COOLEST CAREERS IN CYBER

SANS | GIAC CERTIFICATIONS

サイバーセキュリティの業界では、独自のスキルと能力を持ち、新たな業務を遂行できる知識を持つ人材が求められています。そこで、SANSがおすすめするサイバーセキュリティの仕事20選を紹介します。これらの仕事は最も需要のある職業でもあります。 SANSではスキルアップしたい業務内容ごとにさまざまなコースを提供しておりますので、ぜひ最後までご覧ください！

01 スレットハンター

スレットハンターは、新しいスレットインテリジェンスを既存の証拠に照らし合わせ、リアルタイムの検知メカニズムをすり抜けた攻撃者を特定します。スレットハンターの業務には、スレットインテリジェンス、システムやネットワークのフォレンジック、調査開発プロセスなど、複数のスキルセットが必要です。この仕事は、インシデント対応を、純粋にリアクティブな調査プロセスから、開発中のインテリジェンスに基づいて敵やその足跡を明らかにするプロアクティブなプロセスへと移行させます。

「市販のアンチウイルスシステムで検知できる範囲を超えて、お客様の環境に埋め込まれた脅威の主体を見つけ出すことが、この仕事の特徴です。スレットハンターが攻撃に対してより効果的に対処できるよう、専門知識を提供してくれるマルウェアおよびスレットインテリジェンスのアナリストには感謝しています。」
—*Ade Muhammed*

なぜ重要なのか？

スレットハンターは、従来の検知方法では特定できなかった攻撃者の証拠を積極的に探し出します。長期間にわたって潜伏していた攻撃が見つかることもあり、とても重要な役割です。

SANSがおすすめするコース

SEC504 *GCIH* | FOR508 *GCFA* | FOR572 *GNFA* | FOR578 *GCTI* | FOR610 *GREM* | ICS515 *GRID* | ICS612

02 レッドチーマー

この仕事では、攻撃者の視点から問題や状況を見ることが求められます。組織の検知・対応のポリシーや手順、技術をテストし、測定することで、ブルーチームの能力を向上させることに重点を置きます。この業務には、レッドチーム演習の一種である攻撃シミュレーションの実施が含まれます。レッドチームは、実際の脅威や攻撃者と同様の目的を持って、同じ戦術、技術、手順に従い、攻撃者をシミュレートします。また、検知されないようにカスタムインプラントやC2フレームワークを作成することもあります。

「すべての防御をテストする唯一の方法は、すべて攻撃でその効果を測定することです。セキュリティスキャンは最低限のものであり、レッドチームに様々な地点から様々な操作をさせることで、組織が重要な箇所の弱点を修正するのに役立ちます。」
—*Beeson Cho*

なぜ重要なのか？

レッドチーマーにより、「他社に大きな被害を与えたあの攻撃は、自分たちにも起こりうるのか？」というよく聞かれる問題を解決することができます。レッドチームは、防御側をテストすることで、実際の高度な攻撃に対する組織の準備状況を、防御の観点のみならず全体的に把握することができます

SANSがおすすめするコース

SEC504 *GCIH* | SEC560 *GPEN* | SEC564 | SEC660 *GXPN* | SEC760

03 デジタルフォレンジックアナリスト

デジタルフォレンジックアナリストは、捜査に関わるシステムやデジタル・メディアを分析し、何が起こったのかを判断します。デジタルメディアには、物理的なフォレンジックデータや犯行現場にはない痕跡が含まれています。デジタルフォレンジックアナリストになるためには、証拠収集、コンピュータ、スマートフォン、クラウド、ネットワークのフォレンジック、そして調査的な考え方など、多くのスキルセットが必要です。

「フォレンジックとは、あらゆるシステムやデバイスに深く潜り込み、問題点を突き止めて解決策を導き出すことです」
—*Patricia M*

「データは嘘をつきません。デジタルフォレンジックアナリストは、データを見て、そのストーリーを伝えます。」
—*Anthony Wo*

なぜ重要なのか？

あなたはサイバーセキュリティの世界における探偵であり、事件や犯罪が発生した後、コンピュータ、スマートフォン、クラウドデータ、ネットワークを探索して証拠を探します。学ぶ機会は尽きません。フォレンジック技術は、あなたのキャリアと同様に常に進歩しています。

