H-ISAC Japan Council

日米合同ワークショップ

U.S.-Japan Joint Workshop

2022 年 6 月 15 日 (水)

Wednesday, June 15, 2022

アジェンダ

9:00-9:10 開会あいさつ
エロール・ワイス （Health-ISAC CSO）／深津 博 （医療 ISAC 代表理事）
9:10-10:30
§1. 日米合同企画プログラム
医療分野におけるランサムウェア攻撃の実態 ”経験の共有”
座長：深津 博／エロール・ワイス
米国における被害実態と分析（American Hospital Association：AHA） ~9:30
サイバー攻撃による電子カルテ停止を経験して（つるぎ町立半田病院） ~9:50
被害病院における実態と対策（株式会社ワイ・イー・シー） ~10:10
ディスカッション ~10:30
（休憩）
10:40-11:20
§2. スポンサープログラム
(1) サイバー脅威インテリジェンス活用事例（KELA 株式会社） ~11:00
(2) 医療機器におけるソフトウェア部品表”Bill-Of-Materials;BOM”
（ベクトン・ディッキンソン アンド カンパニー ） ~11:20
11:20-12:40
§3. パネルディスカッション：ランサムウェア対策としてのバックアップソリューション
座長：伊藤春基（医療 ISAC CTO）
富士ソフト株式会社／ルーブリック・ジャパン株式会社 ~11:40
ネットアップ合同会社 ~12:00
Cohesity Japan 株式会社 ~12:20
ディスカッション ~12:40
（昼食休憩）
13:20-15:10
§4. 医療 ISAC 企画プログラム
(1) 病院のサイバーセキュリティ診断を目的としたクラウドファンディング （医療 ISAC） ~13:40
(2) 今求められる外部公開システム管理 （サイファーマ株式会社） ~14:10
(3) 院内環境を死角なく完全保護する「AI 免疫システム」
（ダークトレース・ジャパン株式会社） ~14:40
(4) サイバー攻撃と Active Directory との関係の誤解を解く
（Tenable Network Security Japan 株式会社） ~15:10
（休憩）
15:20-17:00
§5. Health ISAC 企画プログラム
パネルディスカッション：ゼロトラスト
座長: Kanna Wendy
再考！ゼロトラストネットワークアクセスの重要性”VPN を超える最適なアプローチとは”
（ゼットスケーラー株式会社） ~15:45
武田薬品工業のゼロトラストへのアプローチ（武田薬品工業株式会社） ~16:10
電子カルテへのセキュアなリモートアクセス（ゼットスケーラー株式会社） ~16:25
ディスカッション、Q&A ~17:00

Agenda

9:00-9:10 Opening Remarks

Errol Weiss (Health-ISAC CSO)/Hiroshi Fukatsu (Medical ISAC Japan Representative Director)

9:10-10:30

§1. U.S.-Japan Joint Program

Symposium for ransomware attack on healthcare sector"sharing the experiences"

Chairpersons: Hiroshi Fukatsu & Errol Weiss

Damage in the U.S. and Analysis(American Hospital Association:AHA) ~9:30

Experiencing an electronic medical record outage due to a cyber attack

(Handa Hospital, Tsurugi Town, Tokushima) ~9:50

Actual conditions and countermeasures in the affected hospitals(YEC Co., Ltd) ~10:10

Discussion time ~10:30

(Break)

10:40-11:20

§2. Sponsored programs

(1) Cyber Threat Intelligence Use Cases (KELA K.K.) ~11:00

(2) Software Bill-of-Materials of Medical Devices (Becton, Dickinson and Company) ~11:20

11:20-12:40

§3. Panel discussion:Backup solutions as ransomware protection

Chairpersons: Haruki Ito (Medical ISAC Japan CTO)

FUJI SOFT INCORPORATED／Rubrik Japan K.K. ~11:40

NetApp LLC ~12:00

Cohesity Japan K.K. ~12:20

Discussion time ~12:40

(lunch break)

13:20-15:10

§4. Medical ISAC Japan featured programs

(1) Crowdfunding for hospital cybersecurity diagnostics (Medical ISAC Japan) ~13:40

(2) External Attack Surface Management required today (Cyfirma K.K.) ~14:10

(3) AI Immune System for complete protection of the hospital environment without any blind spots

(Darktrace Japan K.K.) ~14:40

(4) Clearing misconceptions about connection between Cyber Attacks and Active Directory

(Tenable Network Security Japan K.K.) ~15:10

(Break)

15:20-17:00

§5. Health-ISAC featured session

Panel Discussion: Zero Trust

Chairpersons: Wendy Kanna

Rethink! The Importance of Zero Trust Network Access "What is the Best Approach Beyond

(Zetscaler K.K.) ~15:45

Takeda's approach to Zero Trust (Takeda Pharmaceutical Company) ~16:10

Remote access solution to EMR (Zetscaler K.K.) ~16:25

Discussion time ~17:00

主催者代表　Organizer

深津　博　Hiroshi Fukatsu

医療 ISAC　代表理事
愛知医科大学医療情報部特任教授、放射線科専門医、
社会医学専門医・指導医

1985 年　名古屋大学医学部卒業
2000 年より名古屋大学医学部附属病院准教授
2006 年より日本医療コンシェルジュ研究所代表
　　医療コンシェルジュの育成（1000 名以上）
　　医師事務作業補助者の基礎知識研修
　　（2000 名以上）を実施。
2009 年より現職
2014 年より一般社団法人メディカル IT セキュリティフォーラム
　　代表理事に就任
2019 年 10 月、団体名を一般社団法人医療 ISAC に改名
同年米国 Health ISAC と包括業務提携を締結

Hiroshi Fukatsu MD, Medical ISAC Japan Representative Director, Professor & Manager of Medical Informatics Division, Aichi Medical University Hospital, Certified Radiologist, Certified Social Medicine Trainer
Graduated from Nagoya University school of Medicine in 1985.
Became Assistant Professor, Nagoya University Hospital in 2000.
Shifted to the current status since 2009.
Also plays a role as the representative director of Japan Medical Concierge Research Institute in 2006
Offered medical concierge training course for more than 1000 students, also offered basic training for medical clerk for more than 4000 students.
Founded Medical IT Security Forum in 2014 and became the representative officer.
Organization name changed to Medical ISAC Japan in October 2019
Established a comprehensive alliance with Health ISAC in 2019.

