【抜粋版】情報セキュリティ対策レポート（第１回）

情報セキュリティの運用・管理体制及び過去に受けたことのある被害状況

平成 29 年 1 月

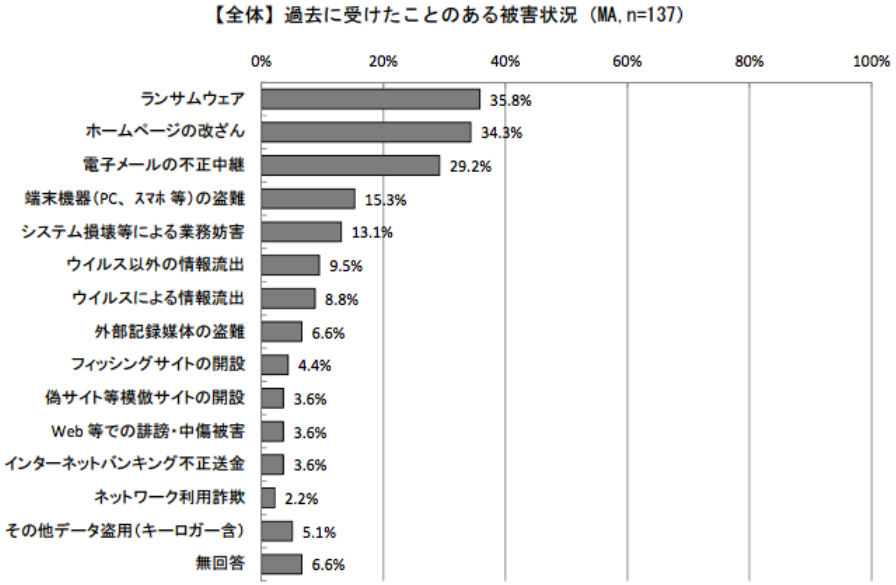
ナレッジコーディネーター

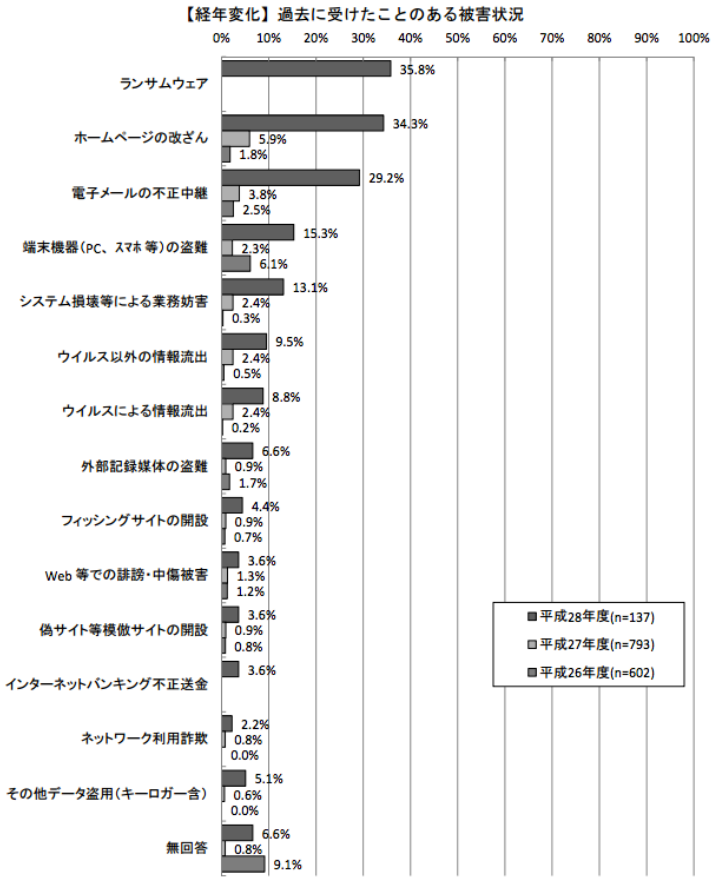
1. 情報セキュリティの運用・管理体制及び過去に受けたことのある被害状況

２０１６年に国家公安委員会が行った「不正アクセス行為対策等の実態調査」より、情報セキュリティの運用・管理体制及び過去に受けた被害状況をまとめる。

① 過去に受けたことがある被害

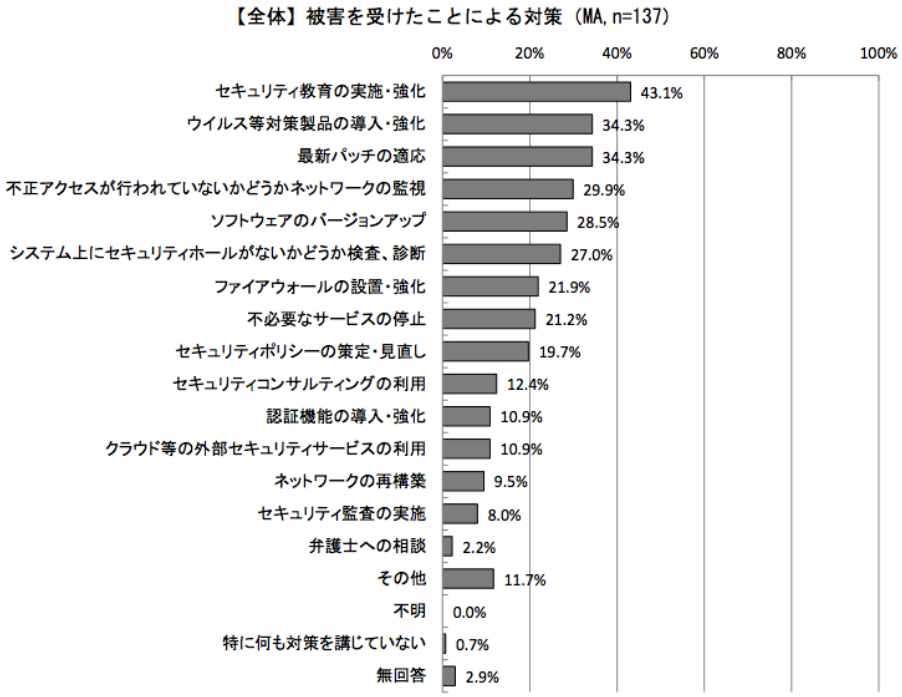
