ＩＰＡ新試験対応の授業実践効果と産学官連携したセキュリティ人材教育

埼玉県立新座柳瀬高等学校

藤巻　朗

昨年度の発表概要

単位制の特徴を活かして系統立てた情報教育の実践

↓

内閣サイバーセキュリティセンター（NISC）が提唱した

CCSF（共通キャリア・スキルフレームワーク）

レベル1 が完全定着した

内閣サイバーセキュリティセンター（NISC）

『教育機関で育てる人材のレベルと企業が必要とする人材のレベルを明確に双方が認識できる仕組みが重要』

↓

「共通キャリア・スキルフレームワーク」（ＣＣＳＦ）を定める

レベル定義と情報処理技術者試験

レベル1（入門レベル）～レベル7（超高度レベル）

「ＩＴパスポート試験」　⇒　レベル1に相当

「情報セキュリティマネジメント試験」⇒　レベル2に相当

↓

３年間系統立てた情報教育の実践により

ＩＴパスポート試験を活用して、

CCSFレベル１を定着させる

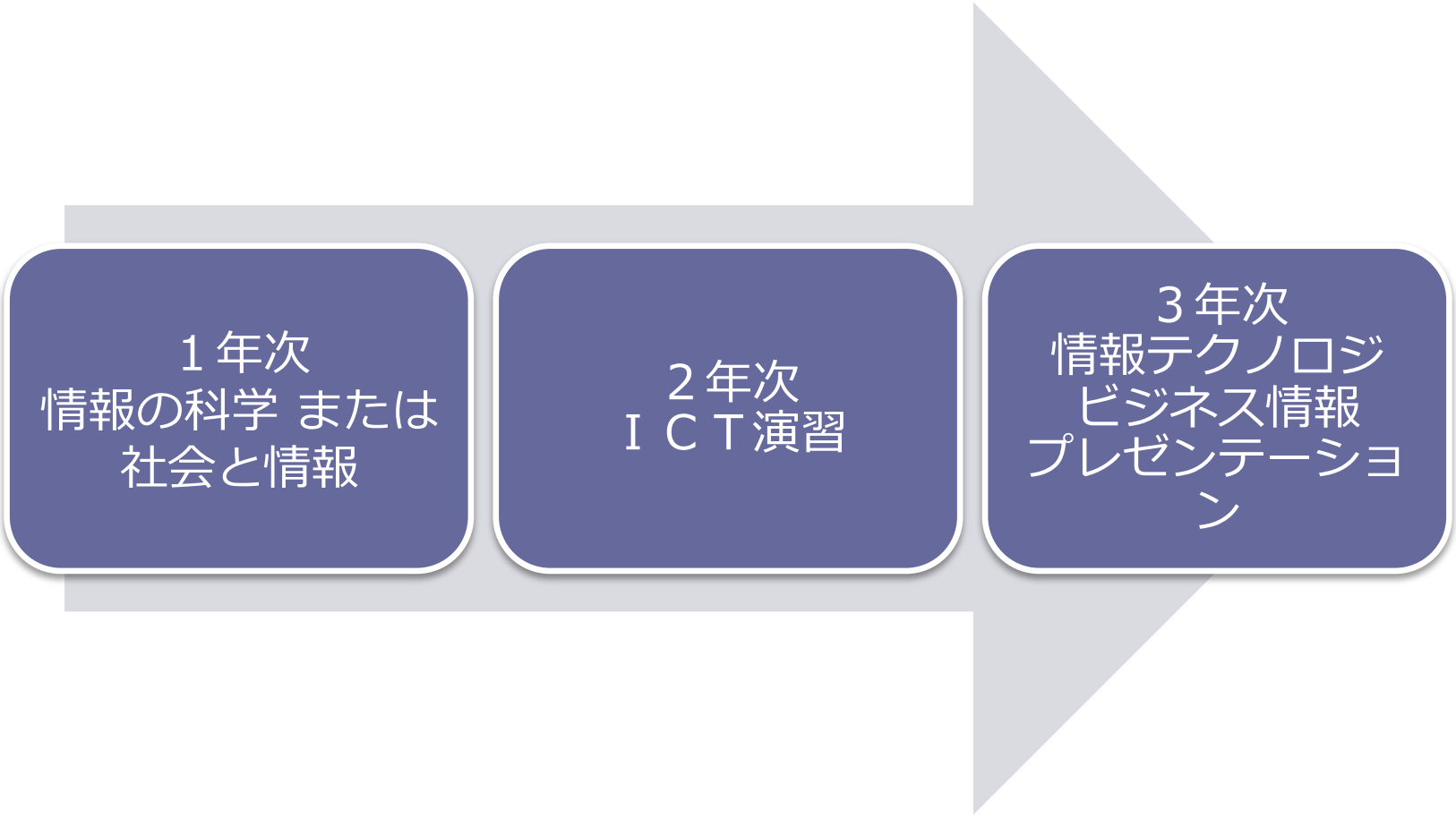
CCSFが定める分野・分類

分野	大分類
テクノロジ系	基礎理論
	コンピュータシステム
	技術要素
	開発技術
マネジメント系	プロジェクトマネジメント
	サービスマネジメント
ストラテジ系	システム戦略
	経営戦略
	企業と法務

