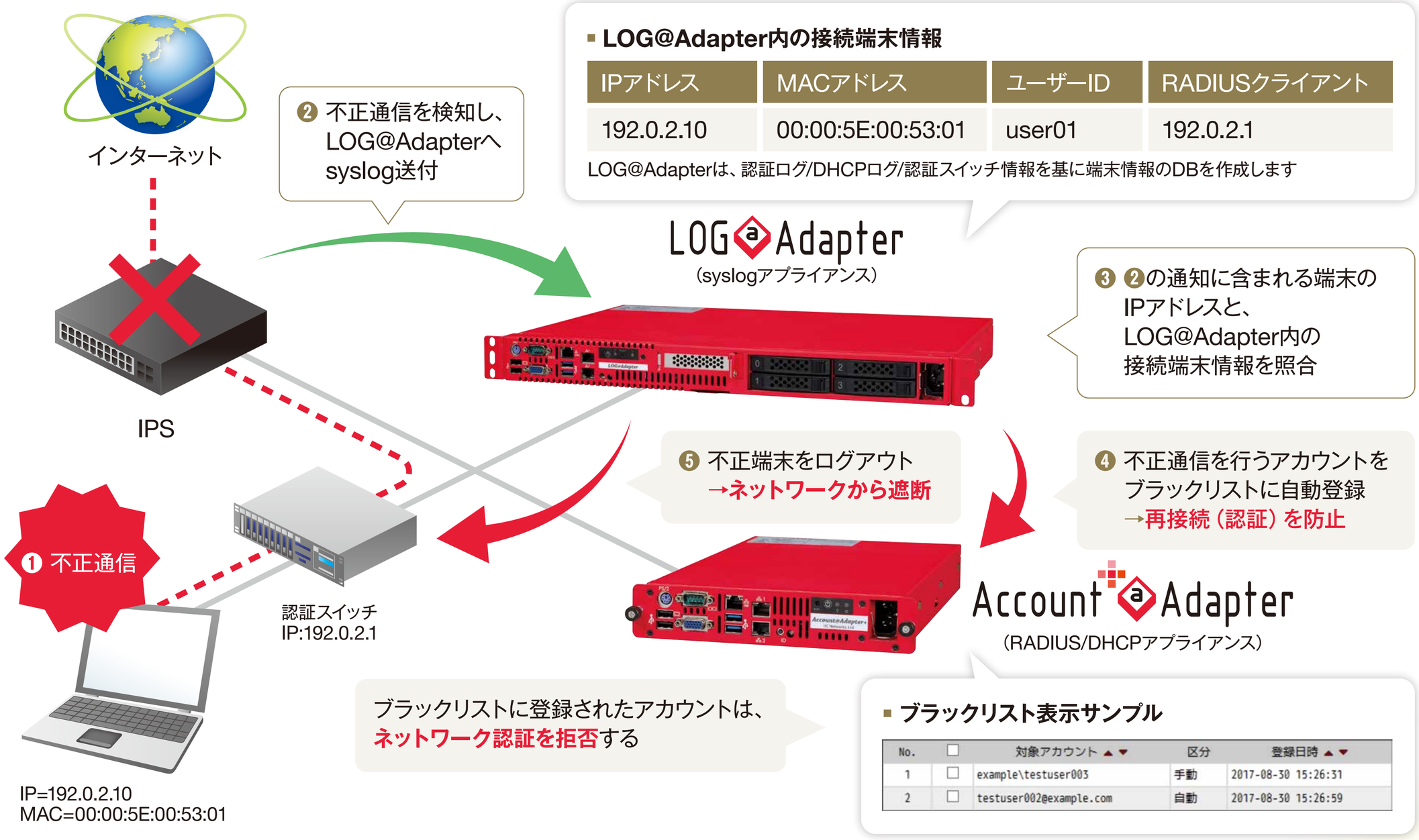
HCNET

不正通信端末遮断ソリューション

情報セキュリティ事故が起きたとき すぐに発生源の特定ができますか？

2017年5月12日、全世界的にランサムウエア「WannaCry」によるサイバー攻撃があり、日本国内においても大企業での感染例が報告されました。「WannaCry」ではWindows® OSのある脆弱性を利用して感染するしくみでした。マイクロソフト®社は2017年3月15日に対策パッチ（MS17-010）を公開しておりましたが、このパッチを適用していなかったコンピュータが感染、被害を拡大させました。

どのようなセキュリティ製品を使用しても
感染・被害をゼロにすることは困難です。
そのため、万が一情報セキュリティ事故が起きたとき、
素早く発生源を特定し、被害拡大を防ぐ必要があります。



■ **LOG@Adapter内の接続端末情報**

IPアドレス	MACアドレス	ユーザーID	RADIUSクライアント
192.0.2.10	00:00:5E:00:53:01	user01	192.0.2.1

LOG@Adapterは、認証ログ/DHCPログ/認証スイッチ情報を基に端末情報のDBを作成します

ブラックリストに登録されたアカウントは、**ネットワーク認証を拒否**する

■ **ブラックリスト表示サンプル**

No.		対象アカウント	区分	登録日時
1	☐	example\testuser003	手動	2017-08-30 15:26:31
2	☐	testuser002@example.com	自動	2017-08-30 15:26:59

- 検知だけで終わらない、遮断と再接続の防止
- ネットワークのエンドポイントで遮断
- 端末の設定変更不要
- syslogのしくみであるため、さまざまなIPS/IDS機器との連係が可能
- 任意のコマンド発行で端末遮断するため、さまざまな有線スイッチや無線コントローラー／アクセスポイントとも連係が可能
- 不正通信端末の可視化と遮断

■ **連係確認機器**

IPS	PaloAlto® Fortigate®+FortiAnalyzer® DAMBALLA　Checkpoint
認証スイッチ	APRESIA®　ALAXALA® Cisco® WLC
DHCP	Account@Adapter+ ISC-DHCP

エイチ・シー・ネットワークス株式会社