サイバー犯罪被害に係る企業・団体を対象としたアンケート調査結果及び対策

【調査の概要】
国内の企業等2,950社等を無作為に抽出（R4.9.9～R4.12.7）。有効回答数590件。

過去１年以内に受けたことのある被害

ホームページの改ざん、メールの不正中継、ランサムウェアによる被害が上位を占める

R4 ※ 被害を受けた団体における割合

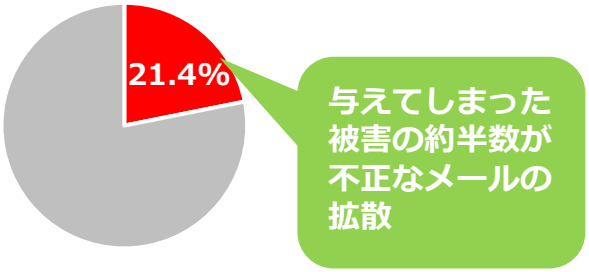
1位	ホームページの改ざん	24.5%
2位	メール不正中継	22.4%
3位	ランサムウェア	12.2%

R3 ※ 被害を受けた団体における割合

1位	ランサムウェア	22.1%
2位	メール不正中継	15.8%
3位	ホームページの改ざん	12.6%

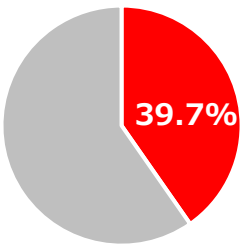
サプライチェーンリスク

自社が被害を受けたことにより関連会社等へ被害を与えてしまった割合が2割以上



■ 被害を与えてしまった

約４割がサプライチェーンリスクに対する対策を実施



■ 対策を行っている

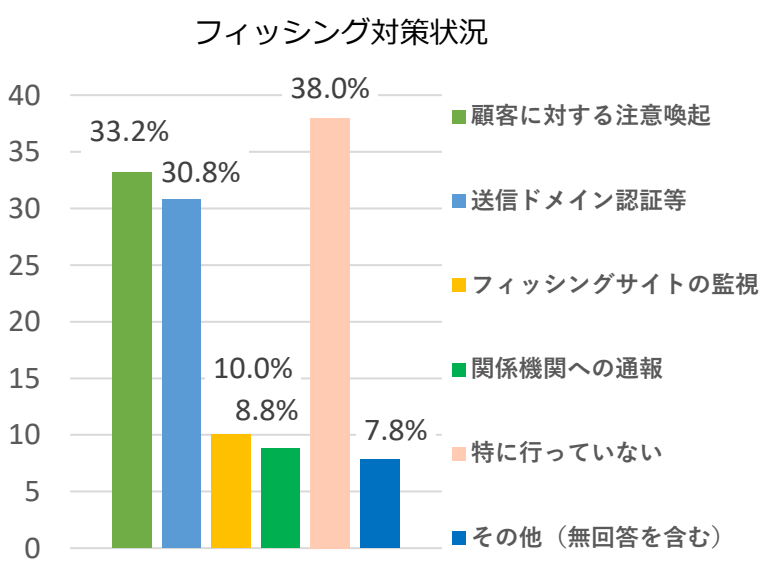
主な対策

- ○ 契約にセキュリティポリシーの遵守を明記
- ○ 取引先等の情報セキュリティ評価を実施
- ○ 関連会社等との情報セキュリティに関する教育・訓練・情報共有等を実施

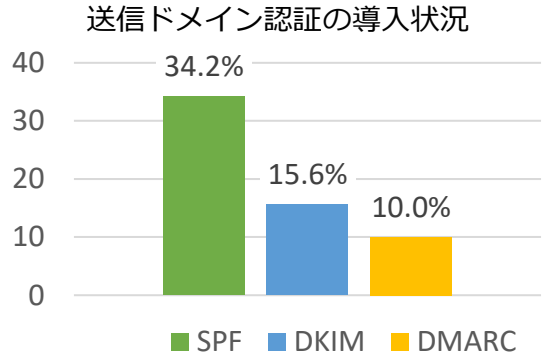
など

顧客に対するフィッシング対策

注意喚起や送信ドメイン認証による対策が多数



送信ドメイン認証はDKIM、DMARCの導入が低調



（参考）送信ドメイン認証技術導入マニュアル【第３版】
DMARCを含めた送信ドメイン認証に関する技術的な導入マニュアルが、迷惑メール対策推進協議会から公表されています。
https://www.dekyo.or.jp/soudan/aspc/report.html

被害に遭わない、被害を与えないために

ホームページの改ざん対策

OSやアプリケーションソフト、VPN機器などに脆弱性があると、ホームページが改ざんされたり、データが漏えいしたりするおそれがあります。

- **OS・Webサーバソフト・CMSの更新**
- **Webアプリケーションの脆弱性対策**
- **WAF（※）の導入**

（※）Web Application Firewallの略

メール不正中継対策

メールの添付ファイルを開いたりすることでマルウェアに感染し、取引先などに不正なメールを拡散させてしまうおそれがあります。

- **不用意にメールの添付ファイルを開いたり、メール本文中のURLをクリックしない**
- **不用意に添付ファイルのマクロを有効にしない**
- **ウイルス対策ソフトの更新**

ランサムウェア対策

VPN機器やリモート・デスクトップ・サービスなどの認証パスワードが脆弱な場合、ネットワークに侵入されるおそれがあります。

- **最新パッチの適用などVPN機器等の脆弱性対策**
- **認証情報の適切な管理やアクセス権等の最小化**
- **データのバックアップ等の取得**

その他の対策

- ○ **IPアドレスで制限**
- ○ **多要素認証などを設定**

より詳しい被害防止対策は警察庁ウェブサイト「ランサムウェア被害防止対策ページ」を御参照ください。

⚠被害に遭ってしまったら

警察に通報・相談をお願いします！！

警察庁 National Police Agency

ご相談は都道府県警察本部のサイバー犯罪相談窓口へ