

WideAngle プロフェッショナルサービス セキュリティ教育&メール訓練のご紹介



2023年7月3日
NTTコミュニケーションズ株式会社

WideAngleとは

「WideAngle」はNTT Comが提供する
グローバル統一の総合セキュリティサービスブランドです

WIDE  ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

プロフェッショナルサービス

マネージドセキュリティサービス

WideAngleという名称には、標的型攻撃など未知の脅威に世界がさらされる中、
広い視野でリスクを見通し、より安心・安全な社会を志す開拓者でありたいという思いを込めています。
NTT Comは、WideAngleブランドのもと総合リスク マネジメント サービスを積極的に展開し、
マネージド セキュリティ サービス プロバイダー（以下MSSP）のグローバル トップ プレイヤーを目指します。

企業を取り巻くセキュリティ脅威

セキュリティ脅威と対策の状況

IPA（情報処理推進機構）の情報セキュリティ10大脅威では、メールを利用した攻撃が毎年上位にランクインしています。これに対して、IPAの情報セキュリティ白書2021では、「ビジネスパートナーや委託先を含めたサプライチェーン全体の対策」、「サイバーセキュリティ演習/訓練の実施」ができていないと回答する企業が半数以上を占めています。このことから、サプライチェーンを含めたセキュリティトレーニングの必要性があるといえます。

順位	組織	昨年 順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4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	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

出典：IPA「情報セキュリティ10大脅威2022」



出典：IPA「情報セキュリティ白書2021」

このようなお困りごとはありませんか

社員の意識向上



- ・社員、組織全体にセキュリティの意識を根付かせたい
- ・人の脆弱性を狙った攻撃が心配だ
- ・在宅環境が増え、個人のセキュリティ意識を向上させたい

導入・運用



- ・安くセキュリティ対策を始めたい
- ・セキュリティ研修に稼働をかけられない
- ・自社のセキュリティ研修が陳腐化している

社外・取引先



- ・サプライチェーン全体のセキュリティ対策を実施したい
- ・取引先からセキュリティ対策状況の説明を求められている

WideAngle プロフェッショナルサービス セキュリティ教育&メール訓練とは

サービス概要

セキュリティ教育&メール訓練は、セキュリティ意識向上トレーニングの「KnowBe4」をプラットフォームとしたサービスです。セキュリティ教育、フィッシングメール訓練、その効果測定分析を組み合わせ、社員一人ひとりに「Human Firewall」のマインドを根付かせます。

「人」をファイアウォールにすることにより、セキュリティ対策製品をすり抜けてきた攻撃を防御できるように開発された次世代の多機能統合型プラットフォームです。

Human Firewall



①トレーニング (セキュリティ教育)

- 1,200種類以上の教育コンテンツ
- 多言語対応
- 情勢に合わせたNTT Comオリジナル動画

②フィッシング (メール訓練)

- 標的型攻撃メールの訓練機能
- Phish Alert ボタンによる通知機能
- 情勢に合わせたNTT Comオリジナルメールテンプレート

③分析 (効果測定分析)

- フィッシングメール訓練結果のレポート
- 組織、部署、個人レベルでリスクをスコア化
- リスクスコアに応じた運用を自動化

サービスの特徴

特徴① トレーニングと効果測定をまとめて管理！

教育とフィッシングメールの模擬攻撃訓練、効果測定を一つのプラットフォームで提供することにより、リスクレベルを可視化し、セキュリティ意識が向上しているかどうか数値化して評価することができます。



① トレーニング (セキュリティ教育)

- 1,200種類以上の教育コンテンツ
- 多言語対応
- 情勢に合わせたNTT Comオリジナル動画

② フィッシング (メール訓練)

- 標的型攻撃メールの訓練機能
- Phish Alert ボタンによる通知機能
- 情勢に合わせたNTT Comオリジナルメールテンプレート

③ 分析 (効果測定分析)

- フィッシングメール訓練結果のレポート
- 組織、部署、個人レベルでリスクをスコア化
- リスクスコアに応じた運用を自動化

特徴② コンテンツは豊富で多言語対応！

セキュリティ講座、海外ドラマ風ビデオ、クイズやゲームなど1,200種類以上のコンテンツを用意。日本語を含む30カ国以上の多言語に対応しています。また、教育動画、フィッシングメール訓練のメールテンプレートはNTT Comオリジナルコンテンツを随時提供し日本の情勢に合ったトレーニングを提供します。



