ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●大規模接種センター騙るフィッシングサイト、対策協議会が注意喚起

https://www.itmedia.co.jp/news/articles/2108/31/news085.html
https://www.antiphishing.jp/news/alert/mhlw_20210830.html
https://twitter.com/MHLWitter/status/1432199880940797953

### このニュースをザックリ言うと･･･

- 8月30日(日本時間)、フィッシング対策協議会より、厚生労働省および自衛隊の大規模接種センターを騙るフィッシングが確認されたとして注意喚起が出されています。

- フィッシングメールは件名「自衛隊 大規模接種センターの概要　予約サイト案内（予約・受付案内）」等とされ、「予約サイト」「お問い合わせ・予約窓口」のリンクから厚労省「コロナワクチンナビ」の偽サイトに誘導され、個人情報(氏名・住所・電話番号・メールアドレス・生年月日等)およびクレジットカード情報(カード番号・有効期限・セキュリティコード)を詐取する模様です。

- 同日、厚労省からもTwitterにて「コロナワクチンナビに銀行口座やクレジットカード番号などの登録を求めることはありません」とする注意喚起が出されています。

### AUS便りからの所感等

- 同協議会からは、厚労省を騙るフィッシングについて8月13日にも「【重要】新しいコロナウイルスの発生の予防と管理」という件名のメールによるフィッシングに注意喚起が出されています。

- また8月24日には、2020年10月に確認された(AUS便り 2020/10/19号参照)「二回目特別定額給付金の特設サイト」を騙るフィッシングが再び確認されているとして、同協議会から注意喚起が出されています。

- 依然として終息の気配を見せない新型コロナウイルス感染症と関連した出来事に便乗して、様々なフィッシングが横行していますが、とにかくWebブラウザー・アンチウイルスおよびUTMのアンチフィッシング機能を有効にし、省庁等からの公式発表、セキュリティ関連各社・団体からの啓発情報、Twitter等における報告を確認し、利用しているサービスについてはブラウザーのブックマーク等からアクセスする等、フィッシングからの各種自衛策を着実に実行することが肝要です。

フィッシング対策協議会
Council of Anti-Phishing Japan

**厚生労働省をかたるフィッシング (2021/08/30)**

▸ メールの件名

自衛隊 大規模接種センターの概要　予約サイト案内（予約・受付案内）

※上記以外の件名も使われている可能性があります。

▸ 詳細内容

厚生労働省をかたるフィッシングの報告を受けています。

1. 2021/08/30 10:00 時点では、フィッシングサイトは稼働中であり、JPCERT/CC に サイト閉鎖のための調査を依頼中です。 類似のフィッシングサイトが公開される可能性が ありますので、引き続きご注意ください。
2. このようなフィッシングサイトにて、氏名、住所、都道府県、郵便番号、電話番号、メールアドレス、生年月日、 カード名義人、カード番号、有効期限、セキュリティコード等を絶対に入力しないよう、ご注意ください。
3. フィッシングサイトは本物のサイトの画面をコピーして作成することが多く、見分けることは非常に困難です。日頃から個人情報の入力を要求された場合は、入力する前に一度立ち止まり、似たようなフィッシングや 詐欺事例がないかを、確認するようにしてください。
4. 類似のフィッシングサイトやメール、SMS を発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご報告ください。 【報告方法】はこちら

自衛隊大規模接種センターの予約については、下記注意事項をご覧頂き、
ページ下部に記載のWeb予約サイト、ＬＩＮＥまたは、専用お問い合わせ・予約窓口（電話）により、予約を行ってください。

■予約サイトへ

■お問い合わせ・予約窓口

□ の部分のリンク
<https://www.v-cysa●●●●.com/> など

予約に関するお願い
自衛隊大規模接種センターでは、原則として、接種券（原本）をお持ちいただいていない場合、ワクチンの接種はできません。接種券がお手元に届いてからご予約いただき、当日、接種券（原本）を必ずお持ち下さい。

■自衛隊 東京大規模接種センター専用
お問い合わせ・予約窓口
開設時間:07時00分～21時00分（毎日）
お電話のおかけ間違いにご注意ください。
一般:0570-056-730
English:0570-056-750
副反応:0570-056-760
※問い合わせのみ



メール文面の例

## ●都健康安全研究センター配布リーフレットのQRコードから不審なサイトへ…注意喚起

https://twitter.com/tocho_shokuhin/status/1430777197871079430
http://www.tokyo-eiken.go.jp/ki_shoku/chuui/

