セキュリティ対策

DCV2026からの抜粋

http://osirix.asia/docs/DCV/latest.pdf

本当に安全な環境が欲しい？

それとも

責任回避を狙う？

※両立しません。

セキュリティ対策の歴史

日本では多くの現場で、セキュリティ対策が「火遊び」になっている。

何かにつけて、専門家が「いたちごっこ」という言葉を使います。これ実際にどういういたちごっこをしてきたのか説明できたら大したもんだと思いますので、ここで歴史をちゃんと見ましょう。(あまりにヤバい話は割愛しています)

以下、HF = Human Factor つまり、人間側の問題を意味します。誰がいつ、がはっきりしない犯罪史なので、おおよその時期と順序になりますがご容赦ください。

対策以前

侵入の始まりは、自分が作ったソフトがどのくらい使われているか知りたくて始まった

- 初期から、大きく分けて侵入とおふざけ、2系統の問題が指摘された。
- 侵入というのはUNIXの世界で始まった。インターネットはもともと研究機関のもの。UNIXワークステーションが相互接続していて、無償で配布されたソフトがきっかけで侵入。
- パソコンはB.I.(Before Internet by Jo Ito)。パソコン通信という電話回線でダウンロードしたプログラムから感染。MS-DOS、Mac(System 7)くらいから、悪意のあるデバイスドライバがあってデータを壊したり画面を操作できなくしたりする"おふざけ"が広まる。これが、いわゆるコンピューターウィルスの始まり
- Windows 3.1では機能が低すぎて侵入なんて無理なので「安全」と感じていた。当時コンピューターウィルスに悩まされたのはMacintoshの方がひどかった。

この頃

パスワードが漏れるのは脅威以前の問題 (HF)

この頃、オンラインシステムで本人じゃない人が入ってくる問題が表面化。これは本人の自己管理能力の問題で、画面の横にパスワードメモを貼ってあったりするのがダメ。

1994

(私事)著者、下宿先の6畳間でLANの構築に成功する。この時点ですでに何件か大学でパソコンウィルスの駆除に付き合った。UNIXの侵入事件も大学で1件は聞いた。

1995

マイクロソフトWindows95発売。ネットワーク機能はまだまだだったが、ウィルス感染能力は一気にMacintoshを追い越す。(これは仕方がないと思う)

[対策]第一世代

そもそも繋がなければ安全、とされた時代

これは成立しないと実際に90年代にDEC(買収されて現在hpの一部門。中型コンピューターのトップ企業で、当時はクラスA*。UNIXの開発に用いられたのもDEC製品)の人が教えてくれた。

結局誰かが繋ぐ

一時的に接続したり、USBメモリでデータを渡したり。この「ちょっと繋ぐだけだから」を彼らは見逃さない
そこで、

物理的に系統分離

事務系、財務系、生産系と分けてネットワークを張ろうとするが、あやまって接続したのに気づかず担当者を呼び出す事案が多発、結局混ざってしまう。この問題はVLANが登場して解決するが、なぜか動物医療の世界は30年経ってもこの図面を引く設計屋がいる。あとあとどうなるか考えないで変な仕組みを入れるな。

2002

当時世界で広く使われていたグループウェア Lotus Notes の国外バージョンに、国家安全保障局(NSA)がバックドアを仕掛けていた事実をとあるハッカーが発見する

[対策]第二世代

通信を防ぐフィルタリングが始まる

侵入を防ぐために、誰と誰が何を通信して良いか、を列記して管理する仕事が発生する。これを、①ルーターレベルでやる、②ハブ(厳密にはL2スイッチ)レベルでやる、③端末ごとのレベルでやる、のレベル別提案で市場が成立する。

おふざけを防ぐため、上記に加えてメールの添付内容などをチェックする機能がつき始める。

この頃

設定が複雑。でも動かさないといけないから全部解除!!

当時は規模にもよるが、Apple LocalTalkや、Netware社のIPXなどのファイル共有がメジャーだったところに、インターネットという考え方が登場する。インターネットは名前の通り、ネットワークを相互に接続してデータを共有するシステム。端末を買い替えずに済むのが大きなメリットとなる。

このタイミングでインターネットと組織内の双方にアクセスできる点を全面に押し出したWindowsが世界を席巻する。ただここには大きな嘘があって、

- インターネットはTCP/IPプロトコルという信号手順
- Windows はまったくことなる、独自のNetBEUIプロトコル
  つまり相互接続はできない。共用できるのはケーブル、ハブ、ルーターなどハードのみ。でも世界は一歩進んだ。(NetWareもイーサネットケーブルが使えたが10BASE-2や、10BASE-5規格が多かった。LocalTalkはRJ11という電話線)問題はこのことが説明されないので、繋がらない、繋がらない、となり、

とりあえずセキュリティ全面解除→繋がる→そのまま放置

かくして簡単に繋がる共有サーバーがいっぱい出てくることになる。

脅威

外から攻撃できないなら・・・トロイの木馬方式誕生

- メールの添付ファイルに悪意のあるプログラムを添付してスパミング(あたりかまわず送信する)を行い、発動すると再感染などを行うタイプのものが現れる。
- 内側から外に出るので、「外部からの攻撃」を防いでも関係ない。90年代後半にはもうあったので、2025年に「外部からの攻撃がー」とか言っているのは30年ずれている。

Excel などのマクロウィルスが大問題に

Excelを開いた瞬間に陰で発動するマクロに悪意のあるコードが入っているパターン

もはやアート。JPEGウィルスが見つかる

圧縮されている画像として知られるJPEGにおいて、圧縮を解凍した瞬間に意図しないプログラムが実行されると言う、もはや芸術級のウィルス。考えた人は天才。

データを盗む、スパイウェア登場

Adwareが登場

パソコンを使っている最中にいきなり広告が出てくるタイプのウィルスが登場する。

この頃

USBメモリで感染。なぜ？

USB端子がどこにもないパソコンが登場
USBメモリだけ認識させないツールも登場

第三世代

ウィルス対策ソフトの市場が成立する

ネットで広まっている悪意のあるプログラムを片っ端から収集し、パターンファイルと呼ばれる辞書を更新しつづけることで感染しても駆除する、というサイクルが普及。

脅威

亜種を簡単に作れるウィルス開発キット登場

最初は数ヶ月おきとかだったが、そのうち数時間ごとにパターンファイル更新するのがあらわれる。(Kaspersky だったと記憶する)しかし、パターンファイルは追いつかなくなる

環境を選んで発病する、潜伏アルゴリズムが開発される

ウィルス対策は、試験管動作するパソコンに感染させて外部から動作内容をチェックして突き止めるのですが、これらの試験管内にいることを検知して、普通のパソコンの環境にいない時には発病しないと言うテクニックが開発されます。
後述しますが、これは一般社会にも影響します。

2007

日本の社会保険庁で、「消えた年金」事件が発覚。この際に実は職員が調査のフリをして端末から自分の同級生たちがどこでどう暮らしているかを検索していた事実が発覚。それが一人や二人じゃなかった。

2010-

北アフリカ諸国で政権が崩壊。「アラブの春」と呼ばれる一連の革命が、FacebookなどのSNSの力に支えられていたと分析されて話題となる。

2014.5

米紙Wall Street Journalで、セキュリテイソフト大手のSymantecの情報セキュリティ担当上級副社長ブライアン・ダイ氏の「ウイルス対策は命が尽きた」発言。「ウイルス対策ではどうやっても収益は出ない」。批判もあったが、正しい。

2015

ヨーロッパでディーゼルゲート事件が発覚。

この頃

ネット通販、株取引の拡大に伴い、クレジットカードが標的に

フィッシング登場

偽物のサイトに誘導してクレジットカード情報を盗む手口がひろまる。
攻撃対象のトレンドがOSからWebへとシフトしていく。

2018

米国でCLOUD法が成立。米国の法執行機関が、米国内に拠点を置くクラウドサービスに対し、データの保存場所を問わずデータの開示を求めることができるようになる。つまりDropboxの文書は必要があれば政府の役人が見れる。

第四世代

ホワイトリストに基づくWebアクセス制限

セキュリティルータービジネスが成立。初期はSonicWallなど。
パターンファイル方式から、Heuristic 解析。プログラムの動作パターン

この頃

Web2.0 - クラウドコンピューティングの時代到来

そもそもパソコンが盗まれる国では手元のパソコンにデータを置かずに、クラウドに置くように

二段階認証が広まる

SoCの普及でIoT(インターネット家電)が広がり始める

脅威

IoTやUTMにさまざまな脆弱性、スパイ動作が見つかる

脅威

ランサムウェア登場

- 対策は原始的なバックアップでよいのだが、意外とバックアップしないし、復元なんてやったことがないため、いざという時にバックアップが途中で止まっていただの、復元先を間違えて止めを刺してしまっただの事故が多発。
- ランサムウェアの動作は、Heuristic解析で見抜けない

脅威?

