何が起こっている？

大手出版社サイバー攻撃などの事例について解説

2024.07.31

株式会社インフォメーション・ディベロプメント
サイバーセキュリティ(CS)事業本部
サイバー・セキュリティ・ソリューション(CSS)部
テクニカルスペシャリスト
松岡　政之

Agenda

- 自己紹介
- 昨今のランサムウェア事情
- 大手出版社事例考察
- まとめ

Agenda

自己紹介

昨今のランサムウェア事情

大手出版社事例考察

まとめ

自己紹介

松岡 政之
MATSUOKA Masayuki

株式会社インフォメーション・ディベロプメント(ID)
サイバーセキュリティ(CS)事業本部
サイバー・セキュリティ・ソリューション(CSS)部
テクニカルスペシャリスト

情報処理安全確保支援士 登録番号015628
ネットワークスペシャリスト
エンベデッドシステムスペシャリスト
AWSソリューションアーキテクトプロフェッショナル

【略歴】

- 2014年　株式会社インフォメーション・ディベロプメント入社
- 金融/保険会社、官公庁等にてセキュリティ対策製品の構築・展開に従事
- 銀行/金融系システム会社等にて
  セキュリティコンサルティング業務に従事
- 金融系システム会社/官公庁等にてクラウド環境の提案/設計/構築/展開に従事
- 現在、上記分野の様々な案件にマルチに参画

