

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。

## ●厚労省のメールサーバーから約10万通のスパム送信…海外からの不正アクセスで踏み台に

<https://www.itmedia.co.jp/news/articles/2305/30/news099.html>

<https://www.mhlw.go.jp/stf/houdou/202305291400.html>



### このニュースをザックリ言うと…

- 5月29日(日本時間)、**厚生労働省**より、同省の**メール中継サーバー**を経由して、**第三者による迷惑メール**が送信されていたと発表されました。
- 発表によれば、メールは**件名が「Re: Can I trust you?」**で、**本文も英文**、**発信元メールアドレスに同省のドメイン名(@mhlw.go.jp)**は使われていなかったとのことです。
- 5月27日～同28日に**約10万件**が送信され、その後同省によって**サーバーへのアクセスは遮断**されており、**情報の漏えい等は発生していない**としています。

### AUS便りからの所感等

- **任意のアクセス元から第三者へメールを送信するような設定(オープンリレー)になっていたか**、サーバー上の**メールアカウントへの不正ログインが行われたかのいずれかが考えられます**が、現時点で詳細な発表はありません。
- **厚労省を騙る巧妙な日本語のフィッシングメールも送信可能な状況にあった可能性があり**、その場合**SPFやDMARC**といった**送信元認証をも通過し**、**スパムと判定されにくいメールが出回っていた恐れ**もあります。
- 「go.jp」下の政府機関に属するサーバーが悪用されたことに注目が行きがちですが、**メールサーバーやクライアントPCへの侵入による不正なメール送信の問題はどの規模の組織でも起こり得る**ことであり、**アンチウイルスやUTMによる社内LANから外部への不審なメール送信の遮断**、**メールサーバー上での不正なログイン試行等の遮断設定**、および**メールアカウントの厳密な管理**がそれぞれ肝要となります。



## 厚労省サーバから「Re: Can I trust you?」10万件 迷惑メールの踏み台に

🕒 2023年05月30日 10時42分 公開

[ITmedia]

厚生労働省は5月29日、同省のサーバを経由し、第三者から約10万件の迷惑メールが送信されたと発表した。海外からの迷惑メール送信の踏み台に使われたとみている。

使われたメールアドレスは厚労省のもの(@mhlw.go.jp)ではないという。

報道関係者各位

### 迷惑メールの送信事案の発生について

このたび、厚生労働省のサーバを経由し、第三者からの迷惑メールが送信されたことが判明しました。メールは英文であり、厚生労働省とは関係がないことが記載されています。使用されているメールアドレスも厚生労働省のメールアドレスではありません。

当該メールを受け取られた方々には、深くお詫の申し上げます。  
事案の概要等は、次のとおりです。

- 概要**  
令和5年5月27日(土)20時頃から、令和5年5月28日(日)20時30分頃までの間に、厚生労働省のサーバから、迷惑メールが送信された。  
メールの件名は「Re: Can I trust you?」であり、メール本文も英文である。  
使用されているメールアドレスは厚生労働省のメールアドレス(@mhlw.go.jp)ではない。  
海外のアドレスを中心に、送信されたメールは約10万件である。  
なお、情報の漏洩等は発生していない。
- 原因**  
原因は、精査中であるが、厚生労働省のメール中継サーバを利用した海外からの電子メールの不正な中継が原因であると考えられる。
- 対応状況**  
迷惑メールの送信が行われたことを確認後、メール中継サーバへのアクセスを遮断する等必要な措置を実施した。
- 再発防止策**  
厚生労働省では、今回の事案に対し、システム運用・保守事業者へ原因究明及び再発防止の徹底を求めるとともに、引き続き、情報セキュリティ対策に取り組む。

報道発表資料より



## ●中古の検温カメラに顔画像保存…削除手順の説明なし？

<https://www.yomiuri.co.jp/national/20230524-OYT1T50072/>  
<https://togetter.com/li/2139720>

