建設業向けサイバーセキュリティ教育動画一覧リスト

NO	対象者			タイトル	注意事項
	ゼネコン	協力会社代表	作業員		
1	○	○	○	現場写真の漏えい	・工事中の建物（内観・外観）を無断で撮影してはいけません。 ・撮影した写真や工事中に知った情報などをSNS等のインターネット上に投稿してはいけません。 ・工事の建物や情報が漏えいした場合、自社の信用の失墜や損害賠償に発展する可能性があります。
2	○	○	○	図面の廃棄	・図面等、客先情報が載っている書類の処分については、事前に提供元へ返却が必要か確認しましょう。廃棄する場合、現場内のオフィス用シュレッダーで裁断しましょう。 ・客先情報が載っていなくても、事業系ごみを家庭系ごみのクリーンステー ションに出すことはできません。 5年以下の懲役、もしくは 1,000万円以下の罰金またはその両方が科せられることがあります。
3	○	○	○	EPS（電気配線シャフト）の不審な機器	・不審な機器を発見した場合は、関係者へ報告しましょう。 ・不審な機器を通じてデータの窃取や改ざんがされる危険性があります。例えば、接続されているデジタルサイネージの表示内容を改変される危険性があります。 ・機器ごとにネットワーク接続の要否について検討し、不要な機器は接続しないようにしましょう。
4	○	○	○	宅配業者を装った偽のSMS	・不審に感じたり、身に覚えのないSMSは、記載されたURLに接続しないようにしましょう。 ・宅配業者や通信業者を装い、SMSを送信することで不審なアプリをインストールさせたり、ログイン情報を窃取する被害が増えています。 ・不正なアプリをインストールした場合、同じ内容の偽のSMSを見知らぬ相手先へ多数送信したり、スマートフォン内のデータやSMSが窃取され、不正使用される可能性があります。
5	○	○	○	車上荒らしによる情報機器等の盗難	・車にパソコン等の情報機器や図面を置きっぱなしにするのはやめましょう。 ・万が一パソコンを紛失したり、盗難されたりした場合に備えて、パスワード保護や暗号化を行い第三者がデータにアクセスできないようにしましょう。また、重要なデータはバックアップを取るようにしましょう。
6	○	○		テレワーク（自宅）による情報漏えい	・業務で知った工事に関する内部情報、機密情報は、たとえ家族でも話してはいけません。 ・テレワークの際は、機器や書類の管理、会議の音声などに十分に注意しましょう。 ・情報が漏えいした場合、自社の信用の失墜や損害賠償に発展する可能性があります。
7	○	○		メールの誤送信	・メールの誤送信で最も多いのは、宛先の間違いと添付ファイルの間違いです。 ・機密情報や個人情報等の重要情報を取り扱う時は、十分に注意して送信しましょう。 ・送信メールを一時保留する機能を利用し、誤送信時に取消可能にすることも対策になります。
8	○	○		Emotetの感染	・Emotetに感染すると、重要な情報の窃取、ランサムウェアへの感染、また社内の他の端末への感染だけでなく、窃取したメール情報を利用し、顧客や取引先へEmotetのばらまきメールを配信する可能性があります。 不審なメールを受信した場合は、添付ファイルや記載されているURLは開かずに、担当者等に確認しましょう。 ・特にマクロ付きのWordやExcel、OneNote、リンクファイル等に注意しましょう。
9	○	○		私物パソコン、私用メールアドレスの業務利用	・私物のパソコンや私用のメールアドレスの業務利用は情報漏えいのリスクが高まるためやめましょう。 ・私物のパソコンは、ウイルス対策が不十分な場合があります。また、ウェブサイトへのアクセスや様々なソフトウェアのインストールにより、ウイルス感染やソフトウェアの脆弱性を悪用されるリスクがあります。 ・私用のメールアドレスは、スパムやフィッシング詐欺のターゲットになりやすくウイルス送信にも使われる等のリスクがあります。
