# 社会を動かすモノのセキュリティに向き合おう

## 産業用制御システムを襲う
## サイバー攻撃の実態・最新動向

佐々木 弘志

情報処理推進機構産業サイバーセキュリティセンター サイバー技術研究室
専門委員

IPA Better Life with IT

# 2017年5月 ランサムウェアWannaCry

2017/5/12（金）頃から世界各地でランサムウェアに感染する被害が発生。
3月にパッチリリースした「MS17-10」によって修正されたSMB v1の脆弱性「CVE-2017-0145」を利用し感染を広げる。Port445/tcpを攻撃。
**ランダムなIPに対して感染拡大活動実施**
**⇒メール開かなくても感染する！**

WannaCry感染に使用される脆弱性を突く通信の記録（Symantec）

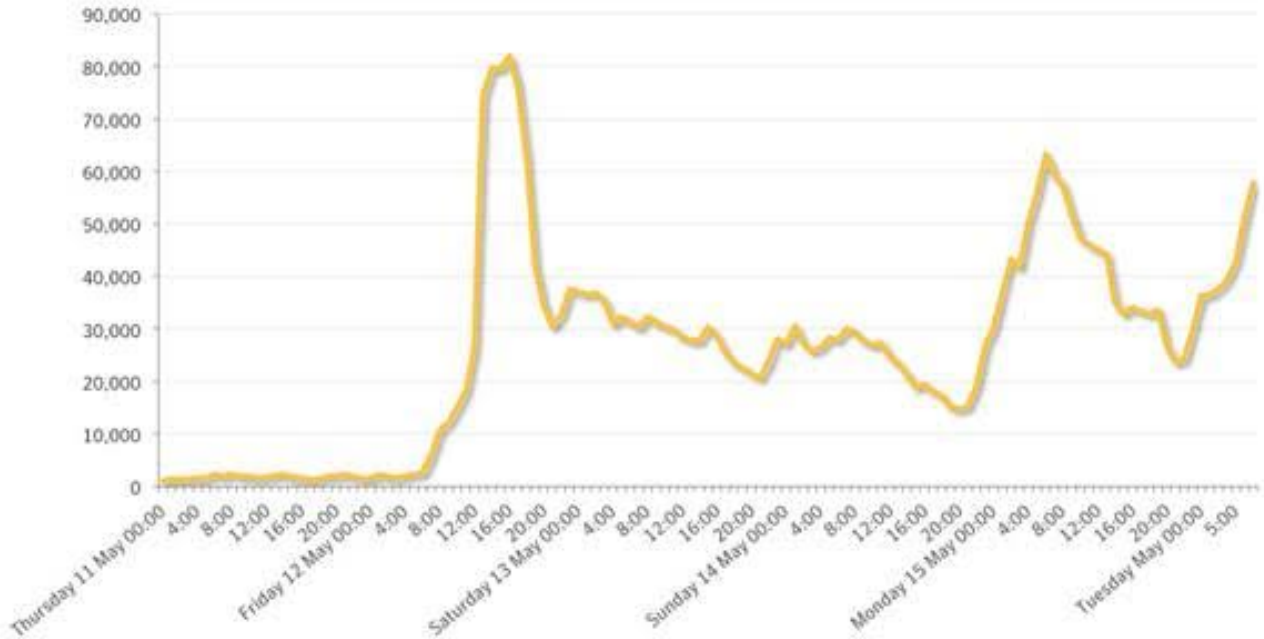
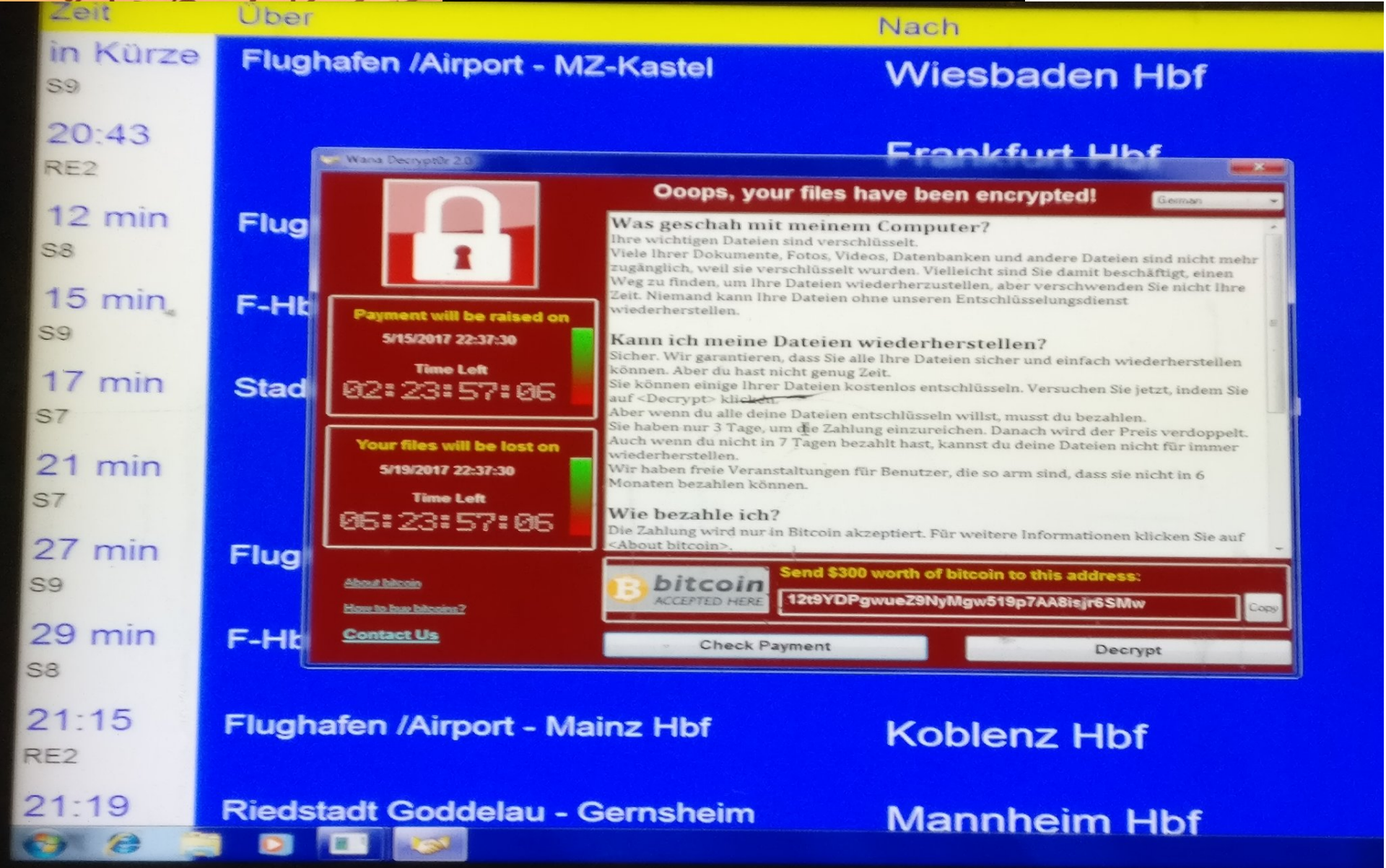
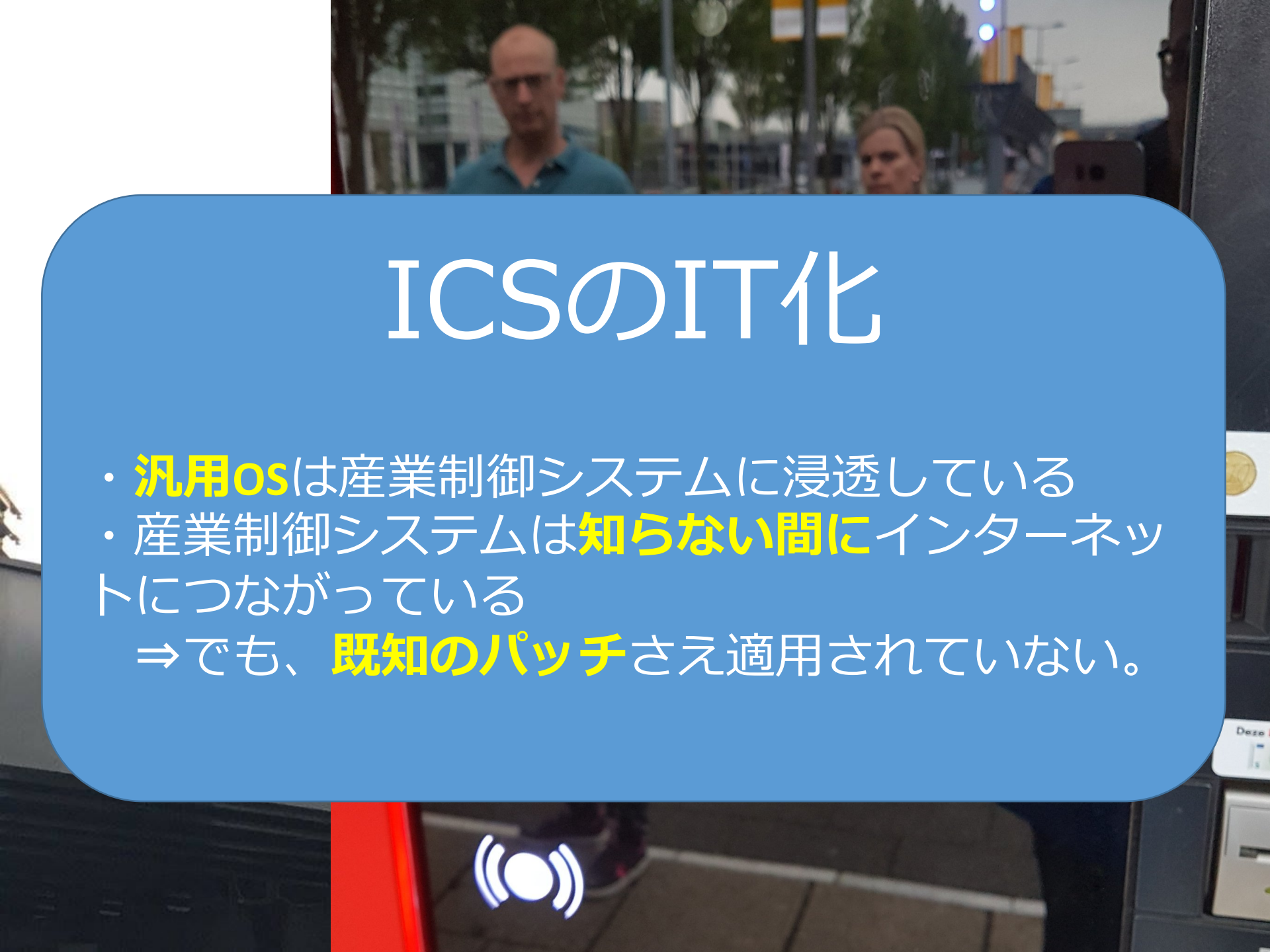