### このニュースをザックリ言うと･･･

- 8月26日(日本時間)、東京都健康安全研究センターより、同センターが過去に配布したリーフレットに印刷されたQRコードから、都のものではない不審なサイトにアクセスする事象が確認されたとして注意喚起が出されています。

- リーフレットは「1歳未満の乳児にはちみつを与えないでください！」と題して2018～2019年に配布されていたもので、印刷されたQRコードは本来東京都の食の安全に関するFAQサイトにアクセスするものだった模様です。

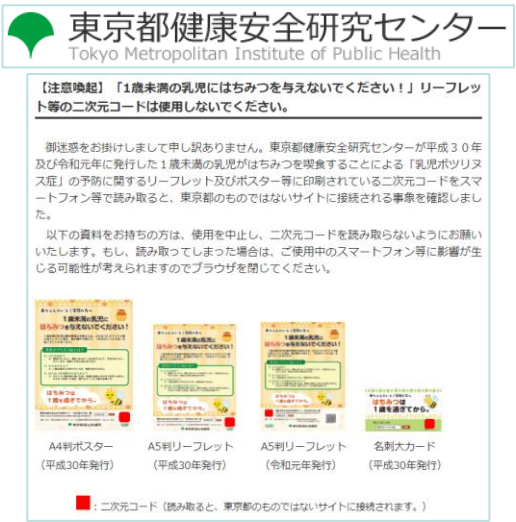
- 同センターでは、当該QRコードを使用せず、またコードを読み取ってサイトにアクセスした場合、先に進まずブラウザーを閉じるよう呼び掛けています。

### AUS便りからの所感

- QRコードのアクセス先は都健康安全研究センターのドメイン(tokyo-eiken.go.jp)でなければgo.jpでもない外部のドメイン名にて設置されたもので、そのドメイン名が失効した後に第三者に取得される「ドロップキャッチ」があったとみられます。

- go.jpドメインを持つ政府機関あるいは地方自治体等が、イベント等の目的で別のドメイン名を取得してサイトを立ち上げ、後年失効してドロップキャッチされるケースは度々発生しています。

- 特にリーフレットや新聞書籍のような印刷物にURLそのものやQRコードの形で掲載されるアクセス先が第三者のサイトとなってしまう恐れを鑑みるならば、可能な限り「既存の企業ドメイン名のサブドメイン等を用いる」方向性をとることが安全といえ、独自のドメイン名を扱う必要があるならば、ドロップキャッチによるリスクを最小限に抑えるよう「サイトの閉鎖時にサイト上での告知や関係各所への通知を十分に行う」「閉鎖後も数年以上はドメインを維持する」等を行うことを強く推奨致します。




## ●打楽器専門店ECサイトにてクレジットカード情報流出発生…最大1,667件

https://www.itmedia.co.jp/news/articles/2108/24/news138.html
https://komakimusic.co.jp/pages/important-notices

### このニュースをザックリ言うと･･･

- 8月23日(日本時間)、打楽器専門店のコマキ楽器より、同社ECサイト「コマキ楽器WEBサイト」が不正アクセスを受け、クレジットカード情報が流出した可能性があると発表されました。

- 被害を受けたのは、2019年11月27日～2021年2月19日に同サイトに入力された1,667件(1,513人)分のクレジットカード情報(カード番号・名義人・有効期限およびセキュリティコード)となっています。

- 2月19日に決済代行事業者からの指摘を受けて同サイトでのカード決済を全停止(のち同サイトで使用していたサーバー・システムは全て破棄)、5月31日までの第三者機関の調査結果により、不正アクセスが発覚したとしています。

### AUS便りからの所感

- 同サイトのシステムにあった一部の脆弱性を突いての不正アクセスによるもので、ペイメントアプリケーションの改ざんが行われたとしており、一部カード情報について不正利用の被害も確認されているとのことです。

- 長年のECサイトからのカード情報流出の事例から、サーバー上にカード情報を保存しない仕様が増えたことで、カード情報を奪取る手口は「カード情報の入力フォームを改ざんし、入力されたカード情報を奪取する」等へ主流が移行しており、今回もプログラムの改ざんにより、フォームから入力されたクレジットカード情報が攻撃者にも送信される等に仕向けられた可能性が考えられます。

- ECサイト構築で良く利用されるソフトウェアにおいて古いバージョンに存在する脆弱性が悪用され、このような改ざんが行われるケースが度々報告されており、これに対する根本的な対策として「使用している各ソフトウェアを常に最新のバージョンに保つ」「不正なリクエストを検知・遮断するソリューションの導入」等を行うようにし、また不正アクセスの事案が発生する前の段階で、第三者機関によるセキュリティ診断を受け、システムの安全性を確認すべきでしょう。