URL　https://journal.ntt.co.jp/article/23454
DOI　https://doi.org/10.60249/23105101

セキュリティ関連の最新標準化動向とコンサルティング

NTTテクノクロスでは，ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission）やITU-T（International Telecommunication Union - Telecommunication Standardization Sector）のセキュリティに関する標準化活動等に取り組んでいます．本稿では，ISO/IEC 27001，ISMAP（Information system Security Management and Assessment Program），ITU-T勧告X.1060のセキュリティ関連の最新標準化動向等とその実践を支援する当社のコンサルティング（3種類）について紹介します．

キーワード：#情報セキュリティ，#クラウドセキュリティ，#セキュリティ統括

武井　滋紀（たけい　しげのり）
中田　美佐（なかだ　みさ）
土屋　直子（つちや　なおこ）
NTTテクノクロス

ISO/IEC 27000シリーズ

■ISO/IEC標準化動向

情報セキュリティマネジメントにおいて国内でもっとも主要な第三者適合性評価制度であるISMS適合性評価制度[(1)]の認証基準として知られているISO/IEC 27001（情報セキュリティマネジメントシステム－要求事項）*1と，そのガイドライン規格であるISO/IEC 27002（情報セキュリティ管理策）*2が，2022年に改訂されました．改訂版では，昨今のサイバー攻撃，プライバシー侵害，クラウドサービスの普及などのセキュリティ脅威やセキュリティ技術の変化への対応が強化されました．改訂版で強化された情報セキュリティ管理策について**図1**に示します．

これらの規格は，ISMS適合性評価制度だけではなく，経済産業省の情報セキュリティ管理基準[(2)]や，政府情報システムのためのセキュリティ評価制度であるISMAP（Information system Security Management and Assessment Program）[(3)]の基準のベースとなっており，本改訂は関連制度にも大きな影響を及ぼします．ISMS取得組織は，移行期間である2025年10月31日までに新しい認証基準への移行審査を受ける必要があります．また，ISO/IEC 27002に基づくクラウドサービスのための規格であるISO/IEC 27017*3についても，現在ISOにて改訂中で数年後に改訂版が発行される予定です．

＊1　ISO/IEC 27001:2022：情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項．
＊2　ISO/IEC 27002:2022：情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策．
＊3　ISO/IEC 27017:2015：情報技術－セキュリティ技術－ISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範．

