Stuxnet

ー　制御システムを狙った
初のマルウエア　ー

JPCERT/CC
小熊　信孝

目次

1. 発見から分析までのニュース

2. Stuxnetと動作の概要

3. Stuxnetの教訓

4. 参考

Stuxnetの発見

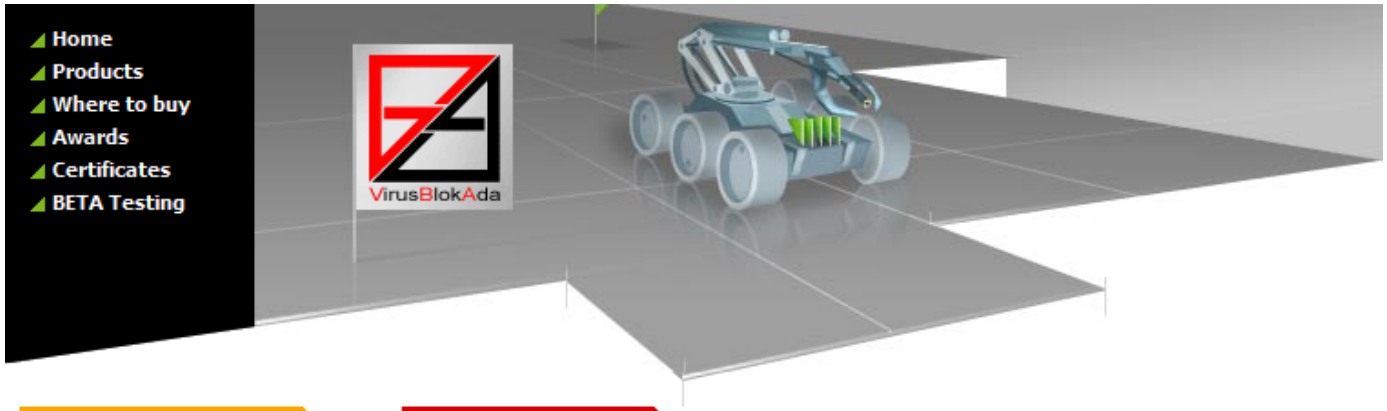
JPCERT CC®

2010年6月17日：ベラルーシに拠点を置くアンチウイルス会社VirusBlokAda 社がマルウエアのサンプルを発見

（当初この報告は世界的には注目されなかった）

Google Earth

Stuxnetの発見



NEWS

2011-01-19
Vba32 build 3.12.14.3 was released

2010-11-10
Vba32 build 3.12.14.2 was released

2010-09-20
Vba32 build 3.12.14.1 was released

2010-08-09
Vba32 build 3.12.14.0 was released

2010-08-03
Vba32 build 3.12.12.8 was released

http://www.anti-virus.by/en/tempo.shtml

Rootkit.TmpHider

Modules of current malware were first time detected by "VirusBlokAda" company specialists on the **17th of June, 2010** and were added to the anti-virus bases as **Trojan-Spy.0485** and **Malware-Cryptor.Win32.Inject.gen.2**. During the analysis of malware there was revealed that it uses USB storage device for propagation.

You should take into consideration that virus infects Operation System in unusual way through vulnerability in processing lnk-files (without usage of autorun.inf file).

So you just have to open infected USB storage device using Microsoft Explorer or any other file manager which can display icons (for i.e. Total Commander) to infect your Operating System and allow execution of the malware.

Malware installs two drivers: mrxnet.sys and mrxcls.sys. They are used to inject code into systems processes and hide malware itself. That's the reason why you can't see malware files on the infected USB storage device. We have added those drivers to anti-virus bases as **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2**. Note that both drivers are signed with digital signature of Realtek Semiconductor Corp. (www.realtek.com).

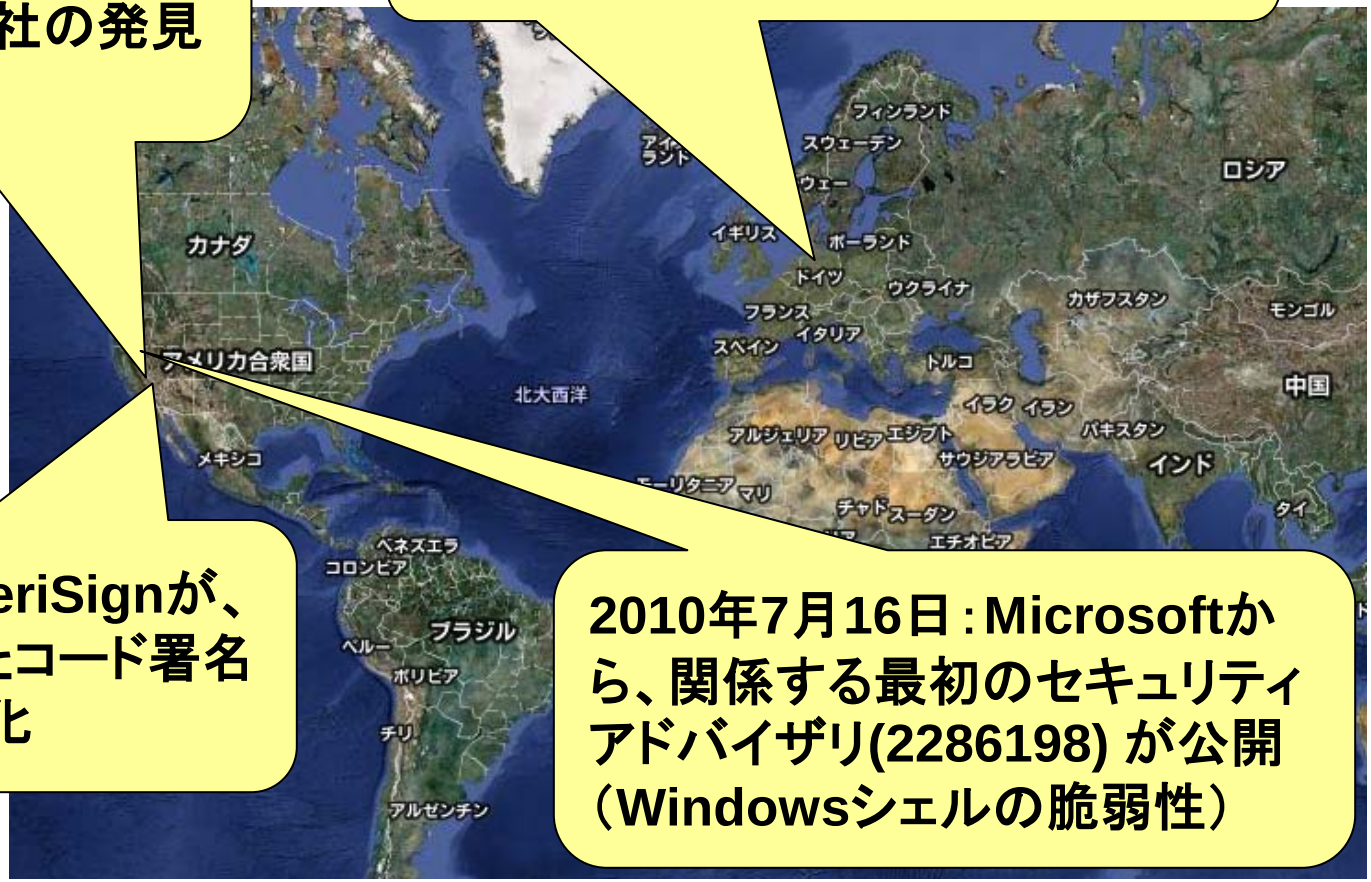
Thus, current malware should be added to very dangerous category causes the risk of the virus epidemic at the current moment.

