Sec22-01_「情報セキュリティ白書2021」の目次

- 1. 概要
  - 「情報セキュリティ白書2021」の章節項の見出しを体系的に切り出したもの
  - 白書の内容検索のため使用することを想定。
  - 原本
    - 情報セキュリティ白書2021【2021年7月20日IPA】
      - https://www.ipa.go.jp/security/publications/hakusyo/2021.html
  - 改版履歴
    - 2021年12月21日 改版
    - 2021年10月28日 初版
- 2. 目次
  - 94
- 3. 目次【詳細項目】
  - ●序章 2020年度の情報セキュリティの概況
  - ●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 2020年度に観測されたインシデント状況
      - 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
        - (1) 新型コロナウイルス感染症に関連する脅威
        - (2) フィッシングとビジネスメール詐欺の傾向
        - (3) 情報漏えいインシデントの状況
        - (4) ランサムウェアによる攻撃の傾向
        - (5) ウイルスのマルチプラットフォーム化
        - (6) 脆弱性を突く攻撃の増加
      - 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
        - (1) 情報セキュリティインシデントの発生状況
        - (2) Web サイト改ざんによる被害
        - (3) フィッシングによる被害
        - (4) 注目された新たな脅威
          - (a) 新たなランサムウェア
          - (b) VPN 製品の脆弱性
          - (c) クラウドサービスからの情報漏えい
          - (d) 「ドコモ口座」を利用した不正送金
    - 1.2 情報セキュリティインシデント種類別の手口と対策
      - (1) 国内の標的型攻撃事例
        - ・事案①：海外拠点を起点とする攻撃
        - • 事案②：BYOD※ 38 端末（VDI 接続）を起点とする攻撃
      - (2) 標的型攻撃の傾向
      - (3) 標的型攻撃の手口（初期侵入段階）
        - (a) 標的型攻撃メール
        - (b) サプライチェーン・海外拠点等への攻撃
        - (c) VPN 製品や公開サーバ等の脆弱性を悪用した攻撃
        - (d) SNS を悪用した攻撃
      - (4) 標的型攻撃の手口（攻撃基盤構築段階）
        - (a) オープンソースソフトウェアや標準的なソフトウェア等を利用した攻撃
        - (b) 認証情報の取得

