サイバー戦国絵巻
～ 技術と社会の攻防史 ～

日本オラクル株式会社 リャンジェニー ルウ
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 茶園 太志
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

データベースセキュリティWG

目次

第 1 章

本日の目的

本日の目的
概要と訴求点

本日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、以下の3つの観点から考察する。

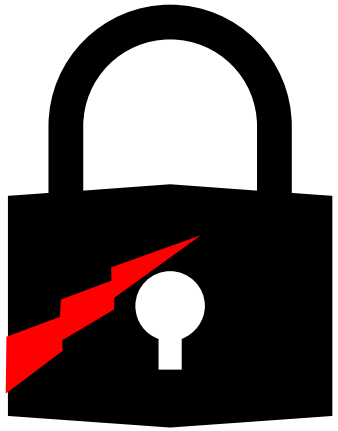
	①技術の革新	②組織的な課題	③社会的な課題
概要	2000年以降に発生した事案を技術の多様化や技術革新により巧妙化するサイバーセキュリティ事案について	技術の過信や旧態依然とした考え方の隙をついたサイバー攻撃を組織的にどのように対処すべきかについて	世間を震撼させたセキュリティ事案の経験から法律の改定、社会通念の再定義を余儀なくさせた事案について
訴求点	技術の進歩は攻撃者と防御側の双方に恩恵を与えている事実を踏まえて、技術の重要性について解説	技術的な対応に加え、組織全体のリスク管理体制を拡充させることが不可欠であることを解説	セキュリティ事案は個人や企業だけなく、国の安全保障や国益の損失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

第 2 章

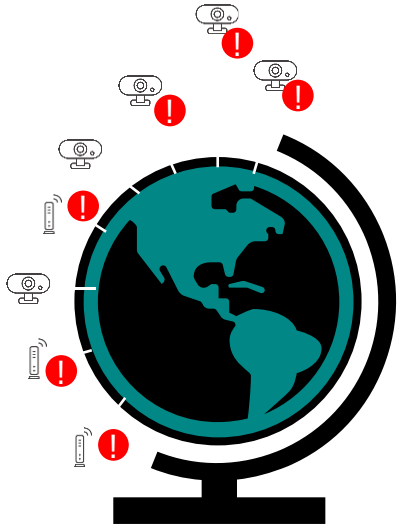
技術の革新によって生じた事案

技術の革新によって生じた事案
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もに巧妙化をした歴史を持つ

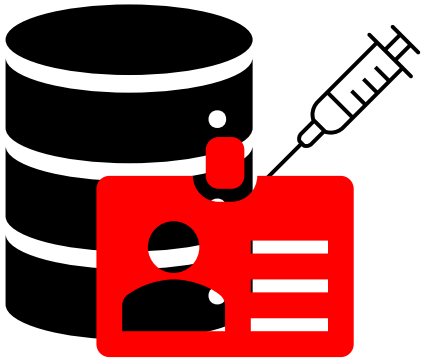


パスワードクラック



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
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」**：郵便で送られたフロッピーのソフトウェアをインストールすると、ハードディスクが暗号化され、「189USDの身代金」を要求
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し、5USDから10USDと少額の身代金が請求され。100万人以上が身代金を支払う。
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「CryptoLocker」**：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復旧が可能だった。現在のランサムウェアの原型
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。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なし。
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が登場
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 小島プレス工業**：トヨタ自動車の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

JNSA

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」でJeff Forristal氏（Rain Forrest Puppy）が、特定のコマンドでサーバの情報共有が強制停止されることを発見

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52万件の個人情報の漏洩、オンラインゲームアカウントの漏洩（※）
- 「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を奪取

