Sec05-02-01\_情報セキュリティ白書2019

1. 改版履歴
   1. 2019年8月19日
2. 目次
   1. 序章　2018年度の情報セキュリティの概況
   2. 第1章 情報セキュリティインシデント・脆弱性の現状と対策
      1. 1.1 2018年度に観測されたインシデント状況
         1. 1.1.1 世界における情報セキュリティインシデント状況
         2. 1.1.2 国内における情報セキュリティインシデント状況
      2. 1.2 情報セキュリ
         1. 1.2.2 ビジネスメール詐欺（BEC）
         2. 1.2.3 DDoS攻撃
         3. 1.2.4 ソフトウェアの脆弱性を悪用した攻撃
         4. 1.2.5 ランサムウェア
         5. 1.2.6 パスワードリスト攻撃
         6. 1.2.7 フィッシングによる詐欺
         7. 1.2.8 偽の警告や偽サイトを用いた詐欺等
         8. 1.2.9 情報漏えいによる被害
      3. 1.3 情報システムの脆弱性の動向
         1. 1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向
         2. 1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向
   3. 第2章 情報セキュリティを支える基盤の動向
      1. 2.1 国内の情報セキュリティ政策の状況
         1. 2.1.1 政府全体の政策動向
         2. 2.1.2 経済産業省の政策
         3. 2.1.3 総務省の政策
         4. 2.1.4 警察によるサイバー犯罪対策
         5. 2.1.5 CRYPTRECの動向
      2. 2.2 国外の情報セキュリティ政策の状況
         1. 2.2.1 国際社会と連携した取り組み
         2. 2.2.2 米国の政策
         3. 2.2.3 欧州の政策
         4. 2.2.4 中国の政策
         5. 2.2.5 アジア太平洋地域でのCSIRTの動向
      3. 2.3 情報セキュリティ人材の現状と育成
         1. 2.3.1 情報セキュリティ人材の状況
         2. 2.3.2 産業サイバーセキュリティセンター
         3. 2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度
         4. 2.3.4 情報セキュリティ人材育成のための活動
      4. 2.4 組織・個人における情報セキュリティの取り組み
         1. 2.4.1 企業における対策状況
         2. 2.4.2 中小企業に向けた情報セキュリティ支援策
         3. 2.4.3 教育機関・政府及び地方公共団体等法人における対策状況
         4. 2.4.4 一般利用者における対策状況
         5. 2.4.5 政府・公共機関による普及啓発活動
         6. 2.4.6 団体・教育機関・学生・民間企業等による普及啓発活動
      5. 2.5 国際標準化活動
         1. 2.5.1 様々な標準化団体の活動
         2. 2.5.2 情報処理関係の規格の標準化（ISO/IEC JTC 1/SC 27）
         3. 2.5.3 信頼性の高いコンピューティング環境の実現に向けたセキュリティ標準（TCG）
      6. 2.6 安全な政府調達に向けて
         1. 2.6.1 ITセキュリティ評価及び認証制度
         2. 2.6.2 スマートカードの評価認証
         3. 2.6.3 暗号モジュール試験及び認証制度
      7. 2.7 その他の情報セキュリティ動向
         1. 2.7.1 情報セキュリティ市場の動向
         2. 2.7.2 データ利活用の実態と動向
         3. 2.7.3 暗号技術の動向
   4. 第3章 個別テーマ
      1. 3.1 制御システムの情報セキュリティ
         1. 3.1.1 インシデントの発生状況と動向
         2. 3.1.2 脆弱性と脅威の動向
