

# IPAX2005

## 情報処理技術者試験の改革に向けて

2005年5月20日

独立行政法人情報処理推進機構  
情報処理技術者試験センター

# 第1部

## テクニカルエンジニア(情報セキュリティ)試験の創設について

試験の名称は、仮称です。

本日の講演内容については、今後の詳細検討の中で見直されることもあります。

# 講演者の紹介

## □ 杉野 隆 教授

- 国土館大学情報科学センター
- 情報処理技術者試験委員

- 所属学会  
日本オペレーションズ・リサーチ学会  
情報処理学会  
経営情報学会  
情報システム学会

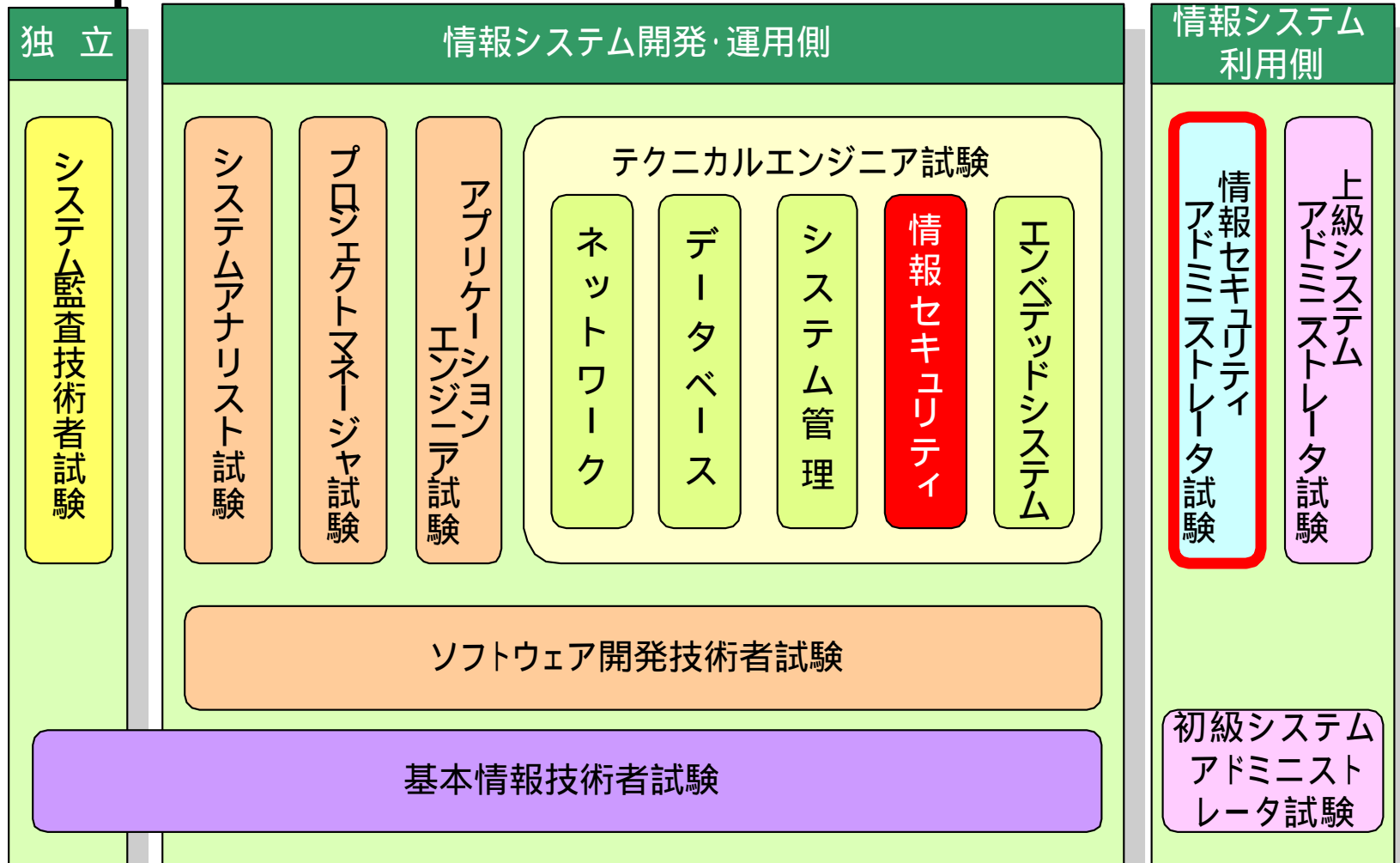
- プロフィール  
1969年～ 新日本製鉄株式会社(情報システム部門)  
1988年～ 新日鉄情報通信システム株式会社(ネットワーク事業部)  
1997年～ 株式会社シリウス(技術開発、ネットワーク技術)  
1999年～ 新潟国際情報大学情報文化学部情報システム学科教授  
2001年～ 現職