エロール・ワイス　Errol Weiss

Health -ISAC　チーフセキュリティオフィサー（CSO）

エロール・ワイスは、2019 年 4 月に Health Information Sharing & Analysis Center（Health-ISAC）の初代チーフセキュリティオフィサーとして入社し、フロリダ州タイタスビルに Health-ISAC の脅威オペレーションセンターを設立、スタッフを配置し、ヘルスケアセクターの IT および情報セキュリティ専門家に関連する有意義で実行可能な脅威インテリジェンスをメンバーに提供しています。

エロールは、情報セキュリティの分野で 25 年以上の経験を有しており、 国家安全保障局（NSA）で脆弱性分析や政府機密システムの侵入を担当した後、フォーチュン 100 社に情報セキュリティサービスを 10 年間提供しました。
信頼できる匿名での情報共有に関する特許の発明者 4 名のうちの 1 人であり、1999 年に世界初の ISAC の創設、実装、運用を担当しました。
2006 年から 2016 年まで、シティグループのサイバーインテリジェンスセンターを設立・運営し、世界中の数千人の社内ユーザーに実用的なインテリジェンスを提供しました。
Health-ISAC 以前は、Bank of America のグローバル情報セキュリティチームでシニアバイスプレジデントエグゼクティブを務めていました。

ジョンズ・ホプキンス大学で技術管理の修士号、バックネル大学でコンピュータ工学の学士号を取得。

Errol Weiss joined Health Information Sharing & Analysis Center (Health-ISAC) in April 2019 as its first Chief Security Officer.　Errol created and staffed Health-ISAC's Threat Operations Center in Titusville, Florida, providing members with meaningful and actionable threat intelligence relevant for IT and infosec professionals in the healthcare sector.

Errol has over 25 years of experience in Information Security.　He began his career with the National Security Agency (NSA) conducting vulnerability analyses and penetrations of classified government systems and then spent ten years delivering Information Security Services for Fortune-100 companies. Errol is one of four named inventors on the patent for Trusted and Anonymous Information Sharing and was responsible for the creation, implementation and operation of the world's first ISAC in 1999. From 2006 to 2016, Errol created and ran Citigroup's Cyber Intelligence Center and provided actionable intelligence to thousands of internal users globally.　Prior to Health-ISAC, Errol was a Senior Vice President Executive with Bank of America's Global Information Security team.

Errol has a M.S. in Technical Management from Johns Hopkins University and a B.S. in Computer Engineering from Bucknell University.

講演要旨＆登壇者プロフィール
Abstract & Speaker Info

§1. 日米合同企画プログラム

医療分野におけるランサムウェア攻撃の実態 ”経験の共有”

Symposium for ransomware attack on healthcare sector “sharing the experiences”

座長：深津　博／エロール・ワイス

Chairpersons: Hiroshi Fukatsu & Errol Weiss

米国における被害実態と分析

Damage in the U.S. and Analysis

ジョン・リギ　John Riggi

米国病院協会

サイバーセキュリティ&リスク担当ナショナルアドバイザー

American Hospital Association (AHA)

National Advisor for Cybersecurity and Risk

プロフィール

ジョンは、30 年近く FBI の高官を務めた後、米国病院協会とその 5000 以上の会員病院を対象に、サイバーセキュリティとリスクに関する初の国家アドバイザを務めています。

ジョンは、FBI と CIA でのサイバー、犯罪捜査、国家セキュリティの経験を生かし、信頼できる戦略的サイバーリスクアドバイザリー・サービスを各国の病院と医療システムに提供しています。

医療界のリーダーや政府機関に信頼されることで、サイバーリスク問題に対するジョン独自の国際的な視点が強化され、AHA の政策と提言活動に大きく貢献しています。ジョンは、2020 年 12 月に行われた上院国土安全保障委員会の病院へのサイバー脅威に関する公聴会で、全米の病院を代表して証言しています。 2021 年、John は、政府に対し、サイバー攻撃の犠牲となった HIPAA を調査することを最優先するよう働きかけました。

FBI では、ホワイトハウスのサイバー対応グループ代表や、CIA の上級代表として、さまざまな指導的役割を果たしました。また、テロ資金調達捜査の全米オペレーション・マネージャーも務めました。また、ワシントン DC では防諜のための現場監視プログラムを、ニューヨークでは金融犯罪やテロ資金調達のための部隊を指揮しました。最終的には上級管理職に昇進し、FBI サイバー課の全国プログラムを率いて、ヘルスケアやその他の重要インフラ部門とミッションクリティカルなパートナーシップを構築しました。ヘルスケアやその他のセクターを標的とした最大規模のサイバー攻撃の捜査において、国家戦略的な役割を果たしました。

また、8 年間にわたり NYFBISWAT チームに所属し、テロ対策における FBI 長官の特別功労賞と、CIA のカテゴリーで最高の賞である George H.W.BushAward for ExcellenceinCounterrorism を受賞しています。

Profile

JohnRiggi,havingspentnearly30yearsasahighlydecoratedveteranoftheFBI,servesasthefirstnationaladvisorforcybersecurityandriskfortheAmericanHospitalAssociationandtheir5000+memberhospitals. Johnleverageshisdistinctcyber,criminalinvestigationandnationalsecurityexperienceattheFBIandCIAtoprovidetrustedstrategiccyberandriskadvisoryservicestothenations'hospitalsandhealthsystems. HistrustedaccesstohealthcareleadersandgovernmentagenciesenhancesJohn'suniquenationalperspectiveoncyberandriskissuesandgreatlycontributestotheAHA'spolicyandadvocacyefforts.Johnrepresentedthenation'shospitalsintestimonybeforetheSenateHomelandSecurityCommitteehearingoncyberthreatstohospitalsinDec.2020.ThisassistedinthepassageofPL116-321,providingregulatoryreliefforHIPAAcoveredvictimsofcyberattacks.In2021,John'sprominentadvocacyencouragedthegovernmenttoraisetheinvestigativeprioritylevelofransomwareattackstoequalthatofterroristattacks.