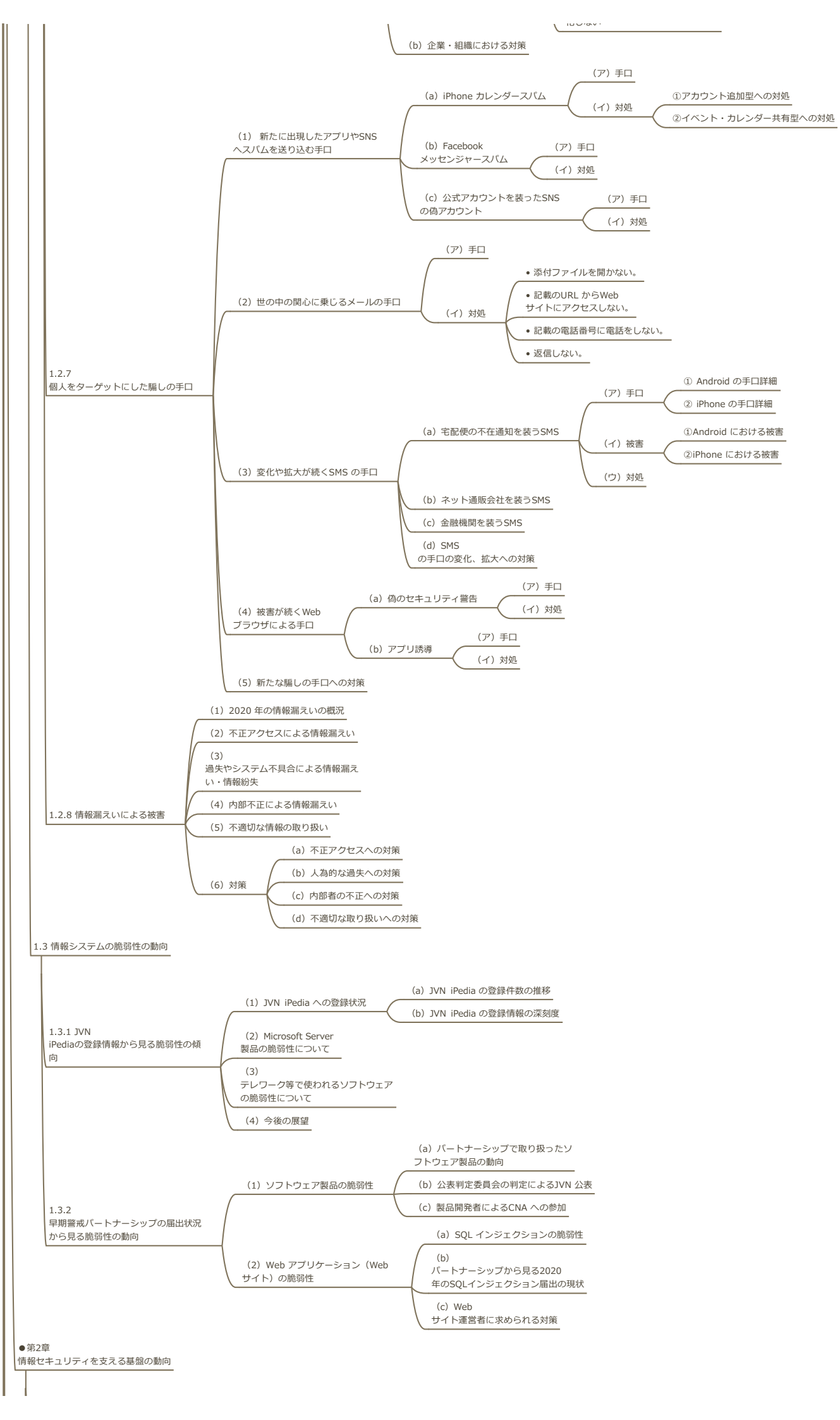
- 1.2.1 標的型攻撃
  - （c）AD サーバを標的とした攻撃
  - （5）標的型攻撃への対策
    - （a）利用者の意識向上
      - ・不審メールに対する注意力の向上
      - • SNS を悪用した手口の周知
      - • マクロ機能の危険性の周知
      - • 標的型訓練メール等で実践的な訓練を実施
    - （b）組織としての対応体制の強化
      - • CSIRT 設置と運用
      - • インシデント対応力の強化
      - • 流行している攻撃の手口や対策の組織内共有
      - • 海外拠点・サプライチェーンを意識したセキュリティの強化
    - （c）システムによる対策
      - • 不審メールを警告する仕組みの導入
      - • 適切な修正プログラムの適用
      - • 通常業務で使わないファイルの実行・ソフトウェアの利用防止
      - • セキュリティ対策の再チェック
      - • ネットワーク構成の変化に合わせた対策
- 1.2.2 新たなランサムウェア攻撃
  - 概要
    - • 人手によるランサムウェア攻撃（human-operated ransomware attacks）
    - • 二重の脅迫（double extortion）
  - （1）新たなランサムウェア攻撃の被害事例
    - （a）国内のゲーム会社の被害事例
    - （b）国内の建設会社の被害事例
  - （2）新たなランサムウェア攻撃の傾向
  - （3）攻撃手口
    - （a）ネットワークへの侵入
      - • リモートデスクトップサービスやVPN 製品を経由した侵入
      - • VPN 製品の脆弱性を悪用した侵入
      - • ウイルスメールによる侵入
    - （b）ネットワーク内の侵害範囲拡大
    - （c）データ窃取
    - （d）データの暗号化・システム停止
    - （e）窃取したデータの公開
  - （4）新たなランサムウェア攻撃への対策
    - （a）企業・組織のネットワークへの侵入対策
      - • 攻撃対象領域（attack surface）の最小化
      - • アクセス制御と認証
      - • 脆弱性対策
      - • 拠点間ネットワークのセキュリティ強化
      - • 攻撃メール対策
    - （b）ネットワーク内の侵害範囲拡大への対策
    - （c）データの暗号化やシステム停止への対策
    - （d）データの窃取とリークへの対策
    - （e）インシデント対応
- 1.2.3 ビジネスメール詐欺（BEC）
  - （1）ビジネスメール詐欺の被害状況
  - （2）2020 年度に報道された事例の概要
  - （3）IPA が情報提供を受けた事例の概要
  - （4）IPA が情報提供を受けた事例
    - （a）事例の概要
      - • 請求書の修正を装い偽の口座を連絡する手口
      - • 詐称用ドメインの取得と悪用
    - （b）請求書の修正を装い偽の口座を連絡する手口
    - （c）詐称用ドメインの取得と悪用
  - （5）ビジネスメール詐欺の騙しの手口
  - （6）ビジネスメール詐欺への対策
    - （a）ビジネスメール詐欺の周知徹底と情報共有
    - （b）電子署名等によるなりすまし防止
    - （c）送金処理のチェック体制強化

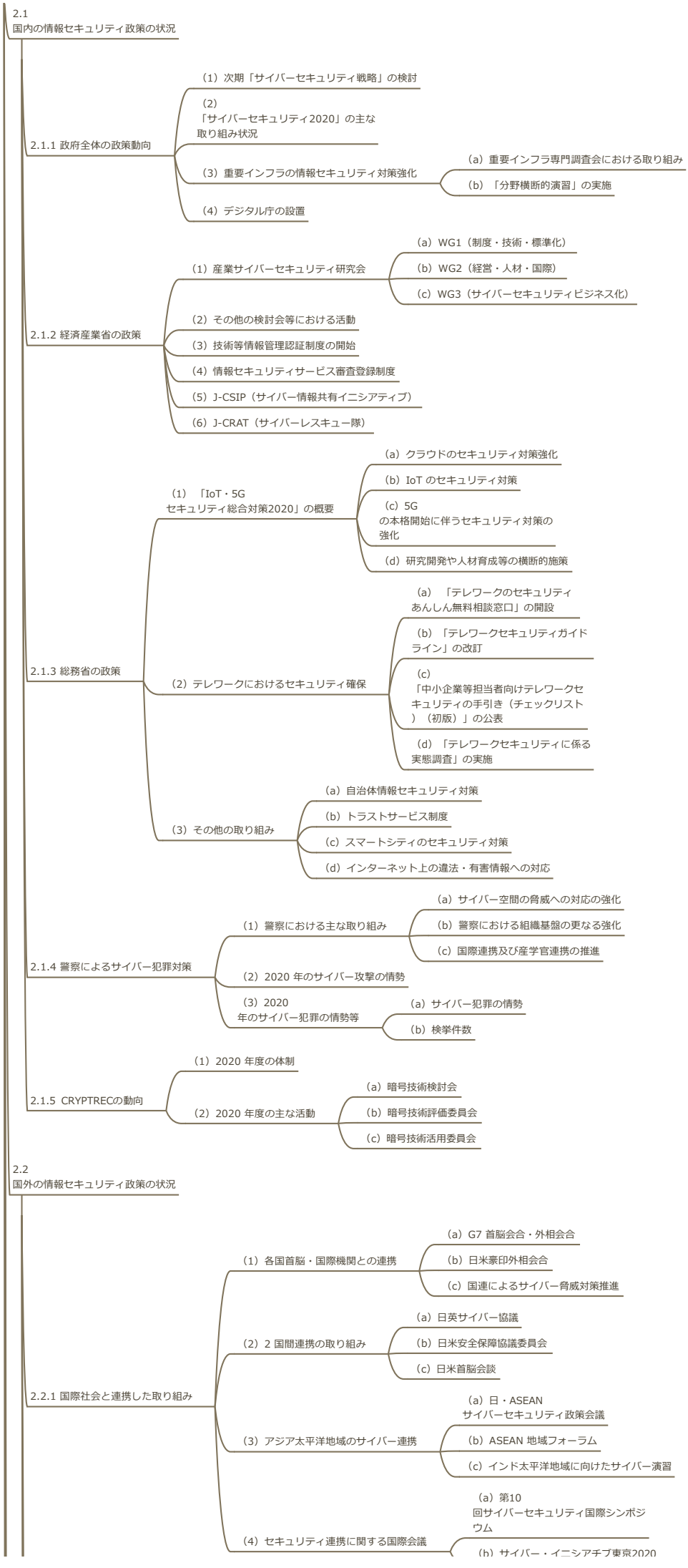
- （d）攻撃に使われるメールアドレスへの対策
- （e）フィッシング・ウイルス・不正アクセス対策

