Yh2020-001\_校正版令和２年サイバ極意編集資料20200120

1. Ver１．０　改定2020/06/12 13:00-
2.  目次
   1. １．編集方針 Introduction
   2. ２．変更・追加内容一覧　Abstract
   3. ３．改定内容
      1. ・「中小企業向けサイバーセキュリティ対策の極意」の改定（追補資料の作成）
      2. ・改定理由
         1. 国のサイバーセキュリティ関連法規、施策対応
            1. サイバーセキュリティ基本法の改定（2019年４月１日施行）対応
            2. サイバーセキュリティ戦略2018(2018年7月）今後の3年間の基本計画
            3. サイバーセキュリティ2019(2019年５月２３日）
         2. 「サイバーセキュリティ経営ガイドライン2.0対応
            1. XXXX年XX月
         3. 中小企業の情報セキュリティ対策ガイドライン第3版対応
3.  ４．はじめに
4.  ５．Keyword
   1. ・DXとサイバーフィジカルセキュリティ
   2. ・ハイブリッドクラウド　クラウド・バイ・ファースト
   3. ・エンドポイントセキュリティ
   4. ・サプライチェーンセキュリティ　NIST　８００−１６１　V2
   5. ・三層構造モデル　サイバーフジカルセキュリティ
   6. ・CMS認証　IC６２４４３認証
   7. ・マールウエア　Emotet
   8. ・改正割賦販売法
   9. ・BEC攻撃
   10. ・政府システムクラウド利用基本法
   11. ・ブロックチェーンとサプライチェーンセキュリティ
   12. ・NIST　８００−１６１　CUI　コントロールと中小企業サプライチェーンSec
   13. ・情報セキュリティ10大脅威
   14. ・ICSセキュリティ　産業用制御システム
   15. ・サイバセキュリティ保険　保証範囲の拡大
   16. ・日本セキュリティ監査協会　２０２０年監査1０大監査テーマ
   17. ・プライバシ保護法の国際化　GDPR
   18. ・フィッティングサイトの巧妙化と増大
   19. ・アジャイル開発とOPDVP
   20. ・５Gサイバセキュリティ
   21. ・Fi-Wi　Open　Wi-Fi　規格
   22. ・VPNの脆弱性攻撃増加　テレワーク
   23. ・NIST　８００−５３　Ver４　プライバシ管理策
   24. ・DXと人材ICT教育
   25. ・改正民法と瑕疵担保期間の延長
   26. ・クラアイドセキュリティ　CASBY
   27. ・ZERO　TRUST
   28. ・経営ガイドラインV2　実践プラティクス２版
   29. ・ISMAP　情報セキュリティ監査ガイドライン
   30. ・ハイブリット先進認証　Moddern Authentificaion　MAM
   31. ・CMMC　セキュリティ成熟モデル　DoDでスタアート
   32. ・SDP　クラウドセキュリティ
   33. ・BCP　ICT　BCPにセキュリティを明示する。
5.  ６．サイバー・フィジカル・セキュリティ対策 フレーム　ワーク
   1. 平成 31 年 4 月 18 日　経済産業商　Verizon１．０
   2. ■我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多 様なニズにきめ細かに対応したモノやサビスを提供し、経済的発展と社会的 課題の解決を両立する超スマト社会「Society5.0」の実現を提唱している。さら に、「Society5.0」の実現へ向けて様々なデタの「つながり」から新たな付加価 値を創出していく「Connected Industries」という概念を提唱し、その実現に向 けた取組を推進している。
   3. サプライチェン
   4. ■「Society5.0」における産業社会では、デタなど様々なつながりが生まれる 「Connected Industries」という形で企業間・産業間のネットワク化が進展し て、従来とは異なる、これまで取引を行うことがなかった主体を新たに巻き込ん だ、より柔軟で動的なサプライチェンを構成することが可能となり、サイバー 空間とフィジカル空間が相互に作用しあう中で、両空間を跨いで構成される新た な形のサプライチェンが新たな付加価値を生み出していくことになる。 一方で、ネットワク化によってサイバー空間とフィジカル空間の両空間を跨い で動的に構成される新たな形のサプライチェンの拡大は、ネットワク化され たサプライチェン上に攻撃起点が広く拡散していくことになり、攻撃側が攻撃 起点を得る機会が増え、防御側が守るべき範囲が急激に拡大することを意味する。 また、サイバー空間とフィジカル空間が相互に作用しあうことは、サイバー攻撃 がフィジカル空間に及ぼす影響も増大していくことを意味し、サイバー攻撃によ る被害は甚大なものになっていく可能性がある。 このように、サイバー空間とフィジカル空間が融合することで新たな価値を生み 出していく「Society5.0」における産業社会では、一方で、サイバー攻撃の起点が 拡大するとともに、サイバー攻撃による被害がフィジカル空間に及ぼす影響も増 大し、これまでとは異なる新たなリスクを伴うことになる。本フレムワクは、 新たな産業社会におけるこうした環境において、付加価値を創造する活動が直面 する新たなリスクに対応していくため示すものである。
   5. ■高度にネットワク化され、動的に構成されるサプライチェンに様々な主体が 参加するような状況においては、一企業が取り組むセキュリティ対策だけでサイバーセキュリティを確保していくことには限界がある。このため、それぞれの企 II 業がセキュリティ・バイ・デザイン等の観点を踏まえて、企画・設計段階から製 品やサビスのサイバーセキュリティ対策を実施することに加え、ビジネス活動 のレジリエンスまで考慮に入れた上で、関連企業、取引先等を含めたサプライチ ェン全体としてセキュリティ対策に取り組むマルチステクホルダによるア プロチや、デタ流通におけるセキュリティも含めて、サイバーセキュリティ 確保に取り組む必要がある。
   6. ■サプライチェンの構造変化 こうした「Society 5.0」においては、企業を中心に付加価値を創造するための 一連の活動であるサプライチェンも、その姿を変えることになる。これまでの サプライチェンは、始めに厳密な企画・設計を行い、それを踏まえて必要な部 品やサビスを調達し、組み立て・加工を行い、最終的な製品・サビスを提供 するという、一連の活動の順番が固定的・安定的な形で展開される、定型的・直 3 線的な構成をとっていた。しかし、「Society5.0」では、サイバー空間とフィジカ ル空間が高度に融合する中で、必要な人に対して、必要な時に、必要なモノやサビスが提供されることになる。付加価値を創造するための一連の活動の起点 は、これまでのように供給者が企画・設計するという固定的なものではなく、需 要者が付加価値の創造活動の起点となることも増大していく。また、付加価値を 創造するための一連の活動の内容自体も、開始時点で設定された“必要性”の変 化に対応した変更や、より有用なデタが得られた場合にその要素を新たな活 動の中に組み込み変化していく。 このように、サプライチェンはサイバー空間とフィジカル空間の両空間を 跨いで、様々なモノやデタが動的につながって構成される付加価値の創造活 動へと変化していくことになる。このように変化したサプライチェンは、従来 の上流から下流へとつながる定型的・直線的なサプライチェンと対比し、 「Society5.0」型のサプライチェンとして捉え、既存のシステムやプロシジ ャなどについても、改めて捉え直すことが必
   7. 要となる。本フレムワクでは、 このような「Society5.0」型のサプライチェンをこれまでの定型的・直線的な サプライチェンとは区別して認識するため、『価値創造過程（以下、「バリュ クリエイションプロセス」とする。）』と定義する。
   8. 大量のデタの流通・連携 →デタの性質に応じた適切な管 理の重要性が増大
   9. フィジカル空間とサイバー空間の 融合 →サイバー空間からの攻撃がフィ ジカル空間まで到達フィジカル空間から侵入してサイバー空間へ攻撃を仕掛けるケスも想定フィジカル空間とサイバー空間 の間における情報の転換作業へ の介入
   10. 複雑につながるサプライチェーン →サイバー攻撃による影響範囲が 拡大
   11. バリュククリエイションプロセスと従来のセキュリティリスクの相違
   12. ■従来のサプライチェンでは、セキュリティ対応をしっかりと行った主体間 で行われる定型的・直線的な取引であれば、そのプロセス全体のセキュリティが 確保される、つまり、参加主体の組織ガバナンス、マネジメントがセキュリティ の確保された信頼できるものであれば、サプライチェンの信頼性も確保され る、という考え方に基づいていた。情報処理を委託する場合も、ISMS などの認 証を取得しているなどセキュリティ対策をしっかりと行っている企業かどうか を重要視していた。したがって、セキュリティを確保するための基点は、組織の マネジメントの信頼性に基礎が置かれていたことになる。 しかし、サイバー空間とフィジカル空間が高度に融合した産業社会における 新たな形の付加価値の創造活動であるバリュクリエイションプロセスでは、 従来のサプライチェンの場合のように、組織のマネジメントの信頼性にのみ 基点を置くことでバリュクリエイションプロセスの信頼性を確保することは 困難となる。
   13. ■三層構造モデル
       1. 第一層　サイバー空間　　※デタの信頼性
       2. 第二層　サイバー・フジカル空間　転写機能の信頼性
       3. 第三層　企業空間　マネジメントの信頼性
   14. ■六層モデル
   15. 構成要素 定義 ソシキ バリュクリエイションプロセスに参加する企業・団体・組織 ヒト ソシキに属する人、及び価値創造過程に直接参加する人 モノ ハドウェア、ソフトウェア、及びそれらの部品 操作する機器を含む デタ フィジカル空間にて収集された情報、及び共有・分析・シミュレションを 通じて加工された情報 プロシジャ 定義された目的を達成するための一連の活動の手続き システ ム 目的を実現するためにモノで構成される仕組み・インフラ
6.  ７．CMS認証
