



データセキュリティ 製品ラインナップ

いつでも どこでも 全てのファイルを暗号化



いつでも どこでも 全てのファイルを暗号化

情報の保護とは、情報を形成するための基本要素である「データファイルの保護」と言えるでしょう。SecureAgeのセキュリティは、その「データファイルの保護」を確実にします。SecureAgeは、本カタログに記載されているソフトウェア製品とハードウェア製品を通じて、強力なセルフディフェンス機能(暗号化と独自のセキュリティアプリケーション)を提供することにより、いつでもどこでも全ての存在するファイルを永続的に保護します。

ユーザビリティとセキュリティの共存

確実なデータの保護には、単にファイルを保護するだけでは不十分です。ユーザの知識レベルを問わず、生産性を犠牲にすることなく、多くの人アクセスして、いつも変わらずに使用できる環境を作ることも重要です。SecureAgeの製品は、どんなユーザも時にはミスをしてしまうことを前提に設計されました。暗号化と独自のアプリケーションにより、ユーザとファイルをオンオフに関わらず常に保護しながらも、特別な意識や作業を必要とさせませんので、ユーザの使用性や効率を損なうことはありません。

管理しやすい環境の提供

暗号化は「環境の構築や維持が複雑で面倒」と思われるかもしれません。SecureAgeのソリューションは、厳重な監視機能を保ったまま、柔軟性を失うことなく、環境に合わせた独自の管理構成を提供します。全てのSecureAge製品は、きめ細かいポリシー設定と堅牢なログ生成で、データを限りなく制御し、あらゆる規模の組織に対応することができます。

目次

- 01 イントロダクション

- 03 セキュアエイジのデータ保護

- 05 エンドポイント ソフトウェア ソリューション
 - SecureData - セキュアデータ
 - SecureFile - セキュアファイル
 - SecureDisk - セキュアディスク
 - SecureEmail - セキュアEメール
 - SecureAPlus - セキュアエープラス
 - Secure NetGuard - セキュアネットガード
 - LockCube - ロックキューブ

- 13 デプロイメント & ハードウェア ソリューション
 - The SecureAge Suite - セキュアエイジスイート
 - Security Management Server - 管理サーバ(SMS)
 - Enterprise SSL VPN - 企業用 SSL VPN
 - Data Diode System - データダイオードシステム

- 17 セキュリティ ソリューション 概要図
 - Endpoint Software
 - Hardware & Network Security
 - Data Diode System for Closed Networks

セキュアエイジのデータ保護

。。。 保存データの保護

データは保存されている間、紛失や盗難に対して内部からも外部からも常に脆弱であり続けます。SecureAgeには、単一のファイルであっても、収集されたボリュームファイルであっても、あらゆる場所、あらゆるメディアに保存されたデータを保護するために設計された、さまざまなソリューションがあります。

非アクティブデータまたはアーカイブデータは、通常、物理ハードウェアおよびネットワークインフラストラクチャよりも寿命が長いものです。SecureAgeソリューションを使用すると、データを新しいメディアにコピーする際、複製、完全削除、およびキー管理等の情報が表示され、管理者は周辺ソリューションの背後にそれらのデータを隠すことができます。暗号化されたデータは、いかなる種類のメディアでも安全に永続的に保存され、そして通常と変わらずに使用することができます。



動作中のデータ保護

盗難および漏洩の大部分は、データの使用中または動作中の攻撃によるものです。SecureAgeは、データがアクティブ状態にある時にもデータ保護を行うソリューションを提供しています。しばしば見られるボリューム暗号化ツールで保護されたデータファイルは、非アクティブでアクセスできない時しか保護されません。

動作中のデータが最も脆弱であると考えられるSecureAgeの製品は、データファイルの使用状況や場所に関係なく、暗号化の完全性と堅牢性を維持することを念頭に開発されました。SecureAgeのソリューションを導入すれば、ファイルがアクティブな状態で開いていても、内部ネットワーク内であっても、またはインターネット上を移動中であっても、ファイルがどこにあっても、どんな状態であれ保護されますので、いつも安全に作業を行うことができます。



マルウェアからの保護

近年見られる進化したマルウェア攻撃は、主にネットワークやシステムを侵害する目的に始まり、攻撃者によっては、機微情報を窃取されてしまいます。

SecureAgeのソリューションツールには、データファイルが未保護な状態になることを防ぐだけでなく、マルウェアの実行を監視および防止する機能があります。SecureAgeのアプリケーションホワイトリスト機能は、未知のプロセス実行を停止させます。アプリケーションバインディング機能は、信頼されたアプリケーションが、攻撃者により未解決の脆弱性を悪用された場合に、被害を最小限に抑えることができます。



多様な製品展開

SecureAge製品は、データ経路の全範囲に対応し、攻撃や漏洩の隙を作りません。エンドポイント、サーバ向けのソフトウェア製品、ハードウェアアプライアンスの管理サーバ、そして仮想マシンやクラウドも含め、セキュリティ製品を多岐にわたり展開しています。

ソリューション製品	保存データの保護	動作中のデータ保護	マルウェアからの保護	製品展開
 SecureData	●	●	●	● ■
 SecureFile	●	●		●
 SecureDisk	●	●		●
 SecureEmail	●	●		●
 SecureAPLus	●	●	●	● ■
 Secure NetGuard		●		■
 LockCube	●			● ■
 管理サーバ (SMS)	●	●	●	▲ ■
 企業用 SSL VPN	●	●		▲
 データダイオードシステム	●	●	●	● ■ ▲

凡例: ● エンドポイントソフトウェア ■ サーバーソフトウェア ■ 仮想マシン ▲ ハードウェアアプライアンス

販売 サービスおよびサポート

複雑な環境や様々なリクエストをお持ちのおお客様のご要望にお応えできるよう、SecureAge製品はカスタマイズが可能です。環境や業務内容、規模の大小を問わず、ニーズを満たす構成をサポートいたします。同様に、ソフトウェア、ハードウェア、保守、サポート、カスタムコード、およびその他専門的で柔軟なサービスオプションをご用意しております。

