「NTTデータ等におけるセキュリティ教育の事例、全社員の情報セキュリティ意識の底上げを目指して」

ｅーアセスメント手法

２００５年7月

株式会社ＮＴＴデータ・コミュニティプロデュース

1．情報セキュリティに対する脅威について

● 情報セキュリティに対する脅威区分

①外部からの脅威

- 不正アクセス
  - ●ポートスキャンやパスワード攻撃
  - ●サービスを停止させるための攻撃（DoS）
- ウィルス・ワームの感染

主に、技術・運用面での脆弱性から生じやすい

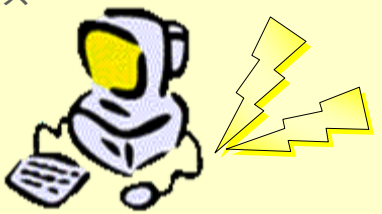
②内部からの脅威

- **故意（モラル欠如）**
  - ●情報漏えい（盗難）・持ち出し、改ざん、なりすまし
- **過失または意識欠落**
  - ●書類の放置・紛失・遺失・軽率な廃棄
  - ●プライベートシーンでの情報漏えい（愚痴こぼし等）
  - ●操作ミス（誤配信、原本上書き）　●インターネットの私的利用
  - ●重要データの自宅持ち帰り　●外部持込データによるウィルス感染
  - ●ID、PWの放置（パソコンに付箋紙で貼っておく）
  - ●バックアップデータを厳重管理していない　●違法サイトへのアクセス

