テレワーク普及で

# フリーアドレスオフィスがニューノーマルに

## - 失敗しない無線LAN構築ポイント -

目次

■ はじめに
テレワークの普及で、フリーアドレスオフィスがニューノーマルに
フリーアドレスオフィスのメリット
■ 1. 無線 LAN の懸念点
■ 2. 失敗しない無線 LAN 構築ポイント
- 設計・構築編
- セキュリティ編
- 運用編
■ 3. クラウド型+フルマネージドのサービス『Hypersonix』
■ まとめ

# はじめに

## テレワークの普及で、フリーアドレスオフィスがニューノーマルに

昨今、新型コロナウィルス感染拡大の影響を受けテレワークでの働き方がニューノーマルになりつつあります。これを受け、オフィスへの出勤スタイルが大きく変化し、フリーアドレスオフィスが改めて注目を集めています。

これまでの出勤といえば毎日当たり前のように会社へ通うものでした。しかしテレワークが普及した今、「**会議のため**」「**集中するため**」**と目的ありきの出勤**に変わりつつあります。そんな新しい出勤スタイルの中で、これまでのように固定席を設け、オフィスを維持していく事は、物理的・コスト的にも勿体ないことです。フリーアドレスオフィスなら、限られたオフィススペースを有効活用でき、集中用ワークスペースや、多様なスタイルのミーティングスペースの確保など、出勤目的に合致した労働環境を提供することが可能です。今後、**テレワークの普及が進むと共にフリーアドレスオフィスも、ニューノーマルなオフィス環境となっていくことでしょう。**

本ホワイトペーパーでは、フリーアドレスオフィスの基盤ともいえる無線 LAN 環境について、機器選定から設計・導入・運用まで、失敗しないためのポイントを多数ご紹介します。

# フリーアドレスオフィスのメリット

## 自分に合ったスタイルで働ける

その日の気分に合わせて自由に席を選べるので、快適に仕事に取り組めて生産性、集中力 UP

## コミュニケーションの活性

部門や役職を超えた円滑なコミュニケーションが生まれる。また、業務にあわせたチーム編成も容易に行える

## 美しいワークスペース

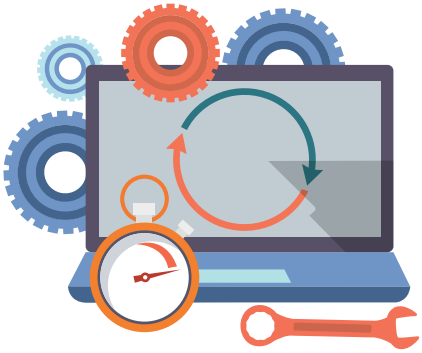
デスク数を抑え、空いたスペースを有効活用。新しいスタイルのミーティングスペースを設置するなど空間演出も思いのまま

| POINT! | これらのフリーアドレスのメリットを享受するには、<br>全オフィスエリアをカバーする快適な無線LAN環境が必要不可欠 |
|---|---|

# 1. 無線LANの懸念点

## 無線LANは有線LANと比べて不安定？

有線 LAN の障害といえば経年劣化や断線程度でしたが、無線 LAN は障害発生時の原因特定から解決までかなりの時間と労力を要します。フリーアドレス化すると無線 LAN をメインに業務が行われるわけですから、全従業員の業務をストップさせない為にも、安定した無線 LAN 環境を構築・運用する必要があります。



## 不正アクセスされない？

物理的なセキュリティ（IC カード等）が施されているオフィス内に入室しないと接続できない有線 LAN と異なり、無線 LAN は外から社内ネットワークへアクセスされる可能性があります。強固な認証システムの採用と適切なセキュリティ設定で、不正アクセスからしっかりと身を守らなければなりません。