ライセンス

階層型ボリュームライセンスによる、永久ライセンス、または年間契約プラン

技術サポート

年間契約または都度対応による、電子メール、電話、またはオンサイトサポート

トレーニング

管理者もしくはユーザ向けの、リモートまたはオンサイトトレーニング

メンテナンス

年間メンテナンスプランによる、ソフト/ハードウェアのアップデートおよびアップグレード

コンサルティング

個別に希望する構成に対応するための、購入前または購入後のコンサルティング

カスタマイズ

個別の製品変更、または要件を満たすためのカスタムコード作成



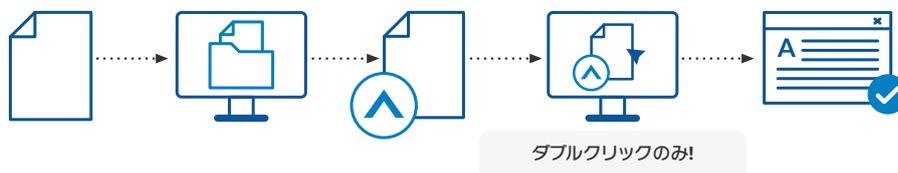
SecureData

自動&透過的ファイル/フォルダ暗号

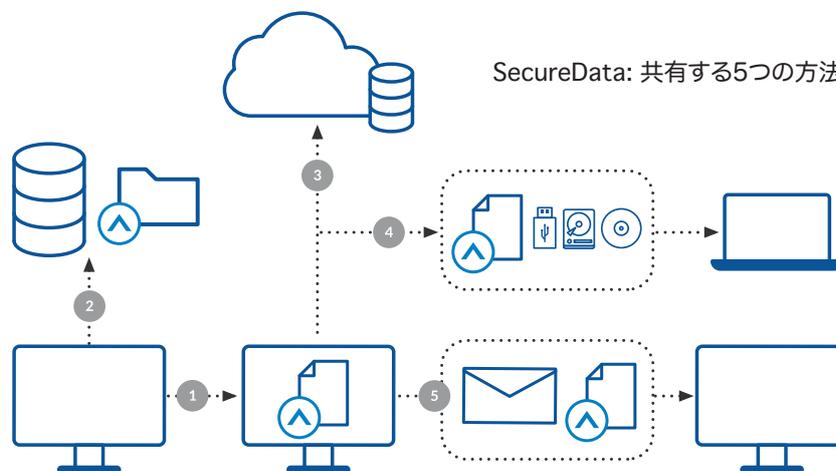
SecureAge SecureDataは、ユーザの思考、作業、認識も必要とせず、すべてのユーザファイルを自動的に透過的に暗号化する、エンドポイントエージェントとして働きます。シームレスなPKIを実装していますので、使用中でも保存中でも、たとえ紛失、盗難されても、各ファイルは個別に暗号化されたまま、永続的に保護されます。



オプション機能であるアプリケーションホワイトリスト、実装のアプリケーションバインディングを用いれば、ウイルス、マルウェア、ランサムウェア、ゼロデイ、APT(高度持続的脅威)、その他の脅威を大切なデータに寄せ付けることはありません。内部または外部からの攻撃、紛失、漏洩、盗難から、すべてのファイルは安全に守られます。



SecureDataによって個別に暗号化されたファイルは、異なるストレージメディア、ネットワークの場所に格納されても、または企業ポリシーに応じて、電子メールに添付されたりクラウドに移動されても、暗号化が維持されます。公開鍵基盤(PKI)の採用により、いつも通りファイルを共有し、アクセスして共同作業を行うことができます。

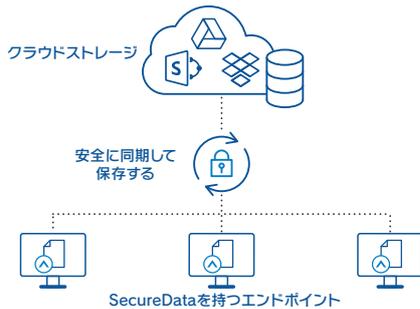


1. ネットワーク転送(直接) 2. 共有ネットワークフォルダ 3. 共有クラウドストレージ
4. 外部メディア 5. 電子メール(暗号化電子メールポリシー)



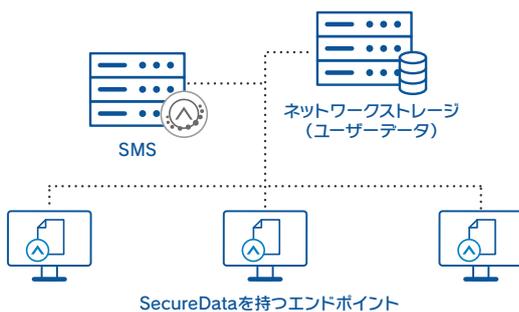
SecureData コンフィグレーション

SecureData クラウドストレージ/バックアップ用



環境や希望の設定に応じて、SecureDataの自動ファイル暗号化は、ファイルがクラウドに移動、保存された場合も持続します。クラウドの所有者または管理者であっても、SecureDataで保護されたユーザーファイルの内容を覗くことはできません。さらに堅牢なログ機能により、クラウドにいつ、誰が、どこで、どのような状態で何を入れたのか明確に記録が残されます。

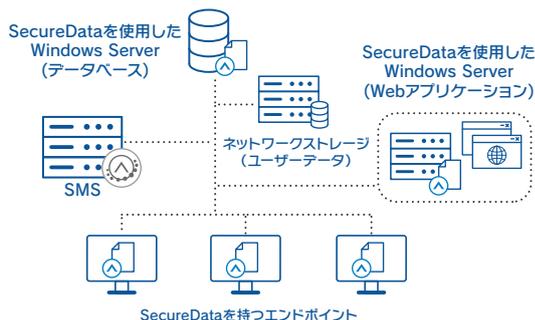
SecureData ローカルネットワークストレージ用



SecureDataがクラウドに格納されるファイルに永続的な暗号化を提供するのと同様、ネットワークドライブ上に置かれたユーザーファイルも常に安全に暗号化されたまま、ファイル所有者はすぐにアクセスすることができます。

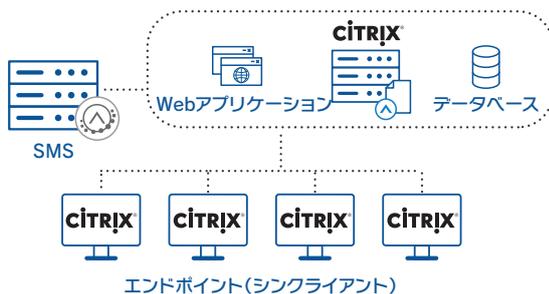
また、SecureDataでは、共有フォルダや共有ドライブの作成が可能です。保存されたファイルは、共有リストに含まれる任意のユーザのみ開いて編集、保存することができます。

SecureData データベースとWebアプリケーション用



同様に、SecureDataは、データベース、Webページ、ユーザーデータおよびストレージサーバやWindowsプロダクションサーバ上にある不可欠なデータを、どんなファイルタイプであれ、暗号化して保護します。Webアプリケーションと関連するデータも安全です。また、データベースファイルが保護されるだけでなく、暗号化されたデータベースファイルに対して行われたクエリは、遅延や特別なプロセスも無く、通常と同様の結果を得ることができます。暗号化されている間も、ファイルコンテンツの検索はいつもと何ら変わることはありません。

