NIST SP（特別出版物） **800-171**
Revision 1 （改訂 1）

非連邦政府組織およびシステムにおける管理対象非機密情報の保護

ロン・ロス **RON ROSS**
パトリック・ヴィスクーソ **PATRICK VISCUSO**
ゲーリー・ギサニー **GARY GUISSANIE**
ケリー・デンプシー **KELLEY DEMPSEY**

本出版物は以下から無料で入手可能：
http://dx.doi.org/10.6028/NIST.SP.800-171

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

㈱エヴァアビエーション　info@EvaAviation.com　訳　2017.03.24（認証の日）

NIST SP（特別出版物） **800-171**
Revision（改訂） 1

非連邦政府組織およびシステムにおける管理対象非機密情報の保護

ロン・ロス
ケリー・デンプシー
コンピュータ・セキュリティー部
米国標準技術研究所（*NIST*）

パトリック・ヴィスクーソ
マーク・リドル
情報セキュリティー監督室
国立公文書館（*NARA*）

ゲーリー・ギサニー
防衛分析研究所
国防総省補佐官

本出版物は以下から無料で入手可能：
http://dx.doi.org/10.6028/NIST.SP.800-171

2016 年 **12** 月

米国商務省
ペニー・プリツカー *Penny Pritzker* 長官

米国標準技術研究所（NIST）
ウィリー・メイ *Willie May*、標準・技術担当商務次官および部長

典拠

本出版物は、2014 年の「連邦情報セキュリティー近代化法」（FISMA）、合衆国法典（U.S.C.）第 44 編・第 3551 条、および公法（P.L.）113 条-283 条に基づく法定責任にもとづき、NIST（米国標準技術研究所）によって作成された。NIST は、連邦政府情報システムのための最小限の要件からなる情報セキュリティー規格（standards）および指針（guidelines）を作成する責任を負うが、これらの規格および指針は国家安全保障システムへの政策権限を執行する関係連邦政府当局者による明示された承認なしにそれらのシステムに適用してはならない。この指針は、行政管理予算局（OMB）の通達 A-130 の要件を満たしている。

本出版物に記載されているものは、商務長官による法的権限により連邦政府機関に命じられ、義務付けられるとした規格および指針を否定するように解釈されてはならない。また、これらの指針は、商務長官、行政管理予算局長、またはその他のすべての連邦政府当局者の既存の権限を変更、あるいはそれらを置換するものと解釈されてはならない。本出版物は、非政府組織が任意に使用できるとともに米国における著作権の対象外である。しかしながら、NIST への帰属を明らかにすることには感謝する。

米国標準技術研究所（NIST）特別出版物（SP）800-171
80 ページ（2016 年 12 月）
CODEN：NSPUE2

本出版物は右から無料で入手可能：http://dx.doi.org/10.6028/NIST.SP.800-171

試行的手順や概念を適切に説明するため、この文書では、一定の商業組織、装置、または資料が特定されることがある。そうした特定は、NIST による推奨や是認を意図しておらず、あるいはその組織、資料、または装置が、必然的に、その目的に利用可能な最善のものであることも意図していない。

本出版物では、与えられた法的責任に従って NIST が現在開発中のその他の出版物を参照することがある。本出版物にある情報は、概念、実践例、および方法論を含め、そのような関連出版物の完成以前であっても連邦政府機関によって使用されることがある。したがって、それぞれの出版物が完成されるまでの間、その時点において運用している要件、指針、および手順が存在する場合には、それらは有効であり続ける。計画策定および移行の目的のために、連邦政府機関は、NIST によるこれらの新しい出版物の作成に密接に従うことを求めるであろう。

各組織は、指定されたコメント公募期間中に出版物の草稿を見直し、NIST へフィードバックを提供することは奨励される。上記以外のすべてのコンピュータセキュリティー部門の出版物は、以下から入手可能である。 **http://csrc.nist.gov/publications**

本出版物へのコメント提出先は以下である。

米国標準技術研究所（NIST）
情報技術研究所、コンピュータ・セキュリティー部
20899-8930 MD（メリーランド州）、ゲイサーズバーグ、ビューロー・ドライブ 100
電子メール：**sec-cert@nist.gov**

