Vol.2011-DPS-146 No.22
Vol.2011-CSEC-52 No.22
2011/3/10

ESG モデルに基づく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††

情報セキュリティ対策を評価するための，セキュリティ統制のモデルを提案する．本モデルは，セキュリティ統制において重要な判断プロセスに着目し，判断に必要な情報の流れで，セキュリティ統制を表記するためのものである．セキュリティ対策の運用現場における統制状況の把握や暗黙的なプロセスとルールの抽出をサポートする．本報告では，モデル定義を示し，セキュリティ対策である運用手順評価へ適用した結果について述べる．

Proposal of evaluation support technique of information security measures with ESG model

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

We propose a model and notation of a security control to evaluate information security measures. This model expresses security control by information flow for security judgments. It supports clarification of present situation of security control and extraction of implicit processes and rules. In this report, our model's definition is shown, and application result of a security procedure evaluation is described.

1. はじめに

情報セキュリティガバナンス[1][2]を実現するには，セキュリティ方針を組織全体に徹底させるセキュリティ統制と評価･改善の PDCA サイクルを回すことが重要である．有効な評価・改善を行うためには，セキュリティ対策の運用においてモニタすべきポイントを明確にする必要がある．

セキュリティ統制を，あらかじめ決められたルールに従って，組織の業務を安全に遂行させることとすれば，その実施手段はセキュリティ基準や運用手順書を作成し，現場に配布することが一般的である．最近の現場でも，ここまでは徹底されるようになってきた．しかし，事件事故は無くなっていない．これまでの経験から，セキュリティ対策として作成・配布した基準や運用手順書が，現場の運用者に正しく解釈されないことが原因でないかと考えている．

間違った解釈が行われる原因の一つに，基準や運用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，その解釈の違い又は自由度が，運用上のミスを導いていると考える．このような点をもとにモニタすべきポイントを抽出する．しかし，そもそも暗黙知の抽出自体が，抽出者の経験や知識に依存してしまう点が多い．一定の評価品質を保つためには，暗黙知を明確にする又は明確にする議論をサポートするための形式的な手法の確立が必要である．

上記のような課題に対して，UML 等のモデリング手法をセキュリティに適用する先行研究がある．UMLsec[3]は，UML の記法を拡張し，独自にプロファイルを追加して，情報システムにおけるセキュリティ仕様を表現するものである．定義されたモデル要素を使って，形式的にセキュリティ対策を表現することができる点では，暗黙知の検出にも利用可能である．しかし，UMLsec はシステム構築における表記法であり，運用手順のようなフローの表記には適していない．

本稿では，これまでに提案した IDEF0 を用いたセキュリティ統制の表現手法[4]を改良し，より厳密なモデル定義を行うことで暗黙知を引き出す手法を提案する．本手法は，基準や承認結果といったセキュリティ統制上重要な情報の取り扱いに着目している．これを Enterprise Security Governance モデル（以下，ESG モデル）として定義し，ESG モデルを用いてセキュリティ運用手順を評価するための手法について述べる．

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

Vol.2011-DPS-146 No.22
Vol.2011-CSEC-52 No.22
2011/3/10

2. セキュリティ統制の表記

筆者らは，機能モデリング技術である IDEF0 を用いてセキュリティ運用手順書を形式的に表現することで，セキュリティ統制に係る情報（ルールや承認結果等）の流れを明確にする手法を提案している．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[5]であり，米国連邦情報処理標準(FIPS183)となっている．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（図 1）．

セキュリティへの適用に関しては，セキュリティの運用手順（図 2）がルールとプロセスにより構成されていることに着目し，プロセスを機能，ルールを制約と IDEF0 の要素に対応させた．モデルの要素に沿って運用手順から情報を抽出し，現場でのヒアリング結果を追記することで現状の姿の表現した（図 3）．プロセスとルールのつながりを，セキュリティ統制に関する情報の流れとして俯瞰できている．この図から出生が明確でない制約情報は，定義のないルールと見なされ，現場の運用者が独自に判断しているプロセスの存在が明確になった．また，制約と出力の関係をモニタするポイントとすることで，運用が正しく行われていること，ひいては統制が正しく行われていることを評価した．社内検証を通じて，未定義のルールを検出でき，人為的に設定したモニタすべきポイントの漏れを見つけることはできた．

しかし，この手法では暗黙知のような手順に載っていない新しい気づきを抽出することはできなかった．これは，比較的容易に運等手順書をモデルに従って置き換えることができ，手順書の表現においてそれ以上の暗黙知を引き出す必要がなかったためである.セキュリティ統制を表記するための,より厳密なモデル定義が必要と考える.

