TDU 東京電機大学 TOKYO DENKI UNIVERSITY

CySec

社会人向けサイバーセキュリティ講座「セキュアシステム設計・開発」の実践

東京電機大学
研究推進社会連携センター **柿崎淑郎**
未来科学部情報メディア学科 寺田真敏

関連するJ17-IS LU

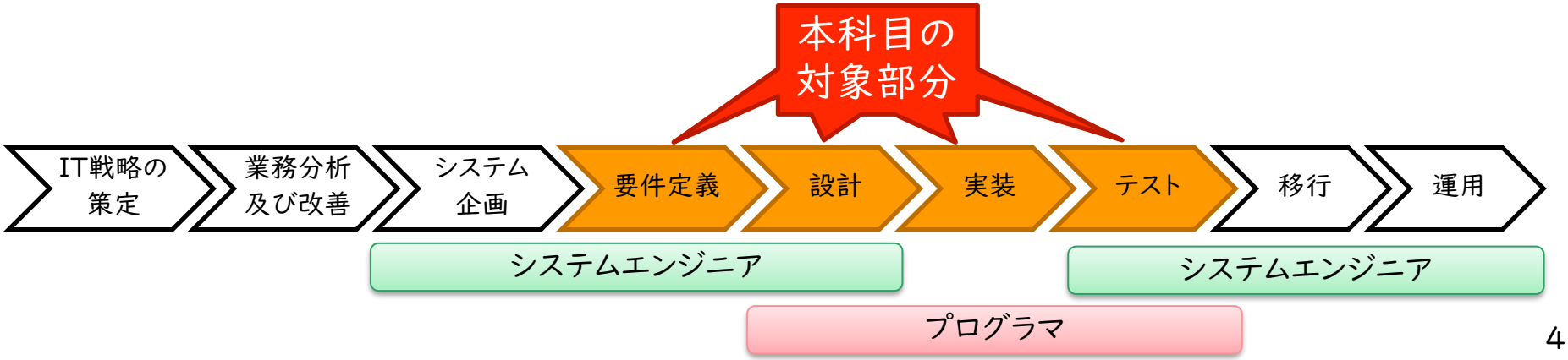
- 1904 リスクアセスメントとリスクマネジメント
- 1905 セキュアシステム設計
- 1906 セキュリティ要求分析
- 1907 セキュアプログラミング
- 1909 ネットワークセキュリティ
- 1910 アプリケーションの脆弱性

教育対象と目標

- 教育対象者
  - システムエンジニア, ソフトウェア開発者
- 教育目標
  - セキュアシステム設計論を修得する
  - コモンクライテリアに基づく保証と評価の実際について,
    演習を通して体得する
  - Webアプリケーションの脆弱性検査手法と
    その基本的対策の能力を獲得する

本実践の特徴
「セキュアシステム設計・開発」

- 社会人向けサイバーセキュリティ講座CySec内の1科目
  - 本科目を含め7科目を修めると履修証明書が交付（法第105条）
  - 大学院修士課程自由履修科目と併用
  - 2015年度開講，2020年度はオンライン授業で継続開講中
  - 本応募でご紹介するのは2019年度までの取り組みおよびその成果です
- システム開発プロセスのVモデルに従って，その各段階におけるセキュリティ対策を要件定義，設計，実装，テストと一連の流れに沿って，実践的に学修することで，セキュリティ・バイ・デザインに基づくセキュアなシステム設計および開発ができるようにする．



「セキュアシステム設計・開発」の位置づけ

サイバーセキュリティ基盤I

サイバーセキュリティ基盤II

基礎科目（CISSP講座）

応用科目

座学中心科目

セキュリティインテリジェンス
と心理・倫理・法

デジタル・フォレンジック

情報セキュリティ
マネジメントとガバナンス

演習中心科目

サイバーディフェンス
実践演習

セキュアシステム設計・開発

「セキュアシステム設計・開発」の構成

- 土曜隔週3コマ（90分/コマ）

- 総論
- セキュアプログラミング（ネイティブアプリケーション）1,2
- セキュアプログラミング（Webアプリケーション）1,2
- セキュアインフラ構築（ネットワーク）
- セキュアインフラ構築（サーバ）
- セキュリティ脅威分析1,2
- プロジェクト・マネジメント演習
- セキュリティ要求仕様と分析手法1,2
- 開発手法コモンクライテリア（ISO/IEC 15408）1,2

