令和６年１月

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2,951社等を無作為に抽出（R5.8.23～R5.9.15）。有効回答数618件。

過去１年以内に受けたことのある被害

ランサムウェア、フィッシング、メールの不正送信による被害が上位を占める

R5　※ 被害を受けた団体における割合

1位	ランサムウェア	17.8%
2位	フィッシング	14.4%
2位	メールの不正送信	14.4%

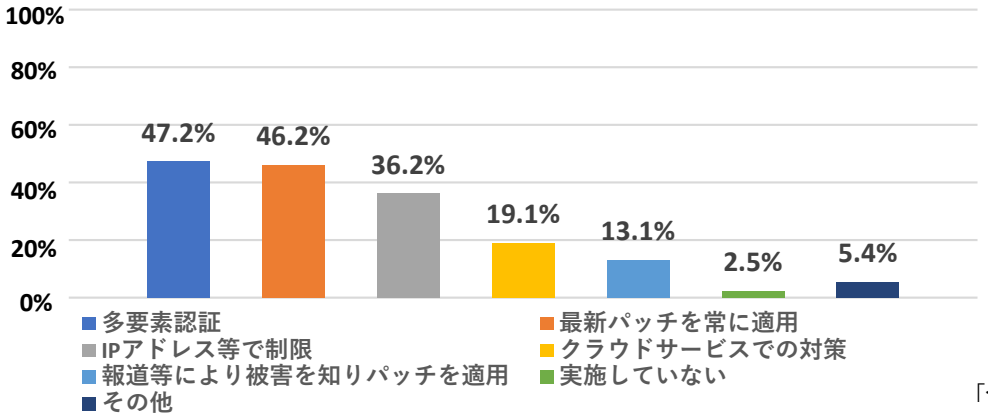
R4　※ 被害を受けた団体における割合

1位	ホームページの改ざん	24.5%
2位	メールの不正送信	22.4%
3位	ランサムウェア	12.2%

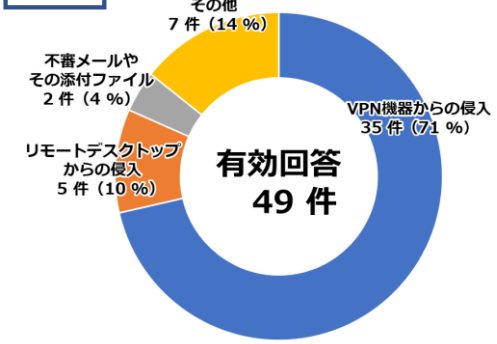
ランサムウェア対策

ランサムウェア被害が高い水準で推移。VPN機器/サービスからの感染が約７割であり、 VPN機器/サービスへの対策を含めた外部からの接続に対するセキュリティ対策が課題。

VPN機器のセキュリティ対策の実施状況



参考

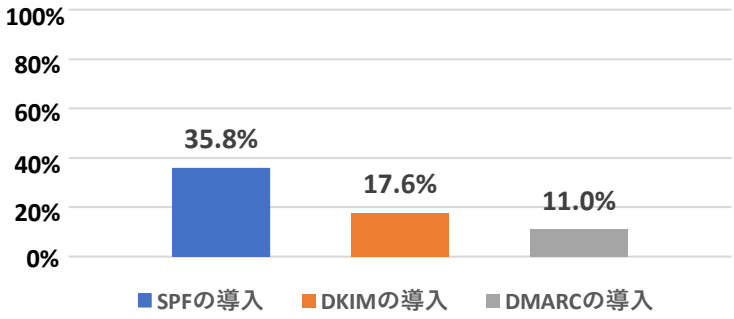


「令和５年上半期サイバー空間脅威情勢」（警察庁）抜粋

フィッシング対策

送信ドメイン認証技術の導入状況は低調であり、導入促進が課題。

送信ドメイン認証の導入状況

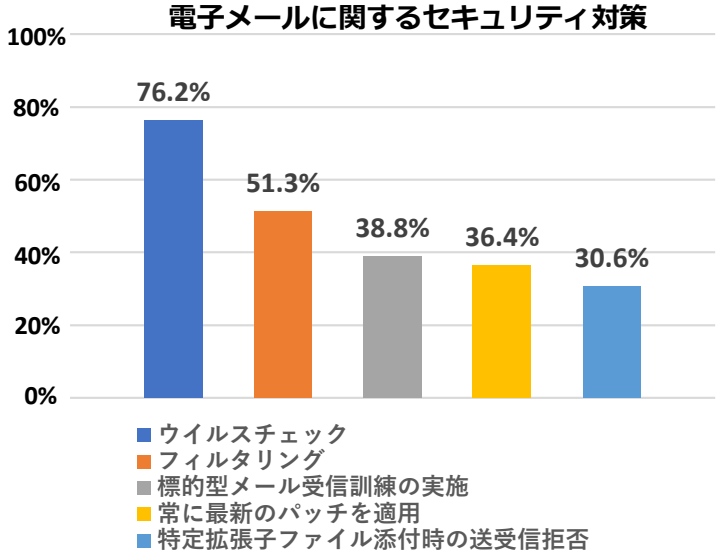


（参考）送信ドメイン認証技術導入マニュアル
DMARCを含めた送信ドメイン認証に関する技術的な導入マニュアルが、迷惑メール対策推進協議会から公表されています。
https://www.dekyo.or.jp/soudan/aspc/report.html

不正送信メール対策

ウイルスチェックやフィルタリングが５割を超えるも、訓練の実施は４割弱であり、意識の底上げが課題。

電子メールに関するセキュリティ対策



被害に遭わない、被害を与えないために

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**
- **IPアドレス等によるアクセス制限**
- **多要素認証等による認証の強化**

フィッシング対策

フィッシングサイトへは、企業の本物のメールアドレスになりすましたメールで誘導するケースが確認されています。

- **送信ドメイン認証技術（※）の導入**
  （※）SPF、DKIM、DMARC
- **取引等のモニタリング強化**
- **公式サイトのお気に入り登録や公式アプリの活用の促進**

不正送信メール対策

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。

- **ウイルス対策ソフトの導入・更新（ウイルスチェックの実施）**
- **フィルタリングの導入（特定の条件を満たすメールの配信を制限）**
- **標的型攻撃メール訓練の実施**

より詳しい被害防止対策は警察庁サイバー警察局のウェブサイトを御参照ください。

https://www.npa.go.jp/bureau/cyber/index.html

⚠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

https://www.npa.go.jp/bureau/cyber/soudan.html