

家庭の冷蔵庫があなたへの陰謀を企てている？ IoT攻撃と組み込み防御

セッションID: JPN-W05

Wolfgang Kandek

Chief Technical Officer
Qualys
@wkandek



About:Me @WKANDEK

- ◆ Qualys – CTO
 - ◆ Responsible for Research and Outreach
 - ◆ Laws of Vulnerabilities
 - ◆ Half-life, Prevalence, Persistence, Exploitation
- ◆ Blog: Laws of Vulnerabilities
 - ◆ <https://laws.qualys.com>
- ◆ Twitter: @wkandek



自己紹介 @XSSNIPER

- ◆ Qualys - 脆弱性調査および脅威インテリジェンス担当ディレクター
- ◆ Google - Technical Lead and Security for Google Plus
- ◆ Microsoft - Technical Lead in Security
- ◆ 書籍：
 - ◆ 「Hacking: The Next Generation」 – O'Reilly
 - ◆ 「Inside Cyber Warfare」 – O'Reilly
 - ◆ 「The Virtual Battlefield」 – IOS Press
- ◆ ICS脆弱性調査：
 - ◆ ICS-CERTアドバイザリの公的な30単位を取得
 - ◆ 1,000件を超える個々の問題がDHSに報告された



2013年とIoTセキュリティを振り返ります





「2013年12月23日から 2014年1月 6日の
間に発生した大規模な攻撃では、
75万通を超える不正なメール
通信が行われました」



Hacked baby monitor alerts parents to dangers

See also [Behavior & Discipline](#) / [Parenting](#) / [Baby Monitors](#) / [Baby & Toddler](#) / [Strange News](#)



Aleksandr Kutsayev/freedigitalphotos.net



August 13, 2013

A hacker's voice was heard through a baby monitor located in the child's bedroom by distraught parents in Houston. The menacing voice was trying to wake the 2-year-old up with curse words then targeted expletives at the parents when they entered the toddler's room, according to a report from [ABC News](#) on Aug. 13.

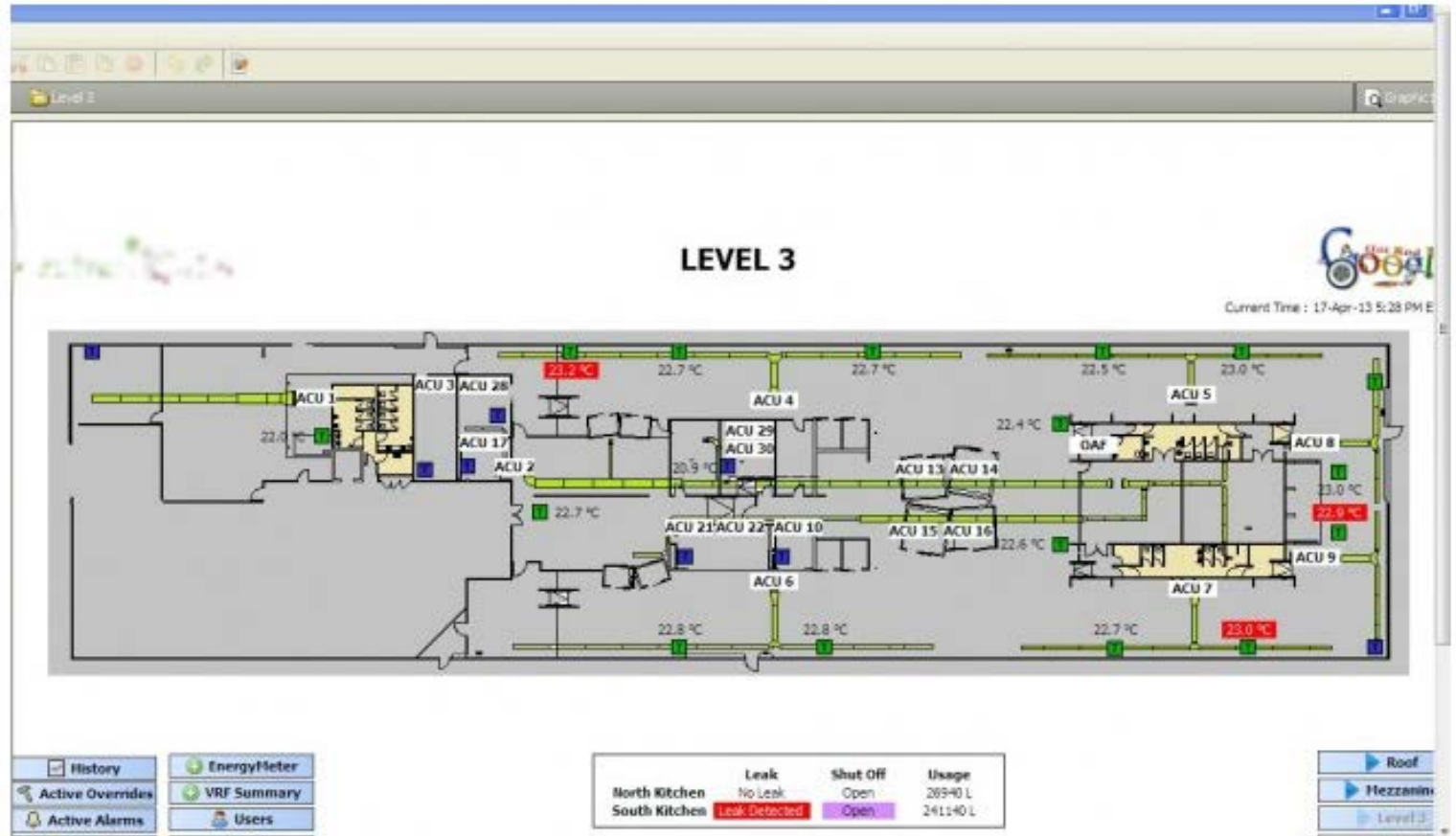
「夜中に娘のエマに対して大声をあげる男の声で目が覚め、
驚いたことにインターネット対応のベビー
モニターが動いているのを発見した。
自分たちが動かしているわけではないのに。」