The screenshot shows the KnowBe4 ModStore interface. At the top, there's a navigation bar with the KnowBe4 logo and a 'ModStore' tab. Below the navigation bar, there's a main banner for '特集コンテンツ セキュリティトレーニング' (Featured Content Security Training) with buttons for '詳細を表示' (Show Details) and 'ライブラリに追加' (Add to Library). Below the banner, there are four category tiles: 'ドラマ風ビデオ' (Drama-style Video), 'ゲーム' (Game), 'テスト付きビデオ' (Video with Test), and 'ニュースレター' (Newsletter). Each tile has a representative icon and a title.

豊富なコンテンツ!
トレーニング
1,200種類以上
メールテンプレート
4,700種類以上

多言語対応!
日本語を含む
30カ国以上の言語に対応

NTTコミュニケーションズ
オリジナルコンテンツも提供!

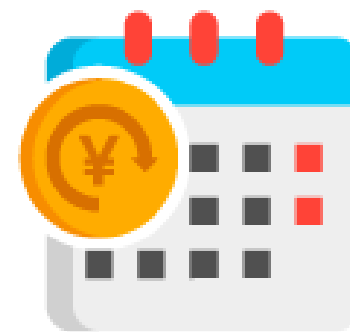
特徴③ 月額で使い放題！どこからでも受講可能！

利用ユーザー数に応じた月額サービスで、教育コンテンツやフィッシングメール攻撃訓練は使い放題。場所やデバイスを選ばないため、どこからでもいつでも受講できます。

コンテンツ
見放題! 使い放題!



月額で
利用可能!



好きな時間に
好きな場所で!