Agenda

自己紹介

昨今のランサムウェア事情

大手出版社事例考察

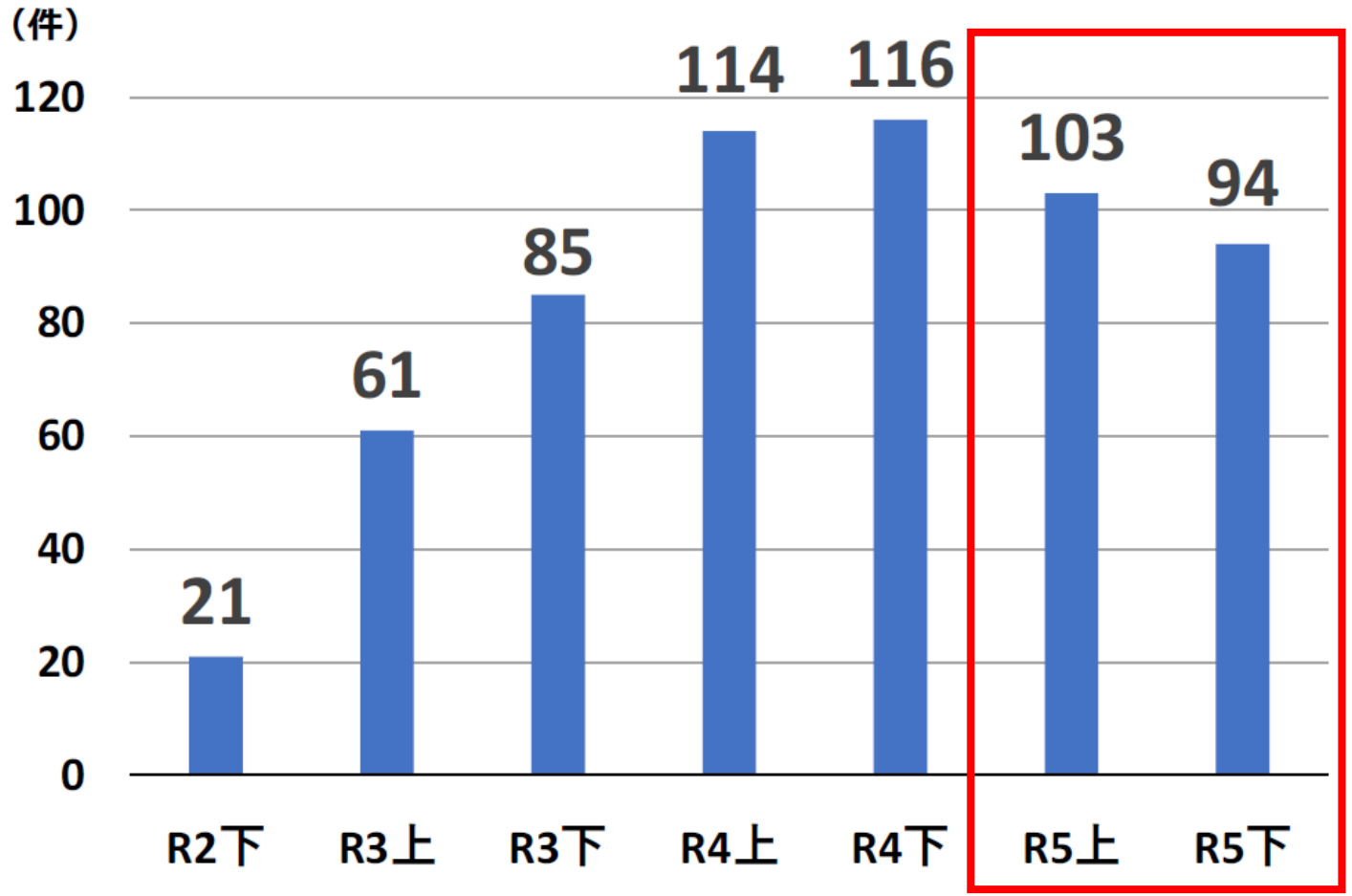
まとめ

昨今のランサムウェア事情

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
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	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグランドサービス）	2017年	2年連続4回目

独立行政法人情報処理推進機構.「情報セキュリティ10大脅威 2024」.
https://www.ipa.go.jp/security/10threats/10threats2024.html

ランサムウェア被害件数(国内)



197件

警察庁.「令和5年におけるサイバー空間をめぐる驚異の情勢等について」.
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェア被害事例

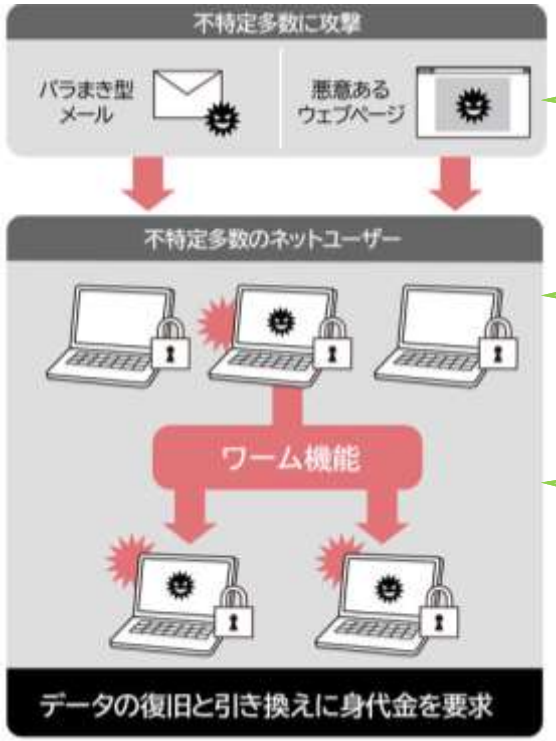
年月	組織名	業種	概要
2024年6月	KADOKAWA	出版	ランサムウェアを含む大規模なサイバー攻撃を受けて個人情報等1.5テラバイトの情報流出
2024年6月	東京海上日動グループ	金融	委託先会計事務所（高野総合会計事務所）がランサムウェア攻撃を受け、グループ3社が契約する顧客情報を含めた個人情報が漏えいした可能性
2024年6月	高野総合会計事務所	サービス	通信機器の設定不備を起因とした不正アクセスによりランサムウェア攻撃を受け、取引先保有の個人情報を含むデータサーバの一部が暗号化
2024年5月	岡山県精神科医療センター	医療 （独立行政法人）	ランサムウェアによるサイバー攻撃を受け、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
2024年3月	日本商工会議所	経済団体	小規模事業者持続化補助金の事務局のサーバが不正アクセス攻撃を受け、データの一部を滅失および暗号化させるランサムウェア被害が発生 データの流出等は確認されていない

