DX推進の下支えとなるシンプルなセキュリティ対策

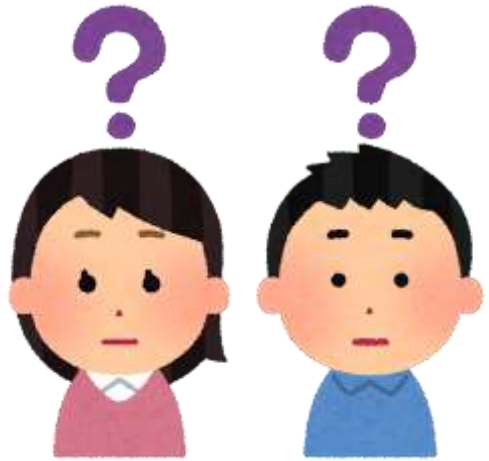
～事故事例から学べば怖くない！？～

杉浦　一洋
セールスエンジニアリング本部 副本部長 兼シニアセールスエンジニア
情報処理安全確保支援士（登録番号 第022881号）

SOPHOS

皆さまに質問です

なぜ、サイバーセキュリティ対策をするのですか？



なぜ、サイバーセキュリティ対策をするのか

スタッフを護るため	従業員の健康管理と同様、通常業務において危険な状態にならないようにするため
会社・組織を護るため	危険予知（KY）活動と同じ、危険に遭わないようにし、常に無事故であれば安心して事業継続できる
儲かるため	利益を出すための活動の中で、必ずリスクが発生しますが、利益とリスクによる損失の引き算でにプラスになるようにするため

どの立場でも対策することに理由があります

サイバーセキュリティの立ち位置

こんなことはしないですよね

- 沼地に家や病院を建てますか
- 屋根も囲いもないところに診察室を作りますか
- 金庫が置いてある部屋に鍵をつけず、誰でも入れるようにしますか

業務を安心して遂行できるための縁の下の力持ち

- 家や病院を建てるときの基礎
- 病院を作るときの屋根、床、壁
- 目立たない存在

安心してITを利用できるようにするための基礎

医療関係で発生したサイバー攻撃（公開情報より）

医療関係で発生したサイバー攻撃（2021年以降）

医療機関	攻撃内容	被害状況	被害時期
市立東大阪医療センター	ランサムウェア	医用画像参照システムのサーバがダウン	2021年5月31日
つるぎ町立半田病院	ランサムウェア（LockBit）	電子カルテが利用不可 新規、救急などの受け入れ停止	2021年10月31日
春日井リハビリテーション病院	ランサムウェア	電子カルテが利用不可	2022年1月12日
社会医療法人大雄会	Emotet	メールアドレス情報が流出	2022年2月8日
医療法人健昌会	Emotet	特になし（ウイルス感染のみ）	2022年3月7日
名古屋大学医学部附属病院	外部からの大量の ログイン試行	個人情報が第三者に閲覧される	2021年3月～9月
東京都済生会向島病院	Emotet	不審メールの送信	2022年4月
秋田赤十字病院	Emotet	不審メールの送信	2022年5月
医療法人ラポール会青山病院	不正アクセス	非公表	2022年4月23日
鳴門山上病院	ランサムウェア（LockBit）	電子カルテ、院内LANシステムが使用不可	2022年6月19日
田沢病院	ランサムウェア	電子カルテが使用不可	2022年10月27日
大阪急性期・総合医療センター	ランサムウェア	電子カルテが利用不可 緊急以外の手術や外来診療の一時停止	2022年10月31日
金沢西病院	ランサムウェア	電子カルテの一部が閲覧不可	2022年12月3日
社会福祉法人あじろぎ会宇治病院	ランサムウェア	個人情報の一部暗号化	2023年1月6日
中津市立中津市民病院	ランサムウェア	財務会計システムの異常	2023年11月13日

