

GSX、医療業界向けセキュリティパッケージ提供へ

グローバルセキュリティエキスパート株式会社（本社：東京都港区海岸1-15-1、代表取締役社長：青柳史郎、証券コード：4417、<https://www.gsx.co.jp/>、以下、GSX）は、医療機関で発生しているサイバー脅威に対し、サイバーセキュリティ対策をパッケージ化した「医療業界向けセキュリティパッケージ」の提供を開始しました。

■医療業界向けセキュリティパッケージ提供の背景

サイバー攻撃の高度化が進み、ファイアウォールやUTM（統合脅威管理）など従来型のセキュリティ対策をすり抜けるような攻撃や、アンチウイルスでは検知が困難な未知のマルウェア、ファイルレスマルウェアによる攻撃が増加しています。こうしたサイバー攻撃によって、情報資産が保存されている社内のエンドポイント（PCや社内サーバ）などに深く侵入した攻撃者が、情報を窃取した後にランサムウェアを実行し、窃取した情報の暴露と暗号化したデータに対する身代金を要求する多重脅迫型の攻撃も頻発しており、被害は拡大する一方です。

昨今、医療機関もその標的となっており、サイバー攻撃の手法の多様化・巧妙化、情報セキュリティに関するガイドラインの整備やクラウドサービス等の普及に伴い、医療機関等を対象とするセキュリティリスクが顕在化していることへの対応として、情報セキュリティの観点から医療機関等が遵守すべき事項等の規定を設けるガイドラインが改定*され、「クラウドサービスへの対応」「認証・パスワードの対応」「サイバー攻撃等による対応」「外部保存受託事業者の選定基準対応」などが改定ポイントとして掲げられています。

*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 第5.1版」

<https://www.mhlw.go.jp/stf/shingi/0000516275.html>

昨年10月には、四国にある町立病院がサイバー攻撃を受け、病院のシステムに侵入して情報を暗号化し、復旧と引き換えに金銭を要求するランサムウェアに感染しました。同病院は身代金の要求を拒否しましたが、患者約8万5千人分の電子カルテが閲覧できなくなり、新規患者の受け入れも一時期停止するなど、医療現場に大きな負担と影響が生まれました。

このようなインシデント事例は、ネットワークやシステムを内部と外部に分けて、その境界線上で対策を講じてきた従来のセキュリティ対策では、高度化するサイバー攻撃を防ぐことができないことを証明しています。さらに、新型コロナウイルス感染症拡大に伴い、医療機関の機器やシステムのセキュリティ対策が不十分なままテレワークやクラウドサービスの活用が普及したことも、サイバー攻撃機会増加の大きな要因になっています。このような状況を踏まえて、サイバー攻撃をいち早く検知し対処するためには、ネットワークやシステムの内部・外部を区別することなく、ログ分析や端末認証、アクセス制御などの対策を総合的に行うことができるセキュリティソリューションの導入が必要になります。

また、2021年12月発行 一般社団法人 医療ISAC「国内病院に対するセキュリティアンケート調査の結果と考察」*の調査によると、雇用期間中、組織として従業員に求めるセキュリティ意識を一定水準で維持するための教育・研修を実施しているかという設問に対し、約60%の医療施設が「できていない」とする回答結果となっています。重要な情報を多く扱う医療業界の従業員には、情報セキュリティに関す

る正しい理解やリテラシーの向上が重要です。

*一般社団法人 医療ISAC | 国内病院に対するセキュリティアンケート調査の結果と考察

https://www.m-isac.jp/wp-content/uploads/2021/12/Report_20211201.pdf

■医療業界向けセキュリティパッケージのサービス提供内容

医療機関では、勢いが止まらない新型コロナウイルス感染症拡大に伴い、感染症患者への対応をはじめ、感染症に関する検査の実施や院内感染防止対策の徹底などの負担が増大し、医療提供体制に逼迫が生じています。このような状況の中、サイバー攻撃によって医療機関のシステムや機器が停止してしまったら、人命にも多大な影響を与えることにもなりかねません。

GSXは、厳しい状況が続く医療機関がサイバー攻撃を適切に防ぐことができるよう、各メーカーと協業し、4つのサイバーセキュリティ対策をパッケージ化しました。GSXは、医療業界の総合的なセキュリティ耐性の向上をご支援いたします。

