

用語集

AI時代に学ぶサイバーセキュリティ

説明の中で出てくる言葉を、最初に出てくる回ごとに並べています。意味のあとに、研修のどこで使うかを書きました。

01

1日目 知る

言葉	意味と、出てくる場面
生成AI	文章や画像を作り出すAIです。本研修では、GoogleのGeminiを無料で使える範囲で使います。
シャドーAI	会社が把握していないまま、社員が個人のアカウントなどで使っているAIサービスです。1日目のS03で、事故との関わりを数字で見ます。
AIエージェント	指示を受けて、ツールの操作やファイルの読み書きまで自分で進めるAIです。渡した権限の範囲で動くため、権限の決め方で事故の大きさが変わります。
ディープフェイク	AIで作った、本人そっくりの偽の音声や映像です。幹部になりすました電話やビデオ会議に使われます。
フィッシング	本物そっくりのメールやSMS、偽サイトで、IDやパスワード、カード番号を入力させる手口です。AIで自然な日本語の文面を作れるようになりました。
ランサムウェア	パソコンやサーバーのデータを暗号化して使えなくし、元に戻す代わりに金銭を求めるウイルスです。盗んだデータを公開すると脅す手口と組み合わせられます。
個人情報	生きている個人を特定できる情報です。氏名、メールアドレス、電話番号などが当たります。
要配慮個人情報	病歴や健康診断の結果のように、扱いに特に配慮が要る個人情報です。漏えいすると、1件でも個人情報保護委員会への報告の対象になります。

言葉	意味と、出てくる場面
匿名化	社名や人名、連絡先、金額などを置き換えて、どこの誰の話か分からなくすることです。1日目の演習では、A社や担当者1のような呼び方に置き換えます。

02

2日目 守る

言葉	意味と、出てくる場面
パスワードの使い回し	同じパスワードを複数のサービスで使うことです。1つのサービスから漏れると、ほかのサービスにも入られます。
リスト型攻撃	漏れたIDとパスワードの組を、別のサービスのログイン画面に次々に試す攻撃です。使い回しがあると成功します。
多要素認証	パスワードに加えて、スマートフォンへの通知や確認コードなど、別の要素も確かめるログインの方式です。2段階認証とも呼ばれます。
パスキー	パスワードの代わりに、スマートフォンやパソコンの指紋認証や顔認証でログインする方式です。偽サイトでは使えないため、フィッシングに強い方式です。
Have I Been Pwned	メールアドレスを入れると、過去の漏えいデータに含まれているかを調べられる無料のサイトです。2日目の演習で使います。
インフォスティーラー	パソコンに入り込み、ブラウザに保存したパスワードやログイン中の情報を盗み出すウイルスです。
ソーシャルエンジニアリング	技術ではなく、人のすきを突いて情報を聞き出す手口です。社員になりすましてヘルプデスクに電話し、パスワードを再設定させた事件を2日目に見ます。
ドメイン	メールアドレスの@より後ろや、URLの会社名に当たる部分です。偽のメールを見分けるときは、正規のドメインと1文字ずつ見比べます。
VPN機器	社外から社内のネットワークにつなぐための機器です。弱点が残っていると、攻撃者の入口になります。

言葉	意味と、出てくる場面
ビジネスメール詐欺	社長や取引先になりすましたメールで、送金やギフトカードの購入を指示する詐欺です。

03

3日目 対応する

言葉	意味と、出てくる場面
インシデント	情報の漏えいやウイルス感染のように、セキュリティ上の問題が起きた出来事です。起きたおそれがある段階も含みます。
EDR	パソコンやサーバーの動きを記録し、怪しい動きを見つけて知らせるソフトです。3日目のシナリオは、EDRの警告から始まります。
CSIRT	会社の中でインシデントに対応するチームです。連絡の窓口になり、初動の指揮と社外への報告をまとめます。
SOC	ネットワークやパソコンの記録を見張り、攻撃の兆しを見つけるチームです。
第一報	インシデントに気づいたあと、経営層や関係先へ最初にする報告です。分かっていないことは推測で埋めず、「調査中」と書きます。
速報と確報	個人情報が出たおそれがあるときに、個人情報保護委員会へ出す報告です。速報は気づいた時点からおおむね3～5日以内、確報は30日以内に出します。不正の目的によるおそれがあるときは、確報の期限が60日以内になります。
オフラインのバックアップ	ネットワークから切り離れた場所に保管するバックアップです。ランサムウェアに暗号化されずに残るため、業務を戻す手段になります。
サプライチェーン攻撃	委託先や取引先のように、つながりのある会社を経由して入り込む攻撃です。

言葉	意味と、出てくる場面
脆弱性	ソフトウェアや機器の弱点です。メーカーが修正版を出したら、早く当てると入れにくくなります。
フォレンジック	パソコンやサーバーに残った記録を調べ、何がいつ起きたかを明らかにする調査です。
机上演習	架空のインシデントの筋書きを使い、誰が何をするかを会議室で確かめる訓練です。3日目のハンズオンは、その小さな版に当たります。
BCP(事業継続計画)	システムが止まっても業務を続けるための計画です。紙の伝票や電話での受注のように、ITなしで回す手順も含まれます。
FDE(フォワード・デプロイド・エンジニア)	募集の案内に出てくる言葉です。顧客の現場に入り、要望の確認から実装と定着までを一貫して担うエンジニアを指します。AIを業務に組み込む仕事では、どのデータをAIに渡すかを決める役目も担います。
セキュリティエンジニア	会社のシステムと情報を守る仕組みを作り、動かす技術者です。ルールづくり、監視、インシデント対応、脆弱性診断のように、仕事は分かれています。



AI時代に学ぶサイバーセキュリティ スタッフサービス・エンジニアリング様向け

© Givery, Inc.

※本教材の演習に登場する企業、人物、数値は架空です。事例の紹介に出てくる企業名は、公開された報道と発表によります。