令和6年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【初学者等向け研修】
Bコース
～リスクの理解と対策～

一般社団法人ソフトウェア協会

今日からあなたも
セキュリティの
関係者です
-事例から学ぶセキュリティ対策-

目次

- 私たちとセキュリティの関係
- セキュリティ対策とは？
- どんなリスクがある？
- 私たちができる対策
- アウェアネスを向上させよう

研修の開始前に・・・

目的

医療機関等の中でセキュリティの基礎知識を身に付けたい人に、セキュリティに興味を持てるような気付きを与えること

受講者の目標

自身もセキュリティの関係者だということを自覚し、自身や自身が所属する組織のセキュリティを守るためにすべきことを理解すること

基本的な対策を学びましょう

ユーザーができる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• パスワードの適切な設定と管理
• 不審なメールへの注意
• USBメモリなどの取扱いの注意
• 社内ネットワークへの機器接続ルールの遵守
• ソフトウェア導入時の注意
• パソコン等の画面ロック機能の設定

家庭内でできる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• 定期的なバックアップの実施
• パスワードの適切な設定と管理
• メールやショートメッセージ、SNSでの不審なURLへの注意
• 偽のセキュリティ警告に注意
• スマートデバイスのアプリや構成ファイル導入時の注意
• スマートフォン等の画面ロック機能の設定

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html

私たちとセキュリティの関係

サイバー攻撃ってどんなイメージ？

サイバー攻撃と聞くと・・・

凄いハッカーが超高度な技術で侵入！

のようなイメージがありますが、すべてがそうではありません

こんなニュースがありました

米カジノ大手ＭＧＭ・シーザーズにサイバー攻撃、大量データ流出か

［１４日 ロイター］- ハッカー集団「スキャタード・スパイダー」は１４日、米カジノ運営のＭＧＭリゾーツ・インターナショナルとシーザーズ・エンターテインメントのシステムに侵入し、６テラバイトのデータを窃取したと明らかにした。

メッセージアプリ「テレグラム」を通じてロイターの取材に応じた同集団の担当者は、窃取したデータを公開する予定はないと述べ、両社に身代金を要求したかどうかについてはコメントを避けた。

ロイターはマルウエアのサンプルをインターネット上で公開している専門家から同集団の連絡先を得た。

シーザーズとＭＧＭに窃取されたデータの量を問い合わせたが、回答はない。

シーザーズは同日、多数のロイヤルティープログラム会員の個人情報が今月７日にハッカーに窃取されたと当局に報告。ブルームバーグと米紙ウォール・ストリート・ジャーナル（ＷＳＪ）は同社が身代金を支払ったと報じた。

ＭＧＭは「サイバーセキュリティー問題」で当局と協力していると発表している。

何が起こったの？

ラスベガスの有名カジノが**ランサムウェア攻撃**に遭い、スロットや支払いシステムがすべて停止し、大量のデータが窃取されてしまった。

ランサムウェアとは？

大切なデータを勝手に暗号化し、復号と引き換えに「身代金」を要求してくるマルウェアの一種。
近年では医療機関での被害も多く、電子カルテが長期間にわたり利用できなかったり、患者情報が流出したりと、大きな被害を引き起こす危険な攻撃です。

出典：ロイター
https://jp.reuters.com/business/NT3WR7RDRBLPBOTPOFGSHP3MME-2023-09-15/

こんなニュースがありました


米カジノ大手ＭＧＭ・シーザーズにサイバー攻撃、大量データ流出か

［１４日ロイター］-ハッカー集団「スキャタード・スパイダー」は１４日、米カジノ運営のＭＧＭリゾーツ・インターナショナルとシーザーズ・エンターテインメントのシステムに侵入し、６テラバイトのデータを窃取したと明らかにした。

メッセージアプリ「テレグラム」を通じてロイターの取材に応じた同集団の担当者は、窃取したデータを公開する予定はないと述べ、両社に身代金を要求したかどうかについてはコメントを避けた。

ロイターはマルウエアのサンプルをインターネット上で公開している専門家から同集団の連絡先を得た。

シーザーズとＭＧＭに窃取されたデータの量を問い合わせたが、回答はない。

シーザーズは同日、多数のロイヤルティープログラム会員の個人情報が今月７日にハッカーに窃取されたと当局に報告。ブルームバーグと米紙ウォール・ストリート・ジャーナル（ＷＳＪ）は同社が身代金を支払ったと報じた。

ＭＧＭは「サイバーセキュリティー問題」で当局と協力していると発表している。

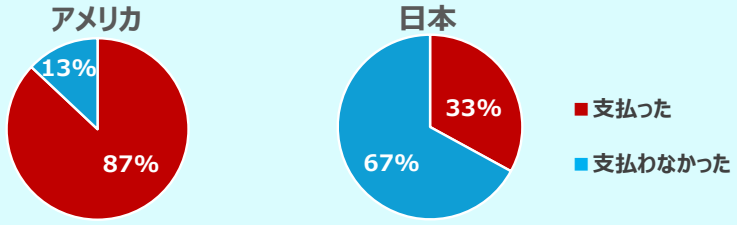
出典：ロイター
https://jp.reuters.com/business/NT3WR7RDRBLPBOTPOFGSHP3MME-2023-09-15/

