プラントネットワークセキュリティ

Plant Network Security

福　山　　真　一[*1]　　**小　川　　永志樹**[*1]
FUKUYAMA Shinichi　　OGAWA Toshiki

プラントをネットワーク経由の不正アクセスから守るための，プラント総合セキュリティ対策サービスを紹介する。このサービスは，通産省“大規模プラントネットワークセキュリティ委員会”での活動成果を基に，プラントにおける総合セキュリティ対策を提供するものである。本サービスは，プラントネットワークに対するリスク分析を基にしたセキュリティポリシーの構築，技術的対策の提供，更に継続的なセキュリティ対策の実施を目指した不正アクセス監視サービスの提供を行うことで，永続的にプラントをセキュアに保つことを目指している。

This paper introduces the plant Integrated Security Countermeasures Service to protect the plant against unauthorized access via networks. This service provides the integrated security countermeasures for the plant based on the activity results of "Large-scale plant network security countermeasures committee" of the Ministry of International Trade and Industry. This service aims to keep the plant secure by providing construction of the security policy based on the risk analysis of the plant network, offering technical countermeasures, and offering the monitoring service against unauthorized access toward executing further continuous security countermeasures.

1. はじめに

当社の顧客である石油，化学，電力，鉄鋼，紙パ，水道などは社会的な重要インフラストラクチャーであり，これらのプラントがサイバーテロリストやクラッカーなどの標的にされた場合，社会生活に大きな支障をきたすことが予想されている。昨今の中央省庁のホームページ改竄に見られるように，ネットワーク経由の脅威は日毎に大きくなっており，DCSを含む制御システムのオープン化の流れを考えるとプラントに対する脅威も現実の問題として認識し，適切な対応を取ることが必要と考えられる。このような認識の下，日本でも平成９年度から11年度にかけて通商産業省委託事業“大規模プラントネットワークセキュリティ対策委員会”(通称PSEC)がユーザ，ベンダ，エンジニアリングの各企業の代表及びセキュリティ有識者により結成され，調査，研究が進められてきた。当社もベンダ企業として，その中核メンバとして活動してきており，今回ここでの成果を基に，プラントのネットワークセキュリティレベルの向上を目指したプラント総合セキュリティ対策サービスを提供することとなった。本稿では，その内容について説明する。

*1 IA事業本部　システム事業部

2. 制御システムの現状

先に説明したPSEC中間報告書の具体的検証のため，IPA(情報処理振興事業協会)の次世代ディジタル応用基盤技術開発事業の一つとして，現状の制御システムのセキュリティの実情を調査するために模擬制御システムを構築し，外部アタッカーによるネットワーク経由のペネトレーションテストを実施した。(**図１**参照)結果として，次ぎのことが明確になった。

① 制御システムの脆弱性は，オープンなOS，オープンな通信プロトコルによる部分が大きい。
② VLnetのようなベンダ独自の通信プロトコルの環境では，侵入が難しい。
③ プロコン等のDCSに接続される機器が脆弱な場合，その機器を踏み台にしたDCSへの不正アクセスは比較的容易である。
④ 適切なパスワードの設定や不必要なネットワークサービスの削除など，基本的なセキュリティ設定をオープンな機器に施すこと(要塞化)で，セキュリティ強度をある程度引き上げることができる。

