【情報漏洩／流出対策】最前線

～ダークウェブ監視と内部不正対策の リーディング企業が組織内外の視点から語る、 サイバーセキュリティとリスクマネジメント～

AGEST

KELA

Forcepoint

Moderator

株式会社AGEST

マーケティング本部

岡部　康弘

Speaker

KELA株式会社

Head of pre-sales

川崎　真

KELA

Speaker

フォースポイント・ジャパン株式会社

Sales Director

布宮　友寛

Forcepoint

IPA
情報セキュリティ
10大脅威 2024 [組織]

1　ランサムウェアによる被害

2　サプライチェーンの弱点を悪用した攻撃

3　内部不正による情報漏えい等の被害

4　標的型攻撃による機密情報の窃取

5　修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

6　不注意による情報漏えい等の被害

7　脆弱性対策情報の公開に伴う悪用増加

8　ビジネスメール詐欺による金銭被害

9　テレワーク等のニューノーマルな働き方を狙った攻撃

10　犯罪のビジネス化（アンダーグラウンドサービス）

IPA

情報セキュリティ

10大脅威 2024 [組織]

1　ランサムウェアによる被害

2　サプライチェーンの弱点を悪用した攻撃

3　内部不正による情報漏えい等の被害

4　標[illegible]撃による機密情報の窃取

2023年　4位
2022年　5位

[illegible]攻撃（ゼロデイ攻撃）

[illegible]害

7　脆弱性対策情報の公開に伴う悪用増加

2023年　10位
2022年　圏外

[illegible]被害

[illegible]な働き方を狙った攻撃

10　犯罪のビジネス化（アンダーグラウンドサービス）

AGENDA

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

04 まとめ

05 最後にお知らせ

01

情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

04 まとめ

05 最後にお知らせ

情報漏洩とは？

“外部に公開すべきではない情報”

が第三者に渡ってしまうこと

“外部に公開すべきではない情報”

認証情報	個人情報	ノウハウ	契約・取引関連
不正侵入 ランサムウェア被害	顧客を奪われる カード不正利用 詐欺被害など	技術の転用 競合の特許申請	株価への影響 取引停止

報道によるイメージ低下

各種対応によるリソース切迫
業務がストップすることによる売上への影響

“外部に公開すべきではない情報”

認証情報	個人情報	ノウハウ	契約・取引関連
不正侵入 ランサムウェア被害	顧客を奪われる カード不正利用 訴訟被害など	技術の転用 競合の特許申請	株価への影響 取引停止

