大学情報基盤における ISOマネジメントシステムの導入と効果

長谷川　孝博，松村　宣顕，永田　正樹

本稿では，情報システムにおける国際規格 (ISO) のマネジメントシステム ISMS，ITSMS，BCMS の基本機能と役割について述べている．さらに，国立大学法人のクラウド情報基盤における ISMS と ITSMS の統合マネジメントシステムが果たしてきた役割と効果について詳述している．情報セキュリティ維持と利用者満足度向上の観点から，情報基盤の運用におけるマネジメントシステムの重要性を明らかにする．

キーワード：ISMS，ITSMS，BCMS，マネジメントシステム，クラウドコンピュータ，情報基盤

1. はじめに

マネジメントシステム (MS: Management System) に，即効性のある組織改革の効果を期待することは難しい．情報システムに関する ISO の MS は，少なくとも 1 年の周期の PDCA (Plan-Do-Check-Act) サイクルを運用規範としている．社員数が数十名の組織であれば，初期の計画 (Plan) と運用 (Do) だけで 1 年程度の歳月が必要である．初期の監査 (Check) では複数の不備や不適合の指摘がなされ，多くの是正措置 (Act) を必要とする．それまでの通常業務に加え，MS の要求要件に従う一見して非効率にも思えるマネジメント活動をあわせながら 1 サイクル目を回しても，まだそれは MS の始まりに過ぎない．MS の真価は，複数年にわたるサイクルをかけた先に見えてくる．たとえば 10 サイクルは一つのよい区切りになる．

一方，近年の ICT (Information and Communication Technology) の進化は目覚ましい．コンテンツは，テキスト，画像，音声，動画，3 次元へと進化し，世界規模の通信に乗せるデータ量は指数関数的に増大を続けている．これらを取り扱う ICT サービスもまた多様かつ高度な進化を迫られている．世界規模の圧倒的な利用者数の通信需要が錯綜する混沌には悪意がはびこりやすくなる．インターネット上の脅威もまた巧妙な進化を遂げている．セキュリティ装置が攻撃の通信やマルウェアを識別するためのパターンファイル (signature) は 24 時間の更新周期でも十分ではない．情報基盤が提供する情報サービスの進化は 10 年一昔の印象が強い．

はせがわ　たかひろ，まつむら　のりあき，ながた　まさき
静岡大学情報基盤センター
〒 432–8561 静岡県浜松市中区城北 3–5–1

本稿では，組織構成員数約 12,000 名の国立大学の情報基盤において，速攻の進化を緩めない ICT サービスを，遅効性のマネジメントシステムで，15 年にわたり運用してきた効果をまとめる．

本稿の前半では，ISO の MS において，情報システムに係わる主要な MS として ISMS [1]，ITSMS [2]，BCMS [3] の役割について詳解している．後半では，国立大学法人のクラウド情報基盤における ISMS と ITSMS の統合 MS による運用を例に，MS の管理策とその効果について論じている．本特集の趣旨を踏まえ，新規性の論述と資料を随所に含めたが，過度の強調はしていない．情報基盤が MS の運用効果を含む組織の総合力で造られ，維持されていることを伝える論述に重きを置いている，あらかじめご承知いただきたい．

2. 砂漠のオアシスとマネジメント

情報システムのマネジメントを砂漠のオアシスで考える（図 1）．砂漠の脅威を知らずに無防備なままさまよい歩く状況は，無防備と無警戒でネットサーフィンをしている状況と似ている．1) 命のより所となるオ

図 1　砂漠のオアシスにマネジメントを考える

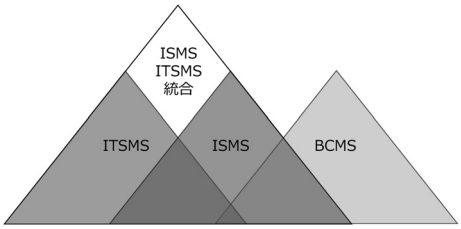

図 2　マネジメントシステムの重なりと統合マネジメントシステムの狙い

アシスの泉に最初に求められるのは，飲んで生きながらえることのできる安全性である．ひとたび安全な水が手に入れば，2) 飲んで美味しい付加価値や利用者満足度の向上を図る．安全で美味しい水まで手に入ったならば，おおかたここで満足してしまうのが人間の常であるが，3) 泉が突然消失してしまう天災や外的要因からの破壊を想定し，備蓄や復旧訓練のある堅牢な営みへと進化させることもある．これらの取り組みを情報システムに置き換えると，1) 安全を守るマネジメントが ISMS: Information Security Management System (ISO/IEC27001), 2) 利用者満足度向上のためのマネジメントが ITSMS: IT Service Management System (ISO/IEC20000-1)，3) 事業継続のためのマネジメントが BCMS: Business Continuity Management System (ISO22301) に対応する．

各 MS は完全独立した規格要件で成り立っているのではなく，裾には共通の重なりがある．たとえば適用範囲を定める，基本方針を定める，組織や人員の役割などを定めることは，いずれの MS にも共通に必要なため，規格の改編によって，これらの共通化が進められている．ISMS の運用コストを 100，ITSMS の運用コストを 100 と仮定した場合，ISMS と ITSMS を併行運用しても合算の運用コストは 200 未満，たとえば 150 や 160 程度に抑えられる．このような二つ以上の MS を同時運用することを統合マネジメントシステムという．図 2 に示すように統合マネジメントシステムの真価は，運用コストが単純和にならないことではなく，異なる MS の統合運用によって単体の MS は到達しえない MS の高みを目指すことである．

