TOKIO MARINE

リスクマネジメント最前線

2025 | No.3

セキュリティ・クリアランス制度の民間適用拡大と企業に求められる対応

ビジネスリスク本部　渡邉　彩恵香　主任研究員（専門分野：リスクマネジメント）
2021 年、東京海上ディーアール（旧東京海上日動リスクコンサルティング）に入社。経済安全保障に関する調査・分析及び民間事業者の対応支援等政治リスク関連コンサルティング、リスクマネジメント体制の構築コンサルティング等に従事。

ビジネスリスク本部　長村　勇汰　主任研究員（専門分野：リスクマネジメント、地政学リスク）
官公庁での勤務後、2024 年に東京海上ディーアールに入社。官公庁・民間向けのサイバー・災害・政変リスクの評価・洗い出し、リスクマネジメント体制の構築コンサルティング等に従事。

2024 年 5 月 10 日に成立した重要経済安保情報の保護及び活用に関する法律（以下、重要経済安保情報保護活用法）の全面施行が、2025 年 5 月 16 日に迫っている。これは世界的に「セキュリティ・クリアランス」と呼ばれる情報保全の仕組みを、民間に拡大する形で法制化したものである。セキュリティ・クリアランスとは、国家が保有する安全保障上重要な情報にアクセスする者を、政府の実施する調査の結果、適当と認められた者に限定すること、及びその際に付与される資格である。

日本ではすでに、特定秘密の保護に関する法律（以下、特定秘密保護法）により、主に公務員に対するセキュリティ・クリアランス制度が運用されていたが、今次の法案成立によって、この制度の対民間適用が拡大した。

本稿では、同制度及び同法の検討過程等を整理した上で、2025 年 1 月 31 日に閣議決定された同法の運用基準を踏まえつつ、民間企業に求められる対応を考察する。

1. セキュリティ・クリアランス制度の背景と必要性

(1) 背景としての経済安全保障

□ 経済安全保障と機微情報の保全

日本におけるセキュリティ・クリアランスの民間適用拡大の背景となったのは、経済安全保障という考え方である。経済安全保障の目指す姿として、しばしば政府や与党・自民党は「戦略的自律性」「戦略的不可欠性」に言及する[1]。前者は重要な製品・技術の供給等を盤石化し他国からの影響を受けない・悪用されないようにすること、後者は技術優位性等をもって日本の存在を国際社会にとって不可欠にすること、と定義され、この両側面が経済安全保障の実現に重要である。

「戦略的自律性」や「戦略的不可欠性」の確保にあたって不可欠な要素のひとつが、機微情報の保全である。たとえば重要な物資のサプライチェーンにおける脆弱性情報が他国に漏洩した場合、他国が悪意をもってその脆弱性を攻

[1] 「経済安全保障の推進に向けて」『第 1 回経済安全保障推進会議』内閣官房（2021 年 11 月 19 日）

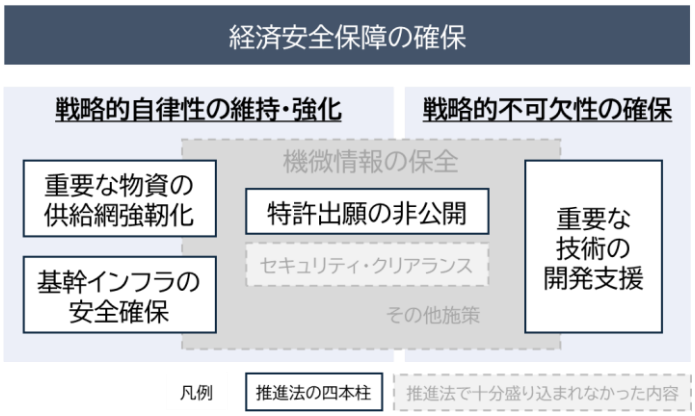
撃することで、当該物資の日本への供給が寸断し「戦略的自律性」が損なわれるリスクがある。また、日本の持つ安全保障に関する最先端技術の情報が漏洩すれば、「戦略的自律性」「戦略的不可欠性」ともに毀損しかねない。こうした背景から、機微情報の保全の実現に大きく貢献しうるセキュリティ・クリアランスの民間適用拡大の機運が高まっていた。

