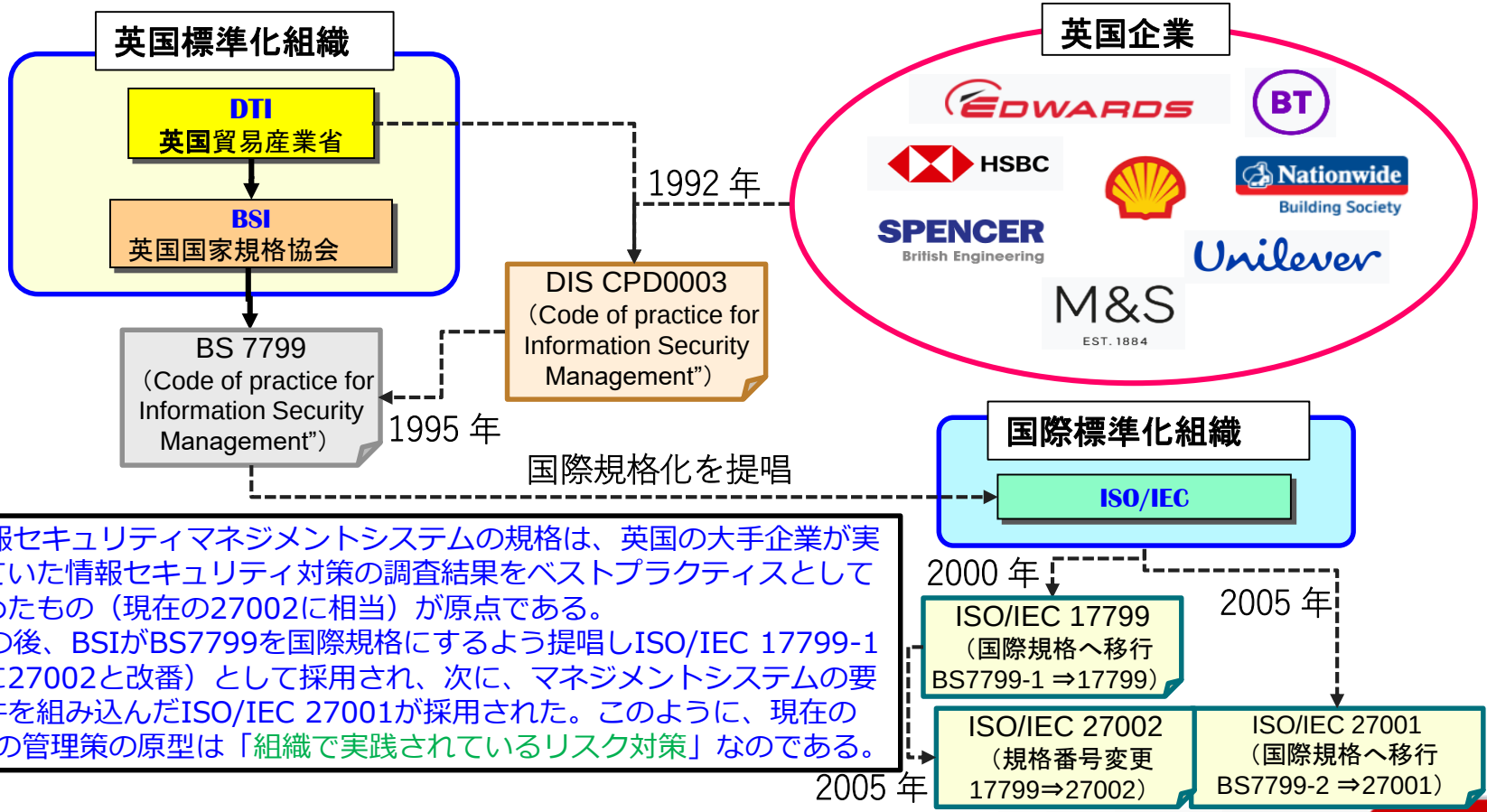
テーマ2
27002規格改定に対する提案活動
（ISMSユーザーによる実施の手引改定提案）