システムが停止し業務に大きな影響を受けただけでなく・・・

20億の身代金を支払った！

アメリカでは、ランサムウェア被害に遭った際に身代金を支払う企業が多いが、支払ってもデータが復旧せずに追加で支払いを要求（二重恐喝）されたり、身代金を支払う組織だと思われてしまうこともあるため、身代金は基本的には支払わないことが大事。

参考：ランサムウェア感染時の身代金支払い率



出典：Proofpoint
https://www.proofpoint.com/jp/blog/threat-insight/is-it-right-to-pay-the-ransom

こんなニュースがありました


米カジノ大手ＭＧＭ・シーザーズにサイバー攻撃、大量データ流出か

［１４日ロイター］-ハッカー集団「スキャタード・スパイダー」は１４日、米カジノ運営のＭＧＭリゾーツ・インターナショナルとシーザーズ・エンターテインメントのシステムに侵入し、６テラバイトのデータを窃取したと明らかにした。

メッセージアプリ「テレグラム」を通じてロイターの取材に応じた同集団の担当者は、窃取したデータを公開する予定はないと述べ、両社に身代金を要求したかどうかについてはコメントを避けた。

ロイターはマルウエアのサンプルをインターネット上で公開している専門家から同集団の連絡先を得た。

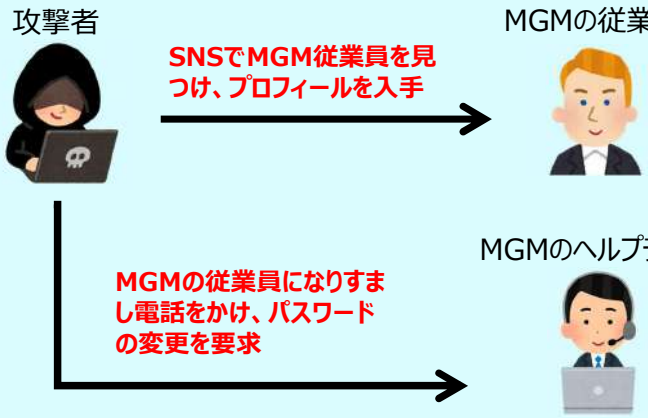
シーザーズとＭＧＭに窃取されたデータの量を問い合わせたが、回答はない。

シーザーズは同日、多数のロイヤルティープログラム会員の個人情報が今月７日にハッカーに窃取されたと当局に報告。ブルームバーグと米紙ウォール・ストリート・ジャーナル（ＷＳＪ）は同社が身代金を支払ったと報じた。

ＭＧＭは「サイバーセキュリティー問題」で当局と協力していると発表している。

出典：ロイター
https://jp.reuters.com/business/NT3WR7RDRBLPBOTPOFGSHP3MME-2023-09-15/

原因は・・・たった10分の電話！



ソーシャルエンジニアリング

ソーシャルエンジニアリングとは

なりすまし

ショルダーハッキング

トラッシング

心理的な隙やミスにつけ込み、
アナログ的な手口で情報を盗み出す手法

日本の医療機関でも・・・

医師を騙るソーシャルエンジニアリングで研修医の個人情報漏えい(新潟県)

新潟県は4月17日、県立坂町病院の事務職員が医師を騙る者に対して当該病院に勤務していた研修医の個人情報を電話で漏えいしていたことが判明したと発表した。

これは同日15時頃に、医師を騙る者から同病院に勤務していた研修医の氏名及び携帯電話番号の問い合わせがあり事務職員が口頭で回答したところ、電話終了後に不審に思った上司が電話内容について確認したところ虚偽の問い合わせであったことが判明したというもの。

漏えいした個人情報は、2014年6月以降に同病院で勤務した研修医52名の氏名及び携帯電話番号。

出典：Scan Net Security
https://scan.netsecurity.ne.jp/article/2018/04/18/40823.html?pickup_list_click2=true

