CDNS

eラーニングシステム
３つの特長

ご利用のためのガイダンス

（株）コミュニケーションデザインネットワークス

目　次

- CDNS eラーニングシステム３つの特長
- CDNS eラーニングシステム 特長－１
- CDNS eラーニングシステム 特長－２
- CDNS eラーニングシステム 特長－３
- ｅラーニングシステムの落とし穴
- セキュリティ教育のゴール
- 自社にとって有効な教育を考える

CDNS eラーニングシステム3つの特長

CDNS eラーニングシステムには、3つの特長があります。

特長－1

組織のさまざまな
状況・機会で求められる
セキュリティ教育
に柔軟的な支援

特長－2

PDCAマネジメント
システムに基づいた
効果的な教育の
実践支援

特長－3

教育結果及び実施した
教育の有効性を評価・
レビューに重点

CDNS eラーニングシステムの特長－１

特長 1

組織のさまざまな状況・機会で求められるセキュリティ教育に柔軟的（いつでも、どこでも、すぐに）な利用が可能です。

【1】マネジメントシステムの取得・運用支援に利用（第三者認証制度等）

ISMS/ISO27001・プライバシーマーク 情報マネジメントシステム	ISMS/ISO27001・プライバシーマーク 情報マネジメントシステム
構　築	**運　用**

【2】個人情報・営業秘密情報等情報管理の取り組みに利用

【3】委託元・取引先からの要求に対する社内教育周知に利用

【4】従業員の情報セキュリティの層別の教育・研修に利用

CDNS eラーニングシステムの特長ー1【1】

【1】マネジメントシステム（第三者認証制度）の取得・運用支援

ISMS/ISO27001やプライバシーマーク等、マネジメントシステムの取得・継続的な運用に活用できます。

- **PDCAサイクル**（教育計画 → 実施 → 評価 → 改善）に基づいた、効果的な教育を実践できます。
- ISMS/ISO27001やプライバシーマークのマネジメントシステムの認証・認定を取得するための規格要求事項を網羅しています。
  ⇒**マネジメントシステムの構築・運営を実現**します。
- 情報セキュリティを進める上で必要な「役割」と「責任」に応じて、**層別の教育**コンテンツをご用意しています。
- 従業員一人ひとりの理解度をチェックし、教育の**有効性を評価**することが可能です。（テスト回答内容の把握）

→おすすめコース

ISMS（ISO27001）/ Pマーク「おまかせパック」・「ピンポイント教育」

CDNS eラーニングシステムの特長ー1【2】

【2】情報管理（マネジメント）の取り組み支援

組織は、個人情報・営業秘密情報・財務情報・証券取引法上の重要情報・知的財産権を有する情報等、さまざまな重要な情報を保有し、内部統制によりその**適正な管理（コンプライアンス／法令順守）**が要求されています。

これらの情報を適切に管理するためには、**法令の理解**や組織は従業員にその**情報の重要性や管理方法を十分周知**し、組織全体で情報管理へ取り組みできる**体制整備（内部統制）**を実施する必要があります。

CDNS eラーニングシステムは、第三者認証制度を取得せずに、情報マネジメントに取り組む事業者様、また、将来的に第三者認証制度の取得を目指す事業者様の**従業員教育、組織体制整備**にお役立ていただくこともできます。

→おすすめコース

：ピンポイント教育「法規適合性理解編」

※「周知・教育コース」もあわせて利用すると有効です。

CDNS eラーニングシステムの特長ー1【3】

【3】委託元・取引先からの要求に対する支援

受託業務で取り扱う情報は、委託元との秘密保持契約の締結を負った上で取り扱うケースが増えてきました。受託業務により委託元から預かった**情報の徹底管理**は必要不可欠です。

万が一、漏えい事故等、事件を起こした場合、**契約違反**となるばかりか、**法令違反**により委託元や関連被害先より**損害賠償請求**を受けることになりかねません。
また、このような事故、事件を起こした結果、信用を失い、事業存続の危機に陥ることもあるでしょう。

