TRE
Time Rise Engineering Ltd.

【参考資料】

ITセキュリティ強化に関する考察

～ 今更聞けないランサムウェア対策と中国情報規制三法・虎の巻 ～

2021.03.16

TRE China.

目次

【昨今の事例と法規制について】

【ITセキュリティ対策について】

昨今の事例と法規制について

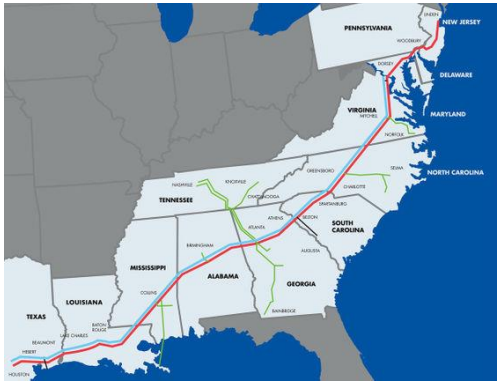
1. サイバー攻撃事例

TRE
Total Solution Provider

Colonial Pipeline

アメリカで最大の石油輸送パイプラインを運営するColonial Pipelineは2021年5月9日にハッカーからランサムウェア攻撃を受け、身代金を要求された。5月19日付けでColonial PipelineのCEOが身代金として440万ドル(約4億8,000万円)を支払ったと明かした。

Colonial Pipelineが運営している全長約5,500マイル(約8,851km)のパイプラインは、アメリカ東海岸で消費されるガソリンとディーゼル燃料の約45%をまかなっている。



Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom - WSJ
https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

大手日系自動車会社

H社は、2020年6月8日にランサムウェアによる大規模な被害を受けた。
6月8日午前に社内サーバーに障害が発生し、このときには既にウイルスが拡散している状態で、国内の4つの工場では完成車検査システムが作動せず、夕方まで出荷を見合わせることとなった。

また、工場や本社では「システムに接続できない」「メールの送受信ができない」という声があり、すぐに全社員のパソコン使用を制限し被害の拡大防止に努めた。
被害は国内にとどまらず、アメリカやトルコ、インドなどの工場でも一時自動車の生産がストップすることに。H社の工場は世界に30か所あり、そのうちの約3割が停止する事態に発展。
詳しい原因や内容についてはセキュリティ上回答できないとのことで公表されていないが、あまりにも大規模であることからH社をターゲットとして用意周到に行われたランサムウェア攻撃であるとの見解が強い。

参考：朝日新聞「H社、サイバー攻撃被害認める　身代金ウイルス拡大か」
ヤフーニュース「H社を狙ったサイバー攻撃。ADのドメインコントローラーの脆弱性が利用された可能性も。」

2. サイバー攻撃：ランサムウェア

ランサムウェアとは

ランサムウェアとは、身代金を意味する「Ransom」と「Software」を組み合わせた造語であり、暗号化などによってファイルを利用不可能な状態にした上で、そのファイルを元に戻すことと引き換えに金銭（身代金）を要求するコンピュータウィルスを指す。
ランサムウェアが世界中のコンピューターに感染し、工場が操業停止に追い込まれた企業が複数あるほか、イギリスでは国営医療サービス事業を行っているNational Health Serviceが被害を受け、手術の中止や診療が行えないといった事態が発生した。

感染経路の例

ウェブサイトからの感染

・改竄された正規のウェブサイトを閲覧することで感染
・不正広告を閲覧することで感染
・ダウンロードしたファイルを開くことで感染

電子メールからの感染

・メール本文に記載されたURLからアクセスして感染
・メールの添付ファイルを開くことで感染

感染すると…

PC・サーバーの利用に制限をかけられる

ファイル暗号化型 ファイルを暗号化し、開けなくなる。

MRB暗号化型 起動ファイルを暗号化し、操作できなくなる。

制限解除のため身代金を要求される

・脅迫画面が表示される。
・仮想通貨（Bitcoinなど）を支払うよう要求される。

3. 中国情報規制の三本柱 （2022年3月 現在）

TRE
Total Solution Provider

法律名称	域内適用	域外適用
サイバーセキュリティ法 2017年6月1日から施行	中国国内におけるネットワークやサイバーセキュリティの管理に関する法律。	規定なし
データセキュリティ法 2021年9月1日から施行	中国国内で行われるデータの取り扱いや管理に関する法律。重要データがどのようなものなのか、その範囲について現在整理が行われている。	中国国外でのデータ取り扱いが中国の国家利益または、公民・組織の権益を侵害した時は法的責任を追及できる。
個人情報保護法 2021年11月1日から施行	中国国内の個人情報の取り扱いに関する法律。個人の権益に重大な影響を及ぼし、または及ぼし得る個人情報取扱活動のリスクの明確化。	中国国外で中国国内の個人情報を取り扱うときに、以下の状況である時は本法が適用される。 ① 中国国内の個人に商品やサービスの提供が目的の時 ② 中国国内の個人の行為を分析・評価する時。 ③ 法律または行政法規が定めるその他状況。

