日本ユニシスグループにおける情報セキュリティ総合戦略

The Information Security Strategy in Nihon Unisys Group

三　口　充　高，大　橋　幸　江

要　約　2000 年以降のネットワークの発達に伴い，IT が社会経済へ急激に浸透したことにより，多くの企業において IT 戦略と経営戦略が同期化した情報経済化が進行している．この情報経済化により，セキュリティ管理対象は従来の書類等の物理的な対象物のみならず，ネットワークを介した情報資産全てへと変化してきている．近年，企業が引起した情報セキュリティ事故は，場合によっては企業存続が危ぶまれるまでの事態となって来ている．このような背景から，経済産業省では世界最高水準の「高信頼性社会実現による経済・文化国家日本の競争力強化と総合的な安全保障向上」を目指し，「情報セキュリティ総合戦略」を 2003 年 10 月に公表した．

この経済産業省の戦略を受け，日本ユニシスグループでは 2004 年 2 月「日本ユニシスグループ情報セキュリテイ総合戦略」を策定した．本稿では，企業における情報セキュリティへの取り組みが急務になった背景を考察するとともに，日本ユニシスグループにおける「情報セキュリテイ総合戦略」の目的と狙いと効果，三つの戦略，推進体制の紹介を行なうとともに戦略を発表してからの 1 年間を振り返り，今後の主な推進上の課題と対策をまとめた．

Abstract　Along with the network popularization since 2000, the rapid penetration of IT into the social economy initiates a progression of information economization that synchronizes the IT strategies and management strategies in a lot of the enterprises. This information economization has brought a change of security management targets from not only physical objects such as conventional papers but also to information assets across the network. In recent years, an information security accident that a company had caused puts its company surviving into jeopardy in some cases. From such a background, The Ministry of Economy, Trade and Industry aimed at "strengthening of competitive edge in economy and cultural national Japan, and improving comprehensive security by achieving a highly reliable social" of the world highest level, and made "Joint information security strategy" public in October, 2003.

Based on the strategy of The Ministry of Economy, Trade and Industry, an IT service company, Nihon Unisys Group, formulated "Nihon Unisys Group joint information security strategy" in February, 2004. This paper examines the background of the urgent need for initiative of the information security, introduces advantages of our goal and purpose, three strategies, and the implementation organization, and writes up as an activity article about problems and measures in the future implementation, looking back over the last year since the announcement of the strategy.

1. は じ め に

インターネットの台頭に伴い，世界中が高度にネットワーク化された IT 社会となった．この IT の急激な社会経済への浸透は，企業における経営戦略に大きく影響を及ぼし，多くの企業において IT 戦略と経営戦略が同期化した情報経済化が進行している．

情報経済化は，企業における情報セキュリティへの考え方を大きく変えてしまうことになっ

た．過去，企業の情報セキュリティ対策は，外部からネットワークを介しての情報改竄や情報破壊等の攻撃から情報資産を守るものが主体であり，企業は被害者であった．しかしながら，昨今の情報セキュリティ事故の多くは，個人情報の漏洩事故であり，いつの間にか企業は，情報セキュリティ事故の加害者となってしまった．

一旦，セキュリティ事故を起こした企業は，一過性の機会損失や，直接の損害賠償額等の損失のみならず，ブランドイメージが失墜し，世の中から社会責任を問われ，場合によっては，企業の存続すら危ぶまれる時代となってきた．

このような情報経済化に伴い，2003 年 10 月経済産業省より，日本の「情報セキュリティ総合戦略」が宣言された．同戦略のもと，2006 年には，企業に情報セキュリティの対応状況の格付けを行う事も同時に方向付けが成された．

日本ユニシスグループでは，経済産業省の「情報セキュリティ総合戦略」を受けて，2004 年 2 月「情報セキュリティ総合戦略」の制定が行なわれた．同戦略は，過去から推進してきた IT 中心の情報セキュリティ対策の範囲を拡大し，情報資産全てに対してのセキュリティ対策を目指したものである．また，日本ユニシスグループ各社のメンバーで構成される「情報セキュリティ委員会」は，情報資産全般についての取り組みを表明する意味から「総合セキュリティ委員会」と改名し，2004 年 4 月より新たな活動を開始した．本稿では，企業における情報セキュリティへの取り組みが急務になった背景を考察するとともに，日本ユニシスグループの情報セキュリティ総合戦略について述べる．

2.　企業における「情報セキュリティ対策」

2.1　社会責任としての情報セキュリティ

少し前まで，多くの企業の情報セキュリティ対策は情報システム中心で，ハッカーの侵入やウイルスへの対応を行い，外部からの情報セキュリティの脅威に対する防御が中心の活動であった．しかしながら，日々，新聞をはじめとする各種メディアで報道される情報セキュリティ事件や，今年 4 月から全面施行された個人情報保護法，等々，社会環境の大きな変化に伴い，企業にとって情報セキュリティ事故は他人事ではなく，自社で起こってもおかしくない自分自身の問題として真剣に取り組むべきものと意識変化が起こってきた．例えば，情報セキュリティ事故が起こった場合，企業の多くは，報道機関を通してトップ自ら状況説明を行い，自己責任を表明している．ある企業では，事故の真の原因を見極めるまでの一定期間，事業活動を停止して企業責任を果たすような時代へと変化してきている．いまや情報セキュリティは，企業の社会責任やコンプライアンスの重要課題となってきた．

