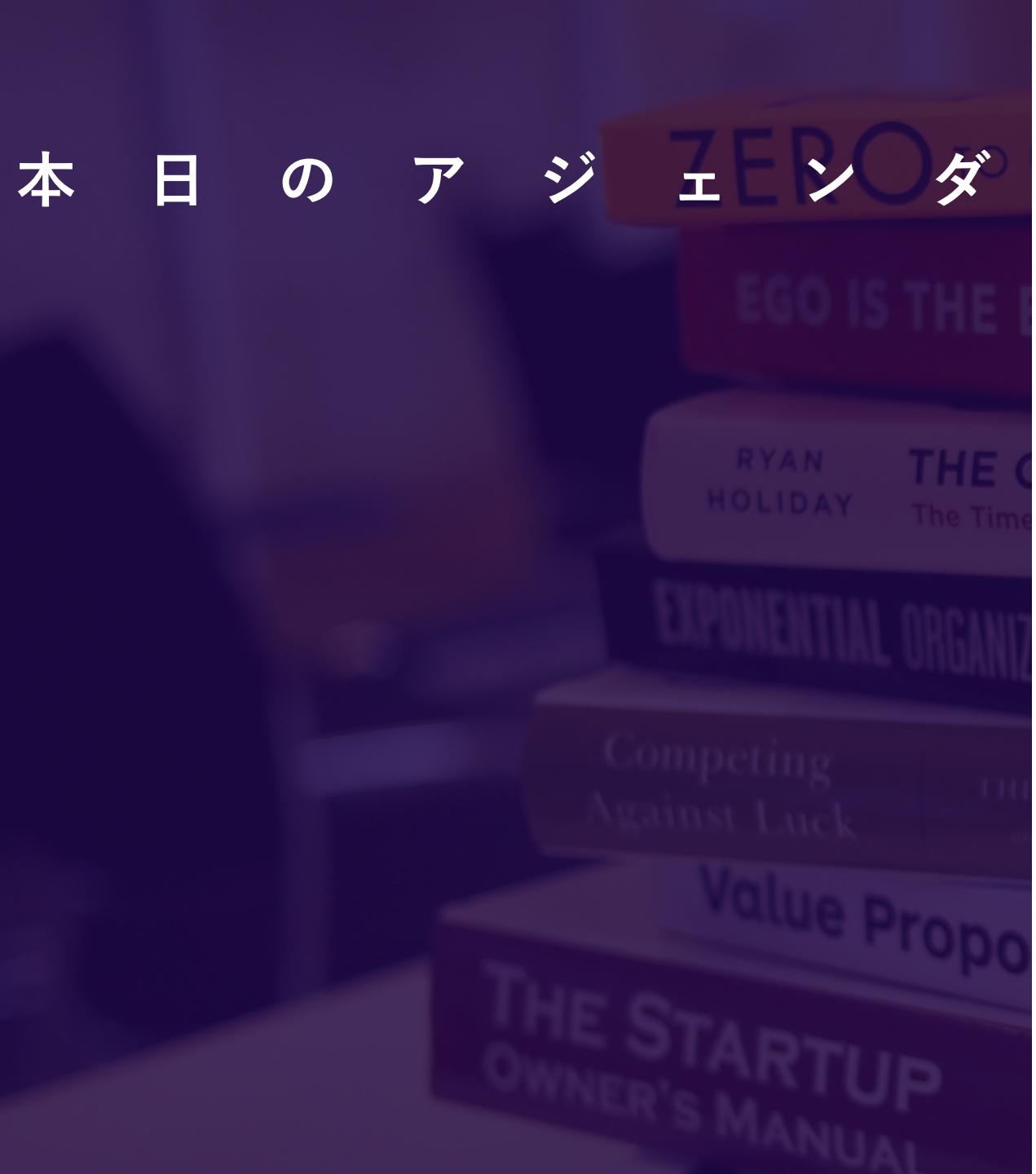
サイバー攻撃を
疑似体験してみませんか？

～ロールプレイング方式で誰でも身に付きやすいセキュリティ教育～

SECURITIER
セキュアプラクティス

２０２４年８月２８日
株式会社ハイパー
セキュリティア推進部
渡会　弘樹

本　日　の　ア　ジ　ェンダ



【1】株式会社ハイパーのご紹介

【2】教育の必要性について

【3】ロールプレイング型
セキュリティ教育ツールのご紹介

主な経歴

- ゴリゴリの新規開拓営業
- パソコン販売１０数年
- セキュリティ専門３年

渡会　弘樹（わたらい　ひろき）

出身　北海道帯広市

年齢　４６歳

特技　演説

趣味　動物の世話　※ねこを飼ってます

カラオケ　※知らないスナックを開拓

ひたすらビールを飲む

子どもと遊ぶ

主な事業

- **ITサービス事業**
  PC、周辺機器、ソフトウェア
- **アスクルエージェント事業**
  事務用品、プリンタトナー
- **サービス＆サポート事業**
  ITインフラ構築、
  システム保守
- **セキュリティ事業**
  コンサル、教育、
  プロダクト販売、導入、
  運用サービス

