CompTIA

CompTIA Security CASE STUDY

About CompTIA

CompTIA The IT Industry Trade Association

CompTIA is a gloabal, not-for-profit IT traide associateion and the voice of the industry.

1982 年、様々な IT 規格の標準化を提言するため、IT ベンダーとパートナー企業がオープンな対話を行う場となるべくグローバルな IT 業界団体としてシカゴで設立。
1990 年、IT 業界の活動を反映するべく、名称を CompTIA（ the Computing Technology Industry Association）に変更。欧米を中心とし 10 拠点に拡大し、2001 年 4 月に CompTIA 日本支局を設立。

CompTIA は、 ICT 業界を中心に 2,000 社以上のメンバー企業と、 3,000 以上の学校機関、 教育事業者とパートナーシップを締結し、 数万人を超える IT プロフェショナルのコミュニティを運営しています。

IT 業界団体として、IT ハードウェア / ソフトウェア、サービスを提供する企業や、業界のキーとなる IT プロフェッショナルなどの成功と成長に貢献できるよう、IT に携わる企業や個人の利益を高めるための「教育」、CompTIA 認定資格での「認定」、IT 業界の声を反映し IT 政策に反映するための「政策支援活動」、IT 業界への「社会貢献」の 4 つを柱として活動を続けています。

メンバー

CompTIA は、ワールドワイドで 2,000 社を超えるメンバー企業とパートナーシップを締結しています。

パートナー

ワールドワイドで、3,000 以上の学校機関、 教育事業者とパートナーシップを締結しています。

認定資格

CompTIA 認定資格試験は、ワールドワイドで 165 以上の国と地域で配信され、グローバルスタンダードとして高く認知されています。

About CompTIA Certificaiton

1993 年、IT 環境の変化に伴い、IT を管理する人材の必要性の高まりから、ビジネス環境において利用されている IT ハードウェア / ソフトウェアを理解し、より複雑な IT 環境の管理 / サポート / 運用を行うスキルを評価する CompTIA A+ の提供を開始。その後、時代のニーズに即した人材を効率的に輩出できるように認定資格が開発されています。CompTIA 認定資格は、業界のエキスパートにより開発され、実践力、応用力を評価するベンダーニュートラルの認定資格として、法人を中心にワールドワイドで 200 万人以上に取得されています（2018 年 4 月現在）。

CompTIA 認定資格の IT 業界各社による試験開発プロセスの信頼性と有効性が認められ、米国規格協会（ANSI）により ISO17024 に認定されています。

IT 業務での「実務能力」を評価する唯一の認定資格　ワールドワイドで 200 万人以上が取得

ベンダーニュートラル / テクノロジーニュートラル

CompTIA 認定資格は、ベンダーニュートラル、テクノロジーニュートラルな認定資格です。中立的な立場で、IT スタッフが業務やキャリアにおいて必要とするスキルを提供します。

グローバル

CompTIA 認定資格は、165 以上の国と地域で配信され、グローバルスキルスタンダードとして高く認知されている認定資格です。CompTIA 認定資格を取得することで、日本国内だけではなく、世界中でスキルを証明することを可能にします。

グローバルスキルスタンダード

CompTIA 認定資格は、「業界の業界による業界のための認定資格」です。様々なコミッティが中心となり、ニーズ調査、職務分析やリサーチを経て、SME（サブジェクトマターエキスパート）と呼ばれる現場関係者により開発が進められます。

スコープ

CompTIA は、エントリーレベルの人材からエキスパートの人材まで、様々な IT 業務や時代のニーズに即した人材を効率的に育成することを目的とした認定プログラムを提供しています。

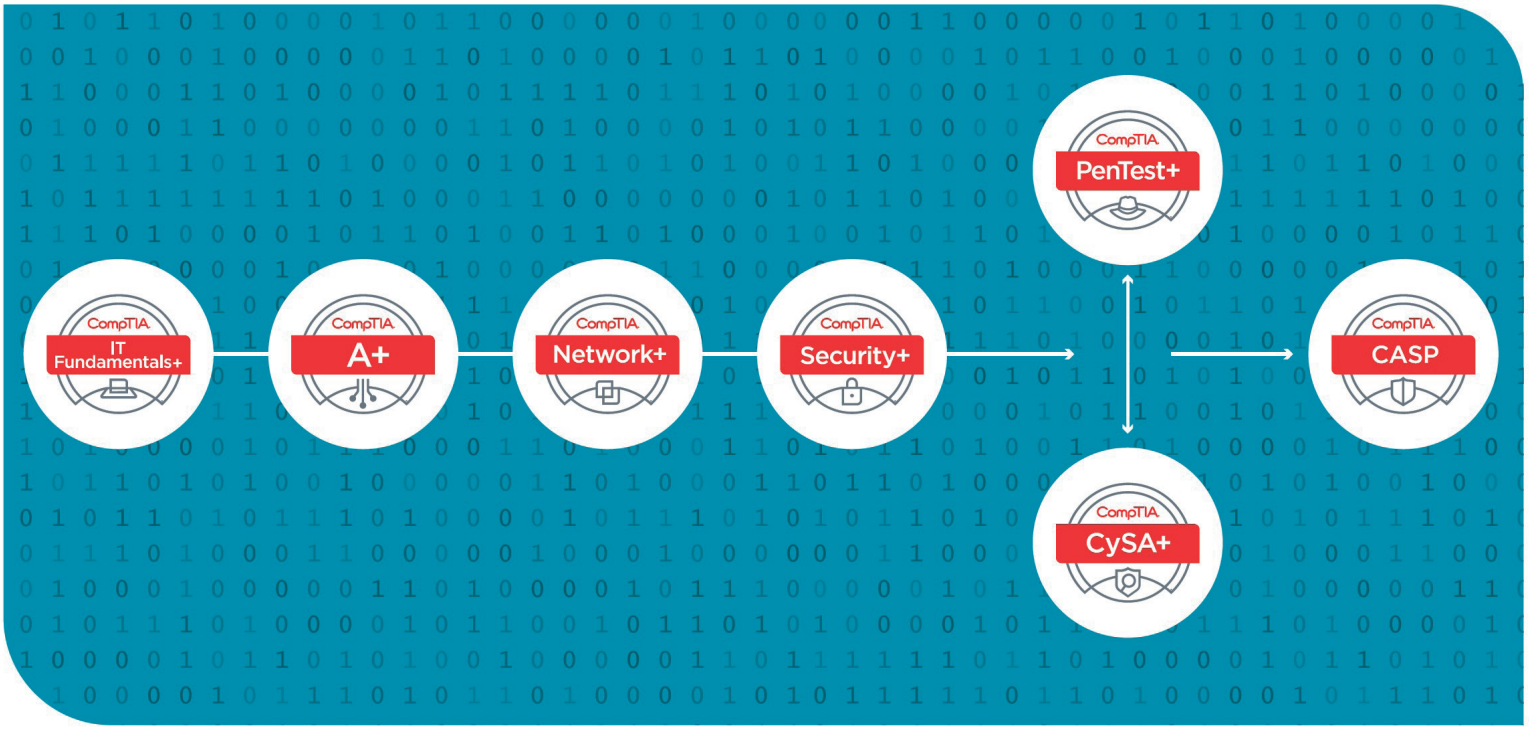
世界的評価

CompTIA 認定資格の IT 業界各社による試験開発プロセスの信頼性と有効性が認められ、米国規格協会（ANSI）により ISO17024 に認定されています。