紀元前より人，物，金の資源のマネジメントにより組織の経営活動は行われてきた．そこには経営資産としての「情報」が含まれていたはずであるが，人，物，金の経営資源と比べれば，それほど大きな資産価値や経営上のリスクをもちえなかったことは想像にたやすい．情報は経営拠点の周辺域に限定された価値であったであろうし，遠く離れた机上から盗み取られることもなかった．世界規模に情報ネットワーク化された近代社会は，人類の数十万年の営みにおける瞬きのような短時間に訪れた．そこでは，ひとたび情報の扱いを誤ると，経営の根幹を揺るがす事態を招くようになった．古からの経営資源に「情報」の資産を組み入れたマネジメントの必要性が認知されるようになった．「情報は経営資産である」との考えである（図 3）．

図 3　情報は経営資産である (Information is an asset)

表 1　情報システムに係わるマネジメントシステムの認証組織数（2019 年 5 月）

MS タイプ	規格番号	認証組織数
ISMS	ISO/IEC27001	5,838
ITSMS	ISO/IEC20000-1	202
BCMS	ISO22301	94

3.　ISMS, ITSMS, BCMS

各 MS の認証組織数を表 1 に示す．組織の安全を確保するための ISMS の認証組織数がほかの MS と比べて桁違いに多い．そこで，ISMS を軸に据えながら，ITSMS，BCMS の各 MS の役割をみていく．

3.1　情報の価値：機密性，完全性，可用性

ISMS によれば，経営資産としての情報の価値として，機密性 (Confidentiality)，完全性 (Integrity)，可用性 (Availability) の三つの観点が規定されている（図 4）．情報の CIA と称して語呂がよい．

それぞれ次を意味する．

- 機密性：情報を漏らさないことの価値．認可されてない個人，団体等またはプロセスに対して使用不可または非公開にする特性
- 完全性：情報が正確であることの価値．資産の正確さおよび完全さを保護する特性
- 可用性：情報サービスを止めないことの価値．認可された個人，団体等が要求したときに，アクセスおよび使用が可能である特性

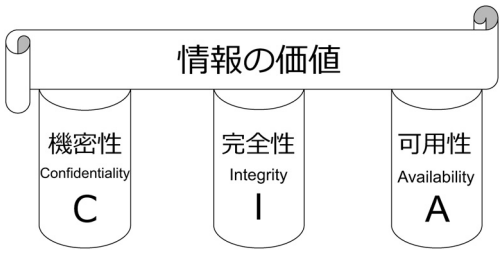

図 4　情報価値の 3 観点：機密性，完全性，可用性

いずれかの価値が，組織内外の要因によって，損なわれるとき，情報セキュリティ事故（または情報セキュリティインシデント）が起きたという．機密性の価値は，漏洩によってその価値が損なわれる，最もわかりやすい観点である．話題性も事欠かないため，社会では機密性の価値のみが情報の価値のように捉えられているような印象を受けることもある．電子情報ばかりではなく，顧客から紙面で回収した個人情報も，漏洩によって深刻な経営打撃を受けるのであれば高い機密性の価値をもつと判断する．機密性の高い情報が消失しただけなら次に示す可用性の事故である．

可用性の価値が損失した状況は，メールサーバや WEB サーバの障害，ネットワーク完全停止などの広範囲な障害から，一刻を争う緊急連絡時にスマートフォンがバッテリー切れで使えなかったという身近な事故まで想定される．どこまでを情報資産とするかは ISMS 上の構築の目的によるが，経営や運営に打撃を与えるのであれば有形・無形，電子・用紙を問わず情報資産として取り扱うことが求められる．グレーなものは情報資産に取り込む方針である．機密性と可用性において「認可された個人，団体」の条件は，一般には ID とパスワードで認証する適用範囲内のスタッフであったり，IT サービスを受ける適用範囲外の利用者であったりする．

完全性の価値は，情報が正しいことの価値である．たとえば銀行の預金額は 1 円のズレが生じても重大なセキュリティ事故である．情報システムにおいてはネットワーク機器の設定情報がよく取り上げられる．マネジメントのマニュアルやドキュメントの最新版が正しく管理されているかも完全性の重要な監査項目の一つである．

WEB の改ざんの事故は，真の原因は機密性にあるかもしれないが，表面的には完全性の価値を損失している状態であり，原因究明と復旧のためのサービス停止を伴うため，結果的に可用性の価値まで損なわれていると判断できる．情報セキュリティ事故における価値の損失は複合的なものが多く，それゆえに，観点を整理しておくことは事故の原因を分析するうえでも重要である．

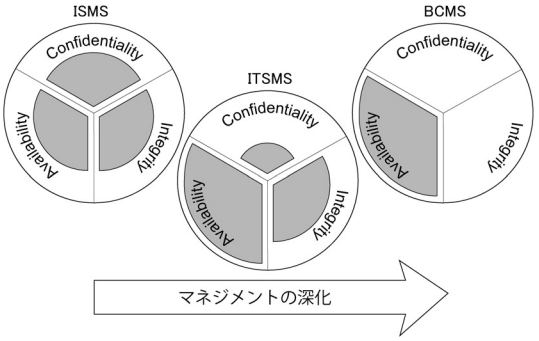

図 5　ISMS，ITSMS，BCMS のカバー領域

3.2　情報の価値と MS の役割

情報の CIA の観点で，ISMS，ITSMS，BCMS のカバー領域をプロットすると図 5 のようになる．ISMS は情報の CIA においてバランスのよい MS であり，均一に中レベルの重要度をもつ．実際にはすべて同じ重要度で運用するのではなく，その組織の目的に応じて，情報の CIA のいずれかに重心を置いた運用を行う．情報サービスが主業務の組織であれば可用性に，個人情報を大量に扱う組織であれば機密性に重心が置かれる．その組織のマネジメントの重心を CIA のどこに置くかは，情報セキュリティの基本方針や運用マニュアルにも表現される．

