情報セキュリティ教育カリキュラム（モデル）

第１部　情報セキュリティの基礎

第１章　情報とマネジメント

経営における情報の資産としての位置付けや価値について学ぶとともに、情報資産に関する最新の動向について修得することを目標とする。

１．情報資産とは

情報資産の定義と対象範囲について学ぶ。

(1)指導すべき内容
- ・情報と情報資産の関係について教える
- ・情報資産とは何か、どのように定義されているかを教える
- ・経営面からの情報資産の範囲を教える

(2)指導上の留意点
- ・情報には電子化情報以外も含む
- ・業務上で作成した情報は全て組織体の情報資産である

２．情報資産の重要性

情報資産の価値、経営への貢献度、経営環境の変化による資産への影響度について学ぶ。

(1)指導すべき内容
- ・企業経営において情報資産が果たす役割について教える
- ・経営管理と情報鮮度について教える
- ・見通し情報の重要性について教える

(2)指導上の留意点
- ・情報価値の収入と支出とのバランスなどを引用して説明する

３．情報資産の健全な運用

情報資産の効果的活用の方策、情報の資産価値維持の方策について学ぶ。

(1)指導すべき内容
- ・情報資産管理のポイントを教える
- ・重要情報の取扱いについて教える
- ・情報の更新など運用面の大切さを教える

(2)指導上の留意点
- ・情報開示方法の不適切さによる企業ダメージの事例を示す
- ・ネットワーク以外からの情報漏洩の事例を示す

４．情報資産をめぐる問題

情報の開示や漏洩など、情報資産をめぐる諸問題について学ぶ。

(1)指導すべき内容
- ・情報の漏洩、情報の優位性について教える
- ・情報資産の所有をめぐる問題について教える

(2)指導上の留意点
- ・予期せぬ開示による価値喪失や権利侵害を示す(特許申請前の内容開示など)

第２章　情報資産とリスク

情報資産に対する脅威となるリスクの種類と実態について修得することを目標とする。

1．リスクとは

リスクの種類と影響について学ぶ。

(1)指導すべき内容
・リスクとは何か、どのように分類されているかを教える
・リスクが顕在化した場合にどのような影響が出るか教える
(2)指導上の留意点
・リスクの顕在化は組織体に損害を与える
・リスクへの対応策が情報セキュリティである

2．情報資産をめぐるリスク

情報資産に対するリスクについて学ぶ。

(1)指導すべき内容
・情報資産に対するリスクの実例として、どのようなものがあるかを教える
・自然災害、故障・障害、不正行為の事例研究を行う
(2)指導上の留意点
・特に、人に起因する不正行為（犯罪等）の対策が重要である

3．情報資産への不正行為

不正行為の種類と内容について学ぶ。

(1)指導すべき内容
・不正行為の種類と内容について教える
・コンピュータシステム、ネットワーク等のハードウェア、ソフトウェアに対する破壊行為、プログラムやデータファイルの改ざん・消去、システムへの不正侵入・不正使用の事例研究を行う
(2)指導上の留意点
・不正行為の最新の事例を示す

第３章　情報セキュリティとは何か

情報セキュリティの基本として、情報取扱の基本原則、情報活用の視点、情報セキュリティの目的について修得することを目標とする。

1．情報取扱の原則

情報を開示する範囲や対象者、情報内容の変更権限、情報の参照や変更に関する記録について学ぶ。

(1)指導すべき内容
・情報開示の範囲、方法および対象者について教える
・情報の利用目的と利用制限について教える
・情報の参照と変更の権限について教える
(2)指導上の留意点
・機密レベルによって情報の取扱が異なる

2．情報の活用と保護の両立

情報資産価値を最大化する情報活用と情報資産保護の両立のさせ方について学ぶ。

(1)指導すべき内容
・情報資産の有効活用と適切な保護について教える
・情報保護だけを優先するのではなく、情報活用も重要であることを教える
(2)指導上の留意点
・情報の鮮度や精度は活用されないことによって低下する
・保護と活用のバランスをとることの難しさと重要性を考慮する

