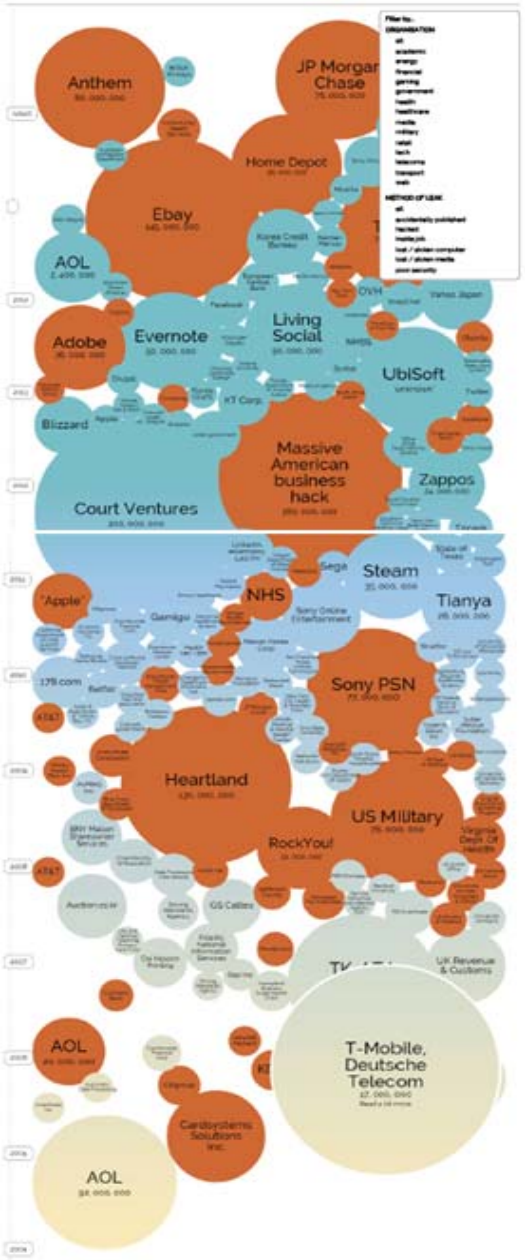
最新探偵小説：サイバー犯罪特別捜査本部！

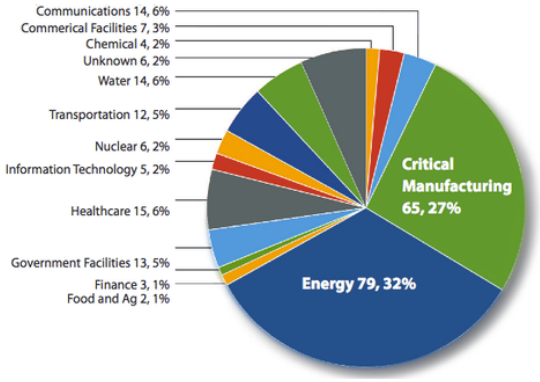
-„Industrie 4.0 made in Germany“の展開する中で-

