TLP:GREEN

今後の日本におけるサイバー環境の変化に伴い、新たなに想定すべき「制御システムにおけるサイバー脅威」

2019年 2月

名和 利男

アジェンダ

1. 日常化した**制御システムへのサイバー攻撃**
   - 2015年-2016年 ウクライナのサイバー攻撃による計画外停電
   - 2017年6月 NotPetyaによる重要インフラ機能喪失
   - 2017年後半 GPSスプーフィングによる重要インフラ機能障害
   - 2018年 DDoS攻撃による重要インフラ機能喪失及び
     重要インフラ事業者のレピュテーション低下

2. 今後の日本における**サイバー環境の変化**

3. 新たなに想定すべき**制御システムにおけるサイバー脅威**

   （*保全の都合上、説明資料及び根拠情報は投影のみ*）

TLP:GREEN

TLP:GREEN

トピック 1

日常化した**制御システムへのサイバー攻撃**

TLP:GREEN

日常化した**制御システムへのサイバー攻撃**

2015年-2016年 ウクライナのサイバー攻撃による計画外停電

2015年12月 **ウクライナ西部**におけるサイバー攻撃による計画外停電

- 2015年12月23日、ウクライナ西部の複数の電力供給会社が、同時的なサイバー攻撃を受けて、イヴァーノ＝フランキーウシク州の**約8万の顧客への電力供給に障害が発生**した。
- ほぼ同時に、電力供給会社の**電話回線にも障害**が発生し、顧客からの全ての電話を受け付けることが出来なくなった。
- 大まかな攻撃プロセスは、次のとおり。
  - ① 電力供給会社に、ウクライナ・エネルギー省を詐称したスピアフィッシングメールが送付される。
  - ② 受信したユーザーが、スピアフィッシングメールの添付ファイルを開く。
    - 添付ファイルは、Microsoft 社のオフィス文書(XLSファイル)で、マクロ型不正プログラムが動作する仕組み
  - ③ オフィス文書に埋め込まれていたマクロ(VBA)が動作し、外部ホストからいくつかのモジュールがダウンロードして組み込み、GmailをC2利用した外部からのリモートコントロールを行われる。
  - ④ その後、およそ6ヵ月間に渡り、オペレーターのユニットPCにラテラルムーブメントして、モニタリングを継続し、**電力網の制御システムにログインするIDやパスワードを特定**して窃取する。

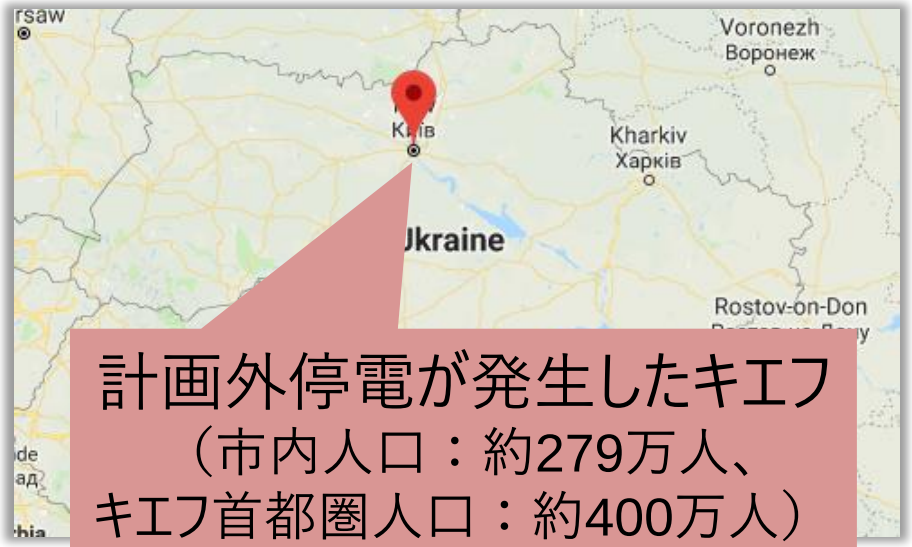
計画外停電が発生した
ウクライナのイヴァーノ
＝フランキーウシク州
（総人口： 約140万世帯、
都市人口：約59万世帯
ウクライナ人：97.5%、
ロシア人：1.8%）

