



企業を襲う新時代の脅威： ランサムウェア被害事例の解説と対策

自己紹介

翁駿暁（オウシュンギョウ）

出身：中国

経歴：

浙江大学情報コンピューターサイエンス学部、早稲田大学大学院 国際情報通信研究科卒業。
シンプレクス株式会社にてカリフォルニア大学ロサンゼルス校金融工学短期研修了したのち、証券会社における取引システムの開発、導入等のメンバー、リーダー等を担当。

アビームコンサルティング株式会社、PwCコンサルティング合同会社にて金融機関を中心としたITコンサルティング業務に従事。

現在、Librus株式会社取締役COOを担当。

社内のIT技術領域全般を管掌し、システム開発およびサイバーセキュリティを中心とした技術戦略の推進を担当

趣味：

ゲーム（PS5、Switch）、筋トレ、格闘技



ランサムウェアとは？

感染すると端末等に保存されているデータを暗号化して使用できない状態とした上で、そのデータを復号する対価として、いわゆる「身代金」（ランサム：英語記載でransom）を要求する不正プログラムのことです。

近年は、「対価を支払わなければ窃取したデータを公開する」と言って脅す、二重恐喝型が多くなっています。

①ランサムウェアを送り込む



②送り込まれたランサムウェアがデータを暗号化・ロック（およびデータの窃取）



③暗号化を復号する鍵と引き換えに身代金を要求

さらに
払わなければ窃取情報を公開
すると脅迫

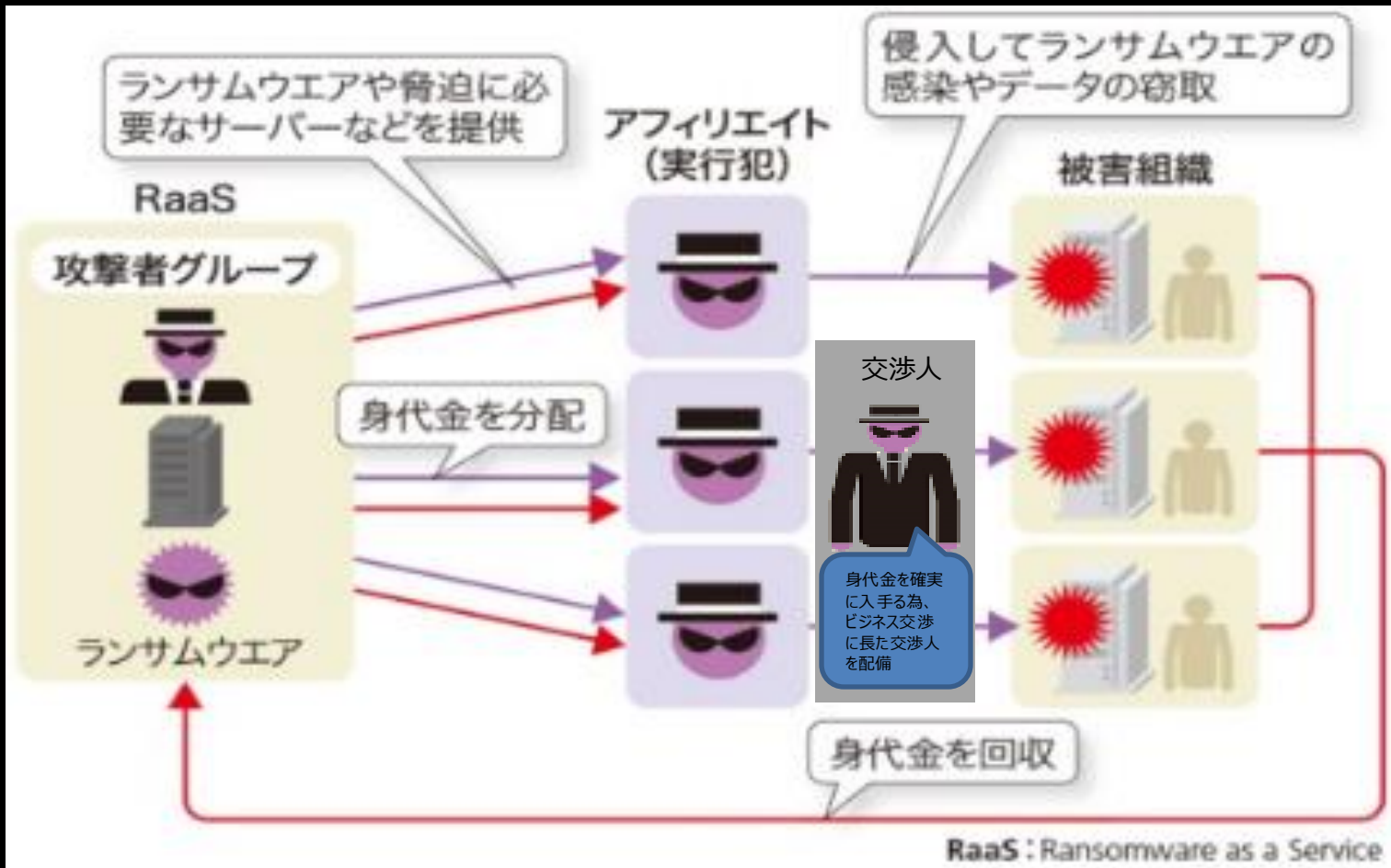


