宇都宮大学における事業継続のための準備態勢の実践例

三原　義樹

大学情報基盤に対し ISMS を実践することで安定運用に努める組織が増加している状況において，組織の目的へのさらなる寄与のため情報基盤の維持は重要なテーマとなっている．組織の事業継続という観点では ISO 22301 が存在するが，情報基盤の事業継続という観点では ISO/IEC 27031 が存在する．本稿ではこれを採用した実践例の一部を紹介する．

キーワード：ISMS，IRBC，BCMS，IT-BCP，情報基盤

1. はじめに

情報基盤の運用においては，外部要因の変化や利害関係者からの要望などによって，課題が現出しては最適な手段が検討され解決が図られ続けている．この手段に対し ISO の国際標準では，最適性よりも目的に鑑みた有効性が重要と考えられている．最適性の議論は別でなされることを期待しつつ，利用者からは見えにくい情報基盤における問題解決の実践例の一部を紹介する．

宇都宮大学は約 2 km 離れた距離に 2 キャンパスがあり，さらに栃木県内に学校園や農場，演習林などの附属施設が分散している．これらを結ぶネットワークや情報サービスを担う宇都宮大学総合メディア基盤センター（以下，センターと略す）は，各種の情報通信インフラや情報通信サービスシステムなどの管理運営を通じて教育研究および地域連携に資する重要な責務を遂行する組織である．そして，情報セキュリティに対する脅威や脆弱性への対応に十分とは言えない資源が奪われ，本来の業務に支障をきたすリスク[1]を認識し，早期から情報セキュリティマネジメントシステム (ISMS; Information security management system) を採用した活動を行うことで業務効率を高め，組織的かつ能動的な情報基盤の運用に努めてきた．この運用に対し，2007 年には ISMS の国際規格 ISO/IEC 27001 の認証を受け，継続的改善を図ることで現在も認証を更新し続けている．特に，国立大学または国立大学の情報系センターにおいては，このように ISMS を運用する事例が増えてきており，情報技術とマネジメントの両輪によって情報基盤の安定運用に努めていることがうかがえる．

2. 事業継続に関するマネジメント

2.1 情報セキュリティと事業継続

ISO/IEC 27001 の要求事項ならびに ISO/IEC 27002 の規範において，情報セキュリティ継続を組織の事業継続マネジメントシステム (BCMS; Business continuity management system) に組み込むための枠組みが記されていることから，組織の BCMS をより適切に運用していく必要がある．そこでセンターでは，事業継続のための ICT 準備態勢 (IRBC; Information and communication technology readiness for business continuity) に関する指針の国際規格である ISO/IEC 27031 を採用することとした．この決定に際し，BCMS の国際規格である ISO 22301 を採用する選択肢も検討したが，センター全体の事業継続よりも，まずは情報通信基盤にかかわる業務について継続させることが優先事項であり，すでに運用している ISMS を深化させることがより実態に即していると判断し IRBC を採用した．

2.2 事業継続に関するマネジメント

詳細になるが，ISMS の国際規格である ISO/IEC 27001 の正式名称は，“Information technology–Security techniques–Information security management systems–Requirements,” BCMS の国際規格である ISO 22031 は “Societal security–Business continuity management systems–Requirements” であることからわかるとおり，ISMS は情報技術における IT

みはら　よしき
宇都宮大学総合メディア基盤センター
〒 321–8585　栃木県宇都宮市陽東 7–1–2
mihar@cc.utsunomiya-u.ac.jp

[1] 目的に対する不確かさの影響 [1]

セキュリティの分類で，BCMS は社会セキュリティ[2]の分類である．この分類の違いは，事業継続に対する要件の対象の違いに表れる．具体的には，ISMS では危機や災害など困難な状況下での情報セキュリティと情報セキュリティマネジメントを継続させるための策が求められているが，BCMS では事業，すなわち組織の存在目的の核となる活動を継続させるための組織の能力を維持管理する策が求められる．一般的に大学には，施設を所掌する事務，職員人事を所掌する事務，財務を所掌する事務がそれぞれ存在し，センター運営に必要な資源，いわゆるヒト・モノ・カネが分散管理されている．この管理体系がセンターの事業継続に必要な資源配置と意思決定の際の制約とならないことが望ましいが，実際は BCMS を実現するためにさまざまな制約を解決しなければならなかった．

組織の事業にとって，もはや IT が欠かせないほど強く依存していると言える．センターにとっては情報基盤の運用そのものが重要な業務の一つであることから，情報基盤の継続性抜きに BCMS を構築することは有効性が低い．そこで，事業継続のための ICT 準備態勢に関する指針である ISO/IEC 27031，“Information technology–Security techniques–Guidelines for information and communication technology readiness for business continuity” に着目した．この ISO/IEC 27031 は ISMS ファミリー規格であり，ISMS の管理策関連の手引規格として整合性と効率性をもって既存の ISMS に組み込むことができ，ISMS を運用している組織にとって利点がある．

