- VOL. 134 -
月刊 赤松事務機 通信
2026 11

IPA、自分の個人情報が漏えいした際の「対処」と「日頃の対策」をご紹介

1.はじめに

直近、国内の幅広いサービス等において、ウェブシステムに係る脆弱性の悪用、サプライチェーンを通じた侵害など、不正アクセスの被害による情報漏えい事案の公表が相次いでいます。特に大量の個人情報を取り扱うオンラインサービスやアカウントサービス等に関するシステムが不正侵入され、個人情報を含むデータが窃取される事案が複数判明しています。一部のサービスでは運転免許証の画像やクレジットカード情報などの情報が流出した事例も報告されています。
その様な状況の中、IPA情報セキュリティ安心相談窓口には、情報漏えいの対象となった一般ユーザー(消費者側)から『自分の情報が漏えいしたという連絡がきたが、どう対応すればよいか』といった相談が数多く寄せられています。
そうしたご不安をお持ちの方に向けて、二次被害のリスクを下げるための対処と、情報漏えいの対象であるかどうかに関わらず、全員が日頃から心がけていただきたい対策について解説をします。

2.情報漏えいの対象となった際に必要な対処

2.1.漏えいした情報の種別を確認する

自分が情報漏えいの対象となった場合、不安や焦りを感じることがあるかもしれません。
しかし、一旦冷静になって、自分に関するどのような情報が漏えいしたのかを以下のような方法で確認してください。
・サービス提供者からの連絡内容を確認する
・サービス提供者のウェブサイトでの案内を確認する
・サービス提供者のサポート窓口に問い合わせて確認する
その次に、漏えいした情報に対して、一つ一つ必要な対処を実施してください。

2.2.ID・パスワードが漏えいした場合

リスク

ID・パスワードが漏えいすると、悪意のある第三者に自分のアカウントへ不正ログインされるリスクがあります。ECサイトであれば勝手に商品を購入される。ネットバンキングであれば不正送金の被害に遭う、SNSであれば身に覚えない投稿をされる、などの被害が発生する可能性があります。その様な二次被害の発生を防ぐために以下を実施してください。

対処

・漏えいしたサービスにて、速やかにパスワードを変更してください。
・パスワードは長く複雑なものにしてください。
・同じパスワードを他のサービスでも使いまわしている場合は、これらのサービスについても同様にパスワードを変更してください。

2.3.クレジットカード情報が漏えいした場合

リスク

クレジットカード情報が漏えいすると、不正な決済のリスクがあります。その様な二次被害の発生を防ぐために以下の対処を実施してください。

対処

・クレジットカード会社に連絡して、不正な利用分がないかの確認、カードの利用停止や再発行について相談してください。
・当面の間、クレジットカードの利用明細に身に覚えのない決済がないか定期的に確認してください。

2.4.メールアドレス、電話番号、住所、氏名が漏えいした場合

リスク

メールアドレス、電話番号、住所、氏名等が漏えいすると、それらの情報がリスト化され、闇サイト等で販売される可能性があります。そのリストを悪用し、様々な詐欺を狙った偽メールや偽SMSが送られてくる、詐欺電話がかかってくる、不審な郵便物が届く、などの可能性があります。偽メール等の文面に漏えいした自分の氏名が記載されているといった状況も考えられます。
その様な詐欺の二次被害の発生を防ぐために以下の対処を実施してください。

対処

・突然に送られてくるメールやSMSは基本的には全て詐欺の偽メールだと考えて、無視して削除する。
・メール内のリンクをクリック/タップしないでください。
・URLからサイトにアクセスして、情報を入力したり、アプリをインストールしないでください。
・画像として埋め込まれているURLリンクにも十分に注意してください。
・不審な郵便物に注意してください（不審な着払いは受け取らない。）

2.5.運転免許証等の本人確認書類が漏えいした場合

リスク

運転免許証等の本人確認書類となる画像が漏えいした場合、悪意のある第三者がネット上の契約で、なりすましてクレジットカードやローンの契約を行い、本人確認資料として悪用される可能性があります。

対処

信用情報機関に本人申告（漏えい事実の登録）をすることで、第三者による不正利用や身に覚えのない契約の抑止に役立ちます。以下の機関へご相談いただくことを検討ください。
〇日本信用情報機構（JICC）〇株式会社シー・アイ・シー（CIC）〇全国銀行個人信用情報センター（KSC）

3.日頃の対策

情報ろうえいの対象であるかどうかに関わらず、以下の対策を全員が日頃から心がけてください。

パスワードは長く複雑にすること、使い回さないこと

パスワードの作成・管理については右記のサイトを参考にしてください。→　チョコっとプラスパスワード

多要素認証やパスキーの設定をする

各種インターネットサービスにおける不正ログイン対策として、多要素認証（SMS認証、認証アプリ、ハードウェアトークン等）やパスキーの設定が可能なサービスは積極的に利用することを推奨します。

フィッシングなどの偽メール等に注意する

・突然に送られてくるメールやSMSは基本的に全て詐欺の偽メールだと考えて、無視してください。
・メール内のリンクをクリック/タップしないでください。
・URLからサイトにアクセスして、情報を入力したり、アプリをインストールしないでください。
・画像として仕込まれているURLリンクにも十分注意してください。
・メールの真偽確認をしたい場合は、正規のサイトを調べてそこから問い合わせしてください。

情報の登録は必要最小限に

・個人情報等をサービスに登録する場合は、本当に必要なサービスに対し、必要最小限の情報に絞るように心がけてください。
・使用しなくなったアカウントは削除するように心がけてください（サービス側で情報が削除されるのかについては、サービスの利用規約やプライバシーポリシーを確認してください）。

