NetApp アンチランサムウェア機能資料

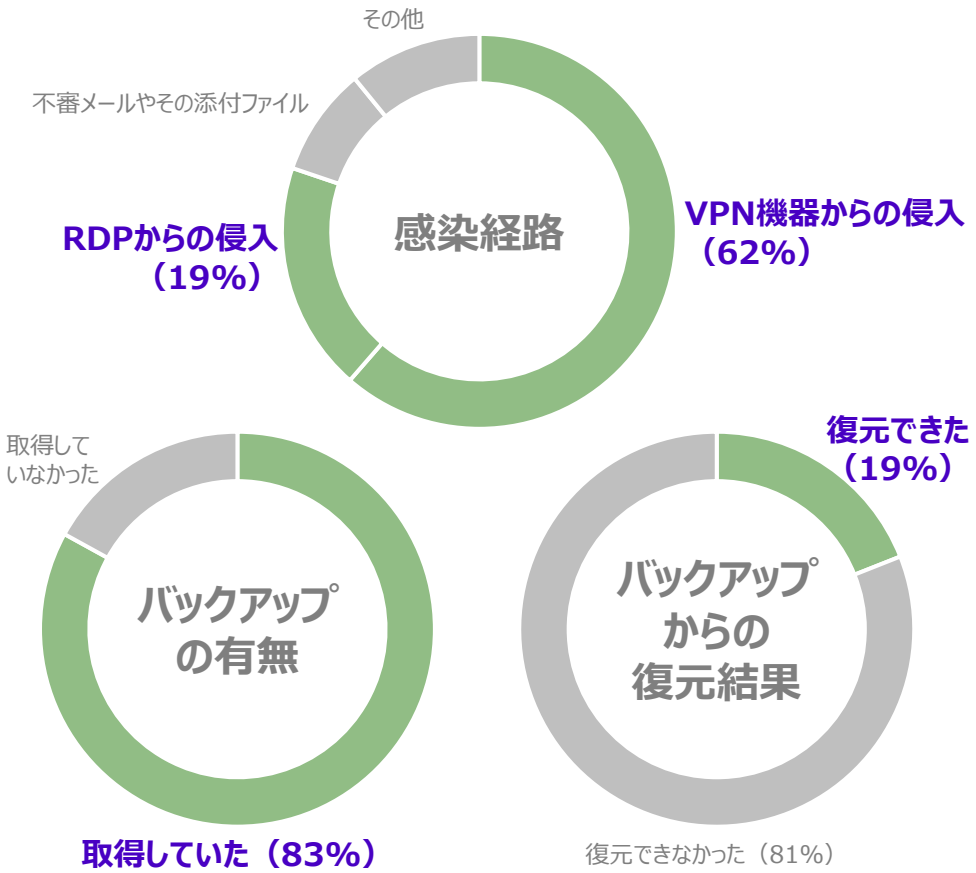
兼松エレクトロニクス株式会社

KEL
KANEMATSU ELECTRONICS LTD.

ランサムウェアに代表されるサイバー攻撃の傾向

- 頻度、巧妙さ、被害件数が増加するサイバー攻撃の脅威
- 「国際的な組織犯罪」としての認識を持つことが重要

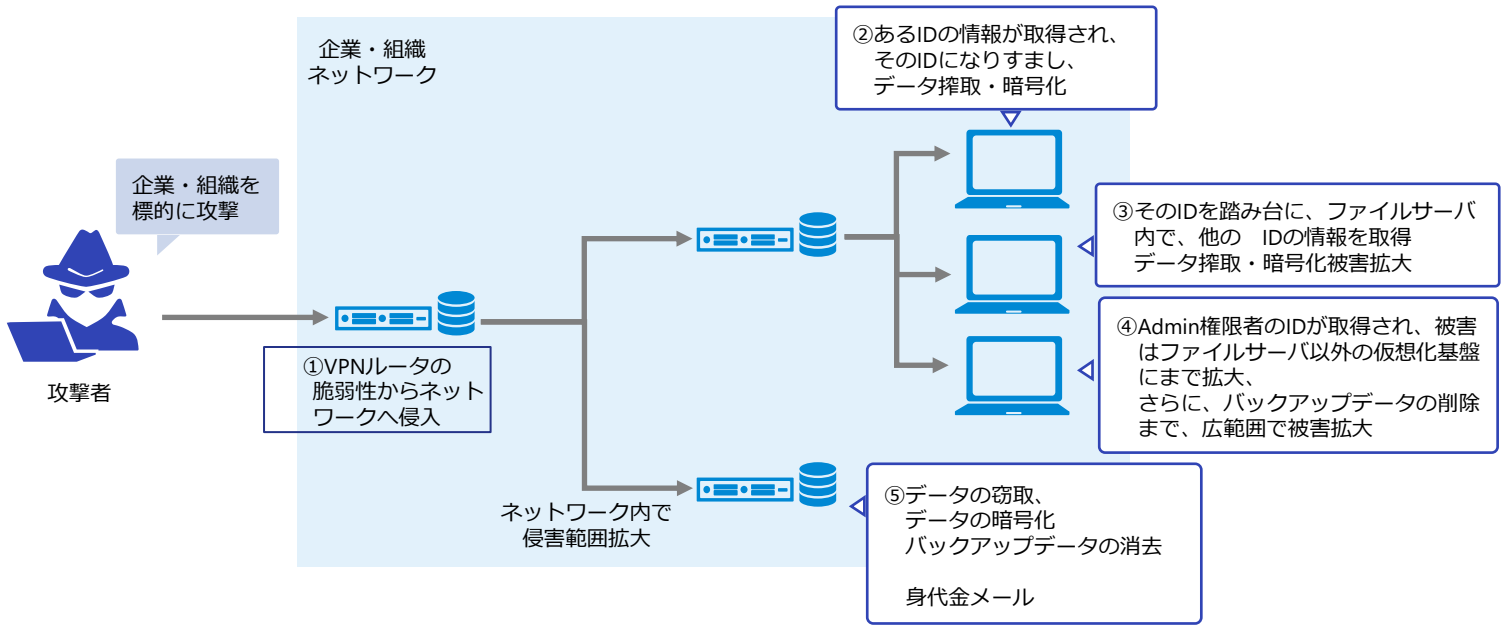
令和4年におけるサイバー空間をめぐる脅威の情勢等について
警察庁, 2023年3月発表 より抜粋



