Vol.2010-CSEC-50 No.41
2010/7/2

IDEF0 を用いた情報セキュリティ対策の評価支援

谷口浩之† 金谷延幸† 鈴木拓也†† 奥原雅之††

情報セキュリティガバナンスの評価をするための，情報セキュリティ対策のモデルと表記法を提案する．本モデルは，情報セキュリティ対策をルールとプロセスとデータとリソースで表現するものである．本提案は，業務のプロセスモデリング手法である IDEF0 に基づいている．本報告では，モデルの基本定義を示し，セキュリティ統制評価プロセスの一部へ適用した結果について述べる．

Proposal of evaluation support technique of information security measures with IDEF0

Hiroyuki Taniguchi† Nobuyuki Kanaya†
Takuya Suzuki†† Masayuki Okuhara††

It proposes the model and the notation of the information security measures to evaluate the information security governance. This model expresses the information security measures by the rule, the process, data, and the resource. This proposal is based on IDEF0 that is the process modeling technique of the business. In this report, the model's basic definition is shown, and the result of application to a part of the security management evaluation process is described.

1. はじめに

情報セキュリティガバナンス[1][2]の目的を達成するには，セキュリティ方針を徹底させる統制と評価・改善のサイクルを回す必要がある．特に，セキュリティ方針を組織の末端まで浸透させることは難しい．このことは，方針を反映して作成したルールや運用手順等が，実際の運用では間違って解釈されていることからわかる．

間違った解釈が行われる原因の一つに，ルールや手順の中の重要な事項が，作成者の経験や常識により省略されているということがある．実際に運用する側は省略された暗黙知を読み取る必要があり，その解釈の違いがリスクの原因になる．また，セキュリティ対策状況を評価する指標の作成においても同様の問題があり，解釈の違いは評価の正確性を失う原因になる．

本稿では、業務プロセスのモデリング・分析手法である IDEF0[3]を適用し，情報セキュリティ対策である運用手順を，正確かつ直感的に理解する手法を提案する．さらに，セキュリティ統制状況を評価するための基準作成方法と適用例について述べる．

2. IDEF0

IDEF0 は，組織活動を機能的側面に着目して記述するためのモデルと方法論[4]であり，米国連邦情報処理標準(FIPS183)となっている．また，品質管理におけるプロセスアプローチ[5]にも親和性が高く，ソフトウェア開発プロセスの分析に使われることもある[6].

IDEF0 における基本的な考え方は，組織活動を構成する個々の作業を，機能・入力・出力・制約・機構の 5 つの要素で示すことである．関連する機能をつなぎ合わせることで，組織活動を表すことができる．

モデル要素

- 機能　組織活動における作業（動詞・動詞句）
- 入力　作業に必要なデータ・オブジェクト（名詞）
- 出力　作業の結果（名詞）
- 制約　作業で守るべき決まりごと（名詞）
- 機構　作業を支える仕組み（名詞）

† （株）富士通研究所
Fujitsu Laboratories Limited.
†† 富士通（株）
Fujitsu Limited.

また，作業の表記法として，アクティビティを表すボックスとデータやオブジェクトの流れを示すアローを用いる（図 1）．アローをつなぎ合わせてアクティビティの関係を表すことで，組織活動を俯瞰可能な図を作成できる．一般的なデータフロー，プロセスフロー，フローチャートに比べ，制約や機構が書けることが差分である，

3. 情報セキュリティ対策表記への IDEF0 適用

3.1 情報セキュリティ対策

情報セキュリティ対策を，情報資産を扱う業務に対する制約と定義できる.この場合，容易に IDEF0 で情報セキュリティ対策を含む表記ができる（図 1）．この図からは，どの業務にどのセキュリティ対策を行っているか，セキュリティ統制の状況が分かる．しかし，情報セキュリティ対策の運用手順に示された機能やプロセスは表現されていないため，具体的な対策を解釈する助けにはならない．

情報セキュリティ対策を正確に解釈するには，運用手順に記された機能やプロセスまで含めて表現する必要がある．IDEF0 の適用では，各機能やプロセスの入出力，機構, また正しい動作をするための制約が必要であり, 基本的に欠けることを許さない．

情報セキュリティ対策の実施で問題となるのが，一つの業務を実施するイベント毎に対策の実施が必要なのか，事前に一括して実施が可能なのかが明確になっていない場合である． IDEF0 の適用では，この区別の曖昧さを許さない．運用手順への表記例（図 2）では，アローにより対策の実施タイミングを区別可能である．

情報セキュリティ対策表記に用いた，モデル要素と表記法の基本定義を以下に示す.

