

**WATSON** Coaching & Consulting Group

## 医療におけるサイバーセキュリティ Vol.2

サイバーセキュリティ対策の5つの視点

The background of the slide features a hand holding a glowing, orange and red digital sphere. The sphere is surrounded by a network of glowing lines and nodes, suggesting a digital or cyber environment. The text 'CYBER SECURITY' is prominently displayed in a large, metallic, textured font across the center of the image. The overall aesthetic is dark and futuristic, with a focus on digital security.

# CYBER SECURITY



# CONTENTS

はじめに	3
サイバーセキュリティ対策の5つの視点	4
① ベンダー/サプライヤーが自分の医療機関に合っているか？	5
② 組織横断的にセキュリティ対策を検討しているか？	6
③ 「完璧」ではなく「改善」をめざす	7
④ 信頼することと検証することは別の話	8
⑤ 対策を施した後も継続してチェック・検証する	9

## はじめに

サイバー攻撃への対策を考えると、医療機関はどうしてもセキュリティソフトウェアベンダーに頼りがちだ。情報システム要員の不在や不足でそうせざるを得ない面がある。

しかし、やむなくそうする場合でも、医療機関として独自の視点はもっておきたい。そうしなければ、ベンダーの言うことをすべて鵜呑みにしてしまう可能性が出てくるからだ。

ベンダーはベンダーとしての意見や提案がある。それ自体を否定する理由はない。重要なのは、医療機関側がサイバー犯罪対策を立案・構築してゆく上で、明確な判断基準をもつということだ。そうすることで、すべてをベンダー任せにするのではなく、医療機関が自らの視点と自らの意思でサイバー犯罪対策を立案できる土壌が生まれる。

その上で、サイバー犯罪対策の立案に際しては、信頼できる第三者に入ってもらい、特定のベンダーに偏らない客観的且つ中立的な視点で、対策の立案と必要な製品を提供してくれるベンダー選定まで行えればベストだろう。

本ホワイトペーパーでは、医療機関がもつべき重要な5つの視点を解説する。

## サイバーセキュリティにおける5つの視点

医療機関がそのサイバーセキュリティ対策を講ずる際、サードパーティベンダー（セキュリティ・ソリューションやツールを提供するベンダー）の関与する度合いは以前にも増して高まっている。サイバー攻撃の手口は高度化・複雑化しており、医療機関が独自にサイバーセキュリティ対策を講ずることは難しい。結果、どうしてもベンダーに頼りがちになるのだが、それが「すべてベンダー任せ」の組織文化を形成し、サイバーセキュリティ対策をベンダーに丸投げしてしまうことを助長しがちだ。

もちろん、個別のサイバーセキュリティ製品やツールについてはそれぞれの専門ベンダーから提供を受けざるを得ないが、その前に医療機関自身がサイバーセキュリティ対策を講ずるに際して、しっかりした「視点」をもつことが求められる。

今回の「医療におけるサイバーセキュリティ Vol. 2」では、個別のセキュリティソリューションやツールを選ぶ前に、医療機関がまず先に意識すべき「5つの視点」について解説する。その5つの視点とは、

- ① ベンダー/サプライヤーが自分の医療機関に合っているか？
- ② 組織横断的にセキュリティ対策を検討しているか？
- ③ 「完璧」ではなく「改善」をめざす
- ④ 信頼することと検証することは別の話
- ⑤ 対策を施した後も継続してチェック・検証するである。

## 医療機関側で サイバーセキュリティ対策 に関する視点をもつ



## ①ベンダー/サプライヤーが自分の医療機関に合っているか？

意中のベンダーと契約する前に、今一度全体感を確認してみるのはいわゆる有効だ。ベンダー各社はそれぞれ異なった製品やソリューション、ツールなどを販売しているだけでなく、それぞれ異なるメンテナンス方針やサイバーセキュリティに対する考え方などをもっている。また、顧客である医療機関との付き合い方においても各ベンダー独自のスタイルがある。

