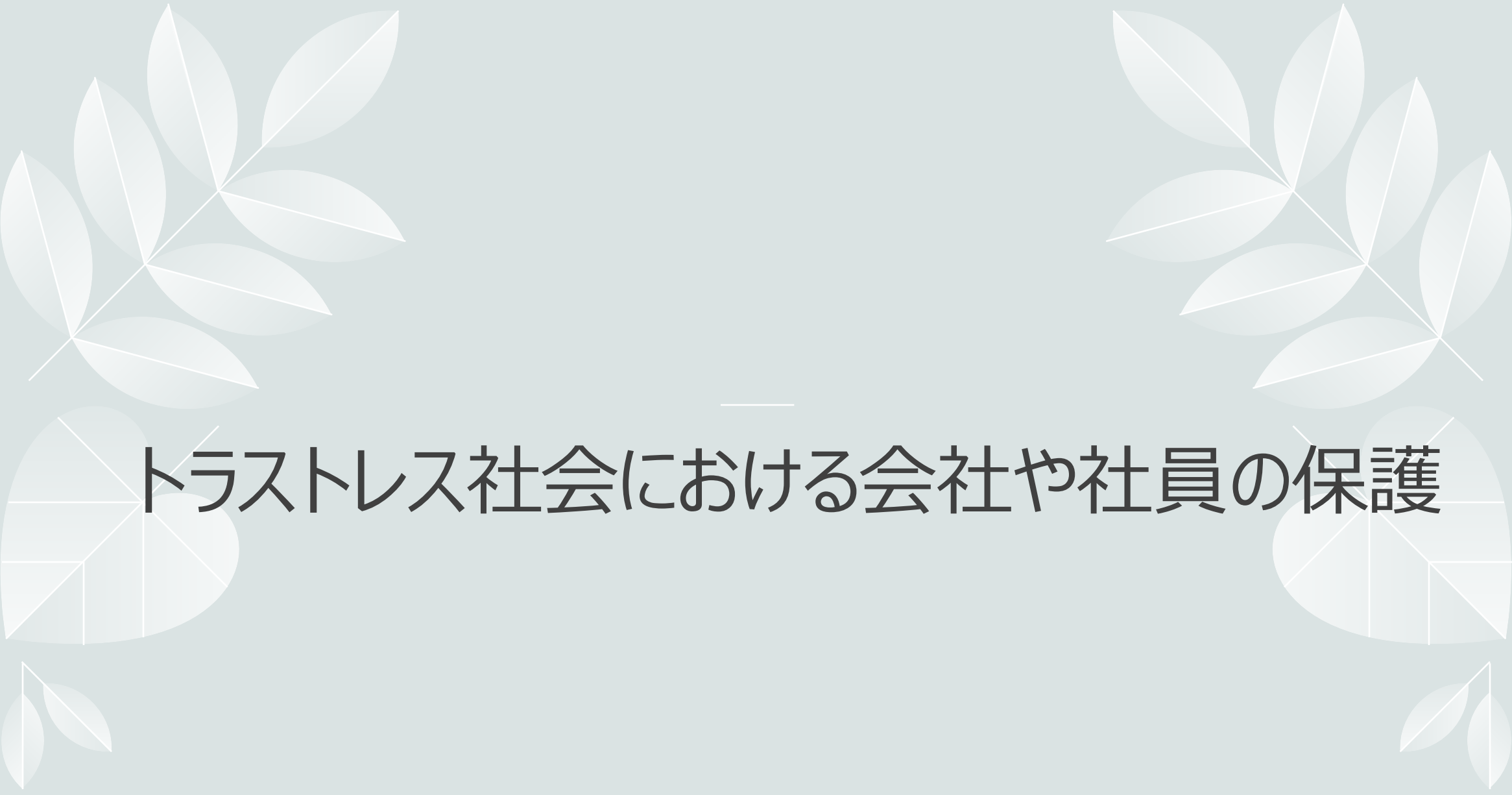


The image features a light gray background with stylized, semi-transparent leaf patterns in the corners. In the top-left and top-right corners, there are clusters of elongated, pointed leaves. In the bottom-left and bottom-right corners, there are larger, more rounded leaf shapes with internal vein details. The central text is positioned between these decorative elements.

