経済産業省
Ministry of Economy, Trade and Industry

資料３

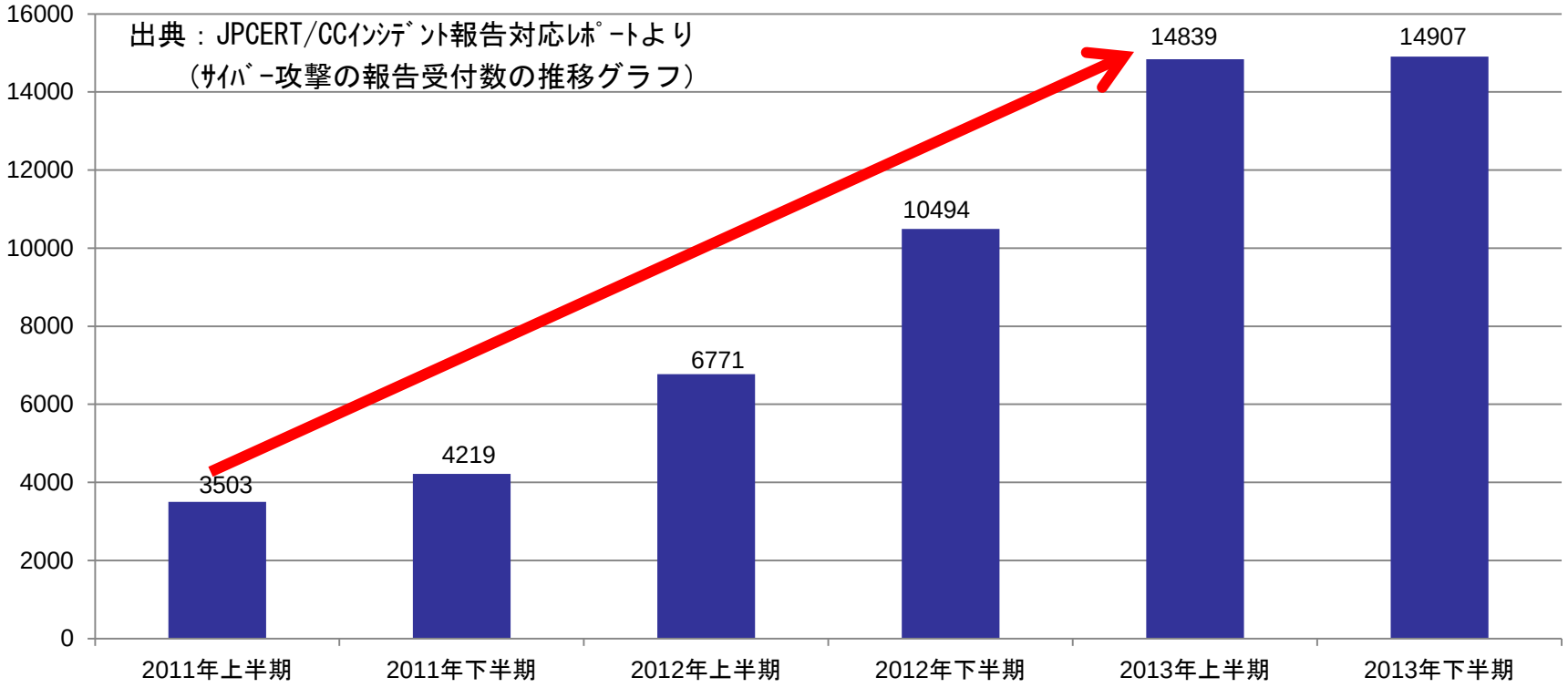
情報セキュリティ分野の人材ニーズについて

平成２７年３月
情報処理振興課

１．情報セキュリティに係る現状

1. 情報セキュリティに係る現状（サイバー攻撃①）

- この１年間で、我が国に対するサイバー攻撃件数は２倍以上に急増。
- IT空間の拡大とともに、サイバー攻撃は巧妙化し、脅威も増大。
  - → 発電所や化学プラント等の重要インフラを狙うサイバー攻撃の脅威
  - → 政府機関や企業の機密情報を狙う標的型サイバー攻撃の増加
  - → スマートフォンやタブレットなどネットワークにつながる機器はどれも標的に
- 個人から重要インフラまで、あらゆる分野に対しての攻撃が増加。今後、早急に対処しないと、被害が連鎖的に拡大し、我が国の産業基盤や個人の生活基盤が著しく損なわれるおそれ。



1．情報セキュリティに係る現状（サイバー攻撃②）

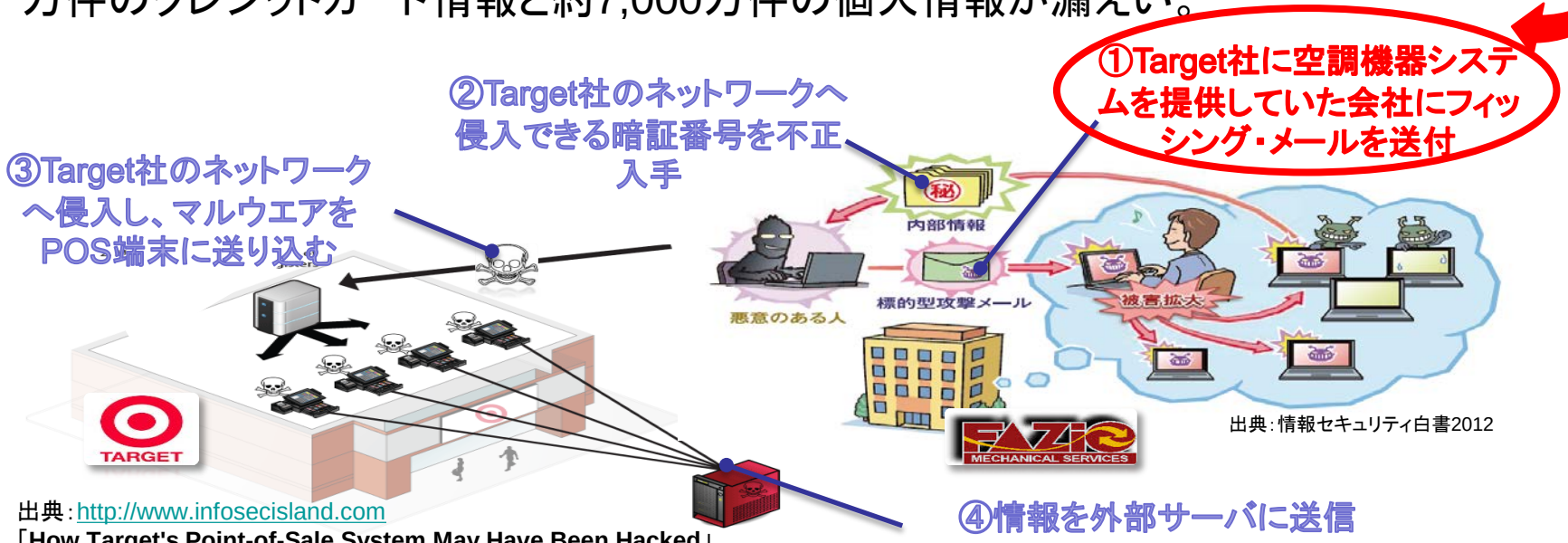
◆ 近年、標的型サイバー攻撃の手口は更に巧妙化しており、従来型ウイルスのような未然防止可能な攻撃ではなくなっている。

