日本を取り巻く
サイバー攻撃の動向と事例
その対策のために

元・陸上自衛隊
システム防護隊初代隊長
前・経済産業省大臣官房
サイバーセキュリティ・情報化審議官
工学博士

伊東　寛

元・陸上自衛隊
システム防護隊初代隊長
前・経済産業省大臣官房
サイバーセキュリティ・情報化審議官
工学博士

1980～2007:
1980年慶應義塾大学大学院（修士課程）修了。同年、陸上自衛隊入隊。技術、情報及びシステム関係の部隊指揮官・幕僚等を歴任。この間、陸自初のサイバー戦部隊であるシステム防護隊の初代隊長を務めた。
2007～2016:
2007年自衛隊を退官し株式会社シマンテック総合研究所主席アナリストに。以後、株式会社ラック ナショナルセキュリティ研究所所長等、民間セキュリティ企業で勤務。
2016: 経済産業省大臣官房サイバーセキュリティ・情報化審議官に着任。
2018: 経産省を5月に退職。

主な著書に『「第5の戦場」サイバー戦の脅威』『サイバーインテリジェンス』『サイバー戦争論』などがある

はじめに

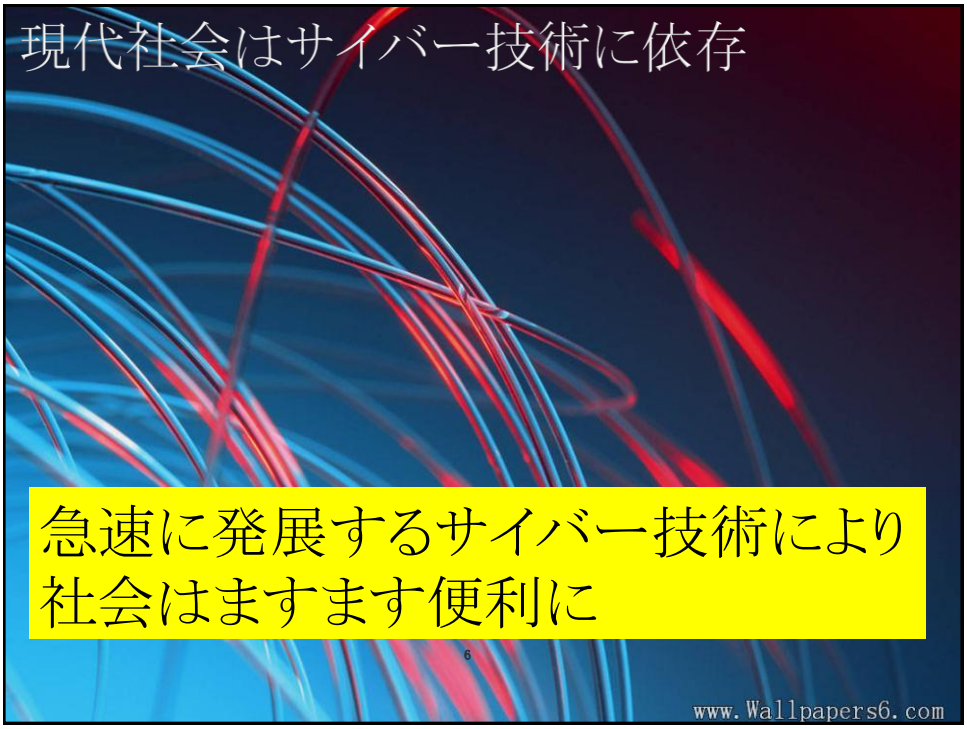
本講演の内容は、公開情報に基づき、発表者が個人的に分析した成果によるものであり、政府関係機関や民間会社等の見解を代表するものではありません。

1.サイバー技術とサイバー攻撃

サイバー技術の利用

- コミュニケーション（メール、チャット、テレビ会議）
- 情報発信（Webサイト、メールマガジン、ブログ、ツイッター）
- 音楽や動画の配信
- 情報検索
- オンラインゲームや賭博
- 商取引・売買（ネットショップ、ネットオークション）
- 銀行業務
- 各種情報処理システム
- 工場内制御システム　　などなど