# トラストレス社会における会社や社員の保護

# 自己紹介

松村 義弘

株式会社エヌ・エス・アール

代表取締役社長



# 会社紹介

## 株式会社エヌ・エス・アール

- ・独立系コンサルティング会社
- ・社員の約 4 割 自衛隊OB/OG
- ・安全保障関係コンサルティング
- ・アウトソーシング



株式会社エヌ・エス・アールは、安全保障、危機管理、情報通信技術、情報セキュリティ技術、プロジェクトマネジメント等の専門知識を活かし、ナショナルセキュリティ(国家安全保障)分野のコンサルティング業務及びアウトソーシング事業を展開しています。



Our Vision  
— 展 望 —

私たちは、  
▶ いかなる脅威からも生命や財産を脅かされることのない安心・安全な社会  
▶ 働き続けることを望む人たちが充実した日々を送ることができる社会  
を目指します。



Our Mission  
— 使 命 —

私たちは、ナショナルセキュリティ(国家安全保障)分野のコンサルティング業務、アウトソーシング事業等を通じて、日本国民の生命と財産を守る安全保障に貢献し、「小さいけど、なくてはならない会社」と評価されるよう努めます。



Our Value  
— 価 値 —

- 感謝と応援**  
私たちは、日本の安全保障に関わる人たちに感謝し、応援します。
- お客様との信頼関係**  
私たちは、現場に寄り添い、お客様の声に真摯に耳を傾け、信頼関係を築きます。
- 革新と進化**  
私たちは、失敗を恐れず、新しい考え方や技術を積極的に取り入れ、絶えず進化し続けることで、お客様のニーズに応えます。
- チームワーク**  
私たちは、信頼と協調を大切にし、すべての社員が一体となって目標達成に向けて取り組みます。
- 個人の充実**  
私たちは、当事者意識を持って仕事に取り組み、自分の言動に責任を持ちます。また、向上心を持ち続け、公私共に調和のとれた生活を大切にします。