*Figure 1. Number of exploit attempts blocked by Symantec of Windows vulnerability used by WannaCry per hour*


Zeit
Über
Nach
in Kürze
S9
Flughafen /Airport - MZ-Kastel
Wiesbaden Hbf
20:43
RE2
Frankfurt Hbf
12 min
S8
Flug
15 min
S9
F-Hb
17 min
S7
Stad
21 min
S7
27 min
S9
Flug
29 min
S8
F-Hb
21:15
RE2
Flughafen /Airport - Mainz Hbf
Koblenz Hbf
21:19
Riedstadt Goddelau - Gernsheim
Mannheim Hbf
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
German
Was geschah mit meinem Computer?
Ihre wichtigen Dateien sind verschlüsselt.
Viele Ihrer Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwenden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseren Entschlüsselungsdienst wiederherstellen.
Kann ich meine Dateien wiederherstellen?
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber du hast nicht genug Zeit.
Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf <Decrypt> klicken.
Aber wenn du alle deine Dateien entschlüsseln willst, musst du bezahlen.
Sie haben nur 3 Tage, um die Zahlung einzureichen. Danach wird der Preis verdoppelt.
Auch wenn du nicht in 7 Tagen bezahlt hast, kannst du deine Dateien nicht für immer wiederherstellen.
Wir haben freie Veranstaltungen für Benutzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.
Wie bezahle ich?
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf <About bitcoin>.
Payment will be raised on
5/15/2017 22:37:30
Time Left
02:23:57:06
Your files will be lost on
5/19/2017 22:37:30
Time Left
06:23:57:06
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt



# ICSのIT化

・**汎用os**は産業制御システムに浸透している
・産業制御システムは**知らない間に**インターネットにつながっている
　⇒でも、**既知のパッチ**さえ適用されていない。

# インターネット経由で産業制御システムが操作されて停電発生（2015年）

ウクライナ西部：3社の電力会社地域
コントロールセンター

攻撃者

操作用端末にリモート接続を行い、変電所を落とすブレーカーをOFFする操作を実施。

事前に対象の情報システムに侵入し、コントロールセンターへのリモート接続情報を窃取


停電発生。
変電所：100kV 7か所
35kV 23か所
225,000顧客が影響。

オペレータが撮影したとされる動画
https://wired.jp/2017/07/27/video-hackers-take-over-power-grid-computer/

# 自己紹介

佐々木　弘志

情報処理推進機構産業サイバーセキュリティセンター
サイバー技術研究室 専門委員

**CIP/IoTセキュリティの文化醸成をミッションとしている**

・産業制御システム開発者（14年）
・マカフィー株式会社
　産業制御システムセキュリティのコンサルタント（6年~）
※2016年より、経済産業省の非常勤アドバイザー
（情報セキュリティ対策専門官）として活動。講演、執筆多数。

主な実績
・**独立行政法人 情報処理推進機構(IPA) 産業サイバーセキュリティセンター**
　**- サイバー技術研究室専門委員 および 事業者向けカリキュラムの講師担当（2017）**
・内閣サイバーセキュリティセンター「EU諸国及び米国における情報共有体制」（2016）
・経済産業省　電力業界セキュリティ政策に関するヒアリング調査（米国・欧州）
　- 平成27年度電気施設保安制度等検討調査(電気設備技術基準国際化調査）（2014）
　- 平成26年度電気施設技術基準国際化調査(電気設備）（2015）
・名古屋工業大学　制御系セキュリティワークショップ共催（2015-2016）

# アジェンダ

**Key Message :**
**産業制御システムセキュリティは、ネットワーク技術者・事業者にとって**
**ひとごとではない！ビジネスチャンスである。**

- 産業制御システムを襲うサイバー攻撃の実態
- IoT時代の産業制御システムセキュリティの考え方
- ビジネスを支える産業制御システムセキュリティ

Industrial Control System (ICS) : 産業制御システム

# 産業制御システムを襲う
# サイバー攻撃の実態

# なぜ産業システムセキュリティが重要なのか？

**産業制御システム（ICS*）のIT化が進むにつれて攻撃されやすくなってきた。**

## 産業制御システムのオープン化

- 制御システム間の通信インタフェースのイーサネット化
- 制御システムの汎用OS化（Windows Embedded, Linuxなどの利用）

## 産業制御システムを狙った攻撃の発生・進化

- 2010年 Stuxnetの登場　イランの核施設を破壊。クローズ環境だったがUSBメモリ経由で感染
  SIEMENS社製のPLCプログラミングソフトStep7/Win CCがハッキングされた
- 2014年 Operation Dragonfly　欧州の電力会社数社の制御システム管理サーバー情報が漏えい
- 2015年 ウクライナ西部　サイバー攻撃により停電（SCADAシステムに侵入）
- 2016年 ウクライナキエフ　サイバー攻撃により停電（時限式、モジュール化）
- 2017年 TRISIS-TRITON-Hatman 安全計装システムを攻撃

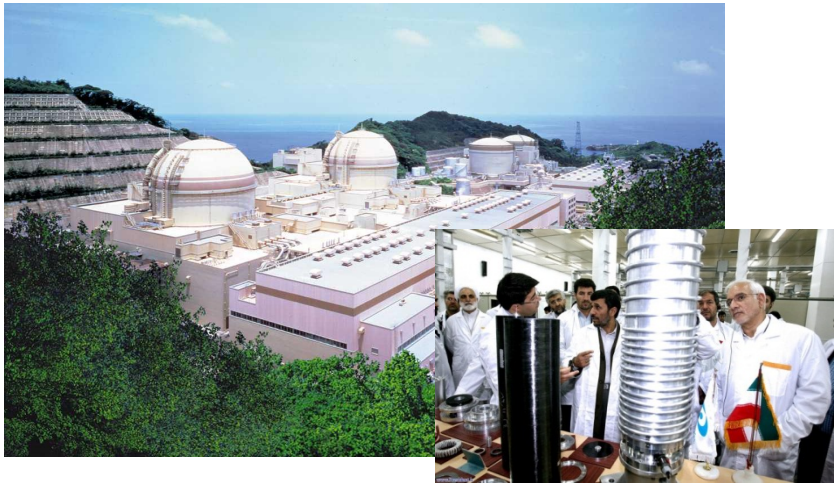
## 世界中で**規制・ガイドライン強化**の動きが進行中

- 制御システムセキュリティ標準の制定（国際：IEC62443　業界：NERC CIP, NIST IR 7628）
- 国家レベルの取り組み（米国：NIST Cybersecurity Framework　EU：NIS Directive）