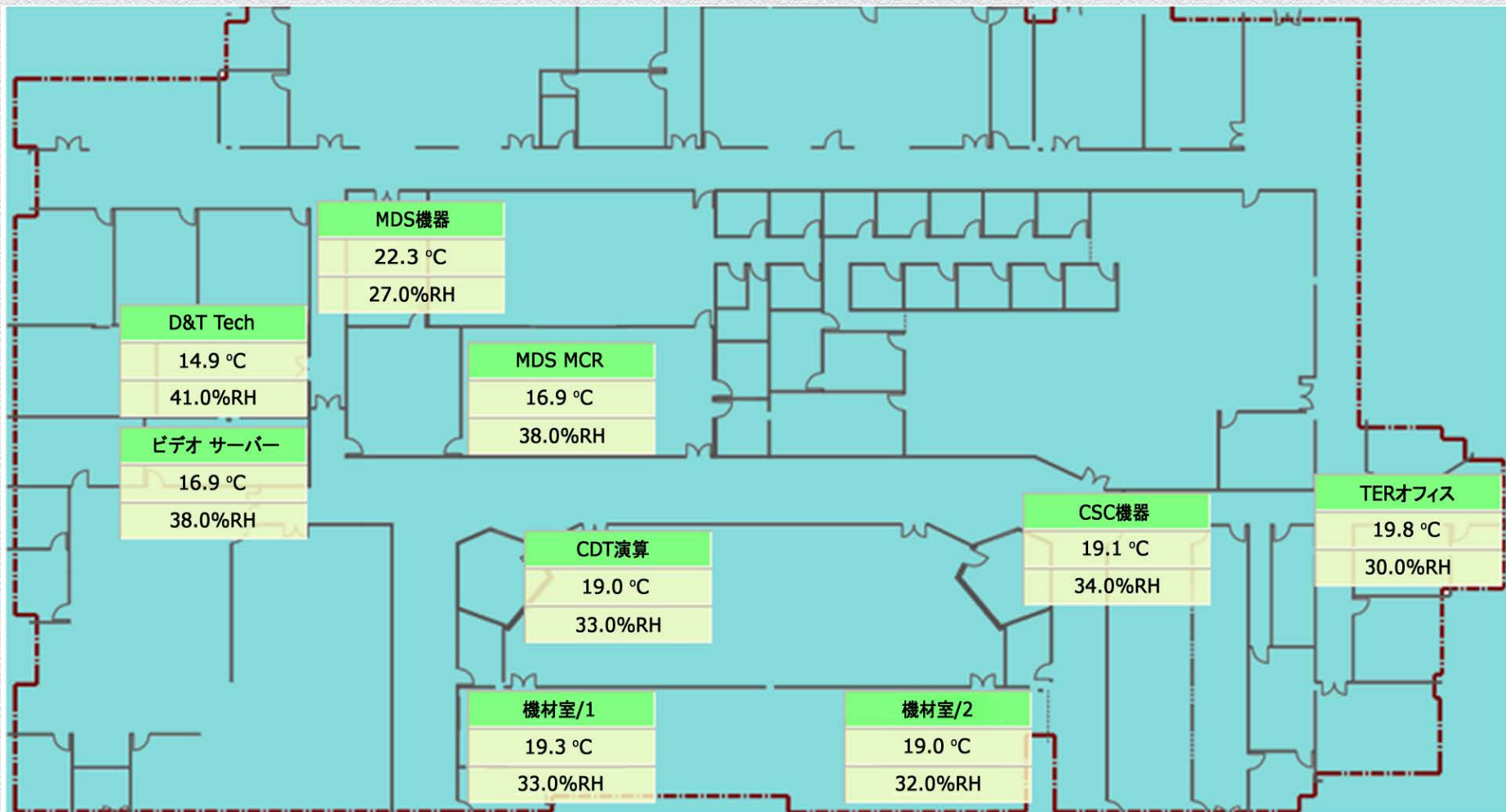


Researchers Hack Building Control System at Google Australia Office

BY KIM ZETTER 05.06.13 | 6:30 AM | PERMALINK

[f Share](#) 0 [t Tweet](#) 1 [g+1](#) 85 [in Share](#) [Pin it](#)





PR5

PR5-D01	
PR5-D01	Closed
PD25#10	Closed
PD36#4	Closed
PD12#7	Closed
PD12#11	Closed
PD12#13	Closed
PD12#14	Closed
PD12#15	Closed
PD25#2	Closed
PD25#8	Closed

PR5-D02	
PR5-D02	Closed
PD6#9	Closed
PD6#12	Closed
PD36#1	Closed
PD42#5	Closed
PD48#6	Closed

PR5-T1	
PR5-T1	Closed
PT3#1	Closed
PT3#6	Closed
PT3#12	Closed
PT6#5	Closed
PT6#8	Closed
PT12#2	Closed
PT12#10	Closed
PT25#4	Closed
PT25#11	Closed

PR5-T2	
PR5-T2	Closed
PT25#9	Closed
PT36#7	Closed
PT42#3	Closed
PT3	Open

PR5-UPS1	
PR5-UPS1	Closed
PU42#6	Closed
PU42#4	Closed
PU36#8	Open
RESERVA	Open
PU12#7	Closed
PU12#5	Closed
PU25#3	Closed
PU25#2	Closed
PU12#3	Open

PR5-UPS2	
PR5-UPS2	Closed
PU30#10	Closed
PU3#13	Closed
PU25#12	Closed
PU12#11	Closed
PU25#9	Closed
PU6#1	Open
PT3#2	Open
PT3#4	Open
PT12#2	Open
PU3#1	Closed
PU12#1	Closed
RESERVA	Open




```
<signature> [REDACTED] /s
signature>
</license></resp>
You looked up the license for: [REDACTED]
This license was generated on: [REDACTED]
The license vendor is: [REDACTED]
The license is for version: [REDACTED]
This license expires on: never
This device is owned by: OBS
The project for this device is: Olympic Broadcasting
```

```
id=i:6670
hostname=s: LAInstallations
hostAddress=s:[REDACTED]
app.name=s:[REDACTED]
app.version=s:[REDACTED]
vm.name=s:Java Hotspot(TM) 64-Bit Server VM
vm.version=s:23.7-b01
os.name=s:Windows 7
os.version=s:6.1
station.name=s: SOCHI_ARENA
lang=s:en
timeZone=s:Europe/Moscow:14400000;0>null>null
hostId=s:[REDACTED]
vmUuid=s:[REDACTED]
brandId=s:[REDACTED]
sysInfo=o:[REDACTED]
```





ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



HOME

ABOUT

ICSJWG

INFORMATION PRODUCTS

TRAINING

FAQ

Control Systems

Home

Calendar

ICSJWG

Information Products

Training

Recommended Practices

Assessments

Standards & References

Related Sites

FAQ

Alert (ICS-ALERT-13-164-01)

[More Alerts](#)

Medical Devices Hard-Coded Passwords

Original release date: June 13, 2013 | Last revised: October 29, 2013



Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

SUMMARY

Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware.