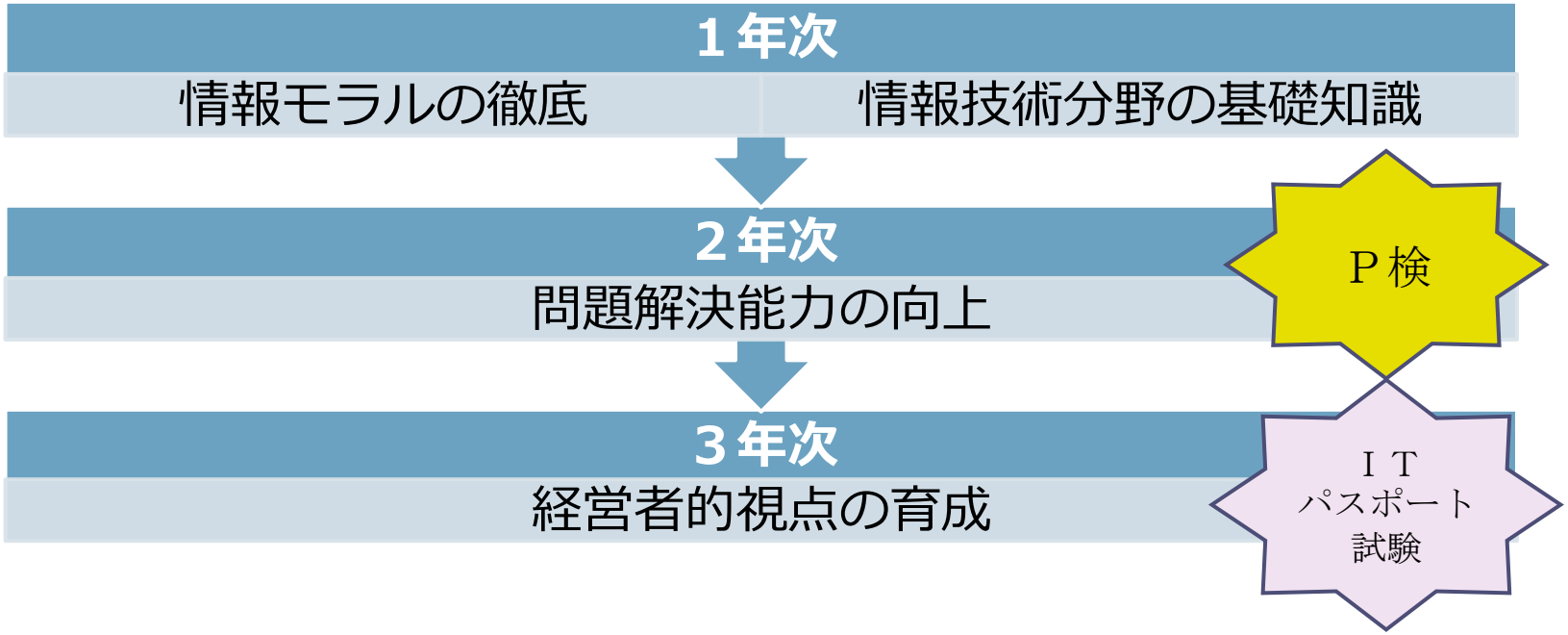
問題解決能力

経営者的視点

３年間系統立てた情報教育の実践



情報セキュリティ人材育成プログラムの内容



（実際に合格者を含めて）ＣＣＳＦレベル１が定着した

今年度は

「情報セキュリティ人材育成プログラム」

↓

「情報セキュリティマネジメント試験」を

活用して、CCSFレベル2の定着を検証する

（先に）結論として

「情報セキュリティマネジメント試験」

（ＣＣＳＦレベル２）への対応が確認できた（後述）

↓

そこで、政府各省庁機関等で取り組んでいる

サイバーセキュリティ人材育成施策への
橋渡し役に向けた今後の方向付け

について検討する

具体的な授業事例

「具体的な授業事例を教えて欲しい」との

昨年度全国神奈川県大会発表コメントより

①　標的型サイバー攻撃

ファイアウォールとボットウイルス

武田一城 「日本の終戦までの最後の1年間とサイバーセキュリティの現状の共通点」
http://www.itmedia.co.jp　2016年09月01日

「ボット」と「C&Cサーバ」

ボットとは

コンピュータを外部から遠隔操作するための

バックドア型不正プログラムの一種

C&Cサーバとは

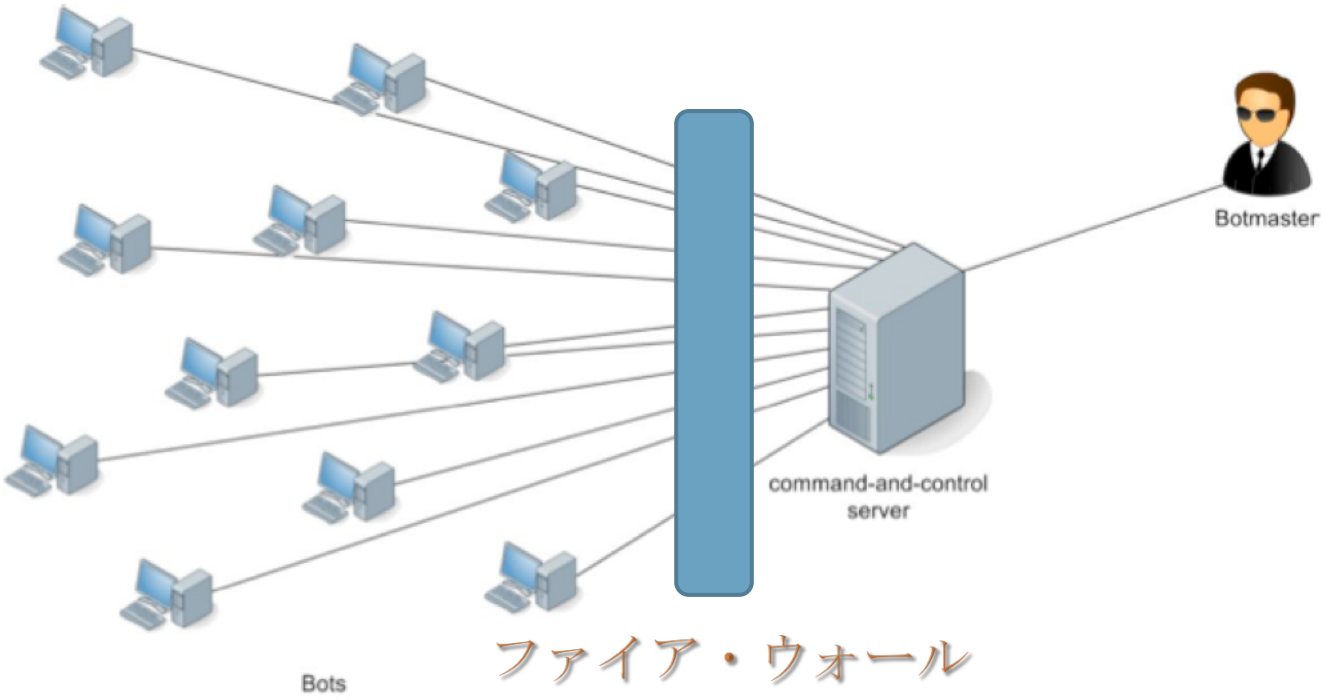
遠隔操作のための指令を送るサーバ

最大の特徴

C&Cサーバから一括して複数のボット感染環境を

遠隔操作できる仕組み（ボットネットワーク）を構成する

如何にしてボットウイルスを
ＦＷ内部へ侵入させるか？



C&C サーバ振る舞い情報抽出・分析システムの提案
情報セキュリティ大学院大学　田中英彦研究室

「絶対国防圏」の設置

サイパン島の陥落

1944年7月18日　サイパン島の陥落により

太平洋戦争の日本の敗戦は決定的

↓

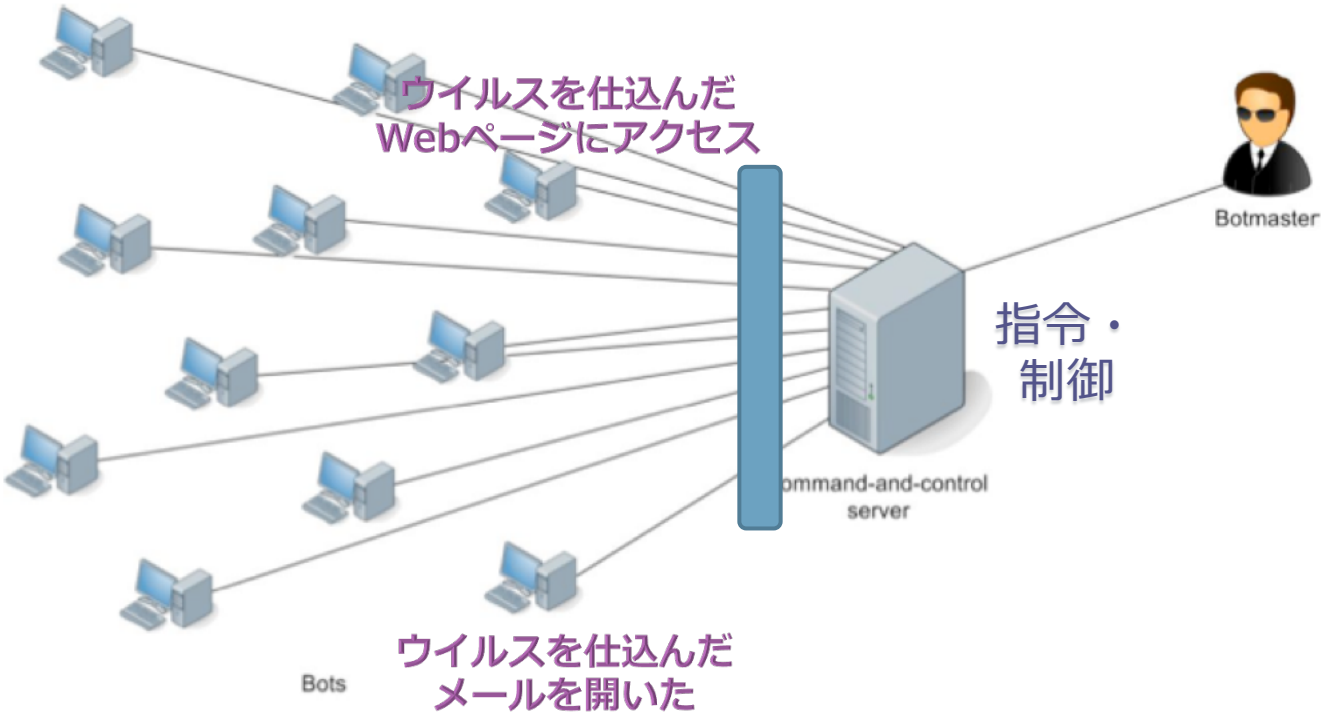
このサイパン島を飛び立った爆撃機の空襲に

日本がさらされるようになる

「絶対国防圏」を突破された後は、

組織的な防御としては壊滅状態

ボットネットの構築



C&C サーバ振る舞い情報抽出・分析システムの提案

情報セキュリティ大学院大学　田中英彦研究室

②　公開鍵認証基盤（ＰＫＩ）