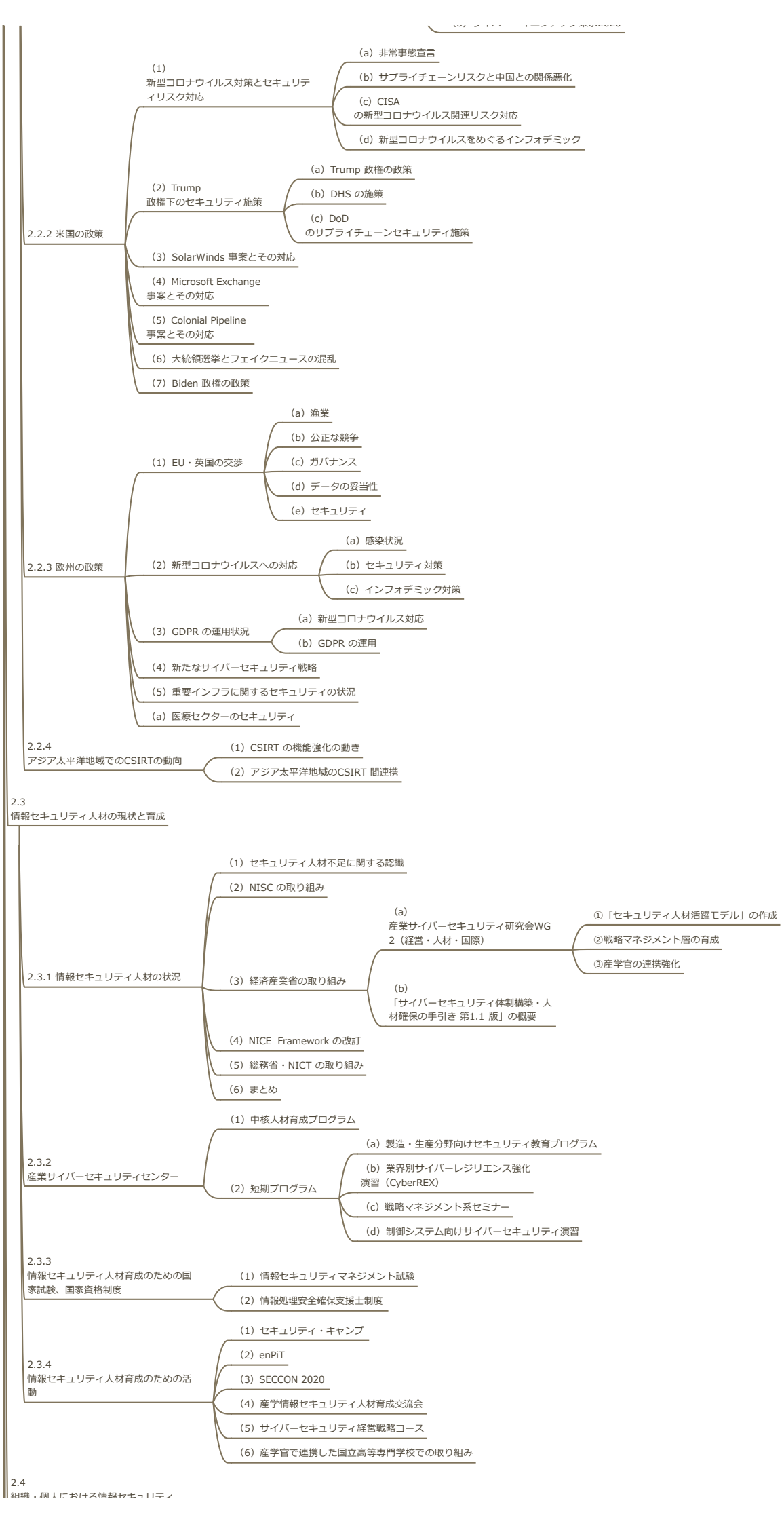
1.2.4 DDoS攻撃
- （1）DDoS 攻撃の動向
  - （a）リフレクション攻撃
  - （b）DDoS 攻撃の規模拡大の事例
  - （c）仮想通貨を要求するDDoS 攻撃の事例
- （2）DDoS 攻撃を行うボットネットの拡大
- （3）DDoS 攻撃への対策
  - （a）DDoS 攻撃の被害に遭った場合の対策
  - （b）攻撃に加担しないための対策

