

OSINT 調査『Discovery』

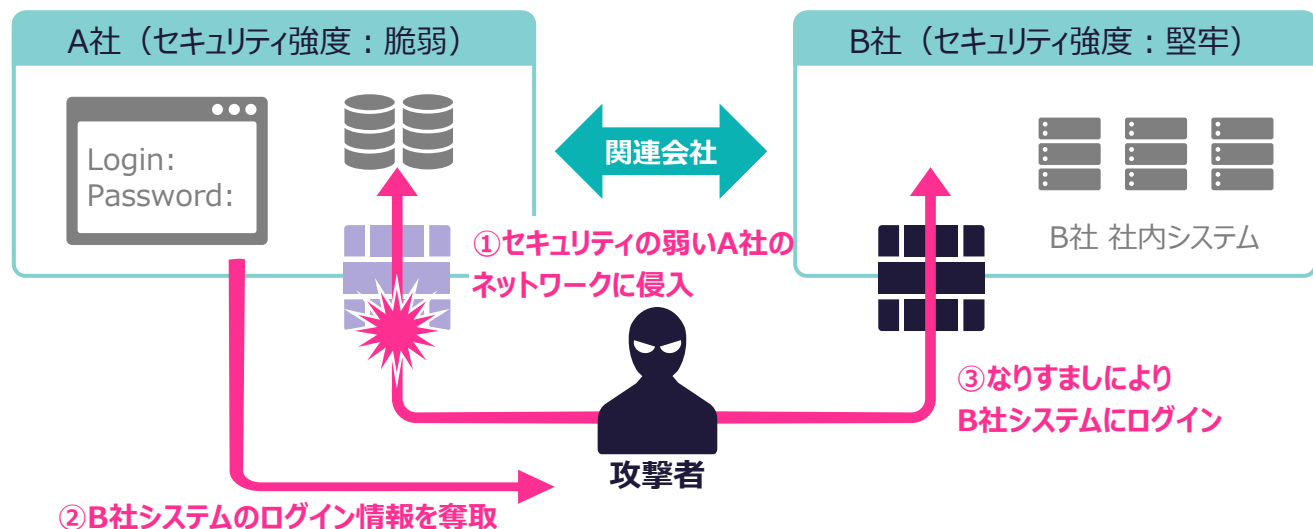
攻撃者に狙われるサプライチェーン

IPA の公開する「情報セキュリティ 10 大脅威 2024」において「**サプライチェーンの弱点を悪用した被害**」は 2 位にランクインしており、6 年連続 6 回目の選出になっています。さまざまな規模の企業が存在するサプライチェーンにおいて、大企業と中小企業では**セキュリティ対策への投資にギャップ**があることがしばしば見受けられます。

攻撃者であるハッカーは、攻撃が成立する確率の高い、**セキュリティ対策が手薄な中小企業への侵入を試みます。**

順位	組織向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した被害
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

サプライチェーンのネットワークを利用した攻撃



ハッカーは、直接侵入が難しいセキュリティの強固なターゲット組織に対し、**比較的セキュリティ対策が手薄な取引先や子会社（＝サプライチェーンの弱点）**などを経由することで、ターゲット組織へと侵入します。つまり、自社のセキュリティ対策が不十分であることは、関係会社のセキュリティを脆弱な状態にしてしまうことに繋がります。セキュリティ対策は自社のみの問題ではなく、対外的にも重要な要素になっています。

公開情報による情報収集

ハッカーは、公開されている様々な情報を収集し攻撃の準備をします。公開情報には、ホームページやSNSアカウントなどの容易にアクセスができるものから、**ダークWeb**で取引されている「**実際の攻撃手法**」や「**正規のユーザ情報**」なども含まれます。

意図していない情報の公開や、漏えいしているユーザ情報などは、**設定の変更**等で対策可能な



ものもあります。企業の中に存在する「**攻撃者を侵入しやすくさせてしまう隙**」を潰しておかなければ、攻撃者から目を付けられやすい状況が続き、いずれは攻撃の餌食となってしまいます。各種公開情報の把握とそれらへの対策は急務です。

企業情報モニタリング Discovery とは？

AI テクノロジーを活用した OSINT 技術に加え、エンジニアによるハッカー視点での、ダーク Web への漏えい情報を含む外部公開情報の収集・調査を行う独自の監視サービスです。



インシデントの監視 および報告

セキュリティインシデントの持続的監視で、タイムリーに対応

- 盗まれた資格情報
- 公開された社内ドキュメント
- 漏洩したソースコード など



コンプライアンスの 準拠と脆弱性予測

本番環境に害を与えない安全な外部スキャンと脆弱性予測

- Web サイトのセキュリティ
- 期限切れのドメインと証明書
- PCIDSS 準拠状況 など



外部からの 攻撃対象を予測

ハッカー目線で外部からの攻撃対象領域を監視

- API と Web サービス
- 保有する Web サイト
- ドメインと SSL 証明書 など

本調査を行う前に、リスクの高い脆弱性の有無や情報漏洩の可能性の有無を簡易的に診断することが可能です。PoCの結果をもとにして本調査の実施をご検討いただけます。

簡易調査 (PoC)

100万円

内容

簡易レポート、情報漏洩の発生有無の調査、脆弱性診断 (Critical, High)

本調査

個別見積

内容

詳細レポート、情報漏洩の詳細情報報告、脆弱性診断 (Critical, High, Medium)

レポートサンプル (抜粋 / 数値および内容はサンプルです)

1. Discovery PoC 簡易レポート

簡易調査

本調査レポートは「企業情報モニタリング Discovery」の PoC 簡易レポートとなります。正式調査を実施する際の事前調査資料として作成するものであり、全ての脅威情報や詳細情報を掲載するものではありません。簡易程度として Critical/High リスク判定された事例のみを抽出して正式調査時に報告されるであろう内容の参照物としてご利用ください。また、正式調査時には Medium リスク以下の報告や、具体的な漏洩情報と脆弱性予測の詳細情報の取得が実施されます。

2. Web

2.1. 脆弱性 Critical Risk レベル

本調査レポートは「企業情報モニタリング Discovery」の PoC 簡易レポートとなります。いくつかの Web サイトではライブラリや CMS のバージョンが古いことが観測されています。Web サイトや Web サービスに構築されている古いコンポーネントは将来的な脆弱性の発現や、攻撃者グループからの侵害ポイントとなる恐れがあります。

3. Mobile

3.1. 脆弱性 Critical/High Risk レベル

本調査レポートは「企業情報モニタリング Discovery」の PoC 簡易レポートとなります。いくつかのモバイルアプリではライブラリや暗号プロトコルが古いことが観測されています。Mobile アプリに構築されている古いコンポーネントは将来的な脆弱性の発現や、攻撃者グループからの侵害ポイントとなる恐れがあります。

2. Web

本調査

2.1. 脆弱性 Critical Risk レベル

2.1.1. www.example.edu

CVEs-3.1	CVE-ID	CWE-ID	References
8.7 High	CVE-2019-0539	CWE-20	https://www.cvedetails.com/vulnerability-list/id/42020/2019-0539/
6.0 High	Not Assigned	CWE-324	https://www.cwe.org/CWE324.html