今日から考える サイバーセキュリティ

～無関心？でも無関係ではいられないセキュリティ～

令和5年度厚生労働省セキュリティ研修事業医療従事者・初学者向けコンテンツ
（作成：一般社団法人ソフトウェア協会）

今回のお話

- セキュリティって私たちに関係あるの？
- セキュリティ対策って何をすればいいの？
- 私たちにできること
- アウェアネスをたかめよう

基本的な対策を学びましょう

医療従事者・一般のシステム利用者向け サイバーセキュリティ対策チェックリスト

NO	チェック項目	チェック欄（○or×）
1	業務に不要なWEBサイトへのアクセスをしていないか	
2	システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っているか	
3	利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン（画面が他人から見えないようにするために、操作しないまま一定の時間が経つと自動的にパスワード付きスクリーンセーバーが起動するようにしたり、または自動的にログオフするように設定すること）等の対策を実施しているか	
4	従業員個人のUSBメモリ等の外部媒体を使用していないか又は業務上、外部媒体の使用が必要な場合は事前に申請し、医療機関が管理している外部媒体を使用しているか	
5	ソーシャルエンジニアリング（人の心理的・社会的な弱点や盲点をついて入手する手法）について理解し、安易にID・パスワードや個人情報等を外部提供しないようにしているか（本人確認やリンク先やメールアドレスの再確認等をした上で回答する等）	
6	見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意しているか（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）	
7	メール送信前にメール送信確認画面を再度表示し確認したり、メールの遅延送信機能（送信ボタンを押しても、すぐに送信されず、任意の時間の経過後メール送信される機能。メール送信の取消等が可能となり、誤送信の防止に有用となる）等を活用し、メールの誤送信を防止しているか	
8	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護しているか なおパスワードは別手段で知らせる、あるいは事前に取り決めておく等の手法とセットで行うこと	
9	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関内の情報システム部門または担当者に確認したり、事前に情報システム部門より、対応方法の連絡がある場合は指示に従って処理をしているか	
10	患者の情報について目的外使用をしていないか	

医療情報システムの安全管理に関するガイドライン医療機関のサイバーセキュリティ対策チェックリスト
https://www.mhlw.go.jp/content/10808000/000936167.pdf

セキュリティって
私たちに関係あるの

サイバー攻撃ってどんなイメージ？

ものすごいハッカー

超高度な技術で侵入

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

Zeba Siddiqui

2023年9月15日 午前 10:44 GMT+9・11日前更新

９月１４日、ハッカー集団「スキャタード・スパイダー」は、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盗んだと明らかにした。写真はラスベガスで１３日撮影（２０２３年　ロイター／Bridget Bennett）

ＭＧＭリゾーツにハッキング、スロットマシン動かず飲み物も現金払い

Chris Palmeri、Katrina Manson

2023年9月13日 16:11 JST

- ハッカーの身元は不明、攻撃者の動機も分かっていない
- ベラージオとコスモポリタンのほとんどの客はハッキングに気付かず

マリナ・ロペス氏は12
ながら、同施設の親会社で
げでひどい目に遭ったと

レストランは現金しか使えず、プールサイドのバーも同じだった。同氏は前日も、カクテル「マルガリータ」の代金を現金で支払わなければならなかった。スロットマシンで遊ばうとする客にはさらに残念なことに、多くのマシンが動いていなかった。

ＭＧＭグランドに泊まったロペス氏は、「遊びに来た人たちは、遊べずに帰っていった」と語った。

20億円の身代金

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

侵入はたった一本の電話、しかも10分で

- SNSで職場や仕事の情報を入手
- 電話でメールの添付ファイルを開かせる

ソーシャルエンジニアリング

日本にはカジノはありませんが・・・

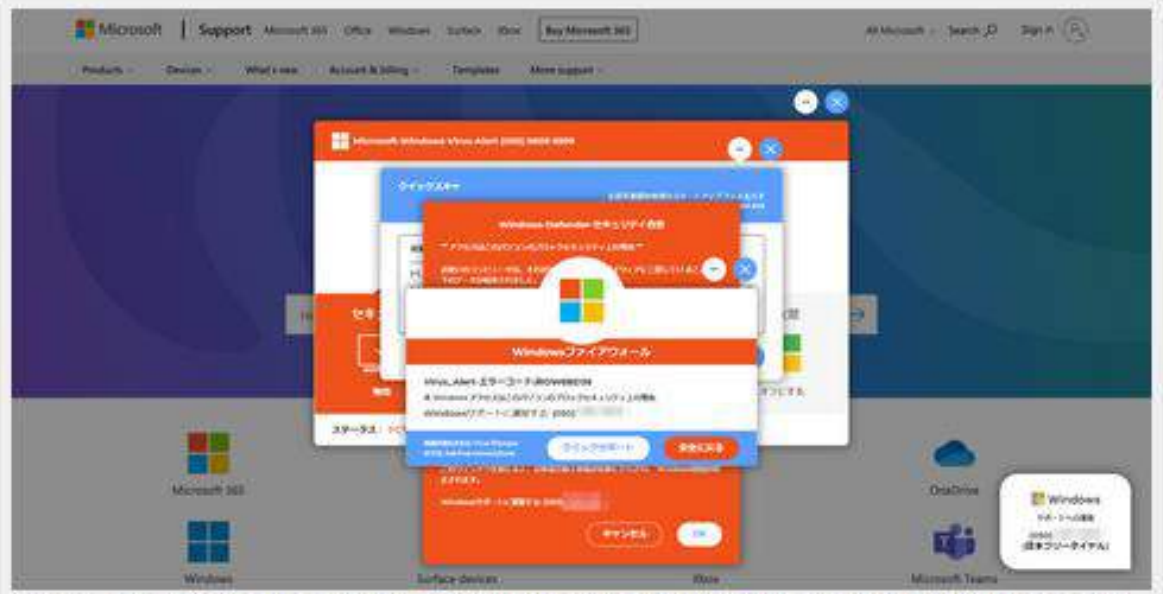
勤務中ニュースサイトを閲覧、サポート詐欺で 104 人分個人情報流出の可能性

公益財団法人福岡市緑のまちづくり協会は9月1日、同協会の公園管理事務所（東平尾公園内）での個人情報流出について発表した。

出典：ScanNetSecurity
https://scan.netsecurity.ne.jp/article/2023/09/11/49930.html

日本にはカジノはありませんが・・・

「システムが壊れている」として、偽プログラムを販売しようとする詐欺サイトの例



ウイルスに感染していると脅し、記載の電話番号に電話させようとする詐欺サイトの例

出典:Internet Watch
https://internet.watch.impress.co.jp/docs/column/dlis/1372031.html

日本にはカジノはありませんが・・・

国立医療機関から被験者情報が流出か、ウイルス感染の偽警告に従い乗っ取られる

テレワーク中の職員が偽警告に従う

国立がん研究センター東病院は2022年3月25日、同病院が研究代表と研究事務局を担当する臨床研究の被験者情報が流出した可能性があると発表した。

出典：日経XTECH
https://xtech.nikkei.com/atcl/nxt/column/18/00598/121500159/

病院ＰＣに「警告」、職員が「サポート窓口」へ電話すると…患者情報流出か

2023/08/05 09:05

この記事をスクラップする

福岡徳洲会病院（福岡県春日市）が４月に不正アクセスを受け、最大で約４万９０００件の患者情報が流出した可能性があることがわかった。現時点で、情報の悪用は確認されておらず、業務にも支障はないという。

