連邦政府の情報セキュリティを飛躍的に向上させる
新たな FISMA 規格およびガイドライン

Ron Ross, Stuart Katzke and Patricia Toth
Computer Security Division
National Institute of Standards and Technology

要約

2002 年に制定された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 と称する）は、連邦政府に対し、その情報と情報システムの保護に関する重要な要求事項を定め、米国国立標準技術研究所（NIST：National Institute of Standards and Technology、以下、NIST と称する）に対しては、連邦政府の FISMA 準拠をサポートするための重要な要求事項を定めている。こうした重要な法律を踏まえ、NIST は、FISMA 導入プロジェクトの一環として、（http://csrc.nist.gov/sec-cert/index.html）情報システムセキュリティに関する重要な規格およびガイドラインの策定を行っている。この最重要プロジェクトは、セキュリティ分類規格の策定、情報システムのセキュリティ管理策の仕様、選択、テストに関する規格およびガイドライン、認証のためのレビューおよび情報システムの運用認可についてのガイドライン、そして、意図した通りの運用を確実に行うための継続的な監視についてのガイドラインを含む。本稿は、NIST による FISMA リスクマネジメントフレームワークの考察および、連邦政府の FISMA 要求事項への準拠をサポートするために、NIST によって策定された一連の関連規格およびガイドラインについて述べたものである（例：FISMA に関する一連文書など）。本稿ではさらに、FISMA リスクマネジメントフレームワークの導入が、政府機関のシステムにいかなる恩恵をもたらし、このリスクマネジメントフレームワークおよび関連規格やガイドラインが、なぜ政府機関の他部門（例：国防総省など）や民間企業に取って関心の高いものであるかについても論じている。

序章

2002 年に制定された連邦情報セキュリティマネジメント法（http://csrc.nist.gov/policies/FISMA-final.pdf）は、連邦政府に対し、その情報と情報システムの保護に関する重要な要求事項を定め、米国国立標準技術研究所（NIST：National Institute of Standards and Technology、以下、NIST と称する）に対しては、連邦政府の FISMA 準拠をサポートするための重要な要求事項を定めている。こうした重要な法律を踏まえ、NIST は、FISMA 導入プロジェクトの一環として、（http://csrc.nist.gov/sec-cert/index.html）情報システムセキュリティに関する重要な規格およびガイドラインの策定を行っている。この最重要プロジェクトは、セキュリティ分類規格の策定、情報システムのセキュリティ管理策の仕様、選択、テストに関する規格およびガイドライン、認証のためのレビューおよび情報システムの運用認可についてのガイドライン、そして、意図した通りの運用を確実に行うための継続的な監視についてのガイドラインを含む。
NIST によって策定されたこれら文書の中で最も重要な規格が FIPS 199「連邦政府の情報および情報システムに対するセキュリティ分類規格（Standards for Security Categorization of Federal Information and Information Systems）」である(FIPS： Federal Information Processing Standard 連邦情報処理規格 http://scrc.nist.gov/publications/fips/index.html#hips199)。この新たな規格は、FISMA の規定する国家セキュリティシステム以外のシステムに対しては強制力のあるものであり、米国政府が、その国家セキュリティシステム以外のセキュリティ情報および情報システムを防衛するための重要な変更を提起している。なお、国家セキュリティシステム以外のセキュリティシステムには、国の重要インフラに匹敵する政府のシステムを含んでいる。

本稿では次の項目についても論じることとする。

- FISMA が連邦政府の IT セキュリティプログラムおよび NIST 規格および研究にもたらす影響
- FISMA リスクマネジメントフレームワークおよび当該プロジェクトに関する一連のガイダンスおよび規格を含む NIST の FISMA 導入プロジェクト
- NIST の FISMA リスクマネジメントフレームワークの重要な特徴
- FISMA のリスクマネジメントフレームワークが連邦政府のセキュリティプログラムにもたらす恩恵
- FISMA リスクマネジメントフレームワークの民間企業および政府他部門（例：国防総省など）の情報システムへの導入