AIが大ブーム。問題はクラウド文書で学習しているという・・・。

- みなさんの文書を食っているそうです。

2024.2

オランダ軍情報保安局(MIVD)と総合情報保安局(AIVD)が、中国政府の支援を受けたハッカーが国防省などで使用されるファイアウォール「FortiGate」のネットワークに侵入したと報告。調査の結果、MIVDは約2万台ものデバイスが中国のハッカーによる被害を受けたことを明らかにした。(https://gigazine.net/news/20240612-chinese-hacker-fortigate/)

脅威

セキュリテイ対策ソフト(VPN)、ハード(UTM)にハッカーが潜り込んでくる時代へ。

はっきり言って、これほどのリスクを冒してまで取り組む価値があるというなら、電子カルテをやるがいい、と思える。私は今後も紙カルテ2.0をお勧めしたい。

環境検知テクニックを一般メーカーが悪用し始める

ライセンス保護にウィルスの技術が応用され始める。どれも悪用だ。

悪意がある、ないはともかく動作原理はウィルスそのもの。なんと、筆頭はOsiriX！

HoroXaust (OsiriX本家)

時間差発病 (OsiriX M.D.)

※うちのVLシリーズは該当部分を消してあります。

ディーゼルゲート。ヨーロッパの自動車メーカーでディーゼル社の検査をごまかしていた事実が発覚

欧州の自動車メーカー、特にドイツで、排ガス試験の場所では極めてクリーンなエンジン運転をするソフトを入れ込んでた。これが結局ユーロディーゼル時代を一撃で終わらせる結果となり、言い訳がましく電気自動車へ全面移行して、いま詰んでいるところ。

Samsung / Xiaomi「特定のソフトを使用した時だけパフォーマンスを変える」ことが発覚

ベンチマークソフトのアプリケーションIDを変更するとスコアが大幅に低下することがバレる。わかりやすく言うと「ベンチマークの時はフルパワー、それ以外では手抜き」動作。

ノックで動作が豹変するカメラユニット

日頃は外部から確認してもなにも変な動作はなさそうなのに、特定のノック(アクセスシーケンス)を行うと通信システムが開放されるものが出てきた。実は生体モニタでも見つかっている。

あなたは、この人たちの頭脳に勝てますか?

冒頭に申し上げたように、火遊び、じゃないですか？

どちらを選ぶかの、判断基準

クラッカー(日本ではハッカーというけど)は、**IT**スキルは**MIT**卒に匹敵するし、攻撃対象の民族性、思考回路まで学んでいる。

つまり、パソコンを攻撃しているのではなく、あなた/御社の思考を読んだ心理戦になっている。

だから、機械では防ぎきれない。

日本人/日本企業のセキュリティ施策は「みんな同じ」「一点突破主義」「大艦巨砲主義」と似るので・・・・・。

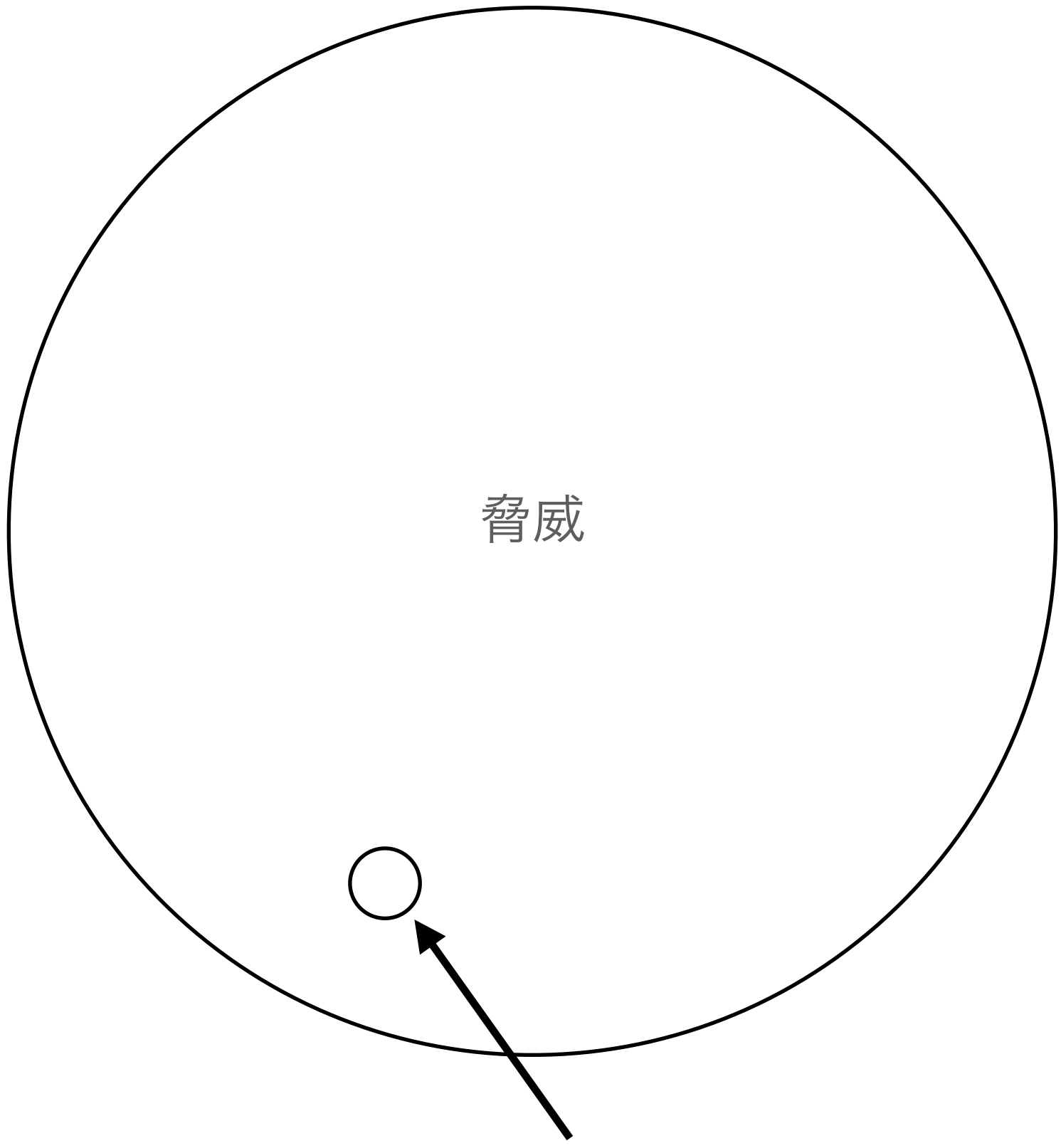
例　陸上競技のトラックは必ず反時計回り。なぜか？

セキュリティは”利益を生むように”入れる

しくじると、仕事がテレビゲームになっちゃう

んー、と思うやり方	おすすめ、と思うやり方
セキュリティ装置、セキュリティソフトを入れて喜ぶ。**(※**一件だけ、感動の重連ルーターを見たことがあります**)**	スタッフに対する情報リテラシー教育を行う **-** 文字で残すことの意味 **-** なぜ**Outlook**じゃだめで、サイボウズや**Gmail**がよくて、**slack**が人気なのか**?**
電話一本で言うことを聞く業者が好き	整然と管理されていると悪いことはできないもの。
診察、検査、オペも口頭指示が好き。紙に書くのはきらい	誓約書をちゃんと書かせる
パソコンよりも紙が信頼できる	外部からの脅威に対応するには オフラインバックアップ プロキシサーバー
パソコンもソフトも買ったら永遠にノートラブルなのが当たり前んじゃないの**?**	
Excelは最強	裏紙を使わない **-** そもそも印刷物を減らす **-** すごい書類が裏紙で出てくる
インターネットに繋がなければデータは漏洩しない。え、漏洩するデータの種類**? ...**	
クラウドが便利。もうこれからはすべてクラウドでいいんじゃない **(※**サービスによってはおすすめできます**)**	他業種のやり方も導入してみたい カンバン方式
私は、記憶力に絶対の自信がある	
在庫管理は発注点主義で十分でしょ**?**	
書類が見つからない時はカルテフォルダ全確認だ**!**	データの整合性の維持 外部公開。患者さんから間違いを指摘してもらうのは恥ずかしくない。 ピアレビュー
(※これは**1**度しか現場で見たことがない。どういうことかというと、違うカルテフォルダに入れたのではという前提で、全部のカルテを棚から出し、手分けして書類を探す作業。よくやっているらしく、**30**分くらいで全部のフォルダを絨毯爆撃していた。良いのか悪いのか・・・**)**	
獣医学会は行く。他の展示会なんかは行くことない。	
業者の院内での作業安全性**?** そんなの知らねえよ。	**IT**関連の展示会も行ってみては**?**

セキュリティセールスに騙されない



自分的にはちゃんと投資したと思ってしまうようですが、本当のセキュリティ対策は数百万程度では買えるようなものでは・・・。

セキュリティの心得

■動物病院の最大のセキュリティホール
(全部がそう、とは申しませんが)

・”自分より賢い奴に出会わないなー”

少なくともなかなか見かけないと感じるのは確か

・”医学に比べればITなんか大したことない”

ITをやっている連中があまり賢そうに見えないのは正しい
(日本は誰でもエンジニアになれる特例国なので)

シンプルなセールス論法と、無知への畏怖、ブランド信仰でつい・・・。

なんと売り子も心底性能を信じてしまっている例も。

徹底して外部からの侵入を防ごうとしていながら、リモートメンテナンスやZoom会議をしようって・・・矛盾に気づかないか?

