CyberDefense

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

CyberDefense

- 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

CyberDefense

(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換えることにより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系統の構築・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

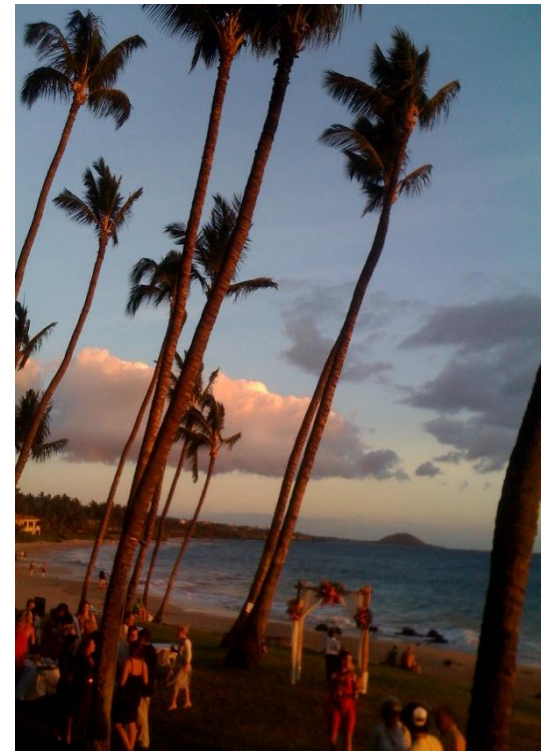
写真提供:SHIMIZU NORTH AMERICA, LLC

NEDO スマートグリッド実証＠ハワイ

CyberDefense

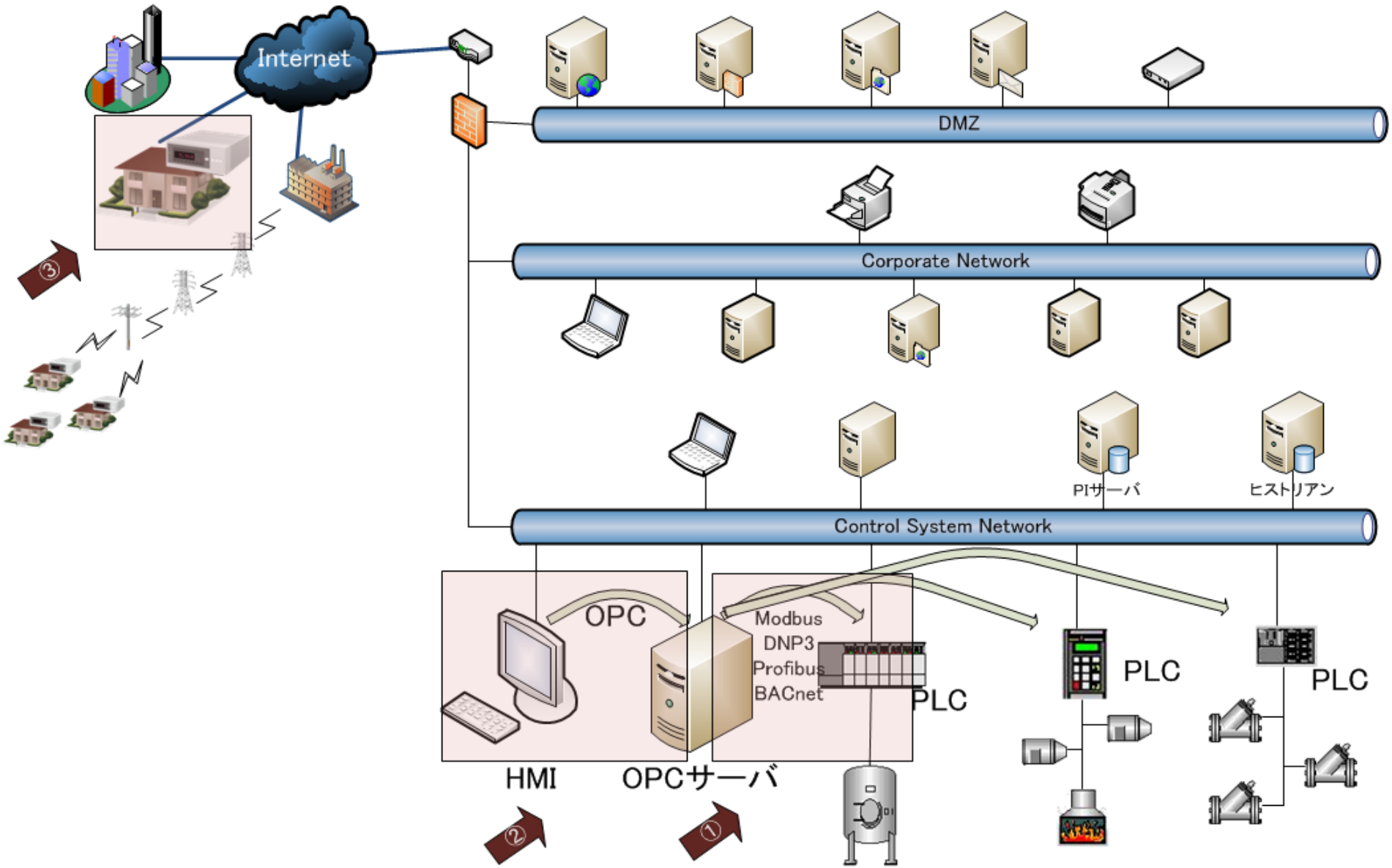
1. マウイ島におけるEVを活用した離島型スマートグリッド実証再生可能エネルギーの出力変動により、顕著化している周波数への影響などの電力系統への影響を緩和するための、EV充電、および電力系統内に設置した蓄電池を制御するEVMS（EV Management System）を構築し、有効性を実証。
2. Kihei地区における1配電用変電所レベルのスマートグリッド実証全米共通の課題である配電系統の信頼性向上を目的として、太陽光発電（以下、PVという）・EVが導入された配電線において、電圧変動や低圧変圧器の過負荷などの影響を緩和し、また上位系統と協調運転が可能なDMS（Distribution Management 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

CyberDefense



大きく分けて、

CyberDefense

- 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)