*OT（Operational Technology）という言葉も多用される

# 制御システムを狙ったサイバー攻撃(2010/07)～Stuxnet～

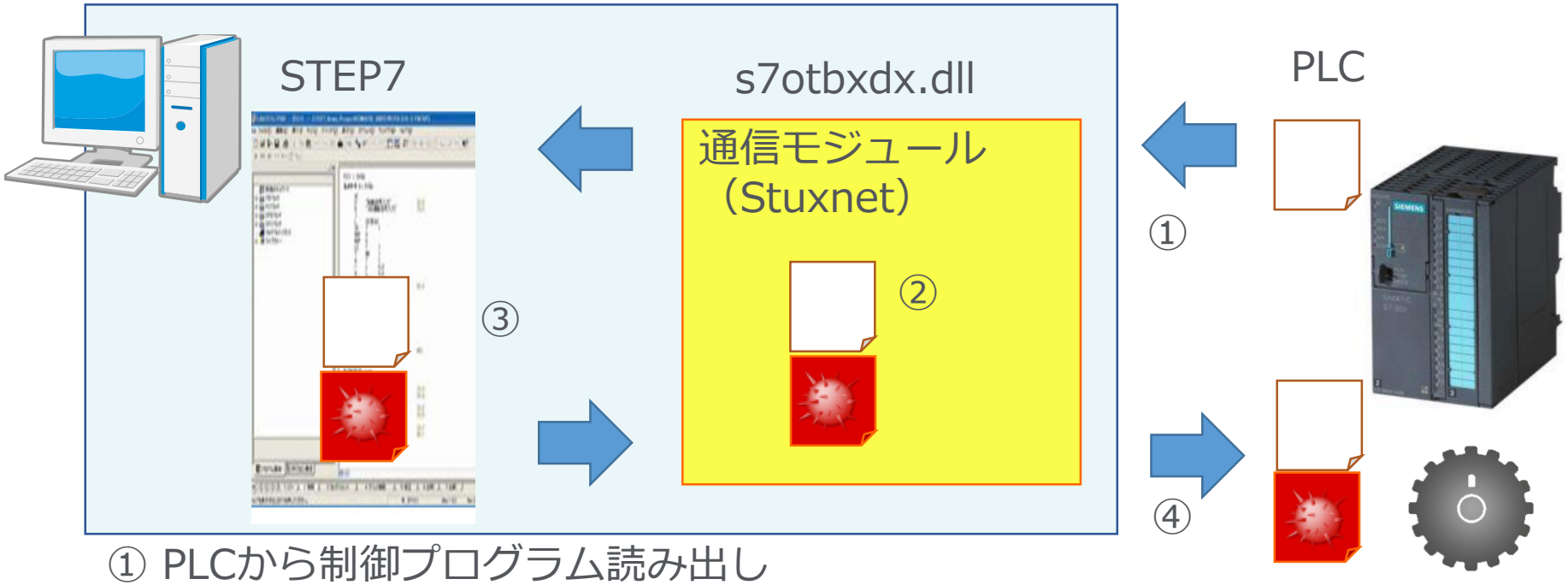
- **2010年7月に発見**
- **イランの核関連施設を狙ったサイバー攻撃**
- **核施設の遠心分離機のモーターが誤動作**



- **USBメモリ経由で施設内のパソコンに感染**
- **産業用制御システムが攻撃対象に**
- **5件の脆弱性（4件は未知の脆弱性）を悪用した高度な攻撃**
- **あまりにも複雑で高度な攻撃のため長らくその目的が不明だった**

米政府はイランによる核兵器開発の進展を遅らせる目的で**ブッシュ政権時代**にコードネーム「Olympic Games」と呼ばれる計画に着手。この計画は**オバマ政権に引き継がれ**オバマ大統領が就任後間もなく、**イランの核開発施設運用に使われているコンピュータに対する攻撃を命じた** The New York Times

# Stuxnet 攻撃のメカニズム

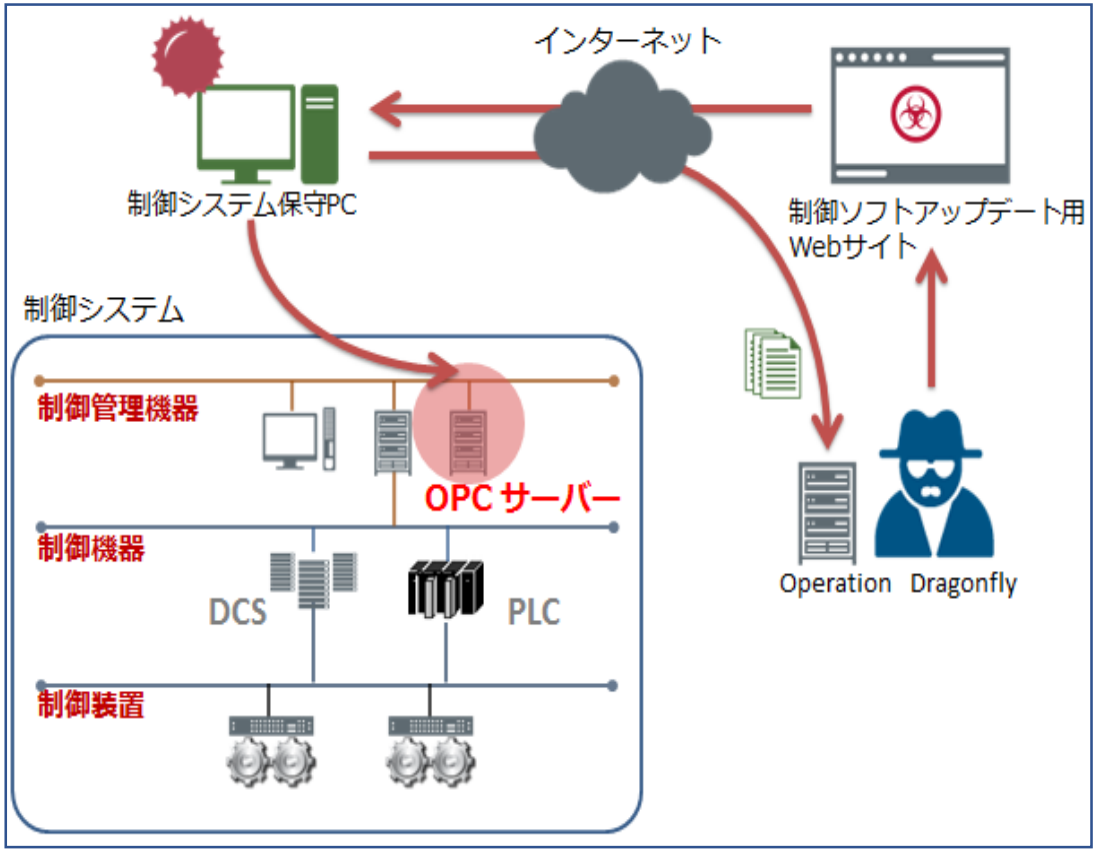



① PLCから制御プログラム読み出し
② 通信モジュールで不正コードを追加
③ 不正なラダープログラム読み出し
④ PLCへ制御プログラムを書込み（感染）

**ラダープログラミングソフト（STEP 7）をハッキング**
**PLCの制御プログラムに不正なコードを追加**

# 制御システムを狙ったサイバー攻撃(2014/06)
# ～Operation Dragonfly～

- 2013年2月より電力業界への攻撃を開始
- 制御システムベンダーのソフトのアップデートサイトをハッキング
- 制御システムベンダーのソフトのアップデータにマルウェアを同梱
- 欧州中心に電力会社数社が感染
- 感染PCのネットワーク内にあるOPCサーバーの情報を収集し外部へ送信