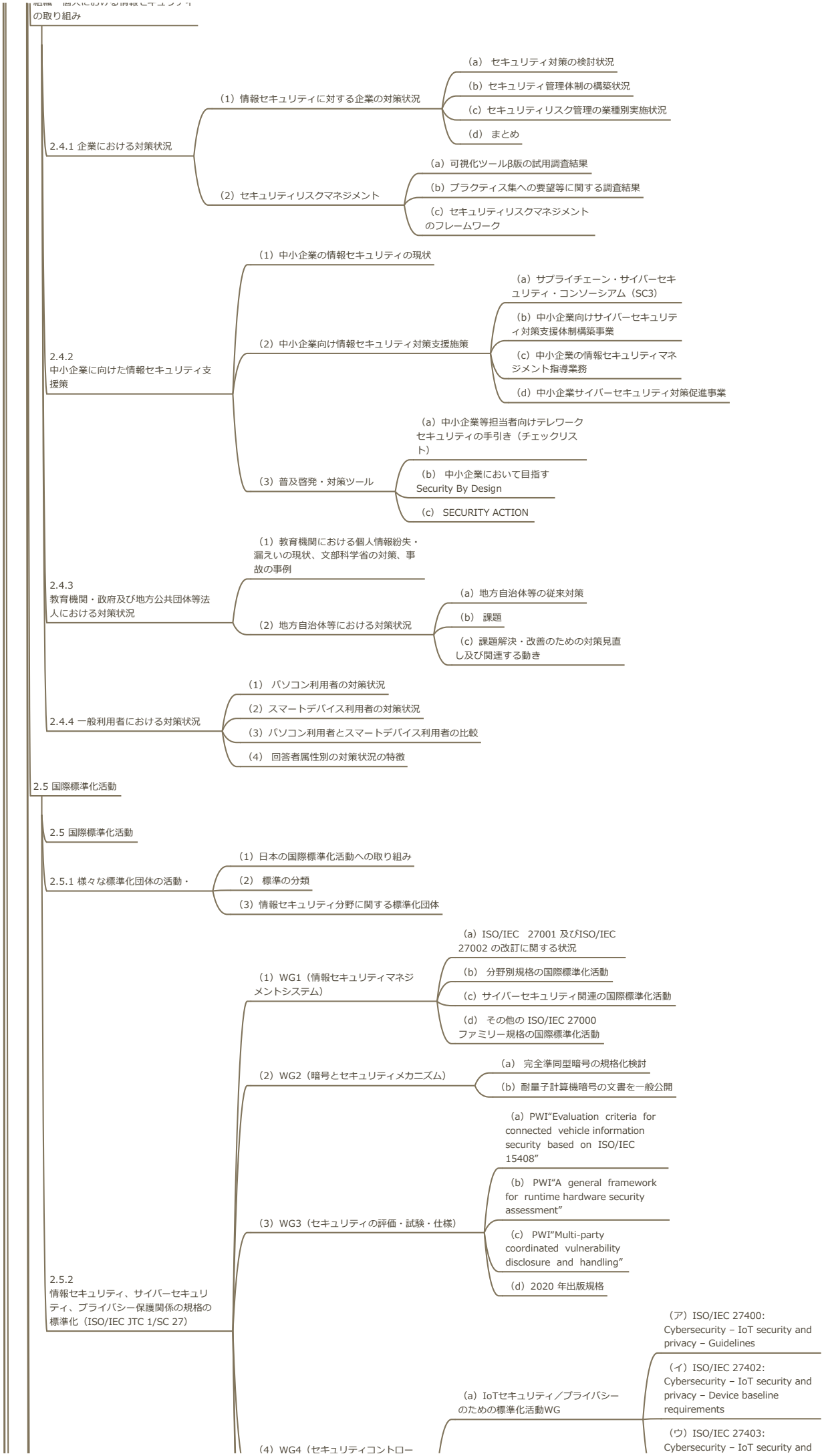
1.2.5 ソフトウェアの脆弱性を悪用した攻撃
- （1）VPN 製品の脆弱性を対象とした攻撃
  - （a）攻撃事例
    - CVE-2019-11510 の脆弱性
    - CVE-2019-11539 の脆弱性
  - （b）脆弱性を狙った攻撃への対策
- （2）Microsoft 製品の脆弱性を対象とした攻撃
  - （a）攻撃事例
    - SMBGhost の脆弱性
    - SMBleed の脆弱性
  - （b）脆弱性を狙った攻撃への対策
- （3）IoT 製品を対象とした攻撃
  - （a）多数のIoT 製品に影響する脆弱性
  - （b）IoT 製品を対象とした攻撃への対策
    - 製品開発者が行うべき対策
    - 製品利用者が行うべき対策