IT 事故の発生は，情報経済に大きな影響を与える可能性がある為，企業は，経営計画の中に情報セキュリティへの取り組みを表明する事が必須となった．情報セキュリティ対策は，従来のような被害者としての守りの対策から，企業としての経営課題と位置付けた攻めの施策へと変化してきている．

2.2　経営課題としての情報セキュリティ

企業における情報セキュリティ対策でもっとも重要なことは，経営トップの強いリーダシップであると言われている．情報セキュリティ対策は，多くの場合，直接事業に利益をもたらすものではなく，情報セキュリティへの費用は事業活動にとって負の要因として捉えられる事が

多い．また，情報セキュリティ対策とともに，業務面の抜本的な見直しが必要とされ，従来は情報の取り扱いが自由にできていたものが，情報セキュリティ面からの規制が加えられ，その取り扱いが面倒になったり，場合によっては取り扱いの拒否や，情報収集にも臆病になるような事態が発生する可能性を持っている．このような状況の中で企業は，内部の心理的抵抗を抑えつつ短期間に意識改革を推進する必要がある．こうした意識改革は，企業トップの強いリーダシップがあって初めて実践できる事である．

経営トップの情報セキュリティ向上の重要性への理解と強い想いがトップダウンの形で発揮される事により，その企業を取り巻く人間に変革への行動を促すのである．情報セキュリティ対策は，「組織的対策・人的対策・技術的対策・物理的対策」の四つの要素から形成されている．情報セキュリティ事故原因の 8 割近くは，人間系による故意を含めたヒューマンエラーと言われている．企業にとっては，このヒューマンエラーへの対応が情報セキュリティ対策の大きな課題となる．従業員はもとより派遣社員，その企業を取り巻く取引先等，企業に関係を持つ全ての人間に，情報セキュリティに対する強い認識を持たせる事が重要である．意識付けには，教育，研修，啓発活動，場合によってはルール違反に対しての罰則も実施することにより，地道な意識改革を行うことが必要とされる．

ある情報セキュリティ先進企業の情報セキュリティ対策責任者は，各人に意識させる程度ではなく，各人の DNA に刷り込む位の対応が必要と発言されている．それ程，個々人に情報セキュリティに対しての意識付けを浸透させていくことが重要である．

企業の情報セキュリティ対策は，地震，火災等の災害の他，社内の犯罪等，様々なリスクと同様に，保有情報資産のリスクを考える必要がある．特に情報は，物品のように管理する事が難しい性質のものであり，情報セキュリティ担当者にまかせているだけでは守りきれないものである．繰り返しになるが，強い経営トップのリーダシップのもと，その情報セキュリティ対策の一つ一つを，その企業と関係を持つ人間の意識に根付かせる事が，企業の経営課題としての情報セキュリティ対策である．

3.　日本ユニシスグループの「情報セキュリティ総合戦略」

経済産業省は世界最高水準の「高信頼性社会実現により経済・文化国家日本の競争力と総合的な安全保障向上」を目指した「情報セキュリティ総合戦略」を 2004 年 10 月に公表した．日本ユニシスグループ情報セキュリティ総合戦略は，経済産業省の「情報セキュリティ総合戦略」の指針に則り，IT サービス企業としてなすべきこととして，日本ユニシスグループ全体の総合的なセキュリティ対策をまとめたものである．

本戦略は，2004 年 5 月にイントラネットに掲載され，グループ全体を対象としてスタートした．日本ユニシス社長からの「情報セキュリティ総合戦略始動について」のメッセージと，日本ユニシスグループ CISO （Chief Information Security Officer）から「情報セキュリティを構築する上で一番重要なのは皆さんの意識です」といったメッセージ，グループの情報セキュリティ総合戦略についての説明が，映像ストリーミング配信とともにグループ全社員に向けて発信された．