Because of the critical and unique status that medical devices occupy, ICS-CERT has been working in close cooperation with the Food and Drug Administration (FDA) in addressing these issues. ICS-CERT and the FDA have notified the affected vendors of the report and have asked the vendors to confirm the vulnerability and identify specific mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks. ICS-CERT and the FDA will follow up with specific advisories and information as appropriate.



「ハードコードされたパスワードの
脆弱性の影響を受けるのは
ベンダー約40社にわたる
約300台の医療機器」



RSACONFERENCE2014
アジア太平洋地域および日本






#RSAC

RSACONFERENCE2014
アジア太平洋地域および日本

AMERICAN
AUTO-MATRIX®
SMART BUILDING SOLUTIONS®

 **QUALYS**
ON DEMAND SECURITY

 #RSAC
RSACONFERENCE2014
アジア太平洋地域および日本

WARNING
 This equipment must be isolated or disconnected from the mains before access.
USE COPPER CONDUCTORS ONLY

Model: 25-100-01-00
 Part No: 25-100-01-00
 Rev: 1.0

This equipment complies with FCC rules for a Class 'B' computing device.
 Operation is subject to the following two conditions:
 1. This device may not cause harmful interference.
 2. This device must accept any interference received, including interference that may cause undesired operation.
 This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.
 Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

