ナンバリングコード [科目ナンバリングについて]

授業科目名	科目区分	時間割	対象年次及び学科
情報セキュリティI Information Security I		前期 月2	3〜 創造工学部
講義題目	水準・分野	DP・提供部局	対象学生・ 特定ﾌﾟﾛｸﾞﾗﾑとの対応
		bcdT	
担当教員	授業形態	単位数	時間割コード
喜田　弘司　, 最所　圭三[Saisho Keizo]	Lx	2	5005130

DP・提供部局

bcdT

授業形態

Lx

関連授業科目

インターネットⅠ、インターネットⅡ、オペレーティングシステム

履修推奨科目

学習時間

講義90分 × 15回 ＋ 自学自習（準備学習 30時間 ＋ 事後学習 30時間）

授業の概要

この授業は，これまで情報セキュリティを体系的に詳しく学んだことがない方を対象に，セキュリティに関する倫理と基本技術を理解することを目的とします．前半に，「セキュリティ倫理編」と題して日々の心構えを具体例で解説します。後半は、「セキュリティ技術編」と題して、暗号技術を基にした技術（各種暗号方式，認証，PKI等）を解説します．

授業の目的

情報セキュリティは，情報系の企業に限らず，すべての企業・組織で必要であり，この人材不足が大きな社会問題となっております．
この背景をふまえ，本講義は，**すべての理系のエンジニアが身につけるべき情報セキュリティの基本技術を学ぶことを目的**とします．
広く網羅的にセキュリティ技術を理解することにより，将来，企業のエンジニアとして就職し，セキュリティ面で困ることがないようになります．

到達目標

・機密情報とは何かを説明できる
・ソーシャルエンジニアリングの例を少なくともひとつ説明できる
・ネットワーク利用に関して、一般ユーザがセキュリティ観点から何を注意すべきかを説明できる
・暗号アルゴリズムを少なくともひとつ説明できる
・様々な認証の特徴を説明できる

・コンピュータウィルスの脅威を説明できる
・最新のサイバーセキュリティの研究事例を少なくともひとつ説明できる

成績評価の方法と基準

期末テストは行わず，レポートと中間テストで成績を評価する．レポートは，A4用紙，数枚程度で授業で説明した内容に関する質問に回答してもらう．中間テストは、きりがよいタイミングで、30分程度の確認テストを行う（レポート６０%、中間テスト４０%）．また、授業内容の理解度および出席確認のためのメモを毎回提出してもらう．

授業計画・授業及び学習の方法・準備学習及び事後学習のためのｱﾄﾞﾊﾞｲｽ

第1回：オリエンテーション:授業の進め方の説明と，そもそもなぜセキュリティが重要なのかを考察

【セキュリティ倫理編】
第2回：機密情報とは？
第3回：ソーシャルエンジニアリングとサイバー攻撃
第4回：ネットワークを利用する際のセキュリティ観点での注意事項
第5回：まとめ、中間テスト

【セキュリティ技術編】

第6回：セキュリティ技術の全体像
第7回：暗号技術1：暗号の基礎、共通鍵暗号、公開鍵暗
第8回：暗号技術2：ハッシュ関数、メッセージ認証、デジタル署名、乱数
第9回：認証技術1：パスワード、生体認証
第10回：認証技術2：認証プロトコル、ID連携
第11回：まとめ、中間テスト
第12回：PKI：トラストモデル、公開鍵証明、認証局
第13回：コンピュータ・ウィルス
第14回：最新の研究事例（人工知能を活用した研究事例紹介）
第15回：まとめ、中間テスト

※理解度等に応じて，適宜，授業内容の順番等を変更することがある．

【自学自習のためのアドバイス】
全回共通：
情報セキュリティは「生もの」と言われることがあります．日々，変化がある分野ですので，世の中の動きをウォッチする習慣が大事です（15分/日）．

