

knowbe4

2026 サイバーセキュリティ 意識向上月間

キット&戦略指南書

CONFIDENTIAL



PAGE >

第1週

第2週

第3週

第4週

ミッションの概要：

2026年 サイバーセキュリティ 意識向上月間

世界中の脅威に対して先手を打つために、チームに必要な情報を提供すること。
それが君に与えられた10月のミッションだ。

「ワークフォースリスク特命チーム (WRD)」とは、今年のすべてのサイバーセキュリティリソースを最大限に活用できる精鋭チーム。

WRDの一員としての君の役割は、君の組織のメンバーが、1週間、いくつかのサイバー脅威に特化した4つのミッションに取り組めるようサポートすることだ。

KnowBe4は、そのために役立つ情報をまとめたリソースを無料で配布している。

チームに必要なナレッジを徹底的に叩き込み、最前線でサイバー脅威に立ち向かえる精鋭へと仕立て上げる。

奴らの襲撃に備えよ。今月はサイバーセキュリティ意識向上月間だ。我が組織のメンバー全員を「エージェント」として再定義し、前線の戦力として投入する。手始めにこの装備キットを活用してくれ。

トレーニングモジュールやポスター、各種文書に加え、脅威に対抗するスキルを宿した4人の「特別エージェント」カードを仕込んである。

あらゆる状況を想定した4つの机上演習シナリオも配備済みだ。対面・オンラインを問わず叩き台にし、組織のレジリエンスを強化するのだ。

...ミッションの成功を期待している。



ツール

ツール (Web) に含まれるもの:

社外秘

- 動画: 組織のAI導入を安全に実現する方法
- ホワイトペーパー: ハイブリッドな業務環境の安全を確保する: 新時代における「人」と「AI エージェント」の保護
- シナリオ教材
- セキュリティ意識向上ウィークリープランナー (Web) では、以下のユーザー向けアセットをすべて、10月を通じて活用できるよう週ごとのテーマ別で提供しています。こちらからご利用ください。

ウィークリープランナー

前線のエージェントたちへ

なお、すべてのコースと教材 (コンテンツ) にアクセスできるのは【2026年10月31日】までだ。タイムリミットまでにすべて叩き込め。

- 6つの無料インタラクティブトレーニングまたは動画モジュール
 - スミッシング・フレンジー (35言語対応)
 - ディープフェイクを用いたソーシャルエンジニアリング攻撃 (35言語対応)
 - 知的財産の保護 (12言語対応)
 - 強固なパスワード、安全なアカウント (35言語対応)
 - ハッキングに負けない習慣: オーディオキャスト (12言語対応)
 - プライバシーの追求ゲーム (13言語対応)
- ワークフォースリスク特命チームスペシャリストのキャラクターカード/ポスター 4枚
- 重要なコンセプトの復習用ポスター4枚とデジタルサイネージ用素材

FOR YOUR
EYES ONLY

ワークフォース リスク特命チームの基礎知識

WRDのエージェントとして過酷な前線に立ち続けることが、いかに過大な負荷を強いるものか、私は誰よりも理解している。だからこそ我々は、新組織員の育成プロセスを極限まで円滑化するバックアップ体制を構築した。

作戦期間となる10月の4週間、各週の重点学習テーマに応じた戦術コンテンツを順次解禁・配備する。

各エージェントは、毎週以下の戦術コンテンツから少なくとも1つ以上を選択し、即座に履修・展開せよ。

- 動画とインタラクティブなトレーニングモジュール
- 啓発ポスター/情報文書
- WRDエージェント キャラクターカード
- 机上演習教材

各週の詳細な作戦テーマについては、本資料の後半で徹底解説する。まずはここで、全体像を把握せよ。

- 第1週: フィッシングとソーシャルエンジニアリング
- 第2週: AIの安全性とディープフェイク
- 第3週: データセキュリティとパスワード
- 第4週: インシデント報告

作戦の全貌を解明したくば、直ちに「セキュリティ意識向上プランナー」へアクセスせよ:

ウィークリープランナー

言っておくが、WRDの装備品 (アセット) を拝めるのはこのプランナーからだけだ。取りこぼすなよ。

WRDスペシャリストプロフィール

ミッションの全貌は理解したな。次はいよいよ、諸君の背中を守る「スペシャリストたち」を紹介する。

今回の「サイバーセキュリティ意識向上月間」に向けて、作戦遂行に欠かせない4つのスキルセットを配備した。以下に示す「4人のスペシャリスト・プロフィール」を活用し、これらのスキルを組織 (エージェント) へ徹底して伝授せよ。

