情報セキュリティマネジメントの変遷と課題

原田要之助[1]

概要

情報セキュリティマネジメントは，情報システムがビジネスに用いられて以来，情報システムの運用の概念の一部として持ち込まれた．情報システムを用いてビジネスを正確に，必要の原則に基づいて管理し，かつ，効率よく処理するための情報システムの運用プロセスでもある．この概念が定着するまでにはさまざまな試行錯誤が繰り返された．情報システムの応用範囲が広がり，組織の末端社員が利用するようになるにつれて，情報セキュリティの重要性が高まり，情報セキュリティマネジメントが重視されるようになった．1990年代には，多くの大企業で，共通の問題となったことから，体系化が進められ，さまざまなガイドラインが作成された．この中では，英国のDTIがとりまとめ，英国の国内規格，さらには，認証制度に繋がったBS7799が国際規格となり，広く用いられるようになった．日本においても，2000年以降，この規格をベースとして国内のさまざまな情報セキュリティに関するガイドラインや制度が構築されている．本稿では，2000年代以降の日本における情報セキュリティマネジメントがどのように変遷を概観し，今後の課題について述べていく．

1 はじめに

情報システムは，ビジネスを正確に，素早く，効率よく処理する目的で導入されて，利用されてきた．1980年代には，多くの大企業が情報システムを用いて，ビジネスの管理コストの低減，ビジネスの迅速化に用いられ，適用範囲を広げてきた．とくに，1980年代後半には，マイケル・ポーターの競争の戦略［1］で提示されたように，情報システムが顧客管理に用いられて，企業の競争優位の戦略的な手段として利用されるようになった． 1990年代には，チャンピーらがビジネスプロセスリエンジニアリング［2］を提唱した．これは，それまでの人手による処理の機械化という概念から，ビジネス自体を再定義して，情報システムの速度，管理できる項目数，検索機能などを前提として，人手によらないビジネスのシステム化を図るものである．この結果，新しい情報システムをベースとしたビジネスモデルが多数，考案されて，購買や取引の形態が劇的に変化した．2000年代には，情報システムがインターネットを介して，さまざまな企業間で接

1 情報セキュリティ研究科　教授

続されて，企業の情報システムへの依存が大きく進んだ［3].

情報セキュリティの位置づけは，情報システムがビジネスで利用されるようになってから，大きく変わっていった．情報システムの開発では，情報システムが外部から見えないという秘匿性があり，心ないプログラマの不正なプログラムによる不正行為が起きるようになった．これを防ぐために，さまざまな対策、例えば内部統制の強化などが行われた．ただし，情報システムは構築時の技術的対策だけでは十分でなく，運用における対策、も重要となることから，システム監査などが用いられ発展することになった．とくに，1990年以降、情報システムが経営に必須なものとして，認知度が高まると，この問題はより深刻化した．例えば，ANAの発券システムのネットワークシステムの些細なミスによるシステムダウンが航空機の正常な運航をできなくなったり，銀行のシステムが止まると企業間の決済ができなくなったりと，より，経営に重大な影響を及ぼすようになった．このような背景から，OECDが1992年に情報セキュリティのガイドラインを策定したことは,経営にとって情報セキュリティが重要な課題であることを示唆したと言えよう．以来,情報セキュリティマネジメントは,情報システムの運用の一部の概念として持ち込まれた．情報システムを用いてビジネスを正確に，必要の原則に基づいて管理し，かつ，効率よく処理するための情報システムの運用プロセスの一部と考えられたからである.情報セキュリティマネジメントの概念が独立して定着するまでにはさまざまな試行錯誤が繰り返された.情報システムの応用範囲が広がり，組織の末端社員が利用するようになるにつれて，情報セキュリティの重要性が高まり，情報セキュリティマネジメントが重視されるようになった．

本稿では、情報セキュリティマネジメントの進展をルーツである情報システムとビジネスとの関係から紐解いていくことのより,情報セキュリティの課題がどのように変化してきたかを分析して、今後の課題や方向性を探る．

2 社会の変化と情報セキュリティについて

2.1 社会に影響を与えたITの進歩

1990年以降，IT技術はさまざまに広がりを見せている。2000年以前のIT技術は要素技術の開発がベースであった．例えば，ネットワークをADSLから光にして，高速化を図るなどである．そのため，技術開発が中心でその利用面からの視点がなおざりにされたため，インフラができても十分に活用されないなどのミスマッチが起きていた．しかし，2000年以降は，利用面からのアプローチがITをリードするようになった．例えば，スマートフォンが広がりLTEと呼ばれる高速な無線の情報通信ネットワークの導入を牽引するなどである．ここでは，2000年以降，普及したIT関連技術を以下に示す.

- クラウド
- スマートフォン
- 検索サービスとこれを核としたビジネスの広がり

- 電子ショッピングの拡大（楽天，Amazon）
- 放送のデジタル化
- メディアのデジタル（写真や映像が高精細なデジタルで保存され，流通するようになっている）
- 地球人口の半数以上が携帯電話を利用（発展途上国の利用率が高まる）
- SNS の広がり
- 高速大容量ブロードバンド
- 組込コンピューターの広がり
- 車の自動運転
- スマートシティ（スマートグリッド・スマートメータ）
- 電子マネー（Bit Coin など）の拡大
- 入退出管理システムの普及
- 監視カメラのデジタル化と広がり

なお，IT 技術の今後の進歩については，マクロ予測をベースに考えておく必要がある．CPU やメモリの速度，ハードディスクの容量，ネットワークの速度については，技術的な限界があると言われながらも継続的に進歩していることが分かる[3]．これを図 2-1 に示す．例えば，半導体の内部の素子数については，内部の物理的な制約があって技術的限界に達して増加しなくなるといつも言われ続けてきた．しかし，結果的には，様々な技術が開発されて，制約を克服してきている．したがって，社会科学的には，図 2-1 のマクロの推移モデルをベースに今後の将来像を想定しておくことが必要であろう．

