タイトル：GXP システムへのサイバーセキュリティの導入

著者:　Jason Nathaniel Young, John Patterson
(Pharmaceutical Engineering, 2018, Vol 38, No4, 59-62)

翻訳:　京都大学大学院医学研究科薬剤疫学分野　大学院生　小島　慶之（Nobuyuki KOJIMA)、大西　龍貴（Tatsuki ONISHI)、准教授　堀部　智久（Tomohisa HORIBE）

最近の WannaCry や Petya のようなサイバー攻撃は、GxP コンピュータ化システムに影響を与え、いかにして自動化製造実践規範（Good automated manufacturing practices; GAMP）®5 に準拠した従来のコンピュータ化システムのバリデーションを使ったサイバースペースからのリスクに対処するかという疑問を呈した。本稿では、GxP コンピュータ化システムのライフサイクル管理と、これに関連した患者の安全に影響を与えうるサイバーセキュリティのリスクを探る。

世界中のいずれの国際製薬技術協会（International Society for Pharmaceutical Engineering；ISPE）の会議を見ても、サイバーセキュリティへの関心が顕著に高まっていることが分かる。残念なことに、この関心の高まりには混乱と誤解も伴っている。サイバーセキュリティの問題を適切に議論するために、サイバーセキュリティとは何であり、どのように実施されるかの簡単な概要から始めたい。

サイバーセキュリティはサイバースペース内のシステムや情報へのリスクを減らすためのステークホルダーによる一連の措置である。これらの措置には重要な情報インフラストラクチャ保護の機密性、完全性、可用性（“CIA トライアド”として知られている)の希求に対応するため、情報セキュリティのあらゆる側面が集約されている。

GxP 規制対象コンピュータ化システムを保護するという状況の中では、サイバーセキュリティはシステムと患者の安全の双方のリスクを減ずる技術的、手順的管理を適用する手法のことである。これは 2 つの方法で達成される：システム脆弱性とデータ完全性への脅威の特定と対処、そしてコンピュータ化システムバリデーション（Computerized Systems Validation; CSV）と是正措置予防措置（Corrective and Preventive Action; CAPA）のための既定のフレームワークと技術管理へのトレーサビリティの提供である。これらの措置は情報セキュリティ管理システム（Information security management system; ISMS）* を介して実施され、これは既定のサイバーセキュリティのフレームワークおよび社内の方針と手順に沿って運用される。

ISMS は標準的サイバーセキュリティの職分と責務に基づいて構築された独立の組織となり、情報セキュリティのガバナンス強化の実施を担う。ISMS には以下のような職位を含む：

- 情報セキュリティ担当主任
- 情報セキュリティ担当者
- 情報セキュリティマネージャー
- 情報システムセキュリティ担当者

職務の適切な分担を確実に行うためには、これらの職位は情報技術（Information Technology; IT）ガバナンスに組み込まれている場合もあるかもしれないが、IT ガバナンスからは独立しているべきで、その一部であってはならない。これは ISMS の重大な要素である、というのもマネジメントの立場であれ、ガバナンスの立場であれ、セキュリティの目的は、その構成が組織の方針と手順に準拠して管理されることを検証することにあるからである。これら既定の職分と責務は、企業内からサイバーセキュリティを集中管理するため、多層防御のような概念を用いて、サイバーセキュリティを実行する方法論に依拠している。いうなれば”多層防御”とは、セキュリティ管理がシステムにセキュリティを供する組織構造の各層で強化されることである。この基本的な概念は、標準化、コンフィギュレーション管理、脆弱性/脅威監視のセキュリティ面を管理する際に堅持される。

このような包括的観点は、GAMP 5 ガイドライン内でのサイバーセキュリティの実施を困難にしうる、というのも、どの業界であれ中央集権的なプロダクションシステムはサイバーセキュリティ管理要件の個別性によって問題となるものだからである。

サイバーセキュリティ職員は決まったように作業するように訓練されているため、企業文化の違いが品質部門と ISMS の間に摩擦を生み出す可能性がある。GAMP 5 の術語とシステムバリデーションの方法は、国際標準化機構（ISO）や情報システムコントロール協会†（ISACA）の定義と齟齬を生じ、コミュニケーション不良を来たしうる。他業界と政府機関の品質部門は ISMS を用いることで、ISO と ISACA のフレームワークに沿ったバリデーションプロセス内の技術的管理とサイバーセキュリティ管理を検証している。米国政府の品質部門は誰一人として、たとえば、他業界の内部機構によって適格とされたシステムに管理的アクセス権限を持たない。政府機関の品質部門は、システム管理をするサイバーセキュリティ担当者にアクセス権限を要求することになる。

