

## 三鷹 ICT 事業者協会からのお知らせ

# 2009 年度 IPA 情報セキュリティセミナー

～ 情報化社会における企業の情報セキュリティ対策について～  
経済産業省・IPA・日本商工会議所と共同で開催 !!

今日、産業や政府活動、国民生活の多くがコンピュータやコンピュータネットワークに依存し、IT は企業の競争力を高めるために必要不可欠な要素となっています。他方、企業や官公庁からの情報漏えい、パソコンの紛失や盗難などの事件が相次いで起きています。

情報セキュリティに関する事件に見舞われた時には、顧客に重大な損害を与え、自社に不利益をもたらすだけでなく、社会的責任を問われ、企業としての信用・信頼を失ってしまう恐れがありますが、このような状況はもはや他人事ではありません。

情報システム上で金銭や個人情報などを狙う手法、コンピュータウイルス・スパイウェアなどの不正なプログラムは、技術的に巧妙化していることに加え、人間の心理を巧みにつく手法を用いるなど、以前より格段に悪質になっています。事業者は事件・事故を未然に防ぐために日々最新の情報を入手し、技術的な対策や社内における人的管理、組織的管理や教育などの対策を講じる必要があります。

このような状況を踏まえ、企業や組織の経営者・部門長、セキュリティ担当者、システム管理者、ウェブサイト運営者、ウェブアプリケーション開発者を主対象に、情報セキュリティの管理面・技術面からの対策に関するセミナーを開催します。

### 開催概要

日 時	マネジメントコース入門編	1月 28日(木)	10:00 ~ 12:30
	マネジメントコース実践編	1月 28日(木)	13:30 ~ 16:30
	技術コース標準編	1月 29日(金)	10:00 ~ 12:30
	技術コース専門編	1月 29日(金)	13:30 ~ 16:30
会 場	三鷹産業プラザ 7階会議室		
講 師	IPA セキュリティセンター <span style="float:right">コース概要は別紙を参照して下さい</span>		
主 催	三鷹 ICT 事業者協会、経済産業省、IPA、日本商工会議所		
参 加 費	無料		
募 集 人 数	マネジメントコース入門編・マネジメントコース実践編・技術コース標準編・技術コース専門編 各100名(募集人数に達し次第締め切ります。)		
申 込 み	申込書に必要事項をご記入のうえ、E-mail、FAXよりお申込みください。 お申込み受付後、受講票を発行します。		
そ の 他	本セミナーは IT コーディネータ協会が後援するセミナーです。IT コーディネータ協会主催セミナーに準じ、4時間で1知識ポイントが年度間の上限なしで付与されます。IT コーディネータの方は、申込書に認定番号を記入して下さい。		

お問合せ：三鷹 ICT 事業者協会 担当：出田、鈴木

〒181-8525 三鷹市下連雀3-38-4 三鷹産業プラザ2F 株式会社まちづくり三鷹内

TEL:0422-40-9669 FAX:0422-40-9750 E-mail:mict-office@mitaka.ne.jp URL: http://www.mitaka-ict.jp/

お申込は FAX または 電子メール [mict-office@mitaka.ne.jp](mailto:mict-office@mitaka.ne.jp) まで