（公開情報より）

なぜ、被害に遭ったのか
非常にシンプルな原因

なぜ、被害に遭ってしまったのか

被害に遭った病院は
オフライン環境
（公開された情報より）

→

コンピュータウイルスは
自然界のウイルスとは異
なり、自然発生はしない

→

なぜ、被害に遭うのか？

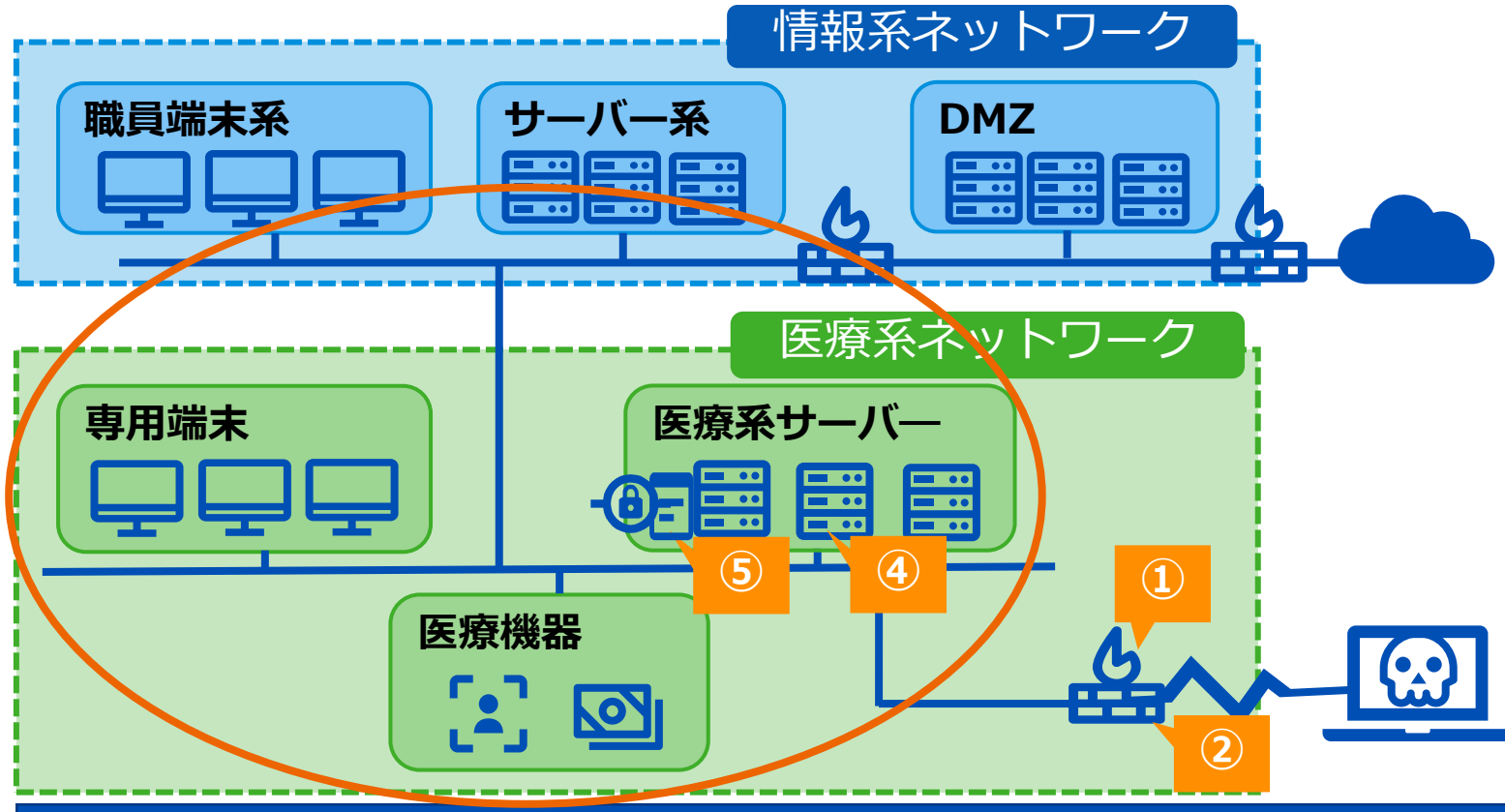
公開された情報を見ると・・・

医療機関	侵入の原因
市立東大阪医療センター	**外部からの不正アクセス**
つるぎ町立半田病院	**VPN機器の脆弱性**
大阪急性期・ 総合医療センター	**給食提供サービス会社のシステムで利用していた VPN機器の脆弱性**

→ **完全なオフライン環境ではない**

“端末がインターネットに接続していない＝オフライン”と誤認識

報道内容から想定される
ランサムウェア被害の侵入経路



攻撃の流れ
①VPN装置の脆弱性を攻撃し、アカウント情報を窃取
②攻撃者が窃取したアカウント情報を使用してログイン
③攻撃者が外部からシステム内部を探索
④サーバーにログイン
⑤ランサムウェア攻撃

