一般口演
# 一般口演8
# セキュリティとプライバシー保護1
2017年11月21日(火) 14:15 〜 15:45 H会場 (10F 会議室1008)

[2-H-2-OP8-3] 「政府機関等の情報セキュリティ対策のための統一基準群」と病院情報セキュリティポリシーの適合性についての考察

小南 亮太, 石割 大範, 中川 陽介, 美代 賢吾 （国立研究開発法人 国立国際医療研究センター）

背景
平成28年度サイバーセキュリティ基本法の改正に伴い、内閣サイバーセキュリティセンター（以下 NISC）より「政府機関等の情報セキュリティ対策のための統一基準群」（以下統一基準群と言う）が決定され、全国の独立行政法人等も同等の情報セキュリティ規程の整備が要求されている。
国立国際医療研究センター（以下 NCGM）でも統一基準群に合わせて規程改訂を行ったが、統一基準群の適用が難しい課題が散見されたため、医療機関に適用する際の課題の考察を行う。
調査方法
1.統一基準群の概要
統一基準群とは、 NISCが規模・業種の如何を問わず行政機関等のサイバーセキュリティに関する対策の基準として策定したものである。
2.各規程の NCGMへの適用の可否の検討
各項目について内容の精査を行い、医療機関の特性上そのまま適用できない項目の抽出を行った。
結果と考察
規程117項目のうち医療機関の課題となり得る項目は10項目であった。
代表的な課題として、下記項目が挙げられる。
1.セキュリティエリアのクラス分け
情報取扱場所での施錠や個人の出入の記録等、厳密な管理を求められているが、患者等も出入りする病棟内をセキュリティレベルの区域ごとに厳密に対応することは現実的ではない。
2.体制の整備
システムごとにセキュリティ責任者を設けることを求められているが、利用部門に運用・報告・対処の責任を負わせることは困難である。
3.外部委託
多様なシステムを保有する医療機関では構築を外部委託することが多いが、委託やクラウド、 Webサービスの利用にあたって、委託者による監査の受入や委託先個人情報の提出を求めることは敷居が高く、業者の選定を阻害する恐れがある。
上記事項を技術的に解決するにはセンサー設置等コストを必要とする。そのため統一基準群を医療機関に沿うように修正し、区域対策の改変、システム管理体制の集約化、委託業者選定基準を変更することで、対応する必要がある。

「政府機関等の情報セキュリティ対策のための統一基準群」と病院情報セキュリティポリシーの適合性についての考察

小南亮太[*1]、石割大範[*1]、中川陽介[*1]、美代賢吾[*1]
*1 国立国際医療研究センター

Consideration on compatibility between " Unified Standard Groups for Information Security Measure for Government Organizations " and hospital information security policy

Ryota Kominami[*1], Hironori Ishiwari[*1], Yosuke Nakagawa[*1], Kengo Miyo[*1]
*1 National Center for Global Health and Medicine

With the amendment of the Basic Act on Cybersecurity in 2016, National Center of Incident readiness and Strategy for Cybersecurity (NISC) decided "Unified Standard Groups for Information Security Measure for Government Organizations", and it also have been required to establish equivalent information security regulations in independent administrative institutions nationwide.

The National Center for Global Health and Medicine (NCGM) also revised the regulations in accordance with the unified standards groups. However, due to some problems which is difficult to apply to the unified standards groups, we examined the issues when applied to medical institutions.

In addition to investigating the differences between other guidelines from ministries and agencies and unified standards groups, we identified the points that are difficult to apply to medical institutions within the unified standards groups.

There are discrepancies in terms of the rating of information and the points such as (1) organization / system improvement, (2) information transport / transmission, (3) management of areas handling information, (4) outsourcing contracts, and (5) cryptographic / electronic signatures, therefore it is necessary to modify the regulation to apply it to medical institutions.

Keywords: security, law, hospital

1. 緒論

平成28年度サイバーセキュリティ基本法の改正に伴い、内閣サイバーセキュリティセンター（以下 NISC）より「政府機関等の情報セキュリティ対策のための統一基準群」1)（以下統一基準群）が決定された。この統一基準群は、平成27年度までは省庁のみを対象とし準拠を求めていたが、平成 28 年度から全国の独立行政法人等に対しても、NISC と所管省庁の規程を参照・準拠する形で、同等の情報セキュリティ規程を整備するよう要求されている。

一方で、医療情報の業界においては、平成29年5月に第5 版が公開された「医療情報システムの安全管理に関するガイドライン」2) （以下「安全管理に関するガイドライン」）のように、情報システムの利用について基準を示した文書があり、内容において統一基準群と少なからず重複する要素を有している。

