SOHO/家庭でインターネットを安全に使うネットワークの構成

エレクトロニック・サービス・イニチアチブ

このスライドで分かる事

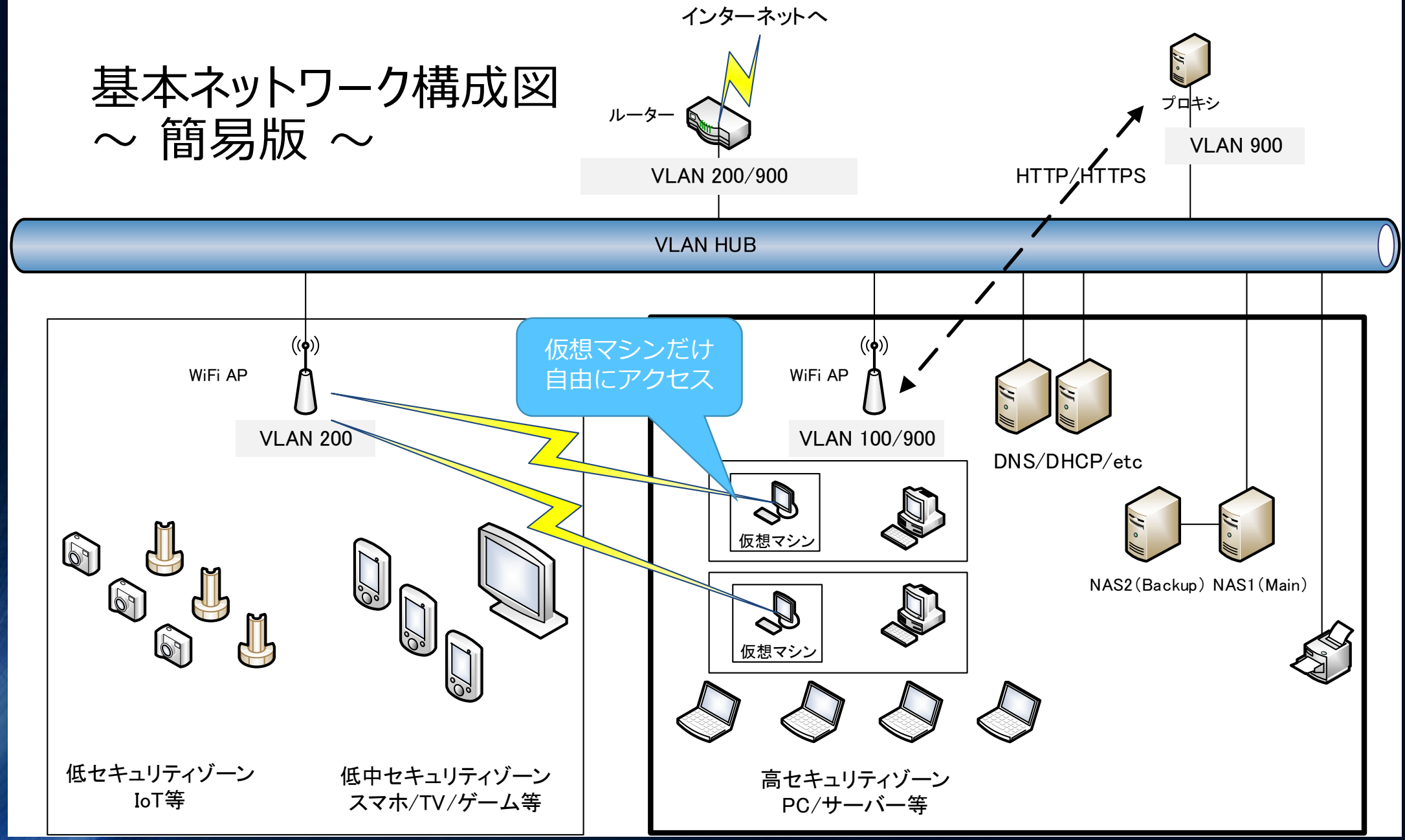
- より安全にインターネットを利用できるネットワーク構成
- より安全なネットワーク構成に必要な機器