公開鍵暗号方式

南京錠

太平洋戦争における日本海軍の暗号

- ミッドウェイ海戦
- 山本五十六連合艦隊司令長官の戦死

米国海軍は日本側の暗号通信を傍受し解読して、

日本軍の作戦計画の全容を事前に知り尽くして

待ち伏せ攻撃をかけた

共通鍵暗号が解読された

暗号化技術

共通鍵暗号方式

共通鍵暗号方式では、暗号化と復号で同じ鍵を利用する。

あらかじめ両者の間で鍵情報を共有しておく必要がある。

公開鍵暗号方式

公開鍵（暗号化）と秘密鍵（復号）の別の鍵が利用される。

受信者は、自分の秘密鍵で受け取った暗号文を復号すればよい。

公開鍵暗号方式（を考える）

公開する「暗号化鍵」と秘密に保持する「復号鍵」

↓

２つの別な鍵

鍵の開いた「南京錠」が「公開鍵」

南京錠を開錠する「鍵」が「秘密鍵」

暗号化と復号

受信者が公開

公開鍵を利用した暗号化は

世界中の誰でもできる

↓

復号できるのは

公開鍵とペアになる秘密鍵だけ

開ける鍵と閉める鍵が別の例

コインロッカーなど

ディジタル署名と認証局（ＣＡ）

送信者が公開

南京錠を開錠する「鍵」が「公開鍵」

署名を検証する鍵

鍵の開いた「南京錠」が「秘密鍵」

ＩＰＡ新試験へ対応

情報セキュリティマネジメント試験

情報セキュリティマネジメント試験とは

2016年春期より新たな試験区分として創設（ＣＣＳＦレベル２）

ITパスポート試験を合格した次のステップとして活用されることを想定

毎年春・秋の年２回実施

時間区分	午前	午後
試験時間	90分	90分
出題形式	四肢択一	多肢選択式
出題数	50問	3問

長文事例解析

ＩＴパスポート試験との比較

レベル１のITパスポート試験範囲と比較して、

セキュリティ・法務といった重点分野を中心に

更に掘り下げられた内容が出題される

↓

より高度なセキュリティ関連分野の知識が要求される

情報漏えい・サイバー攻撃に対応できる

人材育成を重視

定期考査結果より検証

「情報テクノロジ」の期末考査において、
情報セキュリティマネジメント試験の2016年度
春期と秋期午前問題からも一部出題した。

本試験でも60%の正答率で合格 → 60ポイントが目安

実際の出題①

春問14

PCで行うマルウェア対策のうち、適切なものはどれか。