SANSがおすすめするコース

FOR308 | FOR498 *GBFA* | FOR500 *GCFE* | FOR508 *GCFA* | FOR509 | FOR518 | FOR572 *GNFA* | FOR585 *GASF*

04 パープルチーマー

この新しく生まれた職務では、サイバーセキュリティの防御（「ブルーチーム」）と攻撃者（「レッドチーム」）両方のオペレーションを理解する必要があります。日々の活動では、攻撃者のテクニックを整理して模倣性・自動化し、SOCの検知範囲を広げることに役立つ新しいログソースやユースケースをピックアップし、攻撃者のテクニックに対する対応力を高めるためのセキュリティコントロールを提案します。また、従来のブルーチームとレッドチームとの間で、効果的なコミュニケーションができるように調整をします。

「レッドチームとブルーチームの作戦の組み合わせは非常に面白く、両方の側面を見ることができます。私はしばらく前からパープルチームに所属していますが、このチームは私たちに多くのポジティブな変化をもたらしてくれました。」
—*Andrew R*

なぜ重要なのか？

ブルーチームは従来、セキュリティコントロール、ログソース、ユースケースなどについて議論してきました。このギャップを埋めるために、レッドチームとブルーチームが共通言語で話し、組織全体のサイバーセキュリティの態勢を改善するためにブルーチームとレッドチームの架け橋になるのがパープルチームの重要な役割です。

SANSがおすすめするコース

SEC599 *GDAT* | SEC699

05 マルウェア・アナリスト

マルウェアアナリストは、攻撃者に真っ向から立ち向かい、サイバー攻撃への迅速かつ効果的な対応とその抑制を行います。悪意のあるソフトウェアの内部を深く観察し、脅威を理解します。どのように侵入したのか、どのような欠陥が悪用されたのか、何をしたのか、何をしようとしているのか、起こりうることを想定します。

「マルウェアアナリストという仕事は、自身の持つリバースエンジニアリングのスキルと、ソフトウェアを可能な限り混乱させるためにあらゆる手段を講じているマルウェア作者のスキルとを競う絶好の場会を提供してくれます」
—*Bob Pardee*

なぜ重要なのか？

悪意のあるコードの機能を徹底的に解明するという仕事を任されたら、それは最も重要な案件に直面していることを意味します。バイナリを適切に扱い、逆アセンブルし、デバッグし、分析するためには、特定のツール、テクニック、手順、そしてコードが持つ本来の機能を見抜くための知識が必要です。リバースエンジニアは、これらの貴重なスキルを持っており、インシデントレスポンス業務において、捜査官を有利にする転機となります。マルウェアアナリストは、より良い検知のために重要なシグネチャを抽出したり、業界全体に情報を提供するためにスレットインテリジェンスを作成したりするなど、貴重な調査リソースとなります。

SANSがおすすめするコース

FOR518 | FOR585 *GASF* | FOR610 *GREM*

06 最高情報セキュリティ責任者(CISO)

最高情報セキュリティ責任者（CISO）は、ビジネスと情報セキュリティの両側面理解し、IT部門と経営層とのバランスをとる役割を担います。影響力や交渉力に加えて、世界中の市場、政策、法律にも精通している必要があります。CISOはクリエイティブな考え方を持ち、問題解決能力にも長けている必要があります。サイバー犯罪者の頭の中を読み取り、新しい脅威とその解決策を見つけなければなりません。

「CISOは計画をうまく調整します。また、CISOはチームをよく理解し、適切な業務を割り当てて、組織のネットワークとセキュリティを戦略的に守り、テストしていきます。」
—*Anastasia Edwards*

なぜ重要なのか？

最近の傾向として、CISOはビジネス感覚とテクノロジーの知識をバランスよく持ち合わせていることが求められています。これは、情報セキュリティの問題を技術的な観点から把握し、広範なビジネス目標に適用するためのセキュリティ計画を導入する方法を理解し、組織を守るために、より長期的なセキュリティとリスクベースの文化を構築できるようにするためです。

