# サイバーセキュリティ分野における セキュリティ・クリアランス制度の 諸外国の活用動向調査

pwc

www.pwc.com/jp

# エグゼクティブサマリー

2024年5月、日本におけるセキュリティ・クリアランス制度の運用開始に向け、「重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）」が可決・成立しました。セキュリティ・クリアランスは、経済活動の基盤となるインフラやサイバー、人工知能（AI）など、政府が保有する「重要経済安保情報」を指定。漏洩や不正取得に対して罰則を定めるのが通例となっています。情報の厳格な管理・提供ルールが定められることも予想されます。これにより、特定秘密保護法の適用範囲に含まれてなかった基幹インフラ役務を提供する特定社会基盤事業者をはじめ、政府の重要経済安保情報について委託を受ける民間組織の間で、セキュリティ・クリアランスの認定取得が広がる見通しです。

サイバーセキュリティ分野では、政府の委託事業などにおいて有効な情報共有が実施され、事業の成果を高めることや、組織のセキュリティ対策の強化につながることが期待されています。

セキュリティ・クリアランスの認定を受けて適合事業者となる組織は、重要経済安保情報に関わる事業の機会を得られるようになります。一方、セキュリティ・クリアランス保有人材の確保に加え、組織内の制度や業務プロセスを制度に適合するように更新を行う必要性が生じます。各組織に求められる運用や、その際に想定される課題は図表1のとおりです。

**図表1：運用において想定される課題**

| 求められる運用 | 想定される課題 |
|---|---|
| 人材確保 | • 従業員がセキュリティ・クリアランスを受けることに消極的で、必要な人材数が確保できない。<br>• 組織外からセキュリティ・クリアランス保有者や候補者を採用したいが、その知見がない。 |
| 認定の維持 | • セキュリティ・クリアランスを取得した従業員が不注意でクリアランスを失効してしまう。<br>• セキュリティ・クリアランスを保有した従業員の離職率が高い。 |
| 体制整備 | • 組織内の階層構造上の都合で、セキュリティ・クリアランスにより得られる情報が有効活用できない。 |
| 情報の活用と管理 | • セキュリティ・クリアランスの保有により共有される情報を社内で活用するためのプロセスが整備されていない。<br>• セキュリティ・クリアランスを考慮した情報管理の仕組みが整っておらず、情報共有の煩雑化による工数の増加や、誤った情報開示によるインシデントの発生が懸念される。 |

出所：PwC作成

民間組織でサイバーセキュリティに関わる責任者は、セキュリティ・クリアランス制度の運用開始に向けて、自組織のサイバーセキュリティに生じうる影響を把握し、組織内の準備を進めるため、最新情報の収集や、先進事例を把握することが求められています。

PwCは、国内でのセキュリティ・クリアランス制度の運用開始に向けて、既に民間のサイバーセキュリティ分野においてセキュリティ・クリアランス認定に基づいた情報共有が行われている欧米の専門家にインタビューを実施し、民間組織でのセキュリティ・クリアランス認定者に関わる組織運営の具体的な取り組みを調査しました。本調査レポートでは、諸外国の取り組み事例を踏まえ、国内組織で想定される準備策や留意点をまとめました（図表2）。

**図表2：国内での制度開始に向けて想定される準備策**

| 求められる運用 | 組織の対応 | 想定される準備策 |
|---|---|---|
| 人材確保 | 必要なセキュリティ・クリアランス認定者の把握 | • セキュリティ・クリアランス認定者が求められるプロジェクトと人材の整理<br>• 人材確保の計画立案<br>• セキュリティ・クリアランス管理担当の整備 |
| | 内部人材のセキュリティ・クリアランス認定取得支援 | • 組織内へのセキュリティ・クリアランス認定に関する説明<br>• セキュリティ・クリアランス認定取得支援の対象者への奨励施策 |
| | 外部からの採用 | • セキュリティ・クリアランス認定取得経験者の採用<br>• 必要なスキルを持つ人材を採用し、セキュリティ・クリアランス認定の取得を支援<br>• 採用段階からセキュリティ・クリアランスの管理担当者が関与できる体制の構築 |
| 認定の維持 | セキュリティ・クリアランス人材と認定の維持 | • セキュリティ・クリアランスにひも付く報酬や奨励制度の策定<br>• 認定維持管理・モニタリング<br>• 認定維持のための情報提供とトレーニングの提供 |
| 体制整備 | 体制・整備 | • 情報を厳守し活用するためのセキュリティ・クリアランス認定者の配置<br>• セキュリティ・クリアランスを要するプロジェクトに対応可能な再委託先の用意 |
| 情報の活用と管理 | 共有される情報の活用 | • セキュリティ・クリアランスの範囲で共有される情報の活用プロセス整備<br>• 組織内を説得可能な役職にセキュリティ・クリアランス認定者を配置 |
| | 情報管理 | • 情報へのアクセス制限の徹底<br>• 各人の認定レベルを可視化した対人情報共有の制限 |

出所：PwC作成

# 1 はじめに

## 背景

世界情勢の不安定化により、安全保障の概念が経済や技術の分野に拡大し、経済安全保障分野における情報漏洩リスクを低減する情報保全の重要性が世界的に高まっています。そのような中、G7の各国では、民間のサイバーセキュリティ分野においても、セキュリティ・クリアランスを活用した情報の管理や運用が行われています。

国内でも、経済安全保障分野におけるセキュリティ・クリアランス制度の運用開始に向け、具体的な運用に関する政令などの制定に向けた準備が進行中です。2024年5月に可決・成立した重要経済安保情報保護活用法では、経済活動の基盤となるインフラやサイバー、人工知能（AI）などに関する「重要経済安保情報」を保護対象として想定しています。これにより、特定秘密保護法によるセキュリティ・クリアランス制度の範囲に含まれていなかった基幹インフラ役務を提供する特定社会基盤事業者[1]をはじめ、政府の重要経済安保情報について委託を受ける民間組織の間で、セキュリティ・クリアランスの認定取得が広がる見通しです。サイバーセキュリティ分野では、政府の委託事業などにおいて有効な情報共有が実施され、事業の成果を高めることや、組織のセキュリティ対策の強化につながることが期待されています。

