DIGITAL GUARDIAN®

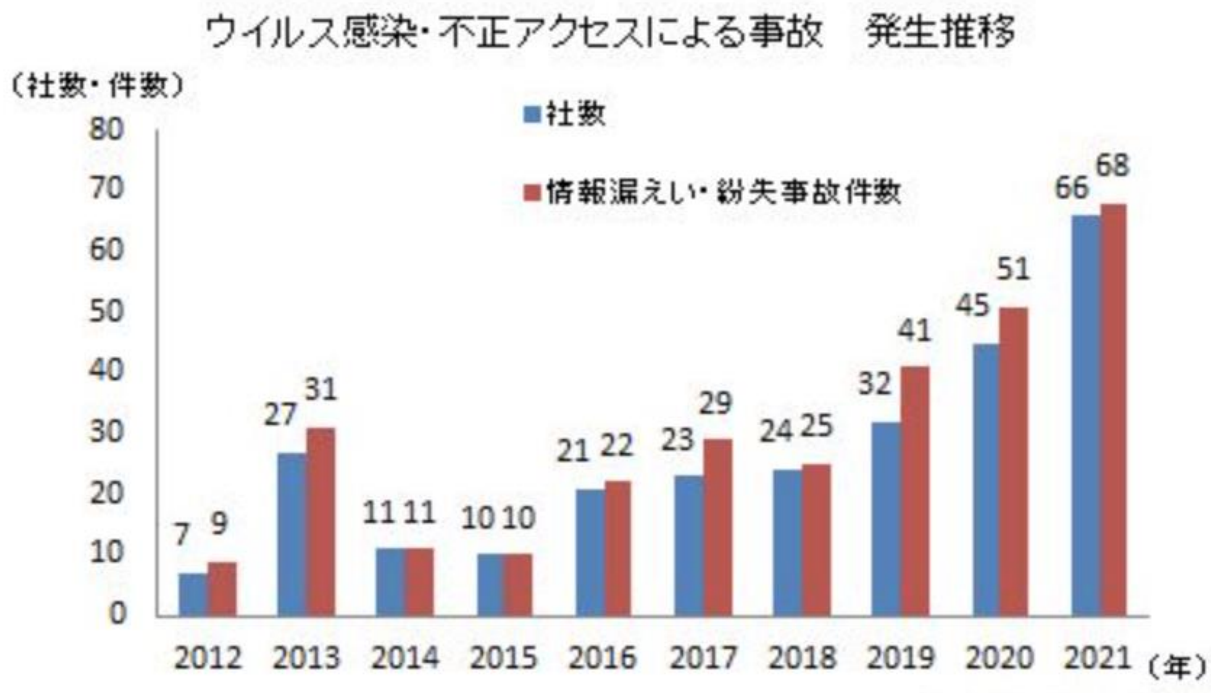
情報漏えいリスクの新しいトレンドと対策

山西 毅
デジタルガーディアン
日本法人 執行役社長 兼 APAC地域担当 Managing Director

情報漏えいリスクトレンド

2021年

- 事故件数は137件（前年比33.0%増）
- 「ウイルス感染・不正アクセス」は事故件数・社数ともに最多を更新

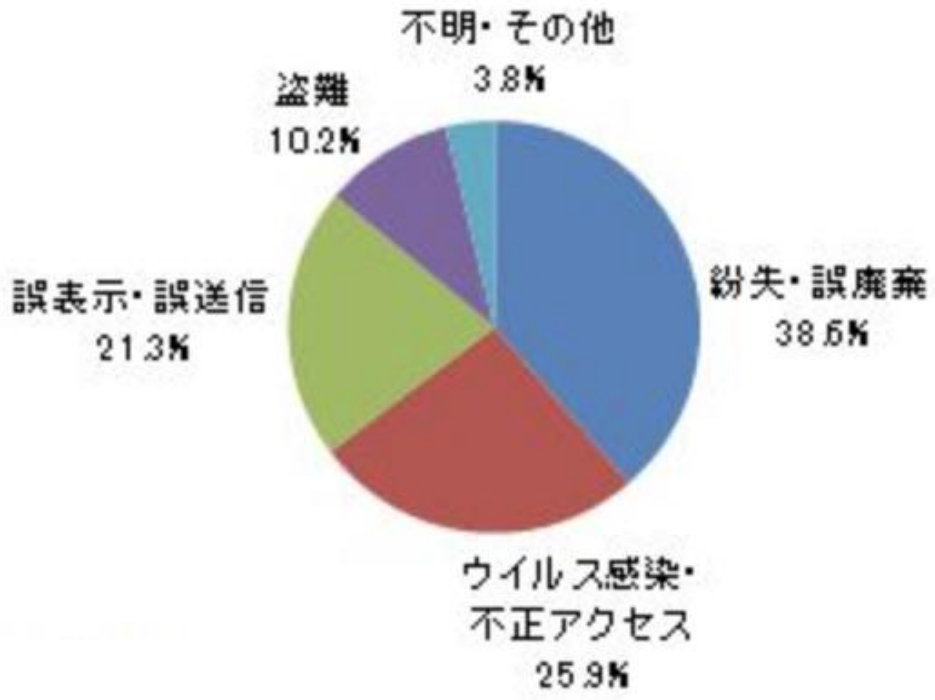


東京商エリサーチ調べ
上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の137件 574万人分（2021年）

