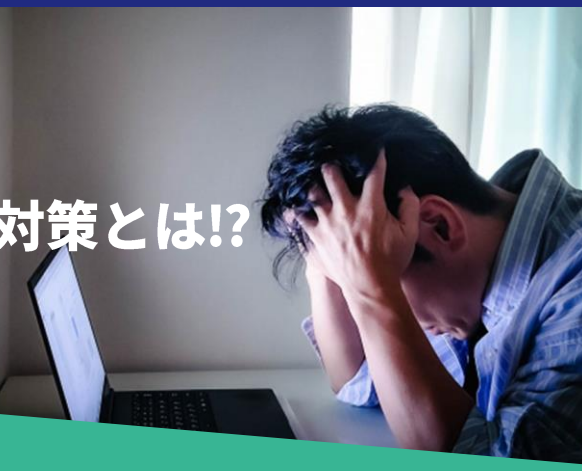
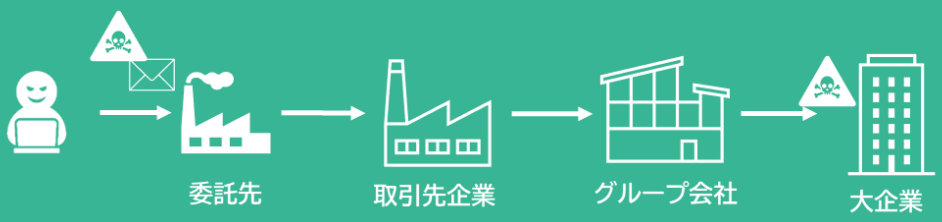
二要素認証・柔軟なアクセス制御でネットワーク内部で起きるリスクを防止　UserLock

企業規模にかかわらず、標的にされる「サプライチェーン攻撃」の対策とは!?



サプライチェーン攻撃とは・・・

商品の企画・開発から、調達、製造、物流、販売までのプロセスと、これに関わる企業で構成されるサプライチェーンには大企業だけでなく、取引先の中小企業も含まれます。



サプライチェーン攻撃とは、セキュリティレベルが高く、侵入が困難な大企業は直接狙わず、セキュリティ対策が手薄な取引先企業を経由した不正アクセスにより、機密情報の搾取や身代金要求を行います。セキュリティ対策にコストをかけることが難しい中小企業が主な最初のターゲットになっているのが特徴です。

サプライチェーン攻撃がもし起こったら・・・

■サプライチェーン内の工場の稼働停止、業務停止
■機密情報流出による損害賠償
■多額の身代金支払いによる企業倒産
■信頼関係の低下による取引先との取引停止

サプライチェーン攻撃の主な手法

取引先の企業への不正アクセスの後、なりすましから**ランサムウェア**に感染させる、といったケースが多く発生しています。サプライチェーン全体で**不正アクセス、なりすまし対策**が重要です。

UTMやエンドポイントセキュリティなどの外部からの攻撃を守る対策は多くの企業様で進めていますが、**ゼロトラスト**の時代、ネットワークの**内部を守る対策**の重要性が高まっています。

ネットワークの 外部 を守る
UTM＋エンドポイントセキュリティ

- ✓ファイアウォール
- ✓ウィルス対策
- ✓ウェブフィルタリング
- ✓IDS/IPS

＋

ネットワークの 内部 を守る
ログイン管理ツール「UserLock」

- ✓内部不正対策
- ✓なりすまし対策
- ✓ログイン管理
- ✓二要素認証

UserLock製品情報はこちら → https://www.isdecisions.jp/userlock

UserLock® Windows Active Directoryと連携するログイン管理ツール

【さまざまな条件でのアクセス制御を実現】

◎ 同時ログイン制御（複数人による同一ID利用禁止）
◎ 接続元（端末・IPアドレス・組織・国）
◎ 接続種類（社内外・ローカル・RDPなど）
◎ 時間（曜日・時間帯・接続時間）

二要素認証＋同時ログイン制御によるなりすまし対策

不正アクセスからの ラテラルムーブメントの脅威

社員のアカウントになりすましながら、より権限が大きいアカウントを狙うためIDとパスワードだけのログイン管理ではリスクが高い

→

二要素認証＋同時ログイン制御でなりすまし対策

本人確認以外のログインを防止するだけでなく、従業員のアカウントの使いまわしなどのリスクを防止

踏み台サーバーを運用したシステムのセキュリティ強化

サプライチェーンの共有ネットワークやサーバーへのログインリスク

共有ネットワークの踏み台サーバーを経由して企業ネットワーク内に不正ログインされてしまう可能性がある

→

二要素認証＋アクセス可視化で踏み台サーバー対策

踏み台サーバーだけでなく、接続先のサーバーにもログイン管理を適用でき、アクセス状況をリアルタイムで監視可能

クローズド環境におけるアクセス制御

クローズド環境で原則インターネット接続が許可されていない

AD情報を外に出さないオンプレミス型のアクセス制御システムが必要で、インターネット接続を必要とするIDaaSは対応不可

→

完全オンプレミスでの二要素認証やアクセス制御を実現

高いセキュリティレベルが求められるクローズド環境でもADだけでは対応できないログイン制御を簡単に実現

参考価格（年間サブスクリプション形式）

※その他レンジの価格や詳細については別途お問い合わせください。

10ライセンス	¥68,700
50ライセンス	¥316,000
100ライセンス	¥550,000

OCEANBRIDGE
株式会社オーシャンブリッジ
〒107-0051 東京都港区元赤坂1-5-12 住友不動産元赤坂ビル7F
Web：https://www.isdecisions.jp/
Mail：userlock@oceanbridge.jp