その他にも、厚生労働省から発行され、平成 22 年度に改正された「医療介護関係事業者における個人情報の適切な取り扱いのためのガイダンス」3)や、平成 30 年度での施行を目指している「医療分野の研究開発に資するための匿名加工医療情報に関する法律案」4)など、医療機関における個人情報の取り扱いに言及しているガイドラインや法律が存在するほか、医療機器の安全性の管理については平成26年度に発行された「JAHIS 製造業者による医療情報セキュリティ開示書ガイド」6)、平成 28 年に改正された「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」7)、同じく平成 28 年に総務省と経済産業省で策定された「IoT セキュリティガイドライン Ver1.0」8)などがあり、安全管理に関するガイドラインはこれらを参照して策定されている。

ガイドラインはいずれも法的に従うことを義務付けるものではないが、独立行政法人の医療機関に対しては統一基準群への準拠性を問うNISCによる監査が開始されており、内部の規程や運用状況について見直さざるを得ない状況となっている。

国立国際医療研究センター（以下 NCGM）でも統一基準群に合わせて平成 28 年度に規程の改訂を行ったが、実際の運用面では統一基準群の適用が難しい課題が散見されたため、医療機関に適用する際の課題の考察を行った。

2. 目的

医療機関における統一基準群の適用の可否を検討し、医療機関特有の課題との齟齬を明らかにする。また、関連する他のガイドラインとの差異を調査し、医療機関において規程として定める際の方針について提言する。

3. 方法

統一基準群とは、NISC が規模・業種の如何を問わず行政機関等のサイバーセキュリティに関する対策の基準として策定したものである。全体で 66 ページからなり、組織・体制の整備、情報セキュリティ対策の基本的枠組み、情報の取り扱い、外部委託、情報システムのライフサイクル、情報システムのセキュリティ要件、情報システムの構成要素それぞれにおける対策、情報システムの利用における対策について、遵守事項を定めている。ここで定められている内容について、（1）他のガイドラインと内容の比較を行い、内容に差異の見られる項目を洗い出したほか、（2）統一基準群の各項目について内容の精査を行い、医療機関の特性上そのまま適用できない項目の抽出を行った。

4. 1. 関連する他ガイドラインとの比較

医療機関における情報システムの管理や運用をとりまとめ定めたものとして、「安全管理に関するガイドライン」との比較を行った。

多くの項目において概ね内容は近しいものであったが、情報の格付・整理については異なる内容となっていた。

統一基準群では、「3.1.1 情報の取扱い 遵守事項(3)」において、「行政事務従事者は、情報の作成時及び府省庁外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること」と定めており、組織内で取り扱う文書、メールを含めたあらゆる文書に対して機密性、完全性、可用性の格付けを徹底して実施することを求めている。これに対し、「安全管理に関するガイドライン」では、6.11 外部と個人情報を含む医療情報を交換する場合の安全管理において、「医療機関等は交換しようとする情報の機密性の整理をする必要がある。基本的に医療情報をやり取りする場合、確実なセキュリティ対策は必須であるが、例えば、予約システムが扱う再診予約情報のように機密性の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる」として、必要以上の対策の実施を求めていない。

統一基準群で示されている情報の格付けは以下の表1のとおりである。

機密性3	秘密文書に相当する機密性を要する情報を含む情報
機密性2	不開示情報に該当すると判断される蓋然性の高い情報を含む情報
機密性1	不開示情報に該当すると判断される蓋然性の高い情報を含まない情報
完全性2	改ざん、 誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適切な遂行に支障を及ぼすおそれがある情報
完全性1	完全性2情報以外の情報
可用性2	その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障を及ぼすおそれがある情報
可用性1	可用性2情報以外の情報

ここで定められている情報の格付けを医療機関に適用した場合、電子カルテや処方箋、検査画像やオーダー指示書の一つ一つに対して、格付けを明記することになる。カルテの場合は、患者からの要望に応じて開示をする場合もあるが、個人情報を大量に含んだものでもあり、機密性のいずれに該当するのか判断が困難である。

4.2. 統一基準群の医療機関への適合性

統一基準群の規程117項目のうち、医療機関の課題となり得る主な項目は5項目であった。

表2 医療機関において課題となる項目

No	基準群 項番	標題
(1)	2.1.1(4)	組織・体制の整備
(2)	3.1.1(6)	情報の運搬・送信
(3)	3.2.1	情報を取り扱う区域の管理
(4)	4.1.1(2)	外部委託に係る契約
(5)	6.1.5(c)	暗号・電子署名