TLP:GREEN

2016年12月 **ウクライナ北部**におけるサイバー攻撃による計画外停電

- 2016年7月頃から、ウクライナ政府機関や重要インフラ事業者を標的とした**大規模なスピアフィッシングメール攻撃**が発生。
  - スピアフィッシングに使われた電子メールは、非常に信頼されている人物から送られたように偽造されており、添付ファイルを開くとマルウェアに感染するというものだった。
  - スピアフィッシング詐欺の標的と窃取された情報から、**重要インフラ事業者へのサイバー攻撃のための事前偵察を行っていた**と推定。
  - 特に、鉄道システムのサーバや、政府機関(省庁職員)のPC、国の年金基金等から情報流出した。

- 2016年12月17日、日付が変わる直前から**ウクライナの首都キエフ北部の**ピヴニシュナ変電所で**計画外停電**が発生。
  - 変電所はマニュアル操作に切り替え、約1時間15分後に電力を回復。
  - 関連するサイバー攻撃は、2016年12月6日から始まり、20日まで継続。
  - マルウェアが、(ゼロデイ)脆弱性やアカウント乗っ取りを使わず、**発送電設備を直接操作**した。

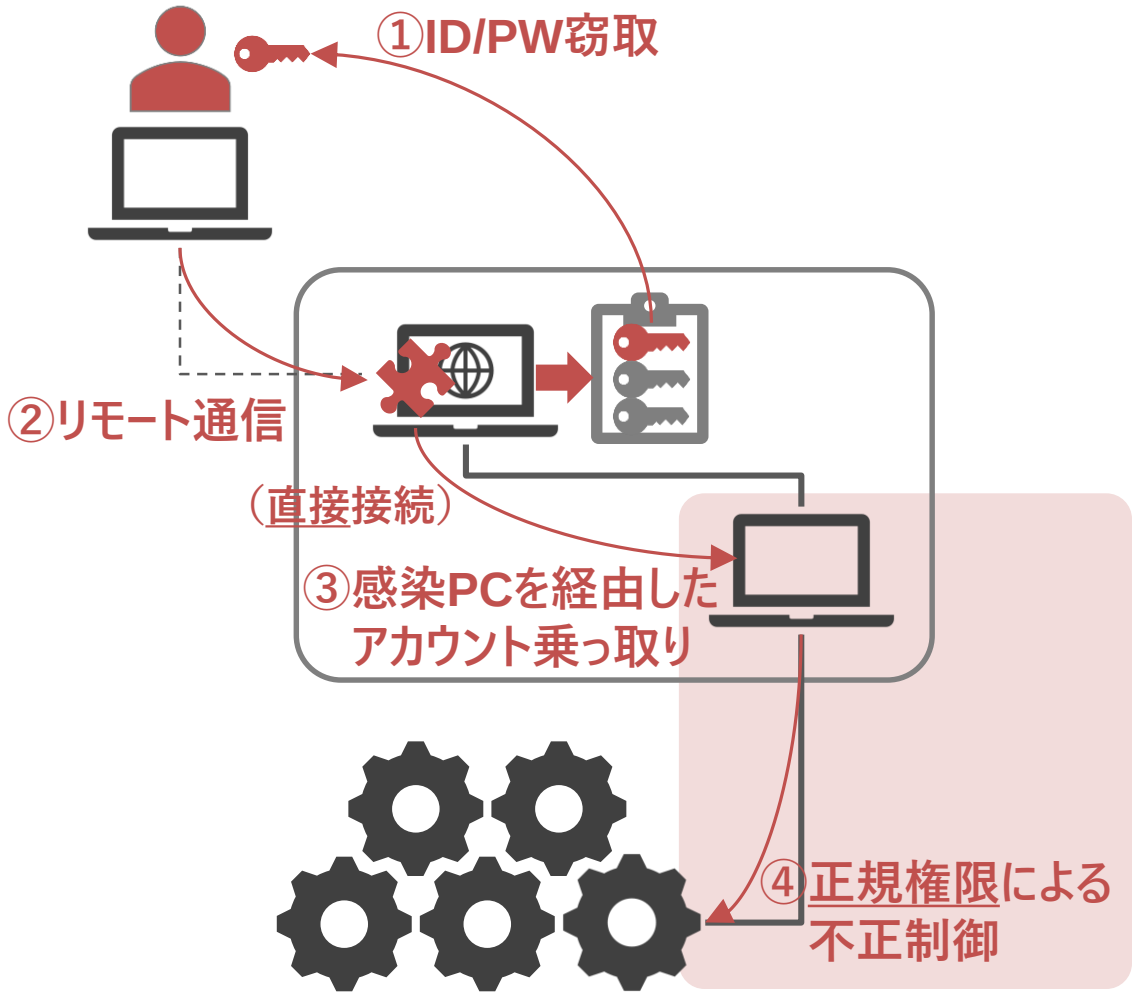


計画外停電が発生したキエフ
（市内人口：約279万人、
キエフ首都圏人口：約400万人）