# 試験の概要

試験の名称は、仮称です。

名 称	テクニカルエンジニア(情報セキュリティ)試験
英語表記	Information Security Engineer Examination
受験資格	なし
免除制度	なし
試験開始	平成18年度春期(予定)

# 試験の位置付け



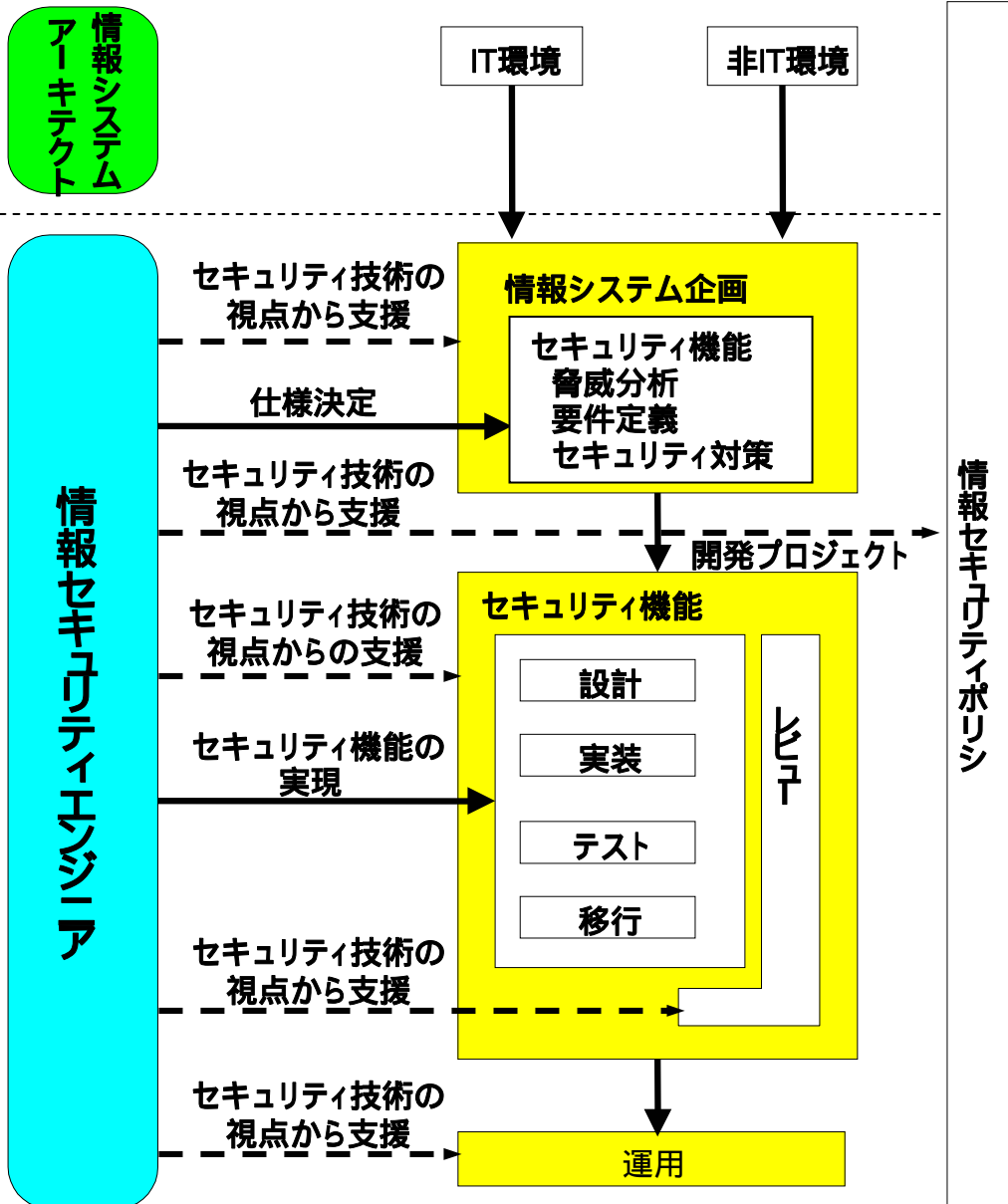
# 対象者のイメージ

**既存のシステムを組み合わせ、適切なセキュリティ機能を提供する情報システムを開発する者、又は支援する者**

**セキュリティ機能を組み込んだ業務アプリケーションの開発を支援する者**

**これらの立場におかれた開発者は、情報システムの開発プロジェクトにおいて、情報セキュリティ技術面からの支援、セキュリティ機能の要件定義、開発を行うプロセスに携わる。**

# 情報セキュリティエンジニアの業務範囲



# 役割と業務 (1/2)

- セキュリティ機能が求められる情報システムの企画・設計・開発・運用において、セキュリティ機能の企画・設計・開発を推進又は支援する業務、若しくはセキュアな開発プロジェクト環境を整備する業務に従事し、次の役割を果たす。

情報システムのぜい弱性・脅威を分析・評価し、これらを適切に回避・防止するセキュリティ機能の企画・設計・開発を推進又は支援する。

## 役割と業務 (2/2)

情報システム又はセキュリティ機能の開発までのプロジェクトにおいて、情報システムに対して与えられる脅威を分析し、適切に回避可能なプロジェクト管理を支援する。

セキュリティ侵犯への対処やセキュリティパッチの適用作業など情報システム運用時のセキュリティ管理作業を技術的な側面から支援する。