暗号化を解除
する代わりに
身代金を払え！



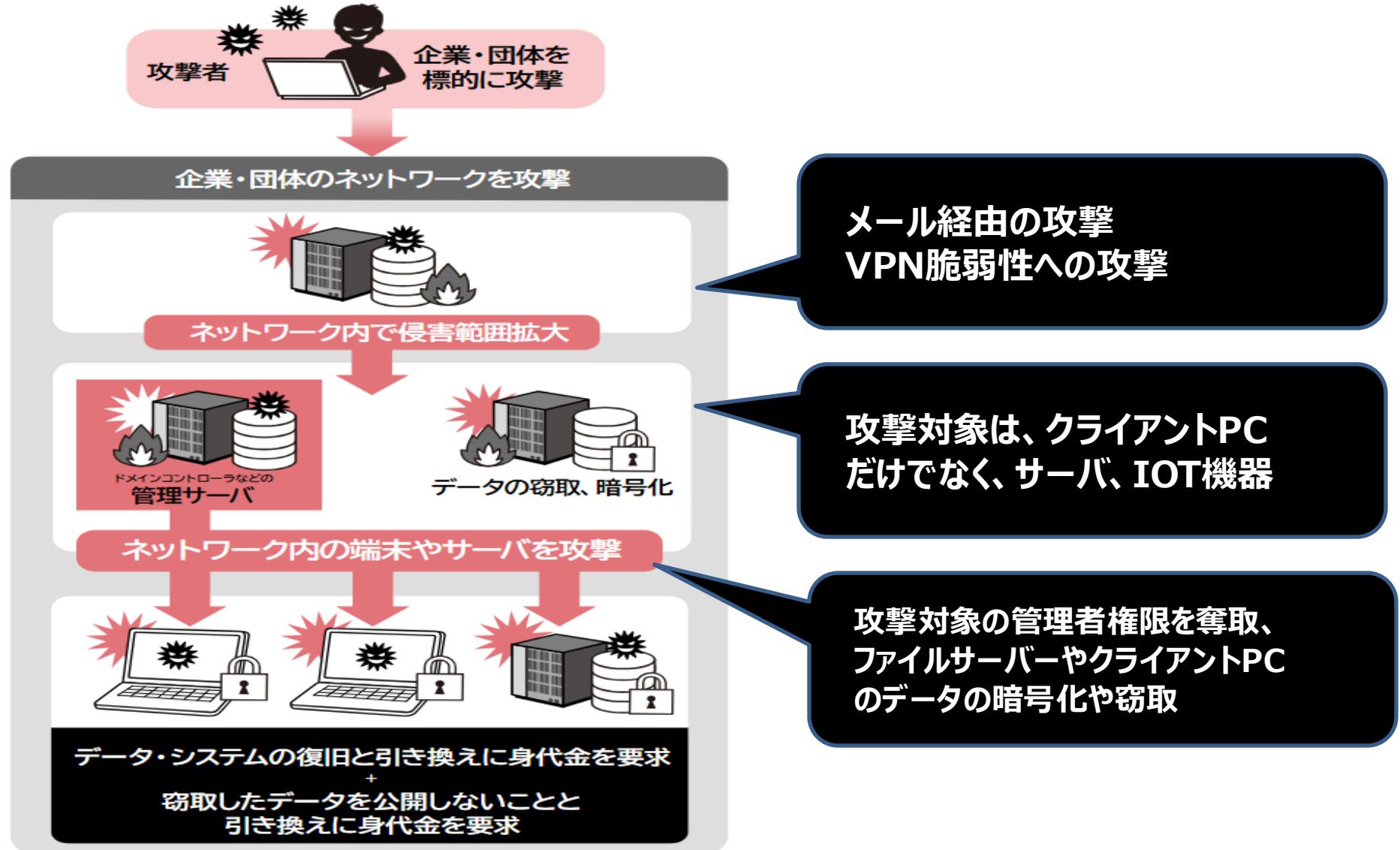
【補足】ランサムウェアは、RaaSというサービスに発展

RaaS (Ransomware as a Service) と呼ばれる攻撃実行犯を支援するクラウドサービスに発展



《注》日経ネットワーク2021年9月号掲載のイメージ図引用

ランサムウェアの現状と脅威



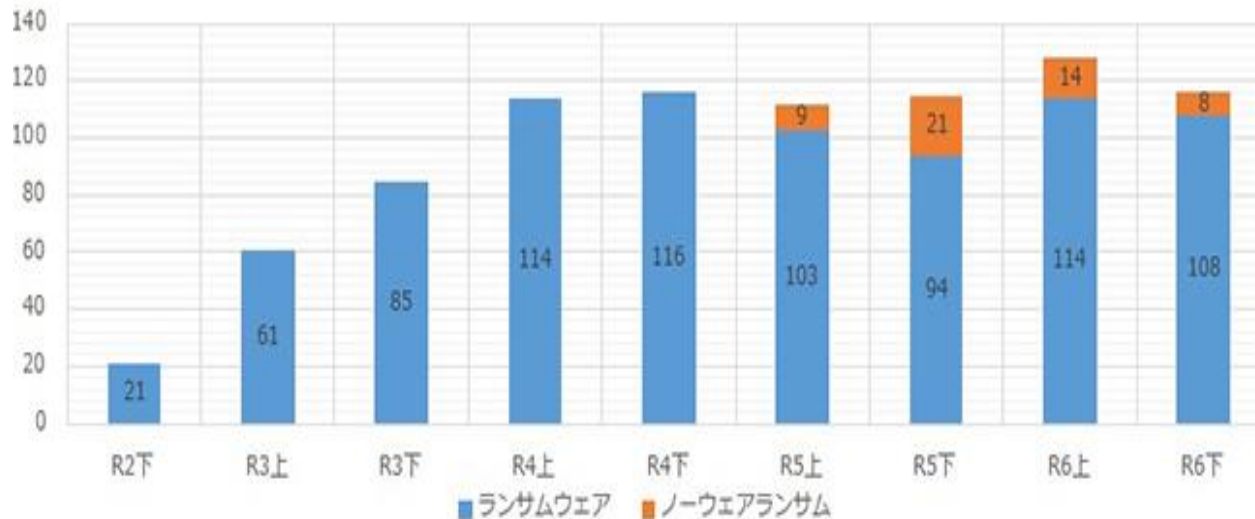
《注》政府広報オンライン右記サイト(<https://www.gov-online.go.jp/useful/article/202210/2.html>) から引用

ランサムウェアの被害傾向

警察庁により公表されている企業・団体等におけるランサムウェア被害の件数は、令和3年より急増し、その後高水準で推移している状況です。

犯行手口を確認すると「**二重恐喝**」という手口が特に多い傾向です。また、近年の事例として、企業・団体等に対してデータを暗号化することなくデータを窃取した上で、企業・団体等に対価を要求する手口（**ノーウェアランサム**）も確認されています。

感染経路として、**リモートデスクトップ**と**VPN機器**によるものが多い状況です。



《注》 上述の情報は、警察庁「令和6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」から引用

近年のランサムウェアの被害事件