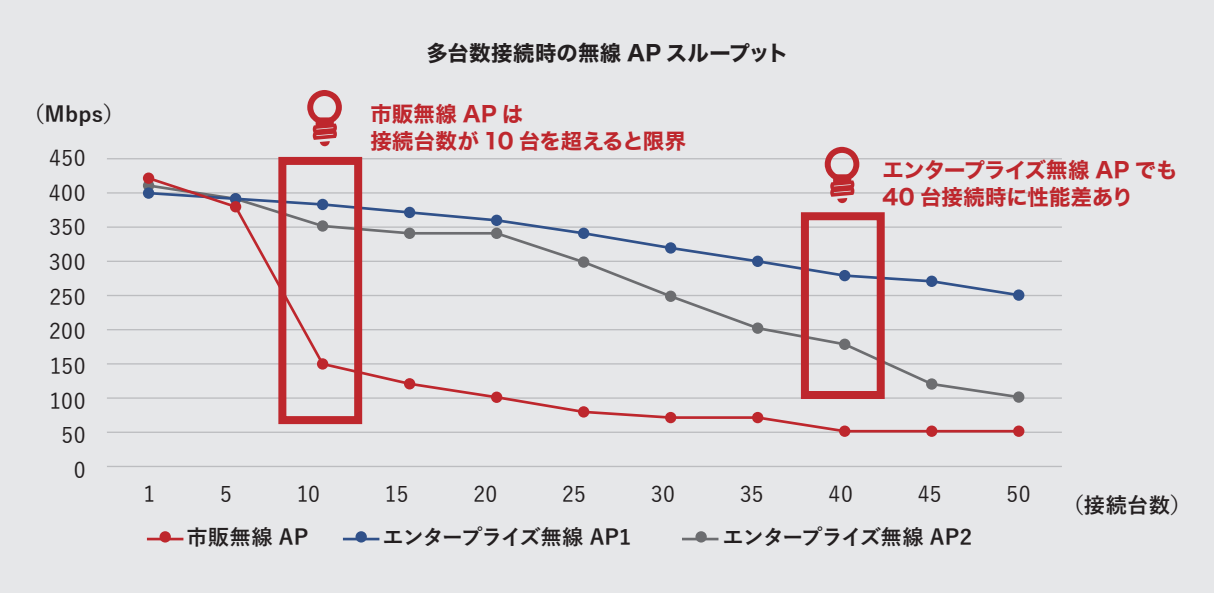
## 大規模・多拠点になるほど管理が煩雑？

大規模・多拠点になればなるほどすぐに駆けつけて対応することが難しくなります。例えば、遠方で急にトラブルが発生したら、当然現場の方とやり取りしなければなりません。遠隔からの指示には限界があり、加えて「無線 LAN が遅い」や「特定の時間帯だけ使えない」などといった曖昧な表現も合わさり、これらの対応には非常に手を焼きます。そのため導入して終わりではなく、リスクマネジメントの観点からもトラブル時にどのように対処するのか、運営体制までしっかりと整えておく必要があります。