正答率　76.9%

解答　イ

ウイルスがPCの脆弱性を突いて感染しないように、

OS及びアプリケーションの修正パッチを適切に適用する

マルウェア対策として

OSやアプリケーションの

最新の修正パッチを適用すること

は、CCSFレベルに関係なく

重要事項として出題される

実際の出題②

秋問27

ランサムウェアに分類されるものはどれか。

正答率　69.2%

解答　エ

感染したPCのファイルを暗号化し、

ファイルの復号と引換えに金銭を要求するマルウェア

IPA 情報処理推進機構　https://www.jitec.ipa.go.jp/

他の解答群

ア　感染したPCが外部と通信できるようプログラムを起動し、遠隔操作を可能にするマルウェア　ボットウイルス

イ　感染したPCに保存されているパスワード情報を盗み出すマルウェア　スパイウェア

ウ　感染したPCのキー操作を記録し、ネットバンキングの暗証番号を盗むマルウェア　キーロガー

実際の出題③

春問24

公開鍵暗号を利用した電子商取引において、

認証局（CA）の役割はどれか。

正答率　69.2%

解答　イ

取引当事者の公開鍵に対する

ディジタル証明書を発行する。

実際の出題④

秋問28

なりすましメールでなく、

EC(電子商取引)サイトから届いたものである

ことを確認できる電子メールはどれか。

正答率　69.2%

解答　ウ

ディジタル署名の署名者のメールアドレスのドメインが

ECサイトのものであり、署名者のディジタル証明書の

発行元が信頼できる組織のものである。

認証局（CA）の役割

ＣＣＳＦレベル１の共通・公開鍵暗号方式の

基礎知識の定着が、それらの応用技術である

PKI（公開鍵認証基盤）の仕組みの理解に繋がる。

実際の出題⑤

春問15

システム管理者による内部不正を防止する

対策として、適切なものはどれか。

正答率　57.7%

解答　ウ

システム管理者の作業を本人以外の者に監視させる。

IPA 情報処理推進機構 https://www.jitec.ipa.go.jp/

セキュリティ管理・運用分野

ＣＣＳＦレベル1の内部統制や監査の基礎知識や

経営者的視点の養成により対応可能である。

①～⑤の正答率

合格基準程度（６０%）の正答率が得られた

