≫≫鹿児島インファーメーションからのお知らせ≪≪

情報セキュリティセミナー 2007

～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・(独)情報処理推進機構(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、不正アクセスを受けたウェブサイトの一時閉鎖などの事件が相次いで起きています。

このような状況はもはや他人事ではなく、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。

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プログラムは常に新たなものが生まれています。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、鹿児島インファーメーションでは、経済産業省、独立行政法人 情報処理推進機構（IPA)、日本商工会議所と共同で、情報セキュリティ対策の専門家である IPA セキュリティセンターの研究員を講師に迎え、企業や組織において情報セキュリティ対策を実施するセキュリティ責任者・担当者、システム管理者、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	基礎コース　　平成 19 年 9 月 21 日（金）　10：00　～　12：00 マネジメントコース　平成 19 年 9 月 21 日（金）　13：00　～　16：30 ※コース概要は別紙を参照して下さい
会　　場	鹿児島大学工学部共通棟 201 号教室
講　　師	独立行政法人 情報処理推進機構（IPA）セキュリティセンター 研究員
主　　催	NPO 法人 鹿児島インファーメーション、経済産業省、 独立行政法人 情報処理推進機構（IPA)、日本商工会議所
後　　援	鹿児島県、鹿児島市、鹿児島大学学術情報基盤センター、鹿児島商工会議所、 社団法人 鹿児島県工業倶楽部、社団法人 鹿児島県情報サービス産業協会
参 加 費	無料
副 読 本	情報セキュリティ読本（定価¥500)、情報セキュリティ教本（定価¥2,500）をセミナー会場にて販売します。
募集人数	基礎コース・マネジメントコース　各 70 名 （募集人数に達し次第締め切ります。）
申 込 み	下記のホームページよりお申込みください。 http://infarmation.org ※ 情報セキュリティセミナー2007 のページをご覧ください。
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（補）の方は、申込書に認定番号を記入して下さい。

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/

別紙

◆ コース概要 ◆

情報セキュリティ対策　基礎コース

対象	企業における情報セキュリティ対策の基礎を理解したい方 （企業でパソコンを使って業務をする方、セキュリティ教育担当者、経営者）
ポイント	企業が直面する情報漏えいの脅威とその対策 （クライアントのセキュリティ）
内容	情報漏えいの原因となるコンピュータウイルス・スパイウェア・フィッシング詐欺等の脅威、被害事例、被害に遭わないために個人が行う対策について解説する。
目次	1. はじめに 2. ウイルス関連 ウイルスとは？ スパイウェアとは？ ボットとは？ ウイルス感染の原因 ウイルス被害対策 3. 不正アクセス 不正アクセスとは？ 侵入行為 復旧対策 4. フィッシング フィッシングとは？ 事例 対策 5. 情報漏えい 情報漏えいの原因 ファイル交換ソフトとは？ 情報漏えい対策 6. 個人レベルの対策 ファイルの拡張子とは？ 怪しいファイルの見分け方 セキュリティレベルの設定 パスワードの設定・管理 電子メールのセキュリティ対策 迷惑メールの取り扱い バックアップ Windows 98/Me パソコンの扱い 7. 終わりに

情報セキュリティ対策　マネジメントコース

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て理解を深めたい方 （セキュリティ教育担当者、経営者、セキュリティ責任者、マネジメントの観点からの対策を担当するセキュリティ担当者、システム管理者）
ポイント	事例を用いたケーススタディによるリスク（脅威・脆弱性）とその対策の解説
概要	具体的な事例を用いて、情報資産を組織的かつ継続的にどう管理すればよいかについて、情報セキュリティ対策ベンチマーク、情報管理等に触れながら説明する。
目次	1. 背景と基礎知識 1.1 情報セキュリティに関わる脅威の傾向 1.2 情報セキュリティ対策の目的、方針 1.3 情報セキュリティマネジメントと PDCA サイクル 1.4 情報セキュリティ対策実施上の問題点と施策ツール 2. 情報セキュリティ対策ベンチマーク 2.1 情報セキュリティガバナンスと自己診断テストの活用 2.2 情報セキュリティベンチマークの概要 2.3 情報セキュリティベンチマークの利用方法 2.4 情報セキュリティベンチマークの診断結果 2.5 情報セキュリティベンチマークの利用状況 3. ケーススタディ ： パソコンの紛失 3.1 事故発生の経緯 3.2 事故対応の流れ 3.3 情報の特定 3.4 事故対応：緊急対策会議での決定 3.5 A 社の事故対応体制 3.6 対外発表のポイント 3.7 再発防止策の例 4. そこにある情報資産－情報資産の洗い出し 4.1 守るべき情報資産とは 4.2 情報資産の例 4.3 情報資産の価値 4.4 情報資産はどこにある？ 4.5 情報資産の洗い出し 4.6 情報の管理責任者、管理担当者、利用者 4.7 機密情報、個人情報、その他の情報 4.8 情報システム、電子文書、紙文書 5. 情報の分類と格付け 5.1 情報の分類と格付けはなぜ必要か？ 5.2 政府機関統一基準の分類と格付け 5.3 機密性、完全性、可用性に応じた情報の分類 5.4 情報の分類と格付けの基準（例） 5.5 情報漏えい防止に留意した情報の分類例 6. 情報のライフサイクルと情報の取扱い 6.1 情報のライフサイクル 6.2 情報の作成と入手 6.3 情報の利用・加工 6.4 情報の保存 6.5 情報の移送（送信と運搬） 6.6 情報の提供 6.7 情報の消去 7. 情報セキュリティポリシーと情報の管理 7.1 情報セキュリティポリシーの構成 7.2 情報セキュリティ基本方針 7.3 情報セキュリティ対策基準 7.4 情報セキュリティ実施手順 7.5 対策基準とガイドライン・実施手順の関係 7.6 情報セキュリティポリシー運用上の留意点 7.7 情報の管理に関する複数の諸規程 8. 情報の管理と対策のヒント 8.1 情報の管理と対策の基本原則 8.2 リスク対応とは 8.3 リスク対応－相互の関係 9. 情報の管理と法令遵守 9.1 IT 社会の変化と法的対応の変遷 9.2 個人情報保護法 9.3 不正競争防止法