\Orchestrating a brighter world NEC

文書番号：SLTH-20-003

遠隔監視制御システム

2020 年 11 月 26 日

コルソス CSDJ / CSDX お客様各位

NEC プラットフォームズ株式会社

コルソス シリーズ（ＣＳＤＪ、ＣＳＤＸ）の サイバーセキュリティ対策について（注意喚起）

拝啓　平素は弊社製品「コルソス」をご愛用賜わり厚く御礼申し上げます。

ネットワークに接続されているＩｏＴ機器につきましては、悪意のある第三者からの不正アクセスが増加してきており、セキュリティ上の脅威が広がってきています。特に、オリンピック・パラリンピック競技大会開が開催される近年、より一層そのリスクが高まっています。

このような状況下、総務省ではＩｏＴ機器を狙ったサイバー攻撃への対策について、該当機器の利用者への注意喚起を行う取り組みも行っています。

総務省　報道資料

https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00093.html

その中では、特に以下の点について指摘がされています。

・容易に推測されるパスワードを使用していたことによるサイバー攻撃

・管理画面トップページに重要施設であることが表示されていることによるサイバー攻撃

現在、「コルソス」は上下水道設備や農業用水、農業集落排水設備の監視用途で幅広くご利用頂いております。遠隔地の情報を収集・活用するための機能として、各種ネットワークに接続可能な仕様になっております。

また、監視状態の確認及びシステムの設定に関してもネットワークを介して可能となっておりますが、その際の ID・パスワードによる認証についても総務省による注意喚起の対象と考えられます。

つきましては、総務省の報道資料での注意喚起に従い、「コルソス」を安全にお使いいただくため、お客様におかれましては、本資料添付（ＣＳＤＪは総合説明書に記載）の『情報セキュリティ上のご注意』をお読みいただき、以下のご対応をお願いいたします。

・ID パスワードを初期値から変更すること
・強度の低い/類推されやすいパスワードを使用しないこと
・第三者からアクセスできるログイン画面の「ID 名称」、「社名ロゴ」に関して適切な表示設定を行うこと
・最新のファームウェアにしてご使用いただくこと

なお、ＩＤ・パスワード、ログイン画面表示の設定変更に関するお問合せは、ご導入を担当された販売店様または弊社へご連絡下さい。

敬具

添付資料（CSDJ 総合説明書 抜粋）

情報セキュリティ上のご注意　ー 必ずお読みください ー

安心してネットワーク接続するために必ずお読みください

本製品は、ネットワークに接続する機器であり、センサーで監視している内容や制御出力している内容等の情報を扱っている機器です。
これらの情報が意図に反して操作、漏洩等した場合、関係者に大きな影響を与えることが考えられます。
情報システムに対するリスクを認識し、対策されるようにお願い致します。

情報セキュリティの確保には、組織的、体系的に取り込むことが必要ですが、本項では本製品を使用する上での注意事項を記載しています。
詳細な情報セキュリティ対策は、参考資料等をご参照ください。
また、情報システムの安全性は、時とともに低下します。脆弱性が突然見つかることも有ります。適宜対策内容を見直すようにして下さい。

情報セキュリティ対策としては、「ウィルス感染」「不正侵入」「情報漏洩」「災害などによる機器障害」が上げられています（国民のための情報セキュリティサイト）。本製品では、下のような対策を取られるようお願い致します。
・ウィルス感染
本製品で使用しているソフトウェアに関するウィルスの報告は有りませんが、今後ウィルスが発生しないとは限りません。不正侵入への対策を行うことで、ウィルスの感染を防ぐようにして下さい。
・不正侵入
本製品は、ネットワークを通してシステムデータの設定や外部出力の制御、センサー等情報の取得等を行うことができます。これら情報の変更、制御、取得等により、CSDJ システムの停止等の重大な被害が発生する可能性が有ります。不正侵入への対策を行い、リスク軽減するようにして下さい。
・情報漏洩
本製品は、被監査機器等の情報をシステムデータや履歴等にて保持します。これら情報は、ネットワークを通して本製品から取得されますので、不正侵入への対策を行い、情報漏洩を防止するようにして下さい。
なお、本製品から取得した情報の漏洩防止は、取得、保持している側にて対策して下さい。
また、SD カードにはシステムデータや履歴が保存されています。盗難防止の対策をして下さい。
・災害などによる機器障害
本製品は、システムデータや履歴データをダウンロードすることができます。定期的にバックアップすることで、速やかに復旧できるようにして下さい。
ハードウェアに係わる機器障害については、システム全体にて検討するようにして下さい。

■不正侵入への対策
・ID、パスワード管理
ID やパスワードは、初期値のまま使用しないで下さい。
安全な（簡単に推測できない、単語をそのまま使用しない、アルファベットや数字、記号が混在している、適切な長さ、使いまわしていない）パスワードを使用して下さい。
また、使用者以外に ID、パスワードを開示しないで下さい。
・ネットワークの防御
外部からの不正なアクセスを遮断するために、ファイアウォール（専用機器または、インターネットプロバイダ提供サービスまたは、ルーター内蔵機能、等）や侵入検知/防止システムを導入して下さい。
・ソフトウェアの更新
脆弱性によるソフトウェアの更新が有った場合は、可能な限り迅速に更新プログラムを適用して下さい。
・ログの取得と管理
不正侵入に気付き、影響範囲の調査等に使用するために、定期的にコントロール履歴やログイン履歴、動作履歴を確認、保管して下さい
正しい時刻で記録するために、定期的に時刻合わせしてください。
（総合説明書関連項目）
コントロール設定__自動応答__アナログ応答
コントロール設定__自動応答__FOMA応答
コントロール設定__DTMFコントロール
コントロール設定__データコントロール
コントロール設定__ブラウザコントロール
監視データを記録する
通報などの履歴を表示する
時計を設定する
通報共通の設定（自動時刻補正）

■情報漏洩対策
・SD カード盗難防止
鍵のかかる場所に設置する等、外部や権限のない人が操作できないようにして下さい。

■災害などによる機器障害対策
・バックアップ
システムデータや履歴を定期的にバックアップして下さい。
（総合説明書関連項目）
データのセーブ（コルソス → PC）
監視データを記録する
通報などの履歴を表示する

■参考資料
・国民のための情報セキュリティサイト（総務省）
（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html）
・セキュリティ担当者のための脆弱性対応ガイド（情報処理推進機構）
（https://www.ipa.go.jp/security/vuln/index.html
→ https://www.ipa.go.jp/files/000058493.pdf）
・地方公共団体のための脆弱性対応ガイド（情報処理推進機構）
（https://www.ipa.go.jp/security/vuln/index.html
→ https://www.ipa.go.jp/files/000059718.pdf）
・制御システム利用者のための脆弱性対応ガイド（情報処理推進機構）
（https://www.ipa.go.jp/security/vuln/index.html
→ https://www.ipa.go.jp/files/000058489.pdf）