1 特定社会基盤事業者とは、国が経済安全保障推進法で、基幹的なインフラ事業を行う事業者として定めた以下の対象事業のうち、省令で作成された基準に該当する事業者です。

【対象事業】
電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、港湾運送、航空、空港、電気通信、放送、郵便、金融、クレジットカード

## セキュリティ・クリアランス制度の概要

セキュリティ・クリアランス制度[2]とは、政府が指定する安全保障上重要な情報にアクセスできる資格者を政府が認定する制度です。政府は、漏洩した場合に日本の安全保障に支障をきたすおそれがある情報を「重要経済安保情報」に指定し、これらの情報へのアクセスに関し国が適性評価調査を実施。信頼性を確認した政府職員や民間事業者の従業員に限定して、当該情報を知る必要性を前提とした情報提供を行います。「重要経済安保情報」の取り扱いには管理ルールが適用され、漏洩には最大で5年以下の拘禁刑などの罰則が科されます。

重要経済安保情報には、サイバー脅威・対策などに関する情報や、サプライチェーン上の脆弱性に関する情報が含まれると想定されるため、サイバーセキュリティ分野にも影響を及ぼすとみられています。

**事業者がクリアランスを得るための適性評価**

事業者が適性正評価調査を受けて適合事業者の認定を得るために、以下のような情報の提示が求められます。

- 組織の基本的事項
- 一定規模の株主や役員、事業などにおける海外との関連情報
- 重要経済安保情報の保護・管理の責任者や体制、規定や教育など
- 重要経済安保情報を取り扱う場所に関する事項

**個人がクリアランスを得るための適性評価**

適合事業者の従業員などの個人が適性評価調査を受けてセキュリティ・クリアランスの認定を得るために、以下のような情報の提示が求められます。

- 重要経済基盤毀損活動との関係に関する事項
- 犯罪および懲戒の経歴に関する事項
- 情報の取り扱いに係る非違の経歴に関する事項
- 薬物の濫用および影響に関する事項
- 精神疾患に関する事項
- 飲酒についての節度に関する事項
- 信用状態その他の経済的な状況に関する事項

## 民間組織に生じる事業の機会

セキュリティ・クリアランス制度の運用が開始されると、認定を受けて適合事業者となる民間組織には、以下に例示するような事業の機会が想定されます。

- 重要経済安保情報に関わる政府プロジェクトへの参画機会獲得

  政府の重要経済安保情報を扱うプロジェクトに参画する事業者には、政府の適性評価調査が実施され、信頼性が確認された適合事業者であることが義務付けられる可能性があります。

- 国際共同プロジェクトなどへの参画機会獲得

  海外の政府機関などが関与するプロジェクトの入札への参加に、セキュリティ・クリアランス保有が条件となっている場合があります。

- 自組織のサイバーセキュリティ対策強化につながる情報取得

  組織のサイバーセキュリティ対策の強化につながりうる国家間の緊張の高まりや、サイバー脅威に関わる情報などが、セキュリティ・クリアランス保有者の範囲でのみ共有される可能性があります。

## 従業員のセキュリティ・クリアランスの運用において想定される組織の課題

適合事業者となる組織は、重要経済安保情報を適切に保護・活用するため、セキュリティ・クリアランスを保有する人材を確保し、関連する組織内の制度や業務プロセスの更新を行う必要性が生じます。そこで求められる運用や、その際に想定される課題は図表1のとおりです。

2 制度の詳細は内閣府のWebサイトや以下のPwCのコラムをご参照ください。
- 「経済安全保障推進法」企業に求められる対応 経済安全保障分野におけるセキュリティ・クリアランス（適格性評価）制度の企業影響について
  https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/economic-security06.html
- 『セキュリティ・クリアランス制度』法制化の最新動向と日本企業が取るべき対応【第1回】諮問委員会での検討状況と企業影響見通し
  https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/economic-security/economic-security07.html

**（再掲）図表1：運用において想定される課題**

| 求められる運用 | 想定される課題 |
|---|---|
| 人材確保 | • 従業員がセキュリティ・クリアランスを受けることに消極的で、必要な人材数が確保できない。<br>• 組織外からセキュリティ・クリアランス保有者や候補者を採用したいが、その知見がない。 |
| 認定の維持 | • セキュリティ・クリアランスを取得した従業員が不注意でクリアランスを失効してしまう。<br>• セキュリティ・クリアランスを保有した従業員の離職率が高い。 |
| 体制整備 | • 組織内の階層構造上の都合で、セキュリティ・クリアランスにより得られる情報が有効活用できない。 |
| 情報の活用と管理 | • セキュリティ・クリアランスの保有により共有される情報を社内で活用するためのプロセスが整備されていない。<br>• セキュリティ・クリアランスを考慮した情報管理の仕組みが整っておらず、情報共有の煩雑化による工数の増加や、誤った情報開示によるインシデントの発生が懸念される。 |

出所：PwC作成

## 本調査レポートについて

本調査レポートでは、民間組織のサイバーセキュリティ分野において、既にセキュリティ・クリアランス認定の運用が進められている欧米の専門家を対象に、組織内での従業員に対するセキュリティ・クリアランスの運用状況に関するインタビューを実施しました。民間組織でのセキュリティ・クリアランス認定者の確保および維持、認定者と非認定者が混在するプロジェクトにおける情報管理、組織内で求められる体制など、具体的な取り組みを中心に専門家の意見を集めました。本調査レポートには、諸外国の取り組み事例を踏まえて、従業員に対するセキュリティ・クリアランスの運用整備に向けて、国内組織で想定される準備策もまとめています。

### インタビュー対象者の拠点と主な従事組織

| 拠点国 | 主な従事組織 |
|---|---|
| 英国 | 金融機関、電力事業者、テクノロジー企業、人材関連企業など |
| 米国 | 通信事業者、テクノロジー企業など |

