# 実務に役立つ
# サイバーセキュリティの基礎

CompTIA
# CySA+
# テキスト
CS0-001対応


TAC

# 目　次

## 第4章　セキュリティマネジメント



## 第5章　インシデント対応



## 第6章　セキュリティツール

# 学習にあたり

## 本書の使い方

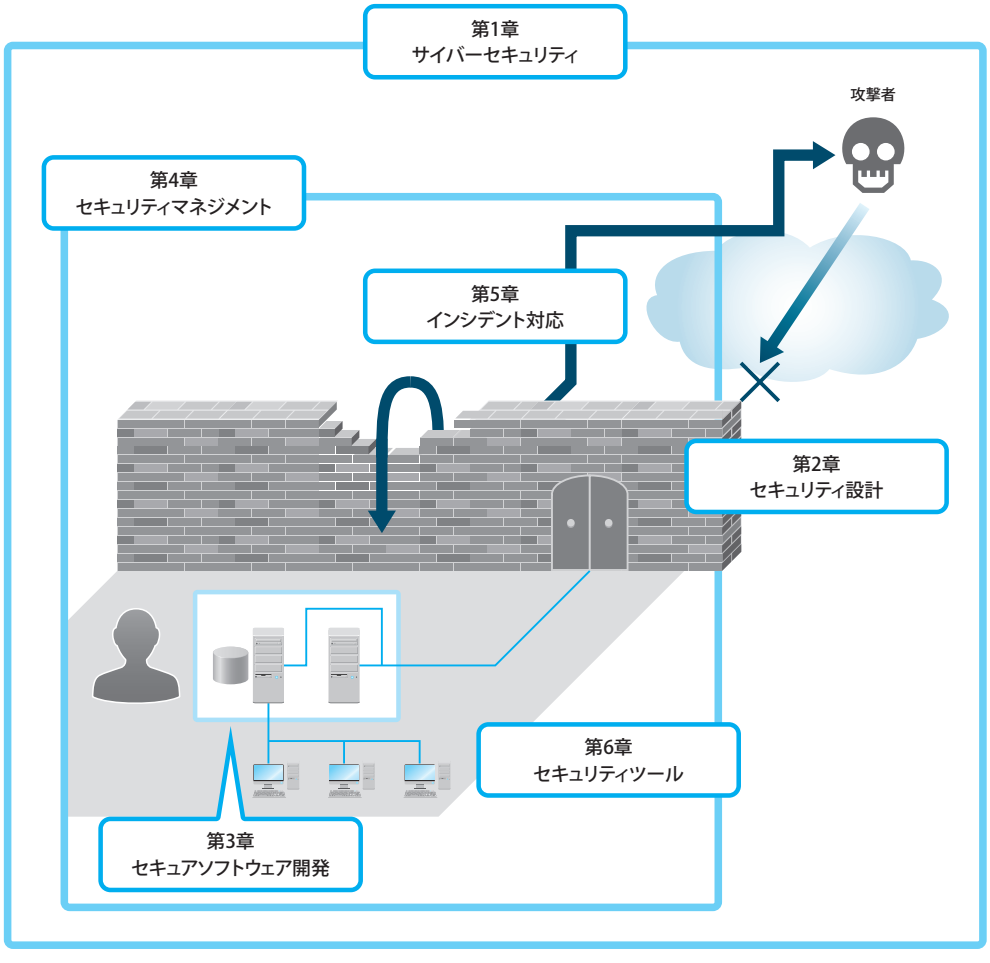
これからCySA+（CS0-001）試験を受験する方は、本書を最初から順番に読み進めていくことをおすすめします。興味のある章から読むこともできますが、本書は、知識を体系的にまとめ学習しやすいように構成されています。
本書は、CySA+（CS0-001）試験に必要な知識が得られるように構成されています。

