RSA CONFERENCE 2014
アジア太平洋地域および日本

Share.
Learn.
Secure.
集約型インテリジェンスの活用

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 Kutsayew/freedigitalphotos.net

August 13, 2013

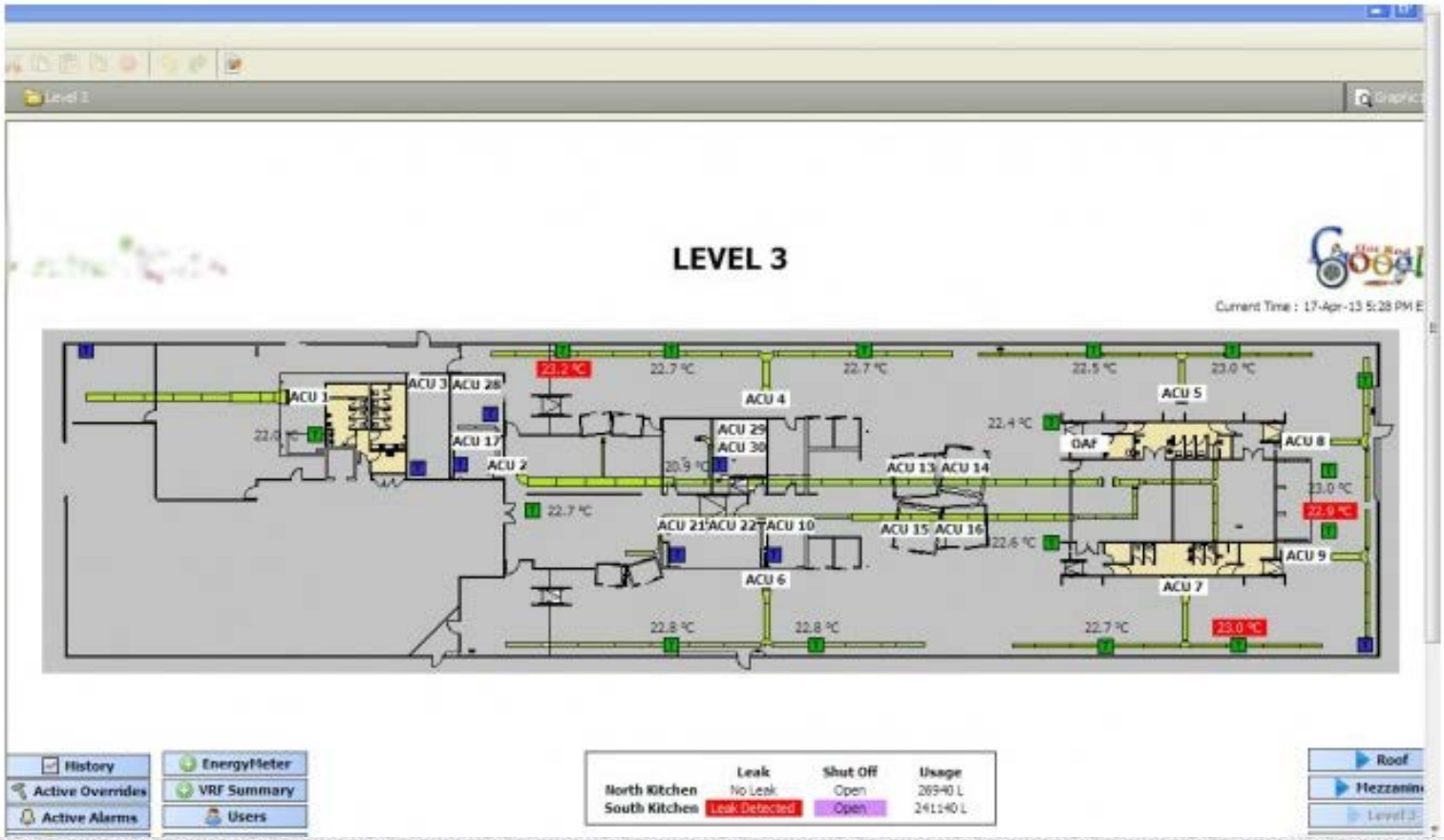
A hacker's voice was heard through a baby monitor located in the child's bedroom by distraught parents in Houston. The menacing voice was trying to wake the 2-year-old up with curse words then targeted expletives at the parents when they entered the toddler's room, according to a report from **ABC News**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

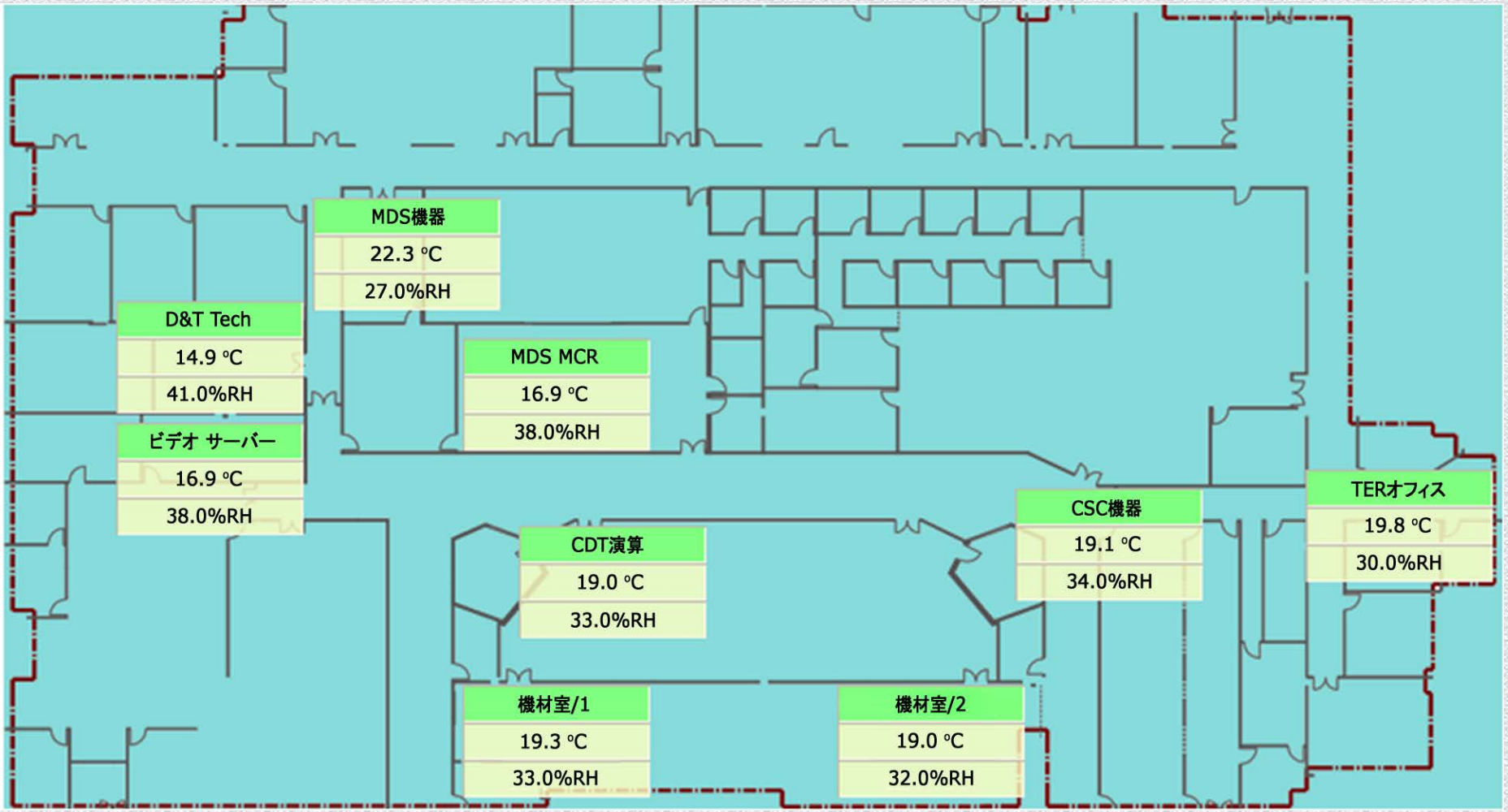
「夜中に娘のエマに対して大声をあげる男の声で目が覚め、
驚いたことにインターネット対応のベビー
モニターが動いているのを発見した。
自分たちが動かしているわけではないのに。」

