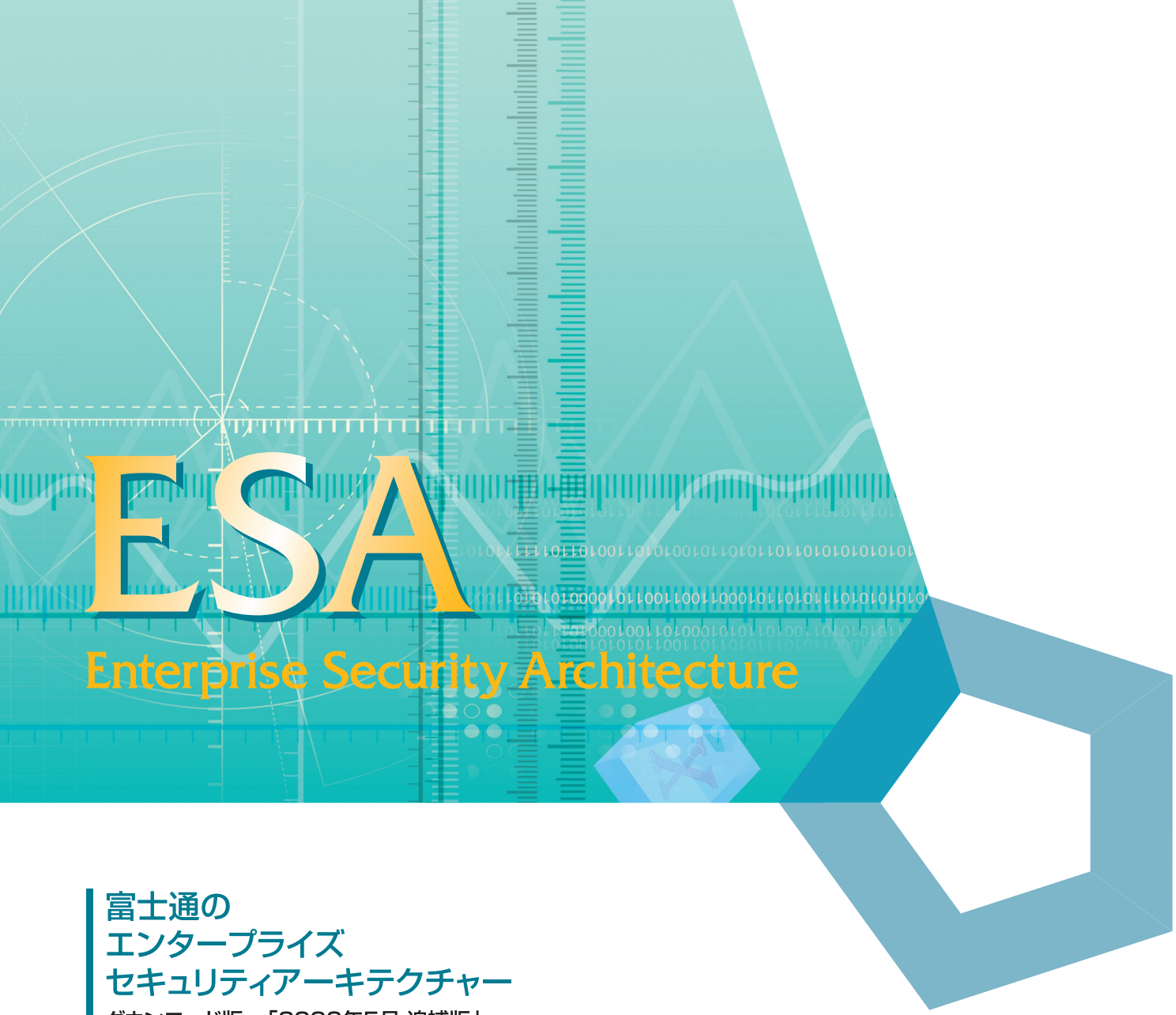

富士通の
エンタープライズ
セキュリティアーキテクチャー

ダウンロード版　「2009年5月 追補版」

富士通株式会社
情報セキュリティセンター

1. セキュリティダッシュボード構築のポイント

「富士通のエンタープライズセキュリティアーキテクチャー」(以下、ESA と呼ぶ)の 18 章では、セキュリティ評価指標とセキュリティダッシュボードについて、以下の観点から基本的な考え方を説明しました。

