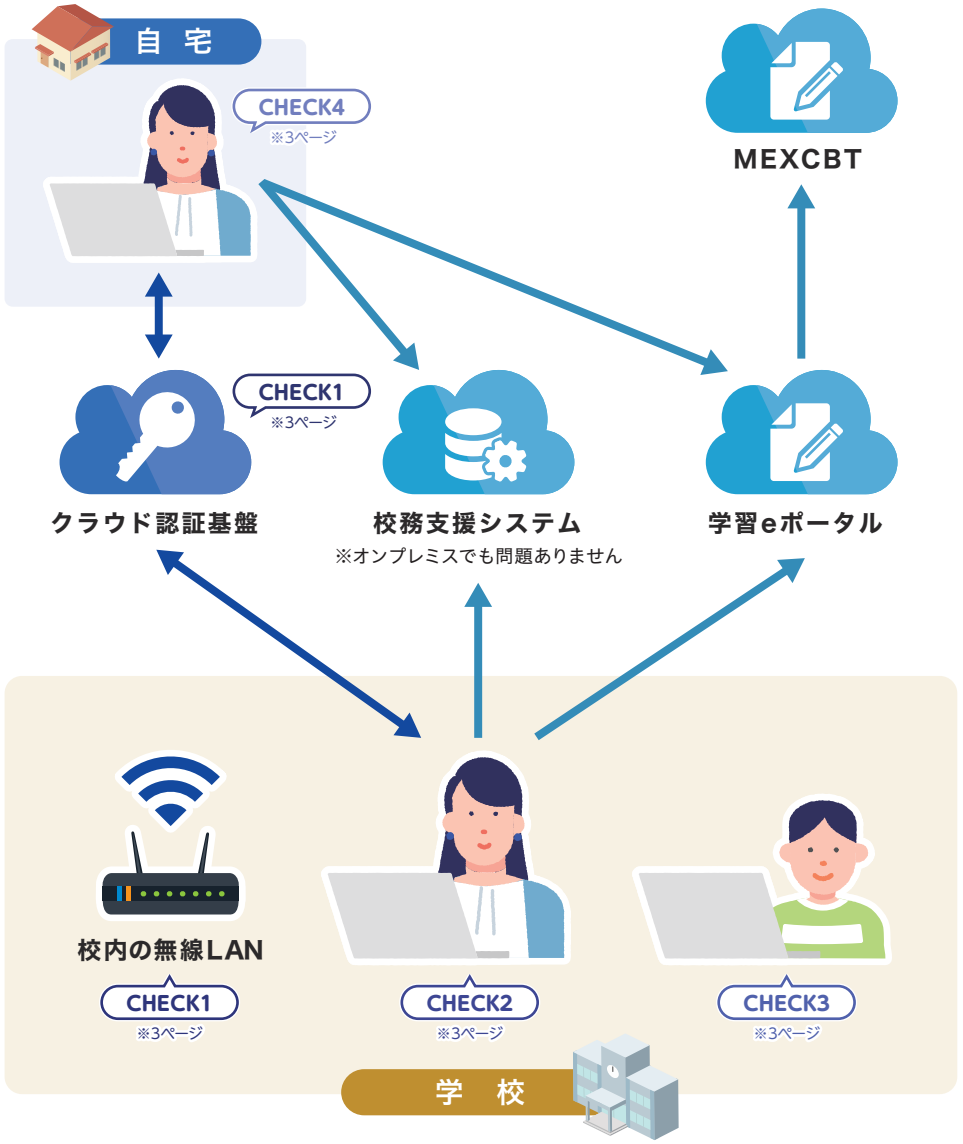
教育情報セキュリティ
ソリューション

校務DXへの備え

Soliton®

教育情報セキュリティチェック①

アクセス認証型（ゼロトラスト）



CHECK1 クラウド認証基盤/無線LAN認証

- クラウドになりすましでアクセスされないように認証を強化したい
- クラウドへのログイン認証が ID/ パスワードのみで不安を感じている

8ページへ

CHECK2 校務端末セキュリティ

- 確実な本人認証を行いたい
- 離席時に自動で画面ロックをかけて、不正利用を防ぎたい

9ページへ

CHECK3 学習端末のフィルタリング

- 不適切 Web サイトへのアクセスを禁止してから、持ち帰り学習を始めたい
- 夜遅くに映像コンテンツを見れないように制限したい

14ページへ

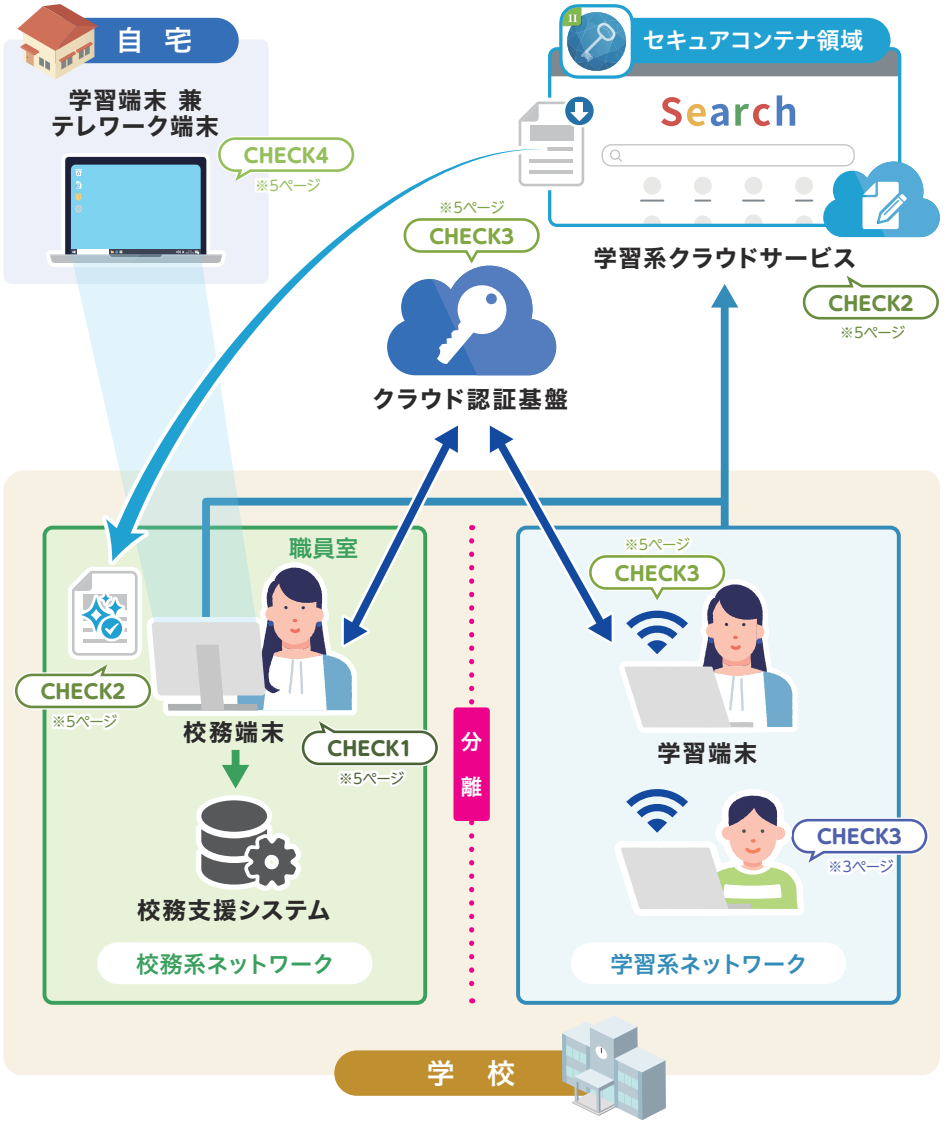
CHECK4 教員のテレワーク

- ロケーションフリーで業務をしたい