1.2.6 ばらまき型メールによる攻撃
- （1）ばらまき型メールによって感染するウイルス
  - （a）Emotet
    - ネットワークを経由した別の端末への感染
    - メールアドレス情報の窃取
    - Outlook のアドレス帳の窃取
    - Outlook のメールデータの窃取
    - Web ブラウザに保存されたアカウント資格情報の窃取
    - Emotet のばらまき型メールの送信
  - （b）IcedID
    - インターネットバンキングの情報窃取
    - ファイルのダウンロード及び実行
    - メールソフトのアカウント情報窃取
    - Web ブラウザに保存されたアカウント情報の窃取
    - 感染した端末の情報の収集
  - （c）Zloader
    - インターネットバンキングの情報窃取
    - スクリーンショットの窃取
    - Web ブラウザに保存されたCookie やパスワードの窃取
    - Web ブラウザ上のキー入力の窃取
  - （d）遠隔操作ウイルス（RAT）
- （2）ばらまき型メールの偽装の手口
  - （a）正規のメールへの返信、転送、及び再送を装う手口
  - （b）メール受信者の興味・関心を惹く題材を悪用する手口
  - （c）実在の組織をかたった手口
- （3）ウイルスに感染させる手口
  - （a）マクロ付きのOffice 文書ファイルを使用する手口
  - （b）パスワード付きのZIP ファイルを使用する手口
  - （c）メール本文中のURLリンクを使用する手口
- （4）ばらまき型メールへの対策
  - （a）一般利用者における対策
    - セキュリティソフトを導入する
    - 不用意にメールや添付ファイル内の指示に従わない
    - OS やソフトウェアのバージョンを常に最新に保つ
    - Word、Excel、PowerPoint ファイルを開いたときにマクロを有効化しない


（b）企業・組織における対策
（ア）手口
（a）iPhone カレンダースパム
（イ）対処
①アカウント追加型への対処
②イベント・カレンダー共有型への対処
（1） 新たに出現したアプリやSNS
へスパムを送り込む手口
（b）Facebook
メッセンジャースパム
（ア）手口
（イ）対処
（c）公式アカウントを装ったSNS
の偽アカウント
（ア）手口
（イ）対処
（ア）手口
（2）世の中の関心に乗じるメールの手口
（イ）対処
• 添付ファイルを開かない。
• 記載のURL からWeb
サイトにアクセスしない。
• 記載の電話番号に電話をしない。
• 返信しない。
1.2.7
個人をターゲットにした騙しの手口
（ア）手口
① Android の手口詳細
② iPhone の手口詳細
（a）宅配便の不在通知を装うSMS
（イ）被害
①Android における被害
②iPhone における被害
（ウ）対処
（3）変化や拡大が続くSMS の手口
（b）ネット通販会社を装うSMS
（c）金融機関を装うSMS
（d）SMS
の手口の変化、拡大への対策
（ア）手口
（a）偽のセキュリティ警告
（イ）対処
（4）被害が続くWeb
ブラウザによる手口
（ア）手口
（b）アプリ誘導
（イ）対処
（5）新たな騙しの手口への対策
（1）2020 年の情報漏えいの概況
（2）不正アクセスによる情報漏えい
（3）
過失やシステム不具合による情報漏え
い・情報紛失
（4）内部不正による情報漏えい
1.2.8 情報漏えいによる被害
（5）不適切な情報の取り扱い
（a）不正アクセスへの対策
（b）人為的な過失への対策
（6）対策
（c）内部者の不正への対策
（d）不適切な取り扱いへの対策
1.3 情報システムの脆弱性の動向
（a）JVN iPedia の登録件数の推移
（1）JVN iPedia への登録状況
（b）JVN iPedia の登録情報の深刻度
1.3.1 JVN
iPediaの登録情報から見る脆弱性の傾
向
（2）Microsoft Server
製品の脆弱性について
（3）
テレワーク等で使われるソフトウェア
の脆弱性について
（4）今後の展望
（a）パートナーシップで取り扱ったソ
フトウェア製品の動向
（1）ソフトウェア製品の脆弱性
（b）公表判定委員会の判定によるJVN 公表
（c）製品開発者によるCNA への参加
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
（a）SQL インジェクションの脆弱性
（2）Web アプリケーション（Web
サイト）の脆弱性
（b）
パートナーシップから見る2020
年のSQLインジェクション届出の現状
（c）Web
サイト運営者に求められる対策
●第2章
情報セキュリティを支える基盤の動向


2.1
国内の情報セキュリティ政策の状況
2.1.1 政府全体の政策動向
（1）次期「サイバーセキュリティ戦略」の検討
（2）
「サイバーセキュリティ2020」の主な
取り組み状況
（3）重要インフラの情報セキュリティ対策強化
（a）重要インフラ専門調査会における取り組み
（b）「分野横断的演習」の実施
（4）デジタル庁の設置
2.1.2 経済産業省の政策
（1）産業サイバーセキュリティ研究会
（a）WG1（制度・技術・標準化）
（b）WG2（経営・人材・国際）
（c）WG3（サイバーセキュリティビジネス化）
（2）その他の検討会等における活動
（3）技術等情報管理認証制度の開始
（4）情報セキュリティサービス審査登録制度
（5）J-CSIP（サイバー情報共有イニシアティブ）
（6）J-CRAT（サイバーレスキュー隊）
2.1.3 総務省の政策
（1）「IoT・5G
セキュリティ総合対策2020」の概要
（a）クラウドのセキュリティ対策強化
（b）IoT のセキュリティ対策
（c）5G
の本格開始に伴うセキュリティ対策の
強化
（d）研究開発や人材育成等の横断的施策
（2）テレワークにおけるセキュリティ確保
（a）「テレワークのセキュリティ
あんしん無料相談窓口」の開設
（b）「テレワークセキュリティガイド
ライン」の改訂
（c）
「中小企業等担当者向けテレワークセ
キュリティの手引き（チェックリスト
）（初版）」の公表
（d）「テレワークセキュリティに係る
実態調査」の実施
（3）その他の取り組み
（a）自治体情報セキュリティ対策
（b）トラストサービス制度
（c）スマートシティのセキュリティ対策
（d）インターネット上の違法・有害情報への対応
2.1.4 警察によるサイバー犯罪対策
（1）警察における主な取り組み
（a）サイバー空間の脅威への対応の強化
（b）警察における組織基盤の更なる強化
（c）国際連携及び産学官連携の推進
（2）2020 年のサイバー攻撃の情勢
（3）2020
年のサイバー犯罪の情勢等
（a）サイバー犯罪の情勢
（b）検挙件数
2.1.5 CRYPTRECの動向
（1）2020 年度の体制
（2）2020 年度の主な活動
（a）暗号技術検討会
（b）暗号技術評価委員会
（c）暗号技術活用委員会
2.2
国外の情報セキュリティ政策の状況
2.2.1 国際社会と連携した取り組み
（1）各国首脳・国際機関との連携
（a）G7 首脳会合・外相会合
（b）日米豪印外相会合
（c）国連によるサイバー脅威対策推進
（2）2 国間連携の取り組み
（a）日英サイバー協議
（b）日米安全保障協議委員会
（c）日米首脳会談
（3）アジア太平洋地域のサイバー連携
（a）日・ASEAN
サイバーセキュリティ政策会議
（b）ASEAN 地域フォーラム
（c）インド太平洋地域に向けたサイバー演習
（4）セキュリティ連携に関する国際会議
（a）第10
回サイバーセキュリティ国際シンポジ
ウム
（b）サイバー・イニシアチブ東京2020

