2024年8月27日

配布資料

経営陣が知っておくべきサイバー犯罪の脅威

サイバーハザード2024

WEB110　吉川誠司

プロフィール

目次

01

情報セキュリティ脅威の概要

2023 年に発生したセキュリティ事故や攻撃の
状況等からの評価

脅威の概要

情報セキュリティ10大脅威

情報セキュリティ専門家を中心に構成する「10大脅威選考会」の協力により、2023年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票により順位付けして解説した資料。

「組織」向けの脅威の順位

順位	脅威の内容	順位	脅威の内容
1位	ランサムウェアによる被害	6位	不注意による情報漏えい等の被害
2位	サプライチェーンの弱点を悪用した攻撃	7位	脆弱性対策情報の公開に伴う悪用増加
3位	内部不正による情報漏えい等の被害	8位	ビジネスメール詐欺による金銭被害
4位	標的型攻撃による機密情報の窃取	9位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	10位	犯罪のビジネス化（アンダーグラウンドサービス）

ランサムウェアとは

最近の特徴

1.データを暗号化し復元と引換えに
　金銭を要求する
2.窃取した情報を公開すると脅す
3.DDoS攻撃を仕掛けると脅す

二重の脅迫が主流となっている。

日本国内の被害件数

2023年中のデータ

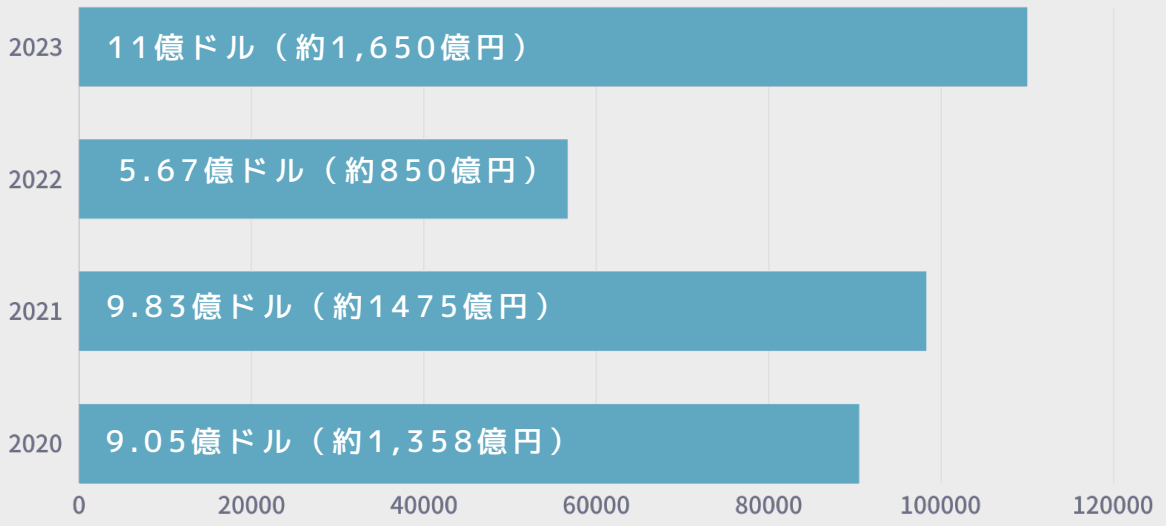
197 件

内、企業が公表したランサムウエア被害数は70件で過去最多

出典：警察庁　令和5年におけるサイバー空間をめぐる脅威の情勢等について

