GlobalSign by GMO

Sier・IT部門向け

サプライチェーン攻撃の脅威
~その対策となる
クライアント証明書とは~

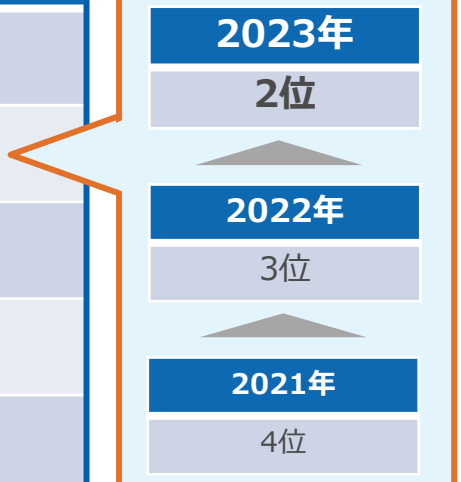
目次

「サプライチェーン攻撃」とは

「サプライチェーン攻撃」とは

攻撃者は大企業へ直接の攻撃が難しいため、セキュリティが比較的手薄な関連企業や取引先企業へ攻撃を行い、その企業を経由してターゲットとなる大企業へ侵入し、大企業の機密情報などを狙うサイバー攻撃を主に指します。

順位	脅威の内容
1位	ランサムウェアによる被害
2位	**サプライチェーンの弱点を悪用した攻撃**
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等のニューノーマルな働き方を狙った攻撃

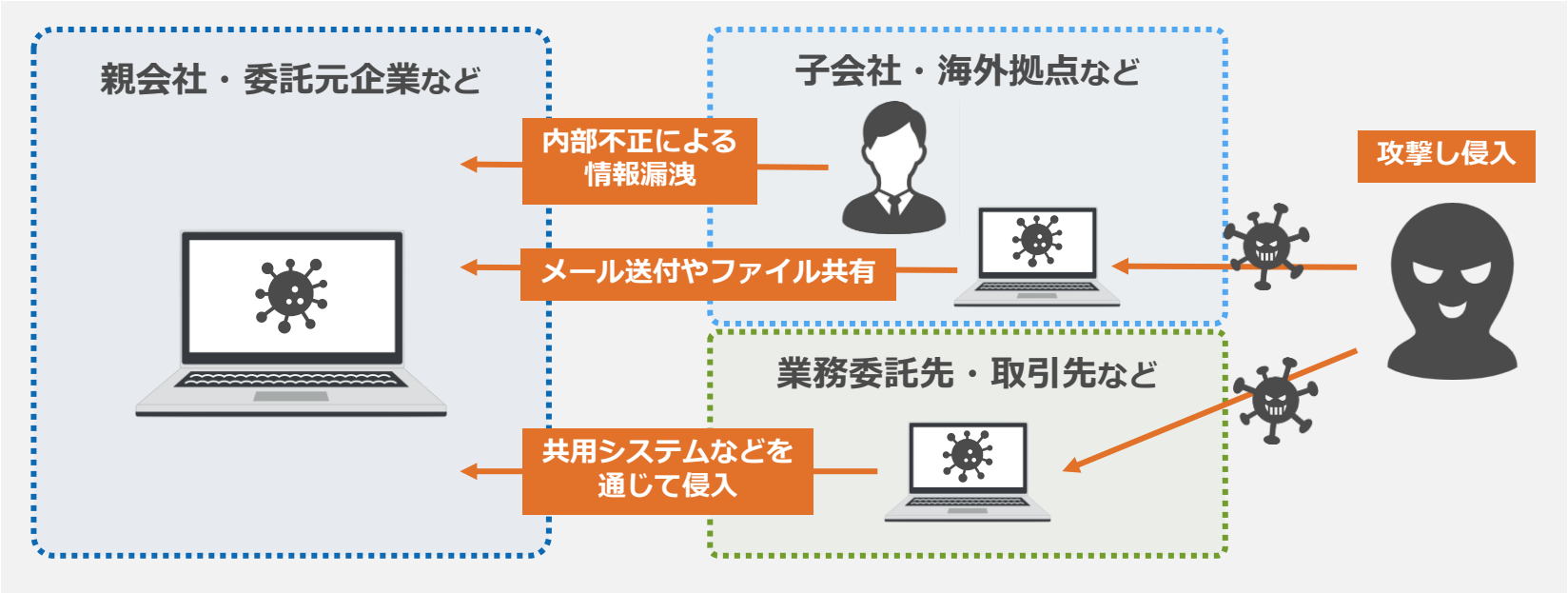


※ 情報処理推進機構：情報セキュリティ10大脅威 2023 を基に作成(https://www.ipa.go.jp/security/10threats/10threats2023.html)