# 2 国内の制度開始に向けて想定される準備策

## 2-1. セキュリティ・クリアランスに関わる人材確保

国内の制度運用開始に向けて、組織は制度を把握し、自組織内において認定者の配置が有益となりうる事業の洗い出しを行うことが求められます。サイバーセキュリティ分野においても、どのポジションにセキュリティ・クリアランス認定者を配置すべきか、求められる人材の役割や人数規模を整理して、人材計画に組み込んでいくことが想定されます。

### 必要なセキュリティ・クリアランス認定者の把握

**想定される準備策**

**セキュリティ・クリアランス認定者が求められるプロジェクトと人材の整理**

- 各事業において、セキュリティ・クリアランス認定者の配置パターンごとに生じうるメリットやデメリットを整理して実施計画を立案する。
- 各事業の実施計画で必要な人材の職位、スキルセット、人数規模を整理する。

**人材確保の計画立案**

- 社内でセキュリティ・クリアランスの取得を支援する候補の人材を整理する。
- 自組織が求める社外の候補者へアプローチの検討、利用可能な人材紹介サービスを把握する。

**セキュリティ・クリアランス管理担当の整備**

- セキュリティ・クリアランスの制度や審査に関する情報収集、組織内および採用候補者の認定の申請・維持・更新に関わるプロセスを管理する担当部門を整備する。

**留意点**

**事業の現場と管理側の認識合わせの実施**

- 経営層や管理職だけで人材計画を推進するのではなく、事業の現場向けにセキュリティ・クリアランス認定者が求められる場面を説明し、現場の意見を収集・分析して計画と実態に隔たりが生じないようにする。

**セキュリティ・クリアランスの審査期間やコストの増加を考慮する**

- 人材確保の計画立案の際には、特に高いレベルの認定ほどセキュリティ・クリアランスの審査期間がかかることを考慮する（米国では6カ月から8カ月、長い場合は1年を要する例もある。英国の民間機関で一定レベルの認定を得るには3年かかる場合もある）。
- 採用や外部委託をする場合、高レベルのセキュリティ・クリアランスを持つ人材ほど雇用のコストは高くなる傾向があることを考慮して予算を確保する。
- サイバーセキュリティ分野で優れたスキルを持ち、かつ高レベルのセキュリティ・クリアランスを取得している人材は希少であることから、維持に要する予算を確保する。

**セキュリティ・クリアランスの認定管理担当の事業現場からの独立**

- セキュリティ・クリアランス取得プロセスには個人の機微な情報が関わるため、従業員の認定審査の管理は、事業の現場とは独立した担当部門が担うことが推奨される。

**海外の取り組み事例**

**セキュリティ・クリアランス人材が求められる場面**

- 通信やサイバーセキュリティの技術に関連してセキュリティ・クリアランスが求められる範囲は広く、例として挙げられるものに、ネットワークエンジニア、ペネトレーションテスター、各プロジェクトマネージャー、SOC（セキュリティ・オペレーション・センター）やNOC（ネットワーク・オペレーション・センター）のオペレーター、インシデント対応者などがある。しかし、十分なスキルを持つサイバー人材自体が不足しており、そこにセキュリティ・クリアランスが加わることでさらに複雑化してしまうことが課題となっている。それでも欧米などでは必要性が急速に高まっている。
- 重要インフラ事業者でサイバーインシデントが発生した場合には、政府に報告する義務が課される。重要インフラ事業者が利用しているセキュリティサービス提供企業からも専門家が調査に派遣されることがあり、彼らは最高レベルのセキュリティ・クリアランスを保有し、インシデント対応支援や調査結果、改善策を政府へ報告する支援を行う。
- セキュリティ・クリアランス取得には時間がかかるため（最高レベルは平均9〜10カ月で、2年を要した例もある）、人材が確保できていることは競合他社に対して差別化できるとともに、入札要件に含まれる場合は参入障壁となる。
- セキュリティ・クリアランスの中でも重要度が高い「Top Secret」の認定を受けた人材がいることで、全ての情報にアクセスして早期に実施判断や作業計画が開始できることから、契約時に主導的な立場に就くことができる。
- 国防や重要インフラに関わる入札には、セキュリティ・クリアランスを取得した適切な人材を確保する必要がある。開始時に十分な人材を確保できることを示せないと大規模な入札から早期に脱落してしまうため、既に人材を確保しているか、またはすぐに確保可能であると実証することが重要である。

**人材計画**

- 連邦機関の業務を受託しているチームの例では、従業員の約70%がセキュリティ・クリアランスを取得している。各チームリーダーを中心に、外部から採用する割合を約40%、社内で認定取得を支援する人材を約60%とし、中長期の人材パイプラインを作成している。
- 需要と供給のバランスに応じて、社外からの採用と社内での取得支援を併用する。事業や時期によってそのやり方は異なる。
- （英国金融機関の例）サイバーセキュリティチームにはSecurity Check（SC）認証を取得した人材がいるものの、その数は少数である。セキュリティ・クリアランス認定者が必要な場合は、外部のコンサルティング会社などの認定者を含めたプロジェクト体制とする。プロジェクト発足を機に、金融機関への転職者を積極的に採用する傾向がある。

**雇用のコストは増え、対象人員は限定的**

- 高位のセキュリティ・クリアランスを持つ人材ほど雇用のコストは高くなる（レベルに応じて15 〜 30%増など）。
- サイバーセキュリティのスキルとTop Secretレベルのセキュリティ・クリアランスを保有する人材は非常に貴重で、一度迎え入れたら、長く活躍できる環境を整えることが重要である。

**セキュリティ・クリアランスを管理する担当部門の存在**

- 組織内に認定に関わるプロセスを扱う部署があり、施設の認定や個人の候補者の認定取得、維持、管理を担っている。

## 内部人材のセキュリティ・クリアランス認定取得支援

**想定される準備策**

**組織内へのセキュリティ・クリアランス認定に関する説明**

- 組織全体向けに、セキュリティ・クリアランス認定を内部人材が取得することによるメリットや、それに伴う制度および運用の変更点、当該者が順守すべき要件などを周知する。
- 認定取得対象者に、審査・維持のために提出が求められる情報や許可されるための条件、また法令・社内のルールで定められた罰則など、制度の詳細を説明する。