# 2. 失敗しない無線LAN構築ポイント
## – 設計・構築編 -

## 1. 適切なスペックの機器を選ぶ

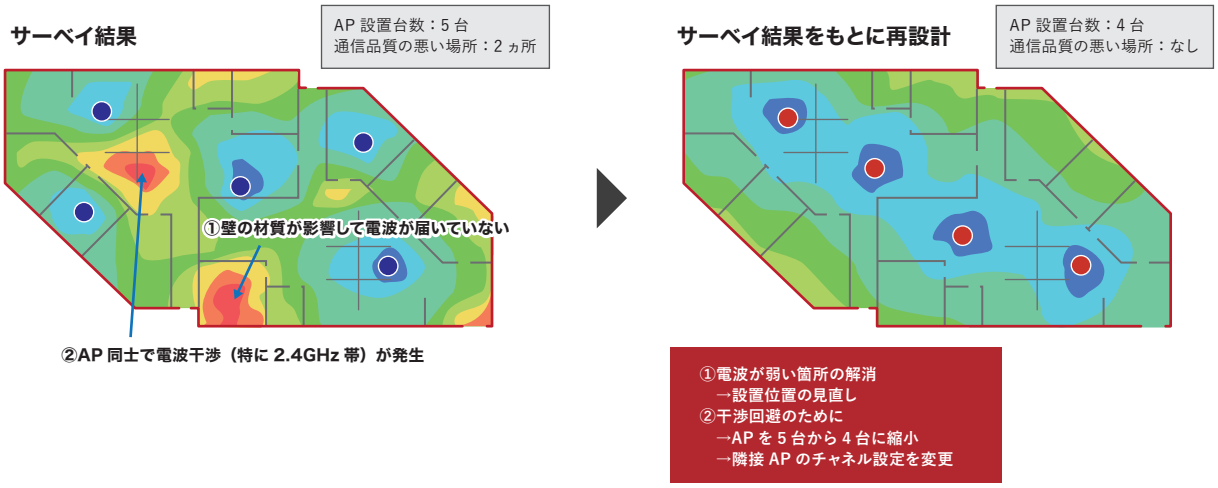
無線アクセスポイント（以下、無線 AP）は、一般家庭から企業向けまで、多数のメーカーから様々な種類のものが提供されています。一つ言えることは、安いからという理由で一般家庭向けのものを導入すると必ず失敗するということ。フリーアドレスオフィスでは、1 台の無線 AP に 30〜40 台の PC やスマホが同時に接続するというのはざらにあります。一般家庭向けの無線 AP は 5 台程度の接続を超えると急激に通信速度が低下し、業務用には不向きです。一方、企業向けの無線 AP はあらかじめ多台数接続を想定して開発されていますので、大勢で密に接続をしたとしても速度低下は緩やかです。ただ企業向けといっても、メーカーや機種によってかなりの差があります。そこで、「多台数接続時のスループット」を軸に無線 AP を選定するようにしましょう。




| POINT! | 多台数接続時のスループットをチェック |
|---|---|

# 2. 設計には細心の注意を払って

無線 LAN のよくある失敗例といえば、電波が届かない場所が生じるというケース。電波は、壁や人など様々な影響を受けやすく、シミュレーションのみで安易に導入してしまうと失敗に繋がります。かといって、これを回避しようと設置台数を増やすと、今度は無線 AP 同士が干渉を起こしスループットの低下を引き起こします。専門業者に事前のサイトサーベイ（現地調査）を依頼し、適切な台数と最適な設置個所を割り出す事をお勧めいたします。




サイトサーベイの実施と同様に設計時に気を付けて頂きたいのが、特定の無線 AP へアクセスが集中しすぎないようにすることです。
ドア付近など導線に近い無線 AP にはアクセスが集中します。前述の通り、多台数による密な接続はスループットの低下の原因となるので、最大接続数の設定や電波強度の調整をしなくてはいけません。
加えて、機器選定の時点でローミング機能（薄い電波を断ち切って最寄りの強い電波を捉える機能）を搭載したタイプの機種を選択することも重要です。

| POINT! | サイトサーベイは必ず実施すべき<br>ローミング機能などを活用し、アクセスの集中を回避させる |
|---|---|

# 2. 失敗しない無線LAN構築ポイント
## – セキュリティ編 -

## 1. 不正アクセスを防ぐ

不正アクセス対策を目的に実装される無線 LAN の認証方式には、ユーザーに対して行うものとデバイスに対して行うものがあります。ユーザー認証は一般的に広く使用されていますが、企業で無線 LAN を扱う場合これだけだと十分なセキュリティ対策とは言えません。例えば、従業員が私物のデバイスを持ち込み、社内ネットワークへ簡単にアクセス出来てしまいますし、万が一パスワードが流出してしまったら、もはや誰からのアクセスも許すことになってしまいます。フリーアドレスオフィスのみならず企業で無線 LAN 環境を構築する際には、ユーザー認証に加えてデバイス認証も行うべきだと言えます。

