

製造情報連携フォーラム SCF2007 デモシステム向け セキュリティ検討報告書

2007 年 11 月
XML コンソーシアム
セキュリティ部会

1. はじめに.....	2
1.1. 概要.....	2
1.2. 対象.....	2
1.3. XML に関するセキュリティ.....	2
1.4. 検討メンバー：.....	3
2. 現状分析 = リスク分析.....	3
2.1. リスク分析の手順.....	3
2.2. 3つの重点課題.....	3
2.3. リスクの種類.....	3
2.4. シナリオ分析.....	4
2.5. モジュールごとのリスク.....	7
3. 対策.....	8
3.1. 方針.....	8
3.2. リスクごとのセキュリティ対策技術.....	9
3.3. 全体のセキュリティ対策.....	10
3.4. XML データの保護.....	11
3.5. モジュールごとのセキュリティ対策.....	12
4. セキュリティ対策の評価.....	14

< 利用条件 >

本書は、本書に記載した要件・技術・方式に関する内容が変更されないこと、および出典を明示いただくことを前提に、無償でその全部または一部を複製、翻案、翻訳、転記、引用、公衆送信等して利用できます。なお、全体を複製、翻案、翻訳された場合は、本書にある著作権表示および利用条件を明示してください。

本書の著作権者は、本書の記載内容に関して、その正確性、商品性、利用目的への適合性等に関して保証するものではなく、特許権、著作権、その他の権利を侵害していないことを保証するものでもありません。本書の利用により生じた損害について、本書の著作権者は、法律上のいかなる責任も負いません。

Copyright (c) XML コンソーシアム 2007 All rights reserved.

1. はじめに

1.1. 概要

XML コンソーシアム セキュリティ部会は、製造情報連携フォーラムが開発したシステムコントロールフェア2007(SCF2007)合同デモンストレーション用システムについて、セキュリティ上のリスクを分析し、対策を検討した。検討は、2007年8月からおよそ2ヶ月にわたって、主にシステム開発仕様書の内容に基づいて、セキュリティ部会の中での討論と、製造情報連携フォーラム参加メンバーとの意見交換を通じて実施した。本報告書で、その検討の結果を報告する。

1.2. 対象

本検討では、SCF2007 合同デモンストレーションのシステムにおいて、業務シナリオで定義された範囲において、あらかじめ指摘された重点課題にかかわる重大なセキュリティリスクとその対策を対象としている。必ずしも対象システムのセキュリティについて網羅的にカバーするものではない。網羅的にセキュリティを検討する手段については4 セキュリティ対策の評価に参考情報を記載する。

1.3. XML に関するセキュリティ

XML コンソーシアムでこれまで継続的に調査を行っている XML に関するセキュリティ技術についても、適用を検討した。今回のシステムに関しては、3.3.1項の認証一元化と、3.4項の XML データの保護について、言及した。

1.4. 検討メンバー：

- 岡廻 隆生 (ソフトバンクテレコム株式会社)
- 岡村 和英 (株式会社ネット・タイム)
- 松永 豊 (東京エレクトロンデバイス株式会社)
- 渡邊 圭太 (シスコシステムズ合同会社)

2. 現状分析 = リスク分析

2.1. リスク分析の手順

本システムは、スープやシチューを生産している製造業において、ある工場の受注オーダーから、生産計画、生産管理、工程管理、製造実行といった一連の管理を対象としている。セキュリティの検討においては、まず開発に当たる製造情報連携フォーラムメンバーが考える本システムにおけるセキュリティ面の重要課題を確認した(3つの重点課題)。次に今回対象とするセキュリティリスクの種類を3点定義し、開発仕様書で定義された5種類の業務シナリオごとに、各シナリオ個々のステップにおける重要課題への関連と該当するセキュリティリスクを特定した。最終的に業務シナリオのステップとシステム内モジュールの関係から、各モジュールに推奨されるセキュリティ機能を導き出した。

2.2. 3つの重点課題

2.2.1. レシピ情報の漏洩防止

食品製造の工場において、材料や配合比率を定義するレシピの情報は、企業の事業上の重要情報であり、情報漏洩の防止の対象となる情報資産である。

2.2.2. 食品安全の確保

食品の安全を確保するために、生産指示の情報が不正に変更されないこと、重要な設備に不正にアクセスされないこと、生産ラインの状況が的確に監視され異常をリアルタイムに検知できることが重要となる。