３．情報セキュリティの目的

情報セキュリティの目的と定義について学ぶ。

(1)指導すべき内容
・情報セキュリティの原則について教える
・管理レベルの維持、向上について教える
・特定の従業員だけでなく、全組織への徹底を教える
(2)指導上の留意点
・経営環境の変化に対応した見直しが必要である

第２部　管理的セキュリティ

第１章　情報セキュリティ管理の基本

情報セキュリティ管理規程、組織・推進体制、機密情報管理、およびアクセスコントロールの基本を修得することを目標とする。

１．情報セキュリティ管理規程の意義と役割

情報セキュリティ管理規程の必要性、目的、および内容について学ぶ。

(1)指導すべき内容
・情報セキュリティポリシーの重要性を教える
・企業経営の立場から情報セキュリティ管理規程の意義を教える
・情報セキュリティ管理規程の一般的な構成と内容を教える
(2)指導上の留意点
・実際に情報セキュリティ管理規程を作成する際には個々の組織の特性も考慮する

２．組織・推進体制

情報セキュリティ管理を推進するための組織と体制について学ぶ。

2.1　責任・権限

組織や社員の責任と権限について学ぶ。

(1)指導すべき内容
・情報セキュリティ管理のための組織を教える
・全体を統括する担当役員および各部門の情報セキュリティ管理者の責任と権限を教える
(2)指導上の留意点
・実際の推進体制に組織の特性を反映させる

2.2　役割と周知徹底

情報セキュリティ担当の役割と情報セキュリティの周知徹底の重要性について学ぶ。

(1)指導すべき内容
・担当役員と情報セキュリティ管理者の具体的な役割を教える
・情報セキュリティの社員全員への周知徹底の重要性と方法を教える
(2)指導上の留意点
・周知徹底のためには、継続的な啓蒙と全員参加が重要である

３．機密情報管理

機密情報の定義、情報の機密レベルおよび機密情報の管理方法について学ぶ。

3.1　機密情報の定義

機密情報の分類と内容について学ぶ。

(1)指導すべき内容
・機密情報とは何か、について教える
・機密情報にはどのような種類があるかを教える
(2)指導上の留意点
・機密情報には取引先の情報も含まれる

3.2　機密レベルの設定・運用

情報に対する機密レベルの設定の重要性、方法と運用について学ぶ。

(1)指導すべき内容
・企業経営に対する影響の観点から機密レベルを設定することを教える
・機密レベルの設定方法と運用の方法を教える
(2)指導上の留意点
・環境の変化に伴い機密レベルは変化する

3.3　機密情報の管理方法

機密情報の保護と開示の方法について学ぶ。

(1)指導すべき内容
・機密情報の保護方法を教える
・機密情報開示の条件設定と開示の方法を教える
(2)指導上の留意点
・機密レベルに応じて保護と開示の方法は異なる
・機密情報の廃棄には十分な注意が必要である

4．アクセスコントロールの意義と目的

不正防止策としてのアクセスコントロールの重要性について学ぶ。

(1)指導すべき内容
・アクセスコントロールとは何か、なぜ重要かを教える
・アクセスコントロールの基本的なルールを教える
(2)指導上の留意点
・アクセスコントロールには、ネットワークを介してのアクセスコントロールだけではなく、物理的なアクセスコントロールも重要である

第2章　リスク分析と情報セキュリティ

リスク分析と情報セキュリティのレベル設定について修得することを目標とする。

1．リスク分析とは

リスク分析の定義と分析の方法について学ぶ。

(1)指導すべき内容
・リスク分析とは何かを教える
・リスク分析の意義と目的について教える
・リスク分析の方法について教える
(2)指導上の留意点
・リスクの定量化についても言及する