生命科学では、品質部門は GxP 規制対象システムに関する GAMP 5 セキュリティ手順の確実な遵守を担保している。これが重要となるのは、GxP 規制対象システムと関連するインフラストラクチャの双方に、サイバーセキュリティ管理がどのように、またどこで実施されているかを、規制当局はこれまで以上に強調しているからである。品質部門がどのように CSV プロセスに伴うサイバーセキュリティを管理、実施していくべきかについての疑問も生じている。

2008 年以来、GAMP 5 は米国国立標準技術研究所（National Institute for Standards and Technology; NIST）と ISO 規格に依拠している。しかしながら、より近年のサイバーセキュリティの方法ははるかに複雑である。サイバーセキュリティ訓練におけるディスカッシ

ョングループでは、この複雑さからの混乱を頻繁に目にする。

品質マネジメントシステム（Quality Management System; QMS）の組織構造と、ISMS 運用とプロセスの統合に関するいくつかの質問の例を挙げる：

- サイバーセキュリティの観点では、QMS 内の GxP 規制対象システムに関する方針と手続きを作成する際の ISMS 代表者の役割は何か？
- 品質部門、セキュリティ関連の検証を行う ISMS のメンバー、IT 部門の間でどのように職務を分担したらよいか？
- GAMP カテゴリ 1（インフラストラクチャ）システムに由来する GxP 規制対象システムへのリスクにはどのように取り組むべきか？
- 脅威と脆弱性への管理はどのように行うべきか？より具体的には、CAPA プロセス内で高度な脅威や脆弱性を追跡し解決するには、一般的な脆弱性や曝露をどのように用いればよいか？

その他の質問は、明確化が必要な CSV プロセス内の分野に焦点を当てている：

- 従来の GAMP カテゴリ 1,3,4,5 の使用法からすれば、初期のリスク評価においてシステムは影響、セキュリティカテゴリ、データ分類にどのように取り組むべきか？
- サイバーセキュリティ要件がデータの完全性に影響するかしないかをどのように定義したらよいか？
- ISO / IEC 27001 や COBIT 5 のようなフレームワークを使用する場合、GAMP 5 や米国連邦規制基準（US Code of Federal Regulations；CFR） 21 第 11 章のような規制に対して、サイバーセキュリティ管理に対するトレーサビリティはどのように使用されるか？
- インターネットセキュリティセンター‡(Center for Internet Security; CIS)のベンチマークやクラウドセキュリティアライアンス‡ (Cloud Security Alliance; CSA)のようなサイバーセキュリティ技術管理基準は、技術的管理のトレーサビリティにどのように用いられるか？
- どのような試験方法や最善の措置を、運転時適格性評価と据付時適格性評価において用いることができるか？

ここに挙げるのは、対処の方策や適格化システムへの影響について合意が必要な重要領域である。

コラボレーション

ISPE 指導チームメンバーである Chris Reid が産業界のためのサイバーセキュリティガイダンスを ISPE、ISACA との協働で作成を宣言したことは幸いである。この取り組みは、ISPE の最高レベルの指導者によって支持されている。議論によるガイダンスがサイバーセキュリティコミュニティに対しては ISACA から、品質部門に対しては IPSE から作成され

ると期待されている。

これを念頭におくと、GxP 関連システムのサイバーセキュリティコミュニティは、ガイダンスでサイバーセキュリティの技術的管理のための追跡方法と同様に職分と責務も扱うべきと想到される。たとえば、ペイメントカード業界（Payment Card Industry; PCI)は、PCI データセキュリティ基準（PCI Data Security Standard ; DSS）を使用しており、ウォルマートから地元のレストランまでのさまざまな組織に、支払いシステムのサイバーセキュリティに対する責務においてのガイダンスを発行している。要件の 1 つには、侵入テストの必要性がある。PCI は、試験、方法、範囲、タイムフレーム、報告メカニズムに関する詳細なガイダンスを提供している。ISPE は新しいガイダンスを作成するにあたり、これらの方法や概念のいくつかを検討するだろう。

