isepa 情報セキュリティ教育事業者連絡会
Information Security Education Providers Association

情報セキュリティ人財アーキテクチャガイドブック

2009年度版

2009年8月
情報セキュリティ教育事業者連絡会

isepa 情報セキュリティ教育事業者連絡会
Information Security Education Providers Association

情報セキュリティ人財アーキテクチャガイドブック

2009年度版

2009年8月
情報セキュリティ教育事業者連絡会

発刊に当って

不況の時こそ新３Ｋを

2月3日に情報セキュリティ政策会議が開催され、第2次情報セキュリティ基本計画が公開されました。特筆すべきは第1次情報セキュリティ基本計画では「事故ゼロ」を目標とする政策が推進されましたが、第2次計画では「事故前提社会」と記載されたことでしょう。これはインターネットが社会インフラとして広く普及したことに起因すると思います。

単純比較ではお叱りを受けるかと思いますが、自動車を見てください。交通のインフラとして広く普及すると共に、残念ながら交通事故で死亡する方は年間約6000人と言われます。便利な反面、事故を起こせば人命を奪ってしまうのが自動車です。その為に社会インフラとして国が道路や法律、警察による運転免許の発行、違反者の取り締まりなどの環境整備を行い、自動車会社は衝突安全性の向上などに人命に配慮した研究開発に努め、学校では交通安全教室など教育で児童に交通ルール遵守を教え、保険会社は損害保険により自動車社会を支えています。つまり事故前提社会として成熟してきていると言えます。

インターネットに目を向けると増加する不正アクセスや情報漏洩もさることながら、ネットを利用した大麻や児童ポルノ販売などの違法行為、プロフへの書き込みによるネットいじめに起因する児童の自殺など目を覆いたくなるような事案も少なくありません。

情報セキュリティ確保には場当たり的な対症療法ではなく、事故前提社会と捉え官民が一体になり推進する必要があると思います。

第2次計画では情報セキュリティ人材育成についても官民一体となって推進すると記載されています。情報セキュリティ教育事業者連絡会（ISEPA）では人材を財産ととらえ人財と定義して、人財育成推進に関わる取組みを業界横断的に実施すると共に、幅広く情報発信を行っております。

ご支援を頂いている業界関係者の皆様に、この場をお借りしてお礼を申し上げます。

不況は底を打ったと報道されるようになりましたが、民間企業では様々なコスト削減を徹底して実施しています。真っ先に削られるのが経費（交際費、交通費）、研究開発費、教育研修費の３Ｋだと言われます。しかしながら不況の時ほど米百俵の精神で人材育成を行うべきではないでしょうか。ご存知の方も多いと思いますが、米百俵とは長岡藩の支藩である三根山藩が百俵の米を窮状に喘ぐ長岡藩に送った時のこと、当時の長岡藩大参事である小林虎三郎は、百俵の米を皆に分け与えることはしなかったそうです。困窮のあまり怒り狂った家臣達が刀を振りかざして「米をだせ！」と詰め寄った時に、小林虎三郎は「百俵の米なんぞ、皆で食ってしまえばそれでおしまいである。それよりこの米を売って得た金で明日の長岡を救う若者を教育しようではないか、そうすれば何千何万俵になってかえってくる」と藩士を説いたそうです。

どんなに良いシステムを導入しようとも、どんなに良いコンサルタントが頑張っても情報セキュリティを確保する主体は、そこで働く人なのです。不況のときこそ「雇用の確保」「研究開発」「教育研修」新３Ｋが必要ではないでしょうか。

企業経営が厳しい中ではありますが、人は城、人は石垣、人は堀と申します。経営者の皆様には是非とも情報セキュリティへのご理解と人財育成の為に必要な教育研修費を確保頂けますようお願い致します。

2009年8月
情報セキュリティ教育事業者連絡会（ISEPA）代表
株式会社ラック　与儀　大輔

目次

はじめに

情報セキュリティ対策は、官民挙げての取組み推進の結果、リスクマネジメントのコンテキストの中で、内部統制管理や事業継続管理と同様に経営課題としての認知が定着してきた。

しかし、情報セキュリティ対策のためには、物理的、技術的、人的、組織的の各々の側面からの対策が必要と言われる通り、多方面からの複合的取組みが必要となる。特に技術面においては、ネットワーク知識、情報システムや情報技術（IT）資源の管理や、それらへのアクセス・利用の管理といった専門知識が必要であり、更にネットワークプロトコルやプログラムの脆弱性を悪用する仕組み、攻撃手法についての知識や対応経験が必要となる。このために情報セキュリティの管理や対策ができる人材は限られ、需要と供給のアンバランスが発生している。このことを踏まえ、セキュアジャパン2009では「情報セキュリティ人材の育成・確保」が重点テーマとして掲げられ、「民間の資格や教育の周知」が政策課題として位置づけられている。

情報セキュリティ教育事業者連絡会（ISEPA）では、情報セキュリティ人財育成にかかわる課題の整理に取り組んできた。その中で、1）企業の中でどのような業務が必要とされているか、2）各業務について、どのような知識、スキル、経験が必要となるか、3）情報セキュリティのスキルを持った人材はどのように処遇されどのようなキャリアパスが描けるか、といった課題に関して、共通認識として整理された体系がない、という問題が存在していることが確認できた。そこで、発足2年目となる2008年度の活動テーマとして、これらの点を整理して「スキルの見える化」を行い、その成果を「情報セキュリティ人財アーキテクチャ」としてまとめる取組みを行った。

ここに掲載するのは、その初年度の活動成果である。「人財アーキテクチャ」は、情報セキュリティについて、組織モデル、職種定義、知識・スキルマップを組み合わせてマップ化した。その結果、企業においてどのような組織でどのような職種が必要であり、その職種はどのような業務を引き受けるのか、それら業務を実施するためにはどのような知識・スキルを身につけていることが必要かを体系的に整理することができた。またキャリアパスモデルも作成して、情報セキュリティに従事する人材にはどのようなキャリアパスの可能性が存在し、就業や昇進の機会が展望できるのかを知る参考資料として整備した。

さらに、それらの知識・スキルを身につけるための教育機会についても、ISEPA会員団体が提供する資格や教育コースを中心に紐付けを行った。その結果、人材を育成する立場、活用し処遇する立場、情報セキュリティ業務のスキルを磨き就業を目指す立場、の各方面に参考としていただけるマッピングを作成できたと考えている。「情報セキュリティ人材の育成・確保」に取組む行政の立場も含め、企業、個人からの参照用に提供したい。

今回まとめたものはその第一版である。技術は絶え間ないイノベーションの渦中にあり、職種、業務は進化する。教育カリキュラムも資格体系もまた変化するものであるので、そのマッピングもまた進化する必要がある。ISEPAでは、カバーする資格や教育機会の充実も含めて改良改版に継続的に取組み、よりよいものを提供していきたいと考えている。

本書のねらいと意義を理解いただき、多方面で活用していただけることを期待している。

巻頭インタビュー

我が国の情報セキュリティ人財像と、ISEPAに期待すること

内閣官房情報セキュリティセンター（NISC）
情報セキュリティ補佐官 **山口　英** 氏

聞き手
情報セキュリティ教育事業者連絡会（ISEPA）
代表 **与儀　大輔**

我が国の情報セキュリティ人財像と、ISEPAに期待すること

内閣官房情報セキュリティセンター（NISC）
情報セキュリティ補佐官 **山口　英** 氏

聞き手　情報セキュリティ教育事業者連絡会（ISEPA）
代　表 **与儀　大輔**

与儀：セキュア・ジャパン2009では「情報セキュリティ人材の育成・確保」が重点テーマの一つに掲げられました。ISEPAでは、2008年度に「人財アーキテクチャ」を開発し、このほど「人財アーキテクチャガイドブック」として発刊する運びとなりました。

そこで今日は、日本の情報セキュリティ政策の立案推進の中核である内閣官房情報セキュリティセンターの山口情報セキュリティ補佐官に、日本における情報セキュリティ人材に求められるもの、そのあり方、育成・確保のために何が必要か、等についてお話を伺いたいと思います。どうぞよろしくお願いします。

資格の作り込み＝ニーズマッチングと成熟度

与儀：ISEPAでは、情報セキュリティの教育事業者が中心となって連係し、民間の情報セキュリティ資格の普及と教育・人財育成の拡大に取り組んでいるのですが、不況の影響もあり、事業者各社は厳しい状態が続いています。やはり費用執行をするにあたって経営層の理解がまだまだ低い現状で、セキュリティの位置づけは、それ自身が付加価値を生むのではなくていわゆる保険的だ、と思っている方が意外に多いと実感しています。情報漏洩事故などが多発する中、利益を滅失させないためにもセキュリティ人財を育成する必要があるよ、と訴えてはいるんですが、情報セキュリティ人材を増やしたら利益も増えるのかと言う人が多いのも事実です。

山口：例えばベンダー資格であるCCNA[1]やMCSE[2]を見てみると参考になるのではないかと思います。これらの資格は、製品の普及に伴いエンジニアの教育が必要不可欠であることから、マーケットにおける人材のニーズを分析し、グローバルな意味とローカルな意味をちゃんと考えてつくられてきたように感じます。また、講師育成も行い、マーケットニーズに合わ

1. Cisco Certified Network Associate
2. Microsoft Certified Systems Engineer

せて普及を進め、10年程経ってようやくうまくいき始めている。現在のISEPA関係の、民間団体が推進しているセキュリティの資格に関しても、ニーズマッチができているか、グローバライズ・ローカライズへの注意をはらっているのか、エスカレーションのモデル資格の体系等について設計できているか、という点について再点検が必要だと思います。

与儀：はい。確かに資格制度の体系化や見える化は必要であると感じておりますし、事故前提社会の対応力強化に人財育成は必要不可欠であると思います。

山口：セキュリティ・リスクマネジメント分野の観点でのマーケットとの整合性をよく考えて展開するのが第一歩ではないでしょうか。例えばCISSP[3]やCISA[4]などは世界で普及・展開していますが、日本国内への適合のためには、民間での競争環境における切磋琢磨の中でもう少し検討が行われる必要があるのではないかとも思います。

是非そこを頑張ってほしいという意味も込めてISEPA発足の際に内閣官房情報セキュリティセンターも後援団体になって、色々な形で意見交換を継続してきたと思います。マーケットにおいて必要とされているものに対して各資格制度がどのように合わせていくのかという議論と、政府機関で活用してくれと言うなら政府のニーズに本当に合っているのかの点検が必要でしょう。その中で需要側と供給側の対話という構造が生まれてくることが大事だと思います。その対話を通して、よりよい資格制度が生まれてくれば、一歩進んで資格の積極活用という道も、企業等に見えてくるでしょう。

与儀：そうですね。セキュリティもITの一部分で必要不可欠になって来た今は、資格制度は更に成熟していかないといけないですからね。

資格の見える化

与儀：その中でセキュア・ジャパン2009などでも記載がありますが、保有スキルの見える化ということを言われています。資格は保有スキルを客観的に証明するツールという位置づけもあり、どの資格を取ったら何ができるのか、とか、この仕事のためにはどの資格が最適なのか、とかを見える化する必要があると考えています。またキャリアとの紐付けも必要でしょう。例えばCISO[5]になるにはどのようなキャリアパスが存在し、必要スキルは何なのか、それを得る為に必要な教育と資格は何かなどです。

そこで、ISEPAでは「情報セキュリティ人財アーキテクチャ」というものを作りました。キャリアステップ・キャリアパスというものと、職種に紐付いてその人が何をインプットされて何をアウトプットするか、どの資格はどんなスキルセットを保証し、どのような職種に対応可能か、これらの対応付けをする。そしてキャリアパスモデルも組み立てて、スキルと資格と仕事とキャリアパスの関係の見える化をするというものです。業務もかなり細分化してキャリアパスも一本の道だけではありませんから、いわゆる役に立つガイドを出そうとしているのです。

山口：共通のフレームワークを作ろうとするのは良い試みですね。ISEPAの事務局機能を支えているJNSA（日本ネットワークセキュリティ協会）では情報セキュリティプロフェッショナル教科書[6]も執筆されましたね。情報セキュリティ人財アーキテクチャのように枠組みを提示して見える化を進めることは大変素晴らしい活動だと思います。スキルセットに対しての、分類とか仕事との紐付けとか、コンピテンシーの定義とか、多角的に利用可能なフレームワークができてくるとより見えやすくなります。

今、結局いい資格なら国の資格、民間の資格にかかわらず、適切に評価されようとしています。国の資格と民間の資格の垣根は下がってきていると感じています。頑張ればさまざまな形で社会認知はされていくのではないかと思いますよ。

そのためには教育や資格取得で何が達成されるのかについて、是非分かりやすい形で提示していただければと思います。それからどういう特徴があるか、例えば継続教育の有無、幅広いセキュリティの中でもどういう領域に対して重点化

3. Certified Information Systems Security Professional
4. Certified Information Systems Auditor
5. Chief Information Security Officer
6. 情報セキュリティプロフェッショナル教科書　㈱アスキー・メディアワークス刊

しているかということなどについて、明らかにしていくことが大切です。今、ISEPAの皆さんがそのようなことを考えて進めてくれるというのは新たなチャレンジであり、とても大変だと思いますが良いことだと思いますね。

与儀：はい。ありがとうございます。苦労を含めてご理解頂けると、この「情報セキュリティ人財アーキテクチャ」の価値が正しく認知されると思います。また、作成しているメンバーは全員ボランティアで活動していますので、たいへん励みになります。

労働力構造の変化と情報セキュリティスキルニーズの再点検

山口：我が国としてどういう人材が求められるかという議論は常にあるわけです。これはIT戦略本部でも行われていた高度IT人材の育成という課題があって、それをどういうレベルで作っていくのかという時に、大学でやるべきこともあるし、民間の教育や資格を使うところもあるだろうし、それぞれのターゲットドメインに対して最適化をみんなで考えているのが現状ではないでしょうか。

我々のミッションは、この国として求められる人材像は何なのかということについて経常的に議論を行うことだと思っています。そして、官民での適切な役割分担をどのように行うかを考えることでしょう。今何が問題なのか、国のやっている事業、民間における事業、各々における適切な役割分担ということについて、再度議論を行う時期にきています。現在、そういう方向で準備しています。

与儀：人も技術も社会も多様化し継続的に変化するわけですから、それに対応する柔軟な教育プログラム、習熟度を確認するための厳格な試験、スキルを客観的に証明する意味での資格の位置づけも重要であり、ニーズに対応して必要な人材像も変わってきますね。

山口：キーワードは若年労働者の減少と、ITのインフラ化だと思っています。今後の少子化の進展に伴う若年労働者数の減少という問題を考えると、労働力の維持と同時に、全年齢における個々の労働者の生産性の向上を考えなければいけないと思います。これは、今までのように単にOJTを通してスキルを得ていくだけでなく、ある明示的なスキルの付与のメカニズムを社会で作っていかないと達成できません。

これを企業の中の社員教育の中で作るのか、あるいは、例えば大学・教育機関を利用し、キャリアパスの中で企業から教育機関に派遣する方法をとるのか、そういったことも考えながら労働力全体のスキルアップと生産性のアップをやっていかなければなりません。そのような中で、民間資格や国の資格の在り方については再度議論していくべきだろうと考えています。

与儀：確かにそうですね。現場では自身も習っていないトレーナーが本当に必要なOJTが出来るのかというような声も多数聞かれます。

山口：例えば外国人労働者を活用するなら国際化した資格制度が必要になるし、高齢者と女性の労働力を活用するならば、彼らにいかにスキルを与えて労働力として活用するかを考えなければいけません。このように官民の役割分担、雇用側と被雇用側の関係等を踏まえて、今の資格制度やスキルをどう作っていくかを考える必要があります。その点に関して定常的に点検を行いながら前に進んでいく作業が要ると思っています。

与儀：我々教育事業者においても国内事業者さんもいますし、ワールドワイドなライセンサーもいます。例えば監査であれば日本セキュリティ監査協会のCAIS[7]があれば日本システム監査協会もあり、海外にあるISACA[8]がやっているCISAというものもあります。先ほど海外から人が来るときはグローバルな観点が必要というところがありましたが、ご承知のようにインターネットはボーダレスな訳で、その中でグローバルな観点を取り入れることも必要になってくると思います。

7. Certified Auditor for Information Security　最高情報セキュリティ責任者
8. Information Systems Audit and Control Association, 情報システムコントロール協会

山口：グローバル化を担保する資格とかスキルを与えるメカニズムはよく見ておかないといけないし、グローバルに使える格好で日本がハンドルできるのかには注意しないといけないですね。

教育の構造変化と官民の役割

山口：アメリカの場合、企業で求められる人材のベースは大学で教え、その先の専門知識については大学を含めて民間でも教育するという考え方です。

一方、日本の場合は、企業においては大学は役に立たないと考えられており、OJTの教育体制がすごく充実していたと思います。それが人材流動化、企業における教育コストの圧縮等の流れの中で、大学教育、資格制度を企業が非常に期待してきている。そういうシステムの変化と資格の役割、民間事業者の役割をどう位置づけるかというのは今一度考えるべきだと思うのです。

与儀：そういった意味でセキュリティの人材育成においても幅広い意味での産学連携が求められるということですね。より具体的な連携を加速させていく必要があると思うのですが、そういう取組みを、内閣官房として支援する試みとかお考えはございますか？例えば産学連携窓口とか。

山口：内閣官房の役割は、政策の方向性の取りまとめや、省庁が連携して動くべき内容についての総合調整を図っていくことです。その中で必要なものは各省庁と協力しながら推進しています。例えば「先導的ITスペシャリスト育成促進」事業などでは、実際に産業界との間の調整を文科省とNISCとIT担当室[9]と皆でやりながら実施しています。

しかし、一番人材を使う産業界における人材に対するスキル要件がまだうまく見えてない状態では、事業の組み立てが難しいのです。産業界のIT・セキュリティ人材に対する要求はまだ“こなれ感”がありません。人材はどうあるべきかという話もちゃんと出て来ないと、国に対する産学連携お見合い促進期待論になると、いつも陥る落とし穴に嵌ってしまうのではないでしょうか。

与儀：とはいえ所管の官庁があるわけですね。学関係では文科省があります。それから経産省、総務省と各々役割があり役割分担をされている訳だと思います。でも人財育成について考えるのは一体になって考えていく問題だと思うんですね。

人材ニーズの再点検と再定義へ

山口：どういうスキルの人材が要るのかという点検という意味では内閣官房で継続的に関与していきますが、人材育成側と産業界の対話は、内閣官房でできる話ではなくて、その繋がりを確保していく仕組みが要るということです。今はそこのメカニズムがすごく弱いと思います。実際に産業界からは、セキュリティに特化した人材はそんなに必要なく、ITにすごく強い人材にセキュリティのコショウをまぶした人材というイメージが要求されることもあります。そうすると大学では、セキュリティ特化のコースウェアの組み直し・改善が必要になってきます。

また、内部統制が非常に重要になってきていて、その中でリスクを見ていくので、その視点からは「情報セキュリティ」という言葉は適当ではないかも知れないという意見もあります。そうなるとそこに合致する人材はどこでどう育成されるのかという疑問も出てきます。

2007年にスキルセットなどに関する検討を実施してみて、教育・資格にも様々な特徴があるというのも良く分かりました。今意識しているのは、スキルの資格やスキルの集合などを有する人への需要、使う側とのミスマッチがどれくらいあるかということです。そこに踏み込んでいかないと、政策として取り組んでいくための対話がうまくできないのではないかと思っています。現状での問題点について、官民の関係者が再度考える必要があるのではないかと思っています。

与儀：ISEPAでは、情報セキュリティ人財アーキテクチャというものを作ったとお話しましたが、これからセキュリティ人財の

9. 内閣官房情報通信技術担当室

実態調査をしようかと考えています。ISEPAは情報セキュリティの教育を受けた有資格者にリーチできるという強みがあります。そこに対してのアンケートですね、実際その資格が業務の役に立っているのかとか、教育を受ける上での障害は何なのかとか、キャリアステップと合っているのかとか、そういうものを人材側に調査を実施したいと思います。

もう一方で雇用をする企業側にもセキュリティ人財は本当に会社にとって必要なのか、先ほど補佐官がおっしゃったように、ITのフレームワークがメインで、それのコショウ的な要素がセキュリティでしょという人もいますし。セキュリティが入っているITのフレームワークが当たり前という人もいますね。我々が考えたキャリアパスやフレームワークにずれはないのか、セキュリティだけに特化する業務があるのか、それだけ特化する資格を作る必要があるのかなども検証する必要があると思います。資格の中にはITの全体像と更にセキュリティを知っているということを認証する資格もあります。その辺の有効性や、資格を取っている側と有資格者を雇用する側においてどういうギャップがあるのか、あるいは合っているのかというのを民間団体としても調査検証をやろうと思っています。

山口　英氏（やまぐち・すぐる）

内閣官房情報セキュリティセンター情報セキュリティ補佐官
奈良先端科学技術大学院大学情報科学研究科教授

1964年生まれ。大阪大学基礎工学部卒。工学博士。大学では、大規模分散処理環境構築、ネットワークセキュリティなどの研究に従事。2004年から内閣官房情報セキュリティセンターの情報セキュリティ補佐官として、日本の情報セキュリティ戦略と具体的な対策の立案に携わっている。現在JPCERTコーディネーションセンター及び日本ネットワークインフォメーションセンターの理事も務める。

山口：それはいい話ですね。

与儀：それに先立ってISEPAでは、Webのトップページで【ISEPA加盟団体のセキュリティ資格保有者一覧】を公開しています。今まで各団体バラバラだった取得者の人数推移をひとつのポータルで見られるようにして、3ヵ月ごとに増えているのか減っているのかを１ヵ所で見える化しています。

山口：私が現在気になっているのは高齢化の中での労働人口推移です。どこの国でも高齢化が起きると一般的に高齢者を支えないといけなくなり、自己再投資や子供に対する投資などが減ってくるので、人材育成に対する投資がしぼむことになります。高齢者を支えながら大学に子供を2人送り込むという投資ができなくなっているからこそ、今進学率が頭を打っているのではないかと考えます。

大学への進学率は落ちる可能性があるにも関わらず、今の資格制度の多くは大学・大学院を出た人の取得を前提に組んでいるように見受けられます。しかし、今後、高卒・専門学校卒で働く人たちが増えるということを考えると、彼らがある一定の職域を担当できるような資格も選択肢に加えながら幅を広げていくことも必要になると思います。

本当にこれからITがインフラ化する中で、必要な人材はどう確保し、セキュリティやリスク管理の知識・スキルは誰に対して与えていくのかを考えておかなければなりません。

例えば、高校の授業において、「情報」を必須化してセキュリティを徹底して教え、セキュリティの必要性と感覚は社会に出る人間なら身に付いているようにしておくという施策も考えられます。

いずれにせよ、複数の領域にかかわる統計情報を解析し、省庁や業界の縦割りを見直し、その中でわが国の人材のイメージをつかみながら人材政策を進めることが必要なのではないかと思います。

今すぐ必要な人材、スキルは？

与儀：可及的速やかに必要なセキュリティ人財っていうのはイメージされていますか？例えば今年度育成していくのに本当に

必要なセキュリティ人財ってどういう人材像なのかなど。

山口：経営層やマネジメントクラスに対し、リスクマネジメントにITという要素が含まれてきていることを理解してもらうための再教育の実施が一番必要だと思います。これだけビジネスがITインフラに依存しているのにも関わらず、認識がない経営者が多い。

先日発表された内閣府の「特定分野における事業継続に関する実態調査」（平成21年7月14日発表）（http://www.bousai.go.jp/oshirase/h21/090714kisya.pdf）によると、重要インフラ分野として定義されている事業者を調査した結果、BCPを策定しているのは証券77.4%、銀行・地域金融機関は36.5%、病院に至っては4.8%というレベルでした。これら業種はある程度IT依存度が高いにも関わらずこの結果です。これは経営者のリスクマネジメント意識の欠如であると考えられます。このような状況を改善するために、この国の基幹業務に携わる人たちへのエグゼクティブトレーニングが必要なのではないかと思います。

政府においても、ITとリスクマネジメント両方を理解している人材は非常に少ないですね。事故前提社会であることを認識して俯瞰的に見えるようなリーダークラスをこれから育成していくということが必要です。

与儀大輔（よぎ・だいすけ）

情報セキュリティ教育事業者連絡会代表
株式会社ラック　執行役員　セキュリティ能力開発センター長

1971年生まれ。日本体育大学体育学部卒。大学時代はアメリカンフットボール部に所属し甲子園ボウルにも出場。1994年 横河電機株式会社入社。制御システム販売を経て情報セキュリティ事業に従事。2007年　株式会社ラック入社。日本の情報セキュリティ強化には人財育成が欠かせないことから海外民間資格の日本導入や教育コースを多数展開すると共に、情報セキュリティ教育事業者連絡会を立上げ現在に至る。
兼務：株式会社ITプロフェッショナル・グループ代表取締役社長・CEO、情報セキュリティ大学院大学客員研究員、NPO日本ネットワークセキュリティ協会　幹事

与儀：CSO[10]などは兼務でやっている方が多いですよね。「我が社に危機管理委員会は組織上ちゃんとありますし、危機管理委員長は社長です」と、でも実際リスクマネジメントやBCM[11]について一切社長は知りません、などという笑えない現実がありますね。また危機管理の中でも情報セキュリティに関しては、一応インシデントレスポンスチームを発足させ、総務部や情シス部などの部長クラスが、組織図としては入っていますが、結局統制が取れてないとか権限が与えられないといった理由から、インシデント対応を発動しなきゃいけないときに発動できない、機能できない、大失敗しました、などというのが最近散見されますよね。

山口：ISEPAへの提言としては、現状を是正していくためにはトップマネジメント育成が急務であることから、エグゼクティブトレーニングのトレーナー資格のようなものを民間事業者で作ってはいかがか、ということです。

トップマネジメントのリーダーシップの下でのリスクマネジメントであるべきだと思います。ITリスクが顕在化したときに責任と権限を明確に与えてあれば現場は動ける。それを与えるのはエグゼクティブマネジメント層だからです。

与儀：なるほど効果的に感じますし今までにない観点ですね。人財アーキテクチャにも取り込んで位置づけていくとよさそうですね。

山口：人材をマーケットニーズに対して適合させていくことは、国よりも民間の方が上手だと思います。一方で、全体の大きな

10. Chief Security Officer 最高セキュリティ責任者
11. Business Continuity Management 事業継続管理

意味での労働力の中でのポートフォリオは、国で検討するべき部分がさまざまあります。そのような意味で、第2次情報セキュリティ基本計画やセキュア・ジャパン2009で触れている「官民の適切な役割分担」は非常に大切なことであり、その中で両側のいい特性をきちんと伸ばしていけばいいと思います。

今回ISEPAが策定した情報セキュリティ人財アーキテクチャは民間側だからこそ作ったところもあって、非常に有意義な取り組みだと評価していますし、うまく活用されるようになっていけばいいと思うのです。是非頑張ってほしい。
同時に政府の側では、所得からの教育に対する再投資傾向、企業内労働力の再配置に対しての資格制度の活用とかスキル付与の傾向を考えなければならないのです。

今後もISEPAにはぜひ協力してもらいたいと思います。そういう健全な関係が今後も情報セキュリティの領域、ITの領域で維持できていくことがいいことじゃないかなと思いますね。

ISEPAに期待すること

与儀：最後に一言、我々 ISEPAは発足から約2年です。この間NISC、総務省、経産省をはじめとするオブザーバーやアドバイザーの皆様からご支援を頂きながら、民間事業者の寄り合いで頑張って何とかやってくることができました。我々の活動に今後期待することを補佐官からお願いします。

山口：４点申し上げます。

1．資格というのは分かりにくいので、この資格は何を要求し、取得者はどのようなスキルが身につき、取得者のキャリアパスはどのようになるのか、ということの見える化を推進して欲しい。
2．時代、インフラ等の変化への資格のキャッチアップをさらに推進して欲しい。
3．ITのインフラ化に伴い、ITの対象業務がどんどん拡大しており、リスク管理の実施、対象業務に対しての知識が求められる。ITは全業種で使われていることを踏まえ、リスク管理に資格がどう向き合うのか、よく考えていって欲しい。
4．多くの意見を集約して政策を作っていくことが必要なので、国の政策に対しては是非積極的に事業者側からの意見のインプットをお願いしたい。

与儀：是非そういった意味では今後ともご支援ご指導もいただきたいと思います。我々からもいろんなアウトプットを出していきたいと思います。

民間がボランティアベースで作り上げた成果である、情報セキュリティ人財アーキテクチャも、我々としてはどんどん公開して利用を促進していきます。そこでISEPAに対しても今後も変わらぬご支援をぜひ我々お願いしたいと思います。

山口：ぜひ力強い成果を上げてください、期待しています。

与儀：心強いお言葉です。今日はいろいろ教えていただいてどうもありがとうございました。

情報セキュリティ人財アーキテクチャガイド
2009年度版

1．概説：作成の背景、前提条件、目的

1．1　作成の背景

情報セキュリティ人材の育成と維持は、企業などの組織運営にとどまらず、わが国の情報セキュリティの政策や戦略上も重要な課題になっている。これは様々な政策文書や調査結果でも人材不足が謳われている。しかし、情報セキュリティ人材に関わる質と量、ミスマッチなどの問題に対する有効な解決手段がないのが現状である。そうした背景から、これらの問題を解決するために、様々な立場や組織、職種などに対応でき、中長期の視点からの情報セキュリティ人材のライフサイクルでの運用管理モデルが必要であると考えた。

【参考】第2次情報セキュリティ基本計画での「人材育成・活用」に関する指摘

情報セキュリティに係る人材育成・確保に関する施策のニーズや問題点は、依然、多く存在する。例えば、政府機関においては情報セキュリティに携わる人員の不足や、短期のローテーションによって政府機関内部における知見が蓄積されない等の問題が指摘されている。