2．情報セキュリティのレベルの考え方

情報資産の機密レベルに応じて情報セキュリティの強度レベルを設定することの意義と方法を学ぶ。

(1)指導すべき内容
・リスク分析の結果に応じて情報セキュリティの強度レベルを設定することを教える
・情報セキュリティの強度レベル設定の方法について教える
(2)指導上の留意点
・情報セキュリティの脆弱性が対外的に影響を及ぼすこともある

3．情報セキュリティの評価

リスクの変化に応じて情報セキュリティを常に見直し、対策を講じることの重要性を学ぶ。

3.1 自己点検

当事者が自ら常に、情報セキュリティの状況を自己点検することの意義を学ぶ。

(1)指導すべき内容
・情報セキュリティについて、定期的に自己点検することの重要性を教える
・自己点検の結果、不備が発見された場合の対応策について教える
(2)指導上の留意点
・点検はセルフアセスメントシート等を利用して行う

3.2 定期的レビュー

情報セキュリティ推進部門が情報セキュリティの状況を定期的にレビューすることの重要性を学ぶ。

(1)指導すべき内容
・定期的にレビューし、情報セキュリティの状況を確認することの重要性を教える
・情報せキュリティが確保されてない場合の対応策について教える
(2)指導上の留意点
・情報セキュリティの PDCA サイクルの確立が必要である

第３章　バックアップ対策

障害および災害に備えたバックアップ対策について修得することを目標とする。

１．バックアップの基本

バックアップの必要性と考え方について学ぶ。

(1)指導すべき内容
・バックアップの対象としてどのようなものがあるかを教える
・バックアップのタイミングについて教える
・業務の優先度と回復許容時間を考慮した対策について教える
・バックアップの適切な保管方法・場所について教える
(2)指導上の留意点
・復元可能な状態にすることが重要である

２．障害からの復旧

障害から復旧させる方法について学ぶ。

(1)指導すべき内容
・冗長性を持たした情報システムの構成について教える
・情報システムの代替運転機能について教える
・データを復旧する機能について教える
(2)指導上の留意点
・バックアップ機能については人間系を重視する
・万一障害が発生してもその影響を最小限に止め、できるだけ速やかに復旧させることが重要である

３．災害からの復旧

大災害から復旧させる機能について学ぶ。

(1)指導すべき内容
・遠隔地での代替運転機能について教える
・回復許容時間に応じたバックアップ機能について教える
(2)指導上の留意点
・人間系が重要であり、訓練が必要である
・万一災害が発生してもその影響を最小限に止め、できるだけ速やかに復旧させることが重要である

第４章　緊急事態への対応

大規模災害の発生に備えた緊急時対応計画と訓練の重要性について修得することを目標とする。

１．計画の策定

緊急時対応計画の重要性と策定方法について学ぶ。

(1)指導すべき内容
・緊急時対応計画とは何か、どのような内容か、なぜ重要かを教える
・計画の策定方法について教える
(2)指導上の留意点
・実行性のある計画でないと意味がない

２．定期的訓練

緊急時に備えた訓練を定期的に実施することの重要性と実施方法を学ぶ。

(1)指導すべき内容
・定期的訓練はなぜ必要かを教える
・具体的な訓練の実施方法を教える
(2)指導上の留意点
・訓練は実際の環境に合わせて実施する

３．計画の見直し

訓練の実施結果やリスクの変化を勘案して、計画を定期的に見直しすることの重要性と見直し方法を学ぶ。

(1)指導すべき内容
・情報環境の変化に伴うリスクへの影響分析について教える
・定期的な計画の見直しの重要性について教える
・計画の見直し方法について教える
(2)指導上の留意点
・リスクに関する情報収集に努める

第５章　システム監査

当事者から独立した立場の監査人が第三者の目で情報セキュリティの状況を監査し、関係者に助言・勧告するシステム監査について修得することを目標とする。

１．システム監査の意義と目的

情報セキュリティに関するシステム監査の意義と目的について学ぶ。

(1)指導すべき内容
・システム監査とは何かを教える
・情報セキュリティ監査の重要性を教える
・費用対効果の高いセキュリティ対策を可能とするため、システム監査が有効であることを教える
(2)指導上の留意点
・経営の観点から効率性を評価する