### ▼代表的な認証方法

| ユーザー認証 | | デバイス認証 | |
|---|---|---|---|
| パスワード認証 | Active Directory 連携(PEAP) | 証明書認証 (EAP-TLS) | MACアドレス フィルタリング |
| ユーザー名とパスワードを入力して行う認証 | サーバ側が証明書を発行し、クライアント側で ID とパスワードを入力して行う認証 | RADIUS サーバとクライアントの相互で「証明書」を持つコンピュータだけが接続できる認証 | 特定の MAC アドレスからしか接続できないようにする機能 |

続いて、お勧めのデバイス認証システム「クライアント証明書認証（EAP-TLS）」についてご紹介します。クライアント証明書認証とは、管理側が発行した証明書をインストールしたデバイスのみ無線 LAN にアクセスを許可する、という認証方式です。証明書認証であれば、パスワードの漏えいや辞書攻撃による被害がなくなり、数ある無線 LAN 認証の中で最上級のセキュリティレベルとも言われています。しかし、認証局を社内に構築してそれぞれのデバイスへ固有の証明書をインストールしなければならないため、運用側の負荷が難点ではあります。

**POINT!**

ユーザー認証＋デバイス認証がマスト
デバイス認証にはクライアント証明書認証（EAP-TLS）が◎

# ㊙裏技　パスワード認証で、擬似的「デバイスの認証」？

パスワード認証（WPA2 / 3 Personal）といえば、SSID とそれに紐づくパスワードで認証をする方式で、一般的に「ユーザー認証」のための仕組みと言えます。ですが、ちょっとした工夫で疑似的な「デバイスの認証」になります。パスワード認証はどのみちユーザー認証として採用され、低コストなので、裏技のような感覚でぜひご活用ください。

では、その方法についてご紹介していきます。

ポイントは、パスワードをユーザーに教えないということです。パスワードを従業員に教えず、情報システム部などの管理者がアクセスを許可するデバイスに直接パスワードを入力していくのです。ユーザーはパスワードを知らされないため、私物デバイスから無線 LAN に接続することができません。（ちなみに、パスワードの流出も防止できます。）また、そのパスワードの文字数を最大の 63 文字にしておけば、辞書攻撃で割り出せる確率を極めて低く抑えることも可能です。さらに、Active Directory があるような環境では、グループポリシーで無線 LAN プロファイルの一括適用を行うとスムーズに導入できます。

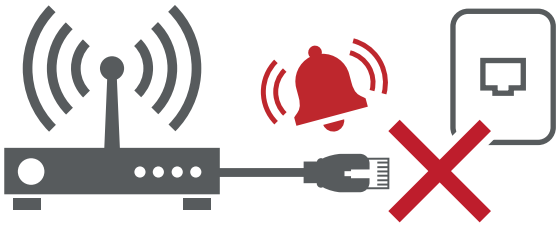
# 2. 不正アクセスポイントの設置を許さない

ここでもう一つ注意して頂きたいのが情報システム部門の管理下にない不正なアクセスポイント（通称、野良AP）を従業員ないしは悪意あるものに設置され、使われてしまうというケースです。いくら強固な認証方式を採用した無線 LAN を導入したとしても、認証システムが不十分もしくは全く施されていない不正な AP が存在しては、元も子もありません。ここでは不正 AP の設置を許さない、簡単にできる二つの対策方法についてご紹介します。

| POINT! | 管理下にないAPの設置を許さない |
|---|---|

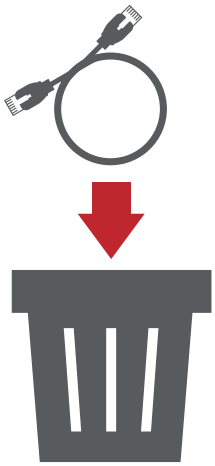
## 方法①：不正APを検知する無線APを導入する

一つ目は、不正 AP を検知する機能を搭載した無線 AP を導入することです。万が一社内ネットワークに不正な無線 AP が設置されたとしても、検知しアラートで知らせてくれます。



