社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（67）
2005－CSEC－28（67）
2005／3／23

セキュリティソリューション提案支援ツールの開発

伊川 宏美　　安細 康介　　永井 康彦

株式会社 日立製作所 システム開発研究所

〒212-8567 川崎市幸区鹿島田 890

E-mail:　{igawa, an, y-nagai}@sdl.hitachi.co.jp

あらまし　情報システムが社会や企業活動の基盤となってきており，これに伴い，情報システムに対してセキュリティポリシーを策定し，それに基づいたセキュリティ対策の実施や監査・診断を継続的に行うことが重要となってきている．しかしながら，ポリシー策定や監査・診断により対策が不足している点を特定しても，これを実現・解決する手段となるセキュリティソリューションの選択は SE やコンサルタントの経験やノウハウに依存しているのが現状である．また，多種多様なソリューションの中から対象情報システムにコスト対効果の高いものを選択することは困難となっている．そこで本稿では，経験やノウハウの少ないSEやコンサルタントでもコスト効果の高い最適なセキュリティソリューションを提案することができるツールを検討し，開発を行ったので報告する．

キーワード　セキュリティソリューション，セキュリティ診断，セキュリティ対策，最適化，情報セキュリティ

Development of a Support Tool for Selection of Security Solutions

Hiromi IGAWA　Kousuke ANZAI　Yasuhiko NAGAI

Systems Development Laboratory, Hitachi, Ltd.

890 Kashimada, Saiwai-ku, Kawasaki, 212-8567 Japan

E-mail:　{igawa, an, y-nagai}@sdl.hitachi.co.jp

Abstract　Information systems are playing a growing roll in all aspects of social and business activities. Along with it, not only making security policies, it has become important to enforce security countermeasure and audit continually to information system. However, it is difficult to select the cost-effective solutions to solve the lack of security countermeasure. And, SE/consultant now determines that solution based on their experiences or knowledge. In this paper, we propose a support tool for selection of security solutions. By using this tool, system engineers can select cost-effective solutions for security countermeasures.

Keyword　Security Solution, Security Audit, Security Countermeasure, Optimization, Information Security

1.　はじめに

情報システムが社会，企業活動の基盤となってきており，これに伴い，情報システムに対してセキュリティポリシーを策定し，それに基づくセキュリティ対策の実施や監査・診断を継続的に行うことが重要となってきている．このことは，ISMS（情報セキュリティマネジメントシステム）認証[1]や，プライバシーマーク認証[2]等の認証取得を目指す組織が増加してきたことにも現れている．

また，セキュリティポリシーの策定や，セキュリティ監査・診断の作業を支援する支援ツールが提案されている[3][4]．これらは，セキュリティ対策の国際標準や業界標準をポリシー構成部品や監査・診断の評価チェックシートとして用い，ポリシー作成の効率化や品質向上，セキュリティ対策の不足点の評価を行うものである．

しかし，これらの支援ツールはセキュリティポリシーの作成や，現状のセキュリティ対策状況の分析と対策不足点の提示を支援するにとどまるものであり，対策不足点に対して具体的な実現手段の選択を支援するものではなく，これらの実現手段の選択は SE やコンサルタントの経験やノウハウに依存しているのが現状である．このため，特に経験やノウハウの少ない SE やコンサルタントでは，実現手段となる多種多様な製品/サービス/ソリューション（製品/サービスの組合せ）からコスト対効果の高いものを選択することは困難な作業となっている．

そこで，報告者らは，対象情報システムの策定したポリシーに対して，あるいは現状のセキュリティ対策状況の改善のためにコスト対効果の観点から最適なソリューションを選択し，さらに，選択したソリューションを提案する際には，そのソリューションを実施することによる対策効果も示せることが必要・有効であることから，そのソリューションを実施することによる対策効果を示すことを特徴とするセキュリティソリューションの選択・効果表示方法と，その方法に基づく支援ツールを開発した．本支援ツールを用いることにより，経験やノウハウの少ない SE やコンサルタントでもコスト対効果の高いソリューションを提案することが可能となる．