Researchers Hack Building Control System at Google Australia Office

BY KIM ZETTER 05.06.13 | 6:30 AM | PERMALINK

Share 0 Tweet 1 +1 85 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
ignature>
</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

Print | Tweet | Send | Share

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」

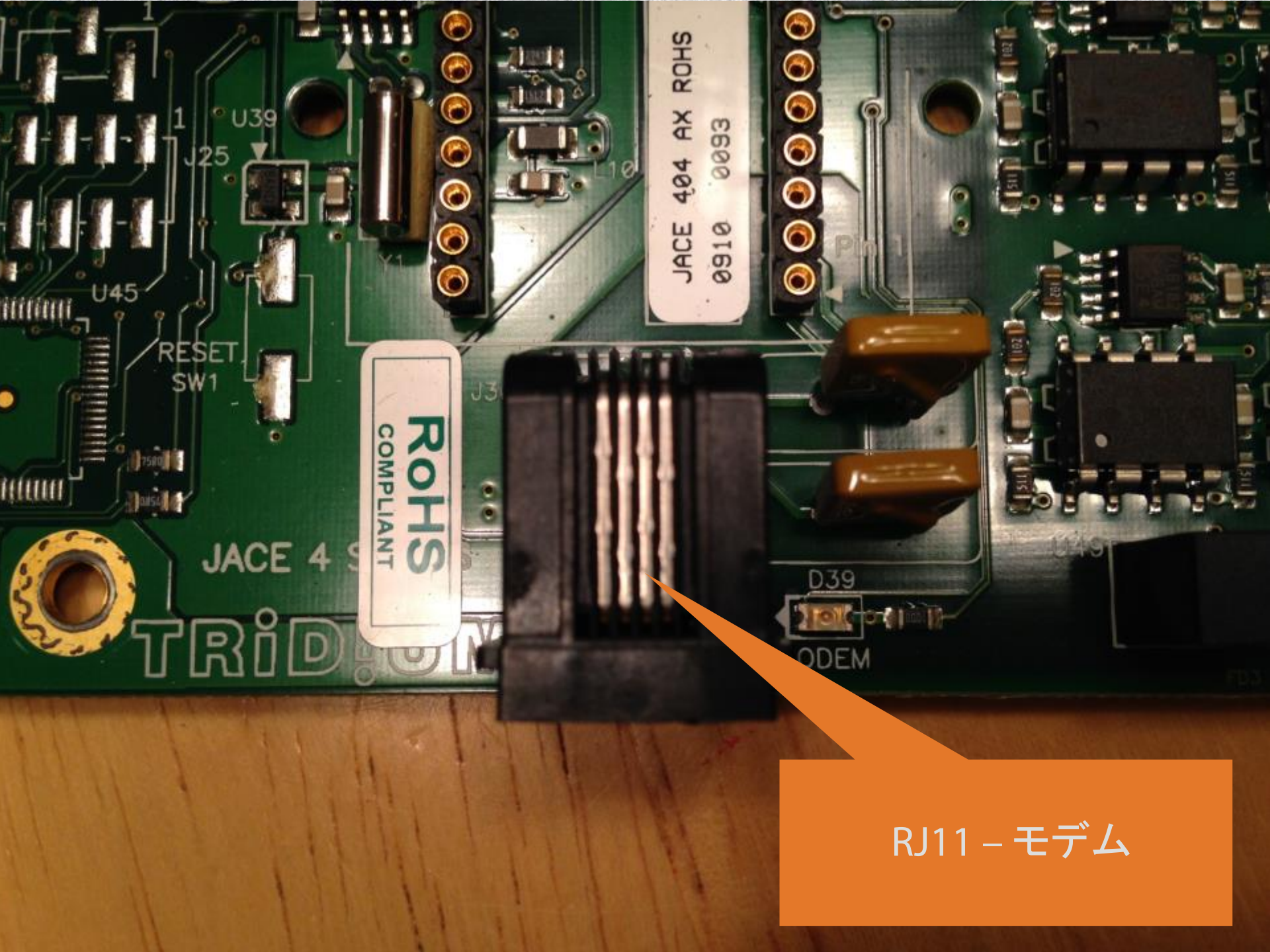

Niagara AX
INTEGRA™
AMERICAN
AUTO-MATRIX
SMART BUILDING SOLUTIONS


AMERICAN
AUTO-MATRIX®
SMART BUILDING SOLUTIONS®

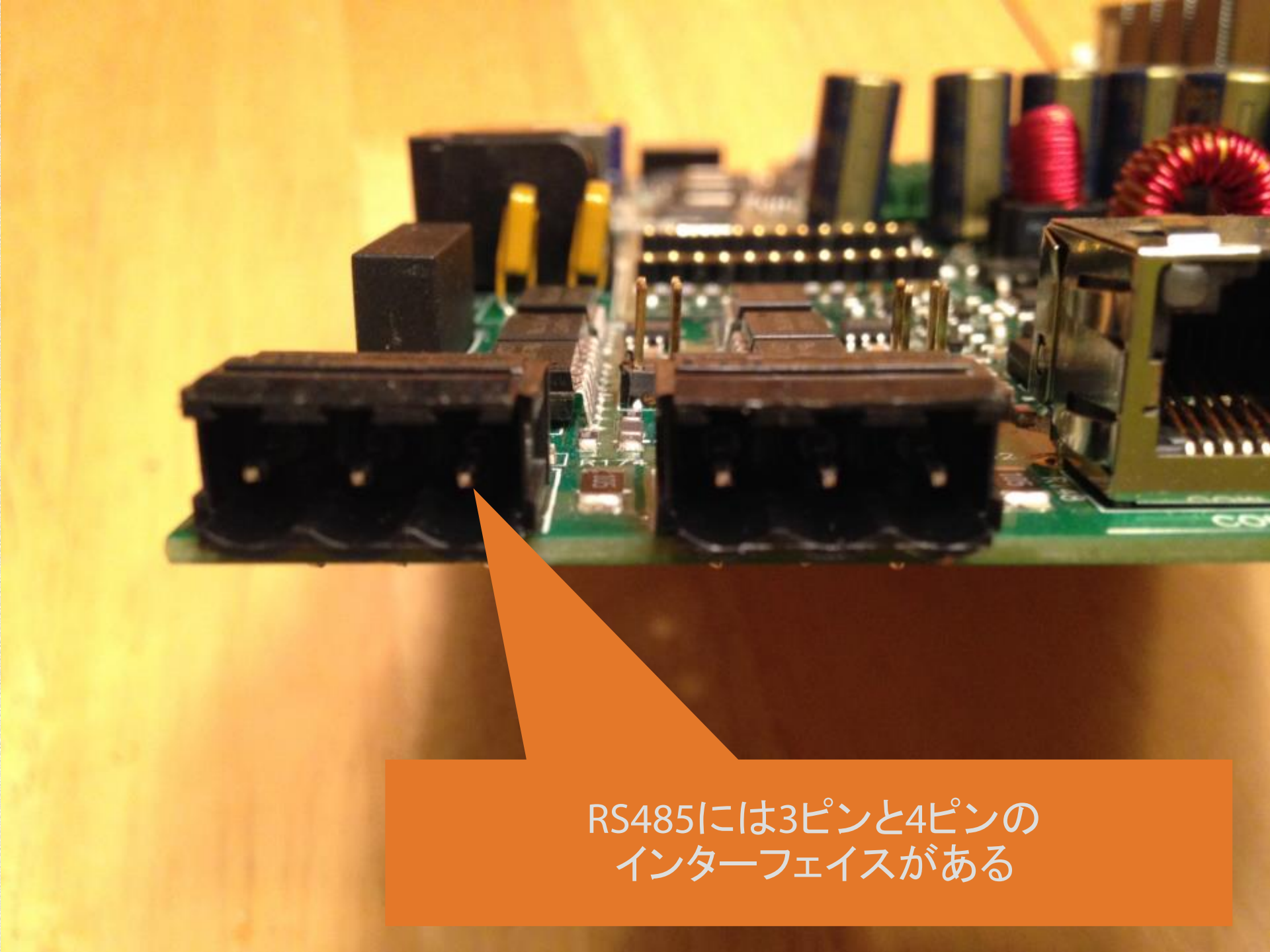

WARNING
COM 3
RS-485
COM 4
RS-485
COM 1
RS-232
COM 2
RS-232