   1. CMS認証は、CMS（IE6244321)に基づいた第三者認証制度。情報セキュリティマネジメントシステムであるISMS適合性評価制度を運営するJIPDEC（一般財団法人日本情報経済社会推進協会）により、CMS適合制度として２０１４年にスタト。
   2. 経済産業省が国際的に適用する認証基盤の確立のために実施した。
   3. 現在は、ISMSACが運営。
7.  ８．個人情報保護とシステム監査　※SAAJ　２０１９年２月
   1. ２０１７年５月３０日に全面施行された新個人情報保護法では、「要配慮個人情報」として人種、信条、社会的身分等について、より慎重な取り扱いが要求されるようになりました。一方　　ビックデタの活用のため一定のルルに従って匿名加工した個人情報については、かならずしも本人の同意をえなくてもよいと原則が明確にされました。
   2. グロバルな情報流通社会の中かで個人情報の自国外への移転も成約をうけている。
   3. EUでは「一般デタ保護規則（GDPR)」が２０１８年５月に適用され、EU域外への個人情報移転について厳格な制限が規定されています。
8.  ９．２０１４年１１月１６日「サイバーセキュリティ基本法」が成立。
   1. 同法第１４条「重要インフラ事業者等におけるサイバーセキュリティの確保と促進」が規定されている
9.  １０．情報漏洩防止対策　２０１６年度個人情情報の保護に関する法律施行状況の概要
   1. （個人情報保護委員会２０１７年１１月）
   2. 従業員が起こした情報漏洩事故の原因区分より
      1. 原因区分　不注意　８０％　意図的　４％　不明　７％
      2. おこした者区分　従業員　６７％　第三者　２４％　不明・その他　９％
10.  １１．DXレポト
    1. ２０１８年９月経済産業省が「DXレポト」を発表
       1. 「デジタル技術を駆使して新しいサービスや新しいビジネスモデルを 作り出す。」
       2. レガシシステム「老朽化、複雑化、ブラックボックス」
    2. 「２０２５年崖」毎年１２兆円の経済損失が生じる可能性が有ると試算
11.  １２．マルウエア　Emotet　への対応　 Jpcert/cc 2019/12/02
    1. ■外部からなりすましメルが届いたという報告があった場合どうすればよいか？
    2. ・なりすましメル送信者として表示されているアカントの端末がEmoteに 感染してメル情報やアドレス情報などが搾取された
    3. ・メルの送受信をしたことがある方や（取引先）の端末がEmotetに感染
       1. アドレス帳を搾取された（連絡をうけた方はEmotetに感染して いなが、メルアドレスがEmotetの送信先リストに加えられた）
    4. Emotetの感染有無を確認するためにはどうするばよいですか？
    5. ・EmoCheckによる感染有無の確認
       1. ＝＝処理省略＝＝
    6. ・なりすまされた本人へのヒアリング
       1. ※word file マクロ設定を確認
    7. ・ウイルス対策ソフトでスキャン
       1. マルウェアが検出されなくても定期的にスキャンする
    8. ・端末の自動起動設定の確認
       1. Emotetが存在する可能性の高いフォルダに含まれるEXECファイルが 設定されていないか確認をする
       2. 例：自動起動レジストリ、サビス、タスクスケジュルラ、

#### スタートアップフォルダ

* 1. ・メルサーバのログ確認
     1. 例：なりすましメル、Word添付メル、外部へ大量に送信
  2. ・ネットワークトラフィックログの
     1. 例：外部IPへ複数ポトにたいしてC2通信していない
        1. ・Emotetに窃取されたれメールの送信をとめることができますか
           1. 例：不特定多数の攻撃インフラがら送信されるため送信は

###### 停止できない

添付ファイルは取得されない

* + - * 1. 例：過去に送受信したメルアドレスと表示名
        2. 過去１８０日に送受信したメル件名とメル本文　１６０KB
        3. Webブラウザに保存されていた認証情報も漏洩する可能性がある
    1. ■感染するとどのような被害が起こるか

1.  １３．改正割賦販売法　２０１８年６月１日施行
   1. 加盟店を含むすべてのクレジットカド情報を取り扱う事業者に、カド情報保護対策が義務付けられた。カド会社、決済代行事業者、サビスプロバイダに加えてクレジットカド情報を自社システムで保持する加盟店は、PCI DSSへの準拠がもとめｔられている。脆弱性スキャン　年４回、PTT 1回年
2.  １４．サプライチェーンの定義
   1. サプライチェーンリスクは「悪意ある者が、妨害を目的に、悪意を持って望ましくない機能を投入する、または、保 護されたシステムの設計、完全性、製造、生産、流通、設置、操作、または保守を破壊し、当該システムの機能、 使用、または操作を監視、否認、中断する、または、縮退させるリスク」14 であると定義されています。サプライチェ ンへの脅威としては、妨害行為、改ざん、偽造、知的財産権の侵害、盗難、破壊、中断、漏洩、侵入、流用、輸出 規制違反、汚職、ソシャル・エンジニアリング、インサイダ脅威、擬似インサイダ脅威、国外所有などが挙げ られます。
   2. Section 806, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, http://www.gpo.gov/fdsys/pkg/BILLS111hr6523enr/ pdf/BILLS111hr6523enr.pdf Axelrod, C. Warren, "Mitigating Software Supply Chain Risk," ISACA JOnline, August, 2013, http://www.isaca.org/Journal/ archives/2013/Volume4/Pages/JOnlineMitigatingSoftwareSupplyChainRisk.aspx 15 Goertzel, Karen M., et al. State of the Art Report on Supply Chain Risk Management for the OfftheShelf (OTS) Information and Communications Technology (ICT) Supply Chain, U.S. Department of Defense, Information Assurance Technology Analysis Center (IATAC), (2010), p. 40. HYPERLINK "https://www.csiac.org/content/state-art-report-soar-security-risk-management-shelf-ots-information-and-communications-tech"https://www.csiac.org/content/stateartreportsoarsecurityriskmanagementshelfotsinformationandcommunicationstech
3.  １５．「中小企業の経営者のサイバーリスク意識調査２０１９」
   1. 一般社団法人　日本損害保険協会　２０２０年１月
   2. 調査目的：損保協会が２０１８年に日本企業１，１１３社に実施した「サイバー保険に関する調査２０１８」の結果、企業規模が小さくなるほどサイバーリスクにたいする危機意識が低く、取り組みが進んでいない実態が明らかになった
   3. ・サイバー攻撃があった祭の被害・損失
      1. 被害イメジは、「機密情報・個人情報の盗難」６８．９％
      2. 「企業イメジ・信用力の低下」も大企業と中小企業の経営者の回答に開きがある
   4. ・サイバー攻撃対策への必要性
      1. 「必要だとかんじている」中小企業　２２．９％　大企業　６６．７％
   5. ・今後打つべき対策　「OSやソフトウエアの脆弱性管理、ウイルス対策ソフト
      1. 導入」・・中小企業経営者　３０％
   6. 「社員教育・研修・訓練の実施」大企業　４６．４％
4.  １６．制御システムセキュリティの脅威と対策の動向
   1. およびCSSCの研究概要について
      1. 技術研究組合制御システムセキュリティセンタ
   2. ・制御システムネットワーク　図
      1. ・制御システムと情報セキュリティ
         1. 制御セキュリティ
            1. 可用性完全性機密性
            2. USBポート、リモートメンメンテナンス、端末入れ替
            3. 物理的侵入
            4. ※IEC６２４４３は制御システムの全レイヤ/プレイヤをカバ
            5. 先行する評価認証の規格（EDSA認証等）がIEC６２４４３へ
            6. 採用される方向
            7. シナリオベースのリスクアセスメントを繰り返し実施
            8. ※事業継続上の脅威を発見しうるサイバー攻撃シナリオを作成
            9. それらのシナリオに対する対策チェックリストにより、個別の
            10. シナリオの発現可能性を評価する。
      2. ・我が国の制御システムでの脅威
      3. ・EDS認証の全体像
      4. ・リスク分析
5.  １７．ビジネスメル詐欺（BEC)の事例
   1. サイバー情報共有インニシアティブ（JCSIP)運用状況２０１９年
      1. IPA
         1. １０月１２月
         2. 事例１：国内組織を狙った攻撃
         3. 事例２：海外グルプ企業を狙った攻撃
         4. Emotetへの感染を狙う攻撃メル
   2. ・ビジネんスメル詐欺（BEC)の事例
   3. ・日本語ばらまき型メール等の動向
   4. ・OLE機能を悪用した文書ファイルの手口（追加）
6.  １８．政府情報システムにおけるクラウドサービスの利用に関わる基本方針
   1. 平成３０年６月７日
   2. 各府省情報化統括責任者（CIO)連絡会議決決定
      1. ・基本方針