3.1　情報セキュリティ 3 カ年計画

日本ユニシスグループでは 2004 年度を初年度とする「総合セキュリティ戦略 3 カ年計画」

を実行中である．3カ年計画を進めるに至った背景とわれわれが認識していた課題を整理すると図1の通りである．

日本ユニシスグループの課題を解決していくためには，グループ全体を網羅した情報セキュリティ強化対策を打ち出し，計画的かつ継続的に実施していくことが必要である．

図1　日本ユニシスグループにおける情報セキュリティ推進上の課題

3.2　目的と狙いと効果

総合戦略の目的は以下の3点である

1）“情報セキュリティ”ブランドの確立

企業セキュリティ格付けで，最高基準レベルを取得し，情報セキュリティを新たな強みとすることにより，情報セキュリティのブランドを確立する．

2）深い理解と高い意識によるセキュリティ文化の浸透

戦略では，人間系での対策を最重要課題として掲げている．既に，セキュリティポリシ・プロシージャの策定や教育等を実施しているものの，制度やルールが十分身についた行動には至っていないのが現状である．グループの経営者，従業員の情報セキュリティに対する深い理解と高い意識を持たせる為の具体的な施策を実行することにより，セキュリティ文化を根付かせ，浸透させる．

3）国家が目指す世界最高水準の「高信頼性社会」実現への貢献

ITサービス企業として，安心して使えるITサービス基盤を構築，提供することにより政府が主導となって進める取組みに積極的に参画していくことを通じて，国家が目指す「高信頼性社会」の実現に貢献していく．

これら三つの目的を果たすことにより，企業価値と信頼性の向上を図りITビジネスの更なる拡大を狙っていく．日本ユニシスグループが新たな顧客価値を創出し，ビジネスを拡大・展開していくためには，情報セキュリティに関して単に「守り」の視点から対応するだけではなく，そこから生み出される技術・ノウハウを活かしたグループの高度なセキュリティソリュー

ション開発，高度な情報セキュリティ基盤の提供など，企業の情報セキュリティの高度化を実現し，生産性向上およびコスト削減など，「攻め」の視点からも対応していくことが必要であり，その結果として，日本ユニシスグループの IT サービスビジネスの拡大に繋がると考えている．

* 企業セキュリティ格付け制度は経産省「情報セキュリティ総合戦略」の施策として挙げられており、2006年に制度化される予定。
** NUL、USOL、UAL、A-tas、UISの5社を取得あるいは拡張対象とする。

図 2　3 年後のビジョンと目標

3.3　三つの戦略

「人・組織的対策」「制度的対策」「技術的対策」に「事前対応策」・「事後対応策」の両面からの対策を行い，その過程から生み出される情報セキュリティ確立のためのプロセス，ノウハウ，そして物理的な仕組みをグループの新たな強みの一つとして位置付け，グループ全体の競争力を図ること，また，三つの戦略における具体的対策を計画的に実施していくことが重要と考えている（図 3）．

図 3 “ 高信頼性 IT サービス企業 ” 実現のための三つの戦略

3.4　推 進 体 制

グループの情報セキュリティに関する決定機関として CISO を委員長とする「グループ総合セキュリティ委員会」を設置，実働チームとして「グループ総合セキュリティ戦略推進チーム」

を編成し，その下に「人・組織対策」「制度対策」「技術対策」のワーキンググループを置き，具体的対策を検討する体制をとっている（図 4）．推進チームは推進者会議を開催し，課題や推進方法などを議論している．

また，具体的対策を実施するにあたり，セキュリティ対策専任部隊が実行支援する体制を敷いている．

図 4　日本ユニシスグループ総合セキュリティ推進体制（2005 年度版）

日常の情報セキュリティ対策推進においては図 5 の通りとした．

図 5　情報セキュリティ対策ならびに個人情報管理者/担当者の役割（2005 年度版）

4. 「情報セキュリティ総合戦略」の取組

3章で，日本ユニシスグループの「総合セキュリティ戦略3カ年計画」の概観について述べたが，本章では，初年度である2004年に注力した活動について述べる．

4.1 啓 発 活 動

情報セキュリティレベルを上げる，また，情報セキュリティ文化を根付かせるには，役員・従業員に対する継続的教育は重要ではあるものの，それ以外の施策も併用して全グループ従業員の意識を高めなければその実現は難しい．その為，我々は教育以外で「情報セキュリティを意識させる」,「毎日何らかの形で自然に情報セキュリティに関することに触れる，触れさせる」為にはどうしたら良いかを考えた．

4.1.1 情報セキュリティ文化を根付かせる工夫 —情報セキュリティ向上レベルの目標設定

情報セキュリティを意識させるために,「情報セキュリティ向上レベルの目標設定」を実施することにした（2004年度は一部の会社にて実施し，2005年度は全グループ会社にて実施している）．日本ユニシスにおいては，一段組織（一般には部）毎に情報セキュリティ向上レベルの目標を設定，各部署メンバに周知徹底させた．また，その目標項目の確認方法を決定させ，毎月進捗状況を情報セキュリティ戦略ホームページに掲載した．なお，第三者の客観的な目で監査する必要があることから，情報セキュリティ専任部隊が監査を実施し，監査報告書に関してはイントラネットにて社内公開した．

