医療機関等へのサイバー攻撃

こんな人間です

- 経歴

07年　某大学ラグビー部卒業、翌年同大工学部卒

08年　日経入社　社会部配属（警視庁1課担当）

10～13年　西部支社（暴力団取材など）

13～15年　社会部（警視庁2課、公安担当）

→マウントゴックス事件でセキュリティに片足を突っ込む

16～18年　日経ビジネス編集部（セキュリティ、個人情報、「敗軍の将兵を語る」「謝罪の流儀」企画担当）

→企業不祥事の取材の傍ら、主要取材テーマのうち一つがセキュリティに

21年　調査報道グループ（「国費解剖」企画担当、セキュリティの調査報道）

→業務の半分がセキュリティに

22年　企業報道ユニット（セキュリティ担当、「サイバーカオス」企画担当）

九州大SECKUN　3期生

- 趣味

海外ベンダのレポートのザッピング、RPA作成、ホームジムで筋トレ

- バイブル

デビッド・サンガー

「サイバー完全兵器」

NIKKEI

日経のサイバー関連調査報道

就活生の「辞退予測」情報、説明なく提供　リクナビ
【イブニングスクープ】

就活　＋フォローする

2019年8月1日 18:00 (2019年8月1日 22:16更新) [有料会員限定]

保存

リクナビは年80万人の就活生が利用している

連載企画「サイバーカオス　解明コンティ」　まとめ読み

サイバーセキュリティー　＋フォローする

2022年5月22日 2:00

保存

認証情報、「公開のまま」700件
ソフト開発ツール「ギットハブ」、専門家はリスク指摘

データの世紀　＋フォローする

2022年1月12日 0:00 [有料会員限定]

保存

インターネット上で使うソフトウエアの開発支援ツール「GitHub(ギットハブ)」を巡り、利用ルールの順守が求められている。ツール内でプログラムを公開し、多数の技術者の知見を共有できるが、誤って重要情報を公開すると機密漏洩につながりかねない。ツールを狙ったサイバー攻撃も絶えない。

病院に相次ぐサイバー攻撃　遅れる医療の防衛、日経調査
大規模3病院に侵入　3分の2でパスワード漏れも

サイバー防衛　＋フォローする

2022年5月28日 16:32 (2022年5月28日 16:34更新) [有料会員限定]

保存

病院へのサイバー攻撃が相次いでいる。国内の大規模病院3カ所がハッカーから侵入された可能性の高いことが日本経済新聞の調査で分かった。大型病院100カ所の情報を闇サイトで調べたところ、3病院のシステムに侵入したプログラムが販売されてい

企業の漏洩パスワード6割が脆弱　推測容易で瞬時に突破

ット・IT　＋フォローする

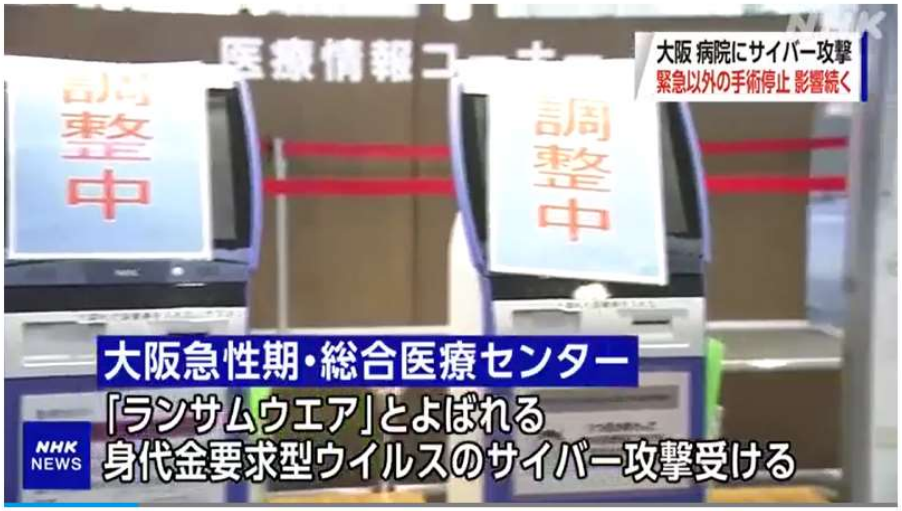
022年8月26日 22:31 [有料会員限定]

保存

医療機関等の直近のサイバーリスク

1. ランサムウエア攻撃

■2018　奈良県の宇陀市立病院で電カル使用不能に
■2021　市立東大阪医療センターの遠隔読影システムが停止
■　　徳島県つるぎ町立半田病院で電カル使用不能に
■2022　大阪急性期・総合医療センターで電カル使用不能に