モデル要素

- アクティビティ　（動詞・動詞句）
  - ✧ 制約アクティビティ　情報セキュリティ対策の機能やプロセス
  - ✧ 業務アクティビティ　情報セキュリティ対策の対象業務
- 入力データ　　アクティビティの対象となるデータ・オブジェクト（名詞）
- 出力データ　　アクティビティの結果となるデータ・オブジェクト（名詞）
- 条件データ　　アクティビティの実行条件となるデータ・オブジェクト（名詞）
- リソース　　アクティビティの主体（名詞）

表記法

- ボックス　　アクティビティを示す
- アロー　　データやオブジェクトの流れを示す
  - ✧ 縦軸アロー　アクティビティ実施に非同期な流れ
  - ✧ 横軸アロー　アクティビティ実施に同期的な流れ

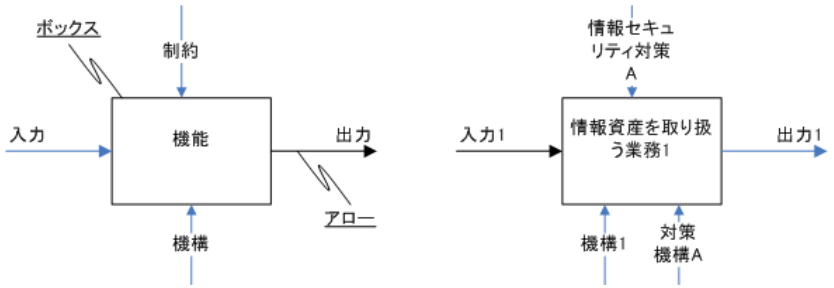

図 1　IDEF0 表記法と表記例

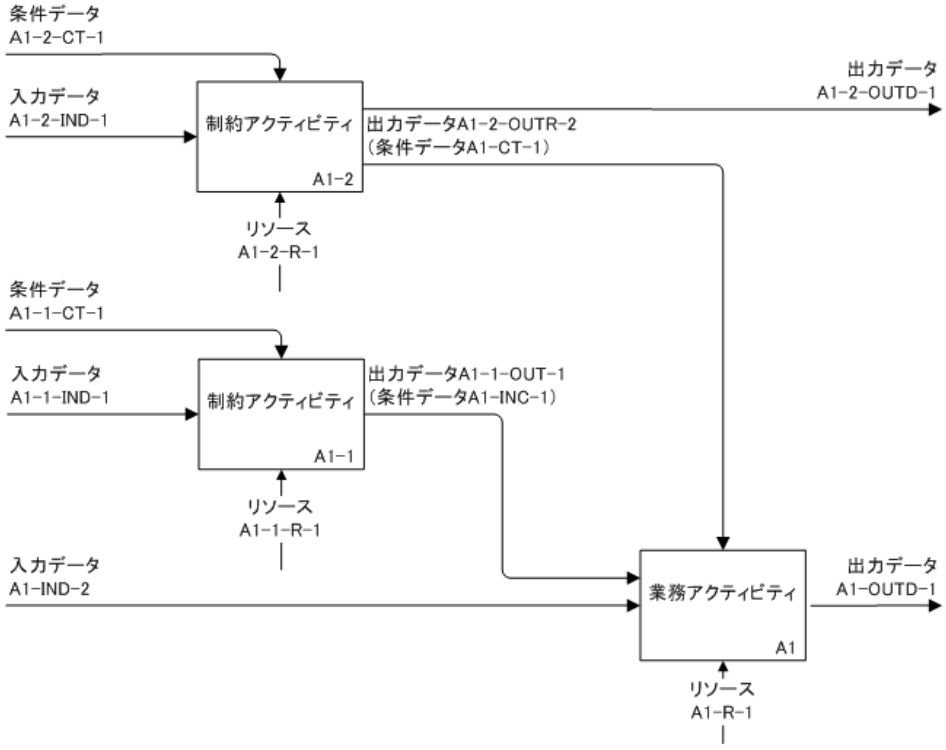

図 2 情報セキュリティ運用手順の IDEF0 表記例

3.2 適用例「情報機器持ち出し」に関する運用手順の IDEF0 表記

「情報機器の持出し手順」(図 3) を提案した基本定義に基づき IDEF0 表記したものを示す（図 4）．作成手順は，①運用手順からの IDEF0 要素の抽出，②運用手順に沿った各アクティビティの関連付けの 2 段階である．