- セキュリティダッシュボードの利用者
- ダッシュボードへの入力情報
- セキュリティ評価指標の決定
- セキュリティダッシュボードの設計～実装
- セキュリティダッシュボードの将来像

本章では、当社での社内実践を踏まえ、セキュリティダッシュボードの設計～実装を行う上でのポイントを説明します。

1.1 データの収集

対象となるデータは syslog やアプリケーションログなどのファイル形式のデータだけでなく、データベースに格納されている場合も考えられます。従って、データコレクタには、syslog プロトコルやファイル転送機能(ftp など)の他に、ODBC などのデータベースインターフェースの実装が必要になる場合があります。また、測定が自動化されておらず、自動的に収集できないデータに対しては、データ入力システムを用意する必要があります。例えば、Web ベースでの入力インターフェースを実装し、定型化されたフォームに入力を行うことで、過不足なく必要な情報のみをデータ化することができます。

情報セキュリティに関する活動は一般的に組織活動の一環として実施されるため、セキュリティダッシュボードの表示内容も必然的にこれら組織ごとに集計、分析されるケースが多くなります。さらに、ESA の 18.1 節で説明したダッシュボードの利用者によっては、これら組織を束ねた、より上位の組織ごとに集計、分析が必要となる場合もあります。このため、集約する各データには以下のような項目が含まれるべきです。

- 組織を一意に識別するための情報(組織コード)
- 組織の階層構造を表すための情報

集約するデータの各レコードに、これらの項目があらかじめ含まれるようにすることで、データ集約後の組織単位での集計、分析処理が容易となります。なお、これらの項目と組織名称、組織人員数などの対応付けは一般的にマスタ情報として人事部門などが保管していることが多く、これらの項目をキーにマスタ情報を参照することで、必要となる組織名称や人員数に関する情報を正確かつ効率的に入手することができます。一般に、すでにシステム化されている情報を利用する場合は、これらのキー項目が含まれていることが多いのですが、伝票や帳票などにより人手で運用されているプロセスだと、取り扱う情報にこれらのキー項目が含まれていないことがあります。例えば報告書のような形で情報を収集している場合は、組織名を記載する欄はあるものの組織コードは記載する欄がないということが起こり得ます。このような場合、人手による組織名の記述は省略方法などに個人差(ブレ)が生じるため、そのままでは入力データとして利用できないといった課題が発生します。このような問題を避けるためには、人手による業務プロセスを設計する際に、コード欄をあらかじめ用意するといった配慮が必要になります。

集約したデータをデータベースに格納する場合、データベースの一貫性を確保するため、データの正規化を行いその構造を統一する必要があります。正規化の作業の一つとして、データベースの各レコードを一意に判別するための項目(キー)を取り決めておくことが重要です。例えば、あるセキュリティ対策の組織単位での実施状況をデータベースに取り込む際には、前述した組織コードがキーの候補となるでしょう。もし、集約されたデータに組織コードが含まれていない場合は、本機能にて組織コードをデータベースの各レコードに追加するのではなく、データが生成される段階で組織コードが含まれるようにするべきです。

特に、集約される各データが複数のシステムに分散して存在している場合は、それぞれのシステムの設計指針の違いにより各データの構造が統一されておらず、上記のような組織コードが含まれていないケースが想定されます。その場合、企業/組織のシステム全体として、対象となるデータの構造に対する統一化された指針をあらかじめ策定し、各データが生成される段階からこの指針に従った設計を行うことがとりわけ重要になります。

1.2 情報の可視化

ESA の 18.1 節で説明したように、表示情報への変換を行う際には、異なる立場、職責を持つセキュリティダッシュボードの利用者像を想定し、それぞれにどのようなデータソース(データベース上の生データ)を使って、どのようなロジックで表示情報を作成するのかを考慮する必要があります。