- 端末にデータを保存したまま、持ち出すことに不安を感じている

10,12ページへ

教育情報セキュリティチェック②

ゼロトラストを意識した境界防御型



CHECK1 校務端末セキュリティ

- ゼロトラストに向けて、端末ログイン時に多要素認証を行いたい
- 教育委員会の導入実績が多いソリューションだと安心する

9ページへ

CHECK2 校務端末のインターネット閲覧/ファイル取込

- 校務端末から安全にインターネット閲覧したい
- ファイルの安全性を確認してから、校務端末に取り込みたい

10,11ページへ

CHECK3 クラウド認証基盤/無線LAN認証

- クラウドシフトを考えると、ID/ パスワードの管理が課題
- クラウドの利用時、多要素認証とシングルサインオンを必須化したい

8ページへ

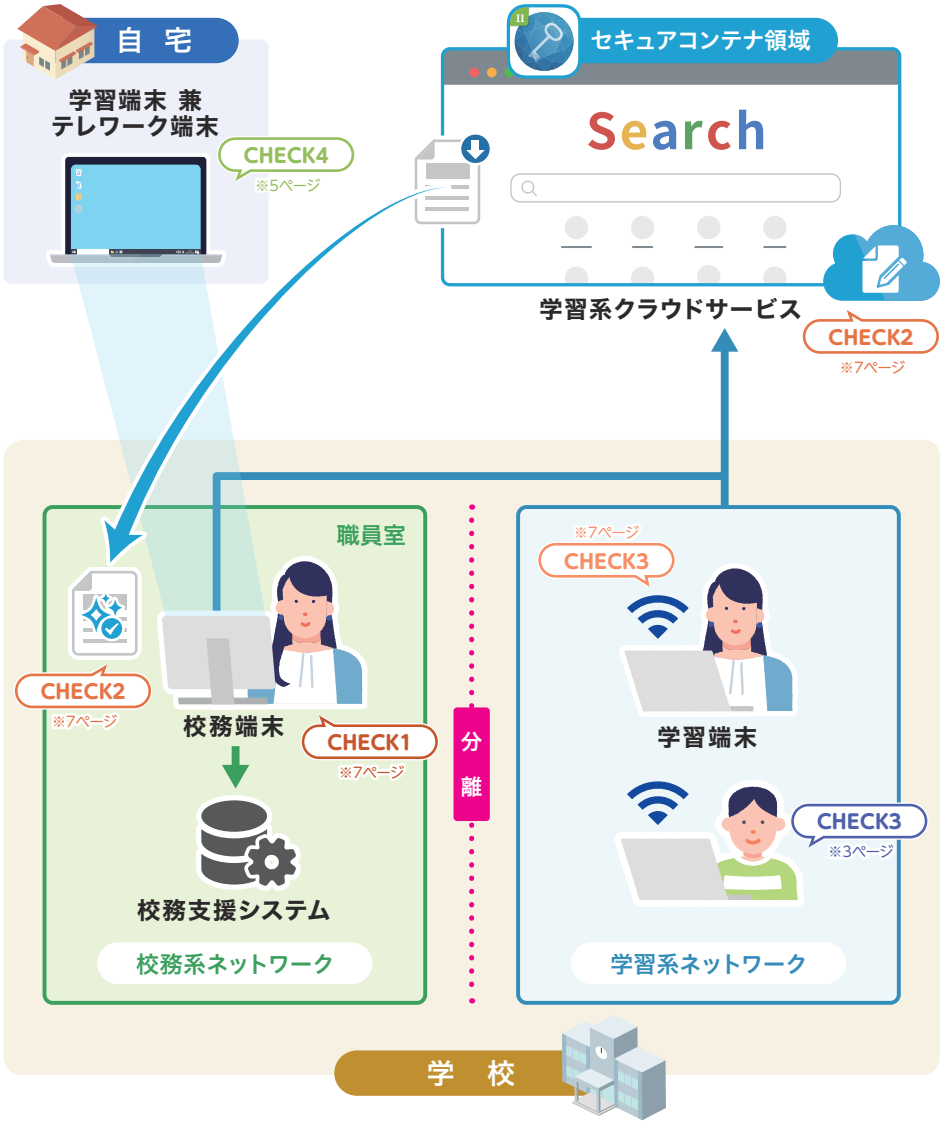
CHECK4 教員のテレワーク

- いつもの操作感でテレワークをしたい
- でも、端末にはデータを残したくない

12,13ページへ

