

ネットワークスペシャリスト 解答例

【午 後 I】

問1 ルータの更改（配点 50 点）

設問1（23点:(1)3点×3, (2)5点, (3)4点, (4)5点）

- (1) a : バックボーン
b : ルータ
c : デフォルトゲートウェイ
- (2) 不正なルータからの誤った経路情報を取得し, 正しい経路制御ができない問題
- (3) 長くなるようにする。
- (4) LSA の交換が完了し, 正しい経路を広告できる状態

設問2（27点:(1)(完答4点)×2, (2)5点, (3)5点, (4)5点, (5)1点×4）

- (1) (大阪本社) (ウ)
(東京支社) (ア), (イ)
- (2) 全てのインタフェースのコストを 1011 以上にする。
- (3) 隣接ルータへ直ちにリンクダウンを通知し LSA を更新させるため
- (4) ケーブルに対応するポートを書いたシールを貼付する。
- (5) ① L3SW10
② R11
③ R20
④ R30 (①～④: 順不同)

問2 ネットワークの改善（配点 50 点）

設問1（10点:(1)2点×3, (2)4点）

- (1) a : プライベート
b : グローバル
c : PoE+
- (2) PC が属するサブネット

設問2（17点:(1)5点, (2)2点, (3)完答4点, (4)3点×2）

- (1) 一斉学習時の E サービスの不具合が生じているのは一部かつ不特定の PC だから
- (2) d : 帯域保証 又は ギャランティ
- (3) (iii), (iv)
- (4) (PC 台数) 327(台)
(エントリー数) 120,000

設問 3 (23 点:(1)5 点, (2)2 点×4, (3)5 点×2)

- (1) 前のリクエスト処理終了まで次のリクエスト処理が待たされるから
- (2) e : リクエスト
f : レスポンス
g : ストリーム ID
h : 並列
- (3) (調整) UDP の保持時間が短くなるように変更する。
(効果) 無通信状態の NATP 変換エントリが早期に解放され, NAT 変換テーブルの枯渇を防げる。

問 3 セキュア Web ゲートウェイの導入 (配点 50 点)

設問 1 (22 点:(1)4 点, (2)4 点×2, (3)2 点, (4)2 点×2, (5)2 点×2)

- (1) 複数機器にまたがるログを時系列で照合し解析するため
- (2) ① 登録した FQDN や IP アドレス宛での通信をブロックするため
② Web サイトへのアクセス履歴の確認を行うため (①, ②:順不同)
- (3) L3SW の DHCP リースログ
- (4) a : syslog サーバ
b : 認証サーバ
- (5) c : 10080
d : 443

設問 2 (6 点:(1)4 点, (2)2 点)

- (1) SWG サービスのルート証明書
- (2) C&C サーバ

設問 3 (22 点:(1)2 点×2, (2)4 点, (3)2 点×3, (4)4 点, (5)4 点)

- (1) ① 2
② 7 (①, ②:順不同)
- (2) (B), (A), (H), (I), (E), (I), (K)
- (3) (送信元) 内部セグメント
(宛先) SWG サービス
(プロトコル/宛先ポート番号) TCP/443
- (4) アクセスを許可する送信元アドレスを J 社の SWG-GIP だけに変更する。
- (5) 経由する機器の削減

【午 後 II】

問 1 社内ネットワークの IPv6 対応 (配点 100 点)

設問 1 (6 点:2 点×3)

- a : ターゲット IP アドレス
- b : ブロード
- c : リプライ

設問 2 (29 点:(1)2 点×3, (2)5 点, (3)5 点, (4)3 点×2, (5)2 点, (6)5 点)

- (1) d : 16
 - e : 48
 - f : 64
- (2) データリンク層で通信可能な範囲
- (3) 他のノードで使用されている LLA や GUA を設定してしまい, IP アドレスの重複が発生することを防ぐため
- (4) (GUA) 2001:db8:aabb:1:8:800:200c:417a
(プレフィックス長) 64
- (5) g : デフォルトルータ
- (6) IP アドレスから PC を特定しにくいから

設問 3 (15 点:(1)2 点, (2)(完答 4 点)×2, (3)5 点)

- (1) h : TCP
- (2) (IPv6 アドレス) 2001:db8:xxxx::10, 2001:db8:xxxx::20
(FQDN) ns1.example.net. , ns2.example.net.
- (3) IPv6 が不通でも自動的に IPv4 を利用した通信に切り替わり, 通信を継続できるから

設問 4 (50 点:(1)5 点, (2)5 点, (3)5 点, (4)2 点×9, (5)5 点, (6)5 点, (7)2 点, (8)5 点)

- (1) 外部への経路情報の漏えいや, 外部からの攻撃, 外部から社内の機器への直接接続を防ぎ, 安全性を高めるため
- (2) traceroute6 で通信経路を調査するときどの機器を経由したのかが容易に判別できる。
- (3) サブネットプレフィックスとデフォルトルータとしての情報を RA メッセージで送る。
- (4) ア : fe80::1
イ : b
ウ : fc80::2
エ : c
オ : fe80::1
カ : d
キ : fe80::2
ク : f
ケ : fe80::1
- (5) ホップリミットが 0 になるまで相互に転送し合ったのちに破棄する。
- (6) 最長一致判定が用いられ, 項番 2 のほうが長いから
- (7) i : NAPT
- (8) 経路上の最小 MTU サイズ

問2 IoTシステムの設計（配点 100 点）

設問1（12 点:2 点×6）

- a : 消費
- b : 非セルラー
- c : セルラー
- d : ISM
- e : 干渉
- f : 3GPP

設問2（10 点:2 点×5）

- g : 2
- h : G メーター管理サーバ
- i : SIM
- j : 372
- k : REST

設問3（48 点:(1)2 点×5, (2)メッセージ 2 点, 理由 5 点, (3)2 点, (4)5 点×2, (5)内容 5 点, 攻撃名 4 点, (6)5 点×2）

(1) l : トランスポート

- m : 順不同
- n : 重複
- o : 同期
- p : バックオフ

(2) (メッセージ) (viii)

(理由) トークン値が一致しているから

(3) (ACK) (v)

(4) (理由) 既に受信した ACK と同一のメッセージ ID の ACK だから

(処理) 何も処理を行わずにパケットを破棄する。

(5) (内容) 送信元 IP アドレスを DDoS 攻撃対象のサーバの IP アドレスに偽装する。

(攻撃名) リフレクション攻撃

(6) (判断できること) ClientHello の送信元が偽装されていないこと

(対応) ハンドシェークを中断し、パケットを破棄する。

設問4（30 点:(1)5 点, (2)5 点, (3)5 点, (4)5 点, (5)5 点, (6)5 点）

- (1) ネットワークや G メーター管理サーバの処理を分散して負荷を軽減できる。
- (2) 電池の消耗を抑え、長時間稼働が可能になる。
- (3) データ送信ごとに TCP の 3 ウェイハンドシェークを行う必要があるから
- (4) LPWA 閉域接続と IPsec で攻撃から保護されているから
- (5) 1 時間ごとの LP ガスの流量積算値を正確に測定できない。
- (6) G メーター管理サーバに設定された時刻データを定期的に GET で取得して補正する。

以上