全コメントは FIA(Freedom of Information Act)に基づく公開対象となる

コンピュータシステム技術に関する報告

国立標準技術研究所（NIST）の情報技術研究所（ITL）は、米国の計測・標準インフラへの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および社会福祉に貢献している。ITL は情報技術（IT）の開発ならびに生産的利用を促進するために、試験、試験方法、参照データ、概念実証（POC）、および技術分析等を開発している。ITL は、連邦政府情報システムにおける国家安全保障関連情報以外の情報に対する費用対効果の高いセキュリティーおよびプライバシーのための管理、運営、技術、物理的な規格および指針の開発に責任を持っている。本 SP（特別出版物）800 シリーズは、情報システムのセキュリティーに関する ITL の調査研究、指針、普及活動ならびに産業界、政府、および学術機関との協働活動について報告するものである。

摘要

非連邦政府の情報システムおよび組織に存在する「機密指定はされてないが管理対象となる情報」（以降、管理対象非機密情報または単に CUI（CUI : Controlled Unclassified Information）と記述）を保護することは連邦政府機関にとって極めて重要であり、連邦政府が指定された任務（mission）および事業運用を成功裏に遂行する能力に直接的な影響をおよぼす可能性がある。本出版物は、以下の場合における CUI の機密性を守るための推奨要件を連邦政府機関に提供する。すなわち、(i) CUI が非連邦政府の情報システムおよび組織に存在する、(ii) CUI が連邦政府機関を代理して収集・維持されていない、あるいは情報システムを連邦政府機関に代わって使用または運用されていない、(iii) CUI の機密性は CUI カテゴリーまたはサブカテゴリーを認可する法律、規則、または政府横断のポリシーによって規定され、「CUI レジストリー」に記載されるが、そうした機密性を守るための特定の保護要件が存在しない場合である。本要件は、CUI を処理、格納、通信またはそれらの構成要素にセキュリティー保護機能を提供する非連邦政府の情報システムおよび組織の全構成要素に適用される。本要件は、連邦政府機関と非連邦政府組織の間で締結された契約手段またはその他の合意の中で、連邦政府機関によって使われることを意図している。

キーワード

契約者情報システム（ Contractor Systems ）、管理対象非機密情報（Controlled Unclassified Information）、CUI レジストリー（CUI Registry）、大統領令（Executive Order）13556、FIPS 出版物 199、FIPS 出版物 200、FISMA, NIST SP 800-53、非連邦政府情報システム（Nonfederal Systems）、セキュリティー評価（Security Assessment）、セキュリティー管理（Security Control）、セキュリティー要件（Security Requirement）。

謝辞

著者は、キャロル・ベイルス（Carol Bales）、マット・バレット（Matt Barrett）、ジョン・ボエンズ（Jon Boyens）、デヴィン・ケイシー（Devin Casey）、クリス・エンロー（Chris Enloe）、ジム・フォッティ（Jim Foti）、ロブ・グレン（Rob Glenn）、リッチ・グローバート（Rich Graubart）、ヴィッキー・ミケッティ（Vicki Michetti）、マイケル・ニールス（Michael Nieles）、パット・オーレイリー（Pat O ’Reilly）、カレン・クイグ（Karen Quigg）、メアリー・トーマス（Mary Thomas）、マット・ショル（Matt Scholl）、ムルギ・スパーヤ（Murugiah Souppaya）、およびパット・トス（Pat Toth）の貢献に感謝し、またそれを高く評価する。彼らの思慮深く建設的な意見は、本出版物の全般的な品質、完璧性、および有用性を高めている。ペギー・ハイメス（Peggy Himes）とエリザベス・レノン（Elizabeth Lennon）には、彼らの優れた管理および技術編集支援に対して、心からの感謝を表明する。

注意書

「連邦情報セキュリティー近代化法」（FISMA：Federal Information Security Modernization Act）は、連邦政府機関が、下記の情報への不正なアクセス、利用、開示、通信の途絶、改ざん、または毀損から生ずるリスクに対応した情報セキュリティー保護を特定し、提供することを求めている。すなわち、(i) 政府機関により、または政府機関に代わって、(ii) 政府機関により、または政府機関の契約者により、あるいは政府機関を代理するその他の組織によって使用・運用される情報システムで、収集・維持される情報である。本出版物は、*非連邦政府* の情報システムおよび組織にある「管理対象非機密情報」（CUI）の*機密性* の保護に焦点を当て、その目標を達成するためのセキュリティー要件を推奨している。これは、FISMAで規定されている情報セキュリティー要件をどのような形においても変更するものではなく、また連邦政府機関が、法令の全条項、OMBによって設定されたポリシー、およびNISTによって開発された支援セキュリティー規格および指針に従う責任を変えるものでもない。