## 期待する技術水準 (1/2)

- 情報システムでは、多くのコンポーネントにおいてセキュリティ機能が求められる。情報セキュリティ技術の専門家として、他の専門家と協力しながら情報セキュリティ技術を適用して、セキュアな情報システムを開発・運用するため、次の幅広い知識・経験・実践能力が要求される。

情報セキュリティ対策のうち、技術的な対策について基本的な技術と複数の特定の領域における応用技術を持ち、これらの技術を対象システムに適用するとともに、その効果を評価できる。

## 期待する技術水準 (2/2)

情報セキュリティ対策のうち、運用的な対策について基本的な知識と適用場面に関する技術をもつとともに、情報セキュリティマネジメントの基本的な考え方を理解し、これを適用するケースについて具体的な知識をもち、評価できる。

情報技術のうち、ネットワーク、データベース、システム開発環境について基本的な知識をもち、情報システムの機密性、責任追跡性などを確保するために必要な暗号、フィルタリング、ロギングなどの要素技術を理解している。

情報システム開発における工程管理について基本的な知識と具体的な適用事例の知識をもつ。

# 情報セキュリティアドミニストレータ試験(SS)との相違点



- テクニカルエンジニア(情報セキュリティ)試験(TS)の新設に伴い、情報セキュリティ関連業務を開発側と利用側に分け、それぞれをTSとSSが分担することを明確にする。
- TS: 情報システムの開発側にあつて、主として情報セキュリティシステムの設計・開発を業務とする。  
SS: 情報システムの利用側にあつて、主として情報セキュリティ環境の確保を業務とする。
- SSは情報セキュリティポリシーの作成・管理・運用を通じて、TSの業務への指針を与える。運用業務は、TSの技術的支援を受けながら、SSがシステム管理エンジニアと連携して実施する。

