

## PRESS RELEASE

日本ダイレックス株式会社

### 物理的遮断に匹敵する最高レベルのサイバーセキュリティ

日本ダイレックス、完全な一芯一方向通信装置「DualDiode」の販売で  
米 OWL（アウル）社とマスターディストリビューション契約を締結  
重要ネットワークへの侵入・情報漏えい対策の世界標準的ソリューション  
電力など主要インフラ業界に向けて販売・サポートを開始

ネットワークインテグレーターの日本ダイレックス株式会社（本社：東京都千代田区、代表取締役：若山政敏）が、物理的かつ論理的なサイバー攻撃によって改変・改造が難しいハードウェア品質ベースの専用設計による一芯一方向通信装置ソリューション「DualDiode Technology<sup>®</sup>」（デュアルダイオード）をグローバルで展開する米 Owl Computing Technologies Inc.（本社：コネチカット州、以下：アウル）と国内のマスターディストリビューション契約を締結。本日より、電力など国内の重要インフラ事業者に向け、販売活動を開始します。

#### 一方向通信ソリューション出現の背景

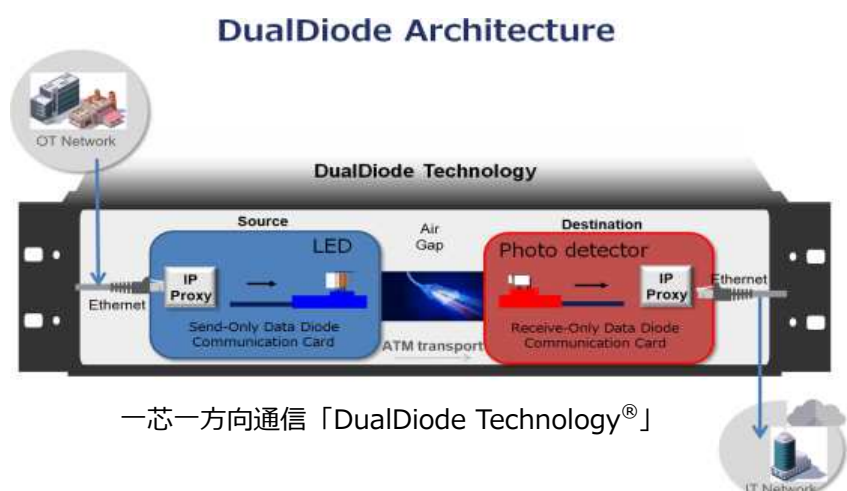
ICT 社会の中で、情報ネットワークセキュリティのリスクは高まる一方であり、重要なインフラである程、外部ネットワークと接続することは重大なリスクを伴います。サイバー攻撃に対する最大の防御は、他のネットワークと物理的に分離・遮断すること（エアギャップ）ですが、すべての通信が不可能になります。IoT 時代を迎え、特に産業制御システム(ICS：Industrial Control Systems)がビジネス系のネットワークやインターネットと相互接続してグローバル対応することが求められる現在、重要ネットワークといえども物理的遮断・隔離だけでは済まされません。ここに物理的なアクセスや論理的なアクセスで改竄させられないようなセキュリティ耐性のあるハードウェアベースの一芯一方向通信装置が求められる理由があります。

#### 一方向通信とは

内部ネットワークと外部のネットワークを繋ぐものの、エアギャップに匹敵するセキュリティ強度とされるのがデータダイオード（DataDiode）と呼ばれる一方向通信です。ハードウェアレベルで片方向しか通信できないように考案された特殊な通信装置で、いわゆるダイオードのように一方向にしか通信を許さない仕組みです。外部とネットワーク接続していないクローズなシステム、例えば、原子力発電所の最高セキュリティレベルの内部状況に対して、安全性を損なわないで外からモニタリングすることを可能にします。

#### 一芯一方向通信「DualDiode Technology<sup>®</sup>」

アウルの一芯一方向通信装置 DualDiode は、送信専用通信カードの発光素子（LED）と受信専用通信カードの受光素子（光検出器）を一芯光ケーブルで繋ぐ光方式を採用、両通信カードを直列に接続します。通信信号が送信・受信の逆方向に伝送されることがなく、ハードウェアベースの一方向通信を実現。受信側からの通信はエアギャップに相当する分断といえる状態となります。