何が起こったの？

病院の事務職員が、医師を騙る者からの問い合わせを電話で受け、同病院に勤務していた研修医52名分の個人情報（氏名・電話番号）を回答してしまった。

＝ なりすまし

ソーシャルエンジニアリングの被害に！

皆さんも無関係ではない！

セキュリティ対策って何をすればいいの？

セキュリティ対策って何をすればいいの

リスクから自分たち・組織を**守る**！

ために大切なことは・・・

リスクを**理解**する

リスクへ**対策**する

＋

リスクを**意識**する

どんなリスクがある？

リスクを理解しよう

業務中に関係ないサイトを見たり

個人情報を簡単に教えたり

関連する事例を紹介します

こんなニュースがありました①

Software Association of Japan

福岡徳洲会病院　個人情報など５万件余が一時閲覧可能な状態に

08月03日　19時59分

春日市にある「福岡徳洲会病院」でパソコンが一時、何者かに遠隔操作され、患者の個人情報などおよそ４４００人分、５万件余りが外部から閲覧可能な状態になっていたことがわかりました。
これまでに実際の情報流出や被害は確認されていないということですが、病院では「再発防止に努める」としています。
「福岡徳洲会病院」によりますと、ことし４月４日、職員が休憩中に業務用のパソコンで外部のホームページを閲覧していた際に画面に警告が表示され、記載された電話番号に連絡して指示に従って操作したところ、パソコンが遠隔操作に切り替わり、金銭を要求されたということです。
いわゆる「サポート詐欺」の被害にあったとみられ、後日、専門業者が調査した結果、ウイルスへの感染は確認されなかったものの、データベースに登録されていた患者の氏名や住所などのほか、職員の氏名やメールアドレスなど、最大でおよそ４４００人分、５万件余りの情報が、およそ２時間にわたって外部から閲覧可能な状態になっていたということです。
これまでのところ、実際の情報流出や被害は確認されていないということですが、病院では対象の患者などに個別に謝罪したうえで専用の相談窓口を設けて対応にあたっているということです。
福岡徳洲会病院は「ご心配をおかけしたことをおわび申し上げます。事態を重く受け止め、管理態勢を強化し再発防止に努めます」としています。

出典：NHK News Web
https://www3.nhk.or.jp/fukuoka-news/20230803/5010021438.html

何が起こったの？

サポート詐欺被害に遭い、患者の氏名や住所、職員の氏名やメアドなど最大約50,000件の情報が、一時外部から閲覧可能な状態になっていた。

サポート詐欺とは？

インターネットを利用中に、「ウイルスに感染しました」「パソコンが壊れています」といった警告画面が表示され、利用者が表示されている電話番号に焦って電話してしまうと、サポートの名目で金銭を騙し取られる詐欺のことです。

こんなニュースがありました①

Software Association of Japan

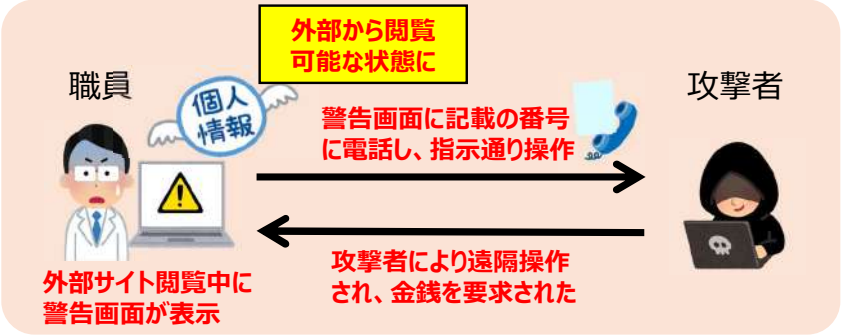
福岡徳洲会病院　個人情報など５万件余が一時閲覧可能な状態に

08月03日　19時59分

春日市にある「福岡徳洲会病院」でパソコンが一時、何者かに遠隔操作され、患者の個人情報などおよそ４４００人分、５万件余りが外部から閲覧可能な状態になっていたことがわかりました。
これまでに実際の情報流出や被害は確認されていないということですが、病院では「再発防止に努める」としています。
「福岡徳洲会病院」によりますと、ことし４月４日、職員が休憩中に業務用のパソコンで外部のホームページを閲覧していた際に画面に警告が表示され、記載された電話番号に連絡して指示に従って操作したところ、パソコンが遠隔操作に切り替わり、金銭を要求されたということです。
いわゆる「サポート詐欺」の被害にあったとみられ、後日、専門業者が調査した結果、ウイルスへの感染は確認されなかったものの、データベースに登録されていた患者の氏名や住所などのほか、職員の氏名やメールアドレスなど、最大でおよそ４４００人分、５万件余りの情報が、およそ２時間にわたって外部から閲覧可能な状態になっていたということです。
これまでのところ、実際の情報流出や被害は確認されていないということですが、病院では対象の患者などに個別に謝罪したうえで専用の相談窓口を設けて対応にあたっているということです。
福岡徳洲会病院は「ご心配をおかけしたことをおわび申し上げます。事態を重く受け止め、管理態勢を強化し再発防止に努めます」としています。

出典：NHK News Web
https://www3.nhk.or.jp/fukuoka-news/20230803/5010021438.html

原因は・・・外部サイトの閲覧！



影響は？

- 患者・職員情報最大5万件の漏えい可能性
- 患者への謝罪
- 被害患者からの相談への対応

こんなニュースがありました②

他自治体職員のなりすまし電話にだまされ個人情報を漏洩 - 鹿児島市

鹿児島市は、他自治体職員をかたる電話に職員がだまされ、住民の個人情報を漏洩したことを明らかにした。

同市によれば、9月12日に他市の職員を名乗る人物より、住民の課税に関する問い合わせの電話へ対応したが、その後同市へ電話で確認したところ、該当する職員が存在せず、なりすましであることが判明したという。