(1) 組織・体制の整備

統一基準群では、組織内でのシステム・セキュリティに関して、最高情報セキュリティ責任者(CISO)や CSIRT(Computer Security Incident Response Team)など、システム・セキュリティについての管理責任者を設けることが求められている。

管理責任体制の一つとして、部署ごとに「課室情報セキュリティ責任者」を定めることが求められており、運用・報告・一次対処の責任を負うこととなっている。これは、薬剤システムや検査システムなど、多様なシステムが存在する医療機関においては、各システムの主利用部門に当該システムのセキュリティ対応の管理責任も課すこととなる。現場の医療従事者に対してセキュリティ事案の一次対応を担わせるのは、技術的にも運用的にも困難である。

(2) 情報の運搬・送信

要管理対策区域外に要保護情報を運搬・送信する際の手法について、安全確保に留意した方策を定めることを求められている。医療機関では、レセプトオンライン請求やがん登録など、省庁から送信方法を定められたデータ送信業務が存在する。これらについては、例外事項として規程に定めるか、省庁として送信方法の見直しが必要である。

(3) 情報を取り扱う区域の管理

個人情報を取り扱うエリア、もしくは機器の存在する場所に対して、物理的対策と入退室管理を統一基準群では求めている。しかし、医療機関では患者が病棟に泊まっており、ベッドサイドには患者の状態を管理するモニタや電子カルテ等の機器が設置されているのが一般的である。また症状によってはナースステーションで患者を診るケースもある。患者が急変し危急の対応を要する場合もある医療機関においては、病室単位で入退室記録を行うのは現実的ではないため、基準を医療機関の特性に応じて読み替える必要がある。

(4) 外部委託に係る契約

医療機関における外部委託については、平成5年に策定された「病院、診療所等の業務委託について」5)が医療関連サービス振興会より発表されていたが、情報システムについての外部委託は記載されていなかった。統一基準群では、情報システムについて外部委託する場合の委託先業者へのセキュリティ対策を規定しているが、この中で(ア)情報セキュリティ監査の受入れ(イ)サービスレベルの保証、の2点を仕様に含めることを求めている。このうち(ア)については、医療機関側が監査主体として委託業者を監査することを受け入れるように求めているものである。この基準は、省庁における基準としてはあり得ると思われるが、医療機関に限らず独法がシステムベンダーに対してセキュリティ対策の状況を監査するというのは、技術的に不可能であると言わざるを得ないほか、費用面でも医療機関、委託業者双方に負担をかける行為であり、業務の遂行を阻害する可能性が高い。

この点については、「政府機関の情報セキュリティ対策のための統一基準群(案)」に対する意見募集の結果の概要 9)の中でも指摘されており、「情報セキュリティに関して信頼性の高いサービスを提供しているかどうかは、各契約当事者ではなく第三者による事業者の監査レポートや実績等により十分に確認可能であるため、各省庁は実地監査ではなく、多様なこれらの情報により確認するのが妥当である。また、複数の利用機関からの監査の受入れは、それ自体が重大なセキュリティ懸念を生じうることから、国際的な機関による代表代理監査を許容可能とすべきである」と指摘し、当該規定の削除を求めている。

(5) 暗号・電子署名

統一基準群では、電子署名が必要な業務においてはGPKI(政府認証基盤)を使用することを定めているが、医療機関で

はレセプトオンライン請求などでは HPKI（保健医療福祉分野公開基盤）を使用することが定められているほか、学術機関では国立情報学研究所が発行する UPKI を使用するケースもあるため、一律に GPKI の使用を求めることはできない。

5. 考察

結果にて示した統一基準群の課題について、医療機関に適用するためにはそれぞれ以下のような規程の読み替えが必要である。

（ア）情報の格付

統一基準群に示される格付の区分は行政事務文書に限定して適用するものとし、医療業務で使用される文書には別の格付を設けるべきである。例えば、個人情報の有無、患者本人以外への情報提供の有無を基準とし、何も明示しなければ個人情報無し、本人以外への提供無しである、というルールを設けること等が考えられる。

（イ）組織・体制の整備

医療機関における情報セキュリティ対策においては、情報システムに明るいとは限らない各部署の責任者に「課室情報セキュリティ責任者」として運用・報告・一次対処の責任を負わせるのではなく、迅速な報告のみをその責とするべきである。各システムのセキュリティ対応は、医療機関内の情報システム部門に集約して運用と対処が行えなければ、診療行為と並行しての迅速な対処、判断は困難である。