2. 最適セキュリティソリューション選択・対策効果表示方法の要件

本章では，1章で挙げた課題を解決する最適セキュリティソリューションの選択方法と，対策効果表示方法の要件について述べる．

2.1. 最適セキュリティソリューション選択方法の要件

報告者らは，これまでに，セキュリティポリシーに対してコスト対効果の高い最適な実現手段の組合せを選択する方法[5]を提案している．これはセキュリティポリシーの重要度と，ポリシーと実現手段候補との関連度，実現手段候補の満足度を各々ファジイ集合として定義し，これらのファジィ合成演算により計算される機能過不足度を目標関数とする最適化問題を解くことで，コスト対効果の高い最適な実現手段を決定するものである．本ソリューション選定問題に対しても，基本的にこの既提案方法を採用している．

しかしながら，既提案方法は，実現手段候補間が独立な場合に利用できるものであり，ソリューション/製品/サービス個々をそのまま実現手段候補として適用しようとすると，ソリューション/製品/サービス間には，ソリューションには製品やサービスが含まれかつある製品やサービスは複数のソリューションの構成要素となっているなどの包含関係や依存関係があることから，そのままでは利用できない．

そこで，本最適セキュリティソリューション選択方法としては，ソリューション/製品/サービス間の対応関係を明確化し，これらの包含関係や依存関係を考慮して対象情報システムに最適なソリューションや製品/サービスを選択できることを1つ目の要件（1-1）としている．

また，対象情報システムに対するセキュリティ対策は適切な順序で継続的に行っていくことが必要である．このため，選択した最適なソリューションの実施順序を明らかにすることを2つ目の要件（1-2）としている．

2.2. 対策効果表示方法の要件

対策効果の表示方法としては，まずは選択された最適セキュリティソリューションや製品/サービスによって対象情報システムのセキュリティポリシー個々がどの程度達成できるかの達成状況を表示できることが選択手段による効果を把握するために必要である．次に，効果的にセキュリティ対策を実施するようガイダンスするために，重要度の高いセキュリティポリシーに対応するソリューションを優先表示することが有効である．さらに，その中でも対策効果の高いセキュリティポリシー，すなわち現状のセキュリティ対策の達成状況と，提案するソリューション実施後のセキュリティ対策の達成状況との差が大きいセキュリティポリシーに対応するソリューションの順や各ソリューションが適用されるセキュリティ管理サイクルの位置づけからその実施順序を考

慮してソリューションを優先順位付け表示することが有効と考える.

そこで, 上記の観点で, 各セキュリティポリシーに対する現状のセキュリティ対策の達成状況(以下, 現状達成度;全て新規対策の場合は値が0)と, 提案するソリューションを実施することによるセキュリティ対策の達成状況(以下, 改善達成度)を用いて, そのソリューションを実施することによる対策効果を表示できることを1つ目の要件(2-1)としている. さらに, 効果的なソリューション実施順序のガイダンスとしてソリューションを優先順位付け表示できることを2つ目の要件(2-2)としている.

3. 最適セキュリティソリューション選択・対策効果表示方法

本章では, 2章で検討したそれぞれの課題を解決するための要件を実現するための方法について述べる. 実現すべき方法は以下の2つである.

(1)最適セキュリティソリューション選択方法

(2)対策効果表示方法

3.1. 最適ソリューション選択方法

要件(1-1)は, ソリューションは一般に製品/サービスの組合せを構成要素として構成されることから, 選択候補製品/サービスと選択候補ソリューションとの対応関係付けを行い, まずポリシーに対する直接的な実現手段となる最適な製品/サービスの組合せを選択し, 次に製品/サービスとソリューションとの対応関係に基づき, 選択された製品/サービスで構成可能となるソリューションを特定することで実現する.

ソリューションの構成要素となる製品/サービスとソリューションの対応関係付けのイメージを図 3-1(a)に示す. この図では, それぞれを結んだ線は対応関係があることを意味している.

ここで, 図の製品 B とサービス B のように製品がサービスの前提になっているものもありうる. これは製品とサービスに依存関係があり, 両方のセットでセキュリティ対策となるものがあるからである. 他の製品/サービスについては全て単体で効果があるものとなる.

そして, 現状導入済み製品/サービスがある場合はその満足度と, 導入済み製品/サービスとセキュリティポリシーの関連度と, セキュリティポリシーの重要度を用いて, ファジィ演算に基づいて導入済み製品/サービスによるポリシーの現状達成度を計算する[5]. これは従来の監査/診断支援ツール[4]が提供している GAP 分析に相当するものである.

