サイバー戦国絵巻
～ 技術と社会の攻防史 ～

NTTデータ先端技術株式会社　浅田祐介
デロイトトーマツサイバー合同会社　北野 晴人
株式会社LASINVA（在籍当時）茶園太志
NTTデータ先端技術株式会社　羽田久美子
日本オラクル株式会社　リャン ジェニールウ
日本オラクル株式会社　大澤 清吾

データベースセキュリティWG

はじめに
本書の目的と狙い

本書は、サイバーセキュリティに関する技術の変遷、社会に衝撃を与えた事案、さらには法制度に影響を及ぼした事例について解説する資料である。また、本書はセキュリティ攻撃の技法や対応方針に関する知見を、専門家ではなく一般読者を対象として提供することを目的としている。

第5章では、実際に発生した事例を取り上げ、調査報告書の内容を簡潔に要点を整理した形で解説する。各事例の詳細については、原資料である調査報告書に記載されているため、必要に応じて参照されたい。

サイバーセキュリティの重要性を認識している読者も多いと考えられるが、一方で、さまざまな制約のもと十分なセキュリティ対策を講じることが困難な組織が多いのも事実である。本書は、繰り返されるセキュリティ・インシデントに対する警鐘の意を込めて記載している。

過去の事例を振り返り、現在も発生し続けるサイバーセキュリティ上の課題について、読者自身が考察を深める契機となることを期待する。

目次

自己紹介：
本書執筆メンバー

株式会社LASINVA（在籍当時）

茶園 太志

デロイト トーマツ サイバー合同会社

北野 晴人

日本オラクル株式会社

リャン ジェニー ルウ

NTTデータ先端技術株式会社

羽田 久美子

NTTデータ先端技術株式会社

浅田 祐介

日本オラクル株式会社

大澤　清吾

第 1 章

セキュリティに際しての本書の目指したこと

セキュリティとサイバー攻撃の歴史
2000年以降を中心

2000年以降に発生したセキュリティ事案の増大(深刻化)は増す傾向にあり、近年は金銭を目的としたサイバー攻撃に加え、社会通念を覆す事案、国家安全保障を脅かす状況に至っている状況である。

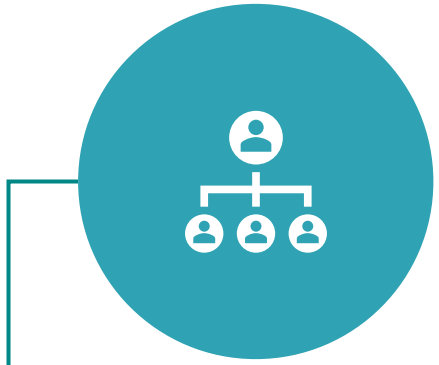
攻撃ツールより、手口の巧妙化が本格化している現代において、我々が目指すべきものが何か？について2章以降で解説する

サイバー攻撃の歴史

	2003	2010	2015	2017	2021
代表的なインシデント	**ワーム.Blaster** • 50数万台のPCが感染 • 世界中で猛威をふるう	**オーロラ作戦** • ゼロデイ脆弱性を用いた、特定の企業を標的とした攻撃	**年金機構情報漏洩** • 不審メールに起因する不正アクセスにより、約100万件の個人情報が外部へ流出した	**ダークウェブ** • 専用のブラウザでしかアクセスできない匿名性が極めて高い環境 • アクセス元の特定が困難であり、犯罪者にとって絶好なツール	**WannaCry** • SMBv1の脆弱性を悪用し、150ヵ国30万台のPCに感染	**米インフラ企業攻撃** • パイプラインを運営する会社がサイバー攻撃を受け、数日創業停止になり、ガソリン供給がストップした
トレンド	世間を騒がせて自己満足する愉快犯が多かった	標的型攻撃という脅威の存在が世の中に知らされるきっかけとなった	標的型攻撃という脅威が一般的に知られるようになった	古くから存在したランサムウェアは攻撃者の絶好のツールになっており、暗号資産・ダークウェブの台頭によるサイバー攻撃が産業化した		サイバー攻撃による重要インフラの被害が社会活動にも影響

本書の狙い
概要と訴求点

本書はサイバーセキュリティの歴史とそれを繰り返す、現代に対する警笛をとりまとめたものであり、以下の3つの観点から考察する。

	①技術の革新	②組織的な課題	③社会的な課題
概要	 2000年以降に発生した事案を技術の多様化や技術革新により巧妙化するサイバーセキュリティ事案について	 技術の過信や旧態依然とした考え方の隙をついたサイバー攻撃を組織的にどのように対処すべきかについて	 世間を震撼させたセキュリティ事案の経験から法律の改定、社会通念の再定義を余儀なくさせた事案について
訴求点	技術の進歩は攻撃者と防御側の双方に恩恵を与えている事実を踏まえて、技術の重要性について解説	技術的な対応に加え、組織全体のリスク管理体制を拡充させることが不可欠であることを解説	セキュリティ事案は個人や企業だけなく、国の安全保障や国益の損失させるリスクを踏まえ社会や法整備の変える事案について説明

第 2 章

技術の革新によって生じた事案

技術の革新によって生じた事案
繰り返される攻撃手法と被害の拡大化

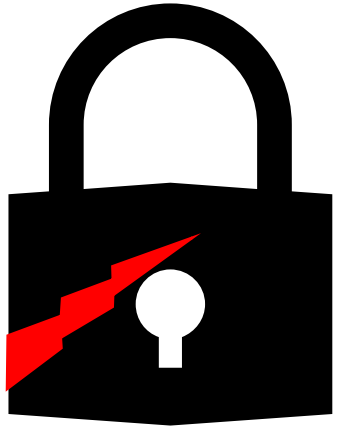
サイバーセキュリティにおける様々な攻撃は、技術の進歩とともに、高度化・複雑化、その結果、被害が拡大化する傾向にある。

一方、人の無防備さを突いて、情報を取得し、大規模なデータ搾取する事例もあり、サイバーセキュリティは高度な技術ありきではなく、個人の意識でセキュリティの脆さを補うことは可能であり、そのためには正しい情報と手法を理解していくのが得策である。

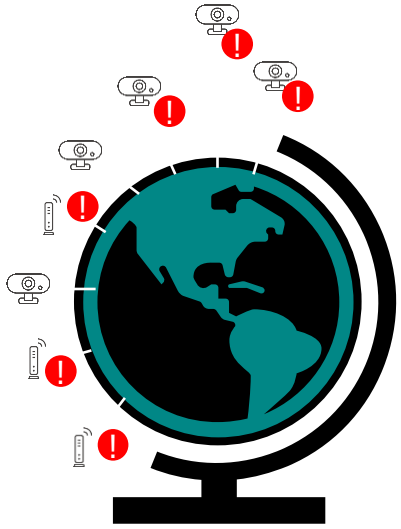
本章では技術に焦点をあてた課題について説明する。

技術の革新によって生じた事案
標的型攻撃の歴史

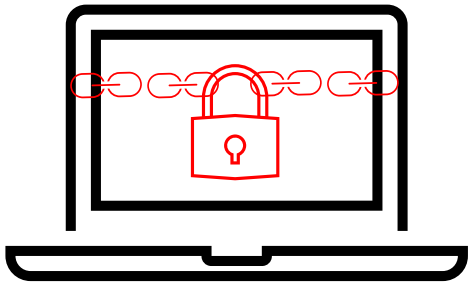
機密情報の摂取などを狙ったサイバー攻撃において利用される攻撃手法の1つが標的型攻撃であり、その攻撃方法は技術の進化とともに巧妙化した歴史を持つ



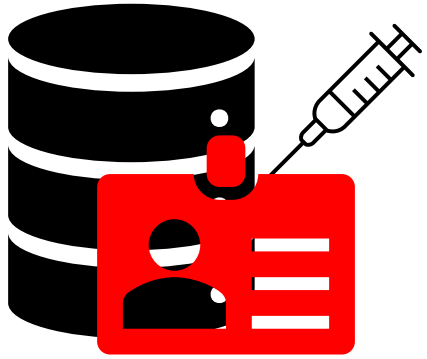
パスワードクラック



DDoS



ランサムウェア



SQLインジェクション

技術の革新によって生じた事案
パスワードクラックの歴史

技術の進化とともに、パスワードクラックの手法も巧妙化してきた。シンプルな推測から高度な計算処理を用いた攻撃まで、その歴史をたどる

汎用から専用へ、進化する計算の波

コンピュータ普及と一般化

総当たり攻撃(ブルートフォース)や辞書攻撃

ブルートフォースは1980年頃から注目された

専用ツール化

パスワードクラックツールの登場

ハッシュ値を逆算するためのツールなどが開発された

知能化する計算、攻防の新時代

AI・機械学習

パスワードクラック手法の高度化

AI・機械学習の進歩に伴い、より精度の高いパスワード推測が可能

攻撃対策の回避

リバースブルートフォース攻撃

一つのパスワードでIDを次々と変え不正ログインを試みるため、アカウントロックが効果しない

連鎖する侵害、拡散するリスク

潜在的な二次被害

リスト型アカウントハッキング

過去に流出したIDやパスワードを用い、複数のサイトで同じパスワードを使いまわしているようなケースでは被害が拡大

アカウント情報が漏洩する事案
ディスクユニオンのユーザーアカウントとパスワードの漏洩（2022年）

オンラインショップに登録されたEメールアドレス、ログインパスワードが漏洩

■ 2022年6月

- 第三者からの情報提供により、漏洩の可能性があることを確認
- 氏名、住所、電話/FAX番号、Eメールアドレス、ログインパスワード、会員番号が約70万件流出した可能性がある
- ４日後にユーザー向けにメールアドレスとパスワードを他社サイトで流用しないように呼び掛ける

パスワードが平文で保存されていたため、奪取された情報を使って、他社サイトへ容易にアクセスを試せる状況であった。同一のアカウント・パスワードを他社で流用している場合には被害が出る。

