令和3年度日本水道協会関西地方支部水道実務講習会

サイバー攻撃の現状と サイバーセキュリティ対策

立命館大学情報理工学部
上原哲太郎

1

自己紹介

- 1995 京大院博士退学
- 1996 和歌山大学講師
  - 情報処理センター勤務
    学内ITインフラ担当
  - 同時に地元自治体の
    情報セキュリティ対策支援を
    始める（住基ネットがきっかけ）
- 2003 京大院工助教授
  - 附属情報センター勤務
    事務情報化を担当
- 2006 京大学術情報メディアセンター准教授
- 2011 総務省技官（通信規格とセキュリティ）
- 2013より現職

Beyond Borders

2

2021年10月3日 和歌山市の水管橋落橋

- 復旧は早かった！
  - 10月5日工事着手
    →10月8日応急工事完了
    10月9日給水開始
  - 仁坂知事10月13日blog

「全国から168台の給水車が集まってくれました。松井一郎大阪市長率いる日本水道協会関西地方支部のご協力で全国から来てくださった方々、それに給水車を20台も出してくださった信太山の連隊を中心とする自衛隊、もちろん県内から応援に来てくださった給水部隊の皆さんに心から感謝します」

https://www.yomiuri.co.jp/local/wakayama/news/20211009-OYTNT50237/

Beyond Borders 3

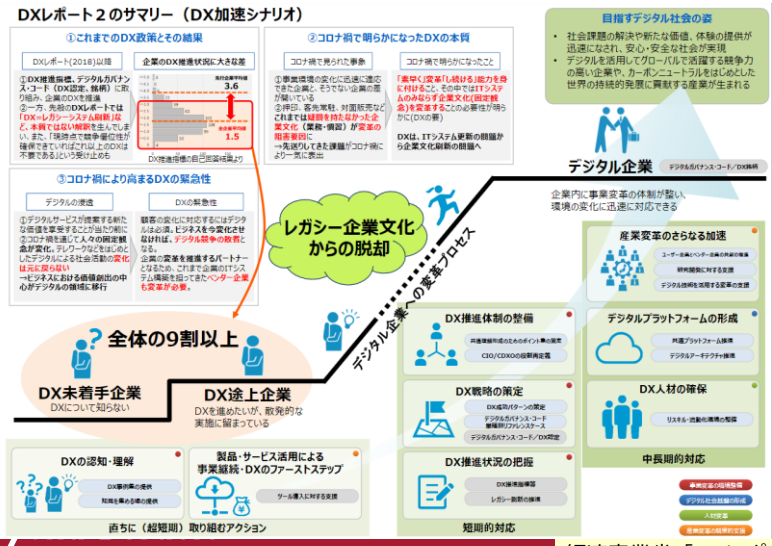
しかしこれは？

https://togetter.com/li/1784485

- 原因は吊り材の破断を目視点検で見逃し
- 目視では死角になり難しかったが…
- Googleストリートビューは捉えていた
  - デジタル技術を使えば事前に分かったはず
- これも「デジタル敗戦」

Beyond Borders 4

デジタル・トランスフォーメーション(DX)

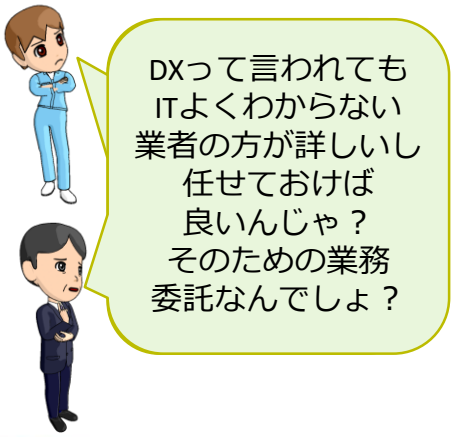


経済産業省「DXレポート２」

インフラ分野も負けていない

R3.2.9 国交省「インフラ分野のデジタル・トランスフォーメーション施策」

DXは現業部門だけではなく 事務も含め総体的に進めるべき



事務職員も
技術職員も
ITとなると…

- **担当者任せにする**
- **業者任せにする**

DXは業務と
ITの融合で進む
各自の主体性が
とても重要

しかし…ITには事故がつきまとう

- 三菱電機　連続するサイバー攻撃被害
  - 2019年6月　防衛機密の漏洩につながる流出
  - 2020年11月　クラウドから顧客情報流出
  - 2021年10月　子会社から顧客情報流出
- カプコン　大規模なランサム攻撃被害
  - 2020年11月　システム障害
    - 流出データがTorのOnionサイトにて公開される被害
- 富士通　情報共有ツールに不正アクセス
  - 2021年5月　政府情報システムの情報が流出
    - 実際には2018年ごろから被害を受けていたと判明
- パナソニック　サイバー攻撃で情報流出
  - 2021年11月発表　被害は6月から

事業への影響は深刻

- 2017年WannaCryマルウェアでは世界中で操業停止など事業への影響
  - 日産英工場が被害　ルノー含め2日間操業停止
- オリンパス 2021年9月ランサム攻撃被害
  - 欧州・中東・アフリカ地域での事業を一時停止
  - 10月　北米でも一部事業停止　復旧に1ヶ月
- ニップン　ランサム攻撃で業務マヒ
  - 第1四半期　第2四半期の決算報告を延期