SecureData シンクライアント (Citrix) 用



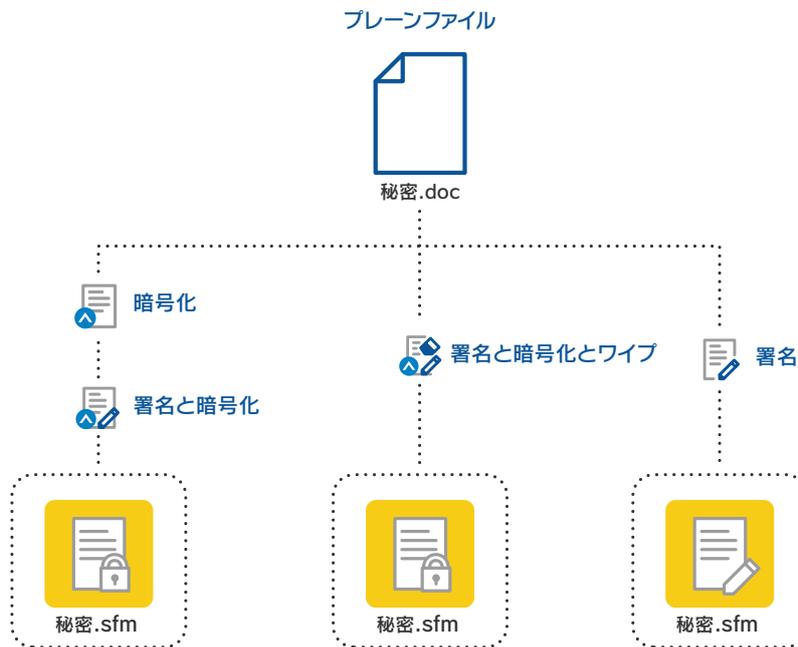
共有ワークステーションまたはシンクライアント環境でも、スタンドアロンと同じく、ファイルレベルの暗号化と包括的なデータ保護を行うことができます。ユーザ数やワークステーション共有の目的を問わず、各ユーザの暗号ペアキーに関連付けられているファイルにアクセスして、コンテンツの表示や編集を行うことができます。ここでも、ネットワーク管理者は、ファイル内容を知ることができません。



SecureFile

ミッションクリティカルなデータ用ファイル暗号化とデジタル署名

SecureFileでは、コンプライアンスやファイル共有目的で、暗号化とデジタル署名を用い、選択されたファイルに対して包括的なPKIベースの書類セキュリティを提供でき、それは一般のファイル暗号化ツールを超越した機能と言えます。SecureFileは、選択されたファイルの暗号化または署名付きのコピーを生成し、オリジナルファイルはそのままの状態に残します。



選択済みファイルは保護され、ファイルタイプは、他者と共有されている場合、完全性と信頼性を確保して隠されます。その場合、両エンドでSecureFileアプリケーションが必要です。

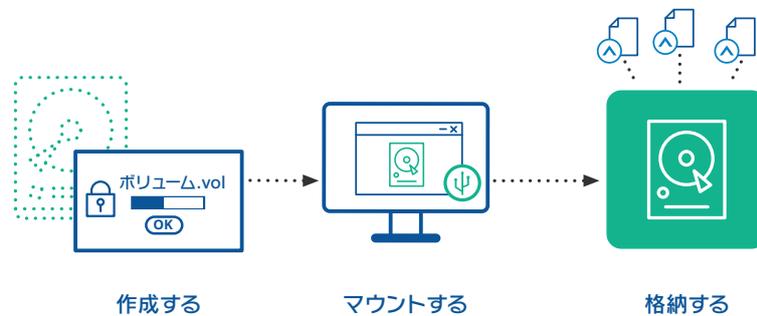


最も重要なポイントは、SecureAgeのPKI機能で、SecureFileの受信者を複数選択できることです。SecureFileの作成者は、公開鍵が存在するユーザーリストの中から、SecureFileのコピーを共有するユーザーを選択するだけです。SecureDataは集中型で単一ファイルとして存在しますが、SecureFileは各受信者にローカルコピーを生成します。

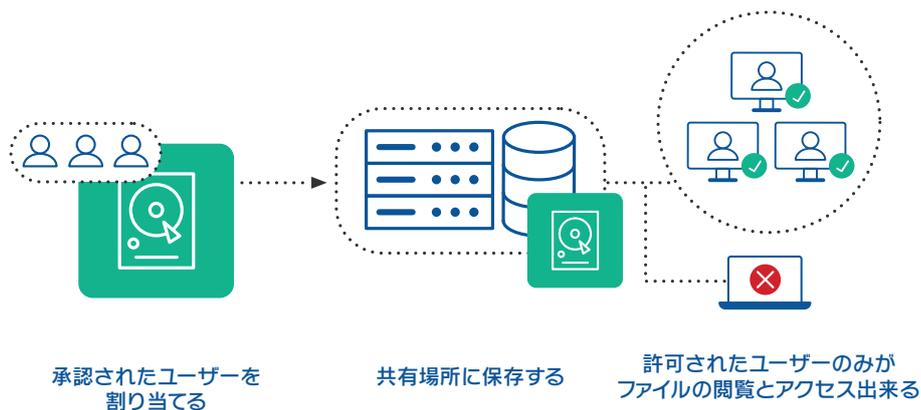


ボリューム暗号化で機密データを迅速かつ安全に保管

SecureDiskは、Windowsベースのエンドポイントまたはサーバー上で仮想ディスクボリュームを作成し管理します。SecureDiskボリュームに保存されているすべてのファイルは暗号化されて、完全に見えない状態になります。全ディスク暗号化(FDE)と同等の利点がSecureDiskに付属しているだけでなく、ユーザーが選択する任意のサイズで複数のボリュームを作成し、どこにでも保存できるという柔軟性も備えています。



SecureDiskボリュームを作成するには、サイズ、名前、保存場所を決定するだけで済みます。一度作成してマウントすると、SecureDiskボリュームのサイズ制限までファイルをアンマウントするまで、ボリューム内にドラッグすることができます。その後は、鍵がない人には見えなくなり、アクセスできなくなります。ボリュームは、メディア、ネットワークドライブ、またはクラウド上に保存でき、そこから呼び出すことができます。



PKI基盤のSecureDiskは、使いやすく強力な共有機能を提供します。SecureDiskボリュームの作成者は、作成時または作成後に、共有アクセスできる他ユーザを追加できます。承認ユーザの公開鍵でコンテンツを暗号化していることで可能になる機能です。共有ボリュームを承認ユーザに都合の良いストレージ場所に配置することで、シームレスで安全なファイル共有を可能にします。