SANSがおすすめするコース

MGT512 *GSLC* | MGT514 *GSTRT* | MGT520 | MGT521

07 ブルーチーマー - オールラウンドなディフェンダー

この業務内容は、組織によってさまざまな呼び名で肩書が設定されていますが、多くの場合、幅広いタスクと知識が求められます。オールラウンドなディフェンダーであるブルーチーマーは、小規模な組織においては特に、主要なセキュリティ窓口となる可能性があり、エンジニアリングやアーキテクチャ、インシデントのトリアージや対応、セキュリティツールの管理など、様々な業務に対応しなければなりません。

「今日では、防御に長け、システムを強化する方法を理解している人材が必要です。」
—*David O*

なぜ重要なのか？

こうしたオールラウンドな業務は、細かな業務に特化した役職を持つ本格的なセキュリティ・チームを編成する予算がない中小規模の組織でよく見られ、非常に重要な立場であると言えます。オールラウンドなディフェンダーは、必ずしも正式な名前のついた職種ではありませんが、すべてのことのために少しでも多くの防御を行う、広範囲なディフェンダーを意味しています。

SANSがおすすめするコー

SEC450 | SEC503 *GCIA* | SEC505 *GCWN* | SEC511 *GMON* | SEC530 *GDSA* | SEC555 *GCDA* | SEC586

08 セキュリティアーキテクト＆エンジニア

ネットワークによる制御とデータに関する制御を効果的に組み合わせ、予防、検知、レスポンスのバランスをとるように設計、実装、調整しなければなりません。セキュリティアーキテクトとエンジニアは、企業のディフェンスを前提に、あらゆる層でセキュリティ対策を行います。このとき、ビジネス面と技術上の要件のバランスをとり、さまざまなセキュリティポリシーや手順を考慮して、組織のセキュリティを実装します。

「セキュリティアーキテクトは、ワークフロー、ネットワーク、ビジネス要件、プロジェクト計画、そして時には予算の制約も理解する必要があります。非常に多様な役割を担っています」
—*Chris Bodill*

なぜ重要なのか？

セキュリティアーキテクトとエンジニアは、エンドポイントからクラウドまで、ネットワークやアプリケーションを介して送受信される組織の重要なデータを保護するためのスキルを備えた、ブルーチームの一員であり、サイバーディフェンダーです。

SANSがおすすめするコース

SEC503 *GCIA* | SEC505 *GCWN* | SEC511 *GMON* | SEC530 *GDSA*

09 インシデントレスポンスチームメンバー

このダイナミックでテンポの速い業務内容は、攻撃者がまだその攻撃を展開している間に、攻撃者を特定し、封じ込め、根絶することです。

「インシデントは必ず発生するものであり、これらのインシデントによる組織の損失を管理し、軽減するために、適切なスキルセットを持った人材を確保することが重要です。」
—*Anita Ali*

なぜ重要なのか？

侵入を防ぐことが究極の目標ですが、現実的には攻撃者による攻撃は最終的には成功してしまうということを想定しておく必要があります。侵入が確認できたら、インシデント・レスポンダーは、攻撃者を突き止め、被害を最小限に抑え、最終的に組織内のシステムから排除しなければなりません。この業務には、迅速な思考、確かな技術力と文書作成能力、攻撃者が悪用する技術などに精通している必要があります。さらに、インシデント・レスポンダーは、様々な専門分野を持つチームの一員として働かなければなりません。最終的には、専門家から経営者まで幅広い層に、その調査結果を効果的に伝える必要があります。

SANSがおすすめするコース

SEC402 | SEC504 *GCIH* | FOR508 *GCFA* | FOR509 | FOR518 | FOR572 *GNFA* | FOR578 *GCTI* | FOR610 *GREM*

10 サイバーセキュリティ・アナリスト/エンジニア

サイバーセキュリティ業界の中でも特に給与が高い業務であり、高度なスキルが求められます。脅威の検知、脅威の分析、脅威からの防御について高い能力と知識が必要です。組織のデータのセキュリティと完全正を維持するための重要な業務です。