キャリアパス / ロードマップ

CompTIA 認定資格を取得することにより、他認定ベンダーから提供されている認定資格へのキャリアパスの基盤を作ることができます。また、他ベンダーで提供されている認定資格での実務経験を免除される等のキャリアパスがあります。

CompTIA Cybersecurity Career Pathway



CompTIA IT Fundamentals

CompTIA IT Fundamentals は、PC やスマートフォン、タブレットなどのハードウェアコンポーネントと機能、互換性やネットワーク、セキュリティ、基本的な IT リテラシーに関するスキルを評価する認定資格です。
学生や職種転換などにより IT 業界での就業を希望される方に最適な認定資格です。

- 学生
- 内定者 / 新入社員
- セールスアソシエイト
- マーケティングスペシャリスト
- カスタマーサポート

CompTIA A+

CompTIA A+ は、PC やタブレット、モバイルといったハードウェア、Windows、iOS や Android といった OS やソフトウェア、またプリンターなどの周辺機器に関連したスキルを評価する「ポスト PC 時代」の人材育成に最適な認定資格です。
IT 運用管理業務における、12 ヶ月程度の実務スキルを評価します。

- テクニカルサポート
- フィールドサポートエンジニア
- IT サポートエンジニア
- IT 管理者

CompTIA Network+

CompTIA Network+ は、「ネットワーク技術」に携わる職種において、実務上共通して必須なネットワークの構成、運用、トラブルシューティングなどスキルをはじめ、セキュリティや、ツールを用いたトラブルシューティング、仮想化などのスキルを網羅する認定資格です。
ネットワーク関連業務の 9 ヶ月程度の実務スキルを評価します。

- ネットワークエンジニア
- ネットワーク管理者
- IS コンサルタント
- ネットワークフィールドエンジニア

CompTIA Security+

CompTIA Security+ は、セキュリティに特化したワールドワイドの認定資格です。脅威や脆弱性の分析、セキュリティを考慮したネットワーク設計、リスクマネジメントやアイデンティティ管理などのスキルを網羅する認定資格です。
セキュリティ関連業務の 2 年程度の実務スキルを評価します。

- セキュリティスペシャリスト
- セキュリティコンサルタント
- セキュリティエンジニア
- セキュリティ管理者

CompTIA CySA+

CompTIA CySA+ は、IT セキュリティにおける分析と、セキュリティ全体の改善を実行するために必須となるスキルを評価する認定資格です。企業 / 組織の重要なインフラやデータのセキュリティを維持するために必要となる脅威検出 / 脅威分析のツールを使用、分析、監視するスキルを証明します。
セキュリティ実務者としての 3 ～ 4 年の実務スキルを評価します。

- セキュリティアナリスト
- 脆弱性アナリスト
- サイバーセキュリティスペシャリスト
- セキュリティエンジニア

CompTIA PenTest+

CompTIA PenTest+ は、ネットワーク上の脆弱性を特定、報告、管理するための実践的なペネトレーションテストを行うサイバーセキュリティプロフェッショナル向けの認定資格です。ペネトレーションテストの手法、脆弱性評価、また攻撃があった際のネットワークを回復するために必要となるスキルを評価します。

- ペネトレーションテスター
- ペネトレーションテストアナリスト
- 脆弱性評価アナリスト
- 脆弱性評価マネージャ
- 脆弱性管理エンジニア
- ネットワークセキュリティマネージャ

CompTIA CASP

CompTIA Advanced Security Practitioner（CASP）は、セキュリティ要件、リスク管理、インシデント対応、クリティカルなエンタープライズセキュリティでのスキルを網羅する認定資格です。
IT 全般の管理者として 10 年、そのうちセキュリティ管理者として 5 年以上の実務スキルを評価します。

- サイバーセキュリティプロフェッショナル
- IS プロフェッショナル
- 情報セキュリティアナリスト
- セキュリティアーキテクト

セキュリティの概念、実装、運用管理において
「How to（どのようにすべきか）」を理解し
スキルを身に付ける認定資格

Security+

Protect Your Organization with Security+ Certification

CompTIA Security+ 認定資格を保有する
社員を登用することでビジネスを
セキュリティの脅威から保護できます

価値ある認定資格
米国国防総省は Security+ 認定資格を非常に高く評価し、指令書 8570.01-M により取得を必須と規定しています。

グローバルな認知
CompTIA Security+ は、国際的に認知された資格としての信用があります。現在、世界 147 カ国で Security+ 認定資格を持つプロフェッショナルが活躍しています。

脆弱性の軽減
セキュリティ違反は、収益や生産性の損失につながると同時に、会社の評判を著しく傷つける恐れもあります。Security+ 認定資格を持つ社員を登用することで、セキュリティ脅威を確実に管理できます。

費用対効果：ROI
顧客データが危険にさらされることで、組織にとり、重大な経済的損害が生じる可能性があります。
CompTIA Security+ 認定資格を持つスタッフに投資することで、効率的に企業のリスクを軽減し、ビジネスを安全でコントロールされた状態に保つことができます。

高いスキルを有する社員
採用担当マネージャの 91% が、専門知識 / 技術を確認する上で CompTIA 認定資格が有効であると述べています。Security+ 認定資格では、ネットワークセキュリティ、コンプライアンスと運用セキュリティ、脅威と脆弱性、ホスティングセキュリティ、アクセスコントロールと認証マネジメントに加え、暗号化のスキルが証明されます。[1]

信頼される専門知識 / 技術
Security+ 認定資格を取得することで、組織の IT セキュリティ問題に対する、信頼性の高い情報源の役割を担うことになります。

ロイヤリティの高い社員
認定資格を取得している社員の 84% は、会社を辞めずに働き続けるため、スキルの高い従業員から長期に渡り恩恵を受けることができます。[2]

需要の高い人材
セキュリティ脅威がかつてないほど増大するに伴い、あらゆる IT 専門分野の中でもセキュリティプロフェッショナルやセキュリティ資格を有する IT スタッフのニーズが高まっています。

キャリアの向上
Security+ 認定資格は、セキュリティや IT システム管理分野でより高い報酬が得られるキャリアを目指す上で役立ちます。

より良い給与を得る
Security+ 取得により、知識とスキルを証明し、より高い報酬を得ることができます。一部のセキュリティスペシャリスト、セキュリティアーキテクト、セキュリティエンジニアの年収は 86,000 ドルに上ります。[3]

