<table>
<tr><td colspan="4">航　空　自　衛　隊　仕　様　書</td></tr>
<tr><td rowspan="2">仕様書の
種　　類</td><td>内容による分類</td><td colspan="2">役　務　仕　様　書</td></tr>
<tr><td>性質による分類</td><td colspan="2">個　別　仕　様　書</td></tr>
<tr><td>物品番号</td><td></td><td colspan="2">仕　様　書　番　号</td></tr>
<tr><td rowspan="5">品　　名
又は
件　　名</td><td rowspan="5">部外委託教育（SANS SECURITY 401 Security Essentials-Network, Endpoint, and Cloud（試験付））</td><td colspan="2">空シス隊ＬＰＳ－Ｘ００１２２</td></tr>
<tr><td>承　認</td><td>令和８年７月２７日</td></tr>
<tr><td>作　成</td><td>令和８年７月２７日</td></tr>
<tr><td>改　正</td><td>令和　年　月　日</td></tr>
<tr><td>作成部
隊等名</td><td>航空システム通信隊</td></tr>
</table>

1　総則

1.1　適用範囲

この仕様書は，部外委託教育（SANS SECURITY 401 Security Essentials-Network, Endpoint, and Cloud（試験付））について規定する。

1.2　用語及び定義

この仕様書で用いる主な用語及び定義は，次による。

1.2.1

講師

当該契約に基づき，指定された場所において教育を実施する者

1.2.2

サイバー防護関連業務従事者

航空システム通信隊において，サイバー攻撃等への対処に関連する業務に携わる者

1.2.3

サイバー攻撃等

サイバー攻撃及びサイバー攻撃と同様の影響を発生させる情報システムの誤操作並びにサイバー攻撃以外によるコンピュータ・ウイルスの混入等

2　役務に関する要求

2.1　役務内容等

被教育者に対し，サイバー防護関連業務従事者としての能力向上のためにSANS SECURITY 401 Security Essentials-Network, Endpoint, and Cloud（試験付）の講義及び実習を実施する。

2.1.1　履行場所

契約の相手方が指定する場所（航空自衛隊市ヶ谷基地から公共交通機関を利用して概ね１時間３０分以内で移動できる場所）とする。ただし，オンラインで受講する場合は，受講者の所定とする。

2.1.2　教育期間

令和８年１０月１９日（月）～令和８年１０月２４日（土）

2.1.3　被教育者

２名

2.1.4　教育内容

別紙による。

2.1.5　１日の教育時間

９時間（基準）

2.1.6　到達目標

a)　サイバーセキュリティの基礎原則を理解し，説明できる。

b)　ネットワーク及びクラウド環境のセキュリティ対策を実践できる。

c)　脆弱性の発見と対策が実践できる。

d)　セキュリティインシデントの検知，分析及び対応が実践できる。

e)　実務で活用できる防御技術を習得し，GIAC Security Essentials Certification(GESC)を取得できるレベルの知識・技術が身についている。

2.2　講師の条件

SANS 認定インストラクターであり，サイバーセキュリティに関する高度な知識を有するとともに講師実績があること。

2.3　教材

a)　契約の相手方は，SANS Institute が提供する SANS SECURITY 401 の教材を被教育者に配布し，当該教材を基に教育を実施するものとする。

b)　契約の相手方は，当該契約に基づく教育の終了後，被教育者に提供した教材を官側に提供するものとする。

2.4　試験に関する要求

契約の相手方は，被教育者に GIAC 試験の受験に関する手続きを実施すること。

3　検査

検査は，関係契約条項及び契約担当官の定めるところによる。

4　その他の指示

4.1　不測事態発生時の対処

a)　講師が急病等の理由により教育を実施できない場合，速やかに代替講師を差し出すものとする。

b)　参加人数が開催基準を満たさない等により，部外教育コース自体の開催が中止される場合は，契約担当官と協議するものとする。

4.2　その他

本仕様書に規定のない事項又は疑義が生じた場合は，速やかに契約担当官と書面により協議するものとする。

別紙

教育内容		
区分	教育項目	
	以下の教育項目（合計：３，１５０分（基準））を実施する。	
講習 実習	SANS SECURITY 401 Security Essentials-Network, Endpoint, and Cloud（試験付）	1) ネットワークセキュリティとクラウドの基礎 防御可能なネットワークアーキテクチャ プロトコルとパケット分析 仮想化，クラウド，AIの基礎 ワイヤレスネットワークのセキュリティ保護 Tcpdump Wireshark AWS VPCフローログ 2) 多層防御 多層防御 IAM，認証，パスワードセキュリティ セキュリティフレームワーク データ損失防止 モバイルデバイスのセキュリティ パスワード監査 データ損失防止 モバイルデバイスのバックアップ・リカバリ 3) 脆弱性管理と対応 脆弱性評価 ペネトレーションテスト 攻撃と悪意のあるソフトウェア Webアプリケーションセキュリティ セキュリティ運用とログ管理 ネットワーク検出 バイナリファイルの分析と特性評価 Webアプリケーションのエクスプロイト SIEMログ分析 4) データセキュリティ技術 暗号化 暗号化アルゴリズムと導入 暗号化の適用 ネットワークセキュリティディバイス エンドポイントセキュリティ ハッシュと暗号検証

講習 実習	SANS SECURITY 401 Security Essentials- Network, Endpoint, and Cloud (試験付)	暗号化と復号 Snort3 と Zeek による侵入検知とネットワークセキュリティ監視 5) Windows と Azure のセキュリティ Windows セキュリティインフラストラクチャ Windows as a Service Windows アクセス制御 セキュリティ構成の適用 Microsoft クラウドコンピューティング Windows プロセスエクスプロレーション Windows ファイルシステムアクセス許可 Windows システムセキュリティポリシーの適用 PowerShell によるスピードとスケールの向上 6) コンテナ, Linux, Mac のセキュリティ Linux の基礎 コンテナ化されたセキュリティ Linux のセキュリティ強化とインフラストラクチャ macOS セキュリティ Linux の権限 Linux コンテナ Linux のログ記録と監査