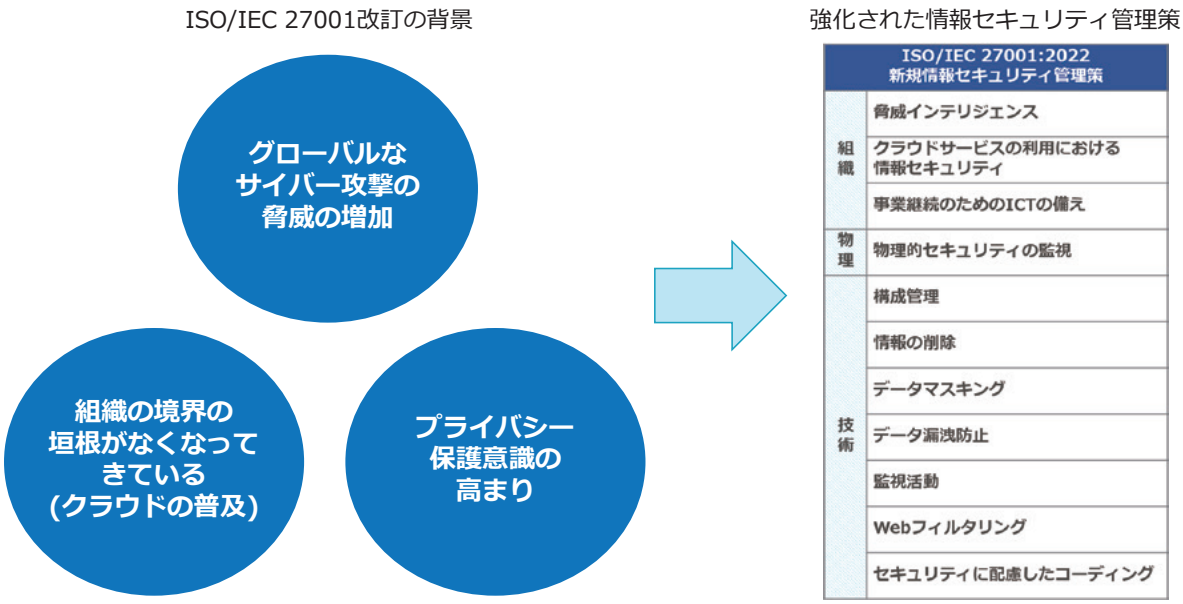


図1　改訂版で強化された情報セキュリティ管理策

■ISO/IEC 27001，ISO/IEC 27017コンサルティング

情報セキュリティマネジメントに課題を感じている，または強化したいと考えている組織は，組織のニーズにこたえるコンサルティングサービスを活用することがポイントになります．ISO/IEC 27001やISO/IEC 27017のコンサルティングサービスを提供する会社は数多くありますが，NTTテクノクロスでは，ISO標準化活動にも参画し規格を熟知したコンサルタントが組織のニーズにきめ細かく対応した，ISO/IEC 27001:2022移行コンサルティングやISO/IEC 27017コンサルティングを行っています．

また，NTTグループのセキュリティ規程は，最新のリスクマネジメントを強く意識し，米国国立標準技術研究所（NIST）のCybersecurity Frameworkや SP800-37，SP800-53[4]も考慮したものに改訂され，NTTグループ各社は新規程に沿った対応が必要となります．このような対応の支援のため，NTTテクノクロスでは，ISOセキュリティ規格に加えNISTやNTTグループ新旧規程にも詳しいコンサルタントが，セキュリティ規程の改訂や強化を行うコンサルティングも提供しています[5]．

ISMAP

■ISMAP最新動向

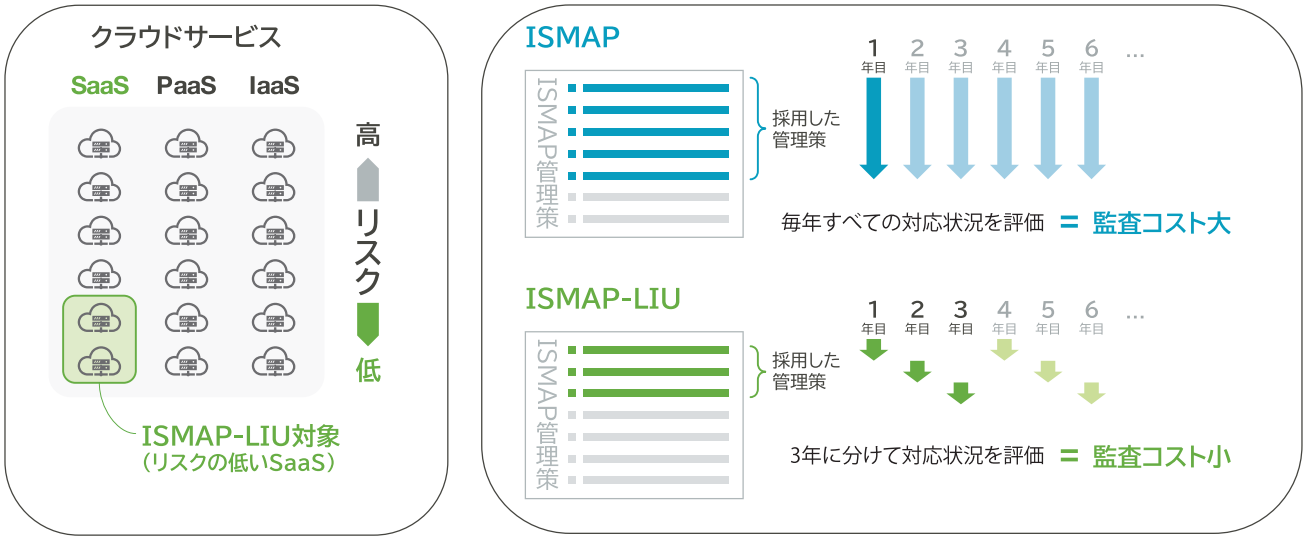
政府機関等が一定のセキュリティ水準を満たしたクラウドサービスを調達できるよう，クラウドサービスのセキュリティを評価し，サービスリストに登録する制度であるISMAPの運用が2020年6月3日に開始されてから，主管省庁により普及に向けてプレスリリースや講演，暫定措置等が行われています．また，制度当初より登録にかかる負担が大きいとの声があったため，2022年11月1日より，リスクの小さな業務・情報の処理に用いるSaaS（Software as a Service）を対象としたISMAP-LIU（Low Impact Use）*4が開始されました．これは，主管省庁が定めた「対象業務一覧」に該当するSaaS，または複数の行政機関による「影響度評価」で「低位」と評価されたSaaSに適用されます．ISMAPではリスクアセスメントによって採用した全管理策への対応を約1年ごとに評価するのに対し，ISMAP-LIUでは3年間で全管理策への対応を評価することで，ISMAP-LIUクラウドサービスリストに登録する制度です（2023年7月時点）．ISMAPとISMAP-LIUの仕組みの違いについて**図2**に示します．なお，ISMAP-LIUへの登録は2023年5月時点では0件であり，デジタル庁はISMAP-LIU登録促進のため，2023年5月19日にさらなる特別措置[6]を公表しています．本特別措置では，移行期間内の一度に限り，監査の負担を軽減できる一方，特別措置登録サービスリストの開示は政府機関等に限定されます．