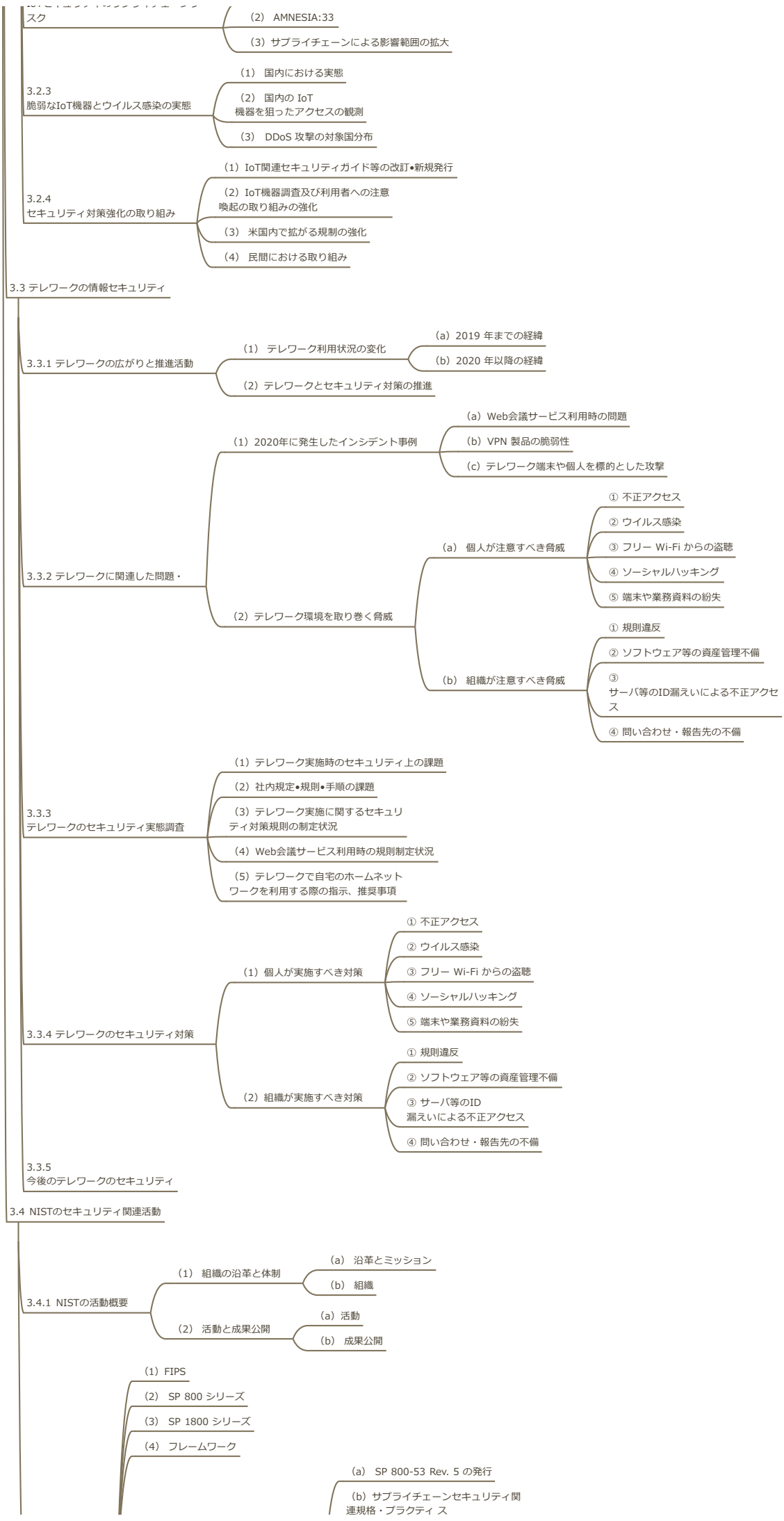

(1)
新型コロナウイルス対策とセキュリティリスク対応
(a) 非常事態宣言
(b) サプライチェーンリスクと中国との関係悪化
(c) CISA
の新型コロナウイルス関連リスク対応
(d) 新型コロナウイルスをめぐるインフォデミック
2.2.2 米国の政策
(2) Trump
政権下のセキュリティ施策
(a) Trump 政権の政策
(b) DHS の施策
(c) DoD
のサプライチェーンセキュリティ施策
(3) SolarWinds 事案とその対応
(4) Microsoft Exchange
事案とその対応
(5) Colonial Pipeline
事案とその対応
(6) 大統領選挙とフェイクニュースの混乱
(7) Biden 政権の政策
2.2.3 欧州の政策
(1) EU・英国の交渉
(a) 漁業
(b) 公正な競争
(c) ガバナンス
(d) データの妥当性
(e) セキュリティ
(2) 新型コロナウイルスへの対応
(a) 感染状況
(b) セキュリティ対策
(c) インフォデミック対策
(3) GDPR の運用状況
(a) 新型コロナウイルス対応
(b) GDPR の運用
(4) 新たなサイバーセキュリティ戦略
(5) 重要インフラに関するセキュリティの状況
(a) 医療セクターのセキュリティ
2.2.4
アジア太平洋地域でのCSIRTの動向
(1) CSIRT の機能強化の動き
(2) アジア太平洋地域のCSIRT 間連携
2.3
情報セキュリティ人材の現状と育成
2.3.1 情報セキュリティ人材の状況
(1) セキュリティ人材不足に関する認識
(2) NISC の取り組み
(3) 経済産業省の取り組み
(a)
産業サイバーセキュリティ研究会WG
2（経営・人材・国際）
①「セキュリティ人材活躍モデル」の作成
②戦略マネジメント層の育成
③産学官の連携強化
(b)
「サイバーセキュリティ体制構築・人材確保の手引き 第1.1 版」の概要
(4) NICE Framework の改訂
(5) 総務省・NICT の取り組み
(6) まとめ
2.3.2
産業サイバーセキュリティセンター
(1) 中核人材育成プログラム
(2) 短期プログラム
(a) 製造・生産分野向けセキュリティ教育プログラム
(b) 業界別サイバーレジリエンス強化
演習（CyberREX）
(c) 戦略マネジメント系セミナー
(d) 制御システム向けサイバーセキュリティ演習
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
(1) 情報セキュリティマネジメント試験
(2) 情報処理安全確保支援士制度
2.3.4
情報セキュリティ人材育成のための活動
(1) セキュリティ・キャンプ
(2) enPiT
(3) SECCON 2020
(4) 産学情報セキュリティ人材育成交流会
(5) サイバーセキュリティ経営戦略コース
(6) 産学官で連携した国立高等専門学校での取り組み
2.4
組織・個人における情報セキュリティ


組織一個人における情報セキュリティの取り組み
2.4.1 企業における対策状況
（1）情報セキュリティに対する企業の対策状況
（a） セキュリティ対策の検討状況
（b）セキュリティ管理体制の構築状況
（c）セキュリティリスク管理の業種別実施状況
（d） まとめ
（2）セキュリティリスクマネジメント
（a）可視化ツールβ版の試用調査結果
（b）プラクティス集への要望等に関する調査結果
（c）セキュリティリスクマネジメントのフレームワーク
2.4.2 中小企業に向けた情報セキュリティ支援策
（1）中小企業の情報セキュリティの現状
（2）中小企業向け情報セキュリティ対策支援施策
（a）サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）
（b）中小企業向けサイバーセキュリティ対策支援体制構築事業