また制御システムへの対策を考えた場合，以下を考慮する必要がある。

① 24時間稼働が前提であるので,機器を止めることが難しい。
② 製品寿命が長く，機器の入れ替えが難しい。

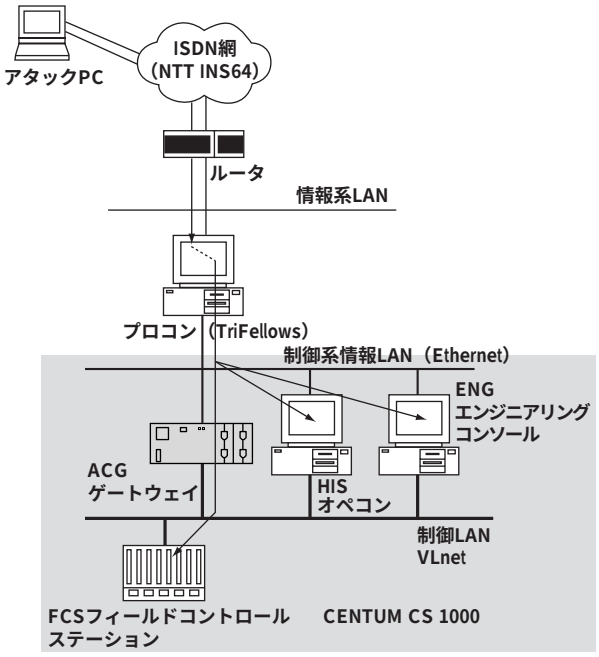

図１　PSECペネトレーションテストシステム構成

③ 操作出力，可変パラメータ，測定値，制御プログラムなどの改竄の防止が第一優先。（これらの値の改竄はプラント事故につながる）

④ 既存プラントは，ネットワークセキュリティに対する対策が殆ど取られておらず，プラントの数としてはこの状態のものが最も多い。

以上を前提に対策を考えた場合，制御システム自身をセキュアな環境で囲い込むことが妥当であると考えられる。このアプローチと利点としては，DCSの機種に依存することなくサービスを提供できるため，他社DCSが導入されているプラントでもサービス対象とできることが挙げられる。

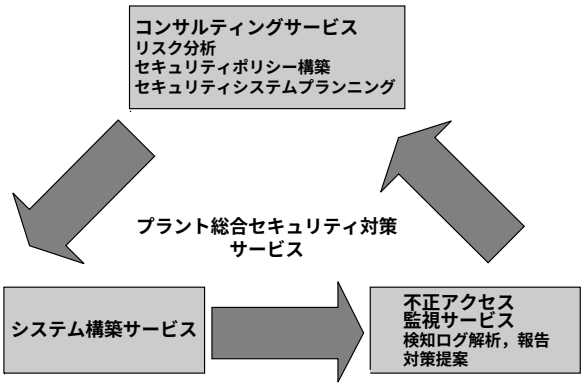

図２　セキュリティ対策サイクル

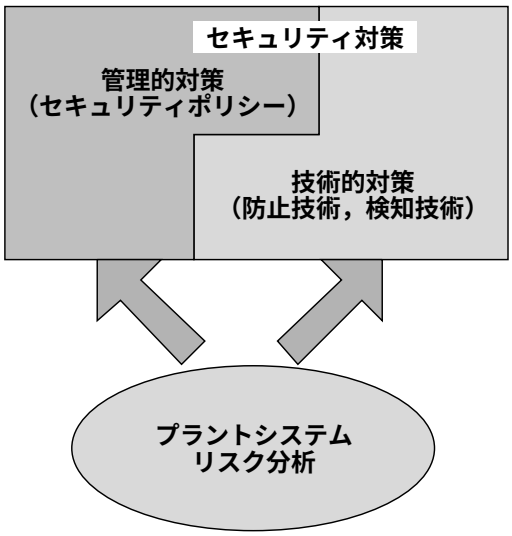

図３　セキュリティ対策の考え方

3.　セキュリティ対策サイクル

セキュアな環境を維持するためには，**図２**で示すようなサイクルを永続的に廻す必要がある。これは，日毎に新しいセキュリティホールが発見され，或いは新しい不正アクセス手法が生まれているからである。プラント総合セキュリティ対策では，このサイクルの各局面についてサービスメニューを用意して，永続的にプラントをネットワークの脅威から守ることを想定している。

またセキュリティ対策には，**図３**に示すように２つの側面がある。現在100%のセキュリティを確保できる技術は存在しないため，管理的対策と技術的対策を併せて実施することで，バランスのとれたセキュリティ対策を取る必要がある。またセキュリティ対策を行う場合，対象とするシステムのリスクを分析し，リスクがもたらす損失の度合いから優先順位を明確にした上で，対策を検討する必要がある。システムのセキュリティ上の脆弱性は，システムの一番弱い部分で決まるという特性があることから，リスク分析無しに闇雲に対策を行うと十分な投資効果が上がらない恐れがある。このことから，本サービスでは，リスク分析をベースにしたサービス展開を行っている。

またプラントにおけるセキュリティ対策を検討する場合，**表１**で示す制御系システムの特長を十分考慮する必

表１　システムに対する考え方

項　目	情報系	制御系
システム形態	人が中心のクライアント,サーバ	装置が中心の自動制御機器の連携
ネットワーク接続機器	コンピュータ,周辺機器	制御装置（専用機またはコンピュータ）
不正アクセスに関する考え方	情報漏洩・破壊	誤動作・事故
不正アクセスの意識	経営者も含め意識が出てきた	問題意識が低い