全てが致命的

報道によるイメージ低下

各種対応によるリソース切迫
業務がストップすることによる売上への影響

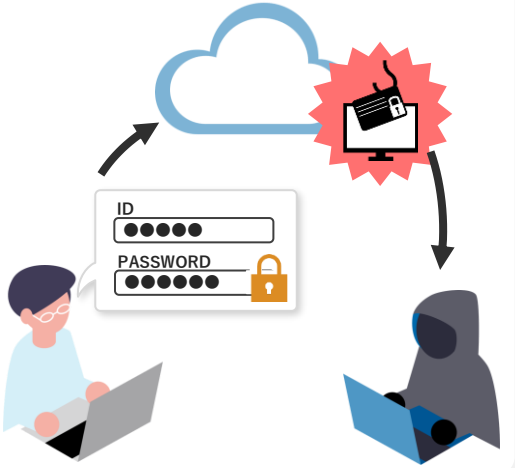
情報はどこから流出する？

自社が攻撃を受けて
情報流出

不正な持ち出しによる
情報流出（内部不正）

取引先が攻撃被害に遭い情報流出
（サプライチェーン攻撃）

利用中のサービス元が
攻撃被害に遭い情報流出



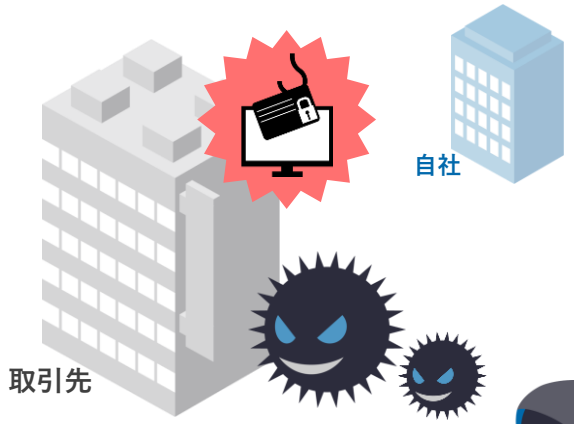
情報はどこから流出する？

自社の努力だけでは
防げない領域がある

情報流出のリスクを
０にすることは難しい

取引先が攻撃被害に遭い情報流出

（サプライチェーン攻撃）



- 自社に関連する機密情報
- 取引先自身の機密情報

利用中のサービス元が

攻撃被害に遭い情報流出

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

04 まとめ

05 最後にお知らせ

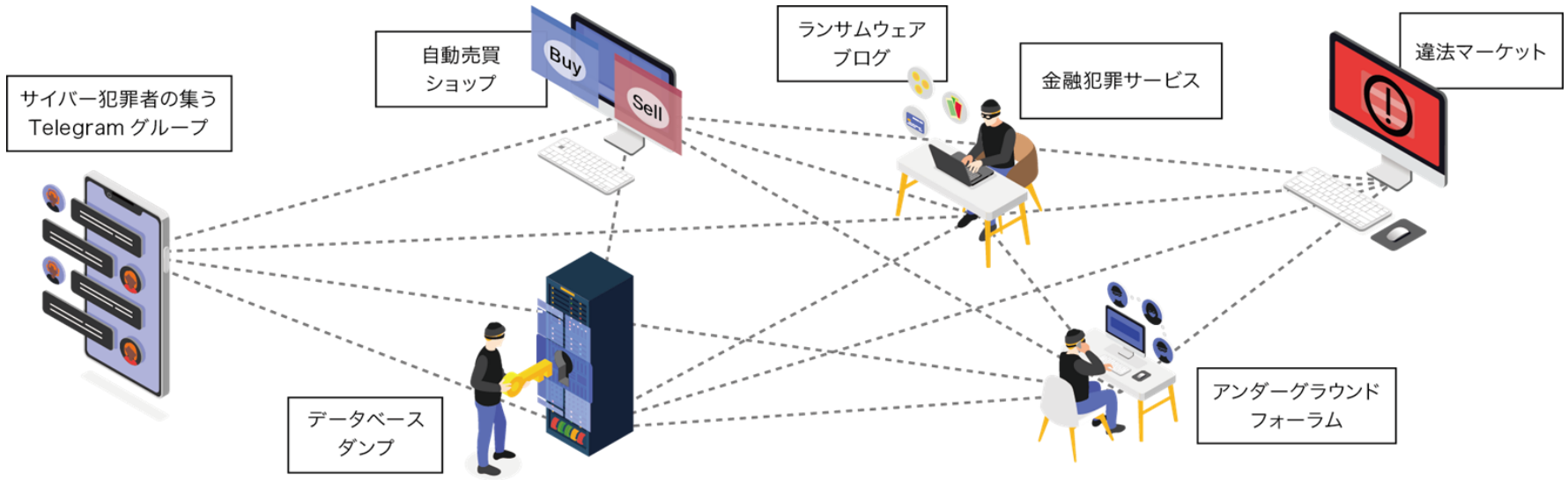
リスクの深掘り

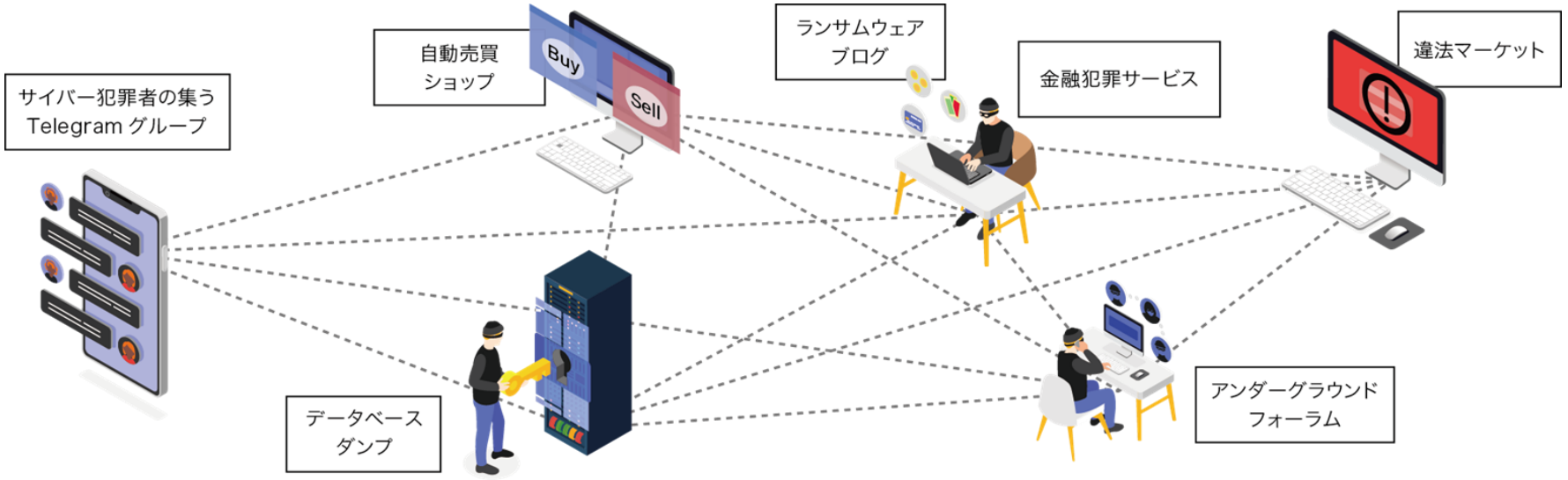
組織の外部という視点

Q.

流出した情報は
どこで、だれが、どのように
扱っているのか？

サイバー犯罪者達は、インターネット上で コミュニティ（エコシステム）を形成





エコシステムでは

不正に入手した情報の公開／売買

マルウェアの売買

犯罪活動の情報収集

などが行われている

Q.

サイバー犯罪コミュニティでは、
どのように情報が公開されるのか？

流出したクレジットカード情報

漏洩カード情報を取り扱う

専用のチャネルが数多く存在

流出したクレジットカード情報

実在するTelegramチャネル

以下が揃った情報は“Fullz”と呼ばれる
- カード番号
- 有効期限
- CVV

日本国内のカードも大量に流通

初期アクセス情報

2023年7月27日　闇フォーラム“Exploit.in”