ITSMS は，利用者満足度向上に重きを置いた MS であり，すなわち提供する情報サービスの可用性の向上に MS の重心を寄せている．ここでは可用性を情報サービスの「使いやすさ」と読み替えてもわかりやすい．個人情報の漏洩事故が少ないサービスであることは利用者満足度の向上には必須であり，ITSMS にも機密性の重要度は存在する．

最後に BCMS は，可用性のみに重心を置いた MS である．図中にはマネジメントの深化の矢印を入れているが，これは ISMS，ITSMS，BCMS の運用の順番を意味しているのではない．実際に ITSMS や BCMS を単体で導入している組織も存在する．どの MS から着手してもその組織が提供する情報サービスの品質向上に寄与するが，図 6 に示すように方向性の違いがある．

図 6 において，横軸は情報サービスの不便と便利の軸，縦軸は安心と不安の軸である．不安は危険，安心は安全に置き換えてもよい．③象限にあるサービスは，マネジメントの不在のサービスであり，早急な改善または終息が必要である．④象限にあるサービスは ISMS

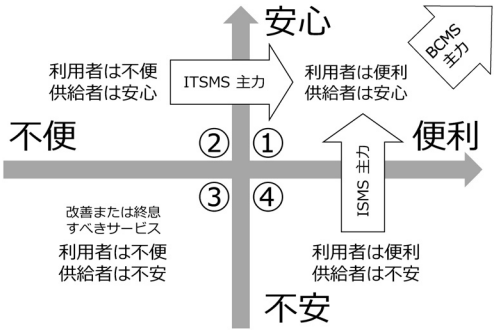

図 6　ISMS，ITSMS，BCMS の作用

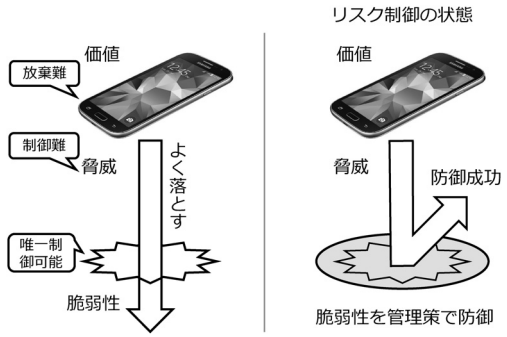

図 7　携帯端末を落下させる事故のリスクアセスメント

が①象限にリフトさせる力を発揮し，②象限にあるサービスは ITSMS が①象限にシフトさせる力を発揮する．BCMS は安心と便利の程度を補強する役割を担う．座標中のプレイヤーとなる情報サービスの供給者と利用者は，MS の活動を通して相互理解の機会を得ることになる．ISO の MS には相互理解を引き出す要求要件が多く盛り込まれている．

3.3　リスクアセスメント

本稿を展開していくにあたり，すべての MS の要求要件であるリスクアセスメントについて述べる．「リスク」とは情報の価値の CIA を損なう恐れのある危険であり，その程度を定められたリスクアセスメント手法で数値化したものをリスク値という．リスクアセスメントには再現性と比較可能性が求められる．たとえばある事象のリスク値を手法 A と手法 B で求めた結果が大きく異なったり，またある事象のリスク値を同じ手法で求めた結果が実施者 X と実施者 Y で大きく異なったりしてはならない．簡単に言えばリスクアセスメント手法をあまり複雑にしないことである．10 段階のレベル値を選択させるより，4 段階のレベル値を選択させるほうが，実施者の主観による結果の偏差は小さくなる．大規模な情報基盤にはびこるリスクは実にさまざまであり，精細ではなくとも大局を捉える簡便なリスクアセスメント手法が実用性もある． 身近な事故の例を用いてリスクモデルを述べる．図 7 は，携帯端末を落下で破壊する事故のモデルである．情報セキュリティリスク値が，価値（情報資産価値），脅威，脆弱性から構成されている簡単なリスクモデル式を先に示しておく．

$$\text{リスク値} = (\text{資産価値}) \times (\text{脅威レベル}) \times (\text{脆弱性レベル})$$

ここで，携帯端末には多くの個人情報が集積されているからといって金庫にしまう利用者はいない．資産価値を携帯することのリスクを冒しても資産を運用することの利益が大きいと判断しているのであるから，資産価値を小さくしてリスク値を小さくするのは本末転倒である．車は大事故を起こすかもしれないが手放せないのと似ている．

大切に運用していても月に 1, 2 回は落下させてしまうのだから，脅威も直接制御することは難しい．窃盗が多いからといって泥棒を自分で捕まえないのと似ている．落下の事故が頻発し，20 回目には打ち所が悪くて資産を破壊してしまった．これは，落下の脅威に対し，適切な管理策が講じられていないことが原因であった．そこで，新しい携帯にはストラップやプロテクタを付ける管理策を講じたとする．携帯が掌中から滑り落ちた回数が 100 回目で破損したのであれば，資産損壊のリスクを 1/5 に低減できたことになる．すなわち，リスク対策の基本は「脆弱性」に適切な管理策を講じ，リスク値を減じることである．情報システムでは「脆弱性 (vulnerability)」を「セキュリティホール」と読み替えるとわかりやすい．車の例では，任意保険をかけたり，定期点検をしたり，安全運転を心がけるなど，複数の対策を講じて資産の運用リスク値を受容可能レベルにまで低減している．

