NIST Special Publication 800-30
Revision 1

リスクアセスメントの実施の手引き

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

情報セキュリティ

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

2012 年 9 月

米国商務省　長官代理
Rebecca M. Blank

米国国立標準技術研究所　標準技術担当次官兼所長
Patrick D. Gallagher

コンピュータシステムの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、以下、ITL と称す）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。ITL は、テストの開発、テスト技法の開発、参照データの作成、概念実証の実施および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。ITL の責務には、連邦政府の情報システムにおいて、国家安全保障にかかわらない情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、管理面、運用面、技術面および物理面での標準およびガイドラインを策定することが含まれる。本 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 ITL の調査、ガイドラインおよびアウトリーチの努力、ならびに業界団体、政府機関および学術機関との共同活動について報告する。

文書の効力

NIST は、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果たすために、この文書を作成した。NIST は、連邦政府情報システムに対する、最低限の要求事項を含んだ情報セキュリティ標準およびガイドラインを作成する責務がある。ただし、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対する政策権限を行使する適切な連邦政府当局者による明確な承認がない限り、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、OMB（行政管理予算局）Circular A-130 の第 8b(3)項『Securing Agency Information Systems（政府機関の情報システムの保護）』の要求事項との一貫性を保っており、これは Circular A-130 の付録 IV『Analysis of Key Sections（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、Circular A-130 の付録 III『Security of Federal Automated Information Resources』に記載されている。

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機関に対して適用と順守を義務づけた標準およびガイドラインを否定するものと解釈してはならない。また、本書に示すガイドラインは、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による既存の公式文書に変更を加えたり、これらに取って代わるものと解釈してはならない。本文書は、政府以外の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が、出典明記を求む。[1]

NIST Special Publication 800-30, 95 頁
(2012 年 9 月)
CODEN: NSPUE2

この文書中で特定される商業的組織、装置、資料は、実験的な手順または概念を適切に説明するためのものである。したがって、NIST による推薦または保証を意味するものではなく、これら組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもない。

本文書には、割り当てられた法的責任に従って NIST が現在作成している他の文書への参照が含まれている。本文書における概念および方法論を含む情報は、前述の関連文書が完成する前であっても使用してかまわない。したがって、各文書が完成するまでは、既存の要求事項、ガイドライン、および手順（存在する場合）が引き続き有効である。政府機関は、計画作成および移行を目的として、NIST によるこれらの新文書の作成状況を知りたいと考えるかもしれない。

各組織においても、パブリックコメントの募集期間中に、すべての公開ドラフト文書を閲覧し、コメントを NIST へ提出することができる。すべての NIST 発行文書は、//csrc.nist.gov/publications から入手できる。

本文書に関するコメントは、以下の宛先に送付願いたい。

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

[1] 著作権に関するこの記述は、SP800-30 Revision 1 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 情報処理推進機構に帰属する。

NIST の標準およびガイドラインへの準拠

FISMA の規定に従って [2]商務長官は、NIST が策定した標準およびガイドラインに基づいて、連邦政府の情報システムに関する標準およびガイドラインを定めるものとする。商務長官は、連邦政府の情報システムの運用の効率またはセキュリティを向上させるのに必要と判断されたレベルまで、標準の適用と順守を義務づけるものとする。商務長官が定める標準には、情報セキュリティに関する最低限の要求事項を示すか、さもなければ連邦政府の情報および情報システムのセキュリティを向上させるのに必要となる、情報セキュリティ標準を含めるものとする。

- 連邦情報処理規格(FIPS: Federal Information Processing Standards、以下 FIPS と称す)は、商務省長官の承認を受け、FISMA に従って NIST により発行される。連邦政府機関 [3]には、FIPS の適用と順守が義務づけられている。FISMA は、連邦政府機関がこれらの標準を順守することを要求している。したがって政府機関は、これらの標準の使用を放棄することはできない。
- Special Publications は、推奨および手引きとなる文書として、NIST が策定し発行する文書である。連邦政府機関は、国家安全保障にかかわらないすべてのプログラムとシステムにおいて、FIPS によって義務づけられている NIST Special Publications に従わなければならない。FIPS200 は、SP800-53(改訂を含む)の使用を義務づけている。さらに、S 行政管理予算局のポリシー(行政管理予算局が作成した、FISMA および Agency Privacy Management への報告に関するインストラクションを含む)には、国家安全保障にかかわらないすべてのプログラムとシステムにおいて、政府機関が特定の NIST Special Publication に従わなければならない旨が記載されている。[4]
- 省庁間共同報告(NISTIRs)および ITL Bulletins など、上記以外のセキュリティ関連の発行文書でも、NIST の活動に関する技術面での情報やその他の情報を提供している。これらの発行文書は、行政管理予算局によって指定されている場合に限り必須になる。
- NIST のセキュリティ標準およびガイドラインへの準拠に関するスケジュールは、行政管理予算局によって規定され、その内容は行政管理予算局のポリシー、指令、または覚書(例:FISMA への年次報告に関する手引き)に記載されている。[5]

---

[2] 電子政府法(公法第 107-347)は、米国の経済的利益と国家安全保障上の利益に対する情報セキュリティの重要性を認識している。連邦情報セキュリティマネジメント法と命名された電子政府法第 III 編は、それぞれの組織が、組織の業務と資産をサポートする情報システムに対するセキュリティを提供する、組織全体にわたるプログラムを作成、文書化および実施する必要性を強調している。

[3] 本文書では「政府機関」という用語をより一般的な用語である「組織」の代わりに使用している箇所があるが、これは、その使用が、連邦法または連邦政府ポリシーなどの、その他のソースドキュメントに直接関連する場合に限る。

[4] 連邦政府機関は、行政管理予算局のポリシーに則り、特定の NIST Special Publications に従わなければならないが、どのように手引きを適用するかについては、政府機関の裁量に任されている。連邦政府機関は、連邦政府機関のミッション、業務上の機能、および運用環境に合わせて、NIST Special Publications が規定するセキュリティ概念および原則を適用する。したがって連邦政府機関が NIST の手引きを適用した結果、異なるセキュリティソリューションとなることもあるが、それらのソリューションは受け入れられるものであり、NIST の手引きに準拠し、行政管理予算局が定める、連邦政府機関の情報システムに対する適切なセキュリティ(Adequate Security)にも適合するものである。連邦政府における情報の共有および透明性の確保は優先度が高いため、政府機関は情報セキュリティソリューションを開発する際に、互恵(reciprocity)についても考慮する。政府機関が NIST Special Publications に準拠しているかどうかを評価する場合には、監査官、評価者、監査人およびアセサー(assessor)は、その手引きに記載されているセキュリティ概念および原則の意図を考慮し、政府機関が自身のミッション／業務上の責任、運用環境、および組織固有の状況に合わせてどのように手引きを適用したかを考慮する。

[5] 特に明記しない限り、本章から参照される NIST 発行文書(FIPS と Special Publication)はすべて最新版である。

謝辞

本文書は、連邦政府向けの統一された情報セキュリティフレームワークを構築するための継続的な取り組みの一環として、民生、防衛および情報コミュニティの代表からなる Joint Task Force Transformation Initiative Interagency Working Group（以下、省庁間作業グループと称す）によって作成された。NIST は、献身的な努力をもって本文書の作成に大きく寄与してくれた、米国商務省および国防総省、国家情報長官室、国家安全保障システム委員会の最高幹部の方々、ならびに省庁間作業グループのメンバーに感謝の意を表する。最高幹部、省庁間作業グループのメンバーおよび関連組織には、以下の方々が含まれる:

国防総省

Teresa M. Takai
DoD Chief Information Officer

Richard Hale
Deputy Chief Information Officer for Cybersecurity

Paul Grant
Director, Cybersecurity Policy

Dominic Cussatt
Deputy Director, Cybersecurity Policy

Kurt Eleam
Policy Advisor

国家情報長官室

Adolpho Tarasiuk Jr.
Assistant DNI and Intelligence Community Chief Information Officer

Charlene Leubecker
Deputy Intelligence Community Chief Information Officer

Catherine A. Henson
Director, Data Management

Greg Hall
Chief, Risk Management and Information Security Programs Division

NIST

Charles H. Romine
Director, Information Technology Laboratory

Donna Dodson
Cybersecurity Advisor, Information Technology Laboratory

Donna Dodson
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

国家安全保障システム委員会

Teresa M. Takai
Chair, CNSS

Richard Spires
Co-Chair, CNSS

Dominic Cussatt
CNSS Subcommittee Co-Chair

Jeffrey Wilk
CNSS Subcommittee Co-Chair

省庁間作業グループ

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Jennifer Fabius *The MITRE Corporation*	Kelley Dempsey *NIST*
Deborah Bodeau *The MITRE Corporation*	Steve Rodrigo *Tenacity Solutions, Inc.*	Peter Gouldmann *Department of State*	Arnold Johnson *NIST*
Peter Williams *Booz Allen Hamilton*	Karen Quigg *The MITRE Corporation*	Christina Sames *TASC*	Christian Enloe *NIST*

上記の謝辞に加えて、Peggy Himes 氏と Elizabeth Lennon 氏（両者とも NIST）には、優れた技術編集および管理上の支援をいただいたことに心から感謝したい。著者は、また、国内外の公共および民間部門の個人および団体からいただいた多大な貢献にも深く感謝している。彼らの建設的で思慮深いコメントによって、本文書の全体的な質、完全さと実用性が高められた。

情報セキュリティの共通基盤の構築

公共および民間部門の機関との提携

NIST は、FISMA が要求する標準およびガイドラインを策定するにあたって、他の連邦政府機関および民間部門に助言を求めることにより、情報セキュリティの向上を図り、不要でありかつコスト高につながる努力の重複を避けると同時に、NIST 発行文書が、国家安全保障にかかわるシステムを保護するために採用される標準およびガイドラインへの補足となるよう努めている。NIST は、包括的なパブリックレビューおよび信用度調査プロセス(vetting process)に加えて、国家情報長官室(ODNI)、国防総省(DOD)、国家安全保障システム委員会(CNSS)と連携して、連邦政府全体にわたる情報セキュリティの共通基盤の構築に努めている。情報セキュリティの共通基盤を利用することで、連邦政府のインテリジェンス部門、防衛部門、および民生部門、ならびに彼らの受託業者は、情報システムの運用および使用により生じる組織の業務と資産、個人、他の組織、および国家に対するリスクを、より一貫性のある統一された方法で管理できるようになる。また、情報セキュリティの共通基盤は、セキュリティ認可判断の相互受け入れを実現するための強力な基盤を提供し、情報の共有を容易にする。NIST はまた、公共および民間部門の機関と連携して、NIST が策定したセキュリティ標準およびガイドラインと、ISO と IEC が策定した標準およびガイドラインとの具体的なマッピングと関係の確立に努めている。

目次

序文

「・・・リーダーは、リスクマネジメントプロセスを通じて、サイバースペースを自身が有利になるように利用するアドバーサリや、サイバースペースのグローバルな性質を利用して軍事活動、情報収集活動、ビジネス活動における目的を果たそうとする我々自身の取り組みから生じる、米国の利益に対するリスクについて考慮しなければならない。」

「・・・業務計画を策定する際には、脅威、脆弱性および影響の組み合わせを評価することによって、重要な動向を把握し、脅威の威力の排除あるいは低減、脆弱性の排除あるいは低減、およびすべてのサイバースペース活動の評価、調整、競合排除(deconflict)を行うために努力を傾けるべき分野を決定しなければならない。」

「あらゆる階層のリーダーは、他のあらゆる分野と同レベルの準備体制およびセキュリティを確保することに責任がある」

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

注意書

リスクアセスメントの適用範囲と適用性

- リスクアセスメントは、効果的なリスクマネジメントの重要な一部であり、リスクマネジメント階層内の 3 つのすべての層（組織レベル、ミッション／業務プロセスレベル、情報システムレベル）における意思決定を容易にする。
- リスクマネジメントは継続的な活動であるため、リスクアセスメントはシステム開発ライフサイクル全体にわたって実施される。なお、システム開発ライフサイクルには、システムの調達の前段階（すなわち、マテリアルソリューション分析および技術開発）から始まり、システムの調達（すなわち、技術／製造開発および生産／配備）と、保守（すなわち、運用／サポート）までが含まれる。
- 以下に関しては特定の要求事項は存在しない：(i) なんらかの特定のリスクアセスメントの特徴を定義するための形式、厳密さ、または詳細レベル; (ii) そうしたリスクアセスメントを実施するのに用いられる方法論、ツール、および技術; あるいは (iii) アセスメント結果の形式と内容、および関連する報告手段。組織は、リスクアセスメントをどのように実施するかに関して最大限の柔軟性を有する。また、組織には、組織のさまざまなニーズに対応し、リスクアセスメント活動を組織のより広範なリスクマネジメントプロセスに組み入れるためにも、本文書に記載されている手引きを適用することが推奨される。
- 組織は、また、リスクアセスメントが「測定のための精密計器」とならないことが多く、以下を反映することに注意しなければならない：(i) 採用されている特定のアセスメント方法論、ツールおよび技術の限界; (ii) 使用されるデータの主観性、質、および信頼性; (iii) アセスメント結果の解釈; ならびに (iv) アセスメントを実施する個人またはグループのスキルおよび専門知識。
- コスト、適時性、および使いやすさは、リスクアセスメントを適用するうえで重要な多くの要素の一部である。したがって組織は、可能な場合には常に、リスク関連情報を共有することによって、リスクアセスメントに要する作用レベルの低減に努めるべきである。

第 1 章

はじめに

企業全体にわたるリスクマネジメントを支援するリスクアセスメントの必要性

組織[6]（公共部門であるか、民間部門であるかにかかわらず）は、組織のミッションおよび業務上の機能を成功裏に実施するために情報技術[7]と情報システム[8]に依存している。 情報システムは、オフィスネットワーク、金融システムおよび人事システムに始まり、極めて特殊なシステム（例：産業用／プロセス制御システム、武器システム、通信システム、および環境制御システム）に至るまで、さまざまなエンティティを含む。情報システムは、既知の脆弱性と未知の脆弱性の両方を突いて、システムによって処理、格納、または伝送される情報の機密性、完全性、または可用性を侵害し、組織の業務と資産、個人、他の組織、および国家に負の影響をもたらしうる、深刻な脅威の標的になりやすい。情報システムに対する脅威は、意図的な攻撃、環境破壊、人的ミスまたは機械エラー、および構造上の欠陥を含み、米国の国家安全保障上の利益と経済安全保障上の利益を損なわせる可能性がある。したがって、あらゆる階層のリーダーおよび管理職者が、自身の責務を理解し、情報セキュリティリスク（すなわち、自組織のミッションおよび業務上の機能を支援する情報システムの運用と使用に伴うリスク）の管理に責任を負うことが必要不可欠である。

NIST SP800-39 に記載されているように、リスクアセスメントは、組織のリスクマネジメントプロセスの基本要素の1つである。リスクアセスメントは、情報システムの運用と使用により生じる組織の業務（すなわち、ミッション、機能、イメージ、評判）、組織の資産、個人、他の組織、および国家に対するリスクを特定、評価し、優先順位付けを行うために使用される。リスクアセスメントの目的は、意思決定者に対して情報を提供することと、以下を特定することによってリスク対応を支援することにある：(i) 組織に対する脅威、または、ある組織を介して他の組織に向けられた脅威; (ii) 組織の内部と外部に存在する脆弱性; (iii) 脅威が脆弱性を利用する可能性がある場合に発生する可能性のある影響（すなわち、被害）; ならびに (iv) 被害が発生する可能性。最終結果は、リスクの判断結果（すなわち、通常、被害の度合と、被害が発生する可能性をもとに算出される）である。リスクアセスメントは、リスクマネジメント階層内の 3 つのすべての層、すなわち、第 1 層（組織レベル）、第 2 層（ミッション／業務プロセスレベル）および第 3 層（情報システムレベル）で実施される。第 1 層と第 2 層におけるリスクアセスメントは、たとえば組織のガバナンスおよびマネジメント活動、ミッション／業務プロセス、エンタープライズアーキテクチャ、または情報セキュリティ導入計画のための資金拠出に関連する組織的な情報セキュリティ関連リスクを評価するために実施される。第 3 層におけるリスクアセスメントは、リスクマネジメントフレームワーク（すなわち、セキュリティ分類; セキュリティ管理策の選択、導入、お

[6] 本文書で使用されている「組織」という用語は、割り当てられたミッション／業務プロセスを実施することに責任を負い、それらのプロセスを支援する目的で情報システムを使用する組織的な構造（例：連邦政府機関、または、該当する場合、連邦政府機関の運用上のあらゆるエレメント）内のエンティティ（その規模、複雑さ、または位置づけは問わない）を示している。

[7] 組織は、また、情報技術を共通インフラ、共有サービス群、共通管理策群といった形で管理する。

[8] 情報システムとは、情報の収集、処理、保守、利用、共有、配布、または廃棄を目的として編成された、独立した一連の情報資源である。

よびアセスメント; 情報システムと共通管理策の運用認可; ならびにセキュリティ管理策のモニタリング）の実施をより効果的に支援するために実施される。[9]

1.1 目的および適用範囲

SP800-30 の目的は、連邦政府の情報システムおよび連邦組織におけるリスクアセスメントの実施の手引きを示すことにあり、本文書では SP800-39 に記載されている手引きを詳述している。リスクマネジメント階層内の 3 つのすべての層において実施されるリスクアセスメントは、リスクマネジメントプロセスの一部であり、最高幹部／管理職者に対して、特定されたリスクに対処するための適切な行動方針を決定するのに必要な情報を提供する。とりわけ、本文書は、リスクアセスメントプロセスの各ステップ（すなわち、アセスメントの準備、アセスメントの実施、アセスメントの結果の伝達、およびアセスメントの保守）を実施するための手引きを示し、リスクアセスメントおよび組織のその他のリスクマネジメントプロセスが互いにどのように補完しあい、情報を提供するかについて説明するものである。SP800-30 は、また、継続してモニタリングすべきリスク因子の特定に関する手引きを組織に提供する。この手引きに従うことによって、組織は、リスクが許容できないレベルまで増加しているか（すなわち、組織のリスク許容度を超えているか）、また、別の行動方針を取るべきかについて判断することができる。

本文書は、FISMA の要求事項を満たすものであり、行政管理予算局 が Circular A-130、付録 III『Security of Federal Automated Information Resources』によって規定している、執行機関 [10]向けの情報セキュリティ要求事項に適合する（あるいは、それらの要求事項を上回る）ものである。本文書に記載されているガイドラインは、44 U.S.C.のセクション 3542 が規定する国家安全保障にかかわるシステムを除き、すべての連邦情報システムに適用される。本ガイドラインは、国家安全保障にかかわるシステムに対する同様のガイドラインについても補足を行えるように、技術的な観点から広範囲にわたって作成されたものであり、そうしたシステムに対する政策権限を行使する適切な連邦政府当局者による承認があれば、そうしたシステムに適用することができる。州政府、地方政府、および隊組織はもとより、民間部門の組織においても、必要に応じて本ガイドラインの使用を検討することが推奨される。

1.2 対象と想定する読者

本文書は、以下の方々を含む、さまざまなリスクマネジメント専門家の一助となることを目指している

- リスクマネジメントのモニタリングに責任を持つ者（連邦政府機関の長、最高経営責任者、最高業務執行責任者、リスクエグゼクティブ（機能））。
- 組織のミッション／業務機能の実施に責任を持つ者（例：ミッション／業務遂行の責任者、情報所有者／スチュワード、運用認可権限者）
- IT 製品、サービス、または情報システムの調達に責任を持つ者（例：調達担当者、資材調達担当者、契約担当者）

[9] リスクマネジメントフレームワークについては、NIST SP 800-37 に記載されている。

[10] 執行機関とは、(i) 5 U.S.C., Section 101 により規定される執行部門; (ii) 5 U.S.C., Section 102 により規定される軍の部局; (iii) 5 U.S.C., Section 104(1) により定義される独立機関; ならびに (iv) 31 U.S.C., Chapter 91 の規定を全面的に満たしている完全に政府が所有する企業である。本文書において「執行機関(executive agency)」という用語は、「連邦政府機関(federal agency)」という用語と同義である。

- 情報システム／セキュリティの設計、開発、および導入に責任を持つ者（例：導入計画管理者、エンタープライズアーキテクト、情報セキュリティアーキテクト、情報システム／セキュリティエンジニア、情報システムインテグレータ）
- 情報セキュリティのモニタリング、管理、および運用に責任を持つ者（例：最高情報責任者、上級情報セキュリティ責任者 [11]情報セキュリティの管理者、情報システム所有者、共通管理策の提供者）
- 情報セキュリティ／リスクのアセスメントおよびモニタリングに責任を持つ者（例：システム評価者、侵入テストを実施する者、セキュリティ管理策アセサー、リスクアセサー、第三者である検証者／有効性確認者、監査官、監査人）

1.3 関連する発行文書

本文書に記載されているリスクアセスメントアプローチは、情報セキュリティリスクを管理するのに必要な一連のセキュリティ標準およびガイドラインによって支援される。本文書に加えて、連邦政府向けの統一された情報セキュリティフレームワークを支援する省庁間作業グループによって作成された Special Publications には、以下が含まれる：

- Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;[12]
- Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;
- Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; ならびに
- Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*.

本文書に含まれるリスクアセスメントプロセスおよびアプローチに関連する概念と原則は、国際標準化機構(ISO)と国際電気標準会議(IEC)の標準に記載されているプロセスおよびアプローチに類似し、それらのプロセスおよびアプローチとの一貫性を保つことを意図している。連邦政府およびその受託業者向けのこれらの国際標準の概念と原則を拡張し、リスクアセスメント結果の再利用を促進することは、ISO/IEC 標準および NIST 標準に準拠することが義務付けられている組織の負担を軽減する。

1.4 本文書の構成

本文書は以降、次のように構成されている。

- **第 2 章**では、以下について説明する：(i) リスクマネジメントプロセス、およびそのプロセスにおいてリスクアセスメントがいかに重要であるか; (ii) リスクアセスメントを実施する際に使用される基本用語; ならびに (iii) リスクアセスメントを組織のリスクマネジメントのすべての

[11] 政府機関レベルでは、この役職は、政府機関の上級情報セキュリティ責任者(Senior Agency Information Security Officer)として知られている。組織によっては、この役職を最高情報セキュリティ責任者(Chief Information Security Officer)と呼ぶこともある。

[12] SP800-39 は、情報セキュリティリスクの管理に関する手引きの一次資料として、SP800-30 に取って代わるものである。

層（すなわち、組織レベル、ミッション／業務プロセスレベル、情報システムレベル）にわたってどのように適用できるか。

- **第 3 章** では、以下を含む、情報セキュリティリスクをアセスメントするプロセスについて説明する：(i) リスクアセスメントプロセスの簡単な概要; (ii) リスクアセスメントの準備に必要な活動; (iii) リスクアセスメントの実施に必要な活動; (iv) 組織全体にわたってリスクアセスメント結果を伝達し、リスク関連情報を共有するために必要な活動; ならびに (v) リスクアセスメント結果の保守に必要な活動。
- **（補足）付録** では、以下を含む、リスクアセスメントに関する追加の情報を提供する： (i) 一般的な参考文献; (ii) 用語集; (iii) 略語; (iv) 脅威源; (v) 脅威事象; (vi) 脆弱性および素因的条件; (vii) 脅威事象が発生する可能性; (viii) 組織的影響; (ix) リスクの判断; (x) 情報リスクへの対応; (xi) リスクアセスメント報告に含めるべき必須情報; ならびに (xii) リスクアセスメントの各タスクの概要。

第 2 章

基本項目

リスクアセスメントに関連する基本的な概念

本章では以下を含む、組織内の情報セキュリティリスクのアセスメントに関連する基本的な概念について説明する：(i) リスクマネジメントプロセスの簡単な概要と、そのプロセスにおいてリスクアセスメントが果たす役割; (ii) リスクアセスメントを実施する際に用いられる基本概念; ならびに (iii) リスクアセスメントを組織のリスクマネジメントのすべての層にわたってどのように適用できるか。[13]

2.1 リスクマネジメントプロセス

リスクアセスメントは、NIST SP 800-39『Managing Information Security Risk: Organization, Mission, and Information System View』に定義されているように、組織全体にわたる総体的なリスクマネジメントプロセスの主要なコンポーネントである。リスクマネジメントプロセスは、以下を含む：(i) リスクのフレーム化; (ii) リスクのアセスメント; (iii) リスクへの対応; ならびに (iv) リスクのモニタリング。図 1 に、リスクマネジメントプロセス内の 4 つのステップを示す。この図は、「リスクアセスメント」ステップと、リスクマネジメントプロセスを効果的に機能させるために必要な情報とコミュニケーションの流れも含んでいる。[14]

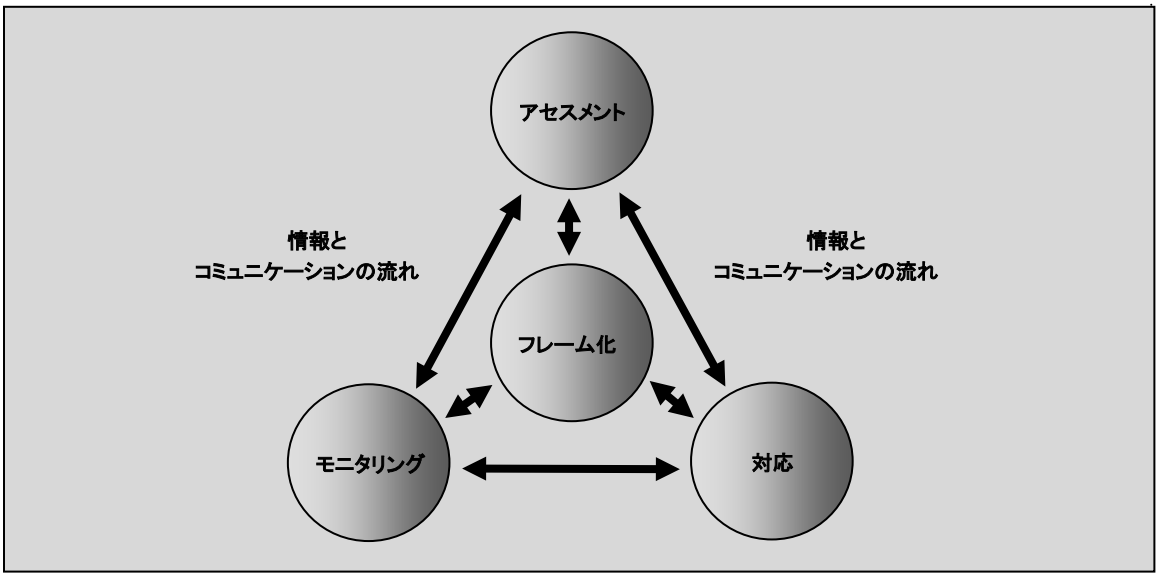


図 1：リスクマネジメントプロセス内のリスクアセスメント

[13] NIST SP 800-39 は、リスクマネジメント階層内の 3 つの層、すなわち、第 1 層（組織）、第 2 層（ミッション／業務プロセス）、および第 3 層（情報システム）に関する手引きである。

[14] 「リスクのフレーム化」ステップのアウトプットの多くは、「リスクアセスメント」ステップと、関連するリスクアセスメントプロセスに対して、重要な入力データを提供する。これらのデータは、たとえば、リスクマネジメント戦略、組織のリスク許容度、リスクアセスメント方法論、想定、制限、およびミッション／業務上の優先順位を含む。

リスクマネジメントの１番目の要素は、組織がどのようにしてリスクをフレーム化するか、あるいは、どのようにしてリスクコンテクストを確立するか（すなわち、リスクにもとづく意思決定が行われる環境を表現すること）を取り扱う。「リスクのフレーム化」要素の目的は、組織がどのようにリスクをアセスメントし、リスクに対応し、リスクをモニタリングしようとしているかを取り扱うリスクマネジメント戦略を立てて、組織が投資と運用に関する意思決定を行う際に通常使用するリスク認識を明確に、かつ透明にすることにある。リスクマネジメント戦略は、リスクを管理するための基盤を構築し、組織内のリスクにもとづく意思決定を下す範囲を明確にする。[15]

リスクマネジメントの２番目の要素は、組織がどのようにして、組織のリスクフレームにおいてリスクをアセスメントするかを取り扱う。「リスクのアセスメント」要素の目的は、以下を特定することにある：(i) 組織（すなわち、業務、資産、または個人）に対する脅威、または、ある組織を介して他の組織または国家に向けられた脅威; (ii) 組織の内部と外部に存在する脆弱性 [16]; (iii) 脅威が脆弱性を利用する可能性がある場合に発生する可能性のある被害（すなわち、負の影響）; ならびに (iv) 被害が発生する可能性。最終結果は、リスクの判断結果（すなわち、通常、被害の度合と、被害が発生する可能性をもとに算出される）である。

リスクマネジメントの 3 番目の要素は、組織がどのようにして、リスクアセスメントの結果にもとづいて決定されたリスクに対応するかを取り扱う。「リスクへの対応」要素の目的は、以下を実施することによって、組織のリスクフレームに準拠した、一貫性のある組織全体にわたるリスク対応を示すことにある：(i) リスクに対応するための代替えの行動方針を策定する; (ii) その代替えの行動方針を評価する; (iii) 組織のリスク許容度に見合った適切な行動方針を決定する; ならびに (iv) 選択された行動方針にもとづいてリスク対応を実施する。

リスクマネジメントの 4 番目の要素は、組織がどのようにして、リスクを長期にわたってモニタリングするかを取り扱う。「リスクのモニタリング」要素の目的は、以下のとおりである：(i) （組織のリスクフレームとの一貫性を保った）リスク対応の現在の有効性を判断する; (ii) 組織の情報システム、およびそれらのシステムが稼働する環境に対する変更の内、リスクに影響を及ぼす変更を特定する;[17] ならびに (iii) 計画されたリスク対応が実施されていて、かつ、組織のミッション／業務機能、連邦法、指令、規制、ポリシー、および標準／ガイドラインから導出され跡をたどることができる情報セキュリティ要求事項が満たされているか否かを確認する。

2.2 リスクアセスメント

本文書は、リスクマネジメントにおける「リスクのアセスメント」要素に焦点を当てていて、組織に対して以下に関する段階的なプロセスを示すものである：(i) どのようにリスクアセスメントに備えるか; (ii) どのようにしてリスクアセスメントを実施するか; (iii) どのようにしてリスクアセ

[15] 明確な、あるいはフォーマルなリスクマネジメント戦略が用意されていない場合、組織の資源（例：ツール、データリポジトリ）および参考文献（例：模範となるリスクアセスメント報告）を使用して、組織のリスクマネジメントアプローチの内、リスクアセスメントに影響を及ぼす側面を識別することができる。

[16] 組織の脆弱性は情報システムに限られるわけではなく、たとえば、ガバナンス構造、ミッション／業務プロセス、エンタープライズアーキテクチャ、情報セキュリティアーキテクチャ、施設、設備、システム開発ライフサイクルプロセス、サプライチェーン活動、外部サービスプロバイダの脆弱性を含む場合がある。

[17] システムが稼働する環境は、以下を含むが、これらに限定されない：脅威スペース; 脆弱性; ミッション／業務機能; ミッション／業務プロセス; エンタープライズアーキテクチャおよび情報セキュリティアーキテクチャ; 情報技術; 職員; 施設; サプライチェーンの結びつき; 組織のガバナンス／文化; 資材調達／調達プロセス; 組織のポリシー／手順; 組織の想定、制限、リスク許容度、および優先順位／トレードオフ。

スメント結果を組織の主要な職員に伝達するか; ならびに (iv) どのようにしてリスクアセスメントを長期にわたって保守するか。リスクアセスメントは、意思決定者に対して情報セキュリティリスクに対する対応を導き情報を提供するために必要な永久的、かつ決定的な情報を提供するための、単なる一時的な活動ではない。むしろ、組織は、システム開発ライフサイクル全体を通して、かつ、リスクマネジメント階層内のすべての層にわたって、リスクアセスメントを継続的に行うことになる。その際、リスクアセスメントの頻度と、アセスメント時に割り当てられる資源は、明示的に定義されたアセスメントの目的と適用範囲に見合ったものになる。

リスクアセスメントは、情報システムと、それらのシステムによって処理、格納、伝送される情報の運用および使用により生じる、組織の業務と資産、個人、他の組織、および米国の経済的利益と国家安全保障上の利益に対してもたらされる可能性のある負の影響を取り扱う。組織は、組織の主要なミッション／業務機能、ミッション／業務プロセス、ミッション／業務セグメント、共通インフラ／支援サービス、または情報システムによくあるリスクを決定するために、リスクアセスメントを実施する。リスクアセスメントは、リスクマネジメント階層内の 3 つのすべての層において組織の担当者によって実施される、多種多様なリスクにもとづく意思決定と活動を支援する。これらの意思決定と活動は、以下を含むが、これらに限定されない:

- 情報セキュリティアーキテクチャの開発
- 情報システム（ミッション／業務プロセスおよび共通インフラ／支援サービスを支援するシステムを含む）の相互接続に関する要求事項の定義
- 情報システムおよび運用環境に対するセキュリティソリューションの設計（セキュリティ管理策、IT 製品、供給業者／サプライチェーン、および受託業者の選択を含む）
- 情報システムの運用、あるいは、それらのシステムによって継承されるセキュリティ管理策（すなわち、共通管理策）の使用に対する認可（または認可の拒否）
- ミッション／業務機能および／またはミッション／業務プロセスを永続的に、または特定期間にわたって（たとえば、新たに発見された脅威または脆弱性が対処されるまで、補完的管理策が置き換えられるまで）変更すること
- セキュリティソリューションの実施（例：特定の IT 製品、またはそれらの製品の設定が、定められた要求事項を満たすか否か）
- セキュリティ ソリューションの運用と保守（例：継続的なモニタリング戦略および計画、継続的な認可）

ミッションおよび業務上の機能、それらを支援するミッション／業務プロセス、情報システム、脅威、および運用環境は時間とともに変化する傾向にあるため、あらゆるリスクアセスメントの有効性と実用性は時間的に限りがある。

2.3 主なリスク概念

リスクとは、発生しうる状況または事象によってエンティティが脅かされる度合であり、以下をもとに算出される：(i) その状況または事象が発生した場合にもたらされる負の影響; ならびに (ii) 発生する可能性。情報セキュリティリスクは、情報または情報システムの機密性、完全性、または可用性の喪失により生じるリスクであり、組織の業務（すなわち、ミッション、機能、イメージ、または評判）、組織の資産、個人、他の組織、および国家に対してもたらされる可能性のある負の影響を反映する。リスクアセスメントは、情報セキュリティリスクを特定し、評価し、優先

順位を付けるプロセスである。リスクアセスメントでは、脅威と脆弱性に関する情報を慎重に分析し、状況または事象が組織にもたらす負の影響の度合と、そうした状況または事象が発生する可能性について判断する必要がある。

リスクアセスメント方法論は、通常、以下を含む：(i) リスクアセスメントプロセス（第 3 章に記載されているように）; (ii) 重要な用語およびアセスメントが可能なリスク因子、ならびにそれらの因子間の関連性を定義する、明示的なリスクモデル; (iii) リスクアセスメント時にそれらのリスク因子が取りうる範囲値と、それらの因子の値を機能的に組み合わせてリスクを評価できるよう、それらの因子の組み合わせがどのように特定／分析されるかを規定する、アセスメントアプローチ（例：定量的、定性的、または半定量的）; ならびに (iv) 一貫した詳細レベルで問題空間を適切にとらえて対処するために、リスク因子の組み合わせがどのように特定／分析されるかについて説明する、分析アプローチ（例：脅威を重視した、資産／影響を重視した、または脆弱性を重視した）。リスクマネジメントプロセス内の「リスクのフレーム化」ステップにおいて策定されるリスクマネジメント戦略の要素のうちの1つである、リスクアセスメント方法論は、組織によって定められる。[18] 図 2 に、組織のリスクフレーム内の基本要素と、それらの要素間の関連性を示す。

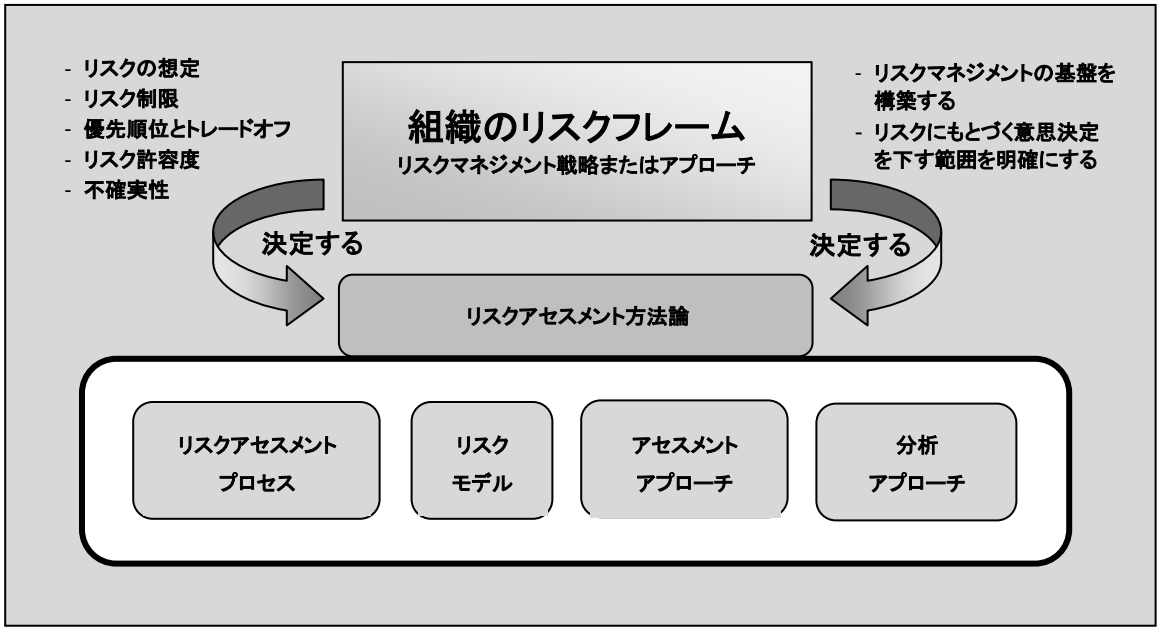


図 2：リスクのフレーム化の要素間の関連性

組織は、単一のリスクアセスメント方法論を使用するか、あるいは複数のアセスメント方法論を使用するかを選択できる。特定の方法論を選択する際には、たとえば、以下を考慮する：(i) 投資計画または計画政策変更の時間枠; (ii) 組織のミッション／業務プロセスの複雑さ／成熟度（エンタープライズアーキテクチャのセグメントごとの）; (iii) その情報システムがシステム開発ライフサイクル内のどのフェーズに入っているか; あるいは (iv) 組織の主要なミッション／業