最近では、委託元からの要求や契約条件として、委託先におけるセキュリティ教育・コンプライアンス教育が求められる傾向にあります。

→おススメコース
：ピンポイント教育 「周知・教育コース」・「法規適合性理解編」

CDNS ｅラーニングシステムの特長ー１【４】

【４】従業員の情報セキュリティ教育・研修支援

従業員は在職中はもとより退職後も会社の**秘密（営業秘密）情報**を許可なく利用したり、第三者や雇用先に開示、提供したりすることは**違法（不正競争防止法等）**です。
従業員の過失や意図的な持ち出し・流出を回避するためにも日頃から従業員への教育を実施することが大切です。

従業員に対しては、情報セキュリティの基礎や概念を学ぶ一般教育に加えて関連法令の内容、情報管理の詳細、緊急時の対応等、具体的な社内ルールを周知・教育する必要があります。

また、**正社員に限らず、全従業員（役員、契約社員、パート社員、アルバイト、外部スタッフ等）が対象**となります。従来の教育・研修プログラムにプラスして情報管理や情報セキュリティの教育を行いましょう。

CDNS ｅラーニングシステムでは、従業員教育に役立つ目的や層別毎に豊富なコンテンツをご用意しています。

→**おススメコース**
：ピンポント教育「情報マネジメント基礎教育コース」・ 「周知・教育コース」

CDNS eラーニングシステムの特長ー２

特長２	PDCAサイクル運用に基づいた、効果的な教育の実践を推進することが可能です

マネジメントシステム（ISMS/ISO27001やプライバシーマーク等の第三者認証制度）で要求されている