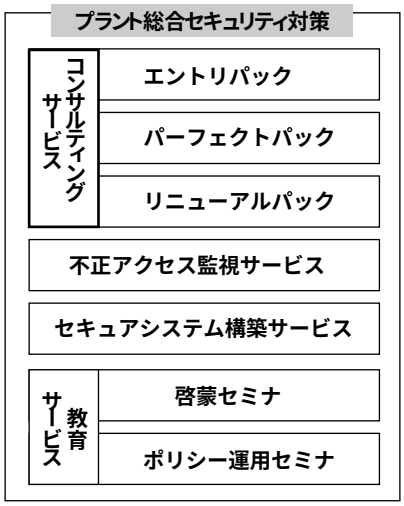

図4　サービスメニュー構成

要がある。またこの部分の認識が，DCSベンダがセキュリティ対策を行う場合の強みとなっている。

4. プラント総合セキュリティ対策

図4に本サービスのメニュー構成を示す。

4.1 コンサルティングサービス

(1) エントリパック

現状のプラントのセキュリティレベルを診断，評価するサービスである。プラント向けに用意された質問票により，セキュリティの充足度を診断し報告する。またオプションで，プラントのプロコン等のコンピュータ向けのスキャナサービスを用意している。このサービスでは，商用のスキャニングツールを利用し，既知のセキュリティホールの有無を検査し，技術的対策を提案する。このサービスは，顧客自身がセキュリティ対策を進める場合の対策の注力点や方向性を提示することを目的としている。**図5**に質問票及び診断報告書の具体例を示す。

(2) パーフェクトパック

プラントのリスク分析，セキュリティポリシーの策定，セキュリティシステムプランニングまでを行う本サービスの中核となるメニューである。リスク分析では，脅威のリストアップを行い，その脅威が現実のものとなった場合，プラントにもたらすであろうリスクを洗い出す。こうして洗い出されたリスクについて，その重要度をプラントへの影響度及び顧客の業務内容から導き出し，各リスクに対して具体的な対策を技術的観点，管理的観点から立案する。セキュリティポリシーはこうして立案された対策か