## 方法②：有線LANへの接続を制限する

二つ目は、原始的ではありますが、有線 LAN に接続できるデバイスを制限する方法です。許可されてないデバイスに有線 LAN が接続されたら自動でこれを切断するアプライアンスを導入したり、MAC アドレス認証を活用することで実現できます。もし、全社的にフリーアドレス化するということであればこれを機に完全に有線 LAN を排除するというのも一つの手です。



# 2. 失敗しない無線LAN構築ポイント
## – 運用編 -

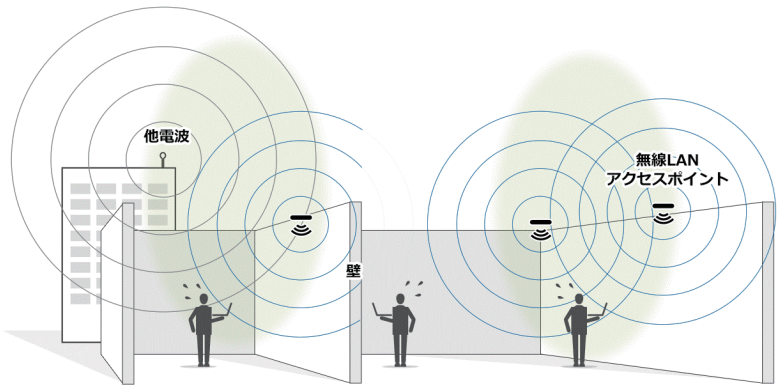
## 1. 安定稼働を維持するために

無線 LAN の電波は様々なモノの影響を受けやすいということは、導入・設計のポイントでもご紹介しました。ゆえにいくら完璧な設計で導入をしても、環境が変化してしまえば崩壊します。

### 度々発生する状況変化とそれに伴う障害例

| | | |
|---|---|---|
| CASE①: 上のフロアーの会社が変わる | ▶ | 電波が変化し、自社の無線 AP と干渉 |
| CASE②: 従業員が増え、デバイスの数が増えた<br>オフィスのレイアウトを変更した | ▶ | 各無線 AP の接続数に偏りが生じ<br>接続過多 AP が発生 |
| CASE③: DFS の作動 | ▶ | 気象レーダーなどの同じ周波数帯を使っている<br>電波を検知し、無線 AP が電波の出力をストップ |

このように無線 LAN 環境は様々な要因を受け、電波状況が変化します。どれほど電波干渉が発生しているのか、無線 AP ごとの接続デバイス数に変化がないか、また、DFS の作動がなかったか、日々状況を把握できる体制を整えなくてはいけません。しかし、これらの情報を得られたとしてもそれに見合う的確な対処を施すには豊富な知識が必要です。情報システム部の仕事は多岐に渡り、通常業務と兼任している場合も多いですから、これらの面倒な運用をすべて代行してもらえるフルマネージドの無線 LAN ソリューションを選ぶというのも一つの手です。