同病院によると、流出した可能性があるのは、患者の氏名や病名、投薬内容など。４月４日、病院のパソコン画面に警告メッセージが出たため、職員がサポート窓口として表示された番号に電話。相手の指示通りにパソコンを操作したところ、データベースに保存していた情報が、外部から一時閲覧できる状態になったという。

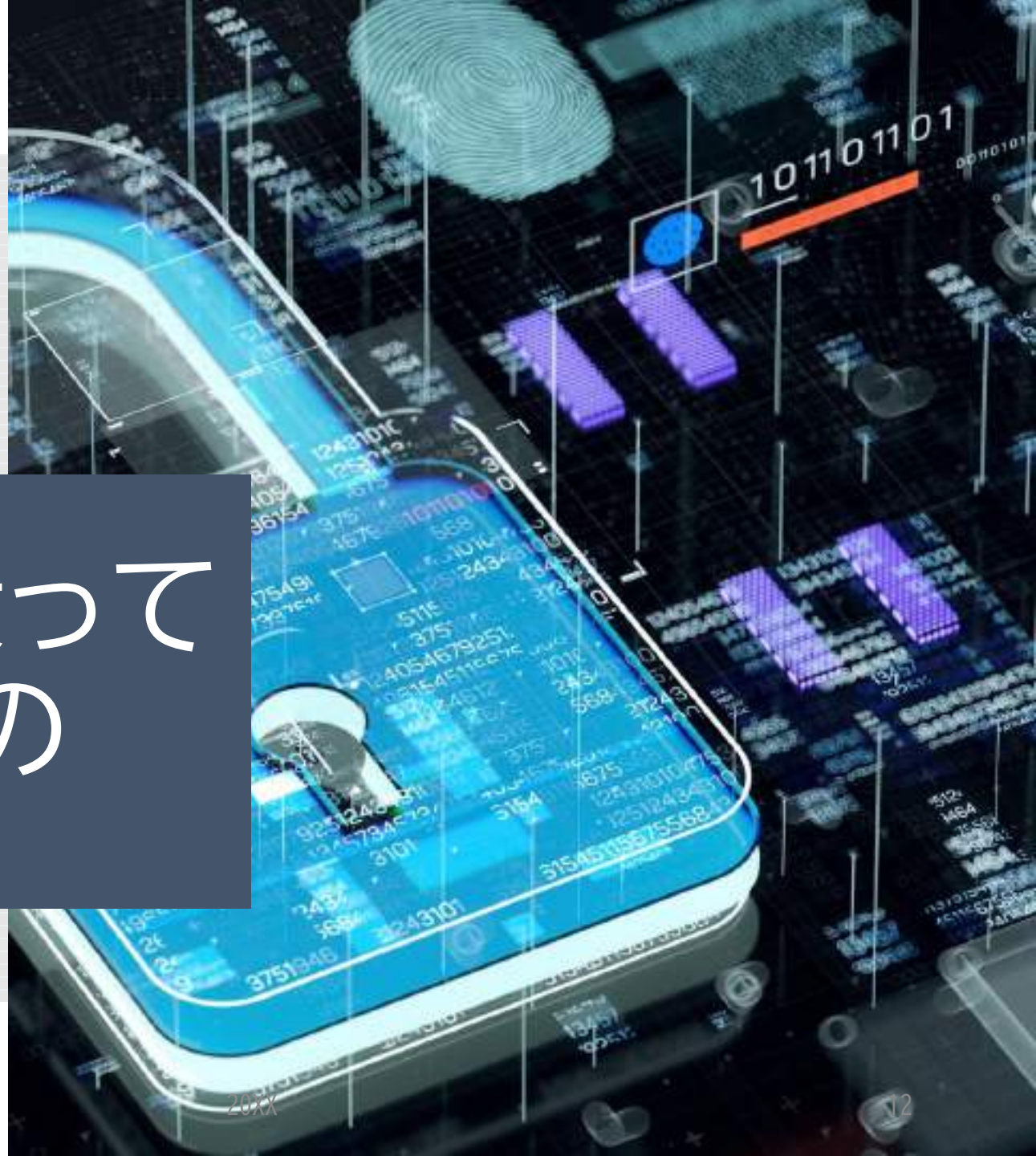
出典：読売新聞オンライン
https://www.yomiuri.co.jp/local/kyushu/news/20230804-OYTNT50146/

人が侵入の入り口

関心がなかったとしても

だれも無関係ではいられない

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

リスクを知り

リスクを管理する

リスクを知ろう

今日って雨ふるんだっけ？

変なメッセージでた！

リスクを知ろう

勤務中ニュースサイトを閲覧、サポート詐欺で 104 人分個人情報流出の可能性

公益財団法人福岡市緑のまちづくり協会は9月1日、同協会の公園管理事務所（東平尾公園内）での個人情報流出について発表した。

出典:ScanNetSecurity
https://scan.netsecurity.ne.jp/article/2023/09/11/49930.html

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

リスクを知ろう

サポート詐欺で職員宅PCが遠隔操作 - 厚生中央病院

全国土木建築国民健康保険組合が運営する厚生中央病院は、職員がサポート詐欺に遭い、パソコンを遠隔から操作されたことを明らかにした。個人情報流出が生じていないか影響について調査している。

同院によれば、偽のセキュリティ警告画面で不安を煽り、サポート窓口などと称した電話番号へ連絡させ、遠隔操作ソフトをインストールさせたり金銭を詐取する「サポート詐欺」に同院職員が騙され、自宅で使用するパソコンを遠隔操作されたもの。同端末には、個人情報が保存されたUSBメモリが接続されていた。

USBメモリには、2020年2月20日から2021年9月17日にかけて同院で診察した新型コロナウイルス感染症に関連する患者771人分の診療内容のほか、2011年3月2日から2013年12月25日に職員の感染対策として行った510人分の検査結果が保存されていた。

同院では個人情報保護委員会へ報告。データをコピーされたり、閲覧された形跡は確認されていないが、要配慮個人情報が含まれており、同院では引き続き情報流出などの影響について調査を進めている。

