

《勤務先における標的型攻撃の意識・実態調査》

～全国の情報システム管理者・従業員を対象に調査～

**従業員の40.7%は勤務先が標的型攻撃の対象になると意識し
情報セキュリティ対策は51.0%が厳しくなったと回答**

～情報システム管理者の79.3%が対策をさらに高めたいと回答し、今後の対策として「ウイルス対策」「ファイアウォール」「従業員への情報セキュリティ教育」「Webフィルタリング」を検討～

情報セキュリティメーカーのデジタルアーツ株式会社(本社:東京都千代田区、代表取締役社長:道具 登志夫、以下 デジタルアーツ、証券コード 2326)は、全国の企業に勤める従業員 1,109名、情報システム管理者 333名を対象に、勤務先における標的型攻撃の意識・実態調査を実施しました。

近年、企業を標的としたサイバー攻撃による被害が増加傾向にあり、機密情報や顧客情報といった重要情報を盗み出し、2次的に悪用される被害も増加傾向にあることから、全国の企業・団体に勤務する従業員には標的型攻撃に対する理解度や意識を、情報システム管理者には勤務先における標的型攻撃の対策の実態調査を行いました。

今回の調査では、従業員は、自分自身のセキュリティ意識は40.7%が「平均的」と考え、勤務先が標的型攻撃の対象になりうる可能性は40.7%が「ある」と回答し、普段から対策として気をつけていることとして、69.1%が「知らない送信者からのメールの添付ファイルは開封しない」と回答しました。勤務先における情報セキュリティに関するルールは、59.1%が「ある」ものの、社内研修受講経験は58.0%が「受けたことはない」と回答しています。

一方、情報システム管理者は、勤務先が標的型攻撃に遭遇する可能性は73.0%が「ある」と回答し、標的型攻撃に遭遇した場合に勤務先での致命的な想定被害として61.0%が「顧客情報の漏洩」を恐れ、被害後の対応として58.9%が「顧客への謝罪」を第一に考えていることがわかりました。また、従業員への教育や情報発信としては、「メールでの注意喚起・情報発信」が57.7%と一番多く、次に「専門部署による研修会・勉強会で直接レクチャー」42.6%、「専門企業からの派遣講師による研修会・勉強会で直接レクチャー」25.8%という結果になりました。

従業員の標的型攻撃への理解度と意識について

- 標的型攻撃と聞いて思い浮かべる内容は、「ウイルスに感染して会社のPCが遠隔操作される」49.1%、「添付ファイルがある不審なメールが送られてくる」46.1%、「外部から会社のWebサイトが改ざんされる」44.6%。
- 勤務先が標的型攻撃の対象になりうるという意識は、「ある」40.7%、「わからない」35.3%、「ない」24.0%。
- 自分自身のセキュリティに関する意識は「平均的と思う」46.9%、「少し高いと思う」19.7%、「少し低いと思う」16.4%。
- 普段から気をつけていることは、「知らない送信者からのメールの添付ファイルは開封しない」69.1%、「不審なWEBサイトを閲覧しない」44.4%、「会社で認められていないソフトをインストールしない」37.9%。
- 勤務先で情報セキュリティに関するルールは、「ある」59.1%、「ない」34.0%、「答えられない」6.9%と回答し、情報セキュリティに関する社内研修受講経験は「受けたことはない」58.0%、「同じ勤務先の専門部署による講習を受けた」29.3%、「外部の専門機関・専門スタッフの講習を受けた」6.7%と回答。
- 昨今の情報セキュリティ事件が社会問題化している風潮を受け、最近の勤務先の情報セキュリティ対策は、「変わらない」47.2%、「少し厳しくなった」28.8%、「だいぶ厳しくなった」22.2%と、51%が「厳しくなった」と回答。