具体的な内容

- 総論
  - セキュリティ・バイ・デザインの考え方
  - 関連するガイドラインやベストプラクティス
  - セキュリティ開発ライフサイクル（SDL）
- セキュアプログラミング（ネイティブアプリケーション）
  - Windowsアプリの安全な実装（C言語で書かれたアプリが題材）
  - バッファオーバーフロー（BOF）が発生する理論と実際の対処
- セキュアプログラミング（Webアプリケーション）
  - Webアプリの安全な実装（PHPアプリケーションが題材）
  - クロスサイトスクリプティング（XSS），SQLインジェクション（SQLi），クロスサイトリクエストフォージェリ（CSRF）などの脆弱性が含まれた仮想マシン上のサンプルアプリを解析しながら修正

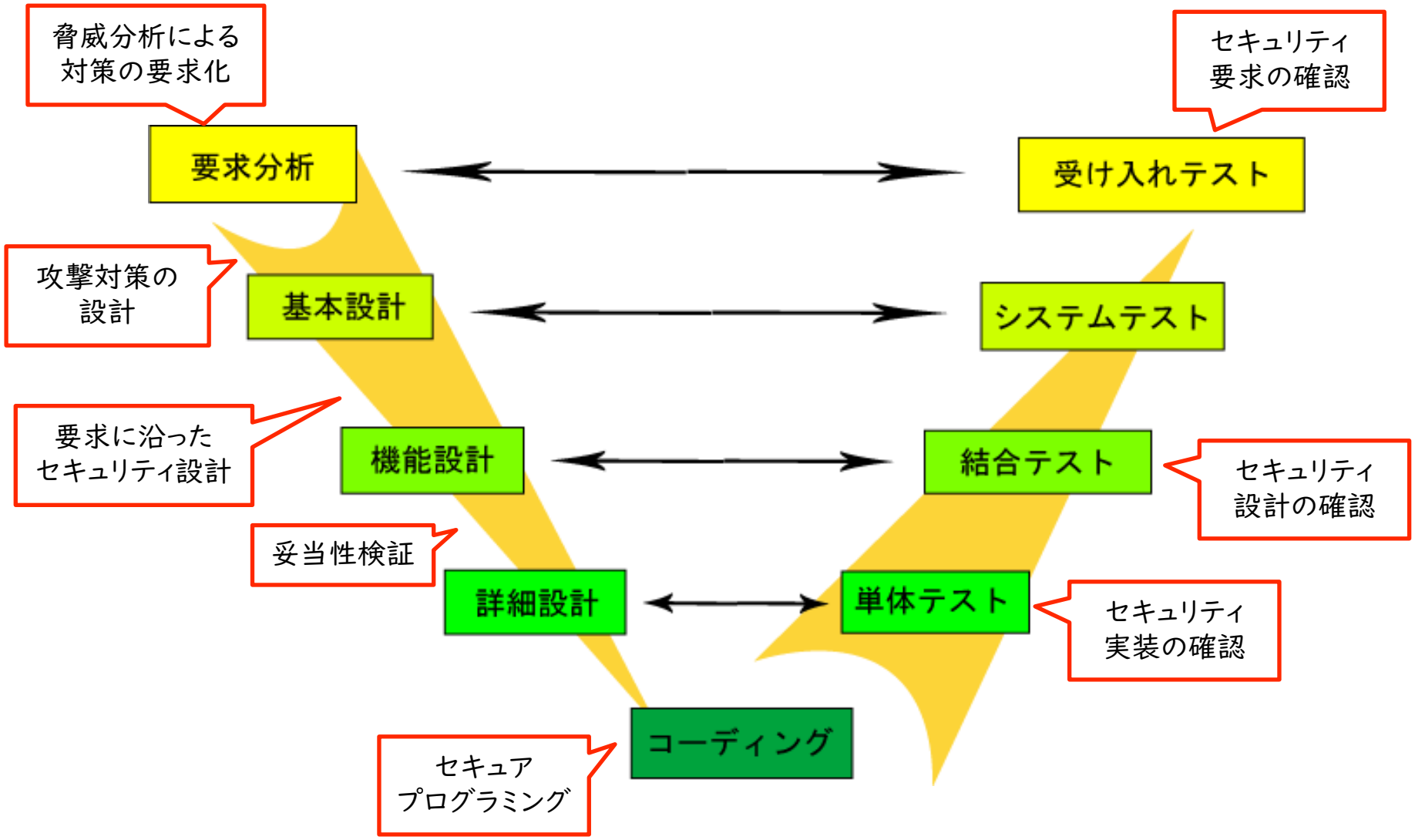
具体的な内容

- セキュアインフラ構築（ネットワーク）
  - サイバー攻撃手法の変遷
  - サイバー攻撃のモデル化と対処
  - 脆弱性の深刻度評価
- セキュアインフラ構築（サーバ）
  - サイバー攻撃とその対応
  - ソフトウェアファイアウォールの正しい設定方法
  - SELinuxの利用方法
  - サーバ堅牢化手法