**セキュリティ・クリアランス認定取得支援の対象者への奨励施策の整備**

- 認定取得時の特別賞与や、認定者に向けた給与の手当など、認定のレベルや求められる具体的なスキルセットに応じた金銭的な奨励施策を整備する。

**留意点**

**セキュリティ・クリアランス認定者とその関係者の理解の促進**

- 認定者のみならず、同じプロジェクトや周辺で働く非認定者にも制度の理解を得ることで、エンゲージメントを高められるようにする。

**セキュリティ・クリアランスの認定審査情報の管理**

- 組織内のセキュリティ・クリアランス認定者に関する情報について管理ルールを整備し、従業員の申請プロセスに関する情報などが照会された場合にルールを順守して対応できるようにする。

### 海外の取り組み事例

**政府や重要インフラ事業者の業務を受託する事業者**

- テクノロジー企業は、必要な技術スキルを持つ技術者に対してセキュリティ・クリアランスの取得を支援している。
- セキュリティ・クリアランスを取得し、サイバーセキュリティ業務に従事できる技術者は、委託元への請求単価が引き上げられる。また、クリアランスのレベルが上がるにつれ単価も向上し、その資金を用いて、社内の技術者がセキュリティ・クリアランスを取得するための環境を整備する。
- 従業員にセキュリティ・クリアランスの申請に要する資金を提供し、取得後のボーナスなどの金銭的インセンティブ制度を導入している。より高レベルのセキュリティ・クリアランスがあるほど企業への見返りが大きくなることから、企業はより高いレベルの取得に対し特別賞与を出して支援している。
- 通常のサイバーセキュリティの請負とセキュリティ・クリアランスを保有した請負の価格を比較すると、報酬は一般的に約10～20%高くなる。高度なセキュリティ・クリアランスを持つ人材の市場価値は高く、特に米国では、Top SecretレベルのSensitive Compartmented Information（SCI）に関わる職務に従事する場合、報酬が最大30%増額されることがある。高レベルの認定に加え、保有スキルがエシカルハッキングである場合や、危険な地域での業務に従事できる場合はさらに報酬が高くなり、当該技術者の収入増加につながる。
- セキュリティ・クリアランスを取得するインセンティブとして、給与だけでなく、仕事の内容も重要である。仕事が刺激的になり、人に話せなくとも個人のキャリアの重要な仕事になる可能性がある。また、長期的な雇用につながりやすい。

**基本的なセキュリティ・クリアランスが必須の重要インフラ事業者**

- （ほとんどの正社員がセキュリティ・クリアランスを保有している組織の場合）セキュリティ・クリアランスの保持は仕事の一部であり、認定取得自体で給与が増えるわけではない。
- 一定レベルの役職への昇進には、高いレベルのセキュリティ・クリアランスの取得が要件とされている。

## 外部からの採用

### 想定される準備策

**セキュリティ・クリアランス認定取得経験者の採用**

- 政府機関やその委託先の職員などで、既にセキュリティ・クリアランスを取得済みの人材を採用する。
- 採用段階でセキュリティ・クリアランスが失効している場合でも、過去に取得実績があれば採用する。
- セキュリティ・クリアランス認定者を紹介可能な人材エージェントに、候補となるスキルを持つ人材を依頼する。

**必要なスキルを持つ人材を採用し、セキュリティ・クリアランス認定の取得を支援**

- 必要な技術的スキルを持つ人材については、セキュリティ・クリアランス認定者でない場合でも、認定取得の見込みのある人材であれば採用し、認定取得を支援する。

**採用段階からセキュリティ・クリアランスの管理担当者が関与できる体制構築**

- セキュリティ・クリアランス管理担当者は候補者の認定の要件を確認し、転職による失効を防ぐ支援をする。
- セキュリティ・クリアランスを管理する担当者が採用段階から参加し、候補者の認定の有効性や再申請の必要性を把握したうえで、採用後に期待される業務への早期着任に向けた準備を整える。

### 留意点

**転職時のセキュリティ・クリアランスの管理**

- 特定のプロジェクトへの従事を含む付帯条件の有無を踏まえ、セキュリティ・クリアランス認定の移行可否や追加手続きの要否を事前に把握する。
- 転職に伴う休職期間中の旅行先など、本人の行動などによりセキュリティ・クリアランス失効につながらないよう、候補者へ注意喚起を行う。
- 以前の勤務先との秘密保持契約（NDA）がある場合、自組織にて期待される業務における影響の有無を確認する。一例として、特定の技術に関わる業務に着任できない場合も想定されるため、事前に把握する。

**認定不適合の場合の採用停止の可能性を合意する**

- セキュリティ・クリアランスが必須のポジションで採用を行う場合は、申請プロセスに不適合が生じた場合に採用を取りやめる可能性も含めて、事前に候補者と合意しておく。

**セキュリティ・クリアランスに関わる費用の問題の把握**

- セキュリティ・クリアランスのない人材を採用して組織で取得を支援した場合、当該従業員が一定期間以内に退職する場合はセキュリティ・クリアランスの取得に要した費用を組織に返済する義務を課すという合意を従業員と締結する。
- 候補者のセキュリティ・クリアランスが前勤務先の民間企業で支援されている場合、転職の際にその費用が請求される可能性などを確認する。

**海外の取り組み事例**

**セキュリティ・クリアランス取得経験者の採用**

- 一定レベル以上の認定者を採用する場合は、既に認定を取得している人材や、過去に認定取得した実績のある人材の採用を試みる。
- 政府機関のセキュリティ・クリアランス関連プロジェクトを担当している民間企業は、政府機関との強い関係を築いている。そのため、政府機関からこれらの民間企業に転職する際、セキュリティ・クリアランスの認定を比較的容易に移行でき、採用されやすくなる（英国）。
- セキュリティ・クリアランスの認定者で高いサイバーセキュリティ技術を持つ人材は、高位のポジションの候補者として評価される。
- サイバーセキュリティでは、国防総省の出身者が専門的スキルと高レベルのセキュリティ・クリアランスを持っている可能性があるため有力な候補者となる。