サービス活用例

既存のセキュリティ教育での課題

メール訓練やWeb研修の受講管理が煩雑
効果測定がしづらい

Web研修の教材の内容がマンネリ化
訓練メールの文面の作成、工夫に苦勞

集合講習のスケジュール調整が手間
講師や会場費用が高



サービス導入効果

教育／メール訓練／効果測定を
同一プラットフォームで実施
受講管理も楽々

豊富なコンテンツから選択するだけ
最新情勢、多言語にも対応

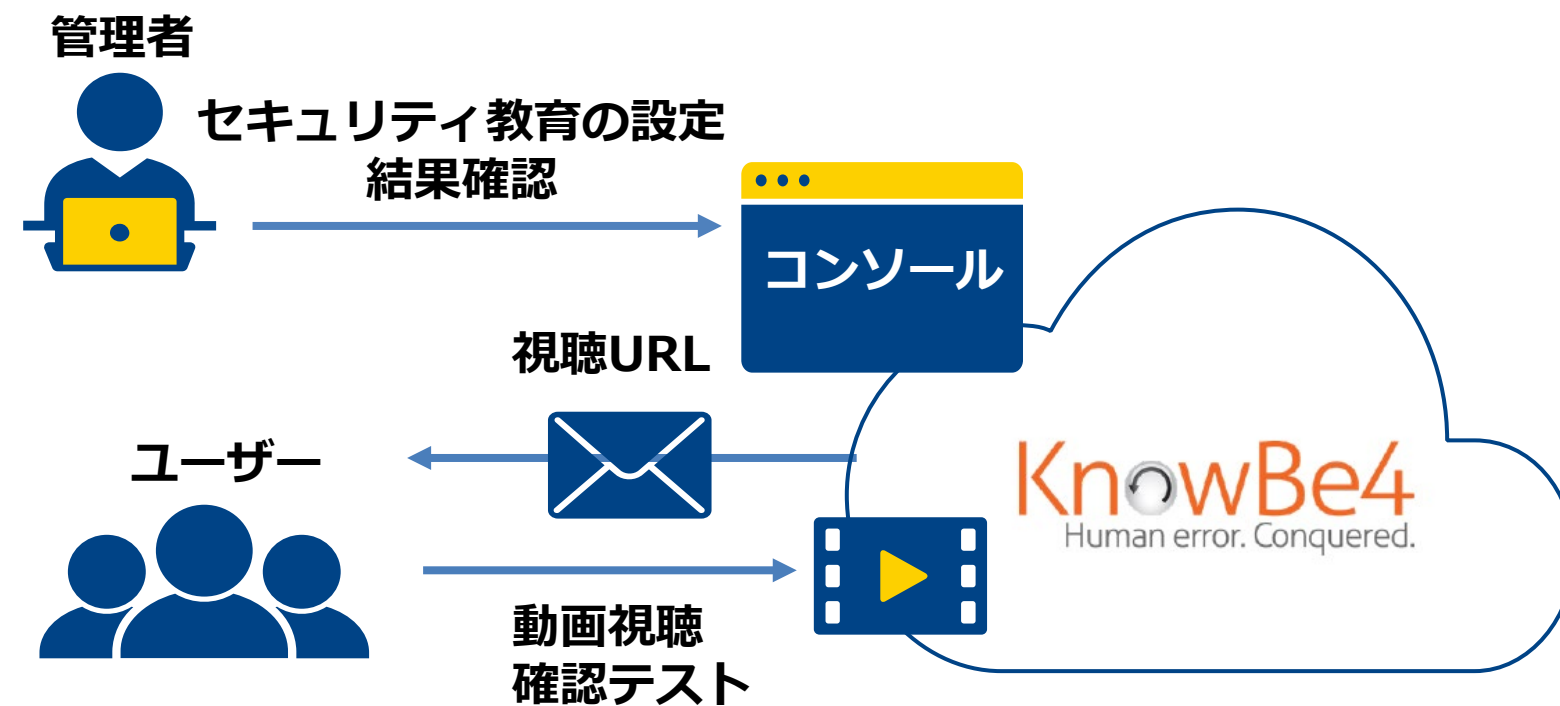
月額料金で何回でもトレーニング実施
時間や場所を選ばず受講できる



サービスの提供機能

提供機能① セキュリティ教育

お客さま管理者がコンソール上で動画コンテンツ・社員を選択し送付することで、KnowBe4上の教育動画を受講することができます。NTT Comオリジナル動画を含む充実した教育コンテンツを用意しており、動画視聴、確認テストがデバイスを問わず、受講可能です。受講結果は自動で集計し、お客さま管理者がコンソール上で確認できます。