一芯一方向通信「DualDiode Technology<sup>®</sup>」

送信側では、産業制御システム(ICS)などが重要情報を提供する際に使用する各種プロトコルを、送信専用マザーボード上に搭載されたプロキシ機能によって、ICS 側には代理応答を返し、且つ受益者側には一方向通信をします。受信側では、受信専用マザーボード上に搭載されたプロキシ機能によって、受益者側の業務系ネットワークに使用されるプロトコルに対し、代理応答をします。それぞれはモジュール化して搭載。両側の各ネットワーク内では双方向通信をしながら各エンドポイントが終端・保護されており、境界で一芯一方向通信を実現しています。

DualDiode では、独自開発による高品質・低遅延の ATM (非同期転送モード：Asynchronous Transfer Mode)データリンクプロトコルを使って、データのみを ATM ペイロードに乗せデータストリーミング化して情報受益者側に転送します。ハードウェア・パイプライン・アーキテクチャーを採用した ATM のチャネルに載せ替えることで、TCP/IP のような階層化プロトコル、即ち通信スタック固有の脆弱性から完全にブレイク (deep protocol break:統合分断)します。

セキュリティレベルの異なるネットワークを接続する場合、その境界を明確にした上で監督管理が容易にできる必要があります。そのためアウル社の DualDiode 製品 OPDS シリーズ (Owl Perimeter Defense Solution) では、電源及び管理コンソールを別々に実装し完全に独立して監督管理できるようにした上で一つの筐体に収納しています。

#### データダイオードの市場での導入状況

欧米では、主要政府機関・団体が整備・運用する法律やガイドラインで、セキュリティレベルの高い重要インフラの ICS には、一方向通信 (DataDiode) を導入することが明記され (※1)、対象ネットワークへの普及が進行しています。取り組みが遅れていた日本でも内閣官房サイバーセキュリティセンターなど各政府機関によりガイドラインが出されるようになってきたことにより、今後は普及が加速するものとみられます。

市場では先行する他社製品が存在したものの、不具合の指摘も見られ、日本ダイレックスには昨年来、顧客企業からの相談が寄せられるようになりました。要請に応じて世界のテクノロジーを涉猟する中、出会ったのがアウル社の一芯一方向通信装置 DualDiode Technology です。

#### DualDiode のグローバルでの導入実績

アウル社の DualDiode は、米国を中心に欧州、中東を含めグローバルで 2,000 以上のシステムの導入実績をもち、発電・変電・配電設備、鉱業、製造プラント、石油・ガスプラント、水処理・廃水処理、金融・銀行など主要インフラ事業者幅広く導入されています。同社はこれまで日本に現地法人・代理店企業がなかったために入札制度の問題やインテグレーション、メンテナンスサービスを実施できないことから参入が遅れていましたが、日本ダイレックスとの事業提携で日本上陸が果たせたこととなります。

#### ネットワーク現場への導入

通信接続において、情報提供者側から情報受益者へのパケットが輻輳等でロスした場合に、情報受益者側から発信される再送要求は、1 方向通信においては情報提供者側に通知することができません。このため 1 芯 1 方向通信装置の導入には、パケットロスが生じないよう、ネットワークの実態把握 (質・量・速さ) 技術が不可欠です。

日本ダイレックスは、ネットワークの実態調査 (アセスメント) サービスを実施しており、計測ネットワーク設計から分析・報告のネットワークインテリジェンス技術に深い知見・経験を保有しています。アウル社の DualDiode 導入の際には、このネットワークの計測技術を駆使して最適設計を行います。また最適設計において 1 方向通信装置のみでは解決できない場合は他のソリューションを組み合わせ提案し、インテグレーションをすることができます。

#### 展開戦略・販売計画

日本ダイレックスは今後、OWL のグローバルでの実績をもとに国内での DualDiode の早期の普及拡販、導入推進を図っていきます。対象分野は、先頃内閣官房サイバーセキュリティセンター (NISC) が定めた「重要インフラの情報セキュリティ対策に係る 第 3 次行動計画」で、重要インフラ分野とされた情報通信、金融、

航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油の13分野に、原子力、防衛、自動車の3分野を独自に加えた16分野と設定し、Sier、リセラーを経由してユーザー企業・各機関に販売を行います。

日本ダイレックスでは、長年培った国内入札ノウハウや、業界で評価の高い計測、制御、最適化設計の知見を生かして安全・最適・円滑で、迅速な導入を図り、国内でのテクニカルサポートも高品位に提供していきます。既に米国アウル社での技術者研修も完了しています。