ランサムウェア被害事例

年月	組織名	業種	概要
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が漏えいした可能性
2024年6月	高野総合会計事務所	サービス	通信機器の設定不備を起因とした不正アクセスによりランサムウェア攻撃を受け、取引先保有の個人情報を含むデータサーバの一部が暗号化
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
2024年3月	日本商工会議所	経済団体	小規模事業者持続化補助金の事務局のサーバが不正アクセス攻撃を受け、データの一部を滅失および暗号化させるランサムウェア被害が発生 データの流出等は確認されていない

ランサムウェアの現状と脅威

従来のランサムウェアの手口



- 不特定多数へメール送信
- 主にクライアントPCを攻撃
- PCのロック、データ暗号化

● 暗号化解除等の見返りに身代金要求

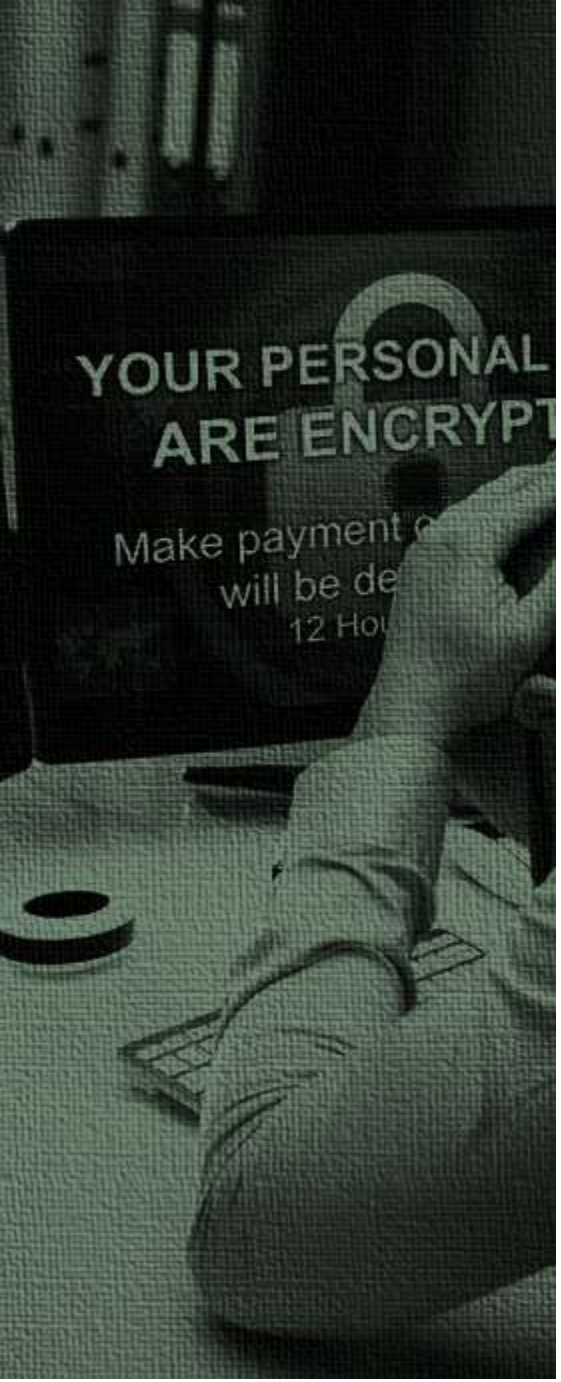
新たなランサムウェアの手口

- メールのほかVPN機器の脆弱性を狙う
- サーバー、制御系システム、クライアントPCを攻撃
- 管理者権限を奪取、ファイルサーバーやクライアントPCのデータの暗号化や窃取

二重恐喝！
（ダブルエクストーション）

● データの復号化の見返りに身代金要求、
● 窃取データの公開を止めるための身代金要求
● 窃取データのダークサイトでの販売

政府広報オンライン.「ランサムウェア、あなたの会社も標的に？　被害を防ぐためにやるべきこと」.
https://www.gov-online.go.jp/useful/article/202210/2.html



