IIJ Internet Initiative Japan

セキュリティ人材育成の教育プログラム開始について

IIJセキュリティ教習所のご紹介

安全をあたりまえに
wizSafe

2021/12/20

セキュリティ本部セキュリティビジネス推進部
セキュリティオペレーションセンター

セキュリティ人材の不足について

経済産業省　「サイバーセキュリティ体制構築・人材確保の手引き」より

（2）「セキュリティ人材」の不足について

企業規模等によっても異なりますが、ユーザー企業でセキュリティ対策の中心となるのは、「セキュリティ統括」分野や「セキュリティ監視・運用」分野等のセキュリティ関連タスクを担うセキュリティ人材です。一方で、情報処理推進機構（IPA）が実施した「CISO 等やセキュリティ対策推進に関する実態調査」[34]によると、日本のユーザー企業で専任の CISO 等の設置状況は 7.5%、CSIRT に 1 名以上の専任のメンバーを配置している企業は 31.1%となっており、多くの場合は他の業務との兼務となっているのが実態です。また、以下は JUAS 調査におけるセキュリティ体制に関する課題のアンケート結果ですが、マネジメントレベル及び実務レベルの「セキュリティ人材」の量的・質的不足が最も大きな課題となっていることが見て取れます。

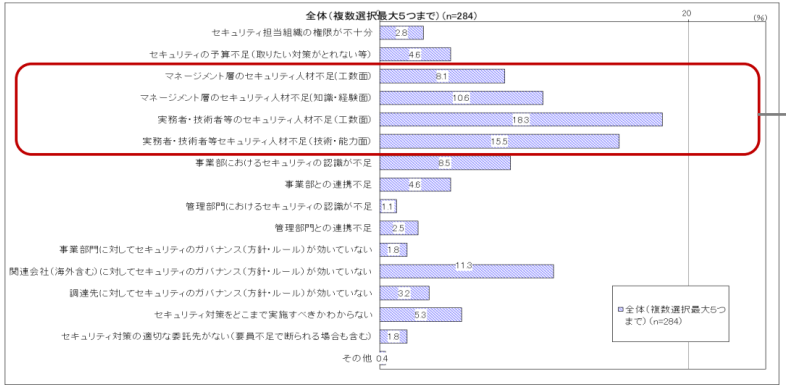


図 23　セキュリティ体制に関する課題（JUAS 調査）

マネージメント層のセキュリティ人材不足（工数面）
マネージメント層のセキュリティ人材不足（知識・経験面）
実務者・技術者等のセキュリティ人材不足（工数面）
実務者・技術者等のセキュリティ人材不足（技術・能力面）

・「サイバーセキュリティ体制構築・人材確保の手引き」（第1.1版）（METI/経済産業省）
https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html

セキュリティ統括人材の確保におけるポイント

安全をあたりまえに wizSafe

経済産業省　「サイバーセキュリティ体制構築・人材確保の手引き」より

表 13　セキュリティ統括人材の確保におけるポイント（企業から得られた意見）

担当業務へのモチベーション	• 限られたリソースの中で自らセキュリティ施策を考え、経営とコミュニケーションしながら事業の安全を実現する達成感 • 「この会社を守りたい」という強い意志とセキュリティへの「やる気」
求められる知識・スキル	• 自社のビジネスの視点から俯瞰的にリスク管理や判断ができる能力 • 理想だけでなく現実解を考えられるバランス力 • 社内外の様々な人と連携しながら経営や事業部門の行動を促すコミュニケーション力 • システム・情報の流れなど自社の仕組みの熟知 • 求められるセキュリティ知識は高い専門性よりも幅広さ • 資格は押さえるべきポイントの把握や知識の棚卸として有効だが、最も期待されているのは知識やスキルを「使いこなす力」 • セキュリティ管理者に必要な能力はコミュニケーション能力、経営センスを持ち経営者に分かりやすく説明できる能力（管理者でも最低限のセキュリティ知識は必要） • 投資判断をするためのセキュリティ技術への理解（攻撃手口の理解等） • 英語を含めた海外とのコミュニケーション能力
育成方法	• ローテーションによって幅広い経験から自社の仕組みを体得する • インフラシステムの経験は自社の仕組みを体得することにつながる • 自分の事業として痛みを感じながら経験を積むことが人を育てる • インシデント対応や報告などの「訓練」はスキルアップに有効 • セキュリティに関するコミュニティに積極的に参加することで、「やるべきこと」が磨かれる
採用	• ユーザー企業にフィットした即戦力人材の確保は困難 • 採用後長い目で自社なりの育成を模索することも必要 • 経験豊富なシニア人材の活躍が人材確保の切り札になる
配置	• マネジメントと専門技術の両方に通じたスーパー人材がいなくともチームでの対応も可能 • 組織機能としてこれらの役割をはたせる配置になっていることが大切