第2回から第5回：授業のスライドで出てきたセキュリティ用語をインターネットや書籍で確認（3時間/週）
第6回から第15回：授業では、下記のリストの「マスタリングTCP/IP 情報セキュリティ編」を中心に進めますが、浅く広くなりがちです。下記のリストの別の書籍も参考に各トピック深掘りして下さい（3時間/週）。体系的に学ぶべきトピックですのでインターネットの情報より教科書での勉強をおすすめします。

教科書・参考書等

- マスタリングTCP/IP 情報セキュリティ編，齋藤孝道，オーム社，ISBN-10: 4274069214
- サイバーセキュリティ入門,猪俣敦夫,共立出版,ISBN-10: 4320009061
- 暗号技術のすべて,IPUSIRON,翔泳社,ISBN-10: 4798148814
- この一冊で全部わかるセキュリティの基本，宮本久仁男，SBクリエイティブ，ISBN-10: 4797388803
- セキュリティのしくみ,増井敏克,翔泳社,ISBN-10: 4798157201

オフィスアワー

・質問は講義中、講義後に受け付ける．

・部屋への訪問は，月曜日 3限 場所は1号館10階11013
・電子メ-ル(kida@eng.kagawa-u.ac.jp)では随時受け付ける。

履修上の注意・担当教員からのメッセージ

- PCを持参すること.授業中に検索，小テストの回答に利用するため.
- 授業の解説を，ただ聞くのではなく，自分で本質を考えながら参加すること.なぜそうしないといけないのか?なぜ必要なのか?など，頭で深掘りし，疑問がある場合には質問することを勧める.

参照ホームページ

特になし

メールアドレス

kida@eng.kagawa-u.ac.jp

教員の実務経験との関連

NECにて，10年以上の間，人工知能のセキュリティへの応用研究をすすめており，製品化、事業化もされています.この経験を活かし，表面的な 解説ではなく，なぜそうしないといけないのか?なぜ必要なのか，セキュリティ対策の本質を事例をもとに講義します.

予備項目７

予備項目８

ナンバリングコード 科目ナンバリングについて

授業科目名	科目区分	時間割	対象年次及び学科
情報セキュリティII Information Security Ⅱ		後期 木3	3〜 創造工学部
講義題目	水準・分野	DP・提供部局	対象学生・ 特定ﾌﾟﾛｸﾞﾗﾑとの対応
		bcdT	
担当教員	授業形態	単位数	時間割コード
喜田　弘司	Lx	2	5005140

DP・提供部局

bcdT

授業形態

Lx

関連授業科目

インターネットⅠ、インターネットⅡ、オペレーティングシステム、情報セキュリティ演習

履修推奨科目

情報セキュリティⅠ

学習時間

講義90分 × 15回 ＋ 自学自習（準備学習 30時間 ＋ 事後学習 30時間）

授業の概要

この授業は，情報セキュリティ技術の基礎を学んでいる方を対象に，高度化する攻撃に対応するためのより高度な技術の習得を目的とします．具体的には、「ネットワークセキュリティ編」と「ハードニング編」からなります．前者は、実際のネットワーク機器の設定を解説し、後者は、サイバー攻撃からサーバを守るハードニングと呼ばれる演習を解説します。なお、本授業は情報セキュリティ演習Ⅱと連動し、本授業は座学を演習Ⅱにて実習します。

授業の目的

情報セキュリティは，現在，攻撃者が圧倒的に有利な状況にあり，これに対応できるICTのエンジニア（ホワイトハッカー）の人材が必要です．ICTの基本技術は，OS，計算機言語，ネットワークであり，本講義では，これらをセキュリティ面から理解を深めます．具体的には，攻撃の手口と，その対策技術を学ぶことにより，将来，セキュリティ関連企業のエンジニアに，あるいは，一般企業の社内セキュリティのエンジニアになるための技術を勉強します．