情報漏えい対策にも変化が必要

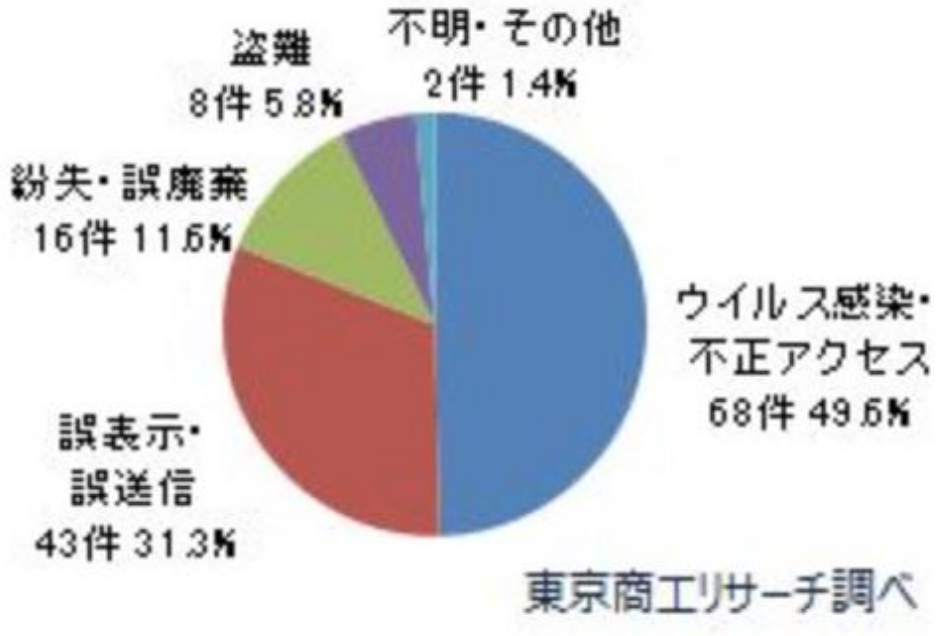
- 新型コロナウイルスの感染拡大による情報漏えい傾向の変化

2019年



出典：東京商工リサーチ
「上場企業の個人情報漏えい・紛失事故」調査（2019年）

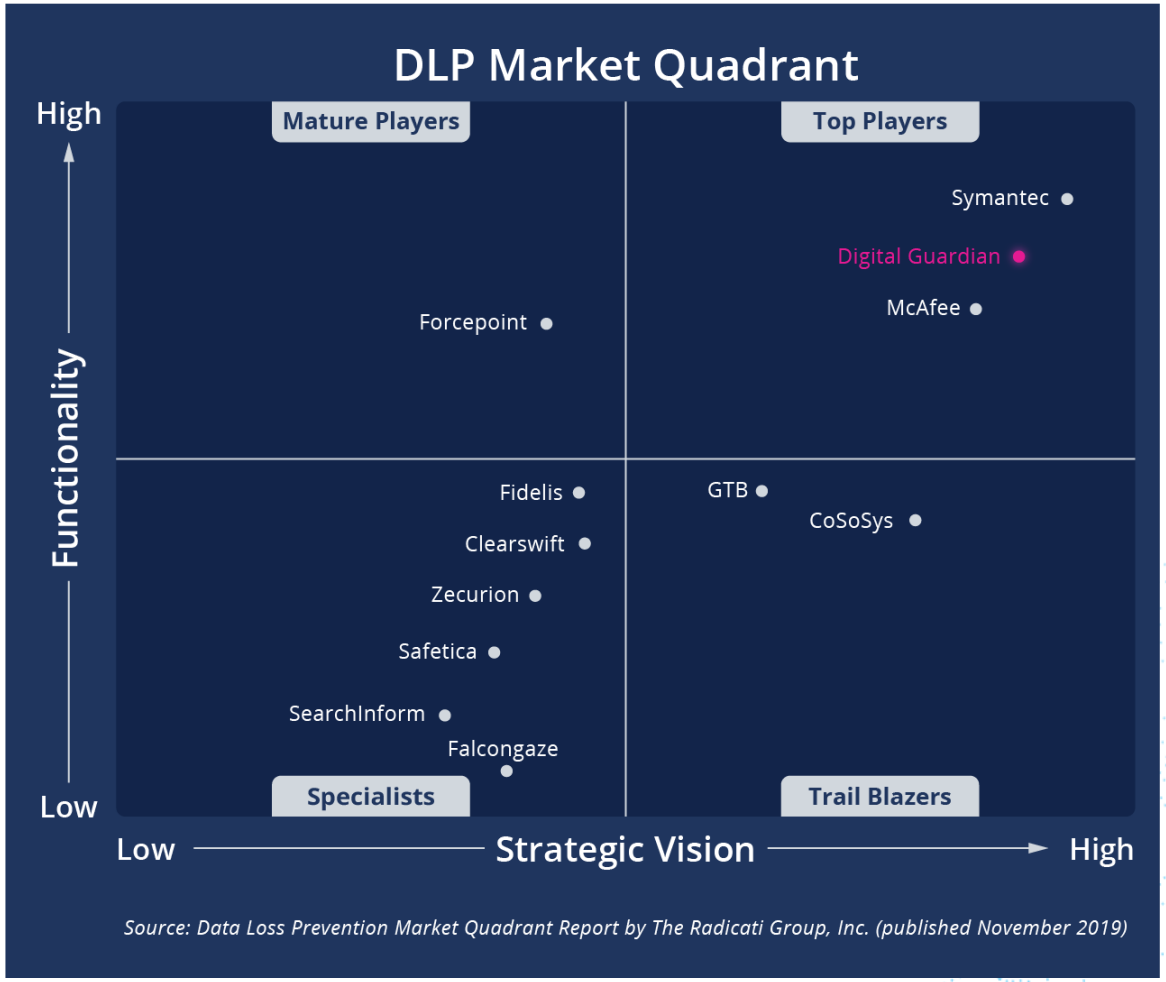
2021年



出典：東京商工リサーチ
「上場企業の個人情報漏えい・紛失事故」調査（2021年）

情報漏洩リスク対策方法と