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

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流出

WAFは有効な対策だが、依然として続く被害

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

※ 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

JNSA

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）

■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。

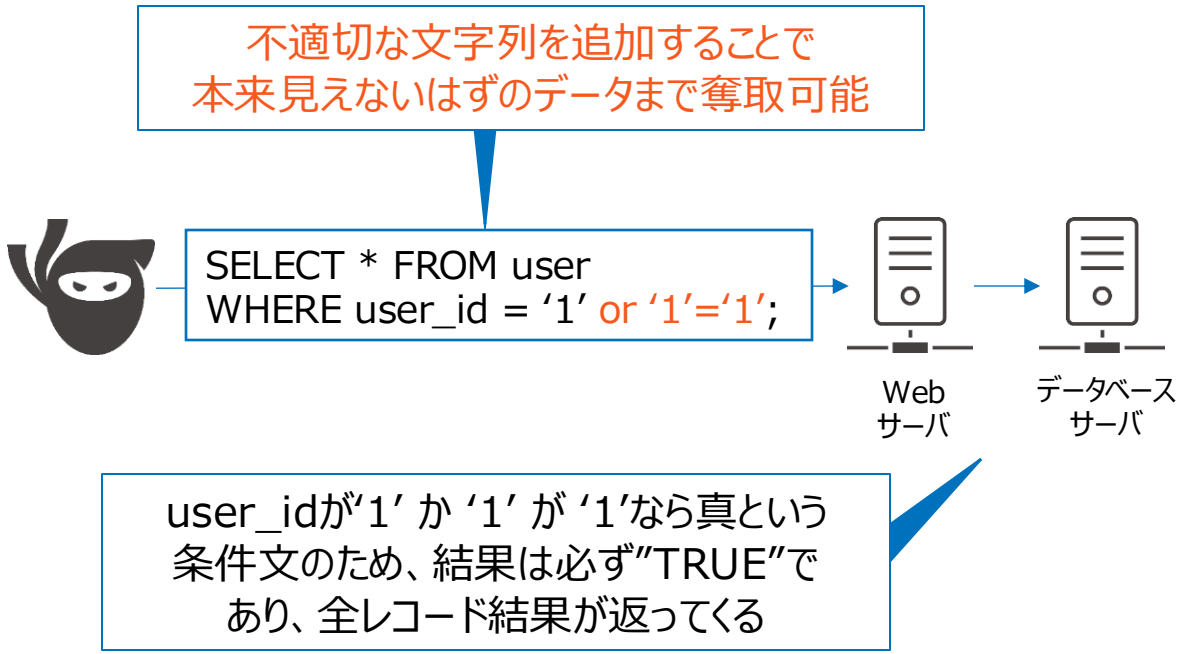


図 SQLインジェクションのイメージ

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

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、以下の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。

■ 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

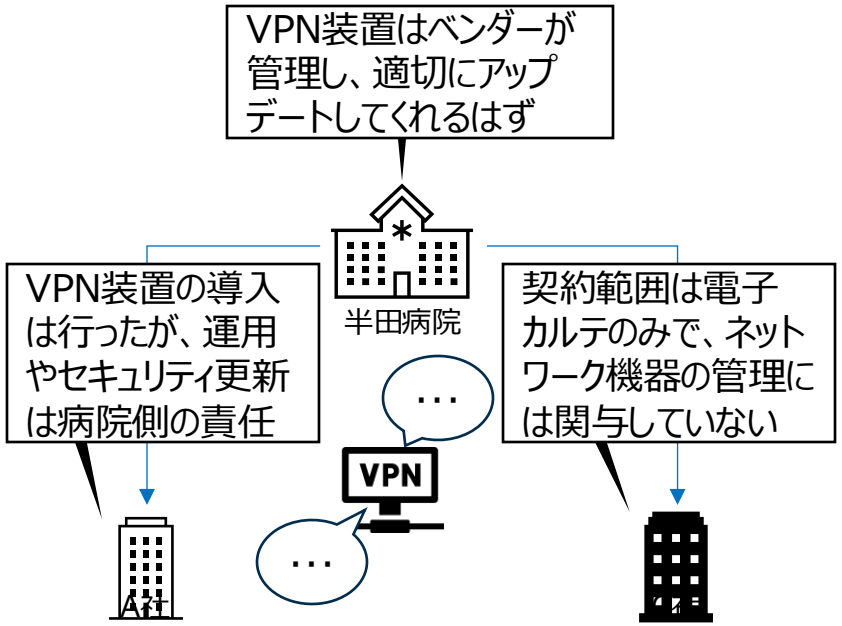
JNSA

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、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

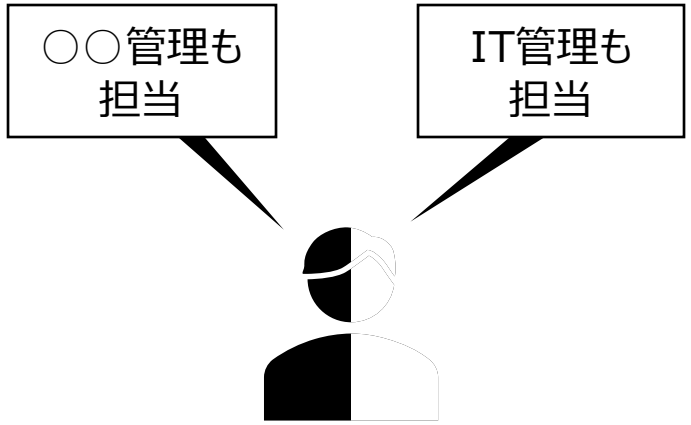
契約の不備

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



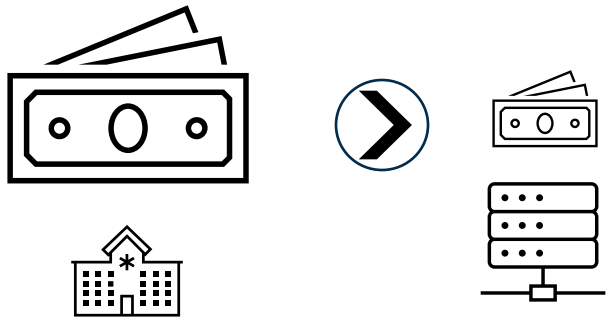
ITリソース不足

- 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



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
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)

JNSA

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	米国大手医療保険会社Anthemがサイバー攻撃で約7,900万人の個人情報が流出し本法律で罰金
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

JNSA

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

＊ 2017年5月に改正個人情報保護法が施行され、個人情報保護委員会が定めるガイドラインに一元化されたため現在は廃止

JNSA

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。

国内外の病院におけるサイバー攻撃被害

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で
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で
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
ランサムウェア攻撃で
監視システム等が停止
新生児が死亡し、
ランサムウェアによる
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)で
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
ランサムウェア攻撃で
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
ランサムウェア攻撃により
データへのアクセスができ
なり、患者の受け入れが
停止。
搬送中だった患者が死亡

第 5 章

クロージング

まとめ
サイバー戦国絵巻

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。
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。

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

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

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