ビジネス（サービス）サプライチェーン攻撃

業務委託先と委託元企業が、一部共通のシステムを利用しているなどの場合に、セキュリティ対策が不足している委託先企業から攻撃者は侵入します。

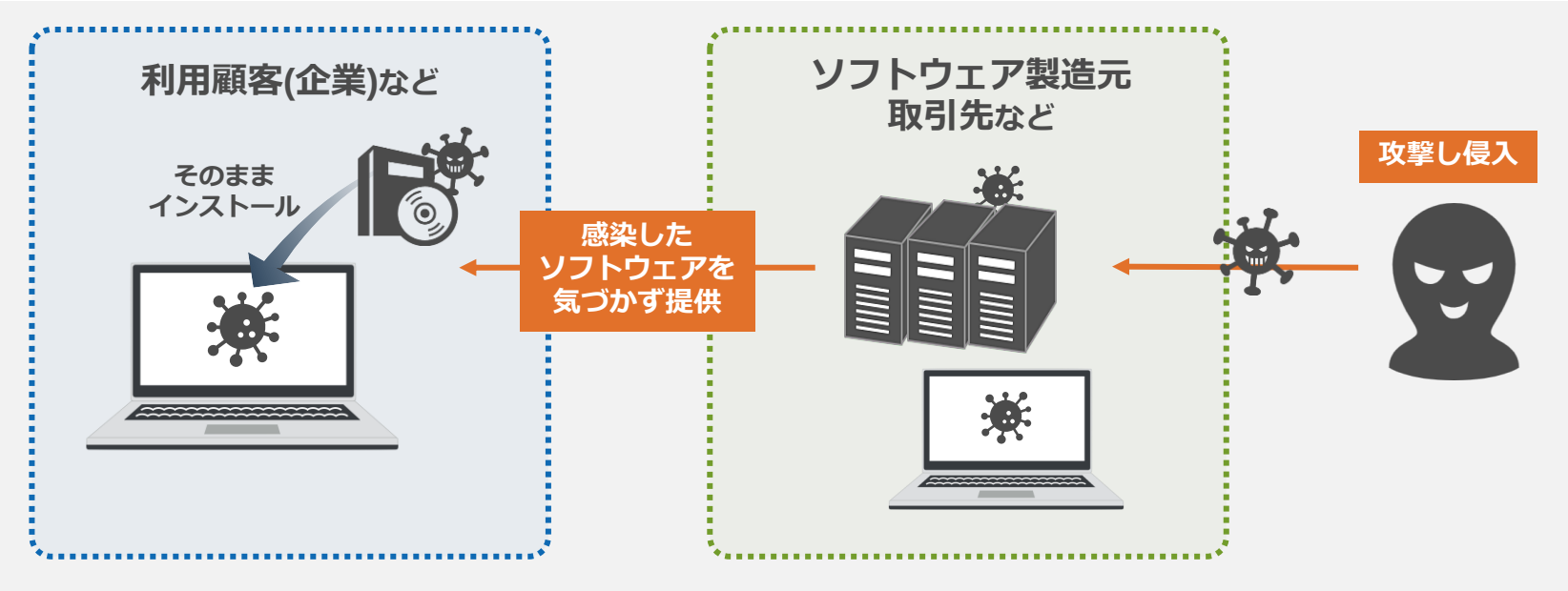
その他に、国外の拠点や子会社から内部不正によるアクセスによって、情報流出する場合もあります。