現代の社会インフラとしてなくてはならないものになった



インターネットの仕組みをご存知ですか？

伝えたい情報を隣の人にどんどん手渡していく仕組み

郵便制度に似ている

郵便局員によるバケツリレー

ハガキで大事な情報は送りませんよね？

他にも問題は多々ある

帰属性問題

「攻撃者の特定」

ネット上の真犯人を見つけることが困難


信濃毎日新聞 統合 2013年（平成25年）2月

PC遠隔操作 30歳男逮捕

容疑者「身

遠隔操作ウイルスに感染したパソコン（PC）から犯行予告が送られた事件で、警視庁など4都府県警の合同捜査本部は9日、ネット掲示板に殺人予告を書き込んだとして、威力業務妨害の疑いで東京都江東区白河、IT関連会社社員片山祐輔容疑者（30）を逮捕した。「全く身に覚えがありません」と容疑を否認している。

【関連記事4・29面】

遠隔操作事件では4人が逮捕された。「真犯人」を名乗る人物は犯行声明や、回の逮捕容疑を含む計予告を書き込んだことを示していた。

片山容疑者は派遣先のPCから、勤務中に告を書き込んでいたれ、捜査本部はこの会宅捜索。同容疑者が一件に関与したとみて、

片山祐輔容疑者＝9日、都内で撮影

遠隔操作事件の構図

逮捕容疑者 片山祐輔容疑者

関与が疑われる事件

警察

遠隔操作

4人を誤認逮捕

男性4人

それぞれ犯行予告の書き込みやメール

インターネットの特性

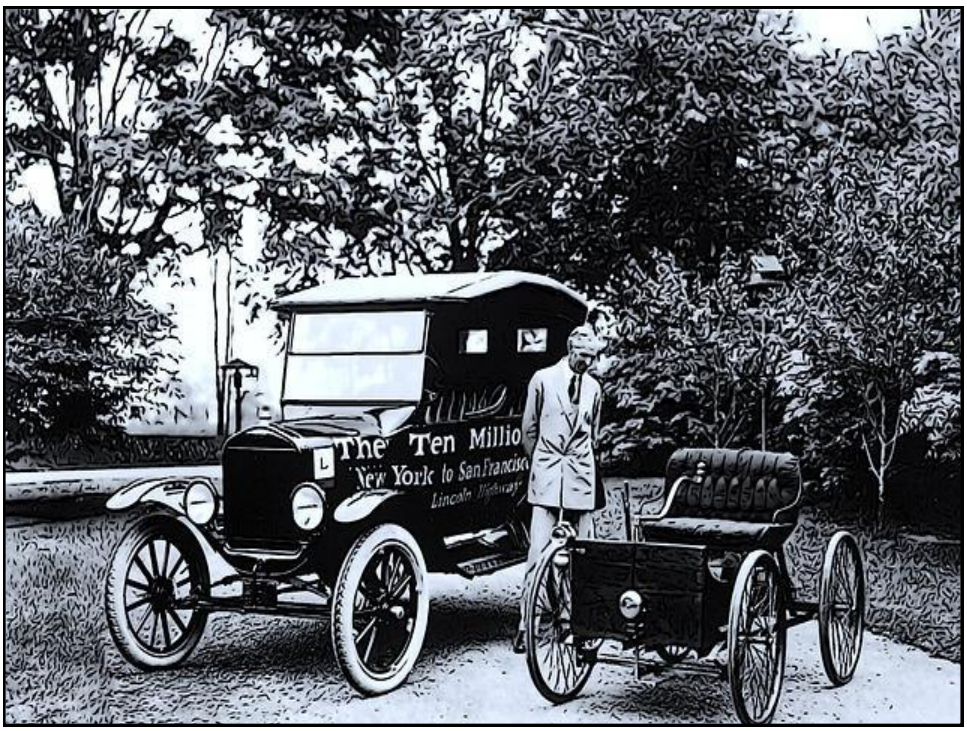
- DARPA が支援したプログラムだが、実際に構築したのは良い人達だった。
- 悪意を想定していない仕様のまま巨大化し、一般利用されるようになった。
  - 発信元が誰かを担保する仕組みが無く、成り済ましが容易。
  - 通信の秘密を保護するようにもなっていない。