◎最新の標的型サイバー攻撃事例

対象を直接、攻撃するのではなく、<u>まず関連システム会社を攻撃し、</u>攻撃対象のネットワークに侵入。

≪米Target Corporation（2013年12月）の事例≫

米売上高第5位の小売業者であるTarget社のPOS端末を狙った攻撃により、4,000万件のクレジットカード情報と約7,000万件の個人情報が漏えい。



出典：情報セキュリティ白書2012

出典：http://www.infosecisland.com
「How Target's Point-of-Sale System May Have Been Hacked」

注）Target社システムのセキュリティを常時監視していた、米FireEye社はネットワークに何者かが侵入していることをTarget社に警告。しかしながら、Target社は速やかな対応ができず、顧客データの流出が続いた。後日、経営層の経費削減という方針により、セキュリティ上の脆弱性を何年も放置していたことが判明。
出典：日経ビジネスオンライン「セキュリティ対策はコストではない～米国で起きた「ターゲットの悲劇」の教訓～」
http://business.nikkeibp.co.jp/article/opinion/20140604/266189/?rt=nocnt

1．情報セキュリティに係る現状（サイバー攻撃③）

◆ 巧妙化したサイバー攻撃に対応するため、情報セキュリティ製品も進化している。一方で、情報セキュリティに関するリスクを認識し、情報セキュリティ製品を適切に活用しなければ速やかな対策が出来ない。

◎最新のセキュリティ対策事例

仮想環境上で、怪しいファイルを実行し、マルウェアかどうかを検知。

≪米FireEye社、サンドボックス技術≫

（概要）

仮想環境上でいったんファイルを実行し、実行後の振る舞いをチェックしてマルウェアかどうかを検知する技術。

検知したマルウェアを自動除去するにはオプション契約が必要。

注）Target社は未契約だったため、除去は手動運用であったため、対策に時間を要した。

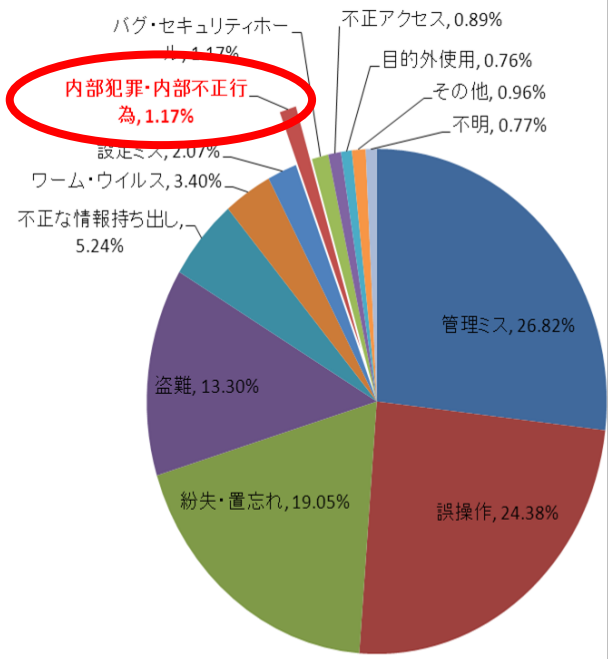
出典：@IT「企業を狙う標的型攻撃――その手口と抜本的な対策とは」

1．情報セキュリティに係る現状（内部不正管理①）

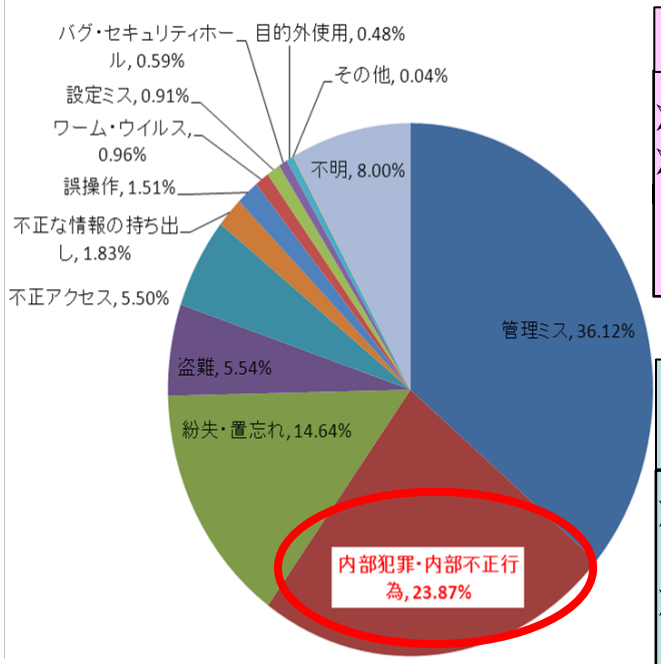
◆ 組織内部者による個人情報漏えいは、外部からの攻撃によるものに比較し、被害規模が大きくなる傾向にある。また、営業秘密が持ち出され、競合企業に漏えいした場合、その損害は多大なものとなる。

