資料7

NISC National Information Security Center

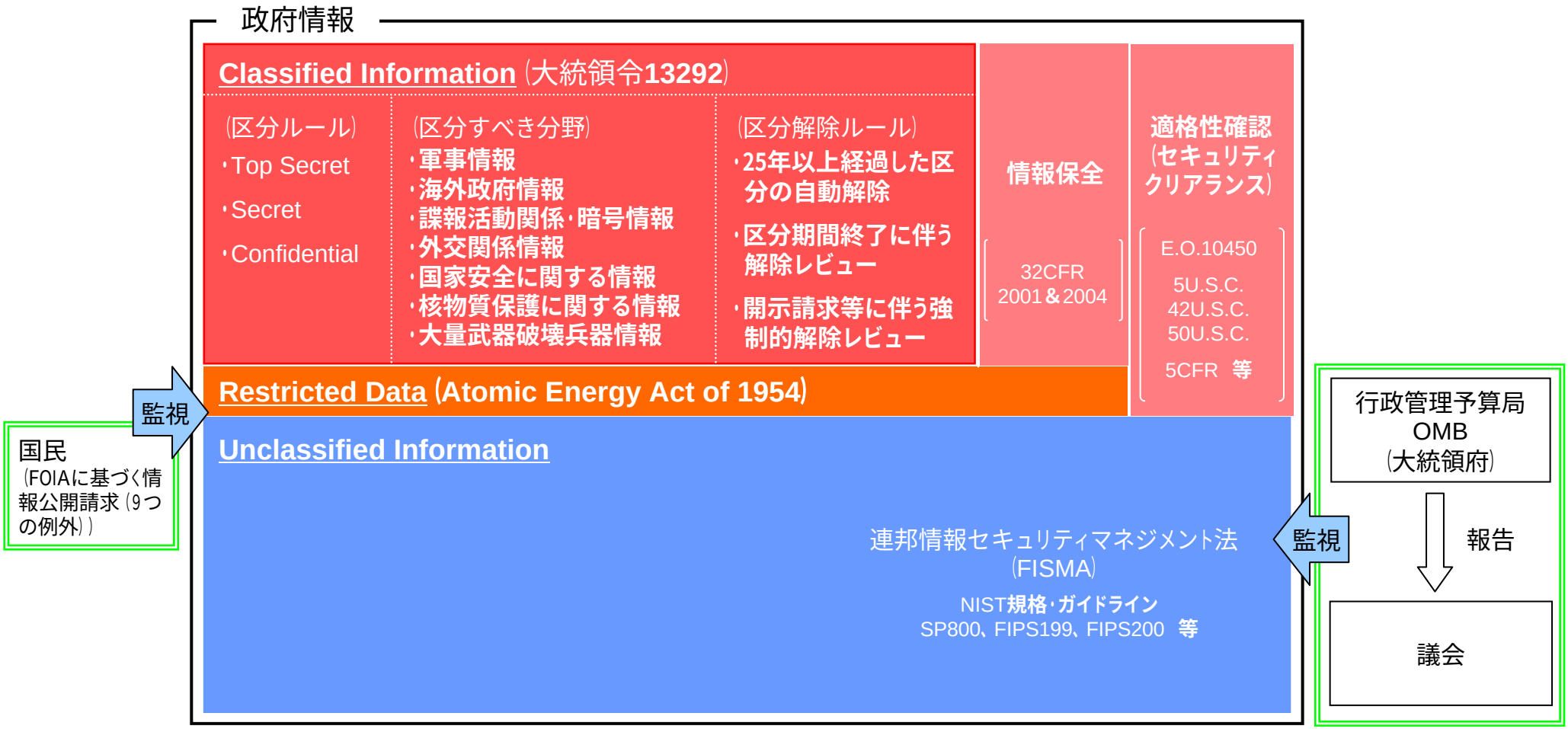
米国政府機関における
情報セキュリティ対策とその評価について

平成21年5月22日

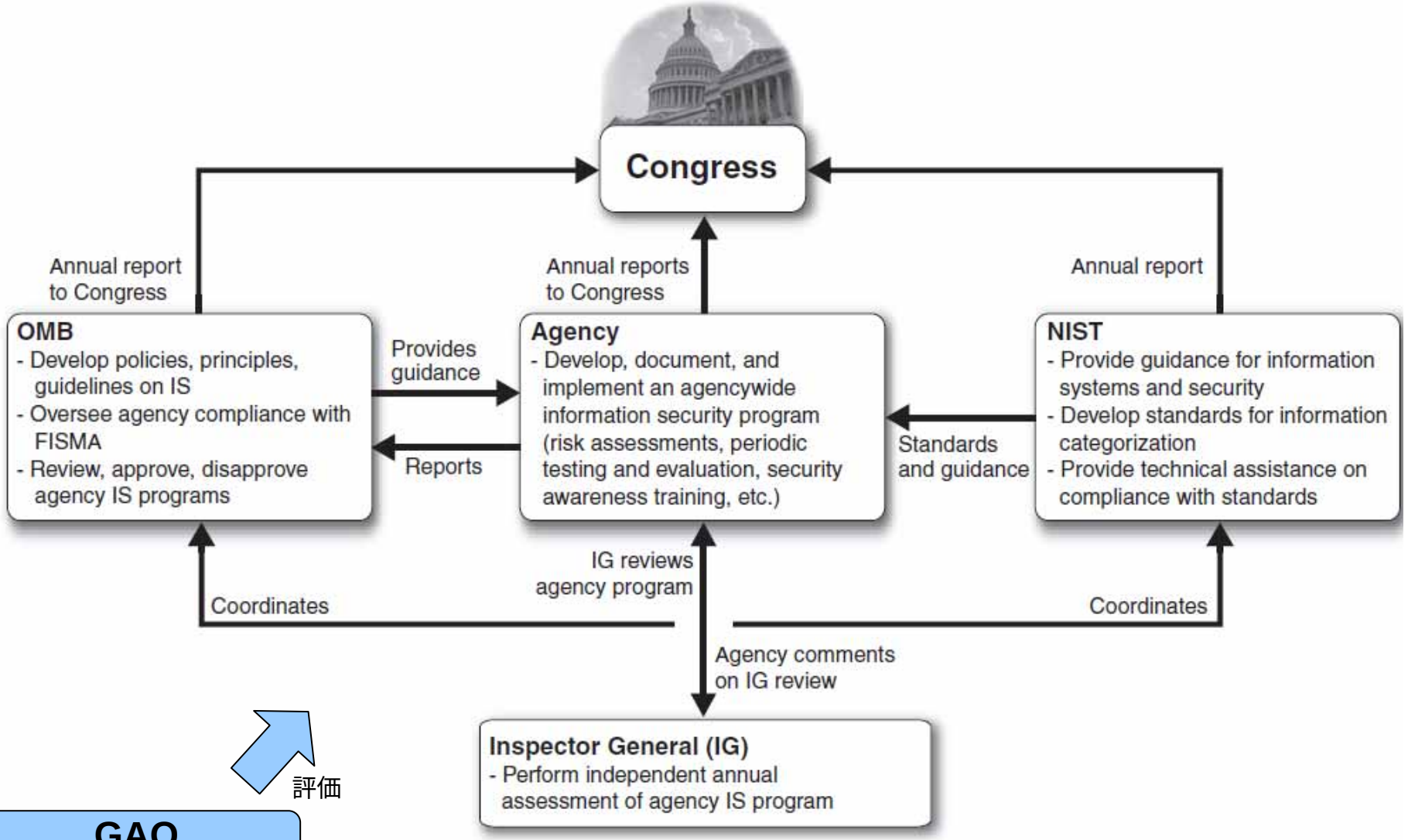
内閣官房情報セキュリティセンター（NISC）

米国政府の情報管理体制

米国政府は、大統領令13292などにより特に秘密管理が必要な情報（Classified Information）を定義し、その情報を扱う者に対しては、適格性の確認を実施している。また、その他の政府情報に関しては、連邦情報セキュリティマネジメント法（FISMA）を策定し、ガイドライン等の提供を行っている。FISMAに基づく取組がなされているかについて、行政管理予算局（OMB）が政府の取組状況をとりまとめ、議会に報告することで、レビューされている。また、情報公開法（FOIA）により、政府全体の情報管理が監視されている。



情報セキュリティに関する制度的枠組み（1）



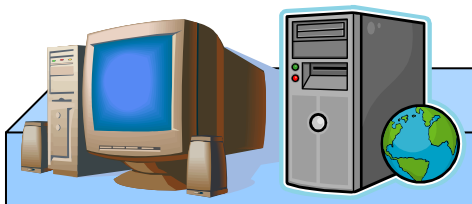
Source: GAO analysis of FISMA and implementing guidance.

