TLP:GREEN

Medical Device Cyber Security Council
医療機器サイバーセキュリティ協議会

ロシアのウクライナ侵攻に伴うサイバー攻撃リスクの顕著な増大に対する緊急の形態と対応

医療機器サイバーセキュリティ協議会事務局　2022/2/28配信

- 全世界の多くのサイバー攻撃者集団が、ロシア側、ウクライナ側にそれぞれ支持を表明し代理戦争を始める勢いで、サイバー攻撃が全面戦争に突入する可能性があります。日本もロシアに対する経済制裁への報復として標的にされる危険性が極めて高くなっており、重要インフラである病院は格好のテロ対象となるため、カルテの消失・医療システムの麻痺による病院機能麻痺を憂慮しており、対応に一刻の猶予も残っていないと判断し、緊急の警戒と対応を呼びかけます。
- 当協議会では、事態の深刻さを鑑みて、医療機関に対するサイバーインシデントの発生に備え緊急点検を呼びかけます。
  - ① 院内及び連携地域病院に対する緊急時連絡網の確認と製販業者の緊急連絡窓口の確認
  - ② 脆弱性に対するパッチ未適用のOSや、デフォルトパスワードのまま利用しているネットワーク機器の総点検
  - ③ 電子カルテなどの代替不能な医療情報システム上のデータのオフラインバックアップの取得
  - ④ システム停止に備えたシステム代替手段の検討と確認
  - ⑤ COLINT(集合による活動）を最大限活用し、「わからないから対処しない」ではなく、適切な相手に相談をする
    - 政府や政府系組織がリリースする注意喚起文章を参照する。有事は適切なサイバーセキュリティお助けサービスを確認しておくk
      - IPA、厚労省、経産省などからのサイバーセキュリティ系文章の参照
      - IPAのサイバーセキュリティお助け隊サービス（ https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html)
    - システムのセキュリティ要件、確認を業者に依頼する
    - MDCSC（ 医療機関と製販業者によるサイバーセキュリティの協議会）に相談する
      - 参加申請: info@mdcsc.jp, 相談：consult@mdcsc.jp