年月	組織名	業種	概要
2025年5月	損害保険ジャパン株式会社	金融	書類保管業務を委託している株式会社ギオンのサーバーがランサムウェアによるサイバー攻撃を受け、約 7万5,000件 の顧客氏名情報が漏えいした可能性があることを公表
2025年2月	株式会社保険見直し本舗	金融	ランサムウェア被害により最大で約 510万件の個人情報 が暗号化された。暗号化されたデータの中に顧客の保険契約情報や相談履歴、協業先企業から受託した個人情報などが含まれていた。
2024年6月	KADOKAWA	出版	ランサムウェアを含む大規模なサイバー攻撃を受けて 個人情報等1.5テラバイト の情報流出
2024年6月	東京海上日動グループ	金融	委託先会計事務所（高野総合会計事務所）がランサムウェア攻撃を受け、 グループ3社が契約する顧客情報 を含めた個人情報に漏えいした可能性
2024年5月	岡山県精神科医療センター	医療 (独立行政法人)	ランサムウェアによるサイバー攻撃を受け、電子カルテを含む情報システムの障害が発生し、患者情報の流出を確認最大 4万人の患者情報 や会議議事録が流出した可能性
2024年5月	株式会社イセトー	情報通信	ランサムウェアによる攻撃を受け、複数のサーバや端末が暗号化イセトーへ業務委託を行っていた委託元保管の情報がリークサイトに漏えい
2023年7月	名古屋港コンテナターミナル	名古屋港運協会	2023年7月4日（火）早朝、名古屋港統一コンテナターミナルシステムがサイバー攻撃（ランサムウェア）によって稼働不可となり、復旧まで3日を要した。