（Security NEXT - 2023/09/22 ）

出典：Security NEXT
https://www.security-next.com/149623

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 ）

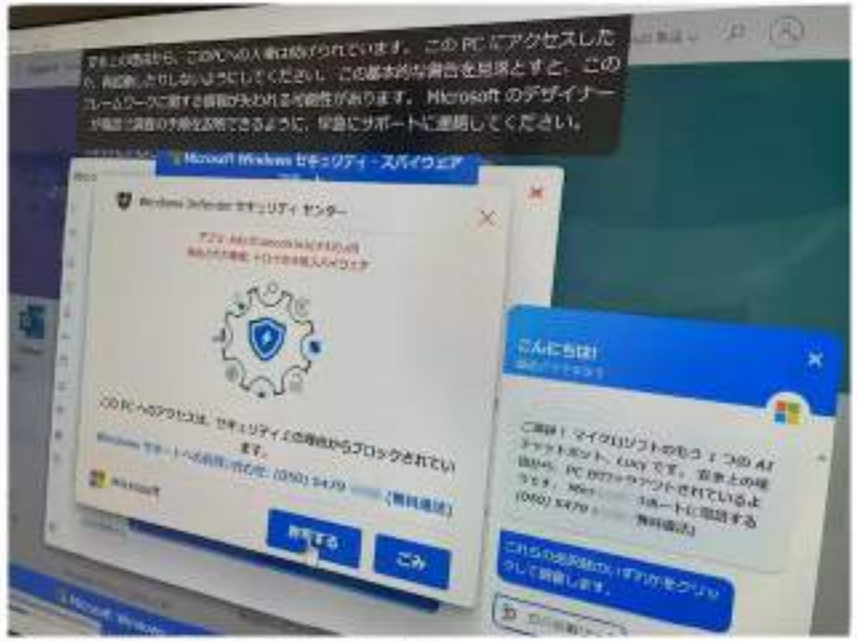
出典：Security NEXT
https://www.security-next.com/149454

ちなみにかなり被害出てます

PCウイルス駆除、サポート詐欺注意　2年半で被害4億円

社会・調査

2023年9月28日 18:31



マイクロソフトを装った偽の警告画面表示（28日、消費者庁）

マイクロソフトを装った偽の警告をパソコンの画面上に表示し、ウイルスの駆除を行うなどと称して多額の金銭を支払わせる被害が相次いでいるとして、消費者庁は28日、消費者安全法に基づく注意喚起を行った。被害額は今年8月までの2年半で4億円を超える。同庁は警告を見たらパソコンの再起動を徹底することなどを呼びかけている。

出典：日本経済新聞
https://www.nikkei.com/article/DGXZQOUE286090Y3A920C2000000/

- 広告をクリックで出たりする
- 400万円支払った人も

リスクを知ろう

- 仕事に関係ないサイトはみない
- おかしいな？と思ったら組織内の相談先へ連絡する
- 外部の人に情報を出す際は確認をもちろんパスワードはおしえない

リスクを知ろう

ここだけの話なんだけど

有名人きてるよーー

リスクを知ろう

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

カルテ情報が記されたラインの画面（原告の長女提供）※一部画像処理しています※

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。

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

殺人被害者のカルテ、業務外で閲覧か　新潟大病院が調査

2020年1月29日 14時18分

新潟大学医歯学総合病院＝新潟市中央区旭町通1番町

新潟市の新潟大学医歯学総合病院で、殺人事件で亡くなった女性（当時20）の電子カルテに院内からアクセスがあったことが病院への取材でわかった。救急治療や司法解剖といった業務とは直接の関係がない部署からで業務外のアクセスの疑いがあり、病院は閲覧の必要があったかどうか調べる方針。

病院によると、アクセスが確認されたのは、昨年11月にJR新潟駅前で刺殺された女性の電子カルテ。同月末から12月初旬ごろにカルテの閲覧履歴を調べて発覚した。

病院では医師、看護師ら医療職員や一部の事務職員に、電子カルテへのアクセス権限があるが、内規で業務外のカルテ閲覧を禁じている。

出典：朝日新聞デジタル
https://www.asahi.com/articles/ASN1Y4DQWN1YUOHB001.html

リスクを知ろう

大学病院の委託先が情報漏えい、社員は自主退職 業務委託契約も終了

近畿大学病院は2月2日、受付業務を委託する株式会社エヌジェーシーの社員による患者情報の漏えいについて発表した。

近畿大学病院は2月2日、受付業務を委託する株式会社エヌジェーシーの社員による患者情報の漏えいについて発表した。

これは2022年11月5日に、受付業務を委託するエヌジェーシーの元社員A氏が、同院を受診した患者B氏の診療情報を記載した電子カルテを表示したパソコン画面を私用スマートフォンで動画撮影し、SNSを通じて共通の友人C氏へ送信したというもの。患者B氏が友人C氏から動画の存在を聞き、11月7日に同院に抗議したことで発覚した。

トップページ

リリース（近畿大学病院で発生した診療情報の流出事案について）

リリース（事案の概要）

リリース（再発防止策）

リリース（個人情報漏洩に関するお詫び）

出典:ScanNetSecurity
https://scan.netsecurity.ne.jp/article/2023/02/24/48964.html

リスクを知ろう

- 患者さんの情報は個人情報
- 目的外使用は罪に問われることも
- 離席するときはPCの画面ロック
- SNSなどに書き込まない

リスクを知ろう

あー仕事おわんねー

家で続きやろう！

リスクを知ろう

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

持ち出した患者情報が医師宅で盗難 - 神奈川県立こども医療センター

神奈川県立こども医療センターは、医師によって許可なく持ち出された患者情報が盗難被害に遭ったことを明らかにした。

同センターによれば、9月2日から翌3日未明にかけて、医師の自宅で盗難事件が発生し、USBメモリを入れた鞄が被害に遭ったもの。就寝前に鞄の存在を確認していたが、起床後に鞄がないことへ気付いたという。

問題のUSBメモリには、患者20人に関するカルテの情報が保存されており、氏名、生年月日、性別、病歴、治療経過などが含まれる。同医師が病院の許可なく持ち帰っていた。

同センターでは対象となる患者と家族に対し、書面を通じて謝罪することにくわえ、担当医師や責任者となる医師などが直接説明や謝罪も行う。

また院内のネットワークに接続する端末については、一部業務を除いてUSBメモリに個人情報を保存できないようシステムの設定を変更するとしている。

（Security NEXT - 2023/09/08 ）

出典:Security NEXT
https://www.security-next.com/149256

リスクを知ろう

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

企業の健診結果を別企業へメールで誤送信 - 日大病院

日本大学病院は、健診センターを受診した企業の従業員の健診結果を、別の企業へ誤ってメール送信したことを明らかにした。

同院によれば、8月23日、健診センターで健診を受けた企業従業員14人分の健診結果データを、別の企業宛てのメールに添付して送信するミスが発生したもの。担当者が健診結果のCSVデータを作成した際に異なるデータを作成してしまったという。