➤ 医療業界向けセキュリティパッケージ詳細はこちらから

[https://gsx-co-jp.s3.ap-northeast-](https://gsx-co-jp.s3.ap-northeast-1.amazonaws.com/informationsecurity/pdf/TheSPFTMedicalIndustryIntroducing.pdf)

[1.amazonaws.com/informationsecurity/pdf/TheSPFTMedicalIndustryIntroducing.pdf](https://gsx-co-jp.s3.ap-northeast-1.amazonaws.com/informationsecurity/pdf/TheSPFTMedicalIndustryIntroducing.pdf)

医療業界向けセキュリティパッケージ概要

セキュリティパッケージに含まれる4つの製品・サービス

厚労省ガイドライン(※)に対応

- ① 端末のセキュリティ(EDR)
 - CROWDSTRIKE**
 - ユーザーが利用するパソコンやサーバー（エンドポイント）における不審な挙動を検知。ランサムウェアによる暗号化もブロックします。
 - 6.5 技術的安全対策
- ② インターネットG/W
 - i-FILTER.**
 - どんなWebアクセスでも、安全な業務環境を実現します
 - シャドール対策やクラウド利用管理にも最適です
 - 6.5 技術的安全対策
- ③ セキュリティ文書テンプレート
 - 様々なセキュリティに関する文書テンプレートを無償で提供いたします
 - 6.3 組織的安全対策
- ④ 情報セキュリティeラーニング
 - Mina Secure**
 - 従業員が意識すべき情報セキュリティに関する3つのコースをオンラインで受講することができます
 - 6.6 人的安全対策

※ 医療情報システムの安全管理に関するガイドライン 第5.1版
Copyright (c) GLOBAL SECURITY EXPERTS Inc., All Rights Reserved.

① 端末のセキュリティ (EDR) : CrowdStrike Falcon

CrowdStrike Falconシリーズは世界176ヶ国、14,687社（2021年10月末現在）で利用されている製品です。

ユーザーが利用するパソコンやサーバー（エンドポイント）の管理、攻撃の自動ブロックと攻撃の検知・対処が可能です。

また甚大な被害を及ぼし、これまでのアンチウイルスでは対応できなかったランサムウェアに対しても有効な実効性を備えています。

- **CrowdStrike Falconの詳細はこちらから**

https://www.gsx.co.jp/informationsecurity/crowdstrike_falcon.html

② **インターネットG/W : i-FILTER**

i-FILTERは、国内シェアNo.1のインターネットセキュリティ製品です。

独自のホワイト運用により、Webによる内部からの情報漏洩も外部からの攻撃も防ぎ、どんなWebアクセスでも安全な業務環境を実現します。

企業内で使用を許可していないIT機器やサービスの無断使用（シャドーIT）の抑制や、Webサイト閲覧制限やSaaSサービスの管理も簡単に実施できます。

- **i-FILTERの詳細はこちらから**

<https://www.gsx.co.jp/informationsecurity/ifatcloud.html>

③ **セキュリティ文書テンプレート**

IT利用が先行して、セキュリティが考慮されたポリシー・ルールがなく、遵守させることができないという課題をお持ちの医療機関に対して、各種セキュリティポリシーに関する文書雛形をリーズナブルな価格でお客様へ提供し(一部無償)、オプションでメールまたはWeb会議システムを通じた助言型支援を行います。これまでに数多くの企業で文書の策定・導入を実施してきた弊社の知見を活かした文書テンプレートを使用することにより、お客様側の文書作成の手間を大幅に削減し、効率的に考慮漏れのない文書を作成していただくことが可能です。

<提供文書テンプレート例>

- ・テレワーク規程およびテレワークガイドライン
- ・セキュリティポリシー
- ・スマートデバイス管理
- ・クラウドサービス利用および委託先管理
- ・CSIRT文書テンプレート

- **セキュリティ文書テンプレートの詳細はこちらから**

<https://www.gsx.co.jp/informationsecurity/teleworkguideline.html>

④ **情報セキュリティeラーニング : Mina Secure®**

情報資産や情報端末を、セキュリティ意識を持って取り扱う、という定期的な従業員教育を行っていない医療機関に対し、従業員の教育啓発に必要なセキュリティ教育コンテンツをeラーニング形式でご提供します。これにより、情報セキュリティ全般についてのセキュリティリスクを低減します。

