テレワークのメリットを活かせる

VAIOの万全セキュリティ SECURITY

必須セキュリティ項目もしっかりカバー

OSや他のハードウェアと独立して機能するセキュリティ専用チップ「TPM (Trusted Platform Module)」を搭載。従来はHDDやSSDに保存していた暗号キーを独立して管理できるようにすることで、ビジネスの現場に必要な強固なセキュリティを実現します*1。また、起動時（パワーオンパスワード）や、HDDへのアクセス時（ハードディスク・パスワード）などに動作するより強固なセキュリティ技術にも対応しています。

*1：TPMは、データやハードウエアの完全な保護を保証するものではありません。
*2 ハードディスク・パスワードはメモを取るなどして、必ず忘れないようご注意ください。

TPMを搭載したPCは、鍵がセキュリティチップ内に保持されるため、不正アクセスや取り外したハードディスクからデータを読み出せません

セキュリティとユーザビリティを両立 Windows Hello対応指紋センサー

センサーに指先を置くだけで瞬時にログインできる指紋認証機能は、スリープ状態からの復帰にも対応。面倒なパスワード入力を省略しつつ、安全性もしっかり確保できます。

* 出荷時設定ではオフ。「VAIOの設定」で設定可能です。

セキュリティロック・スロット

市販のセキュリティワイヤーと接続するための専用スロットを搭載。PCを盗難から守ります。

HDD/SSD遠隔データ消去

盗難・紛失の際に個人情報や機密データを遠隔から消去できる、情報漏えい対策ソリューションTRUST DELETE Biz for VAIO PC。消去実行はBIOS上で処理されるため、一般的な管理システムやプリブートの暗号化ソフトウェアと競合することがほとんどありません。ワンビ株式会社とVAIOの共同開発により、VAIOに搭載されている「PhoenixSecureWipe™」と連携し、OSを含むドライブ内の全データの消去が可能です。

* Phoenix SecureWipe™ はPhoenix Technologies Ltd. の商標です。

暗号化機能付SSD（OPAL2.0準拠）

専用ハードウェアを内蔵するため、BitLockerのようなソフトウェア暗号化に比べPC使用時のパフォーマンスが落ちません。また、製品出荷時から常に暗号化が有効なため、暗号化設定漏れや、ユーザーによる暗号化解除を防ぐことができます。

* 暗号化機能付SSD(OPAL2.0準拠）はBIOS Setupで提供するHDDパスワードもしくはOPAL2.0に対応する暗号化管理ソフトウェアと同時にご利用ください。
* 暗号化管理ソフトウェアは入っていないため、お客様自身でご準備頂く必要がございます。

LTE内蔵のVAIOなら、より確実に消去可能

盗難に気がついた時点で、サーバーからの命令を送信する必要がありますが、端末がオンラインでなければ実行できません。人口カバー率99%のLTEデバイスを搭載したVAIOであれば、起動しすぐにオンラインになるためより確実に命令が実行されます。また、SMSを利用した命令実行にも対応（2018年2月サービス開始予定）。SMS受信は、LTE接続が行われない状態でも確実に消去命令を実行できるため、PCの持ち出しがより安心して行えます。

インテル®Core™プロセッサー
Intel Inside® 飛躍的な生産性を

VAIO株式会社　法人営業部　**https://vaio.com/business/**

本　社　〒399-8282　長野県安曇野市豊科5432
東京オフィス　〒141-0031　東京都品川区西五反田2-11-17　HI五反田ビル

法人営業インサイドセールス
☎ 050-5578-8697
受付時間　月～金　9:00～17:30(12:00～13:00を除く)
※土日祝日、システムメンテナンス、当社指定定休日を除く

本冊子の記載内容は2018年1月現在のものです。　2018.01 VJ2018-B02

VAIOがお勧めするWindows 10 Pro.

2018.1

～テレワーク環境構築ガイド～

モバイルPC セキュリティ完全ガイドブック

COMPLETE GUIDEBOOK

SECURITY

- なぜ、企業のシステムには「セキュリティ」が必要なのか？
- テレワークを活用！そのときセキュリティで押さえるべきポイントとは？
- なぜ、パスワードの使い回しはいけないのか？
- PCを紛失したら、いったいなにが起きるのか？
- なぜ、セキュリティアップデートは重要なのか？
- なぜ、公衆無線LANから会社につないじゃダメなのか？

インテル®Core™プロセッサー
Intel Inside® 飛躍的な生産性を

～システムと人の対策～

そもそもなぜ、企業のシステムには「セキュリティ」が必要なのか？

**いま、多くの企業で柔軟なスタイルで仕事をこなす「働き方改革」が注目されています。
いつでもどこでも仕事ができ、利便性が高まる一方、そこには攻撃者が目を光らせるポイントも増えてしまうというリスクもあります。
まずはその現状を踏まえ、テレワークで考えておくべきシステム側の対策、そして人の対策をすべきポイントを押さえておきましょう。**

テレワークを望んでいたのは従業員だけじゃない？

いま「働き方改革」が注目されています。働き方改革では、自分が購入した私物のPC やスマートフォンを使って仕事をする「BYOD」(Bring Your Own Devices) や、自宅、外出先から企業のネットワークにつないで仕事を行う「テレワーク」が不可欠。これにより、自宅や外出先、出張先でも、事業を継続することが可能になります。昨今では「介護離職のリスク」や「育児への施策充実」も無視できません。いつでも、どこでも働けることは、企業の魅力につながり、多くの人が働きたい場所にするための、重要な施策といえるでしょう。

しかし、ここに問題があります。BYOD やテレワークなどによりビジネスパーソンの「利便性」が高まると、往々にして「セキュリティ」が下がってしまうことが多いのです。

テレワークを実践するということは、PC やスマートフォンなど、会社につながるデバイスを社外へ持ち出す必要があります。これまでであれば、オフィスのデスクにロックされ、大事に管理されていたデスクトップ PC も、いまではほとんどの企業でノート PC に置き換えられるようになりました。持ち歩くということは「落とす」ことも想定できます。もしその PC を「悪い人」が拾ってしまったとしたら、ネットワーク経由で堂々と会社のネットワークに侵入できてしまうかもしれません。

従業員にとって便利なことは、悪いことを考える人にとっても便利なのです。

狙われる理由は単純明快、そこに「お金」があるから！

ところで、**「悪い人」はなぜ狙いを企業に定めているのでしょうか。結論を先にいってしまうと単純明快「お金になるから」なのです。**例えば、マルウェアと呼ばれる不正プログラムは、大事に保管している顧客データや企業のマル秘情報をなんとかして盗み出し、ブラックマーケットで売りさばくことを目的としています。いまではクレジットカード情報は 1 枚につき 0.1 ～ 20 ドルで取引されているといわれています。個人情報や企業の情報はお金になるのです。

さらに、最近では PC のデータを勝手に暗号化し、取り戻したければ指定額のビットコインを支払えと脅迫する「ランサムウェア」の脅威も身近になっています。こちらは大事なプレゼン書類や見積書、営業資料を人質に、直接、あなたやあなたの企業から「お金」を奪うことを目的としています。

そのような現状において、悪い人は「テレワーク」はどう見るでしょうか。これまでであればインターネット上に「高い壁」があり、なかなか侵入をさせてくれない状況でした。ところが、テレワークが実践されるとその高い壁に「新しい入り口」ができても同然です。テレワークで用意された「会社のリモートアクセスの入り口」に対し、こっそり盗んだ従業員の「ID」「パスワード」を使って、堂々と正面から入ってくることすら可能になるかもしれません。

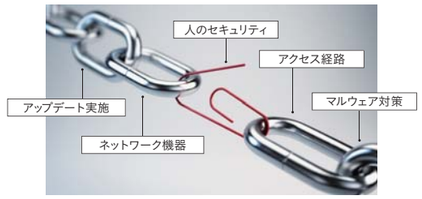
テレワークは便利ながら、実はさまざまなセキュリティ対策が “ 必須 ” なのです。

テレワークは「セキュリティの総合格闘技」

そのようなリスクを下げるためには、テレワークにおいて「多層防御」と呼ばれるような、複数の手段を用いて守るという考え方をする必要があります。以前であれば「セキュリティ対策はこの装置 1 つで安心、大丈夫！」という考えもあったかもしれません。しかし、残念ながらそのような安易な時代は過ぎ去ってしまいました。