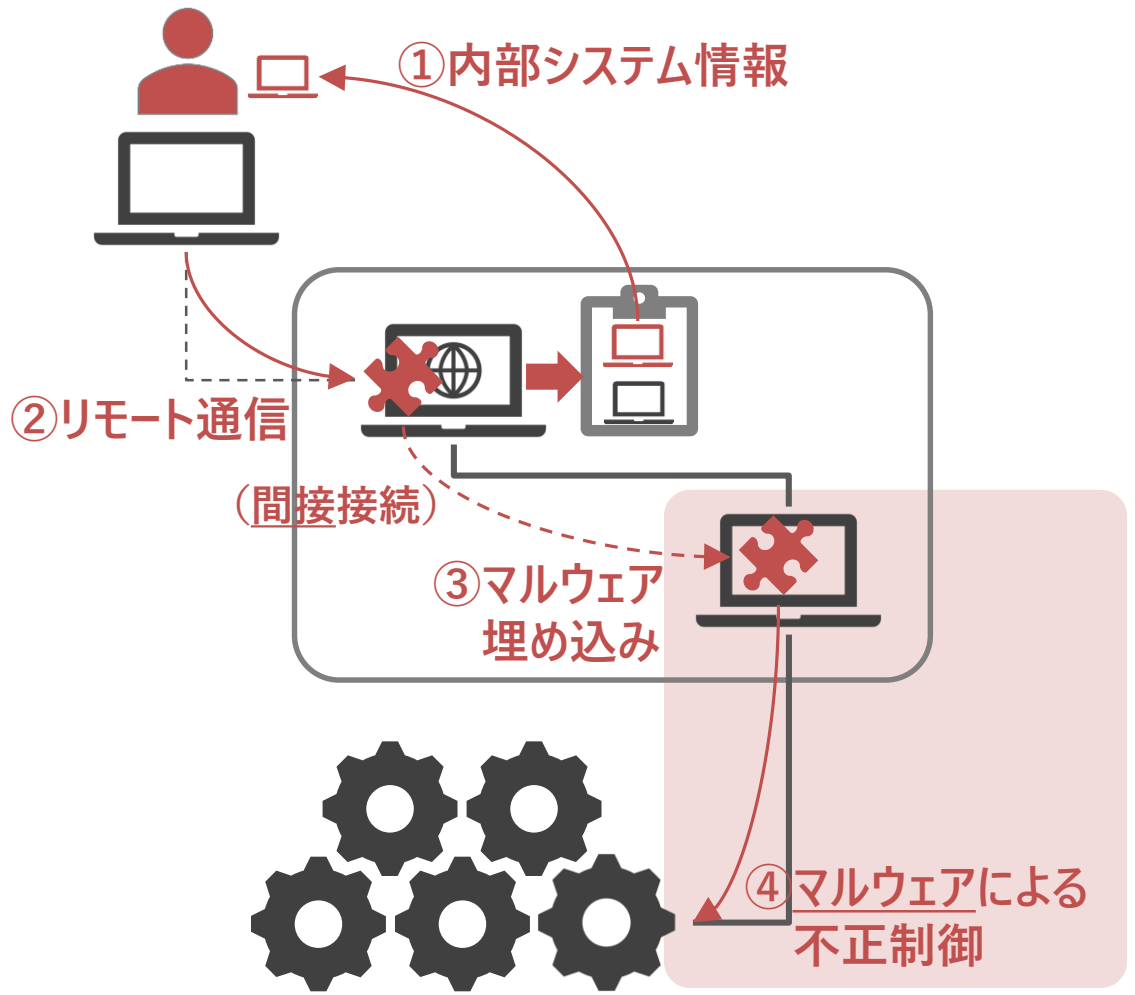
TLP:GREEN

ウクライナの電力会社における制御システムに対する攻撃の変化

【2015年12月】



【2016年12月】



TLP:GREEN

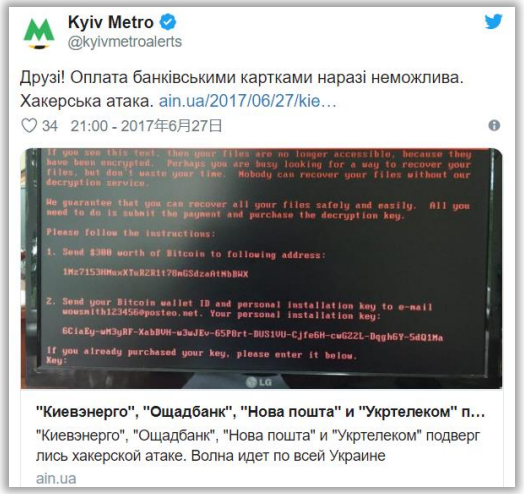
TLP:GREEN

日常化した**制御システムへのサイバー攻撃**

2017年6月 NOTPETYAによる重要インフラ機能喪失

2017年6月ウクライナにおける**NotPetyaによる重要インフラ機能喪失** (1)

- 2017年6月27日、侵害を受けていたウクライナの**会計ソフトベンダー「M.E.Doc」のソフトウェアのアップデート**を通じて、多数のPCが NotPetyaに感染した。
- NotPetyaは、WannaCryと同様、米国のNSAが開発したとされるEternalBlueとEternalRomanceが取り込まれていたため、**高度な感染能力により、さまざまなシステムに拡大**し、機能障害を発生させた。



Kyiv Metro(首都キエフの地下鉄) Alerts のツイート
「皆様へ! 現在、(運賃の)カード払いは不可。ハッキングの影響で」
https://ain.ua/2017/06/27/kievenergo-i-ukrainskie-banki-podverglis-xakerskoj-atake

セキュリティ専門家(ミッコ・ヒッポネン)によるツイート
「PaTyaにより **ATMが使用不能**」
https://twitter.com/mikko

損傷したチェルノブイリ原子力発電所の
放射線監視が停止し、手動に切り替えた
https://www.rt.com/news/394301-ukraine-cyberattacks-disrupt-chernobyl-systems/

TLP:GREEN

2017年6月ウクライナにおける**NotPetyaによる重要インフラ機能喪失** (2)

- NotPetya感染の背景
  - ウクライナでは、通常、企業の納税申告の期限日が6月30日に設定されている。
  - NotPetyaが一気に拡散した6月27日は**納税申告の締め切りの直前**だった。
  - しかし、普段の業務で使っているマシンが機能障害となったため、ウクライナ政府は「NotPetyaに感染した企業」の税務申告の期限日を12月31日まで延長すると発表した。

- NotPetya感染の経緯
  ① 何者かがMEDocのソフトウェア更新サービスのサーバに管理者権限を使ってログイン。
  ② ルート権限を取得し、サーバの設定ファイルを改ざん。
  ③ MEDocの更新版にバックドアを埋め込む。（**2018年4月には完了していた**）