サイバー攻撃受けた大阪の病院 外来診療や緊急以外の手術停止

出典：NHK

医療機関等の直近のサイバーリスク

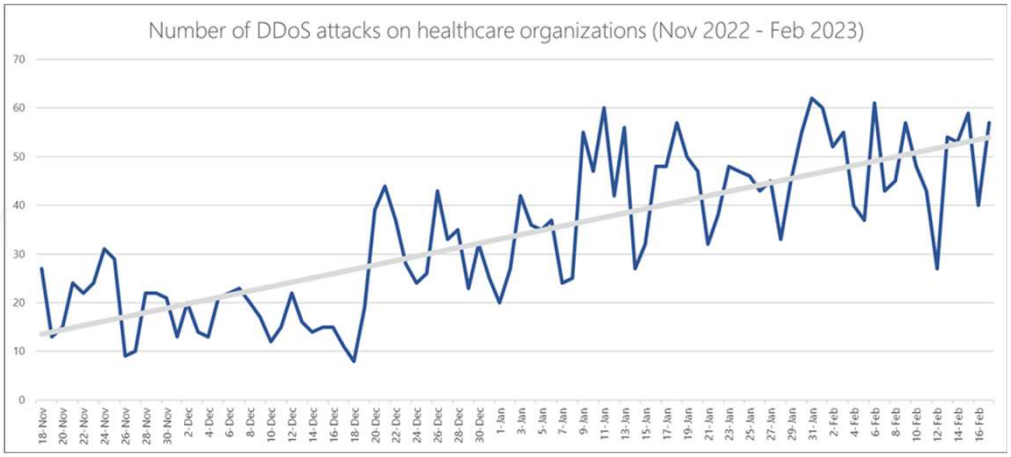
2. DDoS攻撃

- ■Hacktivist=政治信条を動機としたサイバー攻撃集団。直近ではウクライナ侵攻に絡み攻撃を広域展開
- ■9月、2月にも日本の重要インフラ、政府機関、大手メーカーを襲撃
- ■医療機関のリスクは・・・？

March 17, 2023 • 6 min read

KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks

Azure Network Security Team



出典：Microsoft

医療機関等の直近のサイバーリスク

3. Emotet

■メールを通じて自己増殖する「最恐ウイルス」

■2022年年明けから日本で集中的に急拡大

■Excel→LNK→コンテナファイル→OneNoteとMicrosoftといたちごっこ

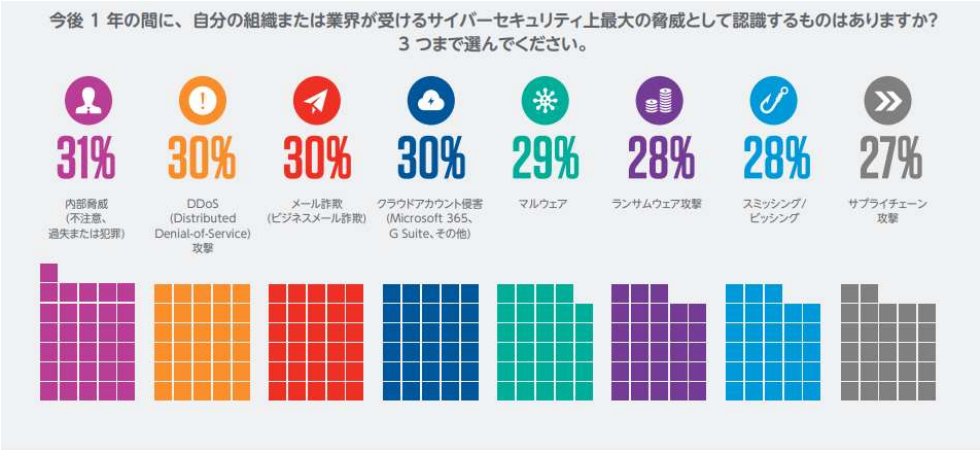
公表日	医療機関名／組織名	公式発表
2/9	社会医療法人 大雄会	当会パソコンへのウイルス感染に伴う不審メール発生に関するお詫びとお知らせ
3/3	那須南病院	那須南病院におけるコンピューターウイルス感染と関係者への不審メール発生に関するお詫びとお知らせ
3/7	医療法人 健昌会	ウイルス感染に伴う不審メール発生に関するお詫び
3/16	公益財団法人 佐々木研究所附属 杏雲堂病院	当院の職員を装った「なりすましメール」に関するお詫びとお知らせ
3/28	東京都済生会向島病院	当院職員を装った不審メールに関するお詫びとお願い
5/20	日本赤十字社 秋田赤十字病院	当院職員を装った不審メールについて

出典：MICIN

医療機関等の直近のサイバーリスク

4. 内部脅威

■メディアの紛失、情報の不正閲覧etc



出典：Proofpoint

■個人情報保護法の改正
→報告義務と通知義務

1. 要配慮個人情報が含まれる事態
2. 財産的被害が生じるおそれがある事態
3. 不正の目的をもって行われた漏えい等が発生した事態
4. 1,000人を超える漏えい等が発生した事態

身体障害、知的障害、精神障害等の障害があること、健康診断その他の検査の結果、保健指導、診療・調剤情報

世界と日本のランサムウエア動向

NEWS

Is ransomware declining? Not so fast, experts say

While some 2022 ransomware statistics indicate a possible 'decline' in activity, threat researchers warn there's more to the picture than the numbers suggest.

By **Alexander Culafi**, Senior News Writer　　Published: **09 Mar 2023**

Recent insights from cybersecurity vendors indicate a ransomware decline in 2022. But experts caution the reality of the situation is more complicated.

IBM's X-Force last month published their annual Threat Intelligence Index report, which claimed defenders were getting better at stopping ransomware attacks. IBM found that a slightly smaller percentage of threat actors managed to successfully execute a ransomware attack in 2022 than the previous year. IBM X-Force's head of research John Dwyer told TechTarget Editorial the drop is the first he has seen in five years.

Ransomware incident response vendor Coveware said in January that it had seen a considerable drop in the percentage of victims deciding to pay the ransomware ransom, from 85% of victims in Q1 2019 to 37% of victims in Q4 2022. Mandiant, meanwhile, told TechTarget Editorial it responded to 15% fewer ransomware incidents in 2022 and saw a 7% decline in the number of victims it tracked on data leak sites.

