2019 年 4 月 26 日

サービス＆セキュリティ株式会社 e-Gate センター

GW（大型連休）に向けたセキュリティ対策

1. 概要

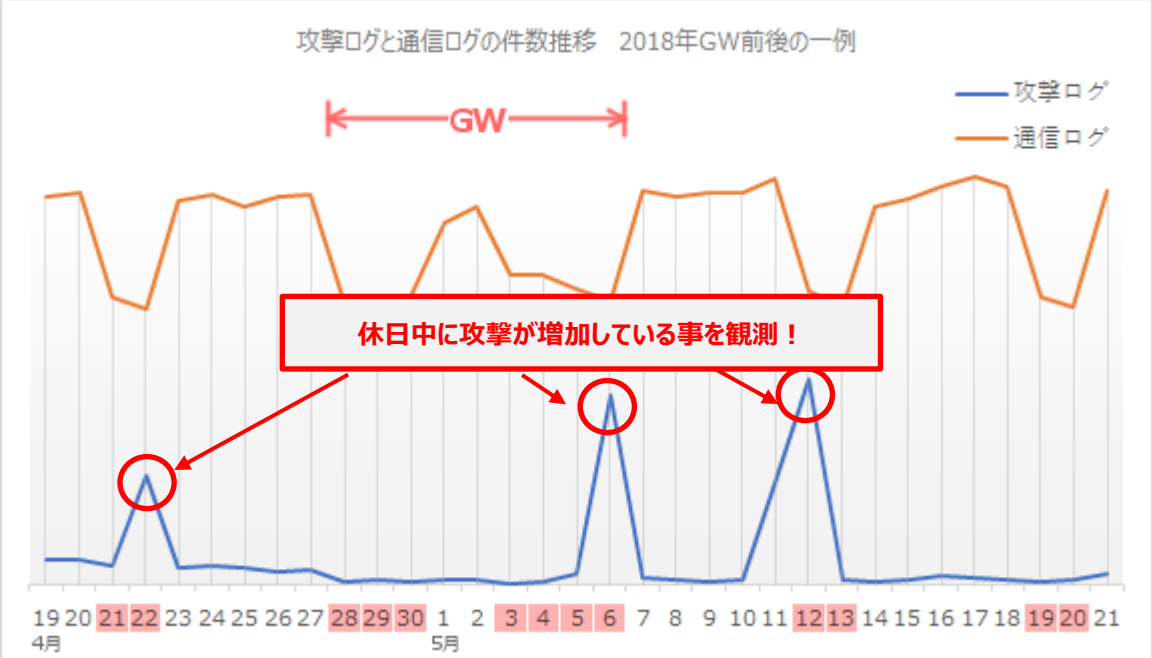
2019 年のゴールデンウィークは 4 月 27 日から 5 月 6 日まで、10 日間の大型連休となる企業が多くなりました。稀に見る大型連休に備えて、社内システムの運用の観点から実施可能なセキュリティ対策をご紹介いたします。

ここで紹介する対策はこの度の連休だけに限らず、日々のセキュリティ運用にも共通する内容となっているため、連休を過ぎてからも基本事項の確認のために是非ご参照ください。

2. 休日中の脅威発生状況

e-Gate センターでは、24 時間体制で日々セキュリティログの監視を行っています。

IPS や UTM の監視においては、主に外部からの脅威発生を検知することが可能です。昨年のゴールデンウィークにおいて、外的脅威の発生が観測された一例として、ある UTM におけるログ量の統計情報を示します。



【図 1 攻撃ログと通信ログの件数推移 2018 年 GW 前後の一例】

この例では、通信ログは業務通信の量を反映して、平日には多く、休日には少なくなっています。

一方で、攻撃を検知した際に発せられる攻撃ログは、休日と関係なく週に 1 日程度の頻度で検知数が跳ね上がっています。検知数は攻撃の種類によっても変化するため、ログ件数がそのまま危険性を示すわけではありませんが、休日・平日の区別なくサイバー攻撃が発生することがわかります。

このように、外部からの攻撃は休日であっても発生するため、インシデント対応の体制は常に必要です。

3. 長期休暇に特有の社内状況

ゴールデンウィークのような長期休暇においては、通常とは違った社内状況があり、システム運用上の脆弱性が発生します。

（１）社内システムの利用者が減少し、使用されないシステムがある

通常、社内の各システムはそれぞれに利用者がいます。システム上の異変が生じた場合には、利用者が真っ先に発見することも多いですが、長期休暇で利用者がいないような状況では発見が遅れ、被害が拡大する恐れがあります。

