ホワイトペーパー
富士通のセキュリティ マネジメントフレームワーク

目次

1. はじめに　～情報セキュリティガバナンス～

今日の企業においては、IT システムは業務に不可欠なインフラになっています。この IT システムをリスクから守るために必要なセキュリティ対策を欠かすことができません。

昨今、毎年のように、新しい攻撃方法が登場しています。攻撃者は、個人を標的としたものから、組織・重要インフラ・国家を標的に変え、攻撃の目的は、情報の窃取など組織的な活動に変遷してきています。そのため、攻撃者の手法はいままでより一層高度化・複雑化してきています。

このような時代背景を受けて、わが国では、2014 年 11 月に「サイバーセキュリティ基本法」が成立しました。また、情報保護管理の観点では、2015 年 3 月に、個人情報保護法の改正案が閣議決定されました。セキュリティ関連法案が今まで以上に整備され、関連事業者には法的な責務が要求されるようになってきています。一般に、セキュリティ対策に掛ける投資金額は、IT 全体に対する投資の 3～5%程度であると言われてきました。

IT 関連投資額は横ばいの一方、情報セキュリティ関連投資額を増やす企業は増加の傾向がみられ [1]ています。また、IT 関連投資額に対する情報セキュリティ関連投資額の割合は、10%前後が多い結果 [1]となっています。

その一方で、企業からの個人情報漏えいや社会システムの停止など、重大なセキュリティ事故は後を絶ちません。このことから、今なお多くの企業が「場当り的」な対応を実施しており、セキュリティ対策に投資効果が現れていないことがわかります。

2005 年 3 月、情報セキュリティガバナンスについて、経済産業省が、コーポレート・ガバナンスとそれを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること [2]、と定義しました。
2008 年 6 月、経済産業省は、「企業における戦略的な情報セキュリティガバナンスの確立に向けて」と題する中間とりまとめを公表しました。

同年、経済産業省は情報セキュリティガバナンスのあり方について、産業構造審議会情報セキュリティ基本問題委員会で検討し、その結果を「企業における戦略的な情報セキュリティガバナンスの確立に向けて」として公表しました。企業の経営陣は、セキュリティに関するリスク管理を自らの経営課題の一つとして捉え直すよう提唱しています。情報資産に係るリスク管理のために、経営者が方針を決定し、組織内の状況をモニタリングする仕組み、株主をはじめとする利害関係者に対する開示と評価の仕組みを構築・運用することが示されています。

2009 年 6 月には「企業における情報セキュリティガバナンスの確立」の普及・促進を図ることを目的として次の文書が取りまとめられました。
・情報セキュリティガバナンス導入ガイダンス

また、「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」報告書において、情報セキュリティガバナンスの実現を促すツールとして、以下の 3 つが提言されました。
・情報セキュリティ対策ベンチマーク
・情報セキュリティ報告書モデル
・事業継続計画策定ガイドライン

これらのツールを活用することで、企業は自身の情報セキュリティ対策の有効性と効率性をわかりやすく伝えることができます。また、企業内部における情報セキュリティ対策の必要性と正当性を説明できるようになり、より一層組織的な情報セキュリティ対策の実施が容易になります。

2. 富士通のセキュリティマネジメントモデル

2.1 セキュリティマネジメントモデルの背景

組織の情報システムのセキュリティを考える際、次の 2 つの視点に気をつける必要があります。一つはセキュリティ機能の視点、もう一つはセキュリティ管理の視点です。
セキュリティ機能は、セキュリティを維持するためにシステムが保有すべき一連の機能です。米国国防総省が 1985 年に出版した Trusted Computer Security Evaluation Criteria（TCSEC、通称オレンジブック）は、セキュリティ機能を記載した最も古い公的で有名な文書です。この文書では、利用者 ID とパスワードを用いて利用者によるログイン、グループ単位で制御したアクセス許可の仕組み、セキュリティログの取得・保管など、今日一般的であるセキュリティ機能の多くを実装しています。その後、各種の暗号方式やアクセス制御技術など、数多くのセキュリティ技術が誕生しました。セキュリティ技術の選択、実装方法はセキュリティ機能の視点で検討する必要があります。