         1. クラウド・バイ・デフォルト原則
   3. ・クラウドサビスの利用メリット＜最新技術を合理的コストで利用
      1. 効率性の向上
      2. セキュリティ水準の向上
      3. 技術革新対応への向上
      4. 柔軟性の向上
      5. 可用性の向
   4. ＜コラム
      1. クラウドサービスが危険だろうとおもいこんではいけない
      2. 正しいクラウドサービスのみを選択
   5. ・具体方針
      1. クラウドサービスの利用検討プロセス
         1. ①業務の基本属性
         2. ②必要なサビスレベル
         3. ③さびｓ・業務の定常性
         4. ④業務量
         5. ⑤取り扱う情報
   6. ※認証制度
      1. ISO２７０１７
      2. JASAクラウドでキュリティ推進協議会CSゴルドマク
      3. 米国　FedRAMP
7.  １９．「個人情報の保護に関する法律についてのガイドライン」
   1. 及び「個人デタのろうえい等の事案が発生した
   2. 場合の対応について」
8.  ２０．Telework and Small Office Network Security　Guide
   1. CIS　Controols
   2. ・Network Security　Checklist P.22 参照
9.  ２１．テレワクセキュリティガイドライン
   1. 総務省　平成３０年　第４版
   2. ■テレワーク情報サイト　総務省
   3. ・テレワークに対する情報セキュリティっ対策のかんがえかた
   4. ・テレワークセキュリティ対策のポイント
   5. ・テレワークセキュリティ対策の解説
   6. ・情報白書　第４節ICTによる多様な人材の労働参加促進
   7. 平成３０年版
   8. ※導入効果　期待する狙いと目的
10.  ２２．ブロックチェンの特性から理解する社会実装の展望
    1. 「ブロックチェンの特性から理解する社会実装の展望効率化・コスト削減
       1. から高付加価値創出」　２０２０年　安田　央奈
    2. ブロックチェンはビジネスにおいて戦略的に重要な技術として選ばれ始めている。ブロックチェンは中央管理者無しに信頼性の高い記録によって取引を成立させることができる特性を持っており、これによって契約やワクフロの効率化・コスト削減効果が期待できる。そして、普及の段階を経て、例えば競争領域での競合他社間の協調のような新たなデタ共有の形といった高付加価値を創出していく。
    3. １．グローバルにおけるブロックチェンの潮流
    4. ２．ブロックチェンの特性
    5. ３．コンソーシアム内での効率化・コスト削減
    6. ４．競争領域での協調による得難い価値
11.  ２３．非金融分野におけるブロックチェンの活用動向調査
    1. 報告書（概要版）　２０１９年１２月　IPA
    2. ※注目分野
    3. ・サプライチェン
    4. ・電力
    5. ・データの記録、管理
    6. １．ブロックチェーン技術の概要
    7. ２．ブロックチェーンの活用動向
    8. ３．ブロックチェーン技術の展望
    9. ４.　ブロックチェン社会実装に関わる展望と課題
12.  ２４．米国におけるブロックチェンの現状
    1. ２０１８年　JETRO　（IPA)
    2. 1 サマリ 世界のブロックチェン市場は 2016～21 年までの 5 年間で年平均 81.2％のペスで成長し、2017 年時 の 9億 4,500万ドルは、2021年には 97億ドルに達することが予測されている。地域別では、2021年時に、 米国が最大市場として世界全体の 40％以上、次に西欧諸国、中国、（日本・中国を除く）アジア太平洋諸国 が続く。大きな支出の伸びが予想されている地域は、南米と日本であり、2016～21 年までの年平均成長率 はそれぞれ 152.5％、127.3％となっている。 ブロックチェンは、仮想通貨以外にも活用が期待されており、今回、仮想通貨、銀行間取引、ヘルスケア、 不動産、サイバーセキュリティ、IoT の事例を取り上げた。 連邦法で規制する動きなどはこれまでみられていない。トランプ政権はブロックチェン技術の活用に積極 的に取り組んでいる一方、仮想通貨がマネ・ロンダリングやテロ組織への資金源、租税回避、詐欺等に悪 用されることを懸念し、連邦政府レベルでは、各関連規制当局において仮想通貨に対する規制を見直す動 きがみられるようになっている。州政府レベルでは、これまでに大多数の州が仮想通貨及びブロックチェ ン技術に関する何らかの法規制を施行又は整備しつつあるが、こうした規制のほとんどは、既存の送金法 における仮想通貨の取引について明確にする内容である。他方で、統一州法委員会は 2017 年 7 月、仮想 通貨に関する州法間の整合性を図るため、「仮想通貨事業法に関する統一規則」を発表したが、これに対し、 ビットコイン財団は、同規則の内容がニュヨク州のビットライセンス規制と酷似している悪法として、州議 会議員・関係者から構成される全米州議会議員連盟に対し、これを採択しないよう呼びかけている。
    3. ■日本ブロックチェン協会　ブロックチェンの定義
    4. 「電子署名とハッシュポインタを使用し改ざん検知が容易なデタ構造を持ち、且つ、
    5. 当該デタをネットワク上に分散する多数ノドに保持させることで、高可用性および
    6. デタ同一性等を実現する技術を広義のブロックチェンと呼ぶ」
13.  ２４．NIST sp800171 (Ver2.o)
    1. ソホジャパン株式会社　２０１９．０９．１３
    2. ■NIST SP800171とは米国政府機関が定めたセキュリティ基準を示すガイドラインです。政府機関だけではなく、取引企業からの情報漏えいを防ぐため、業務委託先におけるセキュリティ強化を要求する内容になっています。
    3. ■サプライチェンのセキュリティ対策の海外の動き
    4. 米国は2016年にDFARS Clause252.2047012を発行、「米国防衛省と取引をするすべての企業に対して、NIST SP800171に準拠したITシステムの整備を要求」しています。
    5. ■各国も米国に追従しNIST　ｓｐ８００−１７２が実質上の国際標準
    6. 国防省と取引をしている全世界の企業に対してNIST SP800171への準拠が要求されており、米国防省と取引をする企業はNIST SP800171への対策は避けられません。
    7. また、米国政府だけの取り組みにとどまらず主要国でも米国に追随する動きがはじまっています。
    8. すなわち、NIST SP800171に準拠しない企業とその製品やサビスは、グロバルサプライチェンからはじき出されてしまうおそれがあるということです。
    9. ■国内での対応
    10. 日本政府は、防衛産業をハイレベルな産業サイバーセキュリティのモデルとすべく、防衛調達の新基準をNIST SP800171と同等にすることを決定しました。新基準への準拠は下請けとなる中小企業も対象となっています。
    11. ※極意へのサプライチェンセキュリティ追補内容
    12. 関連（１７１）での説明する観点から
    13. 組み込む、ただしその網羅性については、ISO2700も
    14. 含めて比較できるよう
14.  ２６．情報セキュリティ１０大脅威　各脅威の解説資料　２０２０年２月
    1. IPA
    2. ■「組織」向け脅威順位
       1. １．標的攻撃による機密情報の窃取
       2. ＜攻撃手口
          1. メールの添付ファイル、リンクを開かせる
          2. ウエブサイトの改ざん
          3. 不正アクセス
       3. ２．内部不正による情報漏洩
          1. アクセス権限の悪用
          2. 在職中に割り当てられたアカウント悪用
          3. 内部情報の不正な持ち出し
       4. ３．ビジネスメール詐欺による金銭被害
          1. 取引先との請求書の偽装
          2. 経営者等のなりすまし
          3. 窃取メールアカウントの悪用
          4. 社外の権威ある第三者へのなりすまし
          5. 詐欺の準備行為と思われる情報の搾取
       5. ４．サプライチェーンの弱点
          1. ＜要因
          2. 委託先組織のセキュリティ対策不足
          3. 委託先組織を適切に選定管理していない
          4. 再委託先や再々委託先の管理が難しい
    3. ※委託元組織からがバンスが効かない委託先組織がセキュリティ対策を
       1. 適切に実施していない。
    4. エアの更新脆弱性の解消リスク低減
    5. ウイルス対策セキュリティソフトに利用攻撃ブック
    6. パスワード搾取PWの管理・認証の強化窃取によるリスク低減
    7. 設定不備設定の見直し誤った設定を攻撃に利用されない
    8. 誘導脅威・手口を知る手口から重要な対策を理解する
15.  ２７．産業用制御システム（ICS)のセキュリティ
    1. １０大脅威と対策２０１９
       1. ２０２０年１月　IPA
       2. 1位　リムーバルメデアや外部機器経由のマルウエア感染
       3. ２位　インターネット及びイントラネット経由のマルウエア感染
       4. ３位　ヒューマンエラと妨害行為
       5. ４ 位　ソーシアルエンジニアリングとフイｯシング
       6. ５位　DOS・DDOS攻撃
16.  ２８．サイバーセキュリティ保険選定・契約時の８大チェック項目
    1. TecTagetジャパン　２０２０年２月２８日
    2. ①保険会社が契約会社を評価するプロセスが自社のセキュリティポリシィ
    3. に違反していないか
    4. ②保証フランの対象外の確認
    5. 暗号化されていないデータが対象可否
    6. ③暗号鍵の管理
    7. ④最新の技術、法規制、への対応
    8. ⑤内容の技術的評価
    9. ⑥その他
    10. 保険金の支払い例、自社のセキュリティポリシイの正確な開示、自社専門家