ユーザーへの呼びかけが即時に行われなかった点が問題視された。

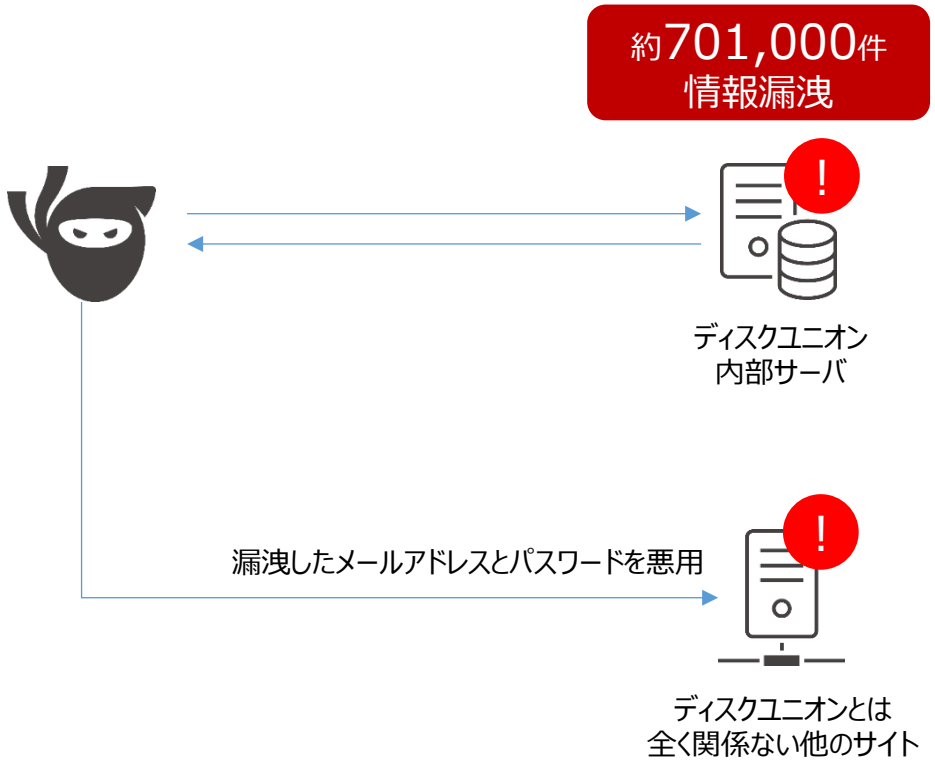


図 情報漏洩イメージ

技術の革新によって生じた事案
DDoS攻撃の歴史

コンピュータの普及とともに始まる	1974年に弱冠13歳の少年が、米イリノイ大学のコンピューター端末を一度にシャットダウンさせたのが、最初の攻撃とされる
インターネットの大手サイトが大規模攻撃が始める	2000年にAmazon, eBay, DELL,等に対する大規模DDoS攻撃 • 金銭的損害は12億ドル相当と推定されているが金銭目的ではなく、自分の技術力を見せつけるために引き起こされた事件だった。 • 大手サイトですらも簡単にサービスダウンさせられる事例として社会にインパクトを与えた
世の中に多数使われるようになったIoT機器が攻撃に使われる	2016年マルウェアMiraiによるIoT機器を使ったDDoS攻撃 • IoT機器がDDoS攻撃に初めて使われた事例
金銭支払いより、誰でもDDoS攻撃が可能になる	DDoSを請け負うDDoSサービスの登場 • 金銭を支払えば、技術がなくても任意のサイトにDDoS攻撃を仕掛けられるサービスが登場した。
マシンパワーが弱いIoT機器を多数乗っ取るよりも少数の強力なVMで効果的な攻撃が行われる	IoTベースのボットネットからより強力なVMベースのボットネットへの移行 • 多くの台数を乗っ取る必要のあるIoT機器を攻撃に使うことから、少数の攻撃専用のVMを使った攻撃で大規模な攻撃を仕掛けることができるようになった。

システム全体が停止に追い込まれる事案
MiraiボットによるIoTを使った攻撃 (2016年)

サーバー、PCに比べるとセキュリティ対策が弱いIoT機器が乗っ取られDDoS攻撃のためのリソースとして利用される事例

■2016年9月の攻撃
- 2016年9月20日セキュリティブログKrebs On Securityが大規模な DDoS 攻撃を受けた。
- 38万を超える IoT 機器この攻撃に利用されたとされる

■2016年10月の攻撃
- DNSサービスの運用会社Dynが攻撃される
- Dynの顧客であった名だたる企業の多くの主要ウェブサイトが一時的に利用できなくなった
(Twitter、Spotify、Reddit、GitHub、Amazon等)

Miraiのソースコードはその後公開され、現在まで多くの亜種が作成されている

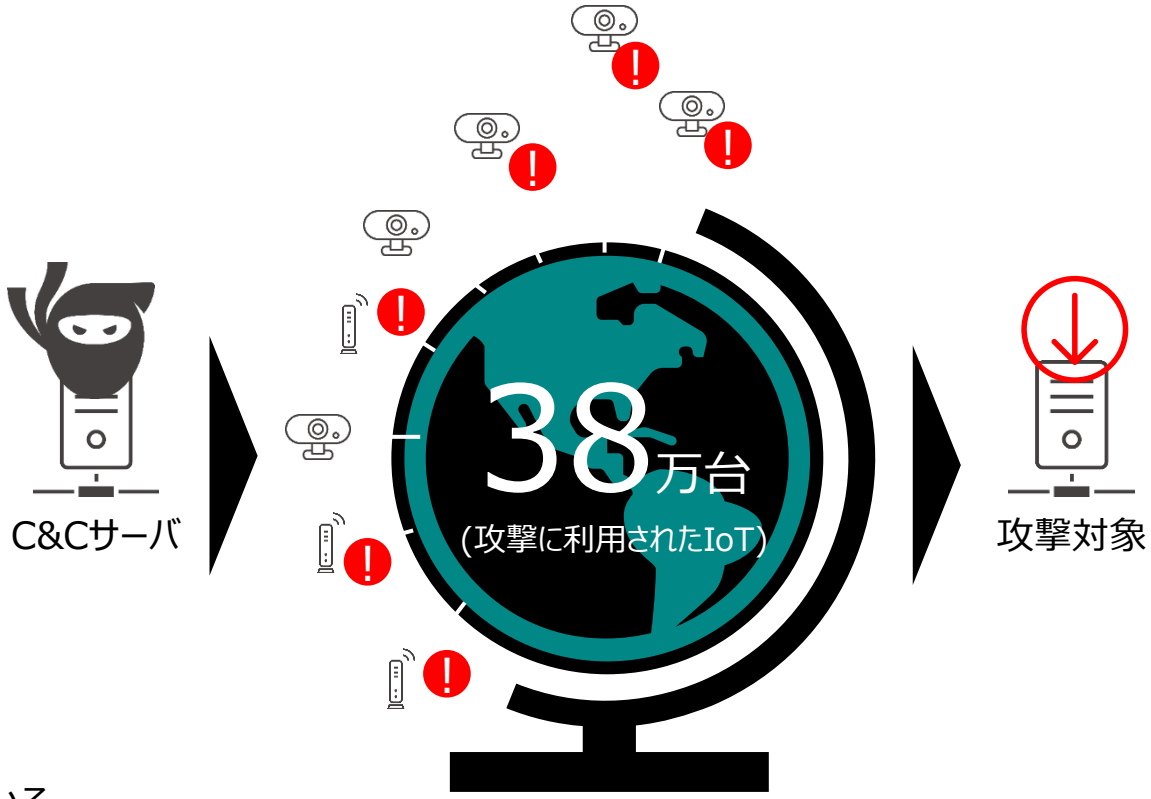


図 Mirai botによる攻撃イメージ

技術の革新によって生じた事案
ランサムウェアの歴史

コンピュータの普及とともに始まる

1989年「AIDS Trojan」
- 配布方法は郵便、送られてきたフロッピーのソフトウェアをインストールするとハードディスクのデータが暗号化されるというもの。そのうえで「身代金を189USD支払え」と脅してくる。研究費用を稼ぐ目的で配布された。

少額の身代金支払いにより
多くの被害者が身代金を支払った

2008年「WinLocker」
- システムファイルを暗号化ロックするもの、身代金は現在のように高額ではなく、5USDから10USDと少額だった。100万人単位の被害者が身代金を支払う。

ビットコインの登場以降、攻撃者の身元秘匿性に
伴うランサムウェアが拡大

2013年「CyptoLocker」
- 現在のランサムウェアの直接の原型といえる。ビットコインを身代金のやり取りに初めて使用したランサムウェア。 5ビットコイン支払えば、実際に復旧が可能であった。

パッチ適用軽視により大規模な被害が発生

2017年「WannaCry」
- 150ヶ国で23万台以上のコンピュータが被害にあった
- 600USD相当のビットコインを要求されるが支払っても解除できた報告はない。

金銭支払いより、誰でもDDoS攻撃が可能になる

2019年RaaS (Ransomware as a Service) を利用した「LockBit」
- ランサムウェアによる攻撃をサービスとして提供・実行するビジネスモデル。

大企業よりもセキュリティ対策が手薄になりがちな
関連企業が狙われるサプライチェーン攻撃

2022年トヨタ自動車の取引先がランサムウェアの被害にあう
- 取引先企業の操業停止を伴ったサプライチェーン攻撃にあたる

システム全体が停止に追い込まれる事案
トヨタ自動車の部品サプライチェーン攻撃 (2022年)

比較的セキュリティ対策が弱くなりがちな企業を攻撃することで大手企業のサービスを停止するサプライチェーン攻撃の事例

■ 2022年2月

- トヨタ自動車の取引先である小島プレス工業が攻撃された
- トヨタの国内全14工場の稼働停止を余儀なくされた
- 攻撃者から、身代金を払わないと重要データを公開すると脅されるが小島プレスは身代金を支払わず、システムを復旧させた
- 工場の停止は１日であったが、500億円ものコストがかかった