- 厳密に管理された仕様が無く、日々変化している
  - 利用されるプロトコル等も（良くも悪くも）変わっていく

- 権威ある管理者がいない
- 国をまたがっているため法律が行き届かない

インターネットは想像以上に信頼できない

11



サイバー技術を取り巻く社会の現状

- あたかも自動車が発明された直後の世界
  - 道路交通法も免許制度も車検制度も無い
  - 信号機も横断歩道も無く
  - タコメーターもドライブレコーダーも無く
  - エアバッグもシートベルトも無い
  - 安全・安心を担保するための技術や法律、リテラシー教育などが備わってない

技術の進歩に社会が追い付いていない

13

サイバー空間は思っている以上に安全ではない

2.世界のサイバー攻撃事例

2007年
エストニア共和国政府機関等へ大規模かつ長期間にわたるサイバー攻撃が行われた

IT先進国であるエストニア

15歳以上のエストニア国民すべてが携行を義務づけられる電子IDカード。
身分証明書、運転免許証、健康保険証として機能するほか、納税、会社登記、処方箋発行（医療）などもこのカード一枚で簡単に済ませることができる。
2002年に導入された。
また、エストニアは世界で初めてオンライン選挙を実施した国でもある。

写真はWIRED.jpより http://pc.nikkeibp.co.jp/article/news/20131025/1109886/?P=2

17

エストニアの国家規模

	エストニア	東京都	単純比率
面積	45,227平方キロメートル	2,194平方キロメートル	20対1
人口	1,364,000人	13,784,212人	1対10
人口密度	1km²当たり31人*	1km²当たり6,283人	1対200
名目GDP	234億ドル（2015年）	10,572億ドル（2015年）	1対45

*北海道でさえ1km²当たり約70人

エストニアに関してはエストニア大使館HPなどから
東京都についてはwikipediaより
基本的に2018年の情報を利用

2007年
エストニア共和国政府機関等へ大規模かつ長期間にわたるサイバー攻撃が行われた

- 大統領府等政府機関、銀行、新聞社のウエブサイトが停止
- 一時的には携帯電話網や救急ネットワークも被害を受けたという
- 攻撃は3週間にわたり続いた
- DDoS攻撃がその主たる手段として利用された

- 当時、このようなことになるとは予想されていなかった

10年も前に大規模な国家レベルのサイバー攻撃事件が

2008年
トルコで送油パイプライン謎の爆発

トルコのパイプラインが爆発炎上。終息まで3週間近く要した。
ロシアによるサイバー攻撃が疑われている。

サイバー攻撃で物理的な被害を与えることができる

http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

2008年
グルジアの政府機関等に対して大規模なサイバー攻撃

2008年8月、ロシアによるグルジアへの軍事作戦に連携し、グルジアの政府機関等に対して大規模なサイバー攻撃が行われた

大統領府、議会、外務省、国防省、メディアなどに重大な被害が発生
- DDoS攻撃
- ウエブサイトの書き換え
- スパムメール
- サイバー封鎖
- 攻撃を要請するスローガン（攻撃対象メアドの掲示）
- 攻撃のための具体的なスクリプトの配布*
- グルジア人ハッカーの連携妨害
- SNSを利用したデマの流布を行ったも

諸外国では、行政機関を狙ったサイバー攻撃がすでに発生

2009年
サイバー技術を利用したスパイ活動

2009年9月、ダライラマ事務所のPCに、サイバースパイソフトウエアが発見された
これは、後にGhostNetと呼ばれることになった

アジア等の政府・外交関係機関にも感染は広がっていた

盗聴盗撮機能を有するマルウエア

2010年
産業用制御システムを目標としたサイバー攻撃

- イラン核施設における、ウラン濃縮用の遠心分離機の回転数を下げて不良品のウランを生成させるもの
- イランの核開発を妨害することが目的と考えられる
- 背後に極めて高度なサイバー技術と、その実行を裏付けた組織的諜報能力の存在がある
- クローズしたシステムであったにもかかわらず被害が発生した

