



企業が求める 情報セキュリティ人材について ～JNSAの新たな取り組み～

2012月1月27日

日本ネットワークセキュリティ協会
事務局長 下村正洋

情報セキュリティ人材の種類と分類
情報セキュリティベンダー企業の人材例
情報セキュリティ産業が要求する人材

情報セキュリティ人材とは

情報セキュリティ人材の種類と分類

情報セキュリティ人材アーキテクチャ 職種別・人材育成マップ

職種	定義	ユーザ 企業	ベンダ 企業
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		

上記のマップは情報セキュリティ教育事業者連絡会(ISEPA)が作成した「情報セキュリティ人材アーキテクチャガイドブック2009年度版」より抜粋し、ユーザ企業、ベンダー企業別の分類を加筆。

ISEPAホームページ: <http://www.jnsa.org/isepa/index.html>

資料URL: http://www.jnsa.org/isepa/images/outputs/jinzai_arch_2009.pdf

情報セキュリティ人材の種類と分類

情報セキュリティ人材アーキテクチャ 職種別・人材育成マップ

	職種	定義	ユーザ 企業	ベンダ 企業
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	証拠証拠の分析を行い、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	■	■

上記のマップは情報セキュリティ教育事業者連絡会 (ISEPA) が作成した「情報セキュリティ人材アーキテクチャガイドブック2009年度版」より抜粋し、ユーザ企業、ベンダー企業別の分類を加筆。

ISEPAホームページ: <http://www.jnsa.org/isepa/index.html>

資料URL: http://www.jnsa.org/isepa/images/outputs/jinzai_arch_2009.pdf

情報セキュリティ企業が必要としている人材(例)

職 務	職 務 概 要
設 計	ネットワーク構築における「要件定義」、「提案書作成」、「設計」の局面を担当する
構 築	ネットワーク構築における「構築」、「検証」の局面を担当する
運用設計	顧客ITシステムの運用最適化に主眼をおき、業務分析、ポリシー設計、手順化、運用体制の設計をコンサルティングする
製品企画	顧客ニーズに対応するために、製品及びサービスの市場動向を予測かつ分析し、製品戦略、販売促進計画の企画及び立案を実施する
製品サポート	自社取扱製品に関し、購入見込み客からの導入前の仕様問い合わせや製品導入後の電話、E-Mail等によるトラブル問い合わせに対するヘルプデスク業務を行い、顧客満足度向上に寄与する
品質管理	自社取扱製品に関する評価・検証を担当し、品質向上に関してメーカーとの交渉窓口となり顧客満足度向上に貢献する
運 用	構築及び販売したシステムの安定稼働を目的とした運用方法の提案・変更及び手順に沿ったオペレーション等を行う
オペレーション サービスデスク	構築したシステムおよび顧客の持つ既存システムの監視、手順に沿った業務の実施などを含む運用業務、および障害時の緊急対応、ベンダコントロールを含むマネジメント業務を行う
保 守	主にネットワークインテグレーション案件で構築したシステムについて構築後の電話、E-Mail等による障害対応に関する問い合わせに対するヘルプデスク業務を行う。
営業サポート	案件受注を目的としたセールスプロセスにおいて、技術者の観点から提案活動全般において営業活動を支援する
マネジメント系 セキュリティコンサルタント	顧客の情報セキュリティ管理システムにおいて、フェーズ全体を通じた助言と、リスク分析、文書策定支援、運用支援業務を行う
技術系 セキュリティコンサルタント	顧客の情報セキュリティ管理システムの構築、運用において、システムのセキュリティ対策の実効性の評価や運用の適切性の評価と対策の提示、内部監査の支援等の業務を行う
教 育	担当分野の専門技術・知識と、研修に関する専門技術を活用し、ユーザーのスキル開発要件に合致した研修カリキュラムや研修コースのニーズの分析、設計、開発、運営、評価を実施する
フォレンジック	顧客の情報セキュリティ管理システムにおいて、セキュリティインシデントの発生時の対策の助言と、インシデントの実態把握および証拠保全のためのコンピュータ上の証拠の収集・保全・分析の業務を主として担当する

ある会社の例であり、主な事業はネットワーク製品・セキュリティ製品の販売、ネットワーク構築、セキュリティシステム構築、ネットワーク系システム開発など。開発技術者は除外してある。

職務と一般的な資格などのマッピング(1)