一方、セキュリティ管理は、このようなセキュリティ機能を持つシステムを効果的に運用する際、そのシステムを取り巻く人・組織が行動すべき規範を示したものです。この分野の先駆として、現在もセキュリティの分野で大きな影響力を持っているのが、ISO 27000 ファミリです。このうち、ISO 27001 は、わが国のセキュリティ管理の公的認証制度として、ISMS（Information Security Management System）適合性評価制度で用いられています。この文書では、セキュリティ対策を有効に実行するために必要となる組織やプロセス、物理的環境、システムへの要求事項など幅広いテーマを取り扱っています。ISO 27001 は ISO 27002 とともに、2013 年に規格が改訂され、翌 2014 年に JIS 化されています。

セキュリティ機能とセキュリティ管理は、いわば車の両輪の関係であり、片方だけで機能するものではありません。そこで、セキュリティ機能とセキュリティ管理の双方を考慮した施策が必要です。富士通では、セキュリティ機能の基準として「富士通エンタープライズセキュリティアーキテクチャ（ESA）」を、セキュリティ管理の基準として「富士通セキュリティマネジメントフレームワーク（SMF）」を制定しました。

2.2 エンタープライズセキュリティアーキテクチャ

大型計算機が誕生した頃、情報セキュリティは「他人のデータには触れることができない」程度の概念でした。1980 年代中頃、米国国防総省がコンピュータのセキュリティ調達基準である「トラステッドコンピュータセキュリティ評価基準」（通称オレンジブック）を策定しました。これにより、認証やログの記録など、情報セキュリティの各種の機能が広く技術者に意識されるようになりました。そして 1990 年代には、いわゆる「オープンの時代」を迎え、情報セキュリティ対策の世界は大きな転機を迎えます。大型計算機の時代は、メーカーが独自に情報セキュリティのコンセプトを策定し、設計し、実装し、出荷していました。しかし、オープンな規格の普及によって、システムは複数のメーカーやベンダーが提供する機器によって構成されることが当然となり、これにともない情報セキュリティ機能も多くの機能部品に細分化されるようになりました。このことはコスト削減や選択の自由度拡大など、多くのメリットを利用者にもたらしました。しかし、その一方で利用者は自らの責任で各構成機器を選択しなければならなくなりました。機器同士の相互接続性、データフォーマットの一致、管理方法の整合性など、統一したシステムとして運用するための配慮は、すべて利用者の責任となりました。特に情報セキュリティの分野では、機器やソフトウェアの組み合わせにより安全性が変化する可能性があるため、利用者は細心の注意を求められます。その結果、不適切な組み合わせによる事故や問題が多数発生することになり、「情報セキュリティは難しい」「情報セキュリティはコストがかかりすぎる」という観念が定着しました。

これを解決するのが、「エンタープライズセキュリティアーキテクチャー（ESA）」です。

ESA は、企業内における情報セキュリティ対策の技術的な基本方針を明確にし、セキュリティのあるべき姿を体系化する文書です。企業は情報セキュリティ対策のシステムを構築する場合あるいは機器を調達する場合、常に自社の ESA への適合性をチェックします。その結果、ESA に適合しないと判断されたシステムや機器は、企業内で採用することは認められません。このような手法で、企業内の情報セキュリティの施策は統一的で整合が取れたものになり、セキュリティ投資が有効で効率的なものとなります。