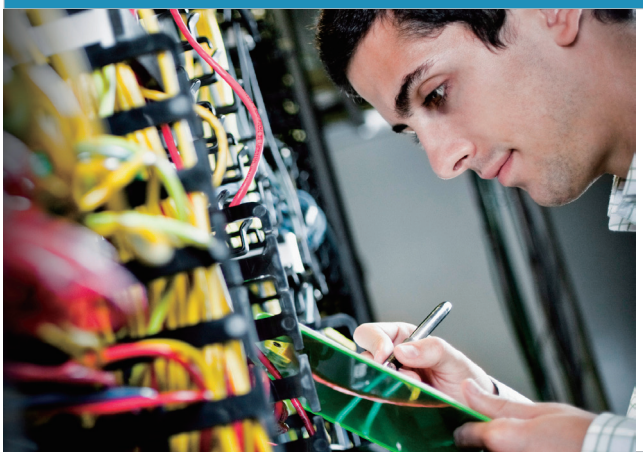
1 出典：CompTIA Employer perceptions of IT Training and Certifi cation
2 出典：CompTIA' s 2nd Annual IT Career Insights Study
3 出典：Bureau of Labor Statistics, Computer and Information Technology Occupations,

" 業界の業界による
業界のための資格"

CompTIA 認定資格は、様々なコミッティが中心となり、ニーズ調査・職務分析・リサーチを経て、SME（サブジェクトマターエキスパート）と呼ばれる現場関係者により開発が進められます。

CompTIA Security+ SME
■海外 / 一部抜粋
- Dept. of Navy
- DoD (Air Force)
- U.S. Army
- US Marine Corp
- State of Minnesota
- IBM
- IBM Managed Security Services
- Cereberus Information Security
- CSRA
- Deloitte & Touché LLP

■日本（50 音順）
- S&J 株式会社
- NRI セキュアテクノロジーズ株式会社
- 日本電気株式会社
- 富士ゼロックス東京株式会社



CompTIA Security+ 取得後は、次のようなキャリアで活躍できます

- セキュリティアーキテクト
- セキュリティエンジニア / セキュリティ管理者
- セキュリティコンサルタント
- 情報保証に携わる技術者

様々なグローバル企業では、自社の社員の育成に CompTIA Security+ を必須 / 推奨資格として活用されています

CompTIA Security+ は、国際的に広く認知されている規格である ISO/ANSI 17024 を取得しており、世界中の多くの企業や学校で活用をいただいています。最も顕著な例としては、米国国防総省の情報保証に関連する全ての人材に対し、CompTIA Security+ は必須資格として活用されています。

CompTIA Security+ 活用事例：米国国防総省での活用事例
米国国防総省（The U.S. Department of Defense: DoD）は、効果的に DoD の情報、情報システム、情報インフラを守るため、十分に訓練され資格を取得した、マネージャ、テクニシャン、コントラクタ、そして、特権的アクセスをもつユーザーなどすべての情報保証を必要とする人材に対し、「DoD Directive 8570.1M（米国国米総省指令 8570.1M ）」を要求しています。
国家の安全に重要な仕事である DoD に携わる全員の知識とスキルが高い水準のレベルであることを保証するため、DoD では、CompTIA A+、Network+、Security+、CompTIA CySA+、CASP を含む資格取得を必須としています

主な出題範囲

CompTIA Security+ 認定資格試験では、アプリケーション、ネットワーク、デバイスのセキュリティを確保するために必要な知識とスキルを証明します。認証管理やアクセス管理の手法といった企業におけるセキュアな環境維持、物理セキュリティコントロール、災害復旧や事業継続といったリスク管理、またフォレンジックのコンセプト、クラウドや組み込みシステムにおけるセキュリティコンセプトや、セキュリティの基本となるネットワークセキュリティのコンセプトなどセキュリティを管理・運用していく上で必須となるスキルが網羅されています。
CompTIA Security+ 認定資格試験には、多肢選択式の問題とパフォーマンスベースの問題の両方が含まれます。

CompTIA Security+（試験番号：SY0-501）	
第 1 章　脅威、攻撃、脆弱性	21%
第 2 章　テクノロジーとツール	22%
第 3 章　アーキテクチャと設計	15%
第 4 章　アイデンティティとアクセス管理	16%
第 5 章　リスク管理	14%
第 6 章　暗号化と PKI	12%

試験実施概要

試験番号	問題数	制限時間	合格ライン
SY0-501	最大で 90 問	90 分	100 ～ 900 のスコア形式 750 以上

認定資格の詳細情報は、下記 Web サイトをご覧ください：

http://www.comptia.jp/cont_certif_securityplus_sy0-501.html

Strengthen your organization's ablity to combat malware and threats with behavioral analytics.

CompTIA CySA+

CompTIA Cybersecurity Analyst（CySA+）を取得することで、組織の重要なインフラやデータのセキュリティを維持するために必要となる脅威検出 / 脅威分析のツールを使用、分析、監視するスキルが習得できます

CompTIA CySA+ とは
CompTIA CySA+ は、ワールドワイドで提供されているベンダーニュートラルな認定資格です。
CompTIA CySA+ を取得することで、企業 / 組織のアプリケーション、システム、データーのセキュリティを維持するために使用される脅威検出ツールの構成や実行、またこれらから得られるデータ分析をするためのスキルと知識を習得していることを証明します。

分析によるアプローチが必要な理由
ある調査によると、データー漏洩の際に必要とされる平均コストは 400 万 US ドルとなっており、これらのデータ漏洩の原因の 48% は、悪意のある攻撃、もしくは犯罪行為によるものと報告されています。
攻撃者が、ファイアーウォールなどの従来のシグネチャベースのソリューションをうまく回避する傾向にあるため、分析によるアプローチが非常に重要となっています。ネットワークを攻撃する脅威を緩和するために、一般的なネットワーク監視ツールからレポートされる False Positive（フォールス・ポジティブ）False Negative（フォールス・ネガティブ）の差異を明らかにし、対策をとるために集中的かつ、スキルを持った人材による分析アプローチが必要です。

CompTIA CySA+ が必要な理由
急増しているより悪質で巧妙な脅威から、企業がセキュリティを維持するためには、データの分析方法、コンテキストへの組み込み方法、また企業のセキュリティ戦略の構築方法を熟知した洞察力を持つ IT スタッフが必要となります。

CompTIA CySA+ 認定資格試験では、綿密なシナリオとパフォーマンスベースの設問により、受験者がアウトプットされたデータを慎重、かつ
警戒心を持って分析できるスキルを習得することができるように設計されています。

CompTIA CySA+ が推奨される人材
CompTIA CySA+ は、セキュリティ全体の状況を改善するための行動分析を実施しようと検討をしている企業 / 組織向けの認定資格です。
CompTIA CySA+ の取得を採用の際の条件とすることで、サイバーセキュリティに関連するオペレーションに適切な人材を雇用することにつながります。

" 業界の業界による
業界のための資格”

CompTIA 認定資格は、様々なコミッティが中心となり、ニーズ調査・職務分析・リサーチを経て、SME（サブジェクトマターエキスパート）と呼ばれる現場関係者により開発が進められます。