ソフトウェアサプライチェーン攻撃

例えば、攻撃者は、ターゲットの組織が利用しているソフトウェアの製造・提供の工程でマルウェアなどを仕込みます。

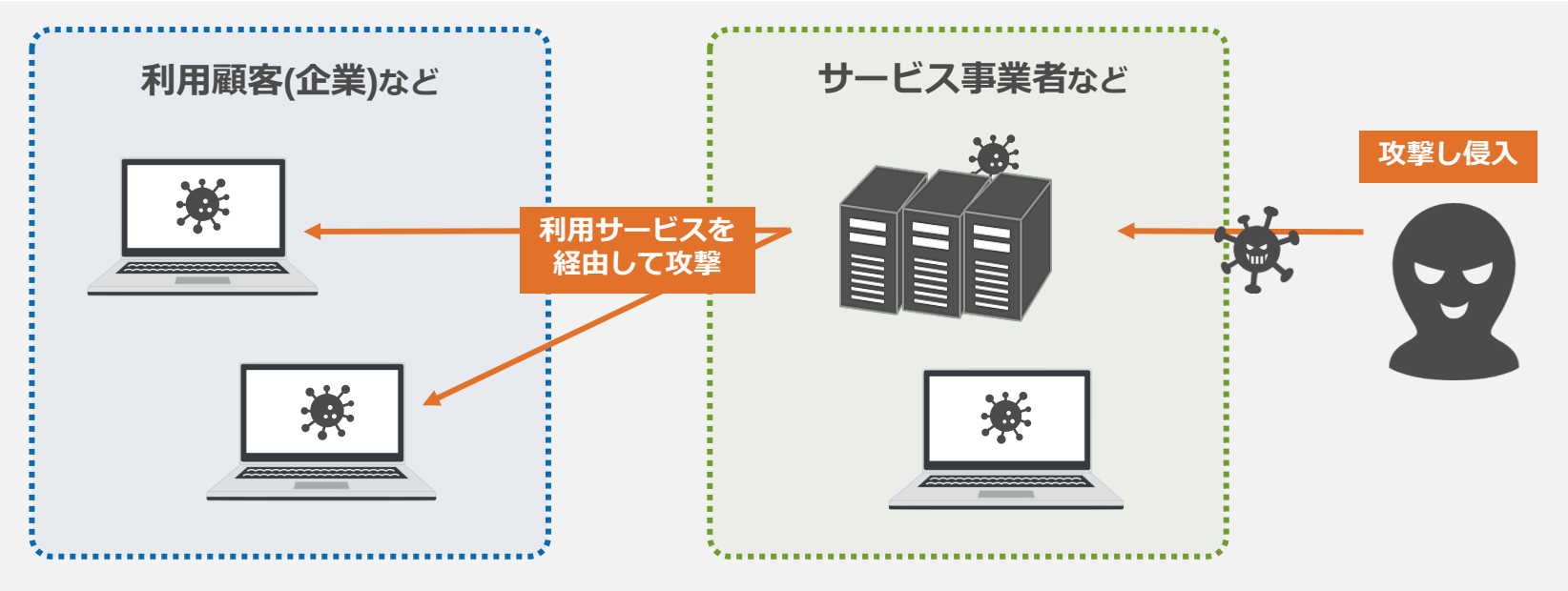
利用する組織がマルウェアなどに気づかず、そのままインストールしてしまうことで、攻撃者はターゲットへの不正アクセスをすることが出来る仕組みです。



サービス（デジタル）サプライチェーン攻撃

攻撃者は、サービス事業者を侵害し、サービスやAPIを介して攻撃します。

例えば、攻撃対象の事業者がサービスを介してネットワークの管理・運用などを行っている場合、攻撃者は侵入さえ出来てしまえば、利用顧客から関連事業者までランサムウェアのようなウイルスをばら撒くことが可能になります。



業務委託先企業のサーバへの不正アクセスにより委託元企業の情報が漏洩した事例

チューリッヒ保険株式会社
(2023年1月)

70万人以上

(過去に契約していた人も含め)
特定のサービスを契約した人の
姓・生年月日・
メールアドレス・顧客IDなど

※ チューリッヒ保険株式会社：個人情報漏えいに関するお詫びとお知らせ を基に作成
https://www.zurich.co.jp/-/media/jpz/zrh/pdf/pr/2023/NewsRelease_20230110_ZurichInsuranceCompanyLtd.pdf

アフラック生命保険株式会社
(2023年1月)

130万人以上

特定のサービスを契約した人の
姓・年齢・性別・証券番号など

※ アフラック生命保険株式会社：個人情報流出に関するお詫びとお知らせ を基に作成
https://www.aflac.co.jp/news_pdf/2023011001.pdf

業務委託先の従業員が機密情報を持ち出したことで その情報が漏洩した事例

株式会社ベネッセコーポレーション
(2014年6月)

2800万件以上

事件後1~2年間

前年黒字から一転して
2年連続赤字決算

※ 日本経済新聞：ベネッセ側に1300万円賠償命令 個人情報流出で東京地裁 を基に作成
https://www.nikkei.com/article/DGXZQOUE242UP0U3A220C2000000/