彼らはそれぞれ、今月のミッションを極めるための『核』となる能力を宿している。どの精鋭を引き連れて前線へ向かうかは、諸君 (エージェント) の判断に委ねる。

フィッシング / ソーシャルエンジニアリング

ゴースト



モットー：
信用せよ
されど確認せよ
そして
もう一度確認せよ

職務：対諜報スペシャリスト

専門分野：プリテキストティングや高度なソーシャルエンジニアリングの早期発見

アドバイス：『大変!今すぐ行動して』との煽りメールはまず疑え

AI脅威/安全性

ガジェット



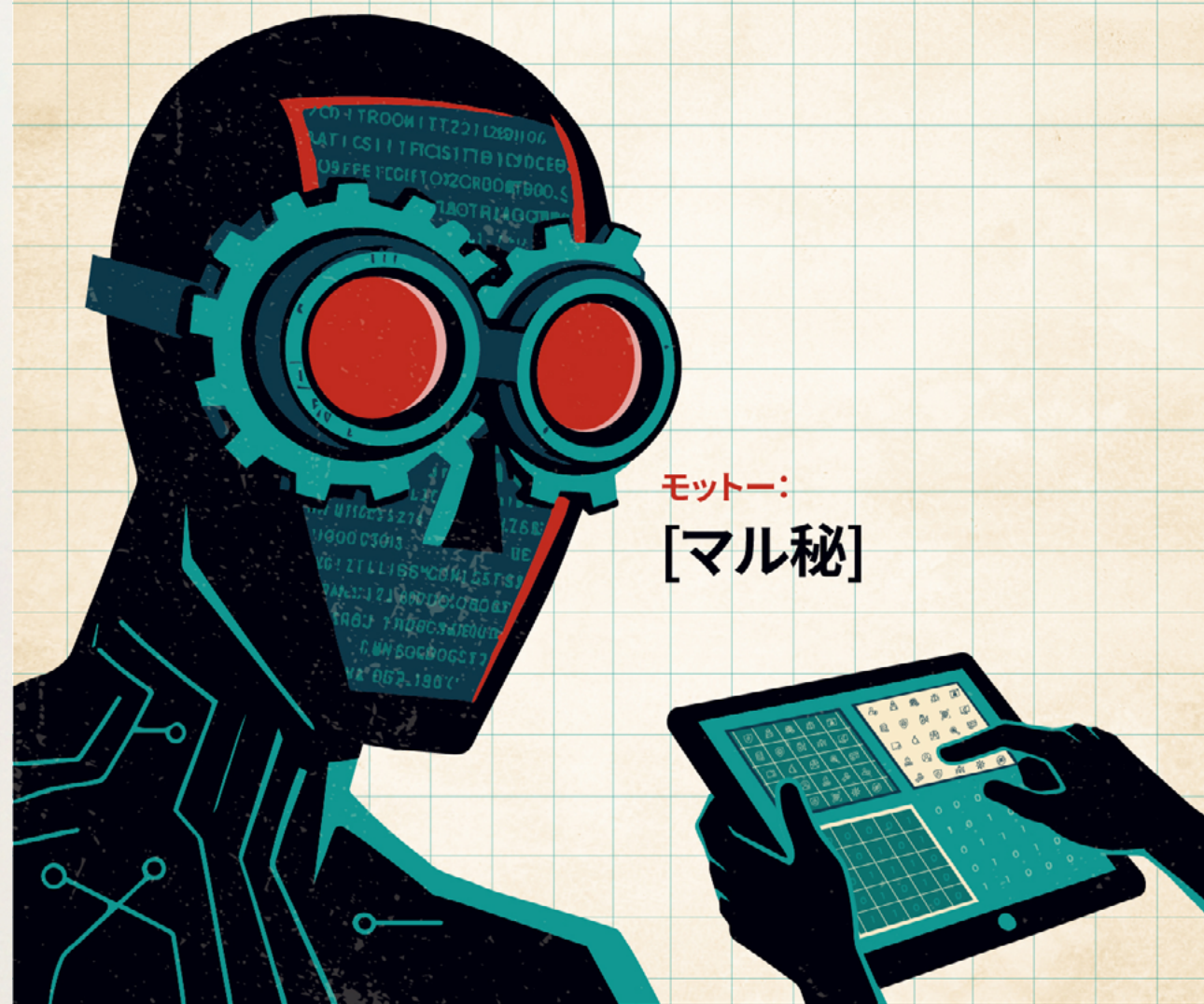
モットー：
装備を研ぎ澄ませ
そして
思考はさらに研ぎ澄ませ

役割：テクノロジー・エキスパート

専門分野：AIの安全性の確保とディープフェイクの検出

アドバイス：「緊急」を煽る不審な電話には、予め決めておいた合言葉で
相手を確認しろ

ロック・キー



モットー:
[マル秘]