CompTIA CySA+ SME
■海外 / 一部抜粋
- ASICS
- Department of Defense
- Department of Treasury
- US Department of Veterans Affairs
- US Navy
- Deloitte and Touche LLC
- Federal Reserve Bank of Chicago
- Amazon (AWS)
- Ricoh USA
- Linux Professional Institute
- University of Phoenix
- Target
- Secure-24 LLC
- Northrop Grumman
- Washington State Patrol
- Boulder Community Health
- Western Governors University
- BlacKnight CyberSecurity International

■日本（50 音順）
- 株式会社アシックス
- S & J 株式会社
- NRI セキュアテクノロジーズ株式会社

CompTIA CySA+ 取得後は、次のようなキャリアで活躍できます

- IT セキュリティアナリスト
- セキュリティオペレーションセンター（SOC）アナリスト
- 脆弱性アナリスト
- サイバーセキュリティスペシャリスト
- 脅威インテリジェンスアナリスト
- セキュリティエンジニア

CompTIA CySA+ は、IT セキュリティアナリストのスキル、また、サイバーセキュリティにより精通したスキルを習得するための IT プロフェッショナル向けのベンターニュートラルな認定資格です。

CompTIA CySA+ は、CompTIA Security+ と CompTIA Advanced Security Practitioner（CASP）の中間に位置付けられ、より高度なセキュリティスキルを育成するためのキャリアパスの役割を果たします。これら 3 つの CompTIA 認定資格を取得することで、セキュリティに関連する実務スキルのキャリアが育成されます。

CompTIA 継続教育プログラム（CE プログラム）の一環で、CompTIA CySA+ は、取得から 3 年間の有効期限が設定されており、承認された更新オプションを実行することで認定資格の更新ができます。CompTIA CySA+ には、多肢選択式の問題とパフォーマンスベースの問題の両方が含まれます。必須ではありませんが、この認定資格の受験者は、CompTIA Security+ またはそれに相応する技術的、実務的スキルを所有していることが望ましい条件とされています。

CompTIA CySA+ 認定資格を取得することで、以下のスキルの習得が可能です。

- オープンソース検出ツールの設定と実行することができる
- データ分析の実行することができる
- 脆弱性、脅威、リスク分析の結果から、組織 / 企業、またはアプリケーション / システムのセキュリティを維持するという目的のために有効な手段を実行することができる

主な出題範囲

CompTIA CySA+（試験番号：CS0-001）	
第 1 章　脅威の管理	27%
第 2 章　脆弱性の管理	26%
第 3 章　サイバーインシデントの対応	23%
第 4 章　セキュリティ設定とツールの設定	24%

試験実施概要

試験番号	問題数	制限時間	合格ライン
CS0-001	最大で 85 問	165 分	100 ～ 900 のスコア形式 750 以上

認定資格の詳細情報は、下記 Web サイトをご覧ください：

http://www.comptia.jp/cont_certif_csaplus_cso-001.html

Government Case Study

米国国防総省での情報保証の役割を担う人材に必須とされる CompTIA 認定資格

米国国防総省（The U.S. Department of Defense: DoD）は、効果的に DoD の情報、情報システム、情報インフラを守るため、十分なスキルを持ち資格を取得した、マネージャ、エンジニア、コントラクタ、そして、特権的アクセスをもつユーザーなどすべての情報保証を必要とする人材に対し、「DoD Directive 8570.1M（米国国米総省指令 8570.1M ）」への準拠を要求しています。
国家の安全に重要な仕事である DoD に携わる全員の知識とスキルが高い水準のレベルであることを保証するため、DoD では、CompTIA A+、Network+、Security+、CSA+、CASP を含む認定資格の取得を必須としています。

米国国防機関の IT 責任者によれば、インシデントの識別および解決、伝達、データ漏えいの防止などにおける職員のスキルが、民間により提供されている IT 認定資格によって向上したといいます。

■情報保証（IA）の認定資格を有する人員は、インシデントとその影響に関する正確な状況を認識する能力が高い。（JITC、BD09）

■認定資格によって共通言語が確立されるため、CND/SP（コンピュータネットワーク防御 / サービスプロバイダ）とヘルプデスクとの間でコミュニケーションが円滑になり、早い段階で問題解決が可能になる。（Agency CISO）

■認定資格は、試験に合格しなかった者まで含めて全員のパフォーマンスを向上させる。（EUCOM 調査）

■軍関係でサイバー人材に対し、トレーニングと認定を行うと離職率が下がる。（INSCOM NCO）

■認定資格の取得者が多くなるほど、データ漏えいの発生件数が少なくなる。（EUCOM 調査）

■ 認定資格が全体像としてのビジョンを伴っていれば（Navy Carrier IAM）、職務に関連するモラルトレーニングが向上する。

FISSEAAnnual Conference における米国国防総省の Defense Information Assurance Program（DIAP） 責 任 者 George Bieber 氏が行ったプレゼンテーション『Certification in DoD』より抜粋（2011 年 3 月）

CompTIA A+ は、IT 技術者の基本スキルを評価するワールドワイドで活用されている認定資格です。267 ヵ国、100 万人以上に取得されています。
「ポスト PC」環境のハードウェア / ソフトウェアのスキルが網羅されています。

CompTIA Network+ は、ネットワークの設計・構築、管理・運用に必須とされるスキルを網羅した認定資格です。最新の改訂では、セキュリティの出題がさらに強化されています。

CompTIA Security+ は、セキュリティ概念、脅威や脆弱性、ツール、対応手順に関連するスキルや、セキュリティインシデントの発生を予防するため定期的に実施されるべき運用手順などのスキルを評価する認定資格です。

CompTIA CySA+ は、組織の重要なインフラやデータのセキュリティを維持するために必要となる脅威検出 / 脅威分析のツールを使用、アウトプットの分析、監視するスキルを評価する認定資格です。

CASP（CompTIA Advanced Security Practitioner）は、より高度な IT セキュリティスキルのニーズに応え開発されました。複雑化するセキュリティインシデントに対応できるように、俯瞰的に思考し、明確なセキュリティソリューションを実装できるスキルを育成する認定資格です。

Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security Network+ CE SSCP	CCNA Security CySA+ GICSP GSEC Security+ CE SSCP	CASP CE CCNP Security CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CASP CE CISM CISSP (or Associate) GSLC	CISM CISSP (or Associate) GSLC
IASAE I	**IASAE II**	**IASAE III**
CASP CE CISSP (or Associate) CSSLP	CASP CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CySA+ GCIA GCIH GICSP SCYBER	CEH CySA+ GICSP SSCP	CEH CFR CySA+ GCFA GCIH SCYBER
CSSP Auditor	**CSSP Manager**	
CEH CySA+ CISA GSNA	CISM CISSP-ISSMP	

Business Case Study

ますます需要が高まるセキュリティ人材の育成に CompTIA 認定資格を活用

ネットワークセキュリティやリスク管理の基本原則を網羅する CompTIA Security+ をベースに、確かな人材育成を目指す

SoftBank

取得対象者	部門のセキュリティ担当者 システムのセキュリティ管理者

取り組みの背景

ICT の進歩に伴い、近年増加しているセキュリティリスク。国内大手の通信キャリアであるソフトバンク株式会社においては、ネットワークインフラを担う企業として、リスクに確実に対応できるセキュリティ人材の育成に取り組んでいる。