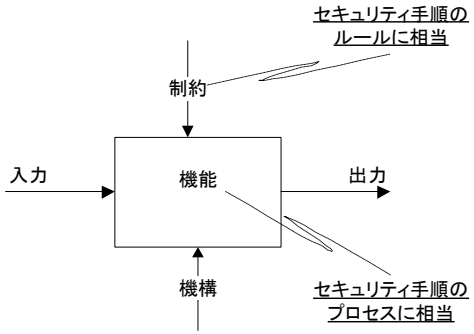

図 1　IDEF0 表記法

情報機器の持出し
業務担当者は、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こと。
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　・セキュリティパッチ適用状況
・機密情報の有無・内容　・持出し期間　・持出し機器識別番号
b　情報機器の責任者の承認を得ること。

図 2　情報セキュリティ対策　運用手順（例）

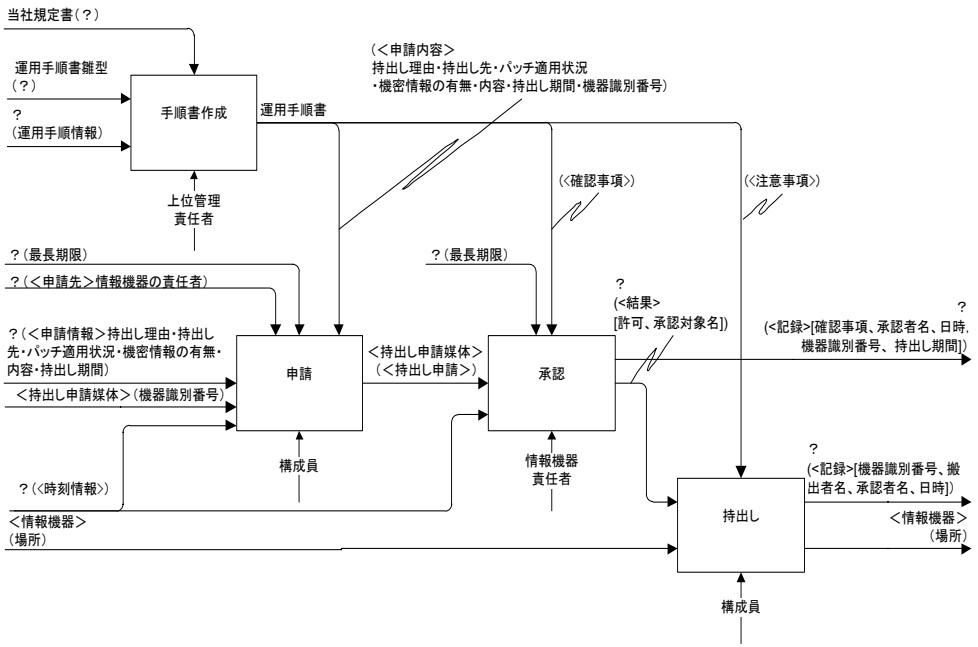

図 3　情報機器の持出し手順の IDEF0 表記例

Vol.2011-DPS-146 No.22
Vol.2011-CSEC-52 No.22
2011/3/10

3. ESG モデル

これまでに提案した IDEF0 表記法に基づくモデルを ESG 基本モデルとする（図 4）．IDEF0 では，機能に対する制約は Box の上側から入力する矢印で表されるが，ESG 基本モデルでは，制約を入力情報に含め，機能の動作に対して入力が同期か非同期かを表すことにしている．例えば，情報機器の持出しにおいて，持出毎に許可を得るのか，１回承認を得られれば持出回数依存せず許可が有られるのかを区別して表現することができるようにするためである．また，Data store は IDEF0 には無く本稿にて新たに追加したもので，情報が明に定義されていることを示すものである．これは視覚的なわかりやすさの向上のためである．この基本モデルを用いて，セキュリティ統制を表現するための定義を示す．

3.1 モデル定義

セキュリティ統制を，あらかじめ決められたルールに従って組織の業務を安全に遂行させることとする．この視点で現場でのセキュリティ運用を見れば，どのような情報をもとに判断（judge）を行っているのかを明らかにすることが重要となる．また，正確な判断を行うためには，判断に必要な入力情報がどのように作成(make)されたのか，異なる主体(actor)間における正確な情報の伝達を行うためには，判断に必要な情報がどのように伝達(transfer)されたのかが重要となる．セキュリティの視点からは，作成と伝達は判断のための情報が毀損する可能性が高いポイントとも言える．このような考え方により，セキュリティ統制の表現を定義した（表 1）（図 5）．