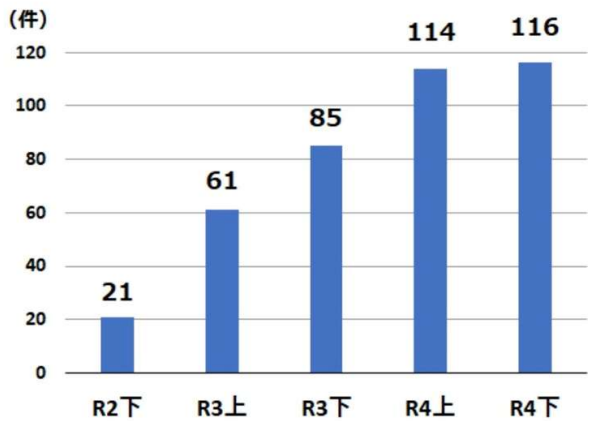
Sponsored News

Modernizing Cyber Resilience Using a Services-Based Model
–Dell Technologies

Defeating Ransomware With Recovery From Backup
–Exagrid

出典：IBM

【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】



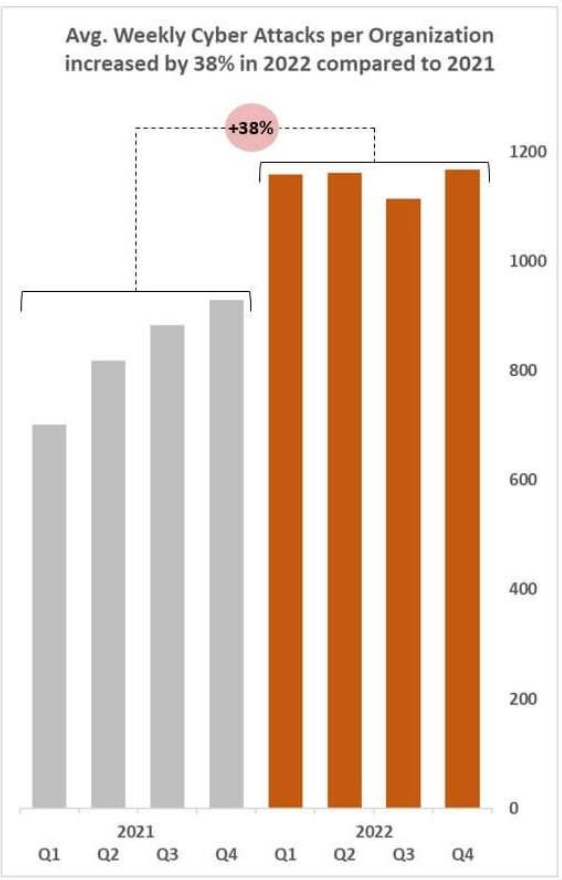
世界

- 大統領令＋制裁による身代金支払いの「非合法化」
- サイバー保険のカバレッジ縮小

日本

- これまでちゃんと報告されていた・・・？
- サイバー保険のカバレッジがもともと小さい

医療機関のリスク増加

