

令和6年度 サイバーセキュリティセミナー



理事 比嘉 靖



令和6年度沖縄県医師会 サイバーセキュリティセミナー

日 時：令和7年3月17日（月）19：00～21：00
場 所：沖縄県医師会館 3階ホール（WEB併用）

司会：沖縄県医師会 比嘉 靖 理事

1. 開会
2. 説明
 - (1) 医療機関向けサイバーセキュリティ対策について (45分)
沖縄県警察本部サイバー犯罪対策課指導係
石川 翔太 様
 - (2) 事例から学ぶ！医療サイバーセキュリティ対策 (45分)
損害保険ジャパン
サイバーセキュリティ・サービス推進部
課長代理 北澤 正 様
 - (3) 標的型攻撃メール訓練について (5分)
沖医メディカルサポート
 - (4) 厚生労働省医療機関におけるサイバーセキュリティ対策チェックリスト支援について (5分)
株式会社琉球光和コンサルティング事業部
事業部長 石川 裕基 様
3. 質疑応答 (20分)
4. 閉会

令和7年3月17日（月）PM7：00より、沖縄県医師会館（3階大ホール）におきまして『令和6年度サイバーセキュリティセミナー』を開催しました。

本セミナーでは、沖縄県警察本部サイバー犯罪対策課の石川翔太様を講師にお迎えし、医療機関を取り巻くサイバー攻撃の最新動向や、現場で今すぐ取り入れられる具体的な対策について、大変分かりやすくご講演いただきました。

印象的だったのは、石川様が示された「オケの理論」や「サプライチェーン攻撃」といった、組織の“最も脆弱な部分”が狙われるという現実です。オケの理論では、セキュリティ対策は一枚一枚の木の板でできた桶に例えられ、一枚でも低い板があるとそこから水（情報）が漏れてしまうように、どんなに高価な対策をしても、一箇所でも脆弱な部分があると情報漏洩につながるという説明がありました。また、サプライチェーン攻撃では、大手企業だけでなく、その子会社や関連会社といったセキュリティ対策が手薄な中小企業が狙われ、そこを經由して大企

業に侵入する手口が紹介され、全ての中小企業や組織が例外なくサイバー攻撃の標的となる可能性があるという点が強調されました。

こうしたサイバー攻撃の手口は年々巧妙化しており、もはや情報システムの担当者だけでなく、経営層を含む職員一人ひとりの情報セキュリティに対する意識と、日々の慎重な行動が、大切な医療情報を守る最前線となっていることを改めて強く実感させられました。石川様は、

被害を防ぐためには情報セキュリティ対策、すなわち安全対策を取る必要があります、それにはコストがかかることも明確に示されました。また、ランサムウェアによる二重脅迫の手口や、VPN装置の脆弱性を突いた攻撃事例（半田病院、大阪急性期・総合医療センターなど）も紹介され、他人事ではないという危機感を覚えました。

以下に資料内容を抜粋し掲載します。

組織のセキュリティ水準はどこで決まるか？

「桶の理論」
組織のセキュリティ水準 = 最も低い部分の水準

全体のセキュリティを高めるには「底上げ」が必要

沖縄県警察 6

1

【参考】IPA情報セキュリティ10大脅威 2025

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い(2016年以降)
1位	ランサムウェアによる被害	2016年	10年連続10回目
2位	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3位	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4位	内部不正による情報漏えい等	2016年	10年連続10回目
5位	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6位	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7位	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8位	分散型サービス妨害攻撃 (DDoS攻撃)	2016年	5年ぶり6回目
9位	ビジネスメール詐欺	2018年	8年連続8回目
10位	不注意による情報漏えい等	2016年	7年連続8回目

選ばれる脅威は毎年ほとんど変わらない！

出典：情報セキュリティ10大脅威 2025

沖縄県警察 7

2

ウイルス名：W32/Hybris 渦巻きを画面に表示して作業の邪魔をする。

ウイルス名：W32/Hybris 渦巻きを画面に表示して作業の邪魔をする。

沖縄県警察 3

3

ランサムウェアによる二重恐喝 (ダブルエクストーション)