重要データのあるところだけではなく、サプライチェーン全体でセキュリティレベルを上げていくことが重要である。

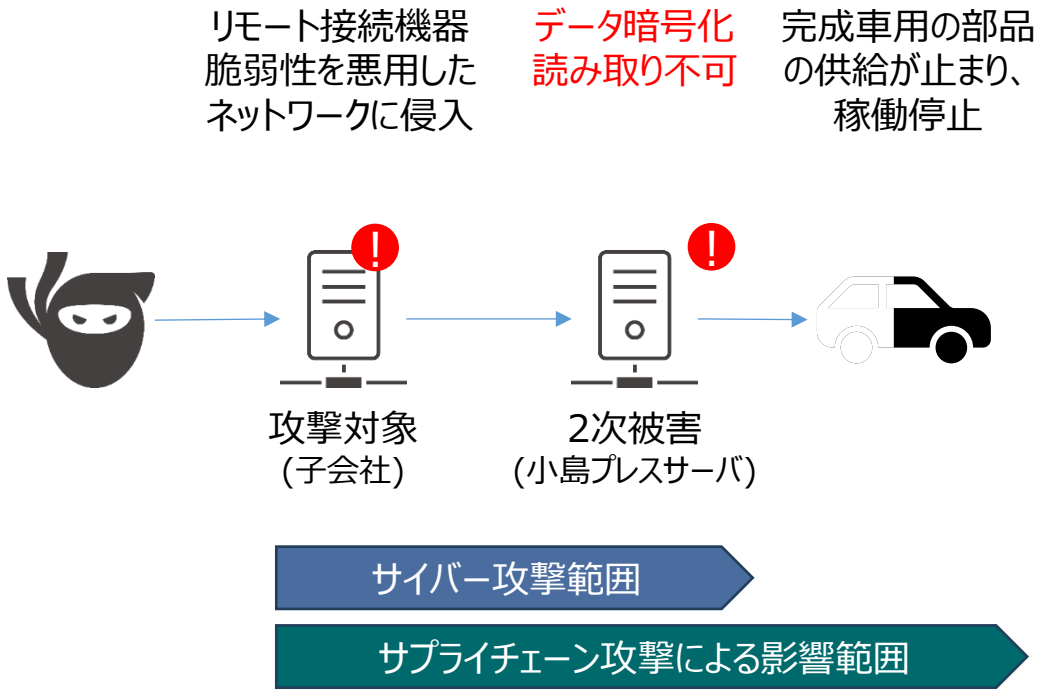


図 サイバー攻撃とサプライチェーンの影響イメージ

技術の革新によって生じた事案
SQLインジェクションの歴史

Webアプリケーションが一般的になった頃から始まる

1998年オンライン・マガジン Phrack に投稿されたJeff Forristal氏 (別名Rain Forrest Puppy) による記事
- 特定のコマンドを入力することによってあるサーバからの情報共有が強制的に停止されることが発見された。

金銭目的の大規模攻撃の発生

2005年
- ➢「価格.com」
  - 「価格.com」を含む14社のWebサイトから、52万件にのぼる個人情報を金銭目的で盗んだ。
  - 金銭を奪取するためにオンラインゲームアカウント情報が盗まれた。

※ 価格.comは同社が受けた攻撃がSQLインジェクションであったかどうか明らかにしていない
- ➢「OZmall」
  - 金銭を奪取するためにオンラインゲームアカウント情報が盗まれた。

クレジットカード情報を盗むケースが多数発生

2010年「モンベル」
- クレジットカード情報が漏洩した。

2013年「エクスコムグローバル」
- 約10万9112件のクレジットカード情報が漏洩

SQLインジェクションが問題となった当初からWAFが対策として有効であったが、いまだに被害はなくならない

2021年
- ➢「サンリオエンターテイメント」
  - 約4万6,000件のメールアドレスが流出
- ➢「メタップスペイメント」
  - 約46万件のクレジットカード情報が流出

データベースの情報が漏洩する事案
メタップスペイメントのSQLインジェクション（2021年）

Webサーバに不適切な情報を入力することで、データベースから本来アクセスできないはずの情報を引き出す事例

■ 2021年10月

- 管理画面のクロスサイト・スクリプティングに関する脆弱性を悪用し、データベース内に格納されていた管理者のアカウント情報 (UserID、パスワード等) を取得
- SQL インジェクション攻撃により、暗号化されたカード番号、マスクされたカード番号及び A 社管理画面の管理者アカウント情報をそれぞれ不正取得した。
- 管理画面上で不正取得したマスクされたカード番号を検索照会することによって、平文のフル桁のカード番号を閲覧

■ 2021年11月

- A社管理画面に不正アクセスを行い、A 社アプリの管理機能 の一つであるファイルアップロード機能を悪用し、バックドアプログラムを設置

カード番号は暗号化されていたが、暗号化されたカード番号を復号可能な管理画面のアカウントが奪取されたため、平文のカード番号が奪取された。

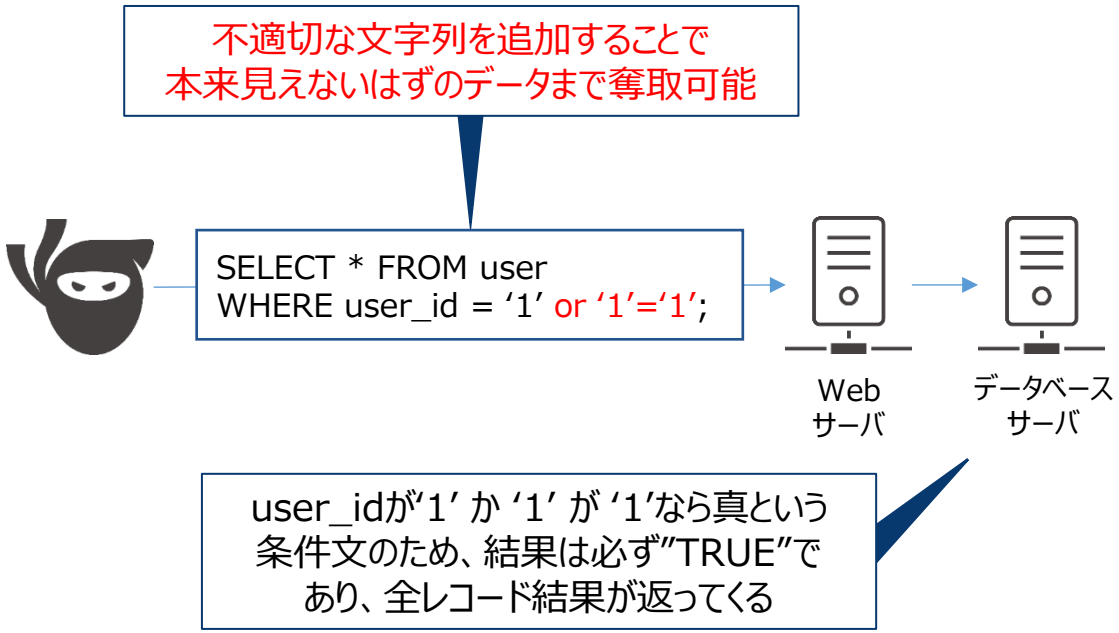


図 SQLインジェクションのイメージ

データベースの情報が漏洩する事案
健康保険大手のAnthemで発生したDBアカウントの奪取（2015年）

フィッシングメールによりマルウェア感染した端末からデータベースアカウント情報が盗まれ、情報漏洩した事例

■2015年1月

- 8000万人を超えるユーザーの社会保障番号・生年月日・メールアドレス・住所・医療識別番号・雇用情報を含む情報が盗み出された
- 顧客からデータ漏洩に関する訴訟を提起され、解決のために1億1500万ドル(約130億円)の費用を払っている
- データ侵害のクリーンアップに約2億3,000万ドルを費やした
- HIPAA(Health Insurance Portability and Accountability Act)にも抵触したため、1600万ドル制裁金が発生

フィッシングメールは1990年代からある、古くからある方式であるが、そこから最終的に最も守るべきDBのログイン情報が盗まれている

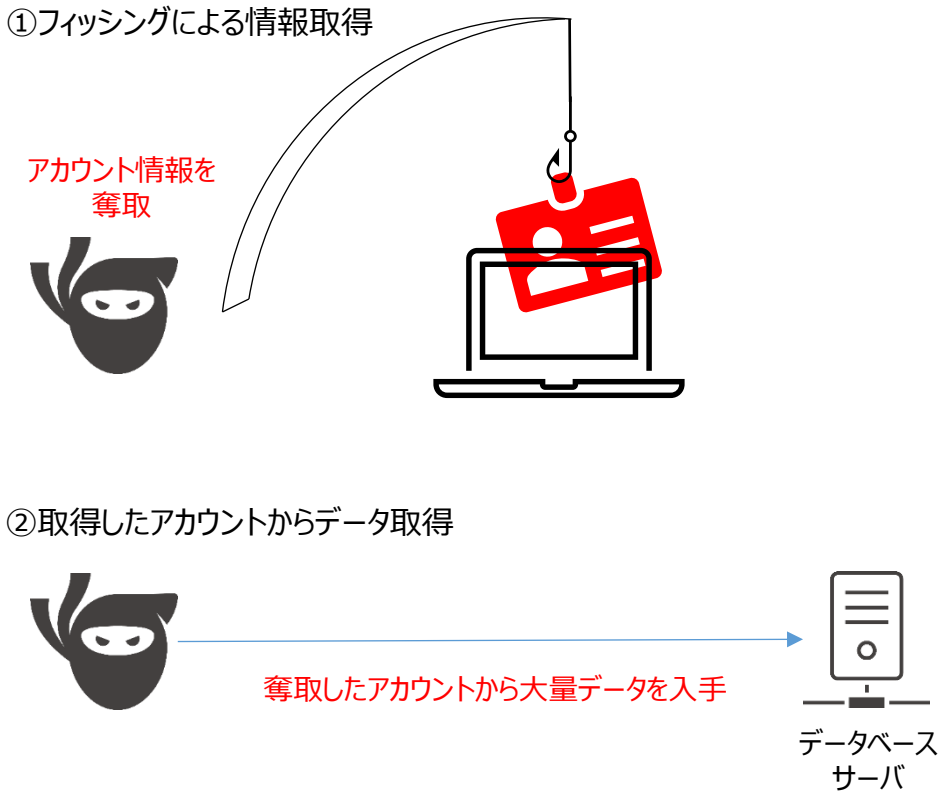


図 フィッシングによる情報入手よる大量データ漏洩

様々な攻撃、技術面での歴史まとめ
繰り返される攻撃手法と被害の拡大化

■ 古くは技術力を見せつけるためなど金銭目的以外の目的が主だったと思われるが、近年では、金銭目的の攻撃が多くおこなわれるようになってきている。ビットコインの登場により、個人情報と紐づけなしで金銭がやり取りできるようになったことも金銭目的攻撃の増加に拍車をかけていると考えられる。