- NotPetya の狙い
  - システムの復旧がほぼ不可能な点から、攻撃者の狙いは**ランサムウェアを隠れ蓑にした破壊行為**であると推定。

TLP:GREEN

日常化した**制御システムへのサイバー攻撃**

2017年後半 GPSスプーフィングによる重要インフラ機能障害

2017年6月 黒海における**GPS位置情報のスプーフィング**(なりすまし)の可能性

- 2017年6月22日、ロシアのノヴォロシースク港沖を航行中の船舶の船長が、搭載している**GPS機器が間違った位置データを表示**していること発見した。
  - 船長は、航法装置が適切に作動していることを確認した後、他の近くの船に連絡して、彼らのAISトレースデータ(船舶を追跡するために使用される自動識別システムからの信号)が、**すべて同じ「間違ったGPS位置データ(ロシアの首都クレムリンから32km離れたヴヌーコヴォ空港近く)」を示していることを確認**した。少なくとも20隻が影響を受けていた。
  - ロシアのノヴォロシースク港は、ケルチ海峡近くの**ロシアのクリミア半島の向かい側**にあり、緊張した黒海地域の北端に位置している**ロシア黒海艦隊のための主要軍港**である。

https://www.youtube.com/watch?v=-CJXLVBI-ew

TLP:GREEN

2017年8月-9月 GPSスプーフィングによる重要インフラ機能障害 (1)

- 2017年8月30日、ラトビアのバルト海沿いの西部で7時間に渡り大規模な**セルラーネットワークの機能停止**した。
- 2017年9月7日、ノルウェーのイーストフィンマルク地区を飛行する**民間航空機が長期間にわたりGPS信号を完全に消失**した。
- 2017年9月13日、ラトビア(米国の911に相当する)112の**緊急電話ホットラインが約16時間停止**した。

https://www.washingtonpost.com/world/europe/latvias-cellphones-stopped-working-russias-war-games-may-be-to-blame/2017/10/05/449162d4-a9d3-11e7-9a98-07140d2eed02_story.html

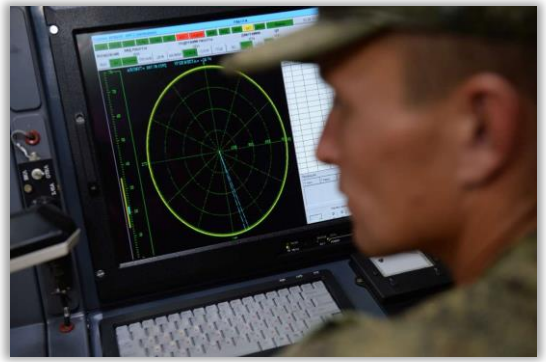
https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305

TLP:GREEN

2017年8月-9月 **GPSスプーフィングによる**重要インフラ機能障害 (2)

- 2017年9月14日から20日までに行われたZapad 2017(**ロシア軍が4年毎に実施するベラルーシ軍と共同演習**)を行った。
  - ラトビアのバルト海沿いの西部のGPS障害やセルラーネットワークの障害は、この**演習の一環で行われた電子戦**であると分析されている。
  - ロシアは、開発しているサイバー攻撃や電子戦の技術を、Zapad2017で**テストしている可能性**がある。
    - ロシアは、FM電波、SATCOM(衛星通信)、携帯電話、GPS、その他の信号を遮断するための攻撃システムを使用するハイブリッド攻撃を完成させている。
      (出典: 2016年12月米陸軍の非対称戦グループ発行 "Russian New Generation Warfare"ハンドブック)

http://www.thedrive.com/the-war-zone/15194/russia-jammed-phones-and-gps-in-northern-europe-during-massive-military-drills