到達目標

1.ルータ等のネットワーク機器の設定ができる
2.パケットキャプチャによりネットワークを流れているデータを分析することができる
3.サイバー攻撃を受けていることを検知し、状況を報告できる
4.サイバー攻撃を受けた場合に、対処方法を提案できる

5.サイバー攻撃を受けた場合に、対処チームの管理ができる

成績評価の方法と基準

期末テストは行わず，レポートと授業内の発表会で成績を評価する．レポートは課題を解いてもらう。発表会は授業内に数回行う予定である。 また、授業内容の理解度および出席確認のためのメモを毎回提出してもらう．

授業計画・授業及び学習の方法・準備学習及び事後学習のためのｱﾄﾞﾊﾞｲｽ

第1回：オリエンテーション

【ネットワークセキュリティ編】
第2回：OSI参照モデル（復習）
第3回：FW、IDS/IPS、WAFなどのセキュリティ機器
第4回：Web技術＋Webサーバ構築演習（IIS）
第5回：Webサーバに対する攻撃とセキュリティ対策
第6回：まとめ　発表会

【ハードニング編】
第7回：Linux　復習
第8回：ハードニング解説　データセンタ見学
第9回：ハードニング１回目　説明＋競技
第10回：ハードニング２回目
第11回：事前対策　解説
第12回：発表会
第13回：データ保護　解説
第14回：事後対策　解説
第15回：全体まとめ

・第8回、第10回、第11回は、Ａグループ、Ｂグループに分かれて授業を実施
・第8回は、Ａグループは、ハードニングの解説を本授業で行い、データセンター見学は、情報セキュリティ演習の時間に実施する。Ｂグループはこれと逆で行う。
・第10回、第11回は、Ａグループは上記のとおり行う。Ｂグループは、第10回と第11回を入れ替える。

【自学自習のためのアドバイス】
全回共通：
情報セキュリティは「生もの」と言われることがあります．日々，変化がある分野ですので，世の中の動きをウォッチする習慣が大事です（15分/日）．

第2回から第6回：ネットワーク技術が基礎になります。インターネットⅠ、インターネットⅡを適宜復習してください（1時間/週）。さらに下記の教科書でより深掘りをして下さい。（2時間/ 週）

第7回：第8回目以降に必要となる技術を中心にしたLinuxの復習の回です。この1回では復習しきれないため、情報システム・セキュリティ実験1で学んだことを復習して下さい(3時間/週)。

第8回から第15回：ハードニングは、ITインフラの総力戦です。オペレーティングシステム、で学んだことを適宜復習して下さい（1時間/週）。さらに、ハードニングで実際に直面した課題をふまえて、その技術を下記リストの教科書で調べて深掘りして下さい（2時間/週）。

教科書・参考書等

- ハッキング・ラボのつくりかた 仮想環境におけるハッカー体験学習,IPUSIRON,翔泳社,ISBN-10: 4798155306
- 動かして学ぶセキュリティ入門講座 ,岩井博樹,ISBN-10: 4797387467
- マジメだけどおもしろいセキュリティ講義 事故が起きる理由と現実的な対策を考える,すずきひろのぶ,ISBN-10: 4774193224
- セキュリティのためのログ分析入門 サイバー攻撃の痕跡を見つける技術,
折原慎吾ら，技術評論社，ISBN-10: 429710041X

- マスタリングTCP/IP 情報セキュリティ編，齋藤孝道，オーム社，ISBN-10: 4274069214
- サイバーセキュリティ入門,猪俣敦夫,共立出版,ISBN-10: 4320009061
- 暗号技術のすべて,IPUSIRON,翔泳社,ISBN-10: 4798148814
- この一冊で全部わかるセキュリティの基本，宮本久仁男，SBクリエイティブ，ISBN-10: 4797388803
- セキュリティのしくみ,増井敏克,翔泳社,ISBN-10: 4798157201