■ 近年では、DDoS攻撃、ランサム攻撃などの攻撃がサービス化され、技術力がなくてもお金を払えば誰でも攻撃者になれるようになってきている。

■ 古くは単一の攻撃手法だけを使っていたが、近年は複数の攻撃手法を組み合わせた攻撃手法が使われるようになってきている

- 人の手によるパスワードクラックから、AI・機械学習を活用したパスワードクラックへ
- あるサイトで奪取したアドレスを他サイトで利用するリスト型アカウントハッキング
- 1台のサーバーを使ったDoSから、複数台の踏み台を使ったDDoS攻撃へ、複数の踏み台もPCを乗っ取ることからIoT機器をボットにより乗っ取ることへ
- SQLインジェクションだけではなく、クロスサイトスクリプティングなどと合わせて重要情報の奪取を行う

第 3 章

組織において生じる課題

組織によって生じた事案
情報セキュリティガバナンス構成要素

本章では組織に焦点をあてた課題について説明する。ここでいう組織とは営利または何らかの目的を持って活動する組織(＝企業等)におけるサイバーセキュリティ事案について説明したい。

一般的に組織におけるセキュリティ統制を浸透させるにあたり、情報セキュリティガバナンス構成要素を取り決め、順守する。
これらを踏まえ業界団体のガイドラインやフレームワークを参照し、それを組織に適用・調整する のが一般的なアプローチとされる。

■ 情報セキュリティガバナンス構成要素

ポリシー	組織の構成員が取るべき行動を宣言する基本方針
スタンダード	基本方針に従い、それらを具体化的に表現した対策基準
プロシージャ	対策基準を詳細・手順化した実施手順
スコーピング	スタンダードの適用基準を定義したもの
テーラリング	適用基準や手順を組織ニーズに合わせてカスタマイズしたもの

必須　任意

■ パスワードに関する基本方針を具体例にすると・・・

- 全従業員は強固なパスワードを使用し、定期的に変更する必要がある。
- パスワードは12文字以上、英大文字・小文字・数字・特殊文字
- パスワード変更手順：従業員は90日ごとに変更
- 管理部門と開発部門のシステムに適用し、外部ベンダーは対象外
- 開発部門はパスワード変更を60日毎多要素認証（MFA）を義務化

組織によって生じた事案
半田病院における調査報告書に列挙されているセキュリティ課題一覧

2021年10月31日に発生した徳島県つるぎ町立半田病院で発生したランサムウェア攻撃について、報告資料ではセキュリティ課題に言及し、これら課題はセキュリティガバナンスを図ることで対処が可能であったと記してある。

半田病院は完全復旧までに約２ヶ月を要したものの、２ヶ月期間中は地域医療を止めることなく、災害対策と位置付け対処したことで、非常に多くの教訓を社会に知らしめた事案となった。

■ 問題視されたセキュリティ課題

端末のパスワードが最小桁数5桁	パスワードのロックアウト設定なし	端末間でパスワードの使いまわし	Administrator IDをそのまま利用	サーバパーソナルFirewall無効化
ドメインユーザが Built-in¥Administrators に所属	UAC無効	病院内のすべてのサーバを「信頼済サイトゾーン」に設定	自己署名証明書で署名されたActiveXコントロールのサイレントインストール許可	
ウイルス対策ソフトを導入するも停止させる	Windows Endpoint Protectionを無効化	Windows、Silverlight(サポート切れ状態)、Acrobat DCのアップデートの未実施		
VPN装置の脆弱性管理の不備	VPN装置への接続元IPアドレス制限を未実施			
USBメモリの利用許可				

一般的な脆弱箇所
Windows環境下における脆弱箇所
電子カルテ動作を優先させた脆弱箇所
ネットワーク機器の脆弱箇所
運用に関する脆弱箇所

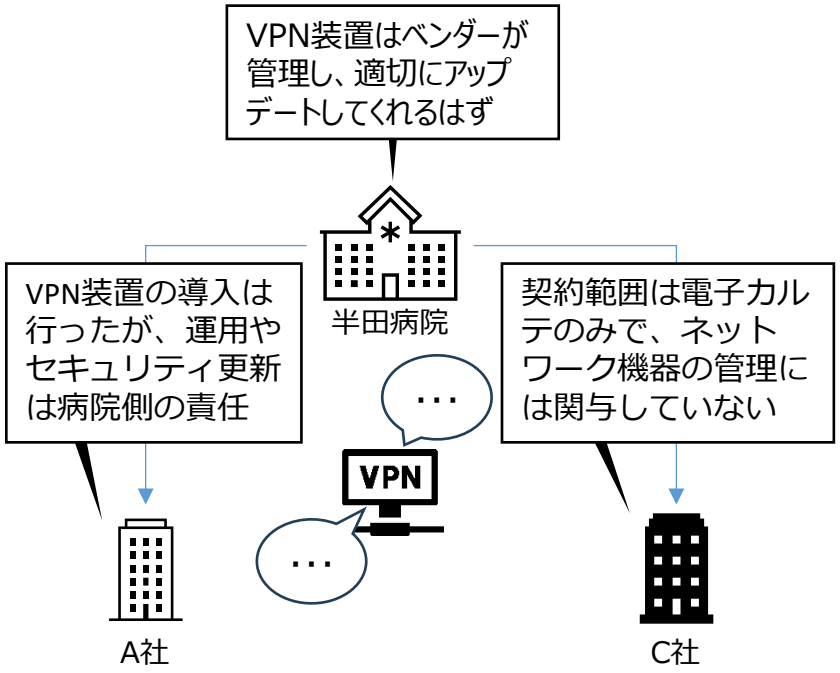
※ 徳島県つるぎ町立半田病院 コンピュータウイルス感染事案 有識者会議調査報告書 (以下、調査報告書)

組織によって生じた事案
半田病院における調査報告書に列挙されている組織的課題

セキュリティ課題と合わせて、医療機関固有の課題として、IT人材や予算不足が想定され、請負とされた関係会社との契約条項や双方の認識の不一致、セキュリティにおけるリテラシーの欠如、地域医療における財政の課題等を調査報告書は言及している

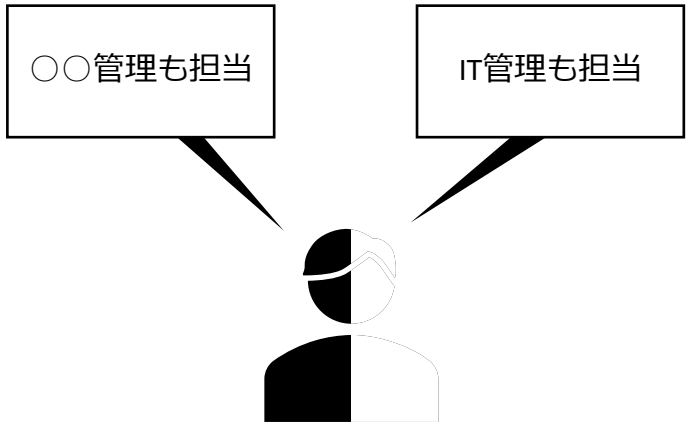
契約の不備

運用をベンダーに依存、攻撃を受けた際に「どこまでが病院側の責任で、どこからがベンダー側の責任なのか」が曖昧であった



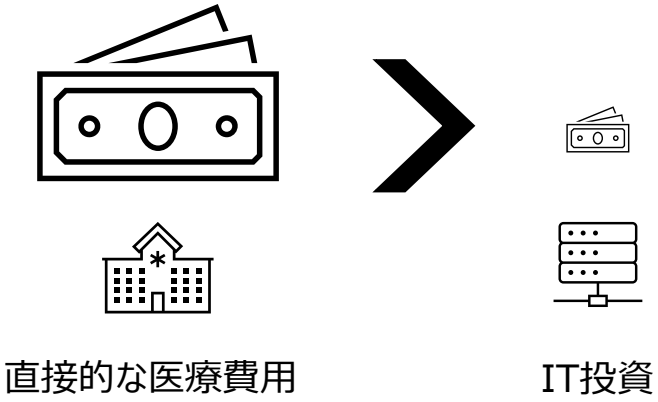
ITリソース不足

- 院内のIT管理は専任者ではなく、他業務と兼任の職員が担当
- サイバーセキュリティに関する知識を持つ担当者がいなかった



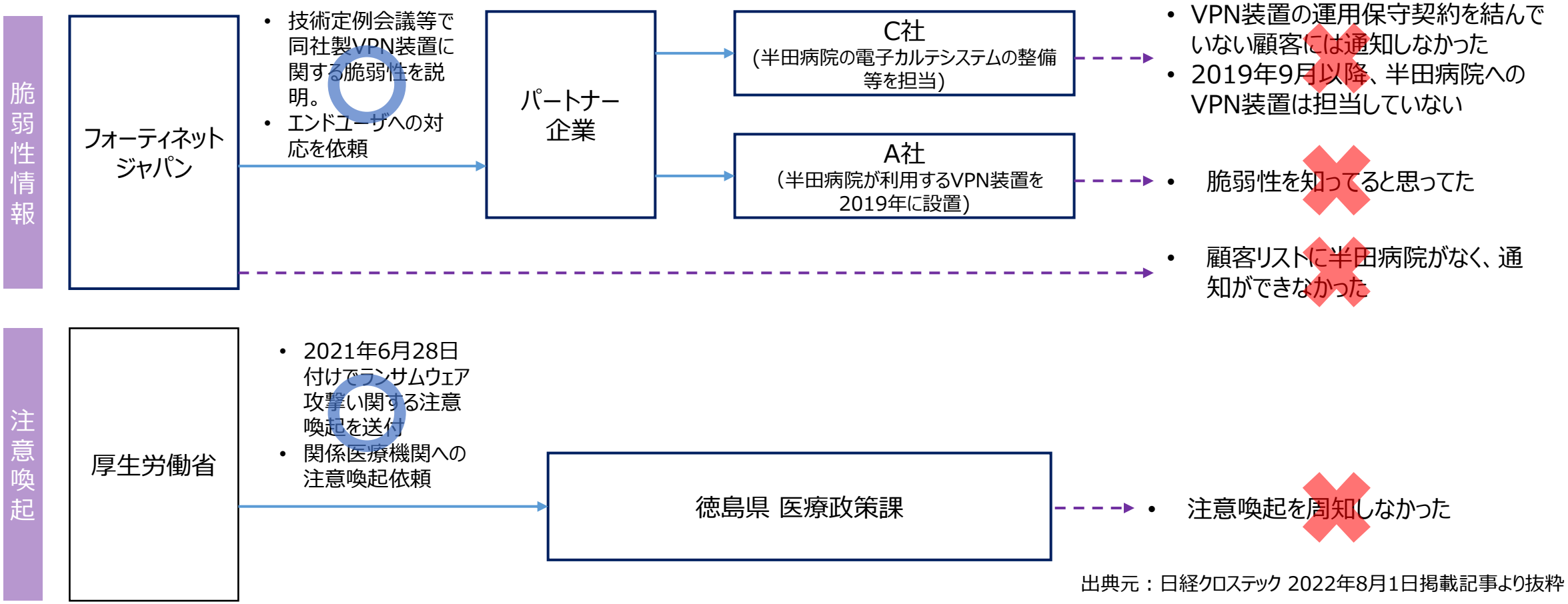
予算配分の問題

- 予算の大部分が医療機器の維持・更新、医療スタッフの確保に充てられ、IT予算が制限された
- ITインフラやセキュリティ対策の予算は、緊急性が低いと判断されやすく、最低限の支出しか確保されていなかった