2023年の支払総額は過去最高

ランサムウェア攻撃による年間総支払額の推移 by Chainalysis　　単位：10000ドル



支払われた身代金の最高額

2024年8月時点のデータ

1位
7,500万ドル
約112億円
米国の自動車ディーラー向けSaaSプロバイダーCDK Global

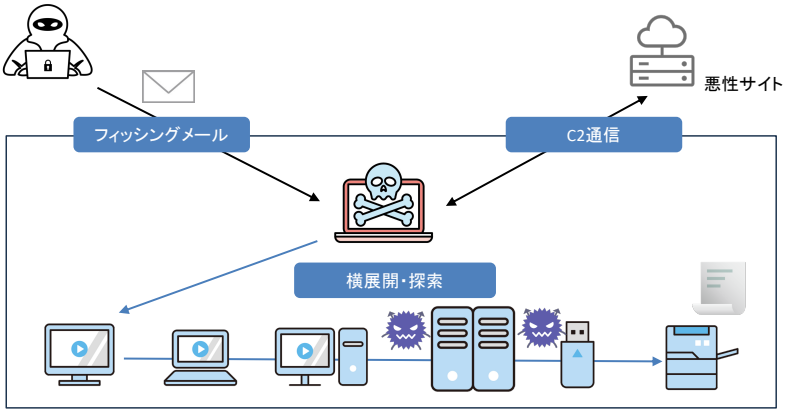
2位
4,000万ドル
約60億円
米国の保険大手CNA Financial

3位
2,200万ドル
約33億円
米国のヘルスケア企業Change Healthcare

コロナで変化した手口

コロナ前の侵入方法

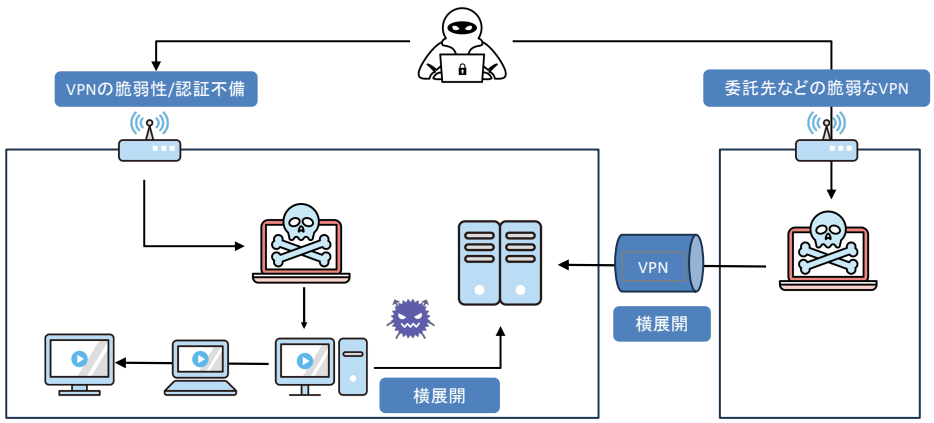
メールの添付ファイルやURLリンク経由で侵入し感染させる手口が主流



コロナで変化した手口

コロナ後の侵入方法

テレワーク等に利用されるVPN機器等の脆弱性や強度の弱い認証情報等を利用して侵入する手口が8割



02

ランサムウェア被害の実例

被害の発覚から復旧までの道のり

日本での主な被害実例

徳島県の半田病院がランサムウェアに感染（2020年10月）

感染による影響

システムへの影響

- 電子カルテの端末や関連するサーバーのデータが暗号化
- ネットワークの遮断や端末の停止
- 自動受付機や自動精算機も使用不能

業務への影響

- 電子カルテが参照できないため過去の検査結果や病歴が分からない
- 予約票が参照できないためいつ誰が来るのか分からない
- 救急や新規患者の受け入れを中止し、手術も可能な限り延期にするなど病院としての機能は事実上停止