主に、組織・人材育成面での脆弱性から生じやすい

③不測の脅威

- 故障及び災害
  - ●地震、雷、火災による、重要書類・データの消失
  - ●ハード故障、システム障害によるデータの消失



このような様々な脅威に対して、再認識が必要！

次に

優先順位付けも含め対策の検討が必要！

2．NTTデータにおけるセキュリティ教育

● eラーニングを使った情報セキュリティ教育からスタート

・平成１１年ごろより情報セキュリティ教育がスタート

当初、90分程度の「eラーニング」を実施

当時のeラーニングは、見て聞いているコンテンツ

↓

ユーザの実施率がなかなか上がらなかった

情報セキュリティポリシーの冊子の配布をしたが、

どの程度読まれたかが不明

・平成１２年、ｅーアセスメント手法へ変更

短い時間で受講できる設問とその解説を組み合わせたコンテンツ

↓

20問程度／平均受講時間20分とし、かつ中断機能で勤務の隙間時間の受講と積み重ねを可能にして、２ヶ月間で全社員が修了できるようにした

３．全員の情報セキュリティ意識を底上げさせるために

● NTTデータ　eーアセスメント手法に切り替えて効果大

・全社員教育を目的とした情報セキュリティ教育の修了率が大幅に向上。

・分かっていないことを“気づかせる”教育効果が向上。（単なるテストではない）

・いつ、だれに、なにを教え、その結果がどうであり、どう評価できたかの結果が数値化でき、課題の抽出分析と対策が、より具体的になった。

４．BS7799やISMS取得に効果あり

● NTTデータ

・平成１３年９月　ビジネス開発事業本部セキュリティ事業部
国内初　BS７７９９取得

・平成１４年５月　公共ビジネス事業本部ナショナルセキュリティビジネス事業部
BS７７９９取得

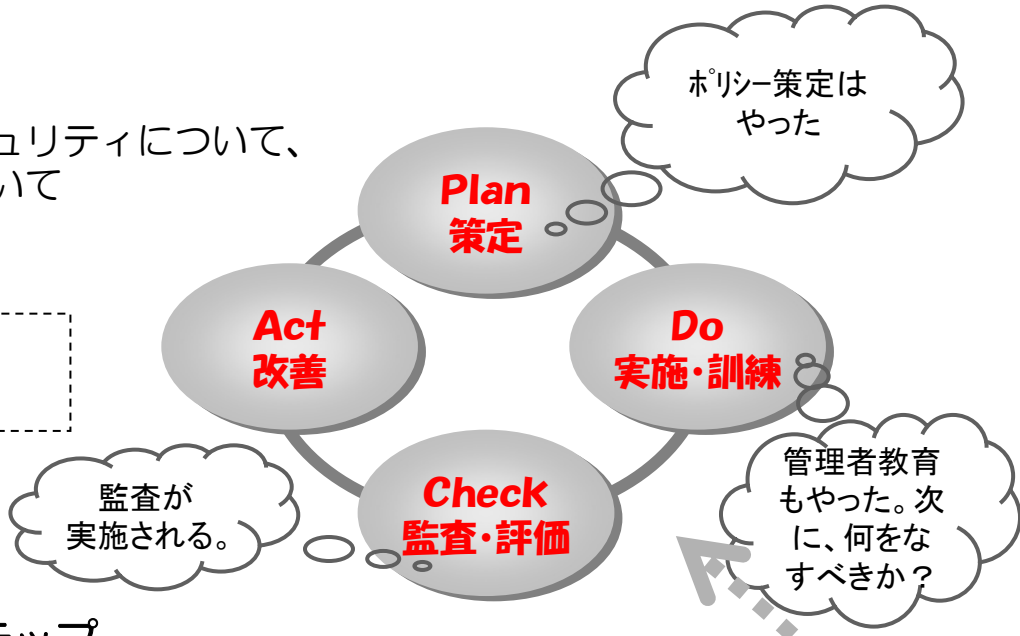
・平成１４年８月　ビジネス開発事業本部セキュリティ事業部
公共ビジネス事業本部ナショナルセキュリティビジネス事業部
ISMS認証取得

5．情報セキュリティマネジメントサイクル

● 継続的な情報セキュリティ対策の取組手法

情報セキュリティを実現するということは、情報セキュリティについて、
組織としての目標及び方針を定め、ＰＤＣＡ手法を用いて
継続的な達成を図っていくことです。

情報セキュリティマネジメントシステム（ISMS）
<information & security & management & system>



● 情報セキュリティ対策で注目すべきサイクルステップ

一般的には、ファイアーウォールの導入など、「物的対策」が先行しているものの、従業員全体の意識底上げなど「人的対策」は立ち遅れがちである。この点からも、「Ｃｈｅｃｋ」を意識した「人的対策」すなわち、人材育成（研修）に着目した取組みを優先することが必要であります。

● 情報セキュリティは低きに流れるため、１組織構成員の過失等が組織全体のセキュリティレベルと評価されます。
そのため、全組織構成員を対象とした情報セキュリティ意識の底上げが喫緊の課題となります。

6．組織における教育・研修の体系

組織の中では、現在、専門的教育から意識啓発レベルの教育まで様々な教育が実施されていますが、一部の社員や管理者向けの研修に留まり、全社員に対する啓発教育はコストや労力の関係で十分に実施されないケースが多く見られます。しかしながら、最近では組織のトップから従業員一人一人まで、全社員を対象とした意識啓発に繋がる“気付かせ”教育の重要性が再認識されてきています。

	対象者の階層	目　　的	具体的取り組み
研修（Training） 〈専門的教育〉	・管理者 ・専門担当者　等	すぐに実務に役立てるために、技能を訓練する。	・技術者向け集合研修 ・e-ラーニング ・マネジメント研修 ・ＯＪＴ　　等
教育 （Education） 〈一般的教育〉	・一般職員 ・新入社員　　等	実務に役立たせるだけでなく、継続的に知識を授与・共有する。	・資料配布 ・集合研修／セミナー ・e-ラーニング　　等
啓発 （Awareness） 〈意識向上〉	・組織に属する全員が対象	問いかけて気付かせる機会を多く与えることで、重要性を認識させる。	・アセスメント手法による“気づかせ”教育

7．早急に実現できる効果的な手法とは

● 全体の意識底上げを目的とした教育、すなわち、「全員教育」を実現するためには・・・

アセスメント手法	e-ラーニング等の教育・研修を、参考書形式ではなく、“設問形式”で実施することにより、日常的に意識すべき情報セキュリティの事柄を効果的に気づかせながら、受講履歴を残し、かつ結果の評価も同時に行える手法。

低負担で効果的に全員教育

意識統一　重点把握　即効性

従来のｅ-ラーニング

より多くの知識を集中的に教育

レベル別　専門的

8．アセスメント手法 の特長 ＃1

1．アセスメント手法の特徴

- 選択問題の形式をとることで、受講者の拘束時間を短縮するとともに、解答しながら意識すべき情報セキュリィを自然に気づかせることができる。
- 受講状況を確認しながら、未修了者に対してフォローができるため、全員受講に向けた取り組みが可能。
- 組織的取り組みを評価するための「記録・ログ」を蓄積することができる。
- 各々のｾｷｭﾘﾃｨﾚﾍﾞﾙがどの位置にあるのかを把握し、学習すべき事項を知るための動機づけとなる。
- 全体の底上げ施策として要求される全員対象の研修受講について、容易に、低負担かつ効果的に実施することが可能。