4. サイバーセキュリティ法・個人情報保護法違反処罰事例

TRE
Total Solution Provider

北京市建設会社行政処分（等級保護義務違反）

2020年6月
インターネットセキュリティ部門の検査において、北京市の建設会社の財務帳表管理システムにおいて、コンピュータウイルスやネットワーク攻撃、ネットワーク侵入など、**ネットワークセキュリティを危険にさらす行為を防止するための技術的な対策がとられておらず**、その結果、外部からの攻撃被害により違法な情報が植え付けられ、**攻撃者の追跡ができなかったことが判明。**
行政処分：
サイバーセキュリティ法第21条、第59条の規定に基づき、建設会社に罰金10万元、安全責任者個人に5万元の行政処分を科した。

寧波市ホールディングス会社行政処分（等級保護義務違反）

2020年4月
公安当局の閲覧により、寧波市のホールディングス会社の**URL（企業ホームページ）がアダルトサイトに悪意を持って改ざんされていることを確認**。同社は、インターネットセキュリティ・インシデントに対する**緊急対応策を策定しておらず、また、システムの脆弱性を適時に処理していなかったため**、ネットワーク・セキュリティを危険にさらす結果となったことが判明。
行政処分：
サイバーセキュリティ法第25条および第59条第1項に基づき、行政処分として罰金1万元を科した。

蘇州市ソフトウェア会社行政処（個人情報保護義務違反）

2020年10月
ネットワークサービス提供者である蘇州市のソフトウェア会社2019年6月から2020年8月にかけて、同ソフトウェア会社が運営するスマートフォン用ゲームアプリについて、ユーザーがダウンロードした後、**初めて実行する際に「ユーザープライバシー同意書」を提供しておらず、提供するサービスとは関係のないユーザーの機密情報を収集する行為があり**、サイバーセキュリティ法第22条および第41条に違反していたことが判明した。
行政処分：
サイバーセキュリティ法の第22条および第41条の個人情報保護の義務を果たしていないとして警告し、同社の責任者に1万元の罰金を科した。

その他一般企業でもよくある通告・指導

×社外のサーバ攻撃の踏み台として利用される
電信局から貴社のIPアドレスを外部のWEBサーバの攻撃の踏み台として利用されているとし、処罰通告を受ける。通信設備に問題があり、早急に通信設備を更新し、当局に報告。

×ホームページのコンテンツ違反
ホームページで禁止文言を利用し、過大な表現で技術紹介を行っているとし是正通告。指摘された内容以外にもホームページ全体のコンテンツ審査、修正を行い当局に報告。

5. サイバーセキュリティ法　（2022年3月 現在）

TRE
Total Solution Provider

ネットワーク運営者として国の定めたセキュリティ等級保護制度に従い、ネットワークが妨害、破壊、または無許可アクセスを受けないように保証し、ネットワークの漏洩、窃取、改竄を防止しなければならない。セキュリティ等級保護制度により、システムの等級判定と保護義務の履行が必要。

システム等級判定の流れ（自社内での初期判断）

① 等級対象の確定
　（データ分類及びシステムの洗い出し）
② システム別で等級判定を実施
③ 初期判断等級の確定

システム初期判断等級確定例

システム名	損害の度合い		
	システム中断の影響	改竄された時の影響	等級判定
メール	市民及び法人の合理的な利益 一般損害	市民及び法人の合理的な利益 一般損害	一等級
企業ホームページ	市民及び法人の合理的な利益 一般損害	社会秩序 一般損害	二等級
在庫管理システム	市民及び法人の合理的な利益 一般損害	市民及び法人の合理的な利益 一般損害	一等級
財務システム	市民及び法人の合理的な利益 一般損害	市民及び法人の合理的な利益 一般損害	一等級