TLP:GREEN

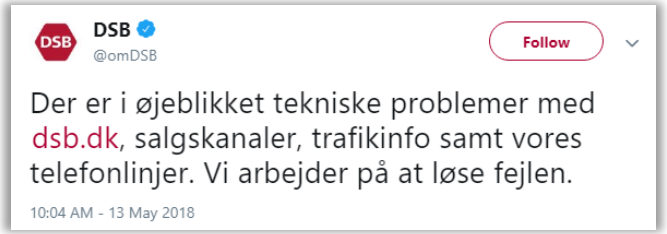
TLP:GREEN

日常化した**制御システムへのサイバー攻撃**

2018年 DDOS攻撃による重要インフラ機能喪失及び重要インフラ事業者のレピュテーション低下

2018年5月 デンマークの鉄道会社DSBへの**DDoS攻撃**

- 2018年5月13日(日曜日)の夜、デンマークの鉄道会社DSB(Danske Statsbaner)がDDoS攻撃を受け、**DSBアプリ、Webサイト、チケット販売機、駅構内のセブンイレブンのキオスクで切符購入ができなくなった**。
  - Rejsekort トラベルカードを持っていた乗客は、列車内の乗務員から切符を購入できたが、約15,000の顧客が影響を受けたと推定。
  - これに対し、DSBの広報担当は、「本事案に関する専門家を迎え入れており、明日の朝までに、すべてのシステムを通常稼働にする」と伝えた。
- このDDoS攻撃の発生と同時に、**内部メールシステムと電話インフラが使用不能**になった。
  - そのため、顧客とコミュニケーションをとる方法は、ソーシャルメディアのみとなった。



https://twitter.com/omDSB/status/995711445454196737

現在、dsb.dkサイト、販売チャネル、交通情報、電話回線に関する技術的な問題が発生しています。私たちはこのエラーを解決するために取り組んでいます。

https://twitter.com/omDSB/status/995898708700123136

dsb.dkサイトへのアクセスエラーが継続して発生していることを認識しました。一部誤解されていますが、私たちはその問題に取り組んでいます。

TLP:GREEN

2018年 デンマークにおけるデジタル化とサイバー脅威の高まり

- 2018年、デンマークは国家戦略「デジタル化のフロントランナーになる」を発表し、2025年までに約170億円を確保し、デジタル化を推進している。
  - デンマークは、3年連続EU内で最もデジタル化が進んでいる国として有名
- デンマークにおけるデジタル化の特徴
  - 小国(小さいところに多くの要素が集積しているため、アクションを取りやすい)、社会保障国家、民主主義国家であること
  - ビッグデータ(スマートフォンから得られる位置情報や、サーバー上のメール、カード会員情報など、ビジネスに役立てるための膨大で複雑な情報)が集積している
  - オープンイノベーション(自社だけでなく他社や大学、自治体など、外部のテクノロジーやアイデア、ノウハウ、データなどを組み合わせイノベーションを促進していくビジネスモデル)

オープンイノベーションが進展していくと、攻撃者も、重要インフラ分野で実装された(新しい)技術情報を得やすくなる。

TLP:GREEN

2018年9月 ドイツの大手電力事業者RWEへの**DDoS攻撃**

- 2018年9月25日、BSI(ドイツ情報セキュリティ機関)が、大手電力事業者RWEのWebサイトに対するDDoS攻撃が発生したと発表した。
  - この発表によると、DDoS攻撃は、発表時においても継続して観測されており、BSIとRWEが対応を協議している。
  - BSIは、これによりWebサイトによるRWEの情報提供に支障をきたしているが、重要度の高いサービスではないため影響は限定的であるとしている。
- 同時期、RWEが石炭の採掘を計画しているハンバッハの森において、ドイツの抗議者たちがキャンプアウト(座り込みに相当)をしており、警察が排除を始めていた。
  - Anonymous Deutsch という匿名のサイバー攻撃集団が、警察が抗議者らの排除を停止しなければ、DDoS攻撃を仕掛けると警告していた。
- このDDoS攻撃と同時に、強い抗議メッセージがYouTubeで公開された。

Cyber-Angriff auf RWE

Ort Bonn
Datum 25.09.2018

Der Energieversorger RWE ist Ziel eines sogenannten Distributed-Denial-of-Service-Angriffs (DDoS) geworden. Durch diese Überlastangriffe ist die Konzernwebseite wiederholt nicht mehr über das Internet erreichbar. Der Angriff hält zum jetzigen Zeitpunkt an. Das BSI steht mit RWE in Kontakt.