2002 年連邦情報セキュリティマネジメント法（電子政府法タイトル Ⅲ）

2002 年に制定された電子政府法（一般法 107-347）（http://csrc.nist.gov/policies/HR2458-final.pdf）は、米国の経済界や国家セキュリティ関連組織に、情報セキュリティの重要性を再認識させるものである。本法

は、電子サービスの開発を促進し、国民の情報へのアクセス利便性の向上を目的として、省庁間の協力を促すものである。また、本法は、情報へのアクセス利便性の拡大を図る傍ら、個人のプライバシー、国家セキュリティ、記録の保存および障害者のアクセス利便性の保護を目的とする。当該規定により、行政管理予算局（OMB：Office of Management and Budget、以下、OMB と称する）内に電子政府局が設立され、その局長は、大統領によって任命されている。電子政府局は、省庁間の協力体制や統合プロジェクトの調整や監視を行い、政府機関の情報やサービスの利便性向上に努める。また、当該局は、革新的な政府機関プロジェクトをサポートすることを目的とした電子政府ファンドや、委託業者の革新的システム開発を支援するプログラムの運用を行なっている。

電子政府法タイトル III は FISMA と称され、連邦情報システムにおいて、情報セキュリティ管理策の効果を拡大していくことの必要性を説いたものである。FISMA は多くの要求事項を規定しているが、とりわけ、連邦政府機関それぞれに対し、その機関全体にわたってセキュリティを向上させるための行動計画を策定し、文書化し、導入することを求めている。セキュリティ向上活動とは、当該政府機関の情報や、業務をサポートする情報システム、資産のセキュリティを改善していく活動をいう。政府機関の情報セキュリティプログラムには、以下の要件が含まれなければならない。

- 政府機関の業務や情報資産に影響を及ぼす**リスクおよび、損害規模の定期的なアセスメント**
- リスクアセスメントに基づいた費用対効果の大きいリスクの低減策に関する**ポリシーおよび実施手順**
- ネットワーク、設備、情報システムまたは、情報システム（グループ）に適切な情報セキュリティをもたらすための**計画**
- 職員、契約社員および、政府機関情報システムを使用する他ユーザに対する**セキュリティ意識向上トレーニング**
- 情報セキュリティポリシー、手順および、導入の効果の**定期的なテストおよび評価。**これには、それぞれの政府機関でリストアップされた情報システムすべてに導入されている、管理的、運用的、技術的管理策を含む。
- あらゆる不具合に関する**復旧活動**の計画、導入、評価および、文書化のプロセス
- **セキュリティインシデント**の検知、報告および、対応手順
- 政府機関の業務をサポートする情報システムや資産を守り、**業務の継続**を保証する計画および手順。

FISMA は、連邦政府機関をサポートするため、NIST に対して、次の事項の策定を義務付けている。

- 連邦政府機関が、リスクレベルに応じ情報セキュリティの適切なレベル付けを行うために利用する**情報および、情報システムの分類規格**
- **各カテゴリに含まれる情報および情報システムのタイプ**を推奨するガイドライン
- それぞれの分類における、情報および情報システムの管理的、運用的、技術的セキュリティ管理策などの必要**最低限の情報セキュリティ要件**

NIST による FISMA 導入プロジェクト

FISMA の規定に対応し、NIST は、FISMA 導入プロジェクトのフェーズ I[1]に着手した。フェーズ I は、図 1（p.3）のリスクマネジメントフレームワークを包含する（下段も参照[1]）。リスクマネジメントフレームワークが「システム指向（情報システムやその情報に焦点をあわせている）」であるのに対し、FISMA 導入プロジェクトは、情報システムやその情報へのセキュリティ違反により、事業体（連邦政府機関、金融機関、電力会社、医療機関など）が被るリスクを管理することを目的とする。従って、リスクマネジメントフレームワークは、FISMA が NIST に定めた上記 3 項目よりもさらに広範である。FISMA 要求事項を満たすため、NIST は、この時機をとらえ、1983 年に発行した FIPS102「システムセキュリティ認証および認可ガイダンス」を改訂することを決定した。リスクマネジメントフレームワークは、リスクアセスメント、セキュリティ計画などに加え、システム開発ライフサイクルで発生するその他のセキュリティ関連の業務を含む。