「単純な分析のサポートから、新しいソリューションの導入、SOCなどのサービス全体の実装まで、調査や管理職一が思い描くタスクやプロジェクトに挑戦することも多く、この職業ほど包括的なものはありません。
—*Harun Kuessner*

なぜ重要なのか？

組織のシステムが攻撃された場合に組織が実施するコンティンジェンシープランを作成するなど、プロアクティブな業務です。攻撃者は常に新しいツールや技術を使用しているため、サイバーセキュリティアナリスト/エンジニアは、こうした最新の攻撃へ対応できるよう、世の中に出回っているツールや技術についての情報を常に収集しておく必要があります。

SANSがおすすめするコース

SEC401 *GSEC* | SEC450 | SEC501 *GCED* | SEC503 *GCIA* | SEC504 *GCIH* | SEC530 *GDSA* | SEC540 *GCSA* | SEC555 *GCDA* | SEC530 *GDSA* | FOR509 | ICS410 *GICSP* | ICS456 *GCIP*

11 OSINT調査員/アナリスト

お客様の要件定義に基づいて、オープンソースやインターネット上のリソースを活用し、調査に関連するデータを収集する業務です。ドメインやIPアドレス、企業、人物像、刊行物、金融取引情報、など幅広い情報収集が必要となり、場合によっては調査対象以外のターゲットについての情報も収集します。調査結果を収集、分析し、クライアントに報告し、クライアントがアクションを起こす前に、対象に関する洞察を得られるようにします。

「OSINT調査員は、独特で巧妙な方法で情報を探し出していくので、退屈することは起きません。ある日は不正行為の調査をし、次の日には行方不明者の捜索に携わります。この仕事は常に自分の能力が試され、クリティカルシンキングのスキルが鋭えられ、自分が役に立っていることを実感できるのです。」
—*Rebecca Ford*

なぜ重要なのか？

インターネット上には、膨大な量のデータが存在します。しかし、その膨大なデータの中から必要な情報を探し出し、収集することは困難を極めます。OSINT調査員は世界中の情報源の中から適切なデータを発見・収集するために必要なスキルとリソースを持たなければなりません。サイバーセキュリティをはじめ、インテリジェンス、軍事、ビジネスなど様々な分野で活躍します。

SANSがおすすめするコース

SEC487 *GOSI* | FOR578 *GCTI*

12 テクニカルディレクター

テクニカルディレクターは、開発チームと協力して技術戦略をたて、リスクを評価し、進捗を測定するための基準と手順を確立し、強力なチームを作りあげます。

「テクニカルディレクターには、サイバーセキュリティの知識、組織のインフラと今後の展開についての戦略的な視点、そしてコミュニケーションスキルが求められます。いずれのスキルも身につけることは難しいもので、組織の規模や業務内容に関わらず、この仕事は非常にやりがいのあるものだと考えています。」
—*Francisco Lugo*

なぜ重要なのか？

テクニカルディレクターは強固な組織に欠かせない存在です。幅広い技術を把握、管理するには多くの時間と知識が必要とされます。サイバーセキュリティ人材が世界的に不足している中、クラウドへの移行がかつてないほど進んだり、法律や技術標準のために遵守しなければならない項目が増えたりして、セキュリティに関する課題は以前に比べてとても複雑になってきています。これら全てを包括的に見ながら、組織づくりをする必要があります。

SANSがおすすめするコース

MGT516 | MGT551 | SEC557 | SEC566 *GCCC*

13 クラウドセキュリティアナリスト

クラウドセキュリティアナリストは、クラウドに関するセキュリティおよびこれらの日々の運用を担当します。セキュリティ管理のためのツールの設計、統合、テストに携わります。また、各種設定の改善点を検討し、組織の全体的なクラウドセキュリティへの姿勢を評価し、組織が意思決定するために必要な専門知識を共有します。

「この業務は、クラッカーやハッカーによるクラウド環境への不正アクセスから組織を守るために、クラウド環境の脆弱性を見つけて改善を行っていくために不可欠です。」
—*Ben Yee*