2.3 IRBC

ISO 22300 では事業継続を，“障害を引き起こすインシデントの発生後，あらかじめ定められた許容レベルで，製品又はサービスを提供し続ける組織の能力” と定義している．事業継続計画 (BCP) を策定しただけでは能力を涵養することはできないため，平常時からマネジメント活動をすることで，組織の目的と乖離しないレジリエンス[3]を有することが肝要である．この考えに大きく寄与するのが IRBC，すなわち “中断（混乱）の予防，検出及び中断（混乱）への対応，並びに ICT サービスの復旧によって事業運営を支援する組織の能力” [3] である．IRBC を ISMS に組み込むことで，情報セキュリティに対する継続的改善を図るプロセスの中で ICT の準備態勢を実現し，これが大きな事業継続マネジメントを支援することにつながっていく．

センターでは実際に IRBC を ISMS に組み込み運用を行ってきた．2015 年 1 月にはこの運用で改めて ISO/IEC 27001 の認証を受け，更新され続けてきている．

ここで IRBC 活動の概要把握のため，IRBC の原則について触れる．ISO/IEC 27031 では

1. インシデントの予防
2. インシデントの検出
3. 対応
4. 復旧
5. 改善

と記されている．

1 は日常の ISMS 活動の中で対応可能である． 2 においては，情報基盤におけるインシデントはバグやパフォーマンスの低下，操作ミス，サイバー攻撃などが含まれ，大規模災害にも備える BCMS と異なり見えにくいところが多い．検出が遅くなり状況が悪化することで復旧計画を困難なものにすることがないよう，日常の予兆監視活動を組み込むことが重要となる．3〜5 のプロセスも ISMS 活動の中で対応可能である．このように IRBC は ISMS への親和性が高い．

すべてを完全な状態で継続させることは有限のコストの中では困難である．そのため，情報基盤の機能ごとに影響を分析し，影響と許容時間・許容範囲・許容レベルを考慮した継続のための要求事項を決定することとなる．次節では，この要求事項を支援する個別事例の一部を紹介する．

3. 事業継続に寄与する個別事例

3.1 太陽光エネルギーと直流蓄給電装置を活用した情報通信基盤

前述のとおり，宇都宮大学には二つのキャンパスがあり，それぞれのキャンパスにセンターの建物がある．センターはそのキャンパス間を結ぶ基幹ネットワークを運用している．2010 年当時，本学のインターネットへの接続が片側のキャンパスのみで構成されており，かつ狭帯域であった．現在では両方のキャンパスからインターネットへ接続し，かつ広帯域であることから，データセンターやクラウドに情報基盤を設置することが容易となっているが，当時は実現が困難であったため，キャンパス間の基幹ネットワークは特に重要であった．加えて，法定電気停電によりキャンパス間基幹ネットワーク装置を含め停止される状態になる．不通とな

[2] 意図的および偶発的な，人的行為，自然現象および技術的不具合によって発生する，インシデント，非常事態および災害から社会を守ること，およびそれらに対応すること [2]
[3] 複雑かつ変化する環境下での組織の適応できる能力 [2]

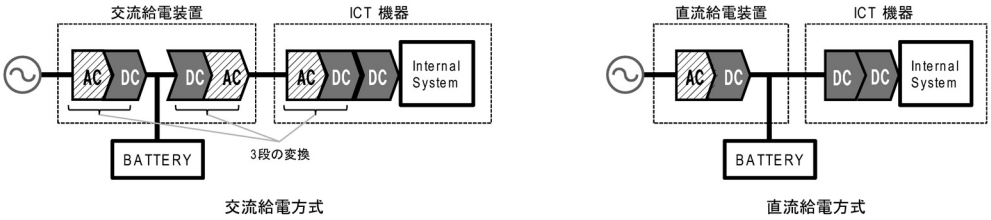

図 1　給電システムの比較図

る状況はもはや許容されるものではないため，キャンパス間通信を継続すべき業務と位置づけ，計画が検討された．まずソーラパネルと直流蓄給電装置をそれぞれのキャンパスのセンターに設置し，コンディショナーを介して発電電力をセンターに引き込んだ．ソーラパネルの設計上の発電能力は，一方が 19 kW でもう一方が 13 kW であり，2018 年の年間交流電力積算量の実績は両キャンパスのセンター合計で約 32,265 kWh であった．

一般的にシャーシ型の基幹スイッチは大きな電力を必要とする．そこで法定電気停電時などの商用電源が停止する際でも必要な通信を維持するため，前述の発電電力を用いて 24 時間以上通信を維持できる基幹スイッチを新たに整備した．なお，この基幹スイッチは直流電源を有する．通信機器の内部基板は直流駆動により稼動するため，図 1 に示すとおり，多段の交流–直流変換を介さず直接直流で駆動することで効率を高め，制限された電力を有効に利用することができる．