[1] フェーズ II では、NIST Special Publication 800-37、800-53 および 800-53A に従い、セキュリティアセスメントを実施する組織を承認するプログラムを規定する。
フェーズ III（現在は、財源が確保されていない。）では、FISMA リスクマネジメントフレームワークを支援するベンダーのツールを評価するプログラムを規定する。

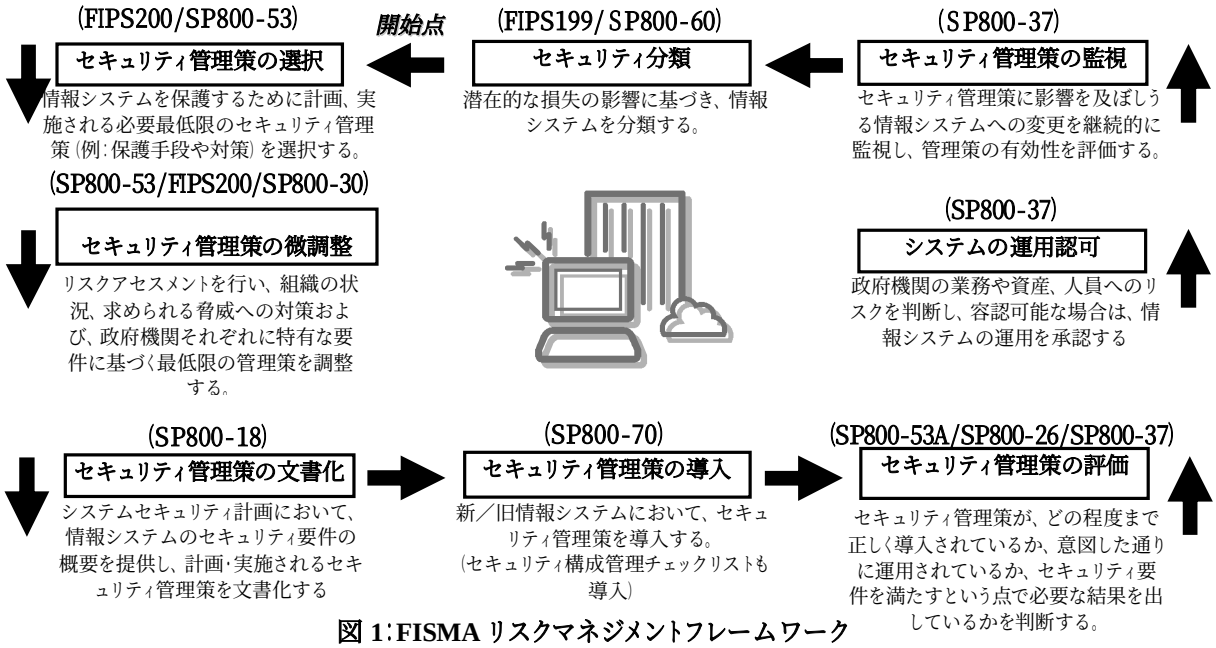

図 1：FISMA リスクマネジメントフレームワーク

図 1 を参考に、NIST による FISMA 導入プロジェクトおよび FIPS199：***連邦政府の情報および情報システムに対するセキュリティ分類規格***を解説する。2004 年 2 月に施行された FIPS199 は、NIST が「連邦政府機関が、脅威レベルに応じて情報セキュリティの適切なレベル付けを行うために利用する、情報および情報システムの分類規格」を策定するという FISMA 要求事項に合致するものであり、国家セキュリティシステム以外のセキュリティシステムに適用される強制力のある連邦規格である。本規格は、発行されたその日に施行された。

