制御システムセキュリティカンファレンス

防御・回復・改善の企業課題について

VEC事務局

村上正志

制御システムセキュリティ対策での課題

1. 何が問題なのか
    1. 脅威の真相
2. どのような対策を考えていくか
    1. 防御
    2. 回復
    3. 改善
3. 何をすれば良いのか
    1. ユーザーの範囲
    2. 制御ベンダーの範囲
    3. SI、エンジニアの範囲
    4. 企業ではできないこと
4. どこまでやれるか
    1. 回復作業
    2. 予算化
    3. 妥当性の証明：査察

何が問題なのか：脅威の真相

1. 組織的攻撃
    1. 組織的サイバー攻撃部隊を持っているとされる国
        1. 中国、北朝鮮、イスラエル、アメリカ、など
    2. 攻撃理由
        1. 敵対国関係、その同盟国関係
        2. 利害競合関係国
    3. 攻撃レベル
        1. 制御の仕組みを知っている者が加わっている
            1. システム設計のみならず、Safetyの仕組みまで知っている
            2. 攻撃されていることを判らせない
2. ターゲット：
    1. 軍事施設や兵器製造施設
    2. 社会インフラの制御システム：社会的ダメージが大きいところ
       電力、ガス、水道、交通、通信、物流
    3. 社会的影響が大きい業界の制御システム
       医薬品、食品、トイレタリー
3. 目的
    1. 痛快犯罪：個人アタッカー
    2. 集団犯罪：同主張のグループアタッカー
    3. 戦争：インターネットを使った軍事兵器

制御システムの攻撃パターン

① インターネットから進入して生産計画を破壊／サーバーを乗っ取り、なりすましでオーダー変更

② SCADAに進入して、正常コマンドを出しているかのようにして誤ったコマンドをコントローラへ吐き出す。

③ 制御システムのコンフィギュレーションPCに侵入して、コマンド変更で誤った制御を行なう。

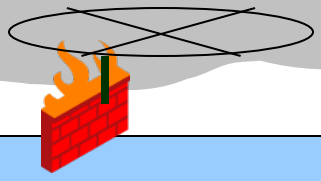
制御システムセキュリティⅠ

The Internet

企業IR

顧客へのサービス

顧客へ提供する製品情報サービス

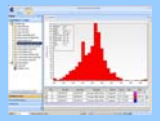


ERP
SCM
CRM

企業経営　事業企画　販売計画

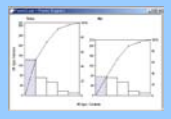
業務用サーバ
生産管理

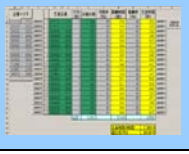
工場経営　商品企画　資産管理



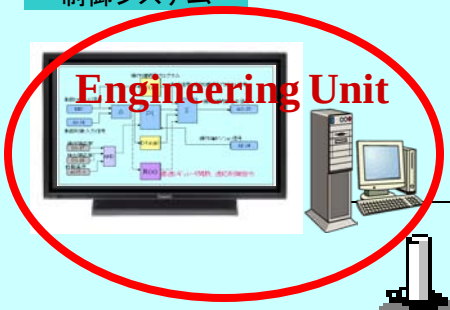
品質保証　人員配置管理

品質管理　設備管理

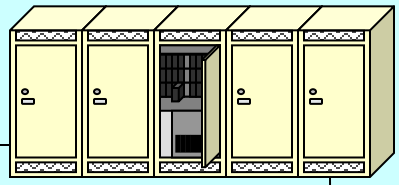


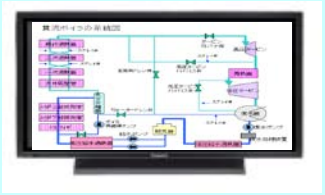


Process Automation
制御システム

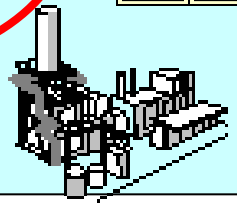


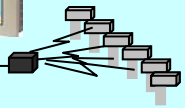
制御システム





制御用ネットワーク





Utility Automation
制御システム

制御システムセキュリティⅡ

どのような対策を考えていくか：防御

1. 軍事兵器化しているので、対策は1企業レベルでは防げない。
2. 防御の体制強化
    1. ユーザーができる範囲
        1. 製品を生産し供給することが役目
    2. 装置ベンダー・制御ベンダーができる範囲
        1. ユーザーが安心して使える制御製品を供給する役目
    3. SI、エンジニアができる範囲
        1. ユーザーの目的を果たす為に役立つ技術を提供する役目
    4. 業界を支える立場の団体の範囲
        1. JPCERT/CCの役目
            1. 防御技術情報の共有
            2. 個別支援：情報センターで終わって欲しくない。
    5. 行政ができる範囲
        1. 社会的安定を維持するために、ユーザー／装置・制御ベンダー／SI、エンジニア／業界団体が機能する環境を整備していく役目

