blancco

ビジネスの継続とデータ消去

不確実な時期に対する5つのヒント

Why Blancco

Blanccoは、データ消去およびモバイルデバイス診断ソフトウェアの業界標準です。
当社のデータ消去ソフトウェアは、何千もの組織に、幅広いIT資産にわたって持続可能なデータサニタイズプロセスを実現するために必要なツールを提供します。
資産を物理的に破壊するのではなく、消去して再利用することに重点を置くことで、組織はセキュリティ態勢を改善し、企業の社会的責任要件に対処すると同時に、ローカルおよびグローバルのデータプライバシー要件へのコンプライアンスを確保できます。

Blanccoのデータ消去ソリューションは、世界中の15を超える行政機関および主要組織によってテスト、認定、承認、推奨されています。
他のデータ消去ソフトウェアは、政府機関、法的機関、および独立した試験所によって設定された厳しい要件のこのレベルのコンプライアンスを誇ることができません。
Blanccoによるすべての消去は、検証および認定され、改ざん防止の監査証跡が作成されます。

世界的な不確実な風潮は、答えよりも多くの問題をもたらします。Blanccoは、既存顧客との会話に基づき、法人ビジネスにおける継続性チームが懸念する5つの領域を定義します。

1. 外部ベンダーやサービスプロバイダーとのアクセス制限

データセンターやデスクトップの計画された廃止プロジェクトは、これまで外部ベンダーによるオンサイトサービスが積極的に利用され行われてきました。
新たなロックダウンポリシーにより、危機的状況における多くのグローバル企業組織にとって、これは運用上の課題となっています。
廃棄資産の蓄積を回避し、これらの問題を克服するために、自組織内における効率的なデータ消去プロセスを展開するためのアドバイスを、Blanccoは提供することができます。
また、完全な監査証跡を残すことができるリモート消去機能を活用する方法を提示することも可能です。
これにより、データ侵害のリスクを排除して廃棄資産を施設から外部へ持ち出すことができるようになり、外部の人間の介入なしに、リスクのない資産償却が可能になります。

2. 予期せぬ正規雇用者、非正規雇用者の減少の中でのデータ消去の確認

企業の困難な状況においては、組織の従業員に計画外の緊急事態の削減または変更が行われることがよくあります。会社を去る個人が使用する会社所有の資産 (または機密の会社データを含む個人資産) は、使用されなくなったときに、完全な監査証跡を残して、適切なデータ消去を施す必要があります。
リモート消去では、従業員が特定のデバイスを使用しなくなった際に、管理者が自宅を離れることなく、対象の従業員の機器のデータを消去することで、これらの懸念を取り除くことができます。 この運用は、以下の2つの主要な懸念を解決します。

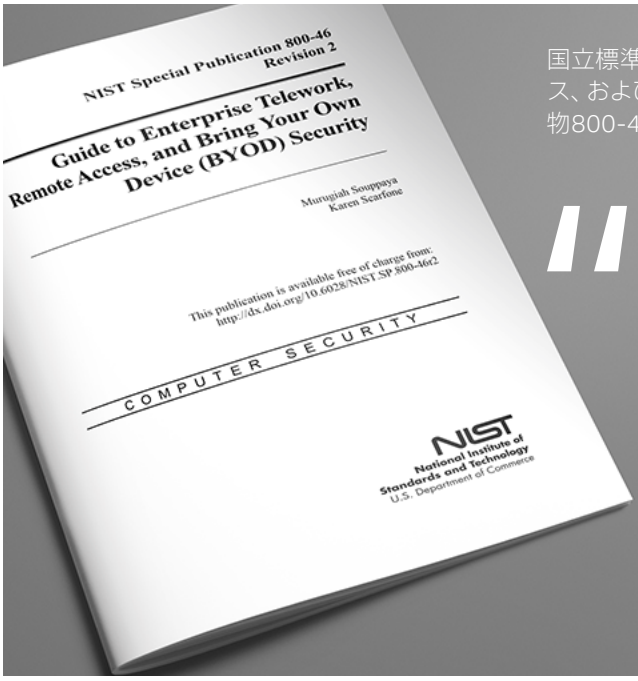
- 資産が機密データを保持したまま移動しない。
- 内部のセキュリティリスクをもたらす可能性のある機密データへの従業員のアクセスを削除。

これらのシナリオでデータ消去プロセスを持つことは、ISO 27001ガイドラインを満たすことにもなります。

3. NISTのセキュリティガイドラインに従い、在宅勤務者とデータを安全に共有

ホームオフィスでデジタルデータを保護することは最も重要です。
従業員が安全なオフィス環境を離れ、通常より安全性の低いリモートの場所から機密性の高いデータを処理し、アクセスすることは避けられません。そのため、企業データと個人データがデータ侵害のリスクにさらされる可能性があります。
在宅環境であっても、個人情報保護法やEU GDPRなどのプライバシー法が確実に遵守されるためのベストプラクティスを施すことが重要です。
これらの環境でデータ保護を向上するためのヒントをいくつか紹介します。:

- ファイルを安全に削除するために、不要になったファイルを随時OSのごみ箱へ入れるようにユーザーに指示します。
  IT管理者はBlancco File Eraserを使用して、遠隔の仕事用コンピューターへシステムがシャットダウンするたびにごみ箱のデータを安全かつ自動的に消去するスクリプトを設定します。
- 保持期間が設定されているWeb会議や、機密事項を含むのディスカッションが含まれる可能性のあるWeb会議の記録は、ユーザーが不要になったときに安全に消去する必要があります。
- ファイル共有、バックアップ、および通信の一時的なソリューション、特にデータがオフィスの物理環境もしくはネットワークの外部に保存されている場合、すべてアクティブなデータ消去が必要になる場合があります。 Blanccoは、これらの懸念に対処するための最良の方法をITチームにアドバイスできます。
- リモートワークの環境では、電子メールによる機密データの共有が増加する可能性があります。このデータの保護は、セキュリティとコンプライアンスの視点から重要です。
  Blanccoを使用することで、リモートマシン上の電子メール添付ファイルのアーカイブをターゲットにして、自動的に消去し、情報流出のリスクを回避できます。



国立標準技術研究所 (NIST) は、「エンタープライズテレワーク、リモートアクセス、および自分のデバイスの持ち込み (BYOD) セキュリティの手引き」の特別刊行物800-46r2で、組織が次のことを実施するようにアドバイスしています。

> ... 必要最小限のデータにのみ、アクセスし、保存をする。

リスクの高いテレワーク (特定の海外旅行など) のために、一部の組織においては、テレワーク前とテレワーク後に完全に消去を施す"代替"デバイスを用意します。
テレワークに必要なデータと許可されたアプリケーションのみが代替デバイスにロードされます。代替デバイスはテレワークにのみ使用され、組織の内部ネットワークに接続されていない場合があります。使用前のデータ消去は、テレワークが行われる前にデバイスがクリーンであることを保証し、使用後のデータ消去は、将来アクセスされるテレワークデータが残っていないことを保証します。

多くの従業員が一時的にオフィス環境からリモート作業に移行しているため、多くの企業において、従業員の仕事へのリモートアクセスを可能にする便利な方法としてBYODポリシーを検討しています。

集中型監査機能をあわせ持つ、リモート消去と自動化は、リモートワーカーのセキュリティイニシアチブをサポートするための鍵

BYODデバイスに保存されている企業データを制限し、保存データが冗長になると削除することは非常に重要です。NIST 800-46r2は次のように述べています。
「組織によっては、BYODデバイスのデータ消去に対処することが特に難しい場合があります。 デバイスは個人用と仕事用の両方に使用されるため、個人データに影響を与えずにテレワークデータをスクラブする必要がある場合があります。」
Blancco File Eraserは、企業がBYODデバイスの個人データに触れることなく企業データを消去できるようにするのに役立ちます。

リモートアクセスサーバーも検討することが重要です。 NIST SP 800-46r2が助言するように、「機密のユーザーデータを一時的に保存する可能性のあるポータルサーバーでは、不要になったときにすぐにそのようなデータをサーバーから消去すると、サーバーのセキュリティ侵害の潜在的な影響を減らすことができます。」

4. バックアップサイトと災害復旧サイトでのデータの保護

危機緊急時において、重要な業務機能のために、企業はバックアップサイトを活用することがよくあります。 今日では、影響を受けた個人によって、企業の一部のサイトが危険にさらされている可能性があり、業務を別のサイトに移管する必要がある可能性があり、これはかつてないほど重要になっています。 例えば、銀行のトレーディングフロアにいる個人が感染者であることが判明した場合、操作 (デスクトップ/ラップトップなどの日常使用機器を含む) は、隔離およびサニタイズルールに準拠するためにバックアップサイトに移動する場合があります。 大規模は移動の前には、輸送中のデータの損失や盗難から保護するためにデバイスを消去する必要があります。 同様に、別の場所にバックアップ機器がある場合は、バックアップ場所の使用を中止するときにそれを消去します。
災害復旧サイトについても同様です。
データ処理とストレージを別のサイトに移動する場合、サイトを安全に使用停止と見なす前に、データを移行するたびに適切なデータ消去と監査証跡が必要になります。

5. 不要になった一時的な仮資産のデータ消去

多くの企業において、従業員の一時的なリモート作業に移行しています。これらの動きの一環として、多くの企業が在宅勤務を容易にするために追加の機器を購入またはレンタルしています。例えば、ラップトップの短期リースを利用すると、職場にデスクトップがあれば、従業員は自宅で仕事ができます。
これらのデバイスを貸手に返却する前に、機密性の高い従業員、会社、または顧客の情報を削除するために完全な消去を施す必要があります。また、完全な監査証跡への準拠を証明するには、消去ごとに証明書を取得する必要があります。
追加の資産調達には、専門的な資産管理ルーチンへの慎重な組み込みも必要です。
特に、デバイスがリモートの従業員またはベンダーへ配送される場合、一連の保管プロセス中において機密データが危険にさらされます。
レンタルでも購入でも、リースまたは会社に返却する前にこれらのデバイスをリモートで消去することが重要です。

対面でのコミュニケーションや、多くの移動を減らすことは、不確実な時期には重要です。集中型監査機能を持ち合わせたリモート消去と自動化は、リモートワーカーのセキュリティイニシアチブをサポートするための鍵です。

今日、特定のファイルやフォルダー、デスクトップとラップトップの全領域、サーバー、SANS、VMをリモートで消去する成熟したプロセスは、 世界中に資産が存在する大企業のベストプラクティスです。

詳細については、当社のウェブサイトをご覧ください。www.blancco.com/ja/