特に、モバイル PC やスマートフォンなどの「デバイスを管理する」こと、外出先や自宅から企業内につなぐための「アクセスラインの安全性確保」、さらには接続しようとしている従業員の本人確認を行う「認証」をそれぞれ考える必要があります。デバイス管理にはノート PC やスマートフォンを紛失したときに適切な対策ができるか、ロックや暗号化は適切にできているかなど、さまざまな対策を多層的に施さねばなりません。

セキュリティとは「鎖」であるとよく例えられます。皆さんの企業にも、PC 暗号化や VPN、ファイアウォール、シングルサインオンなどさまざまなセキュリティ対策が施されていると思います。それらは鎖を構成する「丈夫な鉄の鎖」として運用されています。ところが、そこに「使い回されたパスワード」や「アップデートしていない PC」「どこにあるかわからないスマートフォン」など、しっかり対策ができていない部分があると、セキュリティの鎖を引っ張ったとき、その「弱い鎖」「壊れた鎖」の部分で切れてしまいます。



セキュリティは「鎖」に例えられる。鎖の一つひとつは頑丈だったとしても、1 つでも弱い部分があると、そこが弱点となりあっさり切れてしまいかねない。

テレワークは「セキュリティの総合格闘技」。あらゆるサイバー攻撃のリスクに備え、いかにして対処していくかが重要です。対策は 1 つだけではなく、あらゆる方法で検討しなければなりません。

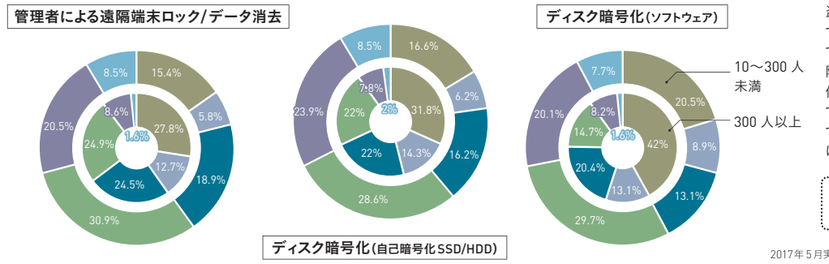
要検討！ 多層防御の必要性

ここで 1 つ、多層防御の例を紹介しましょう。これは盗難／紛失対策に対して、どんな対策を行っているかをアンケート集計した事例です。これを見ると、ソフトウェアによるディスク暗号化は半数近くの大企業が導入済みになっています。ディスク暗号化がされていたとしたら、PC を紛失しても大丈夫…と考えたくなるところですよね。

しかし、もう 1 つの「管理者による遠隔端末ロック／データ消去」を見ると、大企業ですら 3 割以下に落ちてしまいます。万が一 PC を落としたとき、ディスク暗号化をしているから大丈夫だと思っていたら、その従業員がログインパスワードを「使い回し」していたり、「メモとして PC に貼り付け」ていたとしたら、ディスク暗号化は解除されてしまいます。これでは、暗号化の意味がありませんね。そのため、**本来であれば「遠隔端末ロック／データ消去」もセットで実施しなければ、暗号化への投資が無意味なものになってしまいます。**

もちろん、そこには「人」という、システム上もっとも「弱い鎖」があることも考えなければなりません。強いパスワードをどう作るか、使い回しをどう防ぐか、PC をなくすということをなくすことができるのか――システムが取るべき「総合格闘技の種類」や、「人のセキュリティを高める方法」を、このガイドブックで学んでいきましょう。

Q. モバイル PC に対する情報漏洩対策を導入／検討していますか。

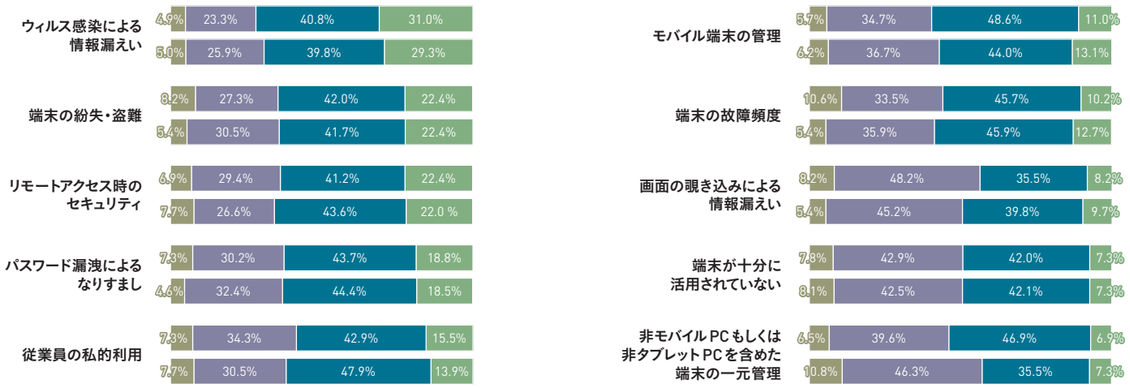


盗難／紛失ソリューションへの対策として、ディスク暗号化は 300 人以上の企業で 42%が導入済みだが、管理者による遠隔端末ロック／データ消去は 27.8%とやや低くなっている。ディスク暗号化が行われていたとしても、ID ／パスワードも合わせて盗まれていて、多要素認証を施していなければ情報が盗まれてしまうリスクが残る。

■導入済 ■導入予定 ■検討中
■興味あり ■興味なし ■知らない

2017年 5 月実施 サンプル数 (n=500) VAIO 株式会社の独自調査より

Q. モバイル PC ／タブレット PC を導入する場合の懸念事項はありますか。



モバイル PC 導入にはさまざまな懸念がある。
これに対し、バランスよく対策を打つことが重要だ。
2017年 5 月実施 サンプル数 (n=500) VAIO 株式会社の独自調査より

～テレワークに潜むリスク～

テレワークを活用！ でもその前に セキュリティで押さえるべきポイントを学ぶ

テレワークはセキュリティの総合格闘技。さまざまなリスクを想定し、適切なソリューションを選ぶ必要があります。とはいえ、いったいどんなリスクがあり、なにを行うべきか分かりにくいというのが実情。そこで、テレワークを実現するにあたり、どんなセキュリティ技術、ソリューションが使えるのかを考えてみましょう。

「企業のセキュリティ」は なにかを入れたら完了？

昨今のサイバー攻撃は、より巧妙に攻撃を仕掛けてきます。その対象は企業内にいる個人、そう、あなたも含まれているのです。個人としては「そんなの情報システム部がやってくれればいいよ」と丸投げしたいところですが、「悪い人」はその気持ちもうまく利用し、企業内に侵入を仕掛けてきます。

一昔前であれば、企業内の情報を守るためにネットワークを会社の外と会社の中に分け、その境界をきっちり守る方法を取れば安心できました。これはいわば、国境に高い壁をつくり、城門で検閲し、中に入れるかどうかをしっかり判断するというもの。

しかし、そのような考え方はいまのクラウド時代には合わなくなってしまいました。**テレワークを活用する現代においては、国境の高い壁の“外”でも、従業員を守れなくてはなりません。**

「境界のない世界」への対策

システムのあり方が変わり、守るべきポイントが増えました。そんな変化に合わせ、守り方も変えなければいけません。そこで、いま「守るべきポイント」を簡潔にご紹介しましょう。

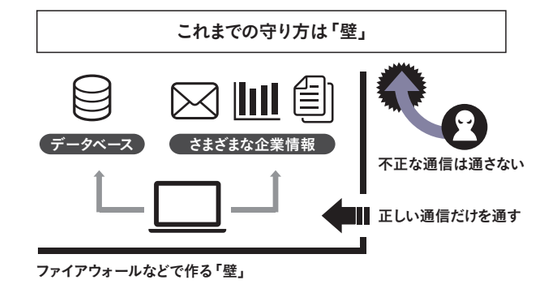
■マルウェアから企業を守る

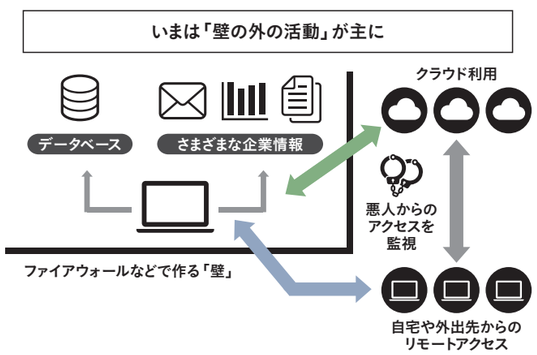
まずはコンピューターを襲う「マルウェア」対策を考えましょう。これはPCにインストールするのが当たり前になった、ウイルス対策ソフトと考えればいいでしょう。

