―米国の「国家産業保全プログラム運用マニュアル
（National Industrial Security Program Operating Manual：NISPOM）」の紹介―

研究センター　業務部　業務２課
福山　尚正

１　はじめに

国家産業保全プログラム運用マニュアル（NISPOM）は、米連邦政府省庁から産業界に開示された秘密情報を保護するための標準を規定したものであり、約 20 年前の初版からセキュリティ脅威の進展に伴い幾度となく改訂されています。また、この NISPOM は、関連する大統領令や規則に伴い制定されたものですが、31 の連邦政府省庁が国防省との同意の下に協定を締結し、産業保全サービスの提供権限を国防省に委ね、連邦政府省庁が一丸となって官民との協調連携による効果的な秘密保全への取り組み内容となっています。

平成２６年４月に､｢防衛装備移転三原則｣が国家安全保障会議及び閣議決定され、国際共同研究・開発・生産を取り巻く環境は急激に変化しつつあります。

そのような中、外国政府から渡された秘密情報をいかに適切に管理すべきか、また、わが国の重要技術をいかに守り育てるかについて、わが国の産業界がとるべき技術情報保全について検討が始まったところです。

本稿は、米国の「国家産業保全プログラム(NISP)」の運用上の枠組みを理解するものとして、「国家産業保全プログラム運用マニュアル（DoD5220.22-M　2006 年 2 月）」の 2016 年 5 月 18 日修正版の中から、全体を概観する第 1 章を焦点として概要を紹介するものです。

２　全般構成

本運用マニュアルでは、施設及び人的セキュリティクリアランス、情報の秘密区分及び標記、立入及び会議への対応等、秘密情報保護のための要求事項が示されています。

次の表で示すように、全体は 11 章からなっており、全般的な枠組みの 1 章、具体的な人的･物的管理要領としての 2 章から 7 章､IT･情報システムに関する 8 章、そして特別事項としての 9 章から 11 章に分かれています。

全　体　の　構　成		
全般的な枠組み	１章	総則と全般的要求事項
人的・物的管理要領	２章 ３章 ４章 ５章 ６章 ７章	秘密取扱許可 セキュリティ訓練とブリーフィング 秘密指定と標記 情報の保護 立入と会議 下請負契約
IT・情報システム	８章	情報システム・セキュリティ
特別事項	９章 １０章 １１章	特別要求事項 国際間のセキュリティ要求事項 その他の情報

※　各章の細部項目は「別紙：NISPOM 目次表」をご参照ください。

3　第１章　総則と全般的要求事項の概要(要約)

（1）序論

ア　目　的
本マニュアルは、秘密情報の不正開示を防止し、合衆国政府の各省庁が契約業者に開示した秘密情報を管理し、又特別なクラスの秘密情報の保護に必要な対策事項について規定している。

イ　権　限
国家産業保全プログラム（NISP）は、大統領令 13526 及び原子力エネルギー法 1954 により指定された情報を保護するため、大統領令 12829 に基づき制定された。 国家安全保障会議による NISP に関する指針の下、国防長官は大統領により NISP の米国政府の代表に指定される。 情報セキュリティ監督室（ISOO）は NISP の履行状況をモニタリングし、関係省庁に履行指令を発するとともに、NISP の運営に関する苦情や提言を処置する。 国防長官は関係機関、エネルギー省長官、原子力規制委員会議長、国家情報長官等の同意の下、本マニュアルの発行と維持管理に対する責任を有する。 国防長官、エネルギー省長官、原子力規制委員会議長、国家情報長官は、それぞれの契約者、ライセンス取得者、証明書保持者等に対し検査・監督を行う。

ウ　適用範囲
本プログラムは、全省庁、合衆国内及び合衆国領土に所在するすべての秘密取扱許可契約者、施設に適用され、入札・契約等、承認プロセスの全てのフェーズに適用される。 また、保護を求める外国政府から契約者に提供された情報についても適用される。

エ　省庁間協定
以下に示す各省庁の長は、国防長官が NISP に対する米国政府代表となることについて協定を締結する。 ①米航空宇宙局局長、②商務長官、③一般調達局長官、④国務長官、 ⑤中小企業庁長官、⑥全米科学財団理事長、⑦財務長官、⑧運輸長官、 ⑨内務長官、⑩農務長官、⑪労働長官、⑫環境保護庁長官、 ⑬司法省長官、⑭連邦準備制度理事会委員長、⑮会計検査院合衆国監査官、 ⑯米国通商代表部行政官、⑰米国際貿易委員会管理部長、 ⑱米国際開発庁管理部長、⑲ＮＲＣ運用管理部長、⑳教育長官、 ㉑保健福祉長官、㉒国土安全保障長官、㉓米国連邦通信委員会副理事長、 ㉔連邦人事管理局施設・保全・契約担当副理事長、㉕公文書管理局局長、 ㉖海外民間投資公社総裁兼最高経営責任者、㉗住宅都市開発省副長官、 ㉘ミレニアム・チャレンジ公社最高経営責任者、 ㉙大統領行政執行局副大統領補佐官、 ㉚社会保障庁安全・事故対策局連合理事、 ㉛合衆国郵便公社郵便検査局長

