無人航空機の第二種型式認証に資するセキュリティリスクアセスメント手法の考察

Security Risk Assessment Method for Class II UAS Type Certification

○ Yuichi Yaguchi (University of Aizu)

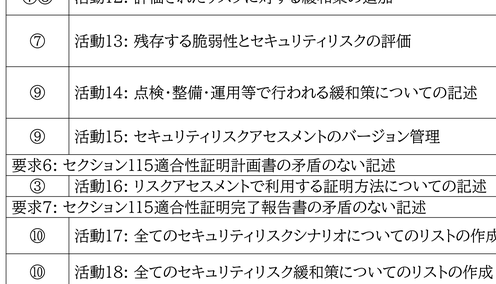
どのようにドローンのセキュリティリスクを評価し、安全性を担保するかの手法を研究しています。

本研究の目的

安全基準に沿ったサイバーセキュリティの適合性証明計画書および適合性証明完了報告書作成に関して、「航空局ガイドライン」で示されている方法の解説および補足を行うものである。「航空局ガイドライン」で提示されている適合性証明案は一通りの活動を規定しているが、その活動を行うための要求の詳細や、活動に必要な前提条件や変数などは提示されていない。

そのため、ReAMo PJ 無人航空機の認証に対応した証明手法の事例検討WG内 115サブWGサイバーセキュリティで議論された内容をもとに、安全基準に合致する適合性証明を実現するための「航空局ガイドライン」の解説と指針を提示することが目的である。

サイバーセキュリティの第二種型式認証プロセス



- リスクアセスメントの基本構成は ISO 27005で提示されている方法（RTCA DO-326A等でも参照)と同等
- 具体化している部分としては、『どのタイミングで、何の活動をするのか』と、『出力が何になるのか』について注目
- 10のプロセス、7の要求、19の活動の必須/推奨をまとめた形で、適合性証明活動の対応表を作成した。

サイバーセキュリティの適合性証明の活動対応表

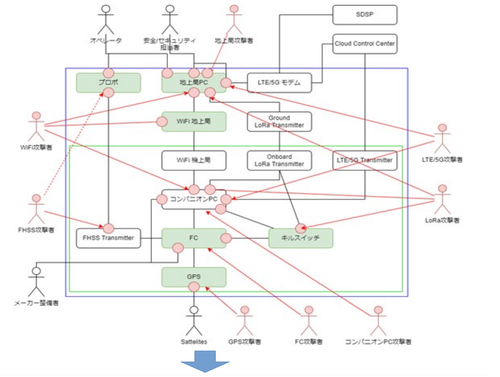
プロセス	活動項目	M/R	手法および出力
要求1: システム環境の明確な記述			
①	活動1: システムの範囲の決定と記述	M	システムブロック図
①	活動2: ネットワークおよびデータフローの記述	R	ネットワーク図 データフロー図
①	活動3: 正常な運用におけるインターフェースとアクターの記述	M	ユースケース図 ステークホルダー表
要求2: サイバーセキュリティの範囲と脅威、攻撃者の定義			
②	活動4: 脅威状態と評価尺度の定義	M	脅威状態定義表 リスク評価尺度定義書
②④	活動5: 攻撃者と攻撃可能な干渉口の抽出	M	ミスユースケース図 攻撃者を含むシステムブロック図 攻撃者定義表 アタックサーフェスリスト
④	活動6: セキュリティ環境におけるセキュリティ境界の定義	M	セキュリティ環境・境界指示図
要求3: サイバーセキュリティリスクの特定			
④	活動7: 資産とリスク重大度の定義	M	資産-脅威リスト
⑤	活動8: 具体的な脅威の抽出と脅威レベルの評価	M	脅威分析表 脅威-対処リスト
⑤	活動9:　既存の緩和策の抽出と防御レベルの評価	M	緩和策リスト 脆弱性クラスリスト
⑤	活動10: 脅威源から脅威事象が引き起こされるシナリオの同定	M	脅威木の構築 カットセットリスト
要求4: 特定されたセキュリティリスクの評価			
⑤⑥	活動11: 脅威シナリオ中に含まれる既存の緩和策を含めたリスクの評価	M	セキュリティリスク分析表
要求5: 評価に基づく緩和策の実施と記述			
⑦⑧	活動12: 評価されたリスクに対する緩和策の追加	R	追加要求の設計 開発者ガイドライン（追加要求）
⑦	活動13: 残存する脆弱性とセキュリティリスクの評価	R	ファジング・テスト結果報告書 ペネトレーション・テスト結果報告書
⑨	活動14: 点検・整備・運用等で行われる緩和策についての記述	M	セクション205 ICAへの記述 セクション200 飛行規程への記述
⑨	活動15: セキュリティリスクアセスメントのバージョン管理	R	バージョン管理ツールの利用 要求管理ツールの利用
要求6: セクション115適合性証明計画書の矛盾のない記述			
③	活動16: リスクアセスメントで利用する証明方法についての記述	M	コンプライアンスマトリクス
要求7: セクション115適合性証明完了報告書の矛盾のない記述			
⑩	活動17: 全てのセキュリティリスクシナリオについてのリストの作成	R	セキュリティリスクシナリオ解析書
⑩	活動18: 全てのセキュリティリスク緩和策についてのリストの作成	R	セキュリティ緩和策妥当性解析書
⑩	活動19: 全てのセキュリティリスク緩和策についての適合性評価の結果の記述	M	コンプライアンスマトリクスへの追記

