プレスリリース
2017 年 4 月 13 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関する日・米・欧の比較調査
～CISO (*1) を置く日本企業の割合は 62.6%、米国の設置率 95.2%、欧州 84.6%と大きく乖離～

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 2017」を 2017 年 4 月 13 日（木）に公開しました。
URL: https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

2015 年 12 月、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 (*2)。またこれを受け、IPA では CISO 等を想定読者に「サイバーセキュリティ経営ガイドライン解説書」を昨年 12 月 8 日に公開しています。

同ガイドラインにはサイバーセキュリティ経営の 3 原則 (*3) があり、うち 1 つに経営者がサイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要とあります。また、CISO には専門知識に加え、経営者との橋渡し役になること、事業への理解が重要であるとされています (*4)。

昨年から実施している「企業の CISO や CSIRT に関する実態調査 2017」では、経営者の情報セキュリティに対する関与と、企業の組織的な対策状況についての現状を把握するため、文献調査・アンケート調査を行っています。アンケート調査では日・米・欧の従業員 300 人以上の企業を対象に実施し (*5) その結果を比較しました。主なトピックは以下のとおりです。

（1） 現在、CISO に期待されている役割、スキルは、セキュリティ偏重。セキュリティ部門と経営層をつなぐ橋渡しとしての役割は、まだ企業では認知されていない。

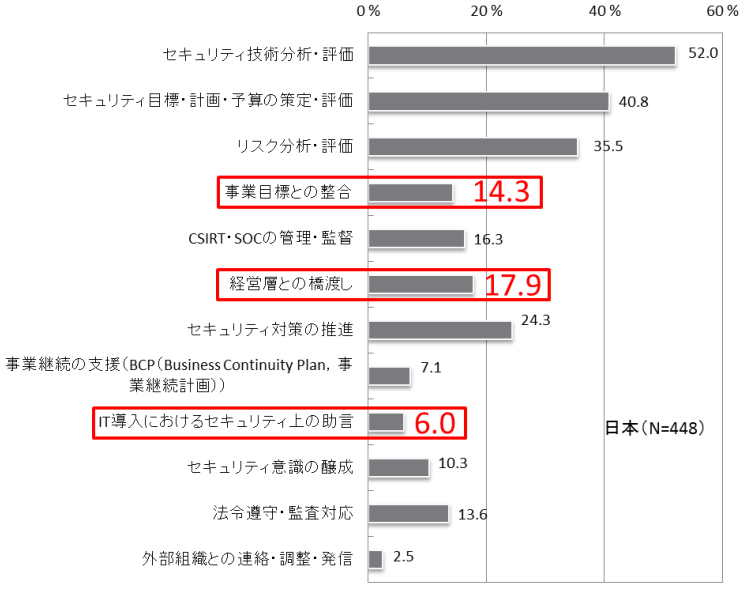

図1：現在重要視されているCISOの役割

(*1) 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) 同ガイドラインはその後、2016 年 12 月に改訂され、最新版は ver1.1 となっている。
(*3) 3 原則：①経営者のリーダーシップが重要　②自社以外（ビジネスパートナー等）にも配慮　③平時からのコミュニケーション・情報共有
(*4) サイバーセキュリティ戦略本部「サイバーセキュリティ人材育成プログラム」（案）
http://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf 、p19
(*5) 得られた回答数は日本 755 件、米国 527 件、欧州 526 件（英 192 件、独 182 件、仏 152 件）

① 経営層とセキュリティ部門をつなぐ橋渡しの役割を重視するのは、17.9%
② 自社の事業目標とセキュリティ対策とを整合させる役割は、14.3%
③ 事業への IT 導入におけるセキュリティ上の助言の役割は、6.0%

また、「CISO に求められるスキル・経験」を聞いたところ自社事業への理解が必要と回答した割合は 14.2%であった。(別紙 1 .)