**人材エージェントを利用した認定者の採用**

- セキュリティ・クリアランス認定者を紹介する人材エージェントを利用して認定者を採用する。
- 高位のセキュリティ・クリアランスの保有者と企業をマッチングするWebポータルサービスがあり、利用している。
- 政府から機密情報の取り扱い許可を受けた（英国のList X認定）民間の人材エージェントは、人材のセキュリティ・クリアランスの承認プロセスの下準備を担うことができるため、そのようなエージェントを使用して効率的に採用する。

**セキュリティ・クリアランスを取りやすそうな人の採用**

- セキュリティ・クリアランス認定者でなくとも、軍や警察の元関係者などは認定が通りやすいことから、採用する場合がある。それら人材向けに技術スキルトレーニングを提供する企業があり、利用している。
- 勤務先の施設にひも付く認定は退職後に失効するものの、長期にわたって取得していた場合は再申請が通りやすいため、候補者とする。

**高い技術力があれば採用後にセキュリティ・クリアランスの取得支援をする**

- サイバーセキュリティでは技術スキルが重要視されるため、必要なスキルがあればセキュリティ・クリアランスのない候補者を採用し、社内で取得を後援することがある。

**採用時の確認**

- Top Secretレベルのセキュリティ・クリアランスを持つ元政府職員などの採用時、場合によっては当該候補者と連邦政府機関の間でNDAが結ばれており、例えば3年間は特定のテクノロジーに関わるスキルを使用することはできないようなケースがある。採用時にNDA締結内容について確認の上、採用を決定している。
- 民間から民間へ転職する場合、前の雇用主がセキュリティ・クリアランスを支援しており、まだその期間を残しながら転職する際は、新たな雇用主が前の雇用主に移籍金のような形で支払うケースがある。

## 2-2. セキュリティ・クリアランス人材と認定の維持

セキュリティ・クリアランスに関わる実務の推進にあたり、認定者が認定を維持することは重要な要件となります。認定は個人に付与されるものの、組織側でも維持管理の万全なサポートすることが推奨されます。

### セキュリティ・クリアランス人材と認定の維持

**想定される準備策**

**セキュリティ・クリアランスにひも付く報酬や奨励制度の策定**

- セキュリティ・クリアランスを取得した従業員が認定を維持するよう、認定レベルに応じた報酬を用意する。
- 高レベルのセキュリティ・クリアランスの審査には家族も対応が求められる場合があるため、家族向けの奨励施策を実施する。

**セキュリティ・クリアランス維持管理、モニタリング**

- セキュリティ・クリアランスを担当部門のシステムで一元管理し、有効期限を追跡して失効しないように更新のプロセスを開始する。
- セキュリティ・クリアランス保有者のルール順守の状況を継続的に監査する。

**認定維持のための情報提供とトレーニングの提供**

- セキュリティ・クリアランスの保有者が認定維持のために行うべきベストプラクティスやバッドプラクティスなどについて教育する。
- 機密情報の扱い方法などは時間の経過とともに更新されるため、定期的にチェックを行い、文書化してトレーニングプログラムに組み込む。
- セキュリティ・クリアランスのさまざまなレベルや無認定者が混在するプロジェクトを想定し、相手の認定状況に応じた情報開示範囲のトレーニングを実施する。
- 高位の認定を得るには経済的に安定していると見なされる必要があるため、財務デューデリジェンスを含めた情報を常に従業員に提供し、財務上の判断が認定失効につながらないようにサポートする。

## 留意点

### セキュリティ・クリアランスが求められる業務は認定にひも付けた制度設計をする

- セキュリティ・クリアランスにひも付く奨励制度は、違反行為や認定を更新できないなどの理由からセキュリティ・クリアランスを失効した従業員は、この恩恵を受けられないようにする。
- 役職に一定レベルのセキュリティ・クリアランスが求められる場合は、認定を失効した際に役職を失う可能性があることを制度化する。

### 手続き漏れなどによる認定失効を回避する仕組みを整える

- 更新手続きの漏れなど、不注意によるセキュリティ・クリアランスの失効が発生しないよう、ツールなどを用いて当事者の手続きを可視化して管理する仕組みを確立する。

## 海外の取り組み事例

### 報酬や人事制度による雇用の維持

- 人材維持のための多数の慣習を確立しているが、大きな動機は給与と報酬である。
- 雇用コストは、保有スキルやセキュリティ・クリアランスのレベルが高いほど上昇する。Confidentialでは通常より15%以上、Secretでは20〜25%、Top Secretでは30%増加する。
- サイバーセキュリティのスキルを持ち、かつTop Secretの認定を受けた人材は非常に限られており、採用が困難である。そのため、組織として適切な人事制度を整え、長期雇用を促進している。
- 株式報酬や達成報酬、場合によっては家族向けの奨励施策を講じてセキュリティ・クリアランス認定者の継続的な雇用を支援している。

### 組織がセキュリティ・クリアランスの維持管理を行う

- セキュリティ・クリアランスの管理は担当部門でツールにより一元管理している。システムで有効期限を管理して全て自動追跡し、更新時期には再認証プロセスを開始する。申請をする社内弁護士がおり、会社がスポンサーとなり申請する。
- セキュリティ・クリアランスの管理には、人事管理関連の市販ツールを使用している。

### 継続的なモニタリング

- 企業は、セキュリティ・クリアランス保有者がセキュリティプロトコルを適用していることを確認するために、抜き取り検査や監査など適切な処置による継続的な審査を実施している。