ランサムウェア（35.8%）、ホームページの改ざん（34.3%）、電子メールの不正中継（29.2%）が過去に受けた被害として３割の企業が経験したことが分かる。また、経年変化の被害状況から H28 年度より被害を受けたと回答する企業が多いことが分かる。サイバー攻撃の対象が拡大していることが推察される。





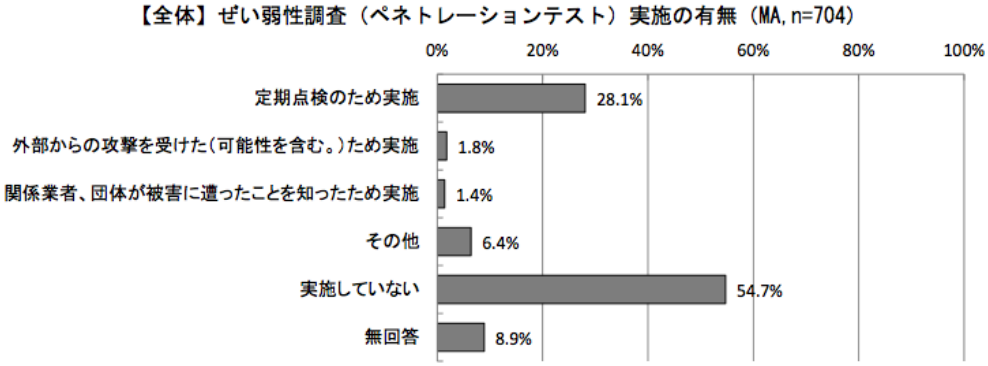
② 被害を受けたことによる対策

被害を受けたことによる対策をみると、セキュリティ教育の実施(43.1%)が最も高い。また、基本的な対策であるウイルス対策ソフトの導入や最新パッチの適応などを行っている。セキュリティポリシーの見直し(19.7%)より、被害が起きてもセキュリティ対策の見直しを行っている企業は少なく、またセキュリティコンサルティングの利用(12.4%)であることから、外部専門機関への協力を求めている企業が少ないことが分かる。