内部犯行等による**被害件数は全体の1%**程度であるが、**個人情報漏えい件数で見ると、内部犯行等によるものは全体の約24%**を占める。

原因別インシデント件数の割合



原因別個人情報漏えい件数の割合



ベネッセHDの事例※1

- 顧客情報約3,500万件漏えい
- 補償等の対策費用として約310億円の特別損失を計上

＝＞上場以来初の赤字に

内部からの営業秘密持ち出しに係る損害賠償請求の事例※2

- 新日鐵住金 がポスコ（韓）に対し約1,000億円の賠償請求中
- 東芝がSKハイニックス（韓）に対し約1,100億円の賠償請求中

出典：2005年～2010年情報セキュリティインシデントに関する調査報告書（NPO日本ネットワークセキュリティ協会（JNSA））を基にIPAが作成

※1 ベネッセ、上場以来初の赤字に…情報流出対策で（読売新聞 2014年10月31日）
http://www.yomiuri.co.jp/economy/20141031-OYT1T50113.html?from=ytop_main7

※2 産業構造審議会 知的財産分科会 営業秘密の保護・活用に関する小委員会（第1回）- 配布資料5 （経済産業省）
http://www.meti.go.jp/committee/sankoushin/chitekizaisan/eigyohimitsu/pdf/001_05_00.pdf

1．情報セキュリティに係る現状（内部不正管理②）

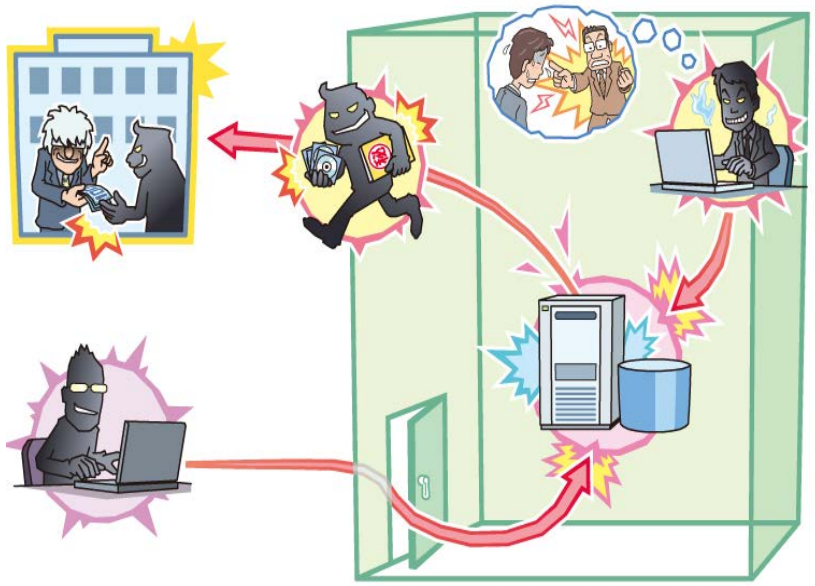
- ◆ 組織内部の権限を持つシステム管理者等の職員や社員が悪意を持てば、攻撃を実行することは容易であり、組織にとって大きな脅威となる。
- ◆ 管理者には、ログの記録や定期監査を行い、不正行為の抑止や早期発見を可能とする社内体制を整備する等の対策が求められる。

主な事例

①委託先社員による個人情報漏えい《2014年7月》
　ベネッセHDの顧客情報に関するデータベースの運用や保守管理を行っていた委託先社員（当時）が同社の管理する個人情報を名簿業者に売却。最大で約3,500万件の個人情報が漏えい。

②委託先社員によるカード偽造《2014年2月》
　株式会社横浜銀行のATMの保守管理業務を請け負っていた富士通フロンテック株式会社の社員（当時）が、ATMの取引データから顧客のカード情報を不正に取得し、2012年5月から2013年10月の期間に、48口座から計2,400万円を引き出し。

③職員による不正アクセス《2013年9月》
　大阪市の職員が上司や同僚の個人ID・パスワードを不正に使用して庁内情報ネットワークにアクセス。



出典：情報セキュリティ白書2014から抜粋

（参考）内部不正ガイドラインの強化

- 2014年9月に、今般の内部不正による事故・事件等を受け、IPAは「組織における内部不正防止ガイドライン※」を改訂。
- 具体的には、**経営層によるリーダーシップの強化、情報システム管理運用の委託における監督強化、高度化する情報通信技術への対応**等の改訂が行われた。

※内部不正のリスクを低減するために、経営者が果たすべき役割、組織の体制、技術対策などが記載されており、IPAより2013年3月に初版を公開。内部不正対策に必要な30の項目を定めており、チェックシートや対策のヒントとなるQ＆A、内部不正事例集を収録。

IPA 「組織における内部不正防止ガイドライン」

改訂のポイント

【経営層によるリーダーシップの強化】
- 経営層の責任の明確化
- 責任者・担当者の能力確保

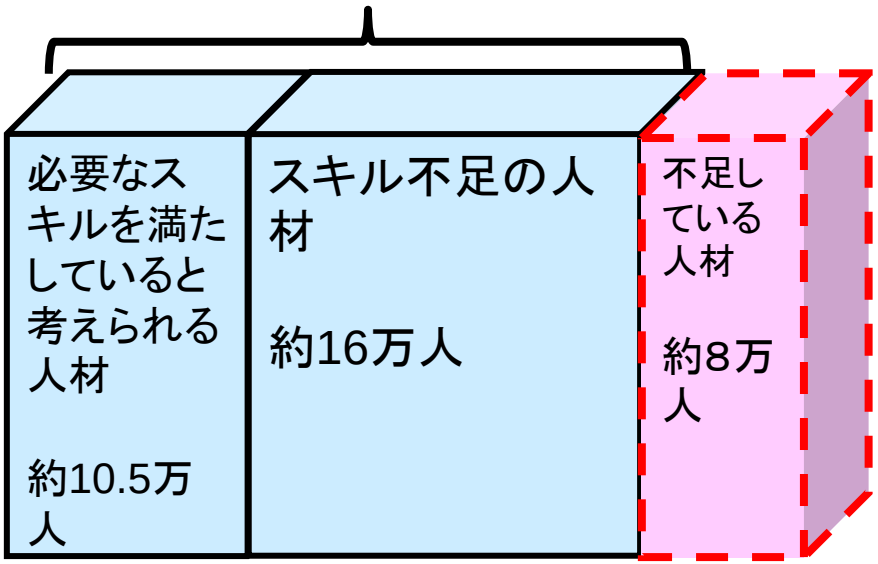
【情報システム管理運用の委託における監督強化】
- システム業務体制の検討
- 業務委託先の評価・監督
- 委託元と委託先の連携