本出版物で適用を推奨されている要件は、「FIPS 200」および「NIST SP 800-53」における中位セキュリティー管理基準（baseline）ならびに提案中のCUI規則（32 CFR Part 2002*「管理対象非機密情報」*）に基づいたものである。セキュリティーの要件および管理は、FISMAで扱われている連邦政府の情報および情報システムに必須の保護要件を提供するために、時間をかけて規定されたものである。「FIPS 200」のセキュリティー要件と「NIST SP 800-53」のセキュリティー管理に適用される適応規準は、それらの要件および管理の排除を是認するものと解釈***されてはならず***、むしろ、この適応規準は、非連邦政府の情報システムと組織における権限のない開示からCUIを保護することに焦点を当てるものである。さらに、このセキュリティ要件は、上に挙げたNIST出版物から派生しているものであるため、各組織は、それらの要件を満たしても、「FIPS 200」および「SP 800-53」のセキュリティーの要件と管理を自動的に満たすものになると推定***してはならない***。

機密性 というセキュリティー目的に加えて、*完全性* および *可用性* という目的も、包括的な情報セキュリティー施策の確立・維持に携わる組織にとっては高い優先事項である。本出版物の主要目的は、CUIの機密性を保護する要件を定義することであるが、機密性と完全性の間には密接な関係が存在する。というのは、システムレベルの基礎になるセキュリティーメカニズムの多くが、双方のセキュリティー目的を支えているからである。本出版物の勧告に関心を持ち、あるいはそれに準拠することを求められる組織は、付属書Eにある中位ベースラインのセキュリティー管理に関する記載事項全体を見直し、組織の個別セキュリティー計画とセキュリティー管理の展開が、組織のミッションと事業運営に対する多様なサイバー脅威および物理的脅威に対処する上で、必要かつ十分な保護を提供するものであることを確実にすることが強く勧められる。こうした脅威への対処は重要なことである。なぜなら、多くの組織は、ミッションと事業の成功において、それぞれの情報技術インフラに依存しているからである。

本出版物への期待

2010 年 11 月 04 日付の大統領令 13556『管理対象非機密情報（*CUI:Controlled Uncassified Information*）』では、CUI 執行機関として指定された米国国立公文書館（NARA）は CUI プログラムを履行するために必要な指令を開発・発行しなければならない、と定めている。この任務付与、および連邦政府横断の一律のポリシーと業務手続きを確立するという CUI プログラムのミッションと整合するように、NARA は、2016 年に、CUI に必要とされる政府横断の管理と標示を確立する最終版の連邦規則を発行しようといている。この連邦規則は、一旦制定されると、CUI プログラムによって確立される保護、標示、普及、および管理除外に関する規格要件を一律に適用するために、それは行政府全機関に義務付けられるものになる。

*連邦政府情報システム*に関して、中位機密性影響レベルで CUI を保護するための提案中の連邦規則の要件は、OMB によって設定される適用可能なポリシー、および NIST によって発行される適用可能な政府横断の規格と指針に基づくものになる。この規則が、OMB および NIST によって既に定められているポリシー、規格、および指針を生み出すことにはならない。しかしながら、この提案中の規則は、行政府全体で一貫した方法によるポリシーの厳守と、規格および指針の利用を必要とするものであり、それにより、連邦政府機関およびその契約者を含む非連邦パートナーに対して、現時点の複雑さを低減するものになるであろう。

連邦政府内 CUI の保護要件明確化に加えて、NARA は、「SP 800-171」を NIST と共同して開発し、非連邦政府の情報システムおよび組織にある CUI を保護するセキュリティー要件を明確にすることによって、非連邦政府組織に関するこれらの要件の潜在的影響を軽減する措置を講じている。これは、契約者を含む非連邦政府組織が、政府固有の取組み方を使おうとするのではなく、自ら既に構築しているシステムや業務手順等を使うことによってセキュリティー要件に準拠することに役立つであろう。それはまた、非連邦政府のシステムに適応されたすべての CUI セキュリティーニーズのための標準化された一律の要件群を提供することになり、非連邦政府組織が、法令および規則上の要件に準拠すること、そして CUI を守るための保護策を一貫して履行することを可能にするであろう。

