資　料　編

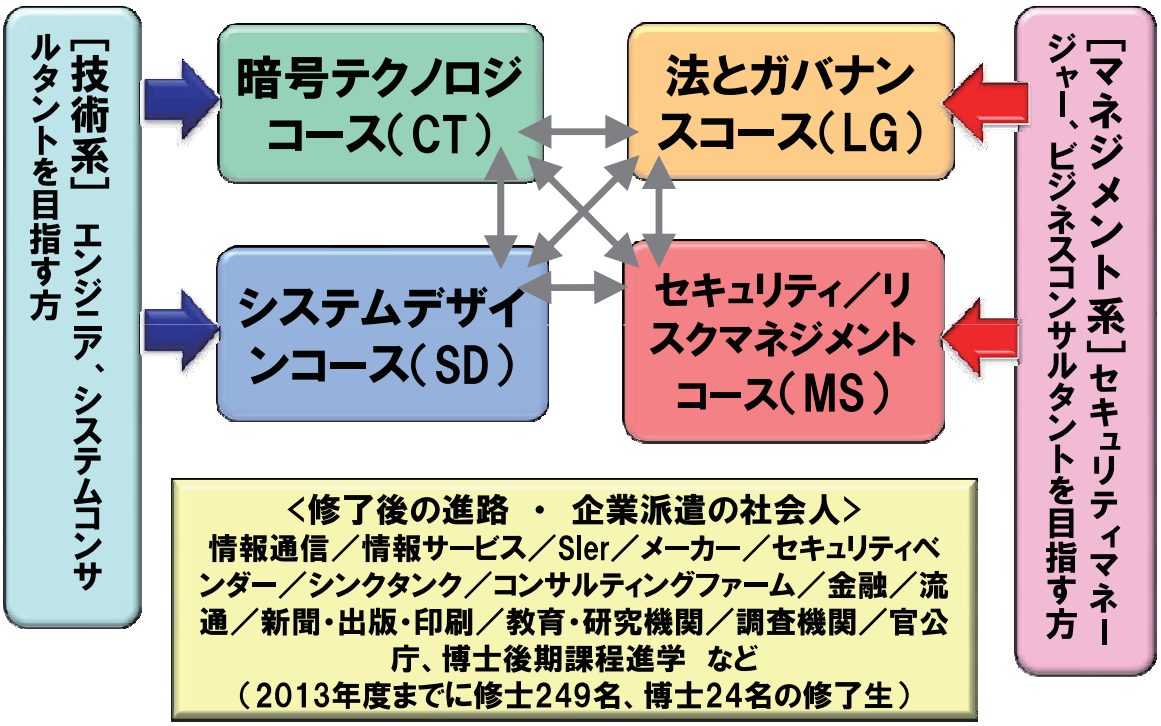
サイバー犯罪に対処するための人材育成について

2015年1月22日
林　紘一郎
情報セキュリティ大学院大学

1

育成する人材像と修士課程コース

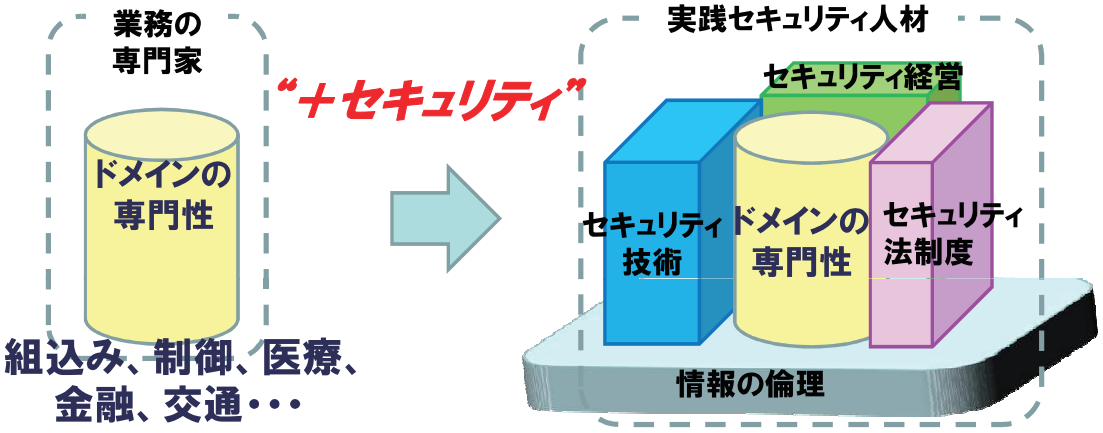
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



2

領域毎の“＋セキュリティ”による実践セキュリティ人材育成

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

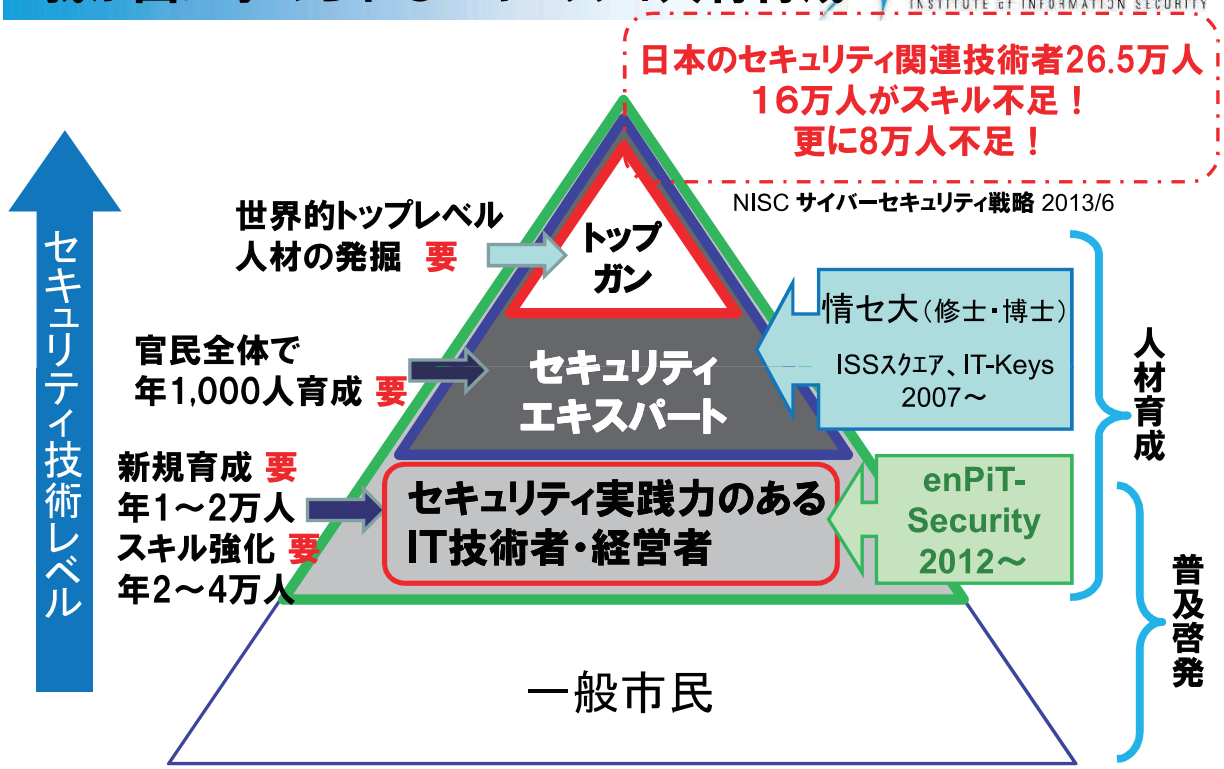


総合的なセキュリティ実践力 ＝《倫理》の土台の上で
《技術・法制度・経営》のベストミックス

3

我が国に求められるセキュリティ人材育成

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



enPiT Security

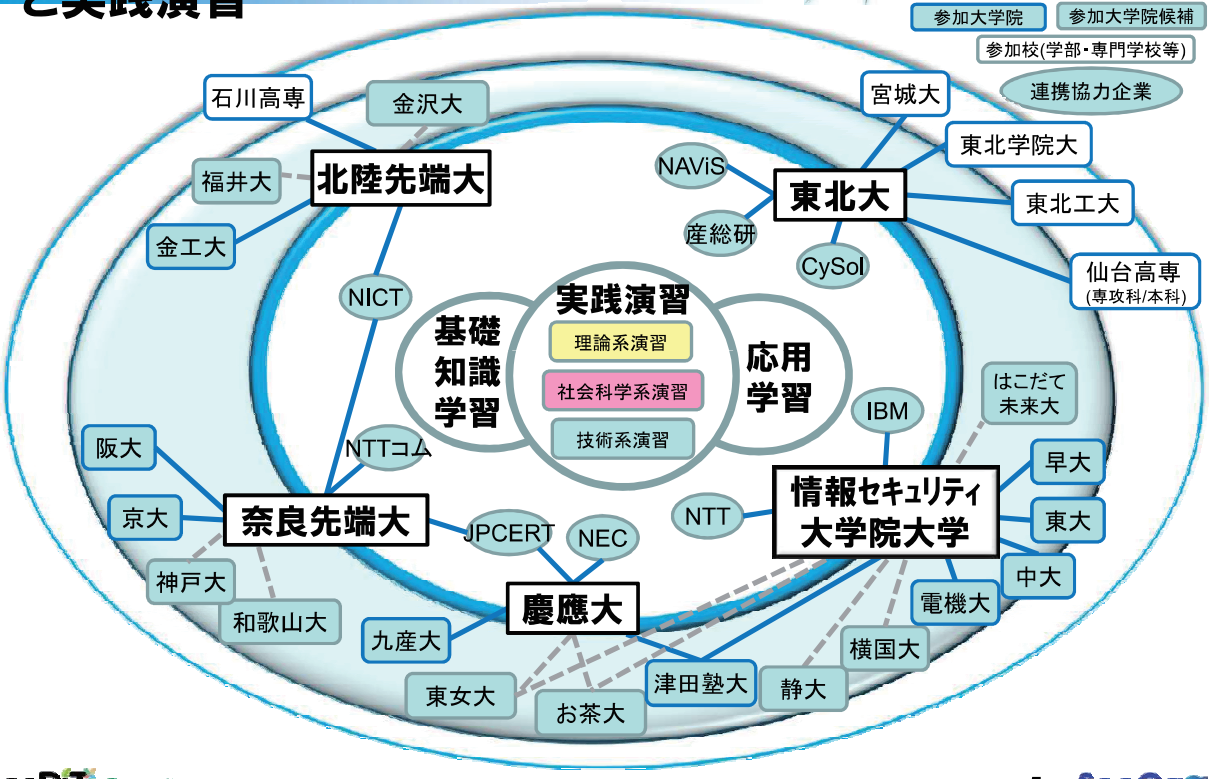
4

SecCap

協力企業・組織との密な連携による講義と実践演習

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

参加大学院　参加大学院候補
参加校(学部・専門学校等)
連携協力企業



enPIT Security

5

SecCap

連携5大学が共同で開講：SecCapコース（2014年度）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

暗号技術，Webサーバ・NWセキュリティから，法制度やリスク管理まで幅広く最新技術と知識を具体的に体験を通して習得

基礎知識学習

共通科目：情報セキュリティ運用リテラシー

基礎科目：所属大学指定科目

演習

- 情報セキュリティ演習

- セキュリティ基礎演習
- ネットワークセキュリティ検査と対策演習
- Webアプリケーション検査と脆弱性対策演習
- デジタルフォレンジック演習
- Capture The Flag（CTF）入門と実践演習
- 無線LANセキュリティ演習
- システム攻撃・防御演習
- システム侵入・解析演習
- リスクマネジメント演習
- インシデント体験演習
- IT危機管理演習
- ハードウェアセキュリティ演習
- ネットワークセキュリティ実践

- インシデント対応とCSIRT基礎演習
- 組織経営とセキュリティマネジメント演習
- 事業継続マネジメント演習

先進科目

理論系	・最新情報セキュリティ理論と応用
技術系	・情報セキュリティ技術特論 ・先進ネットワークセキュリティ技術
社会科学系	・セキュア社会基盤論 ・情報セキュリティ法務経営論

その他の活動

- セキュリティ分野シンポジウム
- 企業インターンシップ
- 交流ワークショップ

enPIT Security

6

SecCap

SecCap実践セキュリティ演習

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

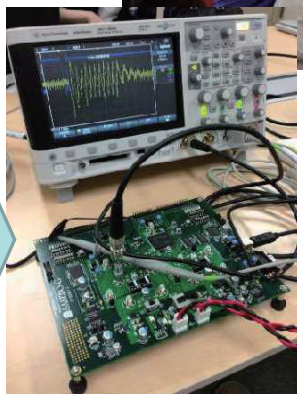
企業等の協力による実環境＆実データを使った演習

各自が演習に取り組む

グループ討議

発表

ハードウェア
セキュリティ
演習



enPiT Security

7

SecCap

習うより慣れよ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

8

日本人の得手と不得手

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

アレンとヤーゴの『金融は人類に何をもたらしたか』(東洋経済、2014年)における藤野の監訳者解説(p.348)から

・トヨタのJITは、世界標準と認められるほどの価値があるが、これを形式知化した教科書や、訓練コースの設計に努力しなかった。
・この間アメリカは、これを徹底的にビジネススクールで教えるとともに、APICS(American Production and Inventory Control Society)が資格制度を作り、今では日本人がそれを受けている。
・日本人に欠けているのは、こうした広い視野をもたらす教養である。
・今後この種の応用が必要なのは、いずれも制御理論に基づく、金融イノベーションと、サプライチェーン・マネジメントである。

私は、この藤野のコメントに、以下を追加したい。
・「セキュリティ・マネジメント」も、この種の応用が必要だし、未だ日本が追い付ける分野である。

9

平時と非常時、PDCAとOODA

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

日本人の不得手の1つとして、次の区分が不明確(あるいは後者の不存在)があるのではないか?

・平時と非常時:
通常は明確に切り分ける必要があるが、3.11の大災害においても、災害緊急事態を発令しなかった(原子力緊急事態の方は発令された)。発令していれば、急を要する事務処理を政令等で実施し、次の国会に法案を提出して承認を得る、ということが可能だった(林・田川・淺井 [2011] 『セキュリティ経営』、勁草書房)。
・PDCAとOODA:
前者は平時におけるリスク管理の基本で、これに習熟している必要があるが、瞬時の決断を要する緊急事態にマニュアルを見ている暇はない(当大学院の博士論文の中に、3.11における外資系企業の対応をサーベイしたものがあるが、「マニュアルではなくチェックリストを使っていた」という)。
OODA(Observe, Orient, Decide and Act)は、朝鮮戦争における航空戦の分析から導かれたもので、前線における対応に適している。日本人は「全員一致」の Kaizen 運動などでは優れているが、このようにCommand and Controlにおける意思決定と、現場における判断とを切り分けることも、必要ではないか?