サイバーセキュリティリスクアセスメント手法の提案

出発地点: 要求①-活動1: システムブロック図

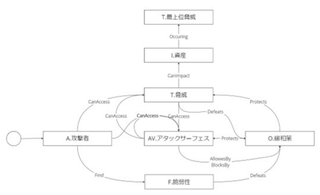
攻撃者特定: 要求①-活動3, 5: 攻撃者を含むシステムブロック図の作成

Attacker	記述	LoT
A.オペレーター	標準オペレーター、内部者	1
A.安全・セキュリティ担当者	内部者、ユーザ側安全、セキュリティ担当	1
A.メーカー整備者	メーカー整備者、内部者	1
A.GPS衛星	GPS衛星、標準	1
A.地上局攻撃者	地上局への攻撃、内部者中心	2
A.WiFi攻撃者	外部からのWiFi侵入	3
A.FHSS攻撃者	外部からのFHSS信号侵入	3
A.LTE/5G攻撃者	外部からのLTE/5G侵入	4
A.LoRa攻撃者	外部からのLoRa侵入	3
A.コンパニオンPC攻撃者	コンパニオンPCへの攻撃、内部者、外部侵入者	3
A.GPS攻撃者	GPS信号への攻撃	3
A.FC攻撃者	FCへの攻撃, 内部者, 外部侵入者	3



資産特定: 要求④-活動7: ブロック図から想起される資産と脅威事象

Asset	記述	SEV	Threat	Fatal Threat
I.地上局PC	地上局PCの乗っ取り/サービス不能	5	T.地上局PC.ID/パスワード漏出 T.地上局PC.ハイジャック T.地上局PC.バックドア侵入	T.機体.ハイジャック
			T.地上局PC.マルウェア混入 T.地上局PC.パラメータデータ書換 T.地上局PC.GCSパラメータデータ書換	T.機体.制御不能 T.機体.計画外飛行
I.地上局PC.GCS	地上局PCのGCS機能の不能/不正	5	T.地上局PC.マルウェア混入 T.地上局PC.GCSパラメータデータ書換 T.地上局PC.DOS	T.機体.制御不能 T.機体.計画外飛行
I.地上局PC.WiFi	地上局PCのWiFi通信不能	5	T.地上局PC.WiFi.サービス拒否 T.地上局PC.WiFi.ネットワークパラメータデータ書換	T.機体.制御不能 T.機体.計画外飛行 T.機体.ハイジャック
I.地上局PC.LoRa	地上局PCのLoRa通信不能	5	T.地上局PC.LoRa.改竄 T.地上局PC.LoRa.サービス拒否	T.機体.制御不能 T.機体.計画外飛行
I.地上局PC.LTE	地上局PCのLTE通信不能	5	T.地上局PC.LoRa.改竄 T.地上局PC.LoRa.サービス拒否	T.機体.制御不能 T.機体.計画外飛行
I.プロポ	プロポ不能/不正	5	T.プロポ.ファームウェア不正更新 T.プロポ.ホッピングパターン漏出	T.機体.制御不能 T.機体.計画外飛行
I.プロポ.FHSS	プロポ通信不能	5	T.プロポ.FHSS.電波干渉 T.プロポ.FHSS.不正電波混入	T.機体.制御不能 T.機体.計画外飛行
I.WiFi	WiFiルータ、ネットワーク	5	T.WiFi.ARP Spoofing T.WiFi.ルーターハイジャック T.WiFi.WPA脆弱出	T.機体.ハイジャック
I.LTE	LTE回線上での侵入	5	T.LTE.なりすまし T.LTE.改竄 T.LTE.サービス拒否	T.機体.ハイジャック
I.コンパニオンPC	コンパニオンPCの不能/不正	5	T.コンパニオンPC.不正ファーム T.コンパニオンPC.バックドア侵入 T.コンパニオンPC.ハイジャック T.コンパニオンPC.ID/パスワード漏出	T.機体.ハイジャック
			T.コンパニオンPC.マルウェア混入 T.コンパニオンPC.不正コード混入 T.コンパニオンPC.パラメータデータ書換 T.コンパニオンPC.サービス拒否	T.機体.制御不能 T.機体.計画外飛行