「世界で最も著名な企業の一つ、年商$1.8B」の

ネットワークアクセスが即日＄5,000で落札

後日、ランサムウェア被害に・・・

2024年5月1日

日本の自動車関連企業（売上規模 $150B）

へのアクセスが＄40,000～で販売

初期アクセス情報

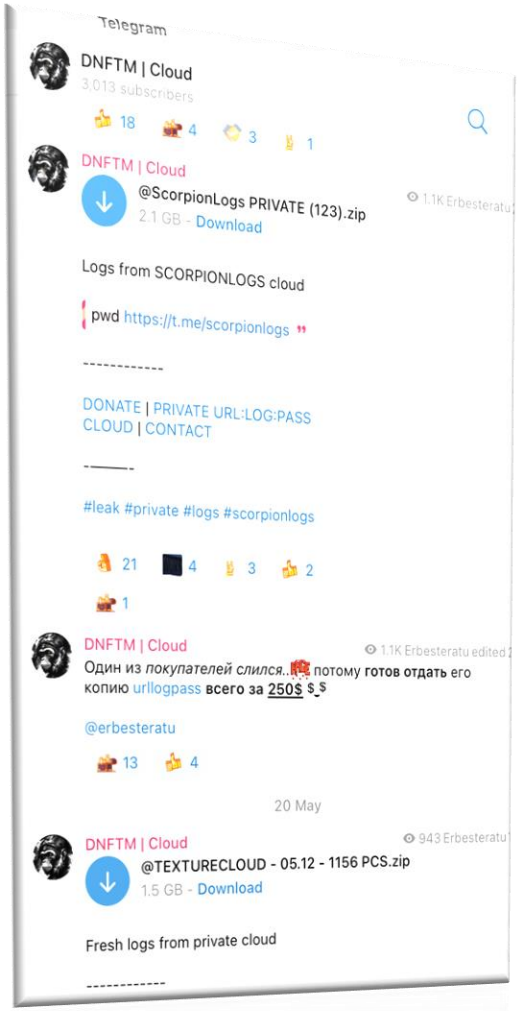
売り出されたアクセス権は、

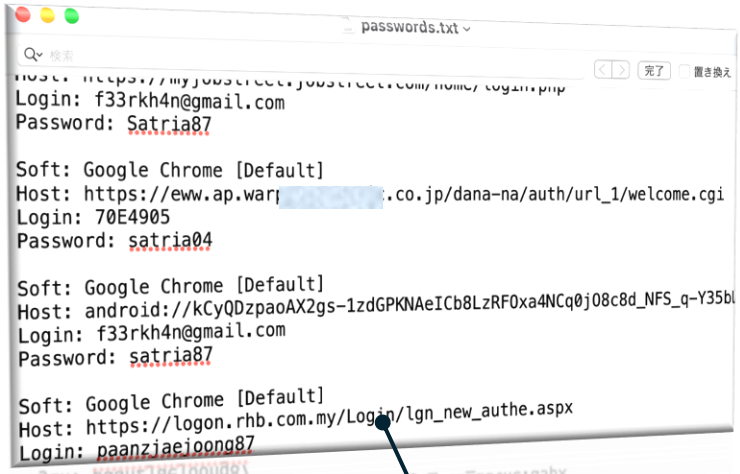
ランサムウェア集団の

「アフィリエイト」によって悪用

多くのランサムウェア被害を生む

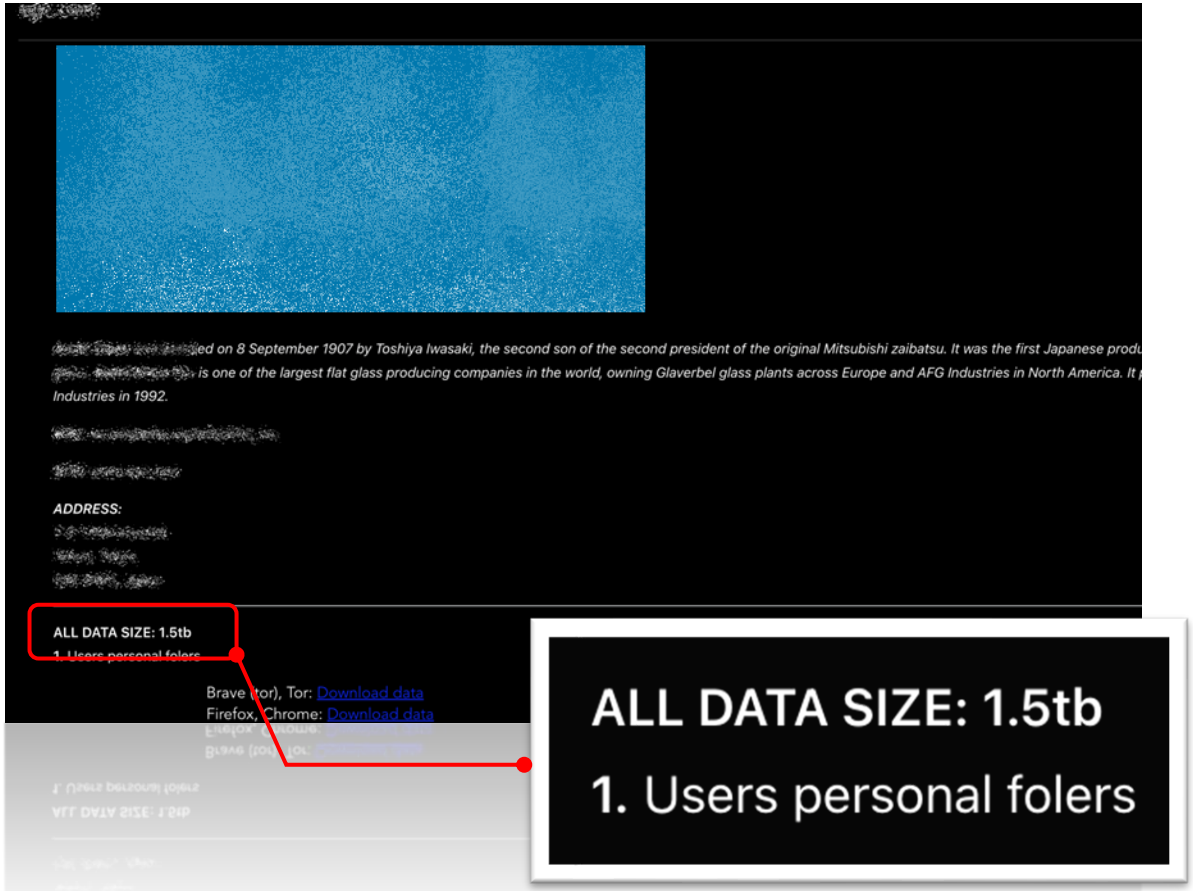
窃取され共有される認証情報





情報窃取マルウェアから窃取された、
某大手電機メーカーの
VPNゲートウェイへのログイン資格情報

不正アクセスにより窃取された情報

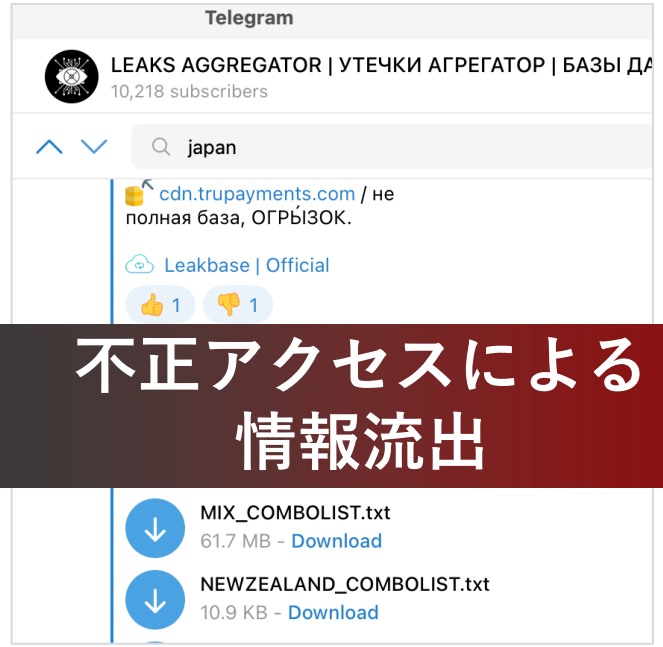


二重脅迫型ランサムウェアによるリークサイトからの流出
企業情報が数TBのボリュームで流出することも

Q.