- 足りない事：より安全なネットワーク構成に必要な設定
  - 環境に合わせた設定の種類は非常に多いので、このスライドの対象外です

より安全にインターネットを利用できる ネットワーク構成

- インターネットの利用は常にリスクが伴います。このスライドではより安全にインターネットを利用できる「仕組み」を紹介します。
- できる限り容易/安価に入手可能な機器を使います。
- できる限り容易に利用可能な環境を目指します。
- 大幅にリスクを軽減可能ですが、リスクがなくなる訳ではありません。
- 残念ながら、実際にこの構成を実装するにはITシステムの専門知識が必要です。

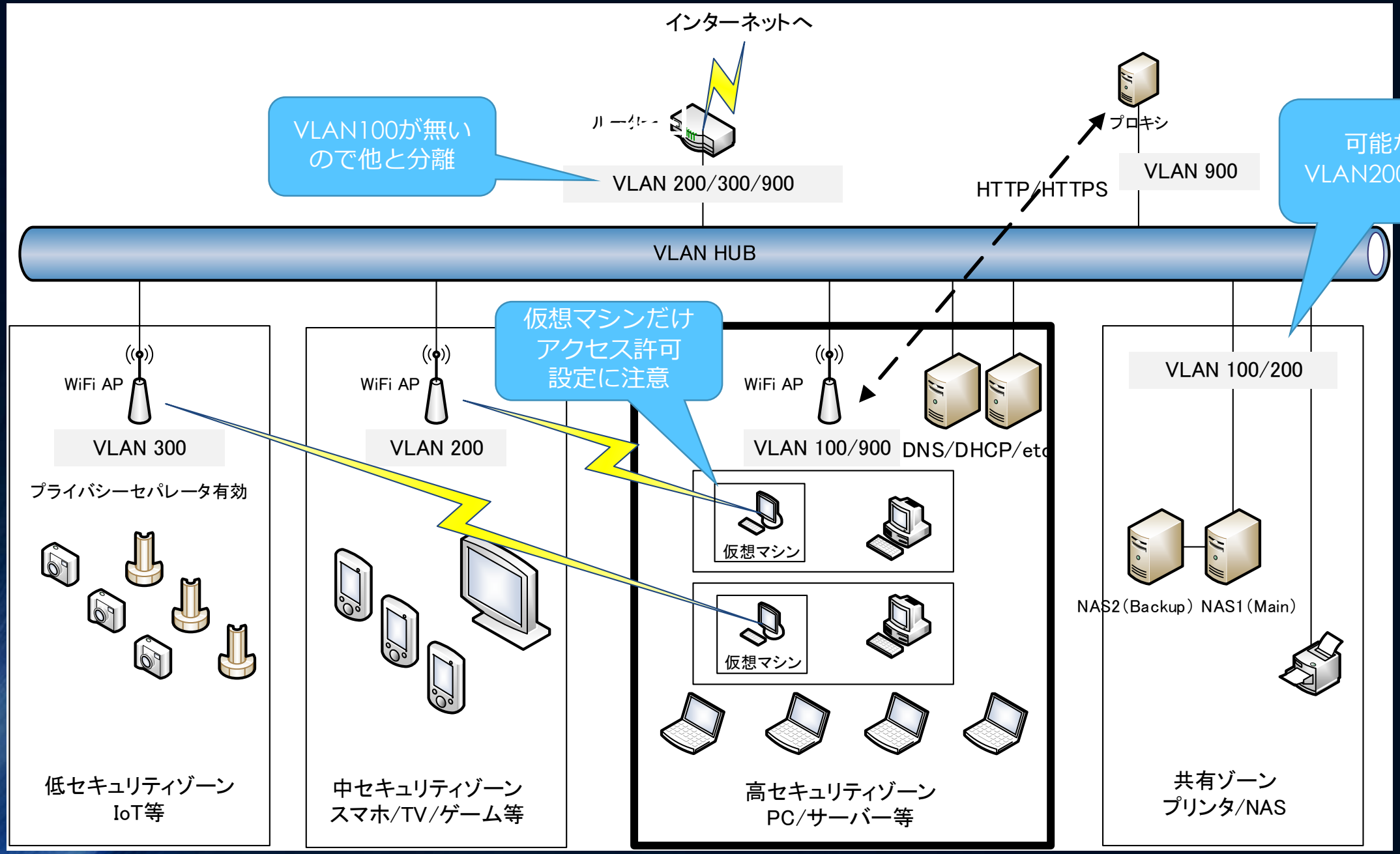
基本ネットワーク構成図
～ 簡易版 ～



簡易版ネットワーク構成の説明

機器コスト：VLAN HUBと
WiFi AP 2台を購入する場合、
最小 1万5千円程度から

- **VLANが3つだけで構成と管理が容易**
  - その分、必要な機器も減り導入コストが少なくなる
  - 代わりにリスクが高くなる
- 高セキュリティゾーンからのインターネットアクセスはローカルネットワークへのアクセスを禁止し、**ローカルネットワーク/ローカルホストへのクロスサイト攻撃が原理的にできない構成**にする
  - 高い安全性を維持するためにはインターネットからローカルネットワーク/ローカルホストへのクロスサイト攻撃を仕組み（プロキシ）で防止することが重要
  - 簡易構成でも「プロキシ」は後述の通り、ホワイトリスト型でアクセス可能なサイトを制御することが重要
- 危険性が高いIoTをネットワーク的に分離しているので、一つにまとめている場合に比べ安全性は高い



基本ネットワーク構成図の説明

機器コスト： 使用する機器に大きく左右されるが、最小５万円程度から

