2018 年 2 月 23 日
独立行政法人情報処理推進機構（IPA）

欧州ネットワーク情報セキュリティ機関（ENISA）「スマート空港のセキュリティ」概要

本概要は、欧州ネットワーク情報セキュリティ機関（ENISA）発行の以下文書の概訳となります。
内容の詳細につきましては、原文をご確認ください。

Securing Smart Airports
https://www.enisa.europa.eu/publications/securing-smart-airports

本概要では、スマート空港のサイバーセキュリティ向上のための上記ガイドについて、以下の項目の概要を日本語でまとめている（【】内は原文の章・節・項番号）。

- 対象読者（Target audience）【1.2 節】
- 政策・規制（EU cyber security policy in civil aviation）【2.2 節】
- 資産（Key asset groups and assets）【3 章】
- 脅威（Threats analysis）【4.2.1 項】
- 攻撃シナリオ（Attack scenarios）【4.2.3 項、5 章】
- 対策（Security good practices）【6 章】
- 課題（Gap analysis and identification of areas of improvement）【7 章】
- 提言（Recommendations）【8 章】

次頁以降に、同ガイドの概要を記す。

従来の空港システムにスマート機器を加え、よりシームレスで安全なサービスの提供を目指すスマート空港では、機能性や利便性が向上するだけでなく、サイバー攻撃の可能性も拡がることになる。空港の責任者は、スマート化に伴う新たな脅威を認識し、空港の運用および旅客の安全を確保するためのセキュリティ対策を検討する必要がある。

本ガイド「スマート空港のセキュリティ」は、スマート空港のサイバーセキュリティおよびレジリエンスの強化を支援することを目的として、机上および業界関係者へのヒアリングによる調査からスマート空港を構成する資産、想定される脅威、攻撃シナリオを洗い出し、対策（グッドプラクティス）、スマート空港の課題、およびセキュリティ強化のための提言等をまとめている。

「スマート空港のセキュリティ」概要（1/6）

掲載項目	概要
対象読者	• 空港運営組織の最高情報セキュリティ責任者（CISO）、最高情報責任者（CIO）、IT 責任者（IT Director）、セキュリティ担当の運営責任者（Head of Operations）、セキュリティ担当者 • 空港にスマートソリューションやサービスを提供している組織 • 空港サービスのサプライチェーン組織（航空管制サービス事業者（ANSP）、航空交通管理（ATM）事業者を含む） • 航空当局、サイバーセキュリティ当局
政策・規制	• 国際条約・EU 政策 – 国際民間航空条約（通称、シカゴ条約）第 17 附属書「保安」 – 欧州航空安全計画 2016–2020（欧州航空安全局（EASA）） – 欧州航空交通管理マスタープラン（単一欧州空域航空管制研究プロジェクト（SESAR）） • EU 規則・指令（抜粋※） – 欧州ネットワーク情報セキュリティ指令（通称、NIS 指令） – 航空交通管理、航空管制サービス等の提供および監督に関する規則（Commission Implementing Regulation (EU) No 2016/1377） – 飛行場、航空交通管理および航空管制業務の領域における規則（Commission Regulation (EC) No 216/2008） ※原文付録（9.2 節）に、スマート空港に関係する主な EU 規則・指令の一覧表あり