2.3 セキュリティマネジメントフレームワーク

情報セキュリティマネジメントシステムを構築・運用する場合、適用範囲を定め、保護すべき情報資産を洗い出し、リスクを分析し、管理策を策定します。この際、マネジメントシステムの文書が重要です。セキュリティ管理の分野では、ポリシー、スタンダード、プロシージャの 3 階層からなる文書構造を採用することが一般的です。また、階層構造の上位文書から整備し、下位文書はその上位文書との整合性を保つ必要があります。この整備された文書に基づき、各種のセキュリティプロセスを実行に移していきます。他の多くの管理プロセスと同様に、セキュリティプロセスにおいても Plan-Do-Check-Act のいわゆる PDCA サイクルを回すことによって、マネジメントシステムを成熟させていきます。この情報セキュリティマネジメントシステムを確立・実施・維持・継続して改善するための要求事項を規格として ISO 化したものが ISO 27001 です。

企業にとって情報セキュリティマネジメントシステムを確立する際、ISO 27001 の要求に沿うことは、一つの実現方法です。一方、企業の成熟度合いにあった自分達のセキュリティマネジメントのフレームワークを考えて、それに基づいたマネジメントシステムを構築することが重要です。そして、継続的に PDCA サイクルを回すことで、より一層、マネジメントシステムを成熟されていくこととなります。

2.4 セキュリティマネジメントモデルの全体像

一般に、多くの企業は情報セキュリティ対策の基本原則を明文化した「情報セキュリティポリシー」を持っています。ESA も当然、情報セキュリティポリシーの要求事項に従って策定されるものです。わが国の情報セキュリティマネジメントシステムは、セキュリティ関連文書を「セキュリティポリシー」「スタンダード」「プロシージャ」 の 3 階層とすることが一般的です。ESA は「スタンダード」の一種であり、「プロシージャ」レベルのセキュリティ実装とのギャップを埋める位置づけの文書になります。

3. 情報セキュリティマネジメントシステム

3.1 情報セキュリティマネジメントシステム

企業におけるマネジメントのプロセスには、企業内統治、セキュリティ要件の遵守、認証維持などのプロセスがあります。
情報セキュリティの ISO 27001 を始め、ISO 9001、ISO 14001、IT サービスマネジメントの ISO 20000 などのマネジメントシステム認証を多くの企業が取得しています。これらマネジメントシステムの根底には、「Plan-Do-Check-Act（計画・実施・点検・処置）」（PDCA）のプロセスモデルがあります。

PDCA を定常的にまわすために、マネジメントシステムを継続的に、構築・運用していくことが、マネジメントシステムにおいて重要です。

ISO 27001 の認証取得は、企業が適切な情報セキュリティ実現のために必ずしも最善策ではありません。

しかし、一般的には、情報セキュリティのマネジメントシステムを構築する際には、ISO 27001 の要求事項、ISO 27002 の管理策に基づいて活動することが有効です。

その際、セクターごとの ISO 27000 ファミリが開発されていますので、必要に応じて追加することが有効です。代表的なものに、クラウド情報セキュリティの ISO 27017、クラウドに関する個人情報の ISO 27018、通信業界に関係する ISO 27011 などがあります。業務必要性に併せて、ISO 27001、27002 に管理策、項目などを追加して活用することになります。

3.2 ISO 27001

ISO 27001 準拠の情報セキュリティマネジメントシステムを構築する場合、一般的には、以下の(1)～(4)のような手順に基づいて構築します。

(1) 構築の準備・計画
(2) ISO 27001 による情報セキュリティマネジメントシステムの確立
(3) 運用開始、内部監査等の評価
(4) 見直し（継続的改善）

管理目的と管理策については、ISO 27001 の附属書Ａに記載があります。14 の管理策グループを 35 の管理目的に分け、それらを 114 の管理策で詳細化したものです。

(1) 構築の準備・計画

まず、トップダウンの推進体制とそれぞれの責任者を明確にした情報セキュリティ組織（委員会）を設立します。次に、必要となる資源を確保し、構築のスケジュール等を作成します。

(2) ISO 27001 による情報セキュリティマネジメントシステムの確立

①STEP1～STEP2 のフェーズ

ISO 27001 の適用範囲を、事業、組織、その所在地、資産及び技術の観点から定義します。次に、ISO 27001 の基本方針を策定します。これは、情報セキュリティに関係する活動の方向性、行動指針となります。