最後に、NARA はまた、CUI 執行機関としての立場で、2017 年に、「連邦調達規則」（FAR）の単一条項を提出する計画である。その条項は、提案中の連邦政府 CUI 規則および「SP 800-171」に包含される要件を契約者に適用するものである。これは、標準化をさらに促進し、契約条項の現在の範囲と類型に従おうとしている相当数の非連邦政府組織に恩恵をもたらすものになろう。現在は、同一の情報に対して、連邦政府の複数機関から、異なる要件や相反する指導があり、それが混乱や非効率を生じさせているからである。このような単一 FAR 条項を定める正式プロセスが始まるまでは、「NIST SP 800-171」の要件が、連邦法および連邦規則の要件に従う連邦政府契約で参照されることになるだろう。必要に応じて、「SP 800-171」は、提案中の連邦政府 CUI 規則および FAR 条項との一貫性を保持するために、更新されることがある。

情報システム（Information System）という用語の定義

法、規則、政府横断のポリシーによって規定されないかぎり、本出版物における*情報システム（information system）*という用語は*システム（system）*という用語に置き換えられている。この変更は、たとえば、汎用情報システム、産業用のプロセス制御システム、サイバーフィジカルシステム、*IoT（Internet of Things）*を構成する個々の装置などを含む情報システムのより広範な、全体論的な定義を反映したものである。コンピュータ処理プラットフォームとテクノロジーはいよいよ全世界にくまなく展開されつつあり、それぞれのシステムおよび構成要素は有線または無線通信により結合されることで、CUI の滅失または毀損による感染性----そうした現象によって有害な結果を招く可能性----は増大している。

重要インフラのサイバーセキュリティーを改善するためのフレームワーク

NIST の『重要インフラ・サイバーセキュリティーを改善するためのフレームワーク』 を履行している組織や、履行を計画している組織は、管理対象非機密情報（CUI）セキュリティー要件と、「NIST SP 800-53」および「ISO/IEC 27001」のセキュリティー管理との直接的なマッピングを、本出版物の付属書 D に見ることができる。このマッピングを確認することで、それらのセキュリティー管理を、識別・保護・検知・対応・回復という「サイバーセキュリティーフレームワーク」の中核機能における特定カテゴリーおよびサブカテゴリーに位置づけることができる。このマッピング情報は、セキュリティー要件への準拠性を論証したい組織にとっては、それぞれの組織が整えた情報セキュリティー対策が NIST や ISO/IEC のセキュリティー管理に沿って構築されている場合には、有用なものとなろう。以下を参照 http://www.nist.gov/cyberframework

目次

正誤表

この表には「SP 800-171」に組み入れられた変更が含まれている。正誤表の改訂には、本出版物における編集上もしくは内容上の訂正、明確化、またはその他の小改訂が含まれる。

日付	種類	変更点	ページ

第 1 章

序論

管理対象非機密情報（CUI）を保護する必要性

現在、連邦政府は、歴史上これまでになく外部のサービスプロバイダーに依存して、多様な連邦政府の任務および事業機能を遂行するために情報システム[1]を運用している。たとえば、多くの連邦政府との契約者は、それぞれの情報システムで、要注意（sensitive）連邦政府情報を日常的に処理、格納、送信することで連邦政府機関にとって必須の製品やサービスの納入を支えている（たとえば、クレジットカードおよびその他の金融サービスの提供、Web および電子メールサービスの提供、機密取扱許可のための身元調査実施、健康管理データの処理、クラウド・サービスの提供、通信・衛星・兵器システムの開発など）。さらに、連邦政府の情報は、州および地方政府、単科大学および総合大学、そして独立調査機関などの組織に頻繁に提供され、またそれらと共有されている。非連邦政府の情報システム[2]および各組織に存在している期間における要注意（sensitive）連邦政府情報の保護は、連邦政府機関にとって極めて重要であり、連邦政府が、重要インフラに関連するミッションおよび機能を含めて、指定されたミッションおよび事業運用を成功裏に遂行する能力に、直接的な影響をおよぼす可能性がある。

