

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。

## ● 「ビジネスメール詐欺」は差し迫った脅威…IPAが注意喚起

<https://japan.zdnet.com/article/35124692/>  
<https://www.ipa.go.jp/security/announce/201808-bec.html>



### このニュースをザックリ言うと…

- 8月27日(日本時間)、情報処理推進機構(IPA)より、いわゆる「**ビジネスメール詐欺(BEC)**」が日本企業にとって差し迫った脅威になったとする注意喚起がなされています。

- BECによる世界的な被害は2018年5月までの累計で125億3694万8299ドル(約1兆3825億円)に上るとされており、IPAへのBECについての情報提供は2015年11月~2018年7月に計17件あり、うち5件で金銭的な被害が確認されているとのことです。

- 今回の注意喚起では、**日本語によるビジネスメール詐欺について初めて実際のメール内容の情報提供があり**、文面の一部が公開されており、こういったケースを踏まえIPAでは、

◆取引先とメール以外の方法で確認する等、取引等に関する社内規程の整備

◆普段と異なるメールに注意する

◆不審と感じた場合の組織内外での情報共有

◆ウイルスや不正アクセスへの対策をとる

等の対策を推奨しています。

### AUS便りからの所感等

- 今回公表された詐欺メールの内容では、メール送信者として企業のCEOをかたり、偽の弁護士との英文でのやりとりを添付する等の巧妙な手口をとっている様子が窺い知れ、ビジネスメール詐欺においてはターゲット企業に特化した攻撃を用意するために、**その企業と他の企業とのメールのやりとりを盗み見る等の準備段階をとる**ことも珍しくありません。

- そういった段階(即ちPCにマルウェアを感染させられる等)に入り込まれることのないよう普段からアンチウイルスやUTMによる防御を固めることも大事ですし、その他の対策も含め、IPAが今回公開しているレポートをよく読み込み、現時点でとられている手続きをより安全なものとするよう見直して頂ければ幸いです。

### ZDNet Japan

#### 「ビジネスメール詐欺」は差し迫った脅威 --IPAが注意喚起

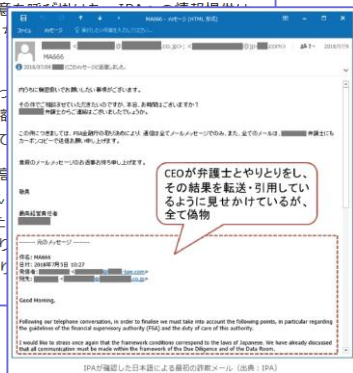
ZDNet Japan Staff 2018年08月28日 12時27分

いいね! 37 ツイート G+ B! 3 Pocket 26

情報処理推進機構(IPA)は8月27日、「ビジネスメール詐欺(BEC)」が日本企業にとって差し迫った脅威になったとして注意喚起を行いました。2015年11月~2018年7月に計17件あり、うち5件で金銭的な被害が確認されているとのことです。

BECは、以前から世界中の企業で脅威となった報告によれば、同2018年5月までの累計損失額3825億円)に上る。7月にIPAとしては初めて

このケースでは、メールの送信者として最前線の偽の弁護士存在にも触れ、受信者に機密扱いと、約5分後に「ビットコインの購入準備のた主旨のメールが送り付けられた。このやり取りは、CEOを自称する攻撃者が偽の弁護士とやり取りを引用していた。



### IPA Better Life with IT 情報処理推進機構

#### 【注意喚起】偽口座への送金を促す「ビジネスメール詐欺」の手口(続報)

~日本語メールの攻撃事例を確認、あらゆる国内企業・組織が攻撃対象となる状況に~

最終更新日: 2018年8月27日  
独立行政法人情報処理推進機構  
セキュリティセンター

IPA(独立行政法人情報処理推進機構、理事長:富田 達夫)は、「ビジネスメール詐欺」(BEC)について2017年4月に注意喚起を行いました。その後IPAへ同様の情報提供が継続しており、2018年7月には、日本語のメールによる攻撃事例を確認しました。あらゆる国内企業・組織が攻撃対象とならう状況と考えられ、新たな事例と手口を詳細に解説するとともに、「ビジネスメール詐欺」について改めて注意喚起を行います。

