TNO report

上水道分野用のSCADA（監視制御システム）セキュリティ グッド・プラクティス ～重要インフラのセキュリティ向上にむけて～

SCADA Security Good Practices for the Drinking Water Sector

TNO | Knowledge for Business

samen tegen cybercrime
NICC

翻訳・監修 IPA

本ページは白紙です

奥付

著者・編集者
Eric Luiijf MSc (Eng) Delft
TNO Defence, Security and Safety
P.O. Box 96864
2509 JG The Hague, The Netherlands
T: +31 70 374 0000
E: eric.luiijf@tno.nl
W: www.tno.nl

発行
National Infrastructure against Cyber Crime (NICC)
A programme of the ICT Uitvoeringsorganisatie (ICTU)
P.O. Box 84011
2508 AA The Hague, The Netherlands
T: +31 70 888 7777
E: nicc@ictu.nl
W: www.ictu.nl
This is a Japanese translation of the report SCADA Good Practice voor de Nederlandse Drinkwatersector, TNO DV 2007 C478, December 2007.

翻訳
Language Unlimited B.V.
Utrecht, The Netherland

日本語翻訳
岡下博子（独立行政法人情報処理推進機構※、IT 働楽研究所）
※2009 年現在非常勤研究員

日本語翻訳協力者
大崎　雅也（水野薬局）
織茂　昌之（日立製作所）
杉野　隆　（国士舘大学）
武本　敏　（日立製作所）
平山　修久（京都大学）
森安　隆　（日立製作所）
渡辺　研司（長岡科学技術大学）
小林　偉昭（独立行政法人情報処理推進機構)
中野　学　（独立行政法人情報処理推進機構）
長谷川智香（独立行政法人情報処理推進機構）

レイアウト
Nicolaas van der Bent, TNO Defence, Security and Safety

表紙写真
Oasen Drinkwater, by Van Eijndhoven

発行日
2009 年 11 月 30 日

概要

オランダ上水道分野 SCADA セキュリティ グッド・プラクティスは、プロセスオートメーション（PA：Process Automation）における監視制御（SCADA:：Supervisory Control and Data Acquisition）や他の情報通信（ICT：Information and Communication Technology）システム、ソフトウェアに対するサイバー的な不正操作への、上水道分野全体の抵抗力の水準を向上させることを目的とする。

水道水の供給と水質を保証し、システムが権限の無い第 3 者から不正に操作されないことを確実にするためには、SCADA 環境、システム、ネットワークの有効な防護が必要不可欠である。水道水の供給停止による社会的影響は深刻であり、SCADA に対するリスクの管理は必須である。想定される影響として、社会不安、公衆衛生への影響や多大な経済的損害が発生することも考えられる。

ICT Implementation Organisation（ICTU）が運営する Dutch National Cyber Crime Infrastructure（NICC） プログラムからの要請により、TNO Defence, Security and Safety 社では 、上水道分野を対象とした 39 項目からなる SCADA セキュリティ グッド・プラクティスをまとめた。これらは、企業の経営層が責任を持って行うべき対策と、プロセスオートメーションの技術面での管理についての対策に分類されている。
これらのグッド・プラクティスは、上水道分野に対し安全に SCADA を使用するためのガイドラインを提供するものである。本書に記した対策は、国際標準、業界標準、SCADA に関わる事業者により適用されたセキュリティ対策成功事例に基づいている。

翻訳に当たって

欧米では電力、水道、ガスを初め多くの重要インフラで使用されている制御システムの機器(センサ、アクチュエータ等)やそれらの監視装置のセキュリティ上の問題が重要インフラ防護の観点から官民一体となって推進されています。今回翻訳して提供します上水道分野の監視制御システムである SCADA のセキュリティ ベスト・プラクティスは、欧米の重要インフラ防護の関係者で有用性が認められ、多くの国で重要インフラの制御システムセキュリティを検討する際の参考資料として活用されています。

日本の重要インフラ制御システムにおいても、汎用製品の利用やオープンなプロトコル TCP/IP の採用が進められており、パソコンやサーバを活用している情報システムと同様、セキュリティ上の脅威への対策が急務となってきています。このガイドは水道分野だけでなく、ガスや電力など他の重要インフラ分野での制御システムのセキュリティ対策にも適用できると考え、有識者の協力を頂いて日本語翻訳し、広く普及・啓発を進めていくことにしました。
皆様の活用をよろしくお願いします。

独立行政法人 情報処理推進機構（IPA) セキュリティセンター
情報セキュリティ技術ラボラトリー長
小林　偉昭

Contents

表・図一覧

表Tables

図

略称一覧

BCP	Business Continuity Planning（事業継続計画）
COTS	Commercial-Off-The-Shelf（市販品）
CPNI	(UK) Centre for the Protection of National Infrastructure
DCS	Distributed Control Systems（分散型制御システム）
DNP	Distributed Network Protocol
DoS	Denial-of-Service（サービス妨害攻撃）
ERP	Enterprise Resource Management（企業資源管理）
EWICS	European Workshop on Industrial Computer Systems Reliability, Safety and Security
GPRS	General Packet Radio Service（無線パケットサービス）
HMI	Human-Machine Interface（ヒューマン・マシン・インターフェース）
ICT	Information and Communication Technology（情報通信技術）
IEC	International Electro-technical Committee（国際電気標準会議）
IEEE	Institute of Electrical and Electronics Engineers（電気電子技術者協会）
IP	Internet Protocol（インターネットプロトコル）
ISA	Instrumentation Systems and Automation Society
ISO	International Organisation for Standardisation（国際標準化機構）
LAN	Local Area Network（ローカルエリアネットワーク）
MAC	Media Access Control（メディアアクセス制御）
MES	Manufacturing Execution System（製造実行システム）
MTU	Master Terminal Unit（マスター・ターミナル・ユニット）
NICC	(NL) Programma Nationale Infrastructuur Cyber Crime (National Cyber Crime Infrastructure programme)
NISCC	(UK) National Infrastructure Security Co-ordination Centre（現 CPNI）
PA	Process Automation（プロセスオートメーション）
PLC	Programmable Logic Controller（プログラマブル・ロジック・コントローラ）
POTS	Plain Old Telephony System
RTU	Remote Terminal Unit（リモート・ターミナル・ユニット）
SCM	Supply Chain Management（サプライチェーンマネジメント）
TCP	Transmission Control Protocol（通信制御プロトコル）
TNO	Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek (Netherlands Organisation for Applied Scientific Research)
UMTS	Universal Mobile Telecommunication System
VEWIN	Vereniging van Waterbedrijven in Nederland (Association of Dutch Drinking Water Companies)
VPN	Virtual Private Network（バーチャルプライベートネットワーク）
WAN	Wide Area network（広域ネットワーク）

1 はじめに

プロセス制御システム（Process control systems）、とりわけ、監視制御システム（SCADA: Supervisory Control And Data Acquisition）[1]は、オランダにおける、水道水の供給と、その水質の保証に必要不可欠なものである。
2007 年 5 月～6 月に実施した National Cyber Crime Infrastructure（NICC）プログラムでは、オランダの水道事業者におけるプロセスオートメーション（PA）環境のセキュリティ対策について、アンケートにより調査した。
その調査結果によると、水道事業者によって SCADA のセキュリティ対策状況に大きな違いがあることがわかった[1]。つまり、いくつかの水道事業者では、水道水の供給と水質の保証に関するリスクとともに運用されている（又はリスクの認識ができていない）場合があり、そのような事業者の SCADA セキュリティには改善の余地があることが判明した。本書はこうした理由から、上水道システムの SCADA セキュリティのグッド・プラクティスとして策定された。

本書は次のように構成されている：
第 2 章は、SCADA とは何か、深刻化するリスク要因（脅威）にはどのようなものがあるか、そしてプロセスオートメーション（PA）環境に存在する脆弱性及びその理由について簡単に記載している。
第 3 章では、水道事業者の経営層（management teams）を対象に、 前述の調査結果[1]と、国際標準や文献に基づく SCADA セキュリティのグッド・プラクティスを記載している。本書に示すグッド・プラクティスは法的効力があるものでも、義務でもないことを改めて強調しておきたい。水道事業者が同じレベルを保証しつつも、企業文化や、組織的、アーキテクチャ上、及び技術的な理由から、全く異なるセキュリティシステムの導入を選択する可能性もある。いずれにせよ、対策が十分ではないリスク要因・脅威（セキュリティギャップ）を把握し、対策を進めるためには、導入しているセキュリティ対策を本書のグッド・プラクティスと照らし合わせてみることが望ましい。グッド・プラクティスは、オランダの水道事業者がオフィス環境の情報セキュリティ対策の基本としている「情報セキュリティマネジメントの実践のための規範」（[3] [6]）と密接に関連している。

グッド・プラクティスの策定にあたっては、水道事業者の中で既にグッド・プラクティスを適用し、実践している事業者がいる可能性も考慮した。その場合、水道事業者は、同業者からグッド・プラクティスの導入方法と実践経験を学ぶことができる。NICC を通してでも良いし、違う方法を取ることもできる。
第 4 章は、同様に、技術面での PA 管理のためのグッド・プラクティスを記載している。
第 5 章は、それぞれのテーマ別に参照できる SCADA セキュリティ関連の文献やウェブサイトの情報を記載している。
第 6 章は、参考文献を記載している。また、付録 A として、グッド・プラクティスを項目別に分類した 2 種類のチェックリストを記載している。