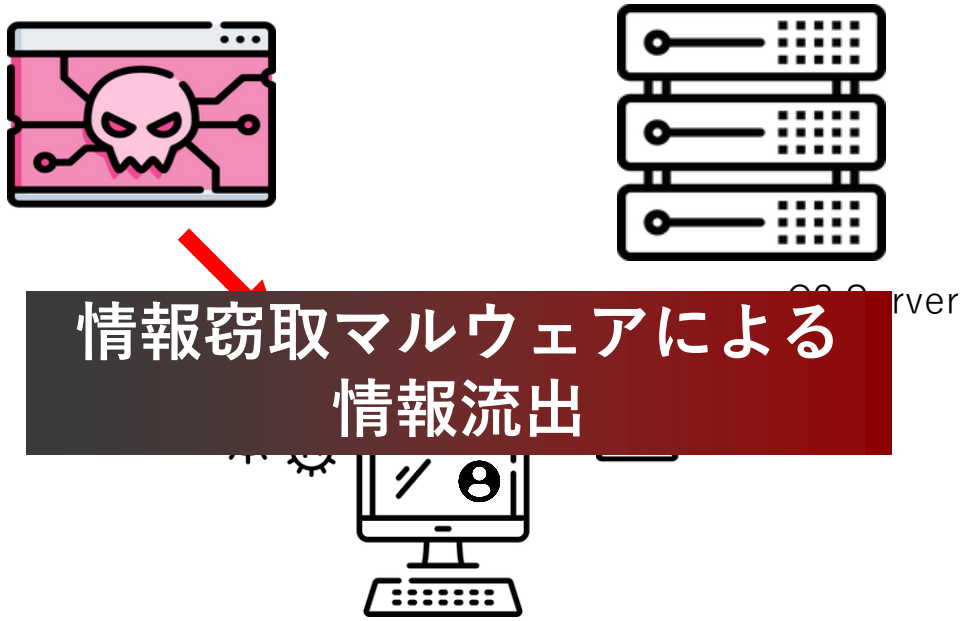
サイバー犯罪者たちは、
どのような手段で
情報を得ているのか？

ダークウェブに流通する資格情報の悪用



不正アクセスによる情報流出

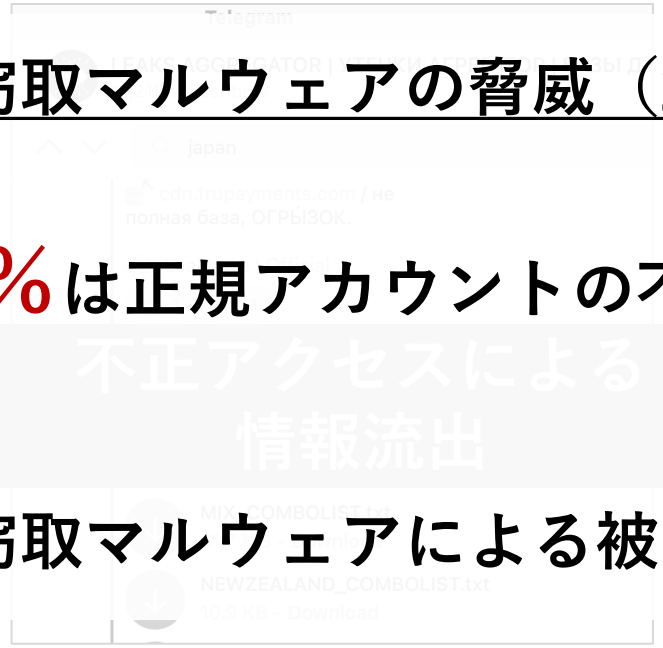
流出した資格情報を再活用し、
パスワードの使い回しを狙う



情報窃取マルウェアによる情報流出

URL ／ Login ID ／Passwordの組合せ情報、
カード情報、個人情報 など

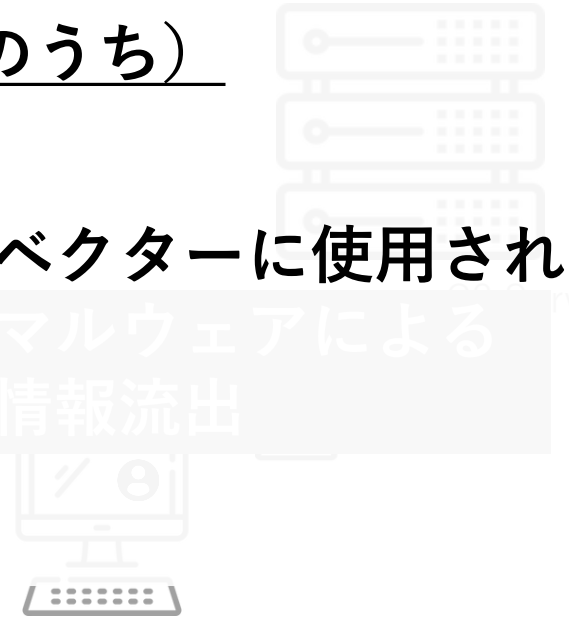
ダークウェブに流通する資格情報の悪用



情報窃取マルウェアの脅威（2023年のサイバー攻撃のうち）

50%は正規アカウントの不正利用が初期アクセスベクターに使用された

情報窃取マルウェアによる被害は266%増



不正アクセスによる情報流出

流出した資格情報を再活用し、
パスワードの使い回しを狙う

情報窃取マルウェアによる情報流出

URL ／ Login ID ／Passwordの組合せ情報、
カード情報、個人情報 など

出典：2024年2月 IBM X-Force脅威インテリジェンスレポート

ここまでのまとめ

- サイバー犯罪者達はネットワーク上で独自のコミュニティを形成
- 犯罪者のコミュニティでは様々な組織の機密情報が公開／売買
- 情報窃取型マルウェアからの情報流出が深刻化

リスクの深掘り

組織の内部という視点

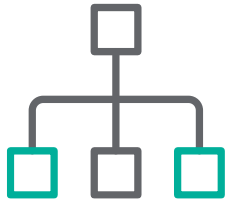
Q.