### セキュリティ・クリアランス維持のための情報提供とトレーニング機会の提供

- セキュリティ・クリアランスを取得した従業員に対して、年に1回、場合によっては2回の受講必須のトレーニングを提供している。セキュリティ・クリアランスの保有者が認定維持のために常に行うべきことを教育する目的で、セキュリティ・クリアランスに違反する可能性のある非倫理的、違法な行為を防ぐための幅広い内容である。
- 機密情報を扱うプロトコルは時間の経過とともに更新されるため、定期的にチェックして文書化し、トレーニングプログラムを用意する。例えば、情報の処理方法、使用できる安全な通信チャネル、機密情報の取り扱い手順などについて、ベストプラクティスを認定者に提供する。
- セキュリティ・クリアランス維持に関するベストプラクティス、バッドプラクティスを共有する。例えば、認定者が飲酒して機密情報を話したことが発覚し、認定を失効した失敗事例を紹介する。
- 高位の認定を得るには経済的に安定していると見なされる必要があるため、巨額の住宅ローンや過度な高級車のローンがあると許可が下りない可能性がある。財務デューデリジェンスを含めた情報を常に従業員に提供し、財務上の判断が認定失効につながらないようにサポートする。
- セキュリティ・クリアランスの担当者が予告なしにセキュリティ・クリアランスのプロトコルに関する質問を行い、対象の従業員がプロトコルにのっとった正しい判断を行えることを確認している。
- セキュリティ・クリアランスの有無が混在するプロジェクトを想定し、相手のクリアランスレベルに応じた情報開示範囲のトレーニングをする。

### 高位認定者が気を付けていた点

- 社内の授賞式などで、受賞者と高レベルのセキュリティ・クリアランスを持つ幹部が接触する際、握手は問題ないが、ハグは不適切な行動と解釈されるリスクがあるため、幹部から断るようにしている。

### 認定が維持できなかった例

- トラブルに巻き込まれたり、セキュリティ・クリアランス維持に関する知識が不足していたりして、認定を失効する例があった。また、現場の上司や同僚の支持を得られないなどの理由で、本人が継続を望まないケースも見られた。
- 高位のセキュリティ・クリアランス認定者が一般的なトラブルに巻き込まれた場合、民間人の場合高い基準が課せられ、認定を失い、仕事を失う可能性もある。

## 2-3. セキュリティ・クリアランスを考慮した体制整備

組織の体制整備では、セキュリティ・クリアランスの認定者がその能力を最大限に発揮できるよう、考慮することが求められます。認定者の優位性が体制上の都合により損なわれることがないような整備が不可欠です。

### 体制整備

#### 想定される準備策

**情報を厳守し活用するためのセキュリティ・クリアランス認定者の配置**

- サイバー脅威に関する情報がセキュリティ・クリアランス認定者のみに共有され、自組織やクライアントの対策に繋げる場合に備え、上職位の人材がセキュリティ・クリアランスを保有して適宜対応を決定できるようにする。
- セキュリティ・クリアランス認定者の評価は、同等かより高位レベルの認定者が実施できる体制を整備する。

**セキュリティ・クリアランスを要するプロジェクトに対応可能な再委託先の準備**

- 政府のセキュリティ・クリアランスを要するプロジェクトを受託する事業者は、再委託先にも認定者が求められることを考慮する必要がある。そのため、適切な候補を事前に選定しておく。

#### 留意点

**職位とセキュリティ・クリアランスレベルの逆転がないような認定者の配置**

- 組織内のポジションとセキュリティ・クリアランスのレベルが逆転することで、上長の承認時や評価時に十分な情報が得られないことが懸念されるため、上職位の人材に高位のセキュリティ・クリアランス取得を奨励する。

**委託先のセキュリティ・クリアランス保有者の人数規模を把握しておく**

- 委託先にて配備可能なセキュリティ・クリアランスの保有者数をレベルに応じて把握し、対応可能な委託先の候補を複数社把握しておく。

#### 海外の取り組み事例

**体制**

- サイバー脅威に関する情報がセキュリティ・クリアランス保有者に共有される一方で、脅威への対処では、事前に関与者を明確にしてクリアランス保有者を配備しておくことは現実的ではないため、上職位者がセキュリティ・クリアランスを保有して適宜決定している。対処における情報共有は技術的なソリューションで管理し、適切なクリアランスを持つ人だけが適切な情報を入手できるようにする。
- 多くのチームでセキュリティ・クリアランスを持つ管理職と実践的な非管理職の人材を雇用している。
- 一定レベルの役職への昇進には高いレベルのセキュリティ・クリアランスの取得が要件とされている。
- 重要インフラ事業者で、取締役会の構成員は全員が高レベルのセキュリティ・クリアランス（英国のEnhanced Developed Vetting：eDV）が標準となっている。取締役会に助言する立場であれば、Developed Vetting（DV）は不要であるものの一定のレベル（Security Check：SC）のクリアランスが必要である。
- 組織内で、自分（SC）よりも職位が低い者が、より高レベルのDVやeDVのクリアランスを保有していたことがあり、ほとんど何も書かれていない事業プランのスライドが提示されてもそれを承認せざるを得ないことがあった。
- 政府のセキュリティ・クリアランスが求められるプロジェクトでは、自社だけではなくの他の委託先にもセキュリティ・クリアランスの認定者が必要になることがあり、その場合は政府からセキュリティ・クリアランスの認可を受けている企業に依頼している。そのような企業の常勤社員は、セキュリティ・クリアランスが失効していても、短期間で再アクティブにできる。

**プロジェクトチーム、アサイン計画**

- 委託元の政府機関ごとにチームを設置している。一定レベル以上の認定人材を見つけるのは難しいため、メンバーは一つのチームに数年間とどまる傾向がある。
- プロジェクト着任にひも付くセキュリティ・クリアランスがある場合は、プロジェクトに着任しない期間が一定期間（数週間）以上になると認定が失効するため、当該人材の配属先は厳格に管理している（英国）。
- 米国では、Sensitive Compartmented Information（SCI）許可（Top Secretよりもさらに高いレベルの保護が必要とされる情報）が必要でない限り、セキュリティ・クリアランス認定者のプロジェクトの移動などが英国やフランスと比べて柔軟に実施可能である。