After we have added a new records to the anti-virus bases we are admitting a lot of detections of **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2** all over the world.

Stuxnetの発見

2010年7月15日：セキュリティブロガーBrian KrebsがVirusBlokAda社の発見を報告

2010年7月16日： Siemens社がサポートサイトに情報を掲載



2010年7月16日：VeriSignが、Stuxnetに使われたコード署名用の証明書を無効化

2010年7月16日：Microsoftから、関係する最初のセキュリティアドバイザリ(2286198) が公開（Windowsシェルの脆弱性）

Google Earth

Stuxnetの影響

2010年10月3日：イランの国営テレビ各局は2日、インターネットを通じイランの核計画を妨害しようとした「核スパイ」数人が逮捕されたと報じた。(AFP)

2010年9月28日：イラン鉱工業省の情報技術部門幹部の話によると、イランが海外から大規模なサイバー攻撃を受けており、産業用パソコン約3万台に感染が見つかった。(トレンドマイクロ)

2010年9月29 日： Virus Bulletin のカンファレンスでシマンテックがStuxnetに関する詳細レポートを報告

Stuxnetの分析

2010年11月12日：Stuxnetの攻撃対象とメカニズムを解明し、レポート(シマンテック)

W32.Stuxnet Dossier
http://www.symantec.com/connect/blogs/w32stuxnet-dossier

Symantec
Security Response

W32.Stuxnet Dossier
Version 1.3 (November 2010)

Nicolas Falliere, Liam O Murchu,
and Eric Chien

Contents

Introduction
Executive Summary
Attack Scenario
Timeline
Infection Statistics
Stuxnet Architecture
Installation
Load Point
Command and Control
Windows Rootkit Functionality
Stuxnet Propagation Methods
Modifying PLCs
Payload Exports
Payload Resources
Variants
Summary
Appendix A
Appendix B
Appendix C
Revision History

While the bulk of the analysis is complete, Stuxnet is an incredibly large and complex threat. The authors expect to make revisions to this document shortly after release as new information is uncovered or may be publicly disclosed. This paper is the work of numerous individuals on the Symantec Security Response team over the last three months well beyond the cited authors. Without their assistance, this paper would not be possible.

Introduction

W32.Stuxnet has gained a lot of attention from researchers and media recently. There is good reason for this. Stuxnet is one of the most complex threats we have analyzed. In this paper we take a detailed look at Stuxnet and its various components and particularly focus on the final goal of Stuxnet, which is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. We have already covered some of these components in our blog series on the topic. While some of the information from those blogs is included here, this paper is a more comprehensive and in-depth look at the threat.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion

Stuxnetの影響

2010年11月23日：IAEAの天野事務局長は、理事国に配布したイラン核問題に関する報告書で、同国が16日にウラン濃縮活動を一時的に停止したことを明らかにした。(時事通信)

2010年11月29日：イランのアハマディネジャド大統領は同国のウラン濃縮施設の遠心分離機がコンピューターウイルスに感染していたことを明らかに。(ロイター)