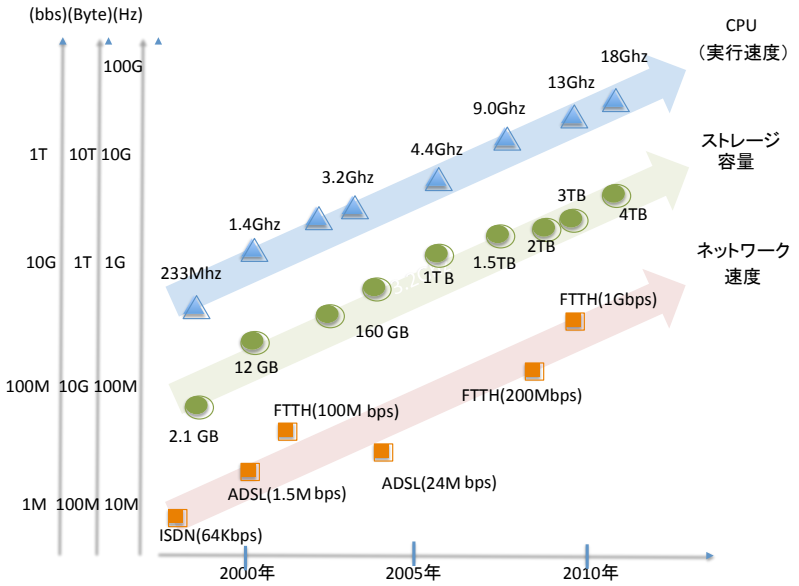


図 2.1　CPU，ストレージ，ネットワークの進歩は継続している　（文献[3]より）

2.2 社会状況の変化

社会情勢はこの10年に大きく変化している．大きなトピックとしては，以下のような項目が挙げられるであろう．まず， 地球温暖化が進み，これに対処するために情報システムが広く用いられるようになってきている．現在は，メッシュに張り巡らされた雨量，風速，温湿度を始め，空気中の成分分析などのセンサーから集められた気象情報や気象衛星からのモニタリング情報を元にして気象の現状を把握し，スーパーコンピュータを用いて数時間先の気象が予測され，メディアやインターネットなどを通じて広く活用されている．とくに，異常気象により局地的な洪水などの災害を事前に予知して生命や財産を守るのに広く活用されるようになっている．また，インターネットの高速化．広帯域化により，クラウドサービスが広く使われるようになった．この結果，企業にとっては，情報システムを最寄りの事業所などに設置する必要がなくなった．すなわち，大企業のみならず，中小企業もインターネットを企業間の情報流通や顧客からの直接の受発注やコミュニケーションに活用するようになった．この結果，企業規模や地理的な条件が企業間競争の制約にならなくなった．さらに，携帯電話などを含めたITの活用はグローバルに広がり、経済的な恩恵をグローバルに広げただけではなく，テロリストのような集団にも広く活用されるなど，弊害も大きくなっている．今後の社会を考えていく上で，情報システムを付加的なものではなく，社会を構成する不可欠の要素と見なすことが求められていると言えよう．社会に影響を与えたトピックを以下に示す．

- 地球環境の変化（温暖化や異常気象）と自然災害の増加→IT によるモニタリングシステムと減災に向けた情報共有
- グローバル化（経済，取引，流通，旅行，情報，・・・）
- 企業への IT の普及（全企業の 99%が PC を活用）
- テロの頻発→テロリストも IT を利用
- 中国，インド，ロシア，ブラジル，南アフリカなどの経済発展→携帯電話やインターネットを利用
- EU の拡大（27 カ国）

2.3 関連法制度の変化

社会がITを広く活用するようになり，社会経済のさまざまな分野で使われるようになると，さまざまな，社会的な問題が起きる．例えば，個人情報はITが広く活用される前には，紙で管理されていた．そのため，紙がコピー機で複写されて持ち出されるリスクはそれほど高くなかった．また，一度に持ち出される量も限られていた．一方，小型のUSBメモリには数ギガの容量のものもあり，これには，1,000万人を超える個人情報を記録できる．また，コピーする手間も，複写と比べると極めて簡単である．したがって，企業などが，紙で実施していた管理方法をそのまま

USBの管理に当てはめると齟齬がでてしまう．個人情報はデータベース化されるとさまざまな活用が可能となり，多くの企業が利用するようになるのは明らかだ．このような背景で，個人情報保護法が施行されたのは自然な成り行きと言えよう．ただし，個人情報保護法も，完全施行から10年経って，ビッグデータを扱う法律としては不備が目立ってきたため，2015年に向けて改正が進められている．

とくに，この10年のITに関連した法律を見てみると，多くの社会問題が起きて，既存の法律では十分に被害者の権利を守れない，違反事項にあてはめられないなどのため逮捕や規制できないなどで立法化されたものが多いと言えよう．

さらには，情報セキュリティに関連するものが多いのも特徴である．とくに，挙げられるのは，2003年以降は，さまざまな法律や制度が作られている．特徴的なものを以下に示す．

- 個人情報保護法完全施行（2005）
- 金融商品取引法の内部統制報告書制度（2007）
- 特定電子メールの送信の適正化等に関する法律（2008）
- 不正競争防止法の改正（2011）
- 不正アクセス禁止法の改正（2012）
- 不正指令電磁的記録：ウイルス作成罪（2011）
- 著作権法改正（2012）
- プロバイダ責任制限法（2007）
- 情報セキュリティ監査制度（2003）
- 情報セキュリティガバナンス制度（2005-2010）

2.4 事件・事故について

2005年以降の10年間の情報セキュリティに関連する事件・事故を，機密性，完全性，可用性の3つの観点から見ていく．まず，機密性については，個人情報漏えい事件だけに限定しても，さまざまな事件や事故が起きている．JNSAは2005年以降，10年間継続して個人情報漏えいについて調査を実施してきている．2011年からは情報セキュリティ大学院大学も協同で調査を実施している．この調査結果を見ると，事故件数が減少していないことが分かる［4］．

◆ 機密性（個人情報漏えい関連）

- Winny利用ＰＣのウイルス(ワーム)（2005）
- Sony子会社へのハッキングによる個人情報の盗みだし（2011）
- 米復員軍事省の管理する退役軍人の約2,000万件の個人情報漏えい（2006）
- 自衛隊のイージス艦機密情報内部漏えい事件（2007）
- 標的型攻撃（事件名？）
- ベネッセによる大規模個人情報の持ち出し事件（2014）