2．アセスメント手法の実施の考え方

アセスメント教材	約100問程度	必要な分野を網羅し、また繰り返し受講する際に、ランダムに出題することなどを考慮した問題数。
受講時出題数	20問	アセスメント受講の負担感を軽減し、業務の合間の受講であっても1回の操作で完了できる時間（20分程度）を想定した出題数。
受講期間	2ヶ月間程度	受講者の勤務都合等を勘案し、無理なく全員が受講することが可能な期間であり、同時に結果として得られるデータの信頼性を確保するために適切な期間。

8．アセスメント手法 の特長　#2

3．アセスメント手法のメリット

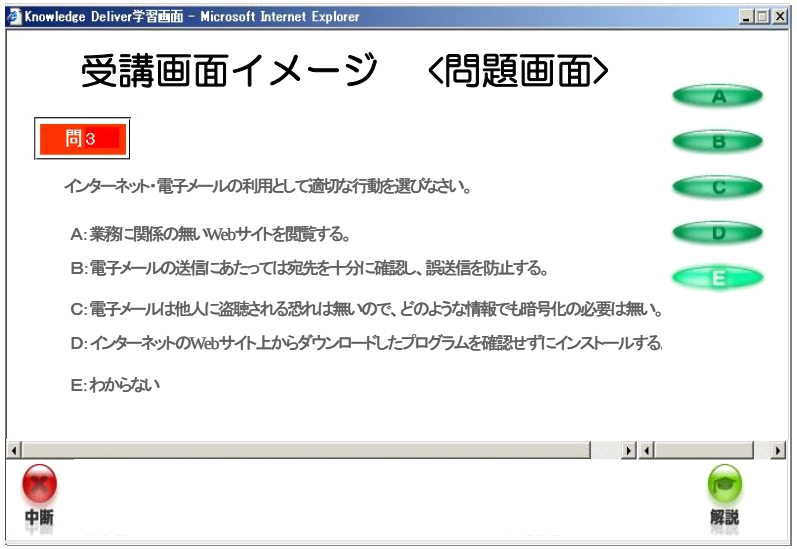
管理者メリット

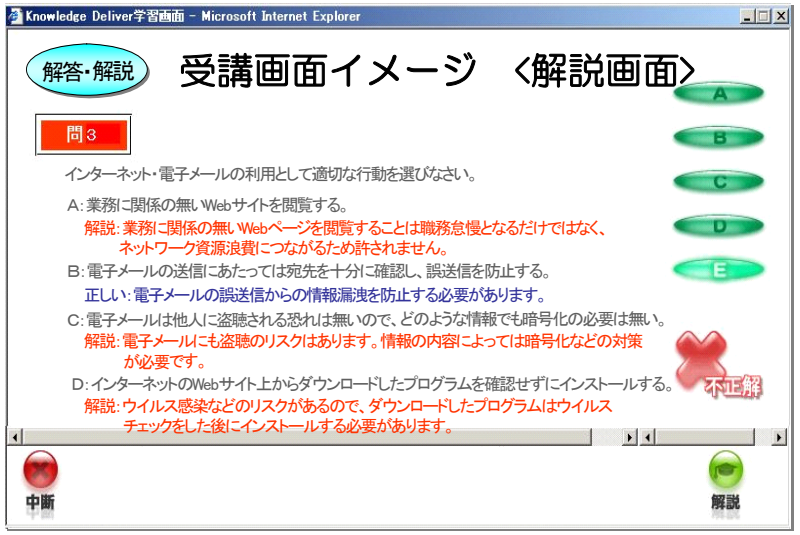
- 「解く」コンテンツであることにより、「見る」コンテンツよりも教育効果が高い。
- 少ない時間で実施できるため、受講者負担が低く、高い実施率を確保できる。
- リアルタイムに受講結果が蓄積されていくため、管理者が教育実績データとしてあるいは組織評価データとして活用できる。
- 設問を回答していく形で受講していくため、管理者が実施状況を細かく把握できる。
- テキストベースの設問であるため、コンテンツの追加やバージョンアップが行いやすい。