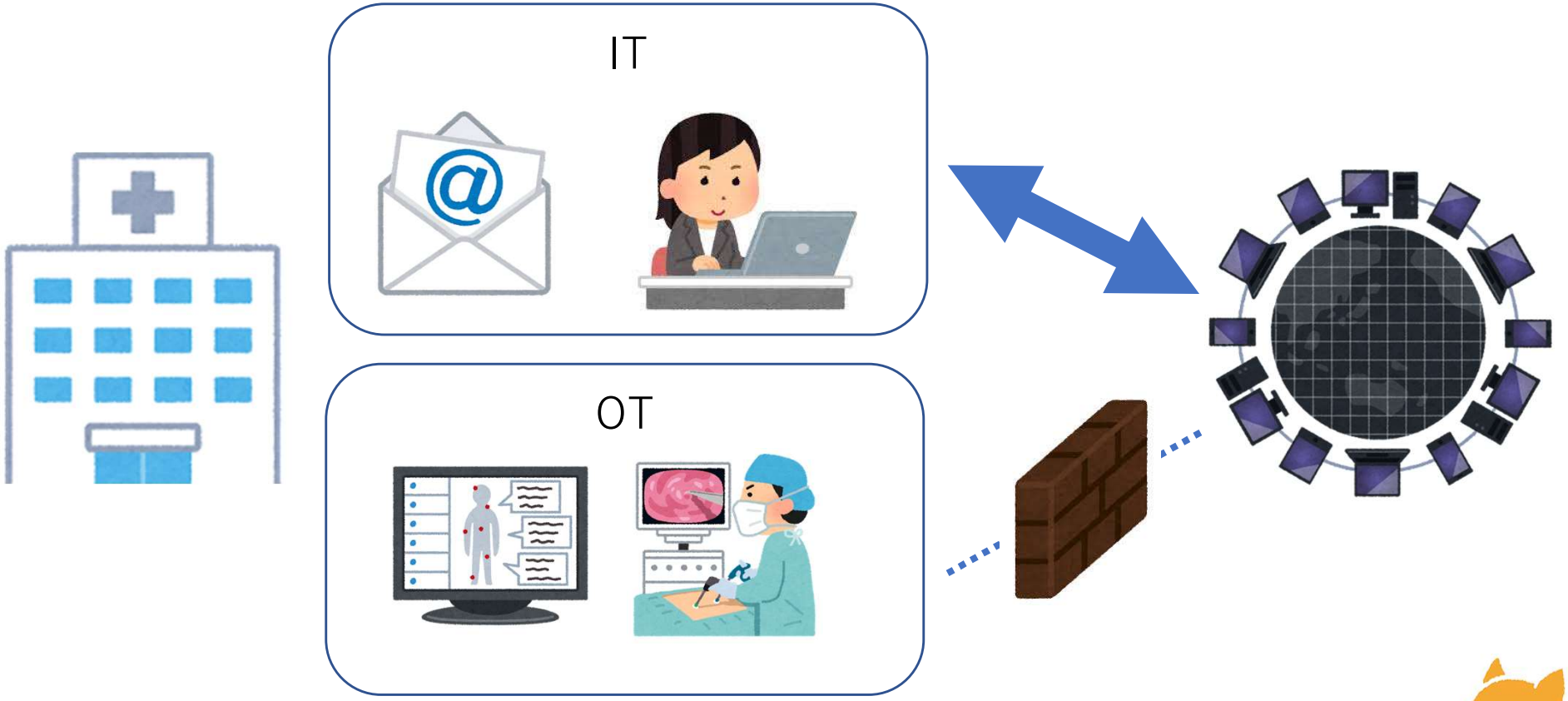


様々ポジショントークはあるものの・・・
「医療機関はヤバイ!」はおおむね共通認識

■オペレーション維持の使命感が強い
■PHIが高価格で売れる
■研究情報を狙う動きも
■セキュリティが脆弱（という一般認識）

出典：Checkpoint Software Technology

エアギャップとは



■エアギャップ＝閉域網＝孤立系
■00年代の電カル普及時に厚労省が推進
■Sierも厚労省の方針に追随

エアギャップの落とし穴

エアギャップ自体は強力な防御手段ではあるものの・・・

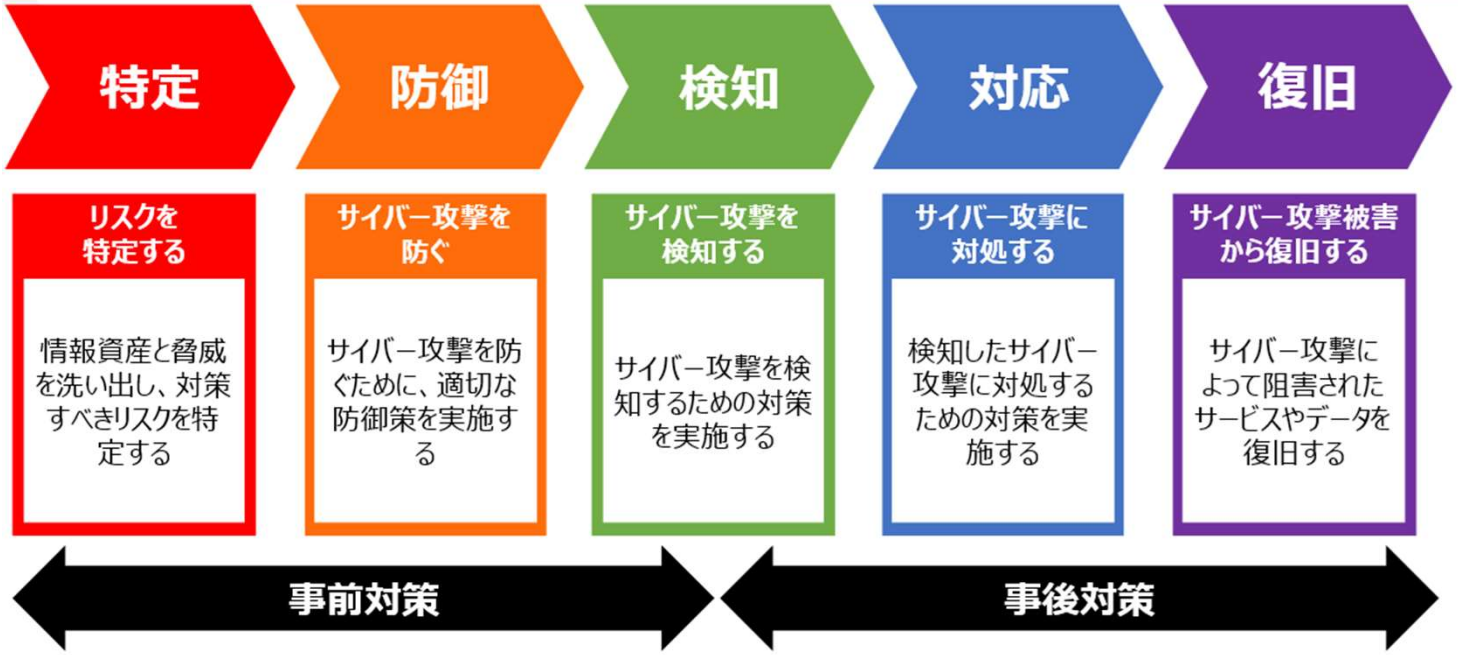
■ネットワーク構成図が更新されない
■保守回線の存在
■Sierやメーカーとの責任分界点が曖昧
■内部の防衛が疎かになりがち
■組織内のセキュリティ人材の育成が進まない