中小企業や組織は被害甚大 一気に事業がマヒする

- 地方公立病院を次々襲うサイバー攻撃

2018年10月
奈良・宇陀市立病院


宇陀市立病院がランサムウエア被害、身代金は支払わず

2018/10/25 15:00

日経XTECH

奈良県の宇陀市立病院は2018年10月23日、10月1日に導入した電子カルテシステムがランサムウエアに感染したと発表した。セキュリティーリサーチャーのpiyokango氏によれば、国内の病院では、公表された被害事例として、初のランサムウエア被害だという。

ランサムウエアに感染したのは、電子カルテシステムのサーバーと一部のクライアントパソコン。サーバーには、10月1日から15日までに来院した3835人の診療記録が保存され、ランサムウエアによって1133人分のデータが暗号化されていた。病院担当者は、「感染に気付いたのが早かったため、すべてのデータが暗号化されなかったとみている」という。またクライアントパソコンの多くは業務時間外で電源が入っていなかったため、感染を免れたとしている。

https://medical.nikkeibp.co.jp/leaf/mem/pub/hotnews/int/201810/558453.html

2021年7月
東大阪医療センター


東大阪医療センターが不正アクセス被害、医用画像に閲覧障害

https://cybersecurity-jp.com/news/55199

2021年11月徳島
つるぎ町立半田病院


MBSNEWS

『手作業でカルテを…』サイバー攻撃受けた病院の現在“犯人の要求には応じない”決定

速報 サイバー被害の病院が守る“地域の命”

先月31日 午前0時半

“ウイルス”の攻撃を受ける

https://www.mbs.jp/news/kansainews/20211129/GE00041282.shtml

社会インフラは常にサイバーテロの標的になっている

- 2008年トルコで石油パイプライン爆発
  - ネット接続された監視カメラ経由で制御系に侵入して管内圧力を上昇させる
- 2010年イランのウラン濃縮施設を狙ったマルウェアが発見される(Stuxnet)
  - ネットから遮断されていたがUSBメモリ経由？で侵入しウラン濃縮を妨害
- 2015年ウクライナでサイバー攻撃による大規模停電が発生
- 2016年米国バーモント州の電力会社がロシアからの攻撃によるマルウェアがシステム内に侵入していたと発表
- 2021年5月米国コロニアルパイプライン社がランサム攻撃により１週間の操業停止に追い込まれる同社は東海岸の燃料供給の45%を担っており大きな影響

水道への攻撃も度々話題になる

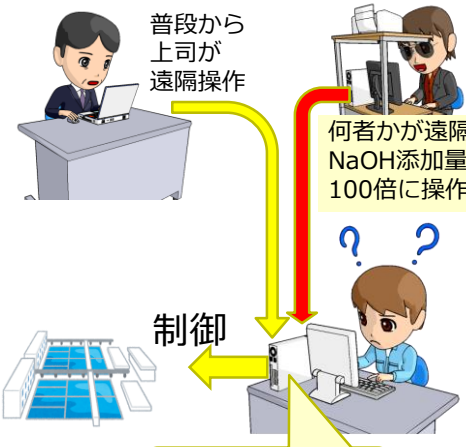
水道施設に「毒混入」狙ったサイバー攻撃、お粗末すぎるセキュリティーの恐怖

2021.02.24

https://xtech.nikkei.com/atcl/nxt/column/18/00676/021700072/

- 2016年米ベライゾン社米国内の水道施設への攻撃を報告
- 2020年米水道協会15件のサイバー被害を報告
- 2021年2月米国フロリダ州オールズマーの浄水場にサイバー攻撃 遠隔操作で水酸化ナトリウムの濃度を変更される
  - 100ppmが11100ppmに

オールズマー浄水施設への攻撃



- TeamViewerで職員同士が遠隔操作し合える環境
- ある職員のPCのカーソルが突然動き出す…
- 上司の操作と誤認して静観したところ
  突然NaOHを100倍に
- 慌てて元に戻し
  遠隔操作を切断
- 原因：
  - Windows 7
  - ファイアウォールなし
  - TeamViewerの
    パスワードが全員同じ

しかしセキュリティ確保しようにも それぞれ言い分がある

- 経営層
  「ITは金食い虫　セキュリティは上乗せコスト」
  「セキュリティ頑張ると業務効率が下がる」
  「せっかく予算つけてやったのに
  　なんで事故が無くならないんだ」

- 情報システム担当
  「とにかくセキュリティは難しい　よく判らない」
  「業者が勧めてきたその装置本当に必要？」
  「経営層に適切な予算が提示できない」
  「リスクがあるならとりあえず禁止すればいいのでは」

- SIer
  「それなりの予算がないと守れない」
  「守るのは最終的には顧客の責任」

そこに戦略は
あるか？！

システム障害はトップの責任

水道は配水さえ止まらなければ…?

