

執筆：SecurityScorecard 中村 悠

編集：SecurityScorecard 中島 朝可・橋本 詩保

SOC 2レポートとは？それを開示する意義は？

セキュリティに携わっている方で、“SOC 2 レポート”という単語を聞いたことがない方はいらっしゃると思いますが、このブログでは、改めて、“SOC 2 レポート”について説明し、その開示の必要性について言及します。

▼SOCレポートとは

SOC(Service Organization Controls)レポートとは、「対象組織が標準化された基準に照らし合わせ、内部統制が遵守されているかについて、第三者が評価したレポート」です。

SOCレポートですが、誕生した当初から、セキュリティに関連する項目への言及があったわけではありません。

SOC レポートとは、外部監査人が、対象組織の財務諸表に影響を与える情報に関する内部会計統制を文書化して提供する文書で、米国公認会計士協会（以下、AICPAと略す）によって定められた要件に従って記載されます。

当初は、財務的な項目で構成されており、組織がSarbanes-Oxley Act法（いわゆる、SOX法）に準拠できているか否かを検証するために使用されていました。その後、SEC（米証券取引委員会）が「Commission Statement and Guidance on Public Company Cybersecurity Disclosures」を発表し、サイバーセキュリティに関する項目が含まれるようになりました。

AICPAが定めた要件によって記載されているため、財務的な観点での記載が中心にあることは納得できます。

SOCレポートには、次の3つの種類があります。

SOC 1 レポート:

財務報告に関連する内部統制の状況进行评估したレポート

SOC 2 レポート:

情報セキュリティ、可用性、プロセスの完全性、機密性、プライバシーの管理状況に関するレポート

SOC 3 レポート:

続きをご覧になりたい場合は

メーカーBlog^

[HTTPS://SECURITYSCORECARD.COM/SOC2-REPORT-JP](https://securityscorecard.com/soc2-report-jp)