JNSA標準化WG
日本ISMSユーザグループ
インプリメンテーション研究会

2020年12月18日

羽田　卓郎

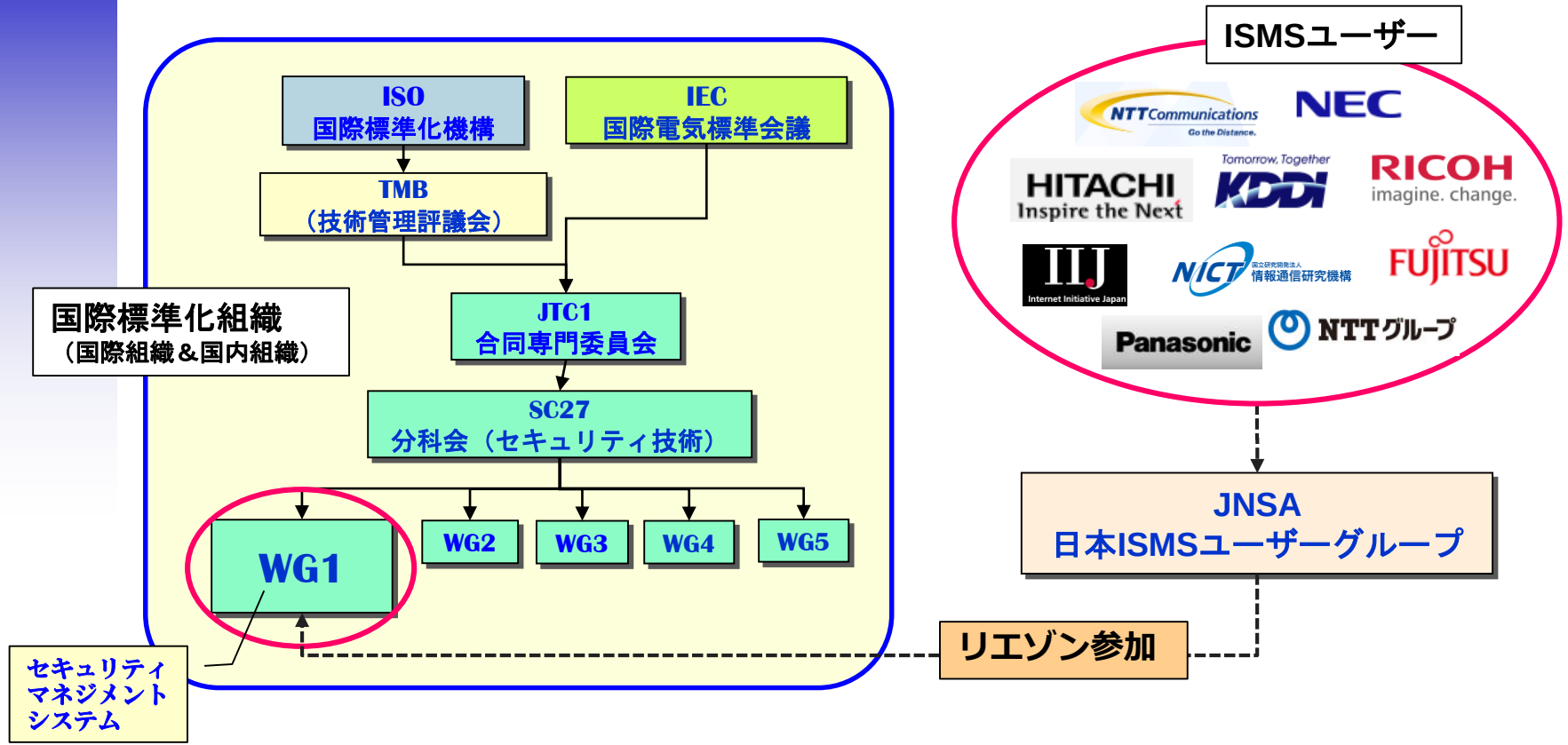
情報セキュリティ規格策定の経緯



情報セキュリティマネジメントシステムの規格は、英国の大手企業が実践していた情報セキュリティ対策の調査結果をベストプラクティスとしてまとめたもの（現在の27002に相当）が原点である。