誤送信先からの指摘で判明。誤送信したデータの削除を依頼した。データは削除済みであることを確認しており、誤送信先以外への流出は確認されていない。

同院では、対象となる受診者に対し説明と謝罪の書面を送付。あわせて個人情報保護委員会と文部科学省へ報告を行っている。

（Security NEXT - 2023/09/28 ）

出典:Security NEXT
https://www.security-next.com/149724

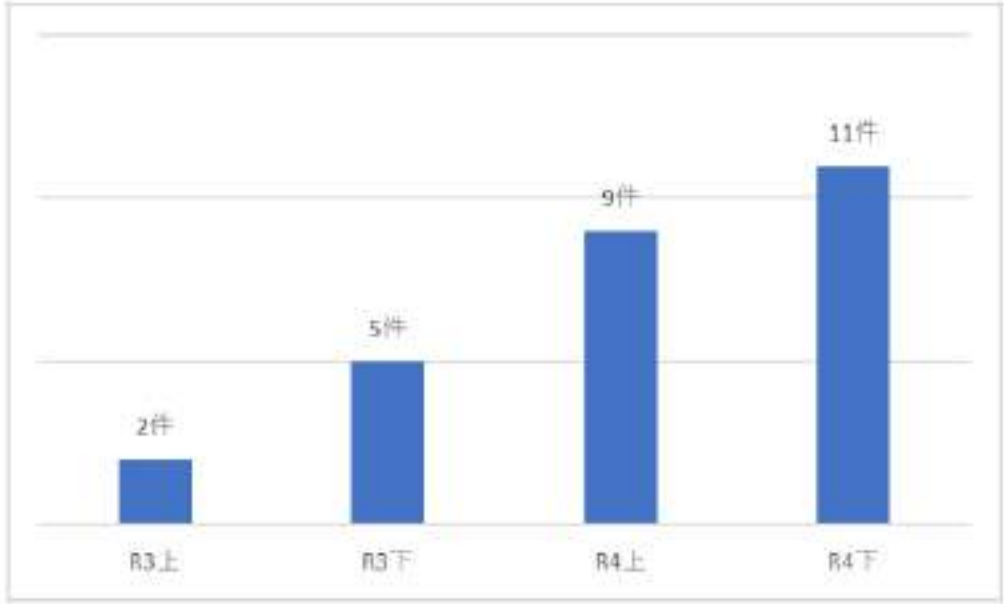
リスクを知ろう

- データを勝手に持ち出さない
- 紛失や盗難だけでなく自宅PCから
  職場のPCにウイルスを持ち込む可能性
- 情報漏えいで損害賠償も

リスクを知ろう

うちは大丈夫！ より うちは大丈夫？

- システムの脆弱性
- 人の脆弱性



医療・福祉分野におけるランサムウェア被害件数

出典：警察庁
https://www.npa.go.jp/bureau/cyber/pdf/20230406_2.pdf

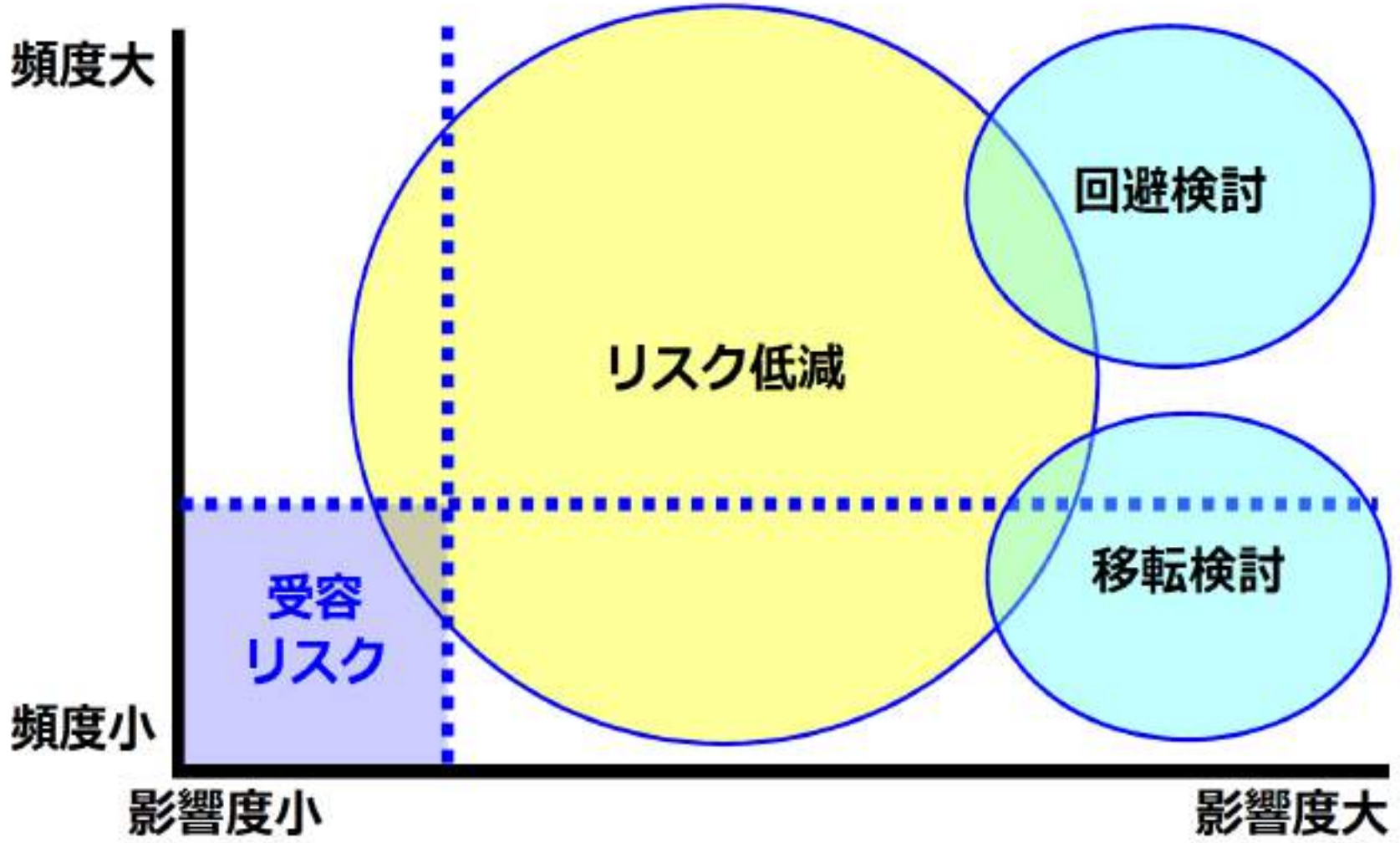
セキュリティ対策って何をすればいいの

リスクから自分たち・組織を守る

リスクを知り

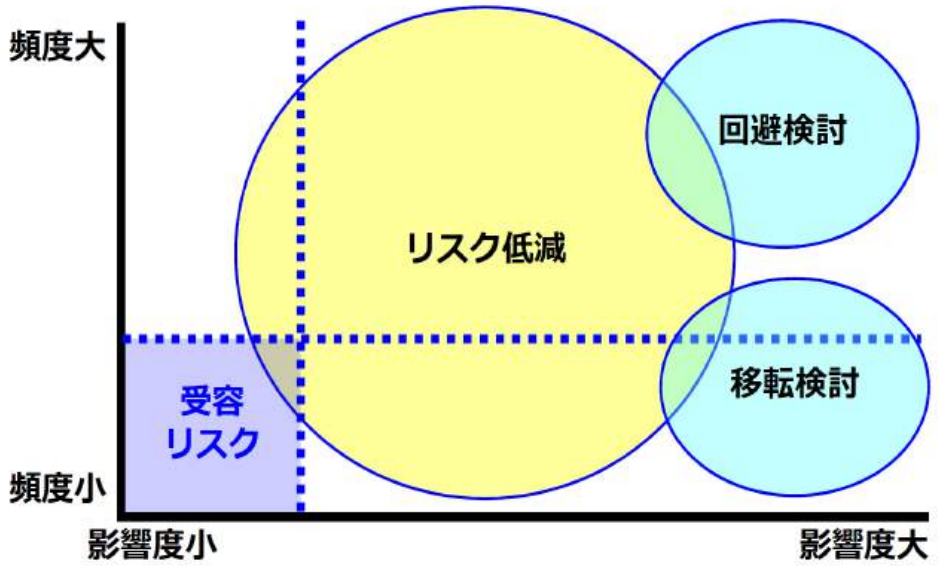