約10年後

被害者に対して、
総額約1300万円の
賠償請求の判決

※ 株式会社ベネッセホールディングス：事故の概要 を基に作成
https://www.benesse.co.jp/customer/bcinfo/01.html

具体的な被害

委託元企業の
機密情報漏洩

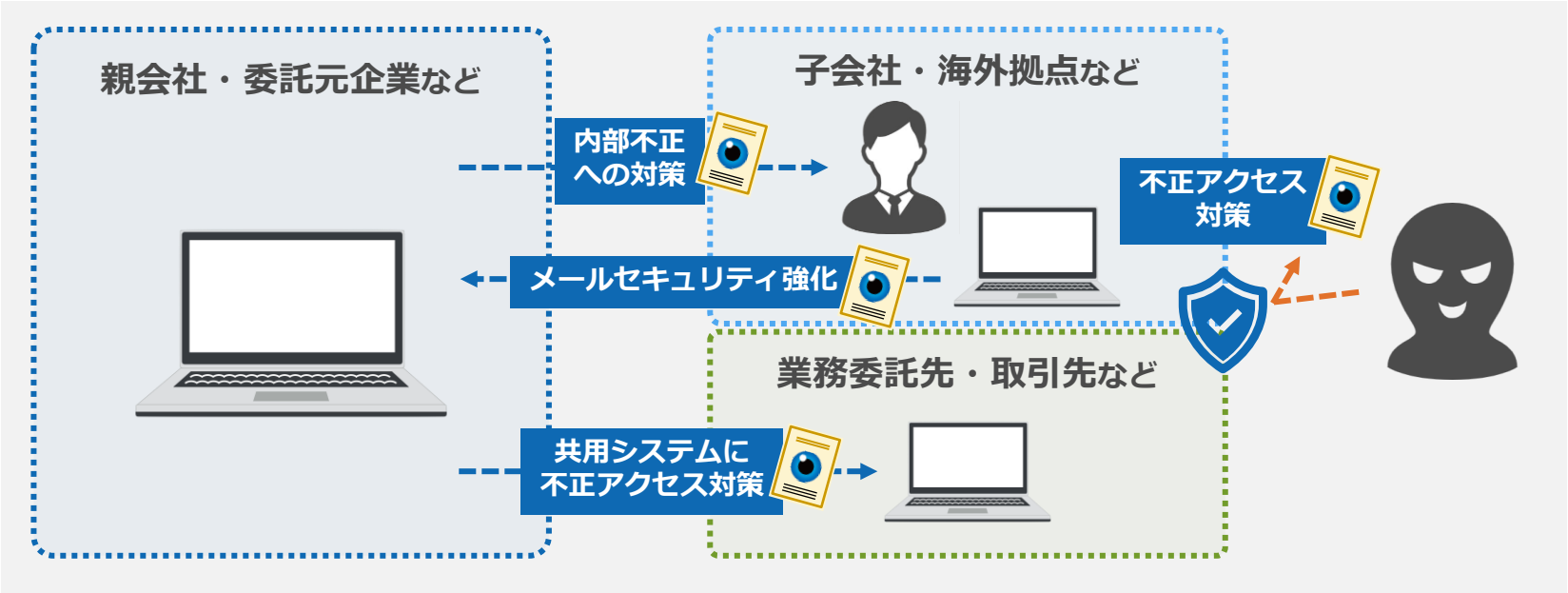
多額の負担
情報漏洩の範囲
原因の調査
取引の停止など

委託元企業の
イメージダウン

業務委託先などの関連企業にも
セキュリティ意識の強化や不正アクセス対策が必要

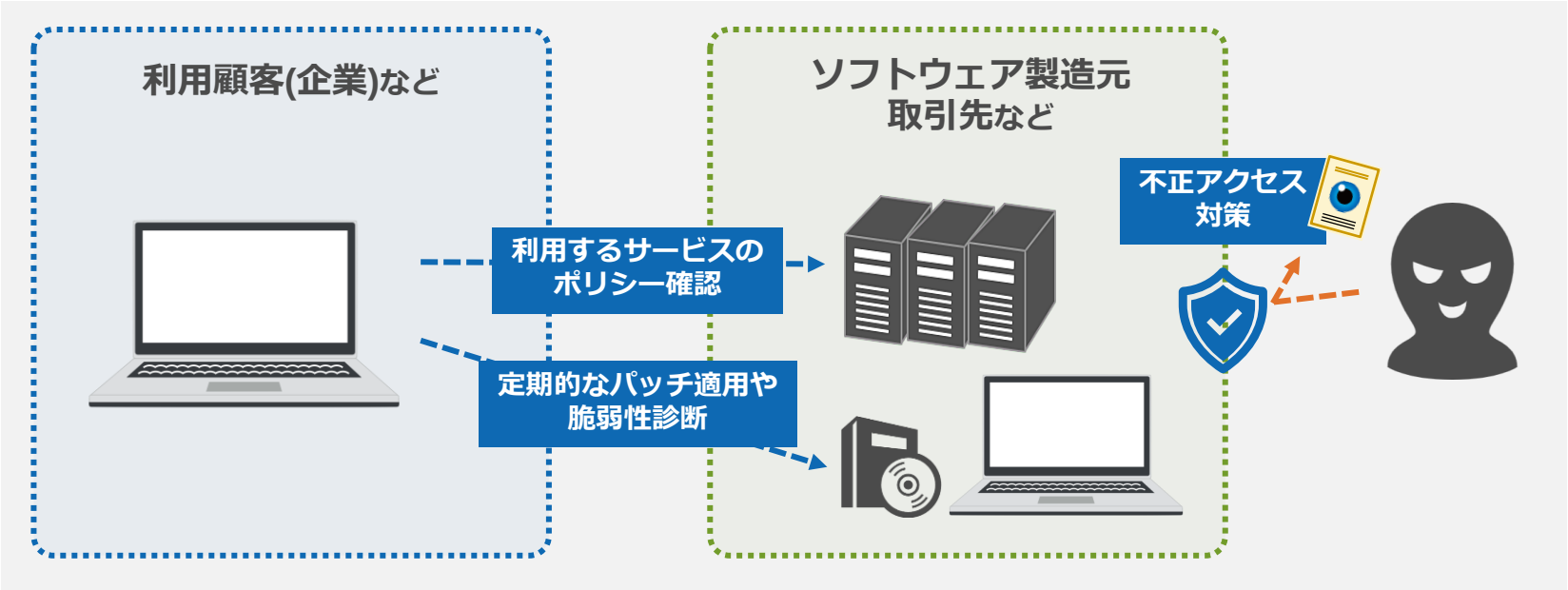
ビジネス（サービス）サプライチェーン攻撃

業務委託元の企業は、内部不正への対策として、正しいアクセス権限の割当や専用のセキュリティ対策ソフトの導入が挙げられます。また、不審なメールのURL・ファイルは開かないなどの社内教育や、委託先と共通のシステムを利用している場合、そのシステムへ不正アクセス対策を導入することも有効です。