10	○	○		ビジネスメール詐欺	・攻撃者は送信元のメールアドレスを詐称したり、日常のメールを盗み見たり、メールアカウントを乗っ取ったりしたうえ、詐欺と見分けづらいメールを送信します。 ・振込先の口座変更など普段とは異なるメール、判断を急がせるメールには注意しましょう。また、電話や口座名義の確認等、複数の手段で確認を行いましょう。
11	○	○		複合機の設置	・複合機をネットワークに接続する時は、ファイアウォール等を通して接続し、外部からの不正なアクセスを遮断する必要があります。 ・外部から不正アクセスされるとコピーやスキャンしたデータが漏えいしたり、複合機を経由して他の機器に攻撃されてしまうリスクがあります。
12	○	○		複合機の廃棄	・複合機の中には、印刷、コピー、スキャン、FAXのデータや通信先等の情報がたくさん保管されています。 ・このようなデータは、ごみ箱などに移動させたとしても完全に削除されないため、初期化機能等を使ってデータを削除する必要があります。 ・廃棄については保守契約先やメーカー等に確認のうえ、情報漏洩が発生しないように正しく対応しましょう。
13	○	○		なりすましによる名刺管理システムの情報窃取	・不審な電話やメールがあった場合は、担当者等に確認しましょう。特に重要情報を取り扱うサービスについては十分に注意しましょう。 ・不審なメールに記載されたURLへのアクセスはやめましょう。 ・重要情報を取り扱うサービスは、2段階認証を利用しましょう。
14	○	○		情報機器の紛失	・寄り道や飲酒は、紛失のリスクを高めます。十分に注意しましょう。 ・パソコン、タブレット等を持ち歩く場合は、肌身から離さないようにしましょう。 ・万が一パソコンを紛失したり、盗難されたりした場合に備えて、パスワード保護や暗号化を行い第三者がデータにアクセスできないようにしましょう。また、重要なデータはバックアップを取りましょう。
15	○	○		USBメモリによる感染	・持ち主が分からない等の不審な機器をパソコンに接続するのはやめましょう。接続するだけでウイルスに感染するリスクがあります。 ・ウイルスに感染した場合、ネットワークを通して他の機器に感染が拡大する可能性があります。パソコンの動作に異変を感じた場合は、接続した機器だけでなく、LANケーブルやWi-Fiなどのネットワークも切断して担当者に連絡しましょう。

16	○	○		ネットワーク機器の廃棄	・ネットワーク機器に、社内ネットワークに接続するための認証情報、ログ情報、管理者のパスワード、機器所有者の情報等が保存されたまま中古で販売されているケースが多数確認されています。 ・ネットワーク機器を廃棄する場合は、機器の情報を正しく削除しましょう。 ・機器にドリルで穴を開ける等の物理的な破壊も有効です。
17	○	○		現場監視カメラの映像の漏えい	・初期設定のID、パスワードは、一般的に知られているものが多いです。不正アクセスされる危険性がありますので変更しましょう。 ・パスワードの未設定、簡単すぎるパスワードなどにも注意しましょう。 ・映像の漏えいだけでなく、ウイルス感染やカメラを経由した他の機器への攻撃に利用される等のリスクもあります。
18	○	○		退職者によるサーバデータの削除	・重要なデータを取り扱う権限があるID、パスワードは、利用者ごとまたは限定したメンバーで共有し、利用者を特定できるようにしましょう。 ・退職者のアカウントは即時に停止し、利用できないようにしましょう。 ・重要なデータは必ずバックアップをとり、不測の事態にも対応できるようにしましょう。
19	○	○		USBメモリの紛失と報告遅延	・重要な機器やデータは、パスワード保護や暗号化を行い、紛失した場合でも第三者がデータにアクセスできないようにしましょう。 ・機器の台帳管理と定期的な棚卸を行い、所持している機器や情報（暗号化やパスワード保護の有無、保存しているデータ）の確認や不要な機器の処分を行いましょう。 ・紛失が判明した時点で直ぐに上司や担当者へ連絡し、機器の情報を伝達しましょう。
20	○	○		ID、パスワードを書いた付箋	・ID、パスワードは利用者ごとに設定しましょう。 ・ID、パスワードを他人にわかるところにメモしたり、表示するのはやめましょう。 ・パソコン等の情報機器とID、パスワードを書いたメモを同時に紛失した場合、不正アクセスされるリスクが高まりますので注意しましょう。
