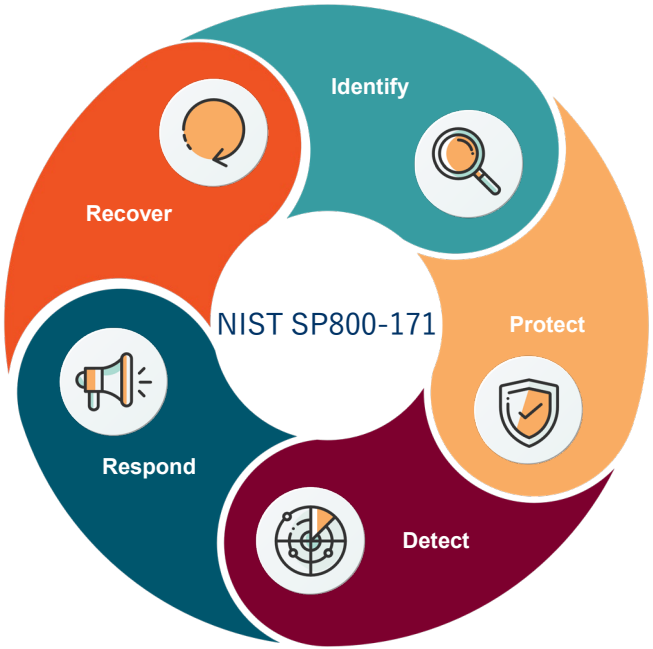
サイバーレジリエンス
ソリューションとは？

サイバーレジリエンス対策



- Identify　特定
- Protect　防御
- Detect　検知
- Respond　対応
- Recover　復旧

NIST SP800-171は米国国立標準技術研究所(NIST: National Institute of Standards and Technology)によるセキュリティのガイドライン

サイバーレジリエンス対策 ★

特定

- IDのアクティビティ監視
- デバイスのアクティビティ監視

防御

- ウイルス対策ソフトの導入
- ファイアウォールの導入
- パスワード管理
- ユーザー権限の管理

セキュリティ脅威の防止対策

サイバーレジリエンス対策 ★★

検知

- 特権IDの不正アクセスを検知
- 内部不正アクセスを検知
- ヒューマンエラー(誤操作)を検知

対応

- 特権IDの不正アクセスを抑制
- 内部不正利用を抑止
- 誤操作の訂正
- データのバックアップ

セキュリティ脅威の早期発見と対処

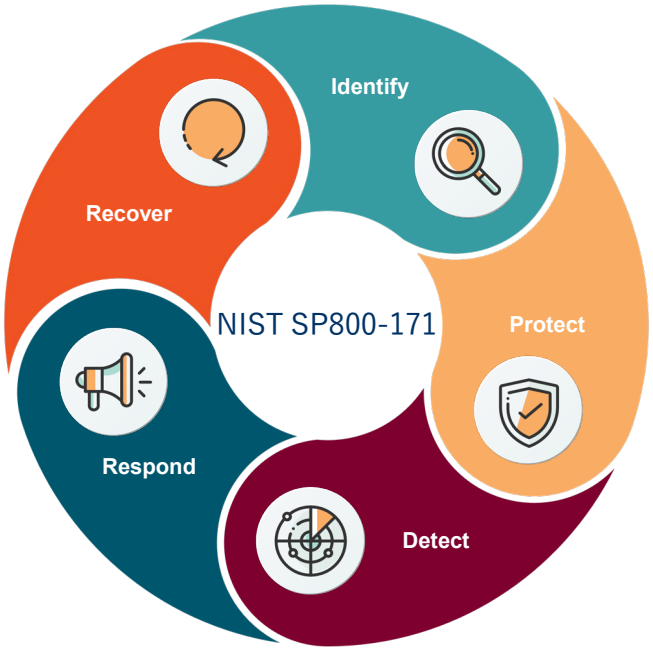
サイバーレジリエンス対策 ★★★

復旧

- データの復旧
- サーバーのベアメタル復旧
- ADオブジェクトの復旧
- ADドメインの復旧
- ADフォレストの復旧
- ADサーバーのベアメタル復旧

事業継続性の対処

サイバーレジリエンス対策



Identify　特定

Protect　防御

Detect　検知

Respond　対応

Recover　復旧

サイバーレジリエンス戦略を強化し、侵害、データ損失、停止が発生した場合でも重要な資産を安全に保つ

NIST SP800-171は米国国立標準技術研究所(NIST: National Institute of Standards and Technology)によるセキュリティのガイドライン