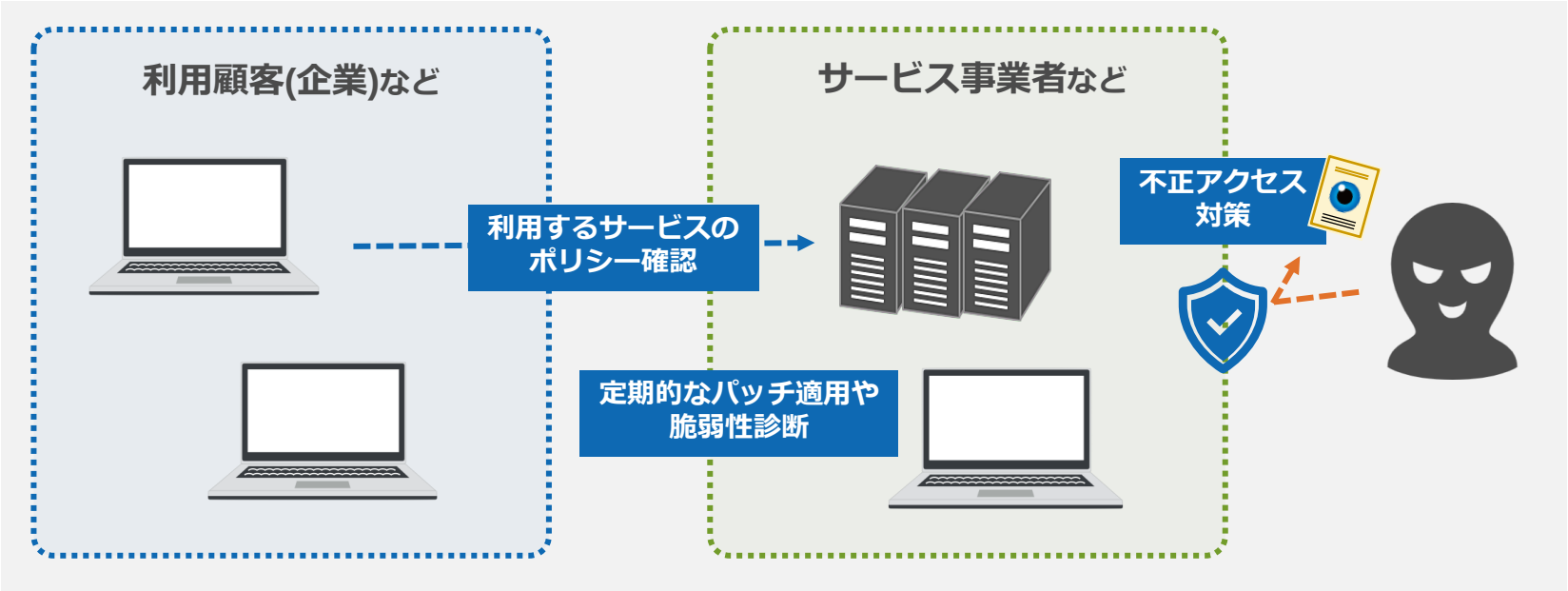
ソフトウェアサプライチェーン攻撃

ソフトウェアの製造元側としては、利用システムへの不正アクセス対策は勿論、アプリケーションの通信の監視や個人情報の管理などが必要です。利用組織は、製造元のセキュリティ状態が信頼できるかどうかを確認した上でソフトウェアを導入し、定期的なアップデートも正しいものか確認した上で行うことが推奨されます。



サービス（デジタル）サプライチェーン攻撃

サービス事業者側としては、利用システムへの不正アクセス対策は勿論、不正な操作が無いかどうかサービスの通信状況の監視やシステムの脆弱性診断などが必要です。利用組織は、そのサービスのセキュリティ状態が信頼できるかどうかを事前に確認した上で利用開始することが推奨されます。