ウイルス対策ソフトは、これまでに発見されたマルウェアの特徴を掴み、それと同一の特徴を持つプログラムを検知するといったものです。皆さんのPCも、パターンファイルと呼ばれる特徴をまとめたデータが日々アップデートされているはずです。これにより、既知のマルウェアはブロックすることが可能になりました。ところが、マルウェアは毎日20万件も増えているというデータがあります。日々これだけの数が増えていると、既知のものはブロックできても、新しく登場する日々20万件の「未知のマルウェア」はブロックできません。

そこで複数の防御策が必要になります。**未知のマルウェアに対しては仮想的なPCの中で挙動を確認する「サンドボックス」技術や、OSやアプリの弱点である「脆弱性そのものを守る」技術、さらにはマルウェア独自の「振る舞いを検知する」技術といった、新しい防御手法が登場しています。これらに加え、ネットワーク上で広まる「感染行為を止める」という方法も使えます。**

このように、「PCだけでマルウェアを検知する」という手法から、「PCで検知し、ネットワークや世界での検出情報を基にPCを守る」という手法へシフトが進んでいます。いまでは「感染されたとしても、情報を盗まれなければいい」という考え方もできるのです。これらは「エンドポイントセキュリティ」と呼ばれ、特に未知の攻撃が行われる「標的型攻撃」対策として注目されています。





これまでのセキュリティモデルは「高い壁の中を守る」ものでしたが、現在では壁の外での活動が中心になるため、考え方を変えなければいけません。

		盗難・紛失	悪意ある第三者による なりすまし	悪意ある第三者による 不正侵入	悪意ある第三者による 盗聴	人為ミス 社内不正	ウイルス 検疫・駆除	改ざん 書き換え	DDos 攻撃
		情報漏洩					サービス妨害		
人的 組織的	セキュリティ全般	情報セキュリティポリシー［リスク分析・セキュリティ基本方針・対策基準・実施手順］							
		対策ベンチマーク / 情報セキュリティマネジメントシステム［ISMS］導入 / 情報漏洩防止対策							
		セキュリティ診断 / 侵入テスト / 監査［内部・外部］/ 教育							
技術的	ネットワークセキュリティ		侵入検知システム［IDS］/ 侵入防止システム［IPS］		通信暗号化［IPSec/IP-VPN］		侵入検知システム［IDS］/ 侵入防止システム［IPS］		DoS/DDoS 対応［フィルタリング］
		ファイアウォール［パケット・フィルタリング］							
			デジタル署名	アクセス制御 / デバイス認証	WLAN［認証・暗号化］		アクセス制御 / デバイス認証		Fake AP
		検疫ネットワーク							
	クライアントセキュリティ 共通	セキュリティ・パッチ / フィッシング対応 / URL フィルタリング							
		個人認証		パーソナルファイヤーウォール	スパイウェア / アドウェア対応		ウイルス駆除	ファイル暗号化	Spam メール対応
		PC 認証			I/O 制御				
		ファイル暗号化							
		遠隔管理							
		シンクライアント							
	クライアントセキュリティ モバイル特有	ディスク暗号化	リモートアクセス						
	サーバセキュリティ	ユーザー認証			バックアップ		アクセス制御 / デバイス認証	ログ / 管理	Spam メール対応
		セキュリティ・パッチ［適用・逐次更新］					セキュリティ・パッチ［適用・逐次更新］		DoS/DDoS 対応（NDS、パケット制限）
		メール・MSG スキャン							
		Trusted OS / Secure OS			DBVS 暗号化		ウイルス駆除	改竄検知・防止	
環境物理的	環境	セキュア・ゾーニング、セキュア・オフィス・施設・設備・什器［入退出管理、監視カメラ、生体認証 / 盗聴・紛失防止備品］							

情報漏えいおよびサービス妨害のリスクに対する対策はさまざまなものが考えられます。特にモバイル利用においては、図表の黄色部分の対策が重要です。

■なりすましから企業を守る

特にテレワークにおいては「なりすまし対策」が重要になります。企業内ネットワークと接続するためには、企業の中からネットワーク越しに「あなた」を特定する必要があります。正しい権限を持つ従業員は接続を許可し、そうでない場合は接続させない仕組みを作ること。言葉にすると簡単ですが、ここにはさまざまなリスクが存在します。

通常のシステムであれば、あなたの「記憶」を利用し、その人だけが知っている情報、つまり「パスワード」を利用します。ところが、昨今はこのパスワードの流出事故が多発しており、悪い人が真っ先に狙う個人情報が、このパスワードなのです。

さらに多くの従業員は、個人で利用しているパスワードと、社内のパスワードを使い回している可能性があります。企業内のIDとは、おそらく名刺に書かれた「メールアドレス」ですよね。個人で利用していたパスワードがどこからか流出すると、会社のメールアドレス、流出したパスワードの組み合わせで、テレワークの入り口であるリモートアクセスルートから堂々と企業に侵入してくるリスクがあるのです。そのため、パスワードの管理や、使い回さないということが対策の1つといえるでしょう。

しかし、従業員に「気をつけよ！」と強いるだけでは足りません。例えば**なりすまし対策として、「社内のネットワークでは利便性を考えパスワードのみでログインできるが、リモートアクセスの場合は生体認証を含む多要素認証」を取り入れるなど、**パスワードの使い回しや、弱いパスワードを付けないように気をつけるだけでなく、多要素認証を要求したり、アクセスそのものをブロックするというIT的な仕組みを取り入れることも重要でしょう。

■ネットワーク侵入から守る

ネットワーク侵入のリスクとして、普及しつつある「無線LAN」からのアクセスにも対策が必要です。有線LANであれば物理的に目で見て侵入がわかるかもしれません。しかし無線LANですと、脅威を検出する仕組みを用意し「見える化」を積極的に進めなければなりません。例えば登録した端末だけが無線LANやリモートアクセスに接続可能にすることが考えられます。先のなりすまし対策と合わせ、端末での認証も組み合わせれば、多層的な防御が行えます。

さらに、リモートアクセスにおいては特定のLTEネットワークからのみ接続を許可することも可能です。特に誰もがつながっているインターネットには接続せず、**専用線のような閉じたネットワークに接続する「閉域網SIM」であれば、インターネットからの脅威リスクを極限まで下げられます。**閉域網SIMを差したPCを端末管理すればリモートアクセスがより安全になります。

「人」を守る、「人」が守る

もう1つ重要なこと、それは「人」です。例えば上記のようなポイントを押さえたとしても、どうしてもノートPCやスマートフォンの「紛失」「盗難」は発生してしまいます。多くの場合、金曜日の夜にちょっと息抜きしたとき、カバンとともに電車の網棚に置きっぱなしにして…ということから、インシデントはスタートします。もしあなたの会社が端末のHDD暗号化を実施しており、遠隔ロック／削除が可能だったとしても、従業員が報告しなければ、すべての仕組みが無駄になってしまいます。

この場合のインシデント対策のスタートは「従業員が正直になくしたことを報告できること」。そのために、なくしたときの連絡先をカードとして配布、財布の中に入れてもらうこと、さらには「なくしたとしても、会社が全力で被害を最小限にすること」を、従業員に伝えることが重要です。

人のセキュリティ意識を高めること、そして人をセキュリティ技術で守ること。この両立がもっとも重要なポイントなのです。

～パスワードを侮るな～

なぜ、パスワードの使い回しはいけないのか？ 最新最強「パスワード活用術」

ありとあらゆるサービスで要求される「パスワード」。サービスがあなたを判断する情報としてあなたの記憶の中だけにある文字列が要求されます。ところが、このパスワードは意外と簡単に漏えいしています。もしあなたが「1つだけのパスワード」を使い回しているとすると、あなたのパスワードを勝手に使った「なりすまし」ができてしまうかも。そこで、パスワードにまつわる「なぜ？」を紐解いていきましょう。