◆ 可用性・完全性

- 全日空の発券システムで障害(2007)
- ファーストサーバの障害とデータ消失(2012)
- みずほ銀行システム障害（2011）
- Gumblerウイルスによる改ざん被害（2009）
- 東京証券取引所システム障害（2005）
- 311東日本大震災に伴う情報システムへの被害（2011）

2.5 情報セキュリティのマネジメントの変遷

情報セキュリティのマネジメントは，時代の技術（例えば，携帯端末やスマートフォンで企業の情報が使われるようになってMDMが必要となった）や時代が要請する規範（例えば，個人情報保護法が制定されて以降，情報管理が厳しく実施されるようになったなど）によって大きく変わってきている．

(1)1990年代前半のセキュリティマネジメント

・メインフレームの情報セキュリティ

1990年代は，企業の情報システムは基幹業務においてはマインフレームが使われており，周辺業務から，コストパフォーマンスのよいミニコンやオフコンが利用されるようになった．これらの情報システムは，マシン室に設置されて情報システム部門が管理することが多かった．そのため，情報セキュリティのマネジメントは，情報システム部門が実施することが多く，マシン室の物理的なセキュリティや企業内の情報システムの一部の利用者に対するIDやパスワード管理が中心となっていた．ネットワークは専用回線でマシンと接続することが多く，企業の情報の漏えい対策として，回線への暗号化やリモートの端末からの情報漏えい防止が中心となっていた．

・黎明期のパソコンと情報セキュリティの管理

パソコンは，大企業では，部門内部の出張費や経費の計算処理などに使われていたため，全社的な情報セキュリティの対象とされることは少なかった．一部の業務では，パソコンを端末としてメインフレームに接続することが一部で，始まっていた．しかし．パソコンの利用は専用端末としての使い方に限られていた．そのため，メインフレーム側で管理すれば十分という認識が一般的であった．すなわち，黎明期のパソコンについては，情報システム部門では情報セキュリティの対策の対象とはされていなかった

・中小企業のパソコン利用の始まり

中小企業において，能力の高まってきたパソコンを用いて企業会計，受発注管理，在庫管理などに使われ始めた．能力の高いパソコンと通常のパソコンをネットワーク接続して利用するパソコンLANが先駆的に使われ始めた．すなわち，中小企業においては，パソコンによる情報の完全性や可用性については，企業全般に影響を与えるため，全社的な情報セキュリティの確立が必要とされたが，対策に多額の費用を支出するまでには至らなかった．

・パソコン通信とインターネットの利用

個人を中心に、個人のパソコンから，電子メールを送受したり電子掲示板に意見を表明するパソコン通信[2]がはやり始めた．一部の企業がパソコン通信をビジネスで使い始めたが，多くは，電子メールの利用にとどまった．一方，1993年頃からそれまで大学や研究機関が主に利用していたインターネットの利用がIT企業を中心に広がり始めた．今までは，海外の情報を調べるためには多大な費用が掛かっていたが，

・情報セキュリティマネジメントのガイドラインの状況

英国のDTI(Department of Trade and Industry)のもとで，英国の大企業が集まって情報セキュリティの管理策をまとめた．これらの企業は，ネットワークを接続したり，情報を交換したりするときに，相手の情報セキュリティの管理状況が分からないままに，自社の機密情報を相手に渡せない．そこで，企業で共通に実施されているベースラインとしてのセキュリティ管理について 1992 年に調査を実施して，その結果をまとめた．企業間での取引に関係することから DTI がまとめ役となったものの，国による規制にすると貿易上不利となるので，自主的なフレームワークと考えて，DISCPD0003”Code of practice for Information Security Management” [5]とした．この規範は，様々な企業の参考になること，規範を維持管理する必要があることから，英国の BSI(British Standard Institute 英国規格協会)が，英国の規格 BS7799-1 [6]として引き継ぐことになった．この経過を図 2-2 に示す．

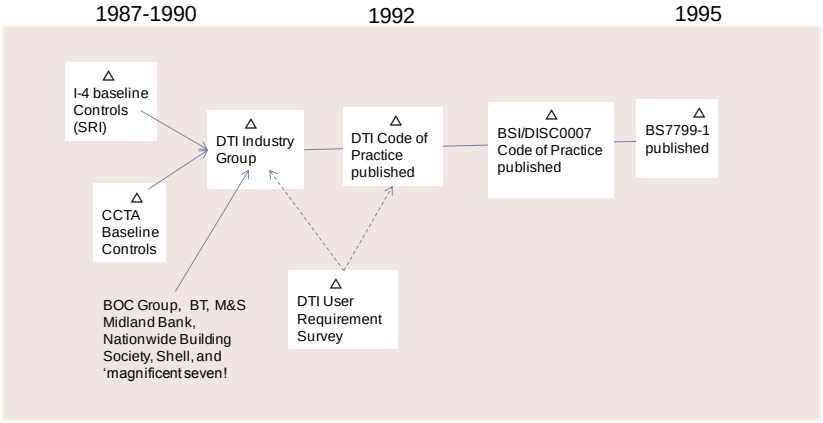


図 2-2 1990-1995 年の情報セキュリティマネジメントガイドライン

(2)1995-2000年代のセキュリティマネジメント

・メインフレームの情報セキュリティが中心

1995年以降は，大企業において，ダウンサイジングが本格化した．すなわち，企業の情報システムに対して，小型のミニコンや高性能はワークステーションをネットワーク

[2] パソコンを電話回線によるダイヤルアップ接続でホストマシンに接続して，共同利用するサービス

で接続して利用することで，メインフレームに比べてコストを劇的に節約できるようになった．また，パソコンもOSにネットワーク対応機能がビルトインされ，直ぐにネットワークに接続して使われるようになった．企業の情報システムがネットワークに依存するようになった始まりでもある．このような複数のシステムをネットワークで接続することから，ネットワークセキュリティの重要性が認識されるようになった．

周辺業務から，コストパフォーマンスのよいミニコンやオフコンが利用されるようになった．これらの情報システムは，マシン室に設置されて情報システム部門が管理することが多かった．そのため，情報セキュリティのマネジメントは，情報システム部門が実施することが多く，マシン室の物理的なセキュリティや企業内の情報システムの一部の利用者に対するIDやパスワード管理が中心となっていた．ネットワークは専用回線でマシンと接続することが多く，企業の情報の漏えい対策として，回線への暗号化やリモートの端末からの情報漏えい防止が中心となっていた．