2.2.3. 法的文書の正確性

法令順守の観点で、関連省庁などによって提出や保存が義務付けられている文書には正確性が求められ、その元となる情報が正しいことを保障する必要がある。そのためには、データの改竄や不正なアクセスの防止が必要になる。

2.3. リスクの種類

2.3.1. 情報漏洩

機密情報が漏洩することにより、被害が予想される。今回のシステムでは、競争上最も重要なレシピ情報の他、原価や生産オーダーの情報は、生産計画やコストなどを類推できる可能性があり、漏洩は経営上の大きなリスクとなる。

2.3.2. データ改竄

システム内に存在するデータについては、二つの観点から不正な変更がありうる。一つは、生産内容やスケジュールに異常をきたす意図による、生産情報や生産指示関連の

情報改竄。もう一つは、外部に公開あるいは提出する必要のある情報の改竄で、こちらは内部関係者による変更も考慮する必要がある。

2.3.3. 不正アクセス

システムに対する不正なアクセスが可能であると、前述の2種類のリスクを含め、さまざまな問題につながる。

2.4. シナリオ分析

5種類のシナリオの各ステップごとに、重要課題とセキュリティリスクに対する対応を分析した。その結果を表1に示す。

表1 業務シナリオのステップごとの重要課題およびセキュリティリスクとの対応

		重要課題			セキュリティリスク			具体例
		レシビ情報 の保護	全 安 品 の 確 保	文 書 的 正 確 性	情 報 漏 洩	デ ータ 改 竄	不 正 ア ク セ ス	
	シナリオ A 後工程での品質ばらつき管理と早期対応							
A-1	後工程において、計量、やぶれ、印字、箱の組み立て異常、をモニタリングする。							
A-2	品質の検査として、抜き取りで、たんぱく質、炭水化物、の数値を検査する。							検査データの改竄
A-3	金属探知の工程において、探知された発生頻度を記録する。							検査データの改竄
A-4	ラインアウトの製品に対して、その数量をオペレータが手入力する。							MES サーバへのデータ不正入力
A-5	上記の数量入力をPHSでオペレータに指示する。							携帯端末への不正アクセス
A-6	上記のさまざまな情報を、オペレータが画面にレイアウトして表示し監視する。							
A-7	品質異常が発見されたら、設備の参照可能な情報を調べ、原因を解明する。							
A-8	品質異常に対応して、必要に応じてラインを止める。							不正なライン停止指示
A-9	計量値が予定より多い場合には、仕込み量を変更する。							
A-10	改善によってレシビ情報を交換し、生産方法を切り替える。							生産管理・MES サーバからのレシビ情報漏洩
		レシビ情報 の保護	全 安 品 の 確 保	文 書 的 正 確 性	情 報 漏 洩	デ ータ 改 竄	不 正 ア ク セ ス	
	シナリオ B 不良原価削減：チョコ停対策と予防保全							

B-1	設備のさまざまな状態値をネットワーク上で必要に応じて参照可能にしておく。									
B-2	設備の稼働状態を常に監視し、稼働していない場合の原因を把握する。									
B-3	設備が停止した場合に、復旧に時間が必要な場合はその見積もり時間を設定。									
B-4	設備の停止の都度、オペレータは停止の原因をシステムに入力する。									停止データの不正入力・改竄
B-5	設備の停止をスケジューラに伝え、再スケジューリングを要求する。									
B-6	チョコ停の時間の累積時間を、装置ごとに計測して記録する。									停止データの改竄
B-7	チョコ停の累積時間をオペレータが画面に表示し監視する。									
B-8	遠隔地にある設備の必要情報を広域網をつかって収集する。									
B-9	チョコ停の原因をしらべ、必要情報と累積稼働時間をまとめてレポートする。									
B-10	ロットに対する装置からの個別実績原価を計算して表示する。									原価情報の漏洩 装置稼働情報の改竄
		レシピ情報の保護	安全食品の確保	文書法的正確性	情報漏洩	データ改竄	不正アクセス			
シナリオ C 生産指示の適正化と段取り替え管理										
C-1	生産計画から生産オーダーを生成しスケジューラにスケジューリングを依頼する。									生産計画情報の漏洩 不正なスケジューリング指示
C-2	スケジューラは、生産オーダーをもとに作業指示(予定作業)を生成する。									
C-3	スケジューラは、段取り替え情報をもとに、最適な生産順序を計算する。									
C-4	スケジューラは、段取り替えのスケジュールを生成して作業者に指示する。									
C-5	作業指示をMESサーバに送り、製造工程に対してディスパッチングを行う。									不正なスケジューリング指示
C-6	ディスパッチングの時点で必要に応じてレシピ情報をアップロードする。									レシピ情報の漏洩
C-7	製造工程は作業指示の結果をMESサーバに送り予定と実績を対応づける。									実績データの改竄
C-8	前工程、後工程の工程進捗状況を可視化し画面に表示する。									
C-9	前工程、後工程のスケジュールから、中間仕掛り在庫量を計算し表示する。									
C-10	実績作業とともに、生産数量をERPに報告する。									実績データの改竄