	① マルウェア 対策	② ランサム ウェア	③ 認証局の 役割	④ ＰＫＩの 仕組み	⑤ 内部不正 の防止
正答率	76.9%	69.2%	69.2%	69.2%	57.7%

（数問のみの結果からでは完全ではない部分もあるが）

ＩＴパスポート試験対応の授業内容が

情報セキュリティマネジメント試験の
午前問題にも対応可能である

午後問題

実際に起こった情報漏えい等に類似した事例解析が中心

春午後問1

情報セキュリティインシデントの管理に関する記述を読んで、

標的型攻撃メールの実際の脅威と具体的な対策を選ぶ設問　11問

内容的に高校生には難易度は高いが

ITパスポート試験の早期合格者数名は６０%程度正解

→　午後問題対策としても対応可能である

サイバーセキュリティ
人材確保加担の第一歩

ITパスポート試験の早期合格者（今年度既に2名）に対して

情報セキュリティマネジメント試験の

受験を積極的に推奨することで

試験勉強を通して知識を確実に定着できる。

↓

今後は

更に上位試験である 情報処理安全対策支援士 まで

視野に入れた施策を検討していく必要あり

２０２０年　東京五輪開催を控え

サイバー攻撃の恰好のターゲットとなる機会の増大は確実

実際、2012年ロンドン五輪期間中は

2億件超えのサイバー攻撃が確認されている

↓

情報セキュリティマネジメント試験に合格した高校生に対して、

（その後も見据えて）

更なる学修が求められることは容易に予想できる。

情報処理安全確保支援士

2016年10月創設　CCSFレベル4

通称：登録セキスペ

「情報セキュリティスペシャリスト試験」

を独立させ、別制度として資格試験を新設。

合格者はIPAに申請・登録する事により

情報処理安全確保支援士と成ることが出来る

サイバーセキュリティ分野初の
登録制の国家資格

「情報処理安全確保支援士」集合研修　配布資料　2017.8.5

情報セキュリティマネジメント試験との比較

情報セキュリティマネジメント	情報処理安全確保支援士
CCSFレベル２	CCSFレベル４
組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを有する	情報セキュリティ技術の専門家として、セキュアな情報システムを企画・要件定義・開発・運用・保守する