受講者メリット

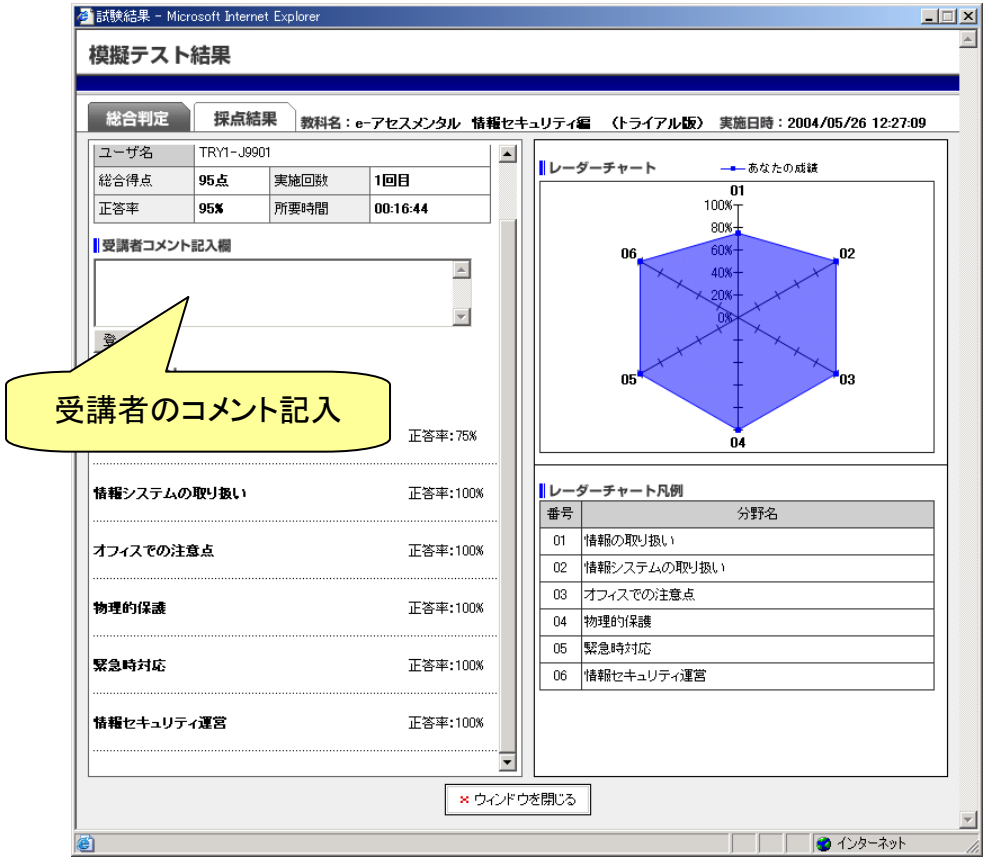
- 「解く」コンテンツであることにより、「見る」コンテンツよりも教育効果が高い。
- 少ない時間で実施できるため、業務の合間に負担無く実施できる。
- 毎回成績がすぐに出るため、自分の弱い部分を把握でき、モチベーションを維持できる。
- テキストベースの設問で構成されているため、システムのレスポンスが早い。
- 音声や動画が無く、音を出したりヘッドフォンをつける必要が無いので、周囲を気にせずに自席で受講することができる。