株式会社ハイパー

本社　東京都中央区日本橋堀留町2-9-6

設立　1990 年5 月18 日

資本金　572,374,646円（2023年12月末現在）

従業員　193人（2023年12月末現在）

関係会社

株式会社リステック
株式会社みらくる
マルチネット株式会社
株式会社メビウス
株式会社ジャスティス
司コンピュータ株式会社

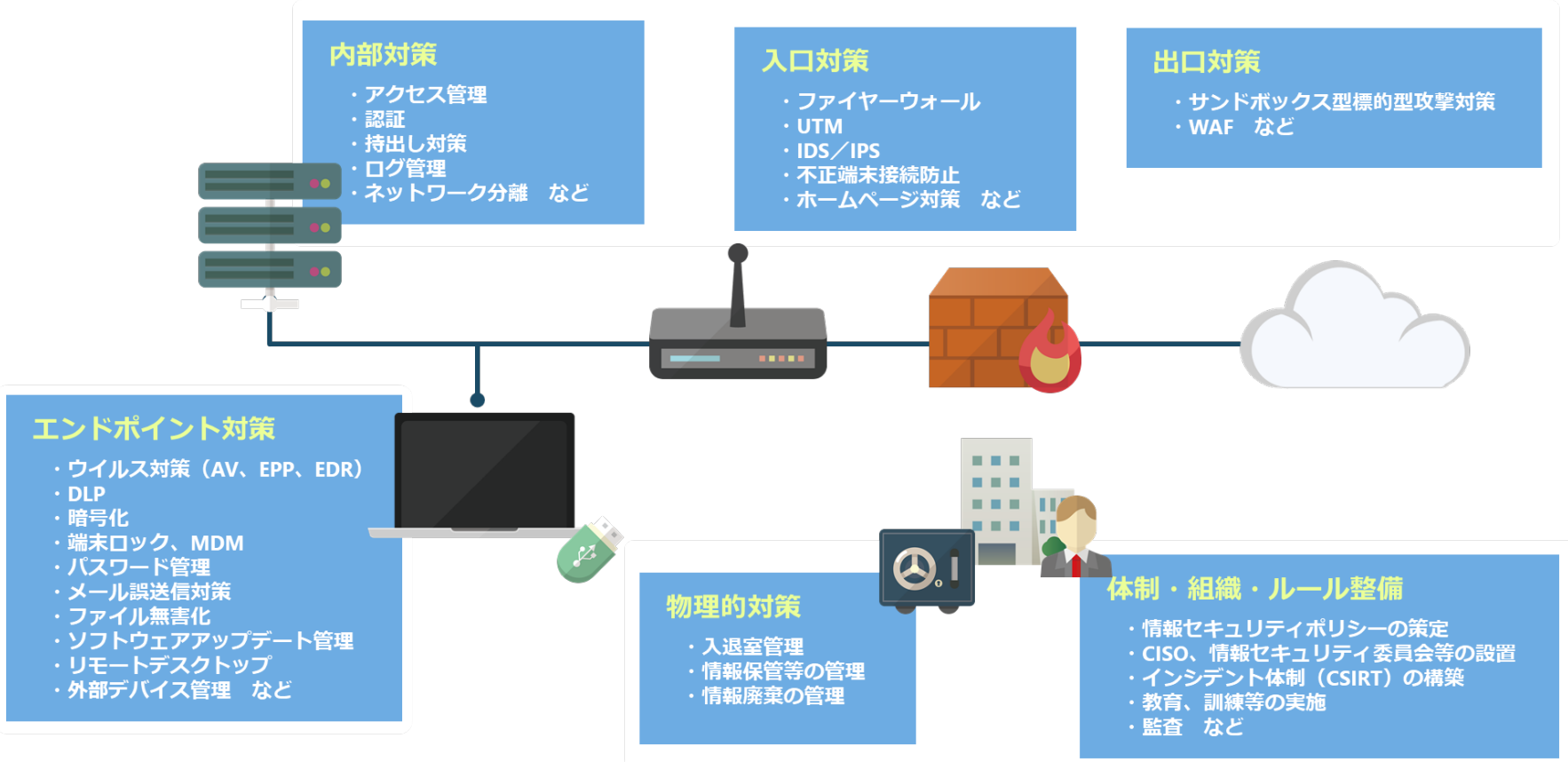
東証一部　2020年3月上場（ 現 スタンダード市場）

セキュリティ事業

セキュリティア推進部

- アンチウイルス事業
- エンドポイントセキュリティ事業
- テレワークソリューション事業
- 自治体向けソリューション事業
- 文教向けソリューション事業
- 医療向けソリューション事業
- 導入支援事業
- サポートセンター事業
- コンサル・教育支援事業

特定メーカーにとらわれない、お客様に最適な製品のご提案をいたします。



＜参考サイト＞セキュリティア特設サイト
https://www.securitier.jp/

弊社では様々なセキュリティ製品を取り扱っています

シグネイチャ検知	ふるまい検知	修復/調査/脅威ハンティング		マルウエアの隔離
EPP (End Point Protection)	**NGAV** (Next Generation Anti-Virus)	**EDR** (Endpoint Detection and Response)	**MDR** (Managed Detection and Response)	**Isolation**

TREND MICRO
ESET
WEBROOT SecureAnywhere
HP WOLF SECURITY
vmware Carbon Black Cloud™
CROWDSTRIKE
cybereason
SOCサービス
SOPHOS XDR MDR
HP Sure Click Enterprise powered by Bromium

NDR (Network Detection and Response)	PPAP対策	GATEWAY	SASE (Secure Access Service Edge)	MFA (Multi-Factor Authentication)	BackUp

DARKTRACE
メール de ファイル
Securemail Plus Filter
CHECK POINT
MRB-cloud
iboss
swivelsecure
SECURITIER CPC CYBER PROTECT CLOUD

HYPER

日本企業の情報セキュリティレベルを上げるため、頑張る企業を応援する情報セキュリティ支援サービス

セキュリティコンサル		セキュリティ診断			セキュリティ教育		
							
企業リスク診断	各種ガイドラインへの準拠監査	AI脆弱性診断	プラットフォーム診断	ペネトレーションテスト	一般社員向け教育	セキュアプラクティス	標的型攻撃メール訓練

セキュリティコンサルティングもハイパーへご相談ください。

HYPER

「ゼロ」にはできないリスク。

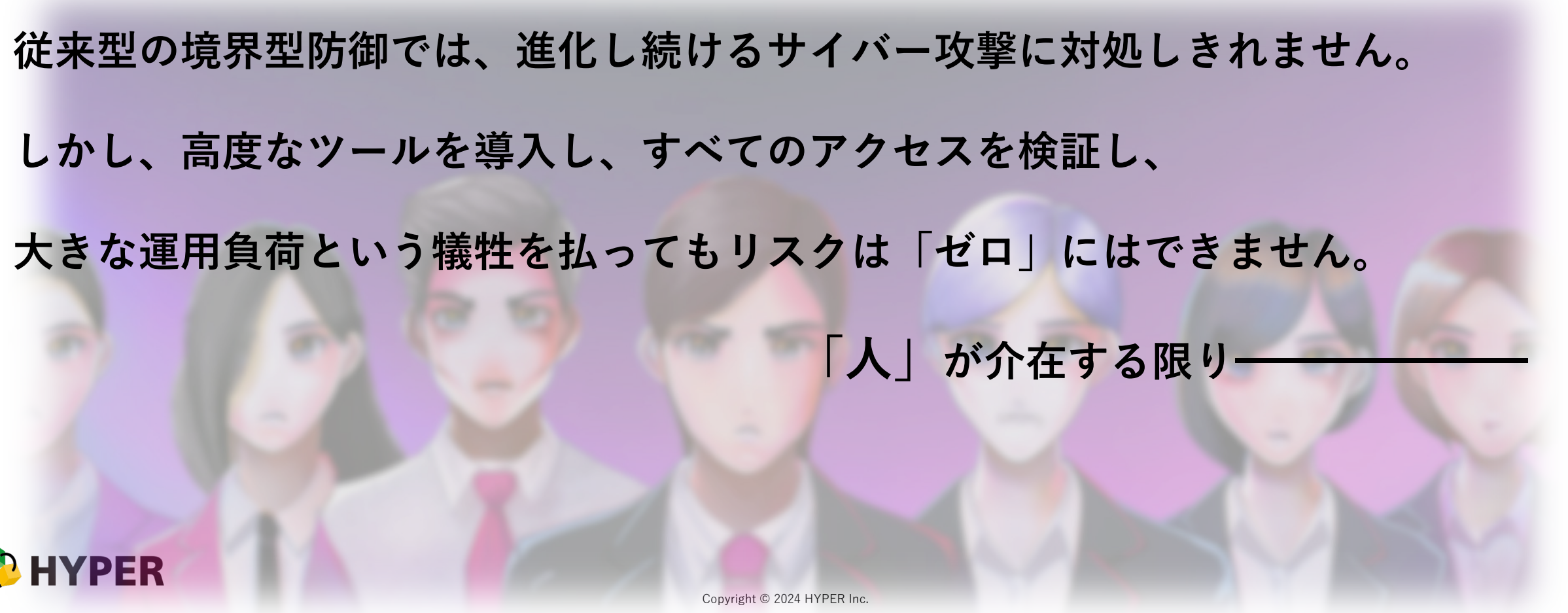
今、情報セキュリティは「ゼロトラスト」を志向しています。

従来型の境界型防御では、進化し続けるサイバー攻撃に対処しきれません。

しかし、高度なツールを導入し、すべてのアクセスを検証し、

大きな運用負荷という犠牲を払ってもリスクは「ゼロ」にはできません。

「人」が介在する限り――――――――



HYPER

ＩＰＡ　情報セキュリティ１０大脅威２０２４

順位	組織	前年順位
１位	ランサムウェアによる被害	１位
２位	サプライチェーンの弱点を悪用した攻撃	２位
３位	内部不正による情報漏えい	４位
４位	標的型攻撃による機密情報の窃取	３位
５位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	６位
６位	不注意による情報漏えい等の被害	９位
７位	脆弱性対策の公開に伴う悪用増加	８位
８位	ビジネスメール詐欺による金銭被害	７位
９位	テレワーク等の ニューノーマルな働き方を狙った攻撃	５位
１０位	犯罪のビジネス化 （アンダーグラウンドサービス）	１０位