対策まとめ

● 社員のセキュリティ意識を高める

：知らない宛先からのメールは開かない等の教育が社内外問わず必要です。

● システムやサーバ等の脆弱性を解消

：定期的な脆弱性診断や、セキュリティソフトを使用した確認が推奨されます。

● 多要素認証の導入

：ID/パスワードに他の認証要素を加えることで、不正アクセス対策になります。

● 内部不正への対策

：組織や取引先の従業員などによる、機密情報の持出や悪用などを指します。

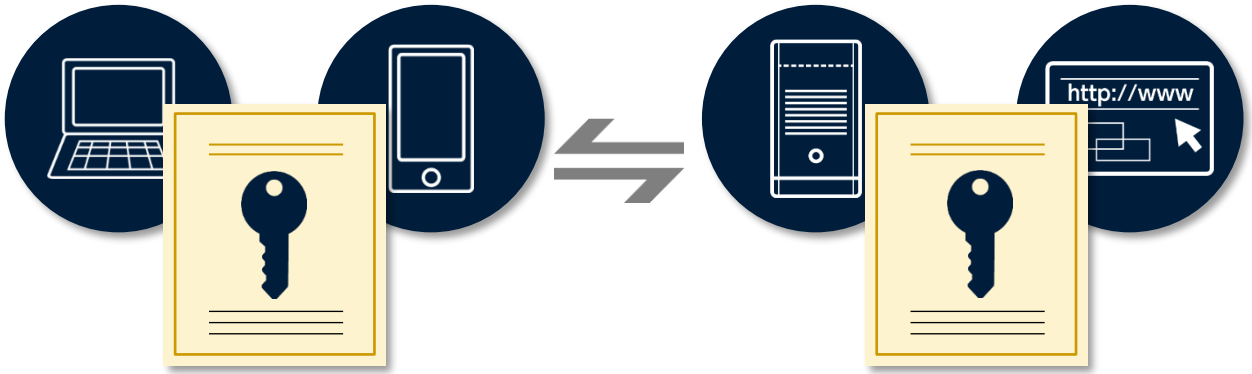
上記2項目の対策となる「クライアント証明書」を紹介します

「クライアント証明書」とは

概要

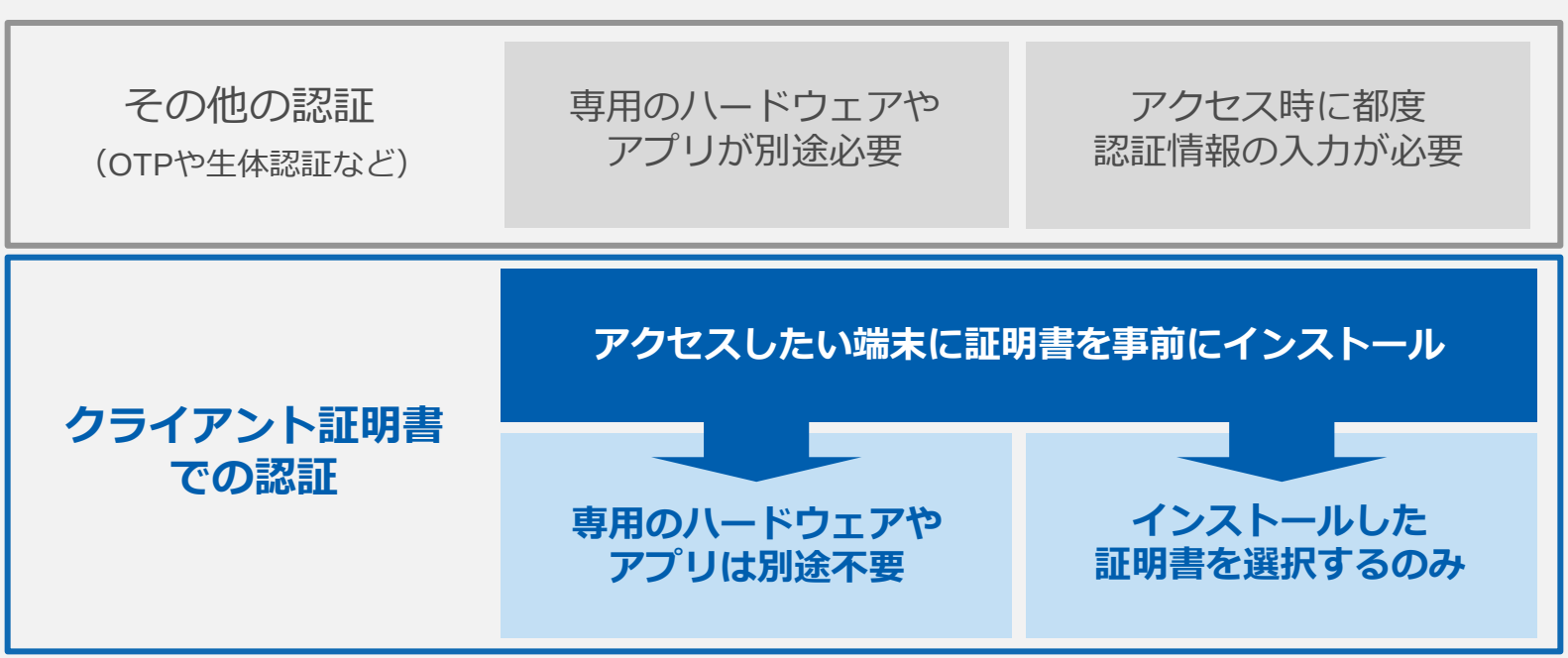
クライアント側（PC・モバイル端末）にインストールする電子証明書の一般名称 ▶ **クライアント証明書**