なぜ重要なのか？

従来のオンプレミス型のソリューションからクラウドへの移行がかつてないほど早く進んでおり、クラウドセキュリティの専門家が不足しています。今日のビジネス界には必須とも言えるマルチクラウドの環境において、組織を安全に保つためにクラウドアナリストによるサポートが必要であると言えます。

SANSがおすすめするコース

SEC401 *GSEC* | SEC488 *GCLD* | SEC510 | SEC541 | SEC557 | SEC588 *GCPN* | FOR509

14 侵入検知／SOCアナリスト

セキュリティオペレーションセンター（Security Operations Center：SOC）のアナリストは、セキュリティエンジニアやSOCマネージャーと協力して、予防、検知、監視、アクティブレスポンスを実施します。SOCアナリストは、インシデントレスポンスチームと密接に連携し、セキュリティに関する問題が検出されると、迅速かつ効果的に対処します。細部にまで目を配り、見落とされがちなことまで見抜くことができるのがアナリストです。

「侵入アナリストは門番であり、ネットワークへの侵入を検知して阻止することで大きなやりがいを得ることができます。」
—*Chuck Ballard*

なぜ重要なのか？

SOCアナリストは、組織が迅速に攻撃を特定し、被害が拡大する前に対処するために行動します。また、セキュリティモニタリング、脆弱性管理、インシデントレスポンスなどを必要とする法律や技術標準などへの対応もサポートします。

SANSがおすすめするコース

SEC450 | SEC503 *GCIA* | SEC504 *GCIH* | SEC511 *GMON* | SEC555 *GCDA* | FOR508 *GCFA* | FOR572 *GNFA*

15 セキュリティアウェアネスオフィサー

セキュリティアウェアネスオフィサーは、セキュリティチームと協力して、組織最大のリスクとなりうる人的リスクを特定し、そのリスクを管理するための行動を考えます。 組織的に安全な行動をとるために、従業員を効果的に訓練し、コミュニケーションを継続的に取るためのプログラムの開発と管理を担当します。洗練されたプログラムは、従業員の行動に影響を与えるだけでなく、強固なセキュリティ文化を生み出します。

「この業務では、これまでの経験を活かして、組織全体の適切なセキュリティ行動に影響を与え、組織の防御力を効果的に高められます。また、脅威の性質は急速に進化しているので、仕事を続けても決して飽きることはありません。」
—*Sue DeRosier*

なぜ重要なのか？

インシデントや侵害の最大の要因は「人」であるにもかかわらず、ほとんどの組織がいまだに技術的な観点からしかセキュリティに取り組んでいることが問題となっています。この業務では、組織がこのギャップを埋め、「人」の観点からも問題にアプローチするための鍵となります。サイバーセキュリティにおいて、最も重要かつ急速に成長している分野のひとつであることは間違いありません。

SANSがおすすめするコース

MGT433 *SSAP* | MGT512 *GSLC* | MGT521

16 脆弱性研究者・エクスプロイト開発者

この業務では、組織や個人が使用している様々なアプリケーションやデバイスにあるゼロデイの脆弱性（未知の脆弱性）を探します。攻撃者より先に脆弱性を発見する必要があります。

「これから、脆弱性研究者は非常に重要な役割を果たすことになると思います。研究者は、ハッカーに悪用される前に脆弱性を特定し、対策を講じることができるので、インシデントが起きてから対応するのではなく、問題を未然に防ぐことができるようになるでしょう。」
—*Anita Ali*

なぜ重要なのか？

IoTデバイスから商用アプリケーションやネットワークデバイスまで、研究者は常に、一般的な製品やアプリケーションの脆弱性を探し出しています。インスリンポンプやペースメーカーなどの医療機器さえも対象としています。攻撃者よりも先に脆弱性を特定するための専門知識がなければ、危険な事態を起こす可能性があります。

SANSがおすすめするコース

SEC660 *GXPN* | SEC661 | SEC760

17 アプリケーションペンテスター

アプリケーションペネトレーションテスターは、攻撃の対象となるすべての脆弱なWebベースのサービス、クライアントサイドアプリケーション、サーバーサイドプロセスなどを調査し、組織のセキュリティの安全性を確かめます。まるで攻撃者のように、セキュリティの障壁を突破できるように、ピボットや横展開などのテクニックをも駆使して、機密情報へのアクセスや企業の内部システムへの侵入を試みます。

