セキュリティコース講義課目詳細

基本科目（必修）

	講座内容	時間	講師
	ルールとモラル　安全に使うには使わせるには	3H	園田
8月13日午後（3時間）	基礎講座では、ノートパソコンの安全な使い方など、身近なを題材として、ルールやモラル、パソコンやネット利用のリスクについて理解し、啓発する立場からどうすべきかなどを考え、議論する。		

専門科目（クラス選択制）（4クラスから一つ受講したいクラスを選択していただきます）

	サーバクラス	Webプログラミングクラス	ネットワーククラス	解析クラス
各コースの概要説明	サーバクラスでは、ITシステムにおけるサーバセキュリティについて重点を置いています。 「砂上の楼閣」と言うことわざがあるように、より安定したシステムを運用するためには、土台となる基礎をしっかりと構築しておかなければなりません。 本クラスでは、セキュアなプラットフォームを実現するために必要となるOSセキュリティを強化するセキュアOS技術と仮想化技術、これらの上で動作するサービス（DNSなど）のセキュリティ、さらに出力されるログの解析についてを学びます。	近年、アプリケーションに対する脅威が拡大しており、開発者自身がセキュリティを考慮して開発に携わることが求められています。Webプログラミングクラスでは、セキュアなアプリケーションの開発を行う上で必要となる、設計、開発、テストについて扱います。 設計では、コーディングの原則、メンテナンシビリティ、テスタビリティ、構造化の考え方など、セキュアアプリケーションを作るうえで重要なコンセプトを説明します。 開発では、主にWebアプリケーションプログラミングの演習を行ないます。 現代の計算機の動作原理とOS上で動くプログラムの構造ついて理解を深め、コマンド/SQLインジェクションの防止やアクセス制限とユーザ認証の重要性について説明します。 テストでは、Webアプリを題材に、どのような問題が潜むのか、また実際にそれらの問題を見つけ出す方法を説明をします。	今やインターネットは、それがない生活を想像できないくらいの勢いで利用されています。それにともない、インターネットを安全に使う、という要求は普通に増えていますが、インターネット経由の攻撃がわれわれのところに到着しうる、ということも現実になっています。 本クラスでは、ネットワークの基礎や構築、そして実際のネットワーク環境上で行われる攻撃および防御について、演習を交えながら学んでいきます。	近年、情報漏洩に代表されるセキュリティ事件・事故が後を絶ちません。そのため、企業においては予防措置の実施は勿論、インシデントの発生を想定した体制作りが必須と言えます。現状、こうしたインシデントレスポンスについての考え方は周知されつつあるものの、実際にインシデントに対応するセキュリティ専門家の育成は十分とは言えません。 そこで解析クラスでは、ネットワーク、ホスト、プログラムの3つ視点からシステム上で発生した事象を正確に把握するための技術・手法、および解析に際して求められる考え方について学習します。 パケット解析では、通信ログからネットワーク上で発生した事象を把握する方法について説明します。ディスク解析では、侵害された可能性のあるホストのディスクを解析し、侵入の痕跡を発見・分析する方法について説明します。マルウェア解析では、実際にマルウェアを実行、解析し、プログラムの動作を把握するための方法について説明します。
日程	サーバクラス講座内容詳細 / 時間 / 講師	Webプログラミングクラス講座内容詳細 / 時間 / 講師	ネットワーククラス講座内容詳細 / 時間 / 講師	解析クラス講座内容詳細 / 時間 / 講師
	セキュアプラットフォーム講座 / 8H / 田口	システム品質設計 / 3H / 岡田	パケット工作から学ぶネットワークセキュリティ / 4H / 吉田	パケット解析 / 4H / 渡辺
8月14日午前・午後・夜間（9.5時間） 8月15日午後・夜間　（5.5時間）	よく利用されているOSの仕組みはrootユーザの権限さえ手に入れてしまえば、すべての情報へアクセスできる仕様になっています。 ソフトウェアの脆弱性からroot権限を奪取されてしまうことも多く、いくらセキュリティ設定を行っても無意味になってしまうこともあります。 万が一、被害を受けたとしてもシステムに与える影響を最小限に抑えることができるセキュアOSの仕組みを理解して、実際にセキュアOSを導入した場合としない場合の違いを体験します。また、仮想化技術の特徴やメリット、弱点なども理解して、これらを組み合わせたセキュアプラットフォームについてを学びます。 キーワード： サーバセキュリティ、仮想化、VM、Xen、セキュアOS、SELinux、TOMOYOLinux、強制アクセス制御	システムとしての品質をしっかり考える。このためには、自分自身のプログラムコーディングの原則論、またシステムとしてのメンテナンシビリティ、テスタビリティ、構造化の考え方など、本質的なセキュリティの観点が必要です。関係する重要なコンセプトのいくつかをディスカッションを交えて学びます。 