令和５年２月１５日

医療システムにおけるサイバー事案対策について

警察庁サイバー警察局
サイバー企画課

医療機関におけるランサムウェア被害（国内）

日本経済新聞

ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃

2021年11月12日 11:30

サイバー攻撃で電子カルテによる診療が中断されている半田病院（2日、徳島県つるぎ町）＝共同

徳島県つるぎ町の町立半田病院を10月末、サイバー攻撃が襲った。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コンピューターウイルス「ランサムウエア」に感染した。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を停止。復旧のめどは立っていない。命を守る地域の重要インフラは大打撃を受けた。

出典：日本経済新聞　https://www.nikkei.com/article/DGXZQOUE071OKOX01C21A1000000/

NHK NEWS WEB

関西 NEWS WEB

大阪急性期・総合医療センター サイバー攻撃で診療影響続く

11月01日　15時55分

「ランサムウエア」と呼ばれる身代金要求型のウイルスによるサイバー攻撃を受けた大阪急性期・総合医療センターでは、１１月１日も緊急以外の手術を停止するなど影響が続いています。
病院を訪れた患者からは「どこかに情報が流出してしまったら怖い」などと不安の声が聞かれました。

大阪・住吉区の大阪急性期・総合医療センターでは、１０月３１日、「ランサムウエア」とよばれる身代金要求型のウイルスによるサイバー攻撃を受け、電子カルテなどのシステムに障害が発生して閲覧などができなくなっています。
このため、病院では３１日に続き、１日も朝から通常の外来診療や緊急以外の手術を停止しているほか、救急患者の受け入れもできない状況だということです。

出典：NHK NES WEB　https://www3.nhk.or.jp/kansai-news/20221101/2000067859.html

医療機関におけるランサムウェア被害（国外）

ランサムウエアで初の死亡例か　病院が標的に

ハッカー攻撃で機器が停止、胎児の危険な兆候を医療スタッフが見逃す結果に

Why Ransomware Attacks Are on the Rise and How the U.S. Can Fight Them

Why Ransomware Attacks Are on the Rise and How the U.S. Can Fight ThemPlay video: Why Ransomware Attacks Are on

出典：https://jp.wsj.com/articles/a-hospital-hit-by-hackers-a-baby-in-distress-the-case-of-the-first-alleged-ransomware-death-11633317285

サイバー攻撃で病院のシステムが停止、救急患者が死亡＝ドイツ

~2分

ドイツのデュッセルドルフ大学病院でランサムウェアが救急医療を妨害し、警察が「過失致死」容疑で捜査を開始した。サイバー攻撃が史上初めて、患者の死亡に直接つながったケースだ。

ケルンの捜査当局によると、死亡した女性患者は9月9日、デュッセルドルフ大学病院で救命処置を受ける予定だった。だが、ランサムウェア攻撃を受けてシステムが停止したため同病院での治療ができなくなり、19マイル（約30キロメートル）離れた別の病院に搬送された。BBCは、攻撃を仕掛けたハッカーが刑事責任を問われる可能性があると報じている。

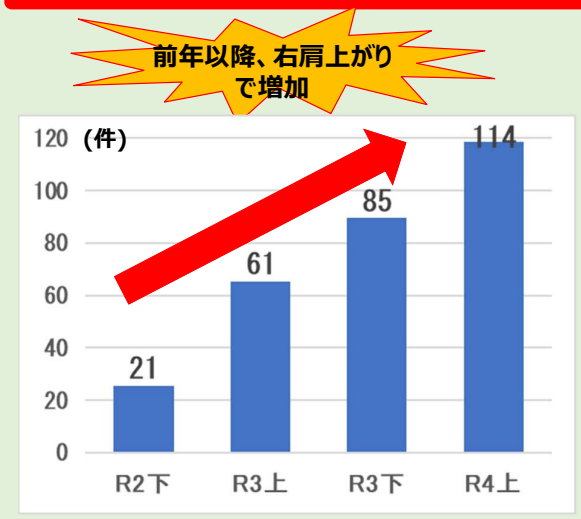
出典：https://www.technologyreview.jp/s/220021/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital

New Ponemon Report Shows Ransomware Continues to Impact Patient Safety, Per Survey of Hospital IT/Security Leaders

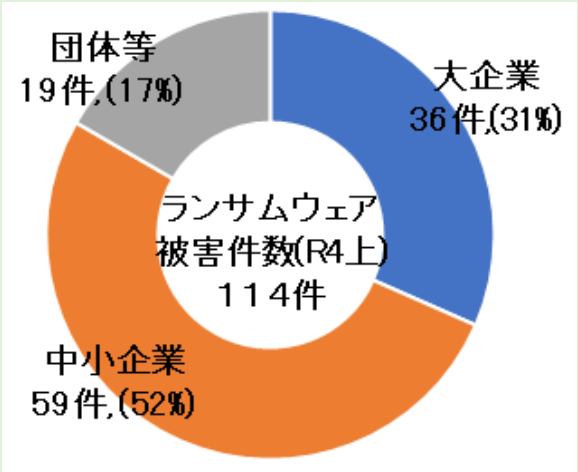
出典：https://www.censinet.com/about/press-releases/new-ponemon-report-shows-ransomware-continues-to-impact-patient-safety-per-survey-of-hospital-it-security-leaders/

ランサムウェア被害が増加傾向（令和４年上期）

ランサムウェア被害の報告件数の推移

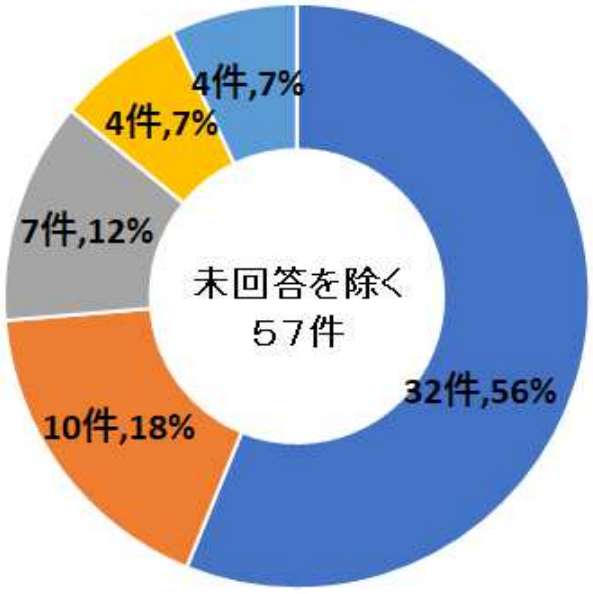


被害企業・団体等の規模別報告件数



VPN機器が侵入経路として狙われている傾向（令和４年上期）

感染原因　（R4上期）

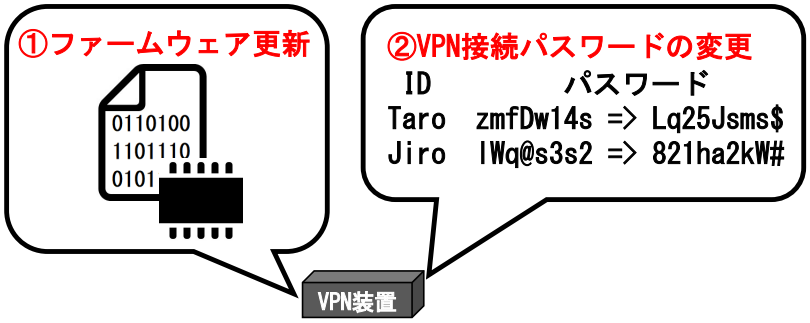


- VPN機器からの侵入
- 不明/調査中
- リモートデスクトップからの侵入