単に製品や安価だから・・・、ネットで調べたら評価が高かったから・・・、といった理由だけでベンダーを選ぶことは避けたい。医療機関と一緒にになってサイバーセキュリティ対策に取り組んでくれるベンダーなのか、製品を売ったら、あとは定められた製品メンテナンスを提供するだけか。サポートセンターの受付時間は平日だけか、土日祝も対応してもらえるのか、などは基本的な重要事項として事前にチェックしたい点だ。

医療機関は、土日祝は外来は休診となるところが大半だが、入院病棟は稼働しており、急患の受付も行うところもある。情報システムは稼働している。サイバー攻撃に平日・土日祝の区別はない。サポートセンターが土日祝に対応しているかどうかだけでなく、いざサイバー攻撃が発生した場合、その対応にも曜日にかかわらず医療機関と一緒にあたってくれる（有償は当然）のか。ベンダーのサービスレベルを確認しておくことはきわめて重要だ。

サイバーセキュリティ対策においては、こうした体制面が重要であり、仮にその辺りに不安が残るベンダーであれば契約を保留することも検討に値する。

ベンダーの提供する  
製品やサービスが  
ニーズに合っているか？



## ② 組織横断的にセキュリティ対策を検討しているか？

医療機関におけるサイバーセキュリティ対策の構築において「部門意識」や「部門ごとの視点」は絶対に避けなければならない。企業においては当然のことだが、医療機関においてもこの点において何ら違いはない。

医療機関には、ITの専門組織を設置できていないところも多い。サイバーセキュリティ対策を講ずる機会に、新たにIT部門を設置してIT活用とセキュリティ対策を両輪として推進するのも良策である。この場合、ITもセキュリティ対策も部門ごとの目線では組織全体の役には立たない。いずれも、ひとたび問題が発生するばそれは即、組織全体に及ぶからだ。

ゆえに、組織横断的なITの推進とセキュリティ対策がきわめて重要であり、そのためには、サイバーセキュリティ対策チームが各部門とも連携を密にしながら組織全体に有効なサイバーセキュリティ対策を構築することが求められる。とくにサイバーセキュリティ対策においては、各部門、各スタッフのサイバーセキュリティに対する理解度をアップさせることが先決だ。その上で、医療機関全体が協力して対策を講ずる必要があることを認識してもらい、対策チームへの協力体制を堅持できるようにする。

また、サイバーセキュリティ対策は医療機関の「プライオリティ」であることを内外に示すためにも、院長や理事長などトップマネジメントの直接的関与も必須事項だ。

## 組織横断型 サイバーセキュリティ対策



### ③ 「完璧」ではなく「改善」をめざす

サイバーセキュリティを含めたセキュリティ対策には、ガイドラインや各種標準など様々な枠組みがある。ベンダー選定や対策の構築に際してこれらに照らして対策の完成度を意識してしまうのはある意味やむを得ない面もある。しかし、こうした枠組みに完全に合致することをめざすことは相応の苦勞と時間を必要とし、最悪はいくら努力しても完全に合致した対策はず、対策を打ち出せず時間だけが過ぎてしまうことになる。

めざすべきは「ある程度の合致」だ。ガイドラインや各種標準に完璧には合致できていないことを敢えて許容することが肝要だ。その上で、重要なことは「継続的な改善」を確実に実施することだ。改善を継続的に行うことで、ガイドラインや各種標準などを満たしてゆく度合いが高まってゆく。

また、仮にある段階でガイドラインや各種標準への完璧な合致を果たしたとしても、サイバー犯罪の手口やパターンは刻々変化してゆくため、後日再び対策を見直し、修正を余儀なくされることになる。完璧をめざして時間や労力を費やすよりも、少しでも早く、まずは第一段階のサイバーセキュリティ対策を講ずることが何よりも求められる。