Industrie 4.0(英:Industry 4.0) は、2011 年のハノーヴァーメッセで、初めて公表されて以来、ドイツ連邦政府が現在最も力を入れ推進しているハイテック戦略。情報工学を産業に組み込み、エルゴノミィも考慮しつつ、資源・素材を効率的に利用、生産・販売・エンドユーザーまでの各プロセスの最適化を目指している。2012 年には、Siegfried Dais (ジークフリート・ダイス Robert Bosch GmbH) を中心に具体的プロモーション委員会を設立。Industrie 4.0 への意気込みは、さらに Henning Kagermann (ヘニング・カゲルマン SAP AG)らへと継承されている。„Cyber-physical System “と „Internet of Things“が、2 つが基盤コンセプトとなっている。2013 年 4 月 14 日には、具体的に Bitkom （Federal Association for Information Technology, Telecommunications and New Media） 、VDMA （Verband Deutscher Maschinen- und Anlagenbau, German Engineering Association） 及び ZVEI（Verband Deutscher Maschinen- und Anlagenbau e.V） が、各詳細テーマに分科会、ワークショッププラットフォームをセット。Industrie 4.0 made in Germany をロゴにし、グローバル化した現在、ドイツが国際経済のイニシアティヴをとるかたちで、新しい産業形態が展開している。デジタル化された情報をソフトウェアープログラミングにのせ、精巧なセンサーで作動するロボットが主役の生産ラインで走らせ、素材とエネルギーの浪費を最小限に抑え、最終製品をエンドユーザーまで届ける。また、一般市民は、IT 機器に組み込まれた Smart Card IC を利用し、時間の無駄なく快適に生活することが、ターゲット。VW、Daimler、BMW 等の自動車メーカー、SIEMENS、KUKA、Bosch 等のグローバルプレイヤー、ドイツの産業をしっかりと支えている各産業界のキー・ノウハウを持つ中堅企業、また、斬新なソフト/ハードウェアーを開発中のベンチャー企業にいたるまで、どのオフィースに立ち寄っても Industrie 4.0, Made in Germany のロゴが、掲げられている。また、ハノーヴァーメッセー2015（13-17.04.2015）では、Industrie 4.0, Made in Germany は、メインテーマとして、多くの来場者の関心の的になった。

しかし、ここで、留意しなければならないことは、複雑にリンクする情報網（下図）に、まったく予期しないサイバー犯罪（Cyber-Criminal）が潜んでいる点である。



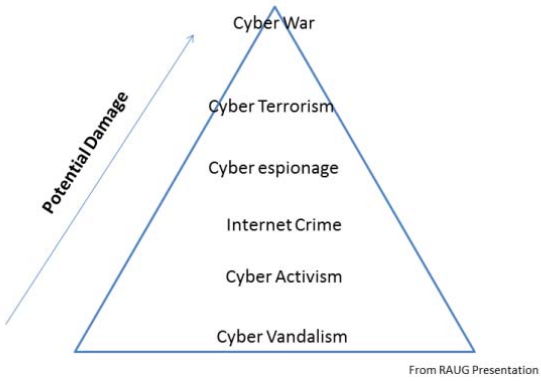
前代未聞の大量の情報を背景とする、予期ぜすと不意に、かつ、無差別大量の人々に被害が出てきている、



サイバー犯罪の件数 ICS-CERT の 2014 年レポート

ICS-CERT のレポートによると、すでに、技術革新を担う重要な企業の最新情報、エネルギー供給源中枢、各政府機関の機密情報、金融その他取引等で、被害が急増している。一個人のプライバシーにはじまり、国家間の戦争さえ起こす潜在性がある凶悪犯罪のリスクが忍び寄ってきている。知能犯のハッカー、また、非常に単純に、プロセスのサボタージュや、電源を切ってしまうことで、デジタル化した社会が、一気に大混乱に陥ってしまう。

長い人類の歴史を見ると、情報は、時間と空間を潜り抜け、人々の好奇心をくすぐりつつ運命的な役割を果たしてきている。デジタル化される以前の情報は、魅力的、妖艶でさえあった。その情報が、現在、情報機器の発達により、キーボタン一押し、マウスのクリックで、時間を超越し、一瞬のうちに、世の中に甚大な影響を及ぼすリスクを持った「思考の弾力性ある凶器*」にさえ変貌してきている。*:ハッカーとサイバー犯罪捜査官は、紙一重といえる。



Year	Accident		対策/Counter measure
2001/2002	Nimda / Code Red	Nimda（ニムダ）は、2001年9月に識別されたワームの一種である。ファイルに感染するコンピュータウイルスでもある。素早く拡散し、Code Red と同様の経済的損害を発生させた。	Better Anti-Mal Ware
2004	APT 1	Chinese Cyber Espionage	Defence in Depth
2008	APT 2	Chinese Cyber Espionage	More Intelligence
2008	Buck Shot Yankee	ウイルスに汚染されたUSB Stickにより、米国防衛庁の情報網がダウン。Pentagonは、14ヶ月かけて、Cleaning作業を行わなければならなかった。	Protect Operational Environment
2009	WiKi Leaks	ウィキリークス (WikiLeaks) は、匿名により政府、企業、宗教などに関する機密情報を公開するウェブサイトの一つ。創始者はジュリアン・アサンジ。投稿者の匿名性を維持し、機密情報から投稿者が特定されないようにする努力がなされている。2006年12月に準備が開始され、それから一年以内に120万を超える機密文書をデータベース化している	Insider Thread
2014	Sony 北朝鮮からのサイバーアタック？	ソニーの100%子会社である映画大手の米Sony Pictures Entertainmentは2014年11月に大規模なサイバー攻撃を受けた。	捜査続行、日本政府の対応は遅い