職務: 暗号スペシャリスト

専門分野: パスキー、多要素認証(MFA)、暗号化

アドバイス: 単語はダメだ。自分だけの「ストーリー(文章)」をパスワードにしろ

スカウト



モットー:
データ侵害
かもしれない
そう感じたら
すぐに
報告が鉄則

職務: 現場特殊工作員

専門分野: インシデント報告・物理セキュリティ

アドバイス: 「何かおかしい」と感じたらためらわず報告しろ

チーム机上戦術シミュレーション

セキュリティ危機の発生に備え、チームの生存率を引き上げる「4つの包括的戦術シミュレーションプラン」を配備した。

技術レベルの差は問わない。本プランの絶対目標は、全作戦員の「役割の明確化」「迅速な意思決定」そして「部署を超えた連携強化」だ。

対応チェックリストの優先順位付けから、予測不能なアクシデントを組み込んだリアリティ重視のシミュレーションまで、多彩なアクティビティを用意している。

実地演習と徹底的なアフターアクション(振り返り)を通じて、インシデント発生時のレスポンス手順、部門間コミュニケーション、そして変化する戦況への適応力を骨の髄まで叩き込め。

現場での装備(アセット) 活用例:

1. マネージャーの初動対応ガイド:

支給された装備(アセット)と指示書を各部署のリーダーへ共有せよ。

各部署に最も関連性の高いトピックを1つ選ばせ、週次ミーティングの場を借りて「30分間のセッション」を執り行わせるのだ。

2. リモートワークを標的にしたサイバー攻撃:

リモートワークが大半を占める職場では、10月の定期的な全社ビデオ会議で、机上演習教材のシナリオカードのセクションをアンケート形式の質問として活用し、簡単な小テストを実施せよ。前週の結果を翌週の会議で話し合い、従業員(エージェント)がどれだけ成長したかをしっかり見定めろ。

3. インスタントメッセージ「きみならどうする?」

毎週決まった作戦曜日を選び、社内チャットの「セキュリティチャンネル」にシナリオカードを1枚投下せよ。カードに対し、脅威の本質と正当な対処法をスレッド内で真っ先に解説し、見事「インシデント報告」を完了させた最速の従業員(エージェント)には、組織の規定に基づき特別報酬(テーマに応じたインセンティブ)を授与する。

WRDエキスパートたちからのアドバイス: キャンペーン戦略

表舞台に立つことは滅多にないが、WRDのバックボーンを支える科学者や研究者たちは、その道を究めた超一流の頭脳集団だ。

本アセットを生み出した彼ら専門家たちは、組織の規模を問わず、以下に示す「主要キャンペーン戦略」が圧倒的な効果を発揮することを、数々の実戦データによって実証している。

司令塔(戦術家)として思考し、現場の実行部隊として展開せよ

我々の目的は、単に知識を共有することではなく、危険な「行動」そのものを変えさせることだ。

一流のスパイ組織が、どのように多角的な裏工作を重ねて一つの『真実』を作り上げるか考えてみてほしい。

それと同じように、我々もあらゆるチャネルを駆使して包囲網を作るのだ。

1週間の中で動画、ゲーム、現場での会話など様々な手を変え、継続的に接触することで、意識せずとも身体が動く「セキュリティの条件反射」を叩き込め。

これにより、受動的だった従業員を、組織を守る『最強の防衛壁』へと変革させることができる。

あらゆる部門から協力者を募る

孤立した情報工作など、最初から破綻している。

鉄壁の防衛文化(セキュリティカルチャー)を築くには、IT部門の枠を飛び越え、あらゆる部署に協力者のネットワークを広げねばならない。

10月は人事、法務、マーケティングの懐へ潜り込み、味方を増やせ。自分たちがWRDの存亡を握る重要人物だと分からせるのだ。

どこの誰とも知らん「IT担当者」の小言など誰も気にとめない。だが、毎日顔を合わせる「信頼できる同僚」からの警告なら、誰だって本気で耳を傾ける。

ミッション遂行に不可欠な情報を優先する

「必要だから」と大量の情報を一度に現場へ投げつけるのは愚策だ。従業員(エージェント)たちがパンクし、ボタンを無感情に連打する消化試合が目に見えている。

組織の急所となる最大の弱点を2つか3つに絞り込み、そこを徹底的に叩け。

フィッシング対策からAIの脅威、パスワード管理、インシデント報告まで、用意された毎週のミッションは、奴らの生存能力(スキル)を高めるためのものだ。余計なノイズは削ぎ落とし、目の前の標的に集中させる。深い情報は、次の戦いまで引き出しにしまっておけばいい。