オ　保全管轄権
保全の管轄権は、各省庁に属するが、次の４つの省庁等が「管轄保全局（Cognizant Security Agency :CSA)」となる。 ①国防省、②エネルギー省、③原子力規制委員会、④国家情報長官 それぞれの CSA は、秘密物件の取扱いや、契約における保全上の管理を、他の CSA に委任することができる。 さらに CSA は保全管理上の責任を、複数の管轄保全事務所（Cognizant Security Office :CSO）に委任することができる。

カ　本マニュアルの適用除外及び例外事項
本マニュアルに関する適用除外、例外事項の要請は CSA が承認した政府チャンネルを介して提出できるが、CONFIDENTIAL（秘）、SECRET（極秘）、TOP SECRET（機密）情報に対して、本マニュアルで規定される保護要求事項より厳しい適用除外、例外事項の要求は認められない。

「権限」の中にあるように、この NISP の政策決定権は国家安全保障会議（National Security Council：NSC）にありますが、「情報セキュリティ監督室（ISOO）は NISP の履行状況をモニタリングし、関係省庁に履行指令を発する」とあるように、ISOO は情報セキュリティの政策履行に関して省庁横断的な拘束力をもっています。

ISOO の責務は次の通りです。[1]

① NISP の実装（機能の組込み）と監視
② 大統領令 12829 を確実に遵守させるため省庁、請負業者、ライセンス及び権限付与者の行動に対する監督
③ 法令、内部ルール、ガイドラインを実装する全機関に対するレビューの実施
④ 機密情報へのアクセスや保管を行う、各省庁、請負業者、ライセンス保有者及び被許諾者の NISP の実装に対するオンサイトレビューの実施
⑤ NISP の履行状況について毎年大統領への報告
⑥ 大統領令 12958「国家安全保障に関する機密情報」に基づいて成立した、米国政府全体を対象とする機密分類プログラムに対する監督
⑦ 国家安全保障会議を通じて大統領に機密分類の政策変更を勧告

また、大統領令 12829 により、NISP の政策に対して勧告を与えるために ISOO を議長とし政府と産業界によって構成される「国家産業保全プログラム政策諮問委員会（National Industrial Security Program Policy Advisory Committee：NISPPAC)」が設けられています。[2]

一方、NISP は 4 つの省庁等（国防省、エネルギー省、原子力規制委員会、国家情報長官）に管轄保全局（CSA）として、それぞれ平等に管轄権を与えています。

その中で、国防長官はエネルギー省長官、原子力規制委員会、国家情報長官の同意と影響を受けるすべての機関と協議の上、米国国家産業保全プログラム運用マニュアル（NISPOM）を発行し、維持するための最終的な責任を有することになっています。

---

[1]「The National Industrial Security Program」
https://www.archives.gov/files/isoo/oversight-groups/nisp/brochure.pdf　p3

[2] 同上　p5

（2）全般的要求事項

ア　概要
契約者は、アクセスまたは保管するすべての秘密情報を保護する。 連邦施設内で作業を実施する場合は、当該施設又は機関の規定に従い秘密情報を保護する。

イ　施設保全責任者
契約者は、秘密取扱施設許可(Facility Clearance：FCL)の一部として、合衆国国籍を持つ従業員を施設保全責任者（Facility Security Officer：FSO）に任命する。 施設保全責任者は、本マニュアル及び関連する連邦政府要求事項の履行の監督・指示を行う。施設保全責任者は、CSA が認めたセキュリティ訓練を修了するものとする。

ウ　インサイダー脅威プログラム
契約者は、想定されるインサイダーの脅威に対するプログラムを整備することが求められる。契約者は、このプログラムを実施するため、インサイダー脅威に対する責任者を合衆国国籍を持つ従業員（秘密取扱許可者）から任命する。この責任者は施設保全責任者が兼務することができる。 会社グループで全体を統括する責任者を指定する場合、グループ内各会社は、その統括責任者をそれぞれの会社の責任者として指名するものとする。