また、情報セキュリティ業務に携わっていく上での明確なキャリアパスが見えないと言った指摘も存在する

情報セキュリティに携わる人材が保有するスキルを業務の上で明確に位置付けることができず、情報セキュリティ業務に対して、適切な人材を配置することが難しくなる可能性もある。

1．2　目的

情報セキュリティ人材の育成・活用・管理のための、実効的かつ相対的な指標を示すことを目指した。具体的には、

・情報セキュリティの業務を実施する側：
　— 情報セキュリティ人材を目指す個人にとっての目標の自己設定や評価ができる
　— 情報セキュリティ人材を育成する組織にとっては、実効性が高い人材の育成、評価や管理ができる
・情報セキュリティの業務を委託する側：
　— 業務を委託する際に、要件に合った適切な人材を要求・調達できる

といった事を達成できる素材を提供していく事を目的としている。

☆「人財アーキテクチャ」の名前にこめた想い：

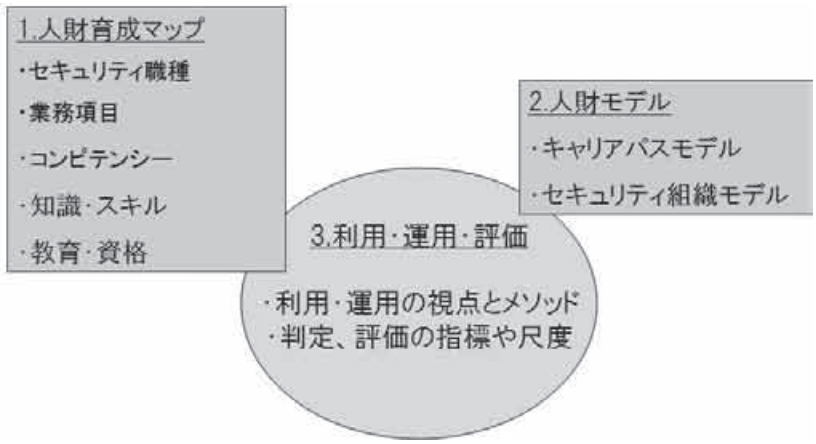
旧来から、「ヒト」「モノ」「カネ」が企業の3大資産と言われてきた。ここでの「ヒト」は、他の2要素「モノ」「カネ」と同じ、いわゆる「有形資産」としての考え方であった。

しかし、われわれは『情報セキュリティ人財アーキテクチャー』での「ヒト」を「有形資産」であると同時に、「ブランド」「イメージ」などと同じ「無形資産」でもあり、その能力（スキル）は「技術」や「特許」などと同じ「知的財産」でもあると考えた。そこで、「人財」という呼び方や考え方を使うことにした。

次に「アーキテクチャー」という言葉を使ったことについては、「コンピューター・アーキテクチャー」などというように、「構造」や「設計」という意味で使われるが、『情報セキュリティ人財アーキテクチャー』では、さらに大きな概念として扱っている。ご存知の方もいると思うが、組織運営の方法論として「エンタープライズ・アーキテクチャー（EA）」という言葉がある。これは、組織（enterprise）の業務手順や情報システムの標準化、組織の最適化を進め、現状（as is）ではなくあるべき姿（to be）としての組織構造を実現するための設計思想・理念（architecture）を意味していて、『情報セキュリティ人財アーキテクチャー』は、いわばこの「EAの情報セキュリティ人材版」という位置づけとした。

1.3　情報セキュリティ人材アークテクチャの概要：

まず現存する教育・資格と情報セキュリティ業務、職種、スキルといった物とを紐付けした。ただそれだけだと、人材のライフサイクルでの運用管理モデルにはならないので、実際の組織における組織モデルや個人のキャリアマップモデルを作成し、またこれらの使用手法や評価のフレームワークまでを提示する事で、人材育成・活用する側、される側の双方にとって使い勝手の良いToBeモデルと成りえる物を提供する事を目指した。特に使用・運用方法や評価についてのフレームワークについては、今までの様々なスキルマップ的な物の問題点として、それらをどう使ったら良いか分からない、自分のスキルや知識レベルの評価をどうやってやればいいのか分からないという問題点に対しての解としての初の試みとなっている。



図表1）セキュリティ人財アーキテクチャー全体概要図

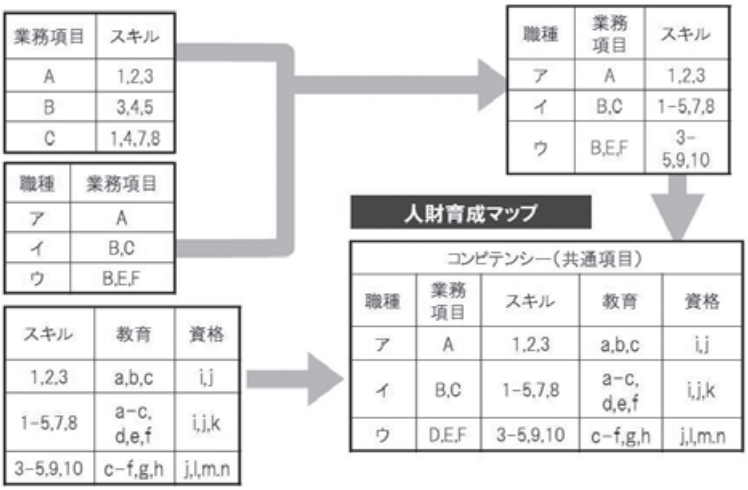
上記でも見てもらえる通り、作成に当っては、「現存する教育・資格と情報セキュリティ業務、職種、スキルといった物とを紐付けしていく」を「人財育成マップ」、「実際の組織における組織モデルや個人のキャリアマップモデル」を「人材モデル」、「これらの使用手法や評価のフレームワークまでを提示」を「運用・評価フレームワーク」と名づけ、それぞれ作成する事にした。

2. 人財育成マップ

人財育成マップでは、以下の5項目を抽出した。各項目の抽出にあたっては、WGメンバーの思いだけで判断するのではなく、既に存在している信頼でき得る、指標となりえる資料からのリストアップを試みた。

- 情報セキュリティ職種
- 業務項目
- コンピテンシー
- 知識＆スキル
- 教育＆資格

それらを、マッピングしていく中で、コンピテンシーについては全人材に当てはまる要素という事で、共通条件という形での取り扱いにし、それ以外の「職種」「業務項目」「知識・スキル」については関連付けを検討し、職種毎に紐付けされた形で提示している。これによって、ある職種では、どんな業務項目があって、その業務をこなすにはどんな知識・スキルが求められていて、必要な知識・スキルの習得にはどのような教育や資格が存在するのかを一覧で見えるようにした。



図表２）人財育成マップ策定プロセス

２．１ 情報セキュリティ職種

職種は現存する職種名から研究、教育に関わる職種を除き、32職種に絞込んだ。これらで、情報セキュリティに関わる業務全体をカバーしていると考える。

1	プリセールスエンジニア	17	オペレーター
2	セールスコンサルタント	18	セキュリティアナリスト
3	テクニカルコンサルタント	19	フォレンジックアナリスト
4	セキュリティエンジニア(要求定義)	20	インシデントハンドラー(プロダクト)
5	セキュリティアーキテクト(製品・ソリューション)	21	インシデントハンドラー(組織)
6	セキュリティアーキテクト(コンサル)	22	フィールドエンジニア
7	セキュリティエンジニア(企画・設計)	23	プライバシーオフィサー
8	セキュリティエンジニア(基盤)	24	プライバシースペシャリスト
9	セキュリティエンジニア(アプリ)	25	CSO/CISO/CIAO
10	セキュリティエンジニア(DB)	26	CSO/CISO/CIAO補佐
11	QAマネージャー	27	セキュリティプロダクトオーナー
12	QAエンジニア	28	セキュリティサービスオーナー
13	セキュリティテスター	29	セキュリティコンサルタント(マネージメント)
14	プログラマー	30	セキュリティアドバイザー
15	プロジェクトマネージャー	31	セキュリティストラテジスト
16	セキュリティシステムアドミニストレーター	32	セキュリティ監査人

図表３）情報セキュリティ職種

また、これらの職種それぞれについては、当然組織体や業種などによって職種に対するイメージや実態が違うという事を前提に考え、各職種に対してISEPAにおける定義を策定した。

	職種	定義
1	プリセールスエンジニア	セキュリティ製品導入を検討する企業に対し、どのような環境なら顧客の要望が実現可能なのか製品・サービスに関する技術的知識を持って営業活動を支援する
2	セールスコンサルタント	顧客システムの現状の把握および問題点の調査し、顧客の状況に合わせて、適用範囲が広範囲な製品・ソリューション対策/提案をする
3	テクニカルコンサルタント	情報セキュリティに関する経験値が高く、技術的見地からのアドバイスやレビューを行う
4	セキュリティアーキテクト(製品・ソリューション)	セキュリティ製品・ソリューション開発の設計、及び管理
5	セキュリティアーキテクト(コンサル)	セキュリティ確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務
6	セキュリティエンジニア(要求定義)	セキュリティ・ソリューションに関する要求定義を行う
7	セキュリティエンジニア(企画・設計)	セキュリティ・ソリューションの企画・設計・最新技術調査、製品評価
8	セキュリティエンジニア(基盤)	セキュリティ・システムの基盤部分(OS・ネットワーク)の全体設計・運用設計・方式設計、開発
9	セキュリティエンジニア(アプリ)	アプリケーションの開発フェーズにおいてセキュリティの確保を行う
10	セキュリティエンジニア(DB)	DBMSを構成要素とするシステムを対象に、セキュリティの確保を行う

11	QAマネージャー	品質保証業務及びそのプロセス改善業務。製品品質に関する顧客窓口業務。開発チームに対する品質保証啓蒙活動
12	QAエンジニア	ソフトウェア開発および開発プロジェクトに対し、品質保証全般のテストを実施。
13	セキュリティテスター	ソースコード解析や脆弱性の洗い出し
14	プログラマー	仕様書や設計書に従って、セキュアプログラミングの知識を持ってプログラムを作る。
15	プロジェクトマネージャー	プロジェクトの計画と実行において総合的な責任を持つ。期日までに成果物を完成させる。
16	セキュリティシステムアドミニストレーター	システムに対するセキュリティ対策を整備し、運用管理を行う
17	オペレーター	提供しているサービスの運用・監視を行う。 ネットワーク監視。ヘルプデスク。サービスシステム維持管理等
18	セキュリティアナリスト	各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を提示
19	フォレンジックアナリスト	証拠証跡の分析を行い、証拠保全、証拠開示手続きも行う
20	インシデントハンドラー(プロダクト)	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
21	インシデントハンドラー(組織)	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
22	フィールドエンジニア	顧客現場で、セキュリティシステム構築に伴う、システム機器の設置から設定保守・修理を行う
23	プライバシーオフィサー	企業・団体内の個人情報保護体制の構築、運用、改善を行う
24	プライバシースペシャリスト	企業の個人情報保護に関して、規定作成から意識向上施策実施までを担当する
25	CSO/CISO/CIAO	情報資産保護を経営の観点から意思決定をし、指揮をとり、組織の情報資産保護の責任をとる
26	CSO/CISO/CIAO補佐	CSO/CISO/CIAOの業務を補佐し、経営陣の意思を現場に浸透させ、施策がきちんと実行されるかを監視する
27	セキュリティプロダクトオーナー	セキュリティ製品の企画から保守にいたるまで製品に関わる全責任をとる
28	セキュリティサービスオーナー	セキュリティサービスの企画から保守にいたるまでサービスに関わる全責任をとる
29	セキュリティコンサルタント(マネージメント)	情報セキュリティ戦略立案から、情報資産の管理・運用方法の策定までに関し、顧客の問題解決を支援する。
30	セキュリティアドバイザー	情報セキュリティ全般に関してのアドバイスを行う
31	セキュリティストラテジスト	企業の経営戦略実現にむけて、セキュリティを活用とした基本戦略を策定、提案、推進する
32	セキュリティ監査人	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する

図表4)情報セキュリティ職種の定義

2.2 業務項目

業務項目は、総務省、経産省、NISCが出した各種報告書から抽出した業務項目を130項目ほどリストアップした。参考にした報告書は以下の6つである。

・内閣官房情報セキュリティセンター：
　1)第一次情報セキュリティ基本計画
　2)セキュアジャパン2007
　3)人材育成・資格制度体系化専門委員会報告書
・総務省：
　4)u-Japan政策パッケージ
・経産省：
　5)グローバル情報セキュリティ戦略
　6)産業構造審議会情報経済分科会情報サービス・ソフトウェア小委員会人材育成ワーキンググループ報告書

2.3 知識・スキル

知識・スキルについては、JNSAの「情報セキュリティ知識分野(SecBoK)」の中項目レベルまでをベースにしている。SecBoKは、情報セキュリティに関わる知識を体系的に分類したもので、策定にあたっては、様々な情報セキュリティの教育カリキュラムや資格の知識分野や試験範囲などを参照している。

＜参照している主な教育・資格＞

・IPA：情報処理技術者試験：テクニカルエンジニア（情報セキュリティ）、情報セキュリティアドミニストレータ
・（ISC）2：CISSPのCBK（共通知識分野）
・ISACA：CISA、CISMの試験範囲
・SANS Institute：GIAC
・CompTIA：Security+の試験範囲
・NISM推進協議会：NISM　　など

「SecBoK」は、元々「情報セキュリティに関するスキルマップ」と呼ばれ、IPAからの委託事業としてJNSAが策定し2003年4月に発表したものである。これは主に情報セキュリティプロフェッショナルの「評価」と「教育」を目的としたものであり、情報セキュリティにたずさわる人材に求められる技術、知識をまとめた上で、自由度を高め、下記に挙げるようなさまざまな利用が可能なものとして作成された。その後、JNSA教育部会による調査や検討をもとに改訂を重ね、2007年度からは知識分野と項目に関しては「情報セキュリティスキルマップ」を「セキュリティ知識分野」または「SecBoK（Security Body of Knowledge）;セックボック」へと名称を変更することになり、今に至っている。

SecBoK自体の構成は、21分野の下に、大項目・中項目・小項目となっている。下の図表では、21分野を記載している。

項番	分野	
1	情報セキュリティマネジメント	
2	ネットワークインフラセキュリティ	
3	アプリケーションセキュリティ	Web
		電子メール
		DNS（Domain Name System）
4	OSセキュリティ	Unix
		Windows
		セキュアOS
5	ファイアーウォール	
6	侵入検知	
7	不正プログラム	
8	セキュアプログラミング技法	
9	セキュリティ運用	
10	コンテンツセキュリティ	
11	認証	
12	PKI（Public Key Infrastructure）	
13	暗号	
14	電子署名	
15	攻撃手法	
16	コンプライアンス？	
17	セキュリティプロトコル	
18	事業継続・災害復旧計画	
19	情報セキュリティ監査	
20	フォレンジック	
21	物理セキュリティ	

図表５）SecBoK

２.４ コンピテンシー

コンピテンシーは、情報セキュリティに直接関連する知識やスキルではなく、ビジネス遂行に当たって、必要なスキルという考え方となっている。様々な文章を検証していく中で、本アーキテクチャでは、「国家公務員採用1種試験　着眼点別評価段階と行動例」からピックアップした。

積極性【意欲・行動力】		経験学習力【課題の認識・経験の適用】	
	自らの考えを積極的に伝えようとしているか		自己の経験から学んだものを現在に適用しているか
	考え方が前向きで向上心があるか		自己や組織の状況と課題を的確に認識しているか
	目標を高く設定し、率先してことに当ろうとしているか		優先度や重要度を明確にして目標や活動計画を立てているか
	困難なことにもチャレンジしようとする姿勢が見られるか		他者から学んだものを自己の行動・経験に適用しているか
社会性【他者理解・関係構築力】		自己統制【情緒安定性・統制力】	
	相手の考えや感情に理解を示しているか		落ち着いており、安定感があるか
	異なる価値観にも理解を示しているか		ストレスに前向きに対応しているか
	組織や集団のメンバーと信頼関係が築けるか		環境や状況の変化に柔軟に対応できるか
	組織の目的達成と活性化に貢献しているか		自己を客観視し、場に応じて統制することができるか
信頼感【責任感・達成力】		コミュニケーション力【表現力・説得力】	
	相手や課題を選ばずに誠実に対応しようとしているか		相手の話の趣旨を理解し、的確に応答しているか
	公務に対する気構え、使命感はあるか		話の内容に一貫性があり、わかりやすく簡潔か
	自らの行動、決定に責任を持とうとしているか		話し方に熱意・説得力があるか
	困難な課題にも最後まで取り組んで結果を出しているか		話題や説明材料を効果的に使っているか

図表６）国家公務員採用I種試験６つの評定項目ごとに設定された着眼点別設定段階と行動の例

２.５　教育・資格

教育・資格は、本バージョンにおいては、ISEPA加盟団体・企業に現存する物をほぼ全て網羅していく形で作成している。

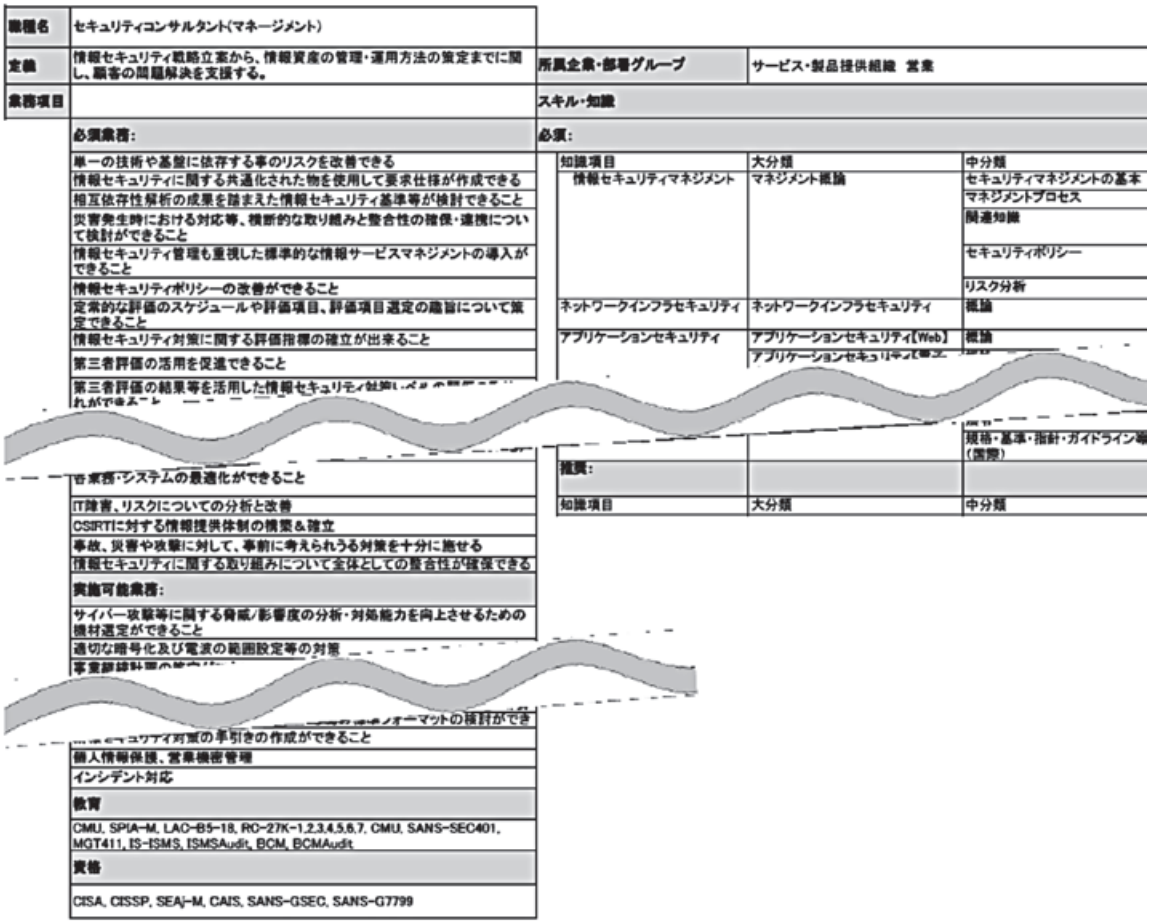
提供団体・企業名・URL	コース・資格名
ISACA http://www.isaca.gr.jp/cism/, http://www.isaca.gr.jp/cisa/	CISA CISM
NTTラーニングシステムズ http://www.learningsite21.com/course/jousemi/	情報セキュリティ専門家養成講座
ひょうご情報教育機構 CMU:http://www.cmuj.jp/curriculum_detail_jp_2008.html http://www.cmuj.jp/08program/index.html	カーネギーメロン大学日本校 情報セキュリティ育成プログラムーベーシックコース 情報セキュリティ育成プログラムーアドバンスドコース
CompTIA http://www.comptia.jp/cont_certif_10.html	Security+
SEA/J http://www.sea-j.net/	情報セキュリティ技術認定　基礎コース 情報セキュリティ技術認定　応用コース・テクニカル 情報セキュリティ技術認定　応用コース・マネージメント
シスコシステムズ http://www.cisco.com/web/JP/event/tra_ccc/ccc/certprog/paths/home.html	CCSP CCIEセキュリティトラック CCNAセキュリティトラック
ソフトピアジャパン http://www.softopia.or.jp/training/sec/sc01.html http://www.softopia.or.jp/training/sec/sc04.html http://www.softopia.or.jp/training/sec/sc07.html	 セキュリティマネージメントコース セキュリティテクニカルコース インシデントレスポンス実践コース
日本セキュリティ監査協会(JASA) https://www.jasa.jp/qualification/training/downf/scopever1	公認情報セキュリティ監査人
LAC http://www.lac.co.jp/academy/library.html	情報セキュリティマネジメントシステム 情報セキュリティ監査 情報セキュリティガバナンス 法と倫理 セキュリティアーキテクチャ 不正アクセス対策 ネットワークインフラセキュリティ ファイアウォールと侵入検知 ネットワークセキュリティ(セキュリティプロトコル) OSセキュリティ 不正プログラム対策 セキュア開発 暗号・電子署名 PKI・認証技術 物理セキュリティ インシデントレスポンス デジタルフォレンジック 事業継続管理 セキュア開発Webアプリケーション(知識編) DBセキュリティ技術者養成コース(知識編) ペンテストコース(知識編) インシデント・レスポンス基礎知識編 実践！インシデント・レスポンス模擬訓練 実践！デジタル・フォレンジックハンズオンコース 実践！マルウェア解析ハンズオンコース 実践！サーバ管理者のためのログ解析コース 実践！アナリスト養成コース 実践！ペンテストコース
リコーヒューマンクリエイツ http://www.rhc.co.jp/r-isap/top_training.html	プライバシーマーク審査員研修 プライバシーマーク制度とJISQ15001入門解説 演習で学ぶJISQ15001:2006規格解説 演習で学ぶプライバシーマーク・リスク分析 演習で学ぶプライバシーマーク・内部規定 演習で学ぶプライバシーマーク・内部監査 プライバシーマーク更新審査に向けた「新JIS対応」 プライバシーマーク取得のための「ラピッドコンサルティング講座」 ISMS審査員研修 ISMS審査員資格更新のための実践集中コース はじめて学ぶISO27001 リスク分析を中心に学ぶISO27001 演習で学ぶISO27001内部監査 経営者のための必修情報セキュリティ ISO27100認証取得のための「ラピッドコンサルティング講座」

提供団体・企業名・URL	コース・資格名
(ISC)2 http://www.isc2.org/japan/Default.aspx	CISSP SSCP
SANS http://www.sans.org/training/courses.php?utm_source=web-sans&utm_medium=text-ad&utm_content=Training_Links_Homepage_courses_trngLinks_hompge&utm_campaign=Training&ref=27999	GIAC Security Essentials Certification GIAC Certified Penetration Tester GIAC Certified Firewall Analyst GIAC Systems and Network Auditor GIAC Certified Incident Handler GIAC Certified Windows Security Administrator GIAC Certified UNIX Security Administrator GIAC Securing Oracle Certification GIAC Secure Software Programmer-Java GIAC Secure Software Programmer-C GIAC Certified Project Manager Certification GIAC Certified Intrusion Analyst GIAC Reverse Engineering Malware GIAC Certified Forensics Analyst GIAC Security Leadership Certification GIAC Certified Incident Manager GIAC Certified ISO-17799 Specialist SEC301: Intro to Information Security SEC401:SANS Security Essentials SEC501:Advanced Security Essentials SEC502: Perimeter Protection In-Depth SEC503: Intrusion Detection In-Depth SEC504:Hacker Techniques, Exploits and Incident Handling SEC505: Securing Windows SEC506: Securing Unix/Linux SEC508: Computer Forensics, Investigation, and Response SEC509:Securing Oracle SEC560: Network Penetration Testing and Ethical Hacking SEC601: Reverse-Engineering Malware: The Essentials of Malware Analysis SEC610: Reverse-Engineering Malware: Malware Analysis Tools and SEC709: Developing Exploits for Penetration Testers and Security AUD429: IT Security Audit Essentials AUD507: Auditing Networks, Perimeters & Systems DEV304: Software Security Awareness DEV319:Intro to Web Application Security DEV422:Web Application Security Essentials DEV534: Java Security Source Code Review DEV536: Secure Coding for PCI Compliance DEV538: Web Application Pentesting Hands-On Immersion DEV541: Secure Coding in Java/JEE DEV544: Secure Coding in .NET DEV545: Secure Coding in PHP DEV548: Secure Coding in C MGT411: SANS 17799/27001 Security & Audit Framework MGT504: Hacking for Managers MGT512: SANS Security Leadership Essentials For Managers MGT525:Project Management and Effective Communications for Security Professionals and Managers
インフォセック http://www.infosec.co.jp/service/management/06.html	ISMS導入・運用コース ISMS内部監査員コース PMS導入・運用コース PMS内部監査員コース 事業継続マネジメントシステムコース 事業継続内部監査員コース
日本システム監査人協会(SAAJ) http://www.saaj.or.jp/csa/index.html	公認システム監査人
日本サードパーティ http://www.jtp.co.jp/education/	Ethical Hacking & Measures(CEH対応コース) スーパークルーズ(CEH対応コース) CEH直前対策コース
KKC情報システム http://www.kkcjoho.co.jp/kansa-edu/	情報セキュリティ監査人研修コース

図表7）情報セキュリティ資格に対応した教育コース一覧

教育・資格については、どの職種には、どういった教育や資格が有効かについてを指し示していこうとしている。

これらの各項目をマップとして、職種毎にまとめた。下記がまとめた物の1例である。各職種毎の詳細は、本ガイドの最後に、全32職種のマップについて紹介していく。



図表８）職種別業務・知識マップのイメージ

３．人財モデルについて

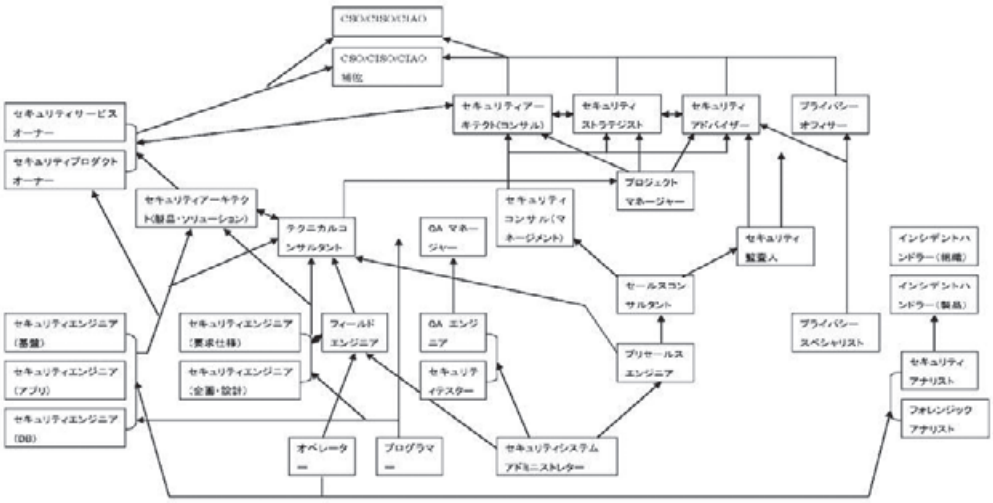
人財モデルでは、人財育成マップを使っていただく為のモデルの提供をしている。キャリアアップをしたい方、キャリアパスを想定して人財を育成していきたい方・組織向けの「キャリアパスモデル」と、実際に組織を編成する上でどのような人財が必要かを確認・検討したい方・組織向けの「セキュリティ組織モデル」という2種類のモデルを作成した。

◎キャリアパスモデル

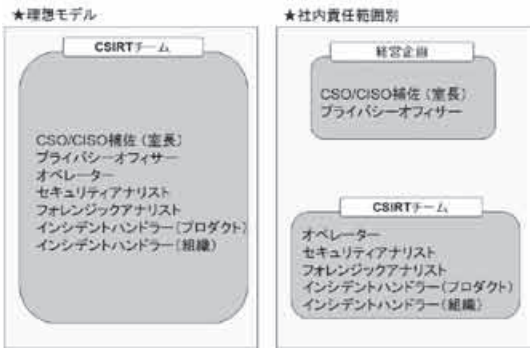
キャリアパスモデルについては、今回職種として提示した全職種を関連付けてパスを策定し、そのうち新社会人の最初のキャリアパスとなりやすい二つの職種をスターティングポイントとして策定を試みた。最終的にはキャリアパスとして、立体的な構造や視点から、情報セキュリティ人材に関わる調査や検討をした結果を提示してみた。検討に際しては、人財育成マップにおける各職種の業務項目の重複が多ければパスとして成り立つ、業務項目・責任範囲が多ければ上位層の職種であるということを前提として、全職種の相関関係を導き出し策定した。