本キットは全体トレーニングの「身代わり」ではないが、使い方次第で現場の防衛力を爆発的に跳ね上げる劇薬となる。

ミッションごとの内訳

これまでに、週ごとの戦術コンテンツ、推奨される戦術レポート、および連動する作戦通達（メール）の概要を提示した。
ここまで読み進めた諸君の脳裏には、今月どのように前線を動かすべきか、すでに明確な作戦プランが描かれているはずだ。
どのような戦術を展開するにせよ、作戦開始日である10月1日、あるいはその直前となる9月最終週の時点で、全エージェントへ「ミッション開始通達」を発信せよ。
以下に、前線へ打電すべきサンプル通達文（メール）を配備する。現場に合わせて調整のうえ、発信せよ。

件名の例：

[ミッション開始] ワークフォースリスク特命チームに配属されました

2026年 サイバーセキュリティ意識向上月間 | ミッション開始

knowbe4

ワークフォースリスク特命チーム
初回の情報共有

CONFIDENTIAL

TOP SECRET

CONFIDENTIAL

エージェント各位。

我々が生きるこのサイバー世界において、諸君らは常に敵の最優先ターゲットだ。しかし同時に、組織を守り抜く『最強の最終防衛線』でもある。

AIを用いたディープフェイク、巧妙化を極めるソーシャルエンジニアリング、ネットワークの暗闇に潜む未知の脅威——これらを打ち破れるのは、研ぎ澄まされた警戒心と、高度な訓練を経た作戦員だけだ。

この戦場はあまりに過酷であり、孤立無援で挑むべきではない。故に我々は、諸君の戦力を底上げするための「特別ブリーフィング」を敢行する。

ミッション概要：
本日より全員を「ワークフォース・リスク特命チーム（WRD）」へと配属する。

これからの1か月間、組織の防衛線を支える「4人のスペシャリスト」から直々に教導を受けること。

4週間に及ぶ連続ミッションに備え、即座に装備を整えよ。毎週、諸君がマスターすべき新たな戦術ノウハウが解禁される。

一瞬の油断が命取りとなる。今月の重点テーマである[※予定している活動やテーマを挿入]に向け、警戒レベルを極限まで引き上げる。

作戦に関する質問は、直ちに作戦本部（[※連絡先を挿入]）へ連絡のこと。

最初のブリーフィングは月曜日に発令される。待機せよ。諸君の健闘を祈る。

フィッシングと ソーシャルエンジニアリング

一流の工作員（スパイ）は、力任せに扉をこじ開けたりはしない。
彼らは巧妙な話術によって、内部の人間自ら鍵を開けさせるのだ。
今週は、強固なシステムフィルターすら潜り抜ける「ソーシャルエンジニアリングの違和感（レッドフラッグ）」と、それらを見破るための防衛術に焦点を当てる。
今週配備された戦術アセットの概要は以下の通りだ。

トレーニングモジュール - スミッシング・フレンジー

手元の端末（SMS）を狙う「スミッシング攻撃」の極めて高い危険性を解説せよ。

巧妙化するサイバー攻撃の新たな『犠牲者』とならぬよう、敵の襲撃パターンと自己防衛プロセスを7分間で叩き込む。

学習内容：

- サイバー犯罪者がテキストメッセージを通じてソーシャルエンジニアリングをどのように悪用するか
- スミッシングの典型的な手口

アセットを利用する

机上演習アセット - フィッシングおよびホエーリング攻撃を見抜く

本演習を通じて、作戦員たちに高度なフィッシングおよびホエーリング（幹部狙い）攻撃を識別し、正確に対処する能力を授ける。
今回展開するのは「CEO詐欺メール」の模擬シミュレーションだ。AIによって完璧に仕組まれた偽装と、その裏に潜む『真の違和感（行動上の警告サイン）』を見極める眼を養え。
偉い役職だろうと新兵だろうと関係ない。全作戦員がクリティカル・シンキングを研ぎ澄ませ、WRDの正式な防衛手順を即座に実行できるよう設計されている。