21	○	○		AIチャットボットによる情報漏えい	・AIチャットボットの利用時等にインターネット上で入力した情報は、公開されたり漏えいが発生する危険性があります。機密情報、顧客情報、個人情報報等を入力するのはやめましょう。 ・翻訳サイトはインターネットサービスのため、同様に情報漏えいの危険性があります。入力する内容は十分注意しましょう。
22	○	○		ホームページの改ざん	・ホームページを改ざんされると、機密データを窃取されたり、アクセスした人をウイルスに感染させたり、詐欺サイトに誘導されたりします。 ・ウェブアプリケーションのセキュリティー対策の実装や、ウェブサーバのOSやソフトウェアのアップデートを行い、脆弱性のない状態を保ちましょう。
23	○	○		SNSアカウントの乗っ取り	・予測されやすいパスワードを設定するのはやめましょう。英語の大文字、小文字、数字、記号を組み合わせて作成しましょう。また重要なサービスは、2段階認証を利用しましょう。 ・アカウントが乗っ取られると、情報漏えいが発生したり、意図しない広告や詐欺サイトの投稿を行われ、企業の信用の失墜に発展する場合があります。
24	○	○		アカウントの使い回し	・アカウントの使い回しはやめましょう。特に客先から発行されたアカウントは注意が必要です。 ・アカウントの使い回しを行うと、利用者による不正が起きた場合、犯人の特定や責任追及が困難になります。 ・アカウント管理者は、組織や個人に対して個別のアカウントを用意し、不正アクセスのリスクを最小限に抑えましょう。
25	○	○		ID、パスワードの使い回し	・IDとパスワードの使い回しはやめましょう。 ・IDとパスワードの使い回しをしている場合、1つのサービスでIDとパスワードが漏洩すると、他のサービスに不正ログインされる危険性があります。 ・重要情報を取り扱うサービスは、2段階認証を利用しましょう。
26	○	○		フリーソフトの利用	・会社や組織で許可されていないフリーソフト等を利用するのはやめましょう。 ・許可されたソフトでも必ず正規サイトからダウンロードを行いましょう。 ・怪しいサイトからフリーソフトをダウンロードすると、ウイルス等が仕込まれていることがあり、気付かぬうちに情報漏えいしていることがあります。
27	○	○		詰所におけるパソコン盗難	・詰所や事務所の施錠管理は当事者意識をもって行いましょう。 ・パソコン、サーバ等の情報機器は、鍵の掛かる部屋やキャビネットに保管したり、ワイヤーを付けたりし、簡単に盗難されないようにしましょう。 ・万が一パソコンを紛失したり、盗難されたりした場合に備えて、パスワード保護や暗号化を行い第三者がデータにアクセスできないようにしましょう。また、重要なデータはバックアップを取りましょう。
28	○	○		FAX誤送信	・FAX送信前に、送信先の番号や宛先をよく確認しましょう ・誤送信により、情報漏えいや取引先から会社の信頼を失う危険性があります。個人情報や機密情報を含んだ書類はFAXを利用しないようにしましょう。 ・頻繁に送信する相手先がある場合は、連絡先を登録し入力ミスを防ぎましょう。
29	○	○		大容量ファイル送信サービスによる情報漏えい	・大容量ファイル送信サービスのように便利なインターネットサービスが多くありますが、利用時には情報漏えいが発生するリスクあることを認識しましょう。特に無料で利用できるものは注意が必要です。 ・インターネットサービスは、会社で許可されたもののみを利用し、サービス自体の安全性や提供元の信頼性を十分に確認して利用しましょう。
30	○	○		フィッシングメール	・攻撃者は、実在する企業や組織などを騙り、送信元のメールアドレス、リンク先のURLやウェブページ等を巧みに偽装して誘導し、アカウント情報等の窃取を行います。 ・メールが通常と異なる内容であったり、不審に感じたりした場合は注意しましょう。 ・重要情報を取り扱うサービスは、2段階認証を利用しましょう。