2010年11月16日：IAEAによりイラン中部ナタンツのウラン濃縮施設で、約8400 台の遠心分離機がすべて停止していることが確認される。（毎日.jp）

2010年11月22日：イランは22日までに約4600台が再稼働したことをIAEAに報告（毎日.jp）

Stuxnetの構造

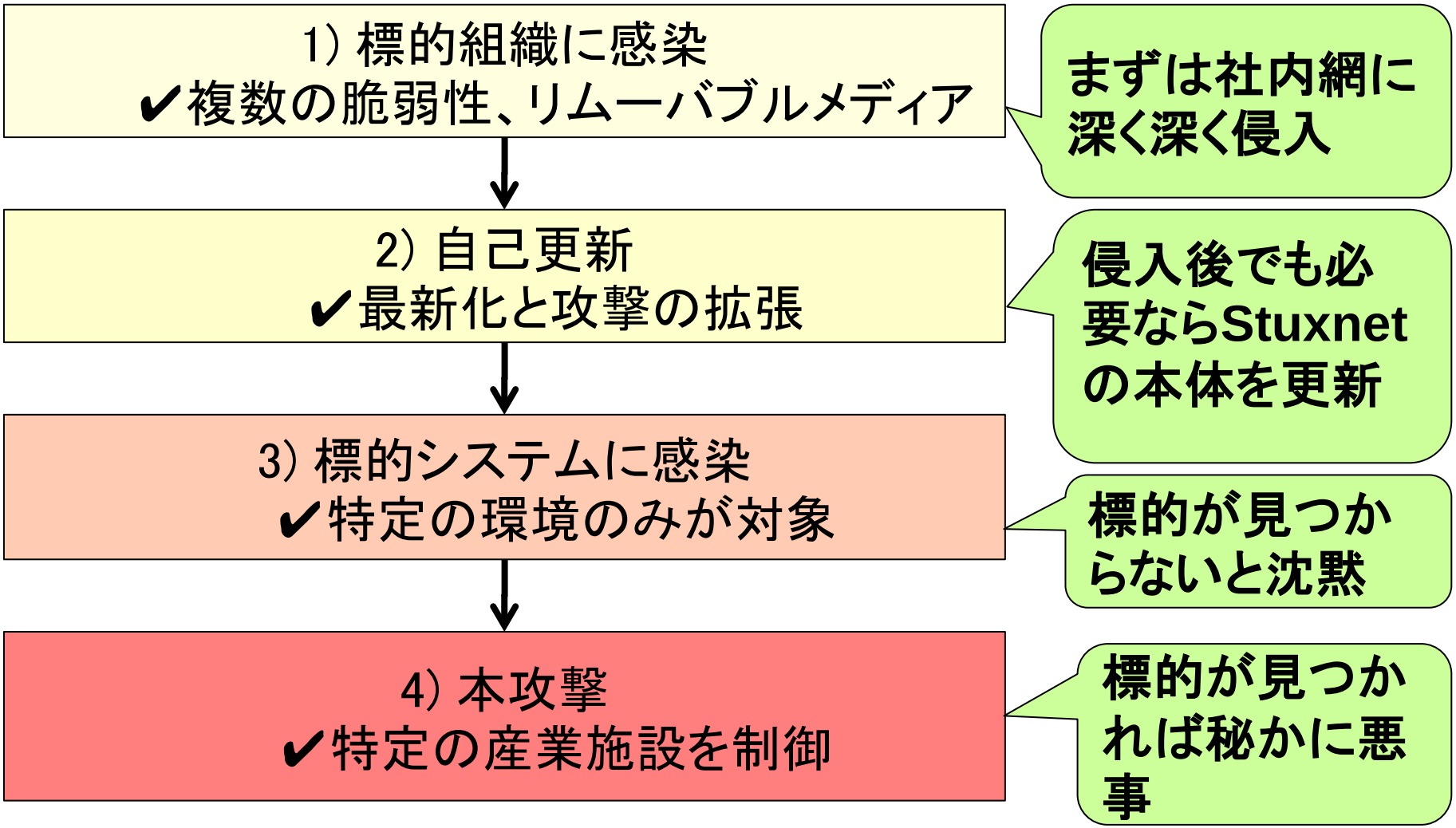
- 亜種を含めて4種類のバイナリが存在するが、いずれもパッケージ化された状態で500～600Kバイトのサイズ

  ⇒　一般的なワームと比べて特別大きいわけではない

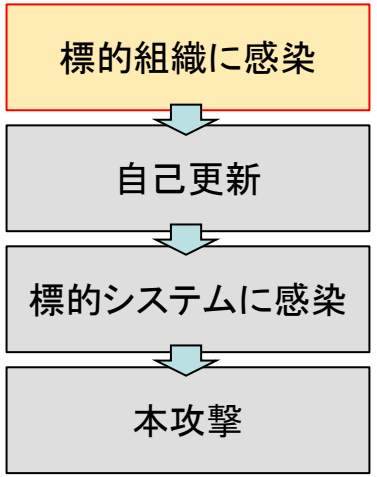
- 環境に応じて動作を変え、多様な形態をとって標的システムに展開
  - ✓ C&Cサーバと通信して動作を変え、自身を最新版に更新
  - ✓ StuxnetのP2P網を介しても自身を最新版に更新
  - ✓ PLCを制御するWinCC/PCS7 (Siemens社製DCS)やPLCにも侵入(コード書換え)

[用語解説]　**C&Cサーバ (Command and Control server)**
マルウェアに対して動作指令を出すためにインターネット上にマルウェア作者が設置するサーバ.

Stuxnetの動作概要



Stuxnetの動作　～標的組織に感染



Windowsシステム上で感染範囲を拡大

- 2000, XP, 2003, Vista, サーバ2008,7, サーバ2008R
- 感染率の高い地域に偏りがある (理由は不明)
  - イランや中国で多数の感染PCが報告されている
  - 幸い日本では皆無に近い

Windowsの複数の脆弱性を利用するなど複数の方法で感染させる

- 利用された複数のゼロデイ脆弱性 (次のシート参照)
- 感染方法 (後述)

一旦感染に成功すると検知されないようにして延命をはかる

- 自身を隠蔽するためにrootkitをインストール
- Mcshield.exeやavguard.exeなど Windowsのセキュリティ関連プロセスを終了させる