安全保護等級の区分

殆どの一般企業は赤枠に該当

等級	
第一級	情報システムが破壊された後、市民、法人、その他の組織の正当な利益に損害を与えるが、国家安全保障、社会秩序、公益を害することはない。
第二級	情報システムが破壊された後、市民、法人、その他の組織の正当な利益に深刻な損害を与えたり、社会秩序や公益に損害を与えたりするが、国家安全を損なうことはない。
第三級	情報システムが破壊された後、市民、法人、その他の組織の正当な利益に特に深刻な損害を与えたり、社会秩序や公益に損害を与えたり、国家安全保障に損害を与えたりする。
第四級	情報システムが破壊された後、社会秩序や公益に特に深刻な損害を与えるか、国家安全保障に深刻な損害を与える。
第五級	情報システムが破壊された後、国家安全保障に特に深刻な損害を与える。

等級と判断基準の関係性

影響範囲	損害の度合い		
	一般損害	深刻な損害	極めて深刻な損害
市民及び法人の合理的な利益	第一級 自主保護	第一級 自主保護	第二級 指導保護
社会秩序	第二級 指導保護	第三級 監督保護	第四級 強制保護
国家安全	第三級 監督保護	第四級 強制保護	第五級 専門機関保護

6. データセキュリティ法　（2022年3月 現在）

TRE
Total Solution Provider

「データセキュリティ法」は中国のデータ分野における基本法であり、データの概念を明確に定義するとともに、データ分類・等級付け保護、リスク評価、監視・早期警報、緊急対応等の各基本制度を確立し、**データ取り扱い活動を行う際に履行すべき各義務を明確化**した法律です。

「サイバーセキュリティ法」、「データセキュリティ法」においては、重要データの範囲が明確に定義されていないため、**国、各地方、および各業界による当該範囲にかかわるリストの策定が見込まれている**。

重要データとは、ひとたび**改ざん・破壊・漏えいされ、または違法に取得もしくは利用されると、国家の安全、公共利益または個人・組織の合法的な権益を侵害し得るデータ**をいう。

重要データのイメージ

業界	重要データ例
自動車	• 軍事管理区、国防科学技術工業組織等の国家機密にかかわる組織、県級以上の共産党機関・政府行政機関などの重要かつ機微な区域における地理情報および人・車両の流れのデータ • 交通量や物流などの経済の運営状況を反映しているデータ • 自動車の充電ネットワークの運営データ • 人相、ナンバープレートなどの車外の映像・画像のデータ • 10万人以上の個人情報 • 国務院の関係機関が指定している国家の安全、公共の利益または個人 • 組織の合法的な権益を侵害し得るその他のデータ
電子商取引	• 電子商取引プラットフォームにおける個人の登録情報 （氏名、性別、年齢、住所、婚姻、学歴、職業、収入、口座、連絡先など） • 電子商取引記録、個人の消費習慣・嗜好、企業の経営などにかかわるデータ • 電子商取引における各当事者の信用記録、信用評価情報
工業	• 世界的に先進的な水準にあり、国民の経済に重要な影響をもたらす工業の研究開発関連のプロジェクトまたはプランのデータ • 国際的な水準にあり、かつ、重大な経済的効果を生み出す科学研究成果の中核となる部分のデータ • 工業と科学技術の発展に向けた重点任務におけるセキュリティ関連の重要な科学技術にかかわるデータ

7. 個人情報保護法　（2022年3月 現在）

TRE
Total Solution Provider

個人情報保護法内容要約：
合法・正当・必要の原則を順守して個人情報を収取・利用しなければならない。

概念：
個人情報とは、電子或いはその他の方式により記録する、自然人個人の身分を識別し得る各種情報を指す。

個人情報認定方法：認識＋関連性
「個人情報保護法」第4条の「個人情報」に関する定義によると、企業は「認識+関連性」の基準を使用し、これにより取り扱うデータの個人情報構成の成否を認定することができる：
① 認識の基準：情報から個人が認識される場合。すなわち、情報自体の特別性から、特定の自然人を認識することができるものである。たとえば、身分証明書番号などである。
② 関連性の基準：個人から情報が生ずる場合。すなわち、特定の自然人が既に知られており、当該特定の自然人が、自らの活動において生ずる情報である。たとえば、既に知られている特定の自然人の位置情報、通話記録などである。

個人情報および個人センシティブ情報の例	
基本情報	氏名、誕生日、性別、民族、国籍、家族、住所、電話番号、メールアドレスなど
身分情報	身分証明書、パスポート、労働許可証、社会保険カード、居住証など
生物識別情報	DNA、指紋、虹彩、顔識別特徴など
ネットワーク身分識別情報	システムアカウント、IPアドレス、電子メールアドレス、関連パスワードなど
健康生理情報	疾病により生ずる関連記録、例えば病症、検査報告書、生育情報、過去の疾患、感染症の病歴など
教育就職情報	個人の職業、職位、就職先、学歴、教育実務経験など
財産情報	銀行口座、識別情報、預金情報、不動産情報、信用調査情報など
通信情報	通信記録および内容、SMS、電子メールなど
連絡先情報	連絡先リスト、友達リスト、電子メールリストなど
ネットワーク利用情報	ウェブサイトの閲覧記録など
常用設備情報	ハードウェアのシリアルナンバー、デバイスのMACアドレスなど
位置情報	行動履歴、高精度の位置情報、宿泊情報、緯度・経度など
その他	婚姻歴、宗教信仰、性的指向、未公開の犯罪記録、十四歳未満の未成年者の個人情報など