図 7 では，簡単のために携帯の落下という一つの脅威の取り扱いを示した．実際の情報資産では，図 8 に示すように，一つの情報資産がもつ複数の脆弱性を複数の脅威が取り巻き，資産価値を破壊したり，窃取したりする機会をうかがっている．リスクアセスメントでは，これらのリスク状態を機密性，完全性，可用性の観点から診断する．すべての情報資産の目録を作成し，重要度，機能，影響，運用マニュアル，廃棄期限，廃棄方法，所有者などを定めていく．構成員数が 1 万名を超える組織の大規模ネットワークでは，多種多様の情報資産を運用しているため，リスクアセスメントの規模と手数は大きくなる．

図 9 に示すように，リスクアセスメントによって検

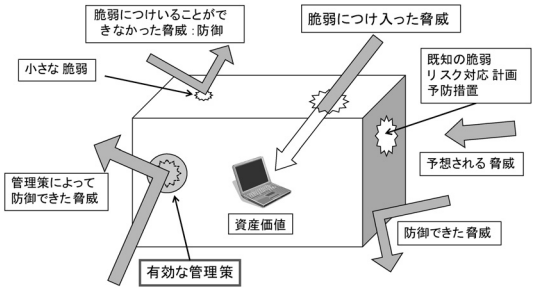

図 8　情報資産を取り巻く複数の脆弱性と脅威

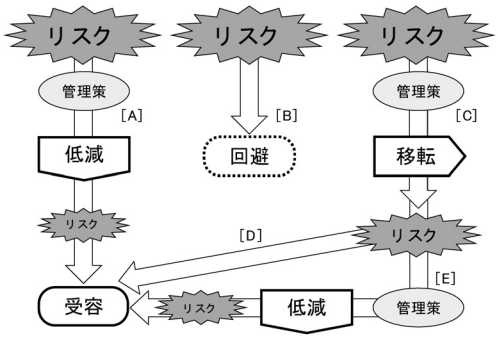

図 9　リスク対応の低減，受容，回避，移転

出されたリスクに対し「低減」,「受容」,「回避」,「移転」のいずれかの選択を行う．図 9 の [A]–[E] について述べる．リスクは通常，管理策によってリスクを受容可能レベルまで「低減」した後に「受容」する [A]．資産を放棄する「回避」は，前述のように通常は難しいが，資産価値が低い場合や，運用のリスクが利益を超えて大きい場合は選択される [B]．「移転」は，経営資源やサービスのアウトソースが相当する [C]．自組織の機密データなどを他組織に預ける必要も生じるため「回避」と同じく判断の難しいリスクの選択の一つであったが，近年では，クラウドコンピューティングサービス（クラウド）の隆盛によって広く行われるようになった．単体の管理策でリスク値が十分に小さくならない場合 [D] は，追加の管理策でリスクを受容基準以下に落とし込むことはよく行われる [E]．追加の管理策として MS オプションを選択することもできる．たとえば，ISMS ではクラウドに関するクラウドセキュリティオプション (ISO/IEC27017) が，2016 年から利用できるようになった．国内で 115 組織が認証（2019 年 5 月時点）しており，2017 年 3 月に広島大学情報メディア教育研究センターが，学術機関における初の認証を果たしている．

情報システムに関する国際規格 MS の概要について述べてきた．MS 規格書の本体はいずれも最小限の要求要件を書き並べた薄い冊子であるが，これに附随または関連するファミリ規格と呼ばれる規格書の群は多岐にわたる．ISMS では，270XX の XX に 00–11，13–18，31–34 などの規格書番号が制定（一部準備中）され続けており，情報セキュリティの MS に多角的視点が求められることをよく表している．筆者らは ISMS と ITSMS の統合マネジメントにおけるリスクアセスメントを効率よく行うための手法を提案している [4]．これらの国際規格の要求要件には OR (Operations Research) の守備範囲とする多くの課題が眠っている．

4.　クラウド情報基盤とマネジメントシステム

国立大学法人静岡大学情報基盤センター（以後，「センター」という）における ISMS と ITSMS の統合マネジメントシステムの運用を例に，本稿の題目である「大学情報基盤における ISO マネジメントシステムの導入と効果」について述べていく．センターでは，2003 年の 11 月に大学の情報系センターとしては初となる ISMS の前身規格の BS7799 を認証した．その後，2013 年 11 月に ITSMS (ISO/IEC20000-1) を追加認証し，統合マネジメントシステムの運用を始めた [5]．適用範囲を，統合マネジメントの運用を開始した 2013 年に，情報基盤センターから情報システムの事務部門へも広げた．2019 年現在，24 名の適用範囲人員となっている．これに対し，教職員と学生からなる適用範囲外の全学構成員の約 12,000 名が MS 上で定義される利用者である．組織図の概要は後半の図 14 に示している．

年単位で PDCA サイクルを回す MS 活動は，初期導入時期を除いて，短期間には劇的な変化が現れにくい組織活動である．静岡大学（以後，「本学」という）で，2010 年 3 月に完成した全学クラウド情報基盤 [6–8] もまた表面的には劇的な変化を伴っても，2003 年から継続してきた ISMS 運用上の成果の一つとして捉えている．

図 10 に，本学のクラウド情報基盤のロケーションを示す．静岡キャンパスと浜松キャンパスは約 6,000 名の同等規模のキャンパスである．2010 年に両キャンパスに設置されていたサーバ室の資産を焼津市内の商用データセンター（焼津 DC）へ完全移設した．焼津 DC 内では，国立情報学研究所が提供する学術情報ネットワーク (SINET5) [9] によりインターネットに接続している．当時はまだ学術機関におけるクラウド利用の是非が議論されている時期であり，本学のクラウド情報基盤は，大学におけるクラウド活用の先駆事例として，文部科学省の主催する学術情報委員会で紹介され

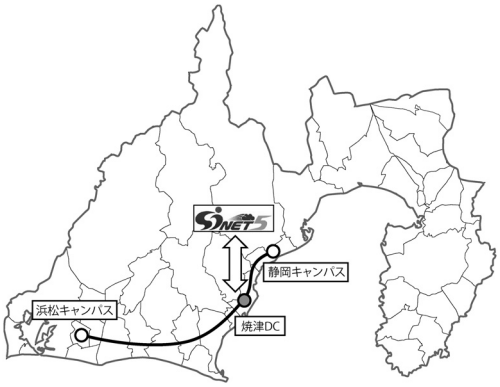

図 10　静岡大学クラウド情報基盤のロケーション

た [6].