「OWL DualDiode」の価格はオープン。2016年から3年間で100システムの出荷を目標としています。

#### アウル社 CEO のコメント

Owl Computing Technologies Inc.のCEO、ロナルド・ムラーツ（Ronald Mraz）博士は、本契約の意義について「これまで拠点が多かったため、当社の一芯一方向通信装置・DualDiodeシステムを日本の主要インフラ産業に適切に提供できずにいましたが、日本ダイレックスというまたとないパートナーを得ることができて嬉しい限りです。今後は我々のDualDiodeに、ネットワークを知悉した日本ダイレックスの実績ある高度な計測・制御・最適化設計技術を組み合わせることによって、日本の市場に安全で高速、しかも信頼性のあるソリューションを最適に導入していけることとなります。これは、我々にとってよりも、日本のすべての市民にとっての朗報と言えるのではないのでしょうか。」と述べています。

### ■一芯一方向通信装置 OWL DualDiode Technology

#### ●概要

- ①ハードウェアベースのサイバーセキュリティ対策装置
- ②一方向のみに設計されたハードウェアを使用
- ③ソフトウェアの改ざんや攻撃を遮断
- ④ハードウェアの変更は不可（不正改竄防止機構内蔵）
- ⑤ネットワークの各エンドポイントを終端・保護
- ⑥ネットワーク間のNon-Routable（IPアドレス、MACアドレスを転送しない）ATMによるプロトコルブレイクを実現
- ⑦送信側と受信側の管理は完全に分離されており、管理コンソールも別々にインターフェースが用意されている。

#### ●アーキテクチャー

- ①ハードウェア DualDiode — 送信専用通信カードと受信専用通信カードを直列に接続したハードウェアを内蔵
- ②エアギャップによるネットワーク分離 — 2つの通信カード（送信専用／受信専用）間にエアギャップを作り電気的な接続を完全に分離
- ③IPプロキシ — IPトラフィックを送信元で一旦終端し、送信先で起動するIPプロキシを内蔵
- ④一芯一方向ハードウェア — 一方向ハードウェアは、単一（一芯）の光ファイバケーブルによって強制的に一芯一方向通信を実現

#### ●セキュリティ属性

- ①ノンルータブル（non-routable） — ルーティング可能な情報（MAC、IPアドレスなど）は、ネットワークの外部にさらされることがなく、ペイロード部分のみがエアギャップ間を転送される。
- ②ATM転送によるディープ・プロトコルブレイク — エアギャップ間一方向転送に信頼性の高い高速ATM転送を採用しており、「ディープ・プロトコルブレイク」を実現している。
- ③ホワイトリスト化された転送制御 — すべてのデータタイプの転送がホワイトリスト化され制御される。

## ■ OWL DualDiode 製品ラインアップ

●製品名：OPDS-100／OPDS-100D／OPDS-1000

●製品共通：

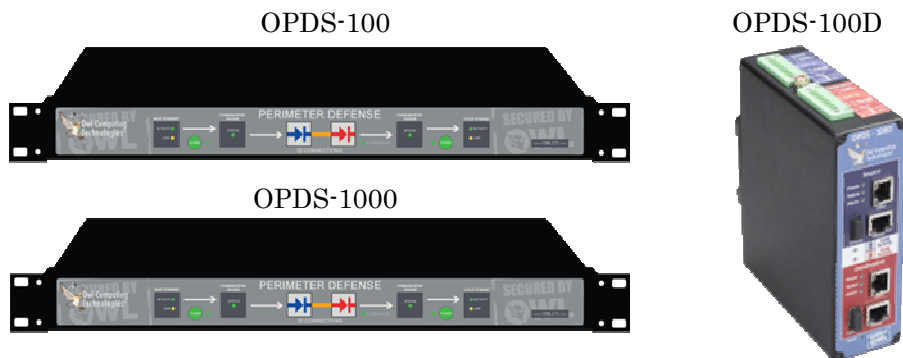
- ・一方向通信の送信部（IP Proxy 部および一方向データ転送部）と受信部（IP Proxy 部および一方向データ転送部）がすべて一筐体に内蔵されたオールインワン構造
- ・主な仕様：Owl CentOS／Owl RBAC／  
Owl コア転送アプリケーション  
(UDP、TCP、File transfer、FTP、email transfer、Syslog、SNMP)

### ① OPDS-100 シリーズ

- ・OPDS-100：19 インチ 1 U 実装可能な機器
- ・OPDS-100D：DIN レールで実装できる耐環境性強度が OPDS-100 より強化された機器
- 一方向転送部の転送速度（ライセンスによりフィールドで変更可能）  
10Mbps / 26Mbps / 52Mbps / 104Mbps