# 本日のアジェンダ

---

- ・ トラストレス社会とは
- ・ 内部脅威が生むジレンマ
- ・ 解決の方向性
- ・ 解決策の例
- ・ まとめ



トラストレス社会とは





# セキュリティ戦略的な ゼロトラスト

「何も信頼せず、常に検証  
する」

社内外問わずすべてのアク  
セスを疑い、検証することで、  
情報資産を守る



# 社会的なゼロトラスト

- ・フェイクニュース
  - ・偽情報
  - ・法令違反・不正行為
- などなど



# トラストレスな社会

信頼が失われた社会

しかし、

本来は、人間の営みには  
信頼は不可欠

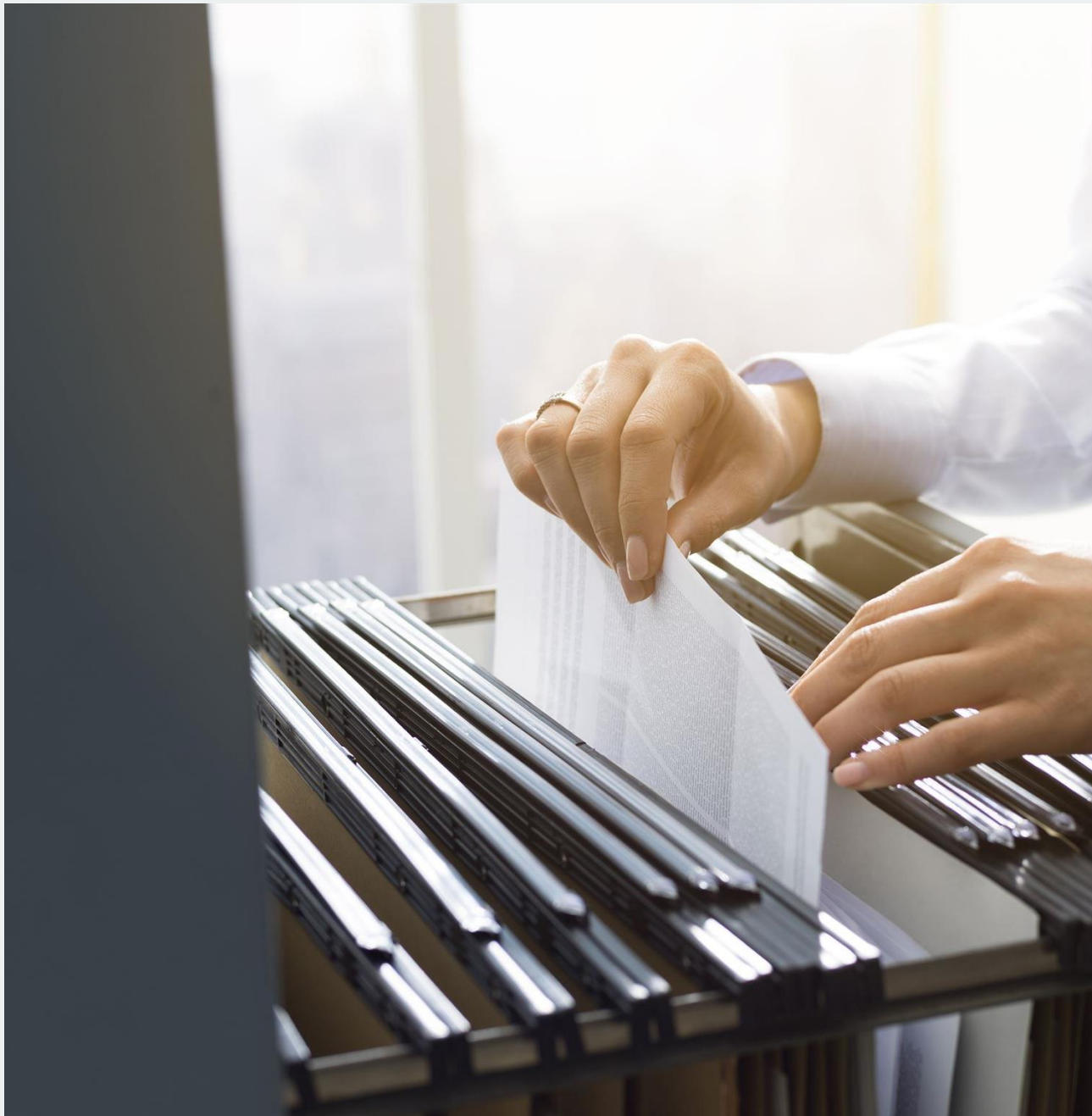
内部脅威が生むジレンマ





# 内部脅威とは

企業や組織の内部にいる  
従業員、契約社員、パート  
ナー企業の関係者、元従  
業員などが、意図的または  
過失に引き起こすセキュリ  
ティリスク



# 内部脅威の具体的な種類①

## 悪意ある社員の脅威

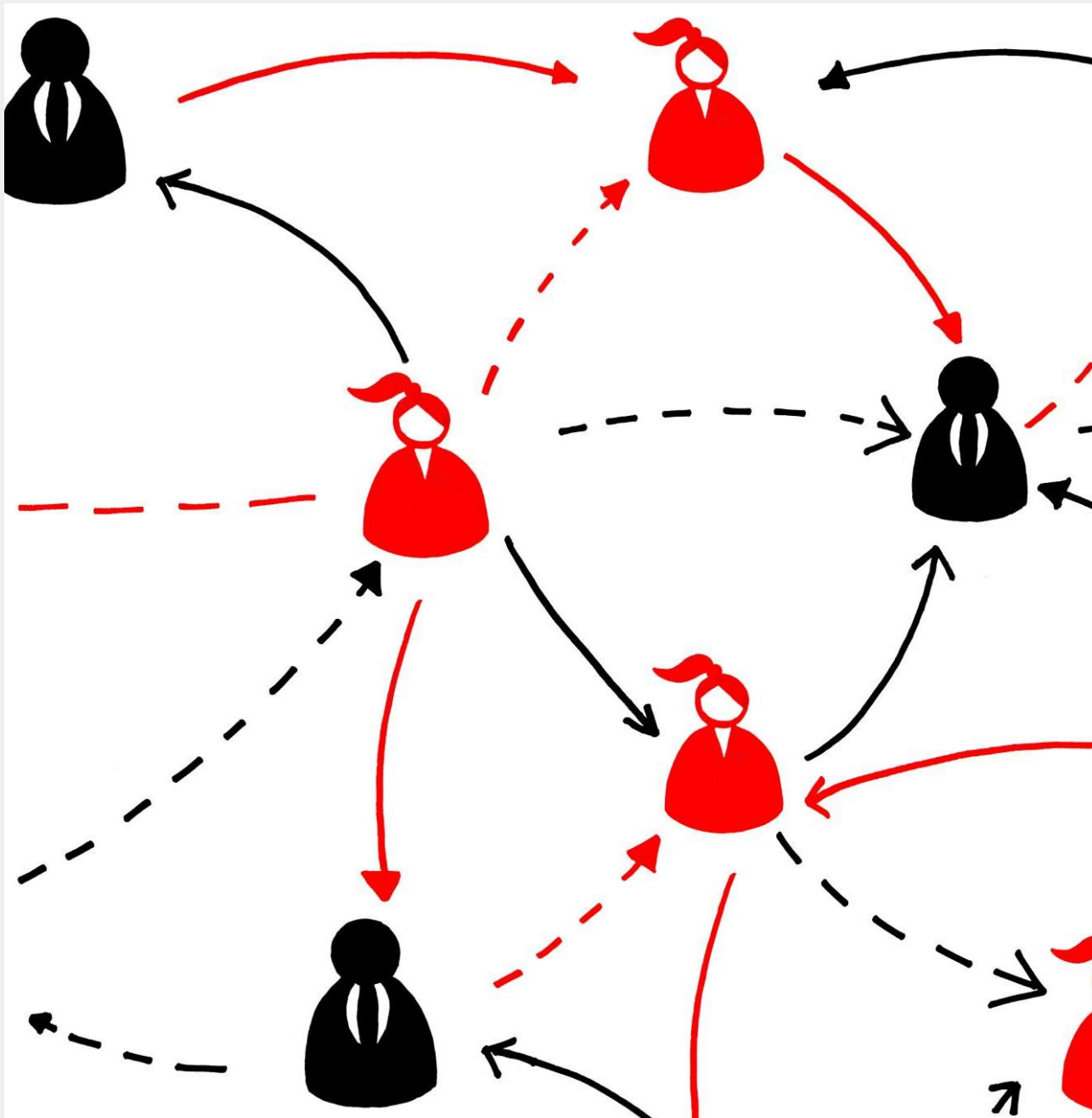
- ・データ窃取
- ・サイバーテロ行為
- ・詐欺・横領
- ・復讐目的の破壊行為