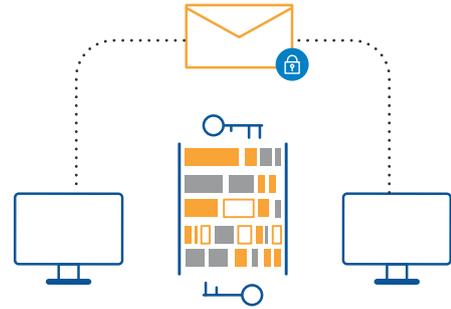
SecureEmail

ポリシーベースの End-to-End 電子メール 暗号化

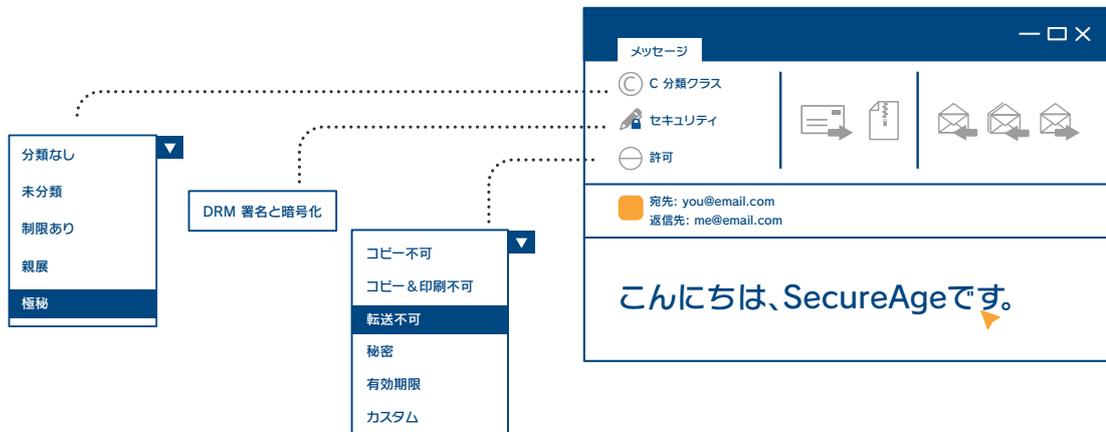
世界的に見られるデータ漏洩は、すべてのデータを、特に電子メールについて暗号化を行う意義を示しています。しかし、電子メールの暗号化は複雑で難解であるとして、多くの企業やユーザが、この重要なステップをスキップしているのではないのでしょうか。

電子メールの暗号化は、電子メールの送信と同じくらい簡単でなければなりません。しかも、直感的で誰にでも使いやすく。

SecureEmailは、ユーザのトレーニングやメールの送受信方法を変更を必要とせずに、信頼性とプライバシーを確保します。



独自のデジタル著作権管理 (DRM) オプションとともに、PKI機能を備えたSecureEmailは、業界最高水準の暗号化と、煩雑な管理と手続きを必要としない強固な鍵管理を提供します。



SecureEmailは、メールクライアントソフトウェアMicrosoft OutlookおよびIBM Notesに直接プラグインし、メールのラベル付けおよび分類のためのドロップダウンメニューを提供します。これらのユーザ定義の分類は、送受信する両ユーザがSecureEmailを使用している場合、受信者側のメッセージの制御を可能にする署名や暗号化、DRMオプションなどのセキュリティレベルにリンクすることができます。

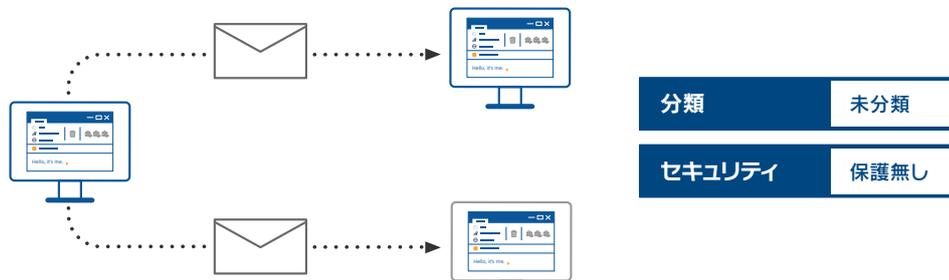




SecureEmail 送信&受信シナリオ

SecureEmailをプラグインインストールしていても、メール作成時に「未分類」や「一般」といったラベルを、「保護無し」や「非暗号」といったセキュリティレベルに紐付ければ、以前と同じように非暗号化メールを送信することができます。一方で、保護無し、非暗号といったラベルのメールは、企業ネットワークにオンライン中、または、オフライン中にかかわらず、ユーザごとに常に適用されるポリシーを相応に設定することで、作為／無作為いずれの危険からも守ることができます。

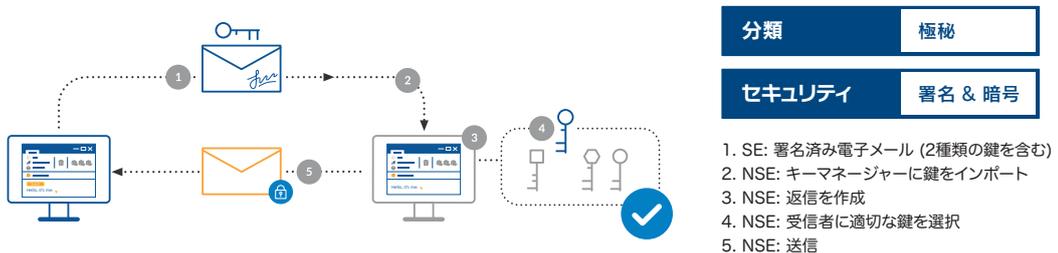
一般のEmail: 社内 & 社外 ネットワーク



暗号化Email: SecureEmail ユーザ to SecureEmail ユーザ



暗号化Email: SecureEmail ユーザ (SE) to Non-SecureEmail ユーザ (NSE)