Stuxnetの動作　～標的組織に感染
拡散に悪用された脆弱性

JPCERT CC®

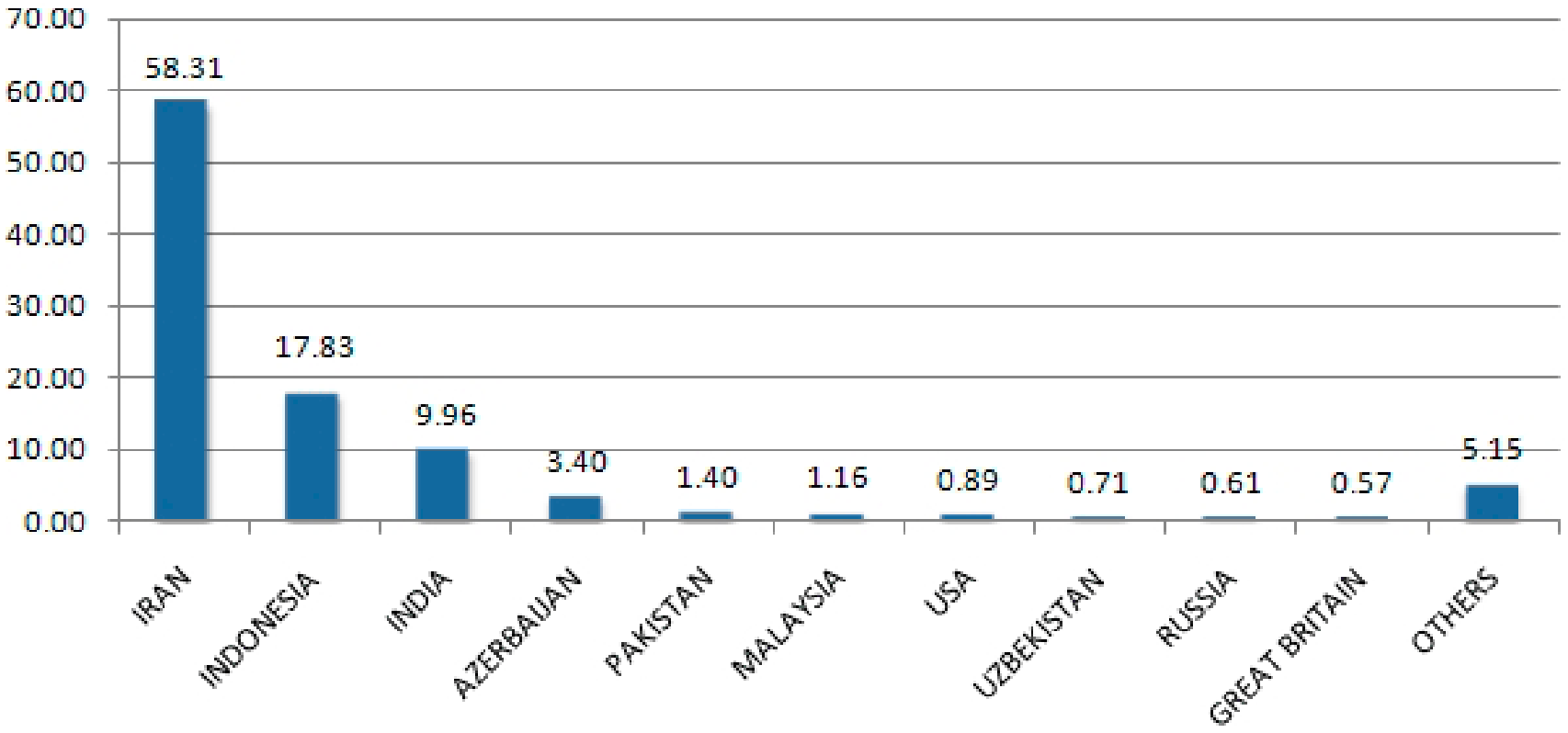
脆弱性の内容	セキュリティ・アドバイザリ	公開日
Windows シェルの脆弱性により、リモートでコードが実行される	MS10-046 ゼロデイ	2010.7.17
印刷スプーラー サービスの脆弱性により、リモートでコードが実行される	MS10-061 ゼロデイ	2010.9.15
Server サービスの脆弱性により、リモートでコードが実行される	MS08-067	2008.10.24
Windows カーネルモード ドライバの脆弱性により、特権が昇格される	MS10-073 ゼロデイ	2010.10.13
タスク スケジューラの脆弱性により、特権が昇格される	MS10-092 ゼロデイ	2010.12.15

$5万~ $50万?