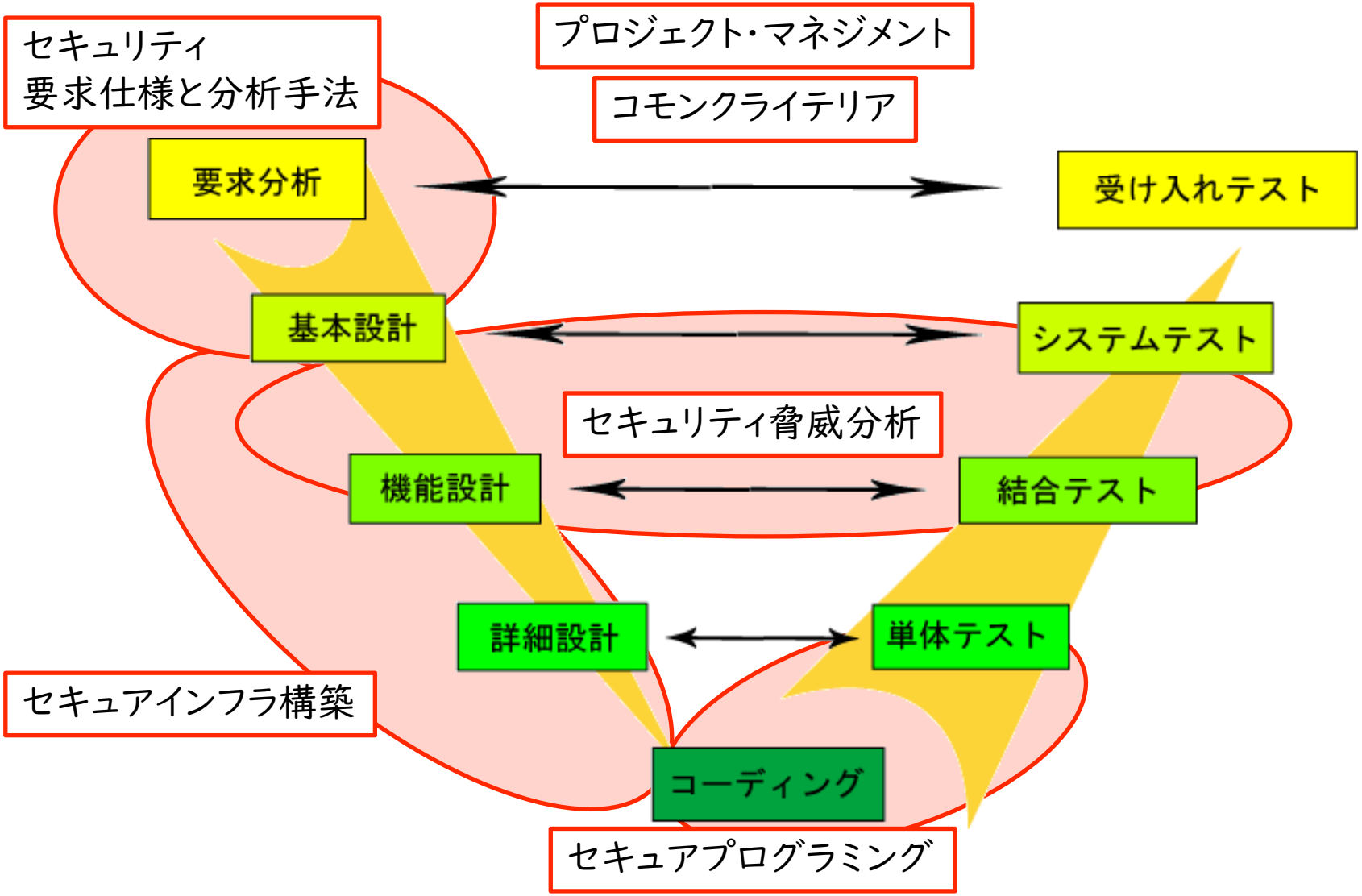
具体的な内容

- セキュリティ脅威分析
  - データフロー図, 脅威ツリー
  - 脅威分類体系STRIDE, 脅威影響評価DREAD
  - 脅威モデリングツール
  - 例題に対する脅威情報の収集と分析演習
- プロジェクト・マネジメント演習
  - スコープマネジメント, スケジュールマネジメント, 品質マネジメント
- セキュリティ要求仕様と分析手法
  - セキュリティ・バイ・デザインの必要性
  - 脅威分析, 被害分析, 攻撃分析
  - ミスユースケース
- 開発手法コモンクライテリア（ISO/IEC 15408）
  - セキュリティターゲット, セキュリティ保証要件, セキュリティ機能要件