9．アセスメント受講画面のイメージ



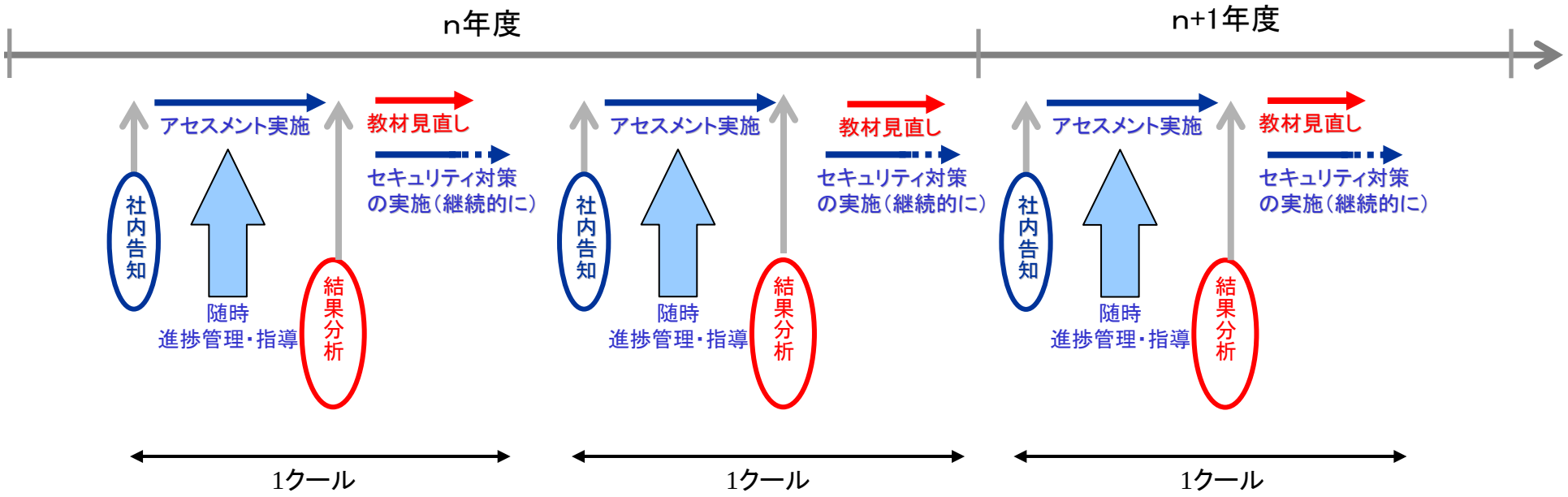


受講画面イメージ　〈結果画面〉



１０．研修計画イメージ

アセスメント実施結果を分析して、情報セキュリティに対する意識向上に向けた継続的活動のために、
自組織体の特性や環境変化に適応した教材見直し等を実施して、PDCAのライフサイクルをまわしていくことが必要です。



１１．情報セキュリティ教育＆評価の目的と要点

● 教育には、「予防策」と「事後防衛策」があります。

「予防策」とは、

全従業員を被害にあわせない、加害者とならない、過失を犯さないこと。
自分が管理している個人情報を漏洩させないためには、それなりの行動知識を習得しておく必要が　あります。

「事後防衛策」とは、

従業員が加害者となって社会的責任を問われた場合、企業としてのリスクを最小限に食い止める必要があり、その場合、企業がやるべき事をやっていたか否かで責任の度合いが異なってきます。

個人情報を扱う全従業員を対象に情報セキュリティ教育（関連法規教育、情報倫理教育を含めた）を実施していたことが申し開きの証拠データ（エビデンス）となります。
それには、あらかじめ受講実績データを確保しておく必要があります。

● 全従業員を被害者、加害者、過失者にさせないために、定期的、継続的かつ適宜的な基礎的教育が不可欠となります。

● 人間は忘れる動物であり、なにもしなければ情報セキュリティ意識やリスク認識は自然に低下する。

＊性善説、性悪説から「性弱説」の考え方。

１２．情報セキュリティ対策ベンチマーク

経済産業省から２００５．３末にパブリックコメント補足資料で提示された「情報セキュリティ対策ベンチマーク」に示されている成熟度構成（５段階）及び「情報セキュリティ報告書モデル」について

＜成熟度構成＞

１．経営層にそのような意識がないか、意識はあっても方針やルールを定めていない。

２．経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実施できていない。

３．経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。

４．経営層の指示と承認のもとに方針やルールをさだめ、全社的に周知・実施しており、かつ責任者による状況の定期的確認　　も行っている。

５．４．に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している。

＜情報セキュリティ報告書モデル＞

情報セキュリティガバナンスのレベル確保をステークホルダーに定期的に説明する資料とする。

１３．コンプライアンス・マネジメントの実務的課題　＃１

米国企業が試行錯誤しながら取り組んできたコンプライアンス・マネジメント経営の実務的課題

「コンプライアンス・マネジメント」 KPMGビジネスアシュアランス社[著]から引用

● **組織の業種・業態により千差万別**であり、また**経済情勢や法規制環境の変化、消費者の価値観の変化等、企業を取り巻く環境変化に伴ってリスクは常に変容する。**

