

第三者による機器検証サービス

『第三者(外部の専門家)が事実・無実・対策の実施を検証し証明書を発行します』

1 機器検証サービスとは

○企業が様々な製品やサービスを提供するにあたり、利害関係のない中立な第三者の評価機関として、専門的かつ客観的な立場から、プロセスの内容や質、事業者の経営や企業統治の状況を確認し、その正当性・適切性について**検証結果を記載した証明書を発行**することが可能です。

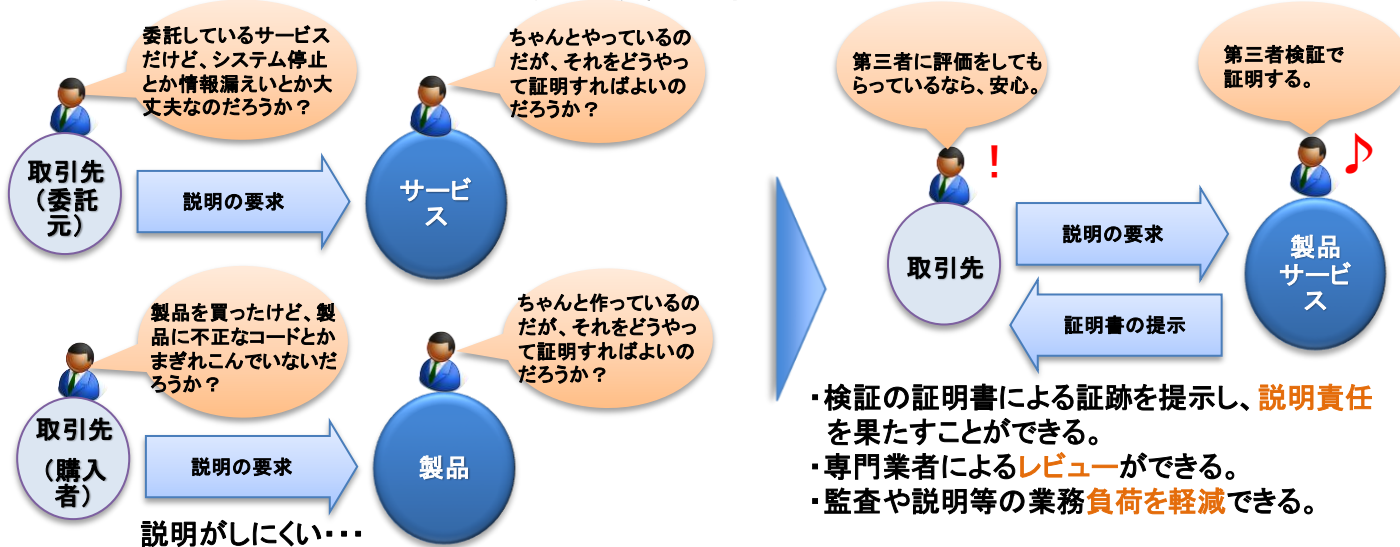
○貴社と貴社の製品やサービスの信頼性の向上を、**経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の「検証手順」**において明記されている**検証手順**等を用いて機器の検証を実施致します。

○機器検証結果に関する**取扱方法及びその明示方法**については、**下記①から③の内容を検証結果報告書として提供**致します。ご要望に応じて検証結果に関する**報告会を開催**致します。

- ① 検出された脆弱性に関する情報と、当該脆弱性が悪用された場合に想定される影響、攻撃の再現手順を記載
- ② 検証結果報告書において、検証結果に対する分析や考察等の追加情報を記載
- ③ 検証結果に基づき、検証対象機器に求められるセキュリティ管理策の提案

2 なぜ第三者による検証が必要とされるのか

企業は製品やサービスを提供していくなかで、提供先からその品質や安全性等について説明を求められることがあります。しかし、自己の正当性・適切性を説明することは難しいものです。第三者から検証書の発行を受けておけば、説明責任を果たすことができます。



3 第三者検証の活用

第三者検証は、**取引先**に対し正当性・適切性の検証を行うことだけでなく、製品、サービスおよび会社の品質への取り組みを**消費者**にアピールすることや内部に対して対策の実施状況をアピールすることに活用することができます。また、**個人情報保護委員会への報告事項「再発防止のための措置」**に、**専門家による有効な対策としても活用**できます。