■実際に起きたセキュリティ事故は退職者によるものが多い

・セキュリティは人が基本。金で解決する問題ではない。

・病院創りがセキュリティを高くする

いずれもウィルス対策ソフトとか、セキュリティルーターでは解決できない。(むしろ逆効果)

↓

日頃からの研鑽と教育、5Sの徹底

患者、物品のID管理

責任の所在の明確化

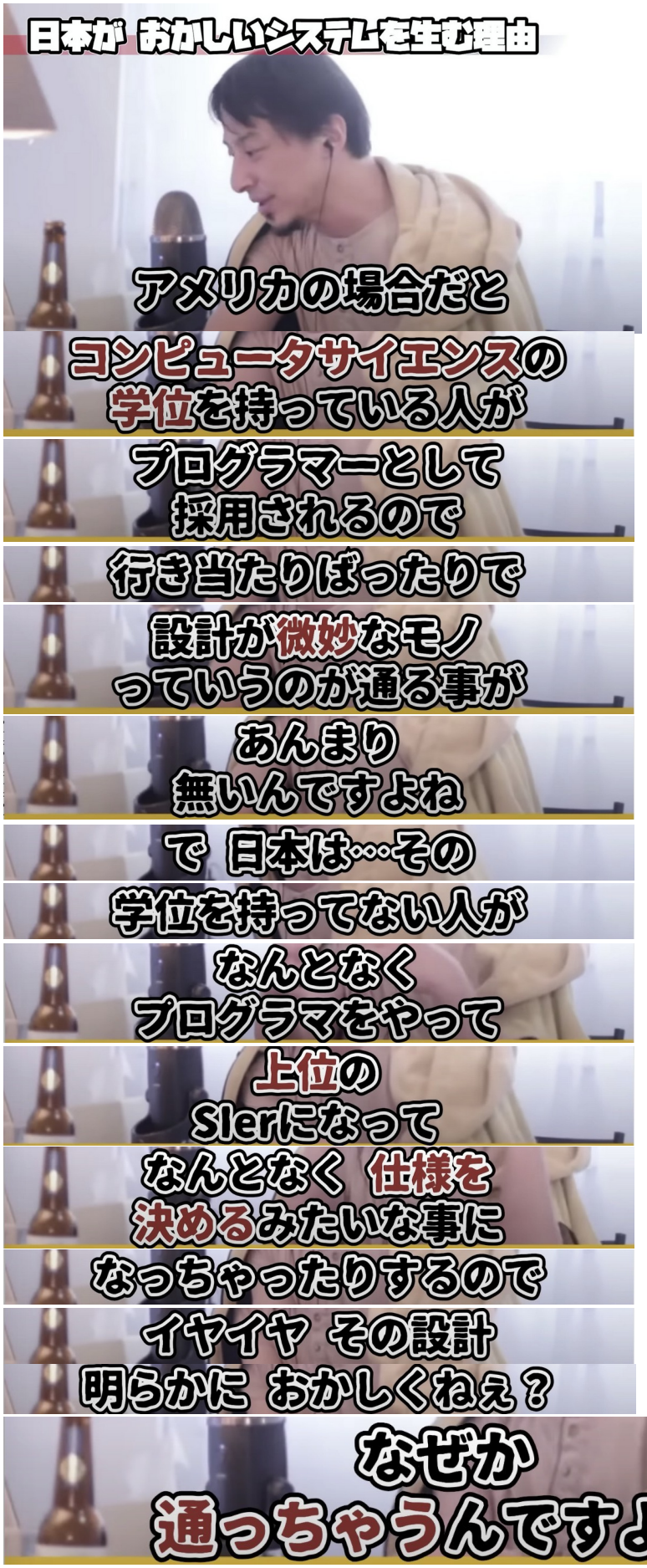
病院のキャリアサイト化(学びが得られる職場)

が最も効果的である。

(そりゃ手間ですよ)

学位が要求されるのは医療だけではない

マイナンバーカード事件から学ぶ日本のIT業界、これからのAI｜【ひろゆき 切り抜き】



※抜粋ですので、切り抜きの切り抜きです。
※私はもう老兵なので自分を売り込むつもりは毛頭ありません。

この文書は、なぜIT業者について学位を確認しろというのか、理由を説明しています。

日本語でコンピューターサイエンスで検索すると、ヒットするページの大半の内容が上っ面だけの、間違いだらけでビックリしました。

本来のスキルは以下のような、

・データ処理の歴史を知ること
・英語で文書を読み書きする技術
・最新の言語ではなく、古い言語を分析する
・シミュレーションと微積、離散化の応用力
・畳み込み … これが一番大変かもしれません … 目の前の課題の構造を分析して、最も合理的に解決するにはどういうアルゴリズムを組み合わせればよいかを判断する。
・関係者の説得と最善の段取りを提示する。ディベート力と呼びますが。

これらはそれなりに高い能力と経験がないと無理です。しかも、日本、国家レベルでは非競争開発が基本なので、
・計算機科学を唱えて、かなり時代遅れな国産OSを作ってみたり
・アナログのまま高画質、高品質のニューなメディアを作ろうとしたり
・行き詰まったらアメリカをパクっちゃえ
ですから。

なので、日本における本物のITエンジニアの頭数は相当少ないのです。現場知らずの人間が、生徒に教えるのが特に難しい分野の一つです。

HoroXaust (一応、ほろこーすとと呼んでます)とは

元祖**OsiriX**の開発を主導していた**Pixmeo**社が起こしたサイバーテロ。

OsiriX Ver.3～最終盤の**Ver.5**に意図せず存在していたバグを悪用し、インターネットに接続している**OsiriX**が起動に失敗するようなコードを返すようにすることで、自社の製品である**OsiriX M.D.**への買い替えを促したもの。

ここでの問題は、本来この問題はセキュリティルーターの設定で簡単に回避することができるものなので、当時対応を求めてきた病院や業者のすべてにセキュリティルーターの有無と、ある場合の設定を案内したが、

設定できた例が一件もなかった

のでした。

つまり、

日本はこの程度
なんです。

さすがにビックリしましたよ。一人くらいいてもいいじゃないですか。
左から右にモノを動かしているのが楽で、この状況に20年以上甘んじていた結果、

もう自国の技術を信じるのはやめて、アジアの方が上だと考えた方がよい

状況にまでなっているのです。

アジアのエンジニアや理系の技術者は日本やイスラエルのように自国語のテキストが用意できなかったために最初に英語力をつけることが求められました。これが決定的で、めまぐるしく技術が進んでいく今日、公開される英語のドキュメントが読めれば、伝言ゲームもないし、誰よりも先に技術に触れることができます。また、プログラミング言語もほとんど英語文法と英語レトリックなので、プログラミングを覚えるのも楽になるおまけつきなのです。

セキュリティルーター意外なデメリット:経営がおろそかになる

他の業界と比べても驚異的な普及率。聞いてもないのに「びっくりするくらい簡単に売れる」と数社が向こうから言ってくる状況。機能と意味を正しく理解した上で導入しているのなら文句はありませんが、

本来、ブラックボックスを買うのは恐ろしいことです。

本来、以下のような業務に集中したいから金で解決できるものは金で解決しようという発想に至ったはず。でもセキュリティルーターのあまりの金額に、かなりの範囲の問題が解決されたと錯覚していないか**?**

診察コストが上がるのは当然として、ここでの問題は**5S**の「しつけ」

■　**IT**サイド

・端末のパトロールをしなくなり、事故る

・データのバックアップを忘れる

上記は初期症状。

■　経営サイド

・スタッフのモチベーションパトロールを怠る

・顧客の付き具合のパトロールを怠り、客が減る

・在庫のパトロールを怠り、不良在庫が増える

飼い主に安心を提供する仕事をしているのだから、安心というのがどういうしくみでできているのかは判っているはず・・・・。「日頃の〜」という言い回しをよくしていますよね。