In various leadership roles at the FBI, John served as a representative to the White House Cyber Response Group and a senior representative to the CIA. He also served as the national operations manager for terrorist financing investigations. John also led counterintelligence field surveillance programs in Washington DC and financial crimes and terrorist financing squads in New York City. John ultimately rose to the ranks of the Senior Executive Service and in that capacity led the FBI Cyber Division national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors. John held a national strategic role in the investigation of the largest cyber-attacks targeting healthcare and other sectors. HealsoservedontheNYFBISWATTeamforeightyears.JohnistherecipientoftheFBIDirector'sAwardforSpecialAchievementinCounterterrorismandtheCIA'sGeorgeH.W.BushAwardforExcellenceinCounterterrorism,theCIAshighestawardinthiscategory.Johnpresentsextensivelyoncybersecurityandrisktopicsandisfrequentlyinterviewedbythemedia.

講演要旨

パンデミックの発生に伴い、病院や医療システムに対するサイバー攻撃は劇的に増加しました。国家や犯罪者のサイバー敵対者は、パンデミック時に配備されたネットワークやインターネットに接続された機器や技術の利用が増えたことを悪用し、記録的な数の攻撃を米国の医療機関に仕掛けました。

私たちが最も懸念しているのは、米国の病院や医療システムを憂慮すべき速度で襲っている、影響力の大きいランサムウェア攻撃です。

これらの攻撃は、医療提供の中断と遅延をもたらし、地域単位で患者の安全を危険にさらすものであり、FBI は最近、病院に対するランサムウェア攻撃を「生命への脅威」犯罪として優先的に扱うと宣言しました。

米国病院協会のサイバーセキュリティとリスクのナショナルアドバイザーであり、元 FBI サイバーシニアエグゼクティブのジョン・リッジが、ロシアのウクライナ侵攻に起因するものを含む最新のサイバー脅威について、国内および国際的な独自の視点を提供します。

また、米国内のランサムウェア被害者への対応に基づき、これらの攻撃への準備、対応、回復の最善の方法についても説明します。

Abstract

Cyber-attacks against hospitals and health systems increased dramatically with the onset of the pandemic. Nation state and criminal cyber adversaries exploited the increased use of network and internet connected devices and technologies deployed during the pandemic to target U.S. healthcare with a record number of attacks. The attacks we are most concerned with are high impact ransomware attacks, which have struck U.S. hospitals and health systems at an alarming rate. These attacks result in the disruption and delay of healthcare delivery, and risk patient safety on a regional basis. The FBI recently declared that they prioritize ransomware attacks on hospitals as “threats to life” crimes. Join John Riggi, National Advisor for Cybersecurity and Risk for the American Hospital Association and former FBI Cyber senior executive, as he provides his unique national and international perspective on the latest cyber threats, including those arising from the Russian invasion of Ukraine. Based upon his work with ransomware victims across the U.S., John will also discuss how best to prepare for, respond to and recover from these attacks.

サイバー攻撃による電子カルテ停止を経験して

Experiencing an electronic medical record outage due to a cyber attack

須藤　泰史　Yasushi Suto
徳島県つるぎ町立半田病院　病院事業管理者
Handa Hospital, Tsurugi Town, Tokushima Prefecture Hospital Business Administrator

プロフィール

1986 年　3 月　徳島大学医学部医学科卒業
1986 年　5 月　徳島大学医学部泌尿器科学教室へ入局
　　以降、教室関連施設で勤務
1999 年　4 月　徳島大学医学部附属病院講師（泌尿器科）
2001 年　4 月　徳島大学医学部講師（泌尿器科学講座）
2003 年　6 月　町立半田病院　泌尿器科医長
　　以降、診療部長、副院長、病院長となり
2020 年　1 月　つるぎ町　病院事業管理者（つるぎ町立半田病院　病院長兼任）
2020 年　4 月　つるぎ町　病院事業管理者　現在に至る

Profile

Mar 1986 Graduated with a degree in Medicine, Faculty of Medicine, The University of Tokushima
May 1986 Entered the Department of Urology, Faculty of Medicine, The University of Tokushima
Worked at the affiliated facilities of the Department of Urology
Apr 1999 Lecturer, Department of Urology, The University of Tokushima Hospital
Apr 2001 Lecturer, Department of Urology, Faculty of Medicine, The University of Tokushima

June 2003 Chief of Urology Department, Handa Hospital
Since then, he has served as chief of the department, deputy chief of the hospital, and director of the hospital.
January 2020: Hospital Business Administrator of Tsurugi Town (also Hospital Director of Tsurugi Handa Hospital)
Apr. 2020 Tsurugi Town Hospital Business Administrator to present

つるぎ町立半田病院

徳島県西部、中山間地域にある 120 床の急性期病院。県西部唯一の分娩施設であり、年間 350 余りの分娩件数がある。また、西部医療圏の小児救急の輪番も多くを担当している。
診療科は、内科・外科・産婦人科・小児科・泌尿器科（人工透析治療も含む）・放射線科・整形外科・眼科・耳鼻科・皮膚科等があり地域医療を担っている。

Tsurugi Handa Hospital

Handa Hospital is a 120-bed acute care hospital located in the mid-mountainous region of western Tokushima Prefecture. It is the only delivery facility in the western part of the prefecture and handles more than 350 deliveries per year. The hospital is also responsible for many of the pediatric emergency rotation shifts in the western medical region.
The hospital provides community medical care through its departments of internal medicine, surgery, obstetrics and gynecology, pediatrics, urology (including dialysis treatment), radiology, orthopedics, ophthalmology, otolaryngology, dermatology, and others.