[18] リスクアセスメント方法論は、その大部分が組織のリスクマネジメント戦略の影響を受ける。しかしながら、リスクアセスメント方法論は、アセスメントの目的および適用範囲と、リスクアセスメントプロセス、リスクモデル、アセスメントアプローチ、分析アプローチに関して組織が選択する具体的な入力データにもとづいて、それぞれのリスクアセスメント向けにカスタマイズすることができる。

務機能を支援する情報および情報システムの重大性／機微度 [19]。組織は、採用されたリスクモデル、アセスメントアプローチ、および分析アプローチを明確にし、アセスメントプロセスの一環として、それぞれのリスク因子になぜそうした値を割り当てたかについての根拠を求めることにより、リスクアセスメントの再現性と繰り返し性を向上させることができる。[20]

2.3.1 リスクモデル

リスクモデルは、アセスメントが必要なリスク因子と、それらの因子間の関連性を定義する。[21] リスク因子は、リスクアセスメントにおけるリスクレベルを決定する際のデータとしてリスクモデル内で使用される特性である。リスク因子は、また、特定の状況、環境、またはコンテクストにおいてリスクレベルに強い影響を及ぼすものをハイライトするための、リスク伝達に広く利用できる。典型的なリスク因子は、脅威、脆弱性、影響、発生可能性、および素因的条件を含む。 リスク因子は、より詳細な特性に分解することができる（たとえば、脅威は脅威源と脅威事象に分解できる）。[22] 組織が、リスクアセスメントを実施する前にこれらの定義を文書化することが重要である。なぜならば、リスクアセスメントは、リスクを効果的に判断するために、脅威、脆弱性、影響およびその他のリスク因子の明確に定義された属性に依存するからである。

脅威

脅威は、情報システムを介して、情報の正規の権限によらないアクセス、破壊、開示、または変更、および／またはサービス妨害によって組織の業務と資産、個人、他の組織、または国家に負の影響をもたらしうる状況または事象である。[23] 脅威事象は、脅威源によって引き起こされる。脅威源は、以下によってその特徴が定義される：(i) 脆弱性の利用を目的とした意図および方法; あるいは (ii) 誤って脆弱性を利用する可能性のある状況および方法。一般的に、脅威源のタイプは、以下を含む：(i) 敵意を持ったサイバー攻撃または物理的攻撃; (ii) 怠慢または過失による人的ミス; (iii) 組織が管理する資源（例：ハードウェア、ソフトウェア、環境制御）の構造上の欠陥; ならびに (iv) 自然災害と人災、アクシデント、組織がコントロールできない障害。脅威源については、さまざまな分類法が既に開発されている。[24] 脅威源の分類法の中には、負の影響のタイプを組織化原理として使用するものがある。複数の脅威源が同一の脅威事象

[19] NIST SP 800-60 は、セキュリティ分類に必要な、情報の重大性および機微度の概念について論じている。

[20] 再現性とは、複数の異なる専門家が同じデータを使用した場合に、同じ結果が生成されるといった特性である。繰り返し性とは、そのアセスメントを将来にわたって繰り返す場合に、過去のアセスメントとの一貫性を保ち、故に比較可能な方法で実施できるといった特性である。繰り返し性は、組織による動向の特定を可能にする。

[21] リスクモデルについての文書は、以下を含む：(i) 各リスク因子の識別情報（定義、説明、値の尺度）; ならびに (ii) それらのリスク因子間の関連性の識別情報（記述的に示された概念上の関連性と、値を組み合わせるためのアルゴリズムの両方）。本セクションに示されていて、付録 D-I に記載されているリスクモデルは、値を組み合わせるためのアルゴリズムを規定していない。

[22] リスク因子は、アセスメントが可能な単一の特性（例：影響の重大さ）を有する場合もあれば、アセスメントが可能なものと、そうでないものが混在する複数の特性を有する場合もある。アセスメントが可能でない特性は、通常、関連するより低レベルの特性を特定するのに役立つ。たとえば、脅威源は、脅威タイプによる分類法を用いた結果、「アセスメントが可能」というよりは「名だけ」であるとみなされる、（特徴的な）脅威タイプを有する。この脅威タイプは、関連する、より詳細な特性を特定するのに役立つ（たとえば、「脅威源」タイプのアドバーサリである場合、関連する特性として能力、意図、標的といった、直ちにアセスメントが可能な特性を有する）。

[23] 組織は、脅威事象を以下のように規定してもよい：(i) 単一の事象、アクション、または状況; あるいは (ii) 関連するアクション、活動、および／または状況の集合および／またはシーケンス。

[24] 付録 D では、脅威源および関連する脅威特性の分類体系の例を示している。

を開始する（または引き起こす）可能性がある。たとえば、サービス妨害攻撃、悪意のあるシステムアドミニストレータによる意図的な行為、管理上の誤り、ハードウェアの故障、または停電により、供給サーバーがオフラインになってしまうことが挙げられる。

それぞれのリスクモデルは、詳細さと複雑さの度合が異なり、それらの度合に応じて脅威事象が特定される。脅威事象がかなりの詳細さをもって特定される場合、脅威シナリオをモデル化、策定し、分析することが可能になる。[25] サイバー攻撃または物理的攻撃につながる脅威事象は、アドバーサリによって採用される戦術、技法、手順によって、その特徴を定義することができる。アドバーサリによってもたらされる脅威事象について理解することにより、組織は、特定の脅威源の能力についての洞察を得ることができる。さらに、誰が攻撃を行っているかについて十分に知ることにより、組織は、アドバーサリがその攻撃を通じて何を得ようとしているかをよりよく理解することができる。起こりうる攻撃の意図、および標的を知ることにより、組織は、考慮すべき最重要の脅威事象を絞り込むことができる。

脅威のシフトとは、アドバーサリが、感知した保護手段／対策（すなわち、セキュリティ管理策）に対して取る対抗措置であり、彼らはそれらの保護手段／対策を回避または打ち破るために、自身の意図／標的の一部の特性を変更する。脅威のシフトは、単一の領域、あるいは複数の領域において発生する。それらの領域には、以下が含まれる：(i) 時間領域（例：攻撃の遅延、または不法に侵入し、さらなる偵察行為を行う）; (ii) 標的領域（例：十分に保護されていない他の標的を選択する）; (iii) 資源領域（例：不確実性を減らすために、または保護手段／対策を打ち破るために、攻撃に資源を追加する）; もしくは (iv) 攻撃計画／攻撃手法領域（例：攻撃に使う武器または攻撃の経路を変更する）。脅威のシフトは、脅威源と、標的となる組織の資産との動的な情報のやりとりからすると、当然起こる。より複雑な脅威源の場合、特定の脆弱性を利用するために、最も楽な道を取る傾向があり、レスポンスが必ずしも予測可能でない。導入された保護手段／対策と、組織の脆弱性が成功裏に利用された場合の影響に加えて、脅威のシフトにもたらされる別の影響は、攻撃者にとって利点となる。攻撃者側のそうした利点は、どのくらいの脅威シフトがいつ発生するかにも影響を及ぼす。

脆弱性と素因的条件

脆弱性とは、脅威源によって利用される可能性がある、情報システム、システムセキュリティ手順、内部統制、または実装における弱点である。[26] 情報システムの脆弱性の多くは、（意図的であるか否かにかかわらず）適用されていないセキュリティ管理策に関連する場合もあれば、適用されているものの、なんらかの弱点を有するセキュリティ管理策に関連する場合もある。しかしながら、組織のミッション／業務機能が進化し、運用環境が変化し、新しい技術が急増し、新たな脅威が出現することから、時間の経過とともに自然に生じる新たな脆弱性について考慮することも重要である。そうした変化を鑑みると、既存のセキュリティ管理策では不十分となり、有効性の再アセスメントが必要になることが考えられる。セキュリティ管理策の有効性は、場合によっては時間の経過とともに低下する傾向にあるため、システム開発ライフサイクル全体を通してリスクアセスメントを保守することの必要性が増すと同時に、組織のセキュリティ体制に

[25] 脅威シナリオは、特定の脅威源、あるいは複数の脅威源によって引き起こされ、その一部が時系列で順序付けられる、一連の脅威事象であり、負の影響をもたらす。

[26] 脆弱性の重大さは、その脆弱性を軽減する／取り除くことの相対的重要性をアセスメントした結果である。脆弱性の重大さは、そうした脆弱性が、ある脅威源によって利用された場合にもたらされる負の影響の度合によって決まる。したがって、脆弱性の重大さは、通常、状況による。

関する現在の状況認識を把握するための、継続的なモニタリング計画の重要性も増す。

脆弱性は、情報システム内でのみ特定されるわけではない。情報システムをより広い意味でとらえると、脆弱性は組織のガバナンス構造にも存在する（例：効果的なリスクマネジメント戦略と、適切な「リスクのフレーム化」が欠如している、政府機関内のコミュニケーションが不足している、ミッション／業務機能の相対的優先順位についての意思決定が一貫していない、あるいはミッション／業務活動を支援するためのエンタープライズアーキテクチャの調整がうまくできていない）。脆弱性は、また、外部との関係に存在したり（例：特定のエネルギー源、サプライチェーン、情報技術、および通信接続業者への依存）、ミッション／業務プロセスに存在したり（例：きちんと定義されていないプロセス、またはリスクを認識していないプロセス）、エンタープライズ／情報セキュリティアーキテクチャに存在したりする（例：アーキテクチャについての意思決定が乏しいために、組織の情報システムが多様性と耐障害性に欠けること）。[27]

一般的にリスクは、単一の、あるいは複数の脆弱性を利用する個々の脅威事象が連なった結果として顕在化する。組織は、特定の脅威源によって引き起こされた事象がどのように被害をもたらす一因となるか、あるいは直接被害をもたらすかを説明する、脅威シナリオを定義する。脆弱性によっては、別の脆弱性が利用されるまで利用されることがないため、脅威シナリオの作成は分析の観点から有用である。したがって、個々の脆弱性の分析よりも、一連の脆弱性が総じて単一の、あるいは複数の脅威事象によってどのように利用されるかを明確にする分析の方が、より有用である。さらに、脅威シナリオはストーリーを語るため、リスク伝達および分析に役立つ。

上述の脆弱性に加えて、組織は、素因的条件についても考慮する。素因的条件とは、組織、ミッション／業務プロセス、エンタープライズアーキテクチャ、または情報システム（その運用環境を含む）に存在する条件の一種であり、一度開始された脅威事象が組織の業務と資産、個人、他の組織、または国家に負の影響をもたらす可能性に影響を及ぼす（すなわち、その可能性を増加／減少させる）。[28] 素因的条件は、たとえば、ハリケーンまたは洪水の起きやすい地域に施設があること（この場合、ハリケーンまたは洪水に晒される可能性が増加する）、または、外部ネットワークとの接続を行わないスタンドアロン型情報システム（この場合、ネットワークベースのサイバー攻撃に晒される可能性が減少する）を含む。容易に是正できない素因的条件により生じる脆弱性は、たとえば、緊急時対応計画における欠陥、時代遅れの技術の使用、または情報システムのバックアップおよび障害迂回メカニズムの弱点／欠陥を含む。あらゆる場合において、これらのタイプの脆弱性は、脅威事象が組織に負の影響をもたらす素因となる。脆弱性（素因的条件に寄与する脆弱性を含む）は、組織の情報システムと運用環境の総合的なセキュリティ体制の一部であり、脅威事象の発生の可能性に影響を及ぼす。

発生可能性

発生可能性は、既知の脅威が既知の脆弱性（または一連の脆弱性）を利用できる確率の分析にもとづく、重み付けされたリスク因子である。そのリスク因子は、脅威事象が開始される可

[27] NIST SP 800-39 は、リスクマネジメント階層内の 3 つのすべての層における脆弱性と、そうした脆弱性が脅威によって利用された場合にもたらされる可能性のある負の影響についての、手引を提供する。

[28] 素因的条件の概念は、susceptibility（影響を受けやすいこと）や exposure（晒されること）といった用語にも関連している。組織は、ある脅威が、ある脆弱性を利用して負の影響を引き起こすことができない場合に、リスクの影響を受けやすい（またはリスクに晒されている）状態ではないと言える。たとえば、データベース管理システムを使用しない組織は、SQL インジェクションの脅威に対して脆弱でなく、故に、そうしたリスクの影響を受けにくい。

能性の予測と、影響の発生可能性（すなわち、脅威事象が負の影響をもたらす可能性）の予測の組み合わせである。アドバーサリによる脅威の場合、発生可能性のアセスメントは、通常、以下にもとづく：(i) アドバーサリの意図; (ii) アドバーサリの能力; ならびに (iii) アドバーサリの標的。アドバーサリによるもの以外の脅威事象では、発生可能性は史実、実験によって得られるデータ、またはその他の因子を用いて予測される。脅威事象が開始される（または発生する）可能性は、特定の時間枠（たとえば、これからの半年間、これからの1年間、または特定の節目に達するまでの期間）に対してアセスメントされることに留意すること。脅威事象が（指定された、または暗黙の）時間枠内で開始される（または発生する）のがほぼ確実である場合、リスクアセスメントは、その事象の推定頻度を考慮するだろう。脅威が発生する可能性は、また、組織の状態（たとえば、組織の主要なミッション／業務プロセス、エンタープライズアーキテクチャ、情報セキュリティアーキテクチャ、情報システム、およびそれらのシステムが稼働する環境を含む）にもとづく場合がある。その場合、素因的条件を考慮すると同時に、権限のない／好ましくない行動に対する保護、被害の発見と最小化、および／またはミッション／業務機能の維持または回復のためのセキュリティ管理策の有無と、導入されている場合の管理策の有効性についても考慮する。影響の発生可能性は、予期される被害の大きさにかかわらず、脅威事象が負の影響をもたらす確率（可能性）を取り扱う。

組織は、通常、脅威事象の総合的な可能性を判断するために、三段階のプロセスを使用する。第一に、組織は、脅威事象が開始される可能性（アドバーサリによる脅威事象の場合）、または発生する可能性（アドバーサリによるもの以外の脅威事象の場合）をアセスメントする。第二に、組織は、一度開始された（または発生している）脅威事象が、組織の業務と資産、個人、他の組織、または国家に負の影響をもたらす、または被害をもたらす可能性をアセスメントする。最後に、組織は、開始／発生の可能性と、負の影響がもたらされる可能性の組み合わせである、総合的な可能性をアセスメントする。

脅威と脆弱性を組み合わせること（すなわち、脅威と脆弱性の 1 対 1 の関係を確立すること）は、ミッション／業務機能レベルで発生可能性をアセスメントする場合には好ましくなく、多くの場合、情報システムレベルでのアセスメントであっても、脅威と脆弱性の数が多いと問題になる。このアプローチは、通常、組織が脅威関連情報を効果的に使用したり、有意な詳細レベルで脅威を特定することを可能にする代わりに、脅威事象と脆弱性の特定の詳細レベルを決定するのに役立つ。脅威の特定の詳細レベルによっては、既知の脅威事象が複数の脆弱性を利用することが分かる場合がある。発生可能性をアセスメントするうえで、組織は、脅威事象が利用する可能性のある脆弱性について検証し、（たとえば、機能面での依存関係、特に外部との依存関係に起因して）セキュリティ管理策が存在しない、またはセキュリティ管理策の導入が不可能な事象に対するミッション／業務機能の脆弱さについても検証する。特定の状況において、情報セキュリティリスクに起因するミッション／業務リスクを減らす最も効果的な方法は、情報システムが侵害された場合に実行可能な次善策を用意できるよう、ミッション／業務プロセスを設計し直すことである。前述の脅威シナリオの概念を用いることは、脅威と脆弱性の組み合わせの欠点の一部を組織が克服することを支援する。

影響

脅威事象がもたらす影響のレベルは、正規の権限によらない情報の開示、正規の権限によらない情報の変更、正規の権限によらない情報の破壊、あるいは情報や情報システムの可用性の喪失によってもたらされることが予期される、被害の大きさである。そうした被害を経験する可能性があるのは、組織内と組織外のさまざまな利害関係者（たとえば、政府機関の長、ミッ

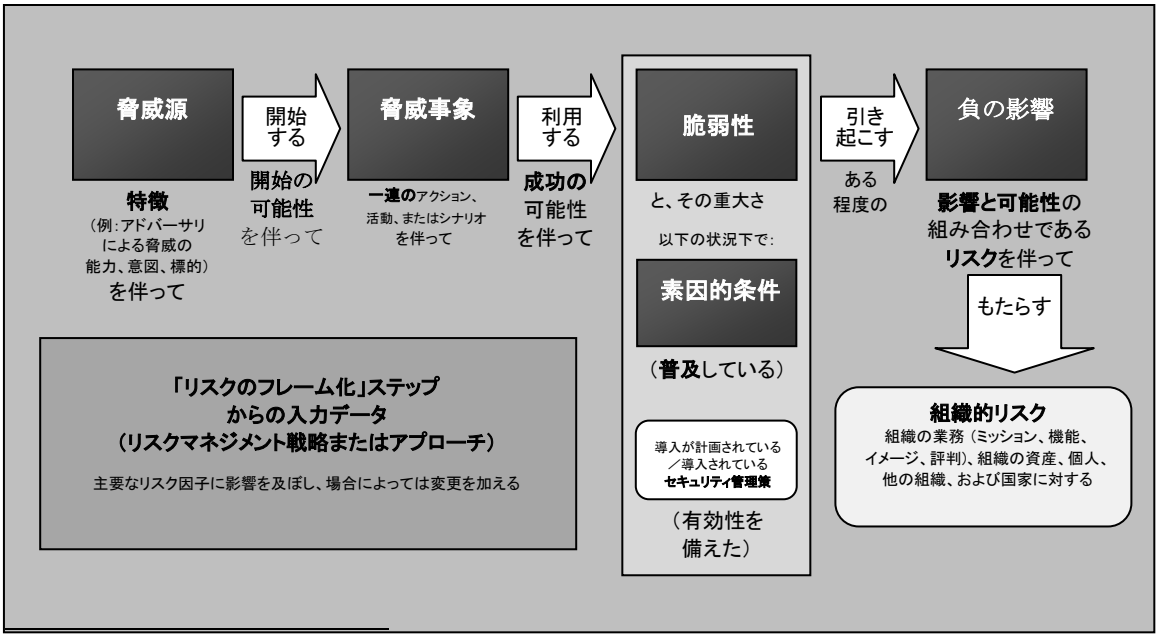
ション／業務遂行の責任者、情報所有者／スチュワード、ミッション／業務プロセス遂行の責任者、情報システム所有者、あるいは、その組織に依存する公共部門と民間部門の個人／団体を含む）、要するにその組織の業務、資産、または個人、その組織と協力関係にある他の組織、または国家に対する既得権利を有するすべての者である。[29] 組織は、以下を明確にする: (i) 影響の判断に用いられるプロセス; (ii) 影響の判断に関連する前提; (iii) 影響に関する情報を得るための情報源および方法; ならびに (iv) 影響の判断に関して達した結論に対する根拠。

組織は、組織が定めた優先順位と価値が、どのようにして価値の高い資産と、組織の利害関係者にもたらされる可能性のある負の影響の特定に寄与するかについて明確に定義する。そうした情報が定義されていない場合、脅威源の標的と関連する組織的影響の特定に関連する優先順位と価値は、通常、戦略的計画およびポリシーから導出することができる。たとえば、セキュリティ分類レベルは、異なるタイプの情報が侵害された場合の組織的影響を示す。プライバシー影響評価と重大性レベル（緊急時対応計画またはミッションへの影響分析／ビジネス影響分析の一部として定義された場合）は、情報資源の破壊、破損、または説明責任が失われることによって組織にもたらされる負の影響を示す。

戦略的計画およびポリシーは、直近の、または近い将来のミッション／業務機能の達成、および長期にわたる組織の実行可能性（これは、機微な情報が侵害されることにより生じる評判の失墜、または制裁措置によって損なわれる可能性がある）の相対的優先順位を明確に、あるいは暗に示す。組織は、最終的な影響判断を行う際には、影響を受ける一連の資源の相対的サイズを含む、脅威事象がもたらす影響の範囲についても考慮する。リスクを許容する前提として、影響が特定の値（レベル）を下回る脅威事象については、さらなる分析は行わないことが明示される場合がある。

リスク

図 3 は、上記の主要リスク因子とそれらの因子間の関連性を含む、リスクモデルの例を示している。各リスク因子は、第 3 章で説明するリスクアセスメントプロセスにおいて使用される。



[29] 「組織の資産」という用語は、たとえば、高位影響のプログラム、施設、基幹業務に関わる情報システム、職員、設備、論理的に関連したシステムの集合を含め、その適用範囲が非常に広くなる場合がある。より広い意味では、組織の資産は、イメージまたは評判などの無形資産を含む、その組織が大事にしている特定の資源または資源群を示す。

図 3: 主要なリスク因子を含む、一般的なリスクモデル

上で述べたように、リスクは、ある脅威事象が発生する可能性と、万が一その事象が発生した場合にもたらされる負の影響をもとに算出される。この定義は、SP800-39 に記載されているリスクマネジメント階層内のすべての層における多くのタイプの負の影響（例：第 1 層においては、組織のイメージまたは評判に対するダメージ、もしくは金銭上の損失、第 2 層においては、特定のミッション／業務プロセスを成功裏に実施することができないこと、第 3 層においては、情報システムインシデントに対処するための資源の消費）に対応する。また、影響間の関連性（例：データの機密性の喪失により、現行の、または将来にわたるミッション／業務の有効性が失われること、データまたはシステムの完全性の喪失により、機微度の高い情報の信頼性が失われること、情報または情報システムが利用できなくなったり、機能が低下すること）にも対応する。この広い定義は、リスクを単一の値、あるいはベクトル（すなわち、複数の値）として表すことを可能にする。ベクトルの場合、異なるタイプの影響は、個別にアセスメントされる。リスク伝達の目的上、リスクは通常、負の影響のタイプ（場合によっては、それらの影響を受ける時間枠）にもとづいて分類される。

集約

組織は、複数の独立したリスクをより一般的なリスクに集約するために、または、低レベルのリスクを高レベルのリスクに集約するために、リスク集約を使用することができる。組織は、また、指定された関連性と依存関係を有する複数の情報システム、および複数のミッション／業務プロセスのリスクアセスメントの適用範囲とスケールを効果的に管理するために、リスク集約を使用することができる。主に第 1 層と第 2 層において実施され、時折第 3 層において実施されるリスク集約は、独立したリスクの集合が組織の業務、資産、および個人にもたらす総合的なリスクをアセスメントする。一般的に、独立したリスク（例：明確に定義されたミッション／業務プロセスを支援する単一の情報システムに関連するリスク）の場合、最悪のケースの影響が、組織の業務、資産、および個人にもたらす総合的なリスクの上限となる。[30] リスク集約の問題の一つに、リスクに対するこの上限が適用できない可能性があることが挙げられる。たとえば、複数のリスクが同時に顕在化する、あるいは、同一のリスクがある期間にわたって繰り返し顕在化する場合には、組織レベルでリスクをアセスメントするのが、組織にとって有益であろう。そうした状況では、発生する総合的なリスクは、組織のリスク対応能力を超える可能性があり、したがって組織の業務と資産に対する総合的な影響（すなわち、ミッション／業務への影響）が、それぞれのリスクに対する初期のアセスメント結果を上回ることになるだろう。

リスクを集約する際には、組織はさまざまなリスク間の関連性について考慮する。たとえば、1 つのリスクが顕在化した場合、別のリスクが顕在化する可能性が高まる、あるいは低くなるといった、因果関係が存在することが考えられる。異なるリスク間に直接の因果関係、または反比例関係がある場合には、それらのリスクを肯定的に、あるいは否定的に、（定性的に）結合したり、（定量的に）相互に関連付けることができる。リスクの結合または相互の関連付け（すなわち、特定のリスクが顕在化する可能性を高める、または低くするリスク間の関連性を特定すること）は、第 1 層、第 2 層、または第 3 層において行われる。

[30] FIPS 199 に従って実施されたセキュリティ分類は、（最高水位線の概念を用いた）最悪のケースの影響分析の例となる。このタイプの影響分析は、組織内の個々の状況に適用された場合に、リスクの上限を示してくれる。

不確実性

不確実性は、以下のような事由により、リスクの評価にはつきものである：(i) 未来が過去に類似する度合は限られていること; (ii) 脅威についての知識が不十分または不完全である（例：アドバーサリの特徴（戦術、技法、手順を含む）について）; (iii) 技術または製品に、まだ発見されていない脆弱性があること; ならびに (iv) 認識されていない依存関係が、予期しない影響をもたらしうること。特定のリスク因子の値につての不確実性は、リスクアセスメントが実施されるリスクマネジメントフレームワーク内のステップ、またはシステム開発ライフサイクル内のフェーズに起因する場合がある。たとえば、システム開発ライフサイクルの初期のフェーズでは、セキュリティ管理策の有無と、導入されている場合の管理策の有効性が未知である可能性があり、ライフサイクルの後のフェーズでは、より十分な情報を得たうえでの意思決定ができなくなるために、管理策の有効性の評価にかかるコストが、メリットを上回る可能性がある。最後に、不確実性は、その他の情報システム、ミッション／業務プロセス、サービス、共通インフラ、および／または組織に関連するリスクについての知識が不完全であることに起因する場合がある。これらのさまざまな理由による、リスクアセスメント結果の不確実性の度合は、結果という形で伝達することができる（例：結果を質的に表現する、特定されたリスクを単一の値で示す代わりに範囲値で示す、あるいは不明瞭な領域をポイントではなく視覚表示を用いることによって）。

2.3.2 アセスメントアプローチ

リスク、およびその要因は、定量的、定性的、半定量的を含む、さまざまな方法でアセスメントできる。組織によって検討される各リスクアセスメントアプローチは、長所と短所を持つ。望ましいアプローチ（または状況に特化した一連のアプローチ）は、組織文化と、とりわけ、不確実性とリスク伝達の概念に対する姿勢にもとづいて選択される。定量的なアセスメントは、通常、そのアセスメントの環境の内外において数値の意味と比例が保たれる場合に、それらの数値の利用にもとづいてリスクをアセスメントするための一連の方法、原則、またはルールを使用する。このタイプのアセスメントは、代替えのリスク対応または行動方針の費用対効果分析を最も効果的に支援する。しかしながら、定量的な結果の意味は、常に明らかであるわけではなく、そうした場合には解説と説明、とりわけ、その結果を使用するにあたっての想定と制限についての説明が必要となる。たとえば、組織は、通常、リスクアセスメントによって得られた数値または結果が信頼できるものか、また、得られた数値の差異が有意であるか否かについて答えを求めるだろう。さらに、主観的な判断が定量的なアセスメント内に埋もれてしまう場合や、かなりの不確実性を伴って数値が決定された場合には、定量化の厳密さが著しく低下する。場合によっては、定量的なアセスメントのメリット（アセスメント結果の厳密さ、繰り返し性および再現性の観点から）よりも、コスト（専門家が費やす時間と労力、そうしたアセスメントの実施に必要なツールの実装と使用）が上回ることがある。

定量的なアセスメントとは対照的に、定性的なアセスメントは、通常、非数値的な分類またはレベル（例：非常に低い、低い、中間、高い、非常に高い）にもとづいてリスクをアセスメントするための一連の方法、原則、またはルールを使用する。このタイプのアセスメントは、リスクに関する結果を意思決定者に伝達することを支援する。しかしながら、定性的なアセスメントにおける範囲値は、ほとんどの場合に比較的小さく、その場合、報告されたリスク間の相対的優先順位付けおよび比較が困難になる。さらに、それぞれの値がかなり明確に定義されているか、あるいは有意な例によってその特徴が定義されていない限り、異なる専門家が自身の体験を頼りにアセスメントを実施した結果、それぞれの結果が著しく異なる可能性がある。定性的なアセスメントの繰り返し性と再現性は、アセスメントされた値に注釈をつけたり（例：この値が高いの

は以下の理由による)、定性的な値を結合するための表やその他明確に定義された機能を使用することによって向上する。

最後に、半定量的アセスメントは、通常、その数値と意味が別の環境では維持されない瓶、スケール、または代表的な数値を使用してリスクをアセスメントするための一連の方法、原則、またはルールを使用する。このタイプのアセスメントは、定量的アセスメントと定性的アセスメントのメリットを提供する。瓶(例:0-15, 16-35, 36-70, 71-85, 86-100)またはスケール(例:1-10)は、意思決定者へのリスク伝達を支援する定性的な言い方に容易に変換することができる(例:スコアが 95 なら「非常に高い」と解釈される)。また、異なる瓶間の、あるいは同一の瓶内の数値の相対的な比較を可能にする(例:スコアがそれぞれ 70 と 71 と判定されたリスク間の差異は比較的有意でないが、スコアがそれぞれ 36 と 70 と判定されたリスク間の差異は比較的有意である)。値の割り当てにおける専門家による判断の役割は、純粋な定量的なアプローチに比べて、より明らかである。さらに、スケールまたは一連の瓶が十分な詳細さを提供する場合、結果間の総体的優先順位付けが、純粋な定性的なアプローチよりも、よりよく支援される。定量的なアプローチと同様に、主観的な判断がアセスメント内に埋もれてしまう場合や、かなりの不確実性を伴って数値が決定された場合には、厳密さが著しく低下する。十分な根拠に基づいた定性的なアプローチにおいて使用される非数値的な分類またはレベルと同様に、それぞれの瓶または範囲値は明確に定義され、有意な例によってその特徴が定義される必要がある。

選択された価値尺度のタイプにかかわらず、アセスメントは、リスク因子の時間要素を明確にする。たとえば、組織は、発生の可能性のアセスメントと影響の重大さのアセスメントに、特定の期間を関連づけることができる。

2.3.3 分析アプローチ

分析アプローチは、リスクアセスメントの方向性または開始点、アセスメントの詳細レベル、類似の脅威シナリオに起因するリスクがどのように取り扱われるかに関して、それぞれに異なる。分析アプローチは、以下のいずれかに分類される:(i) 脅威を重視した; (ii) 資産/影響を重視した; あるいは (iii) 脆弱性を重視した。[31] 脅威を重視したアプローチは、脅威源と脅威事象の特定から始まり、その後、脅威シナリオの作成に重点的に取り組む。続いて、脅威との関連で脆弱性が特定され、アドバーサリによる脅威の場合には、アドバーサリの意図に応じて影響が特定される。資産/影響を重視したアプローチは、懸念される影響または結果、および極めて重要な資産の特定から始まる。その際、場合によっては、ミッションへの影響分析またはビジネス影響分析 [32]の結果を使用したり、それらの影響または結果を招く脅威事象、および/またはそれらの影響または結果を追及する脅威源を特定する。脆弱性を重視したアプローチは、組織の情報システム、または、それらのシステムが稼働する環境における一連の素因的条件または利用できる弱点/欠陥から始まり、その後、それらの脆弱性を利用する可能性のある脅威事象と、脆弱性が利用された場合にもたらされうる結果を特定する。それぞれの分析アプ

[31] 組織は、特定の分析アプローチを選択するうえで、高い柔軟性を有する。組織が取る特定のアプローチは、組織ごとに異なる考慮事項(例:脅威、脆弱性、および影響/資産に関して得られる情報の質と量、組織の最優先事項を扱う特定の方向性、特定の方向性に重点を置いている分析ツールの可用性、あるいは前記の組み合わせ)によって導出される。

[32] ビジネス影響分析(BIA)は、価値の高い資産と、完全性または可用性の喪失による負の影響を特定する。DHS Federal Continuity Directive 2 は、リスクマネジメント階層内の「組織レベル」層と「ミッション/業務プロセスレベル」層における BIA に関する手引きである。NIST SP 800-34 は、リスクマネジメント階層内の「情報システムレベル」層における BIA に関する手引きである。

ローチは、同じリスク因子を考慮に入れるため、順番はことなるものの、同一のリスクアセスメント活動を伴う。リスクアセスメントの開始点が異なることにより、結果が偏り、一部のリスクが特待されない可能性がある。したがって、二番目の方向性からリスクを判断することが、分析の厳密さと有効性を向上させる場合がある（例：脅威を重視した分析アプローチを、資産／影響を重視した分析アプローチで補う）。

分析アプローチの方向性に加えて、組織は、以下の項目間の多対多関係を明確にするための効果的な方法を提供する、より厳密な分析技術（例：グラフにもとづく分析）を適用することができる：(i) 脅威源と脅威事象（すなわち、単一の脅威事象が複数の脅威源によって引き起こされたり、単一の脅威源が複数の脅威事象を引き起こす可能性がある）; (ii) 脅威事象と脆弱性（すなわち、単一の脅威事象が複数の脆弱性を利用したり、単一の脆弱性が複数の脅威事象によって利用される可能性がある）; ならびに (iii) 脅威事象と影響／資産（すなわち、単一の脅威事象が複数の資産に影響を及ぼす、あるいは複数の影響をもたらす可能性や、単一の資産が複数の脅威事象による影響を受ける可能性がある）。[33] 厳密な分析アプローチは、また、リスクアセスメントの対象となる時間枠内で、特定の負の影響が発生する可能性（または特定の資産が危害を受ける可能性）があるか否かについて説明するための手段を提供する。発生回数は、多くても 1 回、あるいは影響の性質と、組織（ミッション／業務プロセスまたは情報システムを含む）がそうした負の影響からどのように回復するかによっては、複数回になる。

2.3.4 組織文化がリスクアセスメントにもたらす影響

各組織が好むリスクモデル、アセスメントアプローチ、および分析アプローチは、さまざまな理由により異なる。たとえば、文化の問題 [34]が組織を、他の組織のモデルに存在するリスク因子が含まれないよう単一の、あるいは複数のリスク因子に対して一定の値を仮定するリスクモデルを使用したい気持ちにさせる場合がある。文化は、また、組織を、定量的なアセスメントを使用した詳細な分析を求めるリスクモデルリスクモデル（例：原子力の安全性）を使用したい気持ちにさせる場合がある。別の選択肢として、組織は、定性的な、または半定量的なアセスメントアプローチを好むかもしれない。組織間の差異に加えて、組織内にも差異が存在する場合がある。たとえば、組織は、システム開発ライフサイクルの初期にはきめの粗い、または高レベルのリスクモデルを使用してセキュリティ管理策を選択し、後により詳細なモデルを使用して組織に与えられたミッション／業務機能に対するリスクをアセスメントすることができる。組織のリスクフレーム [35] は、さまざまな状況において、どのリスクモデル、アセスメントアプローチおよび分析アプローチを使用すべきかを決定する。

[33] たとえば、グラフにもとづく分析技術（例：機能面で依存関係にあるネットワークの分析、アドバーサリによる脅威に対する「攻撃の木」分析、その他のタイプの脅威に対する「故障の木」分析）は、特定の脅威事象を使用して脅威シナリオを生成するための手段を提供する。グラフにもとづく分析技術は、また、1つの事象が別の事象の発生の可能性を変えるといった状況について説明するための手段を提供する。「攻撃の木」分析および「故障の木」分析では、とりわけ、リスクのレベルを判断する目的で、ほぼ同様の脅威シナリオを複数生成することが可能である。自動化されたモデリングやシミュレーションでは、多数の脅威シナリオ（例：「攻撃の木」／「故障の木」、機能面で依存関係にあるネットワークのトラバース）が生成される可能性がある。したがって、グラフにもとづく分析技術は、あらゆる脅威シナリオから適切なサブセットを定義するための、分析を限定する手段を含む。

[34] NIST SP 800-39 は、組織文化がリスクマネジメントにどのように影響を及ぼすかについて説明している。

[35] NIST SP 800-39 は、組織のリスクフレームを、組織のリスクマネジメント戦略（すなわち、リスクを管理するための強固な基盤を確立し、リスクにもとづく意思決定を下す範囲を明確にすること）を支える想定、制限、リスク許容度、優先順位およびトレードオフの一式であると定義している。

リスクモデルの使用

単一のリスクモデル（定められた一連の因子、各因子のアセスメントスケール、因子を結合するためのアルゴリズムによって構成される）は、SP800-30 に依存する公共部門と民間部門の組織の多様なニーズには対応できない。たとえば、アドバーサリによる脅威に重点を置いて、そうした脅威についての詳細な情報を提供する組織もあれば、アドバーサリによるもの以外の脅威に重点を置くことを選択し、それらのタイプの脅威についてはより詳細な情報を提供するが、アドバーサリによる脅威についてはそれほど詳細な情報は提供しない組織もある。したがって、脅威に関する想定が異なるそれぞれの組織によって策定されるリスクモデルは、因子と詳細レベルもそれぞれに異なるだろう。

同様に、単一の組織または利益共同体内でも、ミッション／業務機能が異なる場合や、情報システムの分類が異なる場合、および／またはシステムがシステム開発ライフサイクル内のどの段階にあるかによっては、異なるアセスメントスケールが適切であるだろう。たとえば、ある情報システムについて初めて考える時に実施される初期のリスクアセスメントでは、脅威と脆弱性に関して得られる情報が具体的でなく、極めて不確かである可能性がある。そうしたリスクアセスメントの場合、いくつかの因子のみを使用した定性的なアセスメントが適切であろう。一方、セキュリティ管理策のアセスメントからの情報にもとづいたリスクアセスメントは、はるかに具体的であり、より厳密な評価がなされる可能性がある。そうしたアセスメントの場合、0 から 100 の価値尺度を使用した半定量的なアセスメントの方が、より適切であろう。