キーワード：メンテナンシビリティ、テスタビリティ、構造化	本セッションでは、様々なTCP/IPパケットを送信したり受信したりすることで、普段は意識することの無いネットワーク上でのパケットのやり取りについて体験してもらい、ネットワーク経由でどのようにしてポートの開閉は調査されるのか、どのようにしてOSは推測されるのか、どのようにしてパケットフィルタリングの性能は調査されるのか等について、これらの手法や対策方法について実習を通して学びます。 キーワード：TCP/IP, フラグ, スリーウェイハンドシェイク, パケットフィルタリング, ポートスキャン, OS推測	パケット解析では、通信ログからネットワーク上で発生した事象を把握する方法について説明します。ディスク解析では、侵害された可能性のあるホストのディスクを解析し、侵入の痕跡を発見・分析する方法について説明します。マルウェア解析では、実際にマルウェアを実行、解析し、プログラムの動作を把握するための方法について説明します。
	DNSサーバのセキュリティ / 4H / 塩月	Webアプリケーション開発 / 6.5H / 竹迫	ネットワークの基礎とVPN / 5.5H / 宮本	ハードディスク解析 / 4H / 伊原
	DNS（Domain Name System）は、インターネットを利用する際に誰もがお世話になる非常に基本的なサービスです。そのためDNSサーバにおけるセキュリティ侵害は、多くのインターネット利用者に重大な影響を与えかねません。本講義科目では、DNSサーバの一般的なセキュリティ上の問題点について、特にファーミング攻撃に用いられる脆弱性を中心に実習し、現状のDNSが抱える問題点や安全なDNSサーバの運用方法について考察します。 キーワード： Bind、Windows DNS、ファーミング、ダイナミックアップデート、 クエリIDの推測、バースデイアタック、キャッシュポイゾニング、DNSアンプ	開発では、主にWebアプリケーションプログラミングの演習を行ないます。 簡単なx86プログラミングを体験し、現代の計算機の動作原理とOS上で動くプログラムの構造ついて理解を深めます。そして実際にPerlなどのスクリプト言語を使った掲示板の作成を通してWebアプリケーションの段階的な開発を経験し、コマンド/SQLインジェクションの防止やアクセス制限とユーザ認証の重要性について説明します。 また最近のAjaxブームで利用されるJavaScriptやFlashを利用したリッチクライアントのセキュリティについても扱います。 キーワード：x86、Perl、PHP、SQL、インジェクション、JavaScript、Ajax、JSONP、Flash、AVM、SWF	インターネットに接続されたネットワーク間で安全に通信を行うしくみとして、VPNがあります。ただ、単に「VPN」といってもさまざまな実現方法があり、また、目的によってどのようなしくみを採用するかも異なってきます。 ここでは、VPNが実現することと、VPNの実現方式、そして鍵交換をはじめとする要素技術について、実際にVPNを構築する機器を使いながら学んでいくこととします。 キーワード：TCP/IP, IPsec, IKE, PPTP, 暗号化、鍵交換、	ディスク解析では、侵害された可能性のあるサーバのハードディスクに残された不正アクセス者のデジタル痕跡（足跡）を調べることで、どのような追跡や調査が可能になるのか、ファイルシステムの基本的な動作から、ハードディスクに書き込まれたデータ内容を直接調べる方法などについて扱います。
	ログ解析 / 3H / 園田	Webセキュリティテスト / 5.5H / 国分、望月	侵入検知 / 5.5H / 渡辺	マルウェア解析 / 7H / 村上
	サービスやアプリケーション、そしてOSにもログを記録する機能があります。しかし、その見方、集約する方法、量の推移を見る方法は、断片的に語られているだけで、なかなかまとまった形で学ぶ機会は無いようです。この講座では、様々なログからデータを抽出する方法について、現実の素材を元にして追究してみたいと思います。 キーワード： ログ解析、量的推移、トラフィック解析、絶対計算	Webアプリケーションに潜む脆弱性について、デモを交えながらその危険性と問題点について実感してもらい、また改修方法についての説明をしていきます。また、Webアプリケーションに潜む脆弱性を踏まえ、Webアプリケーションの問題を見つけ出すためのテスト手順と、個別のテスト手法について講義をします。 キーワード：HTTP、XSS、SQLインジェクション、CSRF、テスト、CVSS	セキュリティインシデントを早期に発見し、遅滞無いインシデントレスポンスのために重要な役割を持つ侵入検知システムについて、その基礎知識、動作原理を学び、また現場における構築、運用を想定した演習を行うことで、セキュリティ監視に必要な知見を身につける。 キーワード IDS/IDPS、Snort、tcpdump、WireShark、PCAP、BPF、IP、TCP、UDP、ICMP、パケット、侵入検知、マルウエア	マルウェア解析では、マルウェアの分類や動作原理、その解析手法について解説し、実際に解析を行うことで基本的なリバースエンジニアリング技術を習得する。 また、難読化や耐解析技術等のマルウェアならではのトピックについても取り扱う。 キーワード マルウェア、リバースエンジニアリング、動的分析、静的分析、逆アセンブラ、 デバッガ、耐解析技術、IDA Pro