- 不審メールやその添付ファイル
- その他

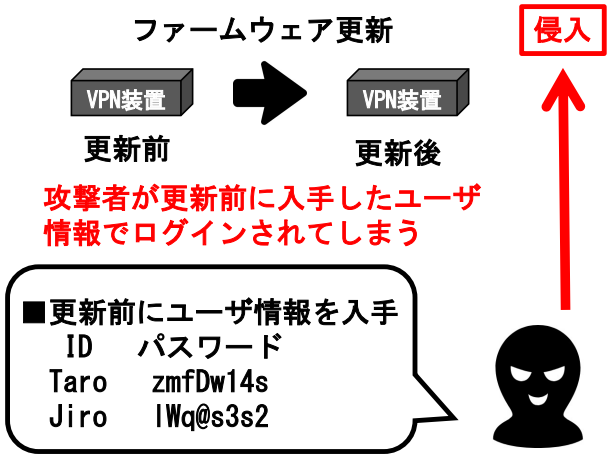
VPN機器からの侵入対策

■VPN装置の脆弱性から侵入されている事案が多い
①VPN装置の脆弱対策版ファームウェアは確実に更新
②<u>VPN装置のファームウェア更新</u>と<u>同時にVPN接続のパスワード変更</u>

〇ファームウェア更新及びパスワード変更



〇VPN接続パスワードを変更する理由

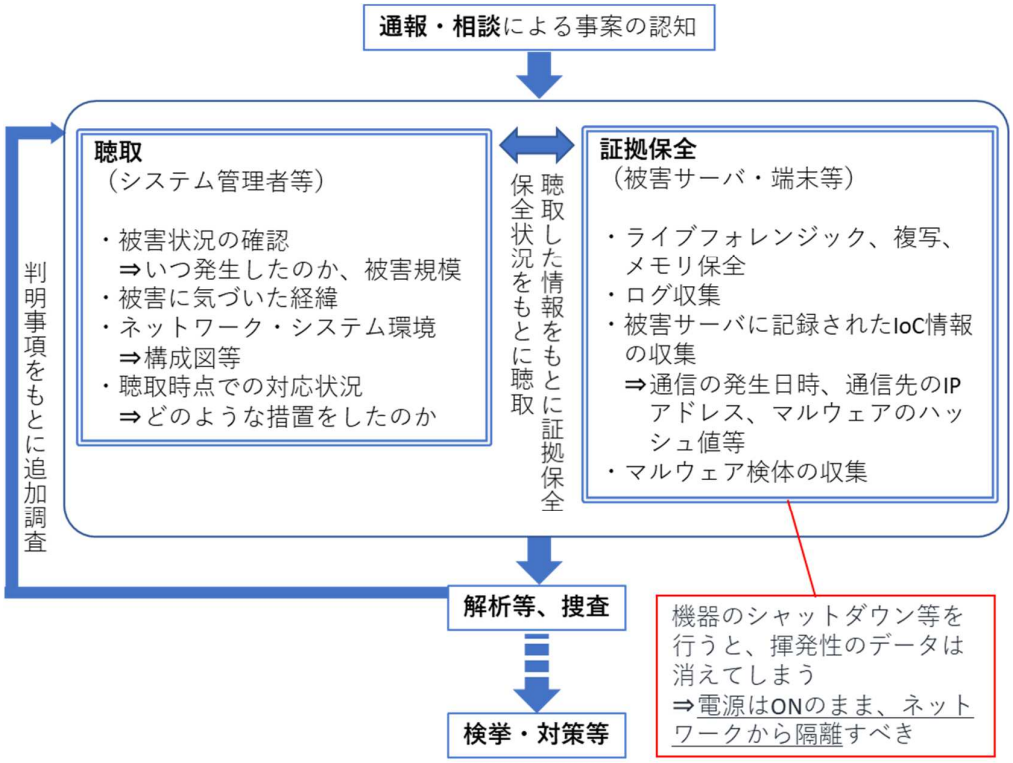


警察におけるランサムウェア事案の初動対応等

【警察の方針】患者への対応やシステム復旧を優先
被害法人に過度の負担はかけない

■初動対応時における捜査活動
〇通信ログの保全依頼（外部接続機器を中心とした可能な範囲）
〇システム担当者からの事情聴取
（内容）・被害端末に関する情報
・インターネットにより接続可能な機器に関する情報
・業務への影響、復旧方針　等
→被害原因（状況、手口、攻撃者情報等）の早期解明
→被害法人のシステムの早期復旧・被害回復の支援
※警察において対応が難しい内容
（医療機関の運営方針にかかる助言、直接の作業、機器の設定等）