CyberDefense

- 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

引用元：http://www.automation.siemens.com

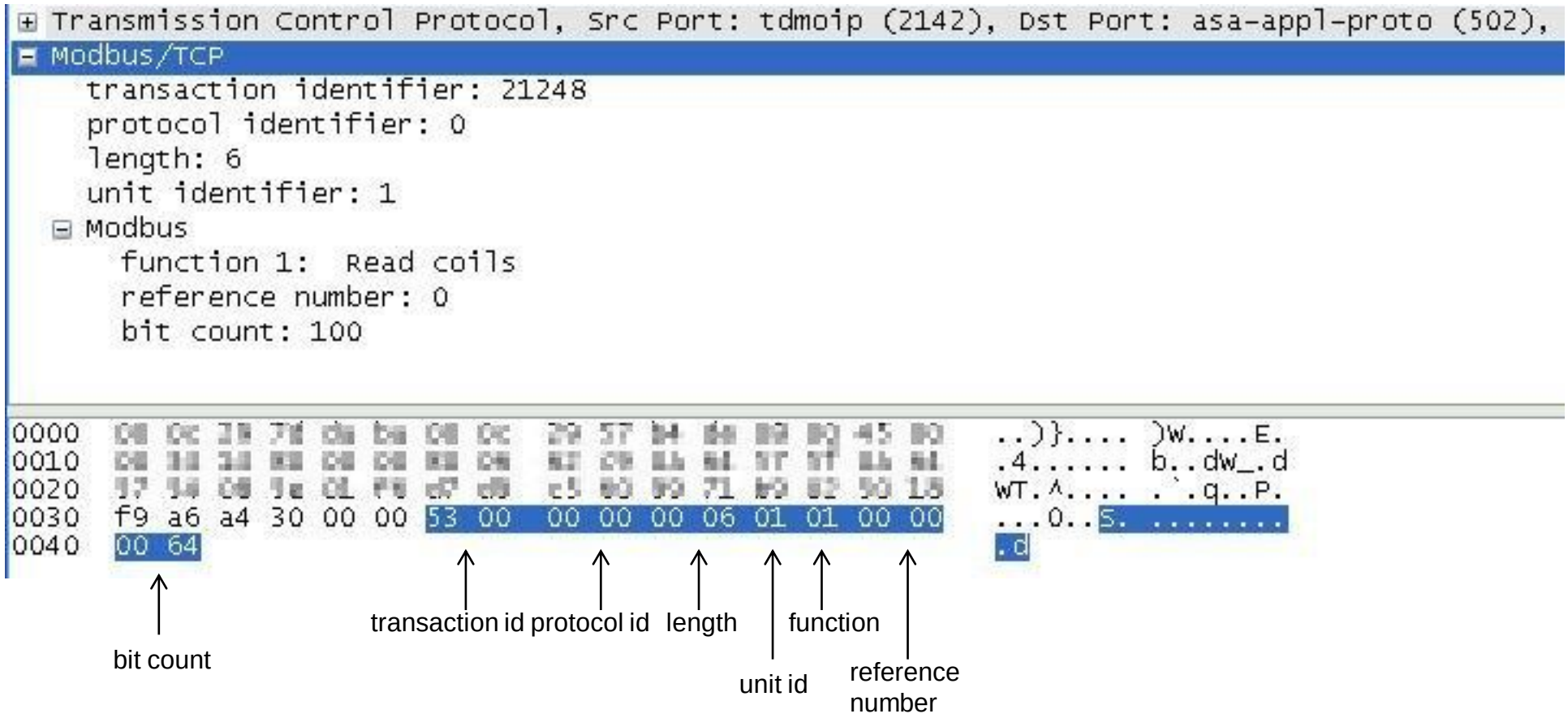
よく使われるプロトコル

CyberDefense

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

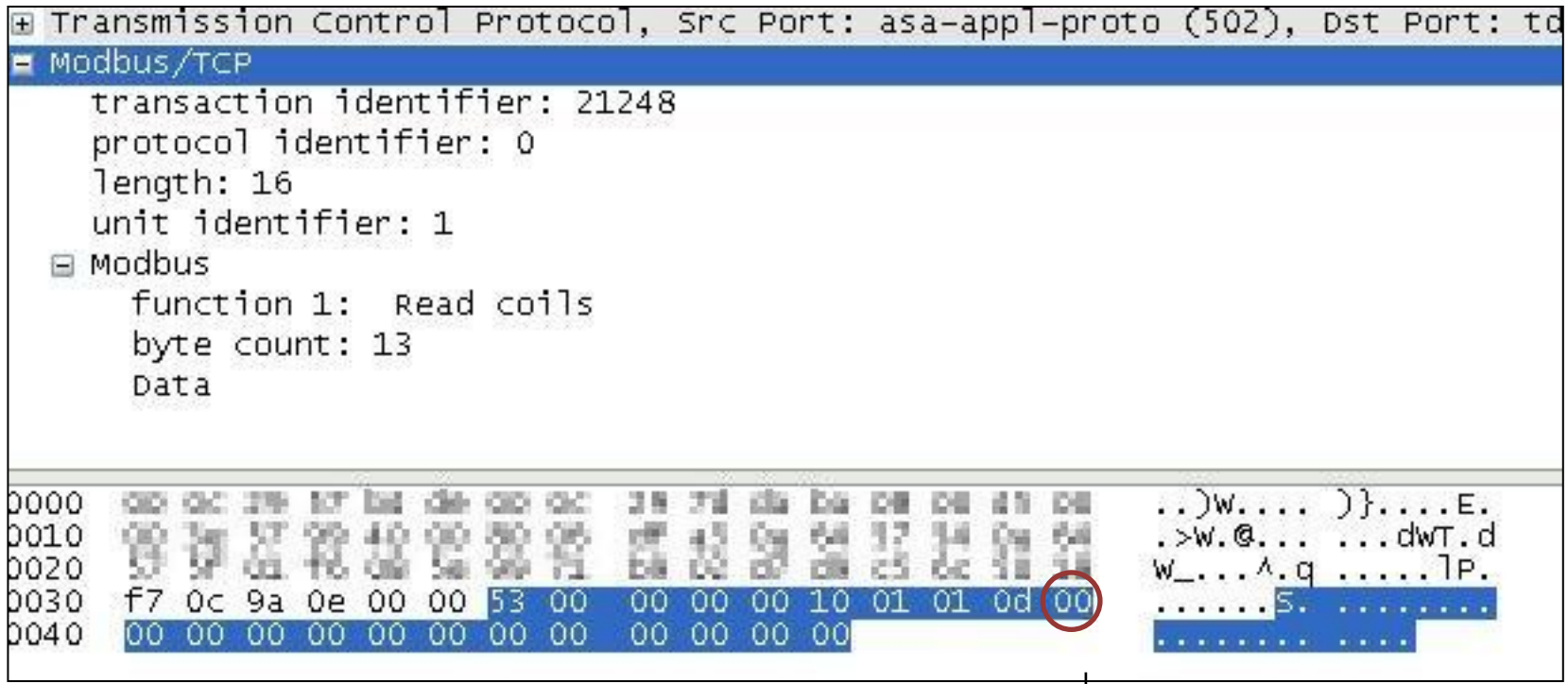
Modbusの仕様（リクエスト）

CyberDefense

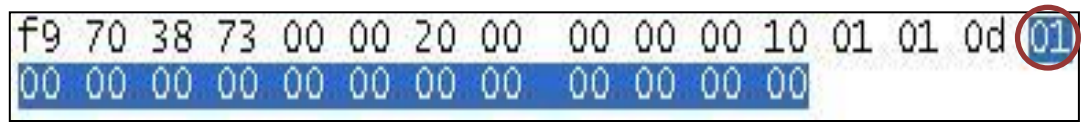


Modbusの仕様（レスポンス）

CyberDefense

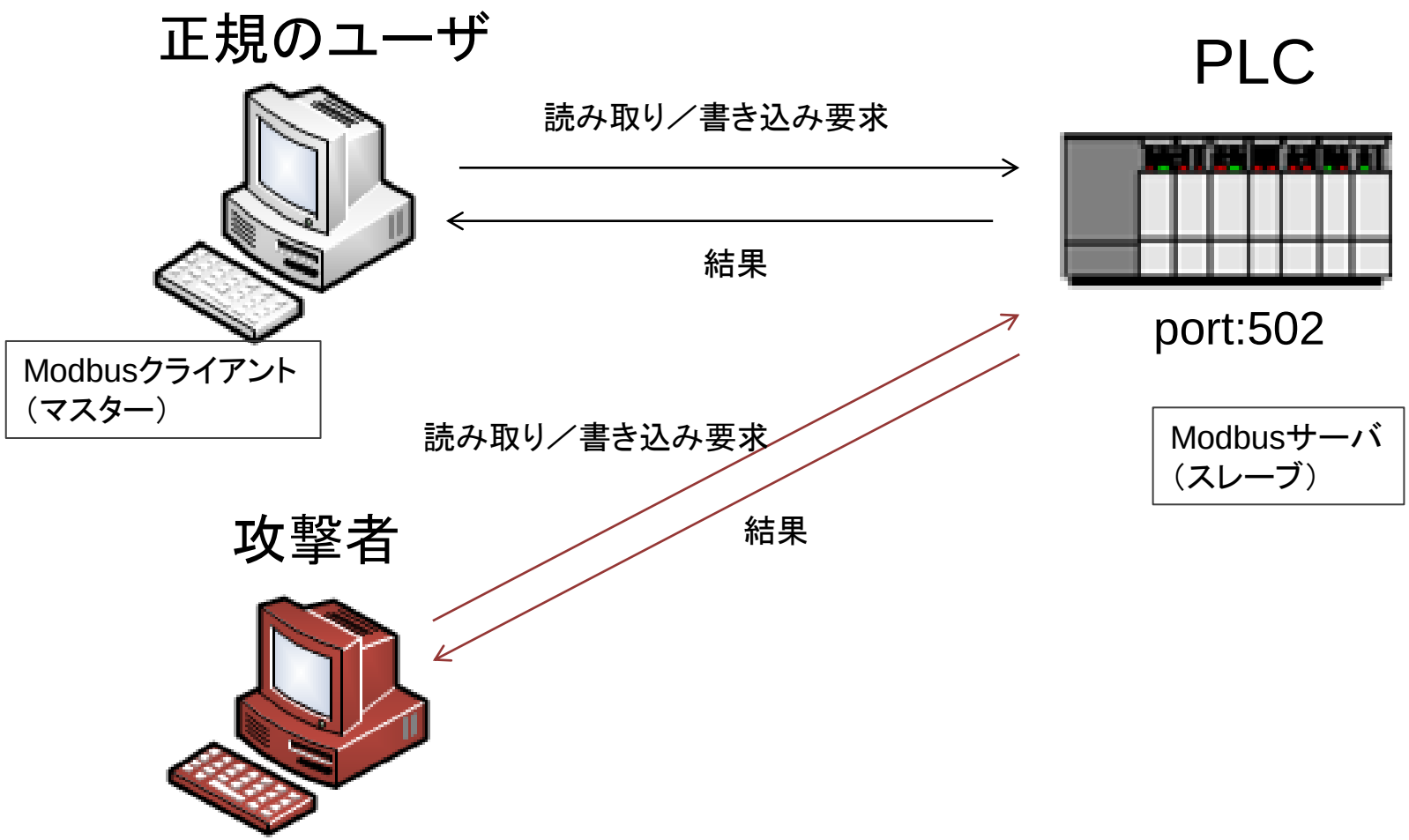


