— AUS（アルテミス・ユーザ・サポート）便り 2021/08/03号 —
https://www.artemis-jp.com

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。

●日本年金機構を騙るフィッシング…対策協議会が注意喚起

https://www.antiphishing.jp/news/alert/nenkinnet_20210802.html
https://www.nenkin.go.jp/oshirase/taisetu/2021/202108/0802mail.html

このニュースをザックリ言うと･･･

- 8月2日(日本時間)、フィッシング対策協議会より、日本年金機構を騙るフィッシングメール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「<日本年金機構>個人年金電子ファイル情報更新」等とされ、「電子年金ファイル」という架空のサービスのために個人年金情報の更新が必要と偽って、基礎年金番号・個人情報(氏名・住所・郵便番号)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)を詐取しようとする偽サイトへ誘導するとされています。

- 同2日には年金機構からも同じく注意喚起が出されており、それぞれこのような不審なメールのリンクをクリックしたり、アクセス先で情報を入力しないよう求めています。

AUS便りからの所感等

- 年金機構を騙るフィッシングは2019年にも発生しており、その際にも同じく「電子年金ファイル」のために情報を入力するよう誘導するものとなっていました(https://www.nenkin.go.jp/oshirase/taisetu/2019/201908/2019081902.html)。

- 同協議会の注意喚起で挙げられている偽サイトは「https://nenkin.go.jp.●●●●.shop/」のURLを使用しているとされていますが、今後も似たような異なるURLを使ったサイトが現れる可能性が考えられます。

- ともあれ、Webブラウザー・アンチウイルスあるいはUTMのアンチフィッシング機能を有効にし、セキュリティ関連各社・団体からの啓発情報やTwitter等における報告を検索しつつ、利用しているサービスへは予めブラウザーのブックマークに登録してアクセスする等の自衛策をとるという鉄則を確実に実行するよう推奨致します。

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

日本年金機構をかたるフィッシング (2021/08/02)

概要

日本年金機構をかたるフィッシングの報告を受けています。

メールの件名

<日本年金機構>個人年金電子ファイル情報更新

※上記以外の件名も使われている可能性があります。

[受信者のメールアドレス]様
■「電子年金ファイル」は、健康保険、厚生年金保険の手続きのみならず、個人のお客様の年金の手続きなどをインターネットで行うことができるサービスです。
■電子年金ファイルを有効にするには、以前に登録した個人年金情報を更新する必要があります。
→ご更新はこちらから
<https://nenkin.go.jp.●●●●.shop/?tokenmail=●●●●@●●●●.cn>
※正確な情報は必ず記入してください。
※こちらのメールは送信専用メールアドレスから配信されております。こちらのメールに返信いただいても、返答できませんのでご了承ください。
※このメールにお心あたりがない場合は、お手数おかけいたしますが本メールを破棄していただけますようお願いいたします。
■日本年金機構
サポート時間:平日10時～18時まで

メール文面の例

ねんきんネット

個人年金情報を更新し、電子ファイルを有効にします。（入力）

[電子年金ファイル] は、健康保険、厚生年金保険の手続きのみならず、個人のお客様の手続きなどをインターネットで行うことができるサービスです。 電子年金ファイルを有効にするには、以前に登録し個人年金情報を更新する必要があります。情報を更新していないユーザーは、その後の年金に影響を与える可能性があります。
間違った情報はフォローアップ年金に影響することに注意してください！個人年金またはクレジットカード情報が誤って入力された場合、それは不正操作とみなされます電子 個人年金ファイルを口座した後、情報を更新するために管轄に行ってください！慎重に取り扱ってください！

1 情報を更新するには、個人年金情報を入力してください

基礎年金番号

半角数字 で入力してください。
（例：7391 4682 5371 9642 8）

氏名 必須

全角文字（姓・名それぞれ23文字以内）で入力してください。
（例：年金）
姓
（例：一郎）
名

生年月日 必須

以下の元号を必ず選択の上、年月日は半角数字で入力してください。
※元号をよくご確認ください。

令和 平成 昭和 大正 明治

（例：10）
年

（例：2） （例：24）

●夏季休暇における情報セキュリティの注意喚起、NISC・IPAより発表

https://www.nisc.go.jp/active/infra/pdf/summer20210721.pdf
https://www.ipa.go.jp/security/topics/alert20210803.html

このニュースをザックリ言うと・・・

- 多くの企業・組織が長期休暇となるお盆の時期を迎えるにあたり、7月21日(日本時間)にNISC、8月3日にIPAより、情報セキュリティに関する注意喚起が出されています。

- 組織内に常駐(あるいはテレワークでネットワークに接続)する人が少なくなる、システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性を指摘、実施すべき項目をまとめています。

- また、従業員等が友人や家族と旅行に出かけた際の、SNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性についても指摘されています。

AUS便りからの所感

- IPA等セキュリティ関連団体・組織では、毎回の長期休暇の前に通常時には生じにくい様々な問題が発生し得ることを鑑み、そういった問題にも早く確実に対応することへの注意を促しており、休暇前にシステムのセキュリティ対策が十分か確認すること、休暇期間中のインシデント対応体制や関係者への連絡方法を調整すること、および休暇明けには不正アクセス・侵入等の痕跡をサーバー等のログから確認することを呼び掛けています。