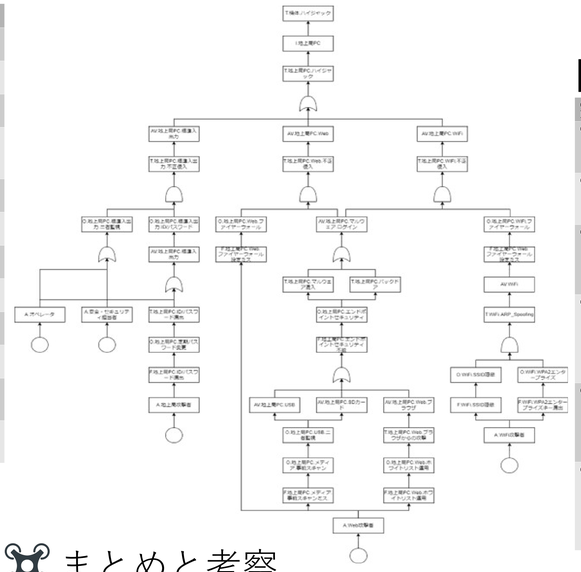
攻撃口特定: 要求④-活動5: アタックサーフェスリストの作成

Access Point	記述	セキュリティ対策	アクセスコントロール	Access by:
AS.地上局PC.標準入出力	地上局PC.標準入出力	O.地上局PC.IDパスワード	ALLOWS	A.オペレーター A.安全・セキュリティ担当者
		O.地上局PC.IDパスワード	BLOCKS	A.地上局攻撃者
AS.地上局PC.GCS	GCSアプリケーション	n/a	ALLOWS	T.地上局PC.マルウェア混入 T.地上局PC.GCS.マルウェア混入 AS.地上局PC.標準入出力
AS.地上局PC.USB	地上局PCUSBポート	O.地上局PC.2者監視	ALLOWS	A.安全・セキュリティ担当者
		O.地上局PC.2者監視	BLOCKS	A.オペレーター A.地上局攻撃者
AS.地上局PC.SDカード	地上局PCSDカード	O.地上局PC.2者監視	ALLOWS	A.安全・セキュリティ担当者
		O.地上局PC.2者監視	BLOCKS	A.オペレーター A.地上局攻撃者
AS.地上局PC.Web	地上局PCのWeb接続(地図情報等)	O.地上局PC.ファイヤーウォール	ALLOWS	A.SDSP(80番 In)
		O.地上局PC.ファイヤーウォール	BLOCKS	A.地上局攻撃者
AS.地上局PC.WiFi	地上局PCのWiFi接続経由	O.WiFi.WPA2	ALLOWS	AS.コンパニオンPC.WiFi
		O.WiFi.WPA2	BLOCKS	A.WiFi攻撃者
AS.地上局PC.LoRa	地上局PCのLoRa接続経由（USB）	n/a	ALLOWS	AS.コンパニオンPC.LoRa A.LoRa攻撃者
AS.地上局PC.LTE	地上局PCのLTE接続経由（Webと同義かも）	O.LTE,SSL通信	ALLOWS	AS.コンパニオンPC.LTE
		O.LTE,SSL通信	BLOCKS	A.LTE/5G攻撃者
AS.プロポ.FHSS	プロポのFHSS経由	O.FHSS,ホッピング	ALLOWS	A.オペレーター
		O.FHSS,ホッピング	BLOCKS	A.FHSS攻撃者
AS.コンパニオンPC	コンパニオンPCログイン	O.コンパニオンPC.USBキー制限	ALLOWS	A.メーカー整備車
		O.コンパニオンPC.USBキー制限	BLOCKS	A.安全・セキュリティ担当者 A.オペレーター A.コンパニオンPC攻撃者