### ② OPDS-1000

- ・19 インチ 1 U 実装可能な機器
- 一方向転送部の転送速度（ライセンスによりフィールドで変更可能）  
104Mbps / 155Mbps / 300Mbps / 600Mbps / 1,000Mbps (1Gbps)



以上

【参考※1】重要インフラのICS への一芯一方向通信（Data Diode）の導入を明記した規程文書などを発行した海外の政府機関などの例：●国際原子力機関（IAEA）「IAEA Nuclear Security Series No. 17」●米・原子力規制委員会（NRC）「REGULATORY GUIDE 5.71」●米・国土安全保障省（DHS）「Seven Strategies to Defend ICSs」●北米電力信頼度評議会（NERC）「Compliance Application Notice — 0024 CIP-002 R3 Routable Protocols and Data Diode Devices」●米・国家安全保障局（NSA） 「括弧」内は文書名

### 【Owl Computing Technologies Inc. について】

米コネチカット州リッジフィールドに本社を置く Owl Computing Technologies Inc.（アウルコンピューティングテクノロジーズ）は設立以来 17 年間にわたり、ネットワークセキュリティ事業に特化して成長してきた独立系ベンチャーです。CEO は Ronald Mraz（ロナルド・ムラーツ）。シングル 1U、オールインワンソリューションのサーバーベースの通信カードシステムを開発し、決定論的一方向転送を実現しています。24 の技術特許を保持し、米国の国防、諜報部門が Cross domain サービス管理に関する技術やソリューションとして有効性を認証したプロダクトのリストである UCDSMO 認証を取得。また米国の機密情報及び最高機密情報取扱許可を受けています。研究開発から製造・技術サポートまで自社で手掛け、Owl DualDiode 技術認定サービス、構成管理サービスも提供。米国防総省、諜報機関、防衛などの政府系および、原子力、電気、ガス、水道、石油・ガス、石油化学、電気通信、金融サービスなどの顧客を持ち、グローバルで 2000 以上の導入実績を誇ります。詳細は、<http://www.owlcti.com/>

## 【日本ダイレックスについて】

40年以上にわたり、ネットワークインテグレーション事業を継続。情報通信ネットワークシステムの構築、保守サービスをはじめ、ネットワークシステムに係るハードウェア、ソフトウェアの開発、製造、販売、賃貸及び輸出入、およびシステムの開発、販売を幅広く手掛けています。技術力に定評があり、特にネットワークシステムの計測、制御、最適化設計に高い評価を得ています。信頼性の高いネットワークを設計構築し、国内の大手顧客企業と長期の関係が継続する中、時代の要請に応える製品・サービスを開発・提供しています。

### <会社概要>

社名：日本ダイレックス株式会社（英文社名 JAPAN DIREX CORPORATION）

所在地：東京都千代田区内神田2丁目5番5号 ヒューリック大手町北ビル7F

創立：1973年3月16日

資本金：8,300万円

代表者：代表取締役：若山政敏（わかやまさとし）

従業員：50名（2016年4月現在）

事業所：東京本社、大阪支店、名古屋支店、福岡営業所

一般第二種電気通信事業者 / ISO 9001 認証取得

### 一般読者からのお問い合わせ先（記事表記上）

日本ダイレックス株式会社 営業グループ  
TEL：03-5207-7160  
E-mail：sales@direx.com  
<http://www.direx.com/>