例えば、企業/組織全体のセキュリティ状況を常に知るべき立場にある CIO/CISO 向けには、通常は組織全体の俯瞰状況を表示し、必要に応じて組織内の特定部門の状況を表示する画面へとドリルダウンするような仕組みが求められるかもしれません。この場合、データソースからそれぞれの表示情報を直接生成する方法のほかに、部門ごとの状況を表示するデータを生成し、生成された全部門のデータに基づいて組織全体の俯瞰状況を表示するようなロジックも考えられます。

また、単体のデータソースを加工して表示させるだけでなく、各データソース間での相関分析を行い、より付加価値の高い表示情報を作成することも必要です。例えば、セキュリティ事故の発生件数に関するデータソースと、セキュリティ教育の実施状況(理解度テストの合格率)や PC へのセキュリティ対策の実施状況に関するデータソースとの相関分析をそれぞれ行うことで、セキュリティ事故の原因がマネジメントの問題なのかコントロールの問題なのか、その切り分けを支援する情報として新たな付加価値を持たせることが可能です。

ダッシュボードサーバは、可視化エンジンと連動して利用者がアクセスするダッシュボード画面を表示する機能です。ESA の 18.4 節で説明したように、本機能の最大の達成目標は、利用者にとって理解しやすく意味のある形で、必要な情報をできるだけコンパクトに配置して表示することです。さらに、ダッシュボード画面が複数ある場合は、直感的な操作でそれぞれの画面遷移が行えるような仕組みを利用者に提供する必要があります。

これらの表示内容と直感的な操作を実現する具体的な仕組みについて、以下、当社での実践例を基に説明します。

図 1.1 CISO 向けセキュリティダッシュボード画面（当社サンプル）

図 1.1 は、CISO 向けセキュリティダッシュボードの当社サンプル画面です。

左側のサイドバーに相関分析、組織選択などの機能群を配置し、中央のメイン画面に全組織のセキュリティ施策の実施状況を俯瞰化して配置しています。メイン画面では、意味を持った必要な情報をコンパクトに表示するため、各組織を個々の立方体で表現し、立方体の各面に現在行われているセキュリティ施策の実施状況を色付けして表示しています。例えば、ある一面を PC のセキュリティ対策実施状況とし、良い評価の場合は青色、悪い評価の場合は赤色に近付くようなグラデーション処理が施されています。

これによって、利用者である CISO の果たすべき役割(組織全体のセキュリティ状況を常に知ること)に必要な情報を同一画面内で完結して表示することに成功しています。もし、一般的なグラフ(棒グラフ、線グラフ、円グラフなど)のみで同じ情報量を表示しようとした場合、同一画面内で利用者が判別できるように表示することは極めて困難となるでしょう。

また、セキュリティ施策の実施状況が芳しくない組織など、場合によってはその詳細情報を得たいこともあるでしょう。その場合、メイン画面上の該当組織の立方体をマウスクリックするか、サイドバーから該当組織を選択すれば詳細情報の画面へと遷移するような直感的なユーザーインターフェースも併せて実現しています。