専門科目（自由選択制：クラスに関係無く同じ時間帯の科目から一つ受講したい科目を選択していただきます。）

日程	Aトラック			Bトラック			Cトラック			Dトラック		
	1-A　クライアントのセキュリティ	4H	吉田	1-B ソフトウェアの不正実行防止（Windows編）	4H	塩月	1-C　文字コードと脆弱性 ＆ブラウザに依存したWebアプリケーションセキュリティ	4H	はせがわようすけ	1-D,2-D　ハニーポット	8H	濱本
自由1 8月16日 午前（4時間）	以前はサーバへの攻撃が主流だったのに対し、今ではクライアントへの攻撃が増加し、主流になりつつあります。 本セッションでは、なぜ攻撃者は攻撃対象をサーバーからクライアントに替えてきているのか、攻撃手法や対策方法ともに解説し、実習を通して学びます。 キーワード：受動的攻撃、能動的攻撃、ブラウザ、シェル接続、逆シェル接続、ファイアウォール、NAT、リバース・テルネット			本講義科目では、ソフトウェアの脆弱性を利用した攻撃手法として典型的ともいえるバッファオーバーフロー攻撃およびフォーマットストリング攻撃を例としてとりあげ、その仕組みを解説すると共に、Windows OSやマイクロソフトの開発環境が提供するソフトウェアの不正実行防止技術がそれらの攻撃に対してどのように働くのか、どのような限界があるのか、またどうすれば有効に使えるのかといったことについて、実習を通して学びます。 キーワード： Windows、バッファオーバーフロー、フォーマットストリング、シェルコード、例外ハンドラ、GSオプション、DEP、ASLR、XPSP2、Vista			[文字コードと脆弱性] 近年成長の著しいWebアプリケーションは、内部ではHTMLやXMLといった文字列データを広範囲に使用しています。また、Webアプリケーションに限らず各プラットフォームにおいてもShift_JISやEUC-JPといったレガシーな文字コードからUnicodeへの遷移において様々な問題が発生しています。 このような過渡期において、文字コードを利用した脆弱性や攻略手法の報告を見かけることが増えてきました。 本講義科目では、文字コードに関連するセキュリティ上の問題点についての理解を深め、その対策について学びます。 キーワード: 文字コード、Unicode、Shift_JIS、パストラバーサル、クロスサイトスクリプティング [ブラウザに依存したWebアプリケーションセキュリティ] Webアプリケーションのセキュリティを考える上では、ブラウザの直接的な脆弱性とはいえないものの、そのブラウザ特有の仕様や挙動について、十分に把握することが必要となる場合が少なからず存在します。 本講義課目では、そういったブラウザ個別の仕様、挙動に起因するWebアプリケーションのセキュリティについて扱います。 キーワード: Internet Explorer、Mozilla Firefox、クロスサイトスクリプティング、クロスドメイン			本講義では、インターネット上におとりサーバを立てて、攻撃者からの攻撃を実際に受けて、攻撃者の行動を観察するシステム、ハニーポットについて解説します。 ハニーポット技術は、サーバの構築、ネットワークの解析、侵入後の解析、ウィルスの解析など、総合的なセキュリティ技術の集大成です。 本講義では、実際にハニーポットの構築手法、収集したデータの解析手法について、実習を交えて講義します。 また、昨今の情勢として、Botプログラムなど、ハニーポットではマルウェア収集も重要な役割となっていますので、マルウェア解析の実習も同時に行います。		
	2-A　暗号と暗号解読 ～古代から現代まで～	4H	上野	2-B　無線LANのセキュリティ	4H	滝崎						
自由2 8月16日 午後（4時間）	暗号は紀元前から使われており、今では個人情報から国家機密まで、情報セキュリティにおいては欠かすことができない技術となっています。 暗号は縁の下の力持ちのようなイメージがあるかもしれませんが、全世界で7000万部も大ヒットした『ダ・ヴィンチ・コード』では、ストーリーの中心となるのは暗号と暗号解読であり、その魅力は人を惹きつけてやみません。 本講座では、三国志の登場人物や忍者が使った古典暗号や、映画に登場する暗号、そして現代の暗号技術まで、その仕組み紹介や暗号解読の実習なども交え、その魅力を追求していきます。 キーワード： 暗号、暗号解読、古典暗号、バーナム暗号、共通鍵暗号、ブロック暗号、ハッシュ、公開鍵暗号、証明書、SSL、量子暗号			PCだけでなくゲーム機の接続ができるようになったことも要因として爆発的に普及した無線LANですが、セキュリティ上の問題が多く存在します。未だに問題のあるセキュリティ技術も現役として使用され、正しい運用をされていることはごく稀です。ここでは、無線LANの技術やそのセキュリティ上の問題点について、実際に問題のある暗号化がどれだけの強度を持つのか演習を通して理解し、その上で無線LANで使用されている暗号技術や問題点などについて、理解を深めます。								

☆本講義課目詳細はあくまで予定です。講義内容および時間帯については予告なく変更することがありますので、ご了承ください。

注：ハニーポットについては午前・午後通しで受講していただきます