情報セキュリティマネジメント試験との比較

情報セキュリティマネジメント	情報処理安全確保支援士

CCSFレベル２

CCSFレベル４

２０２０年　東京五輪開催を控え

2016年4月 改正サイバー法が成立し

NISCの機能強化が盛り込まれた

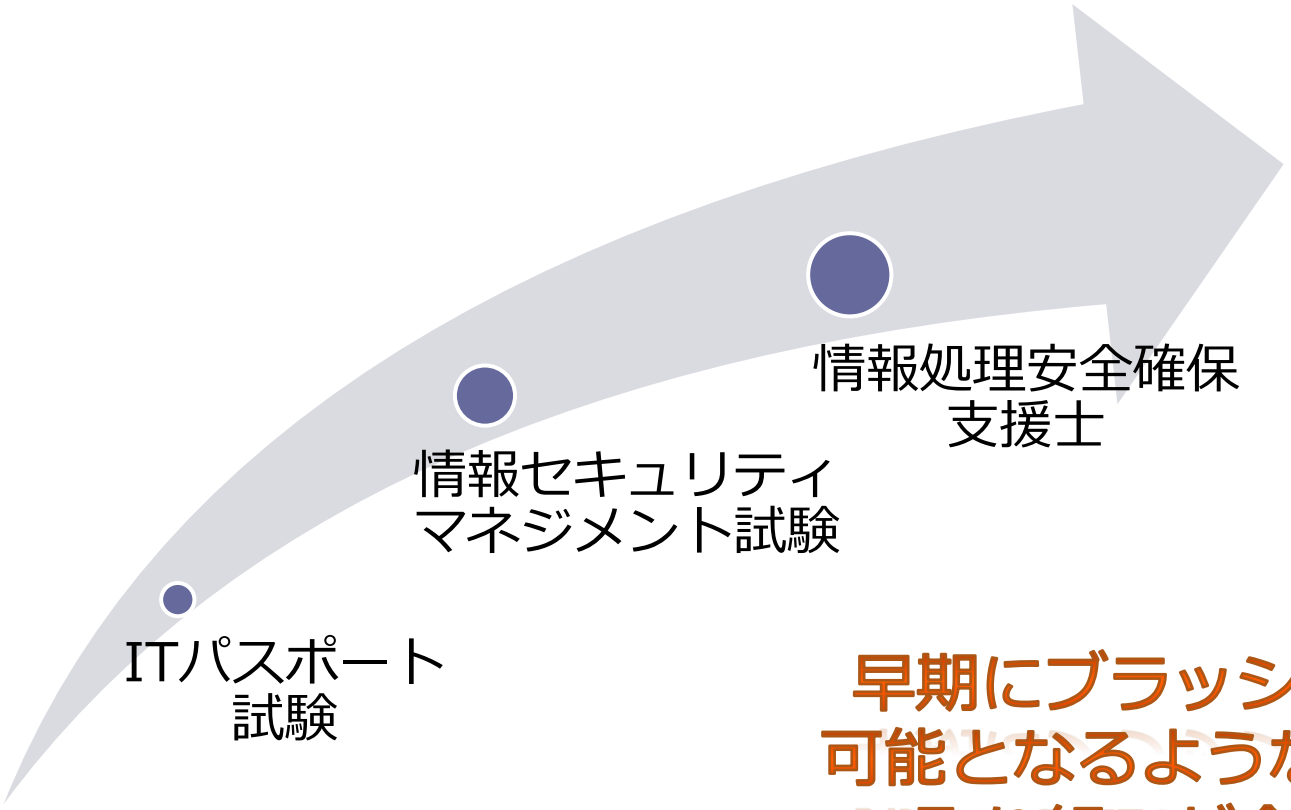
↓

サイバーセキュリティに関する

専門的な知識・技能を有する専門人材の

育成と確保のため国家資格化

東京五輪に向けて



早期にブラッシュアップが可能となるような人材育成の取り組みが今後の課題

今後必要とされる
セキュリティ人材育成計画

今後必要とされる
セキュリティ人材育成計画

政府各省庁でも各々

セキュリティ人材育成施策を策定している。

↓

特に高校の情報教育では、

橋渡し役としてのセキュリティ人材教育

が求められる

今後必要とされる
セキュリティ人材育成計画

① 高等教育機関との連携による系統的なスキル習得

② サイバー対策を踏まえたプログラミング教育

③ 産学官連携による実践的演習の充実

３つの方向性が求められると考える

①　系統的なスキル習得

早期（できれば入社まで）に

情報処理安全確保支援士の有資格者へ

ブラッシュアップ