【高度化する情報通信技術への対応】
- 継続的な対策見直し
- スマートデバイス等への対応
- アクセス権限管理強化
- ログ確保による抑止

（参考）情報セキュリティに係る人材の不足状況

- ◆ しかし、IPAの試算によれば、国内のユーザー企業において、情報セキュリティ人材は大幅に不足（約8万人の不足）。
- ◆ 特に情報関連以外の製造業や卸売業・小売業、医療・福祉等のユーザ業種における人材不足が顕著。

国内のユーザー企業において
情報セキュリティに従事する技術者
約26.5万人



＜IPA試算:「情報セキュリティ人材育成に関する基礎調査」の人材不足数に関する追加分析による。H24調査→H26追加分析。＞

約8万人の業種別内訳

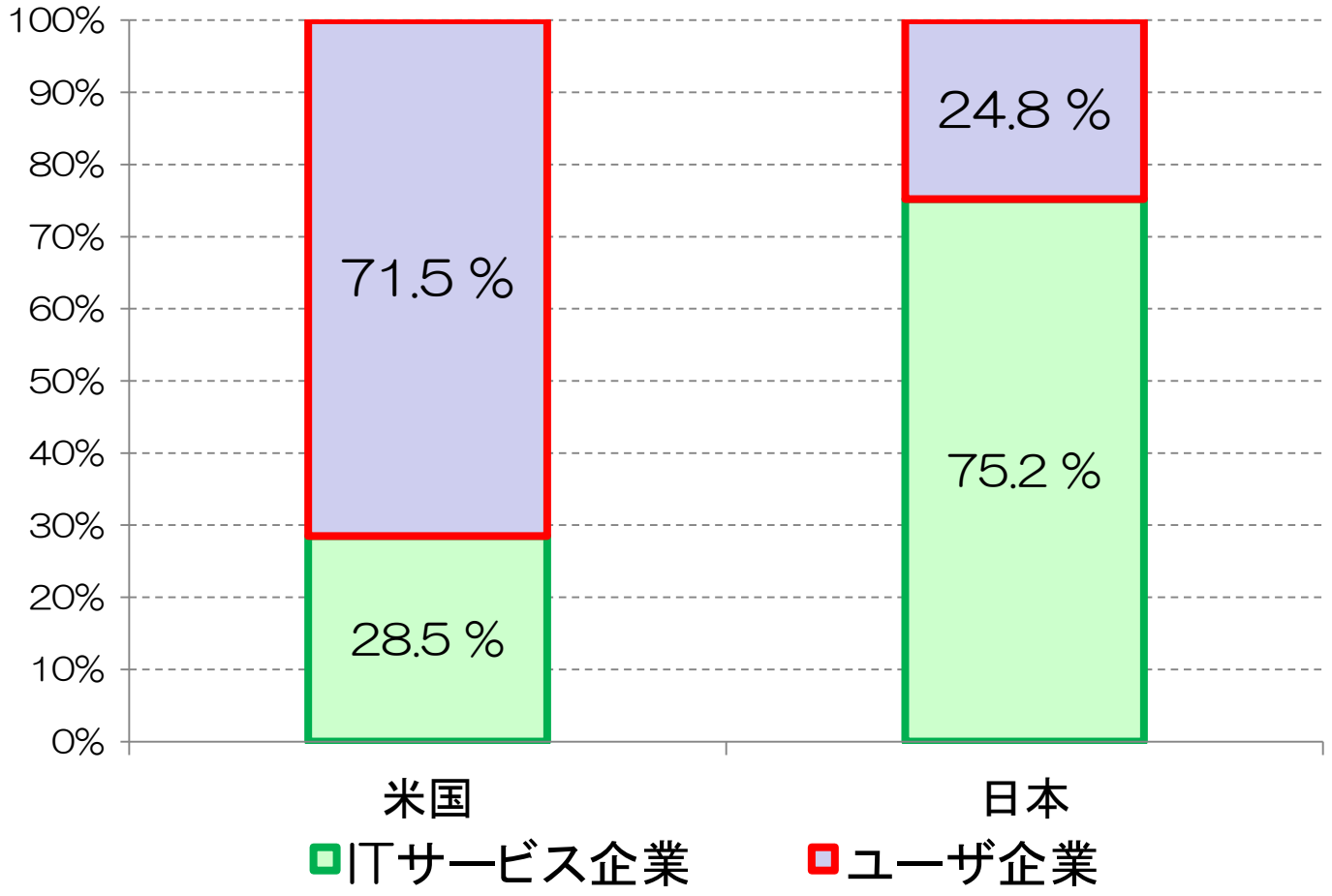
（人）

業種	不足数
農林業・水産業・鉱業	256
建設・土木・工業	2,764
電子部品・デバイス・電子回路製造業	1,403
情報通信機械器具製造業	605
電気機械器具製造業	1,158
その他製造業	15,853
電気・ガス・熱供給・水道業	81
通信業	683
情報サービス業	1,885
その他の情報通信業	1,717
運輸・郵便業	6,718
卸売業・小売業	14,480
金融業・保険業	4,957
不動産業・物品賃貸業	1,547
学術研究・専門技術者	1,014
宿泊業・飲食サービス業	3,535
生活関連サービス業・娯楽業	3,301
教育・学習支援業	2,084
医療・福祉	8,473
複合サービス業	614
その他サービス業	8,462
計	**81,590**