		レシビ情報 の保護	食品安全 の確保	法的文書 の正確性	情報漏洩	データ改竄	不正アクセス	
シナリオ D 中間在庫の管理（在庫適正化）								
D-1	中間在庫用タンクにICタグを装着する。							
D-2	前工程が完了したら、ロットと対応する中間タンクICタグを関係づける。							
D-3	作業者が定期的にタンクの位置をチェックし携帯電話で報告する。							検査結果の改竄
D-4	後工程の開始は、中間在庫の対応付けが行われてから実行する。							
D-5	画面上で、現時点での中間在庫の位置と数量を把握する。							
D-6	スケジューリング結果をもとに将来の中間在庫量の理論値を表示する。							
D-7	適切な中間在庫量（バッファ量）を画面で設定する。							
D-8	生産計画において、中間在庫量を考慮して前工程の生産時期と数量を決める。							
シナリオ E 管理ワークシートと携帯電話の利活用								
E-1	携帯電話の位置認識機能を利用して誰がどこで作業しているかを把握する。							
E-2	異常が発生した場合に、作業者にダイナミックに作業を割り当てる。							不正な作業割り当て指示
E-3	ネットワーク上で利用可能な情報をもとに設備点検記録簿を簡単に作成する。							点検記録の改竄
E-4	点検時に保守マニュアルを携帯電話に（QRコードで）自動ダウンロードする。							
E-5	点検簿の点検項目をあらかじめ設定し、柔軟に拡張できるようにしておく。							
E-6	携帯電話を活用し、点検簿の点検項目の入力を効率化する。							携帯端末への不正アクセス、 点検記録の改竄
E-7	シフト交代時に、必要な情報を自動収集することで引継ぎ簿を容易に作成する。							
E-8	引継ぎ簿のフォーマットを必要に応じて容易にオペレータが変更できる。							不正な変更
E-9	法的文書や管理文書を、必要に応じて本社へ通知する。							法的文書の改竄 重要情報の漏洩

2.5. モジュールごとのリスク

シナリオの分析(2.4項)より、各モジュールにおけるセキュリティリスクを検討した。

2.5.1. 生産管理サーバ

- A-8 不正なライン停止指示
- A-10 生産管理・MES サーバからのレシピ情報漏洩
- B-10 原価情報の漏洩、装置稼動情報の改竄
- C-1 生産計画情報の漏洩、不正なスケジューリング指示
- C-10 実績データの改竄
- E-9 法的文書の改竄、重要情報の漏洩

2.5.2. MES サーバ

- A-4 MES サーバへのデータ不正入力
- A-10 生産管理・MES サーバからのレシピ情報漏洩
- C-5 不正なスケジューリング指示
- C-7 実績データの改竄
- E-2 不正な作業割り当て指示

2.5.3. PIMS サーバ

- A-2 検査データの改竄
- B-4 停止データの不正入力・改竄
- B-6 停止データの改竄
- B-10 原価情報の漏洩、装置稼動情報の改竄

2.5.4. OPC-UA サーバ

該当なし

2.5.5. 品質・保全文書管理

- B-10 原価情報の漏洩、装置稼動情報の改竄
- E-3 点検記録の改竄
- E-6 携帯端末への不正アクセス、点検記録の改竄
- E-8 不正な変更
- E-9 法的文書の改竄、重要情報の漏洩