デジタルガーディアンを選ぶ理由

デジタルガーディアン：
エンタープライズDLPの業界リーダー

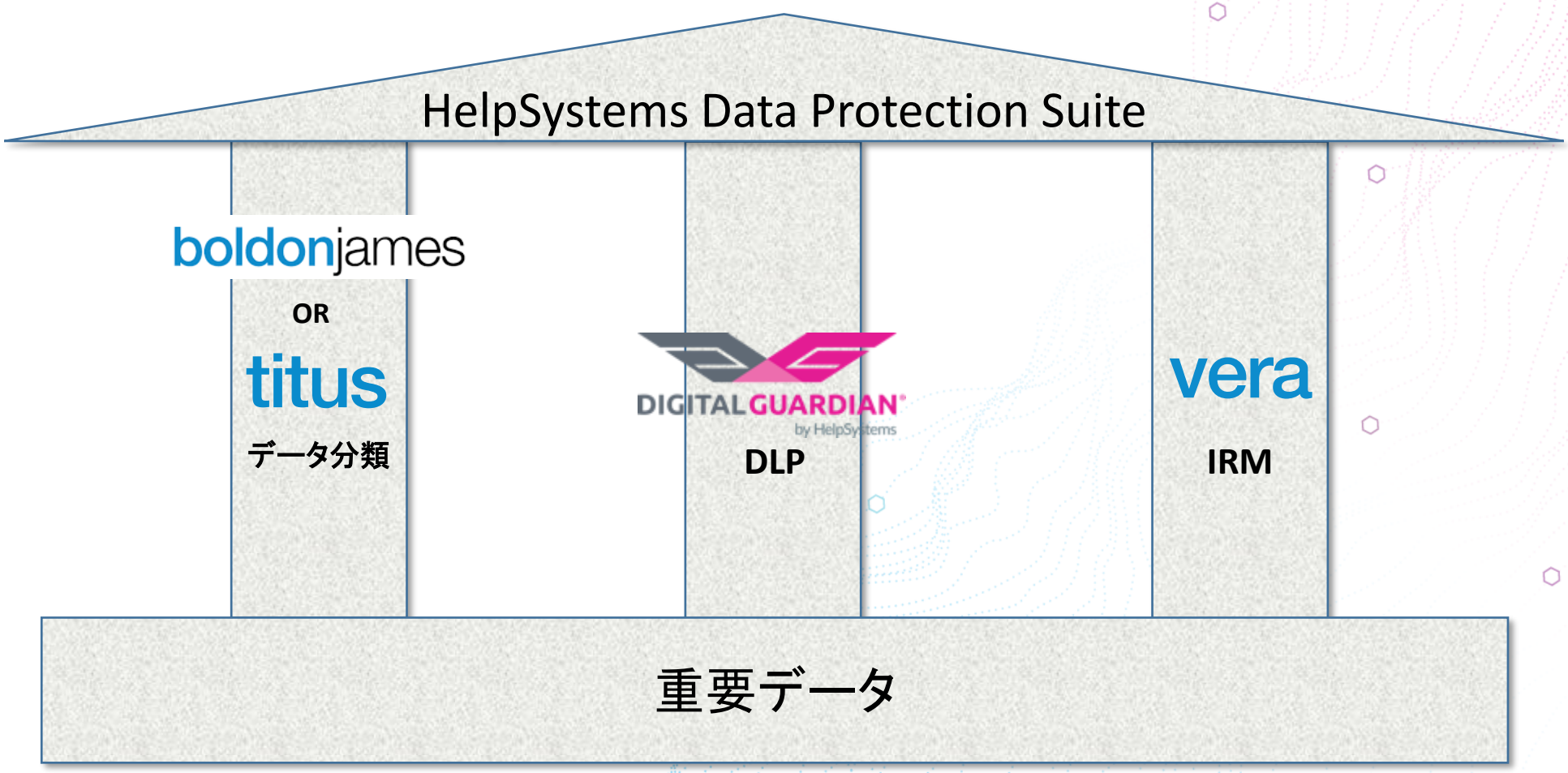


イベント検知、追跡能力

クロスプラットフォーム

クラウド型可視化、分析エンジン

デジタルガーディアン（ヘルプシステムズ）が提唱する包括的な情報保護ソリューション

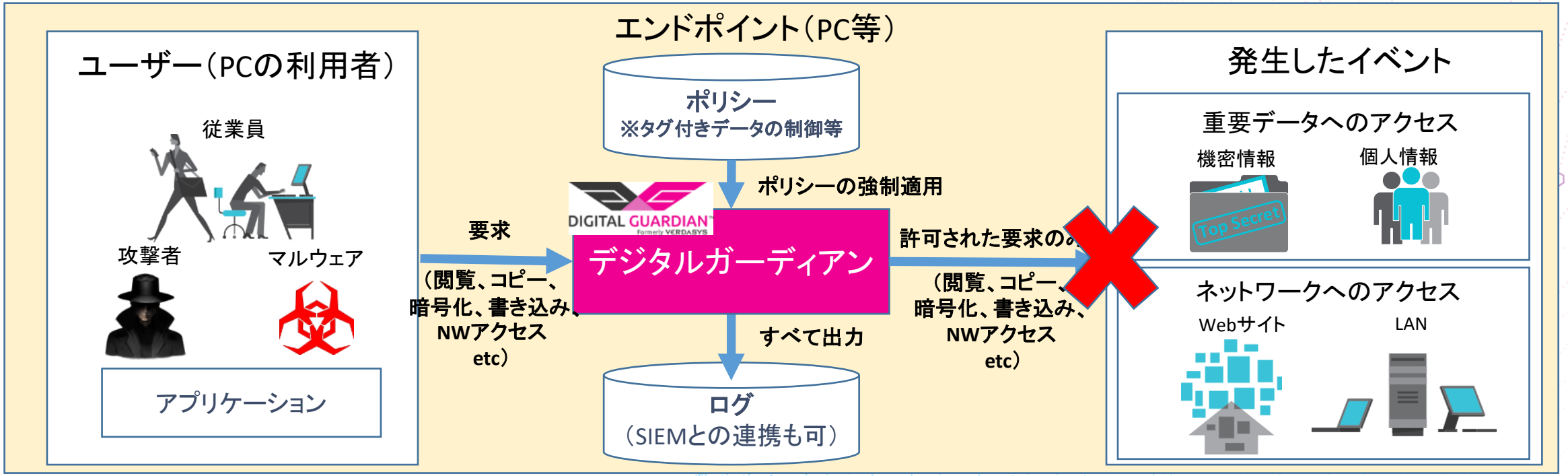


情報漏洩リスク対策

	情報漏洩リスク対策として考慮すべき事項	デジタルガーディアンの強み
1	平常時からのロギング、リスク行動の可視化	ポリシー不要ですべて可視化
2	データの重要性分類、漏洩防止	専用タグ付けと柔軟なポリシー
3	リモートワーク対応	オフライン、リモート会議ツール対応
4	誤操作、誤送信時のリカバリー	2022新機能（IRM）
5	2次漏洩の防止	2022新機能（IRM）
6	データ破壊防止（ランサムウェア）	アプリケーションホワイトリスト
7	社員教育	カスタマイズ可能な違反プロンプト
8	既存ツールとの連携による効果向上	API連携、MIP、SIEM等