非連邦政府の情報システムおよび各組織内の非機密連邦政府情報を保護できるかどうかは、連邦政府によって日常的に使われる様々なタイプの情報を識別するための構造化され統制のとれたプロセスを、連邦政府が提供できるかどうかにかかっている。2010 年 11 月 4 日、大統領は大統領令 13556『管理対象非機密情報』（CUI：Controlled Unclassified Information）に署名した。この大統領令は、保護を必要とする非機密情報を執行部門（executive branch）が取り扱う方法を標準化するために、政府横断の CUI プログラム[3]を設け、そしてこのプログラムを履行する執行機関（Executive Agent）[4]に国立公文書館（NARA： National Archives and Records Administration）を指定した。連邦法、規則、または政府横断のポリシーに従って保護や配布制限を必要とする情報だけが、CUI として指定されることができる。

---

[1] 「情報システム」（*information system*）とは、情報の収集、処理、維持、利用、共有、配布、または廃棄のために明示的に組織された個別の情報資源の集合である。情報システムには、産業/プロセス制御システム、サイバーフィジカルシステム、組込みシステム、およびデバイスなど、特化したシステムも含まれる。「システム」という用語は本出版物では CUI を処理、格納、または送信することができるすべての情報処理プラットフォームを示すものとして用いられている。

[2] 「連邦政府情報システム」（*federal systems*）とは、執行機関、執行機関の契約者、または執行機関を代理する別組織によって利用され、あるいは運用されるシステムである。この規準を満たさない情報システムは、「非連邦政府情報システム」（*nonfederal information system*）である。

[3] 「管理対象非機密情報」は、法、規則、または政府全体のポリシーが保護または配布管理を要求するような情報であり、大統領令 13526「国家安全保障機密情報」（*Classified National Security Information*）Dessembre 29, 2009（または以前の、または後継の大統領令）、または改訂を含む 1954 年の原子力エネルギー法（Atomic Energy Act)で機密扱いにされた情報を除く。

[4] NARA は本権限を NARA の一部門である米国情報保全監察局（ISOO:Information Security Oversight Office）に委任している。

CUI プログラムは、一貫性のない標示、不十分な防護、不必要な制限など、非機密情報を管理・保護する上でのいくつかの欠陥に対処することを意図している。その方法は、手順の標準化と、「CUI レジストリー」 を通じた共通定義の提供の双方による。CUI レジストリーは、CUI の取扱に関する情報、指導、ポリシー、および要件のためのオンラインリポジトリーであり、CUI 執行機関によって発行されるものを含む。 CUI レジストリーは、様々な情報を処理する中で、特に、承認済 CUI 区分および下位区分を識別し、それぞれに一般的説明を規定し、管理の基礎を明らかにし、また CUI を使う手順を設定している。これには、情報の標示、防護、移動、配布、再利用、廃棄が含まれるが、それに限定されるものではない。

大統領令 13356 はまた、CUI プログラムが、開示性、透明性、および政府全体の実践の画一性を重視すること、そしてプログラムの履行が、行政管理予算局（OMB：Office of Management and Budget）によって定められた適用可能なポリシーと、米国標準技術研究所（NIST：National Institute of Standards and Technology）によって発行される連邦標準規格および指針と整合性のある方法で行われることを求めている。CUI 執行機関によって開発された連邦政府 CUI 規則[5]は、CUI の指定、防護、配布、標示、解除、および処分に関して連邦政府機関にガイダンスを提供し、自己点検と監督要件を定め、またプログラムのその他の側面について正確に概説している。

CUI に対する単一状態セキュリティソリューションの実装

CUI は、このような情報が連邦政府機関の一部である連邦政府システムにあっても、非連邦政府組織の一部である非連邦政府システムにあっても、*同じ価値がある*。したがって、本出版物に含まれるセキュリティ要件は、CUI を保護するために連邦政府機関によって使用される標準規格およびガイドラインに対して矛盾せず、補足するものである。

1.1 目的と適用性

本出版物の目的は、下記の期間において、CUI の*機密性* を守るための推奨要件を、連邦政府機関に提供することである。すなわち、(i) CUI が非連邦政府システムおよび組織に存在している期間、(ii) CUI が存在するシステムが連邦政府機関の契約者またはその連邦政府機関を代理するその他の組織[6]によって使用または運用されていない 期間、および (iii) CUI の機密性は、CUI カテゴリーまたはサブカテゴリーを認可する法律、規則、または政府横断ポリシーによって規定され、「CUI レジストリー」[7]に記載されるが、そうした