SP800-39 と 800-30 に記述されている予測では、それぞれの組織またはコミュニティが、自身のリスクに対する見解に適したリスクモデルを定義するであろうとしている（すなわち、どのリスク因子を考慮すべきか、どの因子を組み合わせることができるか、どの因子をさらに分解すべきか、アセスメントされた値をどのようにしてアルゴリズムを使用して結合するかについての、組織またはコミュニティの見解を反映するフォーミュラ）。SP800-39 は、リスクモデルの広範囲にわたって共通のリスク因子を特定している。さらに、SP800-39 では、調整された価値尺度を複数定義することによって、システム開発ライフサイクルの初期段階におけるアセスメントに対して、入手可能な情報によって正当化される以上の詳細な情報の提供を強要することなく、システム開発ライフサイクル全体にわたって情報セキュリティリスクを評価するための、一貫性のあるアプローチの基礎を提供する。

2.4 リスクアセスメントの適用

先に述べたように、リスクアセスメントは、リスクマネジメント階層内の 3 つのすべての層（組織レベル、ミッション／業務プロセスレベル、情報システムレベル）において実施される。図 4 は、NIST SP 800-39 に定義されていて、戦略レベルから戦術レベルまでの複数のリスク視点を示す、リスクマネジメント階層を図示している。従来のリスクアセスメントは、通常、第 3 層レベル（すなわち、情報システムレベル）に焦点を合わせるため、結果として、第1層レベルまたは第 2 層レベルでより適切にアセスメントされるその他の重要なリスク因子（たとえば、主要なミッション／業務機能が、情報システムの相互接続をベースにしたアドバーサリによる脅威に晒されること）を見落とす傾向にある。

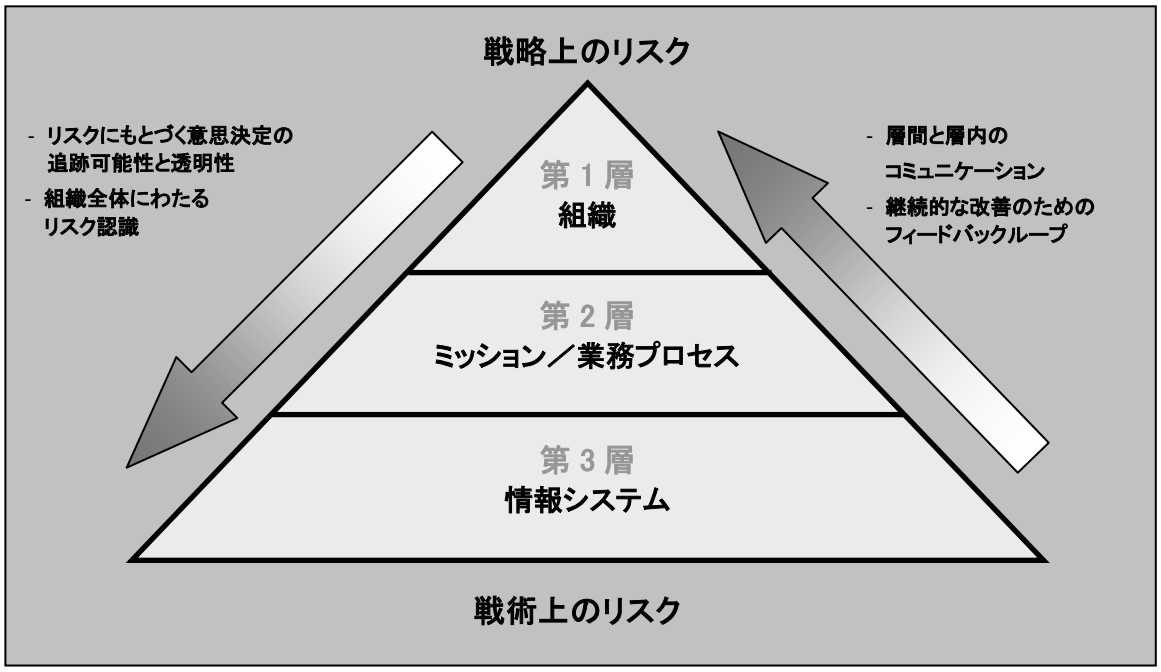


図 4: リスクマネジメント階層

リスクアセスメントは、リスクマネジメント階層内の異なる層におけるリスク対応に関する意思決定を支援する。第 1 層において、リスクアセスメントは、たとえば、以下の項目に影響を及ぼす可能性がある：(i) 組織全体にわたる情報セキュリティ導入計画、ポリシー、手順、および手引き; (ii) 適切なリスク対応のタイプ（すなわち、リスクの許容、回避、軽減、共有、または移転）; (iii) 情報技術／システムに対する投資決定; (iv) 調達; (v) 組織全体にわたる最低限のセキュリティ管理策; (vi) エンタープライズ／セキュリティアーキテクチャへの適合; ならびに (vii) 情報システムと共通管理策に対するモニタリング戦略と継続的な認可。第 2 層において、リスクアセスメントは、たとえば、以下の項目に影響を及ぼす可能性がある：(i) エンタープライズアーキテクチャ／セキュリティアーキテクチャの設計に関する意思決定; (ii) 共通管理策の選択; (iii) 組織のミッション／業務機能を支援する供給業者、サービス、および受託業者の選択; (iv) リスクを認識したミッション／業務プロセスの開発; ならびに (v) 組織の情報システムと、それらのシステムが稼働する環境に対する情報セキュリティポリシーの解釈。最後に、第 3 層において、リスクアセスメントは、たとえば、以下の項目に影響を及ぼす可能性がある：(i) 設計に関する意思決定（セキュリティ管理策の選択、調整、および補足と、組織の情報システムに対する IT 製品の選択を含む）; (ii) 導入に関する意思決定（特定の IT 製品または製品構成がセキュリティ

管理策の要求事項を満たすか否かを含む); ならびに (iii) 運用に関する意思決定（求められるモニタリング活動レベル、情報システムの運用認可の頻度、およびシステムメンテナンスに関する意思決定を含む）。

リスクアセスメントは、また、3 つの層にわたる、セキュリティに関連しないリスクマネジメント活動に対して情報を提供する。たとえば、第 1 層において、リスクアセスメントは以下に対して有用な入力データを提供する：(i) 業務リスクに関する意思決定（組織のミッション／業務機能を果たすための業務継続性を含む); (ii) 組織的リスクに関する意思決定（金銭上のリスク、コンプライアンスに関するリスク、規定に関するリスク、評判に関するリスク、および大規模なプロジェクトの全体にわたる累積調達に関するリスクを含む); ならびに (iii) 多重影響のリスク（サプライチェーンに関するリスクと、パートナーシップに伴うリスクを含む）。第 2 層において、リスクアセスメントは、ミッション／業務プロセスに特化した業務リスク、組織的リスク、多重影響のリスクに対して、同一の有用な入力データを提供する。第 3 層において、リスクアセスメントは、導入計画管理者、情報システム所有者および運用認可権限者と協調して情報セキュリティの専門家が実施する、情報システムのコスト、スケジュール、およびパフォーマンス上のリスクのアセスメントに対して情報を提供する。最善ではない（あるいは非効率的な）情報技術およびセキュリティソリューションを生み出し、割り当てられたミッション／業務機能を最大限の効率と費用対効果をもって実施する組織の能力に影響を及ぼす自己中心的な活動や、ストーブパイプのような活動を排除するためにも、組織内のこの種の協調が不可欠である。

情報セキュリティリスクは、各層におけるセキュリティに関連しないリスクの一因になることに留意することが重要である。したがって、特定の層におけるリスクアセスメントの結果は、その層におけるセキュリティに関連しないリスクのマネジメント活動に対する入力データとなり、それらの活動につながる。[36] さらに、より低い層におけるリスクアセスメントの結果は、より高い層におけるリスクアセスメントに対する入力データとなる。リスクは異なる時間尺度で発生する可能性がある（例：組織の現行の業務に関する情報が開示された場合、それらの業務の有効性がただちに損なわれる可能性がある一方で、戦略的計画に関する情報が開示された場合、将来にわたる業務遂行能力が損なわれる可能性がある）。リスク対応に関する意思決定は、異なる時間枠で実施される場合もある（例：組織のポリシーまたは投資戦略の変更は、場合によっては反映されるのに何年もかかる一方で、個別のシステムの設定の変更は、多くの場合ただちに実施される）。リスク対応に関する意思決定は、異なる時間枠で実施される場合もある（たとえば、組織のポリシーまたは投資戦略の変更は、場合によっては、反映されるのに何年もかかる一方で、個別のシステムの設定の変更は、多くの場合ただちに実施される）。通常、リスクマネジメントプロセスは、第 3 層よりも第 1 層と第 2 層において、よりゆっくりと進む傾向にある。これは、組織の広範囲に及ぶ業務と資産に影響を及ぼす可能性のあるリスクに対して、組織が通常どのように対処するかに起因している（そうしたリスク対応は、組織的な問題または制度上の問題を取り扱う必要があるだろう）。しかしながら、第 1 層における意思決定の中には、緊急な対応が必要なものもある（例：新たに発見された脅威または脆弱性が、組織全体にわたる軽減義務の履行を必要とする場合）。

[36] とりわけ、リスクアセスメント結果は、投資リスクの管理を支援する。NIST SP 800-65 は、情報セキュリティの CPIC（資本計画及び投資管理）プロセスへの統合に関する手引きとなる。

2.4.1 組織層におけるリスクアセスメント

第 1 層において、リスクアセスメントは、リスクを管理するための組織の戦略、ポリシー、手引、および手順を支援する。第 1 層において実施されるリスクアセスメントは、組織の業務、資産、および個人に焦点を当てる（すなわち、複数のミッション／業務分野にわたる包括的なアセスメント）。たとえば、第 1 層におけるリスクアセスメントは、以下を取り扱う可能性がある：(i) 他の組織とは異なる可能性のある、その組織に向けられた特定のタイプの脅威と、それらの脅威がポリシー決定にどのように影響を及ぼすか; (ii) アドバーサリによって利用される可能性のある、組織内の複数の情報システムにおいて発見された体系的な弱点または欠陥; (iii) （意図的であるか否かにかかわらず）組織の情報の消失または侵害により組織にもたらされる可能性のある負の影響; ならびに (iv) モバイルやクラウドなどの新しい情報技術およびコンピューティング技術の使用と、それらの技術を使用してミッション／業務を成功裏に実施するための組織の能力への影響。組織全体にわたるリスクアセスメントは、「リスクのフレーム化」ステップにおいて確立された（すなわち、主に、第 1 層における活動から導出された）想定、制限、リスク許容度、優先順位、およびトレードオフだけを基準にする場合がある。しかしながら、より現実的で意味深いリスクアセスメントは、複数のミッション／業務分野にわたって実施されたアセスメント（すなわち、主に、第 2 層における活動から導出されたもの）にもとづく。第 2 層におけるリスクアセスメントを第 1 層におけるリスクアセスメントに対する入力データとして効果的に利用するための組織の能力は、以下のような考慮によって形成される：(i) 組織のミッション／業務機能およびミッション／業務プロセスにおける類似点; ならびに (ii) その組織または下部組織が、親組織からどの程度自立しているか。分権組織、または多様なミッション／業務機能や運用環境を有する組織の場合、第 2 層におけるリスクアセスメントの結果を正規化するために、専門家による分析が必要になるだろう。最後に、第 1 層におけるリスクアセスメントは、第 2 層におけるリスクの要因を特定する際に組織が用意する業務継続計画(COOP)[37]からの、ミッション遂行に不可欠な機能の特定を考慮する。 第 1 層におけるリスクアセスメントの結果は、第 2 層と第 3 層における組織のエンティティ（部署、人）に伝達される。

2.4.2 ミッション／業務プロセス層におけるリスクアセスメント

第 2 層において、リスクアセスメントは、ミッション／業務プロセスの保護と耐性に関する要求事項の決定と、それらの要求事項を（ミッション／業務プロセスを支援する）ミッション／業務セグメントの一部として、エンタープライズアーキテクチャに割り当てることを支援する。この割り当ては、エンタープライズアーキテクチャに含まれる情報セキュリティアーキテクチャを介して成し遂げられる。第 2 層におけるリスクアセスメントは、特定のミッション／業務プロセス、とりわけ、情報システムが侵害された場合の代替えとなるミッション／業務プロセスに対して、情報システムを使用するか否か、また、使用するのであればいつ、どのように使用するかについての意思決定に情報を提供し、そうした意思決定を導く。第 2 層におけるリスクマネジメントおよび関連するリスクアセスメント活動は、事業継続計画(BCP)の策定と密接に関連する。第 2 層におけるリスクアセスメントは、ミッション／業務セグメントに焦点を当てる。ミッション／業務セグメントは、通常、組織の主要なミッション／業務機能に対する重大性や機微度がそれぞれに異なる複数の情報システムを含む。[38] 第 2 層におけるリスクアセスメントは、また、エンタープライズアーキテクチャの極めて重要な要素としての情報セキュリティアーキテクチャに焦点を当て

[37] NIST SP 800-34 は、情報システムの緊急時対応計画作成(ISCP)に関する手引きである。

[38] 組織のミッション／業務機能に対する情報システムの重大性は、ビジネス影響分析によって特定される場合がある。

て、第 3 層において組織が情報システムによって継承される共通管理策を選択するのを支援する。第 2 層において生成されたリスクアセスメント結果は、第 3 層における組織のエンティティ（部署、人）に伝達され、共有される。これにより、情報システムおよびそれらのシステムが稼働する環境に対するセキュリティ管理策の割り当てに情報が提供され、そうした割り当てが導かれる。第 2 層におけるリスクアセスメントは、また、組織のミッション／業務プロセスのセキュリティおよびリスク姿勢 (risk posture)をアセスメントし、その結果は、第 1 層における組織的リスクのアセスメントに情報を提供する。したがって、第 2 層におけるリスクアセスメントの結果は通常、第 1 層と第 3 層における組織のエンティティ（部署、人）に伝達される。

2.4.3 情報システム層におけるリスクアセスメント

第 2 層におけるコンテクストおよびシステム開発ライフサイクルは、第 3 層におけるリスクアセスメント活動の目的を決定し、その範囲を定める。初期リスクアセスメント（すなわち、以前のリスクアセスメントの更新ではなく、初めて実施されるリスクアセスメント）は、システム開発ライフサイクル内のいずれかのフェーズにおいて実施することができるが、理想的には、「開始」フェーズにおいて実施するのが望ましい。[39] 「開始」フェーズでは、リスクアセスメントは、予定している運用環境において情報システムの機密性、完全性、および可用性に影響を及ぼす、予期される脆弱性と素因的条件を評価する。そうしたアセスメントは、リスク対応に対して情報を提供し、情報システム所有者／導入計画管理者がミッション／業務遂行の責任者と協力して、セキュリティ分類と運用環境にもとづいて必要なセキュリティ管理策についての最終決定を行うことを可能にする。リスクアセスメントは、システム開発ライフサイクルの後のフェーズにおいても実施される。この際、前のフェーズにおいて実施されたリスクアセスメントの結果が更新される。構築後の、または導入後の情報システムに対するリスクアセスメントの結果は、通常、システムの脆弱性についての説明、それぞれの脆弱性に関連するリスクのアセスメント結果（したがって、脆弱性の重大さのアセスメント結果を更新することになる）、およびリスクを軽減するために取ることができる是正措置を含む。リスクアセスメント結果は、評価されたとおりに情報システムを運用することにより生じる、組織および情報システムに含まれる情報に対する総合的なリスクのアセスメントも含む。第 3 層におけるリスクアセスメントの結果は、第 1 層と第 2 層における組織のエンティティ（部署、人）に伝達される。

NIST 800-37 に記述されているように、リスクアセスメント活動は、リスクマネジメントフレームワーク(RMF)の各ステップに組み入れることができる。システム開発ライフサイクルアプローチにおける RMF は、主に第 3 層において実施されるが、たとえば、共通管理策の選択時には、第 1 層と第 2 層において適用される。リスクアセスメントは、セクション 3.1 に記載されているアセスメントの目的と適用範囲を反映する形で、RMF のステップごとに調整が可能である。リスクアセスメントは、システム開発ライフサイクルのさまざまなフェーズにおいて実施されるセキュリティアセスメントのタイプや、そうしたアセスメントの頻度、アセスメント時に適用される厳密さ、使用されるアセスメント手法、アセスメントされる対象のタイプ／数の決定を支援する。後述するように、RMF の一環として実施されるリスクアセスメントのメリットは、初期アセスメントと後続のアセスメントの両方によって実現される。

[39] NIST SP 800-64 は、システム開発ライフサイクルにおけるセキュリティ考慮事項に関する手引きである。

RMF ステップ 1 – 分類

組織は、セキュリティ管理策の選択の準備段階として、リスクエグゼクティブ（機能）によって規定されるリスクマネジメント戦略との一貫性を保った、セキュリティ分類に関する意思決定を行うために、初期リスクアセスメントを使用することができる。初期リスクアセスメントを実施することにより、脅威源、脅威事象、脆弱性、および素因的条件に関して得られた情報を1つにまとめることができる。その結果、組織は、そうした情報を使用して、組織の情報システムおよびそれらのシステムが稼働する環境に内在する既知の、および潜在的な脅威と脆弱性にもとづいて、情報と情報システムを分類することが可能になる。[40] セキュリティ分類に関する意思決定は、初期のベースラインセキュリティ管理策の選択に情報を提供する。ベースラインセキュリティ管理策は、RMF の「選択」ステップに記載されている、組織の調整活動と補足活動の開始点となる。

RMF ステップ 2 –選択

組織は、組織の情報システムおよび運用環境に導入するセキュリティ管理策の選択に情報を提供し、そうした選択を導くために、リスクアセスメントを使用することができる。セキュリティ分類プロセスにもとづいて初期のセキュリティ管理策ベースラインが選択された後、リスクアセスメントは、組織による以下の活動を支援する：(i) 適切な調整の手引きを適用し、具体的なミッション／業務要求事項、想定、制限、優先事項、トレードオフ、または組織が定めたその他の条件にもとづいて管理策を調整する; ならびに (ii) 具体的で信頼できる脅威関連情報にもとづいて管理策を補足する。[41] リスクアセスメントから得られる脅威関連情報は、アドバーサリの能力、意図、および標的に関する極めて重要な情報を提供する。こうした情報は、追加のセキュリティ管理策（関連するコストとメリットも含む）の選択に関する組織の意思決定に影響を及ぼす可能性がある。組織は、（通常、第 1 層と第 2 層における活動である）共通管理策の選択の際にも、リスクアセスメント結果を考慮する。リスクは、共通管理策を導入した結果、単一障害点が生じた場合に招かれる。なぜならば、共通管理策は、複数の情報システムによって継承される可能性のあるセキュリティ能力を提供するからである。リスクアセスメントが更新され洗練されるにつれて、組織は、アセスメント結果を用いて、入手可能な最新の脅威・脆弱性情報にもとづいて現行のセキュリティ管理策の選択を変更する。

RMF ステップ 3 – 導入

組織は、選択されたセキュリティ管理策の別の実施方法を特定するために、リスクアセスメント結果を使用することができる（例：セキュリティ管理策の、ある実装方法と別の実装方法のそれぞれに内在する脆弱性を考慮して）。一部の IT 製品、システムコンポーネント、または構造設計は、特定のタイプの脅威源に対して、他よりも脆弱である。こうした脆弱さは、セキュリティ管理策の開発と導入時に対処される。さらに、導入すべきものとして選択されたセキュリティメカニズムの強度は、リスクアセスメントから得られる脅威関連情報を考慮に入れる場合がある。IT 製品とシステムコンポーネントを個別に設定することにより、脅威事象の分析時に特定された脆弱性を排除できる場合がある。リスクアセスメント結果は、また、あるタイプの技術と別のタイプの技術のそれぞれを使用した場合のコスト、メリット、およびリスクのトレードオフに関する

[40] ある情報システムが存在する前に、初期のリスクアセスメントが実施される場合であっても、そのシステムで使用される予定の特定の技術、そのシステムによって継承される予定の共通管理策、あるいは、そのシステムが稼働する予定の環境に脆弱性が存在する可能性がある。

[41] 補足に関しては、NIST SP 800-53, Revision 4 の調整プロセスに組み入れられる予定である。

意思決定に、あるいは、特定の運用環境（例：特定の技術が利用できないために補完的管理策を使用しなければならない場合）においてセキュリティ管理策がどのように効果的に実施されるかについての決定に情報を提供する。リスクアセスメントが更新され洗練されるにつれて、組織は、アセスメント結果を用いて、脅威スペースが変化した場合に現行のセキュリティ管理策の実施が引き続き有効であるか否かを判断する。

RMF ステップ 4 – アセスメント

組織は、リスクアセスメントに情報を提供するために、セキュリティ管理策アセスメントの結果を使用することができる。（セキュリティアセスメント報告に記載される）セキュリティ管理策アセスメントは、組織の情報システムおよびそれらのシステムが稼働する環境に内在する脆弱性を特定する。導入されたセキュリティ管理策の部分的な、あるいは完全な機能不全、もしくは導入が計画されている管理策の不在は、脅威源によって利用される可能性のある潜在的な脆弱性となる。組織は、リスクアセスメントの結果を使用して、そうした脆弱性の重大さを判断する。その結果は、組織のリスク対応に情報を提供し、そうした対応を導く（例：リスク対応活動の優先順位付け、是正措置のマイルストーンの確立）。

RMF ステップ 5 – 認可

組織は、運用認可権限者に対してリスク関連情報を提供するために、リスクアセスメント結果を使用することができる。組織がリスクアセスメント結果にもとづいて実施するリスク対応は、組織の情報システムと運用環境に対する既知のセキュリティ体制となる。リスクアセスメントの結果は、運用認可権限者に対して、現行のセキュリティ体制をもってそれらのシステムを運用するか、あるいはセキュリティ管理策を追加して組織の業務と資産、個人、他の組織、または国家に対するリスクをさらに軽減するかについてのリスクにもとづく意思決定を下すのに必要な、極めて重要な情報を提供する。

RMF ステップ 6 – モニタリング

組織は、組織の継続的なモニタリングプロセスから得られるセキュリティ関連情報を使用して、リスクアセスメントを継続的に更新することができる。[42] 継続的なモニタリングプロセスは、以下を評価する：(i) セキュリティ管理策の有効性; (ii) 情報システムおよび運用環境に対する変更; ならびに (iii) 連邦政府の法律、規制、指令、ポリシー、標準、および手引きに対する準拠。リスクアセスメントが更新され洗練されるにつれて、組織は、アセスメント結果を用いて、リスクマネジメント戦略を更新し、学んだ教訓をリスクマネジメントプロセスに組み入れて、リスクに対する対応を強化し、組織のミッション／業務機能に合わせて調整された脅威・脆弱性情報の強固な基盤を構築する。

[42] NIST SP 800-137 は、情報システムおよび組織の情報セキュリティの継続的なモニタリングに関する手引きである。

2.4.4 リスクの伝達と情報共有

リスクアセスメントプロセスは、以下を確実にするための、利害関係者間の継続的なコミュニケーションと情報共有を伴う:(i) そうしたアセスメントに対する入力データが最大限に正確であること; (ii) たとえば、他の層におけるリスクアセスメントを支援するために、中間のアセスメント結果を使用できること; ならびに (iii) それらの結果が、リスクマネジメントプロセス内の「リスク対応」ステップに対する有意かつ有用な入力データとなること。リスクが伝達される方法と形式は、組織文化と、法律上、規制上、および契約上の制約の一つの現れである。リスクアセスメント時に生成された情報セキュリティリスクに関する情報やその他のリスク関連情報の伝達は、組織内の他の形式のリスク伝達との一貫性を保つことによって、その効果が発揮される。リスクアセスメントのメリットを最大限に引き出すためには、そうしたアセスメント時に生成された情報がリスクマネジメント階層内の 3 つのすべての層にわたって効果的に伝達され、共有されることを確実にするためのポリシー、手順、および実施メカニズムを確立しなければならない。[43] 組織内のリスク伝達と情報共有の重要性を強調するために、付録 D、E、F、G、H、および I の入力データ表 （すなわち、脅威源、脅威事象、脆弱性、素因的条件、発生可能性、影響、およびリスク）と、（付録 K に記載されている）リスクアセスメント報告に含めることが推奨される要素は、リスクマネジメント階層内の層間のリスク伝達／共有に関する推奨事項を示している。

的を絞ったリスクアセスメント

組織は、**的を絞った**リスクアセスメント、すなわち、特定の質問（例：既知の技術に依存することによってどのようなリスクが生じるか、既に発生したインシデントにもとづいて前に実施されたリスクアセスメントを修正するためのよい方法とは、新たに発見された脅威または脆弱性に関する知識にもとづいてどのようなリスクが新たに特定されるか）に対する答えを生成するために、あるいは特定の意思決定（例：第 2 層や第 3 層でなく第 1 層において管理されるべきリスクの特定）に情報を提供するために、適用範囲が狭く定義されたリスクアセスメントを使用することができる。組織は、組織の広範囲の情報システムに適用される一連の共通の脅威および脆弱性に起因する、第 1 層と第 2 層におけるリスクをアセスメントすることを検討してもよい。第 1 層と第 2 層においてリスクをアセスメントすることにより、組織は、個々の情報システムレベルで考慮される脅威と脆弱性の数を減らすことができ、そうした組織全体にわたるリスクに対する共通のリスク対応策を策定できる。このアプローチは、組織による共通管理策の選択プロセスを支援し、組織全体にわたるリスクアセスメントの有効性と費用対効果を向上させる。

リスクマネジメント階層内の 3 つのすべての層に関しては、以下に関する**特定の要求事項は存在しない**:(i) なんらかの特定のリスクアセスメントの特徴を定義するための形式、厳密さ、または詳細レベル; (ii) そうしたリスクアセスメントを実施するのに用いられる方法論、ツール、および技術; あるいは (iii) アセスメント結果の形式と内容、および関連する報告手段。組織は、リスクアセスメントの実施方法、そうしたアセスメントの適用範囲、その結果の使用方法に関して、**最大限の柔軟性**を有する。組織には、最高幹部／管理職者による十分な情報を得た上でのリスクマネジメント上の意思決定を容易にするために必要な情報を、最も効果的に、かつ最も費用対効果が高くなる形で提供できるよう、本手引を使用することが推奨される。

[43] NIST SP 800-117 と 800-126 は、SCAP (Security Content Automation Protocol)プログラムに関する手引きである。SCAP プログラムは、脅威・脆弱性情報の標準的で一貫性のある伝達手段を提供する。

第 3 章

プロセス

組織内でリスクアセスメントを実施する

本章では、以下を含む、情報セキュリティリスクをアセスメントするためのプロセスについて説明する：(i) リスクアセスメントプロセスの簡単な概要; (ii) リスクアセスメントの準備に必要な活動; (iii) 効果的なリスクアセスメントの実施に必要な活動; (iv) アセスメント結果の伝達と、リスク関連情報の共有に必要な活動; ならびに (v) リスクアセスメント結果の継続的な保守に必要な活動。リスクアセスメントプロセス [44] は、以下の 4 つのステップから成る：(i) アセスメントの準備; (ii) アセスメントの実施; (iii) アセスメント結果の伝達; ならびに (iv) アセスメントの保守。[45] 各ステップは、一連のタスクに分けられる。各タスクの補足の手引きは、リスクアセスメントを実施する組織に対して追加の情報を提供する。リスク表およびアセスメントスケールの例は、適切なタスクの欄に記載されていて、付録に記載されている追加の、より詳細な情報と相互参照される。図 5 は、リスクアセスメントプロセス内の基本ステップを図示し、アセスメントを実施するための具体的なタスクを強調表示している。

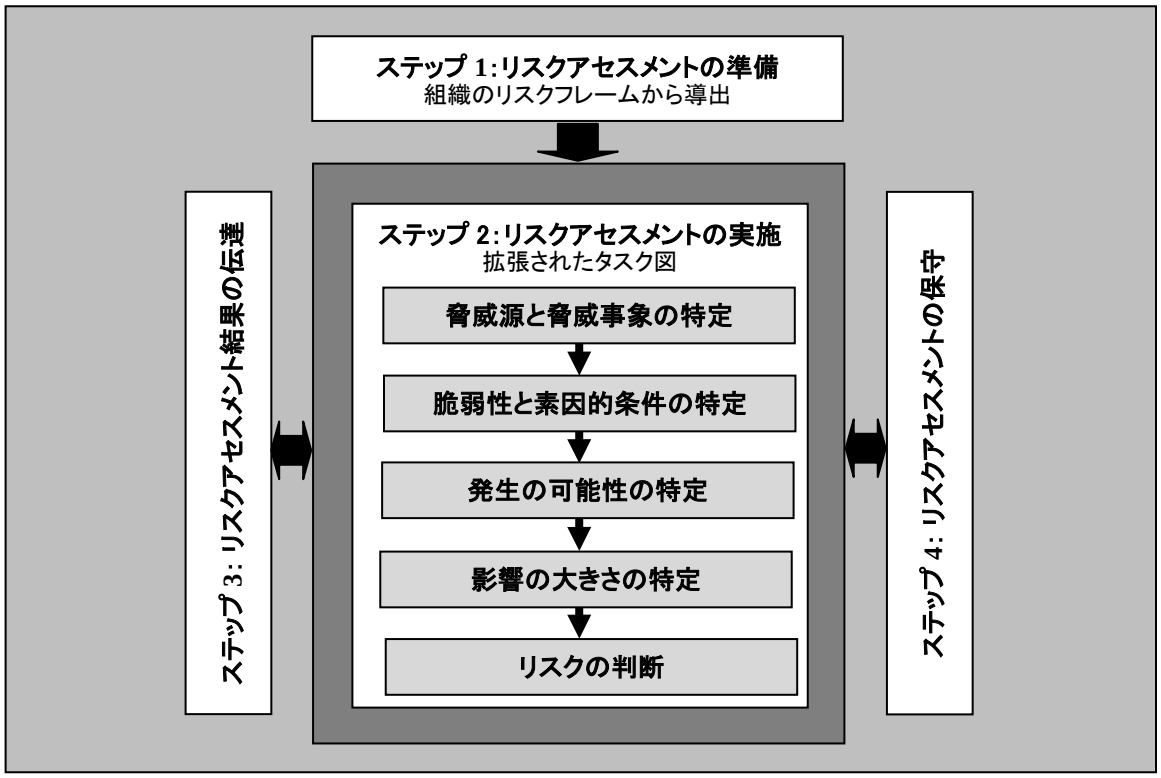


図 5：リスクアセスメントプロセス

[44] 第 3 章に記載されているプロセス記述の意図は、効果的なリスクアセスメントを実現するための必須の要素について、よく使われる表現を用いて説明することにある。これは、それらのアセスメントを実施するうえでの組織の柔軟性を制限することを意図していない。組織は、このプロセス記述の意図との一貫性を保った他の手順を実施してもよい。

[45] 本文書に記載されている 4 つのステップから成るリスクアセスメントプロセスは、NIST SP 800-39 に記載せれている一般的なリスクアセスメントプロセスとの一貫性を保っている。リスクアセスメントに関連する特定の活動を効果的に実施するための、より詳細な手引きを用意する必要があるのなら、追加のステップとタスクが必要になる。

3.1 リスクアセスメントの準備

リスクアセスメントプロセスの 1 番目のステップは、アセスメントの準備である。このステップの目的は、リスクアセスメントのコンテクストを確立することにある。このコンテクストは、リスクマネジメントプロセス内の「リスクのフレーム化」ステップの結果をもとに確立され、情報が提供される。リスクのフレーム化は、たとえば、リスクアセスメントの実施のポリシーと要求事項、採用すべき特定のアセスメント方法論、考慮すべきリスク因子の選択手順、アセスメントの適用範囲、分析の厳密さ、どの程度型にはめるか、ならびに組織全体にわたる一貫性があり繰り返し可能なリスクの判断を容易にするための要求事項に関する情報を特定する。組織は、リスクアセスメントの準備に必要な情報を得るために、リスクアセスメント戦略を実用的な範囲内で使用する。リスクアセスメントの準備は、以下のタスクを含む:

- アセスメントの目的を特定する
- アセスメントの適用範囲を特定する
- アセスメントに関連する想定と制限を特定する
- アセスメントへの入力データとして使用する情報の情報源を特定する、ならびに
- アセスメント時に使用すべきリスクモデルと分析アプローチ(すなわち、アセスメントアプローチと分析アプローチ)を特定する。

ステップ 1:リスクアセスメントの準備

目的を特定する

タスク 1-1: アセスメントが生成する情報と、アセスメントが支援する意思決定の観点から、リスクアセスメントの目的を特定する。

補足の手引き: リスクアセスメントの目的は、アセスメントが適切な情報を生成し、意図している意思決定を支援するのを確実にするためにも、十分な詳細さを持って明記される。組織は、たとえば組織が定めたテンプレートを使用して、リスクアセスメント時に生成された情報をどのように捉えて提供するかについての手引きを用意することができる。付録 Kは、リスクアセスメント報告のテンプレートの例、または推奨されるリスク伝達手段を示している。第3層において、リスクアセスメントは以下を支援する:(i) システム開発ライフサイクル全体にわたる認可に関連する意思決定; (ii) 互恵、とりわけアセスメント情報の再利用; (iii) 第2層におけるリスクマネジメント活動; ならびに (iv) システム開発ライフサイクル全体にわたる計画的なリスクマネジメント活動。第2層において、リスクアセスメントは組織に対して以下を可能にする:(i) 組織のミッション/業務プロセスを支援する複数の情報システム間の依存関係と、リスクがどのようにして許容、拒否、共有、移転、または軽減されるかについて理解する; (ii) 組織のリスク対応(例:依存を減らす、接続を制限する、モニタリングを強化する、または集中させる、および情報/システムの耐障害性を強化する)についての構造上と運用上の意思決定を支援する; (iii) ミッション/業務プロセスの事前のリスク対応戦略および行動方針を定めることができるよう、脅威を特定する; ならびに (iv) 互恵を支援する(とりわけ情報の共有を可能にするために)。第1層において、リスクアセスメントは、(i) リスクエグゼクティブ(機能)を支援する; ならびに (ii) リスクマネジメント戦略に対する重要な入力データとなる。これらの共通の目的に加えて、リスクアセスメントは、特定の質問(例:新たに発見された脆弱性(あるいは脆弱性の集合)に関して、新たな接続を許可する、特定の機能を外部委託する、または新たな技術を採用することによってどのようなリスクが生じるか?)に答えるといった、極めて特殊な目的を有する場合がある。すべての階層におけるリスクアセスメントの結果は、情報セキュリティの要求事項を明確に示すのに役立ち、調達プロセスに情報を提供するために使用できる。

リスクアセスメントの目的は、アセスメントが以下のいずれに該当するかによって左右される:(i) 初期アセスメント; あるいは (ii) リスクマネジメントプロセス内の「リスクへの対応」ステップまたは「リスクのモニタリング」ステップにおいて開始された後続のアセスメント。初期アセスメントの場合、その目的は、たとえば以下を含む:(i) リスクの基礎アセスメントを確立する;あるいは (ii) 組織の業務と資産、個人、他の組織、および国家に対する脅威、脆弱性、影響と、リスクのモニタリングの一環として長期にわたって追跡すべきその他のリスク因子を特定する。「リスクへの対応」ステップにおいて開始されたアセスメントの場合、その目的は、たとえば、代替えのリスク対応の比較分析を行う、また

は特定の質問に答える（上述の「的を絞ったリスクアセスメント」の説明を参照）といったことを含む。これらとは別に、「リスクのモニタリング」ステップにおいて開始された再アセスメントの場合、その目的は、たとえば、以下にもとづいてリスクアセスメントを更新することを含む：(i) 組織の情報システムまたは運用環境に導入されているセキュリティ管理策の有効性の継続的な判断; (ii) 情報システムまたは運用環境に対する変更（例：ハードウェア、ファームウェア、ソフトウェアの変更; システム固有の管理策、ハイブリッド管理策、または共通管理策に対する変更; ミッション／業務プロセス、共通インフラおよび支援サービス、脅威、脆弱性、または施設に対する変更）; ならびに(iii) コンプライアンス検証活動の結果。再アセスメントは、既に発生したインシデントに起因して開始されることもある（例：組織の情報または情報システムを侵害するサイバー攻撃）。

適用範囲を特定する

タスク 1-2: 組織の適用範囲、サポートされている時間枠、および構造上／技術上の考慮事項の観点から、リスクアセスメントの適用範囲を特定する。

補足の手引き: リスクアセスメントの適用範囲は、アセスメントにおいて何が考慮されるかを決定する。リスクアセスメントの適用範囲は、リスクにもとづく意思決定を行うために利用できる情報の範囲に影響を及ぼし、アセスメントとリスクマネジメント戦略を要請する組織の当局者によって決定される。リスクアセスメントの適用範囲を決定することは、組織が以下を決定するのを支援する：(i) アセスメントにおいてどの層が取り扱われるか; (ii) 組織のどの部署が、どのようにアセスメントの影響を受けるか; (iii) アセスメントの結果がどのような意思決定を支援するか; (iv) アセスメントの結果がどれくらいの期間にわたって有効であるか; ならびに (v) アセスメントの更新の必要性に影響を及ぼすものは何か。リスクアセスメントの適用範囲を決定することは、リスクアセスメント報告の形式と内容に加えて、アセスメントの実施結果として共有すべき情報を決定するのを支援する。第3層において、リスクアセスメントの適用範囲は、情報システムの運用認可を下す範囲に依存する場合がある。付録 Kは、リスクアセスメント報告に含まれる可能性のある情報の例、または推奨されるリスク伝達手段を記載している。

組織の適用範囲

組織の適用範囲は、組織または下部組織のどの部署がリスクアセスメント、およびアセスメント実施後のリスクにもとづく意思決定の影響を受けるかを示す（意思決定に関連する活動とタスクを実施することに責任を負う、組織または下部組織の部署を含む）。たとえば、リスクアセスメントは、組織の特定のミッション／業務機能またはミッション／業務プロセスを支援する情報システムに関する意思決定に情報を提供する。これは、特定の情報システムに導入するセキュリティ管理策の選択、調整、または補足に関して、あるいは共通管理策の選択に関しての意思決定を含む。リスクアセスメントは、また、密接にかかわるミッション／業務機能またはミッション／業務プロセスの集合に関する意思決定に情報を提供する。リスクアセスメントの適用範囲は、組織が現時点で依存しているミッション／業務機能、ミッション／業務プロセス、共通インフラ、または共有サービスだけでなく、組織が特定の運用条件の下で使用する可能性のある、これらのものも含む場合がある。

