

# Implementing and Operating Cisco Security Core Technologies (350-701 Japanese Version)

1. Cisco Firepowerのセキュリティインテリジェンスポリシーを使用して、Firepowerブロックベースの2つの基準はどれですか。

A. URL

B. プロトコルID

C. IPアドレス

D. MACアドレス

E. ポート番号

**Answer(s):** A,C

---

2. どのネットワーク監視ソリューションがストリームを使用し、運用データをプッシュして、アクティビティのほぼリアルタイムのビューを提供しますか？

A. SNMP

B. SMTP

C. syslog

D. モデル駆動型テレメトリ

**Answer(s):** D

---

3. 最近の違反の後、組織は、永続性を取り戻す前に、フィッシングを使用してネットワークへの最初のアクセスを取得したと判断しました。フィッシング攻撃から得られた情報は、ユーザーが既知の悪意のあるWebサイトにアクセスした結果です。これが将来起こるのを防ぐために何をしなければなりませんか？

A. アクセスポリシーを変更します。

B. 識別プロファイルを変更します。

C. アウトバウンドマルウェアスキャンポリシーを変更する

D. Webプロキシ設定を変更する

**Answer(s): D**

---

4. パケットTTL、IP/TCPフラグ、ペイロード長など、フロー内で見られる変動をキャプチャするテレメトリデータはどれですか？

A. パケット間バリエーション

B. ソフトウェアパッケージのバリエーション

C. フローインサイトのバリエーション

D. プロセスの詳細のバリエーション

**Answer(s): A**

---

5. エンジニアは、サイト間VPNの実装にL2TPまたはGREoverIPsecのどちらを使用するかを決定しようとしています。何が解決されないに違いありませんか？

A. L2TPはIPパケットカプセル化プロトコルであり、GREoverIPsecはトンネリングプロトコルです。

B. L2TPはTCPポート47を使用し、GREoverIPsecはUDPポート1701を使用します。

C. GRE over IPsecは独自のヘッダーを追加しますが、L2TPは追加しません。

D. GRE over IPsecはスタンドアロンプロトコルとして使用できませんが、L2TPは使用できます。

**Answer(s): C**

---

6. システム管理者がWebトラフィックをWebセキュリティアプライアンスに透過的に送信する2つの方法はどれですか。

A. プロキシ設定をプッシュするようにActiveDirectoryグループポリシーを構成します

B. ネットワークインフラストラクチャでポリシーベースのルーティングを構成する

C. プロキシ自動設定ファイルを参照する

D. ウェブブラウザの設定でプロキシIPアドレスを設定します

E. Webキャッシュ通信プロトコルを使用する

**Answer(s): B,E**

---

7. VPNに接続していないリモートユーザーをフィッシング攻撃から保護するシスコのセキュリティソリューションはどれですか。

A. Cisco Stealthwatch

B. Cisco Umbrella

C. Cisco Firepower

D. NGIPS

**Answer(s): B**

---

8. 同じノード上のアプリケーションまたはコンテナ間の通信を制限するものは何ですか？

A. マイクロセグメンテーション

B. コンテナオーケストレーション

C. マイクロサービス

D. ソフトウェア定義のアクセス

**Answer(s): A**

---

9. エンドポイント用の十分に確立されたパッチソリューションがない場合、企業が脆弱になる2つのリスクはどれですか？（2つ選択してください）

A. exploits

B. ARP spoofing

C. denial-of-service attacks

D. malware

E. eavesdropping

**Answer(s): A,D**

---

10. 組織は、ユーザーのために AAA を実装しています。ネットワーク管理者が入力するすべてのコマンドについて、承認が検証されていることを確認する必要があります。この機能を提供するには、どのプロトコルを構成する必要がありますか？

A. イーポール

B. SSH

C. 半径

D. TACACS+

**Answer(s): D**

---

11. エンジニアがルーターに安全に接続しようとしていて、安全でないアルゴリズムが使用されないようにしたいと考えています。

- A. no iptelnetコマンドを使用してtelnetを無効にします。
- B. ip sshserverコマンドを使用してSSHサーバーを有効にします。
- C. ip ssh port22コマンドを使用してポートを設定します。
- D. crypto key generatersaコマンドを使用してRSAキーを生成します。

Answer(s): D

---

12. 直接接続がない場合でも、2台のコンピューター間でデータを交換するDNSの悪用のタイプはどれですか？

- A. マルウェアのインストール
- B. コマンドアンドコントロール通信
- C. ネットワークフットプリント
- D. データの漏えい

Answer(s): D

---

13. Cisco ISEとpxGridを相互に、および他の相互運用可能なセキュリティプラットフォームと統合するために使用される業界標準はどれですか。

- A. IEEE
- B. IETF
- C. NIST
- D. ANSI

**Answer(s): B**

---

14. ネットワークエンジニアがsnmp-serveruserasmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxxコマンドを入力し、SNMP情報を10.255.255.1のホストに送信する必要があります。この目標を達成するコマンドはどれですか？

A. 10.255.255.1バージョン3myv7内のsnmp-serverホスト

B. 10.255.255.1snmpv3asmith内のsnmp-serverホスト

C. 10.255.255.1バージョン3asmith内のsnmp-serverホスト

D. 10.255.255.1snmpv3myv7内のsnmp-serverホスト

**Answer(s): C**

---

15. 楕円曲線暗号は、現在のどの暗号化技術に取って代わることを目的とした、より強力であり効率的な暗号化方法ですか？

A. 3DES

B. RSA

C. DES

D. AES

**Answer(s): B**

---

16. フィッシング攻撃からユーザーを保護するエンドポイントソリューションはどれですか？

A. Cisco Identity Services Engine

B. ISEポスチャモジュールを備えたCisco AnyConnect

C. Cisco AnyConnect with NetworkAccessManagerモジュール

D. CiscoAnyConnectとUmbrellaRoamingSecurityモジュール

**Answer(s): D**

---

17. 攻撃者は、相互に通信している2つのホストの間に、どのタイプの攻撃でマシンを挿入しますか？

A. LDAPインジェクション

B. 中間者

C. クロスサイトスクリプティング

D. 安全でないAPI

**Answer(s): B**

---

18. Cisco Umbrellaは、クライアントが企業ネットワークの外部で動作している場合、どのようにクライアントを保護しますか？

A. DNSルックアップのレジストリを変更する

B. ActiveDirectoryグループポリシーを使用してCiscoUmbrellaDNSサーバーを適用する

C. CiscoUmbrellaローミングクライアントを使用する

D. 企業のネームサーバーにDNSクエリを強制する

**Answer(s): C**

---

19. Cisco Secure Endpoint と Cisco Umbrella Roaming Client の機能的な違いは何ですか？

A. セキュア エンドポイントはユーザを認証してセグメンテーションを提供し、Umbrella ローミングクライアントはVPN 接続のみを許可します。

B. セキュア エンドポイントはホスト上の悪意のあるアクティビティを停止して追跡し、Umbrella ローミング クライアントは URL ベースの脅威のみを追跡します。

C. Umbrella ローミング クライアントはユーザを認証してセグメンテーションを提供し、セキュア エンドポイントは VPN 接続のみを許可します。

D. Umbrella ローミング クライアントはホスト上の悪意のあるアクティビティを停止して追跡し、セキュア エンドポイントは URL ベースの脅威のみを追跡します。

**Answer(s): B**

---

20. 組織のネットワークに接続するマシンに、組織のマルウェアの発生を防ぐために推奨されるウイルス対策の定義とパッチがあることを保証するシスコのプラットフォームはどれですか。

A. Cisco WiSM

B. Cisco ESA

C. Cisco ISE

D. Cisco Prime Infrastructure

**Answer(s): C**

---