- 現在のサイバー攻撃は、ネットワーク装置やソフトウェアの脆弱性を利用し、**内部ネットワークへの侵入から開始**
- 不正入手した正規従業員のIDとパスワードを利用するなど、**犯罪者は”正規ユーザーになりすまして” ネットワーク内部で活動**する
- サイバー攻撃は、世界で11秒に1回、**日本で16秒に1回**、の頻度で行われている
- システムやデータのバックアップは多くの企業組織で取得されているが、実際にバックアップから**被害直前の水準にまで復元ができた企業組織は驚くほど少ない**

直近のランサムウェア被害

新たなランサムウェア攻撃



ランサムウェア攻撃に対しては、
- 完全な予防策はなく、攻撃されたらの対策が重要
- いつ攻撃されたか？が最も重要(検知と通知)
- その時点でのSnapshotを取得(その直前のSnapshotが1つのリストアの目安)
- 気が付かないと、ID情報を次々に搾取し、基幹システムまで影響が拡大、
  リストアの目途も立たない

【環境】
- EDRはおおよその端末に導入

- ファイルサーバを利用(全国数拠点)
  全国数拠点間でレプリケーションでDR/Backup取得
  Snapshot/レプリケーションは、Daily7 世代取得

- 仮想基盤ストレージも、vVOL機能＋レプリケーション
  を組み合わせた、DR/Backup取得
  Snapshot/レプリケーションは、Daily 7世代取得

【インシデント】
- 不自然なアプリケーションエラーが度々見られた。

- 原因を究明していた最中(約1週間後)
  ある日、ランサムウェアの爆発的な被害に気が付く

- 多数のID情報が取得され、Admin権限まで含まれ、
  AD、仮想基盤など多数のシステムが暗号化される

- 身代金メールが来る

- データ漏洩の可能性、全国ファイルサーバの停止、
  AD、仮想基盤のVMDKのパスワードも取得され、
  全国の業務が完全に停止

- いつから攻撃が開始されたのかが不明

- レジリエンス会社に復旧調査依頼
  (業務再開に数週間～1ケ月かかる可能性)

- 重大な機会損失、業務影響、信用の失墜のリスク

NetAppアンチランサムウェアソリューション

NetAppアンチランサムウェア機能は、以下の2つのソリューションを組み合わせる事がベターです。
・Autonomous Ransomware Protection
・Cloud Insights Storage Workload Security

①ONTAPのアンチランサムウェアプロテクション機能で、
機械学習により、通常と異なるボリューム内のアクセスを検知＝ランサムウェアのふるまい検知と、管理者への通知・感染発覚時間をSnapshotを取得し、明確化

②ONTAPアンチランサムウェアプロテクション機能から、
Cloud Insights Storage Workload Securityに連携し、
タイムラグを補う。
ランサムウェアのなりすましIDと疑われるクライアントを特定し、かつブロックすることで、拡大を防ぐ

ランサムウェア対策のポイント

①ランサムウェアの主要感染原因はNetworkの脆弱性であり、攻撃されたらの対策が重要
②ランサムウェアの最初のターゲットはファイルサーバで、ここで多くのID情報を搾取
③攻撃開始の時間の特定＝速やかに検知・通知
④ランサムウェアは時間を置くほど、より高位の権限情報を取得、主要業務に影響が出る
拡大を防ぐ為、被疑IDの特定・ブロックが重要