情報セキュリティに関する制度的枠組み（2）

行政管理予算局（OMB）
Office of Management and Budget

報告

監視



連邦政府機関の情報システム

Certification & Accreditation（承認と運用認可）

適用

監視

National Security System

- 諜報活動に関わるシステム
- 国家安全保障に関する暗号に関わるシステム
- 軍隊の指揮管制に関わるシステム
- 兵器システムに関わるシステム
- 秘密情報(Classified Information)を取り扱うシステム

適用

適用

NIST*の策定する基準

*NIST (National Institute of Standards and Technology)：**商務省の付属機関**

（　）

CNSS*の策定する基準

*CNSS (Committee on National Security Systems)：
国防総省など関係機関の代表からなる委員会

根拠

連邦情報セキュリティマネジメント法（FISMA）
Federal Information Security Management Act of 2002

FISMA実施状況に係る2008年度OMB報告（1）

「Fiscal Year 2008 Report to Congress on Implementation of The Federal Information Security Management Act of 2002」(OMB) より

＜背景＞

- 各政府機関のCIO(最高情報責任者）及びIG（総括監査官）は、それぞれの機関の情報セキュリティプログラムを毎年度レビューし、その結果をOMBに報告しなければならない。
- OMBは各政府機関からの報告を受けて、当該年度のFISMA実施状況に係るレポートを作成し、連邦議会に報告する。

＜OMBへの報告に当たっての留意点＞

- 主要なシステム（National Security System含む）の「資産台帳（Inventory）」を作成し、メンテナンスしておくこと
- 情報及び情報システムのセキュリティを確保しておくこと
- 最低限許容できるシステム設定基準を決定し、それを遵守すること
- 各政府機関における情報セキュリティ上の課題への「対応方針及びマイルストーン（Plan of Action and Milestones: POA&M）」を策定すること

FISMA実施状況に係る2008年度OMB報告（2）

＜OMB報告の概要＞

- 承認と運用認可（Certification & Accreditation: C&A）
  - ✓ 2008年度には、C&Aを実施したシステムの割合は2007年度の92%から96%に増加。
- 障害対応計画とセキュリティ対策のテスト
  - ✓ 2008年度には、92%のシステムの障害対応計画のテストを行い、セキュリティ対策のテストも93%のシステムで実施。これはそれぞれ前年度の86%から増加、95%から減少。
- 資産台帳
  - ✓ 25の政府機関のうち24機関の総括監査官（IG）から、資産台帳整備が80%終了したと報告。しかし、幾つかの機関からは資産台帳の整備割合が低下したとの報告もあった。これは主に資産台帳の対象とすべきシステムの定義について未だ不十分な点等があることに基づく。
- C&Aプロセスの質
  - ✓ 政府機関のIGの92%からC&Aプロセスの全体的な質は”satisfactory”である旨の報告があった。これは前年度の76%から改善。
- 脅威影響度レベルの評価
  - ✓ 連邦政府機関の管理する全10,679システムのうち、影響度「高」（high impact）のシステムは1,168、影響度「中」（moderate impact）のシステムは4,112、影響度「低」（low impact）のシステムは4,690であり、評価されていないものは709システム。

＜OMB報告の概要(続)＞

- システムのセキュリティに関する職員教育
  - ✓ 2008年度にセキュリティの理解教育を受講した職員の割合は、前年度の88%から89%に増加。
- 契約者運用システムの監督
  - ✓ 政府機関が契約者に運用を委託しているシステムについてもFISMA等の基準に基づくことが要求されているが、「ほぼ常に(almost always)」満たしているとする政府機関は、前年度の12機関から8機関に減少。
- 全省的な対応方針及びマイルストーン（POA&M）
  - ✓ 各政府機関においてセキュリティ上の課題が明らかになった場合、各機関は全省的なPOA&Mを策定することが求められているが、84%の政府機関で欠陥を特定し修正するための効果的なPOA&Mプロセスがあると回答。
- 構成管理
  - ✓ 各政府機関において自分達の政府機関政策としてFederal Desktop Core Configuration(FDCC)を採用と報告。