GXP コンピュータ化システムへの ISMS の支援

なぜ明確な職分と責務が重要となるのか、前出の職分の中から情報セキュリティ担当主任すなわち CISO の責務を見てみよう。

ISACA によれば、CISO は企業の情報セキュリティプログラムに責任を負い、さらに具体的には、ISMS が会社の戦略的サイバーセキュリティ計画に沿って確定、維持されることを担保する。CISO の責務のうちで重要な要素は、QMS を支援する構造を策定することである。CISO はまた、企業のセキュリティ方針と手順を実行するため、QMS を支援する ISMS のガバナンス部分が、情報セキュリティマネージャーの指示と干渉しないことを担保しなければならない。CISO はまた、インフラストラクチャや GxP 規制対象システムを含め、組織全体にわたってサイバーセキュリティ要求を均衡させなければならない。これらすべてを達成するため、戦略的計画には職務の分担作業が含まれ、また、組織規模にあわせてスケールできなければならない。

ISACA によると、ISMS は以下の分野を調整、計画、構成、管理しなければならず、それらのうちいくつかは QMS 内で顕著な役割を果たしている：

- IT 管理フレームワーク
- 戦略
- 企業の構造
- イノベーション
- ポートフォリオ
- 予算とコスト
- 人的資源
- 関係性
- サービス契約
- サプライヤ
- 品質

- リスク
- セキュリティ

サイバーセキュリティの方針と手順が QMS 内で対処されているのを確認することは重要である、なぜならそれらが組織全体のリスクを決定する役割を果たすからである。GxP 規制対象システムと ISMS に関連する問題に対処するひとつの方法は、QMS のセキュリティ機能を支援する情報セキュリティ担当者（またはその他のガバナンス職位）を設けることである。GAMP Records and Data Integrity Guide のいうところのデータスチュワードは、この職務のための優れた選択肢である。

ISMS は、インフラストラクチャのサイバーセキュリティ体制に対する責任があり、インフラストラクチャから GxP 規制対象システムへのリスクに対処するためのプロセスをも明確にしなければならない（逆も同様)。非常に重要な分野はロギング、モニタリング、アーキテクチャ、アクセスコントロールである、なぜならこれらはインフラストラクチャからのサービスを必要とするプロダクションシステムに直接影響するためである。多くは文書化された手順で実施できるが、文書化されていないものは CSV プロセス中に要件の定義と試験に関して、個別の方法が必要かもしれない。

インフラストラクチャに加えて、もうひとつの重要な構成要素は、ISMS による脅威と脆弱性の管理である。GxP 規制対象システムのデータ完全性に影響するものは、CAPA に含めるための明示的方法を備えるべきである。ISMS 運用のほとんどは、アラートや掲示板に対するローカルコンピュータ緊急対応チームの積極的監視、脆弱性スキャンソフトウェアのようなセキュリティデバイスからの結果をモニターすることであり、これには追跡と修復のためのトレーサビリティが活用される。

サイバーセキュリティ管理と試験

職分と責務の問題以外にも、ISPE によるガイダンスがサイバーセキュリティを改善するのに役立つ分野がある。ほとんどは技術的なものであるが、同様に手順に関する例もいくつかある。サイバーセキュリティのリスクに対処するにあたり、プロセスの最も重要な部分は、初期リスク評価にある。初期リスク評価では、使用される技術的管理と試験方法を決定するためにシステムのセキュリティカテゴリ（Security Category; SC）が確立されるべきである。SC は、データ分類、資産評価、脅威モデリング、システムへの影響などの項目の組み合わせからなる。内部の方針と手順に関する判断は、適用されるセキュリティ管理を決定するものであるため、初期リスク評価中になされるべきである。NIST（National Institute for Standards and Technology；米国国立標準技術研究所）は、SC の決定に当たり CIA トライアドのいずれに対してでも、最高レベルのインパクトの使用を推奨している：潜在的インパクトの許容値は低、中、高であるところ、

SC = {（confidentiality, impact), (integrity, impact), (availability, impact,）}

と表現される。

これは、GAMP カテゴリ 3、4、5 に基づく従来の GxP 試験とは異なる。サイバーセキュリティのリスクを検討する際には、すべてのシステムは初期リスク評価中に定義されたコンピュータ化システムの SC によって試験される。インターネットセキュリティセンターによるこれらのベンチマークは、ここに挙げたような方法論と組み合わされて、異なるレベルのセキュリティ管理を提供している。

