プレスリリース
2016 年 5 月 10 日
独立行政法人情報処理推進機構

情報セキュリティに対する経営者の関与、組織的な取り組みについて日・米・欧で比較調査
～日・米・欧で CSIRT (*1) 設置率に差異はないが、日本では CSIRT に対する満足度が欧米の 3 分の 1 ～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、「企業の CISO や CSIRT に関する実態調査 2016」を 2016 年 5 月 10 日（火）に公開しました。
URL：https://www.ipa.go.jp/security/fy27/reports/ciso-csirt/

昨年 12 月に経済産業省と IPA が共同で策定した、“サイバーセキュリティ経営ガイドライン”が公開されました。このガイドラインでは組織の情報セキュリティ対策の推進には経営層の主体的な関与が必要と指摘しています。

IPA では企業経営者の情報セキュリティに対する関与、組織的な対策状況について把握するため、文献・アンケート・ヒアリングの 3 段階で調査を実施しました (*2)。アンケートでは日･米･欧の従業員 300 人以上の企業を対象に実施し(*3)その結果を比較しました(*4)。主なトピックは以下のとおりです。

（1） CISO (*5) が経営層として任命されていると、情報セキュリティ対策の実施率は高くなる。また、この傾向に日・米・欧の差異はない。

表 1．CISOの任命と情報セキュリティ対策推進状況の関係

	地域	経営層としてCISO任命 ※1	CISO任命なし ※2
経営層が参加する情報セキュリティに関する意思決定の場がある	日	89.3%	37.3%
	米	77.4%	39.4%
	欧	78.0%	36.1%
リスク分析を実施している	日	84.9%	43.3%
	米	83.5%	46.8%
	欧	78.0%	42.6%
サイバー攻撃が発生した場合を想定した被害額を推定している	日	71.6%	34.7%
	米	69.4%	27.7%
	欧	81.2%	27.9%

約2倍

※1：日（n=225）、米（n=248）、欧（n=223） ※2：日（n=150）、米（n=94）、欧（n=61）

（2） CSIRT は設置したが、人材の能力・スキル不足を実感しており、現状に満足していない日本

① CSIRT が“期待したレベルを満たしている”と回答した割合は米国 **45.3%**、欧州 **48.8%**に対し日本は **14%**となり、欧米の 3 分の 1 と大きく差が開く結果となった（別紙 2.）。

(*1) Computer Security Incident Response Team の略。サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかわるインシデントに対処するための組織。

(*2) 本調査設計のため、まず文献を調査し日本シーサート協議会会員向けに書面アンケート調査を実施した。その結果を元に日・米・欧の企業向けにウェブアンケートを実施し、更に、CSIRT、CISO を設置している企業を対象にヒアリング調査を実施した。

(*3) 得られた回答数は日本 588 件、米国 598 件、欧州 540 件（英 195 件、独 205 件、仏 140 件）

(*4) 本調査は IPA が実施してきた「情報セキュリティ事象被害状況調査」の後継調査の位置づけ。従前の調査は、1989 年から 2015 年まで 25 回実施され、2015 年 1 月 15 日に公表した 2014 年度版が最後。

(*5) Chief Information Security Officer の略。最高情報セキュリティ責任者。本調査では組織全体の情報セキュリティ対策を統括する CISO または同等の責任者を指す。

② CSIRT 等の有効性を左右する最大の要素として“能力・スキルのある人員の確保”と回答した割合は日本が **73.3%**と最多で、米国 **56.8%**や欧州 **54.2%**と比べ 2 割程度多い（別紙 3.）。

③ 情報セキュリティ人材のスキル面等の質的充足度が十分であると回答した日本の企業は **25.2%**と、米国 **54.3%**や欧州 **61.9%**の半分以下（別紙 4.）。

※ なお、CSIRT および同等組織の設置状況に日・米・欧の差は余り見られない（別紙 5.）。

考察：日本は CSIRT 等への満足度や情報セキュリティ担当者の質的充足度が欧米に比べ低い。日本の CSIRT 等の期待レベルの向上には能力・スキルのある人員の確保が特に重視されており、要求が厳しいことが伺える。

（3） **日米欧とも 50%以上の企業でサイバー攻撃の発生経験はなく、多くの CSIRT で実力は未知数。また、訓練・演習実施の機能が無いと回答した CSIRT は 6 割以上**

① 直近の会計年度にサイバー攻撃が発生していないと回答した日米欧の企業は 50%以上（別紙 6.）

② 設置されている CSIRT 等インシデント対応組織で訓練・演習を実施していると回答したのは日本 **33.4%**、米国 **39.3%**、欧州 **34.7%**と日米欧とも **6 割以上**が実施していない（別紙 7.）

考察：新たなサイバー攻撃に直面することに備え、CSIRT では訓練・演習を実施し、インシデント対応において CSIRT が機能するか確認し、課題を把握しておくことが望まれる。

（4） **日本と欧米とで異なる“情報セキュリティポリシー”“セキュリティリスク”の公表意向**

① 日本に比べ欧米は公表の意向が **10 ポイント以上**少ない（別紙 8.）

② 開示しない理由として、欧米は“自社のセキュリティやリスクの情報を開示したくない”と回答する割合が約半数（米国 **46.2%**、欧州 **50.0%**）であるのに対し、日本は **18.8%**であった。（別紙 9.）

考察：欧米では、セキュリティのポリシーやリスクの情報開示が、例えば、攻撃者に有利な情報になりうることを懸念し、判断していると考えられる。

■アンケート調査（日･米･欧比較）の概要

（1） 調査方法：ウェブアンケート

（2） 調査対象：従業員数 300 人以上の企業の CISO、情報システム/セキュリティ担当部門の責任者及び担当者

（3） 調査期間：2015 年 11 月中旬から 12 月下旬

その他、主な調査項目等に関する詳細は報告書の P27 をご参照ください。

■本件に関するお問い合わせ先
IPA　技術本部　セキュリティセンター　島田／加藤
Tel: 03-5978-7530　Fax: 03-5978-7518　E-mail: isec-info@ipa.go.jp
■報道関係からのお問い合わせ先
IPA　戦略企画部　広報グループ　山北／白石
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp