Q0001

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント1：ネットワークを分割し侵害範囲と不要な通信を制限する設計

次の説明に最も合う用語はどれか。ネットワークを分割し侵害範囲と不要な通信を制限する設計

A. VLAN
B. IDS
C. DDoS緩和
D. ネットワークセグメンテーション

答え・解説

Q0001 正答：D. ネットワークセグメンテーション

解説：ネットワークセグメンテーションは、ネットワークを分割し侵害範囲と不要な通信を制限する設計。ほかの選択肢は目的又は適用場面が異なる。

Q0002

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント2：ネットワークを分割し侵害範囲と不要な通信を制限する設計

ネットワークセグメンテーションの説明として最も適切なものはどれか。

A. ネットワークを分割し侵害範囲と不要な通信を制限する設計
B. スイッチ上で論理的にブロードキャストドメインを分割する技術
C. 不審な通信を検知して通知する仕組み
D. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策

答え・解説

Q0002 正答：A. ネットワークを分割し侵害範囲と不要な通信を制限する設計

解説：ネットワークセグメンテーションの要点は「ネットワークを分割し侵害範囲と不要な通信を制限する設計」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0003

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント3：ネットワークを分割し侵害範囲と不要な通信を制限する設計

用語と説明の組合せとして適切なものはどれか。論点は「ネットワークセグメンテーション」である。

A. VLAN：ネットワークを分割し侵害範囲と不要な通信を制限する設計
B. ネットワークセグメンテーション：ネットワークを分割し侵害範囲と不要な通信を制限する設計
C. IDS：ネットワークを分割し侵害範囲と不要な通信を制限する設計
D. DDoS緩和：ネットワークを分割し侵害範囲と不要な通信を制限する設計

答え・解説

Q0003 正答：B. ネットワークセグメンテーション：ネットワークを分割し侵害範囲と不要な通信を制限する設計

解説：正しい組合せは「ネットワークセグメンテーション：ネットワークを分割し侵害範囲と不要な通信を制限する設計」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0004

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント4：ネットワークを分割し侵害範囲と不要な通信を制限する設計

「ネットワークセグメンテーション」は、ネットワークを分割し侵害範囲と不要な通信を制限する設計。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。ネットワークセグメンテーションはネットワークを分割し侵害範囲と不要な通信を制限する設計。実務では対象、目的、前提条件を併せて確認する。

Q0005

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント5：ネットワークを分割し侵害範囲と不要な通信を制限する設計

組織が「ネットワークを分割し侵害範囲と不要な通信を制限する設計」ために採用すべき概念又は仕組みはどれか。

A. VLAN
B. IDS
C. DDoS緩和
D. ネットワークセグメンテーション

答え・解説

Q0005 正答：D. ネットワークセグメンテーション

解説：この目的に対応するのはネットワークセグメンテーションである。ネットワークを分割し侵害範囲と不要な通信を制限する設計という機能・考え方を持つためである。

Q0006

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント6：ネットワークを分割し侵害範囲と不要な通信を制限する設計

「ネットワークセグメンテーション」について、誤解を避けるための説明として最も適切なものはどれか。

A. ネットワークを分割し侵害範囲と不要な通信を制限する設計
B. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策
C. 不審な通信を検知して通知する仕組み
D. スイッチ上で論理的にブロードキャストドメインを分割する技術

答え・解説

Q0006 正答：A. ネットワークを分割し侵害範囲と不要な通信を制限する設計

解説：ネットワークセグメンテーションはネットワークを分割し侵害範囲と不要な通信を制限する設計。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント7：ネットワークを分割し侵害範囲と不要な通信を制限する設計

「ネットワークセグメンテーション」は、スイッチ上で論理的にブロードキャストドメインを分割する技術。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述はVLANの説明である。ネットワークセグメンテーションはネットワークを分割し侵害範囲と不要な通信を制限する設計。

Q0008

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント8：ネットワークを分割し侵害範囲と不要な通信を制限する設計

次の状況で中心となる論点はどれか。「ネットワークを分割し侵害範囲と不要な通信を制限する設計」ことが求められている。

A. IDS
B. DDoS緩和
C. ネットワークセグメンテーション
D. VLAN

答え・解説

Q0008 正答：C. ネットワークセグメンテーション

解説：中心となる論点はネットワークセグメンテーションである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0009

ネットワークセキュリティ
タグ：ネットワークセグメンテーション
用語：ネットワークセグメンテーションの確認ポイント9：ネットワークを分割し侵害範囲と不要な通信を制限する設計

「ネットワークを分割し侵害範囲と不要な通信を制限する設計」という特徴を持つものを選べ。

A. DDoS緩和
B. IDS
C. VLAN
D. ネットワークセグメンテーション

答え・解説

Q0009 正答：D. ネットワークセグメンテーション

解説：ネットワークセグメンテーションが該当する。定義はネットワークを分割し侵害範囲と不要な通信を制限する設計であり、他の候補とは機能が異なる。

Q0010

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント1：スイッチ上で論理的にブロードキャストドメインを分割する技術

次の説明に最も合う用語はどれか。スイッチ上で論理的にブロードキャストドメインを分割する技術

A. VLAN
B. ステートフルインスペクション
C. IPS
D. NAC

答え・解説

Q0010 正答：A. VLAN

解説：VLANは、スイッチ上で論理的にブロードキャストドメインを分割する技術。ほかの選択肢は目的又は適用場面が異なる。

Q0011

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント2：スイッチ上で論理的にブロードキャストドメインを分割する技術

VLANの説明として最も適切なものはどれか。

A. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
B. スイッチ上で論理的にブロードキャストドメインを分割する技術
C. 不審な通信を検知し遮断まで行う仕組み
D. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み

答え・解説

Q0011 正答：B. スイッチ上で論理的にブロードキャストドメインを分割する技術

解説：VLANの要点は「スイッチ上で論理的にブロードキャストドメインを分割する技術」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0012

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント3：スイッチ上で論理的にブロードキャストドメインを分割する技術

用語と説明の組合せとして適切なものはどれか。論点は「VLAN」である。

A. ステートフルインスペクション：スイッチ上で論理的にブロードキャストドメインを分割する技術
B. IPS：スイッチ上で論理的にブロードキャストドメインを分割する技術
C. VLAN：スイッチ上で論理的にブロードキャストドメインを分割する技術
D. NAC：スイッチ上で論理的にブロードキャストドメインを分割する技術

答え・解説

Q0012 正答：C. VLAN：スイッチ上で論理的にブロードキャストドメインを分割する技術

解説：正しい組合せは「VLAN：スイッチ上で論理的にブロードキャストドメインを分割する技術」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0013

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント4：スイッチ上で論理的にブロードキャストドメインを分割する技術
「VLAN」は、スイッチ上で論理的にブロードキャストドメインを分割する技術。

A. ○
B. ×

答え・解説

Q0013 正答：○
解説：正しい。VLANはスイッチ上で論理的にブロードキャストドメインを分割する技術。実務では対象、目的、前提条件を併せて確認する。

Q0014

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント5：スイッチ上で論理的にブロードキャストドメインを分割する技術
組織が「スイッチ上で論理的にブロードキャストドメインを分割する技術」ために採用すべき概念又は仕組みはどれか。

A. VLAN
B. ステートフルインスペクション
C. IPS
D. NAC

答え・解説

Q0014 正答：A. VLAN
解説：この目的に対応するのはVLANである。スイッチ上で論理的にブロードキャストドメインを分割する技術という機能・考え方を持つためである。

Q0015

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント6：スイッチ上で論理的にブロードキャストドメインを分割する技術

「VLAN」について、誤解を避けるための説明として最も適切なものはどれか。

A. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み
B. スイッチ上で論理的にブロードキャストドメインを分割する技術
C. 不審な通信を検知し遮断まで行う仕組み
D. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

答え・解説

Q0015 正答：B. スイッチ上で論理的にブロードキャストドメインを分割する技術

解説：VLANはスイッチ上で論理的にブロードキャストドメインを分割する技術。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0016

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント7：スイッチ上で論理的にブロードキャストドメインを分割する技術

「VLAN」は、通信状態を追跡しセッション文脈に基づいてパケットを判定する方式。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述はステートフルインスペクションの説明である。VLANはスイッチ上で論理的にブロードキャストドメインを分割する技術。

Q0017

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント8：スイッチ上で論理的にブロードキャストドメインを分割する技術

次の状況で中心となる論点はどれか。「スイッチ上で論理的にブロードキャストドメインを分割する技術」ことが求められている。

A. IPS
B. NAC
C. ステートフルインスペクション
D. VLAN

答え・解説

Q0017 正答：D. VLAN

解説：中心となる論点はVLANである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0018

ネットワークセキュリティ
タグ：VLAN
用語：VLANの確認ポイント9：スイッチ上で論理的にブロードキャストドメインを分割する技術

「スイッチ上で論理的にブロードキャストドメインを分割する技術」という特徴を持つものを選べ。

A. VLAN
B. NAC
C. IPS
D. ステートフルインスペクション

答え・解説

Q0018 正答：A. VLAN

解説：VLANが該当する。定義はスイッチ上で論理的にブロードキャストドメインを分割する技術であり、他の候補とは機能が異なる。

Q0019

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント1：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