[1] 特に特別な事情がない限り、 SCADA をプロセス制御システムの汎用語として用いるものとする。

2 SCADA と SCADA セキュリティ

本章では、SCADA とは何か、SCADA への深刻化する脅威、並びに PA 環境に存在する脆弱性及びその理由について簡単に説明する。本書の内容は、オランダ経済省（Dutch Ministry of Economic Affairs）の同意を得、オランダ国内及び国外におけるイニシアティブやその他の活動の概略など、SCADA の情報セキュリティ問題について詳しく取り上げている TNO-KEMA 報告書"SCADA (in)security: a role for the government?"に基づいている。

2.1 SCADA、 PCS、DCS、RTU、 PLC とは

ISA-95 の製造モデル[14]では、PA を次の 5 つの階層に区分している。

- レベル 0：物理レベル：センサ、アクチュエータ、処理装置
- レベル 1：センサ出力、アクチュエータコマンド、コンピュータ制御・監視（プログラマブル・ロジカル・コントローラ（PLC））
- レベル 2：制御監視システムレベル（SCADA）、ヒューマン・マシン・インターフェース（HMI）
- レベル 3： 製造実行システム（MES: Manufacturing Execution System）：「製造」にあたっての資源・原料・人材（「リソース」）の最適化 支援
- レベル 4：企業資源管理（ERM: Enterprise Resource Management）や サプライチェーンマネジメント（SCM: Supply Chain Management）などのビジネス計画及び物流管理を含む企業資源計画（ERP: Enterprise Resource Planning）

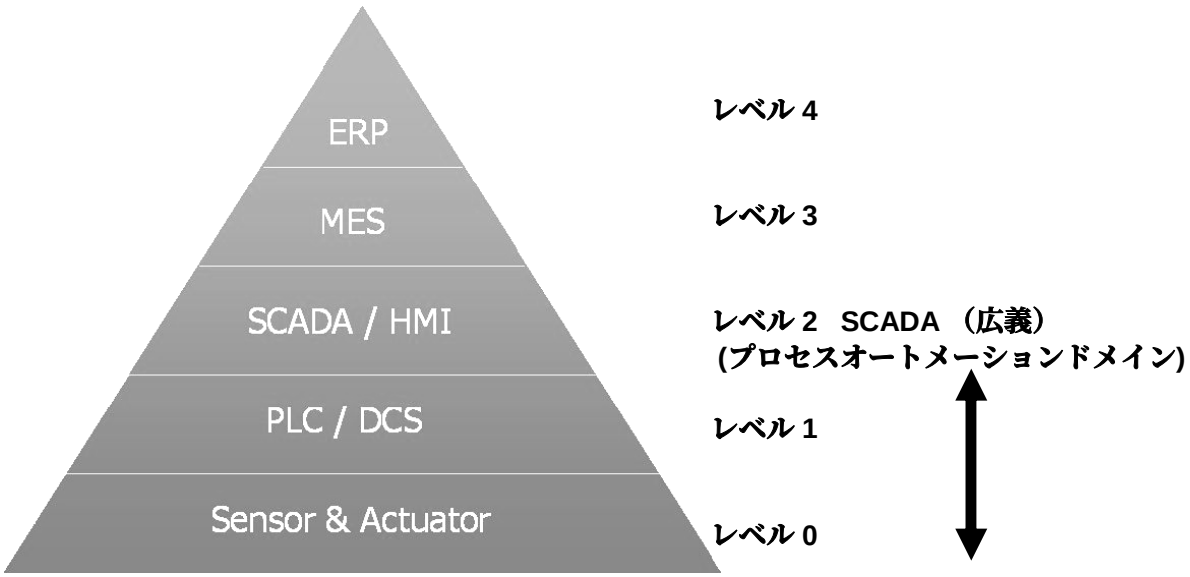

図 1 ISA95-1 の製造モデル

レベル 2 の SCADA/HMI では、以下のタスクを実行する。

1. 各箇所の処理装置の可視化及びオペレーション（人と機械とのインターフェース）
2. プロセス制御システムレベル（通常、PLC）とのデータ交換
3. アラーム管理、動向解析及び報告

4. 過去データのログ作成及び保管（”historian”）
5. バッチ運用 （SCADA パッケージではオプション）
6. ユーザ管理
7. データ解析及び処理
8. 製造実行システム（MES）レベル、経営管理システムレベルとのデータ交換

各レベルには固有のセキュリティ対策があるという認識が重要である。しかし、ここでは、下位 3 レベルにおける情報セキュリティ、及び上位レベルとのデータのやり取りについて取り上げる。

続いて、ISA95-1 のレベル 0、1、2 の主要なシステム構成要素及びその機能について簡単に述べる。SCADA システムの様々な要素及びその機能の全体について、表 1 に示す。ローカル制御装置は水力学、空気力学、電力工学を駆使してセンサ、制御バルブ、モータ、その他の機器から測定データを収集する。この種のローカル制御装置は、1 プロセッサが 1 ボードに搭載されている場合、プログラマブル・ロジック・コントローラ（PLC）と呼ばれる。多くの場合、複数の PLC が 1 台のラックかキャビネットに収容されている。リモート・ターミナル・ユニット（RTU）は、ローカル制御装置の一種で、通常 PLC より処理能力が高く、複数のボードを管理している。各システムは、通常 TCP/IP 等のオープンな通信プロトコルを用いて通信を行う。

例）
レベル 1 の「中枢（検知機能）」が、液面計、流速や水圧の変化（レベル 0）を利用して、漏水しているパイプを検知する。次にこの検知データはメッセージとして（中央）管理センターに送信される（レベル 2）。センターではアラームの発報や、保守チームへの自動通知が行われる。アラームは、管理画面上に論理的に体系化・可視化されて表示されることもある。

SCADA はプロセス制御システム（PCS: Process Control System）の一つの実装例である。分散制御に基づくもう一つの PCS アーキテクチャは分散制御システム（DCS: Distributed Control Systems）と呼ばれ、測定機器から管理コンソールまで、システムの監視及び制御を行う。通常、プロセス制御システムは長距離にわたって散在しており、時には予めプログラムされた制御機能が中央コンピュータシステムに組み込まれている。DCS は主にスタンドアロンの大規模施設に導入され、ローカル制御装置が制御機能を提供する。SCADA と DCS の境界は徐々に曖昧になってきており、そのため、本書を含め多くの文献では SCADA という用語を汎用的に使用している。最も広義には、SCADA をプロセスオートメーションと同意語と見なすことができる。

表1 用語と機能

装置	機能
センサ及び測定機器	現場で電圧、電力、圧力、温度、流速、バルブ位置等の状態を検知するセンサや測定機器。
アクチュエータ	リモート、またはローカルで運用されているポンプ、バルブ、モータ及びブレーカー等の機器。
ローカル制御装置	センサ、アクチュエータの双方、及びネットワーク上の各種機能と通信を行い、次のうち一つ、または複数の役割を果たす。 • センサ及び測定機器からのデータ収集。 • ローカル制御装置に組み込まれたプログラム、または管理コンピュータ／オペレータからのコマンドによる下位アクチュエータの起動と停止。 • 通信プロトコルの変換（複数のプロセス制御システム及び測定機器の相互通信を実現）。 • アラーム状況の識別。 現状、ローカル制御装置はプログラマブル・ロジック・コントローラ(PLC)、リモート・ターミナル・ユニット(RTU)、インテリジェント電子機器(IED)やプロセス自動化制御装置(PAC)等、様々な名称で呼ばれている。 ひとつのローカル制御装置で、データ収集や数十の測定機器及びアクチュエータの制御を行うことが可能。
短距離通信機器	ローカル制御装置とセンサやアクチュエータの間の通信を担う。 アナログ信号／デジタル信号は、比較的短いケーブル、または無線接続を介して伝達される。
中央コンピュータシステム	集中制御と運用システムの役割を担い、オペレータによるプロセスの監視、アラームの受信と確認、データ解析及びアクチュエータへの制御信号の送信を可能にする。中には、ローカル制御装置の自動制御のためのプログラムが組み込まれていることもある。そのような場合を除き、中央コンピュータシステムは、純粋にオペレータとローカル制御装置の間のインタフェースとしての役割を担う。 その他に、計測データやシステム状態データの（履歴）データベースへの保存やレポートの作成といったタスクを実行する。 中央コンピュータシステムはマスター・ターミナル・ユニット (MTU)、またはSCADA サーバとも呼ばれる。ヒューマン・マシン・インターフェースソフトウェア（HMI)を備えたパソコン（PC）であることが多い。
長距離通信機器	ローカル制御装置と中央コンピュータシステムとの間の通信を担う。ネットワークは数キロメートルに及び、専用線、xDSL、ダーク・ファイバー、衛星回線、マイクロ波回線、GSM、GPRS、UMTS、フレームリレー等を使用する。

2.2 上水道システムにおける SCADA

広い意味で、SCADA システム及びネットワーク（すなわち PA）は、オランダにおいて水道水の供給と水質を保証する上で必要不可欠なものである。上水道システムにおいて、SCADA システムは水道水の供給にあたって以下のプロセスの測定、制御、アラーム・イベントの統合監視を、ローカル及びリモートで行う。

- 抽水及び／又は水道源水の取水
- 取水池及び沈殿池への送水
- 浄水／ろ過処理施設への送水
- 浄水及びろ過プロセスの制御及び監視
- 水質管理プロセスの制御及び監視
- 水道水の配水 ・給水
- 圧力ポンプの制御

上記には、管内の流速、貯水タンク内の圧力、ポンプの電源のオン・オフの制御及び監視、バルブの制御、pH 値や濁りなどの水質の監視も含まれる。アラームの表示及び手動による制御オプションの多くは、制御・監視センターに集約されている。これを、上水道システムではしばしば「中央集中監視（central watch）」と呼んでいる。