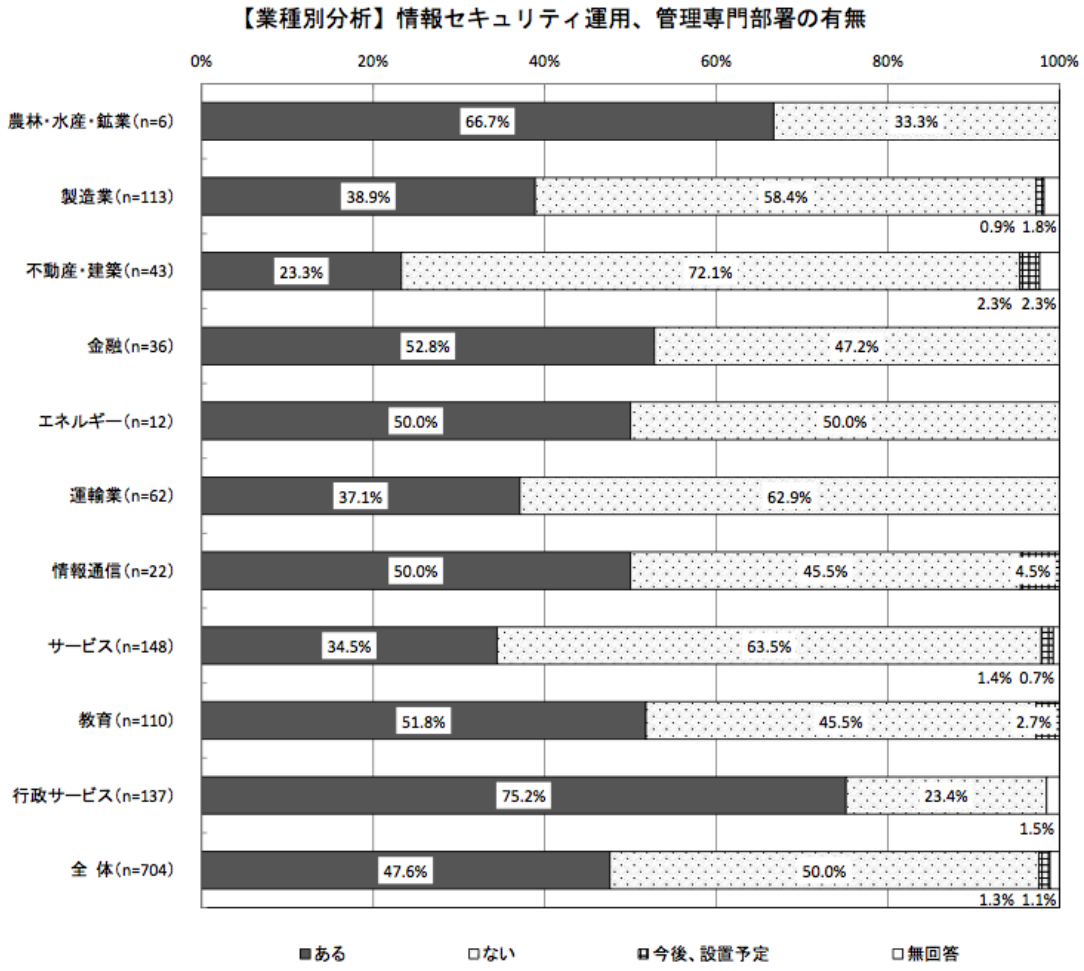
③ 脆弱性調査の実施有無

定期点検のため実施している企業は全体の 28.1%に留まり、過半数の企業は実施していないことが分かる。実施している企業はシステム会社や情報システムを保有している一部の企業のみと推察される。ほとんどのユーザー企業は使用している情報システムの脆弱性チェックを定期的に行っていないことが考察できる。