講演要旨

今回、私どもの病院が、ランサムウェアによるサイバー攻撃を受けて病院機能がストップしてしまう事態を経験いたしました。この詳細をご報告することで、皆様の病院がこのような被害に遭われないように十分な対策をとられることを切に願っております。

[事件の詳細]

2021/10/31 午前 0 時 30 分頃　電子カルテと接続されている全てのプリンターから英文の犯行声明が自動印刷。同時に電子カルテの不具合を確認、システム担当者が対応を開始。「LockBit 2.0」のランサムウェアによるサイバー攻撃ですべてのシステムが使えなくなっていることが判明。

[対応]

1. 事件当日：午前 8 時　病院上層部へ連絡。関係機関（県内の電子カルテ共有ネットワーク・等）および県警のサイバー犯罪対応部署へ連絡。午前 10 時　災害対策本部を立ち上げ、第 1 回目の対 2.策会議を開始。午後4時　県内の報道機関に記者会見。
2. 県警に「LockBit 2.0」への対応を依頼：彼らの Web サイトには、当院への身代金の要求はなし。
3. システム復旧へむけて外部の専門業者に委託。
4. BCP に基づき、南海トラフ地震対策等で運用する予定で準備した紙カルテベースの診療を稼

働。
5. 10/31～1/4 までは医事会計システムと連動のない紙カルテの診療。10/31 の分は早急に入力し 1 月にようやく 10 月分の診療報酬を請求。11 月分は 2 月、12 月分は 3 月に。1 月～3 月は、4 月に請求。
6. 2022/2/17 に画像サーバーが接続。6/15 現在:透析部門・検査部門の一部が未接続。
7. 有識者会議を 2/4・2/28・3/28・5/20(計 4 回)。5 月中に報告書を作成し、6 月上旬につるぎ町議会で報告し、6 月下旬に HP で一般公開予定。
8. 被害総額は、復旧・新たなシステム作りに 2 億円、診療報酬の減収がおおよそ数千万円。

[Take Home Message]
1. サイバー攻撃に備え、セキュリティは万全に！ウイルス対策ソフトの使用・こまめなアップデート・常にセキュリティに関しての情報収集
2. BCP の作成・模擬訓練
3. 復旧に関して:忙しい部署・忙しい人は時期により異なる。いつもと全く違う仕事をしないといけない。不平不満もたまる。聞く耳を！

Abstract
This time, our hospital experienced a cyber-attack by ransomware that brought hospital functions to a halt. By reporting the details of this incident, I sincerely hope that you will take sufficient measures to prevent your hospital from being affected by such an attack.

[Details of the incident]
Around 0:30 a.m. on 10/31/2021, all printers connected to the electronic medical record automatically printed the crime statement in English. At the same time, a malfunction of the electronic medical record is confirmed, and system personnel begin to take action. It was discovered that all systems were disabled due to a cyber attack by "LockBit 2.0" ransomware.

[Response]
1. Day of incident: 8:00 a.m. Contact hospital upper management. Notify related organizations (electronic medical record sharing network, etc. within the prefecture) and the cybercrime response division of the prefectural police. 10:00 a.m.: Disaster response headquarters is set up, and the first meeting on countermeasures is held. 4:00 p.m. Press conference is held for the media in the prefecture.
2. Request to the prefectural police to respond to "LockBit 2.0": No ransom demand was made to our hospital on their website. 3) Request to the police to take action against "LockBit 2.0": No ransom demand was made to our hospital on their website.
3. outsourced system restoration to an external specialist.
4. based on the BCP, paper chart-based medical practice, which was prepared to be operated for Nankai Trough earthquake countermeasures, etc., was put into operation.
5. from 10/31 to 1/4, paper medical records were not linked to the medical accounting system.

10/31 was promptly input and the October reimbursement was finally requested in January. November reimbursement was requested in February, December reimbursement in March, and January to March reimbursement in April. 6.

6. image server will be connected on 2/17/2022; as of 6/15: part of the dialysis and laboratory departments are not connected. 7.
7. Expert meetings were held on 2/4, 2/28, 3/28, and 5/20 (4 times in total); a report will be prepared by the end of May, reported to Tsurugi Town Council in early June, and made publicly available on the website in late June.
8. the total amount of damage is 200 million yen for restoration and creation of a new system, and approximately tens of millions of yen in lost medical fee revenue.

[Take Home Message]

1. take all possible security measures to prepare for cyber-attacks! Use antivirus software, update frequently, and always collect information on security.
2. Create BCP and conduct mock drills. 3.
3. regarding recovery: Busy departments and busy people vary depending on the time of year. You will have to do a completely different job than usual. Complaints will build up. Listen up!

被害病院における実態と対策

Actual conditions and countermeasures in the affected hospitals

小野　健太郎　Kentaro Ono
公認不正検査士(CFE)
株式会社ワイ・イー・シー
執行役員　兼 YEC Global Solutions, Inc.(LA)Director
YEC Co., Ltd
Operating Officer, YEC Global Solutions, Inc.(LA)Director

プロフィール

同社へ入社後、法執行機関、事業会社をメインにフォレンジックツールのソリューション提供及びフォレンジック研修、コンサルティング等を提供していたが、法務・財務知識を包括的に習得するため、M&A アドバイザリー会社へ転職した後、現職へ復帰。
現在は主にデジタルフォレンジックサービス、マルウェア感染時のインシデントレスポンス支援を提供すると共にその後の組織改善や情報セキュリティポリシー策定支援などの各種コンサルティング・アドバイザリー業務に従事。北米では日系企業をベースに内部不正や退職者による情報漏えいに対するアドバイザリー業務を提供している。

Profile

After joining the company, he provided forensic tool solutions, forensic training, consulting, and other services mainly to law enforcement agencies and business companies, but in order to acquire comprehensive legal and financial knowledge, he moved to an M&A advisory firm before returning to his current position.
Currently, he mainly provides digital forensic services and incident response support for malware infections, and also engages in various consulting and advisory services such as subsequent organizational improvement and information security policy formulation support. In North America, he provides advisory services to Japanese companies against internal fraud and information leaks by retirees.

講演要旨

デジタルフォレンジックサービスをはじめとするデータに関わるトータルソリューションを提供している背景から、実際に発生したインシデント内容と実態を共有します。

Abstract

From the background of providing total solutions related to data, including digital forensic services, we will share actual incident contents and realities.

§2. スポンサープログラム

サイバー脅威インテリジェンス活用事例

Cyber Threat Intelligence Use Cases

川崎　真　Makoto Kawasaki
KELA 株式会社 プリセールス責任者
KELA K.K.　Presales Manager

プロフィール

日本と欧米のサイバーセキュリティ企業で 20 年の経験を有する。

Profile

He has 20 years of experience in cyber security companies in Japan, Europe and the United States.

会社紹介

イスラエルに拠点を置くサイバー脅威インテリジェンスを提供するグローバル企業。サイバー軍出身者を中心に高度な技術を駆使しマネージドサービスを提供しています。

About Us

A global cyber threat intelligence company based in Israel. The company provides managed services using advanced technology, led by people with cyber military backgrounds.

講演要旨

ランサムウェアなどの対処のためには通常の防御対策だけではなく、攻撃サイドとの交渉を含めた実戦での経験と高度なダークサイドに関する知識が必要になります。講演ではデモンストレーションを交えながらサイバー脅威インテリジェンスの活用事例をお話します。

Abstract

Dealing with ransomware and other threats requires not only ordinary defensive measures, but also real-world experience and advanced knowledge of the dark side, including negotiation with the attacker side. In the lecture, we will talk about examples of the use of cyber threat intelligence with demonstrations.

医療機器におけるソフトウェア部品表”Bill-Of-Materials;BOM”

Software Bill-of-Materials of Medical Devices

ポール・チュア　Paul Chua

CyberSecurity Officer, Greater Asia, BD

プロフィール

IT、電気通信、ヘルスケア、国土安全保障のために APAC レベルで製品開発と運用を管理した 25 年以上の経験を持つ経験豊富な専門家。

BD に入社する前は、データ分析スタートアップの最高製品責任者であり、ヘルスケア、BFSI、および政府企業向けの AI、および DataFusion-as-a-Service 製品の複数のスイートの開発を担当していた。

Profile

Paul is a seasoned professional with more than 25 years of experience managing product development and operations at APAC level for IT, Telecommunications, Healthcare and Homeland Security. Prior to joining BD,

Paul was the Chief Product Officer of a data analytics startup, where he was responsible for developing multiple suites of AI & Data Fusion-as-a-Service products for the Healthcare, BFSI, and Government enterprises.

講演要旨

このプレゼンテーションでは、医療機器ソフトウェアのライフサイクルにおける SBOM の開発と実行について説明し、実際の経験と潜在的な落とし穴を同時に共有します。

具体的には、成熟した SBOM プロセスを実装する方法は次のとおりです。

1. ソフトウェア開発プロセスを改善する
2. 労力を削減し、脆弱性監視の精度を向上させる
3. 合わせて、脆弱性通知の所要時間が短縮され、リスクが軽減され、利害関係者のインシデント対応が改善される

このプレゼンテーションの目的は、規制へのコンプライアンスを超えた、安全で効果的な接続された医療機器の構築における SBOM の利点を強調することです。

Abstract

This presentation would depict the development and execution of SBOM in a medical device software lifecycle, sharing some real-world experiences and potential pitfalls at the same time. Specifically, how implementing a mature SBOM process will:

1. Improve the software development process
2. Reduce effort and improve accuracy for vulnerability monitoring
3. And result in faster turnaround times for vulnerability notification, reducing risk and improving incident response for stakeholders

The goal of this presentation is to highlight the benefits of SBOM in building safe and effective connected medical devices, that go beyond simply compliance to regulations.

§3. パネルディスカッション

ランサムウェア対策としてのバックアップソリューション

Backup solutions as ransomware protection

座長:伊藤　春樹 （医療 ISC CTO）

Chairpersons: Haruki Ito (Medical ISAC Japan CTO)

プロフィール

電気通信大学 通信工学科卒業後、金融系シンクタンク・建設コンサルタントにてシステムアーキテクトを 10 年間勤務後、医療機器メーカー・医療系システムベンダーにおいて事業開発・品質管理責任者・DevOps 国内責任者等を 16 年間経験後、医療情報システム 3 省ガイドライン、内外法令や ISO27001 適合のためのコンサルティングを実施。

2020 年6月より現職。

Profile

After working as a system architect for 10 years at a financial think tank / a civil work consultanting firm, Haruki started his carrier in healthcate industry in 2021 and have been working as a business development / implementation manager / quality control manager / DevOps domestic manager at a medical equipment manufacturer / medical system vendor for 16

years. Haruki is now providing a consulting service for Japan's 3 ministries | 2 guielines for privacy safety, domestic and foreign regulatories, E-mail security, and ISO27001 compliance for medical facirities, information systems developeres and medial device developers at Medical ISAC Japan. Appointed as CTO in June 2020, and concurrent Auditor-Secretary as Jaruary 2021.

Rubrik によるデータセキュリティソリューション

Data Security Solutions by Rubrik

竹田　周平　Shuhei Takeda
ルーブリック・ジャパン株式会社　営業部長
Rubrik Japan K.K.　Sales Manager

プロフィール

2021 年 9 月より Rubrik Japan にて医療業界担当として、ランサムウェア対策・データセキュリティソリューションの営業担当。前職はピュアストレージにてオールフラッシュストレージの医療業界向け営業担当。

Profile

He has been in charge of sales of anti-ransomware and data security solutions for the medical industry at Rubrik Japan since September 2021. Previously, he was in charge of all-flash storage sales for the medical industry at Pure Storage.

会社紹介

2014 年に米国で設立された Rubrik は、ハイブリッド・クラウド環境に向けたデータ保護のリーディングカンパニーです。ガートナー社が発表した 2020 年度の「データセンター・バックアップ/リカバリ・ソリューションのためのマジック・クアドラント」ではリーダー企業に位置付けられ、フォーブス社の 2020 年度「The Cloud 100」では全体の 9 位にランクされています。

About Us

Founded in the United States in 2014, Rubrik is a leading data protection company for hybrid cloud environments. The company is positioned as a leader in Gartner's 2020 Magic Quadrant for Data Center Backup/Recovery Solutions and ranked 9th overall in Forbes' 2020 "The Cloud 100".

講演要旨

昨年 10 月 31 日の徳島県半田病院様のランサムウェア攻撃事例以降、医療業界に限らず世界的にランサムウェア被害が拡大する中、弊社データセキュリティソリューションがどのように診療活動の継続に貢献できるのか、弊社製品ならではの視点を踏まえて、簡単にご説明差し上げます。特に北米では EPIC のデータ保護ソリューションとして採用が近年加速しており、その背景も含め

てご紹介差し上げます。

Abstract
Since the ransomware attack on Handa Hospital in Tokushima Prefecture on October 31, 2011, we will briefly explain how our data security solutions can contribute to the continuity of medical treatment activities, based on our unique product perspective, as ransomware damage is expanding not only in the medical industry but also worldwide.
Especially in North America, the adoption of EPIC's data protection solutions has been accelerating in recent years, and we will also introduce the background of this trend.