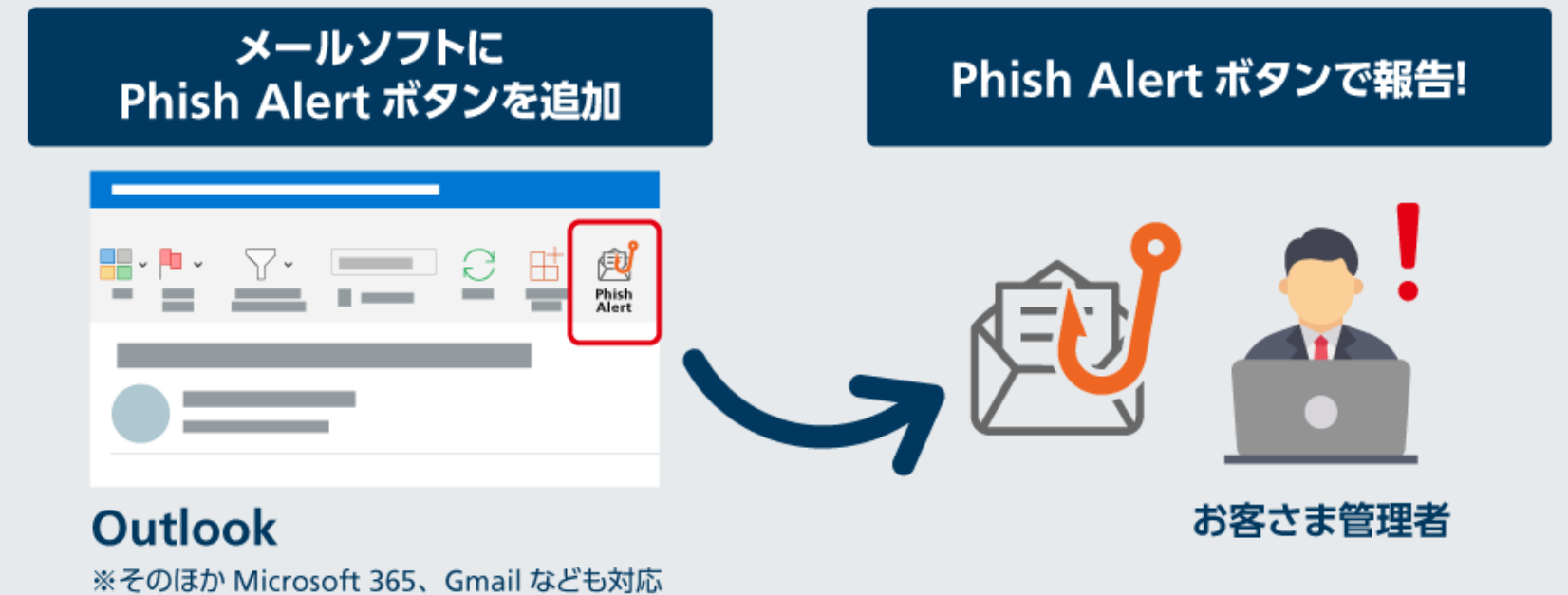
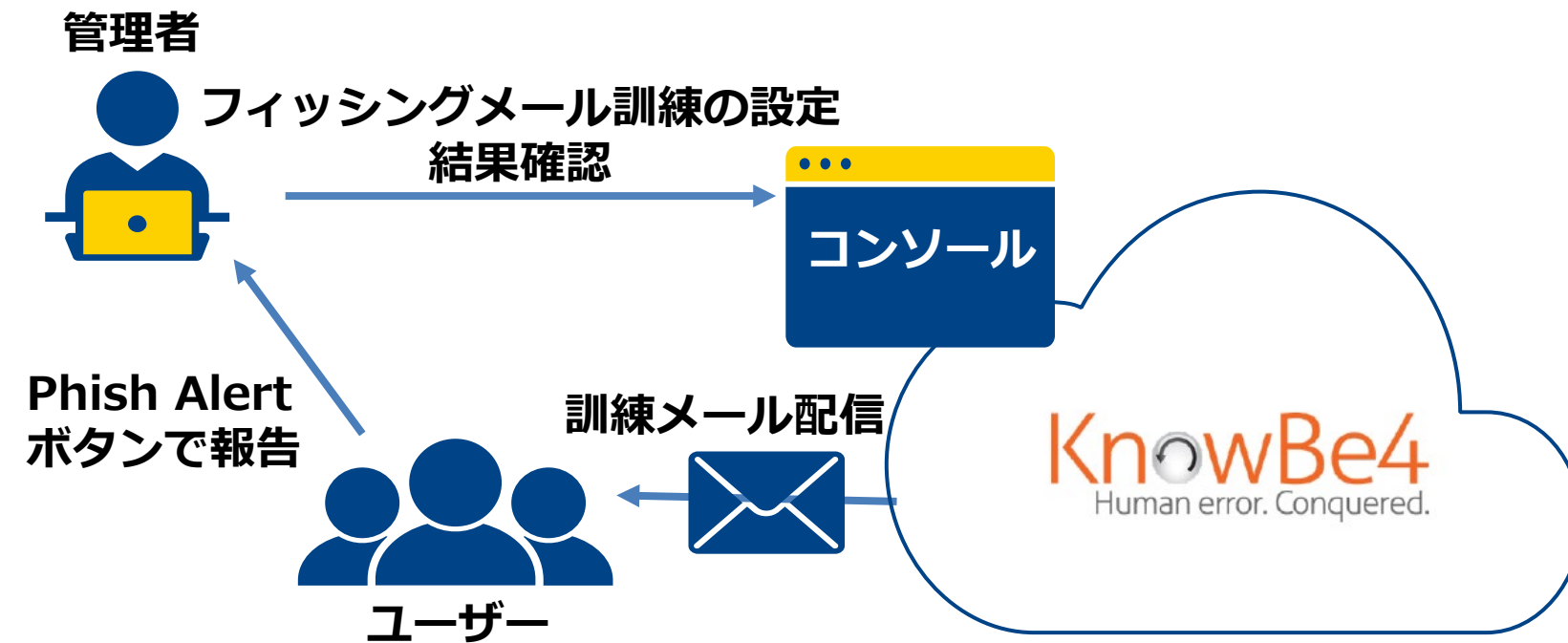


マルチデバイス対応!