赤字は**個人センシティブ情報**：漏えいし、または違法に使用されたときは、自然人の人格上の尊厳に対する侵害、または人身もしくは財産の安全性に対する脅威を容易に引き起こす個人情報

ITセキュリティ対策について

8. なにをしなければいけないのか - 1/2

TRE
Total Solution Provider

①　保有するシステムの洗い出し

社外ネットワーク：（ホームページ等）
アカウント登録必要：外部ユーザーの情報を収集・利用している（プラットフォーム）
アカウント登録不要：広告宣伝・閲覧のみのウェブサイト
特にホームページ等のウェブサイトの場合、広告で規制されている禁止用語に注意すべきである。

社内ネットワーク：　生産管理システム、財務管理システム、人事管理システム、監視カメラシステムなど

②　安全保護等級の判定

保有するシステムに基づき、それぞれのシステムの等級を自己判定する。詳細はP8サイバーセキュリティ法を参照。

自己判定が一級の場合：国家の管理規範及び技術標準に基づいて、自主的に保護を行う。

自己判定が二級もしくはそれ以上の場合：専門家の評価、主管部門の確認と登録承認管理が必要となる。

③　内部管理制度の見直し

- **サイバーセキュリティ責任者と管理者の任命**

- 内部安全管理制度及び操作規程
  緊急対応策の制定などを作成。特に個人情報を取り扱う担当者の権限管理や教育、データ越境の操作手順、重要データなどについては注意が必要。
  また、ルーターやスイッチ等のネットワーク機器のパスワードが初期値のままになっていないか？等の見直しも重要。

- 社内研修の実施

8. なにをしなければいけないのか - 2/2

④ 内部技術措置の見直し

- **コンピュータウィルス等の被害防止のための技術的処置**
  コンピューターウィルスやサイバー攻撃・ネットワーク侵入等、ネットワークのセキュリティに危害を加える行為を防止する措置を講じる。

- **モニタリング等の技術措置を講じ、少なくとも6か月間のログ保存が必要**
  有事の際に原因の調査ができるようにする。

- **データの分類・重要データのバックアップ及び暗号化等の措置を講じる**
  特に個人情報に対し、暗号化、無標識化して、ランク分けしなければならないなどの注意すべき点である。

⑤ 個人情報取り扱い方法の見直し

- **収集・利用：**
  違法収集を禁じ、収集頻度、数量を必要最小限にする。
  同意を得る：目的、方式、範囲などを個人に対し明確かつ分かりやすく提示し、収集・利用の同意得る
  ■個人のセンシティブ情報を収集・利用する場合：
  利用目的、方式、範囲を十分に理解した上、本人の明確な同意を得る必要がある。
  ■14歳以下の個人情報を収集・利用する場合：本人もしくは後見人の明確な同意を得なければならない。

- **保存：**
  安全性確保の義務：重要度ランク分け、暗号化、匿名化などの措置をとる。

- **削除：**
  同意した保存期限を超え、もしくは利用目的を達成した個人情報は即時に削除しなければならない。
  本人が自分の情報を検索、修正、削除、また同意授権の撤回、アカウント抹消などを出来るようにすること。

9. なにをしなければいけないのか（万一の場合）

TRE
Total Solution Provider

クラッキングやフィッシング等、サイバー被害の種類は様々ですが、中でも代表的なものがコンピューターウィルスです。ウィルスのワクチンは、ウィルスが発見された後に開発されます。その為、ウィルス感染の対応方法（感染時の対策）の準備が重要です。（社内のIT部門支援としてウィルスのリカバリー実績のあるIT会社へ依頼する。弊社TREは実績有り）

① ウィルス感染時の初期対応への施策

- **ウィルス等に感染した機器への停止手順（感染時の機器停止の手順書の事前作成）**
  コンピューターウィルスに感染した人が、即座に行う機器への動作手順を決めて、全員に周知しておく。