10

「世界一安全な国」におけるセキュリティ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

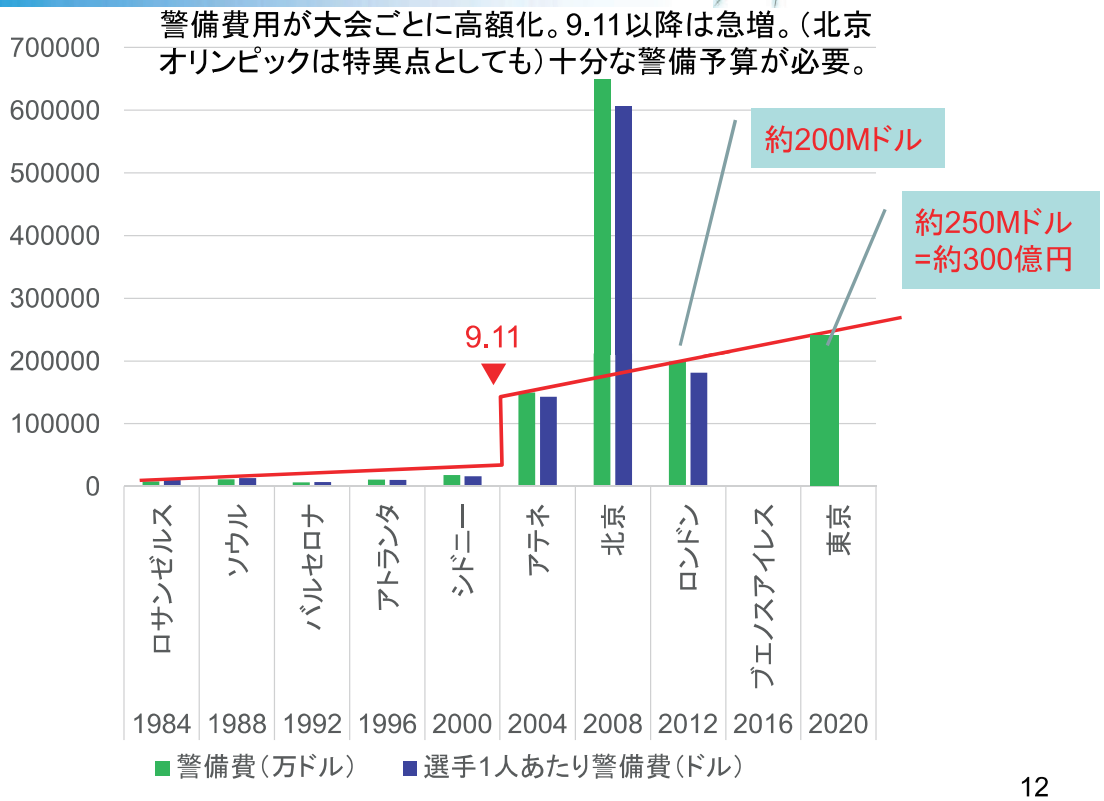
- 「世界一安全」と言われるには、日本人の倫理観・共助の精神・共同体の規範などが与っていたであろう。さらに戦後の経済成長によって、平等な社会に近づき、不満が溜まらなかったことも幸いした。
- 今後は少子高齢化とともに、発展によって生じたゆとりが減少せざるを得ないことに加えて、グローバル化の進展とともに不平等の拡大・移民の扱いなどの難題が生じ、安全環境は脅かされるであろう。
- 従来の安全は、共同体的安全であって「安全はタダ」と思われてきたが、今後は（警備保障会社に頼むように）安全は外部化され、「裕福な人が有償で買うもの」という側面が出てこざるを得まい。
- しかし世界の多くの国で見られる、「他人を見たら泥棒と思え」という社会は悲惨であり、日本が直ちにそこまで激変するとは思われない。旧来の伝統は生き続けるが、綻びも目立つようになるので、前者をなるべく維持し、後者に対して適時の対応を考えるという、ハイブリッドな方法が妥当であろう。
- その際注意すべきこととして、以下の2点が気になった。
  ① 危険が広まるのは早いが、それを修復するには膨大な時間と労力がかかる（発表者は1992年から95年までニューヨーク市に滞在したので、ジュリアーニ以前と以後を見聞した）。
  ② いかなる状況であれ「安全はタダ」ではなく、（機会費用も含めて）何らかのコストはかかっている。「世界一安全な国」には、それを理解するための啓発活動が必要である。

11

（補足）2020オリンピックに向けて

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

警備費用が大会ごとに高額化。9.11以降は急増。（北京オリンピックは特異点としても）十分な警備予算が必要。



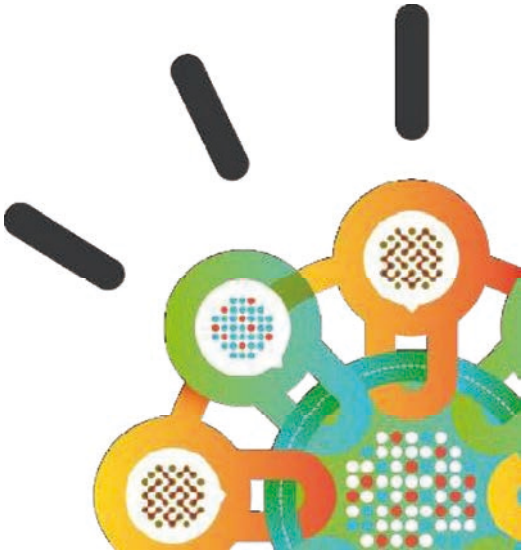
12

IBM Security Services

平成26年度総合セキュリティ対策会議　第一回

民間企業における人材育成の取組

日本アイ・ビー・エム株式会社
徳田敏文



IBM Security Services

セキュリティ人材育成の必要性

- **「攻撃を受けてしまうという前提」**
  社内外のリソースを活用し、セキュリティ・インシデント（事故）発生に備える必要がある時代である
- **「社内」エリアへの対応も急務**

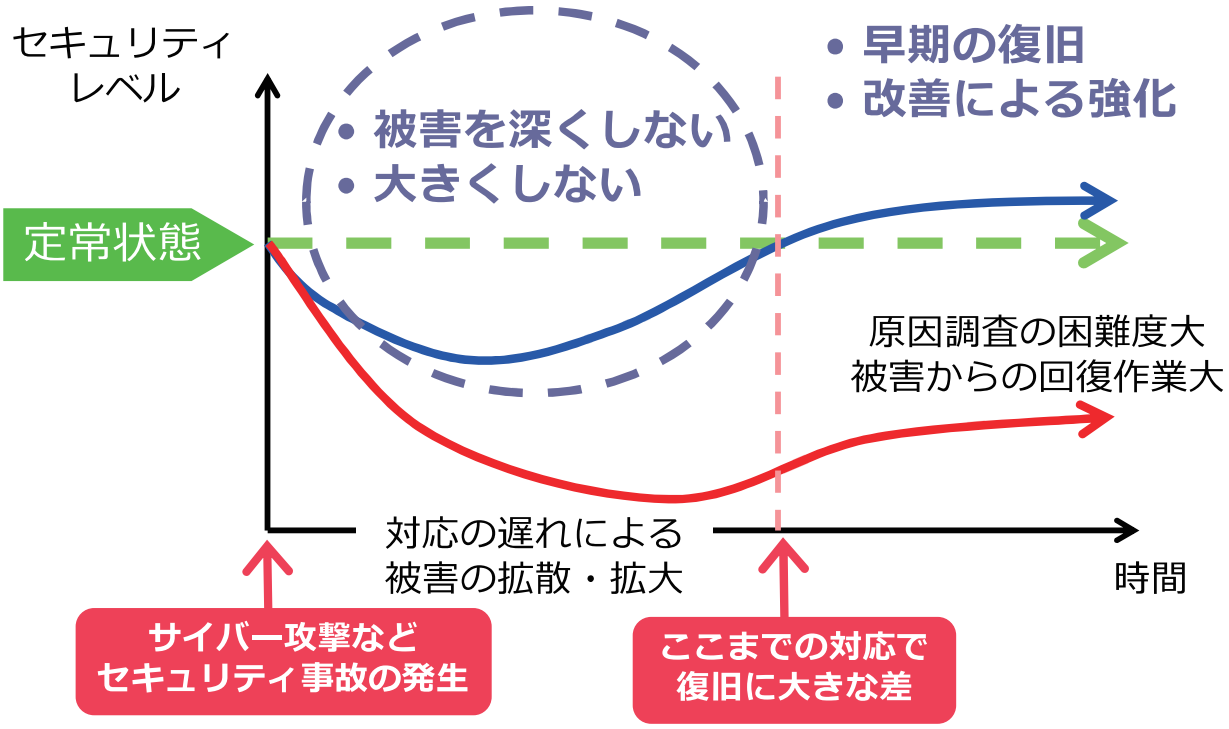
巧妙化する攻撃	**攻撃の高度化・多段階化**によりセキュリティ脅威の発見がますます困難になっている
セキュリティー担当者のスキル・人材不足	IT部門にはセキュリティ担当者の技術力、および**人材が不足**している
IT環境の複雑化	**複雑化する IT 環境**において、単一のセキュリティ対策では追いつかない

2

IBM Security Services

セキュリティ事故発生時の対応による復旧の差

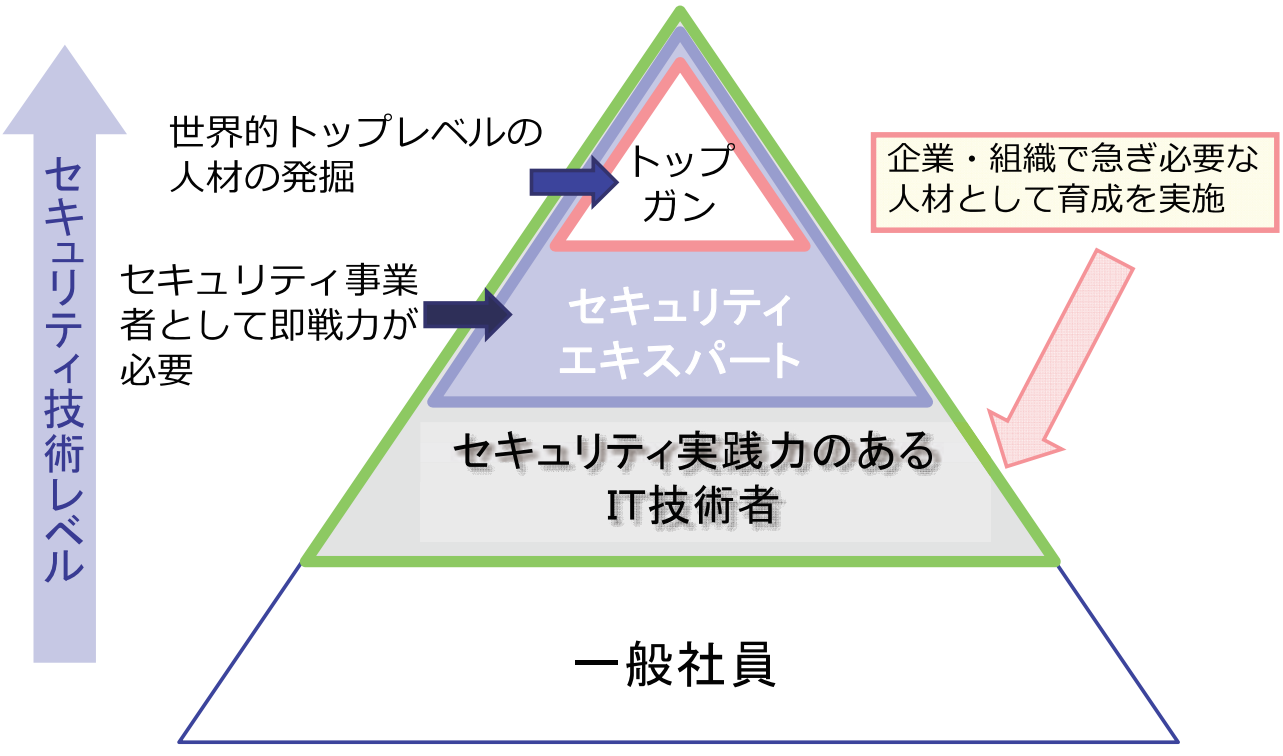
企業経営にインパクトを与える事態へ対応できる人材が必要



3

IBM Security Services

企業におけるセキュリティ人材育成



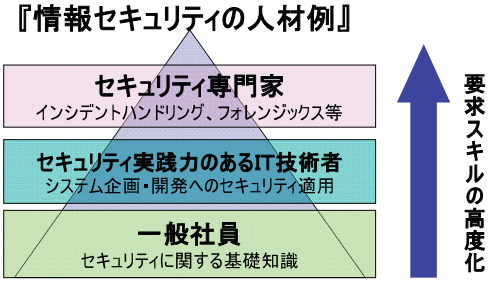
4

IBM Security Services

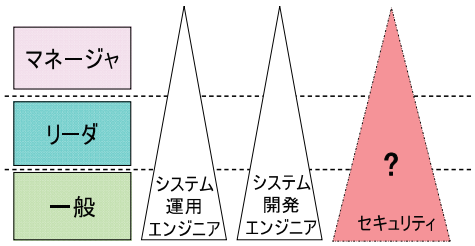
セキュリティ実践力のあるIT技術者

セキュリティ事業者にセキュリティ専門家が必要であることは言うまでもないが、ユーザー企業においてもセキュリティ技術を有した人材が必要となっている。セキュリティ事業者に高度な専門サービスを依頼する場合も、ある程度専門的な知識が必要となる。しかし、ユーザー企業の多くは、セキュリティに関するキャリアパスが設定されていないところが多く、自社での育成も難しい状況となっている。

『情報セキュリティの人材例』



『キャリアパスの例』



- **セキュリティ専門家の知識をうまく活用するためには、セキュリティ実践力のあるIT技術者の養成が重要となる。**
- **情報処理推進機構（IPA）の調査結果において、75%以上の企業が、スキルや人数、または両方で、情報セキュリティ人材不足を感じている。**

＜人材不足の事例＞

- **兼務によりセキュリティ分野に時間を割くことができない。**
- **スキルの習得機会が少ないため、スキルの維持・高度化ができない。**
- **属人化しており、後進の育成が行われていない。**
- **人材を募集しているが、求めるレベルの人材が応募してこない**

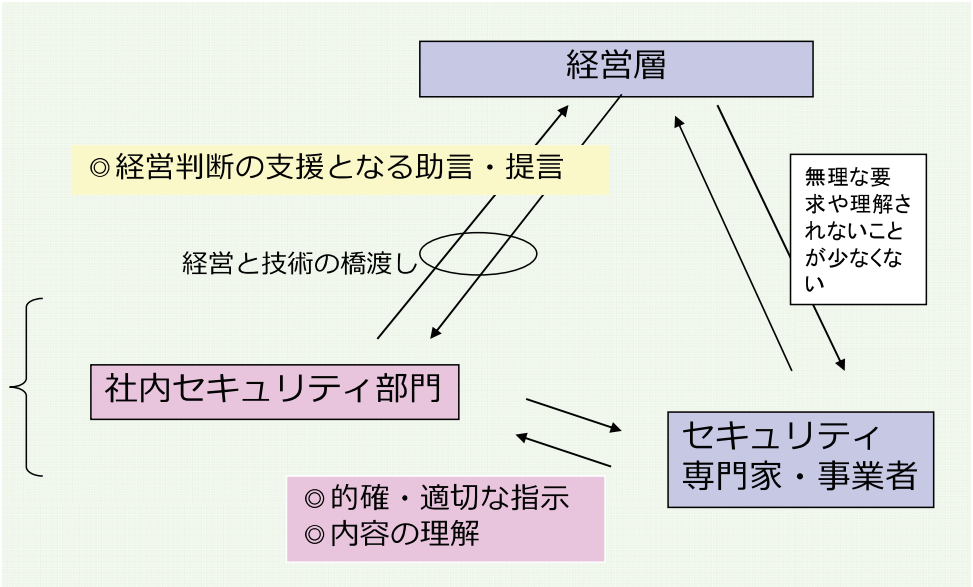
5

IBM Security Services

経営層に関するセキュリティ・アドバイザーとして

- セキュリティ施策に対しての投資対効果に疑問を持たれている
- セキュリティ施策を決めても経営層の理解ひとつで白紙に戻る事がある
- 脅威の設定自体が難しい、他社事例が通用しない