２．システム監査の実施手順

情報セキュリティに関するシステム監査の実施体制、手順について学ぶ。

(1)指導すべき内容
・システム監査は第三者による評価であることを教える
・システム監査基準について教える
・システム監査の実施体制、手順およびスキルについて教える
(2)指導上の留意点
・システム監査のポイントは「情報システムの信頼性、安全性および効率性の向上」、牽いては「情報化社会の健全化を図ること」

第３部　システム的セキュリティ

第１章　アクセスコントロール

情報システムに具備すべきアクセスコントロールの仕組みについて修得することを目標とする。

１．アクセスコントロールの機能

情報システムが具備すべきアクセスコントロール機能について学ぶ。

1.1 リファレンスモニタの概念

リファレンスモニタの概念について学ぶ。

(1)指導すべき内容
・リファレンスモニタの基本的な考え方を教える
・リファレンスモニタの具体的な実現形態を教える
(2)指導上の留意点
・リファレンスモニタは情報セキュリティの基本である

1.2 コントロールの方法

機密レベルとカテゴリの組合せによる情報の利用におけるコントロール方法を学ぶ。

(1)指導すべき内容
・カテゴリの設定方法について教える
・機密レベルとカテゴリを組合せて管理することを教える
(2)指導上の留意点
・オレンジブックを参考にして指導する（米国コンピュータセキュリティセンター（NCSC）から出版された Department of Defense Trusted Computer System Evaluation Criteria(TCSEC)をオレンジブックと呼ぶ）

２．アクセスコントロールの運用

情報を保護するためのアクセスコントロールの運用について学ぶ。

2.1　アクセス権限の設定と付与

アクセスをコントロールするためのアクセス権限の設定と付与について学ぶ。

(1)指導すべき内容
・不正アクセスを防ぐためのアクセス資格設定と付与について教える
・アクセス資格に応じたアクセス権限に基づくコントロール方法を教える
(2)指導上の留意点
・アクセス権限は常に見直し、更新しないとコントロールの意味がない

2.2　アクセスの監視

アクセスは記録され、定期的にチェックされることを学ぶ。

(1)指導すべき内容
・アクセスを常時監視し、定期的にチェックする必要があることを教える
・アクセス監視に関する重要な対策について教える
(2)指導上の留意点
・アクセスの監視は不正発見等の早期発見に生かされなければならない

第２章　暗号

暗号の意義と仕組みおよび暗号化と機密レベルとの関係について修得することを目標とする。

1．暗号の意義

情報セキュリティから見た暗号の歴史と意義について学ぶ。

(1)指導すべき内容
・暗号の内容と歴史について教える
・暗号には秘匿と認証の２つの働きがあることを教える
(2)指導上の留意点
・暗号の強度には高低差がある

2．暗号の仕組み

暗号の仕組みについて代表的な２つの方法を学ぶ。

2.1 共通鍵暗号

共通鍵方式による暗号化の仕組みについて学ぶ。

(1)指導すべき内容
・共通鍵方式による暗号化の考え方を教える
・共通鍵方式の仕組みを教える
(2)指導上の留意点
・具体例として DES を取り上げる

2.2 公開鍵暗号

公開鍵方式による暗号化の仕組みについて学ぶ。

(1)指導すべき内容
・公開鍵方式による暗号化の考え方を教える
・公開鍵方式の仕組みを教える
(2)指導上の留意点
・具体例として RSA を取り上げる

3．機密レベルに応じた暗号化

機密レベルに応じて暗号化を図ることの重要性について学ぶ。

(1)指導すべき内容
・情報の機密レベルと暗号の強度との関係を教える
・機密レベルに応じて暗号化を採用する必要性を教える
(2)指導上の留意点
・暗号の強度は時間とともに低下するので、見直す必要がある