HYPER

ＩＰＡ　情報セキュリティ１０大脅威２０２４

順位	組織	前年順位
１位	ランサムウェアによる被害	１位
２位	サプライチェーンの弱点を悪用した攻撃	２位
３位	内部不正による情報漏えい	４位
４位	標的型攻撃による機密情報の窃取	３位
５位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	６位
６位	不注意による情報漏えい等の被害	９位
７位	脆弱性対策の公開に伴う悪用増加	８位
８位	ビジネスメール詐欺による金銭被害	７位
９位	テレワーク等の ニューノーマルな働き方を狙った攻撃	５位
１０位	犯罪のビジネス化 （アンダーグラウンドサービス）	１０位

教育なしには
防ぎきることができない

HYPER

セキュリティ教育を継続する上での悩み

- ☑ 自社だけだとネタが尽きてしまう
- ☑ 座学だけだと当事者意識の醸成が難しい
- ☑ セキュリティ教育のマンネリ化
- ☑ 標的型攻撃メール訓練に課題を感じている
- ☑ 模擬訓練をしたいが、業務の妨げになるのは避けたい
- ☑ 集合型研修の実施が難しく、履修確認が難しい

ロールプレイング型セキュリティ教育

SECURITIER
セキュアプラクティス

- ☑ 実際に体験するので受講者にわかりやすい
- ☑ 管理者画面で履修状況の確認ができる
- ☑ 利用ユーザ数 無制限！ ※法人単位での利用に限る
- ☑ ユニークな体験型でマンネリ防止
- ☑ 体験後の解説までブラウザで完結できる

イーラーニングも知識学習だけでなく、経験学習の領域へ

WEB上でロールプレイング形式の「体験教育」

＜導入事例＞

『訓練の本当の目的は注意喚起と当事者意識の向上である』

継続しても人事異動や人の入れ替りなどで開封率0%を目指すのも難しく、全体への周知と開封後の行動を学ぶ方向に力を入れたい

国立大学法人信州大学

設立：昭和24年5月31日
職員数：約4,000人
学生数：約11,000人
5キャンパス8学部

過去実施した攻撃訓練での課題

- 開封率にばかり着目し、数字が独り歩きした
  ⇒集計期間中休み・見落とし・口頭で訓練を聞いた人はリテラシー関係なく開封率に反映されない
- 1種類のシナリオしか体験できない
  ⇒件名や文面によって部署に差異が生じる場合あり
- 開封しない者には注意喚起が届かない
  ⇒その時開封しなくてもいつ当事者になるかわからない
- 業務が混乱し、苦情が発生した

導入効果

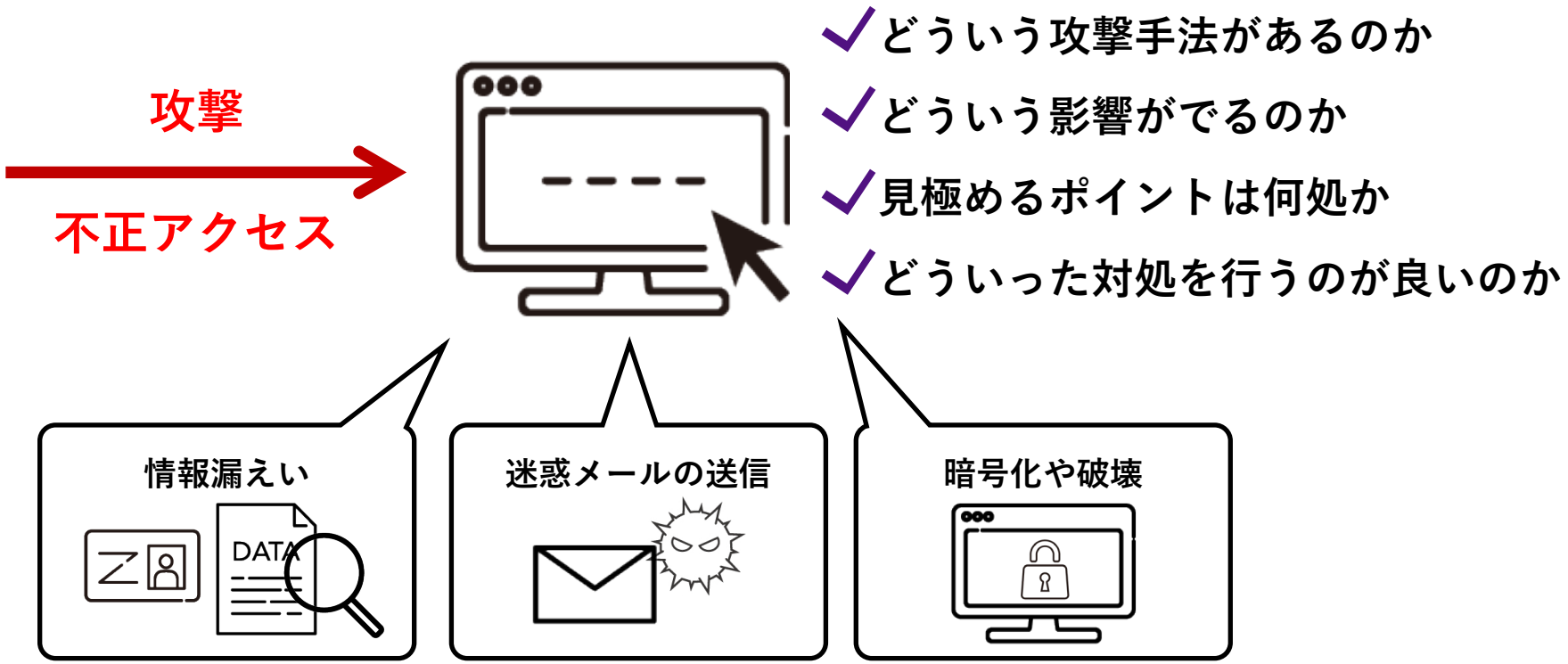
- 全学生・全職員がきちんと最後まで体験できる
  ⇒誤った操作を行わないとシナリオが進行しない仕組み
- 実環境に似た画面で体験ができる
  ⇒自大学で利用しているメールシステムに似たインターフェースを適用可能
- 本当に身になる体験ができる
  ⇒被害に遭わないための注意点やポイントをアレンジして解説
- 最新の攻撃や複数のシナリオを体験できる
  ⇒最新の複数シナリオを素早く導入可能