### このニュースをザックリ言うと…

- 5月24日(日本時間)、読売新聞より、新型コロナウイルス感染症対策で使用されていた**検温カメラが撮影画像が蓄積されたまま中古品として転売**されていた事例が報いられています。
- 発端は5月5日に**Twitterで報告**されたもので、メルカリで購入した2台の検温カメラを**PCIに接続**したところ、それぞれ工事現場や葬儀場で撮影されたとみられる**合計約1,700点の顔画像と体温・測定日時が記録**されている様子が確認できたとしています。
- 同新聞の記事では、カメラに**顔の撮影・記録のための操作画面はなく、取扱説明書にも言及はなかった**としており、一方で**カメラの販売元も、取材に対し「転売・廃棄は想定していなかった」と回答**しています。

### AUS便りからの所感

- 販売元のWebサイトに複数機種種の検温カメラの説明書が掲載されていますが、**顔画像の記録・管理機能がある機種でも説明書に掲載されているものとされていないものがある模様**です。
- 前述のTwitterでの報告では、本来**顔認証等によるドア施開錠機能も備えていたような機器が転用**されていた可能性が指摘されています。
- コロナ感染症の5類移行により、**検温カメラが撤去され、オークションやフリマアプリで売却されるケース**が他にもある模様で、**今後個人情報の流出に繋がる問題となり得ることが懸念**されており、いわゆる**IoT機器から検温カメラをはじめ情報を保存する機能やネットワーク機能がないように見える機器に至るまで、データの消去・設定のリセット等の機能の有無を確認**すること、そういった機能がなく情報が内部に残存する可能性があるものについては**転売せずに破壊・廃棄する等の管理体制**をとるようにしてください。



### 検温カメラに顔画像、転売品に900点保存の例も...購入者「出品者は気づいていないのでは」

2023/05/24 06:51 新型コロナウイルス

この記事をスクラップする

新型コロナウイルス対策で検温に使われたサーマルカメラから顔画像が漏えいしている。ネット上のフリーマーケットで転売された中古品では、1台で1000点近い画像が見つかった事例もある。個人データを消去しないままの転売や廃棄は個人情報保護法に抵触する恐れがあり、サーマルカメラの業界団体は「個人情報をきちんと消去してほしい」と注意を呼びかけている。

## ● Pythonライブラリ管理サービスで2要素認証の要求、2023年末までに…相次ぐコード改ざん受け

<https://news.mynavi.jp/techplus/article/20230529-2690131/>  
<https://blog.pypi.org/posts/2023-05-25-securing-pypi-with-2fa/>

### このニュースをザックリ言うと…

- 5月25日(現地時間)、プログラミング言語Pythonの**ライブラリ管理サービスPyPI**(Python Package Index)より、**ユーザーに対し2要素認証(2FA)を有効化**するよう求めると発表されました。
- PyPI上の**プロジェクトまたは組織を管理する全てのアカウント**について、**2023年末までに2FAを有効化することを義務付け**るとしています。
- PyPIの**ユーザーアカウント**を乗っ取り、**ライブラリにマルウェア等悪意のあるコードを混入させる事例が多発**していることを受けての対応としています。

### AUS便りからの所感

- ソースコード管理・共有サイト「**GitHub**」でも**同様のセキュリティ上の問題**により、**今年3月から2023年中にかけて2FA有効化の義務付け**を進めています。
- 2FAの方法として、PyPIでは**USBキー等のセキュリティデバイス**を推奨している他、複数の**スマホアプリ等が対応するワンタイムパスワード(TOTP)**も紹介しています。
- **大規模なサービスの多くが2FA(ないし多要素認証(MFA))に対応し、また今後は「Passkey」と呼ばれるパスワードレスの認証方法への対応も進む**とみられ、**強固なパスワードを設定したアカウントであっても油断することなく、2FA・MFA等パスワード以外でのアカウント保護手段を採用**するよう心掛けましょう(MFAにおいても他人による大量の不正ログインを承認してしまう**「多要素認証疲れ」等の攻撃手法**があることには**注意が必要**です)。



### Python、2023年末までに「PyPI」で2要素認証を要求

掲載日 2023/05/29 12:57

著者: 後藤大地

Pythonコミュニティは5月25日(現地時間)、「Securing PyPI accounts via Two-Factor Authentication - The Python Package Index」において、2023年末までにPyPI (Python Package Index)でプロジェクトや組織を管理しているすべてのユーザーに対し、2023年末までに二要素認証(2FA: Two-Factor Authentication)を有効化するように求めると伝えた。相次ぐセキュリティインシデントへの対応とされている。