最初のセキュリティ対策、「パスワード」再考

サービスを利用開始するとき、必ず「パスワード」を設定することになります。これはサービスの利用者を特定するため、あなたしか知らない言葉をよりどころに、あなたがあなたであるという判断をするための仕組みです。パスワードはもっとも身近なセキュリティ対策であり、かつもっとも重要な対策ともいえるでしょう。

例えばあなたのメールアドレスに届くメールには、ビジネスだけでなく個人利用としても、他人に知られたくない情報がたくさんあるでしょう。SNS などのサービスも、ダイレクトメッセージを見られたり、不特定多数の友人に勝手にメッセージを送られることは大問題です。でも、そのような行為も「パスワード」が漏れてしまうと、メールやメッセージの覗き見ができてしまうのです。

パスワードは正しくあなたを判断するだけでなく、あなた以外の人間をあなたとして判断しないという、重要な役割を担っています。例えばテレワークにおいて、従業員とそうでない人を判断する方法の 1 つとしてパスワードが使われます。皆さんも情報システム部から「パスワードを強固にしましょう」「パスワードは使い回さないようにしましょう」などという呼び掛けをされているはずです。パスワードを大事にすることは、情報を守ること。パスワードに対してうるさくいわれることには、そのような背景があるのです。

ところであなたはいま、いくつの「パスワード」を持っていますか？　キャッシュカードで使う 4 桁の暗証番号、メールアカウントのパスワード、SNS のパスワード、そしてスマホのロック解除のためのパスワード…。サービスの数だけアカウントが増えていきます。トレンドマイクロ社の「パスワードの利用実態調査 2017」によると、**パスワードを使い回しているという利用者は全体の 8 割以上。実はほとんどの人が、最大でも 4 ～ 5 種類のパスワードを「使い回し」してしまっているのが現状**です。

実はここに、大きな落とし穴があります。もしテレワークにおいて ID を「会社のメールアドレス」にしていた場合、この ID は名刺に書かれている情報ですので、すぐにわかるものといえます。もしその人が「パスワードの使い回し」を行っていて、個人で利用している Web サービスが情報漏えいを引き起こし、パスワードが漏れてしまうと――そう、名刺に書かれた公開情報であるメールアドレス、本名、そして漏れたパスワードがわかれば、もしかしたらあなたになりすまして、悪い人が「テレワーク」という名の情報詐取を行ってしまうかもしれません。

できる限り、パスワードの使い回しをしないこと。特に企業のパスワードは個人と別にすることが望ましいです。もちろん、「abcde」や「qawsedrf」のような、弱いパスワードなんて論外です。

強くて覚えやすいパスワードのつくり方

「パスワードは使い回すな！」「弱いパスワードは使うな」とはいうものの、私たちは強いパスワードのつくり方を誰からも教わっていませんし、使い回さない方法も知りません。記憶に頼れ、頑張れといわれても、数十、数百のサービスを利用する私たちにとって、それは現実的ではありません。

そこでここではパスワードのつくり方のテクニックをお教えしましょう！　図で示した法則であなた流を考えてみてください。

どうですか？　これなら覚えられそうだ！と思ったのではないでしょうか。利用するサービスの名前を追加することで、サービスごとにパスワードが微妙に変わります。覚えるのは駅名と記号、大文字にした位置だけ。もちろん、皆さんのアレンジで「好きな都市の名前」「好きな食べものの名前」などに変えてみてくださいね。

これなら、使い回しもせず、弱くもないパスワードが、ルールに従い簡単に覚えられるのではないかと思います。ぜひ、実践してみてください。

さらにITを活用した対策 なりすましを防ぐ「生体認証」

実はこのパスワードを強固にするという手法は、あなたがあなたであることを認証する方法の 1 つでしかありません。現在ではその認証の手法として、**あなたの記憶に頼ることなく、なりすましを防ぐ方法があります。その 1 つが「生体認証」です。**

生体認証とは、例えば「指紋」や「顔」など、その人を特徴づけ、他人とは違う部分を認識して、本人を確認するというもの。最近ではスマートフォンにも生体認証が搭載されてきましたが、PC にも指紋認証デバイスが搭載され、より強固な認証が行えるようになっています。

指紋認証などの生体認証は、パスワードを入力することなく、一瞬で認証が行えることが特徴です。指紋は犯罪捜査でも使われるように、同じ紋様を持つ人がいないという特徴があります。なりすましを防ぐには、とても便利ですよね。それだけではなく、生体認証はキー入力を監視する「キーロガー」がパスワードの入力内容を盗み出すというリスクや、もっと単純にパスワード入力を肩越しに盗み見る「ショルダーハック」のリスクにも強いといえます。

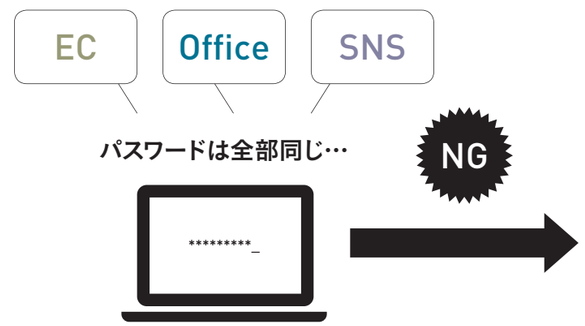
しかし、もしかしたら「指紋が盗まれたら怖い」と思うかもしれません。指紋は取り換えることができませんので、万が一指紋を盗まれたらすべての対策が水の泡になってしまいます。でもご安心を。指紋認証はあなたの指紋そのものを記録することはなく、その特徴点だけを保存しています。そのため、保存された指紋情報から、指紋を復元することはできません。

さらに、指紋情報とハードウェア的に分離されたセキュリティチップが紐づけられているため、保存された指紋情報が悪用されることはありません。生体認証のリスクとメリットを知れば、パスワードをはるかに超える安全策であることがわかるのではないでしょうか。

このほか、Windows 10 の新機能である「 Windows Hello 」や、生体認証やワンタイムパスワードなどを複数の手法を使う「多要素認証」など、現在ではさまざまな機能が実用化されています。**ビジネス、特にテレワークにおいては、利用者の記憶だけに頼るのではなく、さまざまな仕組みを活用し、「パスワードが漏れてもなりすましを防げる」ようにしておくことが重要です。**その上で、強くて使いまわしのないパスワードを使うこと。これが、最新の「パスワード活用術」なのです。

“VAIO流”、強くて使い回さない「パスワード」作成の法則

例 オリジナルルールで作成



fac&5tandA
③ ② ①

①真っ先に思いついた「駅名」をローマ字にしてみましょう。
例えば「gotanda」
次にそのローマ字のなかで「数字」にできそうなものは数字に変えてみます「5tanda」
わかりやすい位置のアルファベットを、大文字に変えてみましょう。
今回は最後の文字を大文字にしましたが、どの場所でもかまいません。
「5tandA」
②何か1つ、パッと思い浮かんだ「記号」を作りましょう。
それを先頭に付けます。これがあなたのパスワードの重要な「カケラ」です！
「&5tandA」
③このパスワードを登録するサービスの「先頭3文字」を、
このパスワードのカケラの頭に付けましょう。例えばTwitterなら「twi」、
Facebookなら「fac」という具合です。
「twi&5tandA」「fac&5tandA」「ins&5tandA」

生体ログオン認証ソリューション比較

ビジネスの情報を守るには、パスワードという記憶に頼る認証方法だけでは足りない時代になりました。「生体認証」を導入することで、複数の認証方法を組み合わせてさらに安全性を高めることができるのです。