ダウンロード用アセット（2点）

- 詐欺にあわないために：受信したフィッシングの報告 - フィッシングメールの一般的な手口や、フィッシングの疑いがある場合の対処法をまとめたポスター形式の注意喚起
- インターネットセキュリティにおけるあなたの役割 - 最も一般的なサイバー犯罪の手口と、それを回避する方法をユーザーに伝えるインフォグラフィック形式の資料

第1週目のアセット

コンテンツの共有

今週の戦術モジュールを前線へ展開する際、潜入と欺瞞のスペシャリスト「ゴースト」の名で打電できるメールテンプレートを配備した。

件名の例：

[第1週目のミッション]「スミッシング」の脅威を阻止する

knowbe4

「スミッシング」の脅威を阻止する

ゴースト

2026年 サイバーセキュリティ意識向上月間 | 第1週目のミッション

エージェント各位。

スペシャリスト・コードネーム「ゴースト」だ。

現在、我々が常に持ち歩くモバイルデバイス（スマートフォン）が、敵対勢力による外部干渉の直接的な標的となっている。敵の攻撃対象領域は、PCのメール受信ボックスから、手元の末端機器へ確実に広がっている。

ミッション：

即座に「スミッシング・フレンジー」ブリーフィングを開始し、完了せよ。

本モジュールは、SMSを悪用したフィッシング（スミッシング）の潜在的危険性を解説し、諸君が敵の新たな犠牲者となるのを防ぐための防衛術を授けるものだ。

本ミッションでの獲得ナレッジ：

- テキストメッセージ（SMS）を介したソーシャルエンジニアリングの手口
- 潜伏するスミッシングの典型的な襲撃パターンと見破り方

アクセスはこちら (<https://training.knowbe4.com/modstore/view/af44ce18-ea58-47c9-a352-fb1f277ec903>)

作戦行動における質問や不明な点があった場合は、直ちに本部（[※連絡先を挿入]）へ報告せよ。油断するな。安全を最優先とし、次なる作戦ブリーフィングの配信まで警戒を維持せよ。

——ゴースト、オーバー（通信終了）。

第2週

AIとディープフェイク

AIの深淵（闇）に深く踏み込み、生成AIツールを悪用して完璧なクローンや精巧なスプーフィング（なりすまし）スクリプトを生み出すサイバー犯罪の闇領域を解説せよ。

AIが作り出す完璧な虚構の前で、エージェントたち（従業員）が頼れる唯一無二の武器は、研ぎ澄まされた自身の「クリティカル・シンキング」だ。何が真実か、その眼で暴き出せ。

動画モジュール - ディープフェイクを用いたソーシャルエンジニアリング攻撃

セキュリティドラマの金字塔『The Inside Man』のキャスト陣が結集。AI音声クローンや動画ディープフェイクを駆使し、完璧な「別人」へと化けるサイバー犯罪者の最新なりすまし工作を目の前で実演する。奴らの高度な化かし合いの手口を、わずか6分間で完全に解剖せよ。

学習内容：

- ディープフェイクやソーシャルエンジニアリングを駆使し、単純な依頼を通じてサイバー犯罪者が組織の防御体制を突破する方法
- 高度なディープフェイク攻撃から自身や組織を守るために注意すべきレッドフラッグ

アセットを利用する

トレーニングモジュール - 知的財産の保護

KnowBe4 Compliance Plusライブラリから厳選配備。我々の心臓部である「知的財産（IP）」がいかに狙われ、どう守り抜くべきか。10分間でその重要性を脳裏に叩き込め。

学習内容：

- IPとは何か、その価値とは
- 知的財産を、盗用、侵害、不慮の漏洩（人工知能による利用を含む）から保護する方法

アセットを利用する

机上演習アセット - AIプロンプトの課題

本演習を通じて、無防備なAIプロンプトがもたらす致命的なデータ流出リスクを特定・排除する能力を叩き込む。参加者は実戦さながらに提示されるプロンプト群を瞬時に精査し、どれが安全で、どれが個人データや機密情報を危険に晒す「毒針」なのかを判定せよ。役職を問わず全作戦員がクリティカル・シンキングを研ぎ澄ませ、組織の「AI利用セキュリティガイドライン」を完遂できるよう設計されている。

ダウンロード用アセット（2点）とデジタルサイネージ

- **本物が偽物か。ディープフェイクを見分ける** - 実際の場面でディープフェイクを見抜くために、文脈の手がかり<4>や批判的思考を活用するよう促すポスター形式の注意喚起
- **フィッシング手口の巧妙化:AIがオンライン詐欺をどう変えているか** - AIによりフィッシング詐欺が見抜きにくくなっていることを解説するインフォグラフィック形式の資料