（２）ノート PC 等、機密データを保持する機器の持ち出しがある

長期休暇の期間にも社外でいくらかの業務を行うため、ノート PC 等の機器の持ち出しをするケースがあります。それらの機器には多少なりとも機密データが保持されていると考えられるため、紛失、盗難、機密情報の漏洩といったリスクが発生します。

（３）社員間の連絡が取りにくく、社内ルールの確認などが困難になる

休暇中は社員がばらばらになるため、何かあった際にも社内ルールの確認などが困難になります。特にゴールデンウィークの時期は ４ 月から部署異動で配属されたメンバーや新入社員などが十分に社内ルールを把握できていないことも想定されます。上記の持ち出し機器に関しても、持ち出した当人が理解していなければ運用ルールが守られず、危険な状態になります。

（４）システム担当者へ連絡が取りにくい

システム担当者も長期休暇に入るため、連絡が取りにくくなる可能性があります。トラブルが発生してもシステム担当者に連絡がつかず、適切な対処がされないまま被害が拡大するといった危険性があります。

（５）システム担当者のインシデント対応が遅れる

システム担当者に連絡がついた場合でも、遠隔地では対応が難しいという可能性もあります。担当者が戻ってから対応ということになると、上記と同じく、被害が拡大する危険性があります。

（６）未確認のメールが累積する

長期休暇の間に、各アカウントへのメールが累積することが想定されます。ユーザーは１つ１つのメールに対する注意が薄れ、標的型攻撃メールの添付ファイルや URL を不用意に開いてしまうといったトラブル発生の可能性が高まります。

（７）各種ソフトウェアの更新が滞る

システムの利用者や管理者が不在の期間は、各種ソフトウェアの更新が滞ることが想定されます。各端末や各サーバの OS、ミドルウェア、アプリケーションなど、それぞれに脆弱性を解消する修正パッチなどが出ている可能性もあるため、アップデートされていない状態は好ましくありません。また、セキュリティソフトの定義情報がアップデートされない場合も、危険性が高くなると言えます。

4. 長期休暇前後に実施すべき対策

各社内状況（脆弱性）に対する対策と、その実施時期は次の通りです。

項番	脆弱性	対策
1	社内システムの利用者が減少し、使用されないシステムがある	① 機器の電源を落とす
2	ノートPC等、機密データを保持する機器の持ち出しがある	② 事前にルールの周知を徹底する ⑤ ルールに従って運用する
3	社員間の連絡が取りにくく、社内ルールの確認などが困難になる	
4	システム担当者へ連絡が取りにくい	③ 社内の連絡体制を明確にする
5	システム担当者のインシデント対応が遅れる	④ 緊急対応の体制を確認しておく
6	未確認のメールが累積する	⑥ メール攻撃への注意喚起を行う
7	各種ソフトウェアの更新が滞る	⑦ ソフトウェアのアップデートを行う ⑧ 定義ファイルの更新を行う ⑨ 通信量の増大に注意する

【図２　長期休暇の脆弱性に対する対策】

【長期休暇前の対策】

① 使用しない機器の電源を落とす

不要な機器の電源を落としておくことであらかじめリスクの低減を図ることが可能です。休暇中に使用しない PC、サーバ、ネットワーク機器などを確認し、可能であれば電源を切ることを検討しましょう。

② セキュリティルールの周知を徹底する

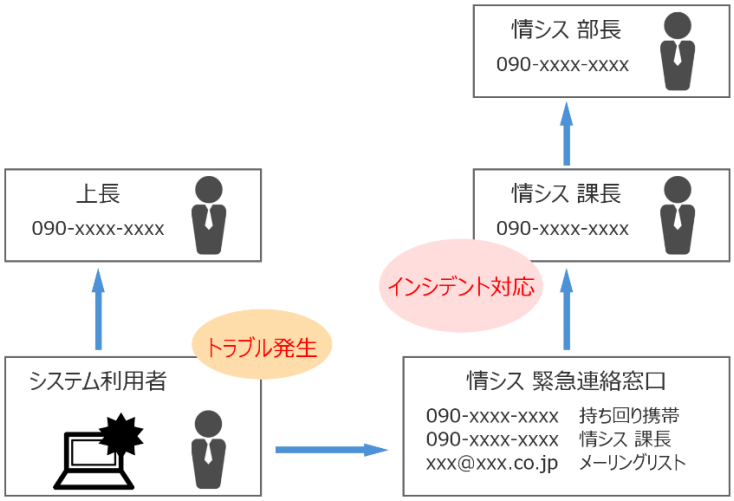
全社的にセキュリティルールや運用ルールの周知を徹底し、休暇中にも個人個人がルールを把握できているように準備しましょう。その中には持ち出し機器に関するルールも含まれるはずです。