対策1：
従業員及び攻撃者の行動を360度可視化を実現

- 従業員、攻撃者、マルウェアによるエンドポイント内の活動は、デジタルガーディアンを必ず経由します。
- デジタルガーディアンはカーネルレベルで稼働します。**システム管理者権限を奪取されても、デジタルガーディアンのプロセスが停止されることはありません。**



対策1：
あらゆるイベントを検知、ロギング、可視化

- アプリケーションの挙動を独自の手法で解析し、データの流出を検知

ファイル関連の操作
- コピー、移動、名前を付けて保存、圧縮等
- USBデバイス（ベンダー、製品名、シリアル番号）
- クラウドストレージとの同期

ファイルの保存元と移動先
- リモート、固定ディスク、リムーバブルメディア
- クラウドストレージ
- カット＆ペースト、プリントスクリーン

流出したデータ
- メールの受信者
- USBメモリ等に保存したデータ
- 印刷やCD/DVDに焼いたータ

システム関連
- ログイン、ログオフ
- レジストリの変更
- プロセスの起動

アプリケーション
- 名前、会社、バージョン
- MD5、SHA1、SHA256
- アクセスしたデータ

ネットワーク操作
- ネットワーク接続（ポート、プロトコル、ドメイン名、IPアドレス）
- アップロード、ダウンロード
- メール（送信者、受信者、本文、添付ファイル）