FIPS199

膨大な数の連邦情報システムにおいて FIPS199 の重要性や潜在的な影響を理解するため、始めに、情報技術の世界が過去 20 年間にどのような変化を遂げたかを理解しなければならない。ごく最近まで、連邦の事業体で一般的な情報システムには、施設において、物理的にスペースを占拠し、組織予算の相当額を費やす大型で高価なスタンドアローン型のメインフレームが含まれていた。当時の情報システムは、効果的な管理を行うために特化したポリシーや手順が必要な「高額商品」として見なされていた。今日の情報システムは、さらに高性能であるが、比較的低コスト（同等な演算能力において）であり、ネットワーク化、ユビキタス化されている。システムは、政府機関のミッションを遂行することと密接に結びついているにも関わらず、多くの場合、一般消費財とみなされている。しかしながら、技術が進化し、次世代情報システムに新たなアクセス方法が導入され、ユーザ人口が拡大すると、これまでのシステムを保護するために採用されていたポリシー、手順、アプローチでは対応が困難になってきた。

従来の方法でビジネスを行うことの問題点

かつて、エイブラヘム・リンカーンは「一握りの人々を欺き続けたり、全ての人々を一時的に欺くことはできても、全ての人々を欺き通すことはできない。」と言っている。この引用句の精神は、政府機関の情報および情報システム（サポートされるべきミッションおよび、提供されるべきサービスを含む）を保護するために駆使される、今日の高度な技術的方法論にあてはめることができる。全ての連邦情報システムを常に高度な技術で保護し続けるための管理および、技術的費用を捻出することは、特に政府機関の予算が困窮している時期には非常に困難である。情報技術が一般消費財である現代においては、費用対効果の高い情報システムセキュリティ（行政管理予算局通達 A-130、付録 III において定義；http//www.whitehouse.gov/omb/circulars/a130/a130trans4.html）を実現するために、セキュリティに関する考え方を根本的に変えることを求められている。つまり、***政府機関のミッションを果たす上でのそのシステムがどの程度重要であるかに基づき、情報システムはが評価され、その優先度が決定されなければならない。***

政府機関の情報システムでは、当該システムへの優先度を決定する際の重要性や機密性の線引きが明らかである。重要な情報インフラの一部として、非常に機密性の高いミッションクリティカルな業務を実行する高優先度の情報システムが存在する傍ら、政府機関の日常的な業務を実行する優先度の低い情報システムも存在する。従って、全ての情報システムに対する防衛策や対策（例：セキュリティ管理策など）の導入は、構築された政府機関の優先度（例：当該システムは、政府機関のミッションをサポートする際に重要性／機密性のどこに位置づけられるか、など）を基に個々のシステムについて調整が行われなければならない。連邦情報システムにおけるセキュリティ管理策のテストや評価に費やされる作業量、当該システムの業務ミッションに対するリスク判断やリスク受容（例：セキュリティの認証と認可）についても、同様に政府機関の優先度に基づくこととする。ごく最近まで、政府機関が自身の情報システムのセキュリティ優先度を決定する際に有効な詳細規格やガイドラインの数は限られていた。その結果、多くの政府機関は、重要性／機密性の低い情報システムを保護するために、非常に多くの管理的、技術的リソースを使い果たし、重要性／機密性が高いシステムを保護するためのリソースが十分ではなかった。ある種の「負荷分散」が必要であった訳である。

FIPS199 および、FISMA リスクマネジメントフレームワークによる新たな時代への先導

連邦政府のセキュリティ分類規格である FIPS199 では、連邦政府の業務や情報資産をサポートする膨大な数の情報システムを保護するに際し、ある種の秩序や規律を導入するための初期段階の手続きを定めている。この規格は、政府機関の情報システムに関する優先度や、システムを保護するための適切な対策の適用を判断する、簡潔かつ、しっかりとした概念に基づいたものである。特定の情報システムに適用するセキュリティ管理策は、システムの重要性および損なわれやすさと釣り合いが取れていなければならない。FIPS199 では、この重要性と損なわれやすさを、機密性（例：情報の不正な公開など）、完全性（例：情報の改ざんなど）または、可用性（例： DoS など）を損うセキュリティ違反の発生により、政府機関の業務（ミッション、機能、印象および、評価）、政府機関の情報資産または人員が受ける潜在的影響に基づき分類している。FIPS199 は、連邦政府に対し、全ての情報のタイプ、システムについて、3 つのセキュリティ目的である機密性、完全性（信頼性、非拒否性を含む）、および可用性に対して、低、中、高度の影響をそれぞれ分類することによって優先度付けを行うことを求めている。