第３章　コンピュータウイルス対策

コンピュータウイルス（以下「ウイルス」とする）の種類と対策について修得することを目標とする。

1．ウイルスとは

ウイルスの定義、ウイルスに関する基本的用語および仕組みについて学ぶ。

(1)指導すべき内容
・ウイルスとは何か、どのような機能があるかを教える
・典型的なウイルスのタイプについて教える
・ウイルス対策の関係者と役割について教える
(2)指導上の留意点
・ワームについてはウイルスのひとつとして扱う

2．ウイルス感染の防止方法

ウイルス感染防止のための具体的な対策について学ぶ。

(1)指導すべき内容
・ウイルス感染防止についての諸作業（予防・発見・駆除・復旧）の流れを教える
・ウイルス感染防止のためのシステム構成を教える
(2)指導上の留意点
・ファイアウォール等の強度について定期的に評価する

3．ウイルスの監視と除去の方法

ウイルスの検知とワクチンによる除去の方法について学ぶ。

(1)指導すべき内容
・ウイルス対策の日常運用について教える
・ウイルスの検知と除去の方法について教える
(2)指導上の留意点
・パターンファイルは定期的に更新する

4．最新の情報収集と自己防衛策

ウイルスの種類と被害に関する情報収集の必要性、無意識に加害者になる可能性、および自己防衛対策の重要性について学ぶ。

(1)指導すべき内容
・最新のウイルスの種類と特徴を教える
・情報収集の必要性と方法について教える
・自己防衛の重要性について教える
(2)指導上の留意点
・無意識に加害者となる場合がある

第４章　不正アクセス対策

不正アクセスの定義、脅威および対策について修得することを目標とする。

1．不正アクセスとは

不正アクセスの定義、脅威、具体的事例について学ぶ。

(1)指導すべき内容
・不正アクセスとは何か、その脅威について教える
・不正アクセスに関する関係者の立場と役割を教える
・不正アクセスの事例研究を行う
(2)指導上の留意点
・企業にとって不正アクセスの事実は社会的信用失墜につながる場合がある

2.不正アクセス対策

不正アクセスを防止するための方法について学ぶ。

(1)指導すべき内容
・セキュリティホールの内容と対策について教える
・不正アクセス防止の方法を教える
(2)指導上の留意点
・ハード、ソフトの両方が機能してはじめて有効な防止策となる

第４部　物理的セキュリティ

第１章　防災対策

災害が発生した場合に、情報資産に対する影響度を最小限にとどめるための対策について修得することを目標とする。

１．地震対策

地震に備えた対策について学ぶ。

(1)指導すべき内容
・設置環境面における考慮点について教える
・地震発生時の人的被害の軽減策について教える
・復旧対策として、バックアップセンター等について教える
(2)指導上の留意点
・緊急時対応計画とのリンク

２．火災対策

火災に備えた対策について学ぶ。

(1)指導すべき内容
・設置環境面における考慮点について教える
・消化設備・排煙設備など、火災関連設備について教える
(2)指導上の留意点
・緊急時対応計画とのリンク

３．風水害対策

風水害に備えた対策について学ぶ。

(1)指導すべき内容
・設置環境面における考慮点について教える
・浸水および漏水等に対する対策について教える
(2)指導上の留意点
・緊急時対応計画とのリンク

第２章　防犯対策

情報資産に対する不正行為の影響を最小限にとどめるために考慮すべき対策について修得することを目標とする。

１，侵入破壊対策

情報資産の設置・保管場所に対する侵入防止・破壊防止対策について学ぶ。

(1)指導すべき内容
・防犯組織の整備など、防犯体制について教える
・建物の構造等で考慮する点や、侵入防止装置など設備面について教える
・建物管理上の留意点について教える
(2)指導上の留意点
・許可のない人の入館を取り締まる