有効性の時間枠

組織は、特定のリスクアセスメントの結果が、リスクにもとづく意思決定に対して、どれくらいの期間にわたって合法的に情報を提供することが可能かを判断する。この時間枠は、通常、リスクアセスメントの目的に関連する。たとえば、第 1 層におけるポリシー関連の意思決定に情報を提供するためのリスクアセスメントは、長期間にわたって有効である必要がある。なぜならば、多くの組織において、ポリシーの変更の統治手順は多大な時間を要するからである。第 3 層における、情報システムの補完的セキュリティ管理策の使用に関する意思決定に情報を提供するために実施されるリスクアセスメントは、必要とされるセキュリティ能力を提供する IT 製品が売り出されるまでの間だけ、有効であるだろう。組織は、リスクアセスメント結果の有用寿命と、現行のアセスメント結果が有効でなくなる（または不適切になる）条件について決定する。リスクのモニタリングは、リスクアセスメントの時間枠の有効性を判断するために使用できる。リスクアセスメント結果に加えて、組織は、リスクのアセスメントに使用されるあらゆるタイプの情報／データの現在性／適時性（すなわち、潜在期 (latency)または有効期間）についても考慮する。これは、情報を再利用し、アセスメント結果の有効性を評価する際には、とりわけ重要である。

構造上／技術上の考慮事項

組織は、リスクアセスメントの適用範囲を明確にするために、構造上／技術上の考慮事項を用いる。たとえば、第 3 層において、リスクアセスメントの適用範囲は、その運用環境における組織の情報システムである場合がある。これは、継承された管理策に内在する脆弱性が考慮されるよう、情報システムをその構造上のコンテクストに置くことを伴う。その一方で、アセスメントの適用範囲は、継承された脆弱性については考慮せずに、情報システムだけに限定される場合もある。第 2 層において、リスクアセスメントの適用範囲は、ミッション／業務セグメントの構造（例：特定のミッション／機能を支援するすべてのシステム、サービス、およびインフラを含む）の観点から定義されることもあ

る。いずれかの層における的を絞ったリスクアセスメントの場合、答えを出すべき特定の質問が、特定の技術の適用範囲を制限する場合がある。

想定と制限を特定する

タスク 1-3: リスクアセスメントが具体的にどのような想定と制限のもとで実施されるかを特定する。

補足の手引き: リスクマネジメントプロセス内の「リスクのフレーム化」ステップの一環として、組織は、組織内で使用されている具体的な想定、制限、リスク許容度および優先順位／トレードオフを明確にして、投資および運用上の意思決定を行う。この情報は、組織のリスクアセスメントに情報を提供し、そうしたアセスメントを導く。組織のリスクマネジメント戦略が言及されない場合、想定と制限は、リスクアセスメントによって特定され、文書化される。「リスクのフレーム化」ステップにおいて組織によって特定され、組織のリスクマネジメント戦略の一部として含まれる想定と制限は、個々のリスクアセスメントにおいて繰り返す必要はない。想定と制限を明確にすることによって、リスクアセスメント用に選択されたリスクモデルがより明瞭になり、アセスメント結果の再現性／繰り返し性が向上し、組織間の互恵の機会が増加する。組織は、たとえば以下を含む、リスクアセスメントに関連する重要な分野における想定について特定する：(i) 脅威源; (ii) 脅威事象; (iii) 脆弱性と素因的条件; (iv) 潜在的影響; (v) アセスメントアプローチと分析アプローチ; ならびに (vi) どのミッション／業務機能が主要であるか。組織は、また、たとえば以下を含む、リスクアセスメントに関連する重要な分野における制限について特定する：(i) アセスメントに利用できる資源; (ii) アセスメントに必要なスキルと専門知識; ならびに (iii) ミッション／業務活動に関連する運用上の考慮事項。たとえば、組織が、脅威と影響をどのようにアセスメントすべきかについての組織の想定では、最悪の場合の予測を使用するか、最良の場合の予測を使用するか、あるいは、それらの端点の間のいずれかを使用することになる。最後に、組織は、組織の想定に関する不確実性、またはリスクアセスメントにおいて使用されるその他の情報を考慮する。想定の不確実性は、組織のリスク許容度に影響を及ぼす可能性がある。たとえば、具体的な、または信頼できる情報がない状態での想定は、そうした不確実性が想定に影響を及ぼすため、組織のリスク許容度を低下させるであろう。以降の各セクションは、リスクアセスメントの想定／制限が特定される分野の代表的な例を代表的な例をいくつか示す。

脅威源

組織は、リスクアセスメント時に考慮されるべき脅威源を決定する。組織は、脅威を特定するために使用されるプロセスと、脅威の特定プロセスに関連するあらゆる想定を明確にする。そうした情報が「リスクのフレーム化」ステップにおいて特定され、組織のリスクマネジメント戦略の一部として含まれる場合、その情報を個々のリスクアセスメントにおいて繰り返す必要はない。リスクアセスメントは、単一の広範囲にわたる脅威源（例：アドバーサリによる）や特定の脅威源（例：信頼されている内部の者による）など、あらゆるタイプの脅威源を取り扱うことができる。表 D-2 は、リスクアセスメントの想定を特定する際に組織によって考慮される、脅威源の分類体系の例を示している。

脅威事象

組織は、リスクアセスメント時に考慮されるべき脅威事象と、そうした事象についての記述に必要な詳細レベルを決定する。脅威事象についての記述は、ごく一般的な用語（例：フィッシング詐欺、分散型サービス妨害）を使用して、または戦術、技法、手順を用いたより記述的な用語を使用して、あるいは、かなり特殊な用語（例：特定の情報システム、技術、組織、役割、または場所の名前）を使用して行うことができる。さらに、組織は、以下を考慮する：(i) リスクアセスメントにおいて具体的な脅威事象を特定する際の開始点として使用できる、代表的な一連の脅威事象; ならびに (ii) 脅威事象がリスクアセスメントの目的に関連するとみなされるのに必要な、確認のレベル。たとえば、組織は、（組織内部またはピア／パートナー組織によって）観測された脅威事象のみを考慮する場合もあれば、あらゆる脅威事象を考慮する場合もある。表 E-2 と表 E-3 は、アドバーサリによる脅威事象と、アドバーサリによるもの以外の脅威事象の典型的な例を、すべての層におけるリスクアセスメントに使用できるだけの詳細レベルで示している。より詳細な情報は、複数の情報源（例：CAPEC(Common Attack Pattern Enumeration and Classification)）から得られる。考慮すべき脅威事象に関する組織の想定と、詳細レベルは、タスク 2-2 に情報を提供する。

脆弱性と素因的条件

組織は、リスクアセスメント時に考慮されるべき脆弱性と、脆弱性についての記述の詳細レベルを決定する。組織は、脆弱性を特定するために使用されるプロセスと、脆弱性の特定プロセスに関連するあらゆる想定を明確にする。そうした情報が「リスクのフレーム化」ステップにおいて特定され、組織のリスクマネジメント戦略の一部として含まれる場合、その情報を個々のリスクアセスメントにおいて繰り返す必要はない。脆弱性は、組織の情報システム（例：ハードウェア、ソフトウェア、ファームウェア、内部コントロール、およびセキュリティ手順）に関連する場合もあれば、それらのシステムが稼働する環境（例：組織のガバナンス、外部との関係、ミッション／業務プロセス、エンタープライズアーキテクチャ、情報セキュリティアーキテクチャ）に関連する場合もある。組織は、また、たとえば、採用されるアーキテクチャと技術、運用環境、および職員を含む、リスクアセスメント時に考慮されるべき素因的条件についても決定

する。表 F-4 は、そうした素因的条件の典型的な例を示している。考慮すべき脆弱性と素因的条件に関する組織の想定と、詳細レベルは、タスク 2-3 に情報を提供する。

発生の可能性

組織は、発生の可能性の特定を行うために使用されるプロセスと、発生の可能性の特定プロセスに関連するあらゆる想定を明確にする。そうした情報が「リスクのフレーム化」ステップにおいて特定され、組織のリスクマネジメント戦略の一部として含まれる場合、その情報を個々のリスクアセスメントにおいて繰り返す必要はない。発生の可能性をどのように特定するかに関する組織の想定は、タスク 2-4 に情報を提供する。

影響

組織は組織の業務（すなわち、ミッション、機能、イメージ、および評判）、組織の資産、個人、他の組織、および国家にもたらされる可能性のある負の影響を特定する。組織は、影響の特定を行うために使用されるプロセスと、影響の特定プロセスに関連するあらゆる想定を明確にする。そうした情報が「リスクのフレーム化」ステップにおいて特定され、組織のリスクマネジメント戦略の一部として含まれる場合、その情報を個々のリスクアセスメントにおいて繰り返す必要はない。組織は、影響について、たとえば特定のミッション／業務プロセスまたは情報資源（例：情報、職員、設備、資金、および情報技術）を含む詳細レベルで対処する。組織は、リスクアセスメントに提供する影響に関する情報に、ビジネス影響分析によって得られた情報を含めることができる。表 H-2 は、組織によって考慮される影響（すなわち、被害）の典型的な例を示している。影響をどのように、また、どの程度詳細に特定するかに関する組織の想定は、タスク 2-5 に情報を提供する。

リスク許容度と不確実性

組織は、許容できるリスクのレベルとタイプを特定する。リスク許容度は、組織全体にわたって一貫性が確保されるよう、組織のリスクマネジメント戦略の一環として特定される。組織は、また、リスク因子がアセスメントされる際の不確実性について、理由をどのように特定するかに関する手引きを用意する。なぜならば単一の、あるいは複数の因子の不確実性は、リスクレベルの評価結果だけでなく、不完全、不十分、または想定に依存する予測をどのようにして補うかにまで波及するからである。組織が APT(advanced persistent threat)について考慮する際には、脅威事象の発生可能性のアセスメントがかなりの度合の不確実性を伴うこともあるため、不確実性についての考慮がとりわけ重要になる。これを補うために、組織は、発生可能性を特定するためのさまざまなアプローチを取ることができる。これらのアプローチは、（予測できるほど近い将来に発生することが確実である）最悪の場合の発生可能性を想定することから始まり、ある事象が観測されていないのなら発生する可能性は低いと想定するまでに至る。組織は、また、どのレベルのリスク（発生可能性と影響の組み合わせ）であれば、リスク因子のさらなる分析が必要でないかについて決定する。

分析アプローチ

リスクアセスメントは、アセスメントアプローチ（すなわち、定量的、定性的、半定量的）と分析アプローチ（すなわち、脅威を重視した、資産／影響を重視した、脆弱性を重視した）の両方を含む。アセスメントアプローチと分析アプローチの組み合わせは、リスクアセスメントのための分析的アプローチ(analytic approach)を形成する。組織は、脅威がどの程度詳細に、かつ、どのような形式で分析されるか（脅威事象または脅威シナリオについての記述の詳細レベルを含む）を決定する。分析アプローチが異なれば、発生可能性を特定する有害事象の特徴定義の詳細レベルも異なる。たとえば、負の影響は、以下のいくつかの方法を用いることによって、その特徴を定義することができる（後述の方が、より詳細である）：(i) （脅威源を最大限に取り入れて発生可能性を特定する）脅威イベント; (ii) 脅威イベントと脅威源を組み合わせる; あるいは (iii) 詳細な脅威シナリオ／攻撃の木。 通常、組織は、極めて重要なミッション／業務機能、共通インフラ、または複数のミッション／業務機能が依存する共有サービス（単一障害点としての）、および重大性と機微度が高い情報システムについては、より詳細な情報を求めるであろう。ミッション／業務遂行の責任者は、ミッション／業務セグメントにおけるリスクの「ホットスポット」（特に懸念される情報システム、サービス、または重要インフラのコンポーネント）に対して、本手引きを拡張してもよい。

情報源を特定する

タスク 1-4: リスクアセスメントにおいて使用される記述的情報、脅威関連情報、脆弱性関連情報、および影響関連情報の情報源を特定する。

補足の手引き: 記述的情報は、組織による、脅威関連情報と脆弱性情報の関連性の特定を可能にする。第1層において、記述的情報は、たとえば、組織内に定着しているリスクマネジメントおよび情報セキュリティガバナンス構造のタイプと、組織が極めて重要なミッション／業務機能をどのように特定し優先順位を付けるかを含む。第2層において、記述的情報は、たとえば、以下に関する情報を含む：(i) 組織のミッション／業務プロセス、機能管理プロセス、および情報の流れ; (ii) エンタープライズアーキテクチャ、情報セキュリティアーキテクチャ、リスクアセスメントの適用範

囲内にあるシステム、共通インフラ、および共有サービスの技術／プロセスの流れの構造; ならびに (iii) 組織が業務を行う外部環境（たとえば、外部のプロバイダとの関係や依存関係を含む）。そうした情報は、通常、構造に関する文書（とりわけ、業務に関しておおまかに説明する文書）、事業継続計画、およびリスクアセスメントの適用範囲内にある組織の情報システム、共通インフラ、および共有サービスのリスクアセスメント報告に記載されている。第3層において、記述的情報は、たとえば、以下に関する情報を含む：(i) 組織の情報システムのデザインと、それらのシステムに使用された技術; (ii) それらのシステムが稼働する環境; (iii) 他の情報システムに対する接続と依存; ならびに (iv) 共通インフラまたは共有サービスに対する依存。そうした情報は、システムに関する文書、緊急時対応計画、ならびに、他の情報システム、インフラ、およびサービスのリスクアセスメント報告に記載されている。

表D-1、E-1、F-1、H-1および I-1に記載されているように、情報源は組織にとって内部であったり、外部であったりする。脅威と脆弱性の両方に対する洞察を提供する内部の情報源は、たとえば、リスクアセスメント報告、インシデント報告、セキュリティログ、トラブルチケットおよびモニタリング結果を含む。内部的には、ある層におけるリスクアセスメント報告からの情報は、他の層におけるリスクアセスメントへの入力データとなることを覚えておこう。ミッション／業務遂行の責任者は、彼らが依存する共通インフラおよび／または支援サービスのみならず、彼らが特定の運用環境において使用する可能性のあるものについても特定することが推奨される。脅威関連情報の外部の情報源は、コミュニティを跨る組織（例：US-CERT(US Computer Emergency Readiness Team)、部門パートナー（例：国防総省のDCISE(Defense Industrial Base Collaborative Information Sharing Environment)を使用したDIB(Defense Industrial Base)、重要インフラ部門向けのISACs(Information Sharing and Analysis Centers)）、調査機関および非政府機関（例：Carnegie Mellon University、Software Engineering Institute-CERT）、ならびにセキュリティサービスプロバイダ）を含む。外部の情報源を使用する組織は、脅威関連情報の適時性、具体性および関連性を考慮する。脅威関連情報の情報源と同様に、脆弱性情報の情報源も、組織にとって内部であったり、外部であったりする（表F-1を参照）。内部の情報源は、たとえば、脆弱性アセスメント報告を含む。脆弱性情報の外部の情報源は、上で特定された脅威関連情報の情報源に類似する。表F-1に記載されているように、素因的条件に関する情報は、たとえば、情報システム、運用環境、共有サービス、共通インフラ、およびエンタープライズアーキテクチャについての記述を含む、さまざまな情報源から入手できる。表H-1に記載されているように、影響に関する情報の情報源は、たとえば、ミッションへの影響分析／ビジネス影響分析、情報システムコンポーネント一覧、およびセキュリティ分類を含む。セキュリティ分類は、組織に割り当てられたミッションを遂行し、組織の資産を保護し、組織の法的責任を果たし、組織の日々の職務を維持し、職員を守るために組織が必要とする情報および情報システムに対して、害を及ぼす事象が発生した場合にもたらされる影響について決定する手段となる。セキュリティ分類は、組織の業務と資産、個人、他の組織、および国家に対するリスクをアセスメントする際に、脆弱性情報および脅威関連情報と共に用いられる。セキュリティ分類は、セキュリティ目的である機密性、完全性および可用性を満たすことができない場合の影響の初期概要を示し、表H-2に記載されている「被害」のタイプ別に伝達される。

リスクモデルと分析的アプローチを特定する

タスク 1-5: リスクアセスメントにおいて使用されるリスクモデルと分析的アプローチを特定する。

補足の手引き: 組織は、リスクアセスメントの実施に使用する単一の、あるいは複数のリスクモデルを定義 (セクション2.3.1を参照)し、どのリスクモデルをリスクアセスメントに使用すべきかを特定する。アセスメント結果の互恵を容易にするために、組織固有のリスクモデルは、付録に定義されているリスク因子（すなわち、脅威、脆弱性、影響、発生可能性、および素因的条件）を含むか、あるいは、それらのリスク因子に変換される。組織は、また、アセスメントアプローチ（すなわち、定量的、定性的、半定量的）、分析アプローチ（すなわち、脅威を重視した、資産／影響を重視した、脆弱性を重視した）を含む、リスクアセスメントにおいて使用される具体的な分析的アプローチを特定する。アセスメント可能なそれぞれのリスク因子は、表現がそれぞれに異なる3つアセスメントスケール（定性的なスケールが1つ、半定量的なスケールが2つ）を含む。組織は、通常、リスクアセスメントにおいて使用されるアセスメントスケールを定義する（あるいは、付録から選択し、調整する）。この際、具体的な値に関して、組織として有意な例を注記し、半定量的なアプローチの瓶間のブレークポイントを定義する。また、ミッション／業務遂行の責任者は、ミッション／業務に特化した例を、さらなる注釈と共に提供する場合がある。組織は、異なる環境において使用される、異なるアセスメントスケールを特定する場合がある。たとえば、低位影響の情報システムでは、定性的な値を使用し、中位および高位影響のシステムでは、最も細かい半定量的な値（0-100）を使用することが考えられる。SP800-39で論じられているように、タスク1-1（リスクの想定）では、リスク因子に適用される相対的な重み付けが、組織によって異なる。したがって、本ガイドラインは、半定量的な値を結合するための具体的なアルゴリズムは指定しない。組織固有のリスクモデルは、リスク因子を結合するためのアルゴリズム（例：公式、表、ルール）を含む。組織固有のリスクモデルが、「リスクのフレーム化」ステップの一環としてリスクマネジメント戦略に含まれていない場合には、本タスクの一環として、値を結合するためのアルゴリズムを指定する。リスク因子を結合するためのアルゴリズムは、組織のリスク許容度を反映する（例として、タスク2-4の「補足の手引き」を参照）。組織固有のリスクモデルは、リスクアセスメント

の準備の一環として以下を実施することによって、改良される：(i) リスクモデルを特定し、そのモデルを使用する根拠を示す（組織固有の複数のリスクモデルを提供する場合）; (ii) リスク因子の値の追加の例を示す; ならびに (iii) アセスメントに特化したあらゆるアルゴリズムを指定する（例：攻撃に対するグラフ分析技術を使用したアルゴリズム）。組織のリスクマネジメント戦略に、前から存在する組織固有のリスクモデルまたは分析的アプローチが定義されていない場合は、リスクアセスメントにおいて使用されるリスクモデルおよび分析的アプローチは、本タスクにおいて定義され、文書化される。

主要な活動の要約 – リスクアセスメントの準備

- リスクアセスメントの**目的**を特定する。
- リスクアセスメントの**適用範囲**を特定する。
- リスクアセスメントがどのような**想定**と**制限**のもとで実施されるかを特定する。
- リスクアセスメントにおいて使用される脅威関連情報、脆弱性情報、および影響に関する情報の**情報源**を特定する（表 D-1、E-1、F-1、 H-1、および I-1 を参照：これらは組織ごとに調整される）。
- リスクアセスメントにおいて使用する**リスクモデル**、**アセスメントアプローチ**、および**分析的アプローチ**を特定する、または改良する。

3.2 リスクアセスメントの実施

リスクアセスメントプロセスの 2 番目のステップは、アセスメントの実施である。このステップの目的は、リスクレベルによって優先順位付けされ、リスク対応に関する意思決定に情報を提供する、情報セキュリティリスク一覧を生成することにある。この目的を達成するために、組織は、脅威および脆弱性、影響および発生可能性、ならびにリスクアセスメントプロセスに伴う不確実性を分析する。本ステップは、また、それぞれのタスクの一環としての極めて重要な情報の収集を含み、リスクアセスメントプロセス内の「アセスメントの準備」ステップにおいて確立されたアセスメントコンテクストに従って実施される。リスクアセスメントに期待されるのは、「アセスメントの準備」ステップにおいて確立された具体的な定義、手引き、および方向性に従って脅威スペース全体を適切に対象化することである。しかしながら、実際のところ、利用可能な資源内で適切な対象化を可能にするには、脅威源、脅威事象、および脆弱性を一般化して完全な対象化を確実にすることと、リスクアセスメントの目的を達成するために必要なだけの具体的で詳細な脅威源、脅威事象および脆弱性をアセスメントすることが求められる。リスクアセスメントの実施は、以下の具体的なタスクを含む:

- 組織に関連する脅威源を特定する。
- それらの脅威源によって生成されうる脅威事象を特定する。
- 特定の脅威事象を介して脅威源によって利用されうる組織内の脆弱性を特定し、さらに、利用が成功するか否かを左右する素因的条件を特定する。
- 特定された脅威源が特定の脅威事象を開始する可能性と、それらの脅威事象が功を奏する可能性を特定する。
- (特定の脅威事象を介して)脆弱性が脅威源によって利用された場合にもたらされる、組織の業務と資産、個人、他の組織、および国家に対する負の影響を特定する。
- 脆弱性が脅威源によって利用される可能性と、そうした利用がもたらす影響との組み合わせである、情報セキュリティリスク(リスクの判断に伴うあらゆる不確実性を含む)を特定する。

上記の具体的なタスクは、明確になることを目的として、逐次的に示されている。しかしながら、実際のところ、タスク間の反復が必要であり、かつ、予期される。[46] リスクアセスメントの目的によっては、組織がこれらのタスクの順番を変えることが有益であると判断することがある。[47] 以下に記載されているタスクに対して組織がいかなる調整を行ったとしても、リスクアセスメントは、アセスメントを開始する組織によって定められた目的、適用範囲、想定、および制限を満たさなければならない。本文書では、組織によるリスクアセスメントプロセス内の個々の

[46] たとえば、脆弱性が特定されるにつれて、新たに特定されたそれらの脆弱性がどのように利用されうるかといった質問に答えることによって、追加の脅威事象が特定される可能性がある。組織が、先に脆弱性を特定し、その後、脅威事象を定義する場合、脆弱性にはうまく対応付けることができず、素因的条件に対応付けられる事象もあるだろう。

[47] たとえば、リスクアセスメントは、ミッションへの影響分析(Mission Impact Analyses)、ビジネス影響分析(Business Impact Analyses)、ミッション／業務のスレッド分析(Mission/Business Thread Analyses)、または業務継続分析(Business Continuity Analyses)などの共通の技法を使用した、第 1 層と第 2 層におけるミッション／業務の影響の特定から始めることができる。そうした分析の結果により、リスクアセサーは、基幹業務に関わる情報システム、データベース、通信リンク、あるいはその他の資産に対する潜在的脅威に焦点を絞り、より詳細な分析を実施することが可能になる。

タスクの実施を支援するために、付録 D から I にかけて一連のテンプレートが示されている。これらの付録は、リスクをアセスメントする組織にとって有用な情報を提供し、極めて重要な計算および分析において生成されたアセスメント結果を記録するのに使用することができる。これらのテンプレートは例であり、組織の具体的なミッション／業務上の要求事項に応じて、組織によって調整される可能性がある。これらのテンプレートの使用が、リスクアセスメントの実施に必ずしも必要であるわけではない。

ステップ 2:リスクアセスメントの実施

脅威源を特定する

タスク 2-1: 懸念される脅威源（アドバーサリによる脅威の場合には、アドバーサリの能力、意図、および標的を含み、アドバーサリによるもの以外の脅威の場合には、影響の範囲を含む）を特定し、特徴を定義する。

補足の手引き: 組織は、懸念される脅威源を特定し、それらの脅威源の特徴を特定する。アドバーサリによる脅威源の場合には、その脅威源の能力、意図、および標的をアセスメントする。アドバーサリによるもの以外の脅威源の場合には、それらの脅威源がもたらす影響の範囲をアセスメントする。リスクマネジメント戦略および「アセスメントの準備」ステップの結果は、たとえば以下を含む、脅威源の特定と特徴定義を実施するうえでの組織の方向性と手引きを用意する：(i) 脅威関連情報を得るための情報源; (ii) 考慮すべき脅威源（タイプ／名前別）; (iii) 使用される脅威の分類体系; ならびに (iv) リスクアセスメントにとって、どの脅威源が懸念されるかを特定するためのプロセス。タスク 1-3 で特定されたように、組織は、具体的で信頼できる脅威関連情報を得られない場合には、脅威源の特定に関する意思決定を含む、脅威源に関するあらゆる想定を明確にする。組織は、また、アドバーサリによる脅威源について、そうした脅威源が特定された組織の脆弱性を利用するために有する時間や、攻撃の規模、および複数の攻撃ベクトルの使用の可能性を考慮しながら、幅広い観点から捉えることができる。APT(Advanced Persistent Threat)の特定と特徴定義は、かなりの不確実性を伴う場合がある。組織は、そうした脅威源について、適切な根拠と参照（必要に応じて分類体系も示す）と共に注記する。

付録 D は、脅威源の特定に使用できる表の例を示している：

- 表 D-1 は、「脅威源の特定」タスクに対する入力データの例を示している。
- 表 D-2 は、脅威源の特定と特徴定義に使用できる、分類体系の例を示している。
- 表 D-3、D-4 および D-5 は、アドバーサリによる脅威源のリスク因子（すなわち、特徴）を能力、意図、および標的の観点からアセスメントするための、アセスメントスケールの例を示している。
- 表 D-6 は、アドバーサリによるもの以外の脅威源によって開始された脅威事象がもたらす影響の範囲をアセスメントするための、アセスメントスケールの例を示している。
- 表 D-7 および D-8 は、脅威源の特定と特徴定義の結果を要約し、文書化するためのテンプレートを示している。

特定のタイプの脅威源が、リスクアセスメントの適用範囲外である場合、あるいは、組織に関連しない場合には、表 D-7 と D-8 の情報は切り捨ててよい。タスク 2-1 において生成された情報は、付録 I のリスク表に対して、脅威源関連の入力データを提供する。

主要な活動の要約 – タスク2-1

- 脅威源関連の入力データを特定する（**表 D-1** を参照：組織によって調整される）。
- 脅威源を特定する（**表 D-2** を参照：組織によって調整される）。
- 脅威源が、その組織に関連し、適用範囲内であるか否かを特定する（**表 D-1** を参照：組織によって調整される）。
- 脅威源のアセスメント結果を作成する、または更新する（アドバーサリによる脅威源の場合には**表 D-7** を参照し、アドバーサリによるもの以外の脅威源の場合には**表 D-8** を参照：組織によって調整される）。
  - 関連する、アドバーサリによる脅威源の場合：
    - アドバーサリの能力をアセスメントする（**表 D-3** を参照：組織によって調整される）。
    - アドバーサリの意図をアセスメントする（**表 D-4** を参照：組織によって調整される）。
    - アドバーサリの標的をアセスメントする（**表 D-5** を参照：組織によって調整される）。
  - 関連する、アドバーサリによるもの以外の脅威源の場合：
    - 脅威源がもたらす影響の範囲をアセスメントする（**表 D-6** を参照：組織によって調整される）。

脅威事象を特定する

TASK 2-2: 起こりうる脅威事象、それらの事象間の関連性、およびそれらの事象を開始する可能性のある脅威源を特定する。

補足の手引き: 脅威事象は、それらの事象を開始する可能性のある脅威源によって、さらにアドバーサリによる脅威源の場合には、攻撃の実施に使用される戦術、技法、手順によっても、その特徴が定義される。組織は、リスクアセスメントの目的を果たすために、十分な詳細さをもってこれらの脅威事象を定義する。第 1 層において、組織レベルに影響を及ぼす脅威事象は、特に注意が必要である。第 2 層において、情報システムの境界を超える(または境界に跨る)脅威事象、システム間の機能面での依存関係または接続性を利用する脅威事象、あるいはミッション／業務遂行の責任者に影響を及ぼす脅威事象は、特に注意が必要である。第 3 層において、特定の情報システム、技術、または運用環境の観点から述べることができる脅威事象は、特に注意が必要である。複数の脅威源が、単一の脅威事象を開始する場合がある。反対に、単一の脅威源が、場合によっては、複数の脅威事象を開始する可能性がある。したがって、脅威事象と脅威源の間には、多対多関係が存在しうる。この場合、リスクアセスメントの複雑さが増大する。リスクアセスメント結果の効果的な利用と伝達を可能にするために、組織は、表 E-2 と E-3 の脅威事象の概要を調整し、それぞれの事象が組織の業務(ミッション、機能、イメージ、または評判を含む)と資産、個人、他の組織、または国家にどのように被害をもたらすかについて特定する。特定されたそれぞれの脅威事象について、組織は、それらの事象間の関連性を特定する。表 E-4 は、脅威事象間の関連性に対する範囲値を示している。組織によって選択された値は、組織のリスク許容度に対して直接的なつながりを有する。リスクを嫌うほど、考慮される範囲値も大きくなる。より大きなリスクを許容する組織、あるいはリスク許容度がより大きい組織では、脅威事象について真剣に検討する前に、実質的な証拠を求める可能性が高い。ある脅威事象が問題とされないと判断された場合には、さらなる検討はなされない。問題とされる脅威事象について、組織は、それらの事象を開始する可能性のあるあらゆる脅威源を特定する。タスク 2-4 での使用のために、組織は、脅威源と脅威事象のそれぞれの組み合わせを個別に特定してもよい。なぜならば、脅威が開始され、成功裏に終わる可能性は、組み合わせごとに異なる可能性があるからである。別の選択肢として、組織は、ある脅威事象を開始する可能性のある、あらゆる脅威源の一式を特定してもよい。

付録 E は、脅威事象の特定に使用できる表の例を示している:

- 表 E-1 は、「脅威事象の特定」タスクへの入力データの例を示している。
- 表 E-2 は、アドバーサリによる脅威事象の代表的な例を、戦術、技法、手順の形式で示している。
- 表 E-3 は、アドバーサリによるもの以外の脅威事象の代表的な例を示している。
- 表 E-4 は、組織に対する脅威事象間の関連性に割り当てられる値の例を示している。
- 表 E-5 は、脅威事象の特定結果を要約し、文書化するためのテンプレートを示している。

タスク 2-2 で生成された情報は、付録 I のリスク一覧に対して、脅威事象関連の入力データを提供する。

主要な活動の要約 – タスク 2-2

- 脅威事象関連の入力データを特定する(**表 E-1** を参照:組織によって調整される)。
- 脅威事象を特定する(アドバーサリによる脅威事象の場合には**表 E-2** を参照し、アドバーサリによるもの以外の脅威事象の場合には**表 E-3** を参照:組織によって調整される)。**表 E-5** を作成する、あるいは更新する。
- 脅威事象を開始する可能性のある脅威源を特定する(**表 D-7** と**表 D-8** を参照:組織によって調整される)。**表 E-5** を更新する。
- 組織に対する脅威事象間の関連性をアセスメントする (**表 E-4** を参照:組織によって調整される)。**表 E-5** を更新する。
- アドバーサリによるリスクの場合、**表 I-5** の「1-6」の欄を更新する(**表 E-5** と**表 D-7** を参照)。アドバーサリによるもの以外のリスクの場合、**表 I-7** の「1-4」の欄を更新する (**表 E-5** と**表 D-8** を参照)。

脆弱性と素因的条件を特定する

タスク 2-3: 懸念される脅威事象が負の影響をもたらす可能性に影響を及ぼす脆弱性と素因的条件を特定する。

補足の手引き: 脆弱性アセスメントの主要な目的は、タスク 2-1 で特定された脅威源と、タスク 2-2 で特定されたそれらの脅威源によって開始される可能性のある脅威事象に対して、組織、ミッション／業務プロセスおよび情報システムがどのように、かつ、どの程度脆弱であるかを理解することにある。第 1 層における脆弱性は、組織全体に広がる可能性があり、脅威事象によって利用された場合、広範囲にわたる負の影響を及ぼす可能性がある。たとえば、組織がサプライチェーン活動について考慮しなかったために、アドバーサリが組織のミッション／業務機能を中断させるために、あるいは組織の機微な情報を得るために利用できる腐敗したコンポーネントを、組織が取得する結果になることが考えられる。第 2 層における脆弱性は、組織のミッション／業務プロセス、エンタープライズアーキテクチャ、複数の情報システムの使用、あるいは共通インフラ／共有サービスの観点から記述できる。第 2 層において、脆弱性は、通常、情報システムの境界を超える（または境界に跨る）。第 3 層における脆弱性は、組織の情報システム内で使用されている情報技術、それらのシステムが稼働する環境、および／またはシステム固有のセキュリティ管理策の欠如または弱点の観点から記述できる。脅威事象と脆弱性の間には、多対多関係が存在しうる。複数の脅威事象が単一の脆弱性を利用したり、反対に、複数の脆弱性が単一の脅威事象によって利用される可能性がある。脆弱性の重大さは、その脆弱性を軽減することの相対的重要性をアセスメントした結果である。初期の段階では、軽減がどの程度計画されていないかが、脆弱性の重大さの代わりとなる。特定の脆弱性に伴うリスクがアセスメントされた後は、実施されているセキュリティ管理策と、その他の脆弱性を考慮した上での影響の重大さと脆弱性への露出が、脆弱性の重大さのアセスメントにおいて考慮される。脆弱性の重大さのアセスメントは、リスク対応を支援する。脆弱性は、さまざまなレベルの細かさと具体さをもって特定することができる。特定の脆弱性アセスメントが提供する詳細レベルは、リスクアセスメントの目的と、以降の「発生可能性と影響の特定」を支援するのに必要な入力データのタイプとの一貫性を保つ。

組織、ミッション／業務プロセス、およびそれらのプロセスを支援する情報システムの規模と複雑さが増加の一途をたどっているため、脆弱性の数も増加する傾向にあり、故に分析の全体的な複雑さも増加すると考えられる。したがって、組織は、アセスメントに関連する、脆弱性の一般的な性質（範囲、数、およびタイプを含む）を理解するために、「脆弱性の特定」タスクを使用し（ タスク 1-3 を参照）、必要に応じて具体的な脆弱性の目録を作成することを選択できる。組織は、アセスメントすべきリスクの空間を小さくするために、どの脆弱性がどの脅威事象に関連するかを特定する。脆弱性の特定に加えて組織は、特定の脆弱性に対する脆弱さを左右するあらゆる素因的条件を特定する。組織（ミッション／業務プロセス、情報システム、および運用環境を含む）内に存在する素因的条件は、脅威源によって開始された単一の、あるいは複数の脅威事象が組織の業務、組織の資産、個人、他の組織、または国家に負の影響をもたらす可能性に影響を及ぼす（すなわち、その可能性を増加／減少させる）。組織は、アセスメントすべきリスクの空間を小さくするために、どの素因的条件がどの脅威事象に関連するかを特定する。組織は、どの層におけるリスク対応が最も効果的であるかについての決定を支援するために、素因的条件の広がりをアセスメントする。

付録 F は、脆弱性と素因的条件の特定に使用できる表の例を示している:

- 表 F-1 は、「脆弱性と素因的条件の特定」タスクへの入力データの例を示している。
- 表 F-2 は、特定された脆弱性の重大さをアセスメントするための、アセスメントスケールの例を示している。
- 表 F-3 は、脆弱性の特定結果を要約し、文書化するためのテンプレートを示している。
- 表 F-4 は、素因的条件の特定と特徴定義に使用できる分類体系の例を示している。
- 表 F-5 は、素因的条件の広がりをアセスメントするための、アセスメントスケールの例を示している。
- 表 F-6 は、素因的条件の特定結果を要約し、文書化するためのテンプレートを示している。

タスク 2-3 で生成された情報は、付録 I のリスク一覧に対して、脆弱性および素因的条件に関連する入力データを提供する。

主要な活動の要約 – タスク 2-3

- 脆弱性および素因的条件に関連する入力データを特定する(**表 F-1** を参照:組織によって調整される)。
- 組織が定めた情報源を使用して、脆弱性を特定する。**表 F-3** を作成する、あるいは更新する。
- 特定された脆弱性の重大さをアセスメントする(**表 F-2** を参照:組織によって調整される)。**表 F-3** を更新する。
- 素因的条件を特定する(**表 F-4** を参照:組織によって調整される)。**表 F-6** を作成する、あるいは更新する。
- 素因的条件の広がりをアセスメントする(**表 F-5** を参照:組織によって調整される)。**表 F-6** を更新する。
- アドバーサリによるリスクの場合、**表 I-5** の「8」の欄を更新する。アドバーサリによるもの以外のリスクの場合、**表 I-7** の「6」の欄を更新する(**表 F-3** と**表 F-6** を参照)。
- アドバーサリによるリスクの場合、**表 I-5** の「9」の欄を更新する。アドバーサリによるもの以外のリスクの場合、**表 I-7** の「7」の欄を更新する(**表 F-2** と**表 F-5** を参照)。

可能性を特定する

タスク 2-4: 懸念される脅威事象が負の影響をもたらす可能性について、以下を考慮しながら特定する:(i) それらの事象を開始する可能性のある脅威源の特徴; (ii) 特定された脆弱性／素因的条件; ならびに (iii) そうした事象を阻止するために導入が計画されている、あるいは導入されている保護手段／対策を反映する、そうした事象に対する組織の脆弱さ。

補足の手引き: 組織は、脅威事象の総合的な可能性を特定するために、3 段階のプロセスを使用する。第 1 に、組織は、アドバーサリによる脅威事象の場合に、脅威事象が開始される可能性をアセスメントし、アドバーサリによるもの以外の脅威事象の場合に、脅威事象が発生する可能性をアセスメントする。第 2 に、組織は、一度開始された、あるいは発生している脅威事象が組織の業務と資産、個人、他の組織、または国家に負の影響をもたらす可能性をアセスメントする。最後に、組織は、開始／発生の可能性と、負の影響がもたらされる可能性の組み合わせである、総合的な可能性をアセスメントする。