システム開発ライフサイクルの中で、FIPS199 および FISMA リスクマネジメントフレームワークは、政府機関のリスク管理プログラムの一部として利用され、それぞれの情報システムに対し適切なセキュリティ管理策を適用し、その管理策が、どの程度まで正しく導入されているか、目的に沿って運用されているか、セキュリティ要件を満たすという点で必要な結果を出しているかを評価し判断する手助けとなるものである。図 1 の FISMA リスクマネジメントフレームワークに基づき、次の行為が、システム開発ライフサイクルの中で、新･旧双方の情報システムに適用される。

- FIPS199 の影響分析に基づいた、情報システム（および、当該システムに存在する情報）の***分類。***（セキュリティ分類の割当てと影響分析の精緻化のガイドである NIST Special Publication 800-60、*情報タイプおよび情報システムのセキュリティ分類へのマッピングに関するガイドライン* 参照）
- FIPS199 セキュリティ分類に基づく情報システムに関するセキュリティ管理策の（開始地点としての）初期***選択。***（NIST Special Publication 800-53、*連邦情報システムにおける推奨セキュリティ管理策*[2] 参照）
- 選択された初期セキュリティ管理策の***微調整。***政府機関に特化したセキュリティ要件、特定の脅威情報、費用対効果分析、代替管理策としての可用性の確保または、その他の特別な条件など、その組織特有の状況に基づく微調整。（NIST Special Publication 800-30、*IT システムのためのリスクマネジメントガイド* 参照）。
- 初期管理策の改良や微調整の根拠や正当性の記述を含み、承認され同意されたセキュリティ管理策のシステムセキュリティ計画における***文書化***（NIST Special Publication 800-18、*情報技術システムに関するセキュリティ計画策定に関するガイダンス* 参照）。
- セキュリティ管理策の情報システムへの***導入***。レガシーシステムでは、選択されたセキュリティ管理策の一部または全部は、既に導入されているかもしれない。（NIST Special Publication 800-64、*情報システム開発ライフサイクルにおけるセキュリティの考慮事項* 参照）

[2] 連邦情報システムに関するセキュリティ管理である FIPS200 は、2005 年 12 月を持って、連邦情報システムの最小セキュリティ基本要件に係る FISMA 立法要件の履行に伴い、NIST Special Publication 800-53 の置き換えを行う。

- セキュリティ管理策の***評価***。適切な手法および手順を用い、セキュリティ管理策がどの程度まで正しく導入されているか、目的に沿って運用されているか、セキュリティ要件を満たすという点で必要な結果を出しているかの判断を行う。[3]（初期公開用ドラフトである、NIST Special Publication 800-53A、*連邦情報システムにおけるセキュリティ管理策の評価に係るガイダンス*参照）
- 計画もしくは、運用されている情報システムからもたらされる政府機関の業務（ミッション、機能、印象または評価を含む）、政府機関の情報資産または人員に対するリスクの***判断***。（NIST Special Publication 800-37、*連邦政府情報システムのセキュリティ認証および認可ガイド*参照）
- 政府機関の業務、情報資産または人員に対するリスクレベルが、承認責任者が容認できるものであった場合のシステム運用（レガシーシステムの場合は、システムの運用継続）の***承認***。（NIST Special Publication 800-37、*連邦政府情報システムのセキュリティ認証および認可ガイド*参照）
- システムに対する変更の文書化、変更に関するセキュリティ影響分析の実施および当該システムのセキュリティ状況を適切な担当上官へ定期的に報告を行うこと、などを含む、情報システムに対して選択されたセキュリティ管理策の継続的***監視***。（NIST Special Publication 800-37、*連邦政府情報システムのセキュリティ認証および認可ガイド* 参照）
- 情報システムまたは、当該システムに関するセキュリティ要件に***大幅な変更***がある場合、政府機関に対し、上の行為[4]が迅速に行われるよう促すことがある。