- **ウィルス感染の通報手順（感染時の通報体制の事前構築）**
  発見者（感染者）が、誰に連絡するかの通報体制を定め、周知させる。

- **ウィルス等に感染した機器のサーバーとネットワーク環境のチェック手順（被害調査委員会の行動規範書の事前作成）**
  有事の際に、予め決められ被害調査委員会の元で、原因の調査を即時に開始する。
  被害状況を経営トップへ報告する。（サーバーの死活、データ流出、身代金、停止によるお客様への影響、想定被害総額、etc）

② ウィルス感染後の復旧対策への施策

- **復旧ポリシーと関連部門へ報告の手順（復旧委員会の行動規範書の事前作成）**
  復旧ポリシーの決定（システム復旧、身代金支払い、その両面の並行活動、etc）、被害調査報告を参考にする。
  関連部門（本社、関係会社、行政機関）へ報告し、協力を求める。

- **システム復旧**
  復旧実績の有るIT会社と連携し、システムの再構築を行う。
  不足情報は、関連会社（得意先、調達先、etc）から入手、紙情報からデータ登録するツールを緊急作成する等して対応する。

- **身代金支払い**
  本社や行政機関から指導を仰ぎ対応する。

10. 内部技術措置の見直し

TRE
Total Solution Provider

機器名 ソフト名	機能概要	中国情報規制の三本柱			優先順位 （参考基準）
		サイバー セキュリティ法	データ セキュリティ法	個人情報 保護法	
ファイヤー ウォール	外部からのサイバー攻撃を防ぎ、通信の記録を取得、保存する。モジュールを追加することで内部からの通信も管理することができる。	◎	◎	◎	高
アンチウイル スソフト	PCのウイルス感染を防ぐ。フィッシングメールチェックやPCウイルスチェックなど行う。	◎	◎	◎	高
バックアップ	データが紛失、窃盗、改竄後に、データを復旧することができる。	○	○	○	高
Windows OS	正規のWindows OSを使用していいない場合や、Windows Updateを行っていない場合、セキュリティリスクが高い。	△	△	△	中
ゲスト用 Wi-Fi	来客用Wi-Fiを準備することで、重要なネットワークにむやみに機器を接続されないようにする。	○			低
IP-guard	情報流出を防ぐ専用システム。データの暗号化、PC資産の管理、日々の操作記録の取得など、様々なITセキュリティ機能を提供する。	○	○	○	オプション （あれば尚安心）

※ 上記は2022年3月時点での弊社参考方案です。セキュリティ対策に万全はなく、時々刻々と技術も変化します。

11. 参考価格

TRE
Total Solution Provider

機器名 ソフト名	内容	機能	優先 順位	参考価格 （RMB・税前）	作業料金 （RMB・税前）
ファイヤーウォール	本体	ファイヤーウォール本体、内部ネットワークと外部ネットワークの通信管理。	高	8,300	2,400
	UTM	外部からの通信内容をチェックし、リスクのある通信を遮断する。	高	4,300	（上記に含む）
	インターネット管理	内部ネットワークの監視を行い、管理と詳細を記録する。内部から外部の通信を分析し、許可されていない通信を遮断する。	高	16,300	2,400
アンチウイルスソフト	ソフト	PCのウイルスを検出・除去・予防するためのソフトウェア	高	エンドポイント型：250/台 サーバー型：2,000~	300/台PC 600/サーバー
バックアップ	システム	重要データをクラウドにバックアップする。	高	300GB：4,000/年	–
Windows OS	正規OS	Windows 正規OS オープンライセンス	中	1,850/台	600/台
ゲスト用 Wi-Fi	AP	ゲストWi-Fiを設定するWi-Fiのアクセスポイント	低	3,100/台	600/台
IP-guard	システム	情報流出を防ぐ専用システム レポーティングサービス付	オプション （あれば尚安心）	1ユーザー：150/月~ 最低契約数20ユーザー	10,000

※ 上記は2022年3月時点での弊社参考価格です。詳しくは、弊社担当までお問合せ下さい。

TRE

TRE

www.tre-china.cn

WeChat

TRE
Total Solution Provider

广州泰昇计算机科技有限公司
Guangzhou TRE Computer Technology Co., Ltd.

中国广东省广州市天河区体育东路140-148号南方证券大厦2004-2005室
Unit 2004-2005, Southern Securities Building, 140-148 Tiyu East Road, Tianhe District, Guangzhou, Guangdong, China

TEL (86) 20-3887-8299
FAX (86) 20-3887-8160
Mail sales@tre-china.cn
Web www.tre-china.cn

【上海オフィス】
上海市漕溪北路18号上海实业大厦34楼H室（レイズビジネスコンサルティング内）

TEL 86 021-6427-0569