被害を疑似体験できるセキュアプラクティスによって当事者意識が芽生えた

セキュアプラクティスとは

▶ ロールプレイング形式の体験型教育ツール

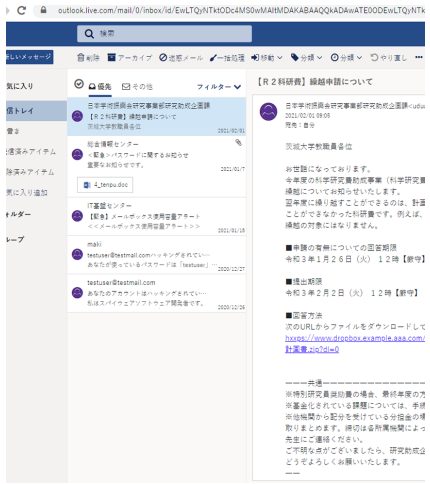
現実に近い場面を設定し、マルウェアに感染した疑似体験を通じて物事を考える際の客観性を高め、
何か事柄が起こった時に適切に対応するための力をつける効果が期待できます。



セキュリティ訓練シナリオ

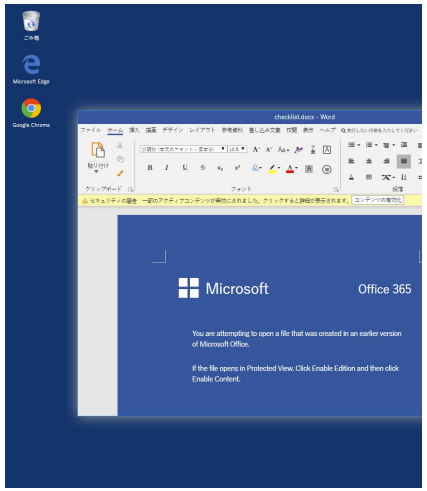
▸ シナリオ例

標的型攻撃メール

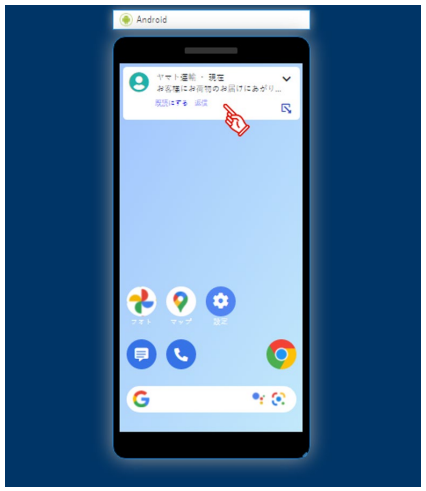


ランサムウェア

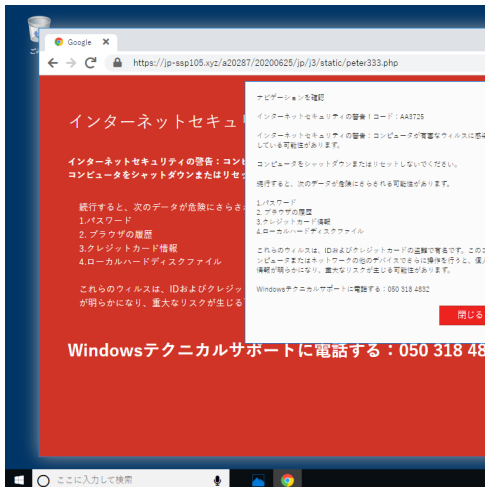
Emotet



スミッシング



サポート詐欺



（Android版 / iOS版）

今後追加予定（仮）：サプライチェーン向けランサムウェア（メールからの感染）
クラウド経由の情報漏えいシナリオ（個人のGoogleドライブを業務で利用した際の情報漏え）
サイバー攻撃基礎編（ファイル偽装）
サイバー攻撃基礎編（トロイの木馬）　等

自社の攻撃を参考にオリジナルシナリオの追加も可能

※新規シナリオの作成依頼は別途ご相談

サポート詐欺とは

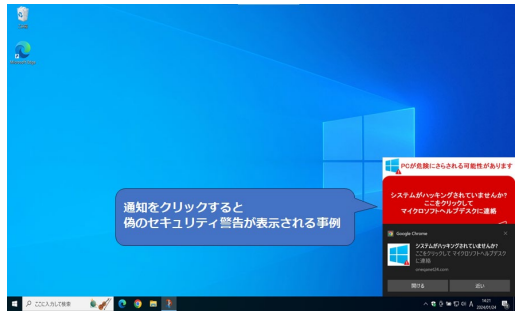
偽のセキュリティ警告を表示させ、慌てた被害者に偽のサポート窓口に電話をかけさせる
その上でサポート料金と称した金銭をだまし取る（マルウェアに感染するケースもある）

手口

警告が表示されるきっかけ

- 不審な広告のクリック
- 不審なサイトに誘導する検索結果をクリック
- アダルトサイトの動画再生ボタンをクリック
- ブラウザの通知機能を悪用した偽のセキュリティ警告通知をクリック