UNIT NUMBER: _____
 P-XXXXXX

USE COPPER CONDUCTORS ONLY

COM 3 RS-485	COM 4 RS-485	COM 1 RS-232	COM 2 RS-232	COM 5 RS-485	COM 6 RS-485

S +





ECHELON
FTT-10A
50031R
T082AB

LA RE-MODCM
M025316-5110
P#850 L#3

RoHS
COMPLIANT

JACE 484
TRIDON

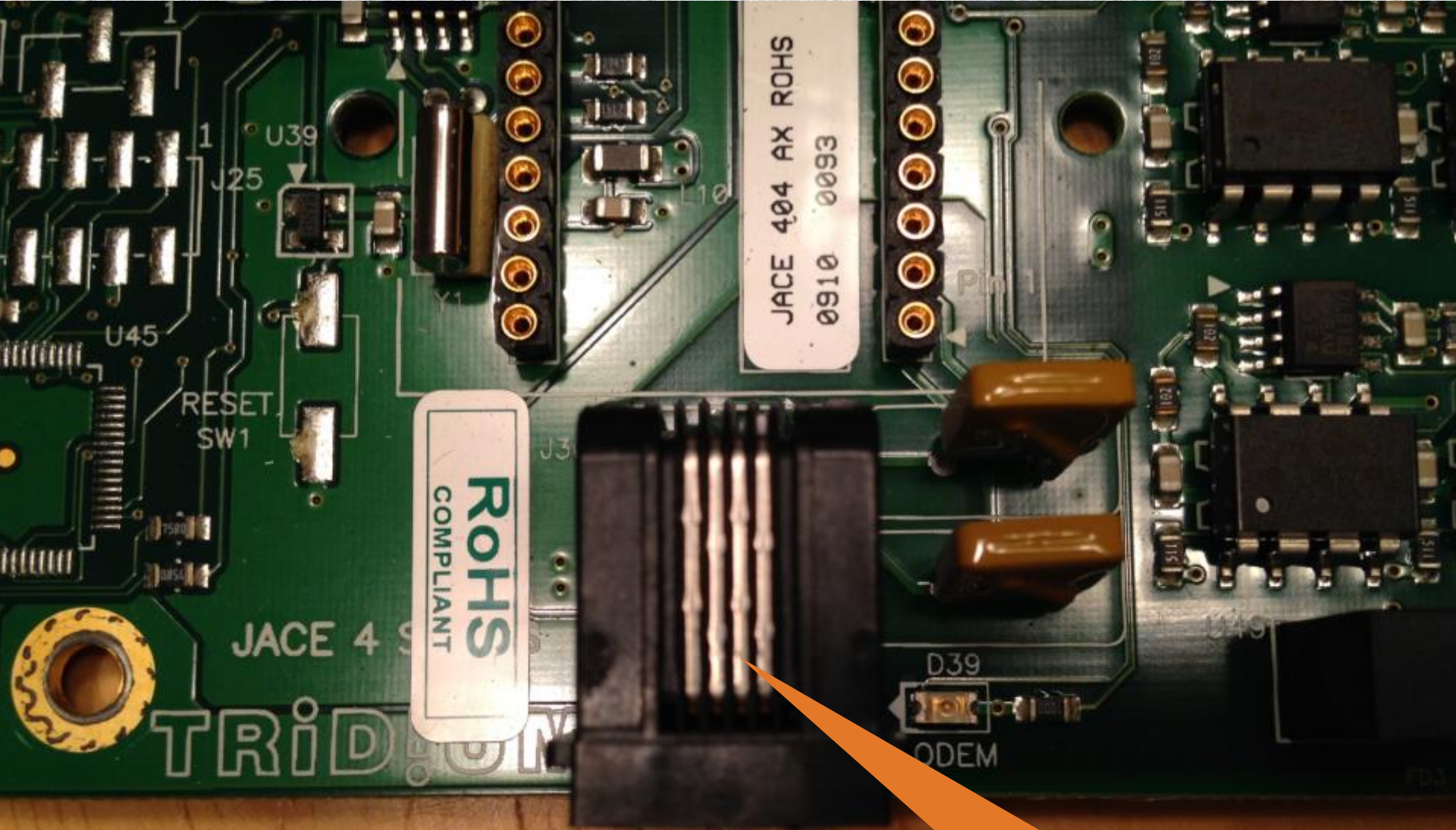
JACE 484 IN 20HS
0010 0003

INTERNAL MODEM



RJ WE-MIDCOM
MIC25310-5110
PV850 LF3

RJ45 – Ethernet

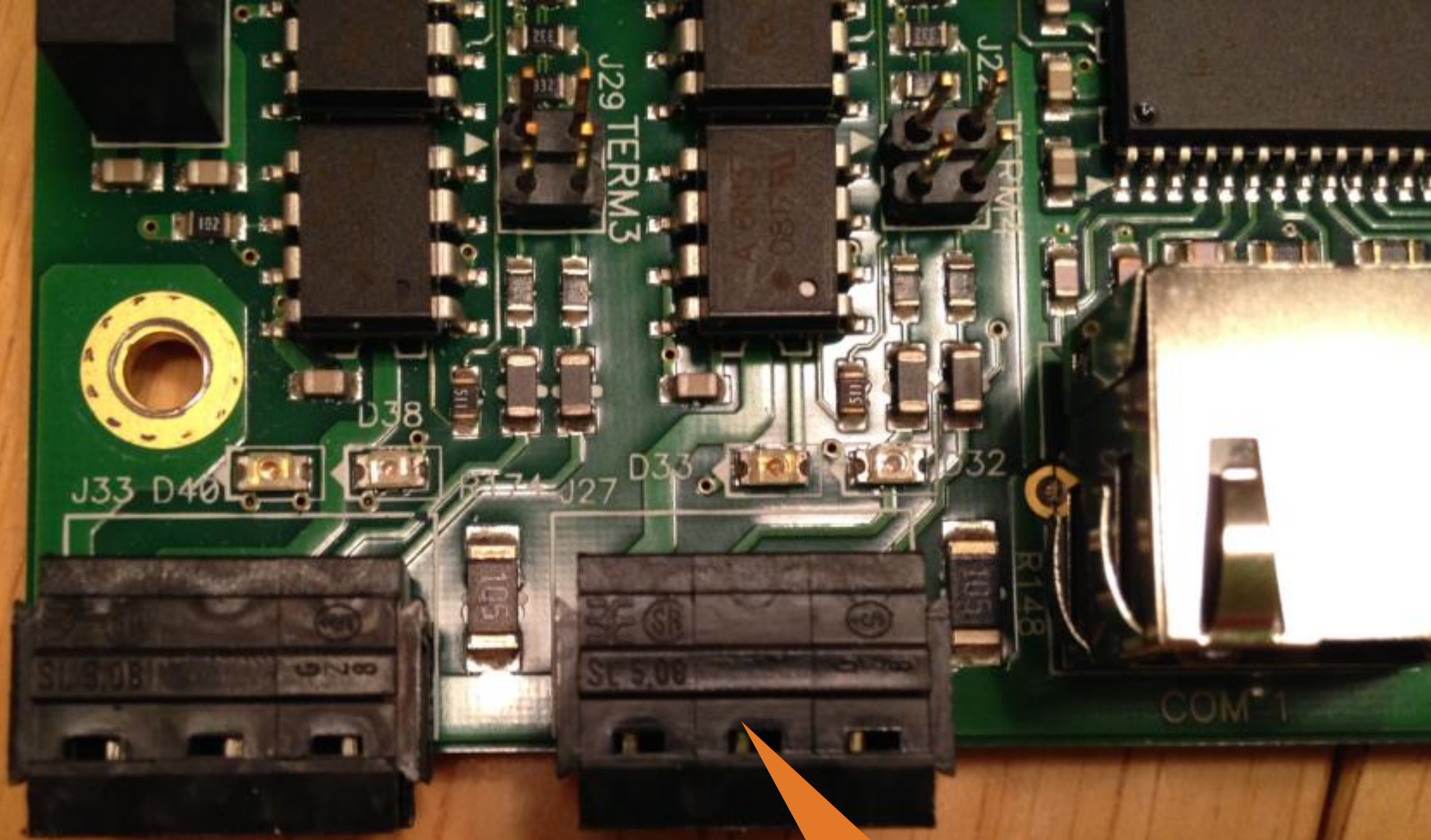


ROHS
COMPLIANT

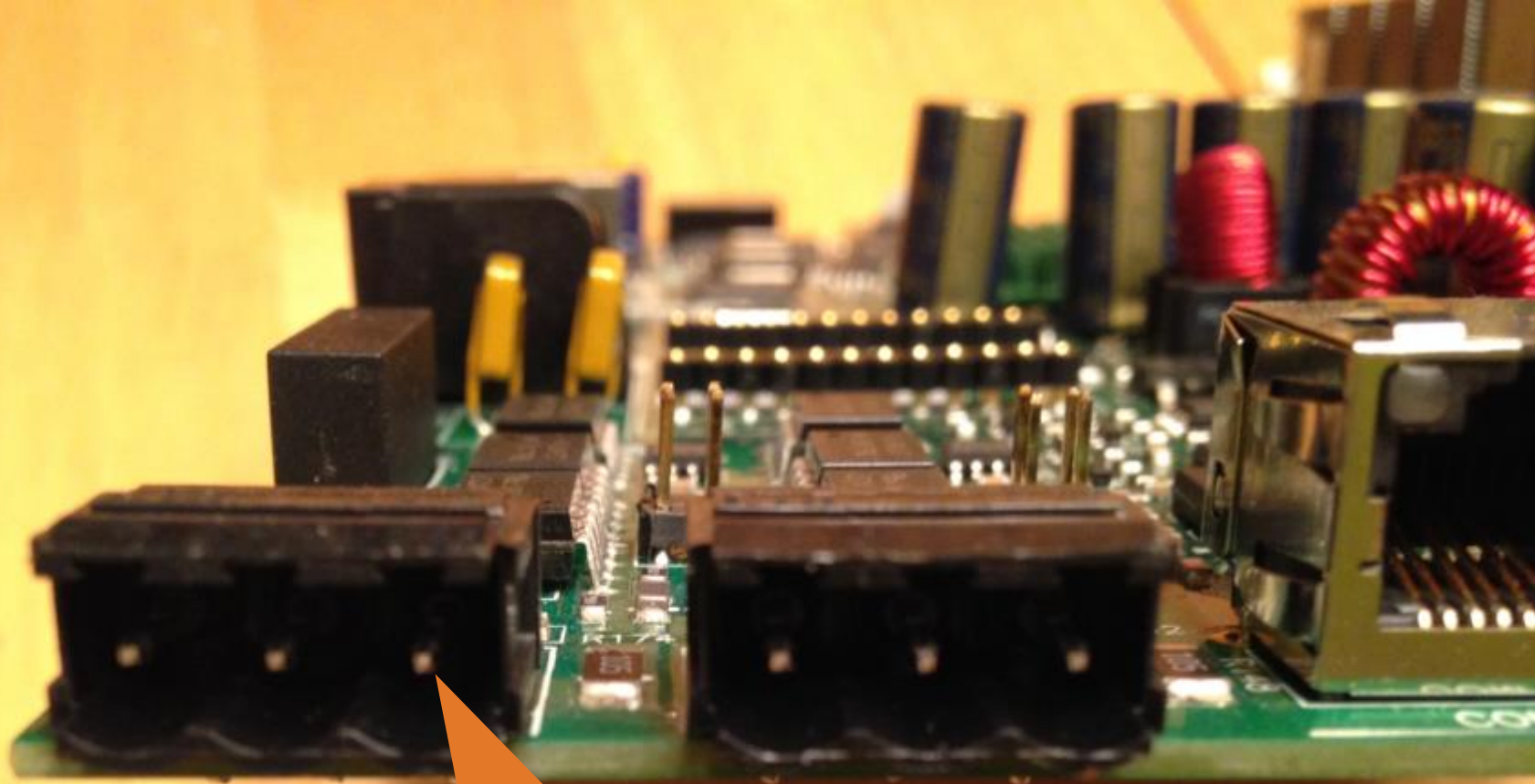
JACE 404 AX ROHS
0910 0093

JACE 4 S
TRID.COM

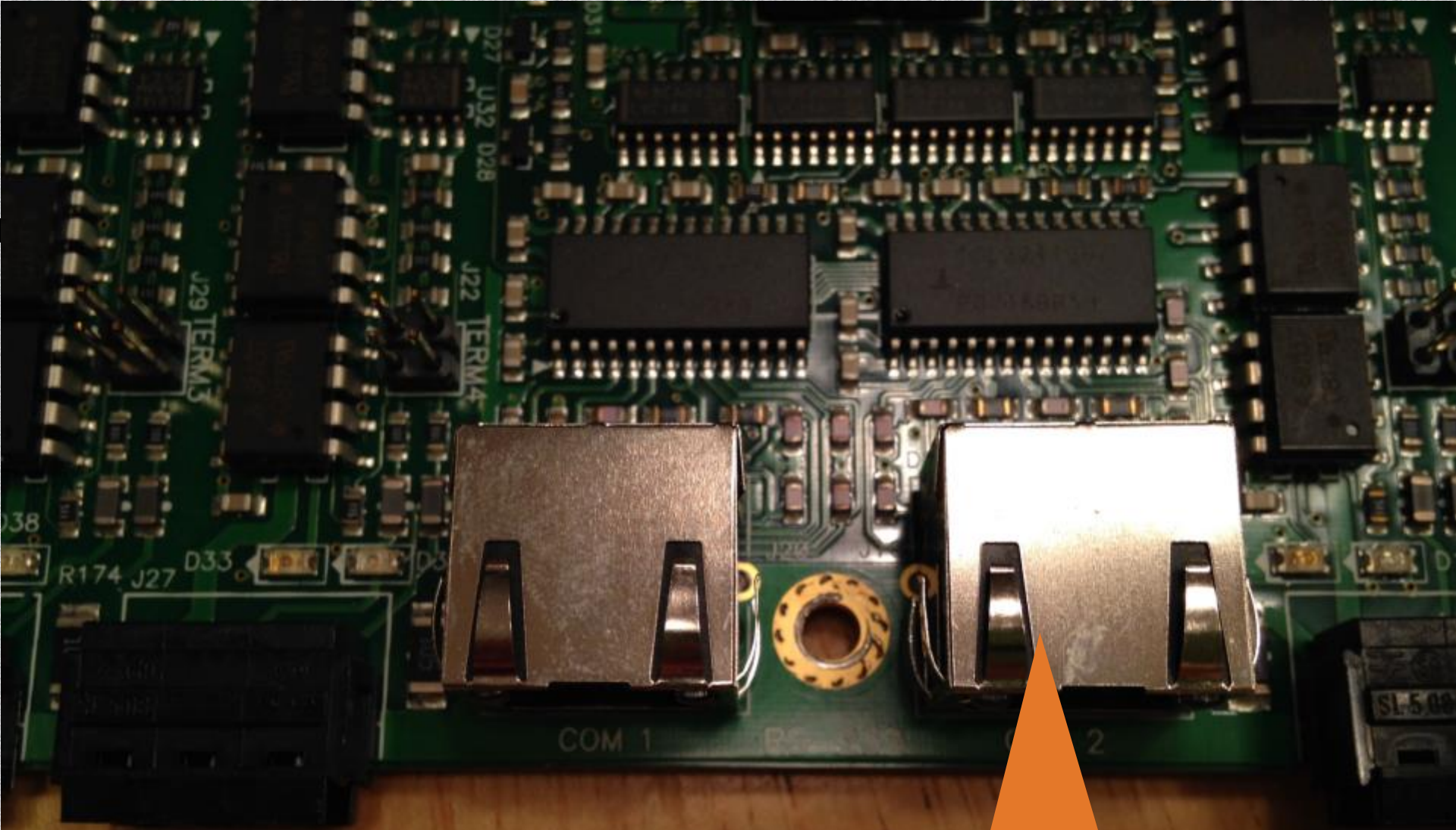
RJ11 - モデム



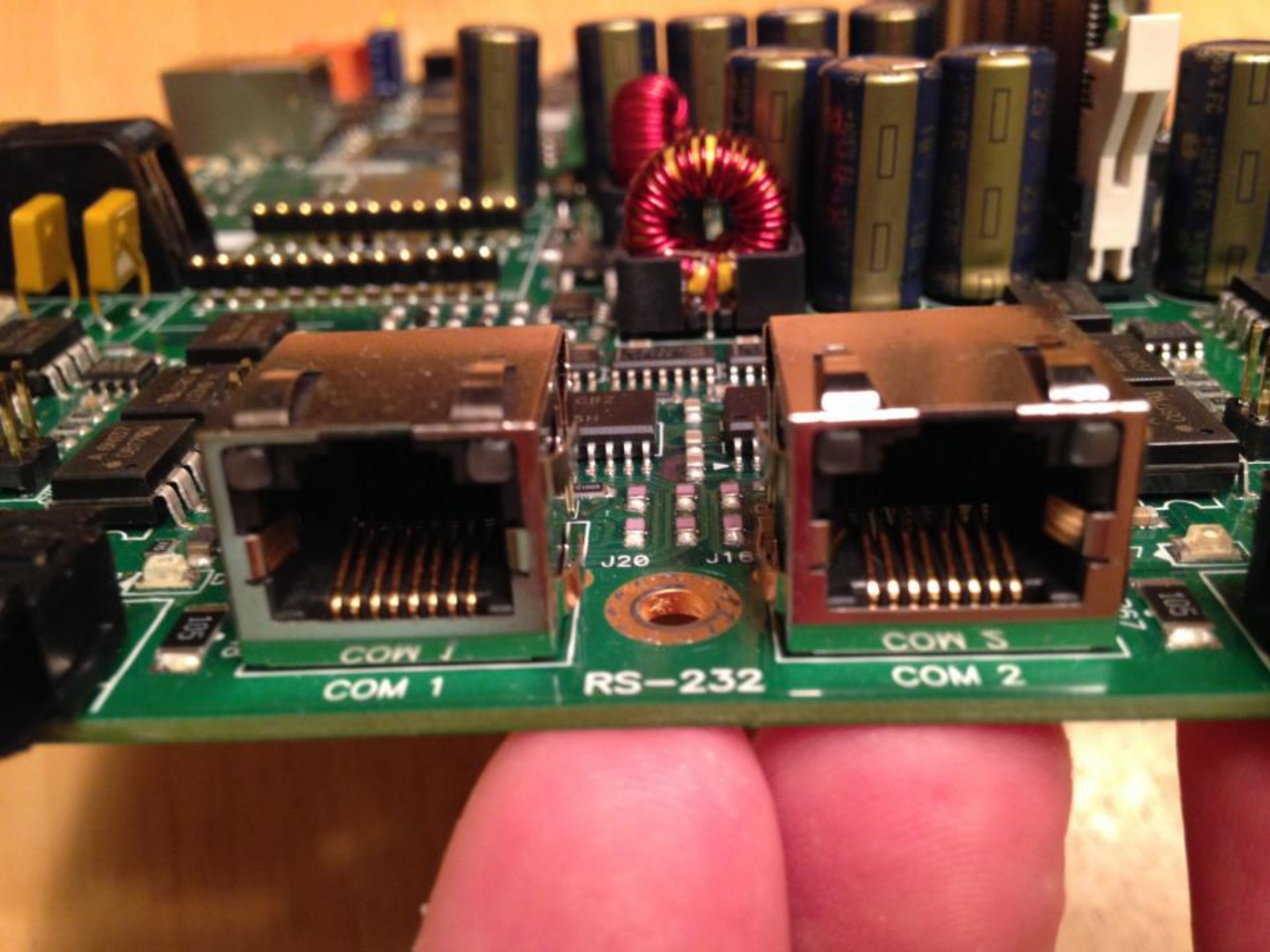
RS485 - シリアル



RS485には3ピンと4ピンの
インターフェイスがある



RJ45経由のRS232



COM 1
COM 1

J20 J16
RS-232

COM 3
COM 2



どのようなプロセッサ
アーキテクチャが
重要かを理解

一般的な組み込みアーキテクチャ

- ◆ プロセッサ
 - ◆ x86
 - ◆ ARM
 - ◆ Motorola PowerPC

- ◆ オペレーティング システム
 - ◆ Windows CE/Embedded
 - ◆ VxWorks
 - ◆ BusyBox
 - ◆ QNX





