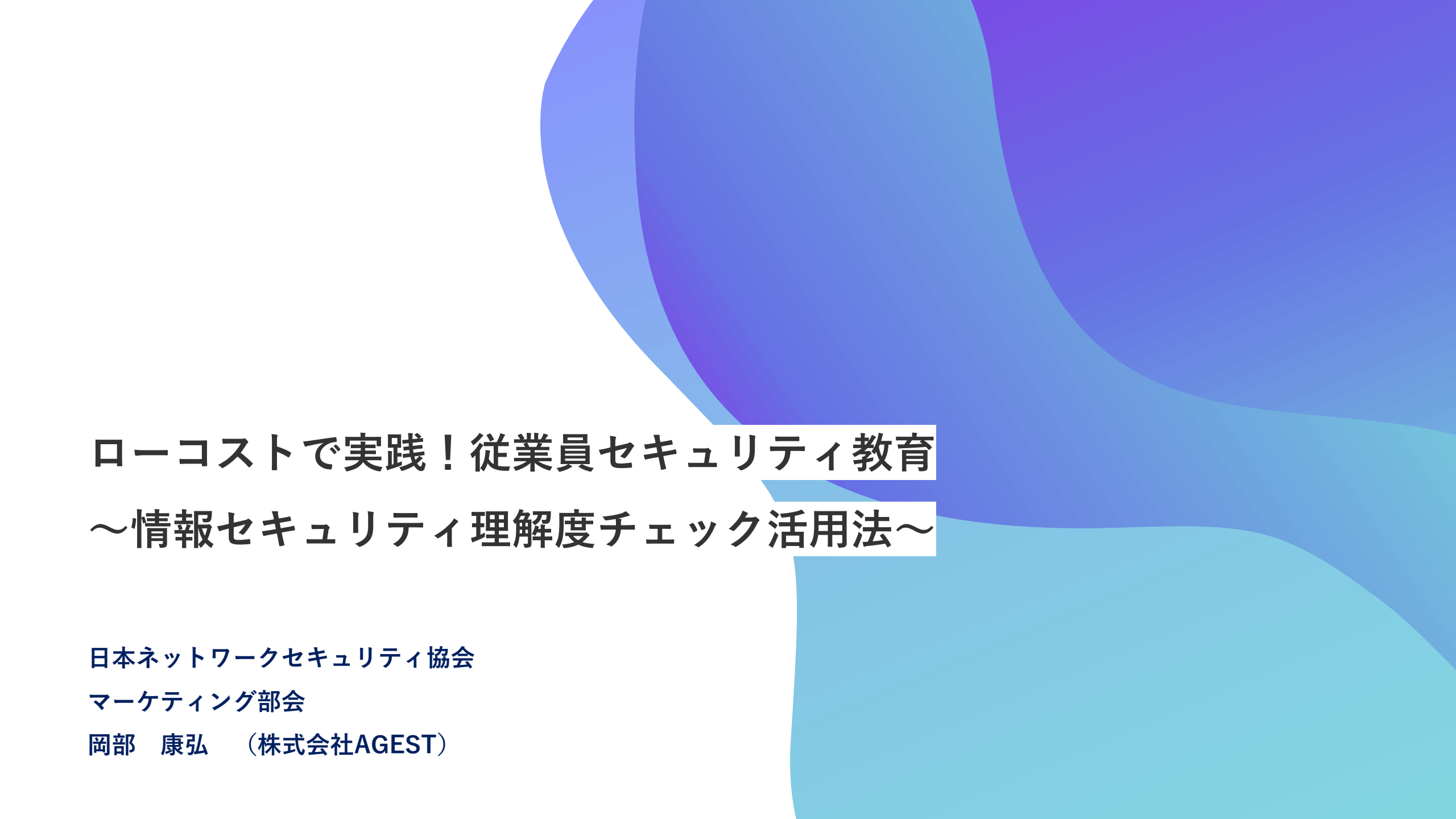




ローコストで実践！従業員セキュリティ教育 ～情報セキュリティ理解度チェック活用法～

日本ネットワークセキュリティ協会
マーケティング部会
岡部 康弘 （株式会社AGEST）

アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



自己紹介

株式会社AGEST

マーケティング本部 マーケティング推進部

岡部 康弘



Interopの基調講演に登壇しました



講演概要

企業のサイバーセキュリティ対策、システム導入だけで万全だと思っていませんか？

「最後の砦」となるのは従業員一人ひとりのセキュリティ意識です。

本講演では、従業員の情報セキュリティリテラシーを測れるJNSAの「情報セキュリティ理解度チェック」をご紹介します。

このツールを活用し、従業員の理解度を可視化、向上させる具体的な手法を解説します。