半田病院と大阪急性期の共通点

◆VPNの脆弱性が侵入口に

◆内部はパスワードの共通化やアンチウイルスの無効化などぼろぼろの状態に

境界防御からレジリエンスへ



出典：Sonic Wall

■2014年に米NISTがサイバーセキュリティフレームワーク（CSF）で事後対策の重要性を強調

■コロナ禍で境界がそもそも曖昧に

■医療DX（医療情報PF、電カル標準化、診療報酬改定DX）

CSF対応は一部で必須要件に

- 自動車業界のガイドラインがCSFに対応
- 防衛装備庁の調達基準はCSF準拠に
- ZホールディングスやNECは供給網にCSF対応を要請

セキュリティを
“買う”だけではなく
“運用する”ことが必要に

CSFに沿った組織体制

■大手
SOC＝監視部隊
CSIRT＝インシデント対応部隊
PSIRT＝製品のアフターマーケットの安全管理部隊
等々・・・

■中堅以下
MSS＝セキュリティ運営の外部委託
vCISO＝情報セキュリティ責任者の委託
などが現実解に

NIKKEI

CSF対応ここまでやれる？

◎3000人／200億円企業のとある電機メーカーの“好事例”

AV(Anti Virus)

FW(Fire Wall)

Mail Security

MXDR(Management Extended Detection & Response)

IAM(Identity & Access Management)

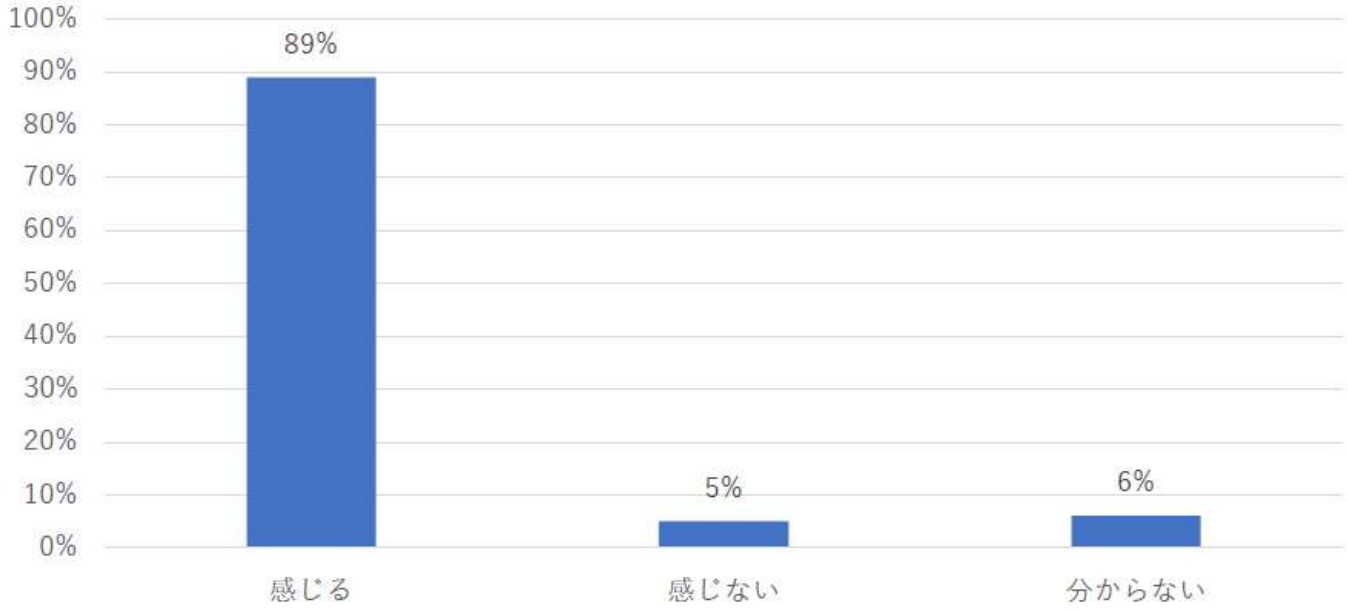
ASM(Attack Surface Management)

VM (Vulnerability Management)

年間計約1億7千万円也!!