エ　標準実施手順
契約者は、各取扱許可施設に対し、本マニュアルの規定を履行しなければならない。そのため規定の履行に効果がある場合、又は CSA が必要とした場合「実施手順」として文書化して整備するものとする。

オ　連邦政府省庁及びそれら省庁の公式信任代表者への協力
契約者は、連邦政府省庁等の実施する検査、調査に協力するものとし、例えば、就業時間中の従業員との個人面接の手配や各種記録の提供などが含まれる。

カ　セキュリティ訓練とブリーフィング
契約者は、合衆国外に所在する者を含め、秘密取扱許可者であるすべての従業員に対して秘密の保護責任について周知するため、必要なブリーフィングや訓練を行うものとする。

キ　セキュリティレビュー
●　政府によるレビューがすべての契約者の秘密取扱許可施設に対して行われる。CSA はレビューの頻度を決めるが、１２か月に１回以上となることはない。このレビューは、通常事前に通知されるが、抜打ち的に実施されることもある。秘密の物件の保管が許可されていない設備内部の調査が必要となる場合は、契約者の代表者立会いの下行われる。 　契約者が複数の CSA の管轄下にある場合、各 CSA はレビューを最小限にするため相互に協定を締結し重複的レビューを回避する。 ●　契約者によるレビューは、継続的な自己点検により実施される。自己点検の結果は公式の報告書として作成され、次の CSA の点検まで保管するものとする。秘密取扱許可施設の管理責任者は、自己点検を実施し、経営陣の支援を受け施設が適切に維持されていることを CSA に対し毎年文書で保証するものとする。また、契約者の自己点検には契約者によって指定された派生的な秘密の抽出点検も含まれる。

ク　ホットライン
各省庁は契約者の従業員が、セキュリティに関する違反を政府に報告できるホットラインを設置し、契約者はそれを従業員に周知するものとする。

「全般的要求事項」の中では、本マニュアルの第２章以降で詳述する「人的・物的管理要領」の前提として、契約者として確立しなければならない保護のための体制の要件が述べられています。

まず、適正な秘密取扱施設の下、「組織」として、セキュリティの職責を果たす責任者である「施設保全責任者」と「インサイダー脅威プログラム責任者」を任命しなければなりません。

次に、「規則等」として、本マニュアルを履行するため、契約者ごとに保護のための具体的な実施手順の文書化を求められています。

さらに、「教育・訓練等」として、秘密を取扱う全従業員に対するセキュリティに関する教育訓練を規定し、セキュリティ体制の「評価・確認等」として、いわゆる内部監査と、政府によるレビュー（監査）の実施を求められています。

（３）　報告に関する要求事項

ア　概要
契約者は次の事象について報告しなければならない。 ①秘密取扱施設許可への影響、 ②秘密取扱者許可（従業者）への影響、 ③秘密情報の保護への影響、 ④従業員のインサイダー脅威への影響、 ⑤秘密情報の紛失または危殆化の兆候

イ　FBI に提出すべき報告
契約者は、想定されるスパイ、サボタージュ若しくは破壊活動に関して速やかにＦＢＩに文書で報告、CSA には写しを提出するものとする。

ウ　CSA に提出すべき報告
以下の事項について CSA に報告しなければならない。 ①秘密を取扱うのに不都合な従業員に関する情報、 ②秘密情報に対する不審な接触、取扱者を危険にさらそうとした者、取扱い者と他国の諜報員との接触、 ③秘密取扱許可者の身上の変更、 ④限定アクセス認証を受けている非合衆国国民である従業員の帰化による市民権の取得、 ⑤秘密関連業務を希望しない従業員、 ⑥「秘密情報の非開示合意文書」の履行拒否、 ⑦秘密取扱施設許可に影響を及ぼす変更（会社の所有権、会社の住所・秘密取扱施設の場所、主要経営陣に係る事項、廃業・破産・組織再編、外国権益に係る事項）、 ⑧秘密取扱施設の保管能力の変更、 ⑨秘密取扱施設の機能喪失等緊急事態、 ⑩セキュリティ装置の脆弱性、 ⑪秘密物件の不正な受領、 ⑫危うい状態にある従業員の情報、 ⑬管理責任終了に伴う秘密物件の処分、 ⑭外国との秘密関連契約

エ　紛失、漏えい、危殆化又は危殆化の疑いに関する報告
CSA に対し、国内外を問わず秘密情報の紛失、危殆化又は危殆化の疑いがあるものについては報告するものとする。契約者は、直ちに予備調査を開始し、秘密情報の紛失、漏えい、危殆化、危殆化の疑いがあると確認した場合、初回報告を速やかに提出する。調査を完了した後、最終報告をするものとする。