第2週目のアセット

コンテンツの共有

スペシャリストGadgetが作成した、今週のアセットである「ディープフェイクを用いたソーシャルエンジニアリング攻撃」モジュールを紹介するメール文例を以下にご紹介します。

件名の例:

[第2週目のミッション] ディープフェイクを見破る

knowbe4

ディープフェイクを見破る

ガジェット

2026年 サイバーセキュリティ意識向上月間 | 第2週目のミッション

エージェント各位。

スペシャリスト・コードネーム「ガジェット」だ。

我々が誇るべき進歩を遂げたAI技術が、敵対勢力の攻撃兵器として悪用されている現状には強い憤りを覚える。実際、最新のAI音声クローンや動画ディープフェイクを駆使し、経営陣や我々の同僚に化けて忍び寄る悪質ななりすまし工作が急増しているのだ。敵が求めているのは機密データと内部アクセス権だ。その奪取のためならば、役職の上下に関わらず、全作戦員が格好の標的とされる。

ミッション:
即座に「ディープフェイクを用いたソーシャルエンジニアリング攻撃」動画ブリーフィングを開始し、完了せよ。本モジュールでは、『The Inside Man』の作戦員たちが、敵がAI音声・動画技術で知人に成りすます高度な欺瞞工作を目の前で実演(デモ)する。

本ミッションでの獲得ナレッジ:

- サイバー犯罪者がAIを悪用して組織の防衛線を突破するプロセス
- 偽装を見破るための決定的な違和感(レッドフラッグ)

アクセスはこちら (<https://training.knowbe4.com/modstore/view/0451be1f-0531-4724-a664-21f109be6308>)

本ミッションに関する不明な点や質疑は、直ちに作戦本部([※連絡先を挿入])へ連絡のこと。最先端のテクノロジーを正しく理解し、これまで以上に自身の「警戒の刃」を研ぎ澄ませ。次なる作戦ブリーフィングの配信まで待機せよ。

——ガジェット、オーバー(通信終了)。

第3週

データセキュリティとパスワード

現代の戦場において、機密データは「金」そのものだ。そして敵対勢力は、それを強奪するためならあらゆる手段を講じてくる。

作戦員(従業員)各自が、自ら防衛しているアセットの絶大な価値を自覚し、万一の漏洩時にいかなる破滅がもたらされるかを完璧に叩き込むことが不可欠だ。

今週は、パスワードマネージャーと多要素認証(MFA)を高度に連携させ、仮に作戦員の個人の防衛線が突破(侵害)されたとしても、組織のコアデータは堅牢な暗号化によって死守される仕組みを解説する。今週のアセットの概要は以下の通りです。

モバイルファーストのトレーニングモジュール - 強固なパスワード、安全なアカウント

手元のモバイル端末から数分でアクセス可能なショート演習。業務(ミッション)領域のみならず、プライベート領域も含めたパスワード/パスフレーズの鉄壁な管理がいかに重要であるかを解説する。5分間の受講で、全領域の暗号防衛線を強化せよ。

学習内容:

- 強固で安全なパスワードの作成方法と、パスフレーズの効果的な活用に関するヒント
- アカウントのセキュリティを脅かすよくあるミスを防ぐ方法
- パスワードおよびパスフレーズのセキュリティに関するベストプラクティス

アセットを利用する

机上演習アセット - パスワード推測ゲーム

本演習において、作戦員(従業員)たちには自ら「ハッカーのロール(役)」を演じてもらい、無防備なパスワードを解読する側へと回ってもらう。

攻撃手法は、SNSの投稿分析などインターネット上に転がるOSINT(公開情報)の収集・分析のみだ。デジタル空間に露出した些細な痕跡から、標的のパスワードを読み解いてみせよ。

ネット上のデジタルフットプリントと脆弱なパスワードの組み合わせがいかに危険か、そして攻撃者がブルートフォース(総当たり)攻撃等を仕掛けてアカウントを容易に掌握する「敵の手口」を、身をもって体感せよ。

インシデント報告

ワークフォース・リスク特命チーム (WRD) において、現場 (前線) の発する微細なシグナルに常に耳を澄ますことは、作戦の成否を分ける極めて重要な任務だ。どんな優秀なエージェントであれ、単独でこの広大な戦場 (サイバー空間) を守り抜くことは不可能である。故に「わずかな違和感であっても、即座にチームへ共有・打電する」という徹底された報告規律が欠かせない。今週の最終ミッションは、不審な異変を察知した際、躊躇なく支援 (バックアップ) を要請し、迅速に通報・連携するプロセスを全作戦員に完全マスターさせることだ。