□ これまでの日本の取組

さて、2022 年に経済安全保障推進法（以下、推進法）が成立し、四つの施策（「四本柱」）が打ち出されたが、機微情報の保全に向けた十分な施策が打ち出されたとは言い難い（図表 1 参照）。

四本柱のうち機微情報の保全に焦点を当てたのは「特許出願の非公開」である。ただし、これは防衛・安全保障に大きな影響を及ぼし得る技術等のうち、新規の発明として特許出願のあったものを限定的に対象とする施策であり、機微情報の保全に広く網をかけるものではなかった。

■ 図表 1 「戦略的自律性」「戦略的不可欠性」と経済安全保障推進法



出典：公開情報をもとに弊社作成

□ 推進法におけるセキュリティ・クリアランスの不在

政府や国会においても機微情報の保全（及びその具体施策としてのセキュリティ・クリアランス）の重要性は主張されていたが、成立した推進法にはセキュリティ・クリアランスは盛り込まれなかった。

代わりに、推進法可決時の衆参両院内閣委員会の附帯決議ではセキュリティ・クリアランスの構築検討に必要な措置を講じることとの趣旨が盛り込まれ、その後の検討を促すこととなった。

(2) 日本におけるセキュリティ・クリアランス制度の狙い

セキュリティ・クリアランスが重点的に検討されてきた具体的な契機のひとつは、同盟国や同志国と同等のセキュリティ・クリアランス制度が日本になかったことで、国際共同研究・開発の場に日本企業が参加できない事例が生じていたことだ[2]。特定秘密保護法や日米相互防衛援助協定等に伴う秘密保護法は、たしかにセキュリティ・クリアランス制度を定めている。しかし、民間企業の持つ各種情報や研究・開発に関する技術情報等の保護をカバーできないこともあり、他国制度に比して不十分な保全措置であると見なされていたのである。

したがって、日本におけるセキュリティ・クリアランス制度の狙いはまず、情報の保全枠組みにおいて同盟国や同志国と比肩することだと言える。制度整備により、情報保全に万全を期しつつ国際的な研究・開発の場に日本企業が参画する、すなわち情報保全の攻めと守りを両立することを目指す。

[2] 「『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議』（第 1 回）議事要旨」内閣府（2023 年 2 月 22 日）

同時に、安全保障上機微な情報の盤石な保全も図っている。推進法の一部施策では、個別に技術流出防止措置を講じることとなっている[3]が、セキュリティ・クリアランス制度を通じて情報保全を強化する狙いがあるとみられる。