スタクスネット事件

産業用制御システム3つの安心

- 狙われる筈がない
- 外と繋がっていない
- 個別独特のシステムなので強い

勘違いです

2010年
産業用制御システムを目標としたサイバー攻撃

- イラン核施設における、ウラン濃縮用の遠心分離機の回転数を下げて不良品のウランを生成させるもの
- イランの核開発を妨害することが目的と考えられる
- 背後に極めて高度なサイバー技術と、その実行を裏付けた組織的諜報能力の存在がある
- クローズしたシステムであったにもかかわらず被害が発生した

クローズしているシステムは安全であるというのは神話にすぎないことを証明した

真に危ないのは人間かもしれない

クローズしたシステムは安心だろうか？

- 外と繋がっていないから大丈夫。それ自体が油断である
- コストを抑える対象としてまずクローズしたシステムが対象となりやすい

- パッチは適時に適用されているか？
- OSは最新のものにバージョンアップしてるだろうか？
- 適切な監視・防護システムの導入は？

内部犯行者や部内協力者がいたらアウト

2012年
サウジアラビアのサウジアラムコのコンピューター3万台以上に被害

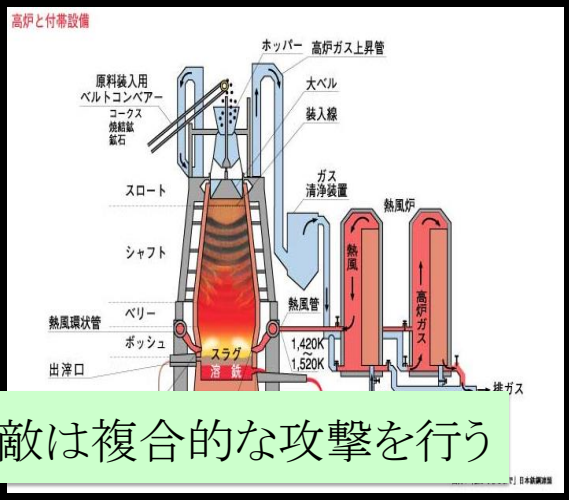
〇WindowsNT上で動き、発症すると感染先のファイル情報を攻撃者に送信
〇その後、それらのファイルを消してしまう
〇さらに、システムのマスターブートレコードを上書し、PCの起動を出来なくする

これだけ大量のPCが同時に停止

2014年製鉄所の溶鉱炉損傷 （ドイツ）

何者かが製鉄所の制御システムに侵入
システムの複数の組込装置に障害を発生させ、大規模な物理的損害を与えた

- PLC
- 警報システム
- 安全計装システム
- マンマシンインターフェイス
- 個々の制御システム
  （負荷測定・負荷分散・エネルギーバランス・その他諸々のシステム）



悪意を持った敵は複合的な攻撃を行う

2015年2016年
変電所へのサイバー攻撃

社会インフラへの攻撃が懸念される

32

社会インフラを狙った攻撃

- テロリストや他国家からなされるサイバー攻撃には、大規模停電のような国民の生命や財産を脅かす明確な意図を持って行われるものがある。

近年、社会インフラを標的として物理的なダメージを与えるサイバー攻撃のリスクが増大している

2017年 フェイクニュースについて

情報操作ということが、日常的に行われる時代になった

- 正しい決定は、正しい情報に基づき、正しく考察して、得られるものだ。
- サイバー攻撃の一つであるフェイクニュースの流布などで、誤った情報を拡散し、かつ、人々の感情に訴え、皆の判断を誤らせることができるとすれば、恐ろしいことだ。