2.3 SCADA のセキュリティの脆弱性とリスク

SCADA システムやネットワークのセキュリティが脆弱化しているのは、多くの技術面及び組織面での進展の結果といえる。まず第一に、SCADA は電子部品やリレー部品がラックに満載されていた時代の、情報セキュリティについて一切考慮しない古典的な PA の産物である。また、SCADA システムやプロトコルは以下の状況にあったため、セキュリティを考慮する必要性もなかった。

- 独自のプロトコル、技術、及び基盤制御システム
- SCADA の動作に関する公開情報が皆無であったこと
- 外部との通信はしない、または、専用線・私設線を使っての二地点間通信のみであること
- 経営管理用ネットワークやインターネットとの接続がないこと
- ハッカーの侵入はあり得ないことを前提に、十分なセキュリティ対策を考慮せずに実装していること
- ネットワークの過負荷やプロトコルの誤動作等に起因するストレス条件下での稼働を考慮しないプロトコルの実装
- パッチ適用の必要がないシステム
- 完全にコントロールされた、外部接続のないセキュアな環境

最近では、実際の運用状況は異なっており、上述の基本原則はもはやあてはまらなくなっている。残念ながら、情報セキュリティに関して、SCADA 技術も運用環境も、急速な技術的進化やこれに伴う運用面の変化に追い付けていない場合がしばしば見受けられる。

- SCADA プロトコルはオープンスタンダードとなり、その詳細をインターネットから入手可能である
- SCADA は Windows や Linux 上のアプリケーションとして動作し、データ転送にはインターネットプロトコル（TCP/IP）を使用する。これらの OS やプロトコルの脆弱性は世界中のハッカーの知るところであり、ツールキットを用いて攻撃される可能性がある
- 現在の HMI は複雑なコマンドの入力を必要とせず、ウェブブラウザをインターフェースとしている
- 現在のビジネス事情では、企業ネットワークとインターネットの接続が不可欠である。自宅からの制御や、メーカ及び SCADA ベンダによる保守のために、SCADA ネットワークへのモデムアクセスポイントが存在する
- ハッカー等の、SCADA システム／ネットワークへの侵入に対するが興味が増大している
- 簡単な検証の結果、不明なパッケージがネットワークを介して送られた際、SCADA システムが過負荷になったり、損壊したりする可能性がある
- 全てのパラメータをリモートアクセスによって設定可能にする統合ウェブサーバは、PLC ボードの新しいオプションであり、無効化できないことがある

- SCADA ベンダによる保守のためのリモートアクセスを可能にするために、SCADA 機器にはモデムが標準装備されていることがある
- 「閉鎖された環境のはず」との認識から、パスワードは変更されず、個人ごとに個別に設定されていない

こうしたことが、SCADA のリスクに全く気づいていない PA 環境で行われている（[9]に記した様々な例も参照のこと）。このような PA 環境は、ハッカー、ウイルス、トロイの木馬、スパム攻撃が日常的になっており、SCADA 環境よりも情報セキュリティへの関心が高い企業情報システムの環境とは、全く異なる文化を有している[10]。また、PA を利用している組織は、PA を防護するための技術の進展に追随できていない。セキュリティが運用プロセスに組み込まれておらず、プロセスの責任者が不明であることも多い。

過去の解析[1]によれば、多くの点において、上水道事業者の SCADA が置かれた環境も何ら変わらない。

- SCADA に特有のセキュリティポリシーというものは、多くの場合存在しない
- 従業員のセキュリティ意識を高めるような対策は殆ど何も行われていない
- 既知のリスク要因に対し、リスク軽減策はまったく実施されていない（「水道分野の人々の懸念事項は何か」）
- 監視を受けずに、第三者が SCADA ネットワークに機器を接続することができる
- ウイルスやワームのスキャンは滅多に実施されない
- 必要なパッチは適用されていないか、または遅れて適用される

表 2 SCADA が脆弱性とは無縁と誤認されている例

想定	実情
専用線を使用しているため、誰も通信網にアクセスできない。	通信を盗聴するのは容易。（例として以下の URL を参照、www.tscm.com/outsideplant.html）
ダイアルアップ接続を使用しているが、誰も電話番号は知らない。	盗聴するか、請求書明細を見れば、発信者電話番号は一目了然。また、電話を掛けまくり、モデムが接続されている電話を自動探知するソフトウェア（War Dialer）もある。
コールバック・モデムを使用しているため、権限の無い者はアクセスできない。	盗聴すれば、コールバックの仕組みを迂回することは容易。盗聴しなくてアクセスできる方法もある。
リモートアクセスシステムはパスワードによって保護されている。	パスワードを盗む手段は広く知られている。一番簡単な手口は、データ通信をスニッファで盗聴する方法である。パスワードが平文としてネットワーク上に送られると、傍受が可能となる。辞書を用いたパスワードの推測方法も常識化している。パスワードそのものやパスワードがまったく変更されていないといった事実を教え合うことも非常に一般的といえる。パスワードが単純で文字数が少ない上にまったく変更されていない、ということはよくある。
軍がセキュア通信に使っているような周波数変調技術を使用している。	周波数変調データを簡単に解読する手法がある。無線 LAN 協会 (WLANA)は、周波数変調ネットワークを含め、全てのネットワークでの暗号化を推奨している。
ベンダとその他少人数しか知らないプロトコルを使用しているので、サイバー攻撃者には SCADA メッセージを判読することはできない。	特定ベンダの独自プロトコルであっても、一般的に、想像以上に多くの人々に知られている。ベンダやコンサルタント、また、同じ SCADA プロトコルを使用している企業の従業員や元従業員らも詳細を知っている。 プロトコルを解析する手順書やソフトウェアもインターネット上で入手することができる。

2.4 水道分野や他の重要インフラ分野で発生した SCADA インシデント

PA が直面する脅威は下記に分類できる。

- セキュリティポリシー未策定、セキュリティ意識の重要性に対する認識不足、アクセス制限の不備、パスワードポリシーの欠如といった組織的脅威
- 爆発、火事、破壊行為による物理的脅威
- ソフトウェアやハードウェアの機能不全、ウイルス、サービス妨害（DoS）攻撃等の技術的脅威

世界中を見ても、SCADA 関連のインシデントが公表されることはあまり無い。稀に公表されても、ヨーロッパ以外での事例が多い。ヨーロッパの企業はこうしたインシデントの発生を伏せておく傾向があり、公表しない、もしくは「技術的な機能不良」と報告するに留まる。オランダの SCADA 報告書[2]には、多くの分野で発生した SCADA システムに関連する公表されたインシデントの一覧表が含まれている。水道事業者が国際的に公表しているインシデントは僅かだが、そのうち１件はオランダで発生したものである。
以下に、上水道分野におけるインシデント事例を紹介する。

- **上下水処理場の制御システムの不正操作（オーストラリア）**
  SCADA システムやネットワークの脆弱性を示す例として最も頻繁に挙げられるのが、元契約作業員である Vitek Boden による、オーストラリア・マルーチー州にある Hunter Watertech 社が運営する上下水処理場のプロセスコントロールシステムに対する不正アクセス事件である。Boden は処理場に SCADA システムを導入した請負業者の技術者であった。導入された SCADA システムは 300 を超えるポンプ場に設置されたローカル制御装置から構成され、各装置は中央コンピュータシステムと無線リンクによって通信を行っていた。導入プロジェクトに 2 年間携わり、プロジェクトの完了も近づいてきた 1999 年、Boden は自社を退職し、Hunter Watertech 社に雇用を求めた。Hunter Watertech 社は雇用を拒否したが、その後まもなくして、下水システムのポンプ場の機能不良や、上水道システムのバルブが勝手に閉じるといった現象が見られるようになった。
  2000 年 4 月 23 日、警察による捜査で Vitek Boden の車から PC と無線装置が発見され、Boden 自身も Hunter Watertech 社 の SCADA システムに対して 46 件に及ぶ不正なリモート操作を行ったことを認めた。
  Boden はアラームの無効化、通信妨害、ポンプの起動停止によって未処理汚水のオーバーフローと放流を引き起こした。2000 年 1 月から 4 月 23 日迄の間に、100 万リットル近くの未処理汚水が周辺に放流されたと見られている[2]。
- **SCADA システムの破壊（南アフリカ Tshwane ）**
  2006 年 8 月 18 日、無法者により南アフリカの Tshwane にある貯水池の SCADA システムが破壊され、Mamelodi と Eersterust (Pretoria)で 11 日間水道水を得ることができない状況となった。
- **浄水場システムへのハッカーの侵入（アメリカ合衆国ペンシルベニア州ハリスバーグ）**

2 http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

アメリカ合衆国ペンシルベニア州ハリスバーグの浄水場の SCADA システムにハッカーが侵入した。これは、ハッカーが水道事業者従業員のノート PC にトロイの木馬をインストールし、リモートから制御することにより実行された。従業員が自宅でログインするやいなや、ハッカーはインターネットから従業員のノート PC 経由で SCADA ネットワークに侵入し、マルウェア（トロイの木馬)とスパイウェアを SCADA システムにインストールした。理論的にはハッカーが SCADA ネットワークを乗っ取り、不正なコマンドの実行しネットワークを完全に過負荷状態にすることも可能であった[3]。

- **配水システムの通信障害（アメリカ合衆国、フォートワース）**
  2007 年 1 月 14 日、分散型 SCADA システムで通信障害が発生し、フォートワースの一部で水道水の供給が 8 時間にわたり停止した。障害により、ポンプと貯水タンクの全てのコントロールが失われた。
- **上水道システムへのハッカーの侵入（アメリカ合衆国）**
  American Water ISAC が、2000 年に、水道事業者の SCADA システムにハッカーが侵入したとの報告を行った。
- **SCADA ソフトウェアエラー**によって塩素レベルが極度に低くなり、アメリカ合衆国マサチューセッツ州ルイストン（Lewiston）で水道水が飲めなくなった（2003 年）。