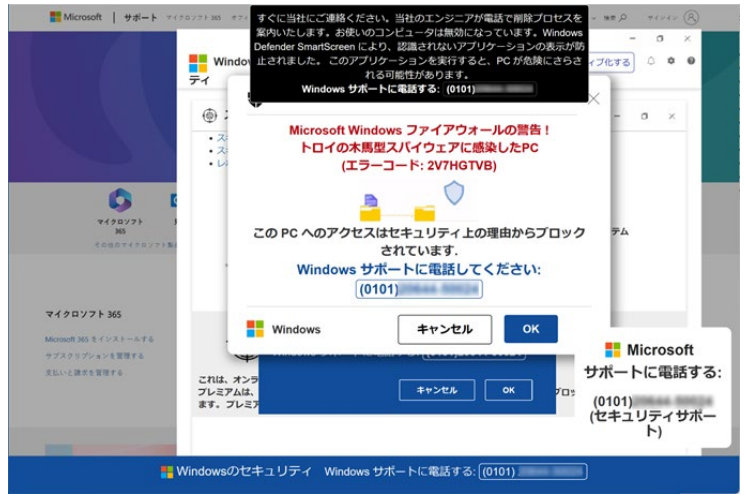
偽広告



通知機能を悪用したポップアップ

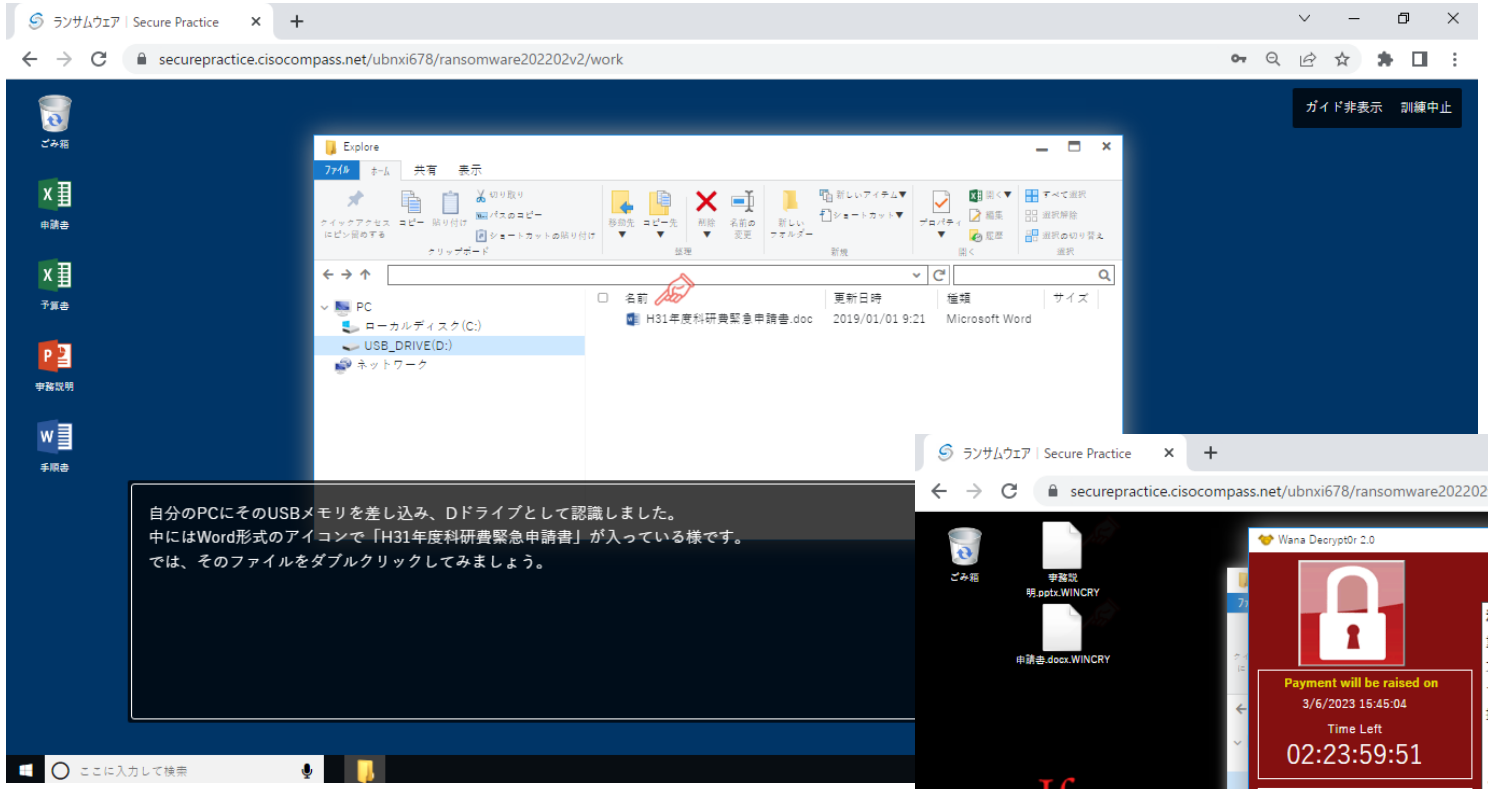
実際の企業を装った偽広告も存在している

偽の「セキュリティ警告画面」が突然表示される

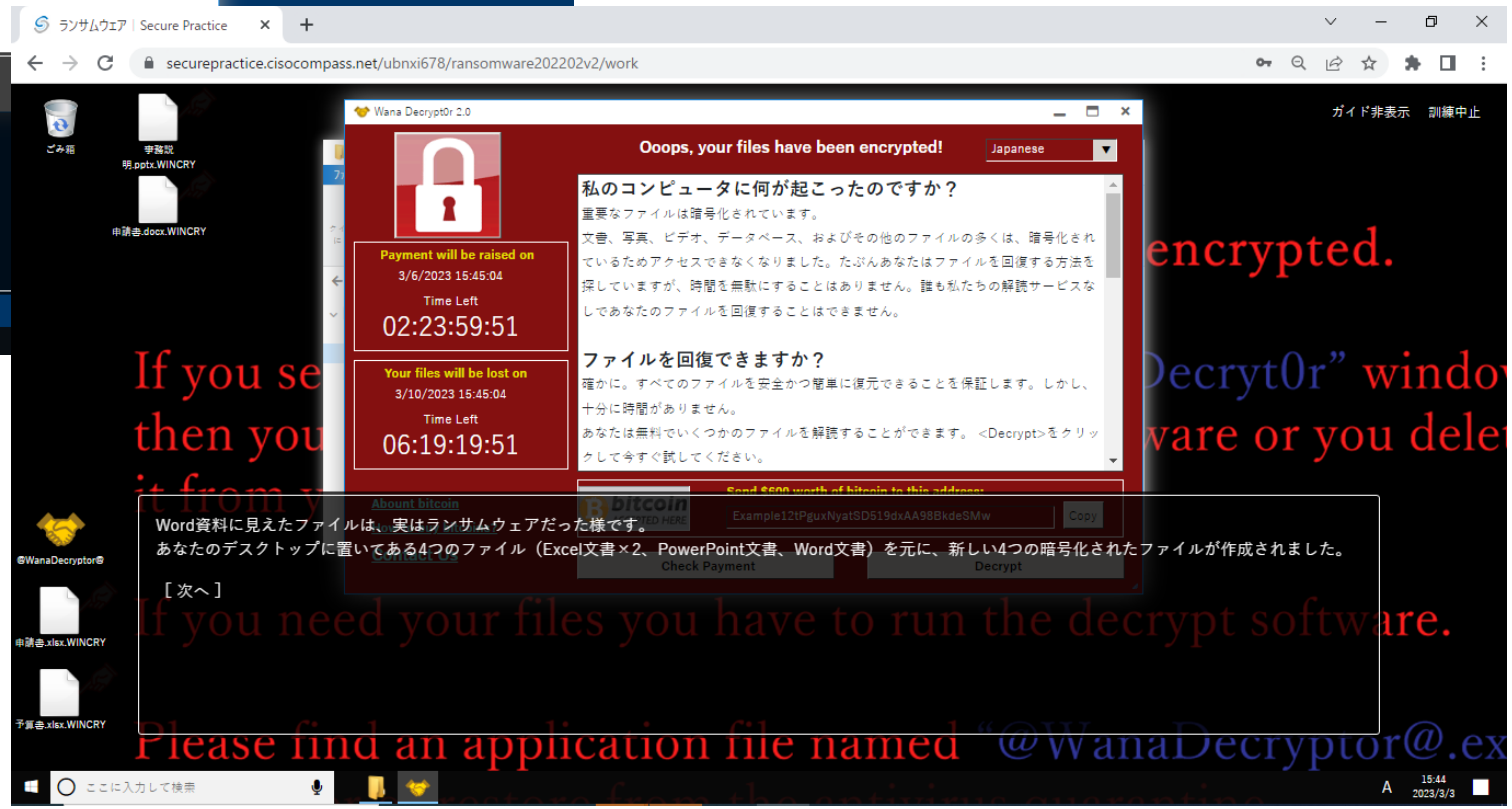


IPA：サポート詐欺の偽セキュリティ警告はどんなときに出るのか？
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20240227.html

