

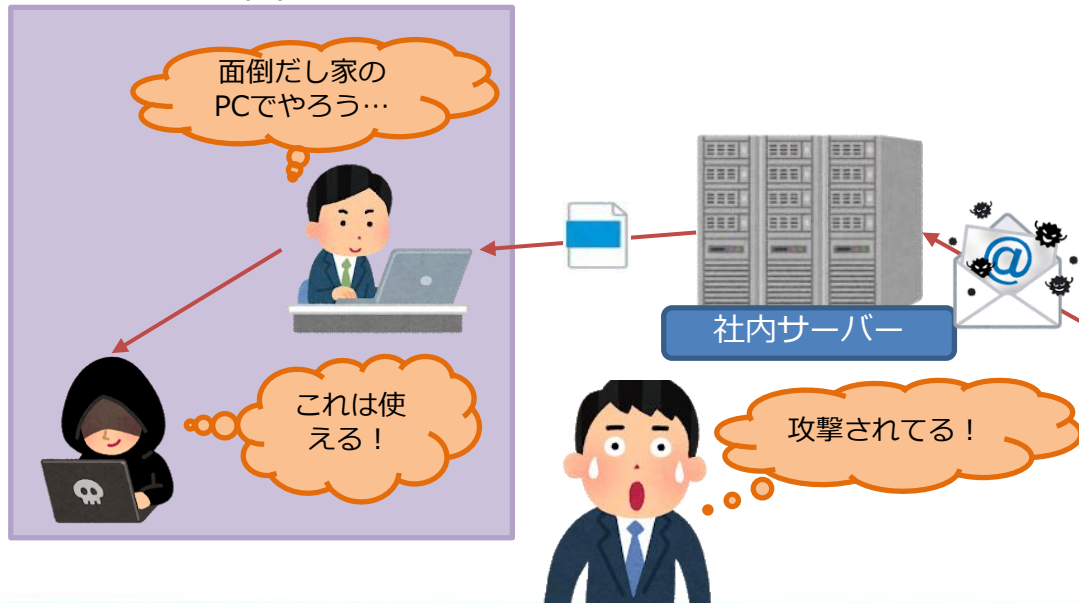
金融業のお客様必見！

**今さら聞けないゼロトラストとは？
今からでも大丈夫！
すぐにできるゼロトラスト実現の仕組み**

そのセキュリティ対策で本当に大丈夫？

企業や自治体が外部からの攻撃や内部不正により、重要情報が漏洩してしまうインシデントが相次いでいます。背景としてテレワークの急速な普及により、既存のセキュリティ対策（「境界防御モデル」ともいわれます）では、対応が困難になっていることが考えられます。そこで、近年注目を集め、重要となってくるのが『ゼロトラストモデル』と呼ばれるセキュリティの考え方です。

内部不正



外部からの攻撃



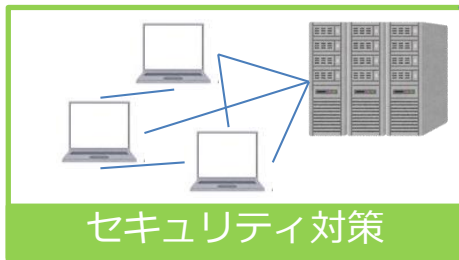
近年注目を集めるゼロトラストとは？

ゼロトラストとは？

『ゼロトラスト』とは『ゼロ』『信頼/信用』とある通り、すべてのアクセスを信用しないセキュリティの考え方です。従来のセキュリティは、外部からの攻撃には意識的な対策をしていましたが、ゼロトラストは内外の境目が存在しないとしたうえで、すべてのアクセスが信用できないものであると仮定しセキュリティを構築します。