しかし、セキュリティ全般に対する知識不足が課題に・・・

- 各部門から選出しているセキュリティ担当者は、セキュリティ全般の知識を有しておらず、部門のセキュリティを仕切る立場として不安がある
- 各システムのセキュリティ管理者においても 特定の分野には詳しいものの総合的なセキュリティ知識は不足していた

CompTIA Security+ 認定資格を導入

CompTIA Security+

CompTIA Security+ は、セキュリティ概念、脅威や脆弱性、ツール、対応手順に関連するスキルや、セキュリティインシデントの発生を予防するため定期的に実施されるべき運用手順等のスキルを評価する認定資格。

CompTIA Security+（試験番号：SY0-501）	
第 1 章　脅威、攻撃、脆弱性	21%
第 2 章　テクノロジーとツール	22%
第 3 章　アーキテクチャと設計	15%
第 4 章　アイデンティティとアクセス管理	16%
第 5 章　リスク管理	14%
第 6 章　暗号化と PKI	12%

取り組み

2020 年までに有取得者 400 名を目標とした育成
Security+ は、Level 1 において導入されている

Level 1: セキュリティ担当者 … Security+
Level 2: セキュリティ専任者 … CISSP
Level 3: セキュリティ専門家 … GIAC

Security+ 導入の理由
■ セキュリティ全般を学べる入門的な資格
■ ベンダーニュートラル
■ グローバルに通用する資格 *

*Security+ 認定資格を有するプロフェッショナルは、世界 147 カ国以上で活躍している。
また、米国国防総省では、Security+ 認定資格を評価し指令書 8570.01-M および 8140 により、取得必須を規定している。

「ネットワークインフラを担う企業として、弊社もセキュリティ人材の育成に力を入れています。しかし、セキュリティ分野は幅広いためどこから知識を身につけるべきか判断しづらいという課題がありました。

セキュリティ全般をカバーできる内容である CompTIA Security+ は、取っ掛かりとして最適であり、まずは基礎知識を習得させたいという目的と合致しました。」

テクノロジーユニット
ネットワーク統括
サービスプラットフォーム開発本部
本部長　　折原　大樹 様

ソフトバンク株式会社
東京都港区東新橋 1-9-1
http://www.softbank.jp/

「セキュリティ全般の知識を身につけるため、Security+ が有効と考えます。」

テクノロジーユニット
ネットワーク統括
サービスプラットフォーム開発本部
本部長　　折原　大樹 様

導入の CompTIA 認定資格
■ CompTIA Security+

Business Case Study

グローバルクラウド案件に対応できる人材強化のため CompTIA 認定資格をスキル基盤として活用

クラウド環境に対応できる広範なテクニカルスキルと、グローバルクラウド案件をマネジメントできる能力を総合的に強化

取得対象者	グローバルクラウド案件の対応を担う プロジェクトマネージャ (PM) およびシステムエンジニア (SE)

NTT コミュニケーションズ株式会社
東京都千代田区内幸町 1 丁目 1 番 6 号
http://www.ntt.com/

「グローバルクラウド案件対応に必要な総合的スキルを習得するため、CompTIA 認定資格が有効と考えます。」

ソリューションサービス部
企画部門　人事・人材育成担当

導入の CompTIA 認定資格
- ■ CompTIA Cloud Essentials
- ■ CompTIA Cloud+
- ■ CompTIA Project+
- ■ CompTIA Security+
- ■ CompTIA CySA+

取り組みの背景

NTT コミュニケーションズ株式会社では、早期より、クラウドによる経営環境の変化に対応したサービスを展開。グローバルネットワークと直結した通信事業者ならではのサービスを展開することで、法人のお客さまの ICT 環境を最適化し、経営改革に貢献しています。
人材育成の観点では、従来の「PM 能力」・「SE 能力」に加え、「グローバルクラウド案件対応能力」の強化が必要となっています。

グローバルクラウド案件に対応しうる人材とは？

- お客さま要件を理解し、カスタマイズ / 最適化できる能力
- 文化 / 商習慣 / 業務プロセス / 品質管理手法等の違いを理解し、海外ベンダーや海外現地法人と協業して、プロジェクトをコントロールし完遂できるマネジメントスキル
- インフラ～アプリケーションに至る幅広い ICT テクニカルスキル、P2V/V2V のマイグレーションスキル / ノウハウ

CompTIA 認定資格を導入　「グローバルで通用する認定資格を！」

CompTIA Cloud Essentials は、ビジネス、技術的側面から見たクラウドコンピューティングの意義や導入によるメリット / デメリットを判断し運用できる知識とスキルを証明する認定資格

CompTIA Security+ は、セキュリティ概念、脅威や脆弱性、ツール、対応手順に関連するスキル、インシデントの発生を予防するため定期的に実施されるべき運用手順等のスキルを評価する認定資格

CompTIA Cloud+ は、クラウドの運用やサービスの提供など、クラウド環境で業務を実行する IT エンジニアが必要とされるスキルとベストプラクティスへの理解を評価する認定資格

CompTIA CySA+ は、IT セキュリティアナリスト、脆弱性アナリスト、脅威インテリジェンスアナリストを対象に開発され、脆弱性、脅威、リスクを特定し対策を講じるといったスキルと知識を評価する中級レベルの認定資格

CompTIA Project+ は、業界を問わずプロジェクトマネジメントに必要な標準知識とベストプラクティスに基づく実務能力を評価する認定資格

取り組み

■ **Off-JT の一つとして活用**
- STEP1: グローバルクラウド案件対応に必要なスキル定義 (「スキルチェックシート」)
- STEP2: チェックシートを用いた個人別スキル棚卸 / 現状把握、強化分野 / 育成計画の立案
- STEP3: 育成計画に基づくスキルアップ施策の実行 (各種研修・資格取得・勉強会への参加 等)
- STEP4: 実案件への応用、ノウハウ蓄積 / 展開

■ **STEP3 の施策例**
- CompTIA 認定資格の早期取得に向けた教材配布 / 受験料支援、取得者によるノウハウ / 事例共有
- ICT テクニカル研修派遣 (NW/ サーバ / ストレージ / 仮想化技術 / セキュリティ 等)
- グローバル PM 育成特設研修　　等

「求められているクラウド人材とは、NW/ サーバ等の ICT のレイヤや商習慣といった壁を越えて「シームレス」に対応できる人材です。
それには、クラウド基盤に関する幅広いテクニカル知識 / スキルに加え、オンプレミスからクラウドサービスへのマイグレーションの手法やノウハウ、また、海外現地法人や海外ローカルベンダー等と協業しプロジェクトを完遂できるプロジェクトマネジメントスキルも備えている必要があります。

そうしたクラウドの総合的スキルを習得するため、グローバルに展開される CompTIA 認定資格、プログラムが最適であると判断し、導入しました。
CompTIA 認定資格プログラムは、2013 年度より導入しており、2014 年度も数多くの取得者を輩出しています。2015 年度以降もさらに拡大していく方針です。クラウド人材の育成、若手社員の早期戦力化を実現する上でも有効と捉えています。」