         3. 3.1.3 海外の制御システムセキュリティの取り組み
         4. 3.1.4 国内の制御システムセキュリティの取り組み
      2. 3.2 IoTの情報セキュリティ
         1. 3.2.1 増大するIoTのセキュリティ脅威
         2. 3.2.2 脆弱なまま販売・運用されるIoT機器の散在
         3. 3.2.3 セキュリティ対策強化への取り組み
      3. 3.3 スマートフォンの情報セキュリティ
         1. 3.3.1 宅配便業者を装う不在通知SMSの手口
         2. 3.3.2 dアカウントを狙ったフィッシング
         3. 3.3.3 アプリ誘導
         4. 3.3.4 公式マーケット上に配布された不正アプリ
      4. 3.4 ITサプライチェーンのセキュリティ
         1. 3.4.1 インシデント、被害の事例
         2. 3.4.2 国内の政策動向
         3. 3.4.3 海外の政策動向
         4. 3.4.4 ITサプライチェーンにおける企業のセキュリティ対策状況
         5. 3.4.5 おわりに
      5. 3.5 AIのトラストとセキュリティ
         1. 3.5.1 本節で扱うAIのスコープ
         2. 3.5.2 AIの社会実装に関わるリスク
         3. 3.5.3 関連組織の活動
         4. 3.5.4 AIのトラストの検討状況
         5. 3.5.5 AIのセキュリティの検討状況
   5. 付録　資料・ツール
      1. 資料A 2018年のコンピュータウイルス届出状況
      2. 資料B 2018年のコンピュータ不正アクセス届出状況
      3. 資料C ソフトウェア等の脆弱性関連情報に関する届出状況
      4. ツール
   6. 第14回IPA「ひろげよう情報モラル・セキュリティコンクール」2018 受賞作品
   7. コラム
      1. サイバーセキュリティ専門家に求められる倫理観
      2. セキュリティ・バイ・デザインの勧め
      3. サイバーセキュリティ目的のリバースエンジニアリングについて ～改正著作権法～
      4. CBPRシステム ～APECの越境個人情報保護～
      5. ネットで目立ちたい？？
      6. サイバーセキュリティリスク対策に「サイバー保険」という選択肢も
      7. Miraiの作成者の末路
      8. 情報セキュリティ10大脅威 2019 ～局面ごとにセキュリティ対策の最善手を～
3. 序章　2018年度の情報セキュリティの概況
   1. 2018年度に起きた情報セキュリティに関する主なインシデントや実施された政策・制度について概況を述べる。
   2. 国外では2018年10月に大手SNS がユーザの個人情報2,900 万件が流出した恐れがあると公表し、また2019 年1 月には大手ホテルチェーンが3 億8,300 万件の顧客情報が流出した恐れがあると公表した等、サイバー攻撃による大規模な被害が発生した。
   3. 一方国内では、このような大規模な被害は確認されなかったものの、ビジネスメール詐欺や不正アクセス・内部不正による情報漏えい、ランサムウェア感染によるデータの暗号化被害、宅配便業者を装ったSMS で不正アプリインストールに誘導する攻撃やEC サイトへのパスワードリスト攻撃等、企業や個人に対する攻撃・被害は継続して確認された。
   4. 他にも、オンラインゲームのサーバが断続的なDDoS（Distributed Denial of Service）攻撃を受け、24 時間体制で対応にあたった事例や、複数の大学でフィッシングメールの被害が発生し、政府から全国の大学へ注意喚起を実施した事例等が報告された。
   5. また、委託先における運用上の過失に起因する情報漏えい被害や配布するアップデートファイルにウイルスを仕掛ける攻撃といった、サプライチェーン上のセキュリティリスクを浮き彫りにするインシデントもあった。
   6. 攻撃の基本的な手口には2017年度から目立った変化はなく、脆弱性の解消や適切なパスワード管理等、従来の対策で防げたはずの被害が多いが、人間の弱点を突く新しい手口も確認されている。
   7. 例えば性的な画像等による脅迫を模した根拠のない脅迫で、仮想通貨を要求するというメールが2018 年の夏ごろから多く確認された。