「スマート空港のセキュリティ」概要（2/6）

<table>
<tr><th>掲載項目</th><th colspan="3">概要</th></tr>
<tr><td rowspan="11">資産</td><td>資産グループ</td><td colspan="2">資産の例</td></tr>
<tr><td>空港管理</td><td colspan="2">資産管理システム、人材管理システム、調達管理システム、財務管理システム等</td></tr>
<tr><td>施設／メンテナンス</td><td colspan="2">ビル管理システム、★各種遠隔制御監視（SCADA）システム（ユーティリティ、エプロン関連制御等）、メンテナンス管理システム、危機管理システム等</td></tr>
<tr><td>職員管理</td><td colspan="2">採用管理システム、職員情報管理システム等</td></tr>
<tr><td>付帯サービス</td><td colspan="2">現金自動支払機（ATM）、モバイル決済システム、POS システム等</td></tr>
<tr><td>旅客管理</td><td colspan="2">★搭乗手続システム、搭乗券無人発行機（Kiosk）、電光掲示板システム、乗客予約記録（PNR）、予約システム（CRS）等</td></tr>
<tr><td>ランドサイド（一般区域）オペレーション</td><td colspan="2">コントロールセンターシステム、車両自動識別（AVI）システム、燃料管理システム、落雷検知システム、駐車場管理システム等</td></tr>
<tr><td>航空会社／
エアサイド（制限区域）オペレーション</td><td colspan="2">★航空交通管理（ATM）システム、★航法援助システム、ADS-B、デパーチャーコントロールシステム（DCS）、気象情報システム、融雪システム、飛行場灯火システム、滑走路制御監視システム、燃料給油システム、★空港資源・インフラ管理システム等</td></tr>
<tr><td>セーフティ ＆
セキュリティ</td><td colspan="2">★入退管理システム、★敷地・施設侵入検知システム、手荷物検査システム、★手荷物搬送システム、監視カメラシステム、爆発物検知システム、消防システム、★共用旅客情報システム（CUPPS）等</td></tr>
<tr><td rowspan="2">IT ＆ 通信</td><td>内部</td><td>★LAN、★VPN、★航空通信、Wi-Fi、IT 機器（ハードウェア・ソフトウェア）、ログ管理システム等</td></tr>
<tr><td>外部</td><td>WAN、クラウドサービス、衛星通信システム、位置情報システム、ネットワークセキュリティ管理システム等</td></tr>
<tr><td colspan="3">★は関係者へのヒアリングにおいて特に重要度が高いと見なされた資産
※原文付録（9.4 節）に、「脅威」「当該脅威の影響を受ける資産」のマッピングあり</td></tr>
<tr><td>脅威</td><td colspan="3">• 自然災害： 火事、洪水、地震等
• サプライチェーン障害： クラウドサービス、ネットワークサービス、電力供給等
• ヒューマンエラー： 設定ミス、誤った利用、対策の回避等
• システム障害： ソフトウェアや機器の不具合、過負荷等
• 悪意による攻撃行為
– サービス妨害（DoS）攻撃
– システムやソフトウェアの脆弱性の悪用
– 認証情報および権限の悪用
– ネットワーク盗聴／データ改ざん
– ソーシャルエンジニアリング攻撃
– 空港内の機器への不正アクセスによるデータ改ざんや機器の乗っ取り
– 物理的侵入
– 空港内の機器のマルウェア感染
– 空港内の機器や人間に対する物理的攻撃
※原文付録（9.4 節）に、「脅威」「当該脅威の影響を受ける資産」のマッピングあり</td></tr>
</table>

「スマート空港のセキュリティ」概要（3/6）

掲載項目	概要
攻撃シナリオ	• ソーシャルエンジニアリング攻撃 第三者が、空港職員に標的型攻撃を行って内部システムの認証情報を窃取し、空港の内部システムに侵入する。 • ネットワーク盗聴／データ改ざん 第三者が、航空無線や GPS 情報を妨害／改ざんし、航法に必要な情報が正しく認識できなくなる。 • 認証情報および権限の悪用 悪意のある内部関係者が、地上オペレーションのコントロールセンターからシステムを不正操作し、SCADA システムに不正なコマンドが送られる。 • 空港内の機器への不正アクセスによるデータの改ざんや機器の乗っ取り 第三者が、パブリックスペースにある搭乗券無人発行機（Kiosk）や、予約システム（CRS）に不正アクセス／操作し、搭乗券が間違った内容で発行されたり、情報が窃取されたりする。 • ネットワーク盗聴／データ改ざん 第三者が、不正なワイヤレスアクセスポイントや脆弱な Wi-Fi を通じて空港の内部システムに侵入する。 • 空港内の機器のマルウェア感染 第三者が、POS システムをマルウェアに感染させ、旅客のカード情報が窃取される。また、同じネットワークにつながっている機器やシステムに感染が拡大する。 • サービス妨害（DoS）攻撃 第三者が、DDoS 攻撃を行い、クラウドサービスや予約システム（CRS）等のオンラインサービスが利用できなくなる。 • システムやソフトウェアの脆弱性の悪用 第三者が、制御システムの脆弱性を悪用し、手荷物搬送システム、飛行場灯火制御監視システム等に侵入する。制御システムは通常直接インターネットにつながっていないが、LAN／Wi-Fi／USB 経由等で侵入される可能性がある。 原文では以下の攻撃シナリオについて、より詳細に「影響を受ける資産」「被害の重要度」「発生可能性」「重要関係者」「二次的影響」「復旧要因・時間」「対策」「課題」等をまとめている。 － 無人搭乗券発行機（Kiosk）への物理アクセスによる侵入（5.1 節） － 手荷物搬送システムへのネットワーク経由の侵入（5.2 節） － ドローンを用いた航空無線の妨害／改ざん（5.3 節）