教育情報セキュリティチェック③

境界防御型



CHECK1 校務端末セキュリティ

- 校務端末になりすましでログインされるのを防ぎたい
- 利便性を高めるためにシングルサインオンしたい

9ページへ

CHECK2 校務端末のインターネット閲覧/ファイル取込

- 校務端末から安全にインターネットを閲覧したい
- インターネットからダウンロードしたファイルを安全に編集したい

10,11,12ページへ

CHECK3 校内無線LAN環境

- 持ち込み端末の無線 LAN 接続を制限したい
- 授業をスムーズに進めるためにもネットワークを安定させたい

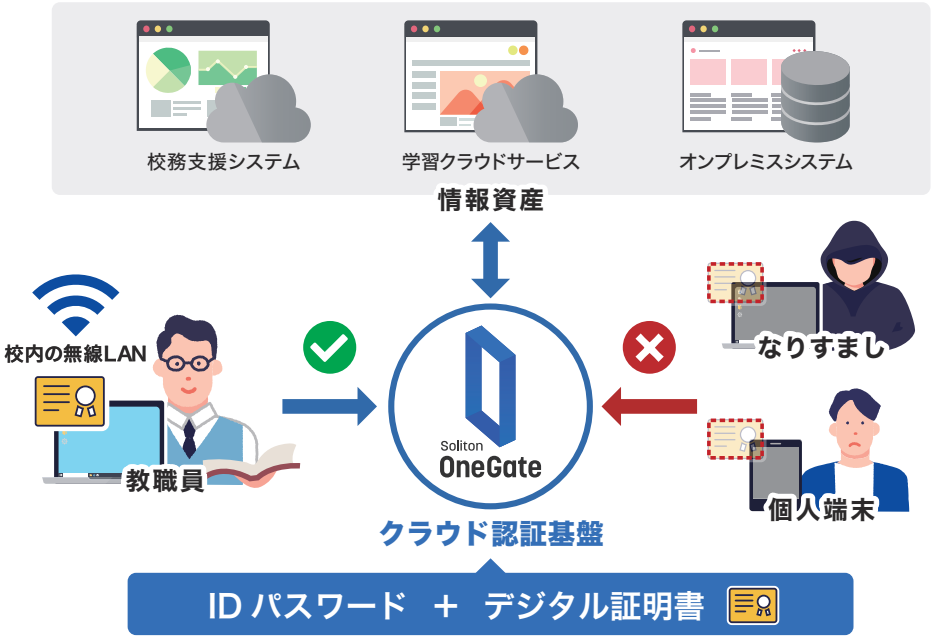
15ページへ

次ページより
ソリューションのご紹介をします

アクセス認証型　ゼロトラ意識

デジタル証明書で守る情報資産への不正アクセス対策

Soliton OneGate



認証情報を一元管理

認証基盤となる OneGate を経由してアプリケーションへアクセスします。ID パスワードとデジタル証明書を組み合わせた多要素認証により、なりすましを防ぎます。

シングルサインオン

OneGate の認証成功後、クラウドサービスに対して SAML 連携またはパスワード代行入力によりシングルサインオンを行います。オンプレミスシステムも同様に対応しています。

リスクベース認証

信頼できないネットワークからのアクセスや通常とは異なるアクティビティを検知した際は、認証方式を追加し、アクセスの真正性を確認します。

無線LAN認証

デジタル証明書を活用し無線 LAN 認証を行い、安全なネットワーク接続が可能です。RADIUS サーバーの設置もゼロコンフィグのため手間はかかりません。

アクセス認証型　ゼロトラ意識　境界防御型

多要素認証で守る校務端末のなりすまし対策

SmartOn® ID

なりすまし排除

重要性分類が高い校務系情報を許可された教職員のみが利用できるよう、端末ログイン時にパスワードに加え、生体情報 (顔や指静脈等)、FeliCa 等の IC カードで多要素認証を行います。