また、リテラシー不足が実際に引き起こしたサイバーセキュリティ事故の事例にも触れ、会社全体で情報資産を守るための、今すぐ始められる一歩をお伝えします。

アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



アジェンダ

はじめに

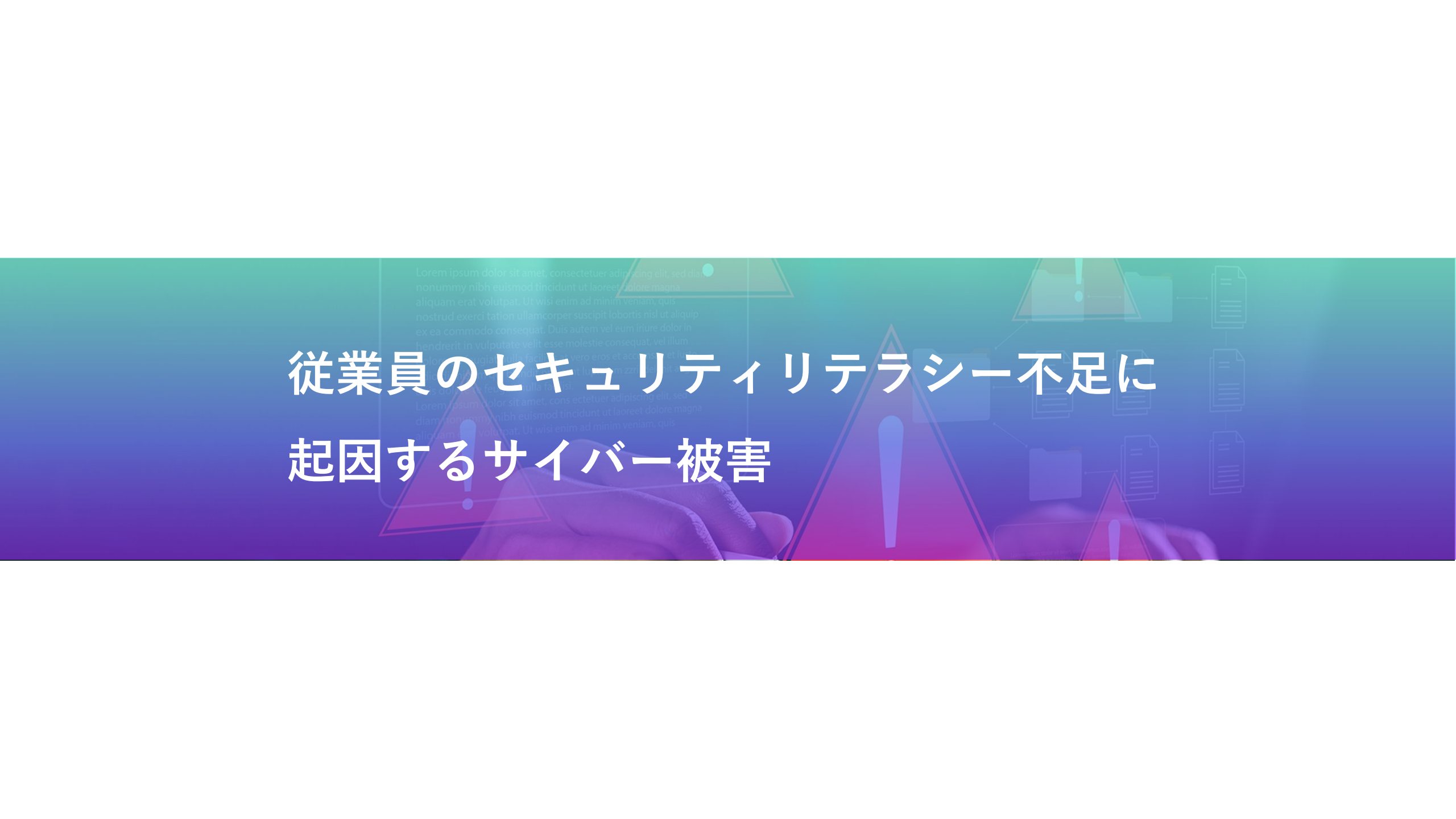
なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ





従業員のセキュリティリテラシー不足に 起因するサイバー被害

1. 音声フィッシング詐欺による認証情報窃取

事象：

従業員が電話でITサポート担当者になりすました攻撃者に騙され、多要素認証（MFA）の認証情報を渡してしまった。

解説：

この手口は「Vishing（ビッシング）」と呼ばれ、メールによるフィッシングと比べて心理的なハードルが低く、従業員が疑いなく指示に従ってしまうケースが増加しています。