具体的には，運用手順書からアクティビティとなる動詞・動詞句として「持出し」「申請」「承認」を抽出し，入出力・リソース・条件となる情報を抽出する．また，各要素を示すデータを含む実体（オブジェクト）がわかる場合は示す．手順書に書かれていない要素は「？」で示す．運用手順に従い，各アクティビティの関係をデータの流れであるアローで示す．

条件については，アクティビティ実施に同期して入力されるのか，非同期に入力されるのか注意が必要である．例えば「申請」というアクティビティにおいて，「申請先である「情報機器の責任者」が「申請」毎に変わるのであれば，横軸アローとして「申請」アクティビティに入力される．ここでは，「情報機器の責任者」は個々の「申請」には不要であり，申請はあらかじめ決まった責任者へ行われるとして縦軸アローを使って表記している．同様に「持出し」アクティビティにおける「許可」は，個々の「持出し」で必要となると手順書に書いてあるので横軸アローを使って表記している．

作成された IDEF0 図は，主に次の視点で情報セキュリティ対策に関する気づきを与えてくれる．

視点

- あいまいな表記（IDEF0 の要素．すべて明確でなければならない）
- 各要素のデータの根拠（データ入手元．明確でなければならない）
- 情報セキュリティ対策実施タイミング（制約アクティビティと業務アクティビティの関係．つながっていなければならない）

上記視点で分析を行うと，本手順書には「承認」における条件が明確になっていないことがわかる．承認は情報機器責任者の主観によって行われており，場合によってはリスク発生の原因と考えることもできる．また，「持出し」の入出力データは定義されていない．どの時点で「持出し」対策を実施すべきか不明であり．現場での解釈によって行われていることがわかる．

各条件データは，条件を含む実体が明確になっていない．各条件はアクティビティの主体がそれぞれ入手したものと解釈できる．場合によっては，間違った情報に基づいている可能性もあり，リスク発生の原因と考えることができる．

分析結果は，手順書の改善か運用評価のための実態調査場所の特定に利用できる．

これらの分析結果からもわかるように，IDEF0 で表記された運用手順（図 4）は，自然言語で書かれた運用手順（図 3）より，正確かつ直感的な理解が可能である．

情報機器の持出し

構成員は、情報機器の持出しを行う場合、持出し毎に以下の手順に従う。

a 情報機器の責任者に持出し申請を行う。以下の内容が明確になっていること。
・持出し理由（持出し先を含む） ・セキュリティ施策の実施状況
・保存情報の内容 ・持込み予定日