「ビジネスメール詐欺」は巧妙に加工したメールのやりとりにより、取引の手口です。IPAは、2017年4月、情報提供を受けた事例と手口の

(参考)【注意喚起】偽口座への送金を促す「ビジネスメール詐欺」

URL: <https://www.ipa.go.jp/security/announce/20170405/>

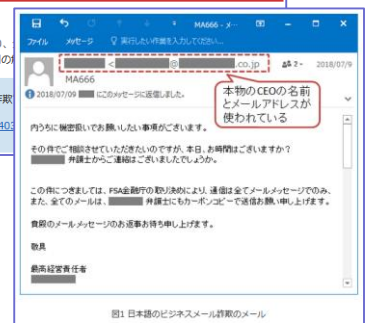


図1 日本語のビジネスメール詐欺のメール

## ●「デンソーウェーブ公式」のQRコードアプリ、位置情報の無断収集を指摘される

<http://nlab.itmedia.co.jp/nl/articles/1808/28/news115.html>



### このニュースをザックリ言うと…

- 8月11日（日本時間）、QRコードの開発元であるデンソーウェーブ社が提供していたスマートフォン向けQRコードアプリに、**特定のQRコードのスキャン時にユーザの位置情報を自動的に送信するという問題**が指摘されました。
- 問題とされたのは、デンソーウェーブ社とアララ社の共同開発による「公式QRコードリーダー“Q”」で、アララ社が提供するQRコード生成サイトにおいて生成された「アクセス解析機能付き」のQRコードをこのアプリでスキャンした場合に位置情報を送信するというものであり、**QRコード作成者は送信された位置情報を取得可能で、GPSによる詳細な情報を送信するオプションもあった**とのことでした。
- 最初の指摘の後8月27日頃にはTwitter等で話題となり、現在は位置情報収集が停止されているとのことでした。

### AUS便りからの所感等

- スマートフォンの仕様上、さすがに全くの無断でというわけではなく、インストール時には位置情報およびGPSによる情報収集について同意を求めていたとされていますが、それでも「QRコードの読み取りだけで位置情報等が送信されてしまう」ことが明確に説明されていなかったこと等に対する指摘・批判の声は少なくありません。

- **スマートフォンの各アプリのインストール時には要求される権限を確認し**、また場合によってはインストール後にも個々の権限付与を無効にする設定を行うこと、特にアップデート時にいくつもの権限追加を要求される場合にも注意を払うことが重要です。

- 今回のケースに関して言えば、QRコード読み取りアプリには非公式ながらもより機能や要求する権限が少ないシンプルなものもあり、そういった代替となるアプリへの切り替えも検討に値するでしょう。

### ねとろぼ

QRコード“読み取り”で位置情報送信の危険性? 一部アプリで物議、サービス提供社は当該機能を停止に  
特定の環境・アプリでQRコードを読み取ると、ユーザーの位置情報がコード作成者に送られる仕組みとなっていました。

1175 ツイート 65 いいね! 65 シェア 61 1 フォーマット 46 Pocket

アララが提供する、デンソーウェーブ公式の(※) QRコードリーダーアプリ「公式QRコードリーダー“Q”」に、特定の環境でコードを読み取ると、ユーザーの位置情報がコード作成者に送信される機能があることが分かり物議を醸しています。デンソーウェーブに問い合わせたところ、提供元のアララとしては、指摘を受けて現在は位置情報の提供を終了しているとのことでした。

※QRコードは1994年にデンソーが開発し、現在はデンソーウェーブが特許を保有

## ●病院で患者9000人分の個人情報入りUSBメモリ紛失

<https://headlines.yahoo.co.jp/hl?a=20180828-00010002-tuliptv-116>



### このニュースをザックリ言うと…

- 8月28日（日本時間）、富山市民病院より、同院の**患者約9000人分の個人情報が入ったUSBメモリーが紛失した**と発表されました。
- 発表によれば、USBメモリーには同院の地域医療部ふれあい地域医療センターの2014年10月～2018年7月の患者の氏名・年齢・疾患名等が記録されており、元の持ち主が別の職員に貸し出した後、8月8日に紛失が発覚したとのことでした。
- 紛失したとみられる執務エリアには外部の人が入ることが考えにくいことから、外部流出の可能性は低いとし、誤って廃棄・焼却された可能性もあるとされています。

### AUS便りからの所感等

- 紛失までの詳しい経緯としては、USBメモリーを借りた職員が8月3日に持ち主に返却しようとした際に、**不在だったため持ち主のPCの上に置いておいた**ところ、8日になって元の持ち主が紛失に気付いた、というもののようです。

- 今回の出来事を反面教師として「**返却の際は元の持ち主に必ず手渡す**」「**情報を破棄したことを記録する**」といった**ルールの徹底**、あるいはUSBメモリーを含めた機器・資産の管理を厳密に行うことも大切ですが、一方で同様の紛失事例が幾たびも発生していることを鑑みれば、USBメモリーを使ったりPC上に情報を保存したりせず、クラウド等で情報をやりとりするといった安全な情報管理手段の導入も検討すべきでしょう。

### YAHOO! JAPAN ニュース

患者9000人分 富山市民病院 個人情報含むUSBメモリーを紛失/富山

8/28(火) 19:39配信

富山市民病院の患者、およそ9000人分の個人情報が入ったUSBメモリーが紛失していたことが明らかになりました。

紛失したのは富山市民病院の患者の個人情報を保存していたUSBメモリーで、およそ9000人分以上あります。

USBメモリーには、患者の氏名や病名、退院日、退院後の医療機関名などが保存されていました。これは会議資料を作成するため職員の間で使用していたデータで、相手職員のノートパソコンの上にUSBメモリーを置いたところ、紛失したということです。

病院は今ところ個人情報がかぼちた事実は確認されていないとしています。