   8. 事実無根の内容であるにも関わらず、指定された仮想通貨の口座には多数の入金が確認されたという。
   9. 政策面に関しては、2018 年度は国内外でセキュリティに関する戦略や法律の実践に向けた体制強化や施策が本格的に展開された、セキュリティ対策の過渡期とも言える年であった。
   10. 国内では、「サイバーセキュリティ戦略」が3 年ぶりに見直され、以前よりもサイバー空間とフィジカル空間の一体化が進み、フィジカル空間への一層の影響が懸念さ
   11. れる中、それらを包括したサプライチェーン上のリスク管理フレームワークの実装、中小企業対策の促進等が盛り込まれた。
   12. また、プロジェクト「NOTICE」や「情報処理支援機関（スマートSME サポーター）」認定制度等、企業の努力だけでは実現が困難な対策を、法律の見直しを含めて検討し、実現した。
   13. 今後も官民が連携し、中小企業も含めたサプライチェーン全体のセキュリティ対策を進めることが求められる。
   14. 国際連携に関しては、日本は米国と、2018 年7 月に重要インフラに対するサイバーセキュリティ、防衛面におけるサイバー連携や国際的なサイバーセキュリティに関する情報共有の強化に向け、協力することを確認した。
   15. 欧州とは個人データの越境移転に関して2018 年7月に包括合意を行い、2019年1月に合意に基づいたデータ移転が可能となった。
   16. 米国では2018 年9月、トランプ大統領が国家サイバー戦略を発表し、サイバー空間の敵対的行動を監視・対抗する、という安全保障重視の姿勢をより鮮明なものとした。
   17. 特に、中国に対しては具体的に企業名を挙げ政府調達を禁止した。
   18. 欧州では、2018 年5 月にGDPR（General Data Protection Regulation：一般データ保護規則）が発効した。
   19. 既に2019 年1 月には、グローバルサービスプロバイダのGDPR 違反が認定され、5,000万ユーロ（約62 億円）の制裁金が科せられた例が報告されている。また、重要インフラ向けのセキュリティ対策規範であるNIS 指令に基づくEU 加盟国の各国内法
   20. 整備については、ほぼ完了している状況である。中国に関しては、前述のとおり米国と対立が続いている一方、米国で政府調達禁止となった中国企業がEU 加盟国の一部で5G ネットワークの調達ベンダとして認められたように、欧州と連携する等で独自の地位を模索している。
   21. 以上のように、セキュリティを国家戦略の一つとして掲げ、各国が独自に、あるいは連携した取り組みを進めている。
   22. 日本は各国の戦略を理解し、必要な連携施策を講じつつ、国家を超えたサイバー脅威に対応する必要がある。
4. 第1章 情報セキュリティインシデント・脆弱性の現状と対策
   1. 1.1 2018年度に観測されたインシデント状況
      1. 1.1.1 世界における情報セキュリティインシデント状況
      2. 1.1.2 国内における情報セキュリティインシデント状況
   2. 1.2 情報セキュリ
      1. 1.2.2 ビジネスメール詐欺（BEC）
      2. 1.2.3 DDoS攻撃
      3. 1.2.4 ソフトウェアの脆弱性を悪用した攻撃
      4. 1.2.5 ランサムウェア
      5. 1.2.6 パスワードリスト攻撃
      6. 1.2.7 フィッシングによる詐欺
      7. 1.2.8 偽の警告や偽サイトを用いた詐欺等
      8. 1.2.9 情報漏えいによる被害
   3. 1.3 情報システムの脆弱性の動向
      1. 1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向
      2. 1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向
5. 第2章 情報セキュリティを支える基盤の動向
   1. 2.1 国内の情報セキュリティ政策の状況
      1. 2.1.1 政府全体の政策動向
      2. 2.1.2 経済産業省の政策
      3. 2.1.3 総務省の政策
      4. 2.1.4 警察によるサイバー犯罪対策
      5. 2.1.5 CRYPTRECの動向
   2. 2.2 国外の情報セキュリティ政策の状況
      1. 2.2.1 国際社会と連携した取り組み
      2. 2.2.2 米国の政策
      3. 2.2.3 欧州の政策
      4. 2.2.4 中国の政策