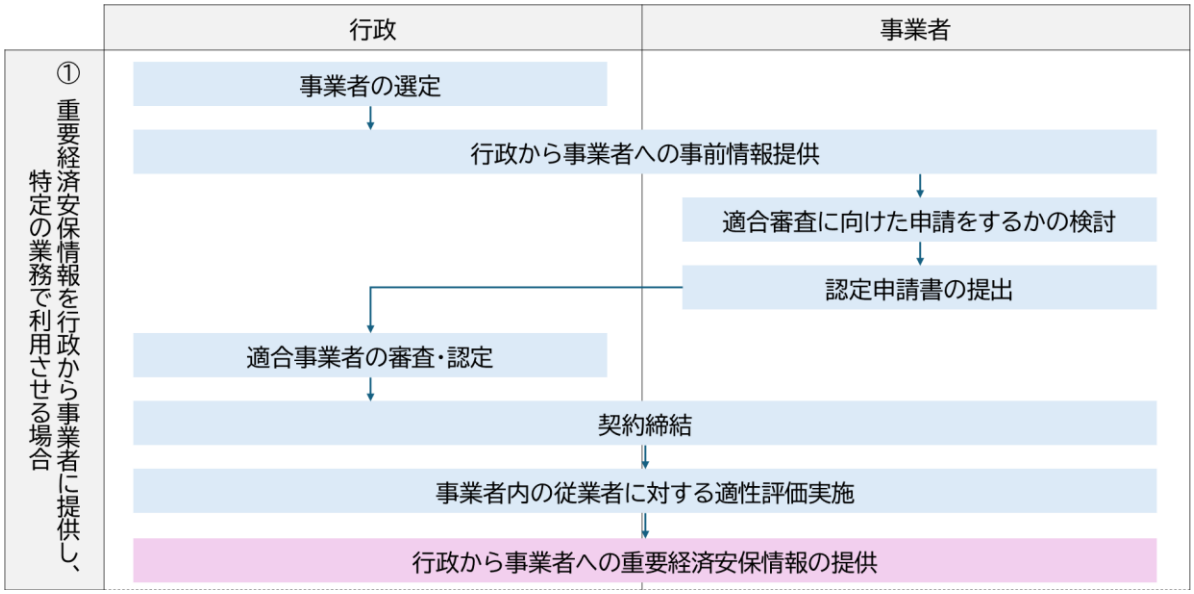
2. セキュリティ・クリアランス制度の民間適用拡大

重要経済安保情報保護活用法では、まず事業者が「適合事業者」として認められ（＝事業者としてのクリアランスを取得し）、さらにそこに所属する特定の従業者が適性評価の結果認められた（＝人に対するクリアランスを取得した）場合にのみ、当該事業者が重要経済安保情報を取り扱うことができることとなっている。同法の要点と、事業者が重要経済安保情報を取り扱うまでのフロー（図表 2）を以下に示す。

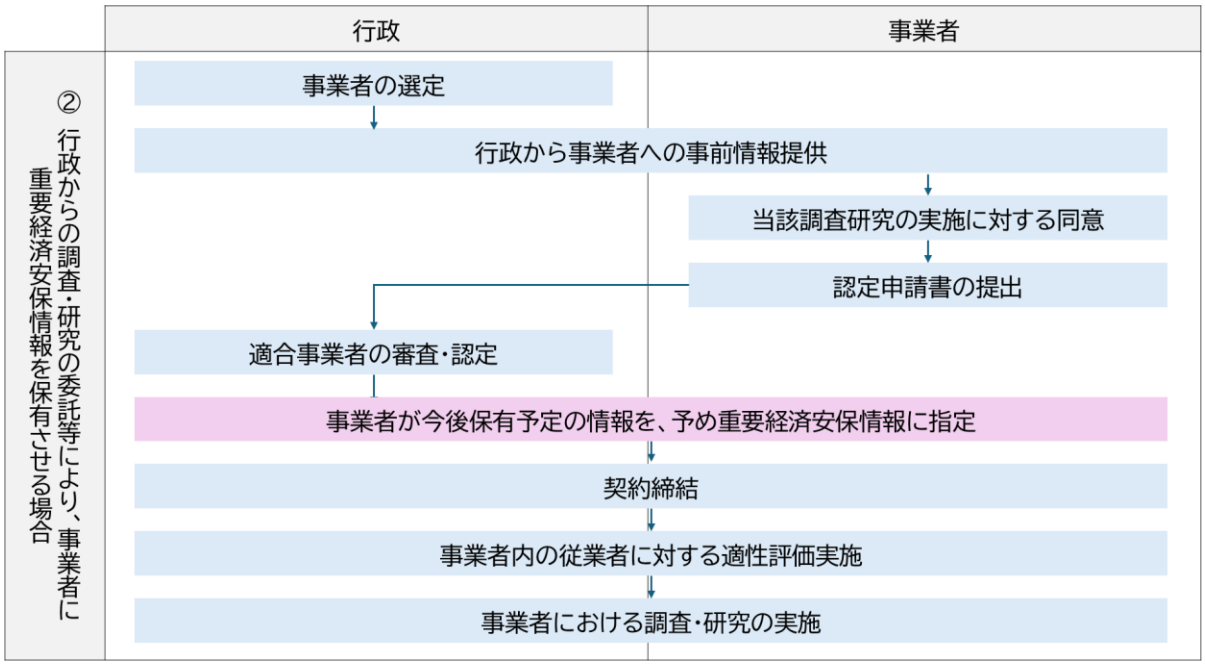
重要経済安保情報保護活用法の要点

- 企業は、「適合事業者」として認定された（＝審査の結果、事業者に対するセキュリティ・クリアランスが付与された）場合に、重要経済安保情報を取り扱うことができる。
  - 重要経済安保情報の取扱いに先立って、行政からの事前の情報（≠重要経済安保情報）共有、事業者における適合審査受検の諾否検討、その後の審査・認定、行政と事業者間の契約締結を行う。
  - その後、原則として下記いずれかのフローで重要経済安保情報を取り扱うこととなる。
    - （パターン①）行政の保有する重要経済安保情報の提供を受け、特定の業務で利用する
    - （パターン②）行政が適合事業者に行わせる調査・研究等の過程で重要経済安保情報が生じ、それを適合事業者が保有・利用する
- 適合事業者は、重要経済安保情報の取扱い従事者をクリアランス取得者に限定すること等を行政との契約で盛り込む必要がある。言い換えれば、適合事業者内の特定の従業者が、適性評価を受け、クリアランスを付与されている必要がある。