シナリオ1: SecureEmailユーザが、初めてNon-SecureEmailユーザに公開キーを提供する



シナリオ2: Non-SecureEmailユーザが、初めてSecureEmailユーザに公開キーを提供する



SecureAPlus

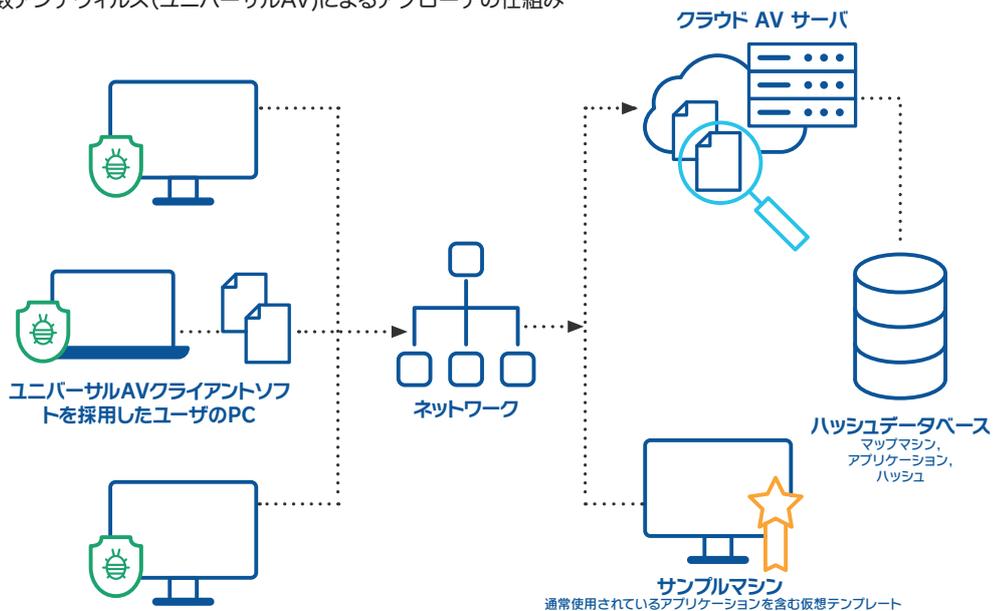
10種類以上のクラウドアンチウイルスとホワイトリスト

SecureAPlusは、ランサムウェアやウイルスといったデジタル脅威からデータを保護するために設計された、特許取得済みのソリューションです。今までのウイルス対策製品では成し得なかった、既知または未知どちらの脅威からもデータを守ります。SecureAPlusのアプリケーションホワイトリストは、未知の脅威を食い止めることができます。



既知の脅威については、クラウド上で実行されている10種類以上のウイルス対策エンジン(ユニバーサルAV)、およびローカルのオフラインアンチウイルスエンジンによって検出されます。未知の脅威は、強力でありながら管理が簡単なアプリケーションホワイトリストのコアコンポーネントによって、完全に阻止されます。承認されたアプリケーションや実行可能ファイルがホワイトリストにない場合、ウイルスやマルウェアは実行されません。

複数アンチウイルス(ユニバーサルAV)によるアプローチの仕組み

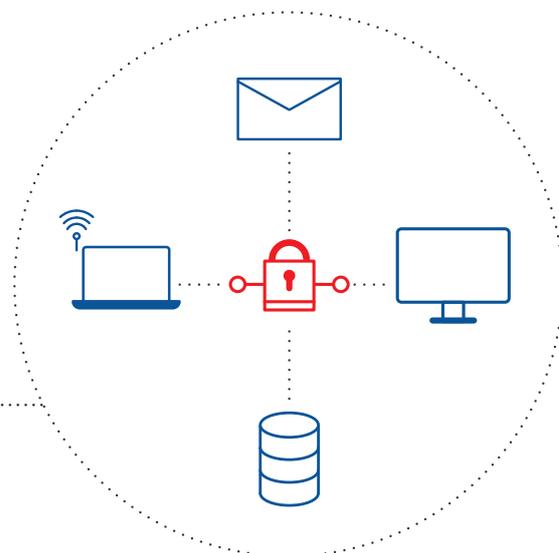




SecureNetguard

Point-to-Point ネットワークセキュリティ

SecureNetguardは、256ビットSSL(Secure Sockets Layer)およびTLS(Transport Layer Security)を使用して、すべての内部トランザクションと通信を保護するPoint-to-Pointネットワークソリューションを提供します。特に、SSL接続にアップグレードできないレガシーソフトウェア通信に適しています。

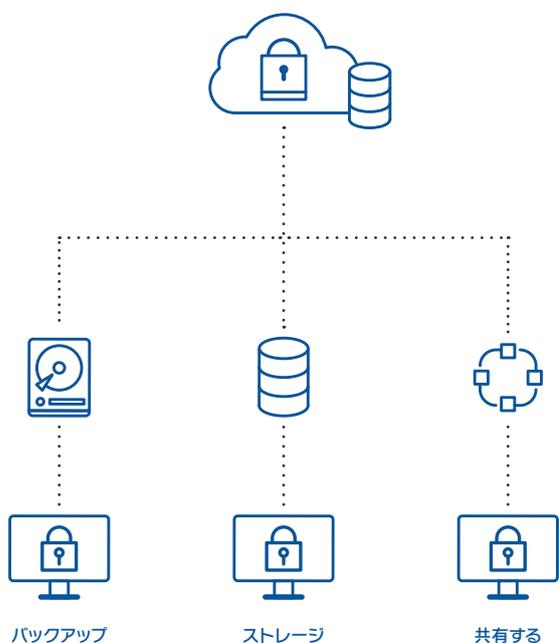


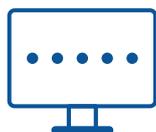
LockCube

暗号化された安全なクラウドストレージ

LockCubeは、暗号化されたクラウドストレージサービスです。ファイル(Microsoft Officeドキュメント、ZIPファイル、PDF、ビデオ、写真、音楽など)をデバイス間で安全にバックアップ、また共有することができます。暗号化は、ファイルがアップロードされる時にユーザーのマシンで行われますので、クラウドに到達する前にセキュリティを提供でき、クラウドプロバイダーがファイルコンテンツにアクセスするのを防ぎます。

適切な鍵がインストールされているPCまたはモバイル機器であれば、ダウンロード時にファイルは透過的に復号化され、すぐに利用することができます。鍵はマシン上、目に見えない形で保存されているため、ユーザーの作業や、手動で暗号化または復号化する必要はありません。アップロードとダウンロードだけの安全かつ利便性に優れた環境を体験いただけるでしょう。





The SecureAge Suite

総合的なエンタープライズセキュリティソリューション

セキュアエイジのセキュリティスイートは、SecureData、SecureFile、SecureDisk、SecureEmail、SecureAPlusの5つのエンドポイントセキュリティソフトで構成されており、故意または偶発的なデータ損失、内部および外部の脅威からの完全な保護に必要な不可欠なコンポーネントを提供する当社のコアソリューションです。

この総合的ソリューションの配置展開には、各エンドポイントへのインストールと、メンテナンス更新のために必要なライセンスのプロビジョニングが必要です。アドオンのサーバーは、集中管理のために多くのオプションと利便性を提供します。



★ ライセンス 🔍 メンテナンス ● オプション

SecureData は、生産性を犠牲にすることなく、すでに確立されたルールや経験を無駄にすることなく、すべてのユーザファイルのシームレスなセキュリティのために、自動&透過的なファイル/フォルダ暗号を提供します。