これらの情報通信基盤を整備した翌年の 2011 年 3 月には本学も東日本大震災を経験した．数日にわたる停電，その後の長期間の計画停電があり，情報基盤の運用が困難であったことに加え，キャンパス間内線電話も不通となり意思疎通に支障があった．このような事態においても常に維持されていたキャンパス間基幹ネットワークを利用し，IP 電話の設置などの対応態勢をとることができた．

また，平時における発電電力は，ネットワーク機器やサーバ群に加え 100 台以上の PC が設置された教室を有するセンター内で無駄なく配分されている．節電に一定の効果があることは言うまでもないが，特に，昼間利用時のピーク電力需要を補う効果には意義がある．

3.2　コンテナ型電源設備を活用した情報基盤

キャンパス間基幹通信の維持に加え，インターネット経路と必要な情報サービスを 24 時間以上維持することを実現するべく，より大容量の蓄給電システムを検討した．まず太陽光エネルギーの蓄給電容量を増加させる案が検討されたが，センターのサーバルームにはそれを拡張できる十分な空間がなかった．そこで，2014 年 3 月，2 キャンパスのそれぞれのセンター建屋外にコンテナ型の電源設備（図 2）を設置した．幅 2.3 m，奥行 6 m，高さ 2.4 m のコンテナ内部に 4,000 Ah の蓄電池が格納されている（図 3）．前項の蓄給電装置と同様に，この電源設備もセンターへ常時給電しているため，商用電力停止時の切替時間が極めて小さく情報基盤に必要な高可用性が実現されている．この電源設備からは直流と交流をそれぞれ給電しており，直流電源を有する低消費電力サーバを導入・接続し，非常時の情報サービス資源を確保している．

図 2　コンテナ型電源装置外観

図 3　コンテナ内の蓄電池

また，長時間の停電により蓄電電力を消費する事態にも備え，緊急発電車両から受電するためのインタフェースも実装されている．

コンテナの懸念点として，夏場の内部温度上昇による蓄電池への影響がある．これに対応するため，コンテナ内に冗長化された空調設備を設置し，常に蓄電池

にとっての適温が維持されており，空調が停止する事態に備え排熱のためのファンも実装されている．

宇都宮の落雷回数は全国でも上位であり，かつそのほとんどが夏に発生している [4]．そして強落雷が多く瞬間的な停電から秒単位の停電まで幾度となく経験している．当然，サーバ類は UPS（無停電電源装置）に接続されているため支障は出にくいが，UPS に接続されていない通信機器類は支障が出る．そこでこの電源設備が巨大な UPS となって，センターの情報基盤の要となる装置類を常時保護し，IRBC をより確実なものとしている．

3.3 ほかの管理策の考察

情報基盤の運用維持に大きな問題となる電力の喪失に対して，発電＋蓄電ではなく発電機の選択肢が考えられる．燃料が許す限り発電可能なので有用であることは間違いない．ただし，燃料と発電機の維持管理が必要となる．一定量の燃料を保管するための施設には，消火栓設備やスプリンクラー，火災報知器設備などが必要で，発電機でも定期的に運転させ点検する必要があり，維持管理コストは小さくない．さらに，発電系へ切り替える操作も訓練が必要である．

一方，ソーラーパネルは基本的にメンテナンスフリーで期待寿命も比較的長い．蓄電池は状況により劣化が起きるため定期的な点検が必要ではあるが，適切な管理がなされているため期待寿命どおり計画性をもって交換することができている．電源装置と電源設備からは常時給電されているため，電源系の切り替え操作も不要である．

大きな電力を必要とするサーバ群はクラウドやデータセンターへ移設されるようになり，そこで高可用性をもって安定運用されるようになってきている．このような状況の変化がある中，そこへのネットワークアクセスを維持・継続させることがより重要と考えることができる．そのために大きな電力を保有することに越したことはないが，「止めない，止まらない」情報基盤，そして緊急時の手順が複雑にならない仕組みという目標には本事例で採用した管理策が適していた．

4. おわりに

センターが有する情報資産に対する情報セキュリティ維持のための ISMS 活動は，センターがもつ役割と権限の範囲内で実現できている．組織と業務を維持する BCMS の実現には，センターだけではなく大学経営者のコミットメントが必要となる．したがって，大学経営陣のコミットメントを含めたセンターの BCMS への実現と並行し，まずはセンターの ISMS 内で実現できる IRBC を実践してきた．平常時・非常時を問わず情報基盤の安定運用に向けた取り組みは今後も続いていく．

参考文献

[1] International Organization for Standardization and International Electrotechnical Commission, “ISO/IEC 27000:2014, Information technology–Security techniques–Information security management systems–Overview and vocabulary,” 2014.

[2] International Organization for Standardization, “ISO 22300:2012, Societal security–Terminology,” 2012.

[3] International Organization for Standardization and International Electrotechnical Commission, “ISO/IEC 27031:2011, Information technology–Security techniques–Guidelines for information and communication technology readiness for business continuity,” 2011.

[4] 気象庁，「雷の観測と統計」，https://www.jma.go.jp/jma/kishou/know/toppuu/thunder1-1.html（2019 年 6 月 6 日閲覧）