どのような対策を考えていくか：回復

1. 回復の目的及び目標：

   協力して、ユーザーの役割を維持できるようにする

2. 役割

   1. ユーザーは、社会に対して製品を安心して安全に使ってもらえるように安定供給する義務を持っている。その為に生産を継続できる努力をしている。
      1. 作業者の安全
      2. 環境への安全
      3. 製品の安全：品質の維持
      4. 安定供給の確保
   2. 装置ベンダーや制御ベンダーはユーザーに安心して生産事業を継続できるような製品を開発し、提供するべく努力している。
   3. SI、エンジニアは、ユーザーの目的をユーザーが目的を果たせるように技術を提供できるように努力している。

3. 回復作業

   1. 応急治療：生産を継続できるようにする。
   2. 治癒治療：元の正常状態に戻す。
   3. どこまで支援ができるか。

どのような対策を考えていくか：改善

1. 改善の目的及び目標
    1. 攻撃に強い生産／制御システムに改善する
2. 対策：手当て
    1. 体制強化
        1. ユーザーとSIと装置ベンダーと制御ベンダーの連携強化
    2. 体質強化
        1. 人、モノ、金、技術、情報
            1. 人：対処できる人材の確保
            2. モノ：ステルス化したサイバー攻撃に強い制御製品
            3. 金：適切と思われる投資の確保
            4. 技術：セキュリティ技術の研究
            5. 情報：JPCERT/CCに登録
                1. ユーザー会員
                2. 制御ベンダー会員

何をすれば良いか

A) 生産システムの健全性を確保
B) 制御システムコンフィギュレーションツールの健全性を確保
C) 監視制御システム製品の健全性を確保
D) 攻撃パターンの解析とワクチン開発：専門研究所＋企業連携
E) ユーザーとベンダーとシステムエンジニア／システムインテグレータの連携ネットワーク
F) それらを支援する組織：サポートサービス
G) 人材確保と育成：エキスパートエンジニア
H) 制御システムセキュリティに関する認識⇒スキルアップ教育

ABCは、現場。DEFは、体制。GHは、体質強化。

何をすれば良いのか：ユーザーの範囲

1. 現状把握
    1. 制御製品のサイバー攻撃に対するリスク把握
2. できる範囲の設定
    1. 体制強化
        1. ユーザーとSIと装置ベンダーと制御ベンダーの連携強化
    2. 体質強化
        1. 人、モノ、金、技術、情報
            1. 人：対処できる人材の確保
                1. エキスパートの育成と確保
                2. 訓練
            2. モノ：ステルス化したサイバー攻撃に強い制御製品を適用する範囲
            3. 金：適切と思われる投資の確保；予算化
            4. 技術：セキュリティ技術の研究：研究しているベンダーもしくはその情報をつかんでいるベンダーを選択
            5. 情報：JPCERT/CCに登録
                1. ユーザー会員
                2. 制御ベンダー会員

何をすれば良いのか：制御ベンダーの範囲

1. 現状把握
    1. メーカー責任の範囲
    2. 製品の企画段階から考慮しなければならないこと
        1. 制御システムセキュリティ対策できる製品／できない製品
    3. サポートサービスでの対策
2. できる範囲の設定
    1. 体制強化
        1. ユーザーとSIと装置ベンダーと制御ベンダーの連携強化
    2. 体質強化
        1. 人、モノ、金、技術、情報
            1. 人：人材の確保
                1. エキスパートの育成と確保
                2. ユーザーサポート訓練：緊急性が高い場合
            2. モノ：ステルス化したサイバー攻撃に強い制御製品を開発
            3. 金：適切と思われる投資の確保；予算化
            4. 技術：セキュリティ技術の研究：研究しているベンダーもしくはその情報をつかんでいるベンダーとなる
            5. 情報：JPCERT/CCに登録
                1. ユーザー会員
                2. 制御ベンダー会員

何をすれば良いのか：SI、エンジニアの範囲

1. 現状把握
    1. 制御システムセキュリティについての情報を入手しているか
    2. 対処できる技術を持っているか
2. できる範囲の設定
    1. 体制強化
        1. ユーザーとSIと装置ベンダーと制御ベンダーの連携強化
    2. 体質強化
        1. 人、モノ、金、技術、情報
            1. 人：人材の確保
                1. エキスパートの育成と確保
                2. ユーザーサポート訓練：緊急性が高い場合
            2. モノ：ツールを持っていて使える
            3. 金：適切と思われる投資の確保；予算化
            4. 技術：セキュリティ技術の研究：コンサルと対策ができるレベル
            5. 情報：JPCERT/CCに登録
                1. ユーザー会員
                2. 制御ベンダー会員

何をすれば良いのか：企業ではできないこと

1. 業界を支える立場の団体の範囲
    1. JPCERT/CCの役目
        1. 防御技術情報の共有
        2. 個別支援：情報センターで終わって欲しくない。
2. 行政でやって欲しいこと
    1. 社会的安定を維持するために、ユーザー／装置・制御ベンダー／SI、エンジニア／業界団体が機能する環境を整備していく役目

どこまでやれるか

1. 回復作業
    1. 応急治療：生産を継続できるようにする。
    2. 治癒治療：元の正常状態に戻す。
    3. どこまで支援できるか。
2. 予算化
3. 妥当性の証明：査察