組織によって生じた事案
事例)契約の不備から生じた情報連携の脆弱さ

注意喚起の徹底はメーカからも監督官庁からもあったものの、結果的に末端まで行き届いていない



出典元：日経クロステック 2022年8月1日掲載記事より抜粋

組織によって生じた事案
3章締め

セキュリティにおいて、組織的な課題が重要な要素として挙げられる。契約の認識不足やITリソース不足、コスト配分の偏り等、医療分野に限らず、日々発生していると考えられる。

組織は本来、営利目的（または社会的目的）のために情報資産を保護すべきだが、さまざまな要因によって十分なセキュリティを確保できないケースが後を絶たない。

しかし、小さな施策を積み上げることで（=スモールスタート）、セキュリティは少なからず強固になっていくと考えられる。
近年では、クラウドサービスを活用し、脆弱箇所を特定するサービスも登場している。

また、データが蓄積されるデータベース層においても、無償ツールを活用したアセスメントが可能なため、今一度、自社のITセキュリティを見直す良い気づけになればと思われる。

以上を踏まえ、本章を締めくくる。

第 4 章

社会に影響を与えた事案

社会に影響を与えた事案

本章では、社会に大きな影響を与えたセキュリティ・インシデントについて解説する。マルウェア感染や不正アクセス、機密情報の流出といった事案は、単に企業や組織に損害を与えるだけでなく、法律の改定や社会通念の見直しを迫る要因となることがある。

一般に、セキュリティ・インシデントが発生すると、企業・組織の被害規模や対応策、再発防止策に関心が集まる。しかし、その影響はそれだけにとどまらず、**法改正や新たなガイドラインの策定、さらには社会全体の意識変化**を引き起こす場合もある。

そこで本章では、法律やガイドラインの改定につながったセキュリティ・インシデント、さらには一般社会にも広く影響を与えた事例を取り上げ、その背景と影響について考察する。

社会に影響を与えた事案
国際/国内におけるガイドラインの一例

	ガイドライン名称	ベストプラクティス(フレームワーク)
国際的なガイドライン	**ISO/IEC規格** 国際標準化機構(ISO)と国際電気標準会議(IEC)が定めるセキュリティ基準	ISO/IEC 27001 (情報セキュリティ管理システムの標準)
	NIST (米国国立標準技術研究所) 米国政府が策定したサイバーセキュリティフレームワーク	NIST SP 800シリーズ (情報セキュリティガイドライン)
	CIS (Center for Internet Security) セキュリティのベストプラクティスを提供する非営利団体	CIS Controls (企業のセキュリティ対策ガイドライン)
日本国内ガイドライン	**組織における内部不正防止ガイドライン - IPA** 従業員や関係者による内部不正（情報漏えい、不正アクセスなど）を防ぐための指針	NIST SP 800-53(米国セキュリティ管理策) ISO 27002 (情報セキュリティ管理策
	サイバーセキュリティ経営ガイドライン – 経済産業省 企業の経営層向けに、サイバーセキュリティ対策の重要性を示したガイドライン	NIST Cybersecurity Framework
	システム管理基準 - IPA 企業の情報システムを適切に管理するための基準	COBIT (ITガバナンスと管理のフレームワーク)
	重要情報を扱うシステムの要求策定ガイド -IPA 重要な情報を扱うシステムの設計や運用に必要な要件を定めたガイドライン	ISO/IEC 27001 (情報セキュリティマネジメント) NIST SP 800-171 (機密データの管理基準)
	個人情報の保護に関する法律についての経済産業業分野を対象とするガイドライン 経済産業分野（企業・商業活動）における個人情報保護のルールを定めたガイドライン	ISO/IEC 27701 (プライバシー情報管理システム)

社会に影響を与えた事案
国際/国内における制定された法律の一例

	法制度名	法律に抵触する事件
海外の法律	**GDPR (一般データ保護規則)** EUの個人情報保護法で、企業が個人データを適切に管理することを義務付ける	2019年、フランスのデータ保護当局CNILはGoogleに対しGDPR違反として5,000万ユーロの罰金
	CISA（Cybersecurity Information Sharing Act） 米国のサイバーセキュリティ情報共有法で、政府と企業間の脅威情報の共有を促進	CISA自体は情報共有の枠組みを提供する法律 (裁判情報なし)
	HIPAA(Health Insurance Portability and Accountability Act) 米国の医療情報保護法で、医療機関や保険会社が患者の個人情報を保護することを義務	米国の大手医療保険会社Anthemがサイバー攻撃を受け、約7,900万人の個人情報が流出により本法律で罰金
国内の法律	**不正競争防止法** 企業間の公正な競争を確保し、不正な手段による利益取得を防ぐことを目的	デンソー事件
	個人情報保護法 企業や団体が個人情報を適切に管理し、無断利用や漏えいを防ぐための法律	ベネッセ個人情報漏えい事件
	サイバーセキュリティ基本法 日本のサイバーセキュリティ対策の基本方針を定めた法律	防衛産業へのサイバー攻撃 (三菱重工・IHI事件 2011年)
	不正アクセス行為の禁止等に関する法律（不正アクセス禁止法） 不正な方法で他人のID・パスワードを使う行為を禁止する法律	「dアカウント」を悪用した家電製品詐取事件
	特定電子メール法 迷惑メールの規制を目的とした法律	株式会社MOTHERによる違反事例

法律・ガイドラインによる整備（法律が制定されるに至った事件）
DENSO(デンソー)内部不正による情報持ち出し

概要	大手自動車部品メーカのデンソーの中国人従業員が、デンソーが保有する営業秘密である図面データを大量に会社貸与のPCにダウンロードし、無断で繰り返し自宅に持ち出していた。 同社が営業秘密の持ち出し事件として認識し、愛知県警がPC1台の横領罪の嫌疑により同人を逮捕した
漏洩したとされる情報	• 産業用ロボット • 各種センサー • ディーゼル燃料の噴射装置等
時期	2006年10月 ～ 12月
その後(後日談)	持ち出されたデータは残っておらず、会社貸与のPCから不正コピー したとみられる私有のPCは破壊されていた。営業秘密の使用・開示につき確認できないため、名古屋地検は処分保留のまま釈放した。

この平成21年改正の契機となったのは、検察が起訴できなかったデンソー事件である。この事件では、被疑者の営業秘密領得行為は立証できるが、中国における使用・開示行為を立証することが困難であったため、結局起訴猶予で決着となった。

出典元：https://jpaa-patent.info/patent/viewPdf/4162

法律・ガイドラインによる整備（法律が制定されるに至った事件）
DENSO(デンソー)内部不正による情報持ち出し

当時の不正競争防止法では「**営業秘密の不正取得**」だけでは処罰できなかった

不正競争防止法

- 不正の競争の目的で、不正な手段で取得し、「自ら使用したり、第三者に開示する行為」が禁じられていた
- DENSOの件では、データを外部へ送信（使用・開示行為）について証拠を得ることができなかった

そこで・・・、窃盗罪が適用されたが、**データ自体は「物」ではない**ため、PCの持ち出しにのみ適用され

窃盗罪 / 横領罪

- 横領罪では、業務上自己の占有する他人の物を横領した者が対象
- 「物」は「財物」と解釈されており、情報そのものが横領罪の対象に含まれていない
- IT・ネットワーク化の進展により、今後営業秘密の侵害が容易になることに対する懸念
- DENSOではデータを「PC」という財物に入れていた

不正競争防止法の改正

犯罪構成要件の変更
- 営業秘密の「領得(＝営業秘密データや機密情報)」自体への刑事罰を導入

不正の競争の目的の変更
- 「不正の利益を得る目的で、又はその保有者に損害を加える目的で」と改めた

法律・ガイドラインによる整備（法律が制定されるに至った事件）
ベネッセコーポレーション 情報漏洩

概要	2014年に発覚した、日本国内最大級の個人情報漏洩事件である。株式会社ベネッセコーポレーション（進研ゼミ・こどもちゃれんじ運営）が保有する顧客データが業務委託先の元社員によって不正に持ち出され、名簿業者に販売された。
漏洩したとされる情報	• 氏名 • 住所 • 電話番号 • 子供の生年月日 • 保護者情報（親の氏名など）
時期	2013年(情報持ち出し開始), 2014年7月9日：ベネッセが情報漏洩を公式発表
その後(後日談)	• 被害者に500円分の補償（お詫び）を提供 • セキュリティ強化と外部委託管理の見直し • 社長が引責辞任 • 元社員の判決：2015年3月、東京地方裁判所で「懲役2年6か月、執行猶予4年」の有罪判決 • 信頼を失い、会員数が減少 • 被害者が集団訴訟を起こし、約2,200人に対し1人あたり1万～3万円の和解金が支払われた • 個人情報保護法が改正（2017年施行）される契機となった