他の分野における SCADA システム関連の公表されているインシデントは、先の 2.3 節に示した SCADA のセキュアでない面を示す例である。

- システム障害を引き起こす、脆弱でしばしばセキュアでない SCADA プロトコル
- ハッカーやウイルスの侵入を許す、脆弱またはセキュアでない企業ネットワークと外部ネットワークとの間の通信回線
- どのような機器が SCADA システムに接続されるかの監視の欠如により、セキュリティ対策を迂回できる保守業者（原子力発電所も同様の状況）
- 変更管理の欠如
- SCADA システム及びネットワークの物理セキュリティの欠如

> 24/08/2007 http://www.zone-h.org/news/id/4651
> ペネトレーションテストを実施することで、時に驚くべき結果が得られることがある。しかし、重要インフラへのペネトレーションテストが驚くべき結果を生み出してはならない。
> Scott Lunsford 氏は、原子力発電所への侵入テストの依頼を受けた。施設の所有者は、インターネットを介して原子力発電所の重要システムにアクセスすることは不可能と主張したが、Lunsford 氏によれば「過去に行ったペネトレーションテストの中で最も容易かった。」という。さらに、「初日のうちにネットワークへの侵入に成功し、一週間後には原子力発電所の SCADA システムを掌握していた。」と述べた。

2.5 上水道システムにおける SCADA セキュリティの必要性

水道水の供給と水質を保証し、SCADA システムが権限のない者に不正操作されないようにするためには、上水道分野における SCADA 環境、システム、ネットワーク（図 1 のレベル 0、1、2）での有効なセキュリティ対策が必要であ

3 http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html

る。上述のハッカー問題、ウイルス、SCADA ネットワークの構成装置間の通信障害は、オランダの上水道分野や他インフラの分野でも起こり得る。

給水停止による社会的影響は甚大になると推察される。結果的に社会不安、公衆衛生への影響、多大な経済的損害などを招く可能性がある。従って、水道水の供給を担う重要インフラ事業者である水道事業者は、企業の全体的なリスクの一環として、SCADA のリスクにも対応しなければならない。

結論として、上水道分野の SCADA システム及びネットワークへの有効なセキュリティ対策は必要不可欠である。その際、アプローチとして情報セキュリティの組織的、物理的、技術的側面すべてに等しく配慮する必要がある。次に記す上水道分野の SCADA セキュリティに関するグッド・プラクティスは、経営層、及び技術面でのプロセスオートメーション管理のためのガイドラインを示す。

3 経営層レベルでのグッド・プラクティス

前章で述べた SCADA リスクの様々な要素を緩和することができる有効な解決策を発見するため、本書では SCADA セキュリティに関するグッド・プラクティスを取り上げた。このグッド・プラクティスは決して法的な基準や法的な要求事項ではないことを強調しておく。
上水道事業者は企業内文化とか企業の組織的、構造的、技術的な特質といった妥当な理由から同程度のレベルを保証する全く別のセキュリティシステムを選択するかもしれない。いずれにせよ、全てのセキュリティ上の欠陥が解消されることを確実にするため、どのような代替セキュリティ対策についても、以下で述べるグッド・プラクティスと照らし合わせて評価することが望ましい。

グッド・プラクティスは２つに大別している。１つは企業経営のレベルのグッド・プラクティスで構成されている。本章ではこれらグッド・プラクティスを記述する。
次章では技術面でのプロセスオートメーションについてのグッド・プラクティスを示す。

上水道分野における企業経営レベルのグッド・プラクティスは、既に上水道分野に存在する全般的な情報セキュリティポリシーの延長であるとともに、リスク管理を一般的な企業文化にしていこうという動きでもある。このグッド・プラクティスは次の主要トピックに仕分けることができる。

- 企業セキュリティポリシーと SCADA 向けセキュリティポリシー
- リスク管理
- 監査
- SCADA システム、各種ネットワークシステム、各種サービスの調達ポリシー

3.1 企業のセキュリティポリシーと SCADA セキュリティポリシー

SCADA システム及びネットワークに対して適切な情報セキュリティ対策を施すには、経営層がセキュリティに注意を払うことが必要である。これには、関連するリスク分析に基づき運用プロセスに組み込まれるセキュリティポリシーや上水道事業者全体に適用し得るリスク管理プロセスが含まれる。

グッド・プラクティス 1
上水道事業者は全般的な情報セキュリティポリシーとその情報セキュリティポリシーと密接に結びついた SCADA 向けセキュリティポリシーを策定している。

グッド・プラクティス 2
一般的な情報セキュリティポリシーは「情報セキュリティマネジメントの実践のための規範」[3]、及び関連する情報セキュリティマネジメントシステムの基準 [6][4] に基づいている。

[4] 注：VEWIN のセキュリティモニタリング及び Amsterdam Municipal Information Security Standard (GIBN) は、 Code of Practice for Information Security からの引用である。.

グッド・プラクティス 3
SCADA 向けセキュリティポリシーの基本的な前提条件は、従業員に対し、セキュリティ対策が全般的な（情報）セキュリティポリシーとオフィス環境のセキュリティに論理的に沿った形で運用されることである。

グッド・プラクティス 4
SCADA 向けセキュリティポリシーは SCADA システム及びネットワークに対する物理的防御を包含しなければならない。

グッド・プラクティス 5
SCADA 環境下ではセキュリティに関する責任、義務、権限は経営陣及び SCADA システムユーザに対して規定される（[8]の 12 参照）。

背景

- SCADA 向けセキュリティポリシー、セキュリティ対策手順、セキュリティ文化の欠如がアメリカにおける SCADA 脆弱性の上位 10 項目に入っている[10]。
- 情報セキュリティポリシーやリスク評価が不十分であれば、後追いの追加セキュリティ対策を実施することになる。従って適切なセキュリティ対策が行われていたのかどうか、セキュリティ上の不備がどこに存在しているのか、といった点が明らかにされないままとなる。
- 「情報セキュリティマネジメントの実践のための規範」に従った情報セキュリティポリシーの多くは 1 日 24 時間 365 日稼働の SCADA 環境には必ずしも適していない。[4][5]によれば「実践のための規範」に含まれる多くの管理策はある程度の補足が必要である。主な補足項目としてアウトソーシング、情報セキュリティとプロセスセキュリティの連携、ICT 環境（SCADA 環境）における物理的セキュリティ、24 時間 365 日稼働における運用手順、ウイルス対策ポリシー、ログ収集と警告、アスセス制御、パスワードポリシー（4、6 節参照）、事業継続マネジメントが挙げられる。SCADA には別の補完的なセキュリティポリシーの策定が推奨される所以である。発生するであろうセキュリティインシデントに関する報告基準を明確にすることもまた賢明な措置である（「情報セキュリティマネジメント実践のための規範」[3]の 11.2 節を参照）。
- 定期的に更新される SCADA セキュリティポリシー文書の最新版に含まれる要素には、上水道事業者の事業目的（水道水の供給と及び品質の確保）から明白かつ明瞭に導き出されるセキュリティ目的、セキュリティ体制、規則及び手順がある（PA に従事あるいは関わっている特定の地位の社員及びその他の従業員の役割と責任とは何か？（潜在的な）セキュリティインシデントを従業員や経営スタッフが見つけた場合、その従業員や経営スタッフは何を期待され、何を禁止されるのか？）。

3.2 リスク管理

グッド・プラクティス 6
プロセスオートメーション/SCADA 環境は、企業のトップレベルにおいて行われるリスク管理プロセスの中に含まれる。

背景
プロセスオートメーション/SCADA 環境は、上水道運用プロセスの根幹であり、水道水の供給及び品質を保証している。SCADA システム及びネットワークにおけるすべてのセキュリティの要素（可用性、信頼性、完全性、機密性）、リスク評価、リスク管理、関連する事業継続計画は、全てがこのために実施される。

3.3 セキュリティ意識

内部統制が必要となる主なリスク要因の１つは人的要因である。人的要因は SCADA 環境においても同様に主要なリスク要因である。セキュリティ意識によって経営者（模範機能）と従業員のセキュリティに集中する姿勢を維持することを助けるだけでなく、さらに組織自体のセキュリティレベルを向上させる。

グッド・プラクティス 7
上水道事業者はセキュリティ意識に関する研修を継続的に実施する。

背景
効果的な情報セキュリティにはセキュリティ意識とセキュリティに対する従業員の姿勢に対して注意を払い続けることが必要である。特に、従業員が重要な運用プロセスに従事する場合はなおさらである。もし上水道事業者の従業員がセキュリティ意識をもっていないとしたら、SCADA システム及びネットワークに関わる第三者（供給者、保守・修理技術者）にもこれが伝わり、意図的、あるいは意図せずに SCADA システムに影響を与え上水道プロセスの不正な運用につながる潜在的なリスクを高めることになる。（[8]の項目 21 参照）