SecureEmailは、ユーザ定義の分類を使用して電子メールのセキュリティを判断し、暗号化を簡単に取り入れることができます。互換性のあるS/MIME利用の第三者メールクライアントであれば、署名、暗号化、DRMなどのオプションも利用可能です。

SecureFile と SecureDisk は、手動によるファイル暗号化と署名、または、コンテンツを自動暗号化してファイル名を隠すボリュームの作成など、特定の状況のためのツールとしてお使いいただけます。

SecureAPlusは、既知および未知の脅威からエンドポイントを保護します。クラウド上の10以上のウイルス対策エンジンを使用して、マルウェアやウイルスを検出しながら、ホワイトリストをローカルに作成、維持、適用し侵入を阻止します。

The SecureAge Suite は エンドポイントのライセンスベース です。あらゆる規模の組織のニーズに合わせて、柔軟に最大限のセキュリティで展開が可能です。

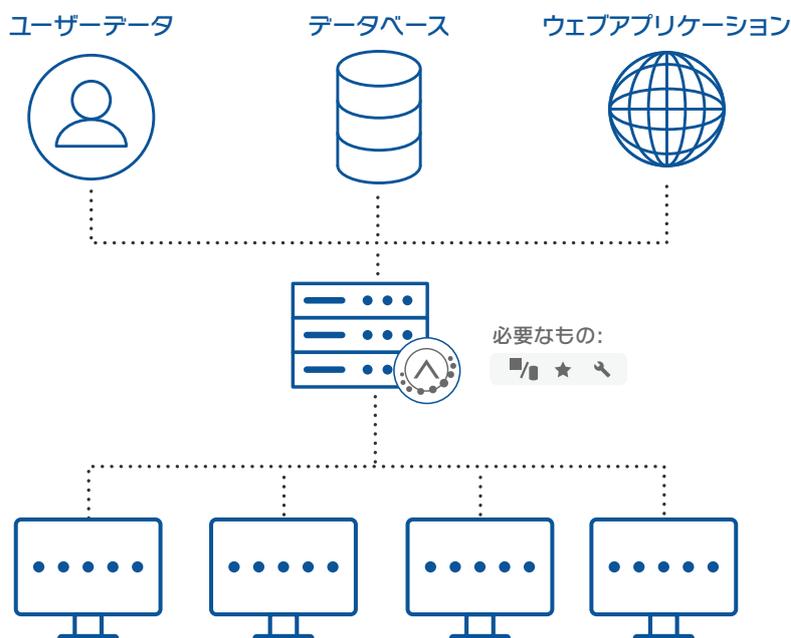


Security Management Server (SMS/管理サーバ)

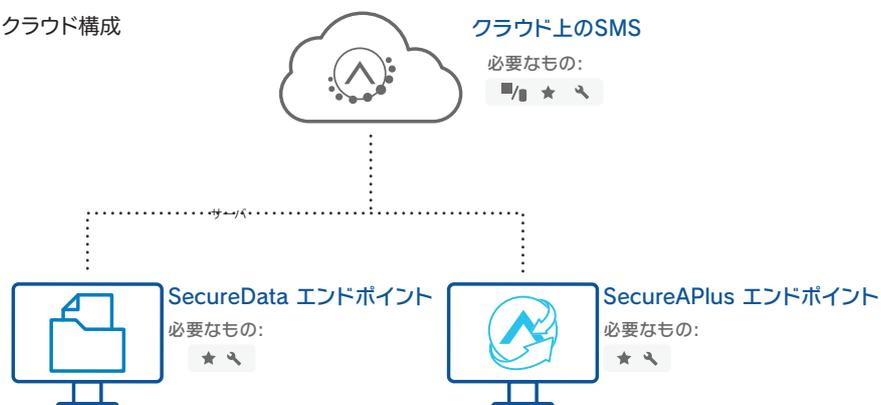
大規模セキュリティ管理をシンプルに

大規模なインストールのために、Security Management Server (SMS)は、暗号キー、個々のユーザープロフィールとポリシー、およびエンドポイントへのソフトウェア更新を、容易に作成や配布、管理を行います。また、ユーザーアクティビティの監視のために、ユーザーマシンからセキュリティログを収集します。物理的なハードウェアの他に、さまざまな展開オプションに適した仮想マシンも選択できます。

デフォルト構成



クラウド構成



■ 仮想マシン ■ サーバ ★ ライセンス 🔧 メンテナンス

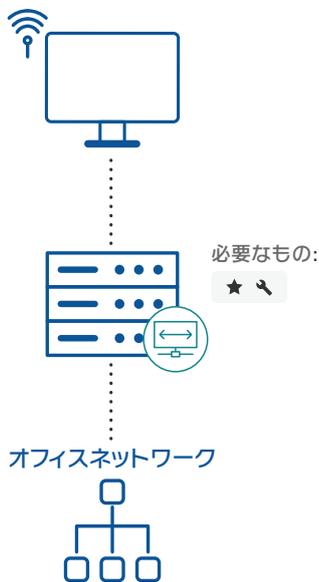


Enterprise SSL VPN

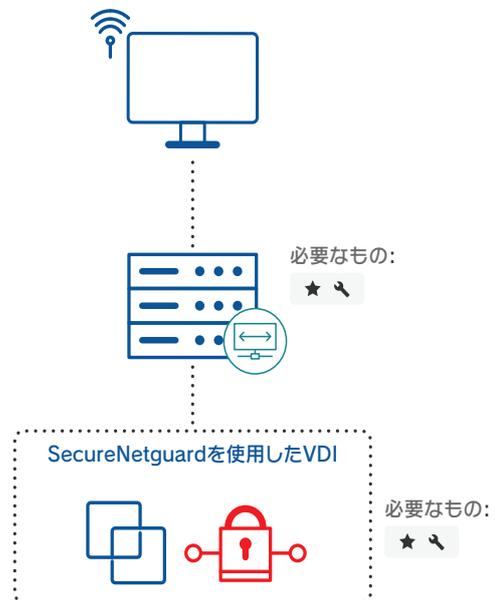
いつでもどこでも安全な接続を

SecureAge Enterprise SSL VPNは大変信頼性が高いうえ、簡単に展開が可能なセキュリティソリューションです。ユーザは十分に確立されたSSL (Secure Sockets Layer) 技術を使用して、企業のネットワークとリソースにリモートからアクセスすることができます。より多くのデバイスを接続使用することができるよう、IPSecオプションもあります。