Active Directory関連情報
- コンピュータ名
- ユーザー名
- グループ、ドメイン　等

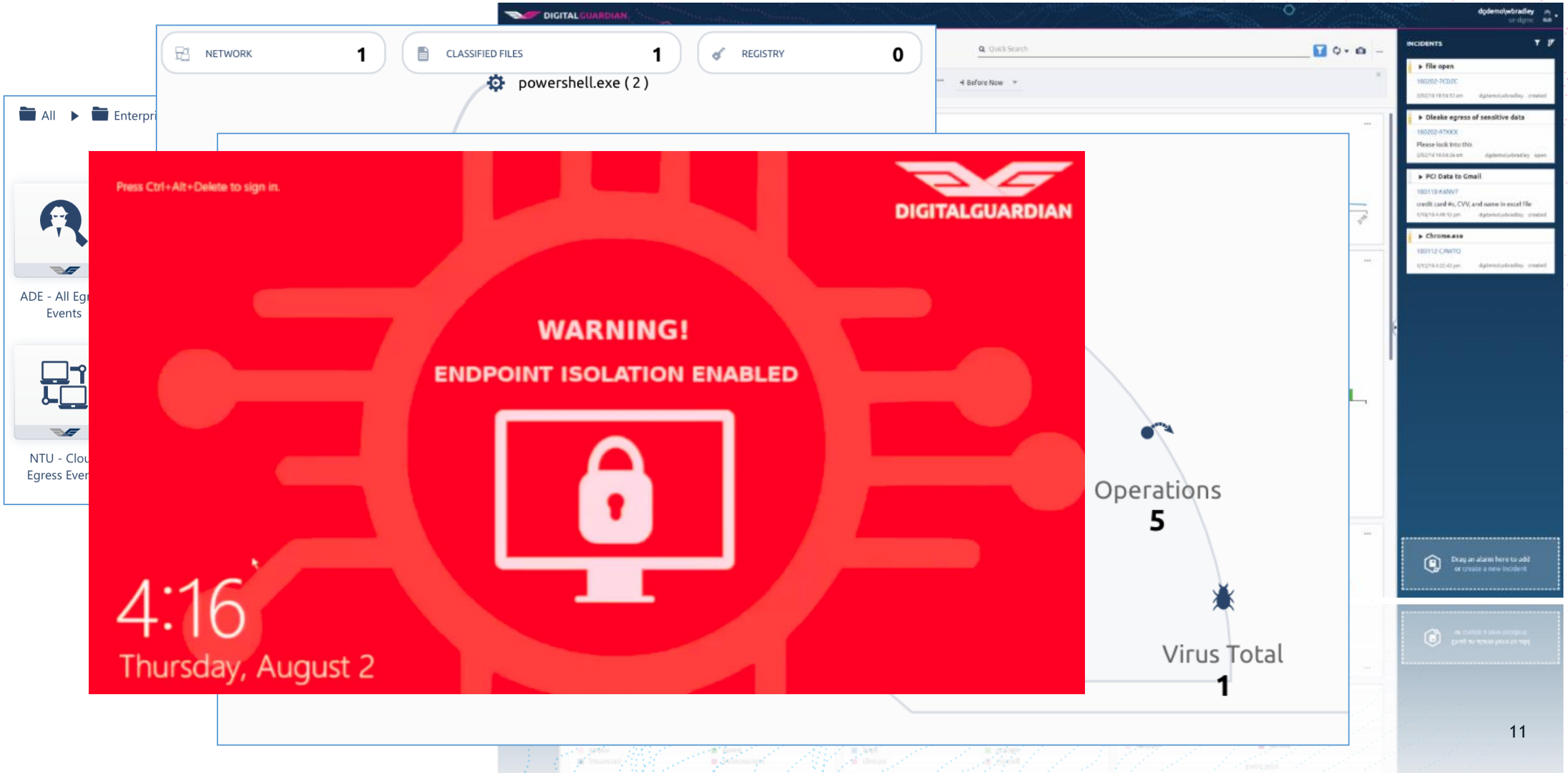
Gartner

DG（注）は、システム内のあらゆるアクションを検知し、制御することができます。高度なマルウェアのみならず、技術的に熟練したインサイダーによる悪意のあるデータ盗難の検出にも成功しています。

（出典）Enterprise Content-Aware DLP Solution Comparison and Select Vendor Profiles, Gartner Research （注）原文は、旧社名の「Verdasys」