初期対応

半田病院のBCP基本方針

POINT 01 今いる入院患者の保護

POINT 02 外来患者は予約患者のみ

POINT 03 電子カルテ復旧に努める

POINT 04 皆で助け合って乗り切ろう！

初期対応

災害対策本部の設置

STEP 01
10月31日に電子カルテの復旧が難しいとの報告をうけた当直医が救急受け入れの不可も判断し関係各位に連絡

STEP 02
同日10時に災害対策本部を設置、BCPに基づく対応を行った

STEP 03
同日午前８時過ぎに病院幹部職員も参集し、災害相当と判断

初期対応

身代金は支払わないことにした

Reasons 01
データが完全に復旧する保証はないこと

Reasons 02
犯人側への資金提供を行うことが自治体の姿勢として理解を得られないこと

Reasons 03
昨今の脅威とも言われる「二重脅迫」といったランサムウェア特有の攻撃者の行動は見受けられなかったこと

初期対応

情報公開

STEP 01
インシデント発生当日に記者会見を行い、病院としての説明や現状を迅速に公表

STEP 02
病院の方針を決定した令和 3 年 11 月 29 日にも記者会見を開催

ココが、ポイント!
一般的にインシデント情報は隠す傾向があるが、国内外を含みメディアからの取材にはできる限り対応し、他病院や事業所が同様の被害にあわないよう、積極的に情報公開と提供を行った。

調査結果

初期侵入経路

Reasons 01 Fortinet 社製のVPN装置は導入当初からソフトの更新が行われておらず、2021年の夏に日本国内でも話題になった「CVE-2018-13379」が放置された状態だった。

Reasons 02 VPN 装置管理者の資格情報がダークウェブで公開されていた

これらの事実を鑑みると電子カルテを始めとした医療機器のメンテナンス等を行う際に接続する VPNが唯一の侵入経路と考えられる。

調査結果

内部侵入

POINT 01 今回のFF レポートからは多くの PC やサーバーの攻撃の相関関係をつかむことができず、攻撃の全体像を解明することはできなかった。

POINT 02 インシデント発覚時刻前後に7台の端末へログオンされていたことが確認されている。その端末でリモート操作ツールが実行された痕跡があり、Windows の資格情報を窃取するためのツールである「Mimikatz」が混入している可能性がある。

POINT 03 ADサーバへのログオンが成功していることから、病院内の環境情報などが盗み見られ、全てのネットワークやシステム、端末にアクセスできた可能性は高く、情報が盗み見または漏洩した可能性は否定できない。

調査結果

水平展開

ログオンに成功している端末 9 台
データの暗号化が確認されている端末 15 台
そのいずれも確認されている端末 16 台
合計 40 台
の端末が今回の攻撃による被害や影響を受けている。

技術的問題点

1.Active Directoryの設定不備

パスワードポリシーの不備

パスワードの最小桁数が5桁に設定されていた。

ロックアウトポリシーの不備

短いパスワードであってもロックアウト設定を行っていれば総当たり攻撃は防げた。

技術的問題点

2.脆弱性の把握と管理

VPN 装置の脆弱性管理を実施していなかった

病院情報システム、検査機器等のリモート保守のために設置された Fortine社の VPN 装置 FortiGate 60E の脆弱性が放置されていた。

2021 年 9 月に同脆弱性を悪用し全世界で 87,000 台の ID、パスワードが公開されたが、その漏洩データに半田病院のID、パスワードが含まれていた。

技術的問題点

2.脆弱性の把握と管理

電子カルテシステム・医事会計システムの動作が不安定になるという理由から脆弱性管理とウイルス対策を実施していなかった

グループポリシーによってWindowsアップデートを実施しない設定となっており、 Windows 10のすべての脆弱性がコンピュータに存在した。

グループポリシーによって、Windows Defenderの動作が無効となっており、既知のマルウェアに対して防御力がなかった。

組織的な問題点　1.サイバー攻撃リスク管理

リスク認識の欠如

半田病院では災害拠点病院としての事業継続計画が策定され訓練も実施されていたが、サイバー攻撃による事業継続リスクが存在するという認識が欠如していた。

組織的な問題点　2.必要なリソースの確保

圧倒的なリソース不足

半田病院の場合、管理責任は院内の 1 人の情報システム責任者に委ねられ、その個人の知見とその業務範囲内で認識するに留まり、サイバー攻撃リスクより医療情報システムの利便性に注がれている状況にあった。

情報セキュリティの重要性を有す管理者や専門知識を有したエンジニア、セキュリティ対策を施した基幹システムの調達などがなされていなかった。

組織的な問題点

3.マネジメントシステムの整備

ISMS

インシデント発生当時、半田病院にはISMSは存在していなかった。つまり情報システムを取り巻く環境の変化やそれにともなう新たな事業継続リスクに関する情報を組織として入手する仕組みがなかった。