これがプラセボ**(**何も設定されていない、ただのハブ**)**だったら、どうします**?**

それでも買いたい理由があるなら、一番気が抜けるのがそちらのパトロール。

個人で数百万のセキュリティを入れるということはもっと大きいリスクを抱えている・・・業者はそこまで見透かしているものです。

セキュリティ対策　初級編
まずは本物のセキュリティーツールを選ぶ

現場で話をしていると、そのエンジニアがどのくらい知っているかはすぐにわかるんです。

○通信システムで対策するなら

■　L2スイッチ(ハードウェアの種類)

見た目はハブと似ている

ハブの一種で、どの機械とどの機械が通信して良いかなどの通信経路(トポロジ)を画面操作で決められる。配線で経路を作るのは時代遅れとする根拠。

■　ポートミラーリングハブ(ハードウェアの種類)

通信を傍受するときに使うハブ。大昔のハブで代用可。ということは・・・

■　スニファー(ソフトウェアの種類)

Wireshark

通信内容をすべて傍受して何が行われているのかを可視化、解析するツール。前述のポートミラーリングハブはこのために使うことが多い。
オープンのWireSharkが有名。DICOMのような特定の業界の通信も解析できるすごいソフト。WireSharkを知らない奴は絶対に信用しない。

■　プロキシーサーバー(ソフトウェアの種類)　おすすめ

特定の通信だけを通すソフトウェアで、Webアクセスだけ、とかメールだけというアプリケーションごとの通信を制御する。フリーのものもある、というかしくみも単純で効果は大きい。否定する人たちは使ったことないのでしょう。いまでもOSはサポートしてますよ。(ちなみにpriXmに標準で入ってます)

■　パケットフィルター(ソフトウェアの種類)　設定が面倒

セキュリティールーターでなくともパケットフィルターが装備されているルーターは多い。

一般的な動物病院には内蔵フィルターで十分でしょう。

上記のスニファーに加えてアクセス制御をする。
デジタル通信信号のレベルで内容を審査して通す、通さないを決める。相当な知識と経験が必要でここが院卒のエンジニアが必要だと主張する根拠です。Windowsファイアウォール、TCP wrapperなどがこれ。

■　イントリュージョンテスター(ソフトウェアの種類)

実際にシステムへの侵入を試みるツール。Nessusなどが知られている。大規模なネットワークはこれで定期的にテストしないといけない。

○通信以外のツール

■通信ではなく、ソフトウェアの動作の統計をとってあやしいと判断するツールもある。たとえば文書作成ツールなのにGPSにアクセスしていたらおかしいと思いますよね? Windows Defenderなどがこれ。

仮想化ソフトウェアの代表格 VMware

■仮想化ソフトウェアを用いてシステムがいつ破壊されてもいいようにするケースもかなりポピュラー。

■VeraCrypt (暗号化対応の仮想ディスク)　←2026年以降はこれ

気づきましたか?

通信の種類は膨大で、企業単独でセキュリティ機器の開発は実質不可能。結局オープンソースソフトの世界で高く評価されているものに少し手を加えた状態のもの、ひどいとそのまんまを商品として、現場に合わせて設定なんかろくにしないで設置していくことになる。それなら最初からオープンソースのまま使った方がいいんじゃないかと思いますけどね。
なお関連機器を買ったら、どういう設定をしたのか提出してもらうこと!

セキュリティ対策　中級編

初級編と中級編の決定的な違いは、定期的な手間がかかることと、実働部隊の仕事に干渉するかしないか、です。それまでは「動いていて当たり前」「あいつらパソコンで遊んでるだけ」などと営業や、工場から言われていた状態から、彼らの業務フローに直接口出しして「少しずつ」会社を変えていく立場へと変わります。いてくれないと困る存在にならないと、上級編への布石が打てません。

まず、矛盾を自覚する

会社/病院の持ち金を減らすことが成果なわけがないでしょう? 経済的な被害を防いだと言い張っているだけです。

1. ここまでの仕事は大きい会社がやることではない

ここまでのセキュリティ施策はお遊びといってもいい。必要条件かも知れませんが、十分条件ではありません。外部に頼んで得体の知れない数百万円の自称セキュリティ機器を買うなら町場の動物病院でもできてる(しれっと100病院以上がこんな状態)。つまり、その程度の「簡単なお仕事」であることを自覚します。

■要確認■
ウィルス対策ソフトやUTMなんかで、結果的にランサムウェアにやられて払うよりも外にお金支払ってないですよね?　結局経済的な被害は同じでは?

経営的に見ればお金が減っている以上、外部からの攻撃を受けたのと変わらない。この手の仕事を委託しているSierも、中には途中で切り捨てれば他の取引先に「あそこはセキュリティに無関心で」などと悪口を吹聴して歩くのがいるので、これ自体も組織としては脆弱性要因。最初から関わってはいけない。

2. メインフレームの延命って、セキュリティ方針と完全に相反している

何十年も手付かずのコンピューターが社内にいる時点で、それはもう脆弱性要因です。外部から攻撃される、とは別に故障した時に部品が手に入らなくて長期化するのも重大インシデント。

3. SIerから全社レベルで無償提供受ける、は脆弱性要因

これもよく見かけた。最初は「まだ開発中なので」みたいなことを言ってきて全社に無償でソフトを提供してきて、やめられなくなったところで有償化に持ち込むケース。これって実質的にセキュリティインシデントですよ。

「あいつら本当に会社の役に立ってんの?」から、まずは「仕事のやり方勝手に変えんなよ」と言われるようにならないといけない

現場、実働部隊の人には仕事のやり方を変える余裕なんかないはずで、本来後方にいる人間に経営者が期待することは、実働の作業効率を上げることのはず。もはや、みせかけのリスク回避を成果と主張し続けるには無理がある。

Sandboxルームの開設

リースアウト品でもよいので、会社/病院で使っているパソコンで小規模の、「何が起きてもいい」サーバールームを設置し、そこで実験できる環境を作る。もちろん職場とは接続しない。インターネットには独立した回線で接続する。

バックアップからのシステム復元を定期的にやる

意外とやってない「復元作業」。いざ本当に壊れた時に復元するはずがとどめを刺す若い衆を何度が見てきました。日頃からSandboxで訓練するんです。

最初は、分院や、海外支社などで取り組めれば理想

子会社という手もありますが、これは相手先をよく吟味しないといけない。

おそらく利益を産んでいない子会社をあてがわれたりするケース

面白いことに自社で開発している範囲では気にしなくても、いざ子会社でプロジェクトを走らせようとしたら先方から(子会社/関連会社の)与信が通らないので、親会社に保証人になってくれ、と言われたりしたら中止するか対象の会社を変更すること。

子会社は一癖ある。知り合いがいないなら特に注意。

海外法人。どっちが親会社かわからないケース

こちらが親会社なのに行ってみたら投資計画書を突きつけられて「本社からこの承認をとりつけてくるのがお前の仕事だ」とマウントをとってくる。これは数社聞いた。

必ず、先にこちらで分厚い実行計画書を作成してから乗り込むべし。(これも実話)

拠点設置担当なら、同じ工場をいくつも作るな

毎回、新しい取り組みを少しずつ入れます。

外部業者に悪役になってもらう

フォローだけちゃんとすればOK。ただ、「業者のミスで」をあんまり大声で言うと、しばらくして「あの人(=追い出した業者)のおかげで仕事がしやすくなった」となった時に立場が危ういので注意。意外とプロのコンサルのやったことは半年くらいで評価が変わることがある。

上記を円滑化するための小技

ちょっと骨のある奴かも、と見られるような小技が現場の人には受ける場合があります。部署のメンバーによってはハラスメントになるので注意しましょう。

サーバーのデータの80%まで、まったく仕事と関係ないファイルを倫理的に問題のあるファイル名で置いておく。

現場の人が欲しがる動画

かつてビデオフォーマット戦争の決め手になった実績。

どうでもいい動画をサーバーの大半に置いておきます。過去の例では「機密文書」というフォルダに、アダルト動画を大量に置いてあったり。※そう言えばホームページ用などで社員の顔写真置いてあるサーバー見かけますけど、あれは止めましょう。

偽物の名簿。社員も騙されちゃう。

名簿も偽物を作って大量に置いておきます。※架空名簿作成ソフトは英語版ならいろいろありますね。

外部に暗号化される前に、もう暗号化しておく

いくつかの現場で、辞めちゃった人が作成したデータがパスワード解除できなくて困っているという事故を見てきました。これを逆手に取ります。

自動的に暗号化されちゃう場合は役に立ちませんが、ファイルを精査するタイプ、特に社内の悪意ある侵入者には初めからこちらで暗号化しておく手もあります。

社外講演、雑誌の取材には軽く応じよう

紹介されました記事は内部に対しても有効です。日経系列の取材は仕事が早いので、取材が終わっても対応する時間をとっておきましょう。ユーザー会とかはのんびりしていることが多いが気をつけないとただの飲み歩きになるので注意。