4.1.2 情報セキュリティ文化を根付かせる工夫 —PC立ち上げ時の情報セキュリティルール紹介

社員が日常業務を通して情報セキュリティに関することに触れる/触れさせることを狙い，各人がPCを立ち上げた時に強制的に情報セキュリティに関するルール/注意事項をイラストで紹介するようことにした（図6）．始めは目新しいこともあり注目を浴びるが，1枚のイラストを2週間掲載すると2〜3日で興味を持たれなくなるため，3枚目のイラストからはセキュリティに関する事故等のニュースを毎日テロップ形式にて掲載することにした．

4.1.3 情報セキュリティ文化を根付かせる工夫 —情報セキュリティ標語キャンペーンの実施

「休み時間にちょっと考えてみようか」,「仲間と飲んだ時に話題になったら良いのでは」，そういった発想から，情報セキュリティに関する標語キャンペーンを実施した．情報セキュリティに関するテーマを決めて標語募集を行い，優秀作品に対し賞金を授与することにした．イントラネットには図7のようにイラスト入りで掲載した．

4.1.4 情報セキュリティ自己監査の実施

情報セキュリティ自己監査は毎年1回以上実施することが情報セキュリティプロシジャにて義務付けられている．2003年度までの情報セキュリティ自己監査はアンケート方式であり，例えば情報セキュリティ基本方針を読んだか？,情報セキュリティプロシージャを読んだか？,

図 6　情報セキュリティに関するルール/注意事項イラスト

図 7　情報セキュリティに関する標語キャンペーン作品

ウィルスパターンファイルは最新版か？　といった形式的なものであった．2004 年度は e-Learning（インターネット/イントラネットによる自己学習システム）を用いた試験方式で対応することにした．以下に例示したような質問方式で，正解の場合は次の質問へと移り，不正解の場合は「解説」の画面となり，解説を読んだ後設問に戻り再度解答することにした．

例）　お客様から次期システム検討にあたり，お客様の秘密情報（お客様から秘密情報と口頭で伝えられた情報）を入手しました．その資料には「秘」「社外秘」とは記されていませんでしたが，お客様からは取扱いを十分注意するようにと指示がありました．このような時，あなたが取るべき行動は以下のどれですか？

① そのまま持ち帰り，必要部数コピーして利用する．メンバーに配布する．

② 予め，お客様との間で秘密保持に関する正式契約を締結し，資料には「秘」とスタンプを押してそのその情報を取扱う．

③ お客様にはあとで秘密保持契約を締結することを伝え，持ち帰った資料はそのまま協力会社に引き渡す．

4.1.5 課　　題

啓発活動については前述した以外にも対応しているが，一方，外部環境として，情報セキュリティ事故についての報道が多くなってきている等もあって，顧客からの情報セキュリティに関する調査，アンケートの提出依頼が多くなっている．一部調査結果によっては取引停止とす

ることを明記しているものもある．また，入札条件として情報セキュリティ要件が盛り込まれ始めたこともあり，社内においても一昨年に比べると情報セキュリティに対する関心度は深まってきている．しかしながら，情報セキュリティ文化を根付かせるまでには至っておらず，情報セキュリティ自己監査での正答率が悪い項目に関しては，情報セキュリティ強化に繋がるよう，継続的な教育及び対策を打っていく必要があると考えている．

4.2　ISMS 認証取得に向けて

日本ユニシスグループとして，ISMS （Information Security Management System）認証及びプライバシ・マークを取得し，継続的に PDCA （Plan-Do-Check-Action）マネジメント・サイクルをまわすことは，結果として，対外的に情報セキュリティブランドを確立するとともに，社内に情報セキュリティ文化を根付かせることにも繋がると考えている．既に，日本ユニシスでは 2002 年にアウトソーシング事業部が，ユニアデックスは 2003 年にサービス統括一部が，エイタスでは 2003 年にアウトソーシング統括部が ISMS 認証を取得しており，ISMS 認証取得に関しては昨年度から計画的に対応を実施している．

4.2.1　ISMS 認証取得体制の確立

2004 年 4 月，総合セキュリティ戦略推進室に情報セキュリティ専任要員として，40 名強のメンバーが集められた．4 月から 5 月にかけ，日本ユニシス及びユニアデックスの情報セキュリティに関るメンバーを講師とした研修と「ISMS 構築コース」の社外研修を受講した．計画では「ISMS 構築コース」受講後，ISMS 認証取得モデル部門にメンバーを派遣し，認証取得支援を実施する予定であったが, 受講後すぐに ISMS 認証取得支援を行うのは困難と判断した．そのため 2 か月間を ISMS 認証取得推進に向けての準備期間と位置付け,

① ISMS 認証作業そのものに習熟し，作業全体を把握する．

② 「手順」「必要な書式」等の標準化を図る．

こととした．

①に関しては，2003 年度に情報セキュリティ委員会にて，日本ユニシスグループの情報セキュリティポリシ等の見直しを行うことを目的に，特定部門で情報資産の洗い出しを行った際のデータを基に，実習/習熟を図った．

