SANSトレーニングロードマップ

トピック / コース番号 / 対応するGIAC
Essentials — ICS410 **ICS/SCADA Security Essentials™** | GICSP
コース名

全般的な基礎スキル

新しくセキュリティに関わる方 | コンピュータ、技術、セキュリティ

コンピュータITの基礎	SEC275 **Foundations: Computers, Technology & Security™** | GFACT
サイバーセキュリティの基礎	SEC301 **Introduction to Cyber Security™** | GISF

この入門コースでは、セキュリティに関する幅広いトピックを取り上げ、実際の事例をふんだんに盛り込んでいます。技術的な問題と経営的な問題をバランスよく取り入れたこのコースは、情報セキュリティの基礎とリスクマネジメントの基本を理解する必要がある受講者にとって魅力的なコースです。

要素技術 | 攻撃、保護、防御、運用

セキュリティに関わる全ての方が知っておくべき知識

セキュリティの基礎	SEC401 **Security Essentials: Network, Endpoint, and Cloud™** | GSEC

SEC401は、情報セキュリティの初心者から、専門分野に特化したベテラン技術者まで、オンプレミスまたはクラウドに関わらず、重要な情報や技術資産を保護しセキュリティを高めるために必要な情報セキュリティスキルと技術を習得することができます。

防御するためのスキル	SEC450 **Blue Team Fundamentals: Security Operations and Analysis™** | GSOC
攻撃者のテクニック	SEC504 **Hacker Tools, Techniques, and Incident Handling™** | GCIH

サイバーセキュリティの業務に携わるすべての技術者は、システムの安全確保、防御、攻撃の仕組みの理解、およびインシデント発生時の対応をするための基本的なスキルを身につけるためにトレーニングを受ける必要があります。セキュリティを確保するためには、組織内で要求されるスキル以上の基礎知識を習得しておく必要があります。

SANS SECURITY AWARENESS：業務別トレーニング

IT管理者のためのセキュリティ基礎

PCI DSS準拠トレーニング

最新の脅威から組織を守るためには、それらの脅威の一歩先を行くために継続的なスキルアップが必要です。各業務に基づいた短いモジュールに分割されているトレーニングを選択して受講し、業務に応じて必要となるセキュリティの概念について理解を深めることができます。

フォレンジックの基礎

フォレンジックとインシデントレスポンス担当者が知っておくべき知識

有事の際のフォレンジック技術とデータ抽出	FOR498 **Battlefield Forensics & Data Acquisition™** | GBFA

クラウドセキュリティの基礎

クラウドセキュリティ担当者が知っておくべき知識

クラウドセキュリティの基礎	SEC488 **Cloud Security Essentials™** | GCLD

サイバーセキュリティに初めて携わる方やスキルアップを目指す方にとって、クラウドセキュリティについての知識は現在多くの組織で必要とされています。これらのコースでは、クラウドセキュリティのために必要な基礎知識を学び、実践的な演習を通じて理解を深めます。

クラウドセキュリティの基本要素

基本的なクラウドセキュリティの概念や原則、用語などについて理解する必要はあるものの、実際にクラウド技術で手を動かすことはない方のためのコースです

クラウドセキュリティ入門	SEC388 **Introduction to Cloud Computing and Security™**

SANS SECURITY AWARENESS：業務別トレーニング

開発者のためのセキュアコーディング

開発者はもちろん、ソフトウェア開発工程に携わる、アーキテクトやテスター、管理者やビジネスオーナー、そしてパートナーを含む様々な業務に応じたトレーニングを活用し、上流工程からセキュリティを意識したアプリケーションを開発できるようにします。

産業用制御システム（ICS）セキュリティ

ICS・OT（Operational Technology）に携わるすべての方が知っておくべき知識

ICSセキュリティの基礎	ICS410 **ICS/SCADA Security Essentials™** | GICSP

管理者のためのICS・OTセキュリティ

ICSセキュリティの基礎	ICS418 **ICS Security Essentials for Leaders™**

セキュリティリーダーシップの基礎知識

すべてのサイバーセキュリティに関する管理職が知っておくべき知識

CISSP®トレーニング	LDR414 **SANS Training Program for CISSP® Certification™** | GISP
セキュリティ意識	LDR433 **Managing Human Risk™** | SSAP
RISK ASSESSMENT	LDR419 **Performing a Cybersecurity Risk Assessment™**

優秀なセキュリティ技術者が増える中、それぞれの組織ではチームや業務を管理するためのリーダーが必要とされています。管理職は必ずしもセキュリティの実務を行うわけではありませんが、ポリシーや業務戦略の策定、技術担当者とのコミュニケーションや業績評価のために、基礎的な技術やフレームワークについて理解しておく必要があります。

SANS SECURITY AWARENESS：業務別トレーニング

全役職員のためのセキュリティ意識向上トレーニング

SANS SECURITY AWARENESSオンライントレーニングでは、全役職員にとって必要となる、緊急性の高いリスクやコンプライアンスに関するモジュールも提供しています。各役職員のセキュリティ行動を促し、組織全体のセキュリティ向上に繋がります。
※モジュールごとで多言語対応というのはここだけでなくSecurity Awarenessの一般的な話なので省いてあります。