値がOffからOnに切り替わった



Modbusサーバへのアクセス

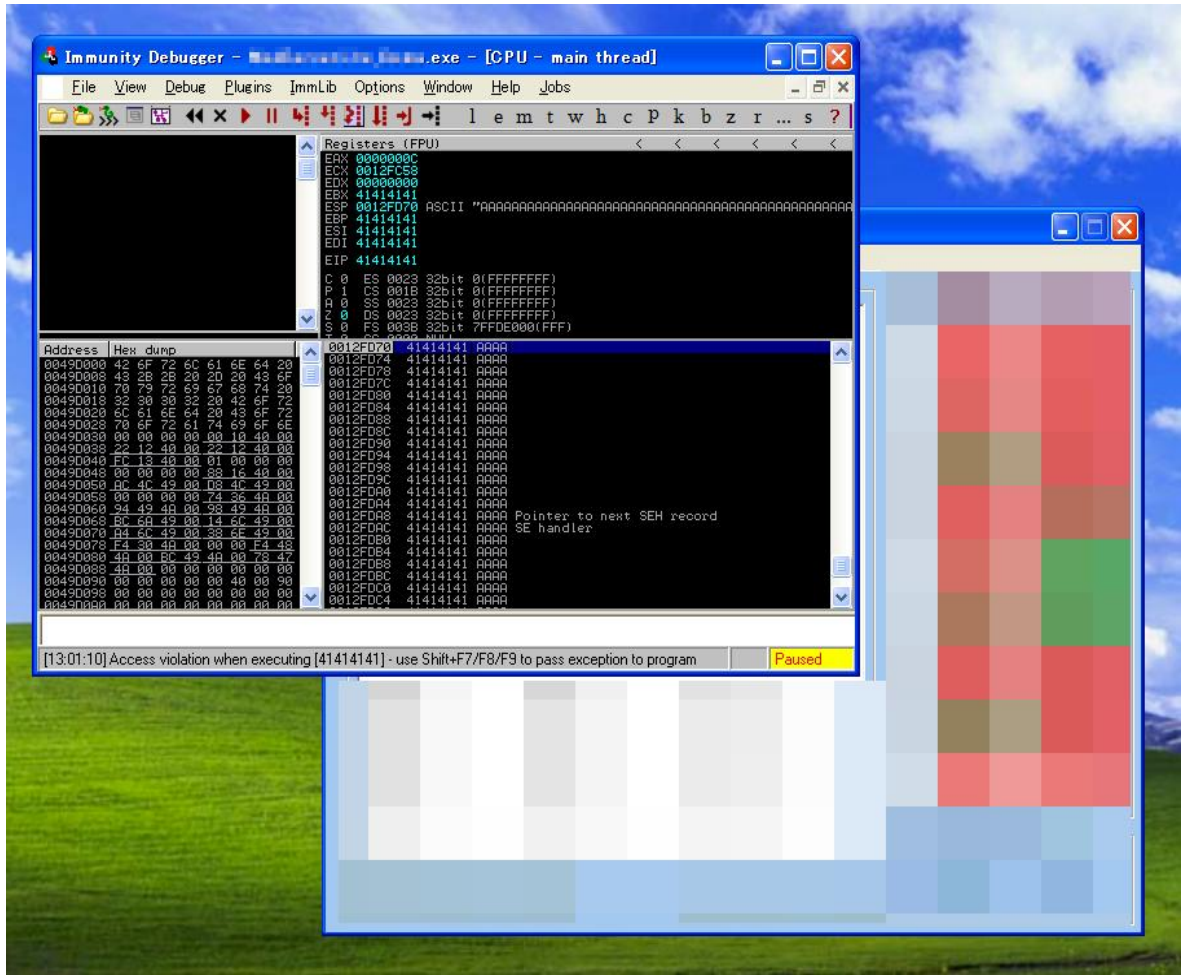
CyberDefense



Modbusサーバの脆弱性

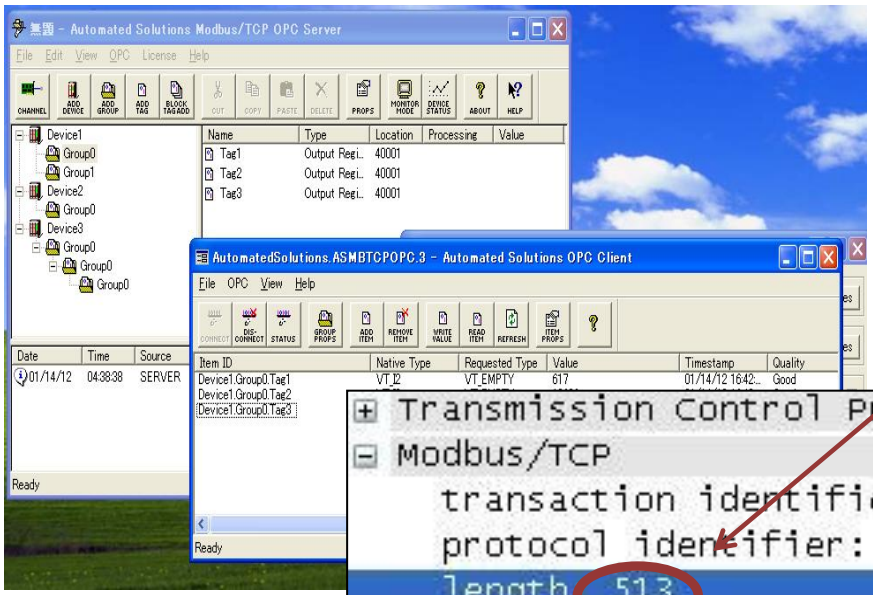
CyberDefense

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

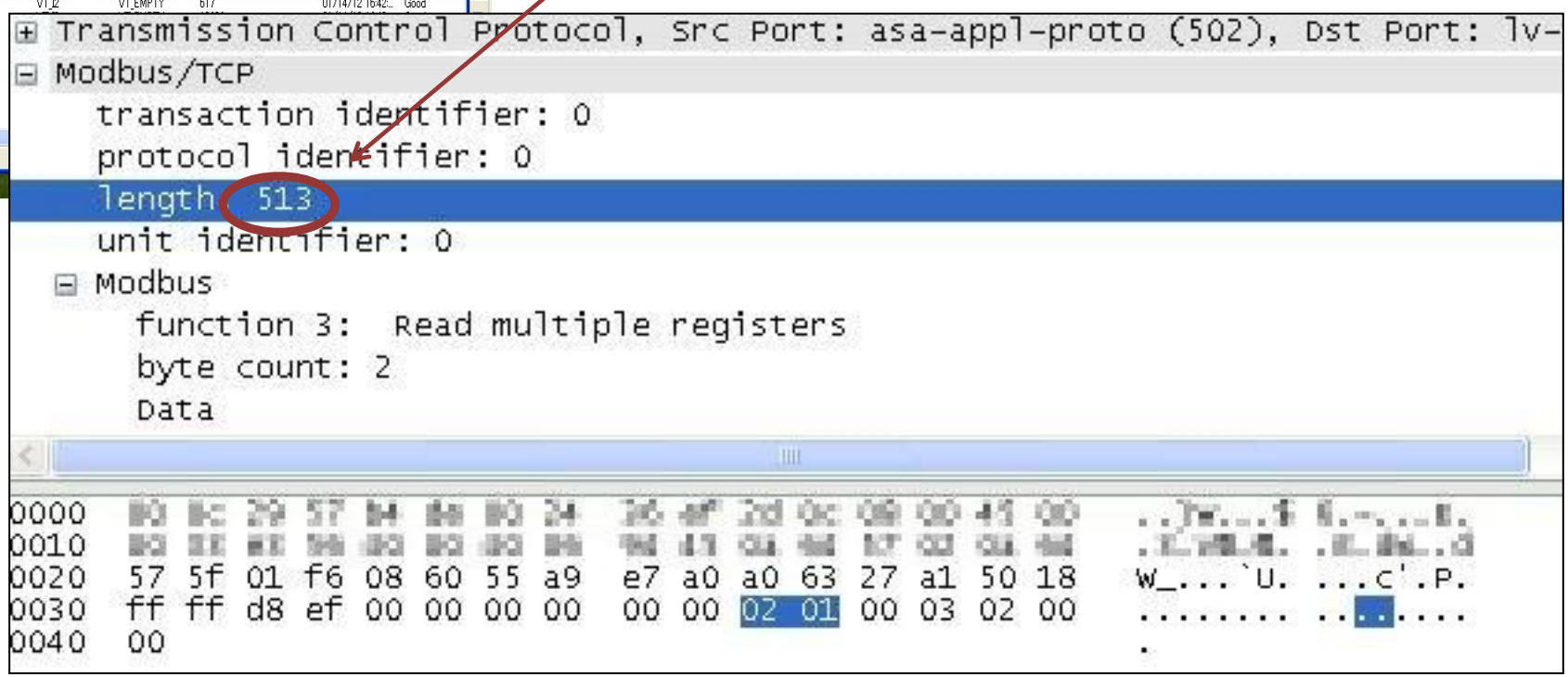


Modbusクライアントの脆弱性

CyberDefense



実際よりも長いlengthを指定することで
クラッシュ



PLCによくある脆弱性

CyberDefense

- 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)