3.4 監査

グッド・プラクティス 8
SCADA システム及びネットワークの EDP 監査を少なくとも年に 1 回実施する。

背景
オランダの民法第 2 部 393 節に年次決算に関する次のような記述がある。「会計士は監査報告書を監査委員会及び役員会に提出する。報告書には最低限自動データ処理の信頼性と継続性に関する調査結果を含めるものとする。」 この条文はコンピューター犯罪法第 1 条の一部分でもある。会計士に対してこの追加業務を課す理由は次の通りである。コンピューターハッキング、サイバーテロあるいはその他のコンピューター犯罪において逮捕あるいは起訴された犯人はセキュリティやセキュリティに類するものが存在せず何の障害もなくシステムやネットワークにアクセスしたため侵入していたとは分からなかったと自己弁護を主張することができる。犯人の弁護士は上水道事業者は適切なレベルのセキュリティ対策が施されていたことを証明するよう要求するかもしれない。簡単に言えば「すべてのセキュリティ計画と詳細を法廷に提出せよ。」ということであり、それらをが公開されることを意味する。そのためほとんどの企業

はセキュリティ手段を公にすることを避けるために起訴を取り下げる。そして常に犯人が釈放されることを許すこととなる。
オランダ民法によれば、年次決算報告書の一部として発行された監査報告書が存在し、SCADA システム及びネットワークについて明示的かつ網羅的な報告をしている場合』には、監査報告書が『ある程度のセキュティ』の存在の証明を要求する法的要件を満たしていると認められ、容疑者が故意に侵害したことを証明できる。この場合、セキュリティ対策の詳細を提出する必要はない。従って、SCADA ネットワークについて明記した監査報告書を年次決算報告書に添付しない場合、犯人の告発が極めて困難となり、また、セキュリティ対策を公にしなければならないリスクを負うことになる。

監査では、最低限次の項目を検証する。

- パスワード及びアクセスポリシー
- SCADA システムとそのネットワーク間接続におけるセキュリティ、SCADA システムとオフィスオートメーション、公衆回線、インターネットとの接続におけるセキュリティ（[8]の項目 9、18 参照）
- リモートで監視や管理されている拠点のセキュリティ状況（[8]の項目 10 参照）
- 存在する可能性のあるモデムアクセスポイント
- セキュリティインシデントの報告、セキュリティログの収集及びフォローアップの方法
- SCADA システムの構成要素とそのネットワークに対する建物の錠、扉の警報等の物理的及び電子的防護（[8]の項目 10、18 参照）

公的監査に加えて、セキュリティ意識教育と同期させ、1 年に数回内部監査を実施することが推奨される。

3.5 SCADA システムとサービスの調達ポリシー

情報セキュリティは SCADA 機器、ソフトウェアとサービスのライフサイクル全体に適用する。調達は、内部のセキュリティ要件を供給業者と第三者に負わせるための重要なステップである。水道事業者が専門的かつ本格的にセキュリティに取り組んでいるということを社外に対してはっきりと明示する助けになる。

グッド・プラクティス 9
供給業者と締結する（大規模な）SCADA システム及びネットワークについての契約には水道水の供給と品質を保証するための継続に関する条項を入れる。

1 供給業者は合意した期間までの間、必要十分な量のスペアパーツの在庫を確保する。
2 供給業者は災害時に解決策の検討を支援する。
3 供給業者は SCADA システムとそのネットワークあるいはどちらか一方がその理由の如何を問わず機能しなくなった場合には SCADA システムとそのネットワークあるいはどちらか一方の入れ替え作業への協力を最優先させる。

4　供給業者はシステムの主要部分（例えば Microsoft OS など）を提供する第三者からのパッチを短期間で検証し、信頼できる確実な手段によりパッチを適用する。

背景

水道水の供給と品質を保証するため、重要な上水供給プロセスを監視・制御する SCADA システムは機能停止や災害時において可能な限り迅速に機能を復旧させなければならない。

グッド・プラクティス 10

水道事業者は、調達前に SCADA システム、ネットワークシステム、ソフトウェアといった情報セキュリティが満たすべき要件を定義する（「情報セキュリティ実践のための規範」（[3]の 12 章参照））。

背景

SCADA システム及びネットワークはしばしば統合されたプロジェクトとして提示されることから、提供されるシステムが満たすべきセキュリティ要件をあらかじめ定義することは重要である。[7]には、技術要件に関し最初に検討すべき一連の事項が記述がされている。また、供給者は上水道事業者からの明確な許可がなければ SCADA システムを供給した事実を第三者に通知してはならないと規定している。

グッド・プラクティス 11

第三者と結ぶ保守・サポート契約にはセキュリティ条項を含める。

セキュリティ条項には最低限、次の項目を規定する。

1　保守・サポート技術者の SCADA システム及びネットワークのセキュリティポリシーに対するコンプライアンス
2　保守技術者に対する身元保証とアクセスについての取り決め
3　企業機密の保護に関する保証（[8]の項目 21 参照）
4　第三者の作業に対する水道事業者による監督
5　企業機密を含む可能性のある情報が記録されている（不良）媒体の廃棄

背景

SCADA システム及びネットワークのための一般企業のセキュリティポリシーは第三者の従業員にも適用される。最も重要な規定は、SCADA システムへのアクセス制限である。第三者は最低限、自社の従業員が信頼できることを保証しなければならない（第三者が自社の従業員の行動に責任を持つこと、犯罪歴が無いことの証明など）。SCADA システムあるいはそのネットワークに第三者の機器やソフトウェア（保守技術者が使用するノート PC やモデムを含む）を接続するための条件に関して合意の上、その内容を書面に記す。第三者が SCADA 環境下のシステムとネットワークに対して行う全ての作業は上水道事業者の監督のもとで行われる。水道水の供給を脅かす重大な機能停止を防ぐためである（[8]の項目 7 参照）。例外事項は上水道事業者のセキュリティ責任者の許可を得た場合のみ認められる。

故障のため交換しなければならなくなった SCADA システムで使用していた情報媒体には（ハードディスクや ROM モジュールなど）企業機密が含まれている可能性がある。このような情報媒体は適切な方法で機密情報が消去もしくは破壊されたことが保証されない限り、水道事業者の構内から持ち出さない旨を合意しなければならない。

4 技術的レベルでのグッド・プラクティス

グッド・プラクティスは大きく次の項目に分類される。
- 多層防御（defense in depth）
- SCADA 環境と OA 環境の分離
- SCADA 環境へのセキュアな接続
- SCADA システム及びネットワーク機器のセキュリティ対策
- SCADA 環境の保護
- SCADA 環境のパスワードポリシー
- 事業継続と SCADA システム及びネットワーク
- SCADA 環境における情報媒体管理

以下のグッド・プラクティスは、現在策定中の標準を含め、様々な参考文献（[3]、[11]、[12]、 [13]）に基づき、記述したものである。

4.1 多層防御

グッド・プラクティス 12
「多層防御[5]」の原則に基づき、SCADA 環境のセキュリティ強化を図る。

背景
公共ネットワークや企業のネットワークからの、SCADA システム及びネットワークへのアクセスに対し、幾重にも防御を施すことにより、仮に一つのセキュリティ対策が破られたとしても SCADA システム及びネットワークに自由にアクセスできないようにする。さらにファイアウォール、簡単に確認できるネットワーク接続及びコールバックシステムに加え、個人ごとの認証、パスワードの定期的変更、侵入探知（[10]の項目 7 参照）、ウイルス対策やパッチを当てる際のセキュリティポリシー等の対策により、悪意のある攻撃を阻止することができる。これにより攻撃者を容易に発見することができ、侵入されるリスクを低減させることが可能となる（[10]の項目 2 参照）。

4.2 SCADA 環境と OA 環境の分離

グッド・プラクティス 13
SCADA 環境のセキュリティを確保し、OA 環境から完璧に分離する。

グッド・プラクティス 14
ネットワークインフラを共有している場合、OA 環境と SCADA/PA 環境を論理的に分離しておくことにより、仮に OA ネットワークが過負荷になったとしても、SCADA 環境の制御が失われることはない。

[5] [10]の脆弱性 2 参照。

背景
厳重かつ簡単なパーティションを OA ネットワークと SCADA/PA 環境の間に築くことにより、SCADA 環境のセキュリティと信頼性を大幅に向上させることができる。SCADA システム及び SCADA ソフトウェアは、ワームによってもたらされる想定外のパッケージやネットワークの過負荷に対し、極めて敏感なため、このようなリスクを阻止する必要がある。
同じネットワークと通信機器を OA 環境と SCADA/PA 環境で同時に使用するため、VPN と集線装置（コンセントレータ）を用いている場合、トロイの木馬やワームが（論理的）OA ネットワークの過負荷を引き起こすリスクがある。そのような場合、集線装置と VPN ネットワークが、SCADA に十分なネットワーク容量を提供できないこともあるため、結果的に SCADA システムの監視・制御機能の損失に繋がる恐れがある。従って、OA ネットワーク側での過負荷の発生に対し、SCADA ネットワークがどの程度敏感であるかを検証することが望ましい。こうしたテストを、少なくとも SCADA 環境の可用性に影響を与える可能性があるネットワーク設定の変更を行うたびに管理された状況下で実施するべきである。

4.3 SCADA 環境へのセキュアな接続

グッド・プラクティス 15
SCADA ネットワークとその他のネットワークとの接続は、必要不可欠なもの以外排除する。

グッド・プラクティス 16
一般的なセキュリティポリシーに基づき、残った必要不可欠な接続及びその接続を通じてやり取りされるデータを詳細にかつ継続的に監視する（[8]の項目 1、2、3 参照）。

グッド・プラクティス 17
SCADA 環境と OA ネットワークの間の接続が不可欠である場合、必要かつ承認されたサービスのみ認めるファイアウォールを設置する。ファイアウォールのログを定期的に確認し、不正な通信や不正アクセス等を解析する。

グッド・プラクティス 18
SCADA 環境を直接インターネットに繋がない。

グッド・プラクティス 19
DoS 攻撃及びインターネットが利用不能になった場合について別途リスク分析を行わない限り、SCADA 環境は情報の伝達にインターネットを使用しない。

