

**<<勤務先における標的型攻撃対策に対する意識・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～

**標的型メール訓練の結果、メールや Web を開くまでの時間が  
増加し、業務生産性が低下したと管理者の約 50%が回答  
～管理者・従業員が意識せず Web やメールを閲覧できる、セキュリティ対策製品の必要性高まる～**

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情報システム管理者 330 名、従業員 1,105 名を対象に、勤務先における標的型攻撃対策に対する意識・実態調査を実施しました。

近年、特定の企業・団体等を狙った標的型攻撃は特にメールによる攻撃が増加傾向にあり、2018 年に警察庁が観測したサイバー犯罪件数は過去最多を記録、組織にとって情報セキュリティへの脅威は増えています。このような状況から企業における標的型攻撃を想定した対策として、主に標的型メール訓練が実施されており、それらの実施状況と意識について、情報システム管理者と従業員を対象に聴取しました。

今回の調査では、Web とメールの現状について、情報システム管理者の 59.1% が、自社の Web とメールの現状に課題を感じており、そのうち 73.8%が「解決をあきらめている」と回答しています。多層防御等のセキュリティ対策を実施したものの課題が解決されないため、社員のセキュリティ意識向上に対策をシフトし、標的型メール訓練を導入しているのではないかと推測されます。

標的型攻撃対策として標的型メール訓練を導入している企業は、71.8%ありました。情報システム管理者・従業員ともに、「導入した製品」よりも訓練メールを含む「社内の教育」の方が対策の効果があつたと回答しており、利用者自身の知識により補っていると実感しています。標的型メール訓練をはじめとする社員教育が一定の効果をもたらしていることを表しています。

一方で、情報システム管理者の 30.8%が、訓練メールの結果は「評価に影響する」と回答しています。そのため、URL (1 つ)・メール(1 通)の安全を確認して開封する時間が以前に比べて長くなったと感じる人が約 50%、そのうち 2～3 倍長くなったと感じる人が 80%以上いました。これは、訓練メールを徹底したことによる効果と反比例して、業務の生産性が低下しているのではないかと推測されます。また、訓練メールや不審なメールを開封してしまった経験のある従業員は 21.0%で、管理者の約 3 分の 1 以下という結果であり、教育や注意等がなされていない(認識していない)ため気付いていない可能性が推測されます。

Web とメールの現状について

- 情報システム管理者の 59.1% が、自社の Web とメールの現状に課題を感じており、そのうち 73.8%が解決をあきらめている

標的型メール訓練について

- 標的型攻撃対策として標的型メール訓練を導入している企業・団体は、71.8%

## PRESS RELEASE

- 情報システム管理者・従業員ともに、半数以上は「社内の教育」と認識しており、「利用者自身の知識で補っている」との実感を持っている。情報システム管理者の半数は「製品の効果」も実感
- 訓練メールを開封してしまった場合、該当社員に何らかの教育を課す・注意する等の対応を取る情報システム管理者は半数だが、「評価に該当する」との回答も 30.8%と厳しい対応
- 一方、開封してしまった場合の対応について認識していない従業員が 32.7%
- 訓練メールや不審なメールを開封してしまった経験のある従業員は 21.0%であるが、教育や注意等がなされていない(認識していない)ため気付いていない可能性も考えられる
- 標的型攻撃対策を行う前後で、メールの安全を確認する時間が「長くなった」と回答した人のうち、URL(1 つ)・メール(1 通)の安全を確認して、開封する時間が「2~3 倍長くなった」と感じると回答したのは、管理者で 70~80%程度、従業員では 80%以上

### 不審な Web とメールの見分け方について

- 不審なメールを見分ける要素は「送信元のメールアドレス」「件名」とする人が 60%以上
- 不審な URL・Web ページを見分ける要素は「ドメイン」とする人が 60~70%
- 情報システム管理者の半数近くは「周りの人からの情報」も活用
- 不審な URL・Web ページを開いてしまった場合の対応について、標的型メール訓練と同様、該当社員に何らかの教育を課す・注意する等の対応を取る情報システム管理者が半数。一方で、従業員が約 80%は「特になし／わからない」と回答しており、管理者と従業員との間で認識の相違がみられる

#### 【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: 2019 年 3 月 28 日(木)~4 月 1 日(月)

調査方法: インターネット調査

有効回答数: 1,435 サンプル(情報システム管理者: 330 サンプル、従業員: 1,105 サンプル)

実施機関: Fastask

今回の調査結果の傾向として、全体的に標的型メール訓練の導入は進んでおり、情報システム管理者と従業員の双方で一定の効果が得られています。しかしながら、訓練メールを開封した経験の有無に管理者と従業員間の回答数に乖離があり、従業員が訓練自体を認識していないことが考えられ、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。また、多種多様なセキュリティ対策製品の導入により標的型攻撃対策が施されていますが、情報システム管理者がセキュリティ対策に対する課題がいまだ残る傾向にある現状をふまえ、標的型メール訓練をはじめとする社員教育により、引き続き従業員一人ひとりのセキュリティ意識を向上していくための教育を企業が行うことに加え、今後は、業務効率化の観点から Web とメールの閲覧において従業員がセキュリティ脅威を意識せず利用できる仕組みを、製品によって対策する必要があると考えます。

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、企業・官公庁をターゲットとする標的型攻撃が増加している現状から、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訴求し続けることで、セキュリティインシデントの減少に寄与してまいり所存です。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。

以上

■ **デジタルアーツについて** <https://www.daj.jp>

デジタルアーツは Web やメール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。

インターネットの黎明期であった 1998 年に初めて国産の Web フィルタリングソフトを世に送り出した先駆者であり、これまでの知見をもとに、情報漏洩対策や標的型攻撃をはじめとするサイバー攻撃対策を実現する、最先端の情報セキュリティ製品を提供しています。

国産メーカーの強みを生かして、製品の企画・開発・販売・サポートまでを一貫して行っており、プロダクト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は、高い評価を得ております。契約更新率 95%以上という実績は、顧客満足度が高い証左です。

国内シェアの 50%以上を占める Web セキュリティソフト「i-FILTER」を中心に、個人・家庭向けの「i-フィルター」、メールセキュリティソフト「m-FILTER」、ファイル暗号化・追跡ソリューション「FinalCode」などの製品を揃えており、ワンストップで Web やメール、ファイルのセキュリティ対策を実現できます。

「より便利な、より快適な、より安全なインターネットライフに貢献していく」という理念のもと、デジタルアーツは全てのステークホルダーの皆さまに信頼される東証一部上場企業として成長を続けています。

※ デジタルアーツ、DIGITAL ARTS、i-FILTER、info board、ARS、Active Rating System、ACTIVE RATING、ZBRAIN、D-SPA、SP-Cache、NET FILTER、White Web、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER File Scan、Mail Detox、FinalCode、i-フィルター、DigitalArts@Cloud、D アラート、当社・当社製品関連の各種ロゴ・アイコンはデジタルアーツ株式会社の商標または登録商標です。

※ 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。

---