２．盗難対策

情報資産の盗難の防止対策について学ぶ。

(1)指導すべき内容
・部外者からの盗難防止策としての、建物等の管理上の留意点について教える
・部内者による盗難に対する防止策について教える
(2)指導上の留意点
・部内者に対する盗難対策も重要である

3．不正使用対策

情報資産、特に情報システムの不正使用防止対策について学ぶ。

(1)指導すべき内容
・内部での情報システムの不正使用防止の必要性について教える
・外部からの情報システムの不正使用防止の必要性について教える
(2)指導上の留意点
・不正使用は人に依存する

第３章　入退館（室）管理

建物への入退館管理、情報資産の設置・保管されている部室への入退室管理について修得することを目標とする。

1．入退館管理

入退館管理を実施するための設備および運用について学ぶ。

(1)指導すべき内容
・入退館管理の設備の具体例について教える
・入退館管理の運用面での留意事項について教える
(2)指導上の留意点
・入退室管理と重複する項目についてはまとめて実施する

2．入退室管理

入退室管理を実施するための設備および運用について学ぶ。

(1)指導すべき内容
・入退室管理の設備の具体例について教える
・入退室管理の運用面での留意事項について教える
(2)指導上の留意点
・入退館管理との差異を意識する

第５部　人的セキュリティ

第１章　不正予防対策

不正行為に対する予防策のあり方について修得することを目標とする。

１．相互牽制

担当者相互間における不正防止のための牽制について学ぶ。

(1)指導すべき内容
- ・相互牽制の意義を教える
- ・内部牽制システムについて教える

(2)指導上の留意点
- ・特定の仕事を特定の人だけにまかせない

２．情報漏洩対策

情報の漏洩防止策について学ぶ。

(1)指導すべき内容
- ・情報管理ルールの周知徹底の重要性を教える
- ・媒体別の情報管理のあり方と情報漏洩防止策を教える
- ・情報漏洩がどのような影響を与えるかを教える

(2)指導上の留意点
- ・いったん漏洩すれば、情報の資産価値は減少する

３．遵守義務と罰則規程

不正防止のために組織体で定められている遵守義務や罰則規程について学ぶ。

(1)指導すべき内容
- ・業務関連法規、業界のガイドライン、組織体の各種規程に基づく遵守義務を教える
- ・業務関連法規、組織体の各種規程による罰則規程を教える

(2)指導上の留意点
- ・規程や慣習などの関連するルールを周知徹底する
- ・業務上過失が問われるケースを理解させる

第２章　情報倫理

情報倫理の社会的な背景と必要性、情報環境における倫理の問題について修得することを目標とする。

１．情報倫理とは

情報倫理が問題となった社会的背景と情報倫理の重要性について学ぶ。

(1)指導すべき内容
- ・法的あるいは技術的手段では対応できない情報セキュリティ上の問題の増大と社会的背景を教える
- ・情報倫理とは何か、その重要性を教える

(2)指導上の留意点
- ・職業倫理との関連に触れる

２．情報管理と情報倫理

情報の活用と管理において望まれる行為規範について学ぶ。

(1)指導すべき内容
- ・情報の活用と管理の場でなされる個人による行為の善悪を判断する規範を教える
- ・個人情報の保護、知的所有権の保護との関連を教える

(2)指導上の留意点
・組織として情報倫理に取り組む姿勢が重要

3．情報システムと情報倫理

情報システムの利用において望まれる行為規範について学ぶ。

(1)指導すべき内容
・情報システムを利用する個人がとる行為の善悪を判断する規範を教える
・ソフトウェアの知的所有権、コンピュータ犯罪の不法性との関連性について教える
(2)指導上の留意点
・組織として情報倫理に取り組む姿勢が重要

第３章　教育訓練

情報セキュリティ管理を徹底するために、教育訓練の必要性と実施方法について修得することを目標とする。

1．教育訓練の必要性

情報セキュリティ教育が必要とされる理由について学ぶ。

(1)指導すべき内容
・情報セキュリティは人に依存するため、教育が重要であることを教える
・効率よい運用のための教育方法を教える
(2)指導上の留意点
・前提となる情報資産教育も含める
・従事者に情報セキュリティの意識を喚起するための教育が重要