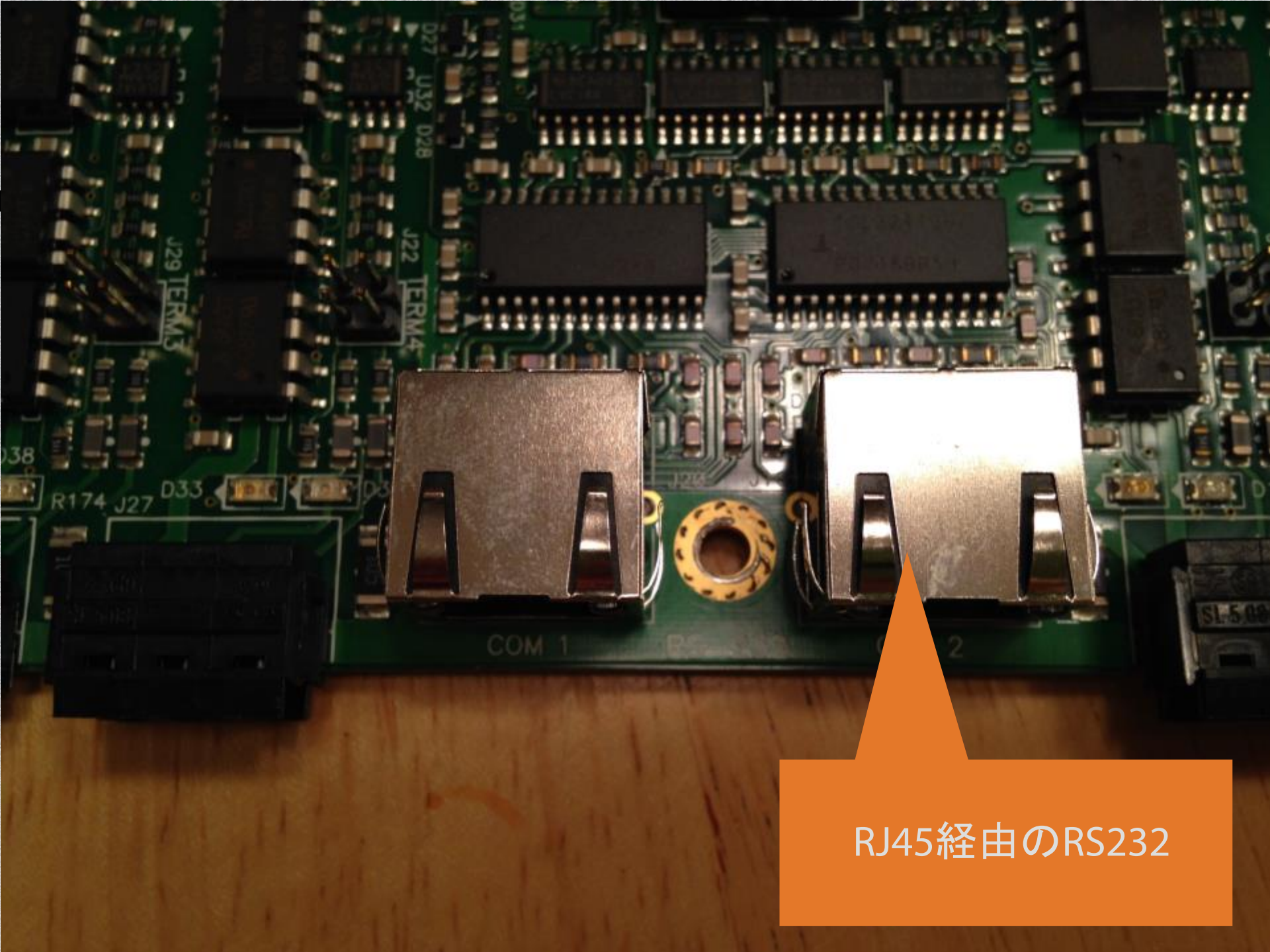

ECHELON
INTERNAL MODEM
ETHERNET
RoHS
JACE 4
TRIDIUM

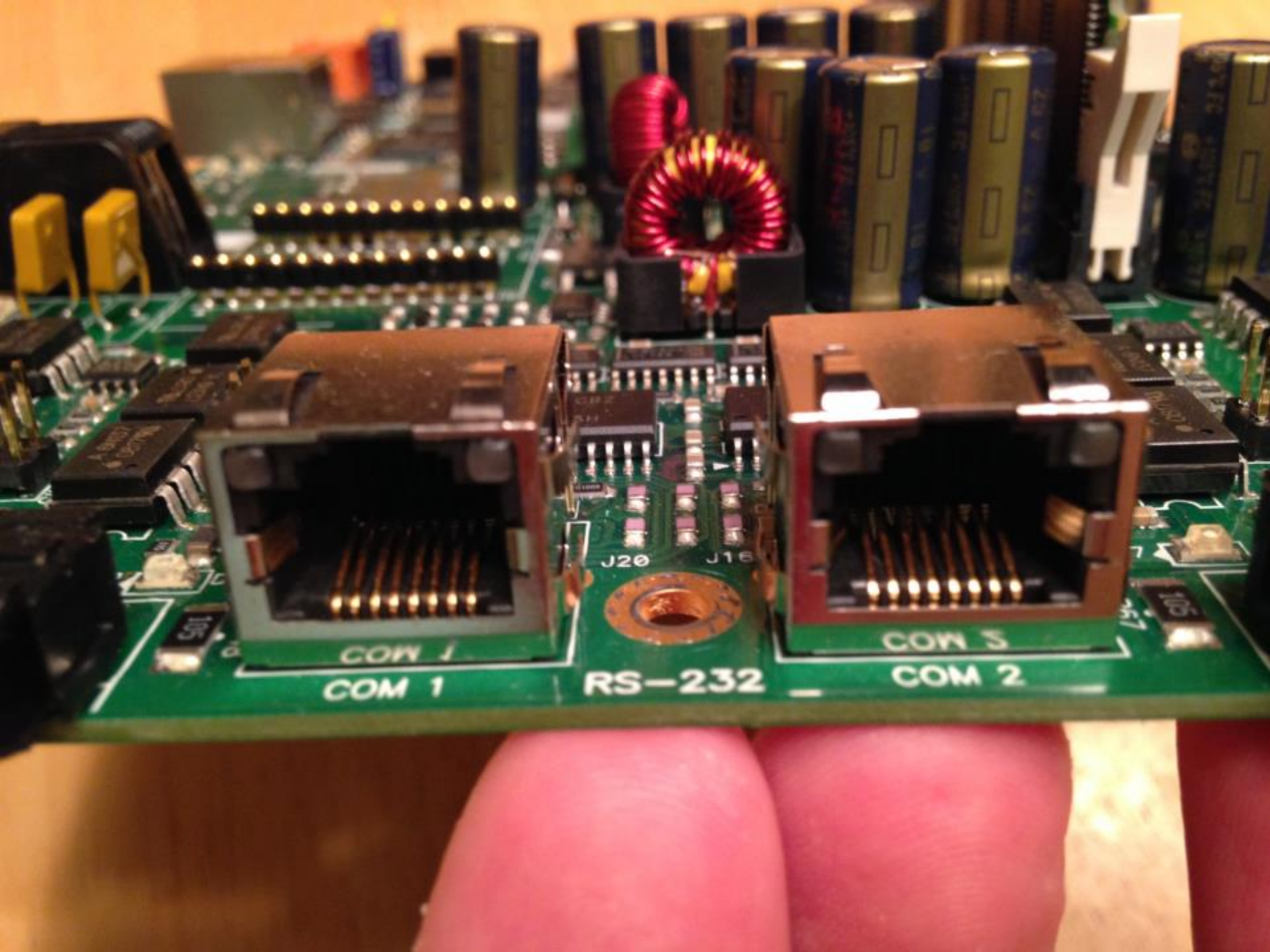

RJ45 – Ethernet


JACE 404 AX ROHS
0910 0093
U39
J25
U45
RESET
SW1
RoHS
COMPLIANT
D39
ODEM
RJ11 – モデム


J29 TERM3
D38
J33 D40
J27
D33
COM 1
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

