

【ニュースリリース】

2023年7月14日
株式会社サイバーセキュリティアクラウド

報道関係者各位

**【イベントレポート】『被害事例』から『先進的取組』まで！
医療機関がサイバーセキュリティの『リアルを語る』セミナー実施**

ハッカー対策サービスを展開するグローバルセキュリティメーカーの株式会社サイバーセキュリティアクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、一般社団法人サイバーセキュリティ連盟（以下「連盟」）が2023年6月29日（木）に開催した「『被害事例』から『先進的取組』まで！医療機関がサイバーセキュリティの『リアルを語る』セミナー」に当社の代表取締役社長 兼 CEO 小池敏弘が登壇しました。



本セミナーは「サイバー攻撃被害事例」の共有を中心に、サイバー攻撃対策に関する医療機関のリアルな現状をお届けしました。セミナーには医療従事者、関係するSIerなど150名超が参加しました。

当日は連盟の代表理事である小池敏弘の挨拶から始まり、厚生労働省副大臣の伊佐進一氏からのご挨拶、徳島県つるぎ町立半田病院の須藤泰史氏、順天堂大学医学部附属順天堂医院を擁する学校法人順天堂の杉村雅文氏にご登壇を頂き、実際に起きた医療機関へのサイバー攻撃状況や被害事例、DXを進める中でも取り組むべきサイバーセキュリティなどについてお話し頂きました。

■ 厚生労働副大臣 兼 内閣府副大臣 伊佐 進一 氏

日本の成長戦略では、AI やグリーントランスフォーメーションなど様々なことが描かれています。そういったことは海外で先行事例があり、日本がどう追いかけていくかだと思っています。重要なことは日本の強みをどう強化していくかで、まさに日本の強みとは医療・介護なのではないかと思っています。日本は医療・介護のデータを統合し活用していくことが鍵となります。世界的に少子高齢化が進んでおり、その中でも特に少子高齢化が進む日本で、どのようにデータを活用していき、創薬などに繋げられるか。その前提としてサイバーセキュリティが重要となっています。

厚生労働省が管轄している医療については、これまで策定したガイドラインの他、医療現場に対しサイバーセキュリティ研修、立ち入り検査、情報共有などを行っています。



■ 事例紹介：身代金要求型ウイルス「ランサムウェア」被害 つるぎ町立 半田病院 つるぎ町 病院事業管理者 須藤 泰史 氏

- 「ランサムウェア」被害

2021年10月31日未明に電源の入っている全てのプリンタから、コピー用紙がなくなるまで英字の犯行声明文が印刷され続ける事態が発生。同日の午前0時30分に電子カルテを確認すると、全く動かない状況だった。犯行声明文には身代金の要求と、支払いがなければ取得したデータを公開する旨が記載されていた。

恐らくVPNの脆弱性が狙われた攻撃だと考えられる。ランサムウェア被害によりシステム復旧、そして新たなシステム構築におよそ二億円が必要と見込まれている。加えて、診療制限をかけていた期間の診療報酬の減収などを含めると、更に数千万円が被害額として上乗せされる。



- 復旧に向けて

まずは電子機器すべてのケーブルを抜き、病院上層部に連絡。また県内の電子カルテ共有ネットワークの被害確認と警察に通報を行った。2021年10月31日午前10時に南海トラフ地震を想定したBCP（事業継続計画）に基づき対策本部を立ち上げ、被害状況から通常診療が続けられないと判断、同日午後4時に記者会見を実施した。

調査の末、電子カルテサーバを始め様々な周辺医療機器に感染が広がっていた。このうち、カルテ端末PC200台中40台が感染しており、コスト削減のために専門業者指導のもと、ウイルス対策ソフトを用いたウイルス駆除作業は自分たちの手作業で行った。

対策本部を設置した大会議室はエリアを4分割し、PCなど電子機器エリア、机と椅子を置いた打ち合わせエリア、職員の食事エリア、災害時の記録「クロノロジー」・組織図・コンタクトリスト・Todoリスト・部門別の復旧状況を掲示するミーティングエリアと用途別に使用した。

- 工夫した点

- ミーティングを毎日行い、問題点・改善点などの報告・情報共有を実施
- 大量の文具、PC、プリンタ、コピー機が必要になるため、借りられるところから借りる
- マスコミ対応は事務長に一本化し、個別対応をしないように調整

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 経営企画部 広報担当：竹谷・川崎
TEL：03-6416-9996 mobile：080-4583-2871(川崎携帯)
FAX：03-6416-9997 E-Mail：pr@cscloud.co.jp

- 「ランサムウェア」被害を通じて感じた「備え」の重要項目

- サイバーセキュリティ向上と確実なバックアップ
- 被害に遭った際にどう事業を継続させるかの BCP 対策
- 電子カルテシステムとは別の簡易バックアップシステムの構築
- 大量の文具、PC、プリンタ、コピー機を備蓄しておく

ランサムウェア被害を完全に防ぐことはできないため、もし攻撃された際にどのようにデータを守るか、どのように事業を継続させるかが重要となる。

まずは自分たちの病院に問題がないか、半田病院が公開している報告書を参考に自院の状況を確認してほしい。

参考：徳島県つるぎ町立半田病院 コンピュータウイルス感染事案有識者会議調査報告書

<https://www.handa-hospital.jp/topics/2022/0616/index.html>

参考：つるぎ町立 半田病院でおきたこと（厚生労働省 セキュリティ教育支援ポータルサイト）

<https://mhlw-training.saj.or.jp/contents/>

■ 事例紹介：順天堂におけるサイバー攻撃に抗する組織・体制構築

学校法人順天堂 情報センター本部 本郷地区情報センター

次長（兼務 センター長補佐）杉村 雅文 氏

- 注視しているサイバー攻撃の脅威対策

ランサムウェア、DDoS 攻撃、フィッシングが挙げられる。特に注意すべき点として、不審なメールには注意し添付ファイルは安易に開かない。複数の眼で確認し、システム担当者に速報することが重要で、スマートフォンもパソコン同様の対応をする必要がある。