b 情報機器の責任者の承認を得る

図 3 情報セキュリティ対策 運用手順書（例）

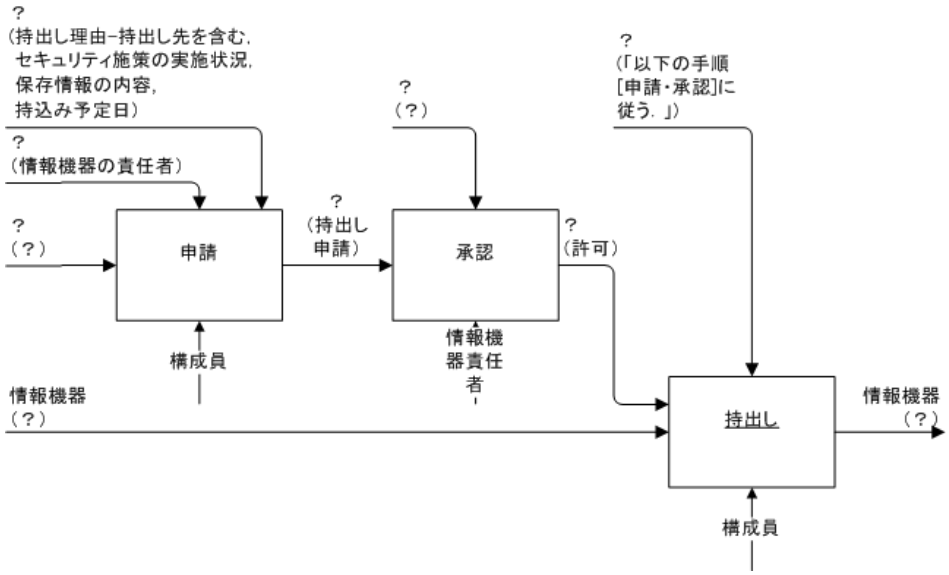

図 4 情報セキュリティ対策 運用手順 IDEF0 表記（例）

4. セキュリティ統制評価への IDEF0 適用

4.1 セキュリティ統制評価

セキュリティ統制評価を，統制として示したセキュリティ対策が運用現場にてどれだけ遵守されているか測定することとする．評価手順は次のように定義する．

評価手順

① あるべきセキュリティ対策の作成
情報セキュリティ運用手順書を分析し，統制によって与えられる条件を明確にする．また，調査・測定対象となりうる条件を実施したという根拠を示すデータまたはオブジェクトを明確にする．

② 運用現場の調査項目の抽出
あるべきセキュリティ対策のデータやオブジェクトを，運用現場の実体と対応させ，統制に関する測定項目を抽出する．

③ 評価対象である運用現場の調査
調査項目について，ヒアリングまたはログ等を参照してデータを収集する．

④ 基準と調査結果の比較
基準と調査結果が同じであることを確認する．また，基準との差分を測定する．

評価を正確に行うためには，統制として示されているものを全て明らかにしておく必要がある．そのためには，項目抽出時に参照する運用手順を補完し，あるべきセキュリティ対策を正確に作成しておくことが重要になる．ここに IDEF0 による形式的な表記を用いることで，要素やデータの流れを明確にできる．

また, IDEF0 の要素を用いることで, 定型的な対策機能やプロセスの定義ができる．これを事前にデータベース化しておくことで，誰もが運用手順の補完時に利用でき，担当者の見落としを避けることができる．さらに，図により全体を俯瞰することができ，不足する情報に関する議論をサポートできる．IDEF0 により，あるべきセキュリティ対策を作成することが容易になると考えられる．

4.2 適用例：「情報機器持出し」のあるべきセキュリティ対策の作成

「情報機器の持出し手順」（図 3）の運用に関して，統制評価の際の基準となる，あるべきセキュリティ対策の作成を行う．

4.2.1 基準となる運用手順の表記

前述した情報機器持出し手順の IDEF0 表記（図 4）を用いる．

4.2.2 情報セキュリティ機能定義による補完

有識者等のノウハウを基本定義に従って蓄積した情報セキュリティ機能定義（表 1）を作成しておく．例えば，この定義によれば，承認機能は，「承認対象名」が必ず入力され，「承認結果」として結果と承認した対象名が出力されること，また，監査証跡に使われる「承認記録」が出力されること，さらに「確認事項」が条件として必須であることが示されている．これを参照することで，承認アクティビティで不明確であった「条件」には「確認事項」があることがわかり，IDEF 0 図上にデータを追加できる．同様に，「承認」と「持出し」の出力に記録を追加した．

表 1　情報セキュリティ機能定義

	機能名	アクティビティ	入力	出力	条件	リソース
1	承認		(<承認対象名>)	(<承認結果>[許可/不許可、承認対象名])、(<承認記録>[確認事項、承認者名、日時])	(<確認事項>)	管理責任者
2	期限設定		(<設定対象名>)、(<返却/削除/廃棄/持出し/持込み/搬入/搬出　予定日>)、(<時刻情報>)	(<設定対象名>、<設定日時>)	(<最長期限>)	
3	搬出	搬出、持出し		(<持出し記録>[搬出対象名、搬出者名、承認者名、日時])		
			:			

さらに，図 4 では「申請」の入力情報が不明であるが，条件に「持込み予定日」を含む申請項目が示されているため，入力にも同様の情報が存在する可能性が高い．情報セキュリティ機能定義表より「予定日」が入力に示されている場合は，同アクティビティに「期限設定」機能があることが予想できる．手順として矛盾しないため，期限設定の要素も申請のデータに追加した．（図 5）