	特徴	セキュリティ向上	導入の容易さ	利便性	生体情報管理	多要素認証	コスト
Windows Hello	Window10 の生体認証機能、Windows Hello 対応 PC と組み合わせることで、パスワード入力の代用として、生体認証を利用	😀 パスワードの常時入力を避けることで、その盗難を抑止	😀😀 クライアント対応のみ	😀😀 瞬時にログイン	😀😀 TPM 紐付けで安全に管理	ー	¥
Windows Hello for Business	Windows10 および Windows Server 2016 により実現される、パスワードを用いない FIDO2.0 に対応した新世代の認証システム	😀😀 認証にパスワード自体を使用せず、生体認証と個体認証の組み合わせによる強固な認証を実現	😀 認証サーバーとクライアントの対応必要	😀😀 瞬時にログイン	😀😀 TPM 紐付けで安全に管理	😀 複数の認証要素の組み合わせ利用に対応	¥¥
3rd party 認証基盤	実績豊富なソリューションが複数存在。製品によって使用できるセンサーデバイスが異なる。PC 内蔵のセンサーが使えるかがチェックポイント。	😀😀 ソリューションによるが、精度の高い認証を提供するものなどあり	😀 認証サーバーとクライアントの対応必要	😀😀 瞬時にログイン	😀😀 ソリューションによる	😀😀 ソリューションによるが、多様な認証方式との柔軟な併用可能	¥¥¥

～PC紛失の顛末～

PCを紛失したら、いったいなにが起きるの？「金曜の終電でPC紛失リスク」を最大限回避

働き方改革が国を挙げて推し進められる一方で、持ち運びができるデバイスの紛失・盗難や、会社の外からのリモートアクセスのリスクが課題となり、多くの企業がテレワークやBYODに二の足を踏んでいるのではないでしょうか。そこで今回は「PCを紛失したときのリスク」を把握し、そのリスクの低減する方法を考え、正しく安全な“働き方改革”を実現する方法を考えてみましょう。

それはいつも、金曜の夜に…

金曜日の夜、1週間の疲れを癒すために仕事終わりにみんなで楽しく飲み会へ。気持ちよく帰宅しようとすると、改札口でハッと気がつきます。「あれ？ カバンがない！」これ、人ごとではないですよね。

いま、オフィスで利用されるPCはほとんどがノート型です。会議にもさっと持ち運べるくらい軽くて便利。出張や出先でもプレゼン資料を仕上げたり、営業資料を確認したりすることができるようになりました。スマートフォンも同様です。いつでもどこでも仕事ができるという意味では、もうすでに働き方改革ができたも同然かもしれません。

しかし、持ち運べるデバイスには「紛失」のリスクが伴います。カフェで、ちょっとトイレに行った隙に盗まれるということもあり得るでしょう。もしそれが単なる物盗りではなく、お勤めの企業を狙う犯行だったとしたら――。企業としては常に最悪のケースを考えていく必要があります。そして、そのリスクに対応できる、セキュリティソリューションを用意することも。

いつでもどこでもを担保しつつ、きちんとした働き方改革を推めるためには、**「従業員が気をつける」という対策だけではなく、「なくしても情報漏えいインシデントにならない」対策が必要なのです。**

PCやスマートフォンを紛失した／盗難にあったときにもっとも避けたいことは「デバイスの中にある情報を盗まれる」ことです。ある意味、PCなどは買い換えが効きます。しかし情報は一度漏えいすると取り戻すことは不可能です。したがって、真っ先に「情報漏えい対策」が必要です。

その方法の1つが「PC内の暗号化」。PC内にあるデータがすべて暗号化されていれば、デバイスを盗んだ悪い人がいくら頑張っても、その暗号化が解けなければ情報漏えいにはならないはずです。この暗号化のための手法はいくつかあり、例えばWindowsの機能である「BitLocker」を利用する方法や、サードパーティーによる暗号化ツール、そしてSSD／ハードディスク自体に組み込まれた暗号化機能を活用することなどが考えられます。

これらの手法はメリット／デメリットがあるので、企業がセキュリティに対してどこまでリスク低減を行うか、従業員が持ち歩くデバイスにどんな情報が含まれるのかを考えつつ、適切な暗号化手法を選択することをお勧めしたいと思います。

暗号化だけでは足りない！？

しかし、それだけでは対策は不十分。いくら暗号化をしていたとしても、従業員ならば認証を通して復号が可能です。もしPCと一緒に、その認証情報、例えば「パスワード」が漏れていたとしたら、暗号化を突破できてしまいます。PCが紛失／盗難されたらすぐに遠隔で消去できる仕組みも合わせて対策することをお勧めしたいと思います。

これは紛失／盗難にあったPCが次にネットワークに接続したタイミングで、PC内のデータを消去できるというもの。特にPCがLTE対応している場合、SMSを使って消去が行えるため、より迅速な対処が可能です。この点では、PC単体でLTEネットワークに接続できる機能が大きなメリットになるでしょう。

そのほか、そもそもデバイスに情報を残さない「シンクライアント」の活用も考えられるでしょう。ただし、完全なシンクライアント端末は選択肢も少なく、利便性を損なうことも多いため、現在ではWindowsデバイスを利用した「ハイブリッドクライアント」を選択する企業が増えています。フルスペックのWindowsであれば、必要なアプリケーション／データのみを仮想化して活用するという方法も取れますし、従業員にとっても慣れた端末を使えますからね。

それでも重要なあなたの役割とは？

このように、いまではPCの紛失／盗難もさまざまなソリューションの組み合わせで、盗まれても情報漏えいインシデントにしないことも可能になりました。多くの情報漏えいの原因は、サイバー攻撃による被害よりも「人的ミス」が多いのです。デバイスを落としたりなくしたりした従業員だけを責めるのではなく、人的ミスがある前提で組織全体での紛失／盗難対策が重要です。

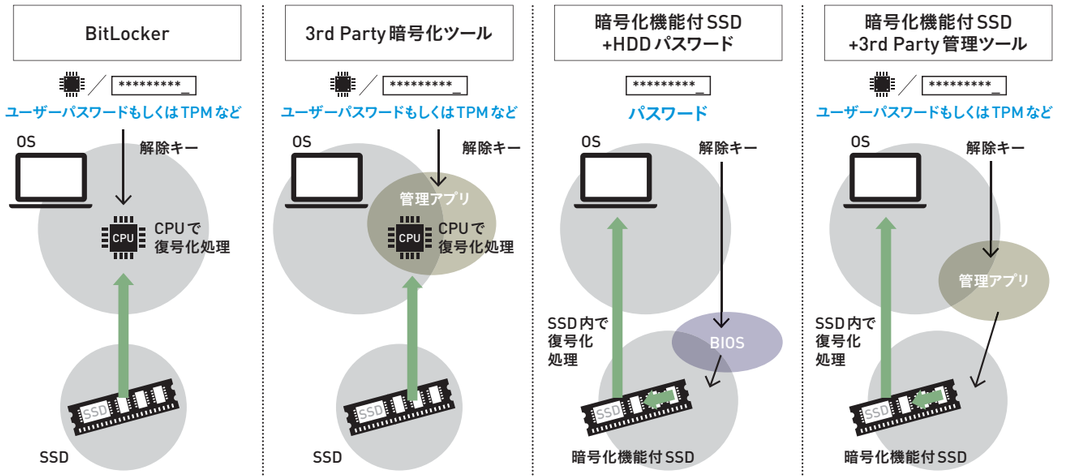
しかし、これらの対策を行っても、落とした人、なくした人が「速やかに報告」しなければ、被害はどんどん大きくなってしまう可能性があります。そのため、次は「人」への対策として、企業が従業員に**「24時間ヘルプサポート付のリモートワイプサービスを導入するなど、我々は紛失対策をしっかりやっている。しかしそれは、あなたが落としたことを正直に報告してはじめて有効になる」**ということを伝える必要があるのです。落としたことを責めるのはもう終わりにして、「落としてもITの仕組みで情報漏えいが防げるから、安心して報告を」と協力を依頼するようにしましょう。

冒頭、紛失は金曜日の夜に起きがちだと述べました。これはつまり、報告が遅れると初動が月曜の朝以降になってしまうということです。企業が48時間以上リスクを放置できなければ、まず社員に対し、紛失／盗難時にどこに連絡すべきかを必ず伝えましょう。これはメールや掲示板ではなく、物理的なカードなどに印刷し、財布などの中に入れてもらうのが適切です。なくしたときの連絡先がPCの中にしかなければ、報告しようがありませんからね。そして報告を受けた情報システム部が、該当のデバイスを判定し、IDのロックやリモートアクセスの通信遮断、そして遠隔消去の作業を滞りなく行えることが必要になります。素早い報告を無駄にせず、少ない手順でリスクを回避すれば、紛失対応も怖くはありません。

