≫≫NPO 法人電子自治体アドバイザークラブからのお知らせ≪≪

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　２月３日（水）９：３０～１２：１５ マネジメントコース実践編　２月３日（水）１３：３０～１６：３０ 技術コース標準編　２月４日（木）９：３０～１２：１５ 技術コース専門編　２月４日（木）１３：３０～１６：３０※コース概要は別紙を参照して下さい
会　　場	奈良商工会議所　中ホール（奈良市登大路町 36-2、近鉄奈良駅前）
講　　師	IPA セキュリティセンター
主　　催	NPO 法人電子自治体アドバイザークラブ、経済産業省、IPA、日本商工会議所
共　　催	帝塚山大学経営情報学部
参 加 費	無料
副 読 本	情報セキュリティ読本三訂版（¥500 円）および 情報セキュリティ教本改訂版（¥2,500）をセミナー会場にて販売します。
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　５０名（募集人数に達し次第締め切ります。）
申 込 み	必要事項をご記入のうえ E-mail、FAX よりお申込みください。お断りする場合以外は特にご連絡致しません。
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。
	奈良県、奈良県市長会、奈良県町村会、奈良県中小企業支援センター、奈良商工会議所にも後援いただいております

お問合せ：NPO 法人電子自治体アドバイザークラブ
FAX：0742-33-7863　　E-mail：　e-aac@nifty.com　　URL：http://eaac.sakura.ne.jp/

きりとり

ＦＡＸ：0742-33-7863

NPO 法人電子自治体アドバイザークラブ　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	ﾌﾘｶﾞﾅ		
住　所	ﾌﾘｶﾞﾅ 〒		
貴　名	ﾌﾘｶﾞﾅ	所属・役職	
ＴＥＬ		ＦＡＸ	
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　□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		

別紙

◆ 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	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、従業者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」（http://www.ipa.go.jp/security/manager/know/sme-guide/index.html）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。
	【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。
目次	1. 情報セキュリティとは 2. 自社診断シート（25 のチェック） 3. さぁ、チェックしてみましょう 4. 参考情報の紹介
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	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。 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。
	【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。
目次	1. 最近の情報セキュリティ事情 2. 情報セキュリティ対策のための管理の枠組み 3. ケーススタディ 1: 従業員の情報の持ち出し 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 5. ケーススタディ 3: 委託先からの情報漏えい 6. 関連法規

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	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。 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。
	【前年度からの変更内容】 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。
目次	1. 情報セキュリティ 10 大脅威 1.1 情報セキュリティ 10 大脅威とは 1.2 情報セキュリティ 10 大脅威の解説 2. 脆弱性関連情報の届出状況 2.1 再確認:脆弱性って？ 2.2 情報セキュリティ早期警戒パートナーシップ 2.3 脆弱性関連情報の届出状況 2.4 SQL インジェクションとは？ 2.5 クロスサイト・スクリプティングとは？ 2.6 DNS キャッシュポイズニングとは？ 2.7 脆弱性届出・対策に関する考察 3. 不正アクセスの届出状況 3.1 ネットワークに流れる不審な通信 3.2 不正アクセス届出状況 3.3 不正アクセスに関する考察 （付録） 情報セキュリティ確保のための基本的な対策 1 基本的な対策方針 2 利用者の対策 3 組織の対策 4 システム管理者・開発者の対策 5 情報セキュリティ対策関連情報

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、生じう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	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。 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。
	【前年度からの変更内容】 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。
目次	1. DNS 経由の不正アクセス 1.1 DNS とは？ 1.2 事例:会社のドメイン情報が乗っ取られる 1.3 何が起きていたのか 1.4 対策の前に 1.5 危険な DNS 設定とは 1.6 LAME delegation の対策 1.7 DNS キャッシュポイゾニング 2. Web アプリケーションの脆弱性 2.1 SQL インジェクションとは 2.2 SQL インジェクション対策 2.3 クロスサイト・スクリプティング 2.4 クロスサイト・スクリプティング対策 3. インシデントレスポンス 3.1 インシデントレスポンスとは 3.2 事例:ウイルス侵入 3.3「検知」のきっかけ 3.4 予防策

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/