感染状況の報告

地域別ホストの感染比率 （2010．9．29現在）

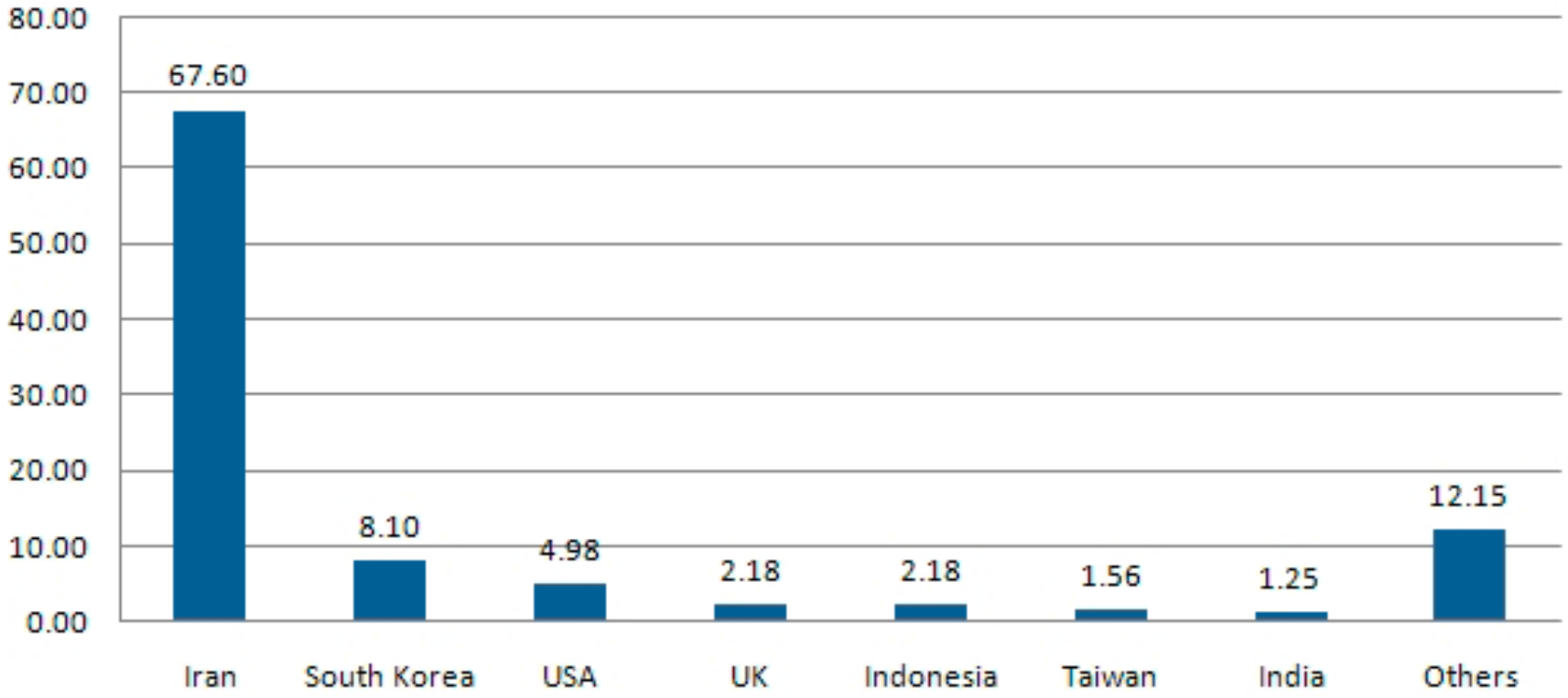
※155を越える国の40,000以上のホストにおける割合



出典：W32.Stuxnet Dossier, Symantec

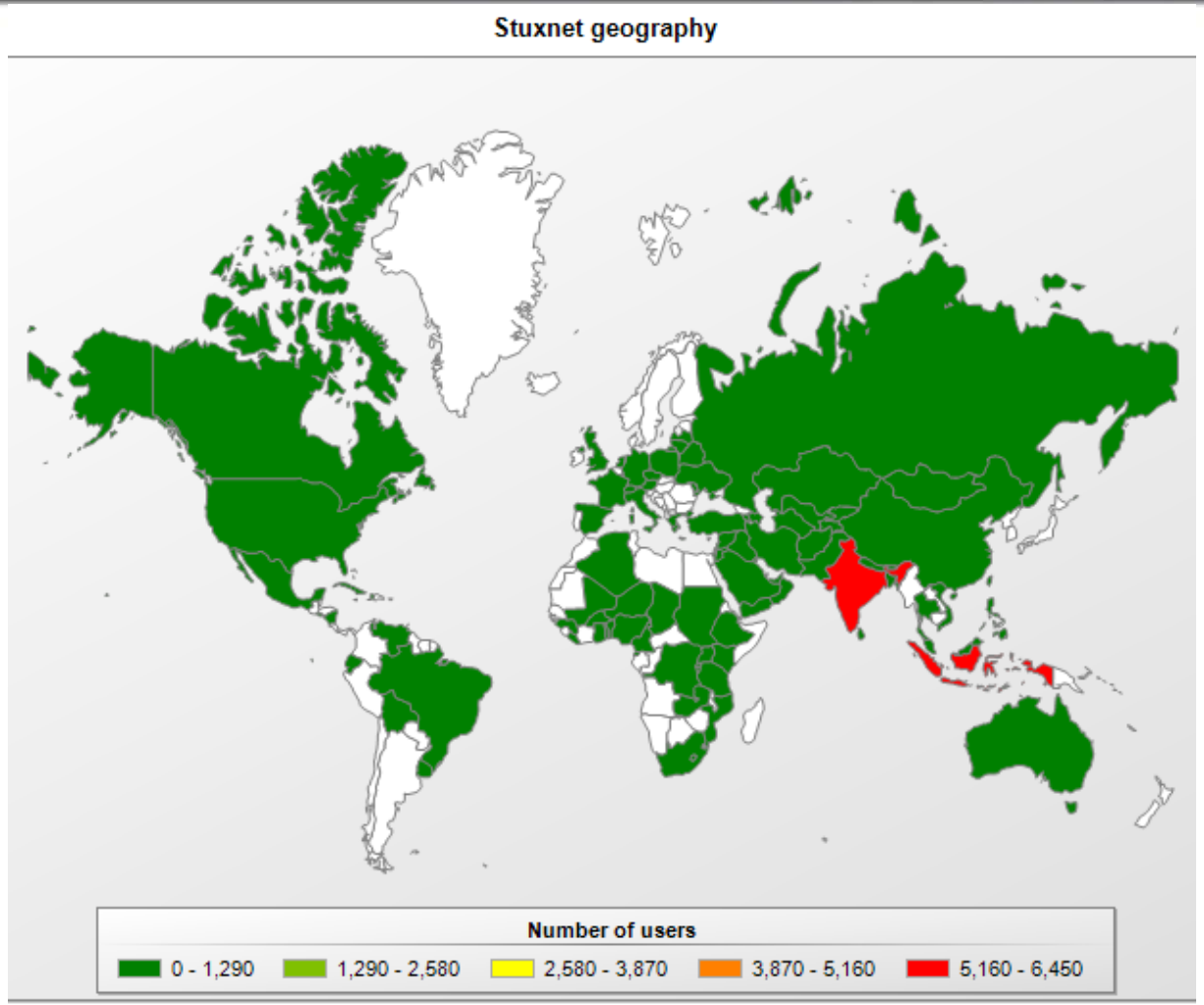
感染状況の報告（つづき）

ターゲットのソフトウエアがインストールされたホストの感染比率　（2010．9．29現在）



出典：W32.Stuxnet Dossier, Symantec

感染状況の報告(つづき)