「スマート空港のセキュリティ」概要（4/6）

掲載項目		概要
対策（グッドプラクティス）	技術的／ツールベースの対策	**適切なセキュリティ対策の実施** GP01：侵入検知システム（IDS） GP02：マルウェア対策ソフト GP03：機器のデフォルトパスワードの変更 GP04：Bring Your Own Device（BYOD）の制御 GP05：内部脅威の監視 GP06：ソフトウェア／ハードウェアのアップデート **ネットワークおよびデータに対するセキュアなアクセスの実施** GP07：システムの堅牢化 GP08：セキュリティリスク分析およびペネトレーションテストの実施 GP09：最低限の権限およびデータアクセス権の付与 GP10：データ暗号化 GP11：ファイアウォール、ネットワークのセグメント化、多層防御 GP12：強度が高いユーザ認証 **その他** GP13：シャットダウン手順／リスクに応じた資産のリモートシャットダウン機能の統合 GP14：アプリケーションセキュリティ、セキュア設計 GP15：災害復旧計画の策定
	ポリシー、標準	**情報セキュリティマネジメント** GP16：情報セキュリティマネジメントシステムの確立および国際標準に沿った対策の実施 GP17：情報セキュリティフレームワークの活用および外部監査による、対策の成熟度およびコンプライアンスの実証 GP18：情報セキュリティ責任者の任命 **プログラムマネジメント** GP19：情報および情報システムの棚卸しの実施 GP20：セキュリティ対策の有効性の検証と報告 GP21：情報の機密度に応じた情報システムの重要度の分類 GP22：リスク分析の実施 GP23　リスクの洗い出しおよびモニタリング GP24：情報セキュリティの継続的監視 GP25：国際標準および方法論的アプローチに従ったリスクの管理 **システム ＆ サービスの調達** GP26：情報システムサービスの提供者への、空港の情報セキュリティ要件への準拠および／または関連基準への認定取得の義務付け GP27：ソフトウェアのインストールに関する明確なルールの制定と徹底 GP28：開発者／SIer への、セキュリティ・プライバシー評価計画および発見された問題に対する検証可能な是正計画の策定・実施の義務付け

「スマート空港のセキュリティ」概要（5/6）

掲載項目		概要
対策（グッドプラクティス）	組織的対策	**職員のセキュリティ** GP29：各職員に対して情報システムへのアクセス権を付与する前における職員（人物）のチェック GP30：ユーザのアクセス管理 GP31：情報および情報システムへのアクセス権の認可前における、各職員に対するアクセスに関する合意書への署名の義務付け GP32：外部サービスプロバイダに対するセキュリティ要件の策定 **セキュリティ意識の向上・訓練** GP33：全ての情報システムユーザに対する基本的なセキュリティ教育の実施 GP34：役割・権限に応じた特別な情報セキュリティ訓練の実施 GP35：セキュリティ訓練内容のドキュメント化およびモニタリング GP36：セキュリティグループやセキュリティ団体との連携 **緊急管理／災害復旧** GP37：危機管理計画（contingency plan）の策定 GP38：災害復旧計画の策定 GP39：危機管理計画および害復旧計画において、各職員が事業継続のために果たすべき役割と責任に関する訓練の実施 GP40：危機管理計画、災害復旧計画の演習および評価の実施 **インシデント対応・報告** GP41：インシデント対応体制の整備 GP42：情報システムに関するインシデント対応において、各職員が果たすべき役割と責任に関する訓練の実施 GP43：情報システムに関連するインシデント対応体制の演習および評価の実施 GP44：情報システム関連のインシデントのドキュメント化およびステータスの追跡
		※原文の付録（9.5 節）に各対策（GP）の内容の説明あり

「スマート空港のセキュリティ」概要（6/6）

掲載項目	概要
課題	GAP1：空港ごとのサイバーセキュリティ対策状況の格差 GAP2：空港のサイバーセキュリティ対策に関する共通のアプローチや、マルチステークホルダーモデルの欠如 GAP3：複雑かつ空港によって異なるネットワークアーキテクチャ、システム／ネットワークの所有者、リモート管理の実態（存在するガイドラインと相違が大きく、ガイドラインを参考にすることが難しい） GAP4：空港のサイバーセキュリティを評価するメトリクスや基準の欠如、およびエビデンスベースのリスク分析や対策の優先度付けに関する理解の欠如 GAP5：ネットワークに関する脅威モデルおよびアーキテクチャ分析の欠如 GAP6：空港当局や国との情報共有の仕組みの必要性 GAP7：空港のスマート化にあたって、マルチステークホルダーが非協力的で独立したアプローチから、相互協力的で連携したアプローチに移行するための、信頼性フレームワーク、およびそのための技術の確立の必要性 GAP8：空港のスマート化に伴うセキュリティ意識および必要なスキルの欠如
提言	• 安全性に係るサイバーセキュリティ対策の優先的実施 • 空港のサイバーセキュリティ対策状況（セキュリティ強度）の把握と、適切な役割分担（最高セキュリティ責任者、最高経営責任者等の参画）およびリソースの割り当て • グッドプラクティスに基づくサイバーセキュリティポリシーおよび対策の見直し • システムのネットワークへの依存（ネットワークを通じた様々なシステムの相互依存性）、およびシステムやネットワークの所有者が頻繁に変わることを踏まえた、ネットワークベースの包括的な脅威／リスク管理ポリシーおよび手順の策定と実施 • スマート空港のサイバーセキュリティに関する共通のガイドライン、標準、メトリクス、情報共有の促進 • スマート空港のサイバーセキュリティの第三者監査および認定の仕組みの確立・促進 • 空港運営者、国際的な航空機関、サイバーセキュリティ組織等の主要なステークホルダーの連携による、サイバーセキュリティ製品およびソリューションの標準の開発 • 空港関連の製品、サービス、ソリューションの開発者・提供者と空港運営者の連携による、必要なサイバーセキュリティ要件を満たす製品、サービス、ソリューションの検討

以上