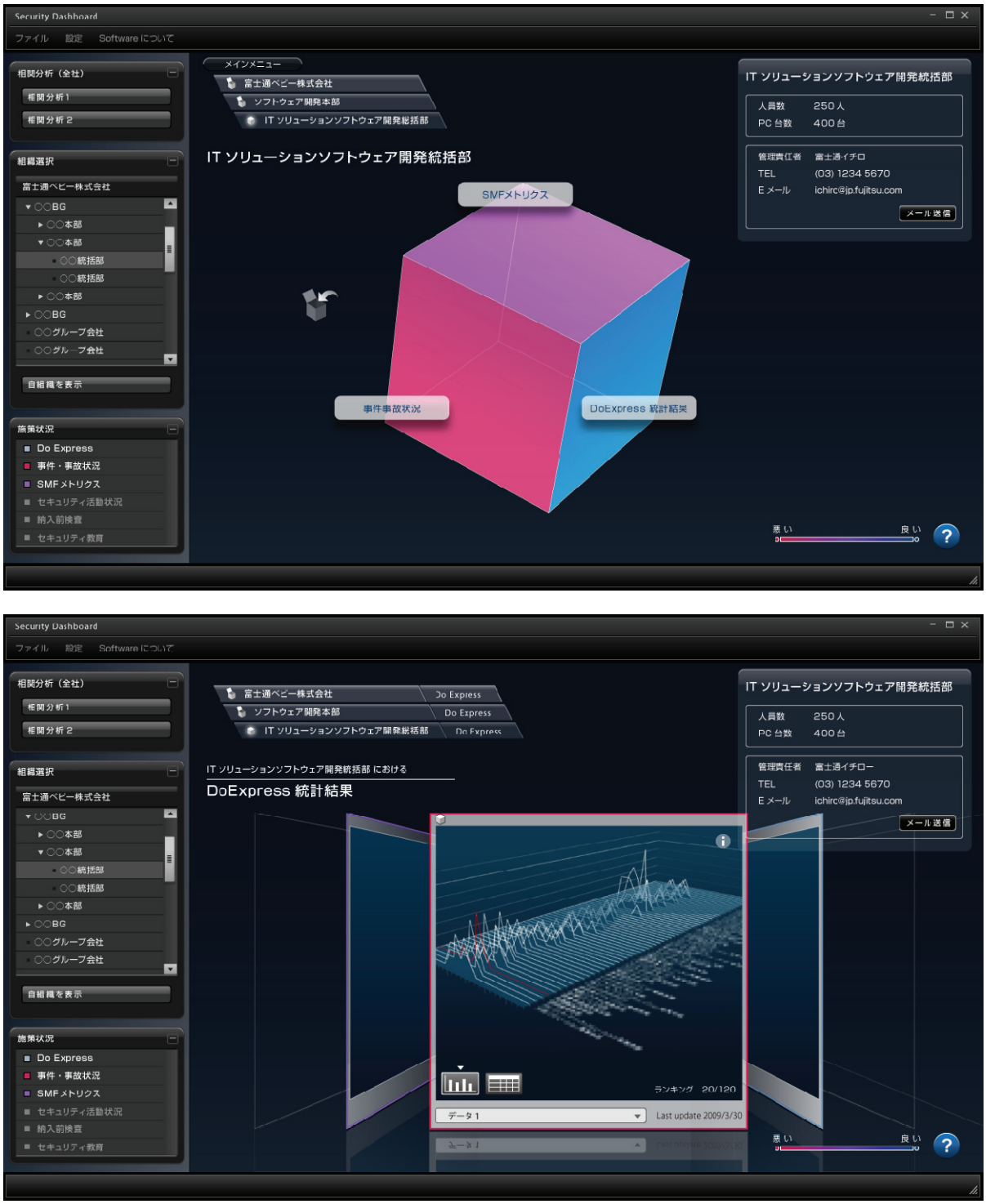

図 1.2 セキュリティ管理者向けセキュリティダッシュボード画面 (当社サンプル)

2. クラウドコンピューティングのためのセキュリティコンセプト

2.1 クラウドコンピューティングとは

「クラウドコンピューティング」とは、拡張性に優れ、抽象化された巨大な IT リソースを、インターネットを通じてサービスとして提供(利用)するというコンピュータの形態であり、2006 年に Google のエリック・シュミット CEO が提唱したコンセプトとされています。本章では、クラウドコンピューティングを実現するデータセンターにおいて、どのようなセキュリティの考え方を採用すればよいかについて考察します。

クラウドコンピューティングとは具体的に何か、どのような技術を利用すればクラウドコンピューティングなのかなどについてはさまざまな議論があり、現状では明確な答えはないと言ってよい状況です。見方を変えると、「最初から一定の方向性を持った「技術」ではなく、さまざまな技術動向が結果としてある「塊」として姿を現した『現象』と理解する」[*1]と考えれば分かりやすいかもしれません。

クラウドコンピューティングで実現されるサービスは、その提供内容により以下の3類型に分類することができます。

- IaaS (Infrastructure as a service)
- PaaS (Platform as a service)
- SaaS (Software as a service)

クラウドコンピューティングは、これらの基盤の上に構築される、「ユーザーが必要とするサーバ環境やアプリケーションをいつでも好きなだけ貸し出します、料金は実際に使用したぶんだけで結構です」というインターネットサービスと表現することができます。クラウドコンピューティングでは利用者からはサービスだけが見え、どのベンダーの製品を使ってサービスが提供されているかということは誰も気にしなくなる時代へと変化することになります。