リスクを管理する

リスク管理の考え方の基本



IPA リスクへの対応 https://www.ipa.go.jp/security/manager/protect/pdca/risk.html を元に作成

リスク管理の考え方の基本



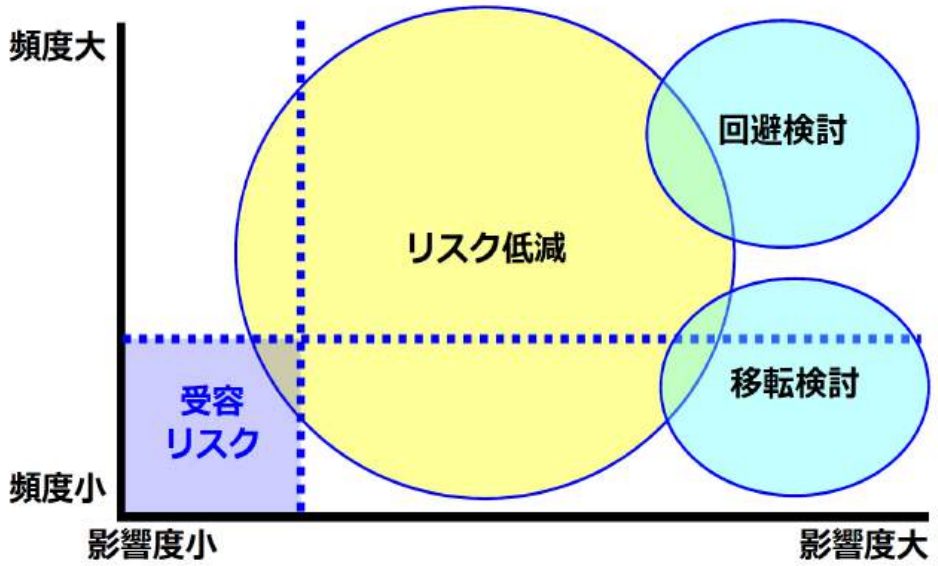
自動車にのるリスク

交通事故

リスク移転

自動車保険

リスク管理の考え方の基本



自動車にのるリスク

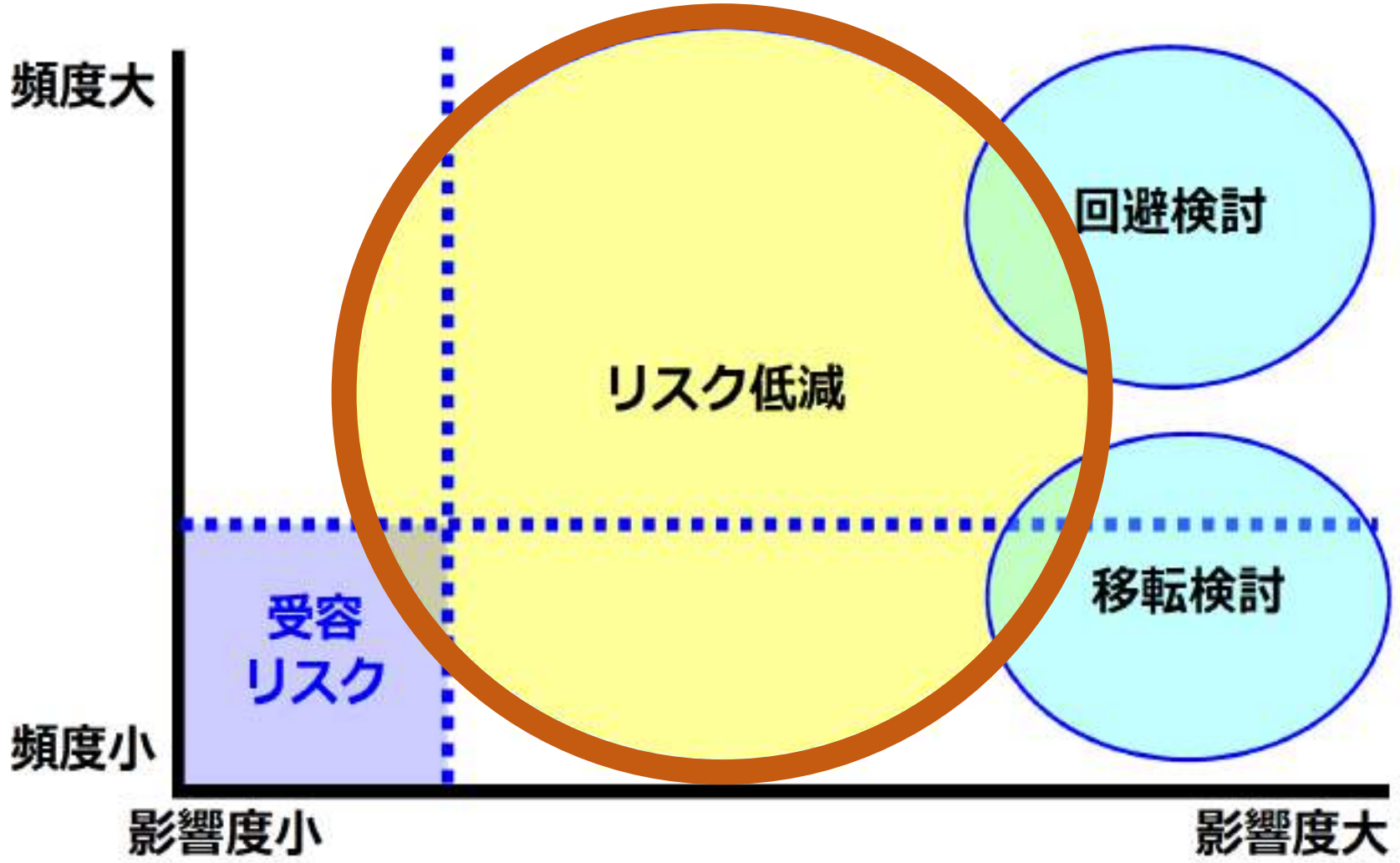
交通事故

リスク回避

免許返納

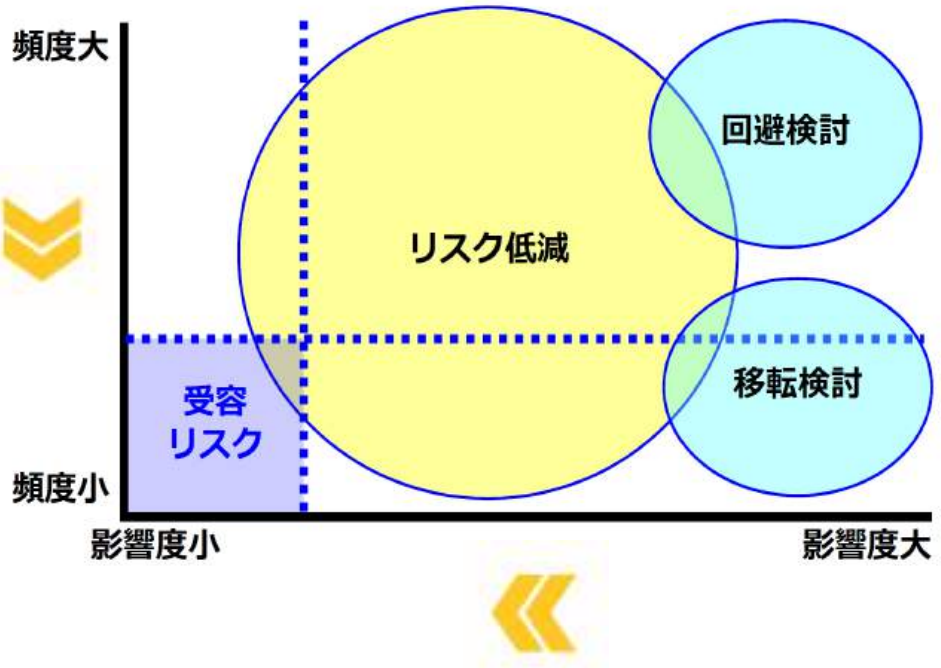
（運転しない）

リスク管理の考え方の基本



IPA リスクへの対応 https://www.ipa.go.jp/security/manager/protect/pdca/risk.html を元に作成

リスク管理の考え方の基本



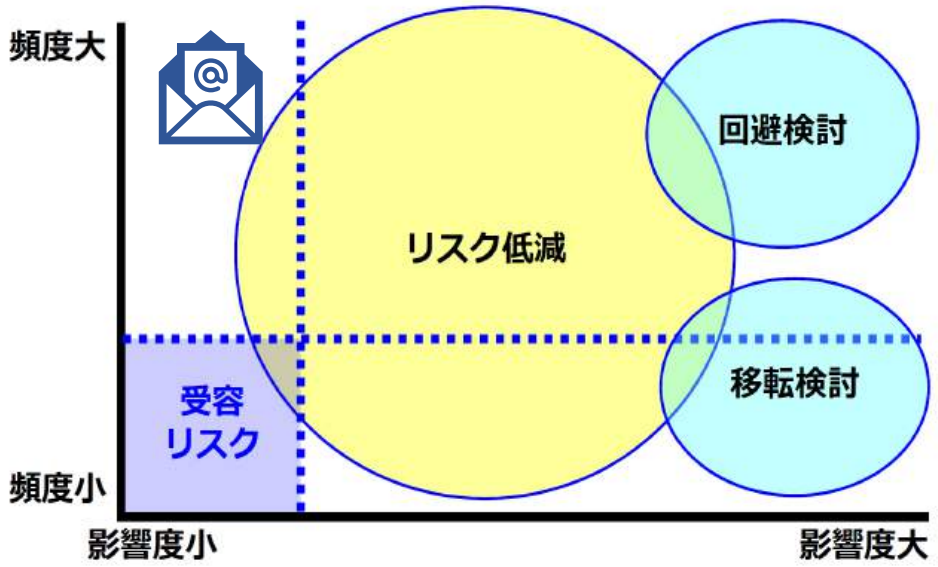
影響度が大きければ小さく

頻度が大きければ小さく

受容リスクにおさめる

セキュリティ対策

リスク管理の考え方の基本



メールのリスク

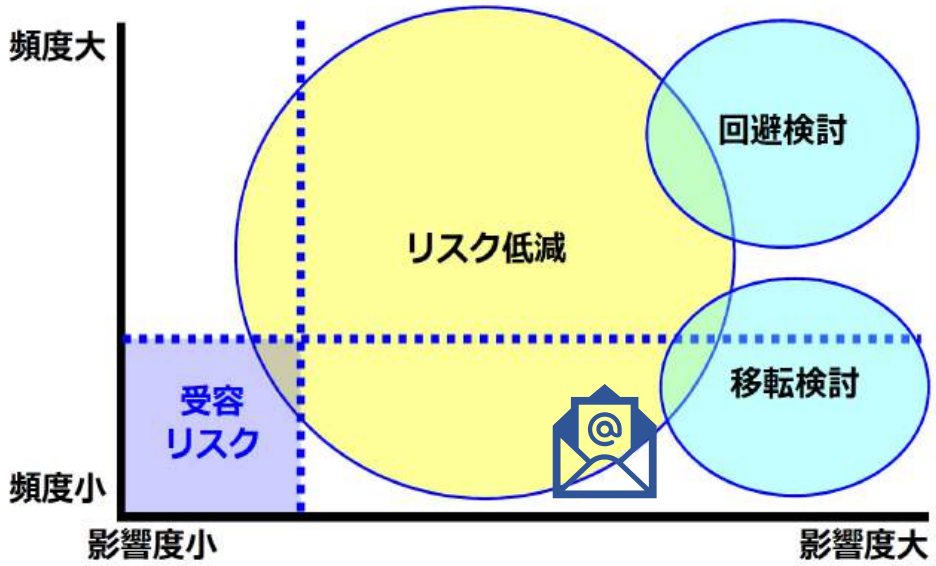
誤送信：

影響度小・頻度大

対策例：

宛先再確認、BCC

リスク管理の考え方の基本



メールのリスク

情報漏洩：

頻度小・影響度大

対策例：

クラウドストレージ

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を守るために

どんなリスクがあるか知り

リスクを管理することが必要

意味を理解して実施

私たちにできること

私たちにできること

経営者

システム管理者

システムユーザー

家庭内

それぞれの役割

社会活動に必要なセキュリティ
現代社会で生きていく上で必要な知識
社会教育によって獲得、交通ルールの様な浸透が必要

組織的活動に必要なセキュリティ
企業・組織の中で活動する上で必要な知識
一般ユーザーの立場とIT関連部門の立場に細分化して考える必要がある

技術者・専門家に必要なセキュリティ
セキュリティの専門家・技術者として必要な知識
特別な育成が必要になる

必要なセキュリティスキルの濃度が異なる

それぞれの役割

管理者

- 情報持ち出しルールの徹底
- 社内ネットワークへの機器接続ルールの徹底
- 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
- 不要なサービスやアカウントの停止または削除