Agenda

自己紹介

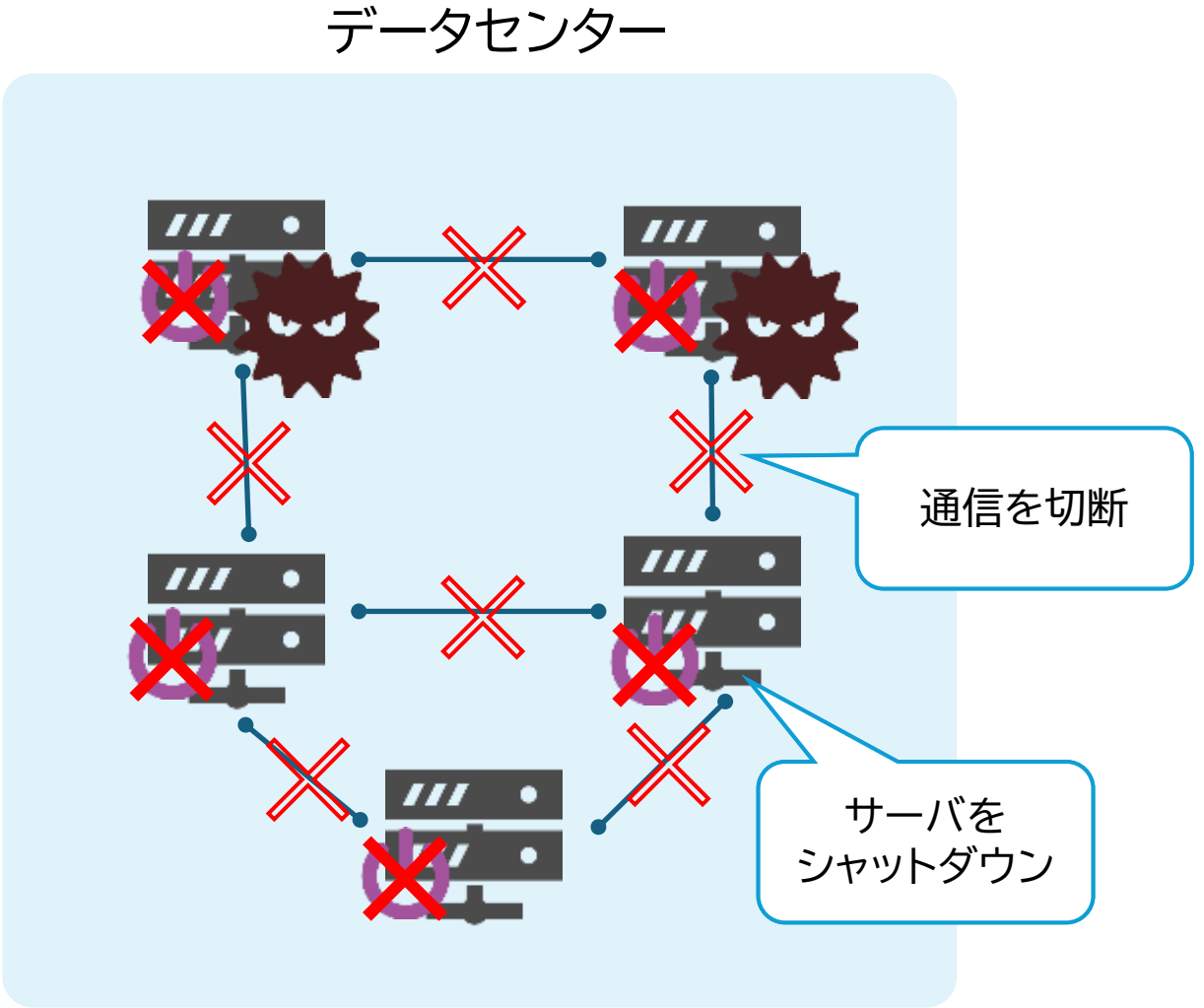
昨今のランサムウェア事情

大手出版社事例考察

まとめ

大手出版社事例概要

- 2024年6月14日、株式会社KADOKAWAがランサムウェアを含むサイバー攻撃を受けたことを発表
- 被害の拡大を防ぐために同社のデータセンター内サーバ間通信の切断およびサーバのシャットダウンを実施
- 社内ネットワークへも被害が及んでいることを確認し、社内業務を一部停止、社内ネットワークへのアクセスを禁止
- パブリッククラウド上のデータは侵害を受けていない
- 同月28日、一部取引先や社内情報に関する情報の漏えいを発表