某Kグループサイバー攻撃事例：時系列情報解説

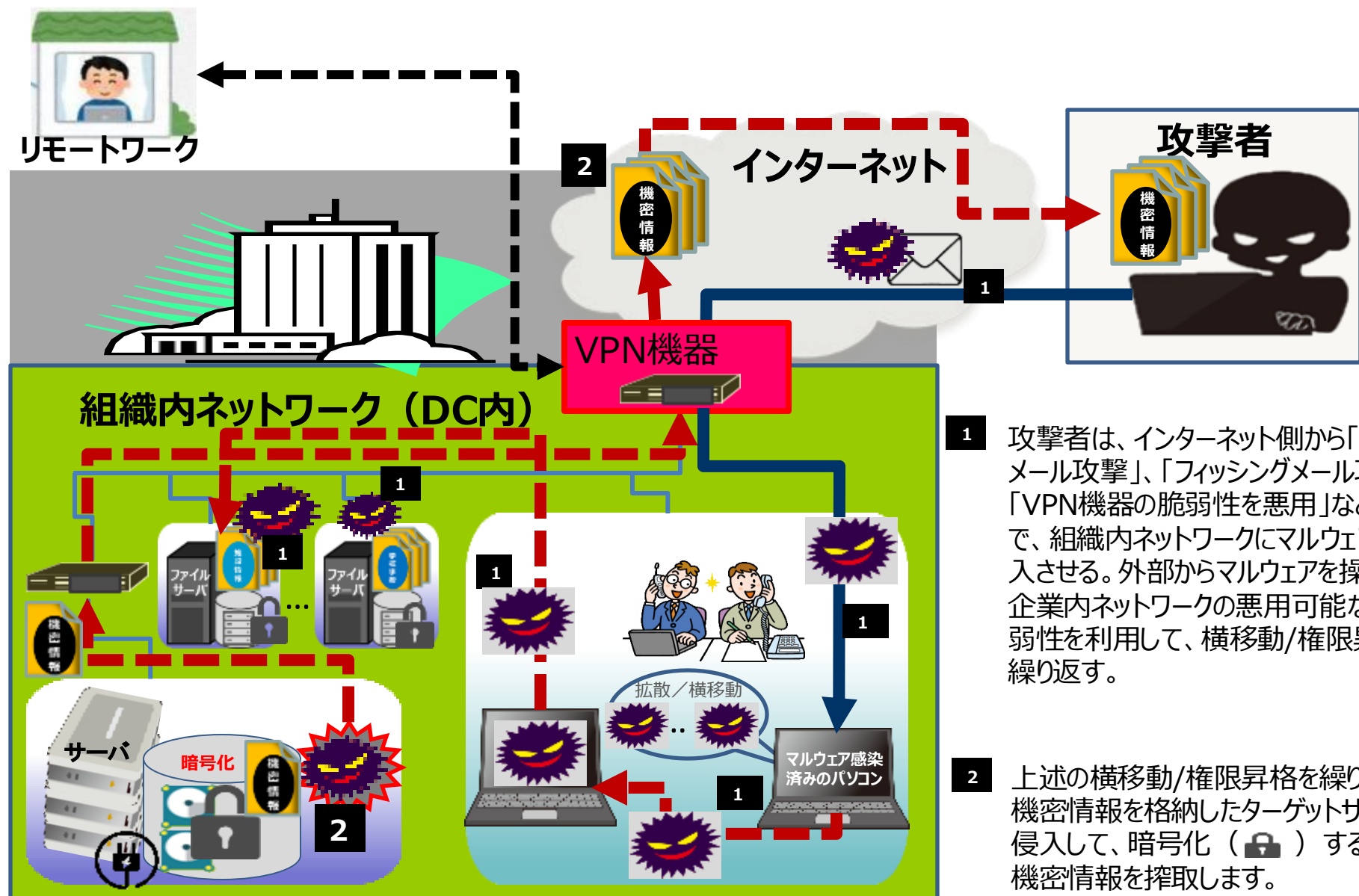
日付	事象
6月8日	午前3時30分頃「ニコニコ」「N予備校」を含むドワンゴ社のウェブサービス全般で正常に利用できない不具合が発生午前8時頃、上記不具合がランサムウェアを含むサイバー攻撃によるものと確認 同日中に対策本部を立ち上げ、通信の切断および データセンター内のサーバのシャットダウン を実施
6月9日	第1報を発表。この時点では外部からの不正アクセスによるシステム障害との情報にとどまる。 外部専門機関などに打診
6月10日	個人情報保護委員会に報告
6月12日	金融庁に障害発生を報告
6月14日	第2報を発表。システムやサービスの停止に伴う影響や支払い遅延に関して言及 情報漏えいに関しては調査中（個人情報・クレジットカード情報の漏えいは現時点では未確認） ドワンゴよりニコニコシステムの復旧（システム全体を再構築）および補償について発表
6月18日	株主総会で被害状況を説明
6月22日	一部報道機関が犯人を名乗る人物のメッセージを公開 KADOKAWAは本報道に対して抗議声明を発表
6月27日	第3報を発表。被害状況を説明するが情報漏えいについては引き続き調査中との言及にとどまる 有価証券報告書の提出期限延長を申請（翌28日に承認） ロシア系ハッカー集団 BlackSuit より、追加の身代金に応じなければ 1.5TBの流出データ を公開すると発表。同時に盗んだ情報の一部とするデータをダークウェブ上に公開（ 取引先情報、従業員の個人情報、「N高等学校」などの在校生や卒業生、保護者の個人情報等 ）
6月28日	取引先および社内情報の漏えいに関するお知らせとお詫びを掲載
7月25日	8月5日よりニコニコサービスを順次再開することを発表
8月16日	2025年3月期に 約36億円の特別損失 を計上する見通しを発表