法律・ガイドラインによる整備（法律が制定されるに至った事件）
ベネッセコーポレーション 情報漏洩

	問題として指摘されたポイント	事件発生後の改訂
個人情報保護法	名簿業者による個人情報取得時、個人および企業からの個人情報取得方法の適正さが不明瞭であることを指摘された	個人データを第三者から提供を受けるときは、第三者の氏名・名称等、当該第三者がその個人データを取得した経緯について確認するとともに、受領年月日、確認した事項等の一定の事項を記録し、一定の期間その記録を保存しなければならない
個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン	媒体の持ち込み、ログの確認など、社内管理体制の問題	社内の安全管理措置の強化 • ログの定期確認、記録機器の使用・持ち込み制限等
	システム開発・管理の委託先における安全管理措置と監督が不完全な点	委託先等の監督強化 • 委託業務の監査、再委託を行う場合の承認申請等
	個人情報の取得時に、提供元の情報の取得方法の適正さが不明な点	第三者からの適正な情報取得の徹底 • 情報が適正に入手されていることを確認等
組織における内部不正防止ガイドライン	• 情報セキュリティ対策に対する体制 • リソース確保の不備	経営者の責任を明確化
	委託業務における監督の不備	委託先のセキュリティ対策の確認、委託内容の確認、再委託時の承認の導入
	スマートフォンなど社員が使用する媒体の使用時における制御の不備	特定の媒体の利用制限やアクセス権限管理、ログ監視の導入

法律・ガイドラインによる整備（法律が制定されるに至った事件）

セキュリティ・インシデントを防ぐ方策として、セキュリティ製品・機能の技術の進歩とともに法律・ガイドラインの整備もお互いに補完する形で進んでいる

技術の進歩

- 各種ファイアウォール
- 暗号化技術
- セキュリティパッチ
- 認証・認可・MFA

＋

法律・ガイドラインの整備

- 個人情報保護法
- 個人情報の保護に関する法律について経済産業分野を対象とするガイドライン
- 組織における内部不正防止ガイドライン

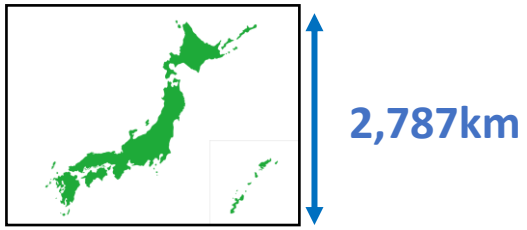
→ 企業におけるセキュリティ対策（動機づけや法令遵守）

社会意識
コロニアルパイプライン

概要	米国最大の石油パイプラインがランサムウェア攻撃を受け、パイプラインがシャットダウンされた。 約一週間に渡りオペレーションが停止し、米国の東海岸へのガソリンの供給に影響を与えた。
時期	2021年5月7日
その後(後日談)	• 後日米国政府が身代金の大部分を回収 • 米国が100万ドルの罰金をコロニアルパイプライン社に対して要求

コロニアルパイプラインとは

- 全長5,500マイル (約8,851km)
  (＝日本は南北に全長約2,787km)
- 1日250万バレル以上の燃料をパイプラインで供給
  (=約3.97億リットル)
- 米国東海岸の燃料供給の45%を担う



社会意識
コロニアルパイプラインへのサイバー攻撃による影響

国家(アメリカ合衆国)

- バイデン大統領による「国家サイバーセキュリティの強化」バイデン大統領令の宣言 (2021年5月21日)
- 米国のエネルギー業界の株価の下落
- 米国東海岸の燃料の45%に影響

企業(コロニアルパイプライン社)

- ランサムウェアの身代金および経済的被害
- 4.4百万ドルの身代金の支払い
- ビジネスの中断
- セキュリティファームへの調査の依頼
- 株価の下落
- アメリカ合衆国運輸省に対する100万ドルの罰金の支払い

消費者(アメリカ在住)

- 米国南東部でのガソリン不足によるガソリンの高騰・売り切れ
- 米国内の航空会社のフライト変更
- 1000以上のガソリンスタンドでガソリンが売り切れた

社会全体 ← 企業 → 個人

社会意識
スプリングヒルメディカルセンター

概要	米国アラバマ州のスプリングヒルメディカルセンターがランサムウェア攻撃を受け、監視機器などが使用不可となった。
時期	2019年7月
その後(後日談)	• ランサムウェア攻撃によってコンピュータが使用不可となっている間に、新生児の脳の損傷の発見が遅れ、9ヶ月後に死亡した。 • その後、新生児の母親が訴訟を起こし、ランサムウェア攻撃が原因となる初の死亡事例となった。

病院におけるサイバー攻撃被害の時系列

2018年1月11日
米国ハンコック地域病院
ランサムウェア攻撃を受け、
電子カルテが利用不可となる。

被害を受けている間は
紙カルテで対応。

身代金を支払い、
攻撃を受けてから
4日後に復旧。

2018年10月16日
奈良県宇陀市立病院
ランサムウェア攻撃を受け、
電子カルテが利用不可
となる。

2019年5月
東京都多摩の
医療センター
マルウェア感染により
情報が一部漏洩

ランサムウェア攻撃に
よる初の死亡事例

2019年7月
米国スプリングヒル病院にて
ランサムウェア攻撃を受け、
監視システムなどが停止。
新生児が死亡し、
ランサムウェア攻撃による
初の死亡事例

2020年12月2日
公立大学法人福島県立医科大学
附属病院にてランサムウェア攻撃
(WannaCry亜種)を受けて
放射線撮影装置に不具合が発生

2021年10月31日
徳島県半田病院にて
ランサムウェア攻撃を受け
電子カルテが利用不可
となった

ランサムウェア攻撃に
よる2件目の死亡事例

2022年9月10日
ドイツ デュッセルドルフ大学病
院にて、ランサムウェア攻撃に
よりデータへのアクセスができな
くなる。
患者の受け入れが停止され、
搬送中だった患者が死亡

社会によって生じた事案
4章締め

- セキュリティインシデントの中には、人々の日常生活に直接被害を与えるもの、人々の生命を脅かすようなものもある
- 普段のセキュリティインシデントでは、漏洩したデータの数や規模といった一次被害に目が行きがちだが、見えていない二次被害として我々の日常生活に大きく影響を与えるものもある。
- そのようなセキュリティインシデントが発生しないように、行動を取り締まる法律や、システム設計や運営、体制におけるガイドラインが存在する。
- しかし、技術の進歩や、金銭をきっかけに、近年セキュリティの脆弱性をついた攻撃が増えている。ガイドラインや法律では対応できない新しい攻撃手法や攻撃パターン、ガイドラインや法律の穴を掻い潜った攻撃やセキュリティインシデントが発生することも考えられる。
- セキュリティインシデントから、一次被害、二次被害と被害を拡大させないためにも、まずはセキュリティ対策を実装する、標的となるデータを中心とした多層防御の考えが大事になる。

第 5 章

ある事案に対するケーススタディと教訓

- 調査報告書より -

大阪急性期・総合医療センターについて
本事案を取り上げた背景

本書は「地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会 - 調査報告書(以下、調査報告書)」をもとに、発生したインシデントについてポイントを絞って説明する

調査報告書の冒頭で、世界的なパンデミックのくだりから医療は人の命を守る24時間365日のシステムであり、その医療システムが外部の攻撃から著しい機能低下に陥った点を取り上げる。

調査報告書は奇しくも2021年10月31日 (大阪急性期・総合医療センターでのランサムウェア感染の1年前) に発生した徳島県半田病院に対するランサムウェア攻撃による医療機能の著しい低下について触れ、

“医療機関において自身も同様の脅威が襲いかかるリスクを持ちうることをすることはまだまだ難しいのも現実です”

と言及している。

調査報告書冒頭の最後は セキュリティ・インシデント対策としての準備体制やBCP、そしてプラス・セキュリティ にふれて締めくくられている。

大阪急性期・総合医療センターについて
本事案を取り上げた背景

本書は「地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会 - 調査報告書(以下、調査報告書)」をもとに、発生したインシデントについてポイントを絞って説明する

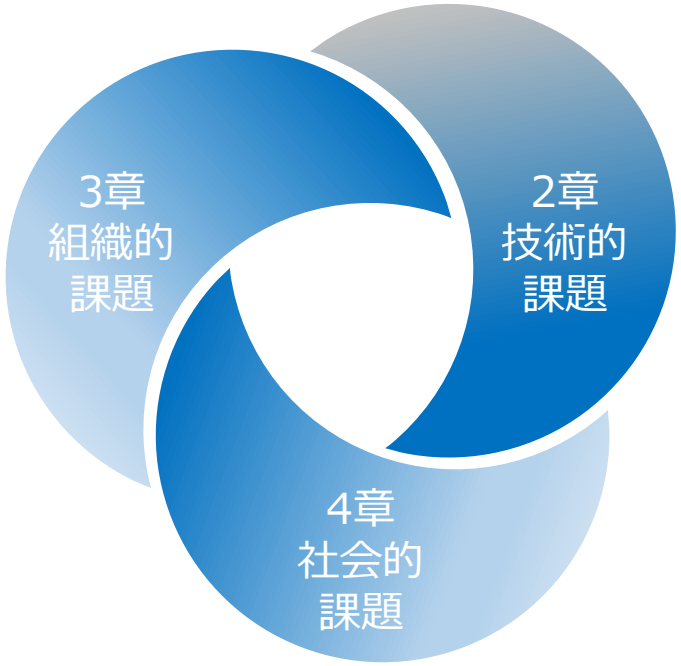
調査報告書の冒頭で、世界的なパンデミックのくだりから医療は人の命を守る24時間365日のシステムであり、その医療システムが外部の攻撃から著しい機能低下に陥った点を取り上げる。