サイバーレンジ

全てのセキュリティ担当者のための実践演習

スキルの確認と実践演習	BootUp CTF Core NetWars Core NetWars Continuous

SANSのサイバーレンジでは幅広いトピックをカバーするインタラクティブな実践演習を通じ、それぞれのスキルの確認と定着を促します。

人工知能（AI）

AIセキュリティの基礎

AI	AIS247 **AI Security Essentials for Business Leaders™**

業務に応じたスキル

システム設計、侵入検知、防御技術

サイバー攻撃からシステムを守るためのスキル

サイバーセキュリティ全般について応用技術	SEC501 **Advanced Security Essentials – Enterprise Defender™** | GCED
監視と運用	SEC511 **Cybersecurity Engineering: Advanced Threat Detection and Monitoring™** | GMON
セキュリティアーキテクチャ	SEC530 **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™** | GDSA

ネットワーク内で何が起きているかを検知するためには、高度なスキルと能力が要求されます。通常ではない挙動を特定するためには、検知・監視ツールの導入や、それらからの出力を分析・利用するためのノウハウが必要となります。

Open-Source Intelligence

OSINT	SEC497 **Practical Open-Source Intelligence (OSINT)™** | GOSI

攻撃者の技術 | 脆弱性の分析、ペネトレーションテスト

攻撃技術に携わる担当者が知っておくべき知識

ネットワークペネトレーションテスト	SEC560 **Enterprise Penetration Testing™** | GPEN
Webアプリケーションテスト	SEC542 **Web App Penetration Testing and Ethical Hacking™** | GWAPT

セキュリティ上の問題点を検出するプロフェッショナルは、システムの防御を担当する専門家とは異なるスキルやノウハウが必要となります。REDチーム（攻撃技術の専門家）とBLUEチーム（防御技術の専門家）にはそれぞれ必要となる知識があり、脆弱性を検出するには、攻撃者側の知識やツールが必要となります。攻撃技術を知ることによって、防御の能力も向上させることができます。

インシデントレスポンスとスレットハンティング | ホストベースのネットワークベースのフォレンジック

フォレンジックとインシデントレスポンス担当者が知っておくべき知識

エンドポイントフォレンジック	FOR500 **Windows Forensic Analysis™** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics™** | GCFA FOR608 **Enterprise-Class Incident Response & Threat Hunting™**
ネットワークフォレンジック	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™** | GNFA
LINUXフォレンジック	FOR577 **LINUX Incident Response and Threat Hunting™**

WindowsやLinuxなどの各ホストやサーバー、またはネットワーク上でのフォンレジックを行い証跡をまとめたり、こうしたスキルを用いてスレットハンティングを行ったりするために、攻撃の分析や初動対応、本格的なインシデントレスポンスやシステム回復のための専門的な知識が必要です。

クラウドセキュリティの要素技術

業務に応じた各要素分析

パブリッククラウド	SEC510 **Cloud Security Controls and Mitigations™** | GPCS
自動化とDevSecOps	SEC540 **Cloud Security and DevSecOps Automation™** | GCSA
監視と検出	SEC541 **Cloud Security Threat Detection™** | GCTD
アーキテクチャ	SEC549 **Cloud Security Architecture™**

世界的なクラウドへの大規模な移行に伴い、パブリッククラウドの利用に伴うセキュリティリスクやメリット、マルチクラウド環境の導入や活用方法、DevOpsの開発プロジェクトにセキュリティを組み込む方法などを理解しているプロフェッショナルが求められています。

産業用制御システム（ICS）セキュリティ

ICS・OT（Operational Technology）に携わるすべての方が知っておくべき知識

ICS防御とインシデントレスポンス	ICS515 **ICS Visibility, Detection, and Response™** | GRID
ICSセキュリティ応用技術	ICS612 **ICS Cybersecurity In-Depth™**

産業用制御システムによって現実世界は動かされており、ICSを守るセキュリティ担当者は極めて重要な役割と言えます。OTや国家安全保障、そして人命を守るために、重要インフラを守るスキルを身につけましょう。

リーダーシップの要素技術

変革するサイバーセキュリティリーダー

テクノロジーリーダーシップ	LDR512 **Security Leadership Essentials for Managers™** | GSLC
セキュリティ戦略	LDR514 **Security Strategic Planning, Policy, and Leadership™** | GSTRT
セキュリティ文化	LDR521 **Security Culture for Leaders™**

運用周りのセキュリティリーダー

脆弱性管理	LDR516 **Building and Leading Vulnerability Management Programs™**
SOC	LDR551 **Building and Leading Security Operations Centers™** | GSOM
フレームワークとコントロール	SEC566 **Implementing and Auditing CIS Controls™** | GCCC