攻撃手法・侵入方法については、公表されませんが、
以下 ● の何れかで侵入し、侵入した環境内の脆弱性を利用して、
横展開 & 権限昇格を続けて、最終的に管理者権限を利用して、
ターゲットの暗号化を実施。

- VPN機器の脆弱性の悪用
- 標的型メール攻撃
- フィッシングメール攻撃
- 内部犯行・漏えいした認証情報の悪用



某Kグループサイバー攻撃事例：想定される侵入方法

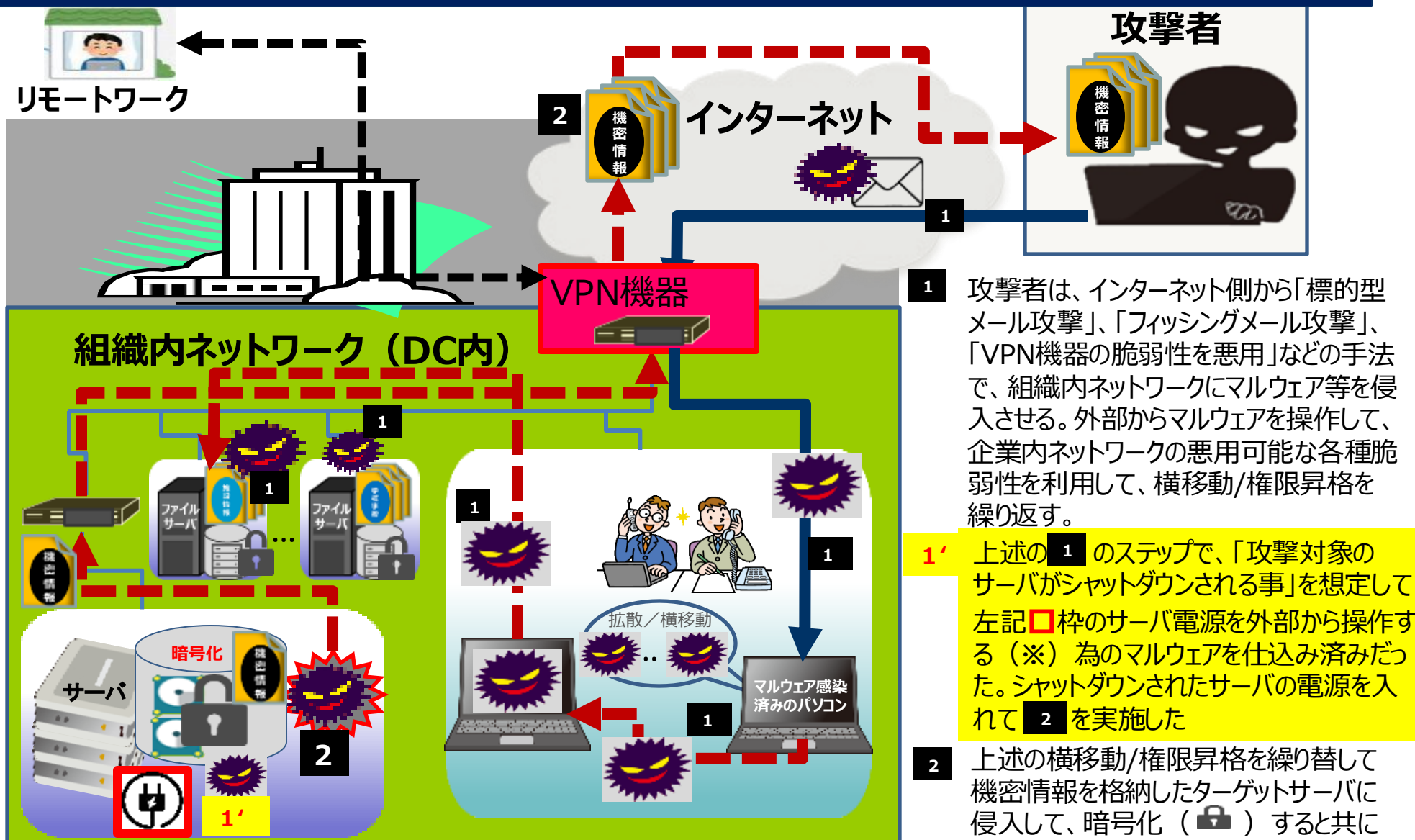


1 攻撃者は、インターネット側から「標的型メール攻撃」、「フィッシングメール攻撃」、「VPN機器の脆弱性を悪用」などの手法で、組織内ネットワークにマルウェア等を侵入させる。外部からマルウェアを操作して、企業内ネットワークの悪用可能な各種脆弱性を利用して、横移動/権限昇格を繰り返す。

2 上述の横移動/権限昇格を繰り返して機密情報を格納したターゲットサーバに侵入して、暗号化（）すると共に機密情報を搾取します。

某Kグループサイバー攻撃事例： 想定攻撃の特徴以下 ■ 部

前ページの想定に加えて、ターゲットのサーバがシャットダウン（電源落とす）後も、攻撃側の活動が継続された事を考慮する



※シャットダウンしたサーバを遠隔で起動操作するWOL（WakeOnLan）の悪用