## 本書の構成

・本書は章・節・項目に分けて構成されています。
・各章の初めには、「この章で学ぶこと」と、その章で学習する節タイトルが表記されています。「この章で学ぶこと」には章全体で学習する内容がまとめられているので、最初にその章で学習する内容の全体像を把握しましょう。
・各節の扉には、その節内で学ぶ項目のタイトルが表記されています。
・各項目の最初には、「学習ポイント」が挙げられています。ポイントをつかみ、効率よく学習を進めてください。
・重要な部分は、**太字**で表記されています。
・欄外には、本文中の※印のついた語句についての補足説明が記載されています。
・節ごとに穴埋め式の確認問題があります。学習した内容の習得度を確認できます。
・章末には選択式の章末問題があります。

※難しい英語名称は名称の後のカッコ（　）内に、読み方とフルスペルを表示しています。
　複数の読み方がある場合には、一般的なものを表示しました。

## CySA+ テキストの全体像



# 第1章

# サイバーセキュリティ

## この章で学ぶこと

サイバーセキュリティはハード面だけでなく、マネジメントも重要な要素となります。
従来はセキュリティ対策を行う場合にはIT部門が中心でしたが、インシデントが組織全体の問題となることが少なくなく、経営者層の関与が重要になってきます。
本章では、サイバーセキュリティの概要やアクセス制御で注意する点などについて学習します。

# 1-1

# サイバーセキュリティ

# 1-1-1 サイバーセキュリティとは

**学習ポイント**

サイバーセキュリティの概要が理解できるようになりましょう。

## 1 サイバーセキュリティとは

**サイバーセキュリティ**は人によっても定義が異なる言葉ですが、2014年11月に日本において「サイバーセキュリティ基本法」が成立され、次のように定義されました。

> 「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう」

端的にいうと、サイバーセキュリティは、情報システムや情報ネットワークにおいて、データを安全に保存、もしくはやり取りするための対策が講じられ、適切に管理されているということです。
つまり、サイバーセキュリティを確保するためには技術面だけでなく、マネジメント面にも注意する必要があります。

### ● セキュリティの被害

サイバー犯罪の被害が、報道で発表されるようなわかりやすい形で判明することは今では希少な事象となってきています。
以前は、いたずらを主な目的としたシステムの侵入などの被害報告でしたが、最近では、メールなどの手段を使ってフィッシングサイトへの誘導やWebサイトの改ざんによる被害が増えています。
以前のフィッシングサイトは、HTTPS対応していないものがほとんどでしたが、近ごろはHTTPS対応しているサイトもあるため、HTTPS対応でも注意する必要があります。そのほか、企業のような組織のシステムなどに侵入し、機密情報が少しずつ引き出される場合もあります。
侵入方法はわかりにくく偽装されているため、被害が判明するのに何か月もたってからということも少なくありません。
また、個人、組織ともに被害が増えてきているのはランサムウェア（身代金要求マルウェア）やメール詐欺による金銭の支払いです。この傾向は今後も続くと思われるため、日ごろから注意する必要があります。

## ● 攻撃者有利の状況

サイバーセキュリティは、攻撃者側が非常に有利な状況にあります。防御側はどれだけ守りを堅くしても1つの穴（脆弱性）が判明すれば侵入することができてしまうためです。

そのため、ある程度の守りをすることはもちろんですが、情報が盗まれても利用できないようにすることが大切です。

## ● セキュリティ対策の主体

かつてセキュリティに関する項目は、IT部門が主体となって進めるものでした。しかし、あらゆるシステムが接続された情報社会となった今、顧客情報が流出したといった事故が発生した場合、その組織の信頼性はすぐに回復できるものではなく、顧客からの信頼を失ってしまえば組織の存続も危うくなります。

現状でIT部門が取り得る対策を施しても情報が漏えいしてしまえば、主体がIT部門から**経営層**に変わらざるを得ないということです。

### ■経営層の関わり

経営層がセキュリティのことはわからないといってIT部門に丸投げしてしまうことがよくありますが、これからは経営的課題として経営層が主体となってサイバーセキュリティを高める努力をする必要があります。

たとえば、トレンドマイクロ社による調査では、2016年度にはセキュリティ侵害を受けた企業の平均被害額は2億円を超えています。この被害額は年々増加しています。

同調査では経営層にセキュリティに対する意識の有無を確認し、それがサイバーセキュリティ対策にどのような影響があるか調べています。

セキュリティが経営リスクと考えている経営層がいる組織と、そうとは思っていない経営層がいる組織では、サイバーセキュリティ投資額の差が2倍以上あることがわかっています。

投資額の大きさに比例して、技術的な安全性は高くなり、教育もよく行われているため、事故の発生が少なくなる傾向があります。

## ● セキュリティ確保の取り組み

企業などの組織におけるセキュリティの取り組みとして、**CSIRT**（シーサート：Computer Security Incident Response Team）や**CERT**（サート：Computer Emergency Response/Readiness Team）と呼ばれる組織を構築することが考えられます。

CSIRTやCERTが組織にあることで、セキュリティ問題が発生した場合に、すべての情報をここに集め、対策や対応策の実行を担うことになります。また、必要であれば外部との窓口としての役割もあります。日常業務としては、外部インシデント情報の収集と、その情報が自組織に影響を与えるかどうかの分析、一般的にセキュリティ対策と呼ばれるものが正常に動作しているかの確認といったものになります。

日本においては各企業にあるCSIRTやCERTと連携する組織として**JPCERT/CC**（ジェーピーサートシーシー：Japan Computer Emergency Response Team/Coordination Center）という団体があります。JPCERT/CCのような組織を利用して、最新情報を集め、連携することで、より企業におけるセキュリティを高めることができます。

# 1-1-2 脅威とは

**学習ポイント**

脅威の定義と具体例について理解できるようになりましょう。

## 1 脅威とは

**脅威**は、JIS Q 2700:2014では「システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。」とされています。具体的には、地震や火災といった現象、不正侵入や破壊といった行為、コンピューターウイルスやマルウェアといった手段、サイバーテロや業務妨害といった目的など、さまざまな視点で表現されます。

また、**インシデント**は情報セキュリティインシデントとして、「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。」とされています。具体的には、不正アクセスや情報漏えい、システム停止などといったものになります。

### ● 脅威の種類

脅威は既知のものと未知のものに分けることができます。既知の脅威は、対応策があるものがほとんどですが、未知の脅威は、その対応策が存在せず、対症療法的な対応になります。

**ゼロデイ攻撃**と呼ばれるソフトウェアなどの不具合を利用した攻撃は、未知の脅威が顕在化してしまったものです。

未知の脅威ではありませんが、最近では個人に対しては、インターネットバンキングやクレジットカード情報の不正利用、スマートフォンやスマートフォンアプリを狙った攻撃などが増えています。また、組織に対しては**APT**（エーピーティー：Advanced Persistent Threat）**攻撃**と呼ばれる攻撃対象が非常に限定された攻撃が行われることが多くなってきました。

APT攻撃は経営者や重要な情報を扱う人材に対して行われます。

| 種類 | 内容 |
|---|---|
| 破壊 | データの破壊、消去 |
| 漏えい | 機密データの漏えい |
| 改ざん | Webページの内容が不正に書き換えられる |
| サービス停止 | サービスの利用を不能にする |
| 不正利用 | 回線、サーバーなどのリソースが不正に利用される |
| 踏み台 | 他のサイトなどを攻撃する際の拠点にされる |

**脅威の例**

# 1-1-3 現状分析の方法

**学習ポイント**

サイバーセキュリティを確保するためには、現状のシステムがどのようになっているかわからなければ対策の打ちようがありません。ここでは現状を把握するための概要について理解できるようになりましょう。

## 1 現状把握の方法

組織が現在運用しているシステムの概要を資料がない状態から調査する場合には、次のような方法が考えられます。これらの方法は攻撃者がシステムの情報を入手する方法と同じです。通常であればシステムの詳細に関する文書があると思われるため、不足あるいは現状と異なる場合や情報を収集する際に利用することになります。
使用する代表的な方法としては、次のようなものがあります。

### ● トポロジーディスカバリー

**トポロジーディスカバリー**は、ネットワーク上の機器とその接続形態を自動検出することです。脆弱なネットワークを特定するには、まず組織ネットワークの全体のトポロジーを把握したうえで、個々のネットワークを分析します。

### ● OSフィンガープリント

**OSフィンガープリント**は、機器が送出するTCP/UDPパケットの特徴などからOSの種類、バージョン、デバイスの種類などを識別することです。

### ● サービスディスカバリー

**サービスディスカバリー**は、機器上で動作するサービスを自動検出することです。

### ● パケットキャプチャ

**パケットキャプチャ**は、ネットワーク上を流れる一つ一つのパケットを捕捉し、解析・集計することです。

### ● ログのレビュー

**ログ**を確認することで、現状のシステムに問題が発生していないか確認することができます。

### ● ルーター/ファイアウォールのACLレビュー

**ルーター**や**ファイアウォール**の**ACL**（エーシーエル：Access Control List）設定を確認することで、アクセスできるところと、アクセスできないところがわかります。

### メールハーベスティング

**メールハーベスティング**はメールアドレスを収集するために行う方法です。使用される方法としては自動生成したメールアドレスを送り、エラーにならないメールアドレスは有効として収集します。

### ソーシャルメディアプロファイリング

**ソーシャルメディアプロファイリング**は、SNS上の投稿などを収集・分析することにより自社製品やサービスの評価を確認し、市場調査を行うことができます。また、サーチエンジンを使用して情報を収集することもあります。

### ソーシャルエンジニアリング

**ソーシャルエンジニアリング**は、話術や会話の盗み聞き、盗み見などの「社会的（social）」な手段によってセキュリティ上、重要な情報を収集することをいいます。ソーシャルエンジニアリングは攻撃者もよく使用する方法です。

### DNSハーベスティング

**DNSハーベスティング**は、ドメイン内のIPアドレスを収集することです。組織内にあるデバイスのIPアドレスと情報を窃取することで、サーバーやクライアントといった調査対象を絞ることができます。

### フィッシング

**フィッシング**は、金融機関などを装ったメールを送りつけて個人情報を窃取する方法です。
問題が発生したといった、緊急性が高い文言が書かれている場合が多いため、思わずメールにあるURLをクリックして偽サイトに誘導され入力してしまう場合があります。

## 2 環境の違い

利用する環境によって守るための方法が異なります。

### 無線と有線の違い

**無線**とは無線通信を利用したものであり、**有線**とはイーサネットをはじめとした通信方法を利用したものです。
無線の場合は電波を利用するため、電波を送受信するアンテナと電波の広がりについて注意する必要があります。また、電波が届く範囲にいる場合に受信することができてしまうため、通信を秘匿しなければ誰でも内容を見ることができます。
有線で通信を行う場合には、通信を行うケーブルを配置する必要があります。ケーブルは、床を高床にして配置する、ネットワーク機器は鍵がかかる場所に配置するといったことが必要になります。このような対策を施さない場合は、ケーブルを傷つけてしまうことがあるばかりでなく、どこからでもケーブルに接続できてしまうため、盗聴機器を設置されてしまう可能性が高くなります。

## ● 仮想環境と物理環境の違い

**仮想環境**の場合、仮想化ソフトウェアに脆弱性がある際には、仮想環境から**物理環境**に問題が派生する場合があります。このような例としてはVM（ブイエム：Virtual Machine）エスケープ※があります。

また、再現なく仮想環境を増やしてしまうVMスプロールといった問題もあります。

仮想環境を設定する場合にも一定の基準を決め、それに従うようにする必要があります。不用意に仮想環境を追加して動作させると、サーバーが想定された性能を発揮することができなくなります。

外部で利用する仮想環境の場合は、専用ホストを用意することで安全性を高めることができます。

物理環境の場合もハードウェアやソフトウェアの脆弱性によって問題が発生する可能性があります。そのため、仮想環境か物理環境かにかかわらず、脆弱性情報を収集し、脆弱性をふさぐ作業が必要になります。

使用している環境が仮想環境であるか、物理環境であるか判断したい時にMACアドレスを見ると判断できる場合があります。

物理環境の場合は、各物理NICに割り当てられた一意なMACアドレスを使用します。

仮想環境のMACアドレスは、仮想マシンの作成時に仮想化ソフトごとに用意された任意のアドレスプールから割り当てられるため、値が近いMACアドレス構成になります。

## ● インターナルとエクスターナルの違い

基本的な考え方は、組織の**インターナル**（内部）と**エクスターナル**（外部）ともに変わりありません。最初にリソースに対して適切なアクセス権を設定し、認証を行い、必要がない通信は行えないようにします。また、通信内容を秘匿したい場合は暗号化を設定する必要があります。

## ● オンプレミスシステムとクラウドシステムの違い

**オンプレミスシステム**とは組織内で稼働しているシステムのことになります。管理はすべて組織内で行う必要があります。

**クラウドシステム**とは、クラウドベンダーが提供する共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることが可能なシステムです。

オンプレミスの場合は、セキュリティを確保するための対策を組織内で行う必要があります。また、組織内の物理的に閉じた環境に構築できるため、物理的セキュリティが確保しやすくなります。ただし、サーバーとデスクトップPCを比較した場合、サーバーのほうが機能が高く、セキュリティ面でも優れていることがほとんどです。

**VMエスケープ**
VM上で任意のプログラムを実行し、ホスト環境の制御を行うことができる。

クラウドの場合は通信経路の安全性の確保と、利用するサービスによってセキュリティ対策の方法は異なります。クラウドシステムを導入する場合は、組織内のITスキルレベルに応じて選択することが大切です。

## 3 ツール

現状の状況を確認する場合に使用するツールには、次のようなものがあります。
詳細については後の章で説明します。

### nmap

**nmap**は、ネットワーク調査およびセキュリティ監査を行うためのオープンソースのツールです。

### ホストスキャン

**ホストスキャン**は、Pingなどによりネットワーク上に存在するホストのIPアドレスを検索します。

### ネットワークマッピング

**ネットワークマッピング**は、ICMP、SNMP、WMI、CDPなどを使用し、ネットワーク上のデバイスとトポロジーを検出します。

### netstat

**netstat**はネットワークコマンドで、tcp/udpの稼働中のポートを表示します。

```
プロトコル  ローカル アドレス  外部アドレス        状態          PID
TCP  0.0.0.0:135          0.0.0.0:0          LISTENING      856
TCP  0.0.0.0:445          0.0.0.0:0          LISTENING      4
TCP  0.0.0.0:902          0.0.0.0:0          LISTENING      2380
TCP  0.0.0.0:912          0.0.0.0:0          LISTENING      2380
TCP  0.0.0.0:49153        0.0.0.0:0          LISTENING      912
TCP  0.0.0.0:49154        0.0.0.0:0          LISTENING      1100
TCP  0.0.0.0:49191        0.0.0.0:0          LISTENING      536
TCP  0.0.0.0:49192        0.0.0.0:0          LISTENING      528
TCP  0.0.0.0:49203        0.0.0.0:0          LISTENING      3016
TCP  127.0.0.1:5354       0.0.0.0:0          LISTENING      1992
TCP  172.25.6.113:139     0.0.0.0:0          LISTENING      4
TCP 172.25.6.113:50125   172.22.1.52:5274    ESTABLISHED    2280
```

**netstat**

### パケットアナライザー

**パケットアナライザー**は、ネットワーク上を流れるパケットを捕捉し、解析します。

## IDS/IPS

**IDS**（アイディーエス：Intrusion Detection System）とは、ネットワークを経由して行われる不正アクセスを自動的に発見して通知するツールです。

**IPS**（アイピーエス：Intrusion Prevention System）は、IDSのように不正アクセスを検知した段階で管理者に知らせ、管理者が対応をとるのではなく、不正アクセスを検知した時点で、あらかじめ管理者が定めた設定にしたがってシステム側で自動的に防御します。

## HIDS/NIDS

**HIDS**（エイチアイディーエス：Host Intrusion Detection System）は、OSが保持するログ情報、コマンド履歴、レジストリなどの情報を解析して脅威を検知し、その結果を管理者に通達します。

**HIPS**（エイチアイピーエス:Host Intrusion Prevention System）は、サーバーにインストールされ、不正アクセスの防御やアクセスログの改ざんなどを防ぎます。不正アクセスがあった場合に自動的にシャットダウンする機能もあります。

## ファイアウォールのルールベースとログ

**ファイアウォール**のフィルタリング設定やログを確認することで、どのようにアクセスが許可・遮断されているかがわかります。また、どのホストにアクセスしているかというような情報も把握することができます。

## syslog

**syslog**は、システム上のログメッセージをIPネットワーク上で転送するための標準規格です。

## 脆弱性スキャナ

**脆弱性スキャナ**は、さまざまな手法で脆弱性をスキャンするツールです。

## 確認問題　1-1 サイバーセキュリティ

次の［　　］に当てはまる言葉を答えてください。

□ 1.　［　①　］は、情報システムや情報ネットワークにおいて、データを安全に保存、もしくはやり取りするための対策が講じられ、適切に管理されているということ。

□ 2.　組織は、セキュリティの取り組みとして［　②　］や［　③　］を構築することがある。

□ 3.　日本において［　②　］や［　③　］と連携する［　④　］という団体がある。

□ 4.　［　⑤　］は、ネットワーク上の機器とその接続形態を自動検出することです。

□ 5.　［　⑥　］は、SNS上の投稿などを収集・分析することにより自社製品やサービスの評価を確認することです。

□ 6.　［　⑦　］は、金融機関などを装ったメールを送り付けて個人情報を窃取する方法です。

**答え**

①サイバーセキュリティ②CSIRT③CERT（②③順不同）④JPCERT/CC⑤トポロジーディスカバリー⑥ソーシャルメディアプロファイリング⑦フィッシング

## 章末問題

**Q1**

製品の出荷前に既知の公開された脆弱性が残存しないかどうかを確認するには、どれを使用しますか。

**a.** nmap
**b.** IPSのログ
**c.** ホストスキャン
**d.** 脆弱性スキャナ

**A d**

正解は「脆弱性スキャナ」です。
製品の出荷前に既知の公開された脆弱性が残存しないかどうかを確認するには、脆弱性スキャナを使用します。脆弱性スキャナは、既知の攻撃パターンに沿ったパケットを送信し、機器がそれらの攻撃へ脆弱でないかどうかを検出・レポートします。
nmapは、ネットワーク調査およびセキュリティ監査を行うためのオープンソースのツールです。
IPSは、ネットワーク上を流れるパケットが既知の攻撃パターンとマッチするかどうかをチェックし、マッチした場合は、パケットを遮断します。IPSのログでは、遮断されたパケットの記録から攻撃の兆候を確認することができます。
ホストスキャンは、Pingなどによりネットワーク上に存在するホストのIPアドレスを検索します。

**Q2**

パスワードリセットに関するIT部門への問い合わせの数を減らすには、どうすればよいですか。

**a.** 手動プロビジョニング
**b.** セルフサービスのリセット
**c.** フェデレーション認証
**d.** フルリセット

**A b**

正解は「セルフサービスのリセット」です。
セルフサービスのリセットにより、ユーザーは自分自身でパスワードをリセットできるため、IT部門へ問い合わせる必要がなくなります。
IT部門による手動リセット（手動プロビジョニング）やフルリセット（パスワード初期値）の場合、IT部門への問い合わせに対する負荷が高まります。
フェデレーションとは、異なるサービス間の連携を行うことです。
フェデレーション認証は、複数サービス間でのID連携を提供するため、ユーザーのパスワード管理負荷が軽減されます。