セキュリティ対策　上級編

ずばり、定期的な"プラットフォーム変更+業務手順変更"

上級編は業務改革とセキュリティ対策が両立する最強の施策になります。

要するに業務系システムの全面刷新を定期的に実施することが最強の対策になります。これが定着していれば

- 担当者のスキルレベルを維持
- 基幹システムを支えているというプライドを持てる

1990年代以前は基幹システムはとても高額で、ダウンサイジングの結果、新型が出るたびに価格が下がったのもあって、積極的に機械を更新していたので結果的にセキュリティ対策になっていました。つまり、これは現代ではロストテクノロジーの一つでもあります。

悲劇の始まりは

- Windows95からパソコンを使い始めた人たちがそれほど大きな変化に振り回されてこなかったことと、
- Webの成立で手元のパソコンをどんどん更新しなくても良くなってしまったこと、
- 自分でコードを書く文化をまったく知らない人が多数を占めてしまったこと、

などなどの環境変化でしょう。来年は違うOSになるかも、と思っていればパソコンへの向き合い方も大きく異なり、バックアップなどもちゃんとやる人間に育ったと思われます。

プラットフォーム変更の例

これらは結果的に強力なセキュリティ対策になります。なぜなら攻略する頃には変わっているから。こう言うと、

「Windows10/11は頻繁にアップデートしているじゃないか」

という反論が返ってきそうですが、今回は業務改革がセットになってる点に注意。仕事のやり方もそっくり変えてしまう経営戦略と、そのためのプラットフォーム変更です。なので、たとえばこれまで全部Macだった組織を全部Windowsに変更する、などはOK。WindowsやMac依存を死守していたらどこまでやっても上級編とは言えません。

※どうしてもWindowsなら、最悪Intel系WindowsからARM系Windowsに移行して、またいつか戻ってくるのも悪くないです。これも意図した例ではないでしょうが、AppleのMacは1984年の発売以後、Motorola、PowerPC、Intel、ARMと定期的にCPUを変更しており、結果として、切り替えのたびにそれまでのマルウェアは原理的に動作しなくなっています。

・全社で一斉にExcelをやめて別のアプリに乗り換える

・基幹システムのメインフレームをやめてLinuxサーバーへ切り替える。しかも定期的に。

注意: 全社規模のアップデート作業はこれには"絶対に"該当しない。

- パソコンを全台入れ替えたとか
- Windows N を Windows N+1 に入れ替えたとか

これは初級レベル。

セキュリティ障害発生時の対処

■流出した恐れがある、との声明を出す

株式会社　　から、令和　年　月　日に報道発表のありました個人情報の不正流出に関して確認しましたところ、上記報道発表のとおり個人情報が不正に持ち出され、第三者に流出していた可能性があることが判明しました。

　現在までの調査の結果、不正に持ち出された個人情報の対象人数は　人分であることが確認されました。

今後、対象者の方には個別にお詫び文書を送付させていただきます。

１、判明の経緯と原因

　○○○○　に対する警察の捜査が実施され、同社の○○○（元　社員　派遣社員　）がサーバに不正アクセスし、顧客から預かった個人情報を不正に持ち出し、第三者に流出させていた可能性があることを確認しました。

２、不正に持ち出された個人情報の内容・時期

　飼い主　氏名、患者名、住所、患者生年月日、犬種、マイクロチップ番号、電話番号、メールアドレス

３、二次被害やおそれの有無

　現在のところ、悪用されるなどの二次被害の発生は確認されておりませんが、引き続き状況の把握に努めます。

４、今後の対応と再発防止のための措置

このような事態を発生させ、飼い主の皆様へ多大なご迷惑とご心配をおかけいたしますことに深くお詫び申し上げます。

　対象者の方に郵送によりお詫びと経緯についてお知らせし、ご相談などが寄せられた場合には適切に対応してまいります。

　また、当院では今回の事態を重く受け止め、本件事業者への個人情報の厳重な取り扱いを指導徹底し、再発防止に努めます。加えて本件事業者への厳正な対応を行ってまいります。

引き続き個人情報の適正な管理に努めます。

５、本件に関する問合せ先

セキュリティ障害発生時の対処2 責任の所在はどこか

■内部の犯行であれば、当人の責任

■セキュリティシステム業者に一定の責任

・実は業者も知らないくらい、重い。だからうちはやらない。
・対処できるとしたセキュリティ項目が破られた場合は当然責任を問われる
・この辺はちゃんと契約書にうまい具合に書いてあって、責任を問えないという見解があるのだが、
日本医師会総合政策研究機構からのレポートでは、民法によれば免責事項は無効である。(下図)

システムの総額程度を上限に賠償の上、業者名は公表あたりか？　これは要確認。

資料・書籍・その他　　2023-08-24

サイバー事故に関し システムベンダーが負う責任：医療DXを推進するために

堤　信之

＜概略＞
数あるサイバー攻撃の中でも、特定の攻撃手法が既に広く世間に周知され、かつ実際に被害も頻発しているようなケースでは、当攻撃手法に関し、システムベンダーは医療機関等に対し、委託契約又は信義誠実の原則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために必要な情報を適時適切に提供する義務を負うと考えられる。
従って、医療情報システムに設置されたFortinet製VPN装置（CVE-2018-13379）の脆弱性を突いたサイバー事故が医療機関に発生した場合、たとえ医療機関とシステムベンダーで締結したシステム保守契約において、当リスクにかかるシステムベンダーの情報提供義務が明記されていなかったとしても、当該装置の脆弱性に関する情報提供がなされていなければ、医療機関からシステムベンダーに対し、「信義誠実の原則」違反を理由に一定の責任を問える可能性がある。

■ネットワーク管理業者にも一定の責任

契約によるが、

・データのバックアップを管理しているかどうかは問われる

・システムのダウンタイムに比例する保守料金減額措置が妥当　　※当社でもPJコースはこうなっている

■犯行動機によっては、院長の責任

警察の取り調べに対して、以下のような供述をした場合には報道発表される

・給料が安かったので・・・

・みんなが仲が悪かった

・データの管理がずさんで簡単に持ち出せた

記者会見の謝罪「悪名は無名に勝る」

テレビ新聞に対しては、基本的には日頃の行いがすべて。企画書をどう書かれるかが勝負。中小企業は第一印象ですでに悪と仮定されていると心得よ。日本を支えているなんてこれっぽっちも思っていませんよ。

だが、最近はネットの世論の方が優位。今なら先に動画作っちゃった方がいい。アップロードすべきだが、しないにしても作ってみて自分たちがどう映るのか確認できるメリットは大きい。テレビ新聞は一過性だがネット記事はずっと残る。しかも、ほとんどの人は見出しと画像しか見ない、報道を鵜呑みにする世代は2020年代のうちにほぼいなくなる。

■事前準備

・箝口令をしく
　・自分の考えで適当なことを言わないよう通達。会社のことをよく言えとは絶対に言うな。
　・そのために、一連の問題の経緯を社員に説明する　なお流出することを前提とする。

日本では現場に来る人が聞いたことはどうでもよくて、基本的に誰が悪くて誰が悪くないかは決め打ちでやってくることが多い。ひどいと歴史的事実とは異なる内容になっているのをわざわざ調べて理解しているのに企画書と違うからと言って、「本当は御社が最初に開発して発売したという事実は理解していますが、あまり売れず知名度も低かった。後続のA社さんの方が知名度も高くて売り上げも大きいので当番組では日本で初めて発売したのはA社さんとして番組を流しますのでご了承ください」なんてことも。

