

COOLEST CAREERS IN CYBER



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仕事でもあります。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！

カリキュラム: ■ New2Cyber ■ サイバーディフェンス ■ デジタルフォレンジック ■ オフェンシブオペレーション ■ サイバーセキュリティリーダーシップ ■ クラウドセキュリティ ■ 産業制御システム ■ パープルチーム **SEC504 GCIH** ← GIAC認定資格

01 スレイトハンター (脅威/警告アナリスト)

スレイトハンターは、新しいスレイトインディ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。スレイトハンターの業務には、スレイトインディジェンス、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、開発中のインディ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。

なぜ重要なのか？

スレイトハンターは、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者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

FOR508 GCFA FOR528 FOR572 GNFA FOR578 GCTI FOR589 FOR608 GEIR
FOR610 GREM SEC497 GOSI SEC504 GCIH SEC541 GCTD ICS515 GRID ICS612

—Ade Muhammed

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。このように侵入したか、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。

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せられたら、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。リパースエンジニアは、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イトインディ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 GIME FOR528 FOR585 GASF FOR610 GREM FOR710 SEC501 GCED

—Bob Pardee

09 サイバーディフェンスインシデントレスポンダー・法執行防諜フォレンジック・アナリスト

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。

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、攻撃者を突き止める、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する必要があります。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く必要があります。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

FOR508 GCFA FOR509 GCGR FOR518 GIME FOR528 FOR572 GNFA
FOR578 GCTI FOR589 FOR608 GEIR FOR610 GREM FOR710 SEC402
ICS515 GRID SEC504 GCIH

—Anita Ali

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。

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つか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クラウド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

SEC488 GCLD SEC510 GPCS SEC541 GCTD SEC401 GSEC FOR509 GCGR
SEC588 GCPN

—Ben Yee

17 アプリケーションペンテスター (セキュアソフトウェアアクセサー)

アプリケーションペネトレーションペスターは、攻撃の対象となすすべての脆弱なWebページのサービス、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、ピットや橋渡り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内部システムへの侵入を試みます。

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

SEC542 GWAPT SEC560 GPN SEC575 GMOB SEC588 GCPN SEC660 GXPN
SEC760

—Dan-Mihal Negrea

02 レッドチーマー (攻撃者エミュレーションスペシャリスト)

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。

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。レッドチーマーは、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 SEC542 GWAPT SEC560 GPN SEC565 GRTP SEC660 GXPN
SEC670 SEC699 SEC760

—Beeson Cho

06 最高情報セキュリティ責任者 (エグゼクティブサイバーリーダーシップ)

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を理解し、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もち、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ればなりません。

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トピックスへ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

LDR512 GSLC LDR514 GSTRT LDR516 LDR520 LDR521 LDR551 GSOM
LDR553 SEC566 GCCC ICS418

—Anastasia Edwards

10 サイバーセキュリティアナリスト・エンジニア (システムセキュリティアナリスト)

サイバーセキュリティ業界の中でも特に給与が高い職業であり、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性を維持するための重要な業務です。

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に、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 GSOC SEC501 GCED SEC503 GCIA SEC530 GDSA
SEC504 GCFA FOR508 GCGR FOR509 GCGR LDR551 GSOM SEC510 GPCS
SEC540 GCSA SEC549 ICS410 GICSP ICS456 GCIP

—Harun Kuessner

14 侵入検知・SOCアナリスト (サイバーディフェンスアナリスト)

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応します。細部にまで目を配り、見落としや抜けがないよう検出することができるのがアナリストです。

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応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 GSOC SEC503 GCIA SEC511 GMON FOR508 GCFA FOR572 GNFA
SEC504 GCIH

—Ali Alhajhouj

18 ICS/OTセキュリティ・アセスメント・コンサルタント (ICS/SCADAセキュリティエンジニア)

片足はオープン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。

なぜ重要なのか？

OT(主にCS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、頻発に起こるものではありません。起こった場合のビジネスへの代償が大きいため、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 GPN

—All Alhajhouj

03 デジタルフォレンジック (サイバーディフェンス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。

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

FOR498 GBFA FOR500 GCFE FOR508 GCFA FOR509 GCGR FOR518 GIME
FOR572 GNFA FOR577 FOR585 GASF SEC501 GCED

—Anthony Wo

07 ブルーチーマー: オールラウンドな ディフェンダー (サイバーディフェンスアナリスト)

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、幅広いスキル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、インシデントリスポンダーや対応、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。

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割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、すべての人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ス

SEC450 GSOC SEC503 GCIA SEC511 GMON SEC530 GDSA SEC586

—David O

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、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。

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抽出し、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、インディジェンス、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

SEC497 GOSI SEC587 FOR578 GCTI FOR589

—Rebecca Ford

15 セキュリアウェアネスオフィサー (セキュリティウェアネス&コミュニケーションマネージャー)

セキュリティ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。

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ない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

LDR433 SSAP LDR512 GSLC LDR521

—Sue DeRosier

19 DevSecOpsエンジニア (情報システムセキュリティ開発者)

この職業は、一番良いとされているツールやプロセスを使って、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バリエーションに加えます。これは、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。

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對して、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

SEC488 GCLD SEC510 GPCS SEC522 GWEB SEC540 GCSA

—Antonio Esmoris

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化・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ビジュアルアップし、攻撃者のテクニックに対する対応力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。

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。一方、レッドチームは従来、ベイトロード、エクスプロイト、インプラント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 SEC504 GCIH SEC568 SEC598

—Andrew R

08 セキュリティアーキテクト (NICE) & 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徹底的に見て、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。

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 SEC511 GMON SEC530 GDSA SEC549

—Chris Bodill

12 テクニカルディレクター (情報システムセキュリティマネージャー)

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。

なぜ重要なのか？

IT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つかないほど進んだり、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

LDR512 GSLC LDR514 GSTRT LDR516 LDR551 GSOM SEC566 GCCC ICS418

—Francisco Lugo

16 脆弱性研究者・エクスプロイト開発者 (脆弱性診断アナリスト)

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。攻撃者よりも先に脆弱性を見発見する必要があります。

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なども対象となります。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、危険な事態を招く可能性があります。

SANSがおすすめするコース

SEC660 GXPN SEC670 SEC760

—Anita Ali

20 メディアエクスプロイテーションアナリスト (サイバー犯罪捜査官)

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、破壊したり、犯罪で使われたファイルシステムを復旧させる仕事かしたい方に向いています。科学的根拠に基づいた証拠を得るために、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。

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

FOR498 GBFA FOR500 GCFE FOR508 GCFA FOR518 GIME FOR572 GNFA
FOR577 FOR585 GASF

—Chris Brown

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。