VPN装置の脆弱性を突いた攻撃は日本特有の被害事例の話も

被害事例における簡単に侵入を許した原因

原因	内容	喩えてるとこういうこと
リモートアクセスVPNのユーザーとパスワードが簡単	誰もが簡単に試せるユーザー名とパスワードでログインが可能 例： ユーザー: user パスワード：password	ダイヤル錠で鍵をかけたが、開錠キーが“1111”など誰でも簡単に試せる番号で設定
Windowsサーバーの管理者のパスワードが簡単	Administratorのパスワードが簡単 例：AdministratorのパスワードがPassword	キャッシュカードの暗証番号が生年月日や電話番号など他人に簡単に見破れそうなものを利用
リモートデスクトップが有効	リモートデスクトップ接続を有効、かつWindowsサーバーのAdministratorのパスワードが簡単	遠隔操作が簡単にできる
全システムのパスワードが同一	全てのシステムのパスワードが同じで簡単なもので設定	マイナンバーカードやキャッシュカードの暗証番号がすべて同じ
セキュリティパッチ未適用	世の中に知られている脆弱性に対応をしていない	世の中に知られている攻撃を止める方法を実施せずに放置

被害に遭った原因は防げる事故ばかりの可能性が高い

どうすれば良いのか
シンプルに考える

誰も守ってくれない

- 事故になった時に名前が出てくるのは病院名や組織でベンダーではない
  - 名前が大きく出てくるのは被害に遭った病院と攻撃名称
  - やり玉に挙げやすいことだけが先に報道される理不尽（人間不信になる）

- 「できない理由」を並べても、事故が起きた時に言い訳にならない
  - ベンダーがパッチ適用を認めないので、対策できませんでした
  - ベンダーに丸投げしていたので、自分たちは何も知りません

- 組織（自分）を守るためにも、責任範囲を明確に
  - 被らなくてもいい責任を被らないようにすべて書面化しておく
  - 小さな契約でもよいので相談先を常に持っておく

医療情報システムの安全管理に関するガイドライン第6.0版を
この目線で見ると理解が深まることも

サイバー攻撃被害に遭わないために

対策	内容
各自が意識する	システム担当者以外の方は特に、普段の任務において意識をしていれば早々に被害に遭うことはありません **不審な点があれば、担当者に速やかに報告する**
誰が担当しているのかを明確に	事故原因の背景として“「誰が担当しているのか」が明確でなかった”というのがあります これを明確にすることで事故の発生率を低減できます
攻撃を防ぐ仕組みを導入する	サイバーセキュリティ対策ソリューションを導入し、攻撃が来ても未然に防げるようにする （喩えるなら、泥棒が侵入しないように施錠すること）

被害事例の原因から見たシンプルな対策

侵入（被害）原因	どうすれば防げたか	対策
脆弱性対応以前にVPN機器が攻撃され、アカウント情報が窃取された	機器の定期保守 リモートアクセスVPNのユーザー管理	最新バージョンの利用 ユーザー管理と多要素認証
サーバーのアカウント情報が窃取され、ログインされた	修正パッチの適用 パスワードの強化	定期的なパッチ適用 パスワードの見直し
攻撃を阻止する機能が利用されていなかった	最新のエンドポイント対策製品がもつ機能のフル活用	最新のエンドポイント対策製品の導入と最新機能の利用

医療情報システムの安全管理に関するガイドライン

医療情報システムの安全管理に関するガイドライン

- ガイドラインがあるとありがたいこと
  - 守りたいものがあり、それをどうやって守るか、その指針と方法をしかるべきところが示されているので、１から考える必要がない
  - 「ガイドラインに沿った対策をしていました」と言い切れる

- 書いてあることを平たく言うと・・・
  - 医療情報システムの管理・運用体制を整えること
  - リスク分析をしてリスクが何かを明らかにし、安全管理対策を講じること
  - インシデント発生時の対応ができる体制にすること
- サイバーセキュリティ対策は安全管理を実現するための技術の１つ