医療機関のセキュリティの現状

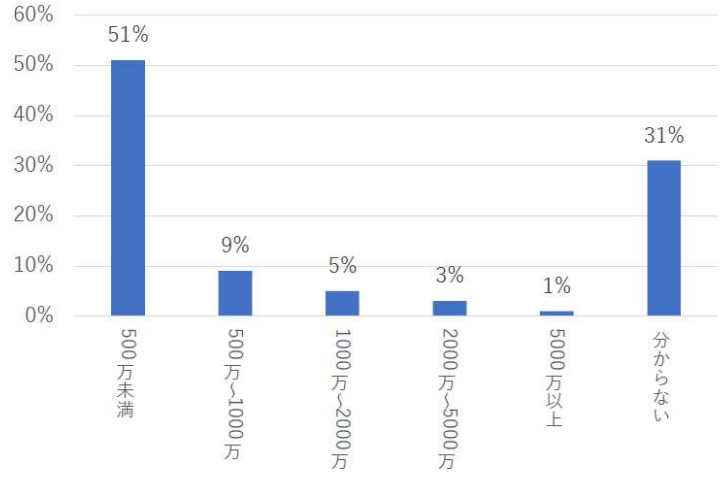
＜サイバー脅威への感度＞



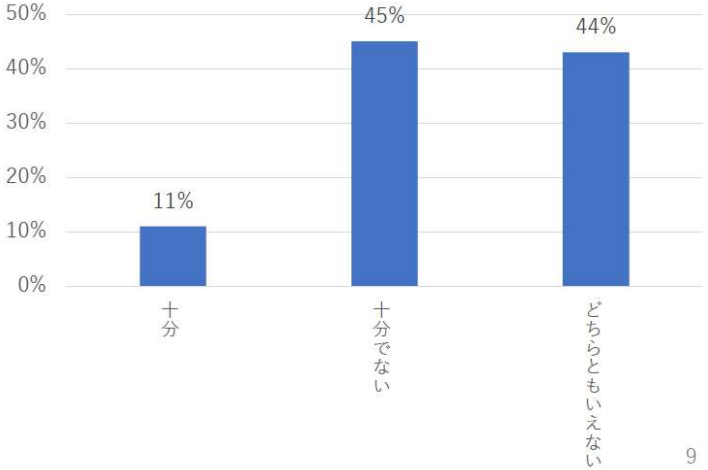
出典：医療ISAC

医療機関のセキュリティの現状

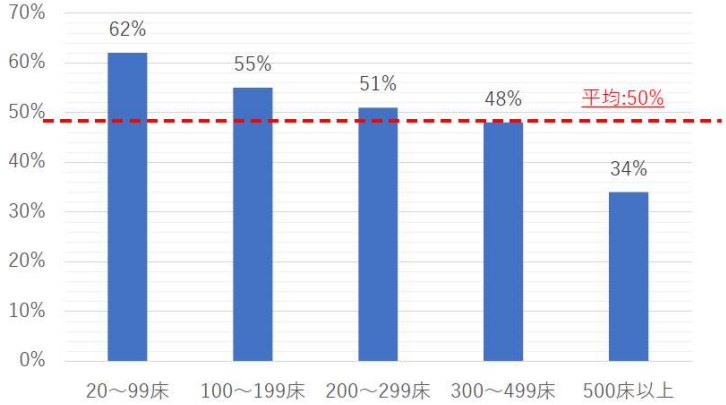
＜年間セキュリティ予算＞



＜セキュリティ予算を十分と感じているか＞



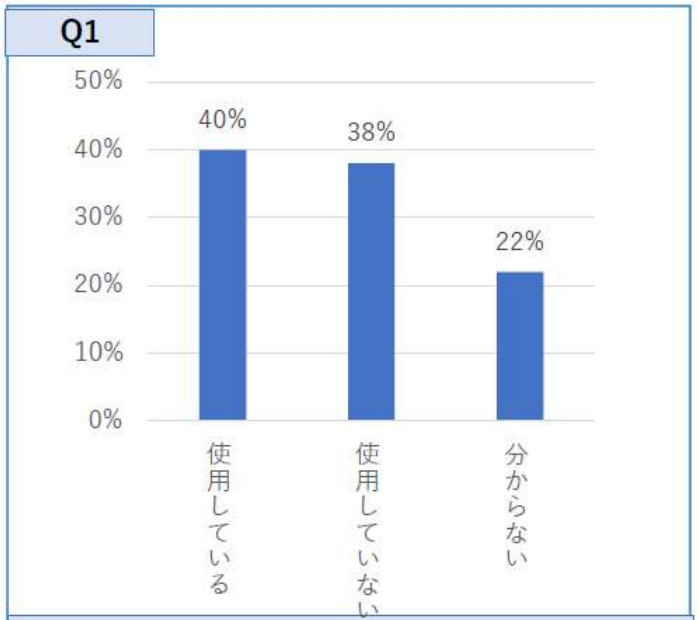
＜年間セキュリティ予算を「500万未満」と回答した病院の病床規模別割合＞



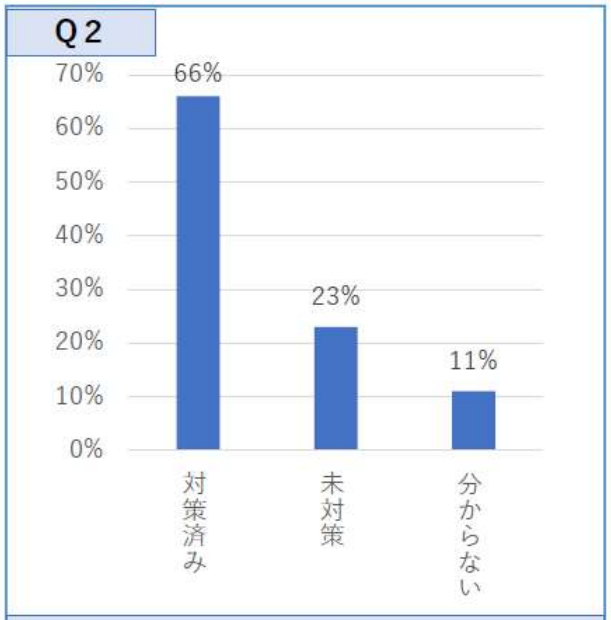
診療報酬改定でセキュリティ要件は加わったが、マイナス査定要件・・・

出典：医療ISAC

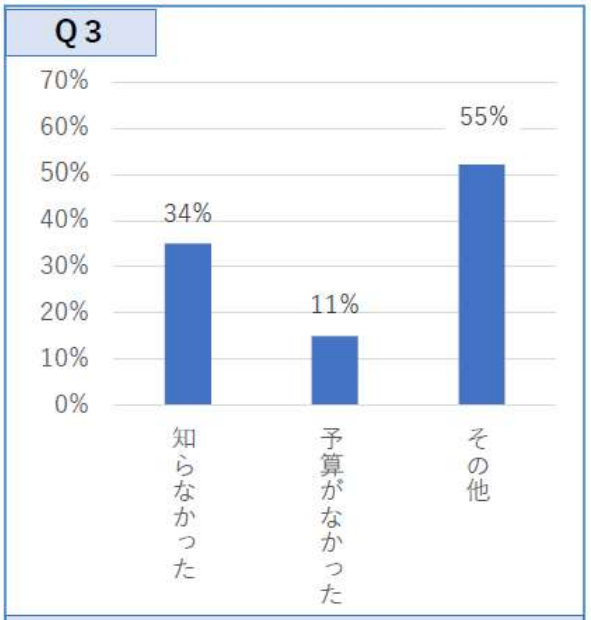
医療機関のセキュリティの現状



脆弱性指摘のあったVPN使用状況



Q1で「使用している」場合の脆弱性対応状況



Q2で「未対応」とした場合の理由

出典：医療ISAC

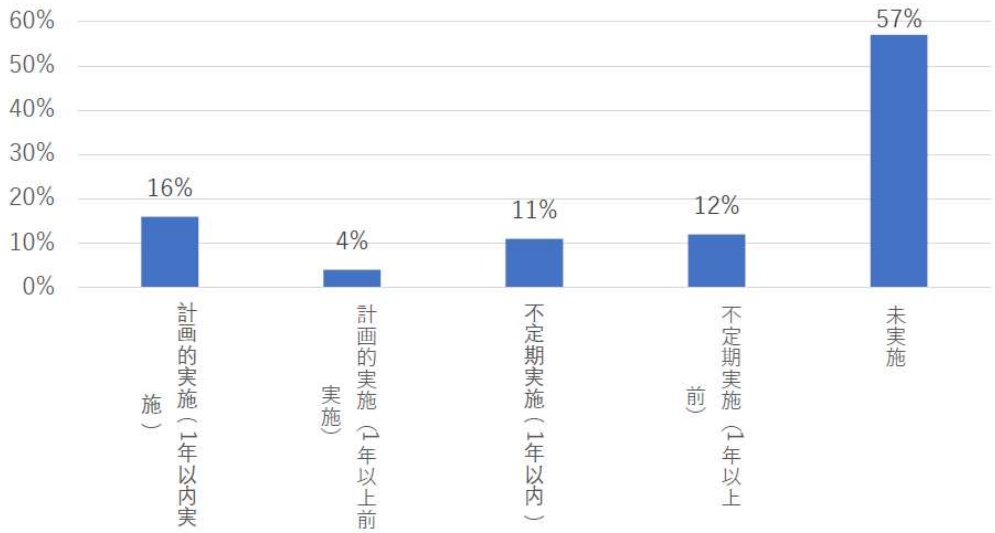
半田病院の教訓は生かされず・・・

医療機関のセキュリティの現状