**セキュリティ・クリアランス認定者の評価**

- セキュリティ・クリアランス認定者のパフォーマンス評価は、上位者のセキュリティ・クリアランス認定者が行っている。
- SCのクリアランスを持つサイバーセキュリティチームの存在は、規制当局やコンプライアンスチームにとって非常に重要であるため、チームの維持と継続のために予算を投入している。パフォーマンス評価は、単なる個人のパフォーマンスだけでなく、組織の成長という全体の観点を含めて評価している（英国）。

**セキュリティ・クリアランス認定者視点で煩雑な点**

- 全ての許可を得られる制度がなく、政府機関ごとにセキュリティ・クリアランスを取得する必要があり、効率的でない（英国）。
- 欧州の多くの国には国民のIDカードがあるが、英国には存在しないため、審査手続きや、認定を得た後の他の政府機関の認定取得への移行が煩雑である。

## 2-4. セキュリティ・クリアランスに基づく情報の活用・管理

セキュリティ・クリアランスが求められるプロジェクトへの対応や、クリアランスに基づく情報共有を自組織のセキュリティ対策強化に活用するためには、組織内の情報活用プロセスの整備が不可欠です。セキュリティ・クリアランスの認定者と非認定者が混在する可能性も考慮して、それらの情報の共有や活用のための管理手順を整備し、順守していく必要性があります。

### 共有される情報の活用

#### 想定される準備策

**セキュリティ・クリアランスの範囲で共有される情報の活用プロセス整備**

- 調査段階で確度が低い脅威情報や、他社の取り組み事例が共有される場合がある。そのような情報に関する組織内での評価や取り扱いなどについて、セキュリティ・クリアランス認定者内での役割や手順を定めておく。

**組織内を説得可能な役職にセキュリティ・クリアランス認定者を配置**

- プロジェクトに関わる情報が共有される場合には、内容を開示せずに組織内で説得しなければならない可能性があることを考慮し、高職位の人材にセキュリティ・クリアランスの認定者を配置する。

#### 留意点

**意思決定層が共有される情報へのアクセスをできるようにする**

- セキュリティ・クリアランスにより得られた情報は、開示範囲は限定されるものの、事業への影響は大きくなる可能性があるため、上位層にセキュリティ・クリアランス認定者を配置することで、組織内の意思決定を円滑に行えるようにする。

#### 海外の取り組み事例

**セキュリティ・クリアランスのコミュニティでの情報共有**

- 重要インフラのシステムに関連したサイバー攻撃が発生した場合、調査結果が出る前の段階で政府からセキュリティ・クリアランスの認定者向けに情報が共有される場合がある（調査の結果、低リスクとなることもある）。
- 政府のサイバーセキュリティ当局からセキュリティ・クリアランスの認定者に情報を提供するのみならず、コミュニティ間で民間の先進的なサイバー防御策の取り組み事例を当局や他の組織向けに紹介する活動も行っている。

**機密となりうる情報**

- サイバーセキュリティに関して、短期的に対策をとることが可能な脆弱性情報や脅威に関する情報は、広く通知されるほうが公益にかなうため、機密情報として共有されることはない。一方で、組織のセキュリティ対策の仕組み（機能や構造、体制）などは極秘となりうる情報である。

**機密情報のビジネス影響と社内展開**

- 委託元の政府機関がセキュリティ・クリアランスのある担当者に、特定の国を脅威と見なすと伝えた場合、当該政府機関や同様の公的機関に提供するシステムでは、その脅威にさらされている国に拠点を置くベンダーなどの利用を避ける必要がある。このように、ビジネス上の決定に影響する事項を、組織内のセキュリティ・クリアランスを保有しない人員とは情報共有できないまま強制する場合があるため、緊張が生じる可能性がある。

## 情報管理

### 想定される準備策

**情報へのアクセス制限の徹底**

- 委託元から受領した情報レベルを明示し、レベルに応じたアクセス制御を実施するためのプロセスやシステムを整備してルールの順守を徹底する。

**各人の認定レベルを可視化した対人情報共有の制限**

- セキュリティ・クリアランスで制限された機密情報の共有にあたり、各人の認定レベルを可視化し、適切な情報共有を行えるようなルールを整備する。

### 留意点

**情報へのアクセス制限をツールで管理**

- 情報の機密度に応じたアクセス制御は、専用のツールなどで管理することで効率化が図れると考えられる。既に導入済みの場合は、そこにセキュリティ・クリアランス制度に応じた情報分類とユーザ権限の分類を追加することで迅速かつ効率的に対応する。

**対人情報共有の制限はトレーニングを実施**

- 相手の認定に応じた会話の制限は、各人の認定レベルの可視化や情報共有のトレーニングを実施することが推奨される。

### 海外の取り組み事例

**情報管理**

- 委託元から受領した機密情報はセキュリティレベルを明確化して、ツールで管理して情報分類やラベル付けを行い、ロールベースアクセス制御やデータ漏洩防止（DLP）機能も有効にしている。
- Top Secretの情報は、十分なセキュリティ管理が適切に行われ、手順とプロセスに関するフレームワークを文書化して整備する必要がある。
- メールを含む全ての文書の上部に機密レベルを表示し、共有可能な部門やセキュリティ・クリアランスのレベルを明示している。
- 重要インフラ施設の組織内で認可レベルを7段階ほどに分類し、それに応じて会議への出席や施設への入室許可を管理していた。各段階ごとに保有するパスの色が異なり、可視化されていた。
- セキュリティ・クリアランスに関わる情報を含む問題が生じた際に、許可されていないチームメンバーと協力するのは大変な負担になる。さらに、特定の業務に認定者が少ないと、ボトルネックを招く可能性があるため、適切な人員配置が求められる。
- インシデント時に一部屋に集合して議論していても、途中で適切なセキュリティ・ クリアランスがない人には退出してもらうといった慣習がある。

**機密の業務を分割してセキュリティ・クリアランス非認定者も扱える取り組み**

- 企業がセキュリティ・クリアランスを受けている場合、組織内で機密に関する業務を分割し、作業者には全容を伝えないことで、セキュリティ・クリアランスの低いレベルの人材でも扱えるようにする例もある。

