SEAGULL 通信

令和２年３月30日発行

No. 11

"security action for guarding technical intelligence"

あなたの会社は大丈夫ですか?!
今回は、身近な脅威「サプライチェーン攻撃」についてです。

サプライチェーン攻撃とは、標的とする企業を直接狙うのではなく、サプライチェーンに関わる取引先企業を踏み台にしたサイバー攻撃のことです。

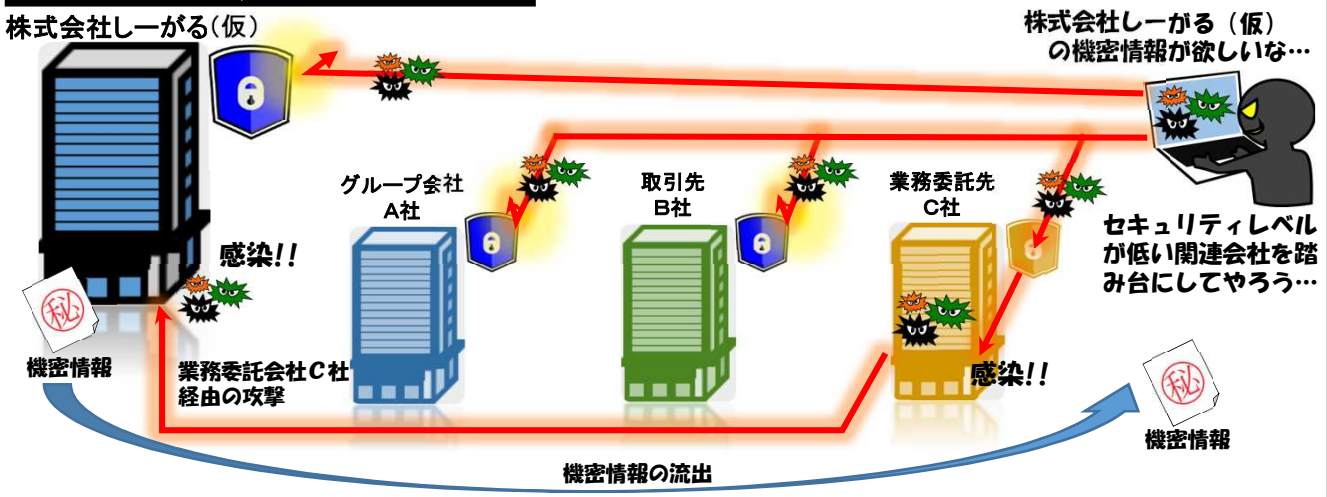
そもそもサプライチェーン（Supply Chain）って何ですか？

直訳すると「供給の連鎖」という意味で、製造会社で言えば、原材料等の調達から、製造、在庫管理、物流、販売、そして顧客の手元に届くまでの一連の流れのことをいいます。

サプライチェーン攻撃の一例

ある会社から機密情報を盗み取ろうとしている犯人がいます。しかし、その会社は大企業でセキュリティが強固でした。そこで、その標的とする企業と取引関係にある比較的セキュリティレベルが低い会社等を踏み台にして、サイバー攻撃を行おうとすることをサプライチェーン攻撃といいます。

取引先の担当者を装った標的型攻撃メール



業務委託先の中でセキュリティレベルの低い「C社」が踏み台にされ、「株式会社しーがる（仮）」が機密情報の流出被害に遭っています。

☆SEAGULL通信からのアドバイス☆

攻撃の踏み台とされないためには、セキュリティ対策ソフトの導入、OSのアップデート等のできることから始めて、セキュリティレベルの向上を図りましょう。

セキュリティレベルの向上は、自社の財産である機密情報を護るだけでなく、取引先等との信頼関係を護ることになるのです。

▼ SEAGULL事務局（外事課内） ▼

〒231-8403 横浜市中区海岸通2丁目4番 神奈川県警察本部

相談窓口 Email：seagull@police.pref.kanagawa.jp