次に, 現状達成度の改善や新規対策のために選択候補となる製品/サービスの満足度と, 選択候補の製品/サービスとセキュリティポリシーの関連度と, セキュリティポリシーの重要度を用いて, 投資可能コストを制約条件とし, ファジィ演算に基づいて最適製品/サービスの組合せを選択する[5].

最後に, 最適製品/サービスについて, 製品/サービスとソリューションの対応関係を用いて, 選択された製品/サービスを各ソリューションに特定し, 選択する最適ソリューションを決定する.

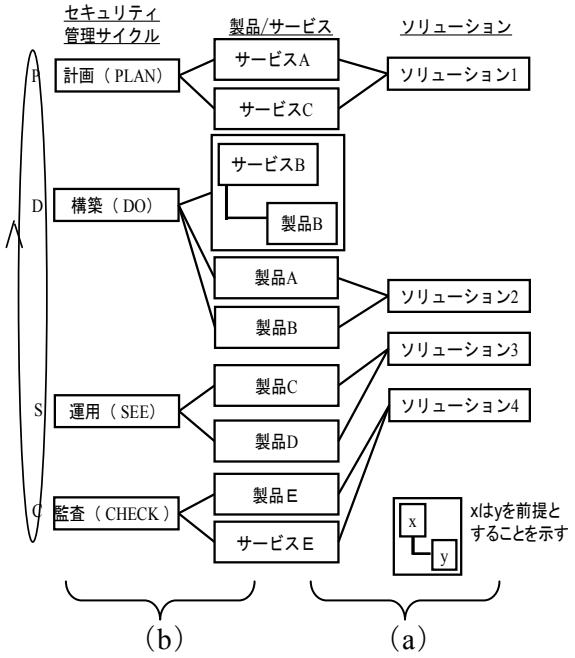

図 3-1 製品/サービスと PDSC との対応関係

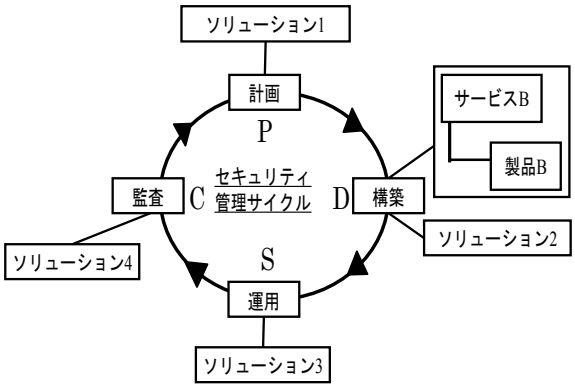

図 3-2 ソリューションと PDSC との対応関係

次に，要件(1-2)については，実施順序付けが可能な基準で製品/サービスとソリューションを分類しておき，最適なソリューションの選択後にその基準を用いて，選択したソリューションや製品/サービスの実施順序付けをすることで実現する．そして，その実施順序付けをするための基準としては，セキュリティ管理サイクル PDSC の分類が適当と考え，適用している．すなわち，計画フェーズ(PLAN)，構築フェーズ(DO)，運用フェーズ(SEE)と監査フェーズ(CHECK)の各フェーズに，製品/サービス/ソリューションを関係付けることとした．図 3-1(b)に製品/サービスと PDSC との対応関係のイメージ図を示す． また，図 3-2 に製品/サービス/ソリューションと PDSC との対応関係のイメージ図を示す．各ソリューションは，ソリューションを構成する製品/サービスがそれぞれ対応する PDSC のフェーズにより対応付けられる．

これらの対応関係と PDSC の実施順序に基づいて，最適なソリューションの選択後，各ソリューションを PDSC の各フェーズに特定し，PDSC の実施順序に基づいて選択したソリューションの実施順序を決定する．

3.2. 対策効果表示方法

要件(2-1)については，セキュリティポリシー個々について，現状達成度と，改善達成度と，重要度を表示することで実現する．

要件(2-2)については，まず、重要度と現状達成度の差分がプラスとなるポリシー(セキュリティ対策が不足しているポリシー)を抽出し，現状達成度と改善達成度を，下記の観点でグラフに示すことで実現する．