次の説明に最も合う用語はどれか。通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

A. IDS
B. ステートフルインスペクション
C. IPsec
D. リバースプロキシ

答え・解説

Q0019 正答：B. ステートフルインスペクション

解説：ステートフルインスペクションは、通信状態を追跡しセッション文脈に基づいてパケットを判定する方式。ほかの選択肢は目的又は適用場面が異なる。

Q0020

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント2：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

ステートフルインスペクションの説明として最も適切なものはどれか。

A. 不審な通信を検知して通知する仕組み
B. IP層で認証・完全性・暗号化を提供するプロトコル群
C. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
D. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

答え・解説

Q0020 正答：C. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

解説：ステートフルインスペクションの要点は「通信状態を追跡しセッション文脈に基づいてパケットを判定する方式」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0021

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント3：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

用語と説明の組合せとして適切なものはどれか。論点は「ステートフルインスペクション」である。

A. IDS：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
B. IPsec：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
C. リバースプロキシ：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
D. ステートフルインスペクション：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

答え・解説

Q0021 正答：D. ステートフルインスペクション：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

解説：正しい組合せは「ステートフルインスペクション：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0022

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント4：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

「ステートフルインスペクション」は、通信状態を追跡しセッション文脈に基づいてパケットを判定する方式。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。ステートフルインスペクションは通信状態を追跡しセッション文脈に基づいてパケットを判定する方式。実務では対象、目的、前提条件を併せて確認する。

Q0023

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント5：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

組織が「通信状態を追跡しセッション文脈に基づいてパケットを判定する方式」ために採用すべき概念又は仕組みはどれか。

A. IDS
B. ステートフルインスペクション
C. IPsec
D. リバースプロキシ

答え・解説

Q0023 正答：B. ステートフルインスペクション

解説：この目的に対応するのはステートフルインスペクションである。通信状態を追跡しセッション文脈に基づいてパケットを判定する方式という機能・考え方を持つためである。

Q0024

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント6：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

「ステートフルインスペクション」について、誤解を避けるための説明として最も適切なものはどれか。

A. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
B. IP層で認証・完全性・暗号化を提供するプロトコル群
C. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
D. 不審な通信を検知して通知する仕組み

答え・解説

Q0024 正答：C. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

解説：ステートフルインスペクションは通信状態を追跡しセッション文脈に基づいてパケットを判定する方式。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0025

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント7：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

「ステートフルインスペクション」は、不審な通信を検知して通知する仕組み。

A. ○
B. ×

答え・解説

Q0025 正答：×

解説：誤り。記述はIDSの説明である。ステートフルインスペクションは通信状態を追跡しセッション文脈に基づいてパケットを判定する方式。

Q0026

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント8：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

次の状況で中心となる論点はどれか。「通信状態を追跡しセッション文脈に基づいてパケットを判定する方式」ことが求められている。

A. ステートフルインスペクション
B. IPsec
C. リバースプロキシ
D. IDS

答え・解説

Q0026 正答：A. ステートフルインスペクション

解説：中心となる論点はステートフルインスペクションである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0027

ネットワークセキュリティ
タグ：ステートフルインスペクション
用語：ステートフルインスペクションの確認ポイント9：通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

「通信状態を追跡しセッション文脈に基づいてパケットを判定する方式」という特徴を持つものを選べ。

A. リバースプロキシ
B. ステートフルインスペクション
C. IPsec
D. IDS

答え・解説

Q0027 正答：B. ステートフルインスペクション

解説：ステートフルインスペクションが該当する。定義は通信状態を追跡しセッション文脈に基づいてパケットを判定する方式であり、他の候補とは機能が異なる。

Q0028

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント1：不審な通信を検知して通知する仕組み

次の説明に最も合う用語はどれか。不審な通信を検知して通知する仕組み

A. IPS
B. DNSSEC
C. IDS
D. ネットワークセグメンテーション

答え・解説

Q0028 正答：C. IDS

解説：IDSは、不審な通信を検知して通知する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0029

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント2：不審な通信を検知して通知する仕組み

IDSの説明として最も適切なものはどれか。

A. 不審な通信を検知し遮断まで行う仕組み
B. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
C. ネットワークを分割し侵害範囲と不要な通信を制限する設計
D. 不審な通信を検知して通知する仕組み

答え・解説

Q0029 正答：D. 不審な通信を検知して通知する仕組み

解説：IDSの要点は「不審な通信を検知して通知する仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0030

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント3：不審な通信を検知して通知する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「IDS」である。

A. IDS：不審な通信を検知して通知する仕組み
B. IPS：不審な通信を検知して通知する仕組み
C. DNSSEC：不審な通信を検知して通知する仕組み
D. ネットワークセグメンテーション：不審な通信を検知して通知する仕組み

答え・解説

Q0030 正答：A. IDS：不審な通信を検知して通知する仕組み

解説：正しい組合せは「IDS：不審な通信を検知して通知する仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0031