ソリューションサービス部
第一プロジェクトマネジメント部門
担当部長　井村　宏之 様

Business Case Study

東京 2020 オリンピック・パラリンピックに向けて、さらなる貢献には、情報セキュリティ人材の育成が必須に

情報通信技術やクラウド環境を取り巻くインシデントに対応できるセキュリティチームメンバーの育成と CSIRT 業務の必須知識としてグローバル資格を採用

取得対象者	グローバル基盤チーム、セキュリティチーム ASICS-CSIRT スタッフ

取り組みの背景

アシックスグループは、スポーツによる青少年の育成を通じて、社会の発展に貢献したいという思いから始まりました。

私たちはその創業の精神を受け継ぎ、60 年以上にわたり、社会環境の変化を捉えながら、独自の製品とサービスを提供し、今日では、フットウエアとアパレル事業を中心に 50 以上の国と地域に拠点を置くまでに成長しました。東京 2020 オリンピック・パラリンピックに向けて、国内のアスリートならびにユーザーへ、スポーツ事業を通じ、よりさらなる貢献を目指します。

ASICS-CSIRT (ASICS Computer Security Incident Response Team) 設立の経緯
2015 年、情報セキュリティ委員会ならびに情報セキュリティ事務局が発足。運用フェーズに入った際、海外オフィスにおいて、緊急性の高いインシデントが発生しました。

現行のスタンダード文書においては、インシデント対応手順とフローは明記されているものの、情報セキュリティ委員会や情報セキュリティ事務局による運用体制では、国内外地域をカバーしつつ、迅速かつ的確なインシデント対応が難しいといった課題がありました。

この機会をふまえつつ、他社チームとの有事の際の情報交換や、インシデント対応時のホットラインと POC (Point of Contact) の設置の必要性　から、インシデントレスポンスチームが結成されました。

CompTIA Security+ 認定資格を導入

CompTIA Security+ は、セキュリティ概念、脅威や脆弱性、ツール、対応手順に関連するスキルや、セキュリティインシデントの発生を予防するため定期的に実施されるべき運用手順等のスキルを評価する認定資格。

取り組み

CompTIA Security+ で得られたスキル知識は、次の領域で活かされています

ASICS-CSIRT における取り組み

1. 事後対応サービス
   (1) インシデントハンドリング：重大度 (緊急・警告・注意・情報) の切り分けとリスクの優先付け
   (2) インシデントレスポンス：国内チームとの情報交換、関係機関 (地元警察) との連携・報告・調整
   (3) 脆弱性管理：当社サーバ・PC に対する脆弱性診断やハッキング手法を用いたセキュリティ監査

2. 事前対応サービス
   (1) アナウンスメント：脅威レポートを元にサイバー攻撃時における警告・注意喚起の実施
   (2) 注意喚起と警告・通知：OSINT 情報を元に、サイバー攻撃に関する情報を収集し、組織内にて共有
   (3) 技術監視 (モニタリング)：監視対象の通信、不正侵入行為、関連する挙動のモニタリングの実施

3. インシデント管理サービス
   (1) リスクマネジメント：当社の情報資産に対するリスク分析やアセスメント (影響度評価) を実施
   (2) サイバーセキュリティ意識向上：情報セキュリティに対する意識向上トレーニングの実施
   (3) セキュリティ監査 (アセスメント)：当社サービス対象に対するペネトレーションテストの実施

「2016 年に社内の情報セキュリティ向上の活動に携わるようになり、それまでと違ってネットワーク・サーバ・運用など総合的にとらえて見る必要があると感じるようになりました。CompTIA の試験はそうした観点で知識を整理出来る非常に適したものであったと感じています。」

IT 統括部 セキュリティチーム　村上 様

「昨年、主担当であったサーバ管理から、セキュリティの運用に業務が移りました。社内セキュリティ強化を推進するためにもまずは基礎知識の習得から、そのきっかけとして今回の認定試験を受けました。今後はより高度なセキュリティ分野の理解を深められるよう CompTIA 認定資格を活用していきます。」

IT 統括部 セキュリティチーム　恒藤 様

「CompTIA Security+ の試験準備を通じ、情報セキュリティの基礎知識を築くことができ、より私の仕事を理解するのにも役立ちました。」

IT 統括部 グローバル基盤チーム　リー 様

株式会社アシックス
神戸市中央区港島中町 7 丁目 1 番 1
www.asics.com

「アシックスは、
東京 2020 オリンピック・
パラリンピック
ゴールドパートナー
（スポーツ用品）です。

当社の将来を見据え、
情報セキュリティ人材の育成
に必要なグローバル資格を
採用しました。

また、インシデントに柔軟に
対応できる CSIRT 人材の育成
には、グローバルに通用する
CompTIA は、適切と考えて
ています。」

IT 統括部
グローバル基盤チーム
セキュリティリード
CompTIA Cybersecurity
Analyst (CSA+) SME
谷本　重和 様

導入の CompTIA 認定資格
■ CompTIA Security+

Business Case Study

「常駐型セキュリティマネジメントサービス」を支える人材の育成に CompTIA Security+/CySA+ を活用

人材育成を視える化し、お客様にセキュリティサービスのクオリティを伝える

取得対象者	お客様の IT インフラ運用業務を担当しているメンバー

取り組みの背景

「情報セキュリティ分野の人材不足」はグローバルな共通課題
経済産業省の調査では、情報セキュリティ分野で不足する人材が、2020 年に 19 万人を超えることが示されています。SCSK 株式会社では、テクノロジーの急速な変化や、それに伴うセキュリティ脅威に適切に対応できる人材の教育や確保が急務となっていると考えます。

企業におけるセキュリティ人材不足の解決策「常駐型セキュリティマネジメントサービス」を提供
さまざまな脅威が顕在化した現在において、IT システムを安全に運用する為には、セキュリティのスキルを持った人材が必須です。同社の「常駐型セキュリティマネジメントサービス」では、SCSK 独自のセキュリティ教育を受けたセキュリティエンジニアと経験豊富なセキュリティアナリストが連携してお客様のシステムの安全な運用に取り組みます。

ログの取得や情報資産の管理など、現場でしか対応できない業務を常駐したセキュリティエンジニアが担当し、セキュリティインシデントの分析など、経験やノウハウが求められる部分は経験豊富なセキュリティアナリストが遠隔でサポートします。

社内でのセキュリティ人材育成の推進
「常駐型セキュリティマネジメントサービス」を支えるための人材育成に、CompTIA 認定資格を活用しています。

CompTIA Security+/CompTIA CySA+ 認定資格を導入

CompTIA Security+ は、セキュリティ概念、脅威や脆弱性、ツール、対応手順に関連するスキルや、セキュリティインシデントの発生を予防するため、定期的に実施されるべき運用手順など、スキルを評価する認定資格です。

CompTIA CySA+ は、IT セキュリティアナリスト、脆弱性アナリスト、脅威インテリジェンスアナリストを対象に開発され、脆弱性、脅威、リスクを特定し対策を講じるといったスキルと知識を評価する中級レベルの認定資格です。