＜院内システム担当者数/常勤者数＞

全体平均	
院内システム担当者数	2.9人
うち、常勤者数	2.6人

＜セキュリティ監査実施状況＞



出典：医療ISAC

やりっぱなしのセキュリティ・・・

ステップを踏んで徐々に強化を

■Step1:自社のリスク評価
- ネットに露出しているIT資産の確認
- 外部への相談体制の構築

■Step2:教育とルール整備
- 院内研修、標的型メール訓練
- セキュリティ関連の規定整備

■Step3:技術対策①ツールの導入
- AV、ゲートウェイの監視、メールセキュリティなど境界防御の整備
- 脆弱性の診断、対応ツールの導入
- サイバー保険

■Step4:技術対策②ツールの運用
- 端末の監視体制の構築
- 脅威インテリジェンス
- データのバックアップ体制（復旧訓練も大事!!）

セキュリティの共助

そうはいっても・・・・

プロジェクトを推進できる人が社内にいない！

セキュリティ企業の言うがままでコストばっかりかからない？

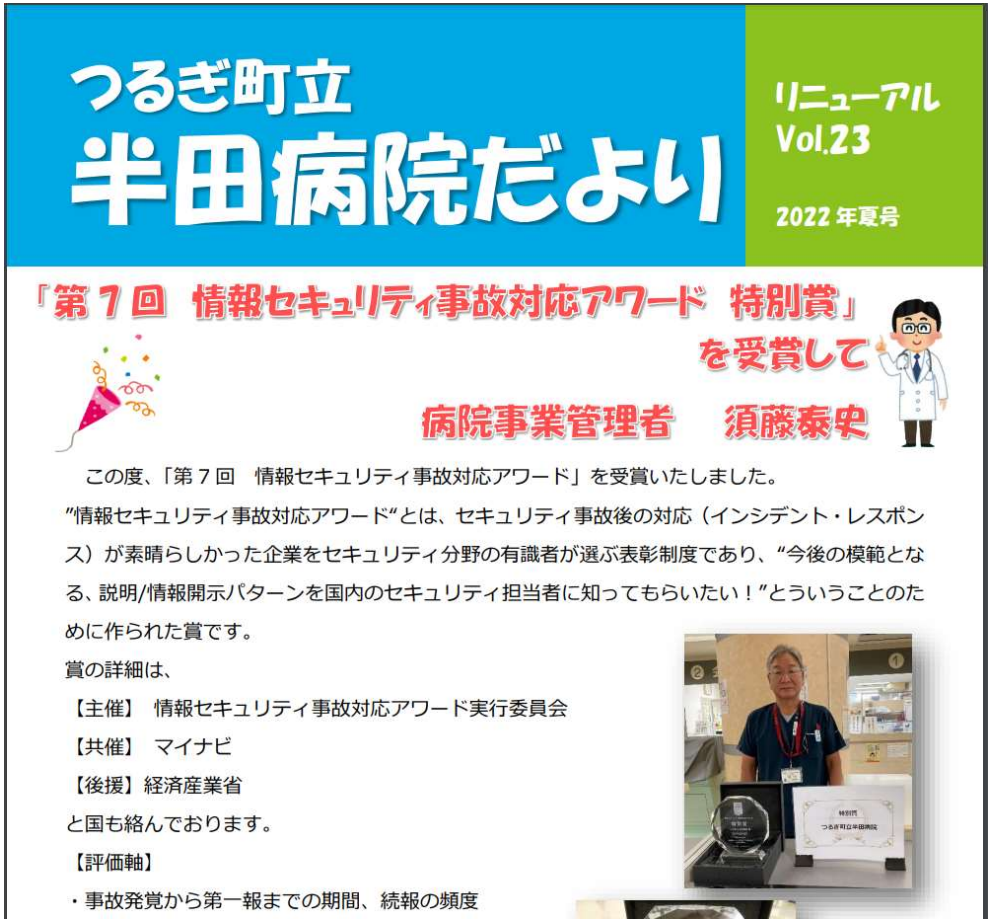
共助の文化をフル活用しましょう

■医療ISAC

■経産省の地域SECUNITY

ノウハウ共有、相談体制、机上演習、人材育成、共同SOC、共同購買
etc・・・

医療機関の強みも忘れずに！