2.5.6. 生産管理

該当なし

2.5.7. スケジューラ

- C-5 不正なスケジューリング指示

2.5.8. MES アプリ

- C-6 レシピ情報の漏洩

2.5.9. 仕掛品管理

該当なし

2.5.10. 品質・保守管理

A-2 検査データの改竄

A-3 検査データの改竄

B-4 停止データの不正入力・改竄

2.5.11. 点検管理

E-6 携帯端末への不正アクセス、点検記録の改竄

2.5.12. 遠隔保守

該当なし

2.5.13. MES 変換器

該当なし

2.5.14. OPC-DA サーバ

該当なし

2.5.15. 無線 I/F 機器

該当なし

2.5.16. SCADA

該当なし

2.5.17. DCS

該当なし

2.5.18. PLC

該当なし

2.5.19. RFID 機器

該当なし

2.5.20. 携帯端末

A-5 携帯端末への不正アクセス

D-3 検査結果の改竄

E-6 携帯端末への不正アクセス、点検記録の改竄

2.5.21. 構内中継網

該当なし

3. 対策

3.1. 方針

今回のデモシステムは4つの階層からなっており、各階層の特性によってセキュリティの要求が異なる。

3.1.1. 計画・管理層と現場管理層

上位の計画・管理層と現場管理層については、人間が操作することが前提となるシステムが配置される。各種のデータベースが存在し、様々な役割の人間が、多様な経路でアクセス可能なため、より厳しいセキュリティ対策が必要になる。

3.1.2. 実行制御層とリアルタイム層

下位の実行制御層とリアルタイム層については、ほとんどが自動運用され、環境的にもセキュリティの厳しい生産現場となるため、アクセスできる人やアクセス手段が限られる。リアルタイム性を損なう類のセキュリティ対策は導入しにくい事情もあり、この階層 2 層の中でのシステム的な対策は最小限にとどめる。その代わりに、物理的、環境的な対策が重要となる。

3.1.3. セキュリティ境界の対策

各階層ではセキュリティ対策の程度も、利用者の種類・数も異なるため、その境界がネットワークで接続されている場合には、不正なアクセスを防ぐ手段が必要になる。使用されるプロトコルの判別まで可能なファイウォールを設置し、システム間連携に必要な通信以外は遮断する。

3.2. リスクごとのセキュリティ対策技術

3.2.1. 情報漏洩

情報漏洩については、事後の対応が難しい。例えばレシピ情報が流出してしまうと、流出の事実を後から確認できても、関与者を特定できても、被害の軽減が難しい可能性がある。従って、予防措置が最も重要となる。

- アクセスポリシーの策定（システム利用者の特定と個々の権限設定）
- アクセス制御（認証、権限確認、アクセス記録）
- データの暗号化（通信路、ディスク上のファイル、データベース内のデータ）

3.2.2. データ改竄

不正なデータの変更は、正しい権限を持った担当者によって行われることも多く、防止も検知も難しい。アクセス制御を徹底するとともに、詳細な変更記録(アクセスログ)を確実に保存し、異常なアクセス(日ごと異なるアクセス内容、アクセス元、曜日や時間帯など)を検知できるようにしておくことが必要となる。

- アクセスポリシーの策定（システム利用者の特定と個々の権限設定）
- アクセス制御（認証、権限確認、アクセス記録）
- 変更記録（ファイルアクセスログ、データベース監査ログ）
- アクセス監視（異常なアクセスの検知）

3.2.3. 不正アクセス

正規の権限を持たないものによるアクセスは、情報漏洩やデータ改竄につながるだけでなく、破壊行動やその他のさまざまな不正につながるため、防止する必要がある。

- ファイアウォール
- 侵入検知/防御システム (IDS / IPS)
- アクセスポリシーの策定 (システム利用者の特定と個々の権限設定)
- アクセス制御 (認証、権限確認、アクセス記録)

3.3. 全体のセキュリティ対策

3.3.1. 認証の一元化

多数のアプリケーションモジュールが連携して動作するシステムでは、個別に認証とアクセス制御が実装されている場合が多い。そうすると、連携するモジュール間でユーザ ID の伝達が難しくなり、連携先ではユーザごとのアクセス制御が行われない状況が起りやすい。また、後からデータアクセスや操作の履歴を調査する場合も、連携先のシステムではユーザが特定できないことがありうる。こうしたことを避けるためには、全体で認証の仕組みと ID 情報を一元化し、システム連携する際にもユーザの操作を追跡できるようにする必要がある。具体的な手段としては 2 種類ある。