問題の電話では、課税権の有無について確認したいとし、問い合わせ対象世帯の子どもの氏名や住所、生年月日を伝えてきたため、子どもの課税権の有無について回答。さらに世帯主2人の氏名、世帯人数、居住年数などを伝えていた。

本来、他自治体から電話による照会があった場合は、折り返し電話をして回答する必要があったが、対応していなかった。同市では対象となる世帯を訪問して謝罪。警察へ相談し、対象世帯の自宅周辺におけるパトロールを依頼した。

(Security NEXT - 2023/09/14) ツイート

出典：Security NEXT
https://www.security-next.com/149454

何が起こったの？

鹿児島市は、別の自治体の職員を名乗る電話を受け、とある市民の課税権の有無を確認された際に、世帯主の氏名や世帯人数などの個人情報を話した。しかし、この電話は自治体とは関係ない不審な電話だったと判明し、情報漏えいとなってしまった。

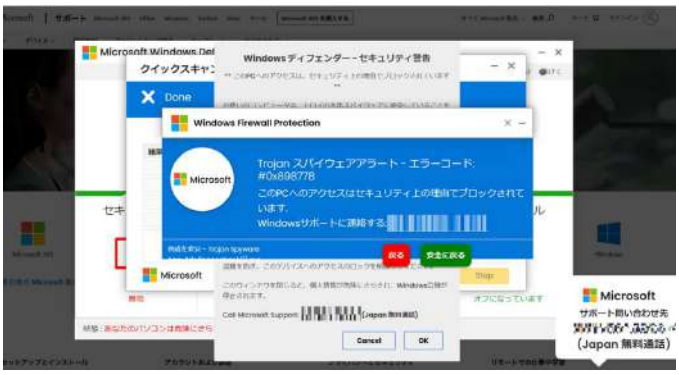
問題は・・・

折り返し対応を行わなかったこと！

本市では、他の自治体からの情報照会には折り返し対応を行うよう決められていました。

恐怖のサポート詐欺

サポート詐欺の警告画面



出典：Microsoft
https://news.microsoft.com/ja-jp/2021/01/29/210129-information/?msockid=368482ae484f6d332030966a49c46c63

900万

日本におけるサポート詐欺サイトへの年間アクセス数（2023年）

4億7000万

日本におけるサポート詐欺による被害総額（2023年）

出典：トレンドマイクロ
https://www.trendmicro.com/ja_jp/about/press-release/2024/pr-20240425-01.html

リスクを理解しよう

- 仕事に無関係なサイトは閲覧しない → 私的利用は危険！
- 組織の相談先（上司やシステム担当者）へ連絡する → すぐに報告が大事！
- 外部の人に情報を出す際は慎重に もちろんパスワードはおしえない → 教える前に確認！

リスクを理解しよう

むやみに個人情報を話したり

SNSに無断で公開したり

関連する事例を紹介します

こんなニュースがありました①

患者のカルテ写真をＳＮＳに投稿 仙台市立病院の管理栄養士

05月24日　18時17分

仙台市立病院は、患者の名前や病名が記載された電子カルテの写真を、２０代の管理栄養士がＳＮＳに投稿し、不特定多数の人が閲覧できる状態になっていたと発表しました。

発表によりますと、先月１５日ごろ、仙台市太白区の仙台市立病院に勤務する２０代の管理栄養士の女性が、患者１人の名前や病名が記載された電子カルテの写真を自身のＳＮＳに投稿していたということです。
今月１５日に、外部から匿名の電話で指摘があったことから病院が投稿に気づき、その日のうちに削除しましたが、およそ１か月間、不特定多数の人が閲覧できる状態になっていたということです。
この管理栄養士は、業務で電子カルテを閲覧できる立場にあり、病院の聞き取りに対して「業務の参考にするため、自分のスマートフォンで撮影した電子カルテの内容の写真を保存する目的でＳＮＳに投稿した」と話しているということです。
病院は患者に謝罪し、現時点で、個人情報の流出による被害は確認されていないとしています。
仙台市立病院の伊藤勝也理事は「今回の件は個人情報の扱いにあたるもので深くおわび申し上げます」と陳謝しました。
病院では、全職員に個人情報の適切な管理や取り扱いについて周知徹底を図るなど、再発防止に向けた対策を進めることにしています。

出典：NHK News Web
https://www.sankei.com/article/20201224-5FHIRXDMPJMMNCLHTL4AIHVZU4/