- **VLANでセキュリティゾーンごとに分離**
- 各ゾーンは基本的にWiFiの利用を想定
  - 有線LANを使っても構わない
- **高セキュリティゾーンは高いセキュリティが必要な物“だけ”を設置**
- **インターネットアクセスには“ホワイトリスト型”のプロキシを利用**
  - プロキシを利用しないアクセス、IoTゾーンへのアクセスは仮想マシンから
- IoTの様にセキュリティ問題の多い物はWiFiのプライバシーセパレータを利用
  - TVが中セキュリティゾーンに配置（DLNA対応）されているが、可能なら低セキュリティゾーンへ
- 共有ゾーンには中高セキュリティゾーンからアクセスする物を配置
  - セキュリティが弱くなる点に注意。本来はここに重要なモノは設置したくない。

低セキュリティゾーン

- **IoTは基本的に脆弱な物が多いので確実に分離**
  - IoT：ネットワークカメラ、スマートスピーカー、TV、AV機器、冷蔵庫など
- スマートスピーカーやネットワークカメラは攻撃が成功した場合、ネットワークから分離していても音声・画像で情報がリークする点に留意
  - これはスマホやPCでも同じ
- 制御・アクセスが必要なIoTがある場合、他のセキュリティゾーンの仮想マシンから低セキュリティゾーンのWiFiに接続するか、有線LANで低セキュリティゾーンのVLANに接続
  - WiFiの場合、基本的には**プライバシーセパレータを有効**にする
  - IoT利用にWiFi接続が必要な物がある場合、仕方ないのでプライバシーセパレータを無効にする（セキュリティレベルが低下する点に注意）
  - 有線LAN経由でVLANに接続した場合、プライバシーセパレータの状態に影響されるVLAN内のデバイスと通信できる
- OSを更新できない**古いスマホなどもこちらに接続**する