この部門に所属する人材を育成していく

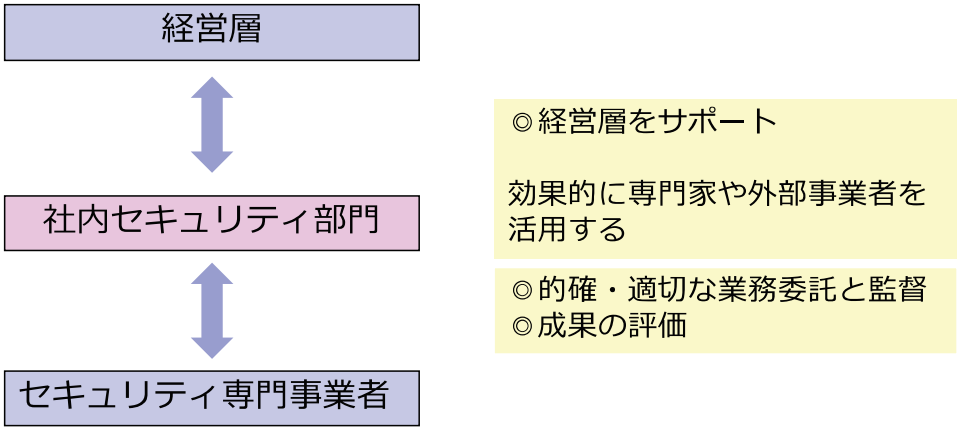


6

IBM Security Services

経営層に関するセキュリティ・アドバイザーとして

- 新聞等メディアで報道された情報セキュリティ上の問題が自社に影響があるか否かすぐに知りたい
- 他社で発生したセキュリティ事故が自社で発生する可能性があるか知りたい
- 事故発生を予防するための適切な施策は何か知りたい



7

IBM Security Services

人材育成の背景と目的（まとめ）

サイバー攻撃等によって情報システムに重大な障害が発生する恐れがあり、組織として一体となった対応が必要となる 。そのため組織を横断したセキュリティ事故等対応の取り組みをリードできる人員が必要となっている。

- セキュリティ事業者だけでなく、ユーザー企業のセキュリティ担当者の育成も重要
- 経営にインパクトのある情報セキュリティ事故防止のための施策を進めるためにも、経営層をサポートする人材の育成が重要
- セキュリティ事故発生時に、セキュリティ専門家・事業者の支援を最大限に活用することを含め、迅速な初動対応により被害を最小限に抑え、適切な再発防止策を立案できる人員を養成できることが理想

8

FUJITSU
shaping tomorrow with you

富士通“セキュリティマイスター”認定制度ご紹介

2015年 1月22日
富士通株式会社
サイバーディフェンス室
セキュリティテクノロジーセンター

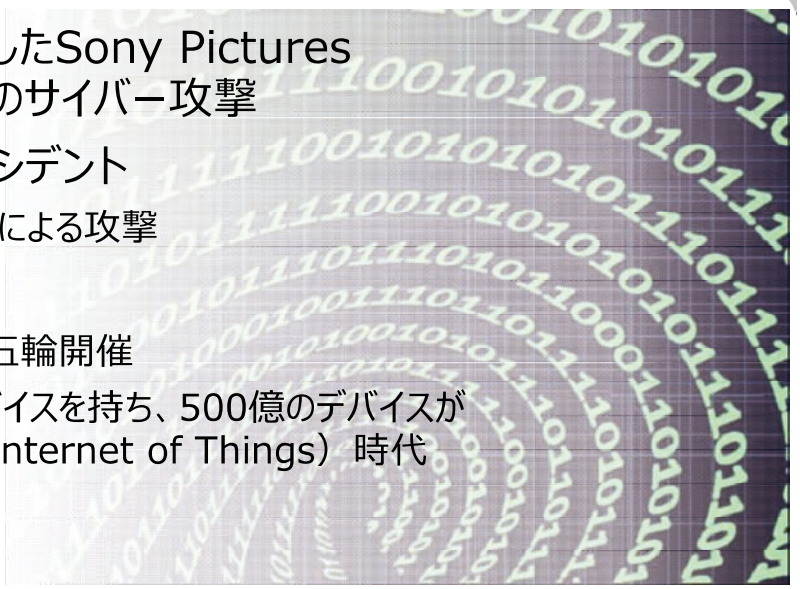
FUJITSU

１．セキュリティマイスター　認定制度　発足の背景

社会問題化するサイバー攻撃

FUJITSU

- 2014年11月下旬に発生したSony Pictures Entertainment(SPE)へのサイバー攻撃
- 止まらない不正ログインインシデント
  - リスト型攻撃、ブルートフォースによる攻撃
- 今後・・・
  - マイナンバー制度導入、東京五輪開催
  - 全世界70億人がデジタルデバイスを持ち、500億のデバイスがインターネットに繋がるIoT（ Internet of Things）時代



ソリューションプロバイダーとして、セキュアなサービスを継続的に提供する社会的責任が、富士通にはあると考えております

セキュリティ特化技術者の育成と認定の要求

FUJITSU

- システムインテグレーションおよびサービス運用の最前線で、「セキュリティ品質の作りこみ」を実践し、出荷時の監査や検査に頼らない堅牢なセキュリティ品質を持つソリューションを実現する「フィールド領域」のエンジニアの育成と認定
- 富士通のプレゼンスを向上させ、ビジネス拡大につなげることができる、競争力を持った「エキスパート領域」のエンジニアの育成と認定
- 富士通の高度なセキュリティ技術の象徴として、グローバルで活躍でき、社外から評価される「ハイマスター領域」のエンジニアの認定

セキュリティ特化技術者の計画的な育成・認定はソリューション・サービスビジネスの経営課題と捉えています。
その為、2014年度から社内認定制度“セキュリティマイスター”を、開始しました。

FUJITSU Security Initiativeの実践に向けて

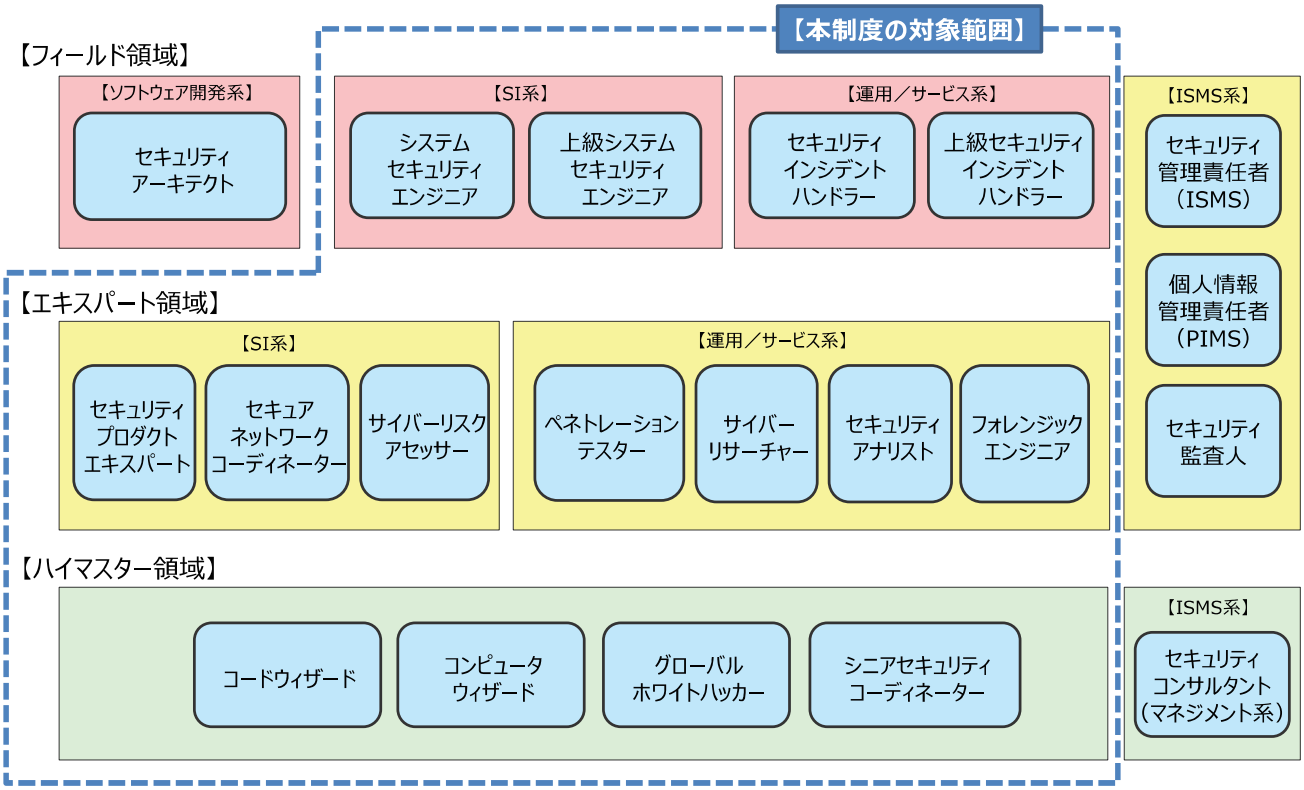
- FUJITSU Security Initiativeを実践する人材を“セキュリティマイスター”という位置づけで、系統的／計画的／継続的に育成および認定するという方針を打ち出しています。
- この制度は、活動領域の違いを示す３つの領域で人材を定義しています。

＜セキュリティマイスター＞

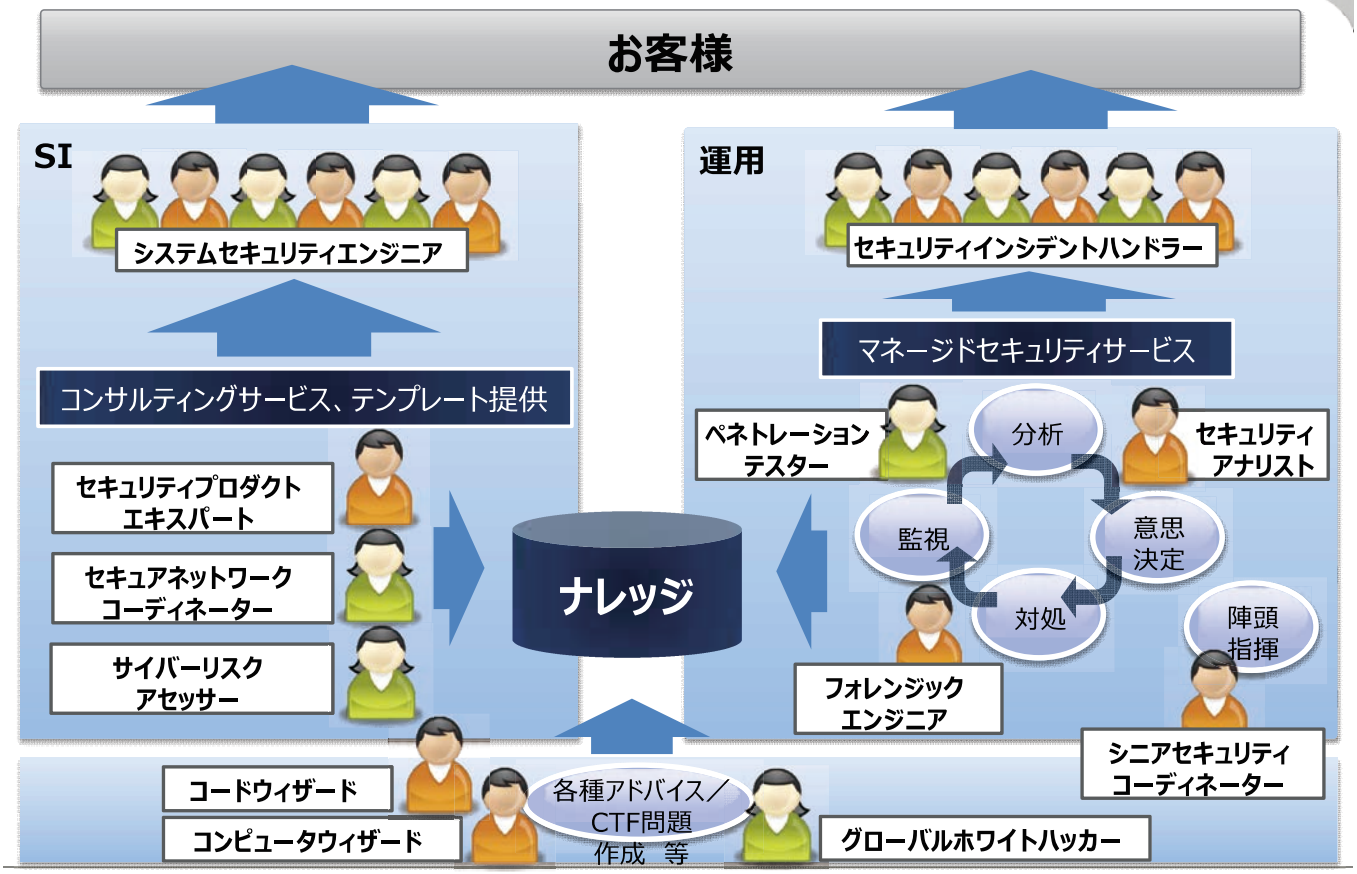
		想定対象部門
	システム開発・サービス運用現場で高度なセキュリティ技術の適用を推進し、お客様業務の安心安全を実現する「フィールド」領域のエンジニアを育成・認定	フィールドSE、サービスエンジニアが所属する部門
	お客様へ最適なソリューションを提供するため、高度なセキュリティ特化技術を持つ「エキスパート」領域のエンジニアを集中的に育成・認定	セキュリティビジネスを行っている部門 またはセキュリティの支援業務を行っている部門
	高度な脅威に対抗するため、業界最高レベルのセキュリティ技術を持つ「ハイマスター」領域の人材を幅広くグループ内から発掘・認定	富士通グループ全体