組織は、懸念される脅威源の特徴(能力、意図、および標的を含む)を考慮に入れながら、脅威事象の開始の可能性をアセスメントする(タスク 2-1 と付録 D を参照)。脅威事象がアドバーサリが有する能力よりも高い能力を要する場合で、かつ、アドバーサリがこの事実を認識している場合には、アドバーサリが当該事象を開始するとは思えない。脅威事象を実行しても意図した目的を果たすことができないとアドバーサリが判断した場合には、アドバーサリが当該事象を開始するとは思えない。そして最後に、アドバーサリが特定の組織または組織のミッション／業務機能を積極的に狙っていない限り、アドバーサリが当該事象を開始するとは思えない。組織は、表 G-2 のアセスメントスケールを使用して、抑止と脅威シフトについての明確な考慮を可能にするアセスメントの根拠を示す。アドバーサリによるもの以外の脅威事象の場合には、表 G-3 を使用して、脅威事象の発生の可能性をアセスメントし、そのアセスメントの根拠を示すことができる。

組織は、特定された脆弱性と素因的条件を考慮に入れて、脅威事象が負の影響をもたらす可能性をアセスメントする(タスク 2-3 と付録 F を参照)。アドバーサリによって開始された脅威事象の場合、組織は、関連する脅威源の特徴を考慮する。アドバーサリによるもの以外の脅威事象の場合、組織は、当該事象の重大さと継続期間の推定(これらは、当該事象についての記述に含まれる)を考慮に入れる。組織は、表 G-4 のアセスメントスケールを使用して、上記のように明確な考慮を可能にするアセスメントの根拠を示す。脆弱性または素因的条件が特定されない脅威事象は、負の影響をもたらす可能性は極めて低い。そうした脅威事象は、後続のリスクアセスメントにおいて考慮がなされるよう、強調表示され、表の最後に(あるいは、別の表に)に移動される可能性がある。しかしながら、現行のアセスメントにおいては、さらなる考慮は必要でない。

脅威事象の総合的な可能性は、以下の項目の組み合わせである：(i) 当該事象が発生する可能性（例：人的ミスまたは自然災害）、あるいはアドバーサリによって開始される可能性; ならびに (ii) その開始／発生が負の影響をもたらす可能性。組織は、表 G-2、G-3 および G-4 の入力データを使用して、脅威事象の総合的な可能性をアセスメントする。決定された発生可能性の値を結合するための具体的なアルゴリズムまたはルールは、以下に依存する：(i) リスクに対する組織の全体的な姿勢（総合的なリスク許容度と、不確実性に対する許容度を含む）; (ii) 異なるリスク因子における不確実性に対する具体的な許容度; ならびに (iii) 組織による、リスク因子の重み付け。たとえば、組織は、以下のルールのいずれかを使用できる（あるいは、異なるルールを定義することができる）：(i) 二つの可能性の値の最大値を使用する; (ii) 二つの可能性の値の最小値を使用する; (iii) 脅威事象が開始された（または発生した）場合に、その事象が負の影響をもたらすと想定した上で、開始／発生の可能性のみを考慮する; (iv) 脅威事象が負の影響をもたらすことが可能ならば、アドバーサリがその事象を開始すると想定した上で、影響の発生可能性のみを考慮する; あるいは (v) 二つの可能性の値の重み付けの平均を使用する。組織は、使用されるルールを明確にする。

付録 G は、脅威事象の発生可能性の特定に使用できる表の例を示している：

- 表 G-1 は、「発生可能性の特定」タスクへの入力データの例を示している。
- 表 G-2 は、アドバーサリによる脅威事象の開始の可能性をアセスメントするための、アセスメントスケールの例を示している。
- 表 G-3 は、アドバーサリによるもの以外の脅威事象の発生の可能性をアセスメントするための、アセスメントスケールの例を示している。
- 表 G-4 は、脅威事象が開始された（アドバーサリによる場合）または発生した（アドバーサリによるもの以外の場合）場合に、それらの事象が負の影響をもたらす可能性をアセスメントするための、アセスメントスケールの例を示している。
- 表 G-5 は、脅威事象の総合的な可能性（すなわち、開始／発生の可能性と、影響がもたらされる可能性の組み合わせ）をアセスメントするための、アセスメントスケールの例を示している。

タスク 2-4 で生成された情報は、付録 I のリスク一覧に対して、脅威事象の発生可能性関連の入力データを提供する。

主要な活動の要約 – タスク 2-4

- 発生可能性の特定関連の入力データを特定する（**表 G-1** を参照：組織によって調整される）。
- 組織が定めた情報源を使用して発生可能性の特定にかかわる因子を特定する（例：脅威源の特徴、脆弱性、素因的条件）。
- アドバーサリによる脅威の場合、脅威事象の開始の可能性をアセスメントし、アドバーサリによるもの以外の脅威の場合、脅威事象の発生の可能性をアセスメントする（**表 G-2** と 表 **G-3** を参照：組織によって調整される）。
- 開始または発生の可能性がある場合に、脅威事象が負の影響をもたらす可能性をアセスメントする（表 **G-4** を参照：組織によって調整される）。
- 脅威事象の開始／発生の総合的な可能性と、脅威事象が負の影響をもたらす可能性をアセスメントする（表 **G-5** を参照：組織によって調整される）。
- アドバーサリによるリスクの場合、**表 I-5** の「7」、「10」、および「11」の欄を更新する（**表 G-2**、**表 G-4**、および**表 G-5** を参照）。アドバーサリによるもの以外のリスクの場合、**表 I-7** の「5」、「8」、および「9」の欄を更新する（**表 G-2**、**表 G-4**、および表 **G-5** を参照）。

影響を特定する

タスク 2-5: 懸念される脅威事象がもたらす負の影響を、以下を考慮しながら特定する：(i) それらの事象を開始する可能性のある脅威源の特徴; (ii) 特定された脆弱性／素因的条件; ならびに (iii) そうした事象を阻止するために導入が計画されている、あるいは導入されている保護手段／対策を反映する、そうした事象に対する組織の脆弱さ。

補足の手引き: 組織は、組織の業務と資産、個人、他の組織、または国家に対してもたらされる可能性のある被害の観点から、負の影響について記述する。脅威事象がどこで発生し、その事象の影響が封じ込められるか、あるいは広がるかは、影響の重大さを左右する。影響のアセスメントは、脅威事象の影響を受ける可能性のある情報資源（例：情報、データリポジトリ、情報システム、アプリケーション、情報技術、通信リンク）、従業員、および物理的な資源（例：建物、電力供給装置）を含む、資産または脅威源の標的の特定を伴う。組織的影響は、第 1 層と第 2 層において定義され、優先順位付けがなされ、「リスクのフレーム化」の一環として第 3 層に伝達される。第 3 層において、影響は、侵害される可能性のある情報システムの能力（例：処理、表示、通信、格納、および取り出し）と資源（データベース、サービス、コンポーネント）に対応付けらえる。

付録 H は、負の影響の特定に使用できる表の例を示している：

- 表 H-1 は、「影響の特定」タスクへの入力データの例を示している。
- 表 H-2 は、組織の業務と資産、個人、他の組織、および国家に対する被害に焦点を当てた、組織に対する負の影響の代表的な例を示している。
- 表 H-3 は、脅威事象がもたらす影響をアセスメントするための、アセスメントスケールの例を示している。
- 表 H-4 は、負の影響を要約し、文書化するためのテンプレートを示している。

タスク 2-5 で生成された情報は、付録 I のリスク一覧に対して、負の影響に関連する入力データを提供する。

主要な活動の要約 – タスク 2-5

- 影響の特定関連の入力データを特定する（**表 H-1** を参照：組織によって調整される）。
- 組織が定めた情報源を使用して影響の特定にかかわる因子を特定する。
- 負の影響と、影響を受ける資産を特定する（**表 H-2** を参照：組織によって調整される）。**表 H-4** を作成する、あるいは更新する。
- 影響を受ける資産に関連する最大の影響をアセスメントする。（**表 H-3** を参照：組織によって調整される）。**表 H-4** を更新する。
- アドバーサリによるリスクの場合、**表 I-5** の「12」の欄を更新する。アドバーサリによるもの以外のリスクの場合、**表 I-7** の「10」の欄を更新する。

リスクを判断する

タスク 2-6: 懸念される脅威事象が組織にもたらすリスクを、以下を考慮しながら特定する：(i) それらの事象がもたらす影響; ならびに (ii) それらの事象が発生する可能性。

補足の手引き: 組織は、発生可能性と影響の組み合わせである、脅威事象がもたらすリスクをアセスメントする。特定された脅威事象に伴うリスクのレベルは、そうした事象によって組織が脅かされる度合を示す。組織は、リスクの判断における不確実性を明確にする。これは、たとえば、組織の想定と主観的な判断／決定を含む。組織は、リスクアセスメント時に特定されたリスクのレベルごとに、懸念される脅威事象の一覧を順序付けることができる（この際、リスクが高い事象に最大の注意が払われるように順序付けが行われる）。組織は、同じレベルで、あるいは類似のスコアでリスクのさらなる優先順位付けを行うことができる。（付録 J を参照）。それぞれのリスクは、特定の脅威事象に対応し、その対応付けは、脅威事象が発生した場合の影響のレベルにもとづいて行われる、。通常、リスクレベルが影響レベルを上回ることはない。また、発生可能性は、リスクが影響レベルを下回るまでリスク軽減するのに役立つ。しかしながら、多数のミッション／業務機能、ミッション／業務プロセス、および支援情報システムを抱える組織の、組織全体にわたるリスクマネジメント上の問題に対処する際には、リスクの上限としての影響が適用されない可能性がある。たとえば、複数のリスクが顕在化した場合、それぞれのリスクが中間レベルであったとしても、それらの中間レベルリスクが集まることによって、組織に対する、より高いレベルのリスクに発展する可能性がある。被害が複数回にわたって発生する状況に対処するには、被害が複数回にわたって発生することと、累積された被害の大きさに対応する影響レベルの組み合わせを、脅威事象として定義することができる。タスク 2-1 からタスク 2-5 まで実施中に、組織は、リスクアセスメントにおける不確実性に関する重要な情報を取り込む。これらの不確実性は、不明情報、主観的な判断、および行われる想定などの情報源から発生する。リスクアセスメント結果の有効性は、その一部が、アセスメントの一環として行われる想定の継続的な適用性について意思決定者が判断できるか否かによって

決まる。不確実性に関する情報は、十分な情報を得た上でのリスクマネジメントに関する意思決定をすぐに支援できるような形で編集され、提示される。

付録 I は、リスクの判断に使用できる表の例を示している:

- 表 I-1 は、「リスクと不確実性の判断」タスクへの入力データの例を示している。
- 表 I-2 と I-3 は、リスクのレベルをアセスメントするための、アセスメントスケールの例を示している。
- 表 I-4 と I-6 は、アドバーサリによる脅威事象と、アドバーサリによるもの以外による脅威事象のそれぞれについて、リスクの判断に使用される主なデータ要素の見出しについての記述である。
- 表 I-5 と I-7 は、アドバーサリによる脅威事象と、アドバーサリによるもの以外による脅威事象のそれぞれについて、リスクの判断に使用される主なデータ要素を要約し、文書化するためのテンプレートを示している。

タスク 2-6 で生成された情報は、付録 I のリスク一覧に対して、リスク関連の入力データを提供する。

主要な活動の要約 – タスク 2-6

- リスクと不確実性の判断関連の入力データを特定する(**表 I-1** を参照:組織によって調整される)。
- リスクを判断する(**表 I-2** と**表 I-3** を参照:組織によって調整される)。アドバーサリによるリスクの場合、**表 I-5** の「13」の欄を更新する。アドバーサリによるもの以外のリスクの場合、**表 I-7** の「11」の欄を更新する。

3.3 リスクアセスメント情報の伝達と共有

リスクアセスメントプロセスの 3 番目のステップは、アセスメント結果の伝達と、リスク関連情報の共有である。[48] このステップの目的は、組織全体にわたる意思決定者が、リスク判断に情報を提供し、そうした判断を導くのに必要な適切なリスク関連情報を有することを確実にすることにある。情報の伝達と共有は、以下の具体的なタスクによって構成される:

- リスクアセスメント結果を伝達する。
- 他のリスクマネジメント活動を支援するために、リスクアセスメントを実行して得られた情報を共有する。

ステップ 3:リスクアセスメント結果の伝達と共有

リスクアセスメント結果を伝達する

タスク 3-1: リスク対応を支援するために、リスクアセスメント結果を組織の意思決定者に伝達する。

補足の手引き: 組織は、リスクアセスメント結果をさまざまな方法で伝達することができる(例:管理職者による概要報告、リスクアセスメント報告、ダッシュボード)。そうしたリスク伝達は、フォーマルな場合と、インフォーマルな場合があるが、その内容と形式は、アセスメントを開始し実施する組織によって決定される。組織は、「リスクアセスメントの準備」の一環として含まれる、リスク伝達および報告に関する具体的な要求事項に関する手引きを用意する(ただし、「リスクのフレーム化」タスクの一環として、リスクマネジメント戦略に含まれる場合を除く)。組織は、同じレベルで、あるいは類似のスコアでリスクの優先順位付けを行う。(付録 J を参照)。付録 K は、リスクアセスメント報告に含まれる可能性のある情報の例や、推奨されるリスク伝達手段を示している。

リスク関連情報を共有する

タスク 3-2:リスクアセスメントにおいて生成されたリスク関連情報を、組織の適切な職員と共有する。

補足の手引き: 組織は、ソース情報と中間結果を共有し、リスク関連情報の共有に関する手引きを用意する。情報共有は、報告や概要報告によって、かつ、リスクアセスメント結果を裏付ける証拠をもってリスク関連データのリポジトリを更新することによって、主に組織内で発生する。情報共有は、情報源、分析プロセス、および中間結果(例:付録 D から I までの完結した一覧表)を文書化することによっても、支援され、これによりリスクアセスメントを容易に保守することが可能になる。情報共有は、他の組織との間でも発生する。

主要な活動の要約 – 情報の伝達と共有

- リスクアセスメント結果を伝達するための適切な方法を特定する (例:管理職者による概要報告、リスクアセスメント報告、またはダッシュボード)。
- 組織の指定された利害関係者にリスクアセスメント**結果**を伝達する。
- 組織のポリシーと手引きに従って、**リスクアセスメント結果**と、結果を裏付ける証拠を共有する。

[48] リスクアセスメントプロセスは、アセスメント活動を実施する職員、本件に関する専門家、および組織の主な利害関係者(例:ミッション/業務遂行の責任者、リスクエグゼクティブ(機能)、最高情報セキュリティ責任者、情報システム所有者/導入計画管理者)との間の、継続的なコミュニケーションと情報共有を伴う。このコミュニケーションと情報共有は、以下を確実にする:(i) リスクアセスメントに対する入力データが最大限に正確であること; (ii) 中間のアセスメント結果を使用できること(例:他の層におけるリスクアセスメントを支援するために); ならびに (iii) 結果がリスク対応に対する有意かつ有用な入力データとなること。

3.4 リスクアセスメントの保守

リスクアセスメントプロセスの 4 番目のステップは、アセスメントの保守である。このステップの目的は、組織が被るリスクについての具体的な知識を最新に保つことにある。リスクアセスメントの結果は、リスクマネジメントに関する意思決定に情報を提供し、リスク対応を導く。リスクマネジメントに関する意思決定（例：調達に関する意思決定、情報システムと共通管理策の運用認可に関する意思決定、接続に関する意思決定）の継続的なレビューを支援するために、組織は、リスクアセスメントを保守し、「リスクのモニタリング」を介して検出されたあらゆる変更を組み入れる。[49]「リスクのモニタリング」は、組織に対して、以下を継続的に行うための手段を提供する: (i) リスク対応の有効性を判断する; (ii) 組織の情報システム、およびそれらのシステムが稼働する環境に対する変更の内、リスクに影響を及ぼす変更を特定する [50] ; ならびに (iii) 遵守状況を確認する。[51] リスクアセスメントの保守は、以下の具体的なタスクを含む：

- リスクアセスメントにおいて特定されたリスク因子を継続的にモニタリングし、それらの因子に対する後の変更を把握する。
- 組織によって実施されるモニタリング活動を反映する形で、リスクアセスメントのコンポーネントを更新する。

ステップ 4:リスクアセスメントの保守

リスク因子をモニタリングする

タスク 4-1: 組織の業務と資産、個人、他の組織、または国家に対するリスクの変化の一因となるリスク因子に対する、継続的なモニタリングを実施する。

補足の手引き: 組織は、信頼できる、リスクにもとづく意思決定を行うのに必要な情報を長期にわたって得られるよう、重要なリスク因子を継続的にモニタリングする。リスク因子（例：脅威源と脅威事象、脆弱性と素因的条件、アドバーサリの能力と意図、標的となっている組織の業務、資産、または個人）のモニタリングは、主要なミッション／業務機能を実施するための組織の能力に影響を及ぼしうる条件の変更についての、極めて重要な情報を提供する。リスク因子の継続的なモニタリングから導出された情報は、頻度にかかわらず、リスクアセスメントをリフレッシュするために使用できる。組織が、リスクアセスメントの現在性を維持するために、リスク対応策の有効性に対する変化を捉えることを試行することも考えられる。その目的は、組織のガバナンス構造および活動、ミッション／業務プロセス、情報システム、ならびに運用環境、さらには組織が被るリスクに影響を及ぼしうるすべてのリスク因子に対する現行の状況認識を維持することにある。したがって、そのリスクアセスメントのコンテクストまたはリスクフレーム（すなわ

[49] リスクマネジメントプロセスの 4 番目のステップである「リスクのモニタリング」については、NIST SP 800-39 に記載されている。アセスメント結果を保守するための、リスクアセスメントプロセス内の本ステップは、時間が経過するにつれ、リスクマネジメントプロセス内の「リスクのモニタリング」ステップおよびリスクマネジメントフレームワーク内の「継続的なモニタリング」ステップと、ある程度重なる。この重なりは、リスクマネジメントプロセス内の活動の多くが補完的であり、互いに補強し合うといった重要な概念が強調される。たとえば、リスクマネジメントフレームワーク内の「継続的なモニタリング」ステップは、導入されているセキュリティ管理策の現在の有効性をモニタリングするために使用でき、その結果は、より広範囲に及ぶ組織のリスクモニタリングプロセスに情報を提供し、そうしたプロセスを導くために使用される。組織レベルでは、リスクのモニタリングは、後続のリスクアセスメントを実施するのに必要な主要なリスク因子のモニタリングを含む場合がある。組織は、リスクマネジメント戦略を使用して、リスクアセスメントを保守するための主要な要求事項を伝達する。そうした要求事項は、たとえば、モニタリングすべきリスク因子と、そうしたモニタリングの頻度を含む。

[50] NIST SP 800-137 は、組織の情報システムおよび運用環境の継続的なモニタリングに関する手引きである。

[51] 遵守状況の確認は、必要なリスク対応策を組織が実施していて、かつ、組織のミッション／業務機能、連邦法、指令、規制、ポリシー、および標準／ガイドラインから導出され跡をたどることができる情報セキュリティ要求事項が満たされているか否かを確認する。

ち、適用範囲、目的、想定、制限、リスク許容度、優先順位、およびトレードオフ）を適用する際に、組織は、実行されるリスク対応計画においてリスク因子が果たす役割についいて考慮する。たとえば、情報システムのセキュリティ体制（すなわち、それらのシステム内で測定されるリスク因子）は、組織のリスク対応の一部しか反映しないといったことが、よく見受けられる。このような場合には、組織レベルまたはミッション／業務プロセスレベルでの対応活動が、そうした対応のかなりの部分を提供することになる。そうした状況では、情報システムのセキュリティ体制のみをモニタリングした場合、組織が被る総合的なリスクを判断するための十分な情報が提供されないだろう。高い能力と十分な資源を備えた、目的を持つ脅威源は、一般に入手可能な保護メカニズムを打ち負かせると考えらえる（例：そうしたメカニズムを迂回する、または不正に変更することによって）。したがって、情報システムが侵害された場合のプロセスレベルのリスク対応策（ミッション／業務プロセスを設計し直すこと、情報技術を賢明に活用すること、代替えの実行プロセスを使用することなど）は、組織のリスク対応計画の重要な要素となりうる。

リスクアセスメントを更新する

タスク 4-2: リスク因子の継続的なモニタリングの結果を使用して、既存のリスクアセスメントを更新する。

補足の手引き: 組織は、リスクアセスメントの更新の頻度と、更新が必要な状況について決定する。そうした決定は、たとえば、組織の主要なミッション／業務機能に対する現行のリスクレベル、および／またはそれらの機能の重要性を含む。リスクアセスメントが実施されてから（組織のポリシー、指令、または手引きによって定義されているように）大幅な変更が発生した場合、組織は、アセスメントの目的、適用範囲、想定、および制限に再訪し、リスクアセスメントプロセス内のすべてのタスクを繰り返す必要があるか否かを判断する。さもなければ、更新は、選択されたリスク因子がどのように変化したかを特定しアセスメントするための、後続のリスクアセスメントによって構成される。これは、たとえば、(i) 新たな脅威イベント、脆弱性、素因的条件、望ましくない結果および／または影響を受けた資産の特定; ならびに (ii) 脅威源の特徴（例：能力、意図、標的、影響の範囲）、発生可能性、および影響のアセスメント。組織は、組織の責任者が、リスクにもとづく判断を継続的に行うのに必要な情報にアクセスできるよう、後続のリスクアセスメントの結果をリスクマネジメント階層内のすべての層のエンティティ（部署、人）に伝達する。

主要な活動の要約 – リスクアセスメントの保守

- 継続的なモニタリングの対象として特定された**リスク因子**を特定する。
- リスク因子のモニタリング活動の**頻度**と、リスクアセスメントの更新が必要となる**状況**を特定する。
- リスクアセスメントの**目的**、**適用範囲**、および**想定**を再確認する。
- 必要に応じて、リスクアセスメントの適切な**タスク**を実施する。
- 後続のリスクアセスメントの**結果**を指定された組織の職員に伝達する。

付録 A

参考文献

法律、ポリシー、指令、指示、標準およびガイドライン

法律

1. E-Government Act [includes FISMA] (P.L. 107-347), 2002 年 12 月.
2. Federal Information Security Management Act (P.L. 107-347, Title III), 2002 年 12 月.

ポリシー、指令、指示

1. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, 2000 年 11 月.
2. Committee on National Security Systems Instruction (CNSSI) No. 4009, *National Information Assurance (IA) Glossary*, 2010 年 4 月.
3. Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*, 2012 年 3 月.
4. Department of Homeland Security Federal Continuity Directive 2 (FCD 2), *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, 2008 年 2 月.

標準

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004 年 2 月.
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006 年 3 月.
3. ISO/IEC 31000:2009, *Risk management – Principles and guidelines*.
4. ISO/IEC 30101:2009, *Risk management – Risk assessment techniques*.
5. ISO/IEC Guide 73, *Risk management – Vocabulary*.
6. ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.

ガイドライン

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, 2006 年 2 月.
2. National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, 2010 年 5 月.
3. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 2010 年 2 月.

4. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, 2011 年 3 月.

5. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, 2009 年 8 月.

6. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, 2010 年 6 月.

7. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, 2003 年 8 月.

8. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, 2008 年 8 月.

9. National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, 2008 年 10 月.

10. National Institute of Standards and Technology Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, 2005 年 1 月.

11. National Institute of Standards and Technology Special Publication 800-70, Revision 2, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, 2011 年 2 月.

12. National Institute of Standards and Technology Special Publication 800-117, Version 1.0, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, 2010 年 7 月.

13. National Institute of Standards and Technology Special Publication 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0*, 2009 年 11 月.

14. National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, 2011 年 9 月.

付録 B

用語集

共通の用語とその定義

本付録 は、SP800-30 内で使用されているセキュリティ用語の定義を示している。本用語集の用語は、NIST によって策定された FISMA 関連のセキュリティ標準およびガイドラインで使用されている用語との一貫性を保っている。特に明記しない限り、本文書で使用されているすべての用語は、CNSSI No. 4009（国家安全保障システム委員会の指示 4009）『National Information Assurance (IA) Glossary（国家情報保証に関する用語集）』に含まれる定義との一貫性を保つ。

適切なセキュリティ (Adequate Security) [OMB Circular A-130, Appendix III]	情報の消失、誤用／悪用、情報への不正アクセスもしくは、改ざんがもたらすリスクや被害の大きさに比例するセキュリティ。
APT (Advanced Persistent Threat) [NIST SP 800-39]	高度な専門知識とかなりの資源を有するアドバーサリ。APT は、複数の異なる攻撃ベクトル（例：サイバー、物理的な、および詐欺）を使用して、自身の目的を達成するための機会の創出を試みる。その目的は、通常、組織の IT インフラ内に自身の存在を確立・拡張し、継続的に情報を引き出す、および／またはミッション、計画、組織の極めて重要な側面を損なわせる（または妨げる）、あるいはそうした行為を将来にわたって行える立場に自身を置くことである。さらに APT は、抵抗しようとする防衛者の取り組みに順応し、目的を果たすのに必要なレベルの情報のやりとりを維持する決意を持って、長期間にわたって継続的に目的を追求する。
アドバーサリ (Adversary) [DHS Risk Lexicon]	有害な活動を行う、または行おうとしている個人、グループ、組織、または政府機関。
政府機関 (Agency)	＜執行機関 (Execution Agency)＞を参照。
分析アプローチ (Analysis Approach)	リスクアセスメントの方向性または開始点、アセスメントの詳細レベル、そして類似の脅威シナリオに起因するリスクがどのように取り扱われるかについて定義するためのアプローチ。
アセスメント (Assessment)	＜セキュリティ管理策アセスメント (Security Control Assessment)＞、または＜リスクアセスメント (Risk Assessment)＞を参照。

アセスメントアプローチ (Assessment Approach)	リスクと、その一因となるリスク因子をアセスメントするためのアプローチ。その分類としては、定量的、定性的、半定量的などがある。
アセサー (Assessor)	＜セキュリティ管理策アセサー (Security Control Assessor)＞、または＜リスクアセサー (Risk Assessor)＞を参照。
攻撃 (Attack) [CNSSI No. 4009]	情報システム資源または情報自体の収集、混乱、否認、機能低下、または破壊を試みる、あらゆる種類の悪意のある活動。
認証 (Authentication) [FIPS 200]	多くの場合、情報システム資源に対するアクセスを許可するための前提条件として、ユーザ、プロセス、またはデバイスの身元を確認すること。
真正性 (Authenticity) [CNSSI No. 4009]	本物であることを示す特性であり、そうであることが確認でき、信頼できることが求められる。送信信号、メッセージ、またはメッセージ発信者の正当性に対する信頼。＜認証 (Authentication)＞を参照。
運用認可 (Authorization) (to operate) [CNSSI No. 4009]	情報システムの運用認可。情報システムの運用を認可し、合意されたセキュリティ管理策の導入について組織の業務（ミッション、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、および国家に対するリスクを明示的に許容する、といった組織の高官による正式な管理判断。
運用認可を出す範囲 (Authorization Boundary) [CNSSI No. 4009]	運用認可権限者によってその運用が認可されるべき情報システムの、すべてのコンポーネント（情報システムが接続されているシステムであっても、個別に運用認可を受けたものは含まない）。
運用認可権限者 (Authorizing Official) [CNSSI No. 4009]	組織の業務（ミッション、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、および国家に対する（容認レベルの）リスクを許容し、情報システムの運用に正式な責任を負う政府機関の高官。
可用性 (Availability) [44 U.S.C., Sec. 3542]	情報へのタイムリーで信頼のおけるアクセスと利用の確保。

最高情報責任者 (Chief Information Officer) [PL 104-106, Sec. 5125(b)]	以下の項目に責任を負う、政府機関の職員: (i) 法律、大統領令、指令、ポリシー、規定や政府機関の上層部によって定められた優先順位に基づいた方法で情報技術が調達され、情報資源が管理されていることを確実にするために、政府機関の執行部の長官や政府機関の他の上級管理職に対して助言や様々な支援を提供すること。 (ii) 政府機関のための健全で統合された情報技術アーキテクチャの開発、保守、および導入促進。 (iii) 政府機関のすべての主要情報資源管理プロセスに関して、効果的かつ効率的な設計および運用を促進する。この活動には、政府機関の作業プロセスの向上も含まれる。
最高情報セキュリティ責任者 (Chief Information Security Officer)	＜政府機関の上級情報セキュリティ責任者 (Senior Agency Information Security Officer)＞を参照。
共通管理策 (Common Control) [NIST SP 800-37]	単独または複数の情報システムによって継承されるセキュリティ管理策。＜セキュリティ管理策の継承 (Security Control Inheritance)＞を参照。
共通管理策の提供者 (Common Control Provider) [CNSSI No. 4009]	共通管理策（すなわち、複数の情報システムによって継承されるセキュリティ管理策）の開発、導入、アセスメント、およびモニタリングに責任を持つ組織の職員。
補完的セキュリティ管理策 (Compensating Security Control) [CNSSI No. 4009]	低位、中位、または高位のベースライン内の推奨されるセキュリティ管理策の代わりに採用できる、管理面、運用面、および／または技術面での管理策（すなわち、保護手段または対策）であり、情報システムに対して推奨管理策と同等の（または匹敵する）保護を提供する。
機密性 (Confidentiality) [44 U.S.C., Sec. 3542]	個人のプライバシーや知財情報の保護手段を含む、情報へのアクセスや情報の開示に対する制限（正式に認定されたもの）を保持すること。
行動方針 (Course of Action) [NIST SP 800-39]	時間段階的な、または、状況依存のリスク対応策の組み合わせ。＜リスクへの対応 (Risk Response)＞を参照。
重要インフラ (Critical Infrastructure)	物理的であるか、仮想であるかにかかわらず、米国にとって不可欠なシステムと資産。そうしたシステムと資産が機能しなくなったり、破壊されたりすると、セキュリティ、国家の経済の安定、国民の健康または安全、あるいは、それらの組み合わせを揺るがす影響がもたらされる。

重要インフラ部門 (Critical Infrastructure Sectors) [HSPD-7]	情報技術; 電気通信; 化学; 交通システム（大量輸送システム、航空輸送システム、海上輸送システム、陸上輸送システム、鉄道およびパイプライン輸送システムを含む）; 救急サービス; ならびに郵便および船舶。
重大性 (Criticality) [NIST SP 800-60]	ミッション／業務機能を成功裏に実施するために組織が情報または情報システムに依存する度合。
サイバー攻撃 (Cyber Attack) [CNSSI No. 4009]	サイバー空間を介した攻撃であり、コンピュータ環境／インフラを中断、無効化、破壊、または不当に制御する目的で、あるいは、そのデータの完全性を破壊する、もしくは管理されている情報を盗む目的で、企業によるサイバー空間の使用を狙う。
サイバーセキュリティ (Cyber Security) [CNSSI No. 4009]	サイバー攻撃によるサイバー空間の使用から保護する、または防御すること。
サイバー空間 (Cyberspace) [CNSSI No. 4009]	インターネット、電気通信網、コンピュータシステム、組み込み式プロセッサおよびコントローラを含む、情報システムインフラの相互依存型ネットワークによって構成される、情報環境内の世界的規模のドメイン。
広域防御 (Defense-in-Breadth) [CNSSI No. 4009]	システム／ネットワーク／サブコンポーネントのライフサイクルのすべての段階（システム／ネットワーク／製品の設計および開発; 製造; 梱包; 組み立て; システム統合; 販売; 運用; メンテナンス; ならびに退去）における利用可能な脆弱性に起因するリスクを特定、管理し、削減するための、計画された、かつ、系統だった一連の総合的な活動。
深層防護 (Defense-in-Depth) [CNSSI No. 4009]	組織の複数の層およびミッションにわたって調節可能な防壁を築くために、人、技術、および業務遂行能力を統合した情報セキュリティ戦略。
エンタープライズ (Enterprise) [CNSSI No. 4009]	明確なミッション／目標と、明確な境界を有する組織。通常、情報システムを使用してそのミッションを遂行し、自身のリスクとパフォーマンスの管理に責任を負う。エンタープライズは、以下のビジネス側面のすべて、あるいは一部によって構成されるだろう：調達、導入計画の管理、財務管理(例：予算)、人材、セキュリティ、ならびに情報システム／情報／ミッションの管理。＜組織(Organization)＞を参照。

エンタープライズアーキテクチャ (Enterprise Architecture) [CNSSI No. 4009]	エンタープライズの情報システム一式についての記述：それらのシステムがどのように設定されているか、どのように統合されているか、どのようにしてエンタープライズの境界の外側の環境と相互に作用するか、エンタープライズのミッションを支援するためにどのように運用されているか、そして、どのようにエンタープライズの総合的なセキュリティ体制に寄与しているか。
運用環境 (Environment of Operation)	情報システムが稼働する物理面、技術面および運用面での環境。これは、以下を含むが、これらに限定されない：ミッション／業務機能; ミッション／業務プロセス; 脅威スペース; 脆弱性; エンタープライズアーキテクチャおよび情報セキュリティアーキテクチャ; 職員; 施設; サプライチェーンの結びつき; 情報技術; 組織のガバナンスと文化; 調達／資材調達プロセス; 組織のポリシーと手順; 組織の想定、制限、リスク許容度、および優先順位／トレードオフ。
執行機関 (Executive Agency) [41 U.S.C., Sec. 403]	5 U.S.C., Sec. 101 で特定する執行部門、5 U.S.C., Sec. 102 で特定する軍の部局、5 U.S.C., Sec. 104（1）で定義される独立機関および 31 U.S.C., 91 章の規定を全面的に満たしている完全に政府が所有する企業。
「故障の木」分析 (Fault Tree Analysis)	トップダウンの演繹的な故障分析。この分析では、システムの望ましくない状態（頂上事象）をブール論理を使用して分析し、一連のより低いレベルの事象を結び付ける。 システムの望ましくない状態を特定し、その望ましくない事象（頂上事象）が現実的にどのように発生するかを特定するために、その運用環境においてシステムを分析するといった、分析的アプローチ。
連邦政府機関 (Federal Agency)	＜執行機関 (Executive Agency)＞を参照。
連邦政府の情報システム (Federal Information System) [40 U.S.C., Sec. 11331]	執行機関、執行機関からの受託者、または執行機関の代理となる他の組織によって使用または運用される情報システム
ハイブリッドセキュリティ管理策 (Hybrid Security Control) [NIST SP 800-53]	情報システムに導入されているセキュリティ管理策の一種。共通管理策としての役割と、システム固有の管理策としての役割を併せ持つ。＜共通管理策 (Common Control)＞と＜システム固有のセキュリティ管理策 (System-Specific Security Control)＞を参照。

影響レベル (Impact Level) [CNSSI No. 4009]	正規の権限によらない情報の開示、正規の権限によらない情報の変更、正規の権限によらない情報の破壊、あるいは情報または情報システムの可用性の喪失によってもたらされることが予期される、被害の大きさ。
影響値 (Impact Value) [CNSSI No. 1253]	ある情報タイプの機密性、完全性、または可用性への侵害によってもたらされる潜在的な影響を評価した結果であり、「低位」、「中位」、または「高位」のいずれかによって表される。
産業用制御システム (Industrial Control System) [NIST SP 800-39]	製造、製品の取り扱い、生産、および販売などの産業プロセスを制御するための情報システム。産業用制御システムは、地理的に分散している資産を管理するのに使用される監視制御情報収集システム、分散制御システム、およびプログラマブル論理制御装置を使用して局所化されたプロセスを管理する、より小規模な制御システムを含む。
情報 (Information) [CNSSI No. 4009]	事実、データ、または意見などの知識を媒体によって、あるいはテキスト、数値、図、地図、物語などの形式で、もしくは視聴覚的に伝達する、あるいは表現すること。
[FIPS 199]	情報タイプの一つの例
情報所有者 (Information Owner) [CNSSI No. 4009]	特定の情報に対する法的権限または運用権限を持ち、その情報の生成、分類、収集、処理、配布、および廃棄に関する管理策の制定に責任を負う職員。
情報資源 (Information Resources) [44 U.S.C., Sec. 3502]	情報および関連資源（人的資源、設備、資金、情報技術など）。
情報セキュリティ (Information Security) [44 U.S.C., Sec. 3542]	機密性、完全性、および可用性を提供するために、情報と情報システムを正規の権限によらないアクセス、使用、開示、中断、変更、または破壊から保護すること。
情報セキュリティアーキテクチャ (Information Security Architecture) [NIST SP 800-39]	エンタープライズのセキュリティプロセス、情報セキュリティシステム、職員および組織のサブユニットの構造と行動についての記述であり、エンタープライズのミッションおよび戦略計画に準拠していることを示すためのもの。
情報セキュリティ導入計画 (Information Security Program Plan) [NIST SP 800-53]	組織全体にわたる情報セキュリティ導入計画に課せられるセキュリティ要求事項の概要を提供し、これらの要求事項を満たすために導入が計画されている、あるいは導入されている計画管理面での管理策および共通管理策を記述する正式な文書。

情報セキュリティリスク (Information Security Risk)	情報および／または情報システムの正規の権限によらないアクセス、使用、開示、中断、変更、または破壊に起因する、組織の業務（ミッション、機能、イメージ、評判を含む）、組織の資産、個人、他の組織、および国家に対するリスク。＜リスク (Risk)＞を参照。
情報スチュワード (Information Steward) [CNSSI No. 4009]	特定の情報に対する法的権限または運用権限を持ち、その情報の生成、収集、処理、配布、および廃棄に関する管理策の制定に責任を負う政府機関の職員。
情報システム (Information System) [44 U.S.C., Sec. 3502]	情報の収集、処理、保守、使用、共有、配布、または廃棄を目的として編成された、独立した一連の情報資源。
情報システムの境界 (Information System Boundary)	＜運用認可を出す範囲 (Authorization Boundary)＞を参照。
情報システム所有者（または、導入計画管理者） (Information System Owner (or Program Manager))	情報システム全体の調達、開発、統合、変更、または運用と保守に責任を負う職員。
情報システムの耐障害性 (Information System Resilience)	攻撃を受けていて、機能が低下した（または弱化した）状態であっても、情報システムを稼働し続けられることと、攻撃が成功した場合でも、必須の機能を遂行する能力を急速に回復できること。
情報システムセキュリティ責任者 (Information System Security Officer)	情報システムまたはプログラムに関する運用面での適切なセキュリティ体制を維持する責任を、政府機関の上級情報セキュリティ責任者、運用認可権限者、管理職者、または情報システム所有者によって割り当てられた個人。
情報システム関連のセキュリティリスク (Information System-Related Security Risk)	情報または情報システムの機密性、完全性、または可用性の喪失により生じるリスクであり、組織の業務と資産、個人、他の組織、および国家に対する影響を考慮する。このリスクは、情報セキュリティリスクのサブセットである。＜リスク (Risk)＞を参照。