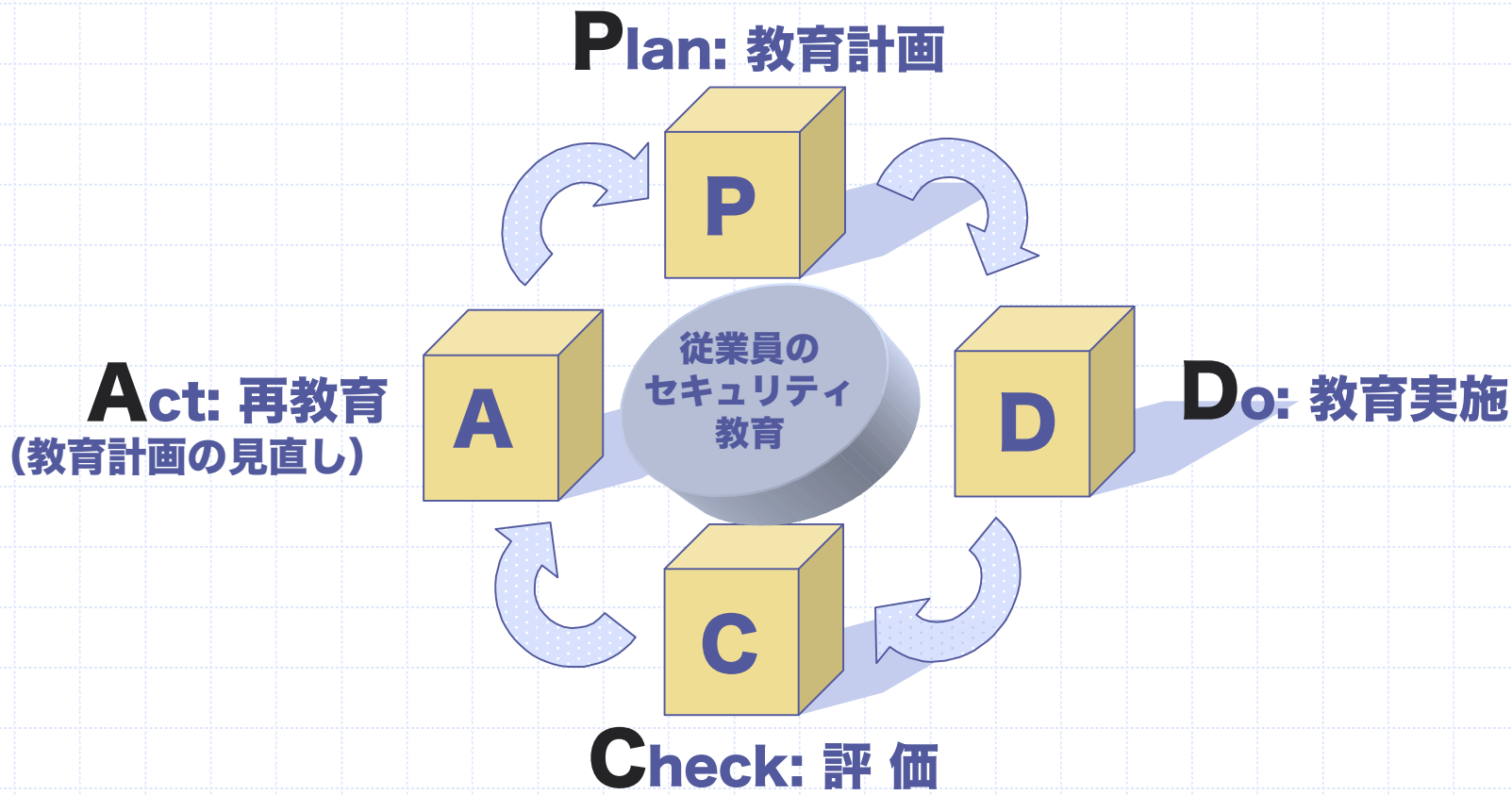
PDCA（計画 → 実施 → 評価 → 改善）サイクルモデル

を利用することで効果的な教育を実施することができます。

この手法は第三者認証制度を取得していない事業者様でも有効に活用し、効果を上げることが可能です。

CDNS eラーニングシステムの特長ー２

セキュリティ教育におけるPDCAサイクル運用



CDNS eラーニングシステムの特長－2

PDCAサイクル運用に基づいた効果的な教育の実践

Plan：計画

教育は**組織の現状**に基づいて行うことが大切です。組織にとって今、**必要とされていることは何なのか、問題点は何なのか**、それを補うためにどのような教育を実践すればよいのか、**教育の目的やテーマ、対象**等について協議し、プランを立てましょう。

Do：実施

教育は計画に沿って、対象となる部署や従業員に対して実施しましょう。教育の内容は**基礎知識を得る概念的な教育**や**自社の詳細なルールを周知するため教育**等さまざまです。期限を定めて教育担当者が進捗管理を行うようにしましょう。

CDNS eラーニングシステムの特長－２

PDCAサイクル運用に基づいた効果的な教育の実践

Check：点検

教育を実施した後は、従業員の**理解度をチェック**しましょう。

チェックには、テストやアンケート、チェックリストを利用する等、**担当者の主観に偏らない基準を設定し、客観的な評価を試みましょう**。（マネジメントシステムを実施する上では、定量的な結果に基づく評価が望ましいとされています。）