ランサムウェアの被害を低減する為の主な対策

攻撃／脅威の内容	対策
VPN機器の脆弱性の悪用 	VPN機器／組織内ハードウェア（電源等機器制御のソフトウェア含）、ソフトウェアの資産管理と脆弱性管理の実施
標的型メール攻撃、フィッシングメール攻撃 	標的型メール攻撃/フィッシングメール攻撃に対する訓練や従業員教育
内部犯行・漏えいした認証情報の悪用 	内部不正等振舞いのリアルタイム監視と怪しい振る舞いの防御
ランサムウェアインシデントが発生した場合に備えて	対象となるシステムとデータのバックアップ（最新の状態のバックアップ）を取り、安全な場所で保管しておく。

ランサムウェア感染された場合、身代金を支払うべきか

【翁 コメント】

以下の理由から、**支払うべきではありません。**

- まず第一に 身代金を支払ったからと言って暗号化されたデータが復旧する保証がありません。
- 次に、支払った場合に、「外国為替及び外国貿易法（外為法）」や「犯罪による収益の移転防止に関する法律（犯収法）」といった法律に抵触する可能性があります。
- 最後に、一度身代金を支払ってしまうと、「脅迫すれば身代金を支払う」企業だと攻撃者に認識され、再度標的になる可能性が高まります。