1. ID/パスワードと併用することで**セキュリティ強化**
2. 証明書がある端末のみアクセス可能な**アクセスコントロール**
3. 電子メールの暗号化や電子署名による**メールセキュリティ強化**



セキュアで利便性の高い認証方法

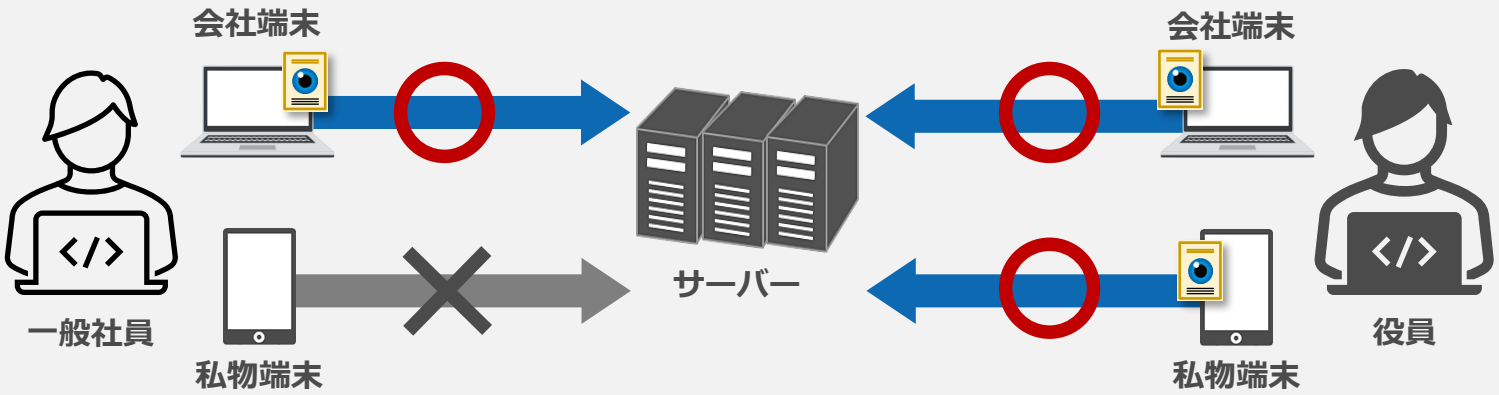
不正アクセス対策として、クライアント証明書は多要素認証の1要素として利用することを推奨しています。多要素認証で良く利用される他の認証方法と比較しても、利便性の高い認証方法になります。



端末ごとでのアクセス制御が可能

一部社員の会社端末へのみ証明書をインストールすることで、信頼した社員の会社端末でのみシステムへのアクセスを可能にできます。また、私物端末へ証明書をインストールすることにより、BYOD もセキュリティリスクの不安なく行えます。