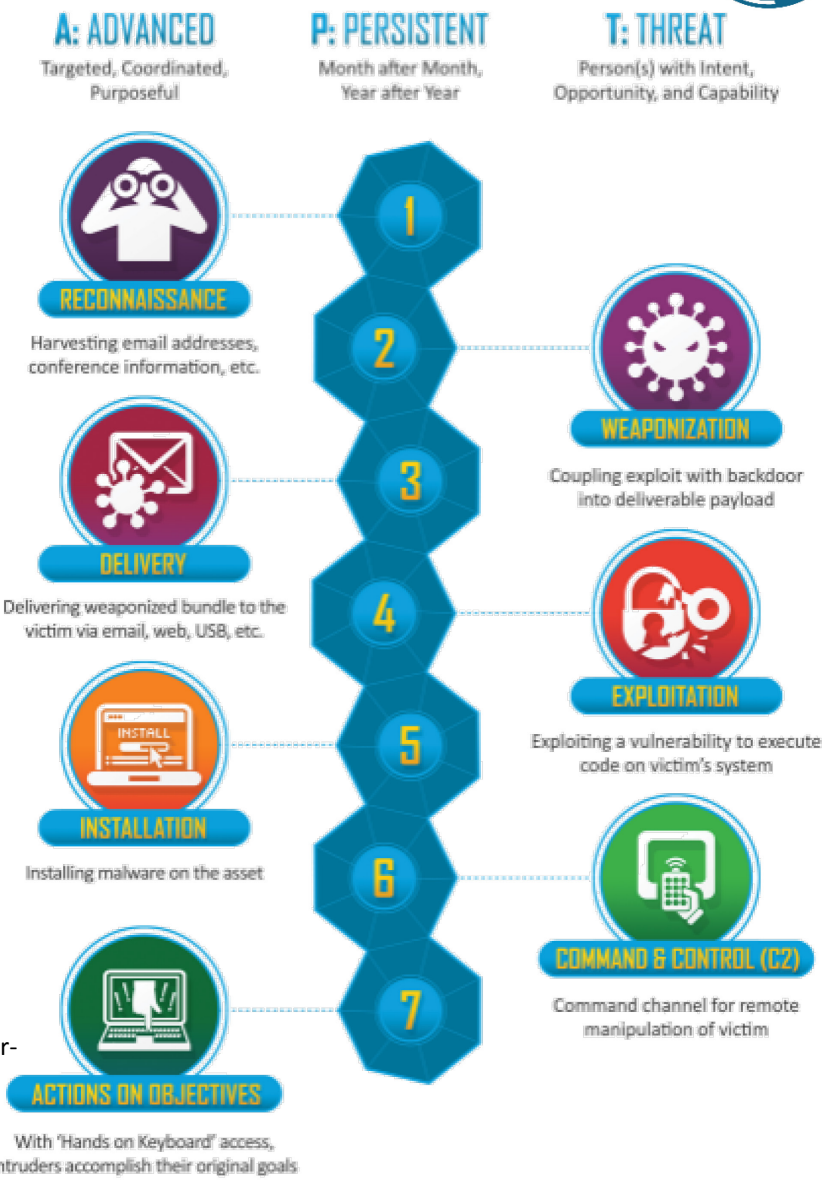

**制御システムのネットワークや運用を理解した攻撃**


12

# Cyber Kill Chain®とは？

Lockheed Martin 社が2009年に提唱した標的型攻撃の手法。
武力行使の手法になぞらえてモデル化しているのが特徴。

| 攻撃段階 | 意味 |
|---|---|
| Reconnaissance | 偵察活動 |
| Weaponization | 武器化 |
| Delivery | デリバリ |
| Exploitation | 脆弱性攻撃 |
| Installation | インストール |
| Command & Control | リモート操作 |
| Actions of Objectives | 目的実行 |




http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

# ICS Cyber Kill Chainとは？

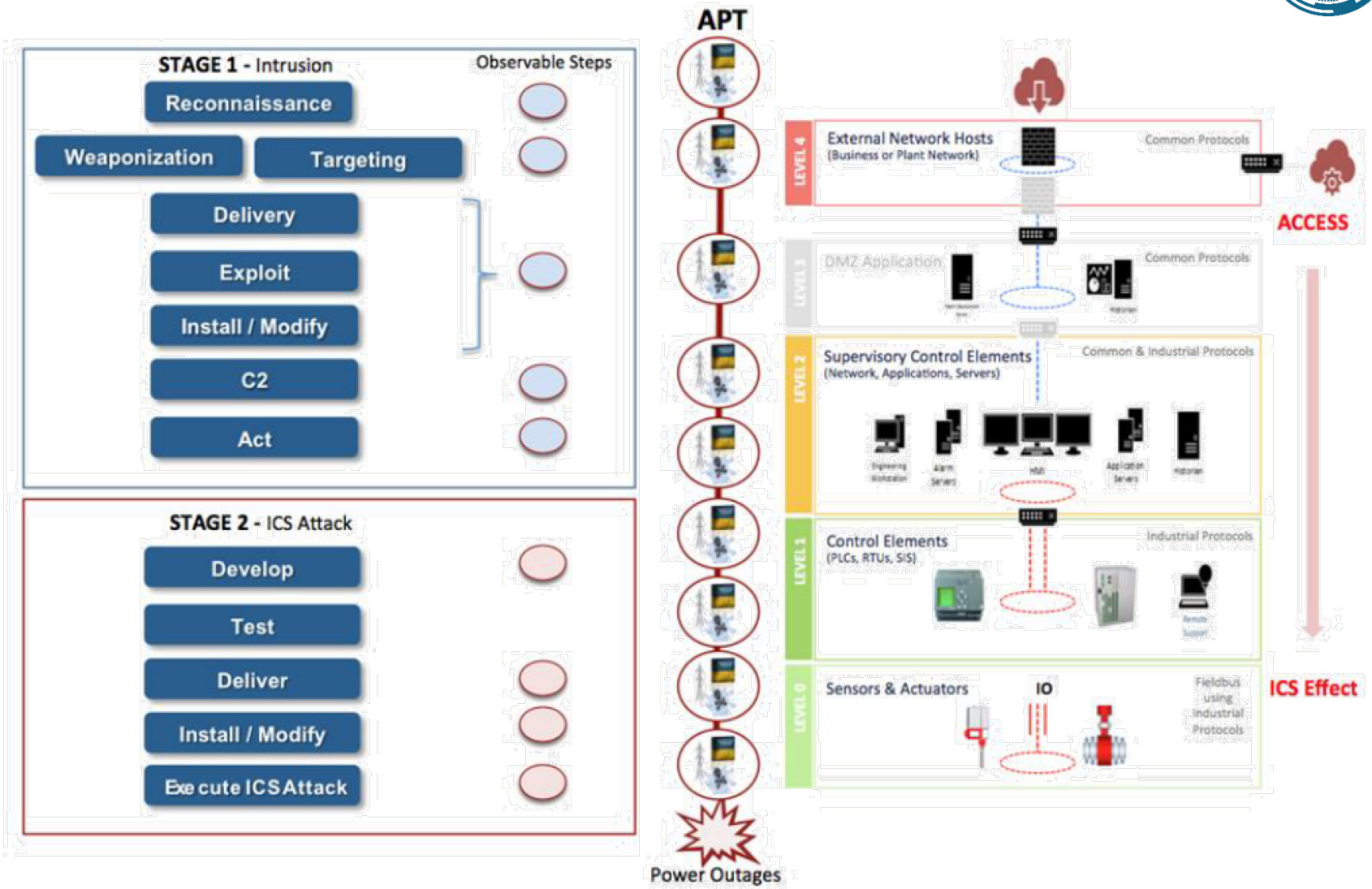


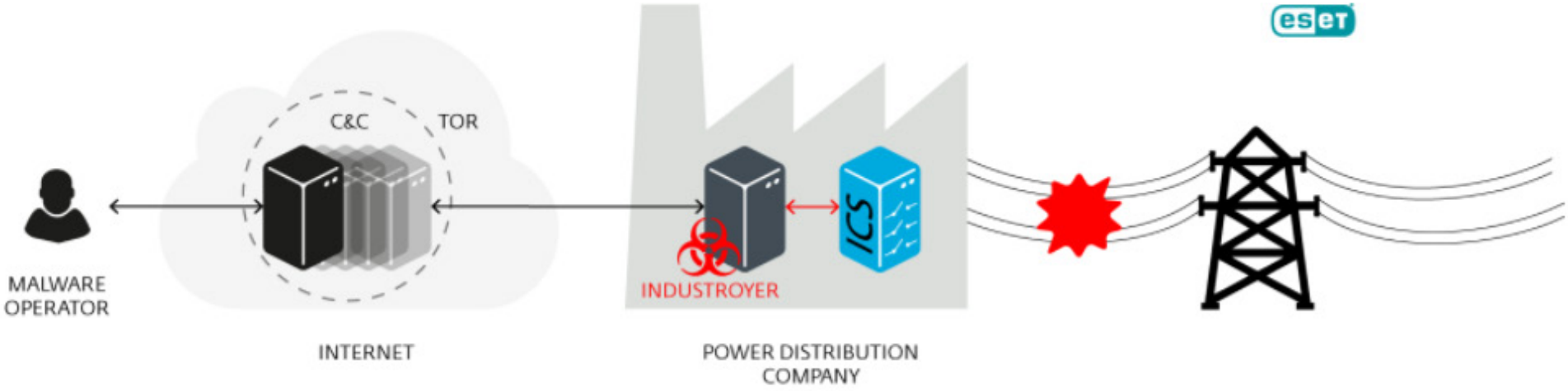

Figure 5: Ukraine Cyber Attack ICS Cyber Kill Chain and Purdue Model Mapping[21]