(1) 重要度の高いセキュリティポリシーに対応するソリューションを優先表示

セキュリティポリシーを重要度の高さにより並び替え，各セキュリティポリシーの重要度，現状達成度，および改善達成度を表す．これにより，重要度の高いセキュリティポリシーの順に対策効果を示すことができる．

(2) 対策効果の高いセキュリティポリシーに対応するソリューションを優先表示

まず，各セキュリティポリシーにおける現状達成度と改善達成度の差分を計算する．次に，(1)の手段で並び替えた結果，重要度が同じであったセキュリティポリシーを，計算した差分の大きさにより並び替え，重要度，現状達成度，および改善達成度を表す．これにより，重要度毎に，対策効果の高いセキュリティポリシーの順に対策効果を示すことができる．

(3) 実施順序を考慮してソリューションを優先順位付け表示

ソリューションと PDSC との対応関係より，各セキュリティポリシーを対策するソリューションがそれぞれ対応する PDSC の位置づけがわかるため，(1)(2)の手段で並び替えた結果，重要度が同じであったセキュリティポリシーを，ソリューションの PDSC の順に並び替え，重要度，現状達成度，および改善達成度を表す．これにより，実施順序を考慮してソリューションを優先順位付け表示することができる．

4. ツールの開発結果

本章では，3章で検討した最適セキュリティソリューション選択方法と，対策効果表示方法，を適用した支援ツールの開発結果について述べる．

4.1. ツールの機能構成

本支援ツールの機能構成を図 4-1 に示す．本支援ツールは，情報システムに対して策定したセキュリティポリシーと，最適な製品/サービスの組合せの選択に用いる

製品/サービスの候補とその満足度等のデータを格納したポリシー(本開発では、ISMS 基準を利用)/製品/サービス情報 DB と，ソリューションの候補と製品/サービスとソリューションの対応関係データや製品/サービスと PDSC との対応関係のデータを格納したソリューション情報 DB を参照して，対象情報システムに対するセキュリティポリシーの重要度，対象情報システムに導入済みの製品/サービス，セキュリティ対策に投資可能なコストを入力すると，入力データを受け付ける入力データ処理機能，GAP 分析機能，最適ソリューション選択機能，対策効果を表示する対策効果表示機能によって，最適なソリューションの一覧表とソリューションを実施することによる対策効果を示したグラフを出力するものである．

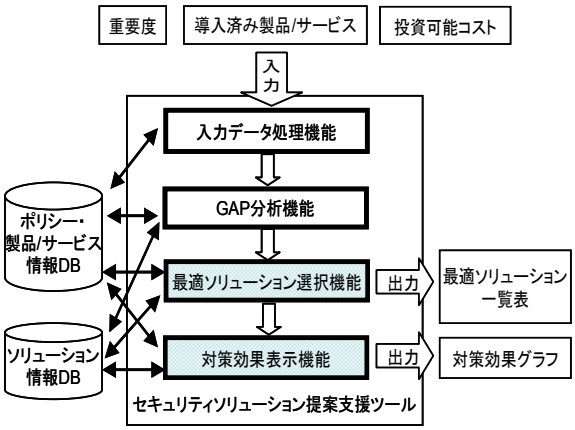

図 4-1 本支援ツールの機能構成

4.2. ツールの機能概要

(1) 入力データ処理機能

対象情報システムにおけるセキュリティポリシーの重要度と，セキュリティ対策に投資可能なコストを入力し，さらに対象情報システムにセキュリティ対策として既に導入している製品/サービスがある場合にはそれらも入力するための機能である．

(2) GAP 分析機能

対象情報システムに導入済みの製品/サービス情報について，ポリシー/製品/サービス情報 DB に格納した各製品/サービスの満足度，コスト，セキュリティポリシーとの関連度のデータを用いて，重要度に対する現状達成度を計算する機能である．既に導入している製品/サービスがない新規対策の場合は，ポリシーに対する現状達成度を全て0に設定する．