その後、BSIがBS7799を国際規格にするよう提唱しISO/IEC 17799-1（後に27002と改番）として採用され、次に、マネジメントシステムの要求条件を組み込んだISO/IEC 27001が採用された。このように、現在のISMSの管理策の原型は「組織で実践されているリスク対策」なのである。

日本ISMSユーザーGと国際標準化組織



テーマ2の2020年研究目的

現在ISO/IEC 27002の改定が進行中であるが、近年のクラウドサービス利用の拡大や、感染症対策によるテレワーク導入促進などへのリスク対応が規格に反映出来ていないという声があり、

「ISMSユーザーの声を国際規格に反映する」

という目的を達成するため、2020年は、

「ISMSユーザーが実際に実施している情報セキュリティ対策で、ISO/IEC 27002の実施の手引に記載されていないものはなにか」

を研究しISO/IEC JTC1 SC27 WG1に提案する。

テーマ2研究の背景

「ISMSユーザーグループ（以下「ISMS-UG」）」は、ISMS認証規格（ISO/IEC 27001）の発行に関連し、「規格を利用するユーザーの声を規格の策定や改定に反映しよう」という目的で参加国の国内にそれぞれ組織化された。 ISMS-UGは当初独立した組織であったが、現在はJNSAに合流して標準化部会のWGとして活動し「ISMSの構築・運用に関わるユーザ視点でのベストプラクティス」を研究しているが、これまではISO/IEC SC27 WG1へのリエゾン参加と日本国内向けの情報発信に留めていた。

テーマ2研究方針

以下の方針で研究を進める。

1. 管理策レベルは国際会議の改定案に従う。
   （ 4月の国際会議で管理策の討議は終了）。
2. ISMS-UGのメンバー組織が採用している情報セキュリティリスク対策で、規格要求事項との紐付けに悩んだり、27002の実施の手引を見ても該当する実施の手引が見つからなかったりした事例を出し合う。
3. ２．の事例について、研究会で27002の実施の手引きに採用したいとしたものを整理しリエゾンを通じて国際標準化組織に提案する。

27002実施の手引追加提案

2ndCD 27002に対する提案を行ない
DIS 27002への採用を目指した。

ISO/IEC 27002実施の手引改定提案：1

管理策			提案概要	国内	国際
#1	9.2.4	利用者の秘密認証情報の管理	シングルサインオン（SSO）の導入によるパスワード漏洩リスクの低減	ー	ー
#2	9.4.1	情報へのアクセス制限	社外ネットワークからのアクセスで同一IDで異なる端末からのアクセスを制限	○	×
#3	9.4.2	セキュリティに配慮したログオン手順	①システムの初期画面に過去のログイン履歴を表示することによって、なりすましによる不正利用を発見する。 ②生体認証を利用する場合には、パスワード等の登録内容を変更できる認証手段と組み合わせた多要素認証とする	× ○	ー ○

○＝採用、×＝不採用、ー＝提案事由解消（又は国際会議へ提出せず）

ISO/IEC 27002実施の手引改定提案：2

管理策			提案概要	国内	国際
#4	11.2.4	装置の保守	機密データの格納されたICT設備や媒体を障害対応等のために組織外に持ち出す場合及び持出後に廃棄する場合のルールを策定する	○	○
#5	12.3.1	情報のバックアップ	クラウドサービスを利用する場合、利用者の操作ミスによるデータ修復や障害時の復旧を確実にするため、どのようなバックアップサービスが提供されるのかを確認し、必要なバックアップができるようにする	○	○
#6	13.1.1	ネットワーク管理策	認可されない機器の接続防止のために、MACアドレス、機器認証、電子証明書等を利用し排他や検知を実施する	○	○

○＝採用、×＝不採用、－＝提案事由解消（又は国際会議へ提出せず）

ISO/IEC 27002実施の手引改定提案：3

管理策			提案概要	国内	国際
#7	13.1.1	ネットワーク管理策	配信負荷をキャッシュで軽減させるための配信サービスを使用する場合には、利用時のプライベート領域のキャッシュを抑止することが望ましい。	○	○
#8	14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	関連情報の「管理策は、アプリケーションの変更にも適用することが望ましい。」は混乱を招くため削除	―	―
#9	14.2.6	セキュリティに配慮した開発環境	クラウドサービス上で開発環境を構築又は運用する場合、仮想ネットワークの外部通信機能が停止又は開発者のみに制限	△	―