◎セキュリティ組織モデル

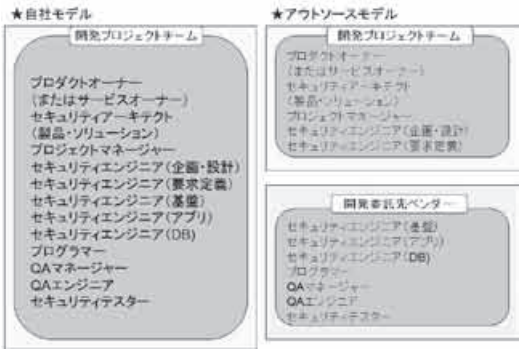
セキュリティ組織モデルについては、「企業内CSIRT」、「情報セキュリティシステム開発プロジェクト」、「組織内情報セキュリティ機能」という３モデルについて策定した。ただ、組織モデルは組織の規模や業務内容により異なるため、自社内のみ、アウトソースする、大・中小企業における違いなどを考慮して策定した。ただし、この報告書で提示しているのはあくまでもモデルであり、このモデルを利用いただくにあたっては、モデルに該当する種類の組織でもその企業・団体の状況に応じて、適宜変えて利用されることがあって構わないと考えている。



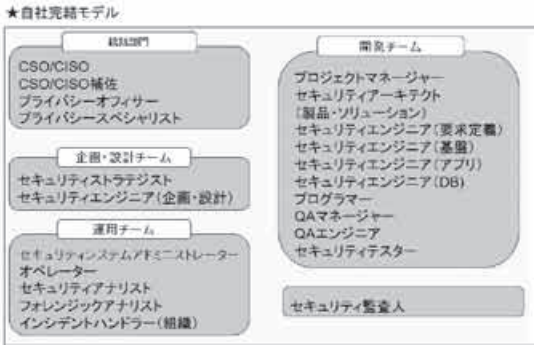
図表9-1 ）キャリアパス モデル



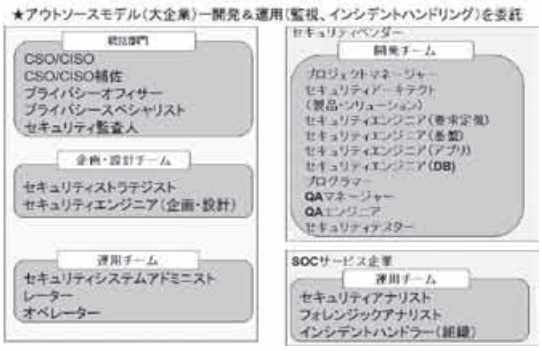
図表9-2 ）組織 モデル①
企業内CSIRT



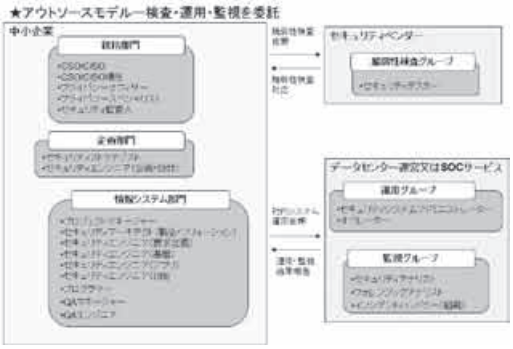
図表9-3 ）組織 モデル②
セキュリティシステム開発プロジェクト



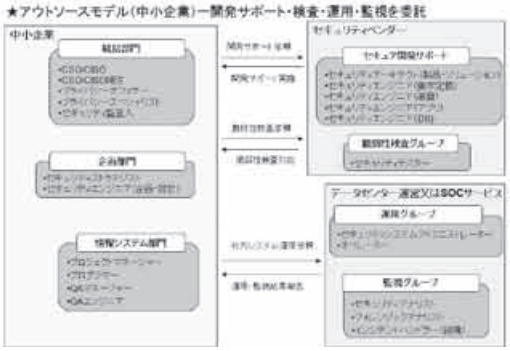
図表9-4 ）組織 モデル③
企業内情報セキュリティ機能



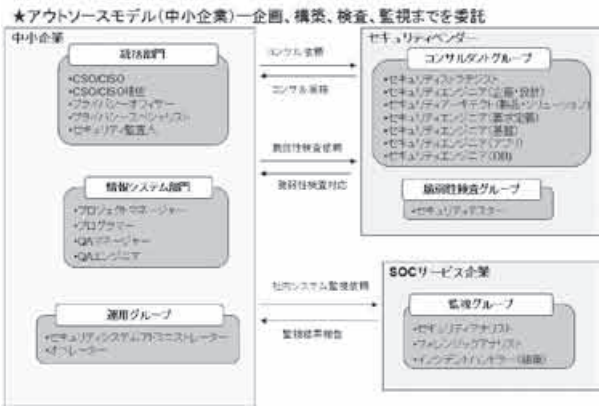
図表9-5 ）組織 モデル④
企業内情報セキュリティ機能



図表9-5 ）組織 モデル⑤
企業内情報セキュリティ機能



図表9-6 ）組織 モデル⑥
企業内情報セキュリティ機能



図表9-7 ）組織 モデル⑦
企業内情報セキュリティ機能

本章では、キャリアパスモデルについては、情報セキュリティにおける２つのキャリアパスの事例を紹介し、育成側、育成される側の双方にとってのガイドラインとして活用いた頂ければ幸いである。「セキュリティ組織モデル」については、「企業内CSIRT」のモデルケースを紹介し、組織やプロジェクト遂行において必要となる人材の特定、ケース毎の必要人材群を特定するガイドラインとし活用いただければ幸いである。

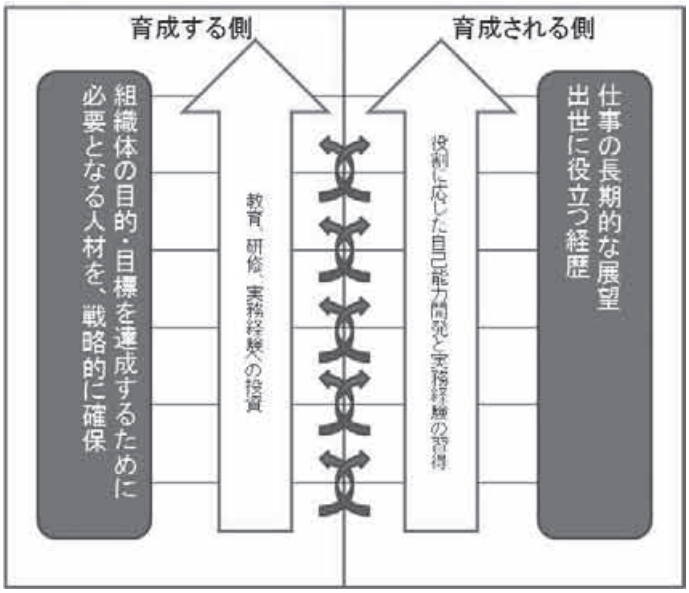
３．１　キャリアパスモデル

（1）キャリアパスの定義

まず初めに、ISEPAにおけるキャリアパスの定義を策定した。キャリアパスの言葉の定義を複数の辞書で調べてみると、「キャリアパス【career path】労働者の能力や適性の観点から見た職歴。また，それを形成するための職種。」のように記載されている辞書が多い。このことから、キャリアパスとは、「仕事の経験を積みながら次第に能力・地位を高くする順序や、そのための一連の職場や職種、あるいはその目的のための職場を異動する経歴のこと」と定義する。

次に、キャリアパスを定義する目的だが、人材の育成側、育成される側にどのようなメリットがあるのかを考えた場合、人財を育成する側としては、組織体の目的・目標を達成するために必要となる人財を、戦略的に確保することが可能となる。人財育成される側、いわゆる個人の立場としては、今の仕事で具体的にどのような実績を上げることができ、それがどのような経歴として身についていくのか、そして次にその実績を元に、どのようなところで自分の強みを見に着けて、という「仕事の長期的な展望」を持って、「出世に役立つ経歴」を重ねていくことが可能となる。

また、組織においてはキャリアパスにより、組織の目的や目標を達成するために必要となる知識や技術が把握できるため、どのような教育、研修や実務経験を受けさせると、組織体にとって必要な能力を身につけていくことができるかを判断することができる。人材育成される側としても、どのような知識や技術が求められているのかを理解することができるため、自己能力を伸ばす方向を定めることができる。結果としてキャリアパスモデルを組織、個人で可視化、共有することにより、達成する目標や期待される能力、人材評価制度などを共有することができる。



図表10 ）経営戦略と人材育成戦略の融合

（2）情報セキュリティ分野におけるキャリアパス

一般論として、「情報セキュリティ分野のキャリアパスは存在するのか」という部分については、IT分野のキャリアパスと特別な差異はないと考えられる。情報セキュリティに関連する技術は、情報システムがあって初めて成立する技術となるため、IT分野の技術を含めてキャリアパスを考えてみた。ただ、情報セキュリティのキャリアパスはIT分野と比較すると、どちらかといえばスペシャリスト寄りであり、かつベースにIT分野があるため、キャリアパスの方向性はより多様になると考える。最終的なキャリアパスとしては、情報セキュリティに携わるエンジニアは、自分の専門領域を徹底的に磨きあげる研究職に近いエンジニアもいれば、IT分野の技術をベースに、自分の得意分野を中心として、情報セキュリティの守備範囲を拡大していくエンジニアに分けられると考えられる。キャリアパスの途中で技術職なのかマネージメント職なのかを選択する分岐点があり、必ずしも経営層を最終キャリアパスとしていないモデルも考えられる。

新社会人として企業に配属された場合、例外を除き最初から研究職など専門性がある職域に配置されることは殆どの企業ではないと考えられる。情報セキュリティに携わるエンジニアはIT分野のエンジニア同様、最初はITのキャリアをベースとしてキャリアを積み上げていくので、システム設計やシステム開発を通じてOS、ネットワーク、データベースなどの技術と組み合わせて情報セキュリティの分野を身につけていくエンジニアが多いと考えた。このように情報セキュリティ部門に配属されても、最初からセキュリティの教育や研修は行われず、プログラミングやオペレーター職種から始まる企業がほとんどであり、配属先のプロジェクト内容に応じ、開発/テスト/仕様書や設計書などのドキュメント作成、手順書に基づき決められた各種設定値や稼働状況の確認に関するオペレーションを実行する中で、情報システムと情報セキュリティを少しずつ理解させる企業が多いと考えられる。

＊キャリアパスと組織モデルの関係

実際のプロジェクトでは、規模の大小にもよるが、個々の強みを発揮しながらチームとして成果を出していくことが求められるため、プロジェクトの中に個人の強みを伸ばしていける環境、ポジションが用意されていることが多い。また、あるメンバーの弱い部分について、その部分が強みであるメンバーと組み合わせて補うといったことも、実際よく行われているため、個々のキャリアパスという単体で取り扱うのではなく、「組織モデル」と合わせて組織やプロジェクトを遂行するにあたり、どのような人財が必要なのかを特定するのに役立つ。

（3）キャリアパスの必要性

ISEPAではキャリアパスに対する共通認識の提示をすることにより、情報セキュリティ人財にとって、段階的な道筋を作るこ

とによって目標意識が高まり、仕事に対するスキルも効率よく高めていくことができると考えている。キャリアパスを明確にすることにより、自分の仕事において、過去の職歴から現在の職務を通して今後の希望や予想による職歴まで一貫して俯瞰することができるため、キャリアパスは仕事の経験やスキルを積みながら自らの能力を高くしていくための順序を系統立て、将来の目的や昇進プラン、キャリアアッププランを具体化、明確化することに活用できる。

キャリアパスは個人の自己啓発で自らのキャリアを磨いていくために活用するものであると同時に企業の人事部門などが大勢の雇用者の適性を的確に把握し各雇用者に最適な職務を与えるための判断材料として活用することもできる。また、企業にとっては、キャリアパスを明確にすることにより、人材と実務のミスマッチによる早期退職を未然に防止する、といった狙いが考えられる。

キャリアパスを個人が形成するときに、自然と実務経験から必要な知識や経験を身につけてキャリアパスを形成できる人財も少なくないが、個人のキャリアパスは、社会・会社組織など様々な制約事項と経緯があって、『現在の自分』があることが多く、その制約の中で、個人がさらに次のキャリアパスに到達しようと考えるのは当然の話だが、しかし、その目標達成を現在の環境の中で満たすことができる場合と、できない場合があるので、個人のキャリアパスを形成する上では、組織体と個人が考えるキャリアパスの整合を取る必要がある。

（4）現状（As Is）とあるべき姿（To Be）

キャリアパスを形成する場合、あるべき姿だけを追いかけても、あまりに現状からかけ離れていると、ギャップを埋めるプランを立てることが難しく、また立てたとしても現実感に乏しいものになってしまうことがある。しかし、懸命に現状認識をしても、それだけではどこへ向かうかが明らかにならない。ただし、現状認識をすることにより課題が明確となり、達成する目標はここ数年の方向や考え方について議論することは可能となる。そこで、少なくともプランを立てるにはAs IsとTo Beが必要となり、そのギャップから考えていくことが重要となる。

ISEPA では、キャリアパスを形成する上で重要なのは、To Beとは組織体からだけ与えてもらうものではなく、自らも考えて定義し、責任をもって遂行するということだと考えている。その枠組みの中でAs Isを明確にするというのが正しいアプローチであり、また、プランを立てて実践していくということは、仮説と検証の繰り返し、つまりPDCAを廻すということになる。このPDCAも育成側、育成される側の両輪で実証していくことが重要だと考えている。なお、現在ISEPAが定義しているキャリアパスは、仮説段階のため、今後の実証実験による検証が必要となることはご了承いただきたい。

（5）キャリアパスの事例

ここからは、ISEPAが仮説定義したキャリアパスマッピングについて、いくつかの代表例をもとに解説を行う

① キャリアパスA：プログラマーからCSO/CISO/CIAOを目指すキャリアパスモデル

職種名	定義
CSO/CISO/CIAO	情報資産保護を経営の観点から意思決定をし、指揮をとり、組織の情報資産保護の責任をとる
CSO/CISO/CIAO補佐	CSO/CISO/CIAOの業務を補佐し、経営陣の意思を現場に浸透させ、施策がきちんと実行されるかを監視する
セキュリティアドバイザー	情報セキュリティ全般に関してのアドバイスを行う
プロジェクトマネージャー	プロジェクトの計画と実行に於いて総合的な責任を持つ。期日までに成果物を完成させる。
テクニカルコンサルタント	情報セキュリティに関する経験値が高く、技術的見地からのアドバイスやレビューを行う
セキュリティエンジニア（企画・設計）	セキュリティ・ソリューションの企画・設計・最新技術調査、製品評価
プログラマー	仕様書や設計書に従って、セキュアプログラミングの知識を持ってプログラムを作る。

キャリア形成の第一歩として、配属先の部門、または新人研修などで社会人としてのマナー、組織・役割、与えられた仕事を理解し正確スピーディーに処理することを学ぶ必要がある。これはどの部署に配属されても同様に必要となるスキルである。そ

の後は、配属先に応じてベースとなるスキルを習得していく。

キャリアパスAでは、配属先での役割はプログラマーとした。プログラマーとして、プログラミング技術を習得しつつ、情報システムの設計工程やセキュリティについての知識を身につけていく。仕様書を読み書きできるようになれば、セキュリティエンジニアとしてステップアップし、開発、製品評価等の経験やセキュリティに関連する業務設計、システム設計等を満遍なく経験していく。その後、情報システムを包括的な視点で見られるようになるため、テクニカルコンサルタントとしてプロジェクトの基盤メンバーとしてさまざまなプロジェクトを横断する実務経験を積み、プロジェクトマネージャーとしてプロジェクトを完遂できる手法を身につけていく。その後は数多くの選択肢が用意されるが、セキュリティアドバイザー、CSO/CISO/CIAO補佐として、経営陣の意向を汲み取りながら、情報セキュリティ全般に関してのアドバイスを行ったり、経営陣の意思を現場に浸透させていき、最終的には、CSO/CISO/CIAOとして企業の経営情報の管理や個人情報の管理の責任を担うことになる。

② キャリアパスB：オペレーターからCSO/CISO/CIAOを目指すキャリアパスモデル

職種名	定義
CSO/CISO/CIAO	情報資産保護を経営の観点から意思決定をし、指揮をとり、組織の情報資産保護の責任をとる
CSO/CISO/CIAO補佐	CSO/CISO/CIAOの業務を補佐し、経営陣の意思を現場に浸透させ、施策がきちんと実行されるかを監視する
セキュリティアーキテクト（コンサル）	セキュリティ確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務
セキュリティコンサルタント（マネージメント）	情報セキュリティ戦略立案から、情報資産の管理・運用方法の策定までに関し、顧客の問題解決を支援する。
セキュリティアナリスト	各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を提示
オペレーター	提供しているサービスの運用・監視を行う。ネットワーク監視。ヘルプデスク。サービスシステム維持管理等

キャリア形成の第一歩として、配属先の部門、または新人研修などで社会人としてのマナー、組織・役割、与えられた仕事を理解し正確スピーディーに処理することを学ぶ必要がある。これはどの部署に配属されても同様に必要となるスキルである。その後は、配属先に応じてベースとなるスキルを習得していく。

キャリアパスBでは、配属先での役割はオペレーターとした。まずは、ベースとなる技術習得として、情報システムやネットワークを運用、監視することにより、OSやネットワーク技術や関連するセキュリティを習得していく。情報システムのシステム管理、ネットワーク管理を包括的に理解できるようになれば、セキュリティアナリストとしてステップアップし、セキュリティデバイスや様々なログを相関的に分析する経験やインシデントレスポンスに関連する業務設計、システム設計等を満遍なく経験していく。その後、情報システム全体に必要なセキュリティを提案できるようになるため、セキュリティコンサルタントとしてプロジェクトの基盤メンバーとしてさまざまなプロジェクトを横断する実務経験を積み、セキュリティアーキテクトとして顧客毎に仕様が異なるプロジェクトに対して必要なセキュリティを確保するための手法を身につけていく。その後は数多くの選択肢が用意されるが、セキュリティアドバイザー、CSO/CISO/CIAO補佐として、経営陣の意向を汲み取りながら、情報セキュリティ全般に関してのアドバイスを行ったり、経営陣の意思を現場に浸透させていき、最終的には、CSO/CISO/CIAOとして企業の経営情報の管理や個人情報の管理の責任を担うことになる。

（6）キャリアパスモデルの利用にあたり

二つのキャリアパスモデルを定義してみたが、キャリアパスモデルはあくまでも参考例としての位置付けであり、個々の立場に応じたキャリアデザインを作成する必要がある。なお、新社会人や若手社員については、自己の目標設定や自己点検は難しいと考えられるため、配属から2, 3年は積極的なメンターの関与が必要と考えられる。また、キャリアパスを過剰に意識し、評価時点においての目的達成度が影響し、個々の理念を見失うこともあるため、キャリアパスを重視するあまり、行き過ぎた目標設定を人材育成側、育成される側で行っていないかは定期的な As is , To be の評価の中で行っていく必要があることを忘れないでいただきたい。

As is 、To be をうまく繰り返すことができるようになれば、キャリアパスを通じて、個人が自分の特質や、仕事の達成感、存在意義、理念を強く認識し、状況に応じた判断をしていく、自分らしいキャリア・モデルの確立ができる手助けとなる。キャリアパスを職種と合わせて明示することで、エンジニアは自分の立ち位置が確認できるようになり、現在の職種とキャリアレベルがどこにあるかを認識し、将来はどこを目指すのかをイメージしやすくなる。これは個人としてのキャリアアップやキャリアシフトという観点でも有効だが、上長とのコミュニケーションにおいても非常に有効となる。スキルやキャリアといった共通の相場観を使ってコミュニケーションすることは、コミュニケーションギャップやロスを少なくし、組織としての開発力強化にも貢献することが期待される。キャリアパスモデルを参考にしていただき、自己認識と将来パスの立案の手助けになれば幸いである。

（7）キャリアパスを形成する手段

今回の報告書では、情報の共有/トレーニングの重要性について踏み込んで考察をしていないが、キャリアを構築していくにあたり、「社内のトレーニング制度が入念に設計・確立されていること」や「社内での情報共有のしくみが充実していること」等の個人・組織として成果を出していく上での環境面での充実度は重要と考える。それらが知見、知識の吸収をより効率的、効果的にしていることは周知の事実であり、特に情報セキュリティに関連したキャリアの場合は、昨今の情報セキュリティに関する事件・事故事例を見てとれるように、企業内全域にわたるメンバー同士で、頻繁に双方の知見を吸収しあうことができる環境が必要となる。組織モデルの中では言及していないが、勉強会やコミュニティのような形で、必要な知見をプロジェクト内外問わず、多くのメンバー間で共有する文化も必要と考える。

3.2　セキュリティ組織モデル

セキュリティ組織モデルについては、「企業内CSIRT」、「情報セキュリティシステム開発プロジェクト」、「組織内情報セキュリティ機能」という3モデルについて策定したが、今回は「企業内CSIRT」を代表例として紹介する。なお、企業内CSIRTの組織モデルを作成するにあたり、以下のJPCERT コーディネーションセンター（以下JPCERT/CC）の資料を参考とした。

JPCERT/CC CSIRTマテリアル
http://www.jpcert.or.jp/csirt_material/

（1）企業内CISRTの編成

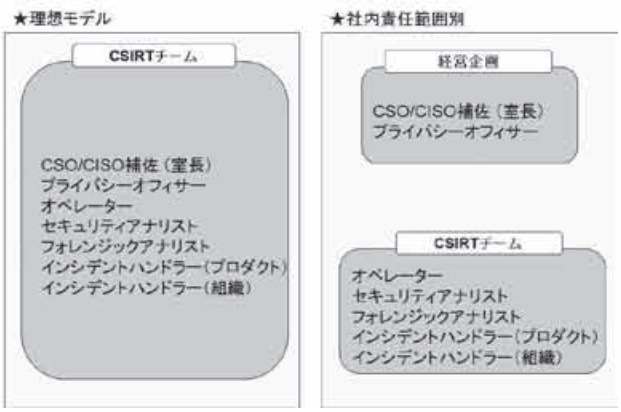
JPCERT/CC の CSIRTマテリアルの組織内CSIRTの定義では、「組織内CSIRT の実装モデル、組織内CSIRTの実装に係る検討は、情報システム部門などに一任するのではなく、会社全体のプランニング・デザインに関わる経営企画部門・総務部門等が担当することが望まれる。なぜなら、CSIRTの実装により、経営層への効率的なレポーティング、ブランドイメージの確立といった全社規模の効果が期待できるためである。」とある。

全社規模での対応が必要ということは、インシデントの種類にかかわらず、社内の対応は常に一貫している必要があり、理想的にはインシデント対応チームは全社的なインシデントレスポンスを行う必要があるため、CSO/CISO補佐（室長）、プライバシーオフィサー、オペレーター、セキュリティアナリスト、フォレンジックアナリスト、インシデントハンドラー（プロダクト）、インシデントハンドラー（組織）が構成される。また、特定のインシデントが発生したときにのみ、インシデント対応に参加することになる部門が発生するが、ここでは個別チームについては言及しないこととする。

前述として、企業内CSIRTを編成するにあたり、全社規模の組織編成が必要とあるが、実際のところ定常的に企業内CSIRTを編成できる企業は稀だと思われる。現実的な企業内CSIRTの編成は、社内責任範囲別など仮想チームを構成する組織が一般的だと考えられる。仮想チームを編成するためには、定常的CSIRTと同じ職種が必要となるが、専門的にインシデントレスポンスを職務として担当するメンバーではない。ただ、ひとたびインシデントが発生すれば、インシデント対応チームのすべてのメンバーが緊密な相互連絡を通じて、可能な限り短時間で、なおかつ可能な限り整然とした方法で、問題の解決に当たる必要がある。

どの場合も、セキュリティアナリスト、インシデントハンドラー、フォレンジックアナリスト、およびオペレーターの各チームの代表者がインシデント対応のコアチームを形成する。各チームは組織の資産保護に関する緊急の必要条件を満たすことがで

きるように、運用に関する評価とリソースの割り振りを行う。チームごとに、そのチームの活動に関して責任を負うリーダーが割り当てられ、インシデントの種類によっては、他のグループも活動に参加する必要がある。



図表11 ）組織モデル　－　企業内CSIRT

（2）必要となる人材とスキル、職種の特定

企業内CSIRTを構成するにあたり必要な人材群は以下の通りとした。今回のモデルでは、企業内CSIRTを構成する上で一般的であろう仮想チームで区分を行った。

経営企画

CSO/CISO補佐（室長）

インシデント対応のコアチームとして機能する
経営陣を含み必要なグループとの間で対応戦略を調整する
CSIRTオペレーションに必要なスタッフを確保する
企業内CSIRTを24 時間体制で運用する場合、シフト勤務の配慮、スキルに応じたチーム編成、シフト責任者を指名する
インシデント対応業務の管理者として機能する
経営陣への説明窓口として機能する
イベントの包括的な記録を維持管理する
処置内容と収集した情報に基づき、状況報告書を適宜作成、提供する
必要だと考えられるすべての連絡調整先を洗い出し、経営陣へ提出する
社内広報部門と定期的な調整を行う
報道メディアを監視し、インシデントに関連する情報を収集する
インシデントに応じた緊急連絡先リストを維持管理する

プライバシーオフィサー

インシデントによる顧客や風評への影響を分析する
組織の規模に応じた個人情報保護管理者を設置する
各事業所の個人情報保護管理者からプライバシーオフィサーへのエスカレーションルールを明確にする
各事業所の個人情報保護管理者からプライバシーオフィサーへの報告ルールを明確にする

CSIRTチーム

セキュリティアナリスト

システムをネットワークから切断しなければならなくなる可能性があるコンピューターウイルスに感染したとき、システムへの影響を最小限に抑えながらコンピューターウイルスを抑制するための手段を決定する
侵入されたシステムに対して設計、実装、運用の問題がないかどうかを分析する

システムログと現状のシステムを検査し、結果を比較検証する
インシデントを検知しやすくなるように、監視システムを適宜調整する
影響を受けたすべての情報資産を特定し、オペレーターなどと連携し、復旧、回復作業を行う
ネットワークへの不正侵入が発生した場合、CIO/CIO補佐官やプライバシーオフィサーから外部機関に対し、アカウント、パスワードの漏えいによるシステム利用者への二次被害の予防対策を依頼するよう調整する

フォレンジックアナリスト

調査のイニシアティブをとり、現場を押収する
証拠を収集、保持する
収集した証拠を一元管理する
デジタルフォレンジックを必要に応じて行う
インシデントに関連する情報システムに対してデジタルフォレンジックを実施する
社内、社外を問わず関連組織の担当者と適宜調整を行う

インシデントハンドラー（組織）

インシデントレスポンスの各チーム間で会議やその他の通信手段を準備する
緊急時を考慮し、代替通信手順を準備、浸透させる
経営陣が設定した経過計画に基づき、状況報告書を公開する
社内広報部門と定期的な調整を行う
修正プログラムのリリース時にシステム利用者や関連する組織への通知を行う

インシデントハンラー（プロダクト）

検査を繰り返し実行し、感染したシステムを特定して、製品に対するリスク評価を実施する
製品に脆弱性が見つかった場合は、CSO/CISO補佐（室長）を中心に、社内広報部門、オペレーターなど、他の組織に協力を依頼する
製品開発部門に対し、脆弱性の検証が必要なことを連絡するとともに、詳細な脆弱性情報を収集し、提供する

オペレーター

システム利用者からの様々な問い合わせに対応する（不審だと思うメールを開いてしまい、コンピューターウイルスに感染したかもしれないなどの相談）
インシデントによりコンピューターウイルスに感染した社内インフラを構成するサーバー群に対して、復旧作業、修正パッチの適用を実施する
社内インフラと接続された社外インフラを構成するネットワーク機材やリモートアクセスサーバー群に対して、復旧作業、修正パッチの適用を実施する
システム利用者へ、ウイルス対策ソフトウェアやパッチの適用を促すようメールなどを通じて連絡する
侵入検知システムを維持管理する
実際の事件、事故事例に応じたモニタリングを設計、実施する
適切なログの収集を取りまとめる
すべてのログを維持および分析する
ネットワークへの脅威と脆弱性が出現したときに、それらを確認する
インシデントの脅威評価を準備する
セキュリティ上の脆弱性を検出して修正する
インシデントレスポンスを向上するために独自のツールを作成する
既存のツールをインシデントレスポンス用に改良する
既存のツールか独自のツールを使ってレポートを実行する

（3）組織モデルを利用するにあたり

組織モデルの代表例として、企業内CSIRTの組織モデルを策定してみたが、事業体における組織構成により必要とされる人材群は異なるであろう。この組織モデルを参考に、皆様の組織に合わせた組織モデルを作成してみてはいかがだろうか。また組織モデルを特定する場合は、職種名に拘るのではなく、実際に業務を遂行できる人財かどうかを重要視して欲しい。引き続き、ISEPAの組織モデルにおいては、どういうスキル・知識を持っているべきかについて提唱していく。

4． 利用・運用の指針

4.1 利用する立場とその視点

「スキルモデル」「人材モデル」を使って、どのように実際の人材の育成や維持・管理をしていくのか、その利用・運用・評価の方法論をモデル、ガイド（指針・手引き）として示す。

まず、本アーキテクチャの目的でも述べているように、このモデルの利用者としては、おもに以下の3者を想定している。

- 育成や管理をするもの
- 人材を目指すもの
- 人材を使う（委託・発注）もの

何のために、どう使うのか、という観点から検討すると、情報セキュリティの業務を実施する側と情報セキュリティ業務を委託する側の、大きくは2つに分類されるであろう。そして、さらに情報セキュリティの業務を実施する側では、育成や管理をするもの（業務の実施主体である組織）と情報セキュリティ人材を目指すもの（個人）の2つに分けられる。

立　場	期待される効果
情報セキュリティの業務を実施する側	①情報セキュリティ人材を目指す個人にとって：目標の自己設定や評価ができる。 ②情報セキュリティ人材を育成する組織にとって：実効性が高い人材の育成、評価や管理ができる。
情報セキュリティの業務を委託する側	業務を委託する際に、要件に合った適切な人材を要求・調達できる。