（ウ）情報の運搬・送信

要保護情報の運搬・送信方法については、行政から指定された方法については例外とする旨を規程に追加するべきである。また、行政への周産期データの提供など、一部の行政指定の送信方法についてはセキュリティ上の懸念事項があるため、行政側の見直しを要求したい。

（エ）情報を取り扱う区域の管理

医療機関における個人情報を取り扱う区域の管理については、より細かい分類で規定するべきである。例えば、事務部門、外来・受付、病棟で、以下のように基準を分けることを提案する。

・事務部門の区域は、施錠による物理的対策をとり、入退室の記録を取る。

・外来、受付の区域は、扉やカウンターによる物理的対策をとり、機器はセキュリティワイヤーで固定する等の対策をとる。営業時間外は扉の施錠、もしくは施錠できるキャビネット等に機器を保管する。

・病棟の区域は、病棟の入口において入退室者の確認を行い、監視カメラ等で区域の入退室者の記録を取る。病室間やナースステーションでの入退室の記録は業務を阻害し、患者救命を遅らせるリスクがあるため行わない。

（オ）外部委託に係る契約

医療機関がシステムベンダーに対して「情報セキュリティ監査の受入れ」を要求し実施するのは困難であるため、「情報セキュリティ監査受診実績の証明を、医療機関が求める時に提出することを仕様に含める」と規定することを提案する。

（カ）暗号・電子署名

GPKI だけでなく HPKI、UPKI を使用する場合も考えられる。電子署名の認証局を制限するのではなく、

・電子署名が必要な場合において自己証明書を使用しない
・企業認証型 SSL サーバ証明書以上の信頼性を基準とする
・電子政府推奨暗号リストで推奨された技術を使用する

といったように、技術的な制限を規定するべきである。

6. 結論

統一基準群は規模の大小を問わずあらゆる機関で使用できるものを目指して策定されたものであり、平成 17 年度に第 1 版が発表されて以来、7 度の改正を経て改良されてきたものである。改正の都度、改正案に対して Web ページ上で意見の募集が行われていたが、いずれもシステムベンダーや情報処理分野の協会による意見であり、医療機関の目線では検討されていない。特に、本論の結果で示した項目については記載の内容のままでは医療機関の特性上適用が困難である可能性がある。独法に対しては統一基準群の内容に基づいて NISC より情報セキュリティ監査が入り、内規についても準拠することを求められるが、対応困難な項目については各医療機関で規程の修正を行い、統一基準群の内容に代わる対策を定めていく必要がある。

参考文献

1) サイバーセキュリティ戦略本部. 政府機関等の情報セキュリティ対策のための統一基準群（平成 28 年度版）. 内閣サイバーセキュリティセンター, 2016[https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf (cited 2016-Oct-21)]
2) 厚生労働省. 医療情報システムの安全管理に関するガイドライン. 医療情報ネットワーク基盤検討会, 2017[http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf (cited 2017-Jul-31)]
3) 厚生労働省. 医療介護関係事業者における個人情報の適切な取り扱いのためのガイダンス. 2017[http://www.mhlw.go.jp/file/06-Seisakujouhou-12600000-Seisakutoukatsukan/0000164242.pdf (cited 2017-Jul-31)]
4) 通常国会. 医療分野の研究開発に資するための匿名加工医療情報に関する法律案. 2017[http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g19305053.htm (cited 2017-Jul-25)]
5) 医療関連サービス振興会. 病院、診療所等の業務委託について. 厚生省健康政策局指導課長通知. 1993[https://ikss.net/medical/pdf/hourei_h50215_14.pdf (cited 2017-Jul-31)]
6) 保健医療福祉情報システム工業会. JAHIS 製造業者による医療情報セキュリティ開示書ガイド. 2014[https://www.jahis.jp/files/user/images/kaiji-manual_Ver2.0.pdf (cited 2017-Aug-18)]
7) 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律.2016[http://www.houko.com/00/01/S35/145.HTM (cited 2017-Aug-18)]
8) 総務省・経済産業省. IoT セキュリティガイドライン Ver1.0. IoT 推進コンソーシアム. 2016[http://www.soumu.go.jp/main_content/000428393.pdf (cited 2017-Aug-18)]
9) サイバーセキュリティ戦略本部.「政府機関の情報セキュリティ対策のための統一基準群（案）」に対する意見募集の結果の概要. 内閣サイバーセキュリティセンター, 2016[https://www.nisc.go.jp/active/general/kijun_comments.html (cited 2016-Oct-21)]