図 11 に，本学のクラウドモデルの概要を示す．下段の両キャンパスには，従前から設置されているサーバやサーバに類する各種の情報機器が存在した．これらの機器にはインターネットと直接通信を行うグローバル IP アドレス（以後，「GIP」という）が割り振られている．GIP 機器は直接的にインターネットからの攻撃の脅威に晒されているため，GIP の総数は，その組織の情報セキュリティレベルを測る指標の一つに成り得る．クラウド情報基盤が完成する 2010 年以前には 600 から 700 の GIP 機器がリスクの「移転」や「回避」の選択肢もほとんどないまま主要両キャンパス内に散在していた．これらの GIP 機器の保守と運用のコストの総量を精度よく測定したり制御したりする手段も限られていた．また，浜松キャンパスのサーバ室には，全学の情報基盤の中核となる基幹システムが設置され，GIP 機器の中枢拠点となっていたが，自然災害による予期せぬ停電対策や，法令点検時における自家発電装置への運用保守にも人手とコストを要していた．

本学のクラウド情報基盤は，浜松キャンパスの基幹システム群のすべてを中段の焼津 DC へ移すこと，両キャンパスに散在した研究教育向けのサーバ群を上段の商用クラウドプロバイダへ送り出すことの二階層構造となっている．中段の焼津 DC を PRCC (Private Cloud Center)，上段の商用クラウドプロバイダを PBCC (Public Cloud Center) とそれぞれ称している．PRCC は調達物のリース資産を収容しているが，PBCC は VPS (Virtual Private Server) と呼ばれる仮想サーバ群で構成されている．VPS とは，1 台の物理的なサーバ上に複数台のサーバ領域をソフトウェア的に構築する技術であり，高密度集約の利点から月額数千円の低価格利用が可能である．VPS は完全なサーバサービスの借用であるため，有形資産としての登録はなく，サービス中止によるサーバ停止後の資産廃棄の費用も発生しない．

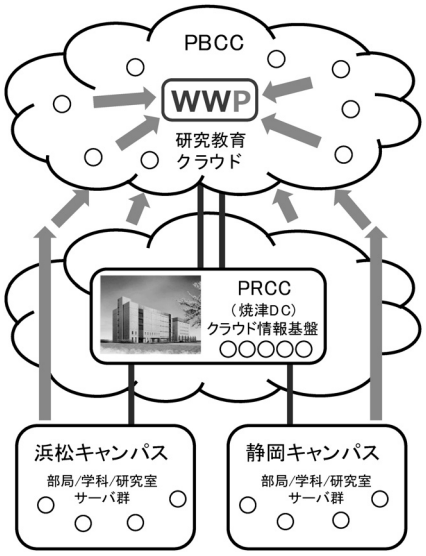

図 11　静岡大学クラウド情報基盤モデル

4.1　クラウド VPS を活用した PBCC

本学ではセンターが一括購入した VPS 資源を，部局担当者の了解の下に利用者は無償で利用できる．ここで部局に割り当てられる VPS の資源は，2010 年以前の各部局における GIP の利用台数に基づく案分値を初期値とした．その後二度の配分調整を行い現在に至っている．

図 12 は，VPS の学内発行台数の変化である．VPS 利用数は，2010 年のサービス開始当初の 150 台規模から始まり，センターが 90 台規模の実験利用を始めた 2014 年頃に約 340 台のピークを迎え，2019 年 3 月に 242 台の利用に収束している．このうち 90 台はセンターの実験利用であるため，2019 年 3 月時点では 153 台の VPS が学内利用者に提供されている．一人の利用者が複数台の VPS を利用しているため，正味の VPS 利用者は 100 名ほどである．本学の教職員数は約 1,150 名に対し，約 10%が VPS を利用している．2020 年度末にはさらに 50 台以上の縮小が予定されている．利用者要求に大きく変動するサーバ資源を PRCC 内に物理資産として収容することなく，PBCC 内の無形で可変なサービス資源として柔軟性の高い運用ができたことはクラウド VPS 利用の長所の一つである．

本学のクラウド情報基盤の立ち上げ当初の基幹システムは，42U サイズのフルラック 4.5 本に収容されていた．その後，高性能化に伴うダウンサイジングが進

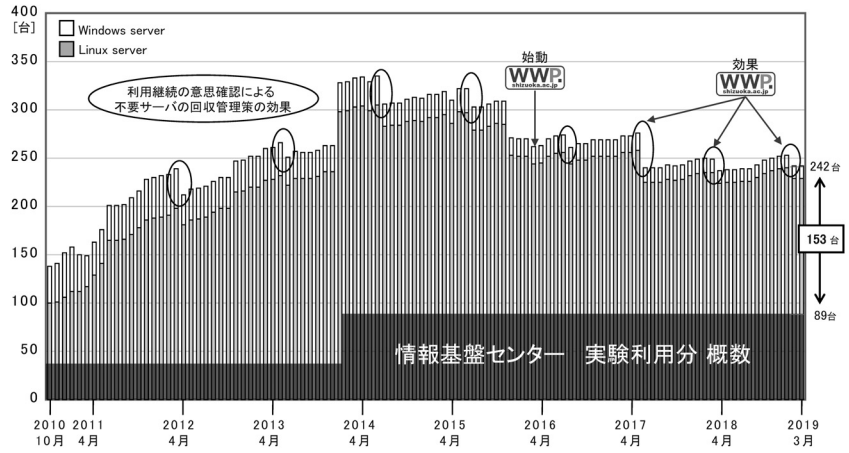

図 12　静岡大学クラウド VPS 利用数の変遷

み，現在はフルラック 2.5 本に縮小され，借用の費用も軽減できている．変動数の大きい研究教育向けのクラウドサーバ群を PBCC においたことは結果的によい判断であった．