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント4：不審な通信を検知して通知する仕組み

「IDS」は、不審な通信を検知して通知する仕組み。

A. ○
B. ×

答え・解説

Q0031 正答：○

解説：正しい。IDSは不審な通信を検知して通知する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0032

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント5：不審な通信を検知して通知する仕組み

組織が「不審な通信を検知して通知する仕組み」ために採用すべき概念又は仕組みはどれか。

A. IPS
B. DNSSEC
C. IDS
D. ネットワークセグメンテーション

答え・解説

Q0032 正答：C. IDS

解説：この目的に対応するのはIDSである。不審な通信を検知して通知する仕組みという機能・考え方を持つためである。

Q0033

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント6：不審な通信を検知して通知する仕組み

「IDS」について、誤解を避けるための説明として最も適切なものはどれか。

A. ネットワークを分割し侵害範囲と不要な通信を制限する設計
B. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
C. 不審な通信を検知し遮断まで行う仕組み
D. 不審な通信を検知して通知する仕組み

答え・解説

Q0033 正答：D. 不審な通信を検知して通知する仕組み

解説：IDSは不審な通信を検知して通知する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0034

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント7：不審な通信を検知して通知する仕組み

「IDS」は、不審な通信を検知し遮断まで行う仕組み。

A. ○
B. ×

答え・解説

Q0034 正答：×

解説：誤り。記述はIPSの説明である。IDSは不審な通信を検知して通知する仕組み。

Q0035

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント8：不審な通信を検知して通知する仕組み

次の状況で中心となる論点はどれか。「不審な通信を検知して通知する仕組み」ことが求められている。

A. DNSSEC
B. IDS
C. ネットワークセグメンテーション
D. IPS

答え・解説

Q0035 正答：B. IDS

解説：中心となる論点はIDSである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0036

ネットワークセキュリティ
タグ：IDS
用語：IDSの確認ポイント9：不審な通信を検知して通知する仕組み

「不審な通信を検知して通知する仕組み」という特徴を持つものを選べ。

A. ネットワークセグメンテーション
B. DNSSEC
C. IDS
D. IPS

答え・解説

Q0036 正答：C. IDS

解説：IDSが該当する。定義は不審な通信を検知して通知する仕組みであり、他の候補とは機能が異なる。

Q0037

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント1：不審な通信を検知し遮断まで行う仕組み

次の説明に最も合う用語はどれか。不審な通信を検知し遮断まで行う仕組み

A. IPsec
B. DDoS緩和
C. VLAN
D. IPS

答え・解説

Q0037 正答：D. IPS

解説：IPSは、不審な通信を検知し遮断まで行う仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0038

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント2：不審な通信を検知し遮断まで行う仕組み

IPSの説明として最も適切なものはどれか。

A. 不審な通信を検知し遮断まで行う仕組み
B. IP層で認証・完全性・暗号化を提供するプロトコル群
C. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策
D. スイッチ上で論理的にブロードキャストドメインを分割する技術

答え・解説

Q0038 正答：A. 不審な通信を検知し遮断まで行う仕組み

解説：IPSの要点は「不審な通信を検知し遮断まで行う仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0039

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント3：不審な通信を検知し遮断まで行う仕組み

用語と説明の組合せとして適切なものはどれか。論点は「IPS」である。

A. IPsec：不審な通信を検知し遮断まで行う仕組み
B. IPS：不審な通信を検知し遮断まで行う仕組み
C. DDoS緩和：不審な通信を検知し遮断まで行う仕組み
D. VLAN：不審な通信を検知し遮断まで行う仕組み

答え・解説

Q0039 正答：B. IPS：不審な通信を検知し遮断まで行う仕組み

解説：正しい組合せは「IPS：不審な通信を検知し遮断まで行う仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0040

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント4：不審な通信を検知し遮断まで行う仕組み

「IPS」は、不審な通信を検知し遮断まで行う仕組み。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。IPSは不審な通信を検知し遮断まで行う仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0041

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント5：不審な通信を検知し遮断まで行う仕組み

組織が「不審な通信を検知し遮断まで行う仕組み」ために採用すべき概念又は仕組みはどれか。

A. IPsec
B. DDoS緩和
C. VLAN
D. IPS

答え・解説

Q0041 正答：D. IPS

解説：この目的に対応するのはIPSである。不審な通信を検知し遮断まで行う仕組みという機能・考え方を持つためである。

Q0042

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント6：不審な通信を検知し遮断まで行う仕組み

「IPS」について、誤解を避けるための説明として最も適切なものはどれか。

A. 不審な通信を検知し遮断まで行う仕組み
B. スイッチ上で論理的にブロードキャストドメインを分割する技術
C. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策
D. IP層で認証・完全性・暗号化を提供するプロトコル群