図表12 ）キャリアプラン策定の効果

この3者が、それぞれの視点と目的で利活用できる共通の枠組みとして示せることを目指している。さらに、この3者が具体的にどのような利用をするのかを想定している。

そこで、ここからはこの2つの分類と3つの立場に分けて、それぞれの視点から利用のイメージを示すこととする。

4.2 業務を実施する側での利用

セキュリティシステムの構築や運用など、適切な情報セキュリティ業務の実施のためには、その業務を行う要員の質（知識やスキル、実績など）が不可欠な要素となる。適切な技術を選択し、システムを設計しても、その実装や運用管理をするのはあくまで人間である。そのため、これらの業務にかかわる要員の質を客観的かつ相対的に評価や確認しておきたい。要員の質が評価や確認できることは、需要側と供給側、つまり業務を実施する側と委託する側、それぞれのメリットとなる。情報セキュリティの業務を実施する側としては、業務の内容や要件に合致した実効性が高い人材の育成、評価や管理ができる。

（1）キャリアプラン策定の要素とプロセス

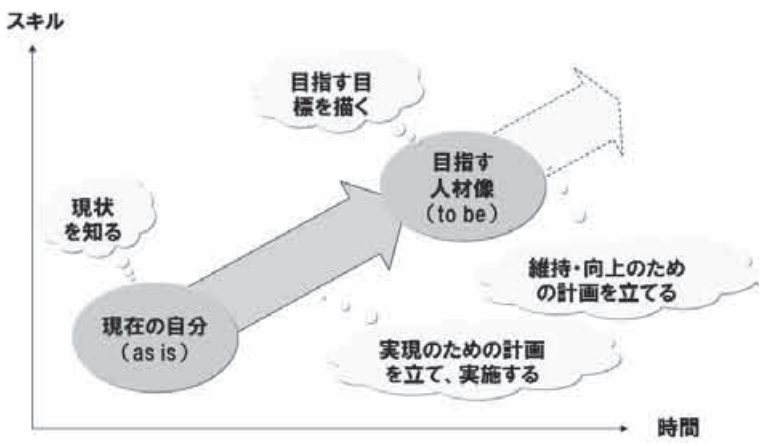
情報セキュリティの業務を実施する側としては、人材育成を実施するための計画、すなわち「キャリアプラン」を策定することになるであろう。

そのためには、まずその人材の現状（知識やスキルレベル）を知る必要がある。この場合、自己申告ではなく、第三者による客観的な評価の結果であることが望ましい。

次に、人材が目指す目標を描くことが必要になる。

続いて、その目指す目標を達成するための計画を立てることになる。

さらに、目標達成後も、それを維持したり、さらに次の目標を目指したりするために、計画を立てることになる。



図表13）キャリアプラン策定のイメージ

そして、この際にキャリアパスモデルや教育、資格などを利用し、キャリアプランを実行していくことになる。

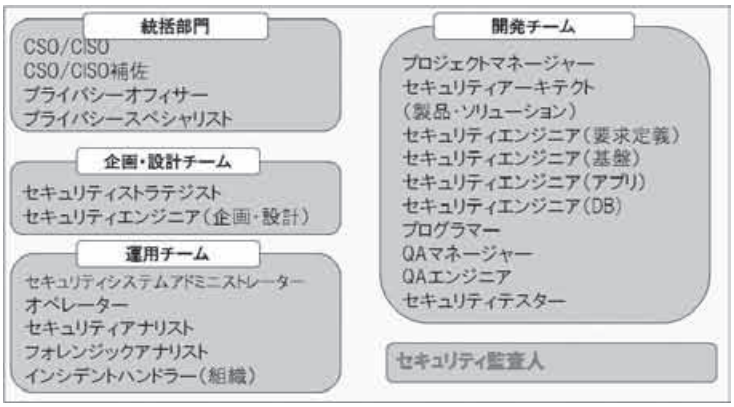
「現状を知る」ために	自分の「現状」（知識やスキルのレベル）の客観的評価結果
「目指す目標を描く」ために	職種（役割）とその業務内容、そこまでのキャリアパス
「目指す目標を実現する計画と実施」のために	現状と目指す目標のギャップ、それを埋めるための手段（教育・資格）
さらなる維持や向上のために	目指す目標を取り巻く今後の環境変化、それに対応するための手段（教育・コミュニティ）

図表14）キャリアプラン策定に必要なもの

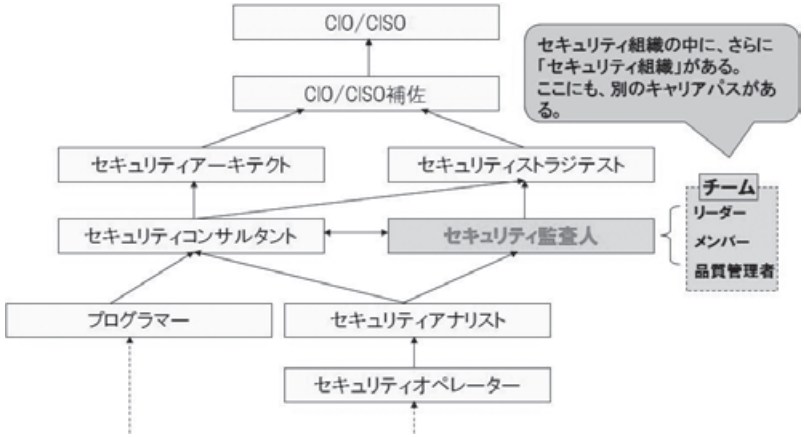
（2）キャリアプランの2つのモデル

キャリアプランを、大きく2つに分類した。1つは職種が変わっていくモデルであり「キャリアチェンジモデル」と呼ぶことにする。もう1つは同じ（もしくは類似する）職種の中で上位のレベルを目指すモデルであり「スキルアップモデル」と呼ぶことにする。

そして、これらのモデルを策定するにあたっては、組織モデルやキャリアパスモデルを参照することになる。



図表15 ）組織モデル –企業内情報セキュリティ機能–

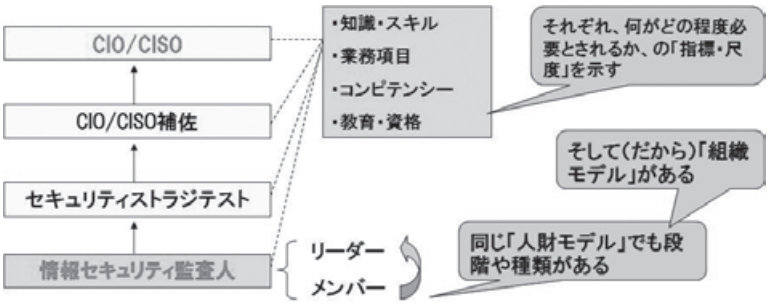


図表16 ）「セキュリティ監査人」のキャリアパス

①キャリアチェンジモデル

キャリアチェンジモデルは、同じ情報セキュリティ分野の中で職種が変わっていくモデルである。情報セキュリティ人材を目指すもの自身の意思、または人材を育成管理する側の方針、事業や業務の都合などで、職種を変えることが想定される。

ここでは、「セキュリティ監査人」の例でそのイメージを示す。

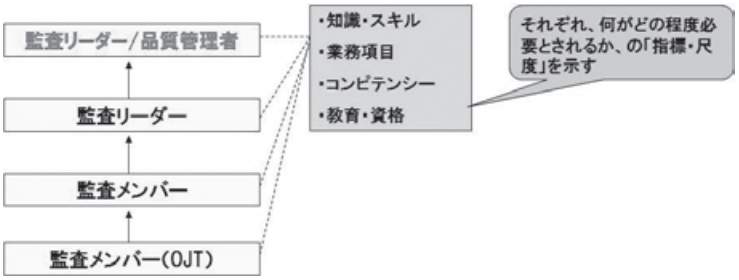


図表17 ）キャリアプラン・イメージ（1）キャリアチェンジ

②スキルアップモデル

スキルアップモデルは、同じもしくは類似する職種の範囲で、上位のレベルを目指すものである。どの職種においても、何段階かのランクが存在すると思われる。この場合、ランクの基準に一般的になるものが、知識やスキルのレベルと業務経験である。これにより、その要員に業務をさせる役割や責任も違ってくる。教育や業務の中で、知識やスキル、経験を身につけ、必要に応じて上位のレベルの役割になっていくことになる。

ここでは、キャリアチェンジモデルと同様に「セキュリティ監査人」の例でそのイメージを示す。



図表18) キャリアプラン・イメージ (2) スキルアップ

4.3 業務を委託する側での利用

業務を委託する側での利用においては、その業務が意図したとおりに適切かつ十分に実施されるようにするために、業務を実施する側の要員、すなわち情報セキュリティ人材の現状を知る必要がある。

前節でも挙げたように、要員の質が評価や確認できることは、需要側と供給側、つまり業務を実施する側と委託する側、それぞれのメリットとなる。情報セキュリティの業務を委託する側としては、業務委託する際に、要件に合った適切な人材を要求・調達でき、ミスマッチ防止が可能になる。

また、この評価や確認の際に一般的に尺度となるのが資格である。その人が資格を所有するか、それがどのような資格かにより、一定水準以上の知識やスキルを持つ要員であるか否かが確認できる。(なお、主な情報セキュリティ関連資格については、本ガイド付録の「情報セキュリティ職種別教育資格マップ」を参照されたい)

情報セキュリティ関連資格は様々存在するが、その資格により習得できる知識が異なる。

前述のようなミスマッチを防ぐためにも、要求する業務内容に専門性やレベルが合致しているかどうか、調達の際に、各資格の試験分野などを見ておくことで確認しておきたい。

また、資格の中には「維持教育」を更新要件としているものがある。情報セキュリティ分野は技術の進歩や環境変化などにより、知識やスキルが陳腐化しやすい。このような仕組みを持つ資格制度では、更新要件を満たさない場合は継続してその資格を所有できない。そのため、知識やスキルが陳腐化した過去のものではなく、現在も維持されたものであることを確認することができる。

さらに、業務が遂行できるかどうかを判断するためには、資格のほかに実績も確認しておきたい。資格はある一定水準以上の知識やスキルがあることを確認できるものであるが、業務の遂行能力そのものを確認できるものではないからである。これらの裏付けとはなるが、その評価や確認の代替手段となるものではない。実績に関しては、経験年数が評価の尺度として使われることが多いが、むしろ経験してきた内容やレベルが重要であり、それを確認しておきたい。

4.4 今後の課題

最後に、この「情報セキュリティ人財アーキテクチャー」の今後の課題を挙げておきたい。現状、認識されている課題には、以下のようなものがある。

・利用にあたってのより具体的な手段を示せていない。
・情報セキュリティ人材を目指すものと育成する側の「非対称性」(同じように「見える化」されていない)。
・ここに示したモデルの有効性の検証ができていない。
・情報セキュリティ関連の資格や教育がすべて網羅できているわけではなく、すべての職種(役割)に対応しての資格や教育が存在していない。

・他のITに関わるフレームワーク（ITSS V3など）との関連などが示せていない。
・情報セキュリティ分野以外の職種とそれに関連する教育や資格の関係が示せていない。（情報セキュリティ分野⇔他分野のキャリアパスが見えない）

これらの課題は、今後の調査研究や実証実験により解決をしていく予定である。そして、その結果や経過については、このガイドの次期バージョン等で公表していく予定である。

情報セキュリティ人財アーキテクチャ
職種別・人財育成マップ
2009年度版

情報セキュリティ人財アーキテクチャ　職種別・人財育成マップ
目　次

情報セキュリティ人財アーキテクチャ 職種別・人財育成マップ

	職種	定義
1	プリセールスエンジニア	セキュリティ製品導入を検討する企業に対し、どのような環境なら顧客の要望が実現可能なのか製品・サービスに関する技術的知識を持って営業活動を支援する
2	セールスコンサルタント	顧客システムの現状の把握および問題点の調査し、顧客の状況に合わせて、適用範囲が広範囲な製品・ソリューション対策/提案をする
3	テクニカルコンサルタント	情報セキュリティに関する経験値が高く、技術的見地からのアドバイスやレビューを行う
4	セキュリティアーキテクト(製品・ソリューション)	セキュリティ製品・ソリューション開発の設計、及び管理
5	セキュリティアーキテクト(コンサル)	セキュリティ確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務
6	セキュリティエンジニア(要求定義)	セキュリティ・ソリューションに関する要求定義を行う
7	セキュリティエンジニア(企画・設計)	セキュリティ・ソリューションの企画・設計・最新技術調査、製品評価
8	セキュリティエンジニア(基盤)	セキュリティ・システムの基盤部分(OS・ネットワーク)の全体設計・運用設計・方式設計、開発
9	セキュリティエンジニア(アプリ)	アプリケーションの開発フェーズにおいてセキュリティの確保を行う
10	セキュリティエンジニア(DB)	DBMSを構成要素とするシステムを対象に、セキュリティの確保を行う
11	QAマネージャー	品質保証業務及びそのプロセス改善業務。製品品質に関する顧客窓口業務。開発チームに対する品質保証啓蒙活動
12	QAエンジニア	ソフトウェア開発および開発プロジェクトに対し、品質保証全般のテストを実施。
13	セキュリティテスター	ソースコード解析や脆弱性の洗い出し
14	プログラマー	仕様書や設計書に従って、セキュアプログラミングの知識を持ってプログラムを作る。
15	プロジェクトマネージャー	プロジェクトの計画と実行に於いて総合的な責任を持つ。期日までに成果物を完成させる。
16	セキュリティシステムアドミニストレーター	システムに対するセキュリティ対策を整備し、運用管理を行う
17	オペレーター	提供しているサービスの運用・監視を行う。 ネットワーク監視。ヘルプデスク。サービスシステム維持管理等
18	セキュリティアナリスト	各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を提示
19	フォレンジックアナリスト	証拠証跡の分析を行い、証拠保全、証拠開示手続きも行う
20	インシデントハンドラー(プロダクト)	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
21	インシデントハンドラー(組織)	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
22	フィールドエンジニア	顧客現場で、セキュリティシステム構築に伴う、システム機器の設置から設定保守・修理を行う
23	プライバシーオフィサー	企業・団体内の個人情報保護体制の構築、運用、改善を行う
24	プライバシースペシャリスト	企業の個人情報保護に関して、規定作成から意識向上施策実施までを担当する
25	CSO/CISO/CIAO	情報資産保護を経営の観点から意思決定をし、指揮をとり、組織の情報資産保護の責任をとる
26	CSO/CISO/CIAO補佐	CSO/CISO/CIAOの業務を補佐し、経営陣の意思を現場に浸透させ、施策がきちんと実行されるかを監視する
27	セキュリティプロダクトオーナー	セキュリティ製品の企画から保守にいたるまで製品に関わる全責任をとる
28	セキュリティサービスオーナー	セキュリティサービスの企画から保守にいたるまでサービスに関わる全責任をとる
29	セキュリティコンサルタント(マネージメント)	情報セキュリティ戦略立案から、情報資産の管理・運用方法の策定までに関し、顧客の問題解決を支援する。
30	セキュリティアドバイザー	情報セキュリティ全般に関してのアドバイスを行う
31	セキュリティストラテジスト	企業の経営戦略実現にむけて、セキュリティを活用とした基本戦略を策定、提案、推進する
32	セキュリティ監査人	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する

この32職種の一覧ファイルはISEPAのWebサイトで閲覧・ダウンロードが可能です。

詳細は http://www.jnsa.org/isepa/ をご覧下さい。

職種名	プリセールスエンジニア		
定義	セキュリティ製品導入を検討する企業に対し、どのような環境なら顧客の要望が実現可能なのか製品・サービスに関する技術的知識を持って営業活動を支援する	所属企業・部署グループ	サービス・製品提供組織　営業

業務項目
必須業務：
情報セキュリティ対策の製品の選定ができること
単一の技術や基盤に依存する事のリスクを認知できる
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティに関する情報収集、分析、共有
実施可能業務：
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
セキュリティ強化に資する新規システムの導入検討
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
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
潜在的に大きなリスクの対処方法のあり方を考えられること
IT障害についての分析ができること
IT障害の要因等の対策検討をして再発防止ができること
各業務・システムの最適化ができること
IT障害、リスクについての分析と改善
教育
LS-0, Hyogo-B, SPIA-T, SANS-SEC301, 401, LACB5-14
資格
SSCP, SEAj-B, SEAj-T, CTIA, SANS-GSEC

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		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
	その他のサーバーアプリ(FTP, IRC, VoIPなど)	概論
ファイアウォール		概論
侵入検知		概論
セキュリティ運用		概論
認証	認証	種類
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論

スキル・知識		
推奨：		
知識項目	大分類	中分類
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
	OSセキュリティ【Unix】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
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
コンテンツセキュリティ	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
PKI(Public Key Infrastructure)	PKI(Public Key Infrastructure)	PKIの利用
暗号	暗号	暗号方式概説
		公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
セキュリティプロトコル		
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
物理セキュリティ	物理的脅威	

職種名	セールスコンサルタント		
定義	顧客システムの現状の把握および問題点の調査し、顧客の状況に合わせて、適用範囲が広範囲な製品・ソリューション対策/提案をする	所属企業・部署名	サービス・製品提供組織　営業

業務項目

必須業務：
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策の製品の選定ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
単一の技術や基盤に依存する事のリスクを認知できる
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティに関する情報収集、分析、共有
セキュリティ強化に資する新規システムの導入検討
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
実施可能業務：
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
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
潜在的に大きなリスクの対処方法のあり方を考えられること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティ監査制度の活用ができること
各業務・システムの最適化ができること
IT障害、リスクについての分析と改善
教育
LS-0, Hyogo-B, SANS-SEC301, 401 501
資格
CISSP, SSCP, CTIA, SEAj-T, SEAj-B, SANS-GSEC

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		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
ファイアウォール		概論
侵入検知		概論
セキュリティ運用		概論
認証	認証	種類
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論

スキル・知識

推奨：		
知識項目	大分類	中分類
アプリケーションセキュリティ	その他のサーバーアプリ(FTP, IRC, VoIPなど)	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
	OSセキュリティ【Unix】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
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
コンテンツセキュリティ	電子透かし	電子透かしの応用形態
認証	認証	種類
		認証方法
		認証機能
		統合認証
		計画と管理
PKI (Public Key Infrastructure)	PKI(Public Key Infrastructure)	PKIの利用
暗号	暗号	暗号方式概説
		公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
セキュリティプロトコル		
物理セキュリティ	物理的脅威	

職種名	テクニカルコンサルタント		
定義	情報セキュリティに関する経験値が高く、技術的見地からのアドバイスやレビューを行う	所属企業・部署名	サービス・製品提供組織　営業・開発

業務項目

必須業務：

- 単一の技術や基盤に依存する事のリスクを改善できる
- 情報セキュリティ機能の明確化出来るスキル
- 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
- 単一の技術や基盤に依存する事のリスクを認知できる
- 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
- セキュリティ強化に資する新規システムの導入検討
- 情報セキュリティ対策の製品の選定ができること

実施可能業務：

- 情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
- 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
- ファイル暗置化ソフトウェアの導入を選定・検討ができること
- 電源監視の導入ができること
- 通信端末の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
- IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
- 情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
- 情報セキュリティの企画・設計段階からの確保ができること
- ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
- 情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
- 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
- 発生頻度の高い箇所のIT障害への対応方策を策定できること
- 情報セキュリティ対策に関する費用対効果の測定ができること
- 情報システムに係るリアルタイム監視機能をもてること
- 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
- 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
- 横断的な監視情報の収集機能がもてること
- 攻撃手法の分析結果情報の共有ができること
- フォレンジック
- IT障害の未然防止ができること
- 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
- ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
- ネットワークの不適正な利用からの被害防止対策ができること
- 情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
- 情報セキュリティ対策の手引きの作成ができること
- 潜在的に大きなリスクの対処方法のあり方を考えられること
- 最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
- 安全なWebサイト構築の為のガイドラインを検討できること
- インターネット定点観測情報共有システムの構築ができること
- 業務・システムの基盤となる共通的なプラットフォームの構築ができること
- 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
- 本人認証を容易に行うことが可能な環境の構築ができること
- 外部記録媒体に保存する情報を自動的に暗号化等するソフトの導入（設計～運用）ができること
- 可視化システムの構築ができること
- コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内規範・運用の推進
- 情報管理の徹底をさせられること
- 情報セキュリティ対策の実施手順及び成果等の共有化ができること
- インシデント対応
- 情報セキュリティ対策の実施状況の自己点検ができること
- 情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
- 情報セキュリティ問題に関するPOC機能を持てること
- 定点観測データの共有ができること
- ネットワーク監視
- 取り組みが不十分な情報セキュリティ対策の具体的な導入運用に当たって参考となる手引きの作成ができること
- 通信の監視が出来ること
- IT障害についての分析ができること
- IT障害の迅速な復旧ができること
- 情報通信の静的な機能維持ができること
- 攻撃手法の分析能力の強化ができること
- IT障害の要因等の対策検討をして再発防止ができること
- 情報セキュリティに関する情報収集、分析、共有
- 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
- IT障害の拡大防止ができること
- 事業継続マネジメント(BCM)
- オフショア・アウトソーシングに関連する固有リスクを把握できること
- 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）
- サイバー攻撃発生時の適時適切な機能回復を持たせられること
- 情報アクセス制御を統合し集中管理ができること
- 各業務・システムの最適化ができること
- IT障害、リスクについての分析と改善
- CSIRTに対する情報提供体制の構築＆確立
- 事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
- 電子文書に係る成りすまし及び改ざんの防止ができること
- ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
- 情報セキュリティに関する取り組みについて全体としての整合性が確保できること
- IP v6によるユビキタス環境構築に向けたセキュリティが確保できること

教育

LS-0, Hyogo-B, SEAj-T, SEAj-B, SPIA-T, LACBS-14, 19,19.20, SSCP, SANS-SEC301, 401, 501, 560, AUDS07,

資格

CISM, SSCP, CISSP, CTIA, SEAj-T, SEAj-B, CCIE-Sec, CCSP, CTIA, SANS-GPEN, SANS-GSNA

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		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
ファイアウォール		概論
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
		感染
		発病・被害
		不正プログラム（マルウェア）の種類
		ウイルス対策
		ウイルス対策ソフトの機能
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		概論
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	
	サービスの不正利用	情報収集
		サービス妨害
		不正操作
	マルウェア	自動実行
		遠隔操作（ボット）
	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
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
フォレンジック		概論
物理セキュリティ	物理的脅威	

推奨：

知識項目	大分類	中分類
ネットワークインフラセキュリティ		無線LAN
アプリケーションセキュリティ	その他のサーバーアプリ(FTP, DNS, VoIPなど)	概論
OSセキュリティ	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
セキュリティ運用	セキュリティ運用	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
		法的要件
	コンテンツ利用の制御	不正コピー対策
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
認証	認証	認証方法
		認証機能
		統合認証
		計画と管理
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
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手法
		監査報告書

職種名	セキュリティアーキテクト（製品・ソリューション）		
定義	セキュリティ製品・ソリューション開発の設計、及び管理	所属企業・部署名	サービス・製品提供組織　営業・開発、自社試算保護組織　開発

業務項目
必須業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
情報セキュリティ機能の明確化出来るスキル
セキュリティ強化に資する新規システムの導入検討
情報セキュリティ対策の製品の選定ができること
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
情報セキュリティの企画・設計段階からの確保ができること
ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
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
単一の技術や基盤に依存する事のリスクを認知できる
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
安全なWebサイト構築の為のガイドラインを検討できること
情報アクセス制限を統合し集中管理ができること
各業務・システムの最適化ができること
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
実施可能業務：
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
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
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
適切な暗号化及び電波の範囲設定等の対策
情報セキュリティのリスクについて定量的評価手法を選定できる
IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
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
内部統制の情報システムセキュリティ対応の要件策定
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
通信端末の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と(調達)
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
セキュア・プログラミングの導入
セキュアなデータベース構築の導入
高い保証レベルを有する情報セキュリティシステムの開発ができること
情報セキュリティシステムの新たな開発ができること
安全性・信頼性の高い情報セキュリティシステムの構築ができること
攻撃等の分析・解析機能の洗い出しができること
情報セキュリティリスクや対策の効果等に係る定量化の定義をする
製品・サービスにおける脆弱性の排除への対処
情報セキュリティに関するリスク定量化手法を考えられること
高信頼性端末の電子認証基盤の開発ができること
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
情報セキュリティ対策に関する費用対効果の測定ができること
情報システムに係るリアルタイム監視機能をもてること
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
攻撃手法の分析結果情報の共有ができること
フォレンジック
IT障害の未然防止ができること
ネットワークの不適正な利用からの被害防止対策ができること
潜在的に大きなリスクの対処方法のあり方を考えられること
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
インターネット定点観測情報共有システムの構築ができること
業務・システムの基盤となる共通的なプラットフォームの構築ができること
アクセス記録の解析、コンピュータウィルス等の動作検証、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
本人認証を容易に行うことが可能な環境の構築ができること
外部記録媒体に保存する情報を自動的に暗号化等するソフトの導入（設計～運用）ができること
可視化システムの構築ができること
情報セキュリティ対策の実施状況の自己点検ができること
IT障害についての分析ができること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
IT障害の拡大防止ができること
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）
サイバー攻撃発生時の適時適切な機能回復を持たせられること
IT障害、リスクについての分析と改善
電子文書に係る成りすまし及び改ざんの防止ができること
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
教育
CMU, SANS-SEC401, 501, 502
資格
CISM, CISSP, CCIE-Sec, SANS-GSEC, SANS-GCFW

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		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
	その他のサーバーアプリ(FTP, IRC, VoIPなど)	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
	OSセキュリティ【Unix】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
ファイアウォール		概論
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
コンテンツセキュリティ	情報の保護	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
		公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
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
フォレンジック		概論
物理セキュリティ	物理的脅威	
推奨：		
知識項目	大分類	中分類
ネットワークインフラセキュリティ		無線LAN
セキュアプログラミング技法	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
セキュリティ運用	セキュリティ運用	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)
	コンテンツ利用の制御	不正コピー対策
		権利管理技術(DRM)の要素技術
		権利記述言語の標準化
		法的要件
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
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手法
		監査報告書

職種名	セキュリティアーキテクト(コンサル)		
定義	セキュリティ確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務	所属企業・部署名	サービス・製品提供組織　企画・開発、自社試算保護組織　企画・開発

業務項目

必須業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
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
情報セキュリティ対策実施状況報告ができること
情報セキュリティ機能の明確化出来るスキル
セキュリティ強化に資する新規システムの導入検討
情報セキュリティの企画・設計段階からの確保ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
攻撃等の分析・解析機能の洗い出しができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
単一の技術や基盤に依存する事のリスクを認知できる
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
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
潜在的に大きなリスクの対処方法の善り方を考えられること
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
安全なWebサイト構築の為のガイドラインを検討できること
情報管理の徹底をさせられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
取り組みが不十分な情報セキュリティ対策の具体的な導入運用に当たって参考となる手引きの作成ができること
情報アクセス制限を統合し集中管理ができること
各業務・システムの最適化ができること
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
実施可能業務：
相互依存性解析の成果を踏まえた情報セキュリティ基準等が検討できること
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
情報セキュリティ対策に関する評価指標の確立が出来ること
調達における成果利用の方策の検討ができること
情報セキュリティのリスクについて定量的評価手法を選定できる
情報セキュリティに関する基準等の浸透状況について情報収集ができること
各利用者の環境に応じた対策の優先度に関する意思決定を支援するツール等の作成ができること
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
ファイル除菌化ソフトウェアの導入を選定・検討ができること
通信端末の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
情報セキュリティリスクや対策の効果等に係る定量化の定義をする
情報セキュリティに関するリスク定量化手法を考えられること
情報セキュリティ対策に関する費用対効果の測定ができること
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
フォレンジック
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティ問題に関するPOC機能を持てること
事業継続マネジメント(BCM)
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
情報セキュリティ対策の手引きの作成ができること
内部統制の情報システムセキュリティ対応の要件策定
情報セキュリティのリスクを検証する手法の整理(統一化)ができること
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策の製品の選定ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
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
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
IT障害の未然防止ができること
インシデント対応
各インフラの政府統一基準に係る必須項目の検査ができること
個人情報保護、営業機密管理
IT障害についての分析ができること
IT障害の迅速な復旧ができること
情報通信の静的な継続維持ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
IT障害の拡大防止ができること
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)
IT障害、リスクについての分析と改善
教育：
CMU, SANS-SEC401, 501
資格：
CISM, CISSP, SANS-GSEC

スキル・知識

必須：		
知識項目	大分類	中分類
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
ファイアウォール		概論
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
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
セキュリティプロトコル		概論
	トランスポート層	SSL(Secure Socket Layer)/
		TLS(Transport Layer Security)
		Socks
	ネットワーク層	IPSec
		IPinIP
	データリンク層	L2TP(Layer2 Tunneling Protocol)
		PPTP
		(Point-to-Point Tunneling Protocol)
		L2F(Layer 2 Forwarding protocol)
		MPLS(Multi-Protocol Label Switch)
		MPOA(Multi-Protocol Over ATM)
	Web関連プロトコル	HTTP(Hyper Text Transfer Protocol)
		SSL(Secure Socket Layer) /
		TLS(Transport Layer Security)
		SOAP(Simple Object Access
		Protocol)
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
		実装手段・ツール
物理セキュリティ	物理的脅威	
推奨：		
知識項目	大分類	中分類
アプリケーションセキュリティ	その他のサーバーアプリ(FTP, IRC, VoIPなど)	概論
OSセキュリティ	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
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
	コンテンツ利用の制御	不正コピー対策
		法的要件
暗号	暗号	公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
攻撃手法	ソシアルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手

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		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

職種名	セキュリティエンジニア（要求定義）		
定義	セキュリティ・ソリューションに関する要求定義を行う	所属企業・部署名	サービス・製品提供組織　企画・開発、自社試算保護組織　企画・開発