②については，メンバーを 9 チームに分け，ステップ毎に各チームの成果物のレビュを行い，良い成果物をピックアップしていくことにした．また，レビュでは ISMS の有識者に評価していただいた．この準備期間でまず ISMS 作業の Plan（情報セキュリティ・マネジメントシステムの構築）工程作業手順を仮想経験した 40 名の体制を作った．

4.2.2　モデル部門の選択

日本ユニシスグループ情報セキュリティ総合戦略において，初年度（2004 年度）は日本ユニシスのモデル部門を対象に対応することにしていたが，グループ各社に拡大していく為に，日本ユニシスだけではなく，ユニアデックス，日本ユニシス・ソリューション，エイタス，日本ユニシス情報システムでもモデル部門を選定することにした．日本ユニシスに関しては，まずスタッフ部門から対象部署を選定し，それ以外の会社に関しては，各社が対象部署を選定した．その結果 13 部署にて，認証を取得または取得可能レベルまで対応することを目標にスタ

ートした．

4.2.3　推進計画の概要

各モデル部門に対し 2 名から 3 名の情報セキュリティ専任メンバーを派遣，モデル部門では ISMS 認証取得責任者，担当者を選定し外部の研修を受講後，各部門の推進を担っていただいた．各モデル部門においては派遣した PM （Project Manager）が中心となり進捗管理表をベースに相互確認を行った．その結果 2005 年 3 月にはモデル部門の内 4 部門が新規認証取得，1 部門が拡大認証を取得することができた．

4.2.4　次年度に向かっての対応

日本ユニシスグループ情報セキュリティ総合戦略における ISMS 認証取得スケジュールは，2006 年度に日本ユニシス全部門が認証を取得する計画としている．その達成のために作成した「2006 年度日本ユニシス全社で ISMS 認証取得する為の 2005 年度 2006 年度の行動方針案」が，2005 年 3 月の総合セキュリティ戦略推進チーム会議にて承認された．方針の骨子は以下の通りである．

① 2006 年度全社で ISMS 認証取得する為の工程表

② 各一段組織（部）での認証取得対応方法

・核になる組織で ISMS 認証を取得し，拡大していく．（一段組織の資産の量，人数，地方の組織があるか等により異なる）

③ ISMS フレームワークの構築

・取得部門の負荷軽減のために，グループ全社統一の ISMS 文書を採用する．

・リスクアセスメントツールをブラッシュアップする．

④ ISMS 内部監査の標準化/簡略化

・情報セキュリティ専任部署総合セキュリティ戦略推進室が対応する．

⑤ 2006 年度，統一認証申請時の全社組織イメージ（図 8）

図 8　2006 年度 統一認証申請時の全社組織イメージ

・経営陣（CISO）
・ISMS 情報セキュリティ委員会（一段組織の管理職で組織する）
・専門委員会（全社共通の特定対応を担当）
・構築実行部隊（情報セキュリティ専任部署/総合セキュリティ戦略推進室）

4.3　個人情報保護法への取組み

日本ユニシスグループの個人情報保護対応についても「情報セキュリティ総合戦略」の一部として，早期に取り組むこととした．このため，2004 年 8 月，総合セキュリティ戦略推進室内に個人情報保護対応とプライバシーマークの認証取得に向け，個人情報保護推進グループを発足させ活動に着手した．

4.3.1　個人情報保護対応の具体的な対策

法律を日本ユニシスグループ全社員及び取引関連企業が一丸となって遵守する為に以下の対策を講じた．

① 個人情報保護推進体制の確立
② 社内規程ガイドラインの制定
③ パートナ等の委託先への対応
④ プライバシーマークの認証取得
（JISQ 15001 に基づくマネジメントシステムの構築）

社内，社外に向け個人情報保護対策を講じる事により内部統制が図られ，PDCA の管理サイクルが廻り，セキュアな環境が実現できてくる．このレベルを客観的に社外に認識してもらうと共に，企業ブランドの向上の為の施策として，プライバシーマークの認証取得も併せて推進した．

4.3.2　個人情報保護推進体制の確立

日本ユニシスの個人情報保護を推進するには，トップダウンで全社員が一体となって対応する事が必須である．社長により CPO（個人情報保護責任者）が任命され，CPO は経営委員会にて「個人情報保護マネジメント・システム」を構築すること，個人情報の適切な取扱い・安全管理を行なうことの表明を行なった．10 月には，個人情報保護に関する基本方針を制定し，社長宣言，CPO ステートメントと共に社内に向けて発表を行い，日本ユニシスに於ける個人情報保護への取組が本格的に始動された．

スタートに際しては，重点項目，推進体制（図 9）を以下の通り定め活動に着手した．

重点項目

① 実態調査・確認等を通じ，基本ルール・ガイドの見直し・策定を行い，教育・研修等による啓発・周知を徹底する．
② 運用体制を整備し，実践的な対応を可能とする手順・要領を作成する．
・基本方針の策定・公開
・規程・ガイド・様式等の整備・周知
・体制の整備
・3 形態（トップ/個人情報管理者＆担当者/全従業員向け）の教育・研修プログラムの