＝＞環境変化に適応した対応ができることが必要であり、教育内容の高いメンテナンス性が求められる。

● 法規制遵守の基本的な役割は、**会社の倫理的な価値観を従業員に浸透させることであり、法令に関する詳細な解説書の配布ではない。**

＝＞企業倫理の価値観を全従業員に浸透させる教育プログラムが求められる。

従業員に会社の倫理的価値観を植え付けることができれば、詳細な法令の理解を促さなくとも自ら会社の倫理価値観に基づく意思決定を促すことができるものである。

● 法律の解説を中心としたコンプランアンス・トレーニングほど従業員にとって退屈なものはない。

実務的な話を盛り込んでほしいという現場との意見が多い。

＝＞現場の目線で従業員の日々の勤務に直接影響のある教育プログラムが求められる。

学問的アプローチ、いわゆる“詰め込み式の教育”は、現場の従業員に真の意味を身につけさせるアプローチとしては限界がある。

● 学習環境の問題点

①受動的学習　②抽象的学習　③実務とは無関係なテーマ選択と不適切な理解度評価

日々の業務に関する法令・規則等を実務的に適用させるアプローチが必須要件である。

１３．コンプライアンス・マネジメントの実務的課題　＃２

● CBT（一般的なe－ラーニング）の問題点

コンピュータ固有の**“インタラクティブな機能”（双方向通信）**を採用したCBTは少ないのが現状である。

紙で作成するテキストが電子的データに変更されただけで、単にページをめくるのが“手からクリックに変わった”ことだけが従来のトレーニングからの変更点となっている。

したがって、もたらされる効果は**従来からの伝統的な学校形式のトレーニングと全く変わらない。**

①学習者がテキストを読み、ビデオやアニメを見る等、**受動的な行為が受講者の役割になっている。**

②法理論や方針等の解説が中心であり抽象的で実務的でない。

③一般的なe－ラーニングは採点や評価がし易いよう設計されているため非実務的なテストやクイズ等が多くなっている。

● コミュニケーション 「情報の伝達と分かち合い」

分厚い資料の配布しても、**従業員に読まれ、理解されるものでなければ「情報の伝達と分かち合い」は実現できない。**

「規制当局に対してコンプライアンス・プログラムを実行していることを説明するために、そうした資料は必要なのだ」とする当事者もいるが、果たしてそれで十分であろうか。

今企業に求められるコンプライアンスに関する説明責任は「実効性」をいかに実現しているかである。

企業は「１つの組織体」であっても、そこで働く「組織体の構成部品」である従業員は価値観も、ものの考え方もそれぞれ違う。 そうした従業員との「情報の伝達と分かち合い」をしていることの説明責任を果たすためにはどのような視点でコミュニケーションすれば良いか。

重要な点は、従業員との間でコミュニケーションをしたという事実を共有化できるシステムを構築することである。

有効なコンプライアンス・コミュニケーションを実現するためには、従業員に関連する法律の内容を理解させることだけではなく、**その従業員の置かれている立場でコンプライアンスの必要性を理解させることが重要となる。**

１４．e-アセスメント方式の主な導入事例

事業者	時期	対象者数	備考
１．ＮＴＴデータ	平成12年～　年２回	全社員10,000人	ＩＳＭＳ＆Ｐマーク取得後の実践
２．大手物販事業者	平成１６年１０月～１１月	全社員7,000人	Ｐマーク取得後の実践研修
３．通信事業者	平成１６年３月から４月 平成１７年２月	全社員350人 全社員600人	派遣社員比率約50%以上 Ｐマーク申請のための研修
４．大手人材派遣事業者	平成17年３月	全社員7,000人	Ｐマーク取得後の実践研修
５．都内自治体	平成17年３月	職員1,000人で部分導入	全職員4,000人の定期的な研修を計画
６．都内自治体	平成17年2月～３月	職員2,500人	全職員人の定期的な研修を計画

●利用者からの主な声

管理者、経営者の声

●受講負担が少ないので、全社員にやらせても、反発が少ない。
●受講率や正答率が随時管理できるので、未受講者や正答率が低い受講者に対する再受講通知や、管理者に対する催促がしやすい。
●全社員に対する研修実施の実績が、数値データとして残るので、社内的にも対外的にも、教育実績として証明できるエビデンスデータが簡単に残せる。
●事前に基礎知識等の冊子を全員に配布したが斜め読み程度であり、e-アセスメンタルを受講してから、しっかり読み直すのが現実であった。

受講者の声

●空いた時間に数問ずつ実施できるので、業務の合間でも無理なく受講できる。これなら定期的にもやれそう。
●問題を解くのは、ただ教科書を読むより、モチベーションを維持できるので、より頭に残りやすい。