2000 年代に入ってからの Cyber Problem
左下・上図 Intel プレゼン資料から抽出　by Setsuko Schwarzer

ハノーヴァーメッセ 2015 に先立って、3 月 25 日および 26 日、ミュンヘンの防衛大学フォーラム：Cyber Defence: “CODE“が、開催された。

ミュンヘンの防衛大学フォーラム：Cyber Defence: “CODE“

第 1 日目は、防衛大学情報工学研究チームの Prof. Dr. Merith Niehuss（メリト・ニーフス）、バイエルン州議会議員 Markus Blume CSU,（マルコス・ブルーメ）、NATO CIS Group で CIS & Cyber Defence 担当の Thomas Franz（トーマス・フランツ少将）、スイス RUAG Schweiz AG 社の CEO Dr. Markus Zoller（マルコス・ツォラー）、McAfee の Part of Intel Security Director Security Architecture である Maurice

Cashman（モーリス・キャシュマン）、European Defence Agency„Information Superiority“の Michael Sieber（ミヒャエル・ジーバー）の各氏が、サイバー（ネット）犯罪の状況をそれぞれの立場からプレゼン。

2 日目は、民間企業 Infineon の Dr. Detlef Houdeau（デトレフ・オイデュー）、バイエルン州政府経産省サイバー関連専門チーム（Sachgebiet IE5 - Cybersicherheit, Bayer. Staatsministerium des Innern, für Bau und Verkehr）から Dr. Oliver Bär（オリバー・ベア）。そして、サイバーセキュリティー専門企業の IABG 社、Dr. Tobias Kiesling （トビアス・キースリング）らが、プレゼン。その後、下記 5 つのテーマのワークショップに分かれ、活発な現場からの声、討論が展開した。（筆者は、Workshop 2:“Industrie 4.0“に参加。）

Workshop 1:ドローン、ジャミング、スプーフィングの脅威
Workshop 2: „Industrie 4.0 “　産業スパイからいかに生産プロセスをまもるか
Workshop 3:予期しない IT 問題についての捜査とその分析
Workshop 4:セキュリティー保護法（案）
Workshop 5: „Big Data“

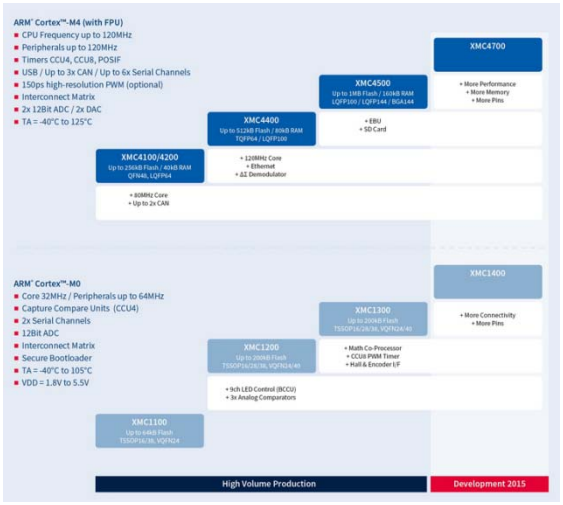
「Workshop 2: „Industrie 4.0 “産業スパイから、いかに生産プロセスを守るか」では、バイエルン州警察庁、特別サイバー犯罪捜査部専門官が、情報学を修得していれば、就職に困らず、サイバー犯罪捜査官として引く手あまた、とユーモアを交えて捜査に翻弄させられている日々をレポート。