提供機能② フィッシングメール訓練

お客さま管理者がコンソール上で訓練メール文案・対象社員を選択することで、本番さながらのフィッシングメール訓練を手軽に実施することができます。NTT Comオリジナルを含む豊富なテンプレートを活用することで、訓練効果アップが期待できます。メールソフトにPhish Alertボタンを組み込むことで、普段の業務中にも怪しいメールを見つけたときに、ボタンを押してお客さま管理者へ報告する習慣を根付かせることができます。



提供機能③ 効果測定分析

お客さま管理者にてセキュリティ教育の受講状況、フィッシングメール訓練の結果をコンソールで確認できます。社員別、グループ別のリスクスコアで、セキュリティ意識の定着状況も可視化されます。



トレーニングの効果も
グラフで分析可能!

各ユーザーの受講状況!

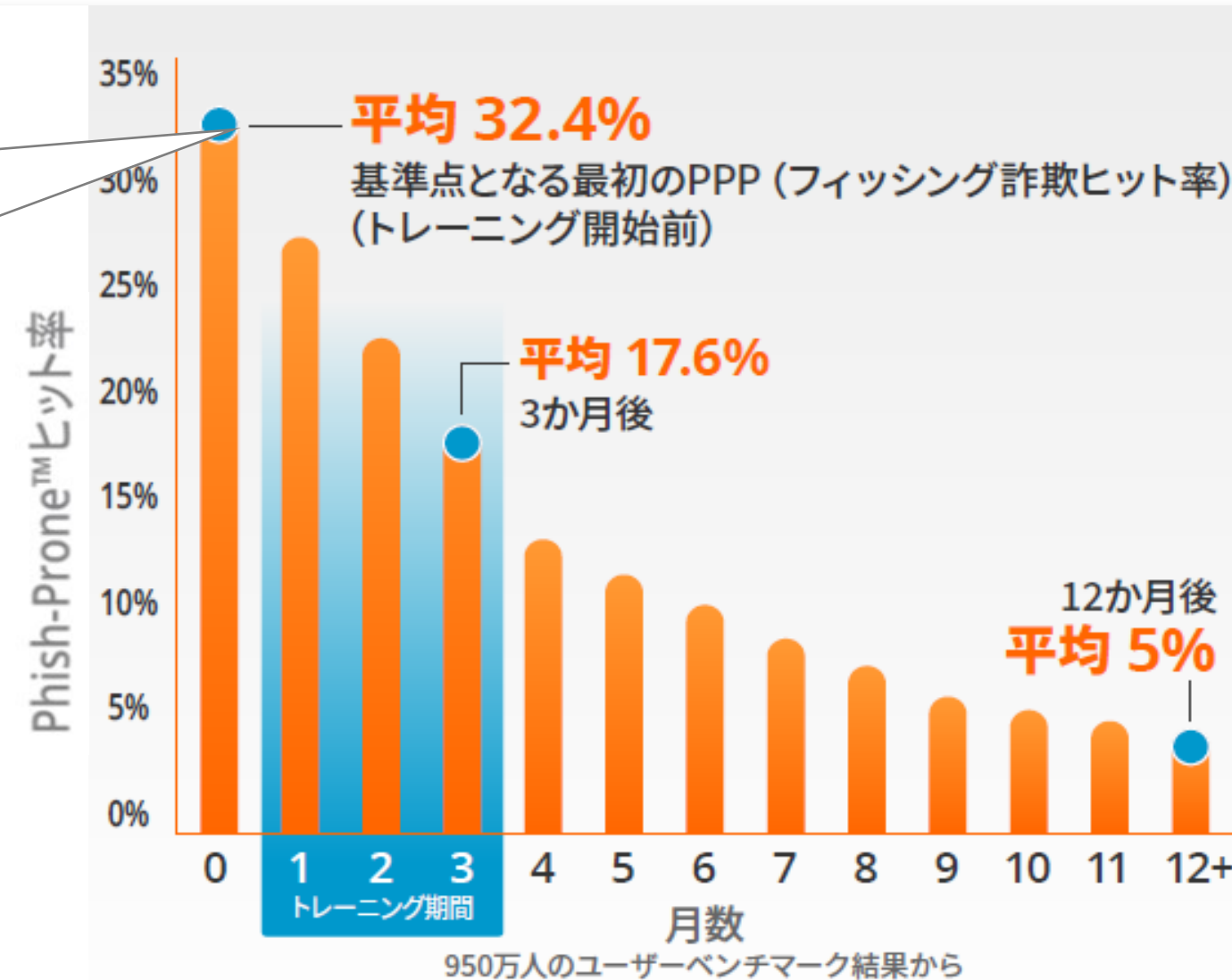
フィッシングメール訓練の
ヒット率!