DIGITAL GUARDIAN®

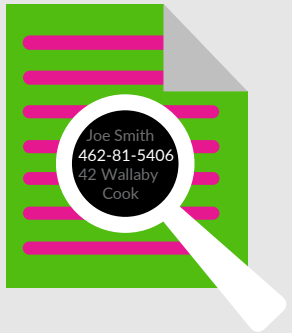
対策1：
すべての脅威を可視化するクラウド型Log分析基盤



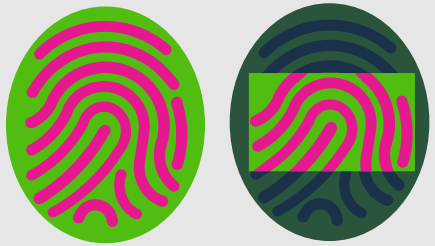
対策2：
重要データの識別が重要です

- DGでは、以下の分析方法が利用可能です。

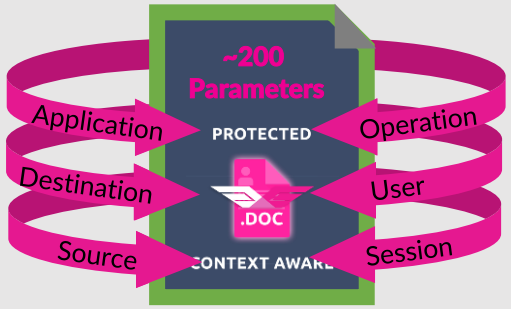
ファイルの内容（コンテンツベース）



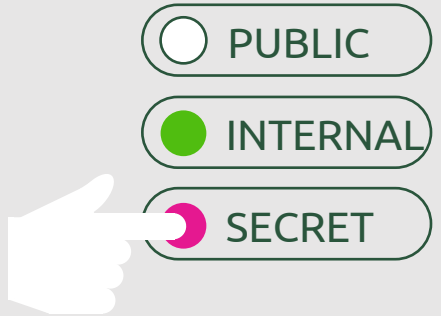
フィンガープリント



コンテキスト

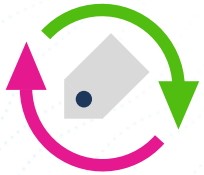


ユーザーによる判定



重要性の変更は不可

派生したファイルへの重要性の継承

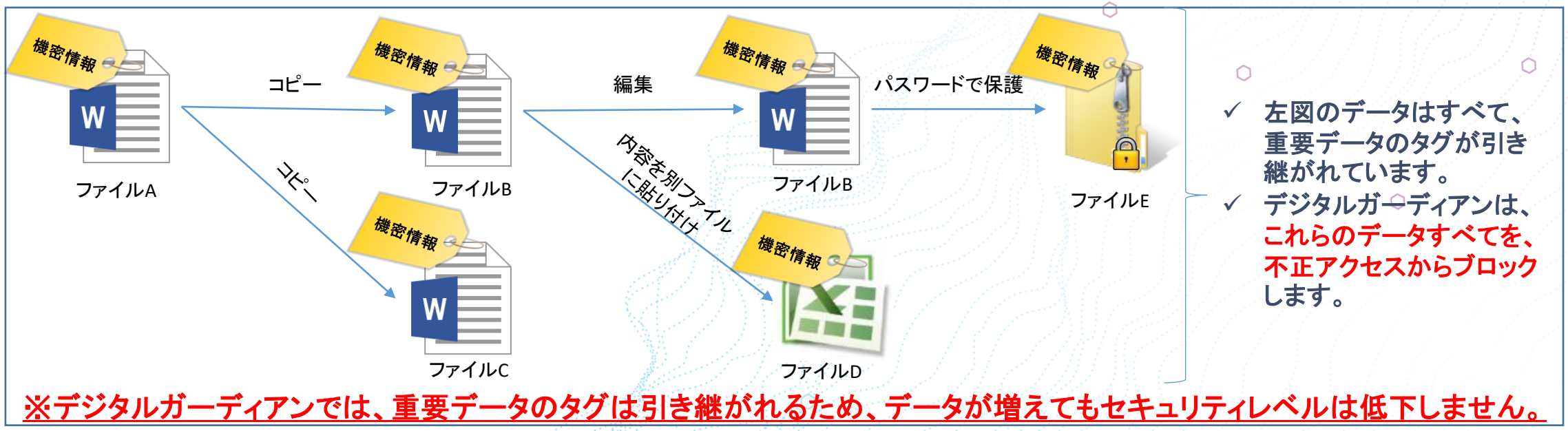


判定結果の持続性

DIGITAL GUARDIAN®

対策2：
デジタルガーディアンは重要データを自動的に探索し、重要データの動きを追跡

- デジタルガーディアンは、**エンドポイント内を自動的に探索し**、重要データの条件に合致する**データを自動的に識別し、タグを付与**します。
  - デジタルガーディアンは様々な切り口を組み合わせて、重要データを定義することが可能です
    【切り口例】正規表現、キーワード、格納場所、作成者、アプリケーション
- 重要データとして**タグが付与**されると、デジタルガーディアンは当該データを**継続的に監視**していきます。
  - タグが付与されたデータについては、**コピーや別名保存等によって派生したデータ、さらに暗号化されても、同じタグは引き継がれます。**
  - デジタルガーディアンでは、**タグが付与されている間**、当該データは重要データとして**保護対象であり続けます**。



※デジタルガーディアンでは、重要データのタグは引き継がれるため、データが増えてもセキュリティレベルは低下しません。

対策3：
オフライン時やリモート会議ツールが落とし穴

リモートワーク需要の高まりに伴い自宅での社用PC利用やWeb会議アプリの利用機会が増え、新たな情報漏洩リスクが課題となっています。デジタルガーディアンDLPエージェントは インターネット非接続時も動作を継続、またWeb会議アプリ利用時の情報漏洩を防止します。

対応できる主なイベント

チャット送信メッセージ内にキーワードを見つけたらブロック
- クレジットカード番号、品番、レシピ、医薬品成分等

会議中のファイル共有をブロック
- 例）重要情報（タグの付いたファイル）共有のブロック

異なるテナントIDからの会議への出席依頼のブロック

情報漏洩対象者の追跡
- 送信者、送信ファイルの確認、各種ロギング

対策3：
Teams, Zoom, Slack, Skypeへの対応（Webexも予定）

- Microsoft Teams
  - MS Teams (themes.exe) へのすべてのファイルのアップロードを制御します。
  - MS Teams (themes.exe) への分類されたファイルのアップロードを制御します。
  - ユーザーのオンラインOneDriveアカウントからMS Teams (themes.exe)へのファイルのアップロードを制御する。
  - 機密コンテンツを含むMS Teams (themes.exe)のチャットを制御します。
- Slack
  - Slack（slack.exe）によるすべてのファイルアップロードを制御します。
  - Slack（slack.exe）による機密ファイルのアップロードを制御します。
  - 機密扱いのコンテンツを含むSlack（slack.exe）チャットを制御します。
- Zoom
  - Zoom（zoom.exe）でのファイルダウンロードを制御します。
  - Zoom（zoom.exe）でのすべてのファイルアップロードを制御します。
  - Zoom（zoom.exe）での機密ファイルのアップロードを制御します。
  - Zoomの画面共有機能を制御します。
- Skype
  - Skype（skype.exe）へのすべてのファイルのアップロードを制御します。
  - Skype（skype.exe）への分類されたファイルのアップロードを制御します。
  - 機密コンテンツを含むSkype（skype.exe）のチャットを制御する。

対策4, 5
重要データ+IRMにより、守備範囲が拡大

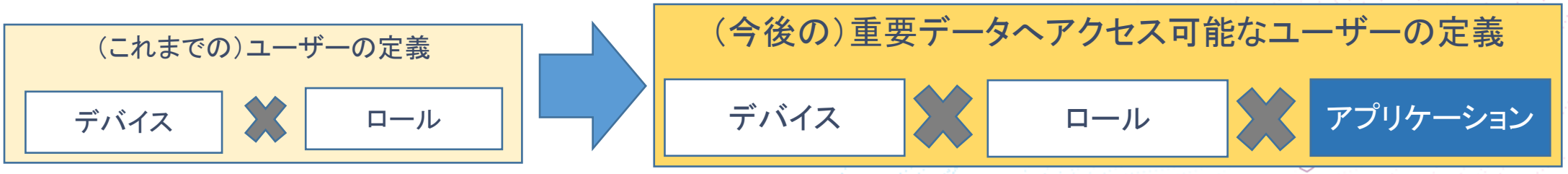
参考：動画「An Introduction to Microsoft Azure Information Protection 」をもとに作成