Vモデルとの対応


脅威分析による
対策の要求化
要求分析
セキュリティ
要求の確認
受け入れテスト
攻撃対策の
設計
基本設計
システムテスト
要求に沿った
セキュリティ設計
機能設計
結合テスト
セキュリティ
設計の確認
妥当性検証
詳細設計
単体テスト
セキュリティ
実装の確認
コーディング
セキュア
プログラミング

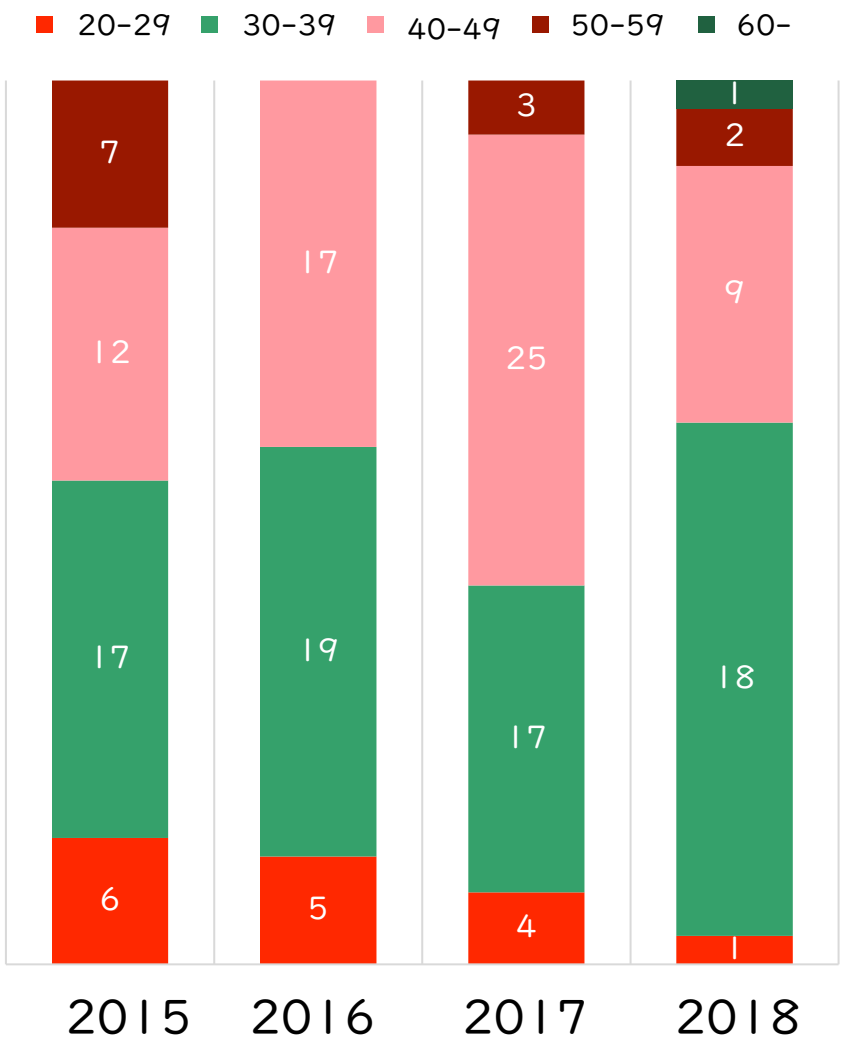
Vモデルとの対応


セキュリティ
要求仕様と分析手法
プロジェクト・マネジメント
コモンクライテリア
要求分析
受け入れテスト
基本設計
システムテスト
セキュリティ脅威分析
機能設計
結合テスト
詳細設計
単体テスト
セキュアインフラ構築
コーディング
セキュアプログラミング