2. 不適切なパスワード管理による不正アクセス

事象：

従業員が複数のサービスで同じパスワードを使い回したり、単純なパスワードを設定したため、他のサービスから流出した情報を使って社内システムに不正ログインされた。

解説：

企業側がシステムで対策を施していても、従業員のパスワード管理意識が低いと、このような「クレデンシャルスタッフィング攻撃」を許すことになります。



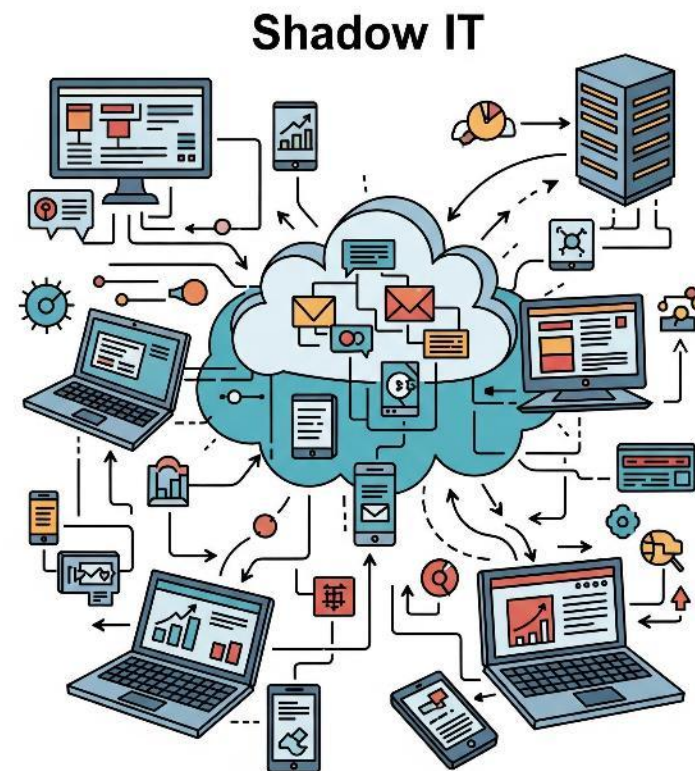
3. シャドーITによる情報漏えい

事象：

従業員が会社の許可なく個人のクラウドストレージやメッセージングアプリを業務で利用した結果、機密情報が意図せず外部に流出。

解説：

リモートワークの普及で顕著になった問題で、従業員が便利さを優先し、企業のセキュリティポリシーを無視することで発生します。



4. メールの誤送信による情報漏えい

事象：

宛先間違いや添付ファイル間違いなど、ヒューマンエラーによるメールの誤送信により、顧客情報や社外秘の資料が無関係な第三者に送付された。

解説：

単純なミスですが、情報漏えいの原因として常に上位に挙げられるものです。これは、送信前の確認不足や、組織的なチェック体制の不備が根底にあります。



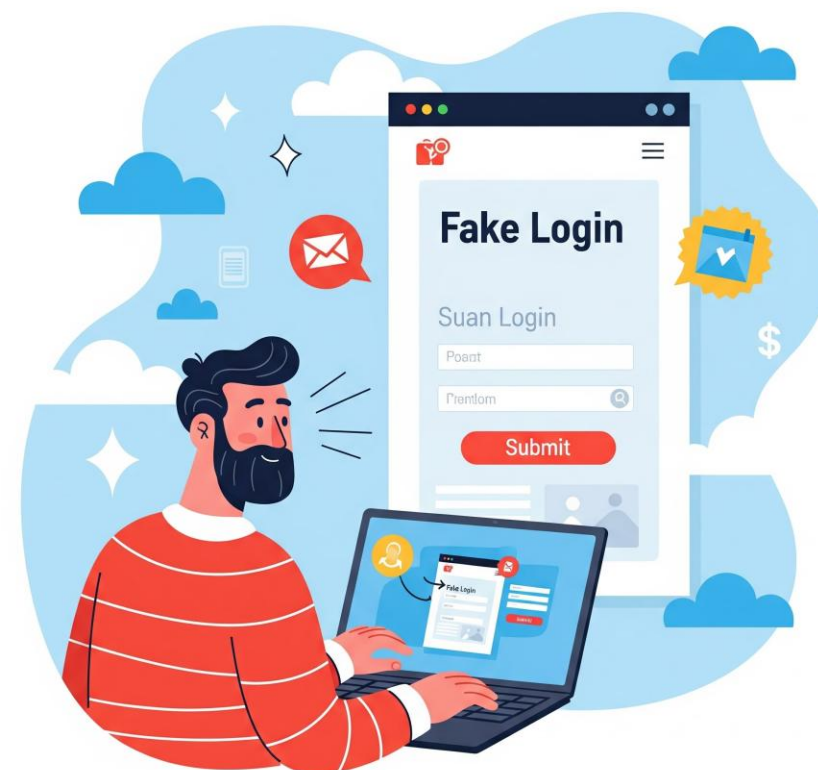
5. 不審なメールの開封によるマルウェア感染

事象：

従業員がフィッシングメールと気づかずに、添付された悪意のあるファイルを開封したり、リンクをクリックしたりした結果、ランサムウェアやEmotetなどのマルウェアに感染。

解説：

攻撃者はAIなどを活用し、より巧妙な文面で従業員を騙そうとします。従業員がメールのヘッダー情報や文面を注意深く確認する習慣がないと、容易に被害に遭ってしまいます。