## コース概要

情報セキュリティ対策 マネジメントコース入門編	
主な対象	中小企業の経営者や管理者で、情報セキュリティ対策の必要性は感じているが、まず何をすべきか分からないという方
概要	<p>重要な情報の保管・持出し・廃棄、ウイルス対策、パソコンやメールを利用する上での注意点、従業員や取引先での機密保持など、中小企業が入門レベルとして最初に取り組むべき情報セキュリティ対策について、「5分でできる！中小企業のための情報セキュリティ自社診断」(<a href="http://www.ipa.go.jp/security/manager/known/sme-guide/index.html">http://www.ipa.go.jp/security/manager/known/sme-guide/index.html</a>)にある25個のチェックポイントを紹介しながら解説する。</p> <p>【前年度からの変更内容】 ウイルスやスパイウェアなどの脅威に対する対策の解説を中心としたものを、情報の管理、従業員の管理など、マネジメントの基礎についての解説を中心としたものに変更する。</p>
目次	<ol style="list-style-type: none"> <li>1. 情報セキュリティとは</li> <li>2. 自社診断シート(25のチェック)</li> <li>3. さあ、チェックしてみましょう</li> <li>4. 参考情報の紹介</li> </ol>
情報セキュリティ対策 マネジメントコース実践編	
主な対象	企業における管理面からの情報セキュリティ対策に関し、具体的に事事故事例から対策のポイントについての理解を深めたい方
概要	<p>情報セキュリティに対する組織的・物理的対策等の管理的取組について、それぞれ事事故事例を踏まえ、事故発生の原因、危険要因を分析し、行うべき対策例や対策のポイントを解説する。</p> <p>事事故事例には、社員の情報持ち出し、私物PCの利用による情報漏えい、委託先からの情報漏えいなど、発生しがちな事故を例示し、シナリオベースのケーススタディを行う。</p> <p>【前年度からの変更内容】 経営者や責任者として理解すべき項目は何かという観点から、体制の整備、ポリシーの作成、情報の管理、従業員や委託先の管理など、組織的対策の基礎について解説し、ケーススタディを中心とした実践的なものに変更する。</p>
目次	<ol style="list-style-type: none"> <li>1. 最近の情報セキュリティ事情</li> <li>2. 情報セキュリティ対策のための管理の枠組み</li> <li>3. ケーススタディ1: 従業員の情報の持ち出し</li> <li>4. ケーススタディ2: 私物PCの業務利用とPCの紛失による業務情報の漏えい</li> <li>5. ケーススタディ3: 委託先からの情報漏えい</li> <li>6. 関連法規</li> </ol>