２．セキュリティマイスター認定制度の概要と活動状況

富士通のセキュリティスキルの体系図



セキュリティマイスター活躍のイメージ



認定の前提スキル

FUJITSU

■ 前提スキル

■ 【フィールド領域】

- ■ ITスキル標準の共通レベル2（基本情報技術者）相当の
  スキルを有していること

■ 【エキスパート領域】

- ■ ITスキル標準の共通レベル4（情報処理技術者試験における高度試験）または
  CISSPの資格を有していること

■ 【ハイマスター領域】

- ■ 富士通グループ外からも認められるコンピュータのスキルを有していること

※FUJITSU Wayに従って行動できる人、安心安全のミッション実行に対する
モチベーションを有する人が望ましい

参考：ITスキル標準V3（IPA）
http://www.ipa.go.jp/jinzai/itss/download_V3_2011.html

人材像定義　例【エキスパート領域】セキュリティアナリスト

FUJITSU

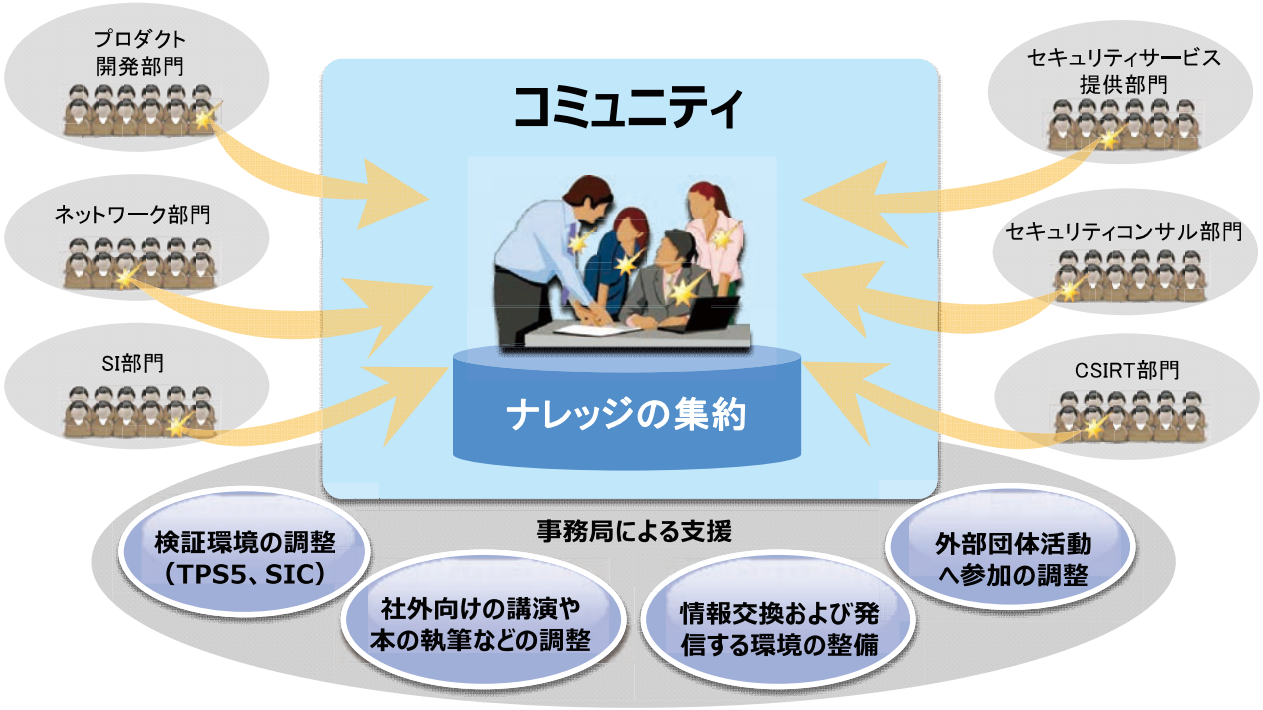
人材概要	スキルマップ				
プロフィットのセキュリティ部門やネットワーク部門に籍を置き、主にネットワーク上のログやパケットを分析する知識を活かし、マネージドセキュリティサービス実施にあたる人材	基礎理論	■	データベース	■■
	アルゴリズムとプログラミング	■	ネットワーク	■■
	コンピュータ構成要素	■	セキュリティ	■■
	システム構成要素	■	サービスマネジメント	■■
	ソフトウェア	■■■	システム監査	
	ハードウェア		システム戦略	
	マルチメディア		法務	

主な業務	各種ログやパケットを収集し、どのような攻撃が行われているのか分析する セキュリティインシデントに対して周辺機器のログを収集し、システムに対する影響範囲を特定する セキュリティインシデントがシステムに影響を与える場合、暫定対処案を提示する 顧客と折衝しSEやCEおよびファーストラインと連携して暫定対処を支援する 必要に応じてフォレンジックエンジニアの出動依頼などの助言を行う フォレンジックの結果から、必要となる恒久対処案を提示する
ビジネス貢献/必要性	MSS内でセキュリティインシデントハンドラーの上級職として機能 企業内CSIRT構築支援ビジネスへ向けたノウハウの提供
標準スキル	セキュリティに関する応酬話法ができる セキュリティ侵害のシナリオを推測できる 各種OSやミドルウェア、プロダクトが出力するログを理解している 各種のログやパケットを相関して考察した上で、誤検知かどうかやインシデントの原因を推測できる grep、awk、sedなどのコマンドを使って目的のログを抽出・整形できる パケットを取得して正常な通信と不正な通信を見分けることができる 代表的なネットワークプロトコルについて理解している 正規表現やSQL文を理解して、書くことができる
推奨スキル	ネットワークスペシャリストまたは各種ベンダー資格（CCIE、LPIC-3、MCSEなど）を取得している GIAC Certified Incident Handlerを取得している

活動のポイント1：コミュニティの形成／維持

FUJITSU

- 社内の各部門に点在しているナレッジの集約化を図り、有効活用するためのコミュニティを形成／維持しています。
- 有識者同士のナレッジ共有により、認定後のスキル向上にも繋がっています。



活動のポイント2：実践的演習の提供

FUJITSU

サイバーレンジを使った実践的防御演習

セキュリティダッシュボードと連携し、「仮説を立てる（ログの調査）」「不正な通信を行っているプロセスを発見する」「対策を検討する」演習

可視化

演習ルーム全面に３つの大画面、各実習者に２画面を提供。

演習環境

サイバーレンジ上に実際のセキュリティインシデント事例から侵害環境を構築し、解析。

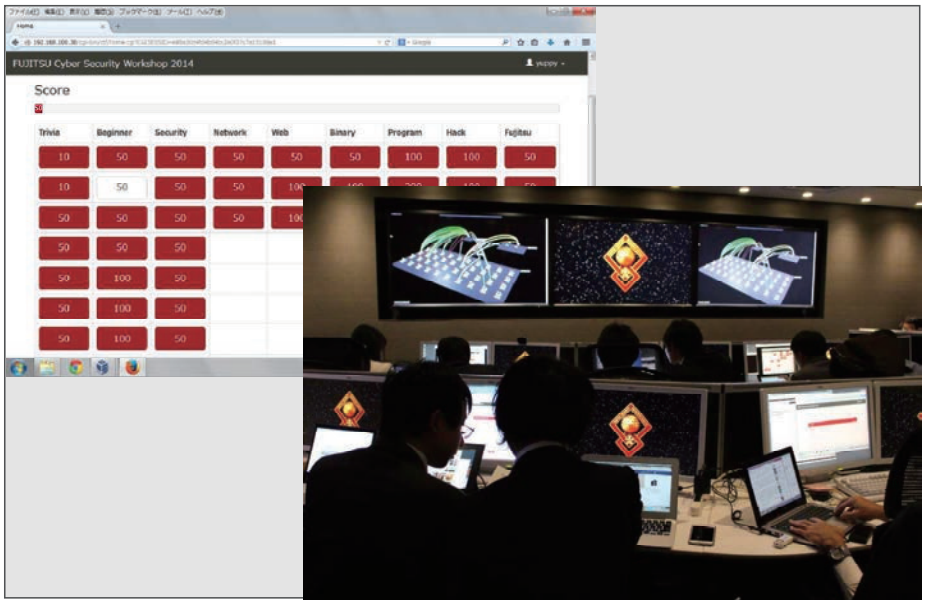
演習内容

解析結果をもとにタイムラインを作成し、各脅威に対する対策、期待できる効果について検討。

活動のポイント3：人材発掘イベントの社内開催

FUJITSU

技術者にスコープをあて、発掘・啓蒙を目指した社内ハッキングコンテスト



＊スコアサーバと参加者

■Webマガジン「FUJITSU JOURNAL」にてレポートを公開中
http://journal.jp.fujitsu.com/2014/12/25/01/

技術者

・技能の重要性の再認識。
・技術力にスコープを当てる。

啓蒙

・セキュリティの必要性を体感・共感。
・人的ネットワーク構築による意識の底上げ。

発掘

・トップガン人材（ハイマスター人材）の発掘。
・もの作りの富士通ならではの人材発掘。

12

FUJITSU

shaping tomorrow with you

平成26年度
総合セキュリティ対策会議

2015年2月10日

デジタルフォレンジック関連の人材育成
― 警察と民間 ―

東京電機大学教授
佐々木良一

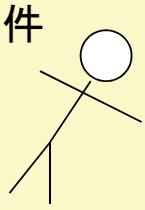
1

デジタル・フォレンジックのイメージ

Forensicというのは「法の」とか「法廷の」という意味を持つ形容詞や、「捜査や法廷で役に立つもの」の意味を持つ名詞（通常Forensics）

Forensic　Medicine：「法医学」
捜査や裁判に必要な情報を医学知識を利用して明らかにする技術や学問

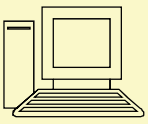
殺人事件



死因は？、凶器は？、犯人の血液型は？

Digital Forensics：「デジタル・フォレンジック」
捜査や裁判に必要な情報を、情報処理技術を用いて明らかにする技術や学問

不正侵入



侵入手口は

侵入経路は？

デジタルフォレンジックをデジタル鑑識と訳す人もいる

2

警察などにおけるDFの適用候補

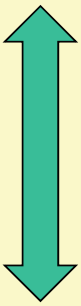
1. 殺人など犯罪の証拠のPCからの確保
（電子メール、インターネット検索履歴、その他）

2. 児童ポルノの保管証拠の確保

3. 不正侵入の被害の実態確認と攻撃者の特定

4. コンピュータウイルスの作成の証拠確保

対象は一般犯罪



対象はコンピュータ関連犯罪

3

DFで使う技術の分類

事前

1. 証拠保全技術
- ① アクセスログや通信ログなどの記録
- ② データの変更の防止やバックアップ

事後

2. 証拠収集技術
- ① 削除されたファイルや物理的に破壊された媒体を復元
- ② 暗号化されたファイルの復号
- ③ 証拠隠滅の痕跡の調査など

事後

3. 証拠分析技術
- ① 得られた大量のデータから有用なデータを抽出する（データマイニング）
- ② 得られたデータが改ざんされていないかの分析

4

警察と民間での対応範囲の違い

＜事前＞

何か起きた時に備えて

事件の発生

＜事後＞

証拠が消える前に

民間は両方

警察は事後のみ

1．証拠保全技術

警察は民間への啓発が必要

2．証拠収集技術

3．証拠分析技術

5

標的型攻撃対策のための適切なログの管理（その1）

＜機器によらない全般的な対策＞

1．各ログ取得機器のシステム時刻を、タイムサーバを用いて同期する。
2．ログは1年間以上保存する。
3．複数のログ取得機器のログを、ログサーバを用いて一括取得する。
4．攻撃等の事象発生が確認された場合の対処手順を整備する。

内閣官房情報セキュリティセンター：
http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf

6

標的型攻撃対策のための適切なログの管理（その2）

＜機器別の対策＞

1．ファイアウォール：「外⇒内で許可した通信」と「内⇒外で許可・不許可両方の通信」のログを取得する。

2．Web プロキシサーバ：接続を要求した端末を識別できるログを取得する。

3．他のシステムや機器の権限を管理するサーバ（LDAP, Radius 等）：管理者権限による操作ログを取得する。

内閣官房情報セキュリティセンター：
http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf 7

標的型攻撃対策のための適切なログの管理（その3）

＜機器別の対策＞

4．メールサーバ：「メールの送受信アドレス」及び「メッセージID」のログを取得する。

5．クライアントPC：マルウェア対策ソフトウェアの検知・スキャンログ・パターンファイルのアップデートログを取得する。

6．DB サーバ・ファイルサーバ：特別なログ設定は不要だが、確実にログを取得する。

内閣官房情報セキュリティセンター：
http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf 8

標的型攻撃対策のための適切なログの管理（その3）

＜機器別の対策＞

4. メールサーバ:「メールジID」のログを取得する。

5. クライアントPC:マルウキャンログ・パターンファイルのアップデートログを取得する。

6. DB サーバ・ファイルサーバ:特別なログ設定は不要だが、確実にログを取得する。

警察もこのようなガイドを出して、捜査時にログがないという問題を解決していくべきではないか

内閣官房情報セキュリティセンター:
http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf

9

警察と民間での対応範囲の違い

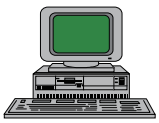
＜事前＞

何か起きた時に備えて

事件の発生

＜事後＞

証拠が消える前に



民間は両方

警察は事後のみ

1. 証拠保全技術

証拠を間違えて消去したりしないようにするために一般の捜査員にも必要

2. 証拠収集技術

3. 証拠分析技術

10

「証拠保全ガイドライン　第3版」

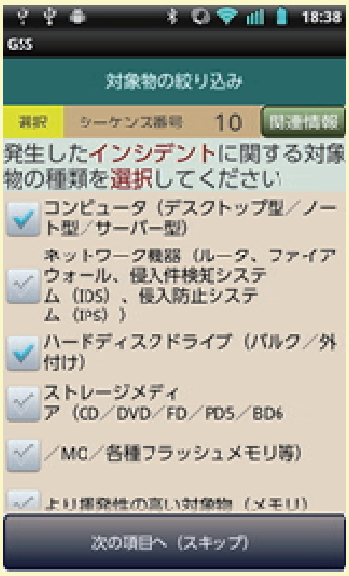
目　次　　全67ページ

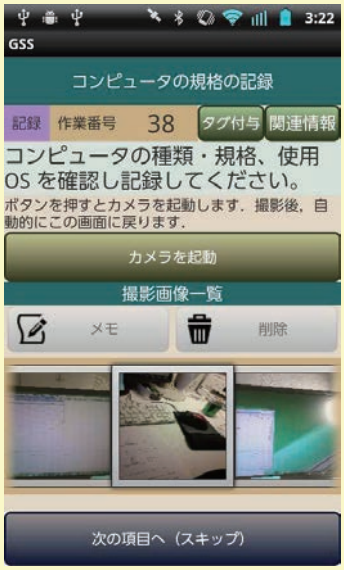
1　事前に行う準備
2　インシデント発生直後の対応
3　対象物の収集・取得・保全
4　証拠保全機器の準備
5　証拠保全作業中・証拠保全作業後
付 録

警察もこのようなものがなければ作成すべき

デジタルフォレンジック研究所会
https://digitalforensic.jp/home/act/products/df-guidline-3rd/　11

DFのためのガイドライン
総合支援システムGSS





GSS:東京電機大学で開発中

慣れない捜査員でも適切に対応するには、このようなシステムが必要に

12

東京電機大学大学院における新たなセキュリティ教育

文科省「高度人材養成のための社会人学びなおし大学院プログラム」の1つで「国際化サイバーセキュリティ学特別コース」として認可。デジタルフォレンジックは6つの科目の1つ。対象は社会人20名、大学院生20名程度

（1）サイバーセキュリティ基盤
（2）サイバーディフェンス実践演習
（3）セキュリティインテリジェンスと心理・倫理・法
（4）デジタルフォレンジック
（5）情報セキュリティとガバナンス
（6）セキュアシステム設計・開発

https://cysec.dendai.ac.jp/

13

Carnegie Mellon University

Master of Science in Information Networking with a concentration in Computer Forensics and Incident Response

14-761: Advanced Information Assurance
14-822: Host-Based Forensics
14-823: Network Forensics
14-824: Advanced Host-Based Forensic Analysis
14-825: Advanced Network Analysis
14-826: Event Reconstruction and Correlation

http://docs.lib.purdue.edu/dissertations/より
The Development of a Standard Digital Forensics Master‘s Curriculum　Kathleen Strzempka　*Kathleen A. Strzempka,*