- 資格は押さえるべきポイントの把握や知識の棚卸として有効だが、最も期待されているのは知識やスキルを「使いこなす力」

- インシデント対応や報告などの「訓練」はスキルアップに有効

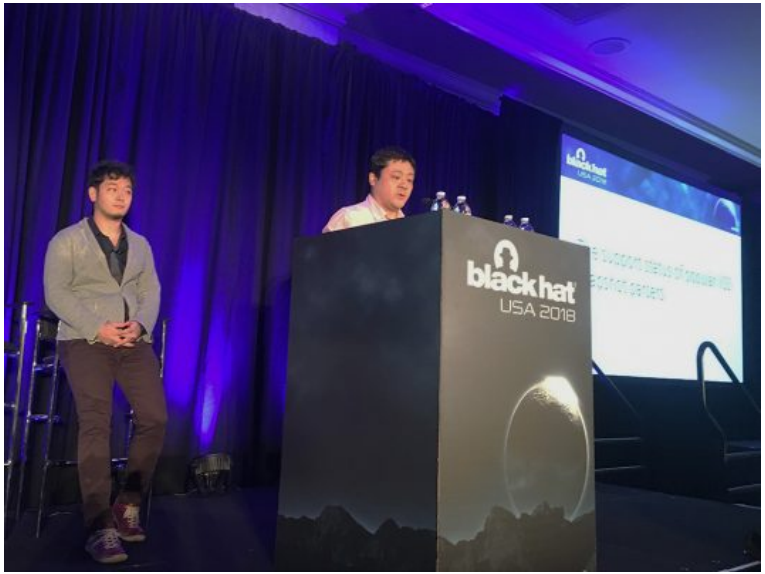
- 採用後長い目で自社なりの育成を模索することも必要

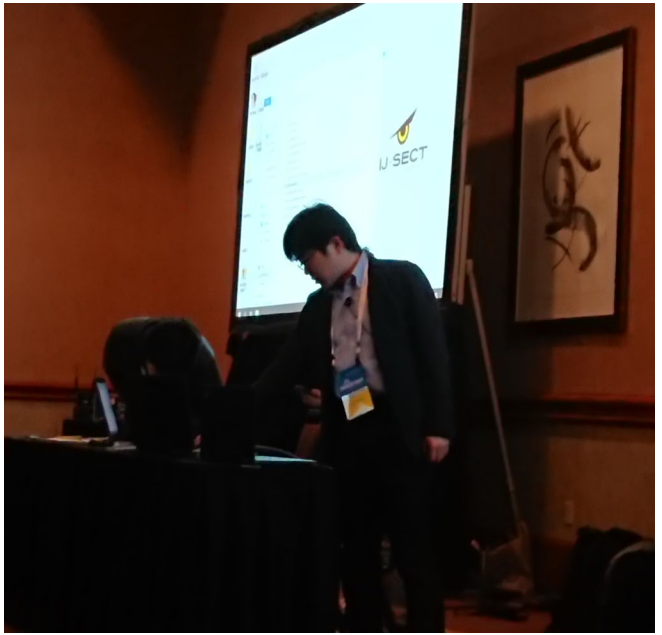
・「サイバーセキュリティ体制構築・人材確保の手引き」（第1.1版）（METI/経済産業省）
https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html