表 1　ESG モデル Activity 定義

judge	入力された情報がルールに一致したかどうかの結果と理由を出力する
make	入力された情報からルールに一致した情報を出力する
transfer	入力された情報をルールに従った方式で送受信する

judge は入力された 1 つ以上の情報と判断ルールに基づき判断した結果と理由を出力する Activity である，結果は OK,NG の 2 値とした．また，入力された情報は変更を受けることなく出力されるとしている．一般的には，承認等で判断がされれば，出力情報として承認結果のみが出力されるとすることが多い．しかし，ESG モデルでは，判断に使われるルールと，判断で得られた情報を承認結果として構成するルールを明確にするため，このような定義を行った．

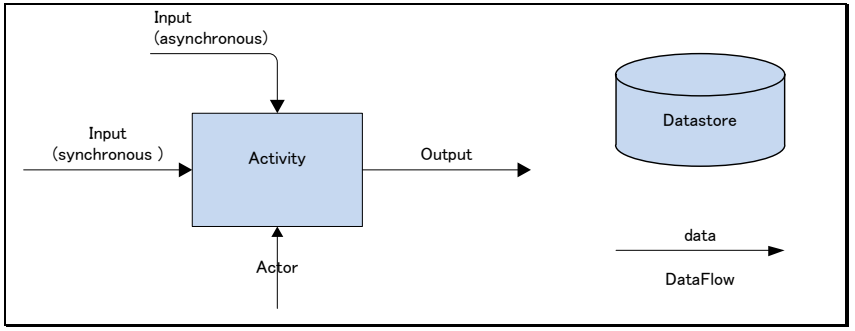

図 4 ESG 基本モデル

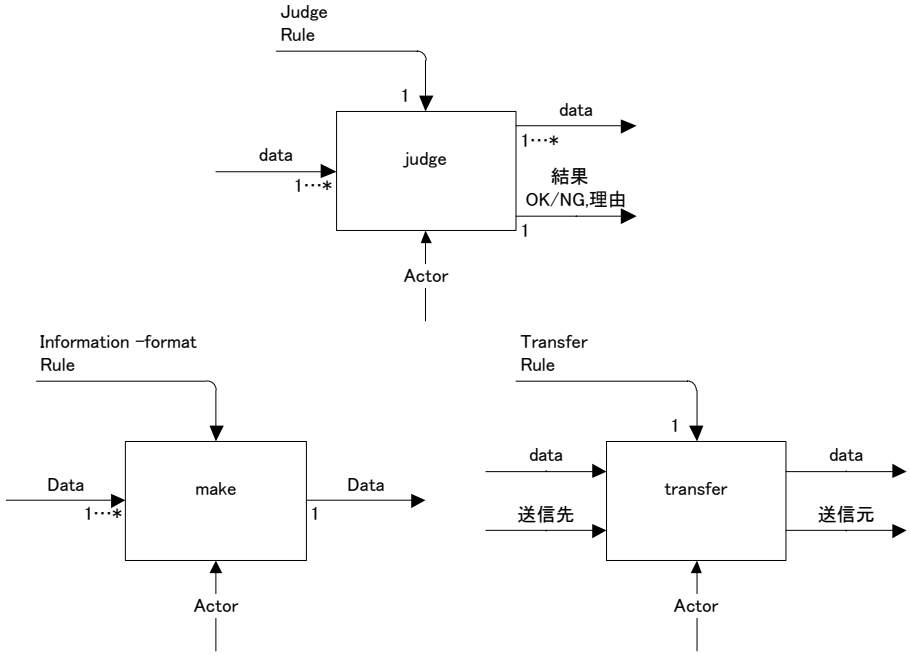

図 5 ESG モデル activity 定義

Vol.2011-DPS-146 No.22
Vol.2011-CSEC-52 No.22
2011/3/10

3.2 フロー表記ルール

ESG モデルの 3 つの activity で，判断に係る情報の流れを表現したものを ESG フローする．ESG フロー作成において考慮した表記ルールを定義した（図 6）．表記ルールも基本的に IDEF0 に基づいているが，分岐(branch)とループ(loop)については追加した．その他，基本モデルとして追加した date store に関するルールも追加している．