    11. 活用（インシデント時）
17.  ２９．移行が進むハイブリットクラウド、Azure環境特有のセキュリティ課題
    1. トレンドマイクロ　２０２０年２月２６日
    2. ※クラウド利用上のクラウド内セキュリティ管理
    3. ■クラウド上にデタやシステムを置く場合事業者とは別にユーザにも
    4. 責任を負うべき分野がある。
    5. それが、「共同責任モデル」と「多層防御」です。
    6. 具体的には、データ、エンドポイント、アカウント、アクセス管理分野
    7. とAzureのセキュリティサービスを組み合た多層防御がベストプラくティス。
18.  ３０．日本セキュリティ監査協会
    1. ２０２０年監査十大テーマ
    2. １．自然災害によるIT被害拡大
    3. ２．クラウド・バイ・デフォルト時代の新しい安全性評価制度の開始
    4. ３．クラウドサービスの障害による大規模なビジネんス影響
    5. ４．DX化の進展によりされに加速するセキュリティ人材不足
    6. ５．働き方改革の推進普及による脅威の発生
    7. ６．プライバシー保護の国際標準化に乗り遅れる日本企業
    8. ７．サプライチェーンの透明化で求められるセキュリティ対策強化
    9. ８．標的型ランサムウエアで倒産危機？システム全てが人質
    10. ９．クラウドサービスの管理・設定ミスによる情報漏洩
    11. １０．安易なアジャイル開発による脆弱なシステムの氾濫
19.  ３１．サイバーセキュリティ関係法令　Q＆Aハンドブック　VER1.0
    1. 令和２年３月２日　NISC
    2. ■サイバーセキュリティに関係する法令として、サイバーセキュリテ基本方法の
    3. 成立や個人情報保護法、不正競争防止法が改正されている。
    4. ２．本書で取り上げる主な法律について
    5. ■サイバーセキュリティ基本法（平成 26 年法律第 104 号） 「サイバーセキュリティ」の定義を置くとともに、基本法として、わが国のサイバーセキュリ ティ政策を推進するための様々な規定を定めている。
    6. ■ 民法（明治 29 年法律第 89 号） 契約に関する規律や、不法行為に基づく損害賠償請求等を規定している。
    7. ■会社法（平成 17 年法律第 86 号） 取締役に対し、サイバーセキュリティを確保するための体制を含む内部統制システム構築義 務を課している。 ○ 個人情報の保護に関する法律（平成 15 年法律第 57 号） 個人情報の取扱いに関する基本法と個人情報取扱事業者に対する義務等を定める。当該義務 の中に個人データの安全管理措置義務が含まれる。また、個人番号を含む個人情報（特定個人情 報）については行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）が規律を定めている。
    8. ■不正競争防止法（平成 5 年法律第 47 号） 不正競争の防止を目的の一つとしており、営業秘密や限定提供デタの保護や、技術的制限手 段の無効化、回避の禁止等を定める。
    9. ■ 著作権法（昭和 45 年法律第 48 号） プログラムを含む著作物の保護と複製権をはじめとする著作権等について規定している。
       1. ■ 労働基準法（昭和 22 年法律第 49 号） 労働基準を定める法律であり、企業の就業規則に関する規定などを置いている。その他、労働 契約に関する基本的な事項を定める労働契約法（平成 19 年法律第 128 号）等がある。 ○ 電気通信事業法（昭和 59 年法律第 86 号） サイバー空間における活動の基盤となるインターネットサビス等の電気通信事業に関する 諸規定や、通信の秘密等を規定している。 ○ 電子署名及び認証業務に関する法律（平成 12 年法律第 102 号） 一定の条件を満たす電子署名を手書き署名や押印と同等に通用する旨等を規定している。
       2. ■ 情報処理の促進に関する法律（昭和 45 年法律第 90 号） 情報処理安全確保支援士に関する規定や、独立行政法人情報処理推進機構（IPA）の業務とし てサイバーセキュリティに関する講習や調査等を措置している。
       3. ■ 国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号） 国立研究開発法人情報通信研究機構（NICT）の業務を定めるとともに、時限的な業務として IoT 機器の調査を行う「NOTICE」に関する規定を措置している。
       4. ■刑法（明治 40 年法律第 45 号） 不正指令電磁的記録に関する罪（いわゆるウィルス罪）をはじめとするサイバー犯罪を処罰す る規定を含む刑罰が規定されている。
       5. ■ 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号） 不正ログインといった不正アクセス行為や、いわゆるフィッシング行為を処罰する旨が規定 されている。
20.  ３２．産業用制御システムセキュリティガイドを読むために
    1. NIST　SP80082 Ver.2
    2. 産業用制御システム（ICS）セキュリティガイドへの導入　２０１８年１２月２５日
    3. 一般社団法人　日本電気工業会　技術部
    4. ■SP800８２ver2 その背景と概要サマリー
    5. ・SCDAシステム、分散制御システ, プログラマブル論理制御装置（PLC)などを含む、産業制御システムのセキュリティを確保するための、ガイダンスがまとまっている
    6. ICSの典型的なシステムトポロジー、脅威と脆弱性、その回避策、がまとめられている。
    7. ３３．米国防衛調達の重要情報CUI管理　２０２０年から第三者認証へ
    8. ■調達先業者はNIST sp800‐171に準拠した体制の自己証明（現行）から
    9. 新たにCMMC制度による認証になる。
    10. サイバーセキュリティ対策水準を５段階で評価する。
21.  ３３.制御システム関連のサイバーインシデント事例
    1. IPA　２０２０年３月
    2. 〜２０１９年ランサムウエアによる操業停止
    3. ■インシデント概要
    4. ２０１９年３月にノルウェに本社を置く世界有数のアルミ生産企業、Norsk Hydroがランサムウェア「LockerGoga」の被害を受け数カ月の長期期間にわたり生産量が低下した。
    5. ４０か国１６０拠点　PC２３，０００台のうち感染１１．０００台、暗号化２、７００台
    6. ３，０００台のサーバのうち１，１００台が感染、５００台が暗号化された。
    7. 特徴てきなのは、製造用のコンピュータも被害を受けた。
    8. ※事業被害ベスのリスク分析においては、自社の制御システムにとって回避すべき事業被害を明確化し、被害に至る攻撃シナリオをもれなく洗い出すことが重要である。
    9. 攻撃シナリオは、過去の発生した制御システムのインシデント事例を含む各種の公開情報を参考にしつつ、自社の制御システムの生じる脅威とその影響を検討するが、具体的な攻撃手順を想定することで、セキュリティ対策を効率的にすすめることが可能となる。
22.  ３４．JPCERT/CCに報告されたフィッシングサイトの傾向
    1. ２０２０年３月１９日　JPCERT/CC
    2. ■年間１９，０００件のインシデント報告の５６％がフィッシングサイト情報の報告
    3. ・タゲット業種　Eコマス、金融
    4. ・半数以上がHTTPS使用
    5. ・フイッシングサイト停止期間半数以上通知後３日で停止
    6. ・巧妙な正常なサイトを偽装
23.  ３０．個人情報保護法改正案
    1. ・個人利用停止案件の緩和
    2. ・開示方法の指定
    3. ・第三者記録の開示請求
    4. ・罰金１億、外国事業者にも対象
24.  ３５．ビジネスメール詐欺の実態調査報告書
    1. JPCERT/CC　2020年３月二十五日
    2. ・調査報告、被害状況、教訓
    3. ・対策　実務面、技術面
    4. ・国際的な取り組み例
    5. ・ビジネんスE－mail 詐欺の対策 /対応
       1. フィッシング対策
       2. 不正アクセス対策
       3. マルウエア対策
       4. 内部不正への取り組み
       5. 検知する仕組み
       6. 研修、訓練
       7. ログの保管
       8. 発覚後のはあく
       9. 騙されて行った送金の取り消し
25.  ３６．5G CYBERSECURITY Preparing a Secure Evolution to 5G
    1. Draft February 2020 2020 04 13 NIST
    2. ■Purpose 82 As 5Gbased networks are deployed in our nation and across the world, there is great promise 83 of positive changes in the way humans and machines communicate, operate, and interact in the 84 physical and virtual world. With cellular networks transitioning from 4G to 5G, it is critical for 85 organizations to understand and address the challenges, opportunities, and risks associated with 86 the use of 5G networks
    3. ■96This project will identify a number of 5G use case scenarios and demonstrate how the 97 components of the 5G architecture can provide security capabilities to mitigate identified risks 98 and meet industry sectors’ compliance requirements.