作成・実施

・構築・運用の支援，情報発信・公開・相談対応

図 9　推進体制

4.3.3　社内規程ガイドの制定

社内規程ガイドの制定に向けて，まず，日本ユニシスの保有する「個人情報」，「個人情報データベース」の洗い出しを実施すべく，各事業部への調査依頼を実施した．保護・管理すべき個人情報の特定が必要となる為，ほとんど全ての個人情報を対象に詳細な内容・取得方法について調査を実施した．回収した調査票から個人情報を整理し，類型化，体系化を行い，あわせてリスクアセスメントを行なった．最終的には，日本ユニシスにおける個人情報の分類基準を情報区分と情報種別により定め，保有する個人情報の分類と管理レベルの設定および統一を図った．

保護・管理すべき個人情報が決定した後，その個人情報をどのように取り扱うのか，適用すべき安全管理措置のレベル設定は何か等の指針を「日本ユニシスにおける個人情報取扱いガイド」として取り纏めた．本ガイドは日本ユニシスにおける個人情報保護マネジメント・システムの運用に当たり，個人情報の取扱いや安全管理措置等を中心に要領・手順を取り纏めたものである．

4.3.4　パートナ等の委託先への対応

日本ユニシスグループは，日本ユニシス株式会社を中核とし，システムサービスを提供する日本ユニシス・ソリューション，サポートサービスを提供するユニアデックスを含む総計 11 社で，トータルな IT サービスを提供している．サービス提供に際してはグループ各社と密接な関係を持つ，パートナ（委託先や協力会社）との協業が必要となってくる．個人情報保護や

安全管理措置を日本ユニシスグループ各社だけが対応するだけでは不十分で，共にサービス提供を行なうパートナにおける個人情報保護への対応状況が大きな鍵となってくる．我々は，日本ユニシスグループがお客様から預託を受けた個人情報に関する取扱いガイドを定義した．そのガイドラインは「個人情報の預託処理に関する手続き」として取り纏め，委託先の選定基準，委託先との契約事項，委託先の監督に関して細かく定義した．現在，この手続きに従い，現行の委託先に対して個人情報保護レベルの調査を実施中であり，調査結果を日本ユニシスグループの個人情報保護レベルに照らし合わせ，レベルが低い委託先については，個別に是正処置等の対応を実施している．

4.3.5　プライバシーマークの認証取得

プライバシーマークとは，ISO や ISMS 等と同じ JIS の規格の中にある個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS　Q 15001）を満たしているものに対して，第三者の立場から与えられる認証である．個人情報保護法はまだ施行されたばかりであり，各省庁のガイドラインが出されているものの，どこから違法でどこまでが合法であるといった事が明確でないところが多く，各企業ともその対応に苦慮しているのが現状である．個人情報保護法は企業に課せられる最低限の義務であり最低必要条件である．プライバシーマークの取得は企業の義務のみならず，個人情報保護や安全管理への対応が一定基準以上である企業としてお墨付きを受けたことになる．

企業にとってプライバシーマーク取得のメリットは，

① 個人情報に関するリスク・マネジメント（リスクの回避・低減等の仕組み）を確立できる
② 顧客・取引先企業の信頼を獲得できる
③ 社員の個人情報保護の意識向上が図れる
④ プライバシーマーク取得事業者を入札資格条件とする受注機会損失を回避することができる
⑤ 受託する側，またはパートナとして選ばれる立場に立てば，企業選択条件のひとつをクリアできる
⑥ プライバシーマークを名刺，封筒，宣伝広告資料，ホームページ上に表示ができ，広く企業の取組み姿勢をアピールできる

と考えている．

また，社内的には，プライバシーマーク取得に向け，社内制度の一斉見直しが行なえる，従業員・協力会社の方々を始めとする個人情報を取り扱う人間の研修・教育の徹底が図れる等，プライバシーマークの取得を大きな目標として全社を揚げて個人情報保護に対する意識が高まってきた事がもっとも大きな成果と考えている．今回，プライバシーマーク取得に向け，活動を続けてきたが，この活動はあくまで情報セキュリティ意識向上のスタートラインにつくための活動であり，今後，個人個人がそれぞれの役割・責任を自覚し，情報セキュリティ・レベルの向上，個人情報の保護に積極的に関与・対応していく環境・文化を継続的に作り上げ維持していく事が最大の課題である．

4.4　技術的な対策

情報セキュリティへの取り組みは，前述した個人情報保護法への対応必要性と言った外的要因もあって，企業は益々厳しい対応を迫られている．「絶対に事故は起こさない」とは言いきれない現状がある．保守的に安全を第一義に考えなるならば，個人情報は取得しない，持ち出さない，利用を制限することを考えねばならないが，それでは企業活動が止まってしまう．