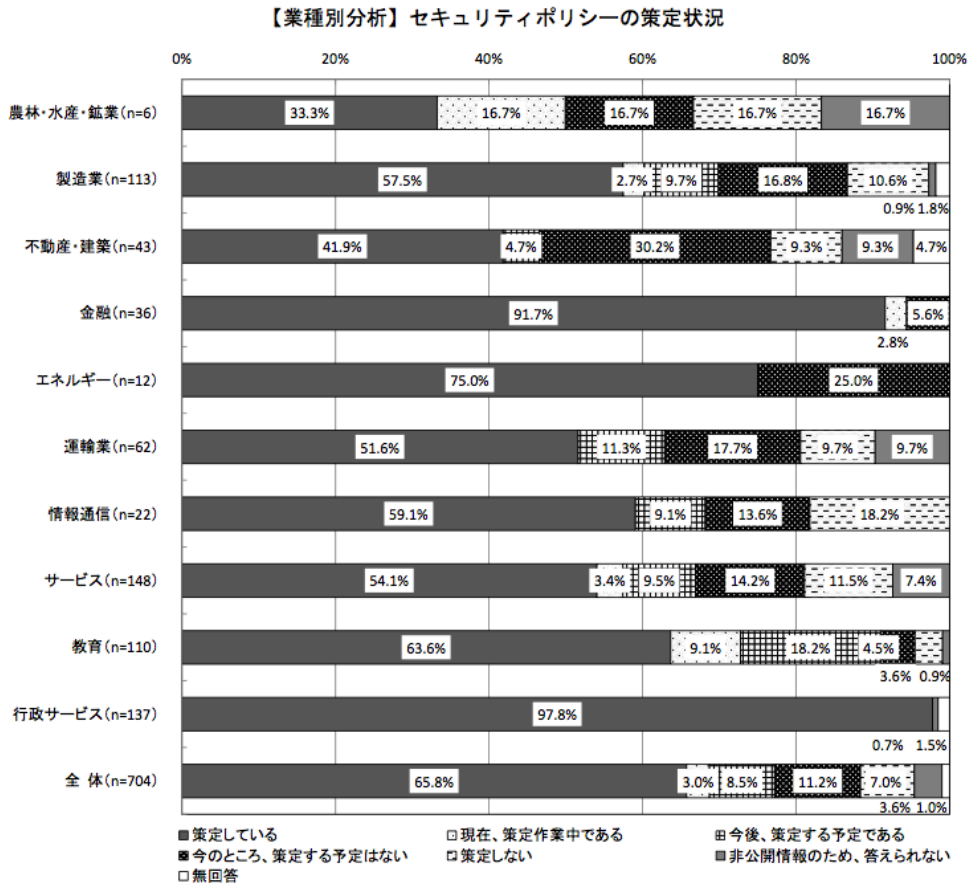
④　情報セキュリティ運用、管理部門の有無

情報セキュリティ運用､管理部門が約半数の企業において設置されていないことが分かる｡業種別にみると、製造業や不動産業、運輸業、サービス業が特に顕著である。



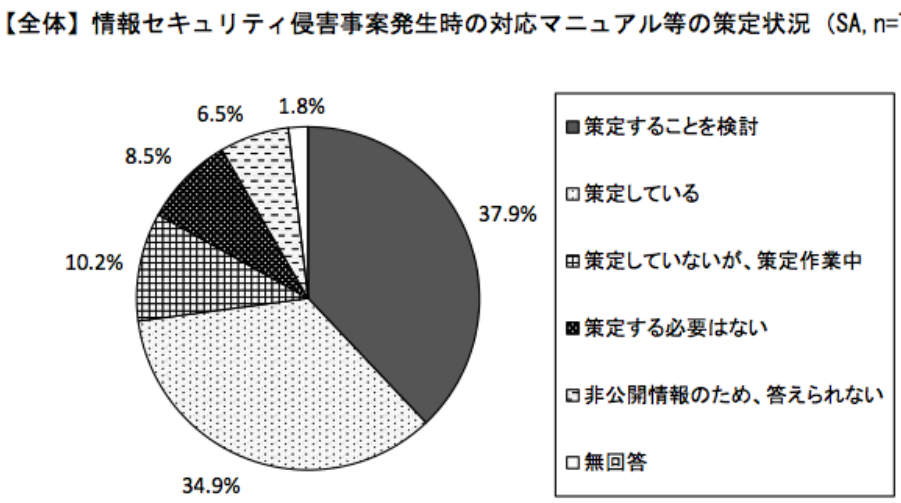
⑤　セキュリティポリシーの策定状況

多くの企業でセキュリティポリシーを策定していることが分かる。特に行政サービスや金融そしてエネルギーはビジネスの性質上セキュリティ対策に対して高い関心があることが分かる。