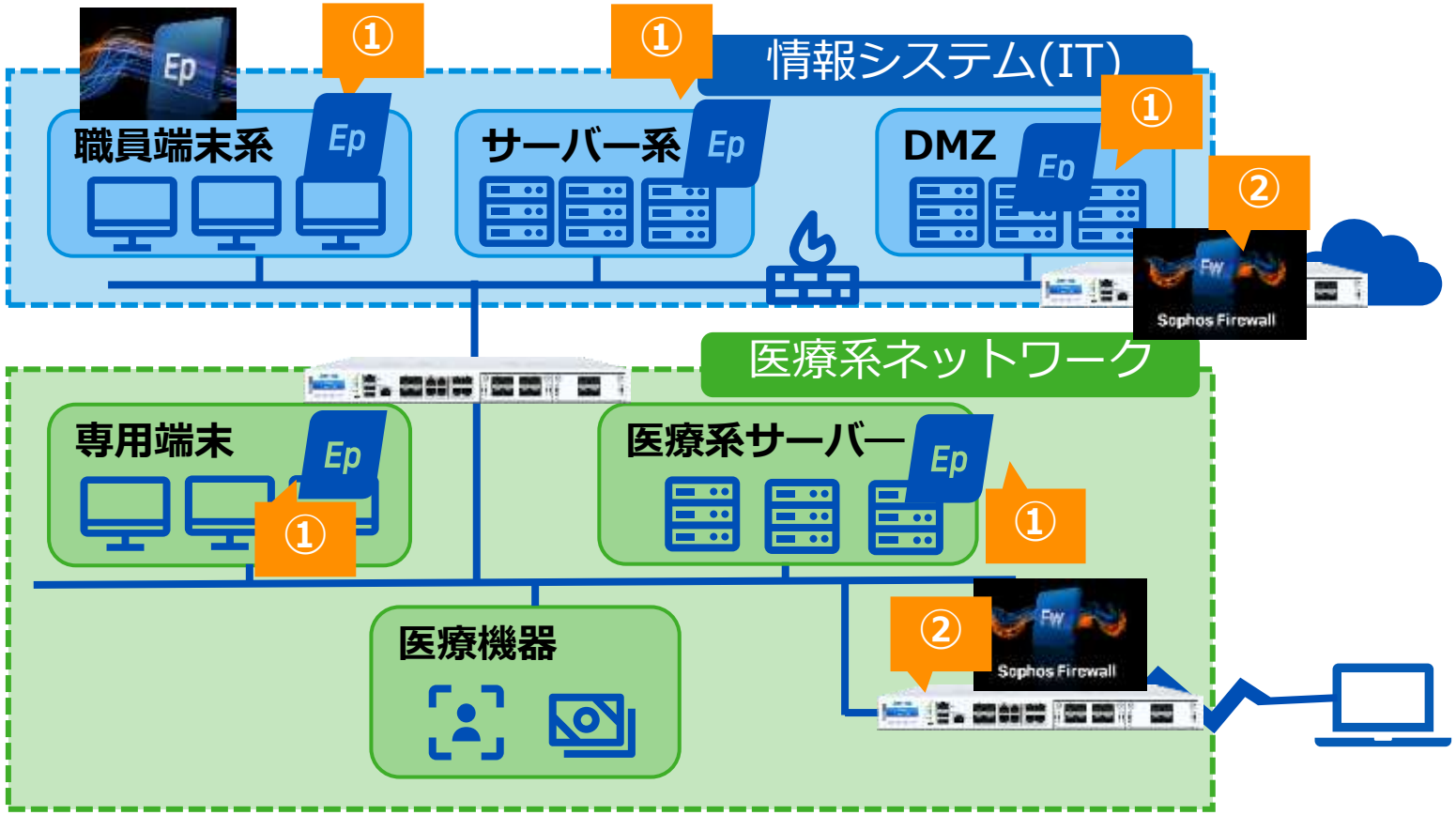
組織や自分自身を守るために説明できる状態にすること

被害事例と第6.0版との関係を読み解くと

侵入（被害）原因	対策	第6.0版システム運用編
脆弱性対応以前に攻撃され、すでにアカウント情報が窃取された	最新バージョンの利用 ユーザー管理と多要素認証	８．利用機器・サービスに対する安全管理措置 １０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置 １４．認証・認可に関する安全管理措置
サーバーのアカウント情報が窃取され、ログインされた	定期的なパッチ適用 パスワードの見直し 権限管理	８．利用機器・サービスに対する安全管理措置 １４．認証・認可に関する安全管理措置
攻撃を阻止する機能が利用されていなかった	最新のエンドポイント対策製品の導入と最新機能の利用	８．利用機器・サービスに対する安全管理措置 ８．１ 不正ソフトウェア対策

ソフォスだったらどう護るか

ソフォスのサイバーセキュリティ対策ソリューション



ソフォスのソリューション
①サーバーや端末にソフォスのエンドポイント製品の導入
②Sophos Firewallによる保護

＋

脅威の兆候を発見する仕組み
③サーバーや端末にEDR/XDR機能を追加
④ EDR/XDRで検知した脅威を24時間365日対応

SOPHOS

まとめ

オフラインではない	物理的に外部からの接続口がゼロではない限り、オフラインではありません
被害事例は防げる事故だった可能性が高い	セキュリティパッチ管理、パスワードの設定や管理不備により被害に遭った可能性が高い
誰もが意識すること	「誰かがやるから知らない」ではなく、関係者すべてが意識することで、サイバー攻撃被害に遭いにくい組織に

「なぜ、対策をするのか」を明確化することも重要

SOPHOS

Cybersecurity as a Service