セキュリティ教育が重要な理由

- セキュリティ事故の多くはヒューマンエラー
- どれだけシステムを強固にしても、最後の砦は結局「ヒト」
- 私たちの「うっかり」「きっと大丈夫」が狙われている



- 従業員のセキュリティ意識が組織の保護に重要です！

アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

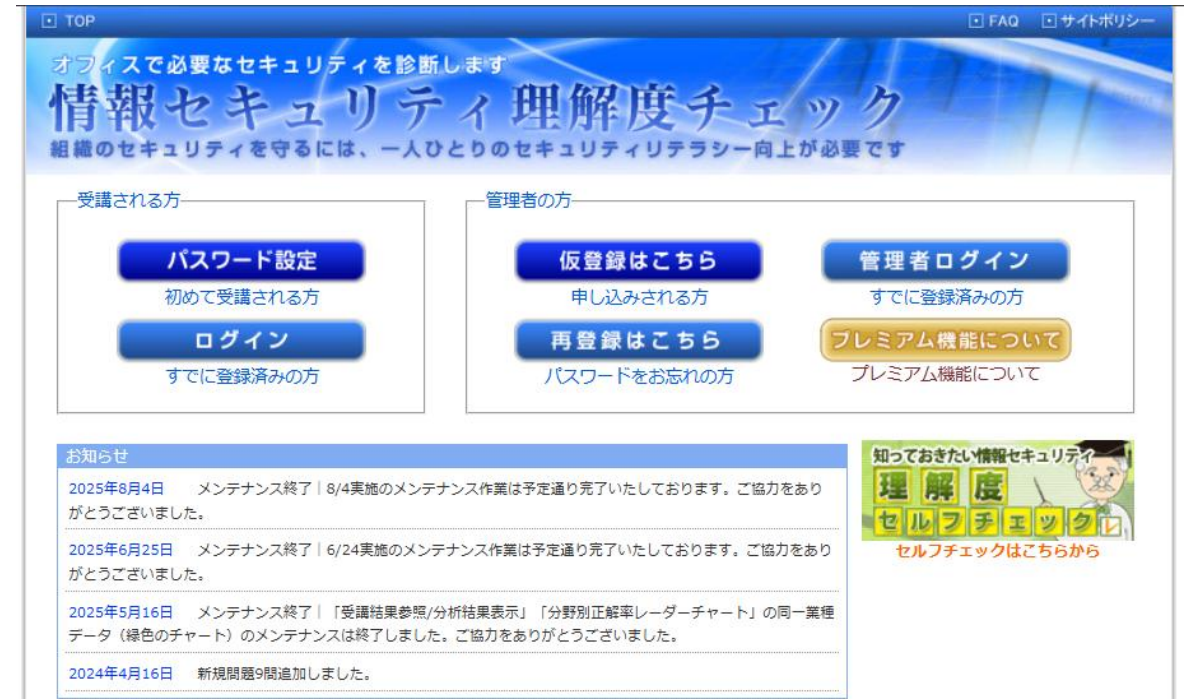
例題と利用方法

まとめ



概要と目的

- JNSA「会員交流部会」内のワーキンググループによって作成
- Webテストにより、セキュリティへの理解度を可視化できる
- 管理者機能付き、プレミアム、セルフチェックの3種類



特徴

- 「管理者機能付き」「セルフチェック」は無料で利用可能
- 「プレミアム」では、さらに独自の設問を追加することができる
- 問題は、基礎的かつ幅広い分野から出題される
- 所要時間約30分（全25問／1回）で、すぐに実施ができる
- 問題は実施毎に出題パターンが変わるため、何度でも学習できる

※このあと実際の問題もお見せします

- 解説付きのため、苦手分野の理解を深めることができる

問題分野

- | | |
|-------------------|--------------------|
| 1.電子メールの知識と利用法 | 5.PCの利用上の注意点 |
| 2.インターネットの利用法と注意点 | 6.オフィスにおける情報セキュリティ |
| 3.ウィルスの知識と対処方法 | 7.ルールや規則の遵守 |
| 4.パスワードの知識と管理 | 8.社外における情報セキュリティ |

特徴

- ・ 自社独自のセキュリティポリシーの浸透度をチェックする
- ・ 業界独自の事情を加味した設問を設定できる

などなど

- 「管理者機能付き」「セキュリティチェック」は無料で利用可能
- 「プレミアム」では、さらに独自の設問を追加することができる
- 問題は、基礎的かつ幅広い分野から出題される
- 所要時間約30分（全25問／1回）で、すぐに実施ができる
- 問題は実施毎に出題パターンが変わるため、何度でも学習できる