・ビジネスに使われるようになったパソコン

一部の先進的な企業では，安価になったパソコンが企業内に広がり，各個人がデスクに１台のパソコンを持ち，電子メールや部門の共通ファイルなどにアクセスしたり，企業の基幹システムにアクセスしたりして業務を遂行するようになった．一方，パソコンは，企業の一部の部門内部の計算処理などに使われていたため，情報システム部門が全社的な情報セキュリティの対象にすることは少なかった．基幹システムへアクセスする利用者管理，パスワード管理，データベースの管理に限られていた．

一方，パソコンの多くは，手軽にダイヤルアップでホストコンピュータに接続できるようになっており，電子メールや外部のサーバと接続して，ウイルスを持ち込み，企業内のパソコンに広がる事件が起きるようになってきた．そのため，企業では，これらのパソコンのウイルス対策が中心の課題となっていた．

・西暦2000年問題

1998年以降の情報システム部門にとっての一番の課題は，西暦2000年問題と呼ばれる，情報システムのプログラムの時刻表記が2000年になることで，プログラムの誤動作が起きる可能性に注目が集まった．これは，情報処理において年号を扱う際に，4桁の数字ではなく，下2桁とすることで情報システムの内部のメモリを削減でき，計算処理を効率化できたからである．また，情報システムが様々なシステムと接続されているため，表記法を合わせないと誤動作する可能性も指摘された．そのため，2000年になる前に利用している情報システムの全てのプログラムを洗い出す必要が起きた．これの対処法は，ソースプログラムに立ち戻って，人海戦術で調べていくことであった．情報システム部門の多くのリソースがこの対応に回されて，情報セキュリティ対策の優先度は落とす企業や組織が多かった．

▪・情報セキュリティのガイドラインの重要性が高まる

多くの企業では，ホストコンピュータ時代には，限られた利用者のみを対象にセキュ

リティ対策を実施すればよかった．しかし，さまざまなビジネスに情報システムが利用されるようになり，利用者も利用方法も大きく変わっていった．また，多くの企業で，遠隔地から情報システムにアクセスすることや関連会社の情報システムと接続することが始まったことから，情報システムの管理や情報セキュリティを組織内部で，どのように管理するか，また，複数に情報システムの管理をどのように統一するかが重要な課題となり，企業は独自にセキュリティのポリシーを策定したり，ガイドラインを作成したりするようになった．日本では，情報システム監査基準が策定されて，セキュリティを含む情報システムの管理に用いられるようになった．また，2000年には政府が，情報セキュリティの管理を高める観点から，情報セキュリティのポリシーを策定することを企業にも求めるようになった．

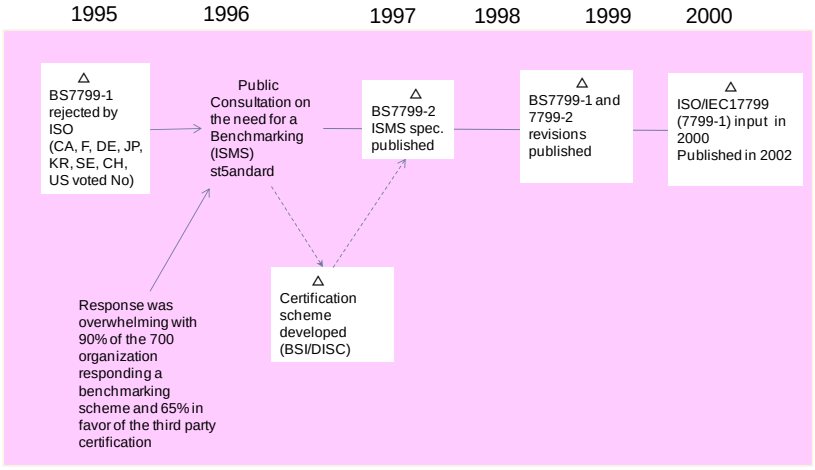
一方，BSI（英国規格協会）では， 1995年当時，品質や環境の国際認証をリードしており，BS7799-1も，国際間で企業が情報セキュリティを国際間で取り決めする際の利用に適しているとして，国際規格としてISOに提唱した．しかし，標準化を担当しているISO/IEC JTC 1/SC 27 - IT Security techniques （情報セキュリティの標準化を担当しているグループ）では，主要国が基準の必要性に疑問を呈して反対した結果．国際規格化は見送られた．

なお，日本では，後年，BS7799-1が紹介されたときに，この実践規範は誰もが従うべきガイドラインと誤解された．これは，多くの日本企業は，省庁などからのガイドラインを利用するという受け身の企業が多かったため，フレームワークなど自社の都合で決めるという新しい概念の取扱いに苦慮したためである．また，多くの企業担当者にとっては，“お上からの通達”の方が，内部での意思決定が楽であったという企業カルチャにもよる．このように，企業からの要請が多かったため，結局は，経済産業省が，JIS X.5080[8]をベースに情報セキュリティ管理基準V.1[9]を2003年に策定している．

1997年には経済産業省では，情報処理サービス業情報システム安全対策実施事業所認定基準[10]を策定して，事業者を認定する制度を準備していたこともあり，英国からのBS7799-1の国際規格化に反対している．ただし，日本企業の一部には，既にDTIの翻訳も出回っており，セキュリティポリシの策定や内部のセキュリティ基準としての利用が始まっていた．さらに，グローバルな企業にとっては，国内と国外で規格が異なることへの反対もあった．

英国では，BS7799-1を利用する組織が増えており，この規格をベースに情報セキュリティを構築していることの認証ニーズが顕在化していた．そこで，1997年に情報セキュリティマネジメントの要求条件をBS7799-2[12]として制定し，この要求条件をもとに国内を対象にした認証制度を開始した．これらの規格は1999年に一部改訂された．また，各国とも，企業が情報セキュリティマネジメントの国際規格を必要としていることから，2000年にBS7799-1が国際規格ISOIEC7799:2000となることを承認した．この経過を図2-3

に示す.