株式会社ドワンゴ.「当社サービスへのサイバー攻撃に関するご報告とお詫び」.
https://dwango.co.jp/news/5131439897051136/
株式会社KADOKAWA.「ランサムウェア攻撃による情報漏洩に関するお知らせとお詫び」.
https://tp.kadokawa.co.jp/.assets/240628_release_f1wyy3RN.pdf

時系列の整理

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および補償について発表 ニコニコ動画（Re:仮）をリリース
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
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

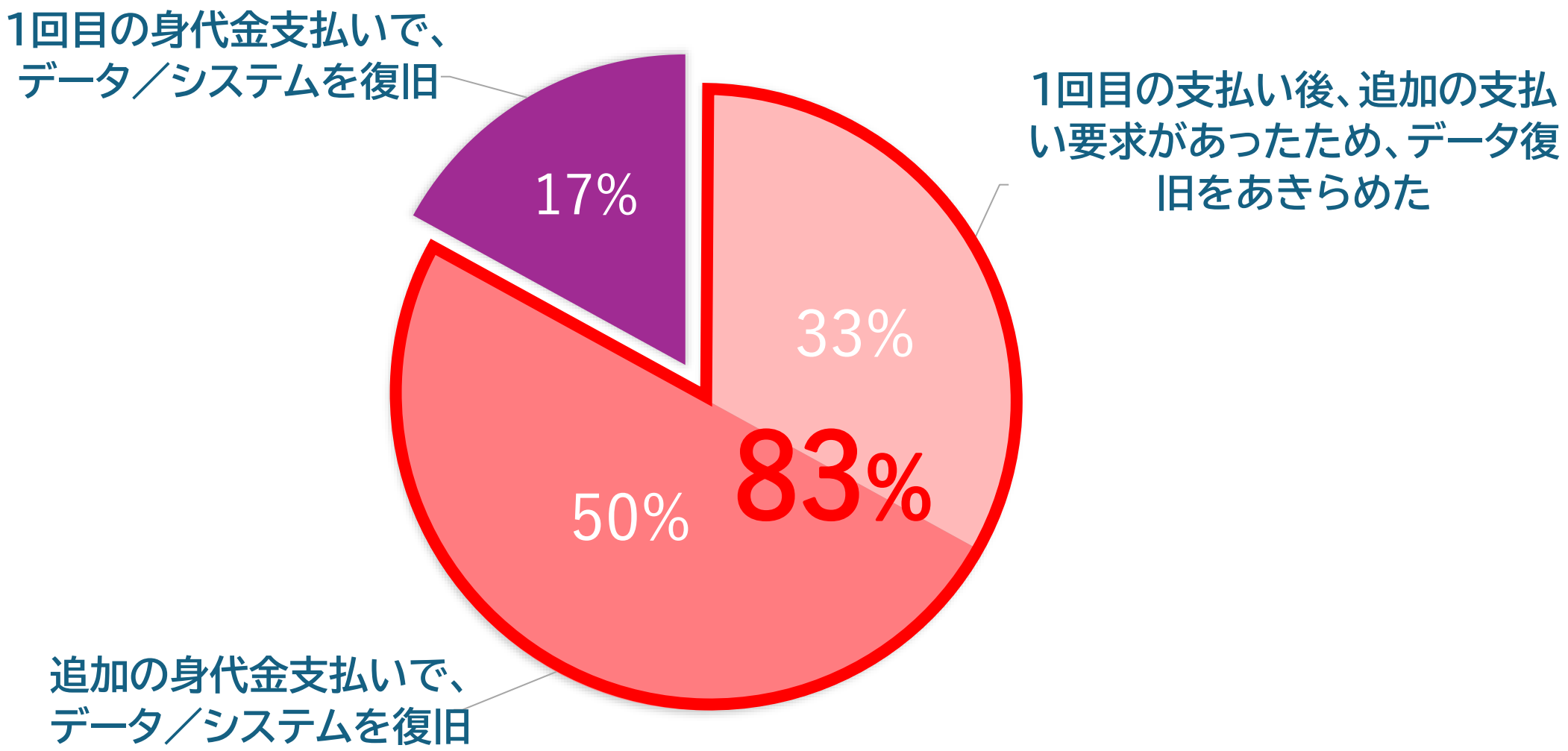
身代金の支払いについて

JPCERT/CC曰く…

⇒　支払うべきではない

JPCERT/CC.「侵入型ランサムウェア攻撃を受けたら読むFAQ」.
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