### 本件に関する報道関係のお問い合わせ先

Direx-owl 広報事務局  
TEL：03-4405-8773 担当：河端、川口  
E-mail：direx-owl@alsarpp.co.jp

## 【ご案内】

### OWL 日本進出記念・Direx スペシャルセミナー開催

米 OWL 社、CEO ほか幹部が来日。OWL のすべてをダイレクトにご説明。デモ実演も実施

より詳細にご取材ご希望の方はぜひご参加下さい。

●6月21日（火）13：00～16：15

●イイノホール&カンファレンスセンターRoomA（4F）

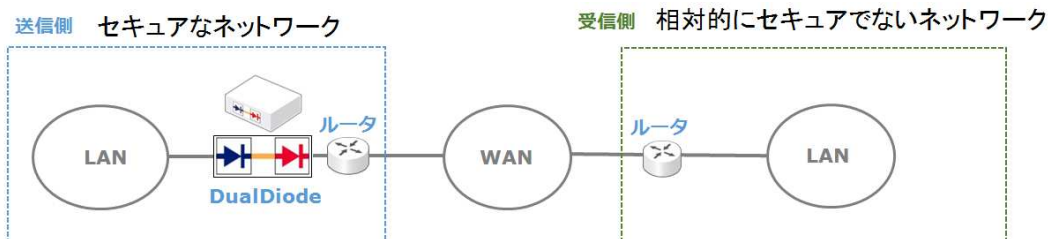
お申込：t0710tak@direx.com 担当：日本ダイレックス 高松利之

# 別紙・技術解説 -1

## ■一芯一方向通信装置（DualDiode）の配備方法

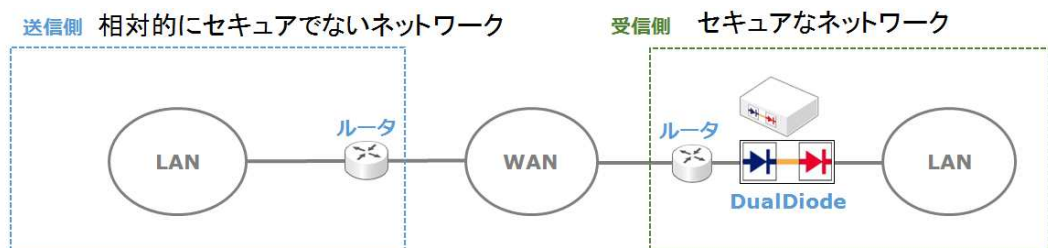
一芯一方向通信装置（DualDiode）は、基本的には、二通りの配備方法があります。（1）重要情報を提供する側のネットワーク側に配備して、必要に応じて外部の機関に通信を使って情報提供はするが、外部からのサイバー攻撃を阻止する利用方法と、（2）情報収集側のネットワークに配備して、外部から効率良く収集するが、従業員が内部の重要情報を漏洩させるようなことのない、インサイダー攻撃を阻止する利用方法です。

### ●1. 情報提供者側防御接続形態（リードダウン：read-down 接続形態）



DualDiode の送信側（Blue 側）と受信側（Red 側）は、独立した個別の管理コンソールが用意されており、管理者の役割に応じて別々に管理する。

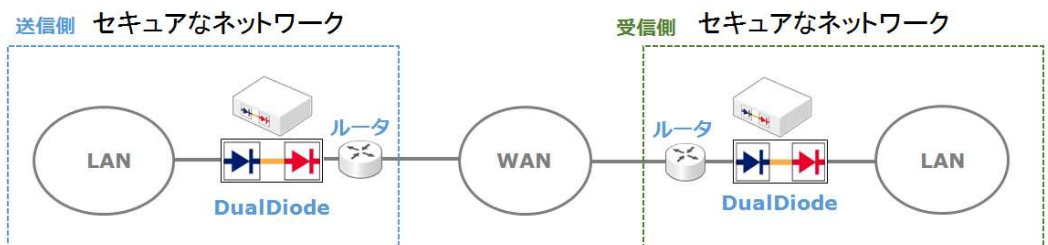
### ●2. 情報受益者側防御接続形態（リードアップ：read-up 接続形態）



DualDiode の送信側（Blue 側）と受信側（Red 側）は、独立した個別の管理コンソールが用意されており、管理者の役割に応じて別々に管理する。

### ●3. 情報提供者側／受益者側防御接続形態（リードダウンアップ：read-down/up 接続形態）

上記の基本的な二通りの配備方法以外に、送信側、受信側両方がセキュアなネットワークで WAN ネットワークなどの相対的にセキュアでないネットワークを経由して一方向転送を実施する接続形態。典型例として複数の研究所間で機密性の高いデータの一方転送を実施するような利用形態があります。



DualDiode の送信側（Blue 側）と受信側（Red 側）は、独立した個別の管理コンソールが用意されており、管理者の役割に応じて別々に管理する。

### ■一方向通信装置の通信方式

一方向通信装置といわれるものの通信方式は、技術的に以下のタイプに分類されます。

- (1) RS-232 ケーブル接続の戻り線をクリップ（切断）して送信専用にしたもの（ケーブル・アセンブリ方式）
- (2) イーサネット通信プロトコルにフィードバック機能を追加したり、なりすましプラットフォームを介在させて、順方向のデータを確保するもの（イーサネットフェイク方式）
- (3) 光・銅線間接続でメディア変換（双方向通信デバイス）だけを単に一方方向に改造したもの（メディアコンバータ・方式）
- (4) 汎用 OS やアプリケーションのアクセス・ルールと非対称暗号化鍵を使って、書き込み専用アクセス権を持つ送信元だけがデータを暗号化し、読み取り専用アクセス権をもつ着信先だけが別の鍵を使って復号することでデータの一方方向を確保するもの（複合ソフトウェア方式）
- (5) ファイアウォールをバックツーバックに接続して入り口側に配備したファイアウォールは送信元からのデータを受付、出口側のファイアウォールは着信先からのトラフィックを拒否することで一方方向性を確保するもの（ファイアウォール方式）