■ 図表 2 適合事業者が重要経済安保情報を取り扱うまでの主なフロー



[3] たとえば、推進法の「サプライチェーン強靭化」施策において、半導体分野で政府の助成金を受ける場合、技術流出防止措置を講じることが追加的に義務化された。



出典：運用基準第 5 章に基づき弊社作成

以上のポイントについて、同法及び施行令、さらに運用基準を参照しながら、企業への影響が想定される部分を中心に整理する。

(1) 重要経済安保情報の指定

以下 3 つの要件のすべてを満たす情報が、重要経済安保情報に指定されうる。基本的には行政機関が保有・利用する情報が念頭にあるものの、下記のとおり民間保有の情報でも指定を受ける可能性がある。

■ 図表 3 重要経済安保情報指定の 3 要件

指定の 3 要件	詳細
1.重要経済基盤保護情報該当性	「重要経済基盤」が該当性判断の 4 類型に該当すること。 **――「重要経済基盤」とは――** • 基幹インフラや重要インフラ等の「基盤公共役務の提供体制」 • 特定重要物資等の「重要物資の供給網」 **――該当性判断の 4 類型――** 第 1 号 外部からの保護措置に関する計画・研究 第 2 号 脆弱性や革新的技術等の安全保障に関するもの 第 3 号 外国政府・国際機関が得た情報で、保護措置を講じているもの 第 4 号 第 2 号・第 3 号に関する情報収集整理・能力等に関するもの
2. 非公知性	不特定多数の者が知らないこと。個別具体的に該否を判断。
3. 秘匿の必要性	安全保障への影響のおそれに鑑み、該否を判断。

出典：運用基準第 2 章第 1 節をもとに弊社作成

※その他、運用基準で判明した留意点（同第 2 節「指定に当たって遵守すべき事項」より）

- 事業者等の提供する情報が 3 要件に当てはまれば、当該情報が指定される可能性あり。

※企業（仮に A 社とする）が行政に提供した情報が、重要経済安保情報に指定されるだけでは、A 社にただちに法の規定が及ぶわけではない。

- ある情報から将来的に重要経済安保情報が出現することが確実な場合、当該情報が指定される可能性あり。

(2) 適合事業者の認定と重要経済安保情報の保有・提供

行政機関から重要経済安保情報の提供を受けることのできる事業者は、審査の結果、適当とされた「適合事業者」のみだ。行政機関は、適合事業者と締結した契約に基づき適合事業者に重要経済安保情報を提供することとなる。

事業者の適合性審査にあたっては、クリアランス保有者にのみ重要経済安保情報を取り扱わせることや、各種責任者の任命、物理的セキュリティの確保、従業員の情報セキュリティ教育等多岐にわたる項目を満たす必要がある（本稿「3．企業に求められる対応とその留意点」）。個別の項目は運用基準を参照されたいが、特に以下 4 つの観点から重要経済安保情報取扱い者として適切であると判定されることが重要である[4]。

- ✓ 当該企業の意思決定に外国の所有・支配・影響がないか
- ✓ 重要経済安保情報を取り扱う者が、その職務を全うできるか
- ✓ 情報保全の教育が、的確な知識の習得につながり、また適切な頻度で継続的に行われるか
- ✓ 物理的セキュリティが、重要経済安保情報の保護に有効か（実地での確認も実施される）

(3) 従業者に対する適性評価

重要経済安保情報の提供を受ける、または保有する事業者が適合事業者として認定されたのち、当該事業者内で重要経済安保情報を取り扱う見込みの従業者に対する適性評価を実施する。

過失だけでなく、自らの意思や他人からの働きかけによって情報を漏洩するおそれがないかを評価する[5]ため、評価対象者のプライバシーに一定程度踏み込む内容となっている。