何が起こったの？

院内の管理栄養士が、患者1名の氏名や病名が書かれた電子カルテの写真をSNSに投稿し、不特定多数の人が閲覧できる状態になっていた。

問題は・・・患者情報を勝手に公開したこと！

患者情報＝大切な個人情報
という理解ができていなかった？

医療機関で働く人には守秘義務があり、家族であろうと患者の個人情報を教えてはいけないことを改めて確認！
※個人用のLINEを業務利用する等にも注意が必要です

こんなニュースがありました②

カルテ漏洩で損賠提訴へ　７０代女性　堺市医療センターと医師

2020/12/24 12:00

産経WEST | できごと

堺市立総合医療センター（同市西区）の女性小児科医が、職務上必要がないにも関わらず皮膚科患者のカルテ情報を閲覧し、院外に漏洩（ろうえい）したために精神的苦痛を受けたとして、患者だった大阪府内の７０代女性が、センターの運営法人と医師を相手取り、計３３０万円の損害賠償を求める訴えを大阪地裁に起こすことが２４日、分かった。２５日にも提訴する。

訴状によると、女性は顔面が腫れるといった症状が現れる「丹毒」を患い、平成２９年１２月２５日に同センターの皮膚科へ通い始めた。小児科医は、自らの職務と関係がないにも関わらず、女性の電子カルテを不正に閲覧。同月２８日、女性の病状や血液検査の結果を記した文面を、女性の長女にラインで一方的に送りつけ、カルテ情報を院外に漏らしたという。女性は長女が心配すると考え、病気の事実を伝えていなかった。

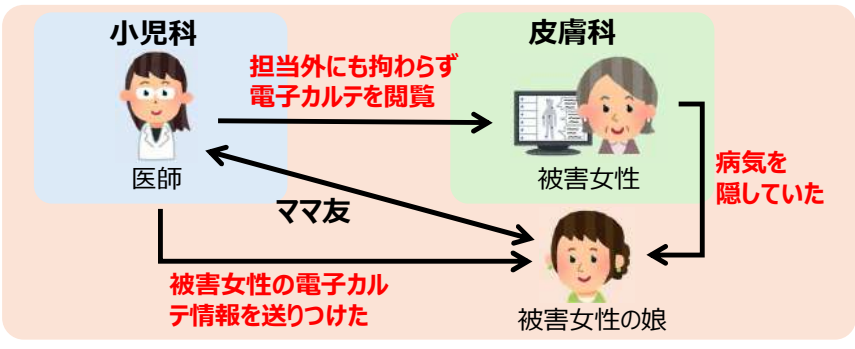
長女と小児科医の関係はいわゆる「ママ友」同士だったが、漏洩当時は疎遠になっていた。

訴状で原告側は、小児科医の行為は、守秘義務の徹底や個人情報の保護をうたった病院の倫理指針に反すると指摘。小児科医を雇用する病院側にも使用者責任があるとした。

出典：産経新聞
https://www.sankei.com/article/20201224-5FHIRXDMPJMMNCLHTL4AIHVZU4/

何が起こったの？

担当外の患者の電子カルテを不正に閲覧し、院外に漏えい。被害者が精神的苦痛を受けたとして損害賠償を求める訴えを起こした。



約5万5千円の賠償金を払うことに！

リスク理解しよう

- 患者や職員の情報は個人情報 ← 改めて注意する！
- 目的外の情報利用は罪に問われることも ← むやみに利用しない！
- 離席するときはPCの画面ロック ← 情報漏えいの防止！
- SNSなどに公開しない ← 公開する前に確認！

リスクを理解しよう

自宅PCでむやみに仕事したり

勝手に個人情報を持ち出したり

関連する事例を紹介します

こんなニュースがありました①

Software Association of Japan

北大病院 患者１７８人の個人情報入ったＵＳＢメモリー紛失

07月24日　18時41分

北海道大学病院は、勤務する臨床検査技師が患者１７８人分の氏名や病名など個人情報が記録されたＵＳＢメモリーを紛失したと発表しました。これまでのところ個人情報の流出は確認されていないということです。

北海道大学病院によりますと、先月２９日、勤務する男性の臨床検査技師が病院から持ち出したＵＳＢメモリーを紛失したことに帰宅後に気づき警察に届け出ました。
臨床検査技師はその後、探しましたが、見つからなかったために４日後に病院に報告したということです。
ＵＳＢメモリーには、動脈硬化の共同研究を行っている東京・品川区の昭和大学病院から提供された患者１７８人の氏名や病名、生年月日など個人情報が記録されていて、パスワードも設定していなかったということです。
北大病院では個人情報を許可された場所から持ち出す場合は誓約書を作成するほか、ＵＳＢメモリー本体や保存されているデータにパスワードを設定することを決めているということです。
これまでのところ個人情報の流出は確認されていないということで、北大病院は患者に経緯を説明した文書を送付し、謝罪をしたとしています。
北大病院は「患者やご家族の皆様に深くお詫び申し上げます。職員に対してより一層の厳重な個人情報の取り扱いの周知徹底を図り再発防止に努めます」とコメントしています。

