任についての担当者のトレーニング、IT 計画の有効性を検証するための IT 計画の演習、および IT 計画の状況における IT 構成要素またはシステムの運用性を確認するためのテストの実施をそれぞれ確実に行うための手順をまとめた計画。

TT&E ポリシー（Test, Training, and Exercise (TT&E) Policy）：担当者のトレーニング、IT 計画の演習実施、IT 構成要素とシステムのテストに関連する、組織の内部要件と外部要件を概括するポリシー。

TT&E プログラム（Test, Training, and Exercise (TT&E) Program）：IT 計画における役割と責任についての担当者のトレーニング、IT 計画の有効性を検証するための IT 計画の演習、および IT 計

画の状況における IT 構成要素またはシステムの運用性を確認するためのテストの実施をそれぞれ確実に行うための手段。

TT&E プログラムコーディネータ（Test, Training, and Exercise (TT&E) Program Coordinator）: TT&E 計画を作成し、TT&E イベントの調整を行う人物。

トレーニング（Training）: 担当者に、ある特定の IT 計画における役割と責任を伝達し、その役割と責任に関わる技能を教えること。

（本ページは意図的に白紙のままとする）

付録E—略語

このガイドで使われている主な略語を以下に定義する。

AF	Alternate Facility（代替施設）
CD	Compact Disk（コンパクトディスク）
CIO	Chief Information Officer（最高情報責任者）
COOP	Continuity of Operations（運用の継続）
FISMA	Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
FPC	Federal Preparedness Circular（連邦準備令）
IEEE	Institute of Electrical and Electronics Engineers（電気電子学会）
IT	Information Technology（情報技術）
ITL	Information Technology Laboratory（情報技術ラボラトリ）
MSEL	Master Scenario Events List（マスタシナリオイベントリスト）
NIST	National Institute of Standards and Technology（米国国立標準技術研究所）
OCIO	Office of the Chief Information Officer（最高情報責任者室）
OMB	Office of Management and Budget（行政管理予算局）
SP	Special Publication（特別刊行物）
TT&E	Test, Training, and Exercise（テスト、トレーニング、および演習）
UTSA	University of Texas-San Antonio（テキサス大学サンアントニオ校）

（本ページは意図的に白紙のままとする）

付録F—印刷資料およびオンライン資料

付録 F では、IT 演習の範囲決定、計画作成、文書化、実施、評価に役立つ印刷物とオンライン情報を紹介する。

- Federal Emergency Management Agency, Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*, June 15, 2004. http://www.fema.gov/pdf/library/fpc65_0604.pdf
- Federal Information Security Management Act of 2002, *Public Law 107-347*, December 2002. http://csrc.nist.gov/policies/FISMA-final.pdf
- Homeland Security Exercise and Evaluation Program, May 2004. http://www.ojp.usdoj.gov/odp/docs/HSEEPv3.pdf
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004. http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems*, February 8, 1996. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government*, October 21, 1998. http://www.fas.org/irp/offdocs/pdd/index.html

（本ページは意図的に白紙のままとする）

付録G—索引

ひ

ふ

ほ

ま