中セキュリティゾーン

- 比較的安全性の高い**新しいスマホなどで利用**
  - とは言っても無暗に余計なアプリをスマホに入れるべきではない
- 現在のゲーム機はネットワーク対応でシステムの更新もされ、比較的安全性が高いと考えられる
  - 海賊版や改造版はリスクが高い。そもそもこういった物は使うべきでない。これはroot化したスマホなども同じ
- 基本構成図にはDLNAなどの為にTVが入っているが、TVもIoTで高リスクのデバイス。可能ならIoTゾーンで利用
  - AVレシーバーなどDLNA対応の機器もこのゾーンを利用
  - TVやAVレシーバーなどインターネット対応機器のセキュリティ更新には期待できず、リスクが高い
  - 基本として、更新されない、あまり更新されない機器は危険だと考える

高セキュリティゾーン

- **ルーターのネットワークからVLAN100を削除しているので完全に分離できる！**
  - インターネットへはWebプロキシからのみアクセス可能
- 高セキュリティゾーンには確実に管理された（**余計なプログラムなどが一切導入されず、最新状態に保たれたOSの機器**）PCなどを配置する
  - 従業員や子供が勝手にインストールできないようアクセス許可を管理
  - WiFiアダプターには「親機」機能もある。勝手にWiFi「親機」を設置させない。
- インターネットから**ダウンロードしてきたプログラムは一切導入・利用しない**
  - 試用してみたい場合、低中セキュリティゾーンのネットワークから行う
- メールは攻撃の入口になりやすい。メールの利用は中セキュリティゾーンで行うのが好ましい
  - 共有ネットワークのVLANはリスクが高い点に注意。重要なモノは高セキュリティゾーンに設置する。NASも可能ならここに置く。

プロキシの説明

- **ローカルホスト、ローカルネットワークへのアクセスは許可しない（重要）**
  - クロスサイト攻撃対策。Squidなどで簡単にローカルホスト、ローカルネットワークへのアクセスを禁止できる
- 利用可能なインターネットサイトは信頼可能なサイトに限る
  - Google、Facebook、Twitter、Yahoo、Microsoftなど
    - ただし、これらのSNS系サイトはリスクが高い
    - Windows Updateの利用に必要なサイトへのアクセス許可を必ず行う
    - AWS等クラウドへのアクセス設定に注意。クラウド全体にアクセス許可を与えると危険
- 高いセキュリティにしたい場合、高セキュリティゾーン機器からは限られた必要なサイトに限り、**自由なインターネットへのアクセスは仮想マシンを使って、中セキュリティゾーンから行う**

利用する機器の説明

機器	説明	備考
ルーター	Fletsなどのルーターで構わない。WiFiルーターでもOK。ただし、WiFiルーターを利用する場合、ルーター専用にしてWiFiは「絶対に使わない」	DHCPはこのルーターで実行。管理用アクセス設定を確実に行うこと。
VLAN HUB	高価なVLAN HUBは必要ないが、ポート数は多めが良い。**SOHOなら24ポート、家庭でも16ポート以上**をオススメします。	管理用アクセス許可設定を確実に行うこと。デフォルトだと誰で設定変更可能。
WiFi AP	VLAN対応のWiFi APは比較的高価なので、複数購入する方が安価。ただし、SOHOの場合は管理性を考慮しVLAN対応/マルチSSIDも検討。	ルーター機能は必要ない。管理用アクセス設定を確実に行うこと。
プロキシ	RaspberryPi、スティックPCでも通常は十分。普通のPCでもOK。	必要な制御が可能なプロキシが使えるOSならどれでもOK。
NAS	価格・拡張性・耐障害性を考えるとNetGearの**ReadyNAS**が検討に値する。これは小さな障害が発生した場合のデータ破壊防止機能がある。	X-RAID2を利用すること。

利用するソフトウェアの説明

ソフトウェア	説明	備考
仮想マシン管理	家庭なら**VMware Workstation Player**がオススメ。SOHOで無償が良い場合、**VirtualBox**が利用できる。	VMware Workstation Playerは個人用途は無償利用可能。VirtualBoxどちらも無償利用可能。ホストマシンは16GB以上のメモリ＋512GB以上のSSDを推奨。
仮想マシン	OSは、最新状態を維持できるOSなら、どれでも構わない。	ホストOSと異なるOS/ウィンドウマネージャーにすると画面上で解り易い。ライセンスを考慮するとLinuxが検討に値する。
プロキシ	Linuxなら**Squid**で十分。 サーバーを高セキュリティゾーンに設置している場合、これを使っても構わない。	高セキュリティゾーンの機器からはプロキシ経由でのみ、インターネットにアクセス可能にする。プロキシでアクセス可能なWebサイトを厳しく管理しないとセキュリティが弱くなります。極力、アクセス可能な外部サイトは少なくします。