マスクあり顔認証

Panasonic CONNECT が提供する顔認証エンジンでは、マスクを装着したまま顔認証することが可能です。色付き・柄あり等のマスクにも対応しています。

離席時に自動ロック

ユーザーが PC から離れた時に自動ロックをします。離席時の覗き見や人の入れ替わりによる不正利用を防止し、セキュリティを向上します。

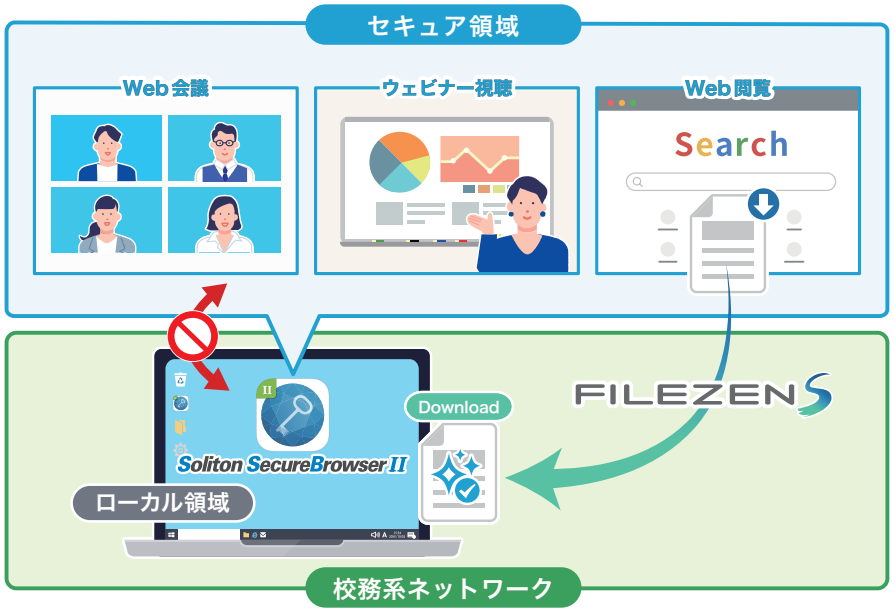
USBメモリ制御

外部デバイスの利用を制限でき、指定した USB のみ利用可能などの設定が可能です。

アクセス認証型　ゼロトラ意識　境界防御型

セキュアな領域で守るインターネット分離対策

Soliton SecureBrowser II
Soliton SecureGateway



セキュアコンテナ方式

端末内に生成したセキュアコンテナ (隔離領域) によって、学習系と校務系のネットワークを端末内で分離します。端末にはデータが残らない仕組みです。

快適なWeb閲覧

端末のリソースを使い、快適な Web 閲覧・専用ビューアーによるファイル閲覧が可能です。操作感は汎用ブラウザと変わりありません。

Web会議も対応

ニューノーマルに必須の Web 会議を安全に実施することが可能です。
動作実績：Teams / Zoom / Webex (ブラウザ版)
※評価推奨

アクセス認証型

校外からのアクセス

校外から情報資産へアクセスする際、セキュアコンテナ内からアクセスすることで、端末にデータが残らない、データを持ち出せない環境をつくることが可能です。

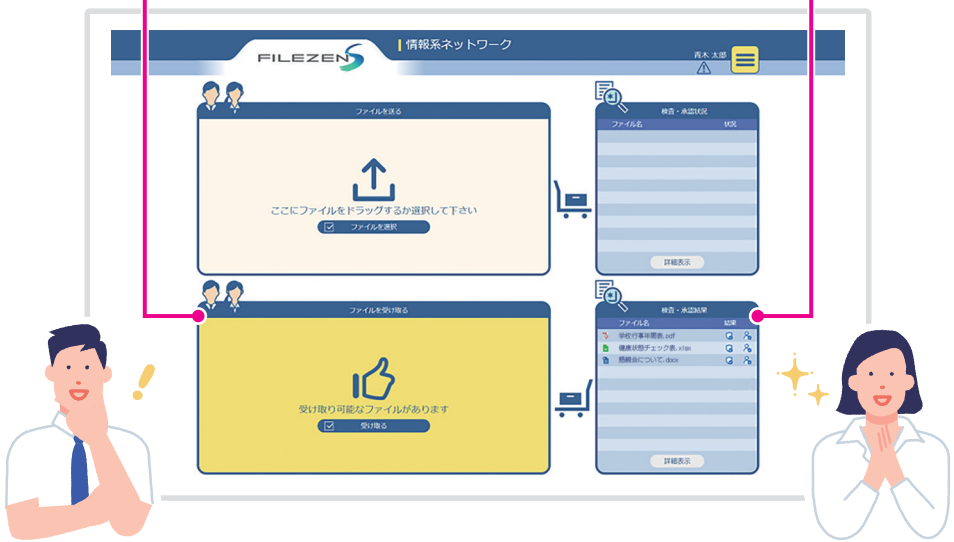
ゼロトラ意識　境界防御型

安全なファイル授受で守るネットワーク分離対策

FILEZEN S

ハイライト表示で操作をナビゲート

無害化や承認状況を可視化



ファイルの授受

Soliton SecureBrowser II との連携により、ダウンロードしたファイルを右クリックで FileZen S へアップロードし、ローカル領域へファイル授受が可能です。ローカル領域から FileZen S へファイルアップロードも可能です。