**オフショアの委託先との情報共有可否**

- インドで英国のオフショアプロジェクトが展開されることがあり、必要に応じて非英国人でもセキュリティ・クリアランスを取得し、許可されたクラウド経由で英国のプロジェクトにアクセスしている。データは英国内にあり、インドのサービスセンターから英国のセンターを経由して情報にアクセスしている。彼らは全ての情報へのアクセス許可はなく、限定的な情報アクセスとなる。
- 委託元の政府の許可があれば、オフショアへの再委託が可能となる。ただし、秘密度の高い業務は許可されず、再委託先の信頼性は、委託元の企業が事前に確認する必要がある（米国）。
- オフショアの拠点は、現地の職員が適切なレベルの認定を得た上でクライアントの承認が必要である。一定レベル以上のセキュリティ・クリアランスに関わる問題が生じた場合は、具体的な内容を共有できないまま問題に対応するため非常に困難になる。十分な規模と能力を持ち、機密性の高いタスクの許可を得た現地チームを構築するには、クライアントにもコストがかかり、価格競争力が低下してしまう。

**情報漏洩防止の取り組み**

- クリアランスレベルに応じて施設内の執務室を物理的に分けている。
- セキュリティ・クリアランスの有無をバッジで色分けして、同じ会議に参加する場合などに誤った情報共有を防ぐようにしている。
- セキュリティ・クリアランスの認定者が登録されたカードを携帯し、情報にアクセスできることを証明できるようにする（大規模な重要インフラ施設など）。
- システムのアカウントにセキュリティ・クリアランスレベルが登録されており、例えばメールの送信先ユーザのセキュリティ・クリアランスレベルでは開示できない情報を送信しようとするとメッセージが表示される。まれにクリアランスレベルの更新が追い付かず、業務の遅延につながる場合がある。煩雑であるが漏洩のリスクは低くなる。

**インシデント対応手順の整備**

- 情報管理のミスやサイバーインシデントの発生時に向けた対応手順を整備し文書化している。

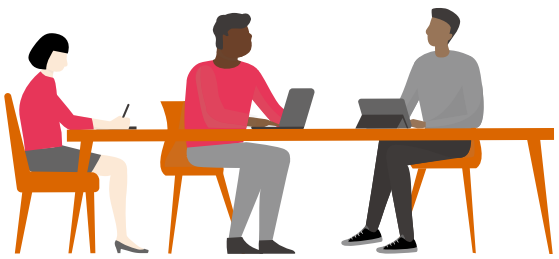
# 3 おわりに

本調査レポートでは、民間組織のサイバーセキュリティ分野においてセキュリティ・クリアランス認定の運用が進んでいる欧米の専門家を対象に、組織内での運用状況に関するインタビューを実施し、国内組織にて想定される準備策やその留意事項を整理しました。

国内のサイバーセキュリティ分野では、ここ数年にわたって人材不足が課題となる中、セキュリティ・クリアランスが求められることにより、プロジェクト体制の整備に適切な人材を確保することがさらに困難になる可能性が想定されます。組織はセキュリティ・クリアランスの制度に関する理解を深め、対象となる従業員には認定取得を奨励し、社外からの採用も含めて適材を確保していくことがますます重要になると考えられます。

各組織では、セキュリティ・クリアランス認定者が適切なポジションに配置され、委託元から提供を受けた情報の業務での取り扱いや、脅威情報を踏まえたセキュリティ防御策の強化を実行可能な体制を整備することが求められます。

制度の運用開始に向けて、各組織は政府が発信する情報を収集し、本調査レポートにまとめた先進的な取り組み事例を参考に、セキュリティ・クリアランスが求められるプロジェクトの円滑な推進や、自組織のセキュリティ防御を高めていけるよう、準備を整えることが肝要です。



## 参考資料：本調査レポートにまとめた準備策のチェックリスト

| 求められる運用 | 組織の対応 | 想定される準備策 |
|---|---|---|
| 人材確保 | 必要なセキュリティ・クリアランス認定者の把握 | □セキュリティ・クリアランス認定者が求められるプロジェクトと人材の整理<br>□人材確保の計画立案<br>□セキュリティ・クリアランス管理担当の整備 |
| | 内部人材のセキュリティ・クリアランス認定取得支援 | □組織内へのセキュリティ・クリアランス認定に関する説明<br>□セキュリティ・クリアランス認定取得支援の対象者への奨励施策の整備 |
| | 外部からの採用 | □セキュリティ・クリアランス認定取得経験者の採用<br>□必要なスキルを持つ人材を採用し、セキュリティ・クリアランス認定の取得を支援<br>□採用段階からセキュリティ・クリアランスの管理担当者が関与できる体制の構築 |
| 認定の維持 | セキュリティ・クリアランス人材と認定の維持 | □セキュリティ・クリアランスにひも付く報酬や奨励制度の策定<br>□認定維持管理・モニタリング<br>□認定維持のための情報提供とトレーニングの提供 |
| 体制整備 | 体制・整備 | □情報を厳守し活用するためのセキュリティ・クリアランス認定者の配置<br>□セキュリティ・クリアランスを要するプロジェクトに対応可能な再委託先の準備 |
| 情報の活用と管理 | 共有される情報の活用 | □セキュリティ・クリアランスの範囲で共有される情報の活用プロセス整備<br>□組織内を説得可能な役職にセキュリティ・クリアランス認定者を配置 |
| | 情報管理 | □情報へのアクセス制限の徹底<br>□各人の認定レベルを可視化した対人情報共有の制限 |

出所：PwC作成

# お問い合わせ先

**PwC Japanグループ**
https://www.pwc.com/jp/ja/contact.html

**www.pwc.com/jp**

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約12,700人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界149カ国に及ぶグローバルネットワークに370,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

発刊年月：2025年4月　　管理番号：I202502-02

© 2025 PwC. All rights reserved.
PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.