部署／個人レベルの
リスクスコア!

導入効果

KnowBe4社のレポートによると、セキュリティトレーニングを開始する前は、フィッシング詐欺ヒット率が平均32.4%だったのに対し、教育とメール訓練を組み合わせることで1年間継続して実施することにより、ヒット率が平均5%まで下がったとの報告があります。このことから、継続した教育とメール訓練が効果的なことが分かります。

セキュリティ教育を受けていない約3人に1人がフィッシングリンクをクリックしてしまう



出典：2022年度版業界別フィッシングベンチマークレポート (<https://www.knowbe4.jp>)

本サービスはセキュリティ教育、フィッシングメール訓練、その効果測定分析を組み合わせ、低価格でトレンドを押さえたセキュリティトレーニングサービスを提供します。

設定サポート（オプション）

設定サポート概要

お客さま管理者に代わり管理者コンソールの設定および運用を代行します。
 お客さま要件のヒアリングを行い、要件に応じて必要なチケット数を見積りします。
 初期設定から運用までフルアウトソーシングにてNTT Comにお任せいただく事も可能です。



設定サポート内容

- スタンダードプラン：以下の設定項目をパッケージとして提供します。
お客さま管理者によるコンソール操作は不要のメニューです。
- カスタマイズプラン：以下の設定項目より設定代行を希望される項目を選択していただきます。
／ワンショットプラン
- 下記の設定項目以外の設定代行を希望される場合は、個別対応（個別費用）となります。

設定項目		内容	スタンダード	カスタマイズ/ ワンショット
初期設定	ユーザー登録	ユーザーアカウントを作成します。 ユーザーをグループで管理したい場合は、グループを作成して対象グループに格納します。	○※	●
	管理者権限設定	ユーザーに管理者権限を割り当てます。	—	●
	グループへのセキュリティロール設定	グループにセキュリティロールを割り当てます。	—	●
	KnowBe4側のホワイトリスト登録	KnowBe4から送信される訓練メールがスパム判定、ブロックされにくくするため、DKIM署名の設定を行います。	●	●
	Phish Alertボタン設定	KnowBe4側でPhish Alertボタンの設定を行います。	—	●
	受講者ホームのダッシュボード設定	受講者ホームに訓練メールのテスト結果、個人のリスクスコアを表示するように設定を行います。	—	●
運用設定	トレーニングキャンペーン	2カ月に1回、NTT Comの推奨する教育コンテンツを3本程度配信します。	●	●
	フィッシングキャンペーン	月1回、NTT Comの推奨する訓練メールを配信します。	●	●
	レポート作成	トレーニングとフィッシングのキャンペーン毎に、結果のレポートを送付します。	●	●
	登録ユーザー情報の更新	ユーザー情報の更新（追加 / 削除 / グループ変更）を実施します。	○※	●

料金・申込方法

【料金】

月額 500円（税込550円） /Seat（ID）

※Seat数にご利用されるユーザー数となります。（例：利用ユーザー数が100名の場合は100Seat）

【申込方法】

本サービスのお申し込みは担当営業にお問い合わせください。

Web（ICT Business Mall）からもお申し込みが可能です。

（[ICT Business Mall TOPページ](#)から、「セキュリティ」をクリック！）

※ICT Business Mallはお客さまご自身での注文のみ受け付けます。

※標準開通日は16営業日です。

その他、本サービスの提供条件などは、ICT Business Mallにも掲載しております。

参考) 従来の標的型メール訓練との違い

年に数回の単発訓練では、驚いてクリックしてしまった人のチェックと注意に終始しがちです。メール訓練を継続的に行い、更にトレーニングと併用することで、実際の攻撃メールに対応できる人材が育成できます。