情報セキュリティ対策 技術コース標準編			
主な対象	企業における情報セキュリティ脅威、および技術面からの対策に関して理解を深めたい方		
概要	<p>近年の情報セキュリティ脅威は「見えない化」が進み、その全貌が分かりにくくなりつつある。さらに、日々新たな攻撃手法が出現しているのが実情であり、適切な対策のためには“敵を知る”ことが大前提となる。</p> <p>本コースではセキュリティ事故防止の視点から、最近の重大な情報セキュリティ脅威の動向と事例を紹介しつつ、それぞれの技術的対策のポイントについて解説する。</p>		
	<p>【前年度からの変更内容】</p> <p>基本的な構成は変わらない。最新の 10 大脅威・脆弱性届出状況・不正アクセス届出状況に基づいた解説に変更する。</p>		
目次	<table border="0"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li>1. 情報セキュリティ 10 大脅威               <ul style="list-style-type: none"> <li>1.1 情報セキュリティ 10 大脅威とは</li> <li>1.2 情報セキュリティ 10 大脅威の解説</li> </ul> </li> <li>2. 脆弱性関連情報の届出状況               <ul style="list-style-type: none"> <li>2.1 再確認：脆弱性って？</li> <li>2.2 情報セキュリティ早期警戒パートナーシップ</li> <li>2.3 脆弱性関連情報の届出状況</li> <li>2.4 SQL インジェクションとは？</li> <li>2.5 クロスサイト・スクリプティングとは？</li> <li>2.6 DNS キャッシュポイズニングとは？</li> <li>2.7 脆弱性届出・対策に関する考察</li> </ul> </li> </ul> </td> <td style="vertical-align: top; border-left: 1px dotted black;"> <ul style="list-style-type: none"> <li>3. 不正アクセスの届出状況               <ul style="list-style-type: none"> <li>3.1 ネットワークに流れる不審な通信</li> <li>3.2 不正アクセス届出状況</li> <li>3.3 不正アクセスに関する考察</li> </ul> </li> <li>(付録)</li> <li>情報セキュリティ確保のための基本的な対策               <ul style="list-style-type: none"> <li>1 基本的な対策方針</li> <li>2 利用者の対策</li> <li>3 組織の対策</li> <li>4 システム管理者・開発者の対策</li> <li>5 情報セキュリティ対策関連情報</li> </ul> </li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li>1. 情報セキュリティ 10 大脅威               <ul style="list-style-type: none"> <li>1.1 情報セキュリティ 10 大脅威とは</li> <li>1.2 情報セキュリティ 10 大脅威の解説</li> </ul> </li> <li>2. 脆弱性関連情報の届出状況               <ul style="list-style-type: none"> <li>2.1 再確認：脆弱性って？</li> <li>2.2 情報セキュリティ早期警戒パートナーシップ</li> <li>2.3 脆弱性関連情報の届出状況</li> <li>2.4 SQL インジェクションとは？</li> <li>2.5 クロスサイト・スクリプティングとは？</li> <li>2.6 DNS キャッシュポイズニングとは？</li> <li>2.7 脆弱性届出・対策に関する考察</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>3. 不正アクセスの届出状況               <ul style="list-style-type: none"> <li>3.1 ネットワークに流れる不審な通信</li> <li>3.2 不正アクセス届出状況</li> <li>3.3 不正アクセスに関する考察</li> </ul> </li> <li>(付録)</li> <li>情報セキュリティ確保のための基本的な対策               <ul style="list-style-type: none"> <li>1 基本的な対策方針</li> <li>2 利用者の対策</li> <li>3 組織の対策</li> <li>4 システム管理者・開発者の対策</li> <li>5 情報セキュリティ対策関連情報</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>1. 情報セキュリティ 10 大脅威               <ul style="list-style-type: none"> <li>1.1 情報セキュリティ 10 大脅威とは</li> <li>1.2 情報セキュリティ 10 大脅威の解説</li> </ul> </li> <li>2. 脆弱性関連情報の届出状況               <ul style="list-style-type: none"> <li>2.1 再確認：脆弱性って？</li> <li>2.2 情報セキュリティ早期警戒パートナーシップ</li> <li>2.3 脆弱性関連情報の届出状況</li> <li>2.4 SQL インジェクションとは？</li> <li>2.5 クロスサイト・スクリプティングとは？</li> <li>2.6 DNS キャッシュポイズニングとは？</li> <li>2.7 脆弱性届出・対策に関する考察</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>3. 不正アクセスの届出状況               <ul style="list-style-type: none"> <li>3.1 ネットワークに流れる不審な通信</li> <li>3.2 不正アクセス届出状況</li> <li>3.3 不正アクセスに関する考察</li> </ul> </li> <li>(付録)</li> <li>情報セキュリティ確保のための基本的な対策               <ul style="list-style-type: none"> <li>1 基本的な対策方針</li> <li>2 利用者の対策</li> <li>3 組織の対策</li> <li>4 システム管理者・開発者の対策</li> <li>5 情報セキュリティ対策関連情報</li> </ul> </li> </ul>		
情報セキュリティ対策 技術コース専門編			
主な対象	ウェブサイトの開発・運営や、システムの運用に関わっている方で、生じるセキュリティ上の問題およびその対応方法について理解を深めたい方		
概要	<p>企業等がウェブサイトを構築する際、開発するウェブアプリケーションにおいて必要なセキュリティ対策について、デモを交えて解説する。</p> <p>また、情報システムの運用時に、セキュリティ事故が発生した際、技術的な調査、および対応の方法を、ケーススタディを通じて解説する。</p>		
	<p>【前年度からの変更内容】</p> <p>基本的な構成は変わらない。最新のセキュリティ動向を踏まえてケーススタディを見直す。</p>		
目次	<table border="0"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li>1. DNS 経由の不正アクセス               <ul style="list-style-type: none"> <li>1.1 DNS とは？</li> <li>1.2 事例：会社のドメイン情報が乗っ取られる</li> <li>1.3 何が起きていたのか</li> <li>1.4 対策の前に</li> <li>1.5 危険な DNS 設定とは</li> <li>1.6 LAME delegation の対策</li> <li>1.7 DNS キャッシュポイズニング</li> </ul> </li> <li>2. Web アプリケーションの脆弱性               <ul style="list-style-type: none"> <li>2.1 SQL インジェクションとは</li> <li>2.2 SQL インジェクション対策</li> <li>2.3 クロスサイト・スクリプティング</li> <li>2.4 クロスサイト・スクリプティング対策</li> </ul> </li> </ul> </td> <td style="vertical-align: top; border-left: 1px dotted black;"> <ul style="list-style-type: none"> <li>3. インシデントレスポンス               <ul style="list-style-type: none"> <li>3.1 インシデントレスポンスとは</li> <li>3.2 事例：ウイルス侵入</li> <li>3.3 「検知」のきっかけ</li> <li>3.4 予防策</li> </ul> </li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li>1. DNS 経由の不正アクセス               <ul style="list-style-type: none"> <li>1.1 DNS とは？</li> <li>1.2 事例：会社のドメイン情報が乗っ取られる</li> <li>1.3 何が起きていたのか</li> <li>1.4 対策の前に</li> <li>1.5 危険な DNS 設定とは</li> <li>1.6 LAME delegation の対策</li> <li>1.7 DNS キャッシュポイズニング</li> </ul> </li> <li>2. Web アプリケーションの脆弱性               <ul style="list-style-type: none"> <li>2.1 SQL インジェクションとは</li> <li>2.2 SQL インジェクション対策</li> <li>2.3 クロスサイト・スクリプティング</li> <li>2.4 クロスサイト・スクリプティング対策</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>3. インシデントレスポンス               <ul style="list-style-type: none"> <li>3.1 インシデントレスポンスとは</li> <li>3.2 事例：ウイルス侵入</li> <li>3.3 「検知」のきっかけ</li> <li>3.4 予防策</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>1. DNS 経由の不正アクセス               <ul style="list-style-type: none"> <li>1.1 DNS とは？</li> <li>1.2 事例：会社のドメイン情報が乗っ取られる</li> <li>1.3 何が起きていたのか</li> <li>1.4 対策の前に</li> <li>1.5 危険な DNS 設定とは</li> <li>1.6 LAME delegation の対策</li> <li>1.7 DNS キャッシュポイズニング</li> </ul> </li> <li>2. Web アプリケーションの脆弱性               <ul style="list-style-type: none"> <li>2.1 SQL インジェクションとは</li> <li>2.2 SQL インジェクション対策</li> <li>2.3 クロスサイト・スクリプティング</li> <li>2.4 クロスサイト・スクリプティング対策</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>3. インシデントレスポンス               <ul style="list-style-type: none"> <li>3.1 インシデントレスポンスとは</li> <li>3.2 事例：ウイルス侵入</li> <li>3.3 「検知」のきっかけ</li> <li>3.4 予防策</li> </ul> </li> </ul>		