出典：NHK NEWS WEB
https://www3.nhk.or.jp/sapporo-news/20230724/7000059420.html

何が起こったの？

勤務する臨床検査技師が、別病院から提供された178名の患者のデータ（氏名・病名など）が記録されたUSBを病院から持ち出し、紛失。

本病院のルール

患者データを許可された場所から持ち出すには、
・**誓約書を作成**すること
・本体やデータに**パスワードを設定**すること

問題は・・・

・ルールを守らずに持ち出したこと！
・紛失から4日後に報告したこと！

こんなパターンも・・・

Software Association of Japan

富士宮市　病院搬送者の個人情報　報道機関などに誤送信

08月21日　17時43分

富士宮市は、病院に搬送された市民１００人分の氏名や住所それに搬送先の病院名などの個人情報が書かれた資料を報道機関などに誤ってメールで送ったと発表しました。

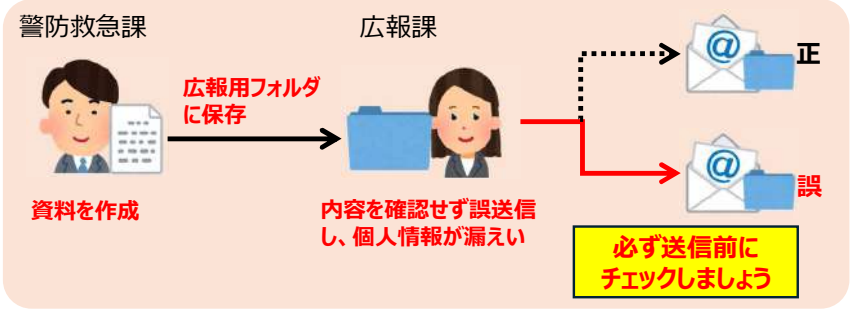
誤送信されたのは、７月、富士宮市内で救急搬送された市民１００人分の氏名と住所、生年月日それに事故の種別と搬送先の病院名などです。
市によりますと、８月１４日、救急搬送の発生件数の７月分のデータをメールで送信する際、元データが書かれた資料を誤ってメールに添付したまま送信したということです。
この資料は警防救急課が作成した文書で、広報用のフォルダに登録され、広報課の職員も内容を確認しないままメールを送信したということです。
資料は報道機関や市公認の情報発信の団体、それに市の地域おこし協力隊など２０か所に誤送信されたもののこれまでに悪用されたという報告はないとしています。
市は個人情報が漏えいした１００人に対し電話などで謝罪しました。
再発防止策として広報用のメールを送信する際は複数の職員で内容をチェックするとしています。
富士宮市の須藤秀忠市長は「情報漏洩事故により多大なるご迷惑とご心配をおかけし、大変申し訳ありません。事態を重く受け止め、再発防止を徹底してまいります」とコメントしています。

出典：NHK NEWS WEB
https://www3.nhk.or.jp/lnews/shizuoka/20230821/3030021278.html

何が起こったの？

市内で緊急搬送された100人の個人情報（氏名・住所・病院名など）が書かれた資料を、誤って報道機関など20か所にメールで送信した。

原因は・・・職員の確認不足！



リスクを理解しよう

- データを勝手に持ち出さない → ルールを確認しよう！
- 職場PCにウイルスを持ち込む可能性 → 基本的に私用PCで仕事しない！
- すぐに上司やシステム担当者に報告 → 報告が大事！
- 情報漏えいで損害賠償の可能性 → 情報漏えいの重大さを知ろう！

リスクを理解しよう

情報セキュリティ事故というと

弱点
システムの脆弱性が原因と思われがちですが・・・
人の脆弱性が原因のものも多い！

リスクを理解し、自身の脆弱性を減らしてください

セキュリティ対策って何をすればいいの

リスクから自分たち・組織を守る！

ために大切なことは・・・

リスクを**理解**する

リスクへ**対策**する

＋

リスクを**意識**する

わたしたちができる対策

私たちにできること

経営者

システム管理者

立場によってできることは変わります

システム利用者

家庭内

それぞれの役割

ユーザーができる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• パスワードの適切な設定と管理
• 不審なメールへの注意
• USBメモリなどの取扱いの注意
• 社内ネットワークへの機器接続ルールの遵守
• ソフトウェア導入時の注意
• パソコン等の画面ロック機能の設定

修正プログラムの適用、つまりアップデートを放置すると、セキュリティ上の欠陥である脆弱性が残り、外部からサイバー攻撃を受けてしまうリスクがあります。

PCやソフトウェアのアップデートを行い、最新の状態を保ちましょう

新しいウイルスは日々発生しているため、パターンファイル（ウイルスの特徴を記録したファイル）を更新していないと、新しいウイルスを検知できなくなるリスクがあります。

PCやスマホのセキュリティソフトのパターンファイルを最新の状態に保ちましょう

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html

それぞれの役割

ユーザーができる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• パスワードの適切な設定と管理
• 不審なメールへの注意
• USBメモリなどの取扱いの注意
• 社内ネットワークへの機器接続ルールの遵守
• ソフトウェア導入時の注意
• パソコン等の画面ロック機能の設定

簡単なパスワードを利用していると、不正アクセスを受けてしまったり、また、パスワードを使い回していると、漏えいした際に同じパスワードを利用しているすべてのシステムにログインされるリスクがあります。