ランサムウェアに備えた防災訓練を！　データを守るための必須施策

Disaster Preparedness Training for Ransomware! Essential measures to protect your data

神原　豊彦　Toyohiko Kanbara
ネットアップ合同会社 チーフテクノロジーエヴァンジェリスト
NetApp LLC　Chief Technology Evangelist

プロフィール
米国 IT プラットフォーム企業での Web 系システム、基幹系システム担当 SE を経て、2009 年に NetApp に入社。
10 年以上 国内外のクラウド関連ビジネスの立ち上げを技術面から担当。国内市場に向けたソリューションの企画・開発に従事。現在は、NetApp 全体のブランディングやプロモーションの企画・推進、データ ファブリックに関するエヴァンジェリスト活動に従事。
クラウドに加え、セキュリティを含む広範なデータ管理分野のエキスパートとして、テクノロジーを活用したお客さまとの"共創"を目指す。

Profile
After working as an SE in charge of web-based systems and mission-critical systems at a US IT platform company, he joined NetApp in 2009.
For more than 10 years, he has been in charge of launching cloud-related businesses in Japan and overseas from a technical perspective. Engaged in planning and developing solutions for the domestic market. Currently, he is engaged in planning and promotion of NetApp's overall branding and promotions, as well as evangelist activities related to data fabrics.
As an expert in a wide range of data management fields including cloud computing and security, he aims to "co-create" with customers by leveraging technology.

会社紹介
ネットアップは、1992 年、カリフォルニア州サンノゼに設立。業界をリードするクラウド データ サービス、ストレージ システム、ソフトウェアを開発し、お客様がデータを最大限に活用できるよう支援することに特化。30 年近くにわたり、主力製品である ONTAP データ管理ソフトウェアを中心

に、30 種類を超える非常に貴重なセキュリティ機能を提供。
https://www.netapp.com/ja/

About Us
NetApp was founded in 1992 in San Jose, California. For nearly 30 years, the company has focused on its flagship ONTAP data management software and more than 30 highly valuable security functionality.
https://www.netapp.com/ja/

講演要旨
ランサムウェアの脅威は医療業界においても対岸の火事ではありません。従来のような「予防」を前提とした対応策では対応が難しい状況にあります。
システム内での発症をいち早く検出し、感染被害を最小化するための抑制と迅速な復旧が必須事項となります。慌てず騒がず落ち着いて対応するためにも、定期的な健康診断と防災訓練を実施するためのヒントをお伝えします。
Abstract
The threat of ransomware is no longer a concern for the healthcare industry. It is difficult to respond to the situation with conventional ″prevention″ based countermeasures.
It is imperative to detect outbreaks in the system as soon as possible, and to control and quickly restore the system to minimize the damage caused by the infection. In order to respond calmly without panicking or making a fuss, we will provide tips for conducting periodic health checks and disaster drills.

バックアップデータをランサムウェアから守る最新技術
Protect your backup data from ransomware with the latest technology

笹 岳二　Gakuji Sasa
Cohesity Japan 株式会社 シニア SE マネージャー
Senior SE Manager, Cohesity Japan K.K.

プロフィール
20 年以上外資 IT メーカー（サン・マイクロシステムズ、NetApp）においてプリセールス SE や SE マネージャーとして従事し、金融、製造のお客様に対して IT インフラの提案活動に従事。
その後、アマゾンウェブサービス(AWS)においてテクニカル・アカウント・マネージャーとして金融、マーケティングのお客様に対してシステム運用面でのアドバイザとして活動してきた。
2020 年 10 月から現職の Cohesity Japan 株式会社に移り、SE マネージャーとして次世代データ管理ソリューションの提案活動を行うプリセールス SE チームのマネジメントを行う役割を担っている。

Profile

Gakuji worked with global IT vendors (Sun Microsystems, NetApp) for more than 20 years in systems engineering & management, proposing solutions for customers in the finance & manufacturing verticals. At Amazon Web Services (AWS), he advised financial and manufacturing customers on systems operations. Joining Cohesity Japan K.K. in October 2020, Gakuji now oversees a team of systems engineers proposing next-generation data management solutions to the Japanese market.

講演要旨

巧妙なサイバー攻撃に対抗するには、従来の侵入予防ソリューションだけではもはや有効とは言えません。万一侵入された時に対抗できるよう、本セッションでは、AI による脅威検知、迅速な大規模復旧、バックアップデータをランサムウェア攻撃から守る最新技術をご紹介します。

Abstract

With increasingly sophisticated cyber-attacks, legacy intrusion prevention systems just don't measure up. In this session, we'll show you how you can respond when you have a cybersecurity incident with the latest technologies for AI-powered threat detection, rapid recovery at scale, and backup data protection from ransomware attacks.

§4. 医療 ISAC 企画プログラム

地域基幹病院をサイバー攻撃から守りたい！病院のサイバーセキュリティ診断費用を支援するためのクラウドファンディングの立ち上げについて

We should like to protect the key hospitals; A crowdfunding to help hospitals to receive cyber security diagnosis launched.

深津　博　Hiroshi Fukatsu
医療 ISC 代表理事　Medical ISAC Japan Representative Director

講演要旨

先般医療 ISAC が企画して四病院団体協議会加盟病院に対して行ったサイバーセキュリティに関するアンケート結果では、回答病院の約9割がサイバーセキュリティに関する脅威を感じていること、5割以上の病院のセキュリティ予算が500万円以下であり、その大半が予算不足を感じていること、具体的な対策としてまずは何から取り組んでよいのかわからない、と感じていること、などの実態が浮かび上がった。
https://m-isac.jp/wp-content/uploads/2022/04/FinalReport_202220331.pdf
医療 ISAC ではこのような状況に対する対策として、まずはサイバーセキュリティに関する診断を受けた上で、その結果に基づいて個別最適化された対策の導入を支援すべきであると考え、その診断費用を賄うためのクラウドファンディングを企画致しました。
上記診断サービスは、医療 ISAC が昨年12月に東京都立の2病院に対する攻撃予兆を察知して、東京都に対して注意喚起を行った結果、攻撃を予防できた際に用いた手法と同一のもので