（2） **日本では CISO が任命されている組織の割合は 6 割程度で、欧米と 20 ポイント以上の差がある。また、日本では多くの CISO が他の役職と兼任であり、専任 CISO の多い欧米とは異なる。**

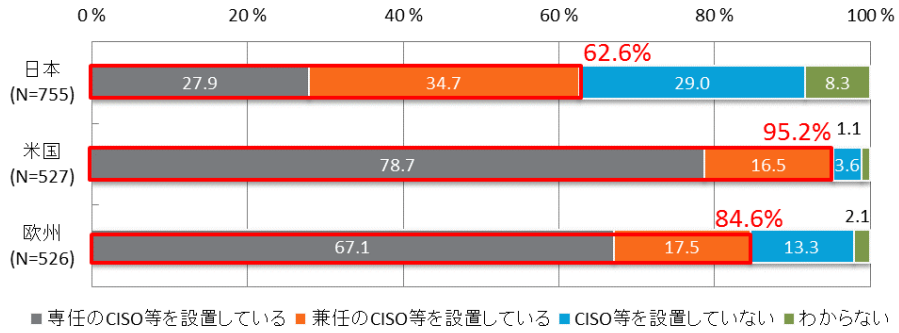

図2：CISO任命率（今回調査）

前回調査での CISO 任命率は、日本 64.3%(n=588)、米国 78.8%(n=598)、欧州 85.0%(n=540)。日本ではあまり変化なし。

（3） **日本では CISO の半数以上(58.7%)が、セキュリティ要員（人数）は十分だと回答。一方現場では不足感が過半数。**（別紙 2.）

① 国内のセキュリティ部門の責任者・担当者の 55%は、要員の人数が不足していると認識。
② 専任 CISO が多い欧米では、量的充足度に CISO と現場の認識にズレはない。

考察：日本の CISO はセキュリティ業務に十分時間を割き、セキュリティ部門の活動内容や業務量の把握に努める必要がある。しかし日本の CISO は兼務が多く、現実的には難しいことがうかがえる。

（4） **CSIRT (*6) を設置したものの、期待したレベルを満たしていると解釈していない日本**

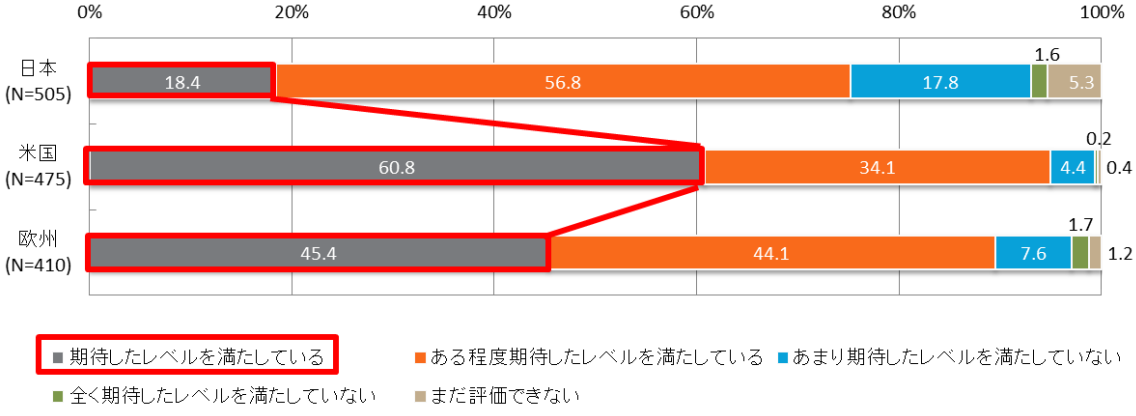

図3：CSIRTの有効性に対する満足度

(*6) 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。

① セキュリティ人材の確保の難しさやスキル不足が満足度の低い原因と考えられる（別紙 3.（A）、（B））。
② 日本の CSIRT 設置率は 66.8%であり、前回調査時の結果 68.2%と比べ大きな変化はない。（別紙 4.）

（5） **経営層の情報セキュリティへの関与は、重要インフラ企業でも 6 割～7 割程度に留まる日本**

① 経営層が、情報セキュリティについて審議し、意思決定する会議の設置率は 65.0%（別紙 5.）。
② 国内拠点の情報セキュリティ対策状況を把握・指示している割合は 67.4%（別紙 6.）

考察：非重要インフラ企業と比べて関与の割合は 15 ポイント程度高い。しかし、特に社会インフラを担う企業においては、経営層のいっそうの関与が期待される。

■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：2016 年 10 月上旬から 11 月上旬

その他、主な調査項目等に関する詳細は報告書の P20 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／小川
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　白石／山北
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp