

標的型メール対応訓練結果

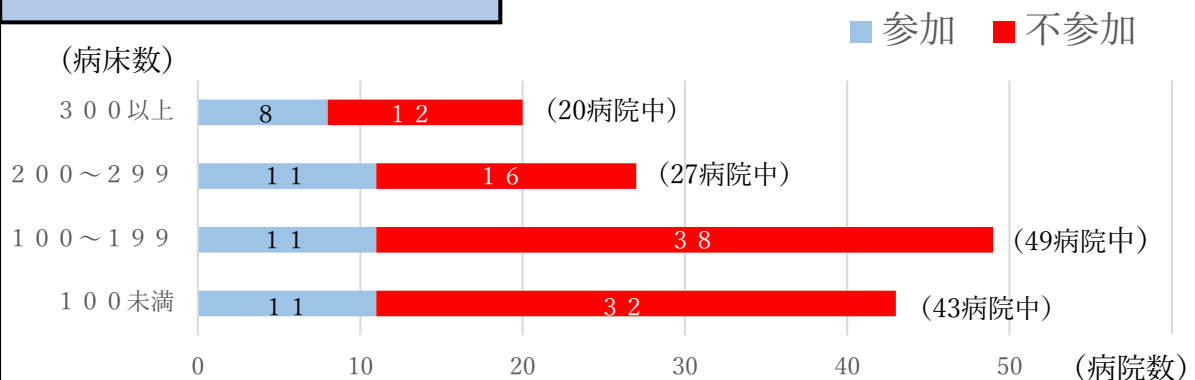


本年1月18日に実施した県内病院対象の標的型メール対応訓練結果をお伝えします。
県内の病院におけるサイバーセキュリティ対策への取組実態の見直し、病院内で医療に従事される皆様への教養等にご活用いただきますよう、よろしくお願い申し上げます。

訓練結果

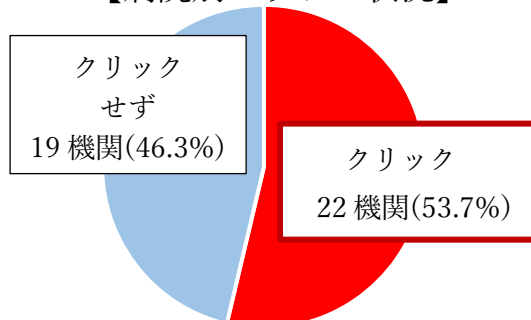
- ◎ 県内 139 病院のうち、41 病院（約 30％）が訓練に参加
- ◎ 参加の 41 病院のうち、22 病院（約 53％）がメール文中の URL をクリック

病床数別の訓練参加状況

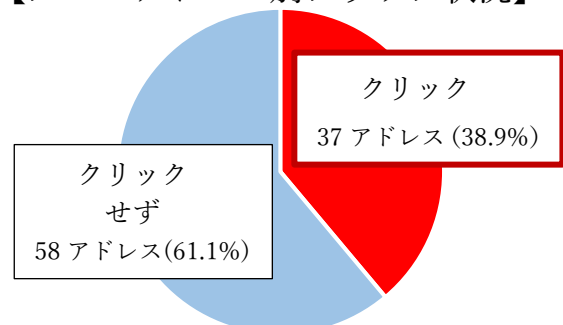


URL のクリック状況（参加：41 病院・95 メールアドレス）

【病院別クリック状況】



【メールアドレス別クリック状況】



クリック状況の内訳詳細分析

【病院別分析】

	病床数			
	100未満	100～199	200～299	300以上
参加病院数	11	11	11	8
クリック数	6	6	7	3
クリック率%	54.5	54.5	63.6	37.5

【メールアドレス別分析】

	病床数			
	100未満	100～199	200～299	300以上
参加アドレス数	23	24	26	22
クリック数	8	10	11	8
クリック率%	28.5	41.6	42.3	36.3

訓練メールの解説（見破るポイント）

今回の送信した
訓練メール

送信元：“医務保険課” <soumu.kg@gmail.com> ①

件 名：【至急山口県からのお知らせ】インフルエンザワクチンについて ②

各病院の管理者 様

このことについてインフルエンザワクチンの連絡いたします。 ③

次のURLにてご確認ください。

<https://x.gw/g9nks> ④

山口県健康福祉部

医務保険課医療指導班

TEL 083-933-2820

FAX 083-933-2939



重要

- ① 公的機関からのメールに、**フリーメール**が使用されている
- ② **【重要】**や**【至急】**等の件名を使用し、確認させようとする
- ③ 不自然な日本語が使用されている
- ④ リンク先のURLが**短縮**されている

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って巧妙に作りこまれた**ウイルス付きメール**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**すると感染し、**情報が漏洩する危険性**があります。

なお、**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**してしまうものがあるので、注意が必要です。

不審メールが届いた場合の対応要領

- ① **メールの文面で内容が完結しないものは、一律に警戒する**
 - ② メール添付ファイルは開かず、メール文中のURLはクリックしない
 - ③ 不審なメールを受信したら、送信元に直接問い合わせる
 - ④ 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し、メールを削除する
- ※ 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、4病院（参加した病院の8.9%）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