FISMA実施状況に係る2008年度OMB報告（4）

＜OMB報告の結論＞

- これまで各政府機関は、ITセキュリティのパフォーマンス評価基準のギャップを縮小する努力を続けてきた。
- 各政府機関は以下の取組に注力する。
  - ✓ 全ての情報システムについてC&Aを100%達成する。
  - ✓ 契約者が運営するシステムについて確実に把握し、監督を行う。
  - ✓ 100パーセント適切なシステムのためにPIAとSORNを維持する。

    （PIA：Privacy Impact Assessment ／ SORN：System of Records Notice）

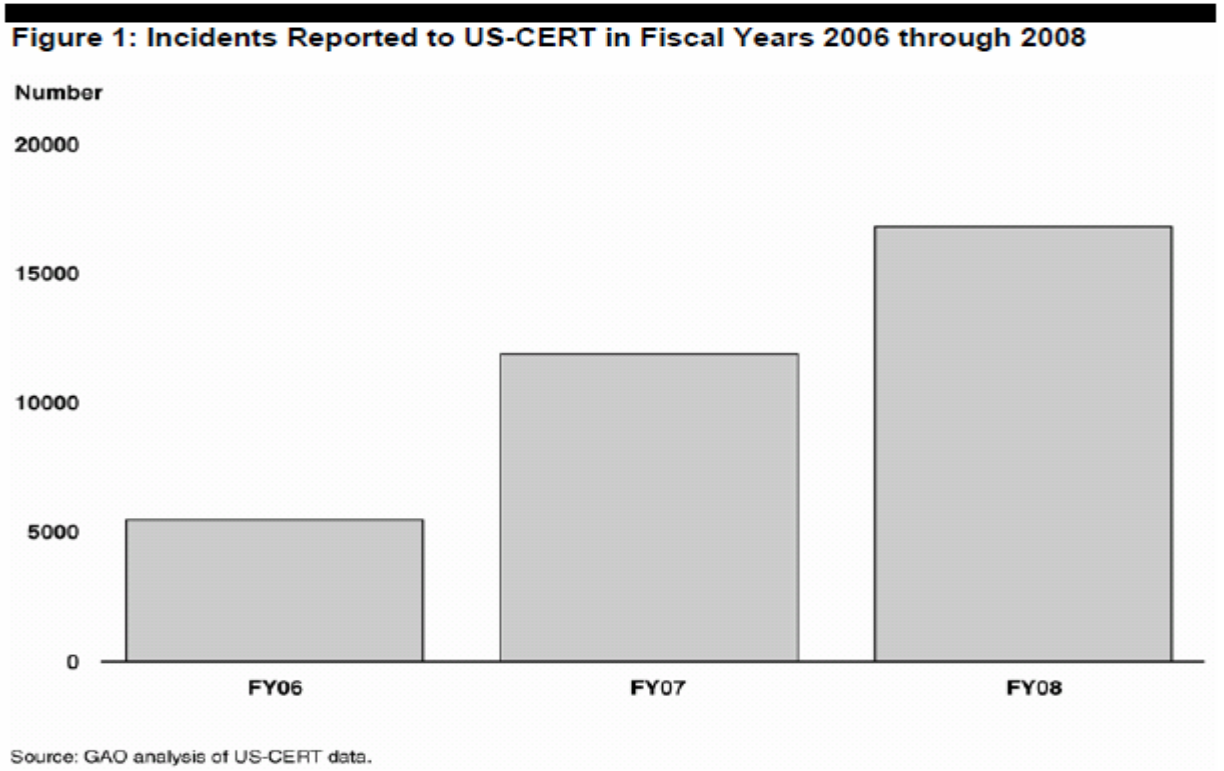
各政府機関の総括監査官による評価

Table 4: Results of IG Assessments for Fiscal Year 2008 FISMA annual report

Agency	Effective POA&M ?	Quality of Certification and Accreditation Process	Completeness of System Inventory	Quality of Privacy Impact Assessment Process
Agency for International Development	Yes	Excellent	96-100%	**Excellent +**
Department of Agriculture	No	Poor	**81-95% +**	**Satisfactory +**
Department of Commerce	Yes	**Satisfactory +**	96-100%	Good
Department of Defense	No	Failing	0	Failing
Department of Education	Yes	Satisfactory	96-100%	**Excellent +**
Department of Energy	Yes	Satisfactory	96-100%	Satisfactory
Environmental Protection Agency	Yes	**Good +**	96-100%	**Excellent +**
General Services Administration	Yes	Satisfactory	96-100%	Satisfactory
Department of Health and Human Services	Yes	**Satisfactory -**	**81-95% -**	**Good -**
Department of Homeland Security	Yes	**Good +**	96-100%	Good
Department of Housing and Urban Development	Yes	Satisfactory	96-100%	**Satisfactory -**
Department of the Interior	No	**Satisfactory +**	96-100%	**Excellent +**
Department of Justice	Yes	**Good -**	96-100%	Excellent
Department of Labor	Yes	Satisfactory	96-100%	Good
National Aeronautics and Space Administration	**Yes**	**Excellent +**	96-100%	Good
National Science Foundation	Yes	Good	96-100%	Excellent
Nuclear Regulatory Commission	Yes	**Satisfactory +**	**96-100% +**	Excellent