答え・解説

Q0042 正答：A. 不審な通信を検知し遮断まで行う仕組み

解説：IPSは不審な通信を検知し遮断まで行う仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0043

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント7：不審な通信を検知し遮断まで行う仕組み

「IPS」は、IP層で認証・完全性・暗号化を提供するプロトコル群。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述はIPsecの説明である。IPSは不審な通信を検知し遮断まで行う仕組み。

Q0044

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント8：不審な通信を検知し遮断まで行う仕組み

次の状況で中心となる論点はどれか。「不審な通信を検知し遮断まで行う仕組み」ことが求められている。

A. DDoS緩和
B. VLAN
C. IPS
D. IPsec

答え・解説

Q0044 正答：C. IPS

解説：中心となる論点はIPSである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0045

ネットワークセキュリティ
タグ：IPS
用語：IPSの確認ポイント9：不審な通信を検知し遮断まで行う仕組み

「不審な通信を検知し遮断まで行う仕組み」という特徴を持つものを選べ。

A. VLAN
B. DDoS緩和
C. IPsec
D. IPS

答え・解説

Q0045 正答：D. IPS

解説：IPSが該当する。定義は不審な通信を検知し遮断まで行う仕組みであり、他の候補とは機能が異なる。

Q0046

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント1：IP層で認証・完全性・暗号化を提供するプロトコル群

次の説明に最も合う用語はどれか。IP層で認証・完全性・暗号化を提供するプロトコル群

A. IPsec
B. DNSSEC
C. NAC
D. ステートフルインスペクション

答え・解説

Q0046 正答：A. IPsec

解説：IPsecは、IP層で認証・完全性・暗号化を提供するプロトコル群。ほかの選択肢は目的又は適用場面が異なる。

Q0047

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント2：IP層で認証・完全性・暗号化を提供するプロトコル群

IPsecの説明として最も適切なものはどれか。

A. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
B. IP層で認証・完全性・暗号化を提供するプロトコル群
C. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み
D. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式

答え・解説

Q0047 正答：B. IP層で認証・完全性・暗号化を提供するプロトコル群

解説：IPsecの要点は「IP層で認証・完全性・暗号化を提供するプロトコル群」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0048

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント3：IP層で認証・完全性・暗号化を提供するプロトコル群

用語と説明の組合せとして適切なものはどれか。論点は「IPsec」である。

A. DNSSEC：IP層で認証・完全性・暗号化を提供するプロトコル群
B. NAC：IP層で認証・完全性・暗号化を提供するプロトコル群
C. IPsec：IP層で認証・完全性・暗号化を提供するプロトコル群
D. ステートフルインスペクション：IP層で認証・完全性・暗号化を提供するプロトコル群

答え・解説

Q0048 正答：C. IPsec：IP層で認証・完全性・暗号化を提供するプロトコル群

解説：正しい組合せは「IPsec：IP層で認証・完全性・暗号化を提供するプロトコル群」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0049

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント4：IP層で認証・完全性・暗号化を提供するプロトコル群

「IPsec」は、IP層で認証・完全性・暗号化を提供するプロトコル群。

A. ○
B. ×

答え・解説

Q0049 正答：○

解説：正しい。IPsecはIP層で認証・完全性・暗号化を提供するプロトコル群。実務では対象、目的、前提条件を併せて確認する。

Q0050

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント5：IP層で認証・完全性・暗号化を提供するプロトコル群

組織が「IP層で認証・完全性・暗号化を提供するプロトコル群」ために採用すべき概念又は仕組みはどれか。

A. IPsec
B. DNSSEC
C. NAC
D. ステートフルインスペクション

答え・解説

Q0050 正答：A. IPsec

解説：この目的に対応するのはIPsecである。IP層で認証・完全性・暗号化を提供するプロトコル群という機能・考え方を持つためである。

Q0051

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント6：IP層で認証・完全性・暗号化を提供するプロトコル群

「IPsec」について、誤解を避けるための説明として最も適切なものはどれか。

A. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
B. IP層で認証・完全性・暗号化を提供するプロトコル群
C. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み
D. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

答え・解説

Q0051 正答：B. IP層で認証・完全性・暗号化を提供するプロトコル群

解説：IPsecはIP層で認証・完全性・暗号化を提供するプロトコル群。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0052

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント7：IP層で認証・完全性・暗号化を提供するプロトコル群

「IPsec」は、DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み。

A. ○
B. ×

答え・解説

Q0052 正答：×

解説：誤り。記述はDNSSECの説明である。IPsecはIP層で認証・完全性・暗号化を提供するプロトコル群。

Q0053

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント8：IP層で認証・完全性・暗号化を提供するプロトコル群