4.2　クラウド VPS の定期回収

クラウド情報基盤の管理策の一つとして有効に機能している「クラウド VPS の定期回収」について述べる．この管理策の効果は，図 12 の毎年度末の VPS の利用数の減に表れている．すべての VPS はセンターが利用者に無償貸与しているため，継続利用とサーバ保守の継続の意思を年度末に行っている．サーバサービスの必要性が，保守の労力を超えるようになった VPS は，利用者の停止申請に基づき，センターが回収廃棄した．VPS の無償貸与は一見すれば不採算なサービスと思われがちであるが，センターはサーバ運用を試みる学内利用者に対し，サーバセキュリティとそれに伴う保守の重要性を能動的に訴える機会を得ることができた．保守不備または放棄のまま研究室の隅に長年放置されるサーバ群 [10] を全学的に一掃していくことにも成功した．ベンダーが OS の保守更新を終了することで，OS のアップグレイドを必要とするサーバが大量に発生する問題を EOL (End Of Life) という．センターが主導する 2 年間の EOL 対応の作業計画に基づき，利用者自身が OS のアップグレイド作業を計画的に遂行している．リスク移転の考えに基づくクラウドであっても，これを ISMS や ITSMS のプロセスに載せてサービス供給することで，クラウドのさらなる真価が発揮できる．

4.3　WEB サイトの WWP 集約

PBCC のクラウド VPS の利用数が減少に転じた理由に WWP (Website by WordPress) の導入効果がある．WWP の構築に至る経緯や機能の詳細は，論文 [11, 12] を，地域利用への展開については論文 [13] を参照されたい．

WWP は WordPress のマルチサイト機能に本学の統合認証システムを連携させた CMS (Content Management System) である．WordPress は世界で最も利用されている CMS であり，頻繁な機能向上を伴ったバージョン更新が行われ続けている．WWP は WordPress を主軸として，すべて OSS (Open Source Software) で構成している．独自の開発部分は 300 行程度のプラグインのみであるため，リリース以後もプログラムのデバックや追加の機能開発に手をかけることなく，少数名のスタッフで運用を行っている．WWP のクラウドサーバは，主メモリ 8 GB の WWP 専従の 1 台のみを用いている．年額の費用 28 万円の中位性能のクラウドサーバであるが，ホスティングしている子サイトの数は 260 サイト（2019 年 5 月）に達しているため，1 サイト当たりの月額コストは 90 円台と安価に抑えられている．WEB サイトのストレージには数十から数百 GB のストレージを提供する商用サービスが一般的であるが，WWP では 1 サイト当たり 300 MB の領域のストレージしか割り当てていない．代わりにデータ量の少ない軽いサイトを作成するための技巧を専用の子サイトにまとめている．運用当初を除いてストレージ増強の要望は受けていない．考えやノウハウを利用者に提供すること，明確な方針を示すことが，大量のクラウド資源節約に結実した例である．

図 13 は，統合マネジメントの観点を交えて作成した学内広報資料である．上図では，最近はごく普通に行われていることであるが，WEB の作成をブラウザのみでワープロと同等の編集が行えることを強調して

図 13　WWP の学内広報資料

いる．最近の WEB のアクセスはスマートフォンが過半数を占めるため，パソコンとスマートフォンの最適化された自動表示切り替えにも対応していることは重要である．下図には WWP の特徴を列挙している．統合認証との連携により常用の公式 ID でログインできること，セキュリティ保守から解放され情報発信に専念できること，WEB の専門知識の多くを必要としないことを強調している．教職員のみがサイトの初期の管理者であるが，学生を含めた複数に管理者権限を委譲する協同管理ができるため，サイト更新を維持しやすい．

WWP 開設以前には，学内に新しい研究プロジェクト，組織，学会会合などが立ち上がるたびに，WEB サイトの設置の相談をよく受けていた．WEB サイトの立ち上げだけを目的している利用者には，サーバ管理技術を必要とする VPS の選択は荷が重いだけでなく，組織の新たなリスクの源となりかねない．であるからといって，これらの情報発信を外注や外部組織に預けてしまうことは，コスト面の損失だけでなく，自組織からの情報発信を行うことの機会損失にほかならない．そこで，WWP では一教職員当たり最大 3 サイトの子サイトを開設できるようにした．

WWP は一つのクラウドサーバに複数の WEB を集約しただけの従前のホスティングサーバではない．WWP が包含する子サイト内の固定ページが新設され

表 2　GIP の脆弱性診断による情報セキュリティの堅牢化

回	脆弱性診断実施日	登録全数	診断完了	重大脆弱性
1	2016-12-20	333	202	34
2	2017-07-14	336	167	20
3	2017-09-08	335	149	18
4	2017-12-01	346	159	18
5	2018-12-06	362	164	6

たり，記事が投稿されたりすると，それらの更新情報がトップページに掲載され，一つの研究室からでも全学規模の情報発信を行える．この機能が WWP に活気を導き続けたことは確信できる．