IDEF0 のルール上，機能が動作するタイミングは，入力と制約の情報が全て揃った時である．ESG モデルでも同様とすれば，分岐(branch)で書かれたルートＡまたはＢは，ＡとＢが同時に存在しなければ，それ以降の activity は一つのルートでしか動作しないことになる．ループ(loop)についても同様である．また，ループ(loop)によって戻る activity は自身でなくても良いとしている．

IDEF0 との大きな差分である分岐とループを追加した理由について述べる．従来の IDEF0 には分岐とループがないため，判断に係る情報の流れ（データフロー）を作成すると，手順上の一つのルートについてトレースした結果を示すフローになる．通常，セキュリティ運用では複数のルートを想定するため，フローが大量になる恐れがある．フローは，後述する暗黙知を明確にする又は明確にする議論を人が行う際の情報となるため，単純化することを優先した．その他のルールの追加も，視覚的なわかりやすさの向上を目的としている．

上記ルールに従って情報機器持出し手順（図 2,図 3）の ESG フローを作成した（図 7）．実際の運用手順との関係が明確になるように各 activity には「申請情報作成」等のラベルを付けている．またセキュリティ統制の対象となるプロセスを統制プロセスとして ESG モデルに基づくフローで表し，統制によって保護される対象を業務プロセスとして統制フローとの関係を示している．業務プロセスにおいては，ESG モデル適用外としている．

3.3 アンチパターンによるフロー表記の補完

ESG フロー作成において定義していない要素を用いることはできないが，generate というセキュリティ統制として認められないモデル定義や表記ルール（アンチパターン）を追加している．generate は make の特殊な場合で，入力がない状態で情報を作成していることを意味する．また，データフローを示す矢印(arrow)の始点がつながれていないオープンな状態を許容している．これは判断に係る情報の発生源が定義されていないことを意味する．

アンチパターンを追加した理由について述べる．ESG モデルに厳密にしたがって ESG フローを作成すると，判断に係る情報のデータフローが表記できなくなる場合がある．例えば，ヒアリングの結果，判断に必要な情報が運用者の思い付きであった場合は，入力すら存在しないため表記できない．この状態はセキュリティが統制されていない状態を示すため，モデルによる表記としては正しい．しかし，後の議論を効率的に行うには，フロー全体が記述できたほうが良い．このためアンチパターンを定義し，あとの議論で確認すべき点を示した．