5章では大阪急性期・総合医療センターのランサムウェア攻撃に関する概要を説明するものであり、攻撃手法や関係者間の対応方針等は本章では割愛とする。

本章は限られた時間で効率的にランサムウェア攻撃の概要および医療現場での混乱渦中下で医療を継続し続けた関係者の奮闘が生々しく記載されている

調査報告書は非常に多くの教訓を余すところなく、伝えしている文書であり、全体の一読を強く推奨する

本章をご一読いただき、対岸の火事と捉えるのでなく、自社のシステムとセキュリティリスクを再考察する一旦となれば幸いです



大阪急性期・総合医療センターについて
サイバー攻撃概要 – 攻撃の推移

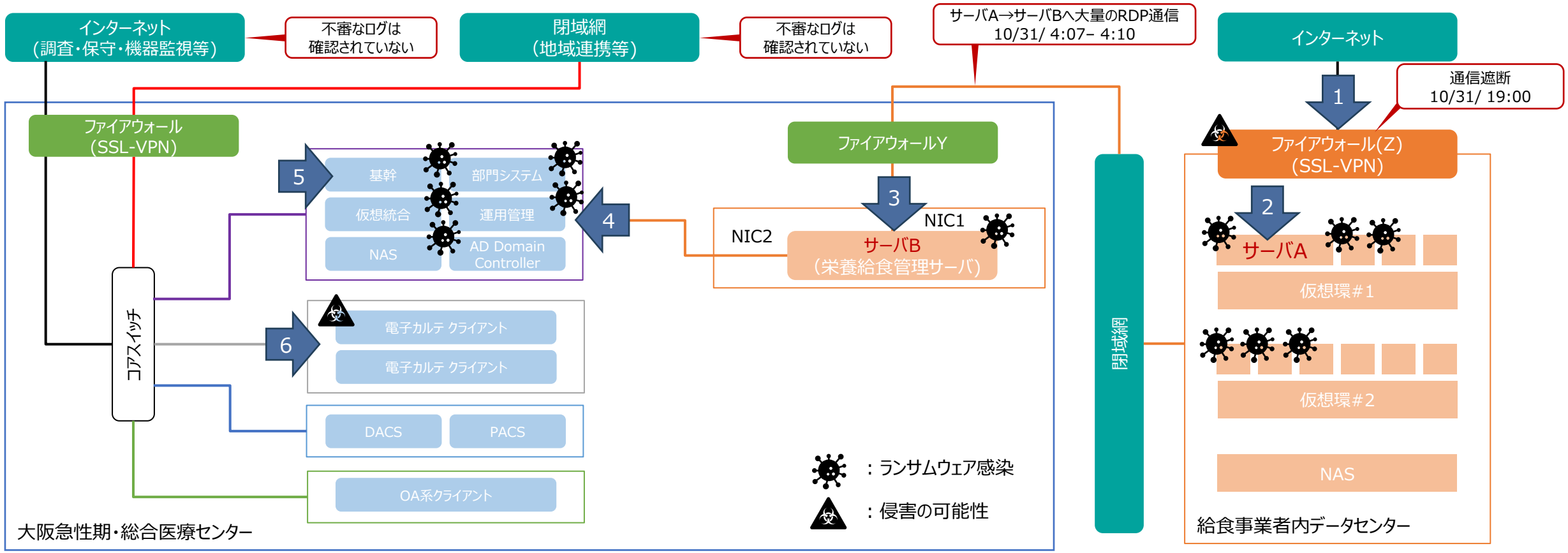
以下、調査結果から推定される情報をとりまとめたものである

1 給食業社へのサイバー攻撃(侵入)	給食事業者が設置・運営する給食システムに、情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入 (漏洩され公開されていたID・パスワード情報を用いて侵入された可能性もある)
2 給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報（IPアドレスやパスワード情報など）を窃取されたため給食事業者内での攻撃拡大
3 病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入、ウイルス対策ソフトのアンインストールも実施
4 病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。
5 他サーバー侵入	病院給食サーバーで窃取した他サーバー認証情報により、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入
6 クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性
7 ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート (身代金要求文書) を表示

出典元：https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf

大阪急性期・総合医療センターについて
サイバー攻撃概要 – ネットワーク構成図と感染状況

本書は感染経路について記載するものであり、出典元にある関係会社にかかる箇所は省略とする



出典元：https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf

大阪急性期・総合医療センターについて
サイバー攻撃概要 – 数字で見る被害の全貌

復旧日数(日)

43日
基幹システム復旧

73日
全体診療システム復旧

診療制限(人)

-61.6%
前年同月比
(15,744人)※1

被害額(円)

数億円
(調査・復旧にかかる費用)
逸失費用：十数億～

※1 調査報告書「表8 大阪急性期・総合医療センター2022年11月診療実績」より抜粋

出典元：https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf

大阪急性期・総合医療センターについて
サイバー攻撃概要 – 復旧にかかる戦術

患者最優先対応 → 情報公開および連携 → 医療継続

患者対応
- 地域医療救急対応
- 外来患者対応
- 入院患者対応
- 電話による患者対応

情報公開
- 関係各所への連携
- ホームページの掲載
- 記者会見(2回)

事業継続
- 対策本部設置
- 関係幹部の招集
- 紙カルテ運用移行
- 関係者への連携徹底

本攻撃に伴う
人的被害 “ゼロ”

出典元：https://www.gh.opho.jp/pdf/report_v01.pdf

大阪急性期・総合医療センターについて
サイバー攻撃概要 – 本事例が訴える教訓(概要)

患者最優先対応

- 復旧長期化を踏まえて、新規患者受け入れ不可、近隣病院への支援依頼実施
- 手動による予約対応、診断の必要性(緊急度)をトリアージしながら各科への判断に委ねる(他医療機関の紹介含む)
- 各診療科の裁量に委ねる(他医療機関への支援、患者転院対応)
- 予約患者に関しては電話で対応し、回線増強による不通状態を回避

情報公開および連携

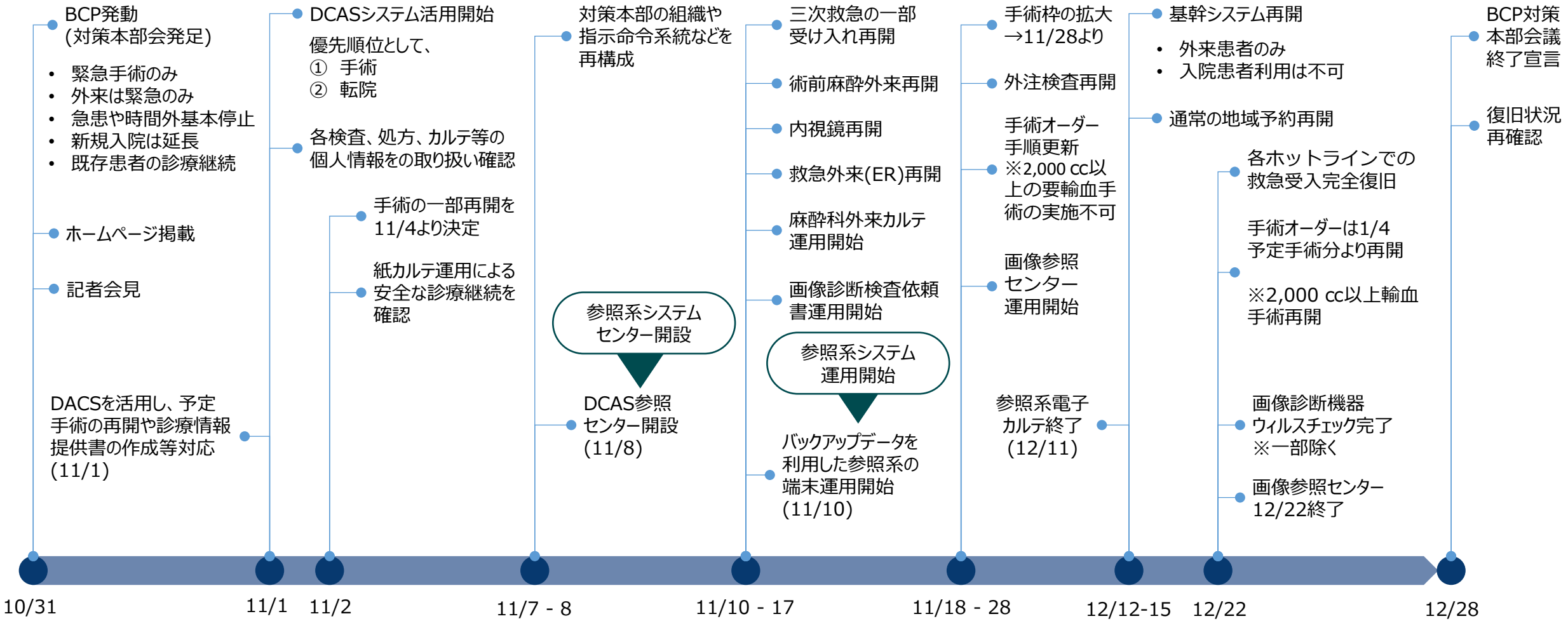
- 機構本部、大阪府、大阪府住吉警察署、大阪市保健所、厚生労 働省、内閣サイバーセキュリティセンターなど、関係各方面に連絡
- 厚生労働省からの専門家チームの受入れ
- ホームページへの速報ベースでの状況掲載と来院患者への口頭説明を実施。情報の隠匿は実施せず、積極的な情報の公開と記者会見を実施

医療継続

- 復旧長期化を踏まえて、新規患者受け入れ不可、近隣病院への支援依頼実施
- 手動による予約対応、診断の必要性(緊急度)をトリアージしながら各科への判断に委ねる(他医療機関の紹介含む)
- 各診療科の裁量に委ねる(他医療機関への支援、患者転院対応)
- 予約患者に関しては電話で対応し、回線増強による不通状態を回避