IIJのセキュリティ人材育成支援に関する活動①

Black Hat USA 2018（以降含む）、Black Hat Japan Trainings 2019など多数のイベントでトレーニングや講演を実施

- デジタル・フォレンジックとマルウェア解析の総合演習を中心に、高度なトレーニングの機会を多数提供。





IIJのセキュリティ人材育成支援に関する活動②

安全をあたりまえに wizSafe

IIJは兵庫県警察様、島根県警察様、北海道警察様のサイバー捜査官育成に2017年から貢献

IIJ、兵庫県警察サイバー捜査官の育成を支援

2017年3月8日

➤ このニュースのPDF版 [156KB]

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：勝 栄二郎、コード番号：3774 東証第一部）は、警察のサイバー空間の脅威への対処能力向上を目的として、2017年4月1日付で、兵庫県警察本部警備部公安第一課の捜査官をIIJセキュリティオペレーションセンター（SOC）にて受け入れることとなりましたのでお知らせいたします。

IIJでは、2015年6月に兵庫県警察本部長の委嘱を受け、当社のセキュリティ情報統括
県警察サイバーセキュリティ対策アドバイザー」に就任し、セキュリティに関する情
策や事案対応への助言等を行ってまいりました。

このたび新たな人材育成支援として、2017年4月1日から2018年3月31日までの1年間
研修生としてSOCにて受け入れる協定を2017年2月21日に締結いたしました。膨大な
するための施設であるSOCでの業務を通じて、ウイルス解析、デジタルフォレンジッ
連事案の捜査に有用な知識、技術の向上を支援してまいります。

IIJ、島根県警察サイバー捜査官の育成を支援

2018年9月18日

➤ このニュースのPDF版 [147KB]

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：勝 栄二郎、コード番号：3774 東証第一部）は、サイバーセキュリティ分野における警察の対処能力の向上を目的として、2018年10月1日付で、島根県警察本部生活安全部生活環境課のサイバー捜査官をIIJセキュリティオペレーションセンター（SOC）（※）に受け入れることとなりましたので、お知らせいたします。

お客様に安心・安全なICT環境を提供するための取り組みとして、IIJではセキュリティ専門の人材育成を事業の一つの柱と位置付けています。この度、人材育成における新たな支援として、同県警察から研修生1名を2018年10月1日から3ヵ月間受け入れる協定を2018年9月18日に締結いたしました。膨大な情報から脅威や攻撃のリスクを迅速に検知・対処するための施設であるSOCでの業務を通じて、ウイルス解析、デジタルフォレンジックなどの技術を習得してもらうことで、サイバー関連事案の捜査に有用な知識、技術の向上を支援してまいります。

IIJでは、2017年5月より島根県警察の委嘱を受け、当社のセキュリティ本部長 齋藤衛が「島根県警察サイバー犯罪対策テクニカルアドバイザー」に就任し、サイバー犯罪捜査および対策に必要な専門知識や技術に関する助言および教育、最新の情報通信技術等の情報提供、被害防止のための広報啓発活動に関する助言などを行っております。また、同年4月より兵庫県警察のサイバー捜査官を継続して受け入れています。

IIJ、北海道警察に協力し、サイバー捜査官の育成を支援

2019年7月1日

➤ このニュースのPDF版 [300KB]

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：勝 栄二郎、コード番号：3774 東証第一部）は、サイバーセキュリティ分野における警察の知見向上を目的に、本日付で、北海道警察本部生活安全部サイバー犯罪対策課の捜査官
（※）に受け入れることとなりましたので、お知らせいたします。

めの取り組みとして、国内で不足するセキュリティ人材の育成を推進しています。
大な情報から脅威や攻撃のリスクを迅速に検知・対処するセキュリティアナリスト
高度な技術、専門性を有するセキュリティ人材を育成しています。

E7月1日から3ヵ月間、北海道警察から研修生1名を受け入れる協定を2019年6月26
グラムを、素養に応じて受講することにより、ウイルス解析、デジタルフォレン
術を習得してもらうことを目指しています。