※このあと実際の問題もお見せします

- 解説付きのため、苦手分野の理解を深めることができる

問題分野

- | | |
|-------------------|--------------------|
| 1.電子メールの知識と利用法 | 5.PCの利用上の注意点 |
| 2.インターネットの利用法と注意点 | 6.オフィスにおける情報セキュリティ |
| 3.ウイルスの知識と対処方法 | 7.ルールや規則の遵守 |
| 4.パスワードの知識と管理 | 8.社外における情報セキュリティ |

実施のメリット

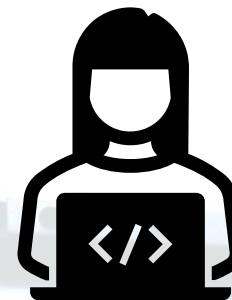
組織（管理者）のメリット

- 組織全体のサイバー防御力UP
- ひとりひとりの受講の有無や成績をチェックできる
- 全国平均と自組織のスコアを比較できる



個人（受講者）のメリット

- セキュリティの基礎を理解できる
- 理解レベルを客観的に把握できる
- 苦手分野を克服することができる



アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam
 nonummy nibh euismod tincidunt ut laoreet dolore magna
 aliquam erat volutpat. Ut wisi enim ad minim veniam, quis
 nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip
 ex ea commodo consequat. Duis autem vel eum iriure dolor in
 hendrerit in vulputate velit esse molestie consequat, vel illum
 dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto
 odio dignissim qui blandit praesent luptatum zzril delenit augue
 duis dolore feugait nulla facilisi.
 Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed
 diam nonummy nibh euismod tincidunt ut laoreet dolore magna
 aliquam erat volutpat.

実際に解いてみましょう！

写真データを加工する必要がある、



写真データを加工する必要がある、フリーソフトで使いやすいものがあつたので使うこと
としました。使用する上で最も適切な方法はどれでしょうか？

以下の選択肢からお選びください

- ☐ こっそりインストールし、使用後はアンインストールする
 - ☐ インストールするときはLANケーブル線をはずして使う
 - ☐ システム管理者にインストールしていいか確認してから使用する
 - ☐ 使い勝手がいいのでほかの人のPCにもインストールする
-



問題：

写真データを加工する必要があり、フリーソフトで使いやすいものがあったので使うこととしました。使用する上で最も適切な方法はどれでしょうか？

選択肢と解答

- こっそりインストールし、使用後はアンインストールする
- インストールするときはLANケーブル線はずして使う
- システム管理者にインストールしていいか確認してから使用する
- 使い勝手がいいのでほかの人のPCにもインストールする

解説：出所の明確でないソフトにはウイルスが含まれるものやスパイウェアが仕掛けられている場合があるので、システム管理者に確認し安全なものを使うようにしましょう。

SNS上での



SNS上での行為について、最も適切でないものはどれでしょうか？

以下の選択肢からお選びください

- ☐ 会社のお客さんと時事問題について議論した
 - ☐ プロフィールに会社の名前、電話番号、所属部署全員の氏名、現在の職務内容を記入した
 - ☐ 社内のサークル仲間とグループを作り趣味の情報交換をした
 - ☐ お客様に依頼されたのでゴルフに行った事や写真を日記に記載した
-



問題：

SNS上での行為について、最も適切でないものはどれでしょうか？

選択肢と解答

会社のお客様と時事問題について議論した

- **プロフィールに会社の名前、電話番号、所属部署全員の氏名、現在の職務内容を記入した**

社内のサークル仲間とグループを作り趣味の情報交換をした

お客様に依頼されたのでゴルフに行った事や写真を日記に記載した

解説：SNSで自社におけるプロフィールを細かく記載する事は社内の情報を不必要に開示することであり、悪用される危険性もあるので、会社名や氏名のみにとどめておいたほうが良いでしょう。

自宅でリモートワークをする場合



自宅でリモートワークをする場合、社外秘情報の管理方法について、不適切なものはどれでしょうか？

以下の選択肢からお選びください

- ☐ 家族であっても社外秘情報が見られないよう注意する
 - ☐ 会社から認められているパソコン以外では社外秘情報を使用しない
 - ☐ 社外秘情報とそうでない情報はしっかりと棲み分けしておく
 - ☐ リモート端末の故障に備え、自宅のPCに社外秘情報をバックアップしておく
-



問題：

自宅でリモートワークをする場合、社外秘情報の管理方法について、不適切なものはどれでしょうか？

選択肢と解答

家族であっても社外秘情報が見られないよう注意する

会社から認められているパソコン以外では社外秘情報を使用しない

社外秘情報とそうでない情報はしっかりと棲み分けしておく

● リモート端末の故障に備え、自宅のPCに社外秘情報をバックアップしておく

解説：自宅のパソコンにバックアップ（コピー）をすること自体が禁止行為になり、コンピューターウイルスに感染した場合は情報漏えいする可能性がありますので、バックアップ（コピー）はしないようにしましょう。