また、教育を受けた従業員毎の評価結果を記録しておきましょう。

CDNS eラーニングシステムの特長ー２

PDCAサイクル運用に基づいた効果的な教育の実践

Act：見直し

見直しは、

<u>１）評価基準に満たなかった従業員に対して行うフォローアップ</u>と、

<u>２）実施した教育自体が、目的を達成することができたかレビューする</u>

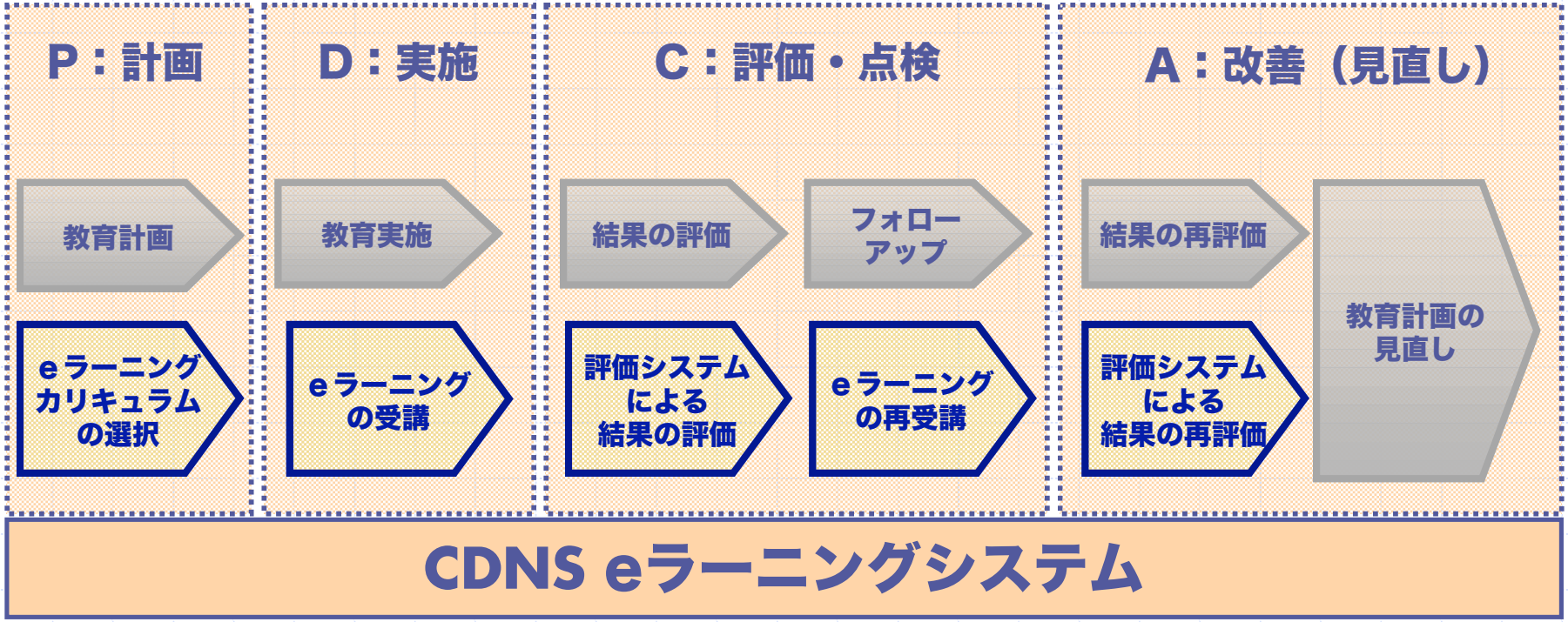
の２通りがあります。

後者のレビューは、教育結果を上層部に報告し、実施した教育の有効性について検討・協議し、その結果を次の教育につなげるようにしましょう。

CDNS eラーニングシステムの特長－2

eラーニングシステムを活用した教育のPDCA

eラーニングシステムを活用すると、教育のPDCAサイクルをスムースに運用することができます。



CDNS eラーニングシステムの特長ー3

特長3	教育結果及び実施した教育の有効性をレビューし、やりっぱなしではなく、その実効性を常に向上させるための仕組みがあります。

CDNS eラーニングシステムの特長ー3

■評価・見直しは、個人と組織のレベルで行いましょう。

③結果の評価

CDNS eラーニングシステムでは、従業員一人ひとりの教育の理解度をテストの点数で評価することができます。また、教育担当者は、従業員の教育結果を一元管理し、進捗状況やテスト結果を随時確認することが可能です。