- いわゆる「事業継続計画」は…
  - 地震などの災害時にいかに素早く水道を復旧させるかに力点が置かれている
  - サイバー攻撃事案は考えられていない
- しかしサイバー攻撃で水が止まる恐れはないわけではない
  - トルコで石油パイプラインが破壊された事例
  - 水道でも物理的損傷を引き起こす操作は可能かも知れない
  - DXの進展により水道事業の根幹をITが支えるITが健全でないと事業が遂行できない

攻撃者は「スキのある組織」を狙う
組織の大小はあまり関係ない

愉快犯→思想犯
- 技術誇示目的
- 思想信条の表現

目的を持つ外部犯
- 怨恨
- 金銭目的
- 破壊工作・諜報

内部の事故
- ミス・ポリシー違反

目的を持つ内部犯
- 怨恨
- 金銭目的

Beyond

最近はメインは「金銭」「諜報」の模様

17

外部脅威を知るには「10大脅威」

- 毎年2月頃に発表
- 15年間作られており変遷がわかる
- 2016年以降は組織と個人に分けてランキング
- 最近の上位は固定している

https://www.ipa.go.jp/security/vuln/10threats2021.html

18

昨年順位	個人
1位	スマホ決済の不正利用
2位	フィッシングによる個人情報等の詐取
7位	ネット上の誹謗・中傷・デマ
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求
3位	クレジットカード情報の不正利用
4位	インターネットバンキングの不正利用
10位	インターネット上のサービスからの個人情報の窃取
9位	偽警告によるインターネット詐欺
6位	不正アプリによるスマートフォン利用者への被害
8位	インターネット上のサービスへの不正ログイン

順位	組織	昨年順位
1位	ランサムウェアによる被害	5位
2位	標的型攻撃による機密情報の窃取	1位
3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	NEW
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ビジネスメール詐欺による金銭被害	3位
6位	内部不正による情報漏えい	2位
7位	予期せぬIT基盤の障害に伴う業務停止	6位
8位	インターネット上のサービスへの不正ログイン	16位
9位	不注意による情報漏えい等の被害	7位
10位	脆弱性対策情報の公開に伴う悪用増加	14位

R ランサムウェアとは

- ファイルサーバ等のデータを暗号化し復号と引き換えに金銭を要求する
  - 広義にはデータ暗号化以外の手段を用いてシステムや端末を使用不能にするものも含む
    - 画面ロック・ライセンス無効化など
- 身代金を払っても復号（システム復元）してもらえるかは判らない
- そもそも身代金を払って良いものか？

現在猛威を振るうランサムウェア Lockbit 2.0

- 脅迫文（画面表示する他プリンタに出力）
- 窃取したデータを公開するWebサイト(Torで匿名化され摘発は困難）

ランサムウェアの種類

ばらまき型

無差別攻撃
精度は低い
データが復元できるとは限らない

標的型

標的型攻撃の一環として行われる

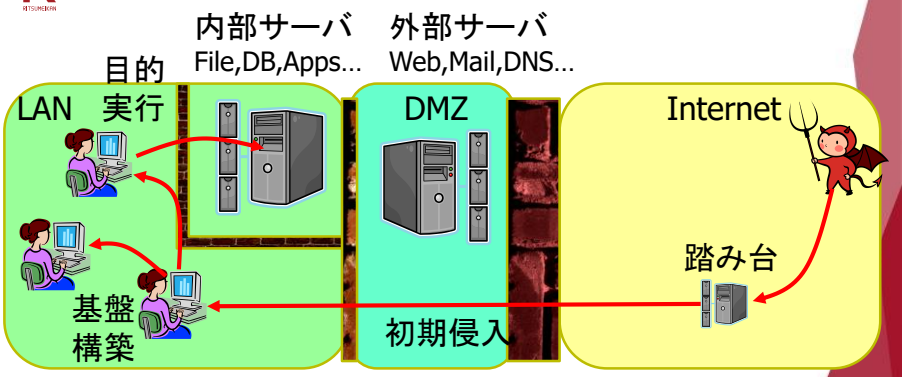
- 証拠隠滅目的
- **金銭目的**

標的型攻撃＋ランサム攻撃

- 攻撃側の組織化が進行
- 主目的は金銭だが諜報を兼ねることも
  - データ窃取も同時に行われる
- 二重脅迫に繋がることが多い
  - ランサムウェアを使わない
    単なるデータ窃取＋脅迫が出てくる可能性