実際の画面イメージ



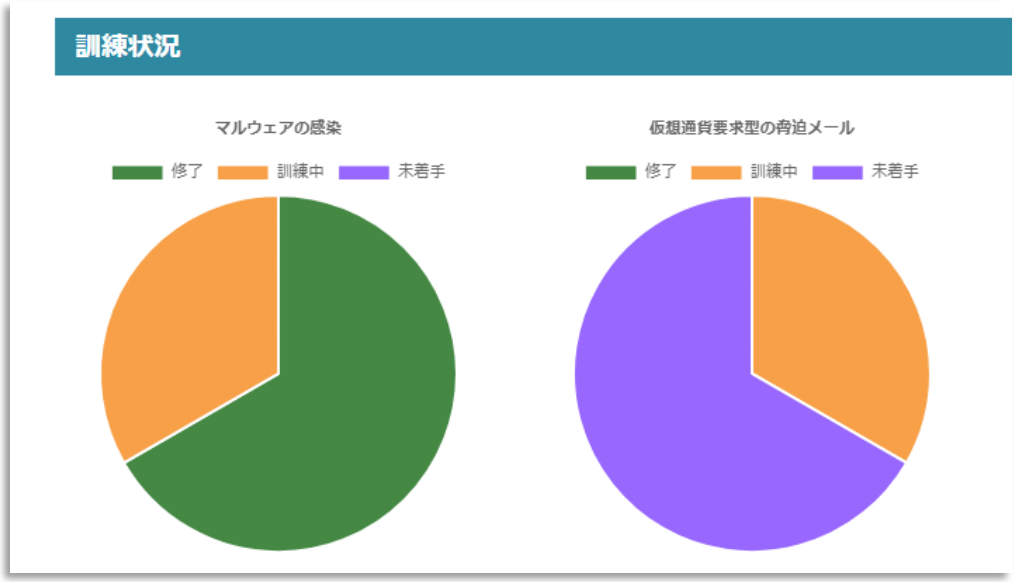
ストーリーに従って
利用者がファイルを
“ダブルクリック”すると
画面が変化



Demo

レポート/修了履歴（CSVダウンロード）

- ユーザー（管理者）がログインした際に、ポータルからアクセス可能
- レポートの表示、CSVダウンロードはシナリオ毎



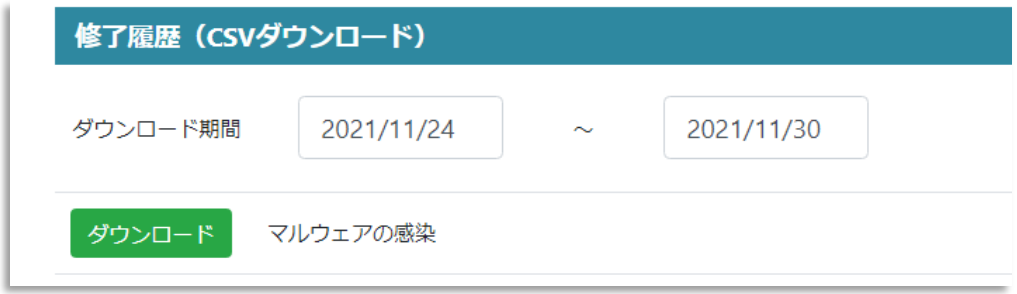
修了
そのシナリオを最後まで完了したユーザー数

訓練中
そのシナリオを開始したが完了していないユーザー数

未着手
ユーザー登録済みで、「修了」でも「訓練中」でもないユーザー数

ユーザー一括登録した場合、登録した人数に対して何人が未実施かがわかる

※自動登録の場合、レポート内での未着手人数の把握はできない



CSV出力項目
“修了日時","アカウント"

※シナリオ名はファイル名に記載

Corporationライセンス費用

年間利用料

￥600,000（税抜）

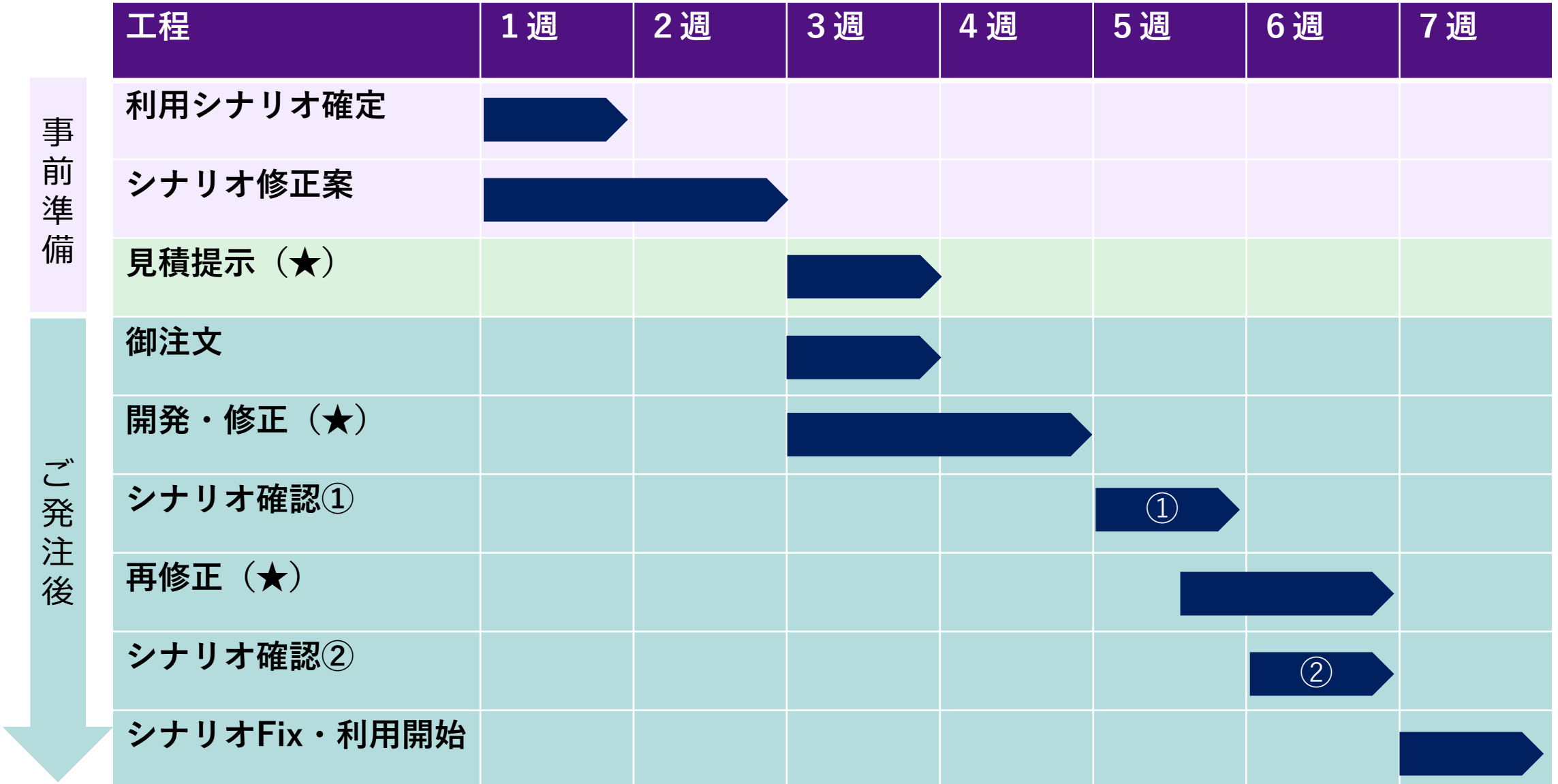
※初年度は別途初回準備作業費用（個別見積）、次年度以降は更新作業費が発生いたします