7

図 2-3　1995-2000年の情報セキュリティマネジメントガイドライン

(3)2000-2005年代のセキュリティマネジメント

・企業の情報処理量の拡大と基幹システムのダウンサイジング

中堅企業ではパソコンとパソコンを相互に接続するローカルネットワーク（LAN）が普及して多くの従業員がパソコンとネットワークに接続されたサーバを共通に使うことで，ビジネス情報の共有が図られ，多く業務が情報システムで実施されるようになった．すなわち，パソコンとサーバによる情報処理形態が企業の内部に広がっていった．さらに，基幹システムを大型のホストコンピュータからサーバとパソコンで処理する形態に移行する企業も増えていった．この現象はダウンサイジングと呼ばれ，多くの企業に広がった．また，戦略的に顧客を囲い込むために，顧客情報を情報システムのデータベースに保存して使うようになった．企業の従業員の多くが電子メールを利用し，サーバにアクセスできるようにするため，情報システム部門が個人へのIDの不要やアクセス権の設定することになった．

・ネットワーク時代（インターネットのインパクト）

大学や研究機関が中心に利用していたインターネットが個人に急激に広がったことや，インターネットをベースにした新しいビジネスモデルを構築したベンチャー企業のビジネスモデルが既存企業のビジネスに影響を与え始めた．とくに，例えば，AMAZONやYahooなどが顧客への物販ビジネスに影響を与え始めた．そのため，多くの企業が，インターネットをビジネスで利用するようになった．

また，インターネットの利用拡大で，ネットワーク機器が劇的に低下したことで，インターネットプロトコルを様々なシステムの接続にも利用するようになった．そのため，多くの企業で，企業内LANとインターネットを接続する形態が急激に伸びた．

・ネットワークセキュリティ

ネットワークで様々な情報システムを接続することから，ネットワークに関する情報セキュリティが注目された．とくに，インターネットは，接続されたあらゆる機器にアクセスできるため，企業にとっては，内部の情報を保護する必要がある．すなわち，外部のインターネットと内部のネットワークを接続する境界には．ファイアーウォールを設置して，不要な外部からのアクセスを遮断，外部からのWebサーバへのアクセスを許可するDMG（非武装地帯）の設定，外部からのアクセスの監視などのネットワークセキュリティが重要な課題となった．また，外部から内部の情報システムにアクセスできるための，アクセス制御も重要なテーマとなった．

・企業の情報セキュリティマネジメントが重要な課題となる

企業では，ビジネスがネットワークに接続されたパソコンやサーバに移行した結果，全ての従業員にIDを与えたり，サーバへのアクセス権を付与したりすることが重要な業務となった．また，ネットワークの機器の接続や設定，日常の運用管理，監視、不正利用対策などの業務量が急増したため，情報システム部門で対応が難しくなった．多くの企業では，業務量が膨大で，人手を必要とすることから，これらの情報セキュリティ関連業務を洗い出して，情報セキュリティマネジメントとして体系化することが増えてきた．ちょうど，この頃，ISMSが認証として利用されるようになってきたため，これをベースに情報セキュリティマネジメントを導入する企業が増えてきた．また，これらの業務を実施する担当部署を設けるケースも増えてきた．

・個人情報保護への対応

2003-2005年の情報システム部門や情報セキュリティ部門にとっての一番の課題は，2004年に制定されて2005年から完全施行された個人情報保護法への対応である．個人情報保護法では，半年間に5,000件以上の個人情報を扱う事業者を個人情報取扱事業者としており，個人情報に関連する様々な対応が義務づけられている．このため，多くの企業が個人情報を厳密に関するするための対応策が必要になった．情報セキュリティ関連では，安全管理措置と呼ばれる，個人情報への物理的な保護，データへのアクセス制限，管理運用が義務づけられた．そのため，情報セキュリティ部門でも，情報システムのプログラムの変更，運用方法導入，各種のルールの整備などの対応に追われた．

・情報セキュリティのガイドライン

各国で，企業の情報セキュリティの問題が大きな課題となり，情報セキュリティを管理するためのガイドラインが策定されて使われるようになった．また，日本では，企業に情報セキュリティ対策を実施するために，経済産業省が中心となって，ISMS を推進した．このベースとなる基準としては，ISO/IEC17799:2000（JIS X.5080）[3]が管理策として用いられ

[3] ISO/IEC17799 が翻訳され，国内の JIS 基準とされる際に，技術基準を表す X が使われた．表題がマネジメントガイドラインとなっているにもかかわらず，技術基準とされたのは，ネットワークセキュリティなど技術に関係する管理策が多かったからである．

るようになった．また，この基準をベースにして情報セキュリティ管理基準が制定された．日本では，2000 年に ISO/IEC17799 の国際規格化に賛成したあと，ISMS の国内での認証制度を検討して，2001 年から，JIPDEC(情報処理開発協会)が ISMS の認証制度のパイロット事業を行い，この成果を受けて 2002 年 4 月より，ISMS の本格運用を始めた．認証規格としては，要求条件を BS7799-2，管理策は ISO/IEC17799:2000 を用いた．この経過を図 2-4 に示す．

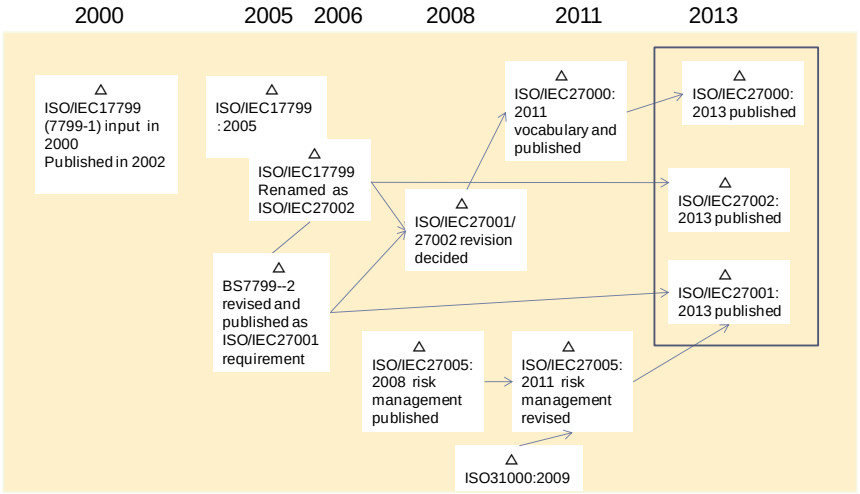


図 2-4 2000-2005 年の情報セキュリティマネジメントガイドライン

2005年には，日本や英国でのISMSの順調な進展が見られることから，BS7799-1が，ISO/IEC27001:2005として国際規格となった．また，同時にISO/IEC17799:2000も内容を見直して，ISO/IEC17799:2005が発行された．この規格は，名称を合わせることから，ISO/IEC27002:2005に名称変更された（内容は変えずに表紙のみ差し替えられた）