### IPA セキュリティセンターについて

IPA は経済産業省の外郭団体です。IPA セキュリティセンターでは、経済産業省の情報セキュリティ政策を実行に移すため、情報セキュリティに対する具体的な対策情報・対策手段を提供するとともに、セキュアな情報インフラストラクチャの整備に貢献するための様々な活動を行っています。

URL <http://www.ipa.go.jp/security/>

F A X : 0422 40 9750

三鷹 ICT 事業者協会 担当 出田・鈴木 行

「2009 年度 IPA 情報セキュリティセミナー」への参加を申込みます

貴社名	フリガナ		
住 所	フリガナ 〒		
貴 名	フリガナ	所属・役職	
T E L		F A X	
E-mail		ITC 認定番号	
参加希望コース	マネジメントコース入門編 技術コース標準編		マネジメントコース実践編 技術コース専門編
貴 名	フリガナ	所属・役職	
T E L		F A X	
E-mail		ITC 認定番号	
参加希望コース	マネジメントコース入門編 技術コース標準編		マネジメントコース実践編 技術コース専門編
貴 名	フリガナ	所属・役職	
T E L		F A X	
E-mail		ITC 認定番号	
参加希望コース	マネジメントコース入門編 技術コース標準編		マネジメントコース実践編 技術コース専門編
貴 名	フリガナ	所属・役職	
T E L		F A X	
E-mail		ITC 認定番号	
参加希望コース	マネジメントコース入門編 技術コース標準編		マネジメントコース実践編 技術コース専門編



## 三鷹 ICT 事業者協会とは

三鷹地域の I C T 事業者が 参加企業の特長、得意分野、強みを しっかりと認識しながら 相互に連携・協力して 情報産業発展の為に寄与する協会です。

URL <http://www.mitaka-ict.jp/>