が可能となるような人材スキル習得の系統化が必要

系統的なスキル習得

情報セキュリティに関連した二つの国家試験

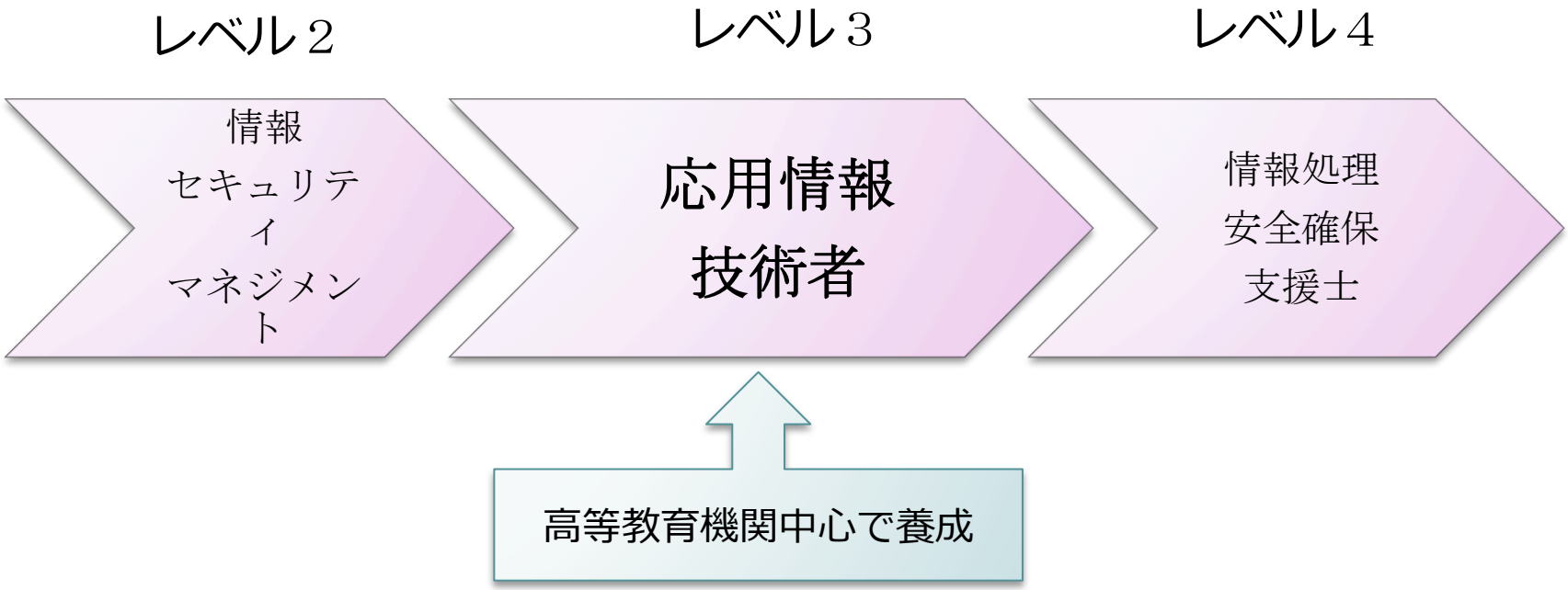
「情報セキュリティマネジメント試験」

「情報処理安全確保支援士」

の間には、CCSFレベル3である

「応用情報技術者試験」が存在する。

系統的なスキル習得


レベル２
レベル３
レベル４
情報セキュリティマネジメント
応用情報技術者
情報処理安全確保支援士
高等教育機関中心で養成

情報処理技術者試験の活用（大学）

情報処理技術者試験を活用している大学・短大は全国で344校

（2016年度）

応用情報技術者試験のシラバスを参考とした

カリキュラムを取り入れている理工・情報系学部

↓

ITパスポート試験等の合格者に対する入試優遇や入学後の単位認定

大学側も、高大連携したスキル習得の系統化を求めている

情報処理技術者試験の活用（大学）

活用内容	大学数
情報処理技術者試験を活用している大学	344校
・入試優遇	228校
・単位認定	106校
・シラバスの一部又は全部を参考とした 授業カリキュラムの策定	93校
・受験対策支援講座の実施	151校
・受験を推奨 （受験料補助、合格者の表彰、報奨金等支給）	132校