⑥　インシデント発生時の対応マニュアルの策定状況

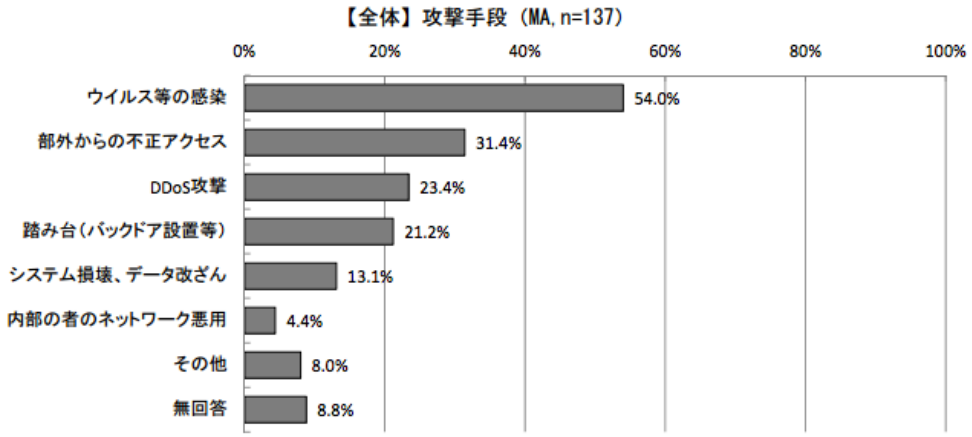
策定している(34.9%)、策定作業中(10.2%)とインシデントへの対策を行っている／行う予定の企業は全体の約４割であることが分かる。6 割の企業はインシデントに対して対策を行ってなく、セキュリティポリシー実施状況(65.8%)と比べると意識に差があることが分かる。



2. 主な攻撃手段と不正ログイン対策

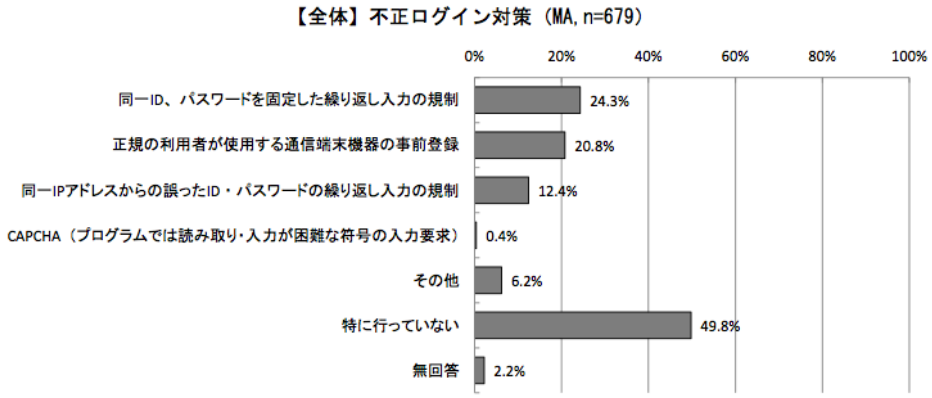
① 攻撃手段

ウイルス等の感染(54%)が最も攻撃手段と多い。部外からの不正アクセス(31.4%)と踏み台(21.2%)、システム損壊(13.1%)と続いているが、ウイルス感染後の連続した攻撃であると推察される。また、DDos 攻撃(23.4%)と相変わらず高く、大企業を狙った攻撃は高い確率で起きていると推察される。



② 不正ログイン対策

主な対策は、同一 ID、パスワードを固定した繰り返し入力の規制(24.3%)、正規の利用者が使用する通信端末の事前登録(20.8%)であり、基本的な対策を行っている。半数の企業は対策を行っていない。これからのことから、不正ログイン対策に対しての関心は低く脆弱性を抱えている状態であることが分かる。



（出所）不正アクセス行為対策等の実態調査調査報告書