**実践的なリスク管理、事前／事後対策まで“総合力”を評価可能**

**NIST基準のサイバーセキュリティ対策評価、Secureworksが提供開始**

2017年12月07日 07時00分更新

文● 大塚昭彦／TECH.ASCII.jp

　Secureworks Japanは12月6日、新しい「サイバーセキュリティ・リスクアセスメント・サービス」の本格提供開始を発表した。米国NIST（国立標準技術研究所）のサイバーセキュリティフレームワーク（CSF）、および米国CIS（インターネットセキュリティセンター）のクリティカルセキュリティコントロール（CSC）を基準とする、2種類の評価サービスがラインアップされている。

|  |  |  |
| --- | --- | --- |
| [http://ascii.jp/elem/000/001/599/1599081/171206_SecureWorks_03a_240x.jpg](http://ascii.jp/elem/000/001/599/1599081/img.html) |  | [http://ascii.jp/elem/000/001/599/1599082/171206_SecureWorks_03b_240x.jpg](http://ascii.jp/elem/000/001/599/1599082/img.html) |
| Secureworks Japan ジェネラル・マネージャーのジェフ・モルツ氏 |  | 同社 セキュリティ＆リスクコンサルティング シニアマネージャの三科涼氏 |

　NIST CSFは、サイバー攻撃への「事前対応」と「事後対応」にかかる5つの機能（特定／防御／検知／対応／回復）について、「企業組織／人」「運用プロセス」「技術」という3つの観点から、包括的な耐性評価を可能にするフレームワーク。評価においては98項目を参照し、個々のセキュリティ対策にかかる事業リスクを合理的に説明できる。セキュリティ向上のためのベストプラクティス、中長期的なセキュリティ体制構築／強化のためのベースラインとしても活用できる。

|  |
| --- |
| [http://ascii.jp/elem/000/001/599/1599083/171206_SecureWorks_13_500x281.jpg](http://ascii.jp/elem/000/001/599/1599083/img.html) |
| NISTサイバーセキュリティフレームワーク（CSF）の概要。組織の包括的なセキュリティ耐性評価が可能 |

　具体的なサービス内容としては、企業が策定しているポリシーやプロセスのドキュメントを収集するとともに、オンサイトでセキュリティ部門やIT部門、総務／人事／法務などサイバー攻撃対応に関連する部門代表者のインタビューを実施し、双方を合わせて分析／評価を行うというもの。これにより、セキュリティ対策整備の現状と「あるべき姿」の乖離点の把握、未整備の対策により生じる影響やリスクの可視化、対策優先度や対策にかかる期間、費用などを把握することができる。

　もうひとつのCIS CSCは、評価項目を上位20項目に絞ったうえで「最も危険な脅威からのリスクを最大限に減らす」ことに注力しているのが特徴。具体的／技術的な対策で構成されており、実践的なうえに更新頻度も高く、より新しいセキュリティリスク対策状況を短期間で評価できるとしている。

|  |
| --- |
| [http://ascii.jp/elem/000/001/599/1599084/171206_SecureWorks_14_500x281.jpg](http://ascii.jp/elem/000/001/599/1599084/img.html) |
| NIST CSFとCIS CSCの違い。なおCSFアセスメントにはCSC評価項目もすべて含まれる |

　Secureworksではすでに、ISO 27000シリーズ／ISMS基準に対応した「情報セキュリティアセスメント」のサービスも提供している。同社 セキュリティ＆リスクコンサルティング シニアマネージャの三科涼氏は、新しいサービスの違いは「電子化された情報に焦点を当て、サイバー攻撃への対応に特化していること」「事前／事後の対策を網羅していること」「より技術的な観点も含まれること」などだと説明した。

|  |
| --- |
| [http://ascii.jp/elem/000/001/599/1599085/171206_SecureWorks_15_500x281.jpg](http://ascii.jp/elem/000/001/599/1599085/img.html) |
| 従来のISO 27000／ISMS対応アセスメントと、新しいNIST CSF/CIS CSCアセスメントのカバー領域の違い |

　オプションを除く参考価格は、NIST CSFを基準とした場合は480万円、CIS CSCを基準とした場合は250万円。アセスメントにかかる期間はNIST CSF基準で約12週、CIS CSCで約10週、さらに改善策のロードマップ策定（CSFオプション）で約6～8週としている。

　同社 ジェネラル・マネージャーのジェフ・モルツ氏は、NIST CSF基準を採用するメリットとして、「コンプライアンス対応」だけでなく「実践的セキュリティ」も同時に実現できることを強調した。「セキュリティ侵害を受けた企業を見ると、コンプライアンス対応に終始してしまい、被害が出てしまったというケースが非常に多い」（モルツ氏）。

**ドキュメント／体系の静的評価から攻撃演習による動的評価までカバー**

　発表会では、今回本格提供を開始するリスクアセスメントと、これまでSecureworksが提供してきた「インシデント管理リテーナー」や「Red Team Testing（レッドチーム演習）」といったサービスとの関係についても説明がなされた。

|  |
| --- |
| [http://ascii.jp/elem/000/001/599/1599086/171206_SecureWorks_22_500x281.jpg](http://ascii.jp/elem/000/001/599/1599086/img.html) |
| Secureworksが提供するリスクアセスメント・サービスの例。今回のような静的なものから、動的（実践的）なものまで |

　インシデント管理リテーナーは、現実に起こりうるインシデントシナリオを素材として机上訓練（ディスカッションなど）や実技訓練を実施するもの。その実施を通じて、参加者自らが現状のセキュリティ対策成熟度を把握するとともに、改善に向けた課題を発見することに活用する。

　また[Red Team Testing](http://ascii.jp/elem/000/001/077/1077315/)（レッドチーム演習）は、Secureworksが電子的な攻撃だけでなく物理的なオフィスへ侵入なども含むあらゆる手段を使って攻撃を行い、「超実践的」なかたちでインシデント対応力を評価する。

　同社 セキュリティ＆リスクコンサルティング Incident Response ＆ Technical Testing マネージャの加藤義登氏は、「組織というものは体系立てて対応をしていかなければならない。何もしていない顧客が、こうした実践的な訓練だけをやっても対応力はつかない。そのため、最初はリスクアセスメントを行い、（ポリシーやプロセスの）ドキュメントレベルで評価したうえで、訓練などより実践的なことをやっていかなければならない」と説明した。

　「Secureworksのひとつの強みとしては、ベースとして（今回のリスクアセスメントサービスのような）ドキュメントレベルの評価もあれば、（インシデント管理リテーナーやRed Team Testingのような）犯罪者集団にも対抗できるような実践的な評価もできる点。対策段階に応じて、組織の評価を支援させていただく」（加藤氏）

**■関連サイト**

* [Secureworks Japan](https://www.secureworks.jp/)