・事前に内輪で練習しておく

　・「どうして社長が出てこない」
　・「その原稿には何が書いてあるんですか?」
　・原稿を読まない　「マニュアルが存在するのか」

　・おじぎの角度は練習して揃える。10数えて。

よく判っている人の例。飛行機の前でANAの入社式

見出しと画像しか見ない人が多数なんですよ。

■どこで記者会見を開くか

・この業界では、会議室はおすすめしない

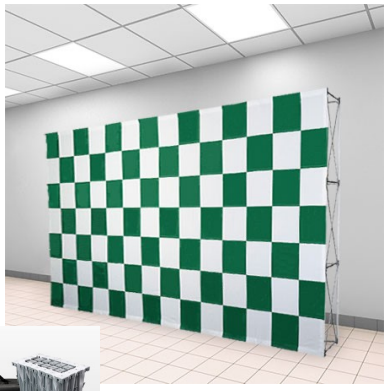
■どうやって袋叩きにあうか

　・まず会社の自己紹介。
　ぜんぜん違う話で報道されたらそれはもう面倒臭い

　　・マスコミは大動物(産業動物)と小動物(愛玩動物)の区別がちゃんとついていない。
　　例えば、大動物の権威に猫業界の話を聞いてしまう

　・ちゃんと戦闘服を着る。全員スーツは金融と政治家がやること

　・バックボード/バックパネルを作っておく



折りたたみ式なら場所を設定できて便利。
出典: http://banner-mall.jp/

■絶対に言わないようにすること

・「自分だけではない。他の業者もやってるじゃないか」

・隠蔽工作　　隠したって無理無理、パターンはばれているよ、となる。

・トカゲの尻尾切り　財閥でもないのに何を生意気な、となる。

■日頃からイメージ戦略に一定の予算を使う

・人集めという観点でもalign(=一石二鳥)する。

　んーでもこの費用対効果を読める経営者は少ないでしょうなあ。

よく判っている人2。もはや話をしているのはバックパネルだろう。

見出しと画像しか見ない人が多数なんですよ。

出典: 各種新聞記事

セキュリティ対策

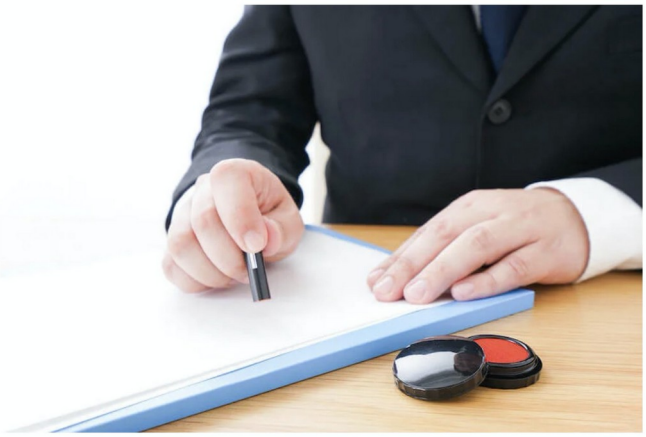
(1)スタッフへの施策

セキュリティ対策　雇い入れ時の誓約

企業法務お役立ち情報　契約書　　更新日：2022年12月15日

従業員の秘密保持誓約書とは？安易な雛形利用は危険！

ツイート　シェア　B! はてブ　LINE で送る　Pocket



この記事を書いた弁護士

西川 暢春（にしかわ のぶはる）

咲くやこの花法律事務所 代表弁護士

出身地：奈良県。出身大学：東京大学法学部。主な取扱い分野は、「問題社員対応、労務・労働事件（企業側）、クレーム対応、債権回収、契約書関連、その他企業法務全般」です。事務所全体で400社以上の企業との顧問契約があり、企業向け顧問弁護士サービスを提供。

・弁護士のプロフィール紹介はこちら

抜粋　正しくは出典元を参考にしてください。

・秘密保持誓約書は入社時、昇進時、退職時の**3**つのタイミングで取得します。

・具体的にどの範囲の情報を秘密にしなければならない対象とするのかが、従業員からみて明確にわかるように記載しなければなりません。

・従業員に誓約させる秘密保持義務の内容について、必要な内容をすべて記載することが重要です。

以下の内容のうち、自社に必要なものがどれかを検討して、漏れなく記載しましょう。

他に開示しないこと
会社の許可なく社外に持ち出さないこと
会社の許可なく複製しないこと
会社の業務以外の目的で使用しないこと
秘密情報の毀損及び漏えいの防止に努めること
万が一、漏えい事故が起こったときは直ちに会社に報告すること

・秘密保持誓約書の内容として例えば以下のものを入れておきましょう。

会社が所持品検査を行うときは異議なく応じること
会社が防犯カメラを設置し、動画の閲覧、保存を行うことを承諾すること
会社が秘密情報の管理状況について調査を行う場合は調査に応じること

・退職後の秘密保持義務についても秘密保持誓約書に明記することが必要です。

退職時に秘密情報をすべて会社に返却すること
退職後に秘密情報を使用しないこと
退職後に秘密情報を他に開示しないこと

在職中または退職後に誓約内容に違反して会社に損害を与えたときは、その全損害を賠償する責任があることを明確に定めておきましょう。

そのほか秘密保持を万全なものにするために、以下の書類もあわせて整備しておきましょう。

・ 身元保証書

身元保証人を付けておくことで、不正な情報利用があった場合に自分だけでなく、身元保証人にも請求されることを認識させ、情報の扱いについて従業員に緊張感を与えることが可能になります。

・就業規則

就業規則にも必ず秘密保持を義務付ける内容をいれておきましょう。

従業員が退職後に自社の顧客を引き抜くことを防止する目的で、秘密保持誓約書を取得しているケースもあると思います。そのような場合は、秘密保持誓約書とは別に顧客引き抜き防止を目的とした誓約書も取得しておかれることをおすすめします。

https://kigyobengo.com/media/useful/1376.html

責任の所在を明確にする

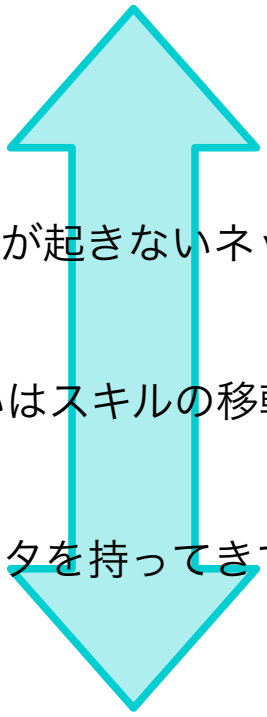
■スタッフごとにハンコを持たせるには

セキュリティ対策

(2)取引業者への施策

業者の選び方

【結論】やるだけやったら本人が要らなくなるように筋道を立てている業者が理想的である



■理想的な業者

1. 構築時には数年先まで考えてトラブルが起きないネットワークを作っているか?

2. 保守契約がある場合、技術移転あるいはスキルの移転をベースに保守シナリオを設計しているか?

3. 自分を要らなくすることで、新しいネタを持ってきてくれる

■理想的でない業者

“いつまでも彼らがいないと何もできない組織作りをゴールとする”

・CE(=IT関連の雑務的なタスク)を何度も請け負うことで組織側の考える力を意図的に低下させる。

・保守は呼び出しがただになる程度(それでも業者が悪いとは言えない。彼らも人件費は発生しているのだから)

ITに限らず、現在物流、税制、労働規約、金融、各種学問のすべてが日々刻々変化し続けるようになったため、勉強し続けないとどんどん置いていかれる。

この状況に対応するには情報リテラシー(※コンピューターリテラシーとは異なる)がカギで、あらゆる関係者との意思の疎通を効率化しなければならない。

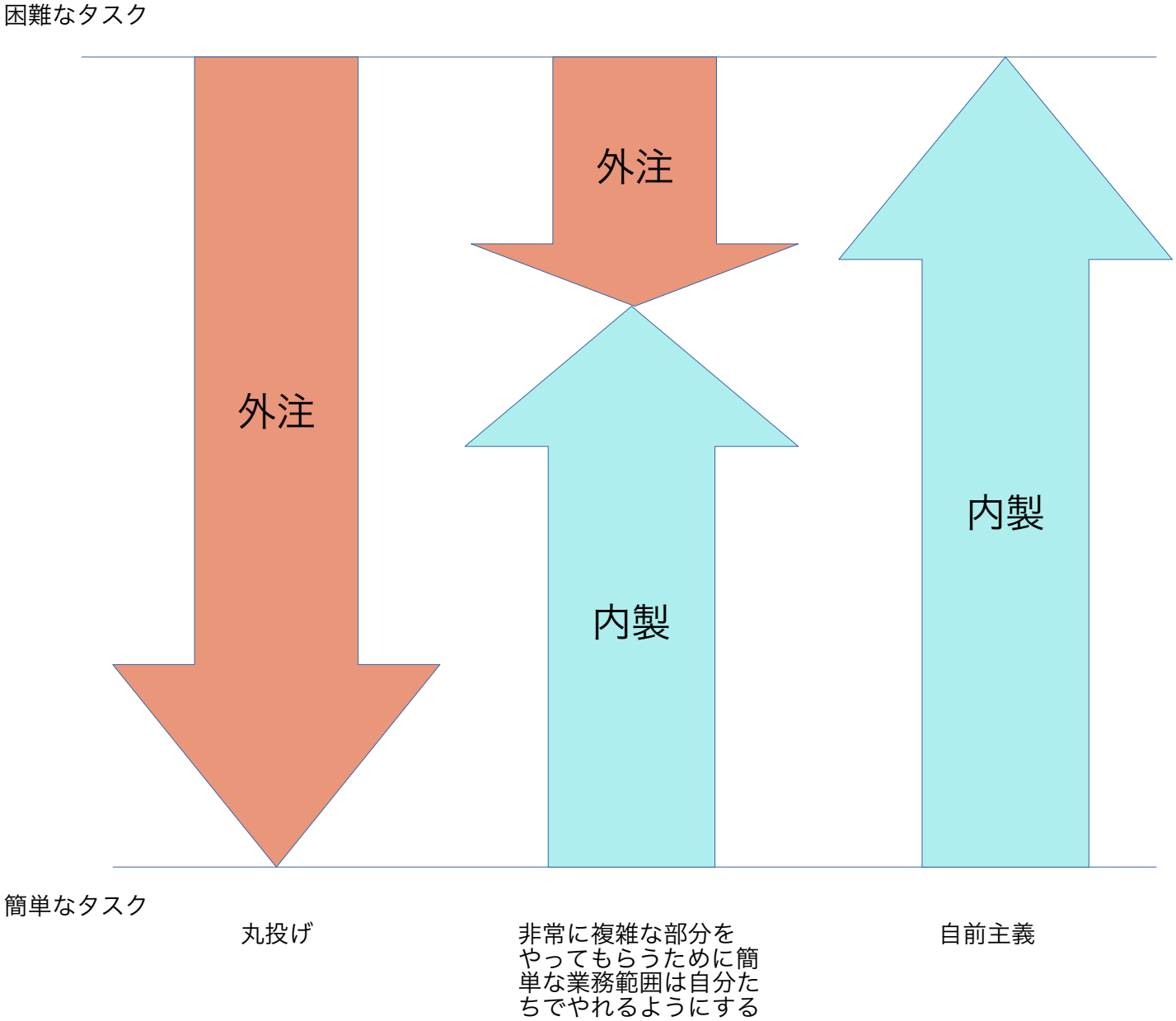
医学よりも大事なものはないのではなく、効率的に医学情報を学べる情報リテラシーを手に入れれば、医学の勉強も短い時間で済むはずで、院内の業務についても効率的な対応をとれる。