何かある前の予防と何かあった時の対処

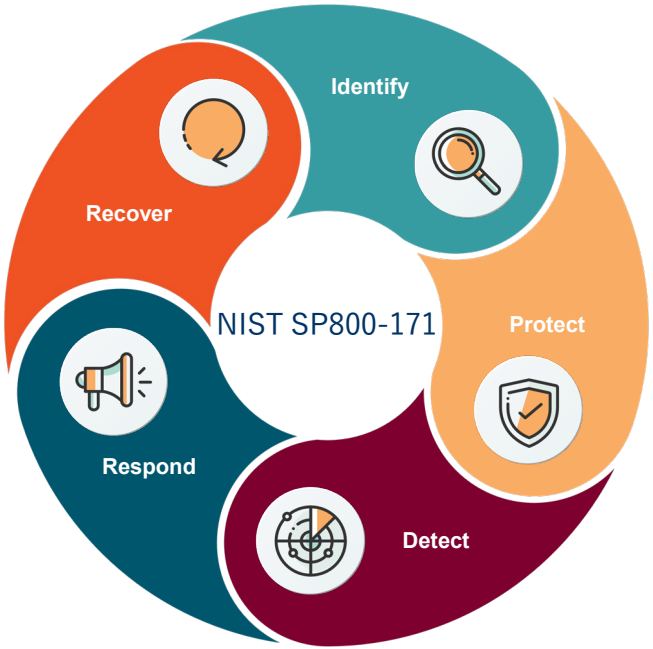
システム運用において以下の課題があり、

- 変更ミス発生時のオブジェクト単位、属性単位のリストア
- 障害復旧時のフォレスト全体、特定ドメインサーバーのリストア
- AD環境の構成変更前（設定変更やバージョンアップなど）の事前検証
- アクセス権の悪用や管理者アカウントの不正利用
- 管理者アカウントの利用状況、特定アクセスの監視

課題解決のために以下の対策が必要である

- ADとAzure ADの災害対策　（影響の軽減）
- ADの疑似環境作成　（復旧手順や構成変更の影響を事前確認）
- 万が一に備えたい　（適切な対応の実施）
- 内部不正による情報漏洩　（万が一に備える）
- セキュリティポリシー違反の追跡（問題ある行動を監視）

Quest Softwareのサイバーレジリエンス対策



- SpecterOps BHE/Enterprise Reporter
- Change Auditor/GPOADmin/Active Roles
- Change Auditor/On Demand Audit
- Change Auditor
- Recovery Manager/On Demand Recovery

セキュリティ脅威で注力すべき点は？

情報セキュリティ10大脅威

内部不正による情報漏えい

順位	組織
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報の搾取
3位	サプライチェーンの弱点を悪用した攻撃
4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
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
8位	ビジネスメール詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

出典：情報セキュリティ10大脅威 2022　最終更新日:2022.08.29

https://www.ipa.go.jp/security/vuln/10threats2022.html

内部の従業員は重要情報にアクセスしやすい

悪意をもって情報を外部に提供してしまう

- ■ アクセス権限の悪用
- ■ 在職中に割り当てられたアカウントの悪用

被害の予防

- □ 利用者IDおよびアクセス権の管理
- □ 重要情報の保護

攻撃の予兆/被害の早期発見

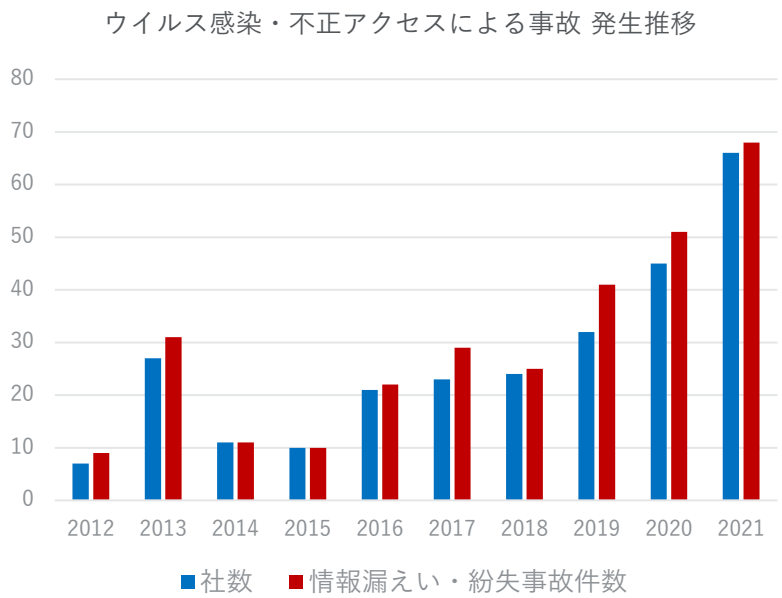
- □ システム操作履歴の監視

出典：情報セキュリティ10大脅威 2022 [組織編]　最終更新日:2022年5月

https://www.ipa.go.jp/files/000096898.pdf

内部不正による情報漏えい対策

不正アクセスに備えた対策



特権IDを利用できる限り、情報漏えいの危険がある

- 2021年は事故件数・社数ともに最多を更新
- 社内システム・サーバーが最多の約6割
- 東証1部上場企業が約8割

出典：上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の137件 574万人分（2021年） 公開日付:2022.01.17
https://www.tsr-net.co.jp/news/analysis/20210117_01.html

検知と対応でゼロトラストを実現

特権IDの利用者でも特定のフォルダ、ファイル、ADオブジェクトへのアクセスを抑制(重要データの保護が可能)

- Change Auditor for Active Directory
- Change Auditor for Windows File Servers

Where Next Meets Now.