③ 社内の連絡体制を明確にする

トラブルが発生したときにどこに連絡すればいいのかといったことを明確にし、社内で共有しましょう。特にシステム関連は緊急連絡の窓口を設けて、その連絡先を周知することで、ユーザーが迷いなく連絡してくれるようになります。

④ システム担当者の緊急対応の体制を確認する

システム担当者として対応できるメンバーの中で互いに休日中の状況を確認し、だれが対応できるのかを確認しておくことで、インシデント発生時に速やかに対応することができます。



【図３ トラブル時の連絡体制の一例】

【休暇中の対策】

⑤ 社内ルールに従って運用する

休暇中は、事前に取り決めたルールに従って行動し、トラブルにも冷静に対応しましょう。

【長期休暇後の対策】

⑥ メール攻撃への注意喚起を行う

システム部や各部署の上長から注意喚起を行い、怪しいメールの添付ファイルを開かないといった基本的な対策について意識向上を図ることで、セキュリティインシデントの予防になります。

⑦ 各種ソフトウェアのアップデートを実施する

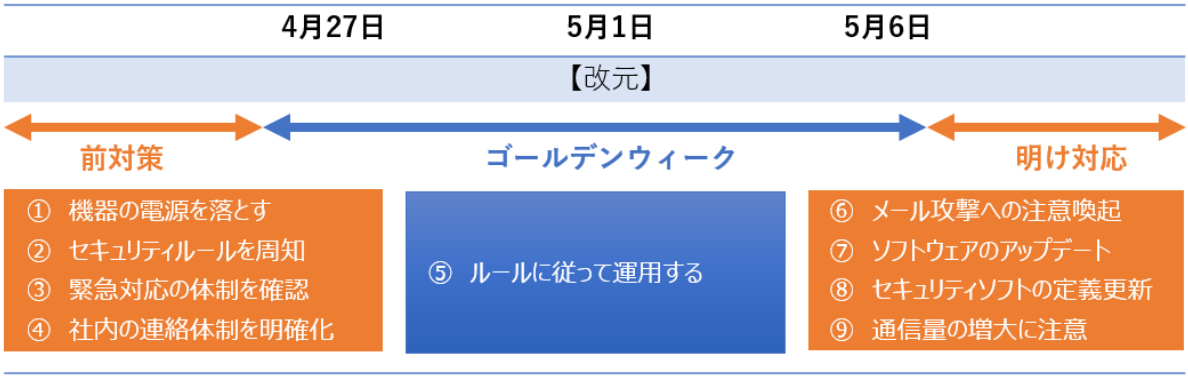
保留されていた OS、ミドルウェア、アプリケーションの更新を速やかに行いましょう。

⑧ セキュリティ製品の定義ファイルを更新する

OS 等の基盤の更新のあとにはセキュリティソフトの定義ファイルも更新が必要です。

⑨ ネットワークの通信量の増大に注意する

累積したメールの配信や、上記のようなソフトウェアの更新が全社のクライアントにおいて行われると、ネットワークの通信量が増大し、帯域がひっ迫する可能性があります。リスクが見込まれる場合は、あらかじめアップデート処理を分散させる等の対策をとる必要があります。



【図４　対策の実施タイミング】

なお、これらの内容は、日々のセキュリティ対策の運用と変わるものではありません。大型連休というリスクの高まる時期に、こうして基本的な対策を確認し、日々のセキュリティ対策へとつなげていくことが望まれます。

5. 改元に伴う脅威増大の可能性について

今年はゴールデンウィーク中に改元があり、元号が平成から令和へと改められます。これに乗じたサイバー攻撃が発生する可能性があるため、注意が必要です。一般的なセキュリティ対策と変わるものではありませんが、セキュリティ情報の収集を行って必要な対策を確認してください。

また、改元に関してはシステムトラブルの可能性が話題になっていますが、個別のシステム障害が発生した場合にはセキュリティインシデントにつながらないかの確認も必要です。前述のとおり、取り決めた連絡体制や緊急対応の体制に従って対応を実施してください。

6. e-Gate の監視サービスについて

以上の長期休暇における対策を行ったうえで、よりセキュリティ対策を強固にするために、”e-Gate”の MSS の導入をご検討ください。e-Gate サービスではゴールデンウィークなどの長期休暇においても、24 時間 365 日で監視を行います。

サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。“e-Gate“のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

■総合セキュリティサービス 「e-Gate」

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。

※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp