民間にも必要なセキュリティクリアランス

アメリカ合衆国情報安全保障監督局

・アメリカ合衆国情報安全保障監督局は、1978 年に設立された国家安全に関わる機密情報を扱う政府機関

レベル 3 -- Top Secret　一般公開されると国家安全に絶大な損害を与えるもの
レベル 2 -- Secret　一般公開されると国家安全に深刻な損害を与えるもの
レベル 1 -- Confidential　一般公開されると国家安全に損害を与える可能性のあるもの

非公開情報を閲覧するにはクリアランス（安全証明）が必要
クリアランスは、それぞれのセキュリティーレベルに見合うだけの身上調査を受けて潔白であることが証明された者にのみに発行される

・戸籍
・経歴、家族、交友関係
・借入金、資産状況
・渡航履歴
・宗教
・政治思想
・職務経歴

アメリカを代表する先進国家には、セキュリティ クリアランス（security clearance）という国家の機密情報にアクセスを許される信用資格についての制度があります。
日本では、外交や安全保障に関する重要秘密を扱う国家公務員の適格性を調べる「秘密取扱者適格性確認制度」が部分的に該当しそうですが、アメリカのように民間企業にまで適用していないため、厳密には日本にはセキュリティ クリアランスに該当するものがありません。
2019 年 5 月米国企業による非米国企業の通信機器使用を禁止する大統領令に、トランプ大統領が署名をしたことが話題になりましたが、これは、米国政府が中国企業の通信機器にはバックドアが仕込まれている可能性を否定できず、5G の通信インフラを中国のベンダーに支配されることに警戒感を示したものでした。
事実 2018 年 10 月 4 日、米 Bloomberg が報じた、Amazon や Apple を含む米国企業約 30 社に加え、さらに CIA や国防総省など政府機関に納入された米スーパーマイクロ社のサーバから、中国人民解放軍がハードウェア・ハックとしてバックドアに利用することを狙った超小型マイクロチップが搭載されていたとする報道は世界を震撼させました。
事の真偽はさておき、アメリカでは産業スパイに対する防衛対策が厳しく、セキュリティ クリアランスがないと米国でコンピュータに限らず、プリンタやスマホなどすべての IoT 機器などを共同で制作することができません。むしろ、中国製品への規制が厳しいこのときに、かえって監視カメラなどの日本製品を売り込むビジネスチャンスなのですが、外国人も多く採用する日本企業はこのセキュリティ クリアランスの審査レベルをクリアしておくことが必要です。そうでないと、たとえば、IoT の脆弱性を見つけるためにアメリカの脆弱性情報データベースである NVD（National Vulnerability Database）を参照したくても、資格がないためにアクセスできなくなるかもしれなどのリスクがありそうです。
セキュリティ クリアランスは、特定秘密保護法よりも、もっと強い制度です。特定機密にアクセスできる人は、家族、戸籍、交際関係、借金の有無、政治思想や、海外渡航歴など徹底的な調査をした上で、情報漏洩などのリスクがないことをチェックされます。今の日本では、海外から優秀な人だと思い雇った後技術が盗まれたとしても、法的に対抗できません。
プライバシー情報まで調べられることに抵抗は感じますが、ワールドワイドにビジネスを展開している日本が、他の国と共同して事業を進めていくためには、世界標準のセキュリティ クリアランスを企業にも取り入れていくことが必要です。