    4. ■概要
    5. セルラネットワクは4Gから5Gに移行し、5Gネットワ​​クはサイバーセキュリティ保護を強化します。このプロジェクトでは、いくつかの5Gユスケスシナリオを特定し、特定されたリスクを軽減して業界セクタのコンプライアンス要件を満たすために5Gアキテクチャコンポネントを強化する方法をそれぞれに示します。このプロジェクトでは、商用およびオプンソス製品が5Gの各ユスケスシナリオのサイバーセキュリティ標準と推奨プラクティスをどのように活用できるかを実証するとともに、5Gのセキュリティ機能の利用方法を紹介します。5Gテクノロジの開発ペスと商用5Gテクノロジの可用性に合わせて、段階的なアプロチが採用されます。
    6. この反復的なアプロチにより、フェズが進化して新しく導入されたセキュリティ機能を利用できるようになり、プロジェクトに柔軟性を追加できます。このプロジェクトにより、無料で利用できるNISTサイバーセキュリティ実践ガイドが作成されます。
    7. ３２．NIST SPECIAL PUBLICATION 18004 Mobile Device Security: Cloud and Hybrid Builds
    8. モバイルテレワク環境に対するセキュリティ対策概要
    9. 改定版に取り込み可能
26.  ３７．セキュリティ仕様策定プロセス（案）
    1. ～Windows Active Directory環境用セキュリティガイドライン対応～
    2. 2020年3月
    3. セキュリティ検討プロジェクトチム
    4. 《目次》
    5. １　序章・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
    6. 2　セキュリティ仕様策定の課題とセキュリティガイドライン　・・・・・・・・・・・・・・・　8
    7. ３　セキュリティ仕様検討プロセス・・・・・・・・・・・・・・・・・・・・・・・・・・・　13
    8. 【参考1：セキュリティ策定の現状と課題】・・・・・・・・・・・・・・・・・・・・・・・　23
    9. 【参考2：SQLインジェクション事件（東京地裁平成26年1月23日判決）】・・・・・・・　27
    10. 【参考3：セキュリティ仕様策定プロセスイメジ図】・・・・・・・・・・・・・・・・・・　29
    11. 【参考4：緩和策実装検討シト例】・・・・・・・・・・・・・・・・・・・・・・・・・・　30
    12. 【参考5：デフォルト緩和策　端末編　＜一覧表】・・・・・・・・・・・・・・・・・・・　31
    13. 【参考5：デフォルト緩和策　端末編　＜詳細】・・・・・・・・・・・・・・・・・・・・　32
    14. 【参考6：デフォルト緩和策　セキュリティ仕様・Webアプリケション編】・・・・・・・・　42
    15. 【参考7：汚染される開発環境】・・・・・・・・・・・・・・・・・・・・・・・・・・・・　46
    16. 【参考8：セキュアコディングガイド】・・・・・・・・・・・・・・・・・・・・・・・・　47
27.  ３８．報システム開発契約のセキュリティ仕様作成のためのガイドライン
    1. 重要インフラや大企業基幹系情報システムの受託開発に際して、ユザ企業とITベンダがセキュリティ仕様を策定する際の、脅威分析とその対策を検討するための参照情報です。セキュリティ攻撃手法ごとにその影響と対策（緩和策）などを説明しています。脅威については、NIST（米国国立標準技術研究所）の委託を受け、世界中の脆弱性情報の採番を行っている非営利法人 HYPERLINK "https://www.mitre.org/"MITRE HYPERLINK "https://www.mitre.org/" が公開する脆弱性を悪用した実際の攻撃を戦術単位で分類したナレッジベス HYPERLINK "https://attack.mitre.org/"ATT&CK Matrix for Enterprise HYPERLINK "https://attack.mitre.org/" をベスに、日本国内で発生したインシデントで実際に使われ、かつ、実績の多いものを有識者が抽出しています。また、脅威に対する対策は、MITRE ATT&CK Matrix for Enterprise の推奨する緩和策に加え、いくつかのガイドラインの緩和策を参照しています。
    2. 本ガイドラインはWindows Active Directory環境を前提とするものです。
    3. 2020年4月の改正民法（債権法）施行に伴い、経済産業省の「情報システム・モデル取引・契約書」の改訂作業を独立行政法人情報処理推進機構社会基盤センタモデル取引・契約書見直し検討部会が実施しました。この見直しに際し、セキュリティ関連に特化して、「モデル取引・契約書」改定版あるいは追補版に盛り込むべき内容を検討し、その結果を提案することを目指しセキュリティ検討プロジェクトチムが設置され、その議論においてユザとベンダがセキュリティ仕様を策定する際の、検討のためのたたき台として一定のセキュリティ設定を提示すべきとなり、本ガイドラインが作成されました。
    4. セキュリティ検討プロジェクトチームメンバ:
       1. HYPERLINK "https://www.ipa.go.jp/ikc/about/committee-01.html#model\_wg1pt"https://www.ipa.go.jp/ikc/about/committee01.html#model\_wg1pt
28.  ３９．Cloud computing Synopsis and Recommandation sp800146
    1. ■クラウドセキュリティの基本概念と概要
29.  ■.Generak Access Contorol Guidnce for Cloud system
    1. SP800210(draft)
30.  ４０．Trend Micro Cloud One 2020年５月７日
    1. トレンドマイクロの「Trend Micro Cloud One」は、パブリッククラウド上で稼働する仮想サーバなどを、セキュリティ上の脅威から守るソフトウエア製品群である。保護対象にインストールして使う。管理サーバ機能はSaaS型で提供する。
    2. Cloud Oneは6つのサービスから成る。まず、保護対象別に（1）仮想サバ向けの「Workload Security」、（2）サバレス環境向けの「Application Security」、（3）ネットワーク向けの「Network Security」、（4）コンテナ向けの「Container Security」、（5）クラウドストレージ向けの「File Storage Security」の5種類がある。加えて（6）クラウド環境の設定の不備を可視化する「Conformity」を提供する。
31.  ４１．VPNが絶対安全とは言い切れない！セキュリティリスクについて詳しく解説
    1. ITSCOM　株式会社
    2. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#VPN"1 インタネットVPNについて
    3. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#VPN-2"1.1 VPNって何?