ユーザー

- 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

- 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

情報処理推進機構　日常におけるセキュリティ対策

日常におけるセキュリティ対策

それぞれの役割

ユーザー

- 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

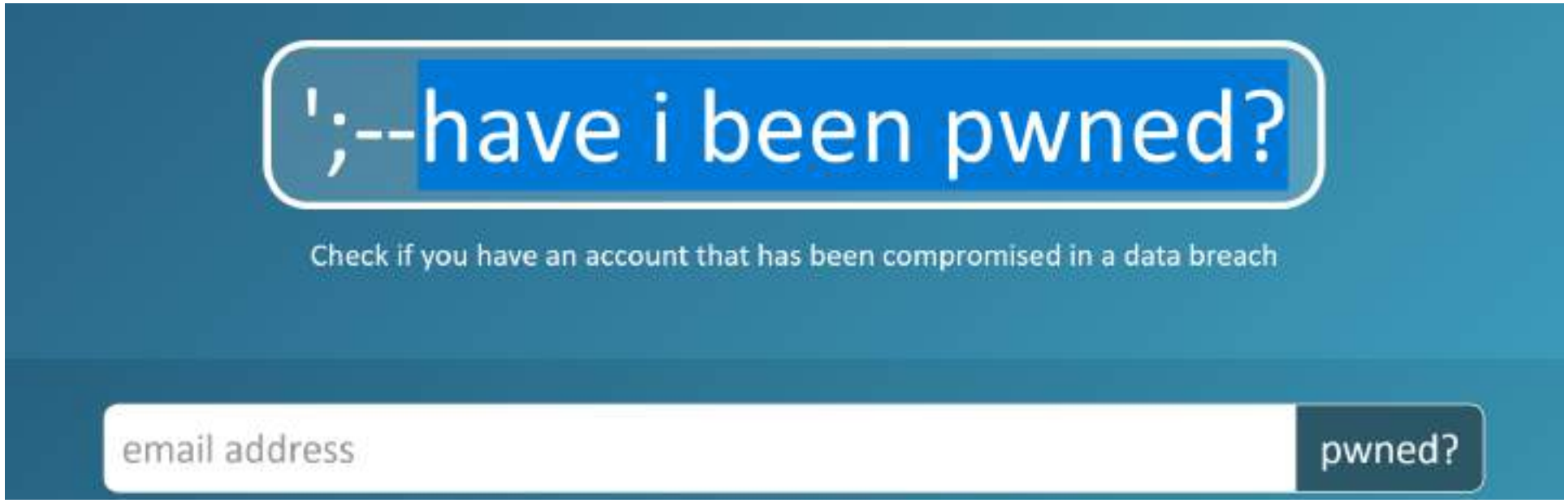
- アップデート忘れずに
- パスワード使いまわさない
- リンクのクリック大丈夫？
- 勝手にソフトいれないで

情報処理推進機構　日常におけるセキュリティ対策

日常におけるセキュリティ対策

メールアドレスが流出しているか確認

have i been pwned?



流出してる？と不安になる前に
アカウント(Eメールアドレス)が漏洩しているかどうかを確認できるサイト。登録して通知をうけることも可能。ドメインごと調べて通知も可能。このほかにEmailhunterというサイトではメールアドレスがネット上に掲載があるかどうか確認できる。

メールアドレスが流出しているか確認

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Peatix: In January 2019, the event organising platform Peatix suffered a data breach. The incident exposed 4.2M email addresses, names and salted password hashes. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Names, Passwords

Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames

Zurich: In January 2023, the Japanese arm of Zurich insurance suffered a data breach that exposed 2.6M customer records with over 756k unique email addresses. The data was subsequently posted to a popular hacking forum and also included names, genders, dates of birth and details of insured vehicles. The data was provided to HIBP by a source who requested it be attributed to "IntelBroker".

Compromised data: Dates of birth, Email addresses, Genders, Names, Vehicle details

IoT機器の感染・脆弱性を確認

am I infected?

家庭内のルーターやウェブカメラなどの
マルウェア感染、脆弱性診断サービス

ユーザーとしてできること

医療従事者・一般のシステム利用者向け サイバーセキュリティ対策チェックリスト

NO	チェック項目	チェック欄（○or×）
1	業務に不要なWEBサイトへのアクセスをしていないか	
2	システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っているか	
3	利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン（画面が他人から見えないようにするために、操作しないまま一定の時間が経つと自動的にパスワード付きスクリーンセーバーが起動するようにしたり、または自動的にログオフするように設定すること）等の対策を実施しているか	
4	従業員個人のUSBメモリ等の外部媒体を使用していないか又は業務上、外部媒体の使用が必要な場合は事前に申請し、医療機関が管理している外部媒体を使用しているか	
5	ソーシャルエンジニアリング（人の心理的・社会的な弱点や盲点をついて入手する手法）について理解し、安易にID・パスワードや個人情報等を外部提供しないようにしているか（本人確認やリンク先やメールアドレスの再確認等をした上で回答する等）	
6	見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意しているか（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）	
7	メール送信前にメール送信確認画面を再度表示し確認したり、メールの遅延送信機能（送信ボタンを押しても、すぐに送信されず、任意の時間の経過後メール送信される機能。メール送信の取消等が可能となり、誤送信の防止に有用となる）等を活用し、メールの誤送信を防止しているか	
8	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護しているか なおパスワードは別手段で知らせる、あるいは事前に取り決めておく等の手法とセットで行うこと	
9	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関内の情報システム部門または担当者に確認したり、事前に情報システム部門より、対応方法の連絡がある場合は指示に従って処理をしているか	
10	患者の情報について目的外使用をしていないか	

医療情報システムの安全管理に関するガイドライン医療機関のサイバーセキュリティ対策チェックリスト
https://www.mhlw.go.jp/content/10808000/000936167.pdf

それぞれの役割

管理者

- 情報持ち出しルールの徹底
- 社内ネットワークへの機器接続ルールの徹底
- 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
- 不要なサービスやアカウントの停止または削除

ユーザー

- 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
- 定期的なバックアップの実施
- 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

- 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
- 不要なサービスやアカウントの停止または削除
- 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