また，ISMAPの申請から登録までの待ち時間を改善するための検討が現在も進められており，最新の規程類についてはISMAPのHP[3]を参照してください．

■ISMAPコンサルティング

各種普及・促進施策にもかかわらず，新規登録するクラウドサービス数が限られるのは，ISMAP管理基準に規定されている1000個以上の管理策への対応や監査法人による厳格な監査への対応が，クラウドサービス事業者にとって多大な負担になっているためと推測されます．その負担を軽減するために，NTTテクノクロスではISMAP運用開始当初より，ISMAP登録支援コンサルティングを提供しています[5]．今まで

＊4 ISMAP-LIU：ISMAPの枠組みのうち，リスクの小さな業務・情報の処理に用いるSaaSサービスを対象とする仕組み．



（a）ISMAP-LIUの対象範囲　　（b）採用した全管理策の評価方法の違い

図2　ISMAPとISMAP-LIUの仕組みの違い

培ってきたISMAP規程類のベースとなった各種セキュリティ規格・基準の知見，各種監査・認証評価制度における監査ノウハウ，NTTグループおよび一般企業において助言してきた各種管理策への対応事例等を活用し，クラウドサービス事業者が苦労することの多いISMAPの管理策の理解や，自社のセキュリティ対策とISMAPの管理策への対応付け，外部からの監査に対応するための証跡の妥当性評価，各種申請書類の記載方法など，さまざまな支援を行っています．

ITU-T勧告X.1060

■X.1060標準化動向

2021年10月にITU-T勧告X.1060[*5]が公開されました．本勧告は，NTTグループなどが提案したセキュリティも含むビジネスリスクに対応する組織のフレームワークです．2022年２月にはTTC標準JT-X1060[*6]として日本語で日本の標準となりました．

背景には，ビジネス環境が変化しSOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）といった組織だけではビジネスにおけるリスク全体に対応することが難しくなったことがあります．そこで「サイバーディフェンスセンター」という概念が提唱されました．これは日本からの提案として，経済産業省サイバーセキュリティ経営ガイドラインや日本セキュリティオペレーション事業者協議会の知見が盛り込まれています．日本のガイドラインやドキュメントを参考に使いやすくなっていることも特徴です．