- 各組織による注意喚起の骨子は、毎回大きく変わるものではありませんが、NISCの注意喚起では「東京2020オリンピック・パラリンピック」に便乗して大会関係者を騙るメールやフィッシングによる攻撃の可能性についても注意するよう呼び掛けています(「AUS便り 2021/07/27号」参照)。

- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有がそういった攻撃による被害を最小限に抑えられるために大切なことと言え、また休暇に入るまでに十分な対応が間に合わなかったとしても、明けてから点検すべきことは多く存在しますし、以後も年末年始等に備えて、準備・点検を行うよう意識して頂ければ幸いです。


夏休みにおける情報セキュリティに関する注意喚起

最終更新日：2021年8月3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

多くの人がお盆休みや夏休みなどの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりがちです。このような場合、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

最近では外出自粛の影響により、逆に家でパソコンなどを利用する時間が長くなり、ウイルス感染やネット詐欺被害のリスクが高まることも考えられます。

これらのような事態とならないよう、(1)組織のシステム管理者、(2)組織の利用者、(3)家庭の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。

■長期休暇における情報セキュリティ対策

また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

■日常的に実施すべき情報セキュリティ対策

被害に遭わないためにもこれらの対策の実施をお願いします。

●送信メールのCc: から他者のメールアドレス漏洩…原因はメール送信システムの不具合

https://www.gssc.kyoto-u.ac.jp/career/kojin_joho/

このニュースをザックリ言うと・・・

- 7月29日(日本時間)、京都大学学生総合支援センターより、同センターからメールを送信するシステムの不具合により、メールアドレスが他者に流出する事象が発生していたと発表されました。

- 同センターのキャリアサポートルームにおいて合同企業説明会に参加した企業とその担当者の氏名・メールアドレスを管理するため3月に導入されたシステムの一環でしたが、4月20日、同6月に開催予定の説明会への参加案内メールを726社742名に送信したところ、うち658名宛のメールの「Cc:」に他社のメールアドレスが最大16名分掲載されたとしています。

- この他、メールの本文にも企業名と部署・担当者名が掲載されていたとみられ、他者に読み取られる状態となっていた模様です。

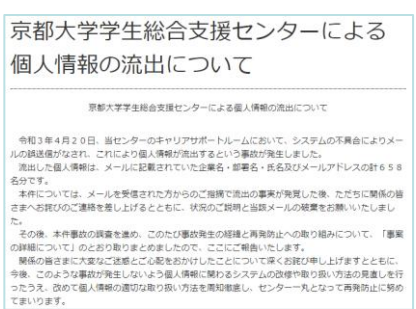
- 同センターでは再発防止策として、案内メールの送信には当該システムのメール送信機能は使用せず、本文への個人名等の記載を控える、送信されたメールにメールアドレスが表示されない「Bcc:」を用いる、メーリングリストの利用等を実施するとしています。

AUS便りからの所感

- システムが送信先の会社毎にメール送信を行い、複数名の送信先がいる会社については1人目を「To:」に、2人目以降を「Cc:」に入れる仕様としていたところ、次の会社への送信の際にCc:をクリアしておらず、以前の送信でCc:に追加されたアドレスが蓄積され、その後のメールにも残るようになっていたことが、漏洩の原因とされています。

- メール送信時、To:やCc:に第三者のメールアドレスが露呈する事故はこれまでも度々報告され、多くはメーラーによる手動設定時のミスで発生していますが、今回はWebシステムによって構築されたとみられる同報メール送信用システムでの不具合によるものであることが特徴であり、また送信先の多くは1社につき1名であったために、不具合が発覚しにくい状況にあったものと考えられます。

- これまで発生した事象を鑑みれば、同センターも行うとしている再発防止策、特にメーリングリストの使用といった、安全性を確保することを念頭に置いたシステム構築をまずは基本とすべきであり、少しでもその安全性に影響するような機能、特に不具合を含むであろう複雑な機能については導入の判断に十分注意を払い、想定される場面全てを洗い出してテストを行う必要があるでしょう。


京都大学学生総合支援センターによる個人情報の流出について

京都大学学生総合支援センターによる個人情報の流出について

令和３年４月２０日、当センターのキャリアサポートルームにおいて、システムの不具合によりメールの誤送信がなされ、これにより個人情報が流出するという事故が発生しました。

流出した個人情報は、メールに記載されていた企業名・部署名・氏名及びメールアドレスの計６５８名分です。

本件については、メールを受信された方からのご指摘で流出の事実が発覚した後、ただちに関係の皆さまへお詫びのご連絡を差し上げるとともに、状況のご説明と当該メールの破棄をお願いいたしました。

その後、本件事故の調査を進め、このたび事故発生の経緯と再発防止への取り組みについて、「事案の詳細について」のとおり取りまとめましたので、ここにご報告いたします。

関係の皆さまに大変なご迷惑とご心配をおかけしたことについて深くお詫び申し上げますとともに、今後、このような事故が発生しないよう個人情報に関わるシステムの改修や取り扱い方法の見直しを行ったうえ、改めて個人情報の適切な取り扱い方法を周知徹底し、センター一丸となって再発防止に努めてまいります。