家庭内ではあなたも管理者

情報処理推進機構　日常におけるセキュリティ対策

日常におけるセキュリティ対策

覚えることがいっぱいすぎる

人は忘れる生きもの

1時間もたてば

聞いたことの半分は忘れてしまう

アウェアネスを高めよう

アウェアネスを高めよう

見えないリスクには対応できない

気づいていないから

見えないのではなく**見えていない**

アウェアネスを高めよう

アンテナがないと情報は受信できない

意識することで

見えていなかったものが見えるようになる

リテラシー≠アウェアネス

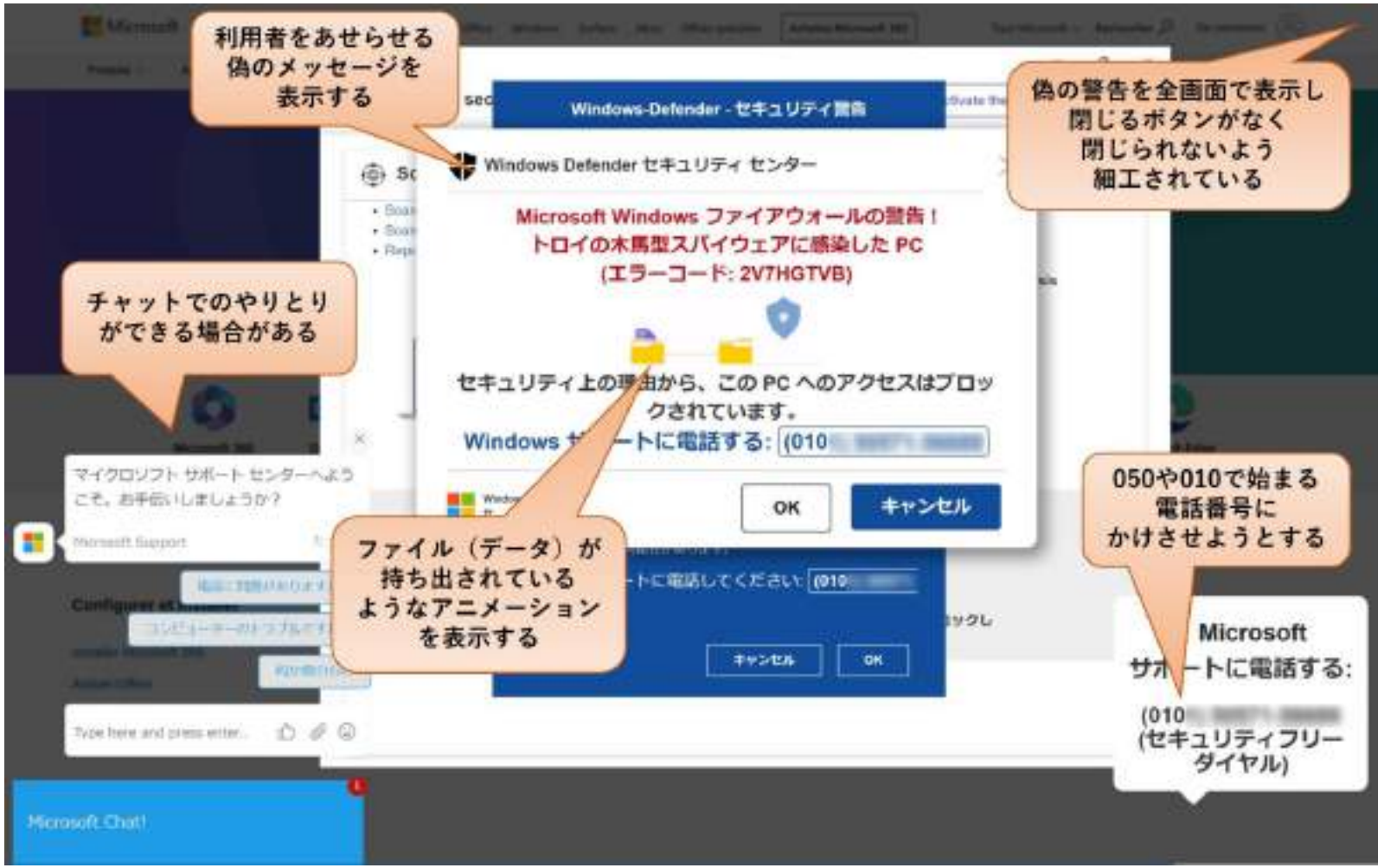
リテラシー

- ある分野における知識や理解力
- 網羅的・体系的
- 技術的要素を含むことがある
- トレーニングでスキルを習得

アウェアネス

- ある事象における気づき・意識
- 事象にフォーカス
- 技術的要素は薄い
- 気づきを得る体験

偽セキュリティ警告(サポート詐欺)画面の閉じ方体験サイト



体験することでアウェアネスを高めよう

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

アウェアネスを高めよう

リスクに気づき

リスクを意識すること

意識すると行動が変わる

インフルエンザを「意識する」

マスクをする

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

意識すると行動が変わる

健康を「意識する」

食生活の変化

体調の管理

情報

意識すると行動が変わる

家の防犯を「意識する」

ドアのカギを2つにする

防犯砂利

カメラをつける

意識すると行動が変わる

地域の防犯を「意識する」

パトロール

隣近所との声掛け

街灯

意識すると行動が変わる

意識すると行動につながる

押し付けられると嫌になる

意識すると行動が変わる

意識していても

高度な手洗いの方法

手洗いを理解しない人を怒る

意識すると行動が変わる

意識していても

高度なブレーキの踏み方

運転が下手な人を怒る

意識すると行動が変わる

意識する

意識させるための工夫

継続的に意識させる取り組み

意識すると行動が変わる

専門家にならなくていい

消防士になるのではなく
火事をおこさない工夫
消火器の使い方

アウェアネスを高めよう

リスクに気づき

リスクを意識すること

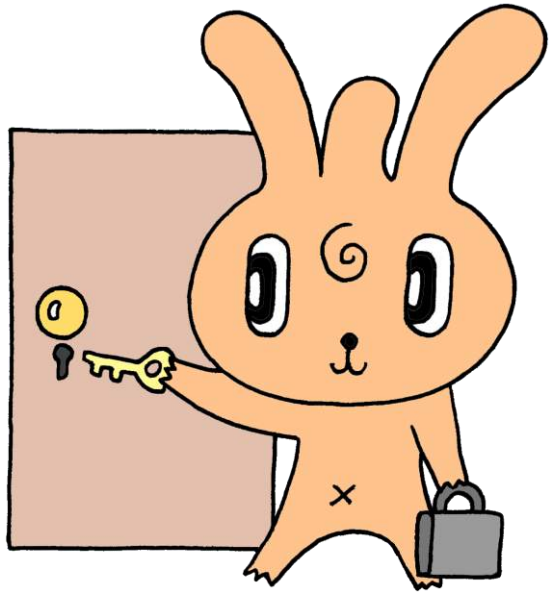
アウェアネスを高めよう

他人事ではなく自分事

相談しやすい環境作り

情報は共有しよう

セキュリティに無関係な人はいない



もっと詳しく知りたくなったら

情報セキュリティ10大脅威 2023

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによる スマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの 個人情報の窃取	8位	脆弱性対策の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの 不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の 不当請求による金銭被害	10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

「情報セキュリティ10大脅威 2023」解説書

- 情報セキュリティ10大脅威 2023 78ページ(PDF:3.6 MB)
- 情報セキュリティ10大脅威の活用法 18ページ(PDF:2.1 MB)
- 情報セキュリティ10大脅威 2023 セキュリティ対策の基本と共通対策 13ページ(PDF:750 KB)
- 情報セキュリティ10大脅威 2023 知っておきたい用語や仕組み 28ページ(PDF:1.8 MB)

「情報セキュリティ10大脅威 2023」簡易説明資料（スライド形式）

- 情報セキュリティ10大脅威 2023【組織編】85ページ(PDF:2.6 MB)
- 情報セキュリティ10大脅威 2023【個人編】84ページ(PDF:2.8 MB)
- 情報セキュリティ10大脅威 2023【組織編】（表現版）85ページ(PDF:2.5 MB)
- 情報セキュリティ10大脅威 2023【個人編】（一般利用者向け）68ページ(PDF:2.9 MB)

「情報セキュリティ10大脅威 2023」簡易説明資料（脅威個別版）

- 情報セキュリティ10大脅威 2023【組織編】（脅威個別版）(ZIP:3.9 MB)
- 情報セキュリティ10大脅威 2023【個人編】（脅威個別版）(ZIP:3.1 MB)

出典：IPA 情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/10threats/10threats2023.html