- **基本は標的型攻撃**なので巧妙

標的型攻撃は進化し続ける

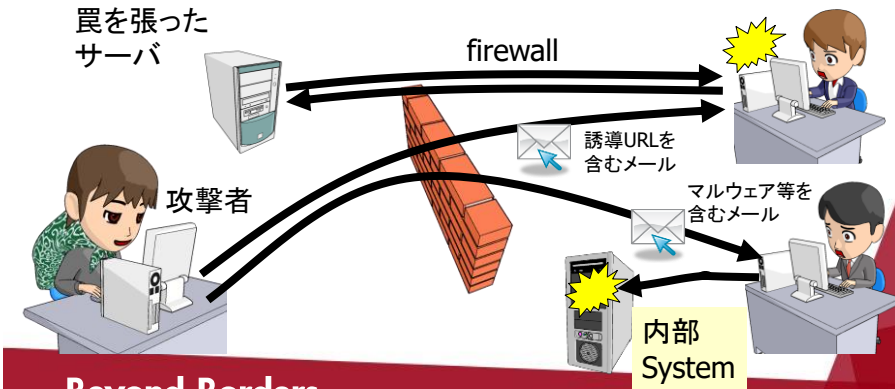


情報収集→初期侵入→基盤構築→内部調査→攻撃先特定→目的実行

- 基本は同じでも環境に対応し続けてる

標的型攻撃のほとんどは E-mailかWeb

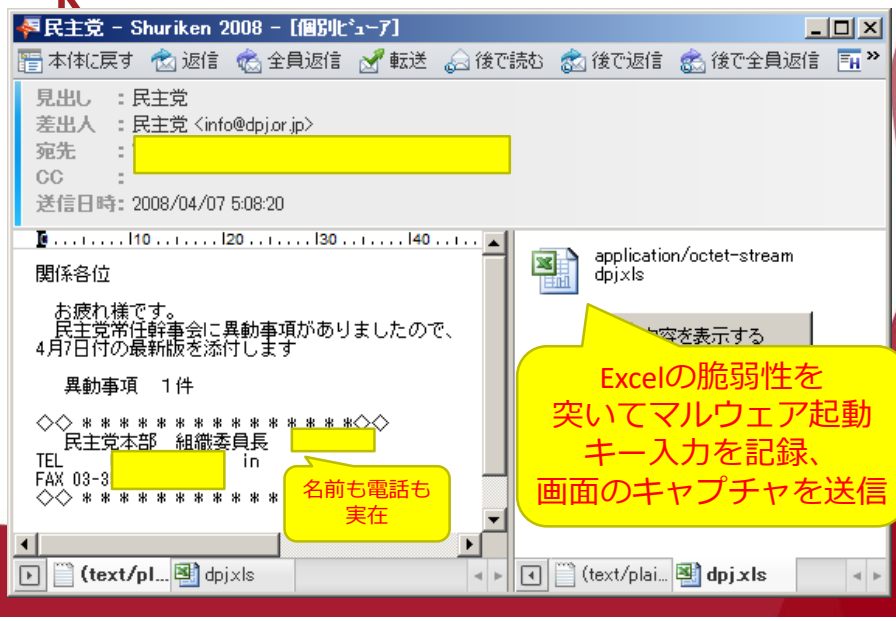
- ファイアウォール(Firewall)では防げない



25

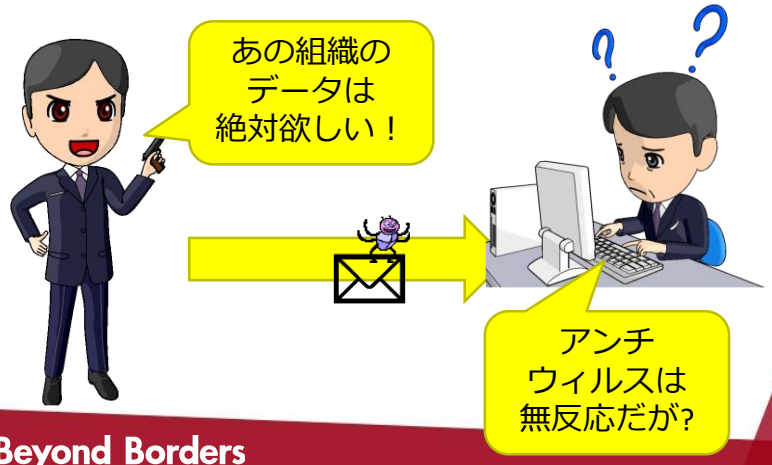
Beyond Borders

メールの日本語が変とは限らない



残念ながら標的型攻撃は「アンチウィルス」が効かない

- 敵は「成功するまで工夫する」



Beyond Borders

攻撃手法の深化

公開サーバの脆弱性を突いた認証回避→侵入

メールの添付ファイルやWebリンク→マルウェア

VPNサーバの脆弱性を突いた認証回避→侵入

テレワーク環境を狙って侵入
- 認証要素を狙う
- BYOD端末を狙う

サプライチェーン攻撃

Beyond Borders 28

標的型攻撃者は テレワークをチャンスと見ている?


狙われた、社内への「接続口」　三菱電機へのサイバー攻撃、ＶＰＮ経由か

有料会員記事

2020年5月8日 5時00分

シェア　ツイート　ブックマーク　スクラップ　メール　印刷

ハッカー集団が三菱電機のネットワークに侵入した仕組み

三菱電機

中国系ハッカー集団

❷19年3月以降、北京、上海など複数拠点のパソコン(PC)やサーバーにウイルス送信

VPN装置

装置から侵入（2019年3月以前？）

日本側に侵入❸（19年4月ごろ）

VPN装置

VPN（社内ネットワークへの接続口）

❹19年4月以降、PCやサーバーにウイルス送信。不正アクセス繰り返す

132台のPCやサーバーがウイルス感染

VPN=仮想プライベートネットワーク

機密や個人情報流出か

ハッカー集団が三菱電機のネットワークに侵入した仕組み

三菱電機 への大規模な サイバー攻撃で、 不正アクセス の起点が「仮想プライベートネットワーク（ＶＰＮ）」と呼ばれる 通信機器 へのハッキングだった可能性が高いことが複数の関係者への取材で分かった。 新型コロナウイルス 対策のため自宅などでの テレワーク が広がる中、ＶＰＮは社外のパソコンを社内ネットワークに接続する手段として急速に利用が進んでいる。（編集委員・須藤龍也、内藤尚志）

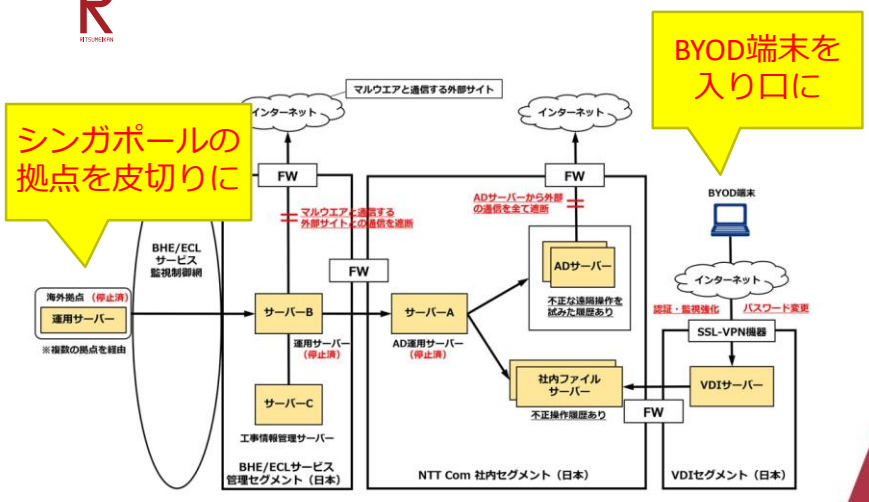
ＶＰＮ装置が外部から不正侵入を受けるリスクについて、米国の政府機関などは今年３月、厳重なセキュリティー対策を講じるよう呼びかけている。