<提供eラーニングコース>

- ・情報セキュリティ研修コース
- ・IPA情報セキュリティ10大脅威2021 個人編
- ・IPA情報セキュリティ10大脅威2021 組織編

- **Mina Secure®の詳細はこちらから**

<https://www.gsx.co.jp/informationsecurity/minasecure.html>

■i-FILTERを提供するデジタルアーツ株式会社からのエンドースメント（賛同文）

デジタルアーツ株式会社は、グローバルセキュリティエキスパート株式会社様の医療業界向けセキュリティパッケージでの発表を心より歓迎します。今後多くのお客様に貴社サービスをご活用頂き、医療業界におけるサイバーセキュリティ水準の向上、社会課題の解決の貢献を期待します。

デジタルアーツ株式会社 代表取締役社長 道具 登志夫

◆グローバルセキュリティエキスパート株式会社について

社名：グローバルセキュリティエキスパート株式会社
東京本社：〒105-0022 東京都港区海岸1-15-1 スズエベイディアム4F
西日本支社：〒541-0047 大阪府中央区淡路町3-1-9 淡路町ダイビル8F
西日本支社名古屋オフィス：〒451-6040 愛知県名古屋市中区牛島町6-1名古屋ルーセントタワー40F
代表者：代表取締役社長 青柳 史郎
証券コード：4417
上場証券取引所：東京証券取引所マザーズ市場
資本金：485,000,000円
設立：2000年4月
コーポレートサイト：<https://www.gsx.co.jp/>

GSXは、サイバーセキュリティ教育カンパニーです

わたしたちは、情報セキュリティ・サイバーセキュリティに特化した専門会社です。高い継続率を誇るセキュリティコンサルティングや、長年のノウハウを踏襲した脆弱性診断、豊富なサイバーセキュリティソリューションをはじめ、日本初のセキュリティ全体像を網羅した教育サービスをご提供しています。

DXが加速し、サイバーセキュリティニーズが拡大する市場で各事業の軸に「教育」と「グローバル」を据え、日本の情報セキュリティレベル向上に貢献します。また、GSXは、中堅企業や地方企業を中心としたユーザー様に対し、それぞれに最適なサービスを提供し、サイバーセキュリティの知見・ノウハウをお伝えすることで、日本全国の企業の自衛力向上をご支援します。

▶ **コンサルティング**

・マネジメントコンサルティング

お客様が抱える情報セキュリティに関する課題について、現状の可視化から、解決に向けた計画策定・体制構築に至るまで、一貫した支援をご提供します。

・テクニカルコンサルティング

ハッカーと同様の技術を持つ専門エンジニア（ホワイトハッカー）が、お客様のネットワークシステムに擬似攻撃を行い、脆弱性の有無を診断して、対策措置、結果報告書までをご提供します。

▶ **セキュリティ教育**

・企業向けセキュリティ訓練

業界シェア No.1*であるトラップメール（GSX 標的型メール訓練サービス）や、ITセキュリティ e ラーニングサービスの Mina Secure®によって従業員のセキュリティリテラシー向上をご支援します。

*出典: ITR「ITR Market View: サイバー・セキュリティ・コンサルティング・サービス市場 2020」
標的型攻撃メール訓練サービス市場—従業員 1,000~5,000 人未満: ベンダー別売上金額シェア (2019 年度)

*出典: ITR「ITR Market View: サイバー・セキュリティ・コンサルティング・サービス市場 2020」
標的型攻撃メール訓練サービス市場—流通業: ベンダー別売上金額シェア (2019 年度)

・エンジニア向け教育講座

セキュリティ全体像を網羅した教育サービスをご提供します。EC-Council セキュリティエンジニア養成講座、日本発のセキュリティ人材資格「セキュリスト (SecuriST) ® 認定脆弱性診断士」などで、セキュリティ人材を育成します。

➤ **IT ソリューション**

・バイリンガル IT プロフェッショナルサービス

バイリンガルの IT 人材リソースをご提供します。グローバル拠点への対応はじめ、国内のバイリンガル対応を必要とするお客様への IT+サイバーセキュリティサービスをご提供します。

➤ **セキュリティソリューション**

・サイバーセキュリティ製品導入・運用サービス

最新の脅威や攻撃手法などに対して有効なサイバーセキュリティ製品・サービスを、実装・運用を組み合わせたワンストップソリューションでご提供します。

※本文中に記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。