次の状況で中心となる論点はどれか。「IP層で認証・完全性・暗号化を提供するプロトコル群」ことが求められている。

A. NAC
B. ステートフルインスペクション
C. DNSSEC
D. IPsec

答え・解説

Q0053 正答：D. IPsec

解説：中心となる論点はIPsecである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0054

ネットワークセキュリティ
タグ：IPsec
用語：IPsecの確認ポイント9：IP層で認証・完全性・暗号化を提供するプロトコル群

「IP層で認証・完全性・暗号化を提供するプロトコル群」という特徴を持つものを選べ。

A. IPsec
B. ステートフルインスペクション
C. NAC
D. DNSSEC

答え・解説

Q0054 正答：A. IPsec

解説：IPsecが該当する。定義はIP層で認証・完全性・暗号化を提供するプロトコル群であり、他の候補とは機能が異なる。

Q0055

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント1：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

次の説明に最も合う用語はどれか。DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

A. DDoS緩和
B. DNSSEC
C. リバースプロキシ
D. IDS

答え・解説

Q0055 正答：B. DNSSEC

解説：DNSSECは、DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0056

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント2：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

DNSSECの説明として最も適切なものはどれか。

A. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策
B. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
C. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
D. 不審な通信を検知して通知する仕組み

答え・解説

Q0056 正答：C. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

解説：DNSSECの要点は「DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0057

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント3：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「DNSSEC」である。

A. DDoS緩和：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
B. リバースプロキシ：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
C. IDS：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
D. DNSSEC：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

答え・解説

Q0057 正答：D. DNSSEC：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

解説：正しい組合せは「DNSSEC：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0058

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント4：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

「DNSSEC」は、DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。DNSSECはDNS応答へデジタル署名を付け真正性と完全性を検証する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0059

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント5：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

組織が「DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み」ために採用すべき概念又は仕組みはどれか。

A. DDoS緩和
B. DNSSEC
C. リバースプロキシ
D. IDS

答え・解説

Q0059 正答：B. DNSSEC
解説：この目的に対応するのはDNSSECである。DNS応答へデジタル署名を付け真正性と完全性を検証する仕組みという機能・考え方を持つためである。

Q0060

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント6：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

「DNSSEC」について、誤解を避けるための説明として最も適切なものはどれか。

A. 不審な通信を検知して通知する仕組み
B. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
C. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
D. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策

答え・解説

Q0060 正答：C. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
解説：DNSSECはDNS応答へデジタル署名を付け真正性と完全性を検証する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0061

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント7：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

「DNSSEC」は、分散した大量通信を吸収・選別しサービス停止を防ぐ対策。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述はDDoS緩和の説明である。DNSSECはDNS応答へデジタル署名を付け真正性と完全性を検証する仕組み。

Q0062

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント8：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

次の状況で中心となる論点はどれか。「DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み」ことが求められている。

A. DNSSEC
B. リバースプロキシ
C. IDS
D. DDoS緩和

答え・解説

Q0062 正答：A. DNSSEC

解説：中心となる論点はDNSSECである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0063

ネットワークセキュリティ
タグ：DNSSEC
用語：DNSSECの確認ポイント9：DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

「DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み」という特徴を持つものを選べ。

A. IDS
B. DNSSEC
C. リバースプロキシ
D. DDoS緩和

答え・解説

Q0063 正答：B. DNSSEC

解説：DNSSECが該当する。定義はDNS応答へデジタル署名を付け真正性と完全性を検証する仕組みであり、他の候補とは機能が異なる。

Q0064

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント1：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

次の説明に最も合う用語はどれか。分散した大量通信を吸収・選別しサービス停止を防ぐ対策

A. NAC
B. ネットワークセグメンテーション
C. DDoS緩和
D. IPS

答え・解説

Q0064 正答：C. DDoS緩和

解説：DDoS緩和は、分散した大量通信を吸収・選別しサービス停止を防ぐ対策。ほかの選択肢は目的又は適用場面が異なる。

Q0065

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント2：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

DDoS緩和の説明として最も適切なものはどれか。

A. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み
B. ネットワークを分割し侵害範囲と不要な通信を制限する設計
C. 不審な通信を検知し遮断まで行う仕組み
D. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策

答え・解説

Q0065 正答：D. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策

解説：DDoS緩和の要点は「分散した大量通信を吸収・選別しサービス停止を防ぐ対策」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0066

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント3：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

用語と説明の組合せとして適切なものはどれか。論点は「DDoS緩和」である。

A. DDoS緩和：分散した大量通信を吸収・選別しサービス停止を防ぐ対策
B. NAC：分散した大量通信を吸収・選別しサービス停止を防ぐ対策
C. ネットワークセグメンテーション：分散した大量通信を吸収・選別しサービス停止を防ぐ対策
D. IPS：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