Vol.2010-CSEC-50 No.41
2010/7/2

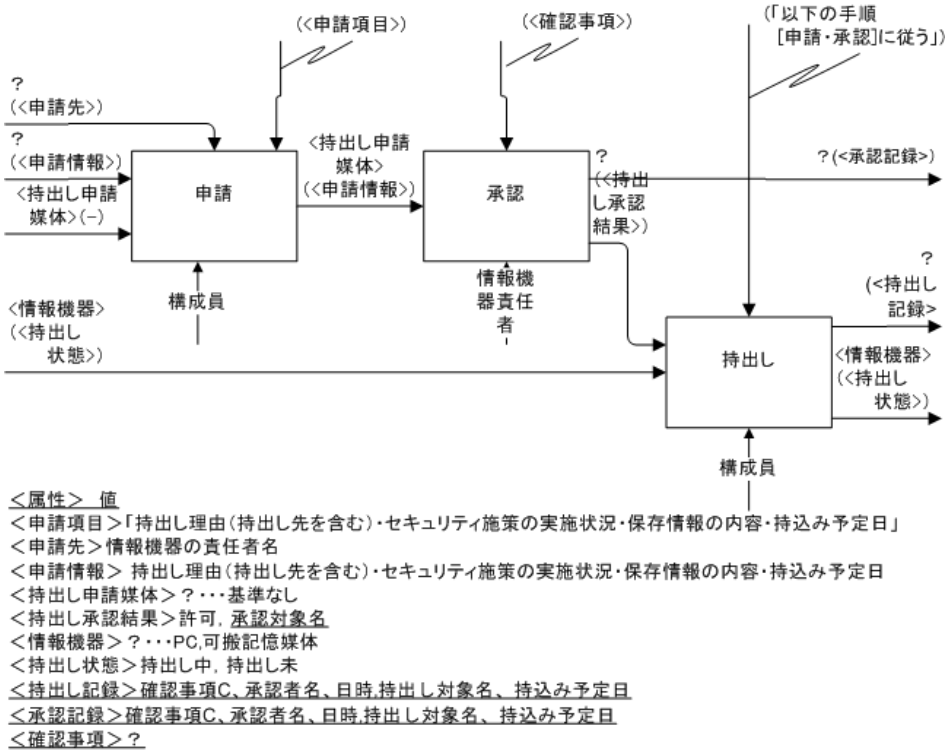

図 5 あるべき「情報機器持出し」対策（情報セキュリティ機能定義による捕捉）

4.2.3 セキュリティ統制フロー定義による補完

他の運用手順の IDEF0 表記を蓄積したセキュリティ統制フロー定義（表 2）を作成しておく．同フロー定義は，表ではなく IDEF0 図そのもの（図 6）で代用可能である．これを参照することで，「条件」である承認アクティビティの「確認事項」や申請アクティビティの「申請項目」は，その実体や入力元が不明確であったが，「運用マニュアル」にあることがわかり，オブジェクトを追加した．また，運用マニュアルは，マニュアル作成アクティビティにより上位管理者が作成していることが分かり，同アクティビティを「情報機器持出し」手順の IDEF0 図に追加した．（図 7）

表 2 セキュリティ統制フロー定義

	フロー名	アクティビティ	入力	出力	条件	リソース
1	手順書作成	運用マニュアル作成	運用手順書ひな型(?)、?(<運用手順情報>)	運用手順書(<申請項目>、<確認事項>、<注意事項>)	当社規定書(?)	上位管理責任者
:						

又は

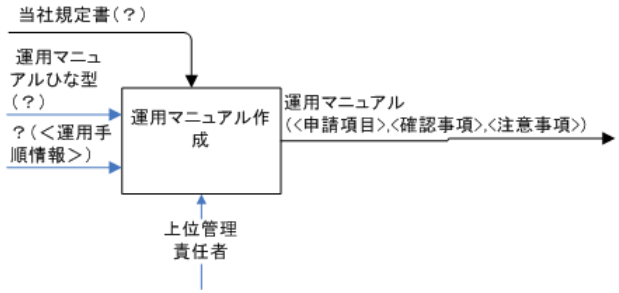

図 6 手順書作成フロー

情報セキュリティ機能定義は，１つの機能（アクティビティ）を入出力・条件・リソースで定義するものであり，必須の要素しか示していない．一方，セキュリティ統制フロー定義は，IDEF0 で書いた「手順書作成」と同等に，運用手順に含まれる全アクティビティの機能定義とその関係を示したものである．