リスクマネジメントフレームワークの重要な特性

FISMA リスクマネジメントフレームワーク、関連する一連の規格および、ガイドラインには、IT セキュリティリソースを費用対効果の点でより効率的に利用できるような、次の特性が含まれる。

- セキュリティ分類規格（FIPS199）は、国家セキュリティシステム以外の全ての連邦政府のセキュリティ情報および情報システムに適用される。これは、情報システムの中の情報および情報システム自体の機密性、完全性、可用性が危険にさらされた場合の最悪の影響評価に基づいたものである。
- セキュリティ分類規格は、組織のシステムの優先度づけをサポートし、最も影響の大きいシステムに対し、優先的にセキュリティ対策を行えるようにする。
- セキュリティ分類規格は、組織のセキュリティ対策レベルの判断をサポートし、組織が自身の情報システムのセキュリティ分類に見合ったセキュリティ対策を導入できるようにする。
- 基本的なセキュリティ管理策と、（可能な場合）1つまたは、それ以上の補強策を含むセキュリティ管理策カタログ。（SP800-53）
- 管理策カタログには、セキュリティレベル低、中および高のそれぞれに対する必要最低限の管理策（ベースライン）が、NIST によって示されている。どのセキュリティレベルの管理策に対しても機能および保証要件を追加でき、セキュリティレベル低の管理策のすべてを包含するよう、管理策集は階層構造になっている（SP800-53）。
- 共通のセキュリティ管理策と、共通のセキュリティ管理策に対するセキュリティ評価結果の再利用という考え方。共通の管理策のセキュリティ評価結果を再利用することによって、情報システムのセキュリティ評価において求められる管理策評価作業を削減できる。情報システムにおける共通のセキュリティ管理策には次の項目が含まれる。

  1）政府機関全体の管理策 （例：トレーニング、人的セキュリティ）
  2）サイト全体の管理策 （例：物理的セキュリティ、緊急時対応計画）；
  3）共通のサブシステム管理策 （例：複数サイトに配置される共通のソフトウェアパッケージ）。
- 作業量が小さいと推定されるセキュリティレベル低のシステムに対する認証および認可については、その認証および認可作業量を著しく削減することとする。
- ベースラインに依存する保証要件（例：特定の必要最小限のベースライン管理策ではその保証要

[3] 評価手続きにおけるセキュリティ管理策の有効性の判断は、付加的管理の採用もしくは、無効な管理の修正といった、是正措置を求めることがある。NIST Special Publication 800-53 参照。

[4] 著しい変更とは、通常、情報システムの保護能力および、システムセキュリティポリシーの施行に影響を及ぼすことがあるハードウェア、ソフトウェアまたは、ファームウェア・コンポーネントに対するあらゆる変更として定義される。事例には、新たなまたは、アップグレードされたオペレーションシステム、ファイヤーウォール、データベース管理システム、ネットワークデバイスまたは、識別および、承認メカニズムの導入が含まれる。

件は同じ）。ベースラインが上るに従い、管理策の開発者／導入者が、導入された管理策の品質、正確性および機密性を立証し、分析するレベルも上ることが求められる。
- 保証要件は、NIST Special Publication 800-53A における管理策評価のアプローチと関連し、これをサポートする。