オ　個人の過失報告
契約者は、本マニュアルの要求事項に違反した従業員に対し、段階的な懲戒処置を確立し、適用するものとする。また、違反行為が個人の責任であり、かつ要求事項に対する意図的な無視、取扱いに対する重大な過失、過失又は不注意の行動パターンがある場合は、従業員に対する管理上の処置意見を CSA の報告に含めるものとする。

「報告」の中では、政府への報告要求事項に対し、契約者は秘密取扱許可従業員に対して報告責任があることを認識させることを求められています。

この際、報告内容に個人に係る情報を含む場合、その情報が情報源を明らかにしないことを条件に得たものであり、報告内容に入れることにより、その情報源が明らかになるようなときは、プライバシー法の規定により当該個人に係る情報を伏せることができるとなっています。

（４）　秘密情報の処理が許可された秘密取扱許可防衛契約者（CDC ： Cleared Defense Contractor）の情報システム（IS）上でのサイバーインシデントについての DoD への報告

ア　概要
本節は、秘密取扱防衛契約者（CDC）について適用され、CDC が保護する情報システムに係るサイバーインシデントに対する報告要求事項を規定する。 本節の報告要求事項は、本マニュアルの１－３０１（FBI に提出すべき報告）、１－３０３（紛失、漏えい、危殆化又は危殆化の疑いに関する報告）に追加されるものである。

イ　DoD に提出すべき報告
CDC は、秘密保護情報システム上のあらゆるサイバーインシデントについて直ちに報告するものとし、最小限次の事項を含めること。 ①利用された技法又は手法、②悪意のあるソフトウェアのサンプル、 ③危殆化された可能性のある DoD プログラムに関する情報、 DoD は報告された情報を保護するとともに、利用・配布する。

ウ　DoD 職員による装置と情報へのアクセス
DoD 職員は、CDC の秘密保護情報システムからどのように漏えいしたか、またどの情報が漏えいしたかを明らかにするため、CDC の装置等にアクセスしフォレンジック分析を実施する場合がある。

4　おわりに

以上、運用マニュアルの「枠組み」理解のために、第１章を焦点に概要を説明してきましたが、個人的な研究として説明事項を精選し、また平易に意訳した部分もあるので、より正確な理解あるいは全体の理解のためには、原文若しくは弊協会の研究小冊子資料「国家産業保全プログラム運用マニュアル（平成２９年３月版)」を参照していただきたいと思います。

民生技術と防衛技術のボーダレス化等により、我が国が保有する重要技術に対する関心が国内外で上昇しています。

産業競争力上重要な先端技術の流出を防ぐため、経済産業省の中に「我が国の技術情報保全の在り方に関する検討委員会」が立ち上げられ、これまでの営業秘密の保護の状況、情報セキュリティの各種基準等も踏まえ、我が国の重要技術の「守り方」についての検討がはじまっています。

防衛省の装備品の調達に係る契約企業に対しては、契約に基づき秘密保全が義務付けられていますが、あくまで防衛に係る秘密等保護法規の対象企業に限定されるものであり、広く防衛調達企業以外の重要情報を保有する企業を対象としたものではありません。

秘密情報保護への対応は、企業だけで出来るものではなく国と一体となって進めなければなりません。米国が国家産業保全プログラムにより国としての統一的な秘密情報保護を重視しているように、我が国も、国がイニシアティブをとり、秘密情報漏えいリスクに係る包括的な調査研究を官民共同で実施し、早急に、我が国に適合した秘密情報保護プログラムを策定しなければならない時期に来ていると思います。

参考資料

１　「National Industrial Security Program Operating Manual(Incorporating Change 2, May 18, 2016)」
https://fas.org/sgp/library/nispom/nispom2006.pdf

２　「国家産業保全プログラム運用マニュアル
平成２９年３月　　公益財団法人　防衛基盤整備協会」

３　「The National Industrial Security Program」
https://www.archives.gov/files/isoo/oversight-groups/nisp/brochure.pdf

４　「安全保障上機微な技術の収集動向の分析
―“2015 Targeting U.S. Technologies”から―」
慶應義塾大学　法学部　非常勤講師／CISTEC　輸出管理アドバイザー　森本　正崇

５　「平成 24 年度情報セキュリティ対策推進事業
（米国連邦政府保有情報の取扱いに関する調査）報告書」
経済産業省商務情報政策局情報政策課情報プロジェクト室

別　紙

NISPOM 目次表