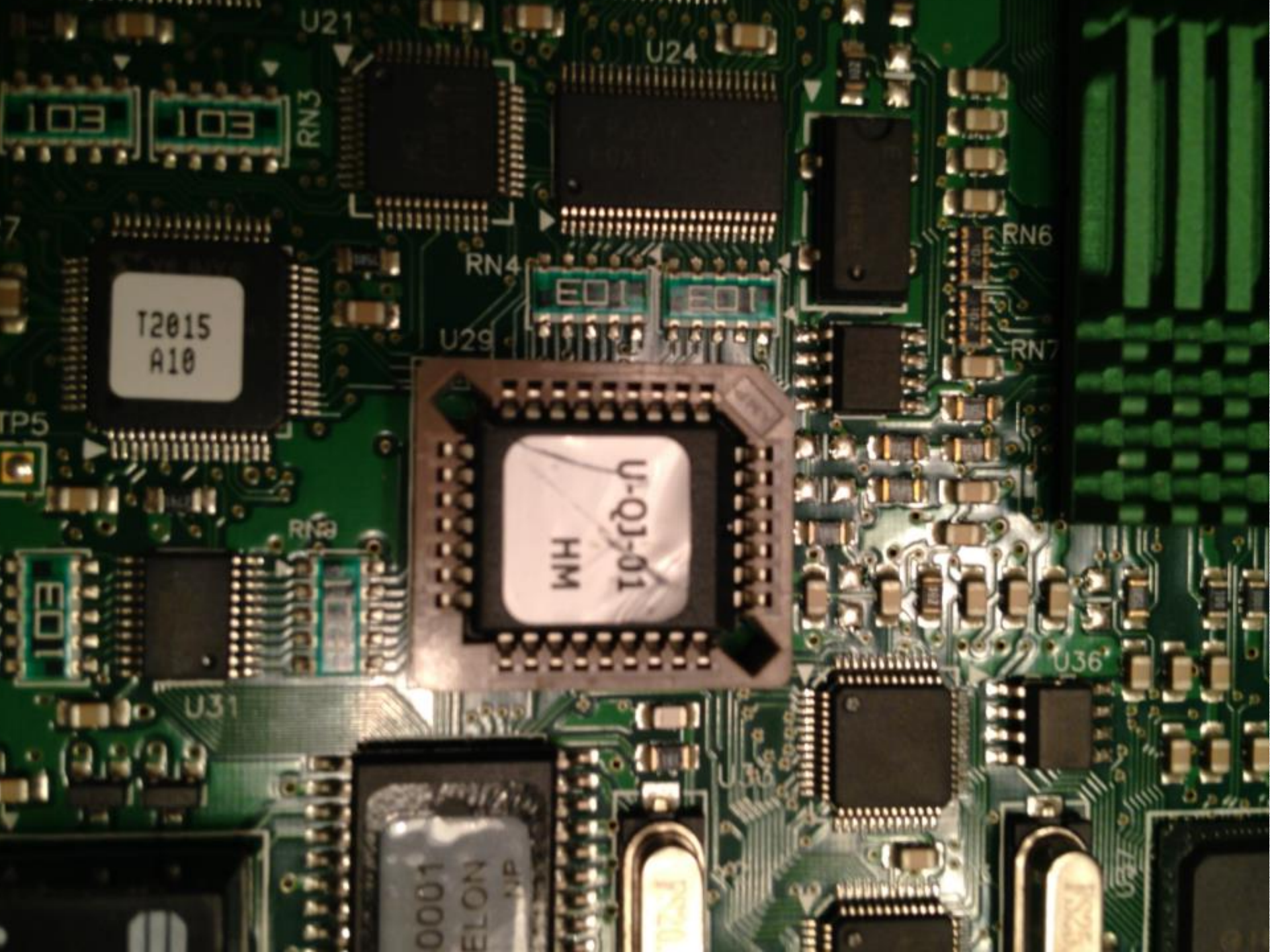

J29 TERM3
J22 TERM4
D27
U32
D28
R174
J27
D33
COM 1
RJ45経由のRS232

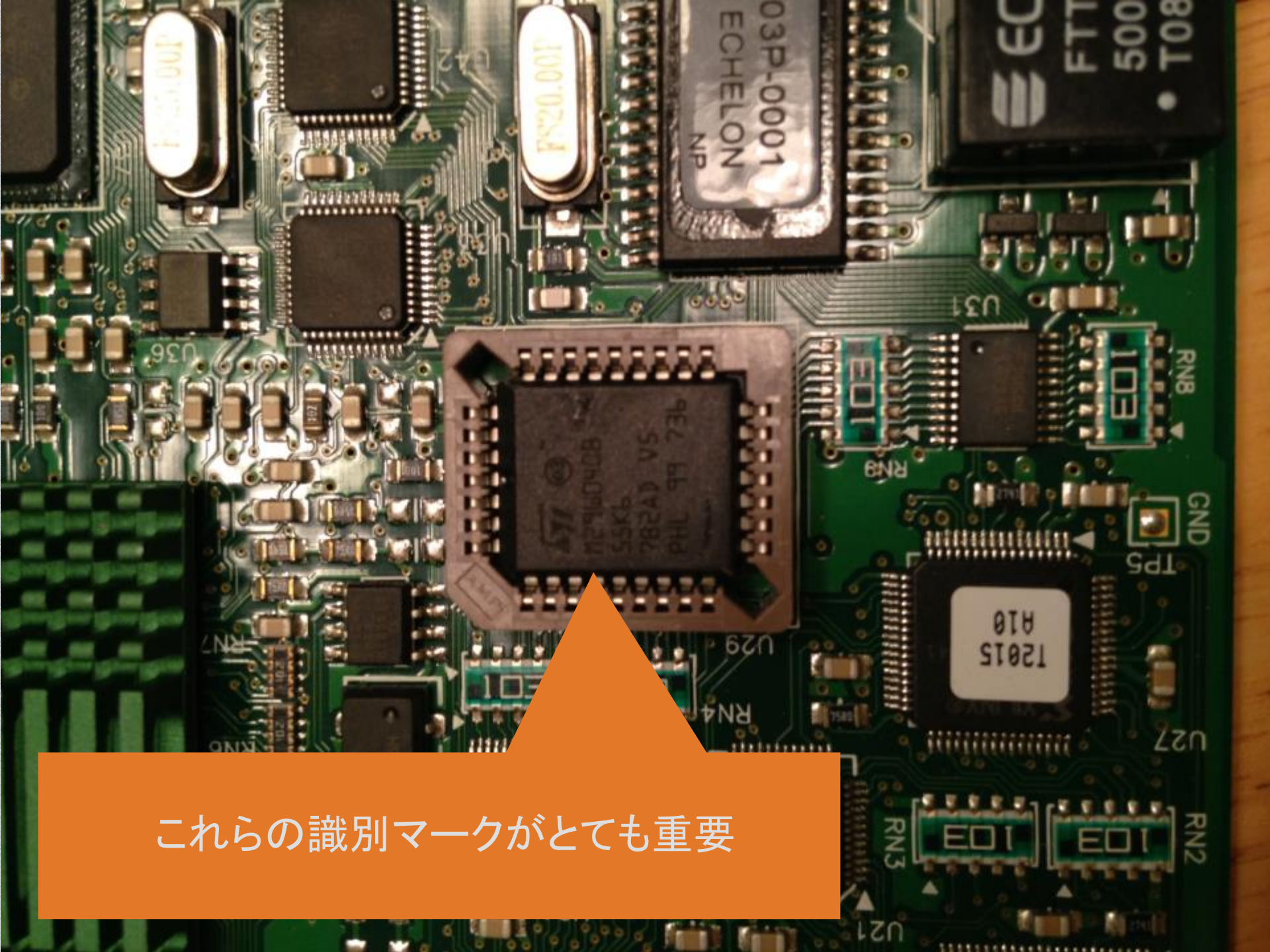

J20
J16
COM 1
COM 2
RS-232


どのような
アーキテクチャが
重要かを理解