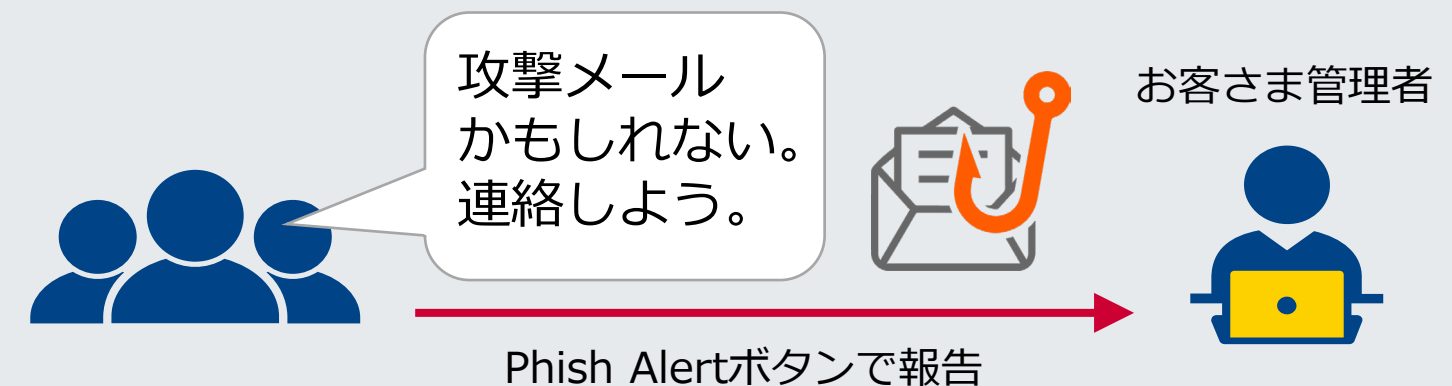
従来の標的型メール訓練 (年1-2回)

単発の訓練で訓練メールに引っかかった人を見つけ、注意喚起するのみに陥りがち



セキュリティ教育&メール訓練

訓練メールだけでなく、実際のメール攻撃を見分けられる人を育てる



セキュリティ教育&メール訓練のメリット

不審メールの報告プロセスの定着

トレーニングの併用による理解度向上

組織のリスク感度がわかる

参考) NTT Comオリジナル教育動画例

タイトル	概要
工場を止めたサプライチェーン攻撃ランサムウェアの事例	サプライチェーンを支える企業がランサムウェアの被害を受け、日本の大手自動車メーカーの工場が止まりました。
町の病院を襲ったランサムウェアの事例	日本の町立病院を襲ったランサムウェアの被害事例をご紹介します。
Emotetが感染拡大する理由	Emotetに感染すると、機密情報が外部へ流出し悪用されたり、ランサムウェアに感染しデータが暗号化や破壊され大きな被害が発生します。 どうして、この感染は拡大するのでしょうか？
狙われる多要素認証の事例	多要素認証は、ユーザーの認証時に複数の情報を使う方法で、不正アクセスを防ぐ有効な対策の一つです。 代表的なものに、パスワードとスマートフォンの認証アプリを使う方法があります。 しかし、このような多要素認証を破る手口が確認されており、プロンプト爆撃と呼ばれています。
USBメモリーの紛失事例から学ぶ情報漏えいの危険性	USBメモリーの紛失事例と情報漏えいの危険性についてをご紹介します。
クラウドサービスからの個人情報流出の事例	米国コミュニケーションツールサービス会社が、顧客企業のユーザー情報を誤って他企業へ開示する事態が発生しました。
メールの誤送信による顧客情報漏えいの事例	普段の業務で使うメールですが、国内でも不注意による誤送信のインシデントが頻発に発生しています。 メールの誤送信による顧客情報漏えいの事例を紹介します。
町職員の内部不正アクセスでの逮捕の事例	2022年7月に福岡県のある町役場の職員が逮捕され、不正アクセス行為の禁止等に関する法律違反の罪で罰金70万円の命令が出されました。
クレジット決済サービスからの情報漏えいで行政処分を受けた事例	クレジット決済サービス会社において、2021年8月から2022年1月にわたるサイバー攻撃により、最大約46万件の個人情報外部に流出しサービス全停止することになりました。 この事例は、セキュリティ対策を実施していましたが、適切な維持運用をしていませんでした。
ビジネスメール詐欺（BEC）の事例	国内企業と海外取引先企業のやりとりにおいて、取引先の担当者になりすました攻撃者が、銀行口座証明書類を偽造し、振込先口座変更を依頼してきた事例です。 これは、IPAビジネスメール詐欺事例集の事例2からの引用です。

※セキュリティ講座、海外ドラマ風ビデオ、クイズやゲームなど1,200種類以上のコンテンツをご用意しています。NTT Comオリジナル教育動画の一部です。