

ユーザ企業においても、情報セキュリティを体系的に学習する機会やサイバーセキュリティ業務に従事するメンバーやアウトソース先のキャリアパスの明示は不可欠

ネットワーク基盤やクラウド環境を取り巻くインシデントに対応できる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



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
078-303-2231
www.asics.com

「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。」

当社の情報セキュリティ人材の育成には、グローバルで通用する国際的な資格体系を有するようなカリキュラムが必要だと考えました。」

IT統括部
セキュリティリード
CompTIA Cybersecurity Analyst (CySA+) SME
谷本 重和 様

導入のCompTIA認定資格

- CompTIA Security+
- CompTIA CySA+

CompTIA日本支局

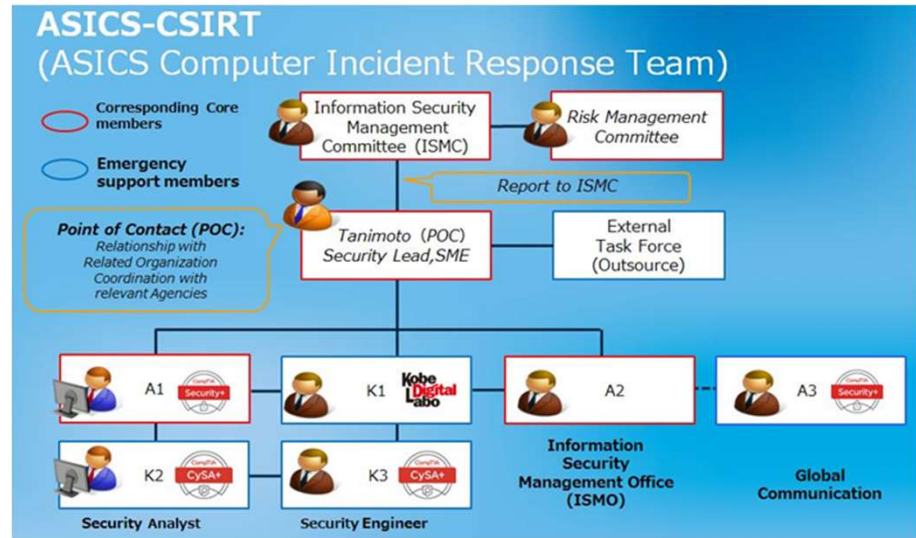
東京都千代田区神田三崎町
3-4-9 水道橋MSビル7F
www.comptia.jp

CompTIAは、1982年、IT業界の要請から発足した非営利の業界団体です。ITに携わる企業や個人の利益を高めるため、「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。米国シカゴ本部を中心に世界に10の拠点をもち、2001年に日本支局が設立されています。

取得対象者

セキュリティチーム (ASICS-CSIRT)
アウトソース先 (外部委託先企業)

取り組みの背景



セキュリティチームには、CompTIA Security+を、アウトソース先には、CompTIA CySA+を導入

CompTIA CySA+は、脅威検出ツールを理解し、組織の脆弱性、脅威およびリスクを特定するために必要となる知識とスキルを評価します。CompTIA Security+は、その上位資格に位置付けられます。

取り組み

CompTIA CySA+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・PCI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

「CySA+を取得することで、セキュリティ診断やCSIRT活動で得られたスキルを客観的に証明することができ、このような資格が今後の活動において重要になると考え受験しました。また、CySA+の受験を通じてこれまでのキャリアで培った知識を整理し、より理解を深めることができました。」

株式会社 神戸デジタル・ラボ 飯島氏
サービス推進本部 セキュリティ事業部
セキュリティ運用支援チーム 兼 KDL-SIRT

「これまでセキュリティ分析官としての業務に携わる中で、自身のスキルレベルを計りかねていたためCySA+を受験しました。CySA+を合格するまでの過程では必須知識の整理ができ、試験の中では実際の業務で発生しうる状況への対応を疑似的に体験できたため、自身のスキルレベルを計るだけでなく向上する上でも有益な試験でした。」

株式会社 神戸デジタル・ラボ 梅津氏
サービス推進本部 セキュリティ事業部
セキュリティ運用支援チーム

CompTIA®