従来のセキュリティ

社内ネットワーク

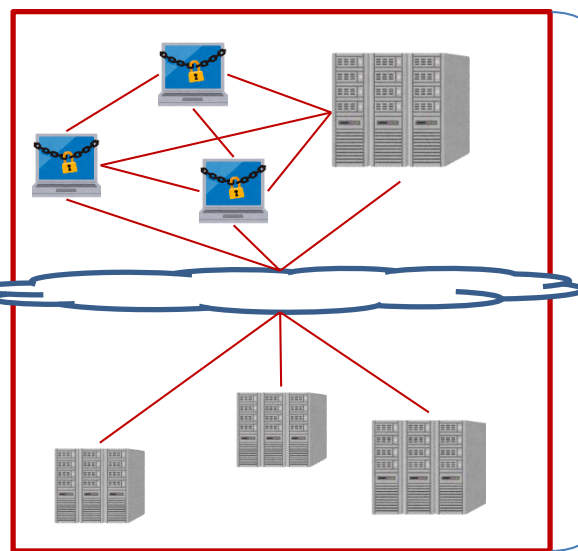


社外ネットワーク



ゼロトラスト

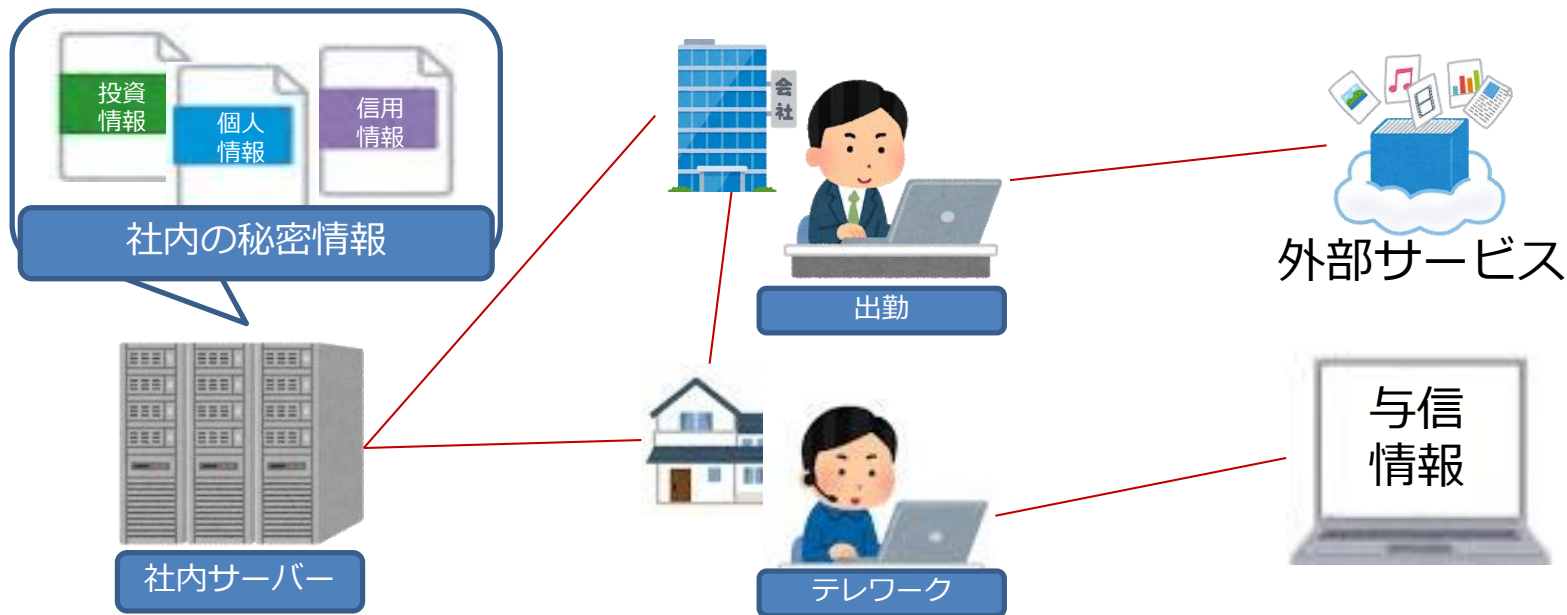
社内ネットワーク



なぜゼロトラストが注目されるのでしょうか？

どうして注目されるの？

様々なクラウドサービスの利用増加やテレワークの普及に伴い、従来とは比べ物にならない程ネットワークの内外を区別することや、それに応じたセキュリティ対策が困難になってきました。したがって保有する個人情報や信用情報など、今まで以上に慎重な管理が必要です。