答え・解説

Q0066 正答：A. DDoS緩和：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

解説：正しい組合せは「DDoS緩和：分散した大量通信を吸収・選別しサービス停止を防ぐ対策」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0067

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント4：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

「DDoS緩和」は、分散した大量通信を吸収・選別しサービス停止を防ぐ対策。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。DDoS緩和は分散した大量通信を吸収・選別しサービス停止を防ぐ対策。実務では対象、目的、前提条件を併せて確認する。

Q0068

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント5：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

組織が「分散した大量通信を吸収・選別しサービス停止を防ぐ対策」ために採用すべき概念又は仕組みはどれか。

A. NAC
B. ネットワークセグメンテーション
C. DDoS緩和
D. IPS

答え・解説

Q0068 正答：C. DDoS緩和

解説：この目的に対応するのはDDoS緩和である。分散した大量通信を吸収・選別しサービス停止を防ぐ対策という機能・考え方を持つためである。

Q0069

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント6：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

「DDoS緩和」について、誤解を避けるための説明として最も適切なものはどれか。

A. 不審な通信を検知し遮断まで行う仕組み
B. ネットワークを分割し侵害範囲と不要な通信を制限する設計
C. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み
D. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策

答え・解説

Q0069 正答：D. 分散した大量通信を吸収・選別しサービス停止を防ぐ対策

解説：DDoS緩和は分散した大量通信を吸収・選別しサービス停止を防ぐ対策。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0070

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント7：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

「DDoS緩和」は、端末の利用者や状態を確認してネットワーク接続を制御する仕組み。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述はNACの説明である。DDoS緩和は分散した大量通信を吸収・選別しサービス停止を防ぐ対策。

Q0071

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント8：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

次の状況で中心となる論点はどれか。「分散した大量通信を吸収・選別しサービス停止を防ぐ対策」ことが求められている。

A. ネットワークセグメンテーション
B. DDoS緩和
C. IPS
D. NAC

答え・解説

Q0071 正答：B. DDoS緩和

解説：中心となる論点はDDoS緩和である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0072

ネットワークセキュリティ
タグ：DDoS緩和
用語：DDoS緩和の確認ポイント9：分散した大量通信を吸収・選別しサービス停止を防ぐ対策

「分散した大量通信を吸収・選別しサービス停止を防ぐ対策」という特徴を持つものを選べ。

A. IPS
B. ネットワークセグメンテーション
C. DDoS緩和
D. NAC

答え・解説

Q0072 正答：C. DDoS緩和

解説：DDoS緩和が該当する。定義は分散した大量通信を吸収・選別しサービス停止を防ぐ対策であり、他の候補とは機能が異なる。

Q0073

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント1：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

次の説明に最も合う用語はどれか。端末の利用者や状態を確認してネットワーク接続を制御する仕組み

A. リバースプロキシ
B. VLAN
C. IPsec
D. NAC

答え・解説

Q0073 正答：D. NAC

解説：NACは、端末の利用者や状態を確認してネットワーク接続を制御する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0074

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント2：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

NACの説明として最も適切なものはどれか。

A. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み
B. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
C. スイッチ上で論理的にブロードキャストドメインを分割する技術
D. IP層で認証・完全性・暗号化を提供するプロトコル群

答え・解説

Q0074 正答：A. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み

解説：NACの要点は「端末の利用者や状態を確認してネットワーク接続を制御する仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0075

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント3：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「NAC」である。

A. リバースプロキシ：端末の利用者や状態を確認してネットワーク接続を制御する仕組み
B. NAC：端末の利用者や状態を確認してネットワーク接続を制御する仕組み
C. VLAN：端末の利用者や状態を確認してネットワーク接続を制御する仕組み
D. IPsec：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

答え・解説

Q0075 正答：B. NAC：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

解説：正しい組合せは「NAC：端末の利用者や状態を確認してネットワーク接続を制御する仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0076

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント4：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

「NAC」は、端末の利用者や状態を確認してネットワーク接続を制御する仕組み。

A. ○
B. ×

答え・解説

Q0076 正答：○

解説：正しい。NACは端末の利用者や状態を確認してネットワーク接続を制御する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0077

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント5：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

組織が「端末の利用者や状態を確認してネットワーク接続を制御する仕組み」ために採用すべき概念又は仕組みはどれか。

A. リバースプロキシ
B. VLAN
C. IPsec
D. NAC

答え・解説

Q0077 正答：D. NAC

解説：この目的に対応するのはNACである。端末の利用者や状態を確認してネットワーク接続を制御する仕組みという機能・考え方を持つためである。

Q0078

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント6：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