Hierzu erklärt Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

"Der Cyber-Angriff auf RWE zeigt deutlich, dass Konflikte sich jederzeit in den Cyber-Raum übertragen können. Im aktuellen Fall ist die Informationswebseite des Unternehmens betroffen, jedoch keine kritische Dienstleistung. Man darf dies daher nicht dramatisieren, aber dennoch müssen wir solche Angriffe ernst nehmen. Denn in Krisensituationen sind Informationen und die Möglichkeit der schnellen Kommunikation über das Internet von besonderer Bedeutung."

Pressekontakt:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn
Telefon: +49 228 99 9582-5777
Telefax: +49 228 99 9582-5455
E-Mail: presse@bsi.bund.de

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriff_RWE_25092018.html

https://www.youtube.com/watch?v=ivbbsJRztwg

https://www.youtube.com/watch?v=-kskw829viw

TLP:GREEN

2018年 ドイツのハンバッハの森における褐炭採掘への反対運動

- 大手電力事業者RWEは、2003年からNRW(ノルトライン＝ヴェストファーレン)州に所有する**ハンバッハの森で樹木を切り倒し、露天掘りによる褐炭採掘**を進めていた。
  - 褐炭は火力発電所の燃料として使われる。
  - ハンバッハの森の面積は、当初約5,500ヘクタールだったが、伐採により樹木が残っているのは200ヘクタールになっていた。
  - RWEは、NRW州政府の許可を受け、**2018年10月から残りの樹木を伐採する予定**だった。
- 2018年9月16日、**約9000人の市民や環境団体の会員**らが、バッハの森に集まり、**樹木の伐採に抗議**するデモを行った。
  - 一部の活動家が、RWEが褐炭の露天掘り作業を妨害。
- 2018年9月19日、ハンバッハの森で取材していたフリージャーナリストが、木の梢に作られた小屋をつなぐ梯子から**転落して死亡**した。

2018年9月19日、
取材中のジャーナリストが転落死する事故

2018年10月5日、
環境保護団体グリーンピースからメルケル首相に対するハンバッハの森の保護を求めた文書

メディアやSNSで炎上して、(自称)Anonymousが出現及び活動した。

TLP:GREEN

トピック 2

今後の日本における**サイバー環境の変化**

今後の日本における**サイバー環境(Cyber Environment)**の変化

【テクノロジー】

- **USBグッズ**のオフィス利用
- ノートPCの**SSD**採用率の増加
- **ビジネスチャット**の利用拡大
- **RCS準拠**のメッセージングサービスの増加
- **キャッシュレス**取引の拡大
- **4K 8Kテレビ**放送の開始
- PSTNから**IP網への移行**
- 高速通信規格**5G**の導入
- 新たな**IoT用無線通信サービス**(LPWA等)
- 次世代無線規格 **Wi-Fi 6**

【Deep Web】

- **オンラインゲーム上のチャット**で闇取引
- オルトコイン情報の流通基盤(**Telegram**)

【対策】

- **CASB**(クラウドセキュリティ)
- EPP/**EDR**(エンドポイントセキュリティ)
- **カード決済のIC対応**(改正割賦販売法)
- **サプライチェーンリスク**の対策(SP800-171)
- **有給休暇**の義務化(働き方改革関連法)