ある。なお、募集期間は 6 月 10 日～7 月 31 日を想定している。

Abstract
According to the survey performed in Feb. 2022 by Medical ISAC Japan for over 5900 hospitals in Japan, nearly 90% of the hospitals feel actual thread in cyber security, more than half of the hospitals can use less than 5 million yen or 50,000$ per year for cyber security. About 40% of the hospitals feel shortage of the cyber security budget and the majority of the hospitals cannot have confidence what to start with for cyber security protection.
https://m-isac.jp/wp-content/uploads/2022/04/FinalReport_202220331.pdf
As Medical ISAC Japan considers that the hospitals should receive the thread intelligence diagnosis and monitoring to notice the one-by-one thread situation and suggest a personalized and optimized solution, we planned and started the crowdfunding for the hospitals to help them receive the thread intelligence diagnosis and monitoring.
The thread intelligence method is identical to the one we succeeded to prevent the attack on two Tokyo metropolitan hospitals in Dec. 2021.
The offering period is from 10 of June to 31 of July.

今求められる外部公開システム管理

External Attack Surface Management required today

佐野　健一　Kenichi Sano
サイファーマ株式会社　エバンジェリスト / プリセールスマネージャー
Cyfirma K.K.　Evangelist / Pre-Sales Manager

プロフィール
2005 年よりセキュリティ業界に従事。
前職はセキュリティ専業会社のインフォセックにてシニアコンサルタントとして、セキュリティ関連のアセスメント・アドバイザー・グランドデザイン策定支援などを実施。
2017 年から 2020 年にかけて大手商社に出向し、セキュリティ戦略立案からインシデント対応まで幅広く携わる。1000 社を超える子会社に対するセキュリティアセスメント施策の計画立案・実行を行う。
その他、2012 年から 2019 年にかけて某財閥系セキュリティ研究部会アドバイザー・外部有識者として活動。

Profile
Kenichi Sano has 17 years of security consultant experience serving multiple clients and industries. Previously, as a senior consultant at Infosec, a security services provider, he led security assessments, advisory services, and assisted in the formulation of grand designs.
From 2017 to 2020, he was seconded to a multinational trading company, to support their

security strategy planning, incident response, and planning/executing security assessment initiatives for over 1,000 subsidiaries.
In addition, from 2012 to 2019, he served as an advisor and external expert for a security research group of a renowned Japanese conglomerate.

講演要旨

ランサムウェア被害の報道が止みません。ランサムウェア攻撃グループの動向から彼らの手法を読み解き、ランサムウェアへの対応するうえで大切なものは何か？彼らの侵入口として利用される外部に公開されているシステムの管理の重要性についてご紹介します。

Abstract

Ransomware incident reporting continue to increase. Based on trend of ransomware gang attack methods, Kenichi Sano will introduce essential security measures against ransomware attacks focusing on the importance of managing internet facing system often targeted by them.

院内環境を死角なく完全保護する AI 免疫システム

AI Immune System for complete visibility and protection of hospital systems

鈴木　真　Makoto Suzuki
ダークトレース・ジャパン株式会社 カントリーマネージャー
Darktrace Japan KK Country Manager

プロフィール

IT 業界の法人営業として、30 年間以上一貫したキャリアを持つ。
2010 年以降は成長著しいサイバーセキュリティ業界に従事、米シマンテック日本法人にて金融・公共部門の営業部長を経た後、執行役員としてテレコムエリアを除く法人営業部隊を統括。
その後、米デル・ テクノロジーズ日本法人では端末における AI セキュリティソリューション等の製品営業部隊を統括した。
2020 年 11 月にダークトレース・ジャパンのカントリーマネージャーに就任し、現在、東京と大阪の両オフィスを統括する。

Profile

Makoto has over 30 years of experience in corporate sales in Japan's IT industry, and has been involving in the fast-growing cybersecurity industry since 2010. At Symantec Japan, Makoto worked as a Senior Sales Manager for financial and public sectors, then was in charge of its corporate sales teams (excluding telecom area) as a Managing Director. Later, at Dell Technologies Japan, he managed its sales force covering various products such as AI security solutions for endpoint. In November 2020, he was appointed as a Country Manager at Darktrace, where he oversees its Tokyo and Osaka offices.

会社紹介

Darktrace（ロンドン証券取引所上場、ティッカーシンボル:DARK）はケンブリッジ大学の数学者らにより 2013 年 に設立されました。

人間の免疫システムに着想を得て開発された Darktrace Immune System は、ネットワーク内 外に分散する組織の従業員・デバイスの挙動や通信の定常状態（生活パターン）を、独自開発の自己学習型 AI によりデジタルインフラの種類を問わず常時機械学習・完全可視化し、定常から逸脱するサイバー脅威をリアルタイムに自動検知・遮断、さらに検知した脅威の調査分析・レポーティングまで高速自動化する世界初の製品・技術で、日本を含む世界 110 か国以上で 6,800 社以上の組織に導入されています。

サイバーセキュリティ業界で欧州最速成長企業（英フィナンシャル・タイムズ、2020 年）で、TIME 誌の 2021 年版「世界で最も影響力のある 100 社」にも選出されました。

About Us

Darktrace (DARK.L), a global leader in cyber security AI, delivers world-class technology that protects over 6,800 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. Darktrace's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it.

Headquartered in Cambridge, UK, the Group has more than 2,000 employees worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

講演要旨

2013 年に世界で初めて AI をサイバーセキュリティに大規模適用した Darktrace の「AI 免疫システム」は、医療 IoT 機器や持ち込み端末を含む院内のあらゆるデバイスやユーザーの「生活パターン」をさながら人間の免疫のごとく自律的に機械学習と可視化を続け、どんな異常も予兆レベルで検知・遮断、さらに異常の原因まで AI が瞬時に自動調査する。

クローズドな院内ネットワークにおける接続状況も診療業務に影響なくゼロベースで自己学習し、院内システムを網羅的に自律保護する次世代の AI セキュリティについて、検知実例とデモを交えて詳説する。

Abstract

Darktrace is a world leading provider of AI for the enterprise, with the first at scale deployment of AI in cyber security back in 2013. Its immune system technology continues to autonomously learn and visualize the normal "pattern of life" of every device, user and network within a hospital, including medical IoT and BYOD devices of which the organization was previously unaware - just like a human immune system. The AI-powered system automatically detects and contains threats at their earliest stages, and even triages, interprets and reports on the full scope of security incidents.