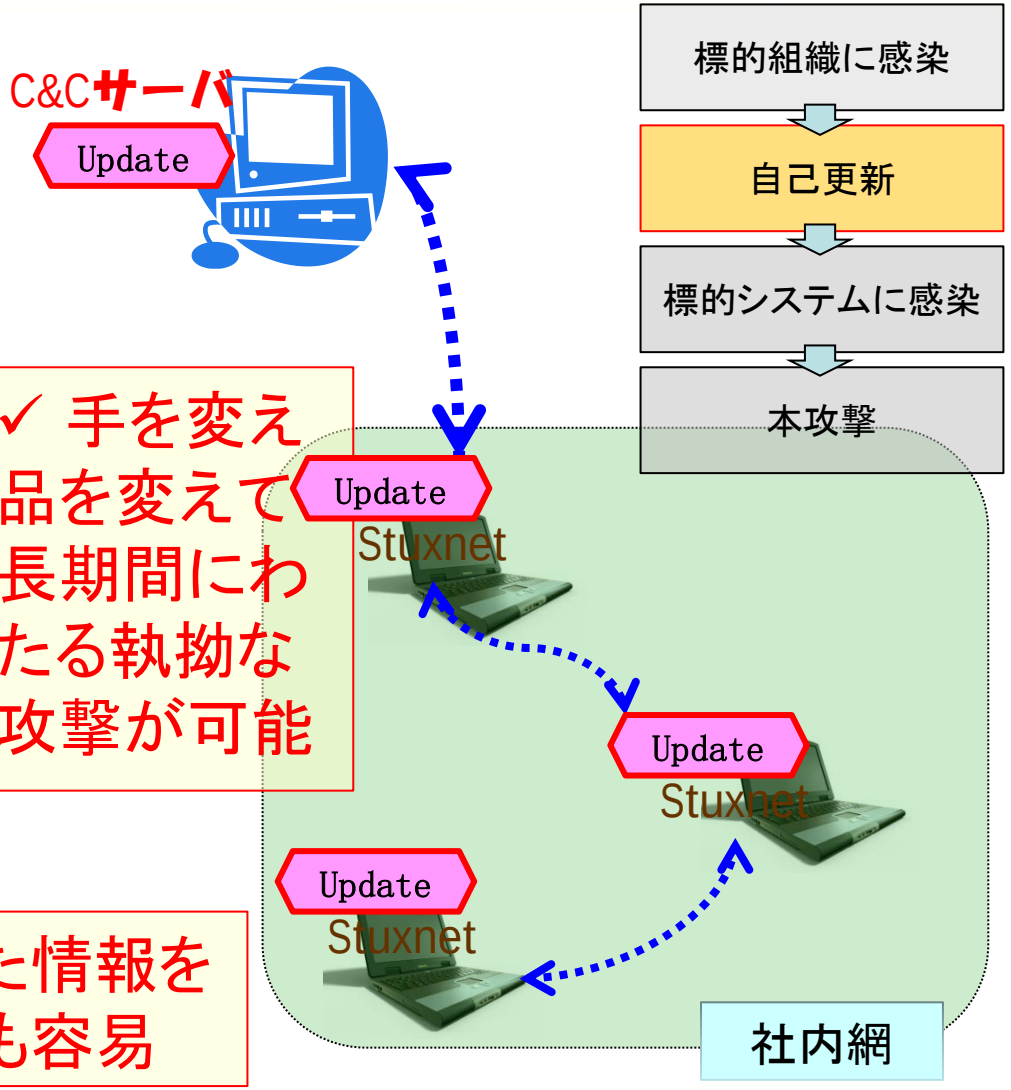


出典:カスペルスキー　マルウェアマンスリーレポート : 2010 年 9 月

Stuxnetの動作　～自己更新

JPCERT CC®

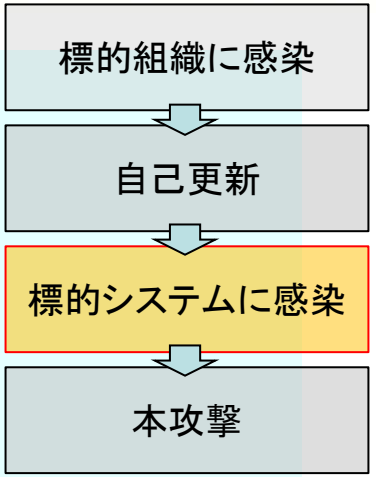
- 社内網からインターネットへのアクセスが可能なら、感染したStuxnetはインターネット上のC&Cサーバに接続して命令を受け取り自身を更新することも可能
- 間接的にインターネットにインターネットへのアクセスが可能で，途中にも感染したStuxnetが存在すれば、P2P通信を介して自身を最新版に更新できる



✓ 手を変え品を変えて長期間にわたる執拗な攻撃が可能

✓ イントラネット内で収集した情報をアップロードするような拡張も容易

Stuxnetの動作　～標的システムに感染



ネットワーク接続があれば…

- ネットワーク経由
  - Windowsのネットワーク共有を悪用する方法
  - 印刷スプーラーの脆弱性を悪用する方法
  - サーバ・サービスの脆弱性を悪用する方法

