S703697-11，S902401-11

正　誤　表

下記の部分に変更がありましたので訂正させていただきます。
ご迷惑をおかけし大変申し訳ございません。

2025 情報処理安全確保支援士「専門知識＋午後問題」の重点対策 第１版 第１刷（電子書籍版含む）

No	訂正箇所	誤	正
1	P.294 下から 3 行目	第 2 フェーズは，サーバからクライアントへのメッセージ送信のフェーズです。このフェーズのポイントは，サーバからデジタル証明書をクライアントに送るところ（Server Certificate）です（このときにルート証明書まですべての証明書，すなわち証明書のチェーンを送る）。デジタル証明書がない場合は，オプションで Diffie-Hellman の鍵交換方式を使用することも可能です（Server Key Exchange）。	第 2 フェーズは，サーバからクライアントへのメッセージ送信のフェーズです。このフェーズのポイントは，サーバからデジタル証明書をクライアントに送るところ（Server Certificate）です（このときにルート証明書まですべての証明書，すなわち証明書のチェーンを送る **※1）。サーバ側にデジタル証明書がない場合，証明書を必要としない鍵交換方式（PSK や匿名 Diffie-Hellman）が選択されます（Server Key Exchange）。** **※1．通常は，ルート証明書は含みません。IoT や組込み系，プライベート CA など相手側が証明書を持たない場合や，証明書管理が難しい場合にルート証明書を含めて送信します。**
2	P.295 10 行目	また，サーバから要求のある場合は Client Certificate でクライアント証明書をサーバに送信しますが，要求されない場合でも Certificate Verify でサーバ側でクライアントの正当性を確認できるように考えられています。	また，サーバから要求のある場合は Client Certificate でクライアント証明書をサーバに送信します。 **（「が，要求されない～（中略）～考えられています」を削除）**
3	P.295 図表 3-2-9	クライアント側の二つ目の説明 クライアントのデジタル証明書＋ルート CA までのディジタル証明書 Web サーバ側の二つ目の説明 サーバのデジタル証明書＋ルート CA までのデジタル証明書	クライアント側の二つ目の説明 クライアントのデジタル証明書＋ルート CA までのディジタル証明書 **※1** Web サーバ側の二つ目の説明 サーバのデジタル証明書＋ルート CA までのデジタル証明書 **※1** **※1．通常は，ルート証明書は含みません。IoT や組込み系，プライベート CA など相手側が証明書を持たない場合や，証明書管理が難しい場合にルート証明書を含めて送信します。**
4	P.712 CSPM　1 行目	IssS	IaaS

株式会社アイテック