14

デジタル・フォレンジック教育総合カリキュラム

将来の講義候補	「デジタルフォレンジック各論」（講義主体：企業、大学） ・DFツール ・スマホ・家電DF ・DFと技術（日本語処理、暗号他）	「ネットワークフォレンジック」（講義主体：大学、企業） ・パケットログ管理 ・SIEM ・自動診断　他	「応用デジタルフォレンジック」 （講義主体：企業、大学） ・E－Discovery ・企業／捜査機関のDF ・法とDF／法廷対応他
最初の講義	東京電機大学大学院2015年度講義 「デジタル・フオレンジック（概論）」 2015年度9月-2016年1月　金曜日（18:10-19:40）		
ベースとなる基礎知識	コンピュータアーキテクチャー ネットワークアーキテクチャー 法律の基礎	プログラミング セキュリティ技術一般 訴訟法の基礎	

現時点でのDF教育計画①

2015年度は後期金曜日18：10－19：40の予定

（1）デジタル・フォレンジック入門（電大　佐々木）
（2）ハードディスクの構造，ファイルシステム（立命館上原）
（3）フォレンジックのためのOS，Windows（立命館上原）
（4）フォレンジック作業の基礎（UBIC　野崎）
（5）フォレンジック作業・データ保全（UBIC　野崎）
（6）フォレンジック作業・データ復元（トーマツ白濱）
（7）フォレンジック作業・データ解析1（トーマツ白濱）
（8）フォレンジック作業・データ解析2（UBIC　野崎）
（9）上記の演習（白濱、野崎）

16

現時点でのDF教育計画②

(10)ネットワークフォレンジック(攻撃法，マルウェア，ログの取り方)(電大:八槇)
(11)上記の演習(電大　八槇)
(12)代表的な対象におけるDFの方法1　情報漏えい
(トーマツ白濱)
(13)代表的な対象におけるDFの方法2
不正会計、e-Discovery　(UBIC　野崎)
(14)法リテラシーと法廷対応(弁護士　桜庭)
(15)デジタル・フォレンジックの今後の展開　(電大　佐々木)
(16)学力考査と解説

現時点でのDF教育計画②

(10)ネットワークフォレンジック(攻撃法，マルウェア，ログの取

報漏えい
(トーマツ白濱)

y　(UBIC　野崎)

(電大　佐々木)

(16)学力考査と解説

警察庁でも専門家向けに、より高度な教育を含むDF教育を実施中だという。

一般の捜査員対策をどうするか

一般の捜査官への教育の例①

・京都府警では警務部が中心となり、各課に呼びかけて15名のサイバー捜査官を選出。

・選出されたサイバー捜査官は、原課に所属しつつ、定期的に研修を受ける形でサイバー犯罪対策に関する教養を身につける。

小林文彦：京都府警察の「サイバー捜査官育成システム」の概要について, 警察学論集, 第67巻, 第10号 (2014年10月), pp.13-24.

19

一般の捜査官への教育の例②

・その教養に当たっては、警察内部の通常のサイバー専科教習の他にサイバー犯罪対策研究会（座長：立命館大学上原先生）から民間の専門家を講師派遣する

・サイバー捜査官は2年の研修を経て、サイバー特別捜査官に昇格し、原課でサイバーに関連した事案への対応にあたる。

他都道府県でもこのような試みはありうるのではないか

小林文彦：京都府警察の「サイバー捜査官育成システム」の概要について, 警察学論集, 第67巻, 第10号 (2014年10月), pp.13-24.

20

一般の捜査官への教育の例③

NEWS RELEASE

date 2015.1.30

京都大学記者クラブ加盟各社 各位

立命館大学広報課

立命館大学情報理工学部と京都府警察による
「サイバーセキュリティ分野を中心としたICT人材育成カリキュラムの協働開発」
に係る連携・協力について

立命館大学情報理工学部と京都府警察は、サイバーセキュリティ分野を中心としたICT人材の育成カリキュラムを協働開発するための連携・協力を行います。

インターネットは、社会・経済活動に重要なインフラとして国民生活を支え、利用者数は1億人を超えます。サイバー空間における社会・経済活動は質量ともに年々増大し、今や現実空間と同視できるほどの公共空間となっています。一方で、サイバー犯罪及びサイバー攻撃も日々高度化し、あらゆる犯罪にインターネットが利用されています。多くの機関・団体において情報セキュリティへの配慮の必要性が高まり、大学等教育機関における情報分野の人材育成にますます注目が集まっています。

21

終りに

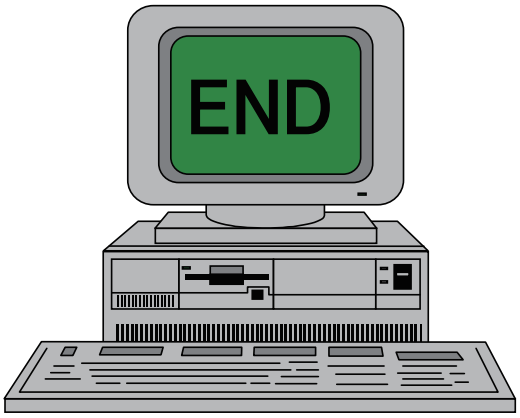
1．デジタル・フォレンジックは民間でも警察でもますます重要になっていく。

2．一方、HDDの大容量化や、SSD（Solid State Drive）の普及により、デジタルフォレンジックが困難に。

3．ネットワークフォレンジックや、ライブフォレンジック、クラウドフォレンジック等新しい多くの技術が重要に。

4．産官学が協力した官民の人材育成がますます重要に。

22



23

(ISC)²概要と資格制度について

2015年2月10日

衣川俊章、CISSP
(ISC)2ジャパン　代表

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

本日のアジェンダ

- 情報セキュリティ専門家に必要な知識・スキル
- (ISC)²概要と提供資格概要
- 各国での人材育成への取組み（当社との関わりの中で）
- サイバー捜査官に必要な知識
- 人材育成―統合的な仕組みの必要性

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

© Copyright 1989 – 2015, (ISC)² All Rights Reserved

本日のアジェンダ

- 情報セキュリティ専門家に必要な知識・スキル
- (ISC)²概要と提供資格概要
- 各国での人材育成への取組み（当社との関わりの中で）
- サイバー捜査官に必要な知識
- 人材育成ー統合的な仕組みの必要性

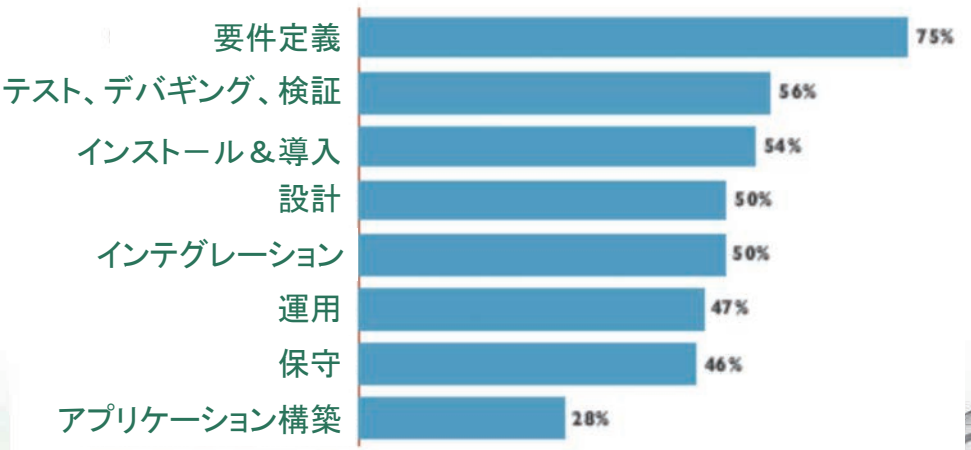
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

3

情報セキュリティ専門家に必要な要素ーソフトウエア開発

要件定義においてのセキュリティ知識の必要性が非常に高い

ソフトウェア開発プロセスでセキュリティ知識が必要なエリア



出展：2013年(ISC)2グローバル情報セキュリティワークフォーススタディ

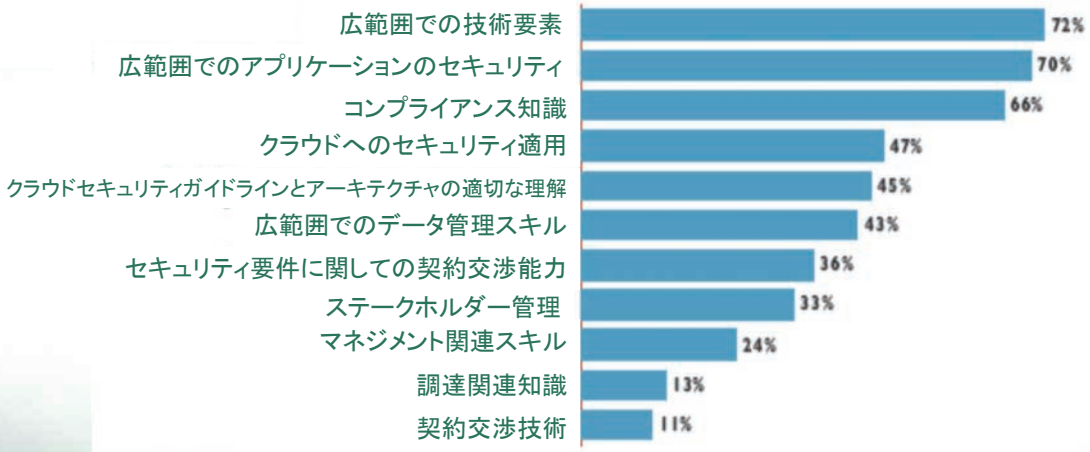
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

4

情報セキュリティ専門家に必要な要素ーモバイルセキュリティ

より広い範囲での技術要素（アプリケーション含む）やコンプライアンスへの知識が求められている

モバイルとBYODのセキュリティで必要なスキル



出展：2013年(ISC)2グローバル情報セキュリティワークフォーススタディ

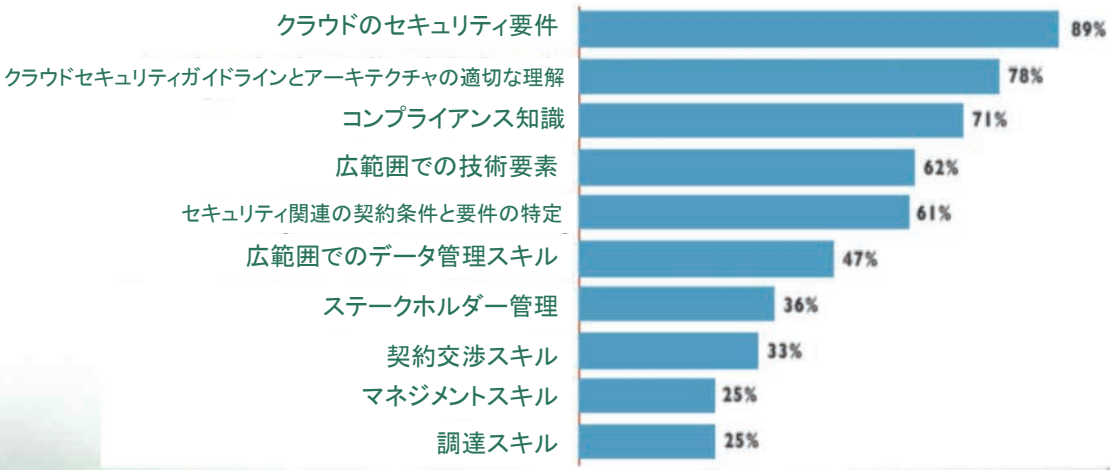
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

5

情報セキュリティ専門家に必要な要素ークラウドセキュリティ

特定の技術要素というより、包括的なセキュリティへの理解やマネジメント観点からの理解が求められている

クラウドで求められるセキュリティスキル・知識



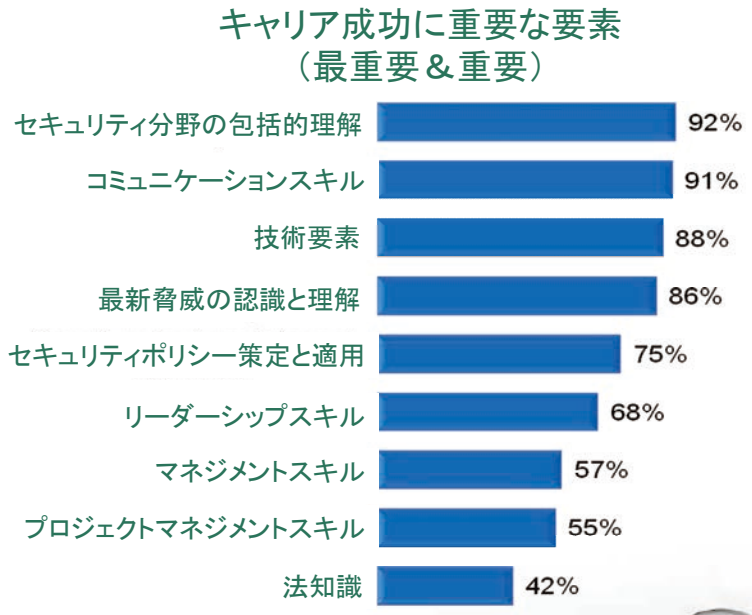
出展：2013年(ISC)2グローバル情報セキュリティワークフォーススタディ

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

6

情報セキュリティ専門家に必要な要素

包括的でかつ専門的なセキュリティスキルと洗練されたコミュニケーションスキルが欲されている



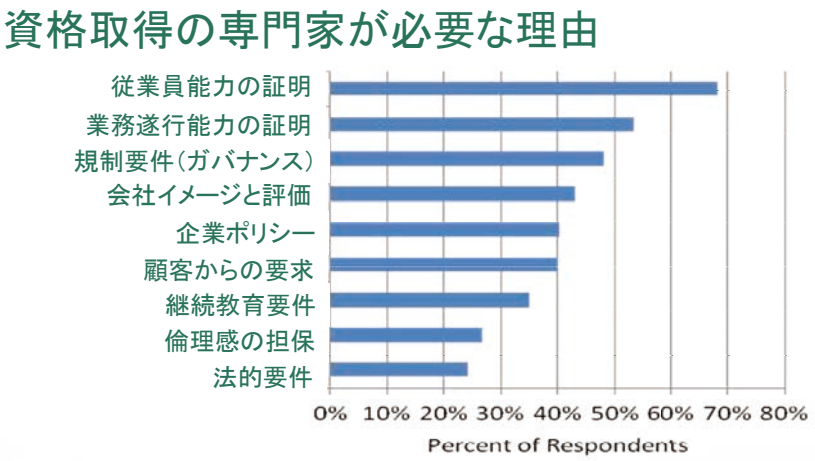
出展：2013年(ISC)2グローバル情報セキュリティワークフォーススタディ

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

7

情報セキュリティ専門家に必要な要素としての資格

資格保有者は、その能力を証明でき、業務遂行能力が高いという評価



出展：2013年(ISC)2グローバル情報セキュリティワークフォーススタディ

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

8

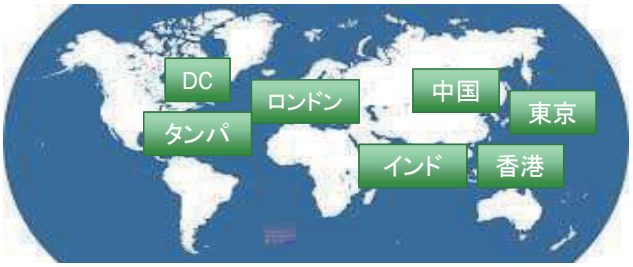
本日のアジェンダ

- 情報セキュリティ専門家に必要な知識・スキル
- (ISC)²概要と提供資格概要
- 各国での人材育成への取組み（当社との関わりの中で）
- サイバー捜査官に必要な知識
- 人材育成ー統合的な仕組みの必要性