（c）中小企業の情報セキュリティマネジメント指導業務
（d）中小企業サイバーセキュリティ対策促進事業
（3）普及啓発・対策ツール
（a）中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）
（b） 中小企業において目指すSecurity By Design
（c） SECURITY ACTION
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
（1）教育機関における個人情報紛失・漏えいの現状、文部科学省の対策、事故の事例
（2）地方自治体等における対策状況
（a）地方自治体等の従来対策
（b） 課題
（c）課題解決・改善のための対策見直し及び関連する動き
2.4.4 一般利用者における対策状況
（1） パソコン利用者の対策状況
（2）スマートデバイス利用者の対策状況
（3）パソコン利用者とスマートデバイス利用者の比較
（4） 回答者属性別の対策状況の特徴
2.5 国際標準化活動
2.5 国際標準化活動
2.5.1 様々な標準化団体の活動・
（1）日本の国際標準化活動への取り組み
（2） 標準の分類
（3）情報セキュリティ分野に関する標準化団体
2.5.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）
（1）WG1（情報セキュリティマネジメントシステム）
（a）ISO/IEC 27001 及びISO/IEC 27002 の改訂に関する状況
（b） 分野別規格の国際標準化活動
（c）サイバーセキュリティ関連の国際標準化活動
（d） その他の ISO/IEC 27000 ファミリー規格の国際標準化活動
（2）WG2（暗号とセキュリティメカニズム）
（a） 完全準同型暗号の規格化検討
（b）耐量子計算機暗号の文書を一般公開
（3）WG3（セキュリティの評価・試験・仕様）
（a）PWI“Evaluation criteria for connected vehicle information security based on ISO/IEC 15408”
（b） PWI“A general framework for runtime hardware security assessment”
（c） PWI“Multi-party coordinated vulnerability disclosure and handling”
（d）2020 年出版規格
（4）WG4（セキュリティコントロー
（a）IoTセキュリティ／プライバシーのための標準化活動WG
（ア）ISO/IEC 27400: Cybersecurity – IoT security and privacy – Guidelines
（イ）ISO/IEC 27402: Cybersecurity – IoT security and privacy – Device baseline requirements
（ウ）ISO/IEC 27403: Cybersecurity – IoT security and

- 3.1.1 インシデントの発生状況と動向
  - （3）制御システムを標的としたランサムウェアによる攻撃事例
  - （4）ネットワーク管理用のソフトウェアの脆弱性に端を発する大規模な感染事例
  - （5）USBメモリやパソコンを接続することによるウイルス感染の増加
- 3.1.2 脆弱性及び脅威の動向
  - （1）脆弱性の動向
  - （2）脅威の動向
- 3.1.3 海外の制御システムのセキュリティ強化の取り組み
  - （1）米国政府の取り組み
  - （2）海事業界のセキュリティ
- 3.1.4 国内の制御システムのセキュリティ強化の取り組み
  - （1） 日本政府の取り組み
  - （2） IPA の取り組み
    - （a）制御システムのセキュリティリスクアセスメント普 及活動
    - （b）制御システムのサイバーセキュリティ人材の育成