U-QJ-01
HM

12015
A10

00001
ELON
MP

103

103

103

103

103

RN7

RN6

RN4

RN5

U24

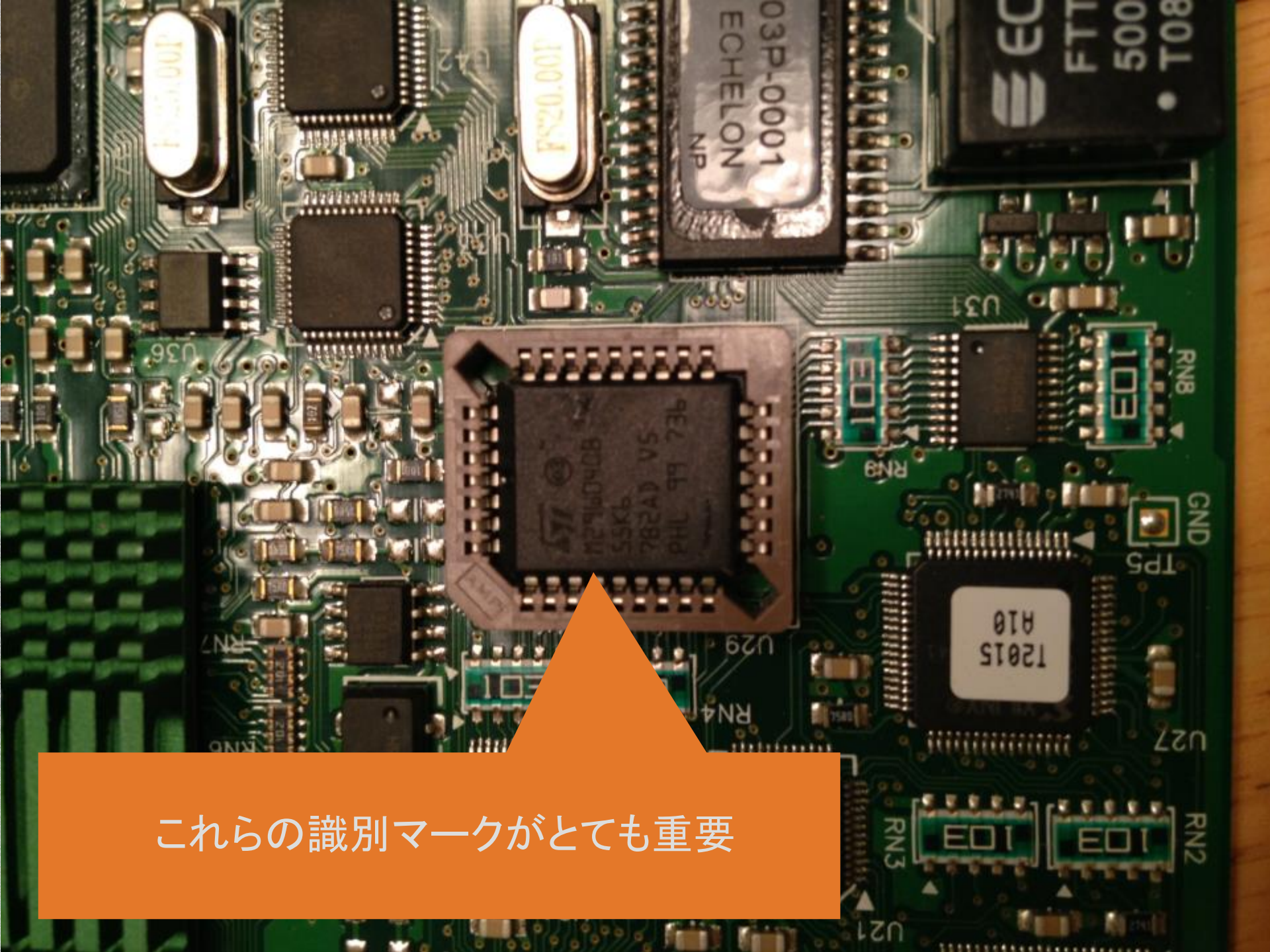
U29

U21

U36

U31

TP5



これらの識別マークがとても重要




Name ▲










 bootrom

 ETH_5103_v450_IE07.bin

fw

File Edit View Go Bookmarks Help

< _working.bin.extracted FLASH0 fw tz >  Search

 tz	 Boot.yes	 dl_end.lst
 dl_start.lst	 Files.lst	 fw.ini
 hw.ini	 vxWorks	 WebServer.out



RTU # 1

Area Served First Floor VAV Boxes

19-Aug-13 1:28 AM EDT

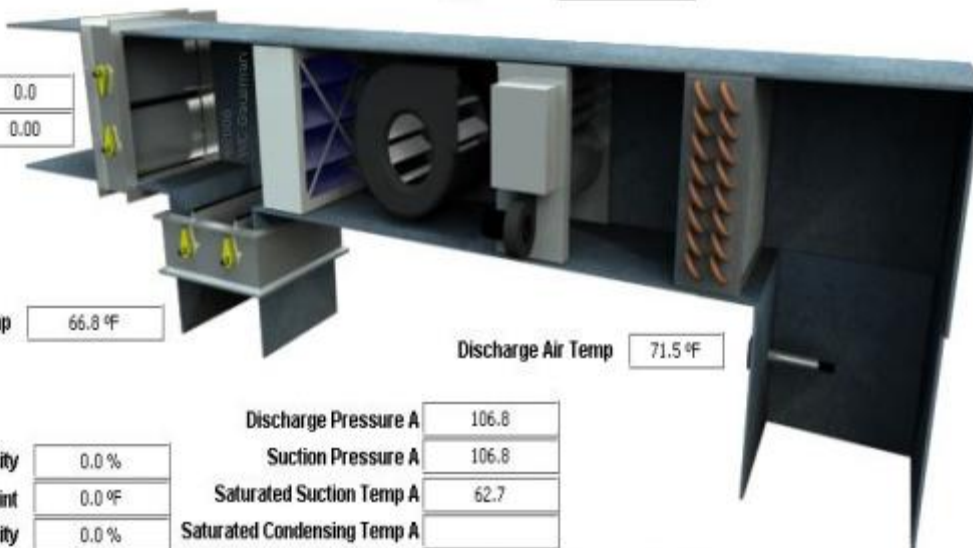
Building Static Press Setpt	0.1 in/wc	Building Static Press	-0.0 %	Outside Air Temp	59.0 °F
Duct Static Press Setpt		Duct Static Press			
Occ Clg Setpt	72.0 °F	UnOcc Clg Setpt	78.0 °F	RTU Effective Control Point	75.50
Occ Htg Setpt		UnOcc Htg Setpt	68.0 °F		

Mixed Air Temp 66.7 °F

Supply Fan Enable On

Supply Fan VFD 0.0 %

Economizer Position 0.0
Economizer Ovrld 0.00



Return Air Temp 66.8 °F

