

内部からの脅威に対して楽観的な日本企業

～企業における情報セキュリティへの取り組みを日本とグローバルで考察～
「2014年 グローバル情報セキュリティサーベイ」の結果を発表

- ✓ 日本企業はインサイダーや外部委託管理、知的財産保護などの内部犯行に対する危機感が低い
- ✓ 内部犯行に関する危機感を持っている日本企業でも、情報セキュリティ予算は現状維持傾向
- ✓ 日本では情報セキュリティ戦略をビジネス戦略に盛り込んでいる企業、また中長期の情報セキュリティ戦略を立てている企業が少ない

EYのメンバーファームである新日本有限責任監査法人は、EYが実施している「EY2014 グローバル情報セキュリティサーベイ」の調査結果(日本語訳版)、およびグローバルをベンチマークとして日本との差異を考察した「EY 2014 グローバル情報セキュリティサーベイ-日本企業の現状と課題」を公表します。

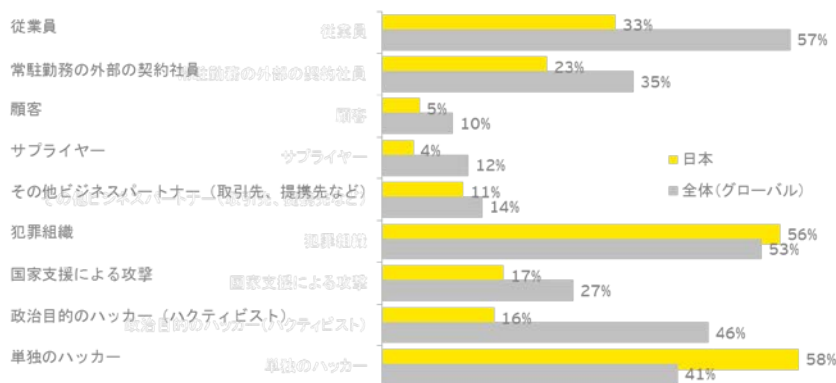
2つの調査の結果、日本企業は依然として内部からの脅威に楽観的で投資の優先度が低く、また情報セキュリティ戦略のアプローチにも課題があることなどが分かりました。

以下は、今回の調査結果から得た日本における傾向の一部です。

内部からの脅威に対して楽観的な日本企業

グローバルでは従業員や常駐する契約社員など組織内部の脅威(サイバー攻撃)を大きく意識していることに対し、日本では依然として犯罪組織やハッカーなど外部からの攻撃を脅威と感じているという結果になりました。また同様に、内部脅威に関連する情報セキュリティ投資の優先度も日本では低い結果となり、危機感だけでなく、具体的施策の実施についても積極的ではないことが見て取れます。

サイバー攻撃を行う物(もしくは人)として最も可能性が高いと考えているもの



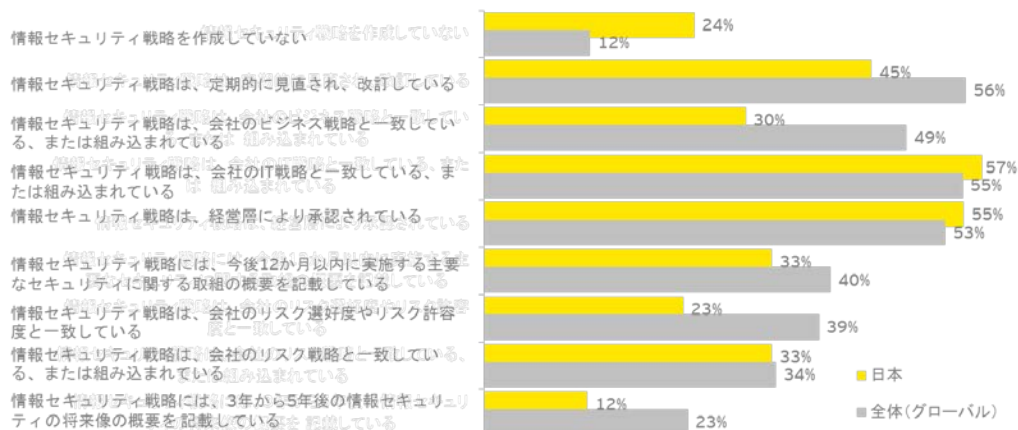
一方で、リスクの原因となりうる脅威や脆弱性についての質問に関して、日本における傾向は投資優先度とは異なり、不適切なデータの保管、従業員の不注意や無自覚といった内容が上位となりました。

2014年に日本で起こった情報流出にかかるインシデントを踏まえると、組織内部から行われる不正アクセスに対する関心が高まっており、脅威認識は今後変化していく可能性があります。

情報セキュリティ対策への戦略的アプローチが課題

今回の調査で、グローバルでは 49%、日本では 30%の企業が情報セキュリティ戦略とビジネス戦略が整合していると回答しました。また、情報セキュリティ戦略の中に 3 年から 5 年の戦略を盛り込んでいるかについては、日本では 12%の企業にとどまりました。さらに日本では、情報セキュリティ管理を行う上で、セキュリティ基準やフレームワークを利用していないと回答した割合が 48%にのぼり、軸足のない中で情報セキュリティ戦略の中長期計画の作成することは困難である現状がうかがえます。

情報セキュリティ戦略について該当するもの



「グローバル情報セキュリティサーベイ」について

グローバル情報セキュリティサーベイは、EY が毎年実施している情報セキュリティに関する調査で、今回で 17 年目となります。この調査は、情報セキュリティの重要な課題を以下の 5 つのカテゴリーに分けて質問し、さまざまな局面における判断に有益な情報を提供することを目的としています。

1. 情報セキュリティ予算と投資
2. セキュリティガバナンス
3. 情報セキュリティの有効性
4. 情報セキュリティ環境
5. 先端技術とトレンド

詳細は、下記資料をご覧ください。

サイバー犯罪に先手を打つ EY による 2014 年グローバル情報セキュリティサーベイ

サイバー犯罪に先手を打つ EY 2014 グローバル情報セキュリティサーベイ — 日本企業の現状と課題

《本件に関するお問い合わせ先》

新日本有限責任監査法人 広報室
 東京都千代田区内幸町2-2-3 日比谷国際ビル
 Tel: 03 3503 1037 / Fax: 03 3503 1041