SANS, E-ISAC: Analysis of the CyberAttack on the Ukrainian Power Grid
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

# CrashOverride/Industroyerとは？

**Stuxnet 以来の最大の制御システムへの脅威**

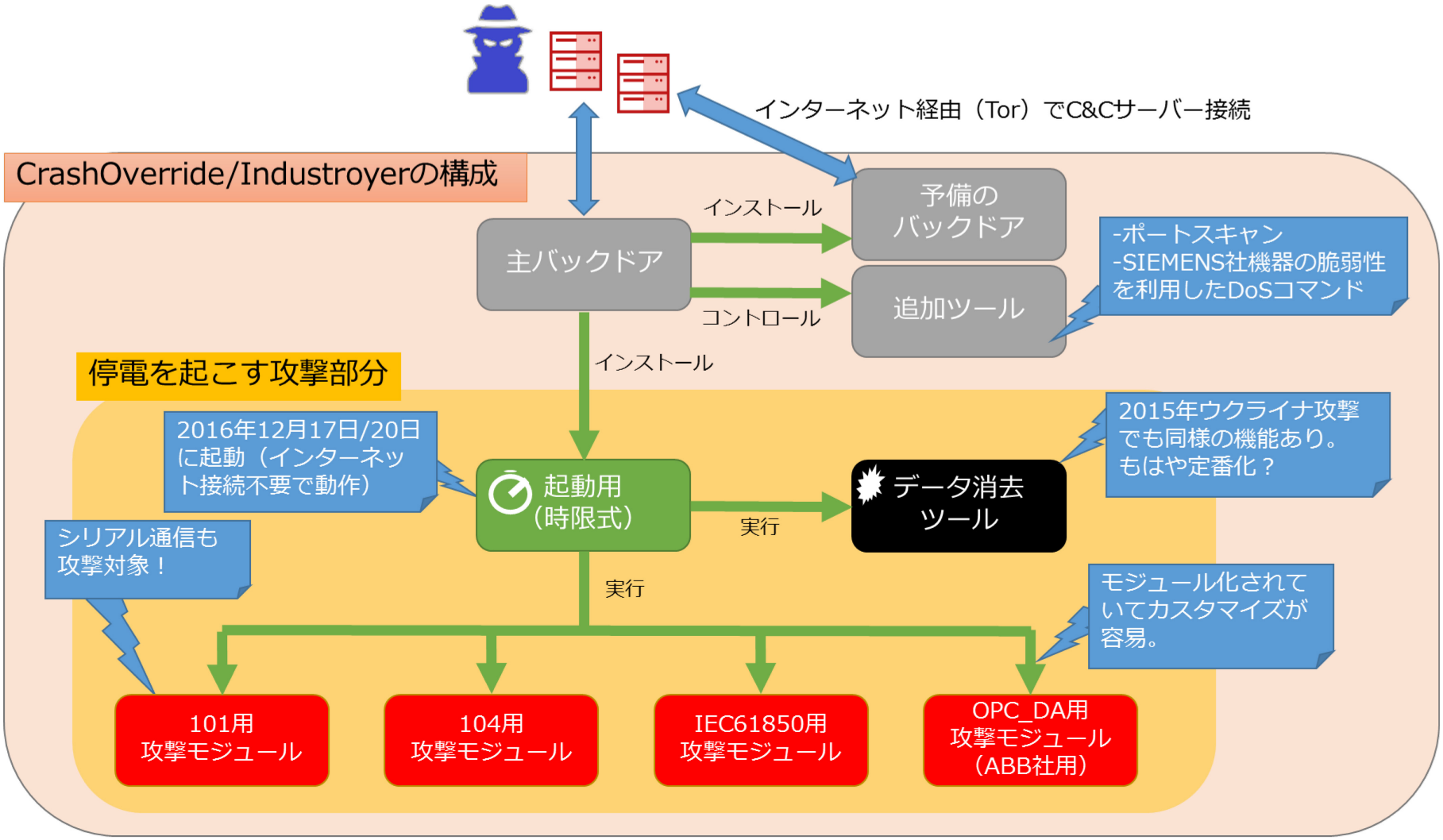
2016年12月ウクライナの首都キエフの電力会社がサイバー攻撃され、１時間の停電が発生した。攻撃に使われたとみられるマルウェアは「CrashOverride」または「Industroyer」 と命名され、解析レポートが出ている。




https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

# モジュール化/時限式実行

**モジュール化されたことにより標的毎のカスタマイズが容易**




https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

# CrashOverride/Industroyer 特徴

**変電所とコントロールセンター間の複数の制御プロトコルに対応**

複数の制御系プロトコルで、「変電所のスイッチ・ブレーカーを探して、それらを停電されるコマンドを送信する」という操作を実現している。

101

104

IEC61850

OPC DA

```
101_config.ini
1  real_process.exe
2  COM1
3  1---
4  COM2
5  2---
6  COM3
7  3---
8  2
9  10
10 15
11 20
12 25
```

Figure 6. An example of a 101 payload DLL configuration.

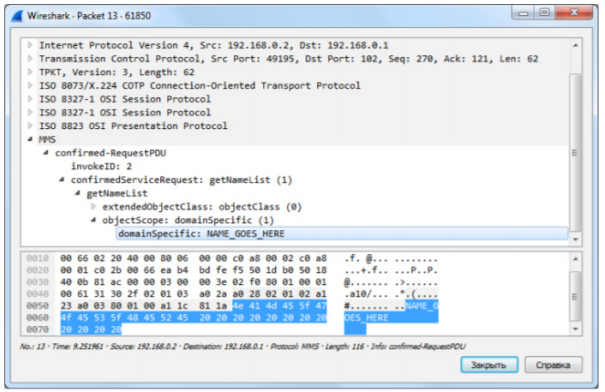



Figure 13. The dissected MMS `getNameList` request in Wireshark.

```
104.ini
1  [STATION]
2  target_ip = 192.168.0.1
3  target_port = 2404
4  logfile = logfile.txt
5  asdu = 1
6  stop_comm_service = 0
7  change = 1
8  first_action = on
9  silence = 0
10 uselog = 1
11 stop_comm_service_name = process01.exe
12 command_type = def
13 operation = range
14 range = 10-15,
```

Figure 8. An example of 104 payload DLL configuration.

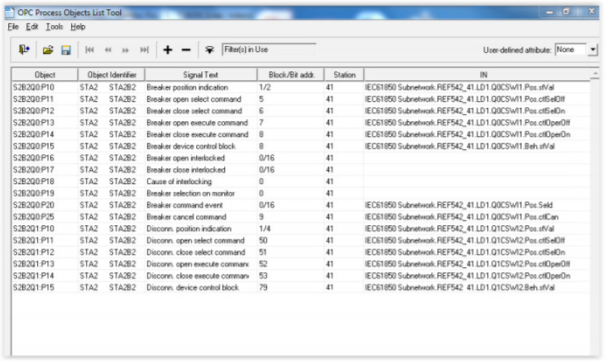



Figure 15. An example of OPC items names in IN field received using OPC Process Objects List Tool.