BCMS

半田病院は災害拠点病院としての事業継続計画が策定され訓練も実施されていることもあり、DMATの支援も功を奏したことで最低限の事業継続ともに監督機関である行政機関や社会への説明・公表も実施されている。また報告書により、原因の追求、善後策を講ずる責任も果たされている。

ベンダーの問題点

適切なセキュリティ対策の欠如

電子カルテシステムを導入している時点で、システムの正常動作を優先するあまり、セキュリティレベルを下げる指示や対応が行われていた

さらに納入システムが閉域網であることを理由に極めて初歩的なセキュリティ対策を継続的に怠った。

半田病院としてはウイルス対策ソフトを導入していたが、電子カルテシステムの導入時に不具合が生じたため同セキュリティ対策ソフトは動作させていなかった。

データの復旧

POINT 01

2018年までにオフラインで保管していたバックアップデータについては Lockbit2.0 の影響を受けなかったため復旧することができた。

POINT 02

それ以降は暗号化されたが、データ復旧を請け負った会社が何らかの方法で修復に必要な手段を入手しデータの復元を行った可能性がある。

03

実例からの学び

BCP対策における情報セキュリティの考え方

事例からの学び

POINT 01

データの完全性の問題

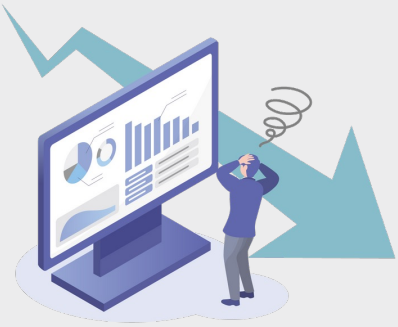
- 身代金を払ってデータを復元できたとしてもそのデータの完全性の担保はできない。
- 復元のために「身代金を支払うことは合理的でない」という判断の一つの根拠と言える。
- 復元した DB での業務は、完全性欠如の可能性に留意しながら進めることが肝要。

事例からの学び

POINT 02

被害額の想定は困難

身代金の支払いやデータ復旧費用…
業務中断による収入減…
システム再構築費用…
風評被害など…多岐にわたる。
これらをすべて数値化し、
一つの金額として提示することは困難。