②STEP3～STEP7 のフェーズ

ISO 27001 の基本方針に基づき、リスクアセスメントの取組方法を策定します。

まず、リスクの識別から行います。情報資産を洗い出し、機密性、完全性、可用性の観点から洗い出した情報資産の重要度合いを評価し、保護すべき情報資産を明確にします。次にその保護すべき情報資産に対して、機密性、完全性、可用性を喪失させる脅威、ぜい弱性、それらが事業に及ぼすリスクを識別します。
続いて、セキュリティのインシデント（事故、障害等）による事業上の損害が発生する可能性を評価し、発生可能性を評価し、リスクの度合いを算定します。受容できうるリスクの度合い、リスク対応の必要性の判定を行います。この判定は、あらかじめリスクの評価基準を定めておく必要があります。

リスクの受容ができない場合、リスク対応として、管理策の採用、リスク保有、リスク回避、リスク移転の選択をします。一般には、管理策を採用し、リスクの低減を図ります。しかし、リスク対応を検討の上、費用対効果が期待できていないなどの場合、情報資産を破棄する、業務の廃止などリスク回避を選択する方法があります。昨今のセキュリティ事件は、さまざまな手法を用いてシステムのぜい弱性を攻撃することでインシデントを発生させるなど、その内容・方法は巧妙化してきています。このため、自社だけで情報資産を守ることよりも、専門の会社に情報資産や情報セキュリティ対策を外部委託（アウトソーシング）し、リスク

を移転する方法が考えられます。その他、リスクの移転として、リスクファイナンスの一種である保険などを利用することがあります。

リスク対応の結果に従い、ISO 27001 の附属書 A「管理目的及び管理策」のリストから、適切な管理目的と管理策を選択し、具体的な対策を選定します。

また、組織の必要に応じて追加の管理目的及び管理策を採用します。

③STEP8～STEP9 のフェーズ

経営陣は、選択した管理目的及び管理策に関する残留リスクを承認し、ISMS を実施する許可を与えます。選択した管理目的及び管理策並びに選択した理由及び除外した理由を記載した適用宣言書を作成します。

(3) 運用開始、内部監査等の評価

構築後、運用を開始し、内部監査及びマネジメントレビューにより、構築したマネジメントシステムを評価します。

(4) 見直し（継続的改善）

評価結果を反映し、作成した仕組み、文書等を改善します。

これは、ISO 27001 に基づく情報セキュリティマネジメントシステムを構築する上で、重要となります。特にリスクアセスメントの方法は、経営陣が残留リスクを承認する上で、投資金額と費用対効果を判断する際に重要となります。判断の根拠がないまま、費用だけで対策を判断してはいけません。事業上の損害、発生の可能性を考え、その損失、対策費用、及びそれによる効果等を踏まえ、損失と費用に見合った対策をとることが重要です。

例えば、毎年実施している情報セキュリティ教育に 1 項目追加することを本年度の施策とする場合、昨年度比で教育費用はほとんど変わらないでしょう。しかし、業務で使用するすべての Web システムに SSL プロトコルによる暗号化を施す対策を講じる場合、システム再構築に多大な費用が掛かる場合があります。セキュリティ事件・事故が発生し、対策に掛かる費用と、リスクを考慮し事前対策の費用を算出し、費用と効果のバランスを検討し、対策の妥当性を判断します。その際、イントラネット内とインターネット上とで発生するリスクの大小、対策内容や脅威、ぜい弱性の洗い出しが十分であることを確認する必要があります。イントラネット内とインターネット上で使用する情報資産の重要度も考慮する必要があります。リスク分析をした結果、イントラネット内は SSL プロトコルが不要とし、インターネット上で個人情報入力を行う時は、SSL プロトコルによる暗号化対策で十分と判断した場合、対象システムと変更費用を抑えられることが可能となります。逆に、イントラネット内にも大きなリスクがあり、事故が起きた時の費用が莫大となる場合、全システムを変更した方が却って、費用対効果が高くなることがあります。