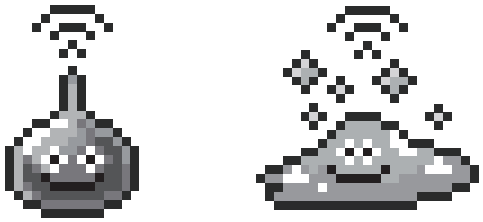


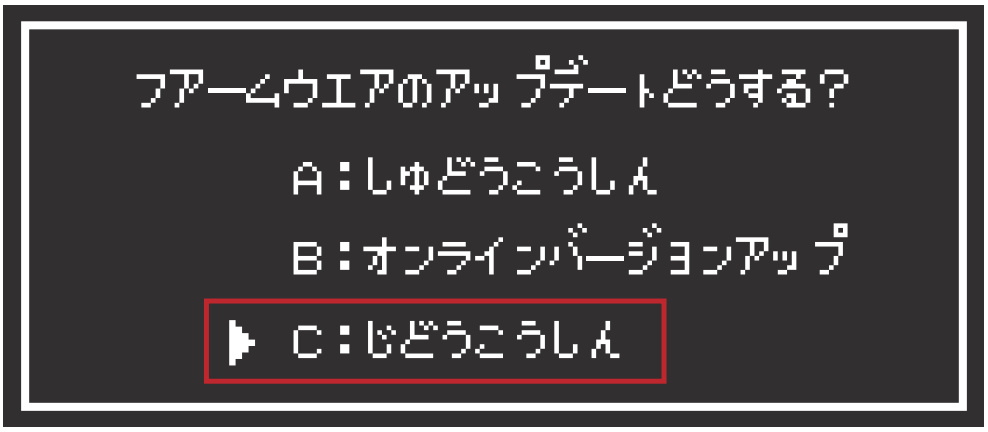

**POINT!**

安定稼働の維持には、日々の監視と適切なマネジメントが必要
運用代行付きサービスを選択するのが◎

# 2. 常に最新のファームウェアを

最後に安全・安定運用において、いかなる機器においても忘れてはならないのが定期的なファームウェアのアップデートです。ですが、情報システム部にとっては地味に大変な作業なのです。オンライン管理画面を使って遠隔で適用できる機種もありますが、どのみち情報システム部のタスクである限り更新漏れのリスクは払拭できません。クラウド型の無線 LAN サービスを選択すれば、リモートで定期的に更新作業を行える上に、一般的アウトソーシングのように出張作業費も抑えられるためお勧めです。

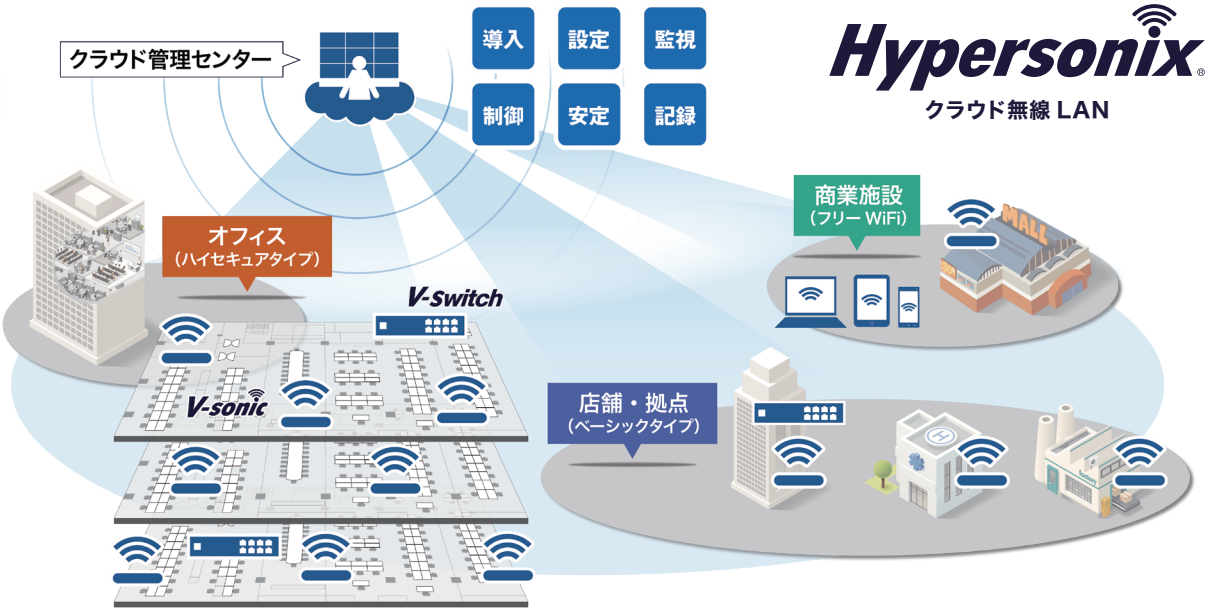




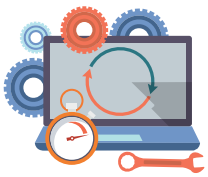

| POINT! | クラウド型の無線LANサービスなら、<br>出張作業費なしでファームウェアをリモートで自動更新してくれる |
|---|---|

# 3. クラウド型+フルマネージドのサービス

Hypersonix( ハイパーソニックス ) は、無線 LAN（Wi-Fi）の導入・運用を丸ごと委託できるサービス。クラウドから各種設定や運用・監視を行いますので、急なトラブルや設定変更でお客様のお手を煩わせることはありません。「無線 LAN 運用はプロに任せる」これこそが、心配しない為の最大のポイントです。