FISMA リスクマネジメントフレームワークが政府機関のセキュリティプログラムにもたらす恩恵

FISMA リスクマネジメントフレームワークでの取り組みを、連邦政府機関の情報システムに採用することによって得られる長期的な効果は、目標がより明確で、費用対効果が大きく、より良いセキュリティが実現できることである。情報システムの相互接続によって、政府機関のオペレーションや情報資産に対するリスクが増大するが、FISMA リスクマネジメントフレームワークは、情報セキュリティに関する共通のアプローチや理解を提供し、異なった組織のリスクマネジメントに一貫性をもたらすものである。政府機関は、これらシステムのセキュリティ分類に基づき、任命されたミッションを遂行するために最も重要な情報システムがどれかを判断し、当該システムを適切に保護することになる。政府機関は、どのシステムが自身のミッションにとって最も重要ではないかについても判断し、こういったシステムの保護に関し、必要以上の資源の割り当ては行わない。

情報システムが一般消費財とみなされ、政府や重要なインフラにおいて国家の最も重要な資産を保護するために日常的に用いられる高度技術時代の現在においては、FISMA リスクマネジメントフレームワークはまさに時宜を得たものである。FISMA リスクマネジメントフレームワーク関連の新たなセキュリティ規格やガイドラインを適切に導入することで、情報システムの保護に関する使用可能なリソースをさらに効果的に割り当て、必要性を判断し、リソースを追加する際の正当性を提示し、政府機関の情報システム[5]セキュリティを大幅に改善できることだろう。

FISMA リスクマネジメントフレームワーク関連ガイドラインの民間のセキュリティプログラムへの利用

NIST ガイドラインは、連邦政府機関を対象にしたものであるが、FISMA リスクマネジメントフレームワーク（関連規格および、ガイダンス文書を含む）は政府だけを対象にしたものではない。FISMA リスクマネジメントフレームワークは、連邦政府と同様に、民間企業にも適用できる。民間企業が、本文書で述べるアプローチを用いることは要求事項ではないが、FIPS199 が連邦政府機関に強制力を持つことで、FIPS199、つまり FISMA リスクマネジメントフレームワークや一連の関連文書が連邦社会における「適正義務」基準となるであろう。重要インフラセクタでは、民間及び政府のセクタが相互に連携しており、重要インフラセクタでは、民間の重要インフラセクタでも政府と同様の「適正義務」基準が適用されることが予想される。結果として、政府は、民間の重要インフラシステムにも、ここで述べられた国家レベルのセキュリティシステム以外の連邦政府のシステムに対すると同様の強固なアプローチを求める可能性があるということである。

さらに、民間セクタが当該アプローチをなぜ採用もしくは、適用しなければならないかについては、次のような別の理由がある。

- NIST は、FISMA リスクマネジメントフレームワークおよび、一連の関連文書を IEEE 情報保証規格ワークグループに対して、産官共通規格（http://issaa.org/）の候補として提出した。IEEE 規格は、情報システム・セキュリティ保証アーキテクチャ（ISSAA：Information System Security Assurance Architecture）と呼ばれる。ISSAA は、IEEE における FISMA リスクマネジメントフレームワークである。NIST の FISMA 関連文書が、それぞれの IEEE 規格（ISSAA 全体の作業の一部として）に関する候補として、IEEE ワークグループに提供される場合でも、当該ワークグループは、NIST 文書を採用したり改変したり、もしくは、自身が望ましいと考えられるアプローチ（ISSAA／FISMA リスクマネジメントフレームワークの目的に整合する範囲において）を採用することができる。
- 管理策カタログおよび、必要最低限の管理策（ベースライン）（NIST Special Publication 800-53 に記載）は、様々なセキュリティ管理策集を参照し、取り入れており、例えば、コモン・クライテリア・パート 2、ISO／IEC17799、COBIT、GAO FISCAM、NIST Special Publication 800-26 自己アセスメントチェックリスト、CMS（健康管理）、D／CID6-3 要件、DoD 方針 8500 および、BIT 機能

[5] 本書が論じる FISMA 関連のセキュリティ規格および、ガイドラインは、FISMA 導入プロジェクトのサイト http://www.csrc.nist.gov/sec-cert からも閲覧が可能である。