ルーター用機器の例

- 家庭用の場合、Fletsなどで有線ルーター設置済みの場合、通常はそれで十分です。
  - WiFiルーターの場合、**WiFi機能をOFF**にして利用、でもOKです。
  - ルーター専用機はビジネス用途向けで価格が高い。家庭用に購入する場合、**有線LANが１Gbps以上のWiFiルーターを購入**します。
  - https://amzn.to/2pBdKEc（NETGEAR WiFi 無線LAN　R6850-100JPS）
- SOHOなどの場合、ルーター専用機をオススメします。
  - https://amzn.to/2Gh2V4y （ヤマハ RTX830 ギガアクセスVPNルーター）
  - 設定に専門知識が必要ですが、Linuxをルーターにすることも可能です。

VLAN HUB機器の例

- HUBは**必ずVLAN対応の製品を購入**。現在はVLAN有り/無しでほぼ価格が同じ。VLANを使わない場合も、リモート管理が可能なVLAN有りを選択します。ケーブル検査機能もありトラブル時に便利です。 PoE対応（LANケーブルで電源供給）のアクセスポイントの場合はLANケーブルのみでアクセスポイントに電源を供給できます。
  - NETGEAR スイッチングハブ ギガビット16ポート　GS116E-200JPS
  - https://amzn.to/2I0Ee9G（NETGEAR PoE無し 16ポート GS116E-200JPS）
  - https://amzn.to/2G02Cf3（NETGEAR **PoE対応** 16ポート JGS516PE-100AJS）
- SOHOの場合は24ポートの方が安心です。別の部屋等、**少ないポートで良い場合もポート数の少ないVLAN対応HUB**にします。
  - https://amzn.to/2FYvpRn （NETGEAR PoE無し 24ポート JGS524E-200AJS）
  - https://amzn.to/2G0Rzm7（NETGEAR **PoE対応** 24ポート JGS524PE-100AJS）
  - https://amzn.to/2Gh3wDk（NETGEAR PoE無し 8ポート GS108E-300JPS）
  - https://amzn.to/2pCdy7L （NETGEAR **PoE対応** 8ポート GS108PE-300AJS）

WiFi　AP（アクセスポイント）機器の例

- ルーター機能は必要ありません。ルーター機能を無効にして今あるWiFi機器を使っても構いません。接続機器が多い場合はサポートする接続数に注意。**PoE対応**にする場合、SOHO用のAPを利用します。
  - https://amzn.to/2Gh8JLo（NETGEAR R6120-100JPS）
  - https://amzn.to/2GoDduS（NETGEAR R6350-100JPS）
- SOHOの場合、管理機能が強い法人向けをオススメします。HUBがPoE対応の場合、PoE対応APが便利です。
  - 以下の機器は**PoE対応、VLAN対応、マルチSSID対応、DHCPサーバー機能なし**、です。
  - https://amzn.to/2G0Gj9b　（NETGEAR PoE対応 WiFi AP WAC505-10000S）
  - https://amzn.to/2G5uTNq　（3台セット）
  - https://amzn.to/2HZewCu　（PoEでない場合、別売り電源アダプター PAV12V-100NAS）

仮想マシンの追加のWiFiネットワークアダプタ

- 高セキュリティゾーンから、**他の低いセキュリティゾーンへのアクセスには「追加のWiFiネットワークアダプタ」を用いて行う**
- 必要な速度などに応じて適当な物を購入する。
  - https://amzn.to/2uep7rj （無線LAN子機 WLI-UC-GNM2S）
  - https://amzn.to/2G8ZRnO （無線LAN 子機 WI-U2-433DMS）
  - https://amzn.to/2pBP0eU （無線LAN 子機 WI-U3-866D）