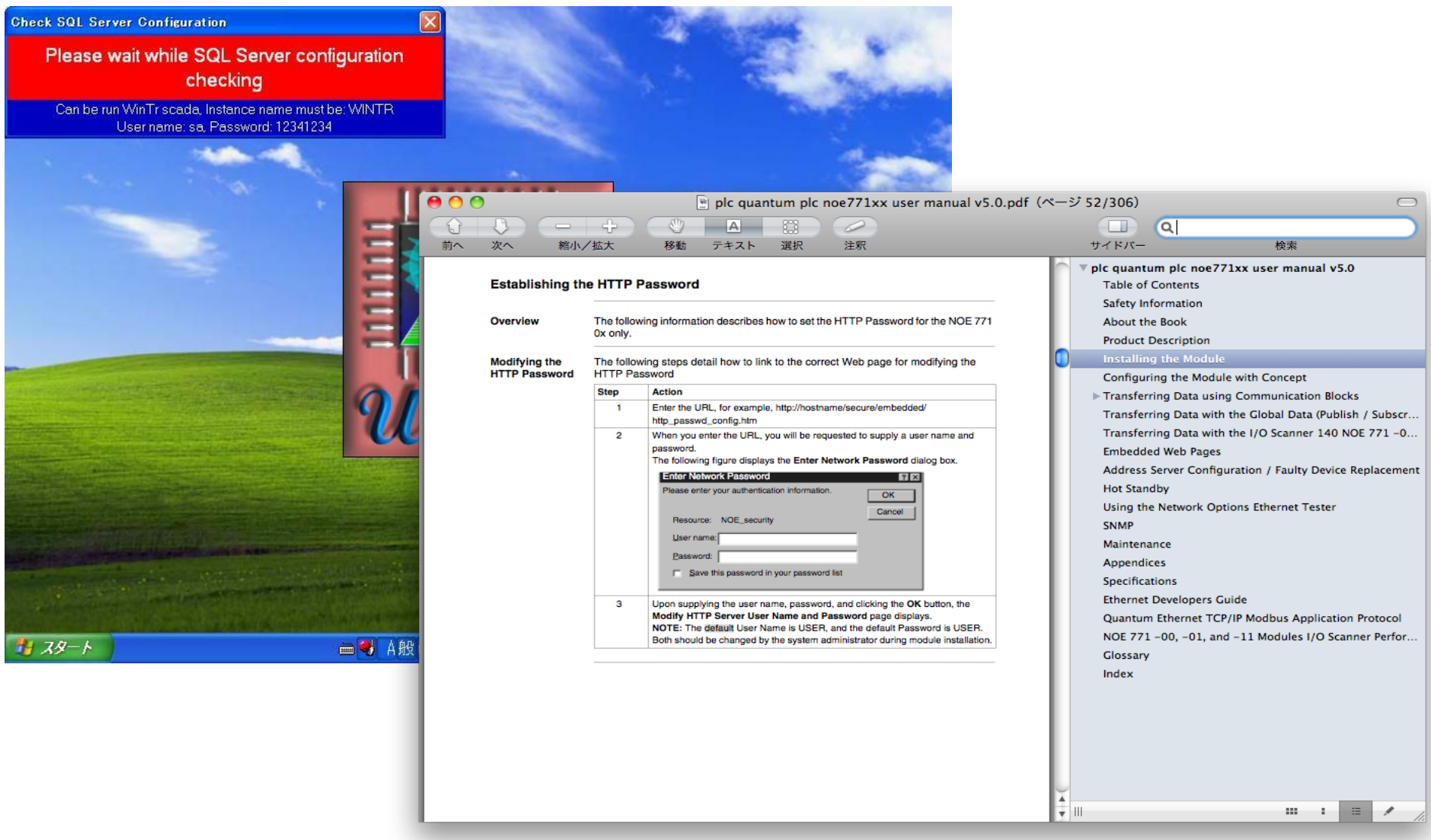
CyberDefense

- 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

引用元：http://www.automation.siemens.com

使われ続けるデフォルト設定

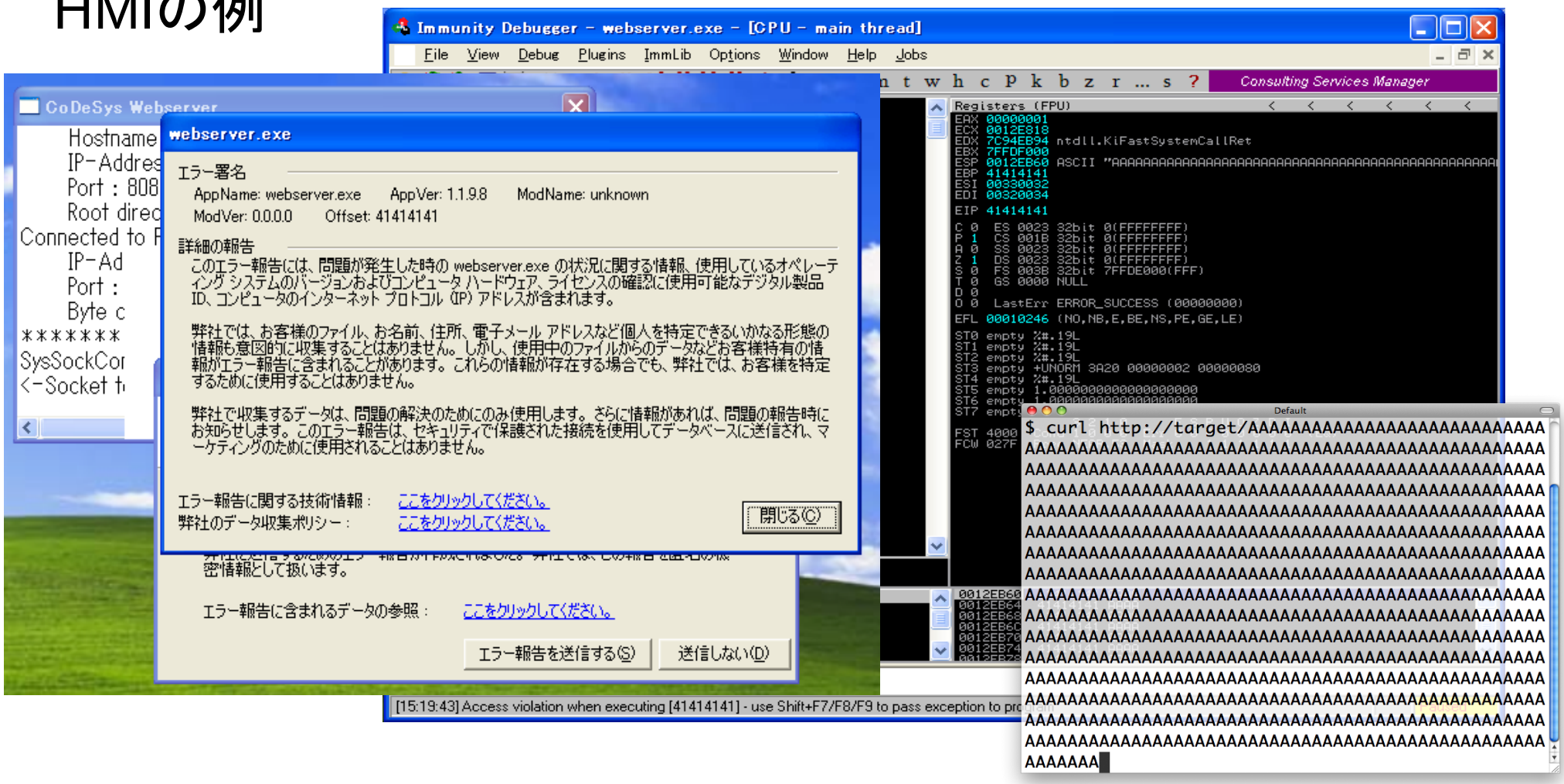
CyberDefense



バッファオーバーフローにより任意のコマンドを実行可能

CyberDefense

HMIの例



制御システムにおける
バッファオーバーフローの特徴

CyberDefense

- 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

CyberDefense

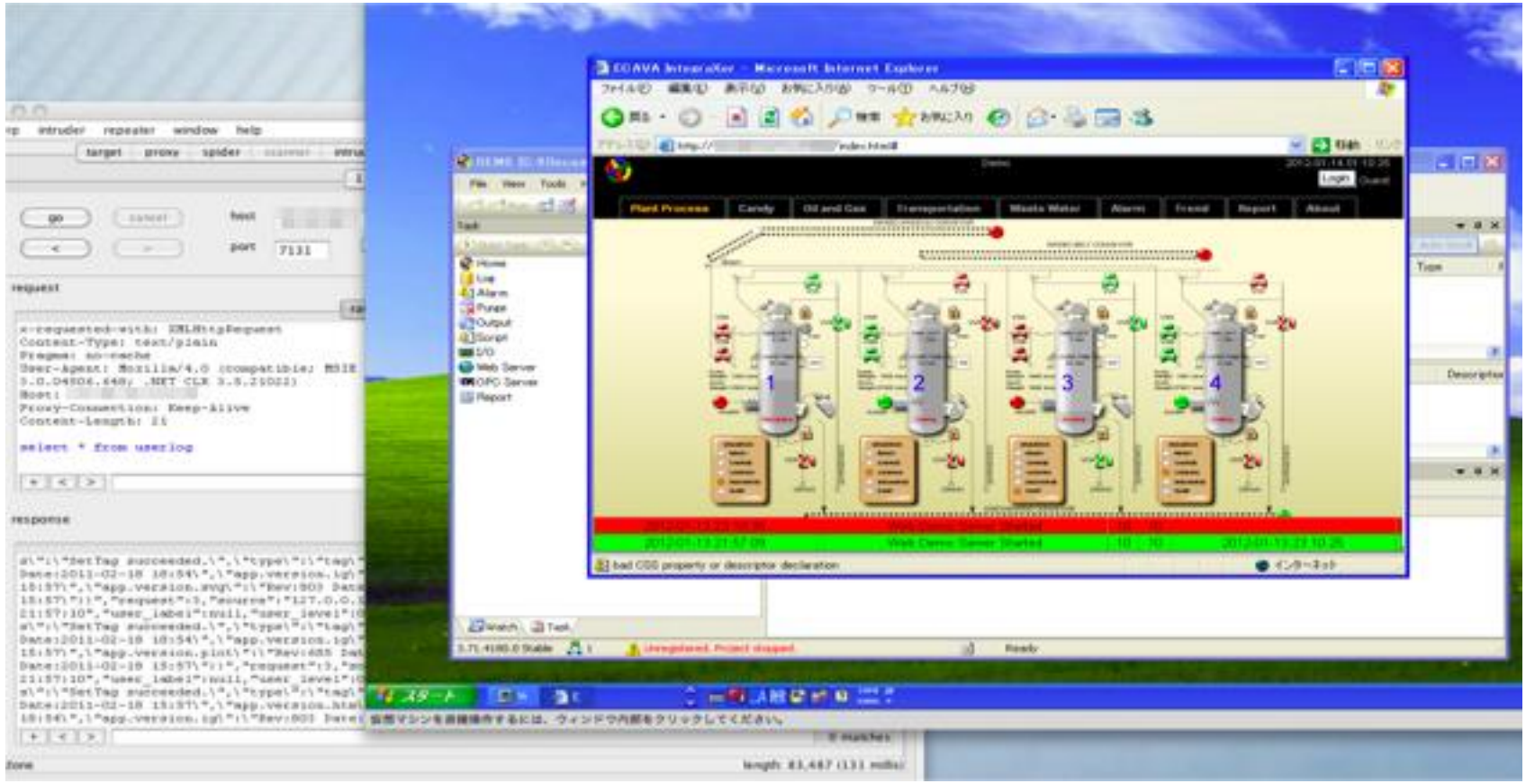
- Webサーバ
- FTPサーバ
- SQLサーバ
- ODBC接続
- 独自プロトコルのサーバ