SC はひとたび確定されると、適切なサイバーセキュリティ管理をデータ完全性の問題に適用するテンプレートを作成するために使用される。ISPE と ISACA からのガイダンスは、この分野で特に有益となる。品質部門がどのように技術上あるいは手順上のサイバーセキュリティを決定すべきかを決定するには、ISMS との時間と調整がいるだろう、というのもこれらの管理の多くがインフラストラクチャの保護内で提供されるからである。この段階で作業の重複を避け、サイバーセキュリティ管理を参照することは有益である。

PII

もう 1 つ考慮すべきことは、個人を特定できる情報（Personally Identifiable Information; PII）を取り扱ういかなるシステムにおいても PII 保護の必要があることである。ここで、典型的な状況に基づいた ISPE と ISACA のガイダンスは、これらの方法を個々の組織で作成するのに必要な作業量を削減するのに役立つ。

保存データ（Data at Rest; DAR）や転送中のデータを保護するために用いられる暗号化は、インフラストラクチャによってデータの一部が状況に応じてどのように提供されるかを明らかにする。たとえば、PII を含む GxP 規制対象のポータブルシステムは、DAR 暗号化によって保護されなければならない。データの機密性と完全性を保護するために考案されたこの種の管理は、通常、インフラストラクチャサービス（例えば Microsoft の BitLocker）によって提供される。

GxP 関連システムのデータ機密性を考慮すると、品質部門の職員はサイバーセキュリティ専門家から多くの恩恵を得ることができる、というのもそれらの専門家は欧州連合（European Union; EU）の一般データ保護規則（General data protection regulation; GDPR）のような規制に精通しており、企業が 72 時間以内にデータ侵害や不正侵入されたシステムを EU に通知することを可能にする報告メカニズムを備えているからである。これが重要であるのは、GDPR が最大 2,000 万ユーロか世界年間売上高の 4%のいずれか高い方の罰金刑を課すことができることによる。

ISPE からのガイダンスは、サイバーセキュリティを向上させるのに役立つ

仕様文書内で示された管理に加え、関連する適格性評価にも ISPE のサイバーセキュリテ

ィ試験ガイダンスを役に立てることができる。たとえば、どの段階で、どのような条件下で侵入テストや簡単な脆弱性スキャンを実行する必要があるのか？PCI DSS 基準は、侵入テストをいつどのように実施すべきか明確なガイダンスを提供し、GxP 環境内での適用に役立つ。たとえば、インターネットを介して公的にアクセス可能なあらゆるシステムでは、侵入テストを毎年実施するのがよい。それ以外のシステムでは、その機能、構成、ネットワーク内の配置によっては、そのような費用のかかる広範な評価を必要としないだろう。適格性評価において、ほとんどの作業を試験方法の作成にあてることになるのは高度に技術的であるからだが、ひとたび職分と責務に対処すれば最も解決の容易な問題となる。

最終的にはリスクの評価と受容の現実的な見解は、“ゴミからはゴミしか生まれない”という IT 格言によって要約することができる。セキュリティギャップがバリデーション中も保たれるならば、サイバーセキュリティは GxP に関連するものであれしないものであれ、いずれもシステムリスクアセスメントに含まれていないと想定することが自然であろう。これは間違いであるのみならず、誤ったセキュリティ感覚をさえ与える。

リスクアセスメントにおいては、データ完全性、リスクの受容や緩和など他の GxP 管理のサイバーセキュリティ要件に適当なリスクレベルを割り当てるために多くの作業がさかれなければならない。これらの管理が CAPA とインシデント対応にどのように影響するかも同様に調査されるべきである。この種の問題を修正するのに、いかなるタイムフレームを許容すべきか？誰が修復を監督するのか？これはどのようなプロセスの機密性にも影響するような全てのゼロデイ§脆弱性に対して言えることである。

要約

サイバーセキュリティへの脅威が頻度も強度も増加する中、ISPE のような組織がそのようなリスクに対処するためのガイダンスを継続的に改善することは重要である。ISACA と ISPE の協働は、生命科学のコミュニティが直面する多くの課題を理解する上で大きな前進となろう。セキュリティ専門家として、私たちの目標は、GAMP 5 を強化し、プロセス内の ISMS の役割を明確にし、GxP 関連のシステムとデータに対するリスクにより包括的な方法で取り組むことである。

本文以上

＜図表の説明＞

表 A　略語と頭字語