資格・受講	実施機関	設計	構築	運用設計	製品企画	製品サポート	品質管理	運用	オペレーション サービスデスク	保守	営業サポート	マネジメント系 セキュリティコンサル	技術系 セキュリティコンサル	教育	フォレンジック
Microsoft Certified Architect プラットフォーム	Microsoft		○			○		○	○	○					
Microsoft Certified Architect セキュリティ	Microsoft		○			○		○	○	○					
Microsoft Certified Systems Engineer	Microsoft	○	○			○		○	○						
Microsoft Certified Systems A dministrator	Microsoft	○	○			○		○	○						
Cisco Certified Network Professional	Cisco	○	○					○	○	○					
Cisco Certified Network Associate	Cisco	○	○					○	○	○					
Red Hat Certified Engineer	Red Hat	○	○					○	○						
LPIC Level 1	LPI-JAPAN	○	○			○		○	○	○					
Project Management Professional	Project Management Institute	○	○	○								○			
ITパスポート試験	情報処理技術者試験	○	○	○	○	○	○	○	○	○	○	○	○	○	○
基本情報技術者試験	情報処理技術者試験		○	○	○	○	○	○	○	○	○	○	○	○	○
応用情報技術者試験	情報処理技術者試験	○				○		○	○	○					
ネットワークスペシャリスト試験	情報処理技術者試験	○	○	○						○					
サービスマネージャ試験	情報処理技術者試験		○	○											
情報セキュリティスペシャリスト試験	情報処理技術者試験	○	○	○								○	○		○
ITストラテジスト試験	情報処理技術者試験											○			
プロジェクトマネージャ試験	情報処理技術者試験	○	○	○								○			

ITの基礎が必須となっている

職務と一般的な資格などのマッピング(2)

資格・受講	実施機関	設計	構築	運用設計	製品企画	製品サポート	品質管理	運用	オペレーションサービスデスク	保守	営業サポート	マネジメント系セキュリティコンサル	技術系セキュリティコンサル	教育	フォレンジック
システム監査技術者試験	情報処理技術者試験											○	○		
公認不正検査士	ACFE JAPAN														○
公認情報セキュリティ主任監査人	日本セキュリティ監査協会														
公認情報セキュリティ監査人	日本セキュリティ監査協会											○	○		
情報セキュリティ監査人補	日本セキュリティ監査協会											○	○		
情報セキュリティ監査アソシエイト	日本セキュリティ監査協会												○		
公認情報システム監査人	ISACA											○			
Certified Information Systems Security Professional	(ISC)2ジャパン											○	○		
SEA/J 情報セキュリティ技術者認定基礎コース	SEA/J	○	○	○	○	○	○	○	○	○	○	○	○	○	○
SEA/J 情報セキュリティ技術者認定応用テクニカル	SEA/J	○	○	○	○	○	○	○	○	○			○		○
SEA/J 情報セキュリティ技術者認定応用マネジメント	SEA/J	○	○	○				○				○	○		
WildPackets Certified Network Analysis	WildPackets	○	○	○		○		○	○	○					
WildPackets Certified Network Engineer	WildPackets	○	○	○	○	○	○	○	○	○	○			○	
TOEIC					500-800										

情報セキュリティの基礎が必須となっている

情報セキュリティ産業が要求する人材

- 二種類の人材に大別

- A. 情報セキュリティを理解している〇〇〇人材

- 技術系

- プログラマー、システムエンジニア、ネットワーク技術者、運用技術者、品質管理者……

- マネジメント系

- 経営管理者(CIO, CSO…), 経営企画、システム企画、情報システム責任者、コンサルタント……

- B. 情報セキュリティプロフェッショナル

- 技術系

- 良性のハッカー、セキュアプログラミング、解析技術者、セキュリティ運用技術者、フォレンジック技術者……

- マネジメント系

- セキュリティコンサルタント、セキュリティマネジメント評価者、情報セキュリティ監査人

- AとBの両方とも育成が必要

- Aは現IT技術者などの再教育＝情報セキュリティ基礎教育

- 定期的な教育実施などが有効
 - 例えば、社会人教育(学習)の支援

- Bは資質保持者の発見と育成＝情報セキュリティ専門教育

- 大学、高校などアカデミーでの発見と教育が有効
 - 例えば、セキュリティキャンプなどの集中教育やコンテスト

質

不足すると脆弱性が増加

力

不足すると防御力、回復力低下