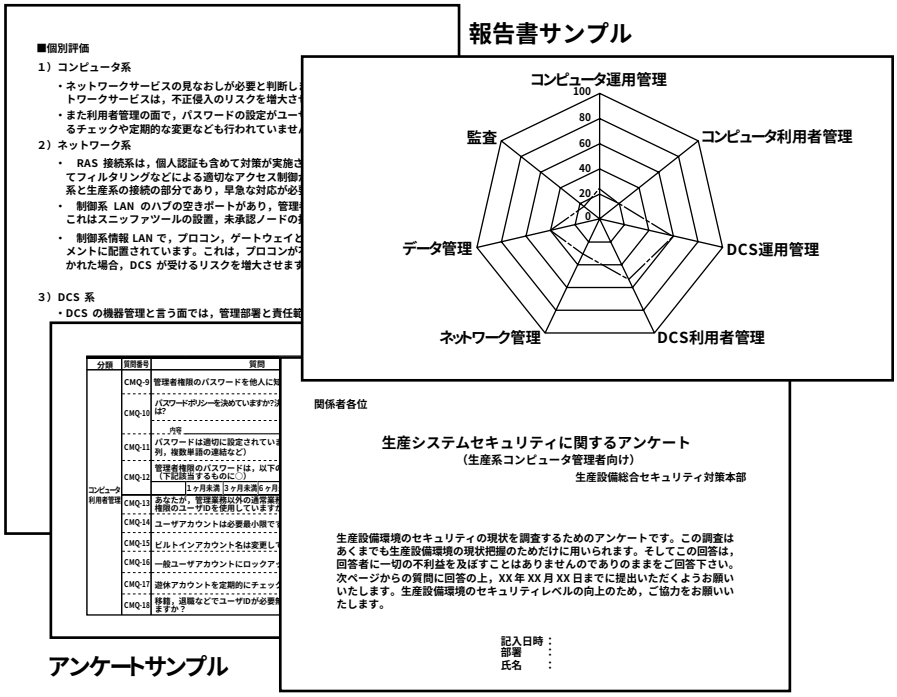

図5　エントリパック質問票，診断報告書例

ら管理的要素を抜き出して，具体的な規定，ガイドライン，手順書として策定する。

(3) リニューアルパック
パーフェクトパックにて，セキュリティ対策を取られた後，システム構成の変更等が発生した時，或いは，不正アクセス監視サービスで新たな脆弱性が発見された時に，再度システムのセキュリティを見直し，更新されたシステムをセキュアに保つことを目的としたサービスである。システム変更部分のリスク分析をベースに，既存システムに与える影響を分析し，対策を提案する。この時，技術的対策に加え，セキュリティポリシーの見直しを行い，必要であれば改訂を行う。

4.2 セキュアシステム構築サービス

コンサルティングサービスで，提案した技術的対策を具体的にセキュリティ技術を組み合わせて実現する。ここでは，ファイアウォールや認証などの新規機器の導入，設定及び既存機器のセキュリティ設定等のサービスを客先の制御システムに対して行う。

4.3 不正アクセス監視サービス

このサービスでは，客先システムに監視ツールを導入し，24時間 365日体制で不正アクセスを監視する。ここで不正アクセスが検知された場合，客先への通知と対策を提案する。不正アクセスは，具体的な侵入行為の前にターゲットのアドレス情報やセキュリティホールの探査が行われるので，そのパターンを検知することで不正アクセスを未然に防止することも期待できる。

4.4 教育サービス

セキュアな環境を維持していくためには，適切に策定されたセキュリティポリシーに従ったシステムの運用，業務の遂行が必要とされる。運用，業務を遂行する者が，セキュリティに対して正しい認識を持ち，セキュリティポリシーの必要性を認識しないと， セキュリティポリシーの適切な運用は期待できない。本サービスでは，プラントオペレータや管理者を対象にしたセキュリティの啓蒙教育とセキュリティポリシーの運用教育を提供し，セキュリティポリシーの適切な運用を支援する。

5. 今後の課題

制御システムの中核を成すDCSにおいて，オープンなプラットフフォームを採用することは，必然的にその脆弱性を背負い込むことになることを自覚して，DCS自体のセキュリティレベルを上げていくことが必要であると考えている。またISO15408のJIS化に象徴されるように，ネットワークに接続される機器は，自身のセキュリティ機能の客観的評価に拠る認証取得が，ユーザから要求されるようになると考えられる。当社では，今後これらの動向を的確にウォッチし，DCS自身で装備すべきセキュリティ機能の開発につなげて行くことを考えている。

１年前のＹ2K問題では，政府からのアンケートに情報システムだけでなく制御システムでの回答を求められ，国を挙げて対応を取ってきた。Y2K問題とネットワークセキュリティ問題は，認知・分析・対策・危機管理など対応の流れは大変良く似ており，米国ではY2K問題の対応はネットワークセキュリティ問題の予行演習であったとも言われている。現在，ネットワークセキュリティの重要性は，ITの世界では急速に認知されてきており，セキュリティポリシーの重要性も認知されつつある。しかしながら，プラントにおけるネットワークセキュリティの重要性の認知度はまだまだ低い状態であることが現実である。従って，本サービスをプラントに浸透させるためには，DCSユーザへの啓蒙活動が最優先と考えている。

6. おわりに

現在，国内及び海外のユーザからプラントのネットワークセキュリティ対策の相談が寄せられており，一部先進的ユーザでは，リスク分析に基づくプラント向けセキュリティポリシーの構築も進められつつある。特に近年，広域網を介した複数プラントの統合や，或いは本社基幹システムへの生産系システムの接続などの事例が多くなってきている。今後は，プラント総合セキュリティ対策サービスを中核にして，ユーザの投資効果が十分に得られるような的確なセキュリティ対策を進めて行きたいと考えている。

参考文献

(1) 通商産業省委託事業大規模プラントネットワークセキュリティ対策委員会, “大規模プラントネットワークセキュリティについて”, 平成10年3月，中間報告書，1998
(2) 同上，平成12年3月，最終報告書，2000
(3) 同上，平成12年3月，資料編，2000
(4) 情報処理振興事業協会, “大規模プラントネットワークセキュリティ 技術開発／実証実験”, 安全性検証実験報告書，平成12年３月，2000