Discharge Air Temp 71.5 °F

Current Cooling Capacity 0.0 %
SAT Cooling Control Point 0.0 °F
Total Cooling Capacity 0.0 %
Compressor A1 Relay CMD
Compressor A2 Relay CMD
Compressor B1 Relay CMD Off

Discharge Pressure A	106.8
Suction Pressure A	106.8
Saturated Suction Temp A	62.7
Saturated Condensing Temp A	
Compressor A1 Feedback	Off
Compressor A2 Feedback	Off
Compressor B1 Feedback	Off
Discharge Pressure B	139.2
Suction Pressure B	108.3
Saturated Suction Temp B	
Saturated Condensing Temp B	77.9

Requested Heat Stages 0
Htg Stage 1 Off
Htg Stage 2 Off
Htg Stage 3 Off
Htg Stage 4 Off

Occupancy



Outside Air Temp 59.0 °F

Hot Water System Enable Set Point 100.0 °F
When out is below this # HW Enables

Hot Water Supply Temp 156.50

Hot Water Return Temp 156.30



HWP-1 Start/ Stop Stop

HWP-2 Start/ Stop Start



Boiler Enable Enable

Parking		Mechanical		Tenants			
L5	L6	Roof		L23	L24	L25	L26
L3	L4	Lease Lobby		L19	L20	L21	L22
L1	L2	Level 6		L15	L16	L17	L18
P1		Level 7		L11	L12	L13	L14
P3	P2	Fitness Center		L7	L8	L9	L10

Alarms

Equipment

Gables Residential Tower



Building Systems
Integration
TDIndustries
Gables Tower

Documentation

- Sequences
- Manuals
- Data Sheets
- Control Drawings



Schedules

- HVAC



History

- Maintenance
- Charts
- History Tables



Reports

- NM-1 All Points Report
- NM-2 All Points Report
- NM-3 All Points Report
- NM-4 All Points Report
- NM-5 All Points Report
- NM-6 All Points Report
- NM-7 All Points Report
- NM-8 All Points Report
- NM-9 All Points Report



列挙してみると

- ◆ インターネット接続
 - ◆ 初めはShodanをベースに、現在はEC2で実行中
 - ◆ 50,000以上の建物
 - ◆ スタジアム、病院、警察署、刑務所、企業、軍事施設など
- ◆ コスト
 - ◆ EC2時間
 - ◆ 調査用のハードウェアとソフトウェア
 - ◆ 合計～500ドル



QUALYS のターゲット

- ◆ シリコンバレーをベースに
- ◆ フル スコープの「レッド チーム」式の評価を明示的にリクエスト
- ◆ 組織やインフラストラクチャの事前知識なし
- ◆ 予行として、ネットワーク セキュリティ チームの監視と企業の全セキュリティ資産