著作権や肖像権の遵守，個人情報の配信の禁止に関する注意喚起を行い，コンテンツの適正監視は，トップページの更新情報リストから効率よく行うことができる．WWP の運用は情報セキュリティの啓蒙啓発と直結する造りを成し，低コストで安定な本学の情報発信源となっている．ISMS と ITSMS の統合マネジメントの運用の中で生まれた成果である．

4.4　脆弱性診断

ISMS の管理策の一つに脆弱性診断がある．脆弱性診断とは，外部との通信が直接可能な GIP のサーバ群に対して，通常は外部の商用ネットワークから情報収集や疑似攻撃を仕掛けてサーバの堅牢性を確認する検査手法である．有償・無償の優良な脆弱性診断ツールがいくつか存在している．EOL を過ぎた OS を利用している場合は致命的 (Critical) な脆弱性として検出される．インターネット上の脅威に晒されているサーバプログラムなどに重大な脆弱性を放置している場合は，脆弱性の程度に応じて Critical や High が検出される．センターでは，キャンパス内に資産上存在する 300 機以上のサーバ群に対し，約 2 年間で 5 回にわたり有償の脆弱性診断ツールで検査を実施した．

表 2 は，脆弱性診断ツールで判定される Critical, High, Medium, Low, Info の 5 段階評価の Critical（重大な脆弱性）のみの検出数の推移を示している．1 回目を 2016 年末に行った．MS を運用している以上，あと数年早く実施しておくべきであったとの反省もある．ただし，MS がなければ，現時点でも全学実施には至っていない可能性が高い．なぜなら MS の審査のなかで，たびたび脆弱性診断について質問を受け，不明瞭な回答しか返すことができていなかった．やがて脆弱性診断はなんとしても実施しなければならない管理策の一つに昇華してきた背景がある．GIP の登録全数は 333 であり，外部ネットワーク診断が到達し，診

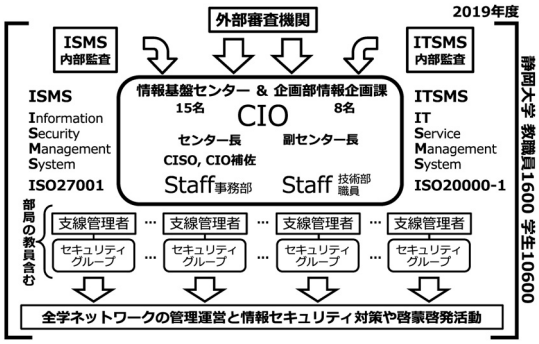

図 14　適用範囲図と情報セキュリティ組織図

断を終えることができた GIP の数が 202 である．その差 131 は GIP 利用の登録はあるが，外部からは存在が見えなかった GIP である．その内訳は，堅牢な防御を行っている，電源を切った状態のサーバ，TV 会議システムなどの装置である．一つ以上の Critical を有する 34 の GIP 機器（主にサーバ）が検出された．以後，集計の結果をすべての GIP 管理者に返信し，繰り返し是正措置を求める管理策を実施した．2 回目には診断完了の数が 167 に，Critical の検出が 20 にまで減じられており，1 回目の診断の結果を観て，自主的にサーバを閉塞した管理者が多くいたと判断している．3 回目，4 回目の結果が横ばいであることから，速やかに是正対応する管理者と，そうでない管理者の 2 タイプが存在することがわかる．それゆえに，1 回目の脆弱性診断は組織全体の脆弱性を大幅に改善できる効果が認められるので，未実施の場合は早急に実施すべきである．

5 回目の診断で，6 台の GIP のサーバにまで絞り込むことができた．内訳の主は保守期限を超えた OS を利用し続けている EOL 問題であり，その根深さを再認識した．その後の所有部局の責任ある指導と取り組みのもと，すべての重大な脆弱性を排除した．脆弱性診断は，1 名の技術スタッフが 1 日で実施できるが，結果の集計や通知などの事後処理に 1 週間ほどを要した．現在，これらの一連の脆弱性診断のプロセスを数コマンドで全自動化するシステムを構築し，MS の核心である持続的改善の取組を進めている．

4.5　組織のセキュリティ

MS 導入の効果事例として，最後に，組織で連携する情報セキュリティ対策の重要性について述べる．適用範囲や組織に関する規格要求要件はどの MS においても冒頭に出てくる共通の要件である．センターの適用範囲を図 14 に示す．

ISMS と ITSMS の統合マネジメントシステムの適用範囲人員は CIO を含む 24 名体制である．ほぼ毎年 1〜2 名の人員の交代や増減は行われている．本学では，歴史的に各部局の配下に技術職員を中心とした支線管理者のチームが配置されており，センターが検出した不正通信などの現場確認や是正対応を担当していた．近年のサイバー攻撃の猛威に対応するため，事故に至った原因の究明や再発防止策の徹底を図るための教員を中心としたセキュリティグループを CISO の指示のもとに追加編成した．セキュリティグループの設置は，2017 年に学内規則化されている．全学では総勢 60 名を超える規模の情報セキュリティ対策チームを構成している．前節で述べた脆弱性診断のような試みが速やかに実施されるためには，全学的な組織規模の協力体制と理解が不可欠である．MS の運用を通じて，適用範囲の枠を超えた組織力の醸成が成されている．