会社概要

会社概要



会社概要

私たちは「戦略」と「テクノロジー」を通じてあらゆるビジネスをより豊かにすることを目指します。

社名	Librus株式会社
設立年月	2017年11月
本社所在地	〒105-0004 東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F
代表取締役 CEO	鎌田光一郎：青山学院大学 法学部卒業。SMBC日興証券株式会社に証券営業、経営管理業務に従事したのちPwCコンサルティング合同会社に転籍。金融機関に対するコンサルティング業務に従事。その後、Librus株式会社を設立、代表取締役に就任。
取締役 COO	翁駿暁：浙江大学 理工学院 情報コンピューターサイエンス学部、早稲田大学大学院 国際情報通信研究科卒業。情報通信学修士。シンプレクス株式会社にカリフォルニア大学ロサンゼルス校金融工学短期研修修了したのち、証券会社における取引システムの開発、導入等のメンバー、リーダー等を担当。その後、アビームコンサルティング株式会社、PwCコンサルティング合同会社に金融機関を中心としたコンサルティング業務に従事。現在はLibrus株式会社取締役COOに就任。
従業員数	105名（2025年6月1日時点、業務委託社員含む）
認証	ISO 9001、ISO/IEC 27001 情報セキュリティサービス基準適合サービスリスト 人材派遣業/人材紹介業
主な所属	公益社団法人経済同友会 一般社団法人ソフトウェア協会など

事業領域

当社はサイバーインテグレーターとして、「システムインテグレート」「サイバーセキュリティ」「マーケティング」の3領域を主軸に事業活動を展開しています。

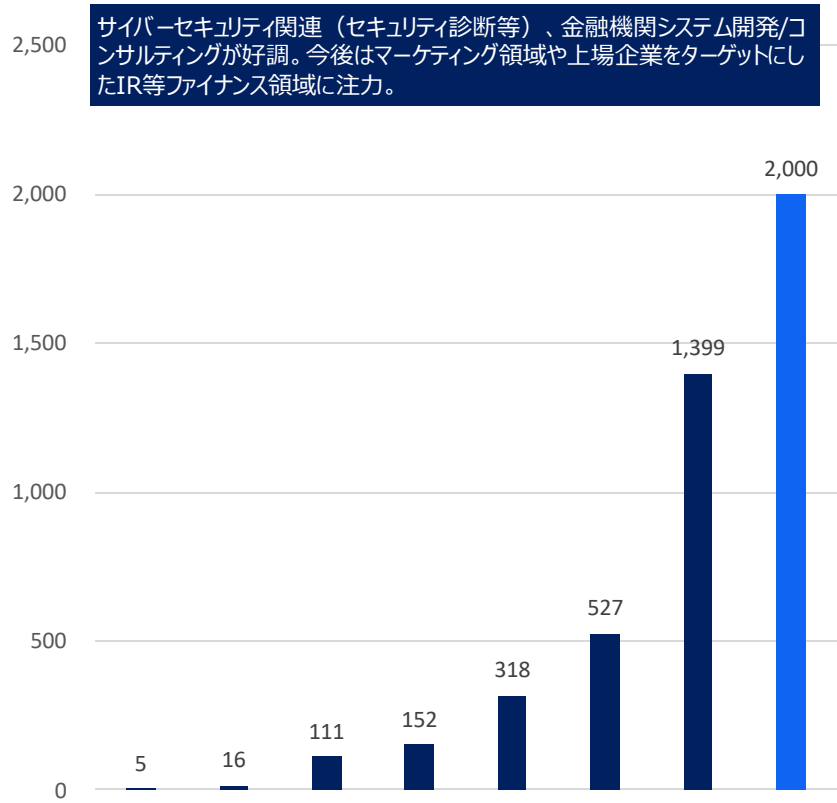
コンサルティング	事業戦略/新規事業/DX	・事業戦略の高度化/デジタル化/その他コスト改善等 ・デジタルや金融ビジネスの知見を活用した新規事業の立ち上げ/運用 ・DXによる事業の最大化やコストの最適化
	マーケティング	・コーポレートサイトやIRサイトのリニューアルを通じたブランディング強化 ・デジタルを通じた自社のブランドや認知度を向上 ・サイト制作や広告運用、マーケティング分析を通じた、収益性の向上
エンジニアリング	システム設計/開発/保守運用	・高品質かつ迅速なウェブ/スマートフォンアプリケーションその他の開発 ・高品質のドキュメントをベースとした低リスク/高品質でプロジェクトの推進 ・コンサルタント、プロジェクトマネージャー、エンジニアの調達支援
	AI/データマネジメント	・DXに伴うデータ分析や活用、基盤構築支援 ・AIを活用した新サービスの立ち上げや既存サービスの高度化支援 ・その他データを活用して企業収益の最適化推進
—	サイバーセキュリティ	・組織のリスク管理の体系化/高度化、セキュリティ診断/SOCなどを通じた、急増するサイバーセキュリティリスクへの対応支援 ・社内の個人情報の検出/管理やWAFソリューション導入支援
—	ファイナンスサービス	・企業価値向上などを目的としたM&A仲介/アドバイザーサービス ・IR/その他財務コンサルティングサービス

業績関連



業績推移

売上高は堅調に成長。売上高経常利益率は10%程度で推移。50億円、100億円規模の年商に達するために総合的な営業力を強化することを企図する。



(単位：百万円) ※創業から8期分。直前期は推計値

Copyright © Librus Inc. All Rights Reserved.