上記 5 つの方式には、以下の問題点があります。

着脱可能なケーブル・アセンブリ方式（上記（1）方式）はセキュリティの観点からは論外として、どれをとっても脆弱性のもととなっているルータブル情報とエラー再送機能を標準とする双方向通信方式を土台にしたものばかりです。

ドメインの境界の曖昧さや構成の難しさから穴だらけの「スイスチーズ」と揶揄されるファイアウォールの組合せによるネットワーク対応（上記（5）方式）や、これまでも同じようにこの種の脆弱性で攻撃を受けてきた汎用 OS のリード/ライトアクセス権を使った一方方向性（上記（4）方式）か、ドメイン隔離を保証するための重要なプロトコル・ブレイク処理をまったく無視したエンド・エンド間をまったく同じ通信プロトコルを使った一方方向（上記（2）方式）や、誤り検出や再送要求 (ARQ)、フロー制御などの処理は行わないで IP パケットをそのままの形で転送する、UDP/IP の単方向性を利用しているものです。（上記（3）方式）

このようにどれをとってもユビキタス時代の利便性と信頼性を追及した機能中心の技術をベースにしたものです。ネットワークの根本的な脆弱性は、ネットワークを構成するノードがルータブル情報 (MAC アドレス、IP アドレス) をもとにアドレス条件が一致すれば、送信と受信の 2 本の論理経路を介してコミュニケーションできる仕組みにあります。

何時でも何処でも接続できる信頼性の高い通信を可能にしたのは、これらの双方向通信技術と汎用 OS 並びに通信アプリケーションによる通信機能にあるのです。この利便性を追及した技術はほとんどがソフトウェアです。「通信あるところに脆弱性あり」「ソフトウェアの機能あるところに脆弱性あり」といわれるほど、品質主導の通信パフォーマンスと防衛主導のセキュリティは完全に相反の関係にあります。ここに、双方向通信を否定して極力ハードウェアをベースにした一方方向通信設計が必要なのです。

DualDiode 一芯一方方向装置の特徴は、アウル社独自の開発による高品質・低遅延の非同期転送モード (ATM : Asynchronous Transfer Mode) データリンクプロトコル (OSI 参照モデルの 2 層) を使って、情報提供者側から転送されてきた階層化プロトコルのヘッダ情報を除去してデータのみを ATM ペイロードに乗せデータストリーミング化して情報受益者側に転送します。ハードウェア・パイプライン・アーキテクチャを採用した ATM のチャンネルに載せ替えることで、TCP/IP のような階層化プロトコル、即ち通信スタック固有の脆弱性から完全にブレイク (deep protocol break: 統合分断) します。

アウル製 DualDiode は、一方向通信のプロトコルに ATM を採用しています。

ATM はもともとルーダブルプロトコルではなく、IP 情報を一切使う事なく一方向通信を可能にするものです。一方向通信の問題の一つに着信先のトラフィック状況やメモリ容量の制限のために瞬間的なトラフィックが原因でデータロスが発生する事で、データの完全性が保証できない点です。その点は、可変長のパケットとは違って ATM の固定長セルを使う事から、送出速度制御が容易に行われ、バーストデータに強い転送品質が得られるように設計されています。

## ■ アウルのセキュリティパッチファイル確認システム

アメリカ合衆国国土安全保障省（United States Department of Homeland Security、略称：DHS が提唱する Seven Strategies to Defend ICS には、重要で且つセキュアなネットワーク内にある通信ノードの脆弱性の標的とした攻撃の防御のためにセキュリティパッチ、OS アップデートなど安全に実施することとしています。そのためアウル社は SSUS（Secure Software Update Service）を開発しました。重要設備へのセキュリティパッチファイルのインストールをする前に予め信用のおけるセキュアなリソースサーバで作成されたセキュリティパッチファイルであるかどうかを DualDiode に実装された SSUS が高速で確認し、本物と判断されたセキュリティパッチファイルのみ重要設備のあるセキュアな LAN に通すことができます。