紛失対策、盗難対策はITソリューションだけではなく、人の教育も重要です。企業は落とした人を犯人扱いするのではなく、早く業務に戻ってもらうことに専念しましょう。そして従業員は万が一のために企業がバックアップしてくれていることを理解し、それが無駄にならないよう、正しく行動するようにしましょう。

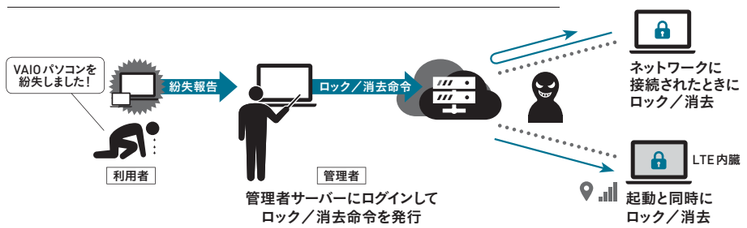
ストレージ暗号化ソリューション比較

PCのSSD／ハードディスクの暗号化にもさまざまな手法があります。信頼性だけでなく、PC管理運用やパフォーマンスへの影響を考慮して選択したいところです。



	BitLocker	3rd Party　暗号化ツール	暗号化機能付きSSD＋HDDパスワード	暗号化機能付きSSD＋3rd Party管理ツール
メリット	・OS標準機能で簡単に利用が可能	・利用者の状態を細かく管理できる ・複数OSの一元管理ができる	・利用開始時にディスク全体の暗号化処理の時間を取られない ・ハードウェアでの暗号化のためパフォーマンスが良い	・利用者の状態を細かく管理できる ・複数OSの一元管理ができる ・パフォーマンスも良い ・利用開始時の暗号化処理もいらない
デメリット	・利用者が解除してしまうなど管理がしにくい ・ソフトウェアで暗号化するためパフォーマンスに影響がある	・ソフトウェアで暗号化するためパフォーマンスに影響がある	・パスワードの集中管理や、パスワード忘れたときの対応がとりにくい	・管理のためのアプリ導入など、コストをかける必要がある
コスト	―	￥￥	￥	￥￥￥

リモート消去ソリューション



ソリューションによっては、消去のみならず、端末のロック、位置情報把握も可能です。また、SMSに対応してLTE内蔵PCをより確実に消去できるものもあります。もし自社で受付体制を取れない場合は、遠隔ロック／消去命令の代行を24時間365日で受け付けるサービスがあるかをチェックしましょう。管理者の負担を軽減できるだけでなく、事故時のオペレーションも円滑に行えます。

～脆弱性が突かれる～

なぜ、アップデートは重要なのか？面倒くさくても「絶対に行うべき」理由

帰宅時や外出前など、急いでいるときに急に始まる「Windows Update」。面倒くさいと思っている人も多いかもしれません。でも実は、これこそが企業と個人を守る最大の防御策なのです。今回は、悪い人たちがどのようにあなたの情報を狙ってくるのかを知り、時間がかかるだけで面倒だと思っていたアップデートの重要性を学びたいと思います。

アップデートは「新機能のため」だけじゃない

皆さんはWindows Updateを行っていますか？　突然始まって、終わるまでは電源をオフにできず、ひたすら終了するのを待つ…。たいていそれは急いでいるときに始まって、なんとかしてキャンセルする方法を探すという方もいるのではないでしょうか。

似たようなものではOSのアップグレードがあります。パワーユーザーほど「新しいWindowsじゃなくても、いまので十分」という評価をしがちです。それに、アップデート作業にはトラブルがつきものです。トラブル回避のため、いまもWindows 7やOffice 2013を使っている企業はあります。それにアップデートを行うと、必要じゃない新機能が勝手に付いてきたり、便利だと思っていた機能がなくなっていたり。皆さんも経験があるのではないでしょうか。

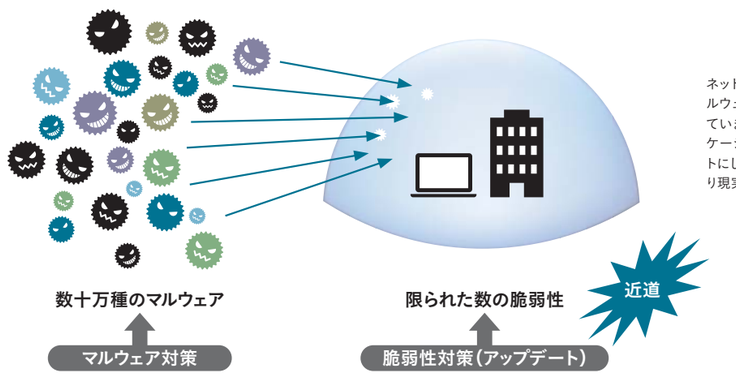
そのような状況ですので、「アップデートはできればしたくない」という気持ちもわからなくはありません。しかし現在においては「最新のアップデートを適宜適用し、できる限り最新のOS、アプリを使う」ことが、サイバー空間で安全を得るためにもっとも近道なのです。

アップデートで安全になる!?

最近のOSやアプリケーションにおいては、**アップデートは新機能追加だけでなく「脆弱性の修正」も重要なポイントになっています。**脆弱性とは、OSやアプリケーションにおける「一撃必殺の弱点」のようなもの。この弱点を突かれてしまうと、PCやシステムを乗っ取られ、こっそりと不正な動作をさせられたり、情報を盗まれたりしてしまいます。ギリシャ神話に登場する不死身のアキレスも、「アキレス腱」という弱点がありました。これこそが脆弱性です。

多くのマルウェアは、この脆弱性を利用してあなたのPCに侵入を仕掛けてきます。現在、ネット上では1日に20万件以上のマルウェア亜種が作成されています。マルウェアを相手にしようとすると、相手は膨大な数になってしまいます。ところが、そのマルウェアを解析してみると、ごく限られた数の「脆弱性」が対象になっている場合があります。**毎日20万件増えるマルウェアそのものに対策を打つより、マルウェアが狙う「脆弱性」を対策したほうが、より現実的**といえるでしょう。

サイバー空間で安全を得るためには



ネット上では1日に20万件以上のマルウェア亜種が出現しているといわれていますが、その多くはOSやアプリケーションにおける脆弱性をターゲットにしているため、ここを防ぐことがより現実的な対策手段になります。

脆弱性対策でチェックしておきたい情報源

	URL	
情報処理推進機構（IPA）	https://www.ipa.go.jp/	企業がウォッチすべき重要なセキュリティ情報を収集できる。各種レポートや白書が充実している
JVN iPedia	http://jvndb.jvn.jp/	情報処理推進機構（IPA）が運営する脆弱性対策情報データベース
警視庁サイバーセキュリティ対策本部（Twitter）	@MPD_cybersec	サイバー空間での犯罪の状況を伝え、適切に注意喚起を行っている
内閣サイバーセキュリティセンター（NISC）（Twitter）	@nisc_forecast	主要なプログラムのアップデート情報や、フィッシングメールなどの注意喚起を行っている
マイクロソフトセキュリティチーム（Twitter）	@JSECTEAM	Windowsなどのセキュリティ情報を定期的に公開している
情報セキュリティのラック（Twitter）	@lac_security	各企業が調査した情報やセキュリティブログの更新情報が確認できる
トレンドマイクロ（Twitter）	@trendmicro_jp	
マカフィー（Twitter）	@McAfee_JP	
カスペルスキー（Twitter）	@kaspersky_japan	
シマンテック（Twitter）	@Symantec_Japan	

Webサイトや Twitter でウォッチしておきたい情報源。できれば常に目に入るよう、各種アカウントをフォローし、セキュリティを身近に意識しておきましょう。

特に気をつけたいテレワーク端末のアップデート

実はこのアップデート、特に「テレワーク」においては重要なポイントです。これまでは企業内のPC端末が接続されるため、適切なアップデートをできているかを管理するのはある程度簡単に行えました。しかし、テレワークではさまざまな場所から接続されるだけでなく、BYOD（Bring Your Own Devices）として、私物のPCやスマートフォンも企業内ネットワークにつながる可能性があります。そのとき、アップデートが正しく行われていない端末が侵入してくると、マルウェアがそこから入り込み、結果、社内全体で感染行動を起こす場合があります。