## 内部脅威の具体的な種類②

### 無意識な過失

- ・誤送信・誤操作
- ・パスワード管理の不備
- ・マルウェア感染
- ・アカウント乗っ取り



## 内部脅威がもたらす リスク

- ・情報漏洩による信用失墜
- ・不正行為による財務的損失
- ・サイバー攻撃による業務停止



# 社員が加害者となる要因

- ・プレッシャーの影響
- ・無理解の問題
- ・仕組みの不備

# 内部脅威が生む ジレンマ

利便性とセキュリティ確保

外部対策と内部対策の  
コストバランス



# 解決の方向性





## 「守る」視点の重要性

- ・守る視点は信頼と安全を築く基盤
- ・疑うのではなく、支える
- ・疑う視点は不安や防衛を生む、守る視点は協力と安心を促進する



# 業務効率を損なわない 設計と利便性のバランス

- ・業務効率を維持しつつ、  
利用者の利便性を高める  
設計が重要
- ・使いやすさと作業効率を  
両立する設計で業務の質  
を向上させる

# 解決策の例





thinklogical

「光ファイバKVM &  
セキュアマトリクス」



**Secure Matrix Switch**



**Fiber-Optical  
KVM**



**SMP Appliance**

# 従来の映像表示システムで起こりうる 情報セキュリティ事故の例

## システム端末からの 情報漏洩事故



HDDを抜き出して持ち去ったり、  
USB端子から情報をコピーするなど  
して情報を抜き取る

各システム端末が足元にあるので、  
その端末からハード的に、あるいは  
ソフト的に直接データを取り出すこ  
とができるしまう

## 映像配線からの 情報漏洩事故



天井や壁の中を通っている映像配線を切  
断してつなぎ、モニタリングできてしま  
う

映像配線は切断してケーブルを足すこと  
ができるしまうので、途中でケーブルの  
経路を変更することで映像が参照できて  
しまう

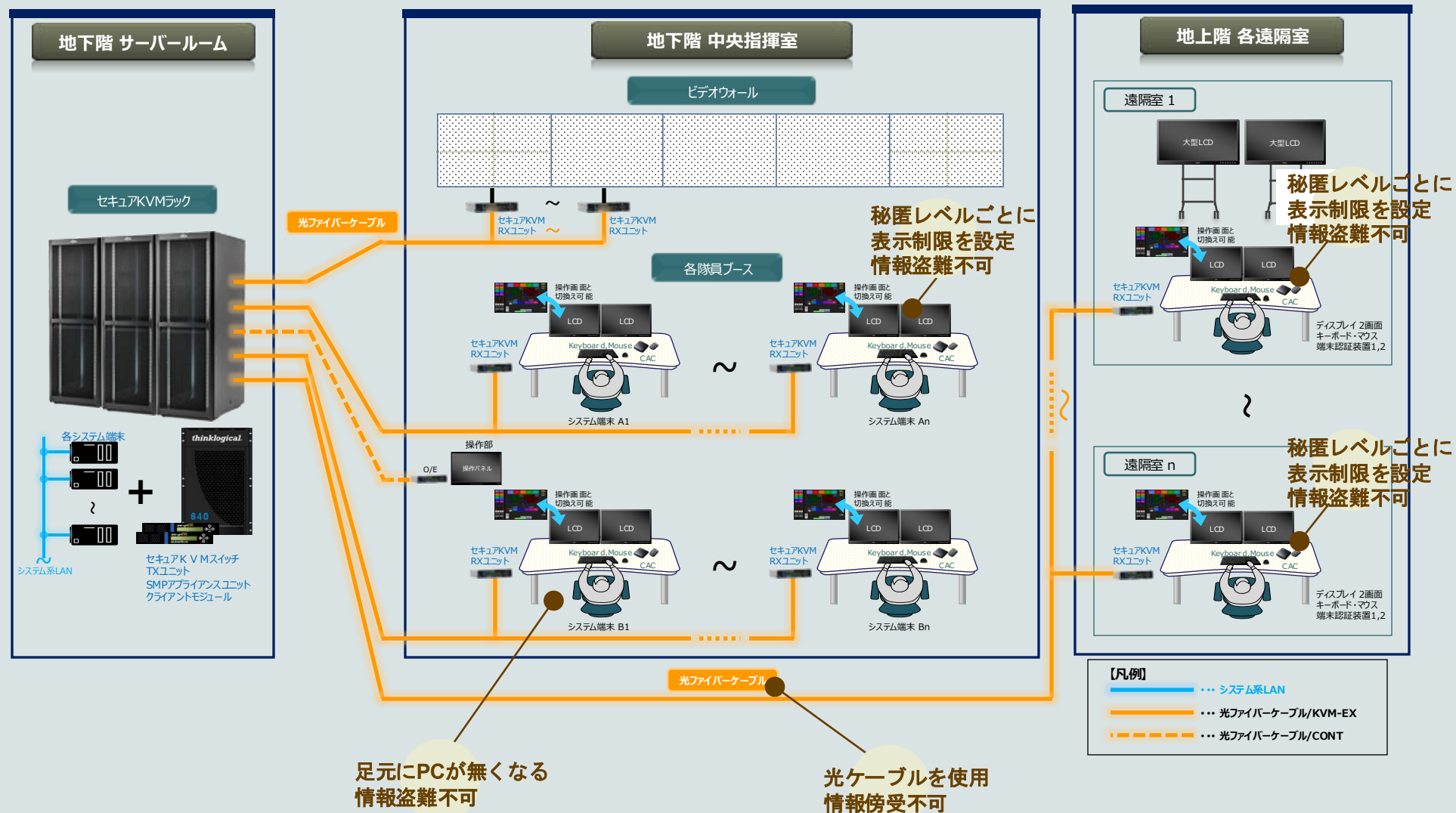
## 特定区画外の 表示映像の漏洩事故



機密情報が表示されているモニターを、  
見てはいけない人も見れてしまう

システム端末の機密区分、表示範囲ご  
とに限定した設定ができないため、表  
示範囲全ての区画で映像が参照できて  
しまう