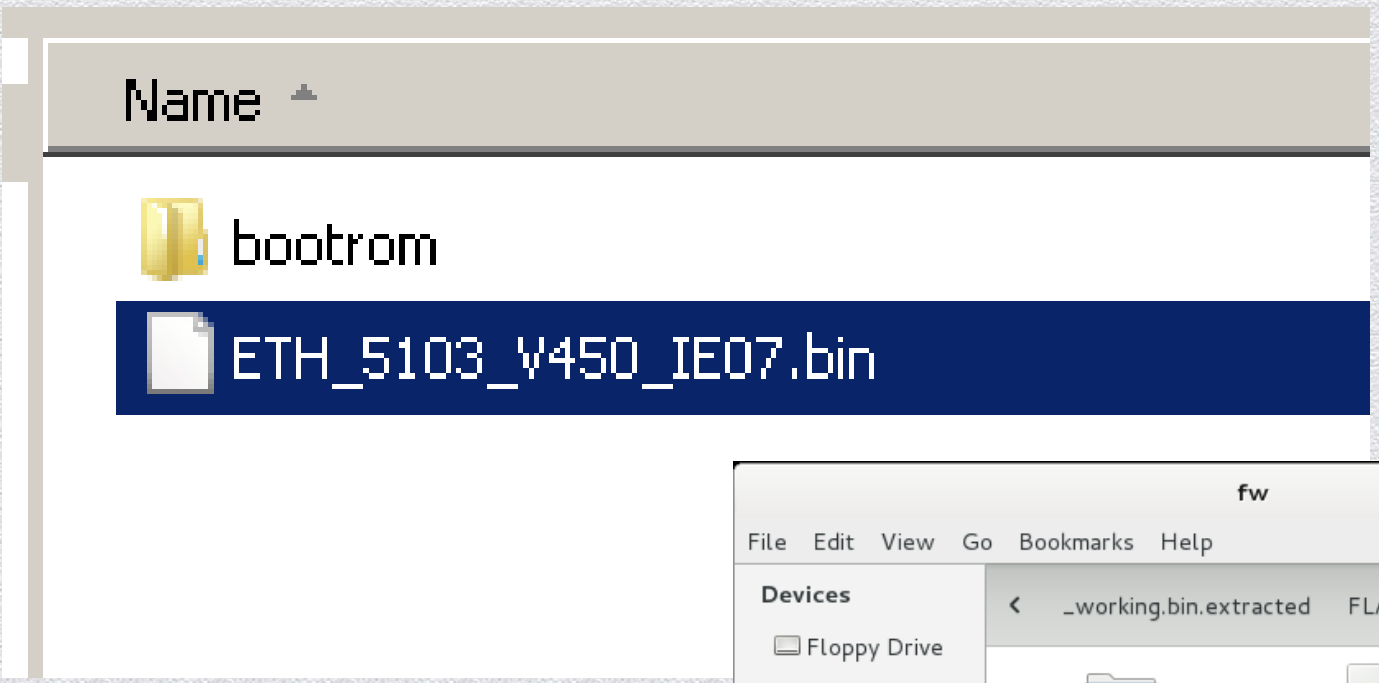
一般的な組み込みアーキテクチャ

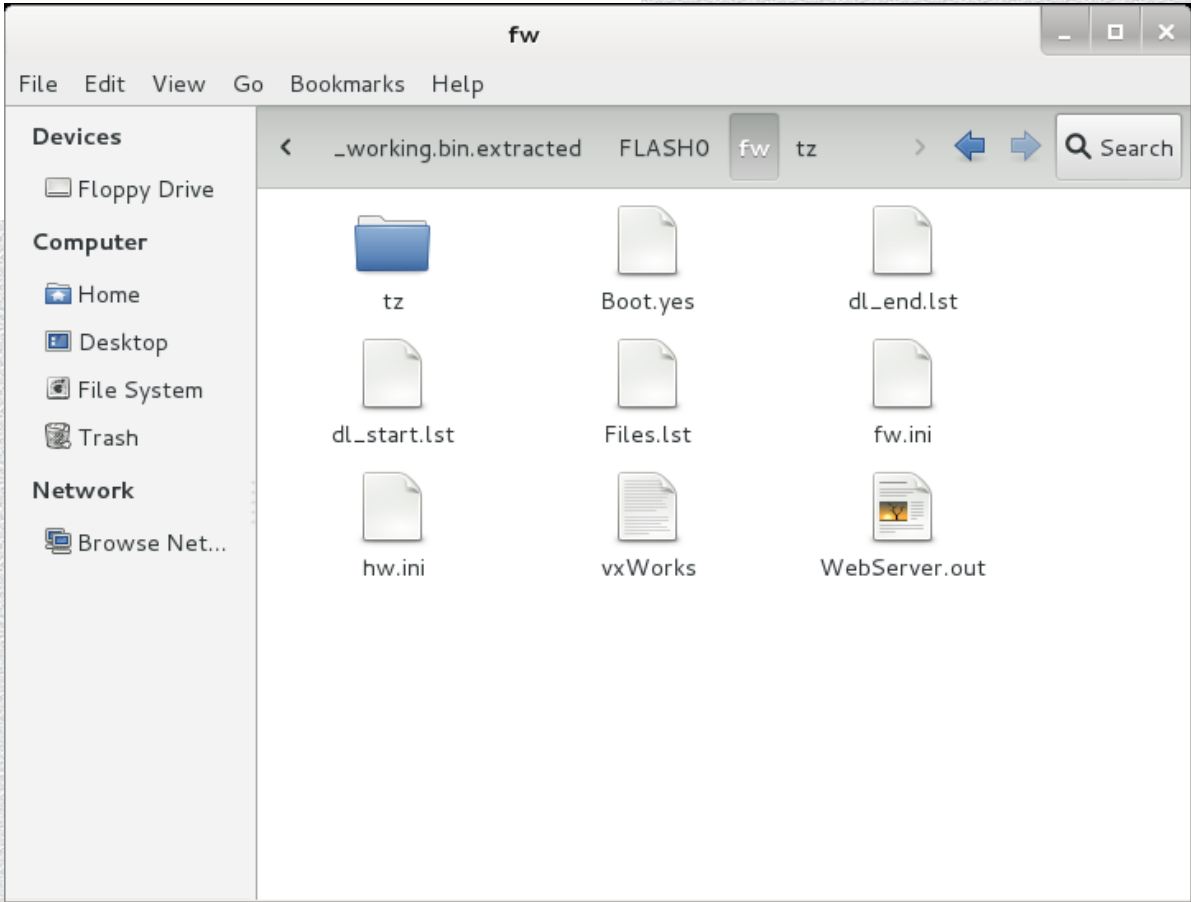
- プロセッサ
  - x86
  - ARM
  - Motorola PowerPC
- オペレーティング システム
  - Windows CE/Embedded
  - VxWorks
  - BusyBox
  - QNX