Office of Personnel Management	Yes	**Satisfactory -**	96-100%	**Excellent +**
Small Business Administration	Yes	Satisfactory	96-100%	Satisfactory
Smithsonian Institution	Yes	Satisfactory	**96-100% +**	**Satisfactory -**
Social Security Administration	Yes	**Good -**	96-100%	**Excellent +**
Department of State	**Yes**	**Good +**	96-100 %	**Good +**
Department of Transportation	**No**	Satisfactory	96-100%	**Satisfactory -**
Department of the Treasury	Yes	Satisfactory	**96-100% +**	Satisfactory
Department of Veterans Affairs	**Yes**	**Satisfactory +**	**96-100% +**	**Satisfactory +**

US-CERTに報告された連邦政府機関におけるセキュリティ事案の件数

- FISMAは、各政府機関に対してセキュリティ事案を取りまとめてUS-CERTに報告することを求めている。
- 2008年度の報告内容は以下の通り。
  - 各政府機関は、セキュリティ事案を報告する手順を持っており、この手順には、US-CERTに報告する手順も含まれている。
  - 25の主要政府機関の内、22の政府機関では、機密情報や重要な情報への参照や変更の記録や監視をすると報告している。



GAOによる2007年度議会報告

「Information security: Progress Reported, but Weaknesses at Federal Agencies Persist」(GAO-08-571T) より

＜GAO報告の要旨＞

- 各政府機関からの報告によれば、C&Aを実施したシステムの割合が増加するなど、米国の政府機関の情報セキュリティ対策は着実な進歩を遂げているとされている。
- 一方、いくつかの政府機関の総括監査官からは、当該政府機関の報告内容に同意しておらず、情報セキュリティ対策を実施するプロセスに弱点があることを指摘している。
- その結果、政府機関からは進歩が報告されているにもかかわらず、各政府機関は情報セキュリティ対策上の欠陥に直面している。
  - ✓ 大半の政府機関は、自身のネットワークへのアクセスを十分に制限したり検知する対策を講じていない。
  - ✓ 各政府機関は、ネットワーク機器の設定を適切に管理したり、主要なサーバ等へのパッチを適切な時期に適用したり、一人の人間が重要なシステムの管理を全て行わないように権限を分散したりする等の点が必ずしもできているわけではない。
- しかしながら、GAOや各省のIGからの数多くの指摘を実施することは可能であり、OMBや他の政府機関も政府全体の情報セキュリティを改善するための取組みを進めており、連邦政府機関の情報セキュリティを改善する機会は十分にある。

(参考) 2007年度の連邦政府機関評価 (下院・政府監視改革委員会)

各政府機関が提出したFISMAレポートに基づき、下院の政府監視改革委員会がまとめた連邦政府機関のセキュリティ評価

FEDERAL COMPUTER SECURITY REPORT CARD May 2008

GOVERNMENTWIDE GRADE 2007: C (2006: C-)