（参考）IT人材が属する分野の日米比較

◆ 米国はユーザ企業側にIT技術者が多いが、逆に日本はユーザ企業側にIT技術者が非常に少ない状況。

日米のIT技術者の分布状況

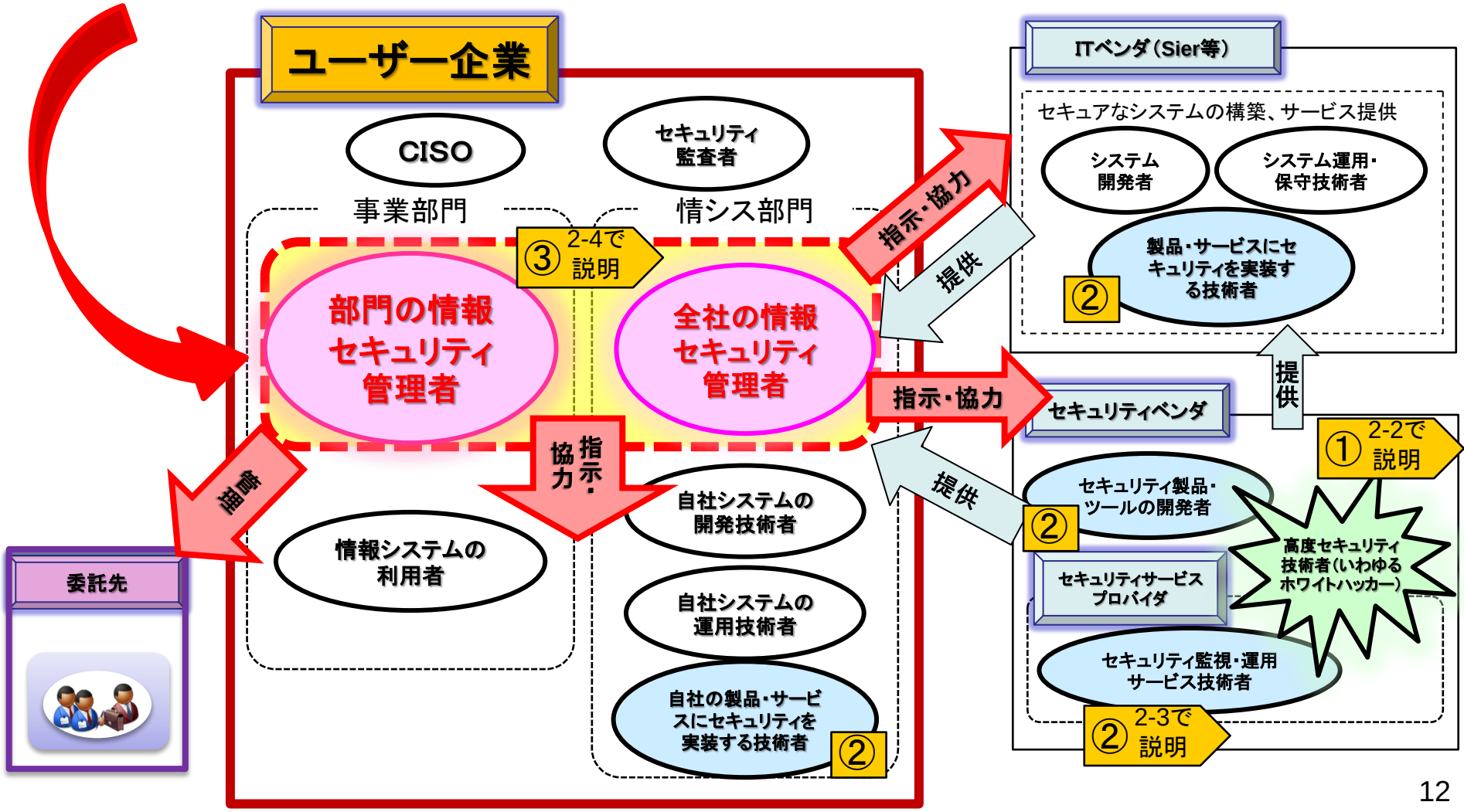


出典：米国労働省 労働統計局統計資料、
NASCOMM、アジア情報化レポート、IPA IT人材白書2010 等

２．今後必要となるセキュリティ人材

2. 今後必要となるセキュリティ人材像

◆ 今後必要となるセキュリティ人材は、①ホワイトハッカーのような高度セキュリティ技術者、②安全な情報システムを作るために必要なセキュリティ技術を身につけた人材、③ユーザー企業において、社内セキュリティ技術者と連携して企業の情報セキュリティ確保を管理する人材。

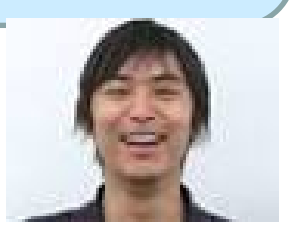


2-2.ホワイトハッカーの育成（セキュリティ・キャンプ）

○若年層のセキュリティ人材を発掘し、世界に通用する善意のトップクラス人材（ホワイトハッカー）を創出するため、IPAが民間企業と連携して、若年層セキュリティ人材（22歳以下）の育成合宿（セキュリティ・キャンプ）を平成16年度から実施。倫理面も含めたセキュリティ技術と、最新のノウハウを、第一線の技術者から若手に伝授する場を創出。これまで約4百名が受講（平成26年度時点）。
○最近ではキャンプ修了者から女性だけのセキュリティコミュニティ発足の動きも出ている。

石森 大貴（いしもり　だいき）**さん**（2007年修了生 24歳（1990年生））
高校時代にセキュリティ・キャンプに参加、その後、擬似ハッキングによる脆弱性診断や官公庁や企業へのセキュリティコンサルを行ない、そこからセキュリティ専門会社のゲヒルンを起業し、現在、代表取締役を務める。このゲヒルンは、社員数わずか十数名ながら高いセキュリティ診断技術ゆえに金融機関などの大手企業からの依頼を多く手掛けている。

丑丸 逸人（うしまる　はやと）**さん**（2010年修了生 25歳（1989年生））
2013年8月、米国で開催された世界最高峰のハッカーコンテストである「DEFCON21 CTF(Capture The Flag)」本戦に参加。ソフトウエアを解析して脆弱性を見つけ出すハッカーとして、日本のチーム「ｓｕｔｅｇｏｍａ２」が全20チーム中6位にランクインする快挙を成し遂げることに貢献した。セキュリティ対策企業でも活躍。
「日本を守る「七人の侍」ーホワイトハッカー、インスペクター、ゲートキーパー（2013/10/03 日経コンピュータ）」で紹介される。



セキュリティ・キャンプが輩出したホワイトハッカー

キャンプ修了生同志の交流を促進

最先端で活躍する技術者を講師として招へい

講師

セキュリティ・キャンプ

若いサイバーセキュリティ人材の発掘と育成

IPA ← 官民連携による推進 → セキュリティ・キャンプ実施協議会

尖った人材がキャンプに参加

2-3. 必要な人材像（セキュリティ技術者）

◆ 安全な情報システムの構築やサービスを実現するために専門的なIT技術者については、従来から情報処理技術者試験において情報セキュリティ分野を専門とする情報セキュリティスペシャリスト試験を実施。