SQLインジェクション(?) in AJAX

CyberDefense

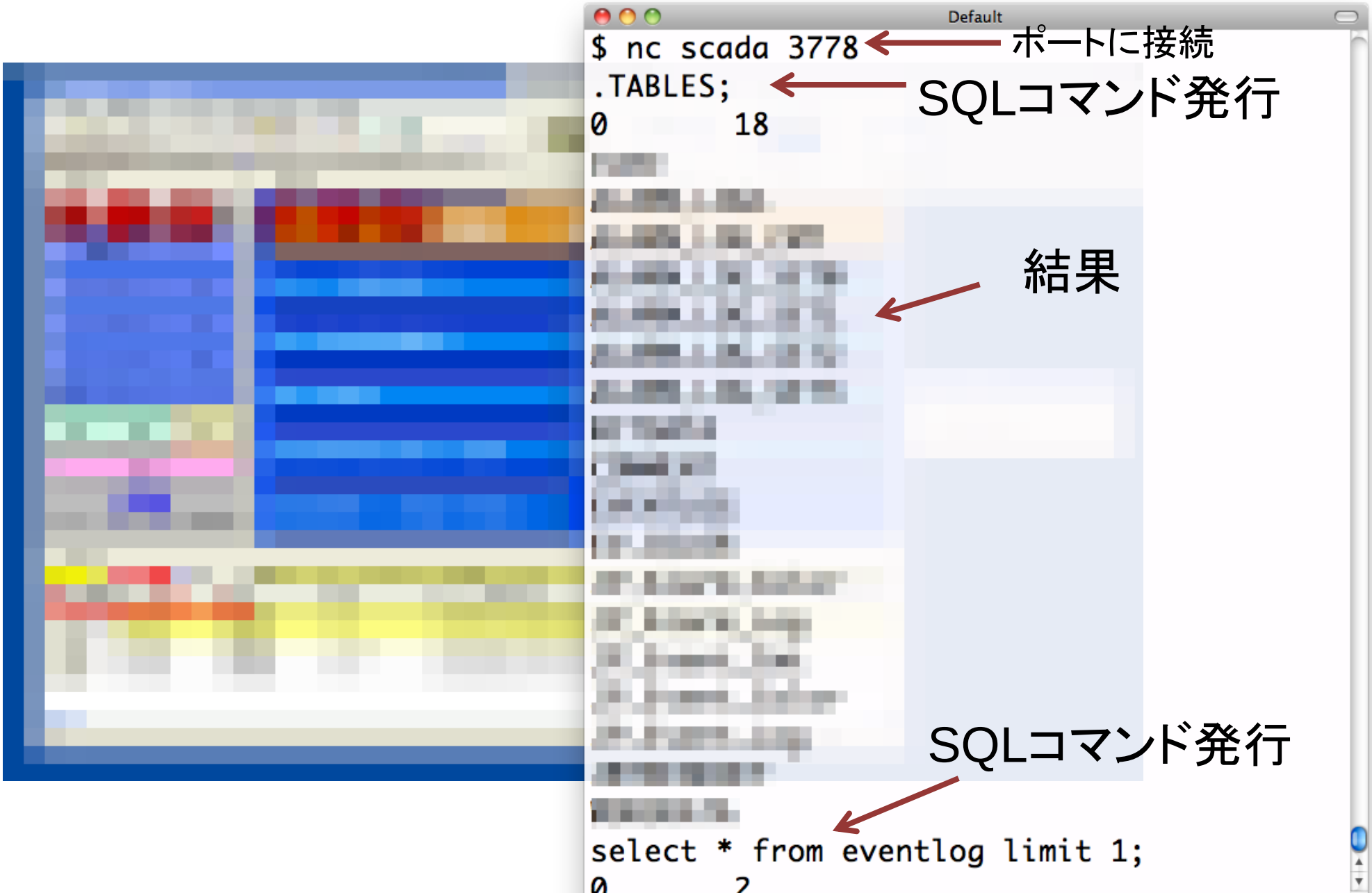
SQLコマンド

結果



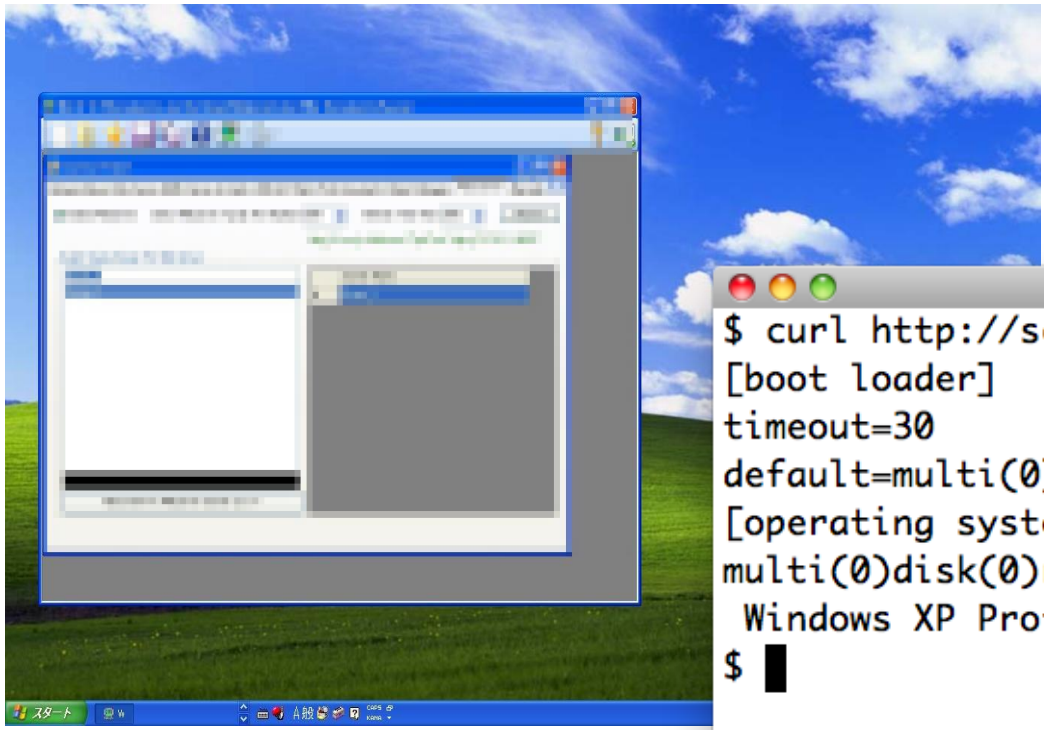
SQLインジェクション(?) in サーバ

CyberDefense



ディレクトリトラバーサル in Webサーバ その1

CyberDefense



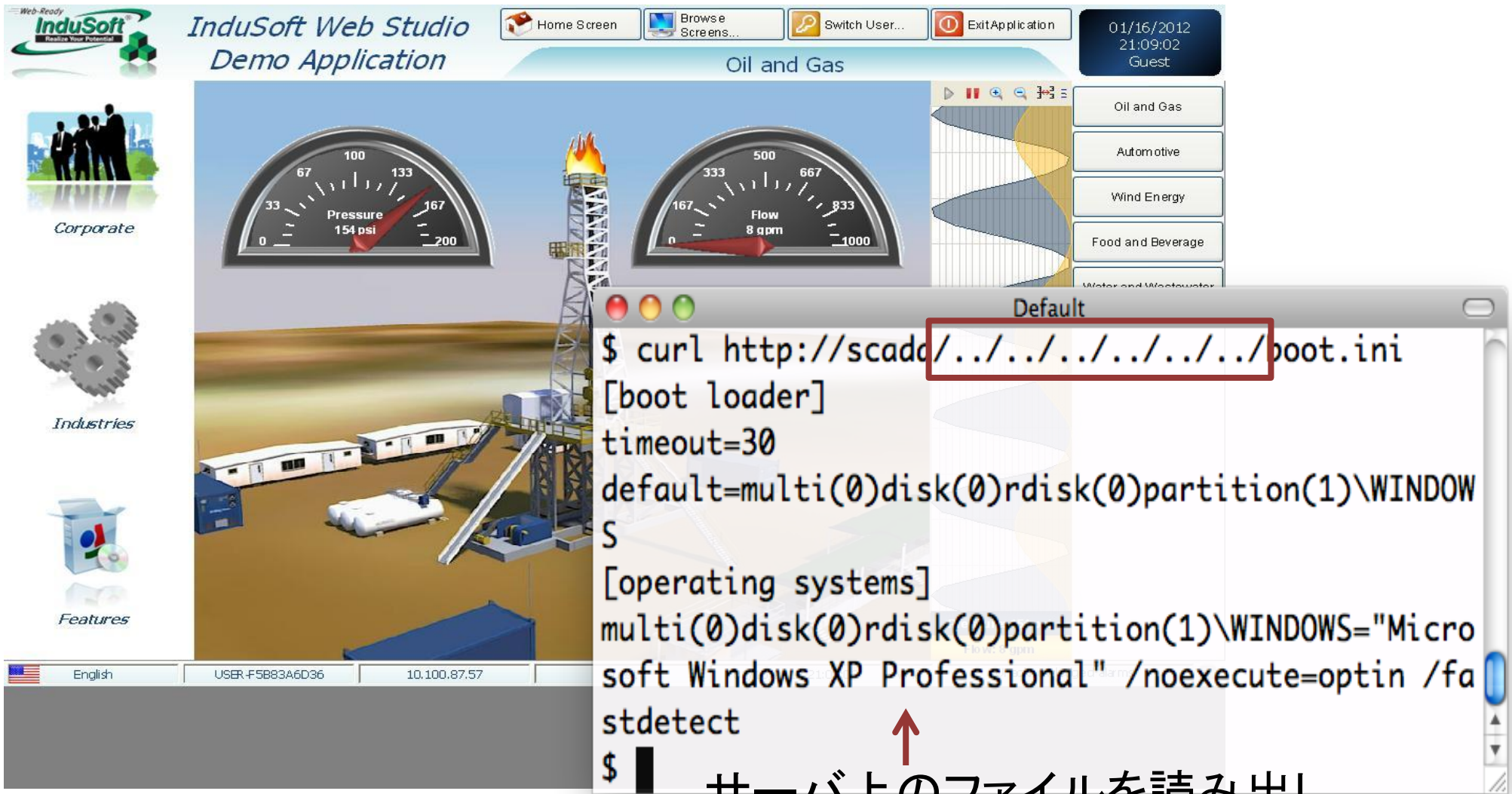
Default

```
$ 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

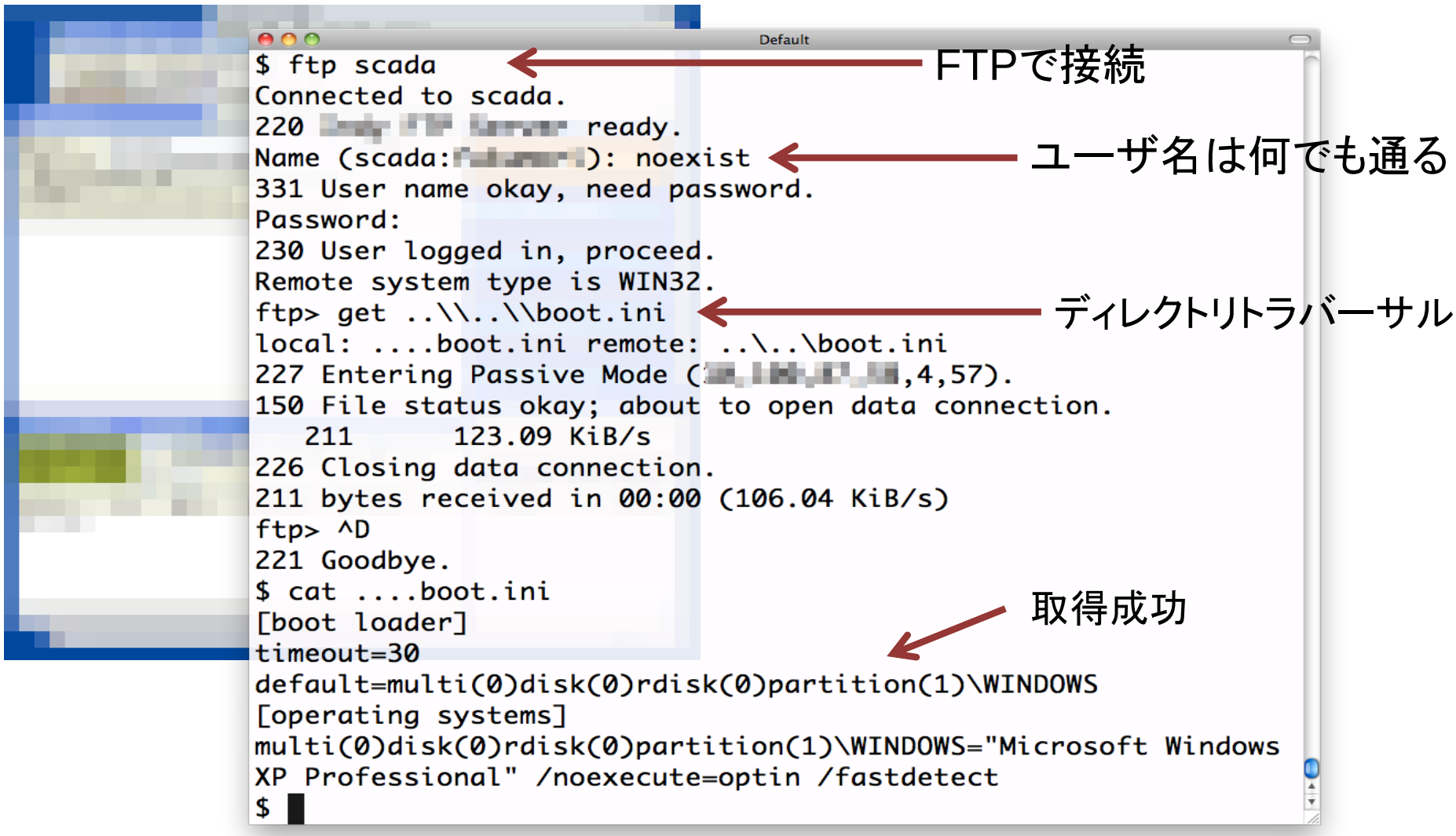
ディレクトリトラバーサル in Webサーバ その2

CyberDefense



ディレクトリトラバーサル in FTPサーバ

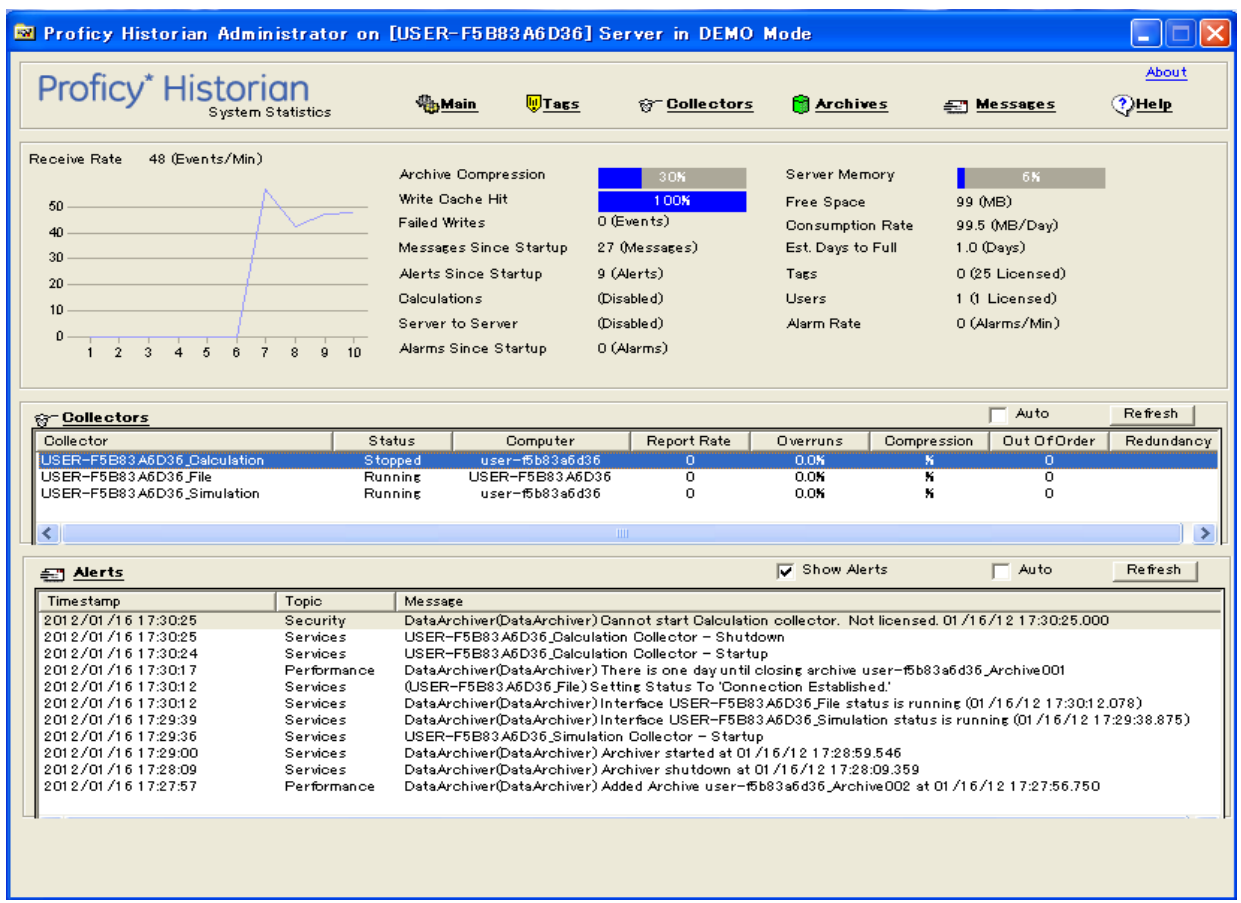
CyberDefense



GE製品にも同様の脆弱性

CyberDefense

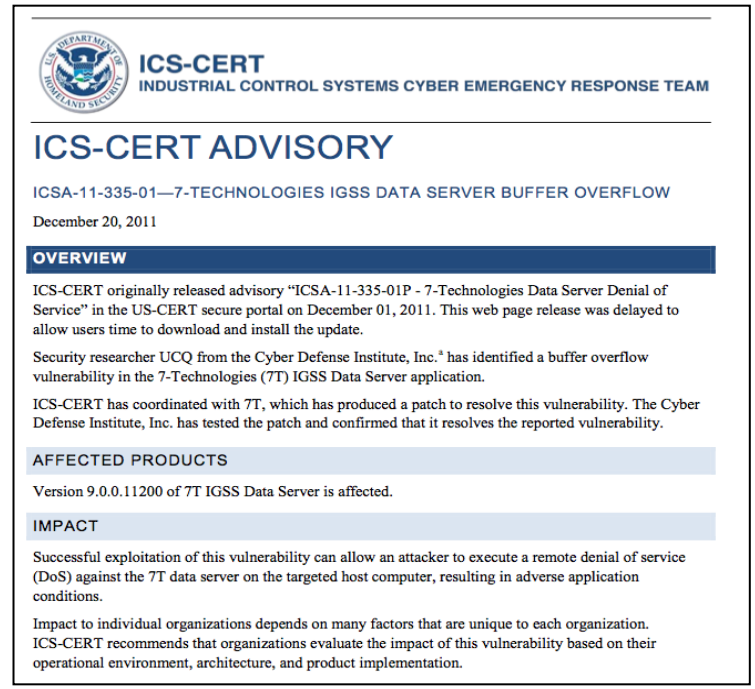
- CVE-2008-0175
- GE Fanuc Proficy Real-Time Information Portal



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

CyberDefense

- UCQによる届け出
- ICSA-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.[a] 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

CyberDefense