業務項目

必須業務
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
内部統制の情報システムセキュリティ対応の要件策定
情報セキュリティ機能の明確化出来るスキル
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と関連
攻撃等の分析・解析機能の洗い出しができること
単一の技術や基盤に依存する事のリスクを認知できる
実施可能業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティ対策の持続的改善の為の構造構築ができること
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
適切な暗号化及び電波の範囲設定等の対策
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
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
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
セキュリティ強化に資する新規システムの導入検討
情報セキュリティ対策の製品の選定ができること
通信環境の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
情報セキュリティの企画・設計段階からの確保ができること
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
セキュア・プログラミングの導入
セキュアなデータベース構築の導入
ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
高い保証レベルを有する情報システムの開発ができること
情報システムの堅牢な開発ができること
安全性・信頼性の高い情報システムの構築ができること
製品・サービスにおける脆弱性の排除への対応
高信頼性端末の電子認証基盤の開発ができること
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
情報セキュリティ対策に関する費用対効果の測定ができること
フォレンジック
IT障害の未然防止ができること
緊急事態対応に向けた取組み
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
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
ネットワークの不適正な利用からの被害防止対策ができること
潜在的に大きなリスクの対処方法の為り方を考えられること
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
安全なWebサイト構築の為のガイドラインを検討できること
インターネット定点観測情報共有システムの構築ができること
業務・システムの基盤となる共通的なプラットフォームの構築ができること
アクセス記録の解析、コンピュータウィルス等の動作検証、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
本人認証を容易に行うことが可能な環境の構築ができること
外部記録媒体に保存する情報を自動的に暗号化等するソフトの導入（設計～運用）ができること
可視化システムの構築ができること
情報管理の徹底をさせられること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ問題に関するPOC機能を持てること
定点観測データの共有ができること
ネットワーク監視
通信の監視が出来ること
IT障害についての分析ができること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
IT障害の再発等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
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
IT障害の拡大防止ができること
オフショア・アウトソーシングに関連する固有リスクを把握できること
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）
サイバー攻撃発生時の適時適切な機能回復を持たせられること
情報アクセス制限を統合し集中管理ができること
各業務・システムの最適化ができること
IT障害、リスクについての分析と改善
事故、災害や攻撃に対して、事前に考えられる対策を十分に施せる
電子文書に係る成りすまし及び改ざんの防止ができること
ネットワークの IP 化に対応した電気通信システムの安全・信頼性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
教育
LS-0, CMU, SPIA-T, LACSS-14,19,20, SSCP, SANS-SEC301, 401, 501,
資格
CISM, SSCP, CISSP, SIEA-T, SEA-B, CTIA, SANS-GSEC

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		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
ファイアウォール		概論
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

スキル・知識

必須：		
知識項目	大分類	中分類
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
	コンテンツ利用の制御	不正コピー対策
		法的要件
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	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
物理セキュリティ	物理的脅威	
推奨：		
知識項目	大分類	中分類
ネットワークインフラセキュリティ		無線LAN
アプリケーションセキュリティ	その他のサーバーアプリ(FTP, RPC, VoIPなど)	概論
OSセキュリティ	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
不正プログラム（マルウェア）	不正プログラム（マルウェア）	感染
		発病・被害
		不正プログラム（マルウェア）の種類
		ウイルス対策
		ウイルス対策ソフトの機能
セキュアプログラミング技法	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
		アプリケーション全般
		XML(Extensible Markup Language)
		PHP(Hype-text Preprocessor)
		JAVA
		Perl
		VB/ASP
		C/C++
		UNIX
		コンパイラ・仮想マシン
		Windows
	データベースとデータウェアハウス	データベースとデータウェア保管庫の脆弱性、リスク、防護
	ソフトウェア開発ライフサイクル（SDLC）	計画
		設計
		実装
セキュリティ運用	セキュリティ運用	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	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
認証	認証	認証方法
		認証機能
		統合認証
		計画と管理
暗号	暗号	公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
攻撃手法	攻撃手法の概論	
	サービスの不正利用	情報収集
		サービス妨害
		不正操作
	マルウェア	自動実行
		遠隔操作（ボット）

職種名	セキュリティエンジニア（企画・設計）		
定義	セキュリティ・ソリューションの企画・設計・最新技術調査、製品評価	所属企業・部署名	サービス・製品提供組織　企画・開発、自社試算保護組織　企画・開発

業務項目

必須業務：
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
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
情報セキュリティ対策の持続的改善の為の構造構築ができること
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
IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
内部統制の情報システムセキュリティ対応の要件策定
情報セキュリティ機能の明確化出来るスキル
情報セキュリティのリスクを検証する手法の整理（統一化）ができること
情報セキュリティ対策の製品の選定ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
情報セキュリティの企画・設計段階からの確保ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
単一の技術や基盤に依存する事のリスクを認知できる
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
実施可能業務：
単一の技術や基盤に依存する事のリスクを改善できる
適切な暗号化及び電波の範囲設定等の対策
情報セキュリティ対策実施状況の適切な確認・評価ができること
各利用者の環境に応じた対策の優先度に関する意思決定を支援するツール等の作成ができること
セキュリティ強化に資する新規システムの導入検討
情報資産のリスク分析ができること
通信端末の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
情報セキュリティ対策に関する費用対効果の測定ができること
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
ネットワークの不適正な利用からの被害防止対策ができること
オフショア・アウトソーシングに関連する固有リスクを把握できること
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
教育
LS-0, CMU, SPIA-T, LACB5-14,19,20, SANS-SEC401, 501
資格
SSCP, CISSP, CTIA, SEAj-T, SEAj-B, CCIE-Sec, SANS-GSEC

スキル・知識

推奨：

知識項目	大分類	中分類
ネットワークインフラセキュリティ		無線LAN
コンテンツセキュリティ	情報の保護	機密性対策
		完全性対策
		可用性対策

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		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
ファイアウォール		概論
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
		感染
		発病・被害
		不正プログラム（マルウェア）の種類
		ウイルス対策
		ウイルス対策ソフトの機能
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	
コンテンツセキュリティ	情報の保護	情報の格付け
	コンテンツ利用の制御	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
		不正コピー対策
		法的要件
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	
	サービスの不正利用	情報収集
		サービス妨害
		不正操作
	マルウェア	自動実行
		遠隔操作（ボット）
	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
	災害	資源供給
		拠点・設備
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
セキュリティプロトコル		概論
事業継続・災害復旧計画	事業継続管理	事業継続計画（BCP）
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		実装手段・ツール
物理セキュリティ	物理的脅威	

職種名	セキュリティエンジニア（基盤）		
定義	セキュリティ・システムの基盤部分（OS・ネットワーク）の全体設計・運用設計・方式設計、開発	所属企業・部署名	サービス・製品提供組織　開発、自社試算保護組織　開発

業務項目

必須業務：

- 単一の技術や基盤に依存する事のリスクを改善できる
- 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
- 情報セキュリティ機能の明確化出来るスキル
- 情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
- セキュアなデータベース構築の導入
- 情報セキュリティシステムの新たな開発ができること
- 安全性・信頼性の高い情報セキュリティシステムの構築ができること
- 製品・サービスにおける脆弱性の排除への対処
- 高信頼性端末の電子認証基盤の開発ができること
- 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
- ネットワークの不適正な利用からの被害防止対策ができること
- 情報セキュリティに関する情報収集、分析、共有
- 情報アクセス制限を統合し集中管理ができること
- 各業務・システムの最適化ができること
- IT障害、リスクについての分析と改善
- 事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
- 電子文書に係る成りすまし及び改ざんの防止ができること
- ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
- ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
- 高い保証レベルを有する情報システムの開発ができること
- 単一の技術や基盤に依存する事のリスクを認知できる
- サイバー攻撃発生時の適時適切な機能回復を持たせられること

実施可能業務：

- 情報セキュリティ対策の持続的改善の為の構造構築ができること
- IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
- セキュリティ強化に資する新規システムの導入検討
- 情報セキュリティ対策の製品の選定ができること
- セキュア・プログラミングの導入
- 攻撃等の分析・解析機能の洗い出しができること
- 横断的な情報セキュリティ基盤の底上げができること
- ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
- 業務・システムの基盤となる共通的なプラットフォームの構築ができること
- 本人認証を容易に行うことが可能な環境の構築ができること
- 情報管理の徹底をさせられること
- 情報セキュリティ対策の実施状況の自己点検ができること
- IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
- 情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
- ファイル秘匿化ソフトウェアの導入を選定・検討ができること
- 情報セキュリティの企画・設計段階からの確保ができること
- ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達

教育

LS-0, Hyogo-B, Hyogo-A, SPIA-T, Hyogo-B, LACB5-14, SANS-SEC401, 501, 502, 504, 505, 506,

資格

SSCP, CISSP, CTIA, SEAj-T, SEAj-B, CCNA-Sec, SANS-GCFW, SANS-GCIH, SANS-GCWN, SANS-GCUX

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		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
	OSセキュリティ【セキュアOS】	セキュアOSのプロテクション・プロファイル(PP)
ファイアウォール		概論
侵入検知		概論

スキル・知識

必須：

知識項目	大分類	中分類
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
	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
	データベースとデータウェアハウス	データベースとデータウェア保管庫の脆弱性、リスク、防護
	ソフトウェア開発ライフサイクル（SDLC）	計画
		設計
		実装
セキュリティ運用	セキュリティ運用	概論
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
	コンテンツ利用の制御	不正コピー対策
		権利管理技術（DRM）の要素技術
		権利記述言語の標準化
		法的要件
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
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		概論
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
フォレンジック		概論
物理セキュリティ	物理的脅威	概論

推奨：

知識項目	大分類	中分類
アプリケーションセキュリティ	その他のサーバーアプリ(FTP, IRC, VoIPなど)	
OSセキュリティ	OSセキュリティ【Unix】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
セキュリティ運用	セキュリティ運用	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）
暗号	暗号	公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
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手法
		監査報告書

職種名	セキュリティエンジニア（アプリ）		
定義	アプリケーションの開発フェーズにおいてセキュリティの確保を行う	所属企業・部署名	サービス・製品提供組織　開発、自社試算保護組織　開発

業務項目

必須業務：
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
情報セキュリティ機能の明確化出来るスキル
情報セキュリティ対策の製品の選定ができること
情報セキュリティの企画・設計段階からの確保ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
セキュア・プログラミングの導入
ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
高い保証レベルを有する情報セキュリティシステムの開発ができること
情報セキュリティシステムの新たな開発ができること
安全性・信頼性の高い情報セキュリティシステムの構築ができること
攻撃等の分析・解析機能の洗い出しができること
製品・サービスにおける脆弱性の排除への対処
安全なWebサイト構築の為のガイドラインを検討できること
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
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
単一の技術や基盤に依存する事のリスクを改善できる
単一の技術や基盤に依存する事のリスクを認知できる
実施可能業務：
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
セキュリティ強化に資する新規システムの導入検討
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
セキュアなデータベース構築の導入
高信頼性端末の電子認証基盤の開発ができること
攻撃手法の分析結果情報の共有ができること
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
ネットワークの不適正な利用からの被害防止対策ができること
情報セキュリティ対策の実施状況の自己点検ができること
電子文書に係る成りすまし及び改ざんの防止ができること
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
IT障害、リスクについての分析と改善
本人認証を容易に行うことが可能な環境の構築ができること
情報セキュリティに関する情報収集、分析、共有
各業務・システムの最適化ができること
教育
LS-0, Hoygo-B, Hyogo-A, SPIA-T, LACB5-14, 19, SANS-DEV319, 422, 538,
資格
SSCP, CTIA, SEAj-T, SEAj-B

スキル・知識

推奨：

知識項目	大分類	中分類
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
	コンテンツ利用の制御	不正コピー対策
		権利管理技術（DRM）の要素技術
		権利記述言語の標準化
		法的要件
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
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
		情報セキュリティ監査手法
		監査報告書

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		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
	OSセキュリティ【Unix】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
ファイアウォール		概論
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
	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
	ソフトウェア開発ライフサイクル（SDLC）	計画
		設計
		実装
セキュリティ運用	セキュリティ運用	概論
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
		公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
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		概論
事業継続・災害復旧計画	事業継続管理	
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
フォレンジック		概論
物理セキュリティ	物理的脅威	概論

職種名	セキュリティエンジニア(DB)		
定義	DBMSを構成要素とするシステムを対象に、セキュリティの確保を行う	所属企業・部署名	サービス・製品提供組織　開発、自社試算保護組織　開発

業務項目

必須業務：
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
情報セキュリティ機能の明確化出来るスキル
情報セキュリティ対策の製品の選定ができること
情報セキュリティの企画・設計段階からの確保ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
セキュアなデータベース構築の導入
ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
高い保証レベルを有する情報セキュリティシステムの開発ができること
情報セキュリティシステムの新たな開発ができること
安全性・信頼性の高い情報セキュリティシステムの構築ができること
攻撃等の分析・解析機能の洗い出しができること
製品・サービスにおける脆弱性の排除への対処
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
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
単一の技術や基盤に依存する事のリスクを改善できる
単一の技術や基盤に依存する事のリスクを認知できる
実施可能業務：
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
セキュリティ強化に資する新規システムの導入検討
高信頼性端末の電子認証基盤の開発ができること
攻撃手法の分析結果情報の共有ができること
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
ネットワークの不適正な利用からの被害防止対策ができること
情報セキュリティ対策の実施状況の自己点検ができること
電子文書に係る成りすまし及び改ざんの防止ができること
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
IT障害、リスクについての分析と改善
本人認証を容易に行うことが可能な環境の構築ができること
情報セキュリティに関する情報収集、分析、共有
各業務・システムの最適化ができること
教育
LS-0, Hyogo-B, Hyogo-A, SPIA-T, LACB4-14, 20, SANS-SEC401, 509
資格
SSCP, CTIA, SEAJ-T, SEAJ-B, SANS-GSOC

スキル・知識

推奨：		
知識項目	大分類	中分類
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
	コンテンツ利用の制御	不正コピー対策
		権利管理技術(DRM)の要素技術
		権利記述言語の標準化
		法的要件
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
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
		情報セキュリティ監査手法
		監査報告書

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		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
	OSセキュリティ【Unix】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
ファイアウォール		概論
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
	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
	ソフトウェア開発ライフサイクル(SDLC)	計画
		設計
		実装
セキュリティ運用	セキュリティ運用	概論
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
		公開鍵暗号
		共通鍵暗号
		ハッシュ関数
		暗号用乱数
		鍵管理
		ゼロ知識証明
		その他の暗号方式
		暗号解読・強度評価
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
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
フォレンジック		概論
物理セキュリティ	物理的脅威	概論

職種名	QAマネージャー		
定義	品質保証業務及びそのプロセス改善業務。製品品質に関する顧客窓口業務。開発チームに対する品質保証啓蒙活動	所属企業・部署名	サービス・製品提供組織　品質管理、自社試算保護組織　品質管理

業務項目

必須業務：

- 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
- 情報セキュリティ対策に関する評価指標の確立が出来ること
- 第三者評価の活用を促進できること
- 第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
- 情報セキュリティ対策実施状況の適切な確認・評価ができること
- 単一の技術や基盤に依存する事のリスクを認知できる
- 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
- ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
- 情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
- 情報管理の徹底をさせられること
- 情報セキュリティ対策の実施状況の自己点検ができること

実施可能業務：

- 単一の技術や基盤に依存する事のリスクを改善できる
- 情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
- ITセキュリティ評価及び認証制度の運用を推進できること
- 情報セキュリティ対策実施状況報告ができること
- 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
- 攻撃等の分析・解析機能の洗い出しができること
- 情報セキュリティに関する情報収集、分析、共有
- オフショア・アウトソーシングに関連する固有リスクを把握できること
- 情報セキュリティ対策の持続的改善の為の構造構築ができること
- 情報セキュリティの企画・設計段階からの確保ができること
- ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
- 安全性・信頼性の高い情報システムの構築ができること
- 製品・サービスにおける脆弱性の排除への対処
- 攻撃手法の分析結果情報の共有ができること
- IT障害の未然防止ができること
- 潜在的に大きなリスクの対処方法のあり方を考えられること
- 安全なWebサイト構築の為のガイドラインを検討できること
- 個人情報保護、営業機密管理
- IT障害についての分析ができること
- IT障害の要因等の対策検討をして再発防止ができること
- IT障害の拡大防止ができること
- IT障害、リスクについての分析と改善

教育

LS-0, Hyogo-B, Hyogo-A, SPIA-T, LACB5-14,19,20,21, SANS-DEV304, 422, 534, 538

資格

SSCP, CTIA, SEAJ-T, SEAJ-B.

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
ファイアウォール		概論
侵入検知		概論
セキュリティ運用	セキュリティ運用	概論
認証	認証	種類
事業継続・災害復旧計画	事業継続管理	事業継続計画(BCP)
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
		情報セキュリティ監査手法
		監査報告書
物理セキュリティ	物理的脅威	

推奨：

知識項目	大分類	中分類
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
	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
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
	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
	ソフトウェア開発ライフサイクル(SDLC)	計画
		設計
		実装
暗号	暗号	暗号方式概説
攻撃手法	攻撃手法の概論	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
セキュリティプロトコル		
フォレンジック		概論

職種名	QAエンジニア		
定義	ソフトウェア開発および開発プロジェクトに対し、品質保証全般のテストを実施。	所属企業・部署名	サービス・製品提供組織　品質管理、自社試算保護組織　品質管理

業務項目
必須業務：
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
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
単一の技術や基盤に依存する事のリスクを認知できる
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
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
実施可能業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
ITセキュリティ評価及び認証制度の運用を推進できること
情報セキュリティ対策実施状況報告ができること
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
攻撃等の分析・解析機能の洗い出しができること
情報セキュリティに関する情報収集、分析、共有
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
IT障害の未然防止ができること
潜在的に大きなリスクの対処方法のあり方を考えられること
安全なWebサイト構築の為のガイドラインを検討できること
個人情報保護、営業機密管理
IT障害についての分析ができること
IT障害の要因等の対策検討をして再発防止ができること
IT障害の拡大防止ができること
IT障害、リスクについての分析と改善
教育
LS-0, Hyogo-B, SPIA-T, LACB5-14,19,20,21, SANS-DEV304, 422, 534, 538
資格
SSCP, CTIA, SEAj-T, SEAj-B

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
ファイアウォール		概論
侵入検知		概論
セキュリティ運用	セキュリティ運用	概論
認証	認証	種類
事業継続・災害復旧計画	事業継続管理	事業継続計画(BCP)
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
		情報セキュリティ監査手法
		監査報告書
物理セキュリティ	物理的脅威	
推奨：		
知識項目	大分類	中分類
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
	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
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
暗号	暗号	暗号方式概説
攻撃手法	攻撃手法の概論	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
セキュリティプロトコル		
フォレンジック		概論

職種名	セキュリティテスター		
定義	ソースコード解析や脆弱性の洗い出し	所属企業・部署名	サービス・製品提供組織　開発・品質管理、自社試算保護組織　開発・品質管理

業務項目

必須業務：
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
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
製品・サービスにおける脆弱性の排除への対処
単一の技術や基盤に依存する事のリスクを認知できる
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
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
潜在的に大きなリスクの対処方法のあり方を考えられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
情報セキュリティ対策の実施状況の自己点検ができること
実施可能業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
ITセキュリティ評価及び認証制度の運用を推進できること
情報セキュリティ対策実施状況報告ができること
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
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
IT障害の未然防止ができること
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
潜在的に大きなリスクの対処方法のあり方を考えられること
安全なWebサイト構築の為のガイドラインを検討できること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
個人情報保護、営業機密管理
IT障害についての分析ができること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
IT障害の拡大防止ができること
IT障害、リスクについての分析と改善
教育
LS-0, Hyogo-B, Hyogo-A, SPIA-T, LACB5-14,19,20,21, C6, SANS-DEV422, 534, 53, SEC301, 560, 617, AUD507
資格
SSCP, CTIA, SEAj-T, SEAj-B, SANS-GPEN, SANS-GSNA,

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
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
セキュリティ運用	セキュリティ運用	概論
認証	認証	種類
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
		情報セキュリティ監査手法
		監査報告書
物理セキュリティ	物理的脅威	

スキル・知識

推奨：

知識項目	大分類	中分類
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
	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
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	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
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
セキュリティプロトコル		
フォレンジック		概論

職種名	プログラマー
定義	仕様書や設計書に従って、セキュアプログラミングの知識を持ってプログラムを作る。

所属企業・部署名	サービス・製品提供組織　開発、自社試算保護組織　開発

業務項目

必須業務：
情報セキュリティ機能の明確化出来るスキル
情報セキュリティの企画・設計段階からの確保ができること
高い保証レベルを有する情報システムの開発ができること
情報システムの新たな開発ができること
安全性・信頼性の高い情報システムの構築ができること
製品・サービスにおける脆弱性の排除への対処
高信頼性端末の電子認証基盤の開発ができること
単一の技術や基盤に依存する事のリスクを認知できる
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
潜在的に大きなリスクの対処方法のあり方を考えられること
情報セキュリティ問題に関するPOC機能を持てること
サイバー攻撃発生時の適時適切な機能回復を持たせられること
実施可能業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティ対策の持続的改善の為の構造構築ができること
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
セキュアなデータベース構築の導入
ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
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
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
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
IT障害の未然防止ができること
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
情報管理の徹底をさせられること
情報セキュリティ対策の実施状況の自己点検ができること
IT障害についての分析ができること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
IT障害の拡大防止ができること
オフショア・アウトソーシングに関連する固有リスクを把握できること
電子文書に係る成りすまし及び改ざんの防止ができること
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
教育
LS-0, Hyogo-B, Hyogo-A, SPIA-T, LACB5-14,19,20, SANS-SEC301, DEV422, 536, 541, 544, 545, 548
資格
SSCP, CTIA, SEAj-T, SEAj-B

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
	OSセキュリティ【セキュアOS】	セキュアOSのプロテクション・プロファイル(PP)
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
	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
	ソフトウェア開発ライフサイクル(SDLC)	計画
		設計
		実装
セキュリティ運用	セキュリティ運用	
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
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
物理セキュリティ	物理的脅威	

推奨：

知識項目	大分類	中分類
セキュアプログラミング技法	データベースとデータウェアハウス	データベースとデータウェア保管庫の脆弱性、リスク、防護
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
	コンテンツ利用の制御	不正コピー対策
		権利管理技術(DRM)の要素技術
		権利記述言語の標準化
		法的要件
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態

職種名	プロジェクトマネージャー		
定義	プロジェクトの計画と実行に於いて総合的な責任を持つ。期日までに成果物を完成させる。	所属企業・部署名	サービス・製品提供組織　開発、自社試算保護組織　開発

業務項目

必須業務：
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
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
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
調達における成果利用の方策の検討ができること
情報セキュリティ対策の持続的改善の為の構造構築ができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
情報セキュリティ機能の明確化出来るスキル
セキュリティ強化に資する新規システムの導入検討
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
情報セキュリティ確保の為の体制整備ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
情報セキュリティの企画・設計段階からの確保ができること
攻撃等の分析・解析機能の洗い出しができること
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
情報セキュリティ対策に関する費用対効果の測定ができること
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
緊急事態対応に向けた取組み
単一の技術や基盤に依存する事のリスクを認知できる
横断的な情報セキュリティ基盤の底上げができること
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
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
潜在的に大きなリスクの対処方法のあり方を考えられること
情報管理の徹底をさせられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
個人情報保護、営業機密管理
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）
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
教育
ILS-G, Hyogo-B, Hyogo-A, LAC-B5-20, SANS-SEC401, MGT525
資格
CISM, CISSP, CTIA, SEAJ-T, SEAJ-B, SANS-GCPM

実施可能業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
ITセキュリティ評価及び認証制度の運用を推進できること
投資効果に係る継続的評価プロセスの導入ができること
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
各利用者の環境に応じた対策の優先度に関する意思決定を支援するツール等の作成ができること
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
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
情報セキュリティのリスクを検証する手法の整理（統一化）ができること
情報セキュリティ対策の製品の選定ができること
通信端末の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と関連
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
製品・サービスにおける脆弱性の排除への対処
組織の緊急対応チーム間の連携体制の整備ができること
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
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
情報システムに係るリアルタイム監視機能をもてること
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
横断的な監視情報の収集機能がもてること
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
攻撃手法の分析結果情報の共有ができること
フォレンジック
IT障害の未然防止ができること
ネットワークの不適正な利用からの被害防止対策ができること
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
安全なWebサイト構築の為のガイドラインを検討できること
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティ対策を実施する者が評価される仕組みの導入
各インフラの政府統一基準に係る必須項目の検査ができること
IT障害についての分析ができること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
IT障害の拡大防止ができること
事業継続マネジメント(BCM)
オフショア・アウトソーシングに関連する固有リスクを把握できること
情報セキュリティ監査制度の活用ができること
各業務・システムの最適化ができること
IT障害、リスクについての分析と改善
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること

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
	OSセキュリティ【セキュアOS】	セキュアOSのプロテクション・プロファイル(PP)
ファイアーウォール	ファイアーウォール	
侵入検知	侵入検知	
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
	セキュアプログラミング留意事項	Webアプリケーション設計
		Webアプリケーション
		データベース
	ソフトウェア開発ライフサイクル(SDLC)	計画
		設計
		実装
セキュリティ運用	セキュリティ運用	
		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		概論
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
物理セキュリティ	物理的脅威	

推奨：		
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	無線LAN
OSセキュリティ	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
不正プログラム(マルウェア)	不正プログラム(マルウェア)	感染
		発病・被害
		不正プログラム(マルウェア)の種類
		ウイルス対策
		ウイルス対策ソフトの機能
コンテンツセキュリティ	コンテンツ利用の制御	不正コピー対策
		権利管理技術(DRM)の要素技術
		権利記述言語の標準化
		法的要件
	電子透かし	電子透かしの基本概念
		電子透かしの方式
		電子透かしの応用形態
認証	認証	種類
攻撃手法	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
	災害	資源供給
		拠点・設備
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)

職種名	セキュリティシステムアドミニストレーター		
定義	システムに対するセキュリティ対策を整備し、運用管理を行う	所属企業・部署名	サービス・製品提供組織　運用、自社試算保護組織　運用

業務項目

必須業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
情報セキュリティ機能の明確化出来るスキル
情報セキュリティのリスクを検証する手法の整理（統一化）ができること
製品・サービスにおける脆弱性の排除への対処
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
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
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
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
IT障害の未然防止ができること
緊急事態対応に向けた取組み
単一の技術や基盤に依存する事のリスクを認知できる
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
ネットワークの不適正な利用からの被害防止対策ができること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
ネットワーク監視
通信の監視が出来ること
IT障害についての分析ができること
情報通信の静的な機能維持ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
IT障害の拡大防止ができること
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）
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
実施可能業務：
第三者評価の活用を促進できること
ITセキュリティ評価及び認証制度の運用を推進できること
調達における成果利用の方策の検討ができること
適切な暗号化及び電波の範囲設定等の対策
IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
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
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
セキュリティ強化に資する新規システムの導入検討
情報セキュリティ対策の製品の選定ができること
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
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
横断的な監視情報の収集機能がもてること
攻撃手法の分析結果情報の共有ができること
フォレンジック
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
潜在的に大きなリスクの対処方法のあり方を考えられること
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報管理の徹底をさせられること
情報セキュリティ問題に関するPOC機能を持てること
個人情報保護、営業機密管理
IT障害の迅速な復旧ができること
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
事業継続マネジメント(BCM)
サイバー攻撃発生時の適時適切な機能回復を持たせられること
情報アクセス制限を統合し集中管理ができること
IT障害、リスクについての分析と改善
CSIRTに対する情報提供体制の構築＆確立
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
教育
LS-0, Hyogo-B, SPIA-T, LACB5-14 ,15, 16, 18, 22, C1, SANS-SEC301, 401, 501, 505, 506
資格
SSCP, CTIA, SEAJ-M, SEAJ-T, SEAJ-B, CCSP, CCNA-Sec, SANS-GCWN, SANS-GCUX

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		概論
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
物理セキュリティ	物理的脅威	概論
推奨：		
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	無線LAN
OSセキュリティ	OSセキュリティ【Unix】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【Windows】	構成・設定管理
		パッチ適用管理
		監査
		ログ管理
		プロセス管理
		サービス管理
		ファイルシステム管理
		アカウント管理
		ネットワーク保護
	OSセキュリティ【セキュアOS】	セキュアOSの基本機能
		Trusted OSに求められる機能
		セキュアOSのアクセス制御モデル
		セキュアOSのプロテクション・プロファイル(PP)
コンテンツセキュリティ	コンテンツ利用の制御	不正コピー対策
		法的要件
攻撃手法	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）

職種名	オペレーター		
定義	提供しているサービスの運用・監視を行う。ネットワーク監視。ヘルプデスク。サービスシステム維持管理等	所属企業・部署名	サービス・製品提供組織　運用、自社試算保護組織　運用

業務項目

必須業務：
情報システムに係るリアルタイム監視機能をもてること
横断的な監視情報の収集機能がもてること
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
個人情報保護、営業機密管理
ネットワーク監視
通信の監視が出来ること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
実施可能業務：
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
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
IT障害の未然防止ができること
緊急事態対応に向けた取組み
教育
LS-0, Hyogo-B, SPIA-T, LACB5-14, SANS-SEC301, 401, 502, 503, 504, 560
資格
SSCP, CTIA, SEAj-T, SEAj-B, CCSP, CCNA-Sec, SANS-GCFW, SANS-GCIH, SANS-GCIA, SANS-GPEN

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	
		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