ではゼロトラスト実現のためにはどのような仕組みが必要なのでしょうか？

ゼロトラスト実現に必要なのは『情報を暗号化すること』『適切に情報を管理すること』です。暗号化技術をIRM（Information Rights Management）といい、指定された相手のみ情報を閲覧・編集可能にします。また、暗号化された情報が適切に扱われているかの管理が正しくできなければ、備えが十分であるとは言えません。正しい範囲で情報が取り扱われているかが常にモニタリング可能な仕組みを構築することが重要です。



暗号化と情報管理を実現するツールはこちら！

FinalCodeはゼロトラスト実現に必要な『情報を暗号化すること』『適切に情報を管理すること』だけでなく『あとから消す』ことも可能であるため、一歩踏み込んだより強固なゼロトラスト実現を支援します。



守る

高度なIRMで指定した人・権限のみ操作可能。
作成された瞬間に守る運用も可能。



- パスワードレス
- 閲覧者指定
- 期間・回数指定
- 印刷・編集制御
- 不正時自動削除
- 印刷・画面透かし設定



追跡する

ファイルが手元を離れたあとも、アクセスログで追跡することが可能。

- アクセスログ確認
- 不正閲覧検知
- 操作ログ確認

日時	ファイル名	接続元IPアドレス	操作
2018/03/08 10:00:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:05:00	機密ドキュメント.pdf	192.168.1.100	ダウンロード
2018/03/08 10:10:00	機密ドキュメント.pdf	192.168.1.100	印刷
2018/03/08 10:15:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:20:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:25:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:30:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:35:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:40:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:45:00	機密ドキュメント.pdf	192.168.1.100	閲覧
2018/03/08 10:50:00	機密ドキュメント.pdf	192.168.1.100	閲覧

いつ どのファイルに 誰が 何をした



“あとから”消せる

渡したファイルを“あとから”削除することが可能。

- リモートファイル削除
- リモート権限変更



■ 暗号化によるゼロトラスト基盤構築
適切な権限設定で必要な相手にのみ情報を共有し、不正なアクセスからデータを防衛。

■ 情報管理による運営の最適化
展開した情報が適切に扱われているか、モニタリング可能な環境を提供。

■ コンプライアンス強化
万一情報が漏洩しても中身を見せないだけでなく、遠隔消去でリスク低減。

詳しくはこちら

FinalCode



デジタルアーツ株式会社

〒100-0004 東京都千代田区大手町1-5-1 大手町ファーストスクエア ウェストタワー14F Tel 03-5220-1110 Fax 03-5220-1130

製品に関するお問い合わせ：Tel **03-5220-3090**【受付時間】平日9:00～18:00（土、日、祝日、弊社指定休業日を除く） E-Mail sales-info@daj.co.jp URL www.daj.jp

■本書は、2021年1月現在の情報を基に作成されています。最新の情報は弊社Webサイトをご参照ください。■Active Directory、Internet Explorer、Microsoft Edge、Microsoft 365およびWindowsは、Microsoft Corporationの登録商標または商標です。Android、GmailおよびGoogle Chromeは、Google LLCの登録商標または商標です。IOSは、Apple Inc.のオペレーティング・システムの名称です。IOSは、Cisco Systems, Inc.の登録商標または商標です。 デジタルアーツ、DIGITAL ARTS、i-FILTER、info board、Active Rating System、D-SPA、NET FILTER、SP-Cache、White Web、ZBRAIN、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER File Scan、Mail Detox、FinalCode、DigitalArts@Cloud、Desk@Cloud、DアラートおよびDコンテンツその他の弊社・弊社製品関連の各種名称・ロゴ・アイコン・デザイン等はデジタルアーツ株式会社の登録商標または商標です。 その他、本書に記載されている各社の社名、製品名、サービス名およびロゴ等は、各社の登録商標または商標です。■本書に記載されている製品の各種ライセンスの定義およびライセンス別の価格については、各製品の価格表をご参照ください。■本書に掲載されている画面および画面設定例は、解説のためのイメージ図であり、実際の画面とは異なる場合がございます。■本書に記載の内容は変更される場合があります。予めご了承ください。■見やすく読みまちがえにくいユニバーサルデザインフォントを採用しています。

2021/1 DD-00000-000