# 新セキュアKVMシステムの構成イメージ





## 導入のメリット

- ・情報の抜き取りが不可能

⇒やる気が起こらない

⇒疑われない安心

- ・使いやすさと作業効率の向上

# Resecurity Risk™

## デジタルリスクモニタリング

デジタルリスク管理を自動化し、  
ダークウェブ、データ漏洩、資格情  
報の侵害、ネットワーク感染、その  
他のセキュリティインシデントによる  
重要な変化を即座に把握できる



## Risk™

リスクを測定してセキュリティ体制を管理する  
監視ソリューション



サイバーセキュリティの対策は、時間をかけずに行うことが求められます。しかし短い時間では潜在的な盲点やセキュリティギャップなどに気づくことは困難です。Risk™ はデジタルリスクの管理を自動化。内部および外部において、組織に影響を与える行動に対するアラート発信とセキュリティの包括的な可視化を実現します。ダークウェブやデータ侵害、資格情報の侵害、ネットワーク感染などがもたらす脅威から守るためのセキュリティ体制を管理することができます。

### » リスクの測定

日々のセキュリティスコアは、監視対象のドメイン、IP、ネットワーク、脆弱性、クラウドサービスのすべてのリスクの概要に基づいて評価。スピーディに修復できる実用的なインテリジェンスで、高いセキュリティスコアを達成します。

### » リスクアセスメント

データポイントを精緻化して充実させ、デジタル資産の弱点や脆弱性がどこにあるのかを把握。新しいデータが発見されると、レポートや電子メールで変更や更新が送信されます。

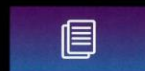
### » おもな特長



組織全体に対する  
詳細なリスク評価



早期に警告する  
セキュリティ通知



自動化された  
セキュリティ体制を  
毎日レポート



状況を  
ダッシュボード  
に表示



リスク管理に  
特化した  
保護型 SaaS

# Resecurity Risk™

## 対象とするリスク

- ・アカウント乗っ取り
- ・ボットネット感染
- ・ビジネスメール詐欺（BEC）
- ・サイバースパイ活動
- ・ブランド評判の悪用
- ・ダークウェブ活動
- ・ドメインスクワッティング
- ・データ侵害
- ・デジタル証明書
- ・公開されたネットワークサービス