(ISC)² について

- アイエスシー・スクエア
- International Information Systems Security Certification Consortiumの略
- 1989年、米国設立以来、グローバルで情報セキュリティ人材育成に注力し続けているNPO

世界135カ国に107,000名（2015年1月）の資格保有者が存在

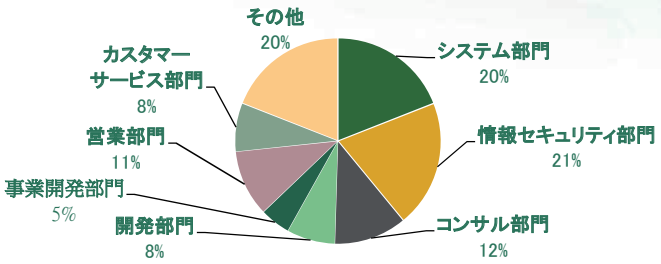


- 日本では2003年に(ISC)²ジャパンを設立し、活動を開始
  - 資格試験、トレーニング含めた全運用をローカライズ

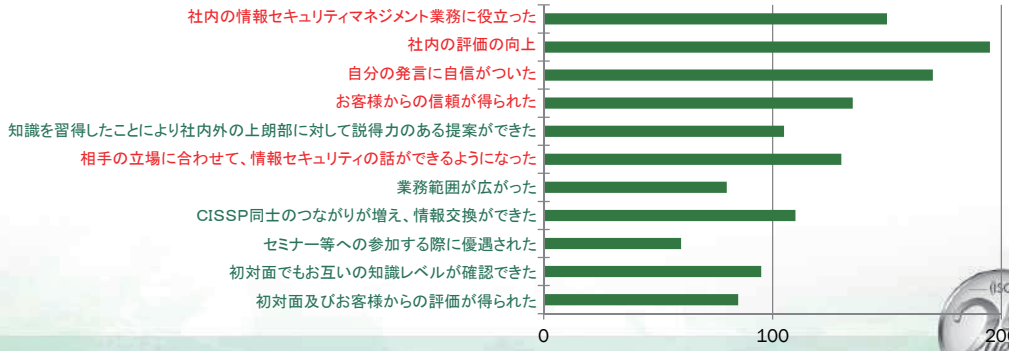
(ISC)²資格データ

日本のCISSPホルダーの所属部署

(2011年度　回答者500名)



CISSPを取得後、実際の業務で役立っていること



プロフェッショナル資格としての(ISC)²資格

- 認証された実務家・専門家が、今現場で通用する事の証明
  - CBKコミッティーによる共通知識分野(CBK)内容の定期アップデートの仕組み
  - 専門家・実務家に必要な知識の体系化、包括的理解を図れるCBKカバレージ及び構成
  - 試験：知識のみではなく実践に必要不可欠な“判断力”を見極める内容
  - 継続教育単位取得の義務付けによって、スキル・知識の維持と向上を証明する仕組み
- ISO17024認証取得による全プロセスへの高信頼性
  - 資格試験開発、運営手法、組織統制など広範囲に渡り世界基準で認められている
- 各国政府レベルでの認知：資格としてだけでなく、人材育成スキームの中に組み込まれている事実

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD. 13

CISSP とは

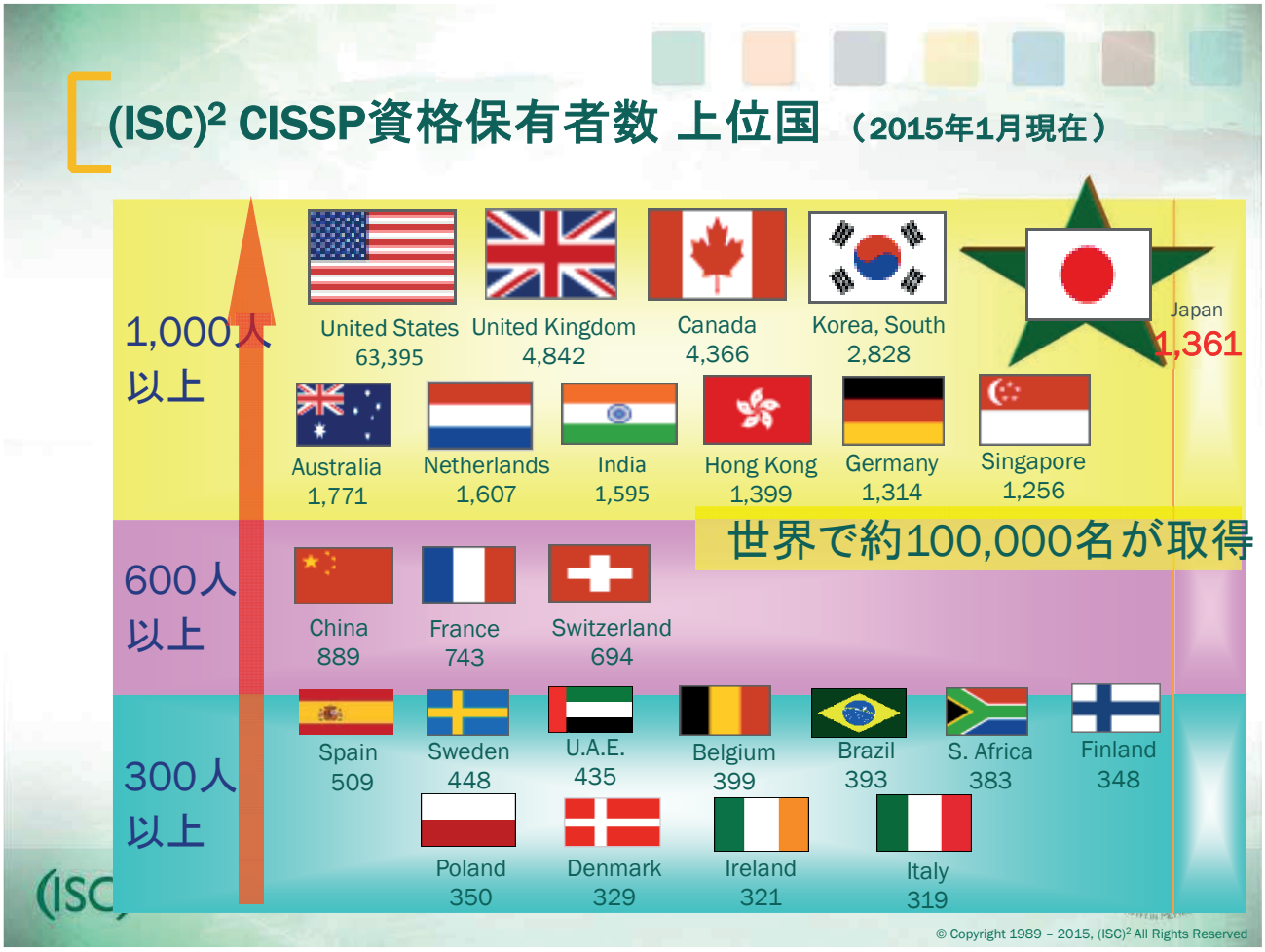
Certified Information Systems Security Professional

- セキュリティ プロフェッショナル認定資格制度（CISSP）は、CBKの8分野についての深い知識を証明するものです。戦略的かつ公平な判断のできるベンダーフリーの認定資格CISSPにより、セキュリティ専門家としてのスキルの裏付けを提供します。
- 欧米のCISO/CSOの85%以上がCISSP保有→キャリアプランの一部 となっている
- 下記のような業務遂行が出来る人間を認証している
  - ◆組織ミッション・事業戦略の理解をし、情報セキュリティの戦略的必要性やメリットを提言
  - ◆コーポレートガバナンス・マネジメントの理解と、それに合わせた組織体の構築やプロセス確立
  - ◆組織に最適な情報セキュリティ対策の策定及び導入指揮・推進
  - ◆企業内、パートナー企業、サードパーティ、規制官庁に対するコンプライアンスのモニタリング＆管理
  - ◆セキュリティ事業におけるリーダーシップとプロジェクトマネージメント

CBK 8ドメイン

1.セキュリティとリスクマネジメント（セキュリティ、リスク、コンプライアンス、法、規制、事業継続）
2.アセットセキュリティ（資産のセキュリティ保護）
3.セキュリティエンジニアリング（エンジニアリングとセキュリティのマネジメント）
4.通信とネットワークのセキュリティ（ネットワークセキュリティの設計と保護）
5.IDとアクセス管理（アクセス制御とID管理）
6.セキュリティ評価とテスト（セキュリティテストの設計、実行、分析）
7.セキュリティオペレーション（基礎概念、捜査、インシデント管理、ディザスタリカバリ）
8.ソフトウェア開発セキュリティ（ソフトウェアセキュリティの理解、適用と執行）

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD. 14



本日のアジェンダ

- 情報セキュリティ専門家に必要な知識・スキル
- (ISC)²概要と提供資格概要
- **各国での人材育成への取組み（当社との関わりの中で）**
- サイバー捜査官に必要な知識
- 人材育成―統合的な仕組みの必要性

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD. 16

他国の状況(欧米)

- イギリス
  - –スコットランドヤード
    サイバー犯罪チームが取得を推進していた。これは組織としての推奨という形ではなく、各捜査員が自主的に現場で活用できる資格として取得をしていったという経緯
  - –イギリス国防省(MoD), 軍隊隊員
    2007年10月より内部スタッフの資格取得を推進し始めている。これは業務上での有効性に加えて、退役後の就職に有利に働くという事まで含めての施策として展開をしている
  - –イギリスNCA/国家犯罪対策庁(National Crime Agency)
    サイバー犯罪担当の職員を採用する際、CISSP資格保有者を優遇している
- ・アメリカ
  NICE-NIST(商務省傘下の政府機関)主導の人材育成プロジェクト)WGメンバー参加
- ・オーストラリア
  Attorneys' General officeとMOUを交わし、SSCPを推奨資格として認定することで決定

他国の状況(アジア)

- 香港
  HK Office of the Gov CIO(政府の情報セキュリティ管轄部署)に100名以上のCISSPが在籍。CISSP取得は必須条件になっている
- シンガポール
  iDAにおいては、CISSP取得に関し最大90%まで資格取得補助を提供している
- マレーシア
  CyberSecurityMalaysia (政府のIT担当であり、マレーシア警察のフォレンジック捜査も担当)では、10分類のクリティカルインフラ産業においては、最低1名のCISSP、1名のSSCPを雇用していなければいけないというポリシーを執行中である
- フィリピン
  政府職員の情報セキュリティ専門家向け育成に関してCISSP/SSCPをベースとすることで(ISC)²と協業契約締結
- 韓国
  KISA(CISSP21名)においては、CISSPが推奨資格となっている
- ・ベトナム
  政府職員へのCISSPトレーニング提供
- ・中国
  CNITSEC(ITセキュリティ人材育成管轄省庁)との協業契約
- ・インド
  政府職員への資格取得向けトレーニング提供

学術機関との連携

- 専門学校・大学・大学院での CISSP/SSCP のカリキュラム採用
  - 米国 Univ. of Fairfax, State Univ. of Colorado, University of South Florida, Univ of Alabamaなど多数
  - Hong Kong Polytechnic University
  - Boxhill Institute Australia
  - APTIKOM and Lembaga Sandi Negara Indonesia
  - National Defense College of the Philippines
  - Royal Holloway Univ. を含めた英国の8大学
  - 情報科学専門学校（岩崎学園）
  - 国際電子ビジネス専門学校、東京電機大学(提携中)

本日のアジェンダ

- 情報セキュリティ専門家に必要な知識・スキル
- (ISC)²概要と提供資格概要
- 各国での人材育成への取組み（当社との関わりの中で）
- **サイバー捜査官に必要な知識**
- 人材育成―統合的な仕組みの必要性

サイバー捜査官に必要な知識

～ISEPAセキュリティ人材アーキテクチャ2009からの抜粋～

職種名	インシデントハンドラー（組織）
定義	攻撃発生時のインシデント分析及び対処と関係部署との調整をおこなう
典型項目	
	必須素養：
	サイバー攻撃、情報漏えいや情報システムの障害等が発生した場合のより迅速かつ的確な対応ができること
	インシデント対応業務の運用技術や蓄積された経験の共有ができること
	インシデント対応
	実施可能素養：
	災害発生時における対応等、横断的な取り組みと整合性の確保・連携について検討ができること
	サイバー攻撃等に関する脅威/影響度の分析・対処能力を向上させるための機材選定ができること
	発生頻度の高い個別のIT障害への対応方策を策定できること
	教育
	LS-0, Hyogo-B, Hyogo-A, SPIA-T, IR, SEAj-T, LACBS-14.16, C1, SANS-SEC401, 504
	資格
	CISSP, CITA, SEAj-T, SANS-GCIH

所属企業・部署グループ	サービス・製品提供組織　運用、自社資産保護組織　運用	
スキル・知識		
必須：		
知識項目	大分類	中分類
情報セキュリティマネジメント	マネジメント概論	セキュリティマネジメントの基本
		マネジメントプロセス
		関連知識
		セキュリティポリシー
		リスク分析
ネットワークインフラセキュリティ	ネットワークインフラセキュリティ	概論
アプリケーションセキュリティ	アプリケーションセキュリティ【Web】	概論
	アプリケーションセキュリティ【電子メール】	概論
	アプリケーションセキュリティ【DNS(Domain Name System)】	概論
OSセキュリティ	OSセキュリティ【共通】	識別・認証
		アクセス制御
		システム(データ)の保護
		ユーザ(データ)の保護
		リソース管理
		セキュリティ監査
		運用管理
		セキュアOS
ファイアーウォール	ファイアーウォール	概論
侵入検知	侵入検知	概論
不正プログラム（マルウェア）	不正プログラム（マルウェア）	概論
セキュアプログラミング技法	セキュアプログラミング技法	プログラミング言語とツール
セキュリティ運用	セキュリティ運用	概論
		定常運用時のセキュリティ確保
		インシデント対応
		（異常時対応）
		運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）
コンテンツセキュリティ	情報の保護	情報の格付け
		保護において留意すべき情報の特徴
		情報の取扱場面（ライフサイクル）
		機密性対策
		完全性対策
		可用性対策
認証	認証	種類
PKI (Public Key Infrastructure)	PKI (Public Key Infrastructure)	PKIの利用
暗号	暗号	暗号方式概説
電子署名	電子署名	必要性と利点
攻撃手法	攻撃手法の概論	
セキュリティプロトコル		
事業継続・災害復旧計画	事業継続管理	概論
フォレンジック		概論
推奨：		
知識項目	大分類	中分類
情報セキュリティ監査	情報セキュリティ監査	情報セキュリティ監査の目的
物理セキュリティ	物理的脅威	

フォレンジック関連では、以下の3職種が上げられている

フォレンジックアナリスト

インシデントハンドラー（組織）

インシデントハンドラー（製品）

・ISEPAとは、「情報セキュリティ教育事業者連絡会」の事で、JNSA傘下で活動

・人材アーキテクチャでは、セキュリティ職種を32種類に分類し、担当業務内容と必要知識・スキルを特定し、知識習得の為の現状存在するトレーニングや資格をマッピングした

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

21

本日のアジェンダ

- 情報セキュリティ専門家に必要な知識・スキル
- (ISC)²概要と提供資格概要
- 各国での人材育成への取組み（当社との関わりの中で）
- サイバー捜査官に必要な知識
- **人材育成―統合的な仕組みの必要性**