今はそう思わないかも知れないけれど、任せたはずのシステムも軌道に乗ると自分でいじれるようにしたいと思うようになり、最終的には独占あるいは再販売を企てて技術移転を求めるようになるのです。Webサイトで経験があるのでは?

他の業界ではよくそういう展開が見られ、ちょっと前に流行ったSalesforceというシステムはその欲望を満たすビジネスモデルになっています。(**病院の考えた拡張部分を同業者に再販できる**)

決めておこう。どこまで自分達でやり、どこから外注にするか

丸投げを決め込んでも、結局外注先に指示を出す仕事は消えない。逆にこの指示が曖昧な現場は「要件定義」とか「茶飲み会」という仕事だけをやって、フェードアウトされる。



ITエンジニアは「ピン・キリ」
オペの腕前と同様、**IT**エンジニアにも格付けがある。

みんなのイメージ

■「プログラミングができる」人はどんなソフトも作れる

ですよね。では同様に

■獣医師免許を持っていれば、どんな手術もできる?

でしょうか?　多くの飼い主はそんなに何段階にも分けて考えてないでしょう。

レベル0: 免許もスキルもない　→問題外
レベル1: 免許はある(のでオペは可能)　→成功するかどうかは別
レベル2: 免許もスキルもある

では、レベル2なら多臓器同時移植もお願いできますか? という話です。

ここではよく問題にされる素行と規律(*)については除外して

*あいさつができるかどうか、仕様書を正しく読める日本語力があるかどうか、後任のコーダーのためにコメントをちゃんと付与できるかどうか、作成したコードについてちゃんと文書を残せるかどうか、チームでコミュニケーションをとりながら仕事ができるかどうか、チェックリストに基づいて作業をさせることができるかどうか、要件定義が書けるかどうか、など。

スキルレベルを評価する目安を示します

・CPUを設計できる　(「アーキテクト」と呼ばれる)
・IP(ネットワークのIPとは違う)が設計できる
・OSが書ける　(アセンブラが使える、を含む)
・プログラミング言語を作り出せる
・デバイスドライバーが作成できる

=== おそらくここに、反りたつ壁がある ===

・iOSアプリが書ける　(ざっくりしてますが・・・)
・スクリプトが書ける
　このあたりが「システムエンジニア」
・スプレッドシートのマクロが書ける
・ちょっとしたWebサイトが作成できる

【参考】中国における料理人には国家資格があって、

・特一級厨師
・特二級厨師
・特三級厨師

・一級厨師
・二級厨師
・三級厨師
・四級厨師
・五級厨師

のように一直線上のランクがあり、下から順番に受けないといけない。

※じゃあアーキテクトはiOSアプリ作れるかというと話は違ってきたりする。
※日本ではアーキテクトの称号を軽々しく使っているが、これはその辺の中小企業の管理職が名刺に「皇帝」と書いているようなもの。アジアの恥と言っていい。

やばい業者を一発で見抜く方法がある　(経験則です)

■こいつは使える、とわかるサイン

・システムエンジニア達のことを「**茶坊主**」と呼んでいる人は意外とまとも。
　使えないITエンジニアを差別的に扱う人は本人が優秀で、彼らがあまりに期待を外すから。
　いない方がましな茶坊主は多数いる。ITエンジニアという職業自体ある意味想像上の生き物。
　何か手に職を付けている人にITスキルをプラスするのが王道。

・契約時に**業者全入れ替えの話を提案**する人は、できるコンサル。
　勝ちパターンを知っていて、現場に合わせるつもりはない。それはそれでOK。
　ま、入れ替えて雰囲気が変われば半分コンサルティングとしては成功したことになるし。
　似て非なる話、後から入れ替えを言い出すのはトカゲの尻尾切り。そいつは使えないコンサル。

■これは使えない、とわかるサイン

【セールス】

・営業にいろいろ聞くと、「開発**部隊**」という言葉が出てくる
　何がカッコイイのか知らないが全国どこに行ってもダメ業者は「部隊」を語る

・提案されたシステムの名前が「〜システム」という名前
　架空のアウトプットの時に固有名詞がつけられないのでこうなる。これは役所や大企業が余興でやるべき内容。中小企業が相手にするべきものではない。

・セキュリティの話しかしない
　何度も言うが、まともなセキュリティは四工大以上の理系学部大学院卒じゃないと無理。

・投資家が後ろにいる国内ITベンチャーは要注意
　3000円のものを300万円で売ってくる

【開発担当】

・「**最新のプログラミング言語**を用いて開発します」
　あなたの資金をダシにして自分のキャリア開発のためにスキルをつけさせてもらおうというとんでもない話。これ何度も出くわしていて、すべてプロジェクトは中止になった。これから学ぶ言語でやるってことですよ!?

【SE/サービス担当】

・現場に来てすぐに電話をかけている
・設定、施工結果の文書を置いていかない。後日の提出もない。
・管理者パスワードを教えてくれない

※いわゆる「電子カルテ」業者はヒトも含めて100社以上話を聞いてきていますが、日本ではいまだに大半の業者が同じアプローチで、似たような仕様で設計されていて、90%以上が同じ失敗を繰り返している。しかも歴史もまったく知らない。
オープンソースで、すぐれたアウトプットを出しているソフトのソースコードから何も学んでない。英語ができないことの悲劇ですね。

パートナー選び　IT業者チェックリスト

これを見て笑える人は相当この染まってます。ひとまず安心。よくわからない方は、要注意。
○プラスポイント　▽マイナスポイント

■肩書き、学位

□エンジニア、セールスフォース**(=**営業担当のこと。製品名ではない**)**は院卒か**?**

　ここは大学名を問える業界ではないので学位フィルターしてください。**F**でも**OK!**

▽彼らがいつまでも傍にいないと困るような仕事をしているか**?**

　▽しょっちゅう呼ばなければならない

□会社は大企業**? (**例えば、富士通とか**IBM**とか**)**　→　一軍**?**二軍**?**三軍**? ....** もっと下もある

▽自称**Google? (**まだいるんですよ**)** いわゆる自称**NTT**と同じノリ

　→□大企業の場合、これも何軍が来た**? (**セールスは当然、彼らは精鋭だと言い張ります**)**
　　□大企業の子会社の名刺だったり　**(**例　キャノン～ソリューションとか**)**
　　□強そうな肩書き

▽親戚、友達**?**

■本業は何**?**　※独断と偏見に基づいています

▽広告代理店　　誰かに委託している可能性が大。優秀なら辞めちゃう。

□設計事務所、デザイン事務所　　困ったら**Too**という会社に振る。**Too**は**Mac**には詳しい

□紹介料で稼ぐのがポリシーの会社　　毎月支払いの関係は意外と悪くなかった

□事務機屋さんの子会社・孫会社　　びっくりするほどダニング・クルーガー**(**別頁**)**している

▽複合機屋さん

□サーバー屋さん　　世界的にはサーバーに詳しいかどうかで判断する。日本はアプリの見た目重視

■ソフトの設計は誰が行っている**?**

○実は獣医

■推進体制

▽会社あるいはプロジェクトリーダーがパワハラ、根性論、体育会系　※ほぼ失敗する

■提案内容

▽飛び込み営業

▽最新の技術をアピールする

▽開発担当もよくわかっていないプログラミング言語を使う計画になっている

　(本人も自分の将来のことがあるから最新の言語を覚えたいと思っていることが多く、こういう面子は致命的である。何か一つの言語を極めていれば普通はこういう発想にならない**)**