対策4,5：
Vera IRMとの連携（2022新機能）

- VeraとDGを連携させることで、以下のメリットが生まれます。
  - DLPでは対応が難しかったデータ漏えい対策
    - 2次漏えい
    - 誤送信
  - 例外の多い業務へのポリシー適用
    - DLPのポリシーによるブロックよりも、非定型業務については、「ファイルさえ開けなければ良い」という考え方へのシフト

対策6：
DLPの機能を使ったランサムウェア対策

- ランサムウェア被害の急増により、データ漏えい対策に加え、**重要データを破壊から守る必要性**
- 重要なデータへのアクセス可能なユーザーの定義にアプリケーションを追加することで、マルウェア（ランサムウェアを含む）による**重要データの搾取や破壊を確実に防ぐ**ことが可能



【重要なデータへのアクセスにおいて、「アプリケーションの限定」を後押しする背景】

アプリケーションホワイトリストは従来型のアンチウィルスソフトやこれまで普及しているその他のセキュリティコントロールと比較して、未知のマルウェアの攻撃を防ぐことにおいて極めて有効である。

NIST Special Publication 800-167

Guide to Application Whitelisting

会社によって正式に許可されたアプリケーションのみが稼働するように制限されたPCの比率は、2017年迄に現行の20%から50%を超えると予想する。

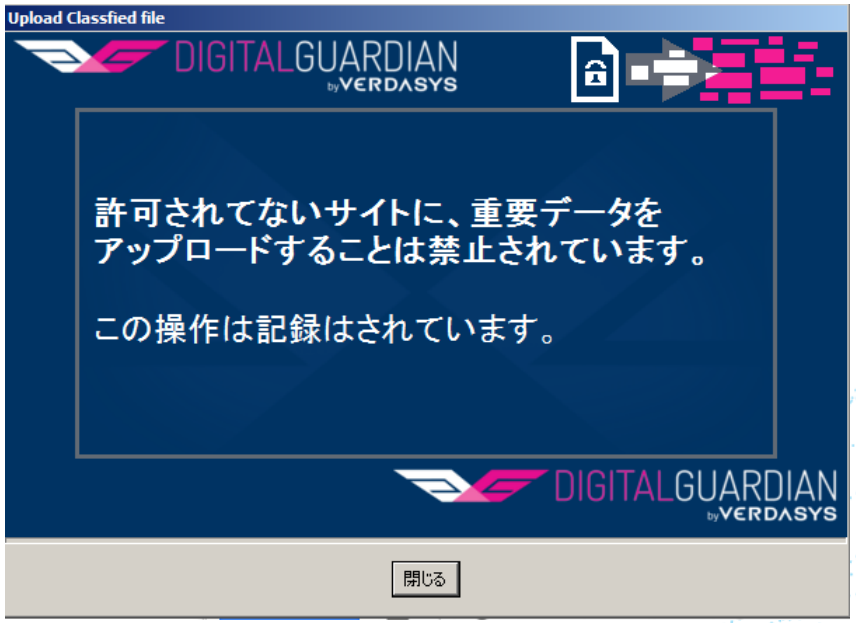
Gartner

対策7：
カスタマイズ可能なプロンプト

- デジタルガーディアンはポリシー違反を検知した際、違反者に対し、リアルタイムで違反を伝えるプロンプトを表示できます。
- プロンプトはHTML形式であるため、自由にカスタマイズすることが可能です。

（例）

（1）ブロックする場合



（2）警告を出し、続行するには理由を入力させる場合

対策8：
既存ソリューションを活かす

- マイクロソフトMIPとの連携
  - MIPラベルに基づいたDLPポリシーの適用
  - DGによるMIPラベル付与（近日実装予定）

- SIEMへのLog取り込み
  - Splunk, Qrader、等

- API
  - DG Log解析基盤ARCとの連携を提案

まとめ

まとめ：これからの情報漏洩対策

Digital Guardian DLPとVera IRMにより多くの情報漏洩シナリオに対応

	情報漏洩リスク対策として考慮すべき事項
1	平常時からのロギング、リスク行動の可視化
2	データの重要性分類、漏洩防止
3	リモートワーク対応
4	誤操作、誤送信時のリカバリー
5	2次漏洩の防止
6	データ破壊防止（ランサムウェア）
7	社員教育
8	既存ツールとの連携による効果向上

ご静聴ありがとうございました

A New Dawn for
Data Loss Prevention.

A New Day for Digital Guardian.