教育効果

- システム開発の各段階におけるセキュリティ対策を一貫して学修
  - セキュリティ業界においても，設計開発，運用，分析は，異なる業務として認識されており，独立したスキルであると理解されている．
  - そのため，それぞれの分野に特化したスキルは有していても，隣接分野には知識がないことは少なくない．
- Vモデルに沿って一連の流れを演習することで，隣接分野への理解を醸成し，分野間コミュニケーションができる人材を育成する
  - 視野が広がることで，専門分野での取り組みを見直すきっかけに
  - 各段階でのセキュリティを徹底することで，システム全体の堅牢性を向上
- セキュリティ・バイ・デザイン，システム開発ライフサイクルの考えを元にしたリスクマネジメントとセキュリティ対策コストの見積もり
  - これは別科目で学修しています（本実践の範囲外）

受講生の年齢層



- 30代～40代中盤が主
  - 次期課長級，次期開発責任者級が多い
- セキュリティユーザ系企業の受講生が増加
  - 社内SOC，社内CSIRT等のメンバが増加

SOC･･･Security Operation Center
CSIRT･･･Computer Security Incident Response Team

受講生の推移

新規受講者数

年度	前期	後期
2015	35	9
2016	42	7
2017	41	14
2018	24	9
2019	54	7
総数	242（大学院生28名を含む）	

年度末修了者数

年度	修了者数
2015	18
2016	35
2017	24
2018	24
2019	26
総数	127

- 101名が最短の1年で修了
  - 教育訓練給付制度の場合，1年以内での修了が要件となっている
- 土曜隔週集中の演習科目は社会人には学びやすい
  - 平日夜間はまとまった時間が確保できない

受講生からの授業評価

年度	2015	2016	2017	2018	2019	平均
興味と関心が深まりましたか？	4.46	4.37	4.38	4.22	4.47	4.38
総合的な満足度	4.40	4.35	4.35	4.35	NA	4.36

NA･･･大学所定アンケートより廃止されたため

- 最低1，最高5の5段階評価
- 全体的に良好な評価である，が...
  - 他6科目と比較しても同程度
  - 評価指標としてはほとんど機能していない

修了生アンケート（自由記述）

- ポジティブな意見
- セキュリティ設計の演習などは業務で行っていたセキュリティ設計のやり方の見直しに役立った．
- 「セキュアインフラ構築（ネットワーク）」は社内と顧客向けの説明に役立った．
- 「開発手法コモンクライテリア」は業務で行っていた内容の振り返りと見直しに役立った．

- 改善要望の意見
- レベルが高く，進行スピードが速く，理解が困難だった．
- 演習の時間が短く，十分に理解できなかった．
- 講義資料の公開が遅く，予習ができなかった．

修了生の追跡調査

- 初年度（2015年度）はセキュリティベンダ系企業の受講者多数
  - 「本プログラムを受けなくても良いのでは？」と思う方々も多数...
    - この方々の口コミが後々に良い影響を与えてくれる
- 2017年度頃からユーザ系企業の受講者が急増
  - 初年度受講生からの口コミが功を奏している（？）
  - 国内でのCSIRTブームと連動するような傾向
- 国際的なサイバーセキュリティ資格CISSPに合格する修了生の情報が聞こえ始める
  - CISSPは全世界で14万人，日本には2758人（2020年7月時点）
  - 具体的な実数は追跡できていません
- 修了生のキャリアアップや転職成功例の情報が聞こえ始める
  - 官公庁ではベンダ系講座よりも大学の学問体系で修了したことが高評価
  - 具体的な実数は追跡できていません

今後の改善

- 2020年度の取り組み
  - セキュアプログラミングをWeb系に集約し，
    プログラミングに不案内な受講生の受講コストを低減
    - ユーザ系企業の受講者が増えたことで，受講者の多様性が広がり，
      プログラミングスキル等の前提知識にバラツキが増加したため
  - セキュアインフラ構築を1単元に統合し，攻防戦化
    - いくつかのグループに分けて，脆弱なサーバを堅牢化し，
      グループ間で攻撃と防衛を行うゲーム形式の演習
    - 新型コロナウイルス対応の影響でオンライン授業になったため未実施
  - 新型コロナウイルス対応によるオンライン授業化
    - 仮想マシン，講義映像，講義資料を見つつ，演習できるか・・・？
      - 演習室であれば，スクリーン×2，卓モニタ，自PCで豊富だが・・・
      - オンデマンド型あるいはリアルタイム型の録画配信で，意外となんとかなった
      - 一時停止できたり，巻き戻しができるのは，非常に高評価だった
    - 演習中に受講生の進捗を把握するのは困難
      - 教室を見回るという行為のオンラインにおける代替手段が見つからない