職種名	セキュリティアナリスト		
定義	各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を提示	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
必須業務:
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
攻撃等の分析・解析機能の洗い出しができること
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
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
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
インシデント対応
IT障害についての分析ができること
攻撃手法の分析能力の強化ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
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
IT障害、リスクについての分析と改善
実施可能業務:
単一の技術や基盤に依存する事のリスクを改善できる
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
第三者評価の活用を促進できること
ITセキュリティ評価及び認証制度の運用を推進できること
調達における成果利用の方策の検討ができること
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
情報セキュリティのリスクについて定量的評価手法を選定できる
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティのリスクを検証する手法の整理(統一化)ができること
情報セキュリティ対策の製品の選定ができること
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
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
攻撃手法の分析結果情報の共有ができること
フォレンジック
教育
LS-0, Hyogo-B, Hyogo-A, SPIA-T, SPIA-IR, LACB5-14, 16, 22, C1, C3, C5, SANS-SEC401, 503, 504, 560, 601, 610, 709, JTP-EHM, SC, CEHRapid
資格
SSCP, CISSP、CTIA, SEAj-T, SEAj-B, SANS-GCFA

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
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
セキュリティ運用	セキュリティ運用	概論
認証	認証	種類
推奨:		
知識項目	大分類	中分類
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
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		
フォレンジック		概論
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
物理セキュリティ	物理的脅威	

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
必須業務:
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
攻撃手法の分析結果情報の共有ができること
フォレンジック
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
インシデント対応
ネットワーク監視
通信の監視が出来ること
IT障害についての分析ができること
攻撃手法の分析能力の強化ができること
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
実施可能業務:
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
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
情報セキュリティ対策の製品の選定ができること
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
攻撃等の分析・解析機能の洗い出しができること
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
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
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
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
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
横断的な監視情報の収集機能がもてること
アクセス記録の解析、コンピュータウィルス等の動作検証、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
定点観測データの共有ができること
情報セキュリティに関する情報収集、分析、共有
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)
教育
LS-0, Hyogo-B Hyogo-A, SPIA-T, SPIA-IR, LACB5-14, 16, 17, 22, C1, C2, C4, SANS-SEC401, 508, JTP-EHM, SC, CEHRapid
資格
SSCP、CTIA, SEAj-T、SANS-GCFA

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
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
フォレンジック		概論

推奨:

知識項目	大分類	中分類
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
LS	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
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
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	

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
必須業務:
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
実施可能業務:
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
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
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
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
教育
LS-0, Hyogo-B, Hyogo-A, SPIA-IR, SEAj-T, LACB5-14,16,22, C1, SANS-SEC401, 504
資格
CISSP, CTIA, SEAj-T, SANS-GCIH

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	
		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	

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
必須業務：
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
実施可能業務：
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, LACB5-14,16,22, C1, SANS-SEC401, 504
資格
CISSP, CITA, SEAj-T, SANS-GCIH

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

スキル・知識

必須：

知識項目	大分類	中分類
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	

職種名	フィールドエンジニア		
定義	顧客現場で、セキュリティシステム構築に伴う、システム機器の設置から設定保守・修理を行う	所属企業・部署グループ	サービス・製品提供組織　運用

業務項目
必須業務:
製品・サービスにおける脆弱性の排除への対処
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
攻撃手法の分析結果情報の共有ができること
IT障害の未然防止ができること
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
ネットワークの不適正な利用からの被害防止対策ができること
アクセス記録の解析、コンピュータウィルス等の動作検証、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
本人認証を容易に行うことが可能な環境の構築ができること
ネットワーク監視
通信の監視が出来ること
IT障害についての分析ができること
IT障害の迅速な復旧ができること
情報通信の静的な機能維持ができること
実施可能業務:
情報セキュリティ対策の製品の選定ができること
ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
安全性・信頼性の高い情報システムの構築ができること
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
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
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
政府統一基準等の導入
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
外部記録媒体に保存する情報を自動的に暗号化等するソフトの導入（設計～運用）ができること
インシデント対応
IT障害の要因等の対策検討をして再発防止ができること
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
IT障害の拡大防止ができること
IT障害、リスクについての分析と改善
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
電子文書に係る成りすまし及び改ざんの防止ができること
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
教育
Hyogo-B, Hyogo-A, SPIA-T, LACB5-14,15,16,22, C1, SANS-SEC301, 401
資格
SSCP, CTIA, SEAj-T, CCNP, CCNA-Sec, SANS-GSEC

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
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
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
セキュリティ運用	セキュリティ運用	概論
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
推奨:		
知識項目	大分類	中分類
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
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
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
フォレンジック		概論
物理セキュリティ	物理的脅威	

職種名	プライバシーオフィサー		
定義	企業・団体内の個人情報保護体制の構築、運用、改善を行う	所属企業・部署グループ	サービス・製品提供　経営、自社資産保護組織　経営

業務項目
必須業務:
潜在的に大きなリスクの対処方法のあり方を考えられること
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティ対策を実施する者が評価される仕組みの導入
情報管理の徹底をさせられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
情報セキュリティ問題に関するPOC機能を持てること
個人情報保護、営業機密管理
情報セキュリティに関する情報収集、分析、共有
実施可能業務:
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
情報セキュリティポリシーの改善ができること
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
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
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
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
情報セキュリティ機能の明確化出来るスキル
セキュリティ強化に資する新規システムの導入検討
情報セキュリティポリシーの策定
情報資産のリスク分析ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
情報セキュリティリスクや対策の効果等に係る定量化の定義をする
横断的な監視情報の収集機能がもてること
情報セキュリティ対策の手引きの作成ができること
情報セキュリティ対策の実施状況の自己点検ができること
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)
各業務・システムの最適化ができること
CSIRTに対する情報提供体制の構築＆確立
政府統一基準等の導入
第三者評価の活用を促進できること
情報セキュリティ対策実施状況報告ができること
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ確保の為の体制整備ができること
情報セキュリティの企画・設計段階からの確保ができること
情報セキュリティ対策に関する基本戦略の立案
情報セキュリティの制度整備
情報セキュリティ対策に関する費用対効果の測定ができること
教育
LAC-B1, 3,4, RC-P*, IS-PMS, PMSAudit
資格
CISM, CISSP

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
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
セキュリティ運用	セキュリティ運用	概論
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
推奨:		
知識項目	大分類	中分類
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
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
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
フォレンジック		概論
物理セキュリティ	物理的脅威	

職種名	プライバシースペシャリスト		
定義	企業の個人情報保護に関して、規定作成から意識向上施策実施までを担当する	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

必須業務：
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
情報セキュリティ対策実施状況報告ができること
情報資産のリスク分析ができること
情報セキュリティの企画・設計段階からの確保ができること
情報セキュリティ対策の手引きの作成ができること
情報管理の徹底をさせられること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ問題に関するPOC機能を持てること
個人情報保護、営業機密管理
実施可能業務：
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
情報セキュリティポリシーの改善ができること
情報セキュリティポリシーの策定
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
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
情報セキュリティ機能の明確化出来るスキル
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
横断的な監視情報の収集機能がもてること
情報セキュリティに関する情報収集、分析、共有
教育
SPIA-M, LAC-B-1,3,4, RC-P*, IS-PMS, PMSAudit
資格

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	マネジメント概論	セキュリティマネジメントの基本
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
推奨：		
知識項目	大分類	中分類
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
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
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
フォレンジック		概論
物理セキュリティ	物理的脅威	

職種名	CSO/CISO/CIAO		
定義	情報資産保護を経営の観点から意思決定をし、指揮をとり、組織の情報資産保護の責任をとる	所属企業・部署グループ	サービス・製品提供組織　経営、自社資産保護組織　経営

業務項目

必須業務：

- 相互依存性解析の成果を踏まえた情報セキュリティ基準等が検討できること
- 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
- 情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
- 情報セキュリティポリシーの改善ができること
- 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
- 情報セキュリティ対策に関する評価指標の確立が出来ること
- 第三者評価の活用を促進できること
- 第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
- 企業に係る指標の選定がはかれること
- 調達における成果利用の方策の検討ができること
- 投資効果に係る継続的評価プロセスの導入ができること
- 情報セキュリティ対策実施状況の適切な確認・評価ができること
- 情報セキュリティ対策実施状況報告ができること
- 情報セキュリティポリシーの策定
- 事業継続計画の策定ができること
- 情報セキュリティ対策に係る行動計画ができること
- 情報セキュリティ対策強化に向けたマイルストーンの検討ができること
- サイバーテロ対策に係る体制の導入ができること
- 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
- 情報セキュリティ確保の為の体制整備ができること
- 情報セキュリティ対策を推進する体制・制度の整備ができること
- 情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
- 情報セキュリティの企画・設計段階からの確保ができること
- 情報セキュリティ対策に関する基本戦略の立案
- 官民の連絡・連携体制の構築
- 情報セキュリティの制度整備
- 情報セキュリティリスクや対策の効果等に係る定量化の定義をする
- 情報セキュリティに関するリスク定量化手法を考えられること
- 組織の緊急対応チーム間の連携体制の整備ができること
- 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
- 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
- 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
- 情報セキュリティ対策に関する費用対効果の測定ができること
- 政府統一基準等の導入
- 緊急事態対応に向けた取組み
- 潜在的に大きなリスクの対処方法のあり方を考えられること
- コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
- 情報セキュリティ対策を実施する者が評価される仕組みの導入
- 情報管理の徹底をさせられること
- 情報セキュリティ対策の実施手順及び成果等の共有化ができること
- インシデント対応
- 情報セキュリティ対策の実施状況の自己点検ができること
- 情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
- 情報セキュリティ問題に関するPOC機能を持てること
- JPCERTなどの監督・関係機関との情報交換等の運用における連携ができること
- 個人情報保護、営業機密管理
- IT障害の拡大防止ができること
- 事業継続マネジメント(BCM)
- オフショア・アウトソーシングに関連する固有リスクを把握できること
- 情報セキュリティ監査制度の活用ができること
- 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）
- 情報アクセス制限を統合し集中管理ができること
- 各業務・システムの最適化ができること
- IT障害、リスクについての分析と改善
- 事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
- 情報セキュリティに関する取り組みについて全体としての整合性が確保できること

実施可能業務：

- 情報セキュリティ対策の持続的改善の為の構造構築ができること
- 情報セキュリティのリスクについて定量的評価手法を選定できる
- 情報セキュリティに関する基準等の浸透状況について情報収集ができること
- 情報セキュリティ監査制度の活用状況について情報収集ができること
- 情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
- 情報セキュリティ対策の製品の選定ができること
- ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
- 情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
- 横断的な監視情報の収集機能がもてること
- 単一の技術や基盤に依存する事のリスクを認知できる
- 情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
- 攻撃手法の分析能力の強化ができること
- IT障害の要因等の対策検討をして再発防止ができること
- 情報セキュリティに関する情報収集、分析、共有

実施可能業務：

- サイバー攻撃発生時の適時適切な機能回復を持たせられること
- CSIRTに対する情報提供体制の構築＆確立
- IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
- 情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
- ITセキュリティ評価及び認証制度の運用を推進できること
- 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
- 内部統制の情報システムセキュリティ対応の要件策定
- 情報セキュリティ機能の明確化出来るスキル
- 情報資産のリスク分析ができること
- 情報セキュリティのリスクを検証する手法の整理（統一化）ができること
- 通信端末の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
- 横断的な情報セキュリティ基盤の底上げができること
- ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
- 最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
- 取り組みが不十分な情報セキュリティ対策の具体的な導入運用に当たって参考となる手引きの作成ができること

教育

RK-27K-6, SANS-MGT512

資格

CISM, CISSP, SANS-GSLC

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		概論
侵入検知		概論
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		概論
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
	コンテンツ利用の制御	不正コピー対策
		法的要件
認証	認証	種類
攻撃手法	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
事業継続・災害復旧計画	事業継続管理	事業継続計画(BCP)
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
物理セキュリティ	物理的脅威	

推奨：

知識項目	大分類	中分類
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
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	

職種名	CSO/CISO/CIAO補佐		
定義	CSO/CISO/CIAOの業務を補佐し、経営陣の意思を現場に浸透させ、施策がきちんと実行されるかを監視する	所属企業・部署グループ	サービス・製品提供組織　経営、自社資産保護組織　経営

業務項目
必須業務：
相互依存性解析の成果を踏まえた情報セキュリティ基準等が検討できること
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
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
情報セキュリティポリシーの改善ができること
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
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
企業に係る指標の選定がはかれること
調達における成果利用の方策の検討ができること
投資効果に係る継続的評価プロセスの導入ができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
情報セキュリティポリシーの策定
事業継続計画の策定ができること
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
サイバーテロ対策に係る体制の導入ができること
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
情報セキュリティ確保の為の体制整備ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
情報セキュリティの企画・設計段階からの確保ができること
情報セキュリティ対策に関する基本戦略の立案
官民の連絡・連携体制の構築
情報セキュリティの制度整備
情報セキュリティリスクや対策の効果等に係る定量化の定義をする
情報セキュリティに関するリスク定量化手法を考えられること
組織の緊急対応チーム間の連携体制の整備ができること
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
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
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
情報セキュリティ対策に関する費用対効果の測定ができること
政府統一基準等の導入
緊急事態対応に向けた取組み
潜在的に大きなリスクの対処方法のあり方を考えられること
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティ対策を実施する者が評価される仕組みの導入
情報管理の徹底をさせられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
情報セキュリティ問題に関するPOC機能を持てること
JPCERTなどの監督・関係機関との情報交換等の運用における連携ができること
個人情報保護、営業機密管理
IT障害の拡大防止ができること
事業継続マネジメント(BCM)
オフショア・アウトソーシングに関連する固有リスクを把握できること
情報セキュリティ監査制度の活用ができること
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)
情報アクセス制限を統合し集中管理ができること
各業務・システムの最適化ができること
IT障害、リスクについての分析と改善
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
実施可能業務：
情報セキュリティ対策の持続的改善の為の構造構築ができること
情報セキュリティのリスクについて定量的評価手法を選定できる
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
情報セキュリティ対策の製品の選定ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
横断的な監視情報の収集機能がもてること
単一の技術や基盤に依存する事のリスクを認知できる
情報セキュリティ対策実施状況を確認するあの標準フォーマットの検討ができること
攻撃手法の分析能力の強化ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
サイバー攻撃発生時の適時適切な機能回復を持たせられること
CSIRTに対する情報提供体制の構築＆確立

業務項目
実施可能業務：
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
ITセキュリティ評価及び認証制度の運用を推進できること
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
内部統制の情報システムセキュリティ対応の要件策定
情報セキュリティ機能の明確化出来るスキル
情報資産のリスク分析ができること
情報セキュリティのリスクを検証する手法の整理(統一化)ができること
通信端末の基本機能のあり方及び所要の機能の確保に必要な推進方策について方向性を得られること
横断的な情報セキュリティ基盤の底上げができること
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
取り組みが不十分な情報セキュリティ対策の具体的な導入運用に当たって参考となる手引きの作成ができること
教育
RK-27K-6, SANS-MGT512
資格：
CISM、CISSP、SANS-GSLC, SANS-GCIM

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		概論
侵入検知		概論
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		概論
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
	コンテンツ利用の制御	不正コピー対策
		法的要件
認証	認証	種類
攻撃手法	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
事業継続・災害復旧計画	事業継続管理	事業継続計画(BCP)
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
物理セキュリティ	物理的脅威	

推奨：

知識項目	大分類	中分類
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
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	

職種名	セキュリティプロダクトオーナー		
定義	セキュリティ製品の企画から保守にいたるまで製品に関わる全責任をとる	所属企業・部署グループ	サービス・製品提供組織　企業、営業、開発、品質管理、運用

業務項目

必須業務：
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
調達における成果利用の方策の検討ができること
適切な暗号化及び電波の範囲設定等の対策
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ対策実施状況報告ができること
IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
情報セキュリティ機能の明確化出来るスキル
情報セキュリティ機能の明確化ができること
情報セキュリティの企画・設計段階からの確保ができること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
製品・サービスにおける脆弱性の排除への対処
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
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
横断的な監視情報の収集機能がもてること
政府統一基準等の導入
緊急事態対応に向けた取組み
単一の技術や基盤に依存する事のリスクを認知できる
ネットワークの不適正な利用からの被害防止対策ができること
潜在的に大きなリスクの対処方法のあり方を考えられること
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
情報セキュリティに関する情報収集、分析、共有
サイバー攻撃発生時の適時適切な機能回復を持たせられること
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
実施可能業務：
ITセキュリティ評価及び認証制度の運用を推進できること
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
情報セキュリティポリシーの策定
情報資産のリスク分析ができること
事業継続計画の策定ができること
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
情報セキュリティ確保の為の体制整備ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
組織の緊急対応チーム間の連携体制の整備ができること
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
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
攻撃手法の分析結果情報の共有ができること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
JPCERTなどの監督・関係機関との情報交換等の運用における連携ができること
個人情報保護、営業機密管理
攻撃手法の分析能力の強化ができること
オフショア・アウトソーシングに関連する固有リスクを把握できること
情報セキュリティ監査制度の活用ができること

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
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		概論
侵入検知		概論
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		プログラミング言語とツール
セキュリティ運用		概論
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		
推奨：		
知識項目	大分類	中分類
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
フォレンジック		概論
物理セキュリティ	物理的脅威	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)

業務項目

教育
LS-0, LAC-B5-20, SANS-SEC401
資格
CISSP、SANS-GSEC

職種名	セキュリティサービスオーナー		
定義	セキュリティサービスの企画から保守にいたるまでサービスに関わる全責任をとる	所属企業・部署グループ	サービス・製品提供組織　営業、開発

業務項目
必須業務：
単一の技術や基盤に依存する事のリスクを改善できる
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
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
情報セキュリティポリシーの改善ができること
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
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
情報セキュリティ対策の持続的改善の為の構造構築ができること
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
情報セキュリティ機能の明確化出来るスキル
セキュリティ強化に資する新規システムの導入検討
情報資産のリスク分析ができること
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策の製品の選定ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
情報セキュリティ機能の明確化ができること
情報セキュリティの企画・設計段階からの確保ができること
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
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
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
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
IT障害の未然防止ができること
単一の技術や基盤に依存する事のリスクを認知できる
潜在的に大きなリスクの対処方法のあり方を考えられること
情報管理の徹底をさせられること
個人情報保護、営業機密管理
事業継続確保への取り組み
IT障害についての分析ができること
IT障害の迅速な復旧ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
IT障害の拡大防止ができること
事業継続マネジメント(BCM)
オフショア・アウトソーシングに関連する固有リスクを把握できること
IT障害、リスクについての分析と改善
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
実施可能業務：
ビルトイン型の情報セキュリティ機能を持った基盤自体を新たに構築する
高い保証レベルを有する情報システムの開発ができること
安全性・信頼性の高い情報システムの構築ができること
情報システムに係るリアルタイム監視機能をもてること
フォレンジック
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
ネットワークの不適正な利用からの被害防止対策ができること
電子文書に係る成りすまし及び改ざんの防止ができること
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
ITセキュリティ評価及び認証制度の運用を推進できること
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
内部統制の情報システムセキュリティ対応の要件策定
事業継続計画の策定ができること
サイバーテロ対策に係る体制の導入ができること
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
情報セキュリティ確保の為の体制整備ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
攻撃等の分析・解析機能の洗い出しができること
製品・サービスにおける脆弱性の排除への対処
組織の緊急対応チーム間の連携体制の整備ができること
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
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
情報セキュリティ対策に関する費用対効果の測定ができること
横断的な監視情報の収集機能がもてること
政府統一基準等の導入
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

業務項目
実施可能業務：
攻撃手法の分析結果情報の共有ができること
緊急事態対応に向けた取組み
横断的な情報セキュリティ基盤の底上げができること
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティ対策を実施する者が評価される仕組みの導入
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
情報セキュリティ監査制度の活用ができること
サイバー攻撃発生時の適時適切な機能回復を持たせられること
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
教育
LS-0, LAC-B5-20, SANS-SEC401
資格
CISSP、CCIE, SANS-GSEC

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
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		概論
侵入検知		概論
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	
		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		
フォレンジック		概論

推奨：

知識項目	大分類	中分類
事業継続・災害復旧計画	事業継続管理	
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）

職種名	セキュリティコンサルタント(マネージメント)		
定義	情報セキュリティ戦略立案から、情報資産の管理・運用方法の策定までに関し、顧客の問題解決を支援する。	所属企業・部署グループ	サービス・製品提供組織　営業

業務項目
必須業務：
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
相互依存性解析の成果を踏まえた情報セキュリティ基準等が検討できること
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
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
情報セキュリティポリシーの改善ができること
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
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
企業に係る指標の選定がはかれること
投資効果に係る継続的評価プロセスの導入ができること
情報セキュリティ対策の持続的改善の為の構造構築ができること
情報セキュリティのリスクについて定量的評価手法を選定できる
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
情報セキュリティ機能の明確化出来るスキル
情報セキュリティポリシーの策定
情報資産のリスク分析ができること
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策の製品の選定ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
情報セキュリティ機能の明確化ができること
情報セキュリティの企画・設計段階からの確保ができること
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
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
情報セキュリティ対策に関する費用対効果の測定ができること
単一の技術や基盤に依存する事のリスクを認知できる
潜在的に大きなリスクの対処方法のあり方を考えられること
最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策の設計
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティ対策を実施する者が評価される仕組みの導入
情報管理の徹底をさせられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
取り組みが不十分な情報セキュリティ対策の具体的な導入運用に当たって参考となる手引きの作成ができること
IT障害についての分析ができること
攻撃手法の分析能力の強化ができること
IT障害の要因等の対策検討をして再発防止ができること
情報セキュリティに関する情報収集、分析、共有
事業継続マネジメント(BCM)
オフショア・アウトソーシングに関連する固有リスクを把握できること
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)
各業務・システムの最適化ができること
IT障害、リスクについての分析と改善
CSIRTに対する情報提供体制の構築＆確立
事故、災害や攻撃に対して、事前に考えられうる対策を十分に施せる
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
実施可能業務：
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
適切な暗号化及び電波の範囲設定等の対策
各利用者の環境に応じた対策の優先度に関する意思決定を支援するツール等の作成ができること
製品・サービスにおける脆弱性の排除への対処
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
情報システムに係るリアルタイム監視機能をもてること
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
ネットワークの不適正な利用からの被害防止対策ができること
電子文書に係る成りすまし及び改ざんの防止ができること
ネットワークのIP化に対応した電気通信システムの安全・信頼性が確保できること
ITセキュリティ評価及び認証制度の運用を推進できること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること

業務項目
実施可能業務：
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
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
内部統制の情報システムセキュリティ対応の要件策定
セキュリティ強化に資する新規システムの導入検討
情報セキュリティのリスクを検証する手法の整理(統一化)ができること
事業継続計画の策定ができること
フォレンジック
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
情報セキュリティ対策の手引きの作成ができること
個人情報保護、営業機密管理
インシデント対応
教育
CMU, SPIA-M, LAC-B5-18, RC-27K-1,2,3,4,5,6,7, CMU, SANS-SEC401, MGT411, IS-ISMS, ISMSAudit, BCM, BCMAudit
資格
CISA, CISSP, SEAj-M, CAIS, SANS-GSEC, SANS-G7799

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		概論
侵入検知		概論
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		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		
フォレンジック		
事業継続・災害復旧計画	事業継続管理	
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)

推奨：

知識項目	大分類	中分類

職種名	セキュリティアドバイザー		
定義	情報セキュリティ全般に関してのアドバイスを行う	所属企業・部署グループ	サービス・製品提供組織　営業

業務項目
必須業務
第三者評価の活用を促進できること
ITセキュリティ評価及び認証制度の運用を推進できること
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
情報セキュリティ機能の明確化出来るスキル
情報セキュリティ対策の製品の選定ができること
安全なWebサイト構築の為のガイドラインを検討できること
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティに関する情報収集、分析、共有
実施可能業務
単一の技術や基盤に依存する事のリスクを改善できる
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
情報セキュリティポリシーの改善ができること
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
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
適切な暗号化及び電波の範囲設定等の対策
情報セキュリティのリスクについて定量的評価手法を選定できる
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティ対策実施状況報告ができること
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
内部統制の情報システムセキュリティ対応の要件策定
セキュリティ強化に資する新規システムの導入検討
情報セキュリティポリシーの策定
情報セキュリティのリスクを検証する手法の整理(統一化)ができること
情報資産のリスク分析ができること
事業継続計画の策定ができること
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
サイバーテロ対策に係る体制の導入ができること
情報セキュリティ確保の為の体制整備ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
情報セキュリティの企画・設計段階からの確保ができること
情報セキュリティ対策に関する基本戦略の立案
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
情報セキュリティの制度整備
情報セキュリティリスクや対策の効果等に係る定量化の定義をする
情報セキュリティに関するリスク定量化手法を考えられること
情報セキュリティ対策に関する費用対効果の測定ができること
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
政府統一基準等の導入
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
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
情報セキュリティ対策の手引きの作成ができること
潜在的に大きなリスクの対処方法のあり方を考えられること
情報セキュリティ対策を実施する者が評価される仕組みの導入
情報管理の徹底をさせられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
JPCERTなどの監督・関係機関との情報交換等の運用における連携ができること
個人情報保護、営業機密管理
取り組みが不十分な情報セキュリティ対策の具体的な導入運用に当たって参考となる手引きの作成ができること
攻撃手法の分析能力の強化ができること
情報セキュリティ監査制度の活用ができること
サイバー攻撃発生時の適時適切な機能回復を持たせられること
情報アクセス制限を統合し集中管理ができること
IT障害、リスクについての分析と改善
CSIRTに対する情報提供体制の構築＆確立
電子文書に係る成りすまし及び改ざんの防止ができること
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること

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		概論
侵入検知		概論
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		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		概論
フォレンジック		概論
事業継続・災害復旧計画	事業継続管理	
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等(国内)
		規格・基準・指針・ガイドライン等(国際)
推奨		
知識項目	大分類	中分類

業務項目
教育
CMU、SANS-MGT512
資格
CISM、CISSP、SANS-GSEC

職種名	セキュリティストラテジスト		
定義	企業の経営戦略実現にむけて、セキュリティを活用とした基本戦略を策定、提案、推進する	所属企業・部署グループ	サービス・製品提供組織　企画、営業、自社資産保護組織 企画

業務項目
必須業務：
単一の技術や基盤に依存する事のリスクを改善できる
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
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること
情報セキュリティポリシーの改善ができること
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
投資効果に係る継続的評価プロセスの導入ができること
情報セキュリティのリスクについて定量的評価手法を選定できる
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ対策実施状況報告ができること
ファイル秘匿化ソフトウェアの導入を選定・検討ができること
情報セキュリティ機能の明確化出来るスキル
セキュリティ強化に資する新規システムの導入検討
情報セキュリティポリシーの策定
情報セキュリティのリスクを検証する手法の整理（統一化）ができること
事業継続計画の策定ができること
情報セキュリティ対策に係る行動計画ができること
情報セキュリティ対策の製品の選定ができること
情報セキュリティ対策強化に向けたマイルストーンの検討ができること
サイバーテロ対策に係る体制の導入ができること
情報セキュリティの企画・設計段階からの確保ができること
情報セキュリティ対策に関する基本戦略の立案
ITセキュリティ評価および認証制度(ISO/IEC15408)を利用した要件定義と調達
情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えること
情報セキュリティの制度整備
情報セキュリティリスクや対策の効果等に係る定量化の定義をする
情報セキュリティに関するリスク定量化手法を考えられること
情報セキュリティ対策に関する費用対効果の測定ができること
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
フォレンジック
潜在的に大きなリスクの対処方法のあり方を考えられること
コーポレートガバナンスと内部統制の情報セキュリティ観点からの企業内構築・運用の推進
情報セキュリティ対策を実施する者が評価される仕組みの導入
情報管理の徹底をさせられること
情報セキュリティ対策の実施手順及び成果等の共有化ができること
インシデント対応
情報セキュリティ対策の実施状況の自己点検ができること
情報セキュリティ対策の実施手順、成果等の対策の統一化ができること
個人情報保護、営業機密管理
情報セキュリティに関する情報収集、分析、共有
IT障害、リスクについての分析と改善
情報セキュリティに関する取り組みについて全体としての整合性が確保できること
実施可能業務：
相互依存性解析の成果を踏まえた情報セキュリティ基準等が検討できること
情報セキュリティ対策の持続的改善の為の構造構築ができること
IP v6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システムの導入ができること
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
情報資産のリスク分析ができること
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
情報セキュリティ確保の為の体制整備ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
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
横断的な情報セキュリティ基盤の底上げができること
情報セキュリティ問題に関するPOC機能を持てること
情報セキュリティに関する共通化された物を使用して要求仕様が作成できる
ITセキュリティ評価及び認証制度の運用を推進できること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
IP化の進展に対応した組込み端末のセキュリティ機能の確保を推進できること
政府統一基準等の導入
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
安全なWebサイト構築の為のガイドラインを検討できること
JPCERTなどの監督・関係機関との情報交換等の運用における連携ができること
情報セキュリティ監査制度の活用ができること
サイバー攻撃発生時の適時適切な機能回復を持たせられること
情報アクセス制限を統合し集中管理ができること
CSIRTに対する情報提供体制の構築＆確立
電子文書に係る成りすまし及び改ざんの防止ができること
IP v6によるユビキタス環境構築に向けたセキュリティが確保できること

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		概論
侵入検知		概論
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		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		概論
フォレンジック		概論
事業継続・災害復旧計画	事業継続管理	
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	
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
推奨：		
知識項目	大分類	中分類

業務項目
教育
CMU、SANS-MGT512
資格
CISM、CISSP、SANS-GSEC

職種名	セキュリティ監査人		
定義	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する	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

