

DFARS/NIST セキュリティ要件適合のための体制構築支援 (コンサルティング)

米国防省 (DoD) が国防調達規則 (DFARS) に基づき契約企業に要求する NIST 基準に対し、そのセキュリティ要件への適合が不可欠となった企業の皆様のための体制構築支援 (コンサルティング) 事業です。

背景

米国は、増加する一方のサプライチェーンからの機微情報の漏えいを極めて憂慮しており、非連邦政府組織を対象にした情報セキュリティ基準 (NIST SP800-171) を策定しました。DoD は、DFARS 252、204-7012 により管理対象防衛情報 (CDI) が含まれる契約には、NIST SP800-171 を適用することとし、下請け企業にも同様の要求を規定したため、DoD と直接契約のない日本企業も米国企業との契約に CDI が含まれる場合、適用対象となります。

NIST SP800-171 とは

米国標準技術研究所 (NIST) が定める情報セキュリティに関する技術標準の一つであり、管理対象非機密情報 (CUI) を保護するために契約相手方や非連邦政府の情報システム及びネットワークで CUI の機密性を確保するために策定されたものです。14 のファミリーに分類された 110 個のセキュリティ要件が記載されています。その内の 7 割が技術的要件であるとともに、その要件がパフォーマンスベースで記載されているため、具体的に何をすればよいのか不明な点が多く、IT 専門家や米国規則に詳しい技術者がいなければ適合が困難であると思われます。

※CDI と CUI : CDI は、DoD により指定された CUI として区分される情報で、DoD は CDI の機密性を守るために契約企業に対し NIST SP800-171 への適合を要求しています。

BSK は、「NIST SP800-171 セキュリティ要件解説書」、「適合状況確認シート」を作成し、具体的な対策を示すことにより、難解な NIST 基準への適合を支援します。

コンサルティングの流れ (4 か月～5 か月)



※NIST 基準に適合していることを証明する SSP の作成だけでなく、実業務が適切に実施できるように情報セキュリティ実施手順等の作成も含めて支援します。

担当部署

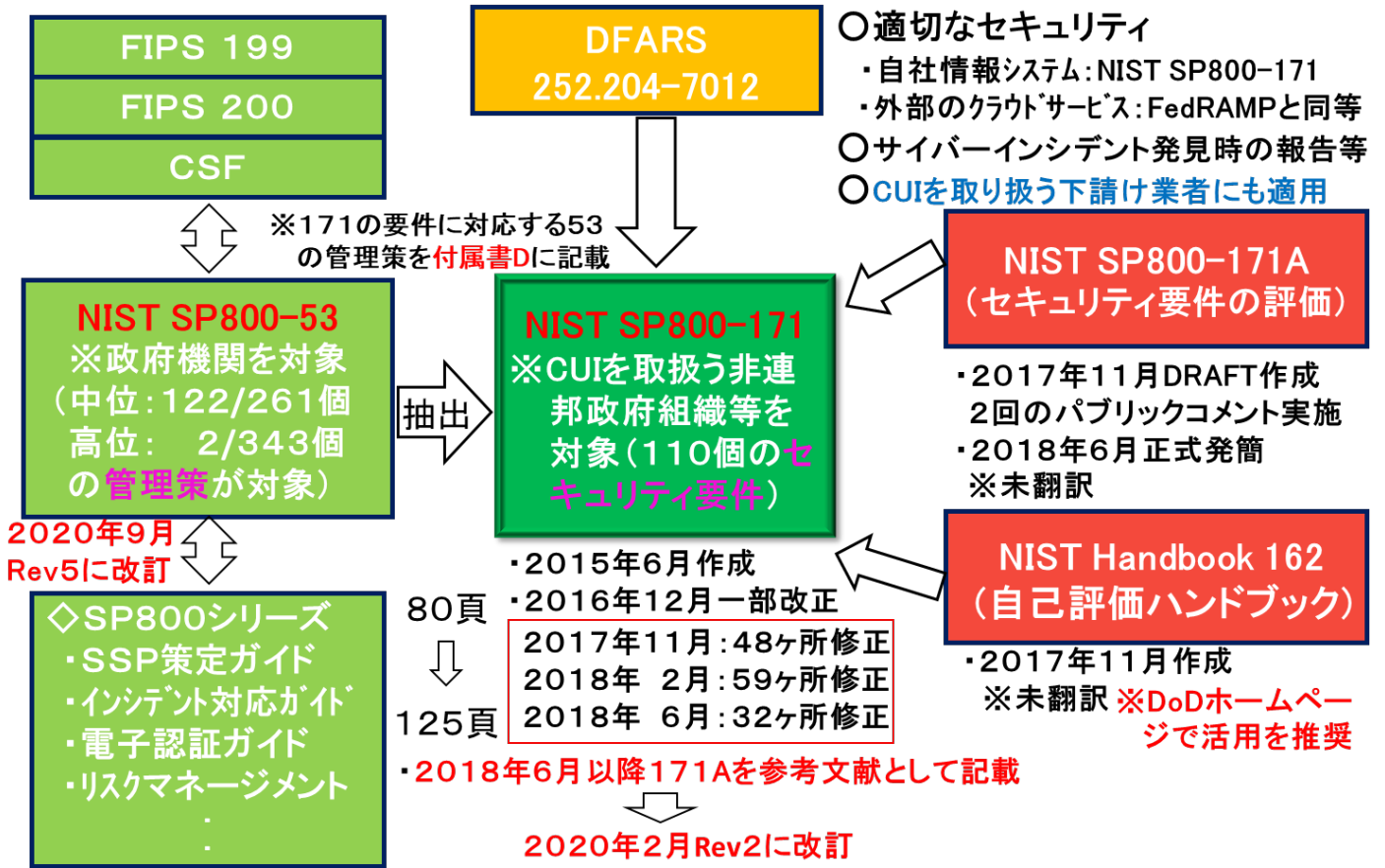
(公財) 防衛基盤整備協会
第 2 事業部 業務第 1 課

部長代理 小島 課長 上野

担当者 : 五十嵐、加納、朝田、遠藤、間野

Tel : 03-3358-8704

NIST SP800-171に関する米国基準等



DFARS/NIST要求に適合する体制の整備

【独自で米国規則を解釈し対応することが困難な企業に対する支援】

◎セキュリティ要件への適合の困難性

- ・ NIST SP800-171は関連する規則が多数存在
- ・ セキュリティ要件の記述が曖昧で適合判断が困難
- ・ システムに関する要求が多数あり専門知識が必要
- ・ 規則の頻繁な改正や修正が発生

~~外資系大手コンサルタント会社に支援を依頼~~

比較的安価なコンサルティングの実施を追及

◇複雑に関連する米国各種規則の要求を含めたNIST SP800-171セキュリティ要件に適合した「情報セキュリティ基準」及び「情報セキュリティ実施手順」を作成し、CDI(CUI)の取扱い業務が適切かつ確実に実施できるようコンサルティングを行いNIST適合化の体制整備を支援します。