指揮統制・AI・サイバー ・ 重要施設のサイバーセキュリティ

D-Cyber

C2 防護層 ・ 指揮統制とサイバー

既存の物理セキュリティおよび制御システムと連携する、重要施設向けのサイバー防護です。



主なメリット

01 **侵入の試みを早期に把握**
脅威や侵入の試みをリアルタイムで監視・検知します。

02 **重要サービスを止めない**
迅速に対応し、サービスの中断を防ぎます。

03 **セキュリティを一つの全体像に**
既存の制御・監視システム、そしてD-Command Controlと統合できます。

仕組み

01 **防護**
重要システムをデジタル攻撃から守ります。

02 **検知**
脅威や侵入の試みをリアルタイムで特定します。

03 **対応**
迅速な対処で重要サービスの稼働を維持します。

04 **統合**
イベントを現場の制御・監視システムと共有します。

仕様

対象	重要施設、国家の重要インフラ
機能	デジタル攻撃からの防護·脅威と侵入のリアルタイム検知·迅速な対応·既存の制御および監視システムとの統合
併用製品	D-FENCE PIDSおよびD-Command Control（物理セキュリティ＋サイバーセキュリティ）
C2ゲートウェイの無線機能(D-Command Control)	セキュリティのためWi-Fi / Bluetooth / セルラー通信は非搭載、ご要望に応じて追加可能
C2ゲートウェイの起動保護(D-Command Control)	外部ストレージからの不正起動を防ぐハードウェア保護
設置(D-Command Control)	セキュアな隔離環境での設置に対応
外部アクセス(D-Command Control)	セキュアなAPI、オペレーターのセキュアなアクセス
連携先(D-Command Control)	ファイアウォール、ウイルス対策、情報セキュリティシステム、IoT・SCADA

入札仕様書の記述例

1. 一般事項

本システムは、D-FENCE Electronic Fencing and Security Systems Ltd.(ISO 9001:2015認証取得の品質マネジメントシステム)のD-Cyber、または本項のすべての要件を満たす承認済みの同等品とすること。

2. 機能

既存の物理セキュリティおよび制御システムと連携する、重要施設向けのサイバー防護です。

3. システムは以下を備えること

- **インフラ防護:** 国家の重要インフラをデジタル攻撃から防護します。
- **リアルタイム検知:** 脅威や侵入の試みを、発生と同時に監視・検知します。
- **迅速な対応:** 迅速に対応し、重要サービスの中断を防ぎます。
- **完全な統合:** 現場の既存の制御・監視システムと連携します。
- **堅牢化C2ゲートウェイ:** 無線機能は標準で非搭載。不正起動を防ぐハードウェア保護を備えています。

4. 技術要件

- **対象:** 重要施設、国家の重要インフラ
- **機能:** デジタル攻撃からの防護·脅威と侵入のリアルタイム検知·迅速な対応·既存の制御および監視システムとの統合
- **併用製品:** D-FENCE PIDSおよびD-Command Control（物理セキュリティ + サイバーセキュリティ）
- **C2ゲートウェイの無線機能(D-Command Control):** セキュリティのためWi-Fi / Bluetooth / セルラー通信は非搭載、ご要望に応じて追加可能
- **C2ゲートウェイの起動保護(D-Command Control):** 外部ストレージからの不正起動を防ぐハードウェア保護
- **設置(D-Command Control):** セキュアな隔離環境での設置に対応
- **外部アクセス(D-Command Control):** セキュアなAPI、オペレーターのセキュアなアクセス
- **連携先(D-Command Control):** ファイアウォール、ウイルス対策、情報セキュリティシステム、IoT・SCADA

5. 検知シーケンス

1. **防護:** 重要システムをデジタル攻撃から守ります。
2. **検知:** 脅威や侵入の試みをリアルタイムで特定します。
3. **対応:** 迅速な対処で重要サービスの稼働を維持します。
4. **統合:** イベントを現場の制御・監視システムと共有します。

6. 提出書類

施工者は設置前に、製造者のデータシート、設置説明書およびゾーン配置図を提出し、承認を得ること。