・情報セキュリティマネジメントの限界

2000-2005年の情報セキュリティは，情報システムの環境が劇的に変わったことから，様々な対応をすることが必要となった．また，情報セキュリティ管理基準が制定されて，企業内の情報セキュリティ対策に用いられたためである．ところが，情報セキュリティの対策については，どの企業もガイドラインを利用するものの，どのように対応するかについては，学びながら対応していくというスタイルとなったため，必要な業務量に見合った人員や人材の確保が難しかった．また，情報セキュリティの認証を目指す場合，大企業をはじめとして，情報セキュリティマネジメントの負荷があまりにも大きく，自社での対応が，人的にも技術的にも，十分に対応できないケースが散見されるようになった．

(4)2005-2010年代のセキュリティマネジメント

・情報システムの統合化

2005年以降の情報システムは，企業の多くのビジネスが情報システムを利用するようになり，基幹システムのダウンサイジングも進んだ結果，企業内部のサーバ数が増加して管理業務が急増した．また，情報セキュリティ部署が把握しない部門内サーバなどもネットワークに接続して利用されることも起きていた．しかし，情報セキュリティ部門の人員では十分に対応できないことも起きていた．この解決として，先進企業では，企業内のサーバの整理・統合を図り，全てが管理される状態を模索した．一部の企業では，重要ではない周辺業務などを外部の企業にアウトソースしたり，外部の情報サービス（後に，クラウドと呼ばれるようになる）を利用したりするようになった．とくに，管理面から，電子メールやWebサーバなどの運用・保守を外部委託するケースも増えてきた．

・企業の情報システムの外部化とクラウドの利用の本格化

情報システムについては，運用・保守にコストが掛かることや必要な人材が不足することから，情報システムの外部への委託やクラウドを利用するようになった．最初は，非コア事業での利用が中心であったが，2008年頃からは，コア事業についても，外部委託やクラウドを利用するケースが増えてきた．このため，外部に企業の重要な情報が持ち出されるなど，情報セキュリティの問題が大きくなった．クラウドのセキュリティが重要な課題として認識されるようになった．

・情報システムのID，アクセス権の管理

企業内で働く従業員，派遣社員，契約企業の社員などが，企業の情報システムにアクセスしてビジネスを実施するようになったため，IDとパスワードの管理が極めて重要になった．しかし，企業のビジネスでの従業員の就業，離職，異動などの情報は，人事部が管理しているため，アクセス権の付与や停止が情報セキュリティ部門となかなか連携されないなどの問題が起きていた．このため，先進企業では，シングルサインオンと呼ばれるもので管理するケースなども増えてきた．

・物理的セキュリティの拡充

情報を隔離する最初の方法として多くの企業では，物理的セキュリティが再認識された．1990年代以前の，ホストコンピュータの時代には，ホストコンピュータを特別な部屋に設置して，関係者以外の立ち入りを厳しく管理した．しかし，2000年以降は，従業員などにパソコンが提供され，また，部門にサーバが設置されたこともあり，これらの機器の物理的なセキュリティが曖昧になっていた．個人情報保護法への対応の必要性から，個人情報を扱う部署の隔離などが必要になり，企業の多くが，物理的セキュリティを見直した．その過程で，多くの企業が，入退室管理システムなどを導入して立ち入りを制限するようになった．また，立ち入りなどを監視する必要性から管理カメラが導入されるようになった．これらの物理的セキュリティは多くの場合，情報が集中監視システムに集められて，不正な立ち入りなどのセキュリティ違反を管理するようになった．

・情報セキュリティマネジメントの重要性の拡大

個人情報保護法が施行されたあと，個人情報を漏えいした企業はその事故について発表することが義務づけられた．とくに，2005-2007年の個人情報漏えい件数はJNSAの調査結果を見ると事件件数や漏えい総数は大きい．このため，多くの企業が，個人情報の漏えいに関するさまざまな対策をとり，自社の情報セキュリティの管理体制を整えるようになった．さらに，自社の管理体制が十分であることを示すために，ISMSやPマークの認証を取得して，自社の情報漏えい対策を実施するようになった．ISMSやPマークの認証を取得する事業所や企業は2005年以降急増した．このことから，情報セキュリティマネジメントの重要性が各企業に認識されるようになったと言えよう．

・企業の情報利活用の多様化に伴う新しい情報セキュリティマネジメントの課題

企業の従業員は，企業の外部でビジネスをする機会が増え，パソコンなどに情報を保存して持ち出すケースも増えてきた．しかし，個人情報の管理など，企業の外部に持ち出しを禁止する企業も多く，ビジネスの効率性と情報セキュリティがバッティングするケースが増えてきた．情報セキュリティ部門では，このような情報の管理をコントロールするために，ガイドラインを決めたり，監視システムを導入したりするケースも増えてきた．