PRESS RELEASE

標的型攻撃における情報システム管理者の意識と対策について

- 勤務先が標的型攻撃の対象になりうるという意識は、「ある」73.0%、「わからない」14.4%、「ない」12.6%。
- 標的型攻撃に遭遇した場合に勤務先での致命的な想定被害は、「顧客情報が漏洩する」61.0%、「人事関連・従業員の情報が漏洩する」30.3%、「自社の製品・サービスに関する情報が漏洩する」28.5%。
- 従業員に対しての教育や情報発信として行っていることは、「メールでの注意喚起・情報発信」57.7%、「専門部署による研修会・勉強会で直接レクチャー」42.6%、「専門企業からの派遣講師による研修会・勉強会で直接レクチャー」25.8%。
- 標的型攻撃で被害を受けた後の事後対応策は、「顧客への謝罪」58.9%、「再発防止策の策定作業」47.4%、「被害状況の調査」45.3%を検討。
- 今後の勤務先のセキュリティ対策について、「更に高めたい」79.3%、「現状維持で良い」19.5%と考え、具体策としては、「ウイルス対策」56.4%、「ファイアウォール」45.8%、「従業員への情報セキュリティ教育」39.8%、「Web フィルタリング」37.1%を検討。

【調査概要】

調査対象： 全国の20歳以上の就業者(男女)

調査期間： 2015年7月23日(木)～25日(土)

調査方法： インターネット調査

有効回答数： 1,442 サンプル(情報システム管理者: 333 サンプル、従業員: 1,109 サンプル)

実施機関： Fastask

今回の調査結果の傾向として、全般的に標的型攻撃やセキュリティにおける意識が情報システム管理者と従業員では乖離があることから、従業員への教育や情報共有において再度見直す必要があると考えます。標的型攻撃の対策として重要なことは不審なメールが送られてきても開かないことですが、まだ約3割の従業員が認識していませんでした。また、不審なメールを開封しないことに加えて、個人で意識している対策として44.4%が「不審なWebサイトを閲覧しない」、37.9%が「会社で認められていないソフトをインストールしない」と半数を下回る数値となっていることから、早急な従業員への教育強化と同時に確実に防げるシステム面での対策も求められます。

デジタルアーツでは定期的に行う情報セキュリティに関する調査を通じて、規模を問わず狙われる企業・官公庁が増えている現状から、経営の根幹を揺るがしかねない機密情報漏洩を防止するための注意喚起を経営層に訴求し続けることで、今後、日本のセキュリティインシデントが減少することを願っております。引き続き、情報セキュリティメーカーとして、全国レベルの調査結果を通じて様々な情報を提供してまいります。

■ デジタルアーツについて <http://www.daj.jp>

デジタルアーツは、フィルタリング技術を核に、情報セキュリティ事業を展開する企業です。製品の企画・開発・販売・サポートまでを一貫して行い、国産初のWebフィルタリングソフトを市場に出したメーカーならではの付加価値を提供しています。また、フィルタリング製品の根幹を支える国内最大級のWebフィルタリングデータベースと、世界27の国と地域で特許を取得した技術力が高く評価されています。国内でトップシェアを誇るWebフィルタリングソフトとして、家庭および個人向け「i-FILTER」、企業向け「i-FILTER」「i-FILTER ブラウザー & クラウド」を提供する他、企業向けとして電子メールセキュリティソフト「m-FILTER」、クライアント型電子メール誤送信防止ソフト「m-FILTER Mail Adviser」、純国産のセキュア・プロキシ・アプライアンス製品「D-SPA」、ファイル暗号化・追跡ソリューション「FinalCode」を提供しています。

※ デジタルアーツ/DIGITAL ARTS、ZBRAIN、アイフィルター/i-FILTER、m-FILTER/m-FILTER MailFilter/m-FILTER Archive/m-FILTER Anti-Spam/m-FILTER File Scan、D-SPA はデジタルアーツ株式会社の登録商標です。

※ FinalCode は株式会社アイキューエスの登録商標です。

※ その他、上に記載された会社名および製品名は、各社の商標または登録商標です。