パスワードは忘れやすいので…



パスワードは忘れやすいので、Aさんは色々な工夫をして忘れないようにしています。このうち、やってはいけないものはどれでしょうか？

以下の選択肢からお選びください

- ☐ ①自分の生年月日を利用したパスワードを設定する
- ☐ ②手帳の目立たないところに、パスワード関連とせずに、思い出すヒントを書いておく
- ☐ ③パスワードを作るための分かりやすい規則を自分で決めて覚えておき、その規則に従って、忘れてもすぐに導き出せるようにしておく
- ☐ ④ペットが我が家に来た日とか、祖母の誕生日のように、他人が知る可能性は低いが自分はいつでも思い出せるようなデータを利用する



問題：

パスワードは忘れやすいので、Aさんは色々な工夫をして忘れないようにしています。このうち、やってはいけないものはどれでしょうか？

選択肢と解答

- 自分の生年月日を利用したパスワードを設定する

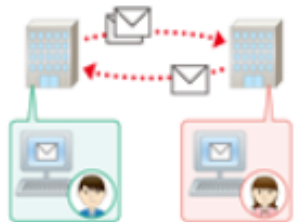
手帳の目立たないところに、パスワード関連とせずに、思い出すヒントを書いておく

パスワードを作るための分かりやすい規則を自分で決めて覚えておき、その規則に従って、忘れてもすぐに導き出せるようにしておく

ペットが我が家に来た日とか、祖母の誕生日のように、他人が知る可能性は低いが自分はいつでも思い出せるようなデータを利用する

解説：他人にすぐに知られてしまうパスワードの設定は禁物です。

フィッシング詐欺の手口は…



フィッシング詐欺の手口はどれでしょうか？

以下の選択肢からお選びください

- ☐ 電話で家族を装い金銭を要求する
- ☐ 出会い系サイトで知り合った人物が高額商品売りつける
- ☐ 金融機関などのホームページに見せかけてカード番号や暗証番号などを盗み取る
- ☐ ホームページ上のボタンやアドレスをクリックさせて不当な請求をする



問題：
フィッシング詐欺の手口はどれでしょうか？

選択肢と解答

- 電話で家族を装い金銭を要求する
- 出会い系サイトで知り合った人物が高額商品売りつける
- 金融機関などのホームページに見せかけてカード番号や暗証番号などを盗み取る
- ホームページ上のボタンやアドレスをクリックさせて不当な請求をする

解説：フィッシング詐欺は、偽の金融機関などのサイトを立ち上げ、カード番号・暗証番号・ID・パスワード等を詐取する手口です。

ちなみに・・・

やってみました・・・が、100点難しい

情報セキュリティベンチマーク結果

第1回：受講日時：2025年08月21日 21時20分～2025年08月21日 21時34分 【2025年08月21日 21時20分～2025年08月21日 21時34分】

総合得点： 84点 / (100点満点) 21問正解 / (全25問)

所要時間：14分20秒

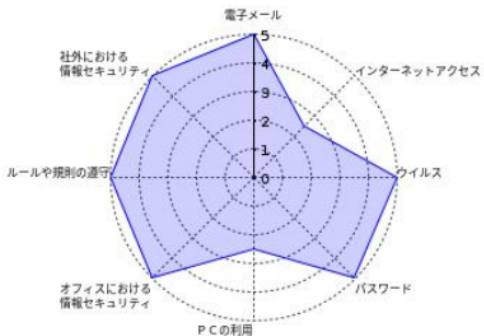
ニックネーム

で

ニックネームが不適切であると事務局で判断した場合、受講結果も含めて削除する場合があります

同意してランキングに登録する！！

分野別正解率		
番号	分野	正解率
C1	電子メール	100.0%
C2	インターネットアクセス	50.0%
C3	ウイルス	100.0%
C4	パスワード	100.0%
C5	P Cの利用	50.0%
C6	オフィスにおける 情報セキュリティ	100.0%
C7	ルールや規則の遵守	100.0%
C8	社外における 情報セキュリティ	100.0%

[詳細](#)

問1(C5) 誤 解答と解説	問2(C8) 正 解答と解説	問3(C5) 誤 解答と解説	問4(C3) 正 解答と解説	問5(C4) 正 解答と解説
問6(C2) 誤 解答と解説	問7(C8) 正 解答と解説	問8(C1) 正 解答と解説	問9(C5) 正 解答と解説	問10(C6) 正 解答と解説
問11(C7) 正 解答と解説	問12(C7) 正 解答と解説	問13(C4) 正 解答と解説	問14(C8) 正 解答と解説	問15(C8) 正 解答と解説
問16(C1) 正 解答と解説	問17(C7) 正 解答と解説	問18(C5) 正 解答と解説	問19(C1) 正 解答と解説	問20(C5) 誤 解答と解説
問21(C2) 正 解答と解説	問22(C5) 正 解答と解説	問23(C6) 正 解答と解説	問24(C1) 正 解答と解説	問25(C8) 正 解答と解説