三菱電機 への一連の攻撃では、ネットワークに侵入した中国系 ハッカー 集団「ＢｌａｃｋＴｅｃｈ（ブラックテック）」が防衛に関する機密や個人情報を流出させたとされる。同社が２月に公表した攻撃の概要では、同社の中国にある拠点でパソコンに コンピューターウイルス の感染が広がり、そこから日本国内の本社へ感染が拡大したとしている。

- 海外拠点や協力会社のVPNサーバから侵入
  - カプコン事件も北米から
- これをテコに徐々に国内のシステムに侵入する際にもVPNを活用
- VPNはセキュリティのためのはずなのに

20.5.8 朝日新聞

NTTコミュニケーションズへの攻撃



テレワークに多要素認証の導入を

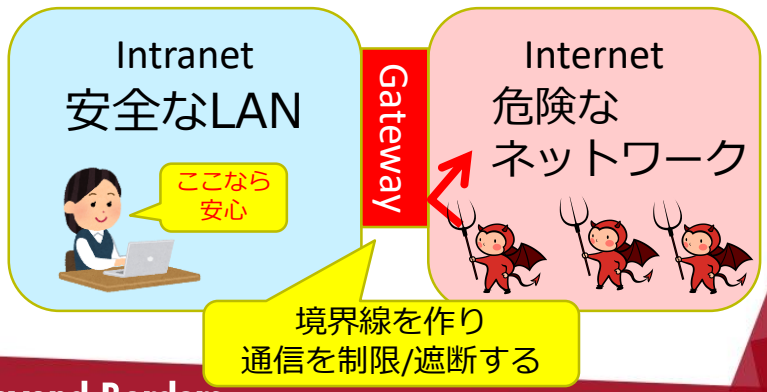
- 以下のうち「2種以上」の認証を使う

- 記憶による認証:Something You Know
  - パスワードや暗証番号など
- 所有による認証:Something You Have
  - ICカードやUSBトークン
    ワンタイムパスワード生成器やSMS/スマホ認証
- 生体認証：Something You Are
  - 指紋認証や静脈認証，顔認証，虹彩認証など

- 最近は「一度2要素に通過するとその機器（パソコン）を2要素目(所有)に設定」が多い

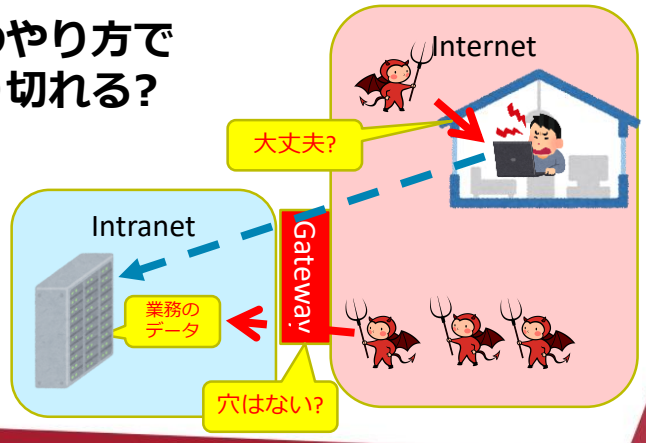
我々がずっと頼ってきたもの

- 境界線防衛モデル
  Perimeter Defense Model



テレワークで開いた「穴」

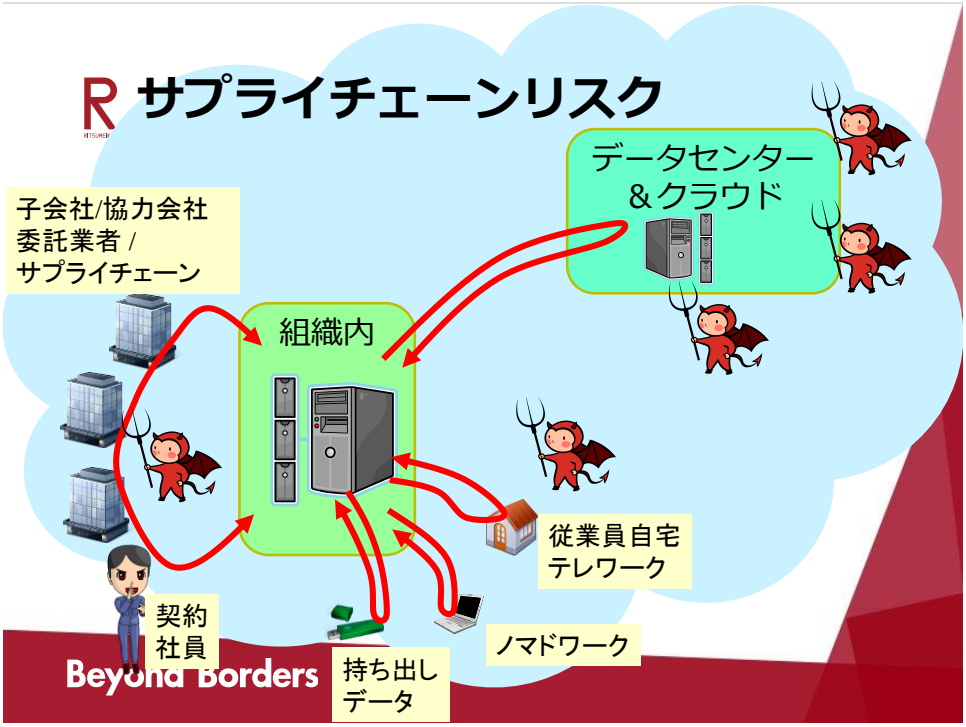
- 境界線防衛の延長の発想が多い
- このやり方で守り切れる?