事例からの学び

POINT 03 セキュリティの観点も含めて委託先を選定する

- システム導入時に、セキュリティ面や保守の責任範囲まで考慮した契約になっていない…
- 委託先がサイバー攻撃を受けることで自社の脅威となることもある…

発注者側がある程度のセキュリティ知識を持ち、高いセキュリティレベルを持つシステムを扱う事業者にインセンティブが発生するように会社選定が行われる必要がある

事例からの学び

POINT 04 ランサム対策で実施すべき３つのポイント

3-2-1ルールに準ずるバックアップ体制

データを3つコピーし、２つの異なる媒体に保存し、1つを別の場所で保管するバックアップの実施

検知機能の向上

EDRやUTMなどの監視体制の構築

VPN機器等の適切な管理

- VPNの機器の洗い出し
- ファームウェアなどの修正プログラムの適用
- VPNアカウントの多要素認証化
- 接続できるMACアドレスを限定

04

まとめ

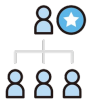
組織の経営者層として必要な行動

組織の経営者層として必要な行動

POINT 01

専門知識を有するCISOの配置

※ CISO（Chief Information Security Officer）＝最高情報セキュリティ責任者



POINT 02

組織としてのサイバー攻撃対応体制の確立

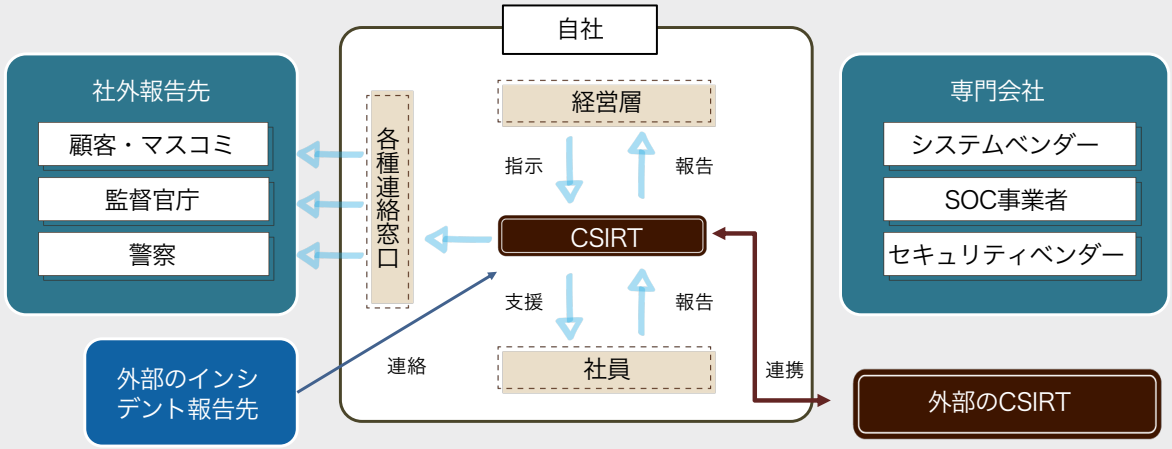
※CSIRTの設置が難しい場合は緊急連絡網だけでも整備しておく

POINT 03

対策予算の確保と継続的な対策の実施

組織の経営者層として必要な行動

CSIRTの概念図



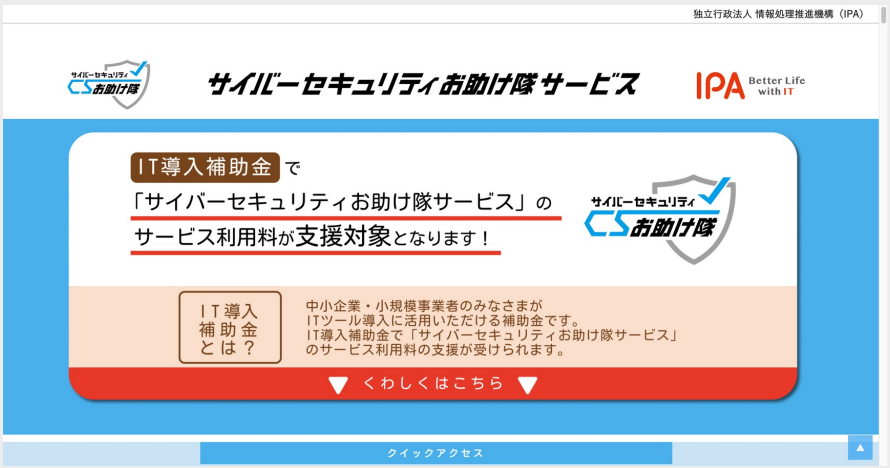
組織の経営者層として必要な行動

基本的なセキュリティ対策の実施

攻撃手法	基本的対策
ソフトウェアの脆弱性	ソフトウェアの更新、セキュリティパッチの適用
マルウェア感染	セキュリティソフトの導入
パスワードの乗っ取り	多重認証の利用、パスワードポリシーの強化
設定不備	設定の見直し（不要なサービスやアカウント）
誘導（ソーシャルエンジニアリング）	手口の教育

組織の経営者層として必要な行動

サイバーセキュリティお助け隊サービスの活用



初年度導入費用10万円～60万円程度でネットワーク監視と端末監視が可能

組織の経営者層として必要な行動

万が一に備えてサイバー保険

サイバー保険で補償されるのは３種類

1. 第三者への賠償責任
2. 自社の復旧費用
3. 事業の中断による逸失利益

ランサムウエアの被害によって支払った身代金は補償対象にならない。

サイバー保険とは | サイバー保険 | 日本損害保険協会
https://www.sonpo.or.jp/cyber-hoken/about/