内部から情報を持ち出すパターンを
具体的に教えて

流出する可能性のある経路

電子メール

ネットワーク

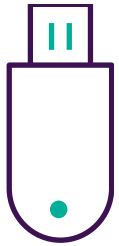


Web

クラウド・アプリ

プリンター

USB



流出する可能性のある経路

電子メール

ネットワーク

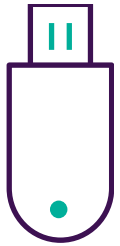
Web

クラウド利用やBYODの増加により、経路や手法も多様化

クラウド・アプリ

プリンター

USB



流出する可能性のある経路

電子メール

もっとも情報漏洩が起こりやすい

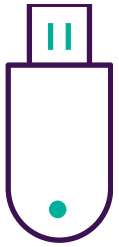
ネットワーク

Web

外部出力も根強い

プリンター

USB



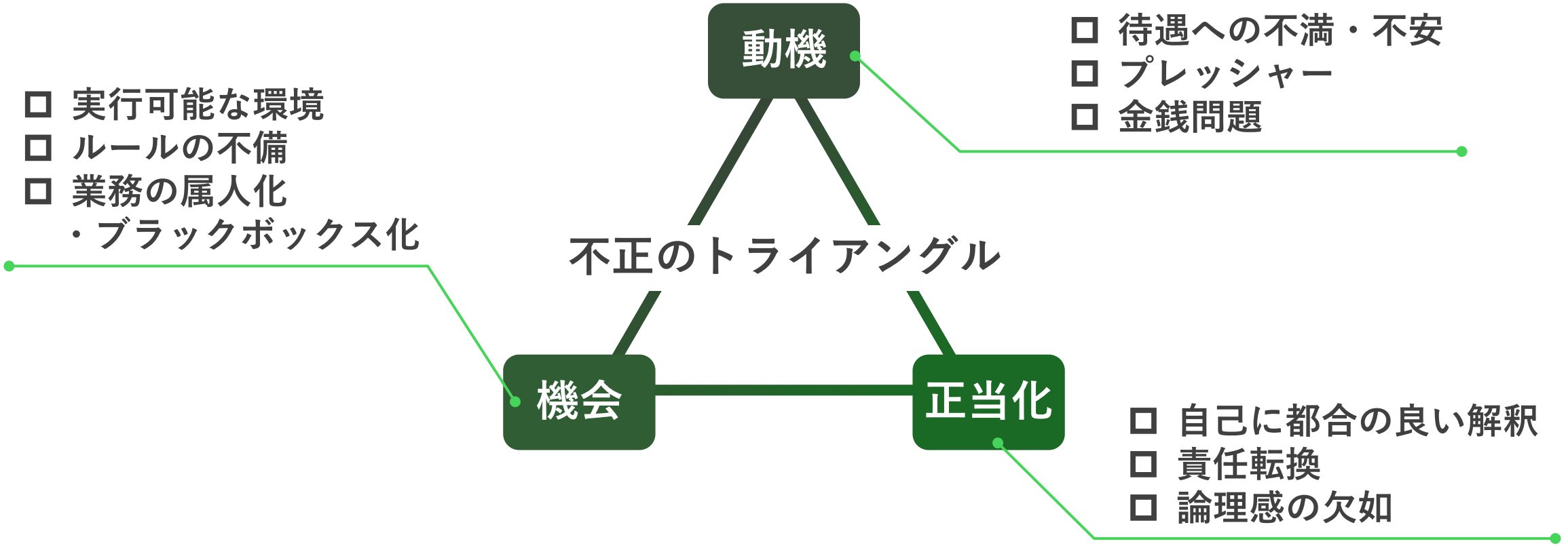
Q.

