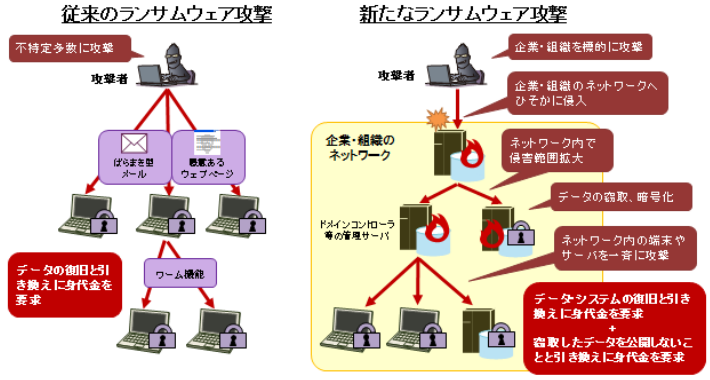
サイバーセキュリティの置き薬

2021年 第7号

ランサムウェアによるサイバー攻撃に関する注意喚起

最近、新たな手口によるランサムウェアの脅威が高まっており、国内においても被害事例が確認されています。新たなランサムウェアは企業の事業継続が脅かされる可能性があるため注意が必要です。



※引用：IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について」（図１従来の/新たなランサムウェア攻撃の差異）

【事例】
ランサムウェアの感染によりデータが窃取、削除されるとともにシステムの一部に障害が発生。攻撃者を名乗るグループがインターネット上に犯行声明を掲載し、窃取した情報の公開停止と引き替えに身代金を要求。実際に情報の一部も公開された。

急増中　新たなランサムウェアの攻撃の手口

- ☐ 不特定多数から特定組織を狙った攻撃に
- ☐ 単なる感染だけでなく、不正アクセス（不正侵入）も
- ☐ 無作為な端末からシステム中枢の感染を狙う
- ☐ 事業継続や個人情報等の重要なデータが狙われる
- ☐ 被害組織の公表前に、窃取データが公開されることも

新たなランサムウェア攻撃は、諜報活動を目的とするような標的型サイバー攻撃と同等の技術が駆使されるため、あらゆる面でのセキュリティの強化で対応する必要があります。例えば、ウイルス対策、不正アクセス対策、脆弱性対策など、基本的な対策を確実かつ多層的に適用することが大切です。

重要 POLICE

○　企業・組織のネットワークへの侵入対策
○　データ・システムのバックアップを確実に

参考URL

ランサムウェアによるサイバー攻撃について【注意喚起】(NISC)
https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf
【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について(IPA)
https://www.ipa.go.jp/security/announce/2020-ransom.html
大型連休等に伴うセキュリティ上の留意点について(NISC)
https://www.nisc.go.jp/active/infra/pdf/renkyu20210426.pdf
最近のサイバー攻撃の状況を踏まえた経営者への注意喚起(経済産業省)
https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf
2021年も増加傾向のランサムウェア、被害に関する共通点とは(LAC)
https://www.lac.co.jp/lacwatch/report/20210405_002585.html

SOS **万が一被害に遭った場合は、警察など関係機関にご相談ください。**