「NAC」について、誤解を避けるための説明として最も適切なものはどれか。

A. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み
B. IP層で認証・完全性・暗号化を提供するプロトコル群
C. スイッチ上で論理的にブロードキャストドメインを分割する技術
D. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

答え・解説

Q0078 正答：A. 端末の利用者や状態を確認してネットワーク接続を制御する仕組み

解説：NACは端末の利用者や状態を確認してネットワーク接続を制御する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0079

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント7：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

「NAC」は、外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み。

A. ○
B. ×

答え・解説

Q0079 正答：×

解説：誤り。記述はリバースプロキシの説明である。NACは端末の利用者や状態を確認してネットワーク接続を制御する仕組み。

Q0080

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント8：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

次の状況で中心となる論点はどれか。「端末の利用者や状態を確認してネットワーク接続を制御する仕組み」ことが求められている。

A. VLAN
B. IPsec
C. NAC
D. リバースプロキシ

答え・解説

Q0080 正答：C. NAC

解説：中心となる論点はNACである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0081

ネットワークセキュリティ
タグ：NAC
用語：NACの確認ポイント9：端末の利用者や状態を確認してネットワーク接続を制御する仕組み

「端末の利用者や状態を確認してネットワーク接続を制御する仕組み」という特徴を持つものを選べ。

A. IPsec
B. VLAN
C. リバースプロキシ
D. NAC

答え・解説

Q0081 正答：D. NAC

解説：NACが該当する。定義は端末の利用者や状態を確認してネットワーク接続を制御する仕組みであり、他の候補とは機能が異なる。

Q0082

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント1：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

次の説明に最も合う用語はどれか。外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

A. リバースプロキシ
B. ネットワークセグメンテーション
C. ステートフルインスペクション
D. DNSSEC

答え・解説

Q0082 正答：A. リバースプロキシ

解説：リバースプロキシは、外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0083

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント2：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

リバースプロキシの説明として最も適切なものはどれか。

A. ネットワークを分割し侵害範囲と不要な通信を制限する設計
B. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
C. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
D. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み

答え・解説

Q0083 正答：B. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

解説：リバースプロキシの要点は「外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0084

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント3：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

用語と説明の組合せとして適切なものはどれか。論点は「リバースプロキシ」である。

A. ネットワークセグメンテーション：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
B. ステートフルインスペクション：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
C. リバースプロキシ：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
D. DNSSEC：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

答え・解説

Q0084 正答：C. リバースプロキシ：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

解説：正しい組合せは「リバースプロキシ：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0085

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント4：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

「リバースプロキシ」は、外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。リバースプロキシは外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0086

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント5：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

組織が「外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み」ために採用すべき概念又は仕組みはどれか。

A. リバースプロキシ
B. ネットワークセグメンテーション
C. ステートフルインスペクション
D. DNSSEC

答え・解説

Q0086 正答：A. リバースプロキシ

解説：この目的に対応するのはリバースプロキシである。外部要求を受けて内部サーバへ中継し内部構成を隠す仕組みという機能・考え方を持つためである。

Q0087

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント6：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

「リバースプロキシ」について、誤解を避けるための説明として最も適切なものはどれか。

A. DNS応答へデジタル署名を付け真正性と完全性を検証する仕組み
B. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み
C. 通信状態を追跡しセッション文脈に基づいてパケットを判定する方式
D. ネットワークを分割し侵害範囲と不要な通信を制限する設計

答え・解説

Q0087 正答：B. 外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

解説：リバースプロキシは外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント7：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

「リバースプロキシ」は、ネットワークを分割し侵害範囲と不要な通信を制限する設計。

A. ○
B. ×

答え・解説

Q0088 正答：×

解説：誤り。記述はネットワークセグメンテーションの説明である。リバースプロキシは外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み。

Q0089

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント8：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

次の状況で中心となる論点はどれか。「外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み」ことが求められている。

A. ステートフルインスペクション
B. DNSSEC
C. ネットワークセグメンテーション
D. リバースプロキシ

答え・解説

Q0089 正答：D. リバースプロキシ

解説：中心となる論点はリバースプロキシである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0090

ネットワークセキュリティ
タグ：リバースプロキシ
用語：リバースプロキシの確認ポイント9：外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み

「外部要求を受けて内部サーバへ中継し内部構成を隠す仕組み」という特徴を持つものを選べ。

A. リバースプロキシ
B. DNSSEC
C. ステートフルインスペクション
D. ネットワークセグメンテーション

答え・解説

Q0090 正答：A. リバースプロキシ

解説：リバースプロキシが該当する。定義は外部要求を受けて内部サーバへ中継し内部構成を隠す仕組みであり、他の候補とは機能が異なる。