情報セキュリティマネジメント人材
（情報セキュリティを利用者側の現場で管理する者）

2-4で説明

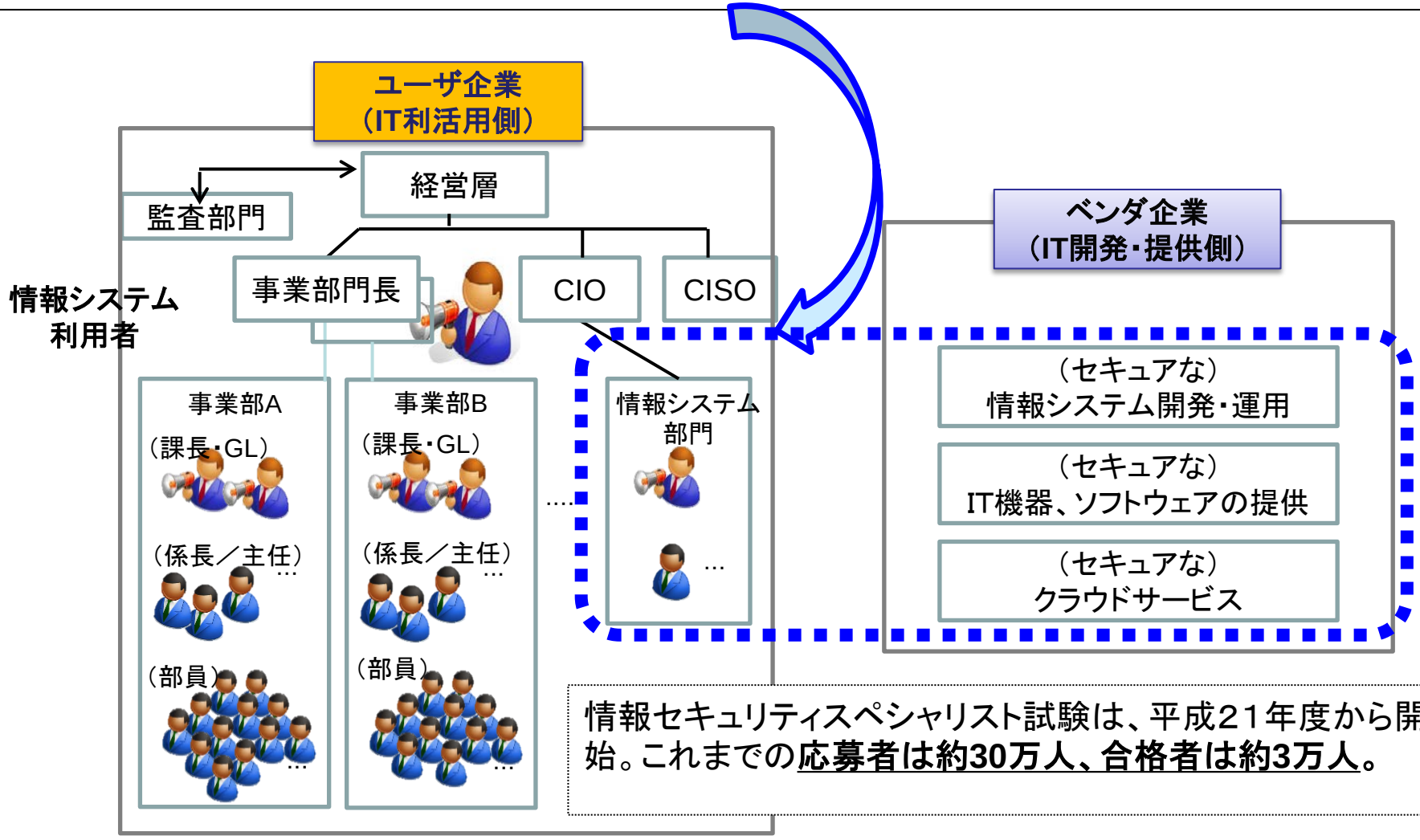
連携して
情報セキュリティ対策を実施

情報セキュリティスペシャリスト人材
（安全な情報システムを作る者）

（典型的な人材像：セキュリティ技術者）
情報セキュリティ分野を専門とするIT技術者であり、**情報システムのセキュリティ機能を実装し、**また、**情報セキュリティ技術の専門家として情報セキュリティ管理を支援する。**

（参考） 情報セキュリティスペシャリスト試験について

◆ 情報セキュリティスペシャリスト試験は、情報セキュリティに従事する技術者（ベンダ企業やユーザ企業の情報システム部門においてセキュリティ技術を専門とする人材）（対象者は青枠）を対象に実施。



情報セキュリティスペシャリスト試験は、平成21年度から開始。これまでの**応募者は約30万人、合格者は約3万人**。

2-4. 必要な人材像（ユーザ企業のセキュリティ管理者）

◆ 今後必要となるセキュリティ人材のうち、育成が十分になされていないのは、ユーザー企業において、一定の技術知識を持ちつつ、自社内で情報セキュリティ対策の実務をリードできるマネジメント人材。