UTM (Unified Thread Management) が異常値として検出するログを当該部局の支線管理者とセキュリティグループ，GIP の場合はその管理者へ直接メール通知する管理策を 2019 年 1 月から始め，効果を上げている．UTM とは，従前の Fire Wall を進化させたセキュリティ装置であり，インターネットの学内ネットワークの門番のような役目を担っている．簡単には，Fire Wall が情報の通信ポート (Port) の遮断や許可を設定する装置であるのに対し，UTM はポート内を通過するデータに不正や異常がないことも検査する．UTM が出力するこれらのログは，時刻，発信元 IP と送信先 IP，脅威や脆弱性の名称を列記した数行のみであり，専門的な知識がなければ解読は難しく，そのほかの通信ログとの照合分析を経なければ，確度も得られない．実際に，medium レベルの通知には是正を必要としない場合が多い．UTM のログの例を示す．

- **critical** vulnerability 2019/06/XX 03:39:45 drop srcip=[OUR IP](57406) distip=[INTERNET IP](80) Bash Remote Code Execution Vulnerability(36729)
- **high** vulnerability 2019/06/XX 03:39:18 drop srcip=[OUR IP](53674) distip=[INTERNET IP](80) Apache Struts ClassLoader Security Bypass Vulnerability(36932)
- **medium** vulnerability 2019/06/XX 03:38:06 drop srcip=[OUR IP](43406) distip=[INTERNET IP](80) Jive Software Openfire Jabber Server Authentication Bypass Vulnerability(32171)

[OUR IP] や [INTERNET IP] には実際の IP アドレ

スが記されて送信される．通知を受けた IP 利用の当事者や所属部局の関係者は，メール本文の URL をクリックすることで，1 日刻みの日付リストに記された Critical，High，Medium の全学総検出数を確認できる．Critical においては，全学規模でも希な検出頻度であるため，部局関係者は，事態の切迫感や重大事故に至る懸念を視覚的に把握できる．真の原因究明と根本原因の是正措置が当事者と組織の連携で速やかに行われている．

5. おわりに

ISMS をはじめとする MS では，本稿で述べたように遅効性の一面もあるがゆえに，その有効性を示すことは規格要件の一つである．本稿では国立大学法人のクラウド情報基盤における長期間の MS の運用を例に，MS の有効性を示すいくつかの管理策と成果について列挙した．ITSMS は 2013 年からの運用であるが，ISMS においては 2003 年から 2019 年までの正味 15 年間の長期の運用にわたる．MS がなければ試みることもなかったであろう数多くの業務改善は紹介しきれていない．その一方で，MS の運用には，スタッフへの負担や費用もかかるのは事実である．筆者らも MS の費用対効果のすべてを明らかにしたとも，有効性の確証に至ったとも考えてはいない．ISO の MS と供に情報基盤運用を続けるかの最終判断は，運用結果の正誤には基づかない．MS は組織の目的を達成するための活動の誤りを是正する仕組みそのものでもある．したがって，継続の最終判断は MS が謳う「経営者のコミットメント」すなわち，経営者の確たる推進の選択に委ねられている．静岡大学は，2021 年の 10 月には新法人化を計画しており，少なくとも現在の体制をそのまま留めていることはない．MS 上でも大きな変更を迫られる．大学情報基盤における MS の運用の効果について真価が問われるときであり，今後の動向を見守りいただきたい．

参考文献

[1] ISO, “ISO/IEC 27001:2013: Informationtechnology–Security techniques–Information security management systems–Requirements,” 2013.

[2] ISO, “ISO/IEC 20000-1:2011: Information technology–Service management–Part 1: Service management system requirements,” 2011.

[3] ISO, “ISO 22301:2012: Societal security–Business continuity management systems–Requirements,” 2012.

[4] 松村宣顕，長谷川孝博，“「関係の合成」の概念を用いた ISMS と ITSMS におけるリスクアセスメントの統合，”情報処理学会論文誌，**60**, pp. 250–259, 2019.

[5] 長谷川孝博，中野光義，“ISMS から ITSMS への取り組みについて，”情報処理学会研究報告，2012-IOT-16, No. 39, 2012.

[6] 文部科学省学術情報委員会，“静岡大学のクラウド活用事例—SINET とクラウド情報基盤の連携—，”http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu4/031/shiryo/1342174.htm（2019 年 6 月 1 日閲覧）

[7] 永田正樹，磯部千裕，安原裕子，古畑智博，高田重利，松村宣顕，山崎國弘，長谷川孝博，井上春樹，“静岡大学での全学クラウドサーバ 232 台のマイグレーションにおける作業実際と運用の要件，”学術情報処理研究，**21**, pp. 13–20, 2017.

[8] 永田正樹，磯部千裕，安原裕子，古畑智博，高田重利，松村宣顕，山崎國弘，長谷川孝博，井上春樹，“パブリッククラウドとオープンソースソフトウェアを用いたトラフィック分散型 eduroam 基盤（静大 IoTE）の構築，”学術情報処理研究，**22**, pp. 12–22, 2018.

[9] 国立情報学研究所，「学術情報ネットワーク」，https://www.sinet.ad.jp （2019 年 6 月 1 日閲覧）

[10] 情報処理推進機構（IPA），“学術組織を狙ったウェブサイト改ざんに注意，”https://www.ipa.go.jp/security/announce/academy_website.html （2019 年 6 月 1 日閲覧）

[11] 長谷川孝博，松村宣顕，古畑智博，井上春樹，“統合認証を導入した WordPress マルチサイトによる WEB サービスの集約，”学術情報処理研究，**20**, pp. 75–81, 2016.

[12] 松村宣顕，古畑智博，名倉栄梨，長谷川孝博，“学術組織向け集中管理 CMS 環境 WWP の機能と活用事例，”大学 ICT 推進協議会 2017 年度年次大会論文集，No. FP1-02, 2017.

[13] 浦野新，松村宣顕，古畑智博，長谷川孝博，“WWP による地方企業における情報発信の活性化，”大学 ICT 推進協議会 2018 年度年次大会論文集，No. MP-2, 2018.