■使ってはいけない差別用語

・茶坊主　　使えないセールスやサービスエンジニア
・**SE /** コーダー　　**IT**エンジニアのランクが低い。コーダーは職業プログラマなら聞こえがいい。
・くすぶり　　うだつがあがらない人のこと

逆にすごい天才級のエンジニアはアーキテクトと呼ぶが、日本政府がいうアーキテクトは眉唾レベル

機密保持誓約書(第三者による緊急対応様式)

□はすべてチェックしてください

日付・期間

■甲・緊急対応を依頼する者

施設名　　担当者署名

■乙・緊急対応を行う者 (インボイス番号:　　)

企業名　　責任者署名

乙は甲の依頼により、＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿を行うにあたって以下に示された機密保持規定を遵守することを約束します。

□原則

・乙は甲の許可なく、施設内のデータの複製、および持ち出しをしない。
・乙は甲の許可なく、遠隔管理ソフトウェア(いわゆるバックドア)の設置を行わない。
・乙は前項の許可を得てバックドアを設置した場合、必ず本紙に記すか書面で甲に報告する。
・バックドアの設置が一時的なものである場合、必ず削除しその旨を本紙に記すか書面で甲に報告する。

□失敗を想定する

・乙は作業を断念することになった場合、着手前の状態を再現あるいは説明することを想定し、現場の状態を写真あるいは文書、動画として保管する。乙は甲の求めに応じてこれをその場で提供する。
・乙と甲は各々、問題源とされる設備のメーカーおよびその関係者の関与が途中から必要となり、費用が発生した場合、および以後の修理を拒否された場合の責任の所在について事前に協議する。
・乙は問題源とされる設備のメーカー、関係する技術者あるいは弁護士、裁判所の求めに対し、甲の許可なく作業内容について証言をすることができるものとする。

□進め方

・はじめに、甲は乙に対し、可能な限り正確に問題の内容を説明するように努める。
・次に、甲は乙の正確な資格を確認する。正確な資格とは(1)身分を偽っていないこと、(2)今回の作業内容が勤務先から許されている職務であることの両方である。
・甲は乙が作業している間、必ず甲あるいは施設の関係者が作業に立ち会うものとする。
・乙は作業の成否に関わらず、発生から30日以内に法定保存文書の保存規則に従って報告する。
・甲は乙から提供された前項の報告を法定保存文書の保存規則に従って保管する。

報告欄　日時　　□作業の成否　成功　失敗　途　　□バックドア　　設置した　　削除した
□病院の経営あるいは顧客のプライバシーに関わるデータを持ち出していません

業者相手のNGワード集

■知らない値段はまず「聞く」こと。

値頃感がずれていると業者を敵に回してしまう。誰も相手しない病院は国内にいくつもある。

❌ こんな小さいサーバーが何十万もするのはおかしくないか?

❌ ACアダプタとかケーブルとか数百円程度のものでしょ?

❌ パソコンは買いきったらずっと面倒見てくれるものなんじゃないの?

❌ 機械に弱い、と言えば甘えることができる

❌ スタッフの若い女の子が代わりに電話して泣きべそかけばなんとかなるだろう

○ ～っていくらくらいするものなの?

■気持ちはわかりますが

・たかが画像の表示になんでこんなに金がかかるのですか?

・医療のスキルに比べれば、他の物の価値はすべて大したことない

・それ(VPNの接続)ってさ、自転車のパンク修理くらいの仕事では?

・そんな、ちょちょいのちょいの作業なら口ハだろ、普通。　こっちはな、命預かってんだよ

・私たちは医療の勉強に忙しいんです。(そのあと医療用語ずらずら)

■名言(すべて本当にあった)

・フリーソフトウェアってタダなんでしょ?　だったらアフターも全部ただやろ普通

・OsiriXってフリーソフトウェアですよね?・・・Mac買ってきたのでいまから手順全部案内してもらえませんか?

・えーっ呼んだら金とるの!?

・むしろこっちが使ってやっているくらいだよ。こっちが金払って欲しいよ

自分たちも「この子(犬猫など)が何かいつもと違うんです。どこが悪いんでしょうか?」と聞かれたら、一通りの検査を提案するではないですか。

業者はいろいろ見てるんです。

・検査機器の校正をちゃんとやっていない病院があることも

・期限切れの薬を出しちゃう病院があることも

・入院患者の散歩をちゃんとできていない病院があることも

・・・・・・

ネットワーク保守の原則確認

□サービス担当の素性を確認せよ
　□正社員か派遣か
　□院卒か (ネットワークの場合。大学は不問)

　　スピードが勝負なので原語のRFCと英語の論文が読めるくらいは必須です

□セキュリティルーターの導入検討時、素性を確認
　□内部設定は報告されるのか
　□設定を行うのは誰か
　　□提案者 □ルーターメーカー(米国 中国)
　□提案者が持っている資格は何か?

□リース契約の場合は試用期間を求める(売り逃げ防止)
□ネットワーク構成図ははじめに提示しない
　※構成図は機密情報です。

□設定を調べたいからと言ってパスワードを教えたり
□自由にサーバーに触らせないこと(同席せよ)

□機器類には「これは～です」シールを貼ること
□ルーターとハブは予備を用意する

舞台裏: 販売方法のメモ

目的: セキュリティ関連機器を売りさばけ

ターゲット: 医療機関

□求人サイトで募集をかけている病院
□移転のお知らせが出ていればすぐに飛び込め
□決済できる人に会えるか？ 基本は院長夫人→院長

ターゲット分析

□医療機関の小さいところはシステム化が遅れている。
口コミサイトは気にしている
「仕事を後回しにすると利子を払うことになる」という一般論を展開

つまり、その病院には大量の「できていないこと」が山積みになっていて、
能力的にそれを感じている。

しかし、すでに山積みになっているということは、改善する余力はない。

販売方法: アイドマの法則に沿って行う

手順1 (Attention)

□セキュリティ関連の世情(ニュース・事件)の発生を好機と捉えよ

手順2 (Interest) 10分でターゲットを落とすこと

病院のセキュリティが甘いところをとにかく大きく指摘する
□ホームページから取る情報
　□レジストラのところに院長の名前が出ていれば印刷しておく
　□フォームがあればクロスサイトスクリプトを試す
□建物の外からWi-Fiのスキャンをする
□待合　監視カメラの設置状況を確認
□待合　自動受付、自動精算が入っているか?
□部屋に通してから待たせることが多いので、壁にLANポートがあれば、LANケーブルを指してスキャ

Desire

OsiriX

【解説】仮想化技術とは何なのか?

この文書の目的: 仮想化技術を極めてわかりやすく説明します

誰に:　仮想化技術の説明が必要な方向け

左図はMacの上でWindowsXPが動作している画面です。

Windowsでしか動かないソフトはMacでは実行できませんが、それならWindowsごと実行してしまえばどんなソフトも実行できるようになるんでは?

というように例えばOSの上でOSを実行する技術が仮想化技術と呼ばれるものです。

もともとは大型コンピューターで銀行や防衛システムを停止させないようにするために開発された技術ですが今日のパソコンでも実装できるようになったのです。

しかも現在の技術レベルでは、複数のOS(仮想マシン)を実行することができます。

左はWindowsXPの上でWindows98と、WindowsNTを同時に動かしている例です。

・ネットワークに接続すれば他のパソコンからは
　3台に見えます
・実行速度はそれほど低下しません
・もちろんベースになっているXPも普通に使えます

これらの実体は、親機(この場合XP)のディスク内にある、仮想ディスクというファイルです。容量はそれなりに大きく個々のディスクサイズ分必要ですが98だと64MB, NTでも1GBもあれば十分なので今では大した負担になりません。

メリットは数多くあります。

上の2例の意味は言うまでもありませんが、他にもウィルスが感染している状態を親機から調べて駆除に生かせますし、数十台ものサーバーのインストールもダビングするだけ。OSそのものの開発時間を短くすることも可能になります。

でも最大のメリットはタイムスリップと言えるでしょう。今日、再インストールや復元作業は容易ではありません。親機からはただのファイルですから、日頃複製することでその時点の仮想マシンの状態がまるごと保存でき、不測の事態でも最後のシステムの状態に戻せるわけです。

もし世界が仮想化されていれば、医療で治療法の重大な選択ミスがあっても、大災害や大事故、果ては核戦争があっても平気なんですが・・・。