セキュリティの最前線で培った確かな実績とノウハウを基に実践力の高い知識・スキルを習得できるプログラムを提供

体系的なプログラムで セキュリティ人材育成を支援

基礎知識から実践を踏まえた応用知識まで、体系的に学べるプログラム。インシデント発生時に適切な判断・対処が行えるセキュリティスペシャリスト育成を支援します。
マルウェア解析やフォレンジックなど、高い知識やスキルが求められる手法を習得する高度プログラムも提供する予定です。

現場ですぐに使える 知識・スキルを習得可能

IIJ SOCの対応事案や、サービス運用の経験ノウハウを基にプログラムを提供。
机上の学習だけでなく実践を想定した演習により、実際の対応時にすぐに役立てられる知識・スキルが身に付きます。

最前線で活躍する IIJセキュリティ専門家が 講師を担当

IIJが提供する各種サービス・ソリューションで実際にインシデント対応支援やサービス運用を行っている担当者が講師を務めます。
最前線で活躍するIIJセキュリティ専門家から直接学ぶことができます。

「IIJセキュリティ教習所」名前に込めた想い

自動車の教習所は…

座学などから
得られる知識

＋

実務や演習などから
得られる技能

➡

運転免許発行

サイバーセキュリティも同様です。
高度化する脅威に対処するために企業の情報システム部門のセキュリティ担当者やCSIRT部門担当者は、セキュリティ知識に限らずITに関する「知識」を学んだ上で、実際の現場で対処するために必要となる「技能」を身に着ける必要があります。

IIJセキュリティ教習所　提供プログラムについて

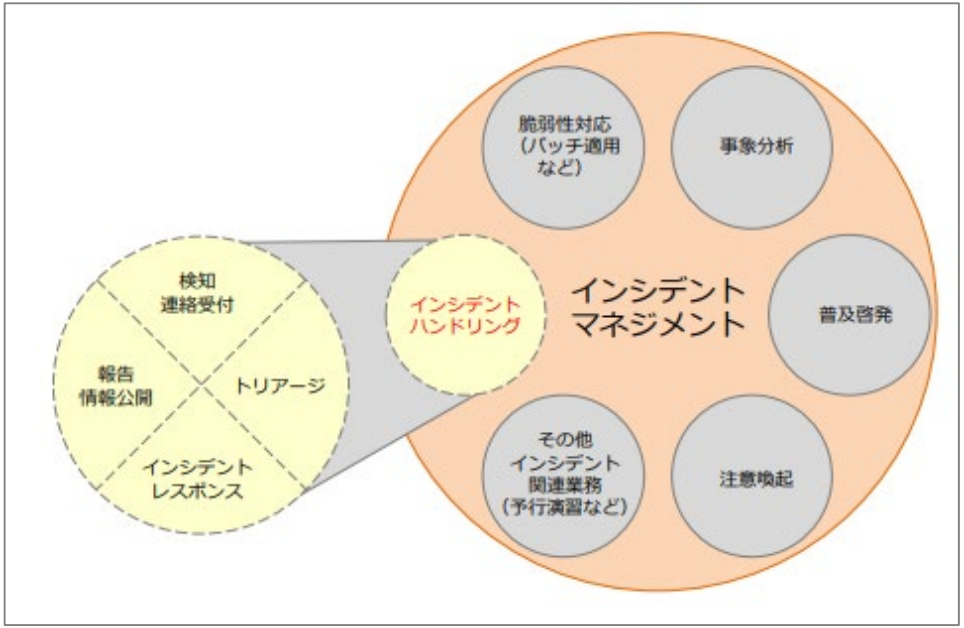
安全をあたりまえに wizSafe

役割・レベルに応じた複数のプログラムを提供予定。
第一弾はインシデントハンドリング実践コースをご提供

役割	 ・自組織内外連絡担当 ・情報発信担当 ・リーガルアドバイザー	 ・リサーチャー ・セキュリティ戦略 ・脆弱性診断士 ・セルフアセスメント	 ・コマンダー ・インシデント管理・処理 ・フォレンジック ・マルウェア解析	 ・IT戦略・システム企画 ・基幹システム構築・運用・保守 ・インフラ構築・運用・保守 ・サポート・ヘルプデスク
高度			マルウェア解析 フォレンジック	
応用	セキュリティ マネジメント セキュリティリスク コンプライアンス		パケット/ログ解析 インシデントハンドリング実践コース 攻撃技術理解・防御 APT対策基礎コース（仮称、2022年3月 提供開始予定） 脆弱性診断・管理 セキュアシステムデザイン	
基礎	セキュリティ基礎			

