

執筆：SecurityScorecard 中村 悠

編集：SecurityScorecard 中島 朝可・橋本 詩保

どのように取引先/関連組織のセキュリティ リスクを把握するべきか

弊社のブログでも、過去に、『サプライチェーン リスク マネジメント』というキーワードを出したことがあります。最近では、経済産業省(※1)(※2)やIPA（独立行政法人 情報処理推進機構）(※3)(※4)の発表資料で使われることが多くなってきました。

この『サプライチェーン リスク マネジメント』ですが、これから導入しようとしている組織、既に導入が進んでいる組織も多くあると耳にします。

一方で、なかなか導入が進まない企業も多くあると伺います。導入が進まない理由の1つとして挙げられるのは、「取引先/関連組織のセキュリティ態勢を把握する方法が分からない。」ということです。

確かに、自組織のセキュリティ態勢であれば、内情も把握できているし、セキュリティ態勢を診断するツールを実行するにしても、組織内の許可を得ることができれば、比較的手に入りやすい情報です。ただ、これが、自社以外の組織となると、とたんにハードルが高くなります。

では、「取引先/関連組織のセキュリティ態勢を確認する方法」として、どのような方法があるのでしょうか。現状、考えられるのは、以下の2つの方法です。

- 取引先/関連企業自身から報告してもらう方法
- 外部から診断ツールで判定する方法

これらの2つですが、もちろん、それぞれに特長が存在します。

続きをご覧になりたい場合は

メーカーBlog^

[HTTPS://SECURITYSCORECARD.COM/SUPPLY-CHAIN-RISK-MANAGEMENT-METHODS-JP](https://securityscorecard.com/supply-chain-risk-management-methods-jp)