パスワードを長く複雑に設定し、使い回しを避けましょう

不審メールに記載されたURLから偽のサイトに誘導され情報を窃取されたり、添付ファイルからマルウェアに感染してしまうリスクがあります。

少しでも怪しいと感じたメールのURLや添付ファイルは絶対に開かないようにしましょう

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html

それぞれの役割

ユーザーができる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• パスワードの適切な設定と管理
• 不審なメールへの注意
• USBメモリなどの取扱いの注意
• 社内ネットワークへの機器接続ルールの遵守
• ソフトウェア導入時の注意
• パソコン等の画面ロック機能の設定

ルールを守らずにUSBメモリを利用し情報を持ち出すと、紛失・盗難時に大切な個人情報が漏えいしてしまうリスクがあります。

USBメモリの利用ルールを確認し、できるだけ私物USBの利用は避けましょう

私物のPCやUSBがウイルスに感染していた場合、組織のネットワークに接続することでウイルスを持ち込んでしまうリスクがあります。

私物のPCやUSBをむやみに組織のネットワークに接続しないようにしましょう

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html

それぞれの役割

ユーザーができる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• パスワードの適切な設定と管理
• 不審なメールへの注意
• USBメモリなどの取扱いの注意
• 社内ネットワークへの機器接続ルールの遵守
• ソフトウェア導入時の注意
• パソコン等の画面ロック機能の設定

職場PCで勝手にソフトウェアをインストールすると、セキュリティ的に問題のあるソフト等をインストールしてしまうリスクがあります。

組織のPCやスマートフォンに勝手にソフトウェアをインストールしないようにしましょう

PCの画面を開いたまま離席したり、ロックをかけていないスマートフォンを放置すると、第三者に情報を閲覧されたり操作されてしまうリスクがあります。

PCやスマートフォンには画面ロックを設定し、席を離れる際には画面ロックをかけましょう

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html

それぞれの役割

家庭内でできる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• 定期的なバックアップの実施
• パスワードの適切な設定と管理
• メールやショートメッセージ、SNSでの不審なURLへの注意
• 偽のセキュリティ警告に注意
• スマートデバイスのアプリや構成ファイル導入時の注意
• スマートフォン等の画面ロック機能の設定

システムの不具合やウイルスによりPCやスマートフォン内のデータが破損してしまうリスクがあります。

重要なデータは、定期的にバックアップを行いましょう

不審メールやショートメッセージ、SNS上に記載されたURLから偽のサイトに誘導され情報を窃取されたり、添付ファイルからマルウェアに感染してしまうリスクがあります。

メールだけでなく、ショートメッセージやSNS上のURLにも注意しましょう

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html

それぞれの役割

家庭内でできる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• 定期的なバックアップの実施
• パスワードの適切な設定と管理
• メールやショートメッセージ、SNSでの不審なURLへの注意
• 偽のセキュリティ警告に注意
• スマートデバイスのアプリや構成ファイル導入時の注意
• スマートフォン等の画面ロック機能の設定