緩和策特定: 要求⑤-活動9: 脆弱性クラスリストの作成

脆弱性クラス	記述	LoP	ICA	飛行規程	110
F.地上局PC.IDパスワード	弱いパスワード、IDの対	2	✓	✓	
F.地上局PC.2者監視	二者監視を怠った	1	✓		
F.地上局PC.ファイヤーウォール	ファイヤーウォールの設定ミス	2	✓		
F.WiFi.WPA2	WPA2の設定の脆弱性	3		✓	
F.LTE,SSL通信	SSL通信設定の脆弱性	3		✓	
F,コンパニオンPC.2者監視	2者監視を怠った	1	✓		
F,コンパニオンPC.LTE.入力制限	入力制限設定ミス	2			
F.FHSS.ペアリング	ペアリングの重複	3		✓	
F.FC,カードロック	カードロックが機能していない・設定ミス	3			
F.FC.USBロック	USBロックが機能していない・設定ミス	3			
F.地上局PC.マルウェアチェック	マルウェアチェックを怠る/すり抜け	2	✓		
F.地上局PC.定期パスワード更新	パスワード更新を怠る	1	✓		
F.地上局PC.WiFi.MAC接続制限	MAC接続制限を怠る	2		✓	

脅威木解析: 各表の項目をルールに基づいて整理



脅威特定: 要求⑤-活動8: 脅威リストの作成

脅威点12	記述	対処	ポリシー	Access By:
T.地上局PC.ハイジャック	地上局PCがハイジャックされ、地上局PCの権限を奪われる	n/a	ALLOWS	A.オペレーター A.安全・セキュリティ管理者 A.整備担当者 AS.地上局PC.Web AS.地上局PC.WiFi
	地上局PCのID/ログイン情報が漏洩することで、不正侵入される	O.地上局PC.定期パスワード更新	BLOCKS	A.地上局PC攻撃者
T.地上局PC.ID/パスワード漏出	地上局PCのID/passが漏出し、外部から侵入可能となる	O.地上局PC.定期パスワード更新	ALLOWS	A.オペレーター A.安全・セキュリティ担当者
			BLOCKS	A.地上局PC攻撃者
T.地上局PC.マルウェア混入	地上局PCにマルウェアが混入され、地上局PCに対してDoSやサービスに対する攻撃が可能となる	O.地上局PC.エンドポイントセキュリティ	ALLOWS/BLOCKS	AS.地上局PC.USB AS.地上局PC.SDカード AS.地上局PC.Web
T.地上局PC.ハングアップ攻撃	地上局PCに対して高負荷を掛けてハングアップさせるなどのDoS攻撃を仕掛ける	O.地上局PC.エンドポイントセキュリティ	BLOCKS	AS.地上局PC.USB AS.地上局PC.SDカード AS.地上局PC.Web
T.地上局PC.バックドア	地上局PCに対してバックドアを仕掛ける	O.地上局PC.エンドポイントセキュリティ	BLOCKS	AS.地上局PC.USB AS.地上局PC.SDカード AS.地上局PC.Web
T.地上局PC.標準入出力.不正侵入	ID/ログイン情報の漏洩などによって不正に侵入される	O.地上局PC.二者監視	ALLOWS	A.オペレーター A.安全・セキュリティ管理者 A.整備担当者
			BLOCKS	A.地上局PC攻撃者
T.地上局PC.GCS.不正侵入	GCSに対して不正侵入を行う	n/a	ALLOWS	AS.地上局PC.標準入出力
T.地上局PC.GCS.マルウェア混入	GCSにマルウェアが混入され、GCSに不備をきたす	O.地上局PC.マルウェアチェック	BLOCKS	AS.地上局PC.USB AS.地上局PC.SDカード AS.地上局PC.Web