このクラウドコンピューティングを支える基盤技術として、仮想化技術があります。クラウドコンピューティングでは価格対性能比の優れた、安価なサーバを用いたスケールアウト構成が基本であり、個々のサーバではなく、システム全体として、高いパフォーマンス、高可用性を実現するようにシステムが構築されます。このようなシステム上でクラウドコンピューティングサービスを提供するためには、物理的なサーバ構

[*1] 西田宗千佳 著:「クラウド・コンピューティング」より引用

成と論理的なサービスを切り離すサーバ仮想化技術が欠かせません。このことは、クラウドコンピューティングに必要となるセキュリティアーキテクチャーを考える上で重要なポイントになります。

2.2 クラウドコンピューティングに対するセキュリティ要件

クラウドコンピューティングに対するセキュリティ要件は、ASP や SaaS に求められる要件と、クラウドコンピューティングという形態のために独自に発生する要件の2種類からなります。

ASP や SaaS に求められる要件に関しては、表 2.2-1 のようにすでにさまざまなガイドラインが発行されており、クラウドコンピューティングのセキュリティを考える上で参考になります。

表 2.2-1 クラウドコンピューティングに関係するガイドライン等

ガイドライン等	概要
経済産業省 「SaaS 向け SLA ガイドライン」 （2008 年 1 月公表）	SaaS を提供するに当たってユーザー企業と提供企業間で合意すべきサービス内容（稼働率、障害復旧時間、データのバックアップ、セキュリティレベル等）とその具体的設定例が示されているガイドライン。本ガイドラインをそのまま利用することで、ASP･SaaS 事業者が適切な情報セキュリティ対策を実施できるように構成されている。
経済産業省 中小企業向け SaaS 活用基盤整備事業（2008 年 3 月公表）	中小・小規模企業にとって、使い易い財務会計機能等の安価なオンライン型ソフトウェアサービスを提供する。国がインフラ整備の初期構築費用、およびアプリケーションのオンライン対応のための移植費用を支援することによって、安価なオンラインサービスの実現を目指す事業。
総務省 「ASP・SaaS の安全・信頼性に係る情報開示指針」（2007 年 11 月公表）	地方公共団体や中小企業など一般の利用者による ASP･SaaS の評価・選択を支援するための指針。安全・信頼性に係る情報開示を必須項目と選択項目に分け、情報開示項目を共通化し、利用者によるASP･SaaS の比較、評価、選択等を容易にすることを目的としている。
総務省 「ASP・SaaS における情報セキュリティ対策ガイドライン」 （2008 年 1 月公表）	ASP･SaaS 事業者が、提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として具体的な対策項目が提示されている。JISQ27001 を参考に ASP･SaaS サービスの特性に基づいたリスクアセスメントの実施により取りまとめられているため、実践的な対策集となっている。

さらに、データ処理の仕組みをあえて意識しないようにするクラウドコンピューティングの本質を考えると、以下のような要件も考慮する必要があります。

- ほかの顧客のデータと確実に分離されていることの証明
- 第三者からのアクセスに対して保護されていることの証明
- データの物理的な保管場所が法令や規定に抵触する場合への考慮(個人情報にかかわるデータ等)
- 第三者がアクセスしていないかどうかのアクセスログの管理と開示
- 性能劣化への懸念
- クラウドコンピューティングサービス提供者間での相互運用性
- 複数サーバで仮想化される場合の商用ソフトウェアのライセンス問題
- データの復旧にどれくらい時間がかかるかの明示

富士通では、これらの要求に応えるために、「Enterprise Security Architecture(ESA) for Cloud」と「Security Management Framework (SMF) for Cloud」の2つのコンセプト整備を行っており、お客様に安心してご利用いただけるクラウドコンピューティングセンターの実現を目指しています。

富士通のエンタープライズセキュリティアーキテクチャー 追補版

2009 年　5 月　追補版発行

著者　富士通株式会社 情報セキュリティセンター ESA プロジェクト

編集・発行　富士通株式会社 情報セキュリティセンター

東京都大田区新蒲田 1-17-25 富士通ソリューションスクエア