    4. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#VPN-3"1.2 VPNを利用する主な場所
    5. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#VPN-4"1.3 VPNの仕組み
    6. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#VPN-5"1.4 VPNのメリット
    7. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#VPN-6"2 VPN導入の失敗例
    8. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i"2.1 セキュリティ意識の低さから起きた情報漏洩
    9. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-2"2.2 コスト重視しすぎた故に通信障害発生
    10. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-3"2.3 リテラシーの低さが原因で顧客からクレーム発生
    11. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#VPN-7"3 リスクもある！インターネットVPNの問題点
    12. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-4"3.1 情報漏洩が起きる可能性がある
    13. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-5"3.2 通信に影響が出る場合がある
    14. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-6"3.3 コストが無駄になる可能性がある
    15. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-7"3.4 ウィルスに感染する可能性がある
    16. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-8"3.5 通信ログが漏れる可能性がある
    17. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-9"4 イッツコムモバイル閉域接続サービスならより安全度が高い
    18. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-10"4.1 インターネット経由ではないネットワークでより安全
    19. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#SIMVPN"4.2 専用SIMだけでVPNアプリは不要
    20. HYPERLINK "https://www.itscom.co.jp/forbiz/column/vpn/236/#i-11"4.3 社外でも社内でもセキュリティポリシーが適用される
32.  ４２．プライバシ・セキュリティ管理策を規定したNST　SP　８００−５３
    1. ManageEngin　ZOHO株式会社
    2. ・NIST　sp８００−５３実践におけるヒント
    3. ・プライバシ管理策
       1. ・権限と目的
       2. ・データの品質と完全性
       3. ・個人参加による個人救済
       4. ・透明性
       5. ・責任説明、監査、およびリスクマネジメント
       6. ・データの最小化と保持
       7. ・セキュリティ
       8. ・使用制限
    4. セキュリティ管理策
       1. ・モバイルコンピュティング
       2. ・クラウドコンピュティング
       3. ・信頼性
       4. ・セキュリティ保証
       5. ・情報システムの回復性
       6. ・インサイダ脅威
       7. ・サプライチェーンとセキュリティ
       8. ・APT攻撃
    5. NIST　ｓｐ８００−５３とNISTｓｐ８００−１７１の違い
       1. ・目的　CIの保護　　CUIの保護
       2. ・対象組織　連邦政府　民間企業
    6. 追加
33.  ４３．パターンランゲージ
    1. トランスフォメションに対応するためのパタン・ランゲジ（略称トラパタ）
    2. 2020年5月14日公開
    3. 独立行政法人情報処理推進機構
    4. 社会基盤センタ
    5. パターンランゲージは、良い実践の秘訣を共有するための方法です。成功 している事例やその道の熟練者に繰り返し見られる「パタン」を抽出し、抽 象化を経て言語（ランゲジ）化しています。そういった成功の“秘訣”とも いうべきものは、「実践知」「センス」「コツ」などといわれますが、なかなか他の 人には共有しにくいものです。パタン・ランゲジは、それを言葉として表現 することによって、秘訣をもつ個人が、どのような視点でどのようなことを考え て、何をしているのかを他の人と共有可能にします。 「パタン」は、いわば型のようなものをもっており、決まったルルで書かれて います。どのパタンも、ある「状況」(context)において生じる「問題」 (problem)と、その「解決」(solution)方法がセットになって記述され、それ に「名前」（パタン名）がつけられています。このように一定の記述形式で 秘訣を記することによって、「名前」（パタン名）に多くの意味が含まれ、そ れが共通で認識され、「言葉」として機能するようになっているのです。
34.  ４４．「デジタル・トランスフォーメーション（DX）推進に向けた企業と IT 人材の実態調査」報告書のポイント
    1. 2020年5月14日公開
    2. 独立行政法人情報処理推進機構
    3. 社会基盤センター
    4. 企業としての問題既存のビジネスモデルや業務スタイルから脱却できておらず、デジタル型ビジネスモデルへの転換が 進んでいない経営層の、デジタルがもたらす変革への理解と認識やIT活用に対する見識が十分ではない。DX実施以前問題としての、変革への抵抗や危機感の共有不足。実施にあたっても、既存の人事制度や組織文化が変革を阻害。従来型システム化技術から脱却できず、先端型IT人材が活躍する環境や場が整えられていない。 個人としての問題デジタル技術による自身を取り巻く環境変化に対する感度の低さや危機感の欠如から、スキルアップ 意欲の低い先端IT業務非従事者。せっかく学んでもそれを活かす場がない。（そのような場を自ら確保しようとしない）自身のキャリアに対する当事者意識が希薄。 DXへの取組みが一部の企業を除いて進展していないという背景には、デジタル化がもたらす第4次産業革 命が進む中で、産業構造や消費者行動・考え方が大きく変化しているにも関わらず、企業の方向性と個人 のあるべき姿が描けていない、という本質的な課題があると考察される。 3.課題解決の方向性 デジタル技術を使うことがDXではなく、企業や事業のあり方そのものの変革が本来のDXであることは言 うまでもないことであるが、上記の考察からはそれに加え、一人一人の“個人”や、さらには“企業と個 人の関係性”の変革も等しく重要な要素であると言うことが出来る。デジタル時代の働く場、スキルアッ プする場としてふさわしい、“個人に選ばれる企業”への変革が企業に求められると同時に、自身のスキル アップ、キャリアアップは自らがマネジするという、“企業に依存しない個人”への変革、そして両者の “新たな関係性の構築”が、デジタル時代を迎えるにあたっての課題解決の方向性と言える。 具体的には、企業には目指すデジタル経営の姿や長期事業ビジョン、そしてその実現のために必要な人 材要件（プロファイル）を明示することが求められる。また、内部的には、個々の人材の能力や価値を正 当に評価し処遇する仕組み作りや、リスクにチャレンジする組織文化の醸成、デジタル技術など新技術の 積極的な採用による業務生産性の向上や継続的にスキルアップ出来る“場”の提供など、エンプロイ・ エクスペリエンス（従業員経験価値）を高める施策が必要である。 一方で個人側には、人生100年時代と言われるまでもなく、個人の就業期間が企業の平均寿命を逆転する 時代の中で、特定の一企業に閉じない、長期視点かつ柔軟なキャリア形成や、“社内価値”に留まらない、 自分自身の市場価値の継続的向上とそのアピルを考えていくことが求められる。
    5. ■調査実施事項と主要ポイント
    6. DXへの取組実態 [実施事項] IT企業、ユザ企業、デジタルビジネス推進部門を設置している企業に対するDX取組み状況 や、そのために必要な人材獲得・育成に関するアンケト調査 （アンケト調査の概要は後述） [主要ポイント]従業員1001名以上の企業群では77.6％がDXに取り組んでいるとしたのに対し、300名以下の企業群では 40%未満となっている。特に、100名以下の企業群では29.2%であり、企業の規模によるDXへの取組みの 格差が大きい。（報告書概要編第1章ポイント①参照）DXへの取組みで成果が出ている企業群では、全社戦略に基づいた全社的取組みであることや、IT業務 が分かる役員の存在比率が高いといった特徴が見られる。また、組織文化やDX推進上の課題認識にお いても成果有り企業と無し企業には大きな違いがある。（報告書概要編第1章ポイント④、⑤参照）
    7. ■企業としての問題既存のビジネスモデルや業務スタイルから脱却できておらず、デジタル型ビジネスモデルへの転換が 進んでいない経営層の、デジタルがもたらす変革への理解と認識やIT活用に対する見識が十分ではない。DX実施以前問題としての、変革への抵抗や危機感の共有不足。実施にあたっても、既存の人事制度や組織文化が変革を阻害。従来型システム化技術から脱却できず、先端型IT人材が活躍する環境や場が整えられていない。
    8. ■ 個人としての問題デジタル技術による自身を取り巻く環境変化に対する感度の低さや危機感の欠如から、スキルアップ 意欲の低い先端IT業務非従事者。せっかく学んでもそれを活かす場がない。（そのような場を自ら確保しようとしない）自身のキャリアに対する当事者意識が希薄。 DXへの取組みが一部の企業を除いて進展していないという背景には、デジタル化がもたらす第4次産業革 命が進む中で、産業構造や消費者行動・考え方が大きく変化しているにも関わらず、企業の方向性と個人 のあるべき姿が描けていない、という本質的な課題があると考察される。
    9. ■課題解決の方向性 デジタル技術を使うことがDXではなく、企業や事業のあり方そのものの変革が本来のDXであることは言 うまでもないことであるが、上記の考察からはそれに加え、一人一人の“個人”や、さらには“企業と個 人の関係性”の変革も等しく重要な要素であると言うことが出来る。デジタル時代の働く場、スキルアッ プする場としてふさわしい、“個人に選ばれる企業”への変革が企業に求められると同時に、自身のスキル アップ、キャリアアップは自らがマネジするという、“企業に依存しない個人”への変革、そして両者の “新たな関係性の構築”が、デジタル時代を迎えるにあたっての課題解決の方向性と言える。 具体的には、企業には目指すデジタル経営の姿や長期事業ビジョン、そしてその実現のために必要な人 材要件（プロファイル）を明示することが求められる。また、内部的には、個々の人材の能力や価値を正 当に評価し処遇する仕組み作りや、リスクにチャレンジする組織文化の醸成、デジタル技術など新技術の 積極的な採用による業務生産性の向上や継続的にスキルアップ出来る“場”の提供など、エンプロイ・ エクスペリエンス（従業員経験価値）を高める施策が必要である。 一方で個人側には、人生100年時代と言われるまでもなく、個人の就業期間が企業の平均寿命を逆転する 時代の中で、特定の一企業に閉じない、長期視点かつ柔軟なキャリア形成や、“社内価値”に留まらない、 自分自身の市場価値の継続的向上とそのアピルを考えていくことが求められる。
35.  ４５．Zoom、Cisco WebEX、TeamsをCASBでセキュリティで比較。結局Zoomは何が駄目?
