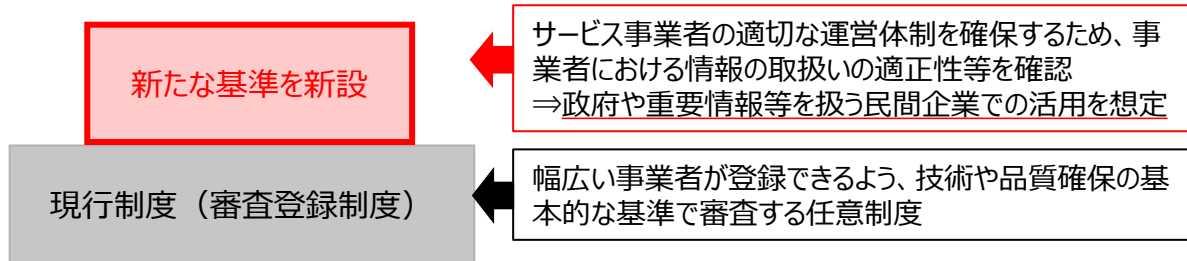


# サイバーセキュリティ・サービス事業者の信頼性強化に向けた制度（中間とりまとめ）

- 今後サイバーセキュリティ・サービスに対するニーズが増加することが見込まれる中、サイバーセキュリティ・サービス提供事業者起因する機微情報流出等のリスクに対応するため、サービス提供事業者の「適切な運営体制」が一層重要となる。特に、政府機関・重プラ、安全保障に係る事業者等においては、十分な「適切な運営体制」を有するサイバーセキュリティ・サービス事業者を選定・活用するニーズが想定される。
- こうしたことを踏まえ、既に技術・品質の基準に基づき登録を行っている現行の「情報セキュリティサービス審査登録制度」に登録しているサイバーセキュリティ・サービス提供事業者を対象に、「事業者の適切な運営体制」を確認する認定制度の創設を検討。2026年度に詳細設計を進め、2027年度中の運用開始を目指す。

## <サイバーセキュリティ・サービス認定制度の概要>

リストに掲載された企業から申請を受け、適切な運営体制を確認、認定。



## <現行制度のサイバーセキュリティ・サービスの種類>

- (1) 情報セキュリティ監査サービス
- (2) 脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス
- (3) デジタルフォレンジックサービス
- (4) セキュリティ監視・運用サービス
- (5) 機器検証サービス

- ✓ 会社の資本関係、従業員管理方法、情報管理体制、使用ツール・データ保管先、サイバーセキュリティ対策等について審査。重大な変更があった際には、再確認を行う。
- ✓ 委託の一定の制限、顧客への情報開示、従業員の適切な管理、インシデント報告も求める
- ✓ 虚偽等の疑いが生じた場合はサーベランスの実施等のうえ、認定取消（取消の事実公表）も可能とする
- ✓ サイバーセキュリティ・サービス事業者が犯罪者グループに身代金を支払いを行わないなどの倫理的な対応も求めることとする