〈参考〉警察における捜査の流れ



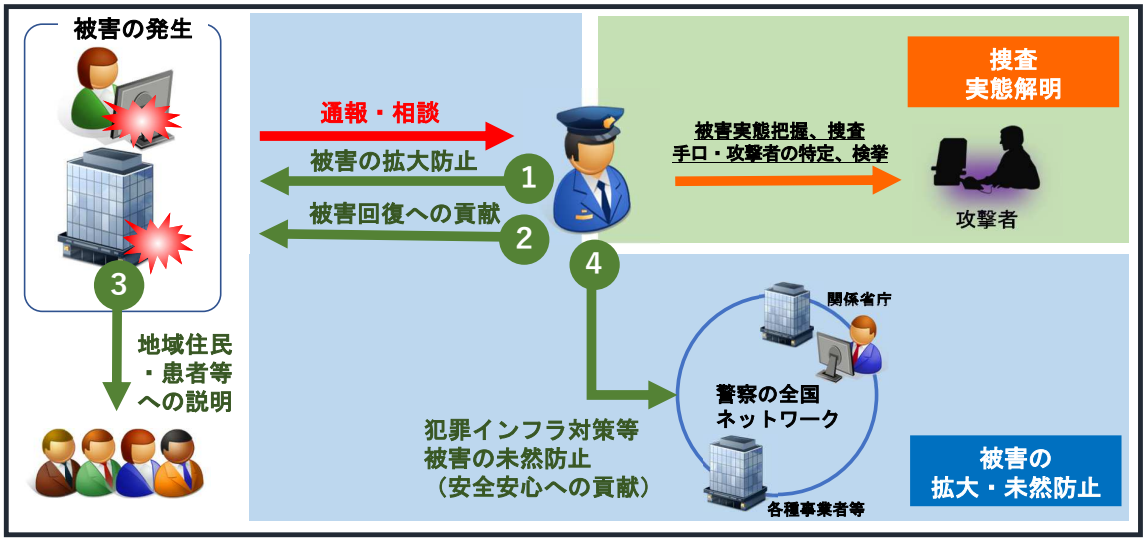
医療情報システムベンダーの皆様へ

■平時における医療機関への支援
〇深刻度の高いぜい弱性について迅速に更新
※特に外部接続機器、重要度の高いシステム
※システムへの検証を実施した上で更新
〇重要度の高いデータのバックアップ
※追記不可メディアやネットワークから切り離して保管
〇各種ログの確認によるインシデントの早期発見

■ランサムウェア被害時（初動時）のお願い
〇通信ログの保全（外部接続機器を中心とした可能な範囲）
〇インターネット接続している機器に関する
情報の提供（医療機関経由で）
※製品名、バージョン、パッチの適用状況、設定情報等

警察に通報することによる病院等におけるメリットについて

① 被害医療機関等における被害の拡大防止（初動対応・再発防止等に関する助言等）
② 被害回復への貢献（被害回復制度等に関する助言、ランサムウェア被害時の被害回復に向けた支援）
③ 地域医療機関として社会的責任を果たしていることの説明（一般に犯罪に遭った際には警察に通報することが期待される）、犯罪の被害者であることの疎明
④ 社会全体の被害の未然防止（安全・安心なサイバー空間の確保に対する社会的貢献）



ランサムウェア被害時の初動対応が重要

○被害発生時には、（医療機関から）警察への通報相談をお願いいたします。

○警察活動にご理解いただき、医療機関の支援、警察との連携をお願いいたします。