This presentation will explain in detail, along with real-world detection examples and a live demo, how Darktrace's self-learning AI technology can defend the integrity of hospital systems autonomously, learning real-time status of even closed hospital networks from scratch, without

affecting normal medical treatment operations.

サイバー攻撃と Active Directory との関係の誤解を解く

Clearing misconceptions about connection between Cyber Attacks and Active Directory

畑瀬　宏一　Koichi Hatase
Tenable Network Security Japan 株式会社　セキュリティエンジニア
Security Engineer, Tenable Network Security Japan K.K.

プロフィール

Tenable 社でセキュリティエンジニアとして、Active Directory に特化したセキュリティ対策製品の拡販に携わっている。

Profile

As a security engineer at Tenable, he is involved in expanding sales of security products focused on Active Directory.

会社紹介

Tenable® は脆弱性管理ソリューションを提供します。世界中のおよそ 4 万の企業と組織が、サイバーリスクを正確に把握し、削減するために Tenable を採用しています。
Nessus® の開発者である Tenable は、脆弱性に対する専門性を基盤に、あらゆるコンピューティングプラットフォーム上のあらゆるデジタル資産を管理、保護できる世界初のプラットフォームを展開しました。Tenable は、フォーチュン 500 の約 6 割、およびグローバル 2000 の約 4 割の企業や、大規模な政府機関などで採用されています。
詳しくは https://jp.tenable.com/ をご覧ください。

About Us

Tenable® is the Cyber Exposure company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at https://www.tenable.com/

講演要旨

ランサムウェアによる被害を防ぐためには、サイバー攻撃と Active Directory の関係を理解しておくことが極めて重要です。
Active Directory のセキュリティ対策について、よくある誤解を解きながら採るべき方法をご説明いたします。

Abstract
To prevent damage from ransomware, it is critical to understand the connection between cyber attacks and Active Directory.
We will explain how to take measures to secure your Active Directory while clearing up common misconceptions.

§5. Health-ISAC 企画プログラム

パネルディスカッション:ゼロトラスト
Panel Discussion: Zero Trust

座長:神流　ウェンディ　武田薬品工業株式会社
セキュリティー・ガバナンス&オーバーサイト統括責任者
Chairpersons: Wendy Kanna　Takeda Pharmaceutical Company Limited
Global Head of Security Governance & Oversight

プロフィール
2016 年 6 月武田薬品工業入社
サイバースレットマネージメント統括責任者(2016 年-2019 年)
シティバンク日本:バイスプレジデント(2004 年～2016 年)
H-ISAC Japan Council　共同代表

Profile
Hired June 2016
Previously Global Head of Cyber Threat Management (2016 - 2019)
Former Vice President, Citibank Japan Ltd. (2004 - 2016)
Co-Chairman, H-ISAC Japan Council

再考！ゼロトラストネットワークアクセスの重要性”VPN を超える最適なアプローチとは”
Rethink! The Importance of Zero Trust Network Access
"What is the Best Approach Beyond VPN?"

丸山　龍一郎　Ryuichiro Maruyama
ゼットスケーラー株式会社　技術副本部長
Zetscaler K.K. Deputy General Manager of Technology

プロフィール
システム開発で 10 年、セキュリティ業界で 25 年以上従事し、企業様環境におけるセキュリティのアーキテクチャ及びソリューション導入のための設計、構築、運用を支援してきました。現職ではSE チームを率いて、企業のゼロトラストアーキテクチャの導入や DX の展開を支援しています。

Profile

With 10 years in systems development and over 25 years in the security industry, I have helped design, build, and operate security architectures and solutions for implementation in corporate environments. In his current position, he leads a team of SEs to help companies implement zero-trust architectures and deploy DX.

講演要旨

昨今、リモートアクセスで利用されている VPN の脆弱性を利用したセキュリティインシデントが多く報告されています。
このセッションでは、再度 VPN を利用する上でのリスクや課題をご理解いただき、ゼロトラストネットワークアクセスの必要性と安全性についてユースケースも含めてご説明させていただきます。

Abstract

Recently, many security incidents have been reported using vulnerabilities in VPNs used for remote access.
In this session, we will help you understand the risks and challenges of using VPN again and explain the necessity and safety of zero-trust network access, including use cases.

武田薬品工業のゼロトラストへのアプローチ

Takeda's approach to Zero Trust

リカス トーマス　Thomas Likas
武田薬品工業株式会社
セキュリティエンタープライズアーキテクチャ責任者
Takeda Pharmaceutical Company
Head of Security Enterprise Architecture

プロフィール

2009 年 11 月武田薬品工業入社
多種のセキュリティアーキテクチャに従事
セキュリティトランスフォーメーション、ゼロトラスト、安全なデータ管理を専門

Profile

Joined Takeda in November 2009
Occupied various Security Architecture roles
Expertise in security transformation, Zero Trust, secure Data practices

講演要旨

ゼロトラストは安全にアプリケーションを導入するための新しいアプローチです。
アプリケーションへのネットワーク/インフラストラクチャ中心のアプローチから、ユーザー/デバイスのアイデンティティとインテリジェンスに基づき評価される、ポリシーエンジンに基づくアクセス制御モデルに移行しています。
当社でのゼロトラストの選定、目標、現在の状況及び今後の展望などを発表いたします。

Abstract

Zero Trust is a new approach for secure application delivery, moving away from the network / infrastructure centric approach where applications can be accessed simply due to network connectivity, to an access model based on a policy engine controlling access evaluating explicit policies based on user / device identity and intelligence factors.
The presentation will revisit Takeda's adoption of Zero Trust, goals, current status and outlook.

(Memo)

一般社団法人医療ＩＳＡＣ

〒103-0021 東京都中央区日本橋本石町 3－3－8 日本橋優和ビル 5F
電話：03－3527－9528　FAX：03－3527－9950

URL：https://m-isac.jp/
Facebook：https://www.facebook.com/medical.isac/