「既存のツールや手法を使うだけではなく、創造性を発揮し、アプリケーションのロジックを理解し、インフラを推測しなければなりません。」
—*Dan-Mihai Negrea*

なぜ重要なのか？

Webアプリケーションは、社内外を問わず業務遂行に欠かせません。これらのアプリケーションには、オープンソースのプラグインが使用されていることが多く、セキュリティ侵害のリスクにさらされる可能性があります。

SANSがおすすめするコース

SEC522 *GWEB* | SEC542 *GWAPT* | SEC560 *GPEN* | SEC588 *GCPN* | SEC642

18 ICS/OT セキュリティ・アセスメント・コンサルタント

片足はオフェンシブなオペレーションの世界へ、もう片足は生活に欠かせない重要なプロセス制御環境へ。システムの脆弱性を発見し、資産の所有者や運営者と協力して、発見した脆弱性を緩和し、攻撃者の悪用を防ぎます。

「この種の業界で働いていると、需要が急速に増加しているため、企業が適切なスキルセットを持つ人材を必死に探し始めていることがわかります」
—*Ali Alhajhouj*

なぜ重要なのか？

OT（主にICSシステム）に影響を与えるセキュリティインシデントは、意図的なものも偶発的なものも含めて、影響は大きいが頻度は低い（HILF）と考えることができ、頻繁に起こるものではありませんが、起こった場合のビジネスへの代償が大きいので、重要な役割です。

SANSがおすすめするコース

ICS410 *GICSP* | ICS456 *GCIP* | ICS515 *GRID* | ICS612 | SEC560 *GPEN*

19 DEVSECOPS エンジニア

この職業は、一番良いとされているツールとプロセスを使って、自動化されたセキュリティの機能を開発し、セキュリティを開発とオペレーションのパイプラインに加えます。これには、脆弱性の管理、モニターとログ、セキュリティのオペレーション、セキュリティのテストやアプリケーションセキュリティなどを含む分野でのリーダーシップが求められます。

「私の見解では、顧客の開発者に柔軟かつ迅速に安全なソリューションを提供する企業から非常に求められている人材です。」
—*Antonio Esmoris*

なぜ重要なのか？

この仕事は、古いセキュリティモデルが継続的なデリバリーパイプラインのボトルネックになっていることに対して、それを解消するためにできた役割です。ITとセキュリティの間に生じたギャップを埋めると同時に、アプリケーションとビジネスが迅速で安全に遂行できるようにすることが目的です。

SANSがおすすめするコース

SEC510 | SEC522 *GWEB* | SEC534 | SEC540 *GCSA*

20 メディアエクスプロイテーションアナリスト

この業務では、デジタルフォレンジックのスキルを調査が必要な様々なメディアに応用します。コンピュータ犯罪に興味があり、ハッキングされたり、破損したり、犯罪で使用されたファイルシステムを復旧させる仕事がしたい方に向いています。科学的根拠に基づく証拠を得るために、様々なソースからコンピュータやメディアのフォレンジック調査をサポートします。

「これは謎解きや犯罪調査のようなものです。未知のものや、技術的に複雑な対策には楽しめる要素があります。機密情報や真の証拠を見つけられる可能性がこの仕事の刺激的なところです。」
—*Chris Brown*

なぜ重要なのか？

この業務においては多くの場合、犯罪行為に関わる証拠に最初に触れ、対応します。テロリズムや防諜、法執行や内部犯行などをはじめ、様々なケースにおいてメディアの入手から最終報告まで任せられており、調査には欠かせない存在です。

SANSがおすすめするコース

FOR308 | FOR498 *GBFA* | FOR500 *GCFE* | FOR508 *GCFA* | FOR518 | FOR572 *GNFA* | FOR585 *GASF*

SANSのトレーニング、インストラクター、 資格の詳細に関しては、**sans.org/roadmap** でロードマップをご覧ください。

SANSトレーニングの計画、詳細につきましては、SANS (**japan@sans.org**)までお問い合わせください。