サイバーレンジ

サイバーディフェンス	Cyber Defense NetWars
デジタルフォレンジックとインシデントレスポンス（DFIR）	DFIR NetWars DFIR NetWars Continuous
産業制御システム（ICS）	ICS NetWars
発電・送電システム（ICS/SCADA）	GRID NetWars

業務内容ごとに特化されたNetwarsを提供しています。これらサイバーレンジでは、それぞれのトピックを深く掘り下げ、実際の事件・事故に基づいた課題やシナリオに挑戦することによってスキルアップできます。

専門家のための高度なスキル

システム防御に関する高度技術 | システムハードニング

各トピックに焦点を当てたコース

トラフィック分析	SEC503 **Network Monitoring and Threat Detection In-Depth™** | GCIA
Pythonプログラミング	SEC573 **Automating Information Security with Python™** | GPYC SEC673 **Advanced Information Security Automation with Python™**
データサイエンス	SEC595 **Applied Data Science and Machine Learning for Cybersecurity Professionals™** | GMLE

Open-Source Intelligence

OSINT	SEC587 **Advanced Open-Source Intelligence (OSINT) Gathering & Analysis™**

攻撃者の高度技術 | 専門的な技術と分野

ネットワーク、Web、クラウド

Exploit開発	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™** | GXPN SEC760 **Advanced Exploit Development for Penetration Testers™**
クラウドペネトレーションテスト	SEC588 **Cloud Penetration Testing™** | GCPN

専門的なペネトレーションテスト

レッドチーム	SEC565 **Red Team Operations and Adversary Emulation™** | GRTP SEC670 **Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control™**
モバイル	SEC575 **iOS and Android Application Security Analysis and Penetration Testing™** | GMOB
製品セキュリティ	SEC568 **Product Security Penetration Testing – Safeguarding Supply Chains and Managing Third-Party Risk™**
ペネトレーションテスト	SEC580 **Metasploit for Enterprise Penetration Testing™**
ワイヤレス	SEC556 **IoT Penetration Testing™** SEC617 **Wireless Penetration Testing and Ethical Hacking™** | GAWN

パープルチーム

パープルチーム戦略	SEC598 **Security Automation for Offense, Defense, and Cloud™** SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses™** | GDAT SEC699 **Advanced Purple Teaming – Adversary Emulation & Detection Engineering™**

フォレンジック、マルウェア分析、スレットインテリジェンス | さまざまな調査に関する専門的なスキル

特定の専門分野に関するスキル

クラウドフォレンジック	FOR509 **Enterprise Cloud Forensics & Incident Response™** | GCFR
ランサムウェア	FOR528 **Ransomware and Cyber Extortion™**
マルウェア分析	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques™** | GREM FOR710 **Reverse-Engineering Malware: Advanced Code Analysis™**

スレットインテリジェンス

サイバースレットインテリジェンス	FOR578 **Cyber Threat Intelligence™** | GCTI FOR589 **Cybercrime Intelligence™**

デジタルフォレンジックとMedia Exploitation

スマートフォン	FOR585 **Smartphone Forensic Analysis In-Depth™** | GASF
MACフォレンジック	FOR518 **Mac and iOS Forensic Analysis and Incident Response™** | GIME
LINUXフォレンジック	FOR577 **LINUX Incident Response and Threat Hunting™**

クラウドセキュリティの専門分野

特定の専門分野に関するスキル

アプリケーションセキュリティ	SEC522 **Application Security: Securing Web Apps, APIs, and Microservices™** | GWEB
クラウドペネトレーションテスト	SEC588 **Cloud Penetration Testing™** | GCPN
クラウドフォレンジック	FOR509 **Enterprise Cloud Forensics and Incident Response™** | GCFR
クラウドセキュリティの設計と実装	LDR520 **Cloud Security for Leaders™**

従来のサイバーセキュリティのスキルをクラウドセキュリティに応用するための方法を学ぶことで、適切な監視、検知、テスト、および防御をすることができます。

SANS SECURITY AWARENESS：業務別トレーニング

ICS技術者のためのトレーニング

産業用制御システム（ICS）をはじめとするOT（Operational Technology）技術者や運用担当者、その他OTに携わる方が重要システムに対するサイバーインシデントの防止、検知、対応を行うために必要なスキルを身につけることができます。

高度なセキュリティリーダーシップ

サイバーセキュリティに関する多様な専門業務を管理するための知識

設計と実装	LDR520 **Cloud Security for Leaders™**
プロジェクトマネジメント	LDR525 **Managing Cybersecurity Initiatives & Effective Communication™** | GCPM
インシデントレスポンス	LDR553 **Cyber Incident Management™**

SANS SECURITY AWARENESS：業務別トレーニング

リーダー・管理者のためのセキュリティの基礎

リーダーシップに焦点を当てた各種モジュールでは、管理職掌の方がチーム・部署を運用するために必要不可欠な、安全なデジタル環境を効率的に構築・運用・維持するためのノウハウを得られます。