同時に、運用基準で示されたとおり、基本的人権の尊重等、対象者の配慮を前提として評価が行われる。

■ 図表 4 適性評価の基本的な考え方と評価項目

項目	詳細
基本的な考え方[6]	適性評価に際しては、対象者の人権尊重等配慮が重ねられている。 • 基本的人権の尊重 • プライバシー保護（対象者の上司等が評価の回答内容を関知しない等） • 調査事項以外の調査禁止 • 評価結果の目的外（所属先での人事評価等）利用禁止 その他対象者の人権やプライバシー配慮の観点から、以下[7]も盛り込まれた。 • 対象者本人の同意がある場合のみ、評価を実施 • 評価の結果認定されなかった場合、その理由を通知されない権利あり

[4] 個別項目については本稿図表 5 及び運用基準第 5 章第 1 節 2(2)を、適合事業者の審査の観点は同(3)を参照。

[5] 自らの意思による漏洩、他者の働きかけによる漏洩、過失による漏洩の 3 点は、運用基準第 4 章第 2 節で漏洩のあり方の 3 類型として提示されたもの。

[6] 運用基準第 4 章第 1 節を参照。

[7] 運用基準第 4 章第 2 節 3 を参照。

項目	詳細
評価項目[8]	• 基本事項 • 家族・同居人の氏名等（父母・兄弟姉妹、配偶者、配偶者の父母・子、同居人） • 重要経済基盤毀損活動との関係 • 犯罪及び懲戒の経歴 • 情報の取扱いに係る非違の経歴 • 薬物の乱用及び影響 • 精神疾患 • 飲酒についての節度 • 信用状態その他の経済的な状況 • その他適性評価手続のために必要な情報

出典：重要経済安保情報保護活用法及び運用基準をもとに弊社作成

3. 企業に求められる対応とその留意点

適合事情者の認定は、情報保全の妥当性を確認するために 14 項目の審査項目（以下、図表 5 参照）に従って審査される。申請及び運用において企業にとっての最大の留意点は、①情報管理体制の整備と②組織内の横断的な連携強化にある。以下、適合事業者とクリアランス取得者となる従業員それぞれに求められる対応を整理した。

(1) セキュリティ・クリアランス取得の必要性の判断

セキュリティ・クリアランス制度の活用が想定される企業としては、防衛分野の他、電力、通信、金融等基幹インフラ分野、医薬品、エネルギー資源等の重要物資のサプライチェーン関連分野、量子、AI、バイオテクノロジー等先端技術開発分野に関わる企業に加えて、それらの事業に関わる技術開発企業やサイバーセキュリティ関連企業等が当てはまるだろう。そして、企業内で情報の取扱いが想定される部門としては、事業戦略・経営企画部門、海外事業部、調達・サプライチェーン開発部門、R＆D 部門、情報システム・サイバーセキュリティ部門、人事部門、法務部門、リスク管理部門等多岐にわたる。

(2) 認定事業者と関連部門に求められる対応

□ 情報管理体制の整備と組織内の横断的な連携

重要経済安保情報に指定される機密性の高い情報を扱う部門やプロジェクトがどこに存在するか、及び社内での情報の共有範囲や情報保護責任者を明確化した上で、情報の取扱いルールや手順を整備することが望ましい。前述のとおり、重要経済安保情報を取り扱う場面としては、行政の保有する重要経済安保情報を利用するパターンと行政と共同での調査・研究等の過程で保有・利用するパターンが想定されており、事業者としては、多岐にわたる部署がクリアランスに関わる可能性があることを踏まえて、全社的な枠組みでの取組を行うことが欠かせない。