毎年、50-100Mrd ユーロ（日本円換算 ca. 6,467,000,000,000- 12,935,000,000,000 円）相当の損害がでており、その傾向は、上昇気味。中国の情報セキュリティー分野の入札に応募したドイツの 2 社が、必死に応募資料を用意しつつも、驚いたことに突然入札キャンセル。結果としてすべて、応募要項に記述したドイツ側のセキュリティ・ノウハウを中国側にとられてしまった例やフランス･イタリアなど欧州内でも、企業機密漏えいがあるとの具体例が、忌憚なく語られた。そして、非常に興味深いことは、サイバーアタック増加の原因：

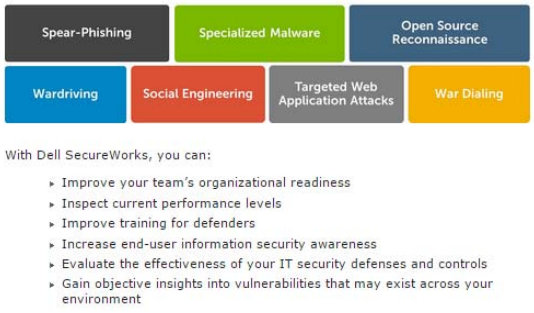
① IT 機器、プログラムの使い方を理解していないために起きる、悪意のない誤作動
② 所属企業へのロイヤリティー欠如（雇用コスト節約のため終身雇用でなく委託契約が増加）によるサボタージュ
③ 本格的な企業スパイ

一般 IT 企業は、このような急激な社会変化の中、①Protection、②Validation（シミュレーションやトレーニング）、③Cyber Security Product として、Trafic Monitoring, Energy Power Station　Management support 等のインテリジェンス・デザイン・サポートをビジネスとしてオファーし始めている。

INFINEON　IC　センサーを下記のコンセプトでオファー



DELL・Intel のコンサルティング・ソリューション



一般に、犯罪が起こると、すぐにその対策に、莫大な投資をしようとするが、中小企業には、その余裕がない。人件費節約の一方で、今度は機密保持に出費しなくてはいけないという、非常に皮肉な現状となってきている。

また、非常にショックなことは、サイバーアタック過程をみると、手元にあるラップトップ、スマートフォーンなどで、意外に簡単に Nato などの軍事機関、公共の報道機関の Domain にアプローチでる。防衛予算などと比較すると、驚くほど安く簡単にできるサイバーアタックへの防止策が、緊急課題になってきている。

NATO の対処現状　国家レベルの法律での取り締まり等の準備は、緊急に必要。武力行使をするなどの古典的な防衛のあり方が、現在知能犯罪対策へと変わってきている

いわゆる Big Data の分析・活用・Smart Data の責任について、私たちは、様々な角度から、現状を真剣に捉えてゆかなければならない。洗練された情報交換の場を作り、サイバーセキュリティーの専門家を中心に、技術革新分野の開発研究・軍備・経済・産業・行政等幅広い分野にわたる協力が必須である。

ラップトップ等のパスワード管理、IT 機器盗難防止にはじまり、パテント・ノウハウ等の信頼に基づくネットワーク上での管理と、情報技術の新たなチャレンジ期に突入したといえる。

（23.04.2015　文･写真 Setsuko Schwarzer）

（参考引用資料）

http://de.wikipedia.org/wiki/Industrie_4.0

http://blog.norsecorp.com/2015/03/13/industrial-control-systems-attacked-245-times-in-2014/

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

http://www.infineon.com/dgdl/Infineon-TLE4966V-1K-DS-v01_00-EN.pdf?fileId=5546d4624b0b249c014b9c86b9394d76

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

http://itpro.nikkeibp.co.jp/atcl/column/14/346926/011500145/

http://www.secureworks.com/consulting/security_testing_and_assessments/red-team-testing/#

http://www.infineon.com/export/sites/default/media/products/Microcontrollers/XMC-MCU-Portfolio-Overview-and-Roadmap.jpg