情報セキュリティベンチマーク結果

第2回：受講日時：2025年08月21日 22時17分～2025年08月21日 22時44分 【

総合得点：92点 / (100点満点) 23問正解 / (全25問)

所要時間：26分53秒

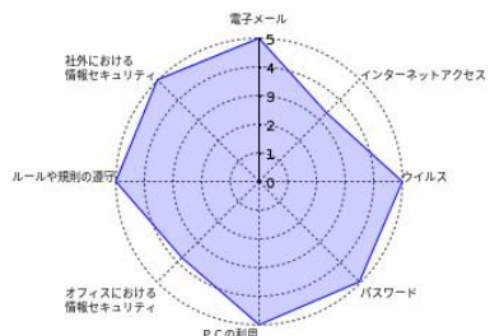
ニックネーム

で

ニックネームが不適切であると事務局で判断した場合、受講結果も含めて削除する場合があります

同意してランキングに登録する！！

分野別正解率		
番号	分野	正解率
C1	電子メール	100.0%
C2	インターネットアクセス	66.7%
C3	ウイルス	100.0%
C4	パスワード	100.0%
C5	P Cの利用	100.0%
C6	オフィスにおける 情報セキュリティ	75.0%
C7	ルールや規則の遵守	100.0%
C8	社外における 情報セキュリティ	100.0%



詳細

問1(C8) 正 解答と解説	問2(C6) 誤 解答と解説	問3(C5) 正 解答と解説	問4(C2) 誤 解答と解説	問5(C8) 正 解答と解説
問6(C3) 正 解答と解説	問7(C6) 正 解答と解説	問8(C2) 正 解答と解説	問9(C6) 正 解答と解説	問10(C8) 正 解答と解説
問11(C1) 正 解答と解説	問12(C6) 正 解答と解説	問13(C3) 正 解答と解説	問14(C7) 正 解答と解説	問15(C4) 正 解答と解説
問16(C7) 正 解答と解説	問17(C1) 正 解答と解説	問18(C4) 正 解答と解説	問19(C8) 正 解答と解説	問20(C2) 正 解答と解説
問21(C8) 正 解答と解説	問22(C3) 正 解答と解説	問23(C1) 正 解答と解説	問24(C4) 正 解答と解説	問25(C5) 正 解答と解説

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duiis dolore feugait nulla facilisi.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim

利用方法

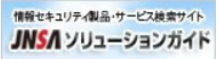
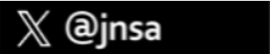


<https://www.jnsa.org/>

管理機能付き



セルフチェック



※ ポスト

- ▶ 2025.7.23 **成果物公開**
調査研究部会 インシデント被害調査ワーキンググループが「インシデント損害額調査レポート 別紙 2025年版」を公開しました。
- ▶ 2025.7.11
JNSAメールマガジン第316号は「話題の生成AIを活用したサイバー対応IT-BCP策定ハンドブックのご紹介」です。JNSA西日本支部今すぐ実践できる工場セキュリティ対策のポイント検討WGリーダー 岡本登様にご執筆いただきました。（夕方の配信後にお読みいただけます）
- ▶ 2025.7.10 **成果物公開**
調査研究部会 データベースセキュリティワーキンググループが報告書を3件公開しました。
- ▶ 2025.7.7 **成果物公開**
調査研究部会 セキュリティ市場調査ワーキンググループが「2024年度 国内情報セキュリティ市場調査報告書」を公開しました。
- ▶ 2025.6.27
JNSAメールマガジン第315号は「サイバーセキュリティイベント「RSAC CONFERENCE 2025」レポート」です。ISC2 小熊慶一郎様にご執筆いただきました。（夕方の配信後にお読みいただけます）
- ▶ 2025.6.24
「JNSA2025年度活動報告会」の参加受付を開始しました。
- ▶ 2025.6.17
組織で働く人間が引き起こす不正・事故対応WGによるインタビュー連載「日本の人事と内部不正」第16回「日立製作所研究開発グループにおける人材戦略と取り組みに関するインタビュー」を公開しました。
- ▶ 2025.6.13
JNSAメールマガジン第314号は「VPNは継続利用が多数派、それでも一部で進む見直し：情報セキュリティ実態調査に見る企業対応」です。NRIセキュアテクノロジーズ株式会社 中土井洋平太様にご執筆いただきました。（夕方の配信後にお読みいただけます）
- ▶ 2025.6.12
2025年度の部会、ワーキンググループの紹介を公開しました。
- ▶ 2025.5.30
JNSAメールマガジン第313号は「医療ITワーキンググループ設立について」です。JNSA社会活動部会医療ITWGリーダー 新善文様にご執筆いただきました。（夕方の配信後にお読みいただけます）
- ▶ 2025.5.28 **成果物公開**
情報セキュリティ教育事業者連絡会（ISEPA）JTAGキャリアデザインWGが報告書「セキュリティ人材の確保と育成」を公開しました。
- ▶ 2025.5.16