    1. HYPERLINK "https://news.yahoo.co.jp/byline/ohmototakashi/20200424-00174931/"https://news.yahoo.co.jp/byline/ohmototakashi/2020042400174931/
    2. ■噂で安全、危険を判断するのではなく、客観的な指標作りが大切
    3. WebEXが取得している認証プログラム
    4. HIPAA、PCI Compliance、SOC2、ISO 27001、SAS 70、Privcy Shield、FISMA、FedRAMP
    5. Zoomが取得している認証プログラム
    6. Trustee / BBB、SOC2、SAS 70、Privacy Shield、FedRAMP
    7. Teamsが取得している認証プログラム
    8. HIPAA、CSA Star、SOC2、ISO 27001、SAS 70、Privcy Shield、ISO 27018、FISMA、SSAE16
    9. 参考情報　Best Practices for Securing Your Virtual Classroom
       1. HYPERLINK "https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtu"https://blog.zoom.us/wordpress/2020/03/27/bestpracticesforsecuringyourvirtu
    10. ■多くの企業がクラウドのセキュリティ評価に課題を抱えている
    11. 新型コロナウィルスによる「緊急事態宣言」発令によって多くの企業が急速にテレワク環境の整備に追われている。テレワーク実現にあたって直ぐに利用を開始できるクラウドサビスの利用を検討する企業が多い。こういったクラウドサービスの利用に伴い情報システム部門を悩ませているのが「クラウドサビスのセキュリティ評価」だ
    12. ■最も安全と評価されたのはCisco WebEX
    13. こちらが、MVISION CloudによるZoom、Cisco WebEX、Teamsの比較結果となる。RISKと書かれた行が総合得点となり数字が小さい程安全性が高いという評価になる。Cisco WebEXが2点で最も安全性が高いという結果になった。次いでTeamsが3点で二番手、最後にZoomが4点で三番手となった。
    14. ■ビジネスリスク
    15. 各種認証プログラム等の取得状況等が評価される。ネット上で「Zoomは危険」という声も目にするが、米国政府が調達するクラウドサービスの基準を満たしていることを証明する「FedRAMP」や、EUと米国間の個人情報転送を認める「Privacy Shield」を取得している点から考えると、一般的な企業が利用する分には十分なセキュリテイに対する配慮が行われていると考えて良いだろう。
    16. 敢えて用途に応じて利用するオンラインビデオ会議サービスを分けるとするならば、医療情報等を扱うビデオ会議の場合には、HIPPAを取得しているWebEXやTeamsが適しているだろう。金融機関等ではPCI Complianceを取得しているWebEXが適しているだろう。
    17. ■テレワクで注目されるゼロトラストとは?従来型VPNではテレワク経由のマルウェア感染拡大を防げない
        1. HYPERLINK "https://news.yahoo.co.jp/byline/ohmototakashi/20200217-00163410/"https://news.yahoo.co.jp/byline/ohmototakashi/2020021700163410/
36.  ４６．ゼロトラストとは?
    1. 企業がクラウドやモバイルを自社の情報システムに採用するようになり、社外でも仕事をする働き方改革を推進するようになると、企業の中と外といった「境界」の定義が曖昧になってきた。このような明確な「境界」が存在しなくなってきた現在の企業ネットワークにおいて、境界にファイアウォールを設置して守るといった「境界型防御」という考え方が通用しなくなってきた。
    2. 場所を守る境界型セキュリティ
    3. インターネットが登場してから、企業のセキュリティは、「社外は危険、社内は安全」という「場所を守る境界型セキュリティ」が主流で有り、企業の外側と内側にファイアウーォルを置き内側を守るという考え方が一般的であった。この考え方では社外からのアクセスに対しては危険と考えアクセス制御を用いるが、社内は安全とみなしアクセス制御は実施しないという考え方に基づいていた。
    4. 境界型セキュリティの限界
    5. しかし、企業が働き方改革等の目的でOffice365やiPhoneといったクラウドサービスやモバイルシステムの導入を進めたことで、従来の境界を定めてファイアウーォル等で企業の中を外部からの侵入者から守るという考え方が通用しなくなってきた。
    6. 経過
    7. １９８０　ホスト型
    8. １９９０　クラサバ
    9. ２００　インターネット対応　＊境界型防御
    10. クラウド・モバイル　＊　社内外の境界型防御が崩壊　＝ゼロトラストへ
    11. 「ゼロトラストアキテクチャ」では、境界型セキュリティで採用されていた「場所」による安全性の判定では無く、「守るべき資産」を定義し、そこにアクセスする「ユザ」や「端末」「アプリケション(サビス)」の信頼性を常に評価するアキテクチャへと変化する。
    12. 例えば、社内からのアクセスであっても、「守るべき資産」に対してアクセスしようとするユザが、ユザは本人か?そのユザはこのリソスにアクセスする権限を持っているか?利用している端末は安全か?といったことを検閲することで、正しい権限を持ったユザが本人だと認められた場合のみ、初めてアクセスが許可される。
    13. ・特徴1:最小権限
    14. ゼロトラストアキテクチャでは、最小権限の考えが適用されるので、ユザが例えIDとパスワードによる認証が成功したとしても、そのユザがアクセス権限を持つアプリケションにのみアクセス可能となる。ポトスキャンなどを実行したとしても、アクセスが許可されているアプリケションの通信ポトにしかスキャンを実施することは出来ない。この特徴によってマルウェアが横方向に感染を拡大する偵察活動を封じることが出来る。
    15. 特徴2:通信セッションの検閲
    16. VPNでは一度接続されたセッションは原則張りっぱなしとなる。例え中間者攻撃等でセッションが奪われていたとしても再検証されることはない。しかし、ゼロトラストアキテクチャでは「10秒前に正常だったセッションが今も正常で有るとは限らない」といった考えに基づき、定期的に検閲する。
    17. 特徴3:高度なユーザ認証
    18. 多要素認証等の認証方式を採用しており、ID/PW以外の要素を用いて正当なユザであることを評価する。
    19. 特徴4:端末の信頼性評価
    20. 証明書等を用いて、アクセスしている端末が会社支給の端末か、私用の端末か?等を判定する。更に、アクセスしている端末のOSバジョンやパッチの適用状況、マルウェア対策アプリのシグネチャ等が最新か?等をチェックし、信頼出来ない端末で有ると判断されれば接続を拒否するといったことが可能になる。
    21. ■NIST８００−２０７　ゼロトラスト
    22. 追加デタセキュリティのために、従来のワイドネットワク協会の下にある小さなリソースグループの周囲にマクロ境界を作成する行為として定義。
    23. 完全な定義はない。
37.  ４７．米国政府やFBI等が外国からのサイバー攻撃に対抗するため「パッチ適用キャンペーン」を呼びかけ
    1. HYPERLINK "https://www.us-cert.gov/ncas/alerts/aa20-133a"https://www.uscert.gov/ncas/alerts/aa20133a
    2. ■米国政府及び、FBI (Federal Bureau of Investigation)、Cybersecurity and Infrastructure Security Agency (CISA)は、公共および民間企業の IT セキュリティ専門家に対して、サイバー攻撃者によって悪用される可能性がある「よく知られた脆弱性」へのパッチ適用を優先して対処するよう HYPERLINK "https://www.us-cert.gov/sites/default/files/publications/AA20-133A\_Top\_10\_Routinely\_Exploited\_Vulnerabilities\_S508C.pdf"呼びかけた。
    3. ■最も悪用された脆弱性トップ10 2016年2019年
    4. 同レポトによると、2016年から2019年の間に最も悪用された脆弱性の上位10件は以下のとおり。
    5. CVE201711882、CVE20170199、CVE20175638、CVE20120158、CVE20190604、CVE20170143、CVE20184878、CVE20178759、CVE20151641、CVE20187600。
    6. ・米国政府の技術分析によると、悪意のあるサイバー犯罪者は、Microsoft の Object Linking and Embedding (OLE) 技術の脆弱性を悪用することが最も多いとされている。OLEは、スプレッドシトなどの他のアプリケションのコンテンツを文書に埋め込むことを可能にする。OLEに次いで2番目に報告された脆弱性技術は、WebフレムワクのApache Strutsであった。
    7. ・トップ 10の中で、中国、イラン、北朝鮮、ロシアの国家系サイバー攻撃者に最も多く利用されている脆弱性は、CVE201711882、CVE20170199、CVE20120158の3つであった。これら3つの脆弱性は、いずれもMicrosoftのOLE技術に関連する。
    8. ・2019年12月現在、中国の国家サイバー攻撃者は、2015年に米国政府が公開した脆弱性（CVE20120158）を頻繁に悪用しており、この脆弱性が最も利用されているとされている。この傾向は、組織がこの脆弱性に対するパッチをまだ広く実装していないことを示唆しており、中国の国家サイバー攻撃者は、この脆弱性が有効である限り、サイバー攻撃手法に組み込み続ける可能性があることを示唆している。