二重恐喝 (ダブルエクストーション)

企業等を標的として、情報を窃取した上で暗号化を行い、当該情報を公開しないこと引き換えに取引に応じるように脅迫する二重恐喝とみられるランサムウェア感染

① VPN装置、リモートデスクトップのばい密性を利用して企業等のネットワークに侵入

② 企業等のネットワーク内で侵害範囲を拡大し、情報を窃取

③ 情報を暗号化して、暗号復号等を要求する

④ 取引に応じない場合は、窃取した情報を公開すると更に脅迫

被疑者

被害者

企業等のネットワーク

VPN装置 リモートデスクトップサービス

沖縄県警察 17

4

ランサムウェアによる二重恐喝 (ダブルエクストーション)

ノーウェアランサム

データを暗号化する(ランサムウェアを用いる)ことなくデータを窃取し対価を要求する手口

① VPN装置、リモートデスクトップのばい密性を利用して企業等のネットワークに侵入

② 企業等のネットワーク内で侵害範囲を拡大し、情報を窃取

③ 窃取に応じない場合は、窃取した情報を公開すると更に脅迫

被疑者

被害者

企業等のネットワーク

VPN装置 リモートデスクトップサービス

沖縄県警察 16

5

つるぎ町立半田病院の事例から

- セキュリティ機器の運用に係る契約が曖昧
 - ・責任分界点を決めていなかった
 - ベンダーはハードウェアのみが保守対象と考えており、セキュリティアップデートは行っていなかった。
- システムのアップデートを怠っていた
 - ・電子カルテなどは常時稼働している。
 - システムを止めると責任問題になると考え、ベンダーも消極的になった。
- 閉域ネットワークを過信した
 - ・一カ所から侵入を許すと全て攻撃される可能性大
 - 先進企業はゼロトラストネットワーク

沖縄県警察 20

6

ランサムウェア感染事案

大阪急性期・総合医療センターの例（2022年10月30日）

サブライチェーンのVPN機器のぜい弱性が放置されていた

沖縄県警察 21

7

ランサムウェアへの対策

- 警察庁において、ランサムウェアによって暗号化された被害データを復号するツールを開発
 - ・被害に遭遇したら相談・通報をお願いします
- 『No More Ransom』というサイトで復号ツールが公開されていることがあります

沖縄県警察 25 25

8

Internet Explorerのサポート終了について

Internet Explorerのサポート終了

- 2022年6月16日にInternet Explorerのサポートが終了しました。
- EdgeのIEモードは、2029年まではサポートが継続される予定です。
- IEでの利用を前提とした業務アプリケーション等は早めの対応を検討しましょう。

沖縄県警察 28

9

パスワードの重要性

- “適切ではない”パスワードの例
 - ・ 生年月日、電話番号、辞書にある言葉
 - ・ 同じパスワードの使い回し
- 適切なパスワードの作り方（例）

- ① 覚えやすい言葉を選ぶ 「ハイサイおじさん」
- ② ローマ字にする haisaiojisn
- ③ 大文字、数字、記号を入れる (基本パスワードの完成) Haisa!ojj3
- ④ サービス名にちなんだ文字を加える [Yahoo!なら] YAHaisa!ojj3

沖縄県警察 31

10

2段階認証を有効にして安全性を高める

Gmailにパスワード認証でログインしたら...

パスワードだけではログインできない

スマートフォン認証も必要 (スマートフォン側)

スマートフォンで「はい」を選択する必要があります

沖縄県警察 32

11

県警サイバー犯罪対策課公式SNS (X・LINE)

サイバー犯罪やサイバーセキュリティに関する情報を随時発信しています!

X https://twitter.com/opp_cyber/

LINE <https://lin.ee/1UTWGD3>

沖縄県警察 33

12

※サイバー保険のご案内については、お知らせコーナーの38ページをご参照ください。