対策[6]などの非常に多くの官民セクタ資源の管理策集と一貫性を保っている。

- 管理策カタログや、その業界に特有の情報技術アプリケーションやシステム要件に合致させるために策定された管理規格には、別途管理策を追加することができる。このような事例としては、SCADA／リアル･タイム処理システム、健康管理／HIPAA および、金融機関／サーベンス･オクスリー（企業改革法）のセキュリティ要件を満たす必要性がある民間セクタが挙げられる。
- 政府に替わり情報システムの運用を行う民間企業（例：委託業者、IT サービスプロバイダ、IT 外注サービスなど）は、FISMA 要件に合致することが求められる。当該企業は、民間の顧客企業に対し、（少なくとも）自らの政府顧客に対すると同様の管理策集の導入／提供は容易に行えるであろう。
- FISMA 導入プロジェクトのフェーズ II では、NIST は、専門家および学術機関と協力して、Special Publication 800-53 に規定されているセキュリティ管理策の評価を行なう能力のある機関を承認するプログラムの構築を計画している。この活動の最終目標は、政府機関に採用され、その政府機関のセキュリティ評価をサポートする優秀なセキュリティ評価機関の確立である。NIST が、信頼のおける専門家もしくは、学術機関とのパートナーシップにより、一般に公開された手続きを経て承認プログラムを実施する場合には、民間企業も自らの管理策評価のために、政府と同様のリソースを用いることが望まれる。例えば、サイバー保険会社が、サイバー保険証書を発行する前に、承認された専門家により、潜在的なクライアントに対してセキュリティ管理策の評価を行うことが想定される。
- NIST の全規格および、ガイドラインは、通常 1 つ以上の公開ワークショップを含むレビューを経ている。一般的なレビュー手順では、NIST は、官民双方の組織から、多くのコメントや意見を受け取り、これを考慮しながら、次のドラフト文書の策定にあたる。多くの場合、政府や業界は同様の要件を持つため、NIST では、特に、NIST 規格／ガイドラインの民間セクタシステムへの適用可能性についての業界レビューやコメントを求めている。こうした調整が適切に行われた時に、我々は、民間企業が NIST ガイダンスを真に活用していると感じることだろう。

結論

FIPS199、FISMA リスクマネジメントフレームワークおよび一連の FISMA 関連ガイドラインは、連邦政府機関が用いるべきプロセス－システムの分類および優先度づけ、システムセキュリティ管理策の選択、文書化、導入、認証および認可、目的とする運用を確実に行うための継続的な監視－に著しい変化をもたらし、費用対効果が大きく、一貫性のある、改善された情報システムセキュリティ管理策の導入と政府機関の全体的なリスクの削減として結実しつつある。我々は、ここで述べられたアプローチが、民間企業にとっても適切であると信じており、これらガイダンスが民間企業で利用されることを奨励する。そして、民間企業でのアプローチや、その適用可能性について、広く意見を交わせることを望んでいる。

---

[6] COBIT（Control Objectives for Information and related technology）は、IT 統括機関（IT Governance Institute：http://www.itgi.org/）によって策定および、推進される情報技術における一般的な公開規格である。GAO（Government Accountability Office：政府説明責任局）、FISCAM（Federal Information System Controls Audit Manual：連邦情報システム管理監査マニュアル：http://www.gao.gov/special.pubs/afm.html）AIMD-12.19.6 2001 年 6 月。NIST Special Publication 800-53 の参考文献および、関連セキュリティ管理の位置づけに関する改訂版NIST Special Publication 800-26 システム･アンケート集(2005 年 4 月)は、http://csrc.nist.gov/publications/nistpubs/index.html 参照。CMS（Centers for Medicare & Medicaid Services：医療保険および、医療扶助サービス･センターは、U.S. Department of Health and Human Services（米国保険社会福祉省:http://www.cms.hhs.gov/）の連邦政府機関である。BITS は、米国大手の 100 金融機関の最高経営責任者によって運営される非営利の金融サービス業の共同体である（http://www.bitsinfo.org/）。