「ガーディアンズ」システムの全体像 Open the World with Your Authentication!

「鍵姫」と「ガーディアンズ」との連携で、「安心」「安全」「公平」な IoT の環境を

スマートフォン

「鍵姫（KAGIHIME)」

Windowsシステム

「ガーディアン プラス」

TBMi AS/400

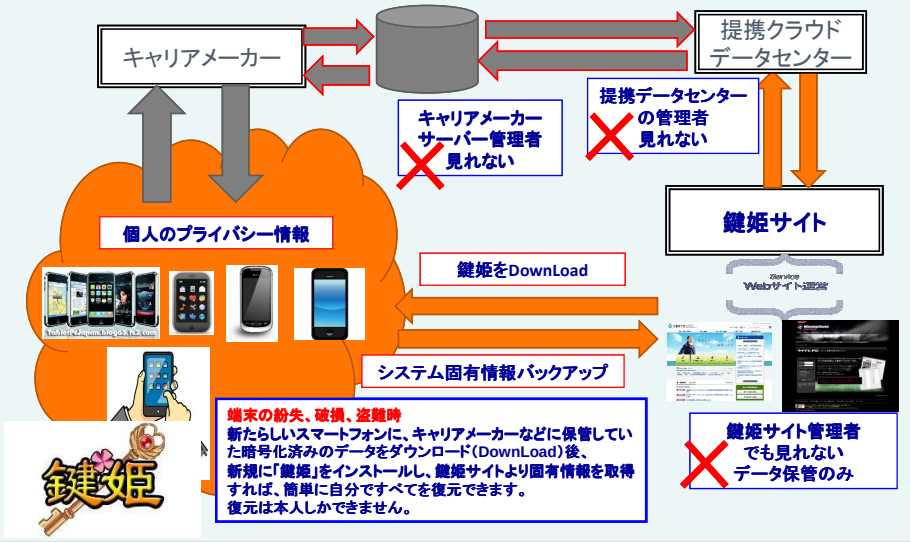
Power's Lock

世界を席巻している「RSA」の成りすましに弱いという欠点を乗り越える
「スーパーガーディアン」の特許技術が土台となり支えます。

スマートフォンでのＷＥＢセキュリティ

１４_４．モバイルセキュリティへの応用 Open the World with Your Authentication!
Kagihime エクスプローラー・連絡帳・ビジネスライン

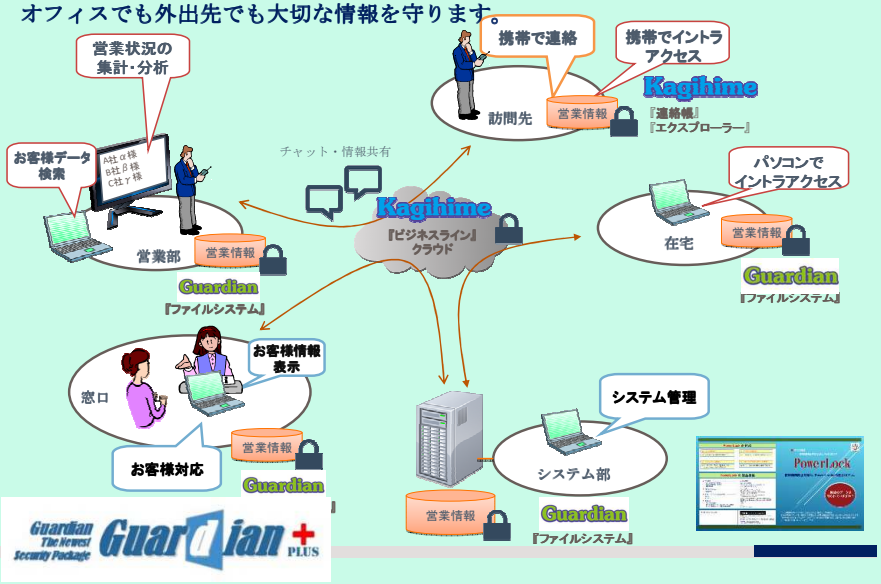
完全に個人のプライバシー情報は他者からの遮断され、万一、ハックされても個人情報や社内の機密は漏洩しない。



ＯＦＦＩＣＥ内でのセキュリティ

１６．オフィスのトータルセキュリティ Open the World with Your Authentication!

オフィスでも外出先でも大切な情報を守ります。



「ガーディアンズ」システムの機能

Open the World with Your Authentication!