インシデントハンドリングとは

CSIRTがインシデントに対して行う活動全般をインシデントマネジメントといい、その中で、インシデント発生時から解決までの一連の活動をインシデントハンドリングといいます。



https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf
「インシデントハンドリングマニュアル」より抜粋

インシデントハンドリング実践コースの特徴

安全をあたりまえに wizSafe

講義の半分以上が実習の超実践型カリキュラム
情報処理安全確保支援士（登録セキスペ）の特定講習として認定済

実施形式	疑似インシデント対応をチーム演習形式で行います
提供内容	1. 最新セキュリティ動向について 2. インシデントハンドリングの流れと実践（ログ解析や切り分け作業） 3. 実践内容の振り返り
習得できる 知識・スキル	IIJセキュリティオペレーションセンターで実際に対応したインシデントを基に構築した疑似インシデントへの対応を通し、インシデントハンドリングに要求される知識やスキルを習得できます。 • インシデント発生の連絡からクローズまでの対応方法 • インシデント発生時の適切な初動対応方法 など
開催概要	• 料金　　：8万円/人（税込） • 研修期間：1日間 • 定員　　：4名～ • 実施場所：インターネットイニシアティブ 本社（飯田橋グラン・ブルーム） • 開催日時：弊社ホームページで公開（第1回は2022年1月21日（金）開催予定） • 対象：法人及び個人の両方を対象。特定講習ですが、登録セキスペの有無は問いません。

登録セキスペの特定講習について

特定講習は、法第26条において、独立行政法人情報処理推進機構の行うサイバーセキュリティに関する講習と同等以上の効果を有すると認められる講習として経済産業省令で定めるものとなっています。これを受けて、情報処理の促進に関する法律施行規則（平成28年経済産業省令第102号、以下「規則」という。）第34条第2項においては、同項に掲げる基準のいずれにも該当する講習として、経済産業大臣が定めるとしています。

引用元：https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html

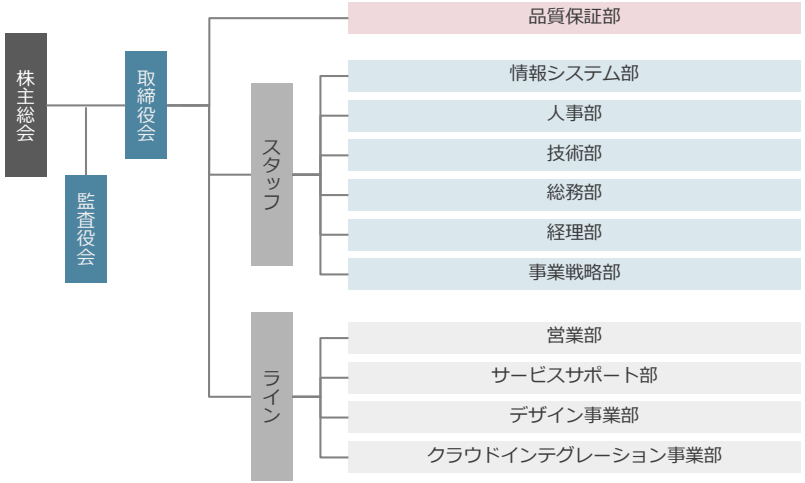
- 登録セキスペでは、「実習」「実技」「演習又は発表を伴う演習」を、3年に1度受講する必要があります。
- この講習のうち、IPAが行う講習を「実践講習」、民間事業者等が行う講習を「特定講習」といいます。
- 特定講習は上記で定められた講習となり、弊社インシデントハンドリング実践コースは特定講習番号「21-007-022」として認定されています。