補足：Cloud Insights Storage Workload Securityの付加効果
退社予定社員のデータ持ち出し等の情報漏洩対策にもなる

**ONTAPの
ボリュームへの書き込みが、
事前と事後でどう違うか？**

ボリュームアクセス
を検知して対処する

無償

- パソコン・モバイル端末・サーバーと同様に、**ストレージ装置への「デバイス攻撃」を検出**
- **データの暗号化処理を自動的に検出し、緊急Snapshotのの取得、**管理者がストレージアクセスの遮断などの「データを守る対策」を検討可
- **イミュータブル 且つ 攻撃耐性の強いSnapshotバックアップ**によりデータの確実な復旧を実現

ONTAP
（Autonomous Ransomware Protection）

＋

**ONTAPへのユーザアクセスが
事前と事後でどう違うか？**

ユーザアクセス
を検知して対処する

有償

サーバx2台
※1台で兼務

FWに
HTTPS(443)

- ユーザーのデータアクセス傾向をモニタリングし、**「通常と異なる動作」**をAIにより検出
- データへのアクセスパターンから**ランサムウェア攻撃を行うユーザを検出し 対応策を発動**
- データの持ち出しや大量削除などを検出
被害拡大を防ぎ、フォレンジックのためのレポートを提供

Cloud Insights
（Storage Workload Security）

NetAppアンチランサムプロテクションの補足

KANEMATSU ELECTRONICS LTD.

適用するONTAPの Verで機能が変わります

ONTAP 9.10.1

「アンチランサムウェアプロテクション」の有効化

- 約30日間の機械学習期間が必要(この間はアンチランサムウェアは起動せず)
- その後、手動でEnableに(オーバーヘッドは2%程度で軽微)
- オンボックスなので、閉鎖セグメントでも利用可能
- オンボックスなので、非常に速い検知
- お客様のファイルサービスでのふるまい方を機械学習し、ふるまい検知
- 管理者へのメール通知(管理者が本当にランサムウェアか調査・対策開始可能)
- 検知時、すぐSnapshot作成(直前のSnapshotがリストアの目安)

ONTAP 9.11.1

Cloud Insights Storage Workload Securityとの連携

- オンボックス「アンチランサムウェアプロテクション」で早期検知
- 若干タイムラグのあるStorage Workload Securityと連携し、なりすましと疑わしいIDの特定とブロックで被害拡大を防ぐ

サージ(大量のデータ操作)の監視

特定の操作(Volume削除など)は多段認証化

ONTAP 9.12.1

fPolicy設定の簡素化

- fPolicyとは、特定の拡張子のファイルの書き込みを制限
- ランサムウェアでよく使用される暗号化後の拡張子をラインナップに加えGUIで簡単にfPolicy設定が可能に

機械学習のデータをSnapMirrorで転送可

- 本番機の学習結果をDRサイトに共有
- DR機・開発機などは、機械学習の効果が上がりにくいので、非常に有効

Tamperproof Snapshotの実装

- リテンション(Snapshotのローテーションルール)期間は、Admin権限でも削除不可のSnapshot
- 海外では、Snapshotの強制削除事案が増加

ONTAP 9.13.1(最新)

学習期間の短縮化と自動起動

- 学習期間の完了をONTAPが判断
  最短7日から最長30日間
  機械学習に十分なそのお客様のファイルサービスのふるまい方を学習
- 手動で「Enable」するのではなく、機械学習が完了と共に自動で「Enable」に

Appendix ②：KELのNetAppへの取り組み

KELのNetApp Businessのご紹介

- **1996年より取引開始～20年超の実績**
- **国内最上位 「Prestige Partner」(※8/1より呼称変更)**
- **NetApp製品専門スタッフによる強力なサポート体制**
  - **プリセールスから、販売・導入・構築、及びポストサポートまで、一貫サポート**
    - 「ISC（Integration Service Certified）」自営構築資格
    - 「LSC（Lifecycle Support Certified）Level1」最高位自営保守資格
      ※国内唯一の最高位 Level1
  - **NetApp製品専門組織を完備（製品担当、プリセールスSE、保守サポート）**
  - **24時間365日コールセンター及びオンサイト対応**
- **Award受賞歴**

NetApp Japan Partner Award	2016	**: Partner of the Year**
NetApp Japan Partner Award	2017	**: Technology Innovation Award**
NetApp Japan Partner Award	2018	**: NetApp University Award**
NetApp Japan Partner Award	2019	**: NetApp University Award**
NetApp Japan Partner Award	2020	**: Partner of the Year**
NetApp Japan Partner Award	2021	**: Momentum Award**
NetApp Japan Partner Award	2022	**: Partner of the Year** **Service Partner of the Year**
NetApp APAC Partner Award	2022	**: APAC Solution Innovation Award**
NetApp Japan Partner Award	2023	**: Partner of the Year**

KEL

KANEMATSU ELECTRONICS LTD.