リモート接続 to
オフィスネットワーク



リモート接続 to
オフィスネットワーク



★ ライセンス 🛠️ メンテナンス

SSL VPN を使用すると、ユーザは安全にネットワークにリモート接続し、ネットワークストレージサービスなどにアクセスすることができます。

NetGuard は、SSL VPNサーバとリモートクライアントを繋ぎ、データ伝送のセキュリティとプライバシーを安全に保ちます。

SSL VPN は、ユーザがCitrixまたはVirtual Desktop Infrastructure (VDI) プラットフォームにアクセス可能とし、遠隔の人員がオフィスアプリケーションやオペレーティングシステムを使用できるようにします。

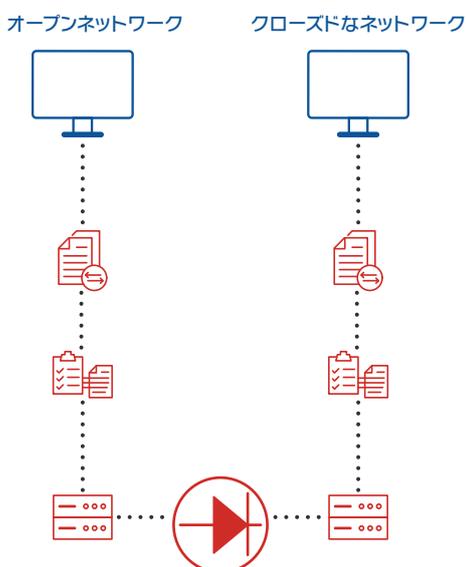


Data Diode System データダイオードシステム

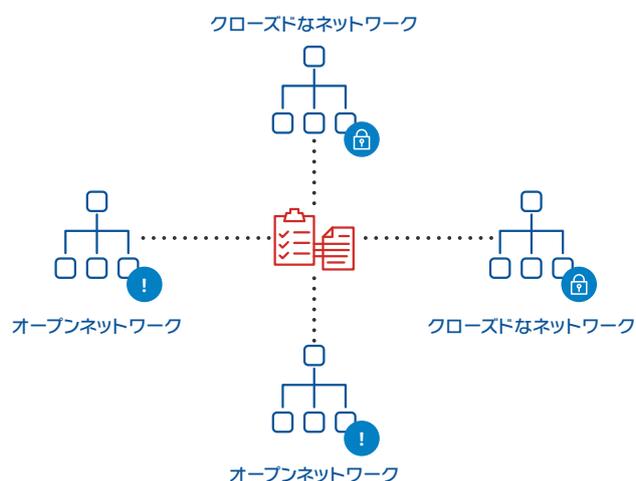
ネットワーク間のエアギャップを埋めて安全に

エアギャップセキュリティネットワークは、セキュリティ保護されたネットワークとセキュリティ保護されていないネットワークを厳密に分離する必要がある組織に向けています。SecureAge Technologyは、これらのオープン（セキュリティ保護されていない）ネットワークと、クローズド（セキュリティ保護されている）ネットワーク間でデータを安全に移動するため、どんな組織にも素早く展開できるデータダイオードシステムを開発しました。

シングルクローズド&
オープンネットワーク構成



複数のクローズド&
オープンネットワーク構成



Closed Network System コアコンポーネント



File Transfer System (FTS)

複数のネットワーク間で、安全かつ簡単にファイルの転送を行えます。Windows ログイン(シングルサインオン)認証、またはローカル認証による専用アカウントを使用して、簡単にアクセスできます。



Data Diode Proxy

SecureAgeで開発されたソフトウェアをインストールしたハードウェアでは、エアギャップのあるネットワークへデータの完全な信頼性を保ったまま一方通信が行えます。



Information Broker (IB)

スマートで安全な相互通信ができるデータダイオードにより、データ転送時でも、データを暗号化し完全な機密性を確保します。IBは、データダイオードのハードウェアエラーのために正常に転送されなかったデータの再送信を可能にし、複数のオープンおよびクローズド・ネットワークのブリッジングも可能にします。

エンドポイント セキュリティソフトウェア

SecureAge の End to End の保護ソリューションは、デスクトップワークステーションでもラップトップコンピュータでも、エンドユーザーの生産性を犠牲にすることなく、セキュリティの強化を実現します。