上記を踏まえ、リスクアセスメントの実施方法を検討し、リスクアセスメントを実施し、経営陣に残存リスクの承認を依頼します。これにより、経営陣の承認基準が明確となり、セキュリティ投資の判断が容易となります。

4. 富士通の考えるセキュリティマネジメントフレームワーク

4.1 セキュリティマネジメントフレームワーク

前章で説明しました ISO 27001 のフレームワークを用いて情報セキュリティマネジメントを実現する手法は、セキュリティマネジメントに関するフレームワークを考えるうえで基本となります。

しかし、企業の情報セキュリティの成熟度によっては、すぐに ISMS 認証取得レベルを実現することが困難な場合があります。自社の身の丈にあったセキュリティマネジメントのフレームワークを考えることが重要となります。今までポリシーやセキュリティの規則は作成したものの、現場に浸透していない場合、チェックシートを作成し、各部門で自己チェックをする方法があります。最初の段階で重要なのは、遵守できていない事項を指摘し、罰則を与える趣旨ではないことを理解していただくことです。自己チェックの特性上、自らの判断のみで及第点とすることができるためです。そのため、実態に即した回答をしていただき、現実の傾向・問題点を知ることが重要です。全社で浸透が十分でない場合には教育や周知方法に課題があることが考えられます。ある特定の項目が多くの部門で遵守されていない場合、その項目は現場の業務に適合していない可能性があります。セキュリティ活動の効果を上げるためには、このような分析を通じて、規則や教育内容等を見直していくことが重要です。また、チェックシート記入のために、チェック項目を確認し、「このような記述が規則にあるのか」と改めて理解を深める人もいるでしょう。

そこで、内部監査を実施することも一案です。最初の段階では、監査実施を通じて、「こういう規則がある。」ことを理解してもらうことに力点を置くことが重要です。規則を遵守していることを確認するより、直接顔を合わせて会話するため、教育の場として活用することができます。そして、現場の実情に適合させて、規則や教育内容等を見直すきっかけとすることができます。

規則等がない場合、公開されているセキュリティに関する基準を利用する方法があります。たとえば、経済産業省の「コンピュータ不正アクセス対策基準」等が参考になります。この際、抽象的な表現ではなく、具体的な対応方法を示す必要があります。「重要な情報は、パスワード、暗号化等の対策を図ること。」という基準では、「重要な情報」を具体的にすることです。「重要な情報」とは、開発中の製品情報とお客様の個人情報です、と明確にすることで、対応策が明確になります。「コンピュータを入力待ち状態で放置しないこと。」の場合、「離席時は、コンピュータのロックかログオフを行うこと。パスワード付きスクリーンセーバを設定すること。設定時間は 5 分以内とすること。」等の記述にします。これに基づいて、自己チェック等を行います。また、内部監査等行う場合、法務部門と調整し、社内規程に明記して周知させる方法があります。

これらの事例は、小さいながらも PDCA サイクルの一運用です。運用が定着し、成熟してから、内部監査活動を行うことで効果的な PDCA サイクルをまわすことが可能となります。

また、ISO 27001 の詳細管理策とマッピングを実施することで、網羅性の確認、見直しすべき項目の判断が可能となります。

前述の「重要な情報」を具体化するには、情報資産を洗い出し、資産ごとに情報区分を決め、重要な情報を定義する必要があり、負荷が掛かります。そのため、まずは、公開、社外秘、極秘の 3 区分を想定し、極秘のみを重要な情報と判断し定義する方法があります。何回も見直しを行い、リスク分析・評価の手法を採り入れて、重要な情報について整理することで、より精度が向上します。

このように、自組織にとって現時点での最適なセキュリティマネジメントのフレームワークを考え、実施することが重要です。さらに、目標を設定し、目標を達成するために活動することで、ISO 27001 相当若しくは、それ以上のマネジメントシステムを実現することが可能となります。

マネジメントシステムの実現のためには、まず、推進組織・体制を構築します。情報セキュリティの施策展開は、トップダウンで推進することが重要です。組織全体の責任者は、トップである組織長が務めます。事務局が組織全体の推進を行い、情報セキュリティ管理責任者を各部に設置し、各部の責任者が各部の推進を