情報技術 (Information Technology) [40 U.S.C., Sec. 1401]	データまたは情報の自動的な入手、格納、操作、管理、移動、制御、表示、切り替え、交換、送信、または受信のために政府機関の執行部門によって利用される機器、相互接続されたシステム、または機器のサブシステム。上記の文章が示す目的のために、執行部門が機器を直接用いる場合には、機器は執行部門によって使用され、契約者が執行部門と以下のような契約を結んでいる場合には、機器は契約者によって使用される：(i) そうした機器の使用が要求されている; あるいは (ii) サービスの実行や製品の設置において、そうした機器をかなりの程度使用することが要求されている。情報技術の定義には、コンピュータ、補助機器、ソフトウェア、ファームウェアや類似の手続き、サービス（補助サービスを含む）、および関連する資源が含まれる。
情報タイプ (Information Type) [FIPS 199]	組織あるいは、状況によっては、特定の法律、大統領令、指令、ポリシー、または規制などによって定められている情報の具体的な分類（例：プライバシー、医療、知財、財務、調査、契約者機密、セキュリティ管理など）。
完全性 (Integrity) [44 U.S.C., Sec. 3542]	不正な改ざんまたは破壊から情報を保護すること（情報の否認防止および真正性の確保を含む）。
発生可能性 (Likelihood of Occurrence) [CNSSI No. 4009, adapted]	既知の脅威が既知の脆弱性（または一連の脆弱性）を利用することができる確率の主観的な分析にもとづく、重み付けされたリスク因子。
管理面での管理策 (Management Controls) [FIPS 200]	情報システムに対するセキュリティ管理策（すなわち、保護手段または対策）であり、リスクの管理と情報システムセキュリティの管理に重点的に取り組む。
ミッション／業務セグメント (Mission/Business Segment)	ミッションとなる分野、共通／共有のビジネスサービス、および組織全体にわたるサービスについて記述する、組織の要素。ミッション／業務セグメントは、ミッション／業務プロセスを共同で支援する単一の、あるいは複数の情報システムに応じて分類される。

国家安全保障にかかわるシステム (National Security System) [44 U.S.C., Sec. 3542]	政府機関、政府機関の委託業者または政府機関の代わりとなる他の組織によって使用される／運用されるすべての情報システム（すべての通信システムを含む）とは、(i) システムの機能、運用、利用が、インテリジェンス活動、国家安全保障にかかわる暗号活動、軍隊の指揮統制、武器または武器システムの一部として一体化した機器に関連するシステム、または、軍隊またはインテリジェンスミッションの達成に直結する重要なシステム（日常的な管理業務や業務アプリケーションに用いられる、たとえば、給与、財務、物流および人材管理のアプリケーションを除く）; あるいは (ii) 特定の手順に従って常に保護されるシステム。ここでいう特定の手順とは、大統領令、あるいは議会制定法が定める基準に従って判断した結果、国家防衛や外交政策上の利益の観点から機密にすることが特別に許可された情報を対象として確立された手順である。
運用面における管理策 (Operational Controls) [FIPS 200]	情報システムに対するセキュリティ管理策（すなわち、保護手段または対策）であり、（システムによって導入され、実行されるものとは対照的に）主に人によって導入され、実行される。
組織 (Organization) [FIPS 200, Adapted]	組織的な構造（たとえば、連邦政府機関、または、該当する場合、連邦政府機関の運用上のあらゆるエレメント）内のエンティティ（その規模、複雑さ、または位置づけは問わない）。
行動計画とマイルストーン (Plan of Action and Milestones) [OMB Memorandum 02-01]	達成すべきタスクを明確化する文書：行動計画とマイルストーンは、計画の中の項目の達成に必要な資源、タスクに見合ったすべてのマイルストーン、およびそのマイルストーンの完了予定日を詳述したものである。
素因的条件 (Predisposing Condition)	組織、ミッション／業務プロセス、エンタープライズアーキテクチャ、または情報システム（その運用環境を含む）に存在する条件の一種であり、一度開始された単一の、あるいは複数の脅威事象が組織の業務と資産、個人、他の組織、または国家に望ましくない結果または負の影響をもたらす可能性に影響を及ぼす（すなわち、その可能性を増加／減少させる）。
定性的なアセスメント (Qualitative Assessment) [DHS *Risk Lexicon*]	非数値的な分類またはレベルにもとづいてリスクをアセスメントするための一連の方法、原則、またはルールを使用するアセスメント。
定量的なアセスメント (Quantitative Assessment) [DHS *Risk Lexicon*]	そのアセスメントの環境の内外において数値の意味と比例が保たれる場合に、それらの数値の利用にもとづいてリスクをアセスメントするための一連の方法、原則、またはルールを使用するアセスメント。

繰り返し性 (Repeatability)	そのアセスメントを将来にわたって繰り返す場合に、過去のアセスメントとの一貫性を保ち、故に比較可能な方法で実施できるといった特性。
再現性 (Reproducibility)	複数の異なる専門家が同じデータを使用した場合に、同じ結果が生成されるといった特性。
残存リスク (Residual Risk) [CNSSI No. 4009]	セキュリティ対策が適用された後に残っているリスク。
リスク (Risk) [CNSSI No. 4009]	発生しうる状況または事象によってエンティティが脅かされる度合であり、以下をもとに算出される：(i) その状況または事象が発生した場合にもたらされる負の影響; ならびに (ii) 発生する可能性。＜情報システム関連のセキュリティリスク (Information System-Related Security Risk)＞を参照。
リスクアセスメント (Risk Assessment) [NIST SP 800-39]	情報システムの運用により生じる組織の業務（ミッション、機能、イメージ、評判を含む）、組織の資産、個人、他の組織、および国家に対するリスクを特定し、評価し、優先順位付けを行うプロセス。 リスクマネジメントの一部であり、脅威と脆弱性の分析を含み、導入が計画されている、あるいは導入されているセキュリティ管理策によって提供されるリスクの軽減を考慮する。「リスク分析」と同義である。
リスクアセスメント方法論 (Risk Assessment Methodology)	リスクモデル、アセスメントアプローチ、および分析アプローチを伴うリスクアセスメントプロセス。
リスクアセスメント報告 (Risk Assessment Report)	リスクアセスメントの実施結果、またはリスクアセスメントプロセスからの正式なアウトプットを含む、報告。
リスクアセサー (Risk Assessor)	リスクアセスメントの実施に責任を持つ個人、グループ、または組織。
リスクエグゼクティブ（機能） (Risk Executive (Function)) [CNSSI No. 4009]	以下の項目が確実に行われることを支援する、組織内の個人またはグループ。(i) 個々の情報システムに対するセキュリティリスク関連の考慮事項（それらのシステムに対する運用認可判断を含む）が、ミッションおよび業務上の機能を実施するうえでの、組織の全体的な戦略目標および目的と照らし合わせて、組織全体にわたる観点から捉えられるようにすること; ならびに (ii) 個々の情報システムに対するリスクの管理が、組織全体にわたって一貫していて、組織のリスク許容度を反映すると同時に、ミッション／業務の成功の妨げとなる他のリスクとともに考慮されること。

リスク因子 (Risk Factor)	リスクモデル内の特性の一つであり、リスクアセスメントにおけるリスクレベルを判断への入力データとして用いられる。
リスクマネジメント (Risk Management) [NIST SP 800-39] [CNSSI No. 4009, adapted]	組織の業務（ミッション、機能、イメージ、評判を含む）、組織の資産、個人、他の組織、および国家に対する情報セキュリティリスクを管理するための計画および支援プロセス。これには、(i) リスク関連活動のコンテクストの確立; (ii) リスクのアセスメント; (iii) 特定されたリスクへの対応; ならびに (iv) 長期間にわたるリスクのモニタリング。
リスクの軽減 (Risk Mitigation) [CNSSI No. 4009]	リスクマネジメントプロセスから推奨された、リスクを減らすための適切な管理策／対策を優先順位付けし、評価し、実施すること。「リスク対応」のサブセット。
リスクモデル (Risk Model)	リスクアセスメント方法論 (アセスメントアプローチと分析アプローチを含む)の主要なコンポーネントの１つであり、主要な用語とアセスメント可能なリスク因子を定義する。
リスクのモニタリング (Risk Monitoring) [NIST SP 800-39]	組織のリスクコンテクスト、リスクマネジメント計画、およびリスク判断を支援する関連活動についての現行の認識を維持すること。
リスクへの対応 (Risk Response) [NIST SP 800-39]	組織の業務（すなわち、ミッション、機能、イメージ、または評判）、組織の資産、個人、他の組織、または国家に対するリスクの許容、回避、軽減、共有、または移転。＜行動方針 (Course of Action)＞を参照。
リスク対応策 (Risk Response Measure) [NIST SP 800-39]	特定されたリスクに対応するために取られる具体的な行為。
根本的原因の分析 (Root Cause Analysis)	特定の一連のリスクの根本にある原因を特定するための、原理ベースのシステムアプローチ。
セキュリティ運用認可 (Security Authorization (to Operate))	＜運用認可 (Authorization (to operate))＞を参照。
セキュリティ分類 (Security Categorization)	情報または情報システムのセキュリティ分類を決定するプロセス。国家安全保障にかかわるシステムと、そうでないシステムのセキュリティ分類に関する方法論については、それぞれ、CNSSI No. 1253 と FIPS 199 に記載されている。

セキュリティ管理策アセスメント (Security Control Assessment) [NIST SP 800-39] [CNSSI No. 4009, Adapted]	セキュリティ管理策がどの程度正しく導入されているか、どの程度意図した通りに運用されているか、情報システムまたは組織のセキュリティ要求事項に対する適合性の観点から所望の結果をどの程度産出しているかを判断するための、管理面、運用面、技術面でのセキュリティ管理策のテストおよび／または評価。
セキュリティ管理策アセサー (Security Control Assessor)	セキュリティ管理策アセスメントの実施に責任を持つ個人、グループ、または組織。
セキュリティ管理策ベースライン (Security Control Baseline) [CNSSI No. 4009]	低位影響、中位影響、または高位影響の情報システムに対して定められた、最低限のセキュリティ管理策一式。
[CNSSI No. 1253]	単一の、あるいは複数の特定のセキュリティ分類に対処するために、情報セキュリティ戦略の計画活動を通じて確立された、一連の情報セキュリティ管理策。この一連のセキュリティ管理策 は、特定のシステムのセキュリティ分類が特定された後に、そのシステムに対して選択された、初期のセキュリティ管理策一式となることを意図している。
セキュリティ管理策の強化 (Security Control Enhancement) [NIST SP 800-39, adapted]	以下を実施するためのセキュリティ能力についての記述：(i) 基本的なセキュリティ管理策に追加の関連する機能を組み入れる; および／または (ii) 基本的な管理策の強度を高める。
セキュリティ管理策の継承 (Security Control Inheritance) [CNSSI No. 4009]	情報システムまたはアプリケーションが、それらのシステムまたはアプリケーションに責任を負うエンティティ以外のエンティティ（システムまたはアプリケーションが設置されている組織にとって内部または外部のエンティティ）によって開発、導入、アセスメント、運用認可、およびモニタリングされるセキュリティ管理策の保護を受けている状況。＜共通管理策 (Common Control) ＞を参照。
セキュリティ管理策 (Security Controls) [FIPS 199, CNSSI No. 4009]	システムとその情報の機密性、完全性、および可用性を保護するために、情報システムに対して規定された、管理面、運用面、技術面での管理策（すなわち、保護手段または対策）。
セキュリティ影響分析 (Security Impact Analysis) [NIST SP 800-37]	情報システムに対する変更がシステムのセキュリティ状態にどの程度の影響をもたらしたかを判断するために、運用認可権限者によって実施される分析。
セキュリティ目的 (Security Objective) [FIPS 199]	機密性、完全性、または可用性。

セキュリティ計画 (Security Plan) [NIST SP 800-18]	情報システムまたは情報セキュリティ導入計画のセキュリティ要求事項の概要を示し、これらの要求事項を満たすために導入が計画されている、あるいは導入されているセキュリティ管理策について記述する正式な文書。＜システムセキュリティ計画 (System Security Plan)＞または＜情報セキュリティ導入計画(Information Security Program Plan)＞を参照。
セキュリティポリシー (Security Policy) [CNSSI No. 4009]	セキュリティサービスの提供に関する一連の基準。
セキュリティ体制 (Security Posture) [CNSSI No. 4009]	企業のネットワーク、情報、およびシステムのセキュリティ状態。企業の防衛を管理し、状況が変わった場合に対応するために導入されている、情報を保障するための資源（例：人、ハードウェア、ソフトウェア、ポリシー）および機能にもとづく。
セキュリティ要求事項 (Security Requirements) [FIPS 200]	処理、格納、または伝送されている情報の機密性、完全性および可用性を確保するために、情報処理システムに課される要求事項。これらの要求事項は、大統領令、指令、ポリシー、標準、指示、規制、手順または組織のミッション／事業事例から導出される。
半定量的なアセスメント (Semi-Quantitative Assessment) [Department of Homeland Security (DHS) *Risk Lexicon*]	その数値と意味が別の環境では維持されない瓶、スケール、または代表的な数値を使用してリスクをアセスメントするための一連の方法、原則、またはルールを使用するアセスメント。
政府機関の上級情報セキュリティ責任者 (Senior Agency Information Security Officer) [44 U.S.C., Sec. 3544]	FISMA が規定する最高情報責任者の職責を果たす責任を有する職員で、最高情報責任者の、政府機関の運用認可権限者、情報システム所有者および情報システムセキュリティ責任者との最初の連絡窓口としての役割を果たす職員。 [注：連邦政府の下位組織では、政府機関の上級情報セキュリティ責任者が担う責務と類似の責務を担う個人を示す用語として「上級情報セキュリティ責任者(Senior Information Security Officer)」または「最高情報セキュリティ責任者(Chief Information Security Officer)」を用いる場合がある。]
上級情報セキュリティ責任者 (Senior Information Security Officer)	＜政府機関の上級情報セキュリティ責任者 (Senior Agency Information Security Officer)＞を参照。
機微度 (Sensitivity) [NIST SP 800-60]	保護の必要性を示すために所有者によって情報に割り付けられる重要性の尺度。

サブシステム (Subsystem) [NIST SP 800-39]	情報システムの主要な一部分またはコンポーネントであり、情報、情報技術、および人員で構成され、ひとつまたは複数の特定の役割を果たす。
セキュリティ管理策の補足 (Supplementation (Security Controls)) [NIST SP 800-39]	組織のリスクマネジメント関連のニーズを十分に満たすために、NIST SP 800-53 または CNSSI No. 1253 から選択したセキュリティ管理策ベースラインに、セキュリティ管理策または管理策を強化したものを追加するプロセス。
システム (System)	＜情報システム (Information System)＞を参照。.
システムセキュリティ計画 (System Security Plan) [NIST SP 800-18]	情報システムのセキュリティ要求事項の概要を示し、これらの要求事項を満たすために導入が計画されている、あるいは導入されているセキュリティ管理策について記述する正式な文書。
システム固有のセキュリティ管理策 (System-Specific Security Control) [NIST SP 800-37]	共通セキュリティ管理策としては指定されていない情報システムのセキュリティ管理策、または、情報システムに導入される予定のハイブリッド管理策の一部。
調整 (Tailoring) [NIST SP 800-53, CNSSI No. 4009]	セキュリティ管理策ベースラインを、以下の活動を通じて修正すること: (i) スコーピングガイダンスの適用; (ii) 補完的セキュリティ管理策の指定(必要な場合); ならびに (iii) 明示的な代入ステートメントと選択ステートメントを使用して、組織が定めたセキュリティ管理策パラメータの値を指定（可能な場合）。
調整されたセキュリティ管理策ベースライン (Tailored Security Control Baseline) [NIST SP 800-39]	セキュリティ管理策ベースラインに調整ガイダンスを適用することによって得られる一連のセキュリティ管理策。＜調整 (Tailoring)＞を参照。
技術面での管理策 (Technical Controls) [FIPS 200]	情報システムに対するセキュリティ管理策（すなわち、保護手段または対策）であり、システムのハードウェア、ソフトウェア、またはファームウェアコンポーネントに含まれるメカニズムを介して、主として情報システムによって導入され、実行される。
脅威 (Threat) [CNSSI No.4009]	組織の業務（ミッション、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、または国家に負の影響をもたらしうるあらゆる状況または事象。要因としては、情報の正規の権限によらないアクセス、破壊、開示、または変更、および／またはサービス妨害(DoS)などがある。

脅威のアセスメント (Threat Assessment) [CNSSI No. 4009]	情報システムまたは企業に対する脅威の大きさを正式に評価し、脅威の性質について記述するプロセス。
脅威事象 (Threat Event)	望ましくない結果または影響をもたらしうる事象または状況。
脅威シナリオ (Threat Scenario)	特定の脅威源、あるいは複数の脅威源によって引き起こされ、その一部が時系列で順序付けられる、一連の脅威事象。「Threat Campaign」と同義である。
脅威のシフト (Threat Shifting)	アドバーサリが、感知した保護手段／対策（すなわち、セキュリティ管理策）に対して取る対抗措置であり、彼らはそれらの保護手段／対策を回避または打ち破るために、害を及ぼすための自身の意図の一部の特性を変更する。
脅威源 (Threat Source) [CNSSI No. 4009]	脆弱性の意図的な利用を目的とした意図および方法、または脆弱性を誤って利用する可能性のある状況や方法。
脆弱性 (Vulnerability) [CNSSI No. 4009]	情報システム、システムセキュリティ手順、内部統制、または実装に存在する弱点で、脅威源によって利用される可能性がある。
脆弱性のアセスメント (Vulnerability Assessment) [CNSSI No. 4009]	セキュリティ対策の適切性を判断し、セキュリティ上の欠陥を特定し、提案されているセキュリティ対策の有効性を予測するためのデータを提供し、そうしたセキュリティ対策の導入後の適切性を確認するための、情報システムまたは製品の体系的な検査。

付録 C

略語

共通の略語

APT	APT (Advanced Persistent Threat)
BCP	事業継続計画 (Business Continuity Plan)
BIA	ビジネス影響分析 (Business Impact Analysis)
CNSS	国家安全保障システム委員会 (Committee on National Security Systems)
COOP	業務の継続 (Continuity of Operations)
DoD	国防総省 (Department of Defense)
DHS	国土安全保障省 (Department of Homeland Security)
DNI	国家情報長官 (Director of National Intelligence)
EA	エンタープライズアーキテクチャ (Enterprise Architecture)
FIPS	連邦情報処理規格 (Federal Information Processing Standards)
FISMA	連邦情報セキュリティマネジメント法 (Federal Information Security Management Act)
ICS	産業用制御システム (Industrial Control System)
IEC	国際電気標準会議 (International Electrotechnical Commission)
ISO	国際標準化機構 (International Organization for Standardization)
IT	情報技術 (Information Technology)
JTF	ジョイントタスクフォース (Joint Task Force)
NIST	米国国立標準技術研究所 (National Institute of Standards and Technology)
NOFORN	他国への開示禁止 (Not Releasable to Foreign Nationals)
ODNI	国家情報長官室 (Office of the Director of National Intelligence)
OMB	行政管理予算局 (Office of Management and Budget)
RAR	リスクアセスメント報告 (Risk Assessment Report)
RMF	リスクマネジメントフレームワーク (Risk Management Framework)
SCAP	セキュリティ コンテンツ オートメーション プロトコル(SCAP) (Security Content Automation Protocol)
SP	特定発行文書 (Special Publication)
TTP	戦術、技法、手順 (Tactic Technique Procedure)
U.S.C.	合衆国法律集 (United States Code)

付録 D

脅威源

脅威事象を開始することができる脅威源の分類体系

本付録は、以下を提供する：(i)「脅威源の特定」タスクに対する、有用であると考えられる入力データについての説明; (ii) そうした脅威源が脅威事象を開始する可能性や影響をアセスメントにするのに使用される、脅威源の分類体系（タイプ、説明、およびリスク因子（すなわち、特徴）ごとの）の例; (iii) それらのリスク因子をアセスメントするための、調整可能なアセスメントスケールの例; ならびに (iv) タスク 2-1（「脅威源の特定」）の結果を要約し、文書化するためのテンプレート。本付録に記載されている分類体系とアセスメントスケールは、組織が開始点として使用することができるが、組織固有の条件に合わせて適切に調整する必要があるだろう。タスク 2-1 のアウトプットである表 D-7 と 表 D-8 は、付録 I のリスク一覧に対して、関連する入力データを提供する。

表 D-1：入力データ – 脅威源の特定

説明	以下の層に提供される		
	第 1 層	**第 2 層**	**第 3 層**

第 1 層から：（組織レベル）
- 信頼できるとみなされた、脅威関連情報の情報源（例：オープンソースおよび／または機密扱いの脅威報告書、前に実施されたリスク／脅威アセスメント）。**(セクション 3.1、タスク 1-4)**
- 第 1 層に特化した、脅威源関連情報および手引き（例：組織のガバナンス、主要なミッション／業務機能、管理／運用上のポリシー、手順、および構造、外部のミッション／業務との関係などに関連する脅威）。
- 脅威源の分類体系（必要ならば、組織によって注釈が付けられる）。**(表 D-2)**
- アドバーサリによる脅威源と、アドバーサリによるもの以外の脅威源の特徴定義。
  - アドバーサリの能力、意図、および標的をアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。**(表 D-3, 表 D-4, 表 D-5)**
  - 影響の範囲をアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。**(表 D-6)**
- 前に実施されたリスクアセスメントにおいて特定された脅威源（適切な場合）。
	いいえ	はい	はい
			もしそうでないなら第 2 層にて提供される

第 2 層から：（ミッション／業務プロセスレベル） - 第 2 層に特化した、脅威源関連情報および手引き（例：ミッション／業務プロセス、エンタープライズアーキテクチャのセグメント、共通インフラ、支援サービス、共通管理策、および外部依存に関連する脅威）。 - アドバーサリによる脅威源と、アドバーサリによるもの以外の脅威源の、ミッション／業務プロセスに特化した特徴定義。	はい（RAR を介して）	はい（ピア共有を介して）	はい
第 3 層から：（情報システムレベル） - 第 3 層に特化した、脅威源関連情報および手引き（例：情報システム、情報技術、情報システムコンポーネント、アプリケーション、ネットワーク、運用環境などに関連する脅威）。 - アドバーサリによる脅威源と、アドバーサリによるもの以外の脅威源の、情報システムに特化した特徴定義。	はい（RAR を介して）	はい（RAR を介して）	はい（ピア共有を介して）

表 D-2:脅威源の分類体系

脅威源のタイプ	説明	特徴

アドバーサリによる
- 個人
  - 外部の者
  - 内部の者
  - 信頼されている内部の者
  - 特権を持つ内部の者
- グループ
  - アドホックな
  - 定着した
- 組織
  - 競争相手
  - 供給業者
  - パートナー
  - 顧客
- 国民国家
	サイバー資源(すなわち、電子的形態の情報、情報および通信技術、ならびにそれらの技術によって提供される通信および情報処理能力)に対する組織の依存を利用しようとする個人、グループ、組織、または国家。	能力、意図、標的

偶発的な - ユーザ - 特権ユーザ/アドミニストレータ	日々の責務を実施する過程で個人が取る誤ったアクション	影響の範囲

構造上の
- IT 機器
  - ストレージ
  - プロセッシング
  - 通信
  - ディスプレー
  - センサー
  - コントローラ
- 環境制御
  - 温度/湿度の制御
  - 電源
- ソフトウェア
  - オペレーティングシステム
  - ネットワーク
  - 汎用アプリケーション
  - ミッションに特化したアプリケーション
	老化、資源の枯渇、または予測されたオペレーティングパラメータを超えるその他の状況に起因する、機器の故障、環境制御の失敗、またはソフトウェアの不具合。	影響の範囲

環境上の
- 自然災害または人災
  - 火事
  - 洪水/津波
  - 爆風/竜巻
  - ハリケーン
  - 地震
  - 爆撃
  - オーバーラン
- 異常な自然現象(例:太陽の黒点)
- インフラの故障/停電
  - 電気通信
  - 電力
	組織が依存するが、組織のコントロールの範囲がである重要インフラ対する自然災害、およびそれらのインフラの故障。
	注: 自然災害と人災は、その重大さ、および/または継続期間の観点から、その特徴を定義できる。しかしながら、脅威源と脅威事象がしっかり特定される場合には、重大さと 継続期間は脅威事象の説明に含まれる(例:カテゴリー5 のハリケーンは、基幹システムを 収容する施設に大きな被害をもたらし、それらのシステムを 3 週間にわたって利用できなくする)。
		影響の範囲

表 D-3:アセスメントスケール – アドバーサリの能力の特徴定義

定性的な値	半定量的な値		説明
非常に高い	96-100	10	このアドバーサリは、非常にと十分な資源を有し、複数回にわたる、継続的な、調整された攻撃が成功裏に行われるのを支援する機会を創出できる。
高い	80-95	8	このアドバーサリは、高いレベルの専門知識を有し、複数回にわたる、調整された攻撃が成功裏に行われるのを支援するための、十分な資源と機会を有する。
中間	21-79	5	このアドバーサリは、複数回にわたる攻撃が成功裏に行われるのを支援するための、適度な資源、専門知識、および機会を有する。
低い	5-20	2	このアドバーサリは、単一の攻撃が成功裏に行われるのを支援するための、限られた資源、専門知識、および機会を有する。
非常に低い	0-4	0	このアドバーサリは、単一の攻撃が成功裏に行われるのを支援するための、非常に限られた資源、専門知識、および機会を有する。

表 D-4:アセスメントスケール – アドバーサリの意図の特徴定義

定性的な値	半定量的な値		説明
非常に高い	96-100	10	このアドバーサリは、組織の情報システムまたはインフラ内の存在を利用し、主要なミッション／業務機能、計画、または企業を弱体化させる、ひどく妨げる、または破壊しようとする。このアドバーサリは、スパイ活動に必要なノウハウの開示について、目標を達成するための自身の能力を妨げる程のものに関してのみ、懸念する。
高い	80-95	8	このアドバーサリは、組織の情報システムまたはインフラ内の存在を維持し、主要なミッション／業務機能、計画、または企業の重要な側面を弱体化させたり、妨げようとする、あるいは、将来にわたってそうした行為を行える立場に自身を置こうとする。 このアドバーサリは、特に将来の攻撃に備えて、攻撃の発覚／スパイ活動に必要なノウハウの開示を最小限に抑えようとする。
中間	21-79	5	このアドバーサリは、組織の情報システムまたはインフラ内に足場を構築し、特定の機密情報または機微な情報を取得したり、変更しようとする、あるいは組織のサイバー資源を奪ったり、途絶させようとする。このアドバーサリは、特に長期間にわたって攻撃を実施する際に、攻撃の発覚／スパイ活動に必要なノウハウの開示を最小限に抑えようとする。このアドバーサリは、これらの目標を達成するために、組織のミッション／業務機能の諸側面を妨げようとする。
低い	5-20	2	このアドバーサリは、機密情報または機微な情報を取得しようとする、あるいは組織のサイバー資源を奪ったり、途絶させようとする。その際、攻撃の発覚／スパイ活動に必要なノウハウの開示を恐れない。
非常に低い	0-4	0	このアドバーサリは、組織のサイバー資源を奪ったり、途絶させたり、あるいいは損なわせようとする。その際、攻撃の発覚／スパイ活動に必要なノウハウの開示を恐れない。

表 D-5:アセスメントスケール – アドバーサリの標的の特徴定義

定性的な値	半定量的な値		説明
非常に高い	96-100	10	このアドバーサリは、偵察によって得られた情報を分析し、特定の組織、企業、計画、ミッション／業務機能を執拗に狙った攻撃を行う。この際、特定の価値の高い、または基幹業務に関わる情報、資源、供給フロー、または機能; 特定の職員または地位; 支援インフラの提供業者／供給業者; あるいはパートナー組織に焦点を当てる。
高い	80-95	8	このアドバーサリは、偵察によって得られた情報を分析し、特定の組織、企業、計画、ミッション／業務機能を執拗に狙った攻撃を行う。この際、特定の価値の高い、または基幹業務に関わる情報、資源、供給フロー、または機能; それらの機能を支援する特

			定の職員; あるいは重要な地位に焦点を当てる。
中間	21-79	5	このアドバーサリは、特定の価値の高い組織（および最高情報責任者などの、重要な地位にいる職員）、計画、または情報を執拗に狙うための、一般に入手可能な情報を分析する。
低い	5-20	2	このアドバーサリは、価値の高い組織または情報を狙うための一般に入手可能な情報を使用して、その類の組織または情報を狙う。
非常に低い	0-4	0	このアドバーサリは、特定の組織または特定のクラスの組織を狙う可能性があるが、そうでない可能性もある。

表 D-6:アセスメントスケール – アドバーサリによるもの以外の脅威源がもたらす影響の範囲

定性的な値	半定量的な値		説明
非常に高い	96-100	10	エラー、アクシデント、または天災の影響は**広範囲に及ぶ(sweeping)**。その範囲は、[第 3 層:情報システム; 第 2 層:ミッション／業務プロセスまたはエンタープライズアーキテクチャのセグメント、共通インフラ、あるいは支援サービス; 第 1 層:組織／ガバナンス構造]の サイバー資源のほぼすべてを含む。
高い	80-95	8	エラー、アクシデント、または天災の影響は**広範囲に及ぶ(extensive)**。その範囲は、[第 3 層:情報システム; 第 2 層:ミッション／業務プロセスまたはエンタープライズアーキテクチャのセグメント、共通インフラ、あるいは支援サービス; 第 1 層:組織／ガバナンス構造]の サイバー資源の大半を含む。その影響は多くの重要な資源に及ぶ。
中間	21-79	5	エラー、アクシデント、または天災の影響は**広範囲に及ぶ(wide-ranging)**。その範囲は、[第 3 層:情報システム; 第 2 層:ミッション／業務プロセスまたはエンタープライズアーキテクチャのセグメント、共通インフラ、あるいは支援サービス; 第 1 層:組織／ガバナンス構造]の サイバー資源のかなりの部分を含む。その影響は、一部の重要な資源に及ぶ。
低い	5-20	2	エラー、アクシデント、または天災の影響は**限られている(limited)**。その範囲は、[第 3 層:情報システム; 第 2 層:ミッション／業務プロセスまたはエンタープライズアーキテクチャのセグメント、共通インフラ、あるいは支援サービス; 第 1 層:組織／ガバナンス構造]の サイバー資源の一部を含むが、重要な資源は一切含まない。
非常に低い	0-4	0	エラー、アクシデント、または天災の影響は**最小である(minimal)**。その範囲は、あるとしても [第 3 層:情報システム; 第 2 層:ミッション／業務プロセスまたはエンタープライズアーキテクチャのセグメント、共通インフラ、あるいは支援サービス; 第 1 層:組織／ガバナンス構造]の サイバー資源のごくわずかしか含まない。

表 D-7:テンプレート – アドバーサリによる脅威源の特定

識別子	脅威源の情報源	範囲内である	能力	意図	標的
組織が定めたもの	表 D-2 とタスク 1-4 または 組織が定めたもの	はい/ いいえ	表 D-3 または 組織が定めたもの	表 D-4 または 組織が定めたもの	表 D-5 または 組織が定めたもの

表 D-8:テンプレート – アドバーサリによるもの以外の脅威源の特定

識別子	脅威源の情報源	範囲内である	影響の範囲
組織が定めたもの	表 D-2 とタスク 1-4 または 組織が定めたもの	はい / いいえ	表 D-6 または 組織が定めたもの

付録 E

脅威事象

脅威源によって開始される脅威事象の代表的な例

本付録は、以下を提供する：(i)「脅威事象の特定」タスクに対する、有用であると考えられる入力データについての説明; (ii) 戦術、技法、および手順によって表されるアドバーサリによる脅威源と、アドバーサリによるもの以外の脅威源の、代表的な例; (iii) それらの脅威事象間の関連性を特定するための アセスメントスケールの例; ならびに (iv) タスク 2-2（「脅威の特定」）の結果を要約し、文書化するためのテンプレート。組織は、必要な能力を有するアドバーサリが特定されなかった場合には、その脅威事象をさらなる検討の対象から外すことができる。[52] 組織は、具体的な TTPs（戦術、技法、および手順）について説明するために提供された脅威事象関連の情報を、十分な詳細さをもって [53]、かつ適切な分類レベル [54] で修正することができる。組織は、本付録に記載されている代表的な脅威事象と、それらの事象間の関連性について断定された／予測された値を開始点として使用することができるが、組織固有の条件に合わせて調整する必要があるだろう。タスク 2-2 のアウトプットである表 E-5 は、付録 I のリスク一覧に対して、関連する入力データを提供する。

表 E-1：入力データ – 脅威事象の特定

説明	以下の層に提供される		
	第 1 層	**第 2 層**	**第 3 層**
第 1 層から：（組織レベル） - 信頼できるとみなされた、脅威関連情報の情報源（例：オープンソースおよび／または機密扱いの脅威報告書、前に実施されたリスク／脅威アセスメント）。(**セクション 3.1、タスク 1-4)** - 第 1 層に特化した、脅威事象関連情報および手引き（例：組織のガバナンス、主要なミッション／業務機能、外部のミッション／業務との関係、管理／運用上のポリシー、手順、および構造などに関連する脅威）。 - アドバーサリによる脅威事象の例（必要ならば、組織によって注釈が付けられる）。(**表 E-2**) - アドバーサリによるもの以外の脅威事象の例（必要ならば、組織によって注釈が付けられる）。(**表 E-3**) - 脅威事象間の関連性をアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。(**表 E-4**) - 前に実施されたリスクアセスメントにおいて特定された脅威事象（適切な場合）。	いいえ	はい	はい もしそうでないなら第 2 層にて提供される

[52] 表 E-2 の各項目は、アドバーサリの能力、意図、および標的に関して、特定のレベルをを暗に想定している。脅威源の特定の結果によっては、いくつかの項目が関連しないとみなされたり、結合される場合がある。さらに、いくつかの項目が、組織のエンタープライズアーキテクチャの観点から書き直される場合がある。

[53] TTPs（戦術、技法、および手順）の詳細レベルは、組織のリスクフレームの一部として定められる。表 E-2 の詳細レベルは、3 つのすべての層におけるリスクアセスメントを支援し、必要に応じて追加の詳細を含めるために調整できることを意図している。ソフトウェアを利用する脅威事象についてのより詳細な説明は、たとえば、CAPEC (Common Attack Pattern Enumeration and Classification)サイト(http://capec.mitre.org)に記載されている。

[54] 表 E-2 の脅威事象は、分類されていないレベルで提供されている。分類されたレベルでの追加の脅威事象に関しては、適切なアクセス権限(security clearance)を持ち、知る必要がある個人であれば、選択された政府機関から情報を入手することが可能である。

第 2 層から:（ミッション／業務プロセスレベル） - 第 2 層に特化した、脅威事象関連情報および手引き（例:ミッション／業務プロセス、エンタープライズアーキテクチャのセグメント、共通インフラ、支援サービス、共通管理策、および外部依存などに関連する脅威）。 - アドバーサリによる脅威事象と、アドバーサリによるもの以外の脅威事象の、ミッション／業務プロセスに特化した特徴定義。	はい（RAR を介して）	はい（ピア共有を介して）	はい
第 3 層から:（情報システムレベル） - 第 3 層に特化した、脅威事象関連情報および手引き（例:情報システム、情報技術、情報システムコンポーネント、アプリケーション、ネットワーク、運用環境などに関連する脅威）。 - アドバーサリによる脅威事象と、アドバーサリによるもの以外の脅威事象の、情報システムに特化した特徴定義。 - インシデント報告	はい（RAR を介して）	はい（RAR を介して）	はい *Via*（ピア共有を介して）

表 E-2:代表的な例 – アドバーサリによる脅威事象 [55]

脅威事象 **（戦術、技法、手順によって特徴が定義される）**	**説明**
偵察を行い、情報を収集する	
ペリミタネットワークの偵察／スキャンを実施する。	アドバーサリは、市販のソフトウェアまたはフリーソフトウェアを使用して、組織のペリミタをスキャンし、組織の IT インフラについてよりよく理解し、功を奏する攻撃をしかけるための能力を高める。
無防備なネットワークに対するネットワークスニッフィングを実施する。	アドバーサリは、情報を伝送するのに使用される露出した 有線の、あるいは無線のデータチャネルにアクセスし、ネットワークスニッフィングによってコンポーネント、資源、およびプロテクションを特定する。
組織の情報のオープンソースディスカバリを使用して、情報を収集する。	アドバーサリは、公的にアクセス可能な情報をあさって、組織の情報システム、業務プロセス、ユーザまたは職員、あるいは外部との関係についての情報を取得し、後の攻撃に使用する。
標的である組織に対する偵察と監視を実施する。	アドバーサリ は、長期にわたってさまざまな手段を使用して（例:スキャン、物理的観測）、組織を検証・アセスメントし、脆弱性を突きとめる。
マルウェアを送り込んで、内部偵察を実施する。	アドバーサリは、組織のペリミタ内にインストールされたマルウェアを使用して、標的を探す。スキャン、探査、または観測はペリミタを超えないため、外部に設置された侵入検知システムによって検知されない。
攻撃用のツールをクラフトする、または作成する	
フィッシング攻撃をクラフトする。	アドバーサリ は、正規の／信頼できる情報源からの通信を偽造して、ユーザ名、パスワード、社会保障番号などの機微な情報を取得する。典型的な攻撃は、電子メール、インスタントメッセージ、あるいは類似の手段を介して発生し、一般的にユーザは、正規のサイトに見せかけたウェブサイトに誘導され、そこで入力した情報は盗み取られる。
スピアーフィッシング（特定の人物を標的としたフィッシング詐欺）をクラフトする。	アドバーサリ は、価値の高い標的（例:最高幹部や上級管理者）を狙ったフィッシング攻撃を採用する。
実装された IT 環境にもとづいて具体的に攻撃をクラフトする。	アドバーサリ は、組織の IT 環境について自身が有する知識を活用して、攻撃を開発する（例:標的型マルウェアをクラフトする）。
偽の／なりすましのウェブサイトを作成する。	アドバーサリは、正規のウェブサイトの複製を作成する。ユーザが偽のサイトにアクセスすると、そのサイトは情報を収集したり、マルウェアをダウンロードする。
偽の証明書をクラフトする。	アドバーサリは、マルウェアまたは接続が正規に見えるよう、認証機関を偽造する、あるいは侵害する。