内部から情報を持ち出すのは
どんな人物なのか？その動機は？

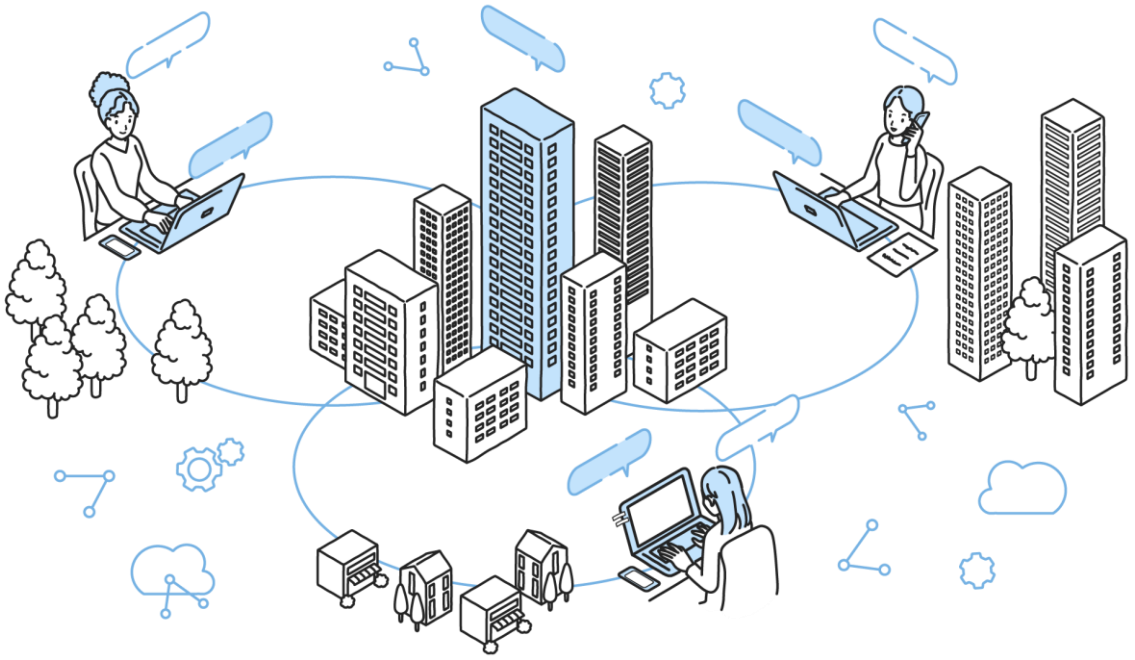
悪意を持って持ち出すパターン

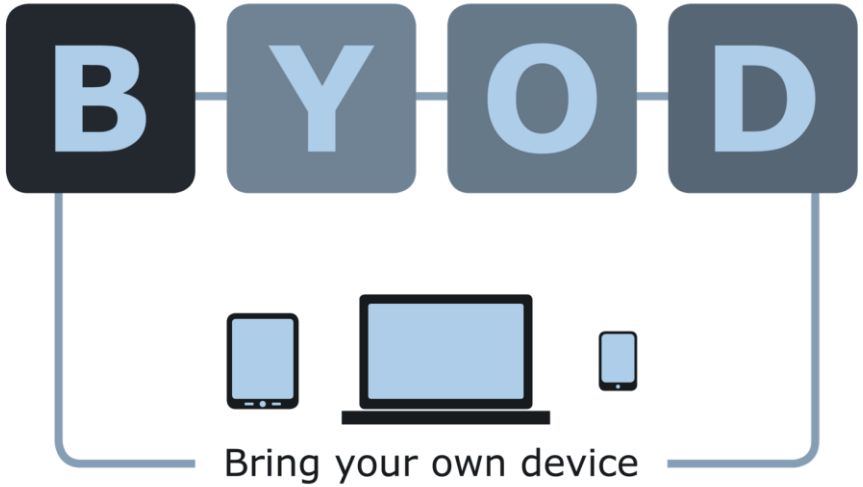
意図せず持ち出すパターン

悪意を持って持ち出すパターン



意図せず持ち出すパターン





ここまでのまとめ

- **情報が持ち出されるパターン**
  メール、クラウドストレージ、物理的な持ち出しなど
- **内部不正のキーは「不正のトライアングル」**
- **悪意なく行った行為が結果的に情報流出に繋がるパターンも・・・**

03 リスクへの対応方法

リスクへの対応方法

内部からの不正な持ち出しへの対策

Q.

内部不正対策を行いたい。

その具体的な方法は？

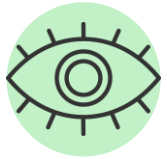
主な手法・テクノロジー

セキュリティ教育

不正アクセス防止

ログ管理

DLP（情報漏洩対策）



UEBA（振る舞い分析）

MDM（モバイルデバイス管理）

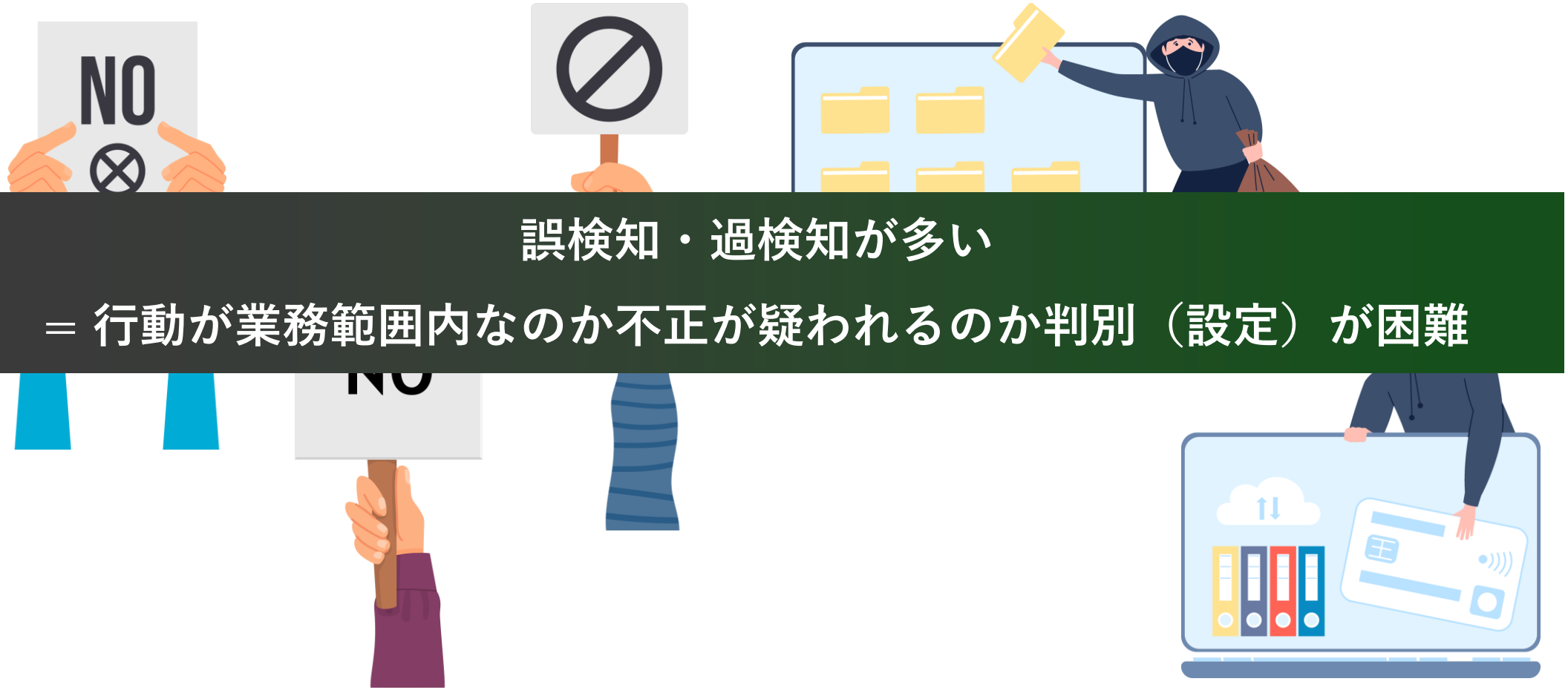
VDI（仮想デスクトップ）

Q.