取り組み

SCSK 株式会社は、セキュリティに特に留意し、セキュリティを保ったシステム運用を支える人材を育てるために、組織的に取り組んでいます。輩出した人材は、お客様施設に常駐してシステム運用におけるセキュリティを支える役割を果たすほか、同社のデータセンターにおいて高度なセキュリティを支える人材としても活躍します。

■ 人材モデルの定義
- セキュリティ運用を支えるために必要な機能や役割を整理し、人材モデルを作成
  人材モデルは、職務の内容や職責に応じ、また、キャリアアップを考慮して、複数のレベルを設定

■ セキュリティに必要なスキル・知識の整理、シラバスの作成
- IPA の「i コンピテンシ ディクショナリ（iCD）」などを参考に、それぞれの人材モデルに求められるスキルや知識を整理した知識体系表を作成
- 知識体系表をもとに、レベル毎に学ぶべき事項を整理したシラバスを作成

■ 教育・研修プログラムの検討と実施
- シラバスに沿って効果的に学習を進めるため、研修プログラムや教材を準備
  試行運用と位置づけた初年度は社外の研修コースを積極的に採用。2 年目からは、社外の研修コースに加えて、自社及び自社のお客様の状況を強く意識した独自の研修コースを開発して採用
- 習得した知識やスキルの状況を測定するための指標として、社内の認定試験に加えて公的資格を採用基礎的なセキュリティ知識習得の確認に CompTIA Security+ を、セキュリティインシデントの対処にかかわる知識の確認に CompTIA CySA+ を活用

「システム運用を支える者が知っておくべきセキュリティ技術の範囲はとても広く、これらを効率的に学ぶことは容易ではありません。また、その学習の状況を正しく把握することも簡単ではありませんでした。CompTIA Security+ の試験範囲は、セキュリティに携わる者が知っておくべき事項の大半をカバーしており、初期の学習者の育成の目的において、とても有益だと思います。　また、CompTIA の試験は、受験場所と受験時間についての選択肢が広く、受験者の負担（お客様施設常駐者の場合はお客様企業の負担にも関係）が少ないことも大きな利点となりました。」

ＩＴマネジメント事業部門
基盤インテグレーション事業本部　セキュリティサービス部
佐藤　直之 様

SCSK 株式会社
東京都江東区豊洲 3-2-20
www.scsk.jp/

「セセキュリティ人材不足が叫ばれる中で、従来からあるインフラ運用業務だけでなく、インシデントハンドリングなど、セキュリティ関係業務もお客様にご提供できるよう人材の底上げを検討し、SCSK 独自の教育プログラムを作成しました。CompTIA Security+ は、最低限抑えておくべき知識が網羅されており、最初に取得すべき必須科目と位置づけました。」

ＩＴマネジメント事業部門
基盤インテグレーション事業本部
セキュリティサービス部
佐藤　直之 様

導入の CompTIA 認定資格
■ CompTIA Security+
■ CompTIA CySA+

Business Case Study

役務領域拡大に向けたセキュリティ / プロマネスキルの強化に、CompTIA 認定資格を活用

新たな分野のチャレンジや、ステッピングストーンを設定することで着実なスキルアップを支援。社員モチベーションの継続的向上に

Fujitsu Marketing Limited

株式会社富士通マーケティング
東京都港区港南 2-15-3
品川インターシティ C 棟
www.fujitsu.com/jp/group/fjm

「 CompTIA 認定資格は、
ゴールを目指す上で 欠かせないステッピングストーンの
一つです。」

FSB 本部 フィールド支援統括部
品質技術部
担当課長　小柴　寿一 様

導入の CompTIA 認定資格
■ CompTIA Security+
■ CompTIA Project+

取得対象者	フィールドサービスビジネス本部　部員

取り組みの背景

カスタマエンジニア（CE）の人材像
ハードウェア、ソフトウェア、施設に関連する専門技術を活用し、お客様の設備に合致した設計・開発を行うことで、インフラ設備の安定稼動をサポート。設計したインフラ環境の品質に責任を持つ。

昨今の CE の役務拡大への対応
セキュリティ / プロジェクトマネジメントスキルの強化
- セキュリティに特化した部隊の形成　→　セキュリティ対策スキルの修得、提案 / 運用スキルの向上
- 保守を展開するリーダーの養成　→　プロジェクトマネジメントスキルの向上 / 実業務への応用

関連する新たなスキル獲得の支援を行うことで、ビジネスチャンスの拡大を狙う。さらに部員のスキルアップのための強力支援を実施。部員のモチベーション向上につながると同時に、事業目的達成に向けたメッセージとなる。

CompTIA Security+/CompTIA Project+ 認定資格を導入

CompTIA Security+ は、セキュリティ概念、脅威や脆弱性、ツール、対応手順に関連するスキルや、セキュリティインシデントの発生を予防するため定期的に実施されるべき運用手順等のスキルを評価する認定資格。

CompTIA Project+ は、小規模から中規模プロジェクトを遂行する際の知識を体系的に学習することができ、業界を問わずプロジェクトマネジメントに必要な標準知識とベストプラクティスに基づく実務能力を評価する認定資格。

取り組み

年間 1 人 1 資格取得の方針に絡めた取り組み
「IT スキルの向上、目にみえる成果」として、各種資格取得の実施
→　期初に自身の資格取得計画を作成し、上長との面談を経て、KPI として設定。進捗状況も確認。

《セキュリティ推奨スキルパス》
Microsoft MTA → **CompTIA Security+** → 情報セキュリティスペシャリスト

《プロジェクトマネジメント推奨スキルパス》
ITIL Foundation → **CompTIA Project+** → PMI PMP → プロジェクトマネージャ

【今後について】
トレーニング経緯、取得状況から、部署毎の弱みを把握することで、強化ポイントを明確化。
自身の希望による資格取得から、組織の戦略的な育成手段としての資格取得へシフト。

「CompTIA 認定資格は、弊社の人材育成フレームワークレベル別育成において、中級レベルの資格取得目標となっております。レベル毎に経験・研修・資格を定義し、スキルの見える化を行うことにより、部員の成長におけるモチベーション向上にも役立っております。
また 以前は A +、Network +の資格取得を推進していたこともあり、CompTIA 資格が各分野の知識を全般的に網羅している為、資格取得後の実務における展開にも有効となっております。」

フィールドサービスビジネス本部
フィールド支援統括部
品質技術部
担当課長　　小柴　寿一 様

Business Case Study

お客様に感動を与える安心と信頼のパートナーを目指し全国に展開する PFU の保守・運用サービス

進化し続ける ICT 業界において、お客様の要望に柔軟に対応できるエンジニア育成に CompTIA 認定資格を活用しています。

取得対象者	カスタマサービス部門の カスタマエンジニア（CE）、インフラ SE、サービス営業、 コールセンター、SOC

取り組みの背景

■急速に拡大する情報セキュリティ分野への対応
国内において、10 秒に一人の割合で被害に遭っていると言われているサイバー攻撃。
PFU では複雑化する多様なセキュリティ脅威に対し、トレンドやレベルに応じたセキュリティインシデントに対応できるエンジニアとアナリストの育成が必要。