[5] 32 CFR Part 2002『管理対象非機密情報』が 2016 年 9 月 14 日に制定、2016 年 11 月 14 日に施行された。

[6] 連邦政府機関を代行して 情報を収集・維持する非連邦政府組織、または連邦政府機関を代理してシステムを運用・使用する非連邦政府組織は、「連邦情報セキュリティー近代化法」（FISMA：Federal Information Security Modernization Act）の要件に従わなければならない。それには、「FIPS 200」の最低限のセキュリティー要件、および「NIST SP 800-53」のセキュリティー管理が含まれる。（44 USC 3554(a)(1)(A)参照）

[7] 本出版物に示す要件は、上級政府機関職員が非連邦政府システムおよび組織に存在する CUI を含め、彼らの管理下の資産および運用を支援する情報に対する FISMA 要件に適合した情報セキュリティ措置のために利用できる。

機密性を保護するための特定の防護要件が存在しない場合である。本要件は、CUI を処理、格納、または送信する非連邦政府システムの構成要素[8]だけに適用され、あるいはそれらの構成要素にセキュリティー保護を提供する非連邦政府システムの構成要素だけに適用される。本 CUI 要件は、連邦政府機関と非連邦政府組織の間で締結される該当する契約手段またはその他の協定の中で、連邦政府機関によって使われることを意図している。CUI ガイダンスおよび CUI「連邦政府調達規則」（FAR：Federal Acquisition Regulation）[9]の中で、CUI 執行機関は CUI 要件[10]への準拠性判断を行う。

CUI を処理、格納、または送信する連邦政府システムを使う連邦政府機関は、提案中の連邦政府 CUI 規則に従って、 最低限、以下に準拠しなければならない。

- 連邦情報処理規格（FIPS）199『連邦政府情報および情報システムのセキュリティーカテゴリー企画』（中位機密性影響度）[11]。

- 「連邦情報処理規格」（FIPS）200『連邦政府情報および情報システムに関する最低限のセキュリティー要件』。
- NIST SP 800-53『連邦政府情報システムおよび組織のためのセキュリティーおよびプライバシー管理』。
- NIST SP 800-60『セキュリティー・カテゴリーに対して情報および情報システムのタイプをマッピングするためのガイド』[12]。

CUI を保護し、CUI を確実に管理するという連邦政府機関の責任は、そうした情報が非連邦政府パートナーと共有される期間においても変わらない。したがって、非連邦政府のシステムを使用する非連邦政府組織 によって CUI が処理・格納・送信される時にも、類似レベルの保護が必要とされる[13]。非連邦政府のシステムおよび組織にある CUI を保護するための具体的な要件は、一貫した保護レベルを維持するために、上述の連邦政府標準規格と指針から引き出される。しかしながら、提案中の連邦政府 CUI 規則にある保護要件の範囲が、機密性

[8] システムの構成要素 には、たとえば、①メインフレーム、ワークステーション、サーバー、②入出力装置、③ネットワーク構成要素、④オペレーティング・システム、⑤バーチャル・マシン、および⑥アプリケーションが含まれる。

[9] NARA は、CUI 執行機関としての立場で、2017 年に、連邦政府 CUI 規則および「NIST SP 800-171」の要件を契約者に適用する単一条項を提出する計画である。このような単一 FAR 条項を制定する正式プロセスが始まるまでは、連邦政府法および規則の要件に従う連邦政府契約に際して「NIST SP 800-171」のセキュリティ要件が参照されることになるだろう。

[10] 姉妹編の FIPS SP 800-171A（2017 年発行が計画されている）は、組織が第 3 章のセキュリティ要件への適合性を判断する上で助けとなる評価手順を提供することになろう。

[11] 「FIPS 出版物 199」は、万一セキュリティーの欠陥（たとえば機密性の欠損）が存在した場合における、組織、資産、または個人に対する 3 種類の潜在的影響値（低位、中位、高位）を規定している。この潜在的影響は、機密性の欠損が、組織の運営、組織の資産、または個人に対して重大な悪影響をおよぼすと予想できる場合には「中位」（*moderate*） になる。

[12] 「NIST SP 800-60」は、CUI レジストリーにある CUI カテゴリーおよびサブカテゴリーとの整合性を取るために改訂中である。

[13] 非連邦政府組織 とは、非連邦政府の情報システムを所有、運用、または維持する組織すべてのことである。非連邦政府組織の例には、州政府・地方政府・部族政府、単科大学・総合大学、および契約者が含まれる。