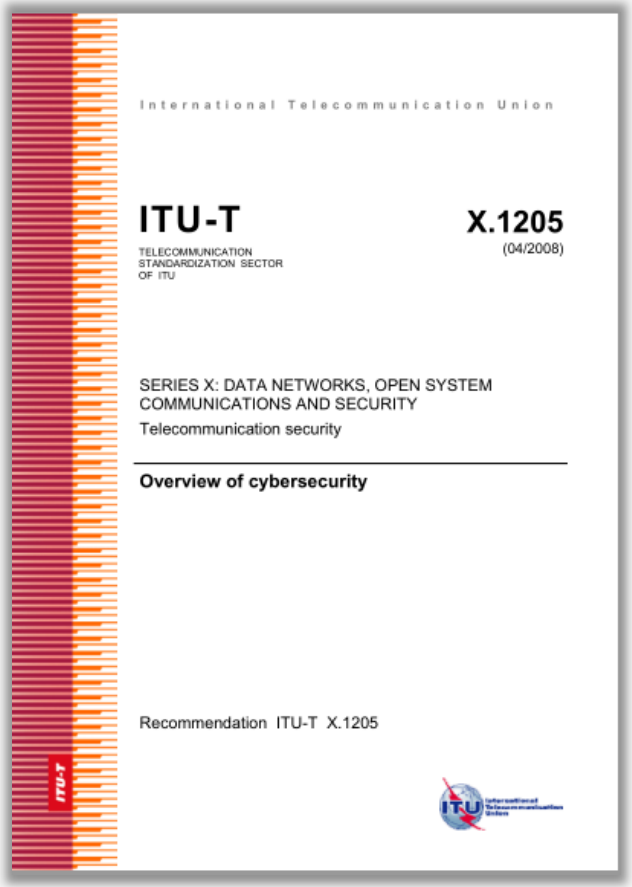
【ビジネス等】

- 少子高齢化に伴う**労働人口の急減**
- ERAB/**ネガワット取引**
- 「**全銀EDIシステム**」の稼働
- **OTT事業**(スポーツ等)の拡大
- 「**スポーツホスピタリティ**」の開始
- **外国人受け入れ**拡大(出入国管理法改正)
- **水道民営化**(水道法改正)

TLP:GREEN

【参考】サイバー環境(Cyber Environment)とは

- サイバー環境(Cyber Environment)には、次の構成要素があると定義されている。
  - ユーザー
  - ネットワーク
  - デバイス
  - 全てのソフトウェア
  - プロセス
  - ストレージ(記憶媒体)或いは経路上の情報
  - アプリーション(特定の作業や業務を目的として基本ソフトウェア上で動作するソフトウェア)
  - ネットワークに直接的及び間接的に接続されることのあるシステム



https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

TLP:GREEN

トピック３

新たなに想定すべき**制御システムにおけるサイバー脅威**

新たなに想定すべき**制御システムにおけるサイバー脅威**の例

- 「**USBグッズ**のオフィス利用」
  - BadUSBによるデータ破壊を利用した誘導工作
- 「ノートPCの**SSD**採用率の増加」+「次世代無線規格 **Wi-Fi 6**」
  - 痕跡及びログの不足によるインシデントの原因究明の困難化
- 「少子高齢化に伴う**労働人口の急減**」+「**外国人受け入れ**拡大(出入国管理法改正)」
  - 不十分な個人信頼性確認のまま採用した経験の浅い技術者の早期退職による内部情報流出
  - メーカー技術者の常駐困難化により(徐々に)利用が始まる(セキュリティレベルの低い)リモート保守への攻撃
- 「**4K 8Kテレビ**放送の開始」
  - PTP(高精度時間プロトコル)の周波数ソースGPS/GNSSに対するタイムスプーフィング攻撃
- 「**サプライチェーンリスク**の対策(SP800-171)」
  - 制御システムの周辺システム(自動消火、警備、ビル管理、防災等)に対するソフトウェアサプライチェーン攻撃
- 「**水道民営化**(水道法改正)」
  - 浄水場の遠隔監視システムのアカウントハイジャックや中間者攻撃による毒物投入

新たなに想定すべき**制御システムにおけるサイバー脅威**の例

（保全の都合上、説明資料及び根拠情報は投影のみ）

TLP:GREEN

本資料に関する連絡先

名和 利男（Toshio NAWA）

SITE: https://www.nawa.to

PGP: 0xE38B4E01

TLP:GREEN