X.1060はあくまでセキュリティ対応組織を構築して運用するフレームワークです．実際にどのようにこの勧告を利用するか，概念をどのように理解するかなど現在もITU-Tの場で議論が進められ，各国での利用も進んでいます．今後も引き続き関係する文書が整備されることで活用が期待されます．

■X.1060コンサルティング

X.1060ではSOCやCSIRTも含めて今後のビジネスリスクも考慮したセキュリティ対応組織づくりを示しています．世界各国が合意した標準であるため，国内や他の国の間でセキュリティとして何をすべきかの共通言語にもなります．一方で，組織づくりのフレームワークだけであるため，実際に組織においてはどのように管理策を決めるのかなど，具体的な実施方法は書かれていません．それぞれの組織においてどのようなかたちになるかもさまざまです．また，この勧告は現在のところ規程類や審査，登録制度などはなく，ベストプラクティス的な活用になります．そのためセキュリティの組織をつくる場合や，見直しや改善をする際には各種アセスメントやコンサルティングを活用して，組織に合ったかたちにする必要があります．そのほかに，X.1060では実施すべきセキュリティの64のサービス（役割）も紹介されています．例えば実際にガバナンスをどうするのか，セキュリティの監視運用や脆弱性の診断はどうするのか，といった実務面についても考える必要があります．前述のISO/IECやISMAPのコンサルティングで情報セキュリティ全体のマネジメント面を強化し，X.1060のコンサルティングで組織体制を強化するような各種のコンサルティングや実務面でのソリューションを合わせて活用することで，より良いセキュリティの対策につなげることが可能です．

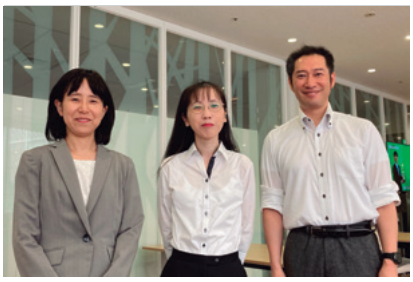
今後の展開

サイバー攻撃の高度化・多様化やクラウドサービスの普及等に対応するため，セキュリティに関する標準化や認証および評価制度も進化しています．そのため各企業や組織において，標準化規格への準拠や認証取得，セキュリティ強化等に取り組む際には，最新規格を参照しつつ規格がつくられた背景や意図，および認証取得の対象となる組織・システムの状況を把握・理解することが非常に重要です．

NTTテクノクロスでは，これらセキュリティ関連の標準化に引き続き貢献するとともに，最新の標準化動向に対応したコンサルティングサービスや最先端の各種セキュリティソリューションの提供を通して，安心・安全な社会の実現に取り組んでいきます．

■参考文献

(1) https://isms.jp/isms.html
(2) https://www.meti.go.jp/policy/netsecurity/is-kansa/
(3) https://www.ismap.go.jp
(4) https://csrc.nist.gov/publications
(5) https://www.ntt-tx.co.jp/products/service/security05.html
(6) https://www.digital.go.jp/policies/security/ismap-liu/



（左から）　土屋　直子／中田　美佐／
武井　滋紀

標準化規格の準拠やその認証取得については，規格のつくられた背景や意図，認証取得の対象となる組織・システムの状況を把握・理解することが非常に重要です．NTTテクノクロスの経験豊かなコンサルティングの活用や最適なセキュリティソリューションの利用により効率良く対応することができます．

◆問い合わせ先

NTTテクノクロス
セキュアシステム事業部　コンサルティング担当
TEL　045-212-7577
E-mail　telework.info-ml@ntt-tx.co.jp

＊5 ITU-T Recommendation X.1060：Framework for the creation and operation of a cyber defence centre.
＊6 TTC標準JT-X1060：サイバーディフェンスセンターを構築・運用するためのフレームワーク．