- 順天堂のサイバーセキュリティ対策の現状

学内 LAN 環境では ID・パスワード承認の他、順天堂メール（ウイルス・迷惑メール対策）強化、ファイアウォール（不正通信遮断）の設置、ウイルス対策ソフトの導入、EDR（AI 振る舞い検知ソフト+ 専門アナリストによる監視サービス）を利用している。

医療 LAN 環境ではインターネットから分離し、ウイルス対策ソフト（EDR）の導入（2023 年 1 月のシステム更新で電子カルテ端末を WAS にてアップデート）、USB 利用制限を実施。

特にサイバーセキュリティ強化のため 2018 年度に EDR を導入。さらにセキュリティ体制整備を行い、セキュリティチーム（JIN-CSIRT）を設置して、学校法人順天堂全学内の法人・医療システムや、ネットワーク環境における情報セキュリティインシデント対応、インシデント対策、セキュリティ教育などの実施を予定している。

- 順天堂医院の医療情報システム

システム更新では「7 年毎の更新」をコンセプトとし、

- 部署最適化から全体最適へ
- オンデマンドで誰でもストレスなく利用できる情報基盤整備
- 情報共有・一元化の推進を軸とした更新

を実施。



【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 経営企画部 広報担当：竹谷・川崎

TEL：03-6416-9996 mobile：080-4583-2871(川崎携帯)

FAX：03-6416-9997 E-Mail：pr@cscloud.co.jp

現行システムからの変更点として、

- 仮想デスクトップ（VDI）環境を構築
 - 多要素認証を採用
 - 電子カルテ端末からのインターネット閲覧
- の3点を変更した。

- 今後の具体的な活動

- ① 職員教育（医療情報システム安全管理責任者設置の届け出）
※ 診療録管理加算の施設基準届け出をしている医療機関は必須
 - ② サイバー攻撃に遭いシステムダウンした際の机上訓練
 - ③ 附属病院・各キャンパスのセキュリティ担当者の任命
 - ④ CISO 任命
- を実施予定。

■ 一般社団法人サイバーセキュリティ連盟について

名称 : 一般社団法人サイバーセキュリティ連盟 (Cyber Security Alliance・CSA)
代表理事 : 小池 敏弘 (株式会社サイバーセキュリティクラウド 代表取締役社長 兼 CEO)
理事 : 小川 隆一 (独立行政法人情報処理推進機構 専門委員)
齋藤 孝道 (明治大学 サイバーセキュリティ研究所 所長)
所在地 : 〒141-0021 東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階
設立 : 2023 年 3 月 31 日
URL : <https://www.cscloud.co.jp/dx-security>

Vision : サイバー攻撃による「深刻な被害」をゼロに
Mission : 日本の DX をもっと安全に
Values : Interested parties oriented : 当事者中心で動かす
Realistic feelings : 生々しくリアルを伝える
Horizontal relationships : 「横の繋がり」を積極的に展開していく

一般社団法人サイバーセキュリティ連盟は「サイバー攻撃による『深刻な被害』ゼロ」を目指して「日本の DX をもっと安全に」する為の様々な活動を展開しています。

■ 株式会社サイバーセキュリティクラウドについて

住所 : 東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階
代表者 : 代表取締役社長 兼 CEO 小池敏弘
設立 : 2010 年 8 月
URL : <https://www.cscloud.co.jp>

サイバーセキュリティクラウドは「世界中の人々が安心安全に使えるサイバー空間を創造する」という経営理念を掲げ、世界有数のサイバー脅威インテリジェンスと AI 技術を活用した、Web アプリケーションのセキュリティサービス、及び脆弱性情報収集・管理ツールといったハッカー対策サービスを提供しています。これからも私たちは WAF を中心としたサイバーセキュリティにおけるグローバルリーディングカンパニーの 1 つとして、情報革命の推進に貢献してまいります。

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 経営企画部 広報担当 : 竹谷・川崎
TEL : 03-6416-9996 mobile : 080-4583-2871(川崎携帯)
FAX : 03-6416-9997 E-Mail : pr@cscloud.co.jp

【IR 情報】

- HP IR 情報一覧 : <https://www.cscloud.co.jp/ir/>
- IR note マガジン : https://note.com/csc_ir

主な展開サービス :

- クラウド型 WAF『攻撃遮断くん』 : <https://www.shadan-kun.com>
- パブリッククラウド WAF の自動運用サービス『WafCharm』 : <https://www.wafcharm.com>
- 厳選された AWS WAF 用のルールセット『Cyber Security Cloud Managed Rules for AWS WAF』 : <https://aws.amazon.com/marketplace/seller-profile?id=baeac351-6b7c-429d-bb20-7709f11783b2>
- 脆弱性情報収集・管理サービス『SIDfm』 : <https://sid-fm.com>

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 経営企画部 広報担当 : 竹谷・川崎
TEL : 03-6416-9996 mobile : 080-4583-2871(川崎携帯)
FAX : 03-6416-9997 E-Mail : pr@cscloud.co.jp