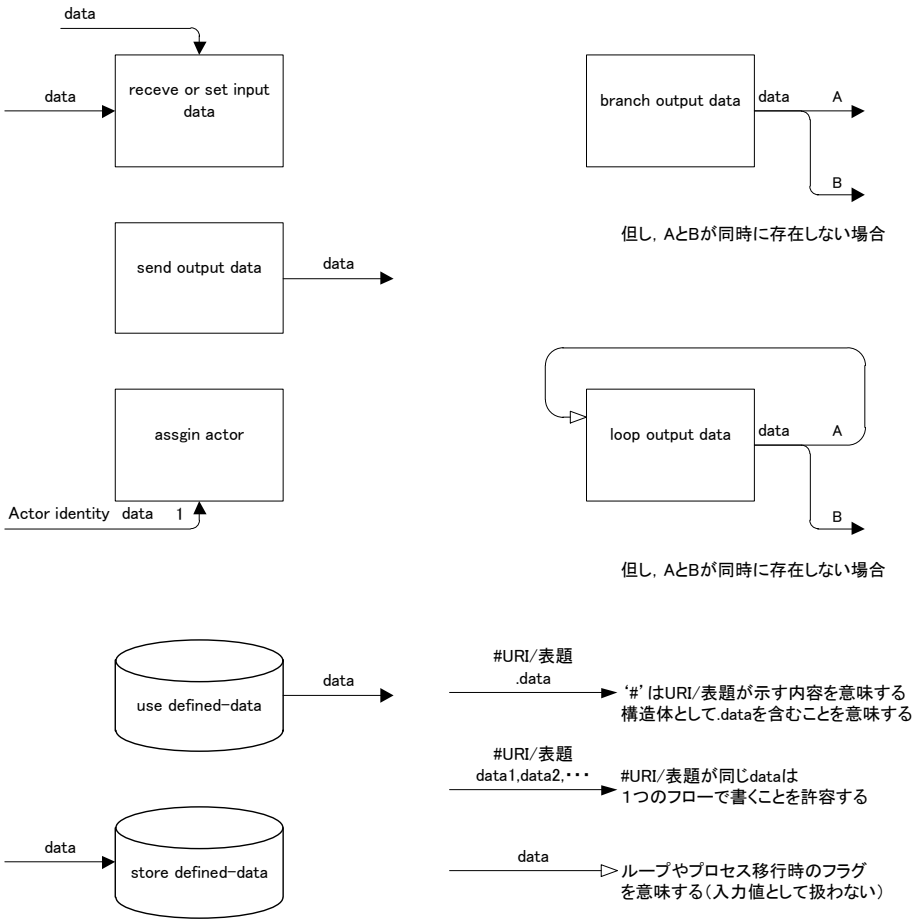

図 6　ESG フロー表記ルール

Vol.2011-DPS-146 No.22
Vol.2011-CSEC-52 No.22
2011/3/10

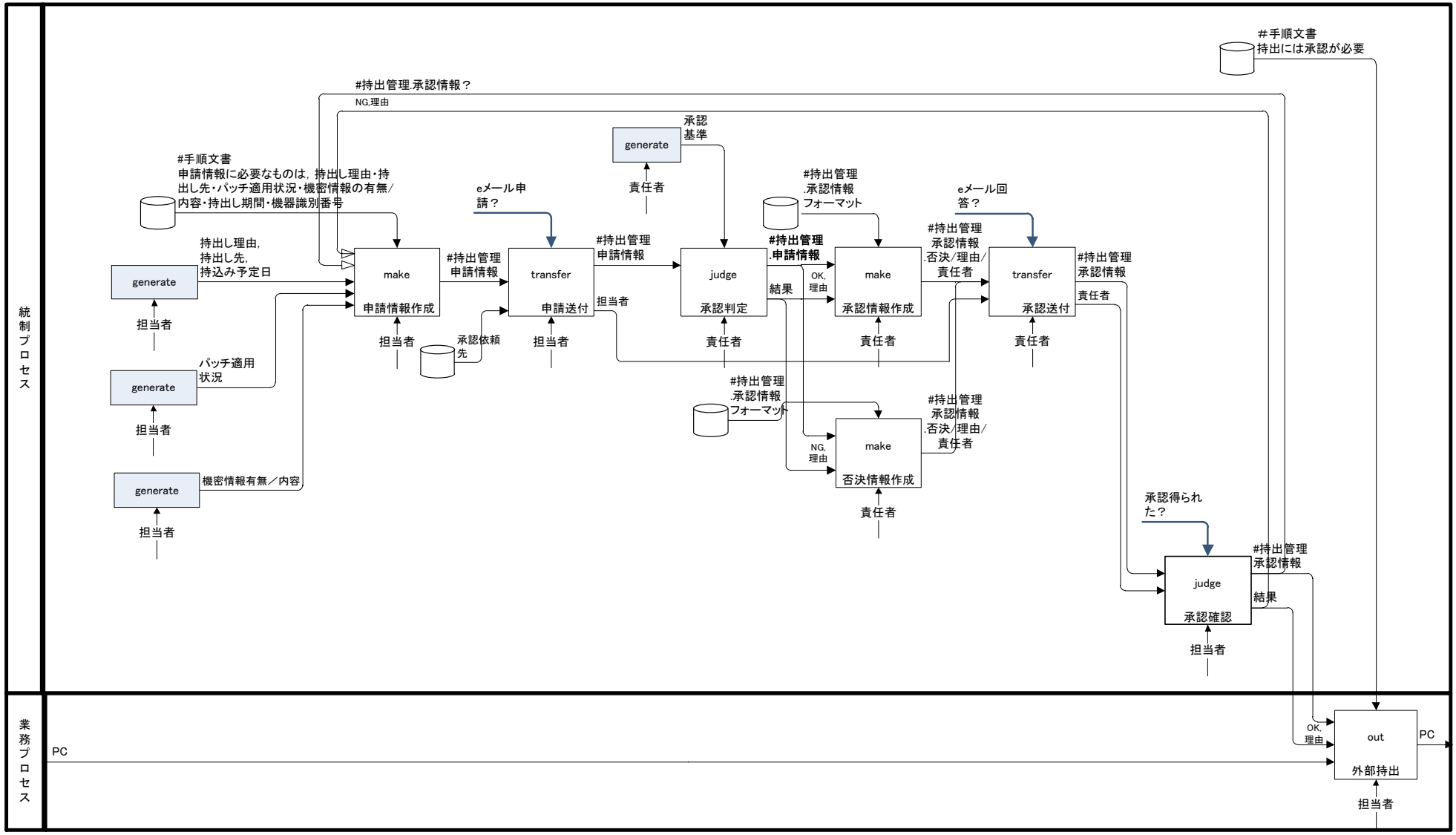

図 7 「情報機器の持出し」手順の ESG フロー

Vol.2011-DPS-146 No.22
Vol.2011-CSEC-52 No.22
2011/3/10

4. セキュリティ運用手順評価への ESG モデル適用

4.1 ESG モデルに基づく暗黙知の抽出

課題に対して提案した ESG モデルの効果について述べる. セキュリティ統制上の脆弱性となりうる暗黙知の抽出を目的として ESG モデルを定義した. 暗黙知とは手順書に明確に示されていない動作・情報を意味する．ESG フロー作成時または作成後に，主に次の視点で暗黙知を抽出する．

- 視点１　アンチパターン（generate,オープンな情報フロー等）
- 視点２　データ不整合（利用が明確でない情報等）

視点１のアンチパターンに着目した抽出は 3.3 節で述べた通り，手順書では明確でない未定義のプロセスとルールを表している. 視点２のデータ整合に着目した抽出は，主にルールとして示された情報に対して，入力として示された情報が明確に利用可能な状態でなければ，利用可能になるための暗黙的な動作があることがわかる．また，あるプロセスの出力が次のプロセスの入力になっている場合，あらゆる出力の要素が次の入力で使われていなければ，データを判別する動作があることがわかる．最終的に，暗黙的な動作の内容については，議論して抽出する．

具体的に,「情報機器の持出し」手順の ESG フロー(図 7)から抽出した暗黙知の例を示す（表 2）.

表 2　「情報機器の持出し」手順における暗黙知（例）

①	不整合	承認取得後の承認確認は担当者が実施している
②	generate	申請書作成時の全入力情報は担当者が独自に作成している
③	generate	承認判定時の常任基準は承認者が独自に作成している
④	不整合	承認確認 NG 時のループで戻る承認（否決）情報は,申請情報作成において利用が明確でない

①に示した「承認確認」は ESG フロー作成時に追記したものである．これは，最終的な「外部持出」の入力の一つが承認 OK であることに対して，承認送付で出力された「#持出管理.承認情報」には OK/NG の二つの要素がある．この点をデータ不整合として，判別する動作が存在するため追加したものである．