TOP FAQ サイトポリシー

オフィスに必要なセキュリティを診断します

情報セキュリティ理解度チェック

組織のセキュリティを守るには、一人ひとりのセキュリティリテラシー向上が必要です

受講される方

パスワード設定
初めて受講される方

ログイン
すでに登録済みの方

管理者の方

仮登録はこちら
申し込みされる方

再登録はこちら
パスワードをお忘れの方

管理者ログイン
すでに登録済みの方

プレミアム機能について
プレミアム機能について

お知らせ

2025年8月4日 メンテナンス終了！8/4実施のメンテナンス作業は予定通り完了いたしました。ご協力ありがとうございました。

2025年6月25日 メンテナンス終了！6/24実施のメンテナンス作業は予定通り完了いたしました。ご協力ありがとうございました。

2025年5月16日 メンテナンス終了！「受講結果参照/分析結果表示」「分野別正解率レーダーチャート」の同一業種データ（緑色のチャート）のメンテナンスは終了しました。ご協力ありがとうございました。

2024年4月16日 新規問題9問追加しました。

知っておきたい情報セキュリティ
理解度セルフチェック
セルフチェックはこちらから

操作については、マニュアルをご覧ください。また、よくある質問についてはこちらからご覧いただけます。

はじめにお読みください（ご利用マニュアル／PDF 150KB）

情報セキュリティ理解度チェックサイトとは？

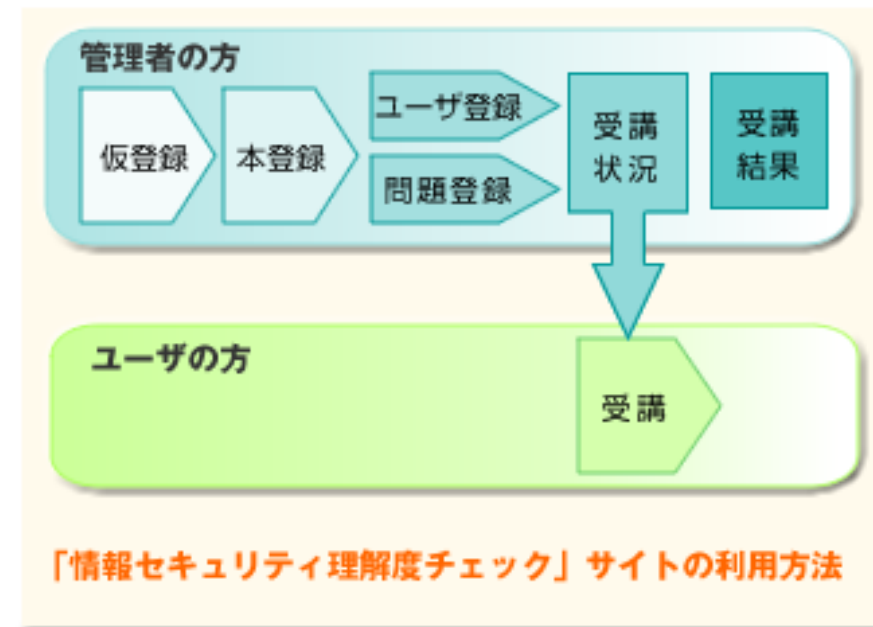
組織の社員・職員がそれぞれパソコンを1台使用し、メールを使つての連絡やインターネットを利用した情報を受発信することが業務の重要な手段となってきています。

そのような状況の中では、社員・職員1人ひとりが適切な情報セキュリティ意識をもち、組織全体の情報セキュリティレベルに合わせた適切な教育を行い、組織全体の情報セキュリティ向上を図ることが求められています。

この「情報セキュリティ理解度チェック」サイトでは、個人として、1人ひとりの受講結果を知ることができます。また、自組織の全体としての情報セキュリティ知識レベルを確認できるだけでなく、さらに同業種の中でのランキングを知ることでも、自組織の情報セキュリティ知識レベルの客観的な把握が可能になります。

この情報セキュリティ理解度チェックサイトを、皆さまの組織の情報セキュリティ向上のための一助としてご活用いただければ幸いです。

<https://slb.jnsa.org/eslb/>



詳しい登録方法はこちらの
「ご利用マニュアル」からご確認いただけます

アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



アジェンダ

はじめに

なぜ、セキュリティ教育が必要なのか？

JNSA「情報セキュリティ理解度チェック」とは？

例題と利用方法

まとめ



まとめ

- セキュリティ事故の多くはヒューマンエラー
- 私たちの「うっかり」「きっと大丈夫」が狙われている
- JNSA「情報セキュリティ理解度チェック」で、
組織のセキュリティリテラシーを可視化することができる
- 可視化された結果を基に対策を講じることで、
組織全体のサイバー防御力をUPさせることができる

ローコストで実践！従業員セキュリティ教育 ～情報セキュリティ理解度チェック活用法～

Fin

ぜひご活用ください