必須業務：
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
情報セキュリティ対策に関する評価指標の確立が出来ること
第三者評価の活用を促進できること
第三者評価の結果等を活用した情報セキュリティ対策レベルの評価の取り入れができること
企業に係る指標の選定がはかれること
情報セキュリティに関する基準等の浸透状況について情報収集ができること
情報セキュリティ監査制度の活用状況について情報収集ができること
情報セキュリティマネジメントシステム適合性評価制度の活用状況について情報収集ができること
情報セキュリティ対策実施状況の適切な確認・評価ができること
情報セキュリティ対策実施状況報告ができること
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること
情報セキュリティ対策の実施状況の自己点検ができること
各インフラの政府統一基準に係る必須項目の検査ができること
情報セキュリティに関する情報収集、分析、共有
情報セキュリティ監査制度の活用ができること
実施可能業務：
相互依存性解析の成果を踏まえた情報セキュリティ基準等が検討できること
情報セキュリティ対策の持続的改善の為の構造構築ができること
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
情報資産のリスク分析ができること
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
情報セキュリティ確保の為の体制整備ができること
情報セキュリティ対策を推進する体制・制度の整備ができること
情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策の整備ができること
情報セキュリティ問題に関するPOC機能を持てること
教育
LS-0, SPIA-M, LAC-B2,3,4, RC-P6, 27K-5, SANS-AUD429, 507, IS-ISMSAudit, PMSAudit, BCMAudit, KKC-CAIS
資格
CISA, SEAj-M, CAIS, SANS-GSNA, CSA

スキル・知識

推奨：		
知識項目	大分類	中分類
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
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	

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
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
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
	コンテンツ利用の制御	不正コピー対策
		法的要件
認証	認証	種類
攻撃手法	ソーシャルエンジニアリング	公開情報の不正利用
		情報の取扱い
		情報の不正入手
コンプライアンス	コンプライアンス	法令
		規格・基準・指針・ガイドライン等（国内）
		規格・基準・指針・ガイドライン等（国際）
事業継続・災害復旧計画	事業継続管理	事業継続計画（BCP）
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
		情報セキュリティ監査手法
		監査報告書
フォレンジック		概論
物理セキュリティ	物理的脅威	

情報セキュリティ人財 対応教育・資格一覧(2009年度)

	対応教育・資格															
職種	ISACA	(ISC)2	NTTラーニングシステムズ	ひょうご情報教育機構	CompTIA	SEA/J	シスコシステムズ	ソフトピアジャパン	JASA	ラック	リコーヒューマンクリエイツ	SANS	インフォセック	SAAJ	日本サードパーティ	KKC情報システム
プリセールスエンジニア		SSCP	LS-0	Hyogo-B	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14		SANS-SEC301, 401, GSEC				
セールスコンサルタント		CISSP, SSCP	LS-0		CTIA	SEAj-T, SEAj-B						SANS-SEC301, 401 501, GSEC				
テクニカルコンサルタント		CISSP, SSCP	LS-0	Hyogo-B	CTIA	SEAj-T, SEAj-B	CCIE-Sec, CCSP	SPIA-T		LAC-B5-14,16,19,20		SANS-SEC301, 401, 501, 560, AUD507, GPEN, GSNA				
セキュリティアーキテクト(製品・ソリューション)	CISM	CISSP		CMU			CCIE-Sec					SANS-SEC401, 501, 502, GSEC, GCFW				
セキュリティアーキテクト(コンサル)	CISM	CISSP		CMU								SANS-SEC401, 501, GSEC				
セキュリティエンジニア(要求定義)		CISSP, SSCP	LS-0	CMU	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14,19,20		SANS-SEC301, 401, 501, GSEC				
セキュリティエンジニア(企画・設計)		CISSP, SSCP	LS-0	CMU	CTIA	SEAj-T, SEAj-B	CCIE-Sec	SPIA-T		LAC-B5-14,19,20		SANS-SEC401, 501, GSEC				
セキュリティエンジニア(基盤)		CISSP, SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B	CCNA-Sec	SPIA-T		LAC-B5-14		SANS-SEC401, 501, 502, 504, 505, 506, GCFW, GCIH, GCWN, GCUX				
セキュリティエンジニア(アプリ)		SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14,19		SANS-DEV319, 422, 538				
セキュリティエンジニア(DB)		SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14,20		SANS-SEC401, 509, GSOC				
QAマネージャー		SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14,19,20,21		SANS-DEV304, 422, 534, 538				
QAエンジニア		SSCP	LS-0	Hyogo-B	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14,19,20,21		SANS-DEV304, 422, 534, 538,				
セキュリティテスター		SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14,19,20,21,C6		SANS-DEV422, 534, 53, SEC301, 560, 617, AUD507, GPEN, GSNA				
プログラマー		SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-14,19,20		SANS-SEC301, DEV422, 536, 541, 544, 545, 548				
プロジェクトマネージャー	CISM	CISSP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B		SPIA-T		LAC-B5-20		SANS-SEC401, MGT525, GCPM				
セキュリティシステムアドミニストレーター		SSCP	LS-0	Hyogo-B	CTIA	SEAj-M, SEAj-T, SEAj-B	CCSP, CCNA-Sec	SPIA-T		LAC-B5-14,16,18,22,C1		SANS-SEC301, 401, 501, 505, 506, GCWN, GCUX				
オペレーター		SSCP	LS-0	Hyogo-B	CTIA	SEAj-T, SEAj-B	CCSP, CCNA-Sec	SPIA-T		LAC-B5-14		SANS-SEC301, 401, 502, 503, 504, 560, GCFW, GCIH, GCIA, GPEN				
セキュリティアナリスト		CISSP, SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T, SEAj-B		SPIA-T, SPIT-IR		LAC-B5-14,16,22,C1,C3,C5		SANS-SEC401, 503, 504, 560, 601, 610, 700, GCIH, GCIA, GPEN, GREM			JTP-EHM, SC, CEHRapid	
フォレンジックアナリスト		SSCP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T		SPIA-T, SPIT-IR		LAC-B5-14,16,17,22,C1,C2,C4		SANS-SEC401, 508, GCFA			JTP-EHM, SC, CEHRapid	
インシデントハンドラー(プロダクト)		CISSP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T		SPIA-T, SPIT-IR		LAC-B5-14,16,22,C1		SANS-SEC401, 504, GCIH				
インシデントハンドラー(組織)		CISSP	LS-0	Hyogo-B, Hyogo-A	CTIA	SEAj-T		SPIA-T, SPIT-IR		LAC-B5-14,16,22,C1		SANS-SEC401, 504, GCIH				
フィールドエンジニア		SSCP		Hyogo-B, Hyogo-A	CTIA	SEAj-T	CCSP, CCNA-Sec	SPIA-T		LAC-B5-16,22, C1		SANS-SEC401, GSEC				
プライバシーオフィサー	CISM	CISSP								LAC-B1,3,4	RC-P*		IS-PMS, PMSAudit			
プライバシースペシャリスト								SPIA-M		LAC-B1,3,4	RC-P*		IS-PMS, PMSAudit			
CSO/CISO/CIAO	CISM	CISSP									RC27K-6	SANS-MGT512, GSLC				
CSO/CISO/CIAO補佐	CISM	CISSP									RC27K-6	SANS-MGT512, GSLC, GCIM				
セキュリティプロダクトオーナー		CISSP	LS-0							LAC-B5-20		SANS-SEC401, GSEC				
セキュリティサービスオーナー		CISSP	LS-0				CCIE			LAC-B5-20		SANS-SEC401, GSEC				
セキュリティコンサルタント(マネージメント)	CISA	CISSP		CMU		SEAj-M		SPIA-M	CAIS	LAC-B5-18	RC-27K-1,2,4,5,6,7	SANS-SEC401, MGT411, GSEC, G7799	IS-ISMS, ISMSAudit, BCM, BCMAudit			
セキュリティアドバイザー	CISM	CISSP		CMU								SANS-MGT512, GSEC				
セキュリティストラテジスト	CISM	CISSP		CMU								SANS-MGT512, GSEC				
セキュリティ監査人	CISA		LS-0			SEAj-M		SPIA-M	CAIS	LAC-B2,3,4	RC-P6, 27K-5	SANS-AUD429, 507, GSNA	IS-ISMSAudit, PMSAudit, IS-BCMAudit	CSA		KKC-CAIS

情報セキュリティ教育事業者連絡会
情報セキュリティ人財アーキテクチャ対応
教育コース

情報セキュリティ人財アーキテクチャ対応教育コース
目　次

1

(ISC)²Japan

〒105-0001 東京都港区虎ノ門4丁目1-17　神谷町プライムプレイス3F
TEL：03-6311-8800　／　FAX：03-6311-8801
e-mail：infoisc2-j@isc2.org
URL：https://www.isc2.org/japan/

情報セキュリティに関する認定資格・学位	・CISSP（Certified Information Systems Security Professional） ・SSCP（Systems Security Certified Practitioner） ・日本行政情報セキュリティプロフェッショナル（JGISP）
資格試験等	・CISSP認定資格試験：250問4択式（日本語・英語併記） ・SSCP 認定資格試験：125問4択式（日本語・英語併記） ・JGISP認定資格試験：125問4択式（日本語・英語併記）
指定の教育・トレーニング／試験対策教科・項目　等	・CISSP　10ドメインレビューセミナー（座学5日間） ・SSCP　7ドメインレビューセミナー（座学3日間） ・JGISP　4ドメインレビューセミナー（座学2日間）
有資格者数・教育定員数	CISSP認定保持者：国内：1,100名以上、 全世界（133カ国）63,000名以上（2009年6月末現在）
その他の資格・学位関連教育・サービス等	（なし）

団体概要

(ISC)² （アイ・エス・シー・スクエア）は米国フロリダ州パームハーバーに本部を置き、東京、ワシントンD.C、ロンドン、香港にて、情報セキュリティ・プロフェッショナルの認定ならびに教育活動を展開する、グローバル非営利団体です。代表的な資格である全世界の情報セキュリティ・プロフェッショナルに対し高水準の専門性を認定するCISSP（シー・アイ・エス・エス・ピー）は、米国、欧州、また日本の政府機関や民間企業において高く評価されています。現在では情報セキュリティの専門家資格としてグローバルスタンダードとなっているCISSPを始めとするキャリアパスや専門領域に合わせた資格をグローバルに提供しています。国内外においてCISSPの持つ国際レベルでの評価、情報セキュリティを包括的・体系的に理解し実践することが要求されるセミナー・試験内容への評価が年々高まっています。
(ISC)² JapanではCISSP公式セミナー及び試験をはじめ、情報セキュリティ実務者向け資格SSCPや日本独自の情報セキュリティ要件に特化した資格JGISPの公式セミナー及び試験を日本語化し、提供しています。

情報セキュリティ人材育成研修

CISSP・SSCP・JGISP公式セミナーは教材及びその他の配布物が日本語で、根幹となるCBK（Common　Body of Knowledge；(ISC)²の提唱するベストプラクティス）（共通言語）に基づき忠実に作成されています。(ISC)²認定の日本人講師は、全員が情報セキュリティの最前線で活躍するCISSP認定保持者です。日本の実例を交えた質の高い講義に加え、自身の理解度診断に役立つ豊富な演習などもあり、受講者の経験・知識をレビューする場としても有効です。また、ドメイン間の関連性などについても理解を深めることができる内容になっています。

■(ISC)²公式CBK ドメインレビューセミナー
【開催場所】　東京都内
【開催スケジュール】　詳細は(ISC)²Japanホームページにてご確認ください。
【申込方法】　(ISC)²Japanホームページでご紹介している販売代理店様にお申込ください。

2

ISACA（情報システムコントロール協会）東京支部

〒108-0075 東京都港区港南2-16-8-3003（株）ラーニング・アーキテクチャ研究所内
TEL：03-5782-8358　／　FAX：03-5782-8312
URL：http://www.isaca.gr.jp/　（国際本部）
　　http://www.isaca.gr.jp/homepage_j.htm（東京支部）

情報セキュリティに関する認定資格・学位	セキュリティに関する認定資格： 公認情報セキュリティマネージャー: Certified Information Security Manager（CISM®） 2002年創設。情報セキュリティのマネジメント、設計、監督を行なえる技能と経験を認定。セキュリティ管理者、セキュリティ担当役員、セキュリティオフィサー、セキュリティコンサルタントなどを対象。
資格試験等	公認情報セキュリティマネージャー（CISM®）認定試験： 年2回実施 - 毎年6月と12月の第2土曜日
指定の教育・トレーニング／試験対策教科・項目　等	トレーニング：受験希望者を対象にISACA東京支部によるレビューコースを年2回実施予定。 試験範囲：情報セキュリティ・ガバナンス、情報リスク・マネジメント、情報セキュリティ・プログラム開発、情報セキュリティ・プログラム管理、インシデント管理と対応。 詳細はISACA東京支部HPを参照。
有資格者数・教育定員数	日本でのCISM資格保有者（2009年8月時点）　243人
その他の資格・学位関連教育・サービス等	ISACA - その他の資格： ＊公認情報システム監査人: Certified Information Systems Auditor（CISA®） 情報システムの監査、セキュリティコントロールに関する技能と経験を認定。 日本での認定者（2009年8月）　2,288人 ＊Certified in the Governance of Enterprise IT®（CGEIT®） 組織のITガバナンス推進を担う専門家としての技能と経験を認定。 日本での認定者（2009年8月）　130人 また、ISACAの会員になることで以下のサービスが受けられます。 ＊ISACA東京支部主催の月例会参加 ＊ISACA Journalの定期購読（年6冊） ＊先進的調査研究成果物入手、ナレッジデータベースへのアクセス ＊国際本部Bookstoreより会員価格にて書籍購入 ＊ISACA国際本部が主催する会議への参加費割引 ＊国際本部、東京支部各種委員会への参加機会提供 詳細はISACA東京支部HPを参照。

ISACA®
ISACAは、160ヶ国以上に86,000 人を超える会員を有し、IT ガバナンス、コントロール、セキュリティ、アシュアランスのリーダとして世界中で認められています。1969 年に設立されたISACA は、国際会議の開催、ISACA Journal®の出版、情報システム監査とコントロールに関する国際的な標準を策定してきました。また、世界中で高い評価を受けている公認情報システム監査人（Certified Information Systems Auditor - CISA®、1978 年設立以来60,000 人以上の専門家が取得）、公認情報セキュリティマネージャー（Certified Information Security Manager - CISM®、2002 年設立以来9,000 人以上の専門家が取得）及び新しいCGEIT™（Certified in the Governance of Enterprise IT™）の認定制度を運営しています。

関連団体：　IT ガバナンス協会®
IT ガバナンス協会（ITGI™）（www.itgi.org ）は、IT 資産のガバナンスに関連した問題について、ビジネスコミュニティにガイダンスを提供する世界的な非営利独立研究団体です。ITGI は、IT が企業目標との整合を通して価値を提供するとともにリスクを緩和し、IT 資源を適切に管理し、IT の成果を測定できるよう支援するために、1998 年に非営利会員団体ISACA によって設立されました。ITGI は、COBIT®（Control Objectives for Information and related Technology ）及びVal IT™ を策定し、企業のリーダ及び取締役会がそれぞれのIT ガバナンスの責任を果たせるよう、またIT 専門家が付加価値サービスを提供できるよう支援するために、独自の研究及びケーススタディを行っています。

3

Infosec
Risk Management Professionals

株式会社インフォセック
Infosec Corporation

〒150-0013 東京都渋谷区恵比寿1-19-19　恵比寿ビジネスタワー17階
TEL：03-5423-8250　／　FAX：03-5423-8251
e-mail：education@infosec.co.jp
URL：http://www.infosec.co.jp/

情報セキュリティに関する認定資格・学位	情報セキュリティマネジメント、個人情報保護マネジメントのための研修を実施しているため、特に認定資格・学位はありません。
資格試験等	（なし）
指定の教育・トレーニング／試験対策教科・項目　等	（なし）
有資格者数・教育定員数	（なし）
その他の資格・学位関連教育・サービス等	ITガバナンス研修、ITIL研修 情報セキュリティリスクコスト可視化サービス セキュリティ診断、セキュリティ監視サービス（JSOC） セキュアITインフラ構築支援、セキュリティ監視システム構築支援 アプリケーション設計レビュー エンドポイント統合管理（BigFix）、セキュリティリスクマネジメント（Skybox View）、アプリケーションセキュリティ（Fortify）

情報セキュリティの最後の砦は、「人」です。そのために、教育や研修を活用する必要があります。インフォセックでは、情報セキュリティ対策、技術、ISMS、プライバシーマークなどのテーマで、情報セキュリティ教育・研修を実施しています。

〔研修概要〕

■情報セキュリティマネジメントシステム（ISMS）導入・運用	ISMS紹介コース ISMS基本研修コース ISMS認証取得研修コース
■ISMS内部監査	ISMS内部監査員養成コース ISMS内部監査員短期養成コース
■個人情報保護マネジメントシステム（PMS）導入・運用	PMS紹介コース PMS基本研修コース PMS認証取得研修コース
■PMS内部監査	PMS内部監査員養成コース PMS内部監査員短期養成コース
■事業継続マネジメント（ＢＣＭ）導入・運用	BCMS紹介コース BCMS基本研修コース BCMS認証取得研修コース
■ＢＣＭ内部監査	BCMS内部監査員養成コース BCM審査員養成コース

4



NRIセキュアテクノロジーズ株式会社
SANS JAPAN事務局

〒100-0005 東京都千代田区丸の内1-6-5　丸の内北口ビル
TEL：03-5220-2298　／　FAX：03-5220-2039
e-mail：info@sans-japan.jp
URL：http://www.sans-japan.jp/

情報セキュリティに関する認定資格・学位	GIAC（Global Information Assurance Certification） ※情報セキュリティの各分野ごとに23のGIACカテゴリーが存在
資格試験等	GIACは情報セキュリティの分野ごとに、当該個人が具体的な専門スキルを有することを証明する認定試験。高度なテクニカル分野のスキルを証明できる世界的唯一の認定資格。 ■試験形態：Webベースの多肢選択式試験、4時間～5時間の制限時間内に100問～200問に解答。資料持込み可。 ※試験時間・問題数は、選択するGIACのカテゴリーごとに異なります。 ■試験会場：テンプル大学テストセンター（試験日は1か月に1回程度） ■認定の有効期間：４年（認定継続には再受験が必要）
指定の教育・トレーニング／試験対策教科・項目　等	【SANSトレーニング】 SANS認定インストラクターによるトレーニングプログラムを年間で数回程度開催。 **SANS Tokyo 2009 Autumn　（2009年10月19日～24日　会場：ＵＤＸカンファレンス）** コース：SEC401: SANS Security Essentials Bootcamp Style SEC504: Hacker Techniques, Exploits and Incident Handling AUD507: Auditing Networks, Perimeters & Systems **SANS Tokyo 2010 Spring（2010年2月15日～20日　会場：ＵＤＸカンファレンス）** コース：SEC401: SANS Security Essentials Bootcamp Style SEC501:Advanced Security Essentials –Enterprise Defender – SEC560:Network Penetration Testing and Ethical Hacking ※このほかにも80以上のコースラインナップ（特設開催随時）
有資格者数・教育定員数	SANSトレーニング：年間約16,000人の受講実績。 GIAC認定試験合格者数：のべ26,226人（2009年6月30日現在、全世界）
その他の資格・学位関連教育・サービス等	（なし）

SANS認定インストラクターによる質の高い講義と演習、豊富で有益な情報量――SANSトレーニングプログラムは、単なる知識の集積ではなく、実務で使えるスキルを身につけてもらうことが目的です。
CISSP、CISA、CISMなどの認定取得者が次に目指すべきはGIAC！　詳しくはオフィシャルサイトをご覧ください。
日本語サイト　http://www.sans-japan.jp/　英語サイト　http://www.sans.org/

5

エヌ・ティ・ティ・コム チェオ株式会社

東京都港区新橋1-18-16　日本生命新橋ビル7階
TEL：03-3539-5728　／　FAX：03-3539-5714
e-mail：info-edu@nttcheo.com
URL：http://www.nttcheo.com/

情報セキュリティに関する認定資格・学位	「NTTコミュニケーションズ　インターネット検定　.com Master」 .com Master ★　　クライアントネットワークにおける情報受信・活用 .com Master ★★　　小規模ネットワークにおける構築・運用・保守および情報発信 .com Master ★★★　SMEネットワークの構築・運用管理 ※本資格はＮＴＴコミュニケーションズ株式会社が実施しています
資格試験等	定期検定：実施時期：7月、12月の第一日曜日※★★★は12月のみ実施／会場：全国主要都市／検定方式：多肢選択・マークシート（ペーパー）方式 通年検定：実施時期：随時　★、★★のみ実施／会場：プロメトリック社公認テストセンタ／検定方式：多肢選択・コンピュータテスト方式 出張検定：実施時期：随時　★、★★のみ実施／会場：原則お客様側の施設利用／検定方式：多肢選択・マークシート（ペーパー）方式
指定の教育・トレーニング／試験対策教科・項目　等	com Master ★　研修：ビジネスで使える（インターネットサービス利用者へのサポートができる）レベルの知識の習得 com Master ★★　研修：インターネット上で情報発信サーバを構築し、運営することができるレベルの知識・スキルの習得 （講師派遣型研修となっております）
有資格者数・教育定員数	非公開
その他の資格・学位関連教育・サービス等	（なし）

「.com Master」は、NTTコミュニケーションズが実施しているIT資格検定です。インターネットがビジネスにおいて不可欠な現在、企業が求めるITスキルを認定する「.com Master」を取得することによって、さまざまな可能性が広がります。「.com Master」は、3つのグレードに分かれているため、目標としている人材像に合ったグレードを受検することができます。受検することによって、知識の整理をすることができるとともに、ITスキルを仕事で活用するための自信にもつながります。また、教育者サイドにとっては、教育の効果やスキルレベルを客観的に把握することができます。
「.com Master」資格の習得、すなわち、時代が求めるインターネットスキルを客観的に認定されることにより、合格者にとって確かな証になるだけでなく、明確な判断基準を得たい企業にとっても確かなものさしになります。ベンダーにとらわれることなく、インターネットに関する最新の知識や技術を習得できますから、業種や職種を問わず広範な活用が期待でき活躍の舞台も広がります。

6

エヌ・ティ・ティ ラーニングシステムズ株式会社

〒105-0004 東京都港区新橋4-21-3　新橋東急ビル
TEL：03-6721-4745　／　FAX：03-3434-2411
e-mail：Kns-call@hot.nttls.co.jp
URL：http://www.nttls.co.jp/

情報セキュリティに関する認定資格・学位	（なし）
資格試験等	・ITILファンデーション ・ITILサービスマネージャ
指定の教育・トレーニング／試験対策教科・項目　等	・CISSP公式セミナー、SSCP公式セミナー、JGISP公式セミナー （外部研修機関　(ISC)^2　https://www.isc2.org/japan/） ・情報セキュリティ専門家養成講座 ・ITILファンデーション ・ITILサービスマネージャ ・.comMaster★ ・.comMaster★★ ・電気通信主任技術者講座
有資格者数・教育定員数	（なし）
その他の資格・学位関連教育・サービス等	・総合セキュリティコンサルティング ・マニュアル制作 ・映像制作、映像ソリューション ・コンテンツ配信、コンテンツ開発サービス ・サーバ関連サービス

NTTラーニングシステムズでは、多角的アプローチが必要とされる光ブロードバンド・ユビキタス時代に対応すべく、「教育・研修」、「Web」、「映像」の３つの事業領域を設けています。独自のノウハウや複合的技術、創造力の蓄積を活かし、3つの領域のシナジー効果をベースにして真のトータルソリューションを実現します。社員一人ひとりの自律的な「気づき」、ビジョンや目的を基本的なプロセスに展開する「考える」力、そしてお客様やパートナーとの間のナレッジや考えの共有を推進する「コミュニケーション」の機会を創出しお客様の視点でニーズを共有しながら、課題解決に結びつくコンサルティング・サービスを提供します。
情報セキュリティ研修においては、セキュリティ専門施設「セキュリティファクトリー」で、スペシャリスト教育、社員、管理者への教育を体系的に実施できる研修カリキュラムを提供しており、目的別、レベル別等にトレーニングマップを体系化し、情報セキュリティに関する段階的な知識・スキル向上をサポートします。また、「情報セキュリティ専門家養成講座」では、情報セキュリティ技術について網羅的・体系的に修得する研修で、情報セキュリティ資格であるCISSP、CISA、情報セキュリティスペシャリスト、Security+、SEA/J等の資格取得に必要な基礎知識を身につけることができ、CISOを目指す方にも対応した講座を提供しております。

7

株式会社ケーケーシー情報システム
情報セキュリティ監査センター

〒602-8466 京都市上京区千本通元誓願寺上る南辻町369番地の3
TEL：075-465-9203　／　FAX：075-465-9246
e-mail：kansacenter@kkcjoho.co.jp
URL：http://www.kkcjoho.co.jp/kansa-edu/

情報セキュリティに関する認定資格・学位	公認情報セキュリティ監査人（CAIS）
資格試験等	①研修修了試験 ②トレーニング修了試験 ③監査経験確認試験
指定の教育・トレーニング／試験対策教科・項目　等	公認情報セキュリティ監査人研修・トレーニング
有資格者数・教育定員数	（なし）
その他の資格・学位関連教育・サービス等	情報セキュリティ監査サービス等

弊社は特定非営利活動法人日本セキュリティ監査協会（JASA）の外部研修実施機関として、公認情報セキュリティ監査人研修・トレーニングの実施を行なっております。

〔研修概要〕
■情報セキュリティ監査人研修・トレーニング５日間コース
■情報セキュリティ監査人研修２日間コース
■情報セキュリティ監査人トレーニング３日間コース
【開講場所】　京都市内
【募集人数】　１０名／１講座
【申込方法】　弊社ホームページからお申し込み下さい。
　　http://www.kkcjoho.co.jp/kansa-edu/

8

CompTIA日本支局

〒101-0061 東京都千代田区三崎町3-4-9　水道橋MSビル7F
TEL：03-5226-5345　／　FAX：03-5226-0970
e-mail：info_jp@comptia.org
URL：http://www.comptia.jp

情報セキュリティに関する認定資格・学位	CompTIA Security+ セキュリティエンジニアの実務能力を評価するために作成されたワールドワイドの認定資格です。2008年5月には、ANSI（米国規格協会）により、ISO17024/17011の認定を受けました。CompTIA Security+では、CompTIA Network+に相当するネットワーク環境の実務経験を持つ方に必須となるセキュリティスキルを評価するために設計され、セキュリティの一般概念、インフラストラクチャセキュリティ、暗号技術、業務・組織面でのセキュリティ策定など、セキュリティに関連する知識と改善能力、問題解決能力などが幅広く問われます。また、CompTIA Security+は、Symantec、VeriSign、RSA Securityなどのセキュリティ業界におけるリーダー企業やFBI、US Secret Serviceなどの専門機関のファンドとサポートにより作成されています。 **認定資格ロゴ**
資格試験等	CompTIA認定資格試験は、日本国内150ヶ所以上のピアソンVUE、プロメトリックの認定テストセンターで毎日受験をすることが可能です。
指定の教育・トレーニング／試験対策教科・項目　等	CompTIA Security+のトレーニングは、テキスト、オープンコース、企業研修などがトレーニングパートナーから提供されています。詳細については、下記URLからご確認ください。 トレーニングパートナー http://www.comptia.jp/cont_school.html
有資格者数・教育定員数	50,000（2008年3月現在、ワールドワイド）
その他の資格・学位関連教育・サービス等	CompTIA A+、CompTIA Network+、CompTIA Server+、CompTIA Linux+、CompTIA Project+、CompTIA CTT+、CompTIA PDI+、CompTIA CDIA+、CompTIA Convergence+

CompTIAは、EDIが様々な規格で利用され情報が飛び交う中、ISOやIEEEに対し標準化を提言するため、各社が集まる場として、1982年に設立されたIT業界団体です。
欧米を中心とし14拠点を持ち、日本では2001年4月に支局が開設されています。IT業界や各種団体、教育機関など100ヶ国22,000機関以上が会員として活動に参加いただいています。（2009年1月現在）

CompTIA認定資格は、各「業務」の基盤となる、技術知識やスキル、問題解決や状況判断などの実務能力を評価します。現在、12の業務分野の認定資格をグローバルに提供しています。（内10分野が日本語にて受験可能、2009年6月現在）グローバルに多数の現場従事者が認定資格試験の開発に関与し、中立的なスキル定義と問題開発がされています。認定数は、ワールドワイドで100万人を突破。CompTIA A+、Network+、Security+は、ISO17011、ISO17024取得しています。

日本国内でも、多くの企業に人材育成方針の一環としてご活用いただき
1. 生産性の向上
2. 売上に対する貢献
3. 業務レベルの質の統一
などの効果を上げています。

詳細については、CompTIA日本支局サイトをご確認ください。
CompTIA日本支局　http://www.comptia.jp

9

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1　ミッドタウン・タワーシスコ受付：21階
TEL：03-6434-6500
e-mail：certification-japan@cisco.com
URL：www.cisco.com/jp/go/training/

情報セキュリティに関する認定資格・学位	【シスコ技術者認定】 －エントリーレベル CCENT（Cisco Certified Entry Networking Technician） －アソシエイトレベル CCNA（Cisco Certified Network Associate） CCNA Security －プロフェッショナルレベル CCSP（Cisco Certified Security Professional） －エキスパートレベル CCIE Security（Cisco Certified Internetwork Expert Security） 【スペシャリスト】 ・Cisco ASA Specialist ・Cisco IPS Specialist ・Cisco Security Sales Specialist ・Cisco Network Admission Control Specialist ・Cisco Security Solutions and Design Specialist
資格試験等	www.cisco.com/jp/go/certification/ Pearson VUE（ピアソンビュー）ジャパンの提携試験センターにて受験可能です。
指定の教育・トレーニング／試験対策教科・項目　等	各トレーニングコースは、シスコの認定ラーニングパートナーにて提供されています。 www.cisco.com/jp/go/clp/ また、試験対策本としてシスコ公式書籍シスコプレスが翔泳社より出版されています。 http://www.seshop.com/se/ciscopress/
有資格者数・教育定員数	非公開
その他の資格・学位関連教育・サービス等	Securityに関連するRouting&Switching, Voice, Wireless, Service Provider, Designの6コースを加え、全7分野、また最高位Cisco Certified ArchitectからエントリーレベルのCCENTまで5つのレベルにて、技術レベル／スキルを評価できる資格があります（2009年8月現在）。 また、資格取得のためや取得保有者のためのコミュニティ、Cisco Learning Network（www.ciscolearningnetwork.com/jp/ ）を2009年9月より、日本語でも展開しています。

