

# 標的型メール対応訓練の結果について



令和7年1月下旬に、県内の病院を対象に標的型メール対応訓練を実施しました。

下記の結果を踏まえ、サイバーセキュリティ対策への各種取組にご活用いただきますよう、よろしくお願いいたします。

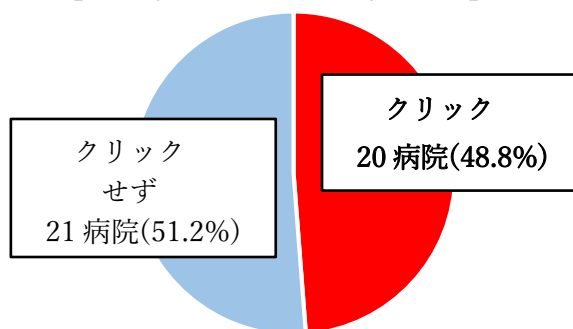
## 訓練結果

### 20 病院（約 49%）が URL をクリック！！

※県内 138 病院のうち、41 病院（90 メールアドレス）に対して実施

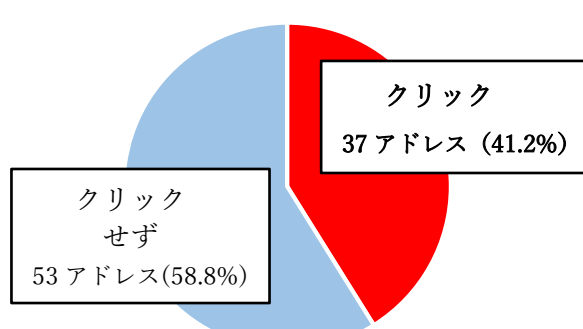
## URL のクリック状況

### 【 病院別クリック状況 】



※前回は 41 病院中、22 病院（53.7%）がクリック（令和6年1月実施）

### 【 メールアドレス別クリック状況 】



※前回は 95 アドレス中、37 アドレス（38.9%）がクリック（令和6年1月実施）

病院別内訳	病床数			
	100未満	100～199	200～299	300以上
参加病院数	12	12	10	7
クリック数	5	5	5	5
クリック率 (%)	41.7	41.7	50	71.4

メールアドレス別内訳	病床数							
	100未満		100～199		200～299		300以上	
アドレス総数	25		22		22		21	
クリック数	12		6		9		10	
クリック率 (%)	48		27.3		40.9		47.6	
アドレス種別	個人用	組織用	個人用	組織用	個人用	組織用	個人用	組織用
	9	16	8	14	7	15	7	14
クリック数	4	8	3	3	4	5	2	8
クリック率 (%)	44.4	50.0	37.5	21.4	57.1	33.3	28.6	57.1

## 標的型メールとは



「**標的型メール**」は、特定の事業者の重要情報を盗むことを目的として関係機関や顧客などを装う等、巧妙に作りこまれたコンピュータウイルスへの感染を目的としたメールです。たった一人の職員がメールの本文中のリンクをクリックしたり、添付ファイルを開封すると、情報が漏えいするおそれがあります。

なお、データを暗号化し、復号のために身代金を要求する「**ランサムウェア**」の感染経路の一つとして、メールを経由して不審ファイルをインストールするものも確認されています。

## 不審メールを見破るポイント

CHECK!!



① 公的機関からのメールに  
**フリーのメールアドレス**が  
使用されている

② **【重要】**など  
受け手に確認し  
なければ！！と  
思わせる件名

送信した訓練メール✉

送信者：“医務保険課” < soumu.kg@gmail.com >

件 名：**【重要】**山口県からのお知らせ】マイナ保険証について

本 文：各病院の管理者 様

このことについてマイナ保険証の連絡いたします。

次のURLにてご確認ください。

③ **URLが短縮されている**  
(カーソルを合わせると  
元のURLが表示されます)

<https://x.gw/g9nks>

④ **日本語が**  
表記が不自然



## メールが届いた場合の対応要領

- 1 添付ファイル、URLがある場合は不審点がないか、いつもよりよく確認する
- 2 不審なメールを受信したら、**送信元に直接問い合わせる**
- 3 送信事実がなければ、職場のシステム部門に速報して**組織内で情報共有**するなど、必要な対策をとる

※今回の訓練で医務保険課への問い合わせを実施した病院は、**3病院（全体の7.3%）**でした。

今回の訓練をきっかけに、不審メールに関して注意意識を持つとともに、対応手順のご確認をよろしくお願いします。



【本件担当】山口県警察本部サイバー犯罪対策課