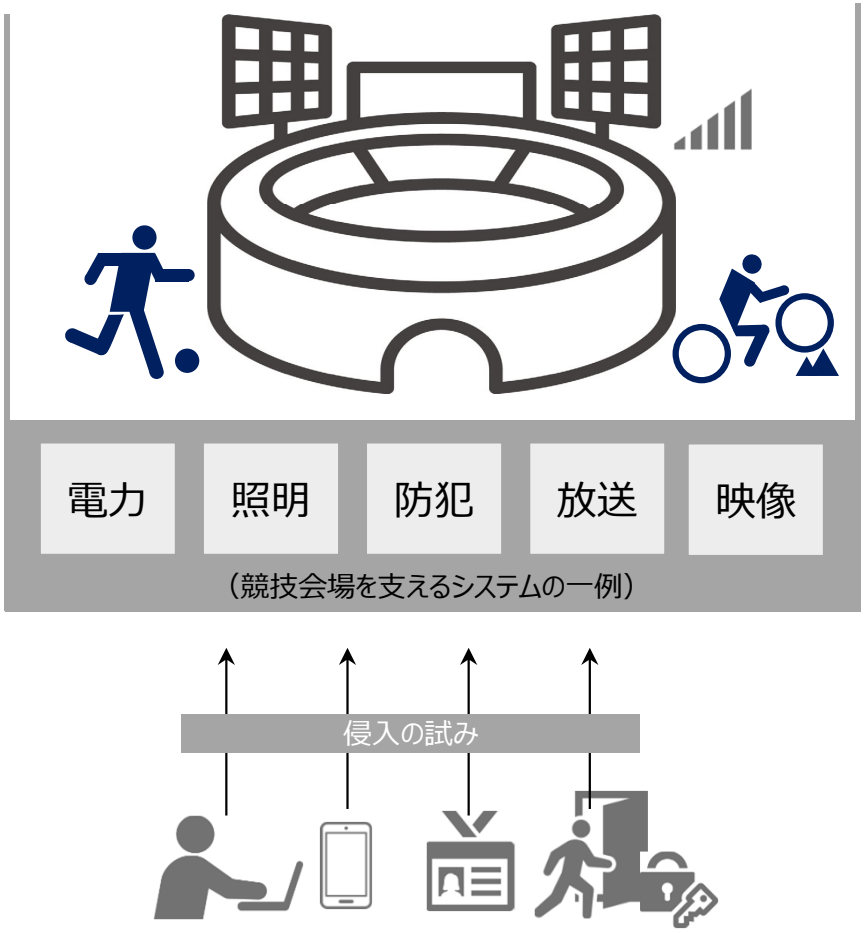
- 2021年に開催された東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）において、内閣サイバーセキュリティセンター（NISC）は競技会場の制御システムに対するペネトレーションテストを実施しました。
- そこで得られた知見については、東京大会の競技会場に限らず参考にできると考えられることから、テスト結果で判明した改善が必要な項目の事例を、攻撃者を利するおそれのない範囲で公開します。自組織のサイバーセキュリティ対策の水準の向上にお役立ていただければ幸いです。

競技会場に対するペネトレーションテスト



テストで判明した改善が必要な項目の事例

認証関連

- 認証情報が暗号化されずにファイル等に保存されている
- 通信経路上の認証情報が暗号化されていない
- 認証処理を技術的に迂回する方法が存在する

通信関連

- 組織内のネットワークから外部のネットワークに対して、意図しない通信が可能（アクセス許可設定のミス、導入した機器そのものの仕組みの理解不足など）
- 通信の改ざんにより設備を不正に操作する方法が存在する

物理セキュリティ関連

- 第３者が近づきやすい箇所にネットワーク機器が設置されている