https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

# ICS Cyber Kill Chain Mapping

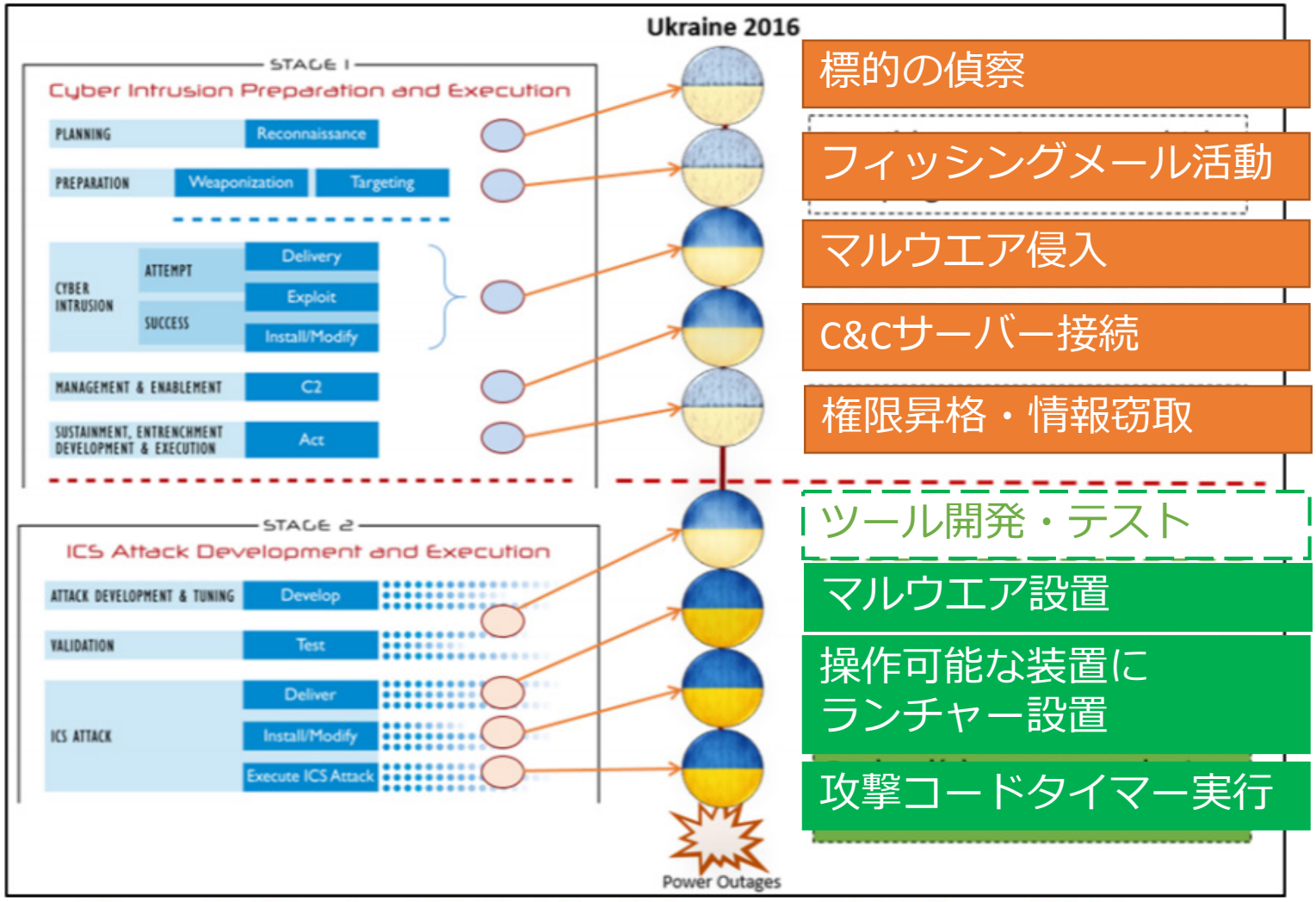
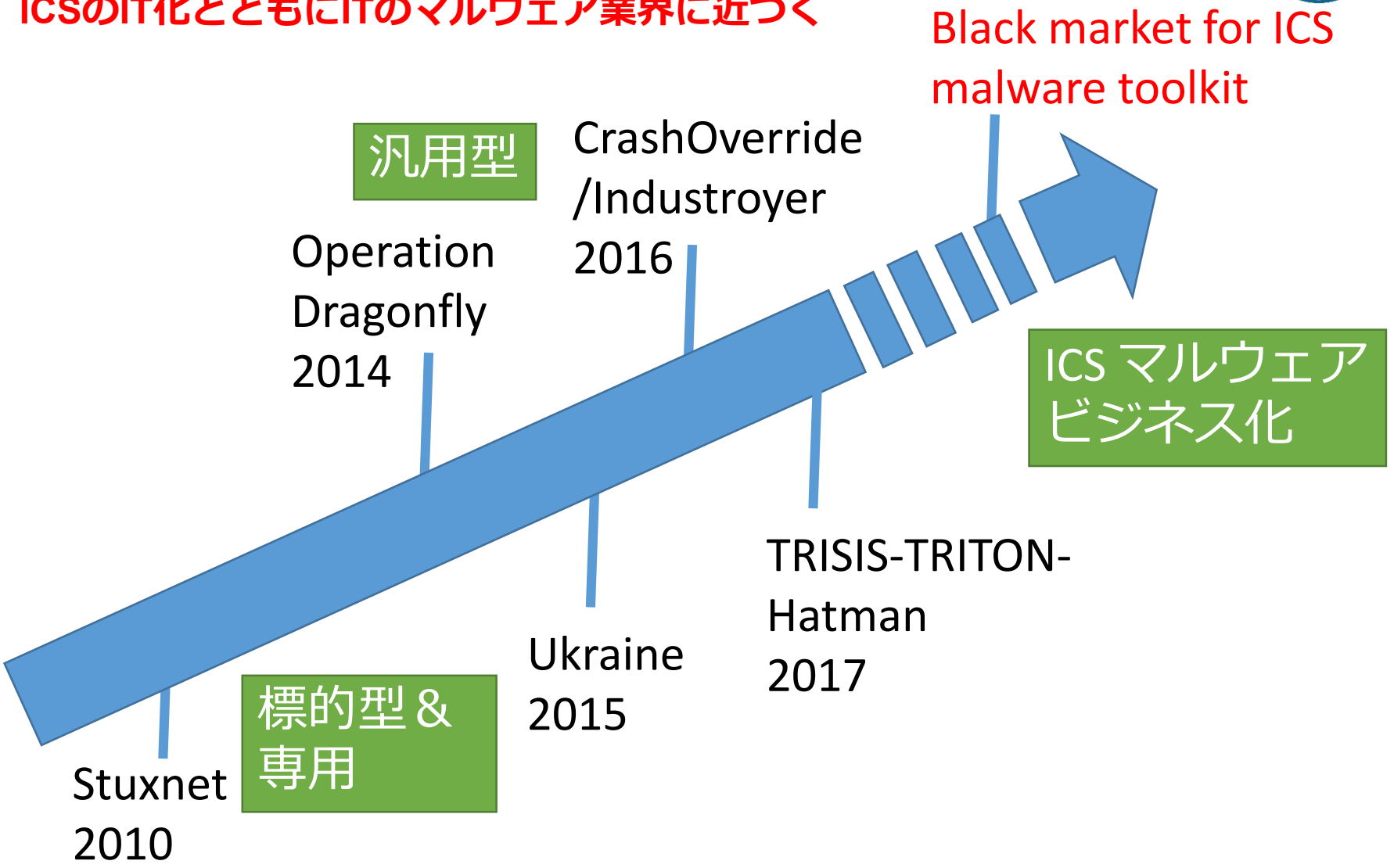



**Figure 11: Mapping ICS Modular Malware to 2016 Observable Events**

SANS, E-ISAC: Modular ICS Malware
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf

# 今後のICS脅威の進化予測

**ICSのIT化とともにITのマルウェア業界に近づく**



# IoT時代の産業制御システム セキュリティの考え方

# Internet of Things (IoT) のセキュリティ層

## クラウド/データセンターのセキュリティ


## 通信網のセキュリティ

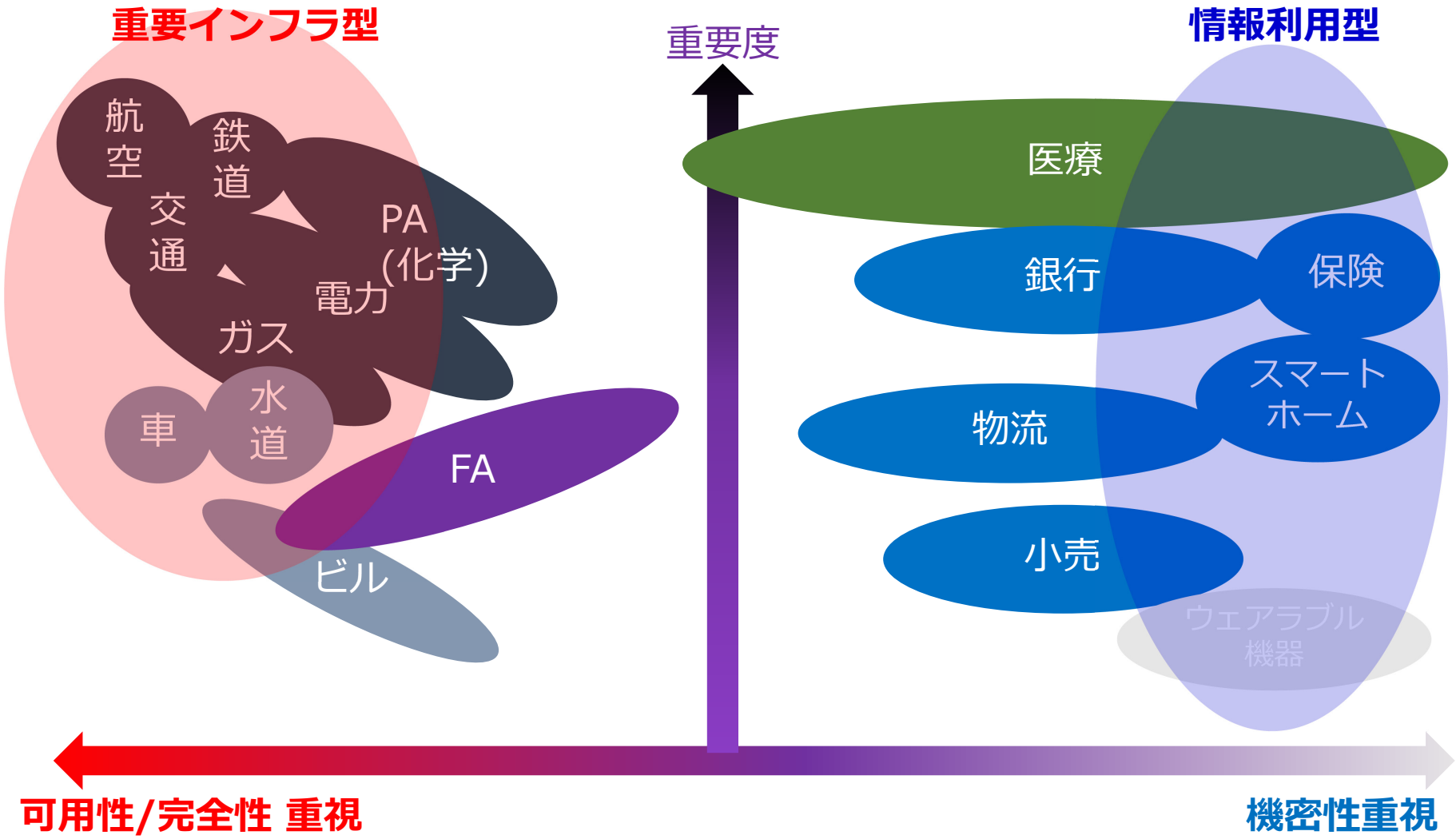
## エッジデバイスのセキュリティ

# IoTを適用する業界別のセキュリティ脅威とIoTの３層におけるセキュリティリスク評価

| IoTが適用される業界 | | IoT活用例 | 主なセキュリティ脅威 | エッジデバイス | | | | 通信網 | | | クラウド | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | S | C | I | A | C | I | A | C | I | A |
| 製造 | FA | 装置リモートメンテナンス | 制御装置異常 | H | L | H | H | L | L | L | L | L | L |
| | PA | 化学反応の歩留まり向上 | プラント動作異常 | H | M | H | H | M | L | L | M | L | L |
| 流通/サービス | 小売 | POS端末情報の活用 | 個人情報漏えい | M | H | M | L | H | M | L | H | M | M |
| | 物流 | 貨物バーコード情報の活用 | 個人情報漏えい | L | L | L | M | L | L | M | H | L | M |
| 金融 | 銀行 | フィンテック・仮想通貨 | 個人情報漏えい | M | H | M | L | H | M | L | H | M | L |
| 公共/インフラ | 電力 | スマートメーター | 停電/メーター改ざん | M | L | M | L | L | M | M | M | H | H |
| | ガス | スマートメーター | ガス停止/メーター改ざん | M | L | M | L | L | M | M | M | H | H |
| | 航空 | 航空機運航の効率化 | 不正操作による航空機事故 | H | L | H | H | L | H | H | L | H | H |
| | 鉄道 | 鉄道運行管理の効率化 | 不正操作による鉄道事故 | H | L | H | H | L | H | H | L | H | H |
| | 水道 | リモート監視 | 遠隔操作による水道機能停止 | L | L | L | H | L | L | H | L | L | H |
| | 交通 | 渋滞解消 | 遠隔操作による自動車事故 | H | L | H | H | L | H | H | L | H | H |
| | ビル | 電力使用量の効率化 | 遠隔操作による火災 | M | L | M | M | L | M | M | L | M | M |
| | 医療 | 遠隔医療 | 個人情報（病歴）漏えい | H | H | H | L | H | H | L | H | H | L |
| 一般消費者 | 個人 | ウェアラブル機器 | 個人情報漏えい | L | M | L | L | M | L | L | M | L | L |
| | 家庭 | スマートホーム | 個人情報漏えい | M | H | H | L | H | H | L | H | H | L |
| | 車 | 自動運転 | 不正操作による自動車事故 | H | L | H | H | L | H | H | L | H | H |