オーディオキャスト - ハッキングに負けない習慣：報告

5分と10分の2部構成で贈る、15分間の音声無線通達 (オーディオキャスト) だ。敵の影を感じた時に、なぜ躊躇なく通報 (SOS) を出さなきゃいけないのか——その真意を脳内に叩き込む。ハンズフリーで耳を傾け、不審な気配を即座に叩き潰す報告スキルを身につける。

学習内容：

- ・セキュリティ上の脅威に直面した際に生じる、報告を妨げる要因
- ・サイバー犯罪対策において報告が重要である理由
- ・状況を分析し、安全な行動を選択するために活用できる意思決定プロセス

パート1にアクセス

パート2にアクセス

ゲーム - プライバシーの追求

地球の裏側まで飛び回る、15分間のスリリングな潜入ミッションだ。ゲームを進めながら、世界各国の複雑なデータプライバシー法を攻略し、いかなる法規制の網 (コンプライアンス) にも引っかからない真のノウハウを身につける。

学習内容：

- ・データプライバシー規制の重要性
- ・データプライバシーに対する地域別および国際的な取り組みの違い

アセットを利用する

ダウンロード用アセット (2点) とデジタルサイネージ

- ・ 強固なパスワードでオンラインでの安全を強化 - 強固なパスワードの重要性に焦点を当てたポスター形式の素材
- ・ 機密データ: 安全な保管とは - 密情報のセキュリティ確保の基本と、その必要性を解説したインフォグラフィック形式の資料

第3週目のアセット

コンテンツの共有

今週のトレーニングモジュールを共有する際に使用できる、スペシャリスト Lock and Keyからのメール文例を以下にご紹介します。

件名の例：

[第3週目のミッション] Vault (ボールド、保管庫の意味) を安全に守る



保管庫を安全に守る

2026年 サイバーセキュリティ意識向上月間 | 第3週目のミッション

エージェント各位。

先日、当組織のスペシャリストがとある領域への潜入 (侵入) を試みたが、厳重な暗号鍵によって見事に阻まれ、作戦は失敗に終わった。

—— そう、機密資産の安全性は、それを施錠する「鍵の強度」にすべてがかかっているのだ。今一度、パスワード管理の基本原則へと立ち返れ。「新人教育のレベルだ」と高を括ってはいならない。どんなに最新鋭の最高級金庫を構えようと、扉が開いたまま (パスワードがずさん) であれば、何の役にも立たないのだから。

ミッション指示：

モバイル対応モジュール「強力なパスワード、安全なアカウント」を開始し、受講を完了せよ。従来のパスワードを凌駕する「パスフレーズ」の圧倒的アドバンテージと、セキュリティの致命傷となり得る典型的なミスを排除するプロセスをマスターせよ。

本ミッションでの獲得ナレッジ：

- ・ 難攻不落なパスワードの構築法と、パスフレーズの効果的運用術
- ・ アカウント侵害を招く「よくある脆弱な設定」の回避アプローチ
- ・ パスワード&パスフレーズ管理におけるグローバル・ベストプラクティス

アクセスはこちら (<https://training.knowbe4.com/modstore/view/c0ee0966-ff3a-4fc2-93bb-2a632811140b>)

本ミッションに関する不明点、質疑は、作戦本部 ([※連絡先を挿入]) まで送信のこと。最後に、作戦行動において『ロード・オブ・ザ・リング』に出てくるお気に入りのセリフを諸君に贈る。『隠しておけ。安全な場所に。』(Keep it secret, keep it safe.)