無知が引き起こす事故

クローズアップ現代＋　2020年11月12日

R サプライチェーンリスク



超高度標的型攻撃
R ：ソフトウェアそのものを改ざん

CNET Japan ＞ ニュース ＞ 企業・業界

米政府などへの大規模サイバー攻撃、SolarWindsのソフトウェア更新を悪用

Catalin Cimpanu （ZDNet.com） 翻訳校正：編集部 2020年12月15日 11時46分

PR | Google Cloud が提案する、業務最適化とイノベーションの実現
PR | 導入事例、製品情報、調査・レポートなど、ホワイトペーパー多数掲載

国家の意を受けているとみられるハッカー集団がSolarWindsのソフトウェア「Orion」のアップデートをトロイの木馬化し、世界各地の企業や政府のネットワークを攻撃していると、米セキュリティ企業FireEyeが米国時間12月13日に発表した。

FireEyeの報告に先立ち、Reuters、The Washington Post、およびThe Wall Street Journalは13日、米財務省と米商務省の国家通信情報管理局（NTIA）が不正侵入の被害を受けたと報じていた。

SolarWindsに対するこのサプライチェーン攻撃は、FireEyeが先ごろ明らかにしていた同社ネットワークへのハッキング被害にも関連しているようだ。

The Washington Postは、情報筋の話として、他の複数の政府機関も影響を受けたと報じている。

またReutersによると、国家安全保障会議（NSC）は事態を重くみて、前日の12日に大統領官邸で異例の協議を行ったという。

The Washington Postの取材に応じた情報筋は、今回の攻撃を「APT29」と関連づけた。APT29とは、ロシアの対外情報庁（SVR）と関連するハッカー集団に対して、サイバーセキュリティ業界が使っているコードネームだ。

- まず米国政府が使うソフトを調べ、開発過程のどこかに入り込んだとみられる
- 「出荷時に」既にソフトがトロイの木馬に

36

セキュリティサービスを狙う攻撃

お知らせ

当社ネットワークに対するマネージド・サービス・プロバイダを経由した第三者からの不正アクセスに係る件

2020-12-11

三菱パワーは、当社のネットワークがマネージド・サービス・プロバイダ（以下「MSP」という）を経由した第三者による不正アクセスを受けたことを確認いたしましたのでお知らせします。
本年10月2日に、当社のパソコンにおいて不審な挙動を検知し、三菱重工と連携して調査を開始しました。詳細内容を確認したところ、翌日にかけて複数のサーバ/パソコンから外部に不正通信があることが判明したため、当該機器をネットワークから遮断する等の初動対策を直ちに行った上、通信ログ等の解析を開始するとともに、関係各所へ通宣、報告を行ってまいりました。
社内調査の結果、本事案において、機微な情報や機密性の高い技術情報、取引先に係る重要な情報、個人情報の流出は確認されませんでした。
また、当社サーバ/パソコンを通じた当社以外の三菱重工グループのネットワークへの不正アクセスは認められませんでした。
関係者の皆様にご心配をおかけしたことをお詫び申し上げます。情報セキュリティ対策および監視体制の強化を今後も継続してまいります。

【確認された不正アクセスの概要】
1．経緯

9/7	攻撃者は、MSPを経由して当社のサーバ1台に不正にアクセスしてマルウェアを感染させ、9/11にかけて当社内のネットワークを偵察。
9/11	攻撃者が感染拡大活動を開始

- 三菱パワーにマネージドサービス経由で侵入
  - 日立システムズ
- 被害は他社でも

BEC:ビジネスメール詐欺
Business Email Compromise

ＪＡＬ３．８億円詐欺被害　ビジネスメールに割り込み偽請求【サイバー護身術】

2018/01/10 10:30 サイバー護身術

日本航空（ＪＡＬ）がビジネスメール詐欺に遭い、約３億８０００万円をだまし取られた。警視庁が詐欺容疑で捜査しているという。ＪＡＬか取引先のパソコンをウイルス感染させてメールを盗み見たり、メールアカウントを乗っ取ったりする手口が使われた可能性があると、専門家は指摘している。（ＩＴジャーナリスト・三上洋）

通称はＢＥＣ　スカイマークでは未遂

ＪＡＬは昨年１２月２０日、偽の請求書メールにだまされて約３億８０００億円の被害に遭ったと発表した。

この話の本質は結局標的型攻撃

フィッシングかマルウェアで一方のメールが覗き見られてる

BEC対策よくある間違い

- 「怪しいメールに気をつけよう」
  「なりすましメール対策をしよう」では防げない
- BECは
  「相手のメールシステムそのもの」が
  乗っ取られて起きる例が多い
  - フィッシングかマルウェアが多い
  - 攻撃者は取引関係のメールを読んだ上で
    偽メールをそのシステムから送るので
    メールは自然だしなりすまし対策も役に立たない
- 取引先のアカウント乗っ取られて
  ないことが大切
  - 多要素認証やフィッシング対策が
    ちゃんと取られているか相互に確認を