クライアント数 無制限　　期間中 いつでも 利用可能

- 利用可能コンテンツ　3点（年度毎に選択可）
- 初回コンテンツ修正 等
  - メーラー（Outlook、Gmail、thunderbird）
  - メール文面（アドレスなど）
  - ガイダンス（企業名・問合せ先など）
  - ストーリー変更

※デモサイトのご利用は営業担当にお申し付けください。
※作成するシナリオ上の社名・団体名は1種類となります。
※複数作成する場合は別シナリオとしてカウント致します。

導入スケジュール　サンプル

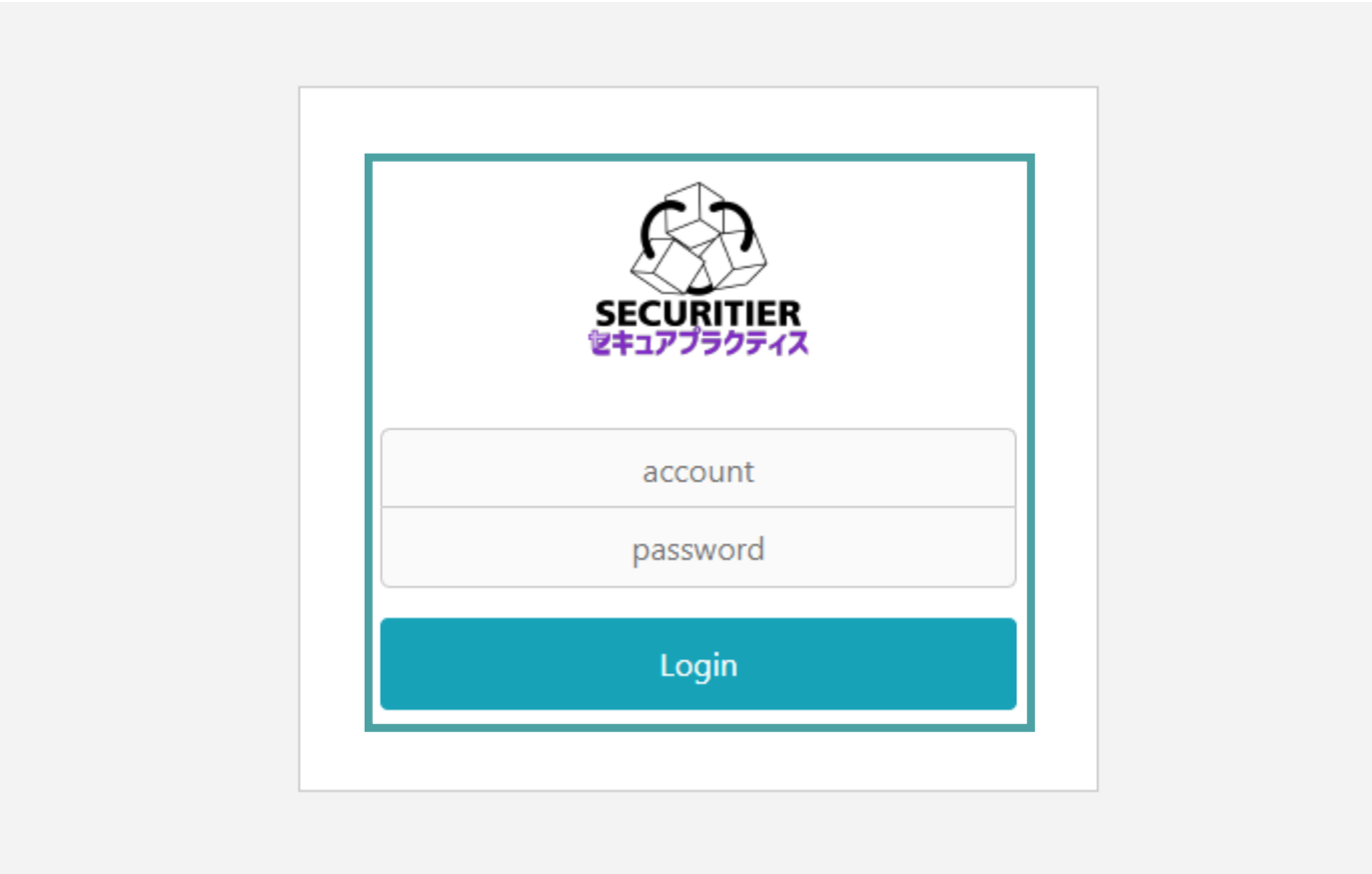


※修正・開発内容によってスケジュールは変動します　★：弊社作業

資料：画面

変更可
別途費用で変更可
変更不可

セキュアプラクティス ログイン画面



ユーザー一括登録、手動ログイン選択時のみ利用

ログイン画面はカスタマイズできません。

ポータルページ
①ホームタブ

変更可

別途費用で変更可

変更不可

ロゴの変更
※画像はご用意ください

サムネイルの並び順

「重要なセキュリティ情報（IPAより）」の表示・非表示

カスタマイズ範囲：体験タブ

変更可
別途費用で変更可
変更不可

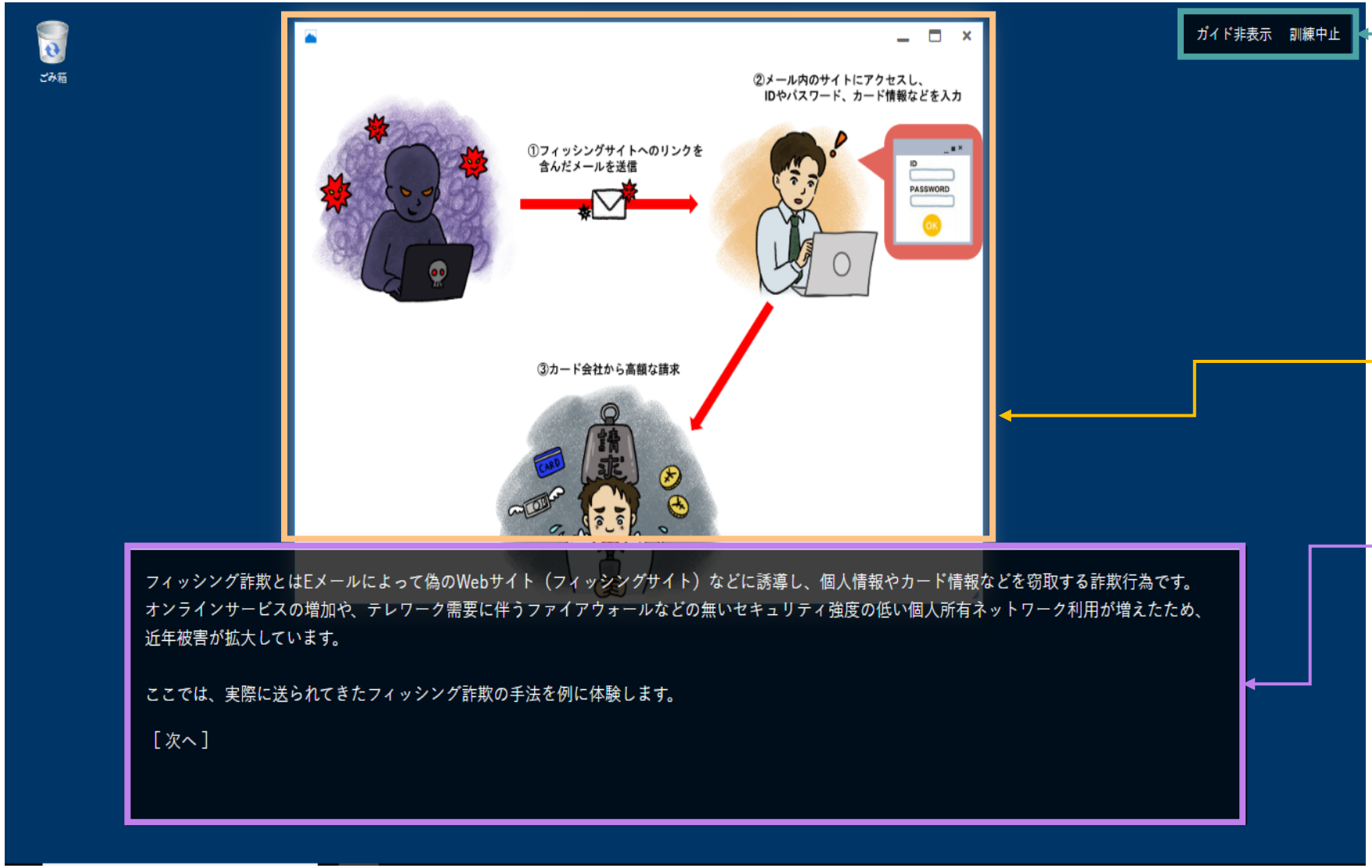
訓練名
（※「標的型メール攻撃」訓練のように同じ訓練ページから複数のシナリオが利用可能なものは、訓練ジャンルである「標的型メール攻撃」の部分）