偽の警告画面が表示され、メッセージに従って電話などしてしまうと、端末を遠隔操作されたり、高額なサポート契約へ誘導されるリスクがあります。

警告画面が表示された場合は、焦らず冷静に対応しましょう

公式アプリ以外から配信されているアプリには、危険なものも含まれていて、それをインストールしてしまうと端末に不正な設定をされてしまうリスクがあります。

アプリのインストールは公式マーケットや信頼できる場所から行いましょう

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html

それぞれの役割

組織内では利用者だとしても・・・

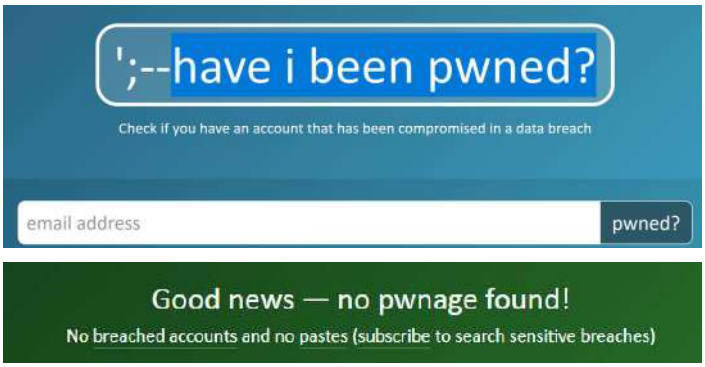
家庭内ではあなたも管理者！

ご家庭のセキュリティを管理しましょう

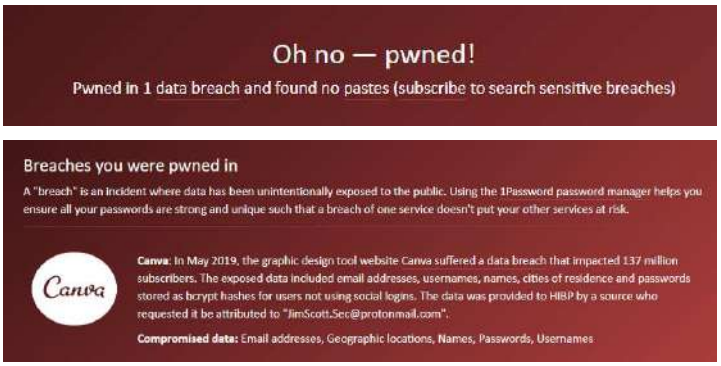
（参考）あなたのメールアドレスは大丈夫？

「*have i been pwned?*」

https://haveibeenpwned.com/



アカウント（Eメールアドレス）が
漏えいしているかどうか確認できるサイト



どこで漏えいしているかを教えてくれる

**漏えいしていた場合は、まずは漏えいしたアカウント（Eメールアドレス）と
紐づくパスワードを変更しましょう！**

（参考）あなたの家のIoT機器は大丈夫？

「*am I infected?*」

https://amii.ynu.codes/

ご家庭のルーターやウェブカメラ等の
マルウェア感染と脆弱性を診断できるサービス

**感染が疑われる場合は、まずはルーターを再起動しましょう！
また、感染防止のためにファームウェア※を最新の状態に保ちましょう！**
※ファームウェアとは、電子機器に組み込まれたハードウェアを動かすためのソフトウェアです

セキュリティ対策って何をすればいいの

リスクから自分たち・組織を守る！
ために大切なことは・・・

リスクを理解する

リスクへ対策する

＋ リスクを意識する

アウェアネスを高める

アウェアネスとは？

アウェアネス（Awareness）＝自覚、意識

セキュリティ上のリスク・対策を意識すること

アウェアネスを高めることで、

意識することで、リスクを理解し、対策ができる！

アウェアネスとは？

新しく家を建てる

家の情報をたくさん調べる

NISAを始める

株価や為替が気になってくる

アウェアネスとは？

セキュリティを意識する

見えなかった**リスク**が見えてくる
知らなかった**情報**が入ってくる

意識しているからこそ目についたり、知ろうとする

アウェアネスとリテラシーの違い

アウェアネス	ITリテラシー
セキュリティの上のリスクを理解し、リスクに対しどのような対処ができるのかを意識すること。	情報システムを守るために必要な情報セキュリティの基本を理解し、実践すること。
意識の向上	**知識の習得**

アウェアネスを高めよう

アウェアネスを高めるには・・

リスクに気づきリスクを意識すること！

行動が変わる！

意識すると行動が変わる

インフルエンザを「意識する」と・・・

インフルエンザに罹りたくない！

- マスクの利用
- 手洗いうがい
- 予防接種

みえないウイルスも
意識することで
リスクがみえるように

行動が変わる！

健康を「意識する」と・・・

いつまでも健康でいたい！

- 食生活の改善
- 体調管理
- 情報の収集

意識すると行動が変わる

セキュリティを「意識する」と・・・

セキュリティ事故の被害に遭いたくない！

情報収集

パスワードの管理

不審メールへの注意

アップデートの実施

行　動　を　変　え　る

セキュリティを「意識」して、安全に利用する！

意識すると行動が変わる

意識すると行動に繋がるけど・・・

強制されたり文句を言われると嫌になる！

意識すると行動が変わる

手洗いの仕方が悪かったんじゃない？

意識が足りないからだ

風邪をひかないように「意識」していても・・・
風邪をひくときはもちろんあります

意識している人を否定しない！

意識すると行動が変わる

専門家にならなくて良い！

消防士になる

火事を起こさない工夫
消火器の使い方

アウェアネスを高めよう

アウェアネスを高めることで、リスクを理解し、リスクへの対策を行ってください！

まとめ

まとめ

事例・事故から学ぶセキュリティ対策！

リスクを理解する

- 人の脆弱性が原因で起こるセキュリティ事故は多い
- どのようなリスクがあるのかをしっかりと理解し行動することで、自身の脆弱性をなくそう

リスクへ対策する

- リスクを理解したうえで、自身の立場でできる、やらなくてはいけない対策の必要性を理解し、しっかりと取り組む

リスクを意識する

- アウェアネスとはリスク・対策を意識すること
- 意識することで、見えなかったリスクや情報がみえてくる＝リスクを理解し対策ができる

セキュリティ対策状況を確認しましょう

ユーザーができる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• パスワードの適切な設定と管理
• 不審なメールへの注意
• USBメモリなどの取扱いの注意
• 社内ネットワークへの機器接続ルールの遵守
• ソフトウェア導入時の注意
• パソコン等の画面ロック機能の設定

家庭内でできる 日常におけるセキュリティ対策
• 修正プログラムの適用
• セキュリティソフトの導入および定義ファイルの最新化
• 定期的なバックアップの実施
• パスワードの適切な設定と管理
• メールやショートメッセージ、SNSでの不審なURLへの注意
• 偽のセキュリティ警告に注意
• スマートデバイスのアプリや構成ファイル導入時の注意
• スマートフォン等の画面ロック機能の設定

出典：IPA
https://www.ipa.go.jp/security/anshin/measures/everyday.html