[55] 脅威源としての APT に限定されるわけではなく、表 E-2 の脅威事象は、通常、APT キャンペーンの流れに従う。キャンペーン内の各段階では、類似の事象がアドバーサリの能力の高い順に記載されている。

脅威事象 （戦術、技法、手順によって特徴が定義される）	説明
見せかけの組織を作成・運営し、悪意のあるコンポーネントをサプライチェーンに送り込む。	アドバーサリ は、極めて重要なライフサイクルパスにおいて、正規の供給業者に見せかけた偽の組織を作成する。これらの組織は、その後、破損した／悪意のある情報システムコンポーネントを組織のサプライチェーンに送り込む。
悪意のある能力を送り込む／挿入する／インストールする	
既知のマルウェアを組織の内部情報システムに送り込む（例：電子メールを介したウイルスによって）。	アドバーサリ は、よく使われる配信メカニズム（例：電子メール）を使用して、既知のマルウェア（例：その存在が知られているマルウェア）を組織の情報システムにインストール／挿入する。
変更が加えられたマルウェアを組織の内部情報システムに送り込む。	アドバーサリ は、電子メールよりも高度な配信メカニズム（例：ウェブトラフィック、インスタントメッセージ、FTP）を使用して、マルウェア（場合によっては、既知のマルウェア に変更を加えたもの）を送り込み、組織の内部情報システムに対するアクセスを試みる。
内部システムの制御を奪い、データを取り出すための、標的型マルウェアを送り込む。	アドバーサリ は、組織の内部情報システムの制御を奪い、機微な情報を特定し、取り出した後に、これらの行為を気付かれないようにするために特別に設計されたマルウェア をインストールする。
取り外し可能なメディアを用意して、マルウェアを送り込む。	アドバーサリ は、マルウェアを含む取り外し可能なメディア（例：フラッシュディスク）を用意し、組織の物理的な境界の外側ではあるが職員がそのメディアを発見する可能性が高い場所に置くことによって（例：施設の駐車場、職員が出席する会議場所での展示）、職員がそれらのメディアを組織の情報システムに使用するよう仕向ける。
非標的型マルウェアをダウンロード可能なソフトウェアおよび／または市販の IT 製品に挿入する。	アドバーサリは、よく使われるフリーウェア、シェアウェア、または市販の IT 製品にエラーを持ち込む、あるいはマルウェアを挿入する。アドバーサリ は、特定の組織を狙うわけではなく、単に、組織の内部情報システムへの侵入地点を探る。これは、モバイルアプリケーションでは特に問題になることに留意すること。
標的型マルウェアを組織の情報システムと情報システムコンポーネントに挿入する。	アドバーサリは、組織の情報システムと情報システムコンポーネント（例：市販の IT 製品）にマルウェアを挿入する。具体的には、（偵察によって得た知識にもとづいて）組織によって使用されるハードウェア、ソフトウェアおよびファームウェアが標的になる。
組織の情報システムの構成を突いて、特殊なマルウェアをシステムに挿入する。	アドバーサリ は、組織の情報システムの構成を突いて、特殊な検知不能のマルウェアをシステムに挿入する。具体的には、組織の情報システム内の偵察結果と配置にもとづいて、基幹業務に関わる情報システムコンポーネントを標的にする。
偽の／改ざんされたハードウェアをサプライチェーンに挿入する。	アドバーサリは、正規の供給業者からのハードウェアの供給を妨害する。アドバーサリ は、そのハードウェアに変更を加えるか、あるいは欠陥のある（もしくは変更が加えられた）ハードウェアで置き換える。
改ざんした重要コンポーネントを組織のシステムに挿入する。	アドバーサリは、サプライチェーン、組織体制を転覆させようとする内部の者、あるいはそれらの組み合わせを介して、基幹業務に関わる情報システムコンポーネントを変更が加えられた、あるいは破損したコンポーネントで置き換える。
汎用のスニファーを組織が管理する情報システムまたはネットワークに挿入する。	アドバーサリは、スニッフィング用ソフトウェアを組織の内部情報システムまたはネットワークにインストールする。
執拗な標的型スニファーを組織の情報システムやネットワークに挿入する。	アドバーサリは、（連続した期間にわたって）ネットワークトラフィックを収集（傍受）できるように設計されたソフトウェアを、組織の内部情報システムまたはネットワーク内に設置する。
悪意のあるスキャンデバイス（例：無線スニファー）を施設内に挿入する。	アドバーサリは、郵便業務あるいはその他の商用配送サービスを使用して組織の郵便仕分け室に、郵便仕分け室からアクセス可能な無線通信をスキャンし、取得した情報を無線でアドバーサリに送信できるデバイスを送りつける。

脅威事象 （戦術、技法、手順によって特徴が定義される）	説明
組織体制を転覆させようとする個人を組織に送り込む。	アドバーサリは、組織のミッション／業務機能に害を与える意思があり、また、そのためのアクションを実施できる個人を組織内に送り込む。
組織体制を転覆させようとする個人を組織の特権的な地位に送り込む。	アドバーサリは、組織のミッション／業務機能に害を与える意思があり、また、そのためのアクションを実施できる個人を、組織内の特権的な地位に送り込む。アドバーサリ は、機微な情報（例：ユーザアカウント、システムファイルなど）にアクセスできるよう、特権的機能を狙う可能性があり、ある特権的機能から別の特権的機能に到達するために、そのアクセスを活用する可能性がある。
利用し、侵害する	
組織の施設に侵入するために、権限を与えられた職員の物理的なアクセスを利用する。	アドバーサリ は、権限のある個人がセキュアな／コントロールされたロケーションに入る際に、施設にアクセスしたり、物理的なセキュリティチェックを迂回する目的で後について行く（ぴったり後ろについていく）。
インターネットに晒されている、設定の不十分な情報システム、あるいは認可されていない情報システムを利用する。	アドバーサリは、インターネットへの接続が認可されていない情報システム、あるいは組織の設定に関する要求事項を満たさない情報システムに対して、インターネットを介してアクセスする。
分割されたトンネルを利用する。	アドバーサリ は、組織の情報システムまたはネットワーク、およびセキュアでないリモート接続に安全に、かつ同時に接続される外部の組織または個人の情報システム（例：遠隔地にあるラップトップ型コンピュータ）を活用する。
クラウド環境における複数利用者による共同利用を巧みに利用する。	アドバーサリは、組織が使用するクラウド環境において実施されているプロセスをもって、複数利用者による共同利用を巧みに利用し、組織のプロセスの動きを観測する、または組織の情報を取得する、もしくは組織のプロセスがタイムリーに、あるいは正確に機能するのを妨げる。
モバイルシステム（例：ノート型パソコン、携帯端末、スマートフォン）の既知の脆弱性を利用する。	アドバーサリ は、可搬型の情報システムが、組織の物理的な保護と企業のファイアウォールの論理的な保護の範囲外であるといった事実を利用して、既知の脆弱性を突いてそれらのシステムを侵害し、システムから情報を収集する。
最近発見された脆弱性を利用する。	アドバーサリ は、組織の情報システムにおいて最近発見された脆弱性を利用して、軽減手段が用意される、あるいは実施される前に、システムの侵害を試みる。
組織の内部情報システムの脆弱性を利用する。	アドバーサリは、組織の内部情報システムの既知の脆弱性を探し出し、それらの脆弱性を利用する。
ゼロデイ攻撃を使用して、脆弱性を利用する。	アドバーサリは、まだ公になっていない脆弱性を利用する攻撃を採用する。ゼロデイ攻撃は、組織によって使用される情報システムとアプリケーションに対するアドバーサリの洞察と、アドバーサリによる組織に対する偵察にもとづく。
組織のミッション／業務遂行の速さに合わせて、情報システムの脆弱性を利用する。	アドバーサリ は、ミッション／業務の遂行に関する組織のニーズとの一貫性が保たれた時間と方法で、組織に攻撃をしかける。
複数利用者による共同利用環境における安全でない、あるいは不完全なデータ削除を利用する。	アドバーサリ は、複数利用者による共同利用環境における安全でない、あるいは不完全なデータ削除を利用して、アクセス権限がない情報を取得する。
複数利用者による共同利用環境における隔離を侵害する。	アドバーサリ は、複数利用者による共同利用環境（例：クラウドコンピューティング環境）における隔離メカニズムを迂回する、あるいは打破し、ホストされたサービスおよび情報／データを観測する、または改ざんもしくはサービス拒否を引き起こす。
物理的なアクセスを介して基幹業務に関わる情報システムを侵害する。	アドバーサリ は、組織の情報システムに対する物理的なアクセスを得て、システムに変更を加える。

脅威事象 （戦術、技法、手順によって特徴が定義される）	説明
外部で使用されていて、企業に再度導入される予定の情報システムまたはデバイスを侵害する。	アドバーサリは、組織にとって外部のシステム／デバイスが再接続された際に、組織が感染するよう、それらのシステム／デバイスにマルウェアをインストールする。
組織の基幹業務に関わる情報システムのソフトウェアを侵害する。	アドバーサリ は、組織の基幹業務に関わる内部情報システムにマルウェア をインストールする、あるいはエラーを起こさせる。
組織の情報システムからのデータ／情報の取り出しを容易にするために、システムを侵害する。	アドバーサリ は、組織の内部情報システムにマルウェア を埋め込む。その後、そのマルウェアは、時間をかけて脆弱な情報を特定し、取り出す。
基幹業務に関わる情報を侵害する。	アドバーサリ は、基幹業務に関わる情報の完全性を侵害し、情報が提供される組織が業務を実施するのを阻止する、あるいは妨げる。
情報システムコンポーネント（ハードウェア、ソフトウェア、およびファームウェア）の設計、製造、および／または販売を侵害する。	アドバーサリは、選択された供給業者による、基幹業務に関わる情報システムコンポーネントの設計、製造、および／または販売を侵害する。
攻撃を実施する（すなわち、直接的な／調整された攻撃用ツールまたは活動）	
通信傍受攻撃を実施する。	アドバーサリ は、暗号化されていない通信、あるいは脆弱な暗号化（例：公に知られている欠陥を含む暗号化）を使用する通信を利用し、それらの通信を狙い、伝送される情報およびチャネルにアクセスする。
無線妨害攻撃を実施する。	アドバーサリは、通信が意図した受信者に到達するのを妨げる、あるいは阻止するために、無線通信を妨害する対策を取る。
アクセス権限のないポート、プロトコル、およびサービスを使用して、攻撃を実施する。	アドバーサリ は、その使用が組織によって認可されていない、入口と出口に対するポート、プロトコル、およびサービスを使用して、攻撃を実施する。
ペリミタを跨いで許可されている、トラフィック／データの移動を利用して、攻撃を実施する。	アドバーサリは、許可されている情報フロー（例：電子メールによる通信、取り外し可能な記憶媒体）を利用して、内部の情報システムを侵害する。これは、アドバーサリがペリミタを介して機微な情報を取得し、取り出すことを可能にする。
シンプルなサービス妨害(DoS)攻撃を実施する。	アドバーサリは、インターネットでアクセスできる資源を意図したユーザが利用できないようにする、あるいはその資源を一時的に、または永続的に効率的に機能しなくする（もしくは、まったく機能しなくする）ことを試みる。
分散型サービス妨害攻撃を実施する。	アドバーサリは、侵害された複数の情報システムを使用して、単一の標的を攻撃し、標的の情報システムのユーザに対してサービス妨害を引き起こす。
標的型サービス妨害攻撃を実施する。	アドバーサリは、依存関係について自身が有する知識にもとづいて、基幹業務に関わる情報システム、コンポーネント、または支援インフラに DoS 攻撃をしかける。
組織の施設に対して物理的攻撃を実施する。	アドバーサリは、組織に施設に対して物理的な攻撃を実施する（例：火を付ける）。
組織の施設を支援するインフラに対して物理的攻撃を実施する。	アドバーサリ は、組織の施設を支援する単一の、あるいは複数のインフラに対して、物理的な攻撃を実施する（例：水道本管を壊す、電力線を切る）。
組織の施設に対してサイバー物理攻撃を実施する。	アドバーサリは、組織の施設に対してサイバー物理攻撃を実施する（例：暖房、通気および空調の設定を遠隔で変更する）。
クラウド環境においてデータをあさる攻撃を実施する。	アドバーサリ は、クラウド環境において実施されている組織のプロセスによって使用され、その後、削除されるデータを取得する。
総当たりのログイン試行／パスワード推測攻撃を実施する。	アドバーサリ は、パスワードのランダムな推測または系統的な推測（場合によっては、パスワード解析用ユーティリティによって支援される）によって、組織の情報システムにアクセスすることを試みる。

脅威事象 （戦術、技法、手順によって特徴が定義される）	説明
非標的型ゼロデイ攻撃を実施する。	アドバーサリ は、まだ公になっていない脆弱性を利用する攻撃を採用する。攻撃は、組織の特定の脆弱性に対するアドバーサリの洞察にもとづくわけではない。
外部から開始されたセッションの乗っ取りを実施する。	アドバーサリは、組織と外部エンティティ（例：現場から離れた場所から接続しているユーザ）の間で既に確立された正規の情報システムセッションを制圧する（乗っ取る）。
内部から開始されたセッションの乗っ取りを実施する。	アドバーサリは、組織と外部エンティティ（例：遠隔地から接続しているユーザ）の間で、あるいは内部ネットワーク内の 2 つのロケーション間で既に確立された正規のセッションを制圧する（乗っ取る）といった明確な目的のもとで、組織の情報システムまたはネットワークにアクセスするために、特定のエンティティを組織内に送り込む。
外部によるネットワークトラフィック変更攻撃（介入者攻撃）を実施する。	組織のシステムの外部で活動しているアドバーサリは、組織と外部エンティティ間のセッションを傍受／通信傍受する。アドバーサリは、その後、組織のシステムと外部システムとの間でメッセージを転送し、それらのシステムがプライベート接続を介してによって互いに直接対話しているように見せかける。だが、実際のところは、すべての通信がアドバーサリによって制御されている。そうした攻撃は、組織がコミュニティクラウド／ハイブリッドクラウド／パブリッククラウドを使用する場合には、特に問題になる。
内部によるネットワークトラフィック変更攻撃（介入者攻撃）を実施する。	組織のインフラ内で活動しているアドバーサリ は、データセッションを傍受し改ざんする。
外部からのソーシャルエンジニアリングを実施して、情報を取得する。	外部に居るアドバーサリは、組織内の個人を説得または騙して、極めて重要な情報／機微な情報（例：個人情報）を開示させるための行動を取る（例：電子メールや電話を使って）。
内部からのソーシャルエンジニアリングを実施して、情報を取得する。	内部に居るアドバーサリは、組織内の個人が極めて重要な情報／機微な情報（例：ミッションに関する情報）を開示するように仕向けるための、行動を取る（例：電子メールや電話を使って）。
重要な地位にいる職員の私有のデバイスを狙って侵害する攻撃を実施する。	アドバーサリ は、組織内の重要な地位にいる職員の私有の情報システムおよびデバイス（ラップトップ型コンピュータ／ノート型パソコン、携帯端末、スマートフォン）にマルウェアを設置し、それらの職員を狙う。その目的は、職員が私有の情報システムまたはデバイスを使用して極めて重要な情報／機微な情報を処理する機会を利用することにある。
基幹業務に関わるハードウェア、ソフトウェア、またはファームウェアを狙って利用する、サプライチェーン攻撃を実施する。	アドバーサリ は、組織にとって基幹業務に関わる機能を実施するソフトウェア、ファームウェアおよびハードウェアのオペレーションを狙い、侵害する（例：ソフトウェアの場合、マルウェアを挿入することによって）。これは、市販の情報システムおよびコンポーネント、あるいは特注の情報システムおよびコンポーネントの両方に対するサプライチェーン攻撃によって、大半が達成される。
結果を達成する（すなわち、負の影響を引き起こす、情報を取得する）	
外部ネットワークのネットワークスニッフィングを介して、機微な情報を取得する。	アドバーサリは、組織（または組織の職員）が情報を伝送するのに使用する露出した有線の、あるいは無線のデータチャネル（例：売店、公衆無線ネットワーク）にアクセスして、通信を傍受する。
機微な情報を取り出して、取得する。	アドバーサリは、機微な情報を探し出し、ひそかに伝送するためのに、組織のシステムにマルウェアを送り込む。
アタッカーが選択したサービスまたは機能の低下または提供拒否を引き起こす。	アドバーサリ は、組織のミッション／業務機能の正確でタイムリーな支援を妨げるために、組織のシステムにマルウェアを送り込む。
基幹業務に関わる情報システムコンポーネントおよび機能の低下／破壊を引き起こす。	アドバーサリは、基幹業務に関わる情報システムコンポーネントを破壊する、あるいは低下を引き起こし、ミッション／業務機能を実施するための組織の能力を妨げる、あるいは排除する。アドバーサリは、こうした行為の発覚を恐れない。

脅威事象 （戦術、技法、手順によって特徴が定義される）	説明
公的にアクセス可能な情報システム上にデータを作成したり、システム上のデータを削除したり、あるいはデータを変更することによって、完全性の喪失を引き起こす。	アドバーサリ は、組織のウェブサイトまたはウェブサイト上のデータを破壊する、あるいは不正に変更を加える。
極めて重要なデータを汚染する、あるいは改ざんすることによって、完全性の喪失を引き起こす。	アドバーサリ は、極めて重要なデータに改ざんされた不正なデータを埋め込む。その結果、組織のデータ／サービスの信頼性が失われたり、次善のアクションが必要となる。
もっともらしいが偽のデータを組織の情報システムに挿入することによって、完全性の喪失を引き起こす。	アドバーサリ は、もっともらしいが偽のデータを組織の情報システムに挿入する。その結果、組織のデータ／サービスの信頼性が失われたり、次善のアクションが必要となる。
アクセス権限のあるユーザによる 、極めて重要な情報および／または機微な情報の開示を引き起こす。	アドバーサリは、（たとえば、ソーシャルエンジニアリングを介して）アクセス権限のあるユーザを誘導し、極めて重要な情報／機微な情報を不注意に露出／開示させる、あるいは取り扱いを誤らせる。
機微な情報を漏らすことによって、正規の権限によらない開示および／または利用不能を引き起こす。	アドバーサリは、組織の情報システム（デバイスとネットワークを含む）を、それらのシステムが取り扱うことを認可されていない分類レベル／機微度を有する情報を取り扱うように仕向けることによって、システムを汚染する。その情報はアクセス権限のない個人に晒されて、その情報システム、デバイス、またはネットワークはその流出が調査され、軽減されるまで、利用できない。
外部に設置された傍受用デバイスを使用して、無線ネットワークトラフィックを傍受し、情報を取得する。	アドバーサリ は、無線ネットワーク上の組織の通信を傍受する。公衆無線アクセスまたはホテルのネットワーク接続を狙うことや、家庭用または組織の無線ルーターのドライブバイ形式による破壊などが、その例である。
不正なアクセスを行う。。	アドバーサリ は、組織の情報システムに対するアクセスして、権限を越える資源にアクセスする。
公的にアクセス可能な情報システムから、機微なデータ／情報を取得する。	アドバーサリ は、組織の公的にアクセス可能なサーバーとウェブページ上の情報をスキャンしたり、あさったりして、機微な情報の発見を試みる。
機会を伺って情報システム／コンポーネントを盗んだり、あさることによって、情報を取得する。	アドバーサリは、組織の物理的な境界の外側に放置された情報システムまたはコンポーネント（例：ラップトップ型コンピュータまたはデータ記憶媒体）を盗む、あるいは、廃棄されたコンポーネントをあさる。
一連の機能の存在を維持する	
アドバーサリによる行為を気付かれないようにする。	アドバーサリ は、侵入検知システムの有効性または組織内の監査能力を阻害する行動を取る。
詳細な監視調査結果にもとづいて、サイバー攻撃を適応させる。	アドバーサリは、監視調査結果と、組織のセキュリティ対策に対応して、行動を適応させる。
活動を調整する	
多段階にわたる攻撃の活動を調整する（例：ホッピング）。	アドバーサリ は、悪意のあるコマンドまたはアクションのもとを、侵害された特定の情報システムから他の情報システムに移動し、分析を困難にする。
複数の情報システムと情報技術を跨ぐ内部からの攻撃と外部からの攻撃を組み合わせた活動を調整する。	アドバーサリ は、組織の施設内の物理的な存在と、成功を収めるためのサイバー手法の両方を必要とする攻撃を組み合わる。物理的な攻撃の各ステップは、メンテナンス要員にドアまたはキャビネットを開けたままにするよう説得するのと同じぐらい簡単である場合がある。
特定の情報を得るために、あるいは所望の成果を収めるために、複数の組織に跨る活動を調整する。	アドバーサリ は、単一の組織を狙うことに計画を制限しない。アドバーサリ は、複数の組織を観測して、対象となる標的から必要な情報を取得する。

脅威事象 （戦術、技法、手順によって特徴が定義される）	説明
既存の存在から、組織の複数のシステムに攻撃を広げるための活動を調整する。	アドバーサリは、組織のシステム内の既存の存在を使用して、自身の制御の範囲を組織の他のシステム（組織のインフラを含む）に広げる。アドバーサリ は、故に、ミッション／業務機能を実施するための組織の能力をさらに低下させることが可能な立場にある。
詳細な監視調査結果にもとづいて、継続的で、適応性のある、変化するサイバー攻撃の活動を調整する。	アドバーサリによる攻撃は、監視調査結果と、組織のセキュリティ対策に対応して、継続的に変化する。
外部（外部の者）、内部（内部の者）、およびサプライチェーン（供給業者）といった攻撃ベクトルを使用して、サイバー攻撃を調整する。	アドバーサリは、場合によっては、組織の業務を妨げる目的で、3 つのすべての攻撃ベクトルを使用して、継続的かつ調整された攻撃を採用する。

表 E-3: 代表的な例– アドバーサリによるもの以外の脅威事象

脅威事象	説明
機微な情報が漏えいする	権限のあるユーザが、デバイス、情報システム、またはネットワークに、それらが取り扱うことを認可されていない分類レベル／機微度を有する情報を格納する、あるいはそうした情報を送信することによって、それらを誤って汚染させてしまう。その情報は、アクセス権限のないユーザによるアクセスに晒されてしまい、結果としてその情報システム、デバイス、またはネットワークは、その流出が調査され、軽減されるまで利用できない。
権限を与えられた特権ユーザによって、極めて重要な情報および／または機微な情報が手荒に扱われる	権限を与えられた特権ユーザが、極めて重要な情報／機微な情報を誤って露出させる。
特権の設定が正しくない	権限を与えられた特権ユーザまたはアドミニストレータが誤って、あるユーザに対して例外的な権限を与えてしまう、あるいは資源に対する権限要求事項を極端に低く設定してしまう。
通信が競合する	競合が原因で、通信性能が低下する。
表示が判読できない	老化した機器であるために、表示が判読できない。
一次的な施設で地震が発生する	一次的な施設で、組織が定めたマグニチュードの地震が発生し、施設が使用不可能になる。
一次的な施設で火事が発生する	一次的な施設で、（アドバーサリによる活動に起因しない）火事が発生し、施設が使用不可能になる。
二次的な施設で火事が発生する	二次的な施設で、（アドバーサリによる活動に起因しない）火事が発生し、施設が使用不可能になる、あるいはソフトウェア、設定、データ、および／またはログのバックアップが完全に使えなくなる。
一次的な施設で洪水が発生する	一次的な施設で、（アドバーサリによる活動に起因しない）洪水が発生し、施設が使用不可能になる。
二次的な施設で洪水が発生する	二次的な施設で、（アドバーサリによる活動に起因しない）洪水が発生し、施設が使用不可能になる、あるいはソフトウェア、設定、データ、および／またはログのバックアップが完全に使えなくなる。
一次的な施設でハリケーンが発生する	一次的な施設で、組織が定めた強度のハリケーンが発生し、施設が使用不可能になる。
二次的な施設でハリケーンが発生する	二次的な施設で、組織が定めた強度のハリケーンが発生し、施設が使用不可能になる、あるいはソフトウェア、設定、データ、および／またはログのバックアップが完全に使えなくなる。
資源が枯渇する	資源が枯渇し、処理性能が低下する。

脅威事象	説明
ソフトウェア製品に脆弱性が発生する	プログラミング言語およびソフトウェア開発環境に内在する欠陥に起因して、よく使われるソフトウェア製品にエラーと脆弱性が生じる。
ディスクのエラーが発生する	ディスクのエラーに起因して、ストレージが駄目になる。
ディスクのエラーが広範囲に及ぶ	同一の供給業者から同時に調達した一連のデバイスの老化に起因して、複数のディスクエラーが発生する。
一次的な施設で暴風／竜巻が発生する	一次的な施設で、組織が定めた強度の暴風／竜巻が発生し、施設が使用不可能になる。
二次的な施設で暴風／竜巻が発生する	二次的な施設で、組織が定めた強度の暴風／竜巻が発生し、施設が使用不可能になる、あるいはソフトウェア、設定、データおよび／またはログのバックアップが完全に使えなくなる。

表 E-4:脅威事象間の関連性

値	説明
確認された (Confirmed)	脅威事象または TTP（戦術、技法、および手順）が、その組織によって目撃された。
予期された (Expected)	脅威事象または TTP が、その組織のピアまたはパートナーによって目撃された。
予期された (Anticipated)	脅威事象または TTP が、信頼できる情報源によって報告された。
予言された (Predicted)	脅威事象または TTP が、信頼できる情報源によって予言された。
可能性がある (Possible)	脅威事象または TTP が、ある程度信頼できる情報源によって述べられた。
該当なし	脅威事象または TTP が、現時点では当てはまらない。たとえば、ある脅威事象または TTP が、組織、ミッション／業務プロセス、エンタープライズアーキテクチャのセグメント、または情報システムに存在しない特定の技術、アーキテクチャ、またはプロセスを前提としている場合; あるいは存在しない素因的条件（例：洪水面に位置している）を前提としている場合。別のケースとして、組織が詳細な、あるいは具体的な脅威関連情報を使用していて、アドバーサリによって脅威事象が開始される、あるいは TTP が使用される可能性がないことがその情報によって示される場合には、その脅威事象または TTP は当てはまらないとみなすことができる。

表 E-5:テンプレート– 脅威事象の特定

識別子	脅威事象の情報源	脅威源	関連性
組織が定めた	表 E-2、表 E-3、タスク 1-4 あるいは 組織が定めたもの	表 D-7、表 D-8 あるいいは 組織が定めたもの	表 E-4、あるいは 組織が定めたもの

付録 F

脆弱性と素因的条件

脅威が成功裏に利用される可能性に影響を及ぼすリスク因子

本付録は、以下を提供する：(i)「脆弱性と素因的条件の特定」タスクに対する有用であると考えられる入力データについての説明; (ii) 素因的条件の分類体系の例; (iii) 脆弱性の重大さと、素因的条件の広がりをアセスメントするための、アセスメントスケールの例; ならびに (iv)「脆弱性と素因的条件の特定」タスクの結果を要約し、文書化するための、一連のテンプレート。本付録の分類体系とアセスメントスケールは、組織が開始点として使用することができるが、組織固有の条件に合わせて適切に調整する必要があるだろう。タスク 2-3 のアウトプットである表 F-3 と表 F-6 は、付録 I のリスク一覧に対して、関連する入力データを提供する。

表 F-1：入力データ – 脆弱性と素因的条件

説明	以下の層に提供される		
	第 1 層	**第 2 層**	**第 3 層**

第 1 層から：（組織レベル）
- 信頼できるとみなされた、脅威関連情報の情報源（例：オープンソースおよび／または機密扱いの脆弱性報告、前に実施されたリスク／脆弱性アセスメント、ミッションへの影響分析／ビジネス影響分析）。(**セクション 3.1、タスク 1-4**)
- 第 1 層に特化した、脆弱性関連情報および手引き（例：組織のガバナンス、主要なミッション／業務機能、管理／運用上のポリシー、手順、および構造、外部のミッション／業務との関係などに関連する脆弱性）。
- 素因的条件の分類体系、（必要ならば、組織によって注釈が付けられる）。(**表 F-4**)
- 脆弱性 と 素因的条件の特徴定義
  - 脆弱性の重大さをアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。(**表 F-2**)
  - 素因的条件の広がりをアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。(**表 F-5**)
  - 組織の事業継続計画と業務継続計画（組織全体に対して、そうした計画が定められている場合）。
	いいえ	はい	はい
			もしそうでないなら第 2 層にて提供される

第 2 層から：（ミッション／業務プロセスレベル） - 第 2 層に特化した、脆弱性関連情報および手引き（例：組織のミッション／業務プロセス、エンタープライズアーキテクチャのセグメント、共通インフラ、支援サービス、共通管理策、および外部依存などに関連する脆弱性）。 - 事業継続計画、ミッション／業務プロセスに対する業務の継続（個別のプロセスまたは事業単位ごとに、そうした計画が定められている場合）。	はい （RAR を介して）	はい （ピア共有を介して）	はい
第 3 層から：（情報システムレベル） - 第 3 層に特化した、脆弱性関連情報および手引き（例：情報システム、情報技術、情報システムコンポーネント、アプリケーション、ネットワーク、運用環境などに関連する脆弱性）。 - セキュリティアセスメント報告（すなわち、脆弱性として特定された、アセスメントされた管理策の欠陥）。 - モニタリング活動の結果（例：自動化された／自動化されていないデータ入力）。 - 脆弱性アセスメント、Red Team による報告、あるいは情報システム、サブシステム、IT 製品、デバイス、ネットワーク、またはアプリケーションの分析から得られたその他の報告。 - 緊急時対応計画、災害復旧計画、インシデント報告。 - ベンダー／製造会社が提供する脆弱性報告。	はい （RAR を介して）	はい （RAR を介して）	はい （ピア共有を介して）

表 F-2: アセスメントスケール – 脆弱性の重大さ

定性的な値	半定量的な値		説明
非常に高い	96-100	10	その脆弱性が晒されていて、利用可能であり、その脆弱性が利用された結果、深刻な影響がもたらされる。 関連するセキュリティ管理策または改善対策が導入されていない、あるいは導入が計画されていない、もしくは、その脆弱性を修正するためのセキュリティ管理策を特定できない。
高い	80-95	8	その脆弱性が晒されていて、利用しやすいこと、および／またはその脆弱性が利用された結果もたらされる影響の重大さからして、非常に懸念される。 関連するセキュリティ管理策、あるいはその他の改善対策が、導入が計画されているものの、導入されていない。補完的管理策が導入されていて、少なくとも、わずかな効果がある。
中間	21-79	5	その脆弱性が晒されていて、利用しやすいこと、および／またはその脆弱性が利用された結果もたらされる影響の重大さからして、適度に懸念される。 関連するセキュリティ管理策、あるいはその他の改善対策が部分的に導入されていて、ある程度効果がある。
低い	5-20	2	その脆弱性が少し懸念されるが、改善対策の効果が向上する可能性がある。 関連するセキュリティ管理策、あるいはその他の改善対策が十分に導入されていて、ある程度効果がある。
非常に低い	0-4	0	その脆弱性は、問題にならない。 関連するセキュリティ管理策、あるいはその他の改善対策がフルに導入、アセスメントされていて、効果がある。

表 F-3::テンプレート – 脆弱性の特定

識別子	脆弱性の 情報源	脆弱性の重大さ
組織が定めたもの	タスク 2-3、タスク 1-4 または 組織が定めたもの	表 F-2 または 組織が定めたもの

表 F-4:素因的条件の分類体系

素因的条件のタイプ	説明
情報関連 - 機密扱いの国家安全保障に関する情報 - コンパートメント - 管理された、非機密扱いの情報 - 個人情報 - 特殊なアクセスの導入計画 - 契約によって定められた - NOFORN(他国への開示禁止) -知財	情報の機微度(あるいは機微度の欠落)、法律または規制上の要求事項、および/または契約上の合意やその他の合意にもとづいて、(情報の作成、伝送、格納、処理、および/または表示の際に)特殊な方法で情報を扱う必要がある。
技術上の - 構造上の - 技術標準への準拠 - 特定の製品または製品種目の使用 - ユーザベースの協調および情報共有のためのソリューションおよび/またはアプローチ - 特定のセキュリティ機能の共通管理策への割り当て - 機能上の - ネットワークでつながっている複数のユーザ - 単一ユーザ -スタンドアロン型/ネットワークでつながっていない - 限られた機能(例:通信、センサー、組込コントローラ)	特殊な方法で技術を使う必要がある。
組織/環境上の - モビリティ - 定位置の(ロケーションを指定) - (半モバイル) - 地上にある、飛行している、水上の、宇宙ベースの - モバイル(例:携帯端末) - 情報システムコンポーネント、ミッション/業務プロセス、エンタープライズアーキテクチャのセグメントに対する物理的/論理的アクセスを有する人々 - それらの人々の規模 - それらの人々の身上調査/信用度調査	組織の環境によって提供される物理的な管理策、手続き上の管理策、および 職員による管理策に依存できること。

表 F-5: アセスメントスケール – 素因的条件の広がり

定性的な値	半定量的な値		説明
非常に高い	96-100	10	組織の**すべての**ミッション/業務機能(第 1 層)、ミッション/業務プロセス(第 2 層)、または情報システム(第 3 層)に適用される。
高い	80-95	8	組織の**大半の**ミッション/業務機能(第 1 層)、ミッション/業務プロセス(第 2 層)、または情報システム(第 3 層)に適用される。
中間	21-79	5	組織の**多くの**ミッション/業務機能(第 1 層)、ミッション/業務プロセス(第 2 層)、または情報システム(第 3 層)に適用される。
低い	5-20	2	組織の**一部の**ミッション/業務機能(第 1 層)、ミッション/業務プロセス(第 2 層)、または情報システム(第 3 層)に適用される。
非常に低い	0-4	0	組織の**少数の**ミッション/業務機能(第 1 層)、ミッション/業務プロセス(第 2 層)、または情報システム(第 3 層)に適用される。

表 F-6: テンプレート – 素因的条件の特定

識別子	素因的条件の 情報源	条件の 広がり
組織が定めたもの	表 F-4、タスク 1-4 または 組織が定めたもの	表 F-5 または 組織が定めたもの

付録 G

発生の可能性

脅威事象が負の影響をもたらす可能性を特定する

本付録は、以下を提供する：(i)「発生可能性 [56] の特定」タスクに対する有用であると考えられる入力データについての説明; ならびに (ii) 脅威事象が開始される／発生する可能性、脅威事象が負の影響をもたらす可能性、および開始された／発生した脅威事象が組織の業務、資産、または個人に被害をもたらす総合的な可能性をアセスメントするための、アセスメントスケールの例。本付録のアセスメントスケールは、組織が開始点として使用することができるが、組織固有の条件に合わせて適切に調整する必要があるだろう。タスク 2-4 のアウトプットである表 G-2、G-3、G-4 と表 G-5 は、付録 I のリスク一覧に対して、関連する入力データを提供する。

表 G-1：入力データ – 可能性の特定

説明	以下の層に提供される		
	第 1 層	**第 2 層**	**第 3 層**
第 1 層から：（組織レベル） - 第 1 層に特化した、可能性関連情報および手引き（例：組織のガバナンス、主要なミッション／業務機能、管理／運用上のポリシー、手順、および構造、外部のミッション／業務との関係などに関連する発生可能性）。 - さらなる考慮を必要としない、組織全体にわたる発生可能性に関する手引き。 - 脅威事象が開始される可能性（アドバーサリによる脅威事象の場合）をアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。**(表 G-2)** - 脅威事象が発生する可能性（アドバーサリによるもの以外の脅威事象の場合）をアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。**(表 G-3)** - 脅威事象が負の影響をもたらす可能性をアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。**(表 G-4)** - 開始された／発生した脅威事象が負の影響をもたらす総合的な可能性をアセスメントするためのアセスメントスケール（必要ならば、組織によって注釈が付けられる）。**(表 G-5)**	いいえ	はい	はい もしそうでないなら第 2 層にて提供される
第 2 層から：（ミッション／業務プロセスレベル） - 第 2 層に特化した、可能性関連情報および手引き（例：ミッション／業務プロセス、エンタープライズアーキテクチャのセグメント、共通インフラ、支援サービス、共通管理策、および外部依存に関連する可能性情報）。	はい（RAR を介して）	はい（ピア共有を介して）	はい
第 3 層から：（情報システムレベル） - 第 3 層に特化した、可能性関連情報および手引き（例：情報システム、情報技術、情報システムコンポーネント、アプリケーション、ネットワーク、運用環境などに関連する可能性情報）。 - 成功した／失敗したサイバー攻撃の履歴データ、攻撃の検出率。 - セキュリティアセスメント報告（すなわち、脆弱性として特定された、アセスメントされた管理策の欠陥）。	はい（RAR を介して）	はい（RAR を介して）	はい（ピア共有を介して）