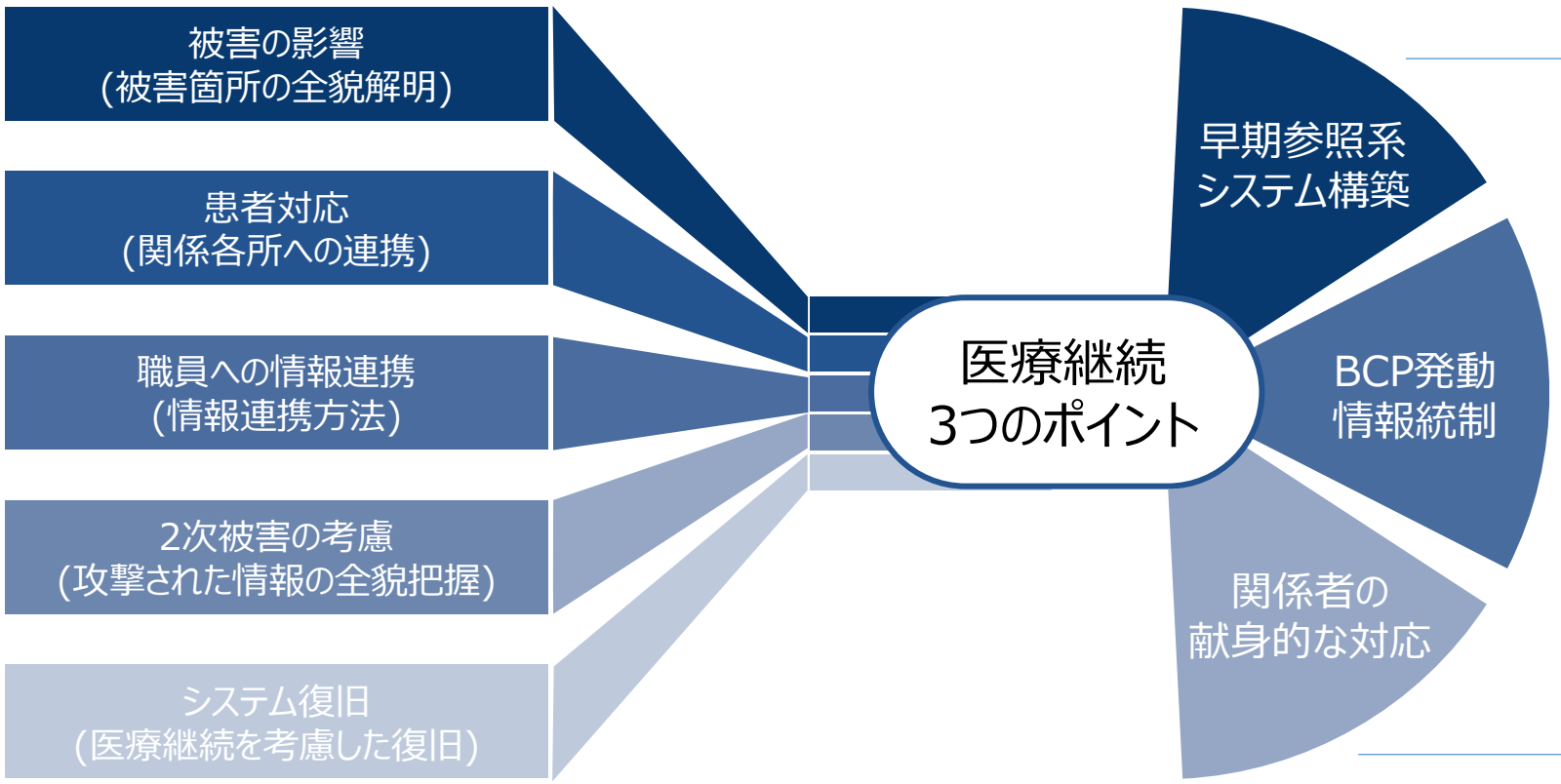
出典元：https://www.gh.opho.jp/pdf/report_v01.pdf

大阪急性期・総合医療センターについて
サイバー攻撃概要 – 本事例が訴える教訓(時系列)



出典元：https://www.gh.opho.jp/pdf/report_v01.pdf - P33

大阪急性期・総合医療センターについて
サイバー攻撃概要 – 本事例が訴える教訓(医療継続と早期復旧のポイント)



- 診療記録文書統合管理システム(DACS)を活用し、予定手術の再開や診療情報提供書の作成等対応
- DACS を参照できる端末増強(2台→20台)
- 11月10日には、バックアップデータを活用した電子カルテの参照端末20台の運用も開始

- 事業継続対策本部が設置できる体制を構築
- インシデントを認知して短時間で幹部を含めて招集
- 速やかな紙カルテ運用に移行
- 対策本部会議で決定した事項を速やかに職員周知

- 関係者との連携と支え
- 職員へのメンタルケア
- 有給休暇が取得しにくい部署への積極的な取得奨励

大阪急性期・総合医療センターについて
サイバー攻撃概要 – 本事例が訴える教訓(3つポイントの実現向けて)

技術

診療記録文書統合管理システム（DACS）に加えて、医用画像管理システム（PACS）がランサムウェア感染を免れていたが幸運し、参照系システムを早期構築することができた(調査報告書では 早期復旧の “切り札” と表している)

一方でサイバー攻撃を想定したネットワーク細分化、参照系システム構築がBCPに組み込まれているわけではないため、医療機関には**大規模システム障害時の迅速な参照系の構築を念頭に入れたBCPを策定**すべきである。

組織

大規模システム障害を想定したBCPやコンティンジェンシープランの準備を進めるべきである。

- 大規模システム障害が発生した時にどのように医療継続を行うか？
- システム復旧に必要なバックアップがランサムウェア攻撃等によって失われないようにするためにどのように確保するか？
- バックア ップからどのように速やかにシステム復旧を行うか？

社会

サイバーセキュリティ被害で改めて、浮き彫りとなった以下の課題は業種を問わず少なからず存在する。
正しい情報を身につけ、セキュリティに対するマインドを向上するだけでも効果はあるはずであり、これらのマインドを社会が持つことも重要である。

① 地域医療への脅威からの保護
② 役割と責任分界点の明確化
③ 閉域網意識の見直し
④ 医療継続支援への更なる取り組み

大阪急性期・総合医療センターについて
本事案を取り上げた背景

本章最後に調査報告の文章を引用して本章をクローズとする

- 今回の事故は病院のシステムが停止する重大なインシデントであったが、本事故に起因した死者を出すことは無く、比較的短期間で病院機能を復旧することができた。これは、病院の医師・看護師をはじめとする全職員とその家族、地域医療機関の関係者、給食事業者をはじめとする様々なサプライヤー、電子カルテシステム・部門システム・医療機器・セキュリティベンダー、大阪府警察本部、大阪府、厚生労働省、ソフトウェア協会の専門家チームなど、すべての関係者の連携や支えがあったからに他ならない。
- 患者の皆様には電子カルテシステムが機能しなくなるという事態で困惑した方も多いと思うが、病院を始めとするすべての関係者が、医療継続のために最大限努力し、医療継続やインシデント対応に取り 組み続けたことには是非ともご評価をいただきたい。残念ながら、昨今はサイバー攻撃も巧妙化しており、いつ、だれに起きてもおかしくない状況である。
- 最後に、病院には重ねてこのような事態を起こさぬよう、サイバーセキュリティに対しても不断の努 力をお願いするとともに、今回、関係したすべての皆様に、心からの感謝の意を伝え、本報告書の括りとする。

出典元：https://www.gh.opho.jp/pdf/report_v01.pdf - P67

第 6 章

総括

サイバーセキュリティにおける課題は、「技術の革新」、「組織運営」、「社会全体のリスク管理」といった多層的な視点から捉える必要がある。

技術の進歩が新たな脅威を生む一方で、組織内部のガバナンスやリソース不足が脆弱性を拡大させる要因となり、最終的には社会全体に影響を及ぼす。本書で取り上げた大阪急性期総合医療センターの事例は、こうした課題が現実にどのような形で顕在化するかを示す象徴的な出来事である。

今後、サイバーセキュリティを単なる技術的課題としてではなく、組織の運営や社会の安全保障と密接に関わる重要な要素として認識し、継続的な対策を講じることが不可欠となる。一方で狙われているのは経営資源となるデータであることは変わっていないのも事実である。

本書が、読者にとって自身の組織や社会におけるセキュリティの在り方を再考する契機となれば幸いである。

参考文献

JVNTA#95530271 Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威

日本で急増するサイバー攻撃、世界サプライチェーンリスク浮き彫りに

トヨタ自動車のランサムウェア被害から学ぶ、企業に必要なセキュリティ対策とは

オズモールの不正アクセスでもウイルス発覚--原因はSQLインジェクションか

【緊急インタビュー】SQLインジェクション攻撃に気づかない企業は山のようにある

「史上最悪のデータ侵害事件」の容疑者として中国人ハッカーが起訴される

Take Out — How Anthem was Breached

京都の会社「イセトー」にランサムウエアによるサイバー攻撃 委託元の150万件近くの個人情報漏えいか | NHK | サイバー攻撃

不正アクセスによる個人情報漏えいに関するお詫びとご報告｜株式会社イセトー

メタップスペイメント 第三者委員会 調査報告書 （公表版）

ディスクユニオン、自社ECで最大約70万件の個人情報漏えいか - ITmedia NEWS

参考文献

半田病院 有識者会議調査報告書 - 調査編

半田病院 有識者会議調査報告書 - 技術編

半田病院 有識者会議調査報告書 - セキュリティコントロールガイドライン v1.0

途切れたセキュリティー情報の「供給網」、なぜ半田病院は脆弱性を放置するに至ったか

大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要

地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会

参考文献

IT用語集 セキュリティインシデントとは

デンソーから13万5000件の設計資料が不正に持ちだされる

不正競争防止法における営業秘密と刑事罰

改正不正競争防止法の概要

事故の概要

「ベネッセ情報漏洩事件」とは何だったのか？その原因と経過から学べる事

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン

個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改正

組織における内部不正防止ガイドライン

IPA「組織における内部不正防止ガイドライン」改訂

Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details

制御システム関連のサイバーインシデント事例9

Cyber Case Study: Colonial Pipeline Ransomware Attack

コロニアル・パイプライン事件他で米国サイバーセキュリティは激変予感

US proposes $1 million fine for Colonial Pipeline ransomware attack

Pipeline outage forces American Airlines to add stops to some long-haul flights, Southwest flies in fuel

コロニアル・パイプライン社へのランサムウェア攻撃　国土安全保障委員会の公聴会で語られた事件の背景とは

参考文献

Colonial Pipeline Company

Our Operations| Energy Infrastructure – Colonial Pipeline

病院で多発するランサムウェア被害とは？セキュリティ対策や原因を解説

ついに日本でも病院がサイバー攻撃の標的に！

ランサムウェア感染から4日で復旧

宇陀市立病院コンピューターウイルス感染事案に係る安全確認の公表

公益財団法人東京都保健医療公社が運営する端末等に対する不正アクセス被害の発生による、メールアドレス等の個人情報の流出と対応について（第二報）

コンピュータウイルス感染の原因及び対策について- 公立大学法人福島県立医科大学附属病院

独病院へのサイバー攻撃で患者死亡か、搬送遅れる 過失致死容疑で捜査

Ransomware Attack at Springhill Medical Center