3.2 IoTの情報セキュリティ

- 3.2.1 継続するIoTのセキュリティ脅威・
  - （1） TVT 社製 NVMS-9000 の脆弱性を狙う Mirai の亜種
  - （2） PixelStor5000 の脆弱性を狙うMirai の亜種「SORA」「UNSTABLE」
  - （3） Zyxel 社製 NAS の脆弱性を狙うMirai の亜種「Mukashi」
  - （4） LILIN 社製 DVR のゼロデイ脆弱性を狙う攻撃
  - （5） Xiongmai 社製 DVR/NVR のゼロデイ脆弱性を狙う攻撃
  - （6） DrayTek 社製ルータのゼロデイ脆弱性を狙う攻撃
  - （7） Gafgyt の亜種「Hoaxcalls/XTC」
  - （8） Netlink 社製 GPON ルータのゼロデイ脆弱性を狙う攻撃
  - （9） Moobot の亜種「LeetHozer」
  - （10）D-Link 社製ルータDIR-865L の脆弱性
  - （11） DrayTek 社製ルータを狙う新種「Bigviktor」
  - （12） Comtrend 社製ルータVR-3033 の脆弱性を狙うMirai の亜種
  - （13） Tenda 社製 AC1900 ルータAC15 の脆弱性
  - （14） F5 社製ロードバランサ BIG-IPの脆弱性を狙う「SORA」の亜種
  - （15） ZeroShell の脆弱性を狙う攻撃
  - （16） ADB ポートを狙うMirai の亜種
  - （17） AvertX 社製ネットワークカメラの脆弱性
  - （18） IoT を狙い始めた「Ngioweb」の亜種
  - （19） AVTECH 社製 IP カメラ／NVR ／ DVRを狙う「Specter」
  - （20） QNAP 社製 NAS の非公開の脆弱性を狙う攻撃
  - （21） Tenda 社製ルータのゼロデイ脆弱性を狙う「Ttint」
  - （22） P2P プロトコルを用いる自爆機能付き「HEH」
  - （23） 新しい脆弱性を狙うMirai の亜種
  - （24） TCP ポート 5501 を狙うMirai の亜種
  - （25） UNIX CCTV 社製 DVR/NVR の脆弱性を狙う「Moobot」の亜種
  - （26）既知の脆弱性を狙う攻撃の再活性化
- 3.2.2 IoTセキュリティのサプライチェーンリ
  - （1） Ripple20


スク
（2） AMNESIA:33
（3）サプライチェーンによる影響範囲の拡大
3.2.3
脆弱なIoT機器とウイルス感染の実態
（1） 国内における実態
（2） 国内の IoT
機器を狙ったアクセスの観測
（3） DDoS 攻撃の対象国分布
3.2.4
セキュリティ対策強化の取り組み
（1）IoT関連セキュリティガイド等の改訂•新規発行
（2）IoT機器調査及び利用者への注意
喚起の取り組みの強化
（3） 米国内で拡がる規制の強化
（4） 民間における取り組み
3.3 テレワークの情報セキュリティ
3.3.1 テレワークの広がりと推進活動
（1） テレワーク利用状況の変化
（a）2019 年までの経緯
（b）2020 年以降の経緯
（2）テレワークとセキュリティ対策の推進
3.3.2 テレワークに関連した問題・
（1）2020年に発生したインシデント事例
（a）Web会議サービス利用時の問題
（b）VPN 製品の脆弱性
（c）テレワーク端末や個人を標的とした攻撃
（2）テレワーク環境を取り巻く脅威
（a） 個人が注意すべき脅威
① 不正アクセス
② ウイルス感染
③ フリー Wi-Fi からの盗聴
④ ソーシャルハッキング
⑤ 端末や業務資料の紛失
（b） 組織が注意すべき脅威
① 規則違反
② ソフトウェア等の資産管理不備
③
サーバ等のID漏えいによる不正アクセス
④ 問い合わせ・報告先の不備
3.3.3
テレワークのセキュリティ実態調査
（1）テレワーク実施時のセキュリティ上の課題
（2）社内規定•規則•手順の課題
（3）テレワーク実施に関するセキュリティ対策規則の制定状況
（4）Web会議サービス利用時の規則制定状況
（5）テレワークで自宅のホームネットワークを利用する際の指示、推奨事項
3.3.4 テレワークのセキュリティ対策
（1）個人が実施すべき対策
① 不正アクセス
② ウイルス感染
③ フリー Wi-Fi からの盗聴
④ ソーシャルハッキング
⑤ 端末や業務資料の紛失
（2）組織が実施すべき対策
① 規則違反
② ソフトウェア等の資産管理不備
③ サーバ等のID
漏えいによる不正アクセス
④ 問い合わせ・報告先の不備
3.3.5
今後のテレワークのセキュリティ
3.4 NISTのセキュリティ関連活動
3.4.1 NISTの活動概要
（1） 組織の沿革と体制
（a） 沿革とミッション
（b） 組織
（2） 活動と成果公開
（a）活動
（b） 成果公開
（1）FIPS
（2） SP 800 シリーズ
（3） SP 1800 シリーズ
（4） フレームワーク
（a） SP 800-53 Rev. 5 の発行
（b）サプライチェーンセキュリティ関連規格・プラクティ ス