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

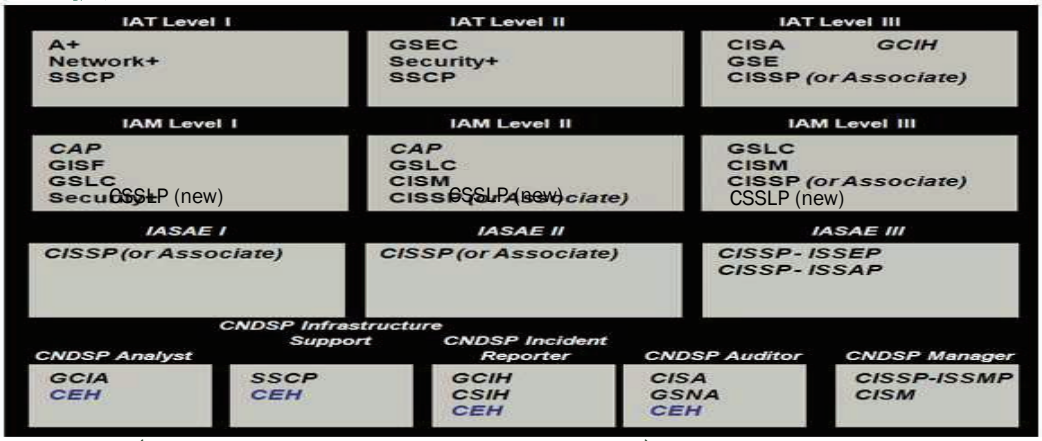
22

8570.1 取得・維持要件

	IAT I-III	IAM I-III	IASAE I-III	CND-A, CND-IS, CND-IR, CND-AU and CND-SPM
初期トレーニング	有	有	有	有
認定の取得 (認定資格リストより)	有 (IAの認定) (6カ月以内)	有 (IAの認定) (6カ月以内)	有 (IAの認定) (6カ月以内)	有 (CND の認定) (6カ月以内)
OJT評価	有 (初期の配属先にて)	無	無	有 (CND-SPMを除く)
CE/Tools認定	有	無	無	有 (CND-SPMを除く)
認定の維持	有 (資格に応じる)	有 (資格に応じる)	有 (資格に応じる)	有 (資格に応じる)
教育継続	有 (資格に応じる)	有 (資格に応じる)	有 (資格に応じる)	有 (資格に応じる)
素行調査	IAのレベルと信用による	IAのレベルと信用による	IAのレベルと信用による	CND-SPのレベルと信用による
特権アクセス 申告書への署名	有	適用外	適用外	有

米国国防総省(DoD) 8570.1

DoDでは、効果的にDoDの情報、情報システム、情報インフラを守るため、十分に訓練され資格を取得した、マネージャ、テクニシャン、コントラクタ、そして、特権的アクセスをもつユーザーなどすべての情報保証を必要とする人材に対し、「DoD 米国国防総省指令8570.1M」を要求しています。対象は職員のみならず納入業者にも拡大



IASAE（Information Assurance System Architect and Engineer）、CNDSP(Computer Network Defense Service Provider)

DoD活用の知識マップ

National Initiative for Cybersecurity Education (NICE)

Security Provision	Information Assurance Compliance	Software Engineering	Enterprise Architecture	Technology Demonstration	Systems Requirements Planning	Test and Evaluation	Systems Development
Operate & Maintain	Data Administration	Info System Security Mgt	Knowledge Mgt	Customer & Tech Support	Network Services	System Administration	Systems Security Analysis
Protect & Defend	Computer Network Defense (CND)	Incident Response	CND Infrastructure Support	Security Program Mgt	Vulnerability Assessment & Mgt		
Analyze	Cyber Threat Analysis	Exploitation Analysis	All-source Analysis	Targets			
Operate & Collect	Collection Operations	Cyber Operational Planning	Cyber Operations				
Oversight & Development	Legal Advice & Advocacy	Strategic Planning & Policy	Education & Training				
Investigate	Investigation	Digital Forensics					

Establishing National Standards

Job

Task/Workrole

Knowledge, Skills, and Abilities (KSA)

参考資料

- サイバー捜査官に必要な知識事例
  - フォレンジックアナリスト
  - インシデントハンドラー（組織）
  - インシデントハンドラー（製品）
- (ISC)² フォレンジック専門家向け資格(CCFP)のご紹介

参考資料

- **サイバー捜査官に必要な知識事例**
  - フォレンジックアナリスト
  - インシデントハンドラー（組織）
  - インシデントハンドラー（製品）
- **(ISC)² フォレンジック専門家向け資格(CCFP)のご紹介**

業務項目＆必要知識ーフォレンジックアナリスト

職種名	フォレンジックアナリスト			
定義	証拠証跡の分析を行い、証拠保全、証拠開示手続きも行う	**所属企業・部署グループ**	サービス・製品提供組織　運用、自社資産保護組織　運用、	
業務項目		**スキル・知識**		
	必須業務：	**必要：**		
	サイバー攻撃、情報漏えいや情報システムの障害等が発生した場合のより迅速かつ的確な対応ができること	知識項目	大分類	中分類
	インシデント対応業務の運用技術や蓄積された経験の共有ができること	情報セキュリティマネジメント	マネジメント概論	セキュリティマネジメントの基本
	攻撃手法の分析結果情報の共有ができること	コンプライアンス	コンプライアンス	法令
	フォレンジック			規格・基準・指針・ガイドライン等（国内）
	OSやアプリケーション等の利用環境の維持ができること			規格・基準・指針・ガイドライン等（国際）
	インシデント対応	フォレンジック		概論
	ネットワーク監視	**推奨：**		
	通信の監視が出来ること	知識項目	大分類	中分類
	IT障害についての分析ができること	ネットワークインフラセキュリティ	ネットワークインフラセキュリティ	概論
	攻撃手法の分析能力の強化ができること	アプリケーションセキュリティ	アプリケーションセキュリティ【Web】	概論
	ファイアウォールのログ等の分析によるサイバー攻撃の予兆把握等ができること		アプリケーションセキュリティ【電子メール】	概論
	実施可能業務：		アプリケーションセキュリティ【DNS(Domain Name System)】	概論
	定常的な評価のスケジュールや評価項目、評価項目選定の趣旨について策定できること	LS	OSセキュリティ【共通】	識別・認証
	サイバー攻撃等に関する脅威/影響度の分析・対処能力を向上させるための機材選定ができること			アクセス制御
	情報セキュリティ対策の製品の選定ができること			システム(データ)の保護
	情報収集、攻撃等の分析・解析、相互連携促進及び情報共有を行う為の体制整備ができること			ユーザ(データ)の保護
	攻撃等の分析・解析機能の洗い出しができること			リソース管理
	コンピュータセキュリティ早期警戒体制の整備ができること			セキュリティ監査
	攻撃手法の分析結果等の情報を適宜提供する為の体制の整備ができること			運用管理
	情報共有体制に対して追加すべき機能・要件等の検討ができること			セキュアOS
	内部統制の仕組みの情報セキュリティの観点からの運用ができること	ファイアーウォール	ファイアーウォール	概論
	情報システムの監視機能、攻撃の分析機能等にIT障害の特徴を迅速に反映させられること	侵入検知	侵入検知	概論
	横断的な監視情報の収集機能がもてること	不正プログラム（マルウェア）	不正プログラム（マルウェア）	概論
	アクセス記録の解析、コンピュータウイルス等の動作検証、電磁的記録の復元等を行う為の資機材の構築ができること	セキュアプログラミング技法	セキュアプログラミング技法	プログラミング言語とツール
	定点観測データの共有ができること	セキュリティ運用	セキュリティ運用	概論
	情報セキュリティに関する情報収集、分析、共有	認証	認証	種類
	情報システムの一元的把握ができること（参照される情報が整理されている）	PKI(Public Key Infrastructure)	PKI(Public Key Infrastructure)	PKIの利用
	教育	暗号	暗号	暗号方式概説
	LS-0, Hyogo-B Hyogo-A, SPIA-T, SPIA-IR, LACB5-14,16, 17, C1, C2, SANS-SEC401, 508, JTP-EHM, SC, CEHRapid	電子署名	電子署名	必要性と利点
	資格	攻撃手法	攻撃手法の概論	
	SSCP、CTIA, SEAj-T、SANS-GCFA	セキュリティプロトコル		
		事業継続・災害復旧計画	事業継続管理	概論
		情報セキュリティ監査	情報セキュリティ監査	情報セキュリティ監査の目的
		物理セキュリティ	物理的脅威	

業務項目＆必要知識ーインシデントハンドラー（組織）

職種名	インシデントハンドラー（組織）			
定義	攻撃発生時のインシデント分析及び対処と関係部署との調整をおこなう	所属企業・部署グループ	サービス・製品提供組織　運用、自社資産保護組織　運用	
業務項目		スキル・知識		
	必須業務：	必要：		
	サイバー攻撃、情報漏えいや情報システムの障害等が発生した場合のより迅速かつ的確な対応ができること	知識項目	大分類	中分類
	インシデント対応業務の運用技術や蓄積された経験の共有ができること	情報セキュリティマネジメント	マネジメント概論	セキュリティマネジメントの基本
	インシデント対応			マネジメントプロセス
	実施可能業務：			関連知識
	災害発生時における対応等、横断的な取り組みと整合性の確保・連携について検討ができること			セキュリティポリシー
	サイバー攻撃等に関する脅威/影響度の分析・対処能力を向上させるための機材選定ができること			リスク分析
	発生頻度の高い個別のIT障害への対応方策を策定できること	ネットワークインフラセキュリティ	ネットワークインフラセキュリティ	概論
	教育	アプリケーションセキュリティ	アプリケーションセキュリティ【Web】	概論
	LS-0, Hyogo-B, Hyogo-A, SPIA-T, IR, SEAJ-T, LACB5-14,16, C1, SANS-SEC401, 504		アプリケーションセキュリティ【電子メール】	概論
	資格		アプリケーションセキュリティ【DNS (Domain Name System)】	概論
	CISSP, CITA, SEAJ-T, SANS-GCIH	OSセキュリティ	OSセキュリティ【共通】	識別・認証
				アクセス制御
				システム（データ）の保護
				ユーザ（データ）の保護
				リソース管理
				セキュリティ監査
				運用管理
				セキュアOS
		ファイアーウォール	ファイアーウォール	概論
		侵入検知	侵入検知	概論
		不正プログラム（マルウェア）	不正プログラム（マルウェア）	概論
		セキュアプログラミング技法	セキュアプログラミング技法	プログラミング言語とツール
		セキュリティ運用	セキュリティ運用	概論
				定常運用時のセキュリティ確保
				インシデント対応
				（異常時対応）
				運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）
		コンテンツセキュリティ	情報の保護	情報の格付け
				保護において留意すべき情報の特徴
				情報の取扱場面（ライフサイクル）
				機密性対策
				完全性対策
				可用性対策
		認証	認証	種類
		PKI (Public Key Infrastructure)	PKI (Public Key Infrastructure)	PKIの利用
		暗号	暗号	暗号方式概説
		電子署名	電子署名	必要性と利点
		攻撃手法	攻撃手法の概論	
		セキュリティプロトコル		
		事業継続・災害復旧計画	事業継続管理	概論
		フォレンジック		概論
		補足：		
		知識項目	大分類	中分類
		情報セキュリティ監査	情報セキュリティ監査	情報セキュリティ監査の目的
		物理セキュリティ	物理的脅威	

業務項目＆必要知識ーインシデントハンドラー（製品）

職種名	インシデントハンドラー（プロダクト）			
定義	プロダクトに確認された脆弱性の分析と関係部署との調整をおこなう	所属企業・部署グループ	サービス・製品提供組織　運用、自社資産保護組織　運用	
業務項目		スキル・知識		
	必須業務：	必要：		
	サイバー攻撃、情報漏えいや情報システムの障害等が発生した場合のより迅速かつ的確な対応ができること	知識項目	大分類	中分類
	インシデント対応業務の運用技術や蓄積された経験の共有ができること	情報セキュリティマネジメント	マネジメント概論	セキュリティマネジメントの基本
	インシデント対応			マネジメントプロセス
	実施可能業務：			関連知識
	災害発生時における対応等、横断的な取り組みと整合性の確保・連携について検討ができること			セキュリティポリシー
	サイバー攻撃等に関する脅威/影響度の分析・対処能力を向上させるための機材選定ができること			リスク分析
	ソフトウェア等の脆弱性の重要度・優先度に係る判断基準の整備等ができること	ネットワークインフラセキュリティ	ネットワークインフラセキュリティ	概論
	発生頻度の高い個別のIT障害への対応方策を策定できること	アプリケーションセキュリティ	アプリケーションセキュリティ【Web】	概論
	情報システムの監視機能、攻撃の分析機能等にIT障害の特徴を迅速に反映させられること		アプリケーションセキュリティ【電子メール】	概論
	教育		アプリケーションセキュリティ【DNS (Domain Name System)】	概論
	LS-0, Hyogo-B, Hyogo-A, SPIA-1R, SEAJ-T, LACB5-14, 16, C1, SANS-SEC401, 504	OSセキュリティ	OSセキュリティ【共通】	識別・認証
	資格			アクセス制御
	CISSP, CTIA, SEAJ-T, SANS-GCIH			システム（データ）の保護
				ユーザ（データ）の保護
				リソース管理
				セキュリティ監査
				運用管理
				セキュアOS
		ファイアーウォール	ファイアーウォール	概論
		侵入検知	侵入検知	概論
		不正プログラム（マルウェア）	不正プログラム（マルウェア）	概論
		セキュアプログラミング技法	セキュアプログラミング技法	プログラミング言語とツール
		セキュリティ運用	セキュリティ運用	概論
				定常運用時のセキュリティ確保
				インシデント対応
				（異常時対応）
				運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）
		コンテンツセキュリティ	情報の保護	情報の格付け
				保護において留意すべき情報の特徴
				情報の取扱場面（ライフサイクル）
				機密性対策
				完全性対策
				可用性対策
		認証	認証	種類
		PKI (Public Key Infrastructure)	PKI (Public Key Infrastructure)	PKIの利用
		暗号	暗号	暗号方式概説
		電子署名	電子署名	必要性と利点
		攻撃手法	攻撃手法の概論	
		セキュリティプロトコル		
		事業継続・災害復旧計画	事業継続管理	概論
		フォレンジック		概論
		補足：		
		知識項目	大分類	中分類
		情報セキュリティ監査	情報セキュリティ監査	情報セキュリティ監査の目的
		物理セキュリティ	物理的脅威	

参考資料

- サイバー捜査官に必要な知識事例
  - フォレンジックアナリスト
  - インシデントハンドラー（組織）
  - インシデントハンドラー（製品）
- (ISC)² フォレンジック専門家向け資格(CCFP)のご紹介