(3) 最適ソリューション選択機能

ポリシー/製品/サービス情報 DB に登録されている選択可能製品/サービス(既に導入している製品/サービスは選択必須)について，同様の情報と重要度を用いて，最適な製品/サービスの組合せと，その組合せによる改善達成度を計算する．次に，選択した最適製品/サービスの組合せについて，ソリューション情報 DB の製品/サービスとソリューションとの対応関係データを検索することで，最適ソリューションを選択する機能である．選択したソリューションを表示した画面例を図 4-2 に示す．新たに必要となる最適ソリューションの組合せ(製品/サービス/ソリューション)と，そのソリューションの実施に必要なコスト，ソリューションに含まれる製品/サービスが一覧表で示される．なお，網がけ部分は現状導入済製品/サービスを示している．

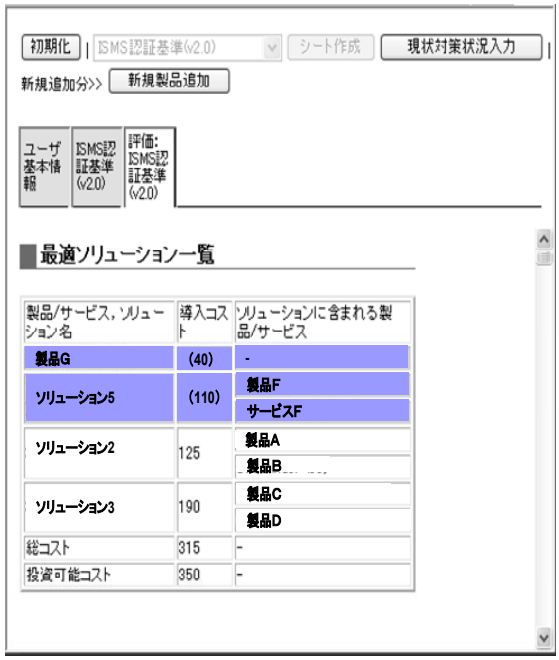

図 4-2 最適ソリューション出力例

最後に，ソリューション情報 DB のソリューションとセキュリティ管理サイクルとの対

応関係データを検索することで，ソリューションの実施順序を決定する．

(4)対策効果表示機能

本機能は，最適なソリューション選択後，そのソリューションを実施することによる対策効果を示す機能である．

最適なソリューション決定後，各セキュリティポリシーについて重要度，現状達成度，改善達成度を示したグラフを表示する(図 4-3 左)．このグラフにより，選択された最適ソリューションによって対象情報システムのセキュリティポリシー個々がどの程度達成できるかの達成状況を表示することができる．

また，この画面上のボタンを切り替えることにより，対策不足のポリシーを抽出し，それらを重要度の高い順，対策効果の高い順，対策順序に基づいた対策効果を示したグラフに表示を切り替えることができる．例えば，図 4-3 左のグラフにおいて，重要度の高低でグラフを表示するボタンを押下した場合，重要度の高いセキュリティポリシーに対応するソリューションを優先表示したグラフ(図 4-3 右)が画面に表示される．これにより，対策不足のポリシーに対して，効果的な実施順序となるソリューションを提示することができる．

5. まとめ

本稿では，経験やノウハウの少ない SE やコンサルタントでもコスト効果の高いソリューションを提案することを支援するための技術として，最適セキュリティソリューション選択・対策効果表示方法を提案し，その方法を適用した支援ツールの開発結果について報告した．

本方法は，対象情報システムの現状のセキュリティ対策不足点に対してコスト対効果の観点から最適なソリューションを選択し，さらに，選択したソリューションを実施することによる対策効果を示すことを特徴としている．

今後は，本支援ツールを事例適用することにより，ツールの有効性の検証と改良を行っていく予定である．

文　献

[1] JIPDEC:情報セキュリティマネジメントシステム(ISMS)合性評価制度．http://www.isms.jipdec.or.jp

[2] JIPDEC:プライバシーマーク制度 http://privacymark.jp/

[3] 諸橋政幸，藤山達也，永井康彦:適応型セキュリティポリシー作成支援ツールの開発，情報処理学会 コンピュータセキュリティ(CSEC)研究会(2002)

[4] http://www.asgent.co.jp/

[5] 永井康彦，藤山達也，荒井正人，柚原直弘:機能的適合性を考慮した情報システムのセキュリティ基本設計法の提案，情報処理学会論文誌，Vol.45， No.4，pp.1163-1175(2004)

図 4-3 対策効果の結果表示グラフ例