グッド・プラクティス 20
定期的に専門家によるリスク分析が行われ、リスクが制御下にあると確認されない限り、SCADA ネットワークは無線アクセスポイント（WiFi）を使用しない。可能なセキュリティオプションは全て使用する（視認できないアンテナ、ビーコンパケットの不使用、WPA2 等の最高レベルの暗号化、MAC 制御など）（[10]の項目 5 参照）。

グッド・プラクティス 21
モデムやその他の外部アクセスポイントを常に監視し、高い信頼性かつ強度を有する認証方式を使用する。リモートアクセスの認証許可は定期的に見直し、継続の必要性を検証する。原則として、認証は必要不可欠な場合のみ認める（[8]の項目７、[10]の項目 3 参照）。

グッド・プラクティス 22
ネットワークを分離する装置（ファイアウォール、ルータ、VPN）と接続（モデム）のセキュリティ対策と設定は、定期的に検証する。

背景
可能な限り、SCADA 環境における不正操作が不可能なようにする。SCADA 環境から他の環境への接続箇所は弱点となる。従って、水道事業者はこのような接続箇所を定期的に監視する必要がある。内部の接続に関しては、適切に設定され、運用されているファイアウォールを多層防御の更なる機能と位置づけることができる。インターネットへの直接接続は、侵入、SCADA システム及びネットワークの可用性を危うくする攻撃やアクセスの喪失（停電、ケーブル障害など）に対して脆弱である。インターネットやその他の公衆回線がテレワークサービス等に使用されているのであれば、高度な認証方式を導入することが推奨される。また、通信インフラや電源供給の機能停止・故障等に備えた計画を準備するのが賢明である。

4.4 SCADA システムとネットワーク機器のセキュリティ対策

グッド・プラクティス 23
SCADA システムを「強化」し、ベンダが提供するセキュリティ対策を最大限に活用する。

グッド・プラクティス 24
SCADA システム及びネットワークの設定手順を文書化する。

グッド・プラクティス 25
SCADA システム及びネットワークの設定変更プロセスを、管理されたプロセスとして確立する。

グッド・プラクティス 26
可能な限り、SCADA システムを最新のウイルス対策ソフトで守る。

背景
SCADA システムを「強化」するとは、システムが以下のように設定されていることをいう。
1 **既知の脆弱性への対策が済んでいる。**
2 **システムの正常な運用に必要としないプロセスは全て設定から削除している。**
3 **不必要なポートやサービスは全て無効化し、ブロックしている。**
4 **デフォルトのアクセスポイントは全て削除している。**

5　水道事業者の SCADA セキュリティポリシーの範囲内で、ベンダが提供するセキュリティオプションを最大限に活かしている。

すなわち、システムの強化やセキュリティオプションの活用により、ハッカーやマルウェアに対しアクセスする隙を与える可能性のある脆弱性の数が減少するという考えに基づいている（[8]の項目 4、6 参照）。内部システムが適切に文書化されており、設定が設定変更管理プロセスと整合していれば、深刻な機能障害や SCADA システム、及びネットワークの損失が発生した際、より早く復旧できる可能性が高まる。

上水道システムを含め、SCADA システムはますます市販のプログラム（Windows、Linux、Open SCADA 等）を利用するようになってきている。さらに SCADA システムはインターネット接続が可能なネットワークに接続され、SCADA ネットワーク上に接続されている第三者の機器の影響にも晒されている。
SCADA 環境に侵入したウイルス、ワーム、トロイの木馬等の悪意あるコード（マルウェア）の早期発見により、マルウェアに感染していない健全な SCADA システム及びネットワークを維持することが可能となる。そして、ウイルス対策ソフトはマルウェアが SCADA 環境に影響を与えるのを防ぐため、常に最新の状態にしておくことにより、水道水の供給と水質を保証することができる。

グッド・プラクティス 27
ハッカーやウイルス、トロイの木馬やその他のマルウェアによるセキュリティ侵害と許容リスクを考慮し、SCADA システムとネットワークのパッチポリシーを策定する。

背景
ソフトウェアやシステムに存在する脆弱性は、すぐにハッカーの知るところとなる。知られてから僅か数日程度で、サイバー犯罪者は脆弱性を悪用する攻撃コードを完成させる。ベンダによってパッチが提供されると、ハッカーはリバースエンジニアリングを行い、パッチがあてられていないシステムを狙って侵入する。SCADA ベンダは、多くの場合マイクロソフト社やその他のソフトウェアベンダが提供するパッチの検証に時間が掛かるため、SCADA システムはパッチが検証され、水道事業者によって実際に導入されるまでの間、高いリスクに晒された状態となる。とりわけ第三者が自社のシステム（ノート PC など）を SCADA ネットワークに接続できる場合、迅速なパッチの導入は感染リスクを最低限に抑えるためにも必須となる。

4.5　SCADA 環境の保護

グッド・プラクティス 28
SCADA システム及びネットワークへの物理的・電子的アクセスは、認可された従業員等に限る。

グッド・プラクティス 29
SCADA ネットワークへの接続は、事前に承認された機器のみに限る。

グッド・プラクティス 30
経験則として、第三者の機器（ノート PC）などは SCADA ネットワーク及び企業ネットワークへ接続させない。運用上例外的に必要となった場合は、接続する前に当該機器及びソフトウェアを最新のウイルス定義ファイルを用いてワームやウイルスに感染していないかスキャンを実施する。
なお、実際の接続は、水道事業者の従業員の立ち会いと責任の下で行う。

背景
第三者が、意図せずにウイルス、ワーム、またはトロイの木馬をインストールしたり、権限外の操作を行うことがある。第三者のノート PC や機器は、必ずしも厳しいセキュリティチェックの対象とならない場合もある。こうした機器がもし（偶然にも）無線ネットワーク接続に対応している場合、第三者にとっても、うっかり SCADA 環境にアクセスしてしまうことがある。このような監視外のアクセスがしばしば見逃されている一方で、管理者は第三者による不正操作や、プロセス制御システムにウイルスが持ち込まれることを心配し、夜も眠れないと訴えている。

4.6 SCADA 環境のパスワードポリシー

グッド・プラクティス 31
水道事業者は、ベンダによって設定されているデフォルトのユーザ名・パスワードを、すみやかに変更する。

グッド・プラクティス 32
重要なシステム機能へのアクセスを許可するパスワードは複雑なものとし、関係者以外には知らせず、定期的に変更する。

グッド・プラクティス 33
個人のパスワードは他人に知らせず、定期的に変更する。

背景
SCADA ネットワークのサービスにアクセスするためには、ユーザはまず自身を認証する必要がある。望まれる複雑度によって、知識ベース（ユーザ名・パスワード）に基づき一因子で行うか、複数因子としてユーザが所有するもの（トークン）、またはユーザの特徴（生体認証）を追加して認証することができる。パスワードのみを使うセキュリティは最も弱いと見なされている。パスワードの弱さは、ユーザによるパスワードの扱い方にある程度依存する。パスワードが権限の無い第三者に解読されるリスクは、パスワードの最低要件（長さ、（アルファベットや数字等の）文字の種類、辞書に載っていないこと等）、使用頻度、及びパスワードの変更頻度に依る。
「情報セキュリティマネジメントの実践のための規範」 [3]の 11.2 項では、パスワードに係る運用及びパスワードポリシーについて触れられている。
SCADA システムは 24 時間 365 日使用され、広範囲に分散した機器で構成されている場合が多いため、パスワードの使用と関連する要件の検討には注意が必要とされる。

- 情報セキュリティの第 1 の原則として、新しいシステムを初めて使用する際、先ずデフォルトのパスワードを削除または変更することである。ベンダのデフォルトパスワードは、通常類推されやすいという記述は書かれていないものの、文書として公開されている。したがって、システムとネットワークは実質無防備状態といえる（[10]の項目 3 参照）。
- 第 2 の原則として、各ユーザは個人の秘密のパスワードを、他者と共有しないことである。各ユーザに各々の行動に対する責任を持たせるとの観点から、「情報セキュリティマネジメントの実践のための規範」はこの点については非常に厳格である。グループ認証は業務内容に適している場合にのみ許可される。
- 組織の規模、関係者の離職率、第三者の存在に応じて、パスワードの変更を定期的に行うことが望ましい。グループで用いるパスワードの場合、当該グループの一人が離職したら、即座にパスワードを変更することが推奨される。

4.7 事業継続と SCADA システム及びネットワーク

グッド・プラクティス 34
SCADA システム及びネットワークの事業継続マネジメントは、「情報セキュリティマネジメントの実践のための規範」 [3]の 14 章に基づき策定する。事業継続管理の重要なところは、水道事業者が、SCADA 環境の重要な構成要素を対象に、しっかりと維持管理し、定期的に訓練を行うという趣旨の事業継続計画を有することである。

グッド・プラクティス 35
SCADA システム及びネットワークの重要なデータは、定期的にバックアップする（[8]の項目 19 参照）。

グッド・プラクティス 36
SCADA のバックアップ媒体は、離れた場所に安全に保管する。

グッド・プラクティス 37
品質の確認プロセスの一環として、バックアップデータを使用してシステム復旧作業が行えることを、定期的に検証する（[8]の項目 19 参照）。

グッド・プラクティス 38
水道事業者は、SCADA 環境の重要な構成要素（システム及びネットワーク）を対象に、しっかりと維持管理され、定期的に訓練を実施するという趣旨の事業継続計画を有する。

背景
SCADA 環境で災害が発生する可能性は否定できない。ここでいう災害はハードウェアやソフトウェアの誤動作、または、落雷の影響、火事、水害、電力関連の問題も含まれるだろう。冗長システムの迅速な展開や SCADA システムの再設定及び効率的な復旧・再起動を統制された形で行い、水道水の供給と水質を保証するには、事前の計画と訓練が必要である。

4.8 SCADA 環境における情報媒体の管理

グッド・プラクティス 39
SCADA 環境で使用される情報媒体は、破棄プロセスを含め、ライフサイクル全体を通じて有効かつ定められた方法で管理する。

背景
SCADA 環境で使用される情報媒体は、設定情報等の機密情報を含んでいる可能性がある。ハードディスクなどの情報媒体を組み込んだ機器、あるいは情報媒体を交換する場合には、データを完全に消去するか、情報媒体を破壊することが望ましい。

5 参考資料

5.1 情報セキュリティ管理

- H.A.M. Luiijf MSc and R. Lassche MSc, *SCADA (on)veiligheid: een rol voor de overheid?(SCADA (in)security: a role for the government?)* TNO-KEMA report, April 2006.
- ISO, Information technology – Security techniques - *Code of practice for information security management framework*, ISO/IEC 17799:2005.