凡例：S:安全性 C:機密性 I:完全性 A:可用性
H:リスク高 M:リスク中 L:リスク低

# 重視するセキュリティ観点によるIoT業界分類



# IoT時代の産業制御システムセキュリティ

新しく発生した脅威は以下の３つと考えられる

エッジデバイスへの「ネットワーク経由での」
サイバー攻撃の機会の発生

各層が相互接続することによるシステム外部からの
侵入口の増加

各層が相互接続することによるシステム内部での
サイバー攻撃の影響範囲の拡大

完全に守りきることは難しい。
エッジデバイス、通信網、クラウド/データセンターの
**多層防御**においてセキュリティを確保する。

# ビジネスを支える
# 産業制御システムセキュリティ

# ICSのIT化 - あるあるダメ事例

- 工場の効率化のため、工場ネットワークを社内ネットワークにつなごう！

⇒工場からどんな通信がくるかわからない。

つなぎたくない。情シス側が難色。⇒　頓挫。

- 工作機械のリモートメンテナンス便利だな！

⇒工場の独断でルーター設置。

⇒情シス監査で発見。ファイアウォールさえない。

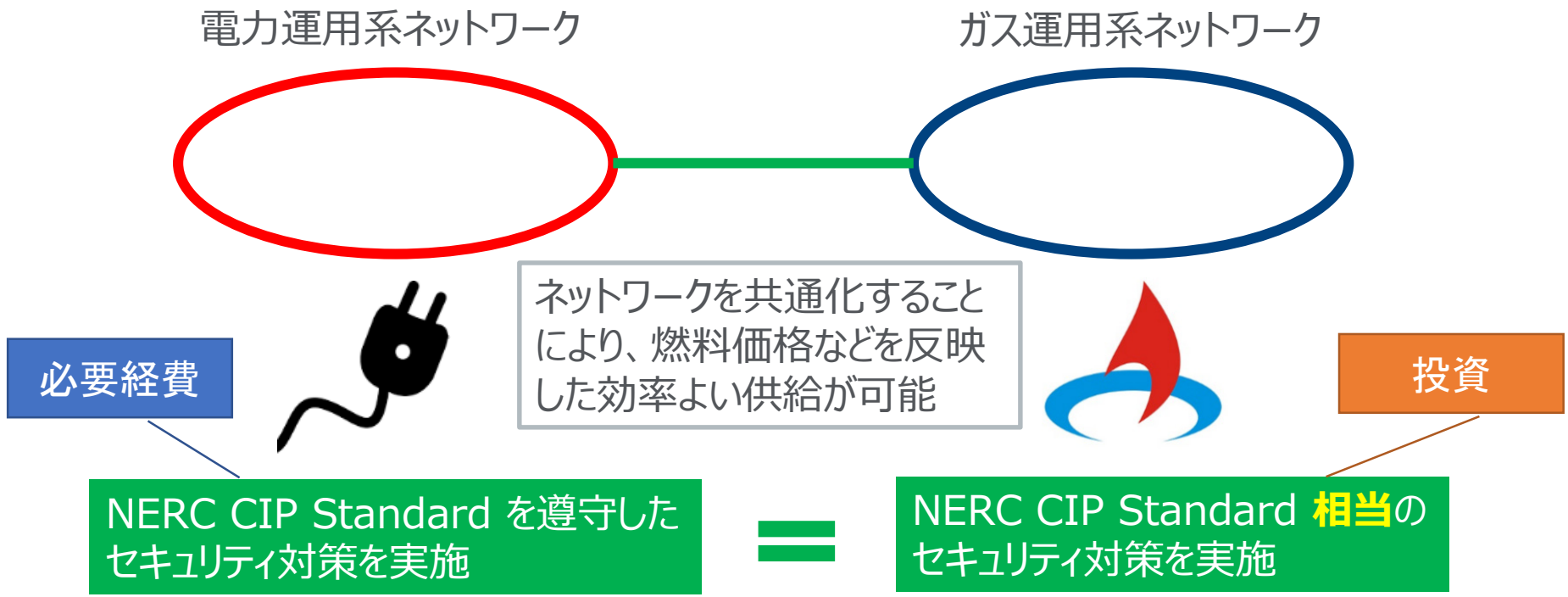
- 重要インフラ設備の海外ベンダーによるリモートメンテナンスは問答無用でダメ。

⇒リモートメンテナンス付の保守費を無駄に払う。

**課題：技術が悪いのではない。ITとICSに関わる人の相互理解が足りない。**
**セキュリティがビジネスを妨げる要因になっている。**

# 産業制御システムセキュリティが ビジネスを支える例（米国電力会社）

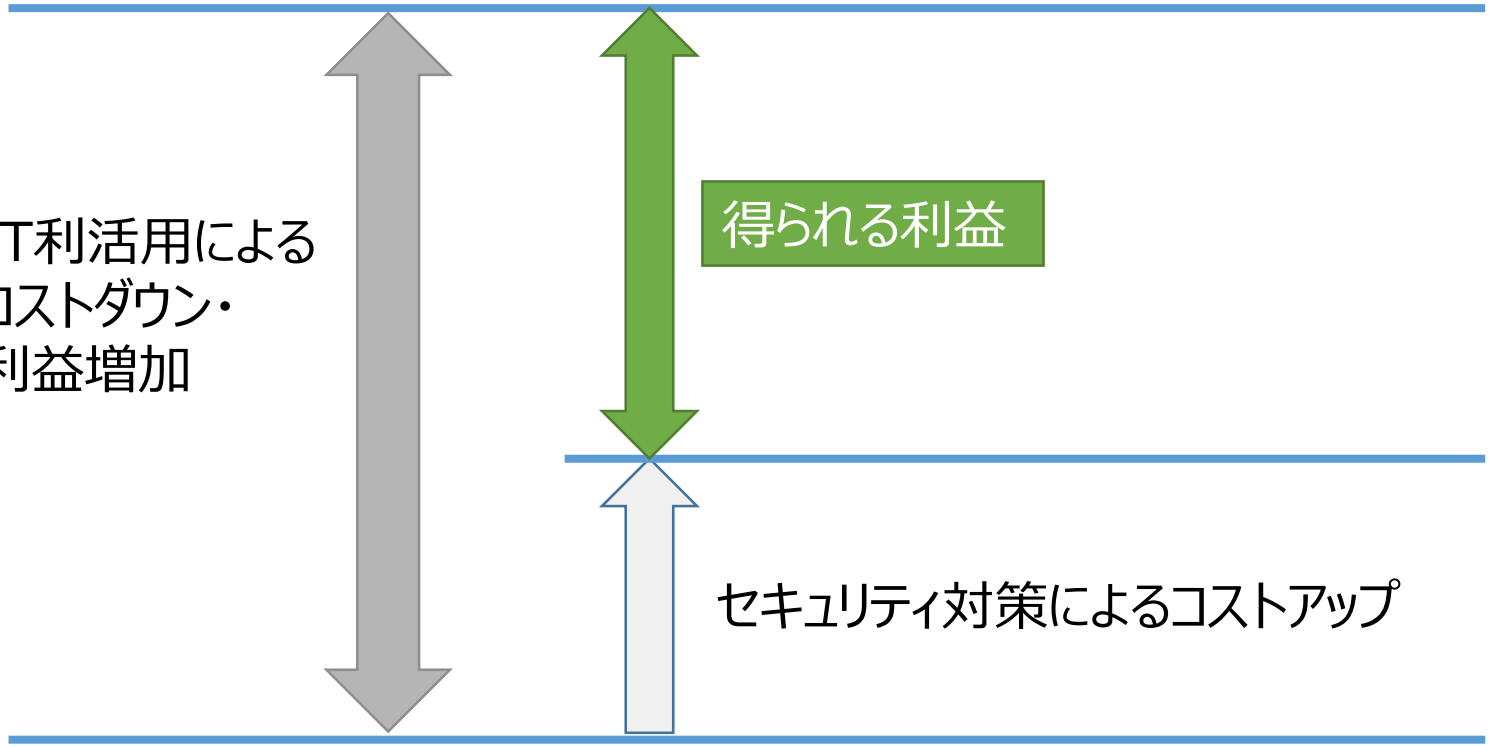
**電力とガスの運用系ネットワークを共用することでガス発電利用時の最適化ができる。**
**ガス側のセキュリティ対策を電力側と同等にすることでリスクを低減。**




電力業界には、NERC CIP Standardというセキュリティの義務規定が存在するが、
ガス業界には義務規定は存在しない。しかし、利益を取るために、ガスの運用系ネットワークにも
電力運用系と同じレベルのセキュリティ対策を実施している。

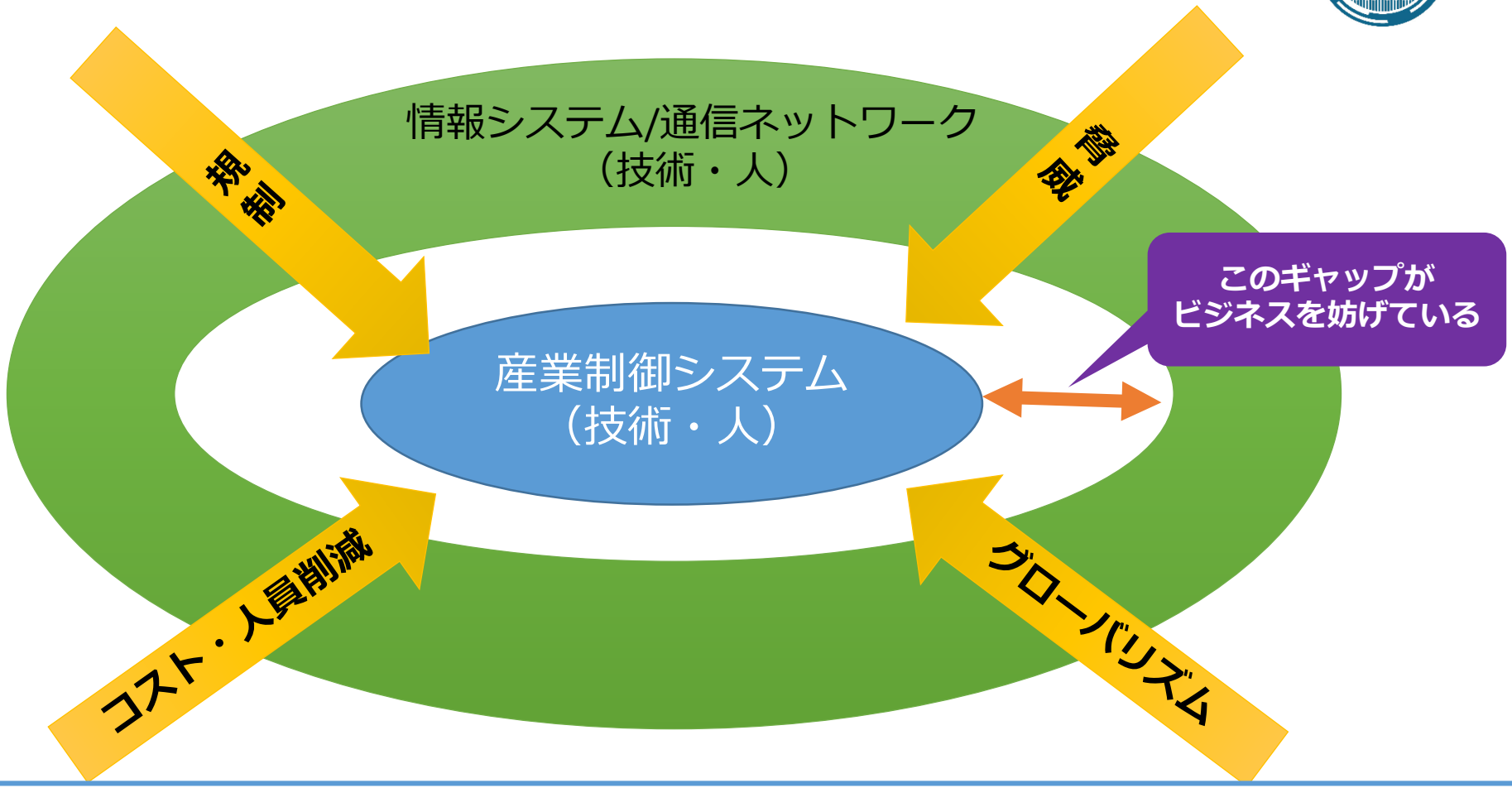
# 産業制御システムセキュリティ対策は ビジネスのための投資である

**適切なセキュリティ対策を実施することで、利益を取ることができる。**




産業制御システムセキュリティは単なるコストではなく利益を生むための**投資**
競争を勝ち抜くための重要な武器となる

# ギャップはビジネスを生む




ネットワーク技術と産業制御システム技術と人と技術の融合は、
さまざま課題解決に向けたビジネスを生む。
セキュリティは互いの共通課題としてのビジネスドライバである。