- 1) シングルサインオン (SSO) - システム全体の ID 情報を統一し、すべてのモジュールが同一の ID 情報を参照する。ID の登録・管理は一元化する。シンプルな管理が実現できるが、全モジュールをこれに合わせる必要があり、既存のシステムに適用するには大きな変更が必要になる。
- 2) ID 連携 - 個別に ID 管理を行うシステム間の ID 同士をマッピングし、ID 情報が異なっても追跡できるようにする。既存のシステムにも、連携部分を付加する形で適用できるが、個々の ID 情報管理と連動したマッピングの運用管理体制を構築する必要がある。ID 連携には、XML を使ったセキュリティ情報の通信規格 SAML¹ (標準化団体 OASIS 策定) が多く使われる。

3.3.2. ネットワークアクセス制御

ネットワークが張り巡らされ、接続が一般的な技術になってきたため、悪意のユーザが不正に機器を接続し、本来接続を想定していない機器から攻撃が行われる可能性が増大している。これを防ぐためには、ネットワーク全域において不正機器の接続を防止する手段が必要になる。総合的にネットワークアクセス制御 (Network Access Control, NAC) といった呼び方をされる技術だが、複数の技術要素からなり、それぞれいろいろな方式がある。

- 1) ユーザ認証 - ネットワークに接続する時点でユーザの ID 提示を求め認証する。
- 2) 機器認証 - 接続される機器自体を認証する。現時点では MAC アドレスによる認証が主流。

¹ OASIS Security Assertion Markup Language (SAML) v2.0

<http://www.oasis-open.org/specs/index.php#samlv2.0>

- 3) 端末検査 – 接続される機器の構成を検査し、ポリシーに適合しているかどうかを判断する。OS 種類、パッチ、ウイルス検査ツールなどを検査する。
- 4) アクセス制御 – 認証や検査の結果、接続を許された機器以外をネットワークに侵入させないための制御を行う。ネットワークスイッチかファイアウォールを利用。

3.3.3. ログ管理

システム内では、不正の抑止と事故発生時の分析のため、各種のログを保存・管理する必要がある。ログの種類としては主に、サーバなどの構成変更を記録するシステムログ、利用者を記録するアクセスログ、データベースのデータアクセスと変更を記録するデータベース監査ログが必要になる。そしてこれらを一元的に保管し、分析を可能にするログ管理のシステムが必要になる。

3.3.4. システム状態の監視

工場内の製造機器に対しては、各種の監視機能が設定され、生産状態を監視できるようになっているが、これらの上位に来る管理系のモジュールに対しても、当然監視が必要になる。主要なサーバに対して、システム稼働、負荷状況、プロセスの稼働などを監視する。

3.4. XML データの保護

今回のシステムではモジュール間連携が主要なテーマとなっており、連携通信の多くで XML データをベースとしたメッセージが利用されている。XML の利点として挙げられる性質のうち、汎用的なことで可読性が高いことがこうした連携に採用される大きな理由になっている。ただしこのことは、そのままでは情報漏洩や改竄につながりやすいことにもつながる。したがって、レシビ情報や生産計画、生産実績など、重要な情報が XML 形式で伝達される場合は、適切な保護を行うことが前提となる。

3.4.1. XML データの漏洩に対する保護

XML データを暗号化する。具体的な手法として標準化団体 W3C が策定した規格 XML Encryption²を利用して、XML データ全体のほか、1 件のデータの中でも必要な部分だけ暗号化することができる。

3.4.2. XML データの改竄に対する保護

XML データに電子署名を付与し、後から署名検証を行うことで、変更されているかどうかを検出できる。具体的な手法として標準化団体 W3C が策定した規格 XML Signature³を利用して、XML データ全体のほか、1 件のデータの中でも必要な部分だけに電子署名を付与することができる。

² W3C XML Encryption WG <http://www.w3.org/Encryption/2001/>

³ W3C XML Signature WG <http://www.w3.org/Signature/>

3.4.3. モジュール間の整合性

暗号化や電子署名などの保護技術を適用した上でデータを伝達した場合、受け取ったモジュールでは、復号や署名検証など対応する処理が必要になる。その際、使用した暗号技術や鍵情報などを伝える必要がある。その手段としては、標準化団体 OASIS が策定した規格 Web Services Security (WS-Security)⁴を使うことができる。ただし WS-Security は、プロトコルとして SOAP を前提にしている。

3.5. モジュールごとのセキュリティ対策

2.5項において重要なリスクが想定されたモジュールに対して、具体的なセキュリティ対策案を検討した。

3.5.1. サーバ関連モジュール

3.5.1.1 生産管理サーバ (A P S O M / P S L X)