—— ロック・キー、オーバー (通信終了)。

机上演習アセット - インシデントレスポンス

組織に忍び寄る「セキュリティ上の危機」を想定し、全作戦員を対象とした包括的な机上戦術演習を敢行する。

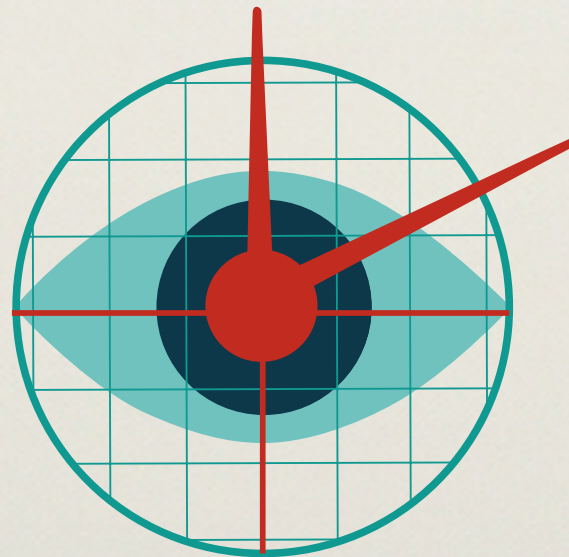
ITや技術の習熟度は問わない。全作戦員が自らの役割を明確にし、迅速な意思決定と部署の垣根を越えた高度なチーム連携を叩き込む。

実戦的なシナリオ演習と体系的なアフター・アクション・レビュー（事後振り返り）を通じ、有事における「公式インシデント対応手順」の完遂、セクション間連携、そして不測の事態にも屈しない「柔軟な現場即応力」を血肉とせよ。

ダウンロード用アセット（2点）とデジタルサイネージ

- 1回の報告で組織全体を保護 - 個人情報、同僚や顧客データを保護するために、不審なメールを速やかに報告することの重要性を強調したポスター形式のアセット
- フィッシング、物理的セキュリティ、データ漏洩 - セキュリティ上の懸念点を直ちに報告することで、小さな問題が重大なインシデントに発展するのを防げる理由を説明したインフォグラフィック形式のアセット

第4週目のアセット



コンテンツの共有

今週のオーディオキャストとゲームモジュールを共有する際に使用できる、スペシャリストScoutからのメール文例を以下にご紹介します。

件名の例：
[第4週目のミッション] チームへの情報共有

knowbe4

チームへの情報共有

スカウト

2026年 サイバーセキュリティ意識向上月間 | 第4週目のミッション

エージェント各位。

スペシャリスト・コードネーム「スカウト」よ。これより、本キャンペーンの締めくくりとなる最終状況報告と作戦ブリーフィングを執り行うわ。

私たちWRDの防衛線は、前線（現場）のリアルタイムな情勢を把握できて初めて機能するの。覚えておいてほしいのだけれど、インシデントの報告（通報）は決して仲間を売る『密告』なんかじゃない。チーム全体でその領域を警備し、悪意ある侵入者を寄せ付けないための「最重要インテリジェンス（戦術情報）の共有」なのよ。

最終ミッション指示：

以下の2つの最終プログラムを即座に遂行し、完了させなさい。

ハッキングに負けない習慣：報告の徹底 情報セキュリティの核となる意思決定プロセスを習得し、リアルタイムで脅威を解読・分析するスキルをマスターすること。

第1部はこちら (<https://training.knowbe4.com/modstore/view/ad7bb017-916b-442f-b1e7-4f96bf6b202f>)

体験型演習「プライバシーの追求」バーチャルで世界中を駆け巡り、グローバルなデータプライバシー保護の実践ナレッジをテストしなさい。

第2部はこちら (<https://training.knowbe4.com/modstore/view/a5ec90a8-956b-4675-8c63-c336812752e7>)

作戦に関する疑問は、直ちに作戦本部（[※連絡先を挿入]）まで連絡を。

WRD全チームを代表して、諸君の健闘に敬意を表するわ。

——スカウト、これより撤収するわ。オーバー（通信終了）。

ミッションの事後報告：

ワークフォースリスクを 常に念頭に置く

WRDの責任者チームは、このミッション資料や提供されたアセットが、皆様のチームにあらゆる種類のサイバー脅威を撃退するために必要なスキルやツールを提供する一助となることを願っています。

強固なセキュリティカルチャーを確立・維持することは、今も継続するミッションです。真の意味での前向きな行動変容とは、最大の攻撃対象である従業員を最大の資産へと転換し、それによって従業員に関連するリスクを低減させる戦略を意味します。

セキュリティ意識の向上やトレーニングに向けた包括的な取り組みを補完するものとして、これらのアセットをご活用ください。また、ご興味をお持ちいただけましたらぜひお問い合わせください。貴社内での次のステップをKnowBe4がどのようにサポートさせていただけるかをご提案いたします。

サイバーセキュリティ意識向上月間を通じて、貴社に役立つ情報やアセットを配信しています。ぜひソーシャルメディアで @KnowBe4 をフォロー・メンションしてください。ハッシュタグ #CyberAware でも、サイバーセキュリティ意識向上月間の最新情報をご覧ください。



knowbe4