■シスコシステムズ合同会社について
シスコは、ビジネスの基盤となるインテリジェントなネットワーキングソリューションから、音声、映像、データ、ストレージ、セキュリティ、エンターテイメントをはじめとする新しい分野、そして、人々の仕事や生活、娯楽、学習のあり方を一変させることのできるネットワークプラットフォームの提案を目指しています。

10

株式会社シマンテック

〒107-0052 東京都港区赤坂1-11-44　赤坂インターシティー9F
TEL：03-5114-4300　／　FAX：03-5114-4011
e-mail：edu_japan@symantec.com
URL：www.symantec.co.jp

情報セキュリティに関する認定資格・学位	シマンテック認定技術者（Symantec Certified Specialist）
資格試験等	2008年2月より開始された新しいシマンテック認定資格制度では、セキュリティ製品を含む各シマンテック製品・バージョンで提供されています。認定資格試験はプロメトリック社から提供されており、随時受付、受験可能です。
指定の教育・トレーニング／試験対策教科・項目　等	Symantec Endpoint Protection 11.0トレーニングが2コース計5日間と対応する資格試験「250-311 Symantec Endpoint Protection 11.0の管理」 Symantec Enterprise Vault 8.0トレーニングが3コース計9日間と対応する資格試験「250-308 Administration of Symantec Enterprise Vault 8.0 for Exchange」 Symantec Backup Exec 12 for Windowsトレーニングが2コース計6日間と対応する資格試験「250-312 Administration of Backup Exec 12 for Windows」 Veritas NetBackup 6.5トレーニングが7コース計19日と対応する資格試験「250-265 NetBackup 6.5 for UNIXデータ保護と管理」、「250-365 Data Protection Administration for Windows using NetBackup 6.5」 Veritas Storage Foundation 5.0トレーニングが2コースで計7日間と対応する資格試験「250-250 Veritas Storage Foundation 5.0 Administration for UNIX」 Veritas Cluster Server 5.0トレーニングが2コースで計8日間と対応する資格試験「250-251 Administration of High Availability Solution for UNIX using Veritas Cluster Server 5.0」「250-351 Administration of Veritas Storage Foundation High Availability 5.0 for Windows」
有資格者数・教育定員数	現在の認定資格制度に移行以来、認定技術者数は全世界で約3000人です。試験毎に時間と合格点が設定されており、平均試験時間は120分、平均合格点は70%です。
その他の資格・学位関連教育・サービス等	シマンテック認定技術者には、認定資格ロゴの提供や認定資格関連の情報の提供、認定技術者フォーラムへの参加が提供されます。

シマンテックは、企業および個人の情報の保護（安全）と管理を実現するためのセキュリティ、ストレージおよびシステム管理ソリューションを提供する世界的リーダーです。カリフォルニア州クパティーノに本社を置き、世界40カ国以上で事業を展開しています。
シマンテックが提供するセキュリティ、ストレージ、システム管理ソリューションは、ソフトウェアとそれに関連するサービスにより構成されます。シマンテックでは、企業におけるソリューションの実装、運用、及び導入効果を高めるため、製品の技術やベストプラクティスを提供する各種トレーニングを提供しております。また、2008年2月に認定資格制度を刷新し、製品やバージョン毎に認定資格試験を提供しております。製品やバージョンの出荷に伴い、認定資格試験も随時更新や追加を行なっております。

11

SEA/J
（セキュリティ・エデュケーション・アライアンス・ジャパン）

〒135-0016 東京都江東区東陽3-23-21　プレミア東陽町ビル
TEL：03-5634-8640　／　FAX：03-5634-8642
e-mail：seajinfo@sea-j.net
URL：http://www.sea-j.net/

情報セキュリティに関する認定資格・学位	・CSBM（Certified Security Basic Master） ・CSPM of Technical（Certified Security Professional Master of Technical） ・CSPM of Management（Certified Security Professional Master of Management）
資格試験等	CBT方式もしくはマークシート方式（認定校による）。 トレーニングを受講せず、受験のみの場合には、プロメトリックによるCBT方式のみ。 実施日時は受験するテストセンター及び申し込み状況による。
指定の教育・トレーニング／試験対策教科・項目　等	SEA/J認定校による各資格認定試験に対応した、SEA/J認定セミナー。 ・CSBM対応 →SEA/J基礎コース（座学/2日間/16章） http://www.sea-j.net/curriculum/basic.html ・CSPM of Technical 対応 →SEA/J応用コーステクニカル編（座学+実機演習/3日間/11章） http://www.sea-j.net/curriculum/technical.html ・CSPM of Management 対応 →SEA/J 応用コースマネジメント編（座学+机上演習/2日間/12章） http://www.sea-j.net/curriculum/management.html
有資格者数・教育定員数	有資格者数（2009年3月31日時点）：CSBM　：4641人 CSPM of Technical　：511人 CSPM of Management　：384人 教育定員数：各認定校による
その他の資格・学位関連教育・サービス等	資格取得者（試験合格者）には、認定証の送付、合格者向けサイトへのアクセス情報が送付されます。また、合格者向けサイトやメール配信などで合格者の方向けのご案内が行われることがあります。

SEA/J（シージェイ）は、日本における情報セキュリティ知識の普及と技術者育成を目的とし、“情報セキュリティ教育には製品やベンダーに偏らない体系的なプログラムが必要である”との考えに賛同したセキュリティベンダー、メーカーによって共同で設立された団体です。
認定セミナーで用いるテキストとその知識範囲に対応した資格試験、及び資格試験合格者への資格認定を行っています。
IPA情報セキュリティスキルマップ等に対応した国産のカリキュラムを提供し、幅広い情報セキュリティの知識について、体系的に必要項目を網羅した基礎知識を身につけていただくことで、一定の知識レベルに基づく現場のコミュニケーションの円滑化や更なるスキルアップの為の土台づくりの一助となるべく活動しております。
また、最近では学校教育の場でも採用いただくケースが増えてきております。

12

財団法人ソフトピアジャパン

〒503-8569 岐阜県大垣市加賀野4丁目1番地7
TEL：0584-77-1166　／　FAX：0584-77-1107
e-mail： training@softopia.or.jp
URL： http://www.softopia.or.jp

情報セキュリティに関する認定資格・学位	（なし）
資格試験等	（なし）
指定の教育・トレーニング／試験対策教科・項目　等	（なし）
有資格者数・教育定員数	（なし）
その他の資格・学位関連教育・サービス等	（なし）

団体概要

財団法人ソフトピアジャパンは、岐阜県が推進する「ソフトピアジャパンプロジェクト」の推進母体として設立された公益法人です。

当財団は、中小企業の情報化・競争力を支援する「産業高度化事業」と地域産業の高度化を担う産業人材の育成・創出を行う「人材育成事業」の２事業に取り組んでいます。

人材育成事業では、情報産業をはじめ、製造業、サービス産業など全産業の全階層を対象に、IT関連研修を実施しています。

情報セキュリティ人材育成研修

情報セキュリティ分野における高度な知識・技術を有する人材育成の拠点として開設した「情報通信セキュリティ人材育成センター」では、“実践型”の研修を基本とした「情報通信セキュリティ人材育成研修（3コース）」を企業・団体様向けに提供します。

(1)「セキュリティマネジメントコース」

情報セキュリティにどのように取り組むべきか、組織の管理者の視点で携わる方を対象に、情報セキュリティポリシーの策定やセキュリティ対策の管理運用を実施するために必要なマネジメントの知識を習得します。

(2)「セキュリティテクニカルコース」

情報セキュリティに対して技術的な視点・側面で携わる方を対象に、情報通信システムの管理上想定すべき脅威について学び、さらにシステムへの攻撃方法としてどのようなものがあるかを、主に技術的観点から学習し、その対策手法について実演を交えながら習得します。

(3)「インシデントレスポンス実践コース」

情報セキュリティの事件・事故への対応を組織としての危機管理ととらえ、体制の整備、対応に携わる方を対象に、情報セキュリティ対策におけるインシデントレスポンスの基礎知識を学習し、インシデント対応実習を通じてシステムが攻撃を受けた際の対処策について習得します。

13

日本サード・パーティ株式会社

東京都港区港南2-15-1　品川インターシティ A棟 13階
TEL：03-5782-7600（代表）　／　FAX：03-5479-4797
e-mail：webmaster@jtp.co.jp
URL：http://www.jtp.co.jp/

情報セキュリティに関する認定資格・学位	認定資格： Certified Ethical Hacker（CEH） コース名： Ethical Hacking and Countermeasures エシカル・ハッキングとセキュリティ対策　5日間コース コース概要：ＥＣ-Ｃｏｕｎｃｉｌ社が提供しているＣＥＨライセンス認定コースです。 Lab環境での実践的なハッキング技術演習によって、インターネット上での最新の攻撃手法のトレンドとその対抗策を身につけます。技術の証明としてCEHの認定資格取得可能レベルを目指します。 ・イントロダクション、倫理と法律　・フットプリンティング　・スキャニング ・列挙攻撃　・Linuxセキュリティ ・ファイアウォールの回避、侵入検知システムとハニーポット ・バッファオーバーフロー　・暗号技術　・システムハッキング等
資格試験等	プロメトリック/ピアソンＶＵＥ試験会場にて随時受けられます。
指定の教育・トレーニング／試験対策教科・項目　等	日本サード・パーティ株式会社　品川トレーニングセンターにて開催 お申し込みホームページアドレス：http://www.jtp.co.jp/education/index.html Certified Ethical Hacker（CEH）試験の直前対策コースも用意しています。
有資格者数・教育定員数	コース定員数：16名/20名
その他の資格・学位関連教育・サービス等	CEHセキュリティ教育コースに加えて、Ｓｕｎ、Ｓｙｍａｎｔｅｃ、ＲｅｄＨａｔ等、ＩＴベンダの要素技術セキュリティ教育も数多く提供しています。弊社独自のレベルの測定と改善のフィードバックを具体的に提示するアセスメントツール及び教育費用対効果を可視化した進捗管理ツールを提供し、ライセンス取得までをトータルサポートいたします。

日本サード・パーティ（ＪＴＰ）は、海外ＩＴメーカに対する日本とアジアパシフィック市場におけるテクニカル・サポートのアウトソーサとして戦略的パートナー契約を締結しています。85社を超える海外ＩＴメーカの技術部門の役割を担い、コンサルティングやビフォア・サービスからアフター・サービスまでさまざまなサービスレイヤーをＢＰＯで提供しています。特に、セキュリティ分野においては、国際標準でもあるCertified Ethical Hacker（CEH）認定資格者を115名有し様々なセキュリティ・プロフェッショナルサービスを提供しています。ハッカー以上の技術力に加え、絶対に悪事を働かないという高い倫理観と道徳心を兼ね備えたエンジニアによって、OSや主なネットワークサービスの脆弱性を検査・診断します。診断の結果、脆弱ポイントが発見されれば、コンサルティングを通じて適切な対策の立案、その実施効果測定、改善というセキュリティプロセス管理によってシステムを脅威から守ります。

各種セキュリティ・サービス

- 脆弱性診断サービス
- コンサルティングサービス
- 監視サービス
- プロセス管理サービス
- 構築・導入・運用サービス
- トレーナ育成サービス

14

特定非営利活動法人　日本システム監査人協会

東京都中央区日本橋茅場町2-8-8　共同ビル65号
TEL：03-3666-6341　／　FAX：03-3666-6342

情報セキュリティに関する認定資格・学位	○公認システム監査人　（システム監査技術者試験合格者およびそれと同等の知見を有する者に対し、さらに所定の実務経験の有無を確認して認定する。書類審査、小論文、面接を課する。年２回、春秋） ○システム監査人補（システム監査技術者試験合格者およびそれと同等の知見を有するが、実務経験の要件を満たしていない者。書類審査。年２回、春秋） 　いずれも、資格認定後は所定の継続教育受講義務を課する
資格試験等	
指定の教育・トレーニング／試験対策教科・項目　等	応募者の資格は、原則、情報処理技術者試験のシステム監査技術者とする。ただし、情報処理技術者試験の他種目の合格者、ＣＩＳＡ，技術士、公認会計士、中小企業診断士、ＩＴコーディネータ等は、所定の研修科目を履修し、一定以上の成績を修めれば、システム監査技術者に準ずるものとして、応募可能である。 他資格者の研修科目は、情報システムに関する知識、システム監査に関する知識、論文およびプレゼンテーションの３つで、基礎資格により、受講すべき科目が違う。 　協会からの委託研修機関 　　（1）インターギデオン　http://www.intergideon.com/ 　　（2）情報システム監査　http://www.isanet.co.jp/
有資格者数・教育定員数	公認システム監査人　４３３名（2008年末現在） システム監査人補　　２７７名（　　〃　　） 　年間取得者数50名程度（公認システム監査人、システム監査人補あわせて） 　公認システム監査人の合格率　40％程度 　（合格は絶対基準で、募集期により変動する）
その他の資格・学位関連教育・サービス等	システム監査実務セミナー（2日ずつ計4日間）では、システム監査の全体過程を経験できるように、受講者が数名のチームを組み、講師が経営者、情報システム部長、業務部門長などを演じてインタビューに応ずるなど、ロールプレイも交え、報告書の作成までを指導する。各２日とも宿泊を伴い、受講者は夕食後も課題に取り組む。 　また、内部統制セミナーなども特定の分野を目指すもの、およびシステム監査に関連する幅広い分野の講師による講義形式の月例研究会を開催している。 ＜自団体の詳細説明＞ 　当協会は、もともと会員同士の研鑽を目的として発足した。有志による部会として発展した各種事業は、NPO活動に係る事業(定款第５条)として定着し、その主な調査・研究活動には、システム監査事例研究会、システム監査基準研究会、情報セキュリティ監査研究会、個人情報保護監査研究会、法人部会、前述の月例研究会などがある。 　このうち、特記するサービスとしては、前述のシステム監査実務セミナーなどを主管しているシステム監査事例研で、不定期に「システム監査普及サービス」を実施していることである。 　これは、会員にシステム監査の実地を勉強してもらうため、外部の稼動しているシステムについて、システム監査を実施し、監査報告書を提出するもの。 　監査を実施する側は、会員でシステム監査経験者をリーダー、未経験者をチーム員とするチームを組み、監査を受ける側は、実際のシステム監査を受け、費用は、交通費など実費程度を支払う。 　システム監査基準研では、各種基準を実務で適用する際の細目などを検討し、体系化をはかっている。

（なし）

15

特定非営利活動法人 日本セキュリティ監査協会

〒103-0025 東京都中央区日本橋茅場町2-8-4　全国中小企業会館5階
TEL：03-5640-7060　／　FAX：03-5640-0666
e-mail：office@jasa.jp
URL：http://www.jasa.jp/

情報セキュリティに関する認定資格・学位

資格区分	役割
公認情報セキュリティ主任監査人	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査チームを編成し監査を実施する場合に監査チームリーダとなって、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する役割を行う。また、公認情報セキュリティ監査人がOJTとして監査チームリーダを務める場合は、これを指導し評価する。
公認情報セキュリティ監査人	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する役割を行う。また、上位の監査人の指導のもとで、OJTとして監査チームリーダを務め、経験を積んで、公認情報セキュリティ主任監査人をめざすことができる。加えて、情報セキュリティ監査人補がOJTとして監査に参加している場合は、これを指導し評価する。
情報セキュリティ監査人補	情報セキュリティ監査制度に対する知識と経験を有し、OJTとして監査に参加する。 監査経験を積んで、公認情報セキュリティ監査人をめざすことができる。
監査アソシエイト	監査チームリーダの要請によりチームの一員として専門知識にもとづく助言を行う。

資格試験等

資格区分（略称）	知識			経験				実証された能力	
	研修		専門分野申告	トレーニング		監査経験		面接審査	推薦書
	受講	修了試験		受講	修了試験	試験	申告		
主任監査人	○	○	○	○	○	○	○	○	○
監査人	○	○	○	○	○	○	○	×	○
監査人補	○	○	×	○	○	×	×	×	×
監査アソシエイト	○	○	○	×	×	×	×	×	○

指定の教育・トレーニング／試験対策教科・項目　等

○ 協会認定研修コース（http://www.jasa.jp/qualification/explanation/course02.html ）
○ 協会認定トレーニングコース（http://www.jasa.jp/qualification/explanation/course05.html ）
上記２コースにつき、下記の外部研修実施機関で受講することが可能です。
株式会社 ケーケーシー情報システム（http://www.kkcjoho.co.jp/ ）
社団法人 中部産業連盟（http://www.chusanren.or.jp/ ）
株式会社 富士通ソーシアルサイエンスラボラトリ（http://www.ssl.fujitsu.com/ ）
リコー・ヒューマン・クリエイツ株式会社（http://www.rhc.co.jp/ ）

有資格者数・教育定員数

資格者数：主任監査人：73名　監査人：183名　監査人補：309名　監査アソシエイト：270名
（2009年7月31日現在、格上げ登録の重複を含む）
教育定員数：協会認定研修コース 最大約50名、協会認定トレーニングコース 最大約25名

その他の資格・学位関連教育・サービス等

情報セキュリティ監査に関する下記の無料セミナーを実施しています。詳細は日本セキュリティ監査協会のWebサイトでご確認ください。　（主催：経済産業省／日本セキュリティ監査協会）
■2009年度全国縦断情報セキュリティ監査セミナー（http://www.jasa.jp/seminar/secf2009lh.html）
■情報セキュリティ監査実践セミナー（http://www.jasa.jp/seminar/practice_seminar.html）

■日本セキュリティ監査協会（JASA）について
2003年4月1日、経済産業省によって施行された「情報セキュリティ監査制度」を着実に浸透させるための運営体として同年10月に設立されました。情報セキュリティ監査に携わる企業・組織・監査人の方々が会員となり、「情報セキュリティ監査制度」の普及・啓発と、民間企業並びに地方公共団体をはじめとする行政機関などにおける情報セキュリティの向上を目指し、情報セキュリティ監査市場の創出、具体的なガイドラインの整備、監査の品質向上、個人情報保護法など他制度との整合性の検討などの活動を行っています。
会長：土居範久（中央大学教授・慶應義塾大学名誉教授／日本学術会議第20期副会長）

16

Carnegie Mellon CyLab Japan

財団法人ひょうご情報教育機構（カーネギーメロン大学日本校）

〒650-0044 神戸市中央区東川崎町1丁目3-3　神戸ハーバーランドセンタービル17F
TEL：078-360-6311　／　FAX：078-360-1617
e-mail：info@cmuj.jp
URL： http://www.cmuj.jp

情報セキュリティに関する認定資格・学位	学位：MSIT-IS（Master of Science in Information Technology – Information Security、修士（情報技術－情報セキュリティ））
資格試験等	（なし）
指定の教育・トレーニング／試験対策教科・項目　等	大学院：カーネギーメロン大学日本校情報セキュリティ研究科修士課程 研　修：情報セキュリティ人材育成プログラム
有資格者数・教育定員数	（なし）
その他の資格・学位関連教育・サービス等	情報セキュリティに関するセミナーの実施等

兵庫県と民間企業19社によって設立された財団法人ひょうご情報教育機構は、カーネギーメロン大学日本校の運営や、情報セキュリティに関する人材育成、調査研究等を行っています。

////////////// 情報セキュリティ人材育成プログラム //////////////

■ベーシックコース （中級者向け／専門的・実践的な知識と実務経験をお持ちの方）
- 講座①　…　バッファオーバーフローの原理
- 講座②　…　トラフィックダンプの解析
- 講座③　…　LANの盗聴
- 講座④　…　ホストへの侵入と攻撃（1）

■アドバンスドコース （中上級者向け／高度な知識と実務経験をお持ちの方）
- 講座①　…　ソフトウェアの脆弱性
- 講座②　…　侵入されたホストのディスク解析
- 講座③　…　無線LANの脆弱性調査
- 講座④　…　ホストへの侵入と攻撃（2）

【開講場所】 カーネギーメロン大学日本校内、情報通信セキュリティ人材育成センター
【募集人数】 1講座あたり　15名
【講　　師】 野川裕記　東京医科歯科大学情報医科学センター副センター長
高倉弘喜　京都大学学術情報ﾒﾃﾞｨｱｾﾝﾀｰﾈｯﾄﾜｰｸ研究部門准教授
齋藤和典　株式会社セキュアウェア代表取締役
マシス・ザッカリー財団法人ひょうご情報教育機構研究員
【申込方法】 カーネギーメロン大学日本校のウェブサイトからお申し込み下さい。
http://www.cmuj.jp

17

株式会社ラック

〒105-7111 東京都港区東新橋1-5-2　汐留シティセンター11階
TEL：03-5537-2610　／　FAX：03-5537-2619
e-mail：info-academy@lac.co.jp
URL：http://www.lac.co.jp/

情報セキュリティに関する認定資格・学位	（なし）
資格試験等	（なし）
指定の教育・トレーニング／試験対策教科・項目　等	（なし）
有資格者数・教育定員数	（なし）
その他の資格・学位関連教育・サービス等	情報セキュリティ関連研修コースの入門～実践や、CISSP CPE認定トレーニングなど『ラックセキュリティアカデミー』として幅広いセキュリティ教育を提供

ラックセキュリティアカデミーは『人材から人財に』をテーマに、グローバルな情報セキュリティ教育に標準をおき、日本国の情報セキュリティ政策・戦略に沿った実践的情報セキュリティ教育の支援を行います。
日本国内最大級の監視センター『JSOC』や、情報セキュリティの最先端技術の研究・調査を行う『サイバーリスク総合研究所』における生の情報を元に、情報セキュリティを専門としない一般社員向けのわかりやすいセキュリティ教育からプロフェッショナルを目指す方向けの高度な教育までを提供します。

＜ラックセキュリティアカデミーのご紹介＞

■基礎コース
オフィスワークに必要な情報セキュリティの知識やルールの習得を目指します。セキュリティを専門としない一般職員向けのコースを取り揃えています。
コース例）新入社員向け情報セキュリティ躾コース、オフィスユーザ向けコース、ほか

■応用コース
理論やメカニズムの習得を目指します。セキュリティ専門家を目指す方向けに体系的に学習できるコースを取り揃えています。
コース例）情報セキュリティスペシャリスト育成コース　全20コース、ほか

■実践コース
業務を実施できる知識を習得し、さらに実践に近い形式（ケーススタディ、ハンズオンなど）で実務的な技術・手法を習得します。
コース例）セキュア開発Webアプリケーションコース、実践！インシデント・レスポンスコース、実践！マルウェア解析ハンズオンコース、ほか

18

RICOH

リコー・ヒューマン・クリエイツ株式会社
リコー情報セキュリティ研究センター

東京都中央区銀座6-14-5　銀座ホウライビル2F

情報セキュリティに関する認定資格・学位	・ISMS審査員 ISMS認証基準への適合性を審査する要員で、財団法人日本規格協会マネジメントシステム審査員評価登録センター（以下、JRCA）が評価登録しています。ISMS審査員資格は３段階に分かれており、その内訳は「主任審査員」「審査員」「審査員補」となっています。 ・プライバシーマーク審査員 プライバシーマーク制度への適合性を審査する要員で、財団法人日本情報処理開発協会（JIPDEC）が評価登録しています。プライバシーマーク審査員資格は3段階に分かれており、「主任審査員」「審査員」「審査員補」となっています。
資格試験等	【ISMS審査員】https://seminar.rhc.co.jp/public/seminar/view/1 【プライバシーマーク審査員】http:/seminar.rhc.co.jp/public/seminar/view/51
指定の教育・トレーニング／試験対策教科・項目　等	・ ISMS審査員 JRCAの定めたカリキュラムにそった教育内容 ・ プライバシーマーク審査員 JIPDECの定めたカリキュラムにそった教育内容
有資格者数・教育定員数	・ ISMS審査員 約4500名 ・ プライバシーマーク審査員 約850名
その他の資格・学位関連教育・サービス等	

リコー情報セキュリティ研究センター（R-ISAP）は情報セキュリティに関する調査研究や教育、コンサルティングを通じてネットワーク社会で事業を展開する皆様の安全性と信頼性の向上に貢献します。従来のマネジメントスキルに加え、詳細管理項目に関連する技術的なスキルを習得することにより、よりセキュアなISMSの構築が実現します。R-ISAPの教育事業では「トータルマネジメント」をサポートするための体制を整えています。

執筆編集者名

情報セキュリティ教育事業者連絡会

【開発者】スキルワーキンググループ

衣川　俊章	(ISC)²ジャパン
長谷川長一	株式会社ラック
安田　良明	株式会社ラック
板見谷剛史	CompTIA日本支局（コンピュータ技術産業協会）
小川　和博	情報システムコントロール協会（ISACA）
柏浦　謙一	日本ユニシス株式会社
加藤　智之	富士通株式会社
北川　隆一	株式会社アドック
小林　浩史	NTTラーニングシステムズ株式会社
小林　佑光	SEA/J（セキュリティ・エデュケーション・アライアンス・ジャパン）
小梁　康志	リコー・ヒューマン・クリエイツ株式会社
塩見　友規	Information Systems Security Association（ISSA）東京支部
清水　猛	ラックホールディングス株式会社
鈴木　弘之	株式会社富士通ソーシアルサイエンスラボラトリ
関取　嘉浩	ＮＲＩセキュアテクノロジーズ株式会社（SANS事務局）
田中　大介	ＮＲＩセキュアテクノロジーズ株式会社
千葉　寛之	株式会社日立製作所
永島　昌和	日本ベリサイン株式会社
楢原　盛史	シスコシステムズ合同会社
正木　健介	セコムトラストシステムズ株式会社
松村　智恵子	SEA/J（セキュリティ・エデュケーション・アライアンス・ジャパン）
村上　晃	株式会社ラック
森竹　由美子	日本ユニシス株式会社
菱川　尚	日立電子サービス株式会社
やすだなお	特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）

【編集者】広報ワーキンググループ

勝見　勉	株式会社情報経済研究所
高橋　さぎり	特定非営利活動法人日本セキュリティ監査協会（JNSA）
千明　志乃	株式会社ラック
松村　智恵子	SEA/J（セキュリティ・エデュケーション・アライアンス・ジャパン）
与儀　大輔	株式会社ラック
吉村　睦美	CompTIA日本支局（コンピュータ技術産業協会）

ISEPAについて

情報セキュリティ教育事業者連絡会（ISEPA）について

情報セキュリティに対する取組みは、官民を挙げて進められていますが、それを担う人材は、ITやネットワークに関する知識、リスク管理に関する知識、経営管理に関する知識等、多方面の知識と経験を必要とし、一朝一夕には育成が困難です。政府機関における取組みが進み企業における対策が浸透するにつれ、情報セキュリティ人材の供給不足は深刻度を増しています。

また、情報セキュリティ人材に必要な知識・スキルの定義や、経験値を測る基準も明確でないという現状があります。2007年度に政府は「人材育成・資格制度体系化専門委員会報告書」などにおいて情報セキュリティ人材育成の重要性を指摘し、情報セキュリティ政策の重点課題と位置付けました。

これを受けて、情報セキュリティ教育事業者連絡会（Information Security Education Providers Association、略称 ISEPA）は、我が国における情報セキュリティ人材の質の向上と量の拡大を効果的に推進することを目的として、産学官連携により2007年10月1日に発足しました。

情報セキュリティ教育事業者連絡会（ISEPA）では、連絡会各会員団体の運営する資格の位置付け、キャリアパスに対する共通認識の提示、施策提案、さらには各種教育機関との連携によるコンテンツの共同利用など、情報セキュリティ人材育成に関する共通基盤づくり、情報セキュリティ教育機会の柔軟で幅広い提供のための活動を進めています。

セキュアジャパン2009では、「情報セキュリティ人材の育成・確保」が、改めて重点取組み課題として設定されました。これに呼応して、内閣官房情報セキュリティセンター、総務省、経済産業省からもオブザーバー参加を得ている情報セキュリティ教育事業者連絡会（ISEPA）では、業界横断的な人材育成支援体制を整備し、人材育成に関する情報を広く社会に発信するとともに、人材育成の拡大に向けた様々な取組みを推進して行きます。

ISEPAメンバリスト

情報セキュリティ教育事業者連絡会（ISEPA）

【会員団体】

（ISC）^{2} Japan

ISACA（情報システムコントロール協会）東京支部

株式会社インフォセック

NRIセキュアテクノロジーズ株式会社（SANS JAPAN事務局）

エヌ・ティ・ティコムチェオ株式会社

NTTラーニングシステムズ株式会社

株式会社ケーケーシー情報システム

CompTIA日本支局（コンピュータ技術産業協会）

シスコシステムズ合同会社

株式会社シマンテック

SEA/J（セキュリティ・エデュケーション・アライアンス・ジャパン）

財団法人ソフトピアジャパン

日本サード・パーティ株式会社

特定非営利活動法人日本システム監査人協会

特定非営利活動法人日本セキュリティ監査協会（JASA）

財団法人ひょうご情報教育機構（カーネギーメロン大学日本校）

株式会社ラック

リコー・ヒューマン・クリエイツ株式会社　リコー情報セキュリティ研究センター

【オブサーバ】

内閣官房情報セキュリティセンター

総務省情報通信政策局

経済産業省商務情報政策局

独立行政法人情報処理推進機構（IPA）

財団法人インターネット協会（IAjapan）

財団法人日本情報処理開発協会（JIPDEC）

ISSA（Information Systems Security Association）東京支部

【事務局】

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）

情報セキュリティ人財アーキテクチャガイドブック
2009年度版

2009年8月20日　初版発行

開発・制作　情報セキュリティ教育事業者連絡会　スキルワーキンググループ
編　　集　情報セキュリティ教育事業者連絡会　広報ワーキンググループ
発　　行　情報セキュリティ教育事業者連絡会（ISEPA）
発 行 所　特定非営利活動法人　日本ネットワークセキュリティ協会
〒105−0003　東京都港区西新橋1−22−12　JCビル3F
sec@jnsa.org
http://www.jnsa.org