シンプルで分かりやすい

直観的に操作できる画面設計です。FileZen S にログイン後、受け取るファイルをダウンロードするだけです。手間がかかる操作やメニューはありません。

セキュリティも安心

ファイルのアップロード / ダウンロード等のログを記録・保管します。上長承認機能により、不正ファイル持出を防止することも可能です。

無害化製品 連携

世界的実績があるファイル無害化製品 OPSWAT と連携が可能です。パスワード付きの zip や Office ファイルにも対応しています。

アクセス認証型

セキュアコンテナで守る テレワークの情報漏洩対策

WrappingBox

校外からWeb閲覧のみ
Soliton SecureBrowser II

無害化連携
FILEZEN S

校内ファイルサーバー連携
Soliton SecureFile

セキュアコンテナ方式

端末内に生成したセキュアコンテナ (隔離領域) にて Web 閲覧の他、アプリケーションを安全に動かすことが可能です。セキュアコンテナ内のデータは持ち出しすることはできません。

ゼロトラ意識　境界防御型

リモートデスクトップ接続

Windows リモートデスクトップの操作ではデータの持ち出しができてしまいますが、WrappingBox 上で起動するとセキュアコンテナ領域で操作することになり、データの持ち出しができません。

ファイル編集

校務支援システム等からダウンロードしたファイルはセキュアコンテナ内で編集が可能です。Word/Excel/PowerPoint の動作を確認済です。事前に指定した校内ファイルサーバーへ保存します。

アクセス認証型

校外からのアクセス

校外からアプリケーションへアクセス、ファイル編集する際は WrappingBox のセキュアコンテナ内からアクセスすることで、情報漏洩対策をすることが可能です。

境界防御型

画面転送方式で守る 端末内データの情報漏洩対策

Soliton SecureDesktop

画面転送方式

画面転送方式のため端末にデータが残らず、情報漏洩対策が可能です。オンプレミス版、クラウドサービス版があります。

使いやすい操作感

タイムラグがなく、直観的に操作が可能です。普段使い慣れた自分の職員室 PC へのリモートデスクトップ操作をするので、慣れない職員でも扱いやすいことが評価されています。

データセンターは国内

日本国内のデータセンターにて運用しています。SLA 完備のため安心して利用可能です。また、国際規格 ISO/IEC27001・ISO/IEC27017 を取得済です。

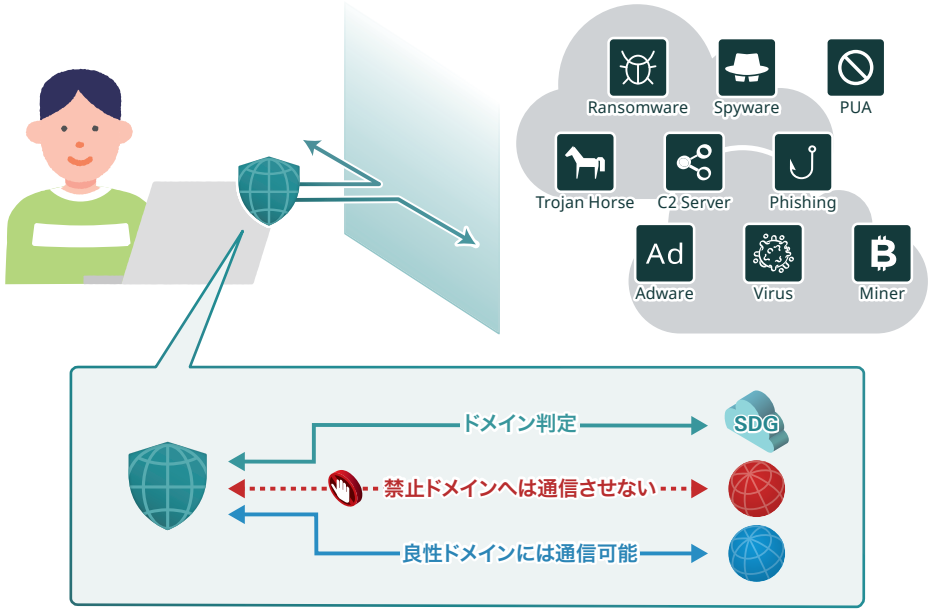
デジタル証明書認証

職員室 PC に接続できる端末は、デジタル証明書がインストールされている端末のみに限定し、アクセスを制御します。多要素認証によってセキュリティを強化します。

アクセス認証型　ゼロトラ意識　境界防御型

DNSフィルタで守る端末の脅威対策

Soliton DNS Guard for Education



有害サイトをブロック

端末にインストールしたソフトウェア (Agent) とクラウド上のサービスが通信を行います。名前解決が発生する前に脅威ドメイン情報によって、通信先の悪性判断を行います。