	2007	2006		2007	2006
DEPARTMENT OF JUSTICE	A+	A-	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	C	D-
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+*	A+	DEPARTMENT OF STATE	C*	F
ENVIRONMENTAL PROTECTION AGENCY	A+	A-	DEPARTMENT OF EDUCATION	C-	F
NATIONAL SCIENCE FOUNDATION	A+*	A+	DEPARTMENT OF COMMERCE	D+	F
SOCIAL SECURITY ADMINISTRATION	A+*	A	DEPARTMENT OF TRANSPORTATION	D	B
HOUSING AND URBAN DEVELOPMENT	A	A+	DEPARTMENT OF LABOR	D	B-
OFFICE OF PERSONNEL MANAGEMENT	A-	A+	DEPARTMENT OF DEFENSE	D-	F
GENERAL SERVICES ADMINISTRATION	B+	A	DEPARTMENT OF THE INTERIOR	F	F
DEPARTMENT OF ENERGY	B+	C-	DEPARTMENT OF TREASURY	F	F
DEPARTMENT OF HOMELAND SECURITY	B+	D	NUCLEAR REGULATORY COMMISSION	F	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	B	DEPARTMENT OF VETERANS AFFAIRS	F	N/A
SMALL BUSINESS ADMINISTRATION	B	B+	DEPARTMENT OF AGRICULTURE	F	F

*Based on Financial Statement reporting and audit results showing "no significant deficiencies" we have confidence these grades accurately reflect agencies' ability to secure data. All other agencies showed "material weakness" or "significant deficiency," which made it more difficult to use FISMA criteria alone to evaluate an agency's information security posture.

採点項目

- Annual Testing
- Plan of action and milestones
- Certification and accreditation
- Configuration management
- Incident Reporting
- Training
- Inventory

- 97 to 100 = A+
- 94 to 96 = A
- 90 to 93 = A-
- 87 to 89 = B+
- 84 to 86 = B
- 80 to 83 = B-
- 77 to 79 = C+
- 74 to 76 = C
- 70 to 73 = C-
- 67 to 69 = D+
- 64 to 66 = D
- 60 to 63 = D-
- 59 and lower = F

(参考) 2003～06年度の連邦政府機関評価 (下院・政府監視改革委員会)

Agency	2006 Score	2006 Grade	2005 Score	2005 Grade	2004 Score	2004 Grade	2003 Score	2003 Grade
Agriculture	29.5	F	24	F	49.5	F	40	F
AID	99	A+	100	A+	99	A+	70.5	C-
Commerce	50	F	67	D+	56.5	F	72.5	C-
DOD*	39.75	F	38.75	F	65	D	65.5	D
Education	57.25	F	71	C-	76.5	C	77	C+
Energy	71.5	C-	46.75	F	48.5	F	59.5	F
EPA	92	A-	97.5	A+	84	B	74.5	C
GSA	95	A	92.5	A-	79.5	C+	65	D
HHS	86.5	B	45.5	F	49.5	F	54	F
DHS	66	D	33.5	F	20.5	F	34	F
HUD	98	A+	67.5	D+	28	F	40	F
Interior	56	F	41.5	F	67	D+	43	F
Justice	90	A-	66.5	D	82.5	B-	55.5	F
Labor	82	B-	99	A+	83	B-	86.5	B
NASA	60.75	D-	80	B-	60	D-	60.5	D-
NRC	53	F	60.5	D-	88	B+	94.5	A
NSF	99	A+	95	A	77.5	C+	90.5	A-
OPM	99	A+	98	A+	72.5	C-	61.5	D-
SBA	89	B+	77	C+	60	D-	71	C-
SSA	96.5	A	99	A+	86	B	88	B+
State	41	F	37.5	F	69.5	D+	39.5	F
Transportation	86	B	71.5	C-	91.5	A-	69	D+
Treasury*	40	F	60.5	D-	68	D+	64	D
VA*	**	**	46	F	50	F	76.5	C
Government-wide Average	**72.9**	C-	**67.3**	D+	**67.2**	D+	**65**	D

***The Inspector General for these agencies did not provide independent evaluations of their agencies' FISMA reports for FY03. Therefore, the scores are based on self-reported numbers submitted by the agencies.**

****The Department of Veterans Affairs did not provide its FY06 FISMA report.**