保護と監査：Change Auditor

Microsoft 環境の変更履歴をリアルタイムに監査

AD、ファイルサーバー、Microsoft 365などの変更履歴をリアルタイムに検知可能。

- AD、ファイルサーバー、Microsoft 365などで発生する重要なアクティビティと変更を監査

  Change Auditorは以下のログを取得

  ・いつ変更したのか？
  ・どこから変更したのか？
  ・どのワークステーションから変更したのか？
  ・誰が変更したのか？
  ・何を変更したのか？
  ・変更前の値は何か？

- 重大な変更やパターン検知の警告をメールで通知
- 重要なADオブジェクトやフォルダのアクセス権を制御し、不正アクセスや変更操作を防止
- AD、Windows、Azure AD、Microsoft 365を横断して可視化

情報セキュリティ10大脅威

予期せぬIT基盤の障害に伴う業務停止

順位	組織
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報の搾取
3位	サプライチェーンの弱点を悪用した攻撃
4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
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
8位	ビジネスメール詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

出典：情報セキュリティ10大脅威 2022　最終更新日:2022.08.29

https://www.ipa.go.jp/security/vuln/10threats2022.html

予期できない事象によりIT基盤が停止する

BCMが適切に実践できていない

- 自然災害
- 作業事故
- 設備障害やシステム障害
- 在職中に割り当てられたアカウントの悪用

被害の予防

- 事業継続マネジメント(BCM)の実践(BCM作成と運用)
- データバックアップ(復旧対策)

出典：情報セキュリティ10大脅威 2022 [組織編]　最終更新日:2022年5月

https://www.ipa.go.jp/files/000096898.pdf

予期せぬIT基盤の障害に伴う業務停止対策

侵入に備えた対策

◆ 従来のアクセス監査だけで十分ですか？

出典：ログを活用したActive Directoryに対する攻撃の検知と対策
最終更新:2017.7.28
https://www.jpcert.or.jp/research/AD_report_20170314.pdf
出典：高度サイバー攻撃への対処におけるログの活用と分析方法
最終更新:2022.5.23
https://www.jpcert.or.jp/research/apt-loganalysis.html

◆ ADフォレストのリストア手順は明確ですか？

出典：ADフォレストの復旧 – AD フォレスト復旧計画の考案
最終更新:2022.9.22
https://learn.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/ad-forest-recovery-devising-a-plan

IT基盤を利用する限り、業務停止の危険がある

- Kerberos KDCの脆弱性
- Netlogonの特権昇格の脆弱性

出典：2014年11月 Kerberos KDC の脆弱性に関する注意喚起
最終更新:2014.11.19
https://www.jpcert.or.jp/at/2014/at140048.html
出典：Netlogon の特権の昇格の脆弱性 (CVE-2020-1472) への早急な対応を
最終更新:2022.09.25
https://www.jpcert.or.jp/newsflash/2020091601.html

復旧でゼロトラストを実現

ADサーバーをフォレスト単位でリストア、サーバー全体をベアメタルリスト(ADサーバーの迅速な復旧が可能)

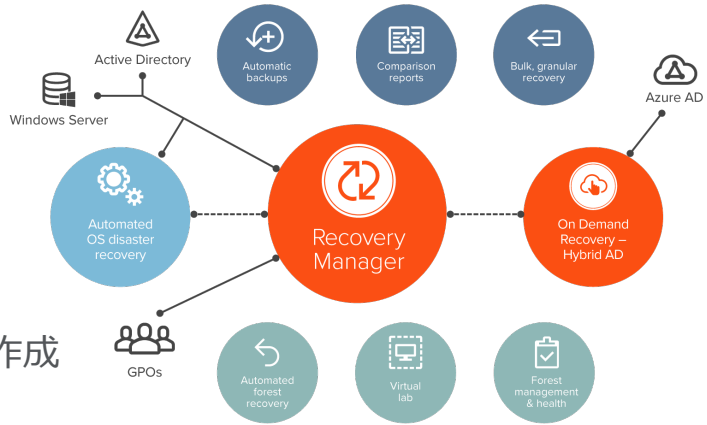
- Recovery Manager for Active Directory

AD復旧：Recovery Manager

人的なミス、セキュリティ侵害、災害発生時の復旧

オブジェクト、属性単位、ディレクトリ単位でADリストアが可能。製品に以下の機能が含まれる。

- バックアップの自動実行
- 稼働中のAD環境とバックアップデータの比較から変更点を確認
- 属性単位でADオブジェクトを復元
- 復元後、ドメインコントローラーの再起動が不要
- OS、システム状態のバックアップ（BMRバックアップ）
- BMRバックアップの暗号化
- BMRリカバリー用のドライバーを含んだブータブルメディアの作成
- マイクロソフト社が推奨する40以上の復旧手順を自動化




Quest
Where Next Meets Now.