■マルチベンダー保守、運用サービスに対する人材育成とスキルパス
業界でいち早く取り組んできたマルチベンダー保守。
お客様へ安心・安全なサービスを継続的に提供するため、ベーススキルを継続的に習得する仕組みとエンジニアのキャリアアップを目的としたスキル体系の明文化。

CompTIA 認定資格の活用

CompTIA Security+ は、セキュリティ概念、脅威や脆弱性、ツール、対応手順に関連するスキルや、セキュリティインシデントの発生を予防するため定期的に実施されるべき運用手順等のスキルを評価する認定資格。

CompTIA Project+ は、小規模から中規模プロジェクトを遂行する際の知識を体系的に学習することができ、業界を問わずプロジェクトマネジメントに必要な標準知識とベストプラクティスに基づく実務能力を評価する認定資格。

取り組み

■セキュリティ分野のスキル標準化
全国で提供するセキュリティオンサイトサービスに対応するエンジニアのベーススキルに Security+ を定義しています。
また、選定したその他研修と組み合わせ、インシデントレベルに応じたアナリストの育成も行っています。

■新入社員研修の教材に利用
カスタマサービス部門の新入社員全員に ベンダーニュートラルな A+ と Network+ を必須としています。

- 社内講師による講習を実施し、合格に向けた支援制度を設け、取得の推進を図っています。取得にあたりテキスト、バウチャーが提供され奨励金制度の充実や次に取得目標とする資格を明確化しモチベーション向上に繋げています。

■ビジネスに連動した ITSS スキル定義に活用
ITSS に準拠したレベル定義に CompTIA 認定資格を活用しています。
各職種に合った資格目標とレベルを設定、職種毎のスキルパスを明確化し活動計画に連動する個人目標となる様に推進しています。

- 全国のカスタマサービス部門の取得者数（2018 年 9 月現在）
  A+: 344 名　Network+: 294 名
  Server+: 169 名　Security+: 384 名　Project+: 146 名

「基礎スキルの習得、スキルレベルの見える化、キャリアアップツールとして CompTIA 認定資格取得は必要不可欠となっています。基礎スキルを身に付け、お客様へ安心・安全なサービスを提供する為に最適な認定資格であると考えています。
カスタマ／システムエンジニアだけでなく、カスタマサービス部門のソリューションを提供する営業やサポート／ SOC 要員へのスキルアップとしても CompTIA 認定資格導入を推進しています。」

サービス支援統括部　品質管理部
教育センター所長　山本　和也 様

株式会社 PFU
神奈川県横浜市西区みなとみらい 4-4-5
横浜アイマークプレイス
http://www.pfu.fujitsu.com/

「 CompTIA 認定資格は各分野の基礎知識を習得するツールとして活用するだけでなく、お客様へのアピールポイントとしても有効です。 」

サービス支援統括部
品質管理部
教育センター
所長　山本　和也 様

導入の CompTIA 認定資格
- CompTIA A+
- CompTIA Network+
- CompTIA Server+
- CompTIA Security+
- CompTIA Project+

2018 年 新資格誕生！

CompTIA PenTest+

※英語試験は、2018 年 7 月 31 日リリース。日本語試開発を予定していますが、詳細のスケジュールは未定です。

CompTIA PenTest+ は、ネットワーク上の脆弱性を特定、報告、管理するための実践的なペネトレーションテストを行うサイバーセキュリティプロフェッショナル向けの認定資格です。ペネトレーションテストの手法、脆弱性評価、また攻撃があった際のネットワークを回復するために必要となるスキルを評価します。効率的に作業を進めるためにフレームワークをカスタマイズし、結果を適切に報告すると共に、IT セキュリティ全般的な状態の改善を図るための戦略を提案できるスキルとベストプラクティスを育成します。

- CompTIA PenTest+ は、全国のピアソン VUE テストセンターで実施されている唯一のペネトレーションテスター向けの認定資格試験です。実践的なパフォーマンスベースの問題も出題され、習得しているスキルと知識、そしてそれらを確実に実践できるスキルを評価します。
- CompTIA PenTest+ は、実践的なペネトレーションテストの手法と、脆弱性評価をカバーしているだけではなく、セキュリティ管理上の弱点となりうる点への改善計画、実装、管理をするためのスキルが網羅されています。
- CompTIA PenTest+ は、従来の PC やサーバー環境に加えて、クラウドやモバイルなどの新しい環境でデバイスをテストを実施するための実践的なスキルと知識が含まれています。

CompTIA PenTest+ 取得後は、次のようなキャリアで活躍できます

- ペネトレーションテスター
- ペネトレーションテストアナリスト
- 脆弱性評価アナリスト
- 脆弱性評価マネージャ
- 脆弱性管理エンジニア
- ネットワークセキュリティマネージャ
- サイバーセキュリティエンジニア
- サイバーセキュリティアナリスト / スペシャリスト
- セキュリティアナリスト
- システムセキュリティエンジニア
- リスクマネジャー / アナリスト
- アプリケーション脆弱性アセスメントエンジニア

CompTIA PenTest+ 認定資格試験の出題内容

計画とスコープ 15%

- 目的達成のために計画の重要性を説明することができる
- 法規制の概念を説明することができる
- コンプライアンスベースのアセスメントの重要な側面を説明することができる

情報収集と脆弱性の識別 22%

- 適切な手法を活用して情報収集を行うことができる
- 脆弱性スキャンを実行することができる
- 脆弱性スキャンの結果を分析することができる
- 情報を搾取するプロセスを説明することができる
- 特殊なシステムに関連する弱点を説明することができる

攻撃とエクスプロイト 30%

- ソーシャルエンジニアリング攻撃との比較対照をすることができる
- ネットワークベースの脆弱性をエクスプロイトすることができる
- ワイヤレスと RF ベースの脆弱性をエクスプロイトすることができる
- アプリケーションベースの脆弱性をエクスプロイトすることができる
- ローカルホストの脆弱性をエクスプロイトすることができる
- 施設に関連する物理的なセキュリティ攻撃を要約することができる
- ポストエクスプロイトの手法を実行することができる

ペネトレーションテストツール 17%

- NMAP を使用して情報収集の演習を行うことができる
- さまざまなツールの使用ケースを比較対照することができる
- ペネトレーションテストの関連するツールからの出力、またはデータを分析することができる
- 基本的なスクリプトを分析することができる（Bash、Python、Ruby、PowerShell）

レポートの作成とコミュニケーション 16%

- ベストプラクティスを活用してレポートを作成することができる
- レポート提出後のアクティビティを説明することができる
- 発見された脆弱性を軽減するための推奨される戦略を提案することができる
- ペネトレーションテストプロセス中のコミュニケーションの重要性を説明することができる

CompTIA 日本支局 www.comptia.jp

facebook.com/CompTIAJP　twitter.com/CompTIA_JP

〒 101-0061
東京都千代田区神田三崎町 3-4-9 水道橋 MS ビル 7F
TEL：03-5226-5345/FAX：03-5226-0970/email：info_jp@comptia.org