内部不正対策において
DLPは現実的な解と思える。

が、国内で普及しない要因は？

ハードルが高いDLPの導入・・・



誤検知・過検知が多い

＝ 行動が業務範囲内なのか不正が疑われるのか判別（設定）が困難

ハードルが高いDLPの導入・・・

誤検知・

＝ 行動が業務範囲

判別（設定）が困難

なぜか？

ハードルが高いDLPの導入・・・

そもそもデータの棚卸ができていないから

ハードルが高いDLPの導入・・・

課題 データの棚卸　重要なデータはどこ？

課題 データの分類　どのデータが重要？

誤検知・過検知が頻発し運用できない・・・

情報漏洩対策を始めるには？

課題 データの棚卸　　重要なデータはどこ？

課題 データの分類　　どのデータが重要？

とにかくこの課題を解決することが第一歩

情報漏洩対策を始めるには？

データの棚卸

データの分類

DSPM

Data Security Posture Management

組織内のデータを可視化／分類することで重要データを明らかにし、

それらを継続してモニタリングすることでデータを保護するための手法

情報漏洩対策を始めるには？

STEP 01

発見・可視化

- データ保存領域の可視化

STEP 02

整理・分類

- 不要なデータの整理
- データの分類

STEP 03

防御

- 重要なデータの移動を検知し、ブロック

STEP 04

監視

- 日々のデータの動きや流れをモニタリング

DSPM
Data Security Posture Management

DLP
Data Loss Prevention

ここまでのまとめ

- 情報を持ち出すことができない仕組みを採用すること
- 実現のための第一歩は、データの棚卸と重要度の見える化
  DSPMという手法
- 内部不正対策の実現には「DSPM」＋「DLP」がおすすめ

リスクへの対応方法

外部に流出した情報の検知と対応

Q.

キャッチした漏洩情報に対する
具体的な対策方法は？

脅威情報を検知した際の推奨対応

- **漏洩の検証と影響範囲の特定**
  - 漏洩の事実、ソースの確認
  - 影響を受けるシステムやデータの特定

- **影響を受けた認証情報のリセット**
  - 漏洩した認証情報の即座の無効化、関連するアカウントのパスワードの変更措置
  - 必要に応じて二要素認証を強化または導入

- **関係者への通知**
  - 漏洩の影響を受ける可能性のあるユーザー、管理者、および他の関係者に対する通知
  - 漏洩の詳細、対応策、およびユーザーが取るべき予防措置についての情報提供

- **セキュリティの監視とログ分析の強化**：
  - セキュリティ監視を強化し、不審なアクティビティがないかどうかのチェック
  - セキュリティログとアクセスログを分析、不正アクセスの兆候の有無を確認

脅威情報を検知した際の推奨対応

- **漏洩の検証と影響範囲の特定**
  - 漏洩の事実、ソースの確認
  - 影響を受けるシステムやデータの特定
- **やることはいろいろあるが、一番重要なポイントは・・・**
  - 漏洩した認証情報の即座の無効化、関連するアカウントのパスワードの変更措置
  - 必要に応じて二要素認証を強化または
- **関係者への通知**

✓ 精度の低いアラート情報に振り回されないのが大事

✓ ノイズ（誤検知）のないアラートを活用する

✓ ソースがはっきりしない脅威情報は利用しないこと！

Q.

サイバー犯罪コミュニティの監視を
自社で行いたい。どうすればいい？

ずばり結論は、

安全性の観点から推奨されません！

なぜ自組織でのダークウェブ監視は非推奨なのか？

そもそもアクセスそのものが難しい

安全にアクセスできる確証がない

- ✓ 招待制のコミュニティ
- ✓ 特殊なツールが必要
- ✓ 犯罪者に自身の身元が割れるリスク

etc…

なぜ自組織でのダークウェブ監視は非推奨なのか？

そもそもアクセスそのものが難しい

安全にアクセスできる確証がない

仮にアクセスできても・・・

- ✓ 招待制のコミュニティ
- ✓ 特殊なツールが必要
- ✓ 犯罪者に自身の身元が割れるリスク

etc…

なぜ自組織でのダークウェブ監視は非推奨なのか？

監視そのものが難しい

多言語に対応する必要がある

✓ 特にロシア語や中国語が多い

独自の隠語が使われる

ターゲット企業が名指しで公開されているとは限らない

✓ 国、売上規模、業種などの情報から推測する必要あり

安全にダークウェブ監視を行うために

アクセス困難なエコシステムへの諜報活動力

高い専門性が要求されるデータ収集と加工技術、それらの自動化

専門的な知見やプラットフォームを有する

脅威インテリジェンスベンダーを活用

ここまでのまとめ

- 事前に情報の流出を察知できれば、先手を打った対策が可能
- サイバー犯罪者コミュニティの監視は危険！！難易度も高い
- 脅威インテリジェンスの知見のある企業・サービスを頼ること

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

04 まとめ

05 最後にお知らせ

本日のまとめ

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

■ 機密情報の流出によって起こる事象は全てが致命的

■ 情報流出は自社の努力だけでは 0 にすることは難しい

本日のまとめ

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

組織“内部”の視点

- 情報が持ち出されるパターン
  メール、クラウドストレージ、物理的な持ち出しなど
- 内部不正のキーは「不正のトライアングル」
- 悪意なく行った行為が結果的に情報流出に繋がるパターンも・・・

本日のまとめ

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

組織“内部”の視点

- 情報を持ち出すことができない仕組みを採用すること
  従業員全体のリテラシー向上も大事
- 実現のための第一歩は、データの棚卸と重要度の見える化
  DSPMという手法
- 内部不正対策の実現には「DSPM」＋「DLP」がおすすめ

本日のまとめ

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

組織“外部”の視点

- サイバー犯罪者達はネットワーク上で独自のコミュニティを形成
- 犯罪者のコミュニティでは様々な組織の機密情報が公開／売買
- 情報窃取型マルウェアからの情報流出が深刻化

本日のまとめ

01 情報漏洩の基本事項を確認

02 リスクの深掘り

03 リスクへの対応方法

組織“外部”の視点

- 事前に情報の流出を察知できれば、先手を打った対策が可能
- サイバー犯罪者コミュニティの監視は危険！！難易度も高い
- 脅威インテリジェンスの知見のある企業・サービスを頼ること

05 最後にお知らせ

KELA

KELA

イスラエルのKELA社が提供するSaaS型のサービス
サイバー戦争で培われた高度なノウハウで、サイバー犯罪コミュニティを監視し、
自組織に関する脅威を事前に排除し、起こり得る攻撃やもたらされる被害を回避します