## 設計・構築をお任せ



- 初期設定 / 導入 / 構築
- デバイス毎の接続設定相談
- MAC アドレス登録、変更、削除
- 干渉波フィルタリング
- チャネルチューニング

## セキュリティをお任せ

- AD/RADIUS 認証などの適用
- ステルスモードの適用
- 各種セキュリティ設定代行

## 運用をお任せ

- 切断 / 遅延の回避
- ファームウェアのアップデート
- 無線アクセスポイントの死活監視
- 電話・メールでの障害切り分け
- ログの記録 / 保管
- 機器故障時の代替機器送付

※先出しセンドバック

**クラウド無線 LAN サービス Hypersonix は、ビジネスユースに最適。**
**フリーアドレスオフィスにも安心してお使いいただけます。**

# まとめ

フリーアドレスオフィスでは、無線LANの安定・安全稼働は大前提

**→無線LANが止まると全従業員の業務がストップしかねない**

設計・構築は専門家の知識を借りながら最新の注意を払って

- ☑ **業務利用に耐えられるスペックのAPを選ぶ**
- ☑ **設計・構築およびセキュリティ設定は綿密に**
- ☑ **安定稼働の維持には 、専門の知識と労力を有する**

工数のかかる無線LAN運用は、アウトソーシングしてしまう方が得策

- ☑ **障害復旧スピードや作業費、証明書発行やファームウェアの適用などを考慮すると、クラウド型サービスが◎**
- ☑ **運用代行から障害復旧まで、フルマネージドサービスが◎**

**詳しい製品概要資料はこちら ＞**

**開発元**

**AMIYA 株式会社 網屋**

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998

**https://www.amiya.co.jp/**

Hypersonixは株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、
著作権の侵害になります。

**販売元**

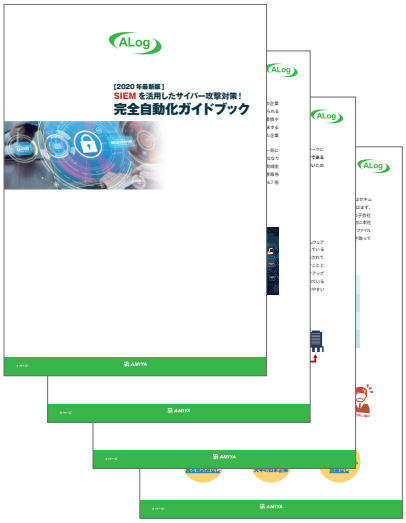
こちらもおすすめ

# テレワーク普及の裏で急増する サイバー攻撃に立ち向かうには

新型コロナウィルスによる強制的なテレワークの普及は、 企業に情報セキュリティ対策を施すための猶予を与えませんでした。その脆弱な体制を突いたサイバーセキュリティ事件が、最近急増しています。今年 3 月の標的型メールの件数は、なんと前月の 6.7 倍にもなりました。しかし報告されている事件は氷山の一角にすぎません。
標的型攻撃の最大の問題は「侵入に気づけないこと」です。

こちらのホワイトペーパーでは、「なぜ標的型攻撃に気づけないないのか」という基礎から、「自動検知するための具体的な仕組みづくり」まで。ログ管理の観点から、効率的なサイバーセキュリティ対策をご紹介しています。

## 見えないサイバー攻撃を自動で検知 SIEMによる脅威の見える化




### ★こんな方に おススメ!

① 標的型攻撃の手法・対策を知りたい
② セキュリティ運用の自動化メソッドを知りたい
③ サイバーセキュリティ対策にログを活用したい

**ホワイトペーパーのダウンロードはこちら ＞**