スマホなど「モノ」でログイン
→パスワード等との二要素認証へ

Beyond Borders

結局どうすれば良いのか？

- 限られた予算の中で
  必要な対策を打つため
  事業とセキュリティ対策の
  バランスは重要
- そのため
  「今組織にとって
  　何がリスクか」を
  見極める必要がある

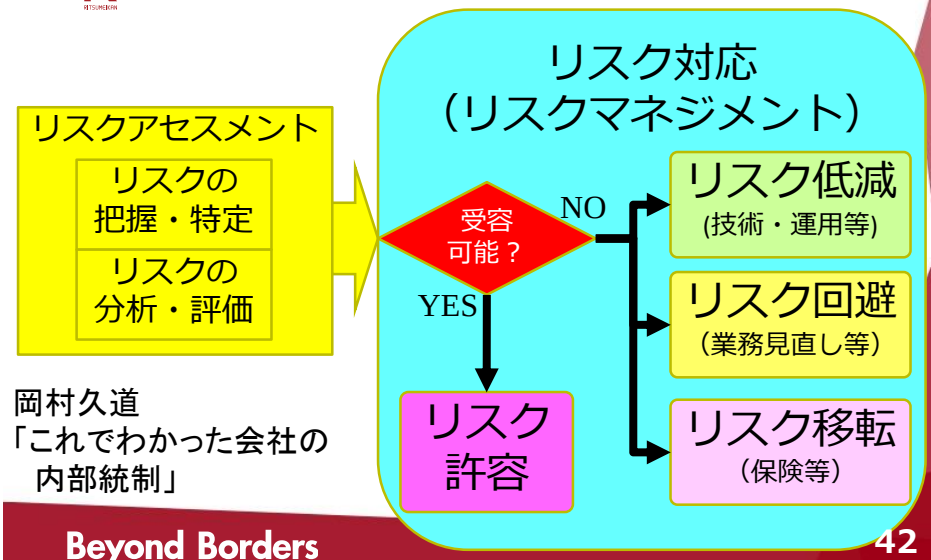
Beyond Borders

40

まず緊急にやるべきこと

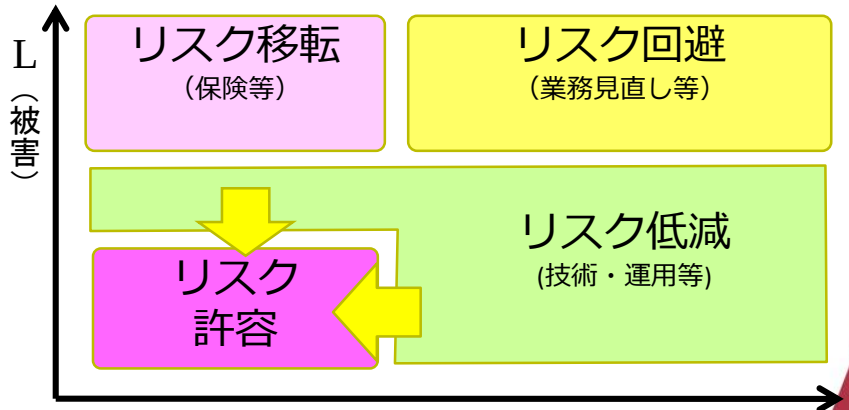
- よくあるソーシャルな手口の啓蒙
  - フィッシングによるパスワード窃取
  - サポート詐欺等による遠隔操作マルウェア導入
- 基本的技術対策の徹底
  - OS等ソフトウェアは最新に保つ(Win7問題等)
  - Windows Updateなど脆弱性対策を迅速に
    - 素早い検証　素早い展開
  - マルウェア（ウィルス）対策は最低限行う
- 早期展開できる技術をまず導入
  - 二要素以上の認証を展開