      5. 2.2.5 アジア太平洋地域でのCSIRTの動向
   3. 2.3 情報セキュリティ人材の現状と育成
      1. 2.3.1 情報セキュリティ人材の状況
      2. 2.3.2 産業サイバーセキュリティセンター
      3. 2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度
      4. 2.3.4 情報セキュリティ人材育成のための活動
   4. 2.4 組織・個人における情報セキュリティの取り組み
      1. 2.4.1 企業における対策状況
      2. 2.4.2 中小企業に向けた情報セキュリティ支援策
      3. 2.4.3 教育機関・政府及び地方公共団体等法人における対策状況
      4. 2.4.4 一般利用者における対策状況
      5. 2.4.5 政府・公共機関による普及啓発活動
      6. 2.4.6 団体・教育機関・学生・民間企業等による普及啓発活動
   5. 2.5 国際標準化活動
      1. 2.5.1 様々な標準化団体の活動
      2. 2.5.2 情報処理関係の規格の標準化（ISO/IEC JTC 1/SC 27）
      3. 2.5.3 信頼性の高いコンピューティング環境の実現に向けたセキュリティ標準（TCG）
   6. 2.6 安全な政府調達に向けて
      1. 2.6.1 ITセキュリティ評価及び認証制度
      2. 2.6.2 スマートカードの評価認証
      3. 2.6.3 暗号モジュール試験及び認証制度
   7. 2.7 その他の情報セキュリティ動向
      1. 2.7.1 情報セキュリティ市場の動向
      2. 2.7.2 データ利活用の実態と動向
      3. 2.7.3 暗号技術の動向
6. 第3章 個別テーマ
   1. 3.1 制御システムの情報セキュリティ
      1. 3.1.1 インシデントの発生状況と動向
      2. 3.1.2 脆弱性と脅威の動向
      3. 3.1.3 海外の制御システムセキュリティの取り組み
      4. 3.1.4 国内の制御システムセキュリティの取り組み
   2. 3.2 IoTの情報セキュリティ
      1. 3.2.1 増大するIoTのセキュリティ脅威
      2. 3.2.2 脆弱なまま販売・運用されるIoT機器の散在
      3. 3.2.3 セキュリティ対策強化への取り組み
   3. 3.3 スマートフォンの情報セキュリティ
      1. 3.3.1 宅配便業者を装う不在通知SMSの手口
      2. 3.3.2 dアカウントを狙ったフィッシング
      3. 3.3.3 アプリ誘導
      4. 3.3.4 公式マーケット上に配布された不正アプリ
   4. 3.4 ITサプライチェーンのセキュリティ
      1. 3.4.1 インシデント、被害の事例
      2. 3.4.2 国内の政策動向
      3. 3.4.3 海外の政策動向
      4. 3.4.4 ITサプライチェーンにおける企業のセキュリティ対策状況
      5. 3.4.5 おわりに
   5. 3.5 AIのトラストとセキュリティ
      1. 3.5.1 本節で扱うAIのスコープ
      2. 3.5.2 AIの社会実装に関わるリスク
      3. 3.5.3 関連組織の活動
      4. 3.5.4 AIのトラストの検討状況
      5. 3.5.5 AIのセキュリティの検討状況
7. 付録　資料・ツール
   1. 資料A 2018年のコンピュータウイルス届出状況
   2. 資料B 2018年のコンピュータ不正アクセス届出状況
   3. 資料C ソフトウェア等の脆弱性関連情報に関する届出状況
   4. ツール
8. 第14回IPA「ひろげよう情報モラル・セキュリティコンクール」2018 受賞作品
9. コラム
   1. サイバーセキュリティ専門家に求められる倫理観
   2. セキュリティ・バイ・デザインの勧め
   3. サイバーセキュリティ目的のリバースエンジニアリングについて ～改正著作権法～
   4. CBPRシステム ～APECの越境個人情報保護～
   5. ネットで目立ちたい？？
   6. サイバーセキュリティリスク対策に「サイバー保険」という選択肢も
   7. Miraiの作成者の末路
   8. 情報セキュリティ10大脅威 2019 ～局面ごとにセキュリティ対策の最善手を～