○＝採用、×＝不採用、△＝保留　－＝提案事由解消（又は国際会議へ提出せず）

ISO/IEC 27002実施の手引改定提案：まとめ

2020年ISO/IEC 27002規格改定提案研究結果：

- 27002実施の手引改定（追加）検討件数：9件

  ※内2件は改定27002では解決する見込みのため、27002Ad hoc会議への提案は7件

- 27002Ad hoc会議への提案結果：採用　6件
- 国際会議による検討の結果、採用　5件

＃１：9.2.4の検討内容

【管理策】9.2.4 利用者の秘密認証情報の管理

【追加案】シングルサインオン（SSO）を導入しパスワードの使いまわしなどによるパスワード漏洩リスクを低減する。

【理由/背景】シングルサインオン（SSO）は単なる利用者の利便性向上だけではない。多数のシステムを利用する場合に複数パスワードを設定することは、パスワードの使いまわし等によるパスワード漏洩のリスクが高くなるため、SSOによってセキュリティ向上が期待できる。

※ISO/IEC27002：2013では、「9.3.1 秘密認証情報の利用」の関連情報にSSOに関する記述があるが、SSOの仕組みを採用するのは利用者ではなく管理者側であるため、A.9.2.4の実施の手引に記述することが望ましい。

＃１：提案結果

【結論】国内：提案事由解消　国際：不提出
【理由】ISO/IEC 27002 CD2ではA.9.2.4とA.9.3.1が統合されたためこの提案は自動的に解消されることになった。…「9.3.1 秘密認証情報の利用」の関連情報にSSOに関する記述が、CD2のA.9.2.4とA.9.3.1の統合された管理策の関連情報に記載される予定。

＃２：9.4.1の検討内容

【管理策】9.4.1　情報へのアクセス制限

【追加案】社外ネットワークから自組織の情報又はサービスにアクセスを許可する場合、同一IDで異なる端末からアクセスすることを制限する。

【理由/背景】社内のネットワークではIDだけでなく、物理的入退管理や接続端末の制限等も行われるため第三者によるなりすましのリスクは低いが、外部ネットワークの場合はIDを成り済まされても検知することは難しい。このため、ログオンする端末を制限することでなりすましのリスクを低減することが望ましいが、現在の実施の手引きにはそのような記述はない。

＃２：提案結果

【結論】国内：採用（①提案No. JP205）国際：不採用
【WG1提案内容】デバイスの使用が組織の内外で行われるかどうかに関係なく、組織のネットワークと情報にアクセスできるエンドポイントデバイスを登録および制御する。…提案は英文のため仮訳（以下同様）
【提案主旨と不採用理由】組織外からのアクセスのほか、端末の持込みやサテライトでの使用の考慮と、PCやスマートフォン、タブレット等の利用で複数ログインもあり得るため、端末の制限ではなく登録端末からのアクセスにすることを提案したが、新しい管理策の「エンドポイント　デバイス」の実施の手引に端末の登録に関する記述が載る予定のため日本からの提案は認められなかった。

#3： 9.4.2の検討内容 - ①

【管理策】セキュリティに配慮したログオン手順

【追加案】

①システムの初期画面に過去のログイン履歴を表示することによって、なりすましによる不正利用を発見する。

【理由/背景】

①ログオン手順では、入力したIDやパスワードの安全性を求めているが、本人でなければ分からない過去の利用履歴の正しさを確認するような対策は現時点では記述されていない。

#3： 9.4.2の検討内容 - ②

【管理策】セキュリティに配慮したログオン手順

【追加案】

②生体認証を外部（公衆ネットワーク等）からのアクセスに対する認証手段とする場合には、パスワード等の登録内容を変更できる認証手段と組み合わせた多要素認証とすることが望ましい。