リスクの把握と評価



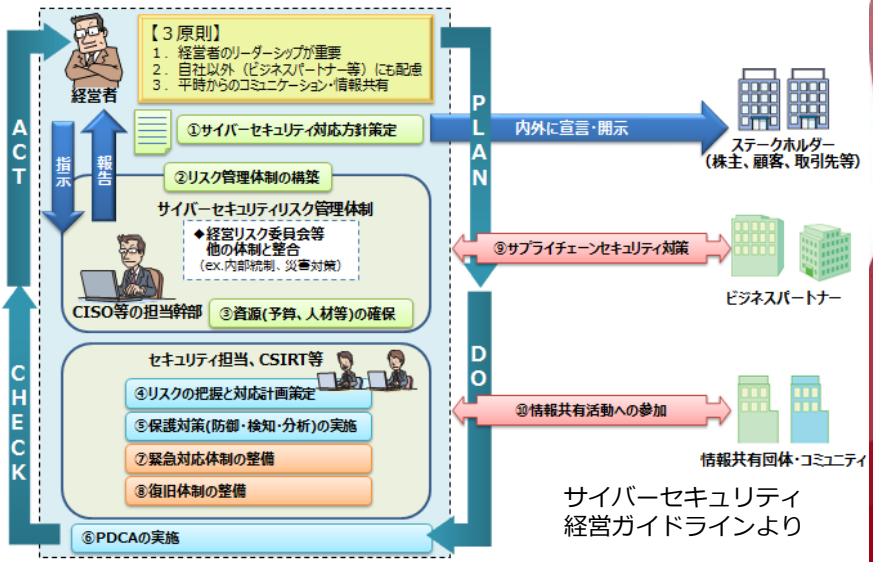
岡村久道
「これでわかった会社の
内部統制」

リスクの大きさ・確率と対応の関係



佐々木良一:「ITリスクの考え方」より

立て直しはまずはガバナンスから



サイバーセキュリティ
経営ガイドラインより

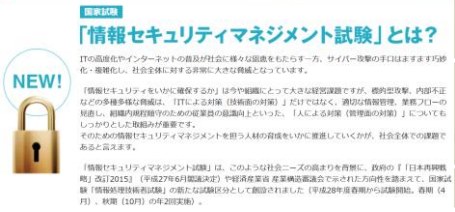
サイバーセキュリティ経営ガイドライン Ver 2.0

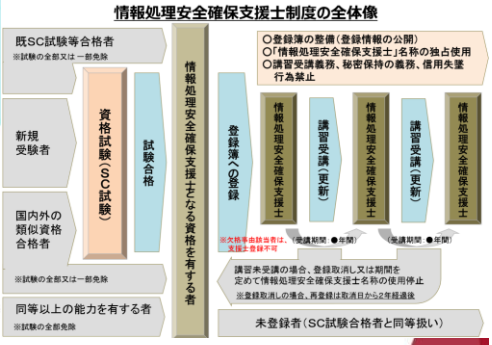
- サイバーセキュリティ経営の３原則
  1. 経営者は、サイバーセキュリティリスクを認識し、**リーダーシップによって対策を進める**ことが必要
  2. 自社は勿論のこと、ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策**が必要
  3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、**関係者との適切なコミュニケーション**が必要

これに沿った重要10項目を提示

セキュリティそのものを投資と捉えるべきとする記述を強調
リスクマネジメントの考え方を明記

情報セキュリティマネジメント試験 情報処理安全確保支援士





あたらしい資格試験
より経営サポートをする層を創出

従来の情報セキュリティスペシャリスト
試験合格者を中心に「士業」に登録・更新制を採る

この辺が情報漏洩保険等に効いてくる　リスク対応力向上にも？

運用でカバーは現場に負荷が高い

アクセス制御が厳しくて手順が増えた
添付ファイルは必ずパスワード？
忙しいのに研修やらe-Learning必修
上司への報告や承認も増えたし
とにかく何かと窮屈になった

別に私、悪いことしようと思ってないのに信用されてない感じがイヤ…

ロイヤリティを下げては逆効果！
セキュリティ向上はシステムで！

そもそもどうしてIT化してるのに効率が落ちるのか

- ルールを決めるのはいいが**実装がひどい**
  監査要件を満たすためだけのものが多い

メールの暗号化はzipのパスワードでいいんじゃ？

毎度毎度違うPWを考えていちいち別便で遅れって?!

ルーチンワークはシステム化しよう！

R 本当に必要なのは何か？

- 情報システム全体を
  最初からセキュリティ対策しておくのは
  もちろんのこととして・・・
- 「仕事のやり方」を変えて効率化を
  - いつまで情報機器を清書機にするのか
    いつまで「印鑑文化」を維持するのか
  - 可能な限りのシステム化を！
- セキュリティ対策で
  「業務効率が常に下がる」のは本末転倒
  「結果的に業務効率が上がる」ことを示し
  「業務のやり方を変える」ことを
  現場に受け入れさせられるかが勝負では？！

Beyond Borders 49

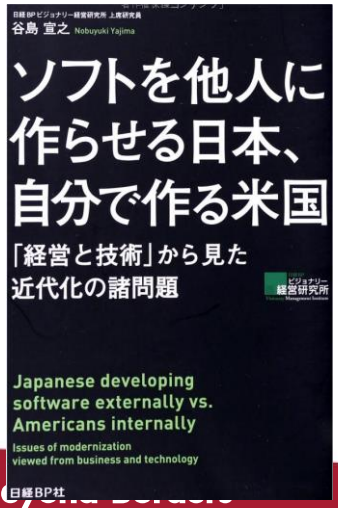
脆弱なのはシステムではなく「人」
R 人にデータを食わせるWebとメール

- 狙われているのは人が直接データを扱う機会
  内部犯行でもサイバー攻撃でもリスク
- 業務フローを見直してシステム化すれば
  セキュリティが向上し業務効率も上がる！

いうのは簡単だが現実は厳しい　例外処理…業務量…

Beyond Borders 50

「技術経営の貧困」から抜け出す



- ユーザ企業・組織こそがIT人材の活用を考えるべき

米国ではIT技術者の6割はユーザ側に在籍
日本ではITサービス企業に7割以上が在籍
（IPA調査 2009年）

まとめ

- セキュリティ対策は必要だが「べからず集」の作成に終始して事業効率の足をひっぱるべきではない
- インフラ部門でもDXの波が来るそれは業務フローの見直しと「効率的かつ安全」なシステムの構築が不可欠
  - とりあえず「メール」が最大のリスクなので「ファイルの送信者が確認できる手法」での授受を
- セキュリティ事故は絶対防げない！脅威の「見える化」は早期発見のためのもの
  - セキュリティ事故の早期検出に投資を
- その対応のためにも「内部人材の育成を」