ビジネス層にあり、ハイレベルな生産計画の遂行とレシピをはじめとする機密情報の保護が重要。

セキュリティ対策:

- システムに対するアクセス制御
- データ種類に対する役割ベースのアクセス制御 - レシピ情報、原価情報、装置稼働情報、生産計画情報、生産実績情報
- 特に重要なデータの暗号化 - レシピ情報、原価情報
- XML メッセージ保護 - MES サーバとスケジューラ向けの生産オーダ
- RDB を持つため、データベース監査ログの記録

3.5.1.2 M E Sサーバ (A P S O M / O A S I S - P P S)

現場管理層にあり、ビジネス層とも連携があり、下位層の制御を行う。

いわば上位層と下位層の境界に位置するサーバであるため、セキュリティ面の問題があると「閉じた」システムを前提とする下位層に重大なリスクを導いてしまう。

不正アクセス防止が重要。

セキュリティ対策:

- システムに対するアクセス制御
- データ種類に対する役割ベースのアクセス制御 - レシピ情報、生産実績情報
- 特に重要なデータの暗号化 - レシピ情報
- XML メッセージ保護 - スケジューラ向けの実績情報、OPC UA サーバ向けの実行指示
- RDB を持つため、データベース監査ログの記録

⁴ Web Services Security 1.0 (XML コンソーシアムによる日本語訳)

<http://www.xmlconsortium.org/wg/sec/wss.html>

3.5.1.3 PIMS 情報サーバ (三井情報開発)

下位層から稼動状況の情報を受け取り、状態監視、稼動状況の記録を行う。

セキュリティ対策:

- システムに対するアクセス制御
- 各種検査および実績データの改竄防止 - データベースのアクセスログ

3.5.1.4 OPC - UAサーバ (デジタル/日立/OPC - J)

上位層から指示を受け取り生産機械の制御、また下位層からフィードバックを受け上位層へ伝達。

セキュリティが必要なシナリオは該当なし。

ただし、品質管理・保全管理サーバ、MES サーバより保護されたメッセージを受け取り、暗号データの復号処理が必要。

3.5.2. 業務アプリケーションモジュール

3.5.2.1 スケジューラ (横河電機)

生産管理サーバから生産オーダを受け取り、MES サーバに指示を発行。

データ保持は無く、不正操作の防止が主眼。

セキュリティ対策:

- システムに対するアクセス制御
- XML メッセージ保護 - MES サーバ向けの予定作業情報。

3.5.2.2 MES アプリ (ケーティシステム)

MES サーバからの進捗管理を受け、実行指示を行う。

実行制御層のため、特にセキュリティを必要としないが、MES サーバから保護されたメッセージを受け取り、暗号データの復号処理が必要。

3.5.2.3 品質・保守管理 (Mfg X / マイクロソフト)

実績などの情報を集積し各種文書を管理するため、改竄と情報漏洩への対策が必要。

セキュリティ対策:

- システムに対するアクセス制御
- データ種類に対する役割ベースのアクセス制御 - レシピ情報、生産実績情報、原価情報
- 特に重要なデータの暗号化 - レシピ情報、原価情報
- XML メッセージ保護 - OPC UA サーバ向けのレシピ情報
- RDB を持つため、データベース監査ログの記録

3.5.2.4 装置点検管理 & 携帯電話 (NTTドコモ)

点検記録の改竄に対する対策が必要。

セキュリティ対策:

- 携帯端末におけるアプリケーションへのアクセス制御

4. セキュリティ対策の評価

本報告書では、業務シナリオと重点課題の範囲において、セキュリティの検討を行った。ただし、システム全体のセキュリティについて検討を行う場合には、客観性と網羅性を持った標準規格に沿った評価を行うことが望ましい。

情報セキュリティマネジメントについては、JIS Q 27001:2006「情報技術 セキュリティ技術 情報セキュリティマネジメントシステム 要求事項」がある(国際標準 ISO/IEC 27001の日本語訳)。想定されるリスクに対してどの程度の対策を行うかといったリスク管理や、PDCA サイクルに沿ったセキュリティ管理などの方針にかかわる内容を評価できる。

より具体的なセキュリティ対策の評価については、JIS Q 27002:2006「情報技術 セキュリティ技術 情報セキュリティマネジメントの実践のための規範」がある(国際標準 ISO/IEC 17799の日本語訳)。この中では本検討でも触れたアクセス制御や、暗号化やネットワークセキュリティを含む通信及び運用管理などについても規定されている。