# TSとSSの役割分担

プロセス		TS	SS
管理		<ul style="list-style-type: none"> <li>情報セキュリティポリシー作成への技術的支援</li> </ul>	<ul style="list-style-type: none"> <li>情報セキュリティポリシーの作成、管理</li> <li>セキュリティ対策の企画推進</li> <li>情報セキュリティポリシーの運用、ユーザ教育</li> </ul>
企画	RFP	<ul style="list-style-type: none"> <li>情報システムの技術的セキュリティ要件の検討、要求定義の作成</li> <li>セキュリティ要求定義を満足する技術的手法 / 製品の検討と選定</li> </ul>	<ul style="list-style-type: none"> <li>情報システムの技術的セキュリティ要件の提示、要求定義の評価</li> <li>情報システムの物理的・管理的セキュリティ要件の検討、要求定義の作成</li> </ul>
開発	設計	<ul style="list-style-type: none"> <li>情報システムに対する脅威・脆弱性の分析と対抗手段の策定又は支援</li> <li>セキュアなモジュール構造の設計</li> <li>セキュアなプロトコル・方式の採用</li> </ul>	
	実装	<ul style="list-style-type: none"> <li>セキュリティ機能の実装</li> </ul>	<ul style="list-style-type: none"> <li>物理的、管理的セキュリティの実装</li> </ul>
	テスト	<ul style="list-style-type: none"> <li>セキュリティ機能のテスト</li> <li>情報システムの脆弱性テスト</li> </ul>	<ul style="list-style-type: none"> <li>セキュリティ機能のテストへの利用者としての参加</li> </ul>
	レビュー	<ul style="list-style-type: none"> <li>プロトコル、方式の安全性の検証</li> </ul>	<ul style="list-style-type: none"> <li>管理的セキュリティ機能・運用形態の妥当性の検証</li> </ul>
運用	移行	<ul style="list-style-type: none"> <li>情報システムのセキュリティを維持するための各種マニュアルの作成</li> </ul>	
	監視	<ul style="list-style-type: none"> <li>セキュリティ侵犯への対抗策実施の技術的支援</li> <li>エンドユーザコンピューティングの技術的支援</li> </ul>	<ul style="list-style-type: none"> <li>セキュリティ侵犯の監視と対処</li> <li>エンドユーザコンピューティングにおける指導、教育</li> </ul>
	運用	<ul style="list-style-type: none"> <li>セキュリティパッチ適用作業の技術的支援</li> </ul>	<ul style="list-style-type: none"> <li>利用部門のセキュリティ責任者</li> <li>セキュリティパッチ情報の収集と適用</li> </ul>

# 試験形式と試験時間

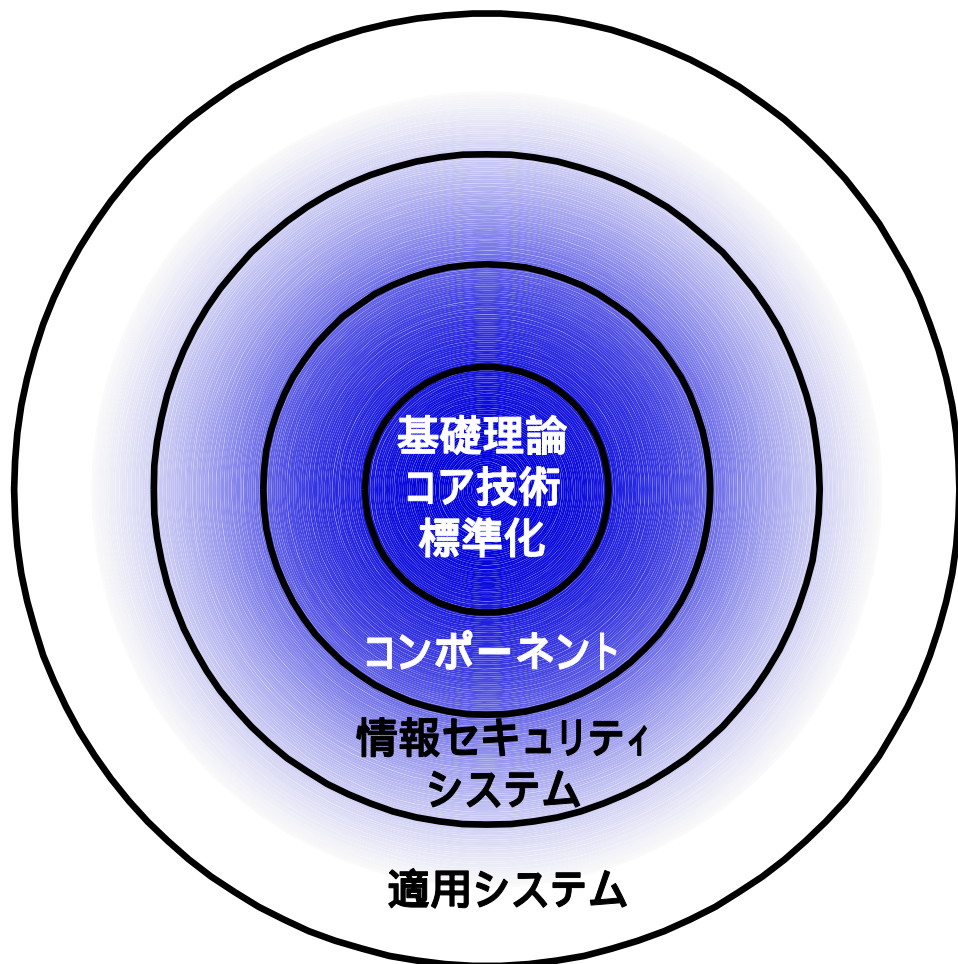
午前	午後	午後
9:30 ~ 11:10 (100分)	12:10 ~ 13:40 (90分)	14:10 ~ 16:10 (120分)
<b>多肢選択式(四肢択一)</b>	<b>記述式</b>	<b>論述式(事例解析)</b>
55問出題して55問解答	4問出題して3問解答	2問出題して1問解答