35

2017年
交通機関へのサイバー攻撃

スウェーデンの交通機関がDDoS攻撃を受け、運行不能に

攻撃の対象は拡大している

サイバー攻撃様相の変化

- これまでは、情報セキュリティにおける「機密性」の重要度が高かった
- つまり、情報の漏えいに備えていればよかった

- IoTやOTの時代となり、「機密性」以外の「可用性」や「完全性」へのリスクが増えてきている

- 攻撃はより多様化しており、備えるべき対象も増えている

3.日本におけるサイバー攻撃の趨勢

日本に対するサイバー攻撃の最近の動向

2015年6月（日本年金機構事件）以降
個人情報漏洩事件に関する報道が
メディアを賑わせ
日本の社会に警報が上がるようになった

攻撃は「個人情報狙い」中心であるように見える

実際は多種多様な攻撃が続いている

ビジネスメール詐欺、仮想通貨発掘、ランサムウエア、サプライチェーンリスクなど

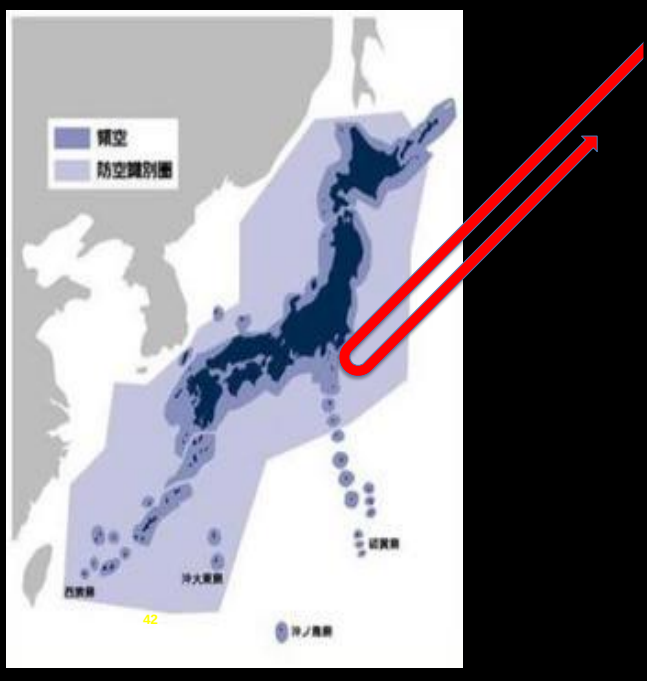
某大手旅行代理店案件について

- 報道ベースでは、個人情報漏洩事件として扱われた
- 時期的には、伊勢志摩サミットの直前である
- 同時期に、警察やセントレイア中部国際空港への攻撃もあった
- サミットへのサイバーテロの事前偵察であったという可能性もある

「個人情報漏洩」の攻撃ばかりが取りざたされているが、
サイバー攻撃はそればかりではないことに留意する必要がある

東京急行を知っていますか？

東京急行



東京急行の目的

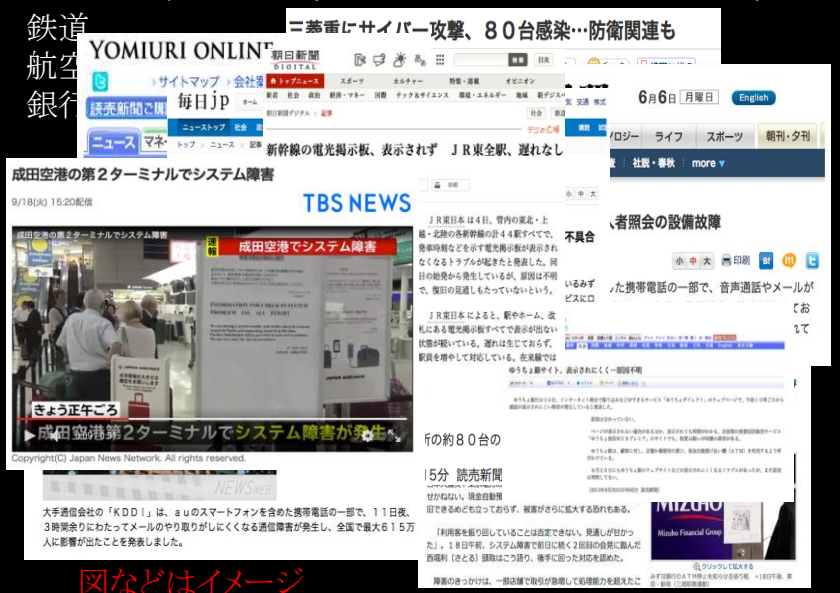
◎反応時間の測定から訓練レベルを推察
◎対応範囲
◎対応した機材／技術、諸元の調査