時間帯制御

端末のインターネット利用時間制限や時間帯ごとのポリシー制御を設定することができます。深夜の利用を制限する等、現場のニーズにお応えします。

ローカルブレイクアウト

プロキシ等のネットワーク機器がボトルネックになるケースが増えています。DNS フィルタ型は端末とWeb サーバ間で直接通信するため、パフォーマンス劣化することなく利用可能です。

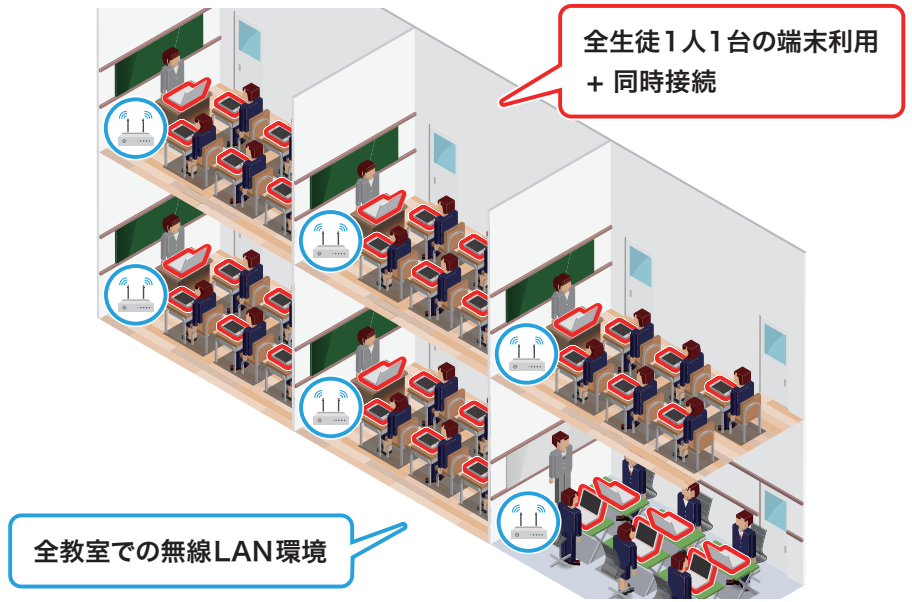
マルチOS対応

Soliton DNS Guard Agent は以下 OS に対応しています。
Windows/ChromeOS/iOS/iPadOS/macOS/Android

境界防御型

デジタル証明書で守る無線LANの不正アクセス対策

NetAttest EPS / NetAttest D3



デジタル証明書認証

ネットワーク認証専用アプライアンス NetAttest EPS より発行したデジタル証明書を許可端末にインストールし、不許可端末からのアクセスを制御します。

Chromebook対応

Windows/iPad の他、Chromebook に対してもデジタル証明書を利用することが可能です。オンライン経由で安全に配布し、システム管理者の負荷を極力削減します。

国産アプライアンス

Web 管理ページや製品マニュアル、コンタクトセンターからのご案内などは全て日本語であり、安心してお使いいただけます。

ネットワークの安定化

DHCP 専用アプライアンス NetAttest D3 により、高速 IP 払い出しを行います。授業をとめないネットワーク環境を実現します。

導入事例

瀬戸内市教育委員会

導入製品

SmartOn® ID（顔認証）

Soliton SecureBrowser II

FileZen

Soliton SecureDesktop

NetAttest EPS

備前市教育委員会

導入製品

SmartOn® ID（顔認証）

Soliton SecureBrowser II

FileZen

NetAttest EPS

滋賀大学

導入製品

SmartOn® ID

（マイナンバーカード認証）

導入実績

Soliton® 教育ソリューションページ

https://www.soliton.co.jp/lp/education/

ED-2304A