    9. ・2019年初頭に発表された米国の業界調査でも同様に、悪意のあるサイバー攻撃者が最も一貫して悪用した脆弱性はMicrosoftとAdobe Flash製品であることがわかった。 業界調査で最も悪用された脆弱性トップ10のうち4つが本アラトのリストにも登場しており、米国政府と民間企業のデータソスがセキュリティを強化するためにどのように相互に補完し合うかが浮き彫りになっている。
38.  ４８．改正民法煮よる瑕疵担保責任の期限延長
    1. ■２０２０年４月の民法改正において、瑕疵担保責任に関する項目が変更された。
    2. ①システム完成後に見つかったバグ責任が１年から５年に延長
    3. ②バグ発見後１年以内であれば損害賠償請求ができる
39.  ４９．ゼロトラスト考察NIST　SP８００−２０７
    1. CISCO　JAPAN　BLOGセキュリティ
    2. ■Zero　Trustの基本と定義
       1. ・必要最小限の特権のみをアクセスに付与しリリスを制限
       2. ・リソースの保護方法、信頼が暗黙にふよされず、継続評価
       3. ・Zero　Trust：情報システム、サビスへのリクエスト毎のアクセス決定を正確に実行する、また、その不確実性を廃除するっために設計されたコンセプトとアイアのコレクション
       4. ・Zero Trust　Architecture(ZTA)：コンセプト、コンポネント、ワクフロ、ポロシイを利用する組織のサイバーセキュリティプラン
    3. ■Zero　Trustと境界セキュリティ
    4. ■Zero Trustの原則
    5. ■Zero　Trusｔの論理アキテクチャ
    6. ■Zero Trust　アキテクチャアプロチ
       1. ・拡張ID
       2. ・マイクロセグメンテション
       3. ・ネットワクインフラとSDP
40.  ５０．リモート署名ガイドライン
    1. 日本トランストテクノロジ協議会　JT2A
    2. ■新型コロナウイルスの影響でテレワク、在宅勤務が多くなり、遠隔（リモト）による電子申請や電子契約の利用が急務となっている。
    3. 日本政府の施策では、2016年からマイナンバカドの利活用が進み、2017年にマイナポタルにおいて各種の申請や手続きの電子化が促進され、また、2019年1月に電子委任状の普及の促進に関する法律が施行され、国民にとっても電子証明書及び電子署名がより身近に利用できる環境が整った。 これらの環境を利用したサビスの中でも、特に電子的な契約では、署名者のIT環境の変化や電子的に契約を行う上での署名鍵の管理の負担軽減のために、リモト署名サビス（＊１）を活用した電子契約サビスも存在している。
    4. 現在では民間事業者が提供する多くの電子契約サビスの中でリモト署名が採用されているが、その方法は様々である。電子契約では、利便性が高く、かつ安全なサビスが求められるが、その安全性や信頼性の指標が定まっていない。
    5. JT2Aでは、経済産業省の2015年度、2016年度の電子署名法研究会の検討結果を受けてリモト署名事業者や関係事業者及びリモト署名の利用者がリモト署名の理解を深め、一定の指標として参照可能なリモト署名サビスのガイドラインを作成した。
41.  ５１．GUID to SSL VPNS 　NIST　SP800133 25/4/2020
    1. ＊テレワクモバイルのセキュリティ関連について基本資料
    2. Guidelines on Securing Public Web Servers SP80044
    3. 中小企業向けっテレワクッ導入に関する実体調査　IPA
42.  ５２．セキュリティ仕様プロセス（案）IPA
    1. セキュリティ検討プロジェクトチム
    2. 〜Windows　AC地ヴェDirectory　環境セキュリティガイドライン対応〜
    3. ■２０２０年４月から施行される民法改正では、請負契約不適合に関する担保責任
    4. の規律が一新された。ベンダは、開発時の背キュリティ水準にそったセキュリティ対策を納入物に施していなければならない。
    5. ベンダの重大な過失により脆弱性があることを知らずに引き渡した場合担保責任の期間が提供されない。
    6. 本書は、情報システム調達に伴うシステム開発業務プロセスにおいて、」最適なセキュリティ仕様を策定する為の理想的なモデルプロセスとして解説したものである。
43.  ５３．エンタプライズ向けパッチ管理技術ガイド　NIST８００−４０　R3
    1. ■パッチ管理の課題
       1. タイミング、優先順位つけ、てすと
       2. パツチ管理の構成　適用に複数のメカ二ズム
       3. その他の課題
    2. ソフトウエアイベントトリ管理
       1. リソース負荷
       2. インストールの副作用
       3. パッチ実装の検証
       4. アプリケーションのホワイトリストへの登録
44.  ５４．　Guid to Enerprise Telework　Remote Access ,AND　Bring Your Own Deviv
    1. NIST80046 r2
    2. ■Guid to Enterprise Telewok,Remote Access,and Bring Your
       1. Own Devicee (BYOD) Securrity NIST 80046
    3. テレワク環境に関するモバイルセキュリティ運用について
45.  ５５．改正民法対応モデル取引・契約書に適したセキュリティガイドライン
    1. IPA 20200421
    2. システム開発関連契約における納品物において、セキュリティ上の不具合による情報漏洩等、その他重大なインシデントが発生したような場合は、ベンダの契約不適合を問われる可能性がでてくる。その課題解決の一助とするべく、セキュリティ検討プロジェクトチムは、企業システムで広く使用されているWindows、Linuxを対象に、MITRE ATT&CKでまとめられたサイバー攻撃の戦術および攻撃手法をベスに、最近の攻撃に利用されている攻撃手法の実績や、攻撃者の観点から見た攻撃手法の利用頻度等を勘案した重み付けを専門家チムで絞り込み、それに対する具体的な対策や緩和策を整理した。また、それらの対策・緩和策に具体的な実装方法を盛り込むために、米国国防総省が提示しているSTIGsをはじめ、その他各ソフトウェアメカが提示するSTIGsに記述された内容と紐付けを実施することで、これまでにない脅威ベスによる実質的で具体的な対策・緩和策を示したセキュリティガイドラインを目指した。
46.  ５６．経産、総務省　クラウド・バイ・デフォルト原則　政府調達サビス　５３への準拠が求めれれる
    1. Ver5.0
       1. ・汎用コンピュティタシステム・サイバーフジカルシステム　CPS
       2. ・クラウド、モバイル、IOT
       3. ・プライバシ保護
       4. ・ISO２７００１やCSFとの整合性
47.  ５７．サイバーセキュリティ経営ガイドラインVer2.0実戦のためのプラクティス集　第２版
    1. ■ガイドライン１０重点１０項目を実践する際に参考となる考え方やヒント、実践手順、　　　　　実践事例が記載されてている。
    2. ■国内で実際におこなわれている事例を基にしたプラクティス集
    3. ■フォーカルポイント
    4. ー指示４　制御システムのセキュリティリスク分析の取り込み
    5. ー指示５　サイバーセキュリティリスク対応　防御・検知・分析　実地体制
    6. Zero　Trust
    7. ー指示７　インシデント発生時の対応体制の整備
    8. ①検知　②報告　③封じ込め　④復旧　・・・参照文献
    9. ー指示８　IT-BCP　NIST　公共事業体の自然災害対応　民間への取り込み
    10. ■第３章から選択事項
    11. ーサイバ保険　保証範囲　・・事業中断も保証範囲
    12. ークラウド　SCO報告書　SCO1　財務関連　SCO2　CIA　内部統制への外部監査
    13. ー工場部門　DX対応とセキュリティ対策
48.  ５８．SDP　ソフトウェアデファイン境界　　CSA　クラウドセキュリティアライアンス
    1. ■SDP software defined parameter
    2. zro trust の本命
    3. Zero Trustの大本命 SDPについて｜技術ブログ｜C&S ENGINEER VOICE
    4. https://licensecounter.jp/engineer-voice/blog/articles/20190920\_zero\_trust\_sdp.htm
       1. ■VPNセキュリティ環境の脆弱性への対策として今後導入が進む
49.  ５９．DXの実現に向けた取り込み
    1. IPA　２０２０年６月９日
    2. ■DXをスピーデイに進めてていくことが求められていいる。
    3. ■投資が実際のビジネんス変革につながらない
    4. ■新しいデジタル技術を導入してもデータ活用・連携が限定的であり、その効果も限的的ある。
    5. ①既存システムに維持・保守・資金や人材を割り引かれる
    6. ②維持・保守コストの増加、技術的負債の増大
    7. ③既存システムの維持・保守できる人材が枯渇し、セキュリティのリスクも高まる。
    8. ◎DX推進指標による自己診断結果を収集分析、自己診断結果と全体データとの比較が可能となる
    9. ベンチマークを作成。
    10. ーDX水推進のための経営のあり方、仕組み
        1. DX推進の枠組み（定性指標） DX推進の取り組み状況（定量指標）
    11. ーDXを実現する上で基盤となるITシステムの構築
        1. ITシステム構築の枠組み（定性指標）ITシステム構築の取り組み状況（定量指標）
    12. ◎日本の企業・中小企業の多くがDX実践で足踏みをしている傾向がある。
    13. ードキュメント
        1. PFデジタル化指標とそのガイダンス
        2. PF変革手引書