行います。組織に対する監査を行う責任者として、監査責任者を設置します。以下は組織の構築例です。

組織全体でマネジメントシステムを構築・運用することが困難である場合、本部、統括部など小さい単位から活動を始める方法があります。

活動組織単位が本部の場合、組織の所属長は本部長になります。活動組織の単位が本部、事業部、統括部と組織の都合に応じた単位で活動することが重要です。個別に監査組織がある場合、その監査組織に情報セキュリティ監査を依頼し、監査責任者として監査活動をしていただく方法があります。

活動が困難である場合、上記のように少しずつ対策を講じることが望ましいですが、情報セキュリティ事故はいつ発生するかわかりません。現状の状況を踏まえ、コンサルタントの支援なども考慮し、マネジメントシステムの構築を進めることを考慮する必要があります。この場合においても、自社に適合したセキュリティマネジメントのフレームワークを検討し、情報セキュリティを構築していくことが不可欠となります。

例えば、経済産業省が推奨する情報セキュリティガバナンスのツールのベンチマークを用いて、ベンチマークを実施することで、自社のセキュリティレベルを把握し、必要に応じて管理策の追加等を行い、ISO 27001 の認証取得や第三者監査を受けられる状態にすることが考えられます。このような方法で、自社に適合したセキュリティマネジメントのフレームワークを作成していくことは、組織をガバナンスする上で重要となります。

4.2 さらに情報セキュリティマネジメントシステムをよくするために

ISO 27001 相当の情報セキュリティ活動を実施している企業は、現状レベルに留まらず、品質、環境、IT サービス、事業継続など、他のマネジメントシステムとの統合を検討する方法があります。これは、組織ガバナンスの観点から、現在利用している情報セキュリティマネジメントフレームワークを組織全体へさらに拡張し、よりよい仕組みにする方法です。

例えば、IT サービスを業務として行っている場合、ISO 20000 を考慮したマネジメントフレームワークとの統合を検討することが挙げられます。

ISO 27001 附属書 A の A16 に「情報セキュリティインシデント管理」があります。附属書 A の A16 には管理策の一つに、「情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立しなければならない。」という要求があります。

例えば、自社で、インターネット販売を業務として行っている場合、お客様から WEB で購入できなくなった、と問合せ（インシデント）が発生した場合、以下の手順を実施します。

1）インシデントを受け付け、管理する
2）その不具合の根本的な原因を特定して、関係する部門と調整し、対策を講じる
3）その対策方針に従い、変更を行い、内部での確認等行う（対象は、ソースプログラムの場合、インフラの場合がある）
4）その変更に問題がない場合、リリースする
5）インシデントを受け付けると同時にセキュリティの管理責任者もしくは、セキュリティ委員会等へエスカレーションする

ISO 20000 における「サービスサポート」と「情報セキュリティ管理プロセス」の部分を比較すると、情報セキュリティでも本質的には同じものと考えられます。情報セキュリティと IT サービスの両方のマネジメントシステムで共通なプロセスを統合することで、より効率的なマネジメントシステムが期待できます。他に、内部監査、文書管理、教育等が統合しやすいプロセスとして挙げられます。ただし、組織の役割が、セキュリティ管理責任者である場合、サービスマネージャである場合、品質責任者である場合など、それぞれ異なる役割であることが考えられます。そのため、組織体制を体系立てたものにする工夫が必要です。

ISO 27001 で適用範囲を決めて、ある工場等のみで取得することがあります。この場合、詳細管理策 ISO 27001 附属書 A の A17「事業継続マネジメントにおける情報セキュリティの側面」「事業継続管理」に記載があるように、工場内で閉じた事業継続を行うことがあります。本来、ある生産ラインが停止したとき時、代替する工場、他の工場からの部品調達方法など、全社的な事業継続を考慮することが、本質的な解決となる場合があります。