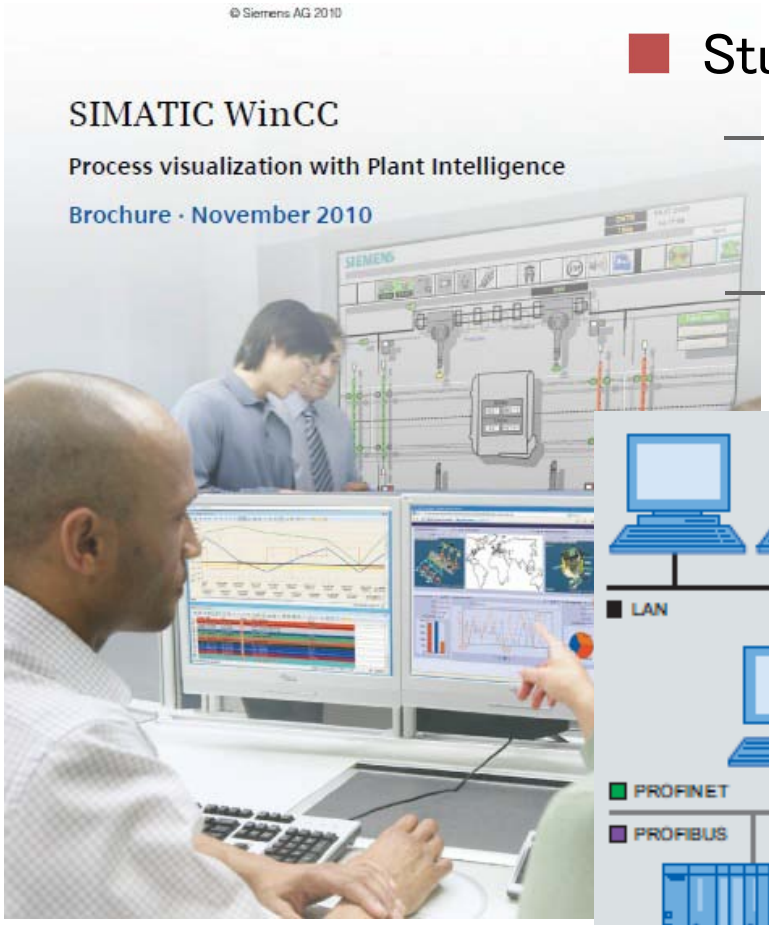
ネットワーク接続がなくても

- リムーバブルデバイス経由　(USBスティックメモリ,etc.)
  - autorun.infを利用する方法
  - .LNK脆弱性を利用する方法

✓クローズド網でも保守用USBメモリやPCが感染経路になる

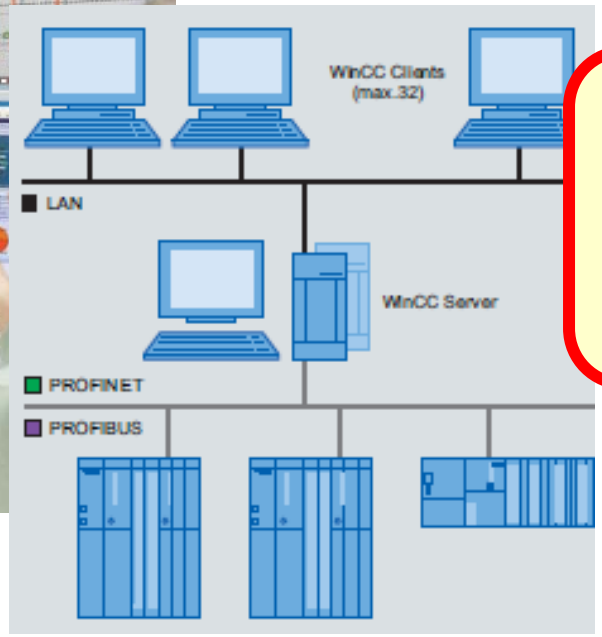
AutoRun.infを無効化する(セキュアUSBメモリ等)だけでは防げない

Stuxnetの動作　～本攻撃



参考：Siemens

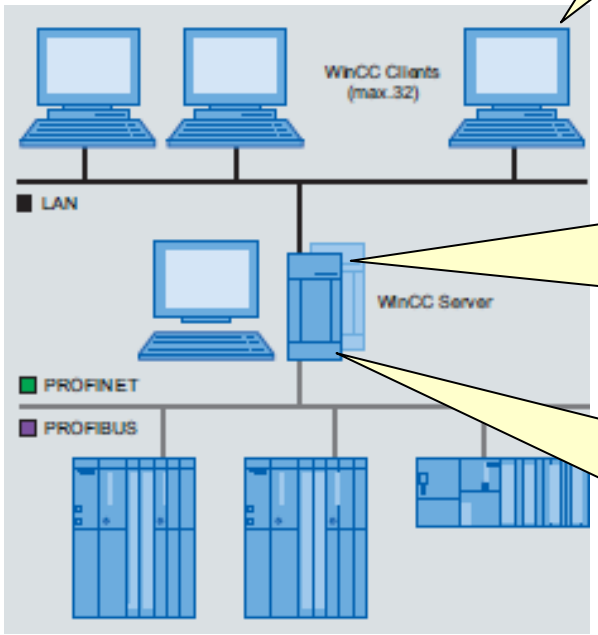
- Stuxnetの標的は：
  - Siemens社製DCSである SIMATIC WinCC/PCS7
  - 配下にある特定のPLC