プロキシ用機器の例

- Window 10 HomeスティックPC
  - Windows版　Squidが利用可能。Linuxに入れ替えも可能
  - https://amzn.to/2G3U5aU　（VANGOOD VG-MN9 Atom X5）
  - 有線LANにはUSBネットワークを利用
  - https://amzn.to/2I2BDw1　（有線LANアダプター LUA4-U3-AGT）
- Raspberry Pi3
  - Linuxが利用可能
  - https://amzn.to/2G0XHKZ　（Raspberry Pi3 コンプリートスターターキット）
- コスト重視の場合、仮想マシンに上記のUSB NICを使いVLAN900に接続させて代用することも可能

NAS用機器の例

- 価格と性能を考慮するReadyNASの４ベイ（HDD4台）モデルがオススメです
  - X-RAID2以外を利用する意味はありません。
  - **リンクアグリゲーションが利用可能なので1台でHUBの2ポートを利用**する。1Gbpsだとシーケンシャルアクセスで帯域を使い切ります。特にバックアップ用にもう一台購入する場合に重要です。
  - スナップショット（ファイルシステム状態の保存）が利用できるので、ディスク容量は大きい方が良い。
  - **バックアップ用にもう一台NASを買っておくと安心**です。
  - https://amzn.to/2ukEq1s （NETGEAR ReadyNAS 214 4ベイモデル）
  - https://amzn.to/2I2BRDn （TOSHIBA 3.5インチ 内蔵 HDD 6TB MD05ACA600）

より安全なネットワーク構成の拡張例
～　自動プロキシ設定、IPルーティング　～

- **VLANはLANを完全に分離するが……**
  - **分離しても「繋がっているネットワーク」などからのリスクは残ります！**
  - VLANだけだとサブネットが一つのSOHOクラスまでが最大限
  - 自動プロキシ設定を利用する（そうしないとかなり使いづらい）
  - **必ずルーターからVLAN100にはアクセスできないようにする**
- **IPルーティングを併用すると、よりきめ細かい制御が可能**
  ＝ より安全性が高く、より使いやすい構成が可能
- 構成の柔軟性は高くなるが、必要な機器、運用負荷も増える
- IPルーティングを併用した構成にする場合、ある程度本格的なルーターを導入する必要がある
  - https://amzn.to/2uioVHu　（NETGEAR マネージスイッチ GSM7212F-100AJS）
  - https://amzn.to/2G5pjig　（NETGEAR マネージスイッチ GSM7224P-100AJS）

その他

- 無用な接続性の問題をできる限り回避するため、可能な限りNETGEAR製品まとめました。
- 既存の機器がある場合は仕方ないですが、新しく構築する場合は同じメーカーでそろえると問題が発生する可能性を少なくできます。
- 安価なWiFi APは同時接続可能な機器が少ないです。多数の機器を接続する場合、対応可能な同時接続数に注意してください。
- PoE対応機器を使用する場合、サポートする電源容量などに注意してください。

自ら設置することが難しい場合

- 細かな設定はこのスライドでは省略しています。
  - ITシステム、特にネットワーク関連の知識がないと複雑な構成・設定は困難だと思われます。
- ネットワーク構築に強い近隣の情報システム会社にお願いすると良いでしょう。
  - 「近隣」は重要です。実際に現場での見積り/作業が必要なので「近隣」の情報システム会社でないと余計なコストが必要になります。
- 専門知識を持った会社の見積りはそれなりになります！
  - 必要な機器の合計価格がオマケに見える見積りになることを覚悟してください。
  - 高ければ良い、というモノではありませんが、技術力/サポート力は概ね価格と比例します。

お問い合わせ先

エレクトロニック・サービス・イニシアチブ

https://www.es-i.jp/

sales@es-i.jp