2.6 情報セキュリティに関連したマネジメントシステム

情報セキュリティを企業に広げるために2000年にISMS（情報セキュリティマネジメントシステム）制度が検討された．また，2001年にISMSのパイロット試験が実施されて情報セキュリティの制度となり得ることが確認された．この結果，2003年からそれまでの安全対策事業者認定制度に変わる新しい認証制度が始まった．最初は，認証に必要となる要求条件となる規格がないので，英国規格協会（以下，BSI(British Standard Institute)という）が英国を対象に実施していたBS7799-2を用いることにした．その後，ISO/IEC27001:2005が要求条件として国際規格となってからは，この規格を要求条件として用いることになった．それまでに，BS7799-2で認証を受けていた事業所は，更新のタイミングで規格を切り替えた．なお，認証を受けている事業者数は，図2-5に示すように増加してきている．2005年に，ISO/IEC27001:2005の国際規格ができるまでは，なだらかな増加であり，国際規格移行後から2009年までは直線的に増加して約3,600事業所になった．2010年からは，増加率が穏やかになった．この結果，2014年8月末には約4546の事業者が認証を受けるまでとなった．ただし，グラフからは，認証を受けている事業者数が減り始め，2014年には，増加が止まったように見える．これは，ISOの認証規格であるISO/IEC27001:2013が改定されたことなどから，一部の事業者が認証の継続を止めたことが影響していると考えられる．長期的には，事業者にとって，情報セキュリティは避けて通ることができないテーマであり，今後も，認証事業者は増加していくものと考えられる．一方，個人情報の保護の観点から，プライバシーマーク制度が実施され，JIS Q.15000を認証の要求条件として事業者が認証を受けている．2014年10月時点で，約15,000社が認証を受けており，ISMS同様に認証企業数は増加している．類似の制度としては，日本公認会計士協会が，主に企業の内部統制の実施状況

を認証するSOCやクラウド・セキュリティ・アライアンス（以下では，CSAという）とBSIがクラウドサービスを提供する事業者に対してのSTAR認証制度がある．

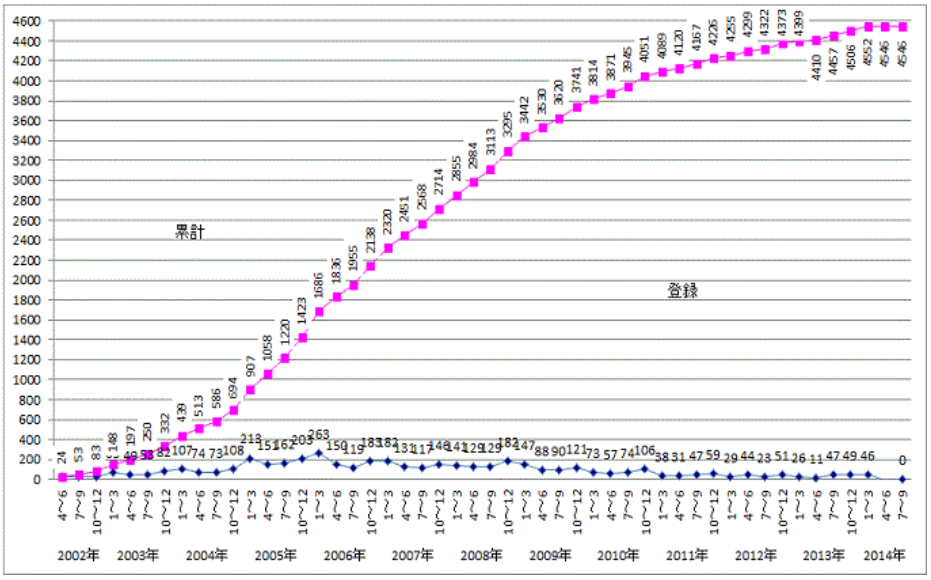


図2-5 ISMS認証事業者数の推移（2014年8月末時点）（出所：JIPDECのISMS事業者数の推移より[24]）

以上より、情報セキュリティマネジメントの課題は，以下にまとめられる

① 情報システムの発展や利用形態の変遷によって，情報セキュリティ対策が時代とともに重要な課題となった

② 企業にとっては，個人情報保護法に伴う情報セキュリティ対策が必須のものとなり，取引先や顧客に対策を実施していることを示すことが求められるようになった

③ 多くの企業にとって，情報セキュリティ対策の関連業務が休息に増えたこと，また，情報セキュリティ対策が技術的にも管理的にも多くの人材を必要としたことから，人材不足が大きな課題となった．

3 情報セキュリティマネジメントの体系化について

ISO/IEC 27001 と 27002 の規格は，ISO/IEC27000:2012[13]の用語を始め，ISMS を実装するための規格 ISO/IEC27003:2010[14]，運用で定量的な管理をする場合の測定項目に関する規格 ISO/IEC27004:200[15]，リスクマネジメントに関する規格 ISO/IEC27005:2011[16]が開発されている．これらの規格は，ISO/IEC27000 ファミリー規格と呼ばれている．これを図 3-1 に示す．なお，現在の規格の，27003，27004，27005 は 2005 年の規格と整合がとられており，ISO/IEC 27001:2013 や 2700:2013 年とは整合しない．現在，ISO/IEC SC27 で改定作業が実施されている．なお，ISO/IEC27000:2014（Overview and Vocabulary：概要と

用語）*4[17]については，ISO/IEC27001:2013 年版との対応がとられている．

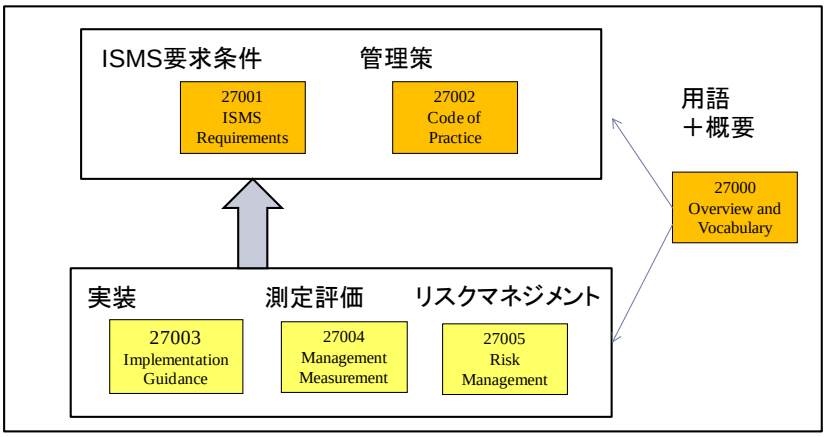


図 3-1 ISO/IEC27000のファミリー規格について

3.1 情報セキュDISC003からの情報セキュリティマネジメントの変容について

ISO/IEC27002:2013[23]は，2章で述べたように，歴史の長い規格である．DISC0003を含めると既に，20年間にわたって5つ目の版が出版されているが，基本的な章構成については，あまり変化はない．章構成について比較したものを表3-1に示す．