標的組織に感染
↓
自己更新
↓
標的システムに感染
↓
本攻撃

WinCCが見つかるとStuxnetの攻撃動作が始まる

Stuxnetの動作　～本攻撃



WinCCソフトウエアを発見すると、開発元によってシステム内にハードコードされたパスワードでログインする

WinCCソフトウエアのSQLデータベースにテーブルを生成し、書き込んだバイナリ・データでWinCCサーバを感染させる

PLCに送られるSTLを書きかえるとともに、それを隠すためにWinCCのPLCとの通信機能に目隠しを挿入

PLC 上のすべてのコードブロックを表示しようと試みても、Stuxnet によって挿入されたコードは表示されない

Stuxnetの動作　～本攻撃

Stuxnetが制御を乗っ取る（最終目的）

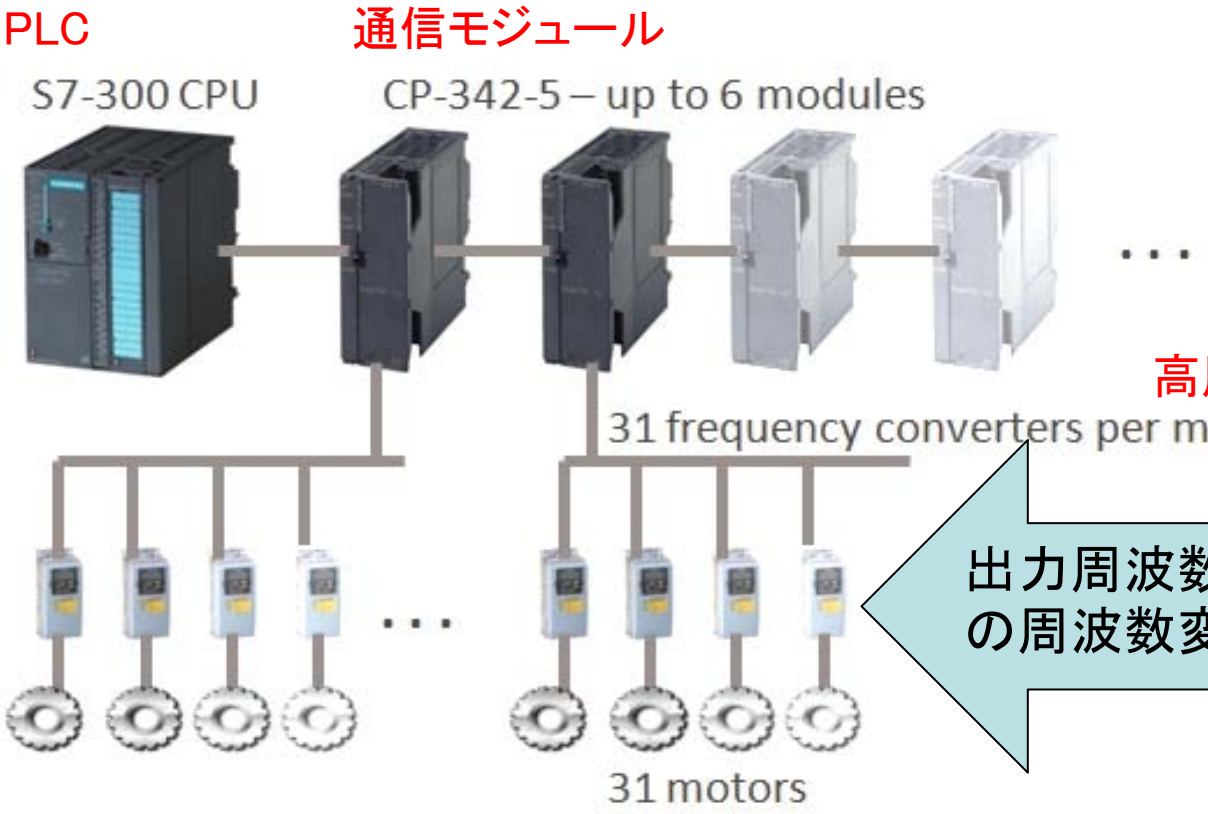
1. 特定の条件に合致することを確認：
   - 特定のベンダーの特殊な周波数変換ドライブがある
   - モーターの動作周波数が807 Hz ～ 1210 Hz

2. 条件に合わなければ何もしない

3. 条件に合えばStuxnetがPLCを制御して本来の動作とは異なったプロセスを行わせる

4. ターゲット装置のセンサーが出す警告信号を止める指令を出して「誤作動」に気付かせない

Stuxnetの動作　～本攻撃
狙いは，特定のシステムの破壊または操業妨害



出力周波数807～1210Hz
の周波数変換装置のみ攻撃

非常に高速のため
用途が限られる

例えば原子炉の
ウラン濃縮用遠心分離機
実害(故障多発)発生の報道

出典：W32.Stuxnet Dossier, Symantec

Stuxnetが打ち砕いた安全神話

- 制御システムはサイバー攻撃と無縁だ
- 制御システムをインターネットと切り離しておけば100%安全だ
- 特殊なシステム構成だから外部にいる攻撃者に分かるはずない
- 新品のUSBメモリだけを使っていれば安全だ
- マルウェアが感染するとコンピュータ自体の動きが異常になる（制御システムは異常停止しない限り，稼働させ続ければよい）

Stuxnetの教訓

Stuxnetにおける事実	Stuxnetに耐えるために求められるもの
脆弱性を衝いて侵入された	• 脆弱性を作り込まない**技術力** • 事前に脆弱性を除去しておく**組織力** • 部分的に多少の脆弱性があっても耐えられる(多層防御)ようにシステムを構成しておく**技術力**
開発者は標的の制御システムを知り尽くしていたと見られる	• システム構成に関する情報が攻撃者に知られても耐えられる防衛ラインを作り込む**技術力**
特定の環境でのみ攻撃動作	• 異常を検知する**眼力(人)**
異常をHMIで表示されないよう隠蔽	• 制御システムの異常も疑ってみて総合的に判断する**眼力(人)**
今でもStuxnetを知らない制御システム運用者も少なくない	• **情報収集**のための**組織力**
ゼロデイ脆弱性が悪用されているので，普通の復旧では再び侵入される	• すみやかなシステム**復旧**と業務継続のための戦略

Stuxnetの教訓

JPCERT CC®

	防御	検知	復旧策
ベンダ	■脆弱性を作り込まない**技術力**	■制御システム用侵入検知システム	
	■多層防御を構成しておく**技術力**		■ユーザー支援サービス／連携
ユーザ	■事前に脆弱性を除去しておく**組織力**	■異常を検知する**眼力**（人）	
	■**情報収集**のための**組織力**	■制御システムの異常も疑ってみて総合的に判断する**眼力**(人)	■すみやかなシステム**復旧**と業務継続のための戦略
	■防衛ラインを作り込む**技術力**		

参考

- Symantec: Win32.Stuxnet Dossier
  http://www.symantec.com/connect/blogs/w32stuxnet-dossier
- ESET: Stuxnet Under the Microscope
  http://blog.eset.com/2010/09/23/eset-stuxnet-paper
- Siemens: Information concerning Malware / Virus / Trojan

  http://support.automation.siemens.com/WW/view/en/43876783
- F-Secure Blog

  http://www.f-secure.com/weblog/
- IBM-ISS: An inside look at Stuxnet

  http://blogs.iss.net/archive/papers/ibm-xforce-an-inside-look-at-stuxnet.pdf
- US-CERT: Control Systems Security Program(CSSP)

  http://www.us-cert.gov/control_systems/

ご清聴ありがとうございました

Email: scada@jpcert.or.jp

余談

- Stuxnetの開発にはイスラエルが関与か？
  それを示唆するコードの埋め込みやレジストリキーの操作（諸説あり）
- 現行バージョンは2012年6月24日に拡散を停止
- 複数の「2010セキュリティニュース」で上位に
- 開発したのはイスラエルと米国らしい（New York Times 2011-1-16）
- ブシェール原子力設備へのサイバー攻撃，チェルノブイリ原発事故に匹敵する大惨事につながった可能性も（AP通信 2011-1-31）