さらに問題なのは、テレワーク端末が「踏み台」にされてしまう場合です。テレワーク端末が社内に接続する前に、別のネットワークでマルウェアに感染していた場合、企業内ネットワークにリモートアクセスで接続したタイミングでマルウェアが活動を開始し、偵察行動を行うかもしれません。テレワーク端末を介し、企業内の重要なデータベースに接続、情報を盗み出される可能性もあります。

そのため、テレワーク端末に対しては企業内のPC以上に、**アップデート管理が重要になります。これはWSUSのようなOSのアップデート状況の確認だけでなく、特にWebブラウザとそのプラグイン、Adobe Acrobat ／ PDF Viewer、Java、MS Officeなどが正しくアップデートされているかを確認できる仕組みが必要です。MDM（Mobile Device Management）ツールの導入を検討するのも1つの手です。**いま話題の「ランサムウェア」もマルウェアの一種。マルウェア対策を行うとともに、バックアップの仕組みも用意しておけば安心です。

企業におけるWindowsならばWindows Updateを選べる時代に

とはいえ、企業におけるOSアップデートは慎重に行いたいもの。Windows 10においては、企業がアップデートの頻度、内容をあらかじめ選択できるサービシングモデルがいくつか用意されています。

例えばWindows 10 Enterpriseでは、半期に一度の大型アップデートについては、4カ月の間を空けてプログラムが提供される「Semi-Annual Channel」（旧：Current Branch for Business（CBB））や、基幹システムなどに用いられる特別な「Long Term Service Channel」（旧：Long Term Service Branch）が用意されています。これらの選択を合わせて行うことで、より柔軟で、安全なアップデートポリシーがつくれるでしょう。

目指すのは、なんらかの脆弱性が発表されたときに、その脆弱性を内包するPCがどこにあり、誰が使っているかがわかること。そしてその脆弱性を修正するため、適切にアップデートが行える、回避策が取れる状況を作っておくことです。逆にいえば、アップデートを適切に行い、脆弱性管理が行えていれば、昨今のサイバー攻撃のほとんどは防げるのです。

～より安全なリモートアクセス～

なぜ、公衆無線LANの接続は危険なのか？最新「リモートアクセス」事情

客先訪問の前の空き時間。カフェでちょっとお仕事というスタイルも当たり前になりました。無料で提供されている公衆無線LANにつないでお仕事したいところですが、おそらく「それは禁止だ！」とされているのではないでしょうか。そこで今回は、カフェでの公衆無線LANを使うのはなぜいけないのか、ということから、会社への正しい「つなぎ方」を考えてみましょう。

カフェや空港の「公衆無線LAN」、便利の裏にある「危険性」って？

最近では多くのカフェや休憩施設、駅構内などに、無料で使える「公衆無線LANサービス」が普及してきました。特に海外からの旅行者には人気で、契約なしに使える通信手段として便利に使われています。しかし、日本のビジネスパーソンにとっては、これらの公衆無線LANサービスは「使うべきではない」とされています。これは、暗号化が行われていないということが理由の1つだということはご存じかもしれません。各企業のセキュリティポリシーにもよりますが、公衆無線LANサービスの一部は暗号化がされておらず、盗聴の可能性があることを考えると、やはり「使わない」にこしたことはありません。

では、実際にどのように「盗聴」ができてしまうのでしょうか。暗号化されていない（SSIDに錠のマークがない）無線LANであれば、その無線ネットワーク内で飛び交う通信は簡単に傍受できます。そこに例えば、SNSやメールサーバーのパスワードが入っていれば、IDとパスワードを盗み出し、なりすましが可能になってしまいます。多くの人は、公衆無線LANにつなげて真っ先にSNSやメールを見ることと考えると、悪い人はそれを待ち構え、わなを仕掛けているかもしれません。もしパスワードが使い回しされていたとしたら、盗んだSNSパスワードを元に、銀行口座にあるお金を盗むこともできてしまうのです。

暗号化された無線LANだったとしても、その暗号化が「弱い」場合もあります。例えばWEPと呼ばれる暗号化アルゴリズムには脆弱性があることが明らかになっているため、少々技術を知る悪い人にとっては、もはや暗号化を行っていないも同然です。また、店舗に固定のパスワードが掲示されていて、それを元に無線LANを利用できる場合も、実はその“共通パスワード”を使うことで暗号化が解除できてしまうので、同じ店舗で無線LANにつながっていれば、盗聴が容易にできてしまいます。

意外なことに、無線LANの暗号化は簡単な条件を満たすだけで盗聴ができてしまう危険性があるのです。これでは、安心して使えない…？　いや、方法はあります。

無線LANの救世主？HTTPSが使えればまずは安心

実は個人利用レベルであれば、公衆無線LANサービスの危険性はグッと下がります。例えばメールやSNSの利用においては、最近ではほとんどのWebサービスが「HTTPS」と呼ばれる、暗号化された通信が利用されています。無線LANは暗号化されていなくても、Webサービスが個別に暗号化されているため、以前よりはリスクが低いといっていいでしょう。ただし、電子メールで古くから使われているPOPなどを使っている場合、パスワードが平文で送られるため、簡単に盗まれてしまう可能性があります。

また、携帯電話事業者が提供する無線LANもほぼ安心といっていいでしょう。先に店舗に提示された「固定パスワード」を使う無線LANは危険であると述べましたが、スマートフォンから携帯電話事業者が用意している無線LANに接続する場合は、そのパスワードが利用者ごとに（スマートフォンのSIMごとに）異なるものが用意されています。これであれば、同じ無線LANにつないだ人が盗聴したとしても、暗合化された通信の中身を見ることはできません。

そのため、個人利用においては、公衆無線LANを「HTTPSでつながっているか」という点などに気をつけながら安全に利用することができるといえます。これはビジネスにおいても同様ですが、**「もっと安全な方法がある」ので、やはり公衆無線LANサービスの利用はお勧めしません。**

公衆無線LANよりも便利で安全LTEネットワークで「冴えたやり方」

ビジネスにおいては、これまで企業内ネットワークにつなぐための手法として仮想的な専用線をつくり出す「VPN」という方法がありました。これを使うことで、万が一暗号化されていない公衆無線LANを経由したとしても、PCと企業ネットワークとの間を個別に暗号化すれば盗聴から情報を防ぐことができました。

しかし、いまではもっと簡単で確実な方法があります。**それはスマートフォン同様、「LTEネットワーク」を利用すること。しかも、そのLTEネットワークで企業のモバイル専用線として使える「閉域網SIM」を利用することです。**

閉域網SIMとは、簡単にいうと「インターネットを経由せず、携帯電話事業者のネットワークから直接企業ネットワークにつなぐ」もの。インターネットを経由しないので、インターネットからの盗聴はもちろん、マルウェアに感染させるための通信からも守ることが可能です。

この方法のメリットはそれだけではありません。テレワークで重要な利用者の認証問題もクリアすることが可能です。**閉域網SIMを持つPC／無線LANルーターを物理的に管理し、それを持つ人を制限することで、「従業員だけしか知り得ない」パスワード、「従業員しか持ち得ない」デバイスの2つの要素で、認証を行うことができるのです。**リモートアクセスのリスクを下げると同時に、メリットを増幅させる方法といえるでしょう。

このメリットを最大限に活かすためには、PC自体がLTE回線に直接つなげられることが望ましいです。最近ではSIMスロットを持ち、LTEで高速通信が可能な製品も増えてきました。これがあれば、公衆無線LANサービスを利用することなく、安全で高速なリモートアクセスが可能になります。

ただし、この仕組みはLTE回線でつなぐことが大前提ですので、海外出張時や自宅でのWi-Fiに接続してリモートアクセスすることを考え、VPNと併用すると、さらに柔軟性が高いテレワークが可能になるでしょう。