監視プラットフォーム

＋

諜報活動のプロによる
アナリストサポート

＝

サイバー犯罪
コミュニティ監視

KELA

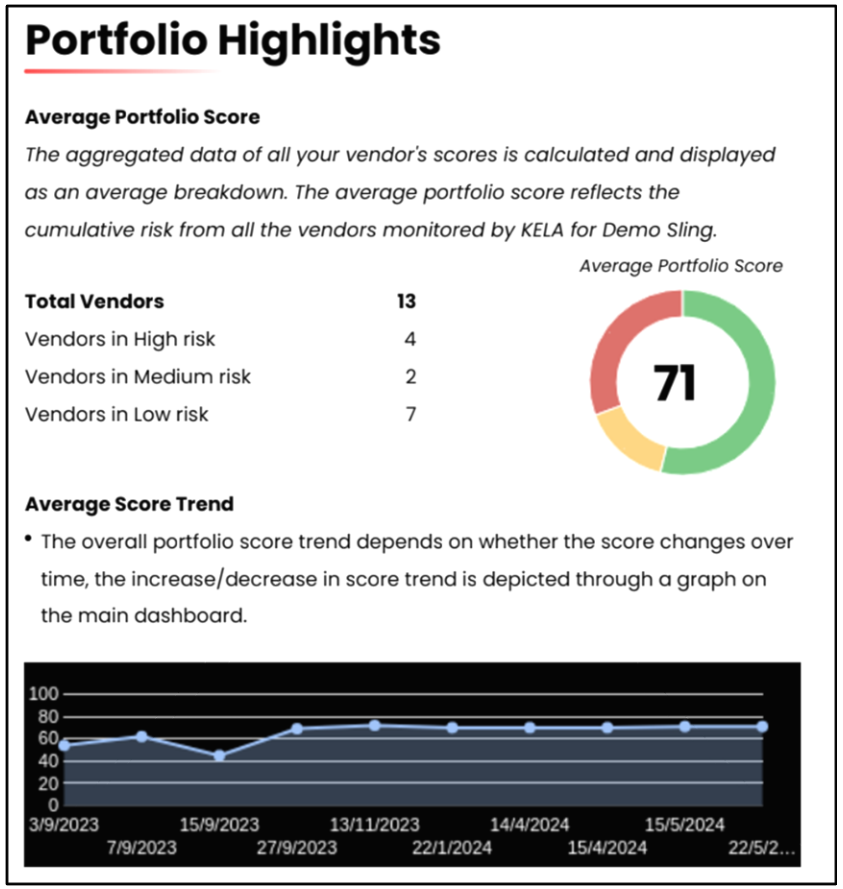
KELA

ご来場特典！

KELA、海外拠点・グループ会社の
リスクを総点検する

セキュリティリスク評価の
無償プログラム

海外拠点やグループ会社などのセキュリティ・リスクを洗い出し、
最新の脅威インテリジェンスに基づき、リスクの深刻さや対策レベルを
評価・数値化



御社のセキュリティリスクを数値化します。

※５ドメインまで


Forcepoint

Forcepoint

STEP 01
発見・可視化
- データ保存領域の可視化

STEP 02
整理・分類
- 不要なデータの整理
- データの分類

STEP 03
防御
- 重要なデータの移動を検知し、ブロック

STEP 04
監視
- 日々のデータの動きや流れをモニタリング

Forcepoint DSPM

Forcepoint DLP

Forcepoint SSE

従来型のDLPで導入障壁が高い要因となっていた
「条件の定義が難しい」という点を、
AIを活用した独自の分析基盤により解消

ファイル管理におけるユーザーの行動制限を極力解消しつつ、
重要データの外部流出の防止を両立

Forcepoint

ご来場特典！

Path	Category	Data Attributes	Classification	Compliance Tags	Actions
D$/財務部/重要分析・企業評価.pdf	Business Documents	Show more (+2) Organization 0.48 Person 0.70 NamedEntity 0.17	内部使用	PII 1.00	
D$/財務部/財務予測.docx	Marketing Documents	Show less HR 1.00 NamedEntity 0.93 Person 0.10 Organization 0.92 Record 0.98 Financial 0.22	機密	PII 1.00	

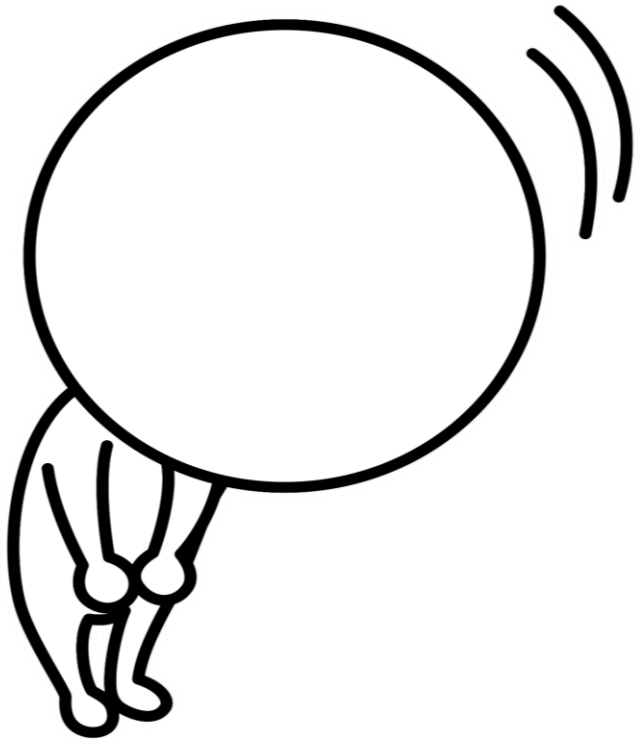
クラウドストレージやファイルサーバー内のデータ棚卸を体験してみませんか？

無償でBox上のデータのアセスメントを実施します。

※上限10GBまで

AGEST

AGEST



KELA／Forcepoint に関する

お問い合わせは

AGESTにお声がけください

本日のテーマ以外でも、
サイバーセキュリティの
お悩みがあればお聞かせください

AGEST

開催予定のセミナー

詳細は AGEST の HP からご確認ください

受付中

開催日時 2024年06月18日 14:00-14:40

2024年6月18日(火)開催オンラインセミナー｜あらゆるテストをワンツールで自動化できる「TestArchitect」の魅力を紹介!

セミナーに申し込む ›

受付中

開催日時 2024年06月25日 14:05-14:55

定期オンラインセミナー｜【Keeper Security】パスワードマネージャー製品説明会オンライン～パスワード管理のベストプラクティス、IDaaSとの違い、製品デモなど…

セミナーに申し込む ›

受付中

開催日時 2024年06月25日 15:05-15:30

2024年6月25日(火)開催オンラインセミナー｜【内部不正対策】内部不正を取り巻く状況と報道事例

セミナーに申し込む ›


Fin