緩和策特定: 要求⑤-活動9: 緩和策リストの作成

セキュリティ緩和策	記述	脆弱性クラスまたは脅威事象
O.地上局PC.IDパスワード	IDとパスワードによる地上局PCのアクセス制限	T.地上局PC.ID/パスワード漏出 F.地上局PC.IDパスワード
O.地上局PC.2者監視	地上局PCの利用で、2者監視で相互監視を行う	F.地上局PC.2者監視
O.地上局PC.ファイヤーウォール	ファイヤーウォール設定による外部からのPCアクセスの遮断	F.地上局PC.ファイヤーウォール
O.WiFi.WPA2	WPA2設定によるWiFiネットワークの堅牢化	F.WiFi.WPA2
O.LTE,SSL通信	SSL通信によるデータの暗号化	F.LTE,SSL通信
O.FHSS,ホッピング	ホッピングパターンによるRC信号の隠蔽	T.FHSS,ホッピングパターン漏出
O,コンパニオンPC.USBキー制限	USBキー制限を付けることによるコンパニオンPCアクセス制限	T.USBキー盗難
O,コンパニオンPC.2者監視	コンパニオンPCの更新で、2者監視で相互監視を行う	F,コンパニオンPC.2者監視
O,コンパニオンPC.LTE.入力制限	コンパニオンPCに対するLTEからの入力制限（出力のみにする）	F,コンパニオンPC.LTE.入力制限
O.FHSS.ペアリング	FHSSペアリングによる機器接続制限	F.FHSS.ペアリング
O.FC,CC経由SDカードロック	CC経由でのSDカードのロック機構	F.FC,カードロック
O.FC,メンテナンス経由SDカードロック	メンテナンスポート経由でのSDカードのロック機構	F.FC,カードロック
O.FC,CC経由USBロック	CC経由でのUSBのロック機構	F.FC,USBロック
O.FC,メンテナンス経由USBロック	メンテナンスポート経由でのUSBのロック機構	F.FC,USBロック
O,地上局PC.マルウェアチェック	地上局PCでのマルウェアチェック	F,地上局PC.マルウェアチェック
O,地上局PC.定期パスワード更新	IDパスワード漏出対策としてのパスワード更新	F,地上局PC.定期パスワード更新
O,地上局PC.WiFi.MAC接続制限	MAC接続制限によるWiFiアクセス制限	F,地上局PC.WiFi.MAC接続制限

アセスメント: カットセットで抽出したシナリオの点数評価

CUID	Attaker	Vulnerability	Threat and Measure	BEID	[A]LoT	[F]LoP	Assets SEV	LoP sum	Res, SEV
CU1	A.オペレーター	n/a	O.地上局PC.標準入出力.ID/パスワード O.地上局PC.標準入出力.二者監視 T.地上局PC.標準入出力.不正侵入 T.地上局PC.ハイジャック T.機体.ハイジャック	BE1	1	0	5	3	-2
CU2	A.安全・セキュリティ担当者	n/a	O.地上局PC.標準入出力.ID/パスワード O.地上局PC.標準入出力.二者監視 T.地上局PC.標準入出力.不正侵入 T.地上局PC.ハイジャック T.機体.ハイジャック	BE2	1	0	5	3	-2
CU3	A.地上局攻撃者	F.地上局PC.ID/パスワード漏出	O.地上局PC.定期パスワード変更 T.地上局PC.ID/パスワード漏出 O.地上局PC.標準入出力.ID/パスワード O.地上局PC.標準入出力.二者監視 T.地上局PC.標準入出力.不正侵入 T.地上局PC.ハイジャック T.機体.ハイジャック	BE3	2	1	5	3	-2
CU4	A.Web攻撃者	F.地上局PC.Web.ファイヤーウォール設定ミス F.地上局PC.メディア審前スキャンミス	O.地上局PC.メディア事前スキャン O.地上局PC.メディア二者監視 T.地上局PC.メディア.挿入時マルウェア感染 O.地上局PC.エンドポイントセキュリティ T.地上局PC.マルウェア混入 O.地上局PC.Web.ファイヤーウォール T.地上局PC.Web.不正侵入 T.地上局PC.ハイジャック T.機体.ハイジャック	BE4	4	2,2	5	2	-2
CU5	A.Web攻撃者	F.地上局PC.Web.ファイヤーウォール設定ミス F.地上局PC.Web.ホワイトリスト運用	O.地上局PC.ホワイトリスト運用 T.地上局PC.Web.ブラウザからの攻撃 O.地上局PC.エンドポイントセキュリティ T.地上局PC.マルウェア混入 O.地上局PC.Web.ファイヤーウォール T.地上局PC.Web.不正侵入 T.地上局PC.ハイジャック T.機体.ハイジャック	BE5	4	2,1	5	2	-1
CU6	A.WiFi攻撃者	F.WiFi.SSID隠蔽ミス F.WiFi.WPA2エンタープライズモード漏出 AS.地上局PC.マルウェアログイン	O.WiFi.SSID隠蔽 O.WiFi.WPA2エンタープライズ T.WiFi.ARP Spoofing O.地上局PC.WiFiファイヤーウォール T.地上局PC.バックドア T.地上局PC.マルウェア混入 T.地上局PC.WiFi.不正侵入 T.地上局PC.ハイジャック T.機体.ハイジャック	BE6	3	2,2,2	5	2	-5

まとめと考察

型式認証のサイバーセキュリティの一連の手法を、機械的に行うことができるように整理 – 尺度としては定性表現に基づく定量化を行い、ある程度簡易化した。

まだ煩雑な部分が多いことから、実例の充実化と、簡易化を進めていきたい。