取引先実績

金融業、情報通信業を中心に大手企業と多岐に渡り取引実績がございます。

企業名	業種	取引概要	ロゴ
株式会社NTTデータグループ	情報通信業	・金融機関向けサイバーセキュリティ対策のコンサルティング協業 ・セキュリティ診断その他	
伊藤忠テクノソリューションズ株式会社	情報通信業	・自動車製造業向けプロジェクトマネジメント支援 ・セキュリティ診断その他	
日本郵政グループ株式会社	金融業その他サービス業	・セキュリティ診断	
日本たばこ産業株式会社	食品業その他	・セキュリティ診断	
日本放送協会	情報通信業	・セキュリティ診断	
デロイトトーマツコンサルティング合同会社	サービス業	・サイバーセキュリティ領域、デジタルマーケティング領域での協業	
ウォルトディズニー・ジャパン株式会社	情報通信業	・セキュリティ診断	
株式会社SBI証券	金融業	・セキュリティ診断 ・ESG戦略に関するコンサルティングサービス	
株式会社三菱UFJフィナンシャル・グループ	金融業	・セキュリティ診断（銀行業/証券業）	

当社の強み



当社は総合的「サイバーインテグレーター」として、デジタル新規事業の創出からマーケティング、サイバーセキュリティ、オペレーション、リスクリングに至るまでオールインワンで支援が可能です。

——— DXによる経営/事業の環境が劇的に変化 ———

——— 当社の特長 ———

DXによる主な恩恵

ビジネス

- ・サービス/製品革新
- ・新規収益モデルの創出
- ・社会的インパクト創出
- ・グローバル展開 など

コーポレート

- ・業務効率化
- ・データ活用
- ・社内外コミュニケーション改善
- ・サステナビリティ推進 など

DXは企業成長における最も重要なファクターの一つである一方で、様々な課題も懸念される

DXによる主な課題

- 1 技術的論点
 - ・システム統合
 - ・サイバーセキュリティ
 - ・デジタルマーケティング
 - ・データ品質管理
 - ・クラウド活用

- 2 組織/文化的論点
 - ・スキルギャップ
 - ・部門間連携不足
 - ・プロジェクト管理
 - ・成果への過剰期待
 - ・継続的なイノベーション文化の欠如
 - ・社員の抵抗感

- 3 外部環境的論点
 - ・法規制への対応
 - ・社会的インパクト創出
 - ・新規収益モデルの創出

- 4 財務的論点
 - ・投資対効果の不透明性
 - ・コスト管理

当社は最高峰の「サイバーインテグレーター」として、あらゆる顧客課題の解決を実現いたします。

「デジタル」に関する総合的な知見による総合的かつ高品質な提案/サービス提供

ベンチャー企業でありながら、クライアント企業の高い評価とその安定性に裏付けられた豊富な大企業/金融機関の実績

「積極性/自由さ」「誠実さ」をスローガンに高難易度案件に果敢に挑戦する姿勢と経験/実績

当社ではサイバーセキュリティ、デジタルマーケティング、フィンテック、システムインテグレートなど様々な高難易度の顧客課題に対して、その領域における第一線のプロフェッショナルが揃っております。

当社はベンチャー企業として創業してから、これまで数多くの大企業、金融機関、官公庁に対して、サービスを提供し、そのいずれもで特にサービスクオリティとデリバリースピードの速さで高い評価を獲得してきました。

「Librus」という社名は「Libera」と「Sinserus」という2語を掛け合わせた造語です。プロフェッショナルファームとして、クライアントに対する誠実さを最優先にしつつも、積極的かつ自由に提案するスタンスを大事にしてきました。

特に当社が強みとする領域



過去実績



スローガン/提供価値

- 1 「積極的、柔軟的、総合的」な提案を行いつつ、顧客の根本的な課題解決を最優先します。
- 2 圧倒的なスピードとクオリティを実現し続け、顧客感動を追求します。
- 3 既存のサービス体系や技術に固執せず、常に最先端かつ最適なサービス提供を行います。

サイバーセキュリティサービス全体像



当社は総合セキュリティベンダーとして、多角的にクライアントのセキュリティ対策を支援することが可能です。