日本ユニシスグループ全社員が情報セキュリティを意識し，機密情報，個人情報の取扱いに関心をもって対応出来るよう，啓発活動として教育，研修，プッシュ型の情報発信を推進してきた．情報セキュリティポリシの見直しから各種ガイドラインの改定と施策を矢継ぎ早に実施した．しかしながら，個々人の意識に情報セキュリティの重要性を意識づけても，ヒューマンエラーを 100% は避けられない．このヒューマンエラーを最大限防止するのが，技術的な対策である．日本ユニシスグループにおいては，情報セキュリティ総合戦略の初年度として最も対策が急務とされた二つの技術的課題に取り組んだ．先ずは，豊洲本社ビルにおける社員カードを鍵とした物理セキュリティの構築（入退室管理の導入）の実施．もう一つは，情報漏洩の対策として外部持ち出し PC 内データの暗号化対策である．

4.4.1　物理セキュリティの構築

物理セキュリティプロジェクトは，フェーズ 1 として豊洲本社ビルの入退館管理システム導入を目的に，2004 年 5 月に発足した．豊洲本社ビルでは，社員，派遣及び協力会社の方々，保険外交員，各種ビルケアの為の外部の方々，総勢数千名が，入館時社員証を呈示するか受付を済ませるだけで，各階の執務室まで出入りする事が可能であった．

物理セキュリティプロジェクトは，JISX 5080「情報セキュリティマネジメントの実践の為の規範」の物理セキュリティ規格を基に構築を開始した．構築推進のための「基本的な考え方」については，日本ユニシスグループ総合セキュリティ委員会及び物理セキュリティプロジェクトで合意し，毎日，豊洲本社ビルの入退室をする数千名のセキュリティレベルの定義や，入室可能範囲の決定を行なった．

検討の結果，入退室の鍵は，現社員証をそのまま利用できる仕組みとし，協力会社及び派遣社員については，別途入退室カードの発行を行なうこととした．また，社員が社員証の携帯を忘れた場合は，社内の第三者が社員であることの身分を証明出来て初めて，入退室カードを貸出することとした．

予定通り 10 月 22 日に本社物理セキュリティシステムの運用が開始された．当初，種々の運用上の問題が発生する事が想定されたが，運用面でのトラブルは無く，物理的な障害，例えば，常時開放されていたドアが頻繁に開閉される事による，ドアヒンジやドアノブの障害程度ですんだ．これらは適時修理する事により解決した．

導入して早 9 か月が経過するが，現在，物理セキュリティ・フェーズ 2 として，豊洲本社ビルの課題の整理とその対応及び，本社物理セキュリティ導入で培ったノウハウを基に，支社支店への物理セキュリティ見直しと対応を予定している．

4.4.2　情報漏洩対策の暗号化

毎日各種マスコミから報道される，情報漏洩事故のニュースは後を絶たない．日本ユニシスグループにおいても情報漏洩対策の手当てが急務とされていた．既に日本ユニシスにおいては，

モバイル PC に暗号化ソフトウェアが導入されていたが，暗号化/複合化の処理が遅く，また保護したいファイルを常に指定しなければならない等の不便さがあり，より効率的な暗号化ソリューションを日本ユニシスグループに展開することが必要とされた．

新たな暗号化ソリューションの選択に際しては，利用者が暗号化を意識せず，ハードディスク全体を暗号化出来る事，暗号化/複合化の処理が高速である事を条件としてツール選定を行なった．決定から実導入着手まで 3 か月で，導入マニュアルの作成，インストールメディアの作成，ヘルプデスクの対応を実施した．実導入に際しては，暗号化ソフトの技術対応要員 3 名，ヘルプデスク要員 2 名，推進事務局 2 名で対応した．今年度は，部分的な暗号化等ではなく，総合的なクライアントセキュリティ対策について推進していく予定である．

5. 「情報セキュリティ総合戦略」の推進課題

日本ユニシスグループ情報セキュリティ総合戦略 3 か年計画が始動され 1 か年が経過した．昨年度は，戦略の 69 アイテムの内，優先順位の高いアイテムについて活動実施し，概ね計画に従い活動が出来たと認識している．個人情報保護法対応に関しては 1 年前倒しに実施，情報セキュリティに対するグループ各社の意識向上も図れた．また，緊急対策に関しても，顧客情報保護の基本方針や，システム開発時における顧客機密情報の取扱要領等を制定しグループ各社への対応を図った．今年度は総合戦略の 2 年目を迎え，日本ユニシスにおいては ISMS 認証取得対象をスタッフ部門から営業部門に広げ，グループ各社においても ISMS の認証拡大計画を推進中である．昨年一年間は，啓発活動や，セキュリティ文化が根付く事を最優先に対応し「情報セキュリティ総合戦略」を推進してきたが，この一年間の経過で新たな推進課題が見えてきた，本章では以下の主要課題について述べるものとする．