「鍵姫」と「ガーディアン プラス」の連携で、真の情報保護施策を実現します

システム管理者のオールマイティな権限から、情報の中身を見る権限を切り離す必要性は理解しても既存システムが追いつかないという場合でも、大丈夫です。

情報データそのものに着目して、誰に見られて良いかの付加情報を加え、しかも正しいユーザーである認証情報などの二重三重の分権方式による暗号化セキュリティならば、極論すれば、アクセス管理もいらない、いつでも・どこでも・誰でもが、ご自分の権限に基づく利用が出来ます、システムとして自動で検証されるシステムとなります。

スマートフォンでのＷＥＢセキュリティ

ハッカーなど不正アクセス

ユーザーであり管理者

サイト管理者

アタック

固有情報などによる暗号化された固体情報や鍵情報や緊急時の登録情報のみ存在

暗号化された緊急時の復元情報の一部情報

保管のみ

（ユーザー特定情報）

メールアドレス
設定パスワード情報

管理のみ

メールアドレス
登録パスワード情報
の暗号化された情報

万一、メールアドレス登録パスワードが成りすまされて、サイトからの復元情報の一部情報が誤送されても、本人以外は復元できません。

ＯＦＦＩＣＥ内でのセキュリティ

サーバー管理者

システム鍵の設定

端末管理者の指定

端末管理者

ユーザーの指定

パブリックフォルダの設定

ユーザー

プライベート鍵の設定

セキュリティフォルダの設定

運用

Guardian The Newest Security Package Guardian PLUS

ＩｏＴでのセキュリティ製品の要件

Open the World with Your Authentication!

1．内部者への対策を装備
2．不正アクセス発生後の対策を装備
3．情報漏洩への抜本的な対策を装備

鍵姫

Guardian The Newest Security Package Guardian+ PLUS

こんな大事な情報をメーカーやクラウドに預けて「大丈夫？」との不安や疑念！

こんな思いにとらわれることなく、ユーザーの方々が、境界のない自身のプライバシー情報（写真などのさまざまな個人や社内の重要機密事項）を便利な機器に託せるようになるメリットがあります。

個人のプライベートな情報を、たとえ、機器を提供したメーカーやシステムを提供したメーカーから勝手に見られないことで、ユーザーでは絶対タッチのできないメーカーなどのサーバーやクラウドのデータセンターに存在するユーザーのプライバシー情報も、仕組みとして保全される方式です。その仕組みが、結果的に、ハッカーや悪意を持った内部者などからの不正アクセスが万一あったとしても、個人や社内の機密情報の内容は保全される事になります。

セキュリティ製品には、1. USABIRITY（利便性） 2. TRACEABIRITY（追跡性） 3. IDENTIFICATION（識別）による秘匿性を備える必要があります。
従来のセキュリティ製品は、アクセス管理がしっかりしているという前提で、内部者は悪さをしないという性善説にのっとり、1. の利便性（ICカード、指紋、静脈などのバイオメトリクス）、さらには万一不正アクセスが発生した後に備えとしての
2. の追跡性（ログシステム）が重視されてきました。しかし、最近の情報漏洩は、このアクセス管理の不備をつくハッキングや、内部者の犯行による事例が目にあまる状態になっていることが明らかになってきました。外部者（ハッカー）による不正アクセスは、従来のアクセス管理の実態がID・パスワードの脆弱性をつかれて侵入を許してきました。また、情報漏洩の大部分を占める内部者の犯行では、システム管理者を筆頭としての内部者が、オールマイティーな権限を有している事に起因しております。
これら既存のセキュリティは、3. IDENTIFICATION（固有な識別による秘匿性）を軽視してきた点ももう一つの起因と言えます。
「ガーディアンズ」のセキュリティは、3. IDENTIFICATIONの本人認証（識別）による秘匿性に着目したシステムで、欧米のセキュリティのアクセス管理とは、一線を画しております。すなわち、システム管理者といえども、ユーザー個人のプライバシー情報の中身を無断でのぞく事ができない為、万一、システム管理者または特定のユーザー個人のID・パスワードがハッキングされ盗まれたとしても、該当のシステム管理者または特定のユーザー個人の情報しかのぞけないというものです。すなわち、人間系の介在を極力回避し、システマチックな認証と連動したセキュリティにしてこそが第3者（内部者やハッカーやウィルス）などの不正アクセスを超えてくる脅威からプライバシーを守り、真の情報保全を実現します。
特に、情報漏洩が発生してしまった後に、ログ等によるTRACEABILITY（追跡性）でたとえ追跡できたとしても、結局は“後の祭り”なのです。
本システムは、不正アクセスが発生した後の対策を備えている仕組みのセキュリティソフトと言えるものです。本システムに装備しているログは、操作記録のみならず、既存のセキュリティのログシステムと異なり、特定の個人が自己の権限を逸脱して、不正アクセスを行おうとして失敗したとの行為記録のログとしての役割を担っております（未然の犯行記録情報）。

IoTの機器では、サーバーもクライアントも関係なく対等に、機器や端末のプライバシーを保全する要件が絶対条件です。
「安心」「安全」「公平」なセキュアな環境を、仕組みとして構築するセキュリティインフラを確立する事が急務と考えます。

製品のご導入やカストマイズなどのお問い合わせは：
サイファーセキュリティ株式会社 ：「ガーディアンズ」の販売会社
info@cyphersecurity.co.jp

技術関連のお問い合わせ：
株式会社コムシーズ ： 「ガーディアンズ」の開発サポート会社
infom@comseeds.com