[56] 本ガイドラインで論じられている「発生可能性(likelihood)」という用語は、厳密な意味での「発生可能性」ではない。むしろ、「発生可能性」のスコアである。リスクアセサーは、統計的な意味で「発生可能性」の関数を定義するわけではない。むしろ、リスクアセサーは、入手可能な証拠、経験、および専門的な判断にもとづいて、スコアを割り当てる（あるいは「発生可能性」のアセスメントを実施する）。したがって標的、意図、および能力などの要素の組み合わせは、脅威が開始される可能性を表すスコアを生成するのに使用できる。また、能力と、脆弱性の重大さなどの要素の組み合わせは、負の影響がもたらされる可能性を表すスコアを生成するのに使用できる。さらに、それらのスコアの組み合わせは、総合的な可能性を表すスコアを生成するのに使用できる。

- 継続的なモニタリング活動の結果（例：自動化された／自動化されていないデータ入力） - 脆弱性アセスメント、Red Team による報告、あるいは情報システム、サブシステム、IT 製品、デバイス、ネットワーク、またはアプリケーションの分析から得られたその他の報告。 - 緊急時対応計画、災害復旧計画、インシデント報告。 - ベンダー／製造会社が提供する脆弱性報告。			

表 G-2：アセスメントスケール – 脅威事象が開始される可能性（アドバーサリによる脅威事象の場合）

定性的な値	半定量的な値		説明
非常に高い	96-100	10	アドバーサリが脅威事象を開始するのは**ほぼ確実である。**
高い	80-95	8	アドバーサリが脅威事象を開始する**可能性は高い。**
中間	21-79	5	アドバーサリが脅威事象を開始する**可能性はある程度ある。**
低い	5-20	2	アドバーサリが脅威事象を開始する**可能性は低い。**
非常に低い	0-4	0	アドバーサリが脅威事象を開始する**可能性はほとんどない。**

表 G-3：アセスメントスケール – 脅威事象が発生する可能性（アドバーサリによるもの以外の脅威事象の場合）

定性的な値	半定量的な値		説明
非常に高い	96-100	10	エラー、アクシデント、または天災が発生するのは**ほぼ確実である、**あるいは **1 年間に 100 回以上**発生する。.
高い	80-95	8	エラー、アクシデント、または天災が発生する**可能性は高い、**あるいは **1 年間に 10 回ないし 100 回**発生する。.
中間	21-79	5	エラー、アクシデント、または天災が発生する**可能性はある程度ある、**あるいは **1 年間に 1 回ないし 10 回**発生する。.
低い	5-20	2	エラー、アクシデント、または天災が発生する**可能性は低い、**あるいは **1 年間に1回未満**発生するが、**10 年おきに 2 回以上**発生する。。.
非常に低い	0-4	0	エラー、アクシデント、または天災が発生する**可能性はほとんどない、**. あるいは **10 年おきに1回未満**発生する。

表 G-4：アセスメントスケール – 脅威事象が負の影響をもたらす可能性

定性的な値	半定量的な値		説明
非常に高い	96-100	10	脅威事象が開始された／発生した場合、負の影響がもたらされるのは**ほぼ確実である。**
高い	80-95	8	脅威事象が開始された／発生した場合、負の影響がもたらされる**可能性は高い。**
中間	21-79	5	脅威事象が開始された／発生した場合、負の影響がもたらされる**可能性はある程度ある。**
低い	5-20	2	脅威事象が開始された／発生した場合、負の影響がもたらされる**可能性は低い。**
非常に低い	0-4	0	脅威事象が開始された／発生した場合、負の影響がもたらされる**可能性はほとんどない。**

表 G-5:アセスメントスケール – 総合的な可能性

脅威事象が開始される／発生する可能性	脅威事象が負の影響をもたらす可能性				
	非常に低い	**低い**	**中間**	**高い**	**非常に高い**
非常に高い	低い	中間	高い	非常に高い	非常に高い
高い	低い	中間	中間	高い	非常に高い
中間	低い	低い	中間	中間	高い
低い	非常に低い	低い	低い	中間	中間
非常に低い	非常に低い	非常に低い	低い	低い	低い

付録 H

影響

脅威事象が組織、個人および国家にもたらす影響

本付録 は、以下を提供する: (i)「影響の特定」タスクに対する有用であると考えられる入力データについての説明; (ii) 組織の業務と資産、個人、他の組織、または国家に対する負の影響の典型的な例; (iii) 脅威事象がもたらす影響と、影響の範囲をアセスメントするための、アセスメントスケールの例; ならびに (iv) タスク 2-5(「影響の特定」)の結果を要約し、文書化するためのテンプレート。本付録のアセスメントスケールは、開始点として使用することができるが、組織固有のあらゆる条件に合わせて適切に調整する必要があるだろう。タスク 2-5 のアウトプットである表 H-4 は、付録 I のリスク一覧に対して、関連する入力データを提供する。

表 H-1:: 入力データ – 影響の特定

説明	以下の層に提供される		
	第 1 層	**第 2 層**	**第 3 層**
第 1 層から:(組織レベル) - 第 1 層に特化した、影響関連情報および手引き(例:組織のガバナンス、主要なミッション／業務機能、管理／運用上のポリシー、手順、および構造、外部のミッション／業務との関係などに関連する影響情報)。 - さらなる考慮を必要としない、組織全体にわたる影響に関する手引き。 - 極めて重要なミッション／業務機能の特定。 - 影響の例(必要ならば、組織によって注釈が付けられる)。**(表 H-2)** - 脅威事象がもたらす影響をアセスメントするためのアセスメントスケール(必要ならば、組織によって注釈が付けられる)。**(表 H-3)**	いいえ	はい	はい もしそうでないなら第 2 層にて提供される
第 2 層から:(ミッション／業務プロセスレベル) - 第 2 層に特化した、影響関連情報および手引き(例:ミッション／業務プロセス、エンタープライズアーキテクチャのセグメント、共通インフラ、支援サービス、共通管理策、および外部依存などに関連する脅威関連情報)。 - 価値の高い資産の特定。	はい (RAR を介して)	はい (ピア共有を介して)	はい
第 3 層から:(情報システムレベル) - 第 3 層に特化した、影響関連情報および手引き(例:情報システム、情報技術、情報システムコンポーネント、アプリケーション、ネットワーク、運用環境などに影響を及ぼす、可能性関連の情報)。 - 成功した／失敗したサイバー攻撃の履歴データ、攻撃の検出率。. - セキュリティアセスメント報告(すなわち、脆弱性として特定された、アセスメントされた管理策の欠陥)。 - 継続的なモニタリング活動の結果(例:自動化された／自動化されていないデータ入力) - 脆弱性アセスメント、Red Team による報告、あるいは情報システム、サブシステム、IT 製品、デバイス、ネットワーク、またはアプリケーションの分析から得られたその他の報告。 - 緊急時対応計画、災害復旧計画、インシデント報告。	はい (RAR を介して)	はい (RAR を介して)	はい (ピア共有を介して)

表 H-2:負の影響の例

影響のタイプ	影響

業務にもたらされる被害	- 現行のミッション／業務機能を実施できない。
	  - 十分にタイムリーに。
	  - 十分な自信および／または正確さをもって。
	  - 計画された資源の制約内で。
	- 将来にわたってミッション／業務機能を実施できない、あるいは、その能力に限りがある。
	  - ミッション／業務機能を回復できない。
	  - 十分にタイムリーに。
	  - 十分な自信および／または正確さをもって。
	  - 計画された資源の制約内で。
	- ノンコンプライアンスに起因する被害(例:金銭上のコスト、制裁措置)。
	  - 該当する法律または規制に対して。
	  - 契約要求事項、あるいは、拘束力のある契約上のその他の要求事項(例:法的責任)に対して。
	- 直接的な金銭上のコスト。
	- 相関的な被害。
	  - 信頼関係が損なわれる。
	  - イメージまたは評判が損なわれる(かつ、将来にわたる、あるいは可能性のある信頼関係も損なわれる)。

資産にもたらされる被害	- 物理的施設に対する損害、あるいは、その喪失。 - 情報システムまたはネットワークに対する損害、あるいは、その喪失。 - 情報技術または機器に対する損害、あるいは、その喪失。 - 構成部品または供給品に対する損害、あるいは、その喪失。 - 情報資産に対する損害、あるいは、その喪失。 - 知的財産の喪失。
個人にもたらされる被害	- 人命に対する危害、または人命の損失。 - 身体的または精神的な虐待。 - なりすまし犯罪。 - 個人情報の喪失。 - イメージまたは評判が損なわれる。

他の組織にもたらされる被害	- ノンコンプライアンスに起因する被害(例:金銭上のコスト、制裁措置)。
	  - 該当する法律または規制に対して。
	  - 契約要求事項、あるいは、拘束力のある契約上のその他の要求事項。
	- 直接的な金銭上のコスト。
	- 相関的な被害。
	  - 信頼関係が損なわれる。
	  - 評判が損なわれる(かつ、将来にわたる、あるいは可能性のある信頼関係も損なわれる)。

国家にもたらされる被害	- 極めて重要なインフラ部門に対する損害、あるいは、その能力が奪われる。
	- 政府の運用継続性の喪失。
	- 相関的な被害。
	  - 他の政府との間の信頼関係、あるいは政府機関以外の機関との間の信頼関係が損なわれる。
	  - .国家の評判が損なわれる(かつ、将来にわたる、あるいは可能性のある信頼関係も損なわれる)。
	- 国家の目的を果たすための現行の、あるいは将来にわたる能力が損なわれる。
	  - 国家安全保障に対する被害。

表 H-3:アセスメントスケール – 脅威事象の影響

定性的な値	半定量的な値		説明
非常に高い	96-100	10	その脅威事象が、組織の業務、組織の資産、個人、他の組織、または国家に対して、複数の**深刻な、または壊滅的な**負の影響をもたらすことが予期される。
高い	80-95	8	その脅威事象が、組織の業務、組織の資産、個人、他の組織、または国家に対して、単一の**深刻な、または壊滅的な**負の影響をもたらすことが予期される。深刻な、または壊滅的な負の影響とは、たとえば、(i) 組織が、組織の主要な機能の内1つ、あるいは複数の機能を実施することができないといった程度と期間にわたって、ミッション遂行能力を低下させる、あるいは失わせる; (ii) 組織の資産に大規模な被害をもたらす; (iii) 金銭上の大きな損失をもたらす; あるいは (iv) 個人に深刻な、または壊滅的な被害（人命の損失、または命にかかわる負傷を含む）をもたらす、脅威事象を意味する。
中間	21-79	5	その脅威事象が、組織の業務、組織の資産、個人、他の組織、または国家に対して、単一の**深刻な**負の影響をもたらすことが予期される。深刻な負の影響とは、たとえば、(i) 組織が、組織の主要な機能を実施することはできるものの、それらの機能の効果が大幅に減少するといった程度と期間にわたって、ミッション遂行能力を大幅に低下させる; (ii) 組織の資産にかなりの被害をもたらす; (iii) 金銭上のかなりの損失をもたらす; あるいは (iv) 個人にかなりの被害（ただし、人命の損失、または命にかかわる負傷を含まない）をもたらす、脅威事象を意味する。
低い	5-20	2	その脅威事象が、組織の業務、組織の資産、個人、他の組織、または国家に対して、単一の**限られた**負の影響をもたらす可能性がある。限られた負の影響とは、たとえば、(i) 組織が、組織の主要な機能を実施することはできるものの、それらの機能の効果が著しく減少するといった程度と期間にわたって、ミッション遂行能力を低下させる; (ii) 組織の資産に軽微な被害をもたらす; (iii) 金銭上の軽微な損失をもたらす; あるいは (iv) 個人に軽微な被害をもたらす、脅威事象を意味する。
非常に低い	0-4	0	その脅威事象が、組織の業務、組織の資産、個人、他の組織、または国家に対して単一の**取るに足りない**負の影響をもたらす可能性がある。

表 H-4:テンプレート – 負の影響の特定

影響のタイプ	影響 影響を受けた資産	最大の影響
表 H-2 または 組織が定めたもの	表 H-2 または 組織が定めたもの	表 H-3 または 組織が定めたもの

付録 I

リスクの判断

組織、個人および国家に対するリスクをアセスメントする

本付録 は、以下を提供する: (i)「リスクの判断」タスクに対する有用であると考えられる入力データについての説明(判断における不確実性についての考慮事項を含む); (ii) リスクのレベルをアセスメントするためのアセスメントスケールの例; (iii) アドバーサリによるリスクの判断、およびアドバーサリによるもの以外のリスクの判断のための内容(すなわち、データ入力)について説明する表; ならびに (iv) タスク 2-6(「リスクの判断」)の結果を要約し、文書化するためのテンプレート。本付録のアセスメントスケールは、開始点として使用することができるが、組織固有のあらゆる条件に合わせて適切に調整する必要があるだろう。表 I-5(アドバーサリによるリスク)と表 I-7(アドバーサリによるもの以外のリスク)は、タスク 2-6 のアウトプットである。

表 I-1: 入力データ – リスク

説明	以下の層に提供される		
	第 1 層	**第 2 層**	**第 3 層**
第 1 層から: (組織レベル) - 組織全体にわたって使用できるようにした、リスク源および不確実性関連の情報(例:アドバーサリの能力、意図、および標的などの、可能性を特定するのに役立つ具体的な情報)の情報源 - さらなる考慮を必要としない、組織全体にわたるリスク(不確実性を含む)に関する手引き。 - 不確実性を特定するための基準。 - 前に実施されたリスクアセスメントによって特定された、リスクの高い事象の一覧 - 発生可能性と影響の組み合わせであるリスクのレベルをアセスメントするためのアセスメントスケール(必要ならば、組織によって注釈が付けられる)。**(表 I-2)** - リスクのレベルをアセスメントするためのアセスメントスケール(必要ならば、組織によって注釈が付けられる)。**(表 I-3)**	いいえ	はい	はい もしそうでないなら第 2 層にて提供される
第 2 層から: (ミッション／業務プロセスレベル) - 第 2 層に特化した、リスク関連情報および手引き(例:ミッション／業務プロセス、エンタープライズアーキテクチャのセグメント、共通インフラ、支援サービス、共通管理策、および外部依存に関連する、リスクおよび不確実性関連の情報)。	はい (RAR を介して)	はい (ピア共有を介して)	はい
第 3 層から: (情報システムレベル) - 第 3 層に特化した、リスク関連情報および手引き(例:情報システム、情報技術、情報システムコンポーネント、アプリケーション、ネットワーク、運用環境などに影響を及ぼす、可能性関連の情報)。	はい (RAR を介して)	はい (RAR を介して)	はい (ピア共有を介して)

表 I-2: アセスメントスケール – (発生可能性と影響の組み合わせである)リスクのレベル

可能性 **(脅威事象が発生し、負の影響をもたらす可能性)**	**影響レベル**				
	非常に低い	**低い**	**中間**	**高い**	**非常に高い**
非常に高い	非常に低い	低い	中間	高い	非常に高い
高い	非常に低い	低い	中間	高い	非常に高い

中間	非常に低い	低い	中間	中間	高い
低い	非常に低い	低い	低い	低い	中間
非常に低い	非常に低い	非常に低い	非常に低い	低い	低い

表 I-3：アセスメントスケール – リスクのレベル

定性的な値	半定量的な値		説明
非常に高い	96-100	10	**非常に高いリスク**とは、その脅威事象が組織の業務、組織の資産、個人、他の組織、または国家に対して、複数の**深刻な、または壊滅的な**負の影響をもたらすことが予期されることを意味する。
高い	80-95	8	**高いリスク**とは、その脅威事象が組織の業務、組織の資産、個人、他の組織、または国家に対して、単一の**深刻な、または壊滅的な**負の影響をもたらすことが予期されることを意味する。
中間	21-79	5	**中間のリスク**とは、その脅威事象が組織の業務、組織の資産、個人、他の組織、または国家に対して、単一の**深刻な**負の影響をもたらすことが予期されることを意味する。
低い	5-20	2	**低いリスク**とは、その脅威事象が組織の業務、組織の資産、個人、他の組織、または国家に対して、単一の**限られた**負の影響をもたらすことが予期されることを意味する。
非常に低い	0-4	0	**非常に低いリスク**とは、その脅威事象が組織の業務、組織の資産、個人、他の組織、または国家に対して、単一の**無視できる**負の影響をもたらすことが予期されることを意味する。

表 I-4：アドバーサリによるリスク一覧の各欄の説明

カラム	見出し	内容
1	脅威事象	脅威事象を特定する。（**タスク 2-2**; **表 E-1**; **表 E-2**; **表 E-5**; **表 I-5**）
2	脅威源	脅威事象を開始する可能性のある脅威源を特定する。（**タスク 2-1**; **表 D-1**; **表 D-2**; **表 D-7**; **表 I-5**）
3	能力	脅威源の能力をアセスメントする。（**タスク 2-1**; **表 D-3**; **表 D-7**; **表 I-5**）
4	意図	脅威源の意図をアセスメントする。（**タスク 2-1**; **表 D-4**; **表 D-7**; **表 I-5**）
5	標的	脅威源の標的をアセスメントする。（**タスク 2-1**; **表 D-5**; **表 D-7**; **表 I-5**）
6	関連性	脅威事象間の関連性を特定する。（**タスク 2-2**; **表 E-1**; **表 E-4**; **表 E-5**; **表 I-5**） 脅威事象間の関連性が; さらなる考慮の必要性に関する組織の基準を満たさない場合には z 残りのカラムはスキップする。
7	攻撃が開始される可能性	単一の、あるいは複数の脅威源が脅威事象を開始する可能性を、脅威源の能力、意図、および標的を考慮に入れて特定する。（**タスク 2-4**; **表 G-1**; **表 G-2**; **表 I-5**）
8	脆弱性 と 素因的条件	脅威事象を開始した脅威源によって利用される可能性のある 脆弱性と、負の影響がもたらされる可能性を増加させ 8 る素因的条件を特定する（**タスク 2-5**; **表 F-1**; **表 F-3**; **表 F-4**; **表 F-6**; **表 I-5**）
9	重大さと 広がり	脆弱性の重大さと、素因的条件の広がりをアセスメントする。（**タスク 2-5**; **表 F-1**; **表 F-2**; **表 F-5**; **表 F-6**; **表 I-5**）
10	開始された攻撃が成功する可能性	一度開始された脅威事象が負の影響をもたらす可能性を、脅威源の能力、脆弱性および素因的条件を考慮に入れて特定する。（**タスク 2-4**; **表 G-1**; **表 G-4**; **表 I-5**）
11	総合的な可能性	脅威事象が開始されて、負の影響をもたらす可能性（すなわち、攻撃が開始される可能性と、開始された攻撃が成功する可能性の組み合わせ）を特定する。（**タスク 2-4**; **表 G-1**; **表 G-5**; **表 I-5**）
12	影響のレベル	脅威事象がもたらす負の影響（すなわち、組織の業務、組織の資産、個人、他の組織、または国家にもたらされる可能性のある被害）を特定する。（**タスク 2-5**; **表 H-1**; **表 H-2**; **表 H-3**; **表 H-4**; **表 I-5**）
13	リスク	開始の可能性と影響の組み合わせであるリスクのレベルを判断する。（**タスク 2-6**; **表 I-1**; **表 I-2**; **表 I-3**; **表 I-5**）

表 I-5：テンプレート– アドバーサリによるリスク

1	2	3	4	5	6	7	8	9	10	11	12	13
脅威事象	脅威源	脅威源の特徴			関連性	攻撃が開始される可能性	脆弱性と素因的条件	重大さと広がり	開始された攻撃が成功する可能性	総合的な可能性	影響のレベル	リスク
		能力	意思	標的								

表 I-6:アドバーサリによるもの以外のリスク一覧の一般的な説明

カラム	見出し	内容
1	脅威事象	脅威事象を特定する。(**タスク 2-2**; **表 E-1**; **表 E-3**; **表 E-5**; **表 I-7**)
2	脅威源	脅威事象を開始する可能性のある脅威源を特定する。(**タスク 2-1**; **表 D-1**; **表 D-2**; **表 D-8**; **表 I-7**)
3	影響の範囲	脅威源がもたらす影響の範囲を特定する。(**タスク 2-1**; **表 D-1**; **表 D-6**; **表 I-7**)
4	関連性	脅威事象間の関連性を特定する。(**タスク 2-2**; **表 E-1**; **表 E-4**; **表 E-5**; **表 I-7**) 脅威事象間の関連性が、さらなる考慮の必要性に関する組織の基準を満たさない場合には、残りのカラムはスキップする。
5	脅威事象が発生する可能性	脅威事象が発生する可能性を特定する。(**タスク 2-4**; **表 G-1**; **表 G-3**; **表 I-7**)
6	脆弱性と 素因的条件	脅威事象を開始した脅威源によって利用される可能性のある 脆弱性と、負の影響がもたらされる可能性を増加させる素因的条件を特定する(**タスク 2-5**; **表 F-1**; **表 F-3**; **表 F-4**; **表 F-6**; **表 I-7**)
7	重大さと 広がり	脆弱性の重大さと、素因的条件の広がりをアセスメントする。(**タスク 2-5**; **表 F-1**; **表 F-2**; **表 F-5**; **表 F-6**; **表 I-5**)
8	脅威事象が負の影響をもたらす可能性	一度開始された脅威事象が負の影響をもたらす可能性を、脆弱性と 素因的条件を考慮に入れて特定する。(**タスク 2-4**; **表 G-1**; **表 G-4**; **表 I-7**)
9	全滝的な可能性	脅威事象が発生して、負の影響をもたらす可能性(すなわち、脅威が発生する可能性と、その脅威事象が負の影響をもたらす可能性の組み合わせ)を特定する。(**タスク 2-4**; **表 G-1**; **表 G-5**; **表 I-7**)
10	影響のレベル	脅威事象がもたらす負の影響(すなわち、組織の業務、組織の資産、個人、他の組織、または国家にもたらされる可能性のある被害)を特定する。(**タスク 2-5**; **表 H-1**, **表 H-2**; **表 H-3**; **表 H-4**; **表 I-7**)
11	リスク	発生可能性と影響の組み合わせであるリスクのレベルを判断する。(**タスク 2-6**; **表 I-1**; **表 I-2**; **表 I-3**; **表 I-7**)

表 I-7:テンプレート– アドバーサリによるもの以外のリスク

1	2	3	4	5	6	7	8	9	10	11
脅威事象	**脅威源**	**影響の範囲**	**関連性**	**事象が発生する可能性**	**脆弱性 と 素因的条件**	**重大さと広がり**	**事象が負の影響をもたらす可能性**	**全滝的な可能性**	**影響のレベル**	**リスク**

付録 J

リスク対応への情報の提供

リスクアセスメント結果の提示を改良するためのアプローチ

リスクアセスメントによって、類似のスコア（例：78、82、83）またはレベル（例：中間、高い）を有する多くのリスクが特定される場合がある。同じ（あるいはほぼ同じ）値を有するリスクが数多く集まっている場合、組織は、類似の値を有する一連のリスク内でリスクの優先順位付けを行い、リスクマネジメントプロセス内の「リスク対応」ステップに十分な情報を提供することを可能にする、リスクアセスメントの結果の提示を改良するための手法を必要とする。[57] そうした手法は、組織のミッション／業務上の要求事項に関連し、組織のリスク許容度との一貫性を保ち、利用可能な資源を最大限に活用することが求められる。優先順位付けは、リスクにもとづく保護の主要なコンポーネントであり、要求事項が十分に満たされない場合に、あるいは、資源の使用が、理にかなった時間枠内にすべてのリスクが軽減されることを可能にしない場合に必要になる。最高幹部／上級管理者による十分な情報を得た上でのリスク対応判断（例：特定のリスクが軽減された理由と、特定のリスクが軽減されなかった理由）を容易にするためには、リスクアセスメント結果に注釈を付けることによってそれらの意思決定者が、類似のスコアを有するそれぞれのリスクについての以下の質問に対する答えを知る（または得る）ことを可能にする必要がある：

時間枠

特定されたリスクが顕在化した場合

- 組織の業務（ミッション、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、または国家に対する差し迫った影響は、どれくらい深刻であるか？
- 組織の業務（ミッション、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、または国家に対する将来の影響は、どれくらい深刻であるか？

上記の質問に対する答えは、組織のリスク許容度とともに、現在の、および将来にわたる組織のニーズにもとづいたリスクの優先順位付けの根拠を示す。差し迫った影響と将来の影響を比較検討する際には、上級管理者が、現在の極めて重要なミッション／業務上のニーズを優先した結果、将来にわたる組織の業務遂行能力が危うくなってもかまわないかどうかについて判断しなければならない。ミッション／業務遂行の責任者とミッション／業務に関する専門家は、ミッション／業務への影響についての最も完全で最新の情報を得るための助言を求められる場合がある。その他の本件に関する専門家または利害関係者の代表は、差し迫った影響と将来の影響についての情報を得るための助言を求められる場合がある（例：個人への影響に関しては、Privacy Officeに相談する）。

累積された影響

- その脅威事象が一度発生した場合に予期される影響は、どのようなものか？

[57] リスクエグゼクティブ(機能)は、組織のリスク許容度と、運用認可権限者によるリスクにもとづく意思決定に対して情報を提供し、そうした意思決定を導くためのその他の要素に関する、ポリシーレベルの手引きを用意する。この手引きは、リスク対応（たとえば、軽減活動を含む）の優先順位付けに影響を及ぼす可能性がある。

- そのリスクが二度以上顕在化した場合に、懸念される期間にわたってもたらされる総合的な影響（すなわち、累積された損失）は、どのようなものか？

組織に対する総合的な影響の1つの側面は、機密性、完全性、または可用性の喪失から復旧するためのコストであることに留意すること。

リスク間の相乗作用

顕在化したリスクが複数のリスクに密接にかかわる場合、リスクの集合が同時に（あるいは、ほぼ同時に）顕在化する可能性が高い。単一のリスクが顕在化した場合にもたらされる負の影響を管理することは、可能であるだろう。一方で、同時に顕在化した複数の高位影響のリスクを管理することは、その組織にとって難題となる可能性があり、その場合、よりいっそう綿密な管理が必要になる。以下の質問は、リスク間の関連性を扱う。

特定のリスクが顕在化した場合の結果として：

- 他の特定されたリスクが顕在化する可能性が高くなるか（あるいは、ほぼ確実になるか）？
- 他の特定されたリスクが顕在化しない可能性が高くなるか（あるいは、ほぼ確実になるか）？
- 他の特定されたリスクが顕在化することへの影響は、特にないか？

特定のリスクが、他のリスクに高度に結合されている場合、あるいは他のリスクが顕在化する結果を招く可能性が高い（そのリスクが顕在化の一因となるか、あるいは同時に顕在化するかにかかわらず）と思われる場合には、他のリスクへの影響が特にないリスクよりも、そのリスクに対してより高い優先順位を与える必要がある。実際に顕在化した特定のリスクが、他のリスクが顕在化する可能性を減少させる場合には、どのリスクの軽減に対してより低い優先順位を与えるかを決定するための、さらなる分析が必要になる。

結論として、組織は、リスクマネジメントプロセス内の「リスク対応」ステップの準備段階として、リスクアセスメント結果の提示を改良することによって、著しく恩恵を受ける。NIST SP 800-39 に記載されている「リスク対応」ステップにおいて、組織は、(i) 異なる行動方針を分析する; (ii) 費用対効果分析を実施する; (iii) 大規模な実装の拡張性に関する問題に対処する; (iv) リスク軽減アプローチ間の相互作用／依存関係（例：セキュリティ管理策間の依存関係）を検証する; ならびに (v) 組織のミッション／業務機能に影響を及ぼすその他の要因をアセスメントする。さらに、組織は、組織のミッション／業務機能を支援する情報システムおよび IT インフラのコスト、スケジュール、およびパフォーマンスに関する問題に取り組む。

注意書

組織は、リスクアセスメントが「測定のための精密計器」とならないことが多く、採用されている特定のアセスメント方法論、ツールおよび技術の限界、そして、使用されるデータの主観性、質、および信頼性を反映することに注意しなければならない。リスクの判断は、選択されたアセスメントアプローチ、発生の可能性と影響値の不確実性、ならびに脅威の特徴定義の誤りによって、非常に大まかになる可能性がある。組織が定めた瓶スケールを使用する瓶間の境界上にあるリスクは、最終的に1つの瓶に割り当てられる必要がある。この決定は、リスクの優先順位付プロセスに大きな影響を及ぼす可能性がある。したがって組織は、リスクの優先順位付けプロセスにおいて、特定のリスクに関する情報を最大限に取り入れて、リスクに割り当てる値（例：非常に低い、低い、中間、高い、非常に高い）が適切に決定されるようにしなければならない。

付録 K

リスクアセスメント報告

情報の必須要素

本付録 は、組織がリスクアセスメントの結果を伝達するのに使用できる情報の、必須要素を示す。[58] リスクアセスメント結果は、意思決定者に対して、組織の情報システムと、それらのシステムが稼働する環境の運用と使用により生じる組織の業務と資産、個人、他の組織、または国家に対する情報セキュリティリスクについての理解を与える。リスクアセスメントにおける情報の必須要素は、リスクアセスメント報告書内の 3 つのセクション（あるいは、組織が選択した、アセスメント結果を伝達するための手段）に記載することができる。それらの 3 つのセクションは、(i) 要旨; (ii) 詳細なリスクアセスメント結果を含む本文; ならびに (iii) 付録。

要旨

- リスクアセスメントの日付を記載する。
- リスクアセスメントの目的を簡単に述べる。
- スクアセスメントの適用範囲を記述する。
  - 第 1 層と第 2 層におけるリスクアセスメントの場合、以下を特定する：組織のガバナンス構造、またはアセスメントに関連するプロセス（例：リスクエグゼクティブ(機能)、予算プロセス、調達プロセス、システムエンジニアリングプロセス、エンタープライズアーキテクチャ、情報セキュリティアーキテクチャ、組織のミッション／業務機能、ミッション／業務プロセス、それらのミッション／業務プロセスを支援する情報システム。
  - 第 3 層におけるリスクアセスメントの場合、以下を特定する：情報システムの名称とロケーション、セキュリティ分類、および情報システムの境界（すなわち、運用認可を出す範囲）。
- 当該リスクアセスメントが初期アセスメントであるか、あるいは後続のアセスメントであるかを記載する。後続のアセスメントである場合には、更新を促した状況について記載し、前回作成されたリスクアセスメント報告への参照を含める。
- 総合的なリスクレベルを記載する(例：非常に低い、低い、中間、高い、または非常に高い)

[58] 本付録に記載されている情報の必須要素は、情報を提供することを目的とした例にすぎない。したがって、リスクアセスメント結果を文書化するための具体的なテンプレートの使用を求めたり、促すことを意図していない。組織は、組織のリスクアセスメントと、関連する報告に含まれる情報のタイプと詳細レベルを決定するうえで、最大の柔軟性を有する。たとえば、第 1 層と第 2 層におけるリスクアセスメントの結果は、管理職者による概要報告またはダッシュボードを介して伝達される可能性がある。一方、第 3 層におけるリスクアセスメントの結果は、リスクアセスメント報告（組織の好みに応じてフォーマルであったり、インフォーマルであったりする）を介して伝達される可能性がある。リスクアセスメント結果を伝達するための情報の必須要素は、アセスメントを実施する組織のニーズを満たすために、適宜、修正されるであろう。

- それぞれのリスクレベル(例:非常に低い、低い、中間、高い、または非常に高い)に関して、特定されたリスクの数を記載する。

報告書の本文

- リスクアセスメントの目的を記載する。これは、アセスメントによって答えらるべき質問事項を含む。たとえば:
  - 特定の情報技術の使用が組織のミッション／業務機能を支援する情報システムに導入された場合に、それらのミッション／業務機能に対するリスクにどのように変化をもたらすか、あるいは
  - リスクマネジメントフレームワークのコンテキストにおいて、リスクアセスメント結果がどのように使用されるか(例:セキュリティ管理策ベースラインを調整する際に使用される初期リスクアセスメント、および／またはその他の意思決定に情報を提供し、そうした意思決定を導き、後続のリスクアセスメントの開始点となる初期リスクアセスメント、セキュリティ管理策アセスメントの結果を組み入れて、運用認可権限者に情報を提供するための後続のリスクアセスメント、リスク対応のための代替えの行動方針の分析を支援する後続のリスクアセスメント、新たな脅威または脆弱性を特定するためのリスクモニタリングにもとづいた後続のリスクアセスメント、インシデントまたは攻撃から得た知識を組み入れるための後続のリスクアセスメント)。
- 想定と制限を特定する。
- リスクアセスメントに対する、リスク許容度関連の入力データを記載する(考慮すべき影響の範囲を含む)。
- リスクモデルと分析的アプローチを特定し、記載する。リスク因子、価値尺度、および値を結合するためのアルゴリズムを特定し、付録として含める、あるいは参照を提供する。
- リスクアセスメントプロセス時のリスク関連の意思決定の根拠を示す。
- リスクアセスメントプロセス内の不確実性について、また、それらの不確実性が意思決定にどのように影響を及ぼすかを記載する。
- リスクアセスメントが組織のミッション／業務機能を含む場合、そのミッション／業務機能(例:ミッション／機能を支援するミッション／業務プロセス、関連するミッション／業務機能間の相互接続と依存関係、およびミッション／業務機能を支援する情報技術)について記載する。
- リスクアセスメントが組織の情報システムを含む場合、そのシステム(例:そのシステムが支援するミッション／業務機能、システムからの情報の流れとシステムへの情報の流れ、他のシステムへの依存、共有サービス、または共通インフラ)について記載する。
- (たとえば、表またはグラフを使用して)意思決定者がリスクを迅速に理解できる形で、リスクアセスメント結果を簡単に示す(例:発生可能性と影響の異なる組み合わせによる脅威事象、異なるリスクレベルの脅威事象の相対的比率)。
- リスクアセスメントが有効となる時間枠(すなわち、アセスメントによる意思決定の支援の有効期限)を特定する
- アドバーサリによる脅威に起因するリスクを記載する(表 F-1 を参照)。

- アドバーサリによるもの以外の脅威に起因するリスクを記載する（表 F-2 を参照）。.

付録

- 参考文献と情報源を記載する。
- リスクアセスメントを実施するチームまたは個人について、連絡先を含めて記載する。
- 結果を理解し、結果の再利用を可能にするために必要な場合には、リスクアセスメントの詳細と、結果を裏付ける証拠（例：表 D-7、D-8、E-5、F-3、 F-6、H-4）を記載する（例：互恵を実現するための、あるいは後続のリスクアセスメントにおける、第 1 層と第 2 層におけるリスクアセスメントに対する入力データとなるように）。

付録 L

各タスクの概要

リスクアセスメントのタスク一覧と、関連するリスクの一覧

表 L-1:リスクアセスメントの各タスクの要約

タスク	タスクについての説明
ステップ 1:リスクアセスメントの準備	
タスク 1-1 目的を特定する **セクション 3.1**	アセスメントが生成する情報と、アセスメントが支援する意思決定の観点から、リスクアセスメントの目的を特定する。
タスク 1-2 適用範囲を特定する **セクション 3.1**	組織の適用範囲、サポートされている時間枠、および構造上／技術上の考慮事項の観点から、リスクアセスメントの適用範囲を特定する。
タスク 1-3 想定と制限を特定する **セクション 3.1**	リスクアセスメントが具体的にどのような想定と制限のもとで実施されるかを特定する。
タスク 1-4 情報源を特定する **セクション 3.1**	リスクアセスメントにおいて使用される記述的情報、脅威関連情報、脆弱性関連情報、および影響関連情報の情報源を特定する。
タスク 1-5 リスクモデルと分析的アプローチを特定する **セクション 3.1**	リスクアセスメントにおいて使用されるリスクモデルと分析的アプローチを特定する。
ステップ 2:リスクアセスメントの実施	
タスク 2-1 脅威源を特定する **セクション 3.2, 付録 D**	懸念される脅威源（アドバーサリによる脅威の場合には、アドバーサリの能力、意図、および標的を含み、アドバーサリによるもの以外の脅威の場合には、影響の範囲を含む）を特定し、特徴を定義する。
タスク 2-2 脅威事象を特定する **セクション 3.2, 付録 E**	起こりうる脅威事象、それらの事象間の関連性、およびそれらの事象を開始する可能性のある脅威源を特定する。
タスク 2-3 脆弱性と素因的条件を特定する **セクション 3.2, 付録 F**	懸念される脅威事象が負の影響をもたらす可能性に影響を及ぼす脆弱性と素因的条件を特定する。

タスク	タスクについての説明
タスク 2-4 可能性を特定する **セクション 3.2, 付録 G**	懸念される脅威事象が負の影響をもたらす可能性について、以下を考慮しながら特定する：(i) それらの事象を開始する可能性のある脅威源の特徴; (ii) 特定された脆弱性／素因的条件; ならびに (iii) そうした事象を阻止するために導入が計画されている、あるいは導入されている保護手段／対策を反映する、そうした事象に対する組織の脆弱さ。
タスク 2-5 影響を特定する **セクション 3.2, 付録 H**	懸念される脅威事象がもたらす負の影響を、以下を考慮しながら特定する：(i) それらの事象を開始する可能性のある脅威源の特徴; (ii) 特定された脆弱性／素因的条件; ならびに (iii) そうした事象を阻止するために導入が計画されている、あるいは導入されている保護手段／対策を反映する、そうした事象に対する組織の脆弱さ。
タスク 2-6 リスクを判断する **セクション 3.2, 付録 I**	懸念される脅威事象が組織にもたらすリスクを、以下を考慮しながら特定する：(i) それらの事象がもたらす影響; ならびに (ii) それらの事象が発生する可能性。
ステップ 3：リスクアセスメント結果の伝達と共有	
タスク 3-1 リスクアセスメント結果を伝達する **セクション 3.3, 付録 K**	リスク対応を支援するために、リスクアセスメント結果を組織の意思決定者に伝達する。
タスク 3-2 リスク関連情報を共有する **セクション 3.3**	リスクアセスメントにおいて生成されたリスク関連情報を、組織の適切な職員と共有する。
ステップ 4：リスクアセスメントの保守	
タスク 4-1 リスク因子をモニタリングする **セクション 3.4**	組織の業務と資産、個人、他の組織、または国家に対するリスクの変化の一因となるリスク因子に対する、継続的なモニタリングを実施する。
タスク 4-2 リスクアセスメントを更新する **セクション 3.4**	リスク因子の継続的なモニタリングの結果を使用して、既存のリスクアセスメントを更新する。