

防衛関連企業における防衛産業サイバーセキュリティ基準対応

EY新日本有限責任監査法人
Technology Risk事業部

■ 防衛産業サイバーセキュリティ基準の概要

防衛省では、調達に当たって防衛関連企業に対して求める情報セキュリティ対策として、2004年から「調達における情報セキュリティ基準」での整備・運用を実施していましたが、昨今のサイバー攻撃の急増、深刻化を受けて、22年3月に「防衛産業サイバーセキュリティ基準」(以下、現行基準)を整備し、23年4月以降の新規契約から適用が開始されました。

現行基準の対象となるのは、注意情報に当たる「保護すべき情報」が該当し、「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」(以下、特約条項)に定められており、「保護すべき情報」は、防衛省との契約に当たって防衛省から指定されるもので、契約相手方(防衛関連企業)は指定された情報を保全するための適切な管理として、現行基準に従って、必要な措置をとることが求められています。

■ 現行基準の特徴

現行基準は、特約条項の別紙の位置付けである「装備品等及び役務の調達における情報セキュリティ基準」とその付紙である「装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領」の構成になっています。

装備品等及び役務の調達における
情報セキュリティ基準

| 条項 | 管理策数 |
|-----------------------|------|
| 第1 趣旨 | - |
| 第2 定義 | - |
| 第3 対象 | - |
| 第4 情報セキュリティ基本方針等 | 5 |
| 第5 組織のセキュリティ | 16 |
| 第6 保護すべき情報の管理 | 29 |
| 第7 情報セキュリティ教育及び訓練 | 4 |
| 第8 物理的及び環境的セキュリティ | 29 |
| 第9 保護システムについての管理策 | 2 |
| 第10 情報セキュリティ事故等への対応 | 5 |
| 第11 情報セキュリティ事故等発生時の対応 | 9 |
| 第12 リスク査定 | 5 |
| 第13 セキュリティ監査 | 10 |
| 第14 防衛省による監査 | 2 |
| 合計 | 116 |

装備品等及び役務の調達における情報セキュリティの確保
に関するシステムセキュリティ実施要領

| 条項 | 管理策数 |
|---------------------|------|
| 第1 趣旨 | - |
| 第2 システムセキュリティ実装計画書 | 6 |
| 第3 構成管理 | 18 |
| 第4 保護システムの基本的防御 | 13 |
| 第5 アクセス制御 | 20 |
| 第6 識別及び認証 | 18 |
| 第7 通信制御 | 12 |
| 第8 システム監視 | 9 |
| 第9 システムログ | 17 |
| 第10 脆弱(ぜいじゃく)性スキャン等 | 6 |
| 第11 バックアップ | 5 |
| 第12 システムメンテナンス等 | 15 |
| 合計 | 139 |

■ ■ ■ ■
The better the question.
The better the answer.
The better the world works.



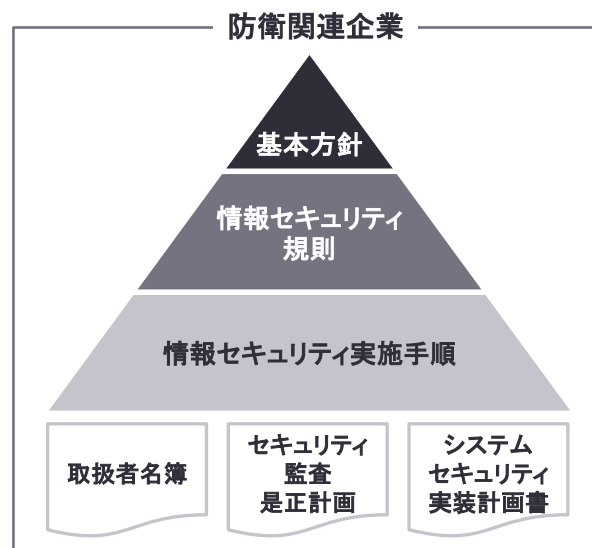
Shape the future
with confidence

■ 防衛省に提出が求められる文書類

防衛関連企業では現行基準の内容に沿った情報セキュリティ基本方針等(情報セキュリティ基本方針、情報セキュリティ規則、情報セキュリティ実施手順)を作成し、防衛省の確認を受ける必要があります。

また、防衛省との契約において、保護すべき情報の取扱者として指名した者のリストである「取扱者名簿」や現行基準に規定する措置を実施・適合していることを証明するための「システムセキュリティ実装計画書」の提出が必要となっており、自社で実施したセキュリティ監査の結果で定められた期限までに対応ができない場合には「是正計画」の提出も必要となっています。




特に、「システムセキュリティ実装計画書」は、保護すべき情報を保護システムで取り扱うまでに防衛省の確認が完了している必要があります。契約締結後の提出から確認完了まで2カ月程度要することが示されているため、防衛省との契約締結が見込まれる場合には事前に準備しておくことが必要となります。



■ EYができること

防衛省との契約に当たって「保護すべき情報」を扱う場合には、防衛産業サイバーセキュリティ基準にのっとり組織的、人的、物理的、技術的な各対策を講じる必要があります。契約前のギャップ分析から体制構築、また契約後における防衛省による情報セキュリティ監査の対応が必要となります。

EYでは、防衛関連のセキュリティ対策に精通した専門家により、それらを一気通貫でご支援することが可能です。

| アセスメント実施、ギャップ分析 | 体制構築、規程類整備支援 | 内部・外部監査支援 |
|--|---|--|
|  <p>現行基準に沿った対応ができているかのアセスメントを実施し、課題整理、改善案を提示します</p> |  <p>現行基準に沿った体制構築を行い、必要な規程類の整備、運用定着を支援します</p> |  <p>現行基準で求められている自社における内部監査支援、また防衛省による情報セキュリティ監査対応を支援します</p> |

お問い合わせ先

EY新日本有限責任監査法人 Technology Risk事業部

URL: ey.com/ja_jp/technology-risk

サービス担当者またはウェブサイトお問い合わせフォームよりお問い合わせください

EY | Building a better working world

EYは、クライアント、EYのメンバー、社会、そして地球のために新たな価値を創出するとともに、資本市場における信頼を確立していくことで、より良い社会の構築を目指しています。

データ、AI、および先進テクノロジーの活用により、EYのチームはクライアントが確信を持って未来を形づくるための支援を行い、現在、そして未来における喫緊の課題への解決策を導き出します。

EYのチームの活動領域は、アシュアランス、コンサルティング、税務、ストラテジー、トランザクションの全領域にわたります。蓄積した業界の知見やグローバルに連携したさまざまな分野にわたるネットワーク、多様なエコシステムパートナーに支えられ、150以上の国と地域でサービスを提供しています。

All in to shape the future with confidence.

EYとは、アーnst・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーnst・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYのメンバーファームは、現地の法令により禁止されている場合、法務サービスを提供することはありません。EYについて詳しくは、ey.comをご覧ください。

EY新日本有限責任監査法人について

EY新日本有限責任監査法人は、EYの日本におけるメンバーファームであり、監査および保証業務を中心に、アドバイザリーサービスなどを提供しています。詳しくは、ey.com/ja_jp/about-us/ey-shinnihon-llcをご覧ください。

© 2026 Ernst & Young ShinNihon LLC.
All Rights Reserved. ED None

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスをを行うものではありません。EY新日本有限責任監査法人および他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家に相談ください。

ey.com/ja_jp