また，④に示した承認確認 NG 時のループにおける「#持出管理.承認情報」は，ESG フロー作成後に補足として運用者にヒアリングして追記したものである．ここではループとして「申請情報作成」に戻るが，申請情報として必要なものには含まれていない．この点をデータ不整合として，暗黙的な動作があること又は不要な情報であることがわかる．

4.2 セキュリティ運用手順評価

ESG フローにより得られた暗黙知の利用例として，セキュリティ運用手順評価について述べる． 運用手順より暗黙知として検出した項目は，セキュリティ対策の運用ミスの原因となりうるものである．特に，セキュリティ対策の運用者に判断が任されているルールがあることは，セキュリティ統制上の弱点として指摘できる．さらに，データ不整合のうち不要な情報の存在は，運用手順上の無駄な動作を引き起こす可能性があり，作業効率上の弱点として指摘できる．特に，インシデント管理等における迅速な作業が必要なものにおいては，重要な評価となる．

図 2 で示した「情報機器の持出し」手順は多くの要素が未定義であり，かつ承認が否決された場合の手順は示されていない．現場での運用において補足されていることが分かり，セキュリティ統制としては不適切な状態であると評価する．

5. おわりに

セキュリティ統制を形式的に表す方法として ESG モデルを提案した. セキュリティ統制の実態調査や運用評価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．これまでの IDEF0 に基づく表記に比べ，暗黙的に行われているプロセスやルールを抽出することが容易にできるようになっている．また，適切な運用手順の改善や運用におけるセキュリティ統制のモニタリングポイント抽出ができる．

本モデルは社内適用にて検証を行っている．今後，本モデルにより導かれた暗黙知に基づく評価と，ノウハウに基づく評価の比較を行う予定である．課題として，データ整合性やデータフローの形式検証の自動化があげられる．

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) Jürjens, Secure Systems Development with UML, 1 ed. Springer, 2005.
4) 谷口,金谷,鈴木,奥原：IDEF0 を用いた情報セキュリティ対策の評価支援,CSEC50,2010
5) FIPS 183 INTEGRATION DEFINITION FOR FUNCTION MODELING (IDEF0),1993