4.相談窓口

「情報漏えいの被害にあったがどう対処すればよいか分からない。」「日頃からどのようなことに気を付ければいいのか？」など、ご不安なことやご質問があればIPA情報セキュリティ安心相談窓口に電話またはメールでご相談ください。

出典：IPA「情報セキュリティ安心相談窓口だより」https://www.ipa.go.jp/security/anshin/attention/2026/mgdayori20261026.html

赤松事務機株式会社
香川県高松市塩上町1丁目7番13号　TEL：087-833-3434　FAX：087-835-2485
URL：https：//www.akamatsu-jimuki.co.jp



赤松事務機株式会社
代表取締役　片松　保佳

『社長のつぶやき VOL.108』

11月になりました。朝晩も冷え込むようになり秋の終わりを感じます。つい先日まで半袖で過ごしたような気がするのですがあっという間に冬を感じるようになりました。季節の変わり目ですので急な温度変化で体調を崩される方も多いようです。皆様は大丈夫でしょうか？帰宅・帰社時に手洗い・うがいを励行してできるだけウイルスを寄せ付けないように注意してお過ごし下さい。

表面にIPAさんから発表されている「個人情報が漏えいした場合の対処と日頃の対策」という内容が記載されています。Timesさんでの免許証画像が含まれる漏えいやインターネット企業であるGMOグループさんでの情報漏えいなどここ数カ月ほぼ毎日企業から何かしらの情報漏えいがあったという報道が出ています。私も十数年情報セキュリティ対策に関わっていますがこれほど毎日そして数多くの有名企業で情報漏えいがあったと報道されることは今までなかったと感じています。様々な媒体で様々なインシデントが取り上げられていますが皆様はどうお感じでしょうか？メディアでは「企業として対策が不十分だった」「対策が後手後手に回っていた」など漏えい企業に対して批判ばかりする論調が目立っています。果たしてそうなのでしょうか？私は批判ばかりの論調に疑問を感じています。なぜならインターネットを使っている以上、法人も個人もサイバー攻撃を100%防ぐことは不可能だからです。これは30年以上前から変わらない事実です。どんなにお金をかけて対策してもどんなに人を教育してITリテラシーを高くしても情報セキュリティに関するインシデントは必ず起きます。言い換えればインターネットという便利なものを使うとういうことは同時に必ずそのリスクを抱えて使っているということです。インターネットは電気や水道と同様の「社会インフラ」になりました。電気や水道は国（地方自治体）や大企業が担保してくれています。残念ながらインターネットは違います。100%自己責任です。インフラでありながら責任は使用者側にあります。企業の責任を問うのは当然のことですが、報道の際には「気を付けましょう」ではなくて「インターネットの世界に個人情報を差し出すことはリスクを伴う」ということをもっと時間を割いて報道すべきです。100%攻撃を防げないのなら少しでも漏えいするリスクを下げるためにどうすればいいかを考えて対策していかなければなりません。これは法人だろうが個人だろうが関係ありません。インターネットを使用することで恩恵を受けているすべての人々がその意識を持たないと立ち行かなくなる時代が今です。最新のAIエージェント（目標に向けて自律的に行動・実行する）を組み合わせた「フロンティアAI」を駆使して攻撃者はサイバー攻撃を自動化し、攻撃にかかる工数を劇的に削減し、結果として攻撃件数は飛躍的にUPしています。ということは今後サイバー攻撃は減るどころか増え続ける一方になることも容易に予想できます。それではどうすればいいか？皆様一人ひとりが真剣に考えて対策をしないといけない時が来ているのです。「便利」と「リスク」はトレードオフの関係、すなわち「便利であればあるほどリスクは高まる」これはセキュリティの世界では常識です。

少し真剣なトーンになってしましましたが、このインターネットが溢れる世界において私にできることは皆様に「危機意識を持って生活（仕事）する」必要性を少しでも理解していただくことです。それだけでリスクはかなり下がります。セキュリティ対策において「システム」と「人」は両輪です。できることから取り組んで自分で自分を守りましょう。

お土産の紹介 ～『治一郎のバウムクーヘン』と『銀の森 プティボワ大阪限定缶』～

大阪出張のお土産は、『治一郎 バウムクーヘン』と
『銀の森　le Petit Bois（プティボワ） OSAKA Limited Edition』です。



治一郎のバウムクーヘン

ちょうど1年前にもご紹介した「治一郎のバウムクーヘン」。前回は洋菓子詰合せでしたが、今回はなんとホールのバウムクーヘン!!朝からテンション爆上がり、嬉し過ぎで拝みました。ほんと普通のバウムクーヘンとは別格。ふんわりしっとりした食感でシフォンケーキのような柔らかさ。二度目ましてですが「なに、これ、うま！」となりました。一気に全部食べられるかもだけど、1183kcal表示を見て我慢我慢…。大切にいただきました(^^♪
■1個（高さ約4㎝・直径約14.5㎝）当たり/1183kcal

銀の森　プティボワ 大阪限定缶

グランフロント大阪店でしか購入できない限定のクッキー・アソート。高級感のある黄色い缶でデザインがとても素敵です。中にはカラフルな色をした小さめなマカロンと、スノーボールクッキーなど7種類がぎっしり詰まっていてまるで宝石箱のよう。クッキーは種類によって食感も違って、色んなフレーバーを楽しめました！
■1セット95g(7品目）当たり/472kcal



弊社では、情報セキュリティ対策商品、UTM(統合脅威管理)
等の取扱いをしております！
HPでも紹介しておりますのでぜひご覧頂ければと思います!!!
対策は早目にしましょう！

ホームページはこちら ▶▶

https://akamatsu-jimuki.co.jp/

