SECURITY AWARENESS / 導入検討ガイド

知っている、から。
気づき、話し、行動できるへ。



対話と推理で学ぶ、体験型セキュリティ研修

社内の意識づくりが必要な理由、体験を行動につなげる考え方、BlueRabbitの研修内容・費用を、社内提案に使える一冊にまとめました。

経営者・管理職・人事 / 研修担当・情報システム担当の方へ
2026年11月4日版 / 表紙イラストは研修のイメージです。

01 / なぜ今、意識づくりが必要か

サイバーリスクは、
現場の判断ともつながっている。

IPA「情報セキュリティ10大脅威 2026」では、組織向けの1位にランサム攻撃、2位にサプライチェーンや委託先への攻撃、3位にAI利用に伴うサイバーリスクが挙げられています。[1]

業務を止めないために

異常を感じたとき、どこへ何を伝えるか。現場からの早い相談が、組織として判断する入口になります。

取引先との信頼を守るために

自社の情報だけでなく、取引先から預かった情報も扱っています。共有方法や権限の確認を、担当者任せにしないことが大切です。

AIを安心して使うために

便利さと情報管理を両立するには、入力してよい情報や確認先を、日常業務の場面で理解する必要があります。

上記はIPAの脅威整理を踏まえた81合同会社の研修上の論点です。意識教育は、更新・認証・バックアップ等の技術対策と組み合わせて進めます。

02 / 体験型で学ぶ意味

自分で判断した経験を、明日の行動へつなぐ。

01 役割を持つ

物語の当事者として考えることで、「自分ならどうするか」を言葉にする機会をつくります。

02 情報を持ち寄る

参加者が異なる情報を持って対話します。思い込みや伝達の不足に気づき、確認・相談する過程を体験します。

03 振り返って意味づけする

判断の理由を共有し、必要な知識を補います。体験と座学を結びつけ、自社の仕事に置き換えて考えます。

04 行動を一つ決める

「不審な依頼は別の経路で確認する」など、明日実践する行動と相談先を具体化します。

政府のセキュリティ施策ポータルでも、JNSAの教育ゲームが、安全に試行・失敗できる体験学習として紹介されています。[2] BlueRabbit自体の効果を検証した資料ではありません。定着率の数値や座学に対する優越性を保証するものではなく、振り返りと継続実践による定着を目指します。

03 / 対話・推理・振り返り

BlueRabbitの研修設計

サイバー攻撃事件を題材に、参加者が登場人物の役割と異なる情報を持ち、対話と推理を進める出張型・対面研修です。

導入・ルール説明 | 15分

目的を共有し、進め方を確認。初めての方も参加しやすいように説明します。

BlueRabbit本編 | 120分

情報を持ち寄り、問いを立て、判断する体験。個々の気づきをチームで共有します。

座学・振り返り | 30〜90分

体験を整理し、報告・相談、情報共有、生成AIの情報管理等の課題につなぎます。

アクションプラン | 15分

自社で変える行動を決めます。合計180〜240分（休憩を除く）です。

対象者や目的に応じて、座学・振り返りの内容を調整します。研修後の運用改善など追加支援は、別途ご相談・お見積りとなります。

04 / 導入の検討

社内提案に使える、
導入条件と確認シート。

5名から / 1名81,000円（税別）

5名の場合：405,000円（税別）
研修・教材・ファシリテーション・座学と振り返りを含みます。交通費・宿泊費等は個別見積りです。貴社オフィスや指定会議室で実施します。

実施前に整理すること

対象部署と参加人数 / 現在困っている場面 / 研修で変えたい行動 / 開催希望時期・会場

研修当日に持ち帰ること

気づいた思い込み / 報告や相談の障害 / 各自が実践する行動 / 部署内で確認するルール

2〜4週間後の振り返り案

行動目標を実践できたか、報告先を説明できるか、困った場面を相談できたかを確認。受講満足度だけでなく、行動の変化を見る運用をおすすめします。

実施前後の質問例：「不審なメールを見つけたら、誰に、何を伝えますか？」
同じ問いを使い、回答の具体性や相談先の理解を確認します。

05 / ご相談・参考資料

まずは、自社の課題から。

資料を読んで気になった点や、社内で検討したいテーマをお聞かせください。人数や時期が未定でも、ご相談いただけます。

BlueRabbit 公式サイト
https://blue.eightone.co/
メール：81@eightone.co

参考資料・出典

[1] IPA「情報セキュリティ10大脅威 2026」
https://www.ipa.go.jp/security/10threats/10threats2026.html
2026年の組織向け脅威の整理を参照。

[2] 国家サイバー統括室 セキュリティ施策ポータル
「情報セキュリティ教育ゲーム（JNSA）」
https://security-portal.cyber.go.jp/curriculum/torikumi/jnsa_kyouikugame.html

参照日：2026年11月4日。本文は81合同会社による要約・研修提案です。IPA・JNSA等による本研修の推薦や効果認証を示すものではありません。掲載条件は作成時点の情報です。正式な内容は個別のお見積りでご確認ください。