平和な時代に、相手の弱点を調べておくことは、
軍隊の基本的任務のひとつである。

43

多発する最近の原因不明のシステム事故

鉄道
航空
銀行



図などはイメージ

日本を取り巻くサイバー攻撃の現状

サイバー上の東京急行が
行われているのではないか？

45

引用：http://www.globalsecurity.org/wmd/world/russia/tu-16-pics.htm

サイバー攻撃には第4番目のものがある

1　いたずらや政治的自己主張

2　金銭目的の犯罪

3　技術資料等知的財産の窃取

4　将来の本格的攻撃に備えた情報収集活動

これまで単なる故障と考えていた事案も
今一度、見直す必要があるかもしれない

それにしては、日本では大規模なサイバー攻撃が起こっていないではないか？

- 日本のシステムの品質が高いから？
- 製品に独自仕様のものが多いから？

日本語の壁

オリパラのように、そもそも日本がターゲットの場合は日本で世界初のサイバー攻撃が起こる可能性もある

4. 終わりに

組織におけるリーダーの役割

何か起こったら

- 慌てない
- 状況を把握する
- 焦点を絞り、なすべきことをせよ
- 即刻、行動せよ。サイバー攻撃は早い
- 上下左右斜め上と会話せよ
- 全員が協力してことに当たる
- 部下を信じ任せることは任せる
- 希望を失わない

訓練していないことはなかなかできない

組織に於けるセキュリティのヒント

家の塀と同じで、高い塀を巡らせても一番低い所や弱い所から泥棒に入られる。
つまり一番弱い部分が全体の強さを決める。
→技術と運用を統括した一元的なセキュリティ対策が必要。

また、いくらセキュリティに投資しても、正面玄関から入られたら何にもならない。
この危険は、ID とパスワードの管理。
標的型攻撃そして内部犯行である。
→人間対策

これらを行うのがリーダーの役目である

リーダーは

- 一般の人と同じ感覚ではだめ
- 特にリーダーシップが重要
- 幅広く、攻撃者の可能行動まで踏み込んだ対策を考える・考えさせる
- 守れない規則を作ってはならない
- やってはいけないではなく、やったらこうなるを教えるように指導
- 日々の勉強を怠らないこと
- 専門家の協力を得る

専門家である必要はないが、
話を聞いて理解できるだけの素養を身につけましょう。

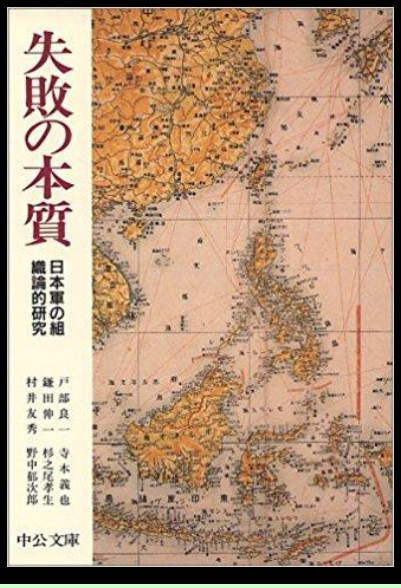
まとめ

- インターネットは想像以上に脆弱
- 世界では10年も前から大規模なサイバー攻撃事件が発生している
- 日本はサイバー上の偵察も受けている
- 2020を控え、もはや他人事ではない
- これまで以上に危機感を持つ必要がある
- 幅広く柔軟に考えることと先手を打つ取り組みが重要
- それはリーダーの仕事である

みなさん自らが、当事者意識を持ち、解決に向けてできることを実行しなければならない

ご興味があれば

平時において、不確実性が相対的に低く安定した状況のもとでは、日本軍の組織はほぼ有効に機能していた、とみなされよう。しかし、問題は危機においてどうであったか、ということである。危機、すなわち不確実性が高く不安定かつ流動的な状況――それは軍隊が本来の任務を果たすべき状況であった――で日本軍は、大東亜戦争のいくつかの作戦失敗に見られるように、有効に機能しえずさまざまな組織的欠陥を露呈した。



いつの日にか私が「サイバー事案　失敗の本質」という本を書く日が来ませんように。