  ISO/IEC17799 は ISO/IEC 27002 として発行される。国際版は www.iso.ch で入手可能。各国語バージョンも存在する（訳注：日本語版は JIS Q 27002 として入手可能）。
- ISO, Information technology -- Security techniques -- *Information security management systems -- Requirements*, ISO/IEC 27001:2005.

  ISO/IEC 17799:2005 と対をなす、情報セキュリティマネジメントフレームワークの認証基準。
- G. Finco, et al., *Cyber Procurement Language for Control Systems, version 1.6*, INL Critical Infrastructure Protection/Resilience Center, Idaho Falls, USA, June 2006. On-line: http://www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

5.2 セキュリティ意識

- Steven S. Smith, *The SCADA Security Challenge: The Race is On*, November 25, 2006.
- NERC, *NERC Top 10 Vulnerabilities of Control Systems, version 2007*, March 2007.
  On-line: http://www.us-cert.gov/control_systems/pdf/ 2007_Top_10_Formatted_12-07-06.pdf

5.3 情報セキュリティ及び SCADA／プロセス制御

- E.M.M. Castelijn, J.G.J. Nijhuis, *Informatiebeveiliging Waterbedrijven (Information Security in Water Companies)*, VEWIN August 2004.
- N. Lammers, N.T.C. Zantkuyl, Update of *Informatiebeveiliging Waterbedrijven (Information Security in Water Companies)*, VEWIN, March 2007.

  上記 2 件の出版物は、ISO/IEC 17799:2005（情報セキュリティマネジメントの実践のための規範）に基づき、水道（上水供給）分野全体で取り組むべき情報セキュリティ問題に対応するためのガイドラインを提供している。後者の資料は、プロセス制御環境でのグッド・プラクティスを提供している。
- K. Stoffler, J. Falco & K. Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*,
  NIST Special Publication SP800-82 (draft), USA, September 2006.
  On-line: http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf

  TNO/KEMA 調査と同じ話題も幾つか取り上げており、SCADA 脆弱性も数件取り上げている。第 5 章は PA 環境の境界における正しいファイアウォールの設定、第 6 章は「情報セキュリティマネジメントの実践のための規範」（[3] [6]）に関連するセキュリティ

対策について、SCADA に特化した対策の詳細を記している。広範囲にわたる文献と参考ウェブサイトの一覧を含む。

- ISA, *ISA-TR99.00.01-2007 -- Security Technologies for Industrial Automation and Control Systems, Instrumentation, Systems, and Automation Society*, (draft) Technical Report 2007. Note: this report will become IEC/TR 62443-5.

  認証・認可技術、ファイアウォール、暗号化、侵入検知技術、既知の脆弱性、推奨される対策を含む、SCADA セキュリティのトピックスを取り上げている。NIST SP800-82 より詳細であり、より広範囲にわたる文献と参考ウェブサイトの一覧を含む。

5.4 SCADA ネットワークセキュリティ

- NISCC, *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, 2005. See the website: http://www.cpni.gov.uk/ go to *Products and Services* and then go to Good Practices. Now select SCADA firewall guidance.
- DoE, *21 Steps to Improve Cyber Security of SCADA Networks, Office of Energy Assurance*, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005.
  On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf
- Luijf, H.A.M., *Slachtoffer van computercriminaliteit, wat dan?(A victim of computer criminality, what now?)*, 'Beveiliging' magazine, November 2007.
- ECP.NL/KWINT programme, *Voorlichtingsmateriaal (potentiële) computercriminelen (Information on (potential) computer criminals)*, 2005.
  On-line: http://www.ecp.nl/download/
  Voorlichtingsmateriaal_tbv_(potentiële)_computercriminelen.pdf
- GovCert.NL, *Van herkenning tot Aangifte (From Detection to Reporting a Crime)*, The Hague, 2005. On-line: http://www.govcert.nl/render.html?it=39

5.5 SCADA 関連ウェブサイト

- http://www.cpni.gov.uk
  主に経営層を対象とした SCADA グッド・プラクティス群（Products and Services をクリックした後、Good Practices を選択）。
- http://www.us-cert.gov/control_systems/index.html
  多数の SCADA セキュリティ関連の文献と参考資料。
- http://csrc.nist.gov/publications/
  SCADA、ファイアウォール、情報媒体管理等を含む、システムとネットワーク情報セキュリティの一部を対象としたグッド・プラクティス。
- http://www.thei3p.org/site_index/
  Institute for Information Infrastructure Protection (I3P)の、アメリカにおける多数の新しい SCADA 関連の研究とグッド・プラクティス。
- http://www.scadasec.net/secwiki/ScadaSec
  様々な SCADA 関連論文、標準化グループ、その他興味深い SCADA 資料へのリンク集。

5.6 米国の水道分野関連参考ウェブサイト

- http://www.waterisac.org
  水道事業者、参考文献、参考資料へのリンク。

6 参考文献

[1] H.A.M. Luiijf, *Analyse SCADA-veiligheid in de Nederlandse drinkwatersector (Analysis of SCADA security in the Dutch drinking water sector)*, report by TNO-DV 2007 C317, July 2007. classification: NICC Confidential

[2] H.A.M. Luiijf and R. Lassche, *SCADA (on)veiligheid: een rol voor de overheid? (SCADA (in)security: a role for the government)* TNO-KEMA report, April 2006.

[3] ISO, Code voor Informatiebeveiliging/*Information technology - Security techniques - Code of practice for information security management framework*, ISO/IEC 17799:2005
Note: is soon to be renumbered to ISO/IEC 27002; the Dutch version was published as NEN-ISO/IEC 17799:2005.

[4] EWICS TC7: *A Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the Needs of Safety Critical Systems*. European Workshop on Industrial Computer Systems - Executive Summary. On-line: http://www.ewics.org/attachments/roadmap-project/RdMapD31ExecSummary.pdf

[5] EWICS TC7: *A Study of the Applicability of ISO/IEC 17799 and the German Baseline Protection Manual to the Needs of Safety Critical Systems*. European Workshop on Industrial Computer Systems. On-line: http://www.ewics.org/attachments/roadmap-project/RdMapD31.pdf

[6] ISO, *Information technology -- Security techniques -- Information security management systems -- Requirements*, ISO/IEC 27001:2005.

[7] Gary Finco et al., *Cyber Procurement Language for Control Systems, version 1.6*, INL Critical Infrastructure Protection/Resilience Center, Idaho Falls, USA, June 2006.

[8] Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy, USA, 2005.
On-line: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[9] *SCADA Security and Terrorism: We're not crying wolf*. On-line: http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[10] NERC, *Top 10 Vulnerabilities of Control Systems*, version 2007.
On-line: http://www.us-cert.gov/control_systems/pdf/2007_Top_10_Formatted_12-07-06.pdf

[11] IEC, *Security for Industrial Process Measurement and Control - Network and system security*, (draft) report, IEC 62443:2007. (note: will be split into 5 parts).

[12] K. Stoffler, J. Falco, K. Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, NIST Special Publication SP800-82 (draft), USA, September 2006.

[13] ISA, *ISA-TR99.00.01-2007 -- Security Technologies for Industrial Automation and Control Systems, Instrumentation, Systems, and Automation Society*, (draft) Technical Report 2007. Note: will become IEC/TR 62443-5.