情報セキュリティマネジメント人材

（情報セキュリティを利用者側の現場で管理する者）

様々な機密情報を、
各重要度やリスクを踏まえて
管理できる

情報セキュリティ上の
トラブルが発生した際に、
適切な事後対応が取れる

情報漏えい等を
防止するための
ルール作りができる

メンバに対して
情報セキュリティの重要性を
教育できる

業務を委託する際、
委託先における
情報セキュリティ対策の
実施状況を確認し指導できる

情報システムを調達する際、
必要な情報セキュリティ要件を
まとめられる

連携して
情報セキュリティ対策を実施

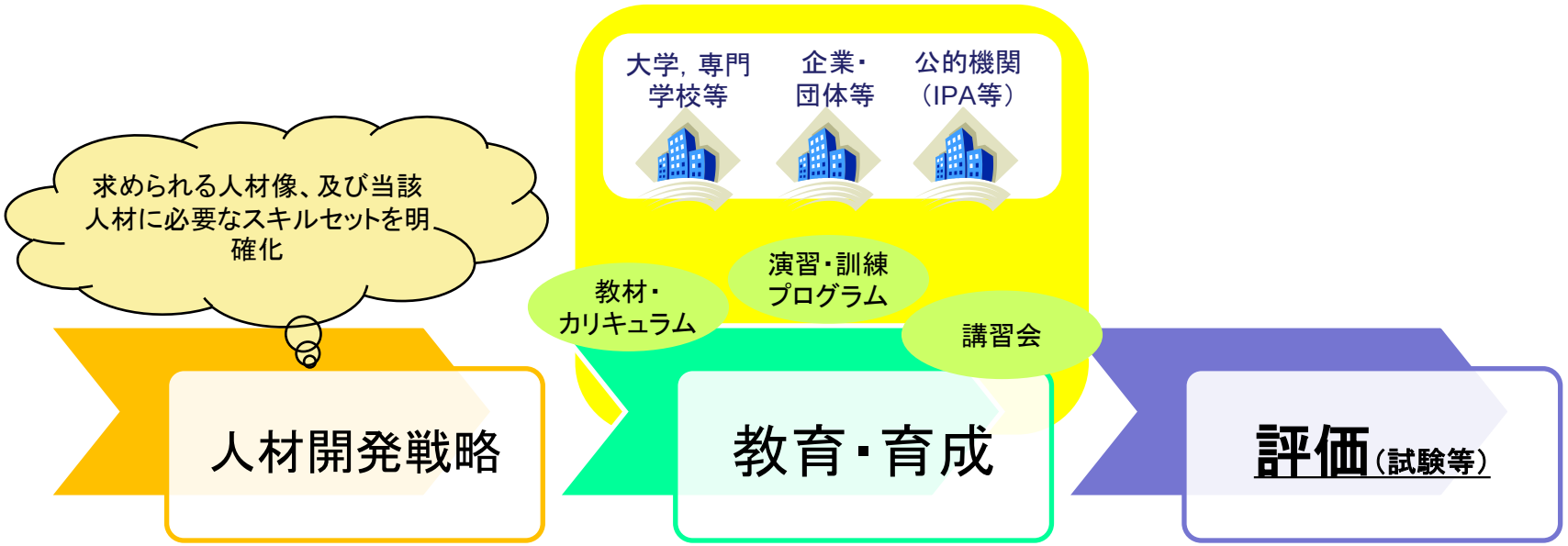
（典型的な人材像：業務部門セキュリティ管理者）
業務部門において、普段は総務や企画等を担当しつつ、情報セキュリティトラブルの発生時には部門長やセキュリティ技術者と連携して被害の最小化を図る。

（参考）
情報セキュリティスペシャリスト人材
（安全な情報システムを作る者）

（典型的な人材像：セキュリティ技術者）
情報セキュリティ分野を専門とするIT技術者であり、情報システムのセキュリティ機能を実装し、また、情報セキュリティ技術の専門家として情報セキュリティ管理を支援する。

2-5. 情報セキュリティマネジメント人材の育成方法

- ◆ 社内での経験を通じて一定のマネジメント能力を有する人材に対して、基本的な情報セキュリティ関連のスキルを身につけさせることが必要。
- ◆ 情報セキュリティマネジメント人材に必要なスキルセットを明確化して、教育コンテンツ・人材育成プログラム等の整備を促進。
- ◆ 教育・人材育成の成果のうち「知識」レベルを客観的に測定・評価（「見える化」）するための情報セキュリティマネジメントに関する試験が必要となる。

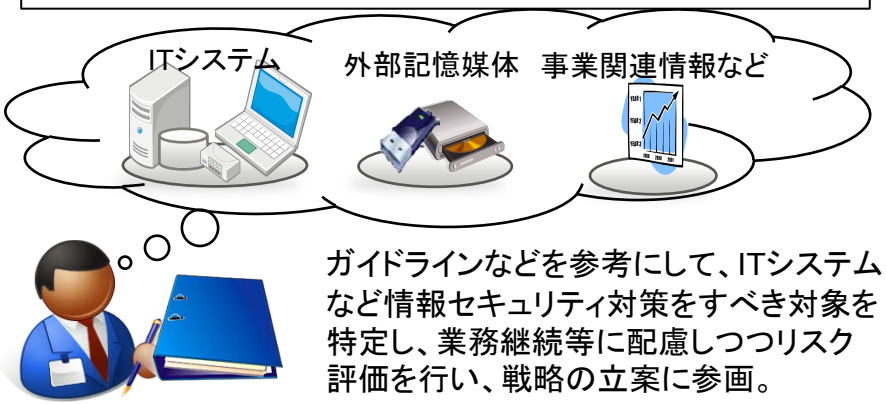


（課題）
情報セキュリティスペシャリスト人材の育成については試験をはじめ研修・教材等の環境が充実しているが、 情報セキュリティマネジメント人材の育成環境は整備できていない。

3.　情報セキュリティマネジメント試験（仮称）に求められる内容

◆ 情報セキュリティマネジメント試験（仮称）を通じて確認する、情報セキュリティマネジメントを行う上で最低限必要な「知識」内容は以下のとおり。

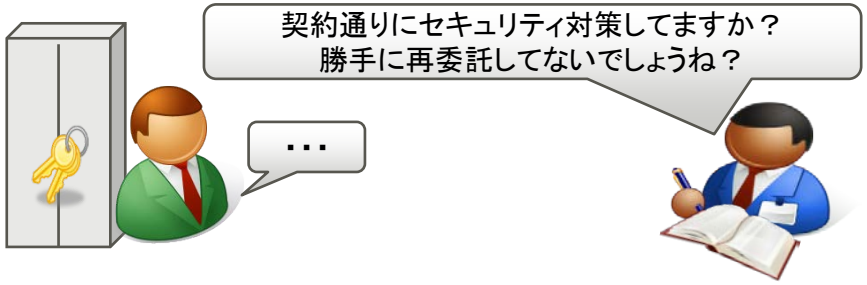
1. 情報セキュリティマネジメントの計画、情報セキュリティ要求事項に関すること



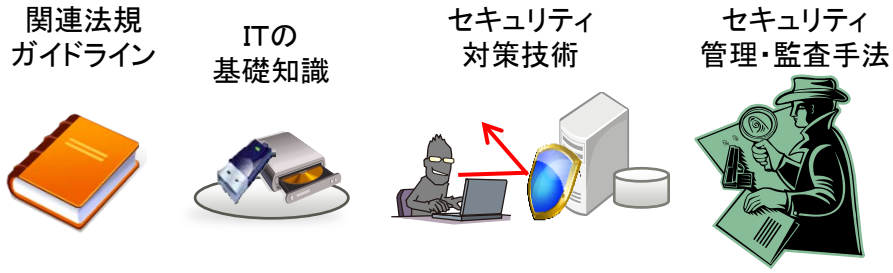
ガイドラインなどを参考にして、ITシステムなど情報セキュリティ対策をすべき対象を特定し、業務継続等に配慮しつつリスク評価を行い、戦略の立案に参画。