加えて、端末にインストールした証明書のコピーを禁止する設定が可能です。そのため、別端末への証明書のコピーによる不正端末からのアクセスを制限できます。

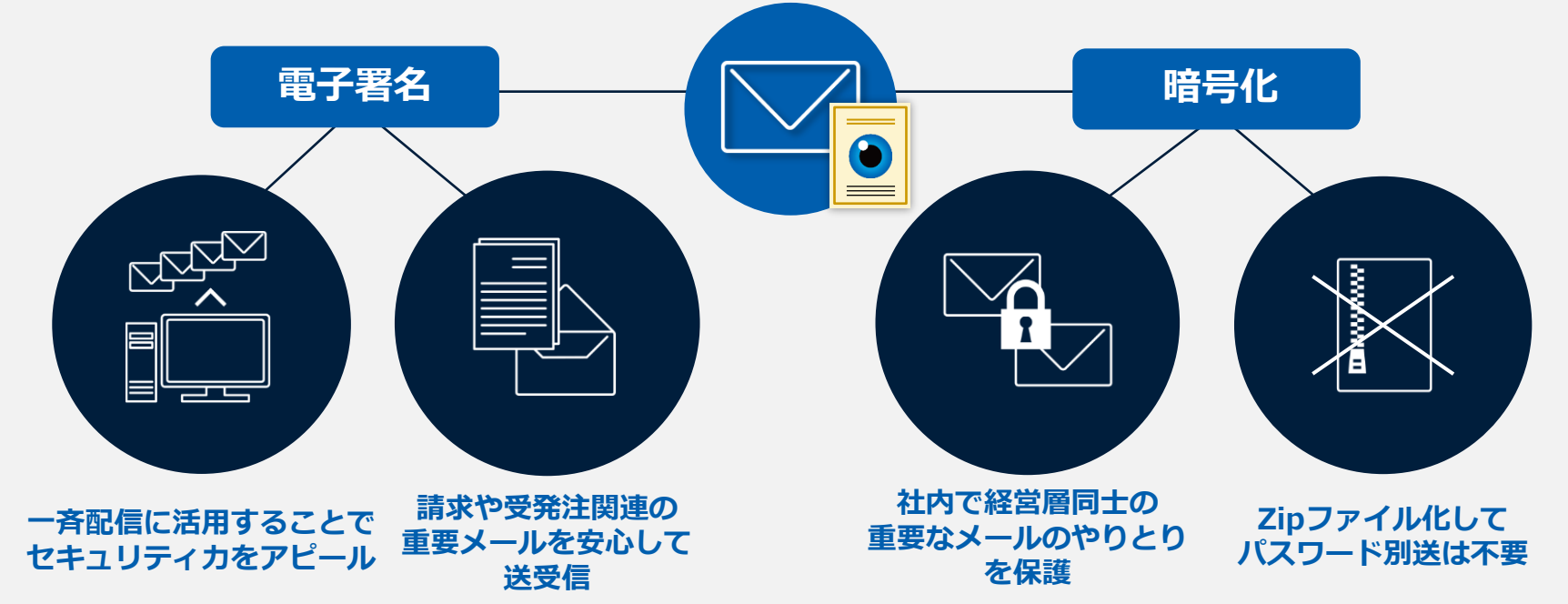


メールセキュリティ強化にも利用可能

クライアント証明書は、

- **電子メールの送信元の身元証明と改ざん検知が可能な電子署名**
- **第3者に添付ファイルも含めてメールを盗聴されないようにする暗号化**

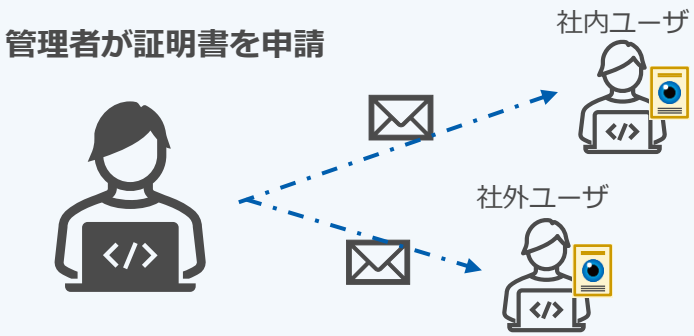
という２つの機能を持ち合わせています。（→ S/MIMEの詳細はこちら）



マネージドPKI Lite byGMO

- ✓ **最短1営業日**で証明書発行可能
- ✓ **初期費用不要**、専用サーバの構築不要
- ✓ ルート認証局として**20年以上の経験**によるサポート
- ✓ **専用の管理画面**で証明書を一括管理・申請

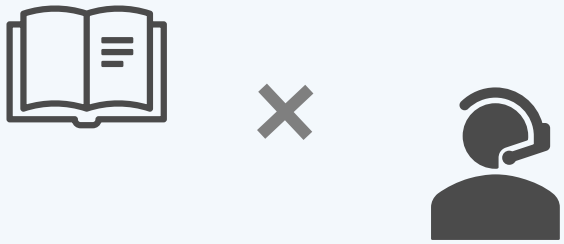
社内外問わず運用しやすい



※ 一部MDMでの配布やシステムとのAPI連携も可能

初めての導入も安心

当社内で検証済みのマニュアルを無料公開



電話orフォームでのお問い合わせサポート

まとめ

まとめ

従来、セキュリティ対策といえば自社への対策ばかり注力される傾向にありましたが、委託先や関係会社を経由するサプライチェーン攻撃は、自社だけの対策では完結しません。自社の情報漏洩対策は勿論、サプライチェーン全体でセキュリティレベルを上げる取り組みが必要になっています。

情報漏洩対策において、自社と関係会社に何が足りないかを見直し、様々なセキュリティ対策を組み合わせて万全な対策をしましょう。その中でも、**クライアント証明書は、アクセス認証時の利便性を向上しつつ、自社と関係会社のアクセスセキュリティをまとめて強化**できます。

クライアント証明書の解説資料など
無料公開中！

ダウンロードはこちら

90日間有効なテスト用証明書
無償提供中！

お申し込みはこちら

※ 証明書の配布までに1営業日前後いただきます。

クライアント証明書に関する
お問い合わせ

03-4545-2300 （受付時間 平日10:00-18:00）

https://jp.globalsign.com/contact/mpki/

GMOグローバルサイン株式会社

〒150-0043
東京都渋谷区道玄坂1-2-3　渋谷フクラス
https://jp.globalsign.com/