【理由/背景】

②パスワード漏洩（盗難や推測により）した場合、速やかに変更することが被害を防止する手段となるが、生体認証は変更することができない。

#3：①の提案結果

【結論】国内：提案事由解消　国際：不提出
【理由】27002：改定27002の実施の手引でカバーされる予定。

#3：②の提案結果

【結論】国内：採用（②提案No. JP206）海外：採用
【WG1提案内容】バイオメトリック認証情報は、一度盗まれた場合は無効にする必要があります。 湿度や経年変化などの使用条件によっては、生体認証を利用できない場合があります。 これらの問題に備えるには、生体認証に少なくとも1つの代替認証技術（パスワード認証など）を伴う必要があります。
【提案主旨と採用理由】この実施の手引では、生体認証を使用するリスクに対処する必要があると国際的にも認識された。

#4： 11.2.4の検討内容

【管理策】装置の保守
【追加案】保守業者や廃棄業者がデータの格納されたICT設備や媒体を障害対応等のために組織外に持ち出す場合、組織はA11.2.5の資産の移動として扱う。また、障害対応の結果継続利用不可の場合にはA.11.2.7の装置のセキュリティを保った処分又は再利用を適用する。
【理由/背景】ICT設備などの障害では、対応を依頼した業者が自社に持ち帰って対応することがある。また、資産の移動には障害対応による持ち出しは言及していないし、障害の程度によっては廃棄処分となる場合がある。

#4：提案結果

【結論】国内：採用（③提案No. JP191）国際：採用

【WG1提案内容】

- 情報を含む機器が組織の敷地外に持ち出された場合、経営者の承認およびその他の適切な手順に従う必要がある。
- 機器が処分されると決定された場合、安全な処分のための管理が適用されるべきである。

【提案主旨と採用理由】機器がサプライヤーまたはメンテナンスサービスプロバイダーに持ち込まれている。そして、機器またはその部品は処分されることがあることに対処すべきことが国際的にも認識された。

#5： 12.3.1の検討内容

【管理策】情報のバックアップ
【追加案】プラットフォームやアプリケーションの運用環境を提供するクラウドサービスを利用する場合、利用者の操作ミスによるデータ修復や障害時の復旧を確実にするため、組織が利用するクラウドサービスにおいて、どのようなバックアップサービスが提供されるのかを確認し、組織にとって必要なバックアップができるように対応することが望ましい。
【理由/背景】クラウド特有のリスクとして、操作ミスによりアカウントや環境の破棄を実施した場合は、バックアップデータごと削除される可能性がある。

#5：提案結果

【結論】国内：採用（④提案No. JP231）国際：採用
【WG1提案内容】組織がクラウドサービスを使用する場合、クラウドサービス環境内の組織の情報、アプリケーション、システムのバックアップコピーを作成する必要があります。 組織は、クラウドサービスの一部として提供される情報バックアップサービスを使用して、バックアップの要件が満たされるかどうか、またどのように満たされるかを決定する必要があります。組織は、必要に応じてバックアップの要件を実装する必要があります。

#5：提案結果

【提案主旨と採用理由】クラウドサービス利用時の情報バックアップの実施の手引追加。 クラウドサービスのお客様は、クラウドサービスの一部として提供される情報バックアップを使用できる。または、独自の情報バックアップを開発して運用する必要があるということを国際的にも認識された。

#6： 13.1.1の検討内容

【管理策】ネットワーク管理策

【追加案】認可されない機器の接続を防止するために、MACアドレス、機器認証、電子証明書等を利用し排他や検知を実施する。

【理由/背景】ISO/IEC 27001：2005では「A.11.4.3 ネットワークにおける装置の識別」という管理策があったが、ISO/IEC 27001：2013ではA.13.1.1に統合されている。しかし、27002：2013の実施の手引きにはそれが反映されていない。認可されない機器の接続は防止されなければならないが、現在の規格・実施の手引ではそのコントロールが示されていない。