表3-1 情報セキュリティ管理策の変遷

ISO/IEC27002'2013	DISC PD0003	BSI7799-1	27002:2000	27002:2005
リスク分析		序文	序文	3
5 情報セキュリティのための方針群	1	3	3	5
6 情報セキュリティのための組織	2	4	4	6
7 人的資源のセキュリティ	4	6	6	8
8 資産の管理	3	5	5	7
9 アクセス制御	7	9	9	11
10 暗号	(8)	(10)	(10)	(12)
11 物理的及び環境的セキュリティ	5	7	7	9
12 運用のセキュリティ	6	8	8	10
13 通信のセキュリティ	6	8	8	10
14 システムの取得，開発及び保守	8	10	10	12
15 供給者関係	–	–	–	–
16 情報セキュリティインシデント管理	–	–	–	13
17 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	9	11	11	14
18 順守	10	12	12	15

*4 この規格は 2010 年，2012 年，2014 年に改定されているので，利用するときには注意されたい．

まず，DTIのDISC0003では，企業の情報セキュリティに関する共通の基盤とするための最小限の情報セキュリティ対策がリストアップされている．また，コントロール目標やコントロール（管理策）という概念は述べられていない．これが，BS7799-1に引き継がれた時点で，リスクベースの概念が導入され，リスク分析を実施して，セキュリティの要求条件を明確にして，管理策を選択するという概念が持ち込まれた．これば，現在のISO/IEC27002のベースとなっている．

なお，リスク分析については，2005年の改訂の時点で，この基準だけで情報セキュリティマネジメントとしての一貫したリスク分析からリスク対策，管理策の導入，見直しができるようになった．これは，BS7799-2が国際規格となっていないためである．しかし，情報セキュリティマネジメントの全体像が示された事は大きい．これによって、情報セキュリティマネジメントが体系化されたと言えよう．ちょうど，2章に述べたように，企業の利用部門での情報システムの導入が進み，ビジネスにとって情報セキュリティは必須のものと時期を一にしている事が分かる．なお，2013年の改定版では，ISO/IEC27001と27002での規格の作られたタイミングの違いで，ずれが生じていた部分や齟齬がある部分の修正が実施されるとともに， 2010年以降の新しいサイバーセキュリティや外部委託に伴う情報セキュリティにフォーカスが当たっている．また，ネットワーク機器などの設定や運用がシステムで行われるようになり，情報セキュリティマネジメントの中止ではなくなったことから，管理策の多くが見直されて削除されている．これも，時代の趨勢を受けたものとなっている．

まとめ

本稿では，情報セキュリティマネジメントを情報システムとの関係で分析した．その結果，情報システムの形態や利用方法，さらには，ビジネスとの関係で，情報セキュリティマネジメントは大きく変遷していることが分かった．また，ISO/IEC27002 の国際規格のルーツや数度にわたる変遷を見ると，情報セキュリティマネジメントの体系化はなされているものの，具体的な管理する対象が変わってきていることが分かる．

今までに，起きたことをベースに見ていくと，今後も，情報システムの技術の進歩，ビジネスの利用の変化によって，情報セキュリティマネジメントの対象が変化していくことが想定される。すなわち，情報セキュリティマネジメントは，これらの変化に追随して行く必要があることが分かる．

謝辞

本稿をまとめるにあたって，情報セキュリティ大学院大学の教員，研究室の学生や研

究生から得られた温かい助言や調査への協力に感謝する.

参考文献

［1］ マイケル・ポーター、競争の戦略、ダイヤモンド社、1982
［2］ マイケル・ハマー、ジェイムス・ジャンピー、Reengineering the Corporation: A Manifesto for Business Revolution、1993
［3］ 原田要之助、通信のダウンサイジングとブロードバンドインターネット、pp.98－108、OutLook 2002、情報通信総合研究所、2002
［4］ 岩本敏男、IT幸福論 pp.47、東洋経済新聞社、2013
［5］ DTI, DISC PD0003, Code of practice for Information Security Management, DTI, 1993年9月
［6］ BS7799-1, Code of practice for Information Security Management, 1997 年9月
［7］ ISACA, CobiT(Control Objectives for IT) version 3, 2000年
［8］ JIS X5080:2002 情報技術－セキュリティ技術－情報セキュリティマネジメンの実践のための規範－, 2002年（廃止）
［9］ 経済産業省, 情報セキュリティ管理基準 （平成15年に経済産業省告示第112号として制定され, 平成20年に改正),
www.meti.go.jp/policy/netsecurity/.../IS_Management_Standard.pdf, 2014年1月アクセス
［10］ 経済産業省, 情報処理サービス業情報システム安全対策実施事業所認定基準（通商産業省告示406号), 1997年制定, 2001年廃止
［11］ ISO/IEC 17799:2000, Code of practice for Information Security Management, 2000年
［12］ BS7799-2, Information security management systems -- Requirements, 1997
［13］ ISO/IEC 27000:2012, Information security management systems - Overview and vocabulary
［14］ ISO/IEC 27003:2010, Information security management system implementation guidance
［15］ ISO/IEC 27004:2009, Information security management measurements
［16］ ISO/IEC 27005:2011, Information security risk management
［17］ ISO/IEC 27000:2014, Information security management systems - Overview and vocabulary
［18］ ISO, Annex SL(normative) Proposals for management system standards, www.unit.org.uy/misc/AnexoSL.pdff, 2014年1月アクセス
［19］ ISO/TMB/TAG対応国内委員会事務局,ISOマネジメントシステム規格の整合化に関して

（ISO/TMB/TAG13-JTCGの動向），2012年5月，
www.jsa.or.jp/stdz/mngment/PDF/mns_4.pdf，2014年1月アクセス

［２０］ ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements，2013年

［２１］ ISO 31000:2009 - Risk management（JIS Q31000:2010 リスクマネジメント-原則及び指針），2009年

［２２］ ISO Guide 73：2009，Risk management-Vocabulary，（JIS Q0073：2010（リスクマネジメント用語），2009年

［２３］ ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls，2013年

［２４］ NPO日本ネットワークセキュリティ協会，情報セキュリティ大学院大学，2011年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，2012年9月