

NEWS RELEASE

報道関係各位

2023年6月5日

【情報セキュリティ研修の実施が義務化】 - 病院職員向けe-learning講座を新規開設 - 空き時間に自分のペースでセキュリティリテラシーをスキルアップ！

アライドテレスिस株式会社（本社 東京都品川区、代表取締役社長 サチエ オオシマ）は、2023年6月5日（月）より、当社のネットワーク研修・トレーニングサービス「ネットドットキャンパス (Net. Campus)」に、病院職員様を対象にした「情報セキュリティ研修 (e-learning)」を開設したことをお知らせします。



知識レベルと業務に合わせて選べる！

10コースをe-learning方式で開設

「診療録管理体制加算」の改定
情報セキュリティ研修の受講が義務化

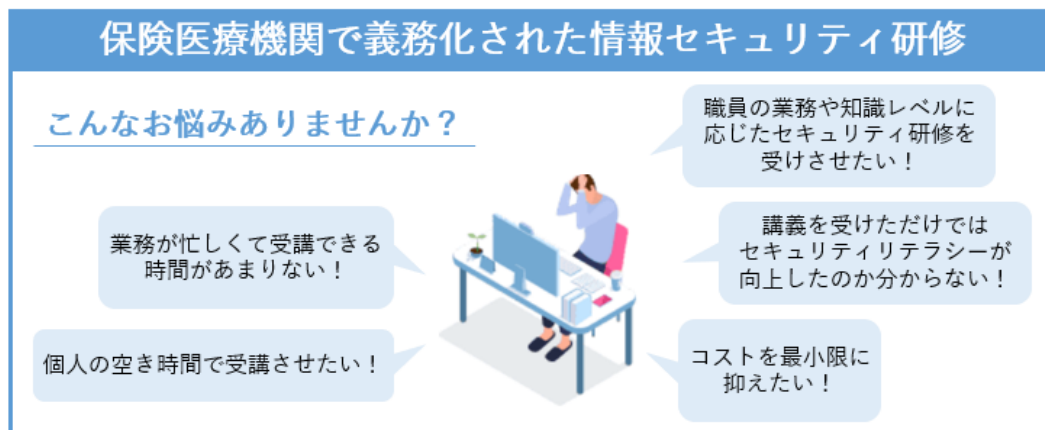
昨今、医療機関を標的としたサイバー攻撃の被害として電子カルテなど医療システムが停止し、医療提供体制に支障が出るなどの状況が増加していることで、リスクマネジメントやセキュリティ対策への意識が高まっています。このような事態を踏まえ、厚生労働省は令和4年度に「診療録管理体制加算」を改定し、非常時に備えたサイバーセキュリティ対策の整備に係る要件を見直しました。保険医療機関が「専任の医療情報システム安全管理者を配置すること」、「定期的に、最低でも年1回の職員を対象とした情報セキュリティ研修を実施すること」を義務付ける改定内容となっています^(※1)。

<いつでも・どこでも受講可能！病院職員の知識レベルに応じたe-learning研修>

そこで当社は、これまでオンライン形式（半日）でご提供していた「医療機関向けセキュリティ講座コース」に追加して、コストを抑えつつ、繁忙を極める医療現場でも病院職員が受講しやすいe-learning研修を設けました。

初級から上級レベルまであわせて全10コースある、このe-learning研修では、受講者となる病院職員のセキュリティリテラシーや業務内容に応じて、必要なコースを選べるようになっています。また、講義時間も20分と短く設定してあるため、空き時間を活用し、短時間で集中して受講できるようになっています。

受講後には、理解度チェック用の設問も用意しており、受講内容の復習や自身の理解度の把握ができます。各コースは受講期間内であれば何度でも受講が可能のため、理解度の向上や振り返りも可能です。



保険医療機関で義務化された情報セキュリティ研修

こんなお悩みありませんか？

- 業務が忙しくて受講できる時間があまりない！
- 個人の空き時間で受講させたい！
- 職員の業務や知識レベルに応じたセキュリティ研修を受けさせたい！
- 講義を受けただけではセキュリティリテラシーが向上したのか分からない！
- コストを最小限に抑えたい！