身代金の支払いについて



proofpoint.「身代金を支払わない結果、日本のランサムウェア感染率は減少？ ランサムウェア感染率/身代金支払率15か国調査 2024」.
https://www.proofpoint.com/jp/blog/threat-insight/japan-ransomware-payment-result-2024

時系列の整理

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） ドワンゴ社よりニコニコシステムの復旧および補償について発表 ニコニコ動画（Re:仮）をリリース
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社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
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

犯行声明

KADOKAWA Corporation

Website

Our team gained access to the Kadokawa network almost a month ago. It took some time, because of the language, to figure out that Kadokawa subsidiaries' networks were connected to each other and to get through all the mess Kadokawa's IT department made there. We have discovered that Kadokawa networks architecture was not organised properly. It was different networks connected to the one big Kadokawas infrastructure being controlled through global control points, such as eSXI and V-sphere. Once we have gained access to the control center we have encrypted the whole network (Dwango, NicoNico, Kadokawa, other subsidiaries).

The second part of our Team downloaded about TB1,5 of data from the networks.

Quickscope of downloaded data:

-contracts

-DocuSigned papers

-various legal papers

-platform users related data (emails, data usage, links opened, etc)

-employee related data (personal info, payments, contracts, emails, etc)

-business planning (presentations, emails, offers, etc)

-projects related data (coding, emails, payments, etc)

-financial data (payments, transfers, planning, etc)

-other internal-use-only papers and confidential data

Once the network was encrypted we contacted Kadokawas management to make a deal with them regarding data protection and network decryption.

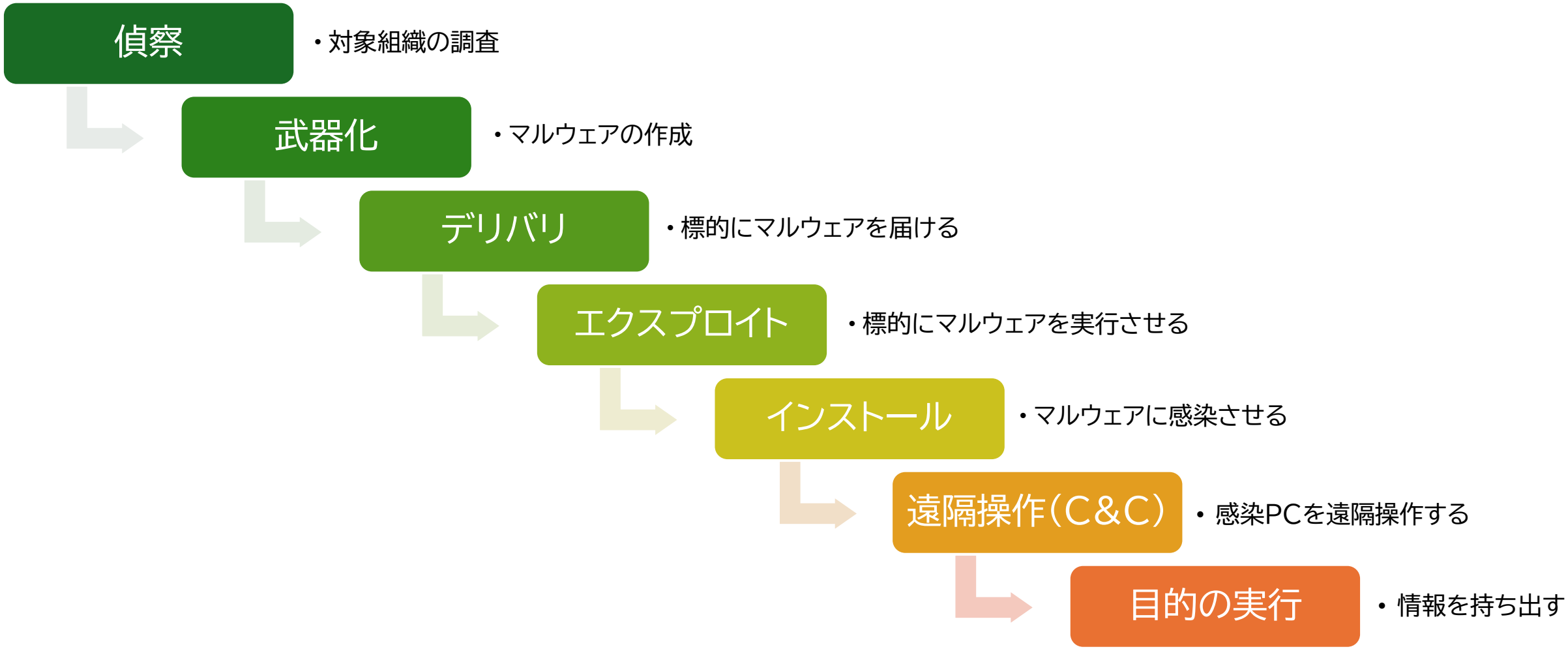
As everyone can see the company is suffering right now and its business processes are being interrupted. Kadokawa and its subsidiaries' services were suspended and the approximate time of recovery was set to the end of July.