SecureData

いつでもどこでも
すべてのファイルを暗号化



SecureFile

ミッションクリティカルな
データ用ファイル暗号化と
デジタル署名



SecureDisk

ボリューム暗号化で機密データ
を迅速かつ安全に保管



SecureEmail

ポリシーベースの End-to-End
電子メール暗号化



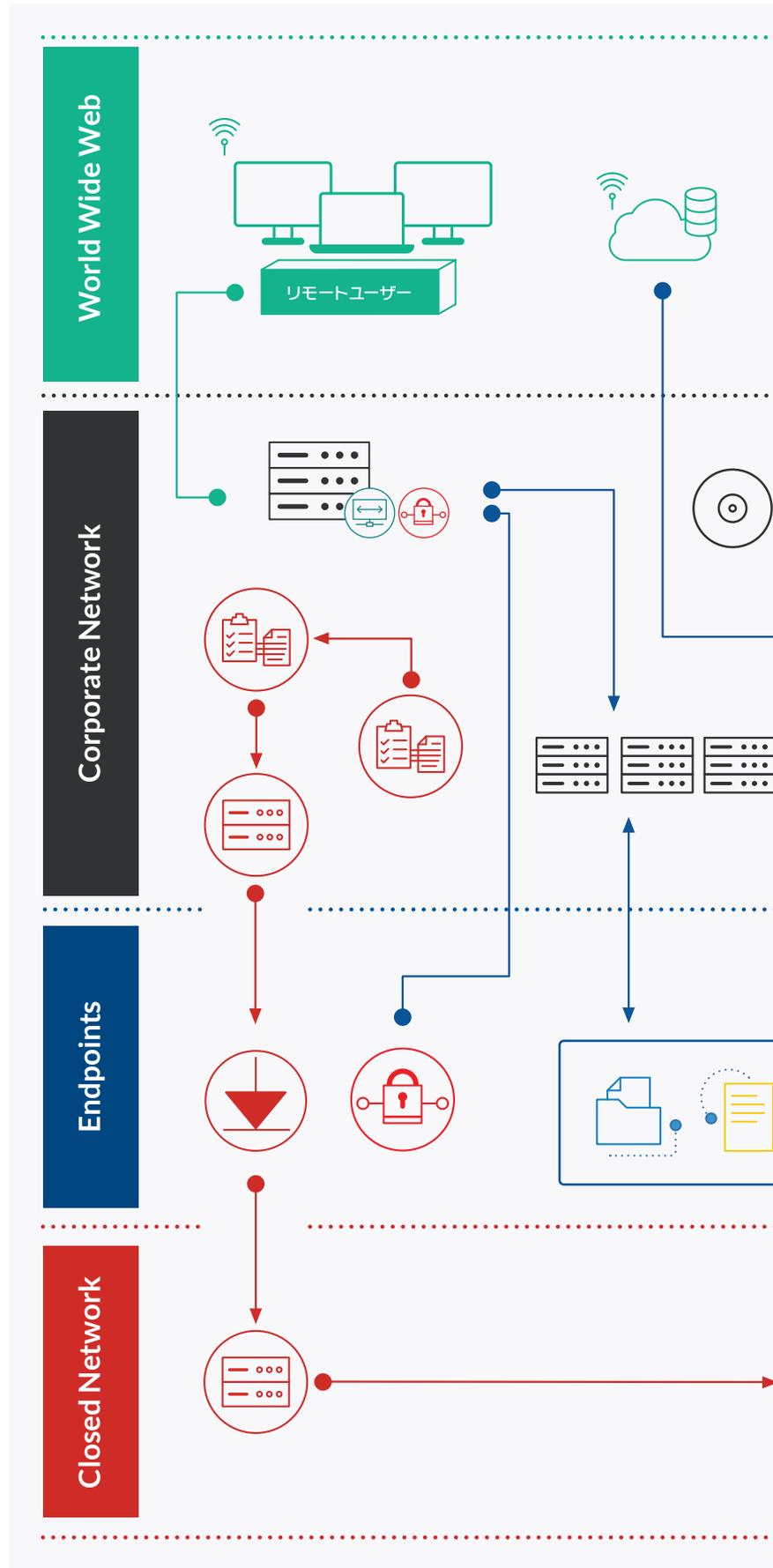
SecureAPlus

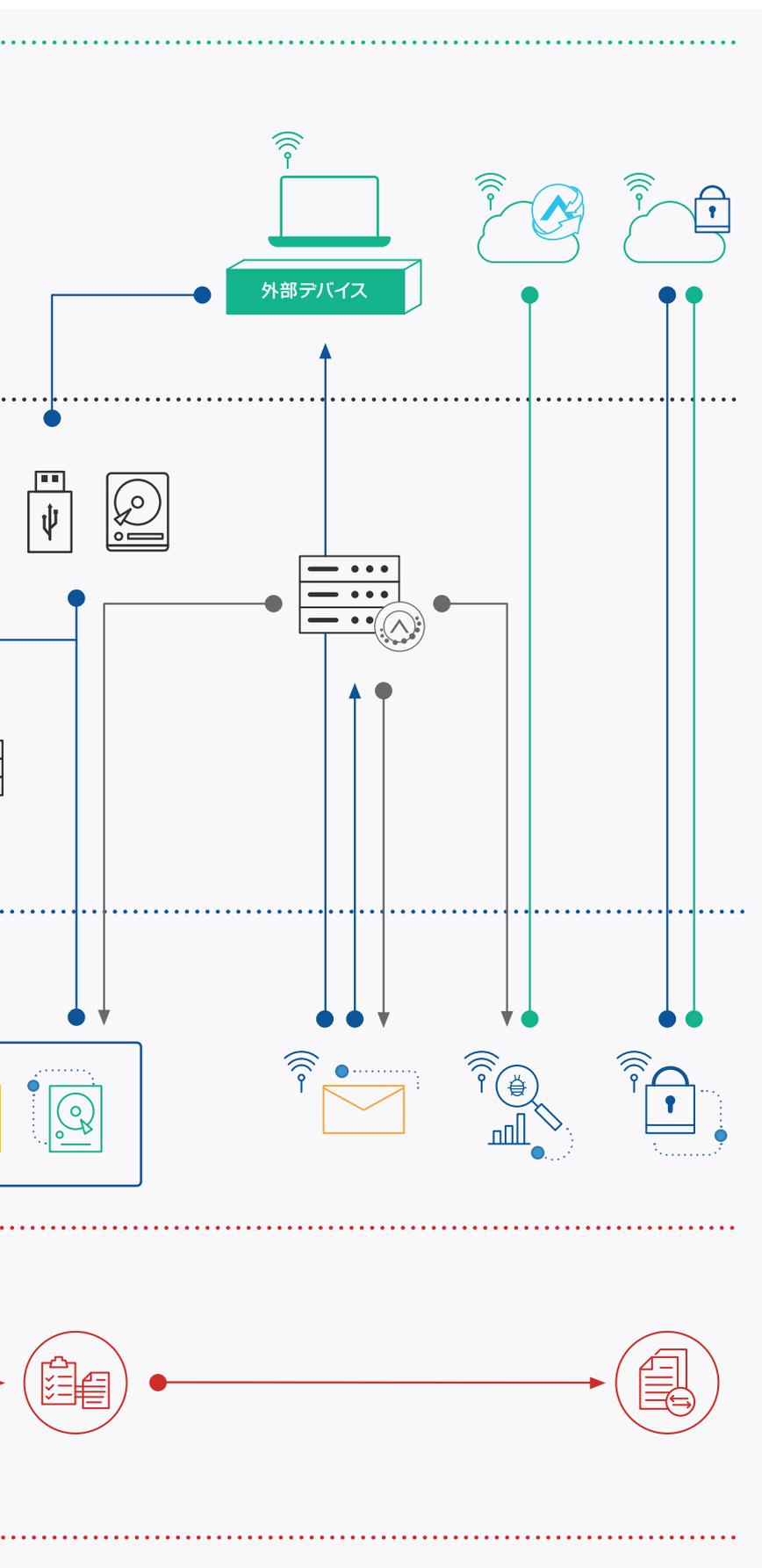
10 以上のクラウド
アンチウイルスとホワイトリスト



LockCube

暗号化された安全クラウド
ストレージ





ハードウェア & ネットワークセキュリティ

当社のネットワークセキュリティソリューションは、ハードウェアにおいても、ITセキュリティチームの負担を最小限に抑え、より厳格なセキュリティを実現するため、フレキシブルな拡張、容易なメンテナンスを提供します。

Security Management Server

大規模なセキュリティ管理をシンプルに



Enterprise SSL VPN

いつでもどこでも
安全に接続



SecureNetguard

Point to Point
ネットワークセキュリティ



Data Diode System for Closed Networks

ネットワーク間のエアギャップを埋めて安全に



File Transfer Software (FTS)

ファイル転送システム



Information Broker (IB)

効率的で暗号化された
ファイル転送管理



Data Diode Proxy

一方向データ伝送





当社のSecureAge代理店は、お客様のニーズに合った最高のセキュリティソリューションについてアドバイスしています。詳細については、または義務デモのスケジュールについては、お問い合わせください：

セキュアエイジ株式会社 ・ 〒105-0001 東京都港区虎ノ門1-16-6 虎ノ門 RAPO-TO ビル UCF 7F

W www.secureage.co.jp C contact us