Vol.2010-CSEC-50 No.41
2010/7/2

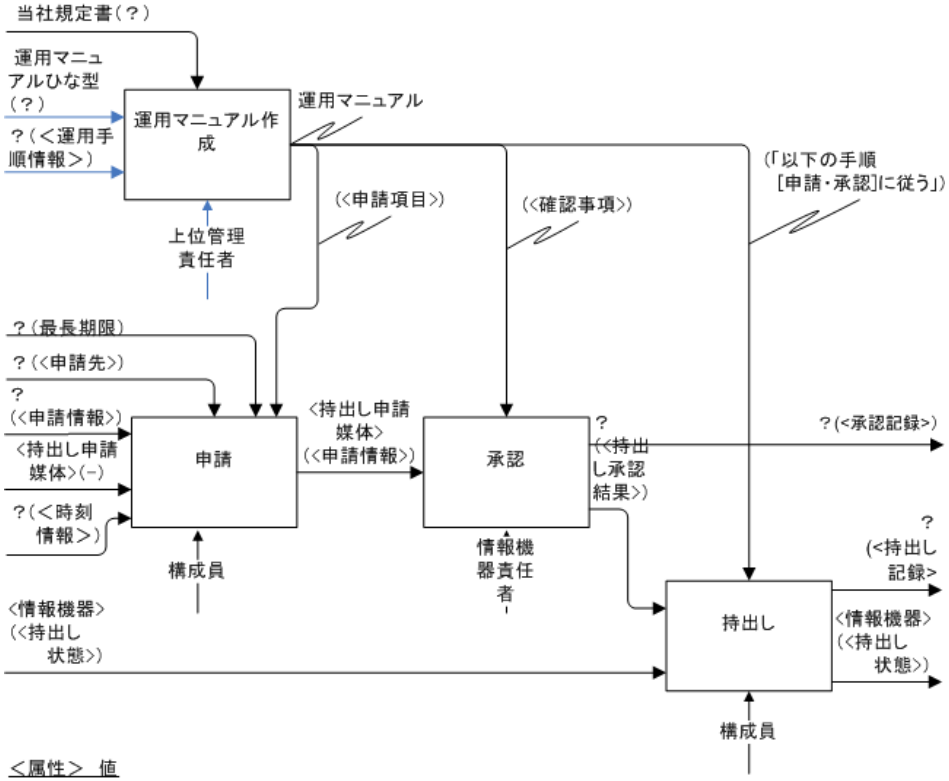

図 7　あるべき「情報機器持出し」対策（セキュリティ統制フロー定義による捕捉）

図 7 は，情報機器持出しにおける，あるべきセキュリティ対策（運用手順）を示している．この図からは，「持出し」「承認」「申請」の各アクティビティにかかる統制内容（縦軸アロー）は，すべて上位責任者によって作成された運用マニュアルに示されていることがわかる．もし，申請や承認が条件通りに行われているものかかわらず，問題が行った場合は，運用マニュアルを疑うことができる．

ここでは，セキュリティ統制評価の際に基準となる，あるべきセキュリティ対策を IDEF0 に基づいて作成する方法について述べた．IDEF0 のモデルに従って形式的に図を作成できるとともに，有識者がもつ機能定義のノウハウを形式的に蓄積し，利用することが可能になるため，誰もが同様の図を作成できると考えられる．ただし，直感的に図を作成できるが，流れを示すアローが増えてくると繁雑になる欠点はある．

5. おわりに

IDEF0 をベースにセキュリティ対策の運用手順を形式的に表す方法を提案した．正確かつ直感的に理解しやすい IDEF0 図の利用は，セキュリティ統制の実態調査や対策手順作成コンサルティングにおける説明・議論の理解度を向上することができる．

また，形式的に対策機能やプロセスを定義できることを利用して，有識者のノウハウを再利用可能にし，セキュリティ統制評価の基準となる，あるべきセキュリティ対策を導く方法を，情報機器持出し対策を例に示した．これまで評価者に依存していた基準作りを，機械的に作成することが可能になった．

今後の課題として，セキュリティ統制評価の残作業への適用，ISO27004 等で示されるセキュリティマネジメントの有効性評価との関係づけ，表記システムの自動化等があげられる．

参考文献

1) 「産業構造審議会情報セキュリティ基本問題委員会中間とりまとめ」経済産業省,2008
2) 「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」経済産業省,2005
3) FIPS 183 INTEGRATION DEFINITION FOR FUNCTION MODELING (IDEF0),1993
4) 熊谷　敏:IDEF0 モデルとその作成プロセス，経営情報学会誌， Vol.6, No.4, pp.97-100,(1998)
5) ISO9001:2008 Quality management systems – Requirement,2008
6) 阿部 昭博, 玉井 哲雄.: IDEF0 を用いたソフトウェア開発プロセスの分析 -- スケジューリングシステムへの適用 --. 経営情報学会誌, 79-98. 1999.