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

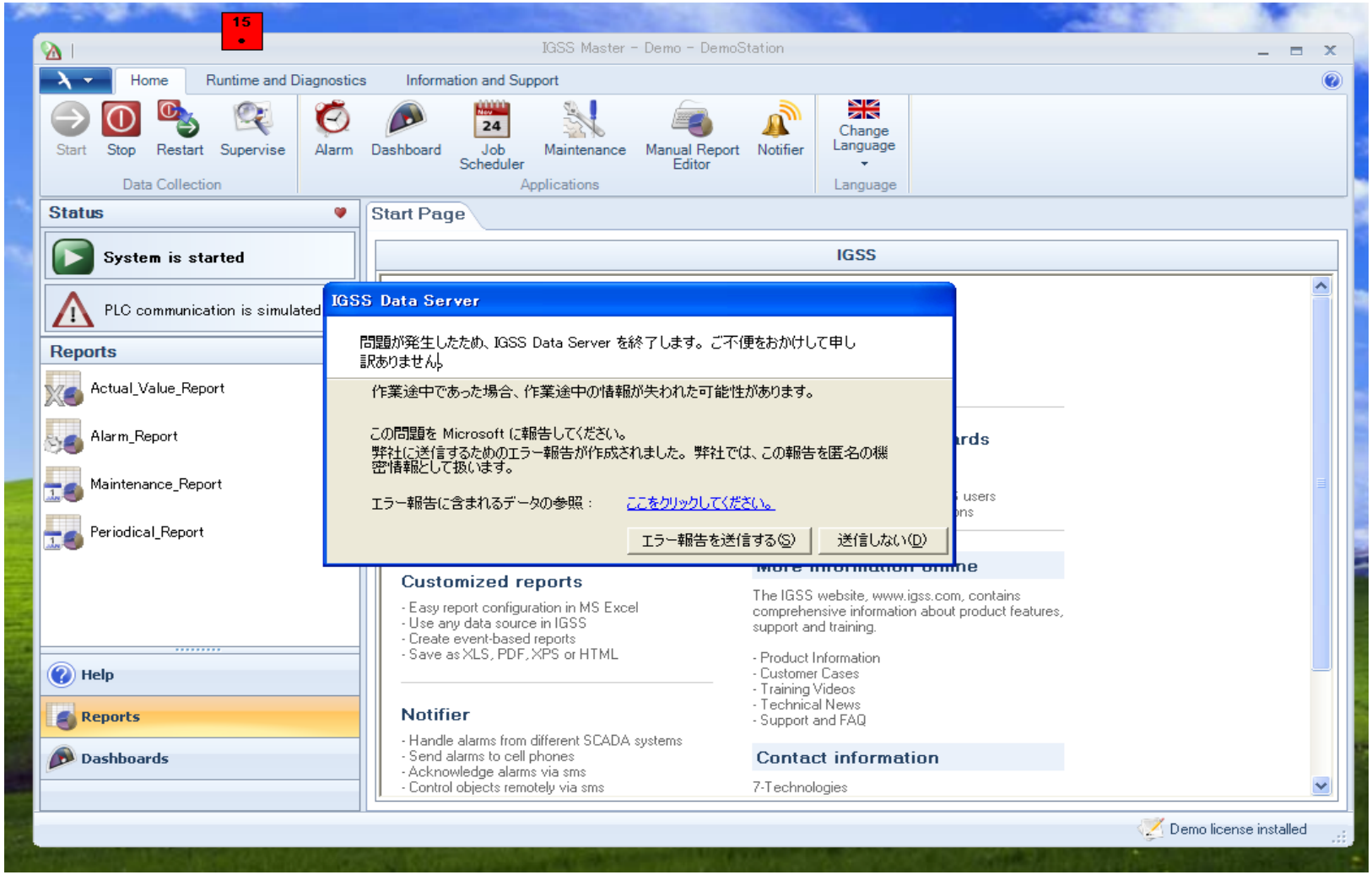
- Request Online
- Request Log
- Request BCL
- Request HDM
- Request ELM
- Request CMDSTAT
- Request RMS
- Request STDREP
- Request ALM
- Request ALMTXT
- Request USERS
- Request DESCR
- Request general file
- Request alarm Note

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)

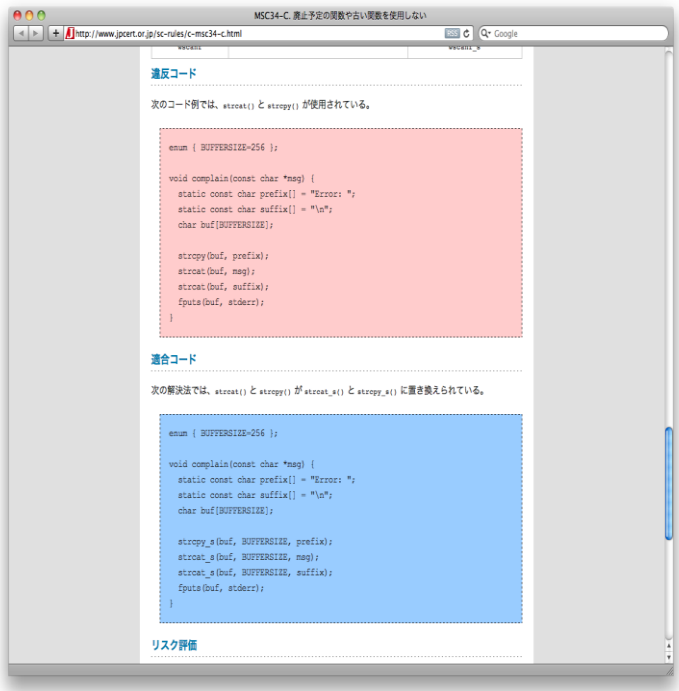
CyberDefense



発想

CyberDefense

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

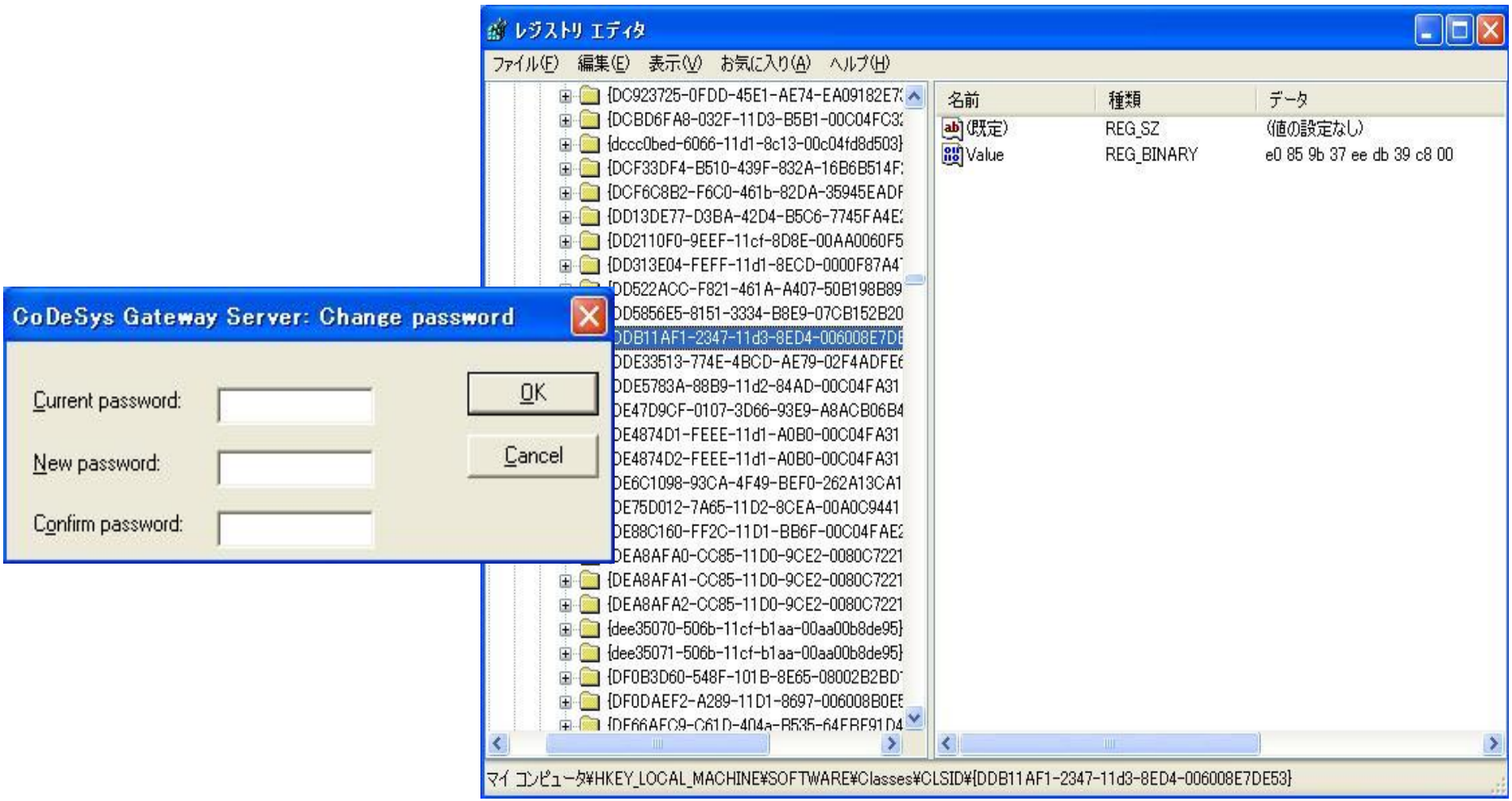


strcpyの危険性については
詳しく解説しているが、
その他の関数については
それほど説明が無い

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-msc34-c.html

パスワードリセット

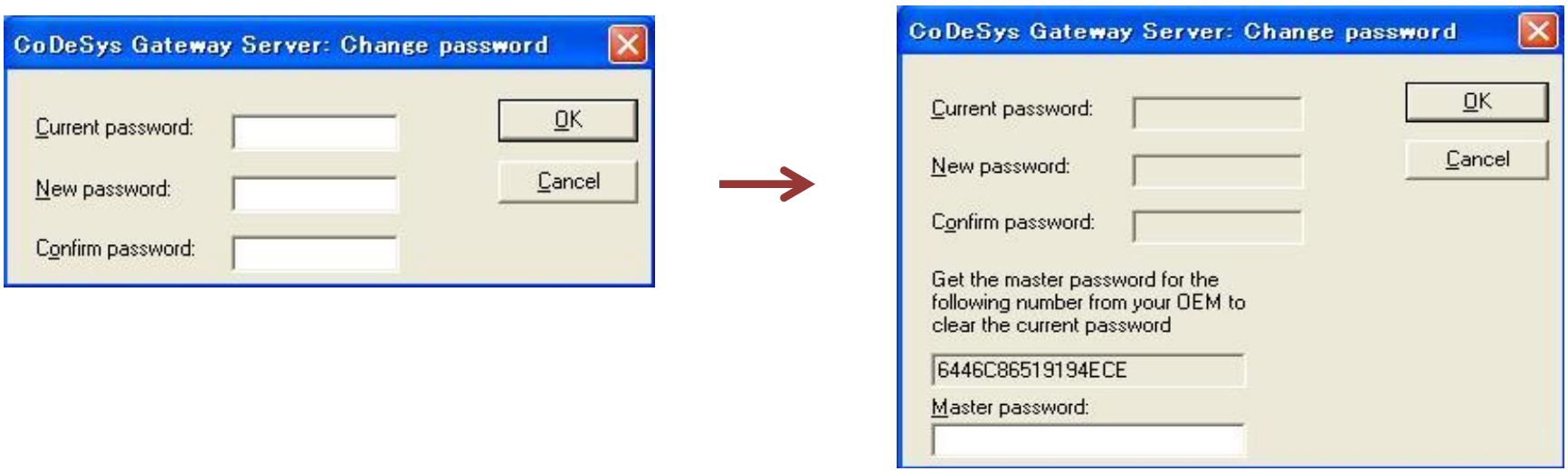
CyberDefense



その他の「仕様」

CyberDefense

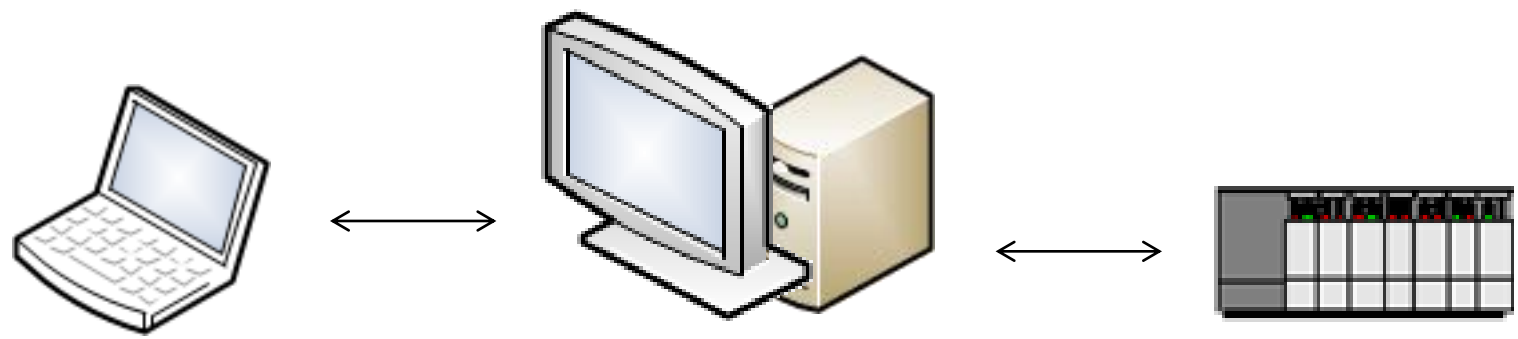
- ポートに接続すれば、ファイル取得、編集、レポート入手、等の命令発行が可能
- とあるキーを入力するとデバッグモードに移行



クライアント側の脆弱性