④フォローアップ／⑤結果の再評価

テストで基準点（合格点）に満たない従業員には再教育を促し、再評価を行うことが可能です。

⑥教育内容・計画の見直し

従業員の教育結果をもとに組織の弱点や状況を把握し、教育自体が有効であったかどうかをレビューし、次回の教育に反映させましょう。

ｅラーニングシステムの落とし穴

- 組織の状況によっては、ｅラーニングシステムを受講するだけでは情報管理のためのルールの周知が不十分なケースがあります。

  ≫必要に応じて、プロジェクト間のミーティングや現場スタッフを巻き込んだ訓練等を実施し、周知できているか確認しましょう。

- ｅラーニングシステムの受講を指示した後、放置しておくと、業務に追われて実行できずに教育が完了していないケースがあります。

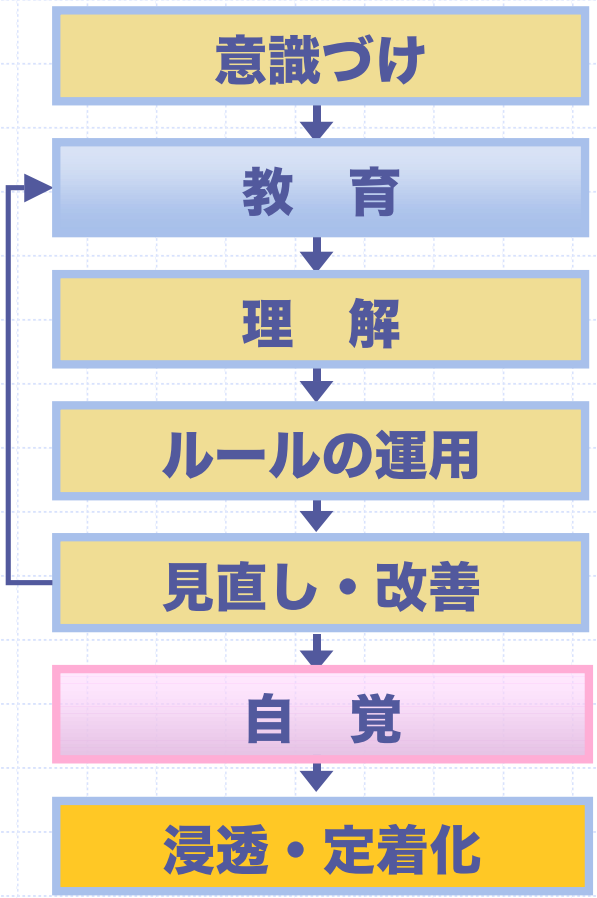
  ≫「やりっぱなし」にならないように、定期的に教育担当者による進捗管理を行い、進捗や結果が思わしくない従業員に対しては必ずフォローし、原因を明らかにし、教育・周知にモレがないようにしましょう。

- ｅラーニングシステムの受講結果で高得点であった従業員が必ずしも日々の運用でルールを守るとは限りません。

  ≫教育内容の理解度と自らの自覚によってルールを順守することは、必ずしも同一ではないということを認識し、日々の点検の中でチェックし、コミュニケーションにより補完しましょう。

セキュリティ教育のゴール
～ 従業員の理解と自覚を目指して ～

- ルールを組織に定着させるには、教育による従業員の理解と自覚が必要です。



◎組織が情報セキュリティに取り組む目的
◎組織が抱えるリスクの認識
◎セキュリティ事故・事件が起こった際に、組織・従業員が被る損失

◎概念的な教育と社内の具体的なルールの周知

◎教育により情報管理に対する理解が深まり、役割と責任を理解

◎情報管理の理解によって、責任感のあるルールの運用が可能
◎順守やインシデント等への対応状況を点検

◎社会情勢の変化や組織の対応レベルに応じてルールを定期的に見直し、改善する

◎組織の一員としてルールを順守することの自覚をもつ

◎意識の定着化とルールに沿った運用の実現

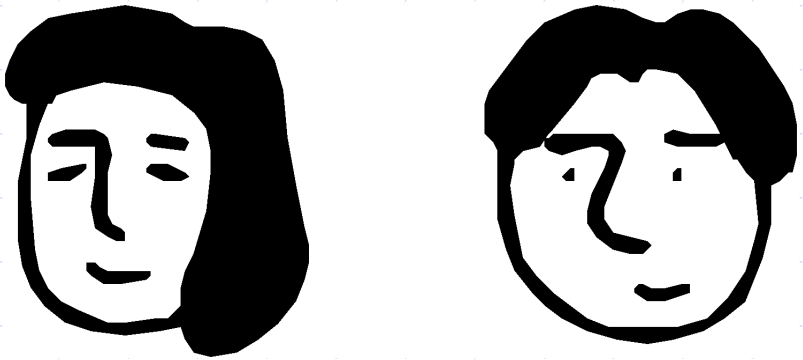
自組織にとって有効なセキュリティ教育を考える

有効なセキュリティ教育を実施するには何が必要でしょうか？

- 情報セキュリティの目標・方針を明確にする
- 守るべき対象（自社にとって価値のある情報・資産・サービス等）を特定する
- 守るべき資産がさらされる脅威を特定する（何から守る？）
- 資産のぜい弱性を、その性質や取扱いプロセスから特定する（その予防策は？）
- 組織の情報セキュリティの目的に沿って、リスク対策のためのルールを整備する
- 従業員や関係者に十分周知・教育する。また常に点検しその実効性を検討する
- 継続的に実施運用し、最適化し、組織に定着させる

情報セキュリティマネジメントシステムへの取り組み

だから、eラーニング！！



情報マネジメントで
組織を変え、人を変え、
仕事を変える！

CDNS

株式会社 コミュニケーションデザインネットワークス
マネジメントシステム構築・運営支援室　06-6946-9827　www,cdns.co.jp