【アライドテレシスのe-learning講座の特長とメリット】

- ① インターネット環境があれば、いつでも・どこでもかんたんに受講ができる
- ② 1コース3,300円（標準価格/税込）で、2か月間何度も受講ができる
- ③ 職員の知識レベルに応じて初級・中級・上級の全10コースをご提供
- ④ 講義受講後の理解度チェックで、受講内容の復習ができる
- ⑤ 学習管理システムで受講状況や理解度チェック結果を閲覧できる

【開催コースの概要】

コース名	レベル	内容	標準価格 (税込)/1名
病院への サイバー攻撃事例	初級	病院を狙ったサイバー攻撃に関して、近年の事例や侵入経路、マルウェアの種類等について説明します。また、脆弱性やウイルスへの対策、被害にあった場合の損害内容についても解説します。	¥3,300
パスワード管理と 認証の重要性	初級	代表的なパスワードハッキング手法の紹介をはじめ、パスワードハッキングへの対策としてパスワード作成方法や多要素認証、パスワードの利用について解説します。	¥3,300
巧妙化する 攻撃メール対策	初級	巧妙化する標的型攻撃メールに関し、実際の攻撃メールや添付ファイルの例を用いて説明します。また、フィッシングメールの見分け方やフィッシングサイト確認方法について解説します。	¥3,300
情報端末の 適切な設定とUSB利用	初級	情報端末を安全に使用するために必要なセキュリティ設定や紛失時の対応、廃棄時の注意点を説明します。また、USBをはじめとする外部記憶装置の扱いやデータ移送について解説します。	¥3,300
インシデント報告の 重要性	初級	インシデント発生時の早期報告の重要性とガイドラインを基にしたインシデント報告の体制やフローの把握等について解説します。	¥3,300
ランサムウェア攻撃の 理解	中級	急増する病院へのランサムウェア攻撃に関して、概要や被害の特徴、影響範囲、求められる対策について解説します。	¥3,300
メールに関する 基本と設定	中級	標的型攻撃メールの特徴をメールヘッダや添付ファイルのサンプルを用いて説明します。また、メール利用時の注意事項や各種設定についてクライアント側、サーバー側で実施できる対策を解説します。	¥3,300
無線LANの セキュリティ対策	中級	病院内で活用される無線LANに関して、基礎知識をはじめ、ガイドラインの内容を基に不正アクセス防止対策や暗号化等について解説します。	¥3,300
リモート回線からの 侵入対策	上級	医療情報システムのリモートメンテナンス回線から侵入するランサムウェア攻撃の原因やガイドラインに基づくVPN機器も含めたリモートアクセスのセキュリティ対策について解説します。	¥3,300
インシデント発生時の 対応	上級	インシデント発生時の迅速な対応について、平時の体制整備からインシデント発生後の各対応フェーズ(検知・初動対応・復旧)までのポイントを解説します。	¥3,300

詳しくは当社Webページをご覧ください。

<https://www.allied-teleasis.co.jp/event/training/net-campus/index.html#e-learning>

サイバー攻撃や情報漏えいの原因はヒューマンエラーによることが多く、また、インシデント発生後の被害の深刻度も発生後の対応により変わります。各職員が最新の事例や情報に触れることでその重要性を認識し、巧妙化する攻撃メールや不審なメールへの見分け方、インシデント発生後の報告などの対応方法について適切に行うことで組織全体のセキュリティが強化されます。充実したコースをご用意しておりますので、ぜひご参加ください。

当社では、今後もサイバーセキュリティを含め、受講者の方々が研修形式に囚われず柔軟に受講いただける各種コースを整備・拡充してまいります。

※1：許可病床数が400床以上の保険医療機関が対象。

注) 研修コース構成や内容は、都合により変更される場合がございます。予めご了承ください。

注) 記載されている商品またはサービスの名称等はアライドテレシスホールディングス株式会社、アライドテレシス株式会社およびグループ各社、ならびに第三者や各社の商標または登録商標です。

《ニュースリリースに対するお問い合わせ先》

アライドテレシス株式会社 マーケティングコミュニケーション部

TEL: 03-5437-6042 E-Mail: pr_mktg@allied-teleasis.co.jp

アライドテレシス株式会社 〒141-0031 東京都品川区西五反田 7-21-11 第2 TOCビル

<https://www.allied-teleasis.co.jp/>