2．対象別教育訓練

情報セキュリティ教育を実施するにあたり、階層別、職種別、部門別など、対象別教育の重要性と実施内容を学ぶ。

2.1　階層別教育訓練（役員、管理者、一般社員）

従業員の階層ごとに、徹底すべき情報セキュリティの内容が異なるため、立場に応じた教育について学ぶ。

(1)指導すべき内容
・経営者・管理職には、立場にふさわしい情報セキュリティ教育について教える
・担当者には、具体的な情報セキュリティ教育について教える
(2)指導上の留意点
・教育訓練の目的の明確化と、具体的なプログラムを作成する

2.2　職種別教育訓練（営業、技術、情報管理者、情報セキュリティ管理者等）

業務特性に合わせた情報セキュリティ教育について学ぶ。

(1)指導すべき内容
・職種により、情報セキュリティに関する役割が異なることを教える
・職種により扱う情報資産が異なり、情報セキュリティ機能にも違いがあることを教える
(2)指導上の留意点
・情報システム職には、電子化情報の保護を重視する
・営業職には、顧客に開示する社内情報、顧客の機密情報･個人情報の取扱いを重視する
・技術職には、機密保持契約(ＮＤＡ)の対象となる情報の取扱いを重視する

2.3　部門別教育訓練

部門特性に合わせた情報セキュリティ教育について学ぶ。

(1)指導すべき内容
・部門ごとに扱う情報が異なることを教える
・部門特性に応じた教育が必要であることを教える
(2)指導上の留意点
・他部門からの転入があった場合や、新入社員が配置された時など、その部門固有の留意事項を徹底させる

3．タイミング別教育訓練

企業での従業員のライフサイクルに合わせた情報セキュリティ教育の重要性と実施内容を学ぶ。

3.1 入社時教育訓練

情報セキュリティに関し、入社時に徹底すべき内容について学ぶ。

(1)指導すべき内容
・新入社員へ情報セキュリティの基本と自社ルールを教える
・中途採用者へ情報セキュリティの自社ルールを教える
(2)指導上の留意点
・他社や研究機関との機密保持契約の有無と、勝手な判断での情報活用を禁止する

3.2 昇進・異動時教育訓練

昇進時や異動時に、教育すべき情報セキュリティの内容について学ぶ。

(1)指導すべき内容
・節目教育として、昇進時や異動時の情報セキュリティ教育の重要性を教える
・管理職昇格時、情報資産と情報セキュリティ管理責任者としての教育を教える
(2)指導上の留意点
・立場や役割が変更され、新たな立場や役割にふさわしい教育であること

3.3 定期的教育訓練

情報セキュリティの継続的な徹底方法としての定期的な教育訓練の重要性と実施方法について学ぶ。

(1)指導すべき内容
・従業員に情報セキュリティに関する注意喚起のための定期的訓練の重要性を教える
・教育内容は常に最新にしておくことを教える
(2)指導上の留意点
・最低限、年一回の教育訓練が必要である

4．学校における情報セキュリティ教育

企業における情報セキュリティ教育と同様に、学校における情報セキュリティ教育の重要性を学ぶ。

4.1 高校における情報セキュリティ教育

高校生として理解すべき情報セキュリティの内容について学ぶ。

(1)指導すべき内容
・インターネット利用におけるマナーとルールについて教える
・不正利用、個人情報保護の具体的内容に絞って教える
(2)指導上の留意点
・携帯電話、パソコンによるインターネットやｅメールの利用機会増など要注意