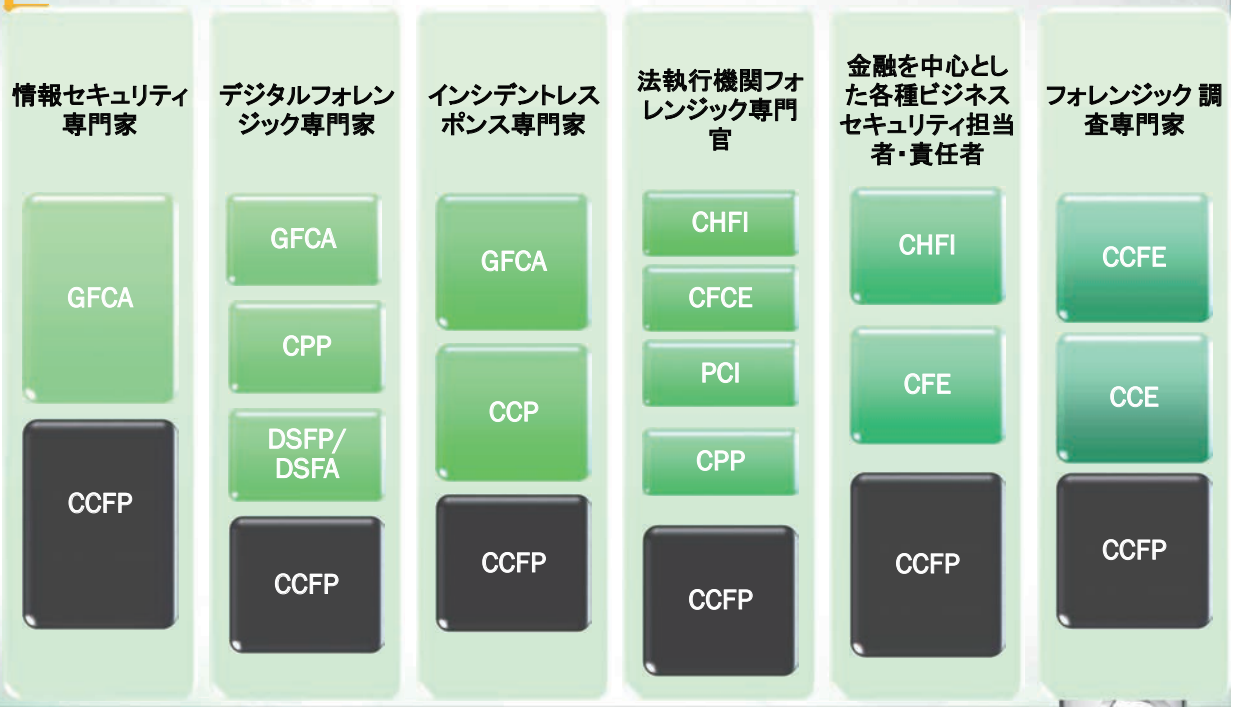
CCFP資格

- Certified Cyber Forensic Professional
- デジタルフォレンジックに関わるプロフェッショナルを認証する資格
- グローバルで通用するデジタルフォレンジックの概念、技術、最適慣行や法体系・規制などへの精通度を測る資格
  - ベンダーフリー、カントリーフリー（各国固有の要件については、モジュールとして追加していく方式　ー2013年米国・韓国版、2014年ヨーロッパ・インド版の開発完了）
- 取得のメリット:
  - フォレンジック技術、プロシージャ、運用に関する標準・基準、裁判所に認められるための、正確、完全かつ信頼性の高いデジタル証拠を確保するための法的および倫理的な原則を理解している事の証明
  - e-discoveryや、マルウェア分析、インシデントレスポンスなどの情報セキュリティ分野にまで適用できる能力の示唆が可能

CCFP資格

- CCFPの6ドメイン
  - Legal and Ethical Principles
  - Investigations
  - Forensic Science
  - Digital Forensics
  - Application Forensics
  - Hybrid and Emerging Technologies
- 受験資格
  - 大学卒＋3年間のフォレンジック業務経験　もしくは6年間のフォレンジック業務経験

CCFP資格　－　競合資格と対象層




ご清聴ありがとうございました
(ISC)2®
INSPIRING A SAFE AND SECURE CYBER WORLD.
(ISC)2
25 years
STRENGTH IN MEMBERSHIP
© Copyright 1989 – 2015, (ISC)2 All Rights Reserved

民間企業における インターン受け入れ例

オラクルにおける警視庁インターンシップの現状

2015年 2月10日

日本オラクル株式会社
データベース事業統括 製品戦略統括本部
テクノロジーディレクター
下道　高志

ORACLE

侵害された資産のタイプで分類した場合のデータ漏洩 / 侵害事例

（ベライゾン社「2012 年度データ漏洩 / 侵害調査報告書」より抜粋）

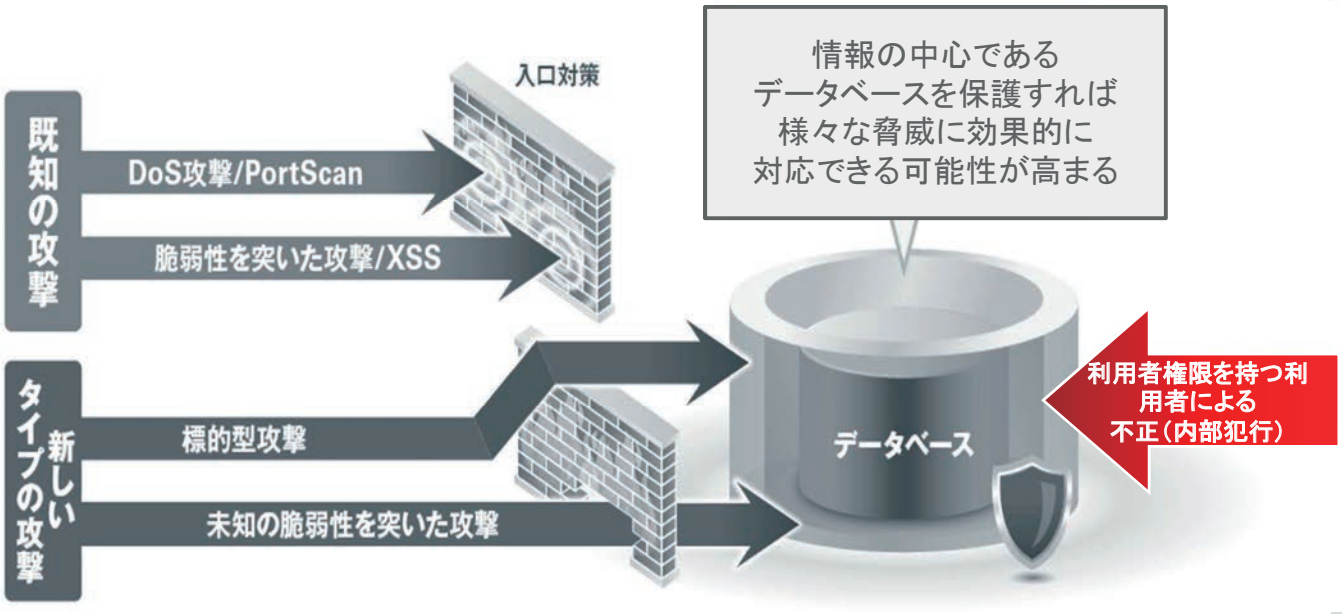
タイプ	カテゴリー	全企業・組織の事例		大規模の企業・組織の事例のみ	
デスクトップ／ワークステーション	ユーザ機器	18%	34%	12%	36%
ウェブ／アプリケーションサーバー	サーバー	6%	80%	33%	82%
データベースサーバー	サーバー	6%	96%	33%	98%
一般従業員／エンドユーザー	人間	3%	1%	5%	<1%
メールサーバー	サーバー	3%	2%	10%	2%
ファイルサーバー	サーバー	1%	<1%	5%	<1%
ノートブック／ネットブック	ユーザ機器	1%	<1%	5%	<1%

（%の説明）
青色：侵入数に対し、侵入の結果実際に漏えいした割合
赤色：企業・組織が持つ全データ数に対する漏えいしたデータ数の割合

ORACLE

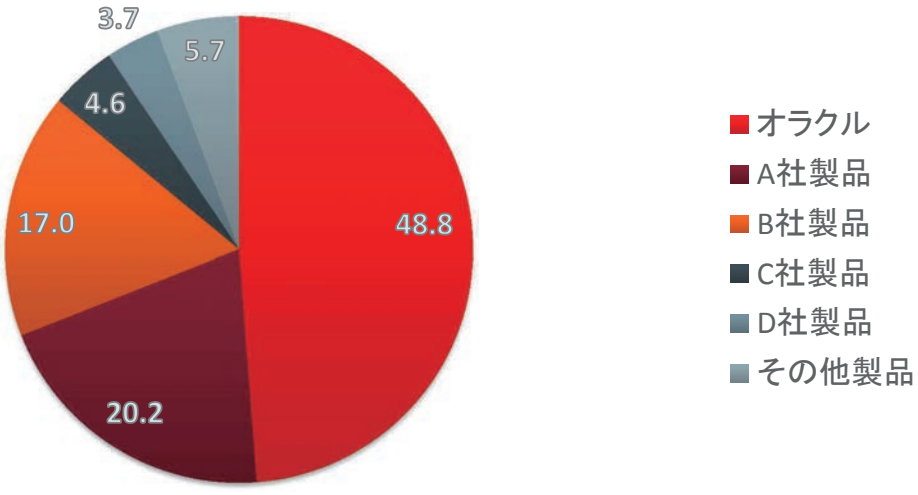
「入口」「出口」対策だけでなく「情報の中心」であるデータベースへの対策も急務

対策が行われている場所を迂回する攻撃が増えている



世界におけるデータベースのシェア

(出所：Gartner 2011 Worldwide RDBMS Market Share Reports)



シェアが高い＝攻撃対象になる割合が高い

警視庁からのインターン受け入れについて

- 人事院が実施している「官民人材交流」に基づき、民間企業がインターン派遣者を受け入れるプログラム
- 警視庁が選抜した若手警察官にIT関連の訓練をするために行っているプログラムの一環
  - 主管は警視庁「サイバー犯罪対策課」（2011年4/1から改称）
  - IT外部研修を修了した警察官の中から、更に優秀な人材を選抜してIT企業に1年間派遣し実習
  - IT企業内での訓練プログラムは受入側企業に任されている
- 研修終了後、サイバー犯罪対策課、各警察署等の関連部署などで活躍。

ORACLE

警視庁からの要請事項

- 企業へのインターンシップ派遣により期待されたこと
  - サイバー犯罪捜査の初動捜査の段階から持つことが有効と考えられるITおよび情報セキュリティに関するスキルの習得
    - 情報セキュリティ技術と関連法制度にかかわる知識
    - 法科学の一部としてIT技術を研究するための一助
  - 企業が持つ技術の動向と人脈
  - 新しい犯罪への対応と、新しい捜査手法確立にむけ、最新の民間動向を知る
  - 企業の風土や考え方、実際にITシステムがどう使われているのか等の知見を習得

ORACLE

オラクルにおけるインターン概要

- 期間1年（4月～3月）
- 捜査員として必要なデータベース技術を身につけることを主たる目的とする
- 複数の部署で、技術取得・実地対応等を経験
- ベンダー側人件費はゼロで実施。オラクルではコントラクター扱いで事務処理

研修概要（1）

- Phase 1（4月～6月）：製品技術部門に在籍
  - オラクルDBを理解し、基本的な操作を習得する段階
    - LinuxとOracle DBがインストール、セットアップできる
    - 基本的なDBA系の設定・管理操作などができる
    - 基本的なSQLが操作できる
    - OSのコマンド操作ができる
  - Big Data Securityに関する基礎知識と製品キャッチアップ
  - 5月末時点でオラクルマスター・ブロンズ取得成功
- Phase 2（7月～9月）：技術サポート部門に在籍
  - DBのインストール、リカバリなどの基礎訓練を実施
  - VPD（仮想化データベース）、標準／ファイングレイン監査など主なセキュリティ機能を習得
  - 必要に応じたOJTと支援

研修概要 （2）

- Phase 3（10月～3月）：コンサルティング部門に在籍
  - パートナー等の研修受け入れに準じた形でOJTと業務アサイン
  - 3月末時点でオラクルマスター・シルバー取得成功
  - Javaを中心としたプログラミング言語習得
  - テーマを決めた継続的な課題研究と成果物作成・部内発表
    - 内部不正による情報改ざん事案を想定した対応方法
- Phase X（随時）
  - 情報セキュリティ関連法律の学習（随時）
    - 不正アクセス禁止法、ウイルス作成罪、刑法改正など関連法令への理解
  - イベント等への参加による人的リレーションや情報セキュリティに特化した知見の習得

インターン派遣者に取得をお願いしている資格

- ORACLE MASTER

  - 日本オラクルがOracleデータベースを中心としたオラクル製品に関する技術者のスキルを認定する制度
  - ORACLE MASTERは、1997年から開始され、2003年には全世界共通の認定資格Oracle Certification Program(OCP)にも準拠し、その技術レベルは世界で認められ、保有者の技術力を保証する客観的な指標として大きな信頼を得ている
  - 現在22万以上のORACLE MASTERが、お客様のビジネスインフラを支えている
  - ITスキル標準(ITSS)に準拠した認定資格である
  - ORACLE MASTERのレベルとITSSの準拠は次の通り
    - Platinum (Level 4) , Gold (Level 3), Silver (Level2), Bronze (Level 1)

地方自治体における事例

ORACLE UNIVERSITY

Oracle University 認定資格採用 事例

株式会社ステーション・ピー
沖縄県宜野湾市

**オラクルの認定資格を取り入れた
官民一体のIT人材育成で地域の雇用を拡大**

Station P

沖縄本島の中南部に位置する宜野湾市では、第3次産業が雇用の86%を占める。同市は、雇用拡大のための施策として重点分野雇用創造事業を展開しているが、なかでも大規模投資を必要としないIT産業は注力分野の1つだ。地域の情報サービス企業である株式会社ステーション・ピー(以下、ステーション・ピー)は、この事業によって人材の確保と育成を実現し、地域の雇用拡大につなげているが、そこで官民のWin-Winの関係構築に貢献しているのがオラクルの認定資格だ。

IT人材の育成を民間に委託し
雇用拡大につなげる

インキュベーション施設として宜野湾ベイサイド情報センターをオープンするなど、地域のIT産業を後押ししている。まにつなげるのがこの事業の狙いだ。
宜野湾市では企業に必要とされる人材に関するヒアリングをおこない、そ

今後、配慮をお願いしたい項目

- ベンダー内だけでなく幅広い外部研修を同時に
  - 製品技術だけの取得でなく、法制度や社会動向に関する知識も同時に学ぶ方が、学習効果がより高いと思われる
    - 点のセキュリティ技術だけでなく、多面アプローチの情報セキュリティ全般を学ぶことが、中核捜査員育成に資すると考えられる
- インターン後のキャリア
  - 取得した技術を実践する環境の整備
    - サイバー犯罪対策として、データベース関連知識と技術を継続的に取得・実践する環境が必要
    - 日本には高度なデータベース技術者・管理者も数多く、引き続き増えています。これは犯罪予備軍も増加することを意味するので、より多くの捜査員に同技術を身につけていただくことを切望します

Hardware and Software
Engineered to Work Together

Microsoft

総合セキュリティ対策会議

日本マイクロソフト：警視庁との交流プログラム

2015年２月10日

日本マイクロソフト株式会社
片山建

警視庁との研修プログラム

- 2010年4月より
  合計10名
- 1年間のプログラム
- 1か月のイントロ
- ５か月～６か月：ネットワーク・プログラミング
- ５か月：製品などセキュリティ研修

研修内容

- ネットワーク関連
- プログラミング
- 製品などセキュリティ研修

成果

- Forensic Guide
- Digital Crime Consortiumなど国際会議への参加
- 覚書

さらに充実した研修のため

- 事前研修の重要性
- 「研修卒業生」の受け入れ先の啓発活動の重要性

Microsoft