5.1 グループ企業との推進

「情報セキュリティ総合戦略」は日本ユニシスグループ 11 社共通の戦略である．戦略の推進に当たっては，グループ各社の情報セキュリティ委員会の協力が必要である．

戦略は，総合セキュリティ推進チーム会議にてグループ各社の全体最適を考え決定するが，推進過程においてグループ各社への考慮不足が散見された．情報セキュリティ対策の実施段階になってグループ各社での推進課題が初めて明らかになる等，決して全体最適とは行かないことが多々発生した．もう一つの推進課題は，グループ各社で戦略の受け止め方に差異がある事である．ある会社は独自方針をグループ全体の方針として貫こうとしたり，全てのお膳立てを待ってから初めて動き出す会社等，推進状況にもグループ各社の考え方の違いが表れてきた．

今年度は，総合セキュリティ推進チームに主要グループ企業から常任メンバーとして参加してもらい，グループ各社と真に問題を共有し推進を図ることにより日本ユニシスグループの全体最適化を目指す予定である．

5.2 情報セキュリティ対策と投資対効果

企業を悩ませているのが,情報セキュリティ対策と投資対効果のバランスではないだろうか．情報セキュリティ対策の「あるべき姿」とは何であろうか？　どのような対策をどのレベルまで実施すればよいのか？その投資額の設定は？と色々思いを巡らせ多くの企業で試行錯誤しているようである．情報セキュリティ対策費用は，通常の IT 投資と違って投資効果 ROI として

捉える事は困難であり，情報セキュリティ投資により，新たなリターンを期待するものではないとも言われている．企業の情報セキュリティ投資として一般的なのは，今回の個人情報保護法等の法律や規制に対応するものである．これらの対応は，企業の安全性としてのブランドイメージの向上，社会的信用度の維持，顧客満足度の向上は図れるものの，あくまで「守り」の視点での情報セキュリティ投資である．

日本ユニシスグループにおいては，昨年度より「情報セキュリティ総合戦略」を掲げ，2006年度に制度化される予定の企業格付け制度において業界最高水準の格付けの取得を目標としている．日本ユニシスグループでは企業が一丸となって，情報セキュリティ対策に取り組むことにより，単に「守り」の情報セキュリティ対策ではなく，日本ユニシスグループで実証される高度なセキュリティへの取組み，各種のソリューション開発，セキュリティ基盤の構築等，数々の「攻め」の情報セキュリティ対策を実現する事を目標としている．そこで培われたノウハウをビジネス展開する事により，お客様の企業価値の向上を図るとともに，最終的には日本ユニシスグループの企業価値向上に寄与すると考えている．また，「攻め」の情報セキュリティ対策は，技術的な対策のみならず，組織的対策が重要と考えている．組織的対策を推進する枠組みとして，日本ユニシスグループ全社におけるISMS認証取得を総合戦略の大きな柱と位置付け，年度別に取得部門を設定し，具体的な目標（KPI）として推進中である．

日本ユニシスグループの「情報セキュリティ総合戦略」は，刻々と変化する社会環境への対応，ITの活用度，従業員のセキュリティへの醸成度等を加味して，柔軟に取り組んでいく事が重要と考えている．

6. おわりに

今日，経営活動を支えるインフラとして情報システムは欠かせないものになっており，情報セキュリティ対策への意識変化は眼を見張るものがある．企業における情報システムの停止はビジネスの停止を意味し，セキュリティへの取り組みの問題は経営者の問題となってきている．情報セキュリティ事故を起こした企業は，被害者ではなく加害者となり社会的責任を問われる時代となった．日本ユニシスグループでは，「情報セキュリティ総合戦略」の2年目を迎え，戦略1（人・組織）戦略2（制度）に関しては，基本的に確立された各種施策や，教育・制度の仕組みを拡大運用すると共に，定着する事が今年度の取り組みである．戦略3（技術的対応）については，種々のテクノロジと各種ソリューションを組み合わせる事により実現するが，個々のソリューションの優劣のみで選択することなく，最終的なゴールを描き，バラバラの技術が混在せぬよう，技術的なデザインとフレームワークを明確にした上で推進すべく，この一年間の活動を踏まえ，改めて計画の改訂を行っている．

情報セキュリティ対策に，「これでおしまい」は無く，永遠に継続対応する必要がある．あわせて対応スピードが最も重要であることは言うまでも無い．2006年に業界最高水準のレベルに達する事を目標として，［情報セキュリティ総合戦略］の2年目の推進を行なって行きたい．

参考文献　［1］　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（概要）

［2］（株)日本経済団体連合会 「企業の情報セキュリティのあり方に関する提言」

執筆者紹介 三　口　充　高（Mitsutaka Mitsukuchi）
現在，日本ユニシス(株)業務推進部 G-IT 資産管理室長.

大　橋　幸　江（Yukie Ohashi）
現在，日本ユニシス(株)業務推進部　総合セキュリティ戦略推進室長.