#6：提案結果

【結論】国内：採用（⑤提案No. JP247）国際：採用
【WG1提案内容】ネットワークへの機器やデバイスの接続を検出、制限、認証する必要があります。
【提案主旨と採用理由】機器やデバイスのネットワークへの接続は、必要に応じて検出、制限、認証する必要がある（ ISO / IEC 27002：2005、11.4.3ネットワーク内の機器識別の内容は有効であり、このコントロールの対象である）について、国際的にも認識された。

#7： 13.1.1の検討内容

【管理策】ネットワーク管理策

【追加案】 CDN (Content Delivery Network) のような配信負荷をキャッシュで軽減させるための配信サービスを使用する場合には、利用時のプライベート領域のキャッシュを抑止することが望ましい。

【理由/背景】大規模なコンテンツ配信や急激な負荷上昇に対応するために、 CDNを利用する組織が増えている。 CDN はコンテンツをキャッシュして分散配信を行う仕組みである。 配信する内容に プライベートな領域 (個人情報など) が含まれる場合は、プライベートな領域がキャッシュされないように設定が必要となる。

#7：提案結果

【結論】国内：採用（⑥提案No. JP247）国際：採用
【WG1提案内容】コンテンツ配信ネットワークなどのネットワークサービスでのキャッシングに関するパラメータは、パフォーマンス、可用性、機密性の要件に応じてユーザーがキャッシングの使用を選択できるようにする。
【提案主旨と採用理由】ネットワークサービスでキャッシングを使用するためのオプションは、セキュリティ機能として言及する必要がある。 組織は、パフォーマンス、可用性、機密性の間のトレードオフを考慮して、ネットワークサービスのキャッシングを選択する。国際的には提案内容に若干の修正を加えて採用することで合意した。

#8： 14.2.3の検討内容

【管理策】オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
【追加案】関連情報の「管理策は、アプリケーションの変更にも適用することが望ましい。」は混乱を招くため削除すべき。
【理由/背景】アプリケーションの変更は、14.2.2の「システム変更管理手順」や14.2.4の「パッケージソフトウェアの変更に対する制限」及び14.2.9の「システムの受け入れ試験」で十分にカバーされているため、あえて14.2.3のプラットフォームの変更に関する対策を流用する必要はないと考える。

#8：提案結果

【結論】国内：不採用　国際：不提出
【理由】27002：CD2ではA.14.2.2～14.2.4が統合されるためこの提案は自動的に解消されることになった。

#9： 14.2.6の検討内容

【管理策】セキュリティに配慮した開発環境
【追加案】クラウドサービス上で開発環境を構築又は運用する場合、仮想ネットワークの外部通信機能が停止又は開発者のみに制限されていることを確実にしなければならない。
【理由/背景】オンプレミスの環境では、開発環境は外部との接続を自ら設定しない限り通信はできないが、クラウドサービスの場合は、既に物理的には通信可能な環境に仮想ネットワークが構築されているため、仮想ネットワークにおける外部通信を意識的に制限しなければ不正アクセスのリスクがある。

#9：提案結果

【結論】国内：保留　国際：不提出

【理由】提案内容を検討した結果、14.2.6（セキュリティに配慮した開発環境）ではなく、13.1.1（ネットワークセキュリティ）の範疇であろうということになった。しかし、内容的にアクセス制御との関連の整理も必要ということで採用は見送ることになった。

⇒クラウド環境の開発環境に対し、ネットワーク経由での第三者からの不正アクセスを防止するための実施の手引の提案であるが、開発者からのアクセスに限定し、他者のアクセスを許さないという点ではアクセス制御の要件でもあるという認識である。

最後に

日本ISMSユーザーグループとしては、初めて国際規格への提案を行ったが、提案9件に対し国際会議での採用5件となった。27002の改定提案には、各国から数千件の修正提案（表現の修正含む）がある中で、わずかではあるが、ISMSユーザー組織から実際に実践しているリスク対策から、重大なインシデントにつながる可能性のあるリスク対策として提案し採用につながったことは大きな成果である。

国際会議への提案と討議での説明を担ってくれた標準化小委員会27002Ah会議のメンバーに感謝の意を表したい。

今後とも、ISMSを実践するユーザー組織を代表し国際規格の充実に向けて提案活動を続けて行ければと考えている。