外部に対する活用

- 第三者検証により、同種製品・サービスに差別化を図ることができる。
- 第三者検証の証明書を公表して、ステークホルダーに安全性や品質に対する積極的な取り組みをアピールすると、販路拡大等の機会が増える。
 - ・ 取引先にアピールできる(BtoB)
 - ・ 個人利用者にアピールできる(BtoC)

内部に対する活用

- 第三者検証により、経営者や現場責任者が自社製品・サービスに係る品質や安全対策を客観的な視点で再点検する。
- 第三者検証書を公表するに至らない場合でも、改善点の提示により、製品・サービスの品質向上に向けた課題を浮き彫りにし、改善へと繋がる。

4 なぜ日本セキュリティ格付機構なのか

日本セキュリティ格付機構は、第三者検証を行う機関として、次のようなメリットを保持しています。

- 公正、中立の格付機関: 格付機関として設立されているため、格付審査に影響力を行使できないように社団法人として運営するなど、公正性、中立性が高い機関。
- 格付機関としてのノウハウ: 格付機関として、様々な格付を実施してきた中で、製品やサービスの提供プロセスの正当性・適切性を判断するノウハウが確立。
- お客様の目的にあわせて検証項目をカスタマイズ: お客様の業種、取引先等の事情により、第三者検証したい内容が異なることに対応し、事前に打ち合わせにより、検証項目をカスタマイズ。

(利用例1) 第三者により製品の品質と安全性が検証されたことをアピールしたい

- A社の製品は、自社センターと通信する機能を備えているが、その機能が顧客の個人情報等の機密情報を漏えいしているのでは、という疑念を顧客に持たれてしまうことにA社は悩んでいた。そこで、その機能が漏えいするような動作を行っていないという**第三者検証**を得ることで、**製品の信頼性を高め、充実したセキュリティ対策をお客様に説明してビジネス拡大に役立てたい。**
- B社は、**自治体から業務を受託するに際し、データセンターの「Tier(ティア: 日本データセンター協会(JDCC)のファシリティスタンダード基準)」を求められ、第三者検証を用いて説明し、納得を得ることにした。**

(利用例2) 第三者による客観的な視点で業務内容の適切性を確認したい

- C社は、重要情報を含む**業務を外部委託しているが、適切な安全管理措置を講じているか現地で確認して欲しい。**また、**ASPサービスについても、サービス終了時のデータ消去等を現地確認して欲しい。**
- D社は、**マンパワーの受託業務(BPO)を行っているが、第三者の視点で業務監査を行い、結果を委託元への報告資料として活用したい。**また、E社は、**企業グループ内でマイナンバー業務を一手に引受けているが、監査結果をグループ会社で共有したい。**
- E社は、**NIST/SP800-171への準拠度を示す第三者検証書**を取得することで、高水準のセキュリティ対策を確実に実施していることを検証したい。

○機器検証の検証手順

次の検証手順を用いて検証します。

- ①**準備**: 契約締結に向けて、必要な情報の整理や検証目的を明記します。
- ②**計画**: 契約締結後、検証体制及び検証環境を構築します。また、検証の実施に向けた検証項目や検証手法の策定を行います。
- ③**検証実施**: 検証依頼者の要望を踏まえ、検証を実施します。
- ④**分析**: 検証結果に基づき、特定・検出された脆弱性や詳細検証によって明らかになった脅威に対して、想定される影響や対応策の案を分析します。
- ⑤**報告**: 検証結果の報告書を作成します。

○免責条項及び留意事項

- ①機器検証サービスにおいて、下記は免責事項となります。
 - ・検証時点における既知の脆弱性に関する検証であり、検証時点以降に発見される脆弱性には対応していません。
 - ・検証環境と異なる環境における脆弱性は検知できません。
 - ・検証後、事業者が明示する期間を経た検証対象システムにおいて生じた事故等については、検証との関係の有無に関わらず免責とします。
- ②機器検証サービスの検証の際に、既知の脆弱性のリスト又は判定の基準、検証環境を記述した資料について、第三者に説明できる記録についで、必要に応じて弊機構は検査実施完了より1年間保管します。
- ③機器検証サービスに用いるツールや手法については、検査対象に関する質問、観察、関連文書や設定値の閲覧、再実施を基本とします。なお、追加的な要件があれば、必要に応じてどのようなツールや手法を使用して検証を行うかをご契約の前にご提示します。