U21
U24
RN3
RN4
RN6
RN7
U29
U31
U36
TP5
T2015
A10
U-QJ-01
HM

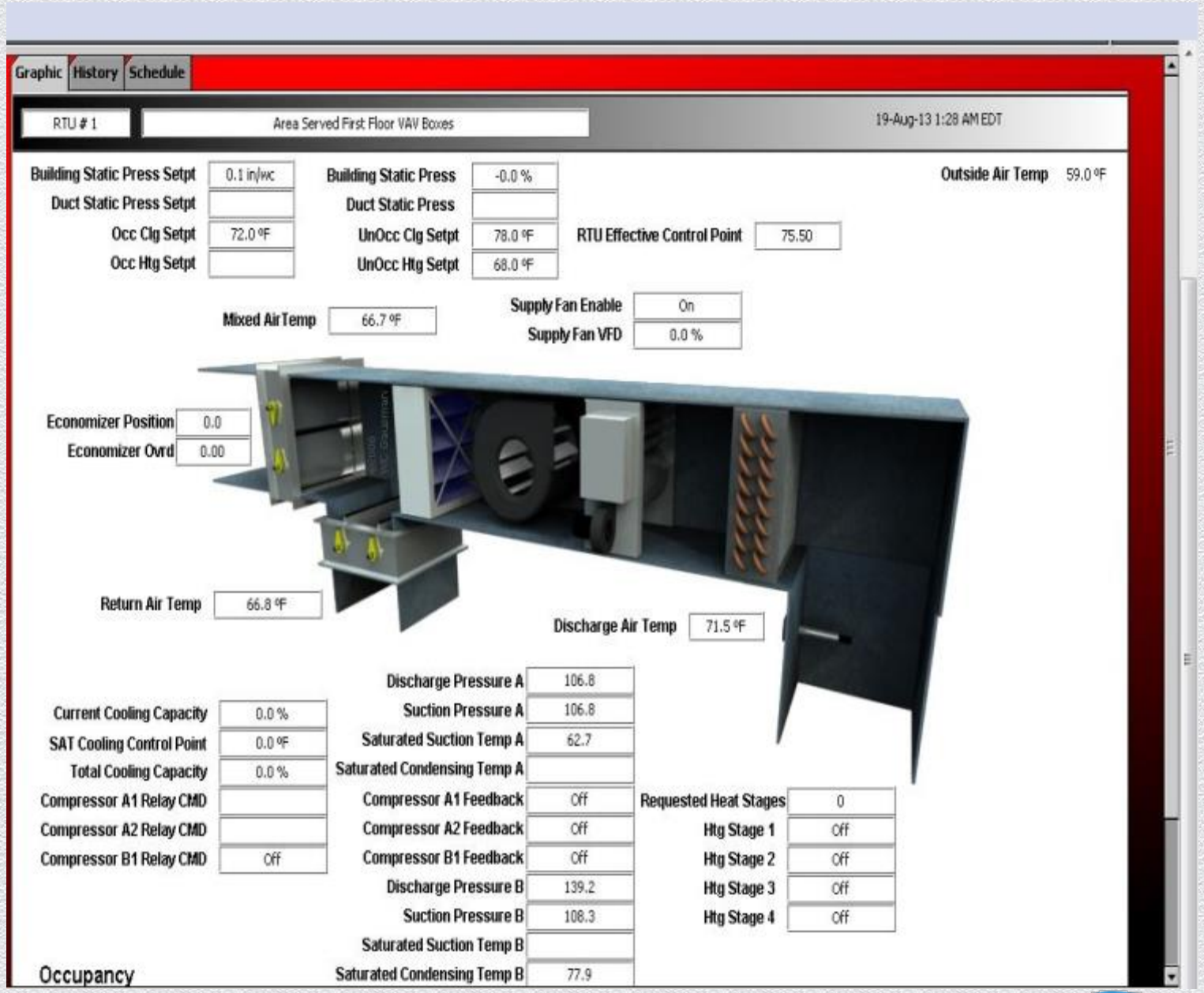

これらの識別マークがとても重要

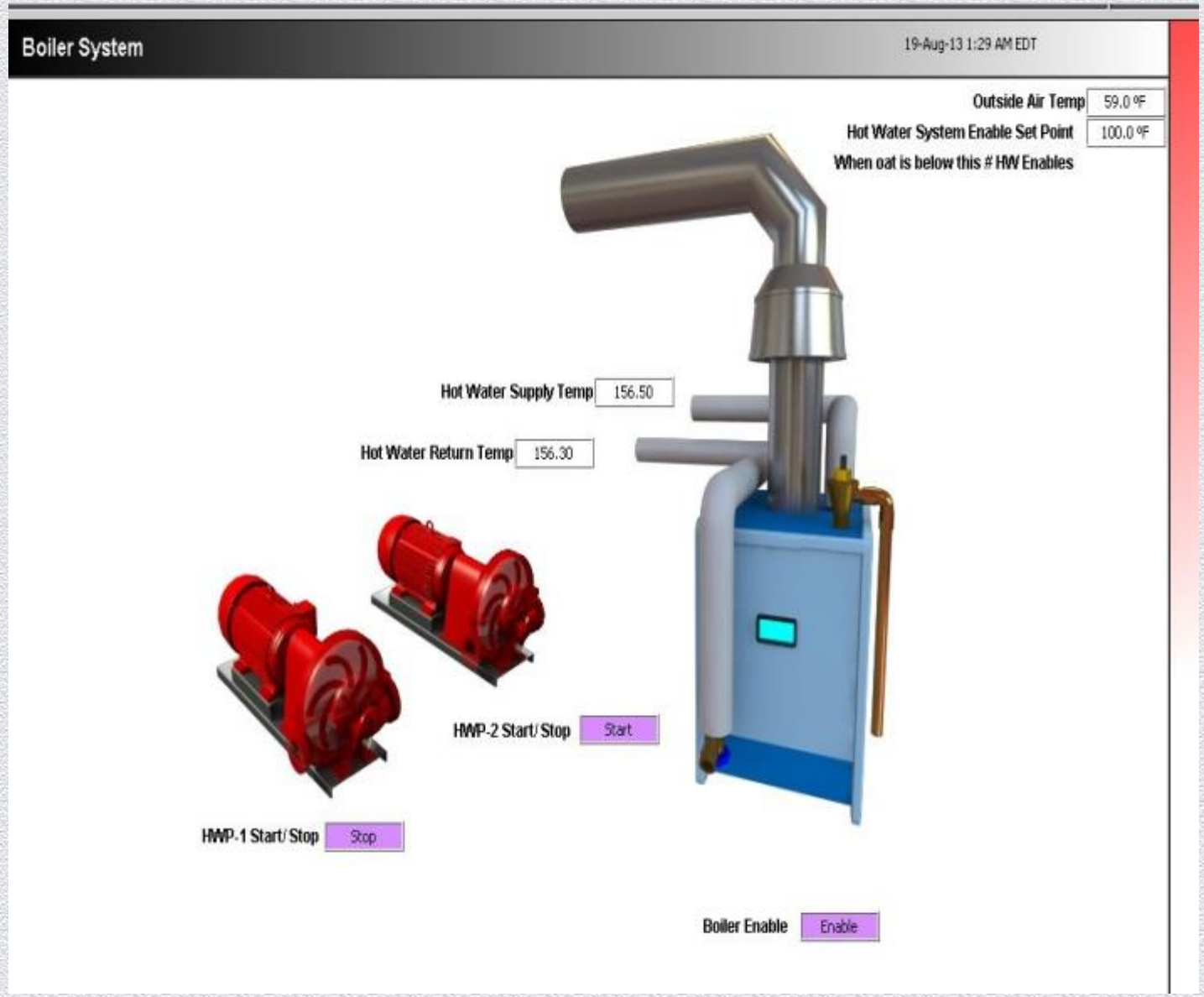

GQ-4X
True USB Universal Programmer
VCC ON VPP

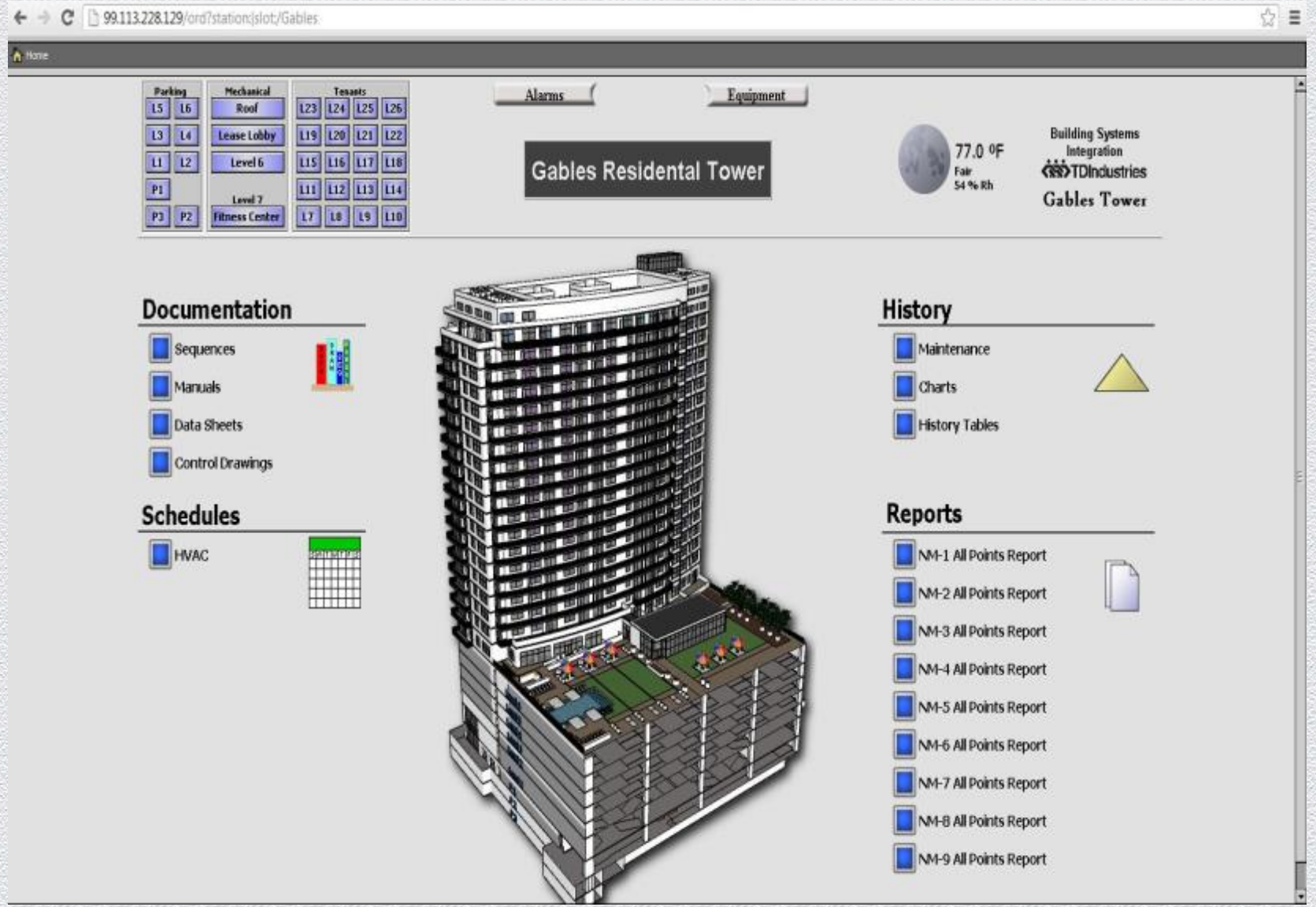




QUALYS
On Demand Security







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

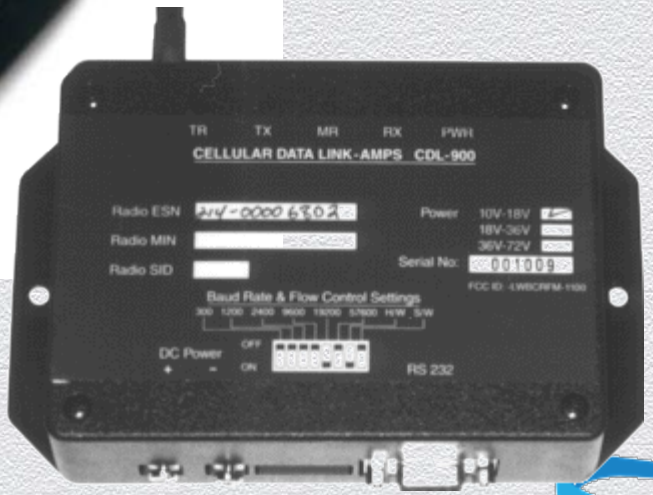
- シリコンバレーをベースに
- フル スコープの「レッド チーム」式の評価を明示的にリクエスト
- 組織やインフラストラクチャの事前知識なし
- 予行として、ネットワーク セキュリティ チームの監視と企業の全セキュリティ資産

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



QUALYS
ON DEMAND SECURITY

#RSAC

RSACONFERENCE2014
アジア太平洋地域および日本

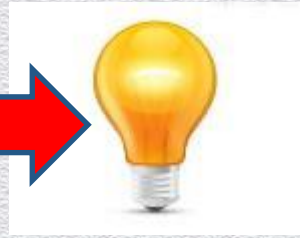

WARNING
COM 3
RS-485
COM 4
RS-485
COM 1
RS-232
COM 2
RS-232

不正アクセス

インターネット

不正アクセス

インターネット



不正アクセス

インターネット

QUALYS
ON DEMAND SECURITY

#RSAC

RSACONFERENCE2014
アジア太平洋地域および日本

アクセス?

- 自動化ネットワークから企業ネットワークへ旋回
  - 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/TTYS0 – 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/

質問はありませんか?


Alaris® PC
Guardrails®