2016年12月21日現在

https://www3.jitec.ipa.go.jp/JitesCbt/index.html

系統的なスキル習得

高校：ＣＣＳＦレベル１、２

ＩＴパスポート試験　／　情報セキュリティマネジメント試験

↓

大学・専門学校：ＣＣＳＦレベル３

応用情報技術者試験（基本情報技術者）

↓

就職前まで（または就職後早期）

情報処理安全確保支援士

②　サイバー対策を踏まえたプログラミング教育

2020年度から小学校におけるプログラミング教育が必修化

コンピュータ技術の原理や思考方法などを学ぶ事で、

問題解決のための手順を順序立てて明確に出来る

「論理的思考力」や「問題解決能力」の向上を目指す

↓

特定のプログラム言語の習得には踏み込まない

「サイバー攻撃対策の手段」として

言語習得の需要が高まる と考えている

マルウェアに代表される不正プログラムの

コード解析により相手の手口を知る

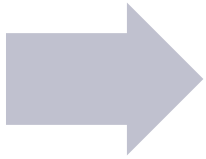
『攻撃の可視化』

が、より効果的な対策を考える第一歩に繋がる

不正プログラムのコード解析

プログラミング

- 問題解決力の向上



不正プログラムのコード解析

- サイバー攻撃対策の手段

脆弱性があるプログラム例（C言語）

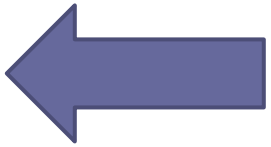
```
15: int main(int argc, char **argv)
16: {
17:     static char *uid;
18:     static char *pass;
19:     (省略, 引数の個数をチェック)
20:     uid = new char[UID_SIZE+1];
21:     pass = new char[PASS_SIZE+1];
22:     getPass(pass, argv[1]);
23:     strcpy(uid, argv[1]);
24:
25:     if (strlen(pass) == 0 || strcmp(argv[2], pass) != 0) {
26:       cout << "認証失敗" << endl;
27:        (省略, uid を出力, 認証失敗時の処理)
28:     } else {
29:       cout << "認証成功" << endl;
30:        (省略, uid を出力)
31:     }
32: }
```

出典

IPA 情報セキュリティスペシャリスト試験
H２８秋　午後Ⅰ問２
https://www.jitec.ipa.go.jp

バッファオーバーフローの脆弱性

```
20:     uid = new char[UID_SIZE+1];
21:     pass = new char[PASS_SIZE+1];
22:     getPass(pass, argv[1]);
23:     strcpy(uid, argv[1]);
```



ヒープベースＢＯＦの
脆弱性

不正な uid、passを入力する事で

利用者認証を回避することが可能になる

③ 産学官連携による実践的演習の充実

ＮＩＳＣの「サイバーセキュリティ2016」の

横断的施策の一つ

実践的サイバー防御演習（CYDER）等を

通じたサイバー人材育成

産学関係機関との協力体制の整備を推進

実践的演習の充実を目指す

実践的サイバー防御演習（CYDER）

標的型攻撃によるインシデントの検知から

対応、報告といったインシデントハンドリング

を一連の流れで体験

↓

実際の機器やソフトウェア等利用した

未知の攻撃によるインシデント発生を想定した訓練

（参考）

「情報処理安全確保支援士」

資格維持集合研修（H29.8.5)

ＩＰＡ・内田洋行人材開発センター主催

グループワークによるケーススステディ

- インシデント対応
- 予防策の検討

初等中等教育機関では

実際に手を動かして学ぶ機会を増やす教育が必要とされると考える

Wire shark ・コマンド等によるパケット解析含

企業等との連携が必要　今後詳細等調査予定

↓

特にタブレット端末やスマートフォンの急激な普及により

逆に扱う機会が減ったキーボードを利用した

『タイピング力』など、重要な要素の一つになる

ICTプロフィシエンシー試験（Ｐ検）

タイピング　３０％以上

かつ

一般問題 及び

Ｗｏｒｄ・Ｅｘｃｅｌ　６０％以上

の得点で合格（４級）

H28 １年次Ｐ検（４級）結果より

受験者　１０１名　合格率　８４．２％

不合格者のうち

タイピングのみの不合格　９３．８％

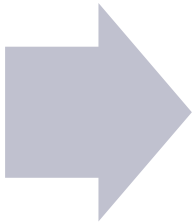
↓

タブレット端末やスマートフォンの急激な普及により

キーボードを扱う機会が減っている

実践的演習の充実のために

アンプラグド



実機で
手を動かす

タイピング力も
重要な要素の一つ

今後必要とされる
セキュリティ人材育成（まとめ）

① スキル習得の系統化

→ （高大連携による）ＣＣＳＦレベル３の定着

② プログラミング教育

→ （不正プログラムなどの）コード解析力の養成

③ 実践的演習の充実（産学連携による）

→ タイピング力の強化

各人材育成施策への橋渡し役としての情報教育

ご清聴感謝いたします