ケーススタディ例

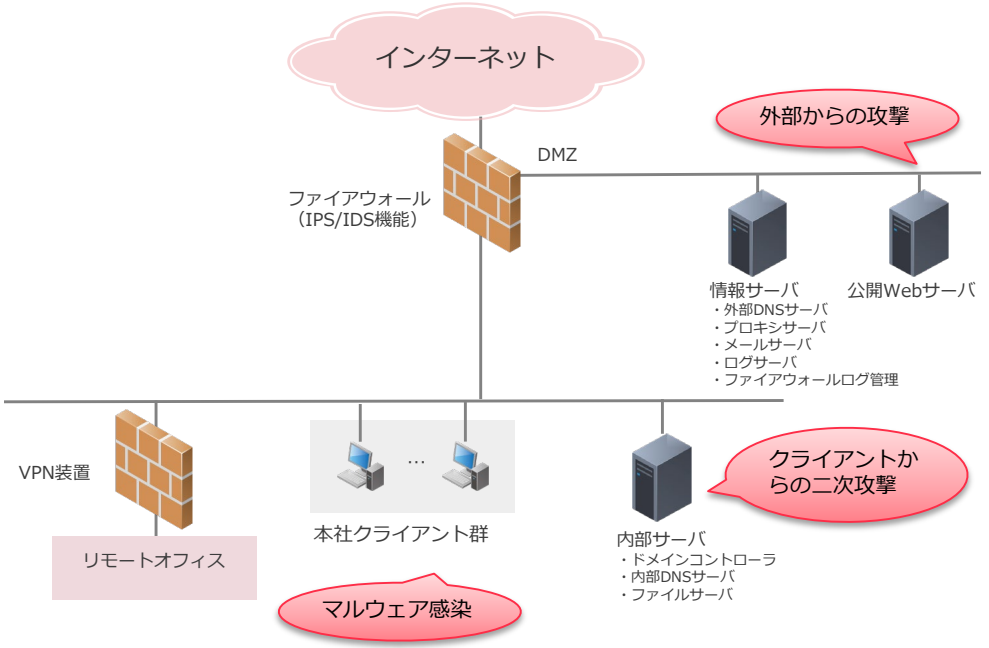
安全をあたりまえに wizSafe

仮想企業のCSIRT担当として端末感染や公開サーバへの攻撃など複数の事案に対応

仮想企業（組織図）



システム構成図



インシデントハンドリング実践コース当日のスケジュール

10:00	事務連絡（注意事項、会場案内、目的など）
10:15	講義（倫理、インシデントハンドリング）
11:00	実習環境の説明・実習の進め方
11:45	昼休み
12:45	実習（ケース1～3）：各ケース90分
17:15	グループワーク
17:35	アンケート
18:00	終了

第1回インシデントハンドリング実践コースの募集に関するお知らせ

安全をあたりまえに wizSafe

本日（12/20）よりコンテンツを公開、参加者の募集を開始
第1回は1月21日実施予定。

詳細は本日公開の弊社ホームページ

https://www.iij.ad.jp/svcsol/security-education/

をご参照ください

安全をあたりまえに wizSafe

設備 / 講師・スタッフの対応について

•感染防止を考慮の上、受講者の座席を配置します。
•会場設備（ドアノブ、机、椅子等）及び使用する機材類（PC、マイク等）を定期的に消毒します。
•定期的にドアの開放による換気を実施します。
•手指消毒用アルコール及び除菌用シートを常設し、必要時にすぐにご利用いただけるようにします。
•講師・スタッフは、手洗い、うがい、手指消毒、マスク着用等の感染防止対策を行い、日常の体調管理に努めます。
•講師・スタッフは、講義実施前に検温実施の上、講義中はマスクを着用します。

まとめ

- IIJセキュリティ教習所は、最新のセキュリティ動向や実習が盛り込まれたプログラムを体系的に提供することで、お客様の安全を実現するために人材育成・トレーニングの面から貢献してまいります。

- 第1弾「インシデントハンドリング実践コース」は本日より募集開始、開催は1月21日となります。

- 第2弾「攻撃技術理解・防御 APT対策基礎コース（仮称）」は2022年3月に参加者の募集を開始する予定です。

wizSafe

安全をあたりまえに