QUALYS のアプローチ

- ◆ 弊社のBAS(ビル自動化システム)データベース内のターゲットを識別(ターゲットに対するポート スキャンは必要なし)
- ◆ インターネット接続BASは通常、企業IPスペースの外部で検出される
- ◆ 弊社のエクスプロイト攻撃インフラストラクチャを構成し、ゼロデイ脆弱性を利用してビル自動化システムにアクセス



インテグレーターの教訓

- ◆ 通常、エンドの組織がIoTをインストールすることはない
- ◆ 通常、HVAC/会議室/Nestサーモスタット/センサーの取り付けはサードパーティ(インテグレーター)に任される
- ◆ 問題が発生した場合、通常はインテグレーターがサポートのために呼び出される
- ◆ インテグレーターにとってクライアント サイトまでの移動に高額な費用や時間がかかることがあるため、リモート アクセスを有効にする





WARNING
 This equipment must be isolated or disconnected from the mains before access.
USE COPPER CONDUCTORS ONLY

Model: 25-100-01-00
 Part No: 25-100-01-00
 Rev: 1.0

This equipment complies with FCC rules for a Class 'B' computing device.
 Operation is subject to the following two conditions:
 1. This device may not cause harmful interference.
 2. This device must accept any interference received, including interference that may cause undesired operation.
 This Class B digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.
 Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

UNIT NUMBER: _____
 P-XXXXXX

USE COPPER CONDUCTORS ONLY

COM 3 RS-485	COM 4 RS-485	COM 1 RS-232	COM 2 RS-232	COM 5 RS-485	COM 6 RS-485

S +



不正アクセス



不正アクセス



不正アクセス



アクセス?

- ◆ 自動化ネットワークから企業ネットワークへ巡回
 - ◆ VLANがCorpNETから自動化ネットワークを分離
 - ◆ どの自動化システムにもAVなし
 - ◆ ケーブル モデム回線は、境界の入出力監視のバイパスを許容している
- ◆ ドメイン認証情報を使用してCorpnetにアクセス
 - ◆ この時点で、この評価は従来の侵入テストになってしまう
 - ◆ ドメイン管理者にエスカレーション
 - ◆ すべてのワークステーション(企業IPと財務データを含む)へのアクセス
 - ◆ CEOのメールへのアクセス

求められるコンセプト実証

- ◆ 企業HQのフロントドアのロック解除
- ◆ IPベースのすべての監視システムの停止
- ◆ アクセス制御データベースの変更(バッジの追加)
- ◆ 経営陣のモバイル デバイスの消去



検討事項

- ◆ デバイスを受け取る前に
 - ◆ ポリシーを持つ
 - ◆ ネットから狙われる点を理解する
 - ◆ リモート管理がどのように実装されているか理解することを主張する
 - ◆ デバイスがインターネットに接続されているかどうかを把握する
 - ◆ 提示された構成と導入を評価する
 - ◆ 貴社の買収担当者も関与させる
 - ◆ 貴社の設備および資産チームと連携を強め、システムをデフォルトのまま受け入れることのリスクを彼らに理解させる
- ◆ 大型資本投資(例、建物購入)には初期からセキュリティ上の関与が必要。



検討事項

- ◆ 貴社ネットワーク上のデバイスの取り扱い
 - ◆ 担当のインテグレーターが誰かを把握
 - ◆ テスト用の予備デバイスがあるか聞く
 - ◆ デバイスに対する評価を実施
 - ◆ テキストの認証情報をクリアする(デバイスがカレンダー更新のために Exchangeサーバーと対話する場合は、そのデバイスにドメイン認証情報がある)
 - ◆ バックドア パスワード
- ◆ ライブラリ
- ◆ デバイスを出入りするトラフィックの監視
- ◆ デバイスと対話できるユーザーの制限を検討
- ◆ デバイス操作の基準を作る
 - ◆ 既知の優れたファームウェア、ファイル、プロセス



優れたリソース

- ◆ /Dev/TTY50 – <http://www.devttys0.com/blog/>
- ◆ Travis Goodspeed – <http://travisgoodspeed.blogspot.com/>
- ◆ Mikeselectricstuff – <http://www.youtube.com/user/mikeselectricstuff?feature=watch>
- ◆ STBUYN – <http://dontstuffbeansupyournose.com/>
- ◆ Cyber Pacifists – <http://www.cyberpacifists.net/>
- ◆ Reversemode – <http://www.reversemode.com/>
- ◆ W00tsec – <http://w00tsec.blogspot.com/>



キット

- ◆ ナットドライバー、トルクス、スクエアを含むスクリュードライバーセット
 - ◆ http://www.amazon.com/s/ref=nb_sb_ss_c_0_14?url=search-alias%3Dindustrial&field-keywords=screwdriver+set
- ◆ はんだ吸い取りキット付きはんだごて
 - ◆ http://www.amazon.com/s/ref=nb_sb_noss_2?url=search-alias%3Daps&field-keywords=soldering
- ◆ はんだ付けなしブレッドボード
 - ◆ <http://www.adafruit.com/products/758?gclid=CMPMiO-y5bwCFZRsfgodHG0ACw>
- ◆ ジャンパー線
 - ◆ http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Dindustrial&field-keywords=jumper+wires+male+to+male



キット

- ◆ コンソール ケーブル
 - ◆ http://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=console+cable
- ◆ TTL Reader
 - ◆ http://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=TTL+to+USB
- ◆ JTAG Reader
 - ◆ <http://blackcatusbjtag.com/>
- ◆ ROM Reader
 - ◆ http://www.amazon.com/s/ref=nb_sb_ss_c_0_14?url=search-alias%3Dindustrial&field-keywords=screwdriver+set
- ◆ Logicアナライザー
 - ◆ <http://www.saleae.com/logic>



キット

- ◆ 逆アセンブラー(該当するチップセットのサポートあり)
 - ◆ <https://www.hex-rays.com/products/ida/>
- ◆ デバッガー
 - ◆ <https://www.immunityinc.com/products-immdbg.shtml>
- ◆ ターミナル ソフトウェア
 - ◆ <http://www.hilgraeve.com/hyperterminal/>
- ◆ 仮想化ソフトウェア
 - ◆ <http://www.vmware.com/>



RSACONFERENCE2014
アジア太平洋地域および日本



質問はありませんか？

RSACONFERENCE2014

アジア太平洋地域および日本