[14] ANSI/ISA-95.00.01-2000: Enterprise Control System Integration 1: Models and terminology. On-line: http://www.isa95.com

付録 A.　グッド・プラクティス　チェックリスト

表 A-1 経営層レベルでのグッド・プラクティス

大項目	グッド･プラクティス	√
企業のセキュリティポリシー	#1 全般的な情報セキュリティポリシーがSCADAセキュリティポリシーと関連づけられているか。	
	#2「情報セキュリティマネジメントの実践のための規範」及び関連するセキュリティ標準を参照しているか。	
	#3 SCADAセキュリティポリシーが全般的な（情報）セキュリティポリシーの論理的な拡張となっているか。	
	#4 SCADAセキュリティポリシーに物理的セキュリティが含まれているか。	
	#5 職務内容、責任、権限が文書化されているか。	
リスク管理	#6 SCADAのリスクを企業（経営）レベルのリスク管理の一部としているか。	
セキュリティ意識	#7 継続的なセキュリティ意識教育を実施しているか。	
監査	#8 SCADA環境を対象に、少なくとも年一回のEDP監査（訳注：会計システムを対象とする監査）を実施しているか。	
調達ポリシー	#9 調達／契約時に災害条項が含まれているか。	
	#10 セキュリティ要件を調達プロセスに入れているか。	
	#11 保守･作業を行う第三者との契約に、セキュリティ条項が含まれているか。	

表 A-2 技術的レベルでのグッド・プラクティス

大項目	グッド･プラクティス	√
多層防御	#12 多層防御の原則が実践されているか。	
SCADA環境とOA環境の分離	#13 SCADA環境とOA環境が分離されているか。	
	#14 共有ネットワークの場合、可用性が保証されているか。	
SCADA環境へのセキュアな接続	#15 必要不可欠でない接続は排除されているか。	
	#16 接続が継続的に監視されているか。	
	#17 ファイアウォールは適切に設定･監視がなされているか。	
	#18 PA環境はインターネットに直接接続していないか。	
	#19 データ送信にインターネットを使用していないか。	
	#20 無線アクセスポイントは存在しないか。	
	#21 モデムや外部アクセスに対し厳重な管理がされているか。	
	#22 ネットワーク分離装置とネットワーク接続に関するセキュリティ対策と設定は、定期的に検証されているか。	
SCADAシステム及びネットワーク機器のセキュリティ対策	#23 それぞれのシステム等はセキュリティ対策が強化･最適化されているか。	
	#24 設定は文書化されているか。	
	#25 設定変更プロセスは管理されているか。	
	#26 ウイルス対策ソフトは最新か。	
	#27 パッチの適用ポリシーは有効か。	
SCADA環境のセキュリティ対策	#28 物理的･電子的なアクセスに対する制御がされているか。	
	#29 SCADAネットワークへの接続は認可された機器のみか。	
	#30 厳重に管理されていない状況において、第三者の機器は接続されていないか。	
SCADA環境のパスワードポリシー	#31 初回使用前にデフォルトのパスワードを変更したか。	
	#32 重要パスワードでは、「複雑であること」「関係者外秘であること」「定期的に変更すること」が守られているか。	
	#33 個人パスワードでは、「他人に漏らさないこと」「定期的に変更すること」が守られているか。	
事業継続計画	#34「情報セキュリティマネジメントの実践のための規範」[3] 14章に沿っているか。	
	#35 SCADAシステム及びネットワーク情報を定期的にバックアップしているか。	
	#36 バックアップ媒体は遠隔地において安全に保管しているか。	
	#37 定期的にバックアップの可用性と完全性の検証をしているか。	
	#38 維持管理され、訓練を積んだ事業継続計画があるか。	
情報媒体の管理	#39 有効的な管理と統制的な廃棄が行われているか。	

IPAの提供する重要インフラ関連事業

IPAでは、重要インフラのセキュリティ対策・信頼性向上の普及活動の一環として、以下のような事業を行っています。

～セキュリティについて～

重要インフラセキュリティフォーラム
重要インフラ事業者、重要インフラ事業者にシステムを提供するベンダー等に対する、情報セキュリティの管理的対策や技術的対策等について普及啓発を実施するため、IPAでは毎年「重要インフラセキュリティフォーラム」を開催しております。
※過去の資料が公開されておりますので、ご参照ください。
2008年度資料
http://www.ipa.go.jp/security/event/2008/infra-sem/
2007年度資料
http://www.ipa.go.jp/security/event/2007/infra-sem/
2006年度資料
http://www.ipa.go.jp/security/event/2006/infra-sem/

2003年度
電力重要インフラ防護演習に関する調査報告書
サイバー事故やサイバーテロに対する演習の実施実績が豊富な米国において実際に行われた電力重要インフラ等に関する演習の実施状況について調査を行い、我が国における重要インフラ等の防護体制について検討しました。
http://www.ipa.go.jp/security/fy15/reports/infra/index.html

2008年度
重要インフラ制御システムセキュリティとITサービス継続に関する調査報告書
重要インフラ制御システムの情報セキュリティに関する国内外の動向を調査し、サービス継続を重視した上での適切なセキュリティ対策について検討し、課題を整理しました。
http://www.ipa.go.jp/security/fy20/reports/ics-sec/index.html

～信頼性について～

2009年度
重要インフラ情報システム信頼性研究会報告書
社会インフラとして広く国民生活に関係する重要インフラ情報システムの信頼性を確保するための具体的方策について産業界・学術界の有識者の知見を集積し、今後の方向性を整理しました。
http://sec.ipa.go.jp/reports/20090409.html/index.html

IPAの提供するセキュリティ関連コンテンツ

IPAセキュリティセンターでは、情報セキュリティ対策の普及啓発活動の一環として、以下のようなコンテンツを提供しています。是非ご活用ください。

●：ユーザ向け　▲：開発者向け　◆：経営者向け

情報セキュリティ対策ベンチマーク▲◆
組織の情報セキュリティマネジメントシステムの実施状況を自らが評価する自己診断ツールです。40の設問に答えることでセキュリティに関する自社の取組みがどの程度のレベルにあるのか分かります。
http://www.ipa.go.jp/security/benchmark/index.html

iLogScanner●▲
ウェブサイトのアクセスログを解析することで、そのサイトへの攻撃痕跡を確認するツールです。運営しているウェブサイトがどれほど攻撃を受けているか等の状況を把握することができます。
http://www.ipa.go.jp/security/vuln/iLogScanner/index.html

安全なウェブサイト運営入門●▲
ウェブサイトの脆弱性による被害を中心とした7つの具体的な事件を題材に、ロールプレイング形式で体験的に学習できるソフトウェアです。事件や事故が発生した場合の被害を理解し、事前対策の必要性を学ぶことができます。
http://www.ipa.go.jp/security/vuln/7incidents/index.html

知っていますか？脆弱性（ぜいじゃくせい）●▲
ウェブサイトの運営者や一般利用者向けに、ウェブサイトにおける代表的な10種類の脆弱性について、わかりやすくアニメーションで解説したものです。脆弱性についての理解を深めることができます。
http://www.ipa.go.jp/security/vuln/vuln_contents/index.html

JVN iPedia●▲
国内の製品開発者から公開された対策情報、および海外の脆弱性関連情報のデータベースに登録された情報に基づき脆弱性関連情報を網羅、蓄積しています。検索機能やRSS配信機能を利用することで効率的に脆弱性関連情報を収集することができます。
http://jvndb.jvn.jp/

MyJVN●▲
JVN iPediaに登録された脆弱性関連情報の中から、利用者が必要とする情報のみを効率的に収集できます。情報収集にかかる時間の節約だけではなく、適切な対策を素早く実施できるようになります。
http://jvndb.jvn.jp/apis/myjvn/

セキュリティ情報RSSポータル●▲◆
インターネット上に発信されている様々な情報から、セキュリティに関する最新情報を収集・整理し、セキュリティに関する情報を利用しやすく提供するシステムです。多数のWebサイト上に散在する最新情報を効率よく確認することができます。
http://www.ipa.go.jp/security/fy19/development/rss/

●：ユーザ向け　▲：開発者向け　◆：経営者向け

暗号技術に関するe-Learning教材▲

システムの選定や調達仕様の作成などに必要な暗号技術に関する知識を、幅広く修得するための教材です。ネットワークを通じて教育を行うので、時間や場所を選ばずに暗号技術に関する学習が行えます。

http://www.ipa.go.jp/security/fy19/development/e_Learning_Cipher/index.html

セキュアプログラミング講座▲

想定される様々な攻撃への対策として留意すべき事項を、ソフトウェア開発工程に沿って解説しています。セキュリティ対策を意識したプログラミングができるようになります。

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html

TCP/IPに係わる既知の脆弱性検証ツール▲

TCP/IP(Transmission Control Protocol / Internet Protocol)を実装したソフトウェアの脆弱性を体系的に検証し、自社で開発したソフトウェアに、既知の脆弱性が再び作り込まれないよう防止するためのツールです。TCP/IP利用機器の脆弱性の有無を簡易判定することができます。

http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html

SIPに係る既知の脆弱性検証ツール▲

SIP (Session Initiation Protocol)を実装したソフトウェアの脆弱性を体系的に検証し、自社で開発されるソフトウェアに既知の脆弱性が再び作り込まれないよう防止するためのツールです。
SIPを実装したソフトウェアの脆弱性の有無を簡易判定することができます。

http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

ITセキュリティ評価・認証に関するe-Learning教材▲

ITセキュリティ評価・認証に関連する専門書を読みこなし活用するための入門的な教材です。「自己学習課題」に取組むことにより、習得した知識を実践に結び付け、実際のシステム開発に生かすことができます。

http://www.ipa.go.jp/security/fy19/development/e_Learning_CC/index.html

5分でできる！情報セキュリティポイント学習●▲◆

主に中小企業で働く方を対象とした、1テーマ5分で情報セキュリティについて勉強できる学習ツールです。あなたの職場の日常の1コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を学ぶことができます。

http://www.ipa.go.jp/security/vuln/5mins_point/index.html

IPAでは今後も関係団体等と協力の下、セキュリティ対策の普及に向けた活動を継続していきます。
上記コンテンツ・報告書等へのお問い合わせ、ご意見がございましたら以下までお寄せ下さい。

IPAセキュリティセンター　isec-info@ipa.go.jp

本ページは白紙です

お問い合わせ先

独立行政法人 情報処理推進機構セキュリティセンター
〒113－6591 東京都文京区本駒込2丁目28番地8号
（文京グリーンコートセンターオフィス16階）
TEL：03－5978－7527　　FAX：03－5978－7518
E-mail：vuln-inq@ipa.go.jp　　URL：http://www.ipa.go.jp/security/

本ガイドは以下のURLからダウンロード可能です
http://www.ipa.go.jp/security/fy21/reports/scada/