シナリオの説明（2048文字）

訓練サムネール画像
※画像はご用意ください

シナリオ名

カスタマイズ範囲：体験ページ



変更可

別途費用で変更可

変更不可

訓練時の簡易メニュー部分

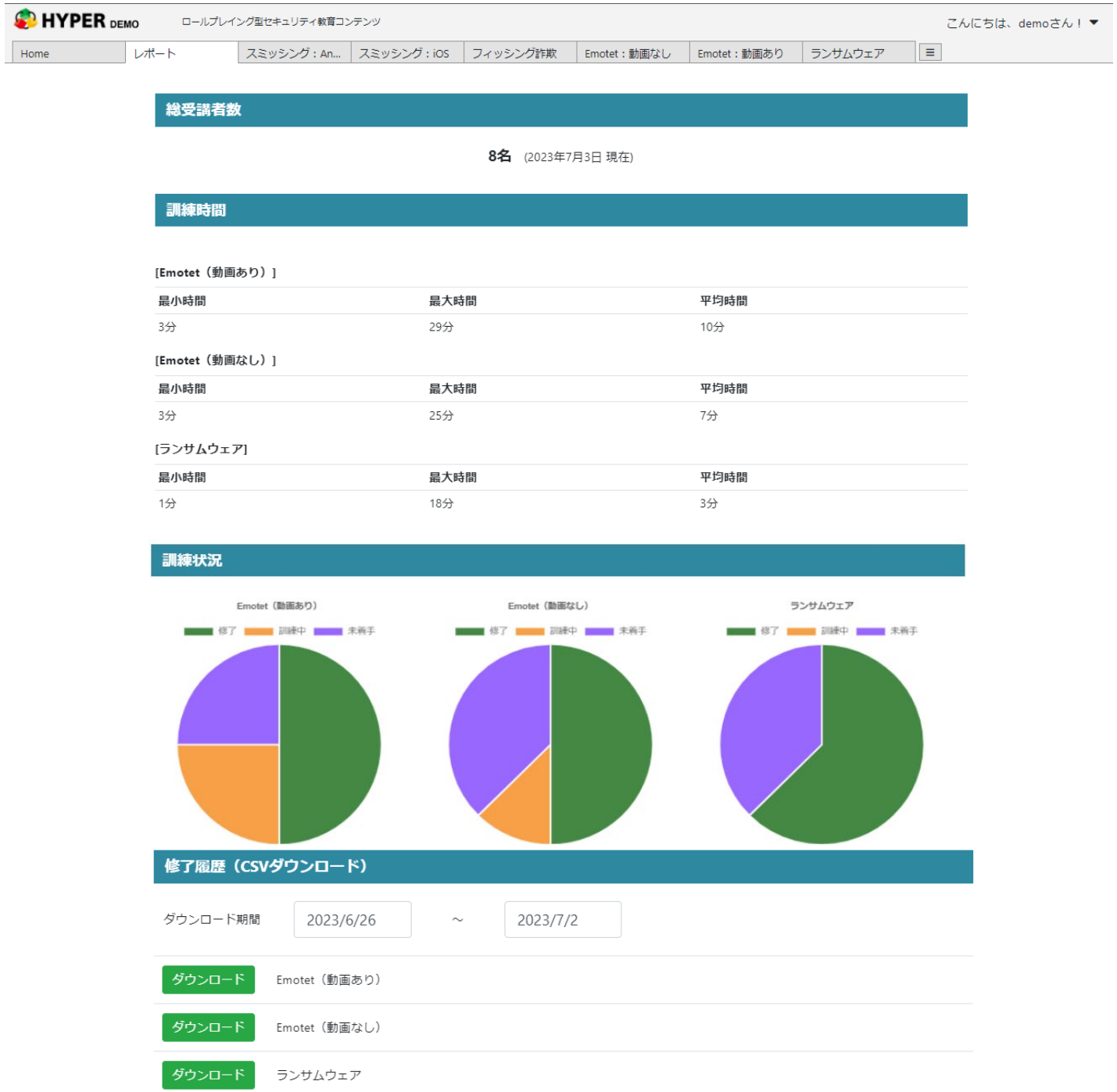
イラスト部分
画像はご用意ください

ガイダンス部分
文章（テキスト）、背景色、縦幅（px指定、最大）、表示速度
※下記変更は不可
枠色、文字サイズ、文字色、フォント、フォントスタイル、行間、文字間

その他、OSやアプリケーションを模した画面の構成や機能にかかわる部分は変更できません。

③レポートタブ
（管理者のみタブ表示）

「レポート」画面はカスタマイズ
できません。



本日のまとめ

- ☑ 体験型学習でユーザの当事者意識を醸成
- ☑ 履修確認で学習状況がわかる
- ☑ 利用ユーザ数 無制限！ ※法人単位での利用に限る
- ☑ カスタマイズによりリアリティある体験
- ☑ いつもと違う体験学習でマンネリ防止

ご提供可能な教育メニュー

▶一般社員向け教育

情報セキュリティやサイバー攻撃の基本などの教育が可能　※訪問、オンライン、eラーニング

▶標的型攻撃メール訓練

疑似的な攻撃メールを社員全体へ送付し開封率や報告体制等の実態を確認

▶体験型教育　「セキュアプラクティス」

マルウェアに感染、フィッシングサイトにアクセスする等をWebブラウザで疑似体験

▶インシデント対応トレーニング

技術者向け。インシデント対応全般（発生前～発生後）の対応の基礎を学ぶ

詳細・お見積りについては別途お打合せさせていただきます。

ご清聴有難うございました！

お問い合わせ先

株式会社ハイパー
セキュリティア推進部

TEL：03-5643-2221　E-mail：security@hyperpc.co.jp

〒103-0012 東京都中央区日本橋堀留町2-9-6 ニューESRビル