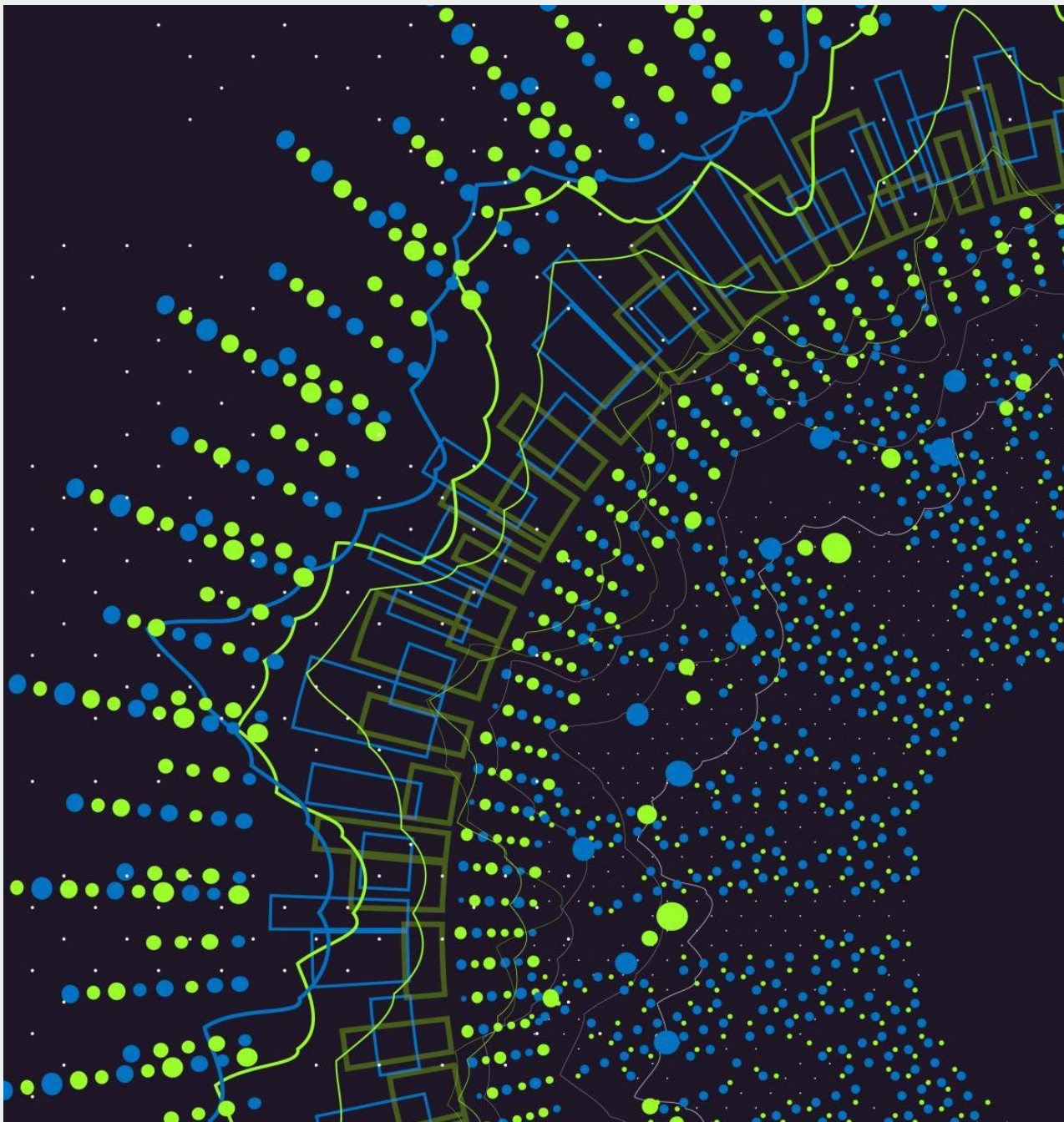
## 機能

### リスク測定

監視対象のドメイン、IP、ネットワーク、脆弱性、クラウドサービスに関連するすべてのリスクを総合的に評価し、日次セキュリティスコアが算出される

### リスク評価

デジタル資産の弱点と脆弱性を理解するために、データポイントを精査し強化します。新しいデータが発見されるたびに、レポートまたはメール通知で変更と更新が送信されます



## 導入のメリット

- ・企業、社員、パートナー会社に関するリスクを把握できる

(可視化してダッシュボードに表示)

- ・リスク発見時に警告（レポートとメール）

# Resecurity Context™

## サイバー脅威インテリジェンスプラットフォーム

日々新たに発生する脅威とセキュリティ課題を、迅速かつ深く調査、分析するためのツール

脅威アクターの調査 etc.



## Context™

企業や政府機関の脅威分析を加速させる  
インテリジェンスプラットフォーム



日々新たな脅威やセキュリティ上の課題が出現する中、効果的なツールを使用してデジタル脅威をタイムリーに、そして詳細に分析することが、これまで以上に重要になっています。

Context™は、分析、予防、調査のワークフローを加速するインテリジェンスプラットフォームです。超高速の検索とデータサイエンスは、アナリストや調査員、SOC/DFIR チーム、リスク管理、Cレベルのセキュリティエグゼクティブの業務を効率化し、サイバー脅威に対する安全に貢献します。

### » 6ステップのプロセス

| 計画                                                                                 | 収集                                                                                     | 変換                                                                   | 分析と提示                                                            | 伝達                                                      | 