CyberDefense

- ActiveX
- ファイルの読み込み

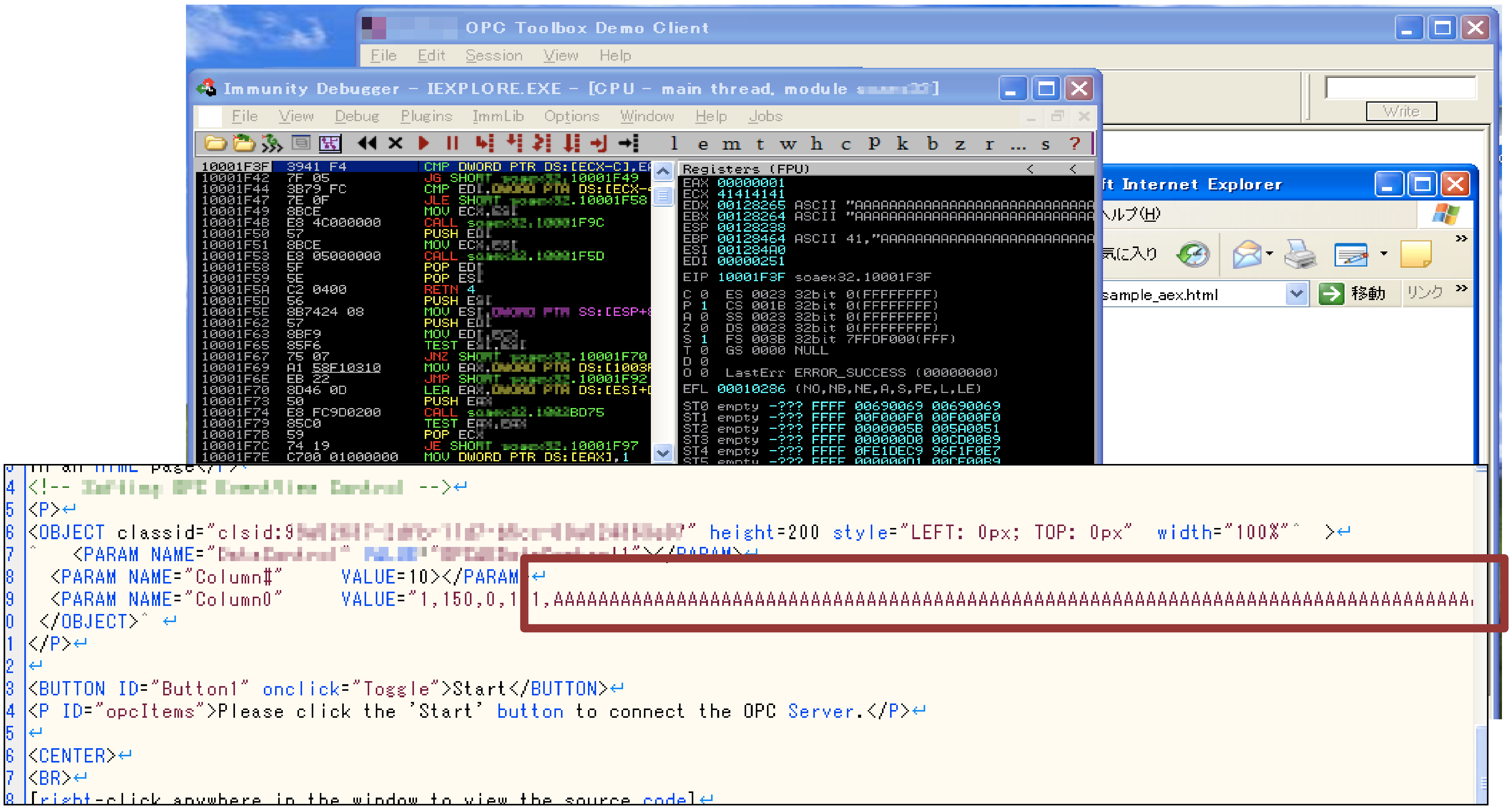


ActiveX

CyberDefense

- 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



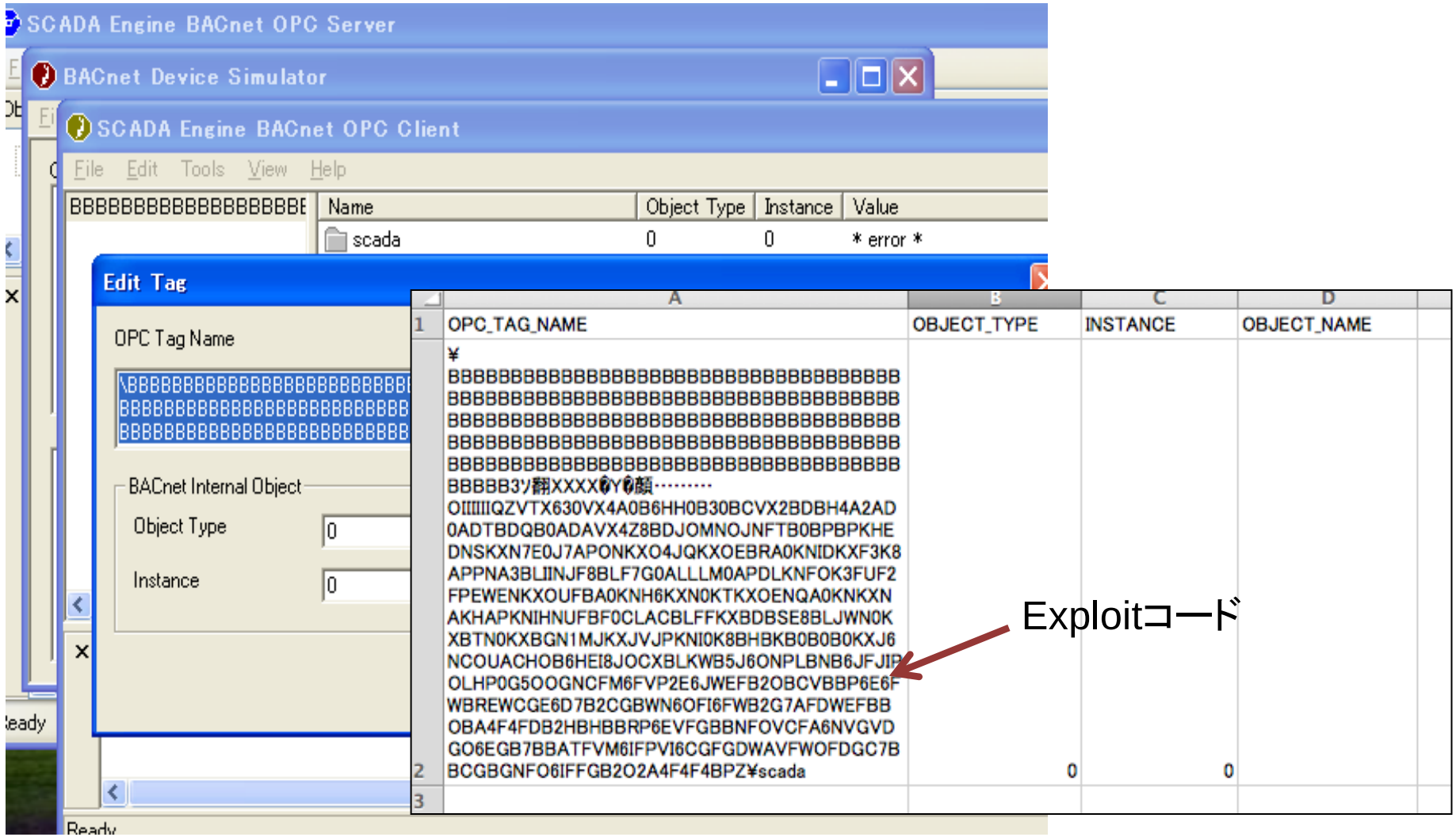
仕様で実装されていた命令

CyberDefense

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

BACnet OPCクライアントでのファイルの読み込み

CyberDefense



スマートメーター

CyberDefense

- 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

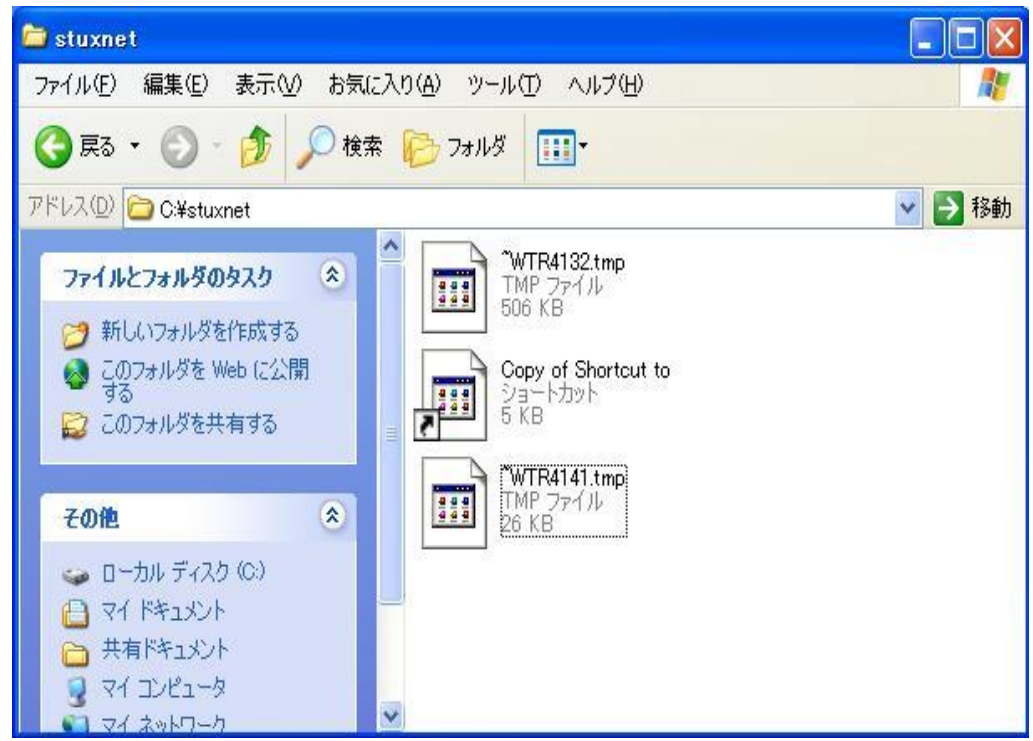
スマートメーターに存在した脆弱性

CyberDefense

- 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

CyberDefense

間違いだらけの Stuxnet対策



Stuxnetに対する　よくある誤解

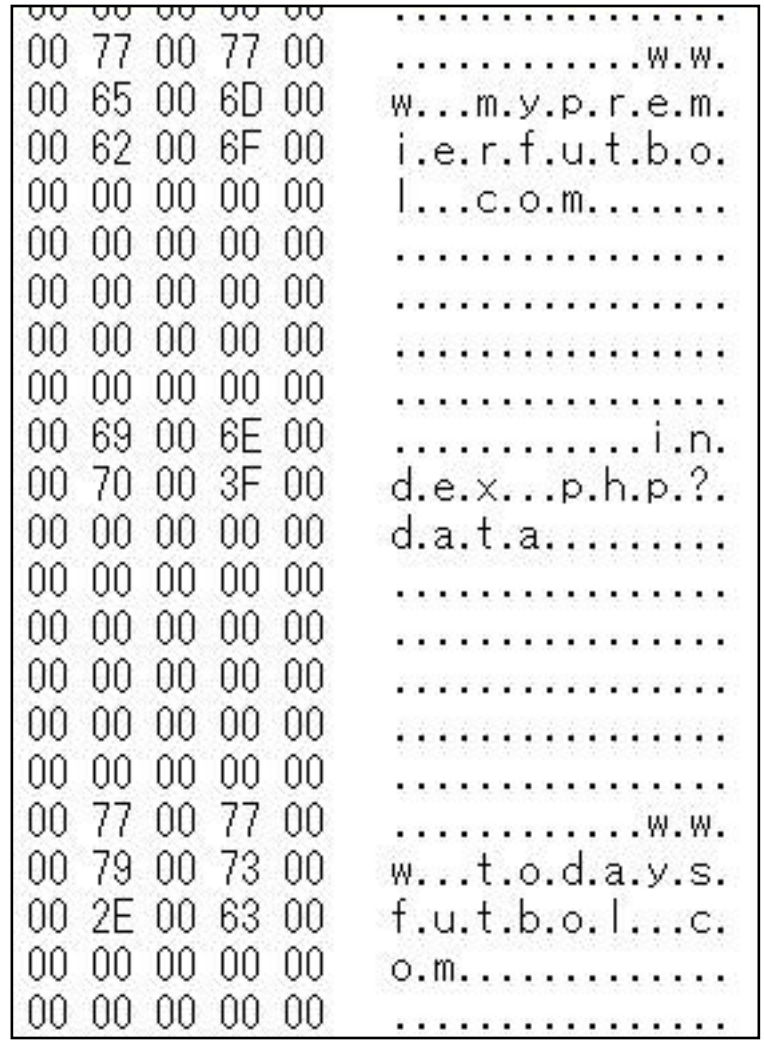
CyberDefense

- 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

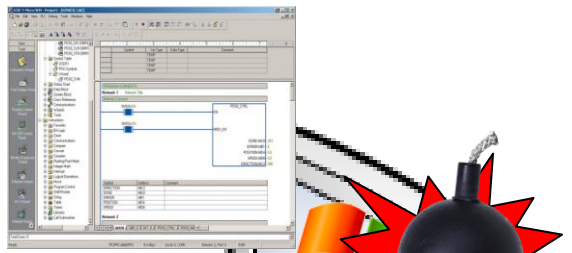
CyberDefense

- 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

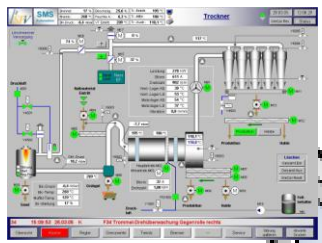


攻撃された場所

CyberDefense



Step7



WinCC

Profibus-DP

PLC

S7-315-2
S7-417

WinCC SQLのデフォルトパスワードを使って感染を広げる

CyberDefense

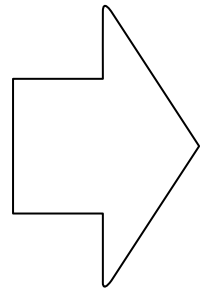
```
mov     esi, ecx
call    sub_1001B332
and     dword ptr [ebp-4], 0
push    3Ch
push    offset a2wsxcder ; "2WSXcder"
push    offset aWinccconnect ; "WinCCConnect"
push    offset aMaster  ; "master"
push    offset a_Wincc  ; ".¥¥WinCC"
push    offset aSqloledb ; "sqloledb"
lea     eax, [ebp-38h]
push    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

CyberDefense

```
4B4 unk_1003A4B4     db 0FBh ; ◁
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 ; ¡
4C2                  db 0F0h ; ◁
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

CyberDefense

- 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

CyberDefense

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