試験形式と試験時間は、今後の詳細検討の中で見直されることもあります。

# 試験で対象とする情報セキュリティエンジニアのスキル範囲のイメージ



- 主領域** :セキュリティ関連の「基礎理論・技術、標準化」、「コンポーネント」、「情報セキュリティシステム」
- 周辺スキル** :適用システムに実装するために必要な周辺知識・技術
- 主な適用システム** :NW、DB、OSセキュリティ、重要なアプリケーション



# 出題範囲(午前の試験)

試験区分 分野	テクニカルエンジニア					情報セキュリティ アドミニストレー タ
	情報セ キュリティ	ネット ワーク	デー タ ベース	シス テム 管理	エン ベ デッド	
コンピュータ科学基礎						
コンピュータシステム						
システムの開発と運用						
ネットワーク技術						
データベース技術						
セキュリティと標準化						
情報化と経営						
監査						

・ は出題範囲であることを、 は出題範囲のうちの重点分野であることを表します。

・ 、 、 は技術レベルを表し、 が最も高度で、 は 及び を、 は を含みます。

出題範囲(午前の試験)は、今後の詳細検討の中で見直されることもあります。

# 出題範囲(午後の試験)(1/2)

## (1) 情報セキュリティシステムの企画・設計・開発に関すること

情報システムの企画・設計・開発、物理的セキュリティ対策、アプリケーションセキュリティ対策、データベースセキュリティ対策、セキュアプログラミング、ネットワークセキュリティ対策、システムセキュリティ対策 など

## (2) 情報セキュリティの運用・管理に関すること

情報セキュリティポリシ、リスク分析、業務継続計画、セキュリティ運用・管理、脆弱性分析、誤使用分析、ユーザセキュリティ管理、障害復旧計画、情報セキュリティ教育、システム監査(のセキュリティ側面) など

## 出題範囲(午後の試験)(2/2)

### (3) 情報セキュリティ技術・関連法規に関すること

アクセス管理技術、ウイルス対策技術、暗号技術、認証技術、セキュリティ応用システム(署名、侵入検知システム、ファイアウォール、セキュアな通信技術(VPNなど)、鍵管理技術、PKIなど)、攻撃手法、監査証跡のためのログ管理技術、耐タンパ技術、情報セキュリティ関連法規、国内・国際標準ガイドライン、著作権法、プライバシー保護、情報倫理 など

### (4) 開発の管理に関すること

開発ライフサイクル管理、システム文書構成管理、配布と操作、人的管理手法(チーム内の不正を起こさせないような仕組み)、開発環境の情報セキュリティ管理 など

# ITスキル標準との対応

職種	専門分野	達成度指標			
		責任性	複雑性	サイズ	タスク特性
ITスペシャリスト	セキュリティ	4 技術チームリーダー (責任者ではない)	4~5 プロジェクトにおける設計・構築・導入の経験と実績	4 ピーク時のプロジェクトの要員10人未満	4~5* セキュリティに特化した領域において独力で実践できる (他を指導するも含む)

\* プロフェッショナルとしての(顕著な)貢献と実績は対比できない。

A decorative graphic on the left side of the slide, consisting of three colored circles (dark teal, light teal, and grey) and a vertical line.

# サンプル問題

午後

**IDSによるセキュリティ監視**

午後

**安全な電子商取引システムの構築**