評価                                                                                            |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------|------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| ユーザーから関心のあるテーマを受け取り、情報収集の基準と方向性を定義。特定の要因に基づいて、AIとMLのメカニズムでソースに優先順位を付け、適切な計画を策定します。 | インデックス化された脅威の痕跡と関連する敵対者のクラウドを継続的に活用して確認します。プラットフォームは、ソース基準に基づいて結果を取得し、さらに充実させてタグ付けします。 | 収集された膨大な量の情報を、暗号解読、言語翻訳、インテリジェンスの生成に適した形式でのデータ削減を通じて、使用可能なデータに変換します。 | 組織が戦略的かつタイムリーな意思決定を行うために、インテリジェンスの提示を様々な形で示せるように最新で、客観的、実用的にします。 | チームメンバー間の円滑な作業のための管理システムを提供。インテリジェンスを使用者が使いやすい形にして伝えます。 | 要件が満たされているか、提供されたインテリジェンスに調整や改善が必要かどうかのフィードバックを提供。お客様の入力に基づいて、結果のスコアリングとMLエンジンのトレーニングに使用できます。 |

# ソリューションの関連

## Risk™

お客様自身による

リスク監視

詳細調査／対策

## Context™

お客様自身による

リスク分析

詳細調査  
／対策



詳細調査  
／対策



## Resecurity

専門家チームによる

- ・レポート
- ・詳細な分析
- ・リスク対策 等

# まとめ



## トラストレスな 社会とは

信頼が失われた社会。

しかし、人間の営みには信頼が必要。

## 内部脅威が生む ジレンマ

内部脅威の重要性が増している。

また、内部脅威が組織運営に関してジレンマを生じさせている。

## 解決の方向性

守る視点は信頼と安全を築く。

業務効率と利便性への考慮も必要。

# 問い合わせ先



Yoshihiro.Matsumura@e-nsr.com



国内代理店 (株) NTTデータ

代理店支援 (株) エヌ・エス・アール

Toru.Takeuchi@e-nsr.com

**Resecurity Risk™** 国内代理店 (株) エヌ・エス・アール

Kei.Kitahara@e-nsr.com