モバイル端末を社内ネットワークに“安全に”接続する方法

公衆無線LAN

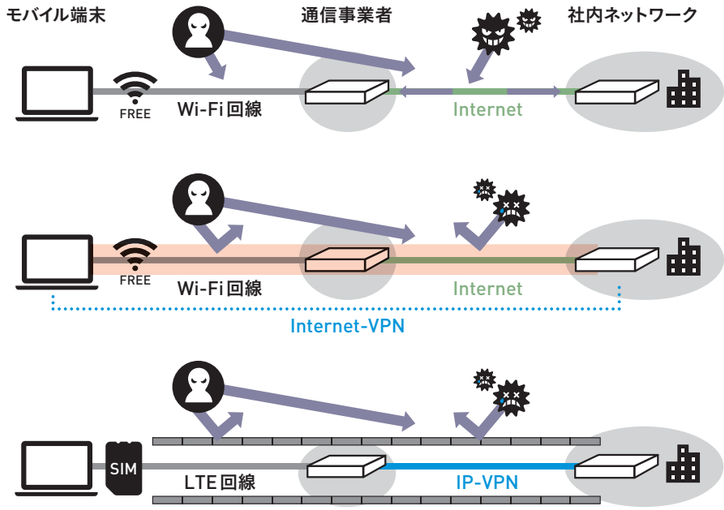
公衆無線LANサービスでは、無線LAN部分もしくはインターネット上での盗聴リスクが残ってしまいます。インターネット経由でのマルウェア感染の可能性もあります。

公衆無線LAN＋Internet-VPN

Internet-VPNを使用することにより盗聴を防ぐことができますが、VPNのID/パスワードが漏れてしまうと、なりすましでログインできるリスクや、ユーザーがVPNの接続する前の通信において盗聴やマルウェア感染のリスクが残ります。

閉域網SIM

閉域網SIMを利用する場合、端末にSIMスロットがあれば単純に対応SIMを差すだけで「モバイル専用線」として安全な接続が可能で、なりすましリスク、マルウェア感染リスクも低くなります。



Internet-VPNと閉域網SIMの比較

	なりすまし	盗聴	端末感染	管理	接続	速度	海外利用	コスト
Internet-VPN	VPNアカウントを守ることでなりすましを防げる	VPNの強度に依存する	VPN接続前にインターネットに接続されるため、その時点での感染リスクがある	アカウントの管理が必要	利用者が認証操作をする必要アリ	有線／無線LANが利用できる	海外であっても同様に利用が可能	￥￥ VPNサーバーとアカウント管理コストが発生
閉域網SIM	閉域SIMはデバイスそのものが認証の鍵になるため、VPNに比べなりすましリスクは低い	インターネットに出ないため、より盗聴に強い	直接インターネットに接続しないためリスクは低い	デバイスそのものの管理のみでOK	操作なしで接続	MVNOの性能に依存する	ローミング対応になるためコスト的に不利	￥￥ MVNO/MNOとの契約が必要

モバイル端末から社内ネットワークにつなげるアクセスラインもさまざまな選択ができるようになりました。インターネット上でVPNを活用する手法以外にも、インターネットに出ない「閉域網SIM」を利用する手法も検討したいところです。

SECURITY

法人専用 VAIO Pro シリーズ 新登場

11.6型ワイド
VAIO® Pro PF

OS Windows 10

カラー ■ブラック ■シルバー ■ブラウン □ホワイト

13.3型ワイド
VAIO® Pro PG

OS Windows 10

カラー ■ブラック ■シルバー

15.5型ワイド
VAIO® Pro PH

OS Windows 10

カラー ■ブラック ■シルバー □ホワイト ■ピンク

2つのサイズから選択可能 今選ぶなら、SIMフリー内蔵PC

特長① 安心の日本製

フラットアルミバームレストや、カーボン天板など、体裁に大きくかかわる部分に日本製部品を使い、タッチパッドや、キーボードなど、高い精度の組み立てが求められる部品を、敢えて国内工場で丁寧に組み立てることで、高い品位を保っています。

特長② 充実の通信機能

モバイルデータ通信機能を内蔵したLTE搭載モデルなら、本体だけでインターネットにアクセス可能。電波状況に応じてWi-FiとLTEの接続を切り替えるので、ストレスなくインターネットにアクセスできます。キャリア・アグリゲーションやMU-MIMOにも対応しています。

対応しているLTEバンド

LTE：1,2,3,4,5,7,8,12,13,17,18,19,20,21,25,26,28,29,30,38,39,40,41,66
3G：1,2,4,5,6,8,19

特長③ 指紋センサー搭載

Windows Hello 対応の指紋認証機能を選択可能。面倒なパスワード入力を省略しつつ、安全性とユーザビリティを両立できます。

特長④ 法人要件に対応

基本的な PC 選定基準をカバーしています。

セキュリティ…P.16
セキュリティロック・スロット
セキュリティチップ（TPM）
パワーオン／ HDD パスワード
Wake On Lan
ポート／スロットの無効化
暗号化機能付 SSD（OPAL2.0 準拠）

ユーザビリティ
VGA ／ HDMI 出力／有線 LAN 端子
振り分けタイプの USB 3.0 端子
段差を抑えたバームレスト
静音キーボード
誤操作を防ぐ 2 ボタンタッチパッド

長期利用
長期利用に耐える高品位設計

特定用途向けOS、Windows 10 IoT Enterprise 2016LTSBモデルも提供可能
Windows 7搭載13.3型ワイド　VAIO Pro® PBもご用意しております

大画面・光学ドライブ・テンキー付き オールインワンノートPC

特長① 高性能CPU搭載

TDP 45W の高速プロセッサー、H プロセッサーラインを採用。マクロ付き Excel ファイルや DB など大きなファイルも快適に作業することが可能です。

特長② ちょっとした持ち出しも可能

最大約 7.6 時間のバッテリーライフ。液晶一体型デスクトップクラスの性能を、会議室にも持ち出せます。

特長③ オフィス利用に最適な全部入り

基本的な PC 選定基準をカバーしています。

セキュリティ…P.16
セキュリティロック・スロット
セキュリティチップ（TPM）
パワーオン／ HDD パスワード
Wake On Lan
ポート／スロットの無効化

ユーザビリティ
VGA ／ HDMI 出力／有線 LAN 端子
振り分けタイプの USB 3.0 端子
テンキー付フルサイズキーボード
誤操作を防ぐ 2 ボタンタッチパッド
データ受け渡しに便利な光学ドライブ

長期利用
長期利用に耐える高品位設計

インテル®Core™プロセッサー
Intel Inside® 飛躍的な生産性を

高品質のワケ

すべての機種で徹底した信頼性評価試験を実施し、堅牢性を追求した製品づくりを行っています。
また、出荷前の全数国内検査により初期不良を最低限度に抑制、信頼を裏切らない1台をお届けします。

信頼性評価試験

あらゆる利用シーンを想定した試験の種類は数十項目に及びます。さらにモバイルノートには持ち運びを想定した厳しい試験を実施しています。

<キーボード水かけ試験> VAIO Pro PF/PGで実施

電源を入れた状態で150ccの水を注ぎ、データを保存するまでの間、異常終了しないことを確認。予期せぬトラブルを防ぎます。

キーボードから内部に水が入りにくい構造を実現

全数国内検査

長野県安曇野市にあるVAIO本社工場の専門の技術者が、約50にも及ぶチェック項目について出荷前に全数国内検査を実施し、初期不良の発生を最低限度に抑制します。

※品質試験は、弊社の規格に基づいて特定の環境のもとで行われています。本製品の品質試験は、無破損・無事故を保証するものではなく、PCのデータを保証するものではありません。

導入ご検討の皆さまへ

PCのことでお困りなら、お気軽にVAIOにお問い合わせください！

開発設計から製造まで行う日本メーカーならではの経験・品質で、PCライフサイクルに付随する多くの業務負担を軽減します。東京オフィスに常駐する経験豊かな技術担当が、お客さまをサポートいたします。

Q. 情シス担当が1人しかいないので、PC入れ替え時の負担が大きい
A. VAIOのキッティングサービスなら、さまざまなお悩みを解決できます

Q. モバイルワークにお勧めのソリューションは？
A. モバイルデータ通信機能を内蔵したLTE搭載モデルにお勧めのSIMカードやソリューションなど、ご要望にあわせてご提案いたします

Q. 会社に来てサポートしてほしい
A. ご指定の場所までサービスエンジニアがお伺いして修理を行う「オンサイトサポート」プランをご用意しております

ご相談は、お気軽に　☎050-5578-8697

受付時間　月～金　9:00～17:30（12:00～13:00を除く）※土日祝日システムメンテナンス、当社指定定休日を除く