つるぎ町立
半田病院だより

リニューアル
Vol.23

2022年夏号

「第７回　情報セキュリティ事故対応アワード　特別賞」を受賞して

病院事業管理者　須藤泰史

この度、「第７回　情報セキュリティ事故対応アワード」を受賞いたしました。

”情報セキュリティ事故対応アワード“とは、セキュリティ事故後の対応（インシデント・レスポンス）が素晴らしかった企業をセキュリティ分野の有識者が選ぶ表彰制度であり、“今後の模範となる、説明/情報開示パターンを国内のセキュリティ担当者に知ってもらいたい！”とういうことのために作られた賞です。

賞の詳細は、

【主催】　情報セキュリティ事故対応アワード実行委員会

【共催】　マイナビ

【後援】経済産業省

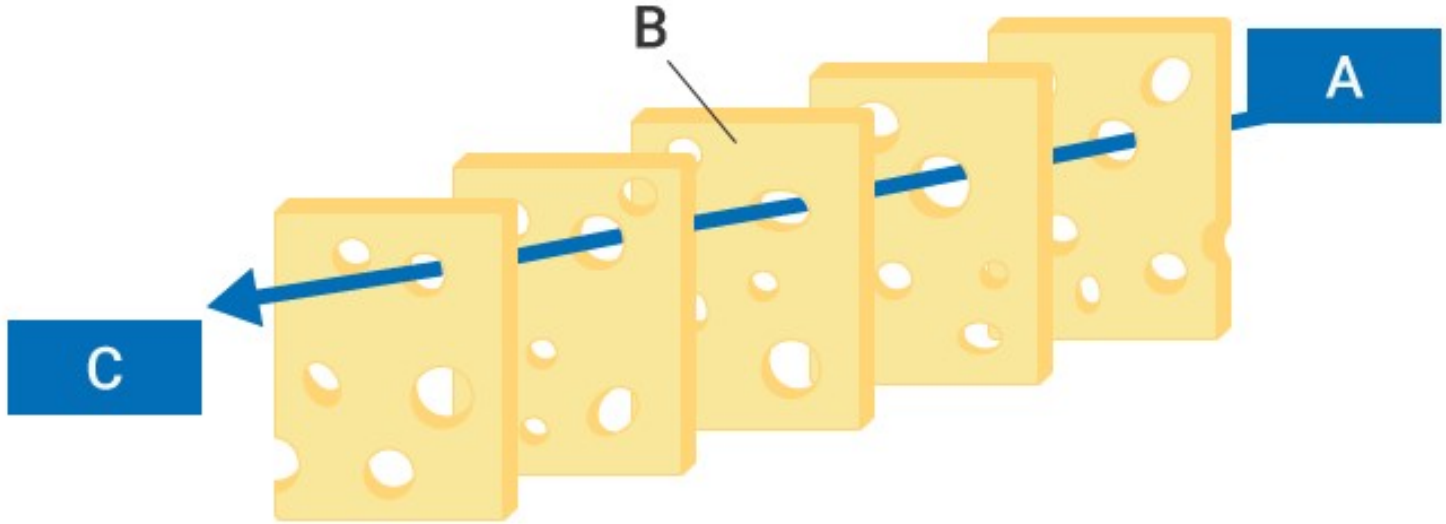
と国も絡んでおります。

【評価軸】

・事故発覚から第一報までの期間、続報の頻度

発覚後すぐに災害用BCPに準拠して対応！

医療機関の強みも忘れずに！



■事故対応の肝は原因事象よりも結果事象

■ダメージコントロールの判断ができることが重要

■ITのセキュリティは「チーズの一枚」に過ぎない

■地域の医療網という強力なセーフティネットの存在

「患者の健康さえ確保できれば病院の勝ちである!!」

NIKKEI

御清聴ありがとうございました