2. 情報セキュリティマネジメントの運用・継続的改善に関すること

3. 外部委託、コンプライアンス（遵守指導等）に関すること



4.（上記1～3の前提となる）情報セキュリティマネジメントの基礎知識に関すること



参考資料

参考：情報セキュリティスペシャリスト試験の概要

情報セキュリティスペシャリスト試験とは・・・

・標的型サイバー攻撃の増加
・新手の不正アクセス
・新型ウィルスの出現

脅威

専門家による適切なセキュリティ管理が必要

機密盗難・機器停止の恐れ（企業の損失拡大の恐れ）

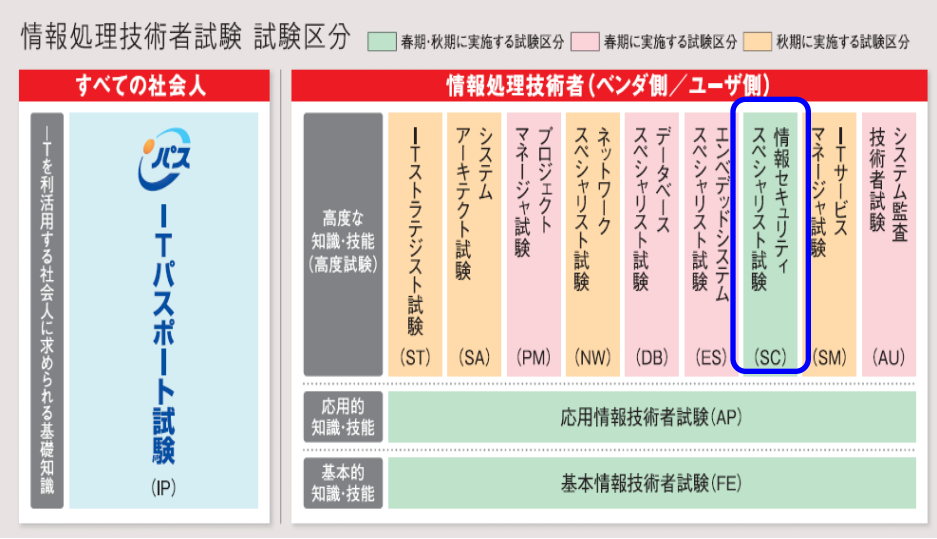
国家試験による評価

セキュリティの専門家を評価する国家試験

【対象者像】

高度IT人材として確立した専門分野をもち、情報システムの企画・要件定義・開発・運用・保守において、情報セキュリティポリシに準拠してセキュリティ機能の実現を支援し、又は情報システム基盤を整備し、情報セキュリティ技術の専門家として情報セキュリティ管理を支援する者

【情報処理技術者試験における位置づけ】



【情報セキュリティスペシャリスト試験の応募者数等（直近3年分）】

	平成25年度	平成24年度	平成23年度
応募者数	56,452	57,944	57,243
（全体に占める応募者割合）	(12.0%)	（11.9%）	(9.9%)
合格率	13.9%	13.8%	13.7%

【出題範囲（午後）】

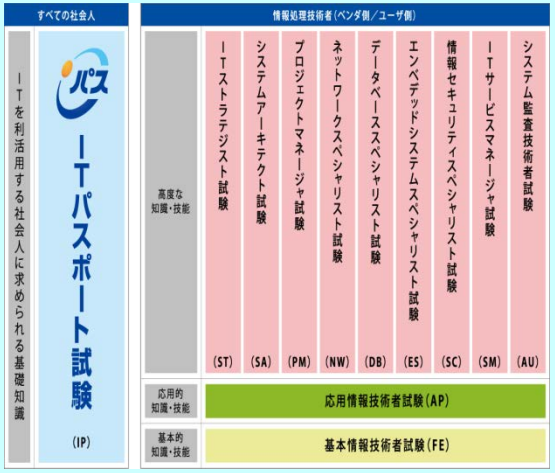
○情報セキュリティシステムの企画・要件定義・開発・運用・保守に関すること（セキュアプログラミングなど）
○情報セキュリティの運用に関すること（不正アクセス対策など）
○情報セキュリティ技術に関すること（ウイルス対策技術など）
○開発の管理に関すること（開発環境の情報セキュリティ管理など）
○情報セキュリティ関連の法的要求事項などに関すること（著作権法、個人情報保護など）

（補足）情報処理技術者試験における情報セキュリティ出題強化

＜背景＞　○ 情報セキュリティの重要性の一層の高まり
　　○ 情報セキュリティ人材の量的・質的な不足

- ✓ 情報セキュリティに関する知識を含め、国民全体のITリテラシーの向上を図ることが必要
  （世界最先端IT国家創造宣言　※ 2013年6月14日閣議決定）
- ✓ 情報セキュリティ人材の発掘、育成、活用を進めることが必要
  （サイバーセキュリティ戦略　※ 2013年6月10日政府公表）

「iパス」をはじめとする情報処理技術者試験の全試験区分において、「情報セキュリティ」に関する出題の強化・拡充を実施



iパス	◆ 情報セキュリティに関する出題比率の大幅な引き上げ（2倍）
基本情報技術者試験（FE） **応用情報技術者試験（AP）**	◆ 午前試験において「中分類11 セキュリティ」の出題比率を引き上げ ◆ 午後試験において「情報セキュリティ分野」を　選択問題から必須問題に変更
高度試験	◆ 午前Ⅰ試験（共通知識）、午前Ⅱ試験において「中分類11 セキュリティ」の出題比率を引き上げ ◆ ITストラテジスト試験（ST）、プロジェクトマネージャ試験（PM）においては、午前II試験の出題範囲に新たに「中分類11 セキュリティ」を追加（高度全区分で出題）

※ IPA　プレス発表「iパス（ITパスポート試験）をはじめとする情報処理技術者試験の出題構成の見直しについて」
http://www.ipa.go.jp/about/press/20131029.html

（注）iパスは 平成26年5月7日以降、iパス以外は26春試験から適用