It is good to see that Kadokawas management is updating public announcements regarding this situation almost every day. It is very good that Kadokawas management decided to tell the "truth" to calm down the public.

But, it is not good that Kadokawa decided to hide some details. Maybe its own IT department decided not to tell all the truth to its own management, anyways, we can prove Kadokawa statements wrong.

First of all, Kadokawas IT department detected our presence within the network 3 days before we had encrypted the network. Admins tried to kick us out from the network, one of our server IP"s was blocked, they have tried to change admin credentials, but we have managed to set undetectable access to the network. We have continued downloading even after Kadokawa admins detected us. They were unable to detect and stop outgoing traffic, because our downloading scripts kept working even after the server's IP was blocked. 1 day before encryption we have detected enormous Kadokawa admins activity trying to stop us unsuccessfully.

サイバーキルチェーン



時系列の整理

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） ドワンゴ社よりニコニコシステムの復旧および補償について発表 ニコニコ動画（Re:仮）をリリース
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社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
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

時系列の整理

日付	事象
7月2日	ダークウェブ上の犯行声明に新たな情報のダウンロード先とみられるリンクを掲載 犯人の主張を確認し主張内容の信憑性について調査中な旨を発表
7月3日	新たに角川ドワンゴ学園の在校生・卒業生などの個人情報漏えいの可能性が高いことを発表
7月5日	漏洩情報の拡散行為に対する警告と法的措置についてを発表
7月10日	漏洩情報の拡散行為に対する措置ならびに刑事告訴等についてを発表
7月12日	悪質な拡散行為等に対する措置の進捗状況についてを発表 ◆ 悪質と認識した情報拡散行為等の件数（7月10日時点） ■ 株式会社ドワンゴ：420件（X:133件／5ちゃんねる:237件／まとめサイト:26件/Discord・その他:24件） ■ 学校法人KADOKAWAドワンゴ学園：53件（X:8件／5ちゃんねる:41件／まとめサイト:1件/その他:3件）
7月29日	第4報を発表 事業活動の回復状況についての報告

KADOKAWA.「KADOKAWA Corporation」.
https://tp.kadokawa.co.jp/

考えられる侵入経路

●ネットワーク機器の脆弱性

●標的型メール攻撃

●内部犯行・漏えいした認証情報の利用

Agenda

自己紹介

昨今のランサムウェア事情

大手出版社事例考察

まとめ

まとめ

- ✓ ランサムウェアの被害は拡大している
- ✓ 情報漏えいを伴う二重恐喝と呼ばれる手口が増加している
- ✓ 大手出版社等の事例から見習うべきポイント、反面教師にすべきポイントがある
  → 教訓として自社のセキュリティ対策に役立てていく必要がある

ご清聴ありがとうございました

INFORMATION DEVELOPMENT
〒102-0076 東京都千代田区五番町12番地1 番町会館
サイバーセキュリティ事業本部
03-3262-9171
marketing@idnet.co.jp