経済産業省が推奨する情報セキュリティガバナンスツールに関する事業継続計画策定ガイドラインの趣旨も、事業継続をトップダウンで組織として推進していくことにあります。全社的な事業継続計画の下、その工場で実施すべき項目を検討することが重要です。

組織の情報セキュリティマネジメントシステムをより成熟させるために、他のマネジメントシステムとの統合、事業継続計画の充実等、ISO 27001 の枠に捉われず、自組織に適合させたセキュリティマネジメントフレームワークを考えていくことが重要です。

5. 富士通の関連製品について

5.1 セキュリティマネジメントフレームワーク策定に関するご支援

富士通は、1994 年より情報セキュリティコンサルティングを開始しております。情報セキュリティポリシーの立案からはじまり、お客様の情報セキュリティ対策の強化支援、情報セキュリティ監査の実施、そして、ISMS やプライバシーマークの認証取得支援と実績を重ねて参りました。これらの経験に基づくノウハウを活かし、お客様環境のセキュリティマネジメントフレームワークの策定、情報セキュリティマネジメントシステムの構築をご支援いたします。

サービス名	概要・関連サイト
情報セキュリティ方針立案コンサルティング	セキュリティに関する各種国際標準および当社のノウハウを基に、全社的な情報セキュリティ方針を立案します。
情報セキュリティ強化支援コンサルティング	現状のシステムを把握し、物理・技術・運用面に関し、情報セキュリティ上の問題点の指摘と、その強化策を立案します。またアプリケーションのセキュリティ機能の設計、製品導入のパラメータ設計および運用面における対策案の作成を支援します。
セキュリティ可視化コンサルティング	「情報セキュリティ対策の評価指標の策定」と「対策状況の可視化」を支援し、経営者によるリスクへの適切な対応と高水準の管理状態の維持、効率的な改善を実現します。
情報セキュリティ監査サービス	経済産業省の告示である「情報セキュリティ監査制度」に基づき「情報セキュリティ監査」を実施します。これによりセキュリティレベルの向上と同時に、信頼性の高い、客観的な評価を提供します。
BS7799 認証取得支援コンサルティング	お客様の ISO 27001(BS7799/ISMS)認証取得に向けたコンサルティング、及び支援を実施します。
統合マネジメント支	組織の認証規格（ISMS 等）遵守のための

援サービス（IMS-S）	組織的なマネジメント活動を支援する SaaS 型アプリケーションサービスです。各種機能・コンテンツを活用することで、容易な統合マネジメントシステムの運用を実現可能にします。
ISO15408 認証取得支援コンサルティング	お客様システムの ISO 15408 認証取得に向けたコンサルティング、及び支援を実施します。
プライバシーマーク取得支援コンサルティング	プライバシーマーク認証取得に向けたコンサルティング、及び支援を実施します。
情報セキュリティ教育コンサルティング	社員のセキュリティ意識向上に向けて、コンサルタントや専門のスタッフがお客様ごとに要件ヒアリングを行い最適なセキュリティ教育を実現します。
体験型教育サービス	お客様の標的型メール攻撃訓練の実施の目的に沿って、訓練実施のストーリーを定め、実施を支援します。
クラウドセキュリティコンサルティング	情報セキュリティの観点からクラウド利用時における課題の整理、クラウド業者、クラウド形態（IaaS、PaaS、SaaS）の選定を支援、安心安全にクラウドを利用するための導入企画、運用についてのコンサルティングを実施します。
クラウドセキュリティ評価・監査サービス	クラウドサービス事業者のサービス運用状況や、クラウド環境で稼動するシステムを、国内外のガイドライン、SLA 等を元に最適な評価・監査項目を作成し、評価・監査します。

6. 引用文献

1. **NRI セキュアテクノロジーズ.** 企業における情報セキュリティ実態調査 2014 第 2 版.
2. **経済産業省.** 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.

お問い合わせ先
富士通株式会社
クラウド事業本部
セキュリティテクノロジーセンター
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

2015 年 3 月