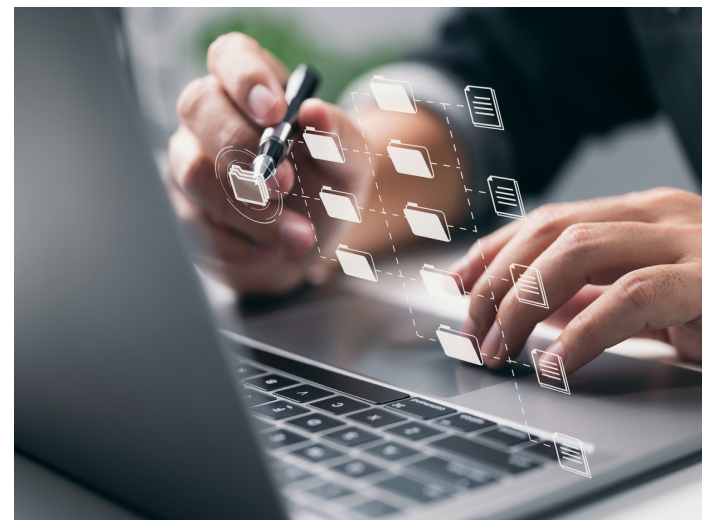
#### ④ 信頼することと検証することは別の話

サイバーセキュリティベンダーの選定に際し、候補ベンダー各社に共通質問書への記入や各種情報提供を求めることは珍しくない。海外では Questionnaire や Request For Information (RFI) などと呼ばれ、検討プロセスにおける重要な作業として定着していることでもある。

数社にこうした情報提供を求めれば、提供される情報量は相応に多くなる。ゆえに、提供された情報はあまり精査せず、そのまま鵜呑みにしてしまうことが多いと思われるが、ここでは「信頼することと検証することは別」という考え方をもって欲しい。検証することは相手に失礼ということはない。ベンダーから提供された情報を元に判断する医療機関側としては、提供された情報が正しいものかどうか検証するのは当然のことだ。国際的にもこの重要性が指摘されている。

この検証作業はその後の契約に向けても大変重要なものだ。選定したベンダーが用意する契約書の内容が、予め提供された各種情報と整合性を維持しているか細かく確認することが不可欠だ。万が一食い違いがあれば、修正を求めるべきだ。その上で、修正が拒まれる場合は契約そのものを再検討する心構えも求められよう。

信頼するベンダーで  
あればこそ  
提供された情報は  
検証する



## ⑤ 対策を施した後も継続してチェック・検証する

サイバーセキュリティ対策は医療機関の情報システム（IT）のあり方と深く関係する。例えば、あるオンプレミスアプリケーションをクラウドに移行した場合やデータストレージをアップグレードした場合などだ。こうした変化は、当初は無かった状況であるため、すでに締結しているサイバーセキュリティベンダーとの契約内容に必ず影響する。モバイルアプリケーションを追加した場合、院内のネットワーク機器を変更したりアップグレードした場合なども既存契約に影響する可能性があるため、契約内容の修正が必要とならないかどうかしっかり検証する必要がある。

医療機関の情報システムは必ず変化、進化してゆくものだ。5年ごとの電子カルテシステムの入れ替えのように定期的なイベントばかりではない。当初は存在しなかったものが追加されたり、システム間連携やデータマネジメントの方法が変わったりすることは頻繁に発生するだろう。

こうしたことを念頭において最初の契約をスタートする必要がある。ひとつの方法として、当初の契約時に先々3年を見渡し、計画されているITシステム関連の追加・修正作業を思い浮かべ、それが発生した場合に契約にどのように影響するのかをベンダーに確認しておくことがあげられる。変化が生じた時に慌てて契約書を見直すのではなく、起こり得ることを契約相手のベンダーと事前に共有しておくことで、その後の契約変更を円滑に進められるようになる。

サイバーセキュリティ  
対策は  
継続的にチェック・  
検証する



# サイバーセキュリティ対策はお済みですか？

セキュリティソフトを導入するだけでは不十分です。

まず重要なのは、

- ① 院内の危機意識と対策の必要性の認識
- ② 情報管理の現状把握とあるべき姿の理解
- ③ 部門を超えた院内全体の協力体制

セキュリティソフト導入と運用体制の整備は最後のステップです。

伴走型コンサルティングでサイバー犯罪対策立案をお手伝いいたします。

お気軽にご相談ください。

**WATSON** Coaching & Consulting Group

<https://www.mycoachwatson.com/>

メールでのお問合せもお気軽に [info@mycoachwatson.com](mailto:info@mycoachwatson.com) まで