[8] 法第 12 条第 2 項を参照。

■ 図表５ 適合事業者申請の際の対応事項

	適合事業者申請の際に申告が必要な事項
体制整備	• 重要経済安保情報の保護全体の責任を有する保護責任者の指名基準及び指名手続 • 重要経済安保情報の取扱い従業者の範囲の決定基準及び決定手続
ルール化	• 重要経済安保情報を取り扱うことができない者には重要経済安保情報を提供してはならないこと • 重要経済安保情報を取り扱うことができない者は、重要経済安保情報を提供することを求めてはならないこと • 重要経済安保情報を取り扱う場所への立入り及び機器の持込みの制限に係る手続及び方法 • 重要経済安保情報を取り扱うために使用する電子計算機の使用の制限に係る手続及び方法 • 重要経済安保情報文書等の作成、運搬、交付、保管、廃棄その他の取扱いの方法の制限に係る手続及び方法 • 重要経済安保情報の伝達の方法の制限に係る手続及び方法 • 重要経済安保情報の取扱いの業務の状況の検査に係る手続及び方法 • 重要経済安保情報文書等の奪取その他重要経済安保情報の漏洩のおそれがある緊急の事態に際し、その漏洩を防止するために他に適当な手段がないと認められる場合における重要経済安保情報文書等の廃棄に係る手続及び方法 • 重要経済安保情報文書等の紛失その他の事故が生じた場合における被害の発生の防止その他の措置に係る手続及び方法
施設整備	• 重要経済安保情報を取り扱う場所において、当該重要経済安保情報の保護に関する業務を管理する者の指名基準・手続、職務内容 • 重要経済安保情報の保護のために必要な施設設備の設置に係る手続
教育実施	• 従業者に対する重要経済安保情報の保護に関する教育の実施内容及び方法

出典：運用基準「第５章 適合事業者に対する重要経済安保情報の提供等 第１節 適合事業者に重要経済安保情報を提供する場合の流れ」に基づき弊社作成

セキュリティ・クリアランス取得・運用に係るプロセスでは、企業側で情報の保護・管理責任者を選定することが求められ、クリアランス取得対象者は、必要性が認められる従業員等に限られる一方で、社内の横断的な対応が必要になるため、クリアランス取得者の範囲をしっかりと見極める必要がある。そのため、クリアランスの取得・運用を統括・モニタリングする部署を設置し、当該部署がプロジェクト推進部門、リスクマネジメント部門、人事部門や法務・総務部門等と緊密に連携できる体制を確立することが望ましい。

その他としては、物理的セキュリティ体制に関して、情報を取り扱う場所の警報装置等の設置、管理方法の整備が求められる。また、教育実施についても求められるためクリアランス保持者や機微な情報を扱う役員や従業員向けの教育を通じて、情報流出の予防措置を講じることも重要である。多岐にわたる情報管理体制を一定の水準以上に保つため、外部専門家の活用も選択肢の一つだろう。

□ 社内教育プログラムの活用

適合事業者に実施が義務付けられている教育の機会を活用しながら、法制度、クリアランス取得者の権利や義務、外部からの不正行為による情報漏洩インシデント発生時の対応等の知識の習得等セキュリティ・クリアランス保持者の情報保全スキルを高めていくことが必要となる。

(3) セキュリティ・クリアランス取得者本人に求められる対応

□ 情報管理の徹底

セキュリティ・クリアランス取得者は情報管理を徹底することが義務付けられる。社外への共有の際には、先方がクリアランスを取得していることが前提となることはもちろん、社内の上司や同僚であってもクリアランスを持っていない社員に対して情報を共有することは目的外使用とみなされるため、意図しない形での漏洩にも注意が必要である。

また、クリアランス取得者であることをむやみに公言することは秘密保全の観点からも望ましくない。スピアフィッシングメールや金銭、利益供与、脅迫等によって機微な情報の不正取得を試みる攻撃者のターゲットとなり得ることにも留意する必要がある。脆弱性に関する情報提供等、社内のセキュリティ担当部門によるクリアランス取得者に対する特別の配慮も検討すべき項目に入るだろう。

[2025 年 3 月 10 日発行]

東京海上ディーアール株式会社

ビジネスリスク本部　渡邉　彩恵香　主任研究員（専門分野：リスクマネジメント）
2021 年、東京海上ディーアール（旧東京海上日動リスクコンサルティング）に入社。経済安全保障に関する調査・分析及び民間事業者の対応支援等政治リスク関連コンサルティング、リスクマネジメント体制の構築コンサルティング等に従事。

ビジネスリスク本部　長村　勇汰　主任研究員（専門分野：リスクマネジメント、地政学リスク）
官公庁での勤務後、2024 年に東京海上ディーアールに入社。官公庁・民間向けのサイバー・災害・政変リスクの評価・洗い出し、リスクマネジメント体制の構築コンサルティング等に従事。

〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6594　Fax. 03-5288-6626　https://www.tokio-dr.jp/