というセキュリティー目的に限定されていること（すなわち完全性や可用性に直接対処していないこと）、そしてNISTの規格および指針に示されているFISMA関連の要件の一部が一意的に連邦政府用であることを認識した上で、本出版物の要件は非連邦政府の組織向けに適応されている。

第2章で説明される適応規準は、提案中の連邦政府CUI規則に示されているCUIの保護のための連邦政府要件を縮小し、または 最小限にすることを意図していない。その意図はむしろ、非連邦政府のシステムおよび組織内で同等の防護手段を可能にし、また促進するような方法で、その要件を示すことであり、中位の機密性に求められる CUI の保護レベルを弱めることではない。本出版物で記述される要件以外の追加要件や別途要件が適用される可能性があるのは、そうした要件が法律、規則、または政府横断のポリシーに基づいている時と、CUI レジストリーに「特定 CUI（CUI-specified）」と指定されている時だけである。特に特定カテゴリー内へのCUI保護要件の規定は、NARAのCUI指針およびCUI FARの中で NARA によって検討され、また契約やその他の協定における具体的な要件として反映される。

CUI 保護を受託した非連邦政府組織が、CUI の処理・格納・通信用に、特定のシステムやシステム構成要素を指定する場合、その組織はその特定のシステムや構成要素へのセキュリティー要件の範囲を限定する可能性がある。アーキテクチャー設計の原則や概念を適用することによって、CUI をそれ自身のセキュリティードメインへ隔離することが（たとえば、ファイアーウォールやその他の境界保護ディバイスを備えたサブネットワークの実装）、非連邦組織が要件を満たし、CUI の機密性を守る上でもっともコスト効果があり、効率的な取り組み方であるかもしれない。セキュリティードメインでは、物理的分離、論理的分離、または両方の組み合わせを利用することもある。この取り組み方では、以下が可能である。すなわち、(i) CUIに適したセキュリティーを合理的に提供すること、そして (ii) 組織のミッションおよび事業運用と資産を保護するために、その組織が通常必要とするレベルを超えたところまで、その組織のセキュリティー体制を拡大しなければならないことを回避することである。認可する法律、規則、または政府横断ポリシーによって求められ、または許される特定の防護を含めて、その組織の CUI 関連のすべての契約または協定のための保護要件を CUI インフラが満たす限り、非連邦政府組織は、複数の政府契約や協定に対して同一のCUIインフラの使用を選択できる。

1.2 対象読者

本出版物は、公共部門と民間部門双方の個人および組織の様々なグループに役立つことを意図している。それには以下が含まれるが、それに限定されるものではない。

- システムの開発ライフサイクル責任を有する個人（プログラム管理者、ミッション/事業オーナー、情報オーナー/管理者、システム設計者・開発者、システム/セキュリティー技術者、システム・インテグレーターなど）。
- 取得または調達責任を有する個人（契約担当官など）。
- システム、セキュリティー、またはリスク管理および監督に責任を有する個人（認可担当官、 CIO（最高情報責任者）、CSO（最高情報セキュリティー責任者）、システムオーナー、情報セキュリティー管理者など）。

- セキュリティーの評価・監視責任を有する個人（監査人、システム評価者、アセッサー、独立検証者/確認者、分析者など）。

上記の役割と責任は、異なる二つの観点から見ることができる。すなわち、(i) 契約手段またはその他のタイプの組織間合意におけるセキュリティー要件を確立し、伝達する組織体としての連邦政府の観点、および (ii) 契約または合意に示されたセキュリティー要件に対応し、それに従う組織体としての非連邦政府の観点 である。

1.3 本出版物の構成

本出版物は、これ以降、以下のように構成されている。

- 第２章では、CUI セキュリティー要件の開発に用いられる前提条件と方法論、要件の形式と構造、および要件を獲得するために NIST 規格および指針に適用される適応規準について記述する。
- 第３章では、非連邦政府システムおよび組織において、CUI の機密性を保護する 14 のセキュリティー要件ファミリーについて記述する。
- 補足の付属書では、非連邦政府のシステムおよび組織における CUI 保護に関連した付加情報を提供する。それには以下が含まれる。 (i) 一般的参照情報、(ii) 定義および用語集、(iii) 本出版物で使われる頭字語、(iv)セキュリティー要件を「NIST SP 800-53」と「ISO/IEC 27001」のセキュリティー管理に関連付ける対応表、 (v) 中位セキュリティー管理ベースラインで採用された適応判断の説明である。