4.2 大学における情報セキュリティ教育

大学生としての情報セキュリティの基本的事項を学ぶ。

(1)指導すべき内容
- ・社会に出る前に修得すべき情報セキュリティの基本を教える
- ・情報セキュリティ関連専攻の学生には、企業教育と同等の内容を教える

(2)指導上の留意点
- ・研究活動において知り得た機密情報の守秘義務や卒業後の開示制限に注意する
- ・大学生全員を対象とする

第６部　情報セキュリティ関連ルール

第１章　個人情報保護

情報資産としての個人情報を保護するためのルールについて修得することを目標とする。

1 個人情報保護の意義

個人情報を保護することの意義について学ぶ。

(1)指導すべき内容
・個人情報とは何か、なぜ保護される必要があるかを教える
・個人情報が有用な情報資産として活用されるようになってきていることを教える
・個人情報の自由な流通と有効活用を促進しながら、一方では個人のプライバシーを守る必要が高まってきていることを教える
(2)指導上の留意点
・個人情報を取り扱う場合の留意点を示す

2 個人情報保護のための法律・ガイドライン

個人情報を保護するために制定されている法律やガイドラインについて学ぶ。

(1)指導すべき内容
・個人のプライバシーを守るために法律やガイドラインが制定されていることを教える
・OECD プライバシーガイドライン、個人情報保護法、個人情報保護ガイドライン、プライバシーマークの概要を教える
(2)指導上の留意点
・プライバシー侵害は犯罪である

第２章　コンピュータ犯罪防止

コンピュータ犯罪を取り締るための法律・ガイドラインについて修得することを目標とする。

1 コンピュータ犯罪の種類

どのようなコンピュータ犯罪が起きているか、その種類について学ぶ。

(1)指導すべき内容
・コンピュータ犯罪とは何か、どのような種類があるかを教える
・コンピュータ犯罪の具体的事例を交えて教える
(2)指導上の留意点
・情報漏洩、不正アクセス等が急増している

2 コンピュータ犯罪防止のための法律・ガイドライン

コンピュータ犯罪を防止するために制定されている法律やガイドラインについて学ぶ。

(1)指導すべき内容
・コンピュータ犯罪を取り締るために法律やガイドラインが整備されていることを教える
・刑法（コンピュータ犯罪関連)、不正アクセス禁止法等の概要について教える
(2)指導上の留意点
・法律・ガイドラインはまだ整備の過程にある

第３章　情報セキュリティ基準・標準

情報セキュリティを確保するための国際および国内の基準・標準の制定のねらいとその概要について修得することを目標とする。

1 情報セキュリティに関する国際基準・標準

情報セキュリティに関する国際基準や標準について学ぶ。

(1)指導すべき内容
・情報セキュリティを確保するために国際基準・標準が制定されていることを教える
・OECD 情報セキュリティガイドライン、ISO17799、ISO15408、BS7799、ISMS 等の制定のねらいと概要を教える
(2)指導上の留意点
・国際基準、標準は必ずしも国際統一基準・標準ではない

2 情報セキュリティに関する国内基準・標準

情報セキュリティに関する国内基準や標準について学ぶ。

(1)指導すべき内容
・国内の基準・標準が制定されていることを教える
・JIS17799、ISMS、システム監査基準、情報システム安全対策基準、コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準等の制定のねらいと概要を教える
(2)指導上の留意点
・あくまでも基準・標準であり、法律のような強制力はないが、諸認定・認可等で利用されてきている

第４章　知的所有権

情報資産の知的所有権について修得することを目標とする。

1 知的所有権とは

情報資産を保護するための知的所有権の意義と役割について学ぶ。

(1)指導すべき内容
・知的所有権とは何かとその意義について教える
・知的所有権の役割について教える
(2)指導上の留意点
・情報資産は無形資産であり、必ずしもその重要性は認知されていない

2 知的所有権法の種類と内容

知的所有権法として制定されている法律の種類と内容について学ぶ。

(1)指導すべき内容
・知的財産を守るための法律として、知的所有権法が制定されていることを教える
・不正競争防止法、著作権法、特許法、商標法等の概要を教える
(2)指導上の留意点
・法の対象範囲は広いため、関連する部分に限定する