オフィスアワー

- 授業終了後、しばらくは自由演習の時間とする。教員やTAが質問を受け付ける。
- 1号館9Fの喜田研(KIDA-LABO)にて先輩がサポートします。

履修上の注意・担当教員からのメッセージ

- PCを持参すること.
- 授業以外にGoogle等で積極的に調べ、課題レポートに反映すること
- 操作方法を覚えるのではなく、技術の本質を考えること

★ 実験が時間通りに終わらないことがあるため、この後の予定は時間に余裕をもたせること
★ 実施場所が香川大学ではない回があり、現地集合の予定です。あらかじめご了承下さい。

参照ホームページ

授業中に指示する

メールアドレス

kida@eng.kagawa-u.ac.jp

教員の実務経験との関連

喜田は、NECにて，10年以上の間，人工知能のセキュリティへの応用研究をすすめており，事業化も成功しています.この経験を活かし，表面的な 解説ではなく，なぜそうしないといけないのか?なぜ必要なのか，コンピュータ技術の本質を理解できるように進めます。

予備項目７

予備項目８

ナンバリングコード [科目ナンバリングについて]

授業科目名	科目区分	時間割	対象年次及び学科
情報セキュリティ演習 Exercise in Information Security		後期 木4	3〜 創造工学部
講義題目	水準・分野	DP・提供部局	対象学生・ 特定ﾌﾟﾛｸﾞﾗﾑとの対応
		cbxT	
担当教員	授業形態	単位数	時間割コード
富永　浩之, 喜田　弘司　[Tominaga Hiroyuki]	Px	1	5005150

DP・提供部局

cbxT

授業形態

Px

関連授業科目

インターネットⅠ、インターネットⅡ、オペレーティングシステム、情報セキュリティII

履修推奨科目

情報セキュリティⅠ

学習時間

実験180分×15回＋自学自習（準備学習 60時間 + 事後学習 60時間）

授業の概要

この授業は，情報セキュリティ技術の基礎を学んでいる方を対象に，高度化する攻撃に対応するためのより高度な技術の習得を目的とします．具体的には、「ネットワークセキュリティ編」と「ハードニング編」からなります．前者は、実際のネットワーク機器の設定を解説し、後者は、サイバー攻撃からサーバを守るハードニングと呼ばれる演習を解説します。なお、本授業は情報セキュリティⅡと連動し、情報セキュリティⅡは座学を本授業にて実習します。

授業の目的

情報セキュリティは，現在，攻撃者が圧倒的に有利な状況にあり，これに対応できるICTのエンジニア（ホワイトハッカー）の人材が必要です．ICTの基本技術は，OS，計算機言語，ネットワークであり，本講義では，これらをセキュリティ面から理解を深めます．具体的には，攻撃の手口と，その対策技術を学ぶことにより，将来，セキュリティ関連企業のエンジニアに，あるいは，一般企業の社内セキュリティのエンジニアになるための技術を勉強します．

到達目標

1.ルータ等のネットワーク機器の設定ができる
2.パケットキャプチャによりネットワークを流れているデータを分析することができる
3.サイバー攻撃を受けていることを検知し、状況を報告できる
4.サイバー攻撃を受けた場合に、対処方法を提案できる

5.サイバー攻撃を受けた場合に、対処チームの管理ができる

成績評価の方法と基準

期末テストは行わず，レポートと授業内の発表会で成績を評価する．レポートは課題を解いてもらう。発表会は授業内に数回行う予定である。 また、授業内容の理解度および出席確認のためのメモを毎回提出してもらう．

授業計画・授業及び学習の方法・準備学習及び事後学習のためのｱﾄﾞﾊﾞｲｽ

第1回：オリエンテーション

【ネットワークセキュリティ編】
第2回：OSI参照モデル（復習）
第3回：FW、IDS/IPS、WAFなどのセキュリティ機器
第4回：Web技術＋Webサーバ構築演習（IIS）
第5回：Webサーバに対する攻撃とセキュリティ対策
第6回：まとめ　発表会

【ハードニング編】
第7回：Linux　復習
第8回：ハードニング解説　データセンタ見学
第9回：ハードニング１回目　説明＋競技
第10回：ハードニング２回目
第11回：事前対策　解説
第12回：発表会
第13回：データ保護　解説
第14回：事後対策　解説
第15回：全体まとめ

・第8回、第10回、第11回は、Ａグループ、Ｂグループに分かれて授業を実施
・第8回は、Ａグループは、ハードニングの解説を本授業で行い、データセンター見学は、情報セキュリティ演習の時間に実施する。Ｂグループはこれと逆で行う。
・第10回、第11回は、Ａグループは上記のとおり行う。Ｂグループは、第10回と第11回を入れ替える。

【自学自習のためのアドバイス】
全回共通：
情報セキュリティは「生もの」と言われることがあります．日々，変化がある分野ですので，世の中の動きをウォッチする習慣が大事です（15分/日）．

第2回から第6回：ネットワーク技術が基礎になります。インターネットⅠ、インターネットⅡを適宜復習してください（1時間/週）。さらに下記の教科書でより深掘りをして下さい。（2時間/ 週）

第7回：第8回目以降に必要となる技術を中心にしたLinuxの復習の回です。この1回では復習しきれないため、情報システム・セキュリティ実験1で学んだことを復習して下さい(3時間/週)。

第8回から第15回：ハードニングは、ITインフラの総力戦です。オペレーティングシステム、で学んだことを適宜復習して下さい（1時間/週）。さらに、ハードニングで実際に直面した課題をふまえて、その技術を下記リストの教科書で調べて深掘りして下さい（2時間/週）。

教科書・参考書等

- ハッキング・ラボのつくりかた 仮想環境におけるハッカー体験学習,IPUSIRON,翔泳社,ISBN-10: 4798155306
- 動かして学ぶセキュリティ入門講座 ,岩井博樹,ISBN-10: 4797387467
- マジメだけどおもしろいセキュリティ講義 事故が起きる理由と現実的な対策を考える,すずきひろのぶ,ISBN-10: 4774193224
- セキュリティのためのログ分析入門 サイバー攻撃の痕跡を見つける技術,
折原慎吾ら，技術評論社，ISBN-10: 429710041X

- マスタリングTCP/IP 情報セキュリティ編，齋藤孝道，オーム社，ISBN-10: 4274069214
- サイバーセキュリティ入門,猪俣敦夫,共立出版,ISBN-10: 4320009061
- 暗号技術のすべて,IPUSIRON,翔泳社,ISBN-10: 4798148814
- この一冊で全部わかるセキュリティの基本，宮本久仁男，SBクリエイティブ，ISBN-10: 4797388803
- セキュリティのしくみ,増井敏克,翔泳社,ISBN-10: 4798157201

オフィスアワー

- 授業終了後、しばらくは自由演習の時間とする。教員やTAが質問を受け付ける。
- 1号館9Fの喜田研(KIDA-LABO)にて先輩がサポートします。

履修上の注意・担当教員からのメッセージ

- PCを持参すること.
- 授業以外にGoogle等で積極的に調べ、課題レポートに反映すること
- 操作方法を覚えるのではなく、技術の本質を考えること

★ 実験が時間通りに終わらないことがあるため、この後の予定は時間に余裕をもたせること
★ 実施場所が香川大学ではない回があり、現地集合の予定です。あらかじめご了承下さい。

参照ホームページ

授業中に指示する

メールアドレス

kida@eng.kagawa-u.ac.jp

教員の実務経験との関連

喜田は、NECにて，